

NSX-T 安裝指南

VMware NSX-T Data Center 1.1



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 © 2017 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

NSX-T 安裝指南 5

1 NSX-T 概觀 6

數據平面 8

控制平面 8

管理平面 8

NSX Manager 9

NSX Controller 9

邏輯交換器 10

邏輯路由器 10

NSX Edge 11

傳輸區域 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 18

NSX Manager 所使用的 TCP 和 UDP 連接埠 19

NSX Controller 所使用的 TCP 和 UDP 連接埠 20

NSX Edge 所使用的 TCP 和 UDP 連接埠 21

由金鑰管理員所使用的 TCP 連接埠 22

安裝概觀 23

3 使用 KVM 24

設定 KVM 24

在 KVM CLI 中管理您的客體虛擬機器 28

4 NSX Manager 安裝 30

使用 vSphere Web Client 在 ESXi 上安裝 NSX Manager 31

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager 33

在 KVM 上安裝 NSX Manager 36

5 NSX Controller 安裝和叢集 40

使用 GUI 在 ESXi 上安裝 NSX Controller 41

使用命令列 OVF Tool 在 ESXi 上安裝 NSX Controller 44

在 KVM 上安裝 NSX Controller 47

將 NSX Controller 加入管理平面 49

初始化控制叢集以建立控制叢集主節點 50

[將其他 NSX Controller 加入叢集主節點](#) 52

6 NSX Edge 安裝 55

[NSX Edge 網路設定](#) 56

[使用 GUI 在 ESXi 上安裝 NSX Edge](#) 61

[使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge](#) 63

[透過 ISO 檔案與 PXE 伺服器安裝 NSX Edge](#) 67

[在裸機上安裝 NSX Edge](#) 72

[透過 ISO 檔案將 NSX Edge 安裝為虛擬應用裝置](#) 74

[將 NSX Edge 加入管理平面](#) 77

7 主機準備 78

[在 KVM 主機上安裝第三方套件](#) 78

[將 Hypervisor 主機新增到 NSX-T 網狀架構](#) 79

[NSX-T 核心模組的手動安裝](#) 84

[將 Hypervisor 主機加入管理平面](#) 88

8 傳輸區域和傳輸節點 91

[關於傳輸區域](#) 91

[為通道端點 IP 位址建立 IP 集區](#) 92

[建立上行設定檔](#) 95

[建立傳輸區域](#) 98

[建立主機傳輸節點](#) 100

[建立 NSX Edge 傳輸節點](#) 105

[建立 NSX Edge 叢集](#) 109

9 解除安裝 NSX-T 111

[取消設定 NSX-T 覆疊](#) 111

[從 NSX-T 中移除主機或完整解除安裝 NSX-T](#) 111

NSX-T 安裝指南

NSX-T 安裝指南 說明了如何安裝 VMware NSX-T[®] 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 的任何人。本資訊是專為具有經驗且熟悉虛擬機器技術和虛擬資料中心操作的系統管理員所撰寫的。本手冊假設使用者熟悉虛擬機器管理服務，例如 VMware vSphere 5.5 或 6.0，包括 VMware ESX、vCenter Server，以及 vSphere Web Client 和 VMware OVF Tool，或是其他具有核心型虛擬機器 (KVM) 的虛擬機器管理服務。

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 概觀

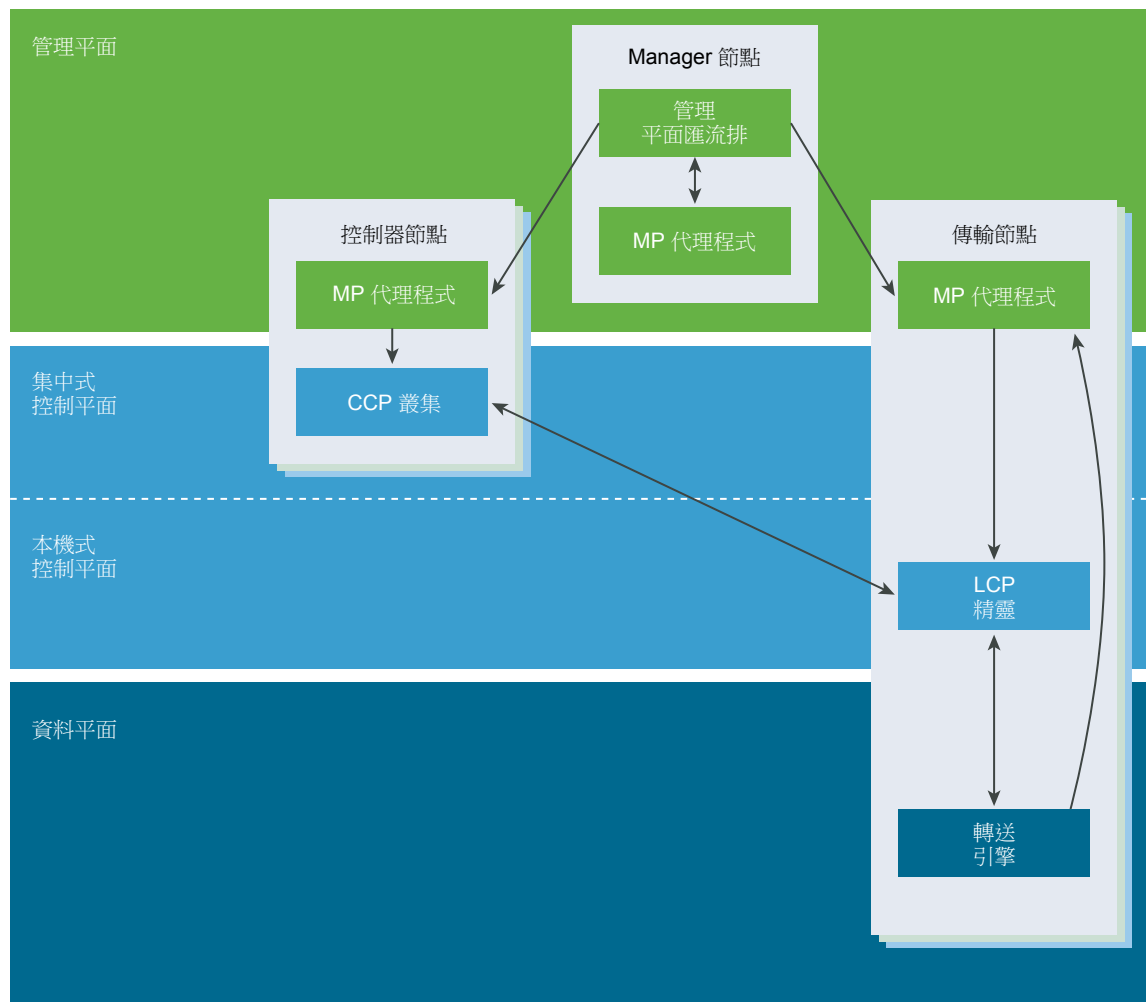
比照伺服器虛擬化透過程式設計的方法來建立、刪除、還原軟體型虛擬機器 (VM) 及建立其快照的方式，**NSX-T** 網路虛擬化會以相似的方式透過程式設計的方法來建立、刪除、還原軟體型虛擬網路及建立其快照。

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 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。各個 **NSX-T** 安裝支援單一 **NSX Manager** 節點，並且不支援 **NSX Manager** 叢集。
- **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：

- 數據平面
- 控制平面
- 管理平面
- NSX Manager
- NSX Controller
- 邏輯交換器
- 邏輯路由器
- NSX Edge
- 傳輸區域
- 主要概念

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。

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。

我們有時候會將控制平面描述為網路的訊號。如果您要處理訊息，以便在靜態使用者組態存在的情況下維護資料平面 (例如，回應虛擬機器 (VM) 的 **vMotion** 是控制平面的責任，但將虛擬機器連線至邏輯網路則是管理平面的責任)。控制平面常會作為資料平面元素彼此間拓撲資訊的反射程式，例如 **VTEP** 的 **MAC**/通道對應。在其他情況下，控制平面則會作用在從某些資料平面元素所收到的資料，以重新設定/設定某些資料平面元素，例如使用 **VIF** 定位器來為通道計算和建立正確的子集網路。

控制平面所處理的物件集包括 **VIF**、邏輯網路、邏輯連接埠、邏輯路由器和 **IP** 位址等項目。

在 **NSX-T** 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。

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** 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 UI** 可以進行變更。

在 **NSX** 中，也有一個執行於所有叢集和傳輸節點上的管理平面代理程式 (**MPA**)。範例使用案例是啟動載入如中央管理節點位址認證、套件、統計資料和狀態等組態。**MPA** 在執行時可相對獨立於控制平面和資料平面以外，並且可在其程序當機或中斷時獨立重新啟動，不過某些案例中，由於執行於相同的主機上，因此仍會產生連帶作用。**MPA** 可以從本機和遠端進行存取。**MPA** 可在傳輸節點、控制節點和管理節點上執行，以便進行節點管理。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 提供可用來建立、設定及監控 **NSX-T** 元件 (例如控制器、邏輯交換器和 **Edge** 服務閘道) 的圖形使用者介面 (GUI) 與 **REST API**。

NSX Manager 是 **NSX-T** 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** 的集中式網路管理元件。它提供用來對連結至 **NSX-T** 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。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 - **Edge** 服務和安全性服務可由 **NSX Manager** 的內建元件提供，或由第三方廠商進行整合。

NSX Manager 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** 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 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 Controller

NSX Controller 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** 架構中的虛擬網路程式設計部署。**NSX-T** 中央控制平面 (CCP) 會以邏輯方式與所有資料平面流量分隔，這表示控制平面中的任何失敗皆不影響現有的資料平面作業。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。

邏輯交換器

NSX Edge 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。

虛擬資料中心的雲端部署具有多種用於多個承租人之間的應用程式。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** 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。

邏輯路由器

NSX-T 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。

邏輯路由器是以傳統網路硬體路由器設定的磁碟分割。它會複寫硬體的功能，在單一路由器內建立多個路由網域。邏輯路由器可執行能夠由實體路由器處理的工作子集，且每個路由器可包含多個路由執行個體和路由表。使用邏輯路由器可能是讓路由器發揮最大用途的有效方式，因為單一實體路由器內的一組邏輯路由器，可執行過去須由數個不同設備執行的作業。

透過 **NSX-T**，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** 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 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。

NSX Edge

NSX Edge 可提供在 NSX-T 部署以外的路由服務和網路連線。

透過 NSX Edge，在不同子網路中位於相同主機上的虛擬機器或工作負載將可相互通訊，而不需要周遊傳統的路由介面。

從 NSX-T 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

傳輸區域會控制邏輯交換器所能連線的主機。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。

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 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。

一個節點若至少包含一個主機交換器，則可作為傳輸節點。當您建立主機傳輸節點，並將該節點新增至傳輸區域後，NSX-T 會在該主機上安裝主機交換器。針對該主機所屬的每個傳輸區域，系統皆會安裝個別的主機交換器。主機交換器會用來將虛擬機器連結至 NSX-T 邏輯交換器，以及用來建立 NSX-T 邏輯路由器上行和下行。

主要概念

用於說明文件和使用界面中的一般 **NSX-T** 概念。

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。
資料平面	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 管理的實體網路或 VLAN 。您可以連結您的邏輯網路，或透過 NSX Edge 將網路覆疊至外部網路。例如，客戶資料中心內的實體網路，或實體環境中的 VLAN 。
網狀架構節點	已向 NSX-T 管理平面登錄、並且已安裝 NSX-T 模組的節點。 Hypervisor 主機或 NSX Edge 若要成為 NSX-T 覆疊的一部分，則必須新增至 NSX-T 網狀架構中。
網狀架構設定檔	代表可與 NSX Edge 叢集建立關聯的特定組態。例如，網狀架構設定檔可能包含無作用對等偵測的通道內容。
邏輯連接埠出口	虛擬機器或邏輯網路的輸入網路流量稱為出口流量，因為這是離開資料中心網路而進入虛擬空間的流量。
邏輯連接埠入口	從虛擬機器輸出至資料中心網路的網路流量稱為入口流量，因為這是進入實體網路的流量。
邏輯路由器	NSX-T 路由實體。
邏輯路由器連接埠	您的邏輯交換器連接埠所能連結到的邏輯路由器連接埠，或實體網路的上行連接埠。
邏輯交換器	為虛擬機器介面和閘道介面提供虛擬第 2 層交換的 API 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。如此，承租人網路管理員將可直接移轉虛擬機器，而無須重新設定。 在多承租人雲端中，許多邏輯交換器可能會並存於相同的 Hypervisor 硬體上，但其各自的第 2 層區段則彼此隔離。邏輯交換器可使用邏輯路由器來連線，而邏輯路由器可提供連線至外部實體網路的上行連接埠。
邏輯交換器連接埠	用來建立虛擬機器網路介面或邏輯路由器介面之連線的邏輯交換器連結點。邏輯交換器連接埠會報告已套用的交換設定檔、連接埠狀態和連結狀態。
管理平面	提供系統的單一 API 進入點、持續保存使用者組態、處理使用者查詢，以及執行系統中的所有管理、控制和資料平面節點的運作工作。管理平面也負責查詢、修改及持續保存使用組態。

NSX 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 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-T 主機交換器或 KVM Open vSwitch	<p>在 Hypervisor 上執行並提供實體流量轉送的軟體。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所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 主機交換器，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。</p> <p>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的通道。網路控制器具有資料中心的全域視圖，且可確保 Hypervisor 主機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。</p>
NSX Manager	主控 API 服務、管理平面和代理程式服務的節點。
Open vSwitch (OVS)	可在 XenServer、Xen、KVM 和其他 Linux 型 Hypervisor 內作為 Hypervisor 主機交換器的開放原始碼軟體交換器。NSX Edge 交換元件以 OVS 為基礎。
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。NSX-T 可將必要的支援軟體套件部署至主機，因為它知道在邏輯交換器上會啟用哪些功能。

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。

VTEP

虛擬通道端點。通道端點可讓 Hypervisor 主機加入 NSX-T 覆疊。NSX-T 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 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 Manager 所使用的 TCP 和 UDP 連接埠
- NSX Controller 所使用的 TCP 和 UDP 連接埠
- NSX Edge 所使用的 TCP 和 UDP 連接埠
- 由金鑰管理員所使用的 TCP 連接埠
- 安裝概觀

系統需求

NSX-T 具有關於硬體資源和軟體版本的特定需求。

Hypervisor

表格 2-1. Hypervisor 需求

Hypervisor	版本	CPU 核心	記憶體
ESXi	■ 6.5	4	16 GB
	■ 6.0 修補程式 P04 版		
RHEL KVM	7.1 (僅限 3.10.0-229 核心)、7.2 (僅限 3.10.0-327 核心)	4	16 GB
Ubuntu KVM	14.04.x (3.13 或 4.4 核心)、16.04.x (僅限 4.4 核心)	4	16 GB

若為 ESXi，NSX-T 並不支援主機設定檔及自動部署功能。



注意 在 RHEL 上，`yum update` 命令可能會更新核心版本，而損及與 NSX-T 之間的相容性。執行 `yum update` 時請務必停用核心更新。此外，在執行 `yum install` 之後，請確認核心版本受 NSX-T 的支援。

NSX Manager 和 NSX Controller

表格 2-2. NSX Manager 和 NSX Controller 資源需求

應用裝置	記憶體	vCPU	磁碟空間
NSX Manager	16 GB	2	140 GB
NSX Controller	16 GB	2	120 GB

vSphere ESXi 5.5 和更新版本支援 NSX Manager 和 NSX Controller 虛擬機器。

NSX Edge

表格 2-3. NSX Edge 資源需求

部署大小	記憶體	vCPU	磁碟空間
小	4 GB	2	120 GB
中	8 GB	4	120 GB
大	16 GB	8	120 GB

表格 2-4. NSX Edge 實體硬體需求

硬體	類型
CPU	<ul style="list-style-type: none"> ■ Xeon 56xx (Westmere-EP) ■ Xeon E7-xxxx (Westmere-EX) ■ Xeon E5-xxxx (Sandy Bridge)
NIC	<ul style="list-style-type: none"> ■ Intel 82599 ■ Intel X540

裸機 NSX Edge 系統需求

產品代碼

- X520QDA1
- E10G42BT (X520-T2)
- E10G42BTDA (X520-DA2)
- E10G42BTDABLK
- X520DA1OCP
- X520DA2OCP
- E10G41BFSR (X520-SR1)
- E10G41BFSRBLK
- E10G42BFSR (X520-SR2)
- E10G42BFSRBLK

- E10G41BFLR (X520-LR1)
- E10G41BFLRBL

NIC PCI 裝置識別碼	說明
0x10F7	IXGBE_DEV_ID_82599_KX4
0x1514	IXGBE_DEV_ID_82599_KX4_MEZZ
0x1517	IXGBE_DEV_ID_82599_KR
0x10F8	IXGBE_DEV_ID_82599_COMBO_BACKPLANE
0x000C	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ
0x10F9	IXGBE_DEV_ID_82599_CX4
0x10FB	IXGBE_DEV_ID_82599_SFP
0x11A9	IXGBE_SUBDEV_ID_82599_SFP
0x1F72	IXGBE_SUBDEV_ID_82599_RNDC
0x17D0	IXGBE_SUBDEV_ID_82599_560FLR
0x0470	IXGBE_SUBDEV_ID_82599_ECNA_DP
0x152A	IXGBE_DEV_ID_82599_BACKPLANE_FCOE
0x1529	IXGBE_DEV_ID_82599_SFP_FCOE
0x1507	IXGBE_DEV_ID_82599_SFP_EM
0x154D	IXGBE_DEV_ID_82599_SFP_SF2
0x154A	IXGBE_DEV_ID_82599_SFP_SF_QP
0x1558	IXGBE_DEV_ID_82599_QSFP_SF_QP
0x1557	IXGBE_DEV_ID_82599EN_SFP
0x10FC	IXGBE_DEV_ID_82599_XAUI_LOM
0x151C	IXGBE_DEV_ID_82599_T3_LOM
0x1528	IXGBE_DEV_ID_X540T
0x1560	IXGBE_DEV_ID_X540T1

NSX Manager 瀏覽器支援

表格 2-5. NSX Manager 瀏覽器支援

瀏覽器	Windows 10	Windows 8.1	Windows 7	Ubuntu 12、14.04	Max OSX 10.9、10.10、10.11
Internet Explorer 11		是	是		
Firefox 50		是	是	是	是
Chrome 54	是	是	是	是	是
Safari 9					是
Microsoft Edge 25	是				

連接埠和通訊協定

下圖說明 **NSX-T** 中所有的節點至節點的通訊路徑、保護及驗證路徑的方式，以及用來建立相互驗證之認證的儲存位置。

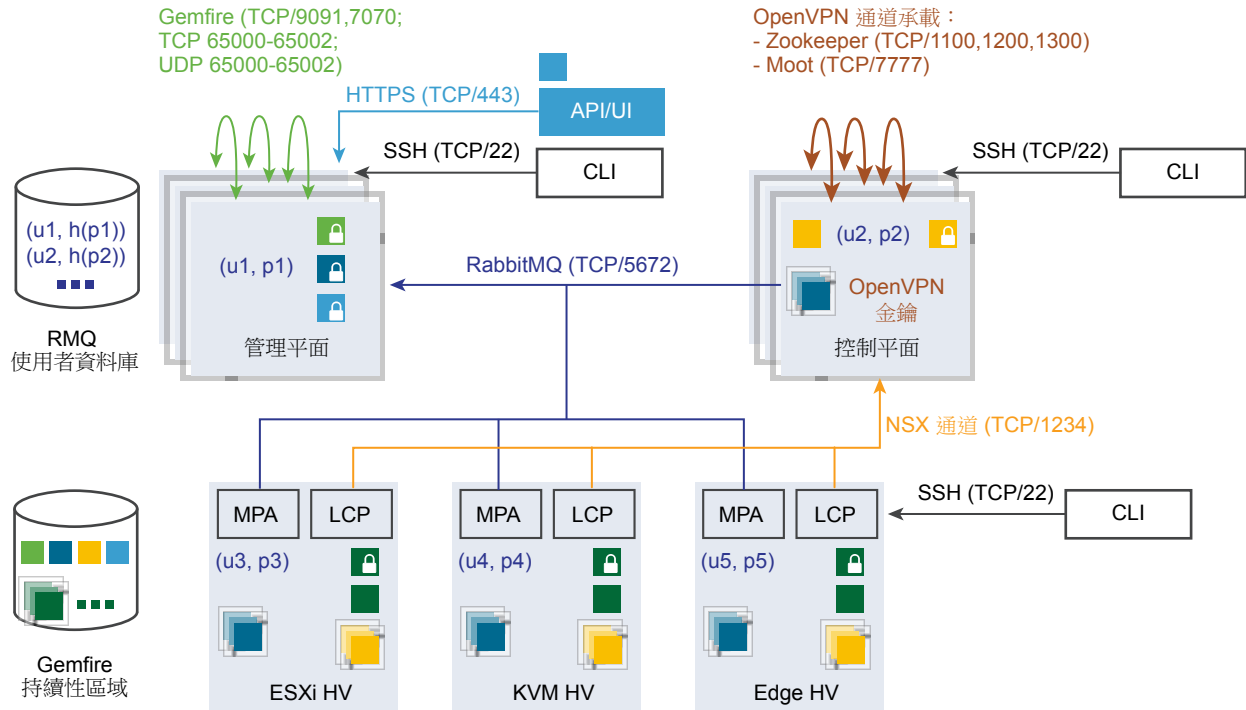
箭頭表示初始通訊的代理程式。依預設，所有憑證皆為自我簽署憑證。北向 **API** 憑證和私密金鑰可被取代。

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。

右上角帶有鎖頭圖示的彩色方形表示私密金鑰。不附鎖頭圖示的方形則為公開金鑰。



- RMQ：每一節點帳戶名稱/共用密碼, TLS
- NSX 通道：每一節點用戶端憑證, TLS
- 叢集：透過 OpenVPN 通道的 zk 和 moot, 共用密碼或憑證驗證
- Gemfire：每一節點用戶端憑證, TLS
- API/UI：工作階段驗證, HTTPS
- CLI：使用者名稱/密碼, SSH

- 🔒 Gemfire 伺服器憑證, 私密金鑰
- 🔒 RMQ 伺服器憑證, 私密金鑰
- 🔒 NSX 通道伺服器憑證, 私密金鑰
- 🔒 API 伺服器憑證, 私密金鑰
- (u2, p2) RMQ 帳戶名稱/共用密碼 (在每一主機/Edge/CCP 中具有唯一性)
- 🔒 NSX 通道用戶端憑證, 私密金鑰

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

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 2-6. 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
任何	Manager	22	TCP	SSH
任何	Manager	123	UDP	NTP
任何	Manager	443	TCP	NSX API 伺服器
任何	Manager	161	UDP	SNMP
任何	Manager	8080	TCP	安裝-升級 HTTP 存放庫
任何	Manager	5671	TCP	NSX 傳訊
Manager	任何	22	TCP	SSH (上傳支援服務包及備份等項目)
Manager	任何	53	TCP	DNS
Manager	任何	53	UDP	DNS
Manager	任何	123	UDP	NTP
Manager	任何	161 和 162	TCP	SNMP
Manager	任何	161 和 162	UDP	SNMP
Manager	任何	514	TCP	Syslog
Manager	任何	514	UDP	Syslog
Manager	任何	6514	TCP	Syslog
Manager	任何	6514	UDP	Syslog
Manager	任何	9000	TCP	Log Insight 代理程式
Manager	任何	33434 - 33523	UDP	Traceroute

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 2-7. 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
任何	控制器	22	TCP	SSH
任何	控制器	53	UDP	DNS
任何	控制器	123	UDP	NTP
任何	控制器	161	UDP	SNMP
任何	控制器	1100	TCP	Zookeeper 仲裁
任何	控制器	1200	TCP	Zookeeper 領導選舉

表格 2-7. 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
任何	控制器	1300	TCP	Zookeeper 伺服器
任何	控制器	1234	TCP	CCP-netcpa 通訊
任何	控制器	7777	TCP	Moot RPC
任何	控制器	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。
任何	控制器	33434 - 33523	UDP	Traceroute
控制器	任何	22	TCP	SSH
控制器	任何	53	UDP	DNS
控制器	任何	53	TCP	DNS
控制器	任何	80	TCP	HTTP
控制器	任何	123	UDP	NTP
控制器	任何	5671	TCP	NSX 傳訊
控制器	任何	7777	TCP	Moot RPC
控制器	任何	9000	TCP	Log Insight 代理程式
控制器	任何	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。
控制器	任何	8080	TCP	NSX 升級
控制器	任何	33434 - 33523	UDP	Traceroute
控制器	任何	514	UDP	Syslog
控制器	任何	514	TCP	Syslog
控制器	任何	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 2-8. 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
任何	Edge	22	TCP	SSH
任何	Edge	123	UDP	NTP
任何	Edge	161	UDP	SNMP
任何	Edge	67 和 68	UDP	DHCP
任何	Edge	1167	TCP	DHCP 後端

表格 2-8. 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
任何	Edge	3784 和 3785	UDP	BFD
任何	Edge	5555	TCP	公有雲
任何	Edge	6666	TCP	公有雲
任何	Edge	8080	TCP	NAPI 和 NSX 升級
任何	Edge	2480	TCP	Nestdb
Edge	任何	22	TCP	SSH
Edge	任何	53	UDP	DNS
Edge	任何	80	TCP	HTTP
Edge	任何	123	UDP	NTP
Edge	任何	161 和 162	UDP	SNMP
Edge	任何	161 和 162	TCP	SNMP
Edge	任何	179	TCP	BGP
Edge	任何	443	TCP	HTTPS
Edge	任何	514	TCP	Syslog
Edge	任何	514	UDP	Syslog
Edge	任何	1167	TCP	DHCP 後端
Edge	任何	1234	TCP	netcpa
Edge	任何	3000 - 9000	TCP	中繼資料 Proxy
Edge	任何	5671	TCP	NSX 傳訊
Edge	任何	6514	TCP	透過 TLS 的 Syslog
Edge	任何	33434 - 33523	UDP	Traceroute

由金鑰管理員所使用的 TCP 連接埠

金鑰管理員使用部分 TCP 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。

表格 2-9. 由金鑰管理員所使用的 TCP 連接埠

來源	目標	連接埠	通訊協定	說明
任何	金鑰管理員	22	TCP	SSH
MP	金鑰管理員	8992	TCP	管理平面對金鑰管理員之通訊
Hypervisor	金鑰管理員	8443	TCP	Hypervisor 對金鑰管理員之通訊
金鑰管理員	任何	22	TCP	SSH

安裝概觀

通常，初始安裝程序的順序如下所示：

- 1 安裝 NSX Manager。
- 2 安裝 NSX Controller。
- 3 將 NSX Controller 加入管理平面。
- 4 初始化控制叢集以建立主要控制器。
即使您的環境中只有一個 NSX Controller，仍須執行此步驟。
- 5 將 NSX Controller 加入控制叢集中。
- 6 在 Hypervisor 主機上安裝 NSX-T 模組。
在安裝 NSX-T 模組時，系統會在 Hypervisor 主機上建立憑證。
- 7 將 Hypervisor 主機加入管理平面。
這會使主機將其主機憑證傳送至管理平面。
- 8 安裝 NSX Edge。
- 9 將 NSX Edge 加入管理平面。
- 10 建立傳輸區域和傳輸節點。

這會使 NSX-T 主機交換器建立於每個主機上。此時，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。

以上是建議的順序，但您不一定要採用此順序。

NSX Manager 可以隨時安裝。

NSX Controller 可以隨時安裝並加入管理平面。

NSX-T 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 (Fabric > Hosts > Add)** UI 或 POST fabric/nodes API 同時執行這兩個程序。

NSX Controller、NSX Edge 和具有 NSX-T 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、邏輯路由器和網元。當 NSX Controller、NSX Edge 和主機加入管理平面時，NSX-T 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 管理指南。

使用 KVM

NSX-T 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。

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

如果您打算將 KVM 用作傳輸節點，或作為 NSX Manager 和 NSX Controller 客體虛擬機器的主機，但您尚未設定 KVM，則可以使用此處說明的程序。

程序

- 1 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</pre>
RHEL	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>

- 2 檢查硬體虛擬化功能。

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

輸出應包含 vmx。

3 確定已安裝 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>

4 (適用於 KVM 用作 NSX Manager 或 NSX Controller 的主機) 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> 檔案：</p> <pre>auto lo iface lo inet loopback auto eth0 iface eth0 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-br0</code> 檔案：</p> <pre>DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge"</pre>

5 (適用於 KVM 用作傳輸節點) 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。

設定比前一個步驟多一個的介面。

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> 檔案：</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> 檔案：</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。

KVM 主機設定為傳輸節點後，系統將會自動建立橋接器介面「`nsx-vtep0.0`」。在 Ubuntu 中，`/etc/network/interfaces` 將會包含下列項目：

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

在 RHEL 中，`nsxa` 將建立名為 `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
```

- 6 若要讓網路變生效，請重新啟動網路，或將 Linux 伺服器重新開機。
- 7 準備用於核心傾印的主機。

Linux 發行版	準備核心傾印
RHEL	<p>執行下列命令：</p> <pre>mkdir /var/cores chmod 1777 /var/cores echo "kernel.core_pattern = /var/cores/core.%e.%t.%p" >> /etc/sysctl.conf sysctl -p</pre> <p>在 <code>/etc/security/limits.conf</code> 中新增以下幾行：</p> <pre>* soft core unlimited * hard core unlimited root soft core unlimited root hard core unlimited</pre>

在 KVM CLI 中管理您的客體虛擬機器

NSX Manager 和 NSX Controller 可以安裝為 KVM 虛擬機器。此外，KVM 可以用作 NSX 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 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 的管理元件。

vSphere ESXi 或 KVM 支援 NSX Manager。您僅能安裝一個 NSX Manager 執行個體。您可以使用 vSphere 的高可用性 (HA) 功能來確保 NSX Manager 的可用性。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，以便在原始主機出問題時，NSX Manager 應用裝置就能在另一台主機上重新啟動。

NSX Manager 支援下列部署方法：

- OVA/OVF
- QCOW2

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 應用裝置具有下列密碼複雜度需求：

- 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

如果密碼不符合複雜度需求，則安裝仍會成功。如果您並未在部署期間為使用者 **admin** 指定足夠複雜性的密碼，則必須在部署之後以 **admin** 身分登入，並回應變更密碼的提示。如果使用者 **root** 也並未擁有足夠複雜性的密碼，請在以 **admin** 的身分登入期間使用下列命令來變更密碼：

```
set user root password <password>
```

備註 在管理員的全新安裝、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，管理員可能需要數分鐘才會啟動。

必須在設定足夠複雜性的密碼後，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。

安裝 NSX Manager 時，請選擇不含底線的主機名稱。如果您指定包含底線的主機名稱，則在部署之後，應用裝置將會具有類似 **nsx-manager** 的預設主機名稱。

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

本章包含以下主題：

- [使用 vSphere Web Client 在 ESXi 上安裝 NSX Manager](#)
- [使用命令列 OVF Tool 在 ESXi 上安裝 NSX Manager](#)
- [在 KVM 上安裝 NSX Manager](#)

使用 vSphere Web Client 在 ESXi 上安裝 NSX Manager

您可以使用 vSphere Web Client 將 NSX Manager 部署為虛擬應用裝置。

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](#)。

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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

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

程序

- 1 找出 NSX Manager 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 (Deploy OVF template)**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。

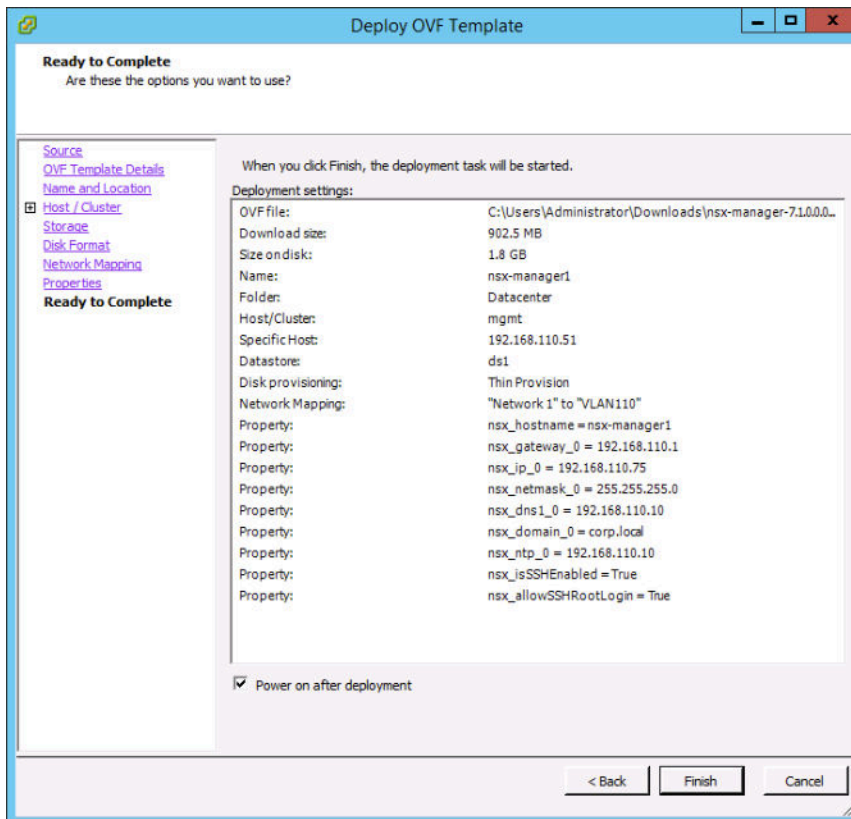
一般而言，您會將 NSX Manager 放置在提供網路管理公用程式的叢集中。

- 6 選取 NSX Manager 的连接埠群組或目的地網路。

例如，如果您使用 vSphere Distributed Switch，您可以將 NSX Manager 放置在名為 Mgmt_VDS - Mgmt 的连接埠群組上。

- 7 設定 NSX Manager 密碼和 IP 設定。

例如，此畫面會在設定所有選項之後顯示最終檢閱畫面。



8 若要獲得最佳效能，請保留 NSX 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 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 元件的主控制台以追蹤開機程序。

在 NSX 元件完全開機後，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
  ...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設網路執行 Ping 偵測。
- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 位址或主機名稱>`。
例如：`https://192.168.110.75`。

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，您可以使用 VMware OVF Tool，這是一種命令列公用程式。

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

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，請進行建立。大多數部署會將 **NSX** 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** 應用裝置到其他網路的靜態路由。準備 **NSX** 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

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

程序

- (適用於獨立主機) 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_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
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- (適用於由 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_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
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- 若要獲得最佳效能，請保留 NSX 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 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 元件的主控制台以追蹤開機程序。

在 NSX 元件完全開機後，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
...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設閘道執行 Ping 偵測。
- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 位址或主機名稱>`。
例如：`https://192.168.110.75`。

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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

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

程序

- 1 下載 NSX Manager QCOW2 映像，然後將其複製到所需的位置。
- 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_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。

如果您要建立多個管理員，請為每個管理員建立個別的 QCOW2 映像複本。在 **guestinfo** 資訊寫入至 QCOW2 映像後，即無法覆寫該資訊。

```
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 若要獲得最佳效能，請保留 NSX 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 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 元件的主控台以追蹤開機程序。

在 NSX 元件完全開機後等待 3 分鐘，然後以管理員的身分登入 CLI。EULA 畫面隨即出現。接受 EULA。然後，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
...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設閘道執行 Ping 偵測。
- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 位址或主機名稱>`。
例如: `https://192.168.110.75`。

備註 您必須使用 HTTPS。不支援 HTTP。

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** 邏輯交換所需的控制平面功能和路由功能。它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-T** 主機交換器或 **Open vSwitch (OVS)**，存在於 **ESX** 和其他 **Hypervisor** 內，例如 **KVM**。

NSX Controller 具有下列支援的部署方法：

- OVA/OVF
- QCOW2

ESX 或 **KVM** 支援 **NSX Controller**。

不支援透過 **PXE** 開機的 **NSX Controller** 安裝。

NSX Controller 必須要有靜態 IP 位址。IP 位址在安裝後即無法變更。

NSX-T 應用裝置具有下列密碼複雜度需求：

- 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

如果密碼不符合複雜度需求，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。

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 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。

安裝 **NSX Manager** 時，請選擇不含底線的主機名稱。否則，主機名稱會設為 **localhost**。

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

本章包含以下主題：

- [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 加入管理平面](#)
- [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](#)

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。

若要支援備份和還原，NSX Controller 應用裝置必須具有靜態管理 IP 位址。不支援使用 DHCP 來指派管理 IP 位址。不支援變更管理 IP 位址。如需備份和還原資訊，請參閱 NSX-T 管理指南。

密碼必須符合密碼強度限制。NSX-T 應用裝置會強制執行下列複雜性規則：

- 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

若要安裝 PXE，您必須提供以 SHA-512 演算法加密的密碼字串來作為根和 Admin 使用者密碼。

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 元件虛擬機器安裝包含 VMware Tools。NSX 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，請進行建立。大多數部署會將 **NSX** 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** 應用裝置到其他網路的靜態路由。準備 **NSX** 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

- 規劃 IPv4 IP 位址配置。在此版本的 **NSX-T** 中，IPv6 不受支援。
- 在 ESXi 主機上部署 OVF 範本的權限。
- 選擇不包含底線的主機名稱。否則，主機名稱會設為 *nsx-manager*。
- 可部署 OVF 範本的管理工具，例如 vCenter Server 或 vSphere Client。

OVF 部署工具必須支援可允許手動設定的組態選項。

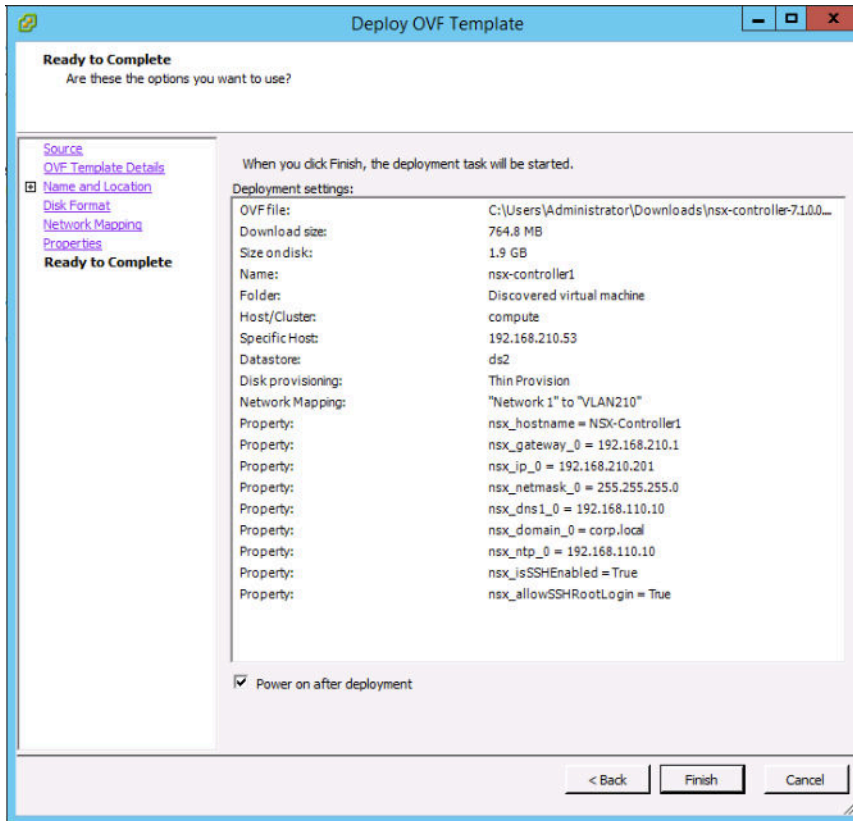
- 必須安裝用戶端整合外掛程式。

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 (Deploy OVF template)**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。
一般而言，您會將 **NSX Controller** 放置在提供網路管理公用程式的叢集中。
- 6 選取 **NSX Controller** 的連接埠群組或目的地網路。
例如，如果您使用 vSphere Distributed Switch，您可以將 **NSX Controller** 放置在名為 **Mgmt_VDS - Mgmt** 的連接埠群組上。

7 設定 NSX Controller 密碼和 IP 設定。

例如，此畫面會在設定所有選項之後顯示最終檢閱畫面。



8 若要獲得最佳效能，請保留 NSX 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 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 元件的主控台以追蹤開機程序。

在 NSX 元件完全開機後，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
...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設閘道執行 Ping 偵測。

- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 加入管理平面](#)。

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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T 中，IPv6 不受支援。
- OVF Tool 4.0 版或更新版本。

程序

- (適用於獨立主機) 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"
--acceptAllEulas
--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_hostname=nsx-controller
<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-controller
Task Completed
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully

```

- (適用於由 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"
--acceptAllEulas
--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_hostname=nsx-controller
<path/url to 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%40vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator%40vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-controller
Task Completed
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- 若要獲得最佳效能，請保留 NSX 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 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 元件的主控制台以追蹤開機程序。

在 NSX 元件完全開機後，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
...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設網道執行 Ping 偵測。
- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 加入管理平面](#)。

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。
- 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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

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

程序

- 1 下載 NSX Controller QCOW2 映像。
- 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_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。

如果您要建立多個控制器，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。

```
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
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-Controller1
Escape character is ^]

nsx-Controller1 login:
```

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

6 若要獲得最佳效能，請保留 NSX 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 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 元件的主控台以追蹤開機程序。

在 NSX 元件完全開機後，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
...
```

請確定 NSX 元件具有必要連線。

- 確定您可以對 NSX 元件執行 Ping 偵測。
- 確定 NSX 元件可以對其預設閘道執行 Ping 偵測。
- 確定 NSX 元件可以針對與 NSX 元件位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX 元件可以對其 DNS 伺服器及其 NTP 伺服器執行 Ping 偵測。
- 如果您啟用了 SSH，請確定您可以使用 SSH 連線至 NSX 元件。

如果未建立連線，請確定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 加入管理平面](#)。

將 NSX Controller 加入管理平面

將 NSX Controller 加入管理平面，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。

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。例如，

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

- 4 在每個 NSX Controller 應用裝置上，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-Controller1> join management-plane NSX-Manager username admin thumbprint <NSX-Manager's-
thumbprint>
Password for API user: <NSX-Manager's-password>
Node successfully registered and controller restarted
```

在每個控制器節點上執行此命令。

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
```

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 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。若您未初始化控制叢集，則控制器將無法與 Hypervisor 主機通訊。

先決條件

- 安裝至少一個 NSX Controller。
- 將 NSX Controller 加入管理平面。
- 選擇共用密碼。共用密碼是使用者定義的共用密碼 (例如「secret123」)。此密碼必須讓叢集中的三個節點共用。

程序

- 1 開啟 NSX Controller 的 SSH 工作階段。

2 執行 `set control-cluster security-model shared-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.
```

執行 `get control-cluster status verbose` 命令，並確定 `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	rpc address	rpc port	global id
557a911f-41fd-4977-9c58-f3ef55b3efe7	192.168.110.34	7777	1

```

10.0.0.1      status      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]
(queueued=0, recved=60324, sent=60324, sid=0x100000f14a10003, lop=PING, est=1459376913497, to=30000, lcxid=0x8, l
zxid=0x10000017a, lresp=604617273, llat=0, minlat=0, avglat=0, maxlat=1088)
/10.0.0.1:35462[0] (queueued=0, recved=1, sent=0)
/10.0.0.1:51724[1]
(queueued=0, recved=45786, sent=45803, sid=0x100000f14a10001, lop=GETC, est=1459376911226, to=40000, lcxid=0x21e
, lzid=0x10000017a, lresp=604620658, llat=0, minlat=0, avglat=0, maxlat=1841)
/10.0.0.1:51725[1]
(queueued=0, recved=60328, sent=60333, sid=0x100000f14a10002, lop=PING, est=1459376913455, to=30000, lcxid=0xc, l

```

```

zxid=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

- 安裝三個 NSX Controller 應用裝置。
- 確定 NSX Controller 節點已加入管理平面。請參閱[將 NSX Controller 加入管理平面](#)。
- 初始化控制叢集以建立控制叢集主節點。
- 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 元件部署至相同的叢集，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控制器上執行 `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`。

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。每個控制器節點也都有一個 UUID。

備註 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控制器上，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

將 Hypervisor 主機新增至 NSX-T 網狀架構。請參閱第 7 章，主機準備。

NSX Edge 安裝

NSX Edge 可提供在 NSX-T 部署以外的路由服務和網路連線。如果您要透過網路位址轉譯 (NAT) 部署第 0 層路由器或第 1 層路由器，則需要 NSX Edge。

NSX Edge 具有下列支援的部署方法：

- OVA/OVF
- 含 PXE 的 ISO
- 不含 PXE 的 ISO

NSX Edge 僅在 ESXi 或裸機上受到支援。KVM 不支援 NSX Edge。

若要安裝 PXE，您必須提供以 SHA-512 演算法加密的密碼字串來作為根和 Admin 使用者密碼。

NSX-T 應用裝置具有下列密碼複雜度需求：

- 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

如果密碼不符合複雜度需求，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。

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。

安裝 NSX Manager 時，請選擇不含底線的主機名稱。如果您指定包含底線的主機名稱，則在部署之後，應用裝置將會具有類似 nsx-manager 的預設主機名稱。

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

本章包含以下主題：

- **NSX Edge 網路設定**
- 使用 GUI 在 ESXi 上安裝 NSX Edge
- 使用命令列 OVF Tool 在 ESXi 上安裝 NSX Edge
- 透過 ISO 檔案與 PXE 伺服器安裝 NSX Edge
- 在裸機上安裝 NSX Edge
- 透過 ISO 檔案將 NSX Edge 安裝為虛擬應用裝置
- 將 NSX Edge 加入管理平面

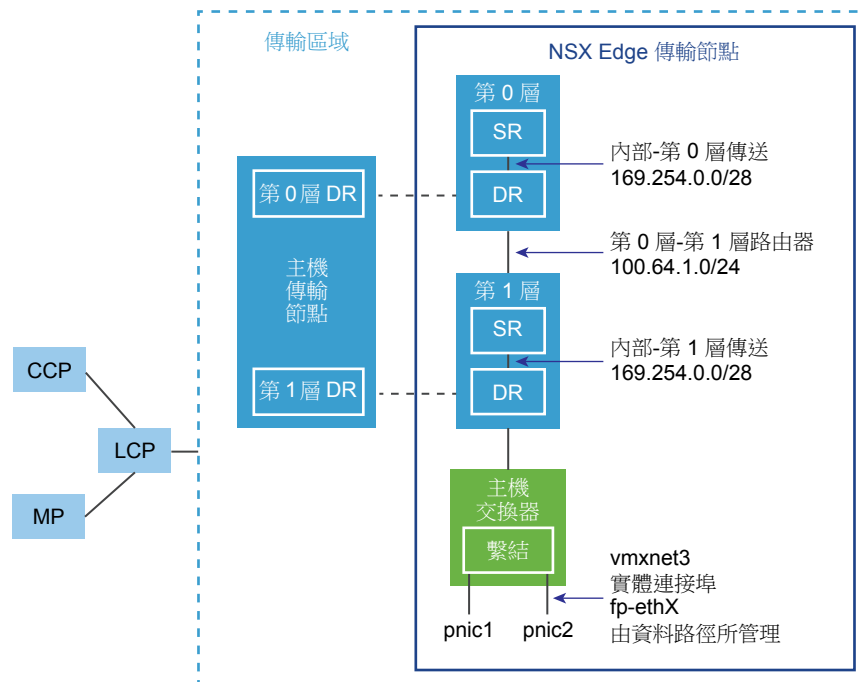
NSX Edge 網路設定

NSX Edge 可透過 ISO、OVA/OVF 或 PXE 開機來安裝。無論採用何種安裝方法，請務必在安裝 NSX Edge 之前備妥主機網路。

傳輸區域內之 NSX Edge 的高階視圖

NSX-T 的高階視圖顯示出一個傳輸區域中的兩個傳輸節點。一個傳輸節點是主機。另一個是 NSX Edge。

圖 6-1: NSX Edge 的高階視圖



當您第一次部署 NSX Edge 時，您可以將其視為空的容器。在您建立邏輯路由器之前，NSX Edge 不會執行任何動作。NSX Edge 可提供第 0 層和第 1 層邏輯路由器的運算支援。每個邏輯路由器都包含一個服務路由器 (SR) 和一個分散式路由器 (DR)。當我們提到某路由器是分散式時，表示它已複製至屬於相同傳輸區域的所有傳輸節點上。在此圖中，主機傳輸節點所包含的 DR 與第 0 層和第 1 層路由器上所包含的相同。如果邏輯路由器將設定成執行 NAT 等的服務，則需要服務路由器。所有的第 0 層邏輯路由器皆具有服務路由器。如果根據您的設計考量而有所需要，則第 1 層路由器也可以具有服務路由器。

依預設，SR 與 DR 之間的連結會使用 169.254.0.0/28 子網路。這些路由器內部轉換連結會在您部署第 0 層或第 1 層邏輯路由器時自動建立。除非 169.254.0.0/28 子網路已用於您的部署中，否則您不需設定或修改連結組態。請注意，在第 1 層邏輯路由器上，僅在您在建立第 1 層邏輯路由器期間選取 NSX Edge 叢集時 SR 才會出現。

針對第 0 層至第 1 層的連線指派的預設位址空間為 100.64.0.0/10。系統會為每個第 0 層至第 1 層的對等連線，提供一個在 100.64.0.0/10 位址空間內的 /31 子網路。此連結會在您建立第 1 層路由器，並將其連線至第 0 層路由器時自動建立。除非 100.64.0.0/10 子網路已用於您的部署中，否則您不需設定或修改此連結上的介面。

每個 NSX-T 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 網狀架構節點。當網狀架構節點後續新增為傳輸節點時，系統將會建立主機或 NSX Edge 的 LCP 連線。

最後，上圖顯示兩個互相繫結以提供高可用性之實體 NIC (pnic1 和 pnic2) 的範例。這些實體 NIC 將由資料路徑進行管理。它們可作為外部網路的 VLAN 上行，或作為受內部 NSX-T 管理之虛擬機器網路的通道端點連結。

最佳做法是為每個 NSX Edge 至少配置兩個實體連結。您可以選擇性地使用不同的 VLAN 識別碼，讓相同實體 NIC 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 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。

您可以執行 `get interfaces` 和 `get physical-ports` 命令，以在 NSX Edge CLI 中檢視實體連結資訊。在 API 中，您可以使用 `GET fabric/nodes/<edge-node-id>/network/interfaces` API 呼叫。實體連結將在下一節中詳細討論。

無論是將 NSX Edge 安裝為虛擬機器應用裝置或安裝在裸機上，視部署而定有多個網路組態選項可供使用。

傳輸區域和主機交換器

若要瞭解 NSX Edge 網路，您必須了解某些關於傳輸區域和主機交換器的知識。傳輸區域可控制 NSX-T 中第 2 層網路的連線。主機交換器是建立在傳輸節點上的軟體交換器。主機交換器的用途是將邏輯路由器上行和下行繫結至實體 NIC。針對 NSX Edge 所屬的每個傳輸區域，皆有單一主機交換器安裝在 NSX Edge 上。

傳輸區域有兩種類型：

- 覆疊適用於傳輸節點之間的內部 NSX-T 通道 - NSX Edge 僅能屬於一個覆疊傳輸區域。

- VLAN 適用於 NSX-T 外部的上行 - 一個 NSX Edge 可以屬於多少個 VLAN 傳輸區域並沒有限制。

一個 NSX Edge 可以屬於零個或許多 VLAN 傳輸區域。如果屬於零個 VLAN 傳輸區域，則 NSX Edge 仍可以具有上行，因為 NSX Edge 上行可使用針對覆疊傳輸區域安裝的相同主機交換器。如果您要讓每個 NSX Edge 皆僅具有一個主機交換器，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。

請注意，如果您需要將相同的 VLAN 識別碼用於傳輸網路中的覆疊流量和其他 VLAN 流量 (例如，用於 VLAN 上行)，您必須在兩個不同的主機交換器上進行這些設定，一個用於 VLAN，而另一個用於覆疊。

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

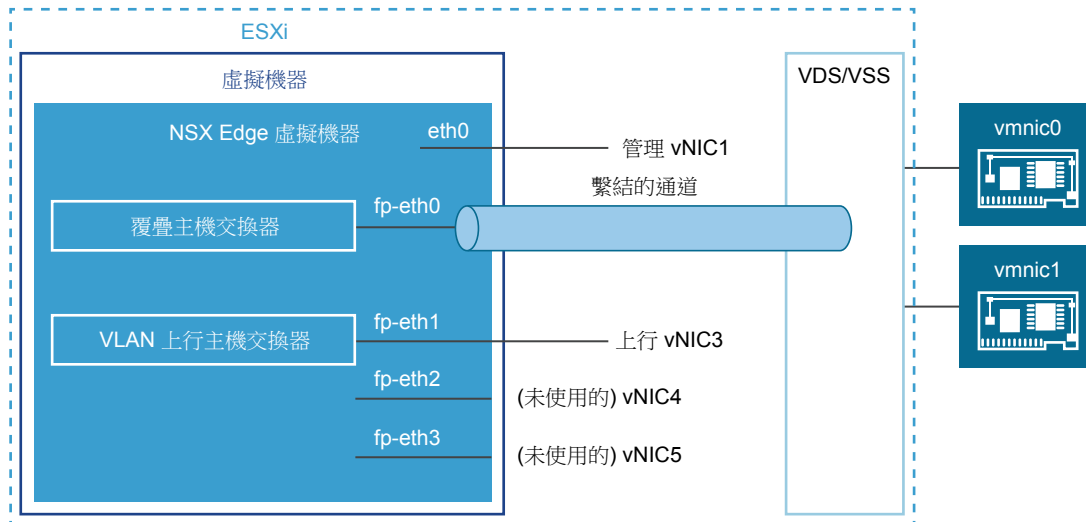
當您將 NSX Edge 安裝為虛擬應用裝置或虛擬機器時，系統將會建立名為 **fp-ethX** 的內部介面，其中 **X** 為 0、1、2 和 3。這些介面會配置給 Top-of-Rack (ToR) 交換器的上行使用，以及供 NSX-T 覆疊通道使用。

當您建立 NSX Edge 傳輸節點時，您可以選取 **fp-ethX** 介面，將上行與覆疊通道建立關聯。您可以選擇 **fp-ethX** 介面的使用方式。

在 vSphere Distributed Switch 或 vSphere 標準交換器上，您至少應該為 NSX Edge 配置兩個 vmnic：一個用於 NSX Edge 管理，而另一個用於上行和通道。

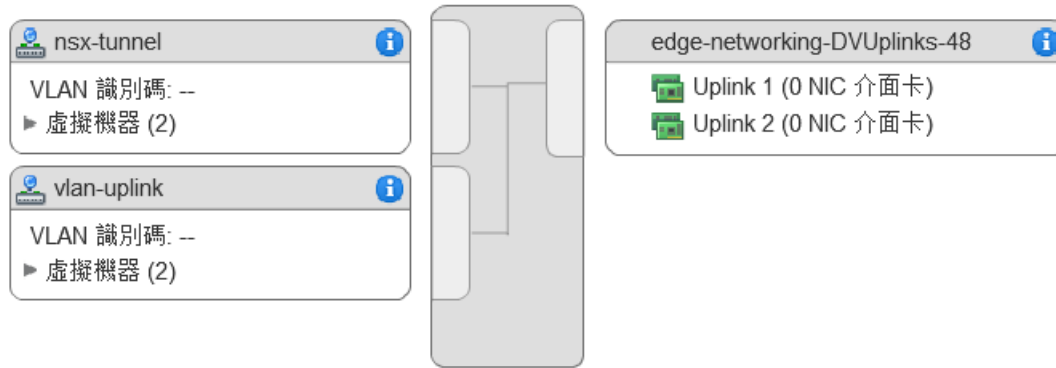
在下列範例實體拓撲中，**fp-eth0** 會用於 NSX-T 覆疊通道。**fp-eth1** 會用於 VLAN 上行。而 **fp-eth2** 和 **fp-eth3** 則不使用。

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)，因此會有兩個主機交換器，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`。這僅為範例。您可以讓您的虛擬機器連接埠群組使用任何名稱。

為 NSX Edge 設定的通道和上行虛擬機器連接埠群組不需要與 VMkernel 連接埠或給定的 IP 位址建立關聯。這是因為這些群組僅用於第 2 層上。如果您的部署會使用 DHCP 將位址提供給管理介面，請確定僅有一個 NIC 指派給管理網路。

請注意，VLAN 和通道連接埠群組會設定為主幹連接埠。這是必要的。例如，在標準 vSwitch 上，您會以下列方式設定主幹連接埠：**主機 > 組態 > 網路 > 新增網路 > 虛擬機器 > 所有 VLAN 識別碼 (4095) (Host > Configuration > Networking > Add Networking > Virtual Machine > VLAN ID All (4095))**。

如果您使用應用裝置型或虛擬機器 NSX Edge，則可以使用標準 vSwitch 或 vSphere Distributed Switch。

您可以將 NSX Edge 和主機傳輸節點部署在相同的 Hypervisor 上。

您可以選擇性地在單一主機上安裝多個 NSX Edge 應用裝置/虛擬機器，而所有已安裝的 NSX Edge 將可使用相同的管理、VLAN 和通道端點連接埠群組。

隨著基礎實體連結已啟用，且虛擬機器連接埠群組已設定的情況中，您可以安裝 NSX Edge。

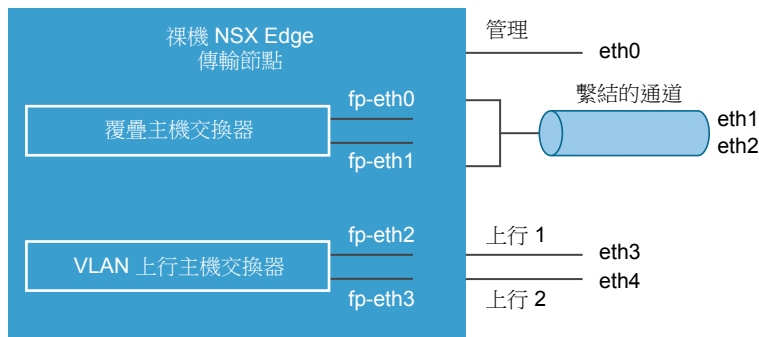
裸機 NSX Edge 網路

裸機 NSX Edge 包含名為 `fp-ethX` 的內部介面，其中 X 為 0、1、2、3，依此類推。建立的 `fp-ethX` 介面數量取決於您裸機 NSX Edge 所擁有的實體 NIC 數量。這些介面可全部或部分配置給 Top-of-Rack (ToR) 交換器的上行使用，以及供 NSX-T 覆疊通道使用。

當您建立 NSX Edge 傳輸節點時，您可以選取 `fp-ethX` 介面，將上行與覆疊通道建立關聯。

您可以選擇 **fp-ethX** 介面的使用方式。在下列範例實體拓撲中，**fp-eth0** 會與 **fp-eth1** 繫結，並且用於 NSX-T 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



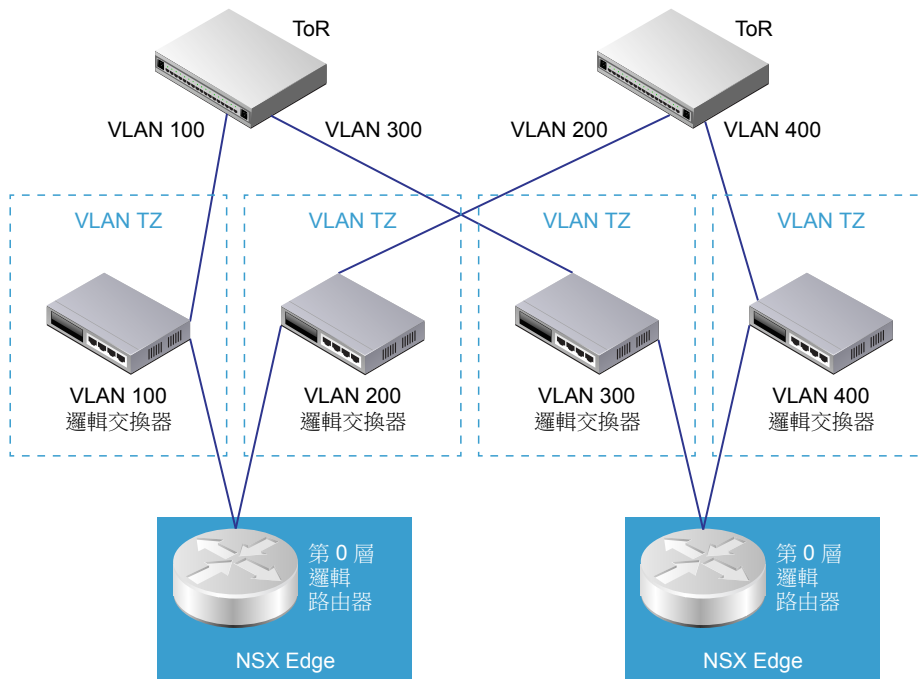
NSX Edge 上行備援

NSX Edge 上行備援可讓兩個 VLAN 相同成本多重路徑 (ECMP) 上行用於 NSX Edge 至外部 TOR 的網路連線。

當您有兩個 ECMP VLAN 上行時，您也應該要有兩個 TOR 交換器，以維持高可用性和完整的網狀連線。每個 VLAN 邏輯交換器各有一個相關聯的 VLAN 識別碼。

當您將 NSX Edge 新增至 VLAN 傳輸區域時，系統將會安裝新的主機交換器。例如，如果您將一個 NSX Edge 節點新增至四個 VLAN 傳輸區域 (如圖所示)，則系統會在 NSX Edge 上安裝四個主機交換器。

圖 6-4：一項適用於 NSX Edge 至 TOR 的建議 ECMP VLAN 設定



使用 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 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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T 中，IPv6 不受支援。
- 在 ESXi 主機上部署 OVF 範本的權限。
- 選擇不包含底線的主機名稱。否則，主機名稱會設為 *localhost*。
- 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。
- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。

程序

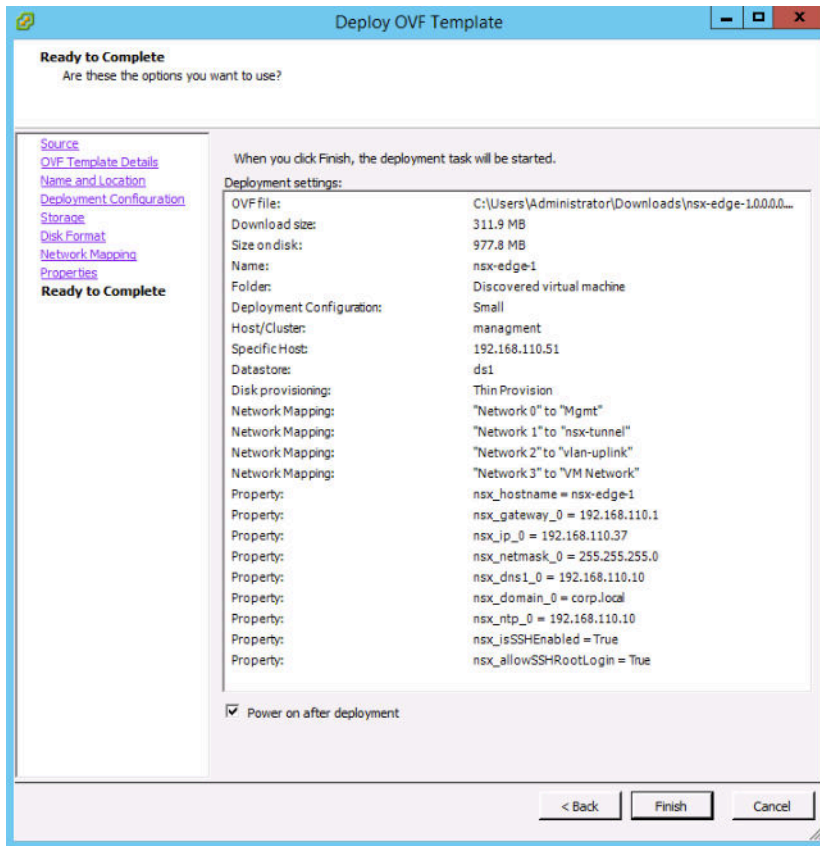
- 1 找出 NSX Edge OVA 或 OVF 檔案。
複製下載 URL，或將 OVA 檔案下載到您的電腦上。
- 2 在管理工具中啟動**部署 OVF 範本 (Deploy OVF template)**精靈，然後導覽或連結至 .ova 檔案。
- 3 輸入 NSX Edge 的名稱，然後選取資料夾或資料中心。
您輸入的名稱會顯示在詳細目錄中。
您所選取的資料夾會用來將權限套用至 NSX Edge。
- 4 選取組態大小：小型、中型或大型。
系統需求會隨著組態大小而有所不同。請參閱 NSX-T 版本說明。
- 5 選取用來儲存 NSX Edge 虛擬應用裝置檔案的資料存放區。
- 6 如果您要安裝在 vCenter 中，請選取要部署 NSX Edge 應用裝置的主機或叢集。
一般而言，您會將 NSX Edge 放置在提供網路管理公用程式的叢集中。

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 設定 NSX Edge 密碼和 IP 設定。

例如，此畫面會在設定所有選項之後顯示最終檢閱畫面。



9 若要獲得最佳效能，請保留 NSX 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 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。如果視窗並未開啟，請確定已允許快顯視窗。

在 NSX Edge 完全開機後，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-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。

請確定 NSX Edge 應用裝置具有必要連線。

- 確定您可以對 NSX Edge 執行 Ping 偵測。
- 確定 NSX Edge 可以對其預設閘道執行 Ping 偵測。
- 確定 NSX Edge 可以針對與 NSX Edge 位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX Edge 可以對其 DNS 伺服器及其 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 登入 NSX Edge。

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，您可以修正此錯誤，方式如下：

- 1 `stop service dataplane`
- 2 `set interface eth0 dhcp plane mgmt`
- 3 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 4 `start service dataplane`

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 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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T 中，IPv6 不受支援。
- 請參閱 [NSX Edge 網路設定](#) 中的 NSX Edge 網路需求。
- 在 ESXi 主機上部署 OVF 範本的權限。
- 選擇不包含底線的主機名稱。否則，主機名稱會設為 *localhost*。
- OVF Tool 4.0 版或更新版本。

程序

- (適用於獨立主機) 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://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
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
```



```

- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully

```

- (適用於由 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
Warning:
- No manifest entry found for: 'nsx-<component>.ovf'.
- File is missing from the manifest: 'nsx-<component>.ovf'.
- ExtraConfig options exists in source.
- Skipping monitor as the --X:waitForIp option is not given.
Completed successfully

```

- 若要獲得最佳效能，請保留 NSX 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 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。如果視窗並未開啟，請確定已允許快顯視窗。

在 NSX Edge 完全開機後，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-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。

請確定 NSX Edge 應用裝置具有必要連線。

- 確定您可以對 NSX Edge 執行 Ping 偵測。
- 確定 NSX Edge 可以對其預設閘道執行 Ping 偵測。
- 確定 NSX Edge 可以針對與 NSX Edge 位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX Edge 可以對其 DNS 伺服器及其 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 登入 NSX Edge。

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，您可以修正此錯誤，方式如下：

- 1 `stop service dataplane`
- 2 `set interface eth0 dhcp plane mgmt`
- 3 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 4 `start service dataplane`

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。請注意，NSX Manager 和 NSX Controller 不支援 PXE 開機安裝。此作業包括自動設定網路設定，例如 IP 位址、閘道、網路遮罩、NTP 和 DNS。

此程序將示範如何在 Ubuntu 上設定 PXE 伺服器。PXE 由兩個元件組成：DHCP 和 TFTP。

DHCP 會以動態方式將 IP 設定散佈至 NSX-T 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 元件 ISO 檔案和安裝設定。

在 PXE 伺服器就緒後，程序會說明如何以預先植入的組態檔來安裝 NSX Edge。

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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

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

程序

- 1 (可選) 建立 kickstart 檔案。

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

kickstart 檔案必須命名為

```
nsxcli.install
```

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

在 kickstart 檔案中，您可以新增所需的 CLI 命令。

例如：

若要設定管理介面的 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 <password>
```

請注意，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 所將存在的相同子網路中。

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

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

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

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

3 安裝 DHCP 伺服器軟體。

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

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

```
INTERFACES="eth1"
```

- 5 (選用) 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` 中，定義 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 確定 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 確定 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 檔案複製或下載至所需的位置。

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

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

- 16 (選用) 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
```

若要修改根密碼，請編輯 `/var/www/html/nsx-edge/preseed.cfg`，並搜尋以下一行：

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

取代雜湊字串。您不需要逸出任何特殊字元，如 `$`、`'`、`"` 或 `\` 等。

您也可以將 `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，您可以新增以下兩行：

```
usermod --password '$6$VS3exId0aKmwW$U3g0V7BF0DXlMRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '$6$VS3exId0aKmwW$U3g0V7BF0DXlMRI.LR0v/VgloxVotEDp00b02hUF8u/' admin; \
```

雜湊字串僅為範例。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 6tgml...` 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。

請務必將 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=trusty --
```

- 18 將以下幾行新增至 `/etc/dhcp/dhcpd.conf` 檔案。

請務必將 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。

- 20 使用裸機安裝指示或 ISO 安裝指示來完成安裝。

- 在裸機上安裝 [NSX Edge](#)
- 透過 ISO 檔案將 [NSX Edge](#) 安裝為虛擬應用裝置

- 21 開啟虛擬機器電源。

- 22 在開機功能表上, 選取 **nsxedge**。

此時會自動設定網路、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**。

- 23 若要獲得最佳效能, 請保留 **NSX** 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** 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** 的主控台以追蹤開機程序。如果視窗並未開啟, 請確定已允許快顯視窗。

在 NSX Edge 完全開機後，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-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。

請確定 NSX Edge 應用裝置具有必要連線。

- 確定您可以對 NSX Edge 執行 Ping 偵測。
- 確定 NSX Edge 可以對其預設閘道執行 Ping 偵測。
- 確定 NSX Edge 可以針對與 NSX Edge 位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX Edge 可以對其 DNS 伺服器及其 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 登入 NSX Edge。

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，您可以修正此錯誤，方式如下：

- 1 `stop service dataplane`
- 2 `set interface eth0 dhcp plane mgmt`
- 3 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 4 `start service dataplane`

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

後續步驟

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

在裸機上安裝 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。此安裝方法通常用於無法存取 PXE 伺服器的概念驗證 (POC) 實驗室中。

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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。
- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T 中，IPv6 不受支援。
- 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 從該磁碟將主機開機。
- 3 選擇**自動安裝 (Automated installation)**。

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 若要獲得最佳效能，請保留 NSX 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 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。如果視窗並未開啟，請確定已允許快顯視窗。

在 NSX Edge 完全開機後，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-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。

請確定 NSX Edge 應用裝置具有必要連線。

- 確定您可以對 NSX Edge 執行 Ping 偵測。
- 確定 NSX Edge 可以對其預設網道執行 Ping 偵測。
- 確定 NSX Edge 可以針對與 NSX Edge 位於相同網路的 Hypervisor 主機執行 Ping 偵測。

- 確定 NSX Edge 可以對其 DNS 伺服器及其 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 登入 NSX Edge。

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，您可以修正此錯誤，方式如下：

- 1 `stop service dataplane`
- 2 `set interface eth0 dhcp plane mgmt`
- 3 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 4 `start service dataplane`

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 裝置。此安裝方法通常用於無法存取 PXE 伺服器的概念驗證 (POC) 實驗室中。

重要 NSX 元件虛擬機器安裝包含 VMware Tools。NSX 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，請進行建立。大多數部署會將 NSX 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 應用裝置到其他網路的靜態路由。準備 NSX 應用裝置要在其上進行通訊的管理虛擬機器連接埠群組。

- 規劃 IPv4 IP 位址配置。在此版本的 NSX-T 中，IPv6 不受支援。
- 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 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 (Connect at power on)**。

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 video	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 (Automated installation)**。

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 若要獲得最佳效能，請保留 NSX 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 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。如果視窗並未開啟，請確定已允許快顯視窗。

在 NSX Edge 完全開機後，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-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。

請確定 NSX Edge 應用裝置具有必要連線。

- 確定您可以對 NSX Edge 執行 Ping 偵測。
- 確定 NSX Edge 可以對其預設閘道執行 Ping 偵測。
- 確定 NSX Edge 可以針對與 NSX Edge 位於相同網路的 Hypervisor 主機執行 Ping 偵測。
- 確定 NSX Edge 可以對其 DNS 伺服器及其 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 登入 NSX Edge。

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，您可以修正此錯誤，方式如下：

- 1 `stop service dataplane`
- 2 `set interface eth0 dhcp plane mgmt`
- 3 將 eth0 放入 DHCP 網路並等候系統將 IP 位址指派給 eth0。
- 4 `start service dataplane`

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。

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 > Edge \(Fabric > Edges\)](#)頁面上。MPA 連線應為「已啟用」。如果 MPA 連線非為「已啟用」，請嘗試重新整理瀏覽器畫面。

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 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 模組，並且向 NSX-T 管理平面進行登錄。

本章包含以下主題：

- 在 KVM 主機上安裝第三方套件
- 將 Hypervisor 主機新增到 NSX-T 網狀架構
- NSX-T 核心模組的手動安裝
- 將 Hypervisor 主機加入管理平面

在 KVM 主機上安裝第三方套件

若要準備讓 KVM 主機成為網狀架構節點，您必須安裝某些第三方套件。

程序

- 針對 Ubuntu 14.04，請執行下列命令：

```
apt-get install libunwind8 libgflags2 libgoogle-perftools4 traceroute
apt-get install python-mako python-simplejson python-support python-unittest2 python-yaml python-netaddr
apt-get install libprotobuf8
apt-get install libboost-filesystem1.54.0 libboost-chrono1.54.0
apt-get install dkms
```

- 針對 Ubuntu 16.04，請執行下列命令：

```
apt-get install libunwind8 libgflags2v5 libgoogle-perftools4 traceroute
apt-get install python-mako python-simplejson python-unittest2 python-yaml python-netaddr
apt-get install libprotobuf9v5
apt-get install libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5
apt-get install dkms
```

- 針對 RHEL 7.2，請執行下列命令：

```
yum groupinstall "Virtualization Hypervisor"
yum groupinstall "Virtualization Client"
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
yum install boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind yum-utils wget net-tools redhat-lsb-core tcpdump wget
```

將 Hypervisor 主機新增到 NSX-T 網狀架構

網狀架構節點是已向 NSX-T 管理平面登錄並已安裝 NSX-T 模組的節點。若要讓 Hypervisor 主機成為 NSX-T 覆疊的一部分，必須先將其新增至 NSX-T 網狀架構。

備註 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。

先決條件

- 對於每個您打算新增至 NSX-T 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
 - (KVM) SHA-256 SSL 指紋
 - (ESXi) SHA-256 SSL 指紋
- (選用) 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。
 - 其中一個自行收集資訊的方法是在 Linux Shell 中執行下列命令：

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

- 另一個方法是使用 ESXi CLI：

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
```

- 若要從 KVM Hypervisor 擷取 SHA-256 指紋，請執行下列命令：

```
# ssh-keyscan -t rsa hostname > hostname.pub
# awk '{print $3}' hostname.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
```

where *hostname* is the hypervisor's hostname or IP address.

- 對於 **Ubuntu**，請確認您已安裝必要的第三方套件。請參閱在 [KVM 主機上安裝第三方套件](#)。

程序

- 1 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
```

- 2 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 3 選取**網狀架構 (Fabric) > 節點 (Nodes) > 主機 (Hosts)**，然後按一下**新增 (Add)**。

- 4 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 x</div>
作業系統 *	ESXi ▼
使用者名稱 *	root
密碼 *	●●●●●●
SHA-256 指紋	

取消

新增

如果您未輸入主機指紋，NSX-T UI 會提示您使用從主機擷取來的預設指紋。

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 網狀架構時，NSX Manager 的**網狀架構 > 節點 > 主機 (Fabric > Nodes > Hosts)** UI 會顯示**部署狀態: 安裝成功 (Deployment Status: Installation Successful)**和**MPA 連線: 已開啟 (MPA Connectivity: Up)**。在您讓網狀架構節點進入傳輸節點之前，**LCP 連線 (LCP Connectivity)**會維持無法使用的狀態。

由於將主機新增至 NSX-T 網狀架構，因此主機上會安裝一組 NSX-T 模組。在 ESXi 上，這些模組會封裝為 VIB。若為 RHEL 上的 KVM，這些模組會封裝為 RPM。若為 Ubuntu 上的 KVM，這些模組會封裝為 DEB。

若要在 ESXi 上進行確認，您可以執行 `esxcli software vib list | grep nsx` 命令，而日期則是執行安裝的當日。

若要在 RHEL 上進行確認，請執行 `yum list installed` 或 `rpm -qa` 命令。

若要在 Ubuntu 上進行確認，請執行 `dpkg --get-selections` 命令。

您可以使用 GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` API 呼叫來檢視網狀架構節點：

```
{
  "resource_type" : "HostNode",
  "id" : "f36d5a79-233c-47c9-9c17-9adc9f8ec466",
  "display_name" : "10.143.1.177",
  "fqdn" : "w1-mvpccloud-177.eng.vmware.com",
  "ip_addresses" : [ "10.143.1.177" ],
  "external_id" : "f36d5a79-233c-47c9-9c17-9adc9f8ec466",
  "discovered_ip_addresses" : [ "192.168.150.104", "10.143.1.177" ],
  "os_type" : "ESXI",
  "os_version" : "6.5.0",
  "managed_by_server" : "",
  "_create_time" : 1480369243245,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1480369243245,
  "_create_user" : "admin",
  "_revision" : 0
}
```

您可以使用 GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` API 呼叫在 API 中監控狀態。

```
{
  "lcp_connectivity_status" : "UP",
  "mpa_connectivity_status" : "UP",
  "last_sync_time" : 1480370899198,
  "mpa_connectivity_status_details" : "Client is responding to heartbeats",
  "lcp_connectivity_status_details" : [ {
    "control_node_ip" : "10.143.1.47",
    "status" : "UP"
  } ],
  "inventory_sync_paused" : false,
  "last_heartbeat_timestamp" : 1480369333415,
  "system_status" : {
```

```

"mem_used" : 2577732,
"system_time" : 1480370897000,
"file_systems" : [ {
  "file_system" : "root",
  "total" : 32768,
  "used" : 5440,
  "type" : "ramdisk",
  "mount" : "/"
}, {
  "file_system" : "etc",
  "total" : 28672,
  "used" : 264,
  "type" : "ramdisk",
  "mount" : "/etc"
}, {
  "file_system" : "opt",
  "total" : 32768,
  "used" : 20,
  "type" : "ramdisk",
  "mount" : "/opt"
}, {
  "file_system" : "var",
  "total" : 49152,
  "used" : 2812,
  "type" : "ramdisk",
  "mount" : "/var"
}, {
  "file_system" : "tmp",
  "total" : 262144,
  "used" : 21728,
  "type" : "ramdisk",
  "mount" : "/tmp"
}, {
  "file_system" : "iofilters",
  "total" : 32768,
  "used" : 0,
  "type" : "ramdisk",
  "mount" : "/var/run/iofilters"
}, {
  "file_system" : "hostdstats",
  "total" : 116736,
  "used" : 2024,
  "type" : "ramdisk",
  "mount" : "/var/lib/vmware/hostd/stats"
} ],
"load_average" : [ 0.03999999910593033, 0.03999999910593033, 0.050000000074505806 ],
"swap_total" : 0,
"mem_cache" : 0,
"cpu_cores" : 2,
"source" : "cached",
"mem_total" : 8386740,
"swap_used" : 0,
"uptime" : 3983605000

```

```
},
"software_version" : "1.1.0.0.0.4649755",
"host_node_deployment_status" : "INSTALL_SUCCESSFUL"
}
```

後續步驟

如果您有大量 Hypervisor (例如 500 個以上), NSX Manager 可能會遭遇高 CPU 使用率和效能方面的問題。若要避免發生問題, 您可以執行位於 NSX 檔案存放區的指令碼 `aggsvc_change_intervals.py`。(您可以使用 NSX CLI 命令 `copy file` 或 API POST `/api/v1/node/file-store/<file-name>?action=copy_to_remote_file` 將指令碼複製到主機)。此指令碼會變更某些處理程序的輪詢間隔。如下所示執行指令碼:

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -i 900
```

若要將輪詢間隔變更回為其預設值:

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

建立傳輸區域。請參閱[關於傳輸區域](#)。

NSX-T 核心模組的手動安裝

除了使用 NSX-T 網狀架構 > 節點 > 主機 > 新增 (Fabric > Nodes > Hosts > Add) 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 核心模組。

在 ESXi Hypervisor 上手動安裝 NSX-T 核心模組

若要準備讓主機參與 NSX-T, 您必須在 ESXi 主機上安裝 NSX-T 核心模組。這可讓您建置 NSX-T 控制平面和管理平面網狀架構。封裝在 VIB 檔案中的 NSX-T 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 VIB, 並使其成為主機映像的一部分。請注意, 每個 NSX-T 版本的下載路徑可能會變更。請務必查看 NSX-T 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 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 彙總服務的主機端程式庫。NSX-T 彙總服務是一種在管理平面節點中執行，且從 NSX-T 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 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 升級以及在 Hypervisor 上解除安裝及監控 NSX-T 模組等作業的通道。
- **nsxa** - 執行主機層級組態，例如主機交換器建立和上行組態。
- **nsxcli** - 在 Hypervisor 主機上提供 NSX-T 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 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 核心模組

若要準備讓主機加入 NSX-T，您必須在 Ubuntu KVM 主機上安裝 NSX-T 核心模組。這可讓您建置 NSX-T 控制平面和管理平面網狀架構。封裝在 DEB 檔案中的 NSX-T 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 DEB，並使其成為主機映像的一部分。請注意，每個 NSX-T 版本的下載路徑可能會變更。請務必查看 NSX-T 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
```

若要進行確認，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` 命令會嘗試解析相依性，並重新執行 NSX-T 安裝。

後續步驟

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

在 RHEL KVM Hypervisor 上手動安裝 NSX-T 核心模組

若要準備讓主機加入 NSX-T，您必須在 RHEL KVM 主機上安裝 NSX-T 核心模組。這可讓您建置 NSX-T 控制平面和管理平面網狀架構。封裝在 RPM 檔案中的 NSX-T 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 RPM，並使其成為主機映像的一部分。請注意，每個 NSX-T 版本的下載路徑可能會變更。請務必查看 NSX-T 下載頁面以取得適當的 RPM。

先決條件

- 存取 RHEL 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 -xvf nsx-lcp-<release>-rhel71_x86_64.tar.gz
```

- 4 導覽至套件目錄。

```
cd nsx-lcp-rhel71_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 相依性，並假設 RHEL 機器可連線至 RHEL 存放庫。

- 6 重新載入 OVS 核心模組。

```
/etc/init.d/openvswitch force-reload-kmod
```

若要進行確認，您可以執行 `rpm -qa | grep nsx` 命令。

```
user@host:~$ rpm -qa | grep nsx

nsxa-<release>.el7.x86_64.rpm
nsx-agent-<release>.el7.x86_64.rpm
nsx-aggservice-<release>.el7.x86_64.rpm
nsx-cli-<release>.x86_64.rpm
nsx-da-<release>.el7.x86_64.rpm
nsx-host-<release>.x86_64.rpm
nsx-host_node_status_reporter-<release>.el7.x86_64.rpm
nsx-lldp-<release>.el7.x86_64.rpm
nsx-logical_exporter-<release>.el7.x86_64.rpm
nsx-mpa-<release>.el7.x86_64.rpm
nsx-netcpa-<release>.el7.x86_64.rpm
nsx-sfhc-<release>.el7.x86_64.rpm
nsx-transport_node_status-<release>.el7.x86_64.rpm
```

後續步驟

將主機新增至 NSX-T 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 模組的安裝。

程序

- 1 開啟 NSX Manager 應用裝置的 SSH 工作階段。
- 2 開啟 Hypervisor 主機的 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 而言具有唯一性的數字字串。

例如：

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

- 4 在 Hypervisor 主機上執行 `/opt/vmware/nsx-cli/bin/scripts/nsxcli` 命令以進入 NSX-T 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。

5 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 (Fabric > Node > Hosts)**的 NSX Manager UI 中，確認主機的 MPA 連線為已啟用 (**Up**)。

您可以透過 **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，且管理平面會將控制平面資訊推送至主機。

您應可在每個 ESXi 主機上的 **/etc/vmware/nsx/controller-info.xml** 中查看 NSX Controller 位址。

```
[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 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 中的重要概念。

本章包含以下主題：

- 關於傳輸區域
- 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 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 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 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。

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 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。

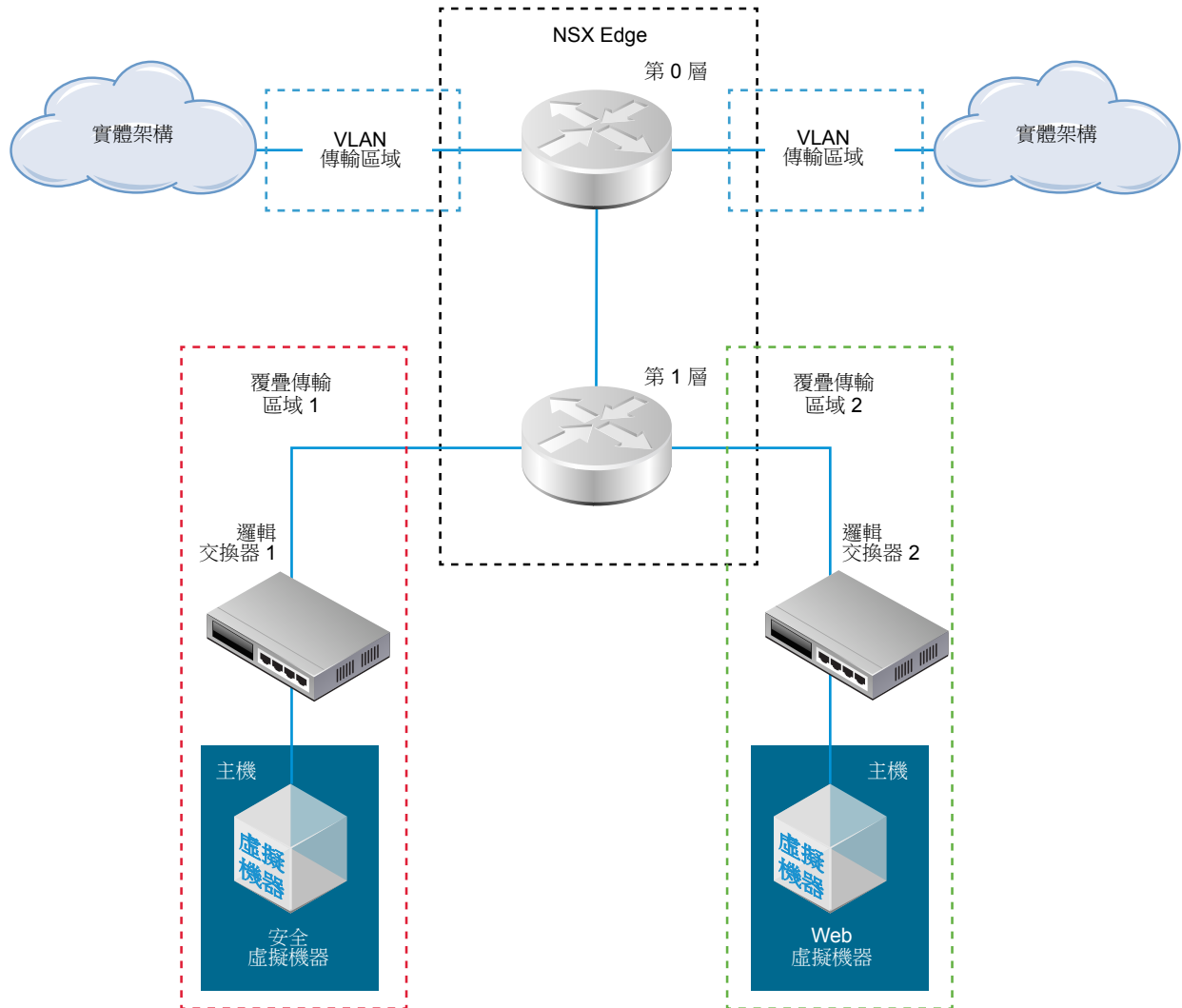
傳輸節點可以是 Hypervisor 主機或 NSX Edge。NSX Edge 可以屬於多個傳輸區域。Hypervisor 主機 (和 NSX-T 邏輯交換器) 則只能屬於一個傳輸區域。

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 邏輯交換器。高安全性虛擬機器會連結至位於 **secure-tz** 的 NSX-T 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。

NSX Edge 傳輸節點可以屬於多個傳輸區域：一個覆疊傳輸區域和多個 VLAN 傳輸區域。VLAN 傳輸區域是用於通往外部環境的 VLAN 上行。

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 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 傳輸區域



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，用來唯一識別開始和終止 NSX-T 框架封裝的 Hypervisor 主機。您可以對通道端點 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，其中一個設計選項會是對 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，使用專用的預設開道新增 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。

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

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

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

程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://<nsx-mgr>>。
- 2 選取**詳細目錄 > IP 集區 (Inventory > IP Pools)**，然後按一下**新增 (Add)**。
- 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

上行設定檔就是主機交換器設定檔，意思是它會針對從 Hypervisor 主機到 NSX-T 邏輯交換器，或從 NSX Edge 節點到 Top-of-Rack 交換器的連結定義原則。

上行設定檔所定義的設定可能會包含整併原則、作用中/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 傳輸節點時套用。

如果 NSX Edge 安裝在裸機上，您可以使用預設的上行設定檔。預設上行設定檔需要一個作用中上行和一個被動待命上行。待命上行不受虛擬機器/應用裝置型 NSX Edge 所支援。當您將 NSX Edge 安裝為虛擬應用裝置時，您必須建立自訂上行設定檔而非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 話雖如此，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主機交換器，且各自使用不同的 VLAN。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

請確定您已瞭解 NSX Edge 網路。請參閱[NSX Edge 網路設定](#)。

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，假設 Hypervisor 主機具有兩個已開啟的實體連結：vmnic0 和 vmnic1。假設 vmnic0 目前正用於管理和儲存網路，而 vmnic1 目前並未使用。這表示 vmnic1 可以用作 NSX-T 上行，但 vmnic0 不行。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。因此，舉例來說，vmnic0/eth0/em0 可用於管理網路，而 vmnic1/eth1/em1 可用於 fp-ethX 連結。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://<nsx-mgr>>。

2 選取**網狀架構 > 設定檔 > 上行設定檔 (Fabric > Profiles > Uplink Profiles)**，然後按一下**新增 (Add)**。

3 輸入下列資訊：

- 上行設定檔名稱
- (選用) 說明
- 整併原則：容錯移轉順序或負載平衡來源 (預設值為容錯移轉順序)
 - 容錯移轉順序 - 從作用中介面卡清單中，一律使用通過容錯移轉偵測準則且排在最前面的上行。此選項不會執行實際的負載平衡。
 - 負載平衡來源 - 根據來源乙太網路 MAC 位址的雜湊來選取上行。
- (選用) 對傳輸網路使用 Link Aggregation Control Protocol (LACP) 的連結彙總群組 (LAG)
- 以逗號分隔的作用中上行名稱清單
- (選用) 以逗號分隔的待命上行名稱清單

您在此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。

- (選用) 傳輸 VLAN
- MTU (預設值為 1600)

例如：

New Uplink Profile [X]

Name: *

Description:

Teaming Policy: *

LAGs

+ INSERT ROW [] COLUMNS ▾

Name *	LACP Mode	LACP Load Balancing *	Uplinks	LACP Time Out

Active Uplinks: *

Standby Uplinks:

Transport VLAN:

MTU: *

您可以使用 `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": [],
        "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"
      },
      "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 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 不允許連線到不同傳輸區域中的虛擬機器。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，NSX-T 主機交換器即會安裝在主机或 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 主機交換器即會安裝在 NSX Edge 上。

主機交換器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主機交換器提供名稱。主機交換器名稱可以是任何所需的名稱。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**網狀架構 > 傳輸區域 (Fabric > Transport Zones)**，然後按一下**新增 (Add)**。
- 3 輸入傳輸區域名稱、主機交換器名稱和流量類型 (覆疊或 VLAN)。

例如：

TRANSPORT ZONES			
<div> + ADD EDIT DELETE ACTIONS COLUMNS </div>			
<input type="checkbox"/>	Transport Zone ↑	ID	Host Switch Name
<input type="checkbox"/>	tz-overlay	efd7...a9ec	overlay-hostswitch
<input type="checkbox"/>	tz-vlan	9b66...b416	vlan-uplink-hostswitch

您可以使用 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

傳輸節點是能夠參與 NSX-T 覆疊或 NSX-T VLAN 網路的節點。

若為 KVM 主機，您可以預先設定主機交換器，或者您可以讓 NSX Manager 執行組態設定。若為 ESXi 主機，則 NSX Manager 一律會設定主機交換器。

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主機，且**網狀架構 > 主機 (Fabric > Hosts)**頁面上的 [MPA 連線] 必須為 [已開啟]。
- 您必須設定傳輸區域。
- 您必須設定上行設定檔 (也稱為主機交換器設定檔)，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 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**網狀架構 > 節點 > 傳輸節點 (Fabric > Nodes > Transport Nodes)**，然後按一下**新增 (Add)**。
- 3 輸入傳輸節點的名稱。
- 4 從下拉式功能表中選取節點。
- 5 (可選) 從下拉式功能表中選取傳輸區域。
- 6 (可選) 若為 KVM 節點，請選取主機交換器類型。

選項	說明
標準	NSX Manager 會建立主機交換器。預設為選取此選項。
已預先設定	主機交換器已設定完成。

若為非 KVM 節點，則主機交換器類型一律為**標準 (Standard)**。

- 7 若為標準主機交換器，請輸入或選取下列主機交換器資訊：
 - 主機交換器名稱。此名稱必須和此節點所屬之傳輸區域的主機交換器名稱相同。

- 上行設定檔。
- IP 指派。您可以選取**使用 DHCP (Use DHCP)**、**使用 IP 集區 (Use IP Pool)**或**使用靜態 IP 清單 (Use Static IP List)**。如果您選取**使用靜態 IP 清單 (Use Static IP List)**，您必須指定由 IP 位址、網道和子網路遮罩構成、並以逗號分隔的清單。
- 實體 NIC 資訊

重要 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，傳輸節點狀態將會是**部分成功 (partial success)**，且網狀架構節點 LCP 連線將無法建立。

Add Transport Node

Name: *

comp-02b

Node: *

comp-02b - 192.168.210.54

Transport Zones:

tz-overlay

Host Switch Type: *

☒ Standard
 ☐ Preconfigured

New Node Switch

Host Switch Name: *

overlay-hostswitch

Uplink Profile: *

uplinkProfile1

IP Assignment: *

Use IP Pool

IP Pool: *

ip-pool-1

OR Create and Use a new IP Pool

Physical NICs:

vmnic1

uplink-1

Save

Cancel

8 若為預先設定的主機交換器，請輸入下列主機交換器資訊：

- 主機交換器外部識別碼。此識別碼必須和此節點所屬之傳輸區域的主機交換器名稱相同。
- VTEP 名稱。

新增主機作為傳輸節點後，主機與 NSX Controller 的連線即會從「CLOSE_WAIT」狀態變更為「已建立」狀態。使用 `esxcli network ip connection list | grep 1234` 命令即可查看此狀態。

```
# esxcli network ip connection list | grep 1234
tcp    0    0  192.168.210.53:20514  192.168.110.34:1234  已建立 (ESTABLISHED)  1000144459  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  已建立 (ESTABLISHED) -
```

您可以使用 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
}

```

當傳輸節點建立成功時，**網狀架構 > 節點 > 主機 (Fabric > Nodes > Hosts)** 上的 **LCP 連線 (LCP Connectivity)** 會變更為 **已開啟 (Up)**。若要查看變更，請重新整理瀏覽器畫面。

後續步驟

建立 NSX Edge 傳輸節點。請參閱[建立 NSX Edge 傳輸節點](#)。

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 NSX-T 主機交換器。

程序

- 1 使用 `esxcli network ip interface list` 命令，在 ESXi 上檢視 NSX-T 主機交換器。

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
...

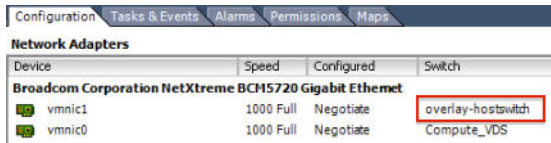
vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network 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 (Configuration > Network Adapters)，在 UI 中檢視已安裝的主機交換器。



用來確認 NSX-T 主機交換器安裝的 KVM 命令為 `ovs-vsctl show`。請注意，KVM 上的主機交換器名稱為 `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"
```

2 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 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
  ...
```


3 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"
}
```

建立 NSX Edge 傳輸節點

傳輸節點是能夠參與 NSX-T 覆疊或 NSX-T VLAN 網路的節點。只要是包含主機交換器的節點皆可以作為傳輸節點。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 (Fabric > Edges)** 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。
- 您必須設定上行設定檔 (主機交換器設定檔)，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 DHCP。

- 主機或 NSX Edge 節點上必須至少有一個未使用的實體 NIC。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**網狀架構 > 節點 > 傳輸節點 (Fabric > Nodes > Transport Nodes)**，然後按一下**新增 (Add)**。
- 3 輸入下列資訊：IP 位址、主機交換器名稱、上行設定檔、IP 集區 (或選取 DHCP) 和實體 NIC 資訊。
 - 輸入 NSX Edge 傳輸節點的名稱
 - 從下拉式清單中選取 NSX Edge 網狀架構節點。
 - 選取傳輸區域。一般而言，NSX Edge 傳輸節點會屬於至少兩個傳輸區域：1) NSX-T 連線的覆疊，和 2) 上行連線的 VLAN。
 - 輸入主機交換器的名稱。Edge 交換器名稱 (有時稱為主機交換器名稱)。Edge 交換器名稱必須符合您在建立傳輸區域時所設定的名稱。
 - 選取上行設定檔。
 - 選取覆疊主機交換器的 IP 集區。若為 VLAN 主機交換器，請將 [IP 集區] 欄位保持空白。覆疊主機交換器僅供用於上行 VLAN 流量，因此不需要覆疊通道端點 IP 位址。
 - 選取虛擬 NIC 和上行。請注意，不同於主機傳輸節點會使用 `vmnicX` 作為實體 NIC，NSX Edge 傳輸節點會使用 `fp-ethX`。

- 選取上行。可用的上行取決於所選上行設定檔中的組態。

例如：

Add Transport Node

Name: *
node-nsx-edge-1

Node: *
nsx-edge-1 - 192.168.110.38

Transport Zones:
tz-overlay
tz-vlan

overlay-hostswitch

Edge Switch Name: *
overlay-hostswitch

Uplink Profile: *
comp-uplink

IP Pool:
comp-tep

Virtual NICs:
fp-eth0
uplink-1

New Node Switch

Edge Switch Name: *
vlan-hostswitch

Uplink Profile: *
vlan-uplink

IP Pool:
Select IP Pool

Virtual NICs:
fp-eth1
uplink-2

Add New Node Switch

Save
Cancel

4 按一下儲存 (Save)以結束。

您可以使用 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
}

```

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

```

{
  "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
  }
},
"pnix_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"
}

```

傳輸節點建立成功時，**網狀架構 > 節點 > Edge (Fabric > Nodes > Edges)** 上的 **LCP 連線 (LCP Connectivity)** 會變更為 **已開啟 (Up)**。您可能需要重新載入瀏覽器畫面才能看到這項變更。

後續步驟

將 NSX Edge 節點新增至 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 建立第 0 層邏輯路由器或第 1 層路由器，您必須將它與 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 (Fabric > Profiles > Edge Cluster Profiles)**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 NSX Manager UI 中，導覽至**網狀架構 > 節點 > Edge 叢集 (Fabric > Nodes > Edge Clusters)**。

2 為 NSX Edge 叢集輸入名稱。

3 選取 NSX Edge 叢集設定檔。

4 按一下**編輯 (Edit)**，然後選取**實體 (Physical)**或**虛擬 (Virtual)**。

「實體」是指在裸機上安裝的 NSX Edge。「虛擬」則是指安裝作為虛擬機器/應用裝置的 NSX Edge。

5 從**可用 (Available)**資料行選取 NSX Edge，然後按一下向右箭頭，將它們移至**已選取 (Selected)**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 管理指南。

解除安裝 NSX-T

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

本章包含以下主題：

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

取消設定 NSX-T 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 在您的虛擬機器管理工具中，從任何邏輯交換器中斷連結所有虛擬機器。
- 2 在 NSX Manager UI 或 API 中，刪除所有的邏輯路由器。
- 3 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。
- 4 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。
- 5 視需要設定新的 NSX-T 覆疊。

從 NSX-T 中移除主機或完整解除安裝 NSX-T

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

下列程序說明如何執行 NSX-T 的完整解除安裝。

程序

- 1 在您的虛擬機器管理工具中，從任何 NSX-T 邏輯交換器中斷連結主機上的所有虛擬機器。
- 2 在 NSX Manager 中，使用網狀架構 > 節點 > 傳輸節點 (Fabric > Nodes > Transport Nodes) UI 或 DELETE /api/v1/transport-node/<node-id> API 來刪除主機傳輸節點。

刪除此傳輸節點會導致 NSX-T 主機交換器從主機上移除。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
```

- 3 在 NSX Manager CLI 中，啟用並啟動 NSX-T 安裝-升級服務。

```
nsx-manager-1> set service install-upgrade enable
nsx-manager-1> start service install-upgrade
```

- 4 從管理平面解除登錄主機，並移除 NSX-T 模組。

移除所有 NSX-T 模組可能需要花費 10 分鐘。

您可以採用數種方法來移除 NSX-T 模組：

- 在 NSX Manager 中，使用**網狀架構 > 節點 > 主機 > 刪除 (Fabric > Nodes > Hosts > Delete)** UI。

在 UI 中，確定已選取**解除安裝 NSX 元件 (Uninstall NSX Components)**。這會使 NSX-T 模組在主機上解除安裝。請注意 在狀態良好的主機上，不應在未選取**解除安裝 NSX 元件 (Uninstall NSX Components)**選項的情況中使用**網狀架構 > 節點 > 主機 > 刪除 (Fabric > Nodes > Hosts > Delete)**。此做法僅供狀態不良的主機作為因應措施。

- 使用 DELETE /api/v1/fabric/nodes/<node-id> API。
- 使用 CLI。

- 1 取得管理員指紋。

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

- 2 在主機的 NSX-T 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 <MANAGER-USERNAME> password <MANAGER-PASSWORD> thumbprint <MANAGER-THUMBPRINT>
```

- 3 在主機上，執行下列命令以移除篩選器。

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

- 4 在主機上，執行下列命令以停止 netcpa。

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

- 5 關閉主機上的虛擬機器電源。

- 6 從主機手動解除安裝 NSX-T 模組。

請注意，目前不支援移除個別模組。您必須在一個命令中移除所有模組。

```
esxcli software vib remove -n nsx-aggsservice -n nsx-da -n nsx-esx-datapath -n nsx-exporter  
-n nsx-host -n nsx-lldp -n nsx-mpa -n nsx-netcpa -n nsx-python-protobuf -n nsx-sfhc -n nsx-  
support-bundle-client -n nsxa -n nsxcli
```

在 RHEL 上，請使用 `sudo yum remove <package-name>` 命令。在 Ubuntu 上，請使用 `apt-get remove <package-name>` 命令。

在這兩個案例中，皆可使用萬用字元來選取 NSX-T 模組。

另外，請移除下列模組：

- 在 Ubuntu 上：tcpdump-ovs、nicira-ovs-hypervisor-node、python-openvswitch、openvswitch-*、libgoogle-glog0、libjson-spirit
- 在 RHEL 上：tcpdump-ovs、openvswitch、kmod-openvswitch、glog、json_spirit

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 覆疊。

如果您要完整移除 NSX-T，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。