

# NSX-T 管理指南

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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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

# 目錄

## 關於管理 VMware NSX-T 6

<b>1</b>	<b>NSX-T 概觀</b>	<b>7</b>
	數據平面	9
	控制平面	9
	管理平面	9
	NSX Manager	10
	NSX Controller	10
	邏輯交換器	11
	邏輯路由器	11
	NSX Edge	12
	傳輸區域	12
	主要概念	13
<b>2</b>	<b>建立邏輯交換器與設定虛擬機器連結</b>	<b>16</b>
	瞭解 BUM 框架複寫模式	17
	建立邏輯交換器	18
	第 2 層橋接	19
	為 NSX Edge 上行建立 VLAN 邏輯交換器	22
	將虛擬機器連線到邏輯交換器	24
	測試第 2 層連線	32
<b>3</b>	<b>設定邏輯交換器和邏輯連接埠的交換設定檔</b>	<b>36</b>
	瞭解 QoS 交換設定檔	37
	瞭解連接埠鏡像交換設定檔	39
	瞭解 IP 探索交換設定檔	41
	瞭解 SpoofGuard	42
	瞭解交換器安全性交換設定檔	45
	瞭解 MAC 管理交換設定檔	46
	建立自訂設定檔與邏輯交換器之間的關聯	46
	建立自訂設定檔與邏輯交換器連接埠之間的關聯	47
<b>4</b>	<b>設定第 1 層邏輯路由器</b>	<b>49</b>
	建立第 1 層邏輯路由器	50
	新增第 1 層邏輯路由器的下行連接埠	50
	在第 1 層邏輯路由器上設定路由通告	51
	設定第 1 層邏輯路由器靜態路由	53

<b>5</b>	<b>設定第 0 層邏輯路由器</b>	<b>56</b>
	建立第 0 層邏輯路由器	57
	連結第 0 層和第 1 層	58
	將第 0 層邏輯路由器連線至 VLAN 邏輯交換器	61
	設定靜態路由	64
	BGP 組態選項	68
	在第 0 層邏輯路由器上設定 BFD	73
	啟用第 0 層邏輯路由器上的路由重新分配	73
	瞭解 ECMP 路由	76
	建立 IP 首碼清單	80
	建立路由對應	81
<b>6</b>	<b>網路位址轉譯</b>	<b>83</b>
	第 1 層 NAT	84
	第 0 層 NAT	90
<b>7</b>	<b>防火牆區段和防火牆規則</b>	<b>93</b>
	新增防火牆規則區段	93
	刪除防火牆規則區段	94
	啟用和停用區段規則	95
	停用和啟用區段記錄	95
	關於防火牆規則	95
	新增防火牆規則	96
	刪除防火牆規則	99
	編輯預設分散式防火牆規則	100
	變更防火牆規則的順序	100
	篩選防火牆規則	101
	在防火牆強制執行中排除物件	101
<b>8</b>	<b>設定群組與服務</b>	<b>103</b>
	建立 IP 集合	103
	建立 IP 集區	104
	建立 MAC 集合	104
	建立 NSGroup	105
	設定服務和服務群組	106
<b>9</b>	<b>DHCP</b>	<b>108</b>
	建立 DHCP 伺服器設定檔	108
	建立 DHCP 伺服器	109
	將 DHCP 伺服器連結至邏輯交換器	110
	從邏輯交換器中斷連結 DHCP 伺服器	110

- 建立 DHCP 轉送設定檔 110
- 建立 DHCP 轉送服務 110
- 將 DHCP 服務新增至邏輯路由器連接埠 111

## 10 設定中繼資料 Proxy 112

- 新增中繼資料 Proxy 伺服器 112
- 將中繼資料 Proxy 伺服器連結至邏輯交換器 113
- 將中繼資料 Proxy 伺服器與邏輯交換器中斷連結 114

## 11 作業和管理 115

- 新增授權金鑰 115
- 管理使用者帳戶 116
- 設定憑證 117
- 設定應用裝置 122
- 管理標籤 122
- 搜尋物件 122
- 尋找遠端伺服器的 SSH 指紋 123
- 備份和還原 NSX Manager 124
- 管理應用裝置和應用裝置叢集 134
- 記錄系統訊息 146
- 設定 IPFIX 149
- 使用 Traceflow 追蹤封包的路徑 150
- 檢視連接埠連線資訊 152
- 監控邏輯交換器連接埠活動 152
- 監控連接埠鏡像工作階段 152
- 監控網狀架構節點 154
- 收集支援服務包 154

# 關於管理 VMware NSX-T

NSX-T 管理指南提供關於為 VMware NSX-T<sup>®</sup> 設定及管理網路的資訊，包括如何建立邏輯交換器和連接埠，以及如何為分層式邏輯路由器設定網路功能。此外也會說明如何設定 NAT、防火牆、SpoofGuard、分組和 DHCP。

## 主要對象

此資訊適用於想要設定 NSX-T 的任何人。這些資訊是針對熟悉虛擬機器技術、網路功能和安全作業的資深 Windows 或 Linux 系統管理員所撰寫的。

## VMware 技術出版品詞彙表

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

# NSX-T 概觀

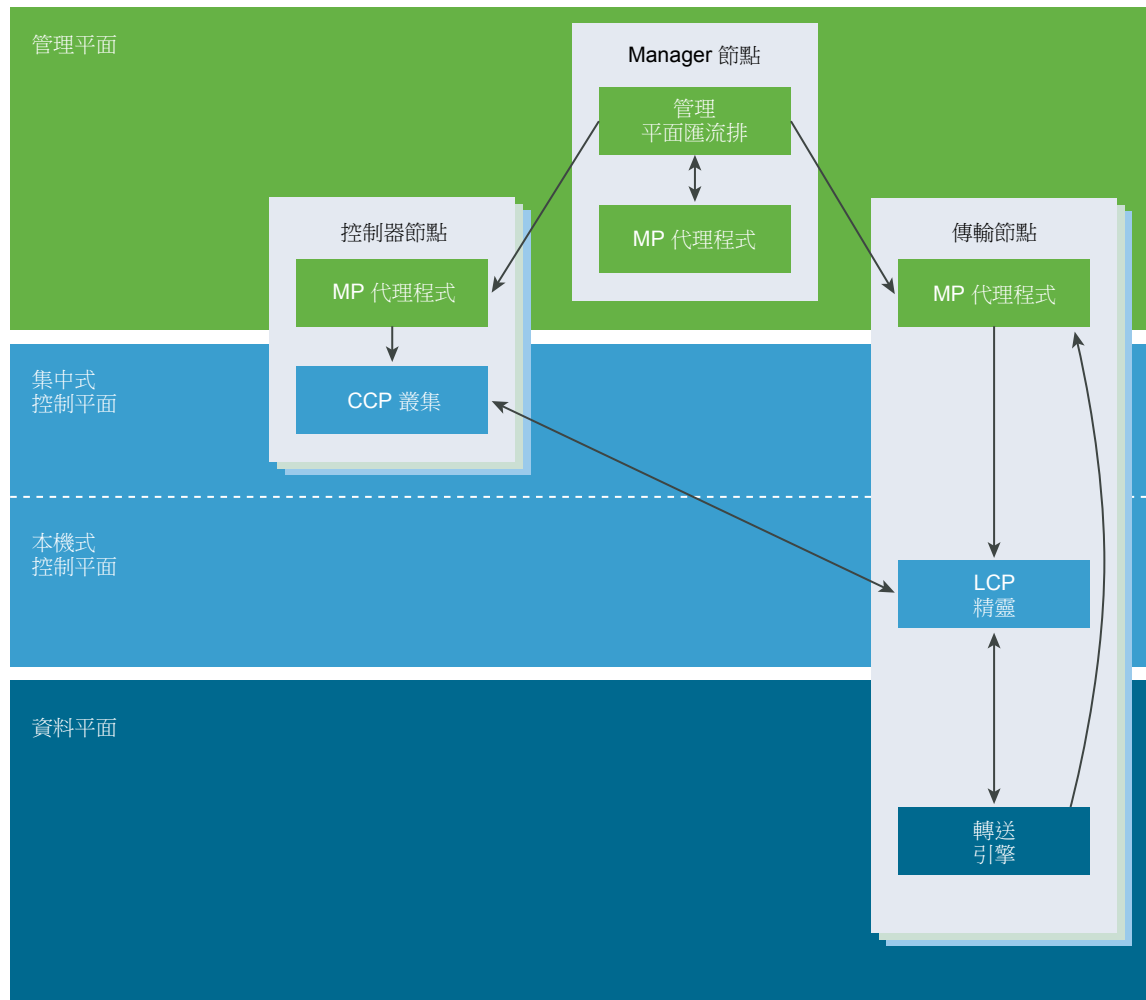
比照伺服器虛擬化透過程式設計的方法來建立、刪除、還原軟體型虛擬機器 (VM) 及建立其快照的方式，**NSX-T** 網路虛擬化會以相似的方式透過程式設計的方法來建立、刪除、還原軟體型虛擬網路及建立其快照。

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 <b>NSX-T</b> 管理的實體網路或 <b>VLAN</b> 。您可以連結您的邏輯網路，或透過 <b>NSX Edge</b> 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 <b>VLAN</b> 。
網狀架構節點	已向 <b>NSX-T</b> 管理平面登錄、並且已安裝 <b>NSX-T</b> 模組的節點。 <b>Hypervisor</b> 主機或 <b>NSX Edge</b> 若要成為 <b>NSX-T</b> 覆疊的一部分，則必須新增至 <b>NSX-T</b> 網狀架構中。
網狀架構設定檔	代表可與 <b>NSX Edge</b> 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	<b>NSX-T</b> 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 <b>API</b> 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 <b>Hypervisor</b> 基礎結構以外、且跨多個 <b>Hypervisor</b> 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 <b>Hypervisor</b> 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 <b>API</b> 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**

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。

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。

**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。

**覆蓋邏輯網路**

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蓋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。

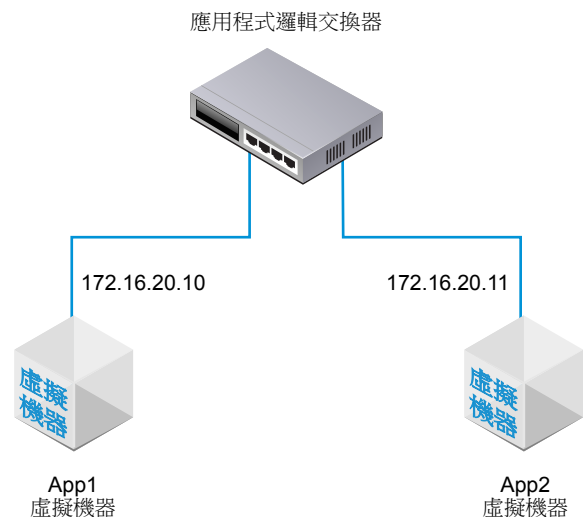
## 建立邏輯交換器與設定虛擬機器連結

NSX-T 邏輯交換器可在從基礎硬體完全分離的虛擬環境中，重現交換功能、廣播、未知單點傳播以及多點傳送 (BUM) 流量。

邏輯交換器類似於 VLAN，兩者皆提供網路連線，可供您連結虛擬機器。虛擬機器接著就能透過 Hypervisor 之間的通道，與連線至相同邏輯交換器的其他虛擬機器進行通訊。每個邏輯交換器皆有虛擬網路識別碼 (VNI)，類似於 VLAN 識別碼。但與 VLAN 不同的是，VNI 可擴充至超出 VLAN 識別碼的限制。

在新增 VLAN 邏輯交換器時，請務必記得對應您所要建置的拓撲。

圖 2-1：邏輯交換器拓撲



例如，此拓撲顯示連線至兩個虛擬機器的單一邏輯交換器。這兩個虛擬機器可位於不同或相同的主機上，也可位於不同或相同的主機叢集中。由於此範例中的虛擬機器位於相同的虛擬網路中，因此虛擬機器上設定的基礎 IP 位址必須位於相同的子網路中。

本章包含以下主題：

- 瞭解 BUM 框架複寫模式
- 建立邏輯交換器
- 第 2 層橋接
- 為 NSX Edge 上行建立 VLAN 邏輯交換器



- 將虛擬機器連線到邏輯交換器
- 測試第 2 層連線

## 瞭解 BUM 框架複寫模式

每個主機傳輸節點皆為一個通道端點。每個通道端點皆有一個 IP 位址。這些 IP 位址可以位在相同的子網路或位在不同的子網路內，取決於您傳輸節點的 IP 集區或 DHCP 的組態而定。

當不同主機上的兩個虛擬機器直接通訊時，單點傳播封裝式流量會在與這兩個 Hypervisor 相關聯的兩個通道端點 IP 位址之間交換，而不需進行洪泛。

不過，如同任何第 2 層網路，有時源自虛擬機器的流量需要進行洪泛，也就是需將流量傳送至屬於相同邏輯交換器的所有其他虛擬機器。第 2 層廣播、未知的單點傳播以及多點傳送流量 (BUM 流量) 皆屬此種情況。請記住單一 NSX-T 邏輯交換器可以跨越多個 Hypervisor。源自指定 Hypervisor 上虛擬機器的 BUM 流量，需要複寫至裝載其他連線至相同的邏輯交換器之虛擬機器的遠端 Hypervisor 上。為了啟用洪泛，NSX-T 支援兩種不同的複寫模式：

- 階層式雙層 (有時稱為 MTEP)
- 源頭 (有時稱為來源)

下列範例說明階層式雙層複寫模式。假設您有一台主機 A，而其中的虛擬機器會連接至虛擬網路識別碼 (VNI) 5000、5001 和 5002。可將 VNI 想成類似於 VLAN，但每個邏輯交換器皆具有與其相關聯的單一 VNI。因此，有時 VNI 和邏輯交換器可互換使用。當我們說一台主機位在 VNI 上，這表示它有虛擬機器連接至包含該 VNI 的邏輯交換器。

通道端點表會顯示主機和 VNI 的連線。主機 A 會檢查 VNI 5000 的通道端點表，並判斷 VNI 5000 上其他主機的通道端點 IP 位址。

其中某些 VNI 連線會與主機 A 的通道端點位於相同的 IP 子網路 (也稱為 IP 區段)。主機 A 會為這些連線建立每個 BUM 框架的個別複本，並將複本直接傳送給每個主機。

其他主機的通道端點則位於不同的子網路或 IP 區段。對於具有一個以上通道端點的區段，主機 A 會指定其中一個端點來作為複寫器。

複寫器會從主機 A 針對 VNI 5000 接收每個 BUM 框架的一個複本。這個複本會在本機的封裝標頭中標記為複寫。主機 A 不會傳送副本給與複寫器位於相同 IP 區段中的其他主機。因此複寫器的責任是在所知範圍內，針對 VNI 5000 上以及與該複寫器主機位於相同 IP 區段的每個主機建立 BUM 框架複本。

VNI 5001 與 5002 將重複上述程序。不同 VNI 的通道端點清單與所產生的複寫器可能會有所不同。

源頭複寫也稱為前端複寫，此模式不具有複寫器。主機 A 僅針對 VNI 5000 上所知的每個通道端點，建立每個 BUM 框架的複本，然後進行傳送。

如果所有主機通道端點皆位於相同子網路上，則選擇任何複寫模式皆無差異，因為行為並無不同。如果主機通道端點位於不同的子網路上，則階層式雙層複寫有助於將負載分散至多台主機。階層式雙層是預設模式。

## 建立邏輯交換器

邏輯交換器會連結至網路中單一或多部虛擬機器。連線至邏輯交換器的虛擬機器可以使用 Hypervisor 之間的通道互相通訊。

### 先決條件

- 確認已設定傳輸區域。請參閱 [NSX-T 安裝指南](#)。
- 確認網狀架構節點已成功連線至 NSX-T 管理平面代理程式 (MPA) 及 NSX-T 本機控制平面 (LCP)。
 

在 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 呼叫中，state 必須是 `success`。請參閱 [NSX-T 安裝指南](#)。
- 確認傳輸節點已新增至傳輸區域。請參閱 [NSX-T 安裝指南](#)。
- 確認 Hypervisor 已新增至 NSX-T 網狀架構，且虛擬機器裝載在這些 Hypervisor 上。
- 自行熟悉邏輯交換器拓撲和 BUM 框架複寫概念。請參閱 [第 2 章，建立邏輯交換器與設定虛擬機器連結與瞭解 BUM 框架複寫模式](#)。
- 確認您的 NSX Controller 叢集處於穩定狀態。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **交換 > 交換器 (Switching > Switches)**。
- 3 按一下 **新增 (Add)**。
- 4 為邏輯交換器指派名稱。

- 5 選取邏輯交換器的傳輸區域。

連結至相同傳輸區域中之邏輯交換器的虛擬機器可互相通訊。

- 6 選取邏輯交換器的複寫模式。

複寫模式 (階層式雙層或源頭) 對於覆疊邏輯交換器為必要，但對於以 VLAN 為基礎的邏輯交換器則為非必要。

複寫模式	說明
階層式雙層	複寫器是主機，即針對相同 VNI 內其他主機的 BUM 流量執行複寫。 每個主機會將每個 VNI 中的一個主機通道端點指定為複寫器。主機會對每個 VNI 執行此動作。
源頭	主機會建立每個 BUM 框架的複本，並將複本傳送至它所知每個 VNI 的每個通道端點。

- 7 (可選) 按一下 **交換設定檔 (Switching Profiles)** 索引標籤並選取交換設定檔。
- 8 按一下 **儲存 (Save)**。

在 NSX Manager UI 中，新的邏輯交換器是可點擊的連結。

## 後續步驟

將虛擬機器連結至您的邏輯交換器。請參閱[將虛擬機器連線到邏輯交換器](#)。

## 第 2 層橋接

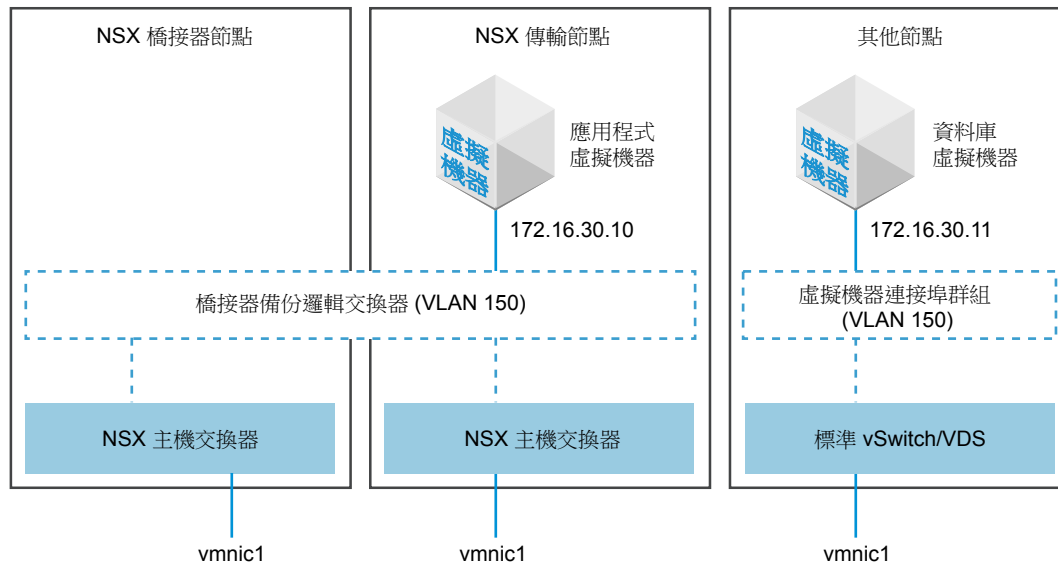
當 NSX-T 邏輯交換器需要對 VLAN 支援的連接埠群組進行第 2 層連線，或是需要連線到位於 NSX-T 部署外部的其他裝置 (例如閘道)，則可以使用 NSX-T 第 2 層橋接器。這對於移轉案例特別有用，因為您需要在實體和虛擬工作負載間分割子網路。

第 2 層橋接涉及的 NSX-T 概念包括橋接器叢集、橋接器端點和橋接器節點。橋接器叢集是橋接器節點的高可用性 (HA) 集合。橋接器節點是進行橋接的傳輸節點。用於橋接虛擬和實體部署的每個邏輯交換器皆有相關的 VLAN 識別碼。橋接器端點會識別橋接器的實體屬性，例如橋接器叢集識別碼和相關的 VLAN 識別碼。

在此版本的 NSX-T 中，由作為橋接器節點的 ESXi 主機提供第 2 層橋接功能。橋接器節點是已新增至橋接器叢集的 ESXi 主機傳輸節點。

在下列範例中，兩個 NSX-T 傳輸節點屬於相同覆疊傳輸區域的一部分。如此可將其 NSX-T 主機交換器 (有時稱為 NSX-T vSwitch，如下圖所示) 連結至相同個橋接器支援的邏輯交換器。

圖 2-2: 橋接器拓撲



左側的傳輸節點屬於橋接器叢集，因此是橋接器節點。

由於邏輯交換器會連結至橋接器叢集，因此稱為橋接器支援的邏輯交換器。為了符合橋接器支援的資格，邏輯交換器必須位於覆疊傳輸區域中，而非 VLAN 傳輸區域中。

中間的傳輸節點不屬於橋接器叢集的一部分。它是一般的傳輸節點，可以是 KVM 或 ESXi 主機。在圖中，此節點上名為「app VM」的虛擬機器會連結至橋接器支援的邏輯交換器。

右側的節點不屬於 NSX-T 覆疊的一部分。它可能是具有虛擬機器的任何 Hypervisor，或是實體網路節點。如果非 NSX-T 節點是 ESXi 主機，則可以使用標準 vSwitch 或 vSphere Distributed Switch 來進行連接埠連結。在此情況中的一項要求是與連接埠連結關聯的 VLAN 識別碼必須符合橋接器所支援邏輯交換器上的 VLAN 識別碼。此外，通訊是在第 2 層上進行，因此兩端裝置必須擁有相同子網路中的 IP 位址。

如前所述，橋接器的目的是啟用兩個虛擬機器之間的第 2 層通訊。當流量在兩個虛擬機器之間傳輸時，流量會周遊橋接器節點。

## 建立橋接器叢集

橋接器叢集是傳輸節點的集合，用來進行橋接並參與高可用性 (HA)。一次僅有一個傳輸節點能產生作用。擁有 NSX-T 橋接器節點的多節點叢集有助於確保永遠至少會有一個 NSX-T 橋接器節點可供使用。若要建立支援橋接器的邏輯交換器，您必須將其與橋接器叢集建立關聯。因此，即使您只有一個橋接器節點，它也必須屬於橋接器叢集才具有實用性。

建立橋接器叢集之後，您稍後可以進行編輯以新增其他橋接器節點。

### 先決條件

- 建立至少一個 NSX-T 傳輸節點以用作橋接器節點。
- 用作橋接器節點的傳輸節點必須為 ESXi 主機。橋接器節點不支援 KVM。
- 建議橋接器節點沒有任何裝載的虛擬機器。
- 傳輸節點僅能新增至一個橋接器叢集。您無法將相同的傳輸節點新增至多個橋接器叢集。

### 程序

- 1 在 NSX Manager UI 中，導覽至**網狀架構 > 組態 > 橋接器 (Fabric > Configuration > Bridges)**。
- 2 為橋接器叢集命名。
- 3 選取橋接器叢集的傳輸區域。  
傳輸區域類型必須為覆疊而非 VLAN。
- 4 從**可用 (Available)**資料行中，選取傳輸節點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

您現在可將邏輯交換器與橋接器叢集建立關聯。

## 建立第 2 層橋接器備份邏輯交換器

當您擁有連線至 NSX-T 覆疊的虛擬機器時，您可能會想讓它們與其他裝置或您 NSX-T 部署外部的虛擬機器之間具備第 2 層連線能力。在此案例中，您可以使用支援橋接器的邏輯交換器。

如需範例拓撲，請參閱圖 2-2。

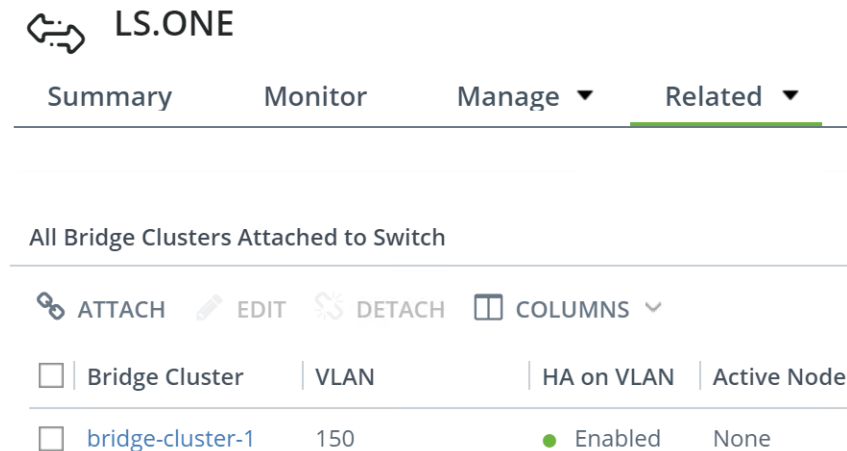
## 先決條件

- 至少一個 ESXi 主機用作橋接器節點。橋接器節點是僅進行橋接的 ESXi 傳輸節點。此傳輸節點必須新增至一個橋接器叢集。請參閱[建立橋接器叢集](#)。
- 至少一個 ESXi 或 KVM 主機用作一般傳輸節點。此節點具有已裝載虛擬機器，且需要與 NSX-T 部署外部的裝置之間具備連線能力。
- NSX-T 部署外部的虛擬機器或其他終端裝置。此終端裝置必須連結至 VLAN 連接埠，且符合支援橋接器之邏輯交換器的 VLAN 識別碼。
- 覆疊傳輸區域中的一個邏輯交換器會用作橋接器備份邏輯交換器。

## 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**交換 > 交換器 (Switching > Switches)**。
- 3 從交換器清單中選取覆疊交換器 (流量類型：覆疊)。
- 4 在交換器組態頁面上，選取**相關 > 橋接器叢集 (Related > Bridge Clusters)**。
- 5 按一下**連結 (ATTACH)**，接著選取橋接器叢集，然後輸入 VLAN 識別碼。

例如：



LS.ONE

Summary Monitor Manage ▼ Related ▼

All Bridge Clusters Attached to Switch

ATTACH EDIT DETACH COLUMNS ▼

Bridge Cluster	VLAN	HA on VLAN	Active Node
bridge-cluster-1	150	● Enabled	None

- 6 如果虛擬機器尚未連線，請將它們連線至邏輯交換器。

虛擬機器必須在與橋接器叢集相同傳輸區域中的傳輸節點上。

您可以測試橋接器的功能，方法為將 Ping 偵測從 NSX-T 內部虛擬機器傳送至 NSX-T 外部的節點。例如，在 [圖 2-2](#) 中，NSX-T 傳輸節點上的應用程式虛擬機器應該可以在外部節點上對資料庫虛擬機器執行 Ping 偵測，以及反向偵測。

您可以監控橋接器交換器上的流量，方法為導覽至**交換 > 交換器 > 監控 (Switching > Switches > Monitor)**。

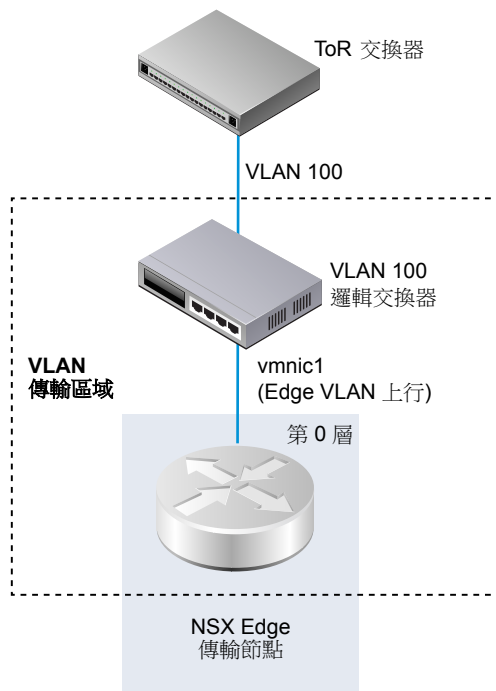
您可以使用 GET <https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics> API 呼叫來檢視橋接器流量：

```
{
  "tx_packets": {
    "total": 134416,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "rx_bytes": {
    "total": 22164,
    "multicast_broadcast": 0
  },
  "tx_bytes": {
    "total": 8610134,
    "multicast_broadcast": 0
  },
  "rx_packets": {
    "total": 230,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "last_update_timestamp": 1454979822860,
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"
}
```

## 為 NSX Edge 上行建立 VLAN 邏輯交換器

Edge 上行會透過 VLAN 邏輯交換器傳送出去。

在建立 VLAN 邏輯交換器時，請務必記得您所要建置的特定拓撲。例如，下列的簡單拓撲顯示 VLAN 傳輸區域內的單一 VLAN 邏輯交換器。VLAN 邏輯交換器具有 VLAN 識別碼 100。這符合連線至 Hypervisor 主機連接埠 (用於 Edge 的 VLAN 上行) 之 TOR 連接埠上的 VLAN 識別碼。



### 先決條件

- 若要建立 VLAN 邏輯交換器，您必須先建立 VLAN 傳輸區域。
- 必須將 NSX-T vSwitch 新增到 NSX Edge。若要在 Edge 上確認，請執行 `get host-switch` 命令。例如：

```
nsx-edge1> get host-switch

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name     : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name     : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- 確認您的 NSX Controller 叢集處於穩定狀態。
- 確認網狀架構節點已成功連線至 NSX-T 管理平面代理程式 (MPA) 與 NSX-T 本機控制平面 (LCP)。

在 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 呼叫中，state 必須是 success。請參閱 NSX-T 安裝指南。

### 程序

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

2 選取**交換 > 交換器 (Switching > Switches)**。

3 按一下**新增 (Add)**。

4 輸入邏輯交換器的名稱。

5 選取邏輯交換器的傳輸區域。

當您選取 VLAN 傳輸區域時，即會顯示 VLAN 識別碼欄位。

6 輸入 VLAN 識別碼。

如果連往實體 TOR 的上行連線沒有 VLAN 識別碼，請在 VLAN 欄位中輸入 0。

7 (可選) 按一下**交換設定檔 (Switching Profiles)**索引標籤並選取交換設定檔。

#### 後續步驟

新增邏輯路由器。

## 將虛擬機器連線到邏輯交換器

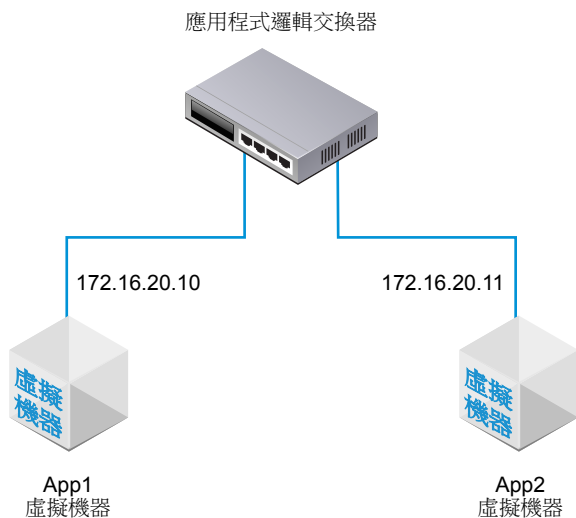
視主機而定，用來將虛擬機器連線到邏輯交換器的組態可能會有所不同。

可以連線至邏輯交換器的受支援主機包含：在 vCenter Server 中受到管理的 ESXi 主機、獨立的 ESXi 主機，以及 KVM 主機。

## 將 vCenter Server 上裝載的虛擬機器連結至 NSX-T 邏輯交換器

如果您有 vCenter Server 中受管理的 ESXi 主機，則可以透過以 Web 為基礎的 vSphere Web Client 來存取主機虛擬機器。在此案例中，您可以使用此程序將虛擬機器連結至 NSX-T 邏輯交換器。

此程序顯示的範例會說明如何將名為 app-vm 的虛擬機器連結至名為 app-switch 的邏輯交換器。



以安裝為基礎的 vSphere Client 應用程式不支援將虛擬機器連結至 NSX-T 邏輯交換器。如果您沒有 (以 Web 為基礎) vSphere Web Client，請參閱[將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T 邏輯交換器](#)。



## 先決條件

- 虛擬機器必須裝載在已新增至 NSX-T 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T 管理平面 (MPA) 和 NSX-T 控制平面 (LCP) 連線。
- 網狀架構節點必須新增至傳輸區域。
- 必須建立邏輯交換器。

## 程序

- 1 在 vSphere Web Client 中，編輯虛擬機器設定，然後將虛擬機器連結至 NSX-T 邏輯交換器。

例如：



- 2 按一下**確定**。

將虛擬機器連結至邏輯交換器後，邏輯交換器連接埠便會新增至邏輯交換器。您可以在**交換 > 連接埠**中的 NSX Manager 上檢視邏輯交換器連接埠。

在 NSX-T API 中，您可以檢視與連結 NSX-T 的虛擬機器與 GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines` API 呼叫

在**交換 > 連接埠**下的 NSX-T Manager UI 中，VIF 連結識別碼符合 API 呼叫中找到的 ExternalID。尋找符合虛擬機器之 externalId 的 VIF 連結識別碼，並確定管理和運作狀態皆為已開啟。

如果兩個虛擬機器連結至相同的邏輯交換器，而 IP 位址也設定在相同的子網路中，則應該可以互相進行 Ping 偵測。

## 後續步驟

新增邏輯路由器。

您可以監控邏輯交換器連接埠上的活動以針對問題進行疑難排解。請參閱[監控邏輯交換器連接埠活動](#)。

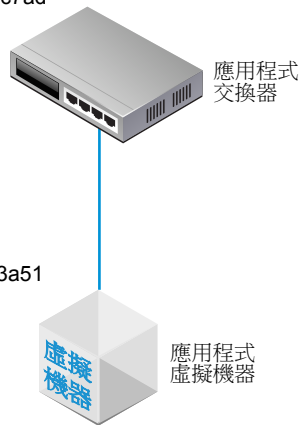
## 將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T 邏輯交換器

如果您擁有的 ESXi 主機是獨立的，則無法透過 Web 型 vSphere Web Client 存取該主機。在此案例中，您可以使用此程序將虛擬機器連結至 NSX-T 邏輯交換器。

此程序顯示的範例會說明如何將名為 app-vm 的虛擬機器連結至名為 app-switch 的邏輯交換器。

交換器的不透明網路識別碼：  
22b22448-38bc-419b-bea8-b51126bec7ad

虛擬機器的外部識別碼：  
50066bae-0f8a-386b-e62e-b0b9c6013a51



#### 先決條件

- 虛擬機器必須裝載在已新增至 NSX-T 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T 管理平面 (MPA) 和 NSX-T 控制平面 (LCP) 連線。
- 網狀架構節點必須新增至傳輸區域。
- 必須建立邏輯交換器。
- 您必須具有 NSX Manager API 的存取權。
- 您必須具有虛擬機器之 VMX 檔案的寫入權限。

## 程序

- 1 使用 (安裝型) vSphere Client 應用程式或某些其他虛擬機器管理工具，編輯虛擬機器並新增 VMXNET 3 以太網路介面卡。

選取任何具名網路。您會在稍後的步驟中變更網路連線。

## 自訂硬體

## 設定虛擬機器硬體

虛擬硬體	虛擬機器選項	SDRS 規則
CPU	1	
記憶體	4096	MB
新增硬碟	40	GB
新增 SCSI 控制器	LSI Logic SAS	
*新增網路	VM Network	
狀態	<input checked="" type="checkbox"/> 開啟電源時連線	
介面卡類型	VMXNET 3	
DirectPath I/O	<input type="checkbox"/> 啟用	
MAC 位址		自動
新增 CD/DVD 光碟機	用戶端裝置	<input type="checkbox"/> 連線...
新增磁碟機	用戶端裝置	<input type="checkbox"/> 連線...

新裝置: 網路 新增

- 2 使用 NSX-T API 發出 GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>` API 呼叫。

在結果中尋找虛擬機器的 `externalId`。

例如：

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735
```

```
{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
  ]
}
```

```

    "biosUuid:4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
  "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
  "local_id_on_host": "5"
}

```

### 3 關閉虛擬機器的電源並從主機解除登錄虛擬機器。

您可以使用虛擬機器管理工具或 ESXi CLI，如此處所示。

```

[user@host:~] vim-cmd /vmsvc/getallvms
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest  vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08


[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5

```

### 4 從 NSX Manager UI 取得邏輯交換器識別碼。

例如：


**app-switch**

Summary
Monitor
Manage ▼
Related ▼

---

**Summary**

---

Name	app-switch
ID	27428a39-9b29-4f73-a1b8-0ffb83c7d4e3
Description	

Admin Status	● Up
Replication Mode	Hierarchical Two-Tier replication
VNI	33672
Logical Ports	0
Traffic Type	Overlay
Transport Zone	TZ.ONE
Created	7/28/2016, 11:35:51 AM by admin
Last Updated	7/28/2016, 11:35:51 AM by admin

## 5 修改虛擬機器的 VMX 檔案。

刪除 **ethernet1.networkName = "<name>"** 欄位並新增下列欄位：

- ethernet1.opaqueNetwork.id = "<logical switch's ID>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<VM's externalId>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

例如：

### 舊內容 (OLD)

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
```

### 新內容 (NEW)

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"
```

- 6 在 NSX Manager UI 中，新增邏輯交換器連接埠，並使用虛擬機器的 `externalId` 來連結 VIF。

例如：

**New Logical Port** [X]

Name: \*

Description:

Logical Switch: \*

Admin State: \* ☒ Up

Attachment Type: \*

Attachment ID:

Switching Profiles Type: \*

Switching Profiles Id:

- 7 重新登錄虛擬機器並開啟其電源。

您可以使用虛擬機器管理工具或 ESXi CLI，如此處所示。

```
[user@host:~] vim-cmd /solo/register /path/to/file.vmx
```

For example:

```
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9
```

```
[user@host:~] vim-cmd /vmsvc/power.on 9
Powering on VM:
```

在 NSX Manager UI 的 **交換 > 連接埠 (Switching > Ports)** 下方，尋找符合虛擬機器之 `externalId` 的 VIF 連結識別碼，並確定管理和運作狀態皆為已開啟。

如果兩個虛擬機器連結至相同的邏輯交換器，而 IP 位址也設定在相同的子網路中，則應該可以互相進行 Ping 偵測。

#### 後續步驟

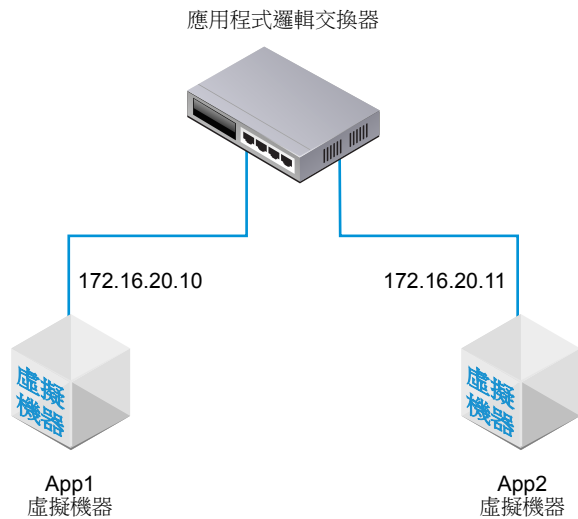
新增邏輯路由器。

您可以監控邏輯交換器連接埠上的活動以針對問題進行疑難排解。請參閱[監控邏輯交換器連接埠活動](#)。

## 將 KVM 上裝載的虛擬機器連結至 NSX-T 邏輯交換器

如果您有 KVM 主機，您可以使用此程序將虛擬機器連結至 NSX-T 邏輯交換器。

此程序顯示的範例會說明如何將名為 `app-vm` 的虛擬機器連結至名為 `app-switch` 的邏輯交換器。



### 先決條件

- 虛擬機器必須裝載在已新增至 NSX-T 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T 管理平面 (MPA) 和 NSX-T 控制平面 (LCP) 連線。
- 網狀架構節點必須新增至傳輸區域。
- 必須建立邏輯交換器。

### 程序

- 1 從 KVM CLI, 執行 `virsh dumpxml <your vm> | grep interfaceid` 命令。

- 2 在 NSX Manager UI 中，新增邏輯交換器連接埠，並針對 VIF 連結使用虛擬機器的介面識別碼。

例如：

**New Logical Port** [X]

Name: \* to-app

Description:

Logical Switch: \* app-tier-01

Admin State: \* ☒ Up

Attachment Type: \* VIF

Attachment ID: 50066bae-0f8a-386b-e62e-b0b9c6013a51

Switching Profiles Type: \* None

Switching Profiles Id:

[Save] [Cancel]

在**交換 > 連接埠 (Switching > Ports)**下的 NSX Manager UI，尋找 VIF 連結識別碼，並確定管理和運作狀態皆為已開啟。

如果兩個虛擬機器連結至相同的邏輯交換器，而 IP 位址也設定在相同的子網路中，則應該可以互相進行 Ping 偵測。

### 後續步驟

新增邏輯路由器。

您可以監控邏輯交換器連接埠上的活動以針對問題進行疑難排解。請參閱[監控邏輯交換器連接埠活動](#)。

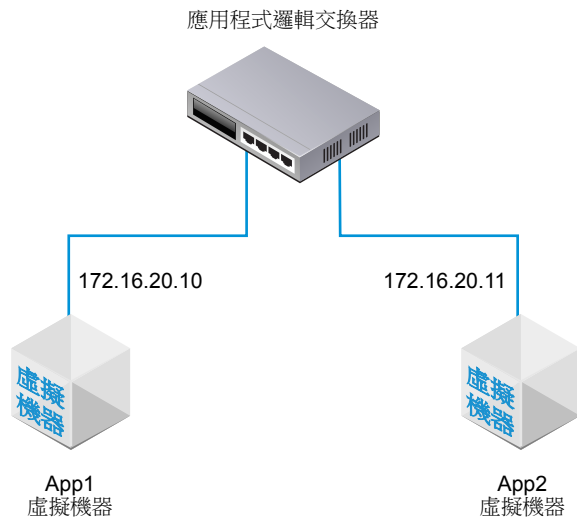
## 測試第 2 層連線

在您成功地設定邏輯交換器並將虛擬機器連結至邏輯交換器後，即可測試已連結虛擬機器的網路連線。

如果您的網路環境有正確設定，則根據拓撲，App2 VM 可以對 App1 VM 執行 Ping 偵測。



圖 2-3：邏輯交換器拓撲



### 程序

- 1 使用 SSH 或虛擬機器主控台，登入連結至邏輯交換器的其中一個虛擬機器。

例如，App2 VM 172.16.20.11。

- 2 對連結至邏輯交換器的第二個虛擬機器執行 Ping 偵測以測試其連線。

```

$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
 64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
 64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
 64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
 2 packets transmitted, 2 received, 0% packet loss, time 1990ms
 rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
  
```

- 3 (可選) 找出導致 Ping 偵測失敗的問題。
  - a 確認虛擬機器網路設定正確無誤。
  - b 確認虛擬機器網路介面卡已連線到正確的邏輯交換器。
  - c 確認邏輯交換器管理狀態為「已啟用」。
  - d 從 NSX Manager，選取交換 > 交換器。

- e 按一下邏輯交換器並記下 UUID 和 VNI 資訊。
- f 從 NSX Controller，執行下列命令以疑難排解問題。

命令	說明
<b>get logical-switch &lt;vni-or-uuid&gt; arp-table</b>	顯示所指定邏輯交換器的 ARP 表格。 輸出範例。  <pre>nsx-controller1&gt; get logical-switch 41866 arp-table VNI      IP      MAC      Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; connection-table</b>	顯示所指定邏輯交換器的連線。 輸出範例。  <pre>nsx-controller1&gt; get logical-switch 41866 connection-table Host-IP      Port      ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; mac-table</b>	顯示所指定邏輯交換器的 MAC 表格。 輸出範例。  <pre>nsx-controller1&gt; get logical-switch 41866 mac-table VNI      MAC      VTEP-IP      Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; stats</b>	顯示所指定邏輯交換器的相關統計資訊。 輸出範例。  <pre>nsx-controller1&gt; get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; stats-sample</b>	顯示所有邏輯交換器時間推移統計資料的摘要。 輸出範例。  <pre>nsx-controller1&gt; get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>

命令	說明
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<b>get logical-switch &lt;vni-or-uuid&gt; vtep</b>	<p>顯示與指定邏輯交換器相關的所有虛擬通道端點。 輸出範例。</p> <pre>nsx-controller1&gt; get logical-switch 41866 vtep VNI      IP          LABEL      Segment MAC      Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c: 28 295422</pre>

連結至邏輯交換器的第一個虛擬機器可以傳送封包給第二個虛擬機器。

# 設定邏輯交換器和邏輯連接埠的交換設定檔

## 3

交換設定檔包含邏輯交換器和邏輯連接埠的第 2 層網路組態詳細資料。**NSX Manager** 支援數種類型的交換設定檔，並且會為每種設定檔類型保有一或多個系統定義的預設交換設定檔。

可供使用的交換設定檔類型如下。

- QoS (服務品質)
- 連接埠監控
- IP 探索
- SpoofGuard
- 交換器安全性
- MAC 管理

---

**備註** 您無法在 **NSX Manager** 中編輯或刪除預設交換設定檔。您可以改為建立自訂交換設定檔。

---

每個預設或自訂交換設定檔皆有唯一的保留識別碼。您可以使用此識別碼，讓交換設定檔與邏輯交換器或邏輯連接埠建立關聯。例如，預設的 QoS 交換設定檔識別碼為 `f313290b-eba8-4262-bd93-fab5026e9495`。

邏輯交換器或邏輯連接埠可與每種類型的其中一個交換設定檔建立關聯。例如，您不能讓兩個不同的 QoS 交換設定檔關聯至一個邏輯交換器或邏輯連接埠。

如果在建立或更新邏輯交換器時未關聯交換設定檔類型，則 **NSX Manager** 會關聯對應的預設系統定義交換設定檔。子邏輯連接埠會繼承父邏輯交換器的預設系統定義交換設定檔。

在建立或更新邏輯交換器或邏輯連接埠時，您可以選擇關聯預設或自訂的交換設定檔。當交換設定檔與邏輯交換器建立關聯或解除關聯時，系統會根據下列準則套用子邏輯連接埠的交換設定檔。

- 如果父邏輯交換器具有與其相關聯的設定檔，則子邏輯連接埠會繼承其父系的交換設定檔。
- 如果父邏輯交換器沒有與其相關聯的交換設定檔，則系統會對邏輯交換器指派預設交換設定檔，且邏輯連接埠會繼承該預設交換設定檔。

- 如果您明確地關聯自訂設定檔與邏輯連接埠，則此自訂設定檔會覆寫現有的交換設定檔。

**備註** 如果您已將自訂交換設定檔與邏輯交換器建立關聯，但想讓其中一個子邏輯連接埠保留預設的交換設定檔，則必須複製預設的交換設定檔，並讓此設定檔與特定的邏輯連接埠建立關聯。

如果自訂交換設定檔關聯到邏輯交換器或邏輯連接埠，則您無法刪除該設定檔。您可以前往 [摘要] 視圖的 [指派至] 區段，然後按一下列出的邏輯交換器和邏輯連接埠，以瞭解是否有任何邏輯交換器和邏輯連接埠與自訂交換設定檔建立關聯。

本章包含以下主題：

- [瞭解 QoS 交換設定檔](#)
- [瞭解連接埠鏡像交換設定檔](#)
- [瞭解 IP 探索交換設定檔](#)
- [瞭解 SpoofGuard](#)
- [瞭解交換器安全性交換設定檔](#)
- [瞭解 MAC 管理交換設定檔](#)
- [建立自訂設定檔與邏輯交換器之間的關聯](#)
- [建立自訂設定檔與邏輯交換器連接埠之間的關聯](#)

## 瞭解 QoS 交換設定檔

QoS 可為需要高頻寬的偏好流量提供高品質的專用網路效能。為了達成此目的，QoS 機制即使在發生網路壅塞時，仍可為偏好的封包排定優先使用充足頻寬、控制延遲和時基誤差以及減少資料遺失。此種網路服務層級是透過有效運用現有網路資源來提供。

在此版本中，支援控管和流量標記，即 CoS 和 DSCP。第 2 層服務類別 (CoS) 可讓您在因發生壅塞而在邏輯交換器中緩衝流量時，指定資料封包的優先順序。第 3 層區別服務代碼點 (DSCP) 會根據其封包的 DSCP 值來偵測封包。無論信任模式為何，系統將一律將 CoS 套用至資料封包。

NSX-T 會信任由虛擬機器套用的 DSCP 設定或在邏輯交換器層級修改並設定 DSCP 值。在每種情況下，DSCP 值皆會傳播至封裝式框架的外部 IP 標頭。如此可讓外部實體網路根據外部標頭上的 DSCP 設定來決定流量的優先順序。當 DSCP 處於信任模式時，系統會從內部標頭複製 DSCP 值。而處於未受信任模式時，系統不會為內部標頭保留 DSCP 值。

**備註** DSCP 設定僅適用於通道流量。這些設定不適用於相同 Hypervisor 內部的流量。

您可以使用 QoS 交換設定檔來設定平均入口和出口頻寬值，以便設定傳輸限制速率。尖峰頻寬速率會用於支援邏輯交換器所允許的高載流量，避免北向網路連結發生壅塞。不過，這些設定無法保證頻寬，僅能協助限制網路頻寬的使用。

QoS 交換設定檔的設定會套用至邏輯交換器並由子邏輯交換器連接埠繼承。

## 設定自訂 QoS 交換設定檔

您可以定義 DSCP 值並設定入口與出口設定來建立自訂 QoS 交換設定檔。

## 先決條件

- 自行熟悉 QoS 交換設定檔概念。請參閱[瞭解 QoS 交換設定檔](#)。
- 識別要排列優先順序的網路流量。

## 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換設定檔 (Switching Profiles)**。
- 3 按一下**新增 (Add)**。
- 4 完成 QoS 交換設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派至自訂 QoS 交換設定檔。 您可以選擇性地描述您在設定檔中修改的設定。
類型	從下拉式功能表中選取 <b>QoS</b> 。
DSCP	<p>從 [模式] 下拉式功能表中選取<b>信任 (Trusted)</b>或<b>未受信任 (Untrusted)</b>選項。</p> <p>當您選取「受信任」模式，內部標頭 DSCP 值會套用至 IP/IPv6 流量的外部 IP 標頭。針對非 IP/IPv6 流量，外部 IP 標頭會採用預設值。以覆蓋為基礎的邏輯連接埠上支援信任模式。預設值為 0。</p> <p>以覆蓋為基礎及以 VLAN 為基礎的邏輯連接埠上支援未受信任模式。針對以覆蓋為基礎的邏輯連接埠，輸出 IP 標頭的 DSCP 值會設為與邏輯連接埠內部封包類型無關的設定值。針對以 VLAN 為基礎的邏輯連接埠，IP/IPv6 封包的 DSCP 值會設為設定值。未受信任模式的 DSCP 值範圍介於 0 至 63 之間。</p> <p><b>備註</b> DSCP 設定僅適用於通道流量。這些設定不適用於相同 Hypervisor 內部的流量。</p>
服務類別	<p>設定流量優先順序層級。</p> <p>以 VLAN 為基礎的邏輯連接埠上支援 CoS。CoS 會分組網路中的類似流量類型，且每個流量類型會根據其本身的服務優先順序層級而視為一個類別。較低優先順序的流量會變慢或在某些情況下會捨棄，可提供較佳的輸送量以處理較高優先順序的流量。CoS 也可以使用 0 封包針對 VLAN 識別碼進行設定。</p> <p>CoS 值範圍從 0 至 7，其中 0 是優先順序最低的服務。</p>
入口	<p>設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>您可以使用平均頻寬來降低網路壅塞。尖峰頻寬速率用來支援高載流量，且高載期間會在高載大小設定中進行設定。您無法保證頻寬。但是，您可以使用設定來限制網路頻寬。預設值為 0，表示停用入口流量。</p> <p>例如，當您將邏輯交換器的平均頻寬設定為 30 Mbps 時，原則便會限制頻寬。您可以為 100 Mbps 的高載流量設定 20 個位元組持續時間的上限。</p>
入口廣播	<p>根據廣播設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>預設值為 0，表示停用入口廣播流量。</p> <p>例如，當您將邏輯交換器的平均頻寬設定為 50 Kbps 時，原則便會限制頻寬。您可以為 400 Kbps 的高載流量設定 60 個位元組持續時間的上限。</p>
出口	<p>設定從邏輯網路至虛擬機器的輸入網路流量自訂值。</p> <p>預設值為 0，表示停用出口流量。</p>

如果並未設定入口、入口廣播及出口選項，則預設值會用來作為通訊協定緩衝區。

## 5 按一下儲存 (Save)。

自訂 QoS 交換設定檔會顯示為連結。

### 後續步驟

將此 QoS 自訂交換設定檔連結至邏輯交換器，讓交換設定檔中已修改的參數可套用至網路流量。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)。

## 瞭解連接埠鏡像交換設定檔

邏輯連接埠鏡像可讓您將連結至虛擬機器 VIF 連接埠之邏輯交換器連接埠的所有進出流量，進行複寫並重新導向。鏡像流量會在 Generic Routing Encapsulation (GRE) 通道中以封裝方式傳送給收集器，以便在周遊網路至遠端目的地的同時，保留所有原始封包資訊。

連接埠鏡像通常用於下列案例：

- 疑難排解 - 分析流量以偵測入侵，以及偵錯和診斷網路上的錯誤。
- 符合性和監控 - 將所有受監控流量轉送至網路應用裝置以進行分析和修復。

與實體連接埠鏡像相較，邏輯連接埠鏡像可以確保擷取到所有虛擬機器網路流量。如果您僅在實體網路實作連接埠鏡像，則某些虛擬機器網路流量會無法進行鏡像。這是因為位於相同主機上之虛擬機器之間的通訊一律不會進入實體網路，因此無法取得鏡像。而透過邏輯連接埠鏡像，即使將虛擬機器移轉至其他主機，您仍可繼續對虛擬機器流量進行鏡像。

針對 NSX-T 網域中的虛擬機器連接埠以及實體應用程式的連接埠，兩者皆有類似的連接埠鏡像程序。您可以轉送連線至邏輯網路之工作負載所擷取到的流量，並將該流量鏡像至收集器。裝載虛擬機器的客體 IP 位址應可存取此 IP 位址。此程序同樣適用於連線至閘道節點的實體應用程式。

## 設定自訂連接埠鏡像交換設定檔

您可以使用不同的目的地及金鑰值建立自訂連接埠鏡像交換設定檔。

### 先決條件

- 自行熟悉連接埠鏡像交換設定檔概念。請參閱[瞭解連接埠鏡像交換設定檔](#)。
- 識別您要重新導向網路流量之目的地邏輯連接埠識別碼的 IP 位址。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換設定檔 (Switching Profiles)**。
- 3 按一下**新增 (Add)**。

#### 4 完成連接埠鏡像交換設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派至自訂連接埠鏡像交換設定檔。 您可以選擇性地描述您修改的設定以自訂此設定檔。
類型	從下拉式功能表中選取 <b>連接埠鏡像 (Port Mirroring)</b> 。
方向	從下拉式功能表中選取選項，將此來源用於入口 (Ingress)、出口 (Egress)或雙向 (Bidirectional)流量。 入口是從虛擬機器至邏輯網路的輸出網路流量。 出口是從邏輯網路至虛擬機器的輸入網路流量。 雙向是從虛擬機器至邏輯網路以及從邏輯網路至虛擬機器的雙向流量。這是預設的選項。
封包截斷	選擇性。範圍是 60 - 65535。
金鑰	輸入隨機 32 位元值以識別來自邏輯連接埠的鏡像封包。 此「金鑰」值會複製到每個鏡像封包之 GRE 標頭中的 [金鑰] 欄位。如果「金鑰」值設定為 0，則預設定義會複製到 GRE 標頭中的 [金鑰] 欄位。 預設 32 位元值是由下列值所組成。 <ul style="list-style-type: none"> <li>第一個 24 位元是 VNI 值。VNI 是封裝式框架 IP 標頭的一部分。</li> <li>第 25 個位元表示第一個 24 位元是否為有效的 VNI 值。1 代表有效值，而 0 代表無效值。</li> <li>第 26 個位元表示鏡像流量的方向。1 代表入口方向，而 0 代表出口方向。</li> <li>其餘的六個位元並未使用。</li> </ul>
目的地	輸入鏡像工作階段的收集器目的地識別碼。 目的地 IP 位址 ID 僅能為網路內的 IPv4 位址，或非由 NSX-T 所管理的遠端 IPv4 位址。您可以新增最多三個目的地 IP 位址，並以逗號分隔。

#### 5 按一下儲存 (Save)。

自訂連接埠鏡像交換設定檔會顯示為連結。

##### 後續步驟

確認自訂的連接埠鏡像交換設定檔可正常運作。請參閱[確認自訂連接埠鏡像交換設定檔](#)。

## 確認自訂連接埠鏡像交換設定檔

在開始使用自訂連接埠鏡像交換設定檔之前，請先確認自訂項目可以正常運作。

##### 先決條件

- 確認已設定自訂連接埠鏡像交換設定檔。請參閱[設定自訂連接埠鏡像交換設定檔](#)。
- 確認已將自訂連接埠鏡像交換設定檔連結至邏輯交換器。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)。

##### 程序

#### 1 找到具有 VIF 連結至已設定連接埠鏡像之邏輯連接埠的兩個虛擬機器。

例如，VM1 10.70.1.1 和 VM2 10.70.1.2 具有 VIF 連結，且其位於相同邏輯網路中。



- 2 在目的地 IP 位址上執行 `tcpdump` 命令。

```
sudo tcpdump -n -i eth0 dst host destination_IP_address and proto gre
```

例如，目的地 IP 位址是 10.24.123.196。

- 3 登入第一個虛擬機器並對第二個虛擬機器執行 Ping 偵測，以確認目的地位址可收到對應的 ECHO 要求和回應。

例如，第一個虛擬機器 10.70.1.1 對第二個虛擬機器 10.70.1.2 執行 Ping 偵測以確認連接埠鏡像。

No.	Time	Source	Destination	Protocol	Length	Info
8	0.748510	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=57/14592, ttl=64
9	0.748521	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=57/14592, ttl=64
30	1.748345	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=58/14848, ttl=64
31	1.748602	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=58/14848, ttl=64
59	2.748266	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=59/15104, ttl=64
60	2.748515	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=59/15104, ttl=64
90	3.748306	10.70.1.1	10.70.1.2	ICMP	140	Echo (ping) request id=0x650c, seq=60/15360, ttl=64
91	3.748563	10.70.1.2	10.70.1.1	ICMP	140	Echo (ping) reply id=0x650c, seq=60/15360, ttl=64

### 後續步驟

將此連接埠鏡像自訂交換設定檔連結至邏輯交換器，讓交換設定檔中已修改的參數可套用至網路流量。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)。

## 瞭解 IP 探索交換設定檔

IP 探索會使用 DHCP 或 ARP 窺探來學習虛擬機器 MAC 和 IP 位址。學習 MAC 和 IP 位址後，這些項目會與 NSX Controller 共用以進行 ARP 隱藏。ARP 隱藏可將連線至相同邏輯交換器之虛擬機器中的 ARP 流量洪泛降至最低。

DHCP 窺探會檢查在虛擬機器 DHCP 用戶端和 DHCP 伺服器之間交換的 DHCP 封包，以學習虛擬機器 IP 和 MAC 位址。

ARP 窺探會檢查虛擬機器的傳出 ARP 和 GARP，以學習 IP 和 MAC 位址。

## 設定 IP 探索交換設定檔

您可以啟用 ARP 窺探或 DHCP 窺探以建立自訂 IP 探索交換設定檔，它會學習 IP 與 MAC 位址來確定邏輯交換器的 IP 完整性。

### 先決條件

熟悉 IP 探索交換設定檔概念。請參閱[瞭解 IP 探索交換設定檔](#)。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的 **交換 (Switching) > 交換設定檔 (Switching Profiles)**。
- 3 按一下 **新增 (Add)**。

#### 4 完成 IP 探索交換設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派至自訂 IP 探索交換設定檔。 您可以選擇性地描述您在設定檔中啟用的設定。
類型	從下拉式功能表中選取 <b>IP 探索 (IP Discovering)</b> 。
ARP 窺探	切換 <b>ARP 窺探 (ARP Snooping)</b> 按鈕以啟用功能。 ARP 窺探會檢查虛擬機器傳出 ARP 和 GARP 以學習虛擬機器 MAC 及 IP 位址。 如果虛擬機器使用靜態 IP 位址而非 DHCP，則適用於 ARP 窺探。
DHCP 窺探	切換 <b>DHCP 窺探 (DHCP Snooping)</b> 按鈕以啟用功能。 DHCP 窺探會檢查虛擬機器 DHCP 用戶端及 DHCP 伺服器之間交換的 DHCP 封包，以學習虛擬機器 MAC 及 IP 位址。

#### 5 按一下儲存 (Save)。

自訂 IP 探索交換設定檔會顯示為連結。

#### 後續步驟

將此 IP 探索自訂交換設定檔連結至邏輯交換器，讓交換設定檔中已修改的參數可套用至網路流量。請參閱 [建立自訂設定檔與邏輯交換器之間的關聯](#)。

## 瞭解 SpoofGuard

SpoofGuard 可協助防止一種稱為「網路詐騙」或「網路釣魚」的惡意攻擊。SpoofGuard 原則可封鎖判定為詐騙的流量。

SpoofGuard 是一種工具，專門設計來防止您環境中的虛擬機器從未獲授權的 IP 位址傳送流量。如果虛擬機器的 IP 位址不符合 SpoofGuard 中相對應之邏輯連接埠和交換器位址繫結的 IP 位址，系統即會完全阻止虛擬機器的 vNIC 存取網路。您可以在連接埠或交換器層級設定 SpoofGuard。您可以基於下列幾個原因而在環境中使用 SpoofGuard：

- 防止惡意虛擬機器取得現有虛擬機器的 IP 位址。
- 確保虛擬機器的 IP 位址不會在未經介入的情況便遭到更改，在某些環境中，建議虛擬機器無法在未經適當的變更控制審查之下即更改其 IP 位址。為了促進此一目的，SpoofGuard 會確保虛擬機器擁有者無法輕鬆更改 IP 位址並順利繼續進行工作。
- 保證分散式防火牆 (DFW) 規則不會被無意 (或故意) 略過 – 對於使用 IP 集合作為來源或目的地的已建立 DFW 規則，虛擬機器的 IP 位址可能在封包標頭中遭到偽造，藉以略過相關規則。

NSX-T SpoofGuard 組態涵蓋下列項目：

- MAC SpoofGuard - 驗證封包的 MAC 位址
- IP SpoofGuard - 驗證封包的 MAC 和 IP 位址
- 動態位址解析通訊協定 (ARP) 檢查，亦即會針對 ARP/GARP/ND 裝載中的 MAC 來源、IP 來源和 IP-MAC 來源對應，進行所有 ARP 和 Gratuitous 位址解析通訊協定 (GARP) SpoofGuard 和芳鄰探索 (ND) SpoofGuard 驗證。

在連接埠層級中，系統會透過連接埠的位址繫結內容提供允許的 MAC/VLAN/IP 白名單。當虛擬機器傳送流量時，如果其 IP/MAC/VLAN 不符合連接埠的 IP/MAC/VLAN 內容，即會遭到捨棄。連接埠層級 SpoofGuard 會負責處理流量驗證，例如流量是否符合 VIF 組態。

在交換器層級中，系統會透過交換器的位址繫結內容提供允許的 MAC/VLAN/IP 白名單。這通常是交換器的允許 IP 範圍/子網路，並由交換器層級 SpoofGuard 負責處理流量授權。

流量必須獲得連接埠層級「和」交換器層級 SpoofGuard 的允許，才能允許進入交換器。連接埠和交換器層級 SpoofGuard 的啟用或停用可使用 SpoofGuard 交換器設定檔來控制。

## 設定連接埠位址繫結

位址繫結會指定邏輯連接埠的 IP 和 MAC 位址，並用來指定 SpoofGuard 中的連接埠白名單。

您可以利用連接埠位址繫結來指定 IP 和 MAC 位址以及邏輯連接埠的 VLAN (如果適用)。當 SpoofGuard 啟用時，它會確保在資料路徑中強制執行指定的位址繫結。除了 SpoofGuard，連接埠位址繫結會用於 DFW 規則轉譯。

### 程序

- 1 在 NSX Manager 中，導覽至 **交換 > 連接埠 (Switching > Ports)**。
- 2 按一下您要套用位址繫結的邏輯連接埠。  
邏輯連接埠摘要隨即顯示。
- 3 在 [摘要] 索引標籤下，展開 **位址繫結 (Address Bindings)**。
- 4 按一下 **新增 (Add)**。  
新增位址繫結對話方塊隨即顯示
- 5 指定您要套用位址繫結之邏輯連接埠的 IP 和 MAC 位址。您也可以選擇性地指定 VLAN。
- 6 按一下 **儲存 (Save)**。

### 後續步驟

當您設定 [SpoofGuard 交換設定檔](#) 時使用連接埠位址繫結。

## 設定交換器位址繫結

位址繫結允許 IP 與 MAC 位址範圍及 VLAN 繫結至交換器。

在 SpoofGuard 中，位址繫結會提供允許的 MAC/VLAN/IP 白名單。啟用對應的 SpoofGuard 之後，SpoofGuard 會確保在資料路徑中強制執行指定的位址繫結。

### 程序

- 1 在 NSX Manager 中，導覽至 **交換 > 交換器 (Switching > Switches)**。
- 2 按一下您要套用位址繫結的邏輯交換器。  
在右窗格中，交換器摘要隨即顯示。
- 3 在 [摘要] 索引標籤下，展開 **位址繫結 (Address Bindings)**。

#### 4 按一下**新增 (Add)**。

[新增位址繫結] 對話方塊隨即顯示。

#### 5 在交換器位址繫結中輸入 MAC 位址和交換器的 IP 範圍 (以及 VLAN，如果適用)。

指定 IP 範圍/子網路後，資料路徑會將繫結套用至交換器上的所有連接埠。

#### 6 按一下**儲存 (Save)**。

#### 後續步驟

現在，您將**設定 SpoofGuard 交換設定檔**並將位址繫結新增至 SpoofGuard 白名單。

## 設定 SpoofGuard 交換設定檔

當設定 SpoofGuard 時，如果虛擬機器的 IP 位址變更，則可能會封鎖來自虛擬機器的流量，直到對應的已設定連接埠/交換器位址繫結使用新的 IP 位址更新為止。

針對包含客體的連接埠群組啟用 SpoofGuard。針對每個網路介面卡啟用時，SpoofGuard 會檢查指定 MAC 的封包及其對應的 IP 位址。

#### 先決條件

在設定 SpoofGuard 之前，新增每個邏輯交換器上的位址繫結或交換器繫結。位址繫結可讓您將 IP 位址和 MAC 位址繫結至連接埠或交換器。[設定連接埠位址繫結](#)[設定交換器位址繫結](#)

#### 程序

#### 1 在 NSX Manager 中，導覽至**交換 > 交換設定檔 (Switching > Switching Profiles)**。

#### 2 按一下**新增 (Add)**。

新的交換設定檔視窗隨即顯示。

#### 3 為設定檔命名並選取 **SpoofGuard** 作為類型。您也可以新增設定檔說明。

#### 4 如果要啟用連接埠層級 SpoofGuard，請選取**連接埠繫結 (port bindings)**，而如果要啟用交換器層級 SpoofGuard，請選取**交換器繫結 (switch bindings)**。

位址繫結是連接埠和交換器 SpoofGuard 的允許白名單。

#### 5 按一下**儲存 (Save)**。

已使用 SpoofGuard 設定檔建立新的交換設定檔。

#### 後續步驟

將 SpoofGuard 設定檔與邏輯交換器相關聯。[建立自訂設定檔與邏輯交換器之間的關聯](#)

## 瞭解交換器安全性交換設定檔

交換器安全性可透過檢查邏輯交換器的入口流量，以及將 IP 位址、MAC 位址和通訊協定與一組允許之位址和通訊協定進行比對來捨棄從虛擬機器傳送的未授權封包，從而提供無狀態的第 2 層和第 3 層安全性。您可以使用交換器安全性，篩除來自網路中虛擬機器的惡意攻擊，藉以保護邏輯交換器的完整性。

您可以透過設定橋接通訊協定資料單位 (BPDU) 篩選器、DHCP 窺探、DHCP 伺服器封鎖以及速率限制選項，來自訂邏輯交換器上的交換器安全性交換設定檔。

## 設定自訂交換器安全性交換設定檔

您可以使用來自允許 BPDU 清單的 MAC 目的地位址，以建立自訂交換器安全性交換設定檔並設定速率限制。

### 先決條件

自行熟悉交換器安全性交換設定檔概念。請參閱[瞭解交換器安全性交換設定檔](#)。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換設定檔 (Switching Profiles)**。
- 3 按一下**新增 (Add)**。
- 4 完成交換器安全性設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派至自訂交換器安全性設定檔。 您可以選擇性地描述您在設定檔中修改的設定。
類型	從下拉式功能表中選取 <b>交換器安全性 (Switch Security)</b> 。
BPDU 篩選器	切換 <b>BPDU 篩選器 (BPDU filter)</b> 按鈕以啟用 BPDU 篩選。 當 BPDU 篩選器啟用時，系統會封鎖所有對 BPDU 目的地 MAC 位址的流量。 BPDU 篩選器啟用時也會停用邏輯交換器連接埠上的 STP，因為這些連接埠不應包含在 STP 中。
BPDU 篩選器允許清單	從 BPDU 目的地 MAC 位址清單按一下目的地 MAC 位址，以便允許對允許目的地之流量。
DHCP 篩選器	切換 <b>伺服器封鎖 (Server Block)</b> 按鈕及 <b>用戶端封鎖 (Client Block)</b> 按鈕以啟用 DHCP 篩選。 「DHCP 伺服器封鎖」會封鎖 DHCP 伺服器至 DHCP 用戶端的流量。請注意，它不會封鎖 DHCP 伺服器至 DHCP 轉送代理程式的流量。 「DHCP 用戶端封鎖」會封鎖 DHCP 要求，以防止虛擬機器取得 DHCP IP 位址。

選項	說明
封鎖非 IP 流量	<p>切換<b>封鎖非 IP 流量 (Block Non-IP Traffic)</b>按鈕以僅允許 IPv4、IPv6、ARP、GARP 和 BPDU 流量。</p> <p>系統會封鎖剩餘的非 IP 流量。允許的 IPv4、IPv6、ARP、GARP 和 BPDU 流量是根據位址繫結及 <b>SpoofGuard</b> 組態中所設定的其他原則而定。</p> <p>依預設，系統會停用此選項以允許非 IP 流量以一般流量方式處理。</p>
速率限制	<p>設定入口與出口廣播及多點傳送流量的速率限制。</p> <p>設定速率限制可保護邏輯交換器或虛擬機器，例如廣播流量風暴。</p> <p>若要避免任何連線問題，最低速率限制值必須 <math>\geq 10</math> pps。</p>

## 5 按一下儲存 (Save)。

自訂交換器安全性設定檔會顯示為連結。

### 後續步驟

將此交換器安全性自訂交換設定檔連結至邏輯交換器，讓交換設定檔中已修改的參數可套用至網路流量。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)。

## 瞭解 MAC 管理交換設定檔

MAC 管理交換設定檔支援兩個功能：MAC 學習和 MAC 位址變更。

MAC 學習可針對在一個 vNIC 後面設定多個 MAC 位址的部署提供網路連線，例如 ESXi 虛擬機器在 ESXi 主機上執行，而 ESXi 虛擬機器中有多個虛擬機器執行的巢狀 Hypervisor 部署。如果沒有 MAC 學習，當 ESXi 虛擬機器的 vNIC 連線至交換器連接埠，其 MAC 位址會是靜態的。在 ESXi 虛擬機器中執行的虛擬機器不具備網路連線能力，因為其封包具有不同的來源 MAC 位址。透過 MAC 學習，vSwitch 會檢查來自 vNIC 之每個封包的來源 MAC 位址，藉此學習 MAC 位址並允許封包通過。如果在特定期間內未使用學習的 MAC 位址，則系統會將其移除。此使用期限內容無法進行設定。

MAC 學習也支援未知的單點傳播洪泛。通常，當連接埠收到的封包具有未知的目的地 MAC 位址時會捨棄封包。如果啟用未知的單點傳播洪泛，則連接埠會將未知的單點傳播流量洪泛至已啟用 MAC 學習和單點傳播洪泛之交換器上的每個連接埠。此內容依預設為啟用，但前提是已啟用 MAC 學習。

MAC 管理交換設定檔也支援虛擬機器變更其 MAC 位址的能力。連線至連接埠且已啟用 MAC 位址變更內容的虛擬機器，可以執行系統管理命令以變更其 vNIC 的 MAC 位址，且仍可在該 vNIC 上傳送和接收流量。僅 ESXi 才支援這個功能，KVM 並不支援。此內容依預設為停用。

如果您啟用 MAC 學習或 MAC 位址變更，請一併設定 **SpoofGuard** 以改善安全性。

如需建立 MAC 管理交換設定檔，以及將設定檔關聯至交換器或連接埠的詳細資訊，請參閱《[NSX-T API 指南](#)》。

**備註** 在此版本中，MAC 管理交換設定檔功能僅能透過 NSX API 使用。您無法透過 NSX Manager UI 使用。

## 建立自訂設定檔與邏輯交換器之間的關聯

若要將自訂交換設定檔套用至網路，您必須建立它與邏輯交換器之間的關聯。



當自訂交換設定檔連結至邏輯交換器時，這些設定檔便會覆寫現有的預設交換設定檔。子邏輯交換器連接埠會繼承自訂交換設定檔。

---

**備註** 如果您已將自訂交換設定檔與邏輯交換器建立關聯，但想讓其中一個子邏輯交換器連接埠保留預設的交換設定檔，則必須複製預設的交換設定檔，並讓此設定檔與特定的邏輯交換器連接埠建立關聯。

---

#### 先決條件

- 確認已設定邏輯交換器。請參閱[建立邏輯交換器](#)。
- 確認已設定自訂交換設定檔。請參閱第 3 章，[設定邏輯交換器和邏輯連接埠的交換設定檔](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換器 (Switches)**。
- 3 按兩下邏輯交換器以套用自訂交換設定檔。
- 4 按一下**管理 (Manage)**索引標籤。
- 5 從下拉式功能表中選取自訂交換設定檔類型。
  - QoS
  - 連接埠鏡像 (Port Mirroring)
  - IP 探索 (IP Discovering)
  - SpoofGuard
  - 交換器安全性 (Switch Security)
- 6 按一下**變更 (Change.)**。
- 7 從下拉式功能表中選取先前建立的自訂交換設定檔。
- 8 按一下**儲存 (Save)**。  
邏輯交換器現在會與自訂交換設定檔建立關聯。
- 9 確認**管理 (Manage)**索引標籤下方顯示具有已修改之組態的全新自訂交換設定檔。
- 10 (可選) 按一下**相關 (Related)**索引標籤，然後從下拉式功能表中選取**連接埠 (Ports)**，以確認自訂交換設定檔已套用于子邏輯連接埠。

#### 後續步驟

如果您不想使用從邏輯交換器繼承而來的交換設定檔，您可以對子邏輯交換器連接埠套用自訂交換設定檔。請參閱[建立自訂設定檔與邏輯交換器連接埠之間的關聯](#)。

## 建立自訂設定檔與邏輯交換器連接埠之間的關聯

邏輯交換器連接埠提供 VIF 的邏輯連線點、連線至路由器的修補程式，或連線到外部網路的第 2 層閘道。邏輯交換器連接埠也會公開交換設定檔、連接埠統計資料計數器以及邏輯連結狀態。

您可以將繼承交換設定檔從邏輯交換器變更為不同子邏輯交換器連接埠的自訂交換設定檔。

#### 先決條件

- 確認已設定邏輯交換器連接埠。請參閱[將虛擬機器連線到邏輯交換器](#)。
- 確認已設定自訂交換設定檔。請參閱第 3 章，[設定邏輯交換器和邏輯連接埠的交換設定檔](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 連接埠 (Port)**。
- 3 按兩下邏輯交換器連接埠以套用自訂交換設定檔。
- 4 按一下**管理 (Manage)**索引標籤。
- 5 從下拉式功能表中選取自訂交換設定檔類型。
  - **QoS**
  - **連接埠鏡像 (Port Mirroring)**
  - **IP 探索 (IP Discovering)**
  - **SpoofGuard**
  - **交換器安全性 (Switch Security)**
- 6 按一下**變更 (Change)**。
- 7 從下拉式功能表中選取先前建立的自訂交換設定檔。
- 8 按一下**儲存 (Save)**。

邏輯交換器連接埠現在會與自訂交換設定檔建立關聯。
- 9 確認**管理 (Manage)**索引標籤下方顯示具有已修改之組態的全新自訂交換設定檔。

#### 後續步驟

您可以監控邏輯交換器連接埠上的活動以針對問題進行疑難排解。請參閱[監控邏輯交換器連接埠活動](#)。

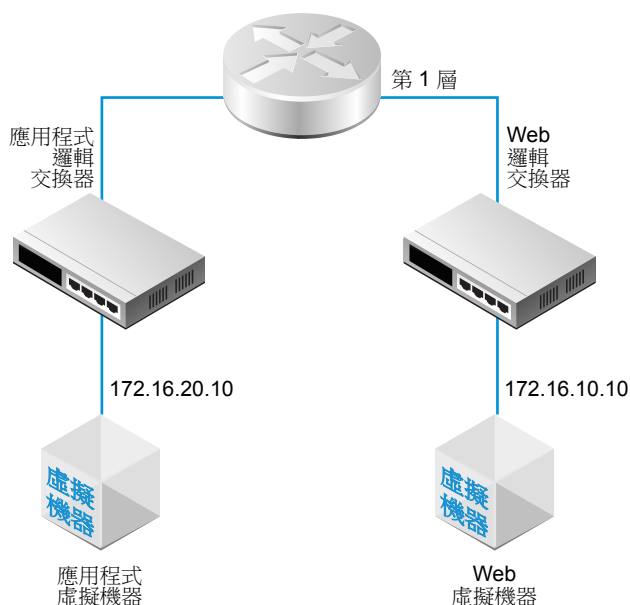


## 設定第 1 層邏輯路由器

NSX-T 邏輯路由器會在虛擬環境中重現從基礎硬體中完全分離的路由功能。第 1 層邏輯路由器具有下行連接埠可連線至 NSX-T 邏輯交換器，以及上行連接埠可連線至 NSX-T 第 0 層邏輯路由器。

當您新增邏輯路由器時，請務必規劃您要建置的網路拓撲。

圖 4-1：第 1 層邏輯路由器拓撲



例如，這個簡單拓撲會顯示兩個連線至第 1 層邏輯路由器的邏輯交換器。每個邏輯交換器皆會連線一部虛擬機器。這兩個虛擬機器可位於不同或相同的主機上，也可位於不同或相同的主機叢集中。如果邏輯路由器並未分隔虛擬機器，則虛擬機器上設定的基礎 IP 位址必須在相同的子網路中。如果邏輯路由器分隔虛擬機器，則虛擬機器上的 IP 位址必須在不同的子網路中。

本章包含以下主題：

- [建立第 1 層邏輯路由器](#)
- [新增第 1 層邏輯路由器的下行連接埠](#)
- [在第 1 層邏輯路由器上設定路由通告](#)
- [設定第 1 層邏輯路由器靜態路由](#)

## 建立第 1 層邏輯路由器

第 1 層邏輯路由器必須連線至第 0 層邏輯路由器，才能獲得北向實體路由器的存取權。

### 先決條件

- 確認已設定邏輯交換器。請參閱[建立邏輯交換器](#)。
- 確認已部署 NSX Edge 叢集，以便執行網路位址轉譯 (NAT) 組態。請參閱 NSX-T 安裝指南。
- 自行熟悉第 1 層邏輯路由器拓撲。請參閱[第 4 章](#)，設定第 1 層邏輯路由器。

### 程序

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

2 選取導覽面板中的**路由 (Routing)**。

3 按一下**新增 (Add)**，然後選取**第 1 層路由器 (Tier-1 Router)**。

4 指派邏輯路由器的名稱。

5 (可選) 選取要連線至這個第 1 層邏輯路由器的第 0 層邏輯路由器。

如果您尚未設定第 0 層邏輯路由器，則可以先暫時將此欄位保持空白，稍後再編輯路由器組態。

6 (可選) 選取要連線至這個第 1 層邏輯路由器的 Edge 叢集。

如果要對 NAT 組態使用第 1 層邏輯路由器，此路由器必須連線至 NSX Edge 叢集。如果您尚未設定 Edge 叢集，則可以先暫時將此欄位保持空白，稍後再編輯路由器組態。

7 按一下**儲存 (Save)**。

在 NSX Manager UI 中，新的邏輯路由器是可點選的連結。

### 後續步驟

建立第 1 層邏輯路由器的下行連接埠。請參閱[新增第 1 層邏輯路由器的下行連接埠](#)。

## 新增第 1 層邏輯路由器的下行連接埠

當您在第 1 層邏輯路由器上建立下行連接埠時，連接埠可作為相同子網路中之虛擬機器的預設閘道。

### 先決條件

確認已設定第 1 層邏輯路由器。請參閱[建立第 1 層邏輯路由器](#)。

### 程序

1 按一下第 1 層邏輯路由器連結以建立連接埠。

2 按一下**組態 (Configuration)**索引標籤。

3 按一下 [邏輯路由器連接埠] 區段下的**新增 (Add)**。

4 為邏輯路由器連接埠指派名稱。

- 5 選取此連接會建立交換器連接埠，或更新現有的交換器連接埠。

如果連接適用於現有的交換器連接埠，請從下拉式功能表選取連接埠。

- 6 以 CIDR 標記法輸入路由器連接埠 IP 位址。

例如，IP 位址可以是 172.16.10.1/24。

您也可以輸入預先設定的 DHCP 服務 IP 位址。

- 7 按一下**儲存 (Save)**。
- 8 (可選) 重複步驟 1-7 以建立額外的第 1 層邏輯路由器連接埠。
- 9 確認第 1 層邏輯路由器可以路由東向-西向虛擬機器流量。

在此範例中，第 1 層邏輯路由器具有兩個連線至兩個邏輯交換器的下行連接埠。每個邏輯交換器皆會連接一部虛擬機器。虛擬機器可以互相執行 Ping 偵測。

```
web-virtual-machine$ ping 172.16.20.10
PING 172.16.20.10 (172.16.20.10): 56(84) data bytes
64 bytes from 172.16.20.10: icmp_req=0 ttl=64 time=178 ms
^C
--- 172.16.20.10 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 178 ms/178 ms/178 ms/0.000 ms
```

```
app-virtual-machine$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 56(84) data bytes
64 bytes from 172.16.10.10: icmp_req=0 ttl=64 time=178 ms
^C
--- 172.16.10.10 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 178 ms/178 ms/178 ms/0.000 ms
```

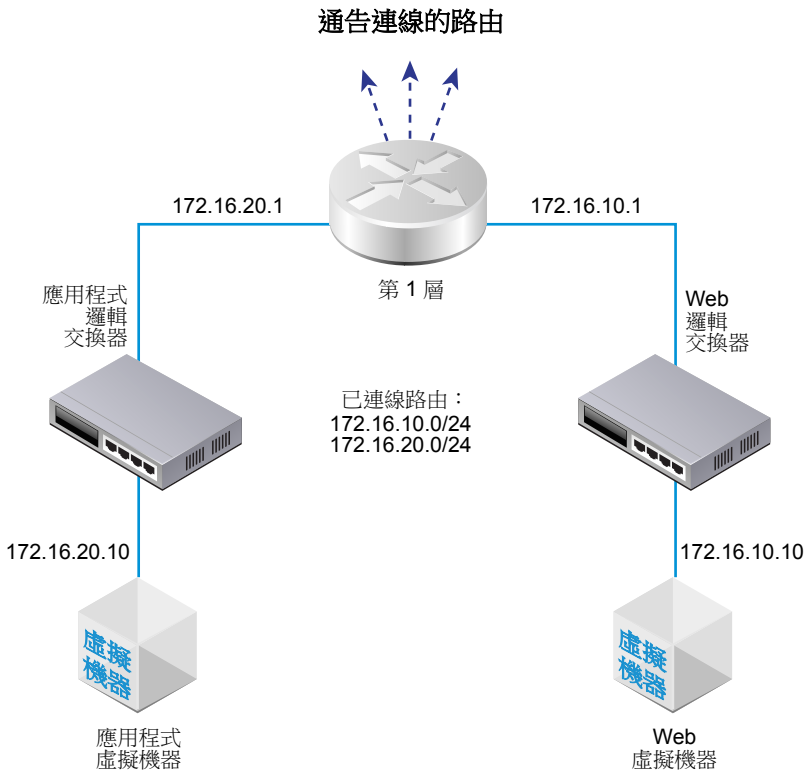
## 後續步驟

可讓路由通告提供虛擬機器與外部實體網路之間，或連線至相同第 0 層邏輯路由器之不同第 1 層邏輯路由器之間的北向-南向連線能力。請參閱[在第 1 層邏輯路由器上設定路由通告](#)。

## 在第 1 層邏輯路由器上設定路由通告

若要在連結至不同的第 1 層邏輯路由器之邏輯交換器的虛擬機器之間，提供第 3 層連線能力，則必須啟用對第 0 層的第 1 層路由通告。您不需要設定第 1 層與第 0 層邏輯路由器之間的路由通訊協定或靜態路由。當您啟用路由通告時，NSX-T 會自動建立 NSX-T 靜態路由。

例如，若要透過其他對等路由器提供往返虛擬機器的連線能力，則第 1 層邏輯路由器必須設定已連線路由的路由通告。如果您不想通告所有已連線的路由，則可以指定要通告的路由。



#### 先決條件

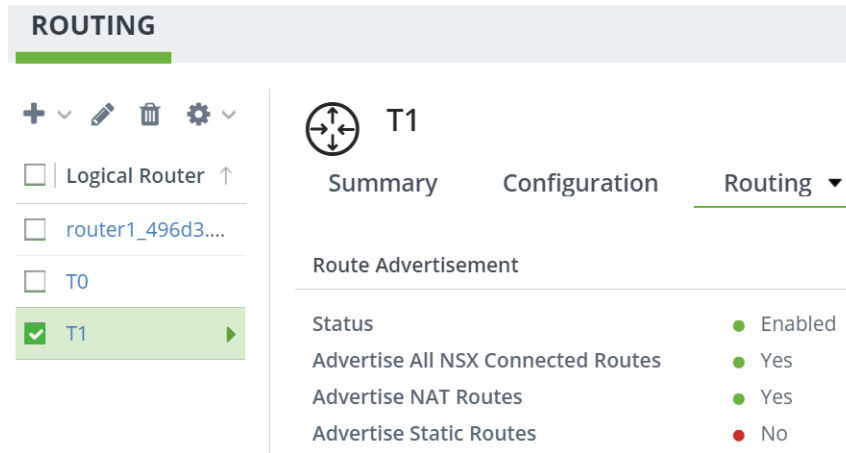
- 確認虛擬機器連結至邏輯交換器。請參閱第 2 章，[建立邏輯交換器與設定虛擬機器連結](#)。
- 確認已設定第 1 層邏輯路由器的下行連接埠。請參閱[新增第 1 層邏輯路由器的下行連接埠](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取**路由 (Routing)**。
- 3 按一下第 1 層邏輯路由器。
- 4 從路由下拉式功能表中選取**路由通告 (Route Advertisement)**。
- 5 按一下**編輯 (Edit)**並確定已啟用 [狀態] 按鈕來啟用路由通告。
- 6 指定要通告的路由，即所有路由或所選路由。
  - 按一下**編輯 (Edit)**並選取**通告所有 NSX 連線的路由 (Advertise All NSX Connected Routes)**。
  - 按一下**新增 (Add)**並輸入要通告之路由的相關資訊。針對每個路由，您可以使用 CIDR 格式來輸入名稱和路由首碼。

## 7 按一下狀態 (Status) 切換按鈕以啟用路由通告。

例如：



## 8 按一下儲存 (Save)。

### 後續步驟

自行熟悉第 0 層邏輯路由器拓撲並建立第 0 層邏輯路由器。請參閱[第 5 章，設定第 0 層邏輯路由器](#)。

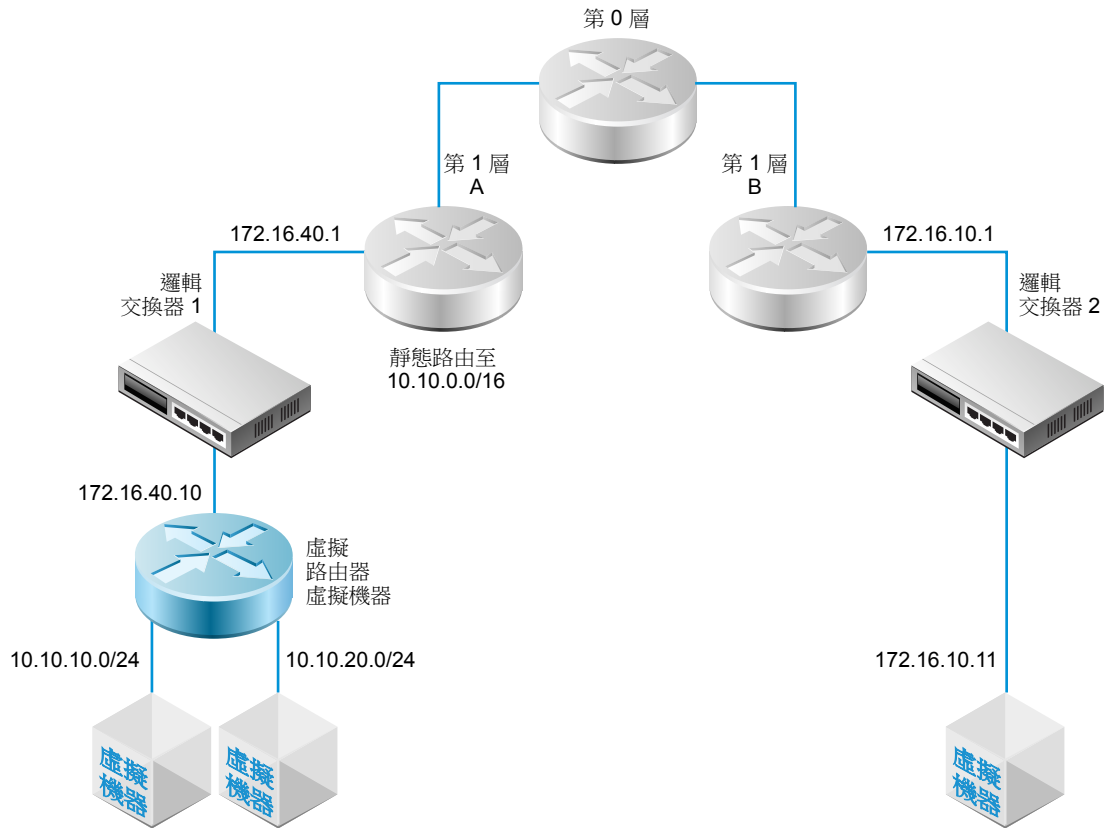
如果您已經有連線至第 1 層邏輯路由器的第 0 層邏輯路由器，則可以確認第 0 層路由器學習連線第 1 層路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

## 設定第 1 層邏輯路由器靜態路由

您可以在第 1 層邏輯路由器設定靜態路由，以提供可透過虛擬路由器存取之從 NSX-T 到一組網路的連線。

例如，在下圖中，第 1 層的 A 邏輯路由器具有通往 NSX-T 邏輯交換器的下行連接埠。此下行連接埠 (172.16.40.1) 會作為虛擬路由器虛擬機器的預設閘道。虛擬路由器虛擬機器和第 1 層的 A 會透過相同的 NSX-T 邏輯交換器來連線。第 1 層邏輯路由器具有靜態路由 10.10.0.0/16，它會摘要可透過虛擬路由器使用的網路。第 1 層的 A 接著會設定路由通告，以對第 1 層的 B 通告靜態路由。

圖 4-2：第 1 層邏輯路由器靜態路由拓撲



#### 先決條件

確認已設定下行連接埠。請參閱[新增第 1 層邏輯路由器的下行連接埠](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 1 層邏輯路由器。
- 4 按一下**路由 (Routing)**索引標籤，然後從下拉式功能表中選取**靜態路由 (Static Route)**。
- 5 選取**新增 (Add)**。
- 6 以 CIDR 格式輸入網路位址。  
例如，10.10.10.0/16。
- 7 按一下**插入列 (Insert Row)**以新增下一個躍點 IP 位址。  
例如，172.16.40.10。
- 8 按一下**儲存 (Save)**。  
新建立的靜態路由網路位址即會顯示在該列中。
- 9 從第 1 層邏輯路由器中，選取**路由 > 路由通告 (Routing > Route Advertisement)**。

- 10 按一下**編輯 (Edit)**，然後選取**通告靜態路由 (Advertise Static Routes)**。
- 11 按一下**儲存 (Save)**。

靜態路由便會跨越 NSX-T 覆疊進行傳播。

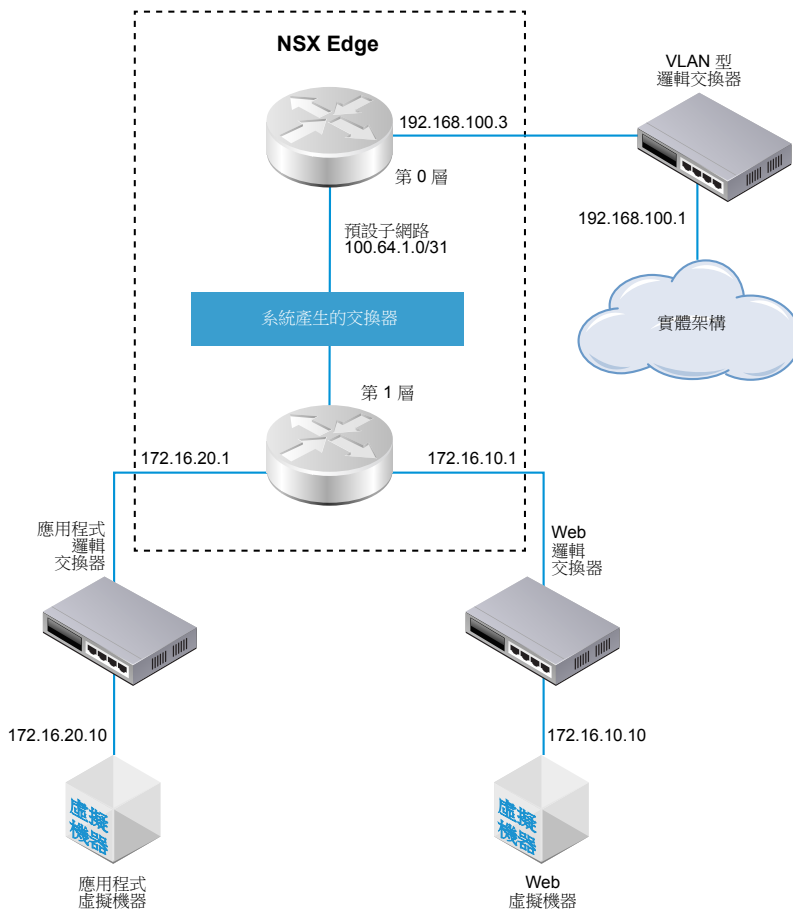
## 設定第 0 層邏輯路由器

NSX-T 邏輯路由器會在虛擬環境中重現從基礎硬體中完全分離的路由功能。第 0 層邏輯路由器會在邏輯和實體網路之間提供開啟與關閉閘道服務。

NSX Edge 叢集可以備份多個第 0 層邏輯路由器。第 0 層路由器支援 BGP 動態路由通訊協定和 ECMP。

當您新增第 0 層邏輯路由器時，請務必對應您要建置的網路拓撲。

圖 5-1: 第 0 層邏輯路由器拓撲





為了方便起見，針對連線至裝載於單一 NSX Edge 節點上的單一第 0 層邏輯路由器，範例拓撲會顯示單一第 1 層邏輯路由器。請記住，這並非建議的拓撲。理想情況下，您應該至少有兩個 NSX Edge 節點以充分利用邏輯路由器設計。

第 1 層邏輯路由器具有各自連結虛擬機器的 Web 邏輯交換器和應用程式邏輯交換器。當您將第 1 層路由器連結至第 0 層路由器時，系統會自動建立第 1 層路由器與第 0 層路由器之間的路由器連結交換器。因此，這個交換器會標記為系統產生。

本章包含以下主題：

- [建立第 0 層邏輯路由器](#)
- [連結第 0 層和第 1 層](#)
- [將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)
- [設定靜態路由](#)
- [BGP 組態選項](#)
- [在第 0 層邏輯路由器上設定 BFD](#)
- [啟用第 0 層邏輯路由器上的路由重新分配](#)
- [瞭解 ECMP 路由](#)
- [建立 IP 首碼清單](#)
- [建立路由對應](#)

## 建立第 0 層邏輯路由器

第 0 層邏輯路由器具有可連線至 NSX-T 第 1 層邏輯路由器的下行連接埠，以及可連線至外部網路的上行連接埠。

### 先決條件

- 確認已安裝至少一個 NSX Edge。請參閱 NSX-T 安裝指南。
- 確認您的 NSX Controller 叢集處於穩定狀態。
- 確認已設定 Edge 叢集。請參閱 NSX-T 安裝指南。
- 自行熟悉第 0 層邏輯路由器的網路拓撲。請參閱第 5 章，設定第 0 層邏輯路由器。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **路由 (Routing)**。
- 3 按一下 **新增**，建立第 0 層邏輯路由器。
- 4 從下拉式功能表中選取 **第 0 層路由器**。
- 5 指派名稱給第 0 層邏輯路由器。
- 6 從下拉式功能表中選取現有的 Edge 叢集，用以支援此 第 0 層邏輯路由器。

**7 (可選) 選取高可用性模式。**

依預設，系統會使用主動-主動式模式。在主動-主動式模式中，流量會在所有成員間進行負載平衡。在主動-待命模式中，所有流量都由選擇的作用中成員處理。如果作用中成員故障，則系統會選擇新成員以成為作用中狀態。

**8 (可選) 按一下**進階**索引標籤，輸入內部-第 0 層傳送子網路的子網路。**

這個子網路負責將第 0 層服務路由器連線至其分散式路由器。如果將此項目保留空白，則會使用預設的 169.0.0.0/28 子網路。

**9 (可選) 按一下**進階**索引標籤，輸入第 0 層-第 1 層傳送子網路的子網路。**

這個子網路負責將第 0 層路由器連線至已連線至此第 0 層路由器的任何第 1 層路由器。如果將此項目保留空白，則系統指派第 0 層至第 1 層連線的預設位址空間為 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。

**10 按一下**儲存**。**

新的第 0 層邏輯路由器會顯示為連結。

**11 (可選) 按一下第 0 層邏輯路由器連結即可檢閱摘要。****後續步驟**

將第 1 層邏輯路由器連結至此第 0 層邏輯路由器。

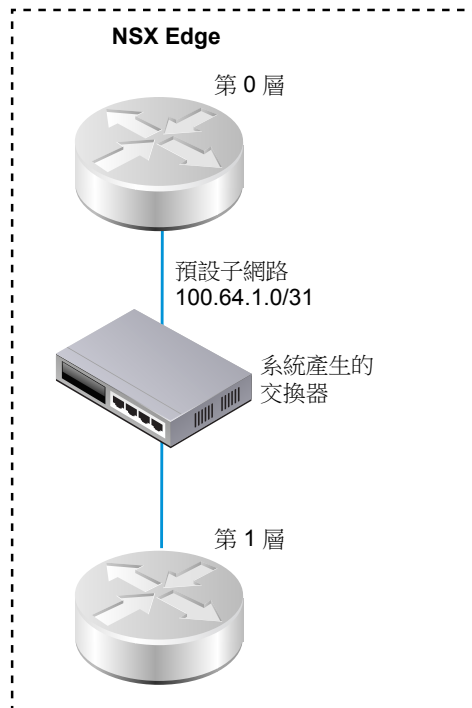
設定第 0 層邏輯路由器，將其連線至 VLAN 邏輯交換器以建立對外部網路的上行連接埠。請參閱[將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。

## 連結第 0 層和第 1 層

您可以連結第 0 層邏輯路由器和第 1 層邏輯路由器，以便第 1 層邏輯路由器取得北向和東向-西向網路連線能力。

當您將第 1 層邏輯路由器連結至第 0 層邏輯路由器時，系統會建立兩個路由器之間的路由器連結交換器。此交換器會在拓撲中標記為系統產生。針對這些第 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。或者，您也可以在第 0 層的**摘要 > 進階**組態中設定位址空間。

下圖顯示範例拓撲。



#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 1 層邏輯路由器。
- 4 從**摘要**索引標籤中，按一下**編輯**。
- 5 從下拉式功能表中選取第 0 層邏輯路由器。
- 6 (可選) 從下拉式功能表中選取 Edge 叢集。

如果路由器要用於服務，例如 NAT，則第 1 層路由器需要由 Edge 裝置提供支援。如果您並未選取 Edge 叢集，則第 1 層路由器無法執行 NAT。

- 7 指定成員與偏好的成員。

如果您選取 Edge 叢集並將成員與偏好的成員欄位保留空白，則 NSX-T 會從指定的叢集為您設定備份 Edge 裝置。

- 8 按一下**儲存**。
- 9 按一下第 1 層路由器的**組態**索引標籤以確認建立新的點對點連結連接埠 IP 位址。  
例如，連結連接埠的 IP 位址可以是 100.64.1.1/31。
- 10 從導覽面板中選取第 0 層邏輯路由器。
- 11 按一下第 0 層路由器的**組態**索引標籤以確認建立新的點對點連結連接埠 IP 位址。

例如，連結連接埠的 IP 位址可以是 100.64.1.1/31。

## 後續步驟

確認第 0 層路由器學習第 1 層路由器所通告的路由器。

## 確認第 0 層路由器已從第 1 層路由器學習路由

當第 1 層邏輯路由器向第 0 層邏輯路由器通告路由時，路由會在第 0 層路由器的路由表中列出為 NSX-T 靜態路由。

### 程序

- 1 在 NSX Edge 上執行 `get logical-routers` 命令，以尋找第 0 層服務路由器的 VRF 號碼。

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 2 執行 `vrf <number>` 命令，以進入第 0 層服務路由器內容。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 在第 0 層服務路由器上，執行 `get route` 命令並確定路由表中顯示預期的路由。

請注意，NSX-T 靜態路由會由第 0 層路由器學習，因為第 1 層路由器是通告路由。

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

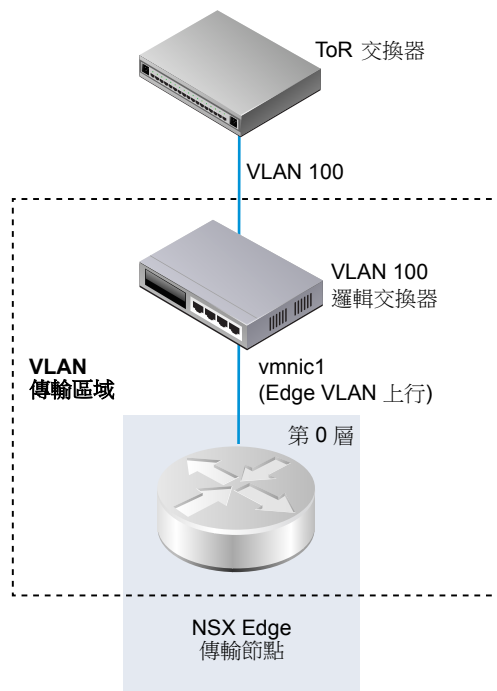
Total number of routes: 7

b	10.10.10.0/24	[20/0]	via 192.168.100.254
rl	100.91.176.0/31	[0/0]	via 169.254.0.1
c	169.254.0.0/28	[0/0]	via 169.254.0.2
ns	172.16.10.0/24 [3/3]	via 169.254.0.1	ns 172.16.20.0/24 [3/3] via 169.254.0.1
c	192.168.100.0/24	[0/0]	via 192.168.100.2

## 將第 0 層邏輯路由器連線至 VLAN 邏輯交換器

若要建立 Edge 上行，請將第 0 層路由器連線至 VLAN 交換器。

下列簡單拓撲會顯示 VLAN 傳輸區域內部的 VLAN 邏輯交換器。VLAN 邏輯交換器具有 VLAN 識別碼，符合 TOR 連接埠上適用於 Edge VLAN 上行的 VLAN 識別碼。



### 先決條件

建立 VLAN 邏輯交換器。請參閱為 [NSX Edge 上行建立 VLAN 邏輯交換器](#)。

建立第 0 層路由器。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 從 **組態 (Configuration)** 索引標籤新增邏輯路由器連接埠。

- 5 輸入連接埠的名稱，例如上行。
- 6 選取上行 (Uplink) 類型。
- 7 選取 Edge 傳輸節點。
- 8 選取 VLAN 邏輯交換器。
- 9 以 CIDR 格式輸入在與 TOR 交換器上已連線連接埠之相同子網路中的 IP 位址。

例如：

New Router Port
✕

**Name: \***

**Description:**

**Type:** ☒ Uplink ☐ Downlink

**Transport Node: \*** TN-edgenode-02a ▼

**Logical Switch:** LS.VLAN.240 ✕ ▼

OR Create a New Switch

**Logical Switch Port:** ☒ Attach to new switch port

**Switch Port Name:**

☐ Attach to existing switch port

**IP Address/mask: \***

Save
Cancel

系統會新增第 0 層路由器的新上行連接埠。

#### 後續步驟

設定 BGP 或靜態路由。

## 確認第 0 層邏輯路由器和 TOR 連線

針對來自第 0 層路由器在上行運作的路由，則必須備妥與 Top-of-Rack 裝置的連線。

## 先決條件

- 確認第 0 層邏輯路由器已連線至 VLAN 邏輯交換器。請參閱[將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。

## 程序

- 1 登入 NSX Manager CLI。
- 2 在 NSX Edge 上執行 `get logical-routers` 命令，以尋找第 0 層服務路由器的 VRF 號碼。

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 執行 `vrf <number>` 命令，以進入第 0 層服務路由器內容。

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 在第 0 層服務路由器上執行 `get route` 命令，以確定預期的路由會顯示在路由表中。  
請留意 TOR 的路由會顯示為已連線 (c)。

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7
```

```

b    10.10.10.0/24      [20/0]      via 192.168.100.254
rl   100.91.176.0/31    [0/0]      via 169.254.0.1
c    169.254.0.0/28     [0/0]      via 169.254.0.2
ns   172.16.10.0/24     [3/3]      via 169.254.0.1
ns   172.16.20.0/24     [3/3]      via 169.254.0.1
c    192.168.100.0/24  [0/0]      via 192.168.100.2

```

## 5 探測 TOR。

```

nsx-edge1(tier0_sr)> ping    192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms

```

此時系統會在第 0 層邏輯路由器與實體路由器之間傳送封包以確認連線。

### 後續步驟

您可以根據網路需求來設定靜態路由或 BGP。請參閱[設定靜態路由](#)或[在第 0 層邏輯路由器上設定 BGP](#)。

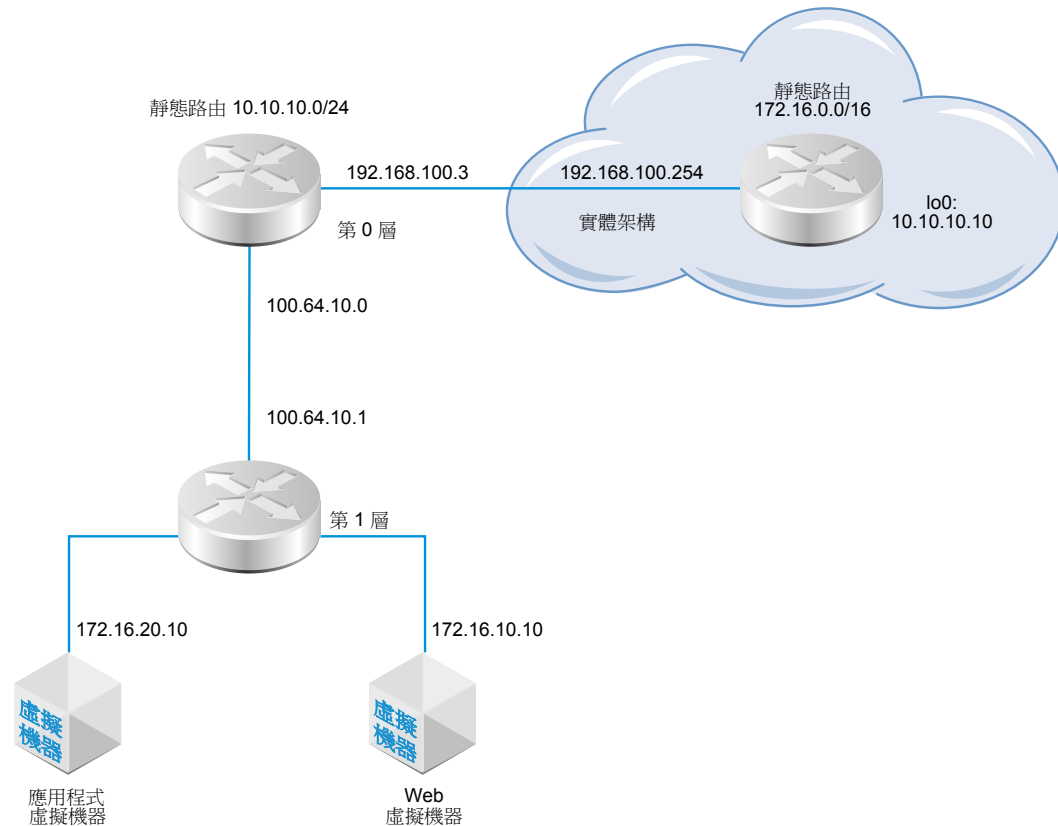
## 設定靜態路由

您可以設定第 0 層路由器到外部網路的靜態路由。在設定靜態路由之後，不需要通告從第 0 層到第 1 層的路由，因為第 1 層路由器會自動具有通往其已連線第 0 層路由器的靜態預設路由。

靜態路由拓撲會顯示第 0 層邏輯路由器以及實體架構中通往 10.10.10.0/24 首碼的靜態路由。為進行測試，系統會在外部路由器回送介面設定 10.10.10.10/32 位址。外部路由器具有通往 172.16.0.0/16 首碼的靜態路由，可用來連線至應用程式及 Web 虛擬機器。



圖 5-2：靜態路由拓撲



#### 先決條件

- 確認實體路由器和第 0 層邏輯路由器已連線。請參閱[確認第 0 層邏輯路由器和 TOR 連線](#)。
- 確認已設定第 1 層路由器可通告連線的路由。請參閱[建立第 1 層邏輯路由器](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**路由 (Routing)**索引標籤，然後從下拉式功能表中選取**靜態路由 (Static Route)**。
- 5 選取**新增 (Add)**。
- 6 以 CIDR 格式輸入網路位址。  
例如，10.10.10.0/24。
- 7 按一下**插入列 (Insert Row)**以新增下一個躍點 IP 位址。  
例如，192.168.100.254。
- 8 按一下**儲存 (Save)**。

新建立的靜態路由網路位址即會顯示在該列中。

## 後續步驟

請確認已正確設定靜態路由。請參閱[確認靜態路由](#)。

## 確認靜態路由

使用 CLI 確認靜態路由已連線。您也必須確認外部路由器可以對內部虛擬機器執行 Ping 偵測，且內部虛擬機器也能對外部路由器執行 Ping 偵測。

## 先決條件

確認已設定靜態路由。請參閱[設定靜態路由](#)。

## 程序

- 1 登入 NSX Manager CLI。

## 2 確認靜態路由。

### a 取得服務路由器 UUID 資訊。

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

### b 從輸出中找到 UUID 資訊。

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

### c 確認靜態路由正常運作。

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31     [0/0]      via 169.0.0.1
ns   172.16.10.0/24    [3/3]      via 169.0.0.1
ns   172.16.20.0/24    [3/3]      via 169.0.0.1
```

### 3 從外部路由器對內部虛擬機器執行 Ping 偵測，以確認可透過 NSX-T 覆疊進行連線。

#### a 連線到外部路由器。

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

#### b 測試網路連線。

```
tracert 172.16.10.10
```

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.64.1.1 (100.64.1.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

### 4 從虛擬機器對外部 IP 位址執行 Ping 偵測。

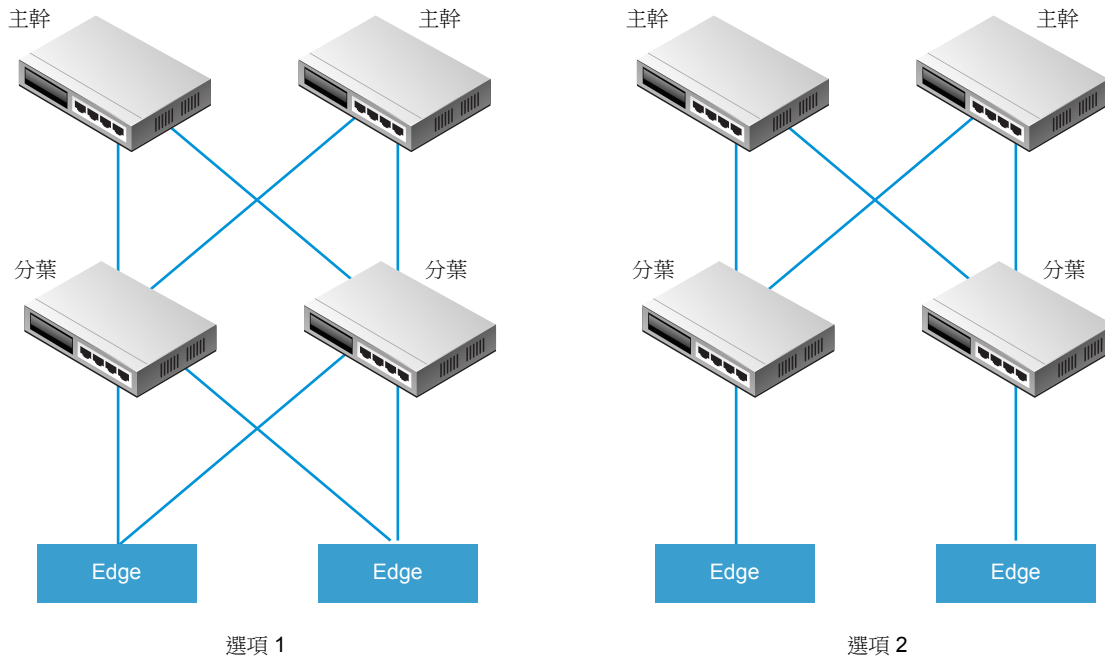
```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

## BGP 組態選項

若要充分利用第 0 層邏輯路由器，拓撲必須設定備援和對稱，且 BGP 介於第 0 層路由器和外部 Top-of-Rack 對等之間。這個設計有助於在連結及節點故障的情況下確定連線能力。

有兩種組態模式：主動-主動與主動-待命。下圖顯示對稱組態的兩個選項。每個拓撲中會顯示兩個 NSX Edge 節點。在主動-主動組態的情況下，當您建立第 0 層上行連接埠時，可以將每個上行連接埠與最多八個 NSX Edge 傳輸節點建立關聯。每個 NSX Edge 節點可以有兩個上行。



針對選項 1，當設定實體分葉節點路由器時，它們應與 NSX Edge 具有 BGP 鄰近關係。路由重新分配應包含與等於所有 BGP 芳鄰之 BGP 度量相同的網路首碼。在第 0 層邏輯路由器組態中，所有的分葉節點路由器應設定為 BGP 芳鄰。

當您在設定第 0 層路由器的 BGP 芳鄰時，如果您未指定本機位址 (來源 IP 位址)，則 BGP 芳鄰組態會傳送至所有與第 0 層邏輯路由器上行相關聯的 NSX Edge 節點。如果您設定本機位址，則組態會前往 NSX Edge 節點，而上行會擁有該 IP 位址。

在選項 1 的情況下，如果上行不在 NSX Edge 節點的相同子網路上，則省略本機位址很合理。如果 NSX Edge 節點上的上行位於不同的子網路上，則應在第 0 層路由器的 BGP 芳鄰組態中指定本機位址，以防止組態前往所有相關聯的 NSX Edge 節點。

針對選項 2，確定第 0 層邏輯路由器組態包含第 0 層服務路由器的本機 IP 位址。分葉節點路由器僅會使用其作為 BGP 芳鄰所直接連線的 NSX Edge 來進行設定。

## 在第 0 層邏輯路由器上設定 BGP

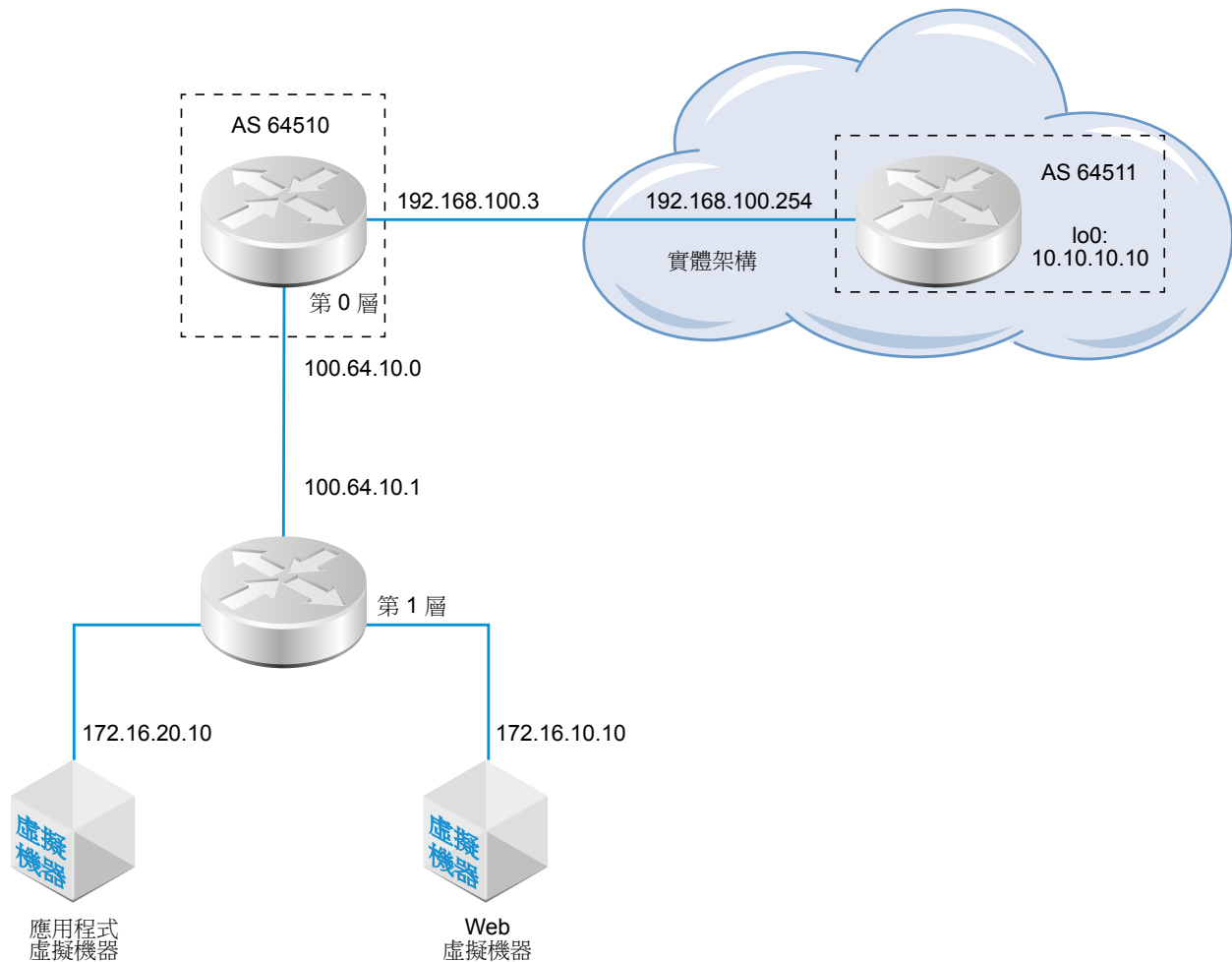
如果要啟用您虛擬機器與外部環境之間的存取，您可以設定第 0 層邏輯路由器與實體基礎結構中之路由器之間的外部 BGP (eBGP) 連線。

當您在設定 BGP 時，必須設定第 0 層邏輯路由器的本機自發系統 (AS) 數目。例如，下列拓撲顯示本機 AS 數目為 64510。您還必須設定實體路由器的遠端 AS 數目。在此範例中，遠端 AS 數目為 64511。遠端芳鄰 IP 位址為 192.168.100.254。芳鄰必須與第 0 層邏輯路由器上的上行位於相同 IP 子網路中。不支援 BGP 多重躍點。

為進行測試，系統會在外部路由器回送介面設定 10.10.10.10/32 位址。

**備註** 系統會從第 0 層邏輯路由器的上行所設定的 IP 位址中，自動選取用於在 Edge 節點上形成 BGP 工作階段的路由器識別碼。當路由器識別碼變更時，Edge 節點上的 BGP 工作階段可能會翻動。當針對路由器識別碼自動選取的 IP 位址遭到刪除，或此 IP 指派所在的邏輯路由器連接埠遭到刪除時，可能會發生此情況。

圖 5-3: BGP 連線拓撲



#### 先決條件

- 確認已設定第 1 層路由器可通告連線的路由。請參閱[在第 1 層邏輯路由器上設定路由通告](#)。這並非 BGP 組態的嚴格先決條件，但如果您有兩層拓撲並打算將第 1 層網路重新分配至 BGP，則此步驟為必要。
- 確認已設定第 0 層路由器。請參閱[建立第 0 層邏輯路由器](#)。
- 確定第 0 層邏輯路由器已學習來自第 1 層邏輯路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

**程序**

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**路由 (Routing)**索引標籤，然後從下拉式功能表中選取 **BGP**。
- 5 按一下**編輯 (Edit)**以設定本機 AS 數目然後按一下**儲存 (Save)**。  
例如，64510。
- 6 按一下**狀態 (Status)**切換按鈕以啟用 BGP。  
[狀態] 按鈕必須顯示為 [已啟用]。
- 7 (可選) 設定路由彙總、啟用正常重新啟動並啟用 ECMP。  
僅在與第 0 層路由器相關聯的 Edge 叢集只有一個 Edge 節點時才支援正常重新啟動。
- 8 按一下**儲存 (Save)**。
- 9 按一下 [芳鄰] 區段下的**新增 (Add)**以新增 BGP 芳鄰。
- 10 請輸入芳鄰 IP 位址。  
例如，192.168.100.254。
- 11 (可選) 從下拉式功能表中選取本機位址。
- 12 請輸入遠端 AS 數目。  
例如，64511。
- 13 (可選) 設定計時器 (保持連線時間及等候時間) 及密碼。
- 14 (可選) 新增位址家族並設定路由篩選和路由對應。

**後續步驟**

測試 BGP 是否正常運作。請參閱[確認來自第 0 層服務路由器的 BGP 連線](#)。

**確認來自第 0 層服務路由器的 BGP 連線**

從第 0 層服務路由器中使用 CLI 來確認 BGP 已連線通往芳鄰。

**先決條件**

確認已設定 BGP。請參閱[在第 0 層邏輯路由器上設定 BGP](#)。

**程序**

- 1 登入 NSX Manager CLI。

- 2 在 NSX Edge 上執行 `get logical-routers` 命令，以尋找第 0 層服務路由器的 VRF 號碼。

```

nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER

```

- 3 執行 `vrf <number>` 命令，以進入第 0 層服務路由器內容。

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 4 確認 BGP 狀態為 `Established, up`。

`get bgp neighbor`

```

BGP neighbor: 192.168.100.254   Remote AS: 64511
BGP state: Established, up
Hold Time: 180s   Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
    Route Refresh: 0 received, 0 sent

```



```
Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044
```

#### 後續步驟

檢查來自外部路由器的 BGP 連線。請參閱[確認南北向連線和路由重新分配](#)。

## 在第 0 層邏輯路由器上設定 BFD

BFD (雙向轉送偵測) 是可偵測轉送路徑故障的通訊協定。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**路由索引**標籤，然後從下拉式功能表中選取 **BFD**。
- 5 按一下**編輯**以設定 BFD。
- 6 按一下**狀態**切換按鈕以啟用 BFD。

您可以選擇性地變更全域 BFD 屬性**接收時間間隔**、**傳輸時間間隔**及**宣告為無作用時間間隔**。

- 7 (可選) 按一下 BFD 對等下的**新增**，讓「靜態路由下一個躍點」新增 BFD 對等項。

指定對等 IP 位址並將管理狀態設為**已啟用**。或者，您也可以覆寫全域 BFD 屬性**接收時間間隔**、**傳輸時間間隔**及**宣告為無作用時間間隔**。

## 啟用第 0 層邏輯路由器上的路由重新分配

當您啟用路由重新分配時，第 0 層邏輯路由器會開始與其北向路由器共用指定的路由。

#### 先決條件

- 確認第 0 層和第 1 層邏輯路由器已連線，以便能夠通告第 1 層邏輯路由器網路，而在第 0 層邏輯路由器上重新分配這些網路。請參閱[連結第 0 層和第 1 層](#)。
- 如果您想要從路由重新分配中篩選出特定的 IP 位址，請確認您已設定路由對應。請參閱[建立路由對應](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**路由索引**標籤，然後從下拉式功能表中選取**路由重新分配**。

## 5 按一下**新增**以完成路由重新分配準則。

選項	說明
名稱與說明	指派名稱給路由重新分配。您可以選擇性地提供說明。 範例名稱為 <b>advertise-to-bgp-neighbor</b> 。
來源	選取您要重新分配的來源路由核取方塊。 靜態 - 第 0 層靜態路由。 NSX 已連線 - 第 1 層已連線路由。 NSX 靜態 - 第 1 層靜態路由。這些靜態路由會自動建立。 第 0 層 NAT - 如果已在第 0 層邏輯路由器上設定 NAT，則系統會產生路由。 第 1 層 NAT - 如果已在第 1 層邏輯路由器上設定 NAT，則系統會產生路由。
路由對應	(選用) 指派路由對應，以便從路由重新分配中篩選出一系列 IP 位址。

## 6 按一下**儲存**。

## 7 按一下**狀態**切換按鈕以啟用路由重新分配。

[狀態] 按鈕會顯示為 [啟用]。

## 確認南北向連線和路由重新分配

使用 CLI 來確認已知的 BGP 路由。您也可以從可連接已連線 NSX-T 之虛擬機器的外部路由器來進行檢查。

### 先決條件

- 確認已設定 BGP。請參閱[在第 0 層邏輯路由器上設定 BGP](#)。
- 確認 NSX-T 靜態路由已針對重新分配進行設定。請參閱[啟用第 0 層邏輯路由器上的路由重新分配](#)。

### 程序

- 1 登入 NSX Manager CLI。
- 2 檢視從外部 BGP 芳鄰所知的路由。

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

b    10.10.10.0/24      [20/0]      via 192.168.100.254
```

### 3 從外部路由器檢查 BGP 路由為已知，並且可透過 NSX-T 覆疊連接虛擬機器。

#### a 列出 BGP 路由。

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

#### b 從外部路由器對已連線 NSX-T 的虛擬機器執行 Ping 偵測。

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

#### c 檢查經過 NSX-T 覆疊的路徑。

```
traceroute 172.16.10.10
```

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  192.168.100.3 (192.168.100.3)  0.640 ms  0.575 ms  0.696 ms
 2  100.91.176.1 (100.91.176.1)  0.656 ms  0.604 ms  0.578 ms
 3  172.16.10.10 (172.16.10.10)  3.397 ms  3.703 ms  3.790 ms
```

### 4 從內部虛擬機器對外部 IP 位址執行 Ping 偵測。

```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

#### 後續步驟

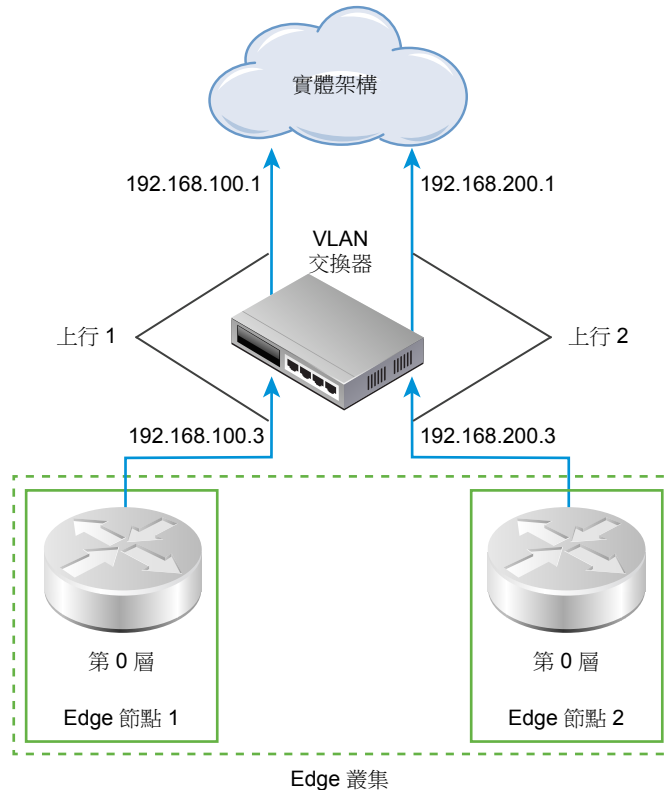
設定其他路由功能，例如 ECMP。

## 瞭解 ECMP 路由

相同成本多路徑 (ECMP) 路由通訊協定可透過對第 0 層邏輯路由器增加上行連接埠，並在 Edge 叢集中為每個 Edge 節點進行設定，藉此提高北向和南向通訊頻寬。ECMP 路由路徑可用於負載平衡流量並為失敗的路徑提供 Fault Tolerance。

針對連結至邏輯交換器的虛擬機器到具現化第 0 層邏輯路由器的 Edge 節點之間，系統會自動建立 ECMP 路徑。最多支援八個 ECMP 路徑。

圖 5-4：ECMP 路由拓撲



例如，此拓撲顯示 Edge 叢集中的兩個第 0 層邏輯路由器。每個第 0 層邏輯路由器皆位於 Edge 節點中，且這些節點屬於叢集的一部分。上行連接埠 192.168.100.3 和 198.168.200.3 會定義傳輸節點如何連線至邏輯交換器，以取得實體網路的存取權。啟用 ECMP 路由路徑時，這些路徑會將連結至邏輯交換器的虛擬機器連線至 Edge 叢集中的兩個 Edge 節點。多重 ECMP 路由路徑可以提高網路輸送量與彈性。

## 新增第二個 Edge 節點的上行連接埠

在啟用 ECMP 之前，您必須設定上行連接埠以將第 0 層邏輯路由器連線至 VLAN 邏輯交換器。

### 先決條件

- 確認已設定傳輸區域和兩個傳輸節點。請參閱 [NSX-T 安裝指南](#)。
- 確認已設定兩個 Edge 節點和 Edge 叢集。請參閱 [NSX-T 安裝指南](#)。
- 確認上行的 VLAN 邏輯交換器是可用的。請參閱 [為 NSX Edge 上行建立 VLAN 邏輯交換器](#)。

- 確認已設定第 0 層邏輯路由器。請參閱[建立第 0 層邏輯路由器](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**組態 (Configuration)**索引標籤以新增路由器連接埠。
- 5 按一下**新增 (Add)**。
- 6 完成路由器連接埠詳細資料。

選項	說明
名稱	為路由器連接埠指派名稱。
說明	提供顯示適用於 ECMP 組態之連接埠的額外說明。
類型	接受預設類型 <b>上行 (Uplink)</b> 。
傳輸節點	從下拉式功能表中指派主機傳輸節點。
邏輯交換器	從下拉式功能表中指派 VLAN 邏輯交換器。
邏輯交換器連接埠	指派新的交換器連接埠名稱。 您也可以使用現有的交換器連接埠。
IP 位址/遮罩	輸入在與 ToR 交換器上已連線連接埠之相同子網路中的 IP 位址。

抽樣檢查路由器連接埠組態。

The screenshot shows the 'New Router Port' configuration dialog. The 'Name' field is 'uplink2'. The 'Type' is 'Uplink'. The 'Transport Node' is 'edge-node-2'. The 'Logical Switch' is 'VLAN-logical-switch-2'. Under 'Logical Switch Port', 'Attach to new switch port' is selected, and the 'Switch Port Name' is 'uplink2-port'. The 'IP Address/mask' is '192.168.200.1/24'. There are 'Save' and 'Cancel' buttons at the bottom.

- 7 按一下**儲存 (Save)**。

系統會將新的上行連接埠新增至第 0 層路由器和 VLAN 邏輯交換器。在兩個 Edge 節點上設定第 0 層邏輯路由器。

#### 後續步驟

建立第二個芳鄰的 BGP 連線並啟用 ECMP 路由。請參閱[新增第二個 BGP 芳鄰並啟用 ECMP 路由](#)。

## 新增第二個 BGP 芳鄰並啟用 ECMP 路由

在啟用 ECMP 路由之前，您必須新增 BGP 芳鄰並使用最近新增的上行資訊來進行設定。

#### 先決條件

確認第二個 Edge 節點已設定上行連接埠。請參閱[新增第二個 Edge 節點的上行連接埠](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**路由 (Routing)**索引標籤，然後從下拉式功能表中選取 **BGP**。
- 5 按一下 [芳鄰] 區段下的**新增 (Add)**以新增 BGP 芳鄰。
- 6 請輸入芳鄰 IP 位址。  
例如，192.168.200.254。
- 7 從下拉式功能表中選取本機位址。  
例如，uplink2 192.168.200.1。
- 8 請輸入遠端 AS 數目。  
例如，64511。
- 9 按一下**儲存 (Save)**。  
隨即顯示新增的 BGP 芳鄰。
- 10 按一下 [BGP 組態] 區段旁的**編輯 (Edit)**。
- 11 按一下 **ECMP** 切換按鈕以啟用 ECMP。  
[狀態] 按鈕必須顯示為 [已啟用]。
- 12 按一下**儲存 (Save)**。

多個 ECMP 路由路徑會將連結至邏輯交換器的虛擬機器連線至 Edge 叢集中的兩個 Edge 節點。

#### 後續步驟

測試 ECMP 路由連線是否正常運作。請參閱[確認 ECMP 路由連線](#)。

## 確認 ECMP 路由連線

使用 CLI 確認已建立連往芳鄰的 ECMP 路由連線。

### 先決條件

確認已設定 ECMP 路由。請參閱[新增第二個 Edge 節點的上行連接埠與新增第二個 BGP 芳鄰並啟用 ECMP 路由](#)。

### 程序

- 1 登入 NSX Manager CLI。
- 2 取得分散式路由器 UUID 資訊。

```
get logical-routers
```

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL

Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0

Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER

Logical Router
UUID          : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf           : 6
type          : DISTRIBUTED_ROUTER
```

- 3 從輸出中找到 UUID 資訊。

```
Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER
```

- 4 輸入第 0 層分散式路由器的 VRF。

```
vrf 5
```

- 5 確認第 0 層分散式路由器已連線至 Edge 節點。

```
get forwarding
```

例如，edge-node-1 和 edge-node-2。

- 6 輸入 **exit** 以離開 **vrf** 內容。
- 7 開啟第 0 層邏輯路由器的作用中控制器。
- 8 確認控制器節點上的第 0 層分散式路由器已連線。

```
get logical-router <UUID> route
```

UUID 的路由類型應該會顯示為 **NSX\_CONNECTED**。

- 9 在兩個 **Edge** 節點上啟動 **SSH** 工作階段。
- 10 啟動工作階段以擷取封包。

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```

- 11 導覽至控制中心並按兩下 **httpdata11.bat** 和 **httpdata12.bat** 指令碼。

如此會傳送大量的 **HTTP** 要求至兩個 **Web** 虛擬機器，且您會看到流量使用 **Edge** 節點雜湊至兩個路徑，這表示 **ECMP** 正常運作。

- 12 停止擷取工作階段。

```
del capture session 0
```

- 13 移除 **bat** 指令碼。

## 建立 IP 首碼清單

**IP** 首碼清單包含已獲派路由通告存取權限的單一或多個 **IP** 位址。系統會依順序處理此清單中的 **IP** 位址。**IP** 首碼清單可透過 **BGP** 芳鄰篩選器或具有進出方向的路由對應來參考。

例如，您可新增 **IP** 位址 **192.168.100.3/27** 至 **IP** 首碼清單，並拒絕路由重新分配至北向路由器。這表示除了 **192.168.100.3/24** **IP** 位址以外，其他所有 **IP** 位址都將共用路由器。

您也可以將 **IP** 位址前面加上 **less-than-or-equal-to (le)** 和 **greater-than-or-equal-to (ge)** 修飾詞，以授與或限制路由重新分配。例如，**192.168.100.3/27 ge 24 le 30** 修飾詞符合長度大於或等於 24 位元且小於或等於 30 位元的子網路遮罩。

---

**備註** 路由的預設動作為**拒絕**。建立可拒絕或允許特定路由的首碼清單時，如果您想要允許其他所有的路由，請務必建立網路位址空白且具備**允許**動作的 **IP** 首碼。

---

### 先決條件

確認您已設定第 0 層邏輯路由器。請參閱[建立第 0 層邏輯路由器](#)。

### 程序

- 1 從瀏覽器登入 **NSX Manager**，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。



- 4 按一下**路由索引**標籤，並從下拉式功能表選取 **IP 首碼清單**。
- 5 選取**新增**。
- 6 指派名稱給 IP 首碼清單。
- 7 按一下**插入資料列**，新增 CIDR 格式的網路位址。  
例如，192.168.100.3/27。
- 8 從下拉式功能表中選取**拒絕或允許**。  
請依照自己的需求，授與或拒絕每個 IP 位址進行通告。
- 9 (可選) 以 **le** 或 **ge** 修飾詞設定 IP 位址數字的範圍。  
例如，可將 **le** 修飾詞設定為 30 並將 **ge** 修飾詞設定為 24。
- 10 按一下**儲存**。

新建立的 IP 首碼清單即會顯示在列中。

## 建立路由對應

路由對應包含 IP 首碼清單序列、BGP 路徑屬性以及關聯動作。路由器會掃描此序列以尋找符合的 IP 位址。如果找到相符項目，則路由器會執行動作並停止掃描。

路由對應可供 BGP 芳鄰層級和路由重新分配參考。在路由對應中參考 IP 首碼清單並套用允許或拒絕的路由對應動作時，路由對應序列中指定的動作會覆寫 IP 首碼清單中的指定規格。

### 先決條件

確認已設定 IP 首碼清單。請參閱[建立 IP 首碼清單](#)。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取第 0 層邏輯路由器。
- 4 選取**路由 (Routing) > 路由對應 (Route Maps)**。
- 5 按一下**新增 (Add)**。
- 6 輸入路由對應的名稱與選用說明。
- 7 按一下**新增 (Add)**，在路由對應中新增項目。
- 8 選取一或多個 IP 首碼清單。
- 9 (可選) 設定 BGP 屬性。

BGP 屬性	說明
AS-path Prepend	在路徑前面加上一或多個 AS (自發系統) 編號，加長路徑並降低其偏好順序。
MED	Multi-Exit Discriminator 會指定 AS 的偏好路徑給外部對等。

BGP 屬性	說明
Weight	設定權重以影響路徑選擇。範圍為 0 - 65535。
Community	<p>以 aa:nn 格式指定社群，例如，300:500。或使用下拉式功能表選取下列其中一項：</p> <ul style="list-style-type: none"> <li>■ NO_EXPORT_SUBCONFED - 不要向 EBGp 對等通告。</li> <li>■ NO_ADVERTISE - 不要向任何對等通告。</li> <li>■ NO_EXPORT - 不要向 BGP 聯盟外部通告</li> </ul>

**10** 在 [動作] 資料行中，選取**允許 (Permit)**或**拒絕 (Deny)**。

您可以允許或拒絕 IP 首碼清單中的 IP 位址通告其位址。

**11** 按一下**儲存 (Save)**。

## 網路位址轉譯

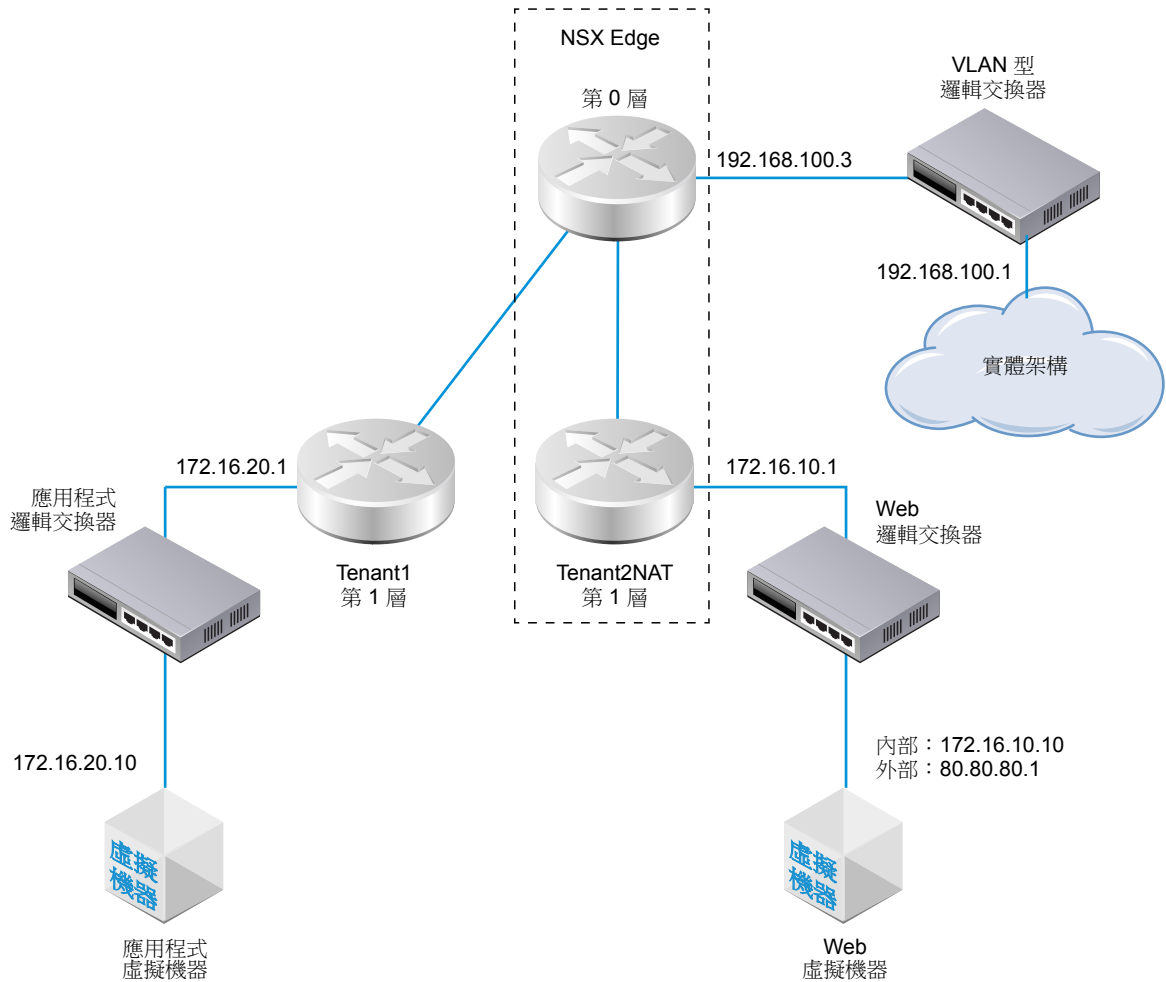
NSX-T 中的網路位址轉譯 (NAT) 可在第 0 層和第 1 層邏輯路由器中設定。

例如，下圖顯示兩個第 1 層邏輯路由器，並在 Tenant2NAT 上設定 NAT。Web 虛擬機器單純設定為使用 172.16.10.10 作為其 IP 位址，並使用 172.16.10.1 作為其預設閘道。

NAT 會在 Tenant2NAT 邏輯路由器對第 0 層邏輯路由器的連線上行強制執行。

為了啟用 NAT 組態，Tenant2NAT 必須在 NSX Edge 叢集上具備服務元件。因此，Tenant2NAT 顯示在 NSX Edge 內部。相較之下，Tenant1 可以位於 NSX Edge 外部，因為它並未使用 Edge 服務。

圖 6-1: NAT 拓撲



本章包含以下主題：

- 第 1 層 NAT
- 第 0 層 NAT

## 第 1 層 NAT

第 1 層邏輯路由器支援來源 NAT 和目的地 NAT。

### 在第 1 層路由器上設定來源 NAT

來源 NAT (SNAT) 會變更封包之 IP 標頭中的來源位址。它也會變更 TCP/UDP 標頭中的來源連接埠。一般使用方式是針對要離開您網路的封包將私人 (RFC1918) 位址/連接埠變更為公用位址/連接埠。

在此範例中，從 Web 虛擬機器擷取封包時，Tenant2NAT 第 1 層路由器會將封包的來源連接埠從 172.16.10.10 變更為 80.80.80.1。具備公開來源位址可以啟用私人網路外部的目的地，以便路由回原始來源。

## 先決條件

- 第 0 層路由器必須具有一個連線至以 VLAN 為基礎之邏輯交換器的上行。請參閱[將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。
- 第 0 層路由器必須將路由 (靜態或 BGP) 和路由重新分配設定在其連往實體架構的上行。請參閱[設定靜態路由](#)、[在第 0 層邏輯路由器上設定 BGP](#) 和 [啟用第 0 層邏輯路由器上的路由重新分配](#)。
- 第 1 層路由器必須各自設定連往第 0 層路由器的上行。Tenant2NAT 必須受 Edge 叢集支援。請參閱[連結第 0 層和第 1 層](#)。
- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱[新增第 1 層邏輯路由器的下行連接埠與在第 1 層邏輯路由器上設定路由通告](#)。
- 虛擬機器必須連結至正確的邏輯交換器。

## 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **路由 (Routing)**。
- 3 按一下要在其上設定 NAT 的第 1 層邏輯路由器。
- 4 在 NAT 下，按一下 **新增 (Add)**。
- 5 針對 [動作] 選取 [SNAT]。
- 6 選取通訊協定類型。  
依預設會選取**任何通訊協定 (Any Protocol)**。
- 7 在 [來源 IP] 位址中輸入虛擬機器的內部 IP 位址。  
如果您將來源 IP 保留空白，則系統會轉譯路由器下行連接埠上的所有來源。在此範例中，來源 IP 為 172.16.10.10。
- 8 針對 [已轉譯的 IP] 位址，輸入虛擬機器的外部 IP 位址。  
請注意，不需要在虛擬機器上設定外部/已轉譯的 IP 位址。僅 NAT 路由器需要知道已轉譯的 IP 位址。  
在此範例中，已轉譯的 IP 位址為 80.80.80.1。
- 9 針對 [目的地 IP] 位址，您可以保留空白或輸入 IP 位址。  
如果您將 [目的地 IP] 保留空白，則 NAT 會套用至本機子網路外部的所有目的地。
- 10 啟用規則。
- 11 (可選) 啟用記錄。

新規則會在 NAT 下方列出。例如：

Tenant2NAT

概視組態路由服務

NAT | 重新整理

未收集任何統計資料

+ 新增 編輯 刪除

識別碼	動作	相符					已轉譯		套用至	統計資料
		通訊協定	來源 IP	來源連接埠	目的地 IP	目的地連接埠	IP	連接埠		
優先順序: 1024										
1036	SNAT	任何	172.16.10.10	任何	任何	任何	80.80.80.1	任何		

### 後續步驟

設定第 1 層路由器以通告 NAT 路由器。

若要從第 0 層路由器對實體架構通告 NAT 路由上游，請設定第 0 層路由器以通告第 1 層 NAT 路由。

## 在第 1 層路由器上設定目的地 NAT

目的地 NAT 會變更封包之 IP 標頭中的目的地位址。它也可以變更 TCP/UDP 標頭中的目的地連接埠。其一般用法是將目的地為公用位址/連接埠的傳入封包，重新導向至您網路內部的私人 IP 位址/連接埠。

在此範例中，封包是接收自應用程式虛擬機器，所以 Tenant2NAT 第 1 層路由器會將封包的目的地連接埠從 172.16.10.10 變更為 80.80.80.1。擁有公用目的地位址可讓私人網路內部的目的地從私人網路外部進行連線。

### 先決條件

- 第 0 層路由器必須具有一個連線至以 VLAN 為基礎之邏輯交換器的上行。請參閱[將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。
- 第 0 層路由器必須將路由 (靜態或 BGP) 和路由重新分配設定在其連往實體架構的上行。請參閱[設定靜態路由](#)、[在第 0 層邏輯路由器上設定 BGP](#) 和 [啟用第 0 層邏輯路由器上的路由重新分配](#)。
- 第 1 層路由器必須各自設定連往第 0 層路由器的上行。Tenant2NAT 必須受 Edge 叢集支援。請參閱[連結第 0 層和第 1 層](#)。
- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱[新增第 1 層邏輯路由器的下行連接埠與在第 1 層邏輯路由器上設定路由通告](#)。
- 虛擬機器必須連結至正確的邏輯交換器。

### 程序

- 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 選取 **路由 (Routing)**。
- 按一下要在其上設定 NAT 的第 1 層邏輯路由器。
- 在 NAT 下，按一下 **新增 (Add)**。

5 在 [動作] 中選取 [DNAT]。

6 選取通訊協定類型。

依預設會選取**任何通訊協定 (Any Protocol)**。

7 在 [目的地 IP 位址] 中輸入虛擬機器的外部 IP 位址。

在此範例中，目的地 IP 位址是 80.80.80.1。請注意，虛擬機器上不需要設定外部 IP 位址。僅 NAT 路由器需要知道外部 IP 位址。

8 針對 [已轉譯的 IP] 位址，輸入虛擬機器的內部 IP 位址。

虛擬機器上必須設定內部 IP 位址。

在此範例中，內部/已轉譯的 IP 位址是 172.16.10.10。

9 在 [來源 IP 位址] 中，您可以將其保持空白，或是輸入一個 IP 位址。

如果您將來源 IP 保持空白，則 NAT 會套用至本機子網路外部的所有來源。

10 啟用規則。

11 (可選) 啟用記錄。

新規則會在 NAT 下方列出。例如：

Tenant2NAT

概視

組態

路由

服務

NAT

重新整理

未收集任何統計資料

新增

編輯

刪除

識別碼	動作	相符					已轉譯		套用至	統計資料
		通訊協定	來源 IP	來源連接埠	目的地 IP	目的地連接埠	IP	連接埠		
優先順序: 1024										
1034	DNAT	任何	任何	任何	80.80.80.1	任何	172.16.10.10	任何		

## 後續步驟

設定第 1 層路由器以通告 NAT 路由器。

若要從第 0 層路由器對實體架構通告 NAT 路由上游，請設定第 0 層路由器以通告第 1 層 NAT 路由。

## 通告第 1 層 NAT 路由至上游第 0 層路由器

通告第 1 層 NAT 路由可讓上游第 0 層路由器學習這些路由。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取**路由 (Routing)**。
- 3 按一下您已設定 NAT 的第 1 層邏輯路由器。
- 4 從第 1 層路由器中，選取**路由 > 路由通告 (Routing > Route Advertisement)**。

- 5 編輯路由通告規則以啟用 NAT 路由通告。



## Tenant2NAT

Summary

Configuration

Routing ▼

NAT

### Route Advertisement

Status	● Enabled
Advertise All NSX Connected Routes	● Yes
Advertise NAT Routes	● Yes
Advertise Static Routes	● No

### 後續步驟

從第 0 層路由器通告第 1 層 NAT 路由至上游實體架構。

## 通告第 1 層 NAT 路由至實體架構

從第 0 層路由器通告第 1 層 NAT 路由可使上游實體架構學習這些路由。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取路由。
- 3 按一下連線至您已設定 NAT 之第 1 層路由器的第 0 層邏輯路由器。
- 4 從第 0 層路由器中，選取路由 > 路由重新分配。
- 5 編輯路由通告規則以啟用第 1 層 NAT 路由通告。



Edit Redistribution Criteria - T1

×

Name: \*

T1

Description:

Sources: \*

☐ Static
☒ NSX Connected
☒ NSX Static
☐ Tier-0 NAT
☒ Tier-1 NAT

Route Map:

×

▼

Save

Cancel

#### 後續步驟

確認 NAT 如預期般運作。

## 確認第 1 層 NAT

確認 SNAT 和 DNAT 規則是否正確運作。

#### 程序

- 1 登入 NSX Edge。
- 2 執行 `get logical-routers` 命令以判斷第 0 層服務路由器的 VRF 編號。
- 3 執行 `vrf <number>` 命令以進入第 0 層服務路由器內容。
- 4 執行 `show route` 命令以確定第 1 層 NAT 位址已顯示。

```

nsx-edge(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 8

t1n 80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 如果您的 Web 虛擬機器設定為提供網頁，請確定您可以在 `http://80.80.80.1` 開啟網頁。
- 6 確定實體架構中第 0 層路由器的上游芳鄰可以對 80.80.80.1 執行 Ping 偵測。
- 7 當 Ping 偵測執行中時，請檢查 DNAT 規則的統計資訊資料行。  
其中應該存在一個作用中工作階段。

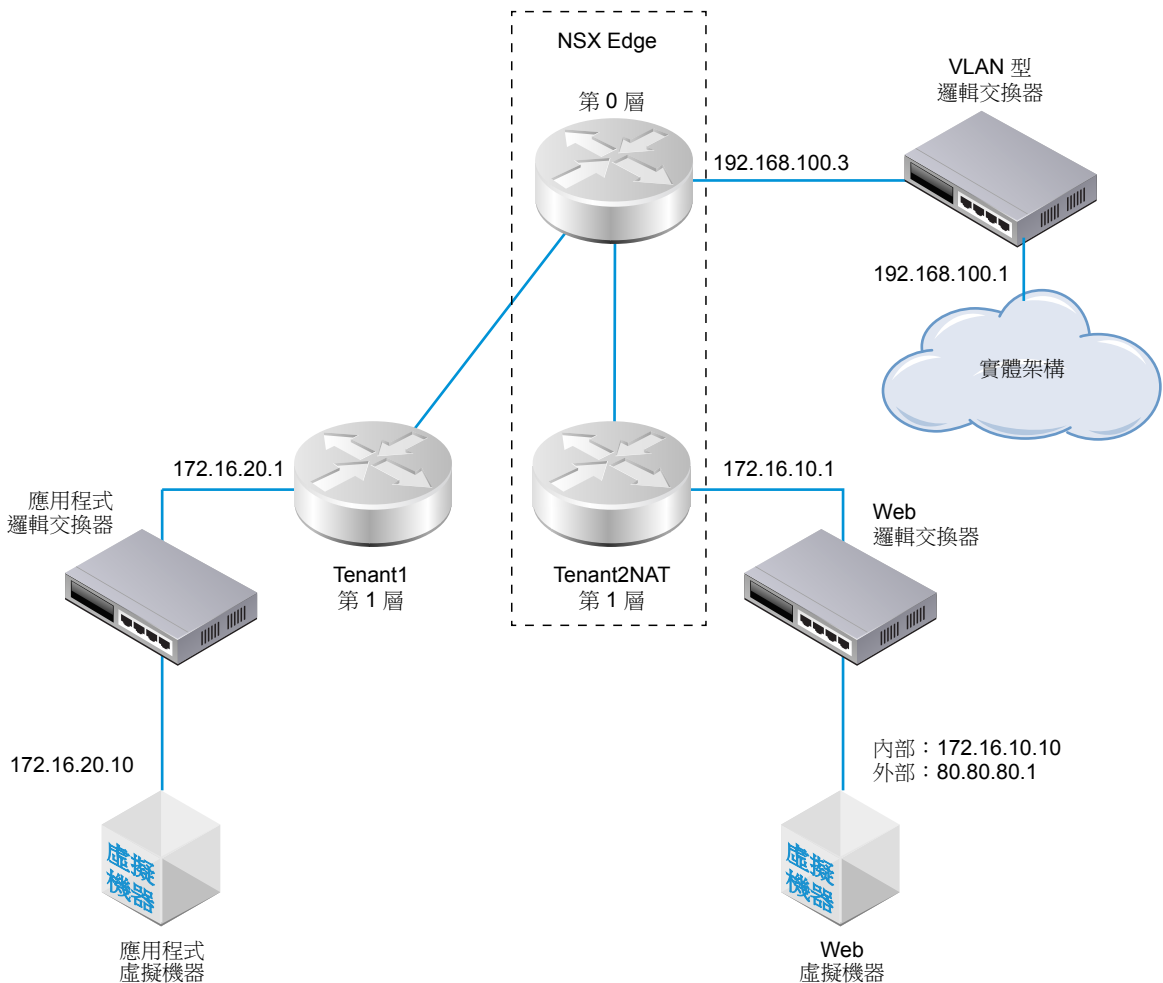
## 第 0 層 NAT

第 0 層邏輯路由器支援自反 NAT。

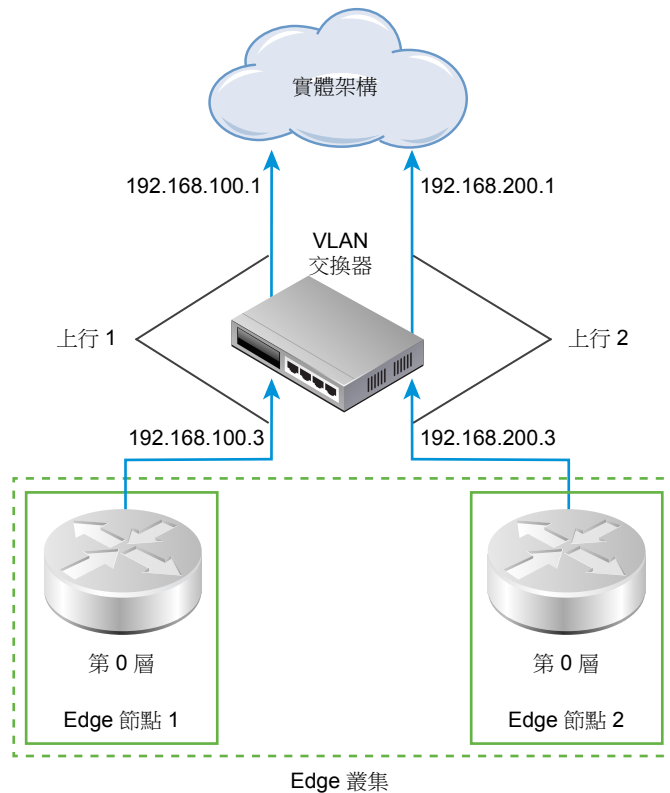
### 自反 NAT

當第 0 層邏輯路由器在主動-主動式 ECMP 模式中執行時，您無法設定可設定狀態 NAT，因為非對稱路徑可能會發生問題。對於主動-主動式 ECMP 路由器，您可以使用自反 NAT (有時稱為無狀態 NAT)。

在此範例中，從 Web 虛擬機器擷取封包時，Tenant2NAT 第 1 層路由器會將封包的來源連接埠從 172.16.10.10 變更為 80.80.80.1。具備公開來源位址可以啟用私人網路外部的目的地，以便路由回原始來源。



不過，涉及兩個主動-主動式第 0 層路由器時 (如下圖所示)，則必須設定自反 NAT。



## 在第 0 層邏輯路由器上設定自反 NAT

當第 0 層邏輯路由器在主動-主動式 ECMP 模式中執行時，您無法設定可設定狀態 NAT，因為非對稱路徑可能會發生問題。對於主動-主動式 ECMP 路由器，您可以使用自反 NAT (有時稱為無狀態 NAT)。

### 先決條件

- 第 0 層路由器必須有兩個連線至以 VLAN 為基礎的邏輯交換器的上行。請參閱[將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。
- 第 0 層路由器必須將路由 (靜態或 BGP) 和路由重新分配設定在其連往實體架構的上行。請參閱[設定靜態路由](#)、[在第 0 層邏輯路由器上設定 BGP](#) 和 [啟用第 0 層邏輯路由器上的路由重新分配](#)。
- 第 1 層路由器必須各自設定連往第 0 層路由器的上行。Tenant2NAT 必須受 Edge 叢集支援。請參閱[連結第 0 層和第 1 層](#)。
- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱[新增第 1 層邏輯路由器的下行連接埠與在第 1 層邏輯路由器上設定路由通告](#)。
- 虛擬機器必須連結至正確的邏輯交換器。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取 **路由 (Routing)**。

- 3 按一下您要設定自反 NAT 的第 0 層邏輯路由器。
- 4 在 NAT 下，按一下**新增 (Add)**。
- 5 針對 [動作] 選取 [自反]。
- 6 針對 [來源 IP] 位址，輸入虛擬機器的外部 IP 位址。  
在此範例中，來源 IP 為 80.80.80.1。
- 7 針對 [已轉譯的 IP] 位址，輸入虛擬機器的內部 IP 位址。  
在此範例中，已轉譯的 IP 位址為 172.16.10.10。
- 8 針對 [目的地 IP] 位址，您可以保留空白或輸入 IP 位址。  
如果您將 [目的地 IP] 保留空白，則 NAT 會套用至本機子網路外部的所有目的地。
- 9 啟用規則。
- 10 (可選) 啟用記錄。

新規則會在 NAT 下方列出。例如：

PLR-1

概視

組態

路由

服務

NAT

重新整理

規則統計資料總計 | 上次更新時間: 9/13/2018, 2:44:27 AM

作用中工作階段

+ 新增

編輯

刪除

封包計數

位元組 資料

識別碼	動作	相符				已轉譯		套用至	統計資料
		通訊協定	來源 IP	來源連接埠	目的地 IP	目的地連接埠	IP		
優先順序: 1024									
1030	自反	任何	80.80.80.1	任何	任何	任何	172.16.10.10	任何	

## 後續步驟

設定第 1 層路由器以通告 NAT 路由器。

若要從第 0 層路由器對實體架構通告 NAT 路由上游，請設定第 0 層路由器以通告第 1 層 NAT 路由。

## 防火牆區段和防火牆規則

防火牆區段用於群組一組防火牆規則。

防火牆區段由一或多個個別的防火牆規則所組成。每個防火牆規則皆包含指示，用以判斷是否應允許或封鎖某個封包；允許使用哪些通訊協定；以及允許使用哪些連接埠等。區段可用於多租戶，例如不同區段中適用於銷售和工程部門的特定規則。

區段也可定義為強制執行可設定狀態或無狀態規則。無狀態規則會視為傳統的無狀態 **ACL**。無狀態區段不支援自反 **ACL**。不建議在單一邏輯交換器連接埠中混用無狀態和可設定狀態規則，如此可能導致未定義的行為。

區段中的規則可以向上或向下移動。對於嘗試通過防火牆的任何流量，封包資訊皆會受到區段中所顯示規則順序的約束，從頂端開始，一路往底部的預設規則依序處理。系統會套用符合封包之第一個規則的設定動作，並執行該規則設定選項中指定的任何處理，且會忽略所有後續規則 (即便後面規則的符合程度更高)。因此，您應將特定規則放在一般規則的上方，以確保這些規則不會被忽略。預設規則位於規則表格的底部，這是一個「概括」(catchall) 規則，不符合任何其他規則的封包都將由預設規則強制執行。

本章包含以下主題：

- [新增防火牆規則區段](#)
- [刪除防火牆規則區段](#)
- [啟用和停用區段規則](#)
- [停用和啟用區段記錄](#)
- [關於防火牆規則](#)
- [新增防火牆規則](#)
- [刪除防火牆規則](#)
- [編輯預設分散式防火牆規則](#)
- [變更防火牆規則的順序](#)
- [篩選防火牆規則](#)
- [在防火牆強制執行中排除物件](#)

### 新增防火牆規則區段

防火牆規則區段會進行獨立編輯和儲存，並且用來將個別的防火牆組態套用至承租人。

**程序**

- 1 選取導覽面板中的**防火牆 (Firewall)**。

確定您位於 [一般] 索引標籤中以便新增 L3 規則。按一下 [乙太網路] 索引標籤以新增 L2 規則。

- 2 若要新增區段，在第一個資料行中按一下輪狀 (⚙️) 圖示或規則，並選取**新增以上區段 (Add Section Above)**或**新增以下區段 (Add Section Below)**。

---

**備註** 對於嘗試通過防火牆的任何流量，封包資訊皆會受到 [規則] 表格中所顯示規則順序的約束，從頂端開始，一路往底部的預設規則依序處理。在某些情況下，兩個以上規則的優先順序對於判定封包的處理方式而言可能很重要。

---

- 3 輸入區段名稱和選用說明。
- 4 選取**可設定狀態 (Stateful)**，**False** 或 **True**。這個選項僅適用於第 3 層。

無狀態防火牆會監控網路流量，並根據來源和目的地位址或其他靜態值來限制或封鎖封包。可設定狀態防火牆可以從端對端監控流量串流。無狀態防火牆在較大流量負載下通常較快且效能更佳。可設定狀態防火牆較能識別未經過驗證及偽造的通訊。一旦定義完成後，便不會在可設定狀態及無狀態之間切換。

- 5 選取希望要套用區段的位置。

---

**備註** 如果您已在區段中使用**套用至 (Applied To)**，它會在該區段中覆寫任何規則中的**套用至 (Applied To)**設定。

---

邏輯連接埠 - 顯示所有邏輯連接埠

邏輯交換器 - 顯示所有邏輯交換器

NSGroup - 顯示所有 NSGroup

- 6 按一下可用連接埠、交換器或群組旁的核取方塊，然後按一下箭頭。  
項目會移至 [已選取] 資料行。
- 7 按一下**儲存 (Save)**以儲存區段。

新增的區段會顯示在**防火牆 (Firewall)**視窗中。

**後續步驟**

將防火牆規則新增至區段。


## 刪除防火牆規則區段

不再需要某個防火牆規則區段時，可將其刪除。

刪除防火牆規則區段時，該區段中的所有規則也會一併刪除。您無法刪除區段，然後在防火牆表格的不同位置再次新增。若要這麼做，您必須刪除區段並發佈組態。然後將已刪除區段新增至防火牆表格，並再次發佈組態。

**程序**

- 1 選取導覽面板中的**防火牆 (Firewall)**。

- 2 確定您位於 [一般] 索引標籤中以便新增 L3 規則。
- 3 按一下 [乙太網路] 索引標籤以新增 L2 規則。
- 4 若要刪除區段，請在第一個資料行中，在您要刪除之區段旁邊的輪狀圖示  上按一下滑鼠右鍵。
- 5 按一下 **刪除 (Delete)** 以移除區段。該區段及其包含的所有規則現在皆已刪除。

## 啟用和停用區段規則

您可以啟用或停用防火牆規則區段中的所有規則。

### 程序

- 1 選取導覽面板中的 **防火牆 (Firewall)**。
- 2 在第一個資料行中按一下輪狀圖示，然後選取 **停用區段規則 (Disable Section Rules)** 或 **啟用區段規則 (Enable Section Rules)**。
- 3 按一下 **儲存 (Save)**。

## 停用和啟用區段記錄

啟用區段規則的記錄會記錄區段中所有規則的封包資訊。視區段中的規則數而定，典型的防火牆區段會產生大量記錄資訊，而這可能會影響效能。

記錄會儲存在 vSphere ESXi 和 KVM 主機上的 `/var/log/dfwpktlogs.log` 檔案中。

### 程序

- 1 選取導覽面板中的 **防火牆 (Firewall)**。
- 2 在第一個資料行中，按一下輪狀  圖示。選取 **停用區段規則的記錄 (Disable Logs for Section Rules)** 或 **啟用區段規則的記錄 (Enable Logs for Section Rules)**。
- 3 按一下 **儲存 (Save)**。

## 關於防火牆規則

NSX-T 會使用防火牆規則來指定網路內外的流量處理。

防火牆提供多個可設定規則集：第 3 層規則 ([一般] 索引標籤) 和第 2 層規則 ([乙太網路] 索引標籤)。第 2 層防火牆規則會在第 3 層防火牆規則之前處理。[組態] 索引標籤包含排除清單，其中包含邏輯交換器、邏輯連接埠和要排除在防火牆強制執行之外的群組。

防火牆規則根據下列方式強制執行：

- 規則會以從上到下的順序處理。
- 在資料表中將後續規則向下移動之前，系統會對規則資料表中的頂端規則檢查每一個封包。
- 系統會強制執行資料表中符合流量參數的第一個規則。

無法強制執行後續規則，因為系統接著會終止該封包的搜尋。由於這個行為，建議您一律在規則資料表頂端放置最精細的原則。這樣可確保它們在更具體的規則之前予以強制執行。

預設規則位於規則表格的底部，這是一個概括規則，不符合任何其他規則的封包都將由預設規則強制執行。在主機準備作業之後，系統會設定預設規則以允許動作。這樣可確保虛擬機器至虛擬機器的通訊，在暫存或移轉階段期間不會中斷。最佳做法是將此預設規則變更為封鎖動作，並透過正控制模型來強制執行存取控制 (例如，網路上僅允許防火牆規則中定義的流量)。

您可以按一下 [資料行] 旁的下拉式箭頭，並檢查要包含在防火牆規則視窗中的資料行來存取防火牆規則選項。可用選項如下。

**表格 7-1. 防火牆規則畫面中的資料行**

資料行名稱	定義
名稱	防火牆規則名稱。
來源	規則的來源可以是 IP 或 MAC 位址，或是 IP 位址以外的物件。若未定義，則來源會符合任何項目。來源或目的地範圍不支援 IPv6。
識別碼	每個規則的唯一系統產生識別碼。
方向	方向規則元素符合封包在周遊介面時所傳輸的方向。入口方向是經過防火牆的入口流量。出口方向是經過防火牆的出口流量。依預設，方向為出入口 (雙向)。
IP 通訊協定	這僅適用於第 3 層規則。支援 IPv4 和 IPv6。預設值為此兩者。
目的地	受規則影響的連線目的地 IP 或 MAC 位址/網路遮罩。若未定義，則目的地會符合任何項目。來源或目的地範圍不支援 IPv6。
服務	服務可能為預先定義的第 3 層連接埠通訊協定組合。若為 L2，則可以是乙太類型。若為 L2 和 L3，您可以手動定義新的服務及服務群組。若未定義，則服務會符合任何項目。
動作 (必要)	可允許、封鎖或拒絕規則所套用的動作。
套用至	定義此規則適用的範圍。若未定義，則範圍將為全部的邏輯連接埠。如果您已在區段中新增「套用至」，則它會覆寫規則。
記錄	可關閉或開啟記錄。記錄會儲存在 ESX 及 KVM 主機上的 /var/log/dfwptlogs.log 檔案。
統計資料	顯示位元組、封包計數和工作階段的唯讀欄位。
備註	規則註解。

以下為預設防火牆規則與其部分資料行選項。

**圖 7-1: 防火牆規則視窗**

GENERAL   ETHERNET   CONFIGURATION									
<span>UP</span> <span>DOWN</span> <span>COLUMNS</span> <span>FILTER</span> <span>OBJECTS</span>									
	Name	ID	Sources	Destinations	Services	Action	Applied To	Log	Stats
☰	default - a3b004... (5) Applied To: 1	4ae3398c-6c...							
1	2b8f904d-b41e-454d-890e-54af...	3165	default - a3b0...	default - a3b0...	Any	Allow	All	No	packets: 0 bytes: 0 sessions: 0

## 新增防火牆規則

防火牆是一種網路安全系統，可根據預先決定的防火牆規則，監視和控制傳入和傳出的網路流量。



系統會在 **NSX Manager** 範圍中新增防火牆規則。使用 [套用至] 欄位，便可以縮小您要套用規則的範圍。您可以在每個規則的來源及目的地層級新增多個物件，這有助於降低要新增的防火牆規則總數。

---

**備註** 依預設，規則符合任何來源、目的地和服務規則元素的預設值，且符合所有介面及流量方向。如果您要限制規則對特定介面或流量方向的影響，則必須指定規則中的限制。

---

### 先決條件

若要使用一組位址，應先手動將每部虛擬機器的 IP 和 MAC 位址與其邏輯交換器建立關聯。

### 程序

- 1 選取導覽面板中的**防火牆 (Firewall)**。

確定您位於 [一般] 索引標籤中以便新增 **L3** 規則。按一下 [乙太網路] 索引標籤以新增 **L2** 規則。

- 2 若要新增規則，請在第一個資料行中，按一下輪狀 (⚙️) 圖示，並在清單底部選取**新增規則 (Add Rule)**。

隨即顯示新的列可用來定義防火牆規則。

---

**備註** 對於嘗試通過防火牆的任何流量，封包資訊皆會受到 [規則] 表格中所顯示規則順序的約束，從頂端開始，一路往底部的預設規則依序處理。在某些情況下，兩個以上規則的優先順序對於判定封包的處理方式而言可能很重要。

---

- 3 系統會在區段頂端新增規則。如果您要在區段中的特定位置新增規則，請選取規則。在第一個資料行中，按一下輪狀 (⚙️) 圖示，並選取**插入以上規則 (Insert Rule Above)**或**插入以下規則 (Insert Rule Below)**。

隨即顯示新的列可用來定義防火牆規則。

- 4 在**名稱 (Name)**資料行的右上角，按一下鉛筆圖示。在 [編輯名稱] 對話方塊中輸入規則名稱。

隨即顯示規則與指定名稱。

- 5 指向新規則的**來源 (Sources)**儲存格，接著按一下鉛筆圖示，然後選取規則的來源。若未定義，則來源會符合任何項目。**編輯來源 (Edit Sources)**對話方塊隨即顯示。

---

**備註** 建立新的防火牆規則時，您可以拖放用於 [來源]、[目的地]、[服務] 及 [套用至] 欄位的物件，而不需每次皆選取這些項目。這有助於加速規則建立程序，尤其是當經常重複使用相同的物件時。

若要這麼做，請按一下防火牆規則視窗左側角中的**物件**，接著從清單中選取物件類型，然後將您需要的物件拖放至右側欄位，即防火牆規則中的 [來源]。

---

表格 7-2. 編輯來源視窗

選項	說明
IP 位址 或 MAC 位址	在以逗點分隔的清單中輸入多個 IP 或 MAC 位址。該清單最多可包含 255 個字元。支援 IPv4 和 IPv6 格式。
物件	<p>按一下箭頭並選取物件。</p> <ol style="list-style-type: none"> <li>選取 IP 集合、邏輯連接埠、邏輯交換器或 NS 群組。</li> </ol> <p>所選容器的可用物件隨即顯示。</p> <ol style="list-style-type: none"> <li>選取一或多個物件並按一下箭頭。若要選取所有可用的物件，按一下 [可用] 旁的核取方塊，然後按一下箭頭。</li> <li>物件會移至所選資料行。</li> <li>按一下 <b>確定 (OK)</b>。</li> </ol>

- 6 指向新規則的目的地 (**Destinations**)儲存格。若未定義，則目的地會符合任何項目。**編輯目的地 (Edit Destinations)**對話方塊隨即顯示。

表格 7-3. 編輯目的地視窗

選項	說明
IP 位址 或 MAC 位址	您可以在以逗點分隔的清單中輸入多個 IP 或 MAC 位址。該清單最多可包含 255 個字元。支援 IPv4 和 IPv6 格式。
物件	<p>按一下箭頭並選取物件。</p> <ol style="list-style-type: none"> <li>您可以選取 IP 集合、邏輯連接埠、邏輯交換器或 NS 群組。</li> </ol> <p>所選容器的可用物件隨即顯示。</p> <ol style="list-style-type: none"> <li>選取一或多個物件並按一下箭頭。若要選取所有可用的物件，按一下 [可用] 旁的核取方塊，然後按一下箭頭。</li> <li>物件會移至所選資料行。</li> <li>按一下 <b>確定 (OK)</b>。</li> </ol>

- 7 指向新規則的服務 (**Service**)儲存格。若未定義，則服務會符合任何項目。

**編輯服務 (Edit Services)**對話方塊隨即顯示。清單已顯示多個預先定義的服務，但您不受限於這些選擇。

- 8 若要選取預先定義的服務，請選取一或多個可用物件然後按一下箭頭。按一下 **確定 (OK)**。
- 9 若要定義新服務，按一下 **新增 (New)**。NSService 對話方塊隨即顯示。

選項	說明
名稱	新服務的名稱。
說明	說明新服務。
服務類型	<ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IP</li> <li>■ L4 連接埠集合</li> <li>■ IGMP</li> </ul>

選項	說明
通訊協定	選取下列其中一項可用通訊協定。
來源連接埠	輸入來源連接埠。
目的地連接埠	選取目的地連接埠。
群組現有服務	按一下選項按鈕以新增現有群組服務。

- 10 指向**動作 (Action)**儲存格然後按一下鉛筆圖示。此為必要參數。[編輯動作] 對話方塊隨即顯示。

選項	說明
允許	允許具有指定來源、目的地和通訊協定的所有 L3 或 L2 流量通過目前的防火牆內容。符合規則且被接受的封包會周遊系統，好像防火牆不存在一樣。
捨棄	捨棄具有指定來源、目的地和通訊協定的封包。捨棄封包是一種無訊息動作，並不會傳送通知給來源或目的地系統。捨棄封包會導致重試連線，直到達到重試臨界值為止。
拒絕	拒絕具有指定來源、目的地和通訊協定的封包。拒絕封包是較委婉的拒絕方式，它會傳送無法連線目的地訊息給寄件者。如果通訊協定是 TCP，則會傳送 TCP RST 訊息。系統會針對 UDP、ICMP 和其他 IP 連線傳送具有以系統管理方式禁止程式碼的 ICMP 訊息。使用拒絕的其中一個好處是，發生一次無法建立連線的情形後，傳送方應用程式即會收到通知。

- 11 指向**套用至 (Applied To)**儲存格，然後按一下鉛筆圖示。[編輯套用至] 對話方塊隨即顯示。

從下拉式清單中選取物件類型。按一下**確定 (OK)**。

- 12 指向**記錄 (Log)**儲存格然後按一下鉛筆圖示。依預設會關閉記錄。選取**是 (Yes)**以啟用記錄，或**否 (No)**以停用記錄。記錄會儲存在 ESX 及 KVM 主機上的 `/var/log/dfwpktlogs.log` 檔案。您也可以在此處寫下備註。請注意，選取**是 (Yes)**將會記錄符合此規則的所有工作階段。啟用記錄可能會影響效能。

- 13 若要讓您的規則生效，請按一下**儲存 (Save)**。

您可以先新增多個規則後再按一下**儲存 (Save)**。

## 刪除防火牆規則

防火牆是一種網路安全系統，可根據預先決定的防火牆規則，監視和控制傳入和傳出的網路流量。您可以新增和刪除自訂的已定義規則。

### 程序

- 1 選取導覽面板中的**防火牆 (Firewall)**。  
確定您位於 [一般] 索引標籤中以便新增 L3 規則。按一下 [乙太網路] 索引標籤以新增 L2 規則。
- 2 在您要移動的規則編號上按一下滑鼠右鍵。  
隨即顯示一個下拉式清單。
- 3 選取**刪除 (Delete)**。  
防火牆規則即會刪除。
- 4 按一下**儲存 (Save)**以使變更生效。

規則即會刪除。

## 編輯預設分散式防火牆規則

您可以編輯預設防火牆設定，用來套用至不符合任何使用者定義防火牆規則的流量。

預設防火牆設定會套用至不符合任何使用者定義防火牆規則的流量。「分散式防火牆」預設規則會顯示在集中式防火牆使用者介面中。預設第 3 層規則會顯示在 [一般] 索引標籤下方，而預設第 2 層規則會顯示在 [乙太網路] 索引標籤下方。

預設分散式防火牆規則會允許所有 L3 和 L2 流量通過您基礎結構中所有準備就緒的叢集。預設規則一律位於規則表格底部，且無法刪除或新增。但是，您可將規則的 [動作] 元素從 [允許] 變更為 [捨棄] 或 [拒絕] (不建議)，並指示是否應記錄該規則的流量。

### 程序

- 1 按一下**防火牆 (Firewall)**。

[一般防火牆] 畫面隨即顯示。

- 2 確定您位於**一般 (General)**索引標籤中以便編輯 L3 規則。按一下**乙太網路 (Ethernet)**索引標籤，即可編輯 L2 規則。

- 3 在**動作 (Action)**資料行下方，展開區段並選取其中一個選項：

- 允許 - 允許具有指定來源、目的地和通訊協定的所有 L3 或 L2 流量通過目前的防火牆內容。符合規則且被接受的封包會周遊系統，好像防火牆不存在一樣。
- 捨棄 - 捨棄具有指定來源、目的地和通訊協定的封包。捨棄封包是一種無訊息動作，並不會傳送通知給來源或目的地系統。捨棄封包會導致重試連線，直到達到重試臨界值為止。
- 拒絕 - 拒絕具有指定來源、目的地和通訊協定的封包。拒絕封包是較委婉的拒絕方式，它會傳送無法連線目的地訊息給寄件者。如果通訊協定是 TCP，則會傳送 TCP RST 訊息。系統會針對 UDP、ICMP 和其他 IP 連線傳送具有以系統管理方式禁止程式碼的 ICMP 訊息。使用拒絕的其中一個好處是，發生一次無法建立連線的情形後，傳送方應用程式即會收到通知。

---

**備註** 不建議選取**拒絕 (Reject)**作為預設規則的動作。

---

- 4 在**記錄 (Log)**資料行下方，展開區段並選取**是 (Yes)**以啟用記錄，或選取**否 (No)**以停用記錄。您也可以在此處寫下備註。請注意，選取 [是] 會記錄符合此規則的所有工作階段。啟用記錄可能會影響效能。
- 5 按一下**儲存 (Save)**並確認您的變更。

## 變更防火牆規則的順序

規則會以從上到下的順序處理。您可以變更清單中規則的順序。

對於嘗試通過防火牆的任何流量，封包資訊皆會受到 [規則] 表格中所顯示規則順序的約束，從頂端開始，一路往底部的預設規則依序處理。在某些情況下，兩個以上規則的優先順序對於判定流量而言可能很重要。

您可以在資料表中將自訂規則上移或下移。預設規則一律位於資料表的底部，且無法移動。

#### 程序

- 1 選取導覽面板中的**防火牆 (Firewall)**。  
確定您位於 [一般] 索引標籤中以便新增 L3 規則。按一下 [乙太網路] 索引標籤以新增 L2 規則。
- 2 在您要移動的規則編號上按一下滑鼠右鍵。
- 3 選取**上移 (Move Up)**或**下移 (Move Down)**。  
規則即會上移或下移一個位置。

## 篩選防火牆規則

您可使用數個準則來篩選規則集以輕鬆修改規則。

#### 程序

- 1 在 [防火牆] 視窗的左上方角落，按一下**篩選器 (Filter)** FILTER。  
[篩選器] 對話方塊隨即顯示。
- 2 對於篩選，您可以搜尋以下項目：
  - 來源 - 搜尋輸入防火牆規則。
  - 目的地 - 搜尋輸出防火牆規則。
  - 套用至 - 搜尋 [套用至] 準則上的規則。
  - 服務 - 可從此清單中選取要允許或封鎖的應用程式或服務。清單中已顯示許多常用服務，但您不受限於這些選擇。使用 [服務] 儲存格可新增尚未顯示的其他服務或應用程式。
- 3 按一下您要進行搜尋的準則，該準則即會顯示在方塊頂端。
- 4 選取搜尋的類型：
  - IP 集合 - 此選項會列出規則來源或目的地的所有 IP 位址。
  - 邏輯連接埠 - 根據邏輯連接埠進行篩選。
  - 邏輯交換器 - 根據邏輯交換器進行篩選。
  - NSGroup - 根據 NSGroup 進行篩選。

篩選結果將顯示在方塊中。

## 在防火牆強制執行中排除物件

您可以在防火牆規則中排除邏輯連接埠、邏輯交換器或 NSGroup。

使用防火牆規則建立區段之後，您可能會想要在防火牆規則中排除 NSX-T 應用裝置連接埠。

**程序**

- 1 選取導覽面板中的**防火牆 (Firewall)**。選取**組態 (Configuration)**索引標籤。  
隨即會顯示排除清單畫面。
- 2 選取視窗右手邊角落的**物件 (Objects)**。
- 3 從下拉式清單中選取**邏輯連接埠 (Logical Ports)**、**邏輯交換器 (Logical Switch)**或 **NSGroup**。
- 4 按兩下您要在防火牆規則中排除的特定連接埠、交換器或群組。若要關閉 **[物件]** 對話方塊，請再次按一下**物件 (Objects)**。  
排除清單中會填入您所要排除的物件名稱和類型。
- 5 若要從排除清單中移除物件，請按一下 **x**。
- 6 按一下**儲存 (Save)**。

## 設定群組與服務

您可以設定群組以組織物件。

您可以使用下列防火牆規則中的群組：

- IP 集合
- MAC 集合
- 服務群組
- NSGroup，其中可包含 IP 集合、MAC 集合、邏輯連接埠、邏輯交換器，以及其他 NSGroup

此外，您也可以建立 IP 集區，以便在您建立傳輸節點時指派 IP 位址。

本章包含以下主題：

- [建立 IP 集合](#)
- [建立 IP 集區](#)
- [建立 MAC 集合](#)
- [建立 NSGroup](#)
- [設定服務和服務群組](#)

### 建立 IP 集合

IP 集合是一組 IP 位址，您可在防火牆規則中當作來源和目的地使用。

IP 集合可以包含個別 IP 位址、一組 IP 範圍以及子網路的組合。您可以指定 IPv4 或 IPv6 位址，或兩者皆指定。IP 集合可以是 NSGroup 的成員。

---

**備註** 防火牆規則不支援將 IPv6 作為來源或目的地範圍。

---

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 (Inventory) > 群組 (Groups)**。
- 3 在主面板頂端選取 **IP 集合**。
- 4 按一下**新增**。

- 5 輸入名稱。
- 6 (可選) 輸入說明。
- 7 輸入個別位址或一組位址範圍。
- 8 按一下**儲存**。

## 建立 IP 集區

建立 L3 子網路時，可使用 IP 集區來配置 IP 位址或子網路。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 (Inventory) > 群組 (Groups)**。
- 3 在主面板頂部選取 **IP 集區**。
- 4 按一下**新增**。
- 5 輸入名稱。
- 6 (可選) 輸入說明。
- 7 按一下**新增**。
- 8 輸入 IP 範圍。

將滑鼠移到任何儲存格的右上角，並按一下鉛筆圖示以進行編輯。

- 9 (可選) 輸入開道。
- 10 輸入包含尾碼的 CIDR IP 位址。
- 11 (可選) 輸入 DNS 伺服器。
- 12 (可選) 輸入 DNS 尾碼。
- 13 按一下**儲存**。

## 建立 MAC 集合

MAC 集合是一組 MAC 位址，您可以在第 2 層防火牆規則中用作來源及目的地，以及用作 NS 群組的成員。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 (Inventory) > 群組 (Groups)**。
- 3 選取主面板頂部的 **MAC 集合**。
- 4 按一下**新增**。
- 5 輸入名稱。



- 6 (可選) 輸入說明。
- 7 輸入 MAC 位址。
- 8 按一下**儲存**。

## 建立 NSGroup

您可以設定 NSGroup 來包含 IP 集合、MAC 集合、邏輯連接埠、邏輯交換器以及其他 NSGroup。您可將 NSGroup 指定為來源和目的地，以及在 **Applied To** 欄位和防火牆規則中指定。

NSGroup 具有下列特性：

- 您可以設定直接成員，這可以是 IP 集合、MAC 集合、邏輯連接埠、邏輯交換器以及其他 NSGroup。
- 您最多可以為邏輯交換器和邏輯連接埠設定五個成員資格準則。對於每個準則，請指定標記並可選擇指定範圍。
- NSGroup 具有直接成員和有效成員。有效成員包含您使用成員資格準則指定的成員，以及屬於此 NSGroup 成員的所有直接和有效成員。例如，假設 NSGroup-1 具有直接成員 LogicalSwitch-1。您新增 NSGroup-2 並指定 NSGroup-1 和 LogicalSwitch-2 作為成員。現在 NSGroup-2 具有直接成員 NSGroup-1 和 LogicalSwitch-2，以及有效成員 LogicalSwitch-1。接著您新增 NSGroup-3 並指定 NSGroup-2 作為成員。NSGroup-3 現在具有直接成員 NSGroup-2，以及有效成員 LogicalSwitch-1 和 LogicalSwitch-2。
- NSGroup 最多可以有 500 個直接成員。
- NSGroup 中有效成員的建議數目上限是 5000 個。超過此限制並不會影響任何功能，但可能會對效能造成不利影響。在 NSX Manager 上，當 NSGroup 的有效成員數目超過 5000 的 80%，記錄檔中會顯示警告訊息 `NSGroup xyz is about to exceed the maximum member limit.Total number in NSGroup is ...`，而當數目超過 5000，系統會顯示警告訊息 `NSGroup xyz has reached the maximum numbers limit.Total number in NSGroup = ...`。在 NSX Controller 中，當 NSGroup 中的已轉譯 VIF/IP/MAC 數目超過 5000，記錄檔中會出現警告訊息 `Container xyz has reached the maximum IP/MAC/VIF translations limit.Current translations count in Container - IPs:..., MACs:..., VIFs:...`。NSX Manager 和 NSX Controller 會每天檢查 NSGroup 的限制數目兩次，分別在上午 7 點和下午 7 點。

對於所有您可新增至 NSGroup 作為成員的物件 (亦即邏輯交換器、邏輯連接埠、IP 集合、MAC 集合和 NSGroup)，您可導覽至任何物件的畫面並選取**相關 (Related) > NSGroup (NSGroups)**，即可查看直接或間接擁有該物件作為成員的所有 NSGroup。例如，在上述範例中，在您導覽至 LogicalSwitch-1 的畫面後，選取**相關 (Related) > NSGroup (NSGroups)** 會顯示 NSGroup-1、NSGroup-2 和 NSGroup-3，因為這三個皆擁有 LogicalSwitch-1 作為直接或間接成員。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**詳細目錄 (Inventory) > 群組 (Groups)**。
- 3 在主面板頂部選取 **NSGroup (NSGroups)**。
- 4 按一下**新增 (Add)**。

- 5 輸入 NSGroup 的名稱。
- 6 (可選) 輸入說明。
- 7 (可選) 按一下**成員資格準則 (Membership Criteria)**，最多指定五個準則。  
準則可套用至邏輯交換器或邏輯連接埠。  
準則可以指定標籤值、範圍值，或兩者。
- 8 (可選) 按一下**成員 (Members)**以選取成員。  
可用的類型為 **IP 集合 (IP Set)**、**MAC 集合 (MAC Set)**、**邏輯交換器 (Logical Switch)**、**邏輯連接埠 (Logical Port)**和 **NSGroup**。
- 9 按一下**儲存 (Save)**。

## 設定服務和服務群組

您可以設定 **NSService** 來指定比對網路流量的參數，例如連接埠和通訊協定配對。您也可以使用 **NSService**，在防火牆規則中允許或封鎖特定的流量類型。

**NSService** 可以是以下類型：

- 乙太
- IP
- IGMP
- ICMP
- ALG
- L4 連接埠集合

L4 連接埠集合支援來源連接埠和目的地連接埠的識別功能。您可以指定個別連接埠或一個連接埠範圍，最多可指定 15 個連接埠。

**NSService** 也可以是其他 **NSService** 的群組。**NSService** 群組可以是以下類型：

- 第 2 層
- 第 3 層及以上

建立 **NSService** 後即無法變更類型。某些 **NSService** 已預先定義。您無法修改或刪除這些項目。

## 建立 NSService

您可以建立 **NSService**，用來指定網路比對所使用的特性，或是定義要在防火牆規則中允許或封鎖的流量類型。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 (Inventory) > 服務 (Services)**。

- 3 按一下**新增 (Add)**。
- 4 輸入名稱。
- 5 (可選) 輸入說明。
- 6 選取**指定通訊協定 (Specify a protocol)**來設定個別服務，或選取**群組現有服務 (Group existing services)**來設定 NSService 群組。
- 7 對於個別服務，請選取類型和通訊協定。  
可用類型包括**乙太 (Ether)**、**IP**、**IGMP**、**ICMP**、**ALG** 和 **L4 連接埠集合 (L4 Port Set)**
- 8 對於服務群組，請選取該群組的類型和成員。  
可用類型包括**第 2 層 (Layer 2)**和**第 3 層及以上 (Layer 3 and above)**。
- 9 按一下**儲存 (Save)**。

# DHCP

DHCP (動態主機組態通訊協定) 可讓用戶端自動從 DHCP 伺服器取得網路組態，例如 IP 位址、子網路遮罩、預設閘道和 DNS 組態。

您可以建立 DHCP 伺服器來處理 DHCP 要求，或建立 DHCP 轉送服務以將 DHCP 流量轉送至外部 DHCP 伺服器。

如果您設定 DHCP 伺服器來提升安全性，請設定 DFW 規則來允許 UDP 連接埠 67 和 68 上的流量僅能用於有效的 DHCP 伺服器 IP 位址。

---

**備註** 以 Logical Switch/Logical Port/NSGroup 作為來源、以 Any 作為目的地，且已設定為捨棄連接埠 67 和 68 之 DHCP 封包的 DFW 規則，將無法封鎖 DHCP 流量。若要封鎖 DHCP 流量，請將 Any 設定為來源以及目的地。

---

本章包含以下主題：

- [建立 DHCP 伺服器設定檔](#)
- [建立 DHCP 伺服器](#)
- [將 DHCP 伺服器連結至邏輯交換器](#)
- [從邏輯交換器中斷連結 DHCP 伺服器](#)
- [建立 DHCP 轉送設定檔](#)
- [建立 DHCP 轉送服務](#)
- [將 DHCP 服務新增至邏輯路由器連接埠](#)

## 建立 DHCP 伺服器設定檔

DHCP 伺服器設定檔會指定 NSX Edge 叢集或 NSX Edge 叢集的成員。具有此設定檔的 DHCP 伺服器會為來自邏輯交換器上虛擬機器的 DHCP 要求提供服務，而該交換器會連線至設定檔中所指定的 NSX Edge 節點。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **DHCP**。

- 3 按一下**伺服器設定檔**，然後按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 從下拉式功能表中選取 **NSX Edge 叢集**。
- 6 (可選) 選取 **NSX Edge 叢集**的成員。

您最多可以指定 2 個成員。

#### 後續步驟

建立 DHCP 伺服器。請參閱[建立 DHCP 伺服器](#)。

## 建立 DHCP 伺服器

您可以建立 DHCP 伺服器，以便為來自連線至邏輯交換器之虛擬機器的 DHCP 要求提供服務。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **DHCP**。
- 3 按一下**伺服器**，然後按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 以 CIDR 格式輸入 DHCP 伺服器的 IP 位址及其子網路遮罩。  
例如，輸入 192.168.1.2/24。
- 6 從下拉式功能表中選取 DHCP 設定檔。
- 7 (可選) 輸入常用選項，例如網域名稱、預設閘道、DNS 伺服器和子網路遮罩。
- 8 (可選) 輸入無類別靜態路由選項。
- 9 (可選) 輸入其他選項。
- 10 按一下**儲存**。
- 11 選取新建立的 DHCP 伺服器。
- 12 展開 **[IP 集區]** 區段。
- 13 按一下**新增**，以新增 IP 範圍、預設閘道、租用持續時間、警告臨界值、錯誤臨界值、無類別靜態路由選項和其他選項。
- 14 展開 **[靜態繫結]** 區段。
- 15 按一下**新增**，以新增 MAC 位址和 IP 位址之間的靜態繫結、預設閘道、主機名稱、租用持續時間、無類別靜態路由選項和其他選項。

#### 後續步驟

將 DHCP 伺服器連結到邏輯交換器。請參閱[將 DHCP 伺服器連結至邏輯交換器](#)。

## 將 DHCP 伺服器連結至邏輯交換器

您必須先將 DHCP 伺服器連結至邏輯交換器，DHCP 伺服器才能處理來自連線至交換器之虛擬機器的 DHCP 要求。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換器 (Switches)**。
- 3 按一下您想要用來連結 DHCP 伺服器的邏輯交換器。
- 4 按一下**動作 (Actions) > 連結 DHCP 伺服器 (Attach DHCP Server)**。

## 從邏輯交換器中斷連結 DHCP 伺服器

您可以從邏輯交換器中斷連結 DHCP 伺服器，以便重新設定您的環境。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 交換器 (Switches)**。
- 3 按一下您想從中中斷連結 DHCP 伺服器的邏輯交換器。
- 4 按一下**動作 > 中斷連結 DHCP 伺服器**。

## 建立 DHCP 轉送設定檔

DHCP 轉送設定檔會指定一或多個外部 DHCP 伺服器。當您建立 DHCP 轉送服務時，必須指定 DHCP 轉送設定檔。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **DHCP**。
- 3 按一下**轉送設定檔**，然後按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 輸入一或多個外部 DHCP 伺服器位址。

### 後續步驟

建立 DHCP 轉送服務。請參閱[建立 DHCP 轉送服務](#)。

## 建立 DHCP 轉送服務

您可以對 DHCP 用戶端與並未於 NSX-T 中建立之 DHCP 伺服器之間的轉送流量建立 DHCP 轉送服務。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **DHCP**。
- 3 按一下**轉送服務**，然後按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 從下拉式功能表中選取 DHCP 轉送設定檔。

### 後續步驟

將 DHCP 服務新增至邏輯路由器連接埠。請參閱[將 DHCP 服務新增至邏輯路由器連接埠](#)。

## 將 DHCP 服務新增至邏輯路由器連接埠

當您將 DHCP 轉送服務新增至邏輯路由器連接埠時，連結至該連接埠的邏輯交換器上的虛擬機器可與轉送服務中設定的 DHCP 伺服器進行通訊。

### 先決條件

- 確認您有已設定的 DHCP 轉送服務。請參閱[建立 DHCP 轉送服務](#)。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**路由 (Routing)**。
- 3 選取連線至所需邏輯交換器的路由器，然後按一下**組態索引標籤**。
- 4 選取連線至所需邏輯交換器的路由器連接埠，然後按一下**編輯**。
- 5 從 **DHCP 服務** 下拉式清單中選取 DHCP 轉送服務，然後按一下**儲存**。

邏輯路由器連接埠會在 **DHCP 服務** 資料行中顯示 DHCP 轉送服務。

當您新增邏輯路由器連接埠時，也可以選取 DHCP 轉送服務。

## 設定中繼資料 Proxy

中繼資料 Proxy 伺服器讓虛擬機器執行個體能夠從 OpenStack Nova API 伺服器，擷取執行個體特定的中繼資料。

下列步驟描述中繼資料 Proxy 的運作方式：

- 1 虛擬機器會將 HTTP GET 傳送至 `http://169.254.169.254:80` 以要求某些中繼資料。
- 2 連線至與虛擬機器相同的邏輯交換器的中繼資料 Proxy 伺服器會讀取要求、對標頭進行適當變更，以及將要求轉送至 Nova API 伺服器。
- 3 Nova API 伺服器會從 Neutron 伺服器要求及接收關於虛擬機器的資訊。
- 4 Nova API 伺服器會尋找中繼資料並將其傳送至中繼資料 Proxy 伺服器。
- 5 中繼資料 Proxy 伺服器會將中繼資料轉送至虛擬機器。

中繼資料 Proxy 伺服器會在 NSX Edge 節點上執行。如需高可用性，您可以將中繼資料 Proxy 設定為在 NSX Edge 叢集中的兩個以上 NSX Edge 節點上執行。

本章包含以下主題：

- [新增中繼資料 Proxy 伺服器](#)
- [將中繼資料 Proxy 伺服器連結至邏輯交換器](#)
- [將中繼資料 Proxy 伺服器與邏輯交換器中斷連結](#)

### 新增中繼資料 Proxy 伺服器

中繼資料 Proxy 伺服器可讓虛擬機器從 OpenStack Nova API 伺服器擷取中繼資料。

#### 先決條件

請確認您已建立 Edge 叢集。如需詳細資訊，請參閱 NSX-T 安裝指南。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **DHCP > 中繼資料 Proxy (DHCP > Metadata Proxies)**。
- 3 按一下 **新增 (Add)**。
- 4 輸入中繼資料 Proxy 伺服器的名稱。



- 5 (可選) 輸入說明。
- 6 輸入 Nova 伺服器的 URL。
- 7 輸入 secret 參數。
- 8 從下拉式清單中選取 Edge 叢集。
- 9 (可選) 選取 Edge 叢集的成員。

例如：

## 新增中繼資料 Proxy 伺服器



名稱 *	metadata-proxy-1
說明	<div></div>
Nova 伺服器 URL *	http://123.1.1.1
密碼 *	●●●●●●
Edge 叢集 *	EDGECLUSTER1
成員	53293932-b4b0-11e8-8ae0-000c298761d2

取消

新增

### 後續步驟

將中繼資料 Proxy 伺服器連結到邏輯交換器。

## 將中繼資料 Proxy 伺服器連結至邏輯交換器

若要將中繼資料 Proxy 服務提供給連線至邏輯交換器的虛擬機器，您必須將中繼資料 Proxy 伺服器連結至交換器。

### 先決條件

確認您已建立邏輯交換器。如需詳細資訊，請參閱[建立邏輯交換器](#)。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **DHCP > 中繼資料 Proxy (DHCP > Metadata Proxies)**。
- 3 選取中繼資料 Proxy 伺服器。
- 4 選取功能表選項**動作 (Actions) > 連結至邏輯交換器 (Attach to Logical Switch)**
- 5 從下拉式清單中選取邏輯交換器。

您還可以將中繼資料 Proxy 伺服器連結至邏輯交換器，方法為導覽至**交換 > 交換器 (Switching > Switches)**，接著選取交換器，然後選取功能表選項**動作 (Actions) > 連結中繼資料 Proxy (Attach Metadata Proxy)**。

## 將中繼資料 Proxy 伺服器與邏輯交換器中斷連結

若要停止對連線至邏輯交換器的虛擬機器提供中繼資料 Proxy 服務，或是要使用不同的中繼資料 Proxy 伺服器，您可以將中繼資料 Proxy 伺服器與邏輯交換器中斷連結。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **DHCP > 中繼資料 Proxy (DHCP > Metadata Proxies)**。
- 3 選取中繼資料 Proxy 伺服器。
- 4 選取功能表選項**動作 (Actions) > 與邏輯交換器中斷連結 (Detach from Logical Switch)**
- 5 從下拉式清單中選取邏輯交換器。

您也可以導覽至**交換 > 交換器 (Switching > Switches)**、選取交換器，然後選取功能表選項**動作 (Actions) > 將中繼資料 Proxy 中斷連結 (Detach Metadata Proxy)**，以將中繼資料 Proxy 伺服器與邏輯交換器中斷連結。

## 作業和管理

您可能需要變更已安裝應用裝置的組態，例如新增授權、憑證以及變更密碼等。您也需要執行一些定期維護工作，包括執行備份。此外，我們提供一些工具，可協助您尋找屬於 **NSX-T** 基礎結構一部分的應用裝置以及由 **NSX-T** 建立的邏輯網路等相關資訊，包括遠端系統記錄、**Traceflow** 以及連接埠連線。

本章包含以下主題：

- [新增授權金鑰](#)
- [管理使用者帳戶](#)
- [設定憑證](#)
- [設定應用裝置](#)
- [管理標籤](#)
- [搜尋物件](#)
- [尋找遠端伺服器的 SSH 指紋](#)
- [備份和還原 NSX Manager](#)
- [管理應用裝置和應用裝置叢集](#)
- [記錄系統訊息](#)
- [設定 IPFIX](#)
- [使用 Traceflow 追蹤封包的路徑](#)
- [檢視連接埠連線資訊](#)
- [監控邏輯交換器連接埠活動](#)
- [監控連接埠鏡像工作階段](#)
- [監控網狀架構節點](#)
- [收集支援服務包](#)

### 新增授權金鑰

您可以使用 **NSX Manager UI** 來新增一或多個授權金鑰。

我們提供下列非評估版授權類型：

- 標準
- 進階
- Enterprise

安裝 NSX Manager 時，預先安裝的評估授權會生效，可供使用 60 天。評估授權可提供 Enterprise 授權的全部功能。您無法安裝或取消指派評估授權。

您可以安裝一或多個非評估版授權，但針對每種類型僅能安裝一個金鑰。安裝 Standard、Advanced 或 Enterprise 授權後，評估授權便不再提供使用。您也可以取消指派非評估版授權。如果取消指派所有非評估版授權，則系統會還原評估授權。

如果您有相同授權類型的多個金鑰，且想要合併這些金鑰，則必須前往 <https://my.vmware.com> 並使用合併金鑰功能。NSX Manager UI 不提供此功能。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 (System) > 組態 (Configuration) > 授權 (License)**。
- 3 按一下**新增**，輸入授權金鑰。
- 4 按一下**儲存**。

## 管理使用者帳戶

NSX-T 應用裝置具備本機管理使用者帳戶 **admin**。您無法建立或刪除使用者。

## 變更 Admin 密碼

您已變更任何 NSX-T 應用裝置上的 Admin 使用者密碼。

#### 程序

- 1 登入 NSX Manager CLI。
- 2 執行 **set user** 命令。

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

密碼必須符合這些密碼複雜性需求：

- 長度至少 8 個字元
- 至少 1 個大寫字元
- 至少 1 個小寫字元

- 至少 1 個數字字元
- 至少 1 個特殊字元

## 帳戶鎖定

連續五次登入嘗試失敗後，系統會將管理員帳戶鎖定 15 分鐘。

針對 NSX Manager、NSX Controller 和 NSX Edge 節點，在第五次連續五次登入嘗試失敗後，系統會將管理員帳戶鎖定 15 分鐘。若要重設遭鎖定的帳戶，請等候 15 分鐘後再次登入。這是刻意設計的行為，因為它會使攻擊者無法透過觀察到登入失敗訊息從「密碼錯誤」變更為「帳戶鎖定」，藉此得知帳戶的存在。

**備註** 這會透過 SSH 或透過主控台套用至管理員登入。

## 設定憑證

您可以在 NSX Manager 中產生憑證簽署要求 (CSR)，然後將其傳送給憑證授權機構 (CA) 以取得伺服器憑證。

CSR 也可以用來產生自我簽署憑證。如果您擁有現有憑證或 CA 憑證，則可將其匯入以供使用。您也可以匯入包含已撤銷憑證的憑證撤銷清單 (CRL)。

## 建立憑證簽署要求檔案

憑證簽署要求 (CSR) 是一種包含特定資訊 (例如組織名稱、一般名稱、位置和國家/地區) 的加密文字。將 CSR 檔案傳送至憑證授權機構 (CA) 以申請數位身分識別憑證。

### 先決條件

- 收集您填妥 CSR 檔案所需的資訊。您必須瞭解伺服器和組織單位的 FQDN、組織、城市、州和國家/地區。
- 確認公用及私密金鑰配對可供使用。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的 **系統 (System) > 設定 (Settings)**。
- 3 按一下 **憑證 (Certificates)** 索引標籤。
- 4 從下拉式功能表中選取 **CSR (CSRs)**。
- 5 按一下 **產生 CSR (Generate CSR)**。
- 6 完成 CSR 檔案詳細資料。

選項	說明
名稱	指派憑證的名稱。
一般名稱	輸入您伺服器的完整網域名稱 (FQDN)。例如，test.vmware.com。

選項	說明
組織名稱	輸入組織名稱與適用尾碼。 例如，VMware Inc。
組織單位	輸入您組織中處理此憑證的部門 例如，IT 部門。
位置	新增您組織所在的城市。 例如，Palo Alto。
州	新增您組織所在的州。 例如，加州。
國家/地區	新增您組織所在的國家/地區。 例如，美國 (US)。
訊息演算法	設定憑證的加密演算法。 RSA 加密 - 用於數位簽章及訊息的加密。因此，建立加密的 Token 時會比 DSA 慢，但分析及確認此 Token 時較快。此加密在解密時較慢而加密時較快。 DSA 加密 - 用於數位簽章。因此，建立加密的 Token 時會比 RSA 快，但分析及確認此 Token 時較慢。此加密在解密時較快而加密時較慢。
金鑰大小	設定加密演算法的金鑰位元大小。 預設值 2048 已足夠，除非您特別需要不同的金鑰大小。許多 CA 需要至少 2048 的值。較大的金鑰大小更為安全，但對於效能影響較大。
說明	輸入特定詳細資料以協助您在日後識別此憑證。

## 7 按一下儲存 (Save)。

自訂 CSR 會顯示為連結。

## 8 選取 CSR，然後按一下動作 (Actions)。

## 9 從下拉式功能表中選取下載 CSR PEM (Download CSR PEM)。

您可以儲存 CSR PEM 檔案以作為記錄及 CA 提交。

## 10 使用 CSR 檔案的內容以根據 CA 註冊程序將憑證要求提交至 CA。

CA 會根據 CSR 檔案中的資訊建立伺服器憑證、使用其私密金鑰進行簽署，以及將憑證傳送給您。CA 也會將根 CA 憑證傳送給您。

## 匯入 CA 憑證

您可以匯入已簽署的 CA 憑證以作為公司的臨時 CA。匯入憑證後，您便有權簽署自己的憑證。

### 先決條件

確認 CA 憑證可供使用。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的系統 (System) > 設定 (Settings)。
- 3 按一下 [憑證] 索引標籤上的匯入 (Import)。

- 4 從下拉式功能表選取**匯入 CA 憑證 (Import CA Certificate)**，然後輸入憑證詳細資料。

選項	說明
名稱	指派名稱給 CA 憑證。
憑證內容	瀏覽至電腦上的 CA 憑證檔案，然後新增該檔案。
說明	輸入此 CA 憑證所含內容的摘要。

- 5 按一下**儲存 (Save)**。

您現在即可簽署自己的憑證。

## 匯入憑證

您可以匯入具有私密金鑰的憑證，以便建立自我簽署憑證。

### 先決條件

確認可以使用憑證。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 (System) > 設定 (Settings)**。
- 3 按一下 [憑證] 索引標籤上的**匯入 (Import)**。
- 4 從下拉式功能表選取**匯入憑證 (Import Certificate)**，然後輸入憑證詳細資料。

選項	說明
名稱	指派名稱給 CA 憑證。
憑證內容	瀏覽到電腦上的憑證檔案，然後新增該檔案。
私密金鑰	瀏覽到電腦上的私密金鑰檔案，然後新增該檔案。
密碼	新增此憑證的密碼。
說明	輸入此憑證所含內容的摘要。

- 5 按一下**儲存 (Save)**。

您現在即可建立自己的自我簽署憑證。

## 建立自我簽署的憑證

使用自我簽署的憑證可能會比使用受信任憑證更不安全。

當您使用自我簽署的憑證時，用戶端使用者會收到警告訊息，例如無效的安全性憑證。然後用戶端使用者必須在第一次連線至伺服器以繼續進行時接受自我簽署的憑證。允許用戶端使用者選取此選項會比其他授權方法提供降低的安全性。

## 先決條件

確認 CSR 可用。請參閱[建立憑證簽署要求檔案](#)。

## 程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**系統 (System) > 設定 (Settings)**。
- 3 按一下**憑證 (Certificates)**索引標籤。
- 4 從下拉式功能表中選取 **CSR (CSRs)**。
- 5 選取現有的 CSR。
- 6 按一下**動作 (Actions)**然後從下拉式功能表中選取 **CSR 的自我簽署憑證 (Self Sign Certificate for CSR)**。
- 7 輸入自我簽署憑證有效天數。  
預設時間範圍是 10 年。
- 8 按一下**儲存 (Save)**。

自我簽署的憑證會顯示在**憑證 (Certificate)**清單中。憑證類型會指定為自我簽署。

## 取代憑證

如果您需要取代憑證，例如可能您的憑證已到期，則可以使用 API 要求來取代現有憑證。

## 先決條件

確認 NSX Manager 中可以使用憑證。請參閱[建立自我簽署的憑證與匯入憑證](#)。

## 程序

- 1 選取導覽面板中的**系統 (System) > 設定 (Settings)**。
- 2 按一下**憑證 (Certificates)**索引標籤，並從下拉式功能表選取**憑證 (Certificates)**。
- 3 按一下您要使用的憑證 ID，從快顯視窗中複製憑證 ID。
- 4 傳送 POST `/api/v1/node/services/http?action=apply_certificate&certificate_id=<CertificateID>` API 要求來取代現有憑證。

```
POST https://192.168.110.201/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

API 要求會重新啟動 HTTP 服務，讓服務可以開始使用新憑證。當 POST 要求成功時，回應代碼為 200 已接受。



## 匯入憑證撤銷清單

憑證撤銷清單 (CRL) 是訂閱者及其憑證狀態的清單。當潛在使用者嘗試存取伺服器時，伺服器會根據該特定使用者的 CRL 項目拒絕其存取。

清單中包含下列項目：

- 遭撤銷的憑證和撤銷的原因
- 憑證的核發日期
- 核發憑證的實體
- 下一版本的預定日期

### 先決條件

確認有可用的 CRL。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 (System) > 設定 (Settings)**。
- 3 按一下**憑證 (Certificates)**索引標籤。
- 4 從下拉式功能表中選取 **CRL (CRLs)**。
- 5 按一下**匯入 (Import)**，然後新增 CRL 詳細資料。

選項	說明
名稱	將名稱指派給 CRL。
憑證內容	複製 CRL 中的所有項目，並將其貼上至此區段中。 範例 CRL。 <pre>-----BEGIN X509 CRL----- MIIB0DCB4zANBgqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMaoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEhMBk G A1UEAxMSU1NMZW5IGRlbW8gc2VydMvyFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFIIwEgIBARcNOTUxMDA5MjMzMjA1wJASAgEDFw05NTEyMDEwMTAwMD a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCsq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi +jZM7Y78TfAzG4jJn/E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
說明	輸入此 CRL 所含內容的摘要。

- 6 按一下**儲存 (Save)**。

匯入的 CRL 會顯示為連結。

## 設定應用裝置

部分系統組態工作必須使用命令列或 API 來完成。

如需完整的命令列介面資訊，請參閱 NSX-T 命令列介面參考。如需完整的 API 資訊，請參閱 NSX-T API 指南。

表格 11-1. 系統組態命令和 API 要求。

工作	命令列 (NSX Manager、NSX Controller、NSX Edge)	API 要求 (僅限 NSX Manager)
設定系統時區	set timezone <timezone>	PUT https://<nsx-mgr>/api/v1/node
設定 NTP 伺服器	set ntp-server <ntp-server>	PUT https://<nsx-mgr>/api/v1/node/services/ntp
設定 DNS 伺服器	set name-servers <dns-server>	PUT https://<nsx-mgr>/api/v1/node/network/name-servers
設定 DNS 搜尋網域	set search-domains <domain>	PUT https://<nsx-mgr>/api/v1/node/network/search-domains

## 管理標籤

您可以將標籤新增至物件，以便更易於搜尋物件。為物件指定標籤時，您也可以指定範圍。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 導覽至物件類別。  
例如，導覽至**交換 (Switching) > 交換器 (Switches)**。
- 3 選取物件。
- 4 選取功能表選項**動作 (Actions) > 管理標籤 (Manage Tags)**。
- 5 新增或刪除標籤。

選項	動作
新增標籤	按一下 <b>新增 (Add)</b> 以指定標籤，並選擇性地指定範圍。
刪除標籤	選取現有的標籤，然後按一下 <b>刪除 (Delete)</b> 。

一個邏輯連接埠最多可以有 15 個標籤。所有其他物件最多可以有 10 個標籤。

- 6 按一下**儲存 (Save)**。

## 搜尋物件

您可以使用各種不同的準則來搜尋物件。

以下是可供搜尋使用的準則：

- 資源類型
- 名稱
- 說明
- 建立時間
- 修改時間
- 建立者
- 修改者
- 標籤

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 按一下位於主視窗窗格右上角的放大鏡圖示。
- 3 針對物件或物件類型輸入規則運算式搜尋模式。

依預設會錨定搜尋模式，即代表已假設字串錨點開頭為 `^`，而字串錨點結尾為 `$`。請勿在搜尋模式中使用這些錨點。例如，如果您想要搜尋開頭為「Logical」的資源，搜尋模式會是 `Logical.*`。如果您想要搜尋結尾為「Switch」的資源，搜尋模式會是 `.*Switch`。

- 4 在顯示結果的視窗中，按一下位於視窗底部的[檢視結果 \(View ... results\)](#)連結，以開啟可讓您縮小搜尋範圍的搜尋窗格。
- 5 指定一或多個用來縮小搜尋範圍的準則。

## 尋找遠端伺服器的 SSH 指紋

某些涉及往來於遠端伺服器複製檔案之 API 要求會需要您在要求主體中提供遠端伺服器的 SSH 指紋。SSH 指紋衍生自遠端伺服器的主機金鑰。

為了透過 SSH 連線，NSX Manager 和遠端伺服器必須具有共同的主機金鑰類型。如果有多個共同的主機金鑰類型，則系統會根據 NSX Manager 上 HostKeyAlgorithm 組態的使用項目來決定偏好的項目。

擁有遠端伺服器的指紋有助於確認您連線至正確的伺服器，並可保護您避免受到攔截式攻擊。您可以向遠端伺服器的管理員要求提供伺服器的 SSH 指紋。或者，您也可以連線至遠端伺服器以尋找指紋。透過主控台連線至伺服器，比透過網路連線更為安全。

NSX Manager 應用裝置是以 Ubuntu 14.04 為基礎，並使用預設的 HostKeyAlgorithm 順序。下表列出 NSX Manager 上依預設存在的金鑰，且會依照最高偏好至最低偏好的順序列出。

表格 11-2. 依照偏好順序列出的 NSX Manager 主機金鑰

NSX Manager 上存在的主機金鑰類型	該主機金鑰類型的預設位置
ECDSA (256 位元)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

表格 11-2. 依照偏好順序列出的 NSX Manager 主機金鑰 (續)

NSX Manager 上存在的主機金鑰類型	該主機金鑰類型的預設位置
RSA	/etc/ssh/ssh_host_rsa_key.pub
DSA	/etc/ssh/ssh_host_dsa_key.pub

## 程序

### 1 登入遠端伺服器的 CLI。

使用主控台進行登入，比透過網路登入更為安全。

### 2 列出 /etc/ssh 目錄中的公開金鑰檔案。

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

### 3 將可用金鑰和 HostKeyAlgorithm 順序進行比較。

此範例中有三個 SSH 金鑰，即 DSA、RSA 和 ED25519。ED25519 在偏好順序中排名最高，因此 NSX Manager 在連線至遠端伺服器時會使用此金鑰。

### 4 取得偏好金鑰的指紋。

```
$ ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub
256 d0:21:3e:ec:52:ff:19:a9:e7:71:b5:7f:63:23:57:f7 root@ubuntu (ED25519)
```

金鑰的指紋是 d0:21:3e:ec:52:ff:19:a9:e7:71:b5:7f:63:23:57:f7。

**備註** 在備份和還原 API 要求時，您必須移除 SSH 指紋中的冒號。

## 備份和還原 NSX Manager

如果 NSX Manager 虛擬應用裝置無法運作，您可從備份還原該裝置的內容。NSX Manager 會儲存虛擬網路所需的狀態。如果 NSX Manager 應用裝置無法運作，資料平面將不會受到影響，但無法進行組態變更。

您可以透過兩種備份方法建立三種類型的備份：

**叢集備份** 此備份包含虛擬網路所需的狀態。

**節點備份** 此備份包含 NSX Manager 應用裝置組態。

**詳細目錄備份** 此備份包含一組 ESX 以及 KVM 主機與 Edge。系統會在偵測和修正管理平面所需狀態，與這些主機之間不一致的還原作業執行期間使用此資訊。

共有兩種備份方法：

**NSX Manager 手動節點備份和叢集備份** 您可以視需要隨時執行手動節點和叢集備份。

**NSX Manager 自動節點備份、叢集備份和詳細目錄備份** 自動備份會根據您設定的排程執行。強烈建議您使用自動備份。請參閱[排程自動備份](#)。

為了確保備份內容為最新版本，請設定自動備份。請務必定期執行叢集和詳細目錄備份。

您可以將 NSX-T 組態還原成任何叢集備份中擷取的狀態。還原備份時，您必須還原至執行與備份應用裝置相同 NSX Manager 版本的新 NSX Manager 應用裝置。

Hypervisor、NSX Manager 應用裝置和 NSX Controller 應用裝置必須具有靜態管理 IP 位址，才能進行備份和還原。不支援變更管理 IP 位址。不支援使用 DHCP 來指派 NSX Manager 和 NSX Controller 應用裝置的管理 IP 位址。只有 DHCP 伺服器已設定為一律將相同 IP 位址提供給指定的 Hypervisor 時，才支援使用 DHCP 來指派 Hypervisor 的管理 IP 位址。

## 備份 NSX Manager 組態

NSX Manager 組態備份由 NSX Manager 節點備份、叢集備份和詳細目錄備份所組成。

### 程序

#### 1 設定備份位置

系統會將備份儲存至 NSX Manager 可存取的遠端 SFTP 位置。您必須先設定備份位置才能進行備份。

#### 2 排程自動備份

您可以排程頻繁的備份來還原無法運作的 NSX Manager 及其組態資料。自動備份依預設為停用。您可以排程在每週的特定幾天，或根據指定時間間隔進行自動備份。強烈建議您使用排程備份。

## 設定備份位置

系統會將備份儲存至 NSX Manager 可存取的遠端 SFTP 位置。您必須先設定備份位置才能進行備份。

### 程序

- 1 登入 NSX Manager 虛擬應用裝置。
- 2 按一下 **系統 > 公程式 > 備份 (System > Utilities > Backup)**。
- 3 若要提供備份位置的存取認證，請按一下頁面右上角的 **編輯 (Edit)**。
- 4 按一下 **自動備份 (Automatic Backup)** 切換按鈕以啟用自動備份。
- 5 輸入 SFTP 伺服器的 IP 位址或主機名稱。
- 6 視需要編輯預設連接埠。
- 7 輸入登入 SFTP 伺服器所需的使用者名稱和密碼。

- 8 在目的地目錄 (**Destination Directory**)欄位中，輸入儲存備份的絕對目錄路徑。
- 9 輸入用來加密備份資料的複雜密碼。  
您需要此複雜密碼才能還原備份。如果您忘記備份複雜密碼，則無法還原任何備份。
- 10 輸入儲存備份之伺服器的 SSH 指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。
- 11 按一下**儲存 (Save)**。
- 12 按一下頁面底部的**立即備份 (Backup Now)**以確認可將檔案寫入至 SFTP 伺服器。

#### 後續步驟

排程自動備份。

### 排程自動備份

您可以排程頻繁的備份來還原無法運作的 **NSX Manager** 及其組態資料。自動備份依預設為停用。您可以排程在每週的特定幾天，或根據指定時間間隔進行自動備份。強烈建議您使用排程備份。

#### 先決條件

- 決定適當的備份位置。選取可防止單一失敗點的位置。例如，請勿將備份放在和應用裝置相同的檔案存放區。若該檔案存放區上發生失敗，則會一併影響應用裝置及其備份。
- 尋找備份存放所在之伺服器的 SSH 指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。備份和還原 API 要求會要求 SSH 指紋不得包含冒號。

#### 程序

- 1 登入 **NSX Manager** 虛擬應用裝置。
- 2 按一下**系統 > 公用程式 > 備份 (System > Utilities > Backup)**。
- 3 按一下頁面右上角的**編輯 (Edit)**。
- 4 按一下**檔案伺服器 (File Server)**，然後確認是否已啟用自動備份。
- 5 按一下頁面頂端的**排程 (Schedule)**。
- 6 若為節點/叢集備份，按一下**每週 (Weekly)**，然後將備份日期和時間設定至 SFTP 伺服器；或按一下**時間間隔 (Interval)**，然後設定備份時間。
- 7 詳細目錄備份依預設為每 30 秒執行一次，且應頻繁執行。請視需要接受或變更預設設定。
- 8 按一下**儲存 (Save)**。

---

**備註** 第一次每週排程備份會於指定的週間日與時間執行。第一次時間間隔排程備份會在儲存已啟用自動備份的備份組態後立即執行。

---

**NSX Manager** 會儲存三種不同的備份檔案：節點層級、叢集層級和詳細目錄。系統會將備份檔案儲存至備份組態中指定的 SFTP 伺服器目錄。在該目錄中，系統將檔案儲存於下列目錄：

- /<使用者指定的目錄>/cluster-node-backups (叢集和節點備份)

- /<使用者指定的目錄>/inventory-summary (詳細目錄備份)

## 還原 NSX Manager 組態

如果您的 NSX Manager 應用裝置無法運作，而您想採取建議的備份動作，則可以還原 NSX Manager 應用裝置。您將需要建立備份時指定的複雜密碼才能還原備份。

### 程序

#### 1 準備還原 NSX Manager 備份

在還原 NSX Manager 備份前，您必須先安裝新的 NSX Manager 應用裝置。新的 NSX Manager 必須部署與先前 NSX Manager 相同的管理 IP 位址。

#### 2 還原叢集備份

叢集備份可用來還原需要的網路狀態。您必須先還原叢集備份，才能還原節點備份。

#### 3 還原 NSX Manager 節點備份

節點備份會還原應用裝置組態，讓 NSX Controller 叢集連線至該應用裝置。您必須先還原叢集備份，才能還原節點備份。所選節點備份檔案的時間戳記需與叢集備份檔案的時間戳記相同。

#### 4 下載備份和還原協助程式指令碼

您必須從 NSX Manager 下載備份和還原協助程式指令碼。

#### 5 還原上次叢集備份後進行的網狀架構變更

備份和還原協助程式指令碼會在備份還原後，將需要的狀態與該指令碼擷取的最新網狀架構狀態進行比對，並提供讓網狀架構狀態在還原備份後符合所需狀態的指示。

#### 6 還原 NSX Controller 叢集

如果無法復原 NSX Controller 叢集，或您因叢集成員資格變更而需要取代一或多個控制器，則應還原整個控制器叢集。

## 準備還原 NSX Manager 備份

在還原 NSX Manager 備份前，您必須先安裝新的 NSX Manager 應用裝置。新的 NSX Manager 必須部署與先前 NSX Manager 相同的管理 IP 位址。

### 先決條件

- 確認您的節點、叢集和最新的詳細目錄備份檔案皆可用於還原。
- 確認您擁有節點和叢集備份檔案的複雜密碼。
- 確認您知道用來建立備份的 NSX Manager 版本，且擁有相同版本的正確安裝檔案 (OVA、OVF 或 QCOW2)。
- 確認您知道指派給用來建立節點備份之 NSX Manager 的 IP 位址。
- 確認在還原程序完成前，沒有人將嘗試對 NSX Manager 進行組態變更。

### 程序

- 1 如果舊的 NSX Manager 應用裝置仍在執行中 (例如，您還原是為了復原已進行的升級)，請將其關機。

## 2 安裝新的 NSX Manager 應用裝置。

- 新的 NSX Manager 應用裝置的版本必須與用來建立備份的應用裝置具有相同版本。
- 您必須使用用來建立節點備份之 NSX Manager 的 IP 位址來設定此應用裝置。

如需有關這些步驟的資訊和指示，請參閱 NSX-T 安裝指南。

### 後續步驟

還原叢集備份。

## 還原叢集備份

叢集備份可用來還原需要的網路狀態。您必須先還原叢集備份，才能還原節點備份。

### 先決條件

- 尋找備份存放所在之伺服器的 SSH 指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。備份和還原 API 要求會要求 SSH 指紋不得包含冒號。

### 程序

#### 1 確認 NSX Manager 的狀態是 STABLE 再還原備份。

```
GET https://192.168.110.201/api/v1/cluster/status
{
  "control_cluster_status" : {
    "status" : "NO_CONTROLLERS"
  },
  "mgmt_cluster_status" : {
    "online_nodes" : [ {
      "mgmt_cluster_listen_ip_address" : "192.168.110.201",
      "uuid" : "422E901F-B167-DA0A-951F-C0278CA8A4BA"
    } ],
    "status" : "STABLE"
  }
}
```

**備註** 在節點備份還原前，控制叢集不會連線至 NSX Manager，因此控制叢集狀態是 NO\_CONTROLLERS。

#### 2 傳送叢集備份還原 API 要求 POST /api/v1/cluster/backups?action=restore，該要求會從遠端位置複製備份檔案，並在 NSX Manager 應用裝置上還原該檔案。請在 API 要求中指定備份檔案和位置資訊。

#### 還原要求欄位：

##### 複雜密碼

建立備份時所指定的複雜密碼。如果您不知道此密碼，則無法還原此備份。

##### 伺服器

備份檔案儲存所在的遠端伺服器。

##### uri

遠端伺服器上的備份檔案路徑。



**還原要求欄位：**

<b>ssh_fingerprint</b>	備份檔案儲存所在之遠端伺服器的 SSH 指紋。請參閱 <a href="#">尋找遠端伺服器的 SSH 指紋</a> 。
<b>使用者名稱</b>	用來登入遠端伺服器以複製備份檔案的使用者名稱。
<b>密碼</b>	用來登入遠端伺服器以複製備份檔案的密碼。

**叢集備份還原要求範例：**

```
POST https://192.168.110.201/api/v1/cluster/backups?action=restore

{
  "restore_file": {
    "passphrase" : "7Taspa5anecR",
    "file_store" : "remote",
    "server" : "192.168.120.151",
    "uri" : "/vol0/backups/backup-cluster-20160314.zip",
    "protocol" : {
      "name" : "scp",
      "ssh_fingerprint" : "b508dfc65562e46e95707c25baf246f1",
      "authentication_scheme" : {
        "scheme_name" : "password",
        "username" : "admin" ,
        "password" : "4uhasWak"
      }
    }
  }
}
```

- 3 等待系統再次回到穩定狀態。
- 4 停用自動備份。
  - a 登入 NSX Manager 虛擬應用裝置。
  - b 按一下 **系統 > 公用程式 > 備份 (System > Utilities > Backup)**。
  - c 按一下頁面右上角的 **編輯 (Edit)**。
  - d 按一下 **自動備份 (Automatic Backup)** 切換按鈕以停用自動備份。

備份和還原協助程式指令碼執行完畢後，您便可重新啟用自動備份。

**後續步驟**

請先重新啟動所有 NSX Controller 來移除所有快取資料，再還原節點備份以及同步 NSX Manager 和 NSX Controller。請參閱[將 NSX Controller 叢集成員重新開機](#)。

## 還原 NSX Manager 節點備份

節點備份會還原應用裝置組態，讓 NSX Controller 叢集連線至該應用裝置。您必須先還原叢集備份，才能還原節點備份。所選節點備份檔案的時間戳記需與叢集備份檔案的時間戳記相同。



**注意** 您必須先還原叢集備份，才能還原節點備份。還原節點備份時，控制器現在會與 NSX Manager 進行通訊，並更新實現的網路狀態以符合 NSX Manager 上設定的所需網路狀態。如果未還原叢集備份，則不會設定需要的網路狀態，而且目前實現的網路狀態將被銷毀。

### 先決條件

- 在 NSX Manager 上完成叢集備份的還原。請參閱[還原叢集備份](#)。
- 確認您已擁有 NSX Manager 的備份。請參閱[備份 NSX Manager 組態](#)。
- 尋找備份存放所在之伺服器的 SSH 指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。備份和還原 API 要求會要求 SSH 指紋不得包含冒號。

### 程序

- 1 確認 NSX Manager 的狀態是 STABLE 再還原備份。

```
GET https://192.168.110.201/api/v1/cluster/status
{
  "control_cluster_status" : {
    "status" : "NO_CONTROLLERS"
  },
  "mgmt_cluster_status" : {
    "online_nodes" : [ {
      "mgmt_cluster_listen_ip_address" : "192.168.110.201",
      "uuid" : "422E901F-B167-DA0A-951F-C0278CA8A4BA"
    } ],
    "status" : "STABLE"
  }
}
```

**備註** 在節點備份還原前，控制叢集不會連線至 NSX Manager，因此控制叢集狀態是 NO\_CONTROLLERS。

- 2 傳送節點備份還原 API 要求 POST /api/v1/node/backups?action=restore，該要求會從遠端位置複製備份檔案，並在 NSX Manager 應用裝置上還原該檔案。請在 API 要求中指定備份檔案和位置資訊。

### 還原要求欄位：

複雜密碼	建立備份時所指定的複雜密碼。如果您不知道此密碼，則無法還原此備份。
伺服器	備份檔案儲存所在的遠端伺服器。
uri	遠端伺服器上的備份檔案路徑。

還原要求欄位：

<b>ssh_fingerprint</b>	備份檔案儲存所在之遠端伺服器的 SSH 指紋。請參閱 <a href="#">尋找遠端伺服器的 SSH 指紋</a> 。
<b>使用者名稱</b>	用來登入遠端伺服器以複製備份檔案的使用者名稱。
<b>密碼</b>	用來登入遠端伺服器以複製備份檔案的密碼。

節點備份還原要求範例：

```
POST https://192.168.110.201/api/v1/node/backups?action=restore

{
  "restore_file": {
    "passphrase" : "7Taspa5anecR",
    "file_store" : "remote",
    "server" : "192.168.120.151",
    "uri" : "/vol0/backups/backup-node-192.168.110.201-20160314.bak",
    "protocol" : {
      "name" : "scp",
      "ssh_fingerprint" : "b508dfc65562e46e95707c25baf246f1",
      "authentication_scheme" : {
        "scheme_name" : "password",
        "username" : "admin" ,
        "password" : "4uhasWak"
      }
    }
  }
}
```

## 後續步驟

下載備份和還原協助程式指令碼。

## 下載備份和還原協助程式指令碼

您必須從 NSX Manager 下載備份和還原協助程式指令碼。

### 先決條件

- 確認用來執行協助程式指令碼的機器符合系統需求。協助程式指令碼需要 python 2 和 TLS 1.2，並已在 Ubuntu 14.04 上進行過確認。

### 程序

- ◆ 下載備份和還原協助程式指令碼。您可以透過命令列或 API 完成此動作。
  - 透過命令列：

執行 `copy file` 命令以將指令碼複製到遠端伺服器。`url` 引數會使用 URL 標準語法 (例如 `scp://user@server/home/path/to/destination`) 來指定指令碼的目的地。

```
nsx-manager-1> copy file backup_restore_helper.py url
scp://backups@192.168.120.151/vol0/backups/scripts/
```

- 透過 API:

傳送此 API 要求，並將輸出儲存至名為 `backup_restore_helper.py` 的檔案。

```
GET https://nsx-manager-1/api/v1/node/file-store/backup_restore_helper.py/data
```

## 後續步驟

還原上次叢集備份後進行的網狀架構變更。

## 還原上次叢集備份後進行的網狀架構變更

備份和還原協助程式指令碼會在備份還原後，將需要的狀態與該指令碼擷取的最新網狀架構狀態進行比對，並提供讓網狀架構狀態在還原備份後符合所需狀態的指示。

### 先決條件

- 確認您已下載備份和還原協助程式指令碼。
- 確認您已從 SFTP 伺服器下載最新的詳細目錄備份。

### 程序

- 1 登入至已下載或複製備份和還原協助程式指令碼的機器。
- 2 執行備份和還原協助程式指令碼，並使用 `-d` 選項來指定要使用的檢查點 (詳細目錄) 檔案。

請提供下列資訊：

<code>-m</code>	NSX Manager IP 位址
<code>-u</code>	NSX Manager 使用者名稱
<code>-p</code>	NSX Manager 密碼
<code>-d</code>	檢查點 (最新詳細目錄備份) 檔案名稱

```
$ python backup_restore_helper.py -m 192.168.110.201 -u admin -p <password> -d
backups/backup_restore_checkpoint_20160318_013354.json
```

- 3 遵循 `backup_restore_helper.py` 指令碼輸出中的指示來更新網狀架構狀態以符合所需狀態。

## 還原 NSX Controller 叢集

如果無法復原 NSX Controller 叢集，或您因叢集成員資格變更而需要取代一或多個控制器，則應還原整個控制器叢集。

在還原控制器叢集前，您必須將管理層所知的叢集成員資格與控制器所知的實際成員資格進行比對，來判斷控制叢集成員資格是否有變更。如果在備份後進行變更，成員資格便會不同。

- 如果無法復原整個叢集，請參閱[重新部署 NSX Controller 叢集](#)。
- 遵循以下步驟以判斷叢集成員資格是否已變更；若已變更，請還原叢集。

#### 先決條件

- 確認您的叢集層級備份為最新版本。
- 執行叢集層級還原。請參閱[還原叢集備份](#)。

#### 程序

- 1 登入 NSX Manager 的 CLI，然後執行 `get management-cluster status` 命令。
- 2 登入 NSX Controller 的 CLI，然後執行 `get managers` 命令以確保控制器登錄至 Manager。
- 3 執行 `get control-cluster status` 命令。
- 4 若要判斷成員資格是否已變更，請將 `get management-cluster status` 命令輸出中的 IP 位址和 `get control-cluster status` 命令輸出中的 IP 位址進行比對。  
如果兩個輸出的所有 IP 位址皆相同，即不需執行任何動作。如果有 IP 位址不同，請繼續進行剩餘的步驟以還原整個控制器叢集。
- 5 登入 NSX Controller 的 CLI，透過執行 `get control-cluster status` 命令來判斷主控制器。  
主控制器輸出將顯示 `is master: true`。
- 6 在非主控制器上執行 `stop service <controller>` 命令。
- 7 登入主控制器，然後執行 `detach control-cluster <ip-address[:port]>` 命令以與上個步驟中的非主控制器中斷連結。
- 8 (選擇性步驟) 請只在 `get management-cluster status` 命令於 NSX Manager 上顯示此控制器時，再於 NSX Manager 上執行 `detach controller <uuid>` 命令來與此控制器中斷連結。
- 9 登入 NSX Controller 的 CLI，然後執行 `deactivate control-cluster` 命令。
- 10 透過下列命令移除啟動程序檔案和 UUID 檔案：`rm -r /opt/vmware/etc/bootstrap-config` 和 `rm -r /config/vmware/node-uuid`
- 11 針對剩餘的非主控制器執行步驟 6-10。
- 12 登入主控制器的 CLI，然後執行 `stop service <controller>` 命令。
- 13 在 NSX Manager 上執行 `detach controller <uuid>` 命令以與此控制器中斷連結。
- 14 登入主控制器的 CLI，然後執行 `deactivate control-cluster` 命令。
- 15 透過下列命令移除啟動程序檔案和 UUID 檔案：`rm -r /opt/vmware/etc/bootstrap-config` 和 `rm -r /config/vmware/node-uuid`
- 16 從 NSX Manager 執行 `get management-cluster status` 命令。如果輸出中仍顯示控制器，請執行 `detach controller <uuid>` 命令以和所有剩餘的控制器中斷連結。

## 後續步驟

遵循列出的順序來完成下列工作。

- 1 完成節點層級還原。請參閱[還原 NSX Manager 節點備份](#)。
- 2 請依照《NSX-T 安裝指南》所述，將 NSX Controller 與管理平面聯結。
- 3 請依照《NSX-T 安裝指南》所述，重新部署 NSX Controller 叢集。

## 管理應用裝置和應用裝置叢集

每個 NSX-T 安裝皆僅需要且僅支援一個 NSX Manager 執行個體。NSX Controller 叢集應有三個成員。NSX Edge 叢集應至少有兩個成員。

如果控制器或 Edge 叢集中的應用裝置變得無法運作，或您因故需將其移除，則可以將其取代為新的應用裝置。

---

**重要** 如果您對 NSX Controller 或 NSX Edge 叢集成員資格進行變更，則隨後必須進行叢集備份以便備份新組態。請參閱[備份和還原 NSX Manager](#)。

---

## 管理 NSX Manager

您可以使用 CLI 命令來檢查 NSX Manager 的狀態。如果 NSX Manager 無法運作且無法復原，則您可以將 NSX Manager 應用裝置重新開機。

## 取得 NSX Manager 狀態

您可以使用 CLI 命令來取得 NSX Manager 的狀態。

### 程序

- 1 登入 NSX Manager 的 CLI。
- 2 執行 `get management-cluster status` 命令。例如，

```
nsx-manager> get management-cluster status
Number of nodes in management cluster: 1
-192.168.110.105
Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52
- 192.168.110.53
- 192.168.110.51
Control cluster status: STABLE.
```

---

**備註** 即便結果說明是管理叢集，但仍可能僅有一個 NSX Manager 執行個體。

---

## 將 NSX Manager 重新開機

您可以使用 CLI 命令將 NSX Manager 重新開機，以從嚴重錯誤中復原。

### 程序

- 1 登入 NSX Manager 的 CLI。
- 2 執行 `reboot` 命令。例如，

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

## 管理 NSX Controller 叢集

NSX Controller 叢集應有三個成員。如果在進行疑難排解後，您判斷其中一個 NSX Controller 應用裝置無法復原，則可以將應用裝置新增至叢集來進行取代，或如有需要，也可以重新部署 NSX Controller 叢集。

NSX Controller 叢集必須擁有多數成員才能正常運作。如果三個成員中有兩個在線上，則表示叢集擁有多數成員。您應將離線的 NSX Controller 重新連線，以還原三個成員的叢集。如果無法將其重新連線，您可新增其他 NSX Controller 應用裝置來進行取代，以重新取得多數成員狀態。請參閱[取代 NSX Controller 叢集的成員](#)。

如果三個成員中僅有一個在線上，則表示叢集並未擁有多數成員，因此將無法正常運作。如果將離線的成員重新連線，則叢集將重新取得多數成員狀態。如果無法將任一離線成員重新連線，則可以重新部署 NSX Controller 叢集。請參閱[重新部署 NSX Controller 叢集](#)。

### 先決條件

透過疑難排解確認應用裝置無法復原。例如，這些步驟或許可以復原應用裝置，而不必進行取代。

- 確認應用裝置具有網路連線，如果沒有，請解決此問題。
- 將應用裝置重新開機。

### 後續步驟

取得 NSX Controller 叢集狀態。請參閱[取得 NSX Controller 叢集狀態](#)。

## 取得 NSX Controller 叢集狀態

您可以從 NSX Manager 找到 NSX Controller 叢集的狀態。您也可以從其命令列介面檢查每個 NSX Controller 的狀態。

取得 NSX Controller 叢集和叢集成員的狀態將有助於判斷 NSX Controller 叢集相關問題的來源。

表格 11-3. NSX Controller 叢集狀態

	是否至少有一個控制器登錄至 NSX Manager?	NSX Controller 叢集具有多數成員嗎?	有任何 NSX Controller 叢集成員已關機嗎?
NO_CONTROLLERS	否	不適用	不適用
UNAVAILABLE	未知	未知	未知
STABLE	是	是	否
DEGRADED	是	是	是
UNSTABLE	是	否	否

#### 程序

- 1 登入 NSX Manager CLI。
- 2 執行 `get management-cluster status` 命令。

```

nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.203 (UUID 564DDA9E-8E84-E374-1F12-C69FAAE6A698) Online
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564DC1B0-259A-9D6C-AF1F-12AEB6951882) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE

```

- 3 登入 NSX Controller CLI。
- 4 執行 `get control-cluster status` 命令。

```

nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true

```

uuid	address	status
03fad907-612f-4068-8109-efdf73002038	192.168.110.51	active
1228c336-3932-4b5b-b87e-9f66259cebcd	192.168.110.52	active
f5348a2e-2d59-4edc-9618-2c05ac073fd8	192.168.110.53	active

### 將 NSX Controller 叢集成員重新開機

如果您需要將 NSX Controller 叢集的多個成員重新開機，則必須針對個別成員逐次重新開機。三個成員的叢集中有一個成員離線時，叢集仍具有多數成員。如果有兩個成員離線，則叢集失去多數成員，因此將無法正常運作。



## 程序

- 1 登入 NSX Manager 的 CLI。
- 2 取得管理和控制叢集的狀態。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 3 登入您需重新開機之 NSX Controller 的 CLI，並將其重新開機。

```
nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y
```

- 4 再次取得管理和控制叢集的狀態。等候控制叢集狀態成為 STABLE，然後再將任何其他成員重新開機。

在此範例中，NSX Controller 192.168.110.53 正在重新開機，而控制叢集的狀態為 DEGRADED。這表示叢集仍具有多數成員，但其中一個成員已關機。如需 NSX Controller 叢集狀態的詳細資訊，請參閱[取得 NSX Controller 叢集狀態](#)。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED
```

NSX Controller 叢集進入 STABLE 狀態後，您便可以安全地將其他成員重新開機。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 3
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online
- 192.168.110.202 (UUID 564D0B9E-DEBD-A19E-233C-C13432CB23FB) Online
```

```
- 192.168.110.203 (UUID 564D666C-EB23-CDC1-8101-95155E9EB916) Online
```

```
Management cluster status: STABLE
```

```
Number of nodes in control cluster: 3
```

```
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
```

```
Control cluster status: STABLE
```

- 5 如果需要個別 NSX Controller 應用裝置狀態的詳細資訊，請登入 NSX Controller 並執行 `get control-cluster status` 命令。

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
  uuid                                address                status
  ----                                -
03fad907-612f-4068-8109-efdf73002038 192.168.110.51         active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52         active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53         not active
```

- 6 重複上述步驟，將其他 NSX Controller 應用裝置重新開機。

## 取代 NSX Controller 叢集的成員

NSX Controller 叢集至少必須有三個成員。如果某個 NSX Controller 應用裝置變得無法運作且您需將其從叢集移除，您必須先新增一個新的 NSX Controller 應用裝置，讓其成為四個成員的叢集。新增第四個成員後，您便可以從叢集移除 NSX Controller 應用裝置。

### 先決條件

- 透過疑難排解確認應用裝置無法復原。例如，這些步驟或許可以復原應用裝置，而不必進行取代。
  - 確認應用裝置具有網路連線，如果沒有，請解決此問題。
  - 將應用裝置重新開機。
- 確認您知道您所要取代之 NSX Controller 的版本，且擁有相同版本的正確安裝檔案 (OVA、OVF 或 QCOW2)。

### 程序

- 1 安裝並設定新的 NSX Controller。

如需有關這些步驟的資訊和指示，請參閱 NSX-T 安裝指南。

- a 安裝新的 NSX Controller 應用裝置。

新的 NSX Controller 必須與將取代的 NSX Controller 具有相同版本。

- b 將新的 NSX Controller 加入管理平面。

- c 將新的 NSX Controller 加入控制叢集。

- 2 從叢集關閉您所要移除的 NSX Controller。
- 3 登入另一台 NSX Controller，查看您所要移除的 NSX Controller 狀態是否為非作用中。

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active
863f9669-509f-4eba-b0ac-61a9702a242b	192.168.110.52	not active

- 4 將控制器從叢集中斷連結。

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

- 5 將控制器從管理平面中斷連結。

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

- 6 確認控制器為作用中，且控制叢集處於穩定狀態。

從 NSX Controller:

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active

從 NSX Manager:

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online
- 192.168.110.202 (UUID 4227F3D2-B7FE-8925-EA45-95ECD829C3E2) Online
- 192.168.110.203 (UUID 4227824A-1BDD-3A72-3EB3-8D306FEAE42D) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
```

```
- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)
```

```
Control cluster status: STABLE
```

## 重新部署 NSX Controller 叢集

如果取代控制器無法解決 NSX Controller 叢集的問題，或是有多個 NSX Controller 應用裝置無法復原，則您可以重新部署整個叢集。NSX Manager 包含所有所需的組態狀態，因此可以用來重新建立您的 NSX Controller 叢集。

在還原 NSX Controller 叢集的過程中，系統不會中斷資料路徑連線。

### 先決條件

- 透過疑難排解確認應用裝置無法復原。例如，這些步驟或許可以復原應用裝置，而不必進行取代。
  - 確認應用裝置具有網路連線，如果沒有，請解決此問題。
  - 將應用裝置重新開機。
- 確認您知道您所要取代之 NSX Controller 的版本，且擁有相同版本的正確安裝檔案 (OVA、OVF 或 QCOW2)。
- 確認您知道指派給 NSX Controller 應用裝置的 IP 位址。

### 程序

- 1 關閉 NSX Controller 叢集中的所有控制器。

## 2 將控制器從 NSX Manager 中斷連結。

- a 登入 NSX Manager CLI。
- b 使用 `get management-cluster status` 命令來取得控制器清單。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c 使用 `detach controller` 命令來中斷連結控制器。

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

## 3 安裝三個 NSX Controller 應用裝置，並建立新的 NSX Controller 叢集。

如需有關這些步驟的資訊和指示，請參閱 **NSX-T 安裝指南**。

- a 安裝三個 NSX Controller 應用裝置。
  - 新的 NSX Controller 應用裝置必須與將取代的 NSX Controller 應用裝置具有相同版本。
  - 指派已用於控制器的相同 IP 位址給新控制器。
- b 將 NSX Controller 應用裝置加入管理平面。
- c 在其中一個 NSX Controller 應用裝置上，初始化控制叢集。
- d 將其他兩個控制器加入控制叢集。

## 管理 NSX Edge 叢集

例如，如果某個 NSX Edge 變得無法運作或需要變更硬體，您可以將其取代。安裝新的 NSX Edge 並建立新的傳輸節點後，您可以修改 Edge 叢集以使用新的傳輸節點來取代舊的傳輸節點。

---

**備註** 移除第 1 層 Edge 叢集會造成第 1 層分散式路由器 (DR) 執行個體暫時停止服務。

---

## 程序

- 1 如果您要取代的 **NSX Edge** 仍在運作中，您可將其置於維護模式以將停機時間縮至最短。如果關聯的邏輯路由器上已啟用高可用性，則進入維護模式會導致邏輯路由器使用不同的 **Edge** 叢集成員。如果 **NSX Edge** 已無法運作，則不需要這麼做。

- a 取得故障網狀架構節點的網狀架構節點識別碼。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
...
```

- b 將故障的 **NSX Edge** 節點置於維護模式。

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-e77c-11e5-8701-005056aeed61?
action=enter_maintenance_mode
```

- 2 安裝新的 **NSX Edge**。

如需有關這些步驟的資訊和指示，請參閱 **NSX-T 安裝指南**。

- 3 使用 `join management-plane` 命令將新的 **NSX Edge** 加入管理平面。

如需有關這些步驟的資訊和指示，請參閱 **NSX-T 安裝指南**。

#### 4 將 NSX Edge 設定為傳輸節點。

如需有關這些步驟的資訊和指示，請參閱 **NSX-T 安裝指南**。

您可從 **API** 取得故障 **NSX Edge** 應用裝置的傳輸節點組態，並使用此項資訊來建立新的傳輸節點。

**a** 取得新網狀架構節點的網狀架構節點識別碼。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
...
```

**b** 取得故障傳輸節點的傳輸節點識別碼。

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
...
}
```

- c 取得故障傳輸節點的傳輸節點組態。

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d 使用 POST /api/v1/transport-nodes 建立新的傳輸節點。

在要求主體中，提供新傳輸節點的下列資訊：

- 新傳輸節點的 **description** (選用)
- 新傳輸節點的 **display\_name**
- 用於建立新傳輸節點之網狀架構節點的 **node\_id**

在要求主體中，從故障的傳輸節點複製下列資訊：

- **transport\_zone\_endpoints**
- **host\_switches**
- **tags** (選用)

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"
}
```



## 5 編輯 Edge 叢集以使用新的傳輸節點來取代故障的傳輸節點。

- a 取得新傳輸節點和故障傳輸節點的識別碼。id 欄位包含傳輸節點識別碼。

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
  {
    "resource_type": "TransportNode",
    "description": "",
    "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
    "display_name": "TN-edgenode-03a",
    ...
  }
}
```

- b 取得 Edge 叢集的識別碼。id 欄位包含 Edge 叢集識別碼。從 members 陣列取得 Edge 叢集的成員。

```
GET https://192.168.110.201/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {

```

```

        "member_index": 1,
        "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
],

```

- c 編輯 Edge 叢集以使用新的傳輸節點來取代故障的傳輸節點。`member_index` 必須符合故障傳輸節點的索引。



**注意** 如果 NSX Edge 仍在運作中，則此動作會中斷。此動作會從故障的傳輸節點，將所有邏輯路由器連接埠移動至新的傳輸節點。

在此範例中，傳輸節點 TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) 已故障，因此將其取代為 Edge 叢集 Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78) 中的傳輸節點 TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3)。

```

POST http://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
    "member_index": 0,
    "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}

```

- 6 (可選) 刪除故障的傳輸節點以及 NSX Edge 節點。

## 記錄系統訊息

以符合 RFC 5424 的格式，記錄來自所有 NSX-T 元件的訊息 (在 ESXi 上執行的元件除外)。您可以設定遠端記錄伺服器來接收記錄訊息。

如需 RFC 5424 的詳細資訊，請參閱 <https://tools.ietf.org/html/rfc5424>。

RFC 5424 會定義下列記錄訊息的格式：

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

來自 NSX Manager 的記錄訊息範例：

```

<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.

```

NSX-T 會產生定期記錄 (設施 `local6` 具有數值 22) 以及稽核記錄 (設施 `local7`，具有數值 23)。所有 API 呼叫皆會觸發稽核記錄。

RFC 5424 會定義下列嚴重性層級：

嚴重性數值	說明
0	緊急：系統無法使用
1	警示：必須立即採取動作

嚴重性數值	說明
2	嚴重：嚴重狀況
3	錯誤：錯誤狀況
4	警告：警告狀況
5	通知：一般但重要的狀況
6	資訊：資訊訊息
7	偵錯：偵錯層級訊息

記錄訊息的結構化資料部分中具有緊急、警示、嚴重或錯誤嚴重性層級的所有記錄，皆包含唯一的錯誤碼。錯誤碼由字串和一個十進位數字組成。字串代表特定模組。

MSGID 欄位則指出記錄訊息的類別。如需類別清單，請參閱[記錄訊息類別](#)。

## 設定遠端記錄

您可以設定 NSX-T 應用裝置及 Hypervisor 以傳送記錄訊息至遠端記錄伺服器。

NSX Manager、NSX Controller、NSX Edge 應用裝置上支援遠端記錄。和 Hypervisor。

您可以根據這些準則篩選要將哪些記錄訊息傳送至記錄伺服器：

- 層級：emerg、alert、crit、err、warning、notice、info、debug
- 設施：程式碼定義於 RFC 5424。設施 local7 用於稽核訊息，local6 則用於非稽核訊息。
- 訊息識別碼或類別：類別和範例列示如下：[記錄訊息類別](#)

如需相關命令和要求的相關資訊，請參閱《NSX-T 命令列參考》和《NSX-T API 指南》。

### 先決條件

- 設定遠端記錄伺服器以接收來自 NSX-T 應用裝置的記錄。
- 判定您要傳送至記錄伺服器的記錄訊息。

### 程序

- 1 登入您要使用遠端記錄設定的 NSX-T 應用裝置。
- 2 使用下列語法以 `set logging-server` 命令設定記錄伺服器。您可以使用逗號分隔且無空格的清單來指定多個設施或訊息識別碼。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>]
```

您可以多次執行命令以新增多個記錄伺服器組態。

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

### 3 (可選) 使用 `get logging-server` 命令檢視記錄組態。

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

## 記錄訊息類別

每個記錄訊息屬於一個類別。您可在 `set logging-server` 命令中使用這些類別來篩選要傳送給記錄伺服器的記錄訊息。

**表格 11-4. 記錄訊息類別**

記錄訊息類別	範例
FABRIC	主機節點 主機準備 Edge 節點 傳輸區域 傳輸節點 上行設定檔 叢集設定檔 Edge 叢集 橋接器叢集和端點
SWITCHING	邏輯交換器 邏輯交換器連接埠 交換設定檔 交換器安全性功能
ROUTING	邏輯路由器 邏輯路由器連接埠 靜態路由 動態路由 NAT
FIREWALL	防火牆規則 防火牆規則區段
FIREWALL_PKTLOG	防火牆連線記錄 防火牆封包記錄
GROUPING	IP 集合 Mac 集合 NSGroup NSService NSService 群組 VNI 集區 IP 集區
DHCP	DHCP 轉送

表格 11-4. 記錄訊息類別 (續)

記錄訊息類別	範例
SYSTEM	應用裝置管理 (遠端 Syslog 和 ntp 等) 叢集管理 信任管理 授權 使用者和角色 工作管理 安裝 (NSX Manager、NSX Controller) 升級 (NSX Manager、NSX Controller、NSX Edge 和主機套件升級) 解析 標籤
MONITORING	SNMP 連接埠連線 Traceflow
-	所有其他記錄訊息。

## 設定 IPFIX

IPFIX (網際網路通訊協定流量資訊匯出) 是網路流量資訊的格式化和匯出標準。當您啟用 IPFIX 時，所有已設定的主機傳輸節點會使用連接埠 4739，將 IPFIX 訊息傳送至 IPFIX 收集器。

若為 ESXi，則 NSX-T 會自動開啟連接埠 4739。針對 KVM 的案例，如果未啟用防火牆，則連接埠 4739 將會開啟，但如果已啟用防火牆，則因為 NSX-T 不會自動開啟連接埠，所以您必須確定連接埠已開啟。

### 先決條件

- 至少安裝一個 IPFIX 收集器。
- 確認 IPFIX 收集器具有 Hypervisor 的網路連線。
- 確認包含 ESXi 防火牆在內的所有相關防火牆皆允許 IPFIX 收集器連接埠上的流量。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的工具 (Tools) > IPFIX。
- 3 按一下**收集器 (Collectors)**索引標籤 (若尚未選取)。
- 4 按一下**設定收集器 (Configure Collectors)**。
- 5 按一下**新增 (Add)**，然後輸入收集器 IP 位址和連接埠。

您最多可以新增 8 個收集器。

- 6 (可選) 在 [收集選項] 區段中，按一下**編輯 (Edit)**以指定觀察網域識別碼。

觀察網域識別碼可識別網路流量源自哪個觀察網域。預設值為 0，表示沒有特定觀察網域。

- 7 按一下**交換器 IPFIX 設定檔 (Switch IPFIX Profiles)**索引標籤。

## 8 按一下**新增 (Add)**以新增設定檔。

設定	說明
作用中逾時 (秒)	即使再收到與流量相關聯的封包，流量仍將逾時的經歷時間長度。預設值為 300。
閒置逾時 (秒)	如果沒有再收到與流量相關聯的封包，流量將會逾時的經歷時間長度 (僅限 ESXi, KVM 會根據作用中逾時讓所有流量逾時)。預設值為 300。
流量上限	在橋接器上快取的流量上限 (僅限 KVM，無法在 ESXi 上設定)。預設值為 16384。
取樣機率 (%)	將會取樣的封包百分比 (近似值)。增加此設定可能會影響 Hypervisor 和收集器的效能。如果所有 Hypervisor 正在傳送更多 IPFIX 封包給收集器，則收集器可能無法收集所有封包。將機率設定為預設值 0.1%，將會讓效能影響保持輕微的狀態。

## 9 按一下**套用至 (Applied To)**以將設定檔套用至一或多個物件。

物件類型為邏輯連接埠和邏輯交換器。

ESXi 和 KVM 上的 IPFIX 會以不同方式取樣通道封包。在 ESXi 上，系統會將通道封包取樣為兩種記錄：

- 具有一些內部封包資訊的外部封包記錄
  - 參考外部封包的 SrcAddr、DstAddr、SrcPort、DstPort 和通訊協定。
  - 包含一些說明內部封包的企業項目。
- 內部封包記錄
  - 參考內部封包的 SrcAddr、DstAddr、SrcPort、DstPort 和通訊協定。

在 KVM 上，系統會將通道封包取樣為一種記錄：

- 具有一些外部通道資訊的內部封包記錄
  - 參考內部封包的 SrcAddr、DstAddr、SrcPort、DstPort 和通訊協定。
  - 包含一些說明外部封包的企業項目。

## 使用 Traceflow 追蹤封包的路徑

當封包從邏輯網路上的一個邏輯連接埠傳輸至相同網路上的另一個邏輯連接埠時，可以使用 Traceflow 檢查封包的路徑。Traceflow 可追蹤插入邏輯連接埠之封包的傳輸節點層級路徑。追蹤封包會周遊邏輯交換器覆蓋，但不會顯示至連結至邏輯交換器的介面。換句話說，實際上系統不會傳送封包給測試封包的預期收件者。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 導覽至 [Traceflow] 畫面。您有兩個選項可供選擇。
  - 選取導覽面板中的**工具 (Tools) > Traceflow**。
  - 選取導覽面板中的**交換 (Switching)**、按一下**連接埠 (Ports)**索引標籤，接著選取連結 VIF 的連接埠，然後按一下**動作 (Actions) > Traceflow**
- 3 選取流量類型。
 

選項包含 [單點傳播]、[多點傳送] 和 [廣播]。

#### 4 根據流量類型指定來源和目的地資訊。

流量類型	指定來源資訊	指定目的地資訊
單點傳播	<p>選取虛擬機器和虛擬介面。</p> <p>如果虛擬機器已安裝 <b>VMtools</b>，或虛擬機器是透過 <b>OpenStack</b> 外掛程式來進行部署 (在此情況下，將使用位址繫結)，將顯示 <b>IP</b> 位址和 <b>MAC</b> 位址。如果虛擬機器具有一個以上的 <b>IP</b> 位址，請從下拉式功能表中選取其中一個。</p> <p>如果未顯示 <b>IP</b> 位址和 <b>MAC</b> 位址，請在文字方塊中輸入 <b>IP</b> 位址和 <b>MAC</b> 位址。</p> <p>這也適用於多點傳送和廣播。</p>	<p>從 [類型] 下拉式功能表中，選取 [虛擬機器名稱] 或 [IP-MAC]。</p> <ul style="list-style-type: none"> <li>如果選取 [虛擬機器名稱]，則請選取虛擬機器和虛擬介面。選取或輸入 <b>IP</b> 位址和 <b>MAC</b> 位址</li> <li>如果選取 [IP-MAC]，則請選取追蹤類型 (第 2 層或第 3 層)。如果追蹤類型是第 2 層，請輸入 <b>IP</b> 位址和 <b>MAC</b> 位址。如果追蹤類型是第 3 層，請輸入 <b>IP</b> 位址。</li> </ul>
多點傳送	步驟同上。	輸入 <b>IP</b> 位址。必須是來自 <b>224.0.0.0 - 239.255.255.255</b> 的多點傳送位址。
廣播	步驟同上。	輸入子網路首碼長度。

#### 5 (可選) 按一下**進階 (Advanced)**以查看進階選項。

#### 6 (可選) 在左側資料行中，輸入所需的值或輸入下列欄位：

選項	說明
框架大小	例如 128
TTL	例如 64
逾時 (毫秒)	例如 10000
Ethertype	例如 2048
裝載類型	從下拉式功能表中選取一個選項。
裝載資料	根據所選裝載類型的裝載格式 ( <b>Base64</b> 、十六進位、純文字、二進位或十進位)

#### 7 (可選) 在左側資料行的 [通訊協定] 下方，從 [類型] 下拉式功能表中選取通訊協定。

#### 8 (可選) 根據所選取的通訊協定來完成下表中的相關聯步驟。

通訊協定	步驟 1	步驟 2	步驟 3
TCP	輸入來源連接埠。	輸入目的地連接埠。	從下拉式功能表中選取所需的 <b>TCP</b> 旗標。
UDP	輸入來源連接埠。	輸入目的地連接埠。	不適用
ICMP	輸入 <b>ICMP ID</b> 。	輸入序列值。	不適用

#### 9 按一下**追蹤 (Trace)**。

隨即顯示連線、元件和層級的相關資訊。輸出包含一個表格，其中會列出觀察類型 (已傳送、已捨棄、已接收、已轉送)、傳輸節點和元件，以及拓撲的圖形對應 (如果選取單點傳播和邏輯交換器作為目的地)。您也可以顯示的觀察結果上套用篩選器 (**全部 (All)**、**已傳送 (Delivered)**、**已捨棄 (Dropped)**)。如果有已捨棄的觀察結果，依預設會套用**已捨棄 (Dropped)**篩選器。否則則會套用**全部 (All)**篩選器。

## 檢視連接埠連線資訊

您可以使用連接埠連線工具來快速視覺化兩個虛擬機器之間的連線，以及進行疑難排解。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **工具 > 連接埠連線**。
- 3 從**來源虛擬機器**下拉式功能表中選取虛擬機器。
- 4 從**目的地虛擬機器**下拉式功能表中選取虛擬機器。
- 5 按一下**執行**。

連接埠連線拓撲的視覺化地圖隨即顯示。按一下視覺化輸出中的任何元件，即可顯示該元件的更多詳細資訊。

## 監控邏輯交換器連接埠活動

您可以監控邏輯連接埠活動，例如疑難排解網路壅塞以及將要捨棄的封包

### 先決條件

確認已設定邏輯交換器連接埠。請參閱[將虛擬機器連線到邏輯交換器](#)。

### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**交換 (Switching) > 連接埠 (Port)**。
- 3 按兩下要監控的邏輯交換器連接埠。
- 4 按一下**監控 (Monitor)**索引標籤。
- 5 選取**開始追蹤 (Begin Tracking)**。

[連接埠追蹤] 頁面隨即開啟。

- 6 開始監控邏輯交換器連接埠上的活動。

您可以檢視雙向連接埠流量來找出捨棄的封包。連接埠追蹤器頁面也會列出連結至邏輯交換器連接埠的交換設定檔。

例如，如果您注意到封包是因為網路壅塞而捨棄，則可為邏輯交換器連接埠設定 **QoS** 交換設定檔，以避免偏好的封包發生資料遺失。請參閱[瞭解 QoS 交換設定檔](#)。

## 監控連接埠鏡像工作階段

您可以監控連接埠鏡像工作階段以用於疑難排解或其他目的。

這項功能具有下列限制：

- 來源鏡像連接埠無法位於一個以上的鏡像工作階段中。



- 目的地連接埠僅能接收鏡像流量。
- 透過 KVM，您可將多個 NIC 連結至相同的 OVS 連接埠。鏡像會發生在 OVS 上行連接埠，這表示連結至 OVS 連接埠之所有 pNIC 上的流量皆會發生鏡像。
- 鏡像工作階段來源和目的地連接埠必須位於相同的主機 vSwitch 上。因此，如果您將具有來源或目的地連接埠的虛擬機器 vMotion 至其他主機，則該連接埠上的流量都將無法再次進行鏡像。
- 在 ESXi 上，當上行連接埠上啟用鏡像時，系統會使用 VDL2 的 Geneve 通訊協定將原始生產 TCP 封包封裝至 UDP 封包。支援 TSO (TCP 分割卸載) 的實體 NIC 可變更封包，以及使用 MUST\_TSO 旗標來標記封包。在具有 VMXNET3 或 E1000 vNIC 的監控虛擬機器上，驅動程式會將封包視為一般 UDP 封包，且無法處理 MUST\_TSO 旗標，而會捨棄封包。

如果有大量流量鏡像至監控虛擬機器，則可能會導致驅動程式的緩衝區循環已滿而造成捨棄封包。若要減輕這個問題，可執行下列一或多個動作：

- 增加 rx 緩衝區循環大小。
- 指派多個 CPU 資源給虛擬機器。
- 使用資料平面開發套件 (DPDK) 來改進封包處理效能。

**備註** 確定監控虛擬機器的 MTU 設定 (若是 KVM，則也包括 Hypervisor 虛擬 NIC 裝置的 MTU 設定) 夠大以處理封包。這一點對於封裝式封包尤為重要，因為封裝會增加封包大小。否則，封包可能會遭到捨棄。對於具備 VMXNET3 NIC 的 ESXi 虛擬機器，這不會是問題，但對於 ESXi 和 KVM 虛擬機器上的其他 NIC 類型可能會發生問題。

**備註** 在涉及 KVM 主機上虛擬機器的第 3 層連接埠鏡像工作階段中，您必須設定夠大的 MTU 大小才能處理封裝所需的額外位元組。鏡像流量會通過 OVS 介面和 OVS 上行。您必須將 OVS 介面的 MTU 設定為至少大於原始封包 (封裝和鏡像前) 大小的 100 個位元組。如果您看到捨棄的封包，請增加主機虛擬 NIC 和 OVS 介面的 MTU 設定。請使用下列命令來設定 OVS 介面的 MTU：

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

**備註** 監控虛擬機器的邏輯連接埠和虛擬機器所在主機的上行連接埠時，視主機為 ESXi 或 KVM 而定，您會看到不同的行為。對於 ESXi，系統會以相同的 VLAN 識別碼標記邏輯連接埠鏡像封包和上行鏡像封包，且會以相同方式向監控虛擬機器顯示。對於 KVM，系統不會以 VLAN 識別碼標記邏輯連接埠鏡像封包，但會標記上行鏡像封包，且會以不同方式向監控虛擬機器顯示。

#### 程序

- 1 從瀏覽器登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的工具 (Tools) > 連接埠鏡像工作階段 (Port Mirroring Session)。
- 3 輸入工作階段名稱。
- 4 從下拉式功能表中選取傳輸節點。

連接埠鏡像工作階段必須位於相同傳輸節點上的 NIC 之間。

- 5 從下拉式功能表中選取方向。

選項有**雙向 (Bidirectional)**、**入口 (Ingress)**和**出口 (Egress)**。

- 6 (可選) 選取封包截斷值。

- 7 按一下**下一步 (Next)**。

- 8 選取來源 PNIC。

- 9 (可選) 切換**封裝式封包 (Encapsulated Packet)**交換器以停用擷取封裝式流量。

此交換器依預設為啟用。

- 10 選取來源 VNIC。

- 11 選取目的地。

您最多可選取 3 個虛擬機器和 3 個 VNIC。

- 12 按一下**儲存 (Save)**。

儲存連接埠鏡像工作階段後，您便無法變更來源和目的地。

## 監控網狀架構節點

您可以從 NSX Manager UI 監控網狀架構節點，例如主機、Edge、Edge 叢集、橋接器、以及傳輸節點。

### 程序

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

- 2 選取導覽面板中的**網狀架構 (Fabric) > 節點 (Nodes)**。

- 3 選取下列其中一個索引標籤。

- 主機
- Edge
- Edge 叢集
- 橋接器
- 傳輸節點

---

**備註** 在 [主機] 畫面中，如果某個主機的 MPA 連線狀態為 [關閉] 或 [未知]，請忽略 LCP 連線狀態，因為此狀態可能不精確。

---

## 收集支援服務包

您可以在登錄的叢集和網狀架構節點上收集支援服務包，並將服務包下載至您的機器或將其上傳至檔案伺服器。

如果您選擇將服務包下載至您的機器，您會取得遊資訊清單檔案和每個節點之支援服務包所組成的單一封存檔案。如果您選擇將服務包上傳至檔案伺服器，則資訊清單檔案和個別服務包會分別上傳至檔案伺服器。

#### 程序

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

2 選取導覽面板中的**系統 (System) > 公用程式 (Utilities)**。

3 按一下**支援服務包 (Support Bundle)**索引標籤。

4 選取目標節點。

可用的節點類型包含管理節點、控制器節點、Edge 和主機。

5 (可選) 指定記錄存留期 (以天為單位) 以排除超過指定天數的記錄。

6 (可選) 切換表示要包含或排除核心檔案和稽核記錄的交換器。

核心檔案和稽核記錄可能包含機密資訊，例如密碼或加密金鑰。

7 (可選) 選取核取方塊，將服務包上傳至檔案伺服器。

8 按一下**啟動服務包收集 (Start Bundle Collection)**以開始收集支援服務包。

依所存在的記錄檔數目而定，每個節點可能會花費數分鐘。

9 監控收集程序的狀態。

狀態欄會顯示已完成支援服務包收集的節點百分比。

10 如果未設定將服務包傳送至檔案伺服器的選項，請按一下**下載 (Download)**以下載服務包。