

NSX-T Data Center 安裝指南

修改日期：2019 年 4 月 23 日

VMware NSX-T Data Center 2.3



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/>

VMware 網站也提供最新的產品更新。

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

Copyright © 2018、2019 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

NSX-T Data Center 安裝指南 5

1 NSX-T Data Center 概觀 6

管理平面 7

控制平面 9

數據平面 9

邏輯交換器 11

邏輯路由器 11

主要概念 12

2 準備安裝 15

系統需求 15

連接埠和通訊協定 19

NSX-T Data Center 安裝高層級工作 25

3 使用 KVM 27

設定 KVM 27

在 KVM CLI 中管理您的客體虛擬機器 32

4 NSX Manager 安裝 34

安裝 NSX Manager 和可用應用裝置 36

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager 37

在 KVM 上安裝 NSX Manager 40

登入新建立的 NSX Manager 42

5 NSX Controller 安裝和叢集 44

從 NSX Manager 自動安裝控制器和叢集 46

使用 GUI 在 ESXi 上安裝 NSX Controller 52

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Controller 54

在 KVM 上安裝 NSX Controller 56

將 NSX Controller 加入 NSX Manager 58

初始化控制叢集以建立控制叢集主節點 60

將其他 NSX Controller 加入叢集主節點 61

6 NSX Edge 安裝 65

NSX Edge 網路設定 67

從 NSX Manager 自動部署 NSX Edge 虛擬機器 71

使用 vSphere GUI 在 ESXi 上安裝 NSX Edge 72

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge 74

使用 ISO 檔案與 PXE 伺服器安裝 NSX Edge 78

將 NSX Edge 加入管理平面 89

7 主機準備 90

在 KVM 主機或裸機伺服器上安裝第三方套件 90

確認 RHEL KVM 主機上的 Open vSwitch 版本 92

將 Hypervisor 主機或裸機伺服器新增至 NSX-T Data Center 網狀架構 93

NSX-T Data Center 核心模組的手動安裝 97

將 Hypervisor 主機加入管理平面 101

8 傳輸區域和傳輸節點 104

關於傳輸區域 104

增強型資料路徑 106

為通道端點 IP 位址建立 IP 集區 107

建立上行設定檔 110

建立傳輸區域 113

建立主機傳輸節點 115

建立裸機伺服器工作負載的應用程式介面 131

設定 Network I/O Control 設定檔 132

建立 NSX Edge 傳輸節點 140

建立 NSX Edge 叢集 143

9 NSX Cloud 元件安裝 145

NSX Cloud 架構和元件 145

安裝 NSX Cloud 元件的概觀 146

安裝 CSM 並連線 NSX Manager 148

連線公有雲與內部部署 150

新增公有雲帳戶 153

部署 PCG 158

取消部署 PCG 163

10 解除安裝 NSX-T Data Center 167

取消設定 NSX-T Data Center 覆疊 167

從 NSX-T Data Center 中移除主機或完整解除安裝 NSX-T Data Center 167

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。

VMware 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

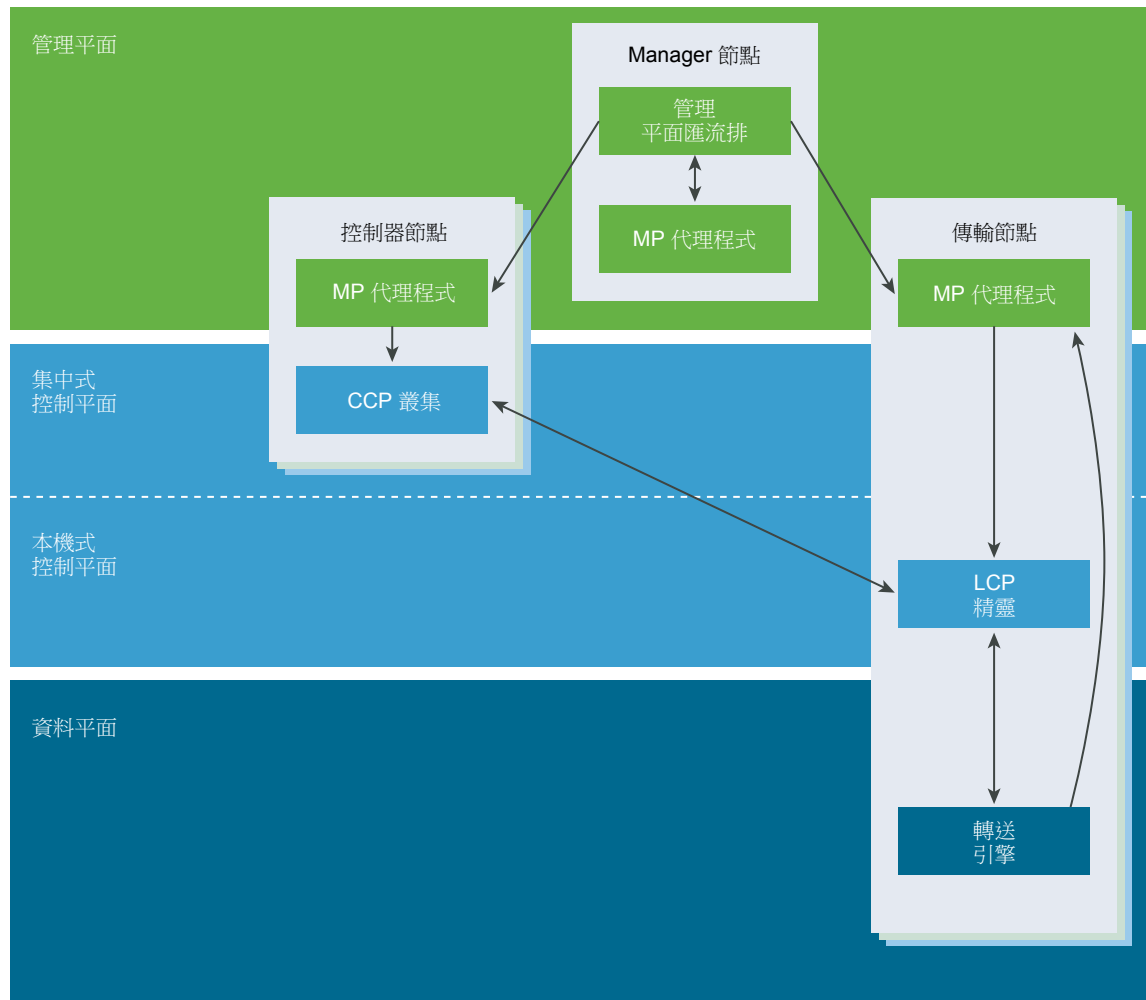
比照伺服器虛擬化透過程式設計的方法來建立、刪除、還原軟體型虛擬機器 (VM) 及建立其快照的方式，**NSX-T Data Center** 網路虛擬化會以相似的方式透過程式設計的方法來建立、刪除、還原軟體型虛擬網路。

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。這三個平面可實作為一組存在於三種類型節點上的程序、模組和代理程式：管理員、控制器和傳輸節點。

- 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。每個 **NSX-T Data Center** 安裝支援單一 **NSX Manager** 節點。
- **NSX Controller** 節點會裝載中央控制平面叢集精靈。
- **NSX Manager** 與 **NSX Controller** 節點可共同裝載於相同的實體伺服器上。

- 傳輸節點會裝載本機控制平面精靈和轉送引擎。



本章包含以下主題：

- 管理平面
- 控制平面
- 數據平面
- 邏輯交換器
- 邏輯路由器
- 主要概念

管理平面

管理平面可提供系統的單一 **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。

就 **NSX-T Data Center** 而言，只要涉及查詢、修改和持續保存使用者組態的處理，皆屬於管理平面的責任，而將該組態向下散佈至資料平面元素的正確子集，則是控制平面的責任。這表示，某些資料會隨著其存在的階段而屬於多個平台。管理平面也會處理查詢最近狀態和來自控制平面的統計資料 (有時直接來自資料平面) 的工作。

管理平面是已設定之 (邏輯) 系統的唯一真實來源，如同使用者透過組態所管理。使用 **RESTful API** 或 **NSX-T Data Center UI** 可以進行變更。

在 **NSX** 中，也有一個執行於所有控制器叢集和傳輸節點上的管理平面代理程式 (**MPA**)。**MPA** 可以從本機和遠端進行存取。在傳輸節點上，它也可以執行與資料平面有關的工作。

在管理平面上執行的工作包括：

- 組態持續保存 (所需的邏輯狀態)
- 輸入驗證
- 使用者管理 -- 角色指派
- 原則管理
- 背景工作追蹤

NSX Manager

NSX Manager 是一個虛擬應用裝置，提供可用來建立、設定及監控 **NSX-T Data Center** 元件 (例如邏輯交換器和 **NSX Edge** 服務閘道) 的圖形使用者介面 (**GUI**) 與 **REST API**。

NSX Manager 是 **NSX-T Data Center** 生態系統的管理平面。**NSX Manager** 會提供彙總的系統視圖，且屬於 **NSX-T Data Center** 的集中式網路管理元件。它可用來設定及協調下列項目：

- 邏輯網路元件 - 邏輯交換和路由
- 網路和 **Edge** 服務
- 安全性服務和分散式防火牆

NSX Manager 提供用來對連結至 **NSX-T Data Center** 所建立之虛擬網路的工作負載進行監控和疑難排解的方法。可讓您順暢地協調內建服務和外部服務。所有的安全性服務 (無論是內建或第三方) 皆會由 **NSX-T Data Center** 管理平面進行部署和設定。管理平面會提供單一視窗以便檢視服務可用性。它也提升了原則型服務鏈結、內容共用和服務間事件處理的執行速度。這簡化了安全性狀態的稽核，使身分識別型控制 (例如，**AD** 和行動性設定檔) 的應用更為精簡。

NSX Manager 也提供 **REST API** 進入點以便自動消耗。此彈性架構可讓您透過任何雲端管理平台、安全性廠商平台或自動化架構，自動執行所有組態及監控層面。

NSX-T Data Center 管理平面代理程式 (**MPA**) 是存在於每一個節點 (**Hypervisor**) 上的 **NSX Manager** 元件。**MPA** 會負責持續保存所需的系統狀態，以及在傳輸節點與管理平面之間傳送非流量控制 (**NFC**) 訊息，例如組態、統計資料、狀態和即時資料。

NSX Policy Manager

NSX Policy Manager 是一個虛擬應用裝置，可提供基於意圖的系統，以簡化 **NSX-T Data Center** 服務的耗用。

NSX Policy Manager 提供圖形化使用者介面 (GUI) 與 REST API，來指定與網路、安全性和可用性相關的意圖。

NSX Policy Manager 接受採用以樹狀結構為基礎之資料模型形式的使用者意圖，並設定 NSX Manager 以實現該意圖。NSX Policy Manager 支援在 NSX Manager 上設定分散式防火牆的通訊意圖規格。

Cloud Service Manager

Cloud Service Manager (CSM) 針對所有公有雲建構提供單一虛擬管理介面管理端點。

CSM 是一個虛擬應用裝置，提供可用來上線、設定及監控公有雲詳細目錄的圖形使用者介面 (GUI) 與 REST API。

控制平面

根據管理平面的組態計算所有暫時執行階段的狀態、散佈資料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。

在 NSX-T Data Center 中，控制平面分為兩個部分，分別是中央控制平面 (CCP)，此平面在 NSX Controller 叢集節點上執行，以及本機控制平面 (LCP)，此平面會在其所控制之資料平面的相鄰傳輸節點上執行。中央控制平面會根據管理平面的組態計算某些暫時執行階段的狀態，並透過本機控制平面散佈資料平面元素所報告的資訊。本機控制平面會監控本機連結狀態、根據資料平面和 CCP 的更新計算最短暫執行階段的狀態，以及將無狀態組態推送至轉送引擎。LCP 會與其裝載所在的資料平面元素產生連帶作用。

NSX Controller

NSX Controller 稱為中央控制平面 (CCP)，是進階的分散式狀態管理系統，可控制虛擬網路和覆疊傳輸通道。

NSX Controller 會部署為高可用性虛擬應用裝置的叢集，將負責進行整個 NSX-T Data Center 架構中的虛擬網路程式設計部署。NSX-T Data Center CCP 會以邏輯方式與所有數據平面流量分隔，這表示控制平面中的任何失敗皆不影響現有的數據平面作業。流量不會經過控制器；而控制器會負責將組態提供給其他 NSX Controller 元件，例如邏輯交換器、邏輯路由器以及 Edge 組態。資料傳輸的穩定性和可靠性是網路功能中的重要考量。若要進一步增強高可用性和延展性，可以在三個執行個體的叢集中部署 NSX Controller。

數據平面

根據控制平面所填入的資料表和控制平面的報告拓撲資訊，執行無狀態的封包轉送/轉換，並保留封包等級統計資料。

資料平面是實體拓撲和狀態 (例如 VIF 位置、通道狀態等等) 的真實來源。如果您正在處理在不同位置間移動封包的作業，這表示您位於資料平面。資料平面也會保留多個連結/通道之間容錯移轉的狀態並處理此作業。每個封包的效能皆至關重要，且對於延遲的要求極為嚴格，或是具有時基誤差需求。資料平面不一定會完全包含在核心、驅動程式、使用者空間或甚至特定的使用者空間處理程序中。根據控制平面所填入的資料表/規則，資料平面會限制為完全無狀態的轉送。

資料平面也可以擁有元件來保留一定數量的功能 (例如 TCP 終止) 狀態。這不同於控制平面所管理的狀態，例如 MAC:IP 通道對應，因為控制平面所管理的狀態是關於如何轉送封包，而資料平面所管理的狀態則限制為如何操縱裝載。

NSX Edge

NSX Edge 可提供在 NSX-T Data Center 部署以外的路由服務和網路連線。

NSX Edge 可做為裸機節點或虛擬機器進行部署。

從 NSX-T Data Center 網域透過第 0 層路由器經由 BGP 或靜態路由來建立外部連線時，則需要 NSX Edge。此外，如果您在第 0 層或第 1 層邏輯路由器上需要網路位址轉譯 (NAT) 服務，則必須部署 NSX Edge。

NSX Edge 閘道可藉由提供一般閘道服務 (例如 NAT) 和動態路由，將隔離的虛設常式網路連線至共用 (上行) 網路。NSX Edge 的一般部署包含在 NSX Edge 會為每個承租人建立虛擬界限的 DMZ 和多承租人雲端環境中。

傳輸區域

傳輸區域為邏輯建構，用於控制邏輯交換器可連線哪些主機。它可跨越一或多個主機叢集。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。

傳輸區域會定義能夠在實體網路基礎結構內相互通訊的主機集合。此通訊會透過定義為虛擬通道端點 (VTEP) 的一或多個介面來進行。

傳輸節點是執行本機控制平面精靈和轉送引擎 (實作 NSX-T Data Center 數據平面) 的主機。傳輸節點由 NSX-T Data Center 虛擬分散式交換器 (N-VDS) 組成，負責根據可用網路服務的組態交換封包。

如果有兩個傳輸節點位於相同的傳輸區域中，則裝載在這些傳輸節點上的虛擬機器將可「看見」並連線至也位於該傳輸區域中的 NSX-T Data Center 邏輯交換器。假設虛擬機器具有第 2 層/第 3 層連線性，則前述連結即可讓這些虛擬機器相互通訊。如果虛擬機器連結至不同傳輸區域的交換器，則虛擬機器無法彼此通訊。傳輸區域無法取代第 2 層/第 3 層連線能力需求，但可限制連線能力。換句話說，屬於相同的傳輸區域是連線的先決條件。符合先決條件後才可能產生連線性，但並不會自動產生。若要達到實際的連線性，第 2 層和 (適用於不同的子網路) 第 3 層網路必須正常運作。

如果某個主機包含至少一個 NSX 管理的虛擬分散式交換器 (N-VDS，以前稱為主機交換器)，則此主機可用作傳輸節點。當您建立主機傳輸節點，並將此節點新增至傳輸區域後，NSX-T Data Center 會在此主機上安裝 N-VDS。針對此主機所屬的每個傳輸區域，系統皆會安裝個別的 N-VDS。N-VDS 會用來將虛擬機器連結至 NSX-T Data Center 邏輯交換器，以及用來建立 NSX-T Data Center 邏輯路由器上行和下行。

邏輯交換器

NSX-T Data Center 平台中的邏輯交換功能，可讓您透過虛擬機器所具備的相同彈性和靈活性，使隔離的邏輯 L2 網路更為快速。

邏輯交換器可呈現出在許多主機之間交換連線的第 2 層，且在其中包含第 3 層的 IP 連線性。如果您要將某些邏輯網路限定於受限的一組主機，或是您有自訂連線需求，則可能會發現需要建立其他邏輯交換器。

這些應用程式和承租人需要相互隔離，以保有安全性、進行故障隔離，以及避免發生 IP 位址重疊的問題。端點 (包括虛擬和實體) 可連線至邏輯區段，並獨立在資料中心網路中的實體位置以外建立連線。此功能可透過從 NSX-T Data Center 網路虛擬化所提供的邏輯網路分離網路基礎結構 (例如覆疊網路中的底層網路) 來啟用。

邏輯路由器

NSX-T Data Center 邏輯路由器可提供南北向連線，讓承租人能夠存取公用網路，此外也提供相同承租人內的不同網路之間的東西向連線。為實現東西向連線，會在主機的核心之間散佈邏輯路由器。

透過 NSX-T Data Center，我們得以建立雙層邏輯路由器拓撲：最上層邏輯路由器是第 0 層，底層邏輯路由器是第 1 層。此結構讓提供者管理員和承租人管理員都能夠完全掌控其服務和原則。管理員可控制及設定第 0 層路由和服務，而承租人管理員則可控制及設定第 1 層。第 0 層介面的北端會與實體網路接觸，而動態路由通訊協定可在此處設定，以便與實體路由器交換路由資訊。第 0 層的南端會連線至多個第 1 層路由層，以及接收來自該層的路由資訊。為了讓資源運用最佳化，第 0 層並不會將所有來自實體網路的路由推送至第 1 層，但會提供預設資訊。

南向的第 1 層路由層會與承租人管理員所定義的邏輯交換器接觸，並提供兩者之間的單躍點路由功能。若要能夠從實體網路存取連結第 1 層的子網路，必須要啟用對第 0 層的路由重新分配。不過，目前並沒有在第 1 層與第 0 層之間執行的傳統路由通訊協定 (例如 OSPF 或 BGP)，而所有路由皆會透過

NSX-T Data Center 控制平面來執行。請注意，雙層路由拓撲並非強制。如果不需要分隔提供者和承租人，則可以建立單層拓撲，而在此案例中，邏輯交換器會直接連線至第 0 層，而且不會有第 1 層。

邏輯路由器由兩個選用部分所組成：分散式路由器 (DR) 和一或多個服務路由器 (SR)。

DR 會跨越虛擬機器連線至此邏輯路由器的 Hypervisor，以及邏輯路由器所繫結的 Edge 節點。就功能而言，DR 負責邏輯交換器和/或連線至此邏輯路由器的邏輯路由器之間的單躍點分散式路由。SR 則負責提供目前未以分散方式實作的服務，例如可設定狀態的 NAT。

邏輯路由器一律具有 DR，且在符合下列任一條件時具有 SR：

- 即使未設定可設定狀態的服務，邏輯路由器仍為第 0 層路由器
- 邏輯路由器是連結至第 0 層路由器的第 1 層路由器，並且已設定沒有分散式實作的服務 (例如 NAT、LB 和 DHCP)

NSX-T Data Center 管理平面 (MP) 負責自動建立將服務路由器連線至分散式路由器的結構。MP 會建立轉換邏輯交換器並為其配置 VNI，然後在每個 SR 和 DR 上建立連接埠、將其連線至轉換邏輯交換器，然後為 SR 和 DR 配置 IP 位址。

主要概念

用於說明文件和使用界面中的一般 **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 將網路覆蓋至外部網路。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 覆蓋的一部分，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	為虛擬機器界面和閘道界面提供虛擬第 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界面或邏輯路由器界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 Controller 叢集	部署為高可用性虛擬應用裝置的叢集，將負責進行整個 NSX-T Data Center 架構中的虛擬網路程式設計部署。

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 管理的虛擬分散式交換器或 KVM Open vSwitch

在 Hypervisor 上執行並提供流量轉送的軟體。NSX 管理的虛擬分散式交換器 (N-VDS，以前稱為主機交換器) 或 OVS 並不會向承租人網路管理員顯示，但會提供可供每個邏輯交換器依賴的基礎轉送服務。若要達到網路虛擬化，則網路控制器必須以網路流量表來設定 Hypervisor 虛擬交換器，且該流量表形成承租人管理員在建立及設定其邏輯交換器時所定義的邏輯廣播網域。

每個邏輯廣播網域的實作方式如下：使用通道封裝機制 Geneve，建立虛擬機器至虛擬機器流量的通道，以及虛擬機器至邏輯路由器流量的通道。網路控制器具有資料中心的全域視圖，且可確保 Hypervisor 虛擬交換器流量表會隨著虛擬機器的建立、移動或移除而進行更新。

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-T Data Center Unified Appliance

NSX-T Data Center Unified Appliance 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、原則管理員或 Cloud Service Manager 的角色來部署應用裝置。目前，應用裝置一次僅支援一個角色。

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。

第 0 層邏輯路由器

提供者邏輯路由器也稱為具有實體網路的第 0 層邏輯路由器介面。第 0 層邏輯路由器是最上層路由器，並且可視為服務路由器的「主動-主動」或「主動-待命」叢集。邏輯路由器會執行 BGP，並且與實體路由器對等。在「主動-待命」模式中，邏輯路由器也可提供可設定狀態的服務。

第 1 層邏輯路由器

第 1 層邏輯路由器是第二層路由器，它會連線至一個第 0 層邏輯路由器以進行北向連線，並連線至一或多個覆疊網路以進行南向連線。第 1 層邏輯路由器可以是提供可設定狀態服務之服務路由器的「主動-待命」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。

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

可讓 Hypervisor 主機加入 NSX-T Data Center 覆疊。NSX-T Data Center 覆疊會在現有的第 3 層網路網狀架構之上部署第 2 層網路；方法是將框架封裝在封包內，並透過基礎傳輸網路來傳送封包。基礎傳輸網路可以是其他第 2 層網路，或者也可以跨越第 3 層界限。VTEP 是執行封裝和解除封裝所在的連線點。

準備安裝

安裝 NSX-T Data Center 之前，請確定您的環境已備妥。

本章包含以下主題：

- [系統需求](#)
- [連接埠和通訊協定](#)
- [NSX-T Data Center 安裝高層級工作](#)

系統需求

NSX-T Data Center 具有關於硬體資源和軟體版本的特定需求。

Hypervisor 需求

Hypervisor	版本	CPU 核心	記憶體
vSphere	支援的 vSphere 版本	4	16 GB
RHEL KVM	7.5 和 7.4	4	16 GB
Ubuntu KVM	16.04.2 LTS	4	16 GB
CentOS KVM	7.4	4	16 GB

NSX-T Data Center 支援在 RHEL 7.5、RHEL 7.4、Ubuntu 16.04 和 CentOS 7.4 上進行主機準備。RHEL 7.5 和 CentOS 7.4 上不支援 NSX Manager 和 NSX Controller 部署。NSX Edge 節點部署僅支援在 vSphere 上進行。

對於 ESXi 主機，NSX-T Data Center 支援 vSphere 6.7 U1 或更高版本上的主機設定檔和自動部署功能。



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。

裸機伺服器需求

作業系統	版本	CPU 核心	記憶體
RHEL	7.5 和 7.4	4	16 GB
Ubuntu	16.04.2 LTS	4	16 GB
CentOS	7.4	4	16 GB

NSX Manager 資源需求

精簡佈建虛擬磁碟大小為 3.1 GB，完整佈建虛擬磁碟大小為 200 GB。

應用裝置	記憶體	vCPU	儲存區	虛擬機器硬體版本
NSX Manager 小型虛擬機器	8 GB	2	200 GB	10 或更新版本
NSX Manager 中型虛擬機器	16 GB	4	200 GB	10 或更新版本
NSX Manager 中大型虛擬機器	24 GB	6	200 GB	10 或更新版本
NSX Manager 大型虛擬機器	32 GB	8	200 GB	10 或更新版本
NSX Manager 超大型虛擬機器	48 GB	12	200 GB	10 或更新版本

備註 NSX Manager 小型虛擬機器應用於實驗室和概念驗證部署。

NSX Manager 資源需求適用於 NSX Policy Manager 和 Cloud Service Manager。

NSX Controller 資源需求

應用裝置	記憶體	vCPU	磁碟空間	部署類型
NSX Controller 小型虛擬機器	8 GB	2	120 GB	實驗室和概念驗證部署
NSX Controller 中型虛擬機器	16 GB	4	120 GB	建議用於中型部署
NSX Controller 大型虛擬機器	32 GB	8	120 GB	為大型部署所需

備註 部署三個 NSX Controller，以確保高可用性並避免 NSX-T Data Center 控制平面出現任何中斷。

各個 NSX Controller 叢集必須位於三個獨立的實體 Hypervisor 主機，以避免單一實體 Hypervisor 主機故障影響 NSX-T Data Center 控制平面。請參閱《NSX-T Data Center 參考設計》指南。

針對沒有任何生產工作負載的實驗室和概念驗證部署，可使用單一 NSX Controller 以節省資源。

您只能從 vSphere OVF 部署使用者介面部署小型和大型虛擬機器的機器尺寸。

NSX Edge 虛擬機器資源需求

部署大小	記憶體	vCPU	磁碟空間	虛擬機器硬體版本
小	4 GB	2	120 GB	10 或更新版本 (vSphere 5.5 或更新版本)
中	8 GB	4	120 GB	10 或更新版本 (vSphere 5.5 或更新版本)
大	16 GB	8	120 GB	10 或更新版本 (vSphere 5.5 或更新版本)

備註 針對 NSX Manager 和 NSX Edge 而言，小型應用裝置會用於概念驗證部署。中型應用裝置適用於一般生產環境，且最多可支援 64 個 Hypervisor。大型應用裝置適用於具有超過 64 個 Hypervisor 的大規模部署。

備註 僅 NSX Edge 虛擬機器支援 VMXNET 3 vNIC。

NSX Edge 虛擬機器和裸機 NSX Edge CPU 需求

備註 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。

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。

備註 由於 NSX-T Data Center 資料平面會使用 Intel 資料平面開發套件 (DPDK) 中的網路功能，因此僅支援 Intel 架構的 CPU。

硬體	類型
CPU	<ul style="list-style-type: none"> ■ Xeon 56xx (Westmere-EP) ■ Xeon E7-xxxx (Westmere-EX 及下一代 CPU) ■ Xeon E5-xxxx (Sandy Bridge 及下一代 CPU)

裸機 NSX Edge 硬體需求

請確認裸機 NSX Edge 硬體有列在下列 URL 中：<https://certification.ubuntu.com/server/models/?release=16.04%20LTS&category=Server>。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。

裸機 NSX Edge 的特定 NIC 需求

NIC 類型	說明	PCI 裝置識別碼
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_BACK	0x10F8
	PLANE	0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9
	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 NSX Edge 的記憶體、CPU 和磁碟需求

記憶體	CPU 核心	磁碟空間
32 GB	8	200 GB

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	i40en 1.1.3-1OEM.670.0.0.8169922
適用於 40GbE QSFP+ 的 Intel(R) 乙太網路控制器 XL710	

NSX Manager 瀏覽器支援

瀏覽器	Windows 10	Windows 8.1	Ubuntu 14.04	Mac OS X 10.11 和 10.12
Internet Explorer 11	是	是		
Firefox 55			是	是
Chrome 60	是	是		是
Safari 10				是
Microsoft Edge 40	是			

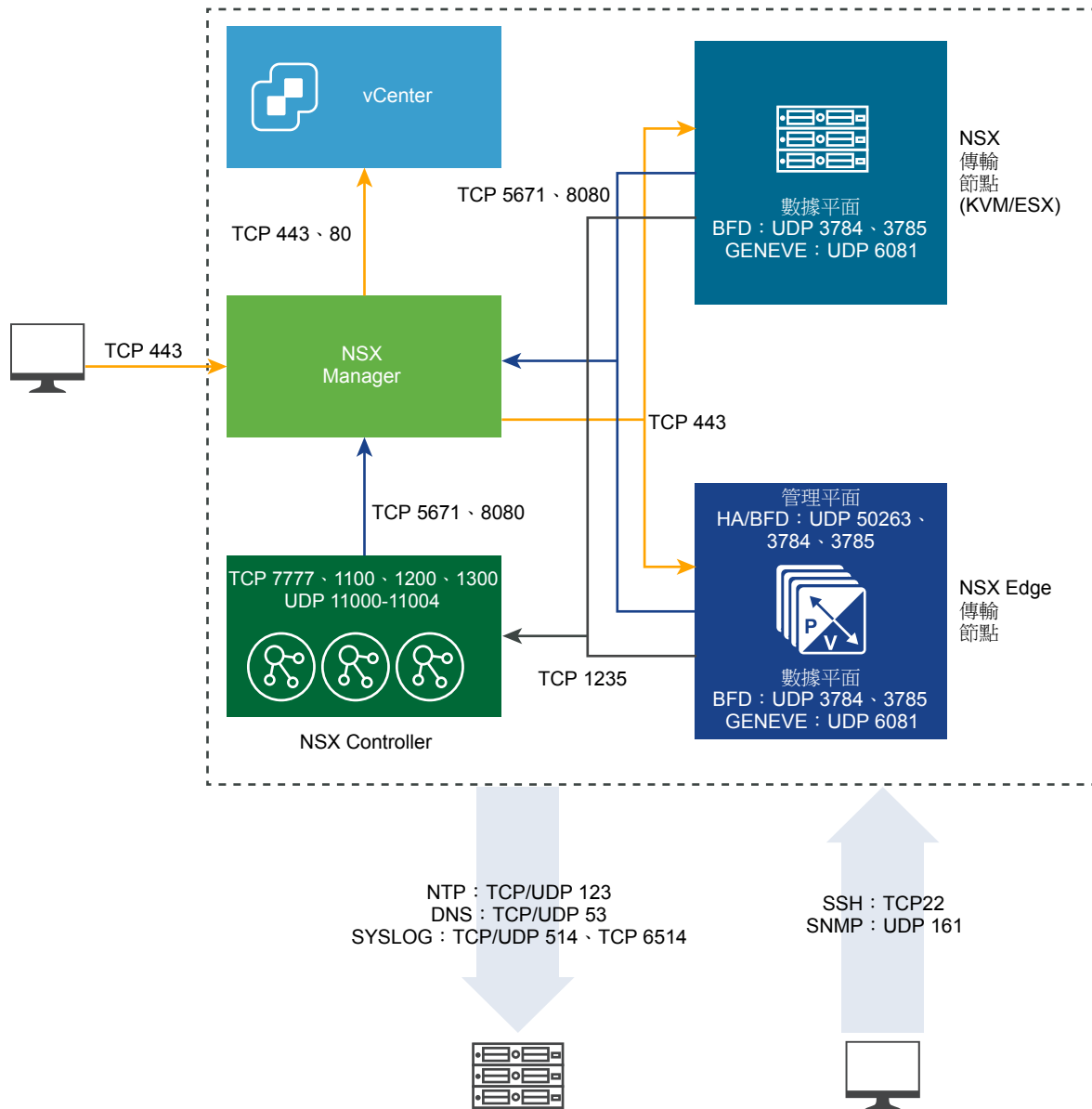
備註 不支援 Internet Explorer 11 相容模式。

支援的瀏覽器最低解析度為 1280 x 800 像素。

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。

圖 2-1: 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
- ESX: netcpa、ESX-DP (在核心內)


在 RMQ 使用者資料庫 (db) 中，密碼會使用無法還原的雜湊功能進行雜湊處理。因此，h(p1) 是密碼 p1 的雜湊。

CCP 中央控制平面

LCP 本機控制平面

MP	管理平面
MPA	管理平面代理程式

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。

表格 2-1. 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
管理用戶端	NSX Manager	22	TCP	SSH (依預設為停用)
NTP 伺服器	NSX Manager	123	UDP	NTP
管理用戶端	NSX Manager	443	TCP	NSX API 伺服器
SNMP 伺服器	NSX Manager	161	UDP	SNMP
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 Controller、NSX Edge 節點、傳輸節點	NSX Manager	5671	TCP	NSX 傳訊
NSX Manager	管理 SCP 伺服器	22	TCP	SSH (上傳支援服務包及備份等項目)
NSX Manager	DNS 伺服器	53	TCP	DNS
NSX Manager	DNS 伺服器	53	UDP	DNS
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	Log Insight 伺服器	9000	TCP	Log Insight 代理程式

表格 2-1. 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	Traceroute 目的地	3343 4 - 3352 3	UDP	Traceroute
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 Controller 所使用的 TCP 和 UDP 連接埠

NSX Controller 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。

表格 2-2. NSX Controller 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 Controller	22	TCP	SSH (依預設為停用)
DNS 伺服器	NSX Controller	53	UDP	DNS
NTP 伺服器	NSX Controller	123	UDP	NTP
SNMP 伺服器	NSX Controller	161	UDP	SNMP
NSX Controller	NSX Controller	1100	TCP	Zookeeper 仲裁
NSX Controller	NSX Controller	1200	TCP	Zookeeper 領導選舉
NSX Controller	NSX Controller	1300	TCP	Zookeeper 伺服器
NSX Edge 節點、傳輸節點	NSX Controller	1235	TCP	CCP-netcpa 通訊
NSX Controller	NSX Controller	7777	TCP	Moot RPC
NSX Controller	NSX Controller	11000 - 11004	UDP	連接至其他叢集節點的通道。若叢集具有 5 個以上的節點，您就必須開啟更多連接埠。
Traceroute 目的地	NSX Controller	33434 - 33523	UDP	Traceroute
NSX Controller	SSH 目的地	22	TCP	SSH (依預設為停用)
NSX Controller	DNS 伺服器	53	UDP	DNS
NSX Controller	DNS 伺服器	53	TCP	DNS
NSX Controller	NTP 伺服器	123	UDP	NTP
NSX Controller	NSX Manager	5671	TCP	NSX 傳訊
NSX Controller	Log Insight 伺服器	9000	TCP	Log Insight 代理程式

表格 2-2. NSX Controller 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 Controller	NSX Controller	11000 - 11004	TCP	連接至其他叢集節點的通道。若叢集具有 5 個以上的節點，您就必須開啟更多連接埠。
NSX Controller	NSX Manager	8080	TCP	NSX 升級
NSX Controller	Traceroute 目的地	33434 - 33523	UDP	Traceroute
NSX Controller	Syslog 伺服器	514	UDP	Syslog
NSX Controller	Syslog 伺服器	514	TCP	Syslog
NSX Controller	Syslog 伺服器	6514	TCP	Syslog

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。

表格 2-3. 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)
NTP 伺服器	NSX Edge 節點	123	UDP	NTP
SNMP 伺服器	NSX Edge 節點	161	UDP	SNMP
NSX Edge 節點	NSX Edge 節點	1167	TCP	DHCP 後端
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。
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	NSX Edge 節點	6666	TCP	NSX Cloud - NSX Edge 本機通訊。
NSX Edge 節點	NSX Manager	8080	TCP	NAPI 和 NSX-T Data Center 升級
NSX Edge 節點	NSX Edge 節點	2480	TCP	Nestdb
NSX Edge 節點	管理 SCP 或 SSH 伺服器	22	TCP	SSH
NSX Edge 節點	DNS 伺服器	53	UDP	DNS
NSX Edge 節點	NTP 伺服器	123	UDP	NTP
NSX Edge 節點	SNMP 伺服器	161 和 162	UDP	SNMP
NSX Edge 節點	SNMP 伺服器	161 和 162	TCP	SNMP
NSX Edge 節點	NSX Manager	443	TCP	HTTPS

表格 2-3. 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	Syslog 伺服器	514	TCP	Syslog
NSX Edge 節點	Syslog 伺服器	514	UDP	Syslog
NSX Edge 節點	NSX Edge 節點	1167	TCP	DHCP 後端
NSX Edge 節點	NSX Controller	1235	TCP	netcpa
NSX Edge 節點	OpenStack Nova API 伺服器	3000 - 9000	TCP	中繼資料 Proxy
NSX Edge 節點	NSX Manager	5671	TCP	NSX 傳訊
NSX Edge 節點	Syslog 伺服器	6514	TCP	透過 TLS 的 Syslog
NSX Edge 節點	Traceroute 目的地	33434 - 33523	UDP	Traceroute
NSX Edge 節點	NSX Edge 節點	50263	UDP	高可用性

由 vSphere ESXi、KVM 主機和裸機伺服器使用的 TCP 和 UDP 連接埠

當 vSphere 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。

表格 2-4. vSphere 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
NSX Manager	vSphere 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
vSphere ESXi 主機	NSX Manager	5671	TCP	NSX Manager 的 AMPQ 通訊通道
vSphere ESXi 主機	NSX Controller	1235	TCP	控制平面 - LCP 至 CCP 通訊
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
vSphere ESXi 主機	NSX Manager	8080	TCP	安裝和升級 HTTP 存放庫
KVM 主機	NSX Manager	8080	TCP	安裝和升級 HTTP 存放庫

表格 2-4. vSphere 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
GENEVE 終止端點 (TEP)	GENEVE 終止端點 (TEP)	6081	UDP	傳輸網路
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

NSX-T Data Center 安裝高層級工作

使用檢查清單追蹤您的安裝進度。

請遵循建議的程序順序。

- 1 安裝 NSX Manager，請參閱 [第 4 章，NSX Manager 安裝](#)。
- 2 安裝 NSX Controller，請參閱 [第 5 章，NSX Controller 安裝和叢集](#)。
- 3 將 NSX Controller 加入管理平面，請參閱 [將 NSX Controller 加入 NSX Manager](#)。
- 4 建立主要 NSX Controller 以初始化控制叢集，請參閱 [初始化控制叢集以建立控制叢集主節點](#)。
- 5 將 NSX Controller 加入控制叢集，請參閱 [將其他 NSX Controller 加入叢集主節點](#)。

新增 Hypervisor 主機後，NSX Manager 會安裝 NSX-T Data Center 模組。

備註 在安裝 NSX-T Data Center 模組時，系統會在 Hypervisor 主機上建立憑證。

- 6 將 Hypervisor 主機加入管理平面，請參閱 [將 Hypervisor 主機加入管理平面](#)。
主機會將其主機憑證傳送至管理平面。
- 7 安裝 NSX Edge，請參閱 [第 6 章，NSX Edge 安裝](#)。
- 8 將 NSX Edge 加入管理平面，請參閱 [將 NSX Edge 加入管理平面](#)。
- 9 建立傳輸區域和傳輸節點，請參閱 [第 8 章，傳輸區域和傳輸節點](#)。

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。

一般安裝順序如下：

- 1 首先安裝 NSX Manager。
- 2 NSX Controller 可在安裝後加入管理平面。
- 3 NSX-T Data Center 模組可以在 Hypervisor 主機加入管理平面之前安裝在該主機上，或者，您可以使用 [網狀架構 > 主機 > 新增 UI](#) 同時執行這兩個程序。
- 4 NSX Controller、NSX Edge 和具有 NSX-T Data Center 模組的主機可以隨時加入管理平面。

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 Controller**、**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 Controller**、**NSX Edge** 和主機。

如需詳細資訊，請參閱《**NSX-T Data Center** 管理指南》。

使用 KVM

NSX-T Data Center 支援 KVM 的方式有兩種：1) 作為主機傳輸節點，以及 2) 作為 NSX Manager 和 NSX Controller 的主機。

表格 3-1. 支援的 KVM 版本

需求	說明
支援的平台	<ul style="list-style-type: none"> ■ RHEL 7.5 ■ RHEL 7.4 ■ Ubuntu 16.04.2 LTS ■ CentOS 7.4

本章包含以下主題：

- [設定 KVM](#)
- [在 KVM CLI 中管理您的客體虛擬機器](#)

設定 KVM

如果您打算以 KVM 作為傳輸節點，或作為 NSX Manager 和 NSX Controller 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 Red Hat) 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 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。

4 安裝 KVM 和橋接器公用程式。

Linux 發行版	命令
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>

5 檢查硬體虛擬化功能。

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

輸出應包含 `vmx`。

6 確認已安裝 KVM 模組。

Linux 發行版	命令
Ubuntu	<pre>kvm-ok INFO: /dev/kvm exists KVM acceleration can be used</pre>
RHEL	<pre>lsmod grep kvm kvm_intel 53484 6 kvm 316506 1 kvm_intel</pre>

- 7 若要讓 KVM 用作 NSX Manager 或 NSX Controller 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 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	<p>編輯 /etc/network/interfaces:</p> <pre> 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 </pre> <p>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:</p> <pre> <network> <name>bridge</name> <forward mode='bridge' /> <bridge name='br0' /> </network> </pre> <p>使用下列命令定義並啟動橋接器網路:</p> <pre> virsh net-define bridge.xml virsh net-start bridge virsh net-autostart bridge </pre>

Linux 發行版

網路組態

您可以使用下列命令檢查橋接器網路的狀態：

```
virsh net-list --all
```

Name	State	Autostart	Persistent
bridge	active	yes	yes
default	active	yes	yes

RHEL

編輯 /etc/sysconfig/network-scripts/ifcfg-management_interface:

```
DEVICE="ens32"
TYPE="Ethernet"
NAME="ens32"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
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"
```

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

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。

執行此步驟後，一旦 KVM 主機設定為傳輸節點，即會建立橋接器介面「`nsx-vtep0.0`」。在 Ubuntu 中，`/etc/network/interfaces` 會包含下列項目：

```
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
```

- 9 若要讓網路變更生效，請重新啟動網路服務 `systemctl restart network`，或將 Linux 伺服器重新開機。

在 KVM CLI 中管理您的客體虛擬機器

NSX Manager 和 NSX Controller 可安裝作為 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，當您開始使用時，可以利用某些簡單的 KVM CLI 命令。

若要在 KVM CLI 中管理您的客體虛擬機器，您可以使用 `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)
```

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。

NSX-T Data Center 部署可以僅有一個 NSX Manager 執行個體。如果在 ESXi 主機上部署 NSX Manager，您可以使用 vSphere High Availability (HA) 功能來確保 NSX Manager 的可用性。

表格 4-1. NSX Manager 部署、平台和安裝需求

需求	說明
支援的部署方法	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
支援的平台	<p>請參閱系統需求。</p> <p>在 ESXi 中，建議將 NSX Manager 應用裝置安裝在共用儲存區。vSphere HA 需要共用儲存區，讓虛擬機器在原始主機失敗時能夠在另一個主機上重新啟動。</p>
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	<ul style="list-style-type: none"> ■ 至少 8 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
主機名稱	<p>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。</p>
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。

表格 4-1. NSX Manager 部署、平台和安裝需求 (續)

需求	說明
系統	<ul style="list-style-type: none"> ■ 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。 ■ 如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。 <p>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。</p> <ul style="list-style-type: none"> ■ 規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。
OVF 權限	<p>確認您擁有在 ESXi 主機上部署 OVF 範本的適當權限。</p> <p>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。</p> <p>OVF 工具版本必須是 4.0 或更新版本。</p>
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 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，則您必須透過 SSH 或從主控台以 **admin** 使用者身分登入 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。

本章包含以下主題：

- [安裝 NSX Manager 和可用應用裝置](#)
- [使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager](#)
- [在 KVM 上安裝 NSX Manager](#)
- [登入新建立的 NSX Manager](#)

安裝 NSX Manager 和可用應用裝置

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

NSX Policy Manager 是一個虛擬應用裝置，可用於管理原則。您可以設定原則以指定 NSX-T Data Center 元件的規則，例如邏輯連接埠、IP 位址和虛擬機器。NSX Policy Manager 規則可讓您設定高層級的使用規則和資源存取規則，無需指定確切的詳細資料即可強制執行這些規則。

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。

備註 建議您使用 vSphere Web Client，而非使用 vSphere Client。如果您的環境中沒有 vCenter Server，請使用 ovftool 來部署 NSX Manager。請參閱[使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager](#)。

程序

- 1 找出 NSX-T Data Center Unified Appliance OVA 或 OVF 檔案。
複製下載 URL，或將 OVA 檔案下載到您的電腦上。
- 2 在 vSphere Web Client 中啟動**部署 OVF 範本精靈**，然後導覽或連結至 .ova 檔案。
- 3 輸入 NSX Manager 的名稱，然後選取資料夾或資料中心。
您輸入的名稱會顯示在詳細目錄中。
您所選取的資料夾會用來將權限套用至 NSX Manager。
- 4 選取用來儲存 NSX Manager 虛擬應用裝置檔案的資料存放區。
- 5 如果您要安裝在 vCenter 中，請選取要部署 NSX Manager 應用裝置的主機或叢集。
- 6 選取 NSX Manager 的連接埠群組或目的地網路。
- 7 指定 NSX Manager 密碼和 IP 設定。
- 8 接受 **nsx-manager** 角色。
 - 從下拉式功能表中，選取 **nsx-policy-manager** 角色，以安裝 NSX Policy Manager 應用裝置。
 - 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。

備註 不支援 **nsx-manager nsx-cloud-service-manager (multi-role)** 角色。

- 9 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 10 開啟 NSX-T Data Center 元件的主控台以追蹤開機程序。
- 11 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 12 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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連線到 NSX Manager GUI。

URL 為 `https://<NSX Manager 的 IP 位址>`。例如，`https://10.16.176.10`。

備註 您必須使用 HTTPS。不支援 HTTP。

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_isSSHEntabled` 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_isSSHEntabled`，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。

先決條件

- 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](#)。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 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。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。

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-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--prop:nsx_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
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:<password>@192.168.110.51
Deploying to VI: vi://root:<password>@192.168.110.51
Transfer Completed
Powering on VM: nsx-manager
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。例如，

```
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
--prop:nsx_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51
```

```
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-manager
Task Completed
Completed successfully
```

- (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。
記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。
- 開啟 NSX-T Data Center 元件的主控台以追蹤開機程序。
- 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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連線到 NSX Manager GUI。

URL 為 `https://<NSX Manager 的 IP 位址>`。例如，`https://10.16.176.10`。

備註 您必須使用 HTTPS。不支援 HTTP。

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。

先決條件

- 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[第 4 章，NSX Manager 安裝](#)。

程序

- 1 下載 NSX Manager QCOW2 映像，並使用 SCP 或 `sync` 將其複製到將執行 NSX Manager 的 KVM 機器。
- 2 (僅限 Ubuntu) 將目前登入的使用者新增為 `libvirtd` 使用者：

```
adduser $USER libvirtd
```


- 3 在您儲存 QCOW2 映像的相同目錄中建立名為 **guestinfo** (不含副檔名) 的檔案，並為其填入 NSX Manager 虛擬機器的內容。

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_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.19"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

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。

- 4 使用 **guestfish** 將 **guestinfo** 檔案寫入 QCOW2 映像中。

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-manager1-build.qcow2 upload guestinfo /config/guestinfo
```

- 5 使用 **virt-install** 命令部署 QCOW2 映像。

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-manager1 --ram
16348 --vcpus 4 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
manager-1.1.0.0.4446302.qcow2,format=qcow2 --nographics

Starting install...
Creating domain...      |    0 B    00:01
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login:
```

在 NSX Manager 開機後，即會顯示 NSX Manager 主控台。

- 6 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 7 開啟 NSX-T Data Center 元件的主控台以追蹤開機程序。
- 8 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 9 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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。

- 10 結束 KVM 主控台。

```
control-]
```

後續步驟

從支援的網頁瀏覽器連線到 NSX Manager GUI。

URL 為 `https://<NSX Manager 的 IP 位址>`。例如，`https://10.16.176.10`。

備註 您必須使用 HTTPS。不支援 HTTP。

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〉。

先決條件

確認已安裝 **NSX Manager**。

程序

- 1 在瀏覽器中，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 捲動至使用者授權合約的底部，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**

NSX Controller 安裝和叢集

NSX Controller 是進階的分散式狀態管理系統，可提供 **NSX-T Data Center** 邏輯交換所需的控制平面功能和路由功能。

NSX Controller 可作為網路內所有邏輯交換器的中央控制點，用來維護所有主機、邏輯交換器和邏輯路由器的相關資訊。**NSX Controller** 可控制執行封包轉送的裝置。這些轉送裝置稱為虛擬交換器。

虛擬交換器 (例如 **NSX** 管理的虛擬分散式交換器 (N-VDS，以前稱為 **hostswitch**) 和 **Open vSwitch (OVS)**) 位於 **ESXi** 和其他 **Hypervisor** (例如 **KVM**) 上。

在生產環境中，您必須具有包含三個成員的 **NSX Controller** 叢集，以避免 **NSX** 控制平面出現任何中斷。每個控制器皆應放置在唯一的 **Hypervisor** 主機上 (總計三個實體 **Hypervisor** 主機)，以避免單一實體 **Hypervisor** 主機故障影響 **NSX** 控制平面。針對沒有任何生產工作負載的實驗室和概念驗證部署，可接受執行單一控制器以節省資源。

表格 5-1. NSX Controller 部署、平台和安裝需求

需求	說明
支援的部署方法	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2 <p>備註 不支援 PXE 開機部署方法。</p>
支援的平台	<p>請參閱系統需求。</p> <p>NSX Controller 可在 ESXi 上作為虛擬機器和 KVM。</p> <p>備註 不支援 PXE 開機部署方法。</p>
IP 位址	<p>NSX Controller 必須要有靜態 IP 位址。IP 位址在安裝後即無法變更。</p> <p>規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。</p>
NSX-T Data Center 應用裝置密碼	<ul style="list-style-type: none"> ■ 至少 8 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

表格 5-1. NSX Controller 部署、平台和安裝需求 (續)

需求	說明
主機名稱	安裝 NSX Controller 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 。
VMware Tools	在 ESXi 上執行的 NSX Controller 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 。
連接埠	確認所需連接埠已開啟。請參閱 連接埠和通訊協定 。

NSX Controller 安裝案例

重要 當您從 OVA 或 OVF 檔案安裝 NSX Controller 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，則您必須透過 SSH 或從主控台以 **admin** 使用者身分登入 NSX Controller。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 Controller，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 Controller。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

- 請勿使用根權限來安裝精靈或應用程式。使用根權限來安裝精靈或應用程式會使支援合約無效。僅在 VMware 支援團隊提出要求時使用根權限。
- 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。
從 OVA 檔案部署 NSX Controller 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。

本章包含以下主題：

- [從 NSX Manager 自動安裝控制器和叢集](#)
- [使用 GUI 在 ESXi 上安裝 NSX Controller](#)

- 使用命令列 **OVF Tool** 在 **ESXi** 上安裝 **NSX Controller**
- 在 **KVM** 上安裝 **NSX Controller**
- 將 **NSX Controller** 加入 **NSX Manager**
- 初始化控制叢集以建立控制叢集主節點
- 將其他 **NSX Controller** 加入叢集主節點

從 NSX Manager 自動安裝控制器和叢集

您可以將 **NSX Manager** 設定為要在 **vSphere ESXi** 主機上自動安裝控制器。在部署後，這些控制器會自動新增至該 **vSphere ESXi** 主機 (由 **vCenter Server** 所管理) 上的控制器叢集。或者，您也可以使用 **NSX Manager REST API** 來自動安裝控制器叢集。

NSX Manager 可讓您將其他控制器自動部署到手動部署的現有叢集。但是，若要從叢集刪除手動新增的控制器，您必須手動將其從叢集中移除。

支援的使用案例

- 建立單節點叢集
- 建立多節點叢集
- 將節點新增至現有叢集
- 從正常運作的叢集中刪除自動部署的控制器

使用 NSX Manager UI 設定控制器和叢集的自動安裝

將 **NSX Manager** 設定為要將控制器自動安裝在 **vCenter Server** 所管理的 **vSphere ESXi** 主機上。在安裝後，這些控制器會自動新增至 **vSphere ESXi** 主機上的控制器叢集。

先決條件

- 部署 **NSX Manager**。
- 部署 **vCenter Server** 和 **vSphere ESXi** 主機。
- 向 **vCenter Server** 登錄 **vSphere ESXi** 主機。
- **vSphere ESXi** 主機必須具有足夠的 CPU、記憶體和硬碟資源，來支援 12 個 vCPU、48 GB RAM 和 360 GB 儲存區。

程序

- 1 登入 **NSX Manager**，網址為 `https://<nsxmanagerIPAddress>/`
- 2 在 **NSX Manager UI** 中，如果沒有登錄的 **vCenter**，請前往**網狀架構**面板，按一下**計算管理程式**，然後新增計算管理程式。
- 3 在 [系統] 頁面中，按一下**新增控制器**。
- 4 在 [一般屬性] 頁面中，輸入頁面上所需的值。

- 5 選取**計算管理程式**。
- 6 (選用) 您可以啟用 SSH。
- 7 (選用) 您可以啟用根存取。
- 8 (選用) 如果您對現有叢集新增節點，請啟用 **[加入現有叢集]**。
- 9 輸入並確認初始化與形成叢集所需的共用密碼金鑰。

備註 新增到此叢集的所有控制器節點都必須使用相同的共用密碼金鑰。

- 10 輸入控制器認證。
- 11 按**下一步**。
- 12 在 **[控制器]** 頁面上，按一下**新增控制器**。
- 13 針對控制器節點輸入有效的主機名稱或完整網域名稱。
- 14 選取叢集。
- 15 (選用) 選取資源集區。資源集區僅提供計算資源集區以部署控制器節點。指派專屬的儲存資源。
- 16 (選用) 選取主機。
- 17 選取資料存放區。
- 18 選取主機用來與主機本身中的不同元件進行通訊的管理介面。
- 19 輸入靜態 IP 位址與連接埠詳細資料 (**<IPAddress>/<PortNumber>**) 及網路遮罩。
- 20 您可以新增多個控制器。按一下 **+** 按鈕，輸入控制器詳細資料，然後開始部署。
- 21 按一下**完成**。
自動安裝控制器的作業便會開始。控制器會先向 **NSX Manager** 登錄，然後形成叢集或加入現有叢集。
- 22 確認控制器是否已向 **NSX Manager** 登錄。
 - a 登入 **NSX Manager** 主控台。
 - b 輸入 `# get management-cluster status`。
管理叢集狀態必須為穩定。
 - c 或者，從 **NSX Manager UI** 確認該管理員連線已啟動。
- 23 確認控制叢集狀態。
 - a 登入控制器 CLI 主控台。
 - b 輸入 `# get control-cluster status`
控制器叢集狀態必須為穩定。
 - c 或者，從 **NSX Manager UI** 確認叢集連線已啟動。

後續步驟

使用 API 將 NSX Manager 設定為自動安裝控制器和叢集。請參閱[使用 API 設定控制器和叢集的自動安裝](#)。

使用 API 設定控制器和叢集的自動安裝

使用 API 將 NSX Manager 設定為要將控制器自動安裝在 vCenter Server 所管理的 vSphere ESXi 主機上。控制器安裝好之後，便會自動新增至 vSphere ESXi 主機上的控制器叢集。

程序

- 1 觸發控制器叢集的自動建立程序之前，您必須根據 POST API 的裝載需求，擷取 vCenter Server 識別碼、計算識別碼、儲存區識別碼和網路識別碼。
- 2 登入 vCenter Server。
`https://<vCenterServer_IPAddress>/mob.`
- 3 在 [值] 資料行中，按一下內容。
- 4 在 [內容屬性] 頁面中，前往 [值] 資料行以搜尋資料中心，然後按一下群組連結。
- 5 在 [群組內容] 頁面中，前往 [值] 資料行，然後按一下資料中心連結。
- 6 在 [資料中心內容] 頁面中，複製您要用來建立控制器叢集的資料存放區值和網路值。
- 7 按一下 **HostFolder** 連結。
- 8 在 [群組內容] 頁面中，複製您要用來建立控制器叢集的叢集值。
- 9 若要擷取 vCenter Server 識別碼，請前往 NSX Manager UI，並從 [計算管理程式] 頁面中複製其識別碼。
- 10 POST `https://<nsx-manager>/api/v1/cluster/nodes/deployments`

```
REQUEST
{
  "deployment_requests": [
    {
      "roles": ["CONTROLLER"],
      "user_settings": {
        "cli_password": "CLIp4$$w4rd",
        "root_password": "ROOTp4$$w4rd"
      },
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "default_gateway_addresses": [
          "10.33.79.253"
        ],
        "management_port_subnets": [
```



```

        {
            "ip_addresses": [
                "10.33.79.64"
            ],
            "prefix_length": "22"
        }
    ]
}
},
{
    "roles": ["CONTROLLER"],
    "user_settings": {
        "cli_password": "VMware$123",
        "root_password": "VMware$123"
    },

    "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-1",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12"
        "default_gateway_addresses": [
            "10.33.79.253"
        ],
        "management_port_subnets": [
            {
                "ip_addresses": [
                    "10.33.79.65"
                ],
                "prefix_length": "22"
            }
        ]
    }
}
],
        "deployment_config": {
            "placement_type": "VsphereClusterNodeVMDeploymentConfig",
            "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
            "management_network_id": "network-13",
            "hostname": "controller-0",
            "compute_id": "domain-s9",
            "storage_id": "datastore-12",
            "default_gateway_addresses": [
                "10.33.79.253"
            ],
            "management_port_subnets": [
                {
                    "ip_addresses": [
                        "10.33.79.66"
                    ],
                    "prefix_length": "22"
                }
            ]
        }
    ]
}

```

```

    }
  },

  "clustering_config": {
    "clustering_type": "ControlClusteringConfig",
    "shared_secret": "123456",
    "join_to_existing_cluster": false
  }
}

Response
{
  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]",
        "cli_username": "admin"
      },
      "vm_id": "71f02260-644f-4482-aa9a-ab8570bb49a3",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "default_gateway_addresses": [
          "10.33.79.253"
        ],
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "management_port_subnets": [
          {
            "ip_addresses": [
              "10.33.79.64"
            ],
            "prefix_length": 22
          }
        ]
      }
    },

    {
      "form_factor": "SMALL"
    },

    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]",
        "cli_username": "admin"
      },

      "vm_id": "38029a2b-b9bc-467f-8138-aef784e802cc",

```

```

    "roles": [
      "CONTROLLER"
    ],
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-1",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12"
    },
    "form_factor": "MEDIUM"
  }
]
}

```

- 11** 您可以使用 API 呼叫檢視部署狀態。GET <https://<nsx-manager>/api/v1/cluster/nodes/deployments>

```

{
  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "12f563af-af9f-48f3-848e-e9257c8740b0",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "15145422-47a1-4c55-81da-01d953151d1f",
        "management_network_id": "network-158",
        "hostname": "controller-0",
        "compute_id": "domain-c154",
        "storage_id": "datastore-157"
      },
      "form_factor": "SMALL",
    },
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "cc21854c-265b-42de-af5f-05448c00777a",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",

```

```

    "vc_id": "feb17651-49a7-4ce6-88b4-41d3f624e53b",
    "management_network_id": "network-158",
    "hostname": "controller-0",
    "compute_id": "domain-c154",
    "storage_id": "datastore-157"
  },

  "form_factor": "MEDIUM",
}
]
}

```

後續步驟

刪除叢集。請參閱[刪除 NSX Controller](#)。

刪除 NSX Controller

從叢集中刪除 NSX Controller。

程序

- 1 登入 <https://<nsx-manager-ip>/>
- 2 按一下 **系統 > 元件**。
- 3 在 [控制器叢集] 下，找到 NSX Controller。
- 4 按一下 **設定** 圖示，然後按一下 **刪除**。
- 5 按一下 **確認**。

NSX-T Data Center 隨即會中斷叢集與 NSX Controller 的連結、將其從 NSX Manager 解除登錄並關閉其電源，然後刪除該 NSX Controller。

後續步驟

使用 GUI 在 vSphere ESXi 主機上安裝 NSX Controller。請參閱[使用 GUI 在 ESXi 上安裝 NSX Controller](#)。

使用 GUI 在 ESXi 上安裝 NSX Controller

如果您偏好採用互動式 NSX Controller 安裝，您可以使用 UI 型虛擬機器管理工具，例如連線至 vCenter Server 的 vSphere Client。

如果密碼不符合需求，則安裝仍會成功。不過，當您首次登入時，系統會提示您變更密碼。

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。

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。

先決條件

- 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](#)。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 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。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。
- 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-controller*。
- 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。

程序

- 1 找出 NSX Controller OVA 或 OVF 檔案。
複製下載 URL，或將 OVA 檔案下載到您的電腦上。
- 2 在管理工具中啟動**部署 OVF 範本**精靈，然後導覽或連結至 .ova 檔案。
- 3 輸入 NSX Controller 的名稱，然後選取資料夾或資料中心。
您輸入的名稱會顯示在詳細目錄中。
您所選取的資料夾會用來將權限套用至 NSX Controller。
- 4 選取用來儲存 NSX Controller 虛擬應用裝置檔案的資料存放區。
- 5 如果您正在使用 vCenter，請選取要部署 NSX Controller 應用裝置的主機或叢集。
- 6 選取 NSX Controller 的連接埠群組或目的地網路。
- 7 指定 NSX Controller 密碼和 IP 設定。
- 8 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 9 開啟 NSX-T Data Center 元件的主控台以追蹤開機程序。

- 10** 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 11** 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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

將 NSX Controller 加入管理平面。請參閱[將 NSX Controller 加入 NSX Manager](#)。

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Controller

如果您偏好將 NSX Controller 安裝自動化，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 Controller 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 Controller，但無法以根使用者身分登入。

先決條件

- 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](#)。
- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 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。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。
- OVF Tool 4.0 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-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

- 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-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<vcenter_password>@192.168.110.24/?ip=192.168.110.51
```

- (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 開啟 NSX-T Data Center 元件的主控制台以追蹤開機程序。
- 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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

將 NSX Controller 加入管理平面。請參閱[將 NSX Controller 加入 NSX Manager](#)。

在 KVM 上安裝 NSX Controller

NSX Controller 是網路內所有邏輯交換器的中央控制點，用來維護所有主機、邏輯交換器和分散式邏輯路由器的相關資訊。

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。

先決條件

- KVM 設定。請參閱[設定 KVM](#)。
- 在 KVM 主機上部署 QCOW2 映像的權限。

程序

- 1 將 NSX Controller QCOW2 映像下載至 `/var/lib/libvirt/images` 目錄。
- 2 (僅限 Ubuntu) 將目前登入的使用者新增為 `libvirtd` 使用者：

```
adduser $USER libvirtd
```

- 3 在您儲存 QCOW2 映像的相同目錄中建立名為 `guestinfo` (不含副檔名) 的檔案，並為其填入 NSX Controller 虛擬機器的內容。

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_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-Controller1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.34"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

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 Controller 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 Controller，但無法以根使用者身分登入。

- 4 使用 `guestfish` 將 `guestinfo` 檔案寫入 QCOW2 映像中。

如果您要建立多個 NSX Controller，請為每個控制器建立個別的 QCOW2 映像複本。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-controller1-build.qcow2 upload guestinfo /config/guestinfo
```

5 使用 virt-install 命令部署 QCOW2 映像。

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-controller1 --ram
16384 --vcpus 2 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
controller-release_version_number.qcow2,format=qcow2 --nographics --noautoconsole
```

在 NSX Controller 開機後，即會顯示 NSX Controller 主控台。

6 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

7 開啟 NSX-T Data Center 元件的主控台以追蹤開機程序。

8 在 NSX-T Data Center 元件開機後，請以 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。

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

9 確認 NSX-T Data Center 元件具有必要的連線。

確認您可以執行下列工作。

- 從另一個機器對 NSX-T Data Center 元件執行 Ping 偵測。
- NSX-T Data Center 元件可以對其預設閘道執行 Ping 偵測。
- NSX-T Data Center 元件可以使用管理介面，對位於相同網路中作為 NSX-T Data Center 元件的 Hypervisor 主機執行 Ping 偵測。
- NSX-T Data Center 元件可以對其 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-T Data Center 元件。

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

將 NSX Controller 加入管理平面。請參閱[將 NSX Controller 加入 NSX Manager](#)。

將 NSX Controller 加入 NSX Manager

將 NSX Controller 加入 NSX Manager，可確保 NSX Manager 與 NSX Controller 能夠相互通訊。

先決條件

- 確認已安裝 NSX Manager。
- 確認您具有登入 NSX Manager 和 NSX Controller 應用裝置的管理員權限。

程序

- 1 開啟 NSX Manager 的 SSH 工作階段。
- 2 開啟每個 NSX Controller 應用裝置的 SSH 工作階段。
例如，NSX-Controller1、NSX-Controller2、NSX-Controller3。

- 3 在 NSX Manager 上，執行 `get certificate api thumbprint` 命令。

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

- 4 在每個 NSX Controller 應用裝置上，執行 `join management-plane` 命令。

```
NSX-Controller1> join management-plane NSX-Manager-IP-address username admin thumbprint <NSX-Manager-thumbprint>

Password for API user: <NSX-Manager-password>
Node successfully registered and controller restarted
```

在每個已部署的 NSX Controller 節點上執行此命令。

請提供下列資訊：

- 具有選用連接埠號碼之 NSX Manager 的 IP 位址
 - NSX Manager 的使用者名稱
 - NSX Manager 的憑證指紋
 - NSX Manager 的密碼
- 5 在您的 NSX Controller 上執行 `get managers` 命令以確認結果。

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

- 6 在 NSX Manager 應用裝置上執行 `get management-cluster status` 命令，並確定 NSX Controller 已列出。

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE
```

```
Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

後續步驟

初始化控制叢集。請參閱[初始化控制叢集以建立控制叢集主節點](#)。

初始化控制叢集以建立控制叢集主節點

在您的 NSX-T Data Center 部署中安裝第一個 NSX Controller 之後，您可以初始化控制叢集。即使您要設定的是僅具有一個控制器節點的小型概念驗證環境，仍須初始化控制叢集。若未初始化控制叢集，控制器將無法與 Hypervisor 主機通訊。在叢集中，只需初始化一個控制器。

先決條件

- 安裝至少一個 NSX Controller。
- 將 NSX Controller 加入管理平面。
- 確認您具有登入 NSX Controller 應用裝置的管理員權限。
- 指派共用密碼。共用密碼是使用者定義的共用密碼 (例如「secret123」)。

程序

- 1 開啟 NSX Controller 的 SSH 工作階段。
- 2 執行 `set control-cluster security-model shared-secret secret <secret>` 命令，並在出現提示時輸入共用密碼。

- 3 執行 `initialize control-cluster` 命令。

此命令會使這個控制器成為控制叢集主節點。

例如：

```
NSX-Controller1> initialize control-cluster
Control cluster initialization successful.
```

- 4 執行 `get control-cluster status verbose` 命令。

確認 `is master` 和 `in majority` 皆為 `true`，而狀態為 `active`，且 Zookeeper Server IP 為 `reachable`, `ok`。

```
nsx-controller1> get control-cluster status verbose
NSX Controller Status:

uuid: 78d5b561-4f66-488d-9e53-089735eac1c1
is master: true
in majority: true
uuid                                address                        status
78d5b561-4f66-488d-9e53-089735eac1c1 192.168.110.34                active
```

Cluster Management Server Status:

uuid id	vpn address	rpc address status	rpc port	global
557a911f-41fd-4977-9c58-f3ef55b3efe7	192.168.110.34	7777		
1	169.254.1.1	connected		

Zookeeper Ensemble Status:

Zookeeper Server IP: 10.0.0.1, reachable, ok
 Zookeeper version: 3.5.1-alpha--1, built on 03/08/2016 01:18 GMT
 Latency min/avg/max: 0/0/1841
 Received: 212095
 Sent: 212125
 Connections: 5
 Outstanding: 0
 Zxid: 0x10000017a
 Mode: leader
 Node count: 33
 Connections: /10.0.0.1:51726[1]
 (queued=0, recved=60324, sent=60324, sid=0x100000f14a10003, lop=PING, est=1459376913497, to=30000, lcxid=0x8, lzxid=0x10000017a, lresp=604617273, llat=0, minlat=0, avglat=0, maxlat=1088)
 /10.0.0.1:35462[0] (queued=0, recved=1, sent=0)
 /10.0.0.1:51724[1]
 (queued=0, recved=45786, sent=45803, sid=0x100000f14a10001, lop=GETC, est=1459376911226, to=40000, lcxid=0x21e, lzxid=0x10000017a, lresp=604620658, llat=0, minlat=0, avglat=0, maxlat=1841)
 /10.0.0.1:51725[1]
 (queued=0, recved=60328, sent=60333, sid=0x100000f14a10002, lop=PING, est=1459376913455, to=30000, lcxid=0xc, lzxid=0x10000017a, lresp=604618294, llat=0, minlat=0, avglat=0, maxlat=1356)
 /10.0.0.1:51730[1]
 (queued=0, recved=45315, sent=45324, sid=0x100000f14a10006, lop=PING, est=1459376914516, to=40000, lcxid=0x49, lzxid=0x10000017a, lresp=604623243, llat=0, minlat=0, avglat=0, maxlat=1630)

後續步驟

將其他 NSX Controller 新增至控制叢集。請參閱[將其他 NSX Controller 加入叢集主節點](#)。

將其他 NSX Controller 加入叢集主節點

擁有 NSX Controller 多節點叢集有助於確保永遠至少會有一個 NSX Controller 可供使用。

先決條件

- 至少安裝三個 NSX Controller 應用裝置。
- 確認您具有登入 NSX Controller 應用裝置的管理員權限。
- 確定 NSX Controller 節點已加入管理平面。請參閱[將 NSX Controller 加入 NSX Manager](#)。
- 初始化控制叢集以建立控制叢集主節點。只需初始化第一個控制器。
- 在 `join control-cluster` 命令中，您必須使用 IP 位址，而非網域名稱。

- 如果您使用 vCenter，且要將 NSX-T Data Center 控制器部署至相同的叢集，請務必設定 DRS 反相似性規則。反相似性規則可防止 DRS 將多個節點移轉至單一主機。

程序

- 1 開啟您每個 NSX Controller 應用裝置的 SSH 工作階段。

例如，NSX-Controller1、NSX-Controller2 和 NSX-Controller3。在此範例中，NSX-Controller1 已初始化控制叢集，並且是控制叢集主節點。

- 2 在非主要 NSX Controller 上，以共用密碼執行 `set control-cluster security-model` 命令。為 NSX-Controller2 和 NSX-Controller3 輸入的共用密碼，必須符合在 NSX-Controller1 上輸入的共用密碼。

例如：

```
NSX-Controller2> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

```
NSX-Controller3> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

- 3 在非主要 NSX Controller 上，執行 `get control-cluster certificate thumbprint` 命令。

命令輸出是對每個 NSX Controller 而言都是唯一的數字字串。

例如：

```
NSX-Controller2> get control-cluster certificate thumbprint
...
```

```
NSX-Controller3> get control-cluster certificate thumbprint
...
```

- 4 在主要 NSX Controller 上，執行 `join control-cluster` 命令。

請提供下列資訊：

- 具有非主要 NSX Controller (在此範例中為 NSX-Controller2 和 NSX-Controller3) 之選用連接埠號碼的 IP 位址

■ 非主要 NSX Controller 的憑證指紋

請勿以平行方式在多個控制器上執行 `join` 命令。請務必在一個控制器加入完成後，再加入另一個控制器。

```
NSX-Controller1> join control-cluster <NSX-Controller2-IP> thumbprint <nsx-controller2's-
thumbprint>
Node 192.168.210.48 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

請執行 `get control-cluster status` 命令以確定 NSX-Controller2 已加入叢集。

```
NSX-Controller1> join control-cluster <NSX-Controller3-IP> thumbprint <nsx-controller3's-
thumbprint>
Node 192.168.210.49 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

請執行 `get control-cluster status` 命令以確定 NSX-Controller3 已加入叢集。

5 在兩個已加入控制叢集主節點的 NSX Controller 節點上，執行 `activate control-cluster` 命令。

備註 請勿以平行方式在多個 NSX Controller 上執行 `activate` 命令。請確保各個控制器皆啟用完成後，再啟用另一個控制器。

例如：

```
NSX-Controller2> activate control-cluster
Control cluster activation successful.
```

在 NSX-Controller2 上執行 `get control-cluster status verbose` 命令，並確定 Zookeeper Server IP 為 `reachable, ok`。

```
NSX-Controller3> activate control-cluster
Control cluster activation successful.
```

在 NSX-Controller3 上執行 `get control-cluster status verbose` 命令，並確定 Zookeeper Server IP 為 `reachable, ok`。

6 執行 `get control-cluster status` 命令以確認結果。

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
  uuid                                address                status
  ----                                -
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.210.47         active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.210.48         active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.210.49         active
```

第一個列出的 UUID 會用於整體的控制叢集。每個 NSX Controller 節點皆具有一個 UUID。

如果您嘗試將控制器加入叢集，但命令 `set control-cluster security-model` 或 `join control-cluster` 失敗，則叢集組態檔可能會處於不一致的狀態。

若要解決此問題，請執行下列步驟：

- 在您嘗試要加入叢集的 NSX Controller 上，執行 `deactivate control-cluster` 命令。
- 在主要控制器上，如果 `get control-cluster status` 或 `get control-cluster status verbose` 命令顯示失敗控制器的相關資訊，請執行 `detach control-cluster <IP address of failed controller>` 命令。

後續步驟

部署 NSX Edge。請參閱[第 6 章，NSX Edge 安裝](#)。

NSX Edge 安裝

NSX Edge 可提供在 NSX-T Data Center 部署以外的路由服務和網路連線。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。

表格 6-1. NSX Edge 部署、平台和安裝需求

需求	說明
支援的部署方法	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 至少 8 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
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 。
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 系統需求 。
NSX 連接埠	<p>確認所需連接埠已開啟。請參閱連接埠和通訊協定。</p> <p>如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 NSX-T Data Center 應用裝置放在管理虛擬機器網路上。</p>

表格 6-1. NSX Edge 部署、平台和安裝需求 (續)

需求	說明
IP 位址	<p>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。</p> <p>規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。</p> <p>不支援 IPv6 格式。</p>
OVF 範本	<ul style="list-style-type: none"> ■ 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 <i>nsx-manager</i>。 ■ 可部署 OVF 範本的管理工具，例如 vCenter Server 或 vSphere Client。 <p>OVF 部署工具必須支援可允許手動設定的組態選項。</p> <ul style="list-style-type: none"> ■ 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，則您必須透過 SSH 或從主控台以 **admin** 使用者身分和密碼 **vmware** 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。

本章包含以下主題：

- [NSX Edge 網路設定](#)
- [從 NSX Manager 自動部署 NSX Edge 虛擬機器](#)
- [使用 vSphere GUI 在 ESXi 上安裝 NSX Edge](#)
- [使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge](#)
- [使用 ISO 檔案與 PXE 伺服器安裝 NSX Edge](#)
- [將 NSX Edge 加入管理平面](#)

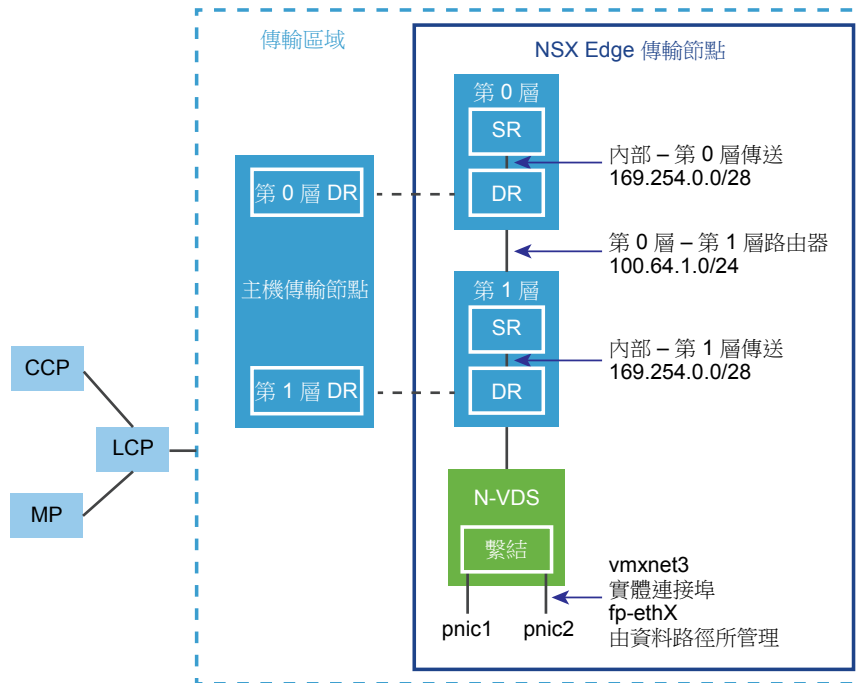
NSX Edge 網路設定

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 Edge 節點是具有容量集區的服務應用裝置，專門用於執行無法散佈到 Hypervisor 的網路服務。您可以將首次部署的 Edge 節點視為空的容器。

圖 6-1: NSX Edge 的高階概觀



NSX Edge 節點是一種應用裝置，可提供用來連線到實體基礎結構的實體 NIC。這些功能包含：

- 對實體基礎結構的連線
- NAT
- DHCP 伺服器

- 中繼資料 Proxy
- Edge 防火牆

如果設定了上述其中一項服務，或在邏輯路由器上定義了用來連線到實體基礎結構的上行，**NSX Edge** 節點上便會具現化 **SR**。**NSX Edge** 節點也是一個傳輸節點 (正如同 **NSX-T Data Center** 中的運算節點)，且與運算節點類似，**NSX Edge** 可以連線至多個傳輸區域，一個用於覆疊，另一個則用於與外部裝置的南北向對等連線。**NSX Edge** 上有兩個傳輸區域：

覆疊傳輸區域 - 加入 **NSX-T Data Center** 網域的虛擬機器所發出的任何流量可能必須要能夠連線至外部裝置或網路。這一般會稱為外部南北向流量。**NSX Edge** 節點會負責將從運算節點收到的覆疊流量解除封裝，以及將傳送至運算節點的流量封裝起來。

VLAN 傳輸區域 - 除了封裝或解除密封流量的功能外，**NSX Edge** 節點也需要有 **VLAN** 傳輸區域，才能提供對實體基礎結構的上行連線。

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** 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。

NSX Edge 的高階概觀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。

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

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。傳輸節點的資料平面中所涉及的主要元件是 N-VDS。N-VDS 會在傳輸節點上的執行中元件之間轉送流量，例如，在虛擬機器之間或在內部元件和實體網路之間。如果是後面這種情況，N-VDS 就必須在傳輸節點上擁有一或多個實體介面 (pNIC)。和其他虛擬交換器一樣，N-VDS 彼此之間不能共用實體介面。在使用另外一組 pNIC 時，則可以與其他 N-VDS 共存。

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。

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。

如需關於傳輸區域的詳細資訊，請參閱[關於傳輸區域](#)。

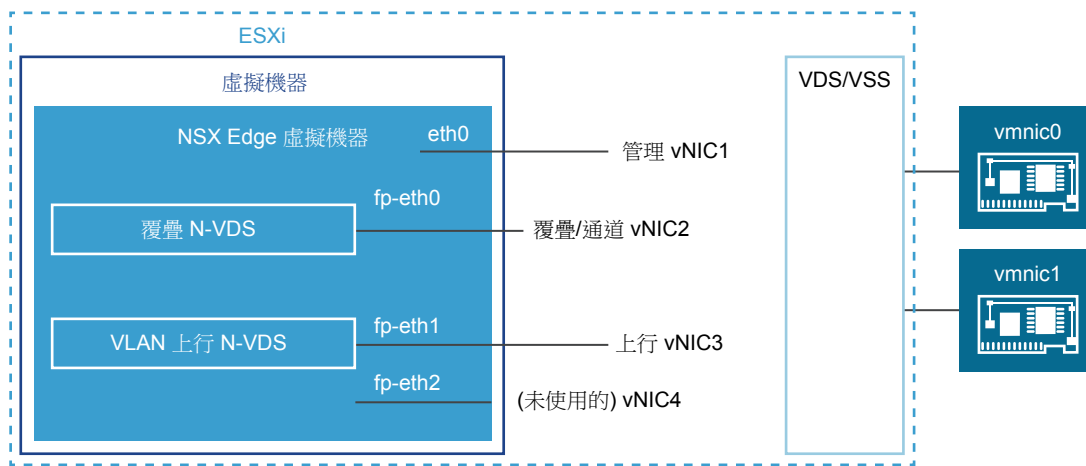
虛擬應用裝置/虛擬機器 NSX Edge 網路

NSX Edge 虛擬機器有四個內部介面：eth0、fp-eth0、fp-eth1 和 fp-eth2。eth0 會保留供管理用途使用，其餘介面則會指派給 DPDK 快速路徑。這些介面會配置給 TOR 交換器的上行使用，以及供 NSX-T Data Center 覆疊通道使用。您可以將介面彈性指派給上行或覆疊。例如，fp-eth0 可以和 fp-eth1、fp-eth2 一起指派給覆疊流量，也可以將後兩者同時指派給上行流量。

在 vSphere 分散式交換器或 vSphere 標準交換器上，您必須對 NSX Edge 配置至少兩個 vmnic 以提供備援功能。

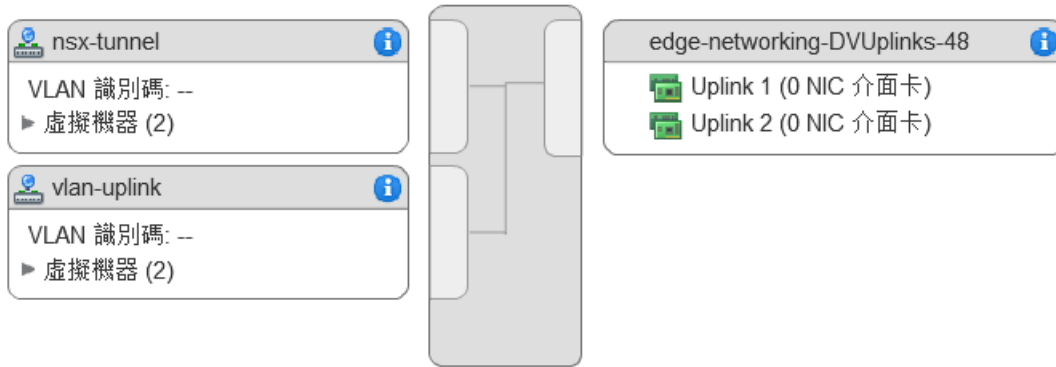
在下列實體拓撲範例中，eth0 會用於管理網路、fp-eth0 會用於 NSX-T Data Center 覆疊流量、fp-eth1 會用於 VLAN 上行，fp-eth2 則不會用到。如果未用到 fp-eth2，您必須將其中斷連線。

圖 6-2：一項適用於 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。

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)**。

NSX Edge 虛擬機器可以安裝在 vSphere 分散式交換器或 vSphere 標準交換器上。

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。

您可以將多個 NSX Edge 虛擬機器安裝在單一主機上，以利用相同的管理、VLAN 和覆疊連接埠群組。

針對 ESXi 主機 (具有 vSphere 而沒有 N-VDS) 上部署的 NSX Edge 虛擬機器，您必須執行下列操作：

- 為這個 NSX Edge 上執行的 DHCP 伺服器啟用偽造的傳輸。
- 針對 NSX Edge 虛擬機器啟用混合模式以接收未知單點傳播封包，因為依預設會停用 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。

裸機 NSX Edge 網路

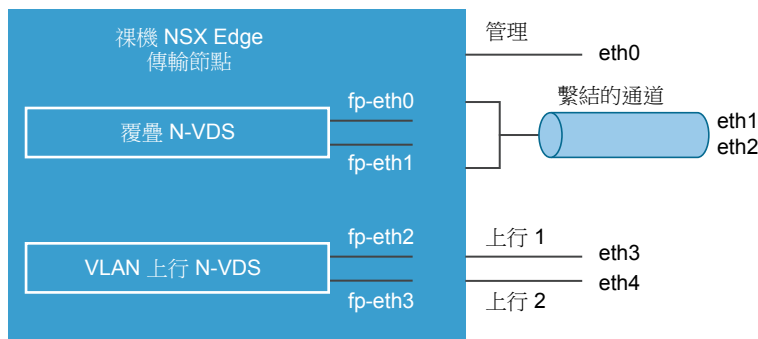
NSX-T Data Center 裸機 NSX Edge 會在實體伺服器上執行，且會使用 ISO 檔或 PXE 開機來安裝。建議您將裸機 NSX Edge 用於除了第 3 層單點傳播轉送外，還需要 NAT、防火牆和負載平衡器等服務的生產環境中。裸機 NSX Edge 與虛擬機器 NSX Edge 的機器尺寸差別在於效能。其可提供亞秒級的聚合、更快速的容錯移轉和更高的輸送量。

在安裝裸機 NSX Edge 節點時，會為管理保留一個專用介面。如果需要備援，則可以使用兩個 NIC 以讓管理平面具備高可用性。這些管理介面也可以是 1G。

裸機 NSX Edge 節點最多支援將 8 個實體 NIC 用於覆疊流量和 Top-of-Rack (TOR) 交換器的上行流量。對於伺服器上的這 8 個實體 NIC，系統會依照命名配置「fp-ethX」分別為其建立一個內部介面。這些內部介面會指派給 DPDK 快速路徑。在為覆疊或上行連線指派 fp-eth 介面時，您可以有完整的處理彈性。

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 6-3：一項適用於裸機 NSX Edge 網路的建議連結設定



從 NSX Manager 自動部署 NSX Edge 虛擬機器

您可以在 NSX Manager UI 中設定 NSX Edge，並將 NSX Edge 自動部署在 vCenter Server 中。

先決條件

- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。
- 如果 vCenter Server 已登錄為 NSX-T Data Center 中的計算管理程式，則可以使用 NSX Manager UI 將主機設定為 NSX Edge 節點，然後在 vCenter Server 上進行自動部署。
- 確認要安裝 NSX Edge 的 vCenter Server 資料存放區至少有 120GB 可供使用。
- 確認 vCenter Server 叢集或主機可存取組態中的特定網路和資料存放區。

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取 **網狀架構 > 節點 > Edge > 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 選取組態大小：小型、中型或大型。
系統需求會隨著組態大小而有所不同。
- 6 指定系統的 CLI 和根密碼。
對根密碼和 CLI 管理員密碼的限制，同樣也適用於自動部署。
- 7 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。
- 8 針對計算管理程式，請從下拉式功能表中選取叢集，或指派資源集區。
- 9 選取用來儲存 NSX Edge 虛擬機器檔案的資料存放區。
- 10 選取要部署 NSX Edge 虛擬機器的叢集。
建議您將 NSX Edge 新增至提供網路管理公用程式的叢集中。
- 11 選取主機或資源集區。一次只能新增一台主機。
- 12 選取 IP 位址，並輸入要放置 NSX Edge 介面的管理網路 IP 位址和路徑。必須以 CIDR 格式輸入 IP 位址。
管理網路必須可以存取 NSX Manager。必須從 DHCP 伺服器接收其 IP 位址。您可以在 NSX Edge 部署後變更網路。
- 13 如果管理網路 IP 位址不屬於與 NSX Manager 網路相同的第 2 層，請新增預設閘道。
確認 NSX Manager 與 NSX Edge 管理網路之間有可用的第 3 層連線。

NSX Edge 部署約 1-2 分鐘即可完成。您可以在 UI 中追蹤部署的即時狀態。

後續步驟

如果 NSX Edge 部署失敗，請導覽至 `/var/log/cm-inventory/cm-inventory.log` 和 `/var/log/proton/nsxapi.log` 檔案以進行問題的疑難排解。

在您將 NSX Edge 新增至 NSX Edge 叢集或設定為傳輸節點之前，請確定新建立的 NSX Edge 節點顯示為「節點就緒」。

使用 vSphere GUI 在 ESXi 上安裝 NSX Edge

如果您偏好採用互動式 NSX Edge 安裝，您可以使用 UI 型虛擬機器管理工具，例如連線至 vCenter Server 的 vSphere Client。

在此版本的 NSX-T Data Center 中，IPv6 不受支援。

先決條件

- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。

程序

- 1 找出 NSX Edge OVA 或 OVF 檔案。
複製下載 URL，或將 OVA 檔案下載到您的電腦上。
- 2 在管理工具中啟動**部署 OVF 範本精靈**，然後導覽或連結至 .ova 檔案。
- 3 輸入 NSX Edge 的名稱，然後選取資料夾或 vCenter Server 資料中心。
您輸入的名稱會顯示在詳細目錄中。
您所選取的資料夾會用來將權限套用至 NSX Edge。
- 4 選取組態大小：小型、中型或大型。
系統需求會隨著組態 NSX Edge 部署大小而有所不同。請參閱[系統需求](#)。
- 5 選取用來儲存 NSX Edge 虛擬應用裝置檔案的資料存放區。
- 6 如果您要安裝在 vCenter Server 中，請選取要部署 NSX Edge 應用裝置的主機或叢集。
- 7 選取要放置 NSX Edge 介面的網路。
您可以在 NSX Edge 部署後變更網路。
- 8 指定 NSX Edge 密碼和 IP 設定。
- 9 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。
記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。
- 10 開啟 NSX Edge 的主控制台以追蹤開機程序。
如果主控制台視窗並未開啟，請確定已允許快顯視窗。
- 11 在 NSX Edge 啟動後，使用管理員權限登入 CLI，使用者名稱為 **admin**，密碼為 **default**。

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 執行 `get interface eth0` 命令以確認 IP 位址已按預期套用。

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

Interface: eth0
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
...
```

如有需要，執行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理介面。(選用) 您可以使用 `start service ssh` 命令啟動 SSH 服務。

14 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。

15 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 DHCP 指派錯誤的 NIC 作為管理，請完成工作以修正問題。

- a 登入 CLI 並輸入 `stop service dataplane` 命令。
- b 輸入 `set interface eth0 dhcp plane mgmt` 命令。
- c 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 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。

在此版本的 NSX-T Data Center 中，IPv6 不受支援。

先決條件

- 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](#)。

- 如果您還沒有目標虛擬機器連接埠群組網路，請建立。建議將 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。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T Data Center 中，IPv6 不受支援。
- 請參閱 [NSX Edge 網路設定](#) 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 4.0 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
```

- (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 開啟 NSX Edge 的主控制台以追蹤開機程序。
- 在 NSX Edge 啟動後，使用管理員權限登入 CLI，使用者名稱為 **admin**，密碼為 **default**。
- 執行 `get interface eth0` 命令以確認 IP 位址已按預期套用。

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

Interface: eth0
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
...
```

如有需要，執行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理介面。(選用) 您可以使用 `start service ssh` 命令啟動 SSH 服務。

- 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 DHCP 指派錯誤的 NIC 作為管理，請完成工作以修正問題。

- 登入 CLI 並輸入 `stop service dataplane` 命令。
- 輸入 `set interface eth0 dhcp plane mgmt` 命令。
- 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 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 ISO 檔案與 PXE 伺服器安裝 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 和 NSX Controller 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。

準備 PXE 伺服器進行 NSX Edge 安裝

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。

先決條件

- 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 網路設定](#) 中的 NSX Edge 網路需求。

程序

- 1 (可選) 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 <mgr-ip> thumbprint <mgr-thumbprint> username <mgr-username> password <mgr-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 (可選) 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** (可選) 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 whois
sudo 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 $6$tmLNLmp$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\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' 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 6tm...` 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

使用裸機或 ISO 檔案安裝 NSX Edge。請參閱[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。

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。

先決條件

- 確認系統 BIOS 模式設為舊版 BIOS。
- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。

程序

- 1 建立具有 NSX Edge ISO 檔案的可開機磁碟。
- 2 從磁碟將實體機器開機。
- 3 選擇**自動安裝**。

在您按 **Enter** 鍵後, 系統可能會暫停 10 秒鐘。

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**。

- 4 開啟 NSX Edge 的主控制台以追蹤開機程序。

如果主控制台視窗並未開啟, 請確定已允許快顯視窗。

- 5 在 NSX Edge 啟動後，使用管理員權限登入 CLI，使用者名稱為 **admin**，密碼為 **default**。

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。

- 6 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**。
- 7 執行 **get interface eth0** 命令以確認 IP 位址已按預期套用。

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

Interface: eth0
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
...
```

如有需要，執行 **set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt** 命令以更新管理介面。(選用) 您可以使用 **start service ssh** 命令啟動 SSH 服務。

- 8 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。

- 9 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 DHCP 指派錯誤的 NIC 作為管理，請完成工作以修正問題。

- a 登入 CLI 並輸入 **stop service dataplane** 命令。
- b 輸入 **set interface eth0 dhcp plane mgmt** 命令。
- c 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 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](#)。

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。

先決條件

- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。

程序

- 1 在獨立主機上或 vCenter Web Client 中建立虛擬機器，並配置下列資源：
 - 客體作業系統：其他 (64 位元)。
 - 3 個 VMXNET3 NIC。NSX Edge 不支援 e1000 NIC 驅動程式。
 - 您的 NSX-T Data Center 部署所需的適當系統資源。

2 將 NSX Edge ISO 檔案繫結至虛擬機器。

請確定 CD/DVD 光碟機裝置狀態設為**開啟電源時連線**。

edge-from-iso: editar configuración

虛擬硬體 虛擬機器選項 SDRS 規則 vApp 選項

CPU	1	
記憶體	2048	MB
Disco duro 1	16	GB
Controladora SCSI 0	VMware 半虛擬化	
Adaptador de red 1	VM Network	<input checked="" type="checkbox"/> 已連線
Unidad de CD/DVD 1	資料存放區 ISO 檔案	<input type="checkbox"/> 已連線
狀態	<input checked="" type="checkbox"/> 開啟電源時連線	
CD/DVD 媒體	[datastore (2)]/nsx-edge-2.3	瀏覽...
裝置模式	模擬 CD-ROM	
虛擬裝置節點	Controladora SAT...	SATA(0:0)
Unidad de disquete 1	用戶端裝置	<input type="checkbox"/> 已連線
Tarjeta de vídeo	指定自訂設定	
Controladora SATA 0		
Dispositivo VMCI		
其他裝置		

3 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 8 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

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。

- 4 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 5 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。

- 6 在 NSX Edge 啟動後，使用管理員權限登入 CLI，使用者名稱為 **admin**，密碼為 **default**。

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。

- 7 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**。

- 8 執行 `get interface eth0` 命令以確認 IP 位址已按預期套用。

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

Interface: eth0
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
...
```

如有需要，執行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理介面。(選用) 您可以使用 `start service ssh` 命令啟動 SSH 服務。

- 9 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。

10 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 DHCP 指派錯誤的 NIC 作為管理，請完成工作以修正問題。

- a 登入 CLI 並輸入 **stop service dataplane** 命令。
- b 輸入 **set interface eth0 dhcp plane mgmt** 命令。
- c 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 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](#)。

存取並確認 NSX Edge 安裝

您可以登入 NSX-T Data Center 虛擬機器或 NSX-T Data Center 裸機主機，確認安裝成功，並視需要疑難排解任何問題。

先決條件

- 確認已設定 PXE 伺服器進行安裝。請參閱[準備 PXE 伺服器進行 NSX Edge 安裝](#)。
- 確認 NSX Edge 使用裸機或 ISO 檔案進行安裝。請參閱[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](#)。

程序

- 1 開啟 NSX-T Data Center 虛擬機器或 NSX-T Data Center 裸機主機的電源。

- 2 在開機功能表上，選取 **nsxedge**。

此時會設定網路、建立磁碟分割，並安裝 NSX Edge 元件。

顯示 NSX Edge 登入提示時，您可以以管理員或根使用者的身分進行登入。

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

- 3 (可選) 若要獲得最佳效能，請保留 NSX-T Data Center 元件所需的記憶體。

記憶體保留是主機保證會為虛擬機器保留的實體記憶體數量下限，即使記憶體過度使用的情況也是如此。請設定一定的保留大小，以確保 NSX-T Data Center 元件具有足夠記憶體來讓執行更有效率。請參閱[系統需求](#)。

- 4 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。

- 5 在 NSX Edge 啟動後，使用管理員權限登入 CLI，使用者名稱為 **admin**，密碼為 **default**。

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。

- 6 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**。
- 7 執行 **get interface eth0** 命令以確認 IP 位址已按預期套用。

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

Interface: eth0
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
...
```

如有需要，執行 **set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt** 命令以更新管理介面。(選用) 您可以使用 **start service ssh** 命令啟動 SSH 服務。

- 8 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。

- 9 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 DHCP 指派錯誤的 NIC 作為管理，請完成工作以修正問題。

- a 登入 CLI 並輸入 **stop service dataplane** 命令。
- b 輸入 **set interface eth0 dhcp plane mgmt** 命令。
- c 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 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](#)。

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。

先決條件

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。

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
```

在 NSX Manager UI 中，NSX Edge 會顯示在**網狀架構 > 節點 > Edge**頁面上。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](#)。

主機準備

在準備讓 Hypervisor 主機與 NSX-T Data Center 搭配運作時，系統會將其視為網狀架構節點。屬於網狀架構節點的主機會安裝 NSX-T Data Center 模組，並且向 NSX-T Data Center 管理平面進行登錄。

本章包含以下主題：

- 在 KVM 主機或裸機伺服器上安裝第三方套件
- 確認 RHEL KVM 主機上的 Open vSwitch 版本
- 將 Hypervisor 主機或裸機伺服器新增至 NSX-T Data Center 網狀架構
- NSX-T Data Center 核心模組的手動安裝
- 將 Hypervisor 主機加入管理平面

在 KVM 主機或裸機伺服器上安裝第三方套件

若要準備 KVM 主機或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。

先決條件

- (Red Hat 和 CentOS) 在安裝第三方套件之前，請安裝虛擬化套件。在主機上，執行下列命令：

```
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) 在安裝第三方套件之前，請安裝虛擬化套件。在 Ubuntu 主機上，執行下列命令：

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

- (裸機伺服器) 不必滿足任何虛擬化必要條件就能安裝第三方套件。

程序

- 在 Ubuntu 16.04.2 LTS 上，確保主機上安裝了下列第三方套件。

```
libunwind8
libgflags2v5
libgoogle-perftools4
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
libprotobuf9v5
libboost-chrono1.58.0
libgoogle-glog0v5
dkms
libboost-date-time1.58.0
libleveldb1v5
libsnappy1v5
python-gevent
python-protobuf
ieee-data
libyaml-0-2
python-linecache2
python-traceback2
libtcmalloc-minimal4
python-greenlet
python-markupsafe
libboost-program-options1.58.0
```

如果 Ubuntu 16.04.2 LTS 上未安裝相依性套件，請執行 `apt-get install <package>` 以手動安裝套件。

- 確認 Red Hat 和 CentOS 主機已登錄，且各自的存放庫均可供存取。

備註 如果使用 NSX-T Data Center UI 準備主機，您必須在主機上安裝下列相依項目。

在 RHEL 7.4 和 CentOS 7.4 上安裝第三方套件。

```
yum-utils
wget
redhat-lsb-core
tcpdump
boost-filesystem
PyYAML
boost-iostreams
boost-chrono
python-mako
python-netaddr
python-six
gperftools-libs
libunwind
snappy
```

```
boost-date-time
c-ares
libev
python-gevent
python-greenlet
```

在 RHEL 7.5 上安裝第三方套件。

```
PyYAML
c-ares
libev
libunwind
libyaml
python-beaker
python-gevent
python-greenlet
python-mako
python-markupsafe
python-netaddr
python-paste
python-tempita
```

- 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相依性。如果主機未登錄，請使用 `yum install <package>` 手動安裝列出的相依項目
- 在裸機伺服器上安裝第三方套件。
 - a 根據您的環境，安裝本主題所列出的 Ubuntu、RHEL 或 CentOS 第三方套件。
 - b 安裝裸機伺服器專屬的第三方套件。

Ubuntu - `apt-get install libvirt-libs`

RHEL 或 CentOS - `yum install libvirt-libs`

確認 RHEL KVM 主機上的 Open vSwitch 版本

如果 OVS 套件存在於主機上，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-vsitchd --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。

- a 刪除下列 Open vSwitch 套件。

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

- b 從 NSX Manger 安裝 NSX-T Data Center 或遵循手動安裝程序進行安裝。

- 2 此外，升級 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>-rhel74_x86_64.tar.gz
```

- d 導覽至套件目錄。

```
cd nsx-lcp-rhel74_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`

後續步驟

將 Hypervisor 主機新增到 NSX-T Data Center 網狀架構。請參閱[將 Hypervisor 主機或裸機伺服器新增至 NSX-T Data Center 網狀架構](#)。

將 Hypervisor 主機或裸機伺服器新增至 NSX-T Data Center 網狀架構

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 Hypervisor 主機或裸機伺服器成為 NSX-T Data Center 覆蓋的一部分，必須先將其新增至 NSX-T Data Center 網狀架構。

如果您已透過手動方式將模組安裝在主機上，並使用 CLI 將主機加入管理平面，則可以略過此程序。

備註 對於 RHEL 上的 KVM 主機，您可以使用 **sudo** 認證執行主機準備活動。

先決條件

- 對於每個您打算新增至 NSX-T Data Center 網狀架構的主機，請先收集下列主機資訊：
 - 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
- 對於 Ubuntu，請確認您已安裝必要的第三方套件。請參閱在 [KVM 主機或裸機伺服器上安裝第三方套件](#)。

程序

- 1 (可選) 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 vSphere 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:A2:4E: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 在 NSX Manager CLI 中，確認 install-upgrade 服務已在執行。

```
nsx-manager-1> get service install-upgrade
```

```
Service name: install-upgrade
Service state: running
Enabled: True
```

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

- 4 選取**網狀架構 > 節點 > 主機**，然後按一下**新增**。
- 5 輸入主機名稱、IP 位址、使用者名稱、密碼和 (選用) 指紋。

例如：

新增主機



名稱 *	comp-02b
IP 位址 *	<div>192.168.210.54 ×</div>
作業系統 *	ESXi ▼
使用者名稱 *	root
密碼 *	●●●●●●
SHA-256 指紋	

取消

新增

至於裸機伺服器，您可以從 [作業系統] 下拉式功能表中選取 **RHEL 伺服器**、**Ubuntu 伺服器**或 **CentOS 伺服器**。

如果您未輸入主機指紋，NSX-T Data Center UI 會提示您使用從主機擷取來的純文字格式的預設指紋。

例如：

無效指紋



輸入的指紋無效。

是否要使用此伺服器提供的指紋？

fa984ff00d4856c1e8db1be005ff908a3f2335bcd67776447e926aba71a006b8

否

新增

成功將主機新增至 NSX-T Data Center 網狀架構時，NSX Manager 的主機頁面會顯示**部署狀態: 安裝成功**和**MPA 連線: 已開啟**。

在您讓網狀架構節點進入傳輸節點之前，**LCP 連線**會維持無法使用的狀態。

6 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。

在 vSphere ESXi 上，這些模組會封裝為 VIB。若為 RHEL 上的 KVM 或裸機伺服器，這些模組會封裝為 RPM。若為 Ubuntu 上的 KVM 或裸機伺服器，這些模組會封裝為 DEB。

- 在 ESXi 上，輸入命令 `esxcli software vib list | grep nsx`。

日期為您執行安裝的那一天

- 在 RHEL 上，輸入命令 `yum list installed` 或 `rpm -qa`。
- 在 Ubuntu 上，輸入命令 `dpkg --get-selections`。

7 (可選) 使用 GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` API 呼叫來檢視網狀架構節點。

8 (可選) 使用 GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` API 呼叫在 API 中監控狀態。

- 9 (可選) 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 Manager IP address>' -u 'admin' -p '<password>' -i 900
```

- c (可選) 將輪詢間隔變更回其預設值。

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -r
```

後續步驟

建立傳輸區域。請參閱[關於傳輸區域](#)。

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-aggsservice_<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。

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-aggsservice** - 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-da** - 收集關於 Hypervisor 作業系統版本、虛擬機器和網路介面的探索代理程式 (DA) 資料。將資料提供給管理平面，以便用於疑難排解工具。
- **nsx-esx-datapath** - 提供 NSX-T Data Center 資料平面封包處理功能。
- **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-lldp** - 提供 Link Layer Discovery Protocol (LLDP) 的支援，這是網路裝置用來在 LAN 上通告其身分識別、能力和芳鄰的連結層通訊協定。
- **nsx-mpa** - 提供 NSX Manager 與 Hypervisor 主機之間的通訊。
- **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-python-protobuf** - 提供通訊協定緩衝區的 Python 繫結。
- **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。
- **nsxa** - 執行主機層級組態，例如 N-VDS 建立和上行組態。
- **nsxcli** - 在 Hypervisor 主機上提供 NSX-T Data Center CLI。
- **nsx-support-bundle-client** - 提供收集支援服務包的功能。

若要進行確認，您可以在 ESXi 主機上執行 **esxcli software vib list | grep nsx** 或 **esxcli software vib list | grep <yyyy-mm-dd>** 命令，其中日期是您執行安裝的當日。

後續步驟

將主機新增至 NSX-T Data Center 管理平面。請參閱[將 Hypervisor 主機加入管理平面](#)。

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。

先決條件

- 確認已安裝必要的第三方套件。請參閱[在 KVM 主機或裸機伺服器上安裝第三方套件](#)。

程序

- 1 以具有管理權限的使用者身分登入主機。
- 2 (可選) 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[將 Hypervisor 主機加入管理平面](#)。

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。

先決條件

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[將 Hypervisor 主機加入管理平面](#)。

將 Hypervisor 主機加入管理平面

將 Hypervisor 主機加入管理平面，可確保 NSX Manager 與這些主機能夠相互通訊。

先決條件

必須完成 NSX-T Data Center 模組的安裝。

程序

- 1** 開啟 NSX Manager 應用裝置的 SSH 工作階段。
- 2** 以管理員認證登入。
- 3** 開啟 Hypervisor 主機的 SSH 工作階段。

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

命令輸出是對此 NSX Manager 而言具有唯一性的數字字串。

例如：

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

- 5 在 Hypervisor 主機上，執行 `nsxcli` 命令以進入 NSX-T Data Center CLI。

備註 針對 KVM，請以 `superuser (sudo)` 的身分執行命令。

```
[user@host:~] nsxcli
host>
```

提示即會變更。

- 6 在 Hypervisor 主機上，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

```
host> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully joined
```

在您的主機上執行 `get managers` 命令以確認結果。

```
host> get managers
- 192.168.110.47    Connected
```

在**網狀架構 > 節點 > 主機**的 NSX Manager UI 中，確認主機的 MPA 連線為**開啟**。

您也可以透過 **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** API 呼叫來檢視網狀架構主機的狀態：

```
{
  "details": [],
  "state": "success"
}
```

管理平面會將主機憑證傳送至控制平面，且控制平面會將控制平面資訊推送至主機。

應查看每台 ESXi 主機上的 `/etc/vmware/nsx/controller-info.xml` 中的 NSX Controller 位址，或使用 `get controllers` 存取 CLI。

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
      <server>10.143.1.47</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
      <server>10.143.1.45</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="2">
      <server>10.143.1.46</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
  </connectionList>
</config>
```

主機對 NSX-T Data Center 的連線會初始化，且會保持在「CLOSE_WAIT」狀態，直到主機升階為傳輸節點。您可以透過 `esxcli network ip connection list | grep 1234` 命令來查看此情況。

```
# esxcli network ip connection list | grep 1234
tcp      0      0 192.168.210.53:45823      192.168.110.34:1234  CLOSE_WAIT    37256  newreno
netcpa
```

若為 KVM，則命令為 `netstat -anp --tcp | grep 1234`。

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp 0 0 192.168.210.54:57794 192.168.110.34:1234  CLOSE_WAIT -
```

後續步驟

建立傳輸區域。請參閱[關於傳輸區域](#)。

傳輸區域和傳輸節點

傳輸區域和傳輸節點是 NSX-T Data Center 中的重要概念。

本章包含以下主題：

- 關於傳輸區域
- 增強型資料路徑
- 為通道端點 IP 位址建立 IP 集區
- 建立上行設定檔
- 建立傳輸區域
- 建立主機傳輸節點
- 建立裸機伺服器工作負載的應用程式介面
- 設定 Network I/O Control 設定檔
- 建立 NSX Edge 傳輸節點
- 建立 NSX Edge 叢集

關於傳輸區域

傳輸區域是定義傳輸節點可連線區域的容器。傳輸節點則是會參與 NSX-T Data Center 覆疊的 Hypervisor 主機和 NSX Edge。若為 Hypervisor 主機，這表示它裝載了會透過 NSX-T Data Center 邏輯交換器進行通訊的虛擬機器。若為 NSX Edge，這表示它將具有邏輯路由器上行和下行。

當您建立傳輸區域時，必須指定 N-VDS 模式，此模式可以是標準或增強型資料路徑。當您將傳輸節點新增至傳輸區域時，會在傳輸節點上安裝與傳輸區域相關聯的 N-VDS。每個傳輸區域支援單一 N-VDS。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，可支援 VLAN 和覆疊網路，且需要支援增強型資料路徑 N-VDS 的 ESXi 主機。

傳輸節點可屬於：

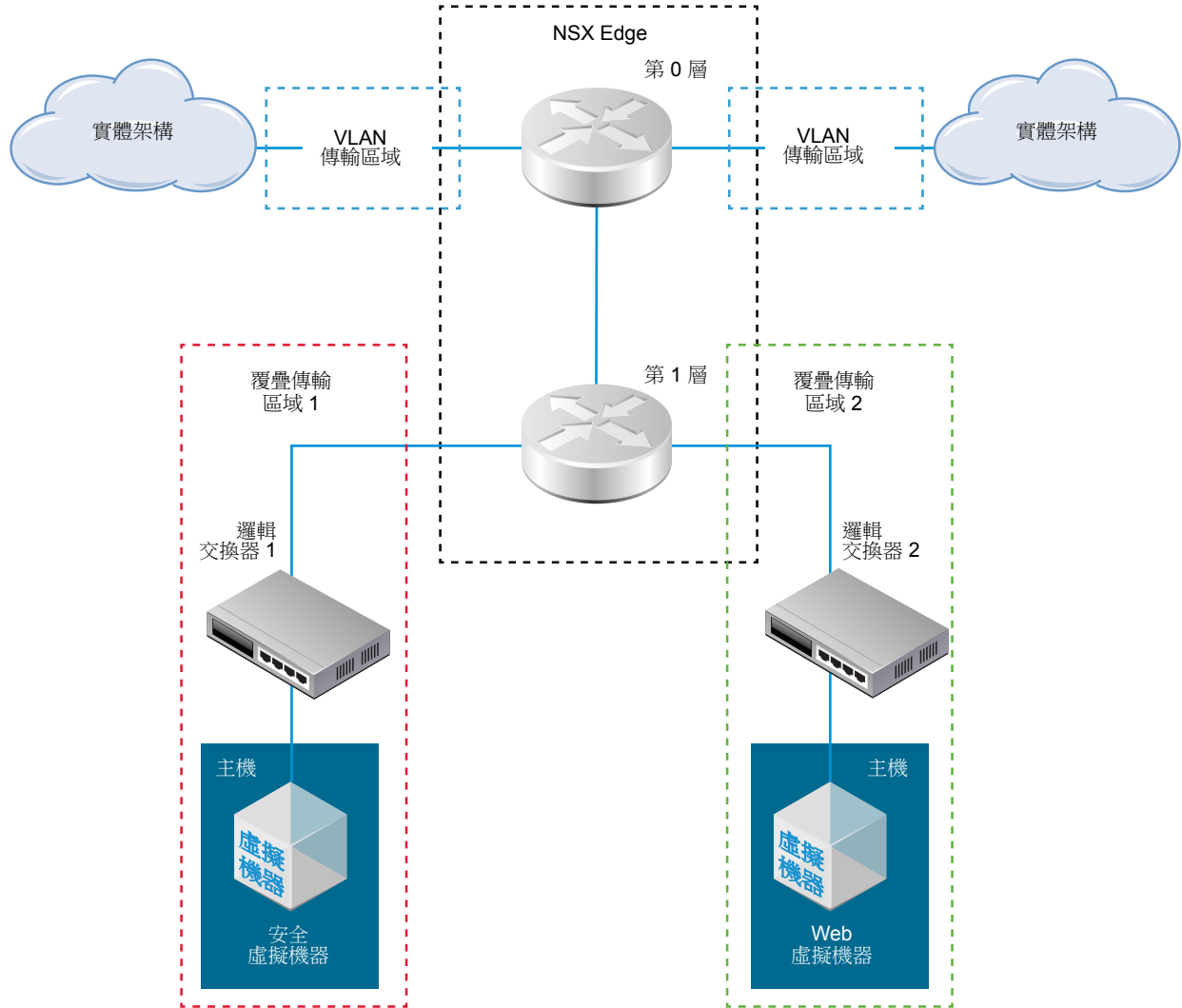
- 多個 VLAN 傳輸區域。
- 最多一個具有標準 N-VDS 的覆疊傳輸區域。
- 多個具有進階資料路徑 N-VDS 的覆疊傳輸區域 (如果傳輸節點在 ESXi 主機上執行)。

如果有兩個傳輸節點位於相同的傳輸區域中，則裝載在這些傳輸節點上的虛擬機器將可連結至也位於該傳輸區域中的 **NSX-T Data Center** 邏輯交換器。假設虛擬機器具有第 2 層/第 3 層連線性，則前述連結即可讓這些虛擬機器相互通訊。如果虛擬機器連結至不同傳輸區域的交換器，則虛擬機器無法彼此通訊。傳輸區域無法取代第 2 層/第 3 層底層連線性需求，但可限制連線性。換句話說，屬於相同的傳輸區域是連線的先決條件。符合先決條件後才可能產生連線性，但並不會自動產生。若要達到實際的連線性，第 2 層和 (適用於不同的子網路) 第 3 層底層網路必須正常運作。

假設單一傳輸節點同時包含一般虛擬機器和高安全性虛擬機器。在您的網路設計中，一般虛擬機器應該要能彼此連線，但無法連線至高安全性虛擬機器。若要達成此目標，您可以將安全虛擬機器放在屬於某個傳輸區域 (名為 **secure-tz**) 的主機上。一般虛擬機器和安全虛擬機器不可位於相同的傳輸節點。一般虛擬機器則位於不同的傳輸區域 (名為 **general-tz**) 上。一般虛擬機器會連結至同樣位於 **general-tz** 的 **NSX-T Data Center** 邏輯交換器。高安全性虛擬機器會連結至位於 **secure-tz** 的 **NSX-T Data Center** 邏輯交換器。位於不同傳輸區域的虛擬機器即使位於相同子網路仍無法彼此通訊。虛擬機器至邏輯交換器的連線才是虛擬機器連線能力的最終控制因素。因此，因為兩個邏輯交換器位於不同的傳輸區域，「Web 虛擬機器」和「安全虛擬機器」並無法彼此連線。

例如，下圖顯示屬於三個傳輸區域的 **NSX Edge**：兩個 VLAN 傳輸區域和一個覆疊傳輸區域 2。覆疊傳輸區域 1 包含主機、**NSX-T Data Center** 邏輯交換器和安全虛擬機器。因為 **NSX Edge** 不屬於覆疊傳輸區域 1，安全虛擬機器與實體架構無法互相存取。相反地，因為 **NSX Edge** 屬於覆疊傳輸區域 2，位於覆疊傳輸區域 2 的 **Web** 虛擬機器可與實體架構通訊。

圖 8-1: NSX-T Data Center 傳輸區域



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。

在增強型資料路徑模式下，您可以設定：

- 覆蓋流量
- VLAN 流量

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 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](#)。

- 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[建立主機傳輸節點](#)。

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。

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 標頭中的來源和目的地 IP 位址，用來唯一識別哪些 Hypervisor 主機起始及終止了覆疊框架的 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，其中一個設計選項將是對 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，您需要在 KVM 主機上，使用專用的預設閘道新增 sub_a 的靜態路由。

這是一個 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。如果路由是使用路由新增命令新增的，則在主機重新開機後無法持續保存路由。

```
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 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**詳細目錄 > 群組 > IP 集區**，然後按一下**新增**。
- 3 輸入 IP 集區名稱、(選用) 說明和網路設定。

網路設定包含：

- IP 位址範圍
- 閘道
- 以 CIDR 標記法表示的網路位址
- (選用) 以逗號分隔的 DNS 伺服器清單

■ (選用) DNS 尾碼

例如：

新增 IP 集區



名稱 * corp-tep

說明

子網路

+ 新增 刪除

<input checked="" type="checkbox"/> IP 範圍 *	閘道	CIDR *	DNS 伺服器	DNS 尾碼
<input checked="" type="checkbox"/> 192.168.250.100 - 192.168.250.200	192.168.200.1	192.168.250.0/24		

取消

新增

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

```
{
  "cursor": "0036e2d8c2e8-f6d7-498e-821b-b7e44d2650a9ip-pool-1",
  "sort_by": "displayName",
  "sort_ascending": true,
  "result_count": 1,
  "results": [
    {
      "id": "e2d8c2e8-f6d7-498e-821b-b7e44d2650a9",
      "display_name": "comp-tep",
      "resource_type": "IpPool",
      "subnets": [
        {
          "dns_nameservers": [
            "192.168.110.10"
          ],
          "allocation_ranges": [
            {
              "start": "192.168.250.100",
              "end": "192.168.250.200"
            }
          ],
          "gateway_ip": "192.168.250.1",
          "cidr": "192.168.250.0/24",
          "dns_suffix": "corp.local"
        }
      ]
    }
  ]
}
```

```

    ],
    "_last_modified_user": "admin",
    "_last_modified_time": 1443649891178,
    "_create_time": 1443649891178,
    "_system_owned": false,
    "_create_user": "admin",
    "_revision": 0
  }
]
}

```

後續步驟

建立上行設定檔。請參閱[建立上行設定檔](#)。

建立上行設定檔

上行設定檔可定義從 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。

上行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。上行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，而是可以在上行設定檔中指定功能，接著可以在建立 NSX-T Data Center 傳輸節點時套用。

待命上行不受虛擬機器/應用裝置型 NSX Edge 所支援。當您安裝 NSX Edge 做為虛擬應用裝置時，使用預設上行設定檔。針對為虛擬機器型 NSX Edge 所建立的每個上行設定檔，設定檔必須僅指定一個作用中上行，且並未指定任何待命上行。

備註 NSX Edge 虛擬機器確實允許多個上行，但前提是要為每個上行建立個別的 N-VDS，且各自使用不同的 VLAN。每個上行需要獨立的 VLAN 傳輸區域。這是為了支援連線至多個 TOR 交換器的單一 NSX Edge 節點。

先決條件

- 自行熟悉 NSX Edge 網路。請參閱 [NSX Edge 網路設定](#)。
- 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 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。

- 2 選取**網狀架構 > 設定檔 > 上行設定檔**，然後按一下**新增**。
- 3 完成上行設定檔詳細資料。

選項	說明
名稱	輸入上行設定檔名稱。
說明	新增選用上行設定檔說明。
LAG	<p>(選用) 對傳輸網路使用連結彙總控制通訊協定 (LACP) 的連結彙總群組 (LAG)。</p> <p>備註 對於 LACP，在 KVM 主機上不支援多個 LAG。</p> <p>新增以逗號分隔的作用中上行名稱清單。</p> <p>新增以逗號分隔的待命上行名稱清單。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。</p> <p>可能的 LAG 雜湊機制選項。</p> <ul style="list-style-type: none"> ■ 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	<p>在 [整併] 區段中，按一下新增，然後輸入詳細資料。整併原則會定義 N-VDS 如何使用其上行以實現冗餘和流量負載平衡。有兩種整併原則模式可用於設定整併原則：</p> <ul style="list-style-type: none"> ■ 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。 <p>備註 在 KVM 主機上，僅支援容錯移轉順序整併原則。不支援負載平衡來源整併原則。</p> <p>(僅限 ESXi 主機) 您可以針對傳輸區域定義下列原則：</p> <ul style="list-style-type: none"> ■ 交換器上設定的每個邏輯交換器的具名整併原則。 ■ 整個交換器的預設整併原則。 <p>具名整併原則：具名整併原則表示對於每個邏輯交換器，您可以定義特定的整併原則模式和上行。此原則類型可讓您根據頻寬需求彈性地選取上行。</p> <ul style="list-style-type: none"> ■ 當您定義具名整併原則時，如果該原則由主機中的連結傳輸區域和邏輯交換器指定，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。
- 5 輸入 MTU 值。
預設值為 1600。

除了 UI 以外，您也可以使用 GET `/api/v1/host-switch-profiles` API 呼叫來檢視上行設定檔：

```
{
  "result_count": 2,
  "results": [
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "16146a24-122b-4274-b5dd-98b635e4d52d",
      "display_name": "comp-uplink",
      "transport_vlan": 250,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [ {
          "uplink_name": "uplink-2",
          "uplink_type": "PNIC"
        } ],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399526,
      "_create_time": 1457984399526,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    },
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "c9e35cec-e9d9-4c51-b52e-17a5c1bd9a38",
      "display_name": "vlan-uplink",
      "transport_vlan": 100,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [],
        "policy": "FAILOVER_ORDER"
      },
      "named_teamings": [
        {
          "active_list": [
            {
              "uplink_type": "PNIC",
              "uplink_name": "uplink-2"
            }
          ],
          "standby_list": [
```



```

    {
        "uplink_type": "PNIC",
        "uplink_name": "uplink-1"
    },
    "policy": "FAILOVER_ORDER",
    "name": "named teaming policy"
  }
]
      "mtu": 1600,
  "_last_modified_time": 1457984399574,
  "_create_time": 1457984399574,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_create_user": "admin",
  "_revision": 0
}
]
}

```

後續步驟

建立傳輸區域。請參閱[建立傳輸區域](#)。

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** 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 在瀏覽器中，以管理員權限登入 **NSX Manager**，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**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。
選項為**標準**和**增強型資料路徑**。
- 6 如果 N-VDS 模式為 [標準]，請選取流量類型。
選項為**覆蓋**和 **VLAN**。
- 7 如果 N-VDS 模式為增強型資料路徑，請選取流量類型。
選項為**覆蓋**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 (可選) 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-hostswitch",
```

```

    "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[建立主機傳輸節點](#)。

建立主機傳輸節點

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，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。

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。

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。

先決條件

- 您必須使用管理平面加入主機，且[網狀架構 > 主機](#)頁面上的 [MPA 連線] 必須為 [已開啟]。

- 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。

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網狀架構 > 節點 > 傳輸節點 > 新增**。
- 3 輸入傳輸節點的名稱。
- 4 從下拉式功能表中選取節點。
- 5 選取此傳輸節點所屬的傳輸區域。
- 6 按一下 **N-VDS** 索引標籤。
- 7 對於 KVM 節點，選取 N-VDS 類型。

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

對於非 KVM 節點，N-VDS 類型一律為**標準**或**增強型資料路徑**。

- 8 對於標準 N-VDS，提供下列詳細資料。

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。
NIOC 設定檔	從下拉式功能表選取 NIOC 設定檔。
上行設定檔	從下拉式功能表中選取上行設定檔。
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	請確定實體 NIC 並未處於使用中狀態 (例如，由標準 vSwitch 或 vSphere Distributed Switch 使用中)。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。 針對裸機伺服器，請選取可以設定為 uplink-1 連接埠的實體 NIC。uplink-1 連接埠會定義在上行設定檔中。 如果裸機伺服器中只有一個網路介面卡，請選取該實體 NIC，以便將 uplink-1 連接埠同時指派給管理和應用程式介面。

9 對於增強型資料路徑 N-VDS，提供下列詳細資料。

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	選取支援增強型資料路徑的實體 NIC。請確定實體 NIC 並未處於使用中狀態 (例如，由標準 vSwitch 或 vSphere Distributed Switch 使用中)。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。
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 <code>esxcli hardware memory get</code> 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 <code>esxcli network ens maxLcores get</code> 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。

10 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。

將主機新增為傳輸節點後，主機對 NSX Controller 的連線會變更為「開啟」狀態。

11 在**傳輸節點**頁面上檢視連線狀態。

12 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 -
```

13 (可選) 使用 GET <https://<nsx-mgr>/api/v1/transport-nodes/<node-id>> API 呼叫來檢視傳輸節點。

```
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "95c8ce77-f895-43de-adc4-03a3ae2565e2",
  "display_name": "node-comp-01b",
  "tags": [],
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ],
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ],
      "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
    }
  ],
  "node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
  "_create_time": 1460051753373,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1460051753373,
  "_create_user": "admin",
  "_revision": 0
}
```

14 將新建立的傳輸節點新增至傳輸區域。

- a 選取傳輸節點。
- b 選取**動作 > 新增至傳輸區域**。
- c 從下拉式功能表中選取傳輸區域。

系統會填入所有其他欄位。

備註 對於標準 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 NSX-T 虛擬分散式交換器。請參閱 [VMkernel 移轉至 N-VDS 交換器](#)。

設定自動建立傳輸節點

如果您擁有 vCenter Server 叢集，則可以在單一或多個叢集中的所有 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。

備註 僅在 vCenter Server 6.5 Update 1、6.5 Update 2 和 6.7 上支援自動建立 NSX-T Data Center 傳輸節點。

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。

先決條件

- 主機必須為 vCenter Server 叢集的一部分。
- 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。
- vCenter Server 應至少具有一個叢集。
- 您必須設定計算管理程式。

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網狀架構 > 節點 > 主機**。
- 3 從 [管理者] 下拉式功能表中選取現有的計算管理程式。
- 4 選取叢集，然後按一下**設定叢集**。

5 完成設定叢集詳細資料。

選項	說明
自動安裝 NSX	切換按鈕以在 vCenter Server 叢集中的所有主機上啟用 NSX-T Data Center 的安裝。
自動建立傳輸節點	<p>切換按鈕以在 vCenter Server 叢集中的所有主機上啟用傳輸節點建立。這是必要的設定。</p> <p>備註 如果預先設定的傳輸節點存在於此叢集中或移至另一個叢集，則 NSX-T Data Center 不會使用叢集之傳輸節點範本中定義的組態來更新預先設定的傳輸節點。若要確保所有節點都具有相同的組態，請刪除預先設定的傳輸節點，然後將該主機新增至叢集。</p>
傳輸區域	從下拉式功能表中選取現有的傳輸節點。
上行設定檔	<p>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。</p> <p>備註 叢集中的主機必須具有相同的上行設定檔。</p> <p>您也可以使用預設上行設定檔。</p>
IP 指派	<p>從下拉式功能表中選取使用 DHCP或使用 IP 集區。</p> <p>如果您選取使用 IP 集區，則必須從下拉式功能表將現有的 IP 集區配置在網路中。</p>
實體 NIC	<p>請確定實體 NIC 並未處於使用中狀態，例如由標準 vSwitch 或 vSphere 分散式交換器使用中。否則，傳輸節點狀態會是部分成功，且網狀架構節點 LCP 連線將無法建立。</p> <p>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。</p> <p>按一下新增 PNIC以增加組態中的 NIC 數目。</p>

系統會以平行方式開始安裝 NSX-T Data Center 並在叢集中的每個主機上建立傳輸節點。整個程序是根據叢集中的主機數目而定。

將新的主機新增至 vCenter Server 叢集時，系統會自動安裝 NSX-T Data Center 並建立傳輸節點。

6 (可選) 檢視 ESXi 連線狀態。

```
# 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
```

7 (可選) 從叢集中的主機移除 NSX-T Data Center 安裝和傳輸節點。

- 選取叢集，然後按一下**設定叢集**。
- 切換 [自動安裝 NSX] 按鈕以停用選項。
- 選取一或多個主機，然後按一下**解除安裝 NSX**。

解除安裝最多需花費三分鐘。

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。

先決條件

- 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[建立主機傳輸節點](#)。

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網狀架構 > 設定檔 > 上行設定檔**，然後按一下**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**項目。
- 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，名為 **lag1**。
- 7 按一下對話方塊底部的**新增**。
- 8 輸入**傳輸 VLAN** 和 **MTU** 的值。
- 9 按一下視窗底部的**新增**。
- 10 選取**網狀架構 > 節點 > 傳輸節點 > 新增**。
- 11 在**一般**索引標籤中輸入資訊。
- 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，您會看到實體 NIC 的下拉式清單，以及建立上行設定檔時所指定的上行下拉式清單。具體來說，您會看到上行 **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。

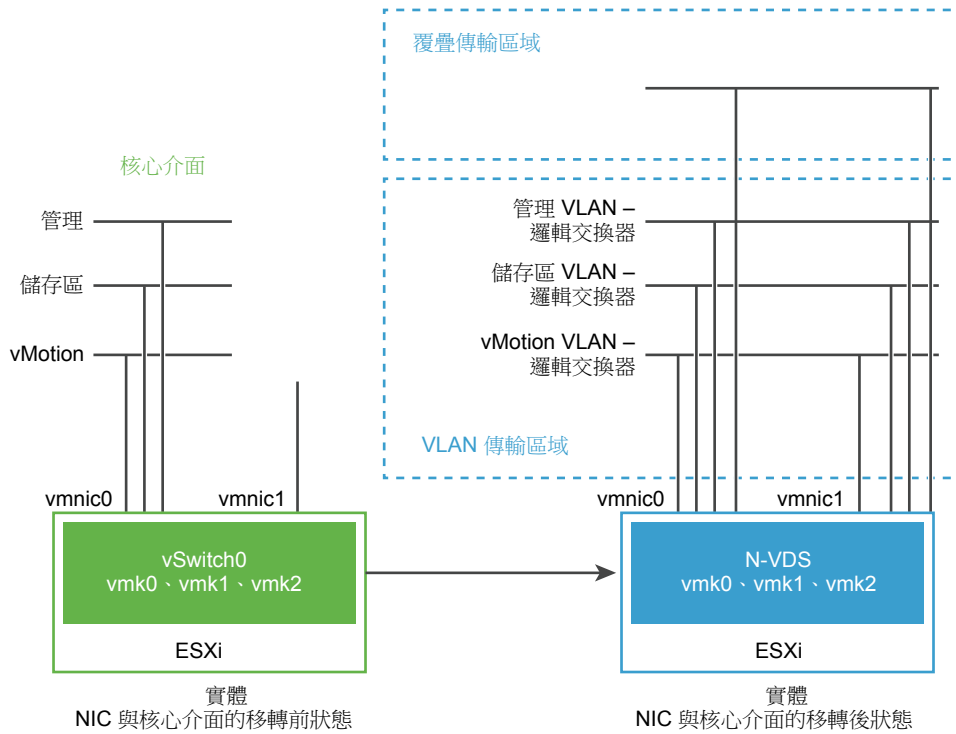
VMkernel 移轉至 N-VDS 交換器

當您建立傳輸節點時，可能必須要將實體 NIC 和核心介面從 vSphere 標準交換器 (VSS) 或 VDS 移轉至 NSX-T Data Center 虛擬分散式交換器 (N-VDS)。移轉後，N-VDS 會處理 VLAN 網路上的流量。

實體 NIC 及其 VMkernel 介面最初連結至 vSphere ESXi 主機上的 VSS 或 VDS。將在這些主機上定義這些核心介面，以提供與管理介面、儲存區和其他介面的連線。移轉後，VMkernel 介面及其相關聯的實體 NIC 連線至 N-VDS，並處理 VLAN 和覆蓋傳輸區域上的流量。

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 以實現冗餘。

圖 8-2：將網路介面移轉到 N-VDS 前後



移轉之前，vSphere 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 或 VDS），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 UI 或 API NSX-T Data Center 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 和覆蓋傳輸區域進行連線。

使用 NSX-T Data Center Manager UI 將 VMkernel 介面移轉至 N-VDS 交換器

NSX-T Data Center Manager UI 可讓您將包括管理介面在內的所有核心介面從 VSS 或 VDS 移轉至 N-VDS 交換器。

在此範例中，請考量具有兩個實體介面卡 vmnic0 和 vmnic1 的 vSphere ESXi 主機。主機上的預設 VSS 或 VDS 交換器已設定對應至 vmnic0 的單一上行。還會在 VSS 或 VDS 上設定 VMkernel 介面 vmk0，以執行節點上的管理流量。目標是將 vmnic0 和 vmk0 移轉至 N-VDS 交換器。

在主機準備過程中，會建立 VLAN 和覆蓋傳輸區域來分別執行管理和虛擬機器流量。還會建立 N-VDS 交換器並為其設定對應至 vmnic1 的上行。移轉後，NSX-T Data Center 會同時將 vmnic0 和 vmk0 從 VSS 或 VDS 交換器移轉至節點上的 N-VDS 交換器。

先決條件

- 確認實體網路基礎結構對 vmnic1 和 vmnic0 提供相同的 LAN 連線。
- 確認未使用的實體 NIC vmnic1 具有與 vmnic0 的第 2 層連線。

- 確保此移轉中涉及的所有 VMkernel 介面都屬於相同的網路。如果將 VMkernel 介面移轉至連線到不同網路的上行，主機可能會無法連線或無法正常運作。

程序

- 1 在 NSX Manager UI 上，移至**網狀架構** -> **設定檔** -> **上行設定檔**。
- 2 使用 vmnic0 做為作用中上行並使用 vmnic1 做為被動上行，以建立上行設定檔。
- 3 移至**網狀架構** -> **傳輸區域** -> **新增**。
- 4 建立覆疊和 VLAN 傳輸區域，可分別處理虛擬機器流量和管理流量。

備註 VLAN 傳輸區域和覆疊傳輸區域中使用的 N-VDS 名稱必須相同。

- 5 移至**網狀架構** -> **節點** -> **傳輸節點**。
- 6 將兩個傳輸區域新增至傳輸節點。
- 7 在 N-VDS 索引標籤中，透過定義將由 N-VDS 使用的上行和實體介面卡，新增 N-VDS。
傳輸節點會透過單一上行連線至傳輸區域。
- 8 若要確保在移轉後 vmk0 和 vmnic0 取得 VLAN 傳輸區域的連線，請針對適當的 VLAN 傳輸區域建立邏輯交換器。
- 9 選取傳輸節點，然後按一下**動作** -> **移轉 ESX VMkernel 和實體介面卡**。
- 10 選取**移轉至邏輯交換器**。
- 11 選取 N-VDS 交換器。
- 12 新增 VMkernel 介面卡和相關聯的邏輯交換器。
- 13 新增對應至 VMkernel 介面的實體介面卡。確保 VSS 或 VDS 交換器上至少保留一個實體介面卡。
- 14 按一下**儲存**。
- 15 按一下**繼續**以開始移轉。
- 16 從 NSX Manager 測試 vmnic0 和 vmk0 的連線。
- 17 或者，在 vCenter Server 中，確認 VMkernel 介面卡與 NSX-T Data Center 交換器相關聯。

VMkernel 介面及其對應的實體介面卡將移轉至 N-VDS。

後續步驟

您可以還原將 VMkernel 移轉至 VSS 或 VDS 交換器的作業。

使用 NSX-T Data Center Manager UI 將 VMkernel 介面移轉還原至 VSS 或 VDS 交換器

若要還原將 VMkernel 介面移轉至 VSS 或 VDS 交換器的作業，請確認連接埠群組存在於 ESXi 主機上。

NSX-T Data Center 需要使用連接埠群組將 VMkernel 介面從 N-VDS 交換器移轉至 VSS 或 VDS 交換器。連接埠群組接受將這些介面移轉至 VSS 或 VDS 交換器的網路要求。會根據頻寬和原則組態決定參與此移轉的連接埠成員。

開始將 VMkernel 移轉回 VSS 或 VDS 交換器之前，請確定 VMkernel 介面正常運作並且 N-VDS 交換器上的連線已開啟。

先決條件

- 連接埠群組存在於 vSphere ESXi 伺服器上。

程序

- 1 在 NSX Manager UI 中，移至**網狀架構** -> **節點** -> **傳輸節點**。
- 2 選取傳輸節點，然後按一下**動作** -> **移轉 ESX VMkernel 和實體介面卡**。
- 3 選取**移轉至連接埠群組**。
- 4 選取 N-VDS 交換器。
- 5 新增 VMkernel 介面卡和相關聯的邏輯交換器。
- 6 新增對應至 VMkernel 介面的實體介面卡。確保至少一個實體介面卡保持連線到 VSS 或 VDS 交換器。
- 7 按一下**儲存**。
- 8 按一下**繼續**以開始移轉。
- 9 從 NSX Manager 測試 vmnic0 和 vmk0 的連線。
- 10 或者，在 vCenter Server 中，確認 VMkernel 介面卡與 VSS 或 VDS 交換器相關聯。

VMkernel 介面及其對應的實體介面卡將移轉至 N-VDS。

後續步驟

您可能想要使用 API 移轉 VMkernel 介面。請參閱[使用 API 將核心介面移轉至 N-VDS](#)。

使用 API 將核心介面移轉至 N-VDS

使用 NSX-T Data Center API 時，確保在移轉管理介面之前，先移轉所有核心介面。

考量將兩個上行連線到各自實體 NIC 的主機。在此程序中，您可以開始將儲存區核心介面 vmk1 移轉至 N-VDS。此核心介面成功移轉至 N-VDS 後，您可以移轉管理核心介面。

請參閱《NSX-T Data Center API 指南》。

先決條件

- 確認實體網路基礎結構對 vmnic1 和 vmnic0 提供相同的 LAN 連線。
- 確認未使用的實體 NIC vmnic1 具有與 vmnic0 的第 2 層連線。
- 確保此移轉中涉及的所有 VMkernel 介面都屬於相同的網路。如果將 VMkernel 介面移轉至連線到不同網路的上行，主機可能會無法連線或無法正常運作。

程序

- 1 使用覆疊傳輸區域所用的 N-VDS 的 `host_switch_name`，建立 VLAN 傳輸區域。
- 2 透過符合 VSS 或 VDS 上 `vmk1` 所用 VLAN 識別碼的 VLAN 識別碼，在 VLAN 傳輸區域中建立 VLAN 支援的邏輯交換器。
- 3 將 vSphere ESXi 傳輸節點新增至 VLAN 傳輸區域。
- 4 擷取 vSphere ESXi 傳輸節點組態。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

其中 `<transportnode-id>` 是傳輸節點的 UUID。

- 5 將 `vmk1` 移轉至 N-VDS。

```
PUT https://<NSXmgr>/api/v1/transport-nodes/<transportnode-id> ?
if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

其中 `<transportnode-id>` 是傳輸節點的 UUID。`<vmk>` 是 VMkernel 介面 `vmk1` 的名稱。`<network>` 是目標邏輯交換器的 UUID。

- 6 確認移轉已成功完成。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

請等到移轉狀態顯示為成功。您也可以在此 vCenter Server 中確認 VMkernel 介面的移轉狀態。

VMkernel 介面已從 VSS 或 VDS 移轉至 N-VDS 交換器。

後續步驟

您可以將其餘的 VMkernel 介面以及 VSS 或 VDS 的管理核心介面移轉至 N-VDS。

使用 API 將管理核心介面從 VSS 或 VDS 移轉至 N-VDS

移轉所有其他核心介面後，繼續移轉管理核心介面。移轉管理核心介面時，將 `vmnic0` 和 `vmk0` 從 VSS 或 VDS 移至 N-VDS。

然後，只需一步即可將實體上行 `vmnic0` 和 `vmk0` 一同移轉到 N-VDS。修改傳輸節點組態，將 `vmnic0` 設定為其中一個上行。

備註 如果您想要分別移轉上行 `vmnic0` 及核心介面 `vmk0`，請先移轉 `vmk0`，然後再移轉 `vmnic0`。如果您先移轉 `vmnic0`，則 `vmk0` 仍會保留在 VSS 或 VDS 上，沒有任何支援上行，並且會中斷與主機的連線。

先決條件

- 確認與已移轉的 `vmknic` 之間的連線。請參閱[使用 API 將核心介面移轉至 N-VDS](#)。
- 如果 `vmk0` 和 `vmk1` 使用不同的 VLAN，必須在連線到 PNIC `vmnic0` 和 `vmnic1` 的實體交換器上設定主幹 VLAN 才能同時支援這兩個 VLAN。

- 確認外部裝置可連線到儲存區 VLAN 支援之邏輯交換器上的介面 vmk1 以及 vMotion VLAN 支援之邏輯交換器上的 vmk2。

程序

- 1 (選用) 在 VSS 或 VDS 上建立第二個管理核心介面，並將此新建立的介面移轉至 N-VDS。
- 2 (選用) 從外部裝置確認與測試管理介面的連線。
- 3 如果 vmk0 (管理介面) 使用與 vmk1 (儲存區介面) 不同的 VLAN，則透過符合 VSS 或 VDS 上 vmk0 所用 VLAN 識別碼的 VLAN 識別碼，在 VLAN 傳輸區域中建立 VLAN 支援的邏輯交換器。
- 4 擷取 vSphere ESXi 傳輸節點組態。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

其中 *<transportnode-id>* 是傳輸節點的 UUID。

- 5 在組態的 `host_switch_spec:host_switches` 元素中，將 `vmnic0` 新增至 `pnics` 資料表，並將其指派給專用上行 `uplink-2`。

備註 移轉虛擬機器核心介面時，我們已將 `vmnic1` 指派給 `uplink-1`。若要成功移轉，並且讓主機在移轉後可以連線，必須將 `vmnic0` (管理介面) 指派給專用上行。

```
"pnics": [
    {
      "device_name": "vmnic0",
      "uplink_name": "uplink-2"
    },
    {
      "device_name": "vmnic1",
      "uplink_name": "uplink-1"
    }
  ],
```

- 6 使用更新的組態將管理核心介面 vmk0 移轉至 N-VDS。

```
PUT api/v1/transport-nodes/<transportnode-id>?if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

其中 *<transportnode-id>* 是傳輸節點的 UUID。*<vmk>* 是 VMkernel 管理介面 vmk0 的名稱。*<network>* 是目標邏輯交換器的 UUID。

- 7 確認移轉已成功完成。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

請等到移轉狀態顯示為成功。在 vCenter Server 中，您可以確認是否要將核心介面卡設定為顯示新的邏輯交換器名稱。

後續步驟

您可以選擇還原將核心介面與管理介面從 N-VDS 移轉至 VSS 或 VDS 交換器的作業。

還原使用 API 將 VMkernel 介面從 N-VDS 交換器移轉至 VSS 或 VDS 交換器的作業

還原 VMkernel 介面時，您必須從管理核心介面移轉開始。然後，將其他核心介面從 N-VDS 移轉至 VSS 或 VDS 交換器。

程序

- 1 確認傳輸節點狀態為成功。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

- 2 擷取 vSphere ESXi 傳輸節點組態，以找到 "host_switch_spec": "host_switches" 元素內定義的實體 NIC。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

```
"pnics": [
  { "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 3 從傳輸節點組態的 "host_switch_spec": "host_switches" 元素移除 vmnic0，以準備管理介面進行移轉。

```
"pnics": [
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 4 使用已修改的組態，將管理介面 vmnic0 和 vmk0 從 N-VDS 移轉至 VSS 或 VDS。

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk0&esx_mgmt_if_migration_dest=<vmk0_port_group_name>
```

其中，<vmk0_port_group> 是在移轉至邏輯交換器之前指派給 vmk0 的連接埠群組名稱。

- 5 確認移轉狀態。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

請等到狀態顯示為「成功」。

- 6 擷取 vSphere ESXi 傳輸節點組態。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

- 7 使用上述傳輸節點組態，將 vmk1 從 N-VDS 移轉至 VSS 或 VDS。

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk1&esx_mgmt_if_migration_dest=<vmk1_port_group>
```

其中，`<vmk1_port_group>` 是在移轉到邏輯交換器之前指派給 `vmk1` 的连接埠群組名稱。

備註 `vmk0` 或 `vmk1` 必須移轉至具備至少一個實體 NIC 的 VSS 或 VDS，因為 VSS 或 VDS 不具有任何與其相關聯的實體 NIC。

8 確認傳輸節點狀態為成功。

```
GET /api/v1/transport-nodes/<transportnode-id>/state.
```

9 執行移轉後驗證來避免出現任何問題。

- a 將上行介面連結至 VSS 或 VDS 之前，不得移轉管理核心介面 `vmk0`。
- b 確認 `vmk0` 從 `vmnic0` 接收其 IP 位址，否則 IP 可能會有所變更，並且 VC 等其他元件可能會透過舊 IP 與主機中斷連線。

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 前往 [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 UI 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 檢查 API 的狀態資訊。

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"
}
```

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。可以選擇新增計算管理程式，因為即使沒有計算管理程式，NSX-T 仍可取得詳細目錄資訊 (例如，獨立主機和虛擬機器)。

在此版本中，此功能支援：

- vCenter Server 版本 6.5 Update 1、6.5 Update 2 和 6.7。
- 與 vCenter Server 進行 IPv6 以及 IPv4 通訊。
- 最多 5 個計算管理程式。

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

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取導覽面板中的**網狀架構 > 計算管理程式**。
- 3 按一下**新增**。

4 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。
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。

5 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)。

計算管理程式面板會顯示計算管理程式的清單。您可以按一下管理程式名稱來查看或編輯管理程式的相關詳細資料，或管理套用至管理程式的標記。

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 核心模組並安裝 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。

程序

- 1 安裝所需的第三方套件。

請參閱在 [KVM 主機或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 [vSphere 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。

請參閱將 [Hypervisor 主機](#)或裸機伺服器新增至 [NSX-T Data Center 網狀架構](#)。

- 4 建立 KVM 主機傳輸節點。

請參閱[建立主機傳輸節點](#)。

- 5 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 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 設定檔採用根據主機上實體介面卡的容量為系統流量保留頻寬的機制。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 版支援針對與虛擬機器和基礎結構服務相關的系統流量進行資源管理，例如 vSphere Fault Tolerance 等。系統流量嚴格與 vSphere 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。用於虛擬機器流量的頻寬保留也會在許可控制中使用。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，來為由 vSphere Fault Tolerance、vSphere vMotion、虛擬機器等產生的流量配置一定量的頻寬。

- 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 Server 會將配置從分散式交換器散佈到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 您可以保留不超過 75% 的實體網路介面卡頻寬。例如，如果連線到 ESXi 主機網路介面卡為 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 交換器上的系統流量設定 Network I/O Control 和頻寬配置

為了保證 NSX-T 主機上執行的系統流量的最小頻寬，請在 NSX-T 分散式交換器上啟用並設定網路資源管理。

程序

- 1 登入 NSX Manager Manager，網址為 `https://<nsx-manager-IP-address>`。
 - 2 導覽至 **網狀架構 > 設定檔**。
 - 3 選取 **NIOC 設定檔**。
 - 4 按一下 **+ 新增**。
 - 5 在 [新增 NIOC 設定檔] 畫面中，輸入所需詳細資料。
 - a 輸入 NIOC 設定檔的名稱。
 - b 將狀態變為 **已啟用**。
 - c 在 [主機基礎結構流量資源] 區段中，選取 [流量類型]，然後為 [限制]、[共用率]、[保留] 輸入值。
 - 6 按一下 **新增**。
- 新的 NIOC 設定檔隨即會新增到 NIOC 設定檔清單。

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

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`。

在下列範例回應中，會顯示套用到主機的 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，請建立新的 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.\n\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-c577ae563a",
            "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` 區段中的 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 # [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
}
```

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。

建立 NSX Edge 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。這類節點包含但不限於 NSX Edge。此程序示範如何新增 NSX Edge 來作為傳輸節點。

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` 代理程式不會建立新憑證。

先決條件

- 您必須使用管理平面加入 NSX Edge，且 **網狀架構 > Edge** 頁面上的 [MPA 連線] 必須為 [已開啟]。請參閱 [將 NSX Edge 加入管理平面](#)。
- 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 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取 **網狀架構 > 節點 > 傳輸節點 > 新增**。
- 3 輸入 NSX Edge 傳輸節點的名稱
- 4 從下拉式清單中選取 NSX Edge 網狀架構節點。
- 5 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。

- 6 按一下 **N-VDS** 索引標籤，然後提供 N-VDS 資訊。

選項	說明
N-VDS 名稱	必須符合您在建立傳輸區域時所設定的名稱。
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。
實體 NIC	不同於使用 <code>vmnicX</code> 作為實體 NIC 的主機傳輸節點，NSX Edge 傳輸節點會使用 <code>fp-ethX</code> 。

- 7 (可選) 使用 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>` API 呼叫來檢視傳輸節點。

GET `https://<nsx-mgr>/api/v1/transport-nodes/78a03020-a3db-44c4-a8fa-f68ad4be6a0c`

```
{
  "resource_type": "TransportNode",
  "id": "78a03020-a3db-44c4-a8fa-f68ad4be6a0c",
  "display_name": "node-comp-01b",
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ],
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ],
      "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
    }
  ],
  "node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
  "_create_time": 1459547122893,
  "_last_modified_user": "admin",
  "_last_modified_time": 1459547126740,
  "_create_user": "admin",
  "_revision": 1
}
```

- 8 (可選) 如需狀態資訊，請使用 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 呼叫。

```
{
  "control_connection_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 1,
    "status": "UP"
  },
  "tunnel_status": {
    "down_count": 0,
    "up_count": 0,
    "status": "UNKNOWN",
    "bfd_status": {
      "bfd_admin_down_count": 0,
      "bfd_up_count": 0,
      "bfd_init_count": 0,
      "bfd_down_count": 0
    },
    "bfd_diagnostic": {
      "echo_function_failed_count": 0,
      "no_diagnostic_count": 0,
      "path_down_count": 0,
      "administratively_down_count": 0,
      "control_detection_time_expired_count": 0,
      "forwarding_plane_reset_count": 0,
      "reverse_concatenated_path_down_count": 0,
      "neighbor_signaled_session_down_count": 0,
      "concatenated_path_down_count": 0
    }
  },
  "pnic_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 4,
    "status": "UP"
  },
  "mgmt_connection_status": "UP",
  "node_uuid": "cd4a8501-0ffc-44cf-99cd-55980d3d8aa6",
  "status": "UNKNOWN"
}
```

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。

先決條件

- 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) 在**網狀架構 > 設定檔 > Edge 叢集設定檔**建立 NSX Edge 叢集設定檔以獲得高可用性 (HA)。您也可以使用預設 NSX Edge 叢集設定檔。

程序

- 1 在瀏覽器中，以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 導覽至**網狀架構 > 節點 > Edge 叢集 > 新增**。
- 3 為 NSX Edge 叢集輸入名稱。
- 4 選取 NSX Edge 叢集設定檔。
- 5 按一下**編輯**，然後選取**實體機器**或**虛擬機器**。
「實體機器」是指在裸機上安裝的 NSX Edge。「虛擬機器」則是指安裝作為虛擬機器/應用裝置的 NSX Edge。
- 6 對於虛擬機器，請從 [成員類型] 下拉式功能表中選取 [NSX Edge 節點] 或**公用雲端閘道節點**。
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]。
- 7 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》。

NSX Cloud 元件安裝

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。

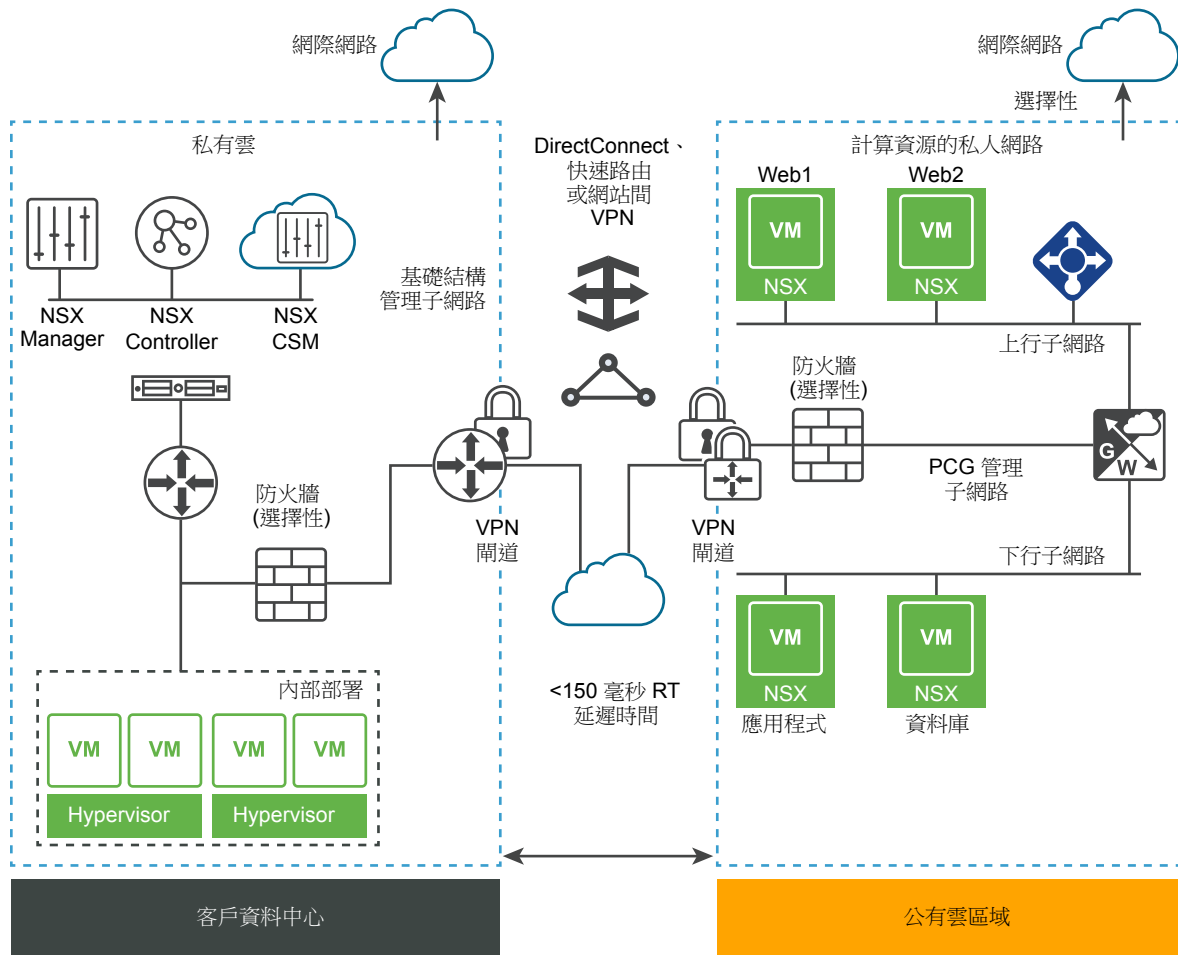
本章包含以下主題：

- [NSX Cloud 架構和元件](#)
- [安裝 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 PCG](#)
- [取消部署 PCG](#)

NSX Cloud 架構和元件

NSX Cloud 將 NSX-T Data Center 核心元件、NSX Manager 及 NSX Controller 與公有雲整合，以在所有實作中提供網路與安全性。

圖 9-1: NSX Cloud 架構



核心 NSX Cloud 元件如下：

- NSX Manager，用於已定義角色型存取控制 (RBAC) 的管理平面。
- NSX Controller，用於控制平面和執行階段狀態。
- Cloud Service Manager，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，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。
- 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。

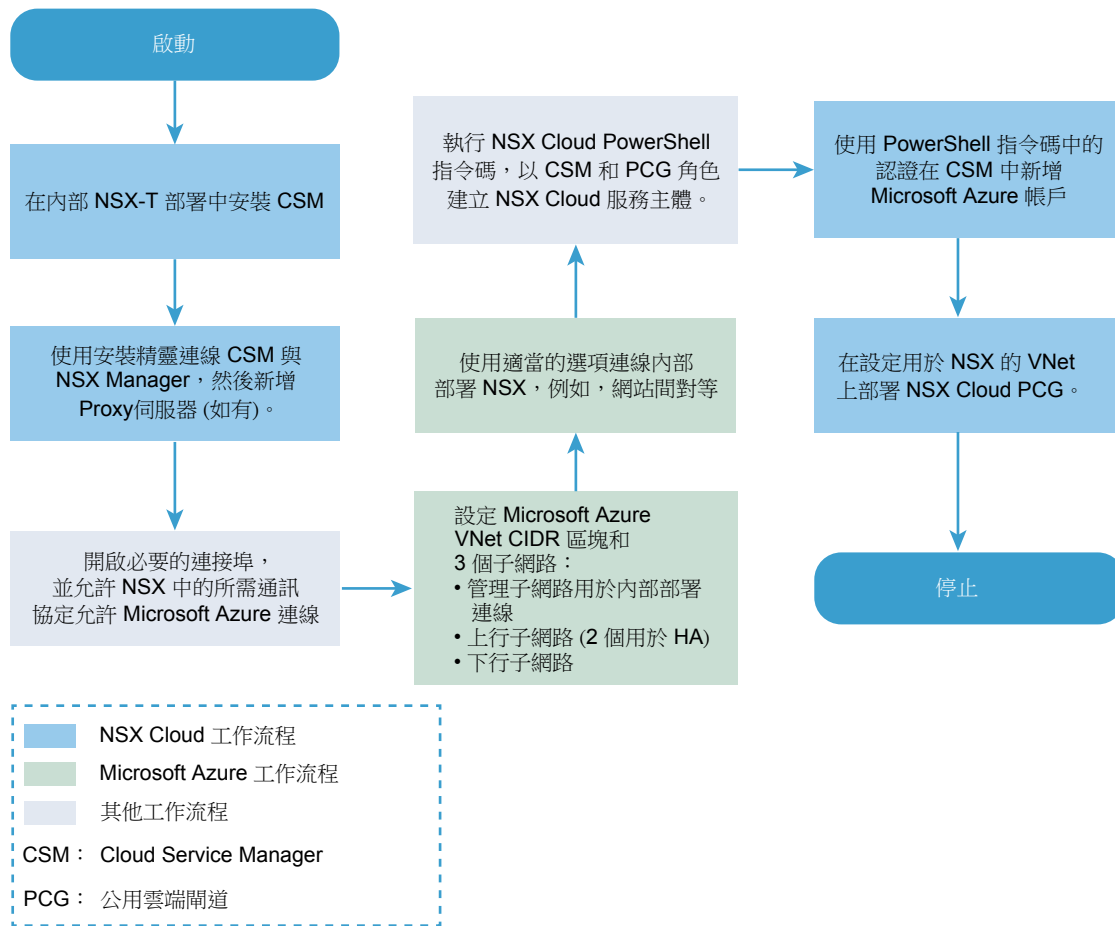
安裝 NSX Cloud 元件的概觀

請參閱這些流程圖，以瞭解啟用 NSX-T Data Center 來管理公有雲中的工作負載虛擬機器的 0 天作業概觀。

Microsoft Azure 的 0 天工作流程

此流程圖顯示將 Microsoft Azure VNet 新增至 NSX Cloud 所涉及步驟的概觀。

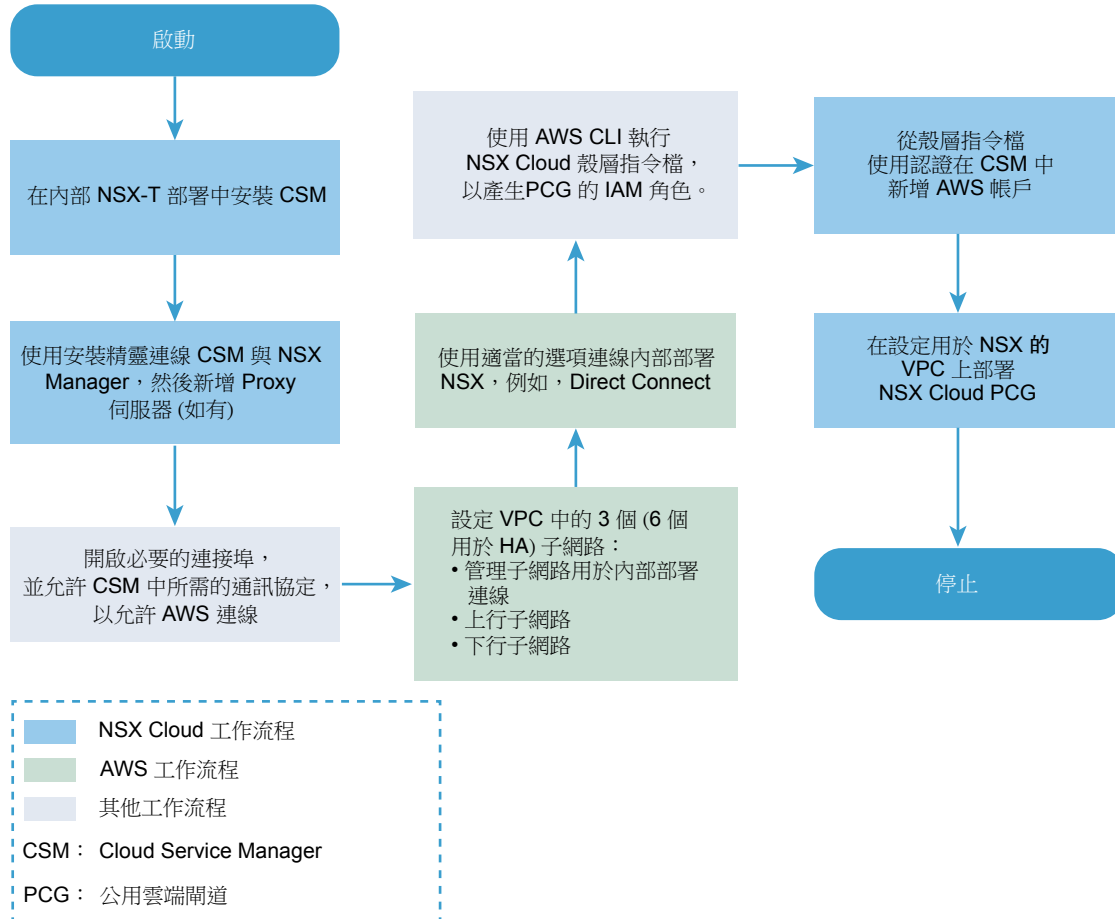
圖 9-2: Microsoft Azure 的 NSX Cloud 0 天工作流程



AWS 的 0 天工作流程

此流程圖顯示將 AWS VPC 新增至 NSX Cloud 所涉及步驟的概觀。

圖 9-3: AWS 的 NSX Cloud 0 天工作流程



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](#)。

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，您還必須能夠使用 NSX-T API 發佈 NSX Manager 的 FQDN。

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》。

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。

先決條件

- 必須安裝 NSX Manager，且您必須擁有登入 NSX Manager 的管理員權限
- 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 開啟 NSX Manager 的 SSH 工作階段。
- 2 在 NSX Manager 上，執行 `get certificate api thumbprint` 命令。

```
NSX-Manager> get certificate api thumbprint
```

此命令的輸出是對此 NSX Manager 而言唯一的數字字串。

- 3 以企業管理員角色登入 CSM。
- 4 按一下 **系統 > 設定**。然後，在標題為**相關聯的 NSX 節點**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。

- 5 輸入 NSX Manager 的詳細資料。

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	輸入具有企業管理員角色的使用者名稱和密碼。
管理員指紋	輸入您在步驟 2 中取得之 NSX Manager 的指紋值。

6 按一下連線。

CSM 會確認 NSX Manager 指紋並建立連線。

(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。

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：

表格 9-1.

來源	目的地	通訊協定/連接埠	說明
PCG	NSX Manager	TCP/5671	從公有雲到內部部署 NSX-T Data Center 的輸入流量 (用於管理平面通訊)。
PCG	NSX Manager	TCP/8080	從公有雲到內部部署 NSX-T Data Center 的輸入流量 (用於升級)。
PCG	NSX Controller	TCP/1234、TCP/1235	從公有雲到內部部署 NSX-T Data Center 的輸入流量 (用於控制平面通訊)。
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
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。

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**。

- 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。

啟用 CSM 以存取 Microsoft Azure 詳細目錄

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。

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。

為了讓 NSX Cloud 在訂閱中運作，您需要建立新的服務主體以授與所需的 NSX-T Data Center 存取權。您還需要為 CSM 和 PCG 建立 MSI 角色。

NSX Cloud 可提供 PowerShell 指令碼以產生服務主體。

此程序分為兩步：

- 1 使用 NSX Cloud PowerShell 指令碼：
 - 建立 NSX Cloud 的服務主體帳戶。
 - 為 CSM 建立角色並將其連結至服務主體。
 - 為 PCG 建立角色並將其連結至服務主體。
- 2 在 CSM 中新增 Microsoft Azure 訂閱。

產生所需角色

NSX Cloud 利用 Microsoft Azure 的受管理服務身分識別 (MSI) 功能來管理驗證，同時保護您的 Microsoft 認證安全。

若要讓 NSX Cloud 在 Microsoft Azure 訂閱中運作，您需要產生 CSM 和 PCG 的 MSI 角色以及 NSX Cloud 的服務主體。

透過執行 NSX Cloud PowerShell 指令碼，可實現此操作。此外，您需要兩個 JSON 格式的檔案做為參數。以所需參數執行 PowerShell 指令碼時，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。

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。

先決條件

- 您必須具有已安裝 AzureRM 模組的 PowerShell 5.0+。
- 您必須是要執行指令碼以產生 NSX Cloud 服務主體之 Microsoft Azure 訂閱的擁有者。

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：

檔案名稱	說明
CreateNSXRoles.ps1	這是 PowerShell 指令碼，用以產生 NSX Cloud 服務主體以及 CSM 和 PCG 的 MSI 角色
nsx_csm_role.json	此檔案包含 CSM 角色名稱和此角色在 Microsoft Azure 中的權限。這是 PowerShell 指令碼的輸入，必須與指令碼位於相同的資料夾。
nsx_pcg_role.json	此檔案包含 PCG 角色名稱和此角色在 Microsoft Azure 中的權限。這是 PowerShell 指令碼的輸入，必須與指令碼位於相同的資料夾。預設 PCG (閘道) 角色名為 nsx-pcg-role。

備註 如果您要在 Microsoft Azure Active Directory 中建立多個訂閱的角色，您必須在相應 JSON 檔案中變更每個訂閱的 CSM 和 PCG 角色名稱，然後重新執行指令碼。

3 以 Microsoft Azure 訂閱識別碼做為參數來執行指令碼。參數名稱為 subscriptionId。

例如，

```
.\CreateNSXRoles.ps1 -subscriptionId <your_subscription_ID>
```

這會建立 NSX Cloud 的服務主體、具有 CSM 和 PCG 的適當權限的角色，並且將 CSM 和 PCG 角色連結到 NSX Cloud 服務主體。

4 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

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](#)

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。

先決條件

- 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。

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。
開道角色名稱	預設值為 <code>nsx-pcg-role</code> 。如果您已變更預設值，此值可以從 <code>nsx_pcg_role.json</code> 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，該帳戶會在數分鐘之內顯示在**帳戶**區段中。

後續步驟

在 [Microsoft Azure VNet 中部署 PCG](#)

啟用 CSM 以存取 AWS 詳細目錄

您的 AWS 帳戶包含一或多個您想要置於 NSX-T Data Center 管理之下的運算 VPC。

此程序分為三步：

- 1 使用需要 AWS CLI 的 NSX Cloud 指令碼執行下列操作：
 - 建立 IAM 設定檔。
 - 為 PCG 建立角色。
- 2 在 CSM 中新增 AWS 帳戶。

產生所需角色

NSX Cloud 利用 AWS IAM 來產生連結到 NSX Cloud 設定檔的角色，為 PCG 提供存取 AWS 帳戶的必要權限。

若要讓 NSX Cloud 在 AWS 帳戶中運作，您需要為 PCG 產生 IAM 設定檔和角色。

透過使用 AWS CLI 執行可建立下列建構的 NSX Cloud 殼層指令檔，可實現此操作：

- NSX Cloud 的 IAM 設定檔。
- 使 PCG 能夠在公有雲詳細目錄上運作的角色。

先決條件

- 您必須使用 AWS 帳戶的存取金鑰和秘密金鑰安裝並設定 AWS CLI。
- 您必須選擇出要提供給指令碼的唯一 IAM 設定檔名稱。開道角色名稱已連結到此 IAM 設定檔
-

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 AWS_create_credentials.sh 的殼層指令檔。
- 2 執行指令碼，然後在系統提示時輸入 IAM 設定檔的名稱。例如，

```
bash AWS_create_NSXCloud_credentials.sh
```

- 3 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。這些值均儲存於執行指令碼之相同目錄中的輸出檔案。檔案名為 aws_details.txt。

備註 依預設，PCG (開道) 角色名稱為 nsx_pcg_service。如果您想要開道角色名稱使用其他值，您可以在指令碼中進行變更。此值對於在 CSM 中新增 AWS 帳戶是必要的，因此如果要變更預設值，您必須記下此值。

後續步驟

在 CSM 中新增 AWS 帳戶

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
秘密金鑰	輸入您帳戶的秘密金鑰

選項	說明
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 <code>nsx_pcg_service</code> 。您可以在檔案 <code>aws_details.txt</code> 中的指令碼輸出中找到此值。

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 [AWS VPC 中部署 PCG](#)

部署 PCG

NSX Public Cloud Gateway (PCG) 會在公有雲和 NSX-T Data Center 內部部署管理元件之間提供南北向連線。

必要條件

- 公有雲帳戶必須已新增至 CSM。
- 部署 PCG 的 VPC 或 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。

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 Microsoft Azure VNet 中部署 PCG

請依照下列指示，在 Microsoft Azure 訂閱中部署 PCG。

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。
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 開道啟用 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 AWS VPC 中部署 PCG

請依照下列指示，在 AWS 帳戶中部署 PCG。

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	預設選取項目為 [已啟用]。這是綠地部署的建議事項。如果您的 VPC 中已啟動虛擬機器，請停用隔離原則。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 <code>us-west-1a</code>) 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 <code>us-west-1b</code>) 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**。

部署 PCG 後建立的建構

將在 NSX Manager 中建立和設定重要 NSX-T Data Center 實體，並且在 PCG 成功部署後在公有雲中建立安全群組。

NSX Manager 組態

將在 NSX Manager 中自動建立下列實體：

- 會建立名為公用雲端閘道 (PCG) 的 Edge 節點。
- PCG 會新增至 Edge 叢集。在高可用性部署中，存在兩個 PCG。
- PCG (或兩個 PCG) 會做為傳輸節點向已建立的兩個傳輸區域進行登錄。
- 會建立兩個預設邏輯交換器。
- 會建立一個第 0 層邏輯路由器。
- 會建立 IP 探索設定檔。此項用於覆疊邏輯交換器。
- 會建立 DHCP 設定檔。此項用於 DHCP 伺服器。

- 會建立名為 **PublicCloudSecurityGroup** 的預設 NSGroup，其中包含下列成員：
 - 預設 VLAN 邏輯交換器
 - 邏輯連接埠，分別用於 PCG 上行連接埠 (如果已啟用 HA)。
 - IP 位址
- 會建立三個預設 Distributed Firewall 規則：
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

備註 這些 DFW 規則封鎖所有流量，並且需要根據特定需求進行調整。

確認 NSX Manager 中的下列組態：

- 1 從 NSX Cloud 儀表板中，按一下 **NSX Manager**。
- 2 瀏覽至**網狀架構 > 節點 > Edge**。公用雲端閘道應會列為 Edge 節點。
- 3 確認部署狀態、管理程式連線和控制器連線均已連線 (狀態顯示**開啟**並具有綠色的點)。
- 4 瀏覽至**網狀架構 > 節點 > Edge 叢集**以確認 Edge 叢集和 PCG 已新增為此叢集的一部分。
- 5 瀏覽至**網狀架構 > 節點 > 傳輸節點**，以確認 PCG 已做為傳輸節點登錄，並且已連線到部署 PCG 時自動建立的兩個傳輸區域：
 - 流量類型 VLAN -- 此項連線至 PCG 上行
 - 流量類型覆疊 -- 此項用於覆疊邏輯網路
- 6 確認是否已建立邏輯交換器和第 0 層邏輯路由器，並且邏輯路由器已新增至 Edge 叢集。

重要 請勿刪除任何 NSX 建立的實體。

公有雲組態

在 AWS 中：

- 在 AWS VPC 中，以名稱 `nsx-gw.vmware.local` 新增類型 A 記錄集。對應到此記錄的 IP 位址與 PCG 的管理 IP 位址相符。這由 AWS 使用 DHCP 進行指派，並且視每個 VPC 而有所不同。
- 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。

表格 9-2. 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

表格 9-3. 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)

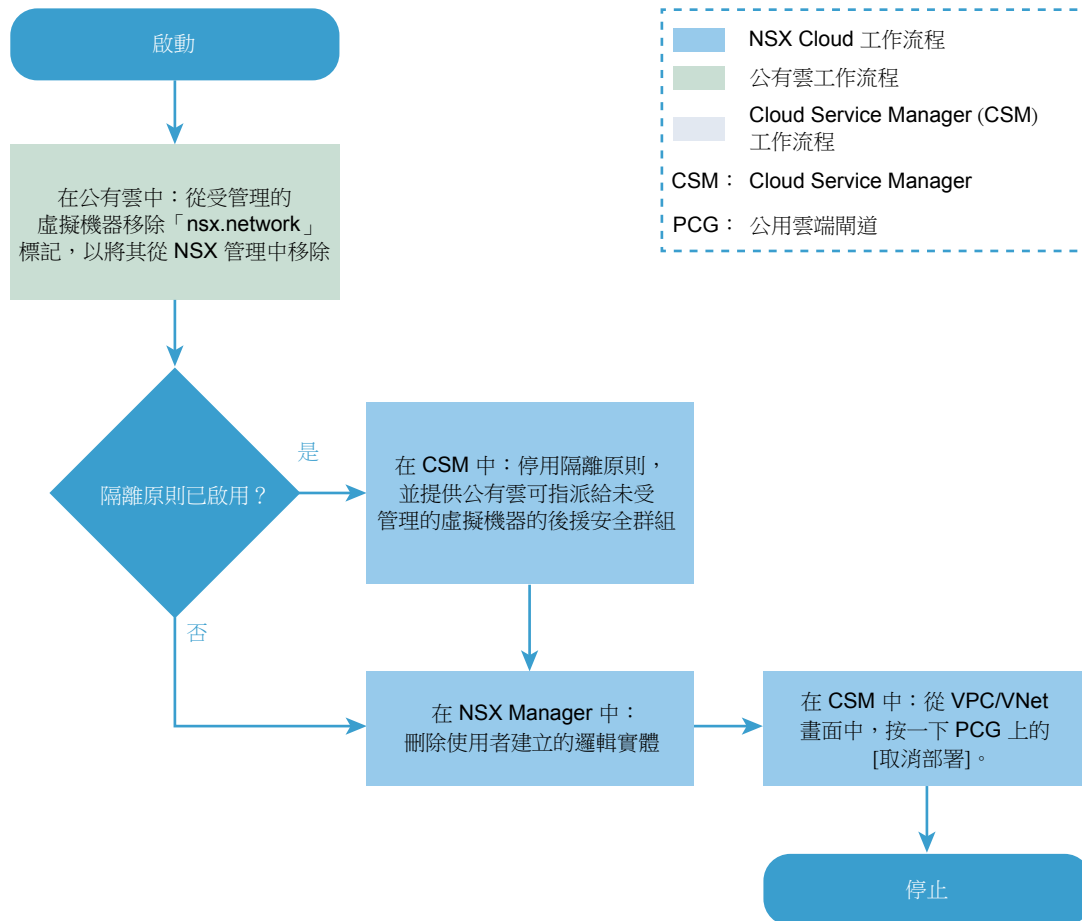
取消部署 PCG

請參閱此流程圖，以瞭解取消部署 PCG 所涉及的步驟。

- 若要取消部署 PCG，必須滿足下列條件：VPC 或 VNet 中的工作負載虛擬機器不得由 NSX 管理。
- 必須停用隔離原則。

- 必須先刪除與 PCG 相關聯的使用者建立的所有邏輯實體。

圖 9-4：取消部署 PCG



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

刪除您在 NSX Manager 中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)

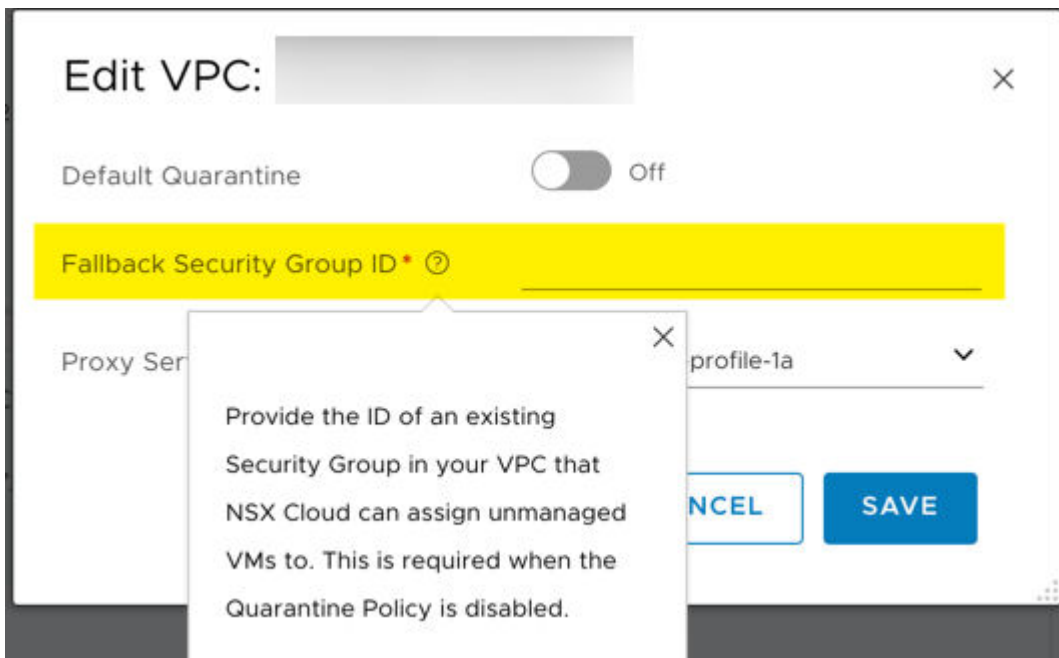
如果先前已啟用，則必須停用隔離原則才能取消部署 PCG。

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[部署 PCG 後建立的建構](#)，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

刪除您在 NSX Manager 中建立的所有邏輯實體。

請參閱以下清單以找到您要刪除的實體：

備註 請勿刪除部署 PCG 時自動建立的邏輯實體。請參閱[部署 PCG 後建立的建構](#)

- 公有雲 DNS 項目
- DDI: DHCP 設定檔
- 路由: SNAT 規則
- 路由: 靜態路由器
- 路由: 邏輯路由器連接埠
- 路由: 邏輯路由器
- 網狀架構節點: Edge 叢集
- 網狀架構節點: 傳輸節點
- 網狀架構節點: Edge
- 網狀架構設定檔: PCG-Uplink-HostSwitch-Profile
- 交換: 邏輯交換器連接埠
- 交換: 邏輯交換器
- 網狀架構傳輸區域: 傳輸區域
- 交換: PublicCloud-Global-SpoofGuardProfile

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**欄道。

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**欄道。

PCG 取消部署後，會自動移除 NSX Cloud 所建立的預設實體。

解除安裝 NSX-T Data Center

您可以移除某個 NSX-T Data Center 覆疊的元素、從 NSX-T Data Center 中移除 Hypervisor 主機，或是完全解除安裝 NSX-T Data Center。

本章包含以下主題：

- 取消設定 NSX-T Data Center 覆疊
- 從 NSX-T Data Center 中移除主機或完整解除安裝 NSX-T Data Center

取消設定 NSX-T Data Center 覆疊

如果您想要刪除覆疊但要保留您的傳輸節點，請遵循下列步驟。

程序

- 1 登入 vSphere Client。
- 2 在您的虛擬機器管理工具中，將所有虛擬機器從任何邏輯交換器中斷連結，然後將虛擬機器連線至非 NSX-T Data Center 網路。
- 3 對於 KVM 主機，使用 SSH 連線至主機，並關閉虛擬機器電源。

```
shutdown -h now
```
- 4 在 NSX Manager UI 或 API 中，刪除所有的邏輯路由器。
- 5 在 NSX Manager UI 或 API 中，刪除所有的邏輯交換器連接埠，然後刪除所有的邏輯交換器。
- 6 在 NSX Manager UI 或 API 中刪除所有的 NSX Edge，然後刪除所有的 NSX Edge 叢集。
- 7 視需要設定新的 NSX-T Data Center 覆疊。

從 NSX-T Data Center 中移除主機或完整解除安裝 NSX-T Data Center

如果您要完整解除安裝 NSX-T Data Center，或僅從 NSX-T Data Center 中移除 Hypervisor 主機，而使該主機不會再次參與 NSX-T Data Center 覆疊，請遵循下列步驟。

下列程序說明如何執行 NSX-T Data Center 的完整解除安裝。

先決條件

如果虛擬機器管理工具為 vCenter Server，請將 vSphere 主機置於維護模式。

程序

- 1 在 NSX Manager 中，選取**網狀架構 > 節點 > 傳輸節點**，然後刪除主機傳輸節點。

刪除此傳輸節點會導致 N-VDS 從主機上移除。您可以藉由執行下列命令來確認這一點。

```
[root@host:~] esxcli network vswitch dvs vmware list
```

在 KVM 上，此命令為：

```
ovs-vsctl show
```

- 2 在 NSX Manager CLI 中，確認 NSX-T Data Center 安裝-升級服務已在執行。

```
nsx-manager-1> get service install-upgrade
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 從管理平面將主機解除安裝，並移除 NSX-T Data Center 模組。

移除所有 NSX-T Data Center 模組可能需要花費 5 分鐘。

您可以採用數種方法來移除 NSX-T Data Center 模組：

- 在 NSX Manager 中，選取**網狀架構 > 節點 > 主機 > 刪除**。
 確定已選取**解除安裝 NSX 元件**。這會使 NSX-T Data Center 模組在主機上解除安裝。
 移除 RHEL 7.4 相依性套件 - json_spirit、python-greenlet、libev、protobuf、leveldb、python-gevent、python-simplejson、glog。
 移除 Ubuntu 16.04.x 相依性套件 - nicira-ovs-hypervisor-node、openvswitch-switch、openvswitch-datapath-dkms、openvswitch-pki、python-openvswitch、openvswitch-common、libjson-spirit。
 請注意 使用未選取**解除安裝 NSX 元件**選項的**網狀架構 > 節點 > 主機 > 刪除**並非解除登錄主機的方法。此做法僅供狀態不良的主機作為因應措施。
- (由計算管理員管理的主機) 在 NSX Manager 中，選取**網狀架構 > 節點 > 主機 > 傳輸節點 > 刪除主機**。
 在 NSX Manager 中，選取**網狀架構 > 節點 > 主機 > 計算管理員 > 設定叢集管理員**，然後取消勾選**自動安裝 NSX**。選取節點，然後按一下**解除安裝 NSX**。
 確定已選取**解除安裝 NSX 元件**。這會使 NSX-T Data Center 模組在主機上解除安裝。
- 使用 DELETE /api/v1/fabric/nodes/<node-id> API。

備註 此 API 不會從 nsx-lcp 服務包移除相依性套件。

移除 RHEL 7.4 相依性套件 - json_spirit、python-greenlet、libev、protobuf、leveldb、python-gevent、python-simplejson、glog。

移除 Ubuntu 16.04.x 相依性套件 - nicira-ovs-hypervisor-node、openvswitch-switch、openvswitch-datapath-dkms、openvswitch-pki、python-openvswitch、openvswitch-common、libjson-spirit。

■ 針對 vSphere 使用 CLI。

a 取得管理員指紋。

```
manager> get certificate api thumbprint
```

b 在主機的 NSX-T Data Center CLI 上，執行下列命令以將主機從管理平面中斷連結。

```
host> detach management-plane <MANAGER> username <ADMIN-USER> password <ADMIN-PASSWORD>
thumbprint <MANAGER-THUMBPRINT>
```

c 在主機上，執行下列命令以移除篩選器。

```
[root@host:~] vsipioctl clearallfilters
```

d 在主機上，執行下列命令以停止 netcpa。

```
[root@host:~] /etc/init.d/netcpad stop
```

e 關閉主機上的虛擬機器的電源，或將其移轉至另一台主機。

f 在主機上，執行下列命令以手動解除安裝 NSX-T Data Center 組態和模組。所有主機類型皆支援此命令。

```
[root@host:~] clear management-plane
```

後續步驟

進行此變更後，主機會從管理平面移除，且無法再次參與 NSX-T Data Center 覆疊。

如果您要完整移除 NSX-T Data Center，請在您的虛擬機器管理工具中關閉 NSX Manager、NSX Controller 和 NSX Edge，然後從磁碟中將其刪除。