NSX-T Data Center 安装指南

修改日期：2020 年 2 月 28 日
VMware NSX-T Data Center 2.4

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

https://docs.vmware.com/tw/

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目錄

NSX-T Data Center 安裝指南 7

1 NSX-T Data Center 概觀 8
主要概念 9
NSX Manager 概觀 11

2 NSX-T Data Center 安裝工作流程 14
適用於 vSphere 的 NSX-T Data Center 工作流程 14
適用於 KVM 的 NSX-T Data Center 安裝工作流程 15
裸機伺服器的 NSX-T Data Center 組態工作流程 15

3 準備安裝 17
系統需求 17
NSX Manager 虛擬機器系統需求 17
NSX Edge 虛擬機器系統需求 20
NSX Edge 裸機需求 21
裸機伺服器系統需求 22
裸機 Linux 容器需求 23
連接埠和通訊協定 23
NSX Manager 所使用的 TCP 和 UDP 連接埠 25
NSX Edge 所使用的 TCP 和 UDP 連接埠 26
由 ESXi、KVM 主機和裸機伺服器使用的 TCP 和 UDP 連接埠 27
安裝 NSX-T Data Center 元件 28
NSX Manager 安裝 28
NSX Edge 安裝 31

4 在 vSphere 上安裝 NSX-T Data Center 34
安裝 NSX Manager 和可用應用裝置 34
使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager 36
將 NSX-T Data Center 設定為在開機時顯示 GRUB 功能表 41
登入新建立的 NSX Manager 42
新增計算管理程式 42
從使用者介面部署 NSX Manager 節點以形成叢集 44
設定叢集的虛擬 IP (VIP) 位址 48
使用 vSphere GUI 在 ESXi 上安裝 NSX Edge 49
使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge 51

5 在 KVM 上安裝 NSX-T Data Center 56
設定 KVM 56
在 KVM CLI 中管理您的客體虛擬機器 61
在 KVM 上安裝 NSX Manager 62
登入新建立的 NSX Manager 65
在 KVM 主機上安裝第三方套件 66
確認 RHEL KVM 主機上的 Open vSwitch 版本 67
使用 CLI 部署 NSX Manager 節點以形成叢集 68
使用 ISO 檔案或 PXE 安裝 NSX Edge 69
透過 ISO 檔案將 NSX Edge 安裝為虛擬應用裝置 69
透過 ISO 檔案在裸機上安裝 NSX Edge 72
在 PXE 伺服器上安裝 NSX Edge 75

6 設定裸機伺服器以使用 NSX-T Data Center 80
在裸機伺服器上安裝第三方套件 80
建立裸機伺服器工作負載的應用程式介面 82

7 設定 NSX Manager 叢集 83
NSX Manager 叢集需求 83
單一站台、雙站台和多個站台的 NSX Manager 叢集需求 83

8 傳輸區域和傳輸節點 87
建立傳輸區域 87
為通道端點 IP 位址建立 IP 集區 89
增強型資料路徑 91
設定設定檔 93
建立上行設定檔 93
設定 Network I/O Control 設定檔 96
新增 NSX Edge 叢集設定檔 105
新增 NSX Edge 橋接器設定檔 106
新增傳輸節點設定檔 106
VMkernel 移轉至 N-VDS 交換器 109
VMkernel 移轉錯誤 113
建立獨立主機或裸機伺服器傳輸節點 116
設定受管理的主機傳輸節點 122
為 ESXi 主機傳輸節點設定連結彙總 123
完全折疊的 vSphere 叢集 NSX-T 部署 124
確認傳輸節點狀態 134
N-VDS 的視覺表示 136
NSX-T Data Center 核心模組的手動安裝 138

在 ESXi Hypervisor 上手動安裝 NSX-T Data Center 核心模組 138
在 Ubuntu KVM Hypervisor 上手動安裝 NSX-T Data Center 核心模組 140
在 RHEL 和 CentOS KVM Hypervisor 上手動安裝 NSX-T Data Center 核心模組 142
NSX Edge 網路設定 143
建立 NSX Edge 傳輸節點 148
建立 NSX Edge 叢集 150

9 自動部署無狀態叢集 152
自動部署無狀態叢集的高階工作 152
必要條件和支援的版本。 153
建立無狀態主機的自訂映像設定檔 153
將自訂映像與參考和目標主機建立關聯 155
設定參考主機上的網路組態 156
將參考主機設定為 NSX-T 中的傳輸節點 157
擷取並驗證主機設定檔 159
驗證主機設定檔與無狀態叢集的關聯 160
更新主機自訂 161
在目標主機上觸發自動部署 162
在套用 TNP 前將主機重新開機 162
在無狀態叢集上套用 TNP 163
在套用 TNP 後將主機重新開機 165
無狀態主機位於目標叢集中的案例 166
無狀態主機位於目標叢集外時的案例 167
對主機設定檔和傳輸節點設定檔進行疑難排解 169

10 從主機傳輸節點中解除安裝 NSX-T Data Center 171
確認用於解除安裝的主機網路對應 171
從 vSphere 叢集中解除安裝 NSX-T Data Center 173
從 vSphere 叢集中的主機上解除安裝 NSX-T Data Center 173
從獨立主機中解除安裝 NSX-T Data Center 174

11 安裝 NSX Cloud 元件 176
NSX Cloud 架構和元件 176
為公有雲安裝和設定 NSX Cloud 元件的概觀 178
將 NSX Cloud 與公有雲連線的 0 天工作流程 178
安裝 CSM 並連線 NSX Manager 178
安裝 CSM 179
將 CSM 加入 NSX Manager 179
(選用) 設定 Proxy 伺服器 180
(選用) 設定適用於 Cloud Service Manager 的 vIDM 180
連線公有雲與內部部署 181

針對混合連線啟用對 CSM 上的連接埠和通訊協定的存取 181
將 Microsoft Azure 網路與內部 NSX-T Data Center 部署連線 182
將 Amazon Web Services (AWS) 網路與內部 NSX-T Data Center 部署連線 183
新增公有雲帳戶 184
設定 Microsoft Azure 詳細目錄的安全存取權 184
設定 AWS 詳細目錄的安全存取權 190
部署或連結 NSX Public Cloud Gateway 193
在自行管理或傳送 VNet 中部署 PCG 195
在自行管理或傳送 VPC 中部署 PCG 196
連結至傳送 VPC 或 VNet 198
自動建立的邏輯實體和雲端原生安全群組 199
取消部署 PCG 203
取消標記公有雲中的虛擬機器 204
停用隔離原則 (如已啟用) 205
刪除使用者建立的邏輯實體 205
從 CSM **取消部署** 206

NSX-T Data Center 安裝指南

《NSX-T Data Center 安裝指南》說明了如何安裝 VMware NSX-T™ Data Center 產品。其中的資訊包含逐步組態指示和建議的最佳做法。

主要對象

此資訊適用於要安裝或使用 NSX-T Data Center 的任何人。本資訊是專為具有經驗且熟悉虛擬機器技術和網路虛擬化概念的系統管理員而撰寫的。

技術出版品詞彙表

VMware 技術出版品將為您提供可能不熟悉的術語詞彙。如需 VMware 技術說明文件中所用專有詞彙的定義，請前往 http://www.vmware.com/support/pubs。

NSX-T Data Center 概觀

1

比照伺服器虛擬化透過編寫程式來建立和管理虛擬機器的方式，NSX-T Data Center 網路虛擬化也會透過編寫程式來建立和管理軟體型虛擬網路。

透過在功能上等同於網路 Hypervisor 的網路虛擬化，我們可在軟體中重現一組完整的第 2 層至第 7 層網路服務 (例如，交換、路由、存取控制、防火牆、服務品質)。因此，這些服務可透過程式設計的方式任意組合，在短短數秒內產生唯一且隔離的虛擬網路。

NSX-T Data Center 的運作方式是實作三個區隔開來但整合在一起的平面：管理、控制和資料。這些平面可實作為一組存在於兩種類型節點上的程序、模組和代理程式：NSX Manager 和傳輸節點。

- 每個節點各自裝載一個管理平面代理程式。
- NSX Manager 節點會裝載 API 服務和管理平面叢集精靈。
- NSX Controller 節點會裝載中央控制平面叢集精靈。
- 傳輸節點會裝載本機控制平面精靈和轉送引擎。

NSX Manager 提供三節點叢集支援，可合併節點叢集上的原則管理員、管理和中央控制服務。NSX Manager 叢集提供使用者介面和 API 的高可用性。聚合管理節點和控制平面節點可減少必須由 NSX-T Data Center 管理員部署及管理的虛擬應用裝置的數目。

NSX Manager 應用裝置針對不同的部署情況提供三種不同的大小。小型應用裝置適用於實驗室或概念證明部署。中型應用裝置適用於最多 64 台主機的部署，大型應用裝置適用於部署到大規模環境的客戶。請參閱 NSX Manager 虛擬機器系統需求和組態上限工具。

本章節討論下列主題：

- 主要概念
- NSX Manager 概觀

主要概念

用於說明文件和使用者介面中的一般 NSX-T Data Center 概念。

計算管理程式	計算管理程式是一種可管理主機和虛擬機器等資源的應用程式。其中一個範例為 vCenter Server。
控制平面	根據管理平面中的組態計算執行階段狀態。控制平面會散佈數據平面元素所報告的拓撲資訊，以及將無狀態組態推送至轉送引擎。
數據平面	根據控制平面所填入的表格，執行封包的無狀態轉送或轉換。資料平面會將拓撲資訊報告至控制平面，並保留封包層級的統計資料。
外部網路	未受 NSX-T Data Center 管理的實體網路或 VLAN。您可以連結您的邏輯網路，或透過 NSX Edge 將網路覆疊至外部網路。例如，客戶資料中心內的實體網路，或實體環境中的 VLAN。
網狀架構節點	已向 NSX-T Data Center 管理平面登錄、且已安裝 NSX-T Data Center 模組的主機。Hypervisor 主機或 NSX Edge 若要成為 NSX-T Data Center 覆疊的一部分，則必須新增至 NSX-T Data Center 網狀架構中。
邏輯連接埠出口	離開虛擬機器或邏輯網路的輸出網路流量稱為出口流量，因為流量離開虛擬網路並進入資料中心。
邏輯連接埠入口	離開資料中心並進入虛擬機器的輸入網路流量稱為入口流量。
邏輯路由器	NSX-T Data Center 路由實體。
邏輯路由器連接埠	您的邏輯交換器連接埠所能連結到的邏輯路由器連接埠，或實體網路的上行連接埠。
邏輯交換器	為虛擬機器介面和閘道介面提供虛擬第 2 層交換的實體。邏輯交換器可為承租人網路管理員提供在邏輯上等同於實體第 2 層交換器的項目，而讓他們能夠將一組虛擬機器連線至通用的廣播網域。邏輯交換器是獨立於實體 Hypervisor 基礎結構以外、且跨多個 Hypervisor 的邏輯實體，可連線至位於任何實體位置的虛擬機器。 在多承租人雲端中，許多邏輯交換器可能會並存於相同的 Hypervisor 硬體上，但其各自的第 2 層區段則彼此隔離。邏輯交換器可使用邏輯路由器來連線，而邏輯路由器可提供連線至外部實體網路的上行連接埠。
邏輯交換器連接埠	用來建立虛擬機器網路介面或邏輯路由器介面之連線的邏輯交換器連結點。邏輯交換器連接埠會報告已套用的交換設定檔、連接埠狀態和連結狀態。
管理平面	提供系統的單一 API 進入點、持續保存使用者組態、處理使用者查詢，以及執行系統中的所有管理、控制和資料平面節點的運作工作。管理平面也負責查詢、修改及持續保存使用組態。
NSX Edge 叢集	與涉及高可用性監控之通訊協定使用相同設定的 NSX Edge 節點應用裝置集合。

NSX Edge 節點	用途為提供 IP 路由和 IP 服務功能所需之運算能力的元件。
NSX 管理的虛擬 Distributed Switch 或 KVM Open vSwitch	NSX 管理的虛擬 Distributed Switch (N-VDS，以前稱為主機交換器) 或 OVS 用於共用 NSX Edge 和計算叢集。覆疊流量設定需要 N-VDS。 N-VDS 具有兩種模式：標準和增強型資料路徑。增強型資料路徑 N-VDS 具有支援 NFV (網路功能虛擬化) 工作負載的效能功能。
NSX Manager	主控 API 服務、管理平面和代理程式服務的節點。NSX Manager 是一種包含在 NSX-T Data Center 安裝套件中的應用裝置。您可以使用 nsx-manager nsx-controller 或 nsx-cloud-service-manager 角色來部署應用裝置。目前，應用裝置一次僅支援一個角色。
NSX Manager 叢集	可提供高可用性的 NSX Manager 的叢集。
Open vSwitch (OVS)	可在 XenServer、Xen、KVM 和其他 Linux 系統的 Hypervisor 內做為虛擬交換器的開放原始碼軟體交換器。
覆疊邏輯網路	使用「第 3 層中的第 2 層」通道實作的邏輯網路，可讓虛擬機器所看見的拓撲能夠與實體網路的拓撲分離。
實體介面 (pNIC)	Hypervisor 安裝所在之實體伺服器上的網路介面。
區段	為虛擬機器介面和閘道介面提供虛擬第 2 層交換的實體。區段可為承租人網路管理員提供邏輯上等同的實體第 2 層交換器，允許其將一組虛擬機器連線至一般廣播網域。區段是獨立於實體 Hypervisor 基礎結構以外、且跨多個 Hypervisor 的邏輯實體，可連線位於任何實體位置的虛擬機器。區段也稱為邏輯交換器。 在多承租人雲端中，許多區段可能會並存於相同的 Hypervisor 硬體上，但其各自的第 2 層區段則彼此隔離。可使用提供外部實體網路連線的閘道連線區段。
第 0 層閘道或第 0 層邏輯路由器	第 0 層閘道在**進階網路與安全性**索引標籤中稱為第 0 層邏輯路由器。它會與實體網路連線，並且可實現為主動-主動或主動-待命叢集。第 0 層閘道會執行 BGP，並且與實體路由器對等。在主動備用模式下，閘道也可提供可設定狀態的服務。
第 1 層閘道或第 1 層邏輯路由器	第 1 層閘道在**進階網路與安全性**索引標籤中稱為第 1 層邏輯路由器。它連線至一個第 0 層閘道進行北向連線，並連線至一或多個覆疊網路進行南向連線。第 1 層閘道可以是提供可設定狀態之服務的主動備用叢集。
傳輸區域	定義邏輯交換器之最大跨距的傳輸節點集合。一個傳輸區域代表一組以類似方式佈建的 Hypervisor，以及連接這些 Hypervisor 上虛擬機器的邏輯交換器。
傳輸節點	能夠參與 NSX-T Data Center 覆疊或 NSX-T Data Center VLAN 網路的節點。對於 KVM 主機，您可以預先設定 N-VDS，或者您可以讓 NSX Manager 執行組態。對於 ESXi 主機，則 NSX Manager 一律會設定 N-VDS。

上行設定檔	定義從 Hypervisor 主機到 NSX-T Data Center 邏輯交換器的連結，或是從 NSX Edge 節點到 Top-of-Rack 交換器之連結的原則。上行設定檔所定義的設定可能會包含整併原則、主動/待命連結、傳輸 VLAN 識別碼和 MTU 設定。在上行設定檔中設定的傳輸 VLAN 只會標記覆疊流量，而 TEP 端點會使用 VLAN 識別碼。
虛擬機器介面 (vNIC)	虛擬機器上提供虛擬客體作業系統與標準 vSwitch 或 vSphere Distributed Switch 之間連線功能的網路介面。vNIC 也可以連結至邏輯連接埠。您可以根據其唯一識別碼 (UUID) 來識別 vNIC。
虛擬通道端點	每個 Hypervisor 都有一個虛擬通道端點 (VTEP)，負責封裝 VLAN 標頭中的虛擬機器流量並將封包路由至目的地 VTEP 進行進一步處理。流量可以路由至不同主機上的另一個 VTEP 或 NSX Edge 閘道以存取實體網路。

NSX Manager 概觀

NSX Manager 提供可讓您管理 NSX-T 環境的 Web 型使用者介面。它也會主控處理 API 呼叫的 API 伺服器。

NSX Manager Web 介面提供了兩種用來設定資源的方法。

- 原則介面：**網路**、**安全性**、**詳細目錄**和**計劃和疑難排解**索引標籤。
- 進階介面：**進階網路與安全性**索引標籤。

原則或進階介面的使用時機

請與您使用的使用者介面保持一致。您會基於幾種原因而選擇使用其中一個使用者介面。

- 如果您要使用 NSX-T Data Center 2.4 或更新版本來部署新環境，在多數情況下，最好的選擇是使用新的原則型使用者介面來建立和管理環境。
  - 某些功能在原則型使用者介面中無法使用。如果您需要這些功能，請使用進階使用者介面來進行所有組態設定。
- 如果您要升級至 NSX-T Data Center 2.4 或更新版本，請繼續使用**進階網路與安全性**使用者介面來進行組態變更。

表 1-1. 原則或進階介面的使用時機

原則介面	進階介面
多數的新部署都應使用原則型介面。	以前使用進階介面所建立的部署，例如，從原則型介面出現之前的版本進行升級。
NSX Cloud 部署	與其他外掛程式整合的部署。例如，NSX Container Plug-in、OpenStack 和其他雲端管理平台。

表 1-1. 原則或進階介面的使用時機 (續)

原則介面	進階介面
僅在原則介面中可用的網路功能： ■ DNS 服務和 DNS 區域 ■ VPN ■ NSX Cloud 的轉送原則	僅在進階介面中可用的網路功能： ■ IPv4 和 IPv6 的第 3 層轉送 ■ 轉送累計計時器 ■ 變更內部傳送網路 IP ■ 第 0 層的 VIP HA 支援 ■ 待命重新放置 ■ 根據第 1 層上的首碼清單的路由通告篩選 ■ 回送建立 ■ BGP MultiHop ■ BGP 來源位址 ■ 以 BFD 和介面作為下一個躍點的靜態路由 ■ 中繼資料 Proxy ■ 連結至隔離區段和靜態繫結的 DHCP 伺服器
僅在原則介面中可用的安全性功能： ■ 端點保護 ■ 網路自我檢查 (東西向服務插入) ■ 內容設定檔 ■ L7 應用程式 ■ FQDN ■ 新增分散式防火牆和閘道防火牆配置 ■ 類別 ■ 自動服務規則	僅在進階介面中可用的安全性功能： ■ 能夠啟用或停用分散式防火牆、身分識別防火牆和閘道防火牆 ■ 分散式防火牆工作階段計時器 ■ 排除清單 ■ CPU 和記憶體臨界值 ■ 無狀態規則的區段 ■ 橋接防火牆 ■ 區段鎖定 ■ 分散式防火牆規則識別碼 ■ 根據來源和目的地中 IP 所建立的分散式防火牆規則

使用原則介面

如果您決定使用原則介面，請使用此介面來建立所有物件。請勿使用進階介面來建立物件。

您可以使用進階介面來修改已在原則介面中建立的物件。原則所建立物件的設定可能會包含**進階組態**的連結。此連結會將您引導至進階介面，以供您微調組態。您也可以直接在進階介面中檢視原則所建立的物件。若為由原則管理、但顯示在進階介面中的設定，則其旁邊會顯示此圖示：⛔。您無法從進階使用者介面修改這些設定。

哪裡可以找到原則介面和進階介面

原則型介面和進階介面會出現在 NSX Manager 使用者介面的不同部分，且使用不同的 API URI。

表 1-2. 原則介面和進階介面

原則介面	進階介面
■ **網路**索引標籤 ■ **安全性**索引標籤 ■ **詳細目錄**索引標籤 ■ **計劃和疑難排解**索引標籤	**進階網路與安全性**索引標籤
以 `/policy/api` 開頭的 API URI	以 `/api` 開頭的 API URI

備註 **系統**索引標籤可用於所有環境。如果您修改 Edge 節點、Edge 叢集或傳輸區域，則最多可能需要 5 分鐘的時間，原則型使用者介面上才會顯示這些變更。您可以使用 `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload` 來立即同步。

如需如何使用原則 API 的詳細資訊，請參閱 NSX-T 原則 API 入門指南。

在原則介面和進階介面中所建立物件的名稱

您所建立的物件會根據用來建立物件的介面而有不同的名稱。

表 1-3. 物件名稱

使用原則介面所建立的物件	使用進階介面所建立的物件
區段	邏輯交換器
第 1 層閘道	第 1 層邏輯路由器
第 0 層閘道	第 0 層邏輯路由器
群組	NSGroup、IP 集合、MAC 集合
安全性原則	防火牆區段
規則	防火牆規則
閘道防火牆	Edge 防火牆

NSX-T Data Center 安裝工作流程

2

您可以在 vSphere 或 KVM 主機上安裝 NSX-T Data Center。您也可以設定裸機伺服器來使用 NSX-T Data Center。

若要安裝或設定任何 Hypervisor 或裸機，請執行工作流程中建議的工作。

本章節討論下列主題：

- 適用於 vSphere 的 NSX-T Data Center 工作流程
- 適用於 KVM 的 NSX-T Data Center 安裝工作流程
- 裸機伺服器的 NSX-T Data Center 組態工作流程

適用於 vSphere 的 NSX-T Data Center 工作流程

使用檢查清單追蹤 vSphere 主機上的安裝進度。

請遵循建議的程序順序。

1 檢閱 NSX Manager 安裝需求。請參閱 NSX Manager 安裝。

2 設定必要的連接埠和通訊協定。請參閱 連接埠和通訊協定。

3 安裝 NSX Manager。請參閱安裝 NSX Manager 和可用應用裝置。

4 登入新建立的 NSX Manager。請參閱登入新建立的 NSX Manager 。

5 設定計算管理程式。請參閱新增計算管理程式。

6 部署其他 NSX Manager 節點以建立叢集。請參閱從使用者介面部署 NSX Manager 節點以形成叢集。

7 檢閱 NSX Edge 安裝需求。請參閱 NSX Edge 安裝。

8 安裝 NSX Edge。請參閱使用 vSphere GUI 在 ESXi 上安裝 NSX Edge。

9 建立 NSX Edge 叢集。請參閱建立 NSX Edge 叢集。

10 建立傳輸區域。請參閱建立傳輸區域。

11 建立主機傳輸節點。請參閱 建立獨立主機或裸機伺服器傳輸節點或設定受管理的主機傳輸節點。

   系統會在每台主機上建立虛擬交換器。管理平面會將主機憑證傳送至控制平面，且管理平面會將控制平面資訊推送至主機。每個主機會透過顯示其憑證的 SSL 來連線至控制平面。控制平面會根據管理平面所提供的主機憑證來驗證憑證。控制器會在成功驗證時接受連線。

安裝後

當主機成為傳輸節點後，您可以隨時透過 NSX Manager UI 或 API 來建立傳輸區域、邏輯交換器、邏輯路由器和其他網路元件。當 NSX Edge 和主機加入管理平面時，NSX-T Data Center 邏輯實體和組態狀態會自動推送至 NSX Edge 和主機。

如需詳細資訊，請參閱《NSX-T Data Center 管理指南》。

適用於 KVM 的 NSX-T Data Center 安裝工作流程

使用檢查清單追蹤 KVM 主機上的安裝進度。

請遵循建議的程序順序。

1 準備 KVM 環境。請參閱設定 KVM。

2 檢閱 NSX Manager 安裝需求。請參閱 NSX Manager 安裝。

3 設定必要的連接埠和通訊協定。請參閱 連接埠和通訊協定。

4 安裝 NSX Manager。請參閱在 KVM 上安裝 NSX Manager。

5 登入新建立的 NSX Manager。請參閱登入新建立的 NSX Manager 。

6 在 KVM 主機上設定第三方套件。請參閱在 KVM 主機上安裝第三方套件。

7 部署其他 NSX Manager 節點以建立叢集。請參閱使用 CLI 部署 NSX Manager 節點以形成叢集 。

8 檢閱 NSX Edge 安裝需求。請參閱 NSX Edge 安裝。

9 安裝 NSX Edge。請參閱使用 ISO 檔案或 PXE 安裝 NSX Edge。

10 建立 NSX Edge 叢集。請參閱建立 NSX Edge 叢集。

11 建立傳輸區域。請參閱建立傳輸區域。

12 建立主機傳輸節點。請參閱 建立獨立主機或裸機伺服器傳輸節點。

   系統會在每台主機上建立虛擬交換器。管理平面會將主機憑證傳送至控制平面，且管理平面會將控制平面資訊推送至主機。每個主機會透過顯示其憑證的 SSL 來連線至控制平面。控制平面會根據管理平面所提供的主機憑證來驗證憑證。控制器會在成功驗證時接受連線。

安裝後

當主機成為傳輸節點後，您可以隨時透過 NSX Manager UI 或 API 來建立傳輸區域、邏輯交換器、邏輯路由器和其他網路元件。當 NSX Edge 和主機加入管理平面時，NSX-T Data Center 邏輯實體和組態狀態會自動推送至 NSX Edge 和主機。

如需詳細資訊，請參閱《NSX-T Data Center 管理指南》。

裸機伺服器的 NSX-T Data Center 組態工作流程

設定裸機伺服器以使用 NSX-T Data Center 時，使用檢查清單追蹤進度。

請遵循建議的程序順序。

1 檢閱裸機的需求。請參閱裸機伺服器系統需求。

2 設定必要的連接埠和通訊協定。請參閱 連接埠和通訊協定。

3 安裝 NSX Manager。請參閱在 KVM 上安裝 NSX Manager。

4 在裸機伺服器上設定第三方套件。請參閱在裸機伺服器上安裝第三方套件。

5 建立主機傳輸節點。請參閱 建立獨立主機或裸機伺服器傳輸節點。

   系統會在每台主機上建立虛擬交換器。管理平面會將主機憑證傳送至控制平面，且管理平面會將控制平面資訊推送至主機。每個主機會透過顯示其憑證的 SSL 來連線至控制平面。控制平面會根據管理平面所提供的主機憑證來驗證憑證。控制器會在成功驗證時接受連線。

6 建立裸機伺服器工作負載的應用程式介面。請參閱建立裸機伺服器工作負載的應用程式介面。

準備安裝

3

安裝 NSX-T Data Center 之前，請確定您的環境已備妥。

本章節討論下列主題：

- 系統需求
- 連接埠和通訊協定
- 安裝 NSX-T Data Center 元件

系統需求

在安裝 NSX-T Data Center 之前，您的環境必須滿足特定硬體和資源需求。

NSX Manager 虛擬機器系統需求

安裝 NSX Manager 之前，請確定您的環境符合支援的需求。

傳輸節點的 Hypervisor 主機需求

Hypervisor	版本	CPU 核心	記憶體
vSphere	支援的 vSphere 版本	4	16 GB
CentOS Linux KVM	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.6、7.5 和 7.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP3、SP4	4	16 GB
Ubuntu KVM	18.04 和 16.04.2 LTS	4	16 GB

表 3-1. NSX Manager 支援的主機

支援說明	Hypervisor
ESXi	對於支援的主機，請參閱《VMware 產品互通性對照表》。
KVM	RHEL 7.4 和 Ubuntu 16.04 LTS

對於 ESXi 主機，NSX-T Data Center 支援 vSphere 6.7 U1 或更新版本上的主機設定檔和自動部署功能。如需詳細資訊，請參閱《VMware ESXi 安裝和設定》說明文件中的〈瞭解 vSphere Auto Deploy〉。

注意　在 RHEL 上，`yum update` 命令可能會更新核心版本，而損及與 NSX-T Data Center 之間的相容性。當您執行 `yum update` 時，停用自動核心更新。此外，在執行 `yum install` 之後，請確認 NSX-T Data Center 支援核心版本。

Hypervisor 主機網路需求

執行 NSX-T Data Center 的 Hypervisor 主機必須有相容的 NIC 介面卡。如需了解支援的 NIC 介面卡，請參閱 VMware 相容性指南。

提示　若要快速識別出相容性指南中的相容卡，請套用下列準則：

- 在 **I/O 裝置類型**下，選取**網路**。
- 或者，若要使用受支援的 GENEVE 封裝，請在**功能**下，選取 GENEVE 選項。
- 或者，若要使用「增強型資料路徑」，請選取 **N–VDS 增強型資料路徑**。

增強型資料路徑 NIC 驅動程式

從 My VMware 頁面下載支援的 NIC 驅動程式。

NIC 卡	NIC 驅動程式
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
適用於 10GbE SFP+ 的 Intel(R) 乙太網路控制器 X710 適用於 40GbE QSFP+ 的 Intel(R) 乙太網路控制器 XL710	i40en 1.2.0.0-1OEM.670.0.0.8169922

NSX Manager 虛擬機器資源需求

精簡佈建虛擬磁碟大小為 3.8 GB，完整佈建虛擬磁碟大小為 200 GB。

應用裝置大小	記憶體	vCPU	磁碟空間	虛擬機器硬體版本
NSX Manager 超小型	8 GB	2	200 GB	10 或更新版本
NSX Manager 小型虛擬機器	16 GB	4	200 GB	10 或更新版本

應用裝置大小	記憶體	vCPU	磁碟空間	虛擬機器硬體版本
NSX Manager 中型虛擬機器	24 GB	6	200 GB	10 或更新版本
NSX Manager 大型虛擬機器	48 GB	12	200 GB	10 或更新版本

備註　自 NSX-T 2.4 起，NSX Manager 可提供多個角色 (之前需要個別的應用裝置)。其中包括原則角色、管理平面角色和中央控制平面角色。中央控制平面角色之前由 NSX Controller 應用裝置所提供。

- NSX Manager 超小型虛擬機器資源需求僅適用於 Cloud Service Manager。
- NSX Manager 小型虛擬機器應用裝置大小適用於實驗室和概念驗證部署，不得在生產環境中使用。
- NSX Manager 中型虛擬機器應用裝置大小適用於一般生產環境，且最多可支援 64 個 Hypervisor。
- NSX Manager 大型虛擬機器應用裝置大小適用於具有超過 64 個 Hypervisor 的大規模部署。

如需使用 NSX Manager 大型虛擬機器應用裝置大小的最大規模，請前往 VMware 組態上限工具，網址為：https://configmax.vmware.com/guest，並從產品清單選取 NSX-T Data Center。

NSX Manager 瀏覽器支援

建議使用下列瀏覽器來搭配 NSX Manager 使用。

瀏覽器	Windows 10	Mac OS X 10.13、10.14	Ubuntu 18.04
Google Chrome 76	是	是	是
Mozilla Firefox 68	是	是	是
Microsoft Edge 44	是		
Apple Safari 12		是	

備註

- 不支援 Internet Explorer。
- 支援的瀏覽器最低解析度為 1280 x 800 像素。
- 語言支援：NSX Manager 已翻譯成多種語言：英文、德文、法文、日文、簡體中文、韓文、繁體中文和西班牙文。但是，由於 NSX Manager 當地語系化是使用瀏覽器語言設定，因此請確定您的設定符合所需的語言。NSX Manager 介面本身沒有語言喜好設定。

網路延遲需求

NSX Manager 叢集中 NSX Manager 之間的最大網路延遲為 10 毫秒。

NSX Manager 與傳輸節點之間的最大網路延遲為 150 毫秒。

儲存區需求

- 最大磁碟存取延遲低於 10 毫秒。
- 建議將 NSX Manager 置於共用儲存區。

- 儲存區應具高可用性，以避免在發生儲存區故障時，儲存區的中斷時造成將所有 NSX Manager 檔案系統放入唯讀模式。

  請參閱您的儲存區技術的說明文件，以瞭解如何設計最佳、高度可用的儲存區解決方案。

NSX Edge 虛擬機器系統需求

安裝 NSX Edge 之前，請確定您的環境符合支援的需求。

僅具有 Intel 架構晶片組的 ESXi 型主機支援 NSX Edge 節點。否則，vSphere EVC 模式可能會讓 NSX Edge 節點無法啟動，並在主控台中顯示錯誤訊息。

備註 僅 NSX Edge 虛擬機器支援 VMXNET 3 vNIC。

NSX Cloud 附註 如果使用 NSX Cloud，請注意 NSX Public Cloud Gateway (PCG) 會針對每個支援的公有雲以單一預設大小部署。如需詳細資料，請參閱部署或連結 NSX Public Cloud Gateway。

NSX Edge 虛擬機器資源需求

應用裝置大小	記憶體	vCPU	磁碟空間	虛擬機器硬體版本
NSX Edge 小型	4 GB	2	200 GB	11 或更新版本 (vSphere 6.0 或更新版本)
NSX Edge 中型	8 GB	4	200 GB	11 或更新版本 (vSphere 6.0 或更新版本)
NSX Edge 大型	32 GB	8	200 GB	11 或更新版本 (vSphere 6.0 或更新版本)

備註

- NSX Edge 小型虛擬機器應用裝置大小適用於實驗室和概念驗證部署。
- NSX Edge 中型應用裝置大小適用於一般生產環境。
- NSX Edge 大型應用裝置大小適用於具有負載平衡功能的環境。請參閱《NSX-T Data Center 管理指南》中的調整負載平衡器資源。

NSX Edge 虛擬機器 CPU 系統需求

若要獲得 DPDK 支援，基礎平台必須符合下列需求：

- CPU 必須具有 AESNI 功能。
- CPU 必須具有 1 GB 大型分頁支援。

硬體	類型
CPU	■ Intel Xeon E7-xxxx (Westmere-EX 及下一代 CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge 及下一代 CPU) ■ Intel Xeon Platinum (所有版本) ■ Intel Xeon Gold (所有版本) ■ Intel Xeon Silver (所有版本) ■ Intel Xeon Bronze (所有版本)

NSX Edge 裸機需求

在設定 NSX Edge 裸機之前，請確定您的環境符合支援的需求。

僅具有 Intel 架構晶片組的 ESXi 型主機支援 NSX Edge 節點。否則，vSphere EVC 模式可能會讓 Edge 節點無法啟動，並在主控台中顯示錯誤訊息。

NSX Edge 裸機記憶體、CPU 和磁碟需求

記憶體	CPU 核心	磁碟空間
32 GB	8	200 GB

NSX Edge 裸機 DPDK CPU 需求

若要獲得 DPDK 支援，基礎平台必須符合下列需求：

- CPU 必須具有 AES-NI 功能。
- CPU 必須具有 1 GB 大型分頁支援。

硬體	類型
CPU	■ Intel Xeon E7-xxxx (Westmere-EX 及下一代 CPU) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge 及下一代 CPU) ■ Intel Xeon Platinum (所有版本) ■ Intel Xeon Gold (所有版本) ■ Intel Xeon Silver (所有版本) ■ Intel Xeon Bronze (所有版本)

NSX Edge 裸機硬體需求

確認裸機 NSX Edge 硬體列於此 URL https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server 中。如果未列出此硬體，則儲存區、視訊卡或主機板元件可能在 NSX Edge 應用裝置上無法運作。

NSX Edge 裸機 NIC 需求

NIC 類型	說明	PCI 裝置識別碼
Intel XXV710	I40E_DEV_ID_25G_B	0x158A
	I40E_DEV_ID_25G_SFP28	0x158B
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514
	IXGBE_DEV_ID_82599_KR	0x1517
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	0x10F8 0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9 0x10FB
	IXGBE_DEV_ID_82599_CX4	0x11A9
	IXGBE_DEV_ID_82599_SFP	0x1F72
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_RNDC	0x0470
	IXGBE_SUBDEV_ID_82599_560FLR	0x1507
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x154D
	IXGBE_DEV_ID_82599_SFP_EM	0x154A
	IXGBE_DEV_ID_82599_SFP_SF2	0x1558
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x1557
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x10FC
	IXGBE_DEV_ID_82599EN_SFP	0x151C
	IXGBE_DEV_ID_82599_XAUI_LOM	
	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Cisco UCS 虛擬介面卡 1387	0x0043

裸機伺服器系統需求

設定裸機伺服器之前，請確定您的伺服器符合支援的需求。

重要 執行安裝的使用者對於有些程序可能需要 sudo 命令的權限。請參閱在裸機伺服器上安裝第三方套件。

裸機伺服器需求

作業系統	版本	CPU 核心	記憶體
CentOS Linux	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.5 和 7.4	4	16 GB
SUSE Linux Enterprise Server	12 SP3	4	16 GB
Ubuntu	18.04 和 16.04.2 LTS	4	16 GB

裸機 Linux 容器需求

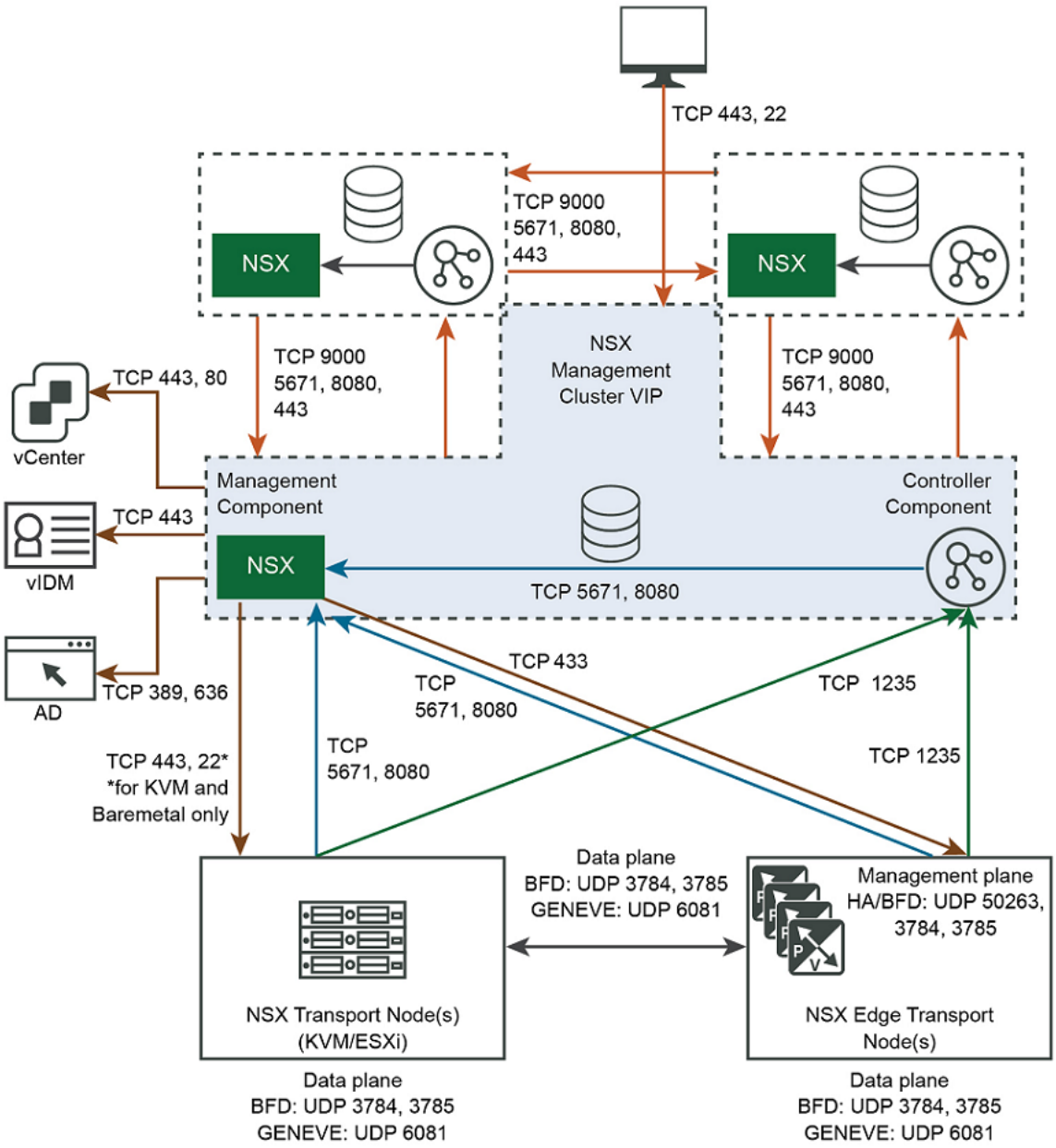
如需裸機 Linux 容器需求，請參閱《適用於 OpenShift 的 NSX Container Plug-in - 安裝和管理指南》。

連接埠和通訊協定

連接埠和通訊協定允許 NSX-T Data Center 中的節點到節點通訊路徑，這些路徑受到保護且經過驗證，並且使用認證的儲存位置來建立相互驗證。

備註 實體和主機 Hypervisor 防火牆上都必須開啟所需的連接埠和通訊協定。

圖 3-1. NSX-T Data Center 連接埠和通訊協定



依預設，所有憑證皆為自我簽署憑證。北向 GUI 和 API 憑證以及私密金鑰皆可取代為 CA 簽署的憑證。

下列是透過回送或 UNIX 網域通訊端進行通訊的內部精靈：

- KVM：MPA、netcpa、nsx-agent、OVS

- ESXi：netcpa、ESX-DP (在核心內)

備註 若要取得 NSX-T Data Center 節點的存取權，您必須在這些節點上啟用 SSH。

NSX Cloud 附註 如需部署 NSX Cloud 所需的連接埠清單，請參閱針對混合連線啟用對 CSM 上的連接埠和通訊協定的存取。

NSX Manager 所使用的 TCP 和 UDP 連接埠

NSX Manager 使用部分 TCP 和 UDP 連接埠與其他元件及產品進行通訊。這些連接埠必須在防火牆中開啟。

您可以使用 API 呼叫或 CLI 命令來指定供傳輸檔案 (預設值為 22) 和供匯出 Syslog 資料 (預設值為 514 和 6514) 的自訂連接埠。若要進行，您將需要依此設定防火牆。

表 3-2. NSX Manager 所使用的 TCP 和 UDP 連接埠

來源	目標	連接埠	通訊協定	說明
NSX Manager	Active Directory	389	TCP	Active Directory
NSX Controller、NSX Edge 節點、傳輸節點	NSX Manager	5671	TCP	NSX 傳訊
NSX Controller、NSX Edge 節點、傳輸節點、vCenter Server	NSX Manager	8080	TCP	安裝-升級 HTTP 存放庫
NSX Manager	NSX Manager	9000	TCP	內部資料存放區存取
NSX Manager	DNS 伺服器	53	TCP	DNS
NSX Manager	DNS 伺服器	53	UDP	DNS
NSX Manager	NSX Edge	443	TCP	HTTPS
NSX Manager	管理 SCP 伺服器	22	TCP	SSH (上傳支援服務包、備份等項目)
NSX Manager	NTP 伺服器	123	UDP	NTP
NSX Manager	SNMP 伺服器	161 和 162	TCP	SNMP
NSX Manager	SNMP 伺服器	161 和 162	UDP	SNMP
NSX Manager	Syslog 伺服器	514	TCP	Syslog
NSX Manager	Syslog 伺服器	514	UDP	Syslog
NSX Manager	Syslog 伺服器	6514	TCP	Syslog
NSX Manager	Syslog 伺服器	6514	UDP	Syslog
NSX Manager	Traceroute 目的地	33434 - 33523	UDP	Traceroute

表 3-2. NSX Manager 所使用的 TCP 和 UDP 連接埠 (續)

來源	目標	連接埠	通訊協定	說明
NSX Manager	vCenter Server	80	TCP	NSX Manager 與計算管理程式 (vCenter Server) 通訊 (若已設定)。
NSX Manager	vCenter Server	443	TCP	NSX Manager 與計算管理程式 (vCenter Server) 通訊 (若已設定)。
NSX Manager	vIDM	443	TCP	vIDM
NSX Manager	NSX Manager	443	TCP	NSX Manager 對 NSX Manager 的通訊
管理用戶端	NSX Manager	22	TCP	SSH (依預設為停用)
管理用戶端	NSX Manager	443	TCP	NSX API 伺服器
SNMP 伺服器	NSX Manager	161	UDP	SNMP

NSX Edge 所使用的 TCP 和 UDP 連接埠

NSX Edge 使用部分 TCP 和 UDP 連接埠與其他元件及產品進行通訊。這些連接埠必須在防火牆中開啟。

您可以使用 API 呼叫或 CLI 命令來指定供傳輸檔案 (預設值為 22) 和供匯出 Syslog 資料 (預設值為 514 和 6514) 的自訂連接埠。若要進行，您將需要依此設定防火牆。

表 3-3. NSX Edge 所使用的 TCP 和 UDP 連接埠

來源	目標	連接埠	通訊協定	說明
管理用戶端	NSX Edge 節點	22	TCP	SSH (依預設為停用)
NSX 代理程式	NSX Edge 節點	5555	TCP	NSX Cloud - 執行個體上與 NSX Cloud 閘道通訊的代理程式。
NSX Edge 節點	DNS 伺服器	53	UDP	DNS
NSX Edge 節點	管理 SCP 或 SSH 伺服器	22	TCP	SSH (上傳支援服務包、備份等項目)
NSX Edge 節點	NSX Controller 節點	1235	TCP	netcpa
NSX Edge 節點	NSX Edge 節點	1167	TCP	DHCP 後端
NSX Edge 節點	NSX Edge 節點	2480	TCP	Nestdb
NSX Edge 節點	NSX Edge 節點	6666	TCP	NSX Cloud - NSX Edge 本機通訊。
NSX Edge 節點	NSX Edge 節點	50263	UDP	高可用性
NSX Edge 節點	NSX Manager 節點	443	TCP	HTTPS

表 3-3. NSX Edge 所使用的 TCP 和 UDP 連接埠 (續)

來源	目標	連接埠	通訊協定	說明
NSX Edge 節點	NSX Manager 節點	5671	TCP	NSX 傳訊
NSX Edge 節點	NSX Manager 節點	8080	TCP	NAPI 和 NSX-T Data Center 升級
NSX Edge 節點	NTP 伺服器	123	UDP	NTP
NSX Edge 節點	OpenStack Nova API 伺服器	3000 - 9000	TCP	中繼資料 Proxy
NSX Edge 節點	SNMP 伺服器	161 和 162	TCP	SNMP
NSX Edge 節點	SNMP 伺服器	161 和 162	UDP	SNMP
NSX Edge 節點	Syslog 伺服器	514	TCP	Syslog
NSX Edge 節點	Syslog 伺服器	514	UDP	Syslog
NSX Edge 節點	Syslog 伺服器	6514	TCP	Syslog
NSX Edge 節點	Syslog 伺服器	6514	UDP	Syslog
NSX Edge 節點	Traceroute 目的地	33434 - 33523	UDP	Traceroute
NSX Edge 節點、傳輸節點	NSX Edge 節點	3784 和 3785	UDP	在資料中的傳輸節點 TEP IP 位址之間的 BFD。
SNMP 伺服器	NSX Edge 節點	161	UDP	SNMP

由 ESXi、KVM 主機和裸機伺服器使用的 TCP 和 UDP 連接埠

當 ESXi、KVM 主機和裸機伺服器用作傳輸節點時，需要特定 TCP 和 UDP 連接埠可供使用。

表 3-4. ESXi 和 KVM 主機所使用的 TCP 和 UDP 連接埠

來源	目標	連接埠	通訊協定	說明
ESXi 主機	NSX Controller	1235	TCP	控制平面 - LCP 至 CCP 通訊
ESXi 主機	NSX Manager	5671	TCP	NSX Manager 的 AMPQ 通訊通道
ESXi 主機	NSX Manager	8080	TCP	安裝和升級 HTTP 存放庫
ESXi 和 KVM 主機	NSX Manager	443	TCP	管理和佈建連線
ESXi 和 KVM 主機	NSX Manager	443	TCP	安裝和升級 HTTP 存放庫
GENEVE 終止端點 (TEP)	GENEVE 終止端點 (TEP)	6081	UDP	傳輸網路

表 3-4. ESXi 和 KVM 主機所使用的 TCP 和 UDP 連接埠 (續)

來源	目標	連接埠	通訊協定	說明
KVM 主機	NSX Manager	5671	TCP	NSX Manager 的 AMPQ 通訊通道
KVM 主機	NSX Controller	1235	TCP	控制平面 - LCP 至 CCP 通訊
KVM 主機	NSX Manager	8080	TCP	安裝和升級 HTTP 存放庫
NSX Manager	ESXi 主機	443	TCP	管理和佈建連線
NSX Manager	KVM 主機	443	TCP	管理和佈建連線
ESXi 和 KVM 主機	Syslog 伺服器	514	TCP	Syslog
ESXi 和 KVM 主機	Syslog 伺服器	514	UDP	Syslog
ESXi 和 KVM 主機	Syslog 伺服器	6514	TCP	Syslog
ESXi 和 KVM 主機	Syslog 伺服器	6514	UDP	Syslog
NSX-T Data Center 傳輸節點	NSX-T Data Center 傳輸節點	3784 和 3785	UDP	TEP 之間的 BFD 工作階段，位於使用 TEP 介面的資料路徑中

安裝 NSX-T Data Center 元件

您必須安裝 NSX Manager 和 NSX Edge 核心元件以使用 NSX-T Data Center。

NSX Manager 安裝

NSX Manager 提供可用來建立、設定及監控 NSX-T Data Center 元件 (例如邏輯交換器、邏輯路由器和防火牆) 的圖形使用者介面 (GUI) 與 REST API。

NSX Manager 會提供系統視圖，且屬於 NSX-T Data Center 的管理元件。

為獲得高可用性，NSX-T Data Center 支援包含三個 NSX Manager 的管理叢集。針對生產環境，建議部署管理叢集。針對概念證明環境，您可以部署單一 NSX Manager。

NSX Manager 部署、平台和安裝需求

下表詳述 NSX Manager 部署、平台以及安裝需求

需求	說明
支援的部署方法	■ OVA/OVF ■ QCOW2
支援的平台	請參閱 NSX Manager 虛擬機器系統需求。 在 ESXi 上，建議將 NSX Manager 應用裝置安裝在共用儲存區。

需求	說明
IP 位址	NSX Manager 必須要有靜態 IP 位址。IP 位址在安裝後即無法變更。
NSX-T Data Center 應用裝置密碼	■ 至少 12 個字元 ■ 至少 1 個小寫字母 ■ 至少 1 個大寫字母 ■ 至少 1 個數字 ■ 至少 1 個特殊字元 ■ 至少 5 個不同字元 ■ 無字典字組 ■ 無回文 ■ 不允許使用四個以上單純字元序列
主機名稱	安裝 NSX Manager 時，請指定不包含無效字元 (如底線) 的主機名稱。如果主機名稱包含任何無效字元，則在部署完成後，主機名稱將會設為 **nsx-manager**。 如需關於主機名稱限制的詳細資訊，請參閱 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上執行的 NSX Manager 虛擬機器已安裝 VMTools。請勿移除或升級 VMTools。
系統	■ 確認已滿足系統需求。請參閱系統需求。 ■ 確認所需連接埠已開啟。請參閱 連接埠和通訊協定。 ■ 確認資料存放區已設定並可在 ESXi 主機上存取。 ■ 確認您具有供 NSX Manager 使用的 IP 位址和閘道、DNS 伺服器 IP 位址、網域搜尋清單，以及 NTP 伺服器 IP 位址。 ■ 如果您還沒有目標虛擬機器連接埠群組網路，請建立。將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。 如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。 ■ 計劃 NSX Manager IPv4 或 IPv6 IP 位址配置。
OVF 權限	確認您擁有在 ESXi 主機上部署 OVF 範本的適當權限。 可部署 OVF 範本的管理工具，例如 vCenter Server 或 vSphere Client。OVF 部署工具必須支援可允許手動設定的組態選項。 OVF 工具版本必須是 4.0 或更新版本。
用戶端外掛程式	必須安裝用戶端整合外掛程式。

備註 在 NSX Manager 的全新安裝、重新開機時，或在第一次登入期間經提示而變更 **admin** 密碼之後，NSX Manager 可能需要數分鐘才會啟動。

NSX Manager 安裝案例

重要 當您從 OVA 或 OVF 檔案安裝 NSX Manager 時 (無論是從 vSphere Client 或命令列)，在虛擬機器的電源開啟之前，系統不會驗證使用者名稱、密碼或 IP 位址等 OVA/OVF 內容值。

- 為 **admin** 或 **audit** 使用者指定使用者名稱時，該名稱必須是唯一的。如果您指定相同名稱，則系統會忽略該名稱並使用預設名稱 (**admin** 和 **audit**)。
- 如果 **admin** 使用者的密碼不符合複雜性需求，您必須透過 SSH 或從主控台以 **admin** 使用者身分和密碼 **default** 登入 NSX Manager。系統會提示您變更密碼。

- 如果 **audit** 使用者的密碼不符合複雜性需求，則系統會停用使用者帳戶。若要啟用帳戶，請透過 SSH 或從主控台以 **admin** 使用者身分登入 NSX Manager，並執行 **set user audit** 命令以設定 **audit** 使用者的密碼 (目前的密碼為空白字串)。
- 如果 **root** 使用者的密碼不符合複雜性需求，則您必須透過 SSH 或從主控台以 **root** 使用者身分和密碼 **vmware** 登入 NSX Manager。系統會提示您變更密碼。

注意　使用 **root** 使用者認證登入時對 NSX-T Data Center 所做的變更可能會導致系統故障，並可能會影響您的網路。使用 **root** 使用者認證時，只能在 VMware 支援團隊的指導下進行變更。

備註　必須在設定夠複雜性的密碼後，應用裝置上的核心服務才會啟動。

在從 OVA 檔案部署 NSX Manager 後，您就無法藉由關閉虛擬機器電源並從 vCenter Server 修改 OVA 設定來變更虛擬機器的 IP 設定。

設定 NSX Manager 供 DNS 伺服器存取

依預設，傳輸節點會根據 NSX Manager 的 IP 位址來加以存取。但也可能根據 NSX Manager 的 DNS 名稱來存取。

透過在 NSX Manager 上啟用 FQDN 使用量 (DNS)，可以在不影響傳輸節點的情況下變更 Manager 的 IP 位址。

您可以透過發佈 NSX Manager 的 FQDN 來啟用 FQDN 使用量。

備註　多站台 Lite 和 NSX Cloud 與部署都需要在 NSX Manager 上啟用 FQDN 使用量 (DNS)。(對所有其他部署類型則是選用的。)請參閱《NSX-T Data Center 管理指南》中的〈NSX-T Data Center 的多站台部署〉和本指南中的第 11 章 安裝 NSX Cloud 元件 。

發佈 NSX Manager 的 FQDN

安裝 NSX-T Data Center 核心元件和 CSM 後，若要啟用使用 FQDN 的 NAT，您將需要在您部署中的 NSX-T DNS 伺服器中設定對應和反向對應項目。

此外，您還必須使用 NSX-T API 啟用 NSX Manager FQDN 的發佈。

範例要求：`PUT https://<nsx-mgr>/api/v1/configs/management`

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

範例回應：

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

如需詳細資料，請參閱《NSX-T Data Center API 指南》。

備註 發佈 FQDN 之後，請如下一節所述，驗證傳輸節點的存取。

驗證傳輸節點透過 FQDN 的存取

發行 NSX Manager 的 FQDN 之後，確認傳輸節點皆已成功存取 NSX Manager。

使用 SSH 登入傳輸節點，例如 Hypervisor 或 Edge 節點，並執行 `get controllers` CLI 命令。

範例回應：

```
Controller IP    Port  SSL     Status       Is Physical Master   Session State    Controller FQDN
192.168.60.5     1235  enabled  connected   true                 up               nsxmgr.corp.com
```

NSX Edge 安裝

NSX Edge 可對 NSX-T Data Center 部署以外的網路 NSX Edge 提供路由服務和連線。如果您要使用網路位址轉譯 (NAT)、VPN 等可設定狀態的服務部署第 0 層路由器或第 1 層路由器，則需要 NSX Edge。

備註 每個 NSX Edge 節點只能有一個第 0 層路由器。不過，一個 NSX Edge 節點上可以主控多個第 1 層負載路由器。同一叢集中可以組合使用不同大小的 NSX Edge 虛擬機器，但不建議這樣做。

表 3-5. NSX Edge 部署、平台和安裝需求

需求	說明
支援的部署方法	■ OVA/OVF ■ 含 PXE 的 ISO ■ 不含 PXE 的 ISO
支援的平台	NSX Edge 僅在 ESXi 或裸機上受到支援。 KVM 不支援 NSX Edge。
PXE 安裝	根使用者和管理員使用者密碼的密碼字串必須以 SHA-512 演算法加密。
NSX-T Data Center 應用裝置密碼	■ 至少 12 個字元 ■ 至少 1 個小寫字母 ■ 至少 1 個大寫字母 ■ 至少 1 個數字 ■ 至少 1 個特殊字元 ■ 至少 5 個不同字元 ■ 無字典字組 ■ 無回文 ■ 不允許使用四個以上單純字元序列
主機名稱	安裝 NSX Edge 時，請指定不包含無效字元 (如底線) 的主機名稱。如果主機名稱包含任何無效字元，則在部署之後，主機名稱將會設為 **localhost**。如需關於主機名稱限制的詳細資訊，請參閱 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。

表 3-5. NSX Edge 部署、平台和安裝需求 (續)

需求	說明
VMware Tools	在 ESXi 上執行的 NSX Edge 虛擬機器已安裝 VMTools。請勿移除或升級 VMTools。
系統	確認已滿足系統需求。請參閱 NSX Edge 虛擬機器系統需求。
連接埠	確認所需連接埠已開啟。請參閱 連接埠和通訊協定。
IP 位址	如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。 計劃 NSX Edge IPv4 或 IPv6 IP 位址配置。
OVF 範本	■ 確認您擁有在 ESXi 主機上部署 OVF 範本的適當權限。 ■ 確認主機名稱不包含底線。否則，主機名稱會設為 *nsx-manager*。 ■ 可部署 OVF 範本的管理工具，例如 vCenter Server 或 vSphere Client。 OVF 部署工具必須支援可允許手動設定的組態選項。 ■ 必須安裝用戶端整合外掛程式。
NTP 伺服器	必須在 Edge 叢集中的所有 NSX Edge 伺服器上設定相同的 NTP 伺服器。

NSX Edge 安裝案例

重要　當您從 OVA 或 OVF 檔案安裝 NSX Edge 時 (無論是從 vSphere Web Client 或命令列)，在虛擬機器的電源開啟之前，系統將不會驗證使用者名稱、密碼或 IP 位址等 OVA/OVF 內容值。

- 為 **admin** 或 **audit** 使用者指定使用者名稱時，該名稱必須是唯一的。如果您指定相同名稱，則系統會忽略該名稱並使用預設名稱 (**admin** 和 **audit**)。
- 如果 **admin** 使用者的密碼不符合複雜性需求，您必須透過 SSH 或從主控台以 **admin** 使用者身分和密碼 **default** 登入 NSX Edge。系統會提示您變更密碼。
- 如果 **audit** 使用者的密碼不符合複雜性需求，則系統會停用使用者帳戶。若要啟用帳戶，請透過 SSH 或從主控台以 **admin** 使用者身分登入 NSX Edge，並執行 **set user audit** 命令以設定 **audit** 使用者的密碼 (目前的密碼為空白字串)。
- 如果 **root** 使用者的密碼不符合複雜性需求，則您必須透過 SSH 或從主控台以 **root** 使用者身分和密碼 **vmware** 登入 NSX Edge。系統會提示您變更密碼。

注意　使用 **root** 使用者認證登入時對 NSX-T Data Center 所做的變更可能會導致系統故障，並可能會影響您的網路。使用 **root** 使用者認證時，只能在 VMware 支援團隊的指導下進行變更。

備註　在設定具有足夠複雜性的密碼之前，您無法啟動應用裝置上的核心服務。

在從 OVA 檔案部署 NSX Edge 後，您就無法藉由關閉虛擬機器電源並從 vCenter Server 修改 OVA 設定來變更虛擬機器的 IP 設定。

將 NSX Edge 加入管理平面

將 NSX Edge 加入管理平面，可確保 NSX Manager 與 NSX Edge 能夠相互通訊。

必要條件

確認您具有登入 NSX Edge 和 NSX Manager 應用裝置的管理員權限。

程序

1 開啟 NSX Manager 應用裝置的 SSH 工作階段。

2 開啟 NSX Edge 的 SSH 工作階段。

3 在 NSX Manager 應用裝置上，執行 `get certificate api thumbprint` 命令。

命令輸出是對此 NSX Manager 而言具有唯一性的英數數字字串。

例如：

```
NSX-Manager1> get certificate api thumbprint
...
```

4 在 NSX Edge 上，執行 **join management-plane** 命令。

請提供下列資訊：

- 具有選用連接埠號碼之 NSX Manager 的主機名稱或 IP 位址
- NSX Manager 的使用者名稱
- NSX Manager 的憑證指紋
- NSX Manager 的密碼

```
NSX-Edge1> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-
thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully registered and Edge restarted
```

在每個 NSX Edge 節點上重複此命令。

5 在您的 NSX Edge 上執行 `get managers` 命令以確認結果。

```
nsx-edge-1> get managers
- 192.168.110.47   Connected
```

6 在 NSX Manager UI 中，選取**系統 > 網狀架構 > 節點 > Edge 傳輸節點**頁面。

NSX Manager 連線應為「已啟用」。如果 NSX Manager 連線不是「已啟用」，請嘗試重新整理瀏覽器視窗。

後續步驟

將 NSX Edge 新增為傳輸節點。請參閱建立 NSX Edge 傳輸節點。

在 vSphere 上安裝 NSX-T Data Center

4

您可以使用使用者介面或 CLI 安裝 NSX-T Data Center 元件、NSX Manager 和 NSX Edge。

請確定您有支援的 vSphere 版本。請參閱 vSphere 支援。

本章節討論下列主題：

- 安裝 NSX Manager 和可用應用裝置
- 使用 vSphere GUI 在 ESXi 上安裝 NSX Edge

安裝 NSX Manager 和可用應用裝置

您可以使用 vSphere Client，將 NSX Manager 或 Cloud Service Manager 部署為虛擬應用裝置。

Cloud Service Manager 是一個虛擬應用裝置，會使用 NSX-T Data Center 元件並與公有雲整合。

必要條件

- 確認已滿足系統需求。請參閱系統需求。
- 確認所需連接埠已開啟。請參閱 連接埠和通訊協定。
- 確認資料存放區已設定並可在 ESXi 主機上存取。
- 確認您具有供 NSX Manager 使用的 IP 位址和閘道、DNS 伺服器 IP 位址、網域搜尋清單，以及 NTP 伺服器 IP 位址。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。

  如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。
- 計劃 NSX Manager IPv4 或 IPv6 IP 位址配置。

程序

1. 在 VMware 下載入口網站上找到 NSX-T Data Center OVA 檔案。

   複製下載 URL，或下載 OVA 檔案。
2. 在 vSphere Client 中，選取要安裝 NSX-T Data Center 的主機。
3. 按一下滑鼠右鍵，然後選取**部署 OVF 範本**以啟動安裝精靈。
4. 輸入下載 OVA URL，或導覽至 OVA 檔案。

5 輸入 NSX Manager 虛擬機器的名稱。

您輸入的名稱會顯示在 vSphere 詳細目錄中。

6 為 NSX Manager 應用裝置選取計算資源。

- 若要安裝在由 vCenter 管理的 ESXi 主機上，請選取要部署 NSX Manager 應用裝置的主機。
- 若要安裝在獨立 ESXi 主機上，請選取要部署 NSX Manager 應用裝置的主機。

7 驗證 OVF 範本詳細資料。

8 若要獲得最佳效能，請保留 NSX Manager 應用裝置所需的記憶體。

請設定保留，以確保 NSX Manager 具有足夠記憶體來讓執行更有效率。請參閱 NSX Manager 虛擬機器系統需求。

9 選取用來儲存 NSX Manager 應用裝置檔案的資料存放區。

10 為每個來源網路選取目的地網路。

11 選取 NSX Manager 的連接埠群組或目的地網路。

12 輸入 NSX Manager 系統根、CLI 管理員和稽核密碼。

密碼必須符合密碼強度限制。

- 至少 12 個字元
- 至少 1 個小寫字母
- 至少 1 個大寫字母
- 至少 1 個數字
- 至少 1 個特殊字元
- 至少 5 個不同字元
- 無字典字組
- 無回文
- 不允許使用四個以上單純字元序列

13 輸入 NSX Manager 的主機名稱。

備註 主機名稱必須是有效的網域名稱。請確定以點分隔的每個主機名稱部分 (網域/子網域) 都必須以字母字元開頭。

14 接受虛擬機器的預設 **NSX Manager** 角色。

從下拉式功能表中，選取 **nsx-cloud-service-manager** 角色，以安裝 NSX Cloud 應用裝置。

15 輸入預設閘道、管理網路 IPv4、管理網路的網路遮罩、DNS 和 NTP IP 位址。

16 啟用 SSH 並允許根 SSH 登入 NSX Manager 命令列。

依預設，基於安全考量，會停用這些選項。

17 確認您所有自訂 OVF 範本規格正確無誤，然後按一下**完成**以開始安裝。

此安裝可能需要 7-8 分鐘時間。

18 從 vSphere Client，開啟 NSX Manager 虛擬機器主控台以追蹤開機程序。

19 在 NSX Manager 開機後，以 Admin 身分登入 CLI 並執行 `get interface eth0` 命令，以確認 IP 位址已如預期般套用。

20 輸入 `get services` 命令，以確認所有服務正在執行。

如果服務未執行，請等待所有服務開始執行。

備註 依預設不會執行下列服務：liagent、migration-coordinator 和 snmp。您可以透過下列方式啟動這些服務：

- `start service liagent`
- `start service migration-coordinator`
- 針對 SNMP：

```
set snmp community <community-string>
start service snmp
```

21 確認 NSX Manager 具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX Manager 執行 Ping 偵測。
- NSX Manager 可以對其預設閘道執行 Ping 偵測。
- NSX Manager 可以使用管理介面，對位於相同網路中做為 NSX Manager 的 Hypervisor 主機執行 Ping 偵測。
- NSX Manager 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。
- 如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Manager。

如果未建立連線，請確定虛擬應用裝置的網路介面卡位於適當的網路或 VLAN。

後續步驟

從支援的網頁瀏覽器登入 NSX Manager。請參閱登入新建立的 NSX Manager 。

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager

如果您偏好將 NSX Manager 安裝自動化或使用 CLI 進行安裝，您可以使用 VMware OVF Tool；這是一種命令列公用程式。

基於安全考量，`nsx_isSSHEnabled` 和 `nsx_allowSSHRootLogin` 依預設皆為停用。當這兩個選項停用時，您將無法對 NSX Manager 命令列進行 SSH 連線或登入。如果您啟用 `nsx_isSSHEnabled`，但未啟用 `nsx_allowSSHRootLogin`，則可以使用 SSH 連線至 NSX Manager，但無法以根使用者身分登入。

必要條件

- 確認已滿足系統需求。請參閱系統需求。
- 確認所需連接埠已開啟。請參閱 連接埠和通訊協定。
- 確認資料存放區已設定並可在 ESXi 主機上存取。
- 確認您具有供 NSX Manager 使用的 IP 位址和閘道、DNS 伺服器 IP 位址、網域搜尋清單，以及 NTP 伺服器 IP 位址。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。

  如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。
- 計劃 NSX Manager IPv4 或 IPv6 IP 位址配置。

程序

1 搭配適當參數執行 `ovftool` 命令。

  程序取決於主機是否為獨立式，或是由 vCenter Server 管理。

  - 針對獨立主機：
    - Windows 範例：

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
```

```
--prop:"nsx_cli_audit-passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

備註 以上的 Windows 程式碼區塊使用反斜線 (\) 表示命令列的接續符號。實際使用時請省略反斜線，並將整個命令放在單一列中。

備註 在上述範例中，10.168.110.51 是要在其中部署 NSX Manager 之主機的 IP 位址。

- Linux 範例：

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
```

```
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@$mgresxhost01
```

結果看起來應類似如下：

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully
```

- 針對由 vCenter Server 管理的主機：
  - Windows 範例：

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
 --allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

備註 以上的 Windows 程式碼區塊使用反斜線 (\) 表示命令列的接續符號。實際使用時請省略反斜線，並將整個命令放在單一列中。

- Linux 範例：

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vcadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vcadmin:$vcpass@$vcip/?ip=$mgresxhost01
```

結果看起來應類似如下：

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully
```

2 若要獲得最佳效能，請保留 NSX Manager 應用裝置所需的記憶體。

請設定保留，以確保 NSX Manager 具有足夠記憶體來讓執行更有效率。請參閱 NSX Manager 虛擬機器系統需求。

3 從 vSphere Client，開啟 NSX Manager 虛擬機器主控台以追蹤開機程序。

4 在 NSX Manager 開機後，以 Admin 身分登入 CLI 並執行 `get interface eth0` 命令，以確認 IP 位址已如預期般套用。

5 確認 NSX Manager 具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX Manager 執行 Ping 偵測。
- NSX Manager 可以對其預設閘道執行 Ping 偵測。
- NSX Manager 可以使用管理介面，對位於相同網路中做為 NSX Manager 的 Hypervisor 主機執行 Ping 偵測。
- NSX Manager 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。
- 如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Manager。

如果未建立連線，請確定虛擬應用裝置的網路介面卡位於適當的網路或 VLAN。

後續步驟

從支援的網頁瀏覽器登入 NSX Manager。請參閱登入新建立的 NSX Manager 。

將 NSX-T Data Center 設定為在開機時顯示 GRUB 功能表

必須將 NSX-T Data Center 應用裝置設定為在開機時顯示 GRUB 功能表，才能重設 NSX-T Data Center 應用裝置的根密碼。

重要 如果在部署應用裝置後未執行組態，且您忘記了根使用者、管理員或稽核密碼，則無法加以重設。

程序

1 以根使用者身分登入虛擬機器。

2 變更 /etc/default/grub 檔案中參數 GRUB_HIDDEN_TIMEOUT 的值。

```
GRUB_HIDDEN_TIMEOUT=2
```

3 (選擇性) 變更 /etc/grub.d/40_custom 檔案中的 GRUB 密碼。

預設密碼為 VMware1。

4 更新 GRUB 組態。

```
update-grub
```

登入新建立的 NSX Manager

安裝 NSX Manager 後，您可以利用使用者介面執行其他安裝工作。

安裝 NSX Manager 後，您可以加入 NSX-T Data Center 的客戶經驗改進計劃 (CEIP)。如需有關此計劃的詳細資訊 (包括如何在之後加入或退出計劃)，請參閱《NSX-T Data Center 管理指南》中的〈客戶經驗改進計劃〉。

必要條件

確認已安裝 NSX Manager。請參閱安裝 NSX Manager 和可用應用裝置。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

使用者授權合約隨即出現。

2 閱讀並接受使用者授權合約條款。

3 選取是否加入 VMware 的客戶經驗改進計劃 (CEIP)。

4 按一下**儲存**

新增計算管理程式

計算管理程式 (例如 vCenter Server) 是一種應用程式，可管理如主機和虛擬機器等資源。

NSX-T Data Center 會輪詢計算管理程式以找出如新增或移除主機或者虛擬機器等變更，並據以更新其詳細目錄。不一定需要新增計算管理程式，因為即使沒有計算管理程式，NSX-T Data Center 仍可取得詳細目錄資訊 (例如，獨立主機和虛擬機器)。

在新增 vCenter Server 計算管理程式時，您必須提供 vCenter Server 使用者的認證。您可以提供 vCenter Server 管理員的認證，也可以專門為 NSX-T Data Center 建立角色和使用者並提供此使用者的認證。此角色必須具有下列 vCenter Server 權限：

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session

Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

如需關於 vCenter Server 角色和權限的詳細資訊，請參閱《vSphere 安全性》文件。

必要條件

- 確認您使用支援的 vSphere 版本。請參閱支援的 vSphere 版本。
- 與 vCenter Server 的 IPv6 和 IPv4 通訊。
- 確認您使用建議的計算管理程式數目。請參閱 https://configmax.vmware.com/home。

> **備註** NSX-T Data Center 不支援讓同一個 vCenter Server 登錄多個 NSX Manager。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 計算管理程式 > 新增**。
3. 完成計算管理程式詳細資料。

選項	說明
名稱與說明	輸入名稱以識別 vCenter Server。 您可以選擇性地說明任何特殊詳細資料，例如 vCenter Server 中的叢集數目。
網域名稱/IP 位址	輸入 vCenter Server 的 IP 位址。
類型	保留預設選項。

選項	說明
使用者名稱和密碼	輸入 vCenter Server 登入認證。
指紋	輸入 vCenter Server SHA-256 指紋演算法值。

如果您將指紋值保留空白，則系統會提示您接受伺服器提供的指紋。

接受指紋後，NSX-T Data Center 需要幾秒鐘的時間才能探索到 vCenter Server 資源並加以登錄。

4 如果進度圖示從**進行中**變更為**未登錄**，請執行下列步驟來解決此錯誤。

a 選取錯誤訊息，然後按一下**解決**。一個可能的錯誤訊息如下：

```
Extension already registered at CM <vCenter Server name> with id <extension ID>
```

b 輸入 vCenter Server 認證，然後按一下**解決**。

現有登錄將被取代 (若有)。

結果

向 vCenter Server 登錄計算管理程式，以及連線狀態顯示為開啟需要一些時間。

您可以按一下計算管理程式名稱，來檢視詳細資料、編輯計算管理程式，或管理套用至計算管理程式的標籤。

從使用者介面部署 NSX Manager 節點以形成叢集

您可以部署多個 NSX Manager 節點，以提供高可用性和可靠性。

部署新的節點後，這些節點會連線到 NSX Manager 節點以形成叢集。建議的叢集 NSX Manager 節點數目為 3。

備註 只有受 vCenter Server 管理的 ESXi 主機支援透過使用者介面部署多個 NSX Manager 節點。

第一個部署的 NSX Manager 節點的所有存放庫詳細資料和密碼會與叢集中新部署的節點同步。

必要條件

- 確認已安裝 NSX Manager 節點。請參閱安裝 NSX Manager 和可用應用裝置。
- 確認已設定計算管理程式。請參閱新增計算管理程式。
- 確認已滿足系統需求。請參閱系統需求。
- 確認所需連接埠已開啟。請參閱 連接埠和通訊協定。
- 確認資料存放區已設定並可在 ESXi 主機上存取。
- 確認您具有供 NSX Manager 使用的 IP 位址和閘道、DNS 伺服器 IP 位址、網域搜尋清單，以及 NTP 伺服器 IP 位址。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。

  如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 應用裝置 > 概觀 > 新增節點**。

3 輸入 NSX Manager 一般屬性詳細資料。

選項	說明
計算管理程式	會填入已登錄的資源計算管理程式。
啟用 SSH	切換按鈕以允許透過 SSH 登入新的 NSX Manager 節點。
啟用根存取	切換按鈕以允許以根使用者身分存取新的 NSX Manager 節點。
CLI 使用者名稱和密碼確認	設定新節點的 CLI 密碼和密碼確認。 密碼必須符合密碼強度限制。 ■ 至少 12 個字元 ■ 至少 1 個小寫字母 ■ 至少 1 個大寫字母 ■ 至少 1 個數字 ■ 至少 1 個特殊字元 ■ 至少 5 個不同字元 ■ 無字典字組 ■ 無回文 ■ 不允許使用四個以上單純字元序列 CLI 使用者名稱已設定為 admin。
根密碼和密碼確認	設定新節點的根密碼和密碼確認。 密碼必須符合密碼強度限制。 ■ 至少 12 個字元 ■ 至少 1 個小寫字母 ■ 至少 1 個大寫字母 ■ 至少 1 個數字 ■ 至少 1 個特殊字元 ■ 至少 5 個不同字元 ■ 無字典字組 ■ 無回文 ■ 不允許使用四個以上單純字元序列
DNS 伺服器	輸入 vCenter Server 中可用的 DNS 伺服器 IP 位址。
NTP 伺服器	輸入 NTP 伺服器 IP 位址。

4 輸入 NSX Manager 節點詳細資料。

選項	說明
名稱	輸入 NSX Manager 節點的名稱。
叢集	從下拉式功能表中指定節點要加入的叢集。
資源集區或主機	從下拉式功能表中為節點指派資源集區或主機。
資料存放區	從下拉式功能表中選取節點檔案的資料存放區。

選項	說明
網路	從下拉式功能表中指派網路。
管理 IP/網路遮罩	輸入 IP 位址和網路遮罩。
管理閘道	輸入閘道 IP 位址。

5 (選擇性) 按一下**新節點**並設定另一個節點。

重複步驟 3-4。

6 按一下**完成**。

已部署新節點。您可以在**系統 > 應用裝置 > 概觀**頁面或 vCenter Server 上追蹤部署程序。

7 等待 10-15 分鐘，讓部署、叢集格式化和存放庫同步完成。

第一個部署的 NSX Manager 節點的所有存放庫詳細資料和密碼會與叢集中新部署的節點同步。

8 在 NSX Manager 開機後，以 Admin 身分登入 CLI 並執行 `get interface eth0` 命令，以確認 IP 位址已如預期般套用。

9 輸入 `get services` 命令，以確認所有服務正在執行。

如果服務未執行，請等待所有服務開始執行。

備註 依預設不會執行下列服務：liagent、migration-coordinator 和 snmp。您可以透過下列方式啟動這些服務：

- `start service liagent`
- `start service migration-coordinator`
- 針對 SNMP：

```
set snmp community <community-string>
start service snmp
```

10 登入第一個部署的 NSX Manager 節點，然後輸入 `get cluster status` 命令，確認節點已成功新增至叢集。

11 確認 NSX Manager 具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX Manager 執行 Ping 偵測。
- NSX Manager 可以對其預設閘道執行 Ping 偵測。
- NSX Manager 可以使用管理介面，對位於相同網路中做為 NSX Manager 的 Hypervisor 主機執行 Ping 偵測。
- NSX Manager 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。
- 如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Manager。

如果未建立連線，請確定虛擬應用裝置的網路介面卡位於適當的網路或 VLAN。

後續步驟

設定 NSX Edge。請參閱使用 vSphere GUI 在 ESXi 上安裝 NSX Edge。

使用 CLI 部署 NSX Manager 節點以形成叢集

使用 CLI 加入 NSX Manager 以形成叢集，可確保叢集中的所有 NSX Manager 節點可以彼此通訊。

必要條件

必須完成 NSX-T Data Center 元件的安裝。

程序

1 開啟第一個部署的 NSX Manager 節點的 SSH 工作階段。

2 使用管理員認證登入。

3 在 NSX Manager 節點上，執行 `get certificate api thumbprint` 命令。

命令輸出是對此 NSX Manager 而言具有唯一性的數字字串。

4 執行 `get cluster config` 命令，以取得第一個部署的 NSX Manager 叢集識別碼。

5 新增 NSX Manager 節點至該叢集。

備註 您必須在新部署的 NSX Manager 節點上執行 join 命令。

請提供下列 NSX Manager 資訊：

- 您要加入之主機名稱或 IP 位址節點
- 叢集識別碼
- 使用者名稱
- 密碼
- 憑證指紋

您可以使用 CLI 命令或 API 呼叫。

- CLI 命令

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- API 呼叫 `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

加入和叢集穩定化程序可能需要 10-15 分鐘。

6 新增第三個 NSX Manager 節點至叢集。

重複步驟 5。

7 在您的主機上執行 `get cluster status` 命令以確認叢集狀態。

8 選取 **系統 > 應用裝置 > 概觀**並確認叢集連線。

後續步驟

建立傳輸區域。請參閱 建立獨立主機或裸機伺服器傳輸節點。

設定叢集的虛擬 IP (VIP) 位址

若要提供 Fault Tolerance 和高可用性給 NSX Manager 節點，請將虛擬 IP 位址 (VIP) 指派給 NSX-T 叢集的成員。

叢集的 NSX Manager 會成為 HTTPS 群組的一部分，提供服務給 API 和 UI 要求。叢集的領導者節點會承擔叢集的集合 VIP 擁有權，以為任何 API 和 UI 要求提供服務。來自用戶端的任何 API 和 UI 要求會導向至領導者節點。

備註 指派虛擬 IP 時，必須在相同的子網路中設定叢集中的所有 NSX Manager 虛擬機器。

如果擁有 VIP 的領導者節點變成無法使用，NSX-T 會選擇新的領導者。新領導者擁有 VIP。它會傳送免費 ARP 封包，通告新的 VIP 至 MAC 位址對應。選擇新的領導者節點後，新的 API 和 UI 要求會傳送至新領導者節點。

將 VIP 容錯移轉到叢集的新領導者節點，可能需要幾分鐘的時間才能正常運作。如果由於先前的領導者節點無法使用而使得 VIP 容錯移轉到新領導者節點，必須重新驗證認證，以便 API 要求會導向至新領導者節點。

備註 VIP 不是設計來做為負載平衡器使用，如果您從**系統 > 使用者 > 組態**中啟用 vIDM **外部負載平衡器整合**，則無法使用此功能。如果您想要使用來自 vIDM 的外部負載平衡器，請勿設定 VIP。如需詳細資料，請參閱《NSX-T Data Center 管理指南》中的設定 VMware Identity Manager 整合。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 移至**系統 > 概觀**。
3. 在虛擬 IP 欄位中，按一下**編輯**。
4. 輸入叢集的 VIP。確保 VIP 為與其他管理節點相同子網路的一部分。
5. 按一下**儲存**。
6. 若要確認叢集狀態和 HTTPS 群組的 API 領導者，請在 NSX Manager 主控台中或透過 SSH 輸入 NSX Manager CLI 命令 `get cluster status verbose`。

   下列是範例輸出，並以粗體標記領導者。

```
Group Type: HTTPS
Group Status: STABLE

Members:
    UUID                                    FQDN                IP
STATUS
    cdb93642-ccba-fdf4-8819-90bf018cd727    nsx-manager         192.196.197.84
UP
    51a13642-929b-8dfc-3455-109e6cc2a7ae    nsx-manager         192.196.198.156
```

```
UP
    d0de3642-d03f-c909-9cca-312fd22e486b       nsx-manager       192.196.198.54
UP

Leaders:
    SERVICE                                    LEADER                                    LEASE
VERSION
    api                                        cdb93642-ccba-fdf4-8819-90bf018cd727      8
```

7 若要疑難排解 VIP 問題，請在 NSX Manager CLI 中確認位於 `/var/log/proxy/reverse-proxy.log` 的 Reverse Proxy 記錄檔和位於 `/var/log/cbm/cbm.log` 的叢集管理程式記錄檔。

結果

對 NSX-T 的任何 API 要求會重新導向至由領導者節點擁有的叢集的虛擬 IP 位址。然後領導者節點會將要求轉送路由至應用裝置的其他元件。

使用 vSphere GUI 在 ESXi 上安裝 NSX Edge

如果您慣用互動式 NSX Edge 安裝，您可以使用 vSphere Web 用戶端。

重要 在 NSX-T 中，NSX Edge 虛擬機器不支援 vMotion。

必要條件

請參閱 NSX Edge 安裝。

程序

1 在 VMware 下載入口網站上找出 NSX Edge 應用裝置 OVA 檔案。

複製下載 URL，或將 OVA 檔案下載到您的電腦上。

2 在 vSphere Client 中，選取要在其中安裝 NSX Edge 應用裝置的主機。

3 按一下滑鼠右鍵，然後選取**部署 OVF 範本**以啟動安裝精靈。

4 輸入下載 OVA URL 或導覽至已儲存的 OVA 檔案。

5 輸入 NSX Edge 虛擬機器的名稱。

您輸入的名稱會顯示在詳細目錄中。

6 為 NSX Edge 應用裝置選取計算資源。

7 若要獲得最佳效能，請保留 NSX Edge 應用裝置所需的記憶體。

請設定保留，以確保 NSX Edge 具有足夠記憶體來讓執行更有效率。請參閱 NSX Edge 虛擬機器系統需求。

8 驗證 OVF 範本詳細資料。

9 選取用來儲存 NSX Edge 應用裝置檔案的資料存放區。

10 接受預設來源和目的地網路介面。

部署 NSX Edge 後，您可以針對其餘網路接受預設網路目的地，然後變更網路組態。

11 從下拉式功能表中選取 IP 配置。

12 輸入 NSX Edge 系統根、CLI 管理員和稽核密碼。

密碼必須符合密碼強度限制。

- 至少 12 個字元
- 至少 1 個小寫字母
- 至少 1 個大寫字母
- 至少 1 個數字
- 至少 1 個特殊字元
- 至少 5 個不同字元
- 無字典字組
- 無回文
- 不允許使用四個以上單純字元序列

13 輸入預設閘道、管理網路 IPv4、管理網路的網路遮罩、DNS 和 NTP IP 位址。

14 (選擇性) 如果您有可用的 NSX Manager，則使用管理平面登錄 NSX Edge。

a 輸入父系 NSX Manager 節點 IP 位址和指紋。

b 執行 API 呼叫 `POST https://<nsx-manager>/api/v1/aaa/registration-token` 以擷取 NSX Manager Token。

15 輸入 NSX Edge 虛擬機器的主機名稱。

16 啟用 SSH 並允許以根使用者身分透過 SSH 登入 NSX Edge 命令列。

依預設，基於安全考量，會停用這些選項。

17 確認您的所有自訂 OVA 範本規格正確無誤，然後按一下**完成**以起始安裝。

此安裝可能需要 7-8 分鐘時間。

18 開啟 NSX Edge 的主控台以追蹤開機程序。

如果主控台視窗並未開啟，請確定已允許快顯視窗。

19 NSX Edge 啟動後，使用管理員認證登入 CLI。

備註 在 NSX Edge 啟動後，如果首次登入時不使用管理員認證，則數據平面服務不會在 NSX Edge 上自動啟動。

20 執行 `get interface eth0.<vlan_ID>` 命令以確認 IP 位址已按預期套用。

```
nsx-edge-1> get interface eth0.100
```

```
Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

備註 在並非由 NSX 管理的主機上啟動 NSX Edge 虛擬機器時，請確認您已在資料 NIC 的實體主機交換器上將 MTU 設定設為 1600 (而非 1500)。

21 執行 `get managers` 命令，以確認 NSX Edge 已登錄。

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

22 確認 NSX Edge 應用裝置具有必要的連線。

如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Edge。

- 您可以對 NSX Edge 執行 Ping 偵測。
- NSX Edge 可以對其預設閘道執行 Ping 偵測。
- NSX Edge 可以對位於相同網路中作為 NSX Edge 的 Hypervisor 主機執行 Ping 偵測。
- NSX Edge 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。

23 疑難排解連線問題。

備註 如果未建立連線，請確定虛擬機器網路介面卡位於適當的網路或 VLAN。

依預設，NSX Edge 資料路徑會宣告所有虛擬機器 NIC，但管理 NIC 除外 (即具有 IP 位址和預設路由的 NIC)。如果將 NIC 錯誤地指派為管理介面，請遵循下列步驟來使用 DHCP，以將管理 IP 位址指派給正確的 NIC。

a 登入 CLI 並輸入 **`stop service dataplane`** 命令。

b 輸入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 將 *interface* 放入 DHCP 網路並等候系統將 IP 位址指派給該 *interface*。

d 輸入 **`start service dataplane`** 命令。

用於 VLAN 上行和通道覆疊的資料路徑 fp-ethX 連接埠會顯示在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中。

後續步驟

將 NSX Edge 加入管理平面。請參閱將 NSX Edge 加入管理平面。

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge

如果您偏好將 NSX Edge 安裝自動化，您可以使用 VMware OVF Tool，這是一種命令列公用程式。

必要條件

- 確認已滿足系統需求。請參閱系統需求。
- 確認所需連接埠已開啟。請參閱 連接埠和通訊協定。
- 確認資料存放區已設定並可在 ESXi 主機上存取。
- 確認您具有供 NSX Manager 使用的 IP 位址和閘道、DNS 伺服器 IP 位址、網域搜尋清單，以及 NTP 伺服器 IP 位址。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。

  如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。
- 計劃 NSX Manager IPv4 或 IPv6 IP 位址配置。
- 請參閱 NSX Edge 安裝 中的 NSX Edge 網路需求。
- 確認您擁有在 ESXi 主機上部署 OVF 範本的適當權限。
- 確認主機名稱不包含底線。否則，主機名稱會設為 *localhost*。
- OVF Tool 4.3 版或更新版本。

程序

- 對於獨立主機，請執行使用適當參數的 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
```

```
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- 對於由 vCenter Server 管理的主機，執行使用適當參數的 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
```

```
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- 若要獲得最佳效能，請保留 NSX Manager 應用裝置所需的記憶體。

  請設定保留，以確保 NSX Manager 具有足夠記憶體來讓執行更有效率。請參閱 NSX Manager 虛擬機器系統需求。

- 開啟 NSX Edge 的主控台以追蹤開機程序。
- NSX Edge 啟動後，使用管理員認證登入 CLI。
- 執行 `get interface eth0.<vlan_ID>` 命令以確認 IP 位址已按預期套用。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

備註 在並非由 NSX 管理的主機上啟動 NSX Edge 虛擬機器時，請確認您已在資料 NIC 的實體主機交換器上將 MTU 設定設為 1600 (而非 1500)。

- 確認 NSX Edge 應用裝置具有必要的連線。

  如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Edge。

  - 您可以對 NSX Edge 執行 Ping 偵測。
  - NSX Edge 可以對其預設閘道執行 Ping 偵測。
  - NSX Edge 可以對位於相同網路中作為 NSX Edge 的 Hypervisor 主機執行 Ping 偵測。
  - NSX Edge 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。

- 疑難排解連線問題。

  備註 如果未建立連線，請確定虛擬機器網路介面卡位於適當的網路或 VLAN。

  依預設，NSX Edge 資料路徑會宣告所有虛擬機器 NIC，但管理 NIC 除外 (即具有 IP 位址和預設路由的 NIC)。如果將 NIC 錯誤地指派為管理介面，請遵循下列步驟來使用 DHCP，以將管理 IP 位址指派給正確的 NIC。

  a 登入 CLI 並輸入 **`stop service dataplane`** 命令。

  b 輸入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 將 *interface* 放入 DHCP 網路並等候系統將 IP 位址指派給該 *interface*。

d 輸入 **`start service dataplane`** 命令。

用於 VLAN 上行和通道覆疊的資料路徑 fp-ethX 連接埠會顯示在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中。

後續步驟

將 NSX Edge 加入管理平面。請參閱將 NSX Edge 加入管理平面。

在 KVM 上安裝 NSX-T Data Center 5

NSX-T Data Center 支援 KVM 的方式有兩種：做為主機傳輸節點，以及做為 NSX Manager 的主機。

請確定您有支援的 KVM 版本。請參閱 NSX Manager 虛擬機器系統需求。

本章節討論下列主題：

- 設定 KVM
- 在 KVM CLI 中管理您的客體虛擬機器
- 在 KVM 上安裝 NSX Manager
- 登入新建立的 NSX Manager
- 在 KVM 主機上安裝第三方套件
- 確認 RHEL KVM 主機上的 Open vSwitch 版本
- 使用 CLI 部署 NSX Manager 節點以形成叢集
- 使用 ISO 檔案或 PXE 安裝 NSX Edge

設定 KVM

如果您打算使用 KVM 做為傳輸節點，或做為 NSX Manager 客體虛擬機器的主機，但您尚未設定 KVM，您可以使用此處說明的程序來設定。

備註 Geneve 封裝通訊協定會使用 UDP 連接埠 6081。您必須在 KVM 主機上的防火牆中允許此連接埠存取。

程序

1 (僅限 RHEL) 開啟 `/etc/yum.conf` 檔案。

2 搜尋行 `exclude`。

3 新增行 `"kernel* redhat-release*"` 來設定 YUM，以避免任何不支援的 RHEL 升級。

```
exclude=[existing list] kernel* redhat-release*
```

如果您計劃執行具有特定相容性需求的 NSX-T Data Center Container Plug-in，請同時排除容器相關模組。

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-* docker-*
```

支援的 RHEL 版本為 7.4 和 7.5。

4 安裝 KVM 和橋接器公用程式。

Linux 發行版	命令
Ubuntu	`apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools`

RHEL 或 CentOS Linux	`yum groupinstall "Virtualization Hypervisor"`
	`yum groupinstall "Virtualization Client"`
	`yum groupinstall "Virtualization Platform"`
	`yum groupinstall "Virtualization Tools"`

SUSE Linux Enterprise Server	啟動 YaSt，然後選取**虛擬化 > 安裝 Hypervisor 和工具**。 YaSt 可讓您自動啟用和設定網路橋接器。

5 確認硬體虛擬化功能。

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

輸出必須包含 vmx。

6 確認已安裝 KVM 模組。

Linux 發行版	命令

Ubuntu	`kvm-ok`
	
	`INFO: /dev/kvm exists`
	`KVM acceleration can be used`

RHEL 或 CentOS Linux	`lsmod | grep kvm`
	
	`kvm_intel   53484  6`
	`kvm         316506  1 kvm_intel`

SUSE Linux Enterprise Server	

7 若要讓 KVM 用做 NSX Manager 的主機，請準備橋接網路、管理介面和 NIC 介面。

在下列範例中，第一個乙太網路介面 (eth0 或 ens32) 會用於 Linux 機器本身的連線。此介面可能會使用 DHCP 或靜態 IP 設定，視您的部署環境而定。將上行介面指派給 NSX-T Data Center 主機之前，請確保供這些上行使用的介面指令碼已進行設定。如果沒有系統上的這些介面檔案，便無法成功建立主機傳輸節點。

備註 介面名稱在不同的環境中可能會有所不同。

Linux 發行版	網路組態

Ubuntu	編輯 /etc/network/interfaces：
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto br0`
	`iface br0 inet static`
	`address 192.168.110.51`
	`netmask 255.255.255.0`
	`network 192.168.110.0`
	`broadcast 192.168.110.255`
	`gateway 192.168.110.1`
	`dns-nameservers 192.168.3.45`
	`dns-search example.com`
	`bridge_ports eth0`
	`bridge_stp off`
	`bridge_fd 0`
	`bridge_maxwait 0`
	
	建立橋接器的網路定義 XML 檔案。例如，請使用下列命令列建立 /tmp/bridge.xml：
	`<network>`
	`<name>bridge</name>`
	`<forward mode='bridge'/>`
	`<bridge name='br0'/>`
	`</network>`
	
	使用下列命令定義並啟動橋接器網路：
	`virsh net-define`
	`bridge.xml`
	`virsh net-start bridge`
	`virsh net-autostart bridge`
	
	使用下列命令確認橋接器網路的狀態：
	`virsh net-list --all`
	
	`Name State Autostart Persistent`
	`----------------------------------------------------------`
	`bridge active yes yes`
	`default active yes yes`

RHEL 或 CentOS Linux	編輯 /etc/sysconfig/network-scripts/ifcfg-*management_interface*：
	`DEVICE="ens32"`
	`TYPE="Ethernet"`
	`NAME="ens32"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`HWADDR="<HWADDR>"`

Linux 發行版	網路組態
	``` ONBOOT="yes" NM_CONTROLLED="no" BRIDGE="br0" ``` 編輯 /etc/sysconfig/network-scripts/ifcfg-eth1： ``` DEVICE="eth1" TYPE="Ethernet" NAME="eth1" UUID="<UUID>" BOOTPROTO="none" HWADDR="<HWADDR>" ONBOOT="yes" NM_CONTROLLED="no" ``` 編輯 /etc/sysconfig/network-scripts/ifcfg-eth2： ``` DEVICE="eth2" TYPE="Ethernet" NAME="eth2" UUID="<UUID>" BOOTPROTO="none" HWADDR="<HWADDR>" ONBOOT="yes" NM_CONTROLLED="no" ``` 編輯 /etc/sysconfig/network-scripts/ifcfg-br0： ``` DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge" ```
SUSE Linux Enterprise Server	

8 針對要用作傳輸節點的 KVM 準備網路橋接器。

在下列範例中，第一個乙太網路介面 (eth0 或 ens32) 會用於 Linux 機器本身的連線。此介面可能會使用 DHCP 或靜態 IP 設定，視您的部署環境而定。

備註 介面名稱在不同的環境中可能會有所不同。

Linux 發行版	網路組態

Ubuntu	編輯 /etc/network/interfaces：
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto eth1`
	`iface eth1 inet manual`
	
	`auto br0`
	`iface br0 inet dhcp`
	`  bridge_ports eth0`

RHEL 或 CentOS Linux	編輯 /etc/sysconfig/network-scripts/ifcfg-ens32：
	`DEVICE="ens32"`
	`  TYPE="Ethernet"`
	`  NAME="ens32"`
	`  UUID="<something>"`
	`  BOOTPROTO="none"`
	`  HWADDR="<something>"`
	`  ONBOOT="yes"`
	`  NM_CONTROLLED="no"`
	`  BRIDGE="br0"`
	
	編輯 /etc/sysconfig/network-scripts/ifcfg-ens33：
	`DEVICE="ens33"`
	`  TYPE="Ethernet"`
	`  NAME="ens33"`
	`  UUID="<something>"`
	`  BOOTPROTO="none"`
	`  HWADDR="<something>"`
	`  ONBOOT="yes"`
	`  NM_CONTROLLED="no"`
	
	編輯 /etc/sysconfig/network-scripts/ifcfg-br0：
	`DEVICE="br0"`
	`   BOOTPROTO="dhcp"`
	`   NM_CONTROLLED="no"`
	`   ONBOOT="yes"`
	`   TYPE="Bridge"`

SUSE Linux Enterprise Server	

重要 在 Ubuntu 上，所有網路組態皆必須在 /etc/network/interfaces 中指定。請勿建立個別的網路組態檔 (例如 /etc/network/ifcfg-eth1)，這可能會導致傳輸節點建立失敗。

KVM 主機設定為傳輸節點後，即會建立橋接器介面「nsx-vtep0.0」。在 Ubuntu 中，`/etc/network/interfaces` 會包含如下的項目：

```
iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

在 RHEL 中，主機 NSX 代理程式 (nsxa) 會建立名為 ifcfg-nsx-vtep0.0 的組態檔，其中包含下列項目：

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

在 SUSE 中，

9 重新啟動網路服務 `systemctl restart network` 或將 Linux 伺服器重新開機，以使網路變更生效。

在 KVM CLI 中管理您的客體虛擬機器

NSX Manager 可安裝為 KVM 虛擬機器。此外，KVM 也可用作 NSX-T Data Center 傳輸節點的 Hypervisor。

KVM 客體虛擬機器管理已超出本指南的涵蓋範圍。不過，以下仍提供一些簡單的 KVM CLI 命令作為入門。

若要在 KVM CLI 中管理您的客體虛擬機器，請使用 `virsh` 命令。以下提供一些常用的 `virsh` 命令。如需其他資訊，請參閱 KVM 說明文件。

```
# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
```

```
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```

在 Linux CLI 中，`ifconfig` 命令會顯示 vnetX 介面，這會呈現為客體虛擬機器建立的介面。如果您新增其他客體虛擬機器，則會新增其他 vnetX 介面。

```
ifconfig
...

vnet0     Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
          inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

在 KVM 上安裝 NSX Manager

NSX Manager 可在 KVM 主機上安裝為虛擬應用裝置。

QCOW2 安裝程序會使用 Linux 命令列工具 guestfish 將虛擬機器設定寫入 QCOW2 檔案中。

必要條件

- KVM 設定。請參閱設定 KVM。
- 在 KVM 主機上部署 QCOW2 映像的權限。
- 確認 guestinfo 中的密碼符合密碼複雜性需求，以便在安裝後登入。請參閱 NSX Manager 安裝。
- 請自行熟悉 NSX Manager 資源需求。請參閱 NSX Manager 虛擬機器系統需求。
- 如果您想要安裝 Ubuntu 作業系統，建議您先安裝 Ubuntu 18.04 版，再將 NSX Manager 安裝在 KVM 主機上。

程序

1. 從 **nsx-unified-appliance > exports > kvm** 資料夾下載 NSX Manager QCOW2 映像。
2. 使用 SCP 或同步將其複製到即將執行 NSX Manager 的 KVM 機器。
3. (僅限 Ubuntu) 將目前登入的使用者新增為 libvirtd 使用者：

   ```
   adduser $USER libvirtd
   ```

4 在您儲存 QCOW2 映像的相同目錄中建立名為 guestinfo.xml 的檔案，並為其填入 NSX Manager 虛擬機器的內容。

內容	說明
■ **nsx_cli_passwd_0** ■ **nsx_cli_audit_passwd_0** ■ **nsx_passwd_0**	密碼必須符合密碼強度限制。 ■ 至少 12 個字元 ■ 至少 1 個小寫字母 ■ 至少 1 個大寫字母 ■ 至少 1 個數字 ■ 至少 1 個特殊字元 ■ 至少 5 個不同字元 ■ 無字典字組 ■ 無回文 ■ 不允許使用四個以上單純字元序列
nsx_hostname	輸入 NSX Manager 的主機名稱。主機名稱必須是有效的網域名稱。請確定以點分隔的每個主機名稱部分 (網域/子網域) 都必須以字母字元開頭。
nsx_role	■ *nsx-manager*：必要。此角色名稱會安裝 NSX Manager 應用裝置。 ■ *nsx-cloud-service-manager*：選用。安裝 NSX Manager 之後，請使用此角色名稱來安裝適用於 NSX Cloud 的 Cloud Service Manager 應用裝置。
nsx_isSSHEnabled	您可以啟用或停用此內容。如果啟用，您可以使用 SSH 登入 NSX Manager。
nsx_allowSSHRootLogin	您可以啟用或停用此內容。如果啟用，您可以使用 SSH 並以根使用者的身分登入 NSX Manager。若要能夠使用此內容，則必須啟用 `nsx_isSSHEnabled`。
■ **nsx_dns1_0** ■ **nsx_ntp_0** ■ **nsx_domain_0** ■ **nsx_gateway_0** ■ **nsx_netmask_0** ■ **nsx_ip_0**	輸入預設閘道的 IP 位址、管理網路 IPv4、管理網路的網路遮罩、DNS 和 NTP IP 位址。

例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
   <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
```

```
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
   </PropertySection>
</Environment>
```

備註 在此範例中，nsx_isSSHEnabled 和 nsx_allowSSHRootLogin 皆已啟用。當這兩個選項停用時，您將無法對 NSX Manager 命令列進行 SSH 連線或登入。如果您啟用 nsx_isSSHEnabled，但未啟用 nsx_allowSSHRootLogin，則可以使用 SSH 連線至 NSX Manager，但無法以根使用者身分登入。

5 使用 guestfish 將 guestinfo.xml 檔案寫入 QCOW2 映像中。

備註 在 guestinfo 資訊寫入至 QCOW2 映像後，即無法覆寫該資訊。

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
guestinfo
```

6 使用 virt-install 命令部署 QCOW2 映像。

VCPU 和 RAM 值均適用於大型虛擬機器。網路名稱和連接埠群組名稱專屬於您的環境。模型必須是 virtio。

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole              \
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

7 確認已部署 NSX Manager。

```
virsh list --all

Id    Name             State
----------------------------------
18    nsx-manager1     running
```

8 開啟 NSX Manager 主控台並登入。

```
virsh console 18
Connected to domain nsx-manager1
```

```
Escape character is ^]

nsx-manager1 login: admin
Password:
```

9 在 NSX Manager 開機後，以 Admin 身分登入 CLI 並執行 `get interface eth0` 命令，以確認 IP 位址已如預期般套用。

10 執行 `get services` 以確認服務正在執行。

11 確認 NSX Manager 具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX Manager 執行 Ping 偵測。
- NSX Manager 可以對其預設閘道執行 Ping 偵測。
- NSX Manager 可以使用管理介面，對位於相同網路中做為 NSX Manager 的 Hypervisor 主機執行 Ping 偵測。
- NSX Manager 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。
- 如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Manager。

如果未建立連線，請確定虛擬應用裝置的網路介面卡位於適當的網路或 VLAN。

12 結束 KVM 主控台。

```
control-]
```

13 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

登入新建立的 NSX Manager

安裝 NSX Manager 後，您可以利用使用者介面執行其他安裝工作。

安裝 NSX Manager 後，您可以加入 NSX-T Data Center 的客戶經驗改進計劃 (CEIP)。如需有關此計劃的詳細資訊 (包括如何在之後加入或退出計劃)，請參閱《NSX-T Data Center 管理指南》中的〈客戶經驗改進計劃〉。

必要條件

確認已安裝 NSX Manager。請參閱安裝 NSX Manager 和可用應用裝置。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

使用者授權合約隨即出現。

2 閱讀並接受使用者授權合約條款。

3 選取是否加入 VMware 的客戶經驗改進計劃 (CEIP)。

4 按一下**儲存**

在 KVM 主機上安裝第三方套件

若要準備讓 KVM 主機成為網狀架構節點，您必須安裝某些第三方套件。

必要條件

- (RHEL 和 CentOS Linux) 在安裝第三方套件前，請執行下列命令來安裝虛擬化套件。

```
yum groupinstall “Virtualization Hypervisor”
yum groupinstall “Virtualization Client”
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
```

  如果您無法安裝套件，可在新安裝時使用 `yum install glibc.i686 nspr` 命令手動進行安裝。

- (Ubuntu) 在安裝第三方套件前，請執行下列命令來安裝虛擬化套件。

```
apt install -y \
qemu-kvm \
libvirt-bin \
virtinst \
virt-manager \
virt-viewer \
ubuntu-vm-builder \
bridge-utils
```

- (SUSE Linux Enterprise Server) 在安裝第三方套件前，請執行下列命令來安裝虛擬化套件。

```
libcap-progs
```

程序

- 在 Ubuntu 上，執行 `apt-get install <package_name>` 手動安裝第三方套件。

Ubuntu 18.04 套件	Ubuntu 16.04 套件
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms make	libboost-chrono1.58.0 libboost-filesystem1.58.0 libgoogle-glog0v5 libgoogle-perftools4 libprotobuf9v5 traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl libboost-date-time1.58.0 libleveldb1v5 python-gevent python-protobuf libboost-program-options1.58.0 dkms

- 在 RHEL 和 CentOS Linux 上，執行 `yum install <package_name>` 手動安裝第三方套件。

  如果您手動準備已登錄至 RHEL 或 CentOS 的主機，則不需要在主機上安裝第三方套件。

RHEL 7.6、7.5 和 7.4	CentOS Linux 7.5 和 7.4
wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump	wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump

- 在 SUSE 上，執行 `zypper install <package_name>` 手動安裝第三方套件。

SUSE Linux Enterprise Server 12.0
python-simplejson python-PyYAML python-netaddr lsb-release

確認 RHEL KVM 主機上的 Open vSwitch 版本

如果 OVS 套件存在於 RHEL 主機上，您必須移除現有的套件並安裝支援的套件。

支援的 Open vSwitch 版本為 2.9.1.8614397-1。

程序

1 確認主機上已安裝目前版本的 Open vSwitch。

```
ovs-vswitchd --version
```

如果您的 Open vSwitch 為較新或較舊的版本，則必須以支援的版本取代此 Open vSwitch 版本。

2 開啟 Open vSwitch 資料夾。

3 刪除下列 Open vSwitch 套件。

- kmod-openvswitch
- openvswitch
- openvswitch-selinux-policy

4 此外，新增 NSX-T Data Center 所需的 Open vSwitch 套件。

a 以管理員身分登入主機。

b 將 nsx-lcp 檔案下載並複製到 /tmp 目錄中。

c 將套件解壓縮。

```
tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz
```

d 導覽至套件目錄。

```
cd nsx-lcp-rhel75_x86_64/
```

e 以支援的版本取代現有 Open vSwitch 版本。

- 對於較新的 Open vSwitch 版本，請使用 `--nodeps` 命令。

  例如，rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps

  rpm -Uvh openvswitch-*.rpm --nodeps

- 對於較舊的 Open vSwitch 版本，請使用 `--force` 命令。

  例如，rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps --force

  rpm -Uvh openvswitch-*.rpm --nodeps --force

使用 CLI 部署 NSX Manager 節點以形成叢集

使用 CLI 加入 NSX Manager 以形成叢集，可確保叢集中的所有 NSX Manager 節點可以彼此通訊。

必要條件

必須完成 NSX-T Data Center 元件的安裝。

程序

1 開啟第一個部署的 NSX Manager 節點的 SSH 工作階段。

2 使用管理員認證登入。

3 在 NSX Manager 節點上，執行 `get certificate api thumbprint` 命令。

命令輸出是對此 NSX Manager 而言具有唯一性的數字字串。

4 執行 `get cluster config` 命令，以取得第一個部署的 NSX Manager 叢集識別碼。

5 新增 NSX Manager 節點至該叢集。

備註 您必須在新部署的 NSX Manager 節點上執行 join 命令。

請提供下列 NSX Manager 資訊：

- 您要加入之主機名稱或 IP 位址節點
- 叢集識別碼
- 使用者名稱
- 密碼
- 憑證指紋

您可以使用 CLI 命令或 API 呼叫。

- CLI 命令

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- API 呼叫 `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

加入和叢集穩定化程序可能需要 10-15 分鐘。

6 新增第三個 NSX Manager 節點至叢集。

重複步驟 5。

7 在您的主機上執行 `get cluster status` 命令以確認叢集狀態。

8 選取 **系統 > 應用裝置 > 概觀**並確認叢集連線。

後續步驟

建立傳輸區域。請參閱 建立獨立主機或裸機伺服器傳輸節點。

使用 ISO 檔案或 PXE 安裝 NSX Edge

您可以在裸機上自動安裝 NSX Edge 裝置，或使用 PXE 將其安裝為虛擬機器。

備註 NSX Manager 不支援 PXE 開機安裝。您也無法設定網路設定，例如 IP 位址、閘道、網路遮罩、NTP 和 DNS。

透過 ISO 檔案將 NSX Edge 安裝為虛擬應用裝置

您可以使用 ISO 檔案手動安裝 NSX Edge 虛擬機器。

重要 NSX-T Data Center 元件虛擬機器安裝包含 VMware Tools。NSX-T Data Center 應用裝置不支援移除或升級 VMware Tools。

必要條件

- 請參閱 NSX Edge 安裝 中的 NSX Edge 網路需求。

程序

1 移至您的 MyVMware 帳戶 (myvmware.com) 並導覽至 **VMware NSX-T Data Center > 下載**。

2 找到並下載 NSX Edge 適用的 ISO 檔案。

3 在 vSphere Client 中，選取主機資料存放區。

4 選取**檔案 > 上傳檔案 > 上傳檔案至資料存放區**、瀏覽至 ISO 檔案，然後上傳。

如果您使用的是自我簽署的憑證，請在瀏覽器中開啟 IP 位址、接受憑證，然後重新上傳 ISO 檔案。

5 在 vSphere Client 詳細目錄中，選取您已上傳 ISO 檔案的主機。或是在 vSphere Client 中，

6 按一下滑鼠右鍵，然後選取**新增虛擬機器**。

7 為 NSX Edge 應用裝置選取計算資源。

8 選取用來儲存 NSX Edge 應用裝置檔案的資料存放區。

9 接受 NSX Edge 虛擬機器的預設相容性。

10 為 NSX Edge 虛擬機器選取支援的 ESXi 作業系統。

11 設定虛擬硬體。

- 新增硬碟 - **200 GB**
- 新增網路 - **VM Network**
- 新增 CD/DVD 光碟機 - **Datastore ISO File**

  您必須按一下**連線**，將 NSX Edge ISO 檔案繫結至虛擬機器。

12 將新的 NSX Edge 虛擬機器開啟電源。

13 在 ISO 開機期間，開啟虛擬機器主控台，然後選擇**自動安裝**。

在您按 Enter 鍵後，系統可能會暫停 10 秒鐘。

在安裝期間，安裝程式會提示您輸入管理介面的 VLAN 識別碼。選取**是**，然後輸入 VLAN 識別碼以便為網路介面建立 VLAN 子介面。如果您不想對封包設定 VLAN 標記，請選取**否**。

在開啟電源期間，虛擬機器會要求透過 DHCP 進行網路組態。如果您的環境不適用 DHCP，則安裝程式會提示您進行 IP 設定。

依預設，根登入密碼為 **vmware**，而管理員登入密碼為 **default**。

當您首次登入時，系統會提示您變更密碼。此密碼變更方法具有嚴格的複雜性規則，所含規則如下：

- 至少 12 個字元
- 至少 1 個小寫字母
- 至少 1 個大寫字母
- 至少 1 個數字
- 至少 1 個特殊字元
- 至少 5 個不同字元
- 無字典字組
- 無回文
- 不允許使用四個以上單純字元序列

重要 在設定具有足夠複雜性的密碼之前，您無法啟動應用裝置上的核心服務。

14 若要獲得最佳效能，請保留 NSX Edge 應用裝置所需的記憶體。

請設定保留，以確保 NSX Edge 具有足夠記憶體來讓執行更有效率。請參閱 NSX Edge 虛擬機器系統需求。

15 NSX Edge 啟動後，使用管理員認證登入 CLI。

備註 在 NSX Edge 啟動後，如果首次登入時不使用管理員認證，則數據平面服務不會在 NSX Edge 上自動啟動。

16 您可以使用三種方法來設定管理介面。

- 未標記的介面。此介面類型會建立頻外管理介面。

  (DHCP) `set interface eth0 dhcp plane mgmt`

  (靜態) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- 已標記的介面。

  `set interface eth0 vlan <vlan_ID> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  (靜態) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- 頻內介面。

  `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  (靜態) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

17 (選用) 啟動 SSH 服務。執行 `start service ssh`。

18 執行 `get interface eth0.<vlan_ID>` 命令以確認 IP 位址已按預期套用。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

備註 在並非由 NSX 管理的主機上啟動 NSX Edge 虛擬機器時，請確認您已在資料 NIC 的實體主機交換器上將 MTU 設定設為 1600 (而非 1500)。

19 (已標記的介面和頻內介面) 在建立新的 VLAN 管理介面之前，必須先清除任何現有的 VLAN 管理介面。

`Clear interface eth0.<vlan_ID>`

若要設定新的介面，請參閱步驟 15。

20 確認 NSX Edge 應用裝置具有必要的連線。

如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Edge。

- 您可以對 NSX Edge 執行 Ping 偵測。
- NSX Edge 可以對其預設閘道執行 Ping 偵測。
- NSX Edge 可以對位於相同網路中作為 NSX Edge 的 Hypervisor 主機執行 Ping 偵測。
- NSX Edge 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。

21 疑難排解連線問題。

備註 如果未建立連線，請確定虛擬機器網路介面卡位於適當的網路或 VLAN。

依預設，NSX Edge 資料路徑會宣告所有虛擬機器 NIC，但管理 NIC 除外 (即具有 IP 位址和預設路由的 NIC)。如果將 NIC 錯誤地指派為管理介面，請遵循下列步驟來使用 DHCP，以將管理 IP 位址指派給正確的 NIC。

a 登入 CLI 並輸入 **`stop service dataplane`** 命令。

b 輸入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 將 *interface* 放入 DHCP 網路並等候系統將 IP 位址指派給該 *interface*。

d 輸入 **`start service dataplane`** 命令。

用於 VLAN 上行和通道覆疊的資料路徑 fp-ethX 連接埠會顯示在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中。

後續步驟

如果您未將 NSX Edge 加入管理平面，請參閱將 NSX Edge 加入管理平面。

透過 ISO 檔案在裸機上安裝 NSX Edge

您可以使用 ISO 檔案，在裸機上手動安裝 NSX Edge 裝置。此作業包括設定網路設定，例如 IP 位址、閘道、網路遮罩、NTP 和 DNS。

必要條件

- 確認系統 BIOS 模式設為舊版 BIOS。
- 請參閱 NSX Edge 安裝 中的 NSX Edge 網路需求。

程序

1 在 **nsx-edgenode > publish > xenial_amd64** 資料夾下找到 NSX Edge 應用裝置 ISO 檔案。

將 ISO 檔案下載到您的電腦。

2 登入裸機的 ILO。

3 按一下虛擬主控台預覽中的**啟動**。

4 選取**虛擬媒體 > 連線虛擬媒體**。

請稍候幾秒，以等待虛擬媒體完成連線。

5 選取**虛擬媒體 > 對應 CD/DVD**，然後瀏覽到 ISO 檔案。

6 選取**下次開機 > 虛擬 CD/DVD/ISO**。

7 選取**電源 > 重設系統 (暖開機)**。

安裝持續時間取決於裸機環境。

8 選擇**自動安裝**。

在您按 Enter 鍵後，系統可能會暫停 10 秒鐘。

9 選取適用的主要網路介面。

在開啟電源期間，安裝程式會要求透過 DHCP 進行網路組態。如果您的環境不適用 DHCP，則安裝程式會提示您進行 IP 設定。

依預設，根登入密碼為 **vmware**，而管理員登入密碼為 **default**。

10 開啟 NSX Edge 的主控台以追蹤開機程序。

如果主控台視窗並未開啟，請確定已允許快顯視窗。

11 NSX Edge 啟動後，使用管理員認證登入 CLI。

備註 在 NSX Edge 啟動後，如果首次登入時不使用管理員認證，則數據平面服務不會在 NSX Edge 上自動啟動。

12 重新開機後，您可以使用管理員或根認證登入。預設根密碼為 `vmware`。

13 您可以使用三種方法來設定管理介面。

- 未標記的介面。此介面類型會建立頻外管理介面。

  (DHCP) `set interface eth0 dhcp plane mgmt`

  (靜態) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- 已標記的介面。

  `set interface eth0 vlan <vlan_ID> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  (靜態) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- 頻內介面。

  `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  (靜態) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

14 執行 `get interface eth0.<vlan_ID>` 命令以確認 IP 位址已按預期套用。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

備註 在並非由 NSX 管理的主機上啟動 NSX Edge 虛擬機器時，請確認您已在資料 NIC 的實體主機交換器上將 MTU 設定設為 1600 (而非 1500)。

15 (已標記的介面和頻內介面) 在建立新的 VLAN 管理介面之前，必須先清除任何現有的 VLAN 管理介面。

`clear interface eth0.<vlan_ID>`

若要設定新的介面，請參閱步驟 13。

16 確認 NSX Edge 應用裝置具有必要的連線。

如果您已啟用 SSH，請確定您可以使用 SSH 連線至 NSX Edge。

- 您可以對 NSX Edge 執行 Ping 偵測。
- NSX Edge 可以對其預設閘道執行 Ping 偵測。
- NSX Edge 可以對位於相同網路中作為 NSX Edge 的 Hypervisor 主機執行 Ping 偵測。
- NSX Edge 可以對其 DNS 伺服器和其 NTP 伺服器執行 Ping 偵測。

17 疑難排解連線問題。

備註 如果未建立連線，請確定虛擬機器網路介面卡位於適當的網路或 VLAN。

依預設，NSX Edge 資料路徑會宣告所有虛擬機器 NIC，但管理 NIC 除外 (即具有 IP 位址和預設路由的 NIC)。如果將 NIC 錯誤地指派為管理介面，請遵循下列步驟來使用 DHCP，以將管理 IP 位址指派給正確的 NIC。

a 登入 CLI 並輸入 **`stop service dataplane`** 命令。

b 輸入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 將 *interface* 放入 DHCP 網路並等候系統將 IP 位址指派給該 *interface*。

d 輸入 **`start service dataplane`** 命令。

用於 VLAN 上行和通道覆疊的資料路徑 fp-ethX 連接埠會顯示在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中。

後續步驟

將 NSX Edge 加入管理平面。請參閱將 NSX Edge 加入管理平面。

在 PXE 伺服器上安裝 NSX Edge

PXE 由數個元件組成：DHCP、HTTP 和 TFTP。此程序將示範如何在 Ubuntu 上設定 PXE 伺服器。

DHCP 會以動態方式將 IP 設定散佈至 NSX-T Data Center 元件，例如 NSX Edge。在 PXE 環境中，DHCP 伺服器允許 NSX Edge 自動要求及接收 IP 位址。

TFTP 是一種檔案傳輸通訊協定。TFTP 伺服器一律會接聽網路上的 PXE 用戶端。當它偵測到任何網路 PXE 用戶端要求 PXE 服務時，即會提供包含在 preseed 檔案中的 NSX-T Data Center 元件 ISO 檔案和安裝設定。

必要條件

- PXE 伺服器必須可在您的部署環境中使用。PXE 伺服器可設定於任何 Linux 發行版上。PXE 伺服器必須有兩個介面，一個用於外部通訊，另一個用來提供 DHCP IP 和 TFTP 服務。

  如果您有多個管理網路，則可以新增從 NSX-T Data Center 應用裝置到其他網路的靜態路由。
- 確認預先植入的組態檔在 -- 後設定了 net.ifnames=0 和 biosdevname=0 參數，以便在重新開機後能夠保留。
- 請參閱 NSX Edge 安裝 中的 NSX Edge 網路需求。

程序

1 (選擇性) 使用 kickstart 檔案，以便在 Ubuntu 伺服器上設定新的 TFTP 或 DHCP 服務。

  kickstart 檔案是一種文字檔，其中包含您在第一次開機後對應用裝置執行的 CLI 命令。

  請根據 kickstart 檔案所指向的 PXE 伺服器為其命名。例如：

```
nsxcli.install
```

  該檔案必須複製到您的 Web 伺服器 (例如在 `/var/www/html/nsx-edge/nsxcli.install` 上)。

  在 kickstart 檔案中，您可以新增 CLI 命令。例如，設定管理介面的 IP 位址：

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

  若要變更 Admin 使用者密碼：

```
set user admin password <new_password> old-password <old-password>
```

  如果您在 preseed.cfg 檔案中指定了密碼，請在 kickstart 檔案中使用相同的密碼。否則，請使用預設密碼「default」。

  若要將 NSX Edge 加入管理平面：

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager password>
```

2 建立兩個介面，一個用於管理，另一個用於 DHCP 和 TFTP 服務。

請確定 DHCP/TFTP 介面位於 NSX Edge 所在的相同子網路中。

例如，如果 NSX Edge 管理介面將位於 192.168.210.0/24 子網路中，請將 eth1 置於相同的子網路中。

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
  address 192.168.110.81
  gateway 192.168.110.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
  address 192.168.210.82
  gateway 192.168.210.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10
```

3 安裝 DHCP 伺服器軟體。

```
sudo apt-get install isc-dhcp-server -y
```

4 編輯 `/etc/default/isc-dhcp-server` 檔案，並新增提供 DHCP 服務的介面。

```
INTERFACES="eth1"
```

5 (選擇性) 如果您要讓此 DHCP 伺服器成為本機網路的正式 DHCP 伺服器，請將 `/etc/dhcp/dhcpd.conf` 檔案中的 **authoritative;** 一行取消註解。

```
...
authoritative;
...
```

6 在 `/etc/dhcp/dhcpd.conf` 檔案中，定義 PXE 網路的 DHCP 設定。

例如：

```
subnet 192.168.210.0 netmask 255.255.255.0 {
   range 192.168.210.90 192.168.210.95;
   option subnet-mask 255.255.255.0;
   option domain-name-servers 192.168.110.10;
   option routers 192.168.210.1;
```

```
   option broadcast-address 192.168.210.255;
   default-lease-time 600;
   max-lease-time 7200;
}
```

7 啟動 DHCP 服務。

```
sudo service isc-dhcp-server start
```

8 確認 DHCP 服務正在執行。

```
service --status-all | grep dhcp
```

9 安裝 PXE 開機所需的 Apache、TFTP 和其他元件。

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

10 確認 TFTP 和 Apache 正在執行。

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```

11 將以下幾行新增至 /etc/default/tftpd-hpa 檔案。

```
RUN_DAEMON="yes"
OPTIONS="-l -s /var/lib/tftpboot"
```

12 將以下一行新增至 /etc/inetd.conf 檔案。

```
tftp    dgram   udp    wait    root    /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 重新啟動 TFTP 服務。

```
sudo /etc/init.d/tftpd-hpa restart
```

14 將 NSX Edge 安裝程式 ISO 檔案複製或下載到暫存資料夾。

15 掛接 ISO 檔案，並將安裝元件複製到 TFTP 伺服器和 Apache 伺服器。

```
            sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
            cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

16 (選擇性) 編輯 /var/www/html/nsx-edge/preseed.cfg 檔案以修改加密密碼。

您可以使用 Linux 工具 (例如 mkpasswd) 來建立密碼雜湊。

```
sudo apt-get install whoissudo mkpasswd -m sha-512

Password:
$6$SUFGqs[...]FcoHLijOuFD
```

a 修改根密碼，編輯 /var/www/html/nsx-edge/preseed.cfg，然後搜尋以下一行：

```
d-i passwd/root-password-crypted password $6$tgmLNLMp$9BuAHhN...
```

b 取代雜湊字串。

您不需要逸出任何特殊字元，如 $、'、" 或 \ 等。

c 將 usermod 命令新增至 preseed.cfg，以設定根使用者和/或管理員的密碼。

例如，您可以搜尋 echo 'VMware NSX Edge' 一行，並新增下列命令。

```
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' admin; \
```

雜湊字串為範例。您必須逸出所有特殊字元。第一個 usermod 命令中的根密碼會取代 d-i passwd/root-password-crypted password 6tgm... 中設定的密碼。

如果您使用 usermod 命令設定密碼，則使用者在第一次登入時將不會看見變更密碼的提示。否則，使用者必須在第一次登入時變更密碼。

17 將以下幾行新增至 /var/lib/tftpboot/pxelinux.cfg/default 檔案。

將 192.168.210.82 取代為您 TFTP 伺服器的 IP 位址。

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/allow_unauthenticated=true
preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/country=manual mirror/http/
hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/
http/directory=/nsx-edge initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```

18 將以下幾行新增至 /etc/dhcp/dhcpd.conf 檔案。

將 192.168.210.82 取代為您 DHCP 伺服器的 IP 位址。

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 重新啟動 DHCP 服務。

```
sudo service isc-dhcp-server restart
```

備註 如果傳回錯誤 (例如：「停止: 未知的執行個體: 啟動: 工作無法啟動」)，請執行 `sudo /etc/init.d/isc-dhcp-server stop`，然後執行 `sudo /etc/init.d/isc-dhcp-server start`。`sudo /etc/init.d/isc-dhcp-server start` 命令會傳回錯誤來源的相關資訊。

後續步驟

使用 ISO 檔案在裸機上安裝 NSX Edge。請參閱透過 ISO 檔案在裸機上安裝 NSX Edge 或透過 ISO 檔案將 NSX Edge 安裝為虛擬應用裝置。

設定裸機伺服器以使用 NSX-T Data Center

6

若要在裸機伺服器上使用 NSX-T Data Center，您必須安裝支援的第三方套件。

NSX-T Data Center 支援裸機伺服器的方式有兩種：做為主機傳輸節點以及做為 NSX Manager 的主機。

請確定您有支援的裸機伺服器版本。請參閱裸機伺服器系統需求。

備註 如果您的 NSX Edge 位於虛擬機器構成要素，且您想要使用 NSX DHCP 服務 (在以 VLAN 為基礎的邏輯交換器上部署)，您必須在部署 NSX Edge 所在的裸機上將偽造的傳輸選項設定為「接受」。請參閱 vSphere 產品說明文件中「偽造的傳輸」。

本章節討論下列主題：

- 在裸機伺服器上安裝第三方套件
- 建立裸機伺服器工作負載的應用程式介面

在裸機伺服器上安裝第三方套件

若要準備裸機伺服器來當作網狀架構節點，您必須安裝某些第三方套件。

必要條件

- 請確認執行安裝的使用者具有管理員權限可執行下列動作，其中一些動作可能需要 sudo 權限：
  - 下載並解壓縮服務包。
  - 執行 dpkg 或 rpm 命令以安裝/解除安裝 NSX 元件。
  - 執行 nsxcli 命令以執行加入管理平面命令。
- 確認已安裝虛擬化套件。
  - Redhat 或 CentOS - `yum install libvirt-libs`
  - Ubuntu - `apt-get install libvirt0`
  - SUSE - `zypper install libvirt-libs`

程序

- 在 Ubuntu 上，執行 `apt-get install <package_name>` 以安裝第三方套件。

Ubuntu18.04	Ubuntu16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0

- 在 RHEL 或 CentOS 上，執行 `yum install` 以安裝第三方套件。

RHEL 7.4、7.5 和 7.6	CentOS 7.4、7.5 和 7.6
tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs	tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs

- 在 SUSE 上，執行 `zypper install <package_name>` 手動安裝第三方套件。

  SUSE 12.0

  ```
  net-tools
  tcpdump
  python-simplejson
  python-netaddr
  python-PyYAML
  python-six
  libunwind
  wget
  lsof
  libcap-progs
  libvirt-libs
  ```

建立裸機伺服器工作負載的應用程式介面

您必須先設定 NSX-T Data Center 並安裝 Linux 第三方套件，再建立或移轉裸機伺服器工作負載的應用程式介面。

NSX-T Data Center 不支援 Linux 作業系統介面繫結。您必須對裸機伺服器傳輸節點使用 Open vSwitch (OVS) 繫結。請參閱知識庫文章 67835：Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T (裸機伺服器在 NSX-T 中支援傳輸節點組態的 OVS 繫結)。

程序

1. 安裝所需的第三方套件。

   請參閱在裸機伺服器上安裝第三方套件。

2. 設定 TCP 和 UDP 連接埠。

   請參閱由 ESXi、KVM 主機和裸機伺服器使用的 TCP 和 UDP 連接埠。

3. 將裸機伺服器新增到 NSX-T Data Center 網狀架構，然後建立傳輸節點。

   請參閱 建立獨立主機或裸機伺服器傳輸節點。

4. 使用 Ansible 指導手冊建立應用程式介面。

   請參閱 https://github.com/vmware/bare-metal-server-integration-with-nsxt。

設定 NSX Manager 叢集

7

下列小節說明如何設定 NSX Manager 叢集、詳細說明叢集需求，並提供特定站台部署的建議。這些小節也說明您可以使用 vSphere HA 搭配 NSX-T Data Center，在執行 NSX Manager 節點失敗的主機時啟用快速復原。

本章節討論下列主題：

- NSX Manager 叢集需求
- 單一站台、雙站台和多個站台的 NSX Manager 叢集需求

NSX Manager 叢集需求

下列需求適用於 NSX Manager 叢集組態：

- 在生產環境中，NSX Manager 叢集必須具有三個成員，以避免管理和控制平面出現任何中斷。

  每個叢集成員應置於總計具有三部實體 Hypervisor 主機的唯一 Hypervisor 主機上。為了避免單一實體 Hypervisor 主機故障影響 NSX 控制平面，這是必要的。建議您套用反相似性規則，以確保所有三個叢集成員都在不同主機上執行。

  一般的生產運作狀態是三個節點 NSX Manager 叢集。但是，您可以新增其他的暫存 NSX Manager 節點，以允許變更 IP 位址。

  重要 NSX-T Data Center 2.4 起，NSX Manager 包含 NSX 中央控制平面程序。此服務對 NSX 的運作非常重要。如果完全失去 NSX Manager，或如果叢集從三個 NSX Manager 縮減到一個 NSX Manager，您將無法對您的環境進行拓撲變更，且以 NSX 為基礎機器的 vMotion 會失敗。

- 針對沒有任何生產工作負載的實驗室和概念驗證部署，您可以執行單一 NSX Manager 以節省資源。NSX Manager 節點可以部署在 ESXi 或 KVM 上。但是，不支援同時在 ESXi 和 KVM 上進行管理程式的混合部署。

重要 NSX-T Data Center 部署中的站台數目可能會影響需求。請參閱 單一站台、雙站台和多個站台的 NSX Manager 叢集需求。

單一站台、雙站台和多個站台的 NSX Manager 叢集需求

您的 NSX Manager 叢集組態將依部署是否為單一站台、雙站台或多個站台而有所不同。

您可以使用 vSphere HA 搭配 NSX-T Data Center，在執行 NSX Manager 節點失敗的主機中啟用快速復原。

備註 請參閱 vSphere 產品說明文件中的《建立和使用 vSphere HA 叢集》。

單一站台需求和建議

下列建議適用於單一站台 NSX-T Data Center 部署。

- 建議您將 NSX Manager 置於不同的主機上，以避免單一主機故障影響多個管理員。
- NSX Manager 之間的最大延遲時間是 10 毫秒。
- 您可以將 NSX Manager 放在不同的 vSphere 叢集中，或放在一般 vSphere 叢集中。
- 建議您將 NSX Manager 放置在不同的管理子網路，或是共用的管理子網路。使用 vSphere HA 時，建議使用共用的管理子網路，以便 vSphere 復原的 NSX Manager 可以保留其 IP 位址。
- 建議您也將 NSX Manager 放置在共用儲存區上。針對 vSphere HA，請檢閱該解決方案的需求。

您也可以使用 vSphere HA 搭配 NSX-T，當 NSX Manager 執行所在的主機發生故障時，提供復原遺失的 NSX Manager。

案例範例：

- 當中部署所有三個 NSX Manager 的 vSphere 叢集。
- vSphere 叢集是由四個或更多個主機所組成。
  - 部署 nsxmgr-01 的 Host-01
  - 部署 nsxmgr-02 的 Host-02
  - 部署 nsxmgr-03 的 Host-03
  - 未部署 NSX Manager 的 Host-04
- vSphere HA 已設定為將任何遺失的 NSX Manager (例如，nsxmgr-01) 從任何主機 (例如，Host-01) 復原到 Host-04。

因此，在任何執行 NSX Manager 的主機遺失時，vSphere 會復原 Host-04 上遺失的 NSX Manager。

雙站台需求和建議

下列建議適用於雙站台 (站台 A/站台 B) NSX-T Data Center 部署。

- 不建議在沒有 vSphere HA 的雙站台案例中部署 NSX Manager。在此案例中，其中一個站台需要部署兩個 NSX Manager，且遺失該站台將會影響 NSX-T Data Center 的作業。
- 可以利用下列考量事項在具有 vSphere HA 的雙站台案例中完成部署 NSX Manager：
  - 單一延伸的 vSphere 叢集包含 NSX Manager 的所有主機。
  - 三個 NSX Manager 全都已部署到一般管理子網路/VLAN，以在復原遺失的 NSX Manager 時允許 IP 位址保留。
  - 如需了解站台之間的延遲時間，請參閱儲存區產品需求。

案例範例：

- 當中部署所有三個 NSX Manager 的 vSphere 叢集。
- vSphere 叢集包含六台以上的主機，站台 A 中有三台主機，而站台 B 中有三台主機。
- 這三個 NSX Manager 會部署到具有一或多其他主機用於放置所復原 NSX Manager 的不同主機：

  站台 A：

  - 部署 nsxmgr-01 的 Host-01
  - 部署 nsxmgr-02 的 Host-02
  - 部署 nsxmgr-03 的 Host-03

  站台 B：

  - 未部署 NSX Manager 的 Host-04
  - Host-05 未部署 NSX Manager
  - Host-06 未部署 NSX Manager
- vSphere HA 已設定為從站台 A 中的任何主機 (例如，Host-01) 將任何遺失的 NSX Manager (例如，nsxmgr-01) 復原到站台 B 中的其中一個主機。

因此，站台 A 失敗時，vSphere HA 會將所有 NSX Manager 復原到站台 B 中的主機。

重要 您必須正確設定反相似性規則，以防止 NSX Manager 復原到相同的一般主機。

多個 (三個或多個) 站台需求和建議

下列建議適用於多站台 (站台 A/站台 B/站台 C) NSX-T Data Center 部署。

在具有三個或多個站台的案例中，您可以部署包含或不含 vSphere HA 的 NSX Manager。

如果您是部署不含 vSphere HA：

- 建議您每個站台使用不同的管理子網路或 VLAN。
- NSX Manager 之間的最大延遲時間是 10 毫秒。

案例範例 (三個站台)：

- 三個不同的 vSphere 叢集，每個站台一個。
- 至少每個站台有一台主機執行 NSX Manager：
  - 部署 nsxmgr-01 的 Host-01
  - 部署 nsxmgr-02 的 Host-02
  - 部署 nsxmgr-03 的 Host-03

故障案例：

- 單一站台故障：在其他站台中的兩個剩餘 NSX Manager 會繼續運作。NSX-T Data Center 處於已降級狀態，但仍可運作。建議您手動部署第三個 NSX Manager，以取代遺失的叢集成員。

- 兩個站台故障：遺失仲裁，因此影響 NSX-T Data Center 作業。

復原 NSX Manager 作業可能最多可能需要 20 分鐘，視環境的狀況而定，例如 CPU 速度、磁碟效能，以及其他部署因素。

傳輸區域和傳輸節點

8

傳輸區域和傳輸節點是 NSX-T Data Center 中的重要概念。

本章節討論下列主題：

- 建立傳輸區域
- 為通道端點 IP 位址建立 IP 集區
- 增強型資料路徑
- 設定設定檔
- 建立獨立主機或裸機伺服器傳輸節點
- NSX-T Data Center 核心模組的手動安裝
- NSX Edge 網路設定
- 建立 NSX Edge 傳輸節點
- 建立 NSX Edge 叢集

建立傳輸區域

傳輸區域會規定哪個主機，也就是哪個虛擬機器可以參與特定網路的使用。傳輸區域用來達成此目的之方法是限制可以「看到」邏輯交換器的主機，因此也會限制到可以連結至邏輯交換器的虛擬機器。傳輸區域可以橫跨一或多個主機叢集。

根據您的需求而定，NSX-T Data Center 環境可以包含一或多個傳輸區域。主機可以屬於多個傳輸區域。邏輯交換器僅能屬於一個傳輸區域。

NSX-T Data Center 不允許連線至位於第 2 層網路中不同傳輸區域的虛擬機器。邏輯交換器的橫跨範圍會限制在單一傳輸區域內，因此不同傳輸區域內的虛擬機器不能位於相同的第 2 層網路上。

覆疊傳輸區域會同時供主機傳輸節點和 NSX Edge 使用。當主機或 NSX Edge 傳輸節點新增至覆疊傳輸區域時，N-VDS 即會安裝在主機或 NSX Edge 上。

VLAN 傳輸區域會供 NSX Edge 和主機傳輸節點用於其 VLAN 上行。當 NSX Edge 新增至 VLAN 傳輸區域時，VLAN N-VDS 即會安裝在 NSX Edge 上。

N-VDS 可將邏輯路由器的上行和下行繫結至實體 NIC，來允許虛擬至實體的封包流量。

當您建立傳輸區域時，您必須為傳輸節點稍後新增至此傳輸區域時，將會在傳輸節點上安裝的 N-VDS 提供名稱。N-VDS 名稱可以是任何所需的名稱。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 傳輸區域 > 新增**。

3 輸入傳輸區域的名稱，並選擇性地輸入說明。

4 輸入 N-VDS 的名稱。

5 選取 N-VDS 模式。

- 套用到所有支援主機的**標準**模式。
- **增強型資料路徑**是僅套用到可屬於一個傳輸區域的 ESXi 主機 6.7 版及更新版本類型之傳輸節點的網路堆疊模式。

6 如果 N-VDS 模式設為 [標準]，請選取流量類型。

選項為**覆疊**和 **VLAN**。

7 如果 N-VDS 模式設為 [增強型資料路徑]，請選取流量類型。

選項為**覆疊**和 **VLAN**。

備註 在增強型資料路徑模式下，僅支援特定的 NIC 組態。確保您設定支援的 NIC。

8 輸入一或多個上行整併原則名稱。這些具名整併原則可供連結到傳輸區域的邏輯交換器使用。如果邏輯交換器找不到相符的具名整併原則，會使用預設上行整併原則。

9 在**傳輸區域**頁面上檢視新的傳輸區域。

10 (選擇性) 您也可以使用 `GET https://<nsx-mgr>/api/v1/transport-zones` API 呼叫檢視新的傳輸區域。


```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
```

```
      "_create_time": 1459547126454,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126454,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    },
    {
      "resource_type": "TransportZone",
      "description": "comp vlan transport zone",
      "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
      "display_name": "tz-vlan",
      "host_switch_name": "vlan-uplink-hostwitch",
      "transport_type": "VLAN",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126505,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126505,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    }
  ]
}
```


後續步驟

(選用) 建立自訂傳輸區域設定檔，並將它繫結至傳輸區域。您可以使用 `POST /api/v1/transportzone-profiles` API 建立自訂傳輸區域設定檔。沒有用於建立傳輸區域設定檔的 UI 工作流程。傳輸區域設定檔建立完成之後，您可以使用 `PUT /api/v1/transport-zones/<transport-zone-id>` API 在傳輸區域中找到它。

建立傳輸節點。請參閱 建立獨立主機或裸機伺服器傳輸節點。

為通道端點 IP 位址建立 IP 集區

您可以對通道端點使用 IP 集區。通道端點是外部 IP 標頭中所用的來源和目的地 IP 位址，用來識別哪些 Hypervisor 主機起始及結束了覆疊框架的 NSX-T Data Center 封裝。您也可以對通道端點 IP 位址使用 DHCP 或手動設定的 IP 集區。

如果您要同時使用 ESXi 和 KVM 主機，其中一個設計選項可能是對 ESXi 通道端點 IP 集區 (sub_a) 和 KVM 通道端點 IP 集區 (sub_b) 使用兩個不同的子網路。在此情況下，您必須在 KVM 主機上，使用專用的預設閘道新增 sub_a 的靜態路由。

Ubuntu 主機上所產生的路由表範例，其中 sub_a = 192.168.140.0，sub_b = 192.168.150.0。(例如，管理子網路可以是 192.168.130.0)。

核心 IP 路由表：

```
Destination         Gateway         Genmask         Iface
0.0.0.0             192.168.130.1   0.0.0.0         eth0
192.168.122.0       0.0.0.0         255.255.255.0   virbr0
192.168.130.0       0.0.0.0         255.255.255.0   eth0
192.168.140.0       192.168.150.1   255.255.255.0   nsx-vtep0.0
192.168.150.0       0.0.0.0         255.255.255.0   nsx-vtep0.0
```

至少有兩種不同方式可新增路由。對於這兩種方法，僅當透過編輯介面新增路由時，才會在主機重新開機後持續保存路由。如果使用 route add 命令新增路由，則在主機重新開機後不會保存該路由。

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

在 /etc/network/interfaces 中的「up ifconfig nsx-vtep0.0 up」之前，新增此靜態路由：

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**進階網路與安全性 > 詳細目錄 > 群組 > IP 集區 > 新增**。

3 輸入 IP 集區詳細資料。

選項	參數範例
名稱與說明	輸入 IP 集區與選擇性說明。
IP 範圍	IP 配置範圍 192.168.200.100 - 192.168.200.115
閘道	192.168.200.1
CIDR	以 CIDR 標記法表示的網路位址 192.168.200.0/24
DNS 伺服器	以逗號分隔的 DNS 伺服器清單 192.168.66.10
DNS 尾碼	corp.local

結果

[IP 集區] 頁面上列出了 IPv4 或 IPv6 位址集區。

您也可以使用 `GET https://<nsx-mgr>/api/v1/pools/ip-pools` API 呼叫來檢視 IP 集區清單。

後續步驟

建立上行設定檔。請參閱建立上行設定檔。

增強型資料路徑

增強型資料路徑是網路堆疊模式，一旦設定，便可提供卓越的網路效能。它主要針對 NFV 工作負載，這需要此模式提供的效能優勢。

只能在 ESXi 主機上以增強型資料路徑模式設定 N-VDS 交換器。ENS 還支援流經 Edge 虛擬機器的流量。

在增強型資料路徑模式下，您可以設定：

- 覆疊流量
- VLAN 流量

支援的 VMkernel NIC

藉由支援多個 ENS 主機交換器的 NSX-T Data Center，每台主機支援的 VMkernel NIC 數目上限為 32。

設定增強型資料路徑的高階程序

做為網路管理員，您必須先使用支援的 NIC 卡和驅動程式準備網路，然後在增強型資料路徑模式下建立支援 N-VDS 的傳輸區域。若要提升網路效能，您可以啟用負載平衡來源整併原則使其能夠感知 NUMA 節點。

高階步驟如下：

1 使用支援增強型資料路徑的 NIC 卡。

請參閱《VMware 相容性指南》，以瞭解支援增強型資料路徑的 NIC 卡。

在《VMware 相容性指南》頁面上的 **IO 裝置**類別下，選取 **ESXi 6.7**、IO 裝置類型為**網路**，並且功能為 **N-VDS 增強型資料路徑**。

2 從 My VMware 頁面下載並安裝最新版的 NIC 驅動程式。

a 移至**驅動程式和工具 > 驅動程式光碟**。

b 下載 NIC 驅動程式：

`Intel 乙太網路控制器 82599、x520、x540、x550 和 x552 系列適用的 VMware ESXi 6.7 ixgben-ens 1.1.3 NIC 驅動程式`

`Intel 乙太網路控制器 X710、XL710、XXV710 和 X722 系列適用的 VMware ESXi 6.7 i40en-ens 1.1.3 NIC 驅動程式`

3 建立上行原則。

請參閱建立上行設定檔。

4 在增強型資料路徑模式下，建立具有 N-VDS 的傳輸區域。

請參閱建立傳輸區域。

備註 為覆疊流量設定的 ENS 傳輸區域：對於執行 11.0.0 版以前的 VMware Tools 版本的 Microsoft Windows 虛擬機器，如果 vNIC 類型為 VMXNET3，請務必將 MTU 設定為 1500。對於執行 vSphere 6.7 U1 和 VMware Tools 11.0.0 及更新版本的 Microsoft Windows 虛擬機器，請務必將 MTU 設定為小於 8900 的值。對於執行其他受支援作業系統的虛擬機器，請務必將虛擬機器 MTU 設定為小於 8900 的值。

5 建立主機傳輸節點。為增強型資料路徑 N-VDS 設定邏輯核心和 NUMA 節點。

請參閱 建立獨立主機或裸機伺服器傳輸節點。

感知 NUMA 的負載平衡來源整併原則模式

當符合下列條件時，為增強型資料路徑 N-VDS 定義的負載平衡來源整併原則模式可以感知 NUMA：

- 虛擬機器上的**延遲敏感度**為**高**。
- 使用的網路介面卡類型為 VMXNET3。

如果虛擬機器或實體 NIC 的 NUMA 節點位置無法使用，負載平衡來源整併原則不會考慮 NUMA 感知來與虛擬機器和 NIC 保持一致。

在下列條件下，整併原則會在沒有 NUMA 感知的情況下運作：

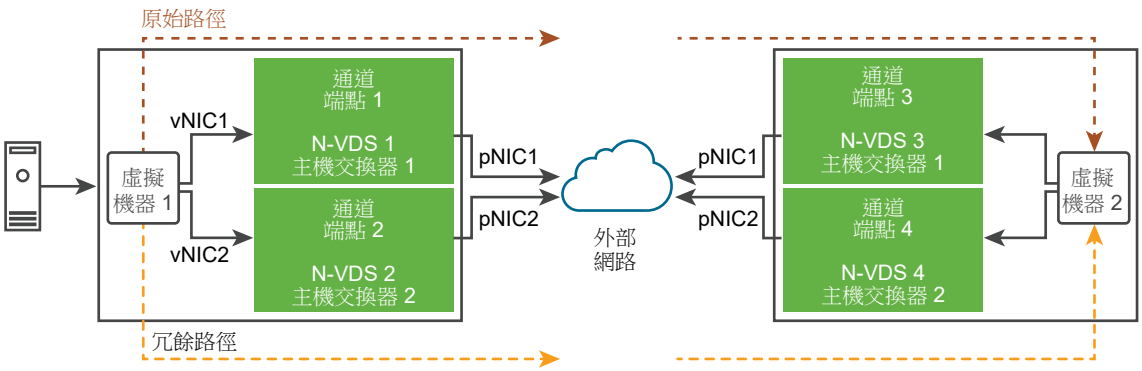
- LAG 上行設定了多個 NUMA 節點中的實體連結。
- 虛擬機器與多個 NUMA 節點具有相似性。
- ESXi 主機無法為虛擬機器或實體連結定義 NUMA 資訊。

對 SCTP 應用程式的 ENS 支援

在 SCTP 環境中，NFV 工作負載會使用多宿主和備援功能來增加應用程式上執行之流量的彈性與可靠性。多宿主是支援從來源虛擬機器到目的地虛擬機器之冗餘路徑的能力。

根據可用作覆疊網路或 VLAN 網路上行的實體 NIC 數目，虛擬機器可使用這些冗餘網路路徑將流量傳送到目標虛擬機器。將 pNIC 釘選到邏輯交換器失敗時，會使用冗餘路徑。因此，增強型資料路徑 N-VDS 會為透過 SCTP 通訊協定路由的流量提供冗餘網路路徑。

圖 8-1. SCTP 應用程式上執行的 ENS 流量



邏輯交換器上的覆疊流量

高階工作如下：

1 準備主機做為 NSX-T Data Center 傳輸節點。

2 在增強型資料路徑模式下，透過兩個 N-VDS 交換器準備 VLAN 或覆疊傳輸區域。

3 在 N-VDS 1 上，將第一個實體 NIC 釘選到交換器。

4 在 N-VDS 2 上，將第二個實體 NIC 釘選到交換器。

增強型資料路徑模式下的 N-VDS 可確保在 pNIC1 變得無法使用時，虛擬機器 1 的流量會透過冗餘路徑路由 - vNIC 1 → 通道端點 2 → pNIC 2 → 虛擬機器 2。請注意，虛擬機器 1 和虛擬機器 2 的 vNIC1 位於一個子網路上。同樣地，虛擬機器 1 和虛擬機器 2 的 vNIC2 位於另一個子網路上。

設定設定檔

設定檔可讓您一致地為多個主機或節點的網路介面卡設定相同的功能。

設定檔是您想讓網路介面卡擁有之內容或功能的容器。您不必為每個網路介面卡設定個別的內容或功能，而是可以在設定檔中指定功能，接著可以在多個主機或節點中套用。

建立上行設定檔

上行是從 NSX Edge 節點到架頂式交換器或 NSX-T Data Center 邏輯交換器的連結。連結是從 NSX Edge 節點上的實體網路介面到交換器。

上行設定檔會定義上行的原則。上行設定檔所定義的設定可以包含整併原則、作用中和待命連結、傳輸 VLAN 識別碼和 MTU 設定。

設定虛擬機器應用裝置型 NSX Edge 節點和主機傳輸節點的上行：

- 如果為上行設定檔設定了容錯移轉整併原則，則只能在整併原則中設定單一作用中上行。待命上行不受支援，且不得在容錯移轉整併原則中進行設定。當您將 NSX Edge 安裝為虛擬應用裝置或主機傳輸節點時，請使用預設上行設定檔。

- 如果為上行設定檔設定了負載平衡來源整併原則，則可以在同一 N-VDS 上設定多個作用中上行。每個上行都會與一個具有不同名稱和 IP 位址的實體 NIC 相關聯。指派給上行端點的 IP 位址可使用適用於 N-VDS 的 IP 指派來進行設定。

您必須使用**負載平衡來源**整併原則來進行流量的負載平衡處理。

必要條件

- 請參閱 NSX Edge 安裝 中的 NSX Edge 網路需求。
- 上行設定檔中的每個上行皆必須對應至 Hypervisor 主機或 NSX Edge 節點上已啟用且可供使用的實體連結。

  例如，Hypervisor 主機具有兩個已開啟的實體連結：vmnic0 和 vmnic1。假設 vmnic0 用於管理和儲存網路，而 vmnic1 並未使用。這可能表示 vmnic1 可以用作 NSX-T Data Center 上行，但 vmnic0 不能。若要進行連結整併，您必須具有兩個未使用的可用實體連結，例如 vmnic1 和 vmnic2。

  在 NSX Edge 中，通道端點和 VLAN 上行可以使用相同的實體連結。例如，vmnic0/eth0/em0 可用於管理網路，而 vmnic1/eth1/em1 可用於 fp-ethX 連結。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 設定檔 > 上行設定檔 > 新增**。

3 完成上行設定檔詳細資料。

選項	說明
名稱與說明	輸入上行設定檔名稱。 新增選用上行設定檔說明。
LAG	(選用) 在 [LAG] 區段中，針對將 Link Aggregation Control Protocol (LACP) 用於傳輸網路的鏈路聚合群組 (LAG)，按一下**新增**。 **備註** 對於 LACP，在 KVM 主機上不支援多個 LAG。 您建立的作用中和待命上行名稱可以是任何代表實體連結的文字。稍後當您建立傳輸節點時，便會參考這些上行名稱。傳輸節點 UI/API 可讓您指定每個具名上行要對應至哪個實體連結。 可能的 LAG 雜湊機制選項： ■ 來源 MAC 位址 ■ 目的地 MAC 位址 ■ 來源和目的地 MAC 位址 ■ 來源和目的地 IP 位址和 VLAN ■ 來源和目的地 MAC 位址、IP 位址和 TCP/UDP 連接埠
整併	在 [整併] 區段中，您可以輸入預設的整併原則，或者選擇輸入具名的整併原則。按一下**新增**來新增命名整併原則。整併原則會定義 N-VDS 如何使用其上行以實現備援和流量負載平衡。您可以在下列模式中設定整併原則： ■ **容錯移轉順序**：同時指定作用中上行與選擇性的待命上行清單。如果作用中上行失敗，待命清單中的下一個上行便會取代作用中上行。此選項不會執行實際的負載平衡。 ■ **負載平衡來源**：會指定作用中上行清單，且傳輸節點上的各介面已釘選到一個作用中上行。此組態可讓您同時使用多個作用中上行。 **備註** ■ 在 KVM 主機上：僅支援容錯移轉順序整併原則，而不支援負載平衡來源和負載平衡來源 MAC 整併原則。 ■ 在 NSX Edge 上：針對預設整併原則，支援負載平衡來源和容錯移轉順序整併原則。針對具名的整併原則，僅支援容錯移轉順序原則。 ■ 在 ESXi 主機上：支援負載平衡來源 MAC、負載平衡來源和容錯移轉順序整併原則。 (ESXi 主機和 NSX Edge) 您可以針對傳輸區域定義下列原則： ■ 每個以 VLAN 為基礎之邏輯交換器或區段的具名整併原則。 ■ 整個 N-VDS 的預設整併原則。 具名整併原則：使用具名整併原則時，表示對於每個以 VLAN 為基礎的邏輯交換器或區段，您可以定義特定的整併原則模式和上行名稱。此原則類型可讓您根據流量操控原則 (例如，根據頻寬需求)，彈性地選取特定的上行。 ■ 當您定義具名整併原則時，如果該原則是連結至以 VLAN 為基礎的傳輸區域，且最終由主機中特定的以 VLAN 為基礎的邏輯交換器或區段所選取，則 N-VDS 會使用此具名整併原則。 ■ 如果您未定義任何具名整併原則，N-VDS 會使用預設整併原則。

4 輸入傳輸 VLAN 值。在上行設定檔中設定的傳輸 VLAN 只會標記覆疊流量，而 TEP 端點會使用 VLAN 識別碼。

5 輸入 MTU 值。

上行設定檔 MTU 預設值為 1600。

全域實體上行 MTU 會為 NSX-T Data Center 網域中的所有 N-VDS 執行個體設定 MTU 值。如果未指定全域實體上行 MTU 值，則會從上行設定檔 MTU (如果有設定) 來推斷 MTU 值，或是使用預設值 1600。上行設定檔 MTU 值可以覆寫特定主機上的全域實體上行 MTU 值。

全域邏輯介面 MTU 會為所有的邏輯路由器介面設定 MTU 值。如果未指定全域邏輯介面 MTU 值，則會從第 0 層邏輯路由器推斷 MTU 值。邏輯路由器上行 MTU 值可以覆寫特定連接埠上的全域邏輯介面 MTU 值。

結果

除了使用者介面以外，您也可以使用 API 呼叫 `GET /api/v1/host-switch-profiles` 來檢視上行設定檔。

後續步驟

建立傳輸區域。請參閱建立傳輸區域。

設定 Network I/O Control 設定檔

使用 Network I/O Control (NIOC) 設定檔為業務關鍵應用程式配置網路頻寬，並解決數種類型的流量爭用一般資源的情況。

NIOC 設定檔引進了一種機制，會根據主機上實體介面卡的容量為系統流量保留頻寬。Network I/O Control 第 3 版改善了網路資源保留以及跨整個交換器進行配置的功能。

適用於 NSX-T Data Center 的 Network I/O Control 第 3 版可支援針對與虛擬機器和基礎結構服務 (例如 vSphere Fault Tolerance) 相關的系統流量進行資源管理。系統流量嚴格與 ESXi 主機相關聯。

系統流量的頻寬保證

Network I/O Control 第 3 版透過使用共用率、保留以及限制的建構，為虛擬機器的網路介面卡佈建頻寬。這些建構可以在 NSX-T Data Center Manager UI 中定義。許可控制中也會使用為虛擬機器流量保留頻寬的機制。當您開啟虛擬機器電源時，許可控制公用程式會確認存在足夠的頻寬，然後將虛擬機器放置在可提供資源容量的主機上。

系統流量的頻寬配置

您可以設定 Network I/O Control，為由 vSphere Fault Tolerance、vSphere vMotion、虛擬機器等所產生的流量配置一定數量的頻寬。

- 管理流量：用於主機管理的流量
- Fault Tolerance (FT) 流量：用於容錯移轉和復原的流量。
- NFS 流量：與網路檔案系統中的檔案傳輸相關的流量。
- vSAN 流量：由虛擬儲存區域網路產生的流量。
- vMotion 流量：用於計算資源移轉的流量。
- vSphere Replication 流量：用於複寫的流量。

- vSphere Data Protection 備份流量：由資料備份產生的流量。
- 虛擬機器流量：由虛擬機器產生的流量。
- iSCSI 流量：用於網際網路小型電腦系統介面的流量。

vCenter Server 會將 vSphere Distributed Switch 中的配置傳播至與該交換器連線的主機上的每個實體介面卡。

用於系統流量的頻寬配置參數

Network I/O Control 服務會透過使用數種組態參數將頻寬配置給基本 vSphere 系統功能所產生的流量。用於系統流量的配置參數。

用於系統流量的配置參數

- 共用率：共用率 (從 1 到 100) 反映了同一實體介面卡上處於作用中的某一系統流量類型與其他系統流量類型的相對優先順序。指派給系統流量類型的相對共用率和其他系統功能所傳輸的資料量決定該系統流量類型的可用頻寬。
- 保留：單一實體介面卡上所必須保證的最小頻寬 (以 Mbps 為單位)。所有系統流量類型所保留的總頻寬不得超過容量最低的實體網路介面卡能夠提供之頻寬的 75%。未使用的保留頻寬會供其他類型的系統流量使用。但是，Network I/O Control 不會將系統流量不使用的容量重新散佈到虛擬機器放置位置。
- 限制：某一系統流量類型在單一實體介面卡上所能耗用的最大頻寬 (以 Mbps 或 Gbps 為單位)。

備註 您可以保留的實體網路介面卡頻寬不能超過 75%。

例如，如果連線到 ESXi 主機的網路介面卡為 10 GbE，則您只能將 7.5 Gbps 頻寬配置給多種流量類型。您可以餘下更多未保留的容量。主機可以根據共用率、限制和使用情況來動態地配置未保留的頻寬。主機僅保留足以供系統功能運作的頻寬。

針對 N-VDS 上的系統流量設定 Network I/O Control 和頻寬配置

若要保證 NSX-T Data Center 主機上執行之系統流量的最低頻寬，請在 N-VDS 上啟用並設定網路資源管理。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 設定檔 > NIOC 設定檔 > 新增**。

3 輸入 NIOC 設定檔詳細資料。

選項	說明
名稱與說明	輸入 NIOC 設定檔名稱。 您可以選擇性地輸入設定檔的詳細資料，例如啟用的流量類型。
狀態	切換以啟用流量資源中所列出的頻寬配置。
主機基礎結構流量資源	您可以接受預設列出的流量資源。 按一下**新增**，然後輸入您的流量資源，以自訂 NIOC 設定檔。 (選用) 選取現有的流量類型，然後按一下**刪除**，以將資源從 NIOC 設定檔中移除。

新的 NIOC 設定檔即會新增到 NIOC 設定檔清單中。

使用 API 針對 N-VDS 上的系統流量設定 Network I/O Control 和頻寬配置

您可以使用 NSX-T Data Center API 設定主機上所執行應用程式的網路與頻寬。

程序

1 查詢主機以顯示系統定義的主機交換器設定檔和使用者定義的主機交換器設定檔。

2 `GET https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true`。

該範例回應顯示套用到主機的 NIOC 設定檔。

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
  "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
  "type-identifier": "NiocProfile"
  },
  "properties": {
  "_create_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of resource creation",
  "readonly": true
    },
  "_create_user": {
  "description": "ID of the user who created this resource",
  "readonly": true,
  "type": "string"
    },
  "_last_modified_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of last modification",
  "readonly": true
    },
```

```
  "_last_modified_user": {
  "description": "ID of the user who last modified this resource",
  "readonly": true,
  "type": "string"
    },

  "_links": {
  "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
  "items": {
  "$ref": "ResourceLink"+
    },

  "readonly": true,
  "title": "References related to this resource",
  "type": "array"
    },
  "_protection": {
  "description": "Protection status is one of the following:
     PROTECTED - the client who retrieved the entity is not allowed to modify it.
     NOT_PROTECTED - the client who retrieved the entity is allowed to modify it
     REQUIRE_OVERRIDE - the client who retrieved the entity is a super user and can modify it,
     but only when providing the request header X-Allow-Overwrite=true.
     UNKNOWN - the _protection field could not be determined for this entity.",
  "readonly": true,
  "title": "Indicates protection status of this resource",
  "type": "string"
    },

  "_revision": {
  "description": "The _revision property describes the current revision of the resource.
    To prevent clients from overwriting each other's changes, PUT operations must include the
             current _revision of the resource,
    which clients should obtain by issuing a GET operation.
                If the _revision provided in a PUT request is missing or stale, the operation
will be rejected.",
  "readonly": true,
  "title": "Generation of this resource config",
  "type": "int"
    },

  "_schema": {
  "readonly": true,
  "title": "Schema for this resource",
  "type": "string"
    },

  "_self": {
  "$ref": "SelfResourceLink"+,
  "readonly": true,
  "title": "Link to this resource"
    },

  "_system_owned": {
  "description": "Indicates system owned resource",
```

```
  "readonly": true,
  "type": "boolean"
    },

  "description": {
  "can_sort": true,
  "maxLength": 1024,
  "title": "Description of this resource",
  "type": "string"
    },

  "display_name": {
  "can_sort": true,
  "description": "Defaults to ID if not set",
  "maxLength": 255,
  "title": "Identifier to use when displaying entity in logs or GUI",
  "type": "string"
    },

  "enabled": {
  "default": true,
  "description": "The enabled property specifies the status of NIOC feature.

  When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
     specified for the traffic resources are enforced.
  When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
guaranteed.

  By default, enabled will be set to true.",

  "nsx_feature": "Nioc",
  "required": false,
  "title": "Enabled status of NIOC feature",
  "type": "boolean"
    },

  "host_infra_traffic_res": {
  "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
  "items": {
  "$ref": "ResourceAllocation"+
    },
  "nsx_feature": "Nioc",
  "required": false,
  "title": "Resource allocation associated with NiocProfile",
  "type": "array"
    },

  "id": {
  "can_sort": true,
  "readonly": true,
  "title": "Unique identifier of this resource",
  "type": "string"
    },
```

```
  "required_capabilities": {
  "help_summary":
                            "List of capabilities required on the fabric node if this profile is
used.
          The required capabilities is determined by whether specific features are enabled in the
profile.",
  "items": {
  "type": "string"
    },
  "readonly": true,
  "required": false,
  "type": "array"
    },

  "resource_type": {
  "$ref": "HostSwitchProfileType"+,
  "required": true
    },

  "tags": {
  "items": {
  "$ref": "Tag"+
      },

  "maxItems": 30,
  "title": "Opaque identifiers meaningful to the API user",
  "type": "array"
    }
  },
  "title": "Profile for Nioc",
  "type": "object"
  }
```

3 如果不存在 NIOC 設定檔，請建立 NIOC 設定檔。

```
POST https://<nsx-mgr>/api/v1/host-switch-profiles
```

```
{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
   Values for limit and reservation are expressed in percentage. And for shares,
   the value is expressed as a number between 1-100.\nThe overall reservation among all traffic
types should not exceed 75%.
   Otherwise, the API request will be rejected.",

  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be rejected by
the API.",
```

```
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },

    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",
      "type": "number"
    },

    "shares": {
      "default": 50,
      "maximum": 100,
      "minimum": 1,
      "required": true,
      "title": "Shares",
      "type": "int"
    },

    "traffic_type": {
      "$ref": "HostInfraTrafficType"+,
      "required": true,
      "title": "Resource allocation traffic type"
    }

  },

  "title": "Resource allocation information for a host infrastructure traffic type",
  "type": "object"
```

4 使用新建立的 NIOC 設定檔的 NIOC 設定檔識別碼更新傳輸節點組態。

```
PUT https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>
```

```
{
    "resource_type": "TransportNode",
    "description": "Updated NSX configured Test Transport Node",
    "id": "77816de2-39c3-436c-b891-54d31f580961",
    "display_name": "NSX Configured TN",
    "host_switch_spec": {
      "resource_type": "StandardHostSwitchSpec",
      "host_switches": [
        {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
        {
```

```
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
         }
        {
         "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
         "key": "NiocProfile"
        }
         ],
        "host_switch_name": "nsxvswitch",
        "pnics": [
       {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
       }
       ],
       "ip_assignment_spec": {
       "resource_type": "StaticIpPoolSpec",
       "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
       }
        }
       ]
     },
      "transport_zone_endpoints": [
       {
       "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
       "transport_zone_profile_ids": [
         {
           "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
           "resource_type": "BfdHealthMonitoringProfile"
         }
       ]
       }
     ],

      "host_switches": [
       {
         "host_switch_profile_ids": [
           {
           "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
           "key": "UplinkHostSwitchProfile"
          },
           {
           "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
           "key": "LldpHostSwitchProfile"
           }
         ],

         "host_switch_name": "nsxvswitch",
         "pnics": [
         {
           "device_name": "vmnic1",
           "uplink_name": "uplink1"
           }
         ],
         "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
```

```
      }
    ],
    "node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
    "_revision": 0
  }
```

5 確認 com.vmware.common.respools.cfg 檔案中的 NIOC 設定檔參數已更新。

[root@ host:] net-dvs -l

```
          switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
   max ports: 2560
   global properties:

   com.vmware.common.opaqueDvs = true ,     propType = CONFIG
   com.vmware.nsx.kcp.enable = true ,     propType = CONFIG
   com.vmware.common.alias = nsxvswitch ,     propType = CONFIG
   com.vmware.common.uplinkPorts: uplink1   propType = CONFIG
   com.vmware.common.portset.mtu = 1600, propType = CONFIG
   com.vmware.etherswitch.cdp = LLDP, listen  propType = CONFIG
   com.vmware.common.respools.version = version3,   propType = CONFIG
   com.vmware.common.respools.cfg:
   netsched.pools.persist.ft:0:50:-1:255
   netsched.pools.persist.hbr:0:50:-1:255
   netsched.pools.persist.vmotion:0:50:-1:255
   netsched.pools.persist.vm:0:100:-1:255
   netsched.pools.persist.iscsi:0:50:-1:255
   netsched.pools.persist.nfs:0:50:-1:255
   netsched.pools.persist.mgmt:0:50:-1:255
   netsched.pools.persist.vdp:0:50:-1:255
   netsched.pools.persist.vsan:0:50:-1:255
   propType = CONFIG
```

6 驗證主機核心中的 NIOC 設定檔。

[root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo

```
Vnic NIOC Info
                    {
      Uplink reserved on:vmnic4
      Reservation in Mbps:200
      Shares:50
      Limit in Mbps:4294967295
      World ID:1001400726
      vNIC Index:0
      Respool Tag:0
      NIOC Version:3
      Active Uplink Bit Map:15
      Parent Respool ID:netsched.pools.persist.vm
     }
```

7 確認 NIOC 設定檔資訊。

[root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo

```
Uplink NIOC Info
            {
    Uplink device:vmnic4
    Link Capacity in Mbps:750
    vm respool reservation:275
    link status:1
    NetSched Ready:1
    Infrastructure reservation:0
    Total VM reservation:200
    Total vnics on this uplink:1
    NIOC Version:3
    Uplink index in BitMap:0
   }
```

結果

NIOC 設定檔已設定 NSX-T Data Center 主機上所執行應用程式的預先定義頻寬配置。

新增 NSX Edge 叢集設定檔

NSX Edge 叢集設定檔定義 NSX Edge 傳輸節點的原則。

必要條件

確認 NSX Edge 叢集可用。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 設定檔 > Edge 叢集設定檔 > 新增**。

3 輸入 NSX Edge 叢集設定檔詳細資料。

選項	說明
名稱與說明	輸入 NSX Edge 叢集設定檔名稱。 您可以選擇性地輸入設定檔詳細資料，例如，雙向轉送偵測 (BFD) 設定。
BFD 探查時間間隔	接受預設設定。 BFD 是偵測通訊協定，可用於識別轉送路徑故障。您可以設定 BFD 用於偵測轉送路徑故障的時間間隔。
BFD 允許的躍點	接受預設設定。 您可以為設定檔設定允許的多重躍點 BFD 工作階段數目。
BFD 宣告無作用倍數	接受預設設定。 您可以設定在將工作階段標記為關閉之前不會接收 BFD 封包的次數。
待命重新放置臨界值	接受預設設定。

新增 NSX Edge 橋接器設定檔

NSX Edge 橋接器設定檔定義 ESXi 橋接器叢集的原則。

橋接器叢集是 ESXi 主機傳輸節點的集合。

必要條件

- 確認 NSX Edge 叢集可用。
- 確認 ESXi 橋接器叢集可用。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 設定檔 > Edge 橋接器設定檔 > 新增**。

3 輸入 NSX Edge 叢集設定檔詳細資料。

選項	說明
名稱與說明	輸入 NSX Edge 橋接器叢集設定檔名稱。 您可以選擇性地輸入設定檔詳細資料，例如，主要和備份節點詳細資料。
Edge 叢集	選取您可以使用的 NSX Edge 叢集。
主要節點	從叢集指定慣用 NSX Edge 節點。
備份節點	如果主要節點失敗，請指定備份 NSX Edge 節點。
容錯移轉模式	選取**先佔式**或**非先佔式**模式。 預設 HA 模式是先佔式，這會在慣用 NSX Edge 節點重新上線時降低流量。非先佔式模式不會造成任何流量下降。

新增傳輸節點設定檔

傳輸節點設定檔會擷取建立傳輸節點所需的組態。傳輸節點設定檔可套用至現有 vCenter Server 叢集，以為成員主機建立傳輸節點。傳輸節點設定檔定義傳輸區域、成員主機、N-VDS 交換器組態 (包括上行設定檔、IP 指派、實體 NIC 至上行虛擬介面的對應等)。

傳輸節點設定檔套用到 vCenter Server 叢集時，會開始建立傳輸節點。NSX Manager 準備叢集中的主機並在所有主機上安裝 NSX-T Data Center 元件。會根據傳輸節點設定檔中指定的組態，為主機建立傳輸節點。

若要刪除傳輸節點設定檔，您必須先從相關聯的叢集中斷連結此設定檔。不會影響現有的傳輸節點。已新增至叢集的新主機將不會再自動轉換為傳輸節點。

傳輸節點設定檔建立的考量事項：

- 您最多可以為每個組態新增四個 N-VDS 交換器：為 VLAN 傳輸區域建立的增強型 N-VDS、為覆疊傳輸區域建立的標準 N-VDS、為覆疊傳輸區域建立的增強型 N-VDS。
- 為 VLAN 傳輸區域建立的標準 N-VDS 交換器數目則沒有限制。

- 在同一主機上執行多個標準覆疊 N-VDS 交換器和 Edge 虛擬機器的單一主機叢集拓撲中，NSX-T Data Center 會提供流量隔離，使經過第一個 N-VDS 的流量與經過第二個 N-VDS 的流量相隔離，依此類推。每個 N-VDS 上的實體 NIC 必須對應至主機上的 Edge 虛擬機器，以允許與外部環境的南北向流量連線。在第一個傳輸區域上移出虛擬機器的封包必須通過外部路由器或外部虛擬機器路由至第二個傳輸區域上的虛擬機器。
- 每個 N-VDS 交換器名稱必須是唯一的。NSX-T Data Center 不允許使用重複的交換器名稱。
- 每個傳輸區域識別碼必須是唯一的。NSX-T Data Center 不允許使用重複的識別碼。
- 您可以在傳輸節點設定檔中最多新增 1000 個傳輸區域。
- 若要新增傳輸區域，它必須由傳輸節點設定檔中存在的任何 N-VDS 實現。

必要條件

- 確認主機均屬於 vCenter Server 叢集。

  vCenter Server 必須至少具有一個叢集。
- 確認已設定傳輸區域。請參閱建立傳輸區域。
- 確認叢集可用。請參閱從使用者介面部署 NSX Manager 節點以形成叢集。
- 確認已設定 IP 集區，或 DHCP 必須可用於網路部署。請參閱為通道端點 IP 位址建立 IP 集區。
- 確認已設定計算管理程式。請參閱新增計算管理程式。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 設定檔 > 傳輸節點設定檔 > 新增**。
3. 輸入可識別傳輸節點設定檔的名稱。

   您可以選擇性地新增傳輸節點設定檔的相關說明。
4. 選取可用的傳輸區域，然後按一下 **>** 按鈕，以在傳輸節點設定檔中包含傳輸區域。

   備註 您可以新增多個傳輸區域。
5. 按一下 **N-VDS** 索引標籤，然後輸入交換器詳細資料。

選項	說明
N-VDS 名稱	如果傳輸節點已連結至傳輸區域，請確保為 N-VDS 輸入的名稱與傳輸區域中指定的 N-VDS 名稱相同。可以建立傳輸節點，而不將其連結至傳輸區域。
相關聯的傳輸區域	顯示相關聯的主機交換器實現的傳輸區域。如果傳輸區域未由傳輸節點設定檔中的任何 N-VDS 實現，則無法新增它。
NIOC 設定檔	從下拉式功能表選取 NIOC 設定檔。 會強制執行流量資源設定檔中指定的頻寬配置。

選項	說明
上行設定檔	從下拉式功能表中選取現有的上行設定檔，或建立自訂上行設定檔。 **備註** 叢集中的主機必須具有相同的上行設定檔。 您也可以使用預設上行設定檔。
LLDP 設定檔	依預設，NSX-T 只會接收來自 LLDP 芳鄰的 LLDP 封包。 但是，NSX-T 可以設定為可將 LLDP 封包傳送至 LLDP 芳鄰，以及接收來自 LLDP 芳鄰的 LLDP 封包。
IP 指派	選取**使用 DHCP**、**使用 IP 集區**或**使用靜態 IP 清單**，以將 IP 位址指派給傳輸節點的虛擬通道端點 (VTEP)。 如果您選取**使用靜態 IP 清單**，您必須指定由 IP 位址、閘道和子網路遮罩構成、並以逗號分隔的清單。傳輸節點的所有 VTEP 都必須位於同一子網路，否則，不會建立雙向流量 (BFD) 工作階段。
IP 集區	如果您已針對 IP 指派選取**使用 IP 集區**，請指定 IP 集區名稱。
實體 NIC	將實體 NIC 新增至傳輸節點。您可以使用預設上行或從下拉式功能表中指派現有的上行。 按一下**新增 PNIC**，為傳輸節點設定其他實體 NIC。 **備註** 您在此欄位中新增的實體 NIC 的移轉取決於您如何設定**僅限 PNIC 的移轉**、**用於安裝的網路對應**和**用於解除安裝的網路對應**。 ■ 若要移轉無相關聯 VMkernel 對應的已用實體 NIC (例如，由標準 vSwitch 或 vSphere 分散式交換器使用)，請確保已啟用**僅限 PNIC 的移轉**。否則，傳輸節點狀態仍為**部分成功**，且網狀架構節點 LCP 連線將無法建立。 ■ 若要移轉具有相關聯 VMkernel 網路對應的已用實體 NIC，請停用**僅限 PNIC 的移轉**，並設定 VMkernel 網路對應。 ■ 若要移轉可用的實體 NIC，請啟用**僅限 PNIC 的移轉**。
僅限 PNIC 的移轉	設定此欄位之前，請考量以下幾點： ■ 瞭解定義的實體 NIC 是已用 NIC 還是可用 NIC。 ■ 決定是否需要將主機的 VMkernel 介面與實體 NIC 一起移轉。 設定欄位： ■ 如果您只想將實體 NIC 從 VSS 或 DVS 交換器移轉至 N-VDS 交換器，請啟用**僅限 PNIC 的移轉**。 ■ 如果您想要移轉已用實體 NIC 及其相關聯的 VMkernel 介面對應，請停用**僅限 PNIC 的移轉**。指定 VMkernel 介面移轉對應後，可用的實體 NIC 會連結至 N-VDS 交換器。 在具有多個主機交換器的主機上： ■ 如果所有主機交換器將僅移轉 PNIC，您可以在單一作業中移轉 PNIC。 ■ 如果部分主機交換器將移轉 VMkernel 介面，且剩餘主機交換器將僅移轉 PNIC： 1 在第一個作業中，僅移轉 PNIC。 2 在第二個作業中，移轉 VMkernel 介面。確保**僅限 PNIC 的移轉**已停用。 在多個主機之間不同時支援僅限 PNIC 的移轉和 VMkernel 介面移轉。 **備註** 若要移轉管理網路 NIC，請設定其相關聯的 VMkernel 網路對應，並保持**僅限 PNIC 的移轉**的停用狀態。如果您僅移轉管理 NIC，則主機會中斷連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。

選項	說明
用於安裝的網路對應	若要在安裝期間將 VMkernel 移轉至 N-VDS 交換器，請將 VMkernel 對應到現有的邏輯交換器。NSX Manager 將 VMkernel 移轉至 N-VDS 上對應的邏輯交換器。 注意 確保將管理 NIC 和管理 VMkernel 介面移轉至一個邏輯交換器，其連線至移轉之前管理 NIC 連線到的同一 VLAN。如果將 vmnic<*n*> 和 VMkernel<*n*> 移轉到不同的 VLAN，就會與主機中斷連線。 注意 對於固定的實體 NIC，請確保實體 NIC 至 VMkernel 介面的主機交換器對應符合傳輸節點設定檔中指定的組態。做為驗證程序的一部分，NSX-T Data Center 會確認對應，以及 VMkernel 介面至 N-VDS 交換器的驗證通過移轉是否成功。設定用於解除安裝的網路對應也是強制性的，因為將 VMkernel 介面移轉到 N-VDS 交換器之後，NSX-T Data Center 不會儲存主機交換器的對應組態。如果未設定對應，可能會在移轉回 VSS 或 VDS 交換器後中斷與服務 (例如 vSAN) 的連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。
用於解除安裝的網路對應	若要在解除安裝期間還原 VMkernel 的移轉，請將 VMkernel 對應到 VSS 或 DVS 上的連接埠群組，以便 NSX Manager 知道必須將 VMkernel 移轉回 VSS 或 DVS 上的哪個連接埠群組。對於 DVS 交換器，請確保連接埠群組的類型為暫時。 注意 對於固定的實體 NIC，請確保實體 NIC 至 VMkernel 介面的傳輸節點設定檔對應符合主機交換器中指定的組態。設定用於解除安裝的網路對應是強制性的，因為將 VMkernel 介面移轉到 N-VDS 交換器之後，NSX-T Data Center 不會儲存主機交換器的對應組態。如果未設定對應，可能會在移轉回 VSS 或 VDS 交換器後中斷與服務 (例如 vSAN) 的連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。

6 若要新增其他 N-VDS 交換器，請按一下 **+ 新增 N-VDS**。

7 按一下**儲存**以完成設定。

後續步驟

將傳輸節點設定檔套用至現有 vSphere 叢集。請參閱設定受管理的主機傳輸節點。

VMkernel 移轉至 N-VDS 交換器

若要將 VMkernel 介面從 VSS 或 DVS 交換器移轉到叢集層級的 N-VDS 交換器，請針對傳輸節點設定檔設定移轉所需的網路對應詳細資料 (將 VMkernel 介面對應至邏輯交換器)。同樣地，若要移轉主機節點上的 VMkernel 介面，請設定傳輸節點組態。若要還原將 VMkernel 介面移轉回 VSS 或 DVS 交換器，請設定要在解除安裝期間實現的傳輸節點設定檔中的解除安裝網路對應 (將邏輯連接埠對應至 VMkernel 介面)。

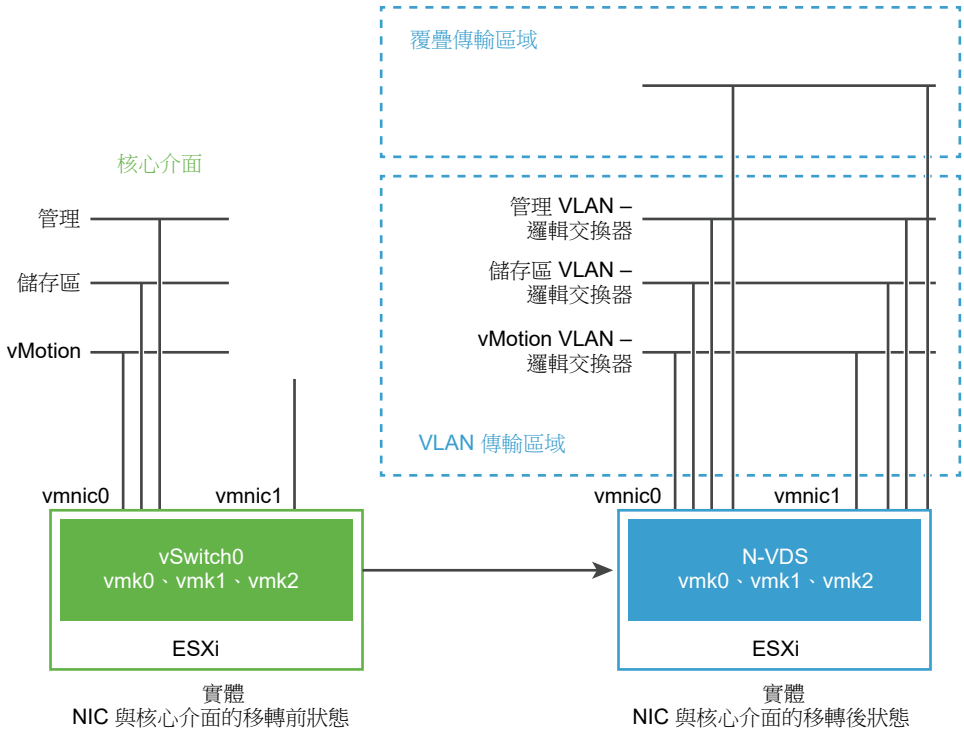
在移轉期間，目前正在使用中的實體 NIC 會移轉至 N-VDS 交換器，而移轉後，可用或免費的實體 NIC 會連結到 N-VDS 交換器。

備註 傳輸節點設定檔已套用到叢集中的所有成員主機。但是，如果您想要限制特定主機上的 VMkernel 介面移轉，您可以直接設定該主機。移轉後，N-VDS 會針對連結至 N-VDS 交換器的這些介面處理 VLAN 和覆疊網路上的流量。

重要 對個別主機進行的設定標有已覆寫旗標。對傳輸節點設定檔的任何進一步更新不會套用到這些覆寫的主機。這些主機會保持已覆寫狀態，直到 NSX-T Data Center 解除安裝為止。

在下圖中，如果主機只有兩個實體 NIC，您可能想要將這兩個 NIC 指派給 N-VDS 以實現備援並指派其相關聯的 VMkernel 介面，以便介面不會中斷與主機的連線。

圖 8-2. 將網路介面移轉到 N-VDS 前後



移轉之前， ESXi 主機具有衍生自兩個實體連接埠的兩個上行 - vmnic0 和 vmnic1。在此，vmnic0 設定為處於作用中狀態 (連結至 VSS)，而 vmnic1 並未使用。此外，還有三個 VMkernel 介面：vmk0、vmk1 和 vmk2。

您可以使用 NSX-T Data Center Manager 使用者介面或 NSX-T Data Center API 移轉 VMkernel 介面。請參閱《NSX-T Data Center API 指南》。

移轉之後，vmnic0、vmnic1 及其 VMkernel 介面將移轉至 N-VDS 交換器。vmnic0 和 vmnic1 均透過 VLAN 和覆疊傳輸區域進行連線。

VMkernel 移轉的考量事項

- PNIC 和 VMkernel 移轉：將釘選的實體 NIC 和相關聯的 VMkernel 介面移轉到 N-VDS 交換器之前，請記下主機交換器上的網路對應 (實體 NIC 與連接埠群組的對應)。
- 僅 PNIC 移轉：如果您計劃僅移轉 PNIC，請確保不會移轉連線到管理 VMkernel 介面的管理實體 NIC。這會導致與主機的連線中斷。如需詳細資料，請參閱新增傳輸節點設定檔中的**僅限 PNIC 的移轉**欄位。
- 還原移轉：計劃針對釘選的實體 NIC 還原將 VMkernel 介面移轉回 VSS 或 DVS 主機交換器之前，請確保您記下主機交換器上的網路對應 (實體 NIC 與連接埠群組的對應)。必須在**用於解除安裝的網路對應**欄位中為傳輸節點設定檔設定主機交換器對應。如果沒有此對應，NSX-T Data Center 不會知道必須將 VMkernel 介面移轉回哪些連接埠群組。這種情況可能會導致 vSAN 網路連線中斷。

- 移轉前登錄 vCenter Server：如果您計劃移轉連線至 DVS 交換器的 VMkernel 或 PNIC，請確保 vCenter Server 已向 NSX Manager 登錄。
- 符合 VLAN 識別碼：移轉後，管理 NIC 和管理 VMkernel 介面必須位於移轉前管理 NIC 連線的相同 VLAN 上。如果 vmnic0 和 vmk0 已連線到管理網路並移轉到不同的 VLAN，則與主機的連線會中斷。
- 移轉至 VSS 交換器：無法將兩個 VMkernel 介面移轉回 VSS 交換器的相同連接埠群組。
- vMotion：在移轉 VMkernel 和/或 PNIC 之前，先執行 vMotion 以將虛擬機器工作負載移動到另一台主機。移轉失敗時，工作負載虛擬機器便不會受到影響。
- vSAN：如果主機上正在執行 vSAN 流量，請透過 vCenter Server 將主機置於維護模式，並在移轉 VMkernel 和/或 PNIC 之前使用 vMotion 功能將虛擬機器從主機中移出。
- 移轉：如果 VMkernel 已連線到目標交換器，您仍可選取要將該 VMkernel 移轉至同一個交換器。此屬性會讓 VMK 和/或 PNIC 移轉作業變為等冪。如果您想要僅將 PNIC 移轉至目標交換器，這個做法很有用。由於移轉作業一律需要至少一個 VMkernel 和一個 PNIC，因此您可以在僅將 PNIC 移轉至目標交換器時選取已移轉至目標交換器的 VMkernel。如果不需要移轉任何 VMkernel，請透過 vCenter Server 在來源交換器或目標交換器中建立暫存 VMkernel。然後，將其與 PNIC 一起移轉，並在移轉完成後透過 vCenter Server 刪除暫存 VMkernel。
- MAC 共用：如果 VMkernel 介面和 PNIC 共用同一個 MAC，且兩者位於相同的交換器上，如果兩者皆會在移轉後用到，則必須將兩者一起移轉到同一個目標交換器。請一律讓 vmk0 和 vmnic0 位於同一個交換器中。

  執行下列命令，以檢查主機中所有 VMK 和 PNIC 使用的 MAC：

  ```
  esxcfg-vmknic -l
  ```

  ```
  esxcfg-nics -l
  ```
- 移轉後建立的 VIF 邏輯連接埠：從 VSS 或 DVS 交換器將 VMkernel 移轉至 N-VDS 交換器之後，會在 NSX Manager 上建立類型 VIF 的邏輯交換器連接埠。您不得在這些 VIF 邏輯交換器連接埠上建立 Distributed Firewall 規則。

將 Vmkernel 介面移轉至 N-VDS 交換器

將 VMkernel 介面移轉至 N-VDS 交換器的高階工作流程：

1 視需要建立邏輯交換器。

2 將 VMkernel 介面和 PNIC 移轉到 N-VDS 交換器的主機上的虛擬機器關閉電源。

3 設定傳輸節點設定檔的網路對應，該網路對應將用於在傳輸節點建立期間移轉 VMkernel 介面。網路對應表示將 VMkernel 介面對應至邏輯交換器。

  如需更多詳細資料，請參閱新增傳輸節點設定檔。

4 確認 vCenter Server 中的網路介面卡對應反映 VMkernel 交換器與 N-VDS 交換器的新關聯。若為釘選的實體 NIC，請確認 NSX-T Data Center 中的對應反映釘選到 vCenter Server 中的實體 NIC 的任何 VMkernel。

5 在 NSX Manager 中，移至**進階網路與安全性 > 網路 > 交換**。在**交換器**頁面中，確認 VMkernel 介面已透過新建立的邏輯連接埠連結至邏輯交換器。

6 移至**系統 > 節點 > 主機傳輸節點**。對於每個傳輸節點，確認**節點狀態**資料行中的狀態為 [成功]，以確認傳輸節點組態已成功驗證。

7 在**主機傳輸節點**頁面中，確認**組態狀態**中的狀態為 [成功]，確認已使用指定的組態成功實現主機。

在使用 NSX-T UI 或傳輸節點 API 將 VMkernel 介面和 PNIC 從 VDS 移轉至 N-VDS 交換器後，vCenter Server 會針對 VDS 顯示警告。如果主機需要連線到 VDS，請從 VDS 中移除該主機。vCenter Server 便不會再針對 VDS 顯示任何警告。

如需有關移轉期間可能會遇到的錯誤的詳細資料，請參閱 VMkernel 移轉錯誤。

還原將 VMkernel 介面移轉至 VSS 或 DVS 交換器

在 NSX-T Data Center 解除安裝期間，還原將 VMkernel 介面從 N-VDS 交換器移轉至 VSS 或 DVS 交換器的高階工作流程：

1 在 ESXi 主機上，在移轉後將連線到主控 VMkernel 介面之邏輯連接埠的虛擬機器關閉電源。

2 設定傳輸節點設定檔的網路對應，該網路對應將用於在解除安裝期間移轉 VMkernel 介面。在解除安裝期間，網路對應會將 VMkernel 介面對應至 ESXi 主機上 VSS 或 DVS 交換器中的連接埠群組。

   備註 透過還原將 VMkernel 移轉至 DVS 交換器上的連接埠群組，可確保連接埠群組類型設定為暫時。

   如需更多詳細資料，請參閱新增傳輸節點設定檔。

3 確認 vCenter Server 中的網路介面卡對應反映 VMkernel 交換器與 VSS 或 DVS 交換器的連接埠群組的新關聯。

4 在 NSX Manager 中，移至**進階網路與安全性 > 網路 > 交換**。在**交換器**頁面中，確認已刪除含有 VMkernel 介面的邏輯交換器。

如需有關移轉期間可能會遇到的錯誤的詳細資料，請參閱 VMkernel 移轉錯誤。

更新主機交換器對應

重要

- 可設定狀態的主機：支援新增和更新作業。若要更新現有對應，您可以將新的 VMkernel 介面項目新增至網路對應組態。如果更新已移轉到 N-VDS 交換器的 VMkernel 介面的網路對應組態，則不會在主機上實現更新的網路對應。
- 無狀態主機：支援新增、更新和移除作業。主機重新開機後，會實現對網路對應組態進行的任何變更。

  若要將 VMkernel 介面更新為新邏輯交換器，您可以編輯傳輸節點設定檔，以便在叢集層級套用網路對應。如果您只想將更新套用到單一主機，則使用主機層級 API 設定傳輸節點。

備註 為個別主機更新傳輸節點組態後，透過傳輸節點設定檔套用的任何新更新都不會套用到該主機。該主機狀態會變為已覆寫。

1 若要更新叢集中的所有主機，請編輯**安裝期間的網路對應**欄位，以更新 VMkernel 與邏輯交換器的對應。

如需更多詳細資料，請參閱新增傳輸節點設定檔。

2 儲存變更。對傳輸節點設定檔所做的變更會自動套用到叢集的所有成員主機 (標有已覆寫狀態的主機除外)。

3 同樣地，若要更新個別主機，請編輯傳輸節點組態中的 VMkernel 對應。

備註 如果您以新的 VMkernel 對應更新**安裝期間的網路對應**欄位，則必須在**解除安裝期間的網路對應**欄位中新增相同的 VMkernel 介面。

如需有關移轉期間可能會遇到的錯誤的詳細資料，請參閱 VMkernel 移轉錯誤。

在無狀態的叢集上移轉 VMkernel 介面

1 使用傳輸節點 API 準備主機並將其設定為參考主機。

2 從參考主機擷取主機設定檔。

3 在 vCenter Server 中，將主機設定檔套用至無狀態的叢集。

4 在 NSX-T Data Center 中，將傳輸節點設定檔套用至無狀態的叢集。

5 將叢集的每個主機重新開機。

叢集主機可能需要幾分鐘時間才能實現更新的狀態。

移轉失敗案例

- 如果移轉因某些原因而失敗，主機會嘗試移轉實體 NIC 和 VMkernel 介面三次。
- 如果移轉仍繼續失敗，主機會保留 VMkernel 與管理實體 NIC (vmnic0) 的連線以執行復原為之前的組態。
- 如果復原也失敗，導致設定為管理實體 NIC 的 VMkernel 遺失，您必須重設主機。

不支援的移轉案例

不支援下列案例：

- 同時移轉來自兩個不同的 VSS 或 DVS 交換器的 VMkernel 介面。
- 在可設定狀態的主機上，網路對應已更新為將 VMkernel 介面對應至另一個邏輯交換器。例如，移轉之前，VMkernel 對應到邏輯交換器 1，而 VMkernel 介面對應到邏輯交換器 2。

VMkernel 移轉錯誤

將 VMkernel 介面和實體 NIC 從 VSS 或 DVS 交換器移轉至 N-VDS 交換器，或將移轉介面還原至 VSS 或 DVS 主機交換器時會發生錯誤。

表 8-1. VMkernel 移轉錯誤

錯誤碼	問題	原因	解決方案
8224	找不到傳輸節點組態指定的主機交換器。	找不到主機交換器識別碼。	■ 確保使用主機交換器名稱建立傳輸區域，然後建立傳輸節點。 ■ 確保在傳輸節點組態中使用有效的主機交換器。
8225	VMkernel 移轉正在進行中。	移轉正在進行中。	等待移轉完成，然後再執行另一個動作。
8226	只有 ESXi 主機支援 VMkernel 移轉。	移轉僅適用於 ESXi 主機。	確保主機為 ESXi 主機，然後再起始移轉。
8227	VMkernel 介面未附加主機交換器名稱。	在具有多個主機交換器的主機上，NSX-T Data Center 無法識別每個 VMkernel 介面與其主機交換器的關聯。	如果主機具有多個 N-VDS 主機交換器，請確保 VMkernel 介面已附加主機所連線之 N-VDS 的主機交換器名稱。 例如，用於解除安裝具有 N-VDS 主機交換器名稱 nsxvswitch1 和 VMkernel1 以及另一個 N-VDS 主機交換器名稱 nsxvswitch2 和 VMkernel2 之主機的網路對應必須定義如下：`device_name: VMkernel1@nsxvswitch1`、`destination_network: DPortGroup`。
8228	在主機上找不到 `device_name` 欄位中使用的主機交換器。	主機交換器名稱不正確。	請輸入正確的主機交換器名稱。
8229	傳輸節點未指定邏輯交換器的傳輸區域。	未新增傳輸區域。	將傳輸區域新增至傳輸節點組態。
8230	主機交換器上沒有任何實體 NIC。	主機交換器上必須至少有一個實體 NIC。	為上行設定檔指定至少一個實體 NIC，並為邏輯交換器指定 VMkernel 網路對應組態。
8231	主機交換器名稱不相符。	如果 `vmk1@host_switch` 中使用的主機交換器名稱與介面的目的地邏輯交換器使用的主機交換器名稱不相符。	確保網路對應組態中指定的主機交換器名稱與介面的邏輯交換器使用的名稱相符。
8232	主機上未實現邏輯交換器。	在主機上實現邏輯交換器失敗。	將主機與 NSX Manager 同步。
8233	網路介面對應中出現未預期的邏輯交換器。	用於安裝和解除安裝的網路介面對應同時列出了邏輯交換器和連接埠群組。	用於安裝的網路對應必須僅包含邏輯交換器做為目的地目標。同樣地，用於解除安裝的網路對應必須僅包含連接埠群組做為目的地目標。
8294	網路介面對應中不存在邏輯交換器。	未指定邏輯交換器。	確保在網路介面對應組態中指定邏輯交換器。
8296	主機交換器不相符。	用於解除安裝的網路介面對應設定了不正確的主機交換器名稱。	確保對應組態中使用的主機交換器名稱與 VMkernel 介面所在的主機交換器中輸入的名稱相符。
8297	VMkernel 重複。	指定進行移轉的 VMkernel 重複。	確保在安裝或解除安裝對應組態中未指定重複的 VMkernel 介面。

表 8-1. VMkernel 移轉錯誤 (續)

錯誤碼	問題	原因	解決方案
8298	VMkernel 介面和目的地的數目不相符。	組態不正確。	確保組態中針對每個 VMkernel 介面均指定了對應的目的地。
8299	無法刪除傳輸節點，因為 VMkernel 介面正在使用 N-VDS 上的連接埠。	VMkernel 介面正在使用 N-VDS 交換器上的連接埠。	將所有 VMkernel 介面移轉從 N-VDS 交換器還原至 VSS/DVS 交換器，然後嘗試刪除傳輸節點。
9412	VMkernel 無法從一個 N-VDS 移轉至另一個 N-VDS。	不支援的動作。	將 VMkernel 介面移轉還原至 VSS 或 DVS 交換器，然後，您可以將 VMkernel 介面移轉至另一個 N-VDS 交換器。
9413	VMkernel 介面無法移轉至不同的邏輯交換器。	在可設定狀態的主機上，連線到邏輯交換器的 VMkernel 無法移轉至另一個邏輯交換器。	將 VMkernel 移轉從邏輯交換器還原至 VSS/DVS 交換器，然後，將 VMkernel 移轉至 N-VDS 上的另一個邏輯交換器。
9414	VMkernel 介面重複。	在安裝和解除安裝對應組態中對應的 VMkernel 介面重複。	確保安裝和解除安裝對應中的每個 VMkernel 介面都是唯一的。
9415	主機上的虛擬機器已開啟電源。	如果虛擬機器已開啟電源，則不會繼續移轉。	關閉主機上虛擬機器的電源，然後再起始 VMkernel 介面移轉。
9416	在主機上找不到 VMkernel。	指定的 VMkernel 在主機上的網路對應組態中不存在。	指定網路對應組態中存在的 VMkernel。
9417	找不到連接埠群組。	未指定存在於網路對應組態中的主機的連接埠群組。	指定網路對應組態中存在的連接埠群組。
9419	在移轉期間找不到邏輯交換器。	找不到在網路介面對應組態中定義的邏輯交換器。	指定網路介面對應組態中存在的邏輯交換器。
9420	在移轉期間找不到邏輯連接埠。	在移轉期間，NSX-T Data Center 找不到在邏輯交換器上建立的連接埠。	確保未從邏輯交換器刪除邏輯連接埠，以便成功執行移轉。
9421	主機資訊遺失，無法驗證移轉程序。	無法從詳細目錄擷取主機資訊。	重試移轉程序。
9423	釘選到 VMkernel 介面的實體 NIC 不會移轉到正確的主機交換器。	在環境中找到釘選的實體 NIC，但 VMkernel 和實體 NIC 未移轉到相同的主機交換器。	釘選到 VMkernel 介面的實體 NIC 必須具有將實體 NIC 對應到相同主機交換器上的 VMkernel 的傳輸節點組態。
600	找不到物件。	邏輯交換器使用的指定傳輸區域不存在。 找不到 VMK 對應目的地中的邏輯交換器。	■ 指定環境中存在的傳輸區域。 ■ 建立所需的邏輯交換器，或使用現有 VLAN 邏輯交換器。
8310	邏輯交換器類型不正確。	邏輯交換器類型為「覆疊」。	建立 VLAN 邏輯交換器。
9424	如果同時設定了僅限 PNIC 的移轉及用於安裝或解除安裝的網路對應設定，則無法進行移轉。	僅當設定了其中一個設定時，移轉才會進行。	確保設定僅限 PNIC 的移轉或用於安裝或解除安裝的網路對應設定。

建立獨立主機或裸機伺服器傳輸節點

您必須先將 ESXi 主機、KVM 主機或裸機伺服器新增至 NSX-T Data Center 網狀架構，然後再設定傳輸節點。

網狀架構節點是已向 NSX-T Data Center 管理平面登錄並已安裝 NSX-T Data Center 模組的節點。若要讓主機或裸機伺服器成為 NSX-T Data Center 覆疊的一部分，必須先將其新增至 NSX-T Data Center 網狀架構。

傳輸節點是參與 NSX-T Data Center 覆疊或 NSX-T Data Center VLAN 網路的節點。

對於 KVM 主機或裸機伺服器，您可以預先設定 N-VDS，也可以讓 NSX Manager 執行組態。對於 ESXi 主機，NSX Manager 會一律設定 N-VDS。

備註 如果您打算透過範本虛擬機器建立傳輸節點，請確定主機上的 `/etc/vmware/nsx/` 中沒有憑證。如果憑證存在，則 netcpa 代理程式不會建立憑證。

裸機伺服器支援覆疊和 VLAN 傳輸區域。您可以使用管理介面來管理裸機伺服器。應用程式介面可讓您存取裸機伺服器上的應用程式。

單一實體 NIC 可為管理和應用程式 IP 介面提供 IP 位址。

雙實體 NIC 可為管理介面提供實體 NIC 和唯一的 IP 位址。雙實體 NIC 還可為應用程式介面提供實體 NIC 和唯一的 IP 位址。

繫結組態中的多個實體 NIC 可為管理介面提供雙實體 NIC 和唯一的 IP 位址。繫結組態中的多個實體 NIC 還可為應用程式介面提供雙實體 NIC 和唯一的 IP 位址。

您可以為每個組態最多新增四個 N-VDS 交換器：為 VLAN 傳輸區域建立的標準 N-VDS、為 VLAN 傳輸區域建立的增強型 N-VDS、為覆疊傳輸區域建立的標準 N-VDS、為覆疊傳輸區域建立的增強型 N-VDS。

在同一主機上執行多個標準覆疊 N-VDS 交換器和 Edge 虛擬機器的單一主機叢集拓撲中，NSX-T Data Center 會提供流量隔離，使經過第一個 N-VDS 的流量與經過第二個 N-VDS 的流量相隔離，依此類推。每個 N-VDS 上的實體 NIC 必須對應至主機上的 Edge 虛擬機器，以允許與外部環境的南北向流量連線。在第一個傳輸區域上移出虛擬機器的封包必須通過外部路由器或外部虛擬機器路由至第二個傳輸區域上的虛擬機器。

必要條件

- 主機必須加入管理平面，且連線必須為 [啟動]。
- 您必須設定傳輸區域。
- 必須設定上行設定檔，或者您可以使用預設上行設定檔。
- 您必須設定 IP 集區，或者網路部署中必須提供 DHCP。
- 主機節點上必須至少有一個未使用的實體 NIC。
- 主機名稱
- 管理 IP 位址
- 使用者名稱

- 密碼
- (選用) (KVM) SHA-256 SSL 指紋
- (選用) (ESXi) SHA-256 SSL 指紋
- 確認已安裝必要的第三方套件。請參閱在 KVM 主機上安裝第三方套件。

程序

1 (選擇性) 擷取 Hypervisor 指紋，以便能在將主機新增到網狀架構時提供此指紋。

a 收集 Hypervisor 指紋資訊。

使用 Linux Shell。

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout
-fingerprint -sha256
```

在主機中使用 ESXi CLI。

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

b 從 KVM Hypervisor 擷取 SHA-256 指紋，並在 KVM 主機中執行命令。

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64
```

2 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。

3 從 [管理者] 欄位中，選取**獨立主機**，然後按一下 **+ 新增**。

4 輸入要新增至網狀架構的獨立主機或裸機伺服器詳細資料。

選項	說明
名稱與說明	輸入用於識別獨立主機或裸機伺服器的名稱。 您可以選擇性地新增用於主機或裸機伺服器的作業系統的說明。
IP 位址	輸入主機或裸機伺服器的 IP 位址。
作業系統	從下拉式功能表中選取作業系統。 根據您的主機或裸機伺服器，您可以選取任何支援的作業系統。請參閱系統需求。
使用者名稱和密碼	輸入主機使用者名稱與密碼。
SHA-256 指紋	輸入用於驗證的主機指紋值。 如果您將指紋值保留空白，則系統會提示您接受伺服器提供的值。NSX-T Data Center 需要幾秒的時間來探索和驗證主機。

5 (必要) 對於 KVM 主機或裸機伺服器，選取 N-VDS 類型。

選項	說明
已建立 NSX	NSX Manager 建立 N-VDS。 預設為選取此選項。
已預先設定	已設定 N-VDS。

對於 ESXi 主機，N-VDS 類型一律設為**已建立 NSX**。

6 輸入標準 N-VDS 詳細資料。可在單一主機上設定多個 N-VDS 交換器。

選項	說明
傳輸區域	從下拉式功能表中選取此傳輸節點所屬的傳輸區域。
N-VDS 名稱	必須與此節點所屬之傳輸區域的 N-VDS 名稱相同。
NIOC 設定檔	對於 ESXi 主機，從下拉式功能表中選取 NIOC 設定檔。
上行設定檔	從下拉式功能表中選取現有的上行設定檔，或建立自訂上行設定檔。 您也可以使用預設上行設定檔。
LLDP 設定檔	依預設，NSX-T 僅從 LLDP 芳鄰接收 LLDP 封包。 但是，NSX-T 可以設定為傳送 LLDP 封包至 LLDP 芳鄰，以及從 LLDP 芳鄰接收 LLDP 封包。
IP 指派	選取**使用 DHCP**、**使用 IP 集區**或**使用靜態 IP 清單**。 如果您選取**使用靜態 IP 清單**，您必須指定由 IP 位址、閘道和子網路遮罩構成、並以逗號分隔的清單。
IP 集區	如果您已針對 IP 指派選取**使用 IP 集區**，請指定 IP 集區名稱。
實體 NIC	將實體 NIC 新增至傳輸節點。您可以使用預設上行或從下拉式功能表中指派現有的上行。 按一下**新增 PNIC**，為傳輸節點設定其他實體 NIC。 **備註** 您在此欄位中新增的實體 NIC 的移轉取決於您如何設定**僅限 PNIC 的移轉**、**用於安裝的網路對應**和**用於解除安裝的網路對應**。 ■ 若要移轉無相關聯 VMkernel 對應的已用實體 NIC (例如，由標準 vSwitch 或 vSphere 分散式交換器使用)，請確保已啟用**僅限 PNIC 的移轉**。否則，傳輸節點狀態仍為**部分成功**，且網狀架構節點 LCP 連線將無法建立。 ■ 若要移轉具有相關聯 VMkernel 網路對應的已用實體 NIC，請停用**僅限 PNIC 的移轉**，並設定 VMkernel 網路對應。 ■ 若要移轉可用的實體 NIC，請啟用**僅限 PNIC 的移轉**。

選項	說明
僅限 PNIC 的移轉	設定此欄位之前，請考量以下幾點： ■ 瞭解定義的實體 NIC 是已用 NIC 還是可用 NIC。 ■ 決定是否需要將主機的 VMkernel 介面與實體 NIC 一起移轉。 設定欄位： ■ 如果您只想將實體 NIC 從 VSS 或 DVS 交換器移轉至 N-VDS 交換器，請啟用**僅限 PNIC 的移轉**。 ■ 如果您想要移轉已用實體 NIC 及其相關聯的 VMkernel 介面對應，請停用**僅限 PNIC 的移轉**。指定 VMkernel 介面移轉對應後，可用的實體 NIC 會連結至 N-VDS 交換器。 在具有多個主機交換器的主機上： ■ 如果所有主機交換器將僅移轉 PNIC，您可以在單一作業中移轉 PNIC。 ■ 如果部分主機交換器將移轉 VMkernel 介面，且剩餘主機交換器將僅移轉 PNIC： 1 在第一個作業中，僅移轉 PNIC。 2 在第二個作業中，移轉 VMkernel 介面。確保**僅限 PNIC 的移轉**已停用。 在多個主機之間不同時支援僅限 PNIC 的移轉和 VMkernel 介面移轉。 **備註** 若要移轉管理網路 NIC，請設定其相關聯的 VMkernel 網路對應，並保持**僅限 PNIC 的移轉**的停用狀態。如果您僅移轉管理 NIC，則主機會中斷連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。
用於安裝的網路對應	若要在安裝期間將 VMkernel 移轉至 N-VDS 交換器，請將 VMkernel 對應到現有的邏輯交換器。NSX Manager 將 VMkernel 移轉至 N-VDS 上對應的邏輯交換器。 注意 確保將管理 NIC 和管理 VMkernel 介面移轉至一個邏輯交換器，其連線至移轉之前管理 NIC 連線到的同一 VLAN。如果將 vmnic<*n*> 和 VMkernel<*n*> 移轉到不同的 VLAN，就會與主機中斷連線。 注意 對於固定的實體 NIC，請確保實體 NIC 至 VMkernel 介面的主機交換器對應符合傳輸節點設定檔中指定的組態。做為驗證程序的一部分，NSX-T Data Center 會檢查對應，如果驗證通過，則檢查 VMkernel 介面到 N-VDS 交換器的移轉是否成功。同時，必須設定解除安裝的網路對應，因為將 VMkernel 介面移轉至 N-VDS 交換器後，NSX-T Data Center 不會儲存主機交換器的對應組態。如果未設定對應，可能會在移轉回 VSS 或 VDS 交換器後中斷與服務 (例如 vSAN) 的連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。
用於解除安裝的網路對應	若要在解除安裝期間還原 VMkernel 的移轉，請將 VMkernel 對應到 VSS 或 DVS 上的連接埠群組，以便 NSX Manager 知道必須將 VMkernel 移轉回 VSS 或 DVS 上的哪個連接埠群組。對於 DVS 交換器，請確保連接埠群組屬於類型暫時。 注意 對於固定的實體 NIC，請確保實體 NIC 至 VMkernel 介面的傳輸節點設定檔對應符合主機交換器中指定的組態。設定用於解除安裝的網路對應是強制性的，因為將 VMkernel 介面移轉到 N-VDS 交換器之後，NSX-T Data Center 不會儲存主機交換器的對應組態。如果未設定對應，可能會在移轉回 VSS 或 VDS 交換器後中斷與服務 (例如 vSAN) 的連線。 如需詳細資訊，請參閱 VMkernel 移轉至 N-VDS 交換器。

7 輸入增強型資料路徑 N-VDS 詳細資料。可在單一主機上設定多個 N-VDS 交換器。

選項	說明
N-VDS 名稱	必須與此節點所屬之傳輸區域的 N-VDS 名稱相同。
IP 指派	選取**使用 DHCP**、**使用 IP 集區**或**使用靜態 IP 清單**。 如果您選取**使用靜態 IP 清單**，您必須指定由 IP 位址、閘道和子網路遮罩構成、並以逗號分隔的清單。
IP 集區	如果您已針對 IP 指派選取**使用 IP 集區**，請指定 IP 集區名稱。
實體 NIC	將實體 NIC 新增至傳輸節點。您可以使用預設上行或從下拉式功能表中指派現有的上行。 按一下**新增 PNIC**，為傳輸節點設定其他實體 NIC。 **備註** 您在此欄位中新增的實體 NIC 的移轉取決於您如何設定**僅限 PNIC 的移轉**、**用於安裝的網路對應**和**用於解除安裝的網路對應**。 ■ 若要移轉無相關聯 VMkernel 對應的已用實體 NIC (例如，由標準 vSwitch 或 vSphere 分散式交換器使用)，請確保已啟用**僅限 PNIC 的移轉**。否則，傳輸節點狀態仍為**部分成功**，且網狀架構節點 LCP 連線將無法建立。 ■ 若要移轉具有相關聯 VMkernel 網路對應的已用實體 NIC，請停用**僅限 PNIC 的移轉**，並設定 VMkernel 網路對應。 ■ 若要移轉可用的實體 NIC，請啟用**僅限 PNIC 的移轉**。
上行	從下拉式功能表中選取上行設定檔。
CPU 組態	在 [NUMA 節點索引] 下拉式功能表中，選取您想要指派給 N-VDS 交換器的 NUMA 節點。使用值 0 表示節點上存在的第一個 NUMA 節點。 您可以執行 `esxcli hardware memory get` 命令以瞭解主機上的 NUMA 節點數目。 **備註** 如果您想變更與 N-VDS 交換器具有相似性的 NUMA 節點數目，您可以更新 NUMA 節點索引值。
	在 [每個 NUMA 節點的邏輯核心數目] 下拉式功能表中，選取增強型資料路徑必須使用的邏輯核心數目。 您可以執行 `esxcli network ens maxLcores get` 命令，以瞭解可在 NUMA 節點上建立的邏輯核心數目上限。 **備註** 如果您耗盡可用的 NUMA 節點和邏輯核心，將無法針對 ENS 流量啟用新增到傳輸節點的任何交換器。

8 對於預先設定的 N-VDS，提供下列詳細資料。

選項	說明
N-VDS 外部識別碼	必須與此節點所屬之傳輸區域的 N-VDS 名稱相同。
VTEP	虛擬通道端點名稱。

9 在**主機傳輸節點**頁面上檢視連線狀態。

將主機或裸機伺服器新增為傳輸節點後，NSX Manager 的連線會在 3-4 分鐘內變更為 [啟動] 狀態。

10 或者，使用 CLI 命令檢視連線狀態。

- 針對 ESXi，請輸入 `esxcli network ip connection list | grep 1234` 命令。

```
# esxcli network ip connection list | grep 1234
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   已建立  1000144459  newreno  netcpa
```

- 針對 KVM，請輸入 `netstat –anp ––tcp | grep 1234` 命令。

```
user@host:~$ netstat –anp ––tcp | grep 1234
tcp  0   0 192.168.210.54:57794  192.168.110.34:1234   已建立 –
```

11 確認您的主機或裸機伺服器上已安裝 NSX-T Data Center 模組。

由於將主機或裸機伺服器新增至 NSX-T Data Center 網狀架構，主機或裸機伺服器上已安裝一組 NSX-T Data Center 模組。

不同主機上的模組會封裝如下：

- RHEL 或 CentOS 上的 KVM - RPM。
- Ubuntu 上的 KVM - DEB
- 在 ESXi 上，輸入命令 `esxcli software vib list | grep nsx`。

  日期為您執行安裝的日期。
- 在 RHEL 或 CentOS 上，輸入命令 `yum list installed` 或 `rpm –qa`。
- 在 Ubuntu 上，輸入命令 `dpkg ––get-selections`。

12 (選擇性) 如果您有 500 個或以上的 Hypervisor，請變更某些程序的輪詢間隔。

如果有 500 個以上的 Hypervisor，NSX Manager 可能會遇到高 CPU 使用量和效能問題。

a 使用 NSX-T Data Center CLI 命令 `copy file` 或 API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file`，將 `aggsvc_change_intervals.py` 指令碼複製到主機。

b 執行指令碼 (位於 NSX-T Data Center 檔案存放區中)。

```
python aggsvc_change_intervals.py –m '<NSX ManagerIPAddress>' –u 'admin' –p '<password>' –i
900
```

c (選擇性) 將輪詢間隔變更回其預設值。

```
python aggsvc_change_intervals.py –m '<NSX ManagerIPAddress>' –u 'admin' –p '<password>' –r
```

結果

備註 對於 NSX-T Data Center 建立的 N-VDS，在建立傳輸節點後，如果您要變更此組態 (例如通道端點的 IP 指派)，則必須透過 NSX Manager GUI 而非主機上的 CLI 來執行此操作。

後續步驟

將網路介面從 vSphere 標準交換器移轉至 N-VDS。請參閱 VMkernel 移轉至 N-VDS 交換器。

設定受管理的主機傳輸節點

如果您擁有 vCenter Server，則可以在所有 NSX-T Data Center 主機上自動安裝並建立傳輸節點，而不需手動設定。

如果已設定傳輸節點，則該節點便不適用於自動建立傳輸節點。

必要條件

- 確認 vCenter Server 中的所有主機已都開啟電源。
- 確認已滿足系統需求。請參閱系統需求。
- 確認傳輸區域可用。請參閱建立傳輸區域。
- 確認已設定傳輸節點設定檔。請參閱新增傳輸節點設定檔。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。

3 從 [管理者] 下拉式功能表中選取現有的 vCenter Server。

頁面會列出所選 vCenter Server ESXi 中的可用 vSphere 叢集和/或主機。您可能需要展開叢集才能檢視 ESXi 主機。

4 從清單中選取單一主機，然後按一下**設定 NSX**。

[設定 NSX] 對話方塊隨即開啟。

a 確認 [主機詳細資料] 面板中的主機名稱。您可以選擇性地新增說明。

b 按**下一步**移動到**設定 NSX** 面板。

c 選取可用的傳輸區域，然後按一下 **>** 按鈕，以在傳輸節點設定檔中包含傳輸區域。

5 確認 [主機詳細資料] 面板中的主機名稱，然後按**下一步**。

您可以選擇性地新增說明。

6 在**設定 NSX** 面板中，選取所需的傳輸區域。

您可選取多個傳輸區域。

7 (選擇性) 檢視 ESXi 連線狀態。

```
# esxcli network ip connection list | grep 1235
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   已建立  1000144459  newreno  netcpa
```

8 從 [主機傳輸節點] 頁面，確認叢集中主機的 NSX Manager 連線狀態為 [啟動]，且 NSX-T Data Center 組態狀態為 [成功]。

您還可以查看傳輸區域是否已套用至叢集中的主機。

9 (選擇性) 從傳輸區域中的主機移除 NSX-T Data Center 安裝和傳輸節點。

a 選取一或多個主機，然後按一下**動作 > 移除 NSX**。

解除安裝最多需花費三分鐘。NSX-T Data Center 解除安裝會移除主機上的傳輸節點組態，主機會從傳輸區域和 N-VDS 交換器中斷連結。在將傳輸節點設定檔重新套用到叢集之前，不會自動設定新增至 vCenter Server 叢集中的任何新主機。

10 (選擇性) 從傳輸區域中移除傳輸節點。

a 選取單一傳輸節點，然後按一下**動作 > 從傳輸區域中移除**。

後續步驟

建立邏輯交換器並指派邏輯連接埠。請參閱《NSX-T Data Center 管理指南》中的〈進階交換〉一節。

為 ESXi 主機傳輸節點設定連結彙總

此程序說明如何建立已設定連結彙總群組的上行設定檔，以及如何設定 ESXi 主機傳輸節點以使用該上行設定檔。

必要條件

- 自行熟悉建立上行設定檔的步驟。請參閱建立上行設定檔。
- 自行熟悉建立主機傳輸節點的步驟。請參閱 建立獨立主機或裸機伺服器傳輸節點。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 設定檔 > 上行設定檔 > 新增**。

3 輸入名稱和 (選用) 說明。

例如，您輸入名稱 **`uplink-profile1`**。

4 在 **LAG** 下，按一下**新增**以新增連結彙總群組。

例如，針對名為 **`lag1`** 的 LAG 新增 2 個上行。

5 在**整併**下方，選取**預設整併**。

6 在**作用中上行**欄位中，輸入步驟 4 中新增的 LAG 名稱。在此範例中，名稱為 **`lag1`**。

7 輸入**傳輸 VLAN** 和 **MTU** 的值。

8 按一下對話方塊底部的**新增**。

9 在**整併**下，按一下**新增**以新增連結彙總的項目。

10 選取**網狀架構 > 節點 > 主機傳輸節點 > 新增**。

11 在**主機詳細資料**索引標籤中，輸入主機的 IP 位址、作業系統名稱、管理員認證和 SHA-256 指紋。

12 在 **N-VDS** 索引標籤中，選取步驟 3 中建立的上行設定檔 **uplink-profile1**。

13 在**實體 NIC** 欄位中，[實體 NIC 和上行] 下拉式清單會反映新的 NIC 和上行設定檔。具體來說，其中會顯示上行 **lag1-0** 和 **lag1-1**，與步驟 4 中建立的 LAG **lag1** 相對應。分別選取 **lag1-0** 和 **lag1-1** 的實體 NIC。

14 輸入其他欄位的資訊。

完全折疊的 vSphere 叢集 NSX-T 部署

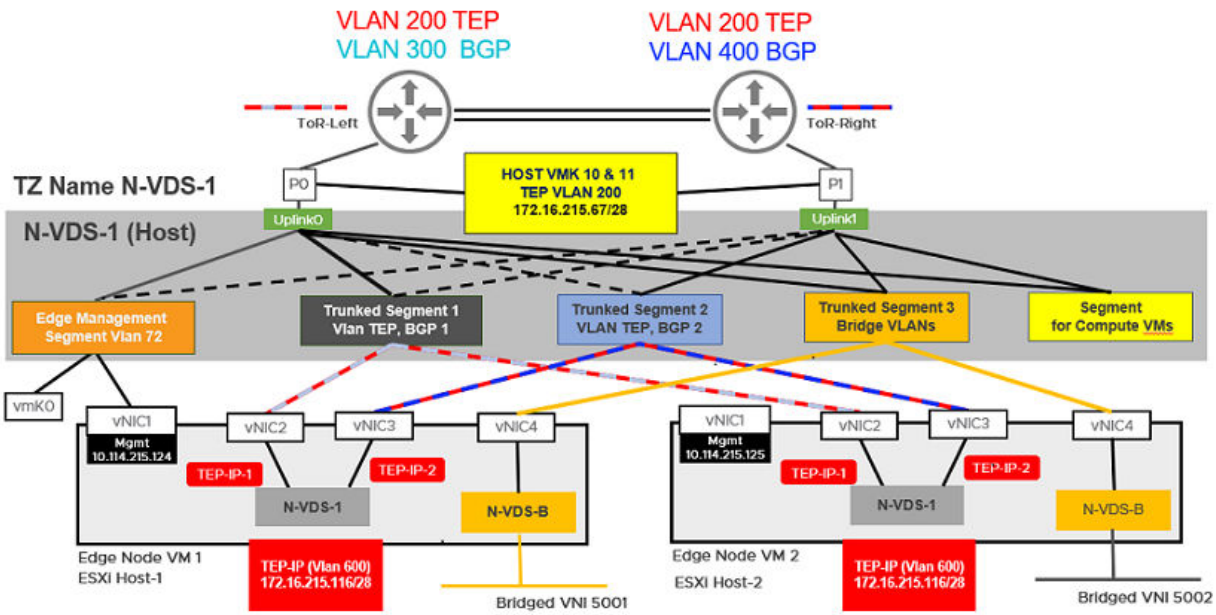
在單一叢集上設定 NSX Manager、執行工作負載虛擬機器的主機傳輸節點，以及 NSX Edge 虛擬機器。叢集中的每台主機都提供為 NSX-T 設定的兩個實體 NIC。

重要　請從 NSX-T 2.4.2 或 2.5 版開始，部署完全折疊的單一 vSphere 叢集拓撲。

此程序中參考的拓撲使用：

- 用叢集中的主機進行設定的 vSAN。
- 每個主機至少有兩個實體 NIC。
- vMotion 和管理 VMkernel 介面。

圖 8-3. 拓撲：管理主機與 NSX Edge 和客體虛擬機器通訊的單一 N-VDS 交換器



備註　即使主機具有四個實體 NIC，但僅有兩個 NIC 可用於部署完全折疊的拓撲。此程序會將主機上的實體 NIC 參考為 vmnic0 和 vmnic1。

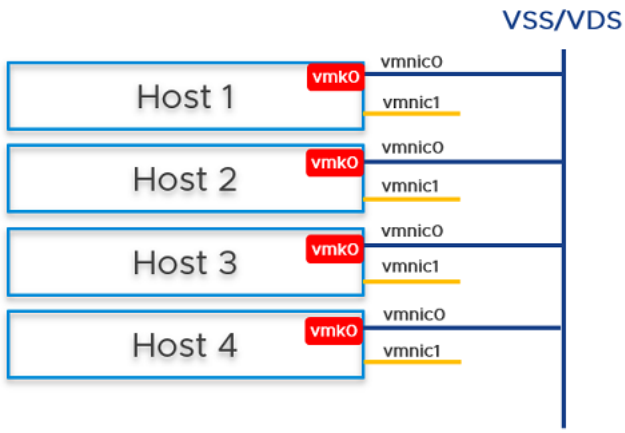
必要條件

- 所有主機都必須是 vSphere 叢集的一部分。

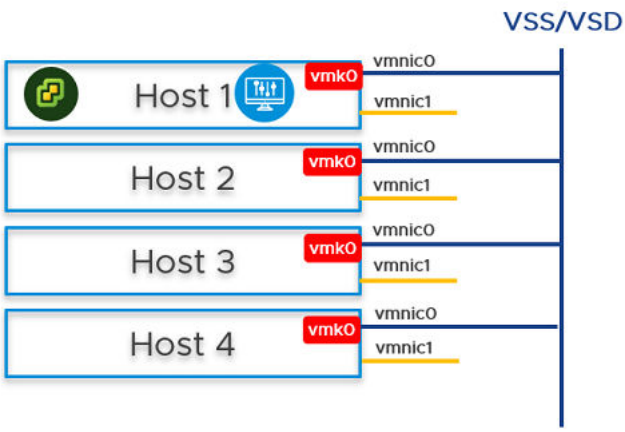
- 每個主機都已啟用兩個實體 NIC。
- 將所有主機登錄至 vCenter Server。
- 在 vCenter Server 上確認共用儲存區可供主機使用。
- 確定用於 TEP 和 HOST TEP 的 VLAN 識別碼與 NSX Edge 不同。

程序

1 在 vSS 或 vDS 上準備四個具有 vmnic0 的 ESXi 主機，vmnic1 可供使用。



2 在主機 1 上，安裝 vCenter Server、設定 vSS/vDS 連接埠群組，然後在主機上所建立的連接埠群組上安裝 NSX Manager。



3 準備 ESXi 主機 1、2、3 和 4 以作為傳輸節點。

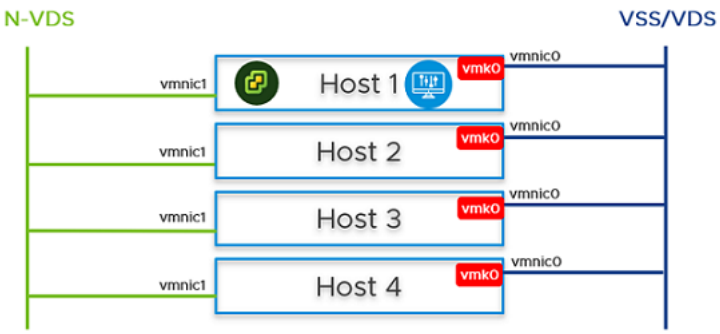
a 使用具名整併原則來建立 VLAN 傳輸區域。請參閱建立傳輸區域。

b 為主機的通道端點 IP 位址建立 IP 集區或 DHCP。請參閱為通道端點 IP 位址建立 IP 集區。

c 為 Edge 節點的通道端點 IP 位址建立 IP 集區或 DHCP。請參閱為通道端點 IP 位址建立 IP 集區。

d 使用具名整併原則來建立上行設定檔。請參閱建立上行設定檔。

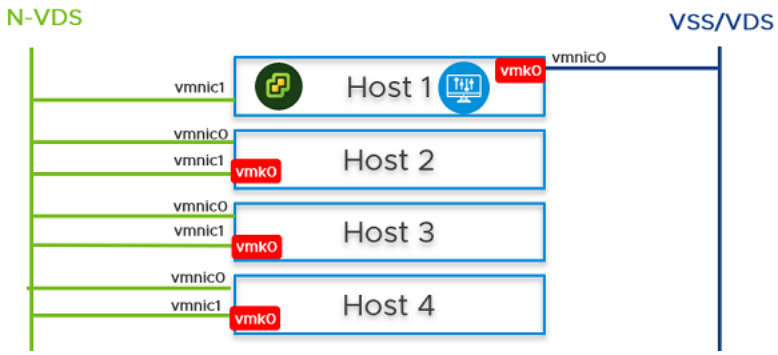
e 藉由套用傳輸節點設定檔，將主機設定為傳輸節點。在此步驟中，傳輸節點設定檔僅會將 vmnic1 (未使用的實體 NIC) 移轉到 N-VDS 交換器。將傳輸節點設定檔套用至叢集主機後，系統會建立 N-VDS 交換器，並將 vmnic1 連線至 N-VDS 交換器。請參閱新增傳輸節點設定檔。



所有主機上的 vmnic1 都會新增至 N-VDS 交換器。因此，在兩個實體 NIC 中，有一個會移轉至 N-VDS 交換器。vmnic0 介面仍會連線至 vSS 或 vDS 交換器，以確定主機的連線可供使用。

4 在 NSX Manager UI 中，為 NSX Manager、vCenter Server、NSX Edge 建立 VLAN 支援的區段。請務必為每個由 VLAN 支援的區段選取正確的整併原則。

5 在主機 2、主機 3 和主機 4 上，您必須同時從 VSS/VDS 將 vmk0 介面卡和 vmnic0 移轉到 N-VDS 交換器。更新每台主機上的 NSX-T 組態。在移轉時，確保 vmnic0 已對應至作用中上行。

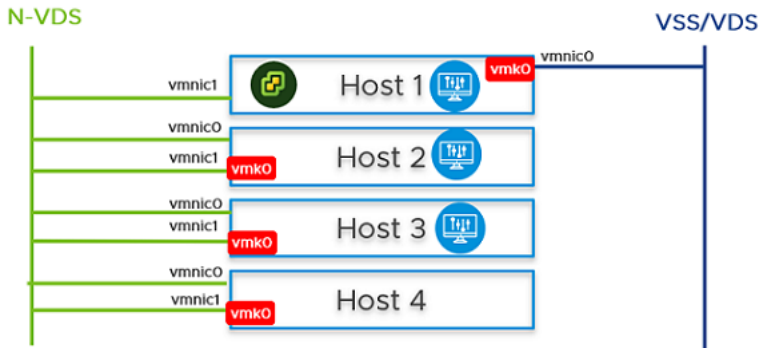


6 在 vCenter Server 中，移至主機 2、主機 3 和主機 4，並確認 vmk0 介面卡已連線至 N-VDS 上的 vmnic0 實體 NIC 並可連線。

7 在 NSX Manager UI 中，移至主機 2、主機 3 和主機 4，並確認兩個 pNIC 均位於 N-VDS 交換器上。

8 建立邏輯區段，並將 NSX Manager 連結到邏輯區段。等待約 10 分鐘讓叢集形成，並確認叢集已形成。

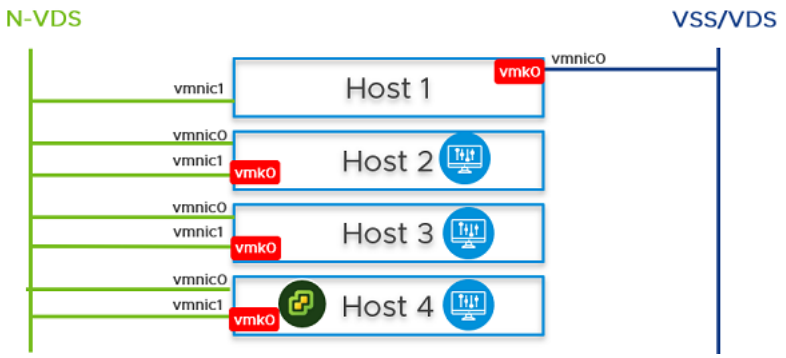
9 在主機 2 和主機 3 上，從 NSX Manager UI 安裝 NSX Manager。



10 關閉第一個 NSX Manager 節點的電源。等待約 10 分鐘。

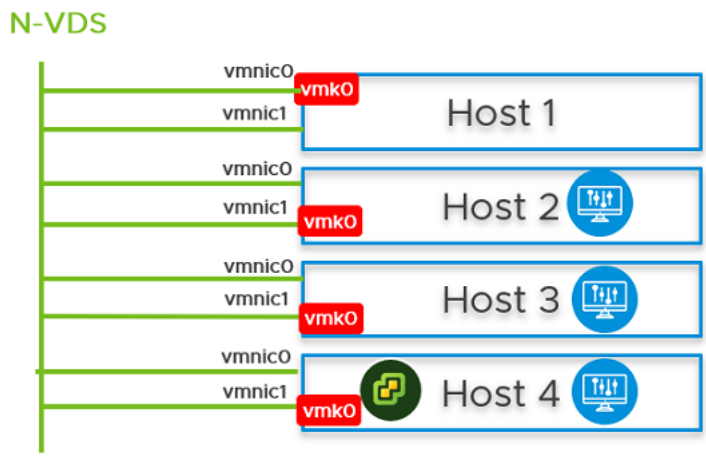
11 將 NSX Manager 和 vCenter Server 重新連結至先前建立的邏輯交換器。在主機 4 上，開啟 NSX Manager 的電源。等待約 10 分鐘，以確認叢集處於穩定狀態。在第一個 NSX Manager 電源關閉的情況下，執行冷 vMotion 以將 NSX Manager 和 vCenter Server 從主機 1 移轉到主機 4。

如需 vMotion 限制的相關資訊，請參閱 https://kb.vmware.com/s/article/56991。



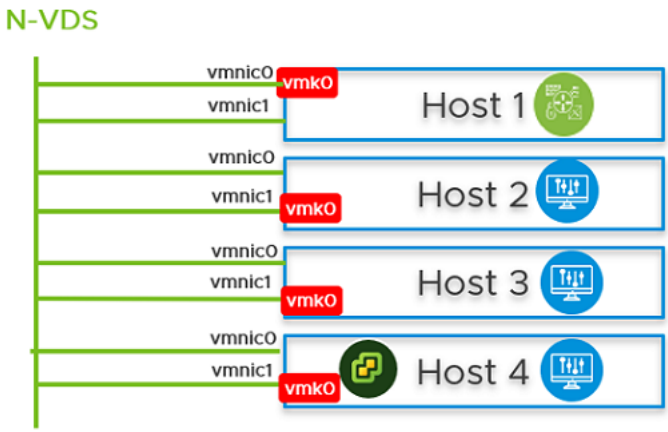
12 從 NSX Manager UI 中，移至主機 1，將 vmk0 和 vmnic0 同時從 VSS 移轉至 N-VDS 交換器。

13 在**用於安裝的網路對應**欄位中，確認 vmk0 介面卡已對應至 N-VDS 交換器上的管理邏輯區段。



14 在主機 1 上，從 NSX Manager UI 安裝 NSX Edge 虛擬機器。

請參閱建立 NSX Edge 傳輸節點。



15 將 NSX Edge 虛擬機器加入管理平面。

請參閱將 NSX Edge 加入管理平面。

16 若要建立南北向流量連線，請使用外部路由器來設定 NSX Edge 虛擬機器。

17 確認 NSX Edge 虛擬機器與外部路由器之間的南北向流量連線。

18 設定並驗證 NSX Manager 與 NSX Edge 虛擬機器之間的 BFD 連線。

19 萬一發生停電而造成整個叢集重新開機的情形，則 NSX-T 管理元件可能不會啟動以及與 N-VDS 通訊。若要避免發生此情況，請執行下列步驟：

注意 任何未正確執行的 API 命令都會導致與 NSX Manager 的連線發生中斷。

備註 在單一叢集組態中，管理元件作為虛擬機器託管於 N-VDS 交換器上。由於安全考慮，管理元件依預設連線的 N-VDS 連接埠會初始化為封鎖的連接埠。如果發生停電而導致四個主機 (建議的最小值) 全都需要重新開機，則在預設重新開機狀態下，管理虛擬機器連接埠會處於已封鎖狀態。若要避免循環相依性，建議在 N-VDS 上建立已解除封鎖狀態的連接埠。已解除封鎖的連接埠可確保叢集重新開機時，NSX-T 管理元件可與 N-VDS 通訊以恢復正常功能。

在子工作結束時，移轉命令會採用：

- NSX Manager 所在主機節點的 UUID。
- NSX Manager 虛擬機器的 UUID，並將其移轉至處於已解除封鎖狀態的靜態邏輯連接埠。

如果所有主機均已關閉電源或均已開啟電源，或者 NSX Manager 虛擬機器移至另一台主機，則在 NSX Manager 恢復運作後，則該虛擬機器會連結至已解除封鎖的連接埠，從而防止與 NSX-T 管理元件的連線發生中斷。

a 前往**進階網路與安全性→交換**，選取 MGMT-VLAN-Segment。在**概觀**索引標籤中，找到並複製 UUID。此範例中使用的 UUID 為 *c3fd8e1b-5b89-478e-abb5-d55603f04452*。

b 若要建立初始化為 **UNBLOCKED_VLAN** 狀態的邏輯連接埠，請建立四個 JSON 檔案，其中 3 個用於 NSX Manager，而 1 個用於 vCenter Server Appliance (VCSA)。將 `logical_switch_id` 的值取代為先前所建立 MGMT-VLAN-Segment 區段的 UUID。

```
mgrhost.json
{
"admin_state": "UP",
"attachment": {
"attachment_type": "VIF",
"id": "nsxmgr-port-147"
},
"display_name": "NSX Manager Node 147 Port",
"init_state": "UNBLOCKED_VLAN",
"logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

c 使用 API 用戶端或使用 curl 命令為 Manager 建立邏輯連接埠。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @mgr.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1574716624192,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 0
```

d 將 NSX Manager 移至靜態建立的邏輯連接埠。

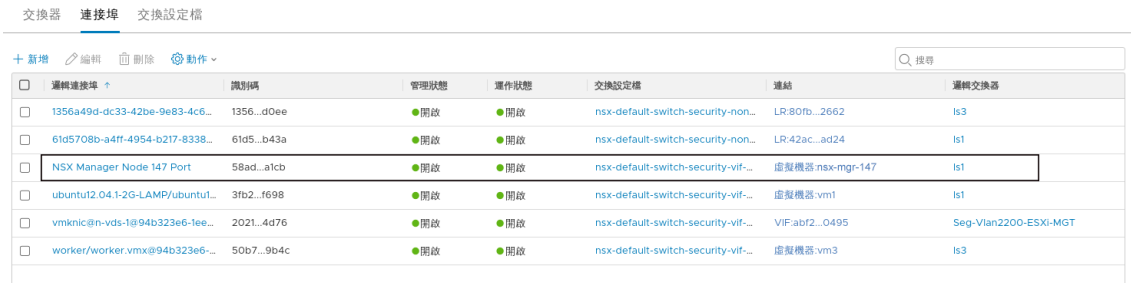
e 若要複製 NSX Manager 虛擬機器執行個體識別碼，請移至 [進階網路與安全性] → [詳細目錄] → [虛擬機器]。選取 NSX Manager 虛擬機器。在**概觀**索引標籤中，找到並複製識別碼。此範例中使用的識別碼為 *5028d756-d36f-719e-3db5-7ae24aa1d6f3*。

f 若要尋找 NSX Manager 安裝所在的主機識別碼，請移至**系統 -> 網狀架構 -> 節點 -> 主機傳輸節點**。選取主機，然後按一下**概觀**索引標籤。尋找並複製主機識別碼。此範例中使用的識別碼為 *11161331-11f8-45c7-8747-34e7218b687f*。

g 將 NSX Manager 從虛擬機器網路移轉至先前在 MGMT-VLAN-Segment 上建立的邏輯連接埠。`vnic_migration_dest` 值是先前為 NSX Manager 建立之連接埠的連結識別碼。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u '<username>:<password>' -H
'Content-Type:application/json' -d @mgrhost.json
'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnic_migration_dest=nsxmgr-port-147'
```

h 在 NSX Manager UI 中，確保靜態建立的邏輯連接埠已開啟。



i 針對叢集中的每個 NSX Manager，重複上述步驟。

確認傳輸節點狀態

請確定傳輸節點建立程序正確運作中。

建立主機傳輸節點後，主機上會安裝 N-VDS。

程序

1 登入 NSX-T Data Center。

2 導覽至 [傳輸節點] 頁面並檢視 N-VDS 狀態。

3 或者，使用 `esxcli network ip interface list` 命令，在 ESXi 上檢視 N-VDS。

在 ESXi 上，命令輸出應包含一個 vmk 介面 (例如 vmk10)，且該介面的 VDS 名稱必須符合您在設定傳輸區域和傳輸節點時所使用的名稱。

```
# esxcli network ip interface list
...

vmk10
   Name: vmk10
```

```
   MAC Address: 00:50:56:64:63:4c
   Enabled: true
   Portset: DvsPortset-1
   Portgroup: N/A
   Netstack Instance: vxlan
   VDS Name: overlay-hostswitch
   VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
   VDS Port: 10
   VDS Connection: 10
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1600
   TSO MSS: 65535
   Port ID: 67108895

 ...
```

如果您使用 vSphere Client，您可以藉由選取主機**組態 > 網路介面卡**，在使用者介面中檢視已安裝的 N-VDS。

用來確認 N-VDS 安裝的 KVM 命令為 `ovs-vsctl show`。請注意，KVM 上的 N-VDS 名稱為 nsx-switch.0。此名稱不符合傳輸節點組態中的名稱。這是出於設計目的。

```
# ovs-vsctl show
...
    Bridge "nsx-switch.0"
        Port "nsx-uplink.0"
            Interface "em2"
        Port "nsx-vtep0.0"
            tag: 0
            Interface "nsx-vtep0.0"
                type: internal
        Port "nsx-switch.0"
            Interface "nsx-switch.0"
                type: internal
    ovs_version: "2.4.1.3340774"
```

4 檢查傳輸節點的已指派通道端點位址。

vmk10 介面會接收來自 NSX-T Data Center IP 集區或 DHCP 的 IP 位址，如下所示：

```
# esxcli network ip interface ipv4 get
Name   IPv4 Address    IPv4 Netmask   IPv4 Broadcast   Address Type  DHCP DNS
-----  --------------  -------------  ---------------  ------------  --------
vmk0   192.168.210.53  255.255.255.0  192.168.210.255  STATIC           false
vmk1   10.20.20.53     255.255.255.0  10.20.20.255     STATIC           false
vmk10 192.168.250.3   255.255.255.0  192.168.250.255  STATIC          false
```

在 KVM 中，您可以使用 `ifconfig` 命令來確認通道端點和 IP 配置。

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet  HWaddr ba:30:ae:aa:26:53
          inet addr:192.168.250.4  Bcast:192.168.250.255  Mask:255.255.255.0
         ...
```

5 如需傳輸節點狀態資訊，請查看 API。

請使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 呼叫。例如：

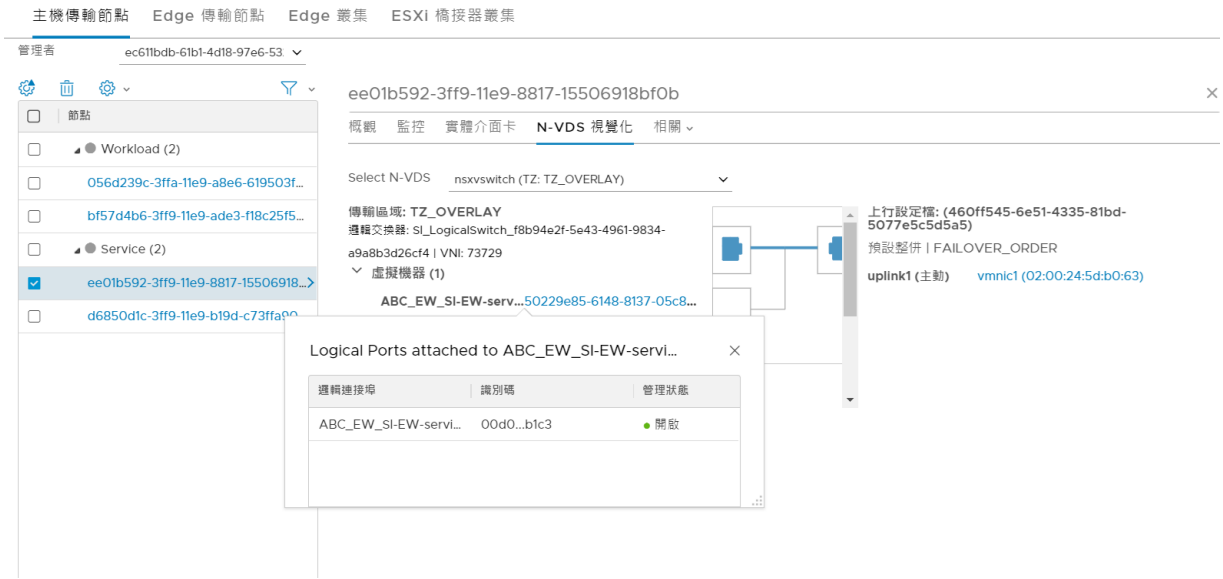
```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

N-VDS 的視覺表示

您可以在個別主機層級取得 N-VDS 的詳細視圖。NSX-T Data Center 為 N-VDS 的上行和傳輸區域相關聯虛擬機器之間的連線狀態提供視覺表示。視覺表示的物件包括整併原則 - 提供虛擬機器連線的上行和實體 NIC。其他一組視覺表示的物件為虛擬機器、相關聯的邏輯連接埠和交換器以及虛擬機器的狀態。視覺表示讓 N-VDS 管理更輕鬆。

備註 只有 ESXi 主機支援視覺化 N-VDS 物件。

圖 8-4. N-VDS 視覺化



程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。

3 在 [管理者] 欄位中，選取**獨立主機**或*計算管理程式*。

4 選取主機。

5 按一下 **N-VDS 視覺化**索引標籤。

6 選取 N-VDS。

NSX-T 以視覺方式表示連線至虛擬機器的上行設定檔、與虛擬機器相關聯的邏輯連接埠、連線至傳輸區域的邏輯交換器。

7 若要檢視連線至虛擬機器的上行設定檔與虛擬機器所連線的邏輯連接埠，請選取虛擬機器。

NSX-T 以視覺方式表示虛擬機器和上行設定檔之間的連線。

8 若要檢視連線至上行設定檔的虛擬機器，請選取上行設定檔。

9 若要檢視與虛擬機器相關聯的邏輯連接埠，請展開邏輯交換器，然後按一下虛擬機器。

邏輯連接埠詳細資料會顯示在單獨的對話方塊中。

備註 邏輯連接埠的管理狀態會顯示在對話方塊中。如果運作狀態為關閉，則不會顯示在對話方塊中。

NSX-T Data Center 核心模組的手動安裝

除了使用 NSX-T Data Center **網狀架構> 節點 > 主機 > 新增** UI 或 `POST /api/v1/fabric/nodes` API 以外，您也可以從 Hypervisor 命令列手動安裝 NSX-T Data Center 核心模組。

備註 您無法在裸機伺服器上手動安裝 NSX-T Data Center 核心模組。

在 ESXi Hypervisor 上手動安裝 NSX-T Data Center 核心模組

若要準備讓主機參與 NSX-T Data Center，您必須在 ESXi 主機上安裝 NSX-T Data Center 核心模組。這可讓您建置 NSX-T Data Center 控制平面和管理平面網狀架構。封裝在 VIB 檔案中的 NSX-T Data Center 核心模組會在 Hypervisor 核心內執行，並提供分散式路由、分散式防火牆和橋接功能等服務。

您可以手動下載 NSX-T Data Center VIB，並使其成為主機映像的一部分。每個 NSX-T Data Center 版本的下載路徑可能會變更。請務必查看 NSX-T Data Center 下載頁面以取得適當的 VIB。

程序

1 以根使用者的身分登入主機，或以具有管理權限的使用者身分登入

2 導覽至 /tmp 目錄。

```
[root@host:~]: cd /tmp
```

3 將 nsx-lcp 檔案下載並複製到 /tmp 目錄中。

4 執行安裝命令。

```
[root@host:/tmp]: esxcli software vib install –d /tmp/nsx–lcp–<release>.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: VMware_bootbank_nsx–aggservice_<release>, VMware_bootbank_nsx–da_<release>,
VMware_bootbank_nsx–esx–datapath_<release>, VMware_bootbank_nsx–exporter_<release>,
VMware_bootbank_nsx–host_<release>, VMware_bootbank_nsx–lldp_<release>, VMware_bootbank_nsx–
mpa_<release>, VMware_bootbank_nsx–netcpa_<release>, VMware_bootbank_nsx–python–
protobuf_<release>, VMware_bootbank_nsx–sfhc_<release>, VMware_bootbank_nsxa_<release>,
VMware_bootbank_nsxcli_<release>
   VIBs Removed:
   VIBs Skipped:
```

根據已安裝在主機上的項目，系統可能會安裝、移除和略過某些 VIB。除非命令輸出指出 `Reboot Required: true`，否則不需要重新開機。

結果

將 ESXi 主機新增至 NSX-T Data Center 網狀架構後，系統會在主機上安裝下列 VIB。

nsx-adf	(自動的診斷架構) 收集並分析效能資料，以產生效能問題的本機 (在主機) 和中央 (跨資料中心) 診斷。
nsx-aggservice	提供適用於 NSX-T Data Center 彙總服務的主機端程式庫。NSX-T Data Center 彙總服務是一種在管理平面節點中執行，且從 NSX-T Data Center 元件擷取執行階段狀態的服務。
nsx-cli-libs	在 Hypervisor 主機上提供 NSX-T Data Center CLI。
nsx-common-libs	提供一些公用程式類別，例如 AES、SHA-1、UUID、點陣圖及其他。
nsx-context-mux	提供 NSX Guest Introspection 轉送功能。允許 VMware Tools 客體代理程式轉送客體內容至內部和已登錄的第三方合作夥伴應用裝置。
nsx-esx-datapath	提供 NSX-T Data Center 數據平面封包處理功能。
nsx-exporter	提供將執行階段狀態報告至在管理平面中執行之彙總服務的主機代理程式。
nsx-host	為安裝在主機上的 VIB 服務包提供中繼資料。
nsx-metrics-libs	提供用於收集精靈度量的度量公用程式類別。
nsx-mpa	提供 NSX Manager 與 Hypervisor 主機之間的通訊。
nsx-nestdb-libs	NestDB 是儲存主機相關 NSX 組態 (所需/執行階段狀態等) 的資料庫。
nsx-netcpa	提供中央控制平面與 Hypervisor 之間的通訊。從中央控制平面接收邏輯網路狀態，並在資料平面中規劃此狀態。
nsx-opsagent	使用管理平面的通訊作業代理程式執行 (傳輸節點實現、連結層探索通訊協定 - LLDP、Traceflow 和封包擷取等)。
nsx-platform-client	提供一般 CLI 執行代理程式，用於集中式 CLI 和稽核記錄收集。
nsx-profiling-libs	提供根據 gpeftool (用於精靈處理程序剖析) 的剖析功能。
nsx-proxy	提供連絡中央控制平面和管理平面的僅限北向連絡點代理程式。
nsx-python-gevent	包含 Python Gevent。
nsx-python-greenlet	包含 Python Greenlet 程式庫 (第三方程式庫)。
nsx-python-logging	包含 Python 記錄。
nsx-python-protobuf	提供通訊協定緩衝區的 Python 繫結。
nsx-rpc-libs	此程式庫提供 nsx-rpc 功能。
nsx-sfhc	服務網狀架構主機元件 (SFHC)。提供一個用來管理 Hypervisor 生命週期的主機代理程式，以便作為管理平面詳細目錄中的網狀架構主機。這提供了

	NSX-T Data Center 升級以及在 Hypervisor 上解除安裝及監控 NSX-T Data Center 模組等作業的通道。
nsx-shared-libs	包含共用的 NSX 程式庫。
nsx-upm-libs	提供扁平化用戶端組態的統一設定檔管理功能，並避免重複資料傳輸。
nsx-vdpi	提供 NSX-T Data Center Distributed Firewall 的深度封包檢查功能。
nsxcli	在 Hypervisor 主機上提供 NSX-T Data Center CLI。
vsipfwlib	提供分散式防火牆功能。

若要確認，您可以在 ESXi 主機上執行 `esxcli software vib list | grep nsx` 和 `esxcli software vib list | grep vsipfwlib` 命令。或者，您也可以執行 `esxcli software vib list | grep <yyyy-mm-dd>` 命令，而日期則是安裝執行當日。

後續步驟

將主機新增至 NSX-T Data Center 管理平面。請參閱使用 CLI 部署 NSX Manager 節點以形成叢集 。

在 Ubuntu KVM Hypervisor 上手動安裝 NSX-T Data Center 核心模組

若要準備讓主機加入 NSX-T Data Center，您需要手動在 Ubuntu KVM 主機上安裝 NSX-T Data Center 核心模組。這可讓您建置 NSX-T Data Center 控制平面和管理平面網狀架構。封裝在 DEB 檔案中的 NSX-T Data Center 核心模組會在 Hypervisor 核心內執行，並提供分散式路由、分散式防火牆和橋接功能等服務。

您可以手動下載 NSX-T Data Center DEB，並使其成為主機映像的一部分。請注意，每個 NSX-T Data Center 版本的下載路徑可能會變更。請務必查看 NSX-T Data Center 下載頁面以取得適當的 DEB。

必要條件

- 確認已安裝必要的第三方套件。請參閱在 KVM 主機上安裝第三方套件。

程序

1. 以具有管理權限的使用者身分登入主機。
2. (選擇性) 導覽至 /tmp 目錄。

```
cd /tmp
```

3. 將 nsx-lcp 檔案下載並複製到 /tmp 目錄中。
4. 將套件解壓縮。

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

5 導覽至套件目錄。

```
cd nsx-lcp-trusty_amd64/
```

6 安裝套件。

```
sudo dpkg -i *.deb
```

7 重新載入 OVS 核心模組。

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

如果 Hypervisor 在 OVS 介面上使用 DHCP，請重新啟動設定 DHCP 的網路介面。您可以在網路介面上手動停止舊 dhclient 程序，然後在此介面上重新啟動新 dhclient 程序。

8 若要確認，您可以執行 `dpkg -l | grep nsx` 命令。

```
user@host:~$ dpkg -l | grep nsx

ii  nsx-agent                          <release>     amd64        NSX Agent
ii  nsx-aggservice                     <release>     all          NSX Aggregation Service Lib
ii  nsx-cli                            <release>     all          NSX CLI
ii  nsx-da                             <release>     amd64        NSX Inventory Discovery Agent
ii  nsx-host                           <release>     all          NSX host meta package
ii  nsx-host-node-status-reporter      <release>     amd64        NSX Host Status Reporter for
Aggregation Service
ii  nsx-lldp                           <release>     amd64        NSX LLDP Daemon
ii  nsx-logical-exporter               <release>     amd64        NSX Logical Exporter
ii  nsx-mpa                            <release>     amd64        NSX Management Plane Agent Core
ii  nsx-netcpa                         <release>     amd64        NSX Netcpa
ii  nsx-sfhc                           <release>     amd64        NSX Service Fabric Host
Component
ii  nsx-transport-node-status-reporter  <release>     amd64        NSX Transport Node Status
Reporter
ii  nsxa                               <release>     amd64        NSX L2 Agent
```

不完整的相依性最有可能導致錯誤。`apt-get install -f` 命令可以嘗試解析相依性，並重新執行 NSX-T Data Center 安裝。

後續步驟

將主機新增至 NSX-T Data Center 管理平面。請參閱使用 CLI 部署 NSX Manager 節點以形成叢集 。

在 RHEL 和 CentOS KVM Hypervisor 上手動安裝 NSX-T Data Center 核心模組

若要準備讓主機加入 NSX-T Data Center，您需要手動在 RHEL 或 CentOS KVM 主機上安裝 NSX-T Data Center 核心模組。

這可讓您建置 NSX-T Data Center 控制平面和管理平面網狀架構。封裝在 RPM 檔案中的 NSX-T Data Center 核心模組會在 Hypervisor 核心內執行，並提供分散式路由、分散式防火牆和橋接功能等服務。

您可以手動下載 NSX-T Data Center RPM，並使其成為主機映像的一部分。請注意，每個 NSX-T Data Center 版本的下載路徑可能會變更。請務必查看 NSX-T Data Center 下載頁面以取得適當的 RPM。

必要條件

連線 RHEL 或 CentOS 存放庫的能力。

程序

1 以管理員身分登入主機。

2 將 nsx-lcp 檔案下載並複製到 /tmp 目錄中。

3 將套件解壓縮。

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

4 導覽至套件目錄。

```
cd nsx-lcp-rhel74_x86_64/
```

5 安裝套件。

```
sudo yum install *.rpm
```

當您執行 yum install 命令時，系統將會解析任何 NSX-T Data Center 相依性，並假設 RHEL 或 CentOS 主機可連線至其各自的存放庫。

6 重新載入 OVS 核心模組。

```
/etc/init.d/openvswitch force-reload-kmod
```

如果 Hypervisor 在 OVS 介面上使用 DHCP，請重新啟動設定 DHCP 的網路介面。您可以在網路介面上手動停止舊 dhclient 程序，然後在此介面上重新啟動新 dhclient 程序。

7 若要確認，您可以執行 `rpm -qa | egrep 'nsx|openvswitch|nicira'` 命令。

輸出中的已安裝套件必須與 nsx-rhel74 或 nsx-centos74 目錄中的套件相符。

後續步驟

將主機新增至 NSX-T Data Center 管理平面。請參閱使用 CLI 部署 NSX Manager 節點以形成叢集 。

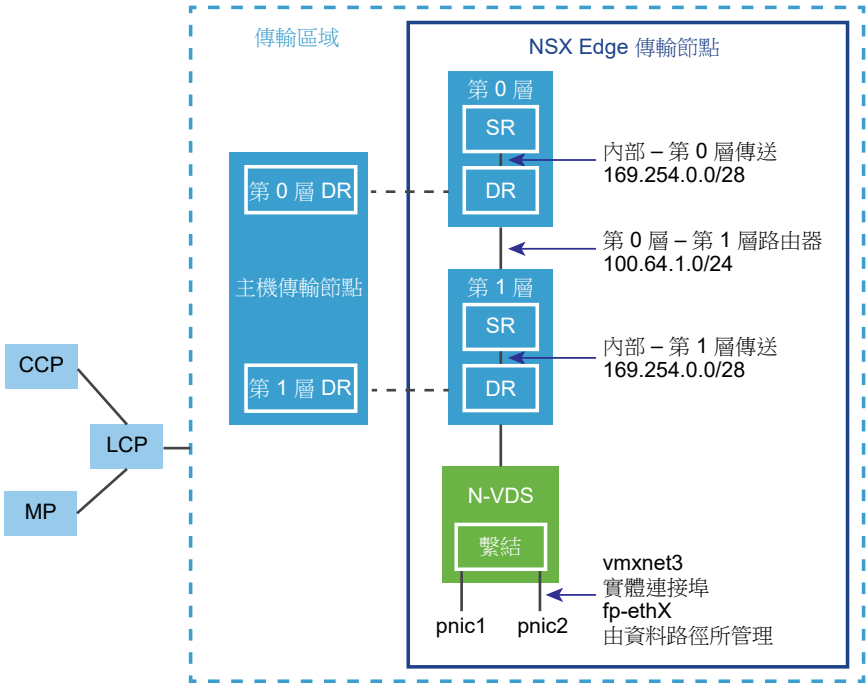
NSX Edge 網路設定

NSX Edge 可使用 ISO、OVA/OVF 或 PXE 啟動來安裝。無論採用何種安裝方法，請務必在安裝 NSX Edge 之前備妥主機網路。

傳輸區域內之 NSX Edge 的高階視圖

NSX-T Data Center 的高階視圖顯示出一個傳輸區域中的兩個傳輸節點。一個傳輸節點是主機。另一個是 NSX Edge。

圖 8-5. NSX Edge 的高階概觀



當您第一次部署 NSX Edge 時，您可以將其視為空的容器。在您建立邏輯路由器之前，NSX Edge 不會執行任何動作。NSX Edge 可提供第 0 層和第 1 層邏輯路由器的運算支援。每個邏輯路由器都包含一個服務路由器 (SR) 和一個分散式路由器 (DR)。當我們提到某路由器是分散式時，表示它已複寫至屬於相同傳輸區域的所有傳輸節點上。在此圖中，主機傳輸節點所包含的 DR 與第 0 層和第 1 層路由器上所包含的相同。如果邏輯路由器將設定成執行 NAT 等的服務，則需要服務路由器。所有的第 0 層邏輯路由器皆具有服務路由器。如果根據您的設計考量而有所需要，則第 1 層路由器也可以具有服務路由器。

依預設，SR 與 DR 之間的連結會使用 169.254.0.0/28 子網路。這些路由器內部轉換連結會在您部署第 0 層或第 1 層邏輯路由器時自動建立。除非 169.254.0.0/28 子網路已用於您的部署中，否則您不需設定或修改連結組態。在第 1 層邏輯路由器上，僅在您於建立第 1 層邏輯路由器期間選取 NSX Edge 叢集時 SR 才會出現。

針對第 0 層至第 1 層的連線指派的預設位址空間為 100.64.0.0/10。系統會為每個第 0 層至第 1 層的對等連線，提供一個在 100.64.0.0/10 位址空間內的 /31 子網路。此連結會在您建立第 1 層路由器，並將其連線至第 0 層路由器時自動建立。除非 100.64.0.0/10 子網路已用於您的部署中，否則您不需設定或修改此連結上的介面。

每個 NSX-T Data Center 部署皆具有一個管理平面叢集 (MP) 和一個控制平面叢集 (CCP)。MP 和 CCP 會將組態推送至每個傳輸區域的本機控制平面 (LCP)。當主機或 NSX Edge 加入管理平面時，管理平面代理程式 (MPA) 會建立對主機或 NSX Edge 的連線，且主機或 NSX Edge 會成為 NSX-T Data Center 網狀架構節點。當網狀架構節點後續新增為傳輸節點時，系統將會建立主機或 NSX Edge 的 LCP 連線。

最後，上圖顯示兩個互相繫結以提供高可用性之實體 NIC (pNIC1 和 pNIC2) 的範例。資料路徑會管理實體 NIC。它們可作為外部網路的 VLAN 上行，或作為受內部 NSX-T Data Center 管理之虛擬機器網路的通道端點連結。

最佳做法是針對部署為虛擬機器的每個 NSX Edge 配置至少兩個實體連結。您可以選擇性地使用不同的 VLAN 識別碼，讓相同 pNIC 上的連接埠群組重疊。找到的第一個網路連結會用於管理。例如，在 NSX Edge 虛擬機器上，找到的第一個連結可能是 vnic1。在裸機安裝上，找到的第一個連結可能是 eth0 或 em0。其餘連結會用於上行和通道。例如，某個連結可能會用於由 NSX-T Data Center 管理之虛擬機器所使用的通道端點。其他連結可能用於 NSX Edge 至外部 TOR 的上行。

透過以管理員身分登入 CLI 並執行 `get interfaces` 和 `get physical-ports` 命令，您可以檢視 NSX Edge 的實體連結資訊。在 API 中，您可以使用 `GET fabric/nodes/<edge-node-id>/network/interfaces` API 呼叫。實體連結將在下一節中詳細討論。

無論是將 NSX Edge 安裝為虛擬機器應用裝置或安裝在裸機上，視部署而定有多個網路組態選項可供使用。

傳輸區域和 N-VDS

若要瞭解 NSX Edge 網路，您必須瞭解某些關於傳輸區域和 N-VDS 的知識。傳輸區域可控制 NSX-T Data Center 中第 2 層網路的連線。N-VDS 是建立在傳輸節點上的軟體交換器。N-VDS 的用途是將邏輯路由器上行和下行繫結至實體 NIC。針對 NSX Edge 所屬的每個傳輸區域，皆有單一 N-VDS 安裝在 NSX Edge 上。

傳輸區域有兩種類型：

- 傳輸節點之間的內部 NSX-T Data Center 通道的重疊。
- NSX-T Data Center 的外部上行的 VLAN。

一個 NSX Edge 可以屬於零個或許多 VLAN 傳輸區域。若為零個 VLAN 傳輸區域，則 NSX Edge 仍可以具有上行，因為 NSX Edge 上行可使用針對覆疊傳輸區域安裝的相同 N-VDS。如果您要讓每個 NSX Edge 皆僅具有一個 N-VDS，即可執行此操作。另一個設計選項，是為了要讓 NSX Edge 屬於多個 VLAN 傳輸區域，即每個上行各一個。

最常見的設計選擇是三個傳輸區域：一個覆疊和兩個 VLAN 傳輸區域，以供備援上行之用。

若要針對用於覆疊流量的傳輸網路和用於 VLAN 流量的其他網路 (例如 VLAN 上行) 使用相同的 VLAN 識別碼，請在兩個不同的 N-VDS 上設定識別碼，一個用於 VLAN，另一個則用於覆疊。

虛擬應用裝置/虛擬機器 NSX Edge 網路

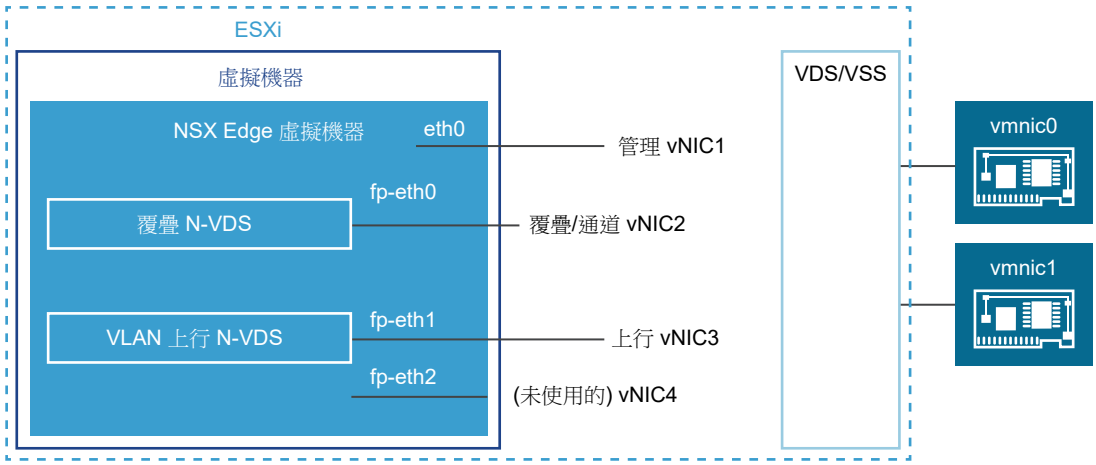
當您將 NSX Edge 安裝為虛擬應用裝置或虛擬機器時，系統將會建立名為 fp-ethX 的內部介面，其中 X 為 0、1、2 和 3。這些介面會配置給 Top-of-Rack (ToR) 交換器的上行使用，以及供 NSX-T Data Center 覆疊通道使用。

當您建立 NSX Edge 傳輸節點時，您可以選取 fp-ethX 介面，將上行與覆疊通道建立關聯。您可以選擇 fp-ethX 介面的使用方式。

在 vSphere Distributed Switch 或 vSphere 標準交換器上，您必須至少為 NSX Edge 配置兩個 vmnic：一個用於 NSX Edge 管理，而另一個用於上行和通道。

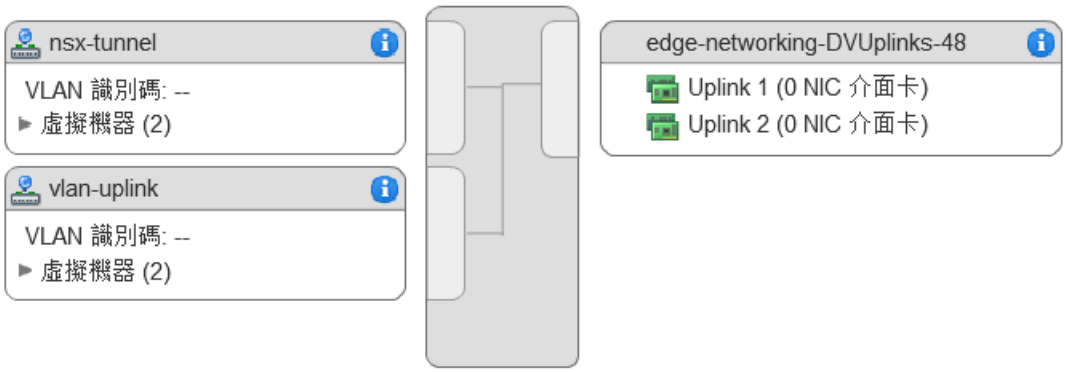
在下列範例實體拓撲中，fp-eth0 會用於 NSX-T Data Center 覆疊通道。fp-eth1 會用於 VLAN 上行。而 fp-eth2 和 fp-eth3 則不使用。vNIC1 會指派給管理網路。

圖 8-6. 一項適用於 NSX Edge 虛擬機器網路的建議連結設定



顯示於此範例中的 NSX Edge 屬於兩個傳輸區域 (一個覆疊，另一個 VLAN)，因此會有兩個 N-VDS，一個用於通道，而另一個用於上行流量。

此螢幕擷取畫面會顯示虛擬機器連接埠群組 nsx-tunnel 和 vlan-uplink。



在部署期間，您必須指定與您的虛擬機器連接埠群組上所設定名稱相符的網路名稱。例如，為了符合範例中的虛擬機器連接埠群組，您的網路 ovftool 設定將如下所示 (如果您使用 ovftool 來部署 NSX Edge)：

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

此處顯示的範例使用虛擬機器連接埠群組名稱 Mgmt、nsx-tunnel 和 vlan-uplink。您可以讓您的虛擬機器連接埠群組使用任何名稱。

為 NSX Edge 設定的通道和上行虛擬機器連接埠群組不需要與 VMkernel 連接埠或給定的 IP 位址建立關聯。這是因為這些群組僅用於第 2 層上。如果您的部署會使用 DHCP 將位址提供給管理介面，請確定僅有一個 NIC 指派給管理網路。

請注意，VLAN 和通道連接埠群組會設定為主幹連接埠。這是必要的。例如，在標準 vSwitch 上，您會以下列方式設定主幹連接埠：**主機 > 組態 > 網路 > 新增網路 > 虛擬機器 > 所有 VLAN 識別碼 (4095)**。

如果您使用應用裝置型或虛擬機器 NSX Edge，則可以使用標準 vSwitch 或 vSphere Distributed Switch。

NSX Edge 虛擬機器可以安裝在 NSX-T Data Center 已備妥的主機上並設定為傳輸節點。共有兩種部署類型：

- NSX Edge 虛擬機器可以使用 VSS/VDS 耗用主機上的單獨 pNIC 的 VSS/VDS 連接埠群組進行部署。主機傳輸節點會耗用主機上安裝的 N-VDS 的單獨 pNIC。主機傳輸節點的 N-VDS 與 VSS 或 VDS 共同存在，兩者均耗用單獨的 pNIC。主機 TEP (通道端點) 和 NSX Edge TEP 可位於相同或不同的子網路。
- NSX Edge 虛擬機器可使用主機傳輸節點之 N-VDS 上的 VLAN 支援的邏輯交換器進行部署。主機 TEP 和 NSX Edge TEP 必須位於不同的子網路。

您可以選擇性地在單一主機上安裝多個 NSX Edge 應用裝置/虛擬機器，而所有已安裝的 NSX Edge 將可使用相同的管理、VLAN 和通道端點連接埠群組。

隨著基礎實體連結已啟用，且虛擬機器連接埠群組已設定的情況中，您可以安裝 NSX Edge。

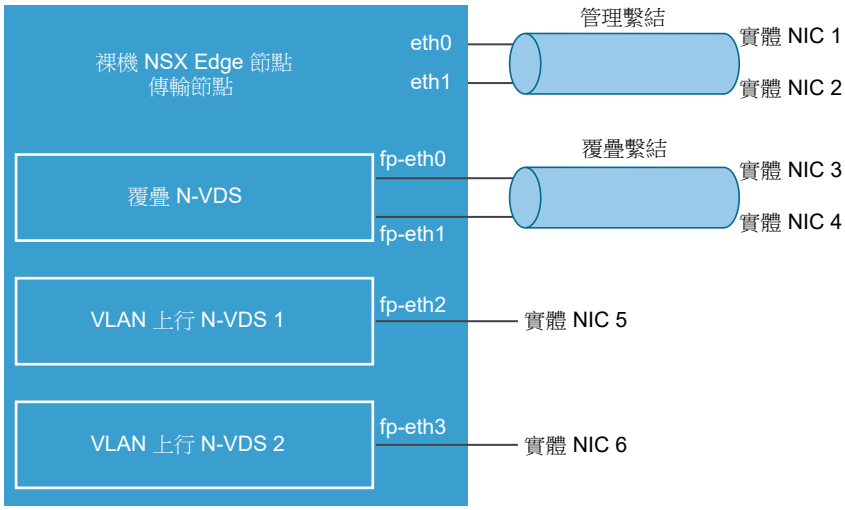
裸機 NSX Edge 網路

裸機 NSX Edge 包含名為 fp-ethX 的內部介面，其中，X 為 0、1、2、3 或 4。建立的 fp-ethX 介面數量取決於您裸機 NSX Edge 所擁有的實體 NIC 數量。這些介面最多有四個可配置給 Top-of-Rack (ToR) 交換器的上行使用，以及供 NSX-T Data Center 覆疊通道使用。

當您建立 NSX Edge 傳輸節點時，您可以選取 fp-ethX 介面，將上行與覆疊通道建立關聯。

您可以選擇 fp-ethX 介面的使用方式。在下列範例實體拓撲中，fp-eth0 會與 fp-eth1 繫結，並且用於 NSX-T Data Center 覆疊通道。fp-eth2 和 fp-eth3 會用作 TOR 的備援 VLAN 上行。

圖 8-7. 一項適用於裸機 NSX Edge 網路的建議連結設定



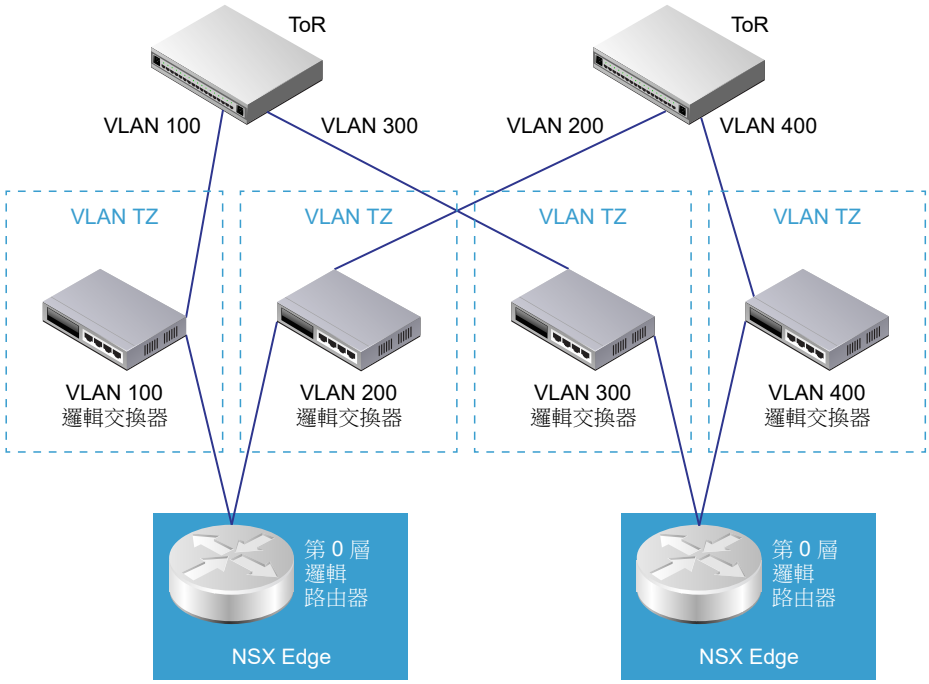
NSX Edge 上行備援

NSX Edge 上行備援可讓兩個 VLAN 相同成本多重路徑 (ECMP) 上行用於 NSX Edge 至外部 TOR 的網路連線上。

當您有兩個 ECMP VLAN 上行時，您還必須要有兩個 TOR 交換器，以實現高可用性和完整的網狀連線。每個 VLAN 邏輯交換器各有一個相關聯的 VLAN 識別碼。

當您將 NSX Edge 新增至 VLAN 傳輸區域時，系統將會安裝新的 N-VDS。例如，如果您將一個 NSX Edge 節點新增至四個 VLAN 傳輸區域 (如圖所示)，則系統會在 NSX Edge 上安裝四個 N-VDS。

圖 8-8. 一項適用於 NSX Edge 至 TOR 的建議 ECMP VLAN 設定



備註 針對 ESXi 主機 (包含 vSphere Distributed Switch (vDS) 和非 N-VDS) 上部署的 Edge 虛擬機器，您必須執行下列操作：

- 啟用偽造的傳輸以使 DHCP 運作。
- 針對 Edge 虛擬機器啟用混合模式以接收未知單點傳播封包，因為預設會停用 MAC 學習。預設會啟用 MAC 學習的 vDS 6.6 或更新版本並不需要此操作。

建立 NSX Edge 傳輸節點

您可以將 NSX Edge 新增至 NSX-T Data Center 網狀架構，並繼續將 NSX Edge 設定為傳輸節點。

傳輸節點是能夠參與 NSX-T Data Center 覆疊或 NSX-T Data Center VLAN 網路的節點。只要是包含 N-VDS 的節點皆可以做為傳輸節點。這類節點包括但不限於 NSX Edge。

NSX Edge 可以屬於一個覆疊傳輸區域和多個 VLAN 傳輸區域。如果虛擬機器需要存取外部環境，則 NSX Edge 必須與虛擬機器的邏輯交換器屬於相同傳輸區域。一般而言，NSX Edge 會屬於至少一個 VLAN 傳輸區域以便提供上行存取。

備註 如果您打算透過範本虛擬機器建立傳輸節點，請確定主機上的 `/etc/vmware/nsx/` 中沒有憑證。如果憑證已存在，則 netcpa 代理程式不會建立憑證。

必要條件

- 您必須設定傳輸區域。
- 確認已設定計算管理程式。請參閱新增計算管理程式。

- 必須設定上行設定檔，或者您可以使用裸機 NSX Edge 節點的預設上行設定檔。
- 您必須設定 IP 集區，或者網路部署中必須提供 IP 集區。
- 主機或 NSX Edge 節點上必須至少有一個未使用的實體 NIC。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 節點 > Edge 傳輸節點 > 新增 Edge 虛擬機器**。
3. 輸入 NSX Edge 的名稱。
4. 輸入 vCenter Server 的主機名稱或 FQDN。
5. 若要獲得最佳效能，請保留 NSX Edge 應用裝置所需的記憶體。

   請設定保留，以確保 NSX Edge 具有足夠記憶體來讓執行更有效率。請參閱 NSX Edge 虛擬機器系統需求。
6. 指定 NSX Edge 的 CLI 和根密碼。

   密碼必須符合密碼強度限制。
   - 至少 12 個字元
   - 至少 1 個小寫字母
   - 至少 1 個大寫字母
   - 至少 1 個數字
   - 至少 1 個特殊字元
   - 至少 5 個不同字元
   - 無字典字組
   - 無回文
   - 不允許使用四個以上單純字元序列
7. 輸入 NSX Edge 詳細資料。

選項	說明
計算管理程式	從下拉式功能表中選取 [計算管理程式]。 計算管理程式是在管理平面中登錄的 vCenter Server。
叢集	從下拉式功能表中指定 NSX Edge 將要加入的叢集。
資源集區或主機	從下拉式功能表中指派 NSX Edge 的資源集區或特定主機。
資料存放區	從下拉式功能表中選取 NSX Edge 檔案的資料存放區。

8 輸入 NSX Edge 介面詳細資料。

選項	說明
IP 指派	選取 **DHCP** 或**靜態** IP。 如果您選取**靜態**，您必須指定由 IP 位址、閘道和子網路遮罩構成、並以逗號分隔的清單。
管理介面	從下拉式功能表中選取虛擬機器網路介面。

9 選取此傳輸節點所屬的傳輸區域。

一個 NSX Edge 傳輸節點至少會屬於兩個傳輸區域：NSX-T Data Center 連線的覆疊和上行連線的 VLAN。

備註 傳輸區域中的多個 VTEP 必須設定為相同的網路區段。如果傳輸區域中的 VTEP 設定為不同網路區段，就無法在 VTEP 之間建立 BFD 工作階段。

10 輸入 N-VDS 資訊。

選項	說明
Edge 交換器名稱	從下拉式功能表中選取覆疊交換器。
上行設定檔	從下拉式功能表中選取上行設定檔。 可用的上行取決於所選上行設定檔中的組態。
IP 指派	針對覆疊 N-VDS，選取**使用 IP 集區**或**使用靜態 IP 清單**。 如果您選取**使用靜態 IP 清單**，您必須指定由 IP 位址、閘道和子網路遮罩構成、並以逗號分隔的清單。
IP 集區	如果您已針對 IP 指派選取**使用 IP 集區**，請指定 IP 集區名稱。
資料路徑介面	選取上行介面的資料路徑介面名稱。

備註 NSX Edge 虛擬機器應用裝置不支援 LLDP 設定檔。

11 在**傳輸節點**頁面上檢視連線狀態。

將 NSX Edge 新增為傳輸節點後，連線狀態會在 10-12 分鐘內變更為 [啟動]。

12 (選擇性) 使用 `GET https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 呼叫來檢視傳輸節點。

13 (選擇性) 如需狀態資訊，請使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 呼叫。

後續步驟

將 NSX Edge 節點新增至 NSX Edge 叢集。請參閱建立 NSX Edge 叢集。

建立 NSX Edge 叢集

擁有 NSX Edge 多節點叢集有助於確保永遠至少會有一個 NSX Edge 可供使用。

若要使用 NAT、負載平衡器等可設定狀態的服務建立第 0 層邏輯路由器或第 1 層路由器，您必須將其與 NSX Edge 叢集建立關聯。因此，即使您只有一個 NSX Edge，它仍必須屬於 NSX Edge 叢集才具有實用性。

NSX Edge 傳輸節點僅能新增至一個 NSX Edge 叢集。

NSX Edge 叢集可用來支援多個邏輯路由器。

建立 NSX Edge 叢集之後，您可以稍後進行編輯以新增其他 NSX Edge。

必要條件

- 至少安裝一個 NSX Edge 節點。
- 將 NSX Edge 加入管理平面。
- 新增 NSX Edge 作為傳輸節點。
- (選用) 建立 NSX Edge 叢集設定檔以實現高可用性 (HA)。您也可以使用預設 NSX Edge 叢集設定檔。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 節點 > Edge 叢集 > 新增**。
3. 為 NSX Edge 叢集輸入名稱。
4. 從下拉式功能表中選取 NSX Edge 叢集設定檔。
5. 從 [成員類型] 下拉式功能表中選取任一 NSX Edge 節點。

   如果虛擬機器部署在公用雲端環境中，請選取 [公用雲端閘道]；否則請選取 [NSX Edge 節點]。
6. 從**可用**資料行選取 NSX Edge，然後按一下向右箭頭，將它們移至**已選取**資料行。

後續步驟

現在，您可以建置邏輯網路拓撲並設定服務。請參閱《NSX-T Data Center 管理指南》。

自動部署無狀態叢集

9

無狀態主機不會持續保存組態，因此需要自動部署伺服器，在主機開啟電源時提供所需的啟動檔案。

本節可協助您使用 vSphere Auto Deploy 和 NSX-T 傳輸節點設定檔來設定無狀態叢集，以使用包含不同版本之 ESXi 和 NSX-T 的新映像設定檔來重新佈建主機。為 vSphere Auto Deploy 設定的主機，會使用自動部署伺服器和 vSphere 主機設定檔來自訂主機。您也可以為 NSX-T 傳輸節點設定檔設定這些主機，以在主機上設定 NSX-T。

因此，您可以為 vSphere Auto Deploy 和 NSX-T 傳輸節點設定檔設定無狀態主機，以重新佈建具有自訂 ESXi 和 NSX-T 版本的主機。

本章節討論下列主題：

- 自動部署無狀態叢集的高階工作
- 必要條件和支援的版本。
- 建立無狀態主機的自訂映像設定檔
- 將自訂映像與參考和目標主機建立關聯
- 設定參考主機上的網路組態
- 將參考主機設定為 NSX-T 中的傳輸節點
- 擷取並驗證主機設定檔
- 驗證主機設定檔與無狀態叢集的關聯
- 更新主機自訂
- 在目標主機上觸發自動部署
- 對主機設定檔和傳輸節點設定檔進行疑難排解

自動部署無狀態叢集的高階工作

用來自動部署無狀態叢集的高階工作。

用來設定自動部署無狀態叢集的高階工作包括：

1 必要條件和支援的版本。請參閱必要條件和支援的版本。。

2 (參考主機) 建立自訂映像設定檔。請參閱建立無狀態主機的自訂映像設定檔。

3 (參考和目標主機) 與自訂映像設定檔建立關聯。請參閱將自訂映像與參考和目標主機建立關聯。

4 (參考主機) 設定 ESXi 中的網路組態。請參閱設定參考主機上的網路組態。

5 (參考主機) 設定為 NSX 中的傳輸節點。請參閱將參考主機設定為 NSX-T 中的傳輸節點。

6 (參考主機) 擷取並驗證主機設定檔。請參閱擷取並驗證主機設定檔。

7 (參考和目標主機) 驗證主機設定檔與無狀態叢集的關聯。請參閱驗證主機設定檔與無狀態叢集的關聯。

8 (參考主機) 更新主機自訂。請參閱更新主機自訂。

9 (目標主機) 觸發自動部署。請參閱在目標主機上觸發自動部署。

   a 套用傳輸節點設定檔之前。請參閱在套用 TNP 前將主機重新開機。

   b 套用傳輸節點設定檔。請參閱在無狀態叢集上套用 TNP。

   c 套用傳輸節點設定檔之後。請參閱在套用 TNP 後將主機重新開機。

10 對主機設定檔和傳輸節點設定檔進行疑難排解。請參閱對主機設定檔和傳輸節點設定檔進行疑難排解。

必要條件和支援的版本。

必要條件和支援的 ESXi 與 NSX-T 版本。

支援的工作流程

- 使用映像設定檔和 HostProfile

必要條件

- 僅支援同質叢集 (叢集內的所有主機都必須是無狀態或可設定狀態)。
- 必須啟用映像產生器服務。
- 必須啟用自動部署服務。

支援的 NSX 和 ESXi 版本

支援的 EXSi 版本	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7
NSX-T Data Center 2.4	是	是	否	否
NSX-T Data Center 2.4.1	是	是	否	否
NSX-T Data Center 2.4.2	是	是	否	否
NSX-T Data Center 2.4.3	是	是	否	否
NSX-T Data Center 2.5	是	是	是	是

建立無狀態主機的自訂映像設定檔

在您的資料中心中，識別準備要作為參考主機的主機。

參考主機第一次啟動時， ESXi 會建立預設規則與參考主機的關聯。在此程序中，我們將新增自訂映像設定檔 (ESXi 和 NSX VIB)，並將參考主機與新的自訂映像建立關聯。具有 NSX-T 映像的映像設定檔可大幅縮短安裝時間。相同自訂映像會與無狀態叢集中的目標主機相關聯。

備註 或者，您可以只將 ESXi 映像設定檔新增至參考和目標無狀態叢集。當您將傳輸節點設定檔套用至無狀態叢集時，即會下載 NSX-T VIB。請參閱新增軟體存放庫。

必要條件

確定自動部署服務和映像產生器服務均已啟用。請參閱使用 vSphere Auto Deploy 重新佈建主機。

程序

1 若要匯入 NSX-T 套件，請建立軟體存放庫。

2 下載 `nsx-lcp` 套件。

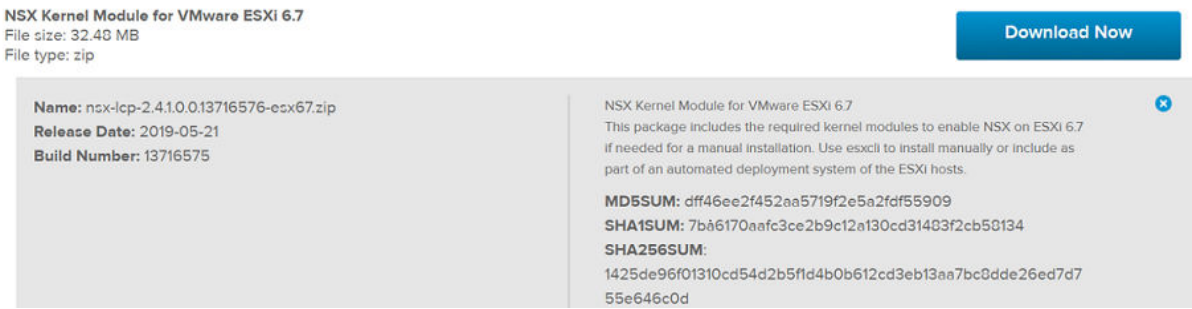
a 登入 `https://my.vmware.com`。

b 在 [下載 VMware NSX-T Data Center] 頁面上，選取 NSX-T 版本。

c 在 [產品下載] 頁面中，搜尋特定 VMware ESXi 版本的 NSX-T 核心模組。

d 按一下**立即下載**，以開始下載 `nsx-lcp` 套件。

e 將 `nsx-lcp` 套件匯入軟體存放庫中。



3 建立另一個軟體存放庫以匯入 ESXi 套件。

vSphere Web Client 會顯示在參考主機上建立的兩個存放庫。

4 建立自訂軟體存放庫，以複製先前匯入的 ESXi 映像和 `nsx-lcp` 套件。

a 從在先前的步驟中建立的 ESXi 軟體存放庫中，選取 ESXi 映像設定檔。

b 按一下**複製**。

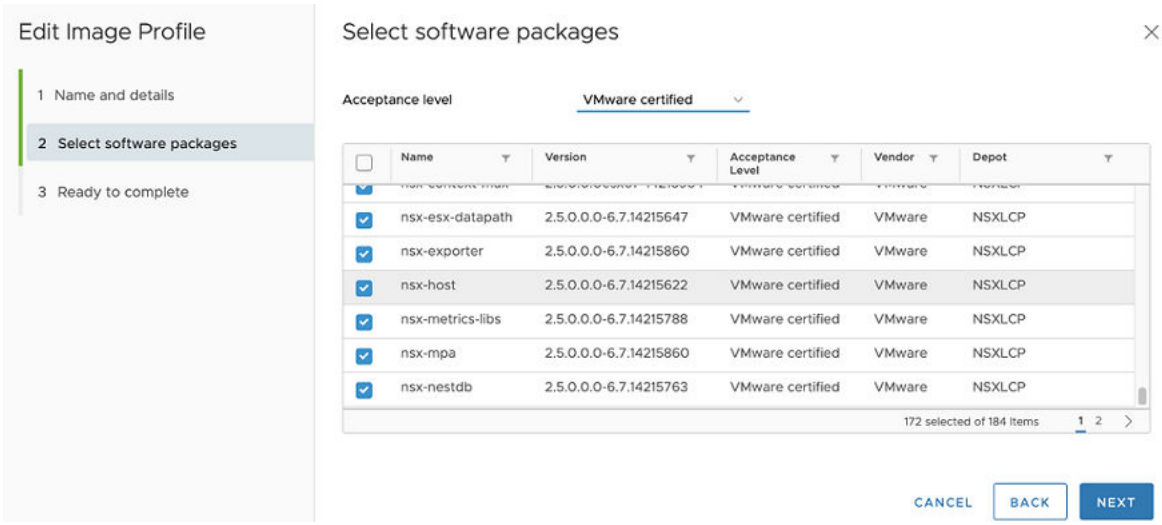
c 在 [複製映像設定檔] 精靈中，輸入要建立的自訂映像名稱。

d 選取必須有複製映像 (ESXi) 可供使用的自訂軟體存放庫。

e 在 [選取軟體套件] 視窗中，選取 **VMware 認證**作為接受層級。 ESXi VIB 已預先選取。

f 從套件清單中識別 NSX-T 套件並手動加以選取，然後按**下一步**。

g 在 [即將完成] 畫面中確認詳細資料，然後按一下**完成**，將包含 ESXi 和 NSX-T 套件的複製映像建立到自訂軟體存放庫中。



後續步驟

將自訂映像與參考和目標主機建立關聯。請參閱將自訂映像與參考和目標主機建立關聯。

將自訂映像與參考和目標主機建立關聯

若要使用包含 ESXi 和 NSX 套件的新自訂映像來啟動參考主機和目標主機，請建立自訂映像設定檔的關聯。

在此程序中，自訂映像只會與參考和目標主機產生關聯，但不會執行 NSX 安裝。

重要 請一併在參考和目標主機上執行此自訂映像關聯程序。

必要條件

程序

1 在 ESXi 主機上，導覽至**功能表 > 自動部署 > 已部署的主機**。

2 若要將自訂映像設定檔與主機建立關聯，請選取自訂映像。

3 按一下**編輯映像設定檔關聯**。

4 在 [編輯映像設定檔關聯] 精靈中，按一下**瀏覽**並選取自訂存放庫，然後選取自訂映像設定檔。

5 啟用**略過映像設定檔簽章檢查**。

6 按一下確定。

結果

後續步驟

設定參考主機上的網路組態。請參閱設定參考主機上的網路組態。

設定參考主機上的網路組態

在參考主機上，系統會建立具有 VMkernel 介面卡的標準交換器，以設定 ESXi 上的網路組態。

此網路組態會擷取到從參考主機擷取的主機設定檔中。在無狀態部署期間，主機設定檔會在每個目標主機上複寫此網路組態設定。

程序

1 在 ESXi 主機上，藉由新增 VMkernel 介面卡來設定 vSphere 標準交換器 (VSS) 或分散式虛擬交換器 (DVS)。

2 確認新增的 VSS/DVS 交換器顯示於 VMkernel 介面卡頁面中。

後續步驟

將參考主機設定為 NSX-T 中的傳輸節點。請參閱將參考主機設定為 NSX-T 中的傳輸節點。

將參考主機設定為 NSX-T 中的傳輸節點

在參考主機與自訂映像設定檔建立關聯，且已設定 VSS 交換器後，請將參考主機設定為 NSX-T 中的傳輸節點。

程序

1 從瀏覽器登入 NSX-T，網址為 https://<NSXManager_IPaddress>。

2 若要尋找參考主機，請導覽至**系統 -> 節點 -> 主機傳輸節點**。

3 建立 VLAN 傳輸區域，以定義虛擬網路的範圍。範圍可藉由將 N-VDS 交換器連結至傳輸區域來定義。N-VDS 可根據此連結存取在傳輸區域內定義的區段。請參閱建立傳輸區域。

4 在傳輸區域上建立 VLAN 區段。已建立的區段會顯示為邏輯交換器。

   a 導覽至**網路 -> 區段**。

   b 選取要連結區段的傳輸區域。

   c 輸入 VLAN 識別碼。

   d 按一下**儲存**。

5 為參考主機建立上行設定檔，以定義 N-VDS 連線至實體網路的方式。請參閱建立上行設定檔。

6 將參考主機設定為傳輸節點。請參閱設定受管理的主機傳輸節點。

   a 在 [主機傳輸節點] 頁面中，選取參考主機。

   b 按一下 [設定 NSX]，然後選取先前建立的傳輸區域、N-VDS 與上行設定檔。

7 在 [要安裝的網路對應] 區段中，按一下**新增對應**，將 VMkernel 新增至區段/邏輯交換器對應。

8 按一下**完成**以開始在參考主機上安裝 NSX-T。

在安裝期間，VMkernel 介面卡和實體 NIC 會從 VSS 或 DVS 交換器移轉至 N-VDS 交換器。安裝後，參考主機的組態狀態會顯示為成功。

備註 參考主機會列在 [其他主機] 下方。

9 在 vCenter Server 中，確認 VSS 交換器上的 PNIC 和 VMkernel 介面卡已移轉並連線至 N-VDS 交換器。

後續步驟

擷取並驗證主機設定檔。請參閱擷取並驗證主機設定檔。

擷取並驗證主機設定檔

從參考主機擷取主機設定檔後，請驗證在主機設定檔中擷取的 NSX-T 組態。其中包含套用至目標主機的 ESXi 和 NSX-T 組態。

程序

1 若要擷取主機設定檔，請從參考主機擷取並設定主機設定檔。

2 驗證所擷取主機設定檔中的 NSX 組態。

結果

主機設定檔中包含主機在進行 ESXi 和 NSX 環境的準備時的相關組態。

後續步驟

驗證主機設定檔與無狀態叢集的關聯。請參閱驗證主機設定檔與無狀態叢集的關聯。

驗證主機設定檔與無狀態叢集的關聯

若要使用 ESXi 和 NSX 組態準備目標無狀態叢集，請將從參考主機擷取的主機設定檔關聯至目標無狀態叢集。

如果沒有與無狀態叢集相關聯的主機設定檔，則無法使用 ESXi 和 NSX VIB 自動部署加入叢集的新節點。

程序

1. 將主機設定檔連結至無狀態叢集，或將其中斷連結。請參閱從主機設定檔連結或中斷連結實體。
2. 在 [已部署的主機] 索引標籤中，確認現有的無狀態主機已與正確的映像相關聯，並且與主機設定檔相關聯。
3. 如果主機設定檔關聯遺失，請選取目標主機，然後按一下 [修復主機關聯]，以強制將映像和主機設定檔更新至目標主機。

後續步驟

更新主機自訂。請參閱更新主機自訂。

更新主機自訂

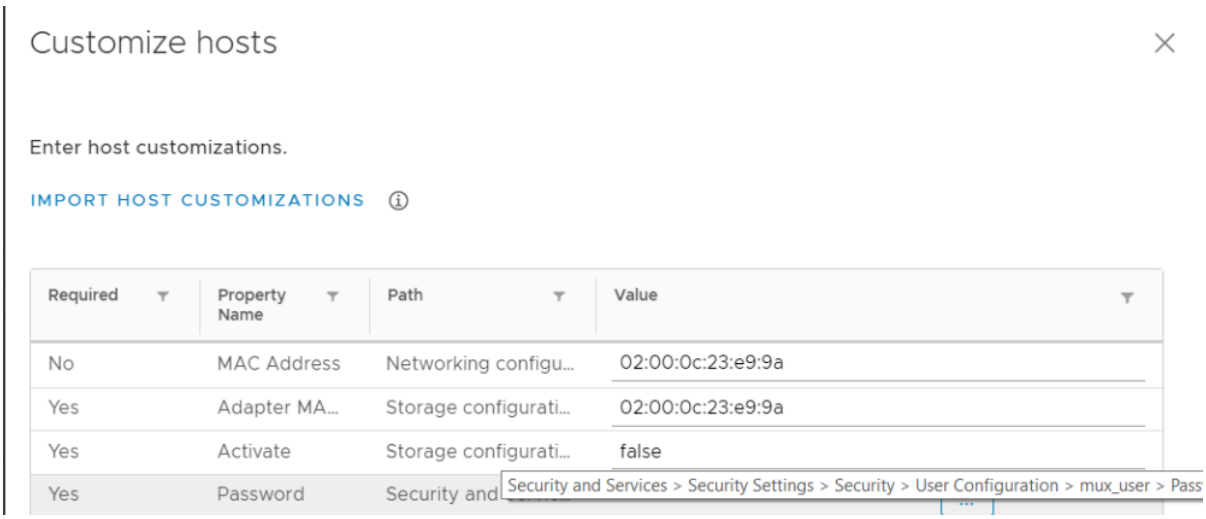
將主機設定檔連結至目標叢集後，主機上可能需要其他自訂項目，才能在該主機上成功自動部署 ESXi 和 NSX-T 套件。

程序

1 將主機設定檔附加到目標叢集後，如果主機未以自訂值進行更新，系統將會顯示下列訊息。

2 若要更新主機自訂，請導覽至主機設定檔，並按一下**動作 -> 編輯主機自訂**。

3 請輸入 ESXi 67ep6、67ep7、67u2 版的 MUX 使用者密碼。



4 確認所有必填欄位均已使用適當的值進行更新。

後續步驟

在目標主機上觸發自動部署。請參閱在目標主機上觸發自動部署。

在目標主機上觸發自動部署

在新節點新增至叢集時，必須手動將其重新開機，讓 ESXi 和 NSX-T VIB 進行設定。

備註 僅適用於無狀態主機。

有兩種方式可讓主機完成相關準備，以為要設定的 ESXi 和 NSX-T VIB 觸發自動部署。

- 在將 TNP 套用至無狀態叢集之前，將主機重新開機。
- 在將 TNP 套用至無狀態叢集之後，將主機重新開機。

如果您想要在主機安裝 NSX-T 時移轉 VMkernel 介面卡，請參閱：

- 無狀態主機位於目標叢集中的案例
- 無狀態主機位於目標叢集外時的案例

後續步驟

在將 TNP 套用至無狀態叢集之前，將主機重新開機。請參閱在套用 TNP 前將主機重新開機。

在套用 TNP 前將主機重新開機

僅適用於無狀態主機。在此案例中，傳輸節點設定檔不會套用至無狀態叢集，這表示不會在目標主機上安裝和設定 NSX-T。

程序

1 將主機重新開機。

目標主機會使用 ESXi 映像來啟動。啟動後，目標主機會持續處於維護模式，直到 TNP 設定檔套用至目標主機且 NSX-T 安裝完成。設定檔會依下列順序套用至主機：

設定檔會依下列順序套用至主機。

- 映像設定檔會套用至主機。
- 主機設定檔組態會套用至主機。
- NSX-T 組態會套用至主機。

2 在 ESXi 主機上，VMkernel 介面卡會連結至名為 <N-LogicalSegment> 的臨時區段，因為該主機還不是傳輸節點。NSX-T 安裝後，臨時交換器會取代為實際的 N-VDS 交換器和邏輯區段。

ESXi VIB 已套用至所有重新開機的主機。 ESXi 主機中有臨時 NSX 交換器。當 TNP 套用至主機時，臨時交換器就會取代為實際的 NSX-T 交換器。

後續步驟

將 TNP 套用至無狀態叢集。請參閱在無狀態叢集上套用 TNP。

在無狀態叢集上套用 TNP

只有在 TNP 套用至叢集時，才會在目標主機上執行 NSX-T 的組態和安裝。

程序

1 請記下從參考主機擷取到主機設定檔中的設定。TNP 設定檔中的對應實體必須具有相同的值。例如，主機設定檔和 TNP 中使用的 N-VDS 名稱必須相同。

如需關於已擷取主機設定檔設定的詳細資訊，請參閱擷取並驗證主機設定檔。

2 新增 TNP。請參閱新增傳輸節點設定檔。

3 確定新的 TNP 設定檔和現有主機設定檔上的下列參數具有相同的值。

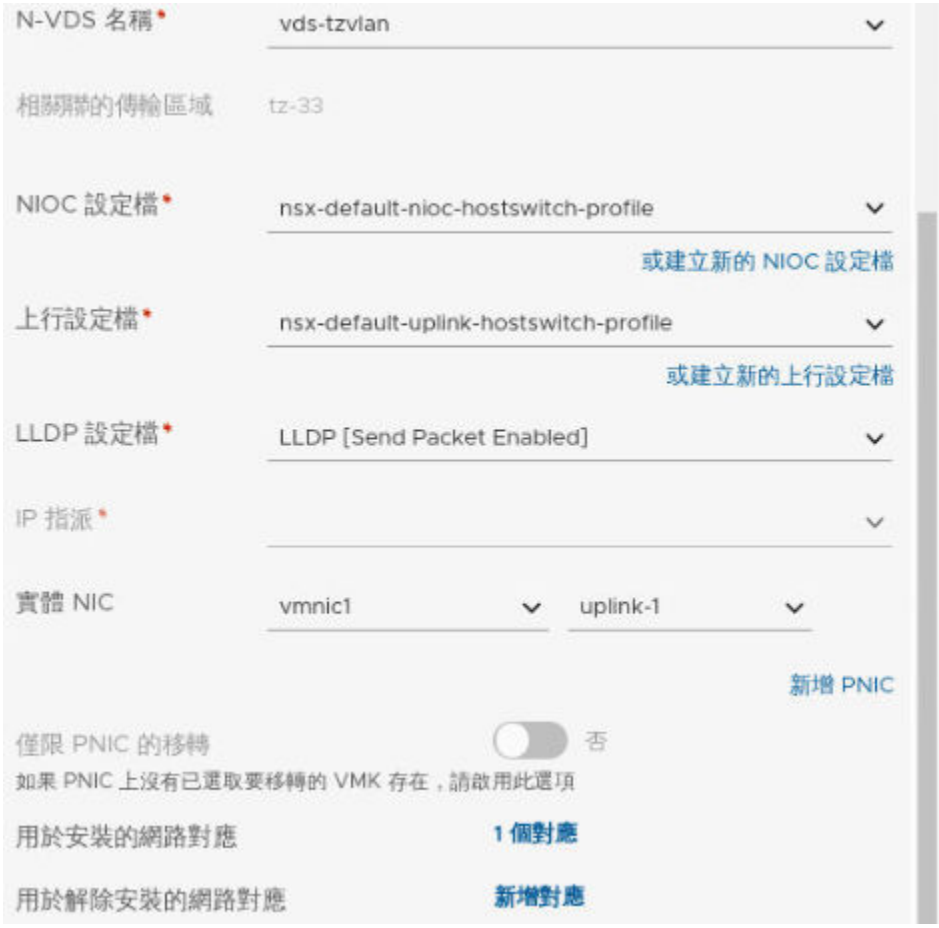
- N-VDS 名稱：確定主機設定檔和 TNP 中參考的 N-VDS 名稱是相同的。
- 上行設定檔：確定主機設定檔和 TNP 中參考的上行設定檔是相同的。
- PNIC：將實體 NIC 對應至上行設定檔時，請先確認主機設定檔中使用的 NIC，並將該實體 NIC 對應至上行設定檔。
- 用於安裝的網路對應：在安裝過程中對應網路時，請先在主機設定檔上確認 VMkernel 至區段的對應，並在 TNP 中新增相同的對應。
- 用於解除安裝的網路對應：在解除安裝過程中對應網路時，請先在主機設定檔上確認 VMkernel 至 VSS/DVS 交換器的對應，並在 TNP 中新增相同的對應。

4 輸入所有必填欄位以新增 TNP。請參閱新增傳輸節點設定檔。

確定新的 TNP 設定檔和現有主機設定檔上的下列參數具有相同的值。

- 傳輸區域：確定主機設定檔和 TNP 中參考的傳輸區域是相同的。
- N-VDS 名稱：確定主機設定檔和 TNP 中參考的 N-VDS 名稱是相同的。

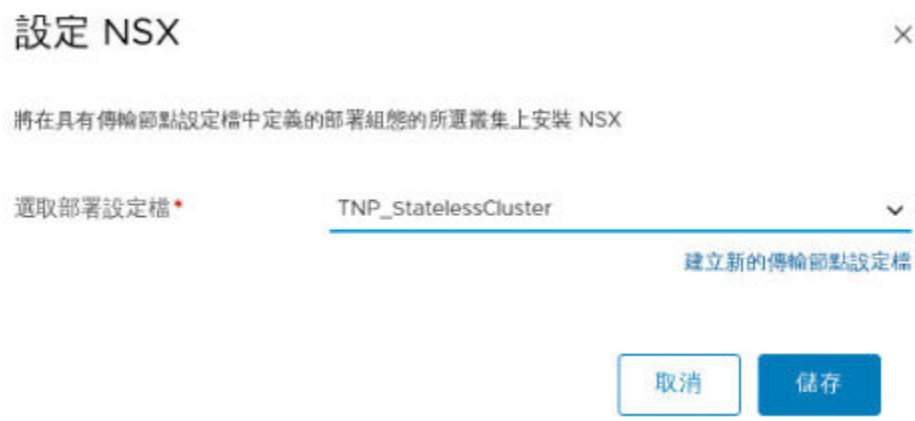
- 上行設定檔：確定主機設定檔和 TNP 中參考的上行設定檔是相同的。
- PNIC：將實體 NIC 對應至上行設定檔時，請先確認主機設定檔中使用的 NIC，並將該實體 NIC 對應至上行設定檔。
- 用於安裝的網路對應：在安裝過程中對應網路時，請先在主機設定檔上確認 VMkernel 至邏輯交換器的對應，並在 TNP 中新增相同的對應。
- 用於解除安裝的網路對應：在解除安裝過程中對應網路時，請先在主機設定檔上確認 VMkernel 至 VSS/DVS 交換器的對應，並在 TNP 中新增相同的對應。



在目標節點上套用 TNP 後，如果 TNP 組態與主機設定檔組態不相符，則節點可能會因為符合性錯誤而無法啟動。

5 確認 TNP 設定檔已成功建立。

6 將 TNP 設定檔套用至目標叢集，然後按一下**儲存**。



7 確認 TNP 設定檔已成功套用至目標叢集。這表示已在叢集中的所有節點上成功設定 NSX。

8 在 vSphere 中，確認實體 NIC 或 VMkernel 介面卡已連結至 N-VDS 交換器。

9 在 NSX 中，確認 ESXi 主機已成功設定為傳輸節點。

後續步驟

或者，您可以在 TNP 套用至叢集後，將目標主機重新開機。請參閱在套用 TNP 後將主機重新開機。

在套用 TNP 後將主機重新開機

僅適用於無狀態主機。在新節點新增至叢集時，請手動將節點重新開機，讓 ESXi 和 NSX-T 套件在節點上進行設定。

程序

1 將 TNP 套用至已備妥主機設定檔的無狀態叢集。請參閱在無狀態叢集上建立和套用 TNP。

2 將主機重新開機。

將 TNP 設定檔套用至無狀態叢集後，當您將任何加入該叢集的新節點重新開機時，該節點將會自動在主機上設定 NSX-T。

後續步驟

請務必將任何加入叢集的新節點重新開機，以在重新開機的節點上自動部署和設定 ESXi 和 NSX-T。

若要疑難排解設定自動部署時關於主機設定檔和傳輸節點設定檔的問題，請參閱對主機設定檔和傳輸節點設定檔進行疑難排解。

無狀態主機位於目標叢集中的案例

本節討論目標叢集中存在無狀態主機的使用案例。

重要 在無狀態目標主機上：

- 在 NSX-T 2.4 和 NSX-T 2.4.1 上，不支援將 vmk0 介面卡從 VSS/DVS 移轉至 N-VDS。
- 在 NSX-T 2.5 上，支援將 vmk0 介面卡從 VSS/DVS 移轉至 N-VDS。

目標主機	參考主機組態	自動部署目標主機的步驟
目標主機已設定 vmk0 介面卡。	從參考主機擷取的主機設定檔已在 N-VDS 交換器上設定 vmk0。 在 NSX-T 中，TNP 僅設定了 vmk0 移轉對應。	1 將主機設定檔連結至目標主機。 vmk0 介面卡會連結至 vSwitch。 2 必要時更新主機自訂。 3 將主機重新開機。主機設定檔會套用至主機。vmk0 會連結至臨時交換器。 4 套用 TNP。 vmk0 介面卡會移轉至 N-VDS。 目標主機已成功部署 ESXi 和 NSX-T VIB。
目標主機已設定 vmk0 介面卡。	從參考主機擷取的主機設定檔在 vSwitch 上有 vmk0，而 vmk1 則位於 N-VDS 交換器上。 在 NSX-T 中，TNP 僅設定了 vmk1 移轉對應。	1 將主機設定檔連結至目標主機。 Vmk0 介面卡會連結至 vSwitch，但 vmk1 未在任何交換器上實現。 2 更新主機自訂 (如有需要)。 3 將主機重新開機。 vmk0 會連結至 vSwitch，而 vmk1 會連結至臨時 NSX 交換器。 4 套用 TNP。 vmk1 介面卡會移轉至 N-VDS。 5 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 目標主機已成功部署 ESXi 和 NSX-T VIB。
目標主機已設定 vmk0 介面卡。	從參考主機擷取的主機設定檔已在 vSwitch 上設定 vmk0，而 vmk1 則設定於 N-VDS 交換器上。 在 NSX-T 中，TNP 已設定 vmk0 和 vmk1 移轉對應。	1 將主機設定檔連結至目標主機。 Vmk0 介面卡會連結至 vSwitch，但 vmk1 未在任何交換器上實現。 2 更新主機自訂 (如有需要)。 3 將主機重新開機。 vmk0 介面卡會連結至 vSwitch，而 vmk1 會連結至臨時 NSX 交換器。 4 套用 TNP。 5 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 目標主機已成功部署 ESXi 和 NSX-T VIB。

目標主機	參考主機組態	自動部署目標主機的步驟
目標主機已設定 vmk0 和 vmk1 介面卡。	從參考主機擷取的主機設定檔在 vSwitch 上有 vmk0，且已在 N-VDS 交換器上設定 vmk1。 在 NSX-T 中，TNP 已設定 vmk1 移轉對應。	1 將主機設定檔連結至目標主機。 Vmk0 和 vmk1 介面卡會連結至 vSwitch。 2 更新主機自訂 (如有需要)。 3 將主機重新開機。 4 套用 TNP。 vmk0 介面卡會連結至 vSwitch，而 vmk1 會連結至 N-VDS 交換器。 5 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 目標主機已成功部署 ESXi 和 NSX-T VIB。
目標主機已設定 vmk0 和 vmk1 介面卡。	從參考主機擷取的主機設定檔已在 N-VDS 交換器上設定 vmk0 和 vmk1。 在 NSX-T 中，TNP 已設定 vmk0 和 vmk1 移轉對應。	1 將主機設定檔連結至目標主機。 Vmk0 和 vmk1 介面卡會連結至 vSwitch。 2 更新主機自訂 (如有需要)。 3 將主機重新開機。 4 套用 TNP。 vmk0 和 vmk1 會移轉至 N-VDS 交換器。 目標主機已成功部署 ESXi 和 NSX-T VIB。

無狀態主機位於目標叢集外時的案例

本節討論無狀態主機存在於目標叢集外時的使用案例。

重要 在無狀態主機上：

- 在 NSX-T 2.4 和 NSX-T 2.4.1 上，不支援將 vmk0 介面卡從 VSS/DVS 移轉至 N-VDS。
- 在 NSX-T 2.5 上，支援將 vmk0 介面卡從 VSS/DVS 移轉至 N-VDS。

.

目標主機狀態	參考主機組態	自動部署目標主機的步驟
主機處於已關閉電源的狀態 (初次啟動時)。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 在叢集上套用 TNP。	從參考主機擷取的主機設定檔在 vSwitch 上有 VMkernel 介面卡 0 (vmk0)，且已在 N-VDS 交換器上設定 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 僅設定了 vmk1 移轉對應。	1 開啟主機電源。 在主機開啟電源後。 ■ 主機會新增至叢集。 ■ 主機設定檔會套用在目標主機上。 ■ vmk0 介面卡會位於 vSwitch 上，而 vmk1 介面卡會位於臨時交換器上。 ■ 會觸發 TNP。 ■ 將 TNP 套用至叢集後，vmk0 介面卡會位於 vSwitch 上，而 vmk1 會移轉至 N-VDS 交換器。 2 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 主機已成功部署 ESXi 和 NSX-T VIB。
主機處於已關閉電源的狀態 (初次啟動時)。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 在叢集上套用 TNP。	從參考主機擷取的主機設定檔已在 N-VDS 交換器上設定 VMkernel 介面卡 0 (vmk0) 和 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 已設定 vmk0 和 vmk1 移轉。	1 開啟主機電源。 在主機開啟電源後。 ■ 主機會新增至叢集。 ■ 主機設定檔會套用在目標主機上。 ■ vmk0 和 vmk1 介面卡會位於臨時交換器上。 ■ 會觸發 TNP。 ■ 將 TNP 套用至叢集後，vmk0 和 vmk1 會移轉至 N-VDS 交換器。 主機已成功部署 ESXi 和 NSX-T VIB。
主機處於已開啟電源的狀態。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 目標主機僅設定了 vmk0 介面卡。	從參考主機擷取的主機設定檔在 vSwitch 上有 VMkernel 介面卡 0 (vmk0)，且已在 N-VDS 交換器上設定 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 已設定 vmk1 移轉對應。	1 將主機移至叢集中。 2 將主機重新開機。 主機重新開機後，主機設定檔會套用在目標主機上。 ■ vmk0 介面卡會連結至 vSwitch，而 vmk1 介面卡會連結至臨時 NSX 交換器。 ■ 會觸發 TNP。 ■ vmk1 會移轉至 N-VDS 交換器。 3 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 主機已成功部署 ESXi 和 NSX-T VIB。
主機處於已開啟電源的狀態。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 目標主機僅設定了 vmk0 介面卡。	從參考主機擷取的主機設定檔已在 N-VDS 上設定 VMkernel 介面卡 0 (vmk0) 和 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 已設定 vmk0 和 vmk1 移轉。	1 將主機移至叢集中。 2 將主機重新開機。 將主機重新開機後，主機設定檔會套用至目標主機。 ■ vmk0 和 vmk1 介面卡會連結至臨時 NSX 交換器。 ■ 會觸發 TNP。 ■ vmk0 和 vmk1 會連結至 N-VDS 交換器。 主機已成功部署 ESXi 和 NSX-T VIB。

目標主機狀態	參考主機組態	自動部署目標主機的步驟
主機處於已開啟電源的狀態。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 目標主機已設定 vmk0 和 vmk1 網路對應。	從參考主機擷取的主機設定檔在 vSwitch 上有 VMkernel 介面卡 0 (vmk0)，且已在 N-VDS 交換器上設定 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 已設定 vmk1 移轉。	1 將主機移至叢集中。 2 將主機重新開機。 主機重新開機後，主機設定檔會套用在目標主機上。 ■ vmk0 介面卡會連結至 vSwitch，而 vmk1 介面卡會連結至臨時 NSX 交換器。 ■ 會觸發 TNP。 ■ vmk1 會移轉至 N-VDS 交換器。 3 (選用) 如果主機與主機設定檔仍不相容，請將主機重新開機，使主機合規。 主機已成功部署 ESXi 和 NSX-T VIB。
主機處於已開啟電源的狀態。它稍後會新增至叢集。 系統已為目標叢集設定預設自動部署規則，且規則已與主機設定檔相關聯。 主機已設定 vmk0 和 vmk1 網路對應。	在參考主機中，主機設定檔已在 N-VDS 交換器上設定 VMkernel 介面卡 0 (vmk0) 和 VMkernel 介面卡 1 (vmk1)。 在 NSX-T 中，TNP 已設定 vmk0 和 vmk1 移轉。	1 將主機移至叢集中。 2 將主機重新開機。 主機重新開機後，主機設定檔會套用在目標主機上。 ■ vmk0 和 vmk1 介面卡會連結至臨時 NSX 交換器。 ■ 會觸發 TNP。 ■ vmk0 和 vmk1 介面卡會移轉至 N-VDS 交換器。 主機已成功部署 ESXi 和 NSX-T VIB。

對主機設定檔和傳輸節點設定檔進行疑難排解

疑難排解主機設定檔和 TNP 用來自動部署無狀態叢集時的問題。

案例	說明
主機設定檔無法移轉。	問題：沒有任何 vCenter Server 可使用包含 NSX-T 組態的主機設定檔。 因應措施：無。
自動部署規則引擎	問題：在自動部署規則中無法使用主機設定檔來部署新叢集。如果部署了新叢集，則主機將會以基本網路進行部署，並維持處於維護模式。 因應措施：從 NSX-T GUI 準備每個叢集。請參閱在無狀態叢集上套用 TNP。
檢查符合性錯誤。	問題：主機設定檔修復無法修正與 NSX-T 組態有關的符合性錯誤。 ■ 在主機設定檔和 TNP 上設定的實體 NIC 不相同。 ■ vNIC 與 LS 對應之間的對應。主機設定檔發現 vNIC 對應的邏輯交換器與 TNP 設定檔不相符。 ■ 在主機設定檔和 TNP 上，已連線至 N-VDS 的 VMkernel 不相符。 ■ 主機設定檔和 TNP 上的不透明交換器不相符。 因應措施：確定主機設定檔與 TNP 上的 NSX-T 組態相符。請將主機重新開機以實現組態變更。主機會啟動。

案例	說明
修復	問題：如果有任何 NSX-T 特定的符合性錯誤，即會封鎖該叢集上的主機設定檔修復。 組態不正確： ■ vNIC 與 LS 對應之間的對應 ■ 實體 NIC 的對應 因應措施：確定主機設定檔與 TNP 上的 NSX-T 組態相符。請將主機重新開機以實現組態變更。主機會啟動。
連結	問題：在設定了 NSX-T 的叢集中，主機設定檔無法在主機層級連結。 因應措施：無。
中斷連結	問題：在設定了 NSX-T 的叢集內中斷連結和連結新的主機設定檔時不會移除 NSX-T 組態。即使叢集符合新連結的主機設定檔，仍會使用先前設定檔中的 NSX-T 組態。 因應措施：無。
更新	問題：如果使用者變更了叢集中的 NSX-T 組態，請擷取新的主機設定檔。請針對所有遺失的設定，手動更新主機設定檔。 因應措施：無。
主機層級傳輸節點組態	問題：anportsport 節點在自動部署後，以個別實體的形式運作。對該傳輸節點的任何更新都可能與 TNP 不相符。 因應措施：請更新叢集。獨立傳輸節點中的任何更新都無法持續保存其移轉規格。移轉可能會在重新開機後失敗。
無法套用主機設定檔，因為 mux_user 密碼原則和密碼未重設。	問題：僅發生在執行版本低於 vSphere 6.7 U3 的主機上。除非重設 **mux_user** 密碼，否則主機修復和主機上的主機設定檔應用程式可能會失敗。 因應措施：在 [原則和設定檔] 下方編輯主機設定檔，以修改 mux_user 密碼原則，並重設 **mux_user** 密碼。
選取要移轉至 NVDS 交換器的 VMkernel 介面卡不支援 PeerDNS 組態。	問題：如果選取要移轉至 NVDS 的 VMkernel 介面卡已啟用對等 DNS，則主機設定檔應用程式會失敗。 因應措施：在必須移轉至 NVDS 交換器的 VMkernel 介面卡上停用對等 DNS 設定，以編輯擷取的主機設定檔。或者，請確定您不會將已啟用對等 DNS 的 VMkernel 介面卡移轉至 NVDS 交換器。
VMkernel NIC 位址的 DHCP 位址未保留	問題：如果參考主機是可設定狀態的，則任何無狀態主機若使用了從可設定狀態之參考主機擷取的設定檔，都將無法保留其 VMkernel 管理 MAC 位址 (衍生自啟動 PXE 的 MAC)。這會導致 DHCP 定址問題。 因應措施：編輯可設定狀態主機的已擷取主機設定檔，並將**判斷如何決定 vmknic 的 MAC 位址**修改為**使用系統進行 PXE 啟動的 MAC 位址**。
vCenter 中的主機設定檔應用程式失敗可能會導致主機上的 NSX 組態錯誤。	問題：如果 vCenter 中的主機設定檔應用程式失敗，則 NSX 組態也可能會失敗。 因應措施：在 vCenter 中，確認已成功套用主機設定檔。請修正錯誤，然後再試一次。
無狀態 ESXi 主機不支援 LAG。	問題：在由 vCenter Server 或 NSX 管理的無狀態 ESXi 主機中，不支援在 NSX 中設定為 LAG 的上行設定檔。 因應措施：無。

從主機傳輸節點中解除安裝 NSX-T Data Center

10

從主機傳輸節點中解除安裝 NSX-T Data Center 的步驟，會根據主機類型及其設定方式而有所不同。

- 確認用於解除安裝的主機網路對應

  從 ESXi 主機上解除安裝 NSX-T Data Center 之前，請先確認您已設定適當的網路對應供解除安裝使用。如果 ESXi 主機將 VMkernel 介面連線至 N-VDS，則需要對應。

- 從 vSphere 叢集中解除安裝 NSX-T Data Center

  如果您已使用傳輸節點設定檔在 vSphere 叢集上安裝 NSX-T Data Center，則可以遵循這些指示，從叢集中的所有主機解除安裝 NSX-T Data Center。

- 從 vSphere 叢集中的主機上解除安裝 NSX-T Data Center

  您可以從 vCenter Server 所管理的單一主機上解除安裝 NSX-T Data Center。叢集中的其他主機不會受到影響。

- 從獨立主機中解除安裝 NSX-T Data Center

  您可以從獨立主機中解除安裝 NSX-T Data Center。獨立主機可以是 ESXi 或 KVM。

確認用於解除安裝的主機網路對應

從 ESXi 主機上解除安裝 NSX-T Data Center 之前，請先確認您已設定適當的網路對應供解除安裝使用。如果 ESXi 主機將 VMkernel 介面連線至 N-VDS，則需要對應。

解除安裝對應會決定在解除安裝後應於何處連接介面。目前有實體介面 (vmnicX) 和 VMkernel 介面 (vmkX) 的解除安裝對應。當您解除安裝時，VMkernel 介面會從其目前的連線移至解除安裝對應中指定的連接埠群組。如果解除安裝對應中包含實體介面，則實體介面會根據 VMkernel 介面的目的地連接埠群組，連線至適當的 vSphere 分散式交換器或 vSphere 標準交換器。

注意 如果實體介面或 VMkernel 介面連線至 N-VDS，則從 ESXi 主機解除安裝 NSX-T Data Center 的作業會中斷。如果主機或叢集參與了其他應用程式 (例如 vSAN)，則這些應用程式可能會受解除安裝所影響。

您可以在兩個位置設定用於解除安裝的網路對應。

- 在傳輸節點組態中 (適用於該主機)。
- 在傳輸節點設定檔組態中 (隨後可套用至叢集)。

  備註 您必須已設定計算管理程式，才能將傳輸節點設定檔套用至叢集。

如果已設定計算管理程式，則主機可同時具有傳輸節點組態和傳輸節點設定檔組態。若兩者都存在，傳輸節點組態將是作用中的組態。請確認用於解除安裝的網路對應已正確設定在作用中的組態上。

在此範例中，叢集 cluster-1 已套用傳輸節點設定檔 TNP-1。主機 tn-1 顯示「組態不相符」。出現此不相符的訊息時，表示已將不同的組態套用至 tn-1。在傳輸節點組態符合傳輸節點設定檔組態之前，這種不相符的狀況會持續存在。傳輸節點 tn-2 使用傳輸節點設定檔中的網路對應，而傳輸節點 tn-1 則使用其本身的組態。

必要條件

- 確認您已設定適當的連接埠群組供解除安裝對應使用。您必須使用 vSphere 分散式交換器暫時連接埠群組或 vSphere 標準交換器連接埠群組。
- 如果您想要在獨立 ESXi 主機的解除安裝對應中使用 vSphere 分散式交換器連接埠群組，請設定計算管理程式。請參閱新增計算管理程式。若未設定計算管理程式，則必須使用 vSphere 標準交換器連接埠群組。

程序

1 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。

2 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。

3 對於每個要解除安裝的主機，請確認在用於解除安裝的網路對應中，每個位於 N-VDS 上的 VMkernel 介面都有一個連接埠群組。新增任何遺漏的對應。

> **重要** 在用於解除安裝的網路對應中，連接埠群組必須是 vSphere 分散式交換器暫時連接埠群組或 vSphere 標準交換器連接埠群組。

   a 若要檢視 VMkernel 介面，請登入 vCenter Server，選取主機，然後按一下**設定 > VMkernel 介面卡**。

   b 如果傳輸節點組態為作用中的組態，請選取主機，然後按一下**編輯** (適用於獨立主機) 或**設定 NSX** (適用於受管理的主機)。按**下一步**，然後按一下**用於解除安裝的網路對應**。在 **VMKNic 對應**與**實體 NIC 對應**索引標籤中檢視對應。

   c 如果傳輸節點設定檔為作用中的組態，請在 **NSX 組態**資料行中，按一下叢集的傳輸節點設定檔名稱，然後按一下**編輯**。在 **N-VDS** 索引標籤上，按一下**用於解除安裝的網路對應**。在 **VMKNic 對應**與**實體 NIC 對應**索引標籤中檢視對應。

從 vSphere 叢集中解除安裝 NSX-T Data Center

如果您已使用傳輸節點設定檔在 vSphere 叢集上安裝 NSX-T Data Center，則可以遵循這些指示，從叢集中的所有主機解除安裝 NSX-T Data Center。

如需傳輸節點設定檔的詳細資訊，請參閱新增傳輸節點設定檔。

注意 如果實體介面或 VMkernel 介面連線至 N-VDS，則從 ESXi 主機解除安裝 NSX-T Data Center 的作業會中斷。如果主機或叢集參與了其他應用程式 (例如 vSAN)，則這些應用程式可能會受解除安裝所影響。

如果您尚未使用傳輸節點設定檔來安裝 NSX-T Data Center，或者您想要從部分叢集的主機中移除 NSX-T Data Center，請參閱從 vSphere 叢集中的主機上解除安裝 NSX-T Data Center。

備註 從叢集中移除主機時不會解除安裝 NSX-T Data Center。請遵循下列指示，從叢集的主機中解除安裝 NSX-T Data Center：從 vSphere 叢集中的主機上解除安裝 NSX-T Data Center。

必要條件

- 確認您要解除安裝的主機已設定網路解除安裝對應。請參閱確認用於解除安裝的主機網路對應。
- 確認您要解除安裝的主機在 vSphere 中處於維護模式。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。
3. 從**管理者**下拉式功能表中選取 [vCenter Server]。
4. 選取您想要解除安裝的叢集，然後按一下**移除 NSX**。
5. 確認 NSX-T Data Center 軟體已從主機中移除。
   a. 以根使用者身分登入主機的命令列介面。
   b. 執行此命令以檢查 NSX-T Data Center VIB

   ```
   esxcli software vib list | grep -E 'nsx|vsipfwlib'
   ```

   如果 NSX-T Data Center 軟體已成功移除，則不會列出 VIB。如果主機上仍有任何 NSX VIB，請連絡 VMware 支援。

從 vSphere 叢集中的主機上解除安裝 NSX-T Data Center

您可以從 vCenter Server 所管理的單一主機上解除安裝 NSX-T Data Center。叢集中的其他主機不會受到影響。

注意 如果實體介面或 VMkernel 介面連線至 N-VDS，則從 ESXi 主機解除安裝 NSX-T Data Center 的作業會中斷。如果主機或叢集參與了其他應用程式 (例如 vSAN)，則這些應用程式可能會受解除安裝所影響。

必要條件

- 確認您要解除安裝的主機已設定網路解除安裝對應。請參閱確認用於解除安裝的主機網路對應。
- 確認您要解除安裝的主機在 vSphere 中處於維護模式。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。
3. 從**管理者**下拉式功能表中選取 vCenter Server。
4. 如果叢集已套用傳輸節點設定檔，請選取叢集，然後按一下**動作 > 卸除 TN 設定檔**。

   如果叢集已套用傳輸節點設定檔，則叢集的 **NSX 組態**資料行會顯示設定檔名稱。
5. 選取主機，然後按一下**移除 NSX**。
6. 確認 NSX-T Data Center 軟體已從主機中移除。
   a. 以根使用者身分登入主機的命令列介面。
   b. 執行此命令以檢查 NSX-T Data Center VIB

   ```
   esxcli software vib list | grep -E 'nsx|vsipfwlib'
   ```

   如果 NSX-T Data Center 軟體已成功移除，則不會列出 VIB。如果主機上仍有任何 NSX VIB，請連絡 VMware 支援。
7. 如果叢集已套用傳輸節點設定檔，而您想要將其重新套用，請選取叢集，按一下**設定 NSX**，然後從**選取部署設定檔**下拉式功能表中選取設定檔。

從獨立主機中解除安裝 NSX-T Data Center

您可以從獨立主機中解除安裝 NSX-T Data Center。獨立主機可以是 ESXi 或 KVM。

注意　如果實體介面或 VMkernel 介面連線至 N-VDS，則從 ESXi 主機解除安裝 NSX-T Data Center 的作業會中斷。如果主機或叢集參與了其他應用程式 (例如 vSAN)，則這些應用程式可能會受解除安裝所影響。

必要條件

如果您要從獨立 ESXi 主機解除安裝 NSX-T Data Center，請確認下列設定：

- 確認您要解除安裝的主機已設定網路解除安裝對應。請參閱確認用於解除安裝的主機網路對應。
- 確認您要解除安裝的主機在 vSphere 中處於維護模式。

程序

1. 從瀏覽器以管理員權限登入 NSX Manager，網址為 https://<nsx-manager-ip-address>。
2. 選取**系統 > 網狀架構 > 節點 > 主機傳輸節點**。
3. 從**管理者**下拉式功能表中選取**無: 獨立主機**。

4 選取主機，然後按一下**刪除**。在顯示的確認對話方塊中，確定您已選取**解除安裝 NSX 元件**，並已取消選取**強制刪除**。按一下**刪除**。

NSX-T Data Center 軟體即會從主機中移除。移除所有 NSX-T Data Center 軟體可能需要花費 5 分鐘。

5 如果解除安裝失敗，請選取主機，然後再按一下**刪除**。在確認對話方塊中，取消選取**解除安裝 NSX 元件**，然後選取**強制刪除**。

主機傳輸節點已從管理平面中刪除，但主機可能仍安裝了 NSX-T Data Center 軟體。

6 確認 NSX-T Data Center 軟體已從主機中移除。

a 以根使用者身分登入主機的命令列介面。

b 請執行適當的命令以檢查 NSX-T Data Center 軟體套件。

表 10-1. 套件清單命令

主機作業系統	命令
ESXi	`esxcli software vib list | grep -E 'nsx|vsipfwlib'`
Red Hat Enterprise Linux 與 CentOS Linux	`rpm -qa | grep -E 'nsx|vsipfwlib'`
Ubuntu	`dpkg -l | grep -E 'nsx|vsipfwlib'`
SUSE Linux Enterprise Server	`zypper packages --installed-only | grep -E 'nsx|vsipfwlib'`

如果 NSX-T Data Center 軟體已成功移除，則不會列出任何套件。如果主機上仍有任何 NSX 軟體套件，請連絡 VMware 支援。

安裝 NSX Cloud 元件

11

NSX Cloud 提供單一虛擬管理介面以管理公有雲網路。

NSX Cloud 不瞭解提供者專屬網路不需要公有雲中的 Hypervisor 存取權。

它提供多項優點：

- 您可以使用與生產環境中相同的網路與安全性設定檔，開發和測試應用程式。
- 開發人員可以管理其應用程式，直到準備好進行部署。
- 透過災難復原，您可以從非計劃的中斷或安全威脅復原到公有雲。
- 如果在公有雲之間移轉工作負載，NSX Cloud 可確保類似安全性原則套用至工作負載虛擬機器，無論其新位置為何。

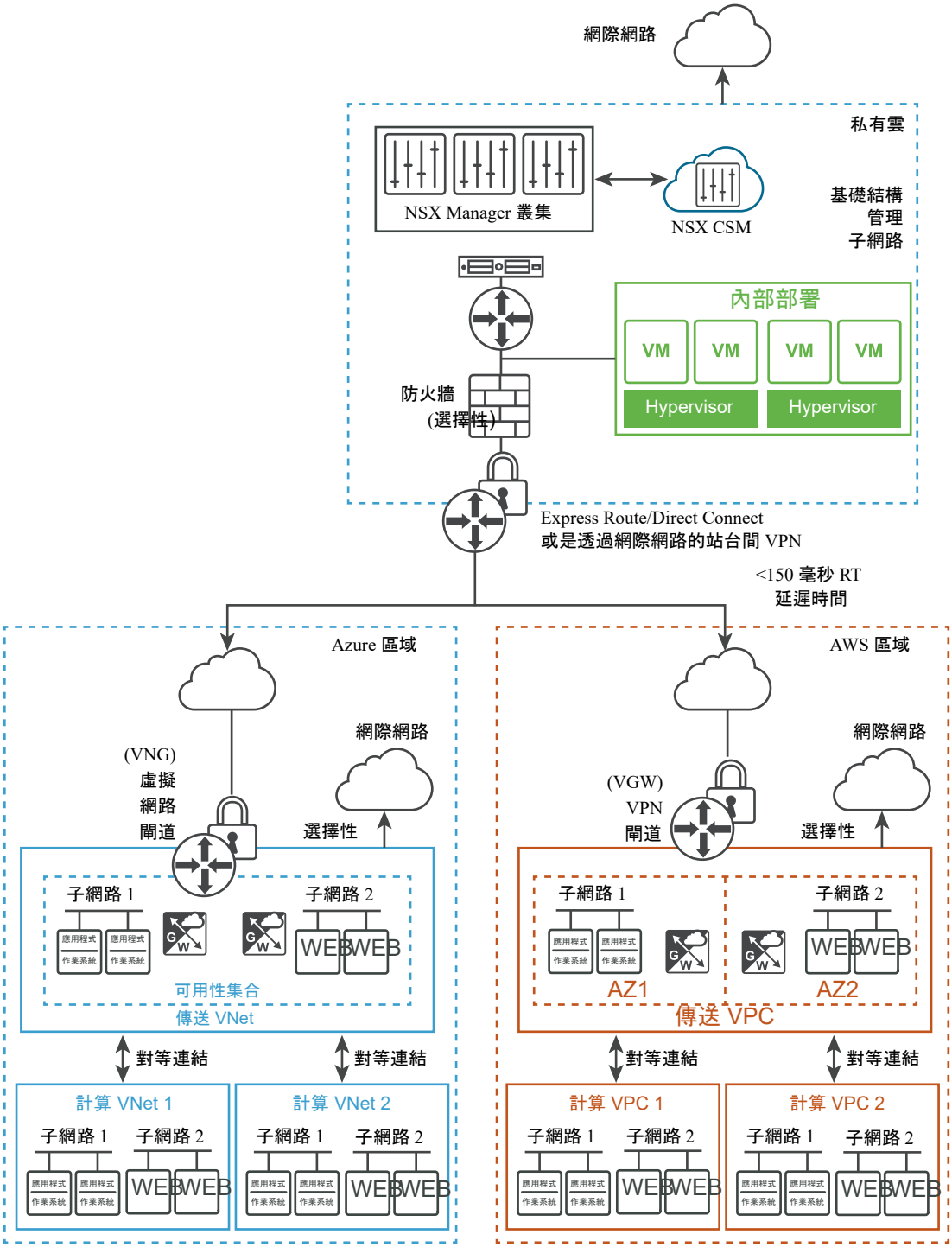
本章節討論下列主題：

- NSX Cloud 架構和元件
- 為公有雲安裝和設定 NSX Cloud 元件的概觀
- 安裝 CSM 並連線 NSX Manager
- 連線公有雲與內部部署
- 新增公有雲帳戶
- 部署或連結 NSX Public Cloud Gateway
- 取消部署 PCG

NSX Cloud 架構和元件

NSX Cloud 將 NSX-T Data Center 核心元件與公有雲整合，以在所有實作中提供網路與安全性。

圖 11-1. NSX Cloud 架構



核心元件

核心 NSX Cloud 元件如下：

- NSX Manager，用於已定義以原則為基礎的路由、角色型存取控制 (RBAC)、控制平面和執行階段狀態的管理平面。

- Cloud Service Manager (CSM)，用於整合 NSX Manager 以向管理平面提供公有雲的特定資訊。
- NSX Public Cloud Gateway (PCG)，用於連線到 NSX 管理和控制平面、NSX Edge 閘道服務，以及與公有雲實體進行以 API 為基礎的通訊。如需詳細資料，請參閱部署或連結 NSX Public Cloud Gateway。
- NSX 代理程式功能，針對工作負載虛擬機器提供 NSX 管理的資料路徑。

部署模式

NSX Public Cloud Gateway 可以是獨立閘道應用裝置或在公有雲 VPC 或 VNet 之間共用，來實現中樞和支點拓撲。

自行管理 VPC 或 VNet 充當傳送 VPC：在 VPC 或 VNet 中部署 PCG 時，它會將 VPC 或 VNet 限定為自行管理，也就是說，您可以將此 VPC 或 VNet 中主控的虛擬機器置於 NSX 管理之下。此 VPC 或 VNet 也有資格成為傳送 VPC 或 VNet，因為您可以使用其上已部署的 PCG 將其他 VPC 或 VNet 中主控的虛擬機器上線。

計算 VPC 或 VNet 連結至傳送 VPC 或 VNet：尚未部署 PCG 但連結至傳送 VPC 或 VNet 的 VPC 或 VNet 稱為計算 VPC 或 VNet。

為公有雲安裝和設定 NSX Cloud 元件的概觀

如需啟用 NSX-T Data Center 來管理公有雲中的工作負載虛擬機器所需步驟的概觀，請參閱檢查清單。

將 NSX Cloud 與公有雲連線的 0 天工作流程

此工作流程提供針對公有雲開始使用 NSX Cloud 所需步驟的概觀。

備註 在規劃部署時，請確定內部部署 NSX-T Data Center 應用裝置和公有雲上所部署的 PCG 之間有良好的連線。此外，傳送 VPC/VNet 必須位於與計算 VPC/VNet 相同的區域中。

表 11-1. 將 NSX Cloud 與公有雲連線的 0 天工作流程

工作	指示
❑ 安裝 CSM 並與 NSX Manager 連線。	請參閱安裝 CSM 並連線 NSX Manager。
❑ 在 CSM 中新增一或多個公有雲帳戶。	請參閱新增公有雲帳戶。
❑ 在傳送 VPC 或 VNet 中部署 PCG 並連結到您的計算 VPC 或 VNet。	請參閱部署或連結 NSX Public Cloud Gateway。
❑ 透過在公有雲中標記並在其上安裝 NSX 代理程式，將工作負載虛擬機器上線。	請依照《NSX-T Data Center 管理指南》中〈工作負載虛擬機器上線〉中的指示進行操作。

安裝 CSM 並連線 NSX Manager

使用安裝精靈連線 NSX Manager 與 CSM，並設定 Proxy 伺服器 (如有)。

安裝 CSM

Cloud Service Manager (CSM) 是 NSX Cloud 的重要元件。

安裝核心 NSX-T Data Center 元件後，安裝 CSM。

如需詳細指示，請參閱安裝 NSX Manager 和可用應用裝置。

備註 您需要在 NSX Manager 上啟用 FQDN 使用量 (DNS) 以安裝 NSX Cloud。請參閱發佈 NSX Manager 的 FQDN。

將 CSM 加入 NSX Manager

您必須將 CSM 應用裝置與 NSX Manager 連線，才能讓這些元件彼此通訊。

必要條件

- 必須安裝 NSX Manager，且您必須擁有管理員帳戶的使用者名稱和密碼，才能登入 NSX Manager。
- 必須安裝 CSM，且您必須擁有 CSM 中指派的企業管理員角色。

程序

1 在瀏覽器中，登入 CSM。

2 當安裝精靈中出現提示時，按一下**開始設定**。

3 在 [NSX Manager 認證] 畫面中，輸入下列詳細資料：

選項	說明
NSX Manager 主機名稱	輸入 NSX Manager 的完整網域名稱 (FQDN) (如果有)。您也可以輸入 NSX Manager 的 IP 位址。
管理員認證	輸入 NSX Manager 的企業管理員使用者名稱和密碼。
管理員指紋	(選擇性) 輸入 NSX Manager 的指紋值。如果您將此欄位保留空白，系統會識別指紋，並顯示在下一個畫面中。

4 (選擇性) 如果您未提供 NSX Manager 的指紋值，或者值不正確，則會顯示**驗證指紋**畫面。選取核取方塊以接受系統探索到的指紋。

5 按一下**連線**。

備註 如果安裝精靈中遺失此設定或您想要變更相關聯的 NSX Manager，請登入 CSM，按一下**系統 > 設定**，然後在標題為**相關聯的 NSX 節點**面板上按一下**設定**。

CSM 會確認 NSX Manager 指紋並建立連線。

6 (選擇性) 設定 Proxy 伺服器。請參閱 (選用) 設定 Proxy 伺服器中的指示。

(選用) 設定 Proxy 伺服器

如果您想要透過可靠的 HTTP Proxy 路由和監控所有網際網路繫結的 HTTP/HTTPS 流量，您可以在 CSM 中設定最多五個 Proxy 伺服器。

來自 PCG 和 CSM 的所有公有雲通訊會透過所選 Proxy 伺服器進行路由。

PCG 的 Proxy 設定獨立於 CSM 的 Proxy 設定。您可以選擇 PCG 沒有任何 Proxy 伺服器或具有不同的 Proxy 伺服器。

您可以選擇以下層級的驗證：

- 認證式驗證。
- 適用於 HTTPS 攔截的憑證式驗證。
- 無驗證。

程序

1 按一下**系統 > 設定**。然後，在標題為 **Proxy 伺服器**的面板上，按一下**設定**。

備註 若使用首次安裝 CSM 時可用的 CSM 安裝精靈，您也可以提供這些詳細資料。

2 在 [設定 Proxy 伺服器] 畫面中，輸入下列詳細資料：

選項	說明
預設值	使用此選項按鈕，表示預設 Proxy 伺服器。
設定檔名稱	提供 Proxy 伺服器設定檔名稱。這是強制性的。
Proxy 伺服器	輸入 Proxy 伺服器的 IP 位址。這是強制性的。
連接埠	輸入 Proxy 伺服器的連接埠。這是強制性的。
驗證	選擇性。如果您想要設定其他驗證，請選取此核取方塊，並提供有效的使用者名稱和密碼。
使用者名稱	如果您選取 [驗證] 核取方塊，這是必要的。
密碼	如果您選取 [驗證] 核取方塊，這是必要的。
憑證	選擇性。如果您想要提供適用於 HTTPS 攔截的驗證憑證，請選取此核取方塊，然後複製並貼上文字方塊中出現的憑證。
無 Proxy	如果您不想使用已設定的任何 Proxy 伺服器，請選取此選項。

(選用) 設定適用於 Cloud Service Manager 的 vIDM

如果您使用 VMware Identity Manager，則可以將其設定為從 NSX Manager 中存取 CSM。

程序

1 為 NSX Manager 和 CSM 設定 vIDM。請參閱《NSX-T Data Center 管理指南》的設定 VMware Identity Manager 整合中的指示。

2 對 NSX Manager 和 CSM 的 vIDM 使用者指派相同的角色，例如，對名為 **vIDM_admin** 的使用者指派**企業管理員**角色。您必須分別登入 NSX Manager 和 CSM，並對同一個使用者名稱指派相同的角色。如需詳細指示，請參閱《NSX-T Data Center 管理指南》中的新增角色指派或主體身分識別。

3 登入 NSX Manager。系統會將您重新導向至 vIDM 登入。

4 輸入 vIDM 使用者的認證。在登入後，您可以按一下 [應用程式] 圖示以在 NSX Manager 和 CSM 之間進行切換。

連線公有雲與內部部署

您必須使用適當的連線選項，將內部部署與公有雲帳戶或訂閱連線。

針對混合連線啟用對 CSM 上的連接埠和通訊協定的存取

開啟必要的網路連接埠，並允許 NSX Manager 上的所需通訊協定以啟用公有雲連線。

允許從公有雲存取 NSX Manager

開啟下列網路連接埠和通訊協定來允許與內部 NSX Manager 部署的連線：

表 11-2.

來源	目的地	通訊協定/連接埠	說明
PCG	NSX Manager	TCP/5671	針對管理平面通訊的從公有雲到內部部署 NSX-T Data Center 的輸入流量。
PCG	NSX Manager	TCP/8080	針對 HTTP 存放庫存取權的從公有雲到內部部署 NSX-T Data Center 的輸入流量，用於升級 NSX Cloud 元件。
PCG	NSX Controller	TCP/1234、TCP/1235	針對控制平面通訊的從公有雲到內部部署 NSX-T Data Center 的輸入流量。
PCG	DNS	UDP/53	從公有雲到內部部署 NSX-T Data Center DNS 的輸入流量 (如果您使用內部部署 DNS 伺服器)。
CSM	PCG	TCP/7442	CSM 組態推送

表 11-2. (續)

來源	目的地	通訊協定/連接埠	說明
任何	NSX Manager	TCP/443	NSX Manager UI
任何	CSM	TCP/443	CSM UI。

重要 所有 NSX-T Data Center 基礎結構通訊都利用基於 SSL 的加密。確保防火牆允許 SSL 流量透過非標準連接埠。

將 Microsoft Azure 網路與內部 NSX-T Data Center 部署連線

必須在 Microsoft Azure 網路和內部部署 NSX-T Data Center 應用裝置之間建立連線。

備註 您必須在內部部署中已安裝 NSX Manager，並將其與 CSM 連線。

概觀

- 將 Microsoft Azure 訂閱與內部部署 NSX-T Data Center 連線。
- 為 VNet 設定必要的 CIDR 區塊以及 NSX Cloud 所需的子網路。
- 將 CSM 應用裝置上的時間與 Microsoft Azure 儲存體伺服器或 NTP 同步。

將 Microsoft Azure 訂閱與內部部署 NSX-T Data Center 連線

每個公有雲都提供與內部部署連線的選項。您可以選擇符合您需求的任何可用連線選項。如需詳細資料，請參閱 Microsoft Azure 參考說明文件。

備註 您必須透過 Microsoft Azure 檢閱並實作適用的安全考量事項和最佳做法，例如所有存取 Microsoft Azure 入口網站或 API 的特殊權限使用者帳戶都應啟用多重要素驗證 (MFA)。MFA 可確保僅可讓合法的使用者存取入口網站，並降低了即使在認證遭竊或遺漏時進行存取的機率。如需詳細資訊和建議，請參考 Azure 資訊安全中心文件。

設定 VNet

在 Microsoft Azure 中，建立可路由 CIDR 區塊，並設定所需子網路。

- 一個建議範圍至少為 /28 的管理子網路，可處理：
  - 內部部署應用裝置的控制流量
  - 雲端提供者 API 端點的 API 流量
- 一個建議範圍為 /24 的下行子網路，適用於工作負載虛擬機器。
- 一或兩個建議範圍為 /24 的適用於 HA 的上行子網路，用於離開或進入 VNet 的南北向流量路由。

如需如何使用這些子網路的詳細資料，請參閱部署或連結 NSX Public Cloud Gateway。

將 Amazon Web Services (AWS) 網路與內部 NSX-T Data Center 部署連線

必須在 Amazon Web Services (AWS) 網路和內部部署 NSX-T Data Center 應用裝置之間建立連線。

備註 您必須在內部部署中已安裝 NSX Manager，並將其與 CSM 連線。

概觀

- 使用最符合您需求的任何可用選項，將 AWS 帳戶與內部部署 NSX Manager 應用裝置連線。
- 為 VPC 設定子網路以及 NSX Cloud 的其他需求。

將您的 AWS 帳戶與內部 NSX-T Data Center 部署連線。

每個公有雲都提供與內部部署連線的選項。您可以選擇符合您需求的任何可用連線選項。如需詳細資料，請參閱 AWS 參考說明文件。

備註 您必須透過 AWS 檢閱並實作適用的安全考量事項和最佳做法；請參閱 AWS 安全性最佳做法。

設定 VPC

您需要下列組態：

- 支援具有高可用性的 PCG 的六個子網路
- 網際網路閘道 (IGW)
- 私有和公有路由表
- 與路由表的子網路關聯
- 已啟用 DNS 解析與 DNS 主機名稱

請遵循下列準則設定 VPC：

1 假設您的 VPC 使用 /16 網路，請針對需要部署的每個閘道，設定三個子網路。

重要 如果使用高可用性，請在不同的可用性區域中設定三個其他子網路。

- **管理子網路**：此子網路用於內部部署 NSX-T Data Center 和 PCG 之間的管理流量。建議的範圍為 /28。
- **上行子網路**：此子網路用於南北向網際網路流量。建議的範圍為 /24。
- **下行子網路**：此子網路包含工作負載虛擬機器的 IP 位址範圍，應相應地調整規模。請記住，您可能需要納入工作負載虛擬機器上的其他介面以進行偵錯。

備註 由於在此 VPC 上部署 PCG 時需要選取子網路，請適當地標記子網路，例如 `management-subnet`、`uplink-subnet`、`downlink-subnet`。

如需詳細資料，請參閱部署或連結 NSX Public Cloud Gateway。

2 請確定您具有已連結到此 VPC 的網際網路閘道 (IGW)。

3 確保 VPC 的路由表將**目的地**設定為 **`0.0.0.0/0`**，而**目標**則為連結至 VPC 的 IGW。

4 請確保已針對此 VPC 啟用 DNS 解析和 DNS 主機名稱。

新增公有雲帳戶

若要新增公有雲端詳細目錄，您需要在公有雲中建立角色以允許 NSX Cloud 存取權，然後在 CSM 中新增所需資訊。

設定 Microsoft Azure 詳細目錄的安全存取權

為了讓 NSX Cloud 在您的訂閱中運作，請建立服務主體以授與所需權限，並根據 Microsoft Azure 功能建立 CSM 和 PCG 的角色以便管理 Azure 資源的身分識別。

備註 如果您已新增 AWS 帳戶至 CSM，請在 **NSX Manager > 網狀架構 > 設定檔 > 上行設定檔 > PCG-Uplink-HostSwitch-Profile** 中將 MTU 更新至 1500，然後新增 Microsoft Azure 帳戶。也可以使用 NSX Manager REST API 完成此操作。

概觀：

- 您的 Microsoft Azure 訂閱包含一或多個您想要置於 NSX-T Data Center 管理之下的 VNet。VNet 可能處於傳送模式或計算模式。在傳送 VNet 中會部署 PCG。您可以連結其他 VNet 至傳送 VNet，並將其中主控的工作負載虛擬機器上線。連結到傳送 VNet 的 VNet 稱為計算 VNet。
- NSX Cloud 提供 PowerShell 指令碼以產生服務主體和角色，該服務主體和角色使用 Microsoft Azure 的受管理身分識別功能來管理驗證，同時確保 Microsoft Azure 認證的安全。您也可以使用此指令碼在一個服務主體下包含多個訂閱。
- 您可以選擇針對所有訂閱重複使用服務主體，或視需要建立新的服務主體。另有一個額外指令碼可供您為其他訂閱建立單獨的服務主體。
- 若有多個訂閱，無論您針對所有訂閱使用單一服務主體，還是使用多個服務主體，都必須為 CSM 和 PCG 角色更新 JSON 檔案，以便在 *AssignableScopes* 區段下新增每個其他訂閱名稱。
- 如果 VNet 中已有 NSX Cloud 服務主體，可以再次執行指令碼並從參數中排除服務主體名稱來進行更新。
- Microsoft Azure Active Directory 的服務主體名稱必須是唯一的。您可以在相同 Active Directory 網域下的不同訂閱中使用相同的服務主體，也可以針對每個訂閱使用不同的服務主體。但是，您無法建立兩個名稱相同的服務主體。
- 您必須是擁有者或具有相應權限，才能在所有 Microsoft Azure 訂閱中建立和指派角色。
- 支援下列案例：
  - **案例 1**：您有一個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱。
  - **案例 2**：相同 Microsoft Azure 目錄下有多個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱，但想要在所有訂閱中使用一個 NSX Cloud 服務主體。

- **案例 3**：相同 Microsoft Azure 目錄下有多個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱，但想要對不同的訂閱使用不同的 NSX Cloud 服務主體。

以下是程序的概述：

1 使用 NSX Cloud PowerShell 指令碼：
   - 建立 NSX Cloud 的服務主體帳戶。
   - 為 CSM 建立角色。
   - 為 PCG 建立角色。
2 (選用) 針對您想要連結的其他訂閱建立服務主體。
3 在 CSM 中新增 Microsoft Azure 訂閱。

備註 如果使用多個訂閱，無論是使用相同或不同的服務主體，您都必須在 CSM 中單獨新增每個訂閱。

產生服務主體和角色

NSX Cloud 提供了 PowerShell 指令碼，可協助您針對一或多個訂閱產生所需的服務主體和角色。

必要條件

- 您必須具有已安裝 AzureRM 模組的 PowerShell 5.0+。
- 您必須是擁有者或具有相應權限，才能在所有 Microsoft Azure 訂閱中建立和指派角色。

備註 Microsoft Azure 的回應時間可能會導致首次執行指令碼時失敗。如果指令碼失敗，請嘗試再次執行。

程序

1 在 Windows 桌面或伺服器上，從 NSX-T Data Center **[下載] 頁面 > 驅動程式與工具 > NSX Cloud 指令碼 > Microsoft Azure**，下載名為 `CreateNSXCloudCredentials.zip` 的 ZIP 檔案。

2 在 Windows 系統中，解壓縮 ZIP 檔案的下列內容：

指令碼/檔案	說明
CreateNSXRoles.ps1	此 PowerShell 指令碼用以為 CSM 和 PCG 產生 NSX Cloud 服務主體和受管理身分識別角色。此指令碼採用下列參數： ■ `–subscriptionId <the Transit_VNet's_Azure_subscription_ID>` ■ (選用) `–servicePrincipalName <Service_Principal_Name>` ■ (選用) `–useOneServicePrincipal`
AddServicePrincipal.ps1	如果您想要新增多個訂閱並為每個訂閱指派不同的服務主體，就必須使用此選用指令碼。請參閱下列步驟中的**案例 3**。此指令碼採用下列參數： ■ `–computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>` ■ `–transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID>` ■ `–csmRoleName <CSM_Role_Name>` ■ `–servicePrincipalName <Service_Principal_Name>`
nsx_csm_role.json	CSM 角色名稱與權限的 JSON 範本。必須將此檔案做為 PowerShell 指令碼的輸入，且此檔案必須與指令碼位於相同的資料夾。
nsx_pcg_role.json	PCG 角色名稱與權限的 JSON 範本。必須將此檔案做為 PowerShell 指令碼的輸入，且此檔案必須與指令碼位於相同的資料夾。 **備註** 預設 PCG (閘道) 角色名稱為 `nsx-pcg-role`。在 CSM 中新增訂閱時，您必須提供此值。

3 **案例 1**：您有一個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱。

a 從 PowerShell 執行個體，移至下載 Microsoft Azure 指令碼和 JSON 檔案的目錄。

b 使用參數 -SubscriptionId 執行名為 CreateNSXRoles.ps1 的指令碼，如下所示：

```
.\CreateNSXRoles.ps1 –subscriptionId <the_single_Azure_subscription_ID>
```

備註 如果您想要覆寫 `nsx-service-admin` 的預設服務主體名稱，也可以使用參數 `-servicePrincipalName`。Microsoft Azure Active Directory 的服務主體名稱必須是唯一的。

4 **案例 2**：相同 Microsoft Azure 目錄下有多個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱，但想要在所有訂閱中使用一個 NSX Cloud 服務主體。

a 從 PowerShell 執行個體，移至下載 Microsoft Azure 指令碼和 JSON 檔案的目錄。

b 編輯每個 JSON 檔案，以便在標題為 「*AssignableScopes*」的區段下新增其他訂閱識別碼的清單，例如：

```
"AssignableScopes": [

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

備註 您必須使用此範例中顯示的格式來新增訂閱識別碼： `"/subscriptions/<Subscription_ID>"`

c 使用參數 `-subscriptionID` 與 `-useOneServicePrincipal` 執行名為 `CreateNSXRoles.ps1` 的指令碼：

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID> -
useOneServicePrincipal
```

備註 如果您想要使用預設名稱 `nsx-service-admin`，請省略此處的服務主體名稱。如果您的 Microsoft Azure Active Directory 中已存在該服務主體名稱，則在不指定服務主體名稱的情況下執行此指令碼會更新該服務主體。

5 **案例 3**：相同 Microsoft Azure 目錄下有多個要使用 NSX Cloud 啟用的 Microsoft Azure 訂閱，但想要對不同的訂閱使用不同的 NSX Cloud 服務主體。

a 從 PowerShell 執行個體，移至下載 Microsoft Azure 指令碼和 JSON 檔案的目錄。

b 依照第二個案例中的步驟 **b** 和 **c**，在每個 JSON 檔案中新增多個訂閱至 *AssignableScopes* 區段。

c 使用參數 -subscriptionID 執行名為 CreateNSXRoles.ps1 的指令碼：

```
.\CreateNSXRoles.ps1 –subscriptionId <One of the subscription_IDs>
```

備註 如果您想要使用預設名稱 nsx-service-admin，請省略此處的服務主體名稱。如果您的 Microsoft Azure Active Directory 中已存在該服務主體名稱，則在不指定服務主體名稱的情況下執行此指令碼會更新該服務主體。

d 使用下列參數執行名為 AddServicePrincipal.ps1 的指令碼：

參數	值
–computeSubscriptionId	Compute_VNet 的 Azure 訂閱識別碼
–transitSubscriptionId	傳送 VNet 的 Azure 訂閱識別碼
–csmRoleName	從 nsx_csm_role.JSON 檔案取得此值。
–servicePrincipalName	新的服務主體名稱

```
./AddServicePrincipal.ps1 –computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
 –transitSubscriptionId <the_Tranist_VNet's_Azure_Subscription_ID>
–csmRoleName <CSM_Role_Name>
–servicePrincipalName <new_Service_Principal_Name>”
```

6 尋找可執行 PowerShell 指令碼的相同目錄中的檔案。其名稱類似於：NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>。此檔案包含在 CSM 中新增 Microsoft Azure 訂閱所需的資訊。

- 用戶端識別碼
- 用戶端金鑰
- 承租人識別碼
- 訂閱識別碼

結果

將會建立下列建構：

- NSX Cloud 的 Azure AD 應用程式。
- NSX Cloud 應用程式的 Azure Resource Manager 服務主體。
- 連結至服務主體帳戶之 CSM 的角色。
- 使 PCG 能夠在公有雲詳細目錄上運作的角色。
- 在您執行 PowerShell 指令碼的相同目錄中，會建立名稱類似於 NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name> 的檔案。此檔案包含在 CSM 中新增 Microsoft Azure 訂閱所需的資訊。

備註 請參閱用於建立 CSM 和 PCG 角色的 JSON 檔案，以取得在角色建立後可供角色使用的權限清單。

後續步驟

在 CSM 中新增 Microsoft Azure 訂閱

備註 為多個訂閱啟用 NSX Cloud 時，您必須將每個單獨的訂閱分別新增至 CSM，例如，如果您總共有五個訂閱，則必須在 CSM 中新增五個 Microsoft Azure 帳戶，並且其他所有值相同但訂閱識別碼不同。

在 CSM 中新增 Microsoft Azure 訂閱

取得 NSX Cloud 服務主體以及 CSM 和 PCG 的詳細資料後，您便可以在 CSM 中新增 Microsoft Azure 訂閱。

必要條件

- 您必須具有 NSX-T Data Center 中的企業管理員角色。
- 您必須具有 PowerShell 指令碼的輸出以及 NSX Cloud 服務主體的詳細資料。
- 執行 PowerShell 指令碼以建立角色和服務主體時，您必須擁有 PCG 角色的值。預設值為 `nsx-pcg-role`。

程序

1 使用具有企業管理員角色的帳戶登入 CSM。

2 移至 **CSM > 雲端 > Azure**。

3 按一下 **+新增**，然後輸入下列詳細資料：

選項	說明
名稱	提供適當的名稱以識別 CSM 中的此帳戶。您可能有多個 Microsoft Azure 訂閱與相同的 Microsoft Azure 承租人識別碼相關聯。命名您的帳戶，然後可以在 CSM 中適當地命名它們，例如 Azure-DevOps-Account、Azure-Finance-Account 等。
用戶端識別碼	從 PowerShell 指令碼的輸出中複製並貼上此值。
金鑰	從 PowerShell 指令碼的輸出中複製並貼上此值。
訂閱識別碼	從 PowerShell 指令碼的輸出中複製並貼上此值。
承租人識別碼	從 PowerShell 指令碼的輸出中複製並貼上此值。
閘道角色名稱	預設值為 `nsx-pcg-role`。如果您已變更預設值，此值可以從 nsx_pcg_role.json 檔案取得。
雲端標籤	依預設，此選項已啟用並允許您的 Microsoft Azure 標記顯示在 NSX Manager 中

4 按一下**儲存**。

CSM 將新增帳戶，該帳戶會在三分鐘之內顯示在**帳戶**區段中。

後續步驟

在自行管理或傳送 VNet 中部署 PCG

設定 AWS 詳細目錄的安全存取權

您可能有一或多個 AWS 帳戶包含您想要置於 NSX-T Data Center 管理之下的 VPC 和工作負載虛擬機器。

概觀：

- 您可以使用傳送/計算 VPC 拓撲，在此拓撲中將 PCG 部署到一個 VPC，使其成為傳送 VPC，並與其連結其他 VPC (稱為計算 VPC)。
- NSX Cloud 提供可從 AWS 帳戶的 AWS CLI 執行的殼層指令檔，以建立 IAM 設定檔和角色，並建立傳送和計算 VPC 的信任關係。
- 支援下列案例：
  - **案例 1**：您想要使用具有 NSX Cloud 的單一 AWS 帳戶。
  - **案例 2**：您要使用 AWS 中由 AWS 主帳戶管理的多個子帳戶。
  - **案例 3**：您想要使用具有 NSX Cloud 的多個 AWS 帳戶。

以下是程序的概述：

1 使用需要 AWS CLI 的 NSX Cloud 殼層指令檔執行下列操作：
   - 建立 IAM 設定檔。
   - 為 PCG 建立角色。
   - (選用) 在主控傳送 VPC 的 AWS 帳戶和主控計算 VPC 的 AWS 帳戶之間建立信任關係。

2 在 CSM 中新增 AWS 帳戶。

產生 IAM 設定檔和 PCG 角色

NSX Cloud 提供殼層指令檔以透過產生 IAM 設定檔和連結至此設定檔的 PCG 角色 (為 AWS 帳戶提供必要的權限)，協助設定一或多個 AWS 帳戶。

如果計劃在兩個不同的 AWS 帳戶中主控連結至多個計算 VPC 的傳送 VPC，可以使用指令碼在這些帳戶之間建立信任關係。

備註 依預設，PCG (閘道) 角色名稱為 `nsx_pcg_service`。如果您想要針對閘道角色名稱使用不同的值，您可以在指令碼中進行變更，但是由於在 CSM 中新增 AWS 帳戶需要此項，因此請記下該值。

必要條件

您必須在 Linux 或相容系統上安裝和設定下列內容，然後再執行指令碼：

- AWS CLI
- `jq` (JSON 剖析器)
- `openssl`

備註 如果要使用多個 AWS 帳戶，必須使用合適的方法對這些帳戶進行對等。

程序

1 在 Linux 或相容的桌面或伺服器上，從 NSX-T Data Center**[下載] 頁面 > 驅動程式與工具 > NSX Cloud 指令碼 > AWS**，下載名為 `nsx_csm_iam_script.sh` 的殼層指令檔。

2 **案例 1**：您想要使用具有 NSX Cloud 的單一 AWS 帳戶。

a 執行指令碼，例如：

```
bash nsx_csm_iam_script.sh
```

b 當提示問題 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 時，輸入 `yes`

c 當系統詢問 `What do you want to name the IAM User?` 時，輸入 IAM 使用者的名稱

備註 在 AWS 帳戶中，IAM 使用者名稱必須是唯一的。

d 當系統詢問 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 時，輸入 `no`

當指令碼執行成功時，會在 AWS 帳戶中建立 IAM 設定檔與 PCG 的角色。這些值儲存於執行指令碼之相同目錄中名為 `aws_details.txt` 的輸出檔案。接下來，依照在 CSM 中新增 AWS 帳戶和在自行管理或傳送 VPC 中部署 PCG 中的指示完成設定傳送或自行管理 VPC 的程序。

3 **案例 2**：您要使用 AWS 中由一個 AWS 主帳戶管理的多個子帳戶。

a 從 AWS 主帳戶執行指令碼。

```
bash nsx_csm_iam_script.sh
```

b 當提示問題 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 時，輸入 `yes`

c 當系統詢問 `What do you want to name the IAM User?` 時，輸入 IAM 使用者的名稱

備註 在 AWS 帳戶中，IAM 使用者名稱必須是唯一的。

d 當系統詢問 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 時，輸入 `no`

備註 使用 AWS 主帳戶時，如果傳送 VPC 有權檢視子帳戶中的計算 VPC，則無需建立與子帳戶的信任關係。若非如此，請依照**案例 3** 的步驟來設定多個帳戶。

當指令碼執行成功時，會在 AWS 主帳戶中建立 IAM 設定檔與 PCG 的角色。這些值均儲存於執行指令碼之相同目錄中的輸出檔案。檔案名稱為 `aws_details.txt`。接下來，依照在 CSM 中新增 AWS 帳戶和在自行管理或傳送 VPC 中部署 PCG 中的指示完成設定傳送或自行管理 VPC 的程序。

4 **案例 3**：您想要使用具有 NSX Cloud 的多個 AWS 帳戶。

備註 確認 AWS 帳戶已對等，然後繼續操作。

a 請記下要主控傳送 VPC 的 12 位數的 AWS 帳戶號碼。

b 依照案例 1 中的步驟 a 到 d 來設定 AWS 帳戶中的傳送 VPC，然後完成在 CSM 中新增帳戶並在其中部署 PCG 的程序。

c 在您要主控計算 VPC 的其他 AWS 帳戶中，從 Linux 或相容系統下載並執行 NSX Cloud 指令碼。

備註 或者，您可以使用具有不同帳戶認證的 AWS 設定檔，以使用相同的系統為其他 AWS 帳戶再次執行該指令碼。

d 當系統詢問 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 時，輸入 `yes`

備註 如果您已將此 AWS 帳戶新增至 CSM，並且想要重複使用該指令碼連線到其他 AWS 帳戶，您可以輸入 `no` 並略過建立 IAM 使用者。

e 當系統詢問 `What do you want to name the IAM User?` 時，輸入 IAM 使用者的名稱

備註 在 AWS 帳戶中，IAM 使用者名稱必須是唯一的。

f 當系統詢問 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 時，輸入 `yes`

g 當系統詢問 `What is the Transit VPC account number?`，請輸入或複製並貼上您在步驟 1 中記下的 12 位數的 AWS 帳戶號碼。

即會在兩個 AWS 帳戶之間建立 IAM 信任關係，並由指令碼產生 ExternalID。

當指令碼執行成功時，會在 AWS 主帳戶中建立 IAM 設定檔與 PCG 的角色。這些值均儲存於執行指令碼之相同目錄中的輸出檔案。檔案名稱為 `aws_details.txt`。接下來，依照在 CSM 中新增 AWS 帳戶和連結至傳送 VPC 或 VNet 中的指示完成連結到傳送 VPC 的程序。

在 CSM 中新增 AWS 帳戶

使用指令碼產生的值新增 AWS 帳戶。

程序

1 使用企業管理員角色登入 CSM。

2 移至 **CSM > 雲端 > AWS**。

3 按一下 **+新增**，然後使用從 NSX Cloud 指令碼產生的輸出檔案 aws_details.txt 輸入下列詳細資料：

選項	說明
名稱	輸入此 AWS 帳戶的說明性名稱
存取金鑰	輸入您帳戶的存取金鑰

選項	說明
秘密金鑰	輸入您帳戶的秘密金鑰
雲端標籤	依預設，此選項已啟用並允許您的 AWS 標記顯示在 NSX Manager 中
閘道角色名稱	預設值為 `nsx_pcg_service`。您可以在檔案 aws_details.txt 中的指令碼輸出中找到此值。

結果

已在 CSM 中新增 AWS 帳戶。

在 CSM 的 [VPC] 索引標籤中，您可以檢視 AWS 帳戶中的所有 VPC。

在 CSM 的 [執行個體] 索引標籤中，您可以檢視此 VPC 中的 EC2 執行個體。

後續步驟

在自行管理或傳送 VPC 中部署 PCG

部署或連結 NSX Public Cloud Gateway

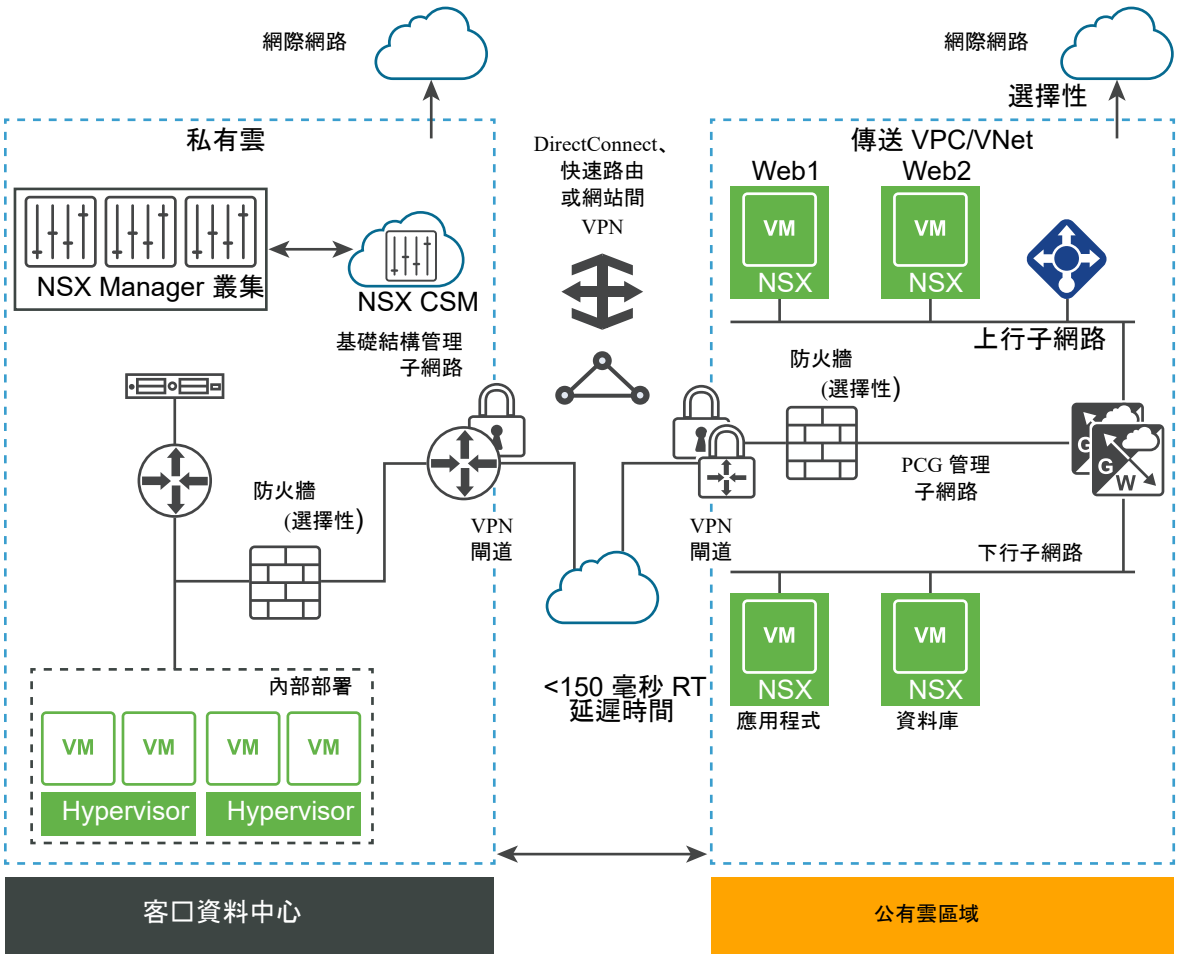
NSX Public Cloud Gateway (PCG) 會在公有雲和 NSX-T Data Center 的內部部署管理元件之間提供南北向連線。

PCG 可以是獨立閘道應用裝置或在公有雲 VPC 或 VNet 之間共用，來實現中樞和支點拓撲。

備註 會針對每個支援的公有雲，以單一預設大小部署 PCG：

公有雲	PCG 執行個體類型
AWS	C4.xlarge **備註** 某些區域可能不支援 C4.xlarge 執行個體類型。如需詳細資料，請參閱 AWS 說明文件。
Microsoft Azure	標準 DS3 v.2

圖 11-2. NSX Public Cloud Gateway 架構



傳送或自行管理 VPC 或 VNet：在 VPC 或 VNet 中部署 PCG 時，它會將 VPC 或 VNet 限定為自行管理，也就是說，您可以將此 VPC 或 VNet 中主控的虛擬機器置於 NSX 管理之下。此 VPC 或 VNet 也將限定為傳送 VPC 或 VNet，因為您可以使用其上已部署的 PCG 將其他 VPC 或 VNet 中主控的虛擬機器上線。PCG 會利用您在 VPC/VNet 中設定的下列子網路。請參閱將 Microsoft Azure 網路與內部 NSX-T Data Center 部署連線或將 Amazon Web Services (AWS) 網路與內部 NSX-T Data Center 部署連線。

- **管理子網路**：此子網路用於內部部署 NSX-T Data Center 和 PCG 之間的管理流量。建議的範圍為 /28。
- **上行子網路**：此子網路用於南北向網際網路流量。建議的範圍為 /24。
- **下行子網路**：此子網路包含工作負載虛擬機器的 IP 位址範圍，應相應地調整規模。請記住，您可能需要納入工作負載虛擬機器上的其他介面以進行偵錯。

計算 VPC 或 VNet：尚未部署 PCG 但連結至傳送 VPC 或 VNet 的 VPC 或 VNet 稱為計算 VPC 或 VNet。

PCG 部署與使用 NSX-T Data Center 元件之 FQDN 及可解析這些 FQDN 的 DNS 伺服器的網路定址方案保持一致。

備註 建議不要使用 IP 位址透過 PCG 將公有雲與 NSX-T Data Center 連線，但如果您選擇該選項，請勿變更您的 IP 位址。

在自行管理或傳送 VNet 中部署 PCG

請依照下列指示，在 Microsoft Azure VNet 訂閱中部署 PCG。

將會部署 PCG 的 VNet 可充當可供其他 VNet 連線的傳送 VNet (稱為計算 VNet)。此 VNet 也可以管理虛擬機器並充當自行管理的 VNet。

請依照下列指示部署 PCG。如果您想要連結至現有的傳送 VNet，請參閱連結至傳送 VPC 或 VNet 。

必要條件

- 公有雲帳戶必須已新增至 CSM。
- 將要部署 PCG 的 VNet 必須適當地調整所需子網路以實現高可用性：上行、下行和管理。

程序

1. 使用具有企業管理員角色的帳戶登入 CSM。
2. 按一下**雲端 > Azure**，然後移至 **VNet** 索引標籤。
3. 按一下您要部署 PCG 所在的 VNet。
4. 按一下**部署閘道**。**部署主要閘道**精靈隨即開啟。
5. 如需一般內容，請遵循下列準則：

選項	說明
SSH 公開金鑰	提供在部署 PCG 時可驗證的 SSH 公開金鑰。此為每個 PCG 部署的必要項。
相關聯的 VNet 上的隔離原則	當您首次部署 PCG 時，請保留此選項為預設**已停用**模式。在虛擬機器上線後，您可以變更此值。如需詳細資料，請參閱《NSX-T Data Center 管理指南》中的**管理隔離原則**。
本機儲存區帳戶	向 CSM 新增 Microsoft Azure 訂閱時，會向 CSM 提供 Microsoft Azure 儲存區帳戶的清單。從下拉式功能表中選取 [儲存區帳戶]。繼續部署 PCG 時，CSM 會將 PCG 的公開可用 VHD 複製到所選區域的此儲存區帳戶。 **備註** 如果 VHD 映像已針對先前的 PCG 部署複製到區域中的此儲存區帳戶，會從此位置使用該映像進行後續部署以減少整體部署時間。
VHD URL	如果您想要使用公用 VMware 存放庫中未提供的其他 PCG 映像，您可以在此輸入 PCG VHD 的 URL。VHD 必須存在於已建立此 VNet 的相同帳戶和區域中。 **備註** VHD 必須採用正確的 URL 格式。建議您使用 Microsoft Azure 中的**按一下以複製**選項。

選項	說明
Proxy 伺服器	選取要用於此 PCG 之網際網路繫結流量的 Proxy 伺服器。將在 CSM 中設定 Proxy 伺服器。您可以選取與 CSM 相同的 Proxy 伺服器 (如果有)、從 CSM 選取不同的 Proxy 伺服器，或選取**無 Proxy 伺服器**。 如需有關如何在 CSM 中設定 Proxy 伺服器的詳細資料，請參閱 (選用) 設定 Proxy 伺服器。
進階	進階 DNS 設定可讓您彈性地選取 DNS 伺服器以解析 NSX-T Data Center 管理元件。
透過公有雲提供者的 DHCP 取得	如果您想要使用 Microsoft Azure DNS 設定，請選取此選項。如果您未選擇任一選項進行覆寫，則此為預設 DNS 設定。
覆寫公有雲提供者的 DNS 伺服器	如果您想要手動提供一或多個 DNS 伺服器的 IP 位址，以解析 NSX-T Data Center 應用裝置以及此 VNet 中的工作負載虛擬機器，請選取此選項。
僅針對 NSX-T Data Center 應用裝置使用公有雲提供者的 DNS 伺服器	如果您想要使用 Microsoft Azure DNS 伺服器來解析 NSX-T Data Center 管理元件，請選取此選項。透過此設定，您可以使用兩個 DNS 伺服器：一個用於 PCG，解析 NSX-T Data Center 應用裝置；另一個用於 VNet，解析此 VNet 中的工作負載虛擬機器。

6 按**下一步**。

7 對於**子網路**，請遵循下列準則：

選項	說明
針對 NSX Cloud 閘道啟用 HA	選取此選項以啟用 High Availability。
子網路	選取此選項以啟用 High Availability。
管理 NIC 上的公用 IP	選取**配置新的 IP 位址**，以向管理 NIC 提供公用 IP 位址。如果您想要重複使用可用的公用 IP 位址，您可以手動提供此公用 IP 位址。
上行 NIC 上的公用 IP	選取**配置新的 IP 位址**，以向上行 NIC 提供公用 IP 位址。如果您想要重複使用可用的公用 IP 位址，您可以手動提供此公用 IP 位址。

後續步驟

將工作負載虛擬機器上線。如需 N 天工作流程，請參閱《NSX-T Data Center 管理指南》中的**工作負載虛擬機器上線及管理**。

在自行管理或傳送 VPC 中部署 PCG

請依照下列指示，在 AWS VPC 中部署 PCG。

將會部署 PCG 的 VPC 可充當可供其他 VPC 連線的傳送 VPC (稱為計算 VPC)。此 VPC 也可以管理虛擬機器並充當自行管理的 VPC。

請依照下列指示部署 PCG。如果您想要連結至現有的傳送 VPC，請參閱連結至傳送 VPC 或 VNet 。

必要條件

- 公有雲帳戶必須已新增至 CSM。
- 將要部署 PCG 的 VPC 必須適當地調整所需子網路以實現高可用性：上行、下行和管理。

- VPC 的網路 ACL 組態必須包含 ALLOW 輸入規則。

程序

1 使用具有企業管理員角色的帳戶登入 CSM。

2 按一下**雲端 > AWS > <AWS_account_name>**，然後移至 **VPC** 索引標籤。

3 在 **VPC** 索引標籤中，選取 AWS 區域名稱，例如 `us-west`。AWS 區域必須是已建立運算 VPC 的相同區域。

4 選取針對 NSX Cloud 設定的運算 VPC。

5 按一下部署閘道。

6 完成一般閘道詳細資料：

選項	說明
PEM 檔案	從下拉式功能表中，選取其中一個 PEM 檔案。此檔案必須位於已部署 NSX Cloud 和已建立運算 VPC 的相同區域中。 這將唯一識別您的 AWS 帳戶。
相關聯的 VPC 上的隔離原則	當您首次部署 PCG 時，請保留此選項為預設**已停用**模式。在虛擬機器上線後，您可以變更此值。如需詳細資料，請參閱《NSX-T Data Center 管理指南》中的**管理隔離原則**。
Proxy 伺服器	選取要用於此 PCG 之網際網路繫結流量的 Proxy 伺服器。將在 CSM 中設定 Proxy 伺服器。您可以選取與 CSM 相同的 Proxy 伺服器 (如果有)、從 CSM 選取不同的 Proxy 伺服器，或選取**無 Proxy 伺服器**。 如需有關如何在 CSM 中設定 Proxy 伺服器的詳細資料，請參閱 (選用) 設定 Proxy 伺服器。
進階	如有需要，進階設定會提供額外選項。
覆寫 AMI 識別碼	使用此進階功能，為 PCG 提供與 AWS 帳戶中的可用 AMI 識別碼不同的 AMI 識別碼。
透過公有雲提供者的 DHCP 取得	如果您想要使用 AWS 設定，請選取此選項。如果您未選擇任一選項進行覆寫，則此為預設 DNS 設定。
覆寫公有雲提供者的 DNS 伺服器	如果您想要手動提供一或多個 DNS 伺服器的 IP 位址，以解析 NSX-T Data Center 應用裝置以及此 VPC 中的工作負載虛擬機器，請選取此選項。
僅針對 NSX-T Data Center 應用裝置使用公有雲提供者的 DNS 伺服器	如果您想要使用 AWS DNS 伺服器來解析 NSX-T Data Center 管理元件，請選取此選項。透過此設定，您可以使用兩個 DNS 伺服器：一個用於 PCG，解析 NSX-T Data Center 應用裝置；另一個用於 VPC，解析此 VPC 中的工作負載虛擬機器。

7 按下一步。

8 完成子網路詳細資料。

選項	說明
針對公用雲端閘道啟用 HA	建議的設定為 [啟用]，用於設定高可用性主動/待命配對，以避免未排程的停機時間。
主要閘道設定	從下拉式功能表中，選取一個可用性區域 (例如 `us-west-1a`) 做為 HA 的主要閘道。 從下拉式功能表中，指派上行、下行和管理子網路。
次要閘道設定	從下拉式功能表中，選取另一個可用性區域 (例如 `us-west-1b`) 做為 HA 的次要閘道。 當主要閘道失敗時，會使用次要閘道。 從下拉式功能表中，指派上行、下行和管理子網路。
管理 NIC 上的公用 IP	選取**配置新的 IP 位址**，以向管理 NIC 提供公用 IP 位址。如果您想要重複使用可用的公用 IP 位址，您可以手動提供此公用 IP 位址。
上行 NIC 上的公用 IP	選取**配置新的 IP 位址**，以向上行 NIC 提供公用 IP 位址。如果您想要重複使用可用的公用 IP 位址，您可以手動提供此公用 IP 位址。

按一下部署。

9 監控主要 (和次要，如果已選取) PCG 部署的狀態。此程序可能需要 10-12 分鐘。

10 成功部署 PCG 後，按一下完成。

後續步驟

將工作負載虛擬機器上線。如需 N 天工作流程，請參閱《NSX-T Data Center 管理指南》中的**工作負載虛擬機器上線及管理**。

連結至傳送 VPC 或 VNet

您可以將一或多個計算 VPC 或 VNet 連結至傳送 VPC 或 VNet。

必要條件

- 確認您擁有一個 PCG 處於**開啟**狀態的傳送 VPC 或 VNet。
- 確認您想要連結的 VPC/VNet 已透過 VPN 或對等連線到傳送 VPC 或 VNet。
- 確認傳送 VPC/VNet 位於與計算 VPC/VNet 相同的區域中。

備註 在以路由為基礎的 IPSec VPN 組態中，您必須指定虛擬通道介面 (VTI) 連接埠的 IP 位址。此 IP 必須位於與工作負載虛擬機器不同的子網路。這會防止將工作負載虛擬機器的輸入流量導向至 VTI 連接埠，因此將它捨棄。

備註 在公有雲中，每個安全群組的輸入/輸出規則數有預設限制，而且 NSX Cloud 會建立預設的安全群組。這會影響可以連結至傳送 VPC/VNet 的計算 VPC/VNet 數目。假設每個 VPC/VNet 有 1 個 CIDR 區塊，則 NSX Cloud 會在每個傳送 VPC/VNet 中支援 10 個計算 VPC/VNet。如果任何計算 VPC/VNet 中有超過 1 個的 CIDR，則每個傳送 VPC/VNet 所支援的計算 VPC/VNet 數目會減少。您可以與公有雲提供者連絡，來調整預設限制。

程序

1 使用具有企業管理員角色的帳戶登入 CSM。

2 按一下**雲端 > AWS/Azure > <public cloud_account_name>**，然後前往 **VPC/VNet** 索引標籤。

3 在 **VPC** 或 **VNet** 索引標籤中，選取您要主控一或多個計算 VPC 或 VNet 的區域名稱。

4 選取針對 NSX Cloud 設定的計算 VPC 或 VNet。

5 按一下**連結至傳送 VPC** 或**連結至傳送 VNET**

6 完成**連結傳送 VPC 或 VNet** 視窗中的選項：

選項	說明
傳送 VPC 或 VNet	從下拉式功能表中選取傳送 VPC 或 VNet。您選取的傳送 VPC 或 VNet 必須已透過 VPN 或對等方式與此 VPC 相連結。 **備註** 如果連線到傳送 VNet，您必須在此 VNet 中設定 DNS 轉寄站。如需詳細資訊，請參閱 Microsoft Azure 說明文件。
預設隔離原則	當您首次部署 PCG 時，請保留此選項為預設**已停用**模式。在虛擬機器上線後，您可以變更此值。如需詳細資料，請參閱《NSX-T Data Center 管理指南》中的**管理隔離原則**。

後續步驟

將工作負載虛擬機器上線。如需 N 天工作流程，請參閱《NSX-T Data Center 管理指南》中的**工作負載虛擬機器上線及管理**。

自動建立的邏輯實體和雲端原生安全群組

在傳送 VPC/VNet 中部署 PCG 並與其連結計算 VPC/VNet 會觸發 NSX-T Data Center 和公有雲中的必要組態。

自動建立的 NSX-T 邏輯實體

在 NSX-T Data Center 中，會建立一組邏輯實體。

重要 請勿刪除任何這些自動建立的實體。

系統實體

您可以在**系統**下查看以下實體：

表 11-3. 自動建立的系統實體

邏輯系統實體	已建立數目	命名	範圍
傳輸區域	為每個傳送 VPC/VNet 建立兩個傳輸區域	■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN	範圍：全域
Edge 傳輸節點	為每個部署的 PCG 建立一個 Edge 傳輸節點，如果在高可用性模式下部署，則建立兩個 Edge 傳輸節點。	■ PublicCloudGatewayTN-<VPC/VNET-ID> ■ PublicCloudGatewayTN-<VPC/VNET-ID>- 慣用	範圍：全域
Edge 叢集	針對部署的 PCG (無論是一個還是高可用性配對) 建立一個 Edge 叢集。	PCG-cluster-<VPC/VNet-ID>	範圍：全域

詳細目錄項目

詳細目錄下會建立下列實體：

表 11-4. 自動建立的詳細目錄項目

邏輯詳細目錄實體	已建立數目	命名	範圍
網域 **備註** **網域**物件是 NSX-T Data Center 2.4 中的實驗性功能，並且自動建立的網域會在使用者介面中顯示。但是，網域不再於 NSX-T Data Center 2.4.1 使用者介面中顯示。	每個傳送 VPC/VNet 一個	cloud-<Transit VPC/VNet-ID>	範圍：在所有 PCG 之間共用
群組	**預設**網域下的兩個群組 **備註** 在 NSX-T Data Center 中，您可以看到預設網域。但在 NSX-T Data Center 2.4.1 中，網域物件不會顯示。	■ cloud-default-route ■ cloud-metadata services	範圍：在所有 PCG 之間共用
群組	一個群組 在傳送 VPC/VNet 層級建立做為在計算 VPC/VNet 層級建立的個別區段的父系群組。	cloud-<Transit VPC/VNet ID>-all-segments	範圍：在所有計算 VPC/VNet 之間共用
群組	兩個群組： ■ 計算 VPC/VNet 之所有 CIDR 的網路 CIDR 群組 ■ 計算 VPC/VNet 內的所有受管理區段的本機區段群組	■ cloud-<Compute VPC/VNet ID>-cidr ■ cloud-<Compute VPC/VNet ID>-local-segments	範圍：在所有計算 VPC/VNet 之間共用

安全實體

表 11-5. 自動建立的安全性實體

邏輯安全實體	已建立數目	命名	範圍
Distributed Firewall (東西向)	每個傳送 VPC/VNet 兩個： ■ 無狀態 ■ 可設定狀態	■ cloud-stateless-<VPC/VNet ID> ■ cloud-stateful-<VPC/VNet ID>	■ 可設定狀態規則，允許本機受管理區段內的流量 ■ 可設定狀態規則，拒絕來自未受管理的虛擬機器的流量
閘道防火牆 (南北向)	每個傳送 VPC/VNet 一個	cloud-<Transit VPC/VNet ID>	

網路實體

在上線的不同階段中建立下列實體：

圖 11-3. 部署 PCG 後自動建立的 NSX-T Data Center 網路實體

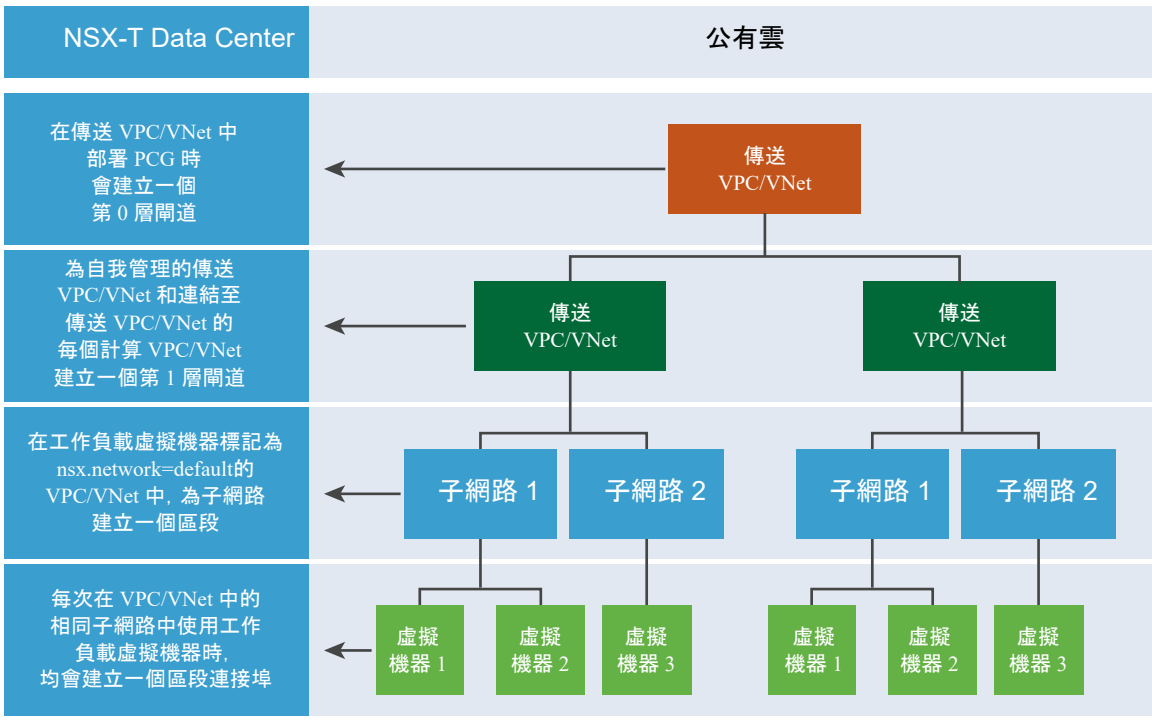


表 11-6. 自動建立的網路實體

上線工作	NSX-T Data Center 內建立的邏輯實體
傳送 VPC/VNet 上部署的 PCG	■ 第 0 層閘道 ■ 基礎結構區段 (預設 VLAN 交換器) ■ 第 1 層路由器
連結到傳送 VPC/VNet 的計算 VPC 或 VNet	■ 第 1 層路由器

表 11-6. 自動建立的網路實體 (續)

上線工作	NSX-T Data Center 內建立的邏輯實體
在計算或自行管理的 VPC/VNet 的子網路中，安裝有 NSX 代理程式的工作負載虛擬機器使用「nsx.network:default」索引鍵:值加以標記	■ 為此特定的計算或自行管理 VPC 或 VNet 的子網路建立區段 ■ 為安裝有 NSX 代理程式的每個標記的工作負載虛擬機器建立混合連接埠
在計算或自行管理 VPC/VNet 的相同子網路中標記更多工作負載虛擬機器	■ 為安裝有 NSX 代理程式的每個標記的工作負載虛擬機器建立混合連接埠

轉送原則

為計算 VPC/VNet (包括自行管理的傳送 VPC/VNet) 設定下列三個轉送規則：

- 透過公有雲網路 (底層) 存取同一個計算 VPC 的任何 CIDR
- 透過公有雲網路 (底層) 路由與公有雲中繼資料服務相關的流量
- 透過 NSX-T Data Center 網路 (覆疊) 路由不在計算 VPC/VNet 之 CIDR 區段或已知服務中的所有項目

自動建立的雲端原生 SG

在您的公有雲中，會建立雲端原生安全群組。

公有雲組態

在 AWS 中：

- 在 AWS VPC 中，以名稱 `nsx-gw.vmware.local` 將類型 A 記錄集新增至 Amazon Route 53 中的私人主控區域。對應到此記錄的 IP 位址符合由 AWS 使用 DHCP 進行指派的 PCG，並且視每個 VPC 而有所不同。Amazon Route 53 之私人主控區域中的此 DNS 項目可供 NSX Cloud 解析 PCG 的 IP 位址。

  備註 當您使用 Amazon Route 53 之私人主控區域中定義的自訂 DNS 網域名稱時，必須針對 AWS 中的 VPC 設定將 **DNS 解析**和 **DNS 主機名稱**設為**是**。

- 已建立 PCG 之上行介面的次要 IP。AWS 彈性 IP 與這個次要 IP 位址相關聯。此組態適用於 SNAT。

在 AWS 及 Microsoft Azure 中：

gw 安全群組會套用到相應 PCG 介面。

表 11-7. 由 NSX Cloud 針對 PCG 介面建立的公有雲安全群組

安全群組名稱	在 Microsoft Azure 中可用嗎?	在 AWS 中可用嗎?	全名
gw-mgmt-sg	是	是	閘道管理安全群組
gw-uplink-sg	是	是	閘道上行安全群組
gw-vtep-sg	是	是	閘道下行安全群組

表 11-8. 由 NSX Cloud 針對工作負載虛擬機器建立的公有雲安全群組

安全群組名稱	在 Microsoft Azure 中可用嗎?	在 AWS 中可用嗎?	說明
隔離	是	否	針對 Microsoft Azure 隔離安全群組
預設	否	是	針對 AWS 隔離安全群組
vm-underlay-sg	是	是	虛擬機器非覆疊安全群組
vm-override-sg	是	是	虛擬機器覆寫安全群組
vm-overlay-sg	是	是	虛擬機器覆疊安全群組 (未在目前版本中使用)
vm-outbound-bypass-sg	是	是	虛擬機器輸出略過安全群組 (未在目前版本中使用)
vm-inbound-bypass-sg	是	是	虛擬機器輸入略過安全群組 (未在目前版本中使用)

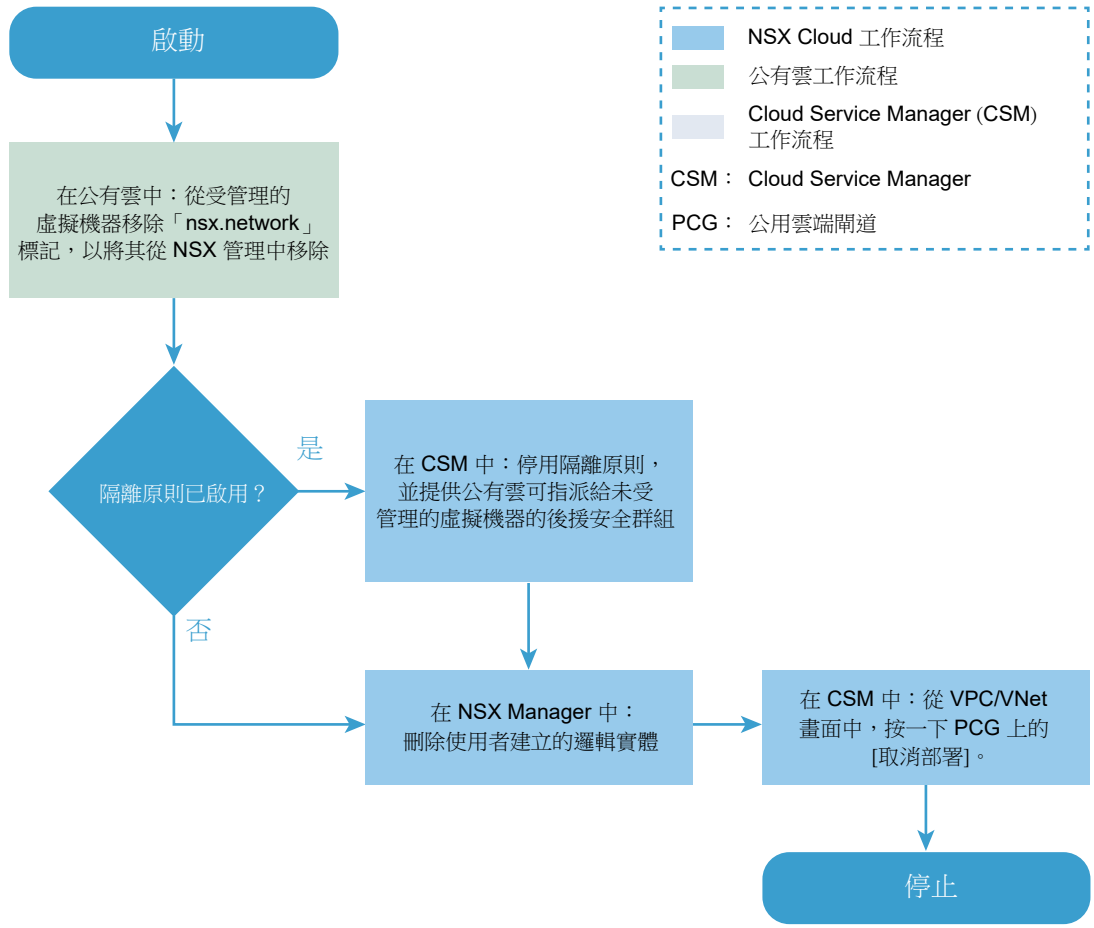
取消部署 PCG

請參閱此流程圖，以瞭解取消部署 PCG 所涉及的步驟。

取消部署 PCG 之前，必須執行下列操作：

- 確保 VPC 或 VNet 中的工作負載虛擬機器均不受 NSX 管理。
- 停用隔離原則。
- 刪除與 PCG 相關聯的使用者建立的所有邏輯實體。

圖 11-4. 取消部署 PCG



程序

1 取消標記公有雲中的虛擬機器

所有虛擬機器必須未受管理，您才可以取消部署 PCG。

2 停用隔離原則 (如已啟用)

如果先前已啟用，則必須停用隔離原則才能取消部署 PCG。

3 刪除使用者建立的邏輯實體

必須先刪除與 PCG 相關聯的使用者建立的所有邏輯實體。

4 從 CSM 取消部署

若要在完成必要條件後取消部署 PCG，請在 CSM 中從**雲端 > <Public_Cloud> > <VNet/VPC>**按一下取消部署閘道。

取消標記公有雲中的虛擬機器

所有虛擬機器必須未受管理，您才可以取消部署 PCG。

移至公有雲中的 VPC 或 VNet，然後從受管理的虛擬機器移除 `nsx.network` 標記。

停用隔離原則 (如已啟用)

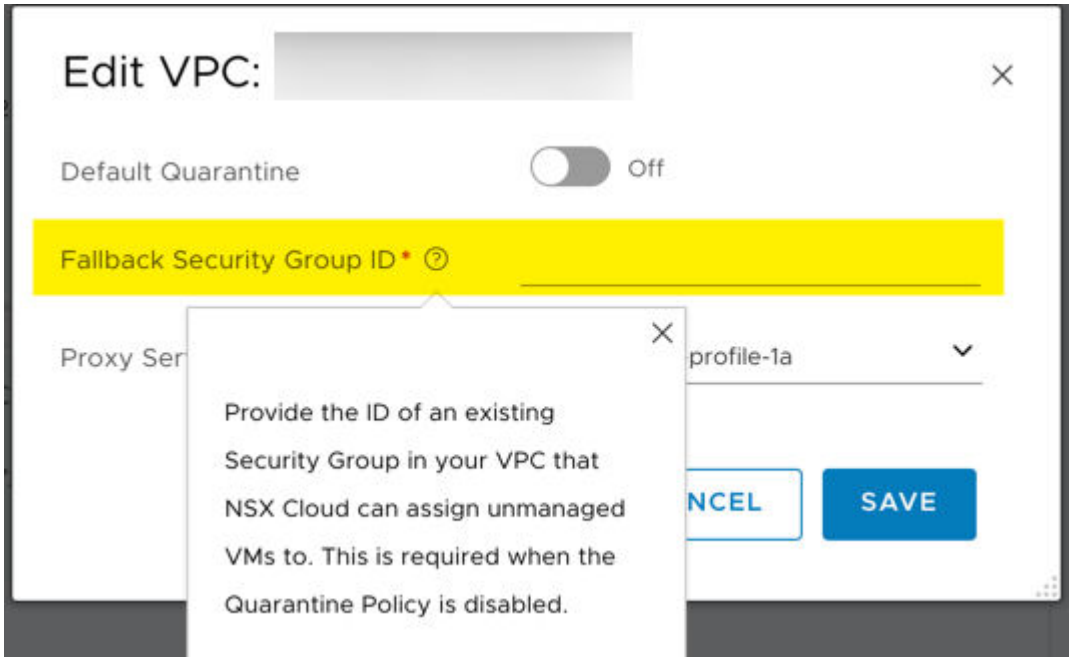
如果先前已啟用，則必須停用隔離原則才能取消部署 PCG。

啟用隔離原則時，您的虛擬機器將獲指派 NSX Cloud 所定義的安全群組。當您取消部署 PCG 時，需要停用隔離原則，並指定從 NSX Cloud 安全群組中移除時可獲指派虛擬機器的後援安全群組。

備註 後援安全群組必須是公有雲中現有的使用者定義的安全群組。您無法將任何 NSX Cloud 安全群組用作後援安全群組。請參閱自動建立的邏輯實體和雲端原生安全群組，以取得 NSX Cloud 安全群組的清單。

針對您要從中取消部署 PCG 的 VPC 或 VNet 停用隔離原則：

- 移至 CSM 中的 VPC 或 VNet。
- 從**動作 > 編輯組態**，關閉**預設隔離**的設定。
- 針對將獲指派虛擬機器的後援安全群組輸入值。



- 此 VPC 或 VNet 中的所有未受管理或隔離的虛擬機器，將獲指派後援安全群組。
- 如果所有虛擬機器均未受管理，會將其指派給後援安全群組。
- 如果停用隔離原則時有受管理的虛擬機器，它們會保留其 NSX Cloud 指派的安全群組。首次從此類虛擬機器移除 `nsx.network` 標記以將其從 NSX 管理移出時，它們也將獲指派後援安全群組。

備註 請參閱《NSX-T Data Center 管理指南》中的〈**管理隔離原則**〉，以取得有關啟用和停用隔離原則的指示以及效果的詳細資訊。

刪除使用者建立的邏輯實體

必須先刪除與 PCG 相關聯的使用者建立的所有邏輯實體。

識別與 PCG 相關聯的實體，然後刪除這些實體。

備註 請勿刪除自動建立的邏輯實體。從 CSM 按一下**取消部署閘道**後，這些會自動刪除。如需自動建立的邏輯實體的清單，請參閱自動建立的邏輯實體和雲端原生安全群組。

從 CSM 取消部署

若要在完成必要條件後取消部署 PCG，請在 CSM 中從**雲端 > <Public_Cloud> > <VNet/VPC>**按一下取消部署閘道。

1 登入 CSM 並移至您的公有雲：

- 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下已部署且正在執行一個或一對 PCG 的 VPC。
- 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。

2 按一下取消部署閘道。

PCG 取消部署後，會自動移除 NSX Cloud 所建立的預設實體。