

NSX-T Data Center 管理指南

修改日期：2019 年 5 月 24 日
VMware NSX-T Data Center 2.3



vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

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

目錄

關於管理 VMware NSX-T Data Center 9

1 邏輯交換器與設定虛擬機器連結 10

瞭解 BUM 框架複寫模式 11

建立邏輯交換器 12

第 2 層橋接 13

建立橋接器叢集 14

建立橋接器設定檔 15

建立第 2 層橋接器備份邏輯交換器 16

為 NSX Edge 上行建立 VLAN 邏輯交換器 17

將虛擬機器連線到邏輯交換器 19

將 vCenter Server 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器 19

將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T Data Center 邏輯交換器 21

將 KVM 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器 26

測試第 2 層連線 27

2 邏輯交換器連接埠 30

建立邏輯交換器連接埠 30

監控邏輯交換器連接埠活動 31

3 邏輯交換器和邏輯連接埠的交換設定檔 32

瞭解 QoS 交換設定檔 33

設定自訂 QoS 交換設定檔 33

瞭解 IP 探索交換設定檔 35

設定 IP 探索交換設定檔 35

瞭解 SpoofGuard 36

設定連接埠位址繫結 37

設定 SpoofGuard 交換設定檔 37

瞭解交換器安全性交換設定檔 38

設定自訂交換器安全性交換設定檔 38

瞭解 MAC 管理交換設定檔 39

設定 MAC 管理交換設定檔 40

建立自訂設定檔與邏輯交換器之間的關聯 40

建立自訂設定檔與邏輯連接埠之間的關聯 42

4 第 1 層邏輯路由器 43

建立第 1 層邏輯路由器 44

- 在第 1 層邏輯路由器上新增下行連接埠 45
- 在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠 46
- 在第 1 層邏輯路由器上設定路由通告 46
- 設定第 1 層邏輯路由器靜態路由 48
- 建立獨立的第 1 層邏輯路由器 50

5 第 0 層邏輯路由器 52

- 建立第 0 層邏輯路由器 54
- 連結第 0 層和第 1 層 55
 - 確認第 0 層路由器已從第 1 層路由器學習路由 56
- 針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器 57
 - 確認第 0 層邏輯路由器和 TOR 連線 59
- 新增回送路由器連接埠 60
- 在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠 61
- 設定靜態路由 62
 - 確認靜態路由 63
- BGP 組態選項 65
 - 在第 0 層邏輯路由器上設定 BGP 66
 - 確認來自第 0 層服務路由器的 BGP 連線 68
- 在第 0 層邏輯路由器上設定 BFD 70
- 啟用第 0 層邏輯路由器上的路由重新分配 70
 - 確認南北向連線和路由重新分配 71
- 瞭解 ECMP 路由 73
 - 新增第二個 Edge 節點的上行連接埠 73
 - 新增第二個 BGP 芳鄰並啟用 ECMP 路由 74
 - 確認 ECMP 路由連線 75
- 建立 IP 首碼清單 77
- 建立社群清單 78
- 建立路由對應 78
- 設定轉送累計計時器 79

6 網路位址轉譯 81

- 第 1 層 NAT 82
 - 在第 1 層路由器上設定來源 NAT 82
 - 在第 1 層路由器上設定目的地 NAT 84
 - 通告第 1 層 NAT 路由至上游第 0 層路由器 86
 - 通告第 1 層 NAT 路由至實體架構 87
 - 確認第 1 層 NAT 88
- 第 0 層 NAT 88
 - 在第 0 層路由器上設定來源和目的地 NAT 88
- 自反 NAT 89

在第 0 層或第 1 層邏輯路由器上設定自反 NAT 91

7 防火牆區段和防火牆規則 93

- 新增防火牆規則區段 94
- 刪除防火牆規則區段 94
- 啟用和停用區段規則 95
- 啟用和停用區段記錄 95
- 關於防火牆規則 95
- 新增防火牆規則 97
- 刪除防火牆規則 98
- 編輯預設 Distributed Firewall 規則 99
- 變更防火牆規則的順序 99
- 篩選防火牆規則 100
- 為邏輯交換器橋接器連接埠設定防火牆 100
- 設定防火牆排除清單 101
- 啟用和停用防火牆 101
- 新增或刪除邏輯路由器的防火牆規則 101

8 虛擬私人網路 103

- 設定 IPSec VPN 104
- 設定 L2VPN 107

9 管理物件、群組、服務和虛擬機器 109

- 建立 IP 集合 109
- 建立 IP 集區 110
- 建立 MAC 集合 110
- 建立 NSGroup 111
- 設定服務和服務群組 112
 - 建立 NSService 112
- 管理虛擬機器的標記 113

10 邏輯負載平衡器 114

- 主要負載平衡器概念 114
 - 調整負載平衡器資源 115
 - 支援的負載平衡器功能 116
 - 負載平衡器拓撲 117
- 設定負載平衡器元件 118
 - 建立負載平衡器 119
 - 設定主動健全狀況監視器 120
 - 設定被動健全狀況監視器 122
 - 新增用於負載平衡的伺服器集區 124

設定虛擬伺服器元件 127

11 DHCP 145

建立 DHCP 伺服器設定檔 145

建立 DHCP 伺服器 146

將 DHCP 伺服器連結至邏輯交換器 147

從邏輯交換器中斷連結 DHCP 伺服器 147

建立 DHCP 轉送設定檔 147

建立 DHCP 轉送服務 148

將 DHCP 服務新增至邏輯路由器連接埠 148

12 中繼資料 Proxy 149

新增中繼資料 Proxy 伺服器 149

將中繼資料 Proxy 伺服器連結至邏輯交換器 150

將中繼資料 Proxy 伺服器與邏輯交換器中斷連結 151

13 IP 位址管理 152

管理 IP 區塊 152

管理 IP 區塊的子網路 153

14 NSX 原則 154

概觀 154

新增強制執行點 155

新增服務 156

新增網域 156

設定 NSX Policy Manager 的備份 157

備份 NSX Policy Manager 158

還原 NSX Policy Manager 158

將 vIDM 主機與 NSX Policy Manager 相關聯 159

管理角色指派 160

15 服務插入 161

概觀 161

登錄服務 162

部署服務執行個體 164

設定流量重新導向 165

監控流量重新導向 165

16 NSX Cloud 166

Cloud Service Manager 166

雲端 166

系統	173
管理隔離原則	176
如何啟用或停用隔離原則	176
停用時的隔離原則影響	177
啟用時的隔離原則影響	178
公有雲的 NSX Cloud 安全群組	179
工作負載虛擬機器上線及管理概觀	180
支援的作業系統	180
如何從 Microsoft Azure 將工作負載虛擬機器上線	180
如何從 AWS 將工作負載虛擬機器上線	181
工作負載虛擬機器上線	182
標記公有雲中的虛擬機器	182
安裝 NSX 代理程式	183
自動安裝 NSX 代理程式	187
管理工作負載虛擬機器	188
存取受管理的工作負載虛擬機器	188
使用 NSX-T Data Center 和公有雲標記分組虛擬機器	189
針對工作負載虛擬機器設定微分割	192
如何搭配使用 NSX-T Data Center 功能與公有雲	192
使用進階 NSX Cloud 功能	195
啟用 Syslog 轉送	195
疑難排解	196
確認 NSX Cloud 元件	196
疑難排解常見問題集	197
17 作業和管理	198
新增授權金鑰	199
管理使用者帳戶和角色型存取控制	199
變更 CLI 使用者的密碼	199
驗證原則設定	200
從 vIDM 主機取得憑證指紋	201
建立 vIDM 主機與 NSX-T 之間的關聯	201
NSX Manager、vIDM 和相關元件之間的時間同步	202
角色型存取控制	203
管理角色指派	207
檢視主體身分識別	208
設定憑證	209
建立憑證簽署要求檔案	209
匯入 CA 憑證	210
匯入憑證	211
建立自我簽署的憑證	211

取代憑證	212
匯入憑證撤銷清單	212
匯入 CSR 的憑證	213
設定應用裝置	214
新增計算管理程式	214
管理標記	216
搜尋物件	216
尋找遠端伺服器的 SSH 指紋	217
備份和還原 NSX Manager	218
備份 NSX Manager 組態	219
還原 NSX Manager 組態	221
還原 NSX Controller 叢集	224
管理應用裝置和應用裝置叢集	225
管理 NSX Manager	225
管理 NSX Controller 叢集	226
管理 NSX Edge 叢集	232
記錄訊息	236
設定遠端記錄	237
記錄訊息識別碼	238
設定 IPFIX	239
設定交換器 IPFIX 設定檔	240
設定防火牆 IPFIX 收集器	241
ESXi IPFIX 範本	242
KVM IPFIX 範本	247
使用 Traceflow 追蹤封包的路徑	409
檢視連接埠連線資訊	410
監控邏輯交換器連接埠活動	411
監控連接埠鏡像工作階段	411
監控網狀架構節點	414
檢視在虛擬機器上執行之應用程式的相關資料	414
收集支援服務包	415
客戶經驗改進計劃	416
編輯客戶經驗改進計劃組態	416

關於管理 VMware NSX-T Data Center

《NSX-T Data Center 管理指南》提供關於為 VMware NSX-T™ Data Center 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 Data Center 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>。

邏輯交換器與設定虛擬機器連結

1

NSX-T Data Center 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。

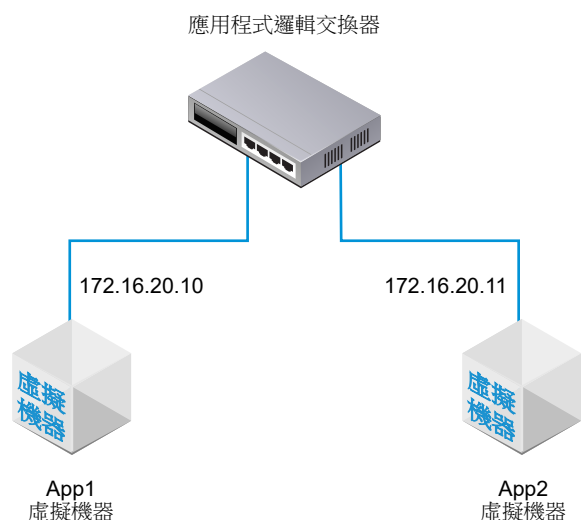
NSX Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

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。

若要查看和編輯 VNI 集區的值，請登入 NSX Manager，導覽至**網狀架構 > 設定檔**，然後按一下**組態索引**標籤。請注意，如果您將集區設定得太小，則所有 VNI 值皆在使用中時，建立邏輯交換器將失敗。如果您刪除邏輯交換器，VNI 值將會重複使用，但必須在 6 小時之後才能使用。

在新增 VLAN 邏輯交換器時，請務必記得對應您所建置的拓撲。

圖 1-1. 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。

本章節討論下列主題：

- 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 Data Center 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 Data Center 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。

必要條件

- 確認已設定傳輸區域。請參閱《NSX-T Data Center 安裝指南》。
- 確認網狀架構節點已成功連線至 NSX-T Data Center 管理平面代理程式 (MPA) 及 NSX-T Data Center 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 Data Center 安裝指南》。

- 確認傳輸節點已新增至傳輸區域。請參閱《NSX-T Data Center 安裝指南》。
- 確認 Hypervisor 已新增至 NSX-T Data Center 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 1 章 [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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **交換 > 交換器**。
- 3 按一下 **新增**。
- 4 輸入邏輯交換器的名稱，並選擇性地輸入說明。
- 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 輸入上行整併原則的名稱。
- 7 將**管理狀態**設定為**開啟**或**關閉**。

8 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。
HEAD	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。

9 (選擇性) 指定 VLAN 標記的 VLAN 識別碼或 VLAN 識別碼範圍。

若要支援連線至此交換器之虛擬機器的客體 VLAN 標記，您必須指定 VLAN 識別碼範圍，也稱為主幹 VLAN 識別碼範圍。邏輯連接埠會根據主幹 VLAN 識別碼範圍來篩選封包，客體虛擬機器可以根據主幹 VLAN 識別碼範圍使用自己的 VLAN 識別碼來標記其封包。

10 (選擇性) 按一下交換設定檔索引標籤並選取交換設定檔。

11 按一下儲存。

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

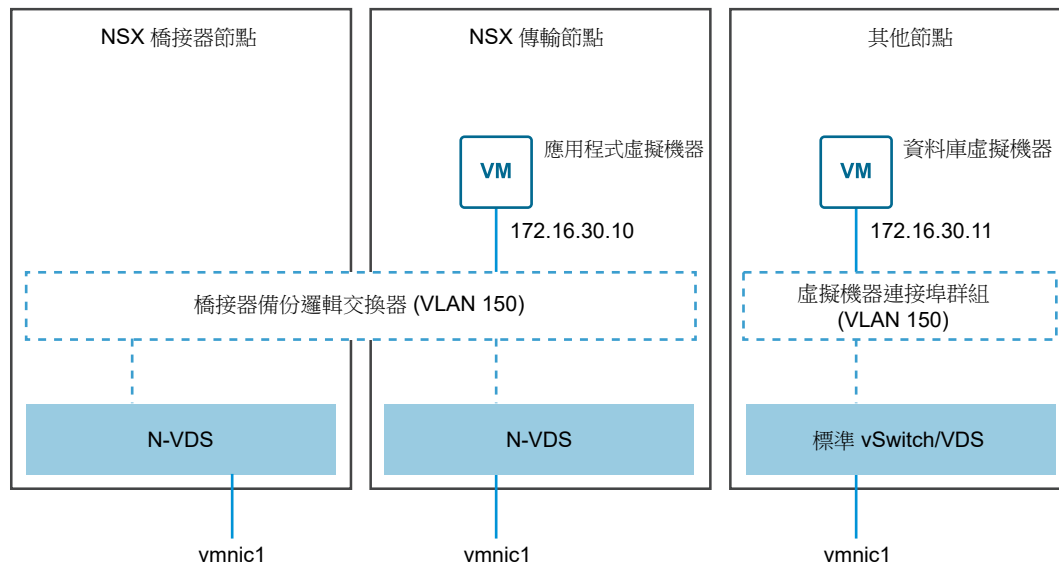
當 NSX-T Data Center 邏輯交換器需要對 VLAN 支援的連接埠群組進行第 2 層連線，或是需要連線到位於 NSX-T Data Center 部署外部的其他裝置 (例如閘道)，則可以使用 NSX-T Data Center 第 2 層橋接器。這對於移轉案例特別有用，因為您需要在實體和虛擬工作負載間分割子網路。

第 2 層橋接涉及的 NSX-T Data Center 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。

您可以使用 ESXi 主機傳輸節點或 NSX Edge 傳輸節點來設定第 2 層橋接。若要使用 ESXi 主機傳輸節點進行橋接，您可以建立橋接器叢集。若要使用 NSX Edge 傳輸節點進行橋接，您可以建立橋接器設定檔。

在下列範例中，兩個 NSX-T Data Center 傳輸節點屬於相同覆疊傳輸區域的一部分。這可讓您將其受 NSX 管理的虛擬分散式交換器 (N-VDS，先前稱為主機交換器) 連結到同一個支援橋接器的邏輯交換器。

圖 1-2. 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 Data Center 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 Data Center 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。

備註 當使用在 ESXi 主機上執行的 Edge 虛擬機器來提供第 2 層橋接時，標準或分散式交換器 (在 VLAN 端上傳送和接收流量) 上的連接埠群組應處於混合模式。若要獲得最佳效能，請注意下列事項：

- 不要讓共用相同 VLAN 集合之同一主機上的其他連接埠群組處於混合模式。
- 主動和備用 Edge 虛擬機器應位於不同主機。如果它們位於同一主機，輸送量可能會下降至 7 Gbps，因為在混合模式中需要將 VLAN 流量同時轉送至這兩個虛擬機器。

建立橋接器叢集

橋接器叢集是可為邏輯交換器提供第 2 層橋接的 ESXi 主機傳輸節點集合。

一個橋接器叢集最多可以使用兩個 ESXi 主機傳輸節點做為橋接器節點。藉由兩個橋接器節點，橋接器叢集將在主動備用模式中提供高可用性。即使您想要使用一個橋接器節點，仍必須建立橋接器叢集。建立橋接器叢集後，您可以稍後新增其他橋接器節點。

必要條件

- 建立至少一個 NSX-T Data Center 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 選取導覽面板中的**網狀架構 > 節點**。
- 2 按一下 **ESXi 橋接器叢集**索引標籤。
- 3 按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 選取橋接器叢集的傳輸區域。
- 6 從**可用**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**資料行。
- 7 按一下**新增**按鈕。

後續步驟

您現在可將邏輯交換器與橋接器叢集建立關聯。

建立橋接器設定檔

橋接器設定檔使 NSX Edge 叢集能夠為邏輯交換器提供第 2 層橋接。

必要條件

- 確認您擁有的 NSX Edge 叢集具有兩個 NSX Edge 傳輸節點。

程序

- 1 選取導覽面板中的**網狀架構 > 設定檔**。
- 2 按一下 **Edge 橋接器設定檔**索引標籤。
- 3 按一下**新增**。
- 4 輸入名稱和 (選用) 說明。
- 5 選取 NSX Edge 叢集。
- 6 選取主要節點。
- 7 選取備份節點。
- 8 選取容錯移轉模式。
選項為**先佔式**和**非先佔式**。
- 9 按一下**新增**按鈕。

後續步驟

您現在可將邏輯交換器與橋接器設定檔建立關聯。

建立第 2 層橋接器備份邏輯交換器

當您擁有連線至 NSX-T Data Center 覆疊的虛擬機器時，您可以設定支援橋接器的邏輯交換器，來為 NSX-T Data Center 部署外部的其他裝置或虛擬機器提供第 2 層連線能力。

如需範例拓撲，請參閱圖 1-2. 橋接器拓撲。

必要條件

- 確認您擁有橋接器叢集或橋接器設定檔。
- 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 Data Center 部署外部的裝置之間具備連線能力。
- NSX-T Data Center 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 選取導覽面板中的**網路 > 交換**。
- 3 按一下覆疊交換器 (流量類型：覆疊) 的名稱。
- 4 按一下**相關 > ESXi 橋接器叢集**或**相關 > Edge 橋接器設定檔**。
- 5 按一下**連結**。
- 6 若要連結至橋接器叢集，
 - a 請選取橋接器叢集。
 - b 輸入 VLAN 識別碼。
 - c 啟用或停用 VLAN 上的 HA。
 - d 按一下**連結**。
- 7 若要連結至橋接器設定檔，
 - a 請選取橋接器設定檔。
 - b 選取傳輸區域。
 - c 輸入 VLAN 識別碼。
 - d 按一下**儲存**。
- 8 如果虛擬機器尚未連線，請將它們連線至邏輯交換器。

虛擬機器必須位於與橋接器叢集或橋接器設定檔相同的傳輸區域中的傳輸節點上。

結果

您可以測試橋接器的功能，方法為將 Ping 偵測從 NSX-T Data Center 內部虛擬機器傳送至 NSX-T Data Center 外部的節點。例如，在 [圖 1-2. 橋接器拓撲](#) 中，NSX-T Data Center 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。

您可以按一下[監控](#)索引標籤，來監控橋接器交換器上的流量。

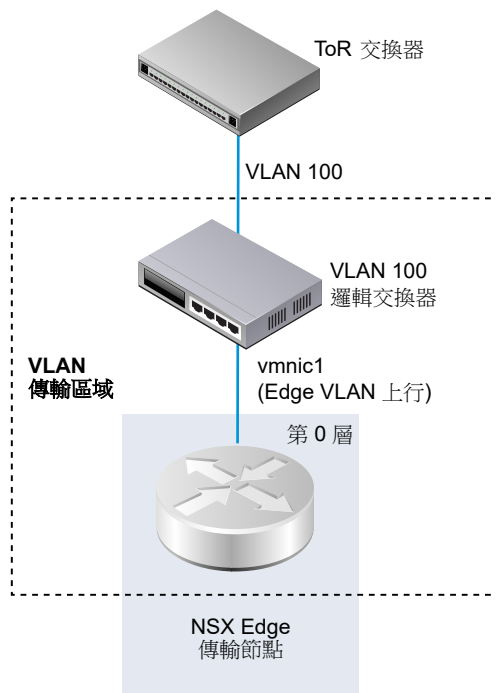
您也可以使用 GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics` API 呼叫來檢視橋接器流量：

```
{
  "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。



必要條件

- 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 Data Center vSwitch 新增到 NSX Edge。若要在 Edge 上確認，請執行 `get host-switches` 命令。例如：

```
nsx-edge1> get host-switches

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 Data Center 管理平面代理程式 (MPA) 與 NSX-T Data Center 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 Data Center 安裝指南》。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**新增**。
- 4 輸入邏輯交換器的名稱。
- 5 選取邏輯交換器的傳輸區域。
- 6 選取上行整併原則。
- 7 對於管理狀態，選取**開啟**或**關閉**。
- 8 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。

- 9 (選擇性) 按一下**交換設定檔**索引標籤並選取交換設定檔。

結果

備註 如果您有兩個 VLAN 邏輯交換器具有相同的 VLAN 識別碼，則這兩個交換器無法連線至相同的 Edge N-VDS (先前稱為主機交換器)。如果您有一個 VLAN 邏輯交換器和一個覆疊邏輯交換器，且 VLAN 邏輯交換器的 VLAN 識別碼與覆疊邏輯交換器的傳輸 VLAN 識別碼相同，則它們同樣無法連線至相同的 Edge N-VDS。

後續步驟

新增邏輯路由器。

將虛擬機器連線到邏輯交換器

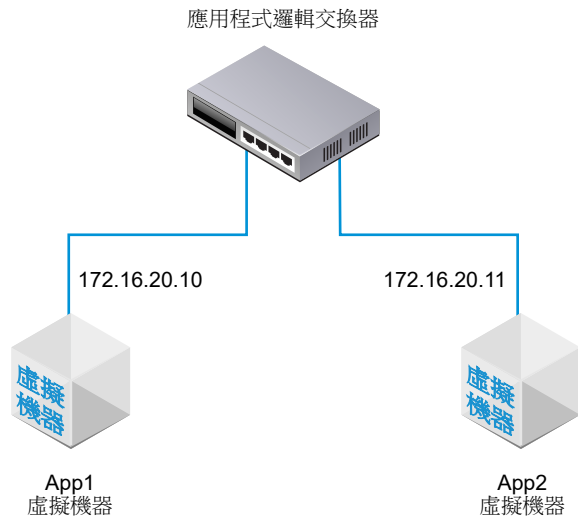
視主機而定，用來將虛擬機器連線到邏輯交換器的組態可能會有所不同。

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 Data Center 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 Data Center 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 Data Center 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 Data Center 邏輯交換器](#)。

必要條件

- 虛擬機器必須裝載在已新增至 NSX-T Data Center 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T Data Center 管理平面 (MPA) 和 NSX-T Data Center 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 Data Center 邏輯交換器。

例如：



- 2 按一下**確定**。

結果

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 Data Center API 中，您可以檢視與連結 NSX-T Data Center 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 Data Center 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《NSX-T Data Center 管理指南》中的〈監控邏輯交換器連接埠活動〉。

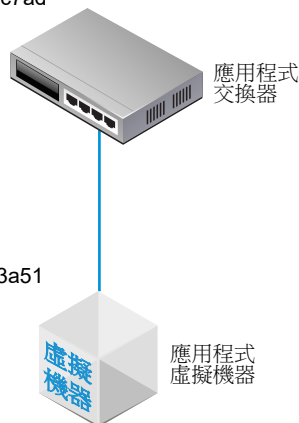
將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T Data Center 邏輯交換器

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 Data Center 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



必要條件

- 虛擬機器必須裝載在已新增至 NSX-T Data Center 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T Data Center 管理平面 (MPA) 和 NSX-T Data Center 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

The screenshot shows the 'Add New Hardware' window in vSphere Client. The 'Add New Network' section is expanded and highlighted in yellow. It shows the configuration for a VMXNET 3 network adapter. The network name is 'VM Network'. The adapter type is 'VMXNET 3'. The 'Open connection at power on' checkbox is checked. Other hardware components like CPU, Memory, Hard Disk, SCSI Controller, CD/DVD Drive, and Floppy Drive are also visible in the list.

- 2 使用 NSX-T Data Center 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 /vmtoolsd/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 /vmtoolsd/power.off 5
Powering off VM:

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

```

4 從 NSX Manager UI 取得邏輯交換器識別碼。

例如：

app-switch

概觀 監控 管理 ▾ 相關 ▾

▽ 摘要 | 編輯

名稱	app-switch
識別碼	b68e7ac3-877a-420e-af47-53e974c17915
位置	
說明	lswitch202 (created through automation)
管理狀態	● 開啟
複寫模式	源頭複寫
VLAN	不適用
VNI	71681
邏輯連接埠	1
流量類型	覆蓋
傳輸區域	transportzone1
上行整併原則名稱	[Use Default]
N-VDS 模式	STANDARD
建立時間	9/10/2018, 12:20:46 PM (由 admin)
上次更新時間	9/26/2018, 2:01:14 PM (由 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

```
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

```

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。
- 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:

```

結果

在 NSX Manager UI 的 **交換 > 連接埠** 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

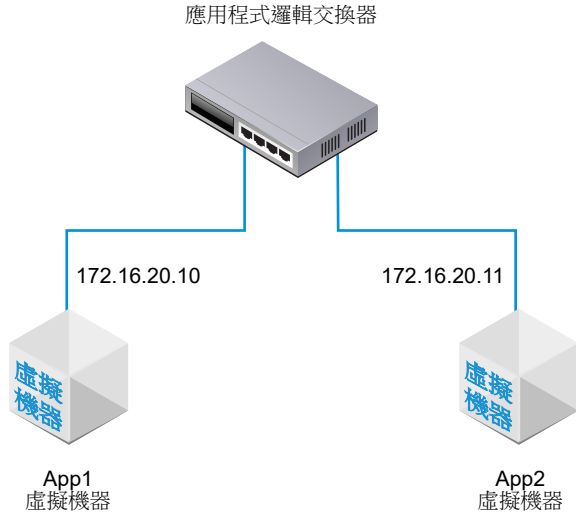
新增邏輯路由器。

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《NSX-T Data Center 管理指南》中的〈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 Data Center 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 Data Center 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。



必要條件

- 虛擬機器必須裝載在已新增至 NSX-T Data Center 網狀架構的 Hypervisor 上。
- 網狀架構節點必須具有 NSX-T Data Center 管理平面 (MPA) 和 NSX-T Data Center 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。

結果

在 **交換 > 連接埠** 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。

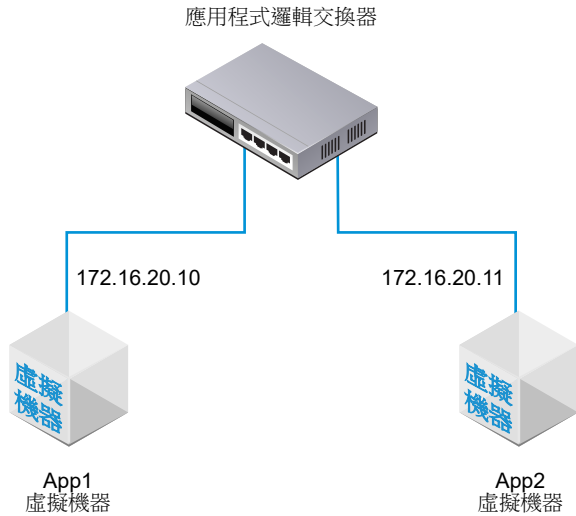
您可以監控邏輯交換器連接埠上的活動以針對問題進行疑難排解。請參閱《NSX-T Data Center 管理指南》中的〈監控邏輯交換器連接埠活動〉。

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 1-3. 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 (選擇性) 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
get logical-switch <vni-or-uuid> arp-table	顯示所指定邏輯交換器的 ARP 表格。 輸出範例。 <pre>nsx-controller1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
get logical-switch <vni-or-uuid> connection-table	顯示所指定邏輯交換器的連線。 輸出範例。 <pre>nsx-controller1> 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>
get logical-switch <vni-or-uuid> mac-table	顯示所指定邏輯交換器的 MAC 表格。 輸出範例。 <pre>nsx-controller1> 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>
get logical-switch <vni-or-uuid> stats	顯示所指定邏輯交換器的相關統計資訊。 輸出範例。 <pre>nsx-controller1> 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>
get logical-switch <vni-or-uuid> stats-sample	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> 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>
get logical-switch <vni-or-uuid> vtep	<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> 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>

結果

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。

邏輯交換器連接埠

2

邏輯交換器具有多個交換器連接埠。路由器、虛擬機器或容器等實體可以透過邏輯交換器連接埠連線至邏輯交換器。

本章節討論下列主題：

- [建立邏輯交換器連接埠](#)
- [監控邏輯交換器連接埠活動](#)

建立邏輯交換器連接埠

邏輯交換器連接埠可讓您將其他網路元件、虛擬機器或容器連線至邏輯交換器。

如需關於將虛擬機器連線至邏輯交換器的詳細資訊，請參閱[將虛擬機器連線到邏輯交換器](#)。如需有關將容器連線至邏輯交換器的詳細資訊，請參閱《適用於 Kubernetes 的 NSX-T Container Plug-in - 安裝和管理指南》。

備註 繫結至容器的邏輯交換器連接埠的 IP 位址和 MAC 位址由 NSX Manager 配置。請勿手動變更位址繫結。

必要條件

確認已建立邏輯交換器連接埠。請參閱[第 1 章 邏輯交換器與設定虛擬機器連結](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的[網路 > 交換](#)。
- 3 按一下[連接埠](#)索引標籤。
- 4 按一下[新增](#)。
- 5 在[一般](#)索引標籤中，完成連接埠詳細資料。

選項	說明
名稱與說明	輸入名稱和 (選用) 說明。
邏輯交換器	從下拉式清單中選取邏輯交換器。

選項	說明
管理狀態	選取 開啟 或 關閉 。
連結類型	選取 無 或 VIF 。
連結識別碼	如果連結類型為 VIF ，請輸入連結識別碼。

6 (選擇性) 在**交換設定檔**索引標籤中，選取交換設定檔。

7 按一下**儲存**。

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

必要條件

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

2 選取導覽面板中的**網路 > 交換**。

3 按一下**連接埠**索引標籤。

4 按一下連接埠的名稱。

5 按一下**監控**索引標籤。

此時會顯示連接埠狀態和統計資料。

6 若要下載主機已知的 MAC 位址的 CSV 檔案，請按一下**下載 MAC 資料表**。

7 若要監控連接埠上的活動，請按一下**開始追蹤**。

[連接埠追蹤] 頁面隨即開啟。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。

結果

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](#)。

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)
- 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。

本章節討論下列主題：

- [瞭解 QoS 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 Data Center 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。這些設定無法保證頻寬，僅能協助限制網路頻寬的使用。您將看到的實際頻寬取決於連接埠的連結速度或交換設定檔中的值 (以較低者為準)。

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。

必要條件

- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**交換設定檔**索引標籤。
- 4 按一下**新增**並選取 **QoS**。
- 5 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。
模式	從 [模式] 下拉式功能表中選取 信任 或 未受信任 選項。 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。 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。 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。
優先順序	設定 CoS 優先順序值。 優先順序值範圍從 0 至 63，其中 0 具有最高的優先順序。
服務類別	設定 CoS 值。 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。 CoS 值範圍從 0 至 7，其中 0 是優先順序最低的服務。
入口	設定從虛擬機器至邏輯網路的輸出網路流量自訂值。 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。 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。
入口廣播	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。 預設值為 0，表示停用入口廣播流量。 例如，當您將邏輯交換器的平均頻寬設定為 50 Kbp 時，原則便會限制頻寬。您可以為 400 Kbp 的高載流量設定 60 個位元組持續時間的上限。
出口	設定從邏輯網路至虛擬機器的輸入網路流量自訂值。 預設值為 0，表示停用出口流量。

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。

- 6 按一下**儲存**。

結果

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或邏輯連接埠，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](#)或[建立自訂設定檔與邏輯連接埠之間的關聯](#)。

瞭解 IP 探索交換設定檔

IP 探索會使用 DHCP 窺探、ARP 窺探或 VM Tools 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。

VM Tools 是一種執行在 ESXi 主控虛擬機器上的軟體，可提供包括 MAC 和 IP 位址的虛擬機器組態資訊。此 IP 探索方法僅適用於在 ESXi 主機上執行的虛擬機器。

備註 對於 Linux 虛擬機器，ARP 流量問題可能會導致 ARP 窺探取得不正確的資訊。可透過使用 ARP 篩選器防止出現此問題。如需詳細資訊，請參閱<http://linux-ip.net/html/ether-arp.html#ether-arp-flux>。

設定 IP 探索交換設定檔

您可以啟用 ARP 窺探、DHCP 窺探或 VM Tools 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。VM Tools IP 探索方法僅適用於裝載 ESXi 的虛擬機器。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**交換設定檔**索引標籤。
- 4 按一下**新增**，然後選取**IP 探索**。
- 5 完成 IP 探索交換設定檔詳細資料。

選項	說明
名稱與說明	輸入名稱和 (選用) 說明。
ARP 窺探	<p>切換 ARP 窺探 按鈕以啟用功能。</p> <p>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。</p>

選項	說明
ARP 繫結限制	指定 ARP 繫結限制 (從 1 到 128)。
DHCP 窺探	切換 DHCP 窺探 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。
VM Tools	切換 VM Tools 按鈕以啟用功能。這個選項僅適用於裝載 ESXi 的虛擬機器。 VM Tools 是一種在裝載 ESXi 之虛擬機器上執行的軟體，可提供虛擬機器的 MAC 和 IP 位址。

6 按一下儲存。

結果

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或邏輯連接埠，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](#)或[建立自訂設定檔與邏輯連接埠之間的關聯](#)。

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 Data Center 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**網路 > 交換**。
- 2 按一下**連接埠**索引標籤。
- 3 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。
- 4 在**概觀**索引標籤中，展開**位址繫結**。
- 5 按一下**新增**。
新增位址繫結對話方塊隨即顯示
- 6 指定您要套用位址繫結之邏輯連接埠的 IP 和 MAC 位址。您也可以指定 VLAN 識別碼。
- 7 按一下**新增**。

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 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。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。

- 3 按一下**交換設定檔**索引標籤。
- 4 按一下**新增**，然後選取 **Spoofguard**。
- 5 輸入名稱和 (選用) 說明。
- 6 若要啟用連接埠層級 SpoofGuard，請將**連接埠繫結**設為已啟用。
- 7 按一下**新增**。

結果

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或邏輯連接埠相關聯。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)或[建立自訂設定檔與邏輯連接埠之間的關聯](#)。

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。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**交換設定檔**索引標籤。
- 4 按一下**新增**，然後選取**交換器安全性**。

5 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。
BPDU 篩選器	切換 BPDU 篩選器 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 伺服器封鎖 按鈕及 用戶端封鎖 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。
封鎖非 IP 流量	切換 封鎖非 IP 流量 按鈕以僅允許 IPv4、IPv6、ARP、GARP 和 BPDU 流量。 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 SpoofGuard 組態中所設定的其他原則而定。 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。
速率限制	設定入口與出口廣播及多點傳送流量的速率限制。 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。 若要避免任何連線問題，最低速率限制值必須 ≥ 10 pps。

6 按一下新增。

結果

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或邏輯連接埠，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](#)或[建立自訂設定檔與邏輯連接埠之間的關聯](#)。

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 位址變更功能可讓虛擬機器變更其 MAC 位址。連線至連接埠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。

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。

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。

設定 MAC 管理交換設定檔

您可以建立 MAC 管理交換設定檔來管理 MAC 位址。

必要條件

自行熟悉 MAC 管理交換設定檔概念。請參閱[瞭解 MAC 管理交換設定檔](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**交換設定檔**索引標籤。
- 4 按一下**新增**，然後選取 **MAC 管理**。
- 5 完成 MAC 管理設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派給 MAC 管理設定檔。 您可以選擇性地描述您在設定檔中修改的設定。
MAC 變更	啟用或停用 MAC 位址變更功能。
狀態	啟用或停用 MAC 學習功能。

- 6 按一下**新增**。

結果

MAC 管理設定檔會顯示為連結。

後續步驟

將交換設定檔連結至邏輯交換器或邏輯連接埠。請參閱[建立自訂設定檔與邏輯交換器之間的關聯](#)或[建立自訂設定檔與邏輯連接埠之間的關聯](#)。

建立自訂設定檔與邏輯交換器之間的關聯

您可以建立自訂交換器設定檔與邏輯交換器之間的關聯，使設定檔能套用至交換器上的所有連接埠。

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。

必要條件

- 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 [邏輯交換器和邏輯連接埠的交換設定檔](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的[網路 > 交換](#)。
- 3 按一下[交換器](#)索引標籤。
- 4 按一下邏輯交換器以套用自訂交換設定檔。
- 5 按一下[管理](#)索引標籤。
- 6 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](#)
 - [IP 探索](#)
 - [SpoofGuard](#)
 - [交換器安全性](#)
 - [MAC 管理](#)
- 7 按一下[變更](#)。
- 8 從下拉式功能表中選取先前建立的自訂交換設定檔。
- 9 按一下[儲存](#)。
邏輯交換器現在會與自訂交換設定檔建立關聯。
- 10 確認[管理](#)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。
- 11 (選擇性) 按一下[相關](#)索引標籤，然後從下拉式功能表中選取[連接埠](#)，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連接埠之間的關聯](#)。

建立自訂設定檔與邏輯連接埠之間的關聯

邏輯連接埠提供 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連接埠的自訂交換設定檔。

必要條件

- 確認已設定邏輯連接埠。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 邏輯交換器和邏輯連接埠的交換設定檔](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**連接埠**索引標籤。
- 4 按一下邏輯連接埠以套用自訂交換設定檔。
- 5 按一下**管理**索引標籤。
- 6 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
 - IP 探索
 - SpoofGuard
 - 交換器安全性
 - MAC 管理
- 7 按一下**變更**。
- 8 從下拉式功能表中選取先前建立的自訂交換設定檔。
- 9 按一下**儲存**。

邏輯連接埠現在會與自訂交換設定檔建立關聯。

- 10 確認**管理**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《NSX-T Data Center 管理指南》中的〈監控邏輯交換器連接埠活動〉。

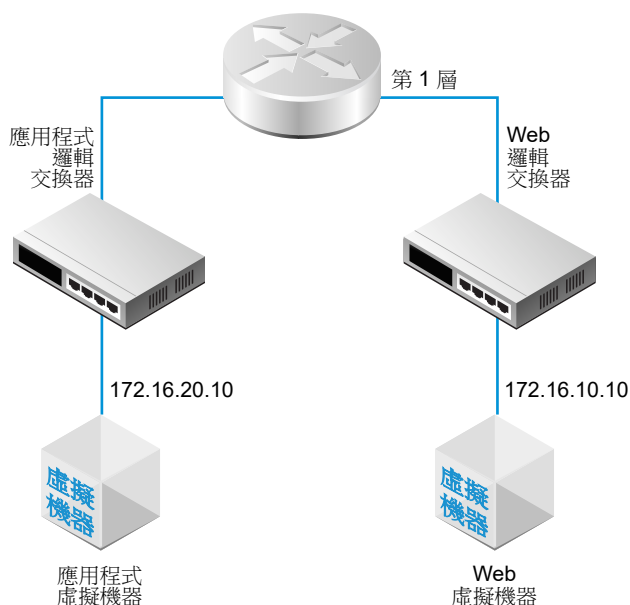
第 1 層邏輯路由器

4

NSX-T Data Center 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 Data Center 邏輯交換器，以及上行連接埠可連線至 NSX-T Data Center 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。

本章節討論下列主題：

- 建立第 1 層邏輯路由器
- 在第 1 層邏輯路由器上新增下行連接埠
- 在第 0 層或第 1 層邏輯路由器上新增 VLAN 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
- 建立獨立的第 1 層邏輯路由器

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。

必要條件

- 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 Data Center 安裝指南》。
- 自行熟悉第 1 層邏輯路由器拓撲。請參閱[第 4 章 第 1 層邏輯路由器](#)。

程序

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

2 選取導覽面板中的**網路 > 路由**。

3 按一下**新增**，然後選取**第 1 層路由器**。

4 輸入邏輯路由器的名稱，並選擇性地輸入說明。

5 (選擇性) 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 (選擇性) 選取要連線至這個第 1 層邏輯路由器的 NSX 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。如果您尚未設定任何 NSX Edge 叢集，則可以先暫時將此欄位保留空白，稍後再編輯路由器組態。

7 (選擇性) 如果您選取了 NSX Edge 叢集，請選取容錯移轉模式。

選項	說明
先佔式	若偏好的節點失敗並復原，則它將會取代其對等項而成為作用中節點。該對等項的狀態會變更為待命。這是預設的選項。
非先佔式	若偏好的節點失敗並復原，則它將會檢查其對等項是否為作用中節點。如果是，則偏好的節點不會取代其對等項，且將會成為待命節點。

8 (選擇性) 按一下**進階**索引標籤，然後輸入**內部第 1 層傳送子網路**的值。

9 按一下**新增**。

在 NSX Manager UI 中，新的邏輯路由器是可點選的連結。

結果

如果此邏輯路由器支援超過 5000 個虛擬機器，您必須對 NSX Edge 叢集的每個節點執行下列命令，以增加 ARP 資料表的大小。

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

您必須在數據平面重新啟動或節點重新開機之後重新執行這些命令，因為變更並非持續性的。

後續步驟

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

在第 1 層邏輯路由器上新增下行連接埠

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。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下路由器的名稱。
- 4 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 5 按一下**新增**。
- 6 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 7 在**類型**欄位中，選取下行。
- 8 對於 **URPF 模式**，請選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 9 (選擇性) 選取邏輯交換器。
- 10 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。
- 11 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。
- 12 (選擇性) 選取 DHCP 轉送服務。
- 13 按一下**新增**。

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 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠

如果您僅有 VLAN 支援的邏輯交換器，可以將交換器連線至第 0 層或第 1 層路由器上的 VLAN 連接埠，以便 NSX-T Data Center 提供第 3 層服務。

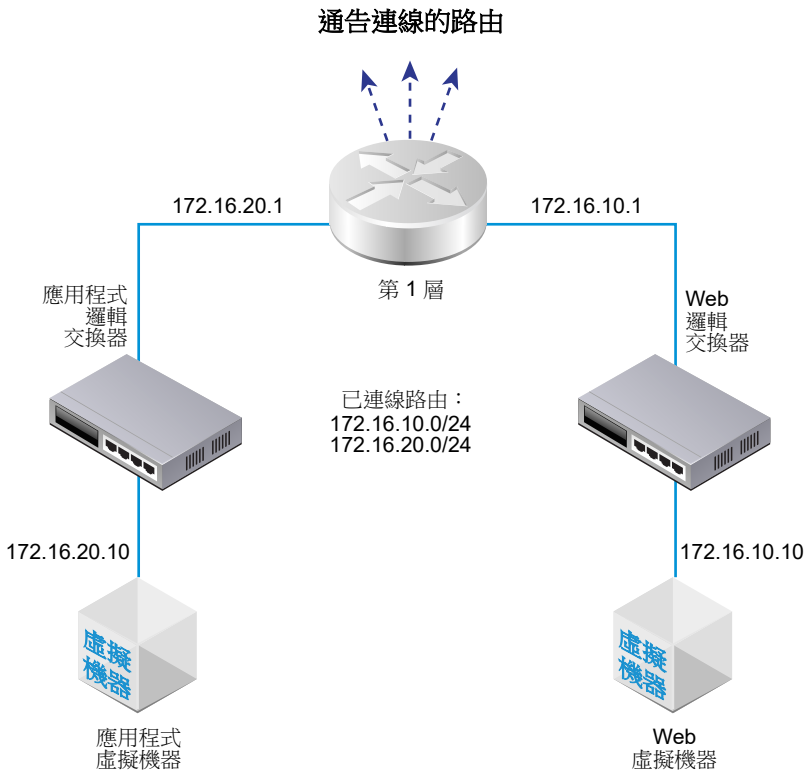
程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下路由器的名稱。
- 4 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 5 按一下**新增**。
- 6 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 7 在**類型**欄位中，選取**集中式**。
- 8 對於 **URPF 模式**，請選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 9 (必要) 選取邏輯交換器。
- 10 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。
- 11 以 CIDR 標記法輸入路由器連接埠 IP 位址。
- 12 按一下**新增**。

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 Data Center 會自動建立 NSX-T Data Center 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。



必要條件

- 確認虛擬機器連結至邏輯交換器。請參閱第 1 章 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。請參閱在第 1 層邏輯路由器上新增下行連接埠。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下第 1 層路由器的名稱。
- 4 從**路由**下拉式功能表中選取**路由通告**。
- 5 按一下**編輯**以編輯路由通告組態。

您可以切換下列參數：

- 狀態
- 通告所有 **NSX** 連線的路由
- 通告所有 **NAT** 路由
- 通告所有靜態路由
- 通告所有 **LB VIP** 路由

- 通告所有 LB SNAT IP 路由

- a 按一下**儲存**。

6 按一下**新增**以通告路由。

- a 輸入名稱和 (選用) 說明。

- b 以 CIDR 格式輸入路由首碼。

- c 按一下**套用篩選器**以設定下列選項：

動作	指定 允許 或 拒絕 。
符合路由類型	選取一或多個下列項目： <ul style="list-style-type: none"> ■ 任何 ■ NSX 已連線 ■ 第 1 層 LB VIP ■ 靜態 ■ 第 1 層 NAT ■ 第 1 層 LB SNAT
前置運算子	選取 GE 或 EQ 。

- d 按一下**新增**。

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 第 0 層邏輯路由器](#)。

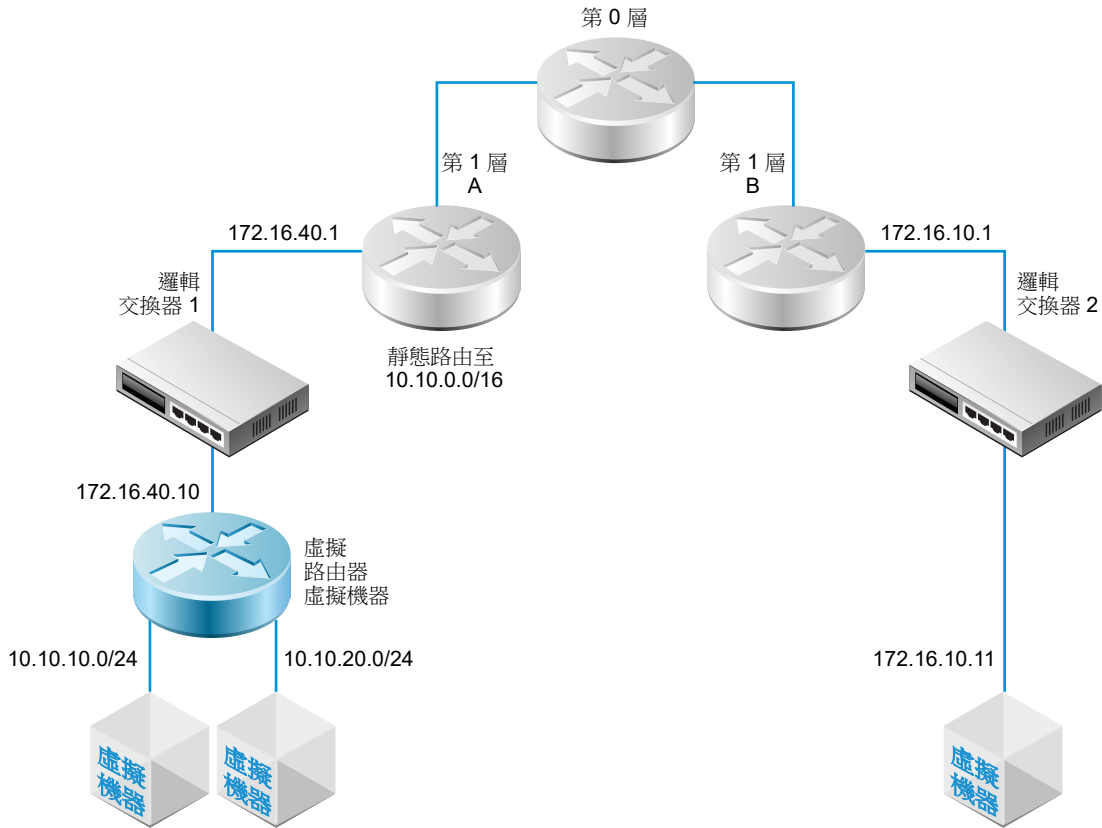
如果您已經有連線至第 1 層邏輯路由器的第 0 層邏輯路由器，則可以確認第 0 層路由器學習連線第 1 層路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

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 Data Center 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 Data Center 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 Data Center 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

**必要條件**

確認已設定下行連接埠。請參閱在**第 1 層邏輯路由器上新增下行連接埠**。

程序

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

2 選取導覽面板中的**網路 > 路由**。

3 按一下第 1 層路由器的名稱。

4 按一下**路由索引**標籤，然後從下拉式功能表中選取**靜態路由**。

5 按一下**新增**。

6 以 CIDR 格式輸入網路位址。

例如，10.10.10.0/16。

7 按一下**新增**以新增下一個躍點 IP 位址。

例如，172.16.40.10。您也可以透過按一下鉛筆圖示，然後從下拉式功能表中選取 **NULL** 來指定空值路由。若要再新增下一個躍點位址，請再按一下**新增**。

8 按一下對話方塊底部的**新增**。

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**。
- 10 按一下**編輯**，然後選取**通告所有靜態路由**。
- 11 按一下**儲存**。

靜態路由便會跨越 NSX-T Data Center 覆疊進行傳播。

建立獨立的第 1 層邏輯路由器

獨立的第 1 層邏輯路由器沒有下行，且無法連線至第 0 層路由器。它具有服務路由器，但沒有分散式路由器。在主動-待命模式下，服務路由器可以在一個 NSX Edge 節點或兩個 NSX Edge 節點上部署。

獨立的第 1 層邏輯路由器：

- 不得連線至第 0 層邏輯路由器。
- 不得具有下行。
- 如果用來連結負載平衡器 (LB) 服務，則只能有一個集中式服務連接埠 (CSP)。
- 可以連線至覆疊邏輯交換器或 VLAN 邏輯交換器。
- 僅支援負載平衡和 NAT 服務。

通常，獨立的第 1 層邏輯路由器會連線至邏輯交換器，此邏輯交換器同時已連線一般的第 1 層邏輯路由器。設定靜態路由和路由通告之後，獨立的第 1 層邏輯路由器可透過一般的第 1 層邏輯路由器與其他裝置進行通訊。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下**新增**，然後選取**第 1 層路由器**。
- 4 輸入邏輯路由器的名稱，並選擇性地輸入說明。
- 5 (必要) 選取要連線至這個第 1 層邏輯路由器的 NSX Edge 叢集。
- 6 (必要) 選取容錯移轉模式和叢集成員。

選項	說明
先佔式	若偏好的節點失敗並復原，則它將會取代其對等項而成為作用中節點。該對等項的狀態會變更為待命。這是預設的選項。
非先佔式	若偏好的節點失敗並復原，則它將會檢查其對等項是否為作用中節點。如果是，則偏好的節點不會取代其對等項，且將會成為待命節點。

- 7 按一下**新增**。
- 8 按一下您剛建立的路由器的名稱。
- 9 按一下**組態索引標籤**，然後選取**路由器連接埠**。
- 10 按一下**新增**。

- 11 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 12 在**類型**欄位中，選取**集中式**。
- 13 對於 **URPF 模式**，請選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 14 (必要) 選取邏輯交換器。
- 15 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。
- 16 以 CIDR 標記法輸入路由器連接埠 IP 位址。
- 17 按一下**新增**。

結果

使用獨立的第 1 層邏輯路由器之前，請注意下列幾點：

- 若要針對獨立的第 1 層邏輯路由器指定預設閘道，您必須新增靜態路由。子網路應為 0.0.0.0/0，且下一個躍點是連線至同一個交換器的一般第 1 層路由器的 IP 位址。
- 不支援獨立路由器上的 ARP Proxy。因此，除非您使用 CSP IP，否則不得在 CSP 的子網路中設定 LB 虛擬伺服器 IP 或 LB SNAT IP。例如，如果 CSP IP 為 1.1.1.1/24，則虛擬 IP 必須為 1.1.1.1 或某些其他子網路 IP 位址。不可為 1.1.1.1/24 子網路中的任何其他位址。
- 對於 NSX Edge 虛擬機器，不能有多個 CSP 連線至 VLAN 支援的相同邏輯交換器，或具有相同 VLAN 識別碼的 VLAN 支援的不同邏輯交換器。

第 0 層邏輯路由器

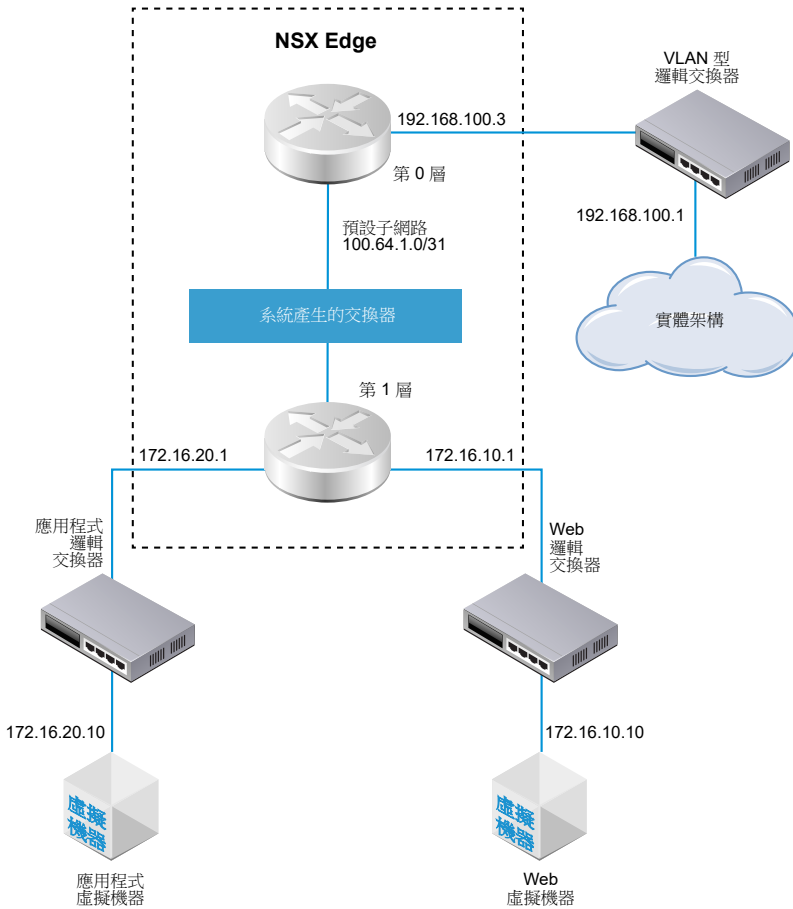
5

NSX-T Data Center 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 Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

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。

本章節討論下列主題：

- 建立第 0 層邏輯路由器
- 連結第 0 層和第 1 層
- 針對 **NSX Edge** 上行，將第 0 層邏輯路由器連線至 **VLAN** 邏輯交換器
- 新增回送路由器連接埠
- 在第 0 層或第 1 層邏輯路由器上新增 **VLAN** 連接埠
- 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
- 建立社群清單
- 建立路由對應
- 設定轉送累計計時器

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 Data Center 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。

必要條件

- 確認已安裝至少一個 NSX Edge。請參閱《NSX-T Data Center 安裝指南》。
- 確認您的 NSX Controller 叢集處於穩定狀態。
- 確認已設定 NSX Edge 叢集。請參閱《NSX-T Data Center 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 第 0 層邏輯路由器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 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 NSX Edge 叢集，用以支援這個第 0 層邏輯路由器。
- 7 (選擇性) 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 (選擇性) 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 (選擇性) 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 (選擇性) 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。

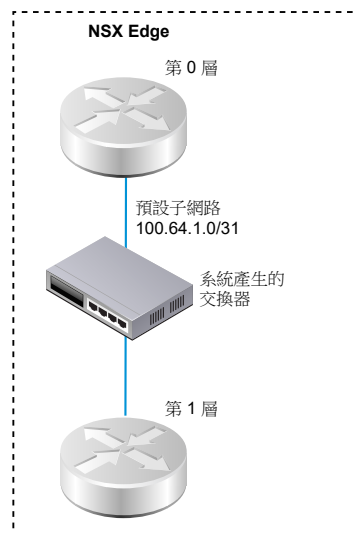
設定第 0 層邏輯路由器，將其連線至 VLAN 邏輯交換器以建立對外部網路的上行連接埠。請參閱[針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。

- 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 (選擇性) 從下拉式功能表中選取 NSX 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 NSX 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 NSX Edge 叢集並將成員與偏好的成員欄位保留空白，則 NSX-T Data Center 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 Data Center 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 Data Center 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

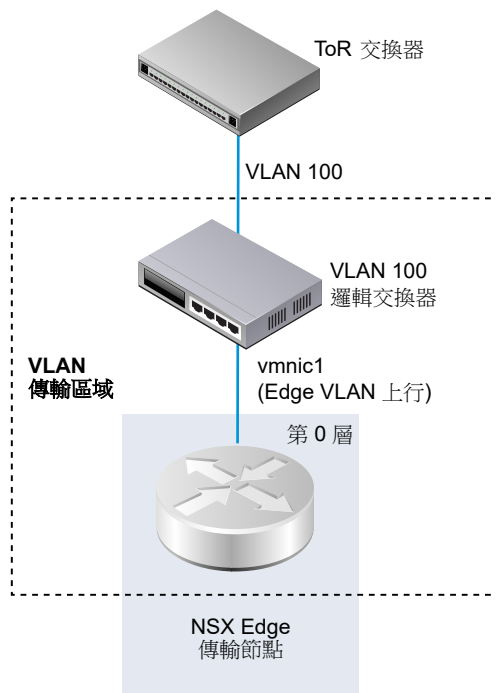
b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]      via 169.254.0.1
c   169.254.0.0/28    [0/0]      via 169.254.0.2
ns  172.16.10.0/24 [3/3] via 169.254.0.1 ns 172.16.20.0/24 [3/3] via 169.254.0.1
c   192.168.100.0/24  [0/0]      via 192.168.100.2

```

針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器

若要建立 NSX Edge 上行，必須將第 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。



必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 選取第 0 層邏輯路由器。
- 4 從**組態**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。

結果

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。

必要條件

- 確認第 0 層邏輯路由器已連線至 VLAN 邏輯交換器。請參閱[針對 NSX Edge 上行，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
```

結果

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](#)。

新增回送路由器連接埠

您可以將回送連接埠新增至第 0 層邏輯路由器。

回送連接埠可用於下列目的：

- 路由通訊協定的路由器識別碼
- NAT
- BFD
- 路由通訊協定的來源位址

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 選取第 0 層邏輯路由器。
- 4 選取**組態 > 路由器連接埠**
- 5 按一下**新增**。
- 6 輸入名稱和 (選用) 說明。
- 7 選取**回送類型**。
- 8 選取 **Edge 傳輸節點**。
- 9 以 CIDR 格式輸入 IP 位址。

結果

系統會新增第 0 層路由器的新連接埠。

在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠

如果您僅有 VLAN 支援的邏輯交換器，可以將交換器連線至第 0 層或第 1 層路由器上的 VLAN 連接埠，以便 NSX-T Data Center 提供第 3 層服務。

程序

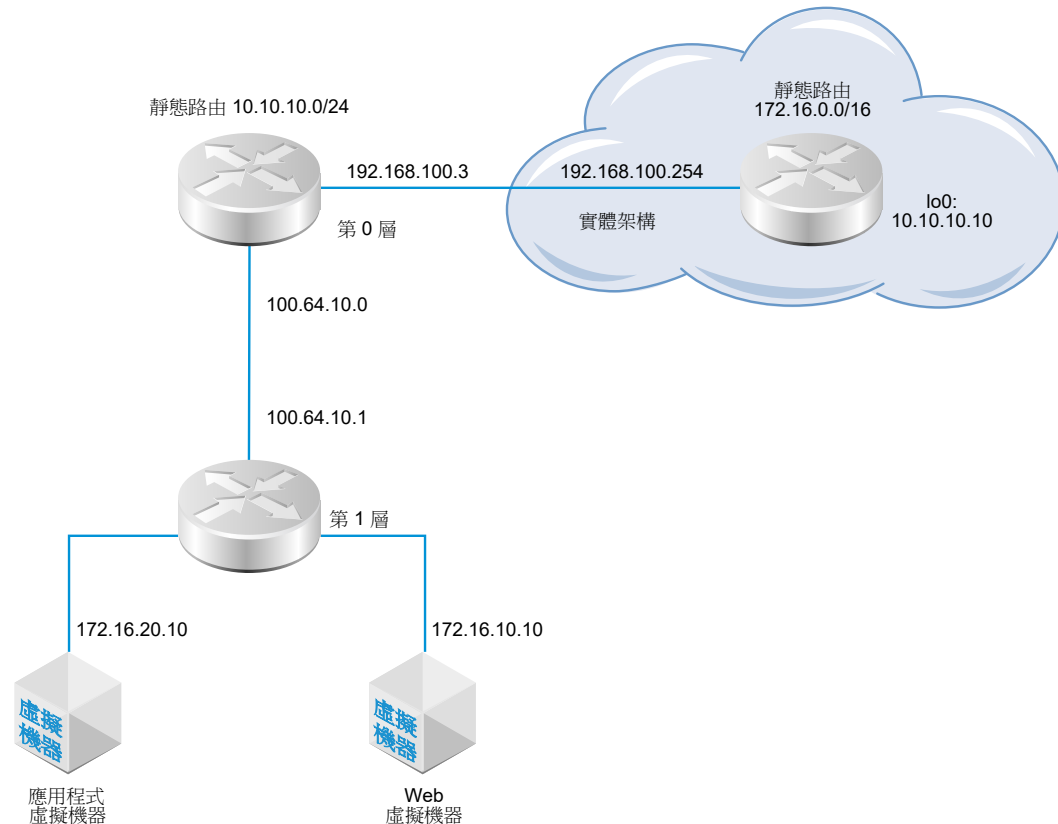
- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下路由器的名稱。
- 4 按一下**組態索引標籤**，然後選取**路由器連接埠**。
- 5 按一下**新增**。
- 6 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 7 在**類型**欄位中，選取**集中式**。
- 8 對於 **URPF 模式**，請選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 9 (必要) 選取邏輯交換器。
- 10 選取此連接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。
- 11 以 CIDR 標記法輸入路由器連接埠 IP 位址。
- 12 按一下**新增**。

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



必要條件

- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的網路 > 路由。
- 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靜態路由。
- 5 選取新增。

- 6 以 CIDR 格式輸入網路位址。

例如，10.10.10.0/24。

- 7 按一下 **+ 新增**以新增下一個躍點 IP 位址。

例如，192.168.100.254。您也可以透過按一下鉛筆圖示，然後從下拉式功能表中選取 **NULL** 來指定空值路由。

- 8 指定管理距離。

- 9 從下拉式清單中選取邏輯路由器連接埠。

清單包含 IPSec 虛擬通道介面 (VTI) 連接埠。

- 10 按一下**新增**按鈕。

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。

必要條件

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 Data Center 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。

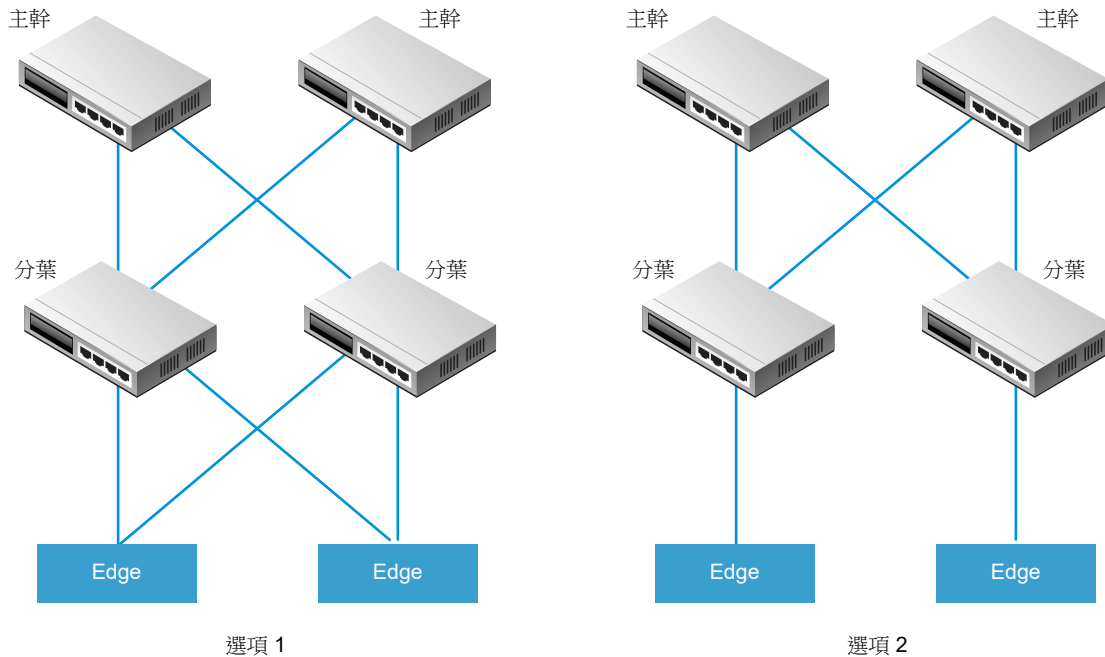
```
ping 10.10.10.10
```

```
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

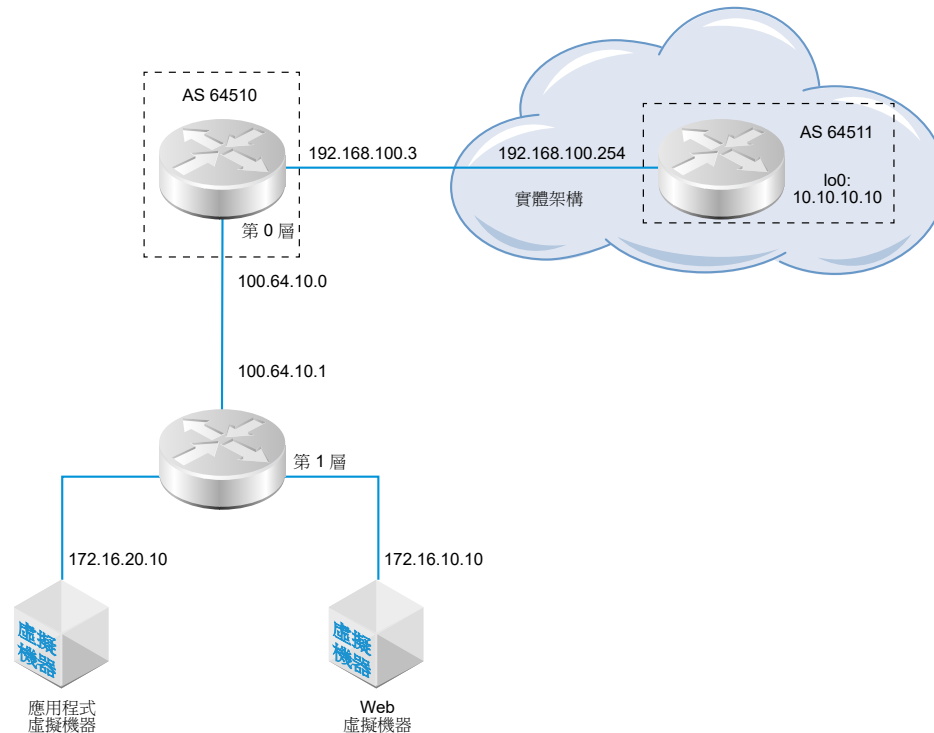
如果要啟用您虛擬機器與外部環境之間的存取，您可以設定第 0 層邏輯路由器與實體基礎結構中之路由器之間的外部 BGP (eBGP) 連線。

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。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



必要條件

- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的網路 > 路由。
- 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 BGP。

5 按一下編輯。

- a 設定本機 AS 數目。

例如，64510。

- b 按一下**狀態**切換按鈕以啟用 BGP。

[狀態] 按鈕必須顯示為 [已啟用]。

- c (選擇性) 按一下 **ECMP** 切換按鈕以啟用 ECMP。

- d (選擇性) 按一下**正常重新啟動**切換按鈕以啟用正常重新啟動。

- e (選擇性) 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 NSX Edge 叢集只有一個 Edge 節點時才支援正常重新啟動。

- f 按一下**儲存**。

6 按一下新增以新增 BGP 芳鄰。**7 請輸入芳鄰 IP 位址。**

例如，192.168.100.254。

8 (選擇性) 指定躍點上限。

預設值為 1。

9 請輸入遠端 AS 數目。

例如，64511。

10 (選擇性) 設定計時器 (保持連線時間及等候時間) 及密碼。**11 (選擇性) 按一下本機位址索引標籤可選取本機位址。**

- a (選擇性) 取消選取所有上行可查看回送連接埠以及上行連接埠。

12 (選擇性) 按一下位址家族索引標籤可新增位址家族。**13 (選擇性) 按一下 BFD 組態索引標籤可啟用 BFD。****14 按一下儲存。****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。

必要條件

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。

備註 在此版本中，不支援虛擬通道介面 (VTI) 連接埠上的 BFD。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 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 (選擇性) 按一下「靜態路由下一個躍點的 BFD 對等」下的**新增**以新增 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。

必要條件

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

- 2 選取導覽面板中的**網路 > 路由**。
- 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 <code>advertise-to-bgp-neighbor</code> 。
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 Data Center 之虛擬機器的外部路由器來進行檢查。

必要條件

- 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 Data Center 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 Data Center 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 Data Center 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 Data Center 覆疊的路徑。

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  100.91.176.1 (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

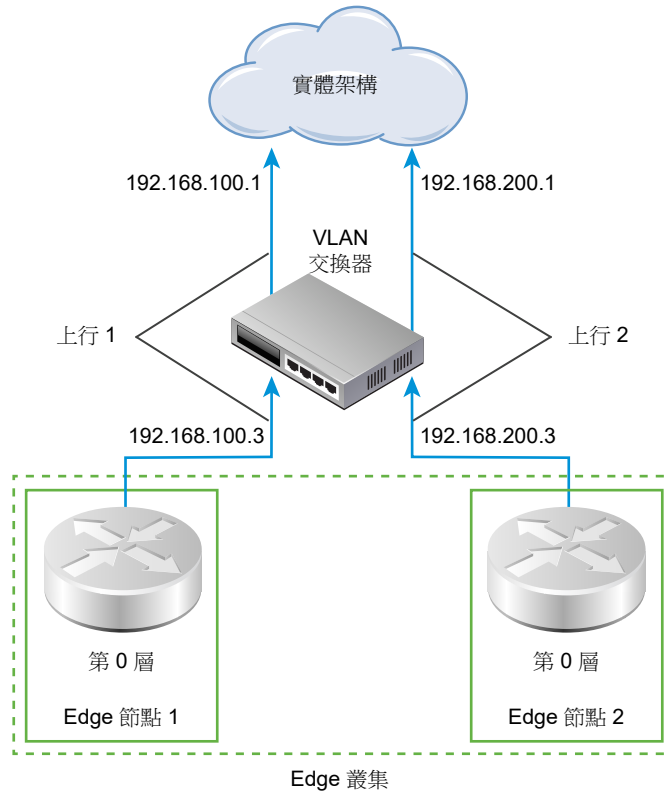
設定其他路由功能，例如 ECMP。

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 NSX 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 NSX 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 NSX 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。

必要條件

- 確認已設定傳輸區域和兩個傳輸節點。請參閱《NSX-T Data Center 安裝指南》。
- 確認已設定兩個 Edge 節點和 Edge 叢集。請參閱《NSX-T Data Center 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 選取第 0 層邏輯路由器。
- 4 按一下**組態索引**標籤以新增路由器連接埠。
- 5 按一下**新增**。
- 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	接受預設類型上行。
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。

- 7 按一下**儲存**。

結果

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。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。

- 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 **BGP**。
- 5 按一下 [芳鄰] 區段下的**新增**以新增 BGP 芳鄰。
- 6 請輸入芳鄰 IP 位址。
例如，192.168.200.254。
- 7 (選擇性) 指定躍點上限。
預設值為 1。
- 8 請輸入遠端 AS 數目。
例如，64511。
- 9 (選擇性) 按一下**本機位址**索引標籤可選取本機位址。
 - a (選擇性) 取消選取**所有上行**可查看回送連接埠以及上行連接埠。
- 10 (選擇性) 按一下**位址家族**索引標籤可新增位址家族。
- 11 (選擇性) 按一下 **BFD 組態**索引標籤可啟用 BFD。
- 12 按一下**儲存**。
隨即顯示新增的 BGP 芳鄰。
- 13 按一下 [BGP 組態] 區段旁的**編輯**。
- 14 按一下 **ECMP** 切換按鈕以啟用 ECMP。
[狀態] 按鈕必須顯示為 [已啟用]。
- 15 按一下**儲存**。

結果

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。

必要條件

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。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，請務必建立不含特定網路位址 (從下拉式清單中選取**任何**) 且具備**允許**動作的 IP 首碼。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**網路 > 路由**。
- 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 按一下**新增**。
- 6 輸入 IP 首碼清單的名稱。

- 7 按一下**新增**以指定首碼。
 - a 以 CIDR 格式輸入 IP 位址。
例如，192.168.100.3/27。
 - b 從下拉式功能表中選取**拒絕**或**允許**。
 - c (選擇性) 以 **le** 或 **ge** 修飾詞設定 IP 位址數字的範圍。
例如，將 **le** 設定為 30 並將 **ge** 設定為 24。
- 8 重複先前的步驟來指定其他首碼。
- 9 按一下視窗底部的**新增**。

建立社群清單

您可以建立 BGP 社群清單，以便根據社群清單來設定路由對應。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 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**社群清單**。
- 5 按一下**新增**。
- 6 輸入社群清單的名稱。
- 7 使用 aa:nn 格式指定社群 (例如 300:500)，然後按 Enter 鍵。重複以新增其他社群。
此外，您還可以按下拉式箭頭，選取下列一或多個項目：
 - NO_EXPORT_SUBCONFED - 不要向 EBGp 對等通告。
 - NO_ADVERTISE - 不要向任何對等通告。
 - NO_EXPORT - 不要向 BGP 聯盟外部通告
- 8 按一下**新增**。

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。

必要條件

確認已設定 IP 首碼清單。請參閱[建立 IP 首碼清單](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 選取第 0 層邏輯路由器。
- 4 選取**路由 > 路由對應**。
- 5 按一下**新增**。
- 6 輸入路由對應的名稱與選用說明。
- 7 按一下**新增**，在路由對應中新增項目。
- 8 編輯資料行與 **IP 首碼清單/社群清單**相符，以選取 IP 首碼清單或社群清單，但不能同時選取兩者。
- 9 (選擇性) 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。
加權	設定權重以影響路徑選擇。範圍為 0 - 65535。
社群	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： <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED - 不要向 EBGp 對等通告。 ■ NO_ADVERTISE - 不要向任何對等通告。 ■ NO_EXPORT - 不要向 BGP 聯盟外部通告

- 10 在 [動作] 資料行中，選取**允許或拒絕**。
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**。

設定轉送累計計時器

您可以設定第 0 層邏輯路由器的轉送累計計時器。

轉送累計計時器會定義在建立第一個 BGP 工作階段之後，路由器在傳送累計通知之前必須等待的時間 (以秒為單位)。若要對 NSX Edge 上使用動態路由 (BGP) 之邏輯路由器的雙主動或主動備用組態進行容錯移轉，則此計時器 (先前稱為轉送延遲) 會將停機時間減少至最短。計時器應該設為在第一個 BGP/BFD 工作階段之後，外部路由器 (TOR) 對此路由器通告所有路由所花費的秒數。計時器值應以路由器必須學習的北向動態路由數目進行直接比例調整。計時器在單一 Edge 節點設定時應設為 0。

程序

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

- 2 選取導覽面板中的**網路 > 路由**。
- 3 選取第 0 層邏輯路由器。
- 4 選取**路由 > 全域組態**
- 5 按一下**編輯**。
- 6 輸入轉送累計計時器的值。
- 7 按一下**儲存**。

網路位址轉譯

6

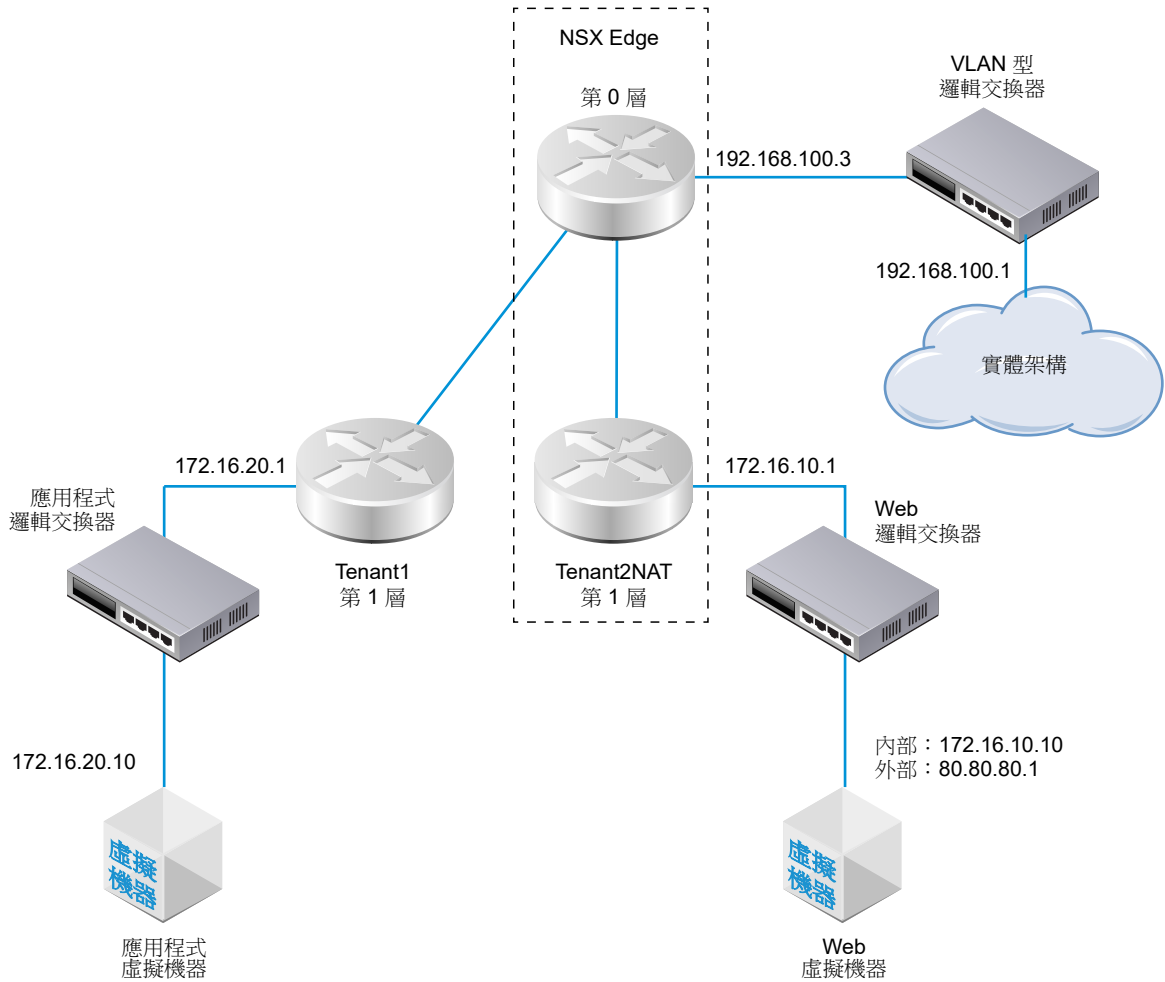
NSX-T Data Center 中的網路位址轉譯 (NAT) 可在第 0 層和第 1 層邏輯路由器中設定。

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



本章節討論下列主題：

- 第 1 層 NAT
- 第 0 層 NAT
- 自反 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。

您可以建立規則來啟用或停用來源 NAT。

在此範例中，封包是接收自 Web 虛擬機器，因此 Tenant2NAT 第 1 層路由器會將封包的來源 IP 位址從 172.16.10.10 變更為 80.80.80.1。擁有公用來源 IP 位址可讓私人網路外部的目的地路由回原始來源。

必要條件

- 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[針對 NSX Edge 上行，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 NSX 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[在第 1 層邏輯路由器上新增下行連接埠與在第 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下要在其上設定 NAT 的第 1 層邏輯路由器。
- 4 選取**服務 > NAT**。
- 5 按一下**新增**。
- 6 指定優先順序值。
值越低表示此規則的優先順序越高。
- 7 對於**動作**，請選取 **SNAT** 以啟用來源 NAT，或選取 **NO_SNAT** 以停用來源 NAT。
- 8 選取通訊協定類型。
依預設會選取**任何通訊協定**。
- 9 (選擇性) 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
如果您將此欄位保留空白，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 位址為 172.16.10.10。
- 10 (選擇性) 對於**目的地 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
如果您將此欄位保留空白，則 NAT 會套用至本機子網路外部的所有目的地。
- 11 如果**動作**為 **SNAT**，則對於**轉譯的 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
在此範例中，已轉譯的 IP 位址為 80.80.80.1。
- 12 (選擇性) 對於**套用至**，請選取路由器連接埠。
- 13 (選擇性) 設定規則的狀態。
此規則預設為啟用。

14 (選擇性) 變更記錄狀態。

依預設會停用記錄。

15 (選擇性) 變更防火牆略過設定。

此設定預設為啟用。

結果

新規則會在 NAT 下方列出。例如：

Tenant2NAT

概觀

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。

您可以建立規則來啟用或停用目的地 NAT。

在此範例中，封包是接收自應用程式虛擬機器，因此 Tenant2NAT 第 1 層路由器會將封包的目的地 IP 位址從 172.16.10.10 變更為 80.80.80.1。擁有公用目的地 IP 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。

必要條件

- 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[針對 NSX Edge 上行，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 NSX 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[在第 1 層邏輯路由器上新增下行連接埠與在第 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下要在其上設定 NAT 的第 1 層邏輯路由器。
- 4 選取**服務 > NAT**。
- 5 按一下**新增**。
- 6 指定優先順序值。
值越低表示此規則的優先順序越高。
- 7 對於**動作**，請選取 **DNAT** 以啟用目的地 NAT，或選取 **NO_DNAT** 以停用目的地 NAT。
- 8 選取通訊協定類型。
依預設會選取**任何通訊協定**。
- 9 (選擇性) 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
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 對於**目的地 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
在此範例中，目的地 IP 位址為 80.80.80.1。
- 11 如果**動作**為 **DNAT**，則對於**轉譯的 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
在此範例中，內部/已轉譯的 IP 位址是 172.16.10.10。
- 12 (選擇性) 如果**動作**為 **DNAT**，則對於**轉譯的連接埠**，請指定轉譯的連接埠。
- 13 (選擇性) 對於**套用至**，請選取路由器連接埠。
- 14 (選擇性) 設定規則的狀態。
此規則預設為啟用。
- 15 (選擇性) 變更記錄狀態。
依預設會停用記錄。
- 16 (選擇性) 變更防火牆略過設定。
此設定預設為啟用。

結果

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**網路 > 路由**。
- 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**。
- 5 編輯路由通告規則以啟用 NAT 路由通告。

結果

Tenant2NAT	
概觀 組態 路由 服務	
路由通告 編輯	
狀態	● 已啟用
通告所有 NSX 連線的路由	● 是
通告所有 NAT 路由	● 是
通告所有靜態路由	● 否
通告所有 LB VIP 路由	● 否
通告所有 LB SNAT IP 路由	● 否
通告的網路	5 網路

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 從瀏覽器以管理員權限登入 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。

結果

編輯重新分配準則 - rule1 ? ×

名稱 *	rule1	
說明	Rule	
來源 *	<input type="checkbox"/> 靜態 <input checked="" type="checkbox"/> 第 1 層 NAT <input checked="" type="checkbox"/> NSX 已連線 <input type="checkbox"/> 第 1 層 LB VIP <input checked="" type="checkbox"/> NSX 靜態 <input type="checkbox"/> 第 1 層 LB SNAT <input type="checkbox"/> 第 0 層 NAT	
路由對應	<div> × ▼ </div>	

取消

儲存

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 `get 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 層邏輯路由器支援來源 NAT、目的地 NAT 和自反 NAT。

在第 0 層路由器上設定來源和目的地 NAT

您可以在主動-待命模式下執行的第 0 層路由器上設定來源和目的地 NAT。

您也可以設定 No NAT、NO_SNAT 或 NO_DNAT，以針對一個 IP 位址或一系列位址停用 NAT。如果有多個 NAT 規則可套用到一個位址，則會套用具有最高優先順序的規則。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的 **網路 > 路由**。
- 3 按一下第 0 層邏輯路由器。
- 4 選取 **服務 > NAT**。
- 5 按一下 **新增** 以新增 NAT 規則。

6 指定優先順序值。

較低的值表示較高的優先順序。

7 對於**動作**，請選取 **SNAT**、**DNAT**、**無 NAT**、**NO_SNAT** 或 **NO_DNAT**。**8** 選取通訊協定類型。

依預設會選取**任何通訊協定**。

9 (必要) 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。

如果您將此欄位保留空白，此 **NAT** 規則會套用至本機子網路外部的所有來源。

10 對於**目的地 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。**11** 對於**轉譯的 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。**12** (選擇性) 如果**動作**為 **DNAT**，則對於**轉譯的連接埠**，請指定轉譯的連接埠。**13** (選擇性) 對於**套用至**，請選取路由器連接埠。**14** (選擇性) 設定規則的狀態。

此規則預設為啟用。

15 (選擇性) 變更記錄狀態。

依預設會停用記錄。

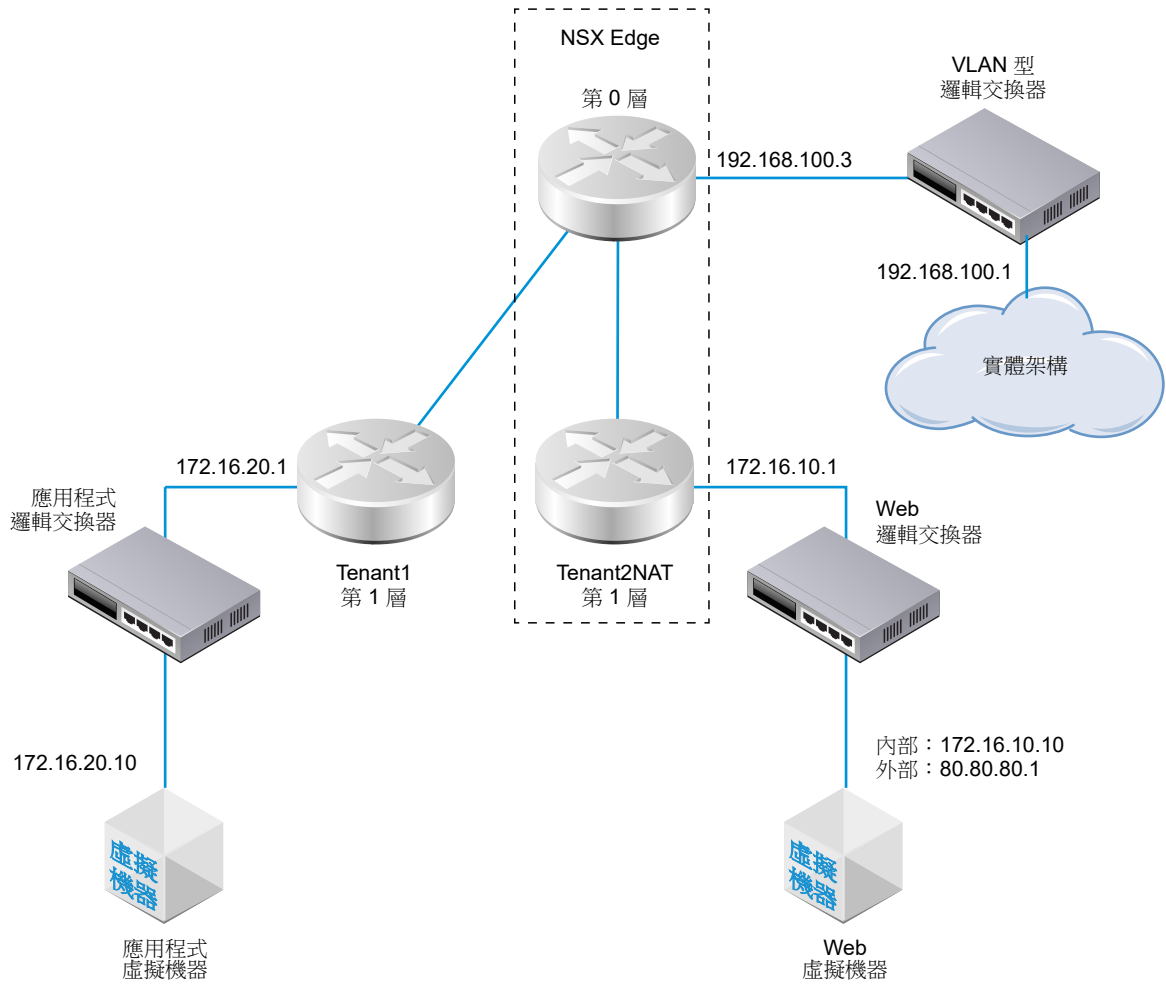
16 (選擇性) 變更防火牆略過設定。

此設定預設為啟用。

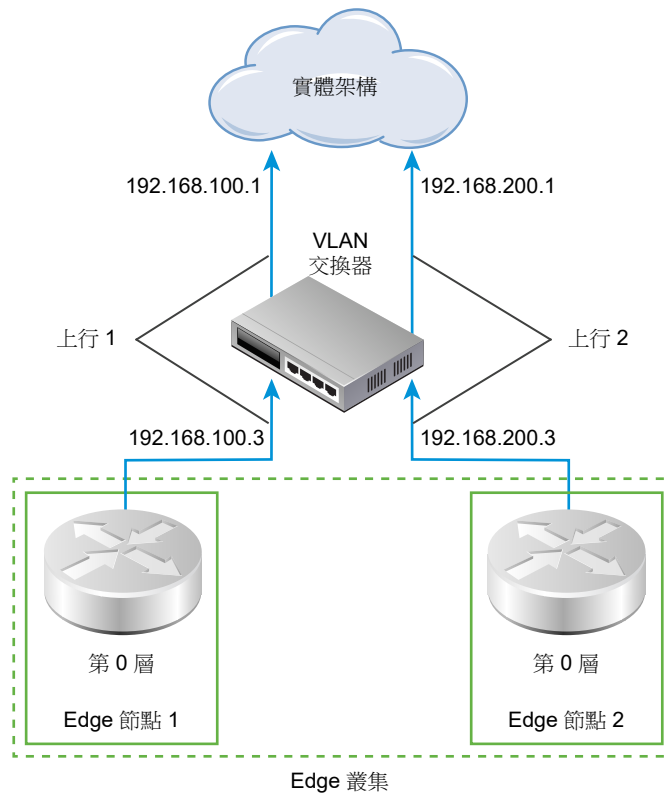
自反 NAT

當第 0 層或第 1 層邏輯路由器在雙主動模式下執行時，您無法設定可設定狀態的 **NAT**，因為非對稱路徑可能會發生問題。對於雙主動路由器，您可以使用自反 **NAT** (有時稱為**乏態 NAT**)。

在此範例中，封包是接收自 **Web** 虛擬機器，因此 **Tenant2NAT** 第 1 層路由器會將封包的來源 IP 位址從 172.16.10.10 變更為 80.80.80.1。擁有公用來源 IP 位址可讓私人網路外部的目的地路由回原始來源。



涉及兩個雙主動第 0 層路由器時 (如此處所示)，必須設定自反 NAT。



在第 0 層或第 1 層邏輯路由器上設定自反 NAT

當第 0 層或第 1 層邏輯路由器在雙主動模式下執行時，您無法設定可設定狀態的 NAT，因為非對稱路徑可能會發生問題。對於雙主動路由器，您可以使用自反 NAT (有時稱為乏態 NAT)。

對於自反 NAT，您可以設定要轉譯的單一來源位址，或設定位址範圍。如果設定來源位址範圍，您必須同時設定轉譯的位址範圍。兩個範圍的大小必須相同。位址轉譯將具有決定性，這表示來源位址範圍中的第一個位址將轉譯為已轉譯位址範圍中的第一個位址，來源範圍中的第二個位址將轉譯為已轉譯範圍中的第二個位址，依此類推。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下您要設定自反 NAT 的第 0 層或第 1 層邏輯路由器。
- 4 選取**服務 > NAT**。
- 5 按一下**新增**。
- 6 指定優先順序值。
值越低表示此規則的優先順序越高。
- 7 對於**動作**，請選取自反。
- 8 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。

9 對於轉譯的 IP，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。

10 (選擇性) 設定規則的狀態。

此規則預設為啟用。

11 (選擇性) 變更記錄狀態。

依預設會停用記錄。

12 (選擇性) 變更防火牆略過設定。

此設定預設為啟用。

結果

新規則會在 NAT 下方列出。例如：

Tier0-LR-1

概觀 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: 2019年3月6日 18:11:02

☒ 作用中工作階段

☐ 封包計數

☐ 位元組 資料

+ 新增

編輯

刪除

識別碼	動作	相符					已轉譯		套用到	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										
2048	自反	任何	80.80.80.1	任何	任何	任何	172.16.10.10	任何		

防火牆區段和防火牆規則

7

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。

備註 邏輯交換器具有稱為 **N-VDS** 模式的內容。此內容來自交換器所屬的傳輸區域。如果 **N-VDS** 模式為 **ENS** (也稱為 **Enhanced Datapath**)，則您無法在 **Source**、**Destination** 或 **Applied To** 欄位中，透過交換器或其連接埠建立防火牆規則或區段。

本章節討論下列主題：

- [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](#)
- [啟用和停用區段記錄](#)
- [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 **Distributed Firewall** 規則](#)
- [變更防火牆規則的順序](#)
- [篩選防火牆規則](#)

- 為邏輯交換器橋接器連接埠設定防火牆
- 設定防火牆排除清單
- 啟用和停用防火牆
- 新增或刪除邏輯路由器的防火牆規則

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**安全性 > Distributed Firewall**。
- 2 對於第 3 層 (L3) 規則，按一下**一般**索引標籤，對於第 2 層 (L2) 規則，按一下**乙太網路**索引標籤。
- 3 按一下現有的區段或規則。
- 4 按一下功能表列上的區段圖示，然後選取**新增以上區段**或**新增以下區段**。

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。

- 5 輸入區段名稱。
- 6 若要使防火牆無狀態，請選取**啟用無狀態防火牆**。此選項僅適用於 L3。

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。

- 7 選取要套用區段的一或多個物件。

物件的類型為邏輯連接埠、邏輯交換器和 NSGroup。如果您選取 NSGroup，它必須包含一或多個邏輯交換器或邏輯連接埠。僅包含 IP 集或 MAC 集的 NSGroup 將被忽略。

備註 區段中的**套用至**將覆寫該區段中任何規則中的**套用至**設定。

- 8 按一下**確定**。

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 按一下區段第一個資料行中的功能表圖示，然後選取**刪除區段**。

您也可以選取區段，然後按一下功能表列上的刪除圖示。

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 按一下區段第一個資料行中的功能表圖示，然後選取**啟用所有規則**或**停用所有規則**。
- 4 按一下**發佈**。

啟用和停用區段記錄

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 按一下區段第一個資料行中的功能表圖示，然後選取**啟用記錄**或**停用記錄**。
- 4 按一下**發佈**。

關於防火牆規則

NSX-T Data Center 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。您可以設定排除清單，其中包含邏輯交換器、邏輯連接埠或要從防火牆強制執行排除的群組。

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)。

備註 對於 TCP 通訊協定，會針對可設定狀態規則自動啟用 TCP 嚴格檢查。這表示，封包只在網路連線以 SYN 封包開始時才符合 TCP 規則。

表 7-1. 防火牆規則的內容

內容	說明
名稱	防火牆規則名稱。
識別碼	每個規則的唯一系統產生識別碼。
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。
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。
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。
動作	規則套用的動作可為允許、捨棄或拒絕。預設為允許。
IP 通訊協定	選項為 IPv4、IPv6 及 IPv4_IPv6。預設為 IPv4_IPv6。若要存取此內容，請按一下進階設定圖示。
方向	選項為傳入、傳出及傳入/傳出。預設為傳入/傳出。此欄位是指從目的地物件的角度而言的流量方向。傳入表示僅會檢查流向物件的流量，傳出表示僅會檢查來自物件的流量，而傳入/傳出則表示會檢查這兩個方向的流量。若要存取此內容，請按一下進階設定圖示。
規則標記	已新增至規則的標記。若要存取此內容，請按一下進階設定圖示。
流量統計資料	顯示位元組、封包計數和工作階段的唯讀欄位。若要存取此內容，請按一下圖表圖示。

備註 若未啟用 SpoofGuard，即無法保證自動探索的位址繫結是可靠的，因為惡意虛擬機器可以宣告另一個虛擬機器的位址。若啟用 SpoofGuard，請確認每個探索的繫結，以便僅顯示已核准的繫結。

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。

必要條件

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 按一下現有的區段或規則。
- 4 在規則的第一個資料行中按一下功能表圖示，然後選取**新增以上規則**或**新增以下規則**。
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。

- 5 在**名稱**資料行中，輸入規則名稱。
- 6 在**來源**資料行中，按一下編輯圖示並選取規則來源。若未定義，則來源會符合任何項目。

選項	說明
IP 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。
容器物件	可用的物件為 IP 集合、邏輯連接埠、邏輯交換器及 NS 群組。選取物件，然後按一下 確定 。

- 7 在**目的地**資料行中，按一下編輯圖示並選取目的地。若未定義，則目的地會符合任何項目。

選項	說明
IP 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。
容器物件	可用的物件為 IP 集合、邏輯連接埠、邏輯交換器及 NS 群組。選取物件，然後按一下 確定 。

- 8 在**服務**資料行中，按一下編輯圖示並選取服務。若未定義，則服務會符合任何項目。
- 9 若要選取預先定義的服務，請選取一或多項可用服務。

- 10 若要定義新服務，請按一下**原始連接埠通訊協定**索引標籤，然後按一下**新增**。

選項	說明
服務類型	<ul style="list-style-type: none"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ L4 連接埠集合
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。

- 11 在**套用**至資料行中，按一下**編輯圖示**並選取物件。

- 12 在**記錄**資料行中，設定記錄選項。

記錄位於 ESXi 和 KVM 主機上的 `/var/log/dfwpktlogs.log` 檔案中。啟用記錄可能會影響效能。

- 13 在**動作**資料行中，選取動作。

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。

- 14 按一下**進階設定**圖示，以指定 IP 通訊協定、方向、規則標記及註解。

- 15 按一下**發佈**。

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路**索引標籤。
- 3 按一下區段第一個資料行中的功能表圖示，然後選取**刪除規則**。
- 4 按一下**發佈**。

編輯預設 Distributed Firewall 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。

預設防火牆規則會套用至不符合任何使用者定義防火牆規則的流量。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資料表底部，且無法刪除。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。

預設第 3 層防火牆規則會套用至所有流量，包括 DHCP。如果您將**動作**變更為**捨棄**或**拒絕**，將會封鎖 DHCP 流量。您必須建立規則以允許 DHCP 流量。

程序

- 1 選取導覽面板中的**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 在**名稱**資料行中，輸入新名稱。
- 4 在**動作**資料行中，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**作為預設規則的動作。

- 5 在**記錄**中，啟用或停用記錄。
啟用記錄可能會影響效能。
- 6 按一下**發佈**。

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**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 選取規則，然後按一下功能表列上的**上移**或**下移**圖示。
- 4 按一下**發佈**。

篩選防火牆規則

當您導覽至防火牆區段時，最初會顯示所有規則。您可以套用篩選器以控制所要顯示的項目，以便僅檢視一部分的規則。如此，管理規則將會更加輕鬆。

程序

- 1 選取導覽面板中的**安全性 > Distributed Firewall**。
- 2 按一下 L3 規則的**一般**索引標籤，或是 L2 規則的**乙太網路** 索引標籤。
- 3 在功能表列右側的搜尋文字欄位中，選取物件或輸入物件名稱的前幾個字元，以縮小要選取的物件清單範圍。

在您選取物件後，即會套用篩選器並更新規則清單，且僅會顯示包含下列任何資料行中之物件的規則：

- 來源
- 目的地
- 套用至
- 服務

- 4 若要移除篩選器，請從文字欄位中刪除物件名稱。

為邏輯交換器橋接器連接埠設定防火牆

對於第 2 層支援橋接器之邏輯交換器的橋接器連接埠，您可以為其設定防火牆區段和防火牆規則。必須使用 NSX Edge 節點建立橋接器。

必要條件

確認交換器已連結至橋接器設定檔。請參閱[建立第 2 層橋接器備份邏輯交換器](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**安全性 > 橋接防火牆**。
- 3 選取邏輯交換器。
交換器必須已連結至橋接器設定檔。
- 4 若要設定第 2 層或第 3 層防火牆，請遵循先前章節中的相同步驟。

設定防火牆排除清單

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 Data Center 應用裝置連接埠。

程序

- 1 選取導覽面板中的**安全性 > Distributed Firewall**。
- 2 按一下**排除清單**索引標籤。
- 3 按一下**新增**。
- 4 選取類型和物件。
可用的類型為**邏輯連接埠**、**邏輯交換器**和 **NSGroup**。
- 5 按一下**確定**。
- 6 若要從排除清單中移除物件，請選取物件並按一下功能表列上的**刪除**。

啟用和停用防火牆

您可以啟用或停用 Distributed Firewall 功能。如果已停用防火牆，則不會強制執行任何規則。

程序

- 1 選取導覽面板中的**安全性 > Distributed Firewall**。
- 2 按一下**設定**索引標籤。
- 3 按一下**編輯**。
- 4 在對話方塊中，將防火牆狀態設定為綠色 (已啟用) 或灰色 (已停用)。
- 5 按一下**儲存**。

新增或刪除邏輯路由器的防火牆規則

您可以新增第 0 層或第 1 層邏輯路由器的防火牆規則，以控制對路由器的通訊。

必要條件

自行熟悉防火牆規則的參數。請參閱[新增防火牆規則](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 3 按一下**路由器**索引標籤 (若尚未選取)。
- 4 按一下邏輯路由器的名稱。

- 5 選取**服務 > Edge 防火牆**。
- 6 按一下現有的區段或規則。
- 7 若要新增規則，請按一下功能表列上的**新增規則**，然後選取**新增以上規則**或**新增以下規則**，或按一下規則第一個資料行中的功能表圖示，然後選取**新增以上規則**或**新增以下規則**，並指定規則參數。
[套用至] 欄位不會顯示，因為此規則僅會套用至邏輯路由器。
- 8 若要刪除規則，請選取規則，按一下功能表列上的**刪除**，或按一下第一個資料行中的功能表圖示，然後選取**刪除**。

結果

備註 如果您將防火牆規則新增至第 0 層邏輯路由器，並且支援路由器的 NSX Edge 叢集在主動-主動式模式下執行，則防火牆只能在無狀態模式下執行。如果您使用 HTTP、SSL、TCP 等可設定狀態的服務設定防火牆規則，防火牆規則將無法按預期運作。為避免此問題，請將 NSX Edge 叢集設定為在主動-待命模式下執行。

虛擬私人網路

8

NSX-T Data Center 支援 NSX Edge 上的 IPSec VPN 和第 2 層 VPN (L2VPN)。

備註 NSX-T Data Center 限制出口版本不支援 IPSec VPN 和 L2VPN。

IPSec VPN

IPSec VPN 透過稱為端點的 IPSec 閘道，來保護透過公用網路連線的兩個網路間流量的安全。NSX Edge 僅支援搭配使用 IP 通道與封裝安全性裝載 (ESP) 的通道模式。

IPSec VPN 使用 IKE 通訊協定來交渉安全性參數。預設 UDP 連接埠設為 500。如果在閘道中偵測到 NAT，則會將連接埠設為 4500。

備註 僅第 0 層邏輯路由器支援 IPSec VPN。

NSX Edge 支援兩種類型的 VPN：原則型 VPN 和路由型 VPN。

原則型 VPN 需要對轉送至 IPSec 服務的封包套用原則。此類型的 VPN 被視為靜態的，因為當本機網路拓撲和組態變更時，原則設定也必須一併更新以適應變更。

路由型 VPN 根據透過特殊介面 (稱為虛擬通道介面 (VTI)，例如使用 BGP 做為通訊協定) 動態學習的路由來提供流量的通道。IPSec 保護流經虛擬通道介面 (VTI) 的所有流量。

L2VPN

L2VPN 連線允許將第 2 層網路從內部部署資料中心延伸至雲端，如 VMware Cloud on Amazon (VMC)。此連線使用路由型 IPSec 通道保護。

延伸網路是具有單一廣播網域的單一子網路，因此您可以在內部部署資料中心與公有雲之間移轉虛擬機器，而無需變更其 IP 位址。

使用 L2VPN 延伸的內部部署網路，除了支援資料中心移轉以外，還對災難復原以及動態參與外部部署計算資源以滿足需求的增加 (稱為「雲端爆裂」) 非常有用。

每個 L2VPN 工作階段都有一個 GRE 通道。不支援通道備援。一個 L2VPN 工作階段延最多可以延伸 4094 個第 2 層網路。

備註 NSX-T Data Center 與 NSX Edge (不論是否在 NSX Data Center for vSphere 中受到管理) 之間可支援 L2VPN。

本章節討論下列主題：

- [設定 IPsec VPN](#)
- [設定 L2VPN](#)

設定 IPsec VPN

您可以僅使用 API 來建立路由型 VPN 和原則型 VPN 工作階段。

備註 NSX-T Data Center 限制出口版本不支援 IPsec VPN。

您無法將 NAT 和 IPsec VPN 一起用於同一網路設定檔。請確保將 NAT 和 IPsec VPN 置於不同的網路設定檔。

必要條件

自行熟悉 IPsec VPN。請參閱 [IPsec VPN](#)。

程序

- 1 在第 0 層邏輯路由器上設定 IPsec VPN 服務。

使用 POST /api/v1/vpn/ipsec/services 呼叫。

```
POST /api/v1/vpn/ipsec/services
{
  "display_name": "IPsec VPN service",
  "logical_router_id": "f81f220f-3072-4a6e-9f53-ad3b8bb8af57"
}
```

- 2 設定無作用對等偵測 (Dead Peer Detection, DPD) 設定檔。

使用 POST /api/v1/vpn/ipsec/dpd-profiles 呼叫。

預設設定檔以 60 秒 DPD 探查時間間隔佈建。

```
POST /api/v1/vpn/ipsec/dpd-profiles
{
  "enabled": "true",
  "dpd_probe_interval": 60,
  "description": "DPD profile",
  "display_name": "DPD profile"
}
```

- 3 設定 IKE 設定檔參數。

使用 POST /api/v1/vpn/ipsec/ike-profiles 呼叫。

```
POST /api/v1/vpn/ipsec/ike-profiles
{
  "digest_algorithms": ["SHA2_256"],
  "description": "IKEProfile for site1",
  "display_name": "IKEProfile site1",
}
```



```
"encryption_algorithms": ["AES_128"],
"ike_version": "IKE_V2",
"dh_groups": ["GROUP14"],
"sa_life_time": 21600
}
```

4 設定 IPsec VPN 的通道設定檔。

使用 POST /api/v1/vpn/ipsec/tunnel-profiles 呼叫。

```
POST /api/v1/vpn/ipsec/tunnel-profiles/
{
  "digest_algorithms": ["SHA1","SHA2_256"],
  "description": "Tunnel Profile for site 1",
  "display_name": "Tunnel Profile for site 1",
  "encapsulation_mode": "TUNNEL_MODE",
  "encryption_algorithms": ["AES_128","AES_256"],
  "enable_perfect_forward_secrecy": true,
  "dh_groups": ["GROUP14"],
  "transform_protocol": "ESP",
  "sa_life_time": 3600,
  "df_policy": "CLEAR"
}
```

5 設定要與 IPsec VPN 對等進行通訊的對等端點。

使用 POST /api/v1/vpn/ipsec/peer-endpoints 呼叫。

```
POST /api/v1/vpn/ipsec/peer-endpoints
{
  "display_name": "Peer endpoint for site 1",
  "connection_initiation_mode": "INITIATOR",
  "authentication_mode": "PSK",
  "ipsec_tunnel_profile_id": "640607f3-bb83-4e54-a153-57939965881c",
  "dpd_profile_id": "4808d04e-572d-480d-8182-61ddaa146461",
  "psk": "6721b9f1f5936956c0a8b4ed95286b452db04dae721eddf0f264f0fcc6e94882b",
  "ike_profile_id": "a4db6863-b6f0-45bd-967e-a2e22c260329",
  "peer_address": "10.14.24.4",
  "peer_id": "10.14.24.4"
}
```

6 設定 VPN 端點的本機端點。

使用 POST /api/v1/vpn/ipsec/local-endpoints 呼叫。

```
POST /api/v1/vpn/ipsec/local-endpoints
{
  "local_address": "1.1.1.12",
  "local_id": "1.1.1.12",
  "display_name": "Local endpoint",
  "ipsec_vpn_service_id": {
    "target_id" : "81388ec0-b5e3-4a9e-b551-e372e700772c"
  }
}
```

7 設定路由型 VPN 工作階段。

使用 POST /api/v1/vpn/ipsec/sessions 呼叫。

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "RouteBasedIPSecVPNSession",
  "display_name": "RouteSession1",
  "ipsec_vpn_service_id": "657bcb55-48ce-4e0f-bfc7-a5a91b2990ae",
  "peer_endpoint_id": "cfc70ab5-16d1-4292-9391-fcee23ccea96",
  "local_endpoint_id": "9d4b44f1-0bfa-4705-ac67-09244a17d42e",
  "enabled": true,
  "tunnel_ports": [
    {
      "ip_subnets": [
        {
          "ip_addresses" : [
            "192.168.50.1"
          ],
          "prefix_length" : 24
        }
      ]
    }
  ]
}
```

8 設定原則型 VPN 工作階段。

使用 POST /api/v1/vpn/ipsec/sessions 呼叫。

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "display_name": "PolicySession1",
  "ipsec_vpn_service_id": "ea071856-9e91-4826-a841-9ec7ee9ea534",
  "peer_endpoint_id": "0c2447d2-8890-4b55-bf02-8c6b1a94d1ce",
  "local_endpoint_id": "161acb63-c3f2-438d-9e5c-cb655e6a1099",
  "enabled": true,
  "policy_rules": [
    {
      "sources": [
        {
          "subnet": "2.2.2.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "3.3.3.0/24"
        }
      ],
      "action": "PROTECT",
    }
  ]
}
```

```

    "enabled": true
  }
]
}

```

設定 L2VPN

您可以僅使用 API 來建立 L2VPN 服務和工作階段。

備註 NSX-T Data Center 限制出口版本不支援 L2VPN。

必要條件

- 自行熟悉 L2VPN。請參閱 [L2VPN](#)。
- 確認第 0 層邏輯路由器已設定上行設定檔。請參閱《[NSX-T Data Center 安裝指南](#)》。
- 確認已設定邏輯交換器。請參閱[建立邏輯交換器](#)。
- 確認未受管理的 NSX Edge 可以在 NSX Data Center for vSphere 中使用。
- 確認已設定 IPsec VPN。設定 [IPsec VPN](#)

程序

1 設定 L2VPN 服務。

使用 POST /api/v1/vpn/l2vpn/services 呼叫。

```

POST /api/v1/vpn/l2vpn/services
{
  "logical_router_id": "b6fe5455-619b-4030-b5f8-8575749f4404",
  "logical_tap_ip_pool": [ "169.254.64.0/28" ],
  "enable_full_mesh": true
}

```

2 設定 L2VPN 工作階段。

使用 POST /api/v1/vpn/l2vpn/sessions 呼叫。

```

POST /api/v1/vpn/l2vpn/sessions
{
  "l2vpn_service_id" : "421de3a2-c6ec-4c42-a891-5bde3b5feb68",
  "transport_tunnels" : [
    {
      "target_id" : "801e5140-6da8-4e78-ab44-f966de75f311"
    }
  ]
}

```

3 設定具有連結的邏輯連接埠。

使用 `POST /api/v1/vpn/logical-ports` 呼叫。

```
POST /api/v1/logical-ports/
{
  "resource_type": "LogicalPort",
  "display_name": "Extend logicalSwitch, port for service",
  "logical_switch_id": "f52abcee-27a7-426c-a128-037db2283582",
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "L2VPN_SESSION",
    "id": "6806c4ea-3b77-4b8a-8af2-ccc47b1ba8a9",
    "context": {
      "resource_type": "L2VpnAttachmentContext",
      "tunnel_id": 10
    }
  }
}
```

4 下載 L2VPN 對等程式碼組態。

`GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/peer-codes`

5 登入內部部署 NSX Data Center for vSphere 未受管理的 NSX Edge CLI。

6 貼上 L2VPN 對等程式碼組態。

7 (選擇性) 監控 L2VPN 工作階段。

- L2VPN 工作階段摘要 `GET /api/v1/vpn/l2vpn/sessions/summary`。
- L2VPN 工作階段統計資料 `GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/statistics`。

管理物件、群組、服務和虛擬機器

9

您可以建立 IP 集合、IP 集區、MAC 集合、NSGroup 和 NSService。您也可以管理虛擬機器的標記。

本章節討論下列主題：

- 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
- 管理虛擬機器的標記

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 群組**。
- 3 在主面板頂端選取 **IP 集合**。
- 4 按一下**新增**。
- 5 輸入名稱。
- 6 (選擇性) 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 群組**。
- 3 在主面板頂部選取 **IP 集區**。
- 4 按一下**新增**。
- 5 輸入名稱。
- 6 (選擇性) 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 (選擇性) 輸入閘道。
- 10 輸入包含尾碼的 CIDR IP 位址。
- 11 (選擇性) 輸入 DNS 伺服器。
- 12 (選擇性) 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 群組**。
- 3 選取主面板頂部的 **MAC 集合**。
- 4 按一下**新增**。
- 5 輸入名稱。
- 6 (選擇性) 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。

NSX Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

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。
- 您最多可以指定五個套用至邏輯交換器、邏輯連接埠或虛擬機器的成員資格準則。針對套用至邏輯交換器或邏輯連接埠的準則，您可以指定標記，並選擇性地指定範圍。針對套用至虛擬機器的準則，您可以將名稱指定為以特定字串開頭、等於或包含特定字串。
- 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。
- 支援的虛擬機器數目上限為 10,000。

對於所有可新增至 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、虛擬機器和 NSGroup)，您可以導覽至任何物件的畫面，並選取**相關 > NSGroup**，以檢視直接或間接以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 > NSGroup** 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 群組**。
- 3 按一下**群組**索引標籤 (若尚未選取)。

- 4 按一下**新增**。
- 5 輸入 NSGroup 的名稱。
- 6 (選擇性) 輸入說明。
- 7 (選擇性) 按一下**成員資格準則**。

準則可套用至邏輯交換器、邏輯連接埠或虛擬機器。對於每個準則，您最多可以指定五個規則，與邏輯 AND 運算子組合使用。針對套用至邏輯交換器或邏輯連接埠的規則，您可以指定標記，並選擇性地指定範圍。針對套用至虛擬機器的規則，您可以將名稱指定為以特定字串開頭、等於或包含特定字串。

您最多可以指定五個準則，與邏輯 OR 運算子組合使用。

- 8 (選擇性) 按一下**成員**以選取成員。

可用的類型為 **IP 集合**、**MAC 集合**、**邏輯交換器**、**邏輯連接埠**和 **NSGroup**。

- 9 按一下**儲存**。

設定服務和服務群組

您可以設定 **NSService** 並指定用來比對網路流量的參數，例如連接埠和通訊協定的配對。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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 服務**。
- 3 按一下**新增**。
- 4 輸入名稱。
- 5 (選擇性) 輸入說明。
- 6 選取**指定通訊協定**來設定個別服務，或選取**群組現有服務**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**、**IP**、**IGMP**、**ICMP**、**ALG** 和 **L4 連接埠集合**。
- 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**和**第 3 層及以上**。
- 9 按一下**儲存**。

管理虛擬機器的標記

您可以在詳細目錄中查看虛擬機器清單。您也可以將標記新增至虛擬機器，以使搜尋更為輕鬆。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 虛擬機器**。
虛擬機器的清單會顯示 4 個資料行：**[虛擬機器]**、**[外部識別碼]**、**[來源]** 和 **[標記]**。您可以在前三個資料行標題中按一下篩選器圖示以篩選清單。輸入一串字元執行部分比對。如果資料行中的字串包含您輸入的字串，則會顯示項目。輸入用雙引號括住的一串字元執行完全比對。如果資料行中的字串與您輸入的字串完全相符，則會顯示項目。
- 3 選取虛擬機器。
- 4 按一下**管理標記**。
- 5 新增或刪除標籤。

選項	動作
新增標籤	按一下 新增 以指定標記，並選擇性地指定範圍。
刪除標籤	選取現有的標記，然後按一下 刪除 。

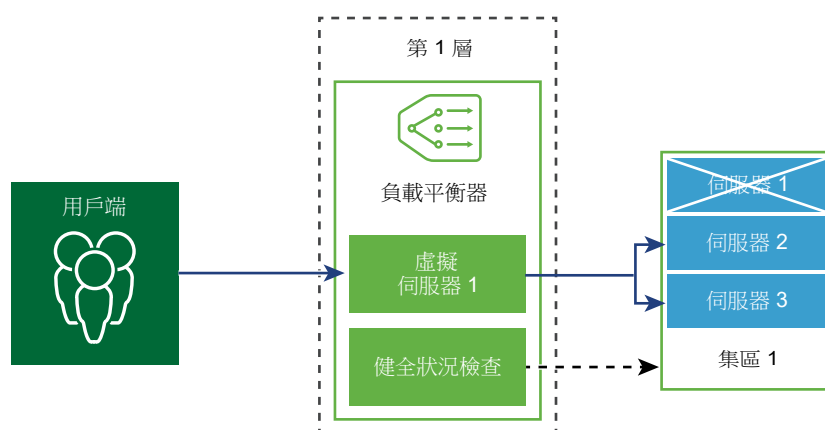
一個虛擬機器最多可以有 15 個標記。

- 6 按一下**儲存**。

邏輯負載平衡器

10

NSX-T Data Center 邏輯負載平衡器可針對應用程式提供高可用性服務，並將網路流量負載散佈在多個伺服器之間。



負載平衡器會在多個伺服器之間均勻地散佈傳入服務要求，以便負載分佈對於使用者是透明的。負載平衡有助於實現最佳資源使用率、最大化輸送量、儘量縮短回應時間，以及避免超載。

您可以將一個虛擬 IP 位址對應至一組集區伺服器，以進行負載平衡。負載平衡器接受虛擬 IP 位址上的 TCP、UDP、HTTP 或 HTTPS 要求，並決定要使用哪個集區伺服器。

根據您的環境需求，您可以增加現有的虛擬伺服器和集區成員來調整負載平衡器效能，以處理高網路流量負載。

備註 僅第 1 層邏輯路由器支援邏輯負載平衡器。一個負載平衡器只能連結至第 1 層邏輯路由器。

本章節討論下列主題：

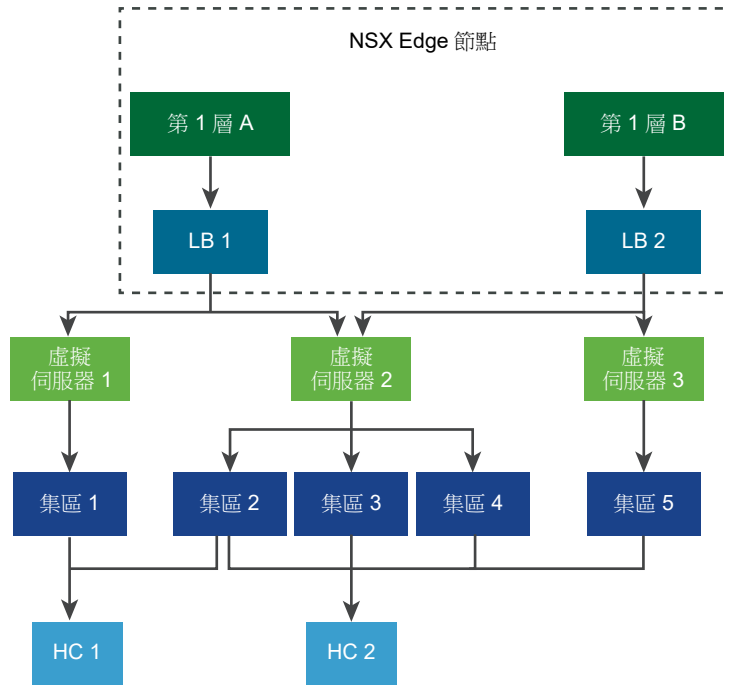
- [主要負載平衡器概念](#)
- [設定負載平衡器元件](#)

主要負載平衡器概念

負載平衡器包括虛擬伺服器、伺服器集區，以及健全狀況檢查監視器。

負載平衡器已連線至第 1 層邏輯路由器。負載平衡器裝載單一或多個虛擬伺服器。虛擬伺服器是應用程式服務的抽象概念，由唯一的 IP、連接埠和通訊協定組合表示。虛擬伺服器將關聯到單一或多個伺服器集區。伺服器集區由一組伺服器組成。伺服器集區包含個別伺服器集區成員。

若要測試每個伺服器是否正確執行應用程式，您可以新增用於檢查伺服器健全狀況狀態的健全狀況檢查監視器。



調整負載平衡器資源

負載平衡器大小包括小型、中型和大型。根據負載平衡器大小，負載平衡器可以裝載不同的虛擬伺服器和集區成員。

負載平衡器已連結至一個第 1 層邏輯路由器。此第 1 層邏輯路由器被裝載於 NSX Edge 節點。NSX Edge 具有機器尺寸為裸機、小型、中型和大型的虛擬機器應用裝置。根據機器尺寸，NSX Edge 節點可以裝載不同數量的負載平衡器。

表 10-1. 負載平衡器服務的負載平衡器縮放

負載平衡器服務	小型負載平衡器	中型負載平衡器	大型負載平衡器
每個負載平衡器的虛擬伺服器數目	10	100	1000
每個負載平衡器的集區數目	20	200	2000
每個負載平衡器的集區成員數目	200	2000	10,000

表 10-2. NSX Edge 節點的負載平衡器縮放

每個 NSX Edge 節點的負載平衡器	小型負載平衡器	中型負載平衡器	大型負載平衡器	集區成員數目上限
NSX Edge 虛擬機器 - 小型	不適用	不適用	不適用	不適用
NSX Edge 虛擬機器 - 中型	1	不適用	不適用	200
NSX Edge 虛擬機器 - 大型	40	4	不適用	5000
NSX Edge 虛擬機器 - 裸機	750	75	7	20,000

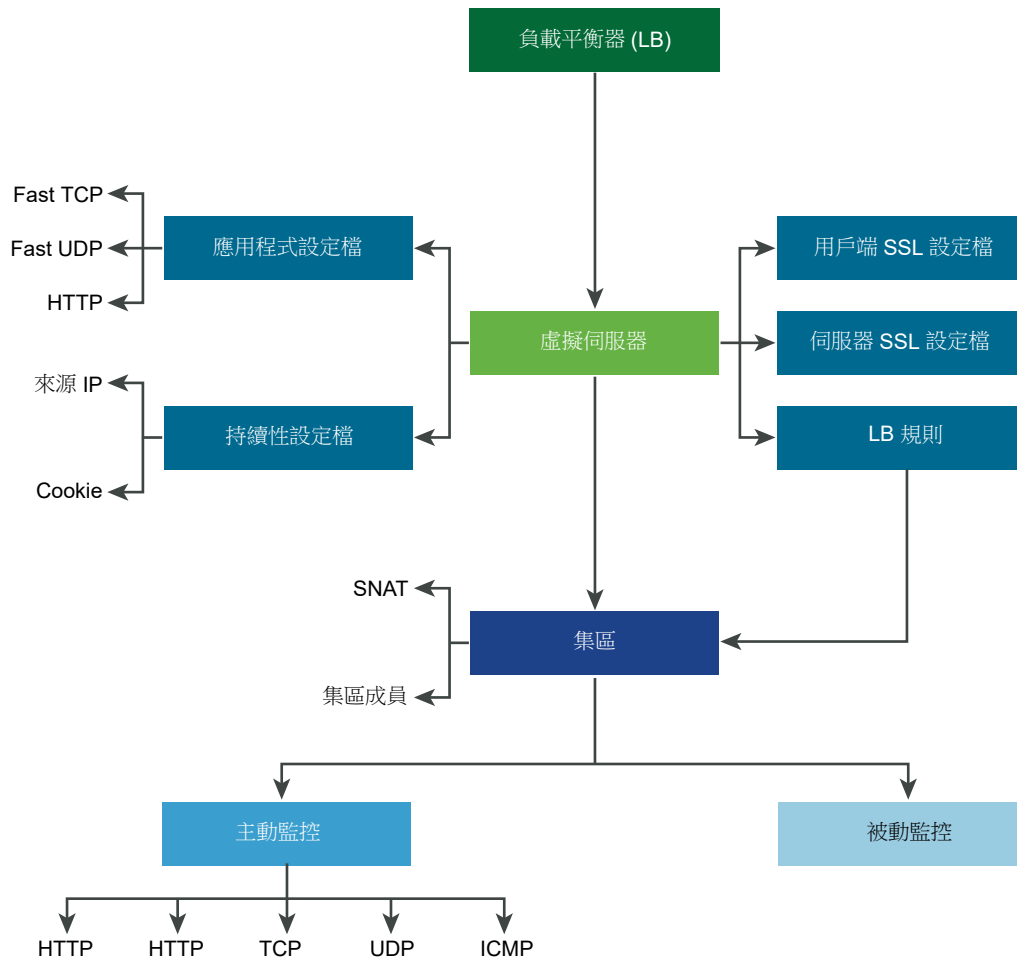
支援的負載平衡器功能

NSX-T Data Center 負載平衡器支援下列功能。

- 第 4 層 - TCP 和 UDP
- 第 7 層 - HTTP 和 HTTPS 及負載平衡器規則支援
- 伺服器集區 - 靜態和動態及 NSGroup
- 持續性 - 來源 IP 和 Cookie 持續性模式
- 健全狀況檢查監視器 - 包括 HTTP、HTTPS、TCP、UDP 和 ICMP 在內的主動監視器和被動監視器
- SNAT - 透明、自動對應以及 IP 清單
- HTTP 升級 - 對於使用 HTTP 升級 (如 WebSocket) 的應用程式，支援針對 HTTP 升級的用戶端或伺服器要求。依預設，NSX-T Data Center 支援並接受使用 HTTP 應用程式設定檔的 HTTPS 升級用戶端要求。

為了偵測非作用中用戶端或伺服器通訊，負載平衡器會使用 HTTP 應用程式設定檔回應逾時功能 (設定為 60 秒)。如果伺服器在 60 秒時間間隔內未傳送流量，NSX-T Data Center 便會結束用戶端和伺服器端的連線。

附註：NSX-T Data Center 2.2 Limited Export 版本不支援 SSL 終止模式和 Proxy 模式。

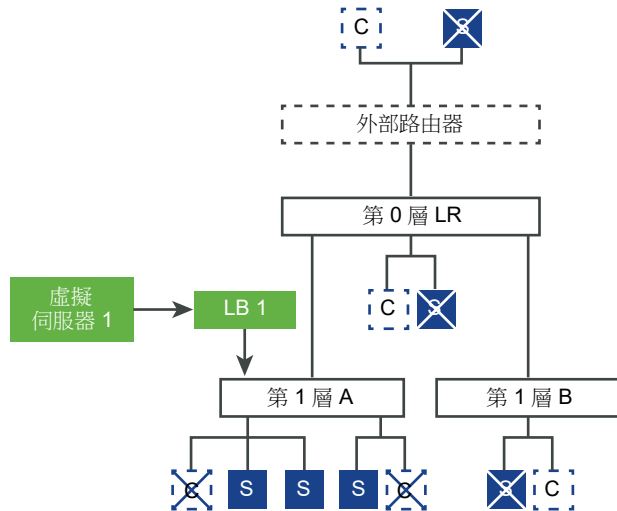


負載平衡器拓撲

負載平衡器通常在內嵌或單一裝載模式下進行部署。

內嵌拓撲

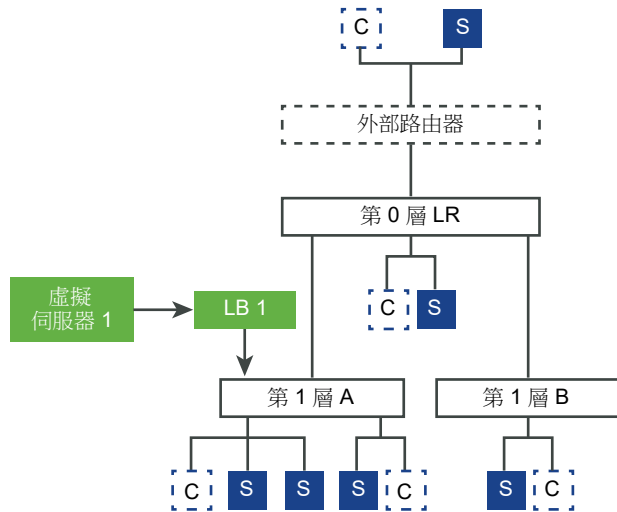
在內嵌模式下，負載平衡器位於用戶端與伺服器之間的流量路徑中。用戶端和伺服器不得連線到相同的第 1 層邏輯路由器。此拓撲不需要虛擬伺服器 SNAT。



單一裝載拓撲

在單一裝載模式下，負載平衡器不在用戶端與伺服器之間的流量路徑中。在此模式下，用戶端和伺服器可位於任意位置。負載平衡器執行來源 NAT (SNAT) 以強制從伺服器到用戶端的傳回流量經過負載平衡器。此拓撲需要啟用虛擬伺服器 SNAT。

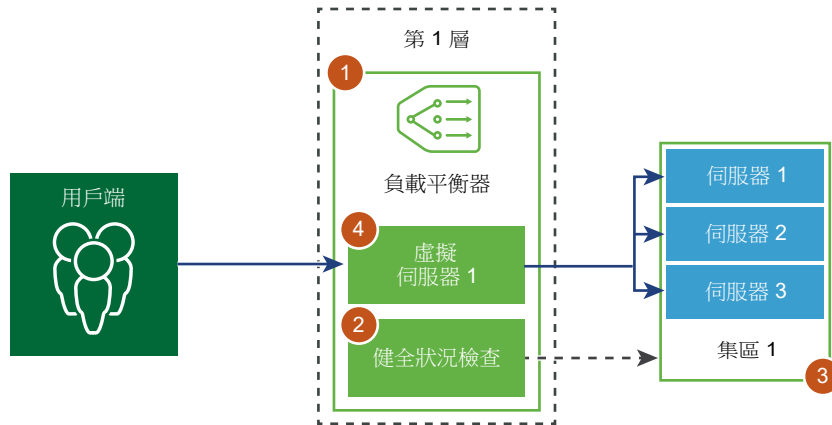
當負載平衡器接收到虛擬 IP 位址的用戶端流量時，負載平衡器會選取伺服器集區成員，並向其轉送用戶端流量。在單一裝載模式下，負載平衡器會以負載平衡器 IP 位址取代用戶端 IP 位址，以便伺服器回應始終傳送到負載平衡器，然後負載平衡器將該回應轉送至用戶端。



設定負載平衡器元件

若要使用邏輯負載平衡器，您必須透過設定負載平衡器並連結至第 1 層邏輯路由器進行啟動。

接下來，您可以設定伺服器的健全狀況檢查監控。然後，您必須為負載平衡器設定伺服器集區。最後，您必須為負載平衡器建立第 4 層或第 7 層虛擬伺服器。

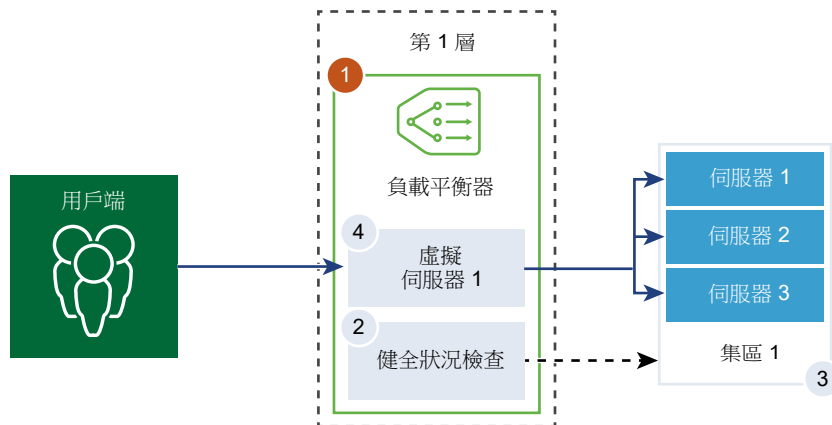


建立負載平衡器

負載平衡器將會建立並連結至第 1 層邏輯路由器。

您可以設定希望負載平衡器新增至錯誤記錄的錯誤訊息層級。

備註 由於列印到記錄的訊息數目影響效能，請避免將具有大量流量的負載平衡器上的記錄層級設定為 [偵錯]。



必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取**網路 > 負載平衡器 > 新增**。
- 3 輸入負載平衡器的名稱和說明。
- 4 根據可用的資源，選取負載平衡器虛擬伺服器的大小和集區成員數目。
- 5 從下拉式功能表中定義錯誤記錄的嚴重性層級。

負載平衡器會將發生的不同嚴重性層級問題的相關資訊收集到錯誤記錄。

- 6 按一下**確定**。
- 7 將新建立的負載平衡器關聯至虛擬伺服器。
 - a 選取負載平衡器，然後按一下**動作 > 連結至虛擬伺服器**。
 - b 從下拉式功能表中選取現有的虛擬伺服器。
 - c 按一下**確定**。
- 8 將新建立的負載平衡器連結至第 1 層邏輯路由器。
 - a 選取負載平衡器，然後按一下**動作 > 連結至邏輯路由器**。
 - b 從下拉式功能表中選取現有的第 1 層邏輯路由器。
第 1 層路由器必須處於主動備用模式。
 - c 按一下**確定**。
- 9 (選擇性) 刪除負載平衡器。

如果您不再需要使用此負載平衡器，必須先從虛擬伺服器和第 1 層邏輯路由器中斷連結負載平衡器。

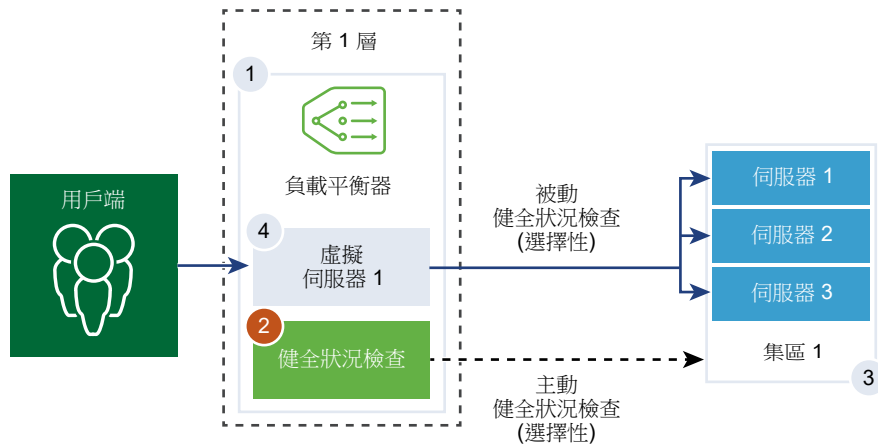
設定主動健全狀況監視器

主動健全狀況監視器可用來測試伺服器是否可用。主動健全狀況監視器使用數種類型的測試，例如傳送基本 ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

無法在特定期間內回應或回應含有錯誤的伺服器已排除在未來連線處理之外，直到後續定期健全狀況檢查發現這些伺服器狀況良好為止。

當集區成員連結到虛擬伺服器，並且該虛擬伺服器連結至第 1 層邏輯路由器之後，會在伺服器集區成員上執行主動健全狀況檢查。第 1 層上行 IP 位址可用於健全狀況檢查。

備註 每個伺服器集區可設定一個主動健全狀況監視器。



程序

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

- 2 選取**負載平衡器 > 網路 > 監視器 > 主動健全狀況監視器 > 新增**。
- 3 輸入主動健全狀況監視器的名稱和說明。
- 4 從下拉式功能表中選取伺服器的健全狀況檢查通訊協定。

您也可以使用 NSX Manager 中預先定義的通訊協定；http-monitor、https-monitor、icmp-monitor、Tcp-monitor 和 Udp-monitor。

- 5 設定監控連接埠的值。
- 6 設定用於監控服務集區的值。

也可以接受預設的主動健全狀況監視器值。

選項	說明
監控時間間隔	設定監視器向伺服器傳送另一個連線要求的時間 (以秒為單位)。
失敗計數	設定當連續失敗次數達到此值時，伺服器被視為暫時無法使用的值。
正常計數	設定在此逾時期間後，伺服器再次嘗試新連線以查看其是否可用的數目。
逾時期間	設定伺服器被視為 [關閉] 之前所經過的測試次數。

例如，如果監控時間間隔設為 5 秒且逾時設為 15 秒，則負載平衡器會每隔 5 秒向伺服器傳送要求。在每次探查時，如果在 15 秒內收到來自伺服器的預期回應，則健全狀況檢查結果為 [正常]。如果沒有收到，則結果為 [嚴重]。如果最近三次健全狀況檢查結果皆為 [啟動]，則伺服器視為 [啟動]。

- 7 如果您選取 HTTP 做為健全狀況檢查通訊協定，請完成下列詳細資料。

選項	說明
HTTP 方法	從下拉式功能表中選取偵測伺服器狀態的方法 (GET、OPTIONS、POST、HEAD 和 PUT)。
HTTP 要求 URL	針對方法輸入要求 URI。
HTTP 要求版本	從下拉式功能表中選取支援的要求版本。 也可以接受預設版本 HTTP_VERSION_1_1。
HTTP 要求本文	輸入要求本文。 適用於 POST 和 PUT 方法。
HTTP 回應代碼	輸入監視器預期與 HTTP 回應本文狀態列相符的字串。 回應代碼是以逗點分隔的清單。 例如，200,301,302,401。
HTTP 回應本文	如果 HTTP 回應本文字串和 HTTP 健全狀況檢查回應本文相符，則伺服器會視為狀況良好。

- 8 如果您選取 HTTPS 做為健全狀況檢查通訊協定，請完成下列詳細資料。

- a 選取 SSL 通訊協定清單。

TLS 版本 TLS1.1 和 TLS1.2 版本均受支援且預設為啟用。TLS1.0 受支援，但預設為停用。

- b 按一下箭頭，將通訊協定移至 [已選取] 區段。

- c 指派預設 SSL 加密方式，或建立自訂的 SSL 加密方式。
- d 如果您選取 HTTP 做為健全狀況檢查通訊協定，請完成下列詳細資料。

選項	說明
HTTP 方法	從下拉式功能表中選取偵測伺服器狀態的方法 (GET、OPTIONS、POST、HEAD 和 PUT)。
HTTP 要求 URL	針對方法輸入要求 URI。
HTTP 要求版本	從下拉式功能表中選取支援的要求版本。 也可以接受預設版本 HTTP_VERSION_1_1。
HTTP 要求本文	輸入要求本文。 適用於 POST 和 PUT 方法。
HTTP 回應代碼	輸入監視器預期與 HTTP 回應本文狀態列相符的字串。 回應代碼是以逗點分隔的清單。 例如，200,301,302,401。
HTTP 回應本文	如果 HTTP 回應本文字串和 HTTP 健全狀況檢查回應本文相符，則伺服器會視為狀況良好。

- 9 如果您選取 ICMP 做為健全狀況檢查通訊協定，請指派 ICMP 健全狀況檢查封包的資料大小 (以位元組為單位)。

- 10 如果您選取 TCP 做為健全狀況檢查通訊協定，可將參數保留空白。

如果未列出傳送及預期值，則會建立三向信號交換的 TCP 連線以驗證伺服器健全狀況。未傳送任何資料。如果列出預期資料，則必須為字串，並且可以是回應中的任何位置。不支援規則運算式。

- 11 如果您選取 UDP 做為健全狀況檢查通訊協定，請完成下列所需的詳細資料。

必要選項	說明
傳送的 UDP 資料	輸入在建立連線後傳送至伺服器的字串。
預期的 UDP 資料	輸入預期從伺服器接收的字串。 僅當接收的字串符合此定義時，才會將伺服器視為 [啟動]。

- 12 按一下完成。

後續步驟

將主動健全狀況監視器與伺服器集區相關聯。請參閱[新增用於負載平衡的伺服器集區](#)。

設定被動健全狀況監視器

負載平衡器會執行被動健全狀況檢查，以在用戶端連線期間監控故障並將造成一致性故障的伺服器標記為 [關閉]。

被動健全狀況檢查可監控經過負載平衡器的用戶端流量是否發生故障。例如，如果集區成員傳送 TCP 重設 (RST) 以回應用戶端連線，則負載平衡器會偵測到該故障。如果出現多個連續故障，負載平衡器會將該伺服器集區成員視為暫時無法使用，並在一段時間內停止傳送連線要求至該集區成員。在一段時間後，負載平衡器會傳送連線要求以檢查該集區成員是否已復原。如果連線成功，則會將該集區成員視為狀況良好。否則，負載平衡器會稍待片刻，然後再次嘗試。

被動健全狀況檢查將下列情況視為用戶端流量發生故障。

- 針對與第 7 層虛擬伺服器相關聯的伺服器集區，無法連線到集區成員。例如，如果集區成員在負載平衡器嘗試連線或在負載平衡器與集區成員之間執行 SSL 信號交換失敗時傳送 TCP RST。
- 針對與第 4 層 TCP 虛擬伺服器相關聯的伺服器集區，集區成員傳送 TCP RST 來回應用戶端 TCP SYN 或完全不回應。
- 針對與第 4 層 UDP 虛擬伺服器相關聯的伺服器集區，無法連線到連接埠或針對用戶端 UDP 封包的回應為目的地無法連線到 ICMP 錯誤訊息。

針對與第 7 層虛擬伺服器相關聯的伺服器集區，發生任何 TCP 連線錯誤 (例如 TCP RST 無法傳送資料或 SSL 信號交換失敗) 時，失敗的連線計數會增加。

針對與第 4 層虛擬伺服器相關聯的伺服器集區，如果傳送至伺服器集區成員的 TCP SYN 未收到任何回應或針對 TCP SYN 的回應為 TCP RST，則伺服器集區成員會被視為 [關閉]。失敗計數會增加。

針對第 4 層 UDP 虛擬伺服器，如果針對用戶端流量的回應為 ICMP 錯誤訊息 (例如無法連線到連接埠或目的地)，則伺服器會被視為 [關閉]。

備註 每個伺服器集區可設定一個被動健全狀況監視器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取 **網路 > 負載平衡器 > 監視器 > 被動健全狀況監視器 > 新增**。
- 3 輸入被動健全狀況監視器的名稱和說明。
- 4 設定用於監控服務集區的值。

也可以接受預設的主動健全狀況監視器值。

選項	說明
失敗計數	設定當連續失敗次數達到此值時，伺服器被視為暫時無法使用的值。
逾時期間	設定伺服器被視為 [關閉] 之前所經過的測試次數。

例如，當連續失敗次數達到設定值 5 時，該成員會被視為在 5 秒內暫時無法使用。在此期間後，該成員會再次嘗試新連線以查看其是否可用。如果該連線成功，則該成員會被視為可用，失敗計數將設為零。但是，如果該連線失敗，則在下一個 5 秒的逾時時間間隔內無法使用。

- 5 按一下 **確定**。

後續步驟

將被動健全狀況監視器與伺服器集區相關聯。請參閱 [新增用於負載平衡的伺服器集區](#)。

新增用於負載平衡的伺服器集區

伺服器集區由一或多個已設定且執行相同應用程式的伺服器組成。單一集區可同時關聯至第 4 層和第 7 層虛擬伺服器。

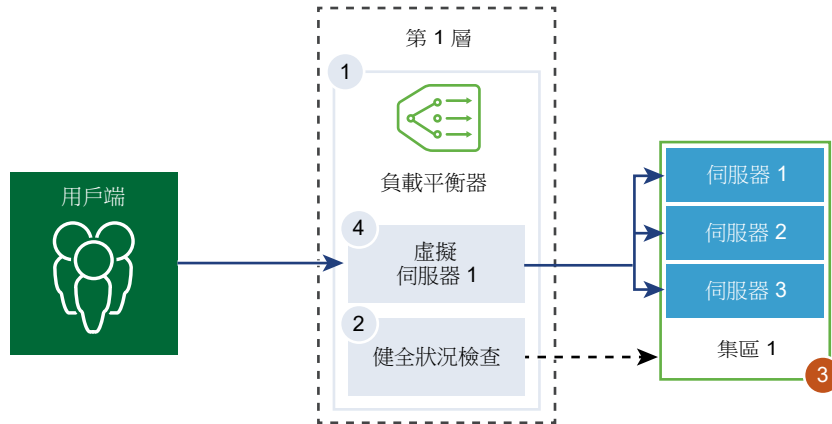
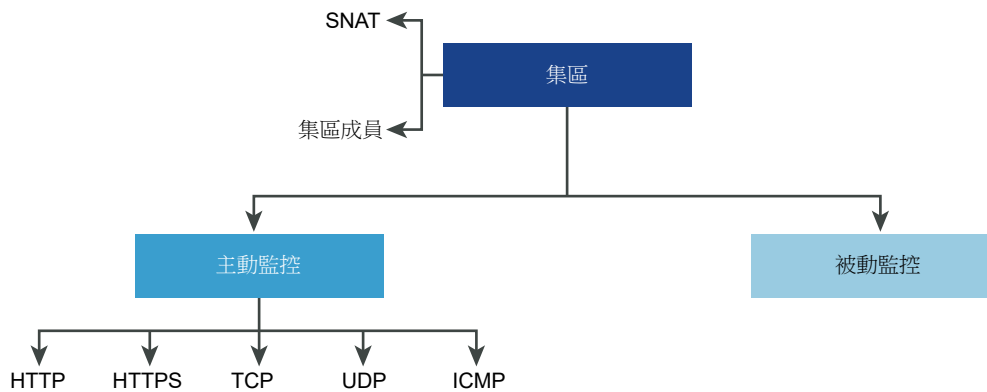


圖 10-1. 伺服器集區參數組態



必要條件

- 如果您使用動態集區成員，則必須設定 NSGroup。請參閱[建立 NSGroup](#)。
- 根據您使用的監控，請確認主動或被動健全狀況監視器已設定。請參閱[設定主動健全狀況監視器](#)或[設定被動健全狀況監視器](#)。

程序

- 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 選取 **網路 > 負載平衡器 > 伺服器集區 > 新增**。
- 輸入負載平衡器集區的名稱和說明。
您可以選擇性地說明伺服器集區所管理的連線。
- 選取伺服器集區的演算法平衡方法。

負載平衡演算法可控制在成員之間散佈傳入連線的方式。可直接在伺服器集區或伺服器上使用演算法。

所有負載平衡演算法均會略過符合下列任意條件的伺服器：

- 管理員狀態設為 [已停用]
- 管理員狀態設為 **GRACEFUL_DISABLED** 且沒有相符的持續性項目
- 主動或被動健全狀況檢查狀態為 [關閉]
- 已達到最大伺服器集區並行連線的連線限制。

選項	說明
ROUND_ROBIN	傳入用戶端要求會在能夠處理該要求的可用伺服器清單中循環。 忽略伺服器集區成員權數 (即使已設定)。
WEIGHTED_ROUND_ROBIN	每個伺服器都指派有表示該伺服器如何相對於集區中的其他伺服器執行的權數值。 該值會決定與集區中的其他伺服器相比，向某個伺服器傳送的用戶端要求數目。 此負載平衡演算法的重點在於，將負載公平地散佈到可用的伺服器資源之間。
LEAST_CONNECTION	根據伺服器上已有的連線數目，將用戶端要求散佈到多個伺服器。 新連線會傳送到具有最少連線數的伺服器。忽略伺服器集區成員權數 (即使已設定)。
WEIGHTED_LEAST_CONNECTION	每個伺服器都指派有表示該伺服器如何相對於集區中的其他伺服器執行的權數值。 該值會決定與集區中的其他伺服器相比，向某個伺服器傳送的用戶端要求數目。 此負載平衡演算法著重於使用權重值公平地將負載散佈至可用伺服器資源。 如果未設定權重值，依預設，此值為 1 ，並會啟用緩慢啟動。
IP-HASH	根據來源 IP 位址雜湊和所有執行中伺服器的權數總計來選取伺服器。

5 切換 [TCP 多工處理] 按鈕以啟用此功能表項目。

TCP 多工處理可讓您在負載平衡器與伺服器之間使用相同的 **TCP** 連線，以從不同的用戶端 **TCP** 連線傳送多個用戶端要求。

6 設定每個集區保持運作的 **TCP** 多工處理連線數目上限，以傳送未來的用戶端要求。

7 選取來源 NAT (SNAT) 模式。

視拓撲而定，可能需要 SNAT，以便負載平衡器從以用戶端為目標的伺服器接收流量。可針對伺服器集區啟用 SNAT。

模式	說明
透明模式	負載平衡器在建立與伺服器的連線時，會使用用戶端 IP 位址和連接埠變更。 不需要 SNAT。
自動對應模式	負載平衡器會使用介面 IP 位址和暫時連接埠，繼續與最初連線至伺服器建立之其中一個接聽連接埠的用戶端進行通訊。 需要 SNAT。 如果元組 (來源 IP、來源連接埠、目的地 IP、目的地連接埠，以及 IP 通訊協定) 在執行 SNAT 程序後是唯一的，則啟用連接埠超載以允許相同的 SNAT IP 和連接埠用於多個連線。 也可以設定連接埠超載係數以允許連接埠可同時用於多個連線的最大次數。
IP 清單模式	指定在連線至集區中的任何伺服器時，將用於 SNAT 的單一 IP 位址範圍，例如，1.1.1.1-1.1.1.10。 依預設，4000 - 64000 連接埠範圍適用於所有設定的 SNAT IP 位址。連接埠範圍 1000 - 4000 將保留用於從 Linux 應用程式起始的健全狀況檢查及連線等。如果存在多個 IP 位址，則會以循環配置資源的方式進行選取。 如果元組 (來源 IP、來源連接埠、目的地 IP、目的地連接埠，以及 IP 通訊協定) 在執行 SNAT 程序後是唯一的，則啟用連接埠超載以允許相同的 SNAT IP 和連接埠用於多個連線。 也可以設定連接埠超載係數以允許連接埠可同時用於多個連線的最大次數。

8 選取伺服器集區成員。

伺服器集區由單一或多個集區成員所組成。每個集區成員具有一個 IP 位址和一個連接埠。

每個伺服器集區成員可設定權數，以在負載平衡演算法中使用。權數指示與相同集區中的其他成員相比，指定的集區成員可以處理多少負載數目。

指定集區成員做為備份成員適用於健全狀況監視器，以提供作用中/待命狀態。如果作用中成員的健全狀況檢查失敗，備份成員會發生流量容錯移轉。

選項	說明
靜態	按一下 新增 以包含靜態集區成員。 您也可以複製現有的靜態集區成員。
動態	從下拉式功能表中選取 NSGroup。 伺服器集區成員資格準則將在群組中定義。您可以選擇性地定義最大群組 IP 位址清單。

9 輸入伺服器集區必須始終擁有的作用中成員的數目下限。

10 從下拉式功能表中選取伺服器集區的主動和被動健全狀況監視器。

11 按一下**完成**。

設定虛擬伺服器元件

針對虛擬伺服器可設定數個元件，例如應用程式設定檔、持續性設定檔和負載平衡器規則。

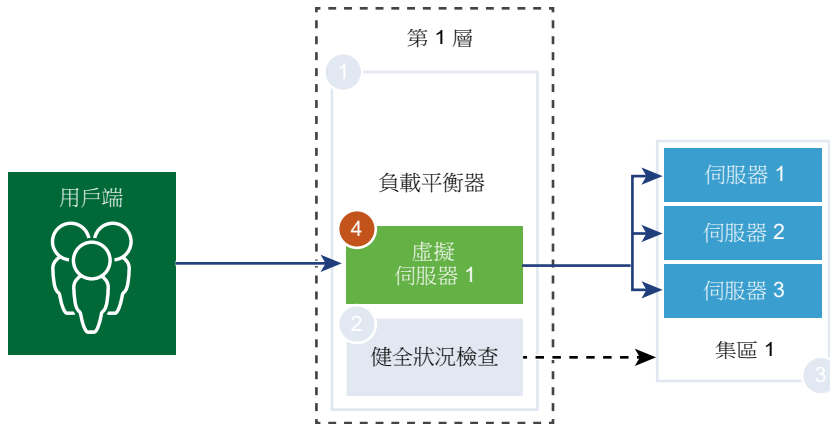
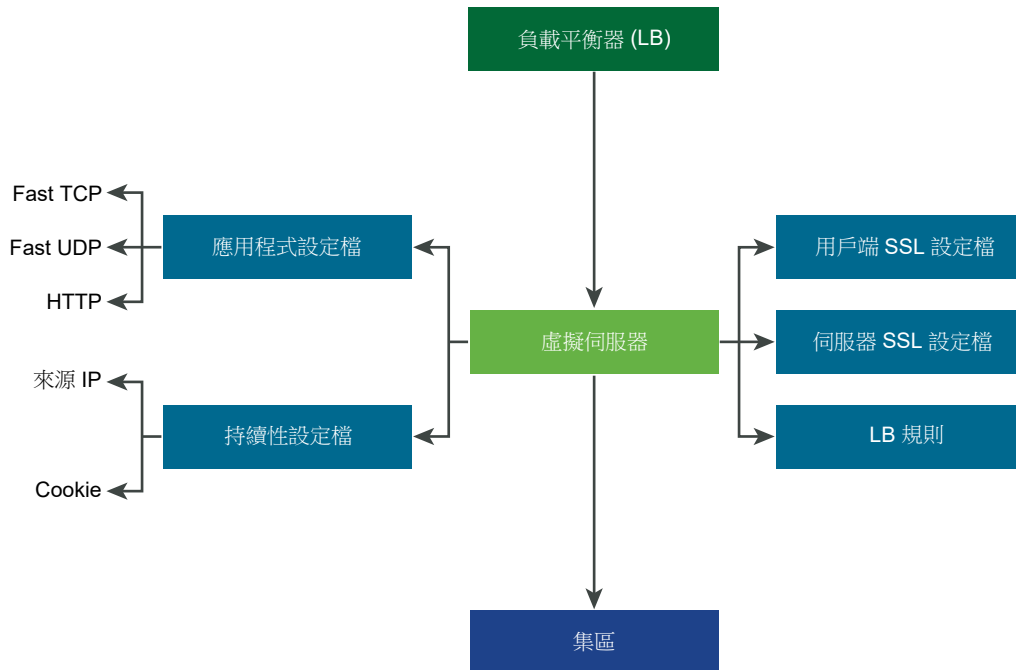


圖 10-2. 虛擬伺服器元件



設定應用程式設定檔

應用程式設定檔與虛擬伺服器相關聯，以提高負載平衡網路流量，並簡化流量管理工作。

應用程式設定檔可定義特定網路流量類型的行為。相關聯的虛擬伺服器會根據應用程式設定檔中所指定的值來處理網路流量。快速 TCP、快速 UDP 和 HTTP 應用程式設定檔是支援的設定檔類型。

沒有應用程式設定檔關聯至虛擬伺服器時，預設會使用 TCP 應用程式設定檔。當應用程式依據 TCP 或 UDP 通訊協定執行並且不需要任何應用程式層級負載平衡 (例如 HTTP URL 負載平衡) 時，將使用 TCP 和 UDP 應用程式設定檔。只想要第 4 層負載平衡 (其效能更快且支援連線鏡像) 時，也會使用這些設定檔。

當負載平衡器需要以第 7 層為基礎採取動作時 (例如將所有映像要求負載平衡至特定的伺服器集區成員或終止 HTTPS 以從集區成員卸載 SSL)，HTTP 應用程式設定檔可同時用於 HTTP 和 HTTPS 應用程式。與 TCP 應用程式設定檔不同，HTTP 應用程式設定檔會先終止用戶端 TCP 連線，然後再選取伺服器集區成員。

圖 10-3. 第 4 層 TCP 和 UDP 應用程式設定檔

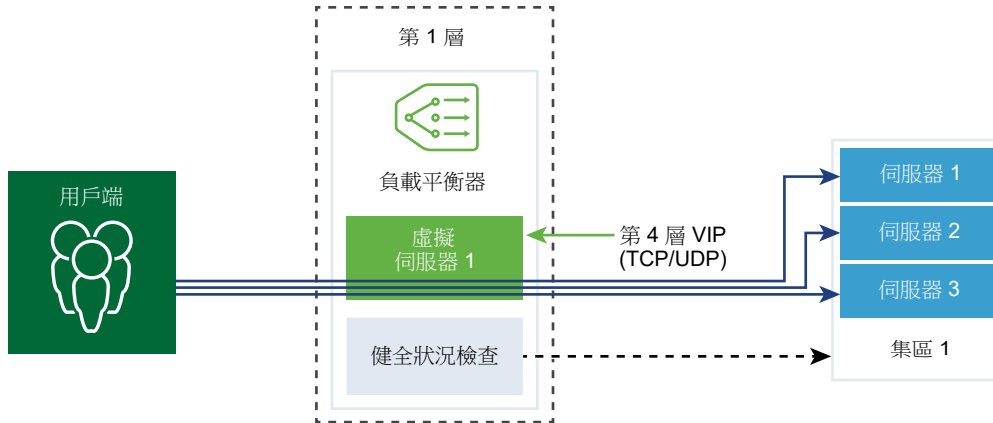
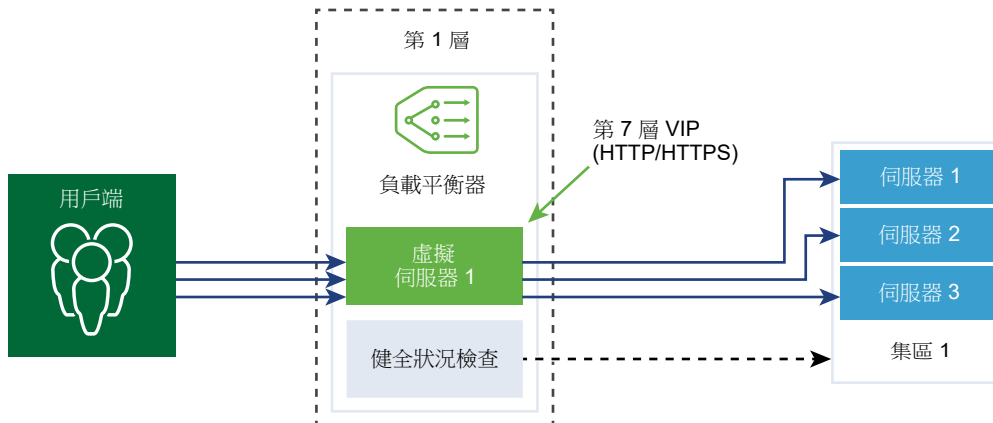


圖 10-4. 第 7 層 HTTPS 應用程式設定檔



程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取網路 > 負載平衡器 > 設定檔 > 應用程式設定檔。
- 3 建立快速 TCP 應用程式設定檔。
 - a 從下拉式功能表中選取新增 > 快速 TCP 設定檔。
 - b 輸入快速 TCP 應用程式設定檔的名稱和說明。

- c 完成應用程式設定檔詳細資料。

也可以接受預設的快速 TCP 設定檔設定。

選項	說明
連線閒置逾時	輸入在 TCP 連線建立之後，伺服器可維持閒置的時間 (以秒為單位)。 將閒置時間設定為實際應用程式閒置時間並增加幾秒的時間，以便負載平衡器不會在應用程式關閉其連線之前關閉。
連線關閉逾時	輸入在關閉連線之前應用程式必須保留 TCP 連線 (FIN 或 RST) 的時間 (以秒為單位)。 可能需要較短的關閉逾時以支援快速連線速率。
HA 流量鏡像	切換按鈕，使所有流量流向鏡像到 HA 待命節點的相關聯的虛擬伺服器。

- d 按一下**確定**。

4 建立快速 UDP 應用程式設定檔。

也可以接受預設的 UDP 設定檔設定。

- 從下拉式功能表中選取**新增 > 快速 UDP 設定檔**。
- 輸入快速 UDP 應用程式設定檔的名稱和說明。
- 完成應用程式設定檔詳細資料。

選項	說明
閒置逾時	輸入在 UDP 連線建立之後，伺服器可維持閒置的時間 (以秒為單位)。 UDP 是無連線的通訊協定。為了負載平衡目的，具有相同流量簽章的所有 UDP 封包，例如來源和目的地 IP 位址或連接埠以及在閒置逾時期間內接收的 IP 通訊協定，都將視為屬於相同的連線並傳送至相同的伺服器。 如果在閒置逾時期間內未收到封包，則關聯流程簽章與所選伺服器的連線將會關閉。
HA 流量鏡像	切換按鈕，使所有流量流向鏡像到 HA 待命節點的相關聯的虛擬伺服器。

- d 按一下**確定**。

5 建立 HTTP 應用程式設定檔。

也可以接受預設的 HTTP 設定檔設定。

HTTP 應用程式設定檔可同時用於 HTTP 和 HTTPS 應用程式。

- 從下拉式功能表中選取**新增 > 快速 HTTP 設定檔**。
- 輸入 HTTP 應用程式設定檔的名稱和說明。

c 完成應用程式設定檔詳細資料。

選項	說明
重新導向	<ul style="list-style-type: none"> ■ 無 - 如果網站暫時關閉，使用者會收到 [找不到頁面] 錯誤訊息。 ■ HTTP 重新導向 - 如果網站暫時關閉或已移動，該虛擬伺服器的傳入要求會暫時重新導向到此處指定的 URL。僅支援靜態重新導向。 例如，如果 HTTP 重新導向設為 <code>http://sitedown.abc.com/sorry.html</code>，則不論實際要求為何，例如 <code>http://original_app.site.com/home.html</code> 或 <code>http://original_app.site.com/somepage.html</code>，傳入要求都將在原始網站關閉時重新導向到指定的 URL。 ■ HTTP 至 HTTPS 重新導向 - 某些安全應用程式可能想要透過 SSL 強制執行通訊，但可以重新導向用戶端要求以使用 SSL，而不是拒絕非 SSL 連線。透過 HTTP 至 HTTPS 重新導向，您可以保留主機和 URI 路徑，並重新導向用戶端要求以使用 SSL。 針對 HTTP 至 HTTPS 重新導向，HTTPS 虛擬伺服器必須具有連接埠 443，並且必須在相同的負載平衡器上設定相同的虛擬伺服器 IP 位址。 例如，<code>http://app.com/path/page.html</code> 的用戶端要求重新導向至 <code>https://app.com/path/page.html</code>。如果主機名稱或 URI 必須在重新導向時進行修改，例如，重新導向至 <code>https://secure.app.com/path/page.html</code>，則必須使用負載平衡規則。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ 插入 - 如果傳入要求中不存在 XFF HTTP 標頭，則負載平衡器會插入具有用戶端 IP 位址的新 XFF 標頭。 ■ 取代 - 如果傳入要求中已存在 XFF HTTP 標頭，則負載平衡器可取代標頭。Web 伺服器會記錄透過要求的用戶端 IP 位址所處理的每個要求。這些記錄可用於偵錯和分析目的。如果部署拓撲需要負載平衡器上的 SNAT，伺服器會使用讓記錄用途失效的 SNAT IP 位址。 做為因應措施，可將負載平衡器設定為插入具有原始用戶端 IP 位址的 XFF HTTP 標頭。伺服器可設定為記錄 XFF 標頭中的 IP 位址，而不是連線的來源 IP 位址。
連線閒置逾時	輸入 HTTP 應用程式可維持閒置的時間 (以秒為單位)，而不是必須在 TCP 應用程式設定檔中設定的 TCP 通訊端設定。
要求標頭大小	指定用來儲存 HTTP 要求標頭的最大緩衝區大小 (以位元組為單位)。
NTLM 驗證	<p>切換負載平衡器的按鈕，以關閉 TCP 多工處理並啟用 HTTP 持續連線。</p> <p>NTLM 是可透過 HTTP 使用的驗證通訊協定。對於具有 NTLM 驗證的負載平衡，主控以 NTLM 為基礎的應用程式的伺服器集區必須停用 TCP 多工處理。否則，透過一個用戶端認證所建立的伺服器端連線可能會用來為另一個用戶端的要求提供服務。</p> <p>如果 NTLM 在設定檔中啟用且關聯至虛擬伺服器，而 TCP 多工處理在伺服器集區中啟用，則 NTLM 優先。不會針對該虛擬伺服器執行 TCP 多工處理。但是，如果同一個集區與另一個非 NTLM 虛擬伺服器相關聯，則 TCP 多工處理可供連線至該虛擬伺服器。</p> <p>如果用戶端使用 HTTP/1.0，則負載平衡器將升級至 HTTP/1.1 通訊協定並設定 HTTP 持續連線。在相同的用戶端 TCP 連線上接收的所有 HTTP 要求會透過單一 TCP 連線傳送到相同的伺服器，以確保不需要重新授權。</p>

d 按一下確定。

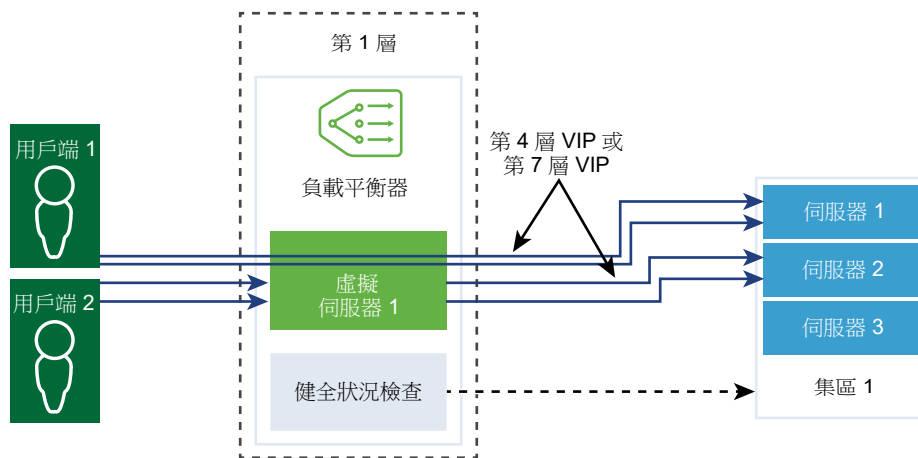
設定持續性設定檔

若要確保可設定狀態的應用程式的穩定性，負載平衡器會實作將所有相關連線導向至相同伺服器的持續性。支援不同類型的持續性以因應不同類型的應用程式需求。

某些應用程式會保持伺服器狀態，例如，購物車。此類狀態可能基於用戶端，並由用戶端 IP 位址或根據每個 HTTP 工作階段進行識別。當應用程式處理同一個用戶端或 HTTP 工作階段的後續相關連線時，可能會存取或修改此狀態。

來源 IP 持續性設定檔會追蹤以來源 IP 位址為基礎的工作階段。當用戶端要求與支援來源位址持續性的虛擬伺服器進行連線時，負載平衡器會先檢查此用戶端之前是否進行過連線，如果是，則會將此用戶端返回至相同的伺服器。如果不是，您可以根據集區負載平衡演算法選取伺服器集區成員。來源 IP 持續性設定檔由第 4 層和第 7 層虛擬伺服器使用。

Cookie 持續性設定檔將插入唯一 Cookie 以在用戶端第一次存取站台時識別工作階段。在後續要求中，用戶端會轉送 HTTP Cookie，而負載平衡器將使用該資訊以提供 Cookie 持續性。Cookie 持續性設定檔僅可供第 7 層虛擬伺服器使用。



程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取網路 > 負載平衡器 > 設定檔 > 持續性設定檔。
- 3 建立來源 IP 持續性設定檔。
 - a 從下拉式功能表中選取**新增 > 來源 IP 持續性**。
 - b 輸入來源 IP 持續性設定檔的名稱和說明。

- c 完成持續性設定檔詳細資料。

也可以接受預設的來源 IP 設定檔設定。

選項	說明
共用持續性	<p>切換按鈕以共用持續性，讓與此設定檔相關聯的所有虛擬伺服器均可共用持續性資料表。</p> <p>如果在關聯到虛擬伺服器的來源 IP 持續性設定檔中未啟用持續性共用，則與此設定檔相關聯的每個虛擬伺服器都將維護私用持續性資料表。</p>
持續性項目逾時	<p>輸入持續性到期時間 (以秒為單位)。</p> <p>負載平衡器持續性資料表維護用於記錄用戶端要求導向至相同伺服器的項目。</p> <ul style="list-style-type: none"> ■ 如果在此逾時期間內未收到來自相同用戶端的新連線要求，則持續性項目到期並且會刪除。 ■ 如果在此逾時期間內收到來自相同用戶端的新連線要求，則會重設計時器，並且將用戶端要求傳送至相黏集區成員。 <p>在此逾時期間到期後，新連線要求會傳送到由負載平衡演算法配置的伺服器。對於 L7 負載平衡 TCP 來源 IP 持續性案例，如果在一段時間內沒有任何新的 TCP 連線，即使現有連線仍在執行，持續性項目也會逾時。</p>
HA 持續性鏡像	<p>切換按鈕，將持續性項目同步至 HA 對等項。</p>
填滿時清除項目	<p>當持續性資料表填滿時清除項目。</p> <p>較大逾時值可能會導致持續性資料表在流量過大的情況下快速填滿。當持續性資料表填滿時，會刪除最舊的項目以接受最新項目。</p>

- d 按一下**確定**。

4 建立 Cookie 持續性設定檔。

- 從下拉式功能表中選取**新增 > Cookie 持續性**。
- 輸入 **Cookie** 持續性設定檔的名稱和說明。
- 切換**共用持續性**按鈕，以在關聯到相同集區成員的多個虛擬伺服器之間共用持續性。

Cookie 持續性設定檔將以 `<name>.<profile-id>.<pool-id>` 格式插入 Cookie。

如果共用的持續性在與虛擬伺服器相關聯的 **Cookie** 持續性設定檔中未啟用，則會使用每個虛擬伺服器的私用 **Cookie** 持續性，並由集區成員限定。負載平衡器將以 `<name>.<virtual_server_id>.<pool_id>` 格式插入 Cookie。

- d 按**下一步**。

- e 完成持續性設定檔詳細資料。

選項	說明
Cookie 模式	從下拉式功能表中選取模式。 <ul style="list-style-type: none"> ■ 插入 - 新增唯一的 Cookie 以識別工作階段。 ■ 前置詞 - 附加至現有的 HTTP Cookie 資訊。 ■ 重新寫入 - 重新寫入現有的 HTTP Cookie 資訊。
Cookie 名稱	輸入 Cookie 名稱。
Cookie 網域	輸入網域名稱。 僅在插入模式下，可以設定 HTTP Cookie 網域。
Cookie 路徑	輸入 Cookie URL 路徑。 僅在插入模式下，可以設定 HTTP Cookie 路徑。
Cookie 竄改	加密 Cookie 伺服器 IP 位址和連接埠資訊。 切換按鈕以停用加密。停用竄改時， Cookie 伺服器 IP 位址和連接埠資訊會以純文字顯示。
Cookie 後援	如果 Cookie 指向處於 [已停用] 或 [關閉] 狀態的伺服器，則選取新的伺服器來處理用戶端要求。 切換按鈕，以在 Cookie 指向處於 [已停用] 或 [關閉] 狀態的伺服器時拒絕用戶端要求。

- f 完成 **Cookie** 到期詳細資料。

選項	說明
Cookie 時間類型	從下拉式功能表中選取 Cookie 時間類型。 當瀏覽器關閉時，工作階段 Cookie 和持續性 Cookie 類型均到期。
閒置時間上限	輸入 Cookie 到期之前可閒置的時間 (以秒為單位)。

- g 按一下完成。

設定 SSL 設定檔

SSL 設定檔可設定獨立於應用程式的 SSL 內容，例如加密清單，並在多個應用程式之間重複使用這些清單。負載平衡器充當用戶端和伺服器時 SSL 內容會有所不同，因此，用戶端和伺服器端支援不同的 SSL 設定檔。

備註 NSX-T Data Center Limited Export 版本不支援 SSL 設定檔。

用戶端 SSL 設定檔是指充當 SSL 伺服器並終止用戶端 SSL 連線的負載平衡器。伺服器端 SSL 設定檔是指充當用戶端並建立與伺服器的連線的負載平衡器。

您可以同時在用戶端和伺服器端 SSL 設定檔上指定加密清單。

SSL 工作階段快取允許 SSL 用戶端和伺服器重複使用先前交涉的安全性參數，避免了 SSL 信號交換期間昂貴的公開金鑰作業。依預設，用戶端和伺服器端已停用 SSL 工作階段快取。

SSL 工作階段票證是一種替代機制，允許 SSL 用戶端和伺服器重複使用先前交涉的工作階段參數。在 SSL 工作階段票證中，用戶端與伺服器交涉是否在信號交換期間支援 SSL 工作階段票證。如果同時支援，伺服器可以將包含已加密 SSL 工作階段參數的 SSL 票證傳送至用戶端。用戶端可以在後續連線中使用該票證以重複使用工作階段。SSL 工作階段票證在用戶端處於啟用狀態，在伺服器端處於停用狀態。

圖 10-5. SSL 卸載

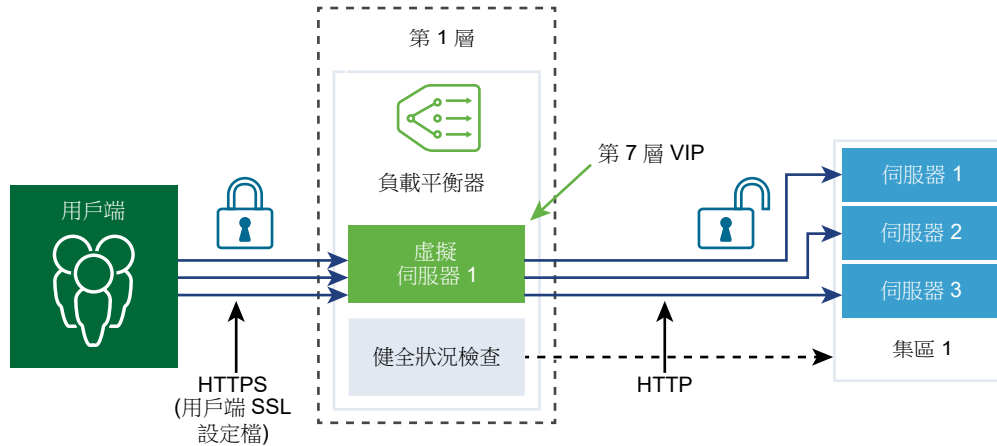
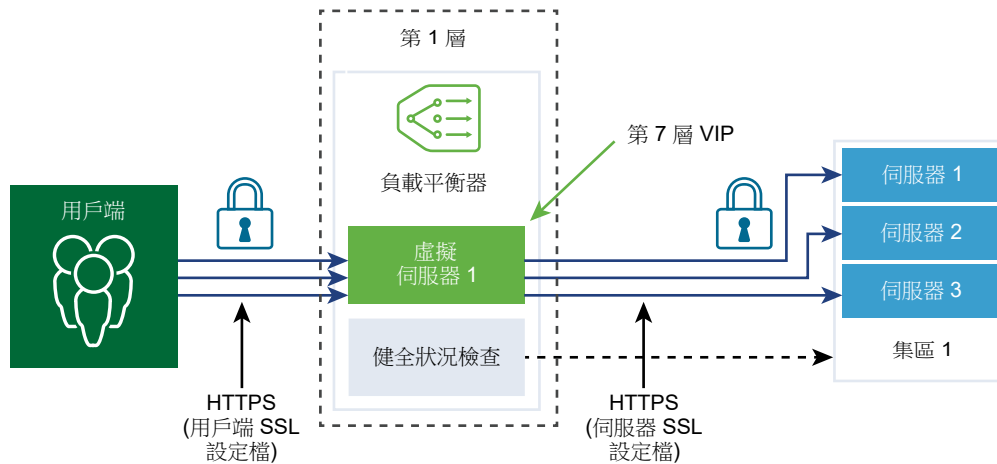


圖 10-6. 端對端 SSL



程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取網路 > 負載平衡器 > 設定檔 > SSL 設定檔。
- 3 建立用戶端 SSL 設定檔。
 - a 從下拉式功能表中選取新增 > 用戶端 SSL。
 - b 輸入用戶端 SSL 設定檔的名稱和說明。
 - c 指派要包含在用戶端 SSL 設定檔中的 SSL 加密方式。

您也可以建立自訂的 SSL 加密方式。

- d 按一下箭頭，將加密方式移至 [已選取] 區段。
- e 按一下**通訊協定和工作階段**索引標籤。
- f 選取要包含在用戶端 SSL 設定檔中的 SSL 通訊協定。

依預設，會啟用 SSL 通訊協定版本 TLS1.1 和 TLS1.2。TLS1.0 亦受到支援，但預設為停用。

- g 按一下箭頭，將通訊協定移至 [已選取] 區段。
- h 完成 SSL 通訊協定詳細資料。

也可以接受預設的 SSL 設定檔設定。

選項	說明
工作階段快取	SSL 工作階段快取允許 SSL 用戶端和伺服器重複使用先前交涉的安全性參數，避免了 SSL 信號交換期間昂貴的公開金鑰作業。
工作階段快取項目逾時	輸入快取逾時 (以秒為單位)，以指定 SSL 工作階段參數必須保留並且可重複使用的時間。
偏好的伺服器加密方式	切換按鈕，以便伺服器從可支援的清單中選取第一個支援的加密方式。 在 SSL 信號交換期間，用戶端向伺服器傳送支援的加密方式排序清單。

- i 按一下**確定**。

4 建立伺服器 SSL 設定檔。

- a 從下拉式功能表中選取**新增 > 伺服器端 SSL**。
- b 輸入伺服器 SSL 設定檔的名稱和說明。
- c 選取要包含在伺服器 SSL 設定檔中的 SSL 加密方式。

您也可以建立自訂的 SSL 加密方式。

- d 按一下箭頭，將加密方式移至 [已選取] 區段。
- e 按一下**通訊協定和工作階段**索引標籤。
- f 選取要包含在伺服器 SSL 設定檔中的 SSL 通訊協定。

依預設，會啟用 SSL 通訊協定版本 TLS1.1 和 TLS1.2。TLS1.0 亦受到支援，但預設為停用。

- g 按一下箭頭，將通訊協定移至 [已選取] 區段。
- h 接受預設的工作階段快取設定。

SSL 工作階段快取允許 SSL 用戶端和伺服器重複使用先前交涉的安全性參數，避免了 SSL 信號交換期間昂貴的公開金鑰作業。

- i 按一下**確定**。

設定第 4 層虛擬伺服器

虛擬伺服器會接收所有用戶端連線，並在伺服器之間進行散佈。虛擬伺服器具有 IP 位址、連接埠和通訊協定。針對第 4 層虛擬伺服器，可指定連接埠範圍的清單而非單一 TCP 或 UDP 連接埠，以支援具有動態連接埠的複雜通訊協定。

第 4 層虛擬伺服器必須與主要伺服器集區 (也稱為預設集區) 相關聯。

如果虛擬伺服器狀態為已停用，則會透過針對 TCP 連線傳送 TCP RST 或針對 UDP 傳送 ICMP 錯誤訊息，拒絕與虛擬伺服器的任何新連線嘗試。即使存在相符的持續性項目，仍會拒絕新連線。作用中連線會繼續處理。如果從負載平衡器刪除或解除關聯虛擬伺服器，則與該虛擬伺服器的作用中連線會失敗。

必要條件

- 確認應用程式設定檔可供使用。請參閱[設定應用程式設定檔](#)。
- 確認持續性設定檔可供使用。請參閱[設定持續性設定檔](#)。
- 確認用戶端與伺服器的 SSL 設定檔可供使用。請參閱[設定 SSL 設定檔](#)。
- 確認伺服器集區可供使用。請參閱[新增用於負載平衡的伺服器集區](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取**網路 > 負載平衡器 > 虛擬伺服器 > 新增**。
- 3 輸入第 4 層虛擬伺服器的名稱和說明。
- 4 從下拉式功能表中選取第 4 層通訊協定。

第 4 層虛擬伺服器支援 Fast TCP 或 Fast UDP 通訊協定，但不可同時支援。對於相同 IP 位址及連接埠的 Fast TCP 或 Fast UDP 通訊協定支援，例如 DNS，必須為每個通訊協定建立虛擬伺服器。

根據通訊協定類型，現有應用程式設定檔會自動填入。

- 5 切換 [存取記錄] 按鈕，以啟用第 4 層虛擬伺服器的記錄。
- 6 按**下一步**。
- 7 輸入虛擬伺服器 IP 位址和連接埠號碼。
您可以輸入虛擬伺服器連接埠號碼或連接埠範圍。
- 8 完成進階內容詳細資料。

選項	說明
並行連線數目上限	設定虛擬伺服器所允許的並行連線數目上限，以便虛擬伺服器不會耗盡相同負載平衡器上主控的其他應用程式的資源。
新連線速率上限	設定與伺服器集區成員的新連線數目上限，以便虛擬伺服器不會耗盡資源。
預設集區成員連接埠	如果未定義虛擬伺服器的集區成員連接埠，請輸入預設集區成員連接埠。 例如，如果虛擬伺服器所定義的連接埠範圍為 2000–2999，並且預設集區成員連接埠範圍設定為 8000–8999，則到虛擬伺服器連接埠 2500 的傳入用戶端連線會傳送到目的地連接埠設定為 8500 的集區成員。

- 9 從下拉式功能表中選取現有的伺服器集區。

伺服器集區由一或多個以相同方式設定且執行相同應用程式的伺服器 (亦稱為集區成員) 組成。

10 從下拉式功能表中選取現有 **sorry** 伺服器集區。

當負載平衡器無法選取後端伺服器以服務於來自預設集區的要求時，**sorry** 伺服器集區可服務於該要求。

11 按下一步。**12** 從下拉式功能表中選取現有持續性設定檔。

持續性設定檔可在虛擬伺服器上啟用，以允許將相關用戶端連線傳送至相同的伺服器。

13 按一下完成。

設定第 7 層虛擬伺服器

虛擬伺服器會接收所有用戶端連線，並在伺服器之間進行散佈。虛擬伺服器具有 IP 位址、連接埠和通訊協定 TCP。

僅具有 HTTP 應用程式設定檔的第 7 層虛擬伺服器支援負載平衡器規則。各種負載平衡器服務都可以使用負載平衡器規則。

每個負載平衡器規則由單一或多個比對條件以及單一或多個動作組成。如果未指定比對條件，則負載平衡器規則一律相符，並且可用來定義預設規則。如果指定多個比對條件，則相符策略會判定必須符合所有條件，還是符合任一條件，即可將負載平衡器規則視為相符項。

將在負載平衡處理的特定階段 (HTTP 要求重寫、HTTP 要求轉送和 HTTP 回應重寫) 實作每個負載平衡器規則。並非所有比對條件和動作均適用於每個階段。

如果虛擬伺服器狀態為已停用，則會透過針對 TCP 連線傳送 TCP RST 或針對 UDP 傳送 ICMP 錯誤訊息，拒絕與虛擬伺服器的任何新連線嘗試。即使存在相符的持續性項目，仍會拒絕新連線。作用中連線會繼續處理。如果從負載平衡器刪除或解除關聯虛擬伺服器，則與該虛擬伺服器的作用中連線會失敗。

必要條件

- 確認應用程式設定檔可供使用。請參閱[設定應用程式設定檔](#)。
- 確認持續性設定檔可供使用。請參閱[設定持續性設定檔](#)。
- 確認用戶端與伺服器的 SSL 設定檔可供使用。請參閱[設定 SSL 設定檔](#)。
- 確認伺服器集區可供使用。請參閱[新增用於負載平衡的伺服器集區](#)。
- 確認 CA 和用戶端憑證可供使用。請參閱[建立憑證簽署要求檔案](#)。
- 確認憑證撤銷清單 (CRL) 可供使用。請參閱[匯入憑證撤銷清單](#)。

設定第 7 層虛擬伺服器集區和規則

對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器規則，並使用比對或動作規則自訂負載平衡行為。

設定第 7 層虛擬伺服器負載平衡設定檔

對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器持續性、用戶端 SSL 和伺服器端 SSL 設定檔。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取 **網路 > 負載平衡器 > 虛擬伺服器 > 新增**。
- 3 輸入第 7 層虛擬伺服器的名稱和說明。
- 4 選取第 7 層功能表項目。
第 7 層虛擬伺服器支援 HTTP 和 HTTPS 通訊協定。
現有的 HTTP 應用程式設定檔會自動填入。
- 5 (選擇性) 按下一步以設定伺服器集區和負載平衡設定檔。
- 6 按一下完成。

設定第 7 層虛擬伺服器集區和規則

對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器規則，並使用比對或動作規則自訂負載平衡行為。

對於比對類型，負載平衡器規則支援 REGEX。支援 PCRE 樣式 REGEX 模式，但對進階使用案例存在一些限制。在比對條件中使用 REGEX 時，支援具名擷取群組。

REGEX 限制包括：

- 不支援字元聯集和交集。例如，請勿使用 `[a-z[0-9]]` 和 `[a-z&&[aeiou]]`，分別改為使用 `[a-z0-9]` 和 `[aeiou]`。
- 僅支援 9 個反向參考，並且不能使用 `\1` 到 `\9` 來參考它們。
- 使用 `\odd` 格式來比對八進位字元，而非 `\ddd` 格式。
- 最上層不支援內嵌式旗標，僅群組內支援這些旗標。例如，請勿使用「`Case (?i:s)ensitive`」，改為使用「`Case ((?i:s)ensitive)`」。
- 不支援前置處理作業 `\l`、`\u`、`\L` 及 `\U`。其中，`\l` - 可將下一個字元轉成小寫 `\u` - 可將下一個字元轉成大寫 `\L` - 可將 `\E` 之前的字元轉成小寫 `\U` - 可將 `\E` 之前的字元轉成大寫。
- 不支援 `(?(condition)X)`、`(?{code})`、`(??{Code})` 及 `(?#comment)`。
- 不支援預先定義的 Unicode 字元類別 `\X`。
- 不支援將具名字元建構用於 Unicode 字元。例如，請勿使用 `\N{name}`，改為使用 `\u2018`。

在比對條件中使用 REGEX 時，支援具名擷取群組。例如，可以使用 REGEX 比對模式 `/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+)/((?<article>.*))` 來比對諸如 `/news/2018-06-15/news1234.html` 的 URI。

然後，變數設定如下：`$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`。設定變數後，可以在負載平衡器規則動作中使用這些變數。例如，可以使用相符的變數 (如 `news.py?year=$year&month=$month&day=$day&article=$article`) 重寫 URI。該 URI 隨即會重寫為 `/news.py?year=2018&month=06&day=15&article=news1234.html`。

重寫動作可以使用具名擷取群組和內建變數的組合。例如，可以將 URI 寫成 `/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`。範例 URI 隨即重寫為 `/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`。

備註 對於具名擷取群組，名稱不能以 `_` 字元開頭。

除了具名擷取群組以外，還可以在重寫動作中使用下列內建變數。所有內建變數名稱皆以 `_` 開頭。

- `$_args` - 來自要求的引數
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_host` - 依優先順序排列 - 要求行中的主機名稱、「主機」要求標頭欄位中的主機名稱，或符合要求的伺服器名稱
- `$_hostname` - 主機名稱
- `$_http_<name>` - 任意要求標頭欄位，`<name>` 為轉換為小寫且虛線以底線取代的欄位名稱
- `$_https` - 如果連線在 SSL 模式下運作則為「on」，其他情況為「」
- `$_is_args` - 如果要求行具有參數則為「?」，其他情況為「」
- `$_query_string` - 與 `$_args` 相同
- `$_remote_addr` - 用戶端位址
- `$_remote_port` - 用戶端連接埠
- `$_request_uri` - 完整原始要求 URI (具有引數)
- `$_scheme` - 要求配置，「http」或「https」
- `$_server_addr` - 接受要求的伺服器的位址
- `$_server_name` - 接受要求的伺服器的名稱
- `$_server_port` - 接受要求的伺服器的連接埠
- `$_server_protocol` - 要求通訊協定，通常是「HTTP/1.0」或「HTTP/1.1」
- `$_ssl_client_cert` - 以 PEM 格式傳回已建立 SSL 連線的用戶端憑證，除第一行外，每一行的前面都會加上定位字元
- `$_ssl_server_name` - 傳回透過 SNI 要求的伺服器名稱
- `$_uri` - 要求中的 URI 路徑

必要條件

確認第 7 層虛擬伺服器可供使用。請參閱[設定第 7 層虛擬伺服器](#)。

程序

- 1 開啟第 7 層虛擬伺服器。
- 2 跳至 [虛擬伺服器識別碼] 頁面。

3 輸入虛擬伺服器 IP 位址和連接埠號碼。

您可以輸入虛擬伺服器連接埠號碼或連接埠範圍。

4 完成進階內容詳細資料。

選項	說明
並行連線數目上限	設定虛擬伺服器所允許的並行連線數目上限，以便虛擬伺服器不會耗盡相同負載平衡器上主控的其他應用程式的資源。
新連線速率上限	設定與伺服器集區成員的新連線數目上限，以便虛擬伺服器不會耗盡資源。
預設集區成員連接埠	如果未定義虛擬伺服器的集區成員連接埠，請輸入預設集區成員連接埠。 例如，如果虛擬伺服器所定義的連接埠範圍為 2000 – 2999，並且預設集區成員連接埠範圍設定為 8000 - 8999，則到虛擬伺服器連接埠 2500 的傳入用戶端連線會傳送到目的地連接埠設定為 8500 的集區成員。

5 (選擇性) 從下拉式功能表中選取現有的預設伺服器集區。

伺服器集區由一或多個以相同方式設定且執行相同應用程式的伺服器 (稱為集區成員) 組成。

6 按一下新增**，針對 HTTP 要求重寫階段設定負載平衡器規則。**

支援的比對類型為 REGEX、STARTS_WITH、ENDS_WITH 等以及反向選項。

支援的比對條件	說明
HTTP 要求方法	比對 HTTP 要求方法。 http_request.method - 要比對的值
HTTP 要求 URI	比對不含查詢引數的 HTTP 要求 URI。 http_request.uri - 要比對的值
HTTP 要求 URI 引數	比對 HTTP 要求 URI 查詢引數。 http_request.uri_arguments - 要比對的值
HTTP 要求版本	比對 HTTP 要求版本。 http_request.version - 要比對的值
HTTP 要求標頭	比對任何 HTTP 要求標頭。 http_request.header_name - 要比對的標頭名稱 http_request.header_value - 要比對的值
HTTP 要求裝載	比對 HTTP 要求的內文內容。 http_request.body_value - 要比對的值

支援的比對條件	說明
TCP 標頭欄位	比對 TCP 來源或目的地連接埠。 tcp_header.source_port - 要比對的來源連接埠 tcp_header.destination_port - 要比對的目的地連接埠
IP 標頭欄位	比對 IP 來源或目的地位址。 ip_header.source_address - 要比對的來源位址 ip_header.destination_address - 要比對的目的地位址
動作	說明
HTTP 要求 URI 重寫	修改 URI。 http_request.uri - 要寫入的 URI (不含查詢引數) http_request.uri_args - 要寫入的 URI 查詢引數
HTTP 要求標頭重寫	修改 HTTP 標頭的值。 http_request.header_name - 標頭名稱 http_request.header_value - 要寫入的值

7 按一下**新增**，針對 HTTP 要求轉送設定負載平衡器規則。

所有比對值都接受規則運算式。

支援的比對條件	說明
HTTP 要求方法	比對 HTTP 要求方法。 http_request.method - 要比對的值
HTTP 要求 URI	比對 HTTP 要求 URI。 http_request.uri - 要比對的值
HTTP 要求 URI 引數	比對 HTTP 要求 URI 查詢引數。 http_request.uri_args - 要比對的值
HTTP 要求版本	比對 HTTP 要求版本。 http_request.version - 要比對的值
HTTP 要求標頭	比對任何 HTTP 要求標頭。 http_request.header_name - 要比對的標頭名稱 http_request.header_value - 要比對的值
HTTP 要求裝載	比對 HTTP 要求的內文內容。 http_request.body_value - 要比對的值

支援的比對條件	說明
TCP 標頭欄位	比對 TCP 來源或目的地連接埠。 tcp_header.source_port - 要比對的來源連接埠 tcp_header.destination_port - 要比對的目的地連接埠
IP 標頭欄位	比對 IP 來源位址。 ip_header.source_address - 要比對的來源位址
動作	說明
拒絕	拒絕要求，例如，透過將狀態設定為 5xx。 http_forward.reply_status - 用於拒絕的 HTTP 狀態碼 http_forward.reply_message - HTTP 拒絕訊息
重新導向	重新導向要求。狀態碼必須設定為 3xx。 http_forward.redirect_status - 要重新導向的 HTTP 狀態碼 http_forward.redirect_url - HTTP 重新導向 URL
選取集區	強制執行對特定伺服器集區的要求。指定集區成員所設定的演算法 (預測工具) 用於選取伺服器集區內的伺服器。 http_forward.select_pool - 伺服器集區 UUID

8 按一下**新增**，針對 HTTP 回應重寫設定負載平衡器規則。

所有比對值都接受規則運算式。

支援的比對條件	說明
HTTP 回應標頭	比對任何 HTTP 回應標頭。 http_response.header_name - 要比對的標頭名稱 http_response.header_value - 要比對的值
動作	說明
HTTP 回應標頭重寫	修改 HTTP 回應標頭的值。 http_response.header_name - 標頭名稱 http_response.header_value - 要寫入的值

9 (選擇性) 按下一步以設定負載平衡設定檔。

10 按一下**完成**。

設定第 7 層虛擬伺服器負載平衡設定檔

對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器持續性、用戶端 SSL 和伺服器端 SSL 設定檔。

備註 NSX-T Data Center 2.2 Limited Export 版本不支援 SSL 設定檔。

如果在虛擬伺服器上設定用戶端 SSL 設定檔繫結，而不是伺服器端 SSL 設定檔繫結，則虛擬伺服器會在 SSL 終止模式 (具有與用戶端的加密連線和與伺服器的純文字連線) 下運作。如果同時設定了用戶端和伺服器端 SSL 設定檔繫結，則虛擬伺服器會在 SSL Proxy 模式 (具有與用戶端和伺服器的加密連線) 下運作。

目前不支援在未關聯用戶端 **SSL** 設定檔繫結的情況下，關聯伺服器端 **SSL** 設定檔繫結。如果用戶端和伺服器端 **SSL** 設定檔繫結未與虛擬伺服器建立關聯，並且應用程式以 **SSL** 為基礎，則虛擬伺服器會在無法感知 **SSL** 的模式下運作。在此情況下，第 4 層必須設定虛擬伺服器。例如，虛擬伺服器可關聯至快速 **TCP** 設定檔。

必要條件

確認第 7 層虛擬伺服器可供使用。請參閱[設定第 7 層虛擬伺服器](#)。

程序

- 1 開啟第 7 層虛擬伺服器。
- 2 請跳至 [負載平衡設定檔] 頁面。
- 3 切換 [持續性] 按鈕以啟用設定檔。
持續性設定檔允許將相關用戶端連線傳送至相同的伺服器。
- 4 選取來源 IP 持續性或 Cookie 持續性設定檔。
- 5 從下拉式功能表中選取現有持續性設定檔。
- 6 按下一步。
- 7 切換 [用戶端 SSL] 按鈕以啟用設定檔。
用戶端 **SSL** 設定檔繫結允許多個憑證，讓不同的主機名稱關聯至相同的虛擬伺服器。
相關聯的用戶端 **SSL** 設定檔會自動填入。
- 8 從下拉式功能表中選取預設憑證。
如果伺服器未主控相同 IP 位址上的多個主機名稱或用戶端不支援伺服器名稱指示 (**SNI**) 延伸，則會使用此憑證。
- 9 選取可用的 **SNI** 憑證，然後按一下箭頭將憑證移至 [已選取] 區段。
- 10 (選擇性) 切換 [強制用戶端驗證] 以啟用此功能表項目。
- 11 選取可用的 **CA** 憑證，然後按一下箭頭將憑證移至 [已選取] 區段。
- 12 設定憑證鏈結深度，以驗證伺服器憑證鏈結的深度。
- 13 選取可用的 **CRL**，然後按一下箭頭將憑證移至 [已選取] 區段。
CRL 可設定為禁止已損毀的伺服器憑證。
- 14 按下一步。
- 15 切換 [伺服器端 SSL] 按鈕以啟用設定檔。
相關聯的伺服器端 **SSL** 設定檔會自動填入。
- 16 從下拉式功能表中選取用戶端憑證。
如果伺服器未主控相同 IP 位址上的多個主機名稱或用戶端不支援伺服器名稱指示 (**SNI**) 延伸，則會使用用戶端憑證。

17 選取可用的 **SNI** 憑證，然後按一下箭頭將憑證移至 [已選取] 區段。

18 (選擇性) 切換 [伺服器驗證] 以啟用此功能表項目。

伺服器端 **SSL** 設定檔繫結會指定是否必須驗證在 **SSL** 信號交換期間提供給負載平衡器的伺服器憑證。啟用驗證後，伺服器憑證必須由自我簽署憑證在相同的伺服器端 **SSL** 設定檔繫結中指定的其中一個受信任的 **CA** 簽署。

19 選取可用的 **CA** 憑證，然後按一下箭頭將憑證移至 [已選取] 區段。

20 設定憑證鏈結深度，以驗證伺服器憑證鏈結的深度。

21 選取可用的 **CRL**，然後按一下箭頭將憑證移至 [已選取] 區段。

CRL 可設定為禁止已損毀的伺服器憑證。伺服器端不支援 **OCSP** 和 **OCSP** 裝訂。

22 按一下**完成**。

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，並建立 DHCP 轉送服務以將 DHCP 流量轉送至外部 DHCP 伺服器。但是，您不應當在某個邏輯交換器上設定 DHCP 伺服器的同時，在相同邏輯交換器連線到的路由器連接埠上設定 DHCP 轉送服務。在此情況下，DHCP 要求將僅會傳遞到 DHCP 轉送服務。

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。

本章節討論下列主題：

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

- 2 選取導覽面板中的**網路 > 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 (選擇性) 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 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 (必要) 從下拉式功能表中選取 **DHCP 設定檔**。
- 7 (選擇性) 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 (選擇性) 輸入無類別靜態路由選項。
- 9 (選擇性) 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。VLAN 邏輯交換器不支援 DHCP 伺服器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 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 > 連結 DHCP 伺服器**。

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 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 Data Center 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 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。

必要條件

- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 路由**。
- 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。

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。

本章節討論下列主題：

- [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。

必要條件

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

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的 **網路 > DHCP**。
- 3 按一下 **中繼資料 Proxy** 索引標籤。

- 4 按一下**新增**。
- 5 輸入中繼資料 Proxy 伺服器的名稱。
- 6 (選擇性) 輸入說明。
- 7 輸入 Nova 伺服器的 URL 和連接埠。
有效的連接埠範圍為 3000 - 9000。
- 8 輸入**密碼**的值。
- 9 從下拉式清單中選取 NSX Edge 叢集。
- 10 (選擇性) 選取 NSX Edge 叢集的成員。

範例

例如：

New Metadata Proxy Server ⓘ ×

Name * metadata-proxy-1

Description

Nova Server URL * https://123.1.1.1:8775

Secret * *****

Edge Cluster * edge_cluster_p1r1 ▼

Members 53524616-c67f-11e8-837f-020046520048 × ▼

CANCEL ADD

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。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > DHCP**。
- 3 按一下**中繼資料 Proxy** 索引標籤。
- 4 選取中繼資料 Proxy 伺服器。
- 5 選取功能表選項**動作 > 連結至邏輯交換器**
- 6 從下拉式清單中選取邏輯交換器。

結果

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**，接著選取交換器，然後選取功能表選項**動作 > 連結中繼資料 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > DHCP**。
- 3 按一下**中繼資料 Proxy** 索引標籤。
- 4 選取中繼資料 Proxy 伺服器。
- 5 選取功能表選項**動作 > 從邏輯交換器中斷連結**
- 6 從下拉式清單中選取邏輯交換器。

結果

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

您可以使用 IP 位址管理 (IPAM) 來建立 IP 區塊以支援 NSX-T Container Plug-in (NCP)。如需有關 NCP 的詳細資訊，請參閱《適用於 Kubernetes 的 NSX-T Container Plug-in - 安裝和管理指南》。

本章節討論下列主題：

- 管理 IP 區塊
- 管理 IP 區塊的子網路

管理 IP 區塊

設定 NSX-T Container Plug-in 需要建立容器的 IP 區塊。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > IPAM**。
- 3 若要新增 IP 區塊，請按一下**新增**。
 - a 輸入名稱和 (選用) 說明。
 - b 以 CIDR 格式輸入 IP 區塊。例如，10.10.10.0/24。
- 4 若要編輯 IP 區塊，請按一下 IP 區塊的名稱。
 - a 在**概觀**索引標籤中，按一下**編輯**。
您可以變更名稱、說明或 IP 區塊值。
- 5 若要管理 IP 區塊的標記，請按一下 IP 區塊的名稱。
 - a 在**概觀**索引標籤中，按一下**管理**。
您可以新增或刪除標記。
- 6 若要刪除一或多個 IP 區塊，請選取區塊。
 - a 按一下**刪除**。
您無法刪除已配置其子網路的 IP 區塊。

管理 IP 區塊的子網路

您可以新增或刪除 IP 區塊的子網路

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > IPAM**。
- 3 按一下 IP 區塊的名稱。
- 4 按一下**子網路**索引標籤。
- 5 若要新增子網路，請按一下**新增**。
 - a 輸入名稱和 (選用) 說明。
 - b 輸入子網路的大小。
- 6 若要刪除一或多個子網路，請選取子網路。
 - a 按一下**刪除**。

原則是規則與服務的組合，其中規則定義資源存取和使用的準則。透過 **NSX** 原則，您可以管理資源存取和使用，且無需擔心低層級詳細資料。

本章節討論下列主題：

- 概觀
- 新增強制執行點
- 新增服務
- 新增網域
- 設定 **NSX Policy Manager** 的備份
- 備份 **NSX Policy Manager**
- 還原 **NSX Policy Manager**
- 將 **vIDM** 主機與 **NSX Policy Manager** 相關聯
- 管理角色指派

概觀

透過 **NSX** 原則，您可以指定虛擬機器、邏輯連接埠、IP 位址和 **MAC** 位址等物件的規則，且無需擔心規則機制。您可以從 **NSX Policy Manager** 而非 **NSX Manager** 管理原則。

設定原則之前，您必須安裝 **NSX Policy Manager**。如需詳細資訊，請參閱《**NSX-T** 安裝指南》。在 **NSX Policy Manager** 中，還必須新增一或多個強制執行點，以提供將套用原則之 **NSX Manager** 的相關資訊。

下列範例說明如何使用原則來管理應用程式的網路。

應用程式具有三個階層 (**Web**、應用程式和資料庫)，您希望下列規則套用至應用程式的虛擬機器：

- 允許 **Web** 層和應用程式層之間的流量。
- 允許應用程式層和資料庫層之間的流量。
- 允許任何系統和 **Web** 層之間的流量。

在 **NSX Manager** 上執行下列步驟：

- 將 **Web** 虛擬機器的工作負載名稱設定為 **Web**，後面跟隨一些識別字串。

- 將應用程式虛擬機器的工作負載名稱設定為 **App**，後面跟隨一些識別字串。
- 將資料庫虛擬機器的工作負載名稱設定為 **DB**，後面跟隨一些識別字串。

在 **NSX Policy Manager** 上執行下列步驟：

- 建立網域並指定下列項目：
 - 建立名為 **WebGroup** 的群組，此群組由工作負載名稱開頭為 **Web** 的虛擬機器組成。
 - 建立名為 **AppGroup** 的群組，此群組由工作負載名稱開頭為 **App** 的虛擬機器組成。
 - 建立名為 **DBGroup** 的群組，此群組由工作負載名稱開頭為 **DB** 的虛擬機器組成。
 - 指定用於控制群組間通訊的安全性原則。
- 驗證網域組態，以確保沒有任何錯誤。
- 選取強制執行點。

在您選取強制執行點之後，**NSX Policy Manager** 便會與強制執行點上的 **NSX Manager** 通訊，這將實作安全性原則。

角色型存取控制

NSX Policy Manager 有兩個內建使用者：**admin** 和 **audit**。您可以將 **NSX Policy Manager** 與 **VMware Identity Manager (vIDM)** 整合，並針對 **vIDM** 所管理的使用者設定角色型存取控制 (RBAC)。

對於 **vIDM** 管理的使用者，適用的驗證原則是 **vIDM** 管理員設定的原則，而非僅適用於使用者 **admin** 和 **audit** 的 **NSX Policy Manager** 驗證原則。

新增強制執行點

強制執行點是要套用原則規則的位置。在此版本中，強制執行點必須為 **NSX-T** 安裝，並且 **NSX Policy Manager** 僅支援一個強制執行點。

程序

- 1 從您的瀏覽器登入 **NSX Policy Manager**，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的 **系統 > 強制執行點**。
- 3 按一下 **新增**。
- 4 請提供下列資訊。

參數	說明
名稱	強制執行點的名稱。
認證	用於登入 NSX Manager 的使用者名稱和密碼。
強制執行位址	NSX Manager 的 IP 位址。
指紋	NSX Manager 的憑證指紋。

- 5 按一下 **儲存**。

新增服務

服務是指您環境中的通訊協定或軟體元件。原則包含套用至服務的規則。

服務範例包括 FTP、HTTP、AD 伺服器、DHCP 伺服器、Oracle 資料庫等。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**基礎結構 > 服務**。
- 3 按一下**新增服務**。
- 4 輸入服務的名稱。
- 5 按一下**設定服務項目**，以新增服務項目。
 - a 按一下**新增服務項目**。
 - b 選取服務類型。
 可用的類型為 **IP**、**IGMP**、**ICMP**、**ALG**、**TCP** 及 **UDP**。
 - c 按一下**其他內容**下拉式清單，以選取內容。
 您可以新增其他項目、編輯或刪除項目。
- 6 按一下**儲存**。

新增網域

網域是具有一般業務目標並且需要套用原則之工作負載的邏輯集合。它包含一組群組及其對應的通訊需求。

如果您計劃建立多個大型網域 (每個都具有超過 200 個結果規則)，請務必依序將其部署到強制執行點，以等待解析目前網域後再繼續解析下一個。如果使用 API 部署這些網域，建議在將網域部署到強制執行點之前建立通訊項目。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**基礎結構 > 網域**。
- 3 按一下**新增網域**，以新增網域。
- 4 指定網域名稱並選擇性地指定說明。
- 5 按**下一步**前往「工作負載群組」步驟。
- 6 按一下**新增群組**，以新增一或多個工作負載群組。對於每個工作負載群組，
 - a 請指定名稱。
 - b 按一下**成員類型**欄位，以選取成員類型。
 可用的選項有**虛擬機器**、**IP 位址**及**成員資格準則**。

- c 對於**虛擬機器**和**IP 位址**，請指定值。
 - d 對於**成員資格準則**，請按一下**設定成員資格準則**，以指定如何選取成員。
- 7 按**下一步**前往「安全性」步驟。
 - 8 按一下**新增區段**以新增防火牆區段，或按一下**新增規則**以新增防火牆規則。
您可以新增多個區段和規則。
 - 9 按**下一步**前往「驗證網域組態」步驟。
此時會顯示該網域的圖形表示。
 - 10 按**下一步**前往「選取強制執行點」步驟。
 - 11 選取一或多個強制執行點。
 - 12 按一下**完成**以部署網域。

設定 NSX Policy Manager 的備份

您可以備份 NSX Policy Manager 來保護 Policy Manager 所儲存的資料。您必須先設定備份內容，然後才能執行備份。

必要條件

確認您擁有備份檔案伺服器的 SSH 指紋。系統僅接受 SHA256 雜湊的 ECDSA 金鑰作為指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**系統 > 公用程式**。
- 3 按一下**設定**。
- 4 按一下**自動備份**切換按鈕以啟用或停用自動備份。
- 5 輸入備份檔案伺服器的 IP 位址或主機名稱。
- 6 視需要編輯預設連接埠。
- 7 輸入登入備份檔案伺服器所需的使用者名稱和密碼。
- 8 在**目的地目錄**欄位中，輸入儲存備份的絕對目錄路徑。
目錄必須已存在。
- 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**排程索引**標籤。

12 選取頻率。

如果選取**每週**，可指定星期幾及時間。如果選取**時間間隔**，可指定時間間隔。

13 按一下儲存。

備份 NSX Policy Manager

您可以自動或手動備份 NSX Policy Manager。

如果您已設定自動備份，便會自動進行。此程序適用於手動起始備份。

必要條件

確認您已設定備份內容。請參閱[設定 NSX Policy Manager 的備份](#)。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**系統 > 公用程式**。
- 3 按一下**立即備份**。

還原 NSX Policy Manager

您可以從備份將 NSX Policy Manager 還原為過去的某個狀態。

必要條件

確認您擁有備份檔案伺服器的 SSH 指紋。系統僅接受 SHA256 雜湊的 ECDSA 金鑰作為指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**系統 > 公用程式**。
- 3 按一下**立即還原**。
- 4 確認有關必要條件和風險的訊息，然後按**下一步**。
- 5 輸入備份伺服器的 IP 位址或主機名稱。
- 6 視需要變更連接埠號碼。
預設值為 22。
- 7 輸入用來登入伺服器的使用者名稱和密碼。
- 8 在**備份目錄**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。
- 10 輸入備份伺服器的 SSH 指紋。

11 按下一步。

12 選取備份。

13 按一下**還原**。

隨即顯示還原作業的狀態。如果您在備份後已刪除或新增網狀架構節點或傳輸節點，則系統將會提示您執行特定動作，例如登入節點並執行指令碼。

還原作業完成後會出現 [還原完成] 畫面，其中會顯示還原的結果、備份檔案的時間戳記，以及還原作業的開始和結束時間。如果還原失敗，畫面會顯示作業失敗的步驟。若要再次嘗試還原作業，您必須使用新原則管理員應用裝置，不能使用作業失敗的應用裝置。

將 vIDM 主機與 NSX Policy Manager 相關聯

若要讓 NSX Policy Manager 與 vIDM 進行整合，您必須提供 vIDM 主機的相關資訊。

vIDM 伺服器應具有憑證授權機構 (CA) 簽署的憑證。否則，可能無法在某些瀏覽器上從 NSX Policy Manager 登入 vIDM，例如 Microsoft Edge 或 Internet Explorer 11。如需在 vIDM 上安裝 CA 簽署憑證的相關資訊，請參閱 <https://docs.vmware.com/tw/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>。

當您向 vIDM 登錄 NSX Policy Manager 時，會指定指向至 Policy Manager 的重新導向 URI。您可以提供完整網域名稱 (FQDN) 或 IP 位址。請務必記住您是使用 FQDN 還是 IP 位址。當您嘗試透過 vIDM 登入 Policy Manager 時，必須以相同方式在 URL 中指定主機名稱，即，如果您向 vIDM 登錄管理程式時使用 FQDN，則必須在 URL 中使用 FQDN，且如果向 vIDM 登錄管理程式時使用 IP 位址，則必須在 URL 中使用 IP 位址。否則，將無法登入。

必要條件

- 確認您擁有 vIDM 主機提供的憑證指紋。請參閱從 [vIDM 主機取得憑證指紋](#)。
- 確認已向 vIDM 主機登錄 NSX Policy Manager 做為 OAuth 用戶端。在登錄程序期間，記下用戶端識別碼和用戶端密碼。如需詳細資訊，請參閱位於 <https://www.vmware.com/support/pubs/identitymanager-pubs.html> 的 VMware Identity Manager 說明文件。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-IP-address>。
- 2 選取導覽面板中的**系統 > 使用者**。
- 3 按一下**組態索引標籤**。
- 4 按一下**編輯**。
- 5 按一下 **VMware Identity Manager 整合** 切換按鈕以切換至已啟用。

6 請提供下列資訊。

參數	說明
VMware Identity Manager 應用裝置	vIDM 主機的完整網域名稱 (FQDN)。
OAuth 用戶端識別碼	向 vIDM 主機登錄 NSX Policy Manager 時所建立的識別碼。
OAuth 用戶端密碼	向 vIDM 主機登錄 NSX Policy Manager 時所建立的密碼。
SHA-256 指紋	vIDM 主機的憑證指紋。
NSX 原則應用裝置	NSX Policy Manager 的 IP 位址或完整網域名稱 (FQDN)。如果指定 FQDN，必須在 URL 中使用 Manager 的 FQDN 從瀏覽器存取 NSX Policy Manager；如果指定 IP 位址，則必須在 URL 中使用 IP 位址。或者，vIDM 管理員可以設定 NSX Policy Manager 用戶端，以便您使用 FQDN 或 IP 位址連線。

7 按一下儲存。

管理角色指派

當 VMware Identity Manager 與 NSX Policy Manager 整合時，您可以新增、變更和刪除對使用者或使用者群組的角色指派。

下列角色會預先定義。您無法新增角色。

- 企業管理員
- 稽核員
- 網站可靠性工程師 (VMware Cloud 部署中提供)
- 雲端服務管理員 (VMware Cloud 部署中提供)
- 雲端服務稽核員 (VMware Cloud 部署中提供)

必要條件

- 確認 vIDM 主機與 NSX Policy Manager 相關聯。如需詳細資訊，請參閱[將 vIDM 主機與 NSX Policy Manager 相關聯](#)。

程序

- 1 從您的瀏覽器登入 NSX Policy Manager，網址為 <https://nsx-policy-manager-ip-address>。
- 2 選取導覽面板中的 **系統 > 使用者**。
- 3 按一下 **角色指派** 索引標籤 (若尚未選取)。
- 4 新增、變更或刪除角色指派。

選項	動作
新增角色指派	按一下 新增 ，接著選取使用者或使用者群組，然後選取角色。
變更角色指派	選取使用者或使用者群組，然後按一下 編輯 。
刪除角色指派	選取使用者或使用者群組，然後按一下 刪除 。

您可以使用服務插入將第三方服務套用至經過路由器的南北向流量和東西向流量。服務通常提供進階安全功能，如入侵偵測系統 (IDS) 或入侵防護系統 (IPS)。

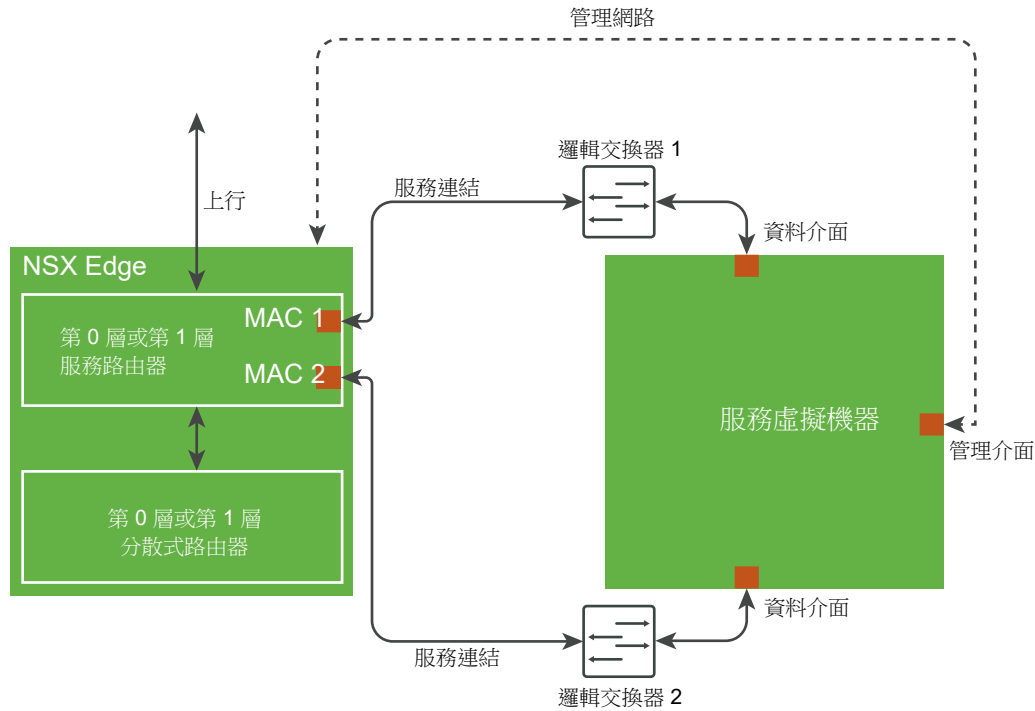
本章節討論下列主題：

- [概觀](#)
- [登錄服務](#)
- [部署服務執行個體](#)
- [設定流量重新導向](#)
- [監控流量重新導向](#)

概觀

您可以設定服務插入，將第 0 層路由器處的南北向流量或第 1 層路由器處的東西向流量重新導向至虛擬機器。虛擬機器中執行的服務可以處理流量，並採取適當的動作。

以下架構圖顯示設定了服務插入的資料流量。



服務插入透過兩個 **Edge** 節點和兩個服務虛擬機器，在主動備用模式下支援高可用性 (HA)。它不會在主動-主動式模式下支援 HA。路由器僅可支援一個服務。

設定服務插入涉及下列步驟：

- 登錄服務。
- 部署服務執行個體。
- 設定流量重新導向。

登錄服務

登錄服務需要執行 API 呼叫。登錄服務後，您可以在 NSX Manager UI 中檢視它。

有關 API 呼叫和輸入參數的詳細資料位於《NSX-T Data Center API 參考》中。

程序

- 1 執行下列 API 呼叫來登錄服務：

```
POST /api/v1/serviceinsertion/services
```

例如，

```
POST https://<nsx-mgr>/api/v1/serviceinsertion/services
{
  "display_name": "NS Service for ABC partner",
  "description": "This service is inserted at T0 router and it provides advanced security",
  "attachment_point": [
```

```

    "TIER0_LR"
  ],
  "functionalities": [
    "NG_FW"
  ],
  "implementations": [
    "NORTH_SOUTH"
  ],
  "transports": [
    "L2_BRIDGE"
  ],
  "vendor_id": "ABC_Partner",
  "on_failure_policy": "ALLOW",
  "service_deployment_spec": {
    "deployment_specs": [{
      "ovf_url": "http://server.com/dir1/ABC-Company-HA-OVF/ABC-VM-ESX-2.0.ovf",
      "name": "NS_DepSpec",
      "host_type": "ESXI",
      "service_form_factor": "MEDIUM"
    }],
    "nic_metadata_list": [
      {
        "interface_label": "eth",
        "interface_index": 0,
        "interface_type": "MANAGEMENT"
      },
      {
        "interface_label": "eth",
        "interface_index": 1,
        "interface_type": "DATA1"
      },
      {
        "interface_label": "eth",
        "interface_index": 2,
        "interface_type": "DATA2"
      }
    ]
  },
  "deployment_template": [{
    "name": "NS_DepTemp",
    "attributes": [{
      "attribute_type": "STRING",
      "display_name": "License",
      "key": "LicenseKey"
    }]
  }]
}

```

- 2 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 3 選取導覽面板中的**合作夥伴服務**。
- 4 按一下目錄索引標籤，並確保服務已登錄。

後續步驟

部署服務的執行個體。請參閱[部署服務執行個體](#)。

部署服務執行個體

登錄服務後，您必須部署服務的執行個體，服務才能開始處理網路流量。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**合作夥伴服務**。
- 3 按一下**部署**。
- 4 輸入執行個體名稱，並選擇性地輸入說明。
- 5 按一下**合作夥伴服務**欄位，然後選取服務。
- 6 選取**部署規格**。
- 7 選取邏輯路由器。
將僅顯示尚未設定服務插入的路由器。
- 8 按下一步。
- 9 按一下**計算管理程式**欄位，然後選取計算管理程式。
- 10 按一下**叢集**欄位，然後選取叢集。
- 11 (選擇性) 按一下**資源集區**欄位，然後選取資源集區 (若已在 vCenter Server 中設定)。
- 12 按一下**資料存放區**欄位，然後選取資料存放區。
- 13 選取**部署模式**。
選項有**獨立**或**高可用性**。
- 14 選取**故障原則**。
選項有**允許**或**封鎖**。
- 15 輸入虛擬機器的 IP 位址。
- 16 輸入虛擬機器的 IP 位址的預設閘道。
- 17 輸入虛擬機器的 IP 位址的子網路遮罩。
- 18 按下一步。
- 19 選取**部署範本**。
- 20 輸入合作夥伴服務的授權。
- 21 按一下**完成**。

結果

部署程序可能需要一些時間，具體取決於廠商的實作。您可以在管理程式 UI 中檢視狀態。部署成功後，狀態將為部署成功。

後續步驟

設定服務執行個體的流量重新導向。請參閱[設定流量重新導向](#)。

設定流量重新導向

部署服務執行個體之後，您可以設定路由器會重新導向至該服務的流量的類型。設定流量重新導向類似於設定防火牆。

如需有關設定防火牆的資訊，請參閱[第 7 章 防火牆區段和防火牆規則](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的[合作夥伴服務](#)。
- 3 按一下服務執行個體的名稱。
- 4 按一下[流量重新導向](#)索引標籤。
- 5 新增或移除區段和規則。

監控流量重新導向

部署服務執行個體並設定流量重新導向後，您可以監控出入服務執行個體的流量。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的[合作夥伴服務](#)。
- 3 按一下服務執行個體的名稱。
概觀索引標籤會顯示服務執行個體的組態和狀態。
- 4 按一下[統計資料](#)索引標籤。
會顯示出入服務執行個體的封包數和資料量的相關資訊。
- 5 按一下[重新整理](#)以更新統計資料。

NSX Cloud 可讓您使用 NSX-T Data Center 管理並保護您的公有雲詳細目錄。

如需 NSX Cloud 元件的清單和說明，請參閱《NSX-T Data Center 安裝指南》中的〈[NSX Cloud 架構和元件](#)〉。

本章節討論下列主題：

- [Cloud Service Manager](#)
- 管理隔離原則
- 工作負載虛擬機器上線及管理概觀
- 工作負載虛擬機器上線
- 管理工作負載虛擬機器
- 使用進階 NSX Cloud 功能
- 疑難排解

Cloud Service Manager

Cloud Service Manager (CSM) 針對公有雲詳細目錄提供單一虛擬管理介面管理端點。

CSM 介面可分為以下類別：

- **搜尋：**您可以使用搜尋文字方塊，尋找公有雲帳戶或相關建構。
- **雲端：**公有雲詳細目錄透過此類別下的區段進行管理。
- **系統：**您可以從此類別存取 Cloud Service Manager 的**設定**、**公用程式**以及**使用者**。

您可以前往 CSM 的**雲端**子區段，來執行所有公有雲作業。

若要執行以系統為基礎的作業，例如，備份、還原、升級和使用者管理，請移至**系統**子區段。

雲端

這些是雲端下的區段：

雲端 > 概觀

可透過按一下**雲端**來存取您的公有雲帳戶。

概觀：此畫面上的每個動態磚表示您的公有雲帳戶，以及該帳戶包含的帳戶數目、區域、VPC 或 VNet 及執行個體 (工作負載虛擬機器)。

您可以執行下列工作：

新增公有雲帳戶或訂閱	您可以新增一或多個公有雲帳戶或訂閱。這可讓您檢視 CSM 中的公有雲詳細目錄，並指示由 NSX-T Data Center 管理的虛擬機器數目及其狀態。 請參閱《NSX-T Data Center 安裝指南》中的〈 新增公有雲帳戶 〉，以取得詳細指示。
部署/取消部署 NSX Public Cloud Gateway	您可以部署或取消部署一或兩個 (針對 High Availability) PCG。您也可以從 CSM 取消部署 PCG。 請參閱《NSX-T Data Center 安裝指南》中的〈 部署 PCG 〉或〈 取消部署 PCG 〉，以取得詳細指示。
啟用或停用隔離原則	您可以啟用或停用隔離原則。如需詳細資料，請參閱 管理隔離原則 。
在網格視圖和卡視圖間切換	卡顯示詳細目錄的概觀。網格會顯示更多詳細資料。按一下圖示可切換視圖類型。

CSM 透過以不同方式呈現公有雲詳細目錄，提供與 NSX Cloud 連線之所有公有雲帳戶的整體視圖。

- 您可以檢視運作的區域數目。
- 您可以檢視每個區域的私人網路數目。
- 您可以檢視每個私人網路的工作負載虛擬機器數目。

雲端下提供四個索引標籤。

另請參閱 [CSM 圖和圖示](#)，以取得 UI 元素的說明。

雲端 > {公有雲} > 帳戶

CSM 的 [帳戶] 區段提供已新增的公有雲帳戶相關資訊。

每張卡片代表您從 [雲端] 下選取之雲端提供者的一個公有雲帳戶。

在此區段中，您可以執行下列動作：

- 新增帳戶
- 編輯帳戶
- 刪除帳戶
- 重新同步帳戶

雲端 > {公有雲} > 區域

[區域] 區段會顯示所選區域的詳細目錄。

您可以依公有雲帳戶來篩選區域。每個區域具有 VPC 或 VNet，以及執行個體。如果您已部署任何 PCG，則可以在此處將其視為具有 PCG 健全狀況指示器的開道。

雲端 > {公有雲} > VPC 或 VNet

VPC 或 VNet 區段會顯示私有雲詳細目錄。

您可以依帳戶和區域來篩選詳細目錄。

- 每張卡片代表一個 VPC 或 VNet。
- 您可在每個 VPC 或 VNet 中部署一或兩個 (對於 HA) PCG。
- 您可以切換至網格視圖來檢視每個 VPC 或 VNet 的更多詳細資料。
- 按一下**動作**可存取下列項目：
 - **編輯組態**：
 - 啟用或停用隔離原則。
 - 變更 Proxy 伺服器選擇。
 - **部署 NSX Cloud 閘道**：按一下此選項，開始在此 VPC 或 VNet 上部署 PCG。如果已部署 PCG 或 PCG 的高可用性配對，則無法使用此選項。請參閱《NSX-T Data Center 安裝指南》中的〈部署 PCG〉，以取得詳細指示。

雲端 > {公有雲} > 執行個體

[執行個體] 區段會顯示 VPC 或 VNet 中的執行個體的詳細資料。

您可以依帳戶、區域及 VPC 或 VNet 來篩選執行個體詳細目錄。

每張卡片代表一個執行個體 (工作負載虛擬機器)，並顯示摘要。

如需有關執行個體的詳細資料，請按一下卡片或切換至網格視圖。

備註 CSM 會針對由 NSX 管理的虛擬機器顯示作業系統版本值，但對於不受 NSX 管理的虛擬機器，至少會詳細顯示作業系統的類型，因為這是從雲端提供者 API 取得。

CSM 圖和圖示

CSM 使用說明性和直覺式圖示來顯示公有雲建構的狀態和健全狀況。

備註 只有在**啟用隔離**設定已開啟時，才會套用隔離工作流程。依預設會關閉該設定。

VNet

圖 16-1. 受 NSX Cloud 管理的虛擬機器狀況良好的 VNet

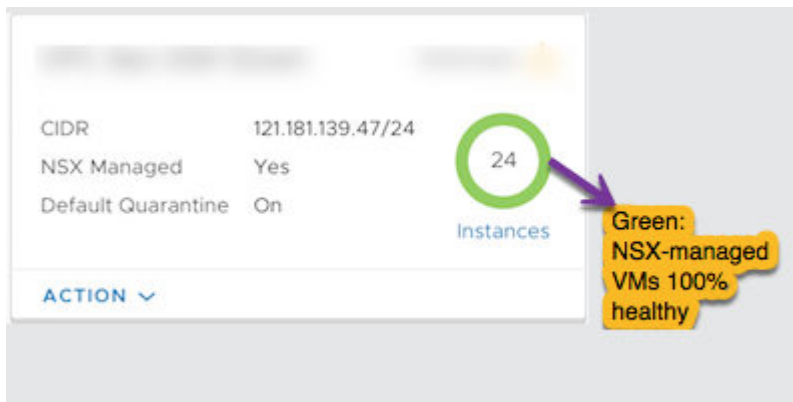


圖 16-2. 受 NSX Cloud 管理的虛擬機器有錯誤的 VNet

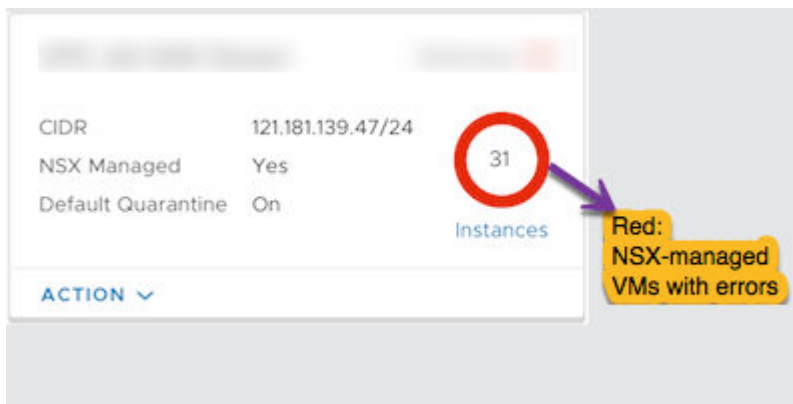


圖 16-3. 虛擬機器電源已關閉的 VNet

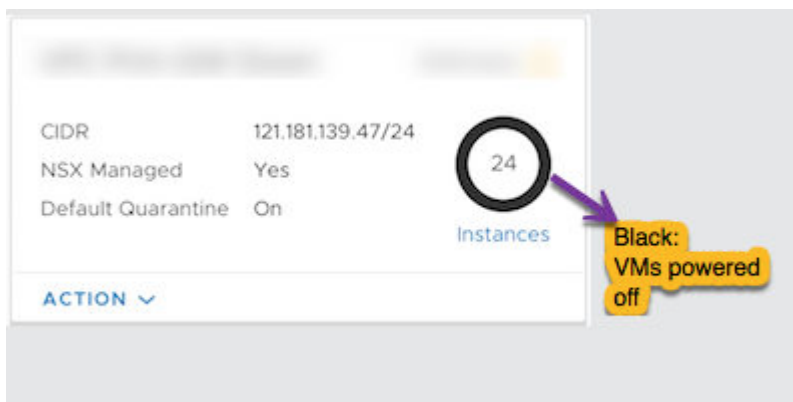


圖 16-4. 顯示 [預設隔離] 狀態的 VNet

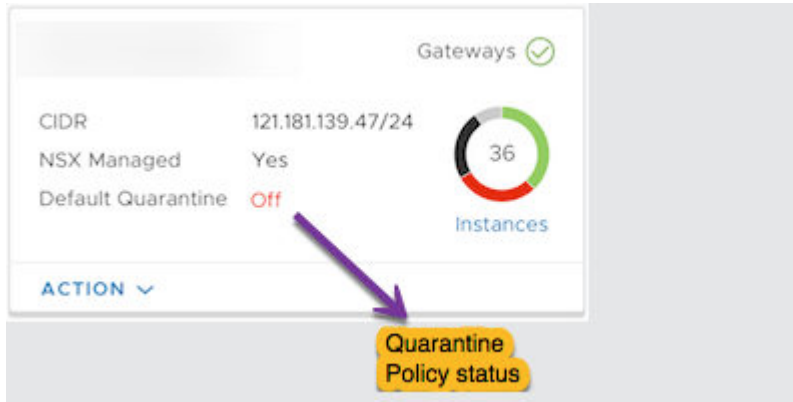
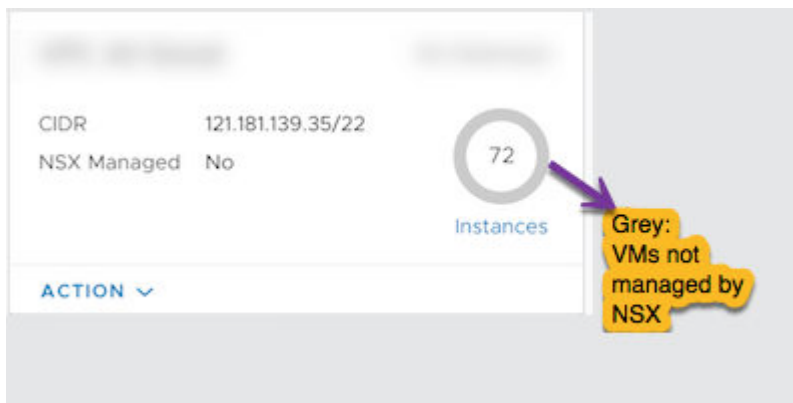


圖 16-5. 虛擬機器不受 NSX Cloud 管理的 VNet



執行個體

受管理的執行個體

圖 16-6. 受 NSX Cloud 管理的狀況良好的執行個體

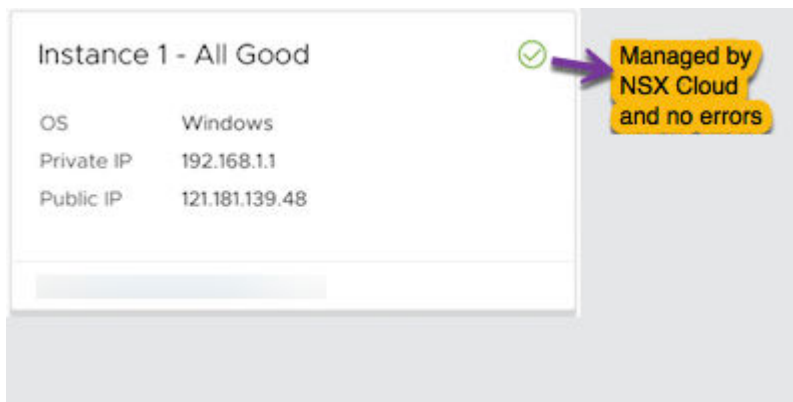


圖 16-7. 受 NSX Cloud 管理的有錯誤的執行個體

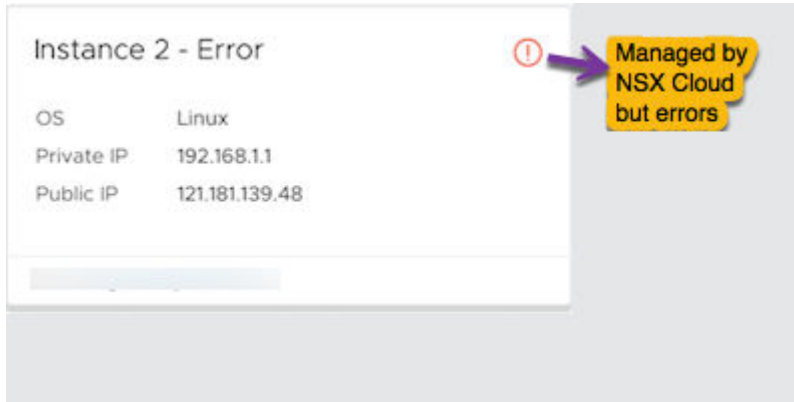


圖 16-8. 受 NSX Cloud 管理的有錯誤且已隔離的執行個體

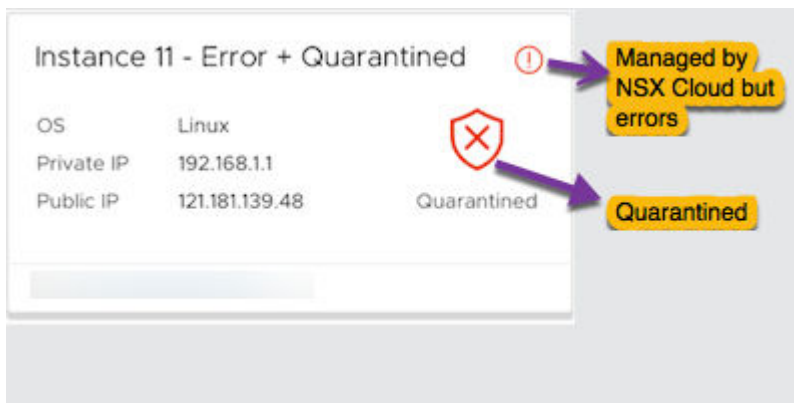


圖 16-9. 已隔離但透過套用 vm-override-sg 網路安全群組加入白名單之受 NSX Cloud 管理的執行個體

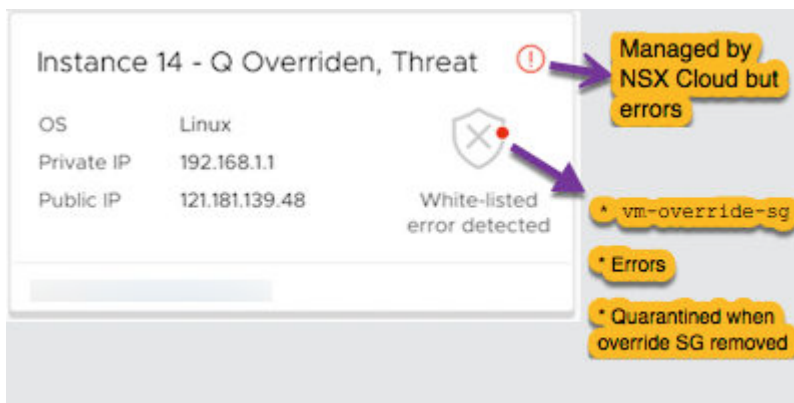
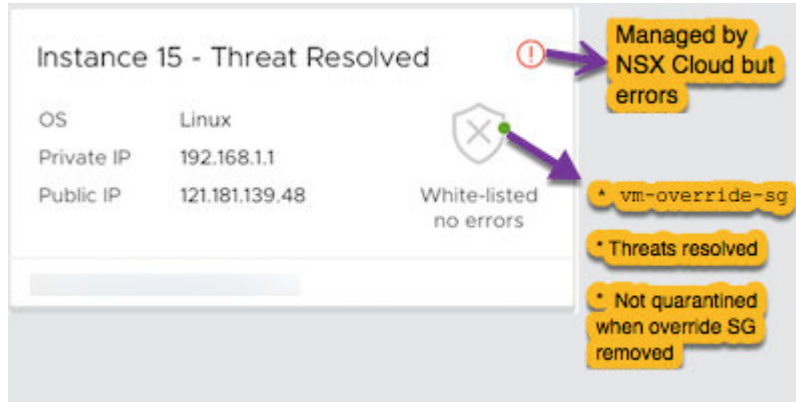


圖 16-10. 已隔離但已解決錯誤並加入白名單的受 NSX Cloud 管理的執行個體。



不受管理的執行個體

圖 16-11. 不受 NSX Cloud 管理且預設已隔離的虛擬機器

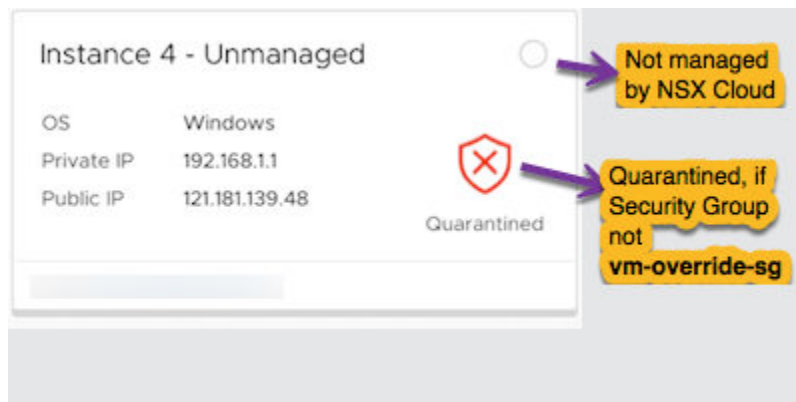
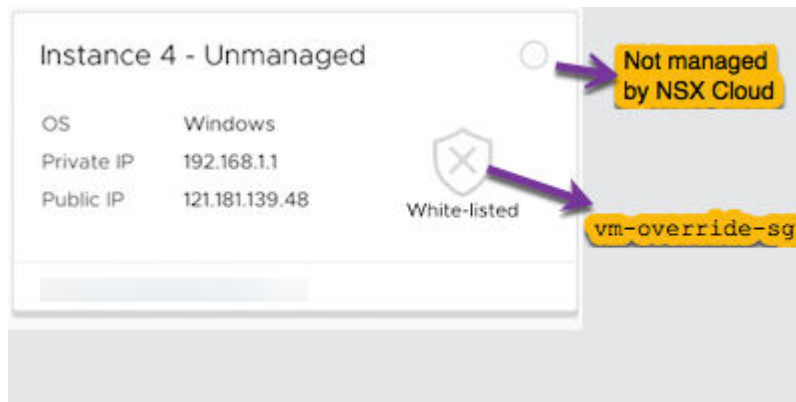


圖 16-12. 不受 NSX Cloud 管理但透過套用 vm-override-sg 加入白名單的虛擬機器



公用雲端閘道 (PCG)

圖 16-13. 主要和次要 PCG 皆開啟的 VNet

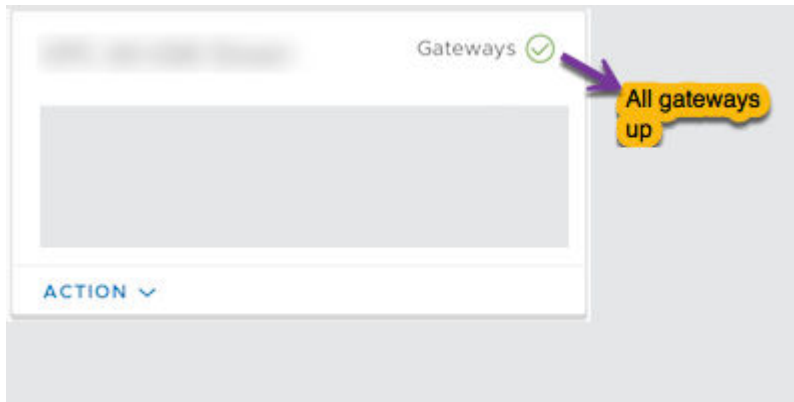


圖 16-14. 主要或次要 PCG 關閉的 VNet

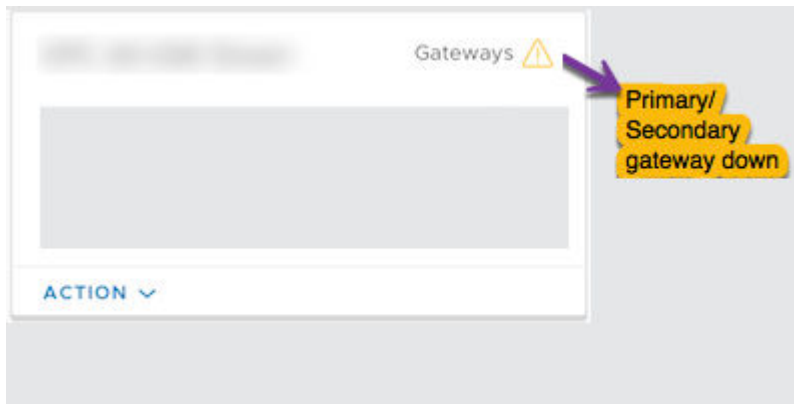
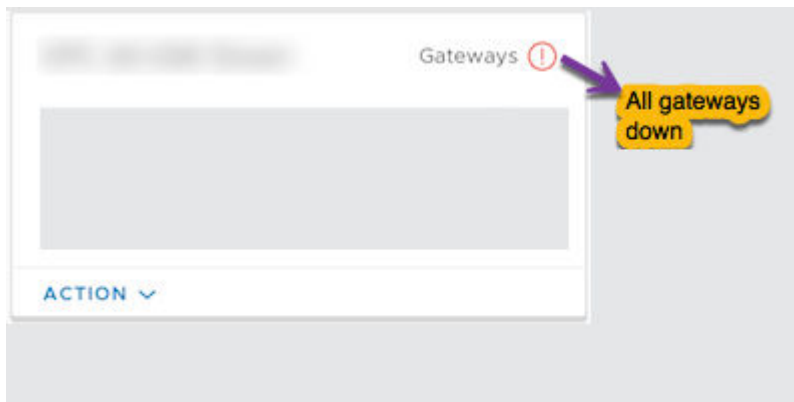


圖 16-15. 主要和次要 PCG 皆關閉的 VNet



系統

這些是系統下的區段：

系統 > 設定

當您安裝 CSM 時，先進行這些設定。之後可進行編輯。

將 CSM 加入 NSX Manager

您必須將 CSM 應用裝置與 NSX Manager 連線，才能讓這些元件彼此通訊。

必要條件

- 必須安裝 NSX Manager，且您必須擁有登入 NSX Manager 的管理員權限
- 必須安裝 CSM，且您必須擁有 CSM 中指派的企業管理員角色。

程序

- 1 開啟 NSX Manager 的 SSH 工作階段。
- 2 在 NSX Manager 上，執行 `get certificate api thumbprint` 命令。

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

此命令的輸出是對此 NSX Manager 而言唯一的數字字串。

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

備註 若使用首次安裝 CSM 時可用的 CSM 安裝精靈，您也可以提供這些詳細資料。

- 5 輸入 NSX Manager 的詳細資料。

選項	說明
NSX Manager 主機名稱	輸入 NSX Manager 的完整網域名稱 (FQDN) (如果有)。您也可以輸入 NSX Manager 的 IP 位址。
管理員認證	輸入具有企業管理員角色的使用者名稱和密碼。
管理員指紋	輸入您在步驟 2 中取得之 NSX Manager 的指紋值。

- 6 按一下**連線**。

CSM 會確認 NSX Manager 指紋並建立連線。

(選用) 設定 Proxy 伺服器

如果您想要透過可靠的 HTTP Proxy 路由和監控所有網際網路繫結的 HTTP/HTTPS 流量，您可以在 CSM 中設定最多五個 Proxy 伺服器。

來自 PCG 和 CSM 的所有公有雲通訊會透過所選 Proxy 伺服器進行路由。

PCG 的 Proxy 設定獨立於 CSM 的 Proxy 設定。您可以選擇 PCG 沒有任何 Proxy 伺服器或具有不同的 Proxy 伺服器。

您可以選擇以下層級的驗證：

- 認證式驗證。
- 適用於 HTTPS 攔截的憑證式驗證。
- 無驗證。

程序

- 1 按一下**系統 > 設定**。然後，在標題為 **Proxy 伺服器** 的面板上，按一下**設定**。

備註 若使用首次安裝 CSM 時可用的 CSM 安裝精靈，您也可以提供這些詳細資料。

- 2 在 [設定 Proxy 伺服器] 畫面中，輸入下列詳細資料：

選項	說明
預設值	使用此選項按鈕，表示預設 Proxy 伺服器。
設定檔名稱	提供 Proxy 伺服器設定檔名稱。這是強制性的。
Proxy 伺服器	輸入 Proxy 伺服器的 IP 位址。這是強制性的。
連接埠	輸入 Proxy 伺服器的連接埠。這是強制性的。
驗證	選擇性。如果您想要設定其他驗證，請選取此核取方塊，並提供有效的使用者名稱和密碼。
使用者名稱	如果您選取 [驗證] 核取方塊，這是必要的。
密碼	如果您選取 [驗證] 核取方塊，這是必要的。
憑證	選擇性。如果您想要提供適用於 HTTPS 攔截的驗證憑證，請選取此核取方塊，然後複製並貼上文字方塊中出現的憑證。
無 Proxy	如果您不想使用已設定的任何 Proxy 伺服器，請選取此選項。

系統 > 公用程式

可用公用程式如下。

備份和還原

遵循相同指示以備份和還原 CSM，與 NSX Manager 的方式相同。如需詳細資料，請參閱[備份和還原 NSX Manager](#)。

支援服務包

按一下**下載**，以擷取 CSM 的支援服務包。此項用於疑難排解。如需詳細資訊，請參閱《NSX-T Data Center 疑難排解指南》。

系統 > 使用者

使用角色型存取控制 (RBAC) 管理使用者。

如需詳細資料，請參閱[管理使用者帳戶和角色型存取控制](#)。

管理隔離原則

瞭解如何啟用或停用隔離原則，並瞭解對工作負載虛擬機器的影響。

NSX Cloud 使用公有雲安全群組進行威脅偵測。例如，啟用隔離原則時，如果帶惡意目的在受管理的虛擬機器上強制停止 NSX 代理程式，會使用 **quarantine** (在 Microsoft Azure 中) 或 **default** (在 AWS 中) 安全群組隔離遭受破壞的虛擬機器。

一般建議：

棕地部署開始為已停用：依預設會停用隔離原則。如果已在公有雲環境中設定虛擬機器，請使用隔離原則的已停用模式，直到工作負載虛擬機器上線。這可確保您現有的虛擬機器不會自動隔離。

綠地部署開始為已啟用：對於綠地部署，建議您啟用隔離原則，以允許虛擬機器的威脅偵測由 NSX Cloud 進行管理。

備註 啟用隔離原則時，在工作負載虛擬機器上套用 **vm_override_sg**，以便能夠使其上線，然後在受到 NSX Cloud 管理後移除此安全群組。適當的安全群組會在兩分鐘內套用到虛擬機器。

如何啟用或停用隔離原則

部署 PCG 時，您可以選擇開啟或關閉隔離原則。請遵循下列步驟，以隨後啟用或停用隔離原則。

必要條件

必須在 VPC 或 VNet 上部署一個或一對 PCG。

程序

- 登入 CSM 並移至您的公有雲：
 - 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下已部署且正在執行一個或一對 PCG 的 VPC。
 - 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。
- 使用下列任一動作啟用選項：

- 在動態磚視圖中，按一下**動作 > 編輯組態**。
- 如果您是在網絡視圖中，請選取 VPC 或 VNet 旁的核取方塊，然後按一下**動作 > 編輯組態**。

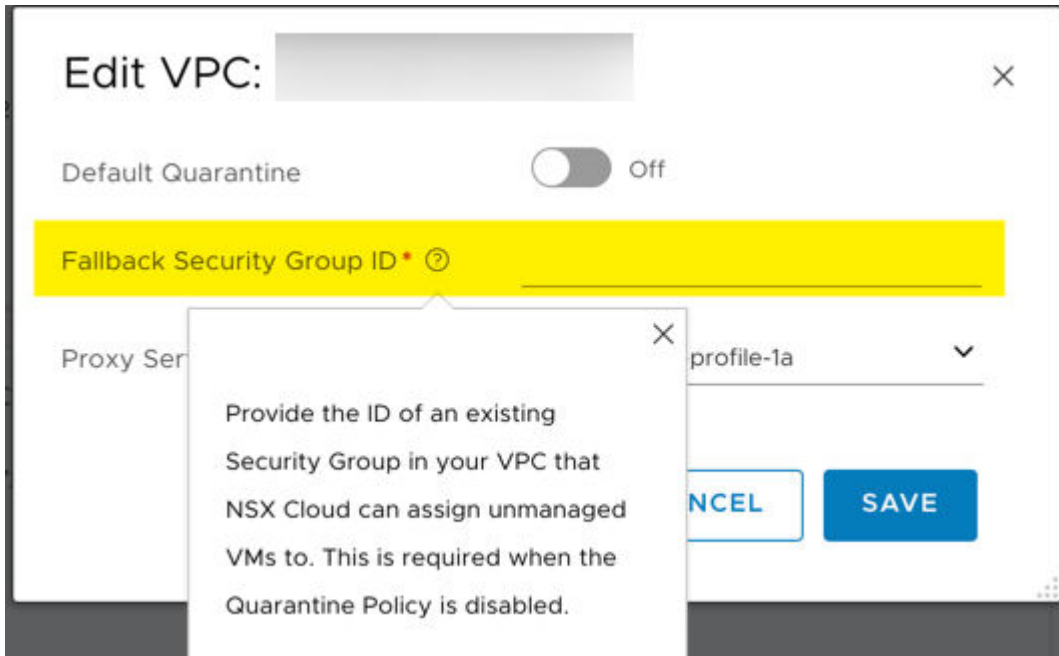


- 如果您是在 VPC 或 VNet 的頁面中，請按一下 [動作] 圖示，移至**編輯組態**。

- 開啟或關閉**預設隔離**以將其啟用或停用。

4 如果要停用隔離原則，您必須提供後援安全群組。

備註 後援安全群組必須是公有雲中現有的使用者定義的安全群組。您無法將任何 NSX Cloud 安全群組用作後援安全群組。請參閱 [公有雲的 NSX Cloud 安全群組](#)，以取得 NSX Cloud 安全群組的清單。



- 此 VPC 或 VNet 中的所有未受管理或隔離的虛擬機器，會在停用隔離原則時獲指派後援安全群組。
- 所有受管理的虛擬機器會保留 NSX Cloud 指派的安全群組。此類虛擬機器首次取消標記，並在停用隔離原則後變得未受管理時，它們也將獲指派後援安全群組。

5 按一下儲存。

停用時的隔離原則影響

隔離原則：已停用

停用隔離原則時：

- NSX Cloud 沒有將任何安全群組指派給此 VPC 或 VNet 中啟動的虛擬機器。您必須將適當的 NSX Cloud 安全群組指派給虛擬機器，才能啟用威脅偵測。

從 Microsoft Azure 入口網站或 AWS 主控台：

- ■ 將 vm-underlay-sg 指派給要使用由 Microsoft Azure 或 AWS 提供之底層網路的虛擬機器。

隔離原則：已啟用，然後停用

下表擷取了如果隔離原則已啟用然後停用，對安全群組指派的影響：

表 16-1. 停用隔離原則對安全群組的影響

虛擬機器-識別碼	受管理嗎?	安全群組	停用隔離原則後，虛擬機器的安全群組
虛擬機器 1	是	vm_underlay_sg	vm_underlay_sg .當您從此虛擬機器移除 <code>nsx.network</code> 標記以將其從 NSX 管理取出時，此虛擬機器還將獲指派後援安全群組。
虛擬機器 2	是	default (AWS) 或 quarantine (Microsoft Azure)	停用隔離原則時您指定的後援安全群組。如需詳細資料，請參閱 如何啟用或停用隔離原則 。
虛擬機器 3	否	vm_override_sg	停用隔離原則時您指定的後援安全群組。
虛擬機器 4	否	default (AWS) 或 quarantine (Microsoft Azure)	停用隔離原則時您指定的後援安全群組。

備註 取消部署 PCG 需要停用隔離原則。請參閱《NSX-T Data Center 安裝指南》中的〈取消部署 PCG〉，以取得詳細資料。

啟用時的隔離原則影響

隔離原則：已啟用

啟用隔離原則時：

- 針對屬於此 VPC 或 VNet 之任何工作負載虛擬機器的所有介面的安全群組 (SG) 或網路安全群組 (NSG) 指派均由 NSX Cloud 管理，如下所示：
 - 未受管理的虛擬機器獲指派 Microsoft Azure 中的 quarantine NSG 和 AWS 中的 default 安全群組，且遭到隔離。這會限制輸出流量，並停止此類虛擬機器的所有輸入流量。
 - 當您在虛擬機器上安裝 NSX 代理程式，並在公有雲中使用 `nsx.network` 進行標記時，未受管理的虛擬機器會變為 NSX 管理的虛擬機器。在預設情況下，NSX Cloud 將指派 vm-underlay-sg 以允許適當的輸入/輸出流量。
 - 如果在 NSX 管理的虛擬機器上偵測到威脅，例如，如果虛擬機器上的 NSX 代理程式已停止，則該虛擬機器仍可指派有 quarantine 或 default 安全群組並遭到隔離。
 - 對安全群組的任何手動變更都將在兩分鐘內還原為 NSX 決定的安全群組。

- 如果您想要將任何虛擬機器移出隔離所，請將 `vm-override-sg` 做為唯一的安全群組指派給此虛擬機器。NSX Cloud 不會自動變更 `vm-override-sg` 安全群組，並且允許 SSH 和 RDP 存取虛擬機器。移除 `vm-override-sg` 將再次導致虛擬機器安全群組還原為 NSX 決定的安全群組。

備註 啟用隔離原則時，將 `vm-override-sg` 指派給您的虛擬機器，然後在其上安裝 NSX 代理程式。執行安裝 NSX 代理程式並將虛擬機器標記為底層的程序後，從虛擬機器移除 `vm-override-sg` NSG。之後，NSX Cloud 將會自動指派適當的安全群組給 NSX 管理的虛擬機器。此步驟是必要的，因為它可確保在針對 NSX Cloud 準備時，虛擬機器未獲指派 `quarantine` 或 `default` 安全群組。

隔離原則：已停用，然後啟用

下表擷取了如果隔離原則已停用然後啟用，對安全群組指派的影響：

表 16-2. 啟用隔離原則對安全群組的影響

虛擬機器識別碼	受管理嗎？	偵測到威脅了嗎？	啟用隔離原則後的安全群組
虛擬機器 1	是	否	<code>vm_underlay_sg</code> 。
虛擬機器 2	是	是	<code>default</code> (AWS) 或 <code>quarantine</code> (Microsoft Azure)
備註 您可以手動將 <code>vm_override_sg</code> 指派給受管理的虛擬機器。這會讓它們離開隔離模式，且可以透過 SSH 或 RDP 存取此類虛擬機器，以修復此問題。請參閱 隔離原則：已啟用			
虛擬機器 3	否	不適用	<code>default</code> (AWS) 或 <code>quarantine</code> (Microsoft Azure)

公有雲的 NSX Cloud 安全群組

下列安全群組由 NSX Cloud 在 PCG 部署時建立：

gw 安全群組會套用到相應 PCG 介面。

表 16-3. 由 NSX Cloud 針對 PCG 介面建立的公有雲安全群組

安全群組名稱	在 Microsoft Azure 中可用嗎？	在 AWS 中可用嗎？	全名
<code>gw-mgmt-sg</code>	是	是	閘道管理安全群組
<code>gw-uplink-sg</code>	是	是	閘道上行安全群組
<code>gw-vtep-sg</code>	是	是	閘道下行安全群組

表 16-4. 由 NSX Cloud 針對工作負載虛擬機器建立的公有雲安全群組

安全群組名稱	在 Microsoft Azure 中可用嗎?	在 AWS 中可用嗎?	說明
隔離	是	否	針對 Microsoft Azure 隔離安全群組
預設	否	是	針對 AWS 隔離安全群組
vm-underlay-sg	是	是	虛擬機器非覆疊安全群組
vm-override-sg	是	是	虛擬機器覆寫安全群組
vm-overlay-sg	是	是	虛擬機器覆疊安全群組 (未在目前版本中使用)
vm-outbound-bypass-sg	是	是	虛擬機器輸出略過安全群組 (未在目前版本中使用)
vm-inbound-bypass-sg	是	是	虛擬機器輸入略過安全群組 (未在目前版本中使用)

工作負載虛擬機器上線及管理概觀

請參閱流程圖，瞭解您公有雲中的上線工作流程概觀。

如需 0 天工作流程，請參閱《NSX-T Data Center 安裝指南》中的〈[安裝 NSX Cloud 元件](#)〉。

支援的作業系統

這是針對您的工作負載虛擬機器，NSX Cloud 目前支援的作業系統清單。

目前支援下列作業系統：

備註 有關例外狀況，請參閱《NSX-T Data Center 版本說明》中的〈[NSX Cloud 已知問題](#)〉一節。

- Red Hat Enterprise Linux (RHEL) 7.2、7.3、7.4、7.5
- CentOS 7.2、7.3、7.4、7.5
- Oracle Enterprise Linux 7.2、7.3、7.4 (Unbreakable Enterprise Kernel 版本不受支援)。

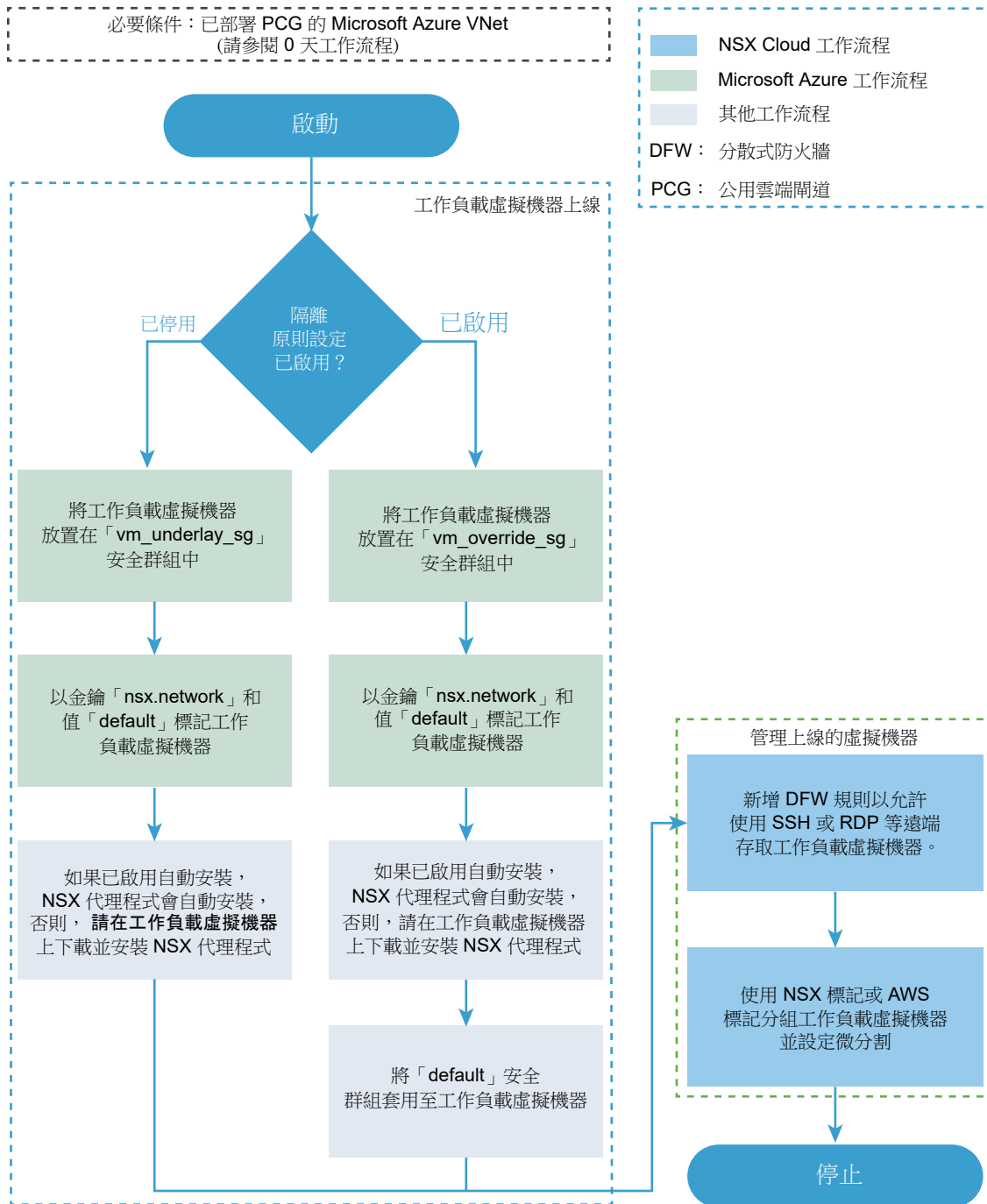
備註 Oracle Enterprise Linux、Red Hat Enterprise Linux 和 CentOS 不支援 SE Linux

- Ubuntu 14.04、16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Sever 2016

如何從 Microsoft Azure 將工作負載虛擬機器上線

請參閱此流程圖，以瞭解從 Microsoft Azure 將工作負載虛擬機器上線所涉及的步驟概觀。

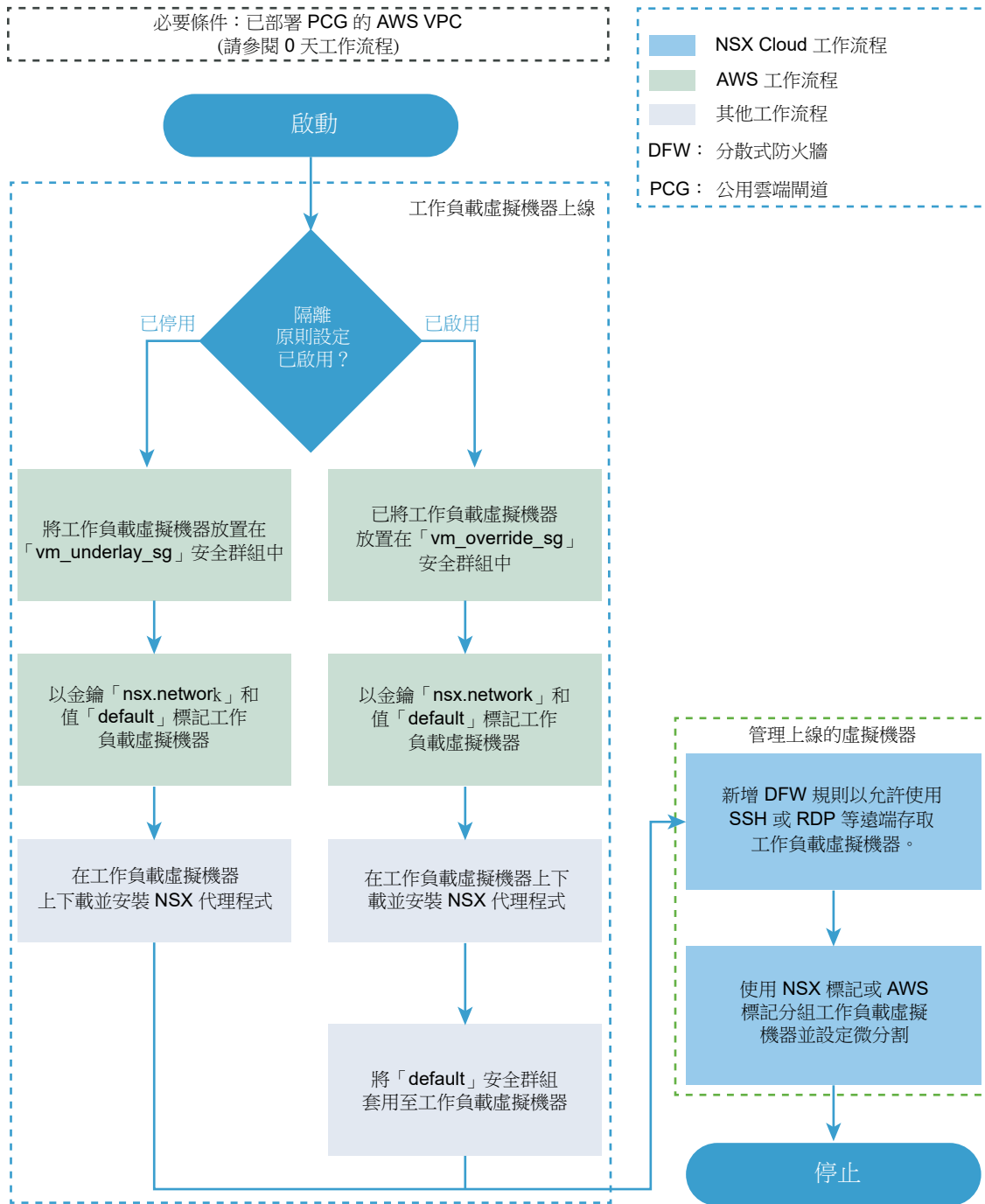
圖 16-16. Microsoft Azure 的 N 天上線工作流程



如何從 AWS 將工作負載虛擬機器上線

請參閱此流程圖，以瞭解從 **AWS** 將工作負載虛擬機器上線所涉及的步驟概觀。

圖 16-17. AWS 的 N 天上線工作流程



工作負載虛擬機器上線

將工作負載虛擬機器上線，並開始使用 NSX-T Data Center 加以管理。

標記公有雲中的虛擬機器

將 **nsx.network** 標記套用至您想要使用 NSX-T Data Center 管理的虛擬機器。

必要條件

主控工作負載虛擬機器的 VPC 或 VNet 必須透過 NSX Cloud 上線。請參閱《NSX-T Data Center 安裝指南》中的〈[新增公有雲詳細目錄](#)〉，以取得詳細資料。

程序

- 1 登入公有雲帳戶，並移至已透過 NSX Cloud 上線的 VPC 或 VNet。
- 2 選取您想要使用 NSX-T Data Center 管理的虛擬機器。
- 3 新增虛擬機器的下列標記詳細資料，並儲存變更。

```
Name: nsx.network
Value: default
```

備註 您可以在虛擬機器層級或介面層級套用此標籤，效果是一樣的。

範例

後續步驟

在這些虛擬機器上安裝 NSX 代理程式。請參閱[安裝 NSX 代理程式](#)。

如果使用 Microsoft Azure，您可以選擇在標記的虛擬機器上自動安裝 NSX 代理程式。如需詳細資料，請參閱[自動安裝 NSX 代理程式](#)。

安裝 NSX 代理程式

在工作負載虛擬機器上安裝 NSX 代理程式

在 Windows 虛擬機器上安裝 NSX 代理程式

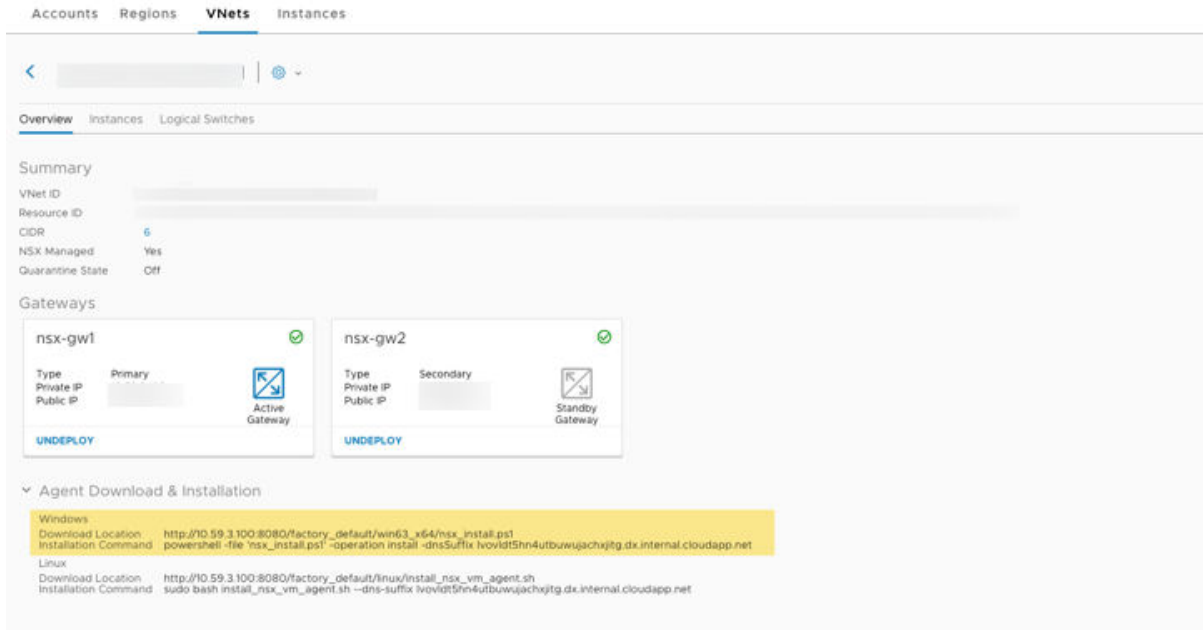
請依照下列指示，在 Windows 工作負載虛擬機器上安裝 NSX 代理程式。

如需目前支援的 Microsoft Windows 版本的清單，請參閱[支援的作業系統](#)。

程序

- 1 登入 CSM 並移至您的公有雲：
 - a 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下已部署且正在執行一個或一對 PCG 的 VPC。
 - b 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。

- 2 從畫面的代理程式下載與安裝區段中，記下位於 **Windows** 下的下載位置和安裝命令。



備註 安裝命令中的 DNS 尾碼會動態產生，以符合部署 PCG 時所選擇的 DNS 設定。

- 3 以管理員身分連線至 Windows 工作負載虛擬機器。
- 4 在 Windows 虛擬機器上，從您從 CSM 記下的下載位置下載安裝指令碼。您可以使用任何瀏覽器 (例如 Internet Explorer)，下載指令碼。指令碼會下載到您的瀏覽器預設下載目錄中，例如 C:\Downloads。
- 5 開啟 PowerShell 提示字元，並移至包含已下載指令碼的目錄。
- 6 使用您從 CSM 記下的安裝命令執行已下載的指令碼。

例如：

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

備註 檔案引數需要完整路徑，除非位於相同的目錄或 PowerShell 指令碼已在路徑中。例如，如果將指令碼下載到 C:\Downloads，但您目前不在該目錄中，則指令碼必須包含位置：*powershell -file 'C:\Downloads\nsx_install.ps1' ...*

- 7 指令碼隨即執行，完成後會顯示訊息，指示 NSX 代理程式是否已成功安裝。

備註 指令碼會將主要網路介面視為預設值。

如需所有指令碼選項的清單和解除安裝指示，請參閱適用於 Windows 虛擬機器的 NSX 代理程式安裝指令碼選項。

後續步驟

管理工作負載虛擬機器

在 Linux 虛擬機器上安裝 NSX 代理程式

請依照下列指示，在 Linux 工作負載虛擬機器上安裝 NSX 代理程式。

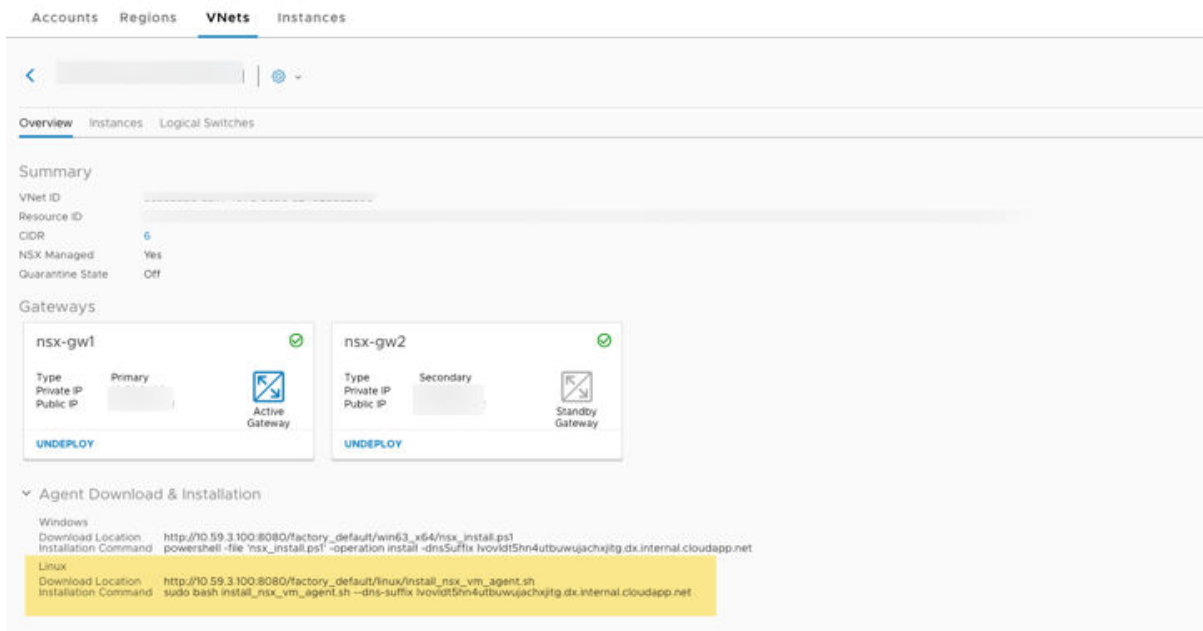
如需目前支援的 Linux 散發清單，請參閱[支援的作業系統](#)。

必要條件

您需要 **wget** 和 **nslookup** 命令以執行 NSX 代理程式安裝指令碼。

程序

- 登入 CSM 並移至您的公有雲：
 - 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下已部署且正在執行一個或一對 PCG 的 VPC。
 - 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。
- 從畫面的**代理程式下載與安裝**區段中，記下位於 **Linux** 下的**下載位置**和**安裝命令**。



備註 安裝命令中的 DNS 尾碼會動態產生，以符合部署 PCG 時所選擇的 DNS 設定。

- 使用超級使用者權限登入 Linux 工作負載虛擬機器。
- 在 Linux 虛擬機器上使用 **wget** 或同等命令，從您從 CSM 記下的**下載位置**下載安裝指令碼。安裝指令碼會下載到執行 **wget** 命令所在的目錄中。
- 變更安裝指令碼的權限，使其成為可執行檔 (如有需要) 並加以執行：

```
$ sudo chmod +x install_nsx_vm_agent.sh
$ sudo bash install_nsx_vm_agent.sh --dns-suffix <>
```

附註：在 Red Hat Enterprise Linux 及其衍生物上，不支援 SELinux。停用 SELinux 以安裝 NSX 代理程式。

- 6 在 NSX 代理程式安裝開始後，與 Linux 虛擬機器中斷連線。畫面上會顯示如下的訊息：
Installation completed!!! Starting NSX Agent service. SSH connection will now be lost.。重新連線至您的虛擬機器，以完成上線程序。

結果

工作負載虛擬機器上已安裝 NSX 代理程式。

備註

- NSX 代理程式成功安裝後，虛擬機器上的連接埠 8888 會顯示為開啟，但在底層模式下已針對虛擬機器封鎖此連接埠，應僅在進階疑難排解需要時使用此連接埠。
- 指令碼會將 eth0 用作預設介面。如需指令碼選項的清單和解除安裝指示，請參閱適用於 Linux 虛擬機器的 NSX 代理程式安裝指令碼選項

後續步驟

[管理工作負載虛擬機器](#)

NSX 代理程式安裝指令碼選項和解除安裝

NSX 代理程式安裝指令碼提供可設定的選項。下表列出了這些選項。

適用於 Windows 虛擬機器的 NSX 代理程式安裝指令碼選項

表 16-5.

選項	說明
<code>--gateway <ip dns></code>	<p>NSX Public Cloud Gateway IP 或 DNS 名稱。</p> <p>如果您想要使用 PCG 的 IP 位址，請指定此選項。未指定此參數時，會使用 PCG 的預設 DNS 名稱。</p> <ul style="list-style-type: none"> ■ AWS 中的 PCG DNS 名稱：nsx-gw.vmware.local ■ Microsoft Azure 中的 PCG DNS 名稱：nsx-gw <p>備註 在 PCG 的 HA 模式下，為「--gateway」選項指定兩個 PCG 名稱，例如，在 Microsoft Azure 虛擬機器中：--gateway "nsx-gw1;nsx-gw2"</p>
<code>--noStart true</code>	<p>在虛擬機器上安裝 NSX 代理程式後，您可以建立該虛擬機器的 VHD。使用此選項執行安裝指令碼。然後，從 Microsoft Azure 入口網站，建立該虛擬機器的 VHD。</p>
<code>--downloadPath <path></code>	<p>這是應下載檔案的目錄路徑。如果路徑中包含逸出字元，請用單引號將其括住。</p> <p>預設值 = %temp%</p>
<code>--silentInstall <true/false></code>	<p>如果設為 true，指令碼會執行無訊息安裝。</p> <p>預設值為 false</p>

表 16-5. (續)

選項	說明
<code>-noSigCheck <true/false></code>	這可讓您指定是否檢查二進位檔上的簽章。 預設值 = <code>false</code>
<code>-logLevel <value></code>	這可讓您指定 NSX 元件的記錄層級 預設值 = 1 詳細資訊 = 3
<code>-operation <install/uninstall></code>	這可讓您指定要執行的作業: <code>install</code> 或 <code>uninstall</code> 預設值 = <code>install</code>
<code>-bundlePath <path></code>	這可讓您指定 NSX 虛擬機器代理程式服務包的本機路徑 預設選項是從 PCG 下載服務包。

從 Windows 虛擬機器解除安裝 NSX 代理程式

- 1 使用 RDP 遠端登入虛擬機器。
- 2 使用解除安裝選項執行安裝指令碼：

```
\nsx_install.ps1 -operation uninstall
```

適用於 Linux 虛擬機器的 NSX 代理程式安裝指令碼選項

表 16-6.

選項	說明
<code>--gateway <ip dns></code>	NSX Public Cloud Gateway IP 或 DNS 名稱。 如果您想要使用 PCG 的 IP 位址，請指定此選項。未指定此參數時，會使用 PCG 的預設 DNS 名稱。 <ul style="list-style-type: none"> ■ AWS 中的 PCG DNS 名稱: <code>nsx-gw.vmware.local</code> ■ Microsoft Azure 中的 PCG DNS 名稱: <code>nsx-gw</code> <p>備註 在 PCG 的 HA 模式下，為「<code>--gateway</code>」選項指定兩個 PCG 名稱，例如，在 Microsoft Azure 虛擬機器中：<code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--no-start</code>	在虛擬機器上安裝 NSX 代理程式後，您可以建立該虛擬機器的 VHD。使用此選項執行安裝指令碼。然後，從 Microsoft Azure 入口網站，建立該虛擬機器的 VHD。
<code>--uninstall</code>	使用此選項執行指令碼，以解除安裝 NSX 代理程式。

自動安裝 NSX 代理程式

目前僅 Microsoft Azure 支援。

在 Microsoft Azure 中滿足下列準則時，會自動安裝 NSX 代理程式：

- 在新增至 NSX Cloud 的 VNet 中的虛擬機器上安裝有 Azure 虛擬機器延伸。請參閱[有關虛擬機器延伸的 Microsoft Azure 說明文件](#)，以取得詳細資料。
- 已使用 `nsx.network` 和值 `default` 標記虛擬機器。

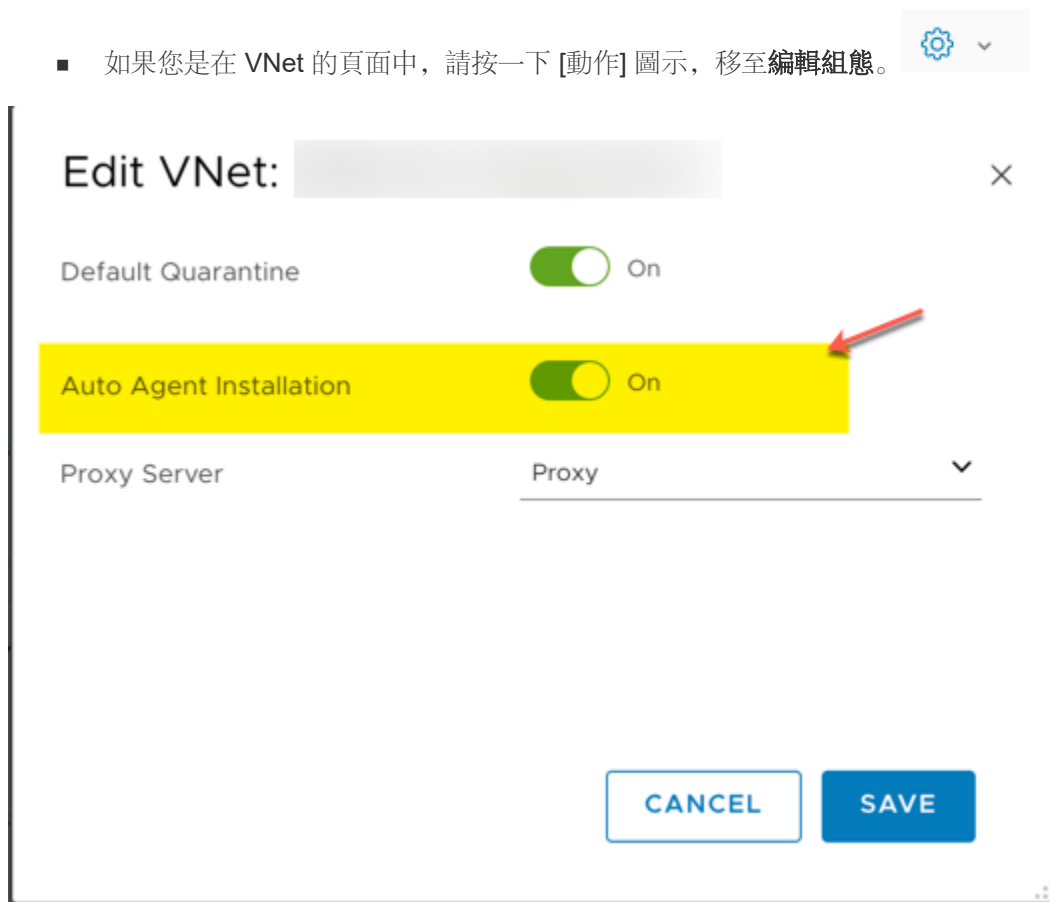
啟用此功能：

- 1 移至雲端 > Azure > VNet。
- 2 選取您想要在其虛擬機器上自動安裝 NSX 代理程式的 VNet。
- 3 使用下列任一動作啟用選項：

- 在動態磚視圖中，按一下動作 > 編輯組態。
- 如果您是在網格視圖中，請選取 VNet 旁的核取方塊，然後按一下動作 > 編輯組態。



- 如果您是在 VNet 的頁面中，請按一下 [動作] 圖示，移至編輯組態。



管理工作負載虛擬機器

成功將工作負載虛擬機器上線後，您可以使用 NSX-T Data Center 進行管理。

存取受管理的工作負載虛擬機器

請依照此工作流程，在底層模式下存取受管理的虛擬機器。

在 VPC 或 VNet 上部署 PCG 時，NSX Cloud 會建立預設防火牆規則，以增強工作負載虛擬機器的安全性。

若要在底層模式下存取受管理的工作負載虛擬機器，您需要新增開啟虛擬機器之存取權的 **Distributed Firewall (DFW)** 規則。

執行下列操作：

- 1 開啟 NSX Manager 主控台。
- 2 移至**防火牆 > 一般 > 新增規則**
- 3 新增具有下列組態的規則。如需詳細指示，請參閱[新增防火牆規則](#)。

表 16-7.

選項	說明
名稱	提供名稱以定義此規則的用途，例如 AllowRemoteAccessToUnderlay 。
來源	選擇 任何 。
目的地	選擇此虛擬機器已連結或所屬的邏輯交換器、連接埠或 NSGroup。
服務	選擇此工作負載虛擬機器的遠端存取服務，例如，適用於 Linux 的 SSH，或適用於 Windows 的 RDP。
動作	選擇 允許 。

使用 NSX-T Data Center 和公有雲標記分組虛擬機器

NSX Cloud 可讓您使用指派給工作負載虛擬機器的公有雲標籤。

NSX Manager 會使用標籤分組虛擬機器，公有雲亦是如此。因此，若要促進虛擬機器分組，NSX Cloud 會將套用到工作負載虛擬機器的公有雲標記提取至 NSX Manager，前提是這些標記符合預先定義的大小和保留字準則。

標籤術語

NSX Manager 中的**標籤**是指公有雲內容中的**值**。公有雲標籤的**金鑰**在 NSX Manager 中稱為**範圍**。

NSX Manager 中 在 NSX Manager 中	公有雲中 標籤的對等元件
範圍	金鑰
標籤	值

標籤類型和限制

NSX Cloud 針對 NSX 管理的公有雲虛擬機器允許三種類型的標籤。

- **系統標籤：**這些標籤是系統定義的標籤，您無法新增、編輯或刪除這些標籤。NSX Cloud 會使用下列系統標記：
 - azure:subscription_id

- azure:region
 - azure:vm_rg
 - azure:vnet_name
 - azure:vnet_rg
 - aws:vpc
 - aws:availabilityzone
- **探索到的標籤：**已新增至公有雲中的虛擬機器的標籤將由 NSX Cloud 自動探索，這些標籤會針對 NSX Manager 詳細目錄中的工作負載虛擬機器顯示。這些標籤無法從 NSX Manager 內進行編輯。探索到的標籤數目沒有限制。這些標籤以 **dis:azure:** 做為前置詞，表示標籤是從 Microsoft Azure 探索到的。

當您對公有雲中的標籤進行任何變更時，這些變更會在兩分鐘內反映在 NSX Manager 中。

依預設啟用此功能。您可以在新增 Microsoft Azure 訂閱或 AWS 帳戶時，啟用或停用 Microsoft Azure 或 AWS 標記探索。

- **使用者標籤：**您可以建立最多 25 個使用者標籤。您具有使用者標籤的新增、編輯、刪除權限。如需管理使用者標記的相關資訊，請參閱[管理虛擬機器的標記](#)。

表 16-8. 標籤類型和限制的摘要

標籤類型	標籤範圍或預先決定的前置詞	限制	企業管理員權限	稽核員權限
系統定義	完整的系統標籤： <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availabilityzone 	範圍 (金鑰): 20 個字元 標籤 (值): 65 個字元 可能的上限: 5	唯讀	唯讀
探索到	從您的 VNet 匯入之 Microsoft Azure 標籤的前置詞: dis:azure: 從您的 VPC 匯入之 AWS 標記的前置詞: dis:aws:	範圍 (金鑰): 20 個字元 標籤 (值): 65 個字元 允許的上限: 無限制 備註 字元限制排除前置詞 dis:<公有雲名稱> 。超過這些限制的標籤不會反映在 NSX Manager 中。 前置詞為 nsx 的標籤將被忽略。	唯讀	唯讀
使用者	使用者標籤可包含允許的字元數目內的任何範圍 (金鑰) 和值, 除了: <ul style="list-style-type: none"> ■ 範圍 (金鑰) 前置詞 dis:azure: 或 dis:aws: ■ 與系統標籤相同的範圍 (金鑰) 	範圍 (金鑰): 30 個字元 標籤 (值): 65 個字元 允許的上限: 25	新增/編輯/刪除	唯讀

探索到的標籤範例

備註 公有雲的標籤格式為 **key=value**, 而 NSX Manager 的標籤格式為 **scope=tag**。

表 16-9.

工作負載虛擬機器的公有雲標記	由 NSX Cloud 探索到?	工作負載虛擬機器的對等 NSX Manager 標籤
Name=Developer	是	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	是	dis:azure:ValidDisTagKeyLength=ValidDisTagValue

表 16-9. (續)

工作負載虛擬機器的公有雲標記	由 NSX Cloud 探索到?	工作負載虛擬機器的對等 NSX Manager 標籤
Abcdefghijklmnopqrstuvwxyz=value2	否 (金鑰超過 20 個字元)	無
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgijuytreswqacvbcdefghijklmnopqrstuvwxyz	否 (值超過 65 個字元)	無
nsx.name=Tester	否 (金鑰具有前置詞 nsx)	無

如何在 NSX Manager 中使用標籤

- 請參閱[管理虛擬機器的標記](#)。
- 請參閱[搜尋物件](#)。
- 請參閱[針對工作負載虛擬機器設定微分割](#)。

針對工作負載虛擬機器設定微分割

您可以針對受管理的工作負載虛擬機器設定微分割。

執行下列作業，以將 Distributed Firewall 規則套用至上線的工作負載虛擬機器：

- 1 使用虛擬機器名稱或標籤或其他成員資格準則建立 NSGroup，例如，針對 **web**、**app**、**DB** 層。如需相關指示，請參閱 [建立 NSGroup](#)。

備註 您可以針對成員資格準則使用下列任何標籤。如需詳細資料，請參閱[使用 NSX-T Data Center 和公有雲標記分組虛擬機器](#)。

- 系統定義的標籤
- 由 NSX Cloud 探索到的 VPC 或 VNet 中的標記
- 或您自己的自訂標籤

- 2 建立防火牆規則區段，並套用至 NSgroup (如有需要)。請參閱[新增防火牆規則區段](#)。
- 3 根據安全性原則的需求，建立防火牆規則，並將 NSGroup 用於來源和目的地。請參閱[新增防火牆規則](#)。

從 CSM 手動重新同步詳細目錄時，或大約在變更從公有雲提取到 CSM 後的兩分鐘內，此微分割會生效。

如何搭配使用 NSX-T Data Center 功能與公有雲

NSX Cloud 為公有雲建立網路拓撲，您不得編輯或刪除自動產生的 NSX-T Data Center 邏輯實體。

使用此清單做為快速參考，以瞭解哪些是自動產生的，以及在套用至公有雲時應如何使用 NSX-T Data Center 功能。

NSX Manager 組態

將在 NSX Manager 中自動建立下列實體：

重要 請勿編輯或刪除任何這些自動建立的實體。

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

備註 雖然已建立 DHCP 設定檔，但在目前版本中不受支援，因為它用於覆疊網路。

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

備註 這些 DFW 規則封鎖所有流量，並且需要根據特定需求進行調整。

確認 NSX Manager 中的下列組態：

- 1 從 NSX Cloud 儀表板中，按一下 **NSX Manager**。
- 2 移至**網狀架構 > 節點 > Edge**。您應該會看到 **PCG-<your-VPC-or-VNet-name>** 做為 Edge 節點。

備註 確認部署狀態、管理程式連線和控制器連線均已連線 (狀態顯示**開啟**並具有綠色的點)。

- 3 瀏覽至**網狀架構 > 節點 > Edge 叢集**，以確認已新增 **PCG-Cluster-<your-VPC-or-VNet-name>**。
- 4 瀏覽至**網狀架構 > 節點 > 傳輸節點**，以確認 PCG 已做為傳輸節點登錄，並且已連線到部署 PCG 時自動建立的兩個傳輸區域：
 - 流量類型 VLAN -- 此項連線至 PCG 上行
 - 流量類型覆疊 -- 此項用於覆疊邏輯網路

備註 目前版本不支援覆疊。

5 確認是否已建立邏輯交換器和第 0 層邏輯路由器，並且邏輯路由器已新增至 Edge 叢集。

- 移至**網路 > 交換 > 交換器**。您應該會看到 **DefaultSwitch-Overlay-<your-VPC-or-VNet-name>** 和 **DefaultSwitch-VLAN-<your-VPC-or-VNet-name>** 交換器已自動建立。
- 移至**網路 > 路由 > 路由器**。您應該會看到 **PCG-Tier0-LR-<your-VPC-or-VNet-name>** 路由器已自動建立。

邏輯交換常見問題集

表 16-10.

問題	回答
部署 PCG 時，NSX Cloud 會建立任何預設交換器嗎？	是。NSX Cloud 為您部署 PCG 所在的每個 VPC 或 VNet 建立兩個預設交換器。交換器命名格式如下所示： DefaultSwitch-Overlay-<vpc-or-vnet-name> DefaultSwitch-VLAN-<vpc-or-vnet-name>
除了 NSX Cloud 所建立的預設邏輯交換器，我可以建立 VLAN 邏輯交換器嗎？	否。請勿建立 VLAN 邏輯交換器。
我可以編輯或刪除 NSX Cloud 建立的預設邏輯交換器嗎？	UI 可讓您編輯或刪除預設邏輯實體，但是，請勿編輯或刪除 NSX Cloud 自動建立的任何項目。
我應建立連接埠嗎？	否。您不需要建立任何連接埠。NSX Cloud 在您標記 AWS 或 Microsoft Azure 中的虛擬機器時建立連接埠。請勿編輯或刪除 NSX Cloud 自動建立的任何連接埠。
我應建立交換設定檔嗎？	否。您不需要建立任何交換設定檔。使用 PublicCloud-Global-SpoofGuardProfile 。請勿編輯或刪除預設交換設定檔。
在哪可以找到邏輯交換器的詳細資訊？	請參閱第 1 章 邏輯交換器與設定虛擬機器連結 。

邏輯路由器常見問題集

表 16-11.

問題	回答
部署 PCG 時，NSX Cloud 會自動建立邏輯路由器嗎？	是。在 VPC 或 VNet 上部署 PCG 時，NSX Cloud 會自動建立第 0 層邏輯路由器。
在哪可以找到邏輯路由器的詳細資訊？	請參閱第 5 章 第 0 層邏輯路由器 。

IPFIX 常見問題集

表 16-12.

問題	回答
針對要在公有雲中使用的 IPFIX，需要任何特定組態嗎？	<p>是。</p> <ul style="list-style-type: none"> ■ NSX Cloud 僅在 UDP 連接埠 4739 上支援 IPFIX。 ■ 收集器必須與已套用 IPFIX 設定檔的虛擬機器位於同一個 VPC 或 VNet 中。 ■ 交換器和 DFW IPFIX：如果收集器與已套用 IPFIX 設定檔的 Windows 虛擬機器位於同一個子網路，在 Windows 虛擬機器上需要收集器的靜態 ARP 項目，因為如果找不到任何 ARP 項目，Windows 會以無訊息方式捨棄 UDP 封包。
在哪可以找到 IPFIX 的詳細資訊？	請參閱 設定 IPFIX 。

連接埠鏡像常見問題集

表 16-13.

問題	回答
針對公有雲中的連接埠鏡像，需要任何特定組態嗎？	<p>只有目前版本中的 AWS 支援連接埠鏡像。</p> <ul style="list-style-type: none"> ■ 對於 NSX Cloud，從工具 > 連接埠鏡像工作階段設定連接埠鏡像。 ■ 僅支援 L3SPAN 連接埠鏡像。 ■ 收集器必須與來源工作負載虛擬機器位於同一個 VPC 中。
在哪可以找到連接埠鏡像的詳細資訊？	請參閱 監控連接埠鏡像工作階段 。

其他常見問題集

表 16-14.

問題	回答
我套用到公有雲中的工作負載虛擬機器的標記在 NSX-T Data Center 中是否可用？	是。如需詳細資料，請參閱 使用 NSX-T Data Center 和公有雲標記分組虛擬機器 。
如何針對受 NSX-T Data Center 管理的工作負載虛擬機器設定微分割？	請參閱 針對工作負載虛擬機器設定微分割 。

使用進階 NSX Cloud 功能

啟用 Syslog 轉送

NSX Cloud 支援 Syslog 轉送。

您可以在受管理虛擬機器上針對 Distributed Firewall (DFW) 封包啟用 Syslog 轉送。如需詳細資料，請參閱《NSX-T Data Center 疑難排解指南》中的[設定遠端記錄](#)。

執行下列操作：

程序

- 1 使用跳躍主機登入 PCG。
- 2 輸入 **nsxcli** 以開啟 NSX-T Data Center CLI。
- 3 輸入下列命令以啟用 DFW 記錄轉送：

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info messageid
FIREWALL-PKTLOG
```

此設定之後，NSX 代理程式 DFW 封包記錄會在 PCG 上的 `/var/log/syslog` 下提供。

- 4 若要針對每個虛擬機器啟用記錄轉送，請輸入下列命令：

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

疑難排解

瞭解 NSX Cloud 提供的驗證和疑難排解選項。

確認 NSX Cloud 元件

最佳做法是在生產環境中部署之前，確認所有元件均已啟動且正在執行。

確認 NSX 代理程式是否已連線至 PCG

若要確認您工作負載虛擬機器上的 NSX 代理程式已連線至 PCG，請執行以下作業：

- 1 輸入 **nsxcli** 命令以開啟 NSX-T Data Center CLI。
- 2 輸入下列命令來取得閘道連線狀態，例如：

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

驗證虛擬機器的介面/網路模式

驗證安裝 NSX 代理程式的介面，如下所示：

- 1 輸入 **nsxcli** 命令以開啟 NSX-T Data Center CLI。
- 2 輸入命令以檢視切換模式，例如：

```
get vm-network-mode
VM-Network-Mode : underlay Interface : eth0
```

在 AWS 或 Microsoft Azure 中驗證虛擬機器介面標記

工作負載虛擬機器必須具有正確的標記才能連線至 PCG。

- 1 登入 AWS 主控台或 Microsoft Azure 入口網站。

2 驗證虛擬機器的 eth0 或介面標記。

`nsx.network` 金鑰必須具有值 `default`。

疑難排解常見問題集

以下列出了一些常見問題。

我已正確標記自己的虛擬機器並且安裝了代理程式，但我的虛擬機器被隔離。我該怎麼辦？

如果您遇到此問題，請嘗試下列作業：

- 檢查 NSX Cloud 標記 `nsx.managed` 及其值 `default` 是否已正確輸入。這區分大小寫。
- 從 CSM 重新同步 AWS 或 Microsoft Azure 帳戶：
 - 登入 CSM。
 - 移至雲端 > AWS/Azure > 帳戶。
 - 從公有雲帳戶動態磚按一下動作，然後按一下重新同步帳戶。

如果無法存取我的工作負載虛擬機器，該怎麼辦？

在某些罕見情況下，與受管理的 Linux 或 Windows 工作負載虛擬機器的連線可能會中斷。請嘗試下列步驟：

從公有雲 (AWS 或 Microsoft Azure)

- 若要允許流量，請確保已正確設定虛擬機器上的所有連接埠，包括受 NSX Cloud 管理的連接埠、作業系統防火牆 (Microsoft Windows 或 IPTables) 和 NSX-T Data Center。

例如，若要允許對虛擬機器 ping，必須正確設定下列內容：

- AWS 或 Microsoft Azure 上的安全群組。如需詳細資訊，請參閱[管理隔離原則](#)。
- NSX-T Data Center DFW 規則。如需詳細資料，請參閱[存取受管理的工作負載虛擬機器](#)。
- Linux 上的 Windows 防火牆或 IPTables。
- 嘗試使用 SSH 或其他方法登入虛擬機器以解決問題，例如，Microsoft Azure 中的序列主控台。
- 您可以將已鎖定的虛擬機器重新開機。
- 如果仍無法存取虛擬機器，請接著將次要 NIC 連結至從中存取該工作負載虛擬機器的工作負載虛擬機器。

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 Data Center** 基礎結構一部分的應用裝置以及由 **NSX-T Data Center** 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。

本章節討論下列主題：

- 新增授權金鑰
- 管理使用者帳戶和角色型存取控制
- 設定憑證
- 設定應用裝置
- 新增計算管理程式
- 管理標記
- 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
- 檢視在虛擬機器上執行之應用程式的相關資料
- 收集支援服務包

■ 客戶經驗改進計劃

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **系統 > 組態 > 授權**。
- 3 按一下 **新增**，輸入授權金鑰。
- 4 按一下 **儲存**。

管理使用者帳戶和角色型存取控制

NSX-T Data Center 應用裝置有兩個內建使用者：admin 和 audit。您可以整合 NSX-T Data Center 與 VMware Identity Manager (vIDM)，並為 vIDM 所管理的使用者設定角色型存取控制 (RBAC)。

對於 vIDM 管理的使用者，適用的驗證原則是 vIDM 管理員設定的原則，而非僅適用於使用者管理和稽核的 NSX-T Data Center 驗證原則。

變更 CLI 使用者的密碼

每個應用裝置具有兩個內建使用者 (即 admin 和 audit)，可供您用來登入及執行 CLI 命令。您可以變更這些使用者的密碼，但無法新增或刪除使用者。

程序

- 1 登入應用裝置的 CLI。

2 執行 `set user` 命令。例如，

```
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

驗證原則設定

您可以透過 CLI 來檢視或變更驗證原則設定。

您可以使用下列命令來檢視或設定密碼長度下限：

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

下列命令適用於登入 NSX Manager UI，或發出 API 呼叫：

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

下列命令適用於在 NSX Manager、NSX Controller 或 NSX Edge 節點上登入 CLI：

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

如需關於 CLI 命令的詳細資訊，請參閱《NSX-T 命令列介面參考》。

依預設，連續五次登入 NSX Manager UI 嘗試失敗後，系統會將管理員帳戶鎖定 15 分鐘。您可以使用下列命令來停用帳戶鎖定：

```
set auth-policy api lockout-period 0
```


同樣地，您可以使用下列命令來停用 CLI 的帳戶鎖定：

```
set auth-policy cli lockout-period 0
```

從 vIDM 主機取得憑證指紋

設定 vIDM 與 NSX-T 的整合之前，您必須先從 vIDM 主機取得憑證指紋。

程序

- 1 使用 SSH 連線至 vIDM 主機，並以 **sshuser** 身分登入。
- 2 執行下列命令以成為 **root** 使用者。

```
su root
```

- 3 編輯 `/etc/ssh/sshd_config` 檔案，將 `PermitRootLogin` 的值變更為 `yes`，並將 `StrictModes` 的值變更為 `no`。

```
PermitRootLogin yes
StrictModes no
```

- 4 執行下列命令以重新啟動 `sshd` 服務。

```
service sshd restart
```

- 5 登出後再以 **root** 使用者身分登入。
- 6 執行下列命令以變更目錄

```
cd /usr/local/horizon/conf
```

- 7 執行下列命令以取得指紋。

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2>/dev/null | openssl x509 -
sha256 -fingerprint -noout -in /dev/stdin
```

例如：

```
openssl s_client -connect vidm.corp.local:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -
fingerprint -noout -in /dev/stdin
```

建立 vIDM 主機與 NSX-T 之間的關聯

若要讓 NSX-T 與 vIDM 進行整合，您必須提供 vIDM 主機的相關資訊。

vIDM 伺服器應具有憑證授權機構 (CA) 簽署的憑證。否則，可能無法在某些瀏覽器上從 NSX Manager 登入 vIDM，例如 Microsoft Edge 或 Internet Explorer 11。如需在 vIDM 上安裝 CA 簽署憑證的相關資訊，請參閱 <https://docs.vmware.com/tw/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>。

當您向 vIDM 登錄 NSX Manager 時，會指定指向至 NSX Manager 的重新導向 URI。您可以提供完整網域名稱 (FQDN) 或 IP 位址。請務必記住您是使用 FQDN 還是 IP 位址。當您嘗試透過 vIDM 登入 NSX Manager 時，必須以相同方式在 URL 中指定主機名稱，即，如果您向 vIDM 登錄管理程式時使用 FQDN，則必須在 URL 中使用 FQDN，且如果向 vIDM 登錄管理程式時使用 IP 位址，則必須在 URL 中使用 IP 位址。否則，將無法登入。

必要條件

- 確認您擁有 vIDM 主機提供的憑證指紋。請參閱[從 vIDM 主機取得憑證指紋](#)。
- 確認已向 vIDM 主機登錄 NSX Manager 作為 OAuth 用戶端。在登錄程序期間，記下用戶端識別碼和用戶端密碼。如需詳細資訊，請參閱位於 <https://www.vmware.com/support/pubs/identitymanager-pubs.html> 的 VMware Identity Manager 說明文件。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 使用者**。
- 3 按一下**組態索引**標籤。
- 4 按一下**編輯**。
- 5 請提供下列資訊。

參數	說明
VMware Identity Manager 應用裝置	vIDM 主機的完整網域名稱 (FQDN)。
用戶端識別碼	向 vIDM 主機登錄 NSX Manager 時所建立的識別碼。
用戶端密碼	向 vIDM 主機登錄 NSX Manager 時所建立的密碼。
指紋	vIDM 主機的憑證指紋。
NSX 應用裝置	NSX Manager 的 IP 位址或完整網域名稱 (FQDN)。如果指定 FQDN，必須在 URL 中使用 Manager 的 FQDN 從瀏覽器存取 NSX Manager；如果指定 IP 位址，則必須在 URL 中使用 IP 位址。或者，vIDM 管理員可以設定 NSX Manager 用戶端，以便您使用 FQDN 或 IP 位址連線。

- 6 按一下**儲存**。

NSX Manager、vIDM 和相關元件之間的時間同步

為了使驗證正常工作，NSX Manager、vIDM 和其他服務提供者 (例如 Active Directory) 必須全部進行時間同步。本節說明如何對這些元件進行時間同步。

VMware Infrastructure

請遵循以下知識庫文章中的指示來同步 ESXi 主機。

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

如需同步虛擬機器和主機的相關資訊，請參閱 https://docs.vmware.com/tw/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html。虛擬機器可能會執行 NSX Manager、vIDM、Active Directory 或其他服務提供者。

第三方基礎結構

請遵循廠商有關如何同步虛擬機器和主機的說明文件。

在 vIDM 伺服器上設定 NTP (不建議)

如果您無法在主機之間同步時間，可以停用同步到主機並在 vIDM 伺服器上設定 NTP。不建議使用此方法，因為需要在 vIDM 伺服器上開啟 UDP 連接埠 123

- 檢查 vIDM 伺服器上的時鐘，並確定其正確無誤。

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- 編輯 /etc/ntp.conf 並新增下列項目 (如果不存在)。

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- 開啟 UDP 連接埠 123。

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

執行下列命令來確認連接埠處於開啟狀態。

```
# iptables -L -n
```

- 啟動 NTP 服務。

```
/etc/init.d/ntp start
```

- 將 NTP 設為在重新開機後自動執行。

```
# chkconfig --add ntp
# chkconfig ntp on
```

- 確認可以連線 NTP 伺服器。

```
# ntpq -p
```

reach 資料行不應該顯示 0。st 資料行應顯示除 16 以外的某些數字。

角色型存取控制

透過角色型存取控制 (RBAC)，您可以限制僅授權使用者可存取系統。系統會將角色指派使用者，且每個角色具有特定權限。

權限分為四種類型：

- 完整存取權
- 執行
- 讀取
- 無

完整存取權可為使用者提供所有權限。執行權限包含讀取權限。

NSX-T Data Center 具有下列內建角色。您無法新增任何新角色。

- 企業管理員
- 稽核員
- 網路工程師
- 網路作業
- 安全工程師
- 安全作業
- 雲端服務管理員
- 雲端服務稽核員
- 負載平衡器管理員
- 負載平衡器稽核員

為 Active Directory (AD) 使用者指派角色之後，如果 AD 伺服器上的使用者名稱已變更，您需要使用新的使用者名稱重新指派角色。

角色和權限

表 17-1. 角色和權限 說明每個角色對於不同作業所具有的權限。使用的縮寫如下：

- EA - 企業管理員
- A - 稽核員
- NE - 網路工程師
- NO - 網路作業
- SE - 安全工程師
- SO - 安全作業
- CS Adm - 雲端服務管理員
- CS Aud - 雲端服務稽核員
- LB Adm - 負載平衡器管理員
- LB Aud - 負載平衡器稽核員

- FA - 完整存取權
- E - 執行
- R - 讀取

表 17-1. 角色和權限

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
工具 > 連接埠 連線	E	R	E	E	E	E	E	R	E	E
工具 > Traceflow	E	R	E	E	E	E	E	R	E	E
工具 > 連接埠 鏡像	FA	R	FA	FA	FA	FA	FA	R	無	無
工具 > IPFIX	FA	R	FA	R	FA	R	FA	R	無	無
防火牆 > 一般	FA	R	R	R	FA	R	FA	R	無	無
防火牆 > 組態	FA	R	R	R	FA	R	FA	R	無	無
加密	FA	R	FA	R	FA	FA	無	無	無	無
路由 > 路由器	FA	R	FA	R	R	R	FA	R	R	R
路由 > NAT	FA	R	FA	R	FA	R	FA	R	R	R
DHCP > 伺服器 設定檔	FA	R	FA	R	FA	無	FA	R	無	無
DHCP > 伺服器	FA	R	FA	R	FA	無	FA	R	無	無
DHCP > 轉送 設定檔	FA	R	FA	R	FA	無	FA	R	無	無
DHCP > 轉送 服務	FA	R	FA	R	FA	無	FA	R	無	無
DHCP > 中繼 資料 Proxy	FA	R	FA	R	FA	無	無	無	無	無
IPAM	FA	R	FA	R	FA	無	無	無	無	無
交換 > 交換器	FA	R	FA	FA	R	R	FA	R	R	R
交換 > 連接埠	FA	R	FA	FA	R	R	FA	R	R	R
交換 > 交換設 定檔	FA	R	FA	FA	FA	FA	FA	R	R	R
負載平衡 > 負 載平衡器	FA	R	無	無	無	無	FA	R	FA	R
負載平衡 > 虛 擬伺服器	FA	R	無	無	無	無	FA	R	FA	R
負載平衡 > 設 定檔 > 應用程 式設定檔	FA	R	無	無	無	無	FA	R	FA	R

表 17-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
負載平衡 > 設定檔 > 持續性設定檔	FA	R	無	無	無	無	FA	R	FA	R
負載平衡 > 設定檔 > SSL 設定檔	FA	R	無	無	FA	R	FA	R	FA	R
負載平衡 > 伺服器集區	FA	R	無	無	無	無	FA	R	FA	R
負載平衡 > 監視器	FA	R	無	無	無	無	FA	R	FA	R
詳細目錄 > 群組	FA	R	FA	R	FA	R	FA	R	R	R
詳細目錄 > IP 集合	FA	R	FA	R	FA	R	FA	R	R	R
詳細目錄 > IP 集區	FA	R	FA	R	無	R	無	無	R	R
詳細目錄 > MAC 集合	FA	R	FA	R	FA	R	FA	R	R	R
詳細目錄 > 服務	FA	R	FA	R	FA	R	FA	R	R	R
詳細目錄 > 虛擬機器	R	R	R	R	R	R	R	R	R	R
詳細目錄 > 虛擬機器 > 建立和指派標籤	FA	R	FA	FA	FA	FA	FA	R	R	R
詳細目錄 > 虛擬機器 > 設定標籤	FA	無	無	無	FA	無	無	無	無	無
網狀架構 > 節點 > 主機	FA	R	R	R	R	R	R	R	無	無
網狀架構 > 節點 > 節點	FA	R	FA	R	FA	R	R	R	無	無
網狀架構 > 節點 > Edge	FA	R	FA	R	R	R	R	R	無	無
網狀架構 > 節點 > Edge 叢集	FA	R	FA	R	R	R	R	R	無	無
網狀架構 > 節點 > 橋接器	FA	R	FA	R	R	R	無	無	R	R
網狀架構 > 節點 > 傳輸節點	FA	R	R	R	R	R	R	R	R	R

表 17-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
網狀架構 > 節點 > 通道	R	R	R	R	R	R	R	R	R	R
網狀架構 > 設定檔 > 上行設定檔	FA	R	R	R	R	R	R	R	R	R
網狀架構 > 設定檔 > Edge 叢集設定檔	FA	R	FA	R	R	R	R	R	R	R
網狀架構 > 設定檔 > 組態	FA	R	無	無	無	無	R	R	無	無
網狀架構 > 傳輸區域 > 傳輸區域	FA	R	R	R	R	R	R	R	R	R
網狀架構 > 傳輸區域 > 傳輸區域設定檔	FA	R	R	R	R	R	R	R	R	R
網狀架構 > 計算管理程式	FA	R	R	R	R	R	R	R	無	無
系統 > 信任	FA	R	無	無	FA	R	無	無	FA	R
系統 > 組態	E	R	R	R	R	R	無	無	無	無
系統 > 公用程式 > 支援服務包	FA	R	R	R	R	R	R	R	無	無
系統 > 公用程式 > 備份	FA	R	無	無	無	無	無	無	無	無
系統 > 公用程式 > 還原	FA	R	無	無	無	無	無	無	無	無
系統 > 公用程式 > 升級	FA	R	R	R	R	R	無	無	無	無
系統 > 使用者 > 角色指派	FA	R	無	無	無	無	無	無	無	無
系統 > 使用者 > 組態	FA	R	無	無	無	無	無	無	無	無

管理角色指派

當 VMware Identity Manager 與 NSX-T Data Center 整合時，您可以新增、變更和刪除對使用者或使用者群組的角色指派。

必要條件

- 確認 vIDM 主機與 NSX-T 建立關聯。如需詳細資訊，請參閱[建立 vIDM 主機與 NSX-T 之間的關聯](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 使用者**。
- 3 按一下**角色指派**索引標籤 (若尚未選取)。
- 4 新增、變更或刪除角色指派。

選項	動作
新增角色指派	按一下 新增 ，接著選取使用者或使用者群組，然後選取角色。
變更角色指派	選取使用者或使用者群組，然後按一下 編輯 。
刪除角色指派	選取使用者或使用者群組，然後按一下 刪除 。

檢視主體身分識別

主體可以是 NSX-T Data Center 元件或第三方應用程式，例如 OpenStack 產品。藉由主體身分識別，主體可以使用身分識別名稱來建立物件，並確保僅具有相同身分識別名稱的實體能夠修改或刪除物件。

主體身分識別具有下列內容：

- 名稱
- 節點識別碼
- 憑證
- 指示此主體存取權的 RBAC 角色
- 指示此主體建立的物件是否受保護的旗標

具有企業管理員角色的使用者 (本機、遠端或主體身分識別)，可以修改或刪除主體身分識別所擁有的物件。不具企業管理員角色的使用者 (本機、遠端或主體身分識別)，無法修改或刪除主體身分識別所擁有的受保護物件，但可以修改或刪除不受保護的物件。企業管理員使用者只能使用 NSX-T Data Center API 但不能使用 NSX Manager UI 來刪除受保護的物件。

主體身分識別僅能使用 NSX-T API 來建立或刪除。如需詳細資訊，請參閱《NSX-T Data Center API 參考》。但是，您可以透過 NSX Manager UI 來檢視主體身分識別。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 使用者**。
- 3 按一下**角色指派**索引標籤。

隨即顯示使用者、使用者群組及主體身分識別。

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。

必要條件

- 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 從瀏覽器以管理員權限登入 **NSX Manager**，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **系統 > 信任**。
- 3 按一下 **CSRS** 索引標籤。
- 4 按一下 **產生 CSR**。
- 5 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。
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。
狀態	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)。

選項	說明
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。

6 按一下儲存。

自訂 CSR 會顯示為連結。

7 選取 CSR，然後按一下動作。

8 從下拉式功能表中選取下載 CSR PEM。

您可以儲存 CSR PEM 檔案以作為記錄及 CA 提交。

9 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。

結果

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。

必要條件

確認 CA 憑證可供使用。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的系統 > 信任。
- 3 按一下憑證索引標籤。
- 4 選取匯入 > 匯入 CA 憑證，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。

結果

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。

必要條件

確認可以使用憑證。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 信任**。
- 3 按一下**憑證**索引標籤。
- 4 選取**匯入 > 匯入憑證**，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**。

結果

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。

必要條件

確認 CSR 可用。請參閱[建立憑證簽署要求檔案](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 信任**。

- 3 按一下 **CSRS** 索引標籤。
- 4 選取現有的 CSR。
- 5 按一下**動作**然後從下拉式功能表中選取 **CSR 的自我簽署憑證**。
- 6 輸入自我簽署憑證有效天數。
預設時間範圍是 10 年。
- 7 按一下**儲存**。

結果

自我簽署的憑證會顯示在**憑證**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，則可以進行 **API** 呼叫來取代現有憑證。

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://nsx-manager-ip-address`。
- 2 選取導覽面板中的**系統 > 信任**。
- 3 按一下**憑證**索引標籤。
- 4 按一下您要使用的憑證 ID，從快顯視窗中複製憑證 ID。
- 5 使用 POST `/api/v1/node/services/http?action=apply_certificate` API 呼叫來取代現有憑證。例如，

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

如需詳細資訊，請參閱《NSX-T API 參考》。

結果

API 呼叫會重新啟動 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

必要條件

確認有可用的 CRL。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 信任**。
- 3 按一下 **CRLS** 索引標籤。
- 4 按一下**匯入**，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	<p>複製 CRL 中的所有項目，並將其貼上至此區段中。</p> <p>範例 CRL。</p> <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTENMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEbMBk G A1UEAxMSU1NMZW51IGRlbW8gc2VydmlVYFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDB a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCsq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSV05CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
說明	輸入此 CRL 所含內容的摘要。

- 5 按一下**儲存**。

結果

匯入的 CRL 會顯示為連結。

匯入 CSR 的憑證

您可以為 CSR 匯入已簽署的憑證。

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。

必要條件

確認 CSR 可用。請參閱[建立憑證簽署要求檔案](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**系統 > 信任**。
- 3 按一下 **CSRS** 索引標籤。
- 4 選取現有的 CSR。
- 5 按一下**動作**，然後從下拉式功能表中選取**匯入 CSR 的憑證**。
- 6 瀏覽至電腦上已簽署的憑證檔案，然後新增該檔案。
- 7 按一下**儲存**。

結果

自我簽署的憑證會顯示在**憑證**清單中。憑證類型會指定為自我簽署。

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

表 17-2. 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 <a href="https://<nsx-mgr>/api/v1/node">https://<nsx-mgr>/api/v1/node
設定 NTP 伺服器	set ntp-server <ntp-server>	PUT <a href="https://<nsx-mgr>/api/v1/node/services/ntp">https://<nsx-mgr>/api/v1/node/services/ntp
設定 DNS 伺服器	set name-servers <dns-server>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/name-servers">https://<nsx-mgr>/api/v1/node/network/name-servers
設定 DNS 搜尋網域	set search-domains <domain>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/search-domains">https://<nsx-mgr>/api/v1/node/network/search-domains

新增計算管理程式

計算管理程式 (例如 vCenter Server) 是一種應用程式，可管理如主機和虛擬機器等資源。NSX-T Data Center 會輪詢計算管理程式以找出如新增或移除主機或者虛擬機器等變更，並據以更新其詳細目錄。可以

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

在此版本中，此功能支援：

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

程序

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

選項	說明
名稱與說明	輸入名稱以識別 vCenter Server。 您可以選擇性地說明任何特殊詳細資料，例如 vCenter Server 中的叢集數目。
網域名稱/IP 位址	輸入 vCenter Server 的 IP 位址。
類型	保留預設選項。
使用者名稱和密碼	輸入 vCenter Server 登入認證。
指紋	輸入 vCenter Server SHA-256 指紋演算法值。

如果您將指紋值保留空白，則系統會提示您接受伺服器提供的指紋。

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

- 5 如果進度圖示從**進行中**變更為**未登錄**，請執行下列步驟來解決此錯誤。
 - a 選取錯誤訊息，然後按一下**解決**。一個可能的錯誤訊息如下：

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

- b 輸入 vCenter Server 認證，然後按一下**解決**。
現有登錄將被取代 (若有)。

結果

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

管理標記

您可以將標記新增至物件使搜尋更為輕鬆。指定標記時，您也可以指定範圍。

NSX Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 導覽至物件類別。
例如，導覽至**交換 > 交換器**。
- 3 按一下交換器的名稱。
- 4 選取功能表選項**動作 > 管理標記**，或按一下 [標記] 旁的**管理**。
- 5 新增或刪除標籤。

選項	動作
新增標籤	按一下 新增 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 刪除 。

一個物件最多可以有 30 個標記。標記的長度上限為 256 個字元。範圍的長度上限為 128 個字元。

- 6 按一下**儲存**。

搜尋物件

您可以使用各種準則在 NSX-T Data Center 詳細目錄中搜尋物件。

搜尋結果會依相關性排序，且您可以根據搜尋查詢來篩選這些結果。

備註 如果您在搜尋查詢中使用同時用作運算子的特殊字元，則必須加上前置反斜線。用作運算子的字元包括：+、-、=、&&、||、<、>、!、(、)、{、}、[、]、^、"、~、?、:、/ 和 \。

程序

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


- 2 在首頁上，輸入物件或物件類型的搜尋模式。

當您輸入您的搜尋模式時，搜尋功能會顯示適用的關鍵字以提供協助。

搜尋	搜尋查詢
以 Logical 作為名稱或內容的物件	邏輯
完整邏輯交換器名稱	display_name:LSP-301
含有特殊字元的名稱，例如！	Logical!

所有相關的搜尋結果都會列出，並依資源類型在不同的索引標籤中分組。

您可以按一下索引標籤，查看某資源類型的特定搜尋結果。

- 3 (選擇性) 在搜尋列中，按一下儲存圖示，以儲存精簡的搜尋準則。
- 4 在搜尋列中，按一下  圖示可開啟進階搜尋資料行，您可在其中縮小搜尋範圍。
- 5 指定一或多個用來縮小搜尋範圍的準則。
- 名稱
 - 資源類型
 - 說明
 - 識別碼
 - 建立者
 - 修改者
 - 標籤
 - 建立日期
 - 修改日期

您也可以檢視最近的搜尋結果和儲存的搜尋準則。

- 6 (選擇性) 按一下**全部清除**，可重設您的進階搜尋準則。

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。

下表將依偏好程度由高至低列出 NSX Manager 所支援的項目。

表 17-3. 依照偏好順序列出的 NSX Manager 主機金鑰

NSX Manager 所支援的主機金鑰類型	金鑰的預設位置
ECDSA (256 位元)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

程序

- 1 以根使用者身分登入遠端伺服器。

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 比較可用的金鑰與 NSX Manager 支援的金鑰。

在此範例中，唯一可接受的金鑰為 ED25519。

- 4 取得金鑰的指紋。

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

備份和還原 NSX Manager

如果 NSX Manager 變得無法運作，您可以從備份還原它。NSX Manager 無法運作時，數據平面不會受到影響，但您無法進行組態變更。

有三種類型的備份：

叢集備份 此備份包含虛擬網路所需的狀態。

節點備份 這是 NSX Manager 節點的備份。

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 Data Center 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。

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 可存取的檔案伺服器。您在進行備份之前，必須設定此伺服器的位置。

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 可存取的檔案伺服器。您在進行備份之前，必須設定此伺服器的位置。

備註 依據設計，NSX Manager 不會刪除備份檔案伺服器上的備份檔案。您必須管理備份輪替，並確保伺服器具有足夠的磁碟空間用於備份。您可以考慮執行自動刪除舊備份的指令碼。

必要條件

確認您擁有備份檔案伺服器的 SSH 指紋。系統僅接受 SHA256 雜湊的 ECDSA 金鑰作為指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。

程序

- 1 從瀏覽器以管理員身分登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 按一下 **系統 > 公用程式 > 備份**。
- 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**。
- 4 按一下 **自動備份** 切換按鈕以啟用自動備份。
- 5 輸入備份檔案伺服器的 IP 位址或主機名稱。
- 6 視需要編輯預設連接埠。
- 7 輸入登入備份檔案伺服器所需的使用者名稱和密碼。
- 8 在**目的地目錄**欄位中，輸入儲存備份的絕對目錄路徑。
目錄必須已存在。如果您有多個 NSX-T Data Center 部署，請針對每個部署使用不同的目錄。
- 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**。

12 按一下頁面底部的**立即備份**以確認可將檔案寫入備份檔案伺服器中。

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。

必要條件

- 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 從瀏覽器以管理員身分登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 按一下**系統 > 公用程式 > 備份**。
- 3 按一下頁面右上角的**編輯**。
- 4 按一下**檔案伺服器**，然後確認是否已啟用自動備份。
- 5 按一下頁面頂端的**排程**。
- 6 若為節點/叢集備份，按一下**每週**，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**，然後設定備份時間。
- 7 詳細目錄備份依預設為每 5 分鐘執行一次，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**。

結果

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 NSX Manager 無法運作，您可以從備份還原。您將需要建立備份時指定的複雜密碼。

備註 不支援還原其中已建立備份之同一 NSX Manager 應用裝置上的備份。

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 還原備份

還原備份後會使網路還原回備份時的狀態、還原 NSX Manager 所維護的組態，以及協調自備份建立後對網狀架構所做的任何變更，例如新增或刪除節點。

3 從 vCenter Server 移除 NSX-T Data Center 延伸

當您新增計算管理程式時，NSX Manager 會新增其身分識別做為 vCenter Server 中的延伸。如果您不想將此 vCenter Server 登錄至任何 NSX-T Data Center 安裝，可透過 vCenter Server 的受管理物件瀏覽器 (MOB) 移除延伸。

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。

備註 不支援還原其中已建立備份之同一 NSX Manager 應用裝置上的備份。

必要條件

- 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。
 - 您必須使用與管理程式備份對應的 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 Data Center 安裝指南》。

後續步驟

還原備份。

還原備份

還原備份後會使網路還原回備份時的狀態、還原 NSX Manager 所維護的組態，以及協調自備份建立後對網狀架構所做的任何變更，例如新增或刪除節點。

備註 不支援還原其中已建立備份之同一 NSX Manager 應用裝置上的備份。

必要條件

- 確認您擁有備份檔案伺服器的 SSH 指紋。系統僅接受 SHA256 雜湊的 ECDSA 金鑰作為指紋。請參閱 [尋找遠端伺服器的 SSH 指紋](#)。
- 確認您擁有節點和叢集備份檔案的複雜密碼。
- 確認您新安裝的 NSX Manager 未設定任何物件。請參閱 [準備還原 NSX Manager 備份](#)。

程序

- 1 從瀏覽器登入全新安裝的 NSX Manager。
- 2 選取導覽面板中的 **系統 > 公用程式**。
- 3 按一下 **還原** 索引標籤。
- 4 按一下 **編輯** 以設定備份檔案伺服器。
- 5 輸入 IP 位址或主機名稱。
- 6 視需要變更連接埠號碼。
預設值為 22。
- 7 輸入用來登入伺服器的使用者名稱和密碼。
- 8 在 **目的地目錄** 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。
- 10 輸入儲存備份之伺服器的 SSH 指紋。
- 11 按一下 **儲存**。
- 12 選取備份。
- 13 按一下 **還原**。

隨即顯示還原作業的狀態。如果您在備份後已刪除或新增網狀架構節點或傳輸節點，則系統將會提示您執行特定動作，例如登入節點並執行指令碼。

還原作業完成後會出現 **[還原完成]** 畫面，其中會顯示還原的結果、備份檔案的時間戳記，以及還原作業的開始和結束時間。如果還原失敗，畫面會顯示作業失敗的步驟，例如 **Current Step: Restoring Cluster (DB)** 或 **Current Step: Restoring Node**。如果叢集還原或節點還原失敗，錯誤可能是暫時性的。在此情況下，並不需要按一下 **重試**。您可以將管理員重新啟動或重新開機，如此還原作業將會繼續執行。

您也可以執行下列 CLI 命令以檢視系統記錄檔，以及搜尋 `Cluster restore failed` 和 `Node restore failed` 字串，藉以判斷是否有叢集還原或節點還原失敗。

```
get log-file syslog
```

若要將管理員重新啟動，請執行下列 CLI 命令：

```
restart service manager
```

若要將管理員重新開機，請執行下列 CLI 命令：

```
reboot
```

結果

備註 如果您在備份後已新增計算管理程式，則在還原後，如果您嘗試再次新增計算管理程式，將會收到指出登錄失敗的錯誤訊息。您可以解決此錯誤並成功新增計算管理程式。如需詳細資訊，請參閱[新增計算管理程式](#)中的步驟 5。如果您想要移除 vCenter Server 中儲存的有關 NSX-T Data Center 的資訊，請依照從 [vCenter Server 移除 NSX-T Data Center 延伸](#)中的步驟操作。

從 vCenter Server 移除 NSX-T Data Center 延伸

當您新增計算管理程式時，NSX Manager 會新增其身分識別做為 vCenter Server 中的延伸。如果您不想將此 vCenter Server 登錄至任何 NSX-T Data Center 安裝，可透過 vCenter Server 的受管理物件瀏覽器 (MOB) 移除延伸。

程序

- 1 以管理員身分登入 vSphere Web client。
- 2 選取 ESXi 主機。
- 3 按一下**管理 > 設定**索引標籤。
- 4 從功能表中選取**進階系統設定**。
- 5 啟用 **Config.HostAgent.plugins.solo.enableMob** 選項。
- 6 登入 MOB。
- 7 按一下**內容**連結，此為內容資料表中**內容**屬性的值。
- 8 按一下 **ExtensionManager** 連結，此為內容資料表中 **extensionManager** 內容的值。
- 9 按一下方法資料表中的 **UnregisterExtension** 連結。
- 10 在**值**文字欄位中輸入 **com.vmware.nsx.management.nsxt**。
- 11 按一下頁面右邊參數資料表下方的**叫用方法**連結。

方法結果顯示為 **void**，但會移除延伸。

- 12 若要確保延伸已移除，請按一下上一頁中的 **FindExtension** 方法，並針對延伸輸入相同的值進行叫用。

結果應為 `void`。

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](#)。
- 依照下列步驟判斷叢集成員資格是否已變更；若已變更，請從備份還原。

必要條件

- 確認您擁有最新備份。
- 執行還原。請參閱[還原備份](#)。

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 完成還原。
- 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 Data Center 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 NSX Controller 或 NSX Edge 叢集中的應用裝置變得無法運作，或您由於任何原因需將其移除，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

您可以檢查 NSX Manager 的狀態，並將其重新開機 (如果變得無法運作)。

取得 NSX Manager 狀態

您可以透過 NSX Manager UI 查看 NSX Manager 的狀態，或使用 CLI 命令來取得狀態。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `http://<nsx-manager-ip-address>`。
- 2 選取導覽面板中的**系統 > 元件**。
會顯示 NSX Manager 的狀態。
- 3 或者，登入 NSX Manager 的 CLI。
- 4 執行 `get management-cluster status` 命令。例如，

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 10.172.121.217 (UUID 42191561-79dc-710a-74f1-d15f10cd2c40) Online
```

```
Management cluster status: STABLE
```

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

```
- 10.172.121.91    (UUID ab35851f-e616-4760-8d7a-c4386c537382)
- 10.172.122.187  (UUID d159b758-c320-411f-aa67-1e2fd35f5ef2)
- 10.172.122.138  (UUID 12a3b19d-26a0-492e-836e-e9a3cc25e799)
```

```
Control cluster status: DEGRADED
```

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。

重新開機 NSX Manager

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 叢集必須具有三個成員用於生產部署，以避免 NSX 控制平面出現任何中斷。每個控制器皆應放置在唯一的 Hypervisor 主機上 (總計三個實體 Hypervisor 主機)，以避免單一實體 Hypervisor 主機故障影響 NSX 控制平面。針對沒有任何生產工作負載的實驗室和概念證明部署，可接受執行單一控制器以節省資源。

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。如果無法重新連線，可將其取代。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。如果無法將任一離線成員重新連線，您可以取代失敗的 NSX Controller 或重新部署 NSX Controller 叢集。請參閱 [重新部署 NSX Controller 叢集](#)。

必要條件

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 17-4. 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: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) 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: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) 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: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) 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: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) 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或您因任何其他原因想要將其從叢集移除，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。

必要條件

- 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 Data Center 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

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
```

結果

備註 已使用 `detach` 命令移除的控制器仍保留一些組態資訊。如果您想要再次將控制器加入任何控制器叢集，必須在控制器上執行下列 CLI 命令以移除失效資訊：

```
deactivate control-cluster
```

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。

必要條件

- 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 Data Center 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 NSX 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 NSX 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 **NSX 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 Data Center 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 Data Center 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 Data Center 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 NSX Edge 叢集以使用新的傳輸節點來取代失敗的傳輸節點。

- 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 NSX Edge 叢集的識別碼。id 欄位包含 NSX Edge 叢集識別碼。從 members 陣列取得 NSX 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 NSX Edge 叢集以使用新的傳輸節點來取代失敗的傳輸節點。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) 已失敗，因此將其取代為 NSX 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 (選擇性) 刪除故障的傳輸節點以及 NSX Edge 節點。

記錄訊息

所有 NSX-T Data Center 元件 (包括 ESXi 主機上執行的元件) 的記錄訊息均符合 RFC 5424 中指定的 Syslog 格式。KVM 主機的記錄訊息採用 RFC 3164 格式。記錄檔位於 `/var/log` 目錄中。

在 NSX-T Data Center 應用裝置上，您可以執行下列 NSX-T Data Center CLI 命令以檢視記錄：

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

在 Hypervisor 中，您可以使用 `tac`、`tail`、`grep` 和 `more` 等 Linux 命令來檢視記錄。您也可以在 NSX-T Data Center 應用裝置上使用這些命令。

如需 RFC 5424 的詳細資訊，請參閱 <https://tools.ietf.org/html/rfc5424>。如需 RFC 3164 的詳細資訊，請參閱 <https://tools.ietf.org/html/rfc3164>。

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
```

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.
```

每個訊息都具有元件 (`comp`) 和子元件 (`subcomp`) 資訊，可協助識別訊息的來源。

NSX-T Data Center 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。

與 API 呼叫相關聯的稽核記錄具有下列資訊：

- 實體識別碼參數 `entId`，用於識別 API 的物件。
- 要求識別碼參數 `req-id`，用於識別特定的 API 呼叫。
- 外部要求識別碼參數 `ereqId`，如果 API 呼叫包含標頭 `X-NSX-EREQID:<string>`。
- 外部使用者參數 `euser`，如果 API 呼叫包含標頭 `X-NSX-EUSER:<string>`。

RFC 5424 會定義下列嚴重性層級：

嚴重性層級	說明
0	緊急：系統無法使用
1	警示：必須立即採取動作

嚴重性層級	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 欄位可識別訊息的類型。如需訊息識別碼清單，請參閱[記錄訊息識別碼](#)。

設定遠端記錄

您可以設定 NSX-T Data Center 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 和 Hypervisor 支援遠端記錄。您必須在每個節點上個別設定遠端記錄。

在 KVM 主機上，NSX-T Data Center 安裝套件透過將組態檔置於 `/etc/rsyslog.d` 目錄中，以自動設定 rsyslog 精靈。

必要條件

- 設定記錄伺服器來接收記錄。

程序

- 1 在 NSX-T Data Center 應用裝置上設定遠端記錄：

- a 執行下列命令來設定記錄伺服器和要傳送至記錄伺服器的訊息類型。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>] [structured-data <structured-data>]
```

如需有關此命令的詳細資訊，請參閱《NSX-T CLI 參考》。您可以多次執行命令以新增多個記錄伺服器組態。例如：

```
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
```

- b 您可以使用 `get logging-server` 命令檢視記錄組態。例如，

```
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
```

2 在 ESXi 主機上設定遠端記錄：

- a 執行下列命令以設定 Syslog 和傳送測試訊息：

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b 您可以執行下列命令以顯示組態：

```
esxcli system syslog config get
```

3 在 KVM 主機上設定遠端記錄：

- a 針對您的環境編輯檔案 `/etc/rsyslog.d/10-vmware-remote-logging.conf`。
- b 將下列行新增至檔案：

```
*.* @<ip>:514;RFC5424fmt
```

- c 執行下列命令：

```
service rsyslog restart
```

記錄訊息識別碼

在記錄訊息中，訊息識別碼欄位可識別訊息的類型。您可以使用 `set logging-server` 命令中的 `messageid` 參數，以篩選傳送至記錄伺服器的記錄訊息。

表 17-5. 記錄訊息識別碼

訊息識別碼	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

表 17-5. 記錄訊息識別碼 (續)

訊息識別碼	範例
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
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) 實現 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。您可以設定交換器和防火牆的 IPFIX。針對交換器，系統會匯出 VIF (虛擬介面) 和 pNIC (實體 NIC) 的網路流量。針對防火牆，系統會匯出分散式防火牆元件所管理的網路流量。

NSX Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

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 Data Center 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 Data Center 不會自動開啟連接埠，所以您必須確定連接埠已開啟。

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。

必要條件

- 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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **工具 > IPFIX**。
- 3 若要設定交換器 IPFIX，請按一下 **交換器 IPFIX 收集器** 索引標籤。
- 4 按一下 **新增**。
- 5 輸入名稱和 (選用) 說明。
- 6 按一下 **新增**，然後輸入收集器的 IP 位址和連接埠。
您最多可以新增 4 個收集器。
- 7 按一下 **儲存**。

設定交換器 IPFIX 設定檔

您可以設定交換器的 IPFIX 設定檔。

程序

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

- 2 選取導覽面板中的**工具 > IPFIX**。
- 3 按一下**交換器 IPFIX 設定**檔索引標籤。
- 4 按一下**新增**以新增設定檔。

設定	說明
名稱與說明	輸入名稱和 (選用) 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。
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。輸入 0 表示沒有特定觀察網域。
收集器設定檔	選取您在上一個步驟中所設定的交換器 IPFIX 收集器。
優先順序	此參數可解決套用多個設定檔時產生的衝突。IPFIX 匯出工具僅會使用具有最高優先順序的設定檔。較低的值表示較高的優先順序。

- 5 按一下**套用至**以將設定檔套用至一或多個物件。

物件的類型為邏輯連接埠、邏輯交換器和 NSGroup。如果您選取 NSGroup，它必須包含一或多個邏輯交換器或邏輯連接埠。僅包含 IP 集或 MAC 集的 NSGroup 將被忽略。

- 6 按一下**儲存**。

設定防火牆 IPFIX 收集器

您可以設定防火牆的 IPFIX 收集器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**工具 > IPFIX**。
- 3 按一下**防火牆 IPFIX 收集器**索引標籤。
- 4 輸入名稱和 (選用) 說明。
- 5 按一下**新增**，然後輸入收集器的 IP 位址和連接埠。
您最多可以新增 4 個收集器。
- 6 按一下**儲存**。

設定防火牆 IPFIX 設定檔

您可以設定防火牆的 IPFIX 設定檔。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的工具 > IPFIX。
- 3 按一下防火牆 IPFIX 設定檔索引標籤。
- 4 按一下新增以新增設定檔。

設定	說明
名稱與說明	輸入名稱和 (選用) 說明。
收集器組態	從下拉式清單中選取收集器。
作用中流量匯出逾時 (分)	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 1。
優先順序	此參數可解決套用多個設定檔時產生的衝突。IPFIX 匯出工具僅會使用具有最高優先順序的設定檔。較低的值表示較高的優先順序。
觀察網域識別碼	此參數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。

- 5 按一下套用至以將設定檔套用至一或多個物件。

物件的類型為邏輯連接埠、邏輯交換器和 NSGroup。如果您選取 NSGroup，它必須包含一或多個邏輯交換器或邏輯連接埠。僅包含 IP 集或 MAC 集的 NSGroup 將被忽略。

- 6 按一下儲存。

ESXi IPFIX 範本

ESXi 主機傳輸節點支援八個 IPFIX 流程範本。

IPv4 範本

範本識別碼：256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
```

```
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv4 封裝式範本

範本識別碼：257

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()
```

IPv4 ICMP 範本

範本識別碼：258

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
```

```

IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port – Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv4 ICMP 封裝式範本

範本識別碼：259

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port– Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL–GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6 範本

範本識別碼：260

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv6 封裝式範本

範本識別碼：261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
```

```

IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP 範本

範本識別碼：262

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port – Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv6 ICMP 封裝式範本

範本識別碼：263

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)

```

```

IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

KVM IPFIX 範本

一個 KVM 主機傳輸節點支援 88 個 IPFIX 流程範本和一個選項範本。

KVM 乙太網路 IPFIX 範本

提供四個 KVM 乙太網路 IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

乙太網路入口

範本識別碼：256。欄位計數：27。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- 898 (長度：變數，PEN：VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度：4)
- flowEndDeltaMicroseconds (長度：4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路出口

範本識別碼: 257。欄位計數: 31。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 8)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路入口 (含通道)

範本識別碼: 258。欄位計數: 34。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- 893 (長度: 4, PEN: VMware Inc. (6876))

- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路出口 (含通道)

範本識別碼: 259。欄位計數: 38。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)

- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 8)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)

- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

KVM IPv4 IPFIX 範本

提供四個 KVM IPv4 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

IPv4 入口

範本識別碼: 276。欄位計數: 45。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)

- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 出口

範本識別碼: 277。欄位計數: 49。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)

- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)

- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 入口 (含通道)

範本識別碼: 278。欄位計數: 52。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)

- IP_DST_ADDR (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)

- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 出口 (含通道)

範本識別碼: 279。欄位計數: 56。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))

- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)

- postMCastOctetTotalCount (長度: 8)

KVM TCP over IPv4 IPFIX 範本

提供四個 KVM TCP over IPv4 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

TCP over IPv4 入口

範本識別碼: 280。欄位計數: 53。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)

- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 出口

範本識別碼: 281。欄位計數: 57。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- OUTPUT_SNMP (長度： 4)
- 未知(369) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IP_SRC_ADDR (長度： 4)
- IP_DST_ADDR (長度： 4)
- L4_SRC_PORT (長度： 2)
- L4_DST_PORT (長度： 2)
- 898 (長度： 變數，PEN： VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度： 4)
- flowEndDeltaMicroseconds (長度： 4)
- DROPPED_PACKETS (長度： 8)
- DROPPED_PACKETS_TOTAL (長度： 8)
- PKTS (長度： 8)

- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 入口 (含通道)

範本識別碼: 282。欄位計數: 60。

欄位包括:

- observationPointId (長度: 4)

- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)

- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 出口 (含通道)

範本識別碼: 283。欄位計數: 64。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- OUTPUT_SNMP (長度： 4)
- 未知(369) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IP_SRC_ADDR (長度： 4)
- IP_DST_ADDR (長度： 4)
- L4_SRC_PORT (長度： 2)
- L4_DST_PORT (長度： 2)
- 893 (長度： 4, PEN: VMware Inc. (6876))
- 894 (長度： 4, PEN: VMware Inc. (6876))
- 895 (長度： 1, PEN: VMware Inc. (6876))
- 896 (長度： 2, PEN: VMware Inc. (6876))
- 897 (長度： 2, PEN: VMware Inc. (6876))
- 891 (長度： 1, PEN: VMware Inc. (6876))

- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)

- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

KVM UDP over IPv4 IPFIX 範本

提供四個 KVM UDP over IPv4 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

UDP over IPv4 入口

範本識別碼: 284。欄位計數: 47。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 出口

範本識別碼: 285。欄位計數: 51。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)

- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)

- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 入口 (含通道)

範本識別碼: 286。欄位計數: 54。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)

- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)

- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 出口 (含通道)

範本識別碼: 287。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)

- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM SCTP over IPv4 IPFIX 範本

提供四個 KVM SCTP over IPv4 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

SCTP over IPv4 入口

範本識別碼: 288。欄位計數: 47。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)

- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 出口

範本識別碼：289。欄位計數：51。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- OUTPUT_SNMP (長度：4)
- 未知(369) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IP_SRC_ADDR (長度：4)
- IP_DST_ADDR (長度：4)
- L4_SRC_PORT (長度：2)
- L4_DST_PORT (長度：2)
- 898 (長度：變數，PEN：VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度：4)
- flowEndDeltaMicroseconds (長度：4)
- DROPPED_PACKETS (長度：8)

- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 入口 (含通道)

範本識別碼: 290。欄位計數: 54。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)

- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)

- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 出口 (含通道)

範本識別碼: 291。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)

- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM ICMPv4 IPFIX 範本

提供四個 KVM ICMPv4 IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

ICMPv4 入口

範本識別碼：292。欄位計數：47。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)

- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)

- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 出口

範本識別碼: 293。欄位計數: 51。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)

- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 入口 (含通道)

範本識別碼：294。欄位計數：54。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IP_SRC_ADDR (長度：4)
- IP_DST_ADDR (長度：4)
- ICMP_IPv4_TYPE (長度：1)
- ICMP_IPv4_CODE (長度：1)
- 893 (長度：4, PEN: VMware Inc. (6876))
- 894 (長度：4, PEN: VMware Inc. (6876))
- 895 (長度：1, PEN: VMware Inc. (6876))
- 896 (長度：2, PEN: VMware Inc. (6876))
- 897 (長度：2, PEN: VMware Inc. (6876))
- 891 (長度：1, PEN: VMware Inc. (6876))
- 892 (長度：變數, PEN: VMware Inc. (6876))
- 898 (長度：變數, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 出口 (含通道)

範本識別碼: 295。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)

- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)

- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM IPv6 IPFIX 範本

提供四個 KVM IPv6 IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

IPv6 入口

範本識別碼：296。欄位計數：46。

欄位包括：

- observationPointId (長度: 4)

- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)

- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 出口

範本識別碼: 297。欄位計數: 50。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 入口 (含通道)

範本識別碼: 298。欄位計數: 53。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))

- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 出口 (含通道)

範本識別碼：299。欄位計數：57。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- OUTPUT_SNMP (長度：4)
- 未知(369) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IPV6_SRC_ADDR (長度：4)
- IPV6_DST_ADDR (長度：4)
- FLOW_LABEL (長度：4)
- 893 (長度：4, PEN: VMware Inc. (6876))
- 894 (長度：4, PEN: VMware Inc. (6876))
- 895 (長度：1, PEN: VMware Inc. (6876))
- 896 (長度：2, PEN: VMware Inc. (6876))
- 897 (長度：2, PEN: VMware Inc. (6876))

- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM TCP over IPv6 IPFIX 範本

提供四個 KVM TCP over IPv6 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

TCP over IPv6 入口

範本識別碼：300。欄位計數：54。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IPV6_SRC_ADDR (長度：4)
- IPV6_DST_ADDR (長度：4)
- FLOW_LABEL (長度：4)
- L4_SRC_PORT (長度：2)
- L4_DST_PORT (長度：2)
- 898 (長度：變數，PEN：VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度：4)
- flowEndDeltaMicroseconds (長度：4)
- DROPPED_PACKETS (長度：8)
- DROPPED_PACKETS_TOTAL (長度：8)
- PKTS (長度：8)
- PACKETS_TOTAL (長度：8)

- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 出口

範本識別碼: 301。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)

- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 入口 (含通道)

範本識別碼: 302。欄位計數: 61。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)

- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)

- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 出口 (含通道)

範本識別碼: 303。欄位計數: 65。

欄位包括:

- observationPointId (長度: 4)

- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))

- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)

- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

KVM UDP over IPv6 IPFIX 範本

提供四個 KVM UDP over IPv6 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

UDP over IPv6 入口

範本識別碼: 304。欄位計數: 48。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 出口

範本識別碼: 305。欄位計數: 52。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)

- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)

- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 入口 (含通道)

範本識別碼: 306。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)

- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)

- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 出口 (含通道)

範本識別碼: 307。欄位計數: 59。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)

- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)

- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM SCTP over IPv6 IPFIX 範本

提供四個 KVM SCTP over IPv6 IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

SCTP over IPv6 入口

範本識別碼: 308。欄位計數: 48。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)

- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)

- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 出口

範本識別碼: 309。欄位計數: 52。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)

- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 入口 (含通道)

範本識別碼: 310。欄位計數: 55。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IPV6_SRC_ADDR (長度： 4)
- IPV6_DST_ADDR (長度： 4)
- FLOW_LABEL (長度： 4)
- L4_SRC_PORT (長度： 2)
- L4_DST_PORT (長度： 2)
- 893 (長度： 4, PEN: VMware Inc. (6876))
- 894 (長度： 4, PEN: VMware Inc. (6876))
- 895 (長度： 1, PEN: VMware Inc. (6876))
- 896 (長度： 2, PEN: VMware Inc. (6876))
- 897 (長度： 2, PEN: VMware Inc. (6876))
- 891 (長度： 1, PEN: VMware Inc. (6876))
- 892 (長度： 變數, PEN: VMware Inc. (6876))
- 898 (長度： 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度： 4)

- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 出口 (含通道)

範本識別碼: 311。欄位計數: 59。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)

- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)

- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM ICMPv6 IPFIX 範本

提供四個 KVM ICMPv6 IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

ICMPv6 入口

範本識別碼：312。欄位計數：48。

欄位包括：

- observationPointId (長度: 4)

- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)

- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv6 出口

範本識別碼: 313。欄位計數: 52。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)

- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)

- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv6 入口 (含通道)

範本識別碼: 314。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)

- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv6 出口 (含通道)

範本識別碼: 315。欄位計數: 59。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)

- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM 乙太網路 VLAN IPFIX 範本

提供四個 KVM 乙太網路 VLAN IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

乙太網路 VLAN 入口

範本識別碼: 316。欄位計數: 30。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路 VLAN 出口

範本識別碼: 317。欄位計數: 34。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 8)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)

- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路 VLAN 入口 (含通道)

範本識別碼: 318。欄位計數: 37。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)

- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

乙太網路 VLAN 出口 (含通道)

範本識別碼: 319。欄位計數: 41。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)

- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 8)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)

- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

KVM IPv4 VLAN IPFIX 範本

提供四個 KVM IPv4 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

IPv4 VLAN 入口

範本識別碼：336。欄位計數：48。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)

- IP_DST_ADDR (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 VLAN 出口

範本識別碼: 337。欄位計數: 52。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- OUTPUT_SNMP (長度： 4)
- 未知(369) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- SRC_VLAN (長度： 2)
- dot1qVlanId (長度： 2)
- dot1qPriority (長度： 1)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IP_SRC_ADDR (長度： 4)
- IP_DST_ADDR (長度： 4)
- 898 (長度： 變數，PEN： VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度： 4)
- flowEndDeltaMicroseconds (長度： 4)
- DROPPED_PACKETS (長度： 8)
- DROPPED_PACKETS_TOTAL (長度： 8)

- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 VLAN 入口 (含通道)

範本識別碼: 338。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)

- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)

- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv4 VLAN 出口 (含通道)

範本識別碼: 339。欄位計數: 59。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)

- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM TCP over IPv4 VLAN IPFIX 範本

提供四個 KVM TCP over IPv4 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

TCP over IPv4 VLAN 入口

範本識別碼：340。欄位計數：56。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)

- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)

- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 VLAN 出口

範本識別碼: 341。欄位計數: 60。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)

- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)

- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 VLAN 入口 (含通道)

範本識別碼: 342。欄位計數: 63。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)

- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv4 VLAN 出口 (含通道)

範本識別碼: 343。欄位計數: 67。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)

- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

KVM UDP over IPv4 VLAN IPFIX 範本

提供四個 KVM UDP over IPv4 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

UDP over IPv4 VLAN 入口

範本識別碼：344。欄位計數：50。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- SRC_VLAN (長度：2)
- dot1qVlanId (長度：2)
- dot1qPriority (長度：1)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IP_SRC_ADDR (長度：4)
- IP_DST_ADDR (長度：4)
- L4_SRC_PORT (長度：2)
- L4_DST_PORT (長度：2)
- 898 (長度：變數，PEN：VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度：4)
- flowEndDeltaMicroseconds (長度：4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 VLAN 出口

範本識別碼: 345。欄位計數: 54。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)

- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 VLAN 入口 (含通道)

範本識別碼: 346。欄位計數: 57。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)

- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)

- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv4 VLAN 出口 (含通道)

範本識別碼: 347。欄位計數: 61。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)

- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM SCTP over IPv4 VLAN IPFIX 範本

提供四個 KVM SCTP over IPv4 VLAN IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

SCTP over IPv4 VLAN 入口

範本識別碼: 348。欄位計數: 50。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)

- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)

- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 VLAN 出口

範本識別碼: 349。欄位計數: 54。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)

- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)

- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 VLAN 入口 (含通道)

範本識別碼: 350。欄位計數: 57。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)

- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv4 VLAN 出口 (含通道)

範本識別碼: 351。欄位計數: 61。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)

- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)

- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM ICMPv4 VLAN IPFIX 範本

提供四個 KVM ICMPv4 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

ICMPv4 VLAN 入口

範本識別碼：352。欄位計數：50。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)

- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 VLAN 出口

範本識別碼：353。欄位計數：54。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- OUTPUT_SNMP (長度：4)
- 未知(369) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- SRC_VLAN (長度：2)
- dot1qVlanId (長度：2)
- dot1qPriority (長度：1)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IP_SRC_ADDR (長度：4)
- IP_DST_ADDR (長度：4)
- ICMP_IPv4_TYPE (長度：1)
- ICMP_IPv4_CODE (長度：1)
- 898 (長度：變數，PEN：VMware Inc. (6876))

- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 VLAN 入口 (含通道)

範本識別碼: 354。欄位計數: 57。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)

- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)

- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv4 VLAN 出口 (含通道)

範本識別碼: 355。欄位計數: 61。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)

- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IP_SRC_ADDR (長度: 4)
- IP_DST_ADDR (長度: 4)
- ICMP_IPv4_TYPE (長度: 1)
- ICMP_IPv4_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))

- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM IPv6 VLAN IPFIX 範本

提供四個 KVM IPv6 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

IPv6 VLAN 入口

範本識別碼：356。欄位計數：49。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- SRC_VLAN (長度： 2)
- dot1qVlanId (長度： 2)
- dot1qPriority (長度： 1)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IPV6_SRC_ADDR (長度： 4)
- IPV6_DST_ADDR (長度： 4)
- FLOW_LABEL (長度： 4)
- 898 (長度： 變數， PEN： VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度： 4)
- flowEndDeltaMicroseconds (長度： 4)
- DROPPED_PACKETS (長度： 8)
- DROPPED_PACKETS_TOTAL (長度： 8)
- PKTS (長度： 8)
- PACKETS_TOTAL (長度： 8)
- 未知(354) (長度： 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 VLAN 出口

範本識別碼: 357。欄位計數: 53。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)

- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)

- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 VLAN 入口 (含通道)

範本識別碼: 358。欄位計數: 56。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)

- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)

- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

IPv6 VLAN 出口 (含通道)

範本識別碼: 359。欄位計數: 60。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)

- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)

- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM TCP over IPv6 VLAN IPFIX 範本

提供四個 KVM TCP over IPv6 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

TCP over IPv6 VLAN 入口

範本識別碼：360。欄位計數：57。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)

- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 VLAN 出口

範本識別碼: 361。欄位計數: 61。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)

- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)

- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 VLAN 入口 (含通道)

範本識別碼: 362。欄位計數: 64。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)

- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)

- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

TCP over IPv6 VLAN 出口 (含通道)

範本識別碼: 363。欄位計數: 68。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)

- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)

- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)
- tcpAckTotalCount (長度: 8)
- tcpFinTotalCount (長度: 8)
- tcpPshTotalCount (長度: 8)
- tcpRstTotalCount (長度: 8)
- tcpSynTotalCount (長度: 8)
- tcpUrgTotalCount (長度: 8)

KVM UDP over IPv6 VLAN IPFIX 範本

提供四個 KVM UDP over IPv6 VLAN IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

UDP over IPv6 VLAN 入口

範本識別碼：364。欄位計數：51。

欄位包括：

- observationPointId (長度： 4)
- DIRECTION (長度： 1)
- SRC_MAC (長度： 6)
- DESTINATION_MAC (長度： 6)
- ethernetType (長度： 2)
- ethernetHeaderLength (長度： 1)
- INPUT_SNMP (長度： 4)
- 未知(368) (長度： 4)
- IF_NAME (長度： 變數)
- IF_DESC (長度： 變數)
- SRC_VLAN (長度： 2)
- dot1qVlanId (長度： 2)
- dot1qPriority (長度： 1)
- IP_PROTOCOL_VERSION (長度： 1)
- IP_TTL (長度： 1)
- PROTOCOL (長度： 1)
- IP_DSCP (長度： 1)
- IP_PRECEDENCE (長度： 1)
- IP_TOS (長度： 1)
- IPV6_SRC_ADDR (長度： 4)
- IPV6_DST_ADDR (長度： 4)
- FLOW_LABEL (長度： 4)
- L4_SRC_PORT (長度： 2)
- L4_DST_PORT (長度： 2)
- 898 (長度： 變數， PEN： VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度： 4)
- flowEndDeltaMicroseconds (長度： 4)
- DROPPED_PACKETS (長度： 8)
- DROPPED_PACKETS_TOTAL (長度： 8)
- PKTS (長度： 8)

- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 VLAN 出口

範本識別碼: 365。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)

- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)

- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 VLAN 入口 (含通道)

範本識別碼: 366。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)

- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)

- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

UDP over IPv6 VLAN 出口 (含通道)

範本識別碼: 367。欄位計數: 62。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)

- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)

- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM SCTP over IPv6 VLAN IPFIX 範本

提供四個 KVM SCTP over IPv6 VLAN IPFIX 範本: 入口、出口、入口 (含通道) 和出口 (含通道)。

SCTP over IPv6 VLAN 入口

範本識別碼: 368。欄位計數: 51。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)

- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)

- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 VLAN 出口

範本識別碼: 369。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)

- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)

- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 VLAN 入口 (含通道)

範本識別碼: 370。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)

- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)

- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

SCTP over IPv6 VLAN 出口 (含通道)

範本識別碼: 371。欄位計數: 62。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)

- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- L4_SRC_PORT (長度: 2)
- L4_DST_PORT (長度: 2)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)

- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM ICMPv6 VLAN IPFIX 範本

提供四個 KVM ICMPv6 IPFIX 範本：入口、出口、入口 (含通道) 和出口 (含通道)。

ICMPv6 入口

範本識別碼：372。欄位計數：51。

欄位包括：

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)

- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)

- BYTES_SQUARED_PERMANENT (長度: 8)
- IP_LENGTH_MINIMUM (長度: 8)
- IP_LENGTH_MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv6 出口

範本識別碼: 373。欄位計數: 55。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- OUTPUT_SNMP (長度: 4)
- 未知(369) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)

- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)

- postMCastOctetTotalCount (長度: 8)

ICMPv6 入口 (含通道)

範本識別碼: 374。欄位計數: 58。

欄位包括:

- observationPointId (長度: 4)
- DIRECTION (長度: 1)
- SRC_MAC (長度: 6)
- DESTINATION_MAC (長度: 6)
- ethernetType (長度: 2)
- ethernetHeaderLength (長度: 1)
- INPUT_SNMP (長度: 4)
- 未知(368) (長度: 4)
- IF_NAME (長度: 變數)
- IF_DESC (長度: 變數)
- SRC_VLAN (長度: 2)
- dot1qVlanId (長度: 2)
- dot1qPriority (長度: 1)
- IP_PROTOCOL_VERSION (長度: 1)
- IP_TTL (長度: 1)
- PROTOCOL (長度: 1)
- IP_DSCP (長度: 1)
- IP_PRECEDENCE (長度: 1)
- IP_TOS (長度: 1)
- IPV6_SRC_ADDR (長度: 4)
- IPV6_DST_ADDR (長度: 4)
- FLOW_LABEL (長度: 4)
- ICMP_IPv6_TYPE (長度: 1)
- ICMP_IPv6_CODE (長度: 1)
- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))

- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)
- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

ICMPv6 出口 (含通道)

範本識別碼：375。欄位計數：62。

欄位包括：

- observationPointId (長度：4)
- DIRECTION (長度：1)
- SRC_MAC (長度：6)
- DESTINATION_MAC (長度：6)
- ethernetType (長度：2)
- ethernetHeaderLength (長度：1)
- INPUT_SNMP (長度：4)
- 未知(368) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- OUTPUT_SNMP (長度：4)
- 未知(369) (長度：4)
- IF_NAME (長度：變數)
- IF_DESC (長度：變數)
- SRC_VLAN (長度：2)
- dot1qVlanId (長度：2)
- dot1qPriority (長度：1)
- IP_PROTOCOL_VERSION (長度：1)
- IP_TTL (長度：1)
- PROTOCOL (長度：1)
- IP_DSCP (長度：1)
- IP_PRECEDENCE (長度：1)
- IP_TOS (長度：1)
- IPV6_SRC_ADDR (長度：4)
- IPV6_DST_ADDR (長度：4)
- FLOW_LABEL (長度：4)
- ICMP_IPv6_TYPE (長度：1)
- ICMP_IPv6_CODE (長度：1)

- 893 (長度: 4, PEN: VMware Inc. (6876))
- 894 (長度: 4, PEN: VMware Inc. (6876))
- 895 (長度: 1, PEN: VMware Inc. (6876))
- 896 (長度: 2, PEN: VMware Inc. (6876))
- 897 (長度: 2, PEN: VMware Inc. (6876))
- 891 (長度: 1, PEN: VMware Inc. (6876))
- 892 (長度: 變數, PEN: VMware Inc. (6876))
- 898 (長度: 變數, PEN: VMware Inc. (6876))
- flowStartDeltaMicroseconds (長度: 4)
- flowEndDeltaMicroseconds (長度: 4)
- DROPPED_PACKETS (長度: 8)
- DROPPED_PACKETS_TOTAL (長度: 8)
- PKTS (長度: 8)
- PACKETS_TOTAL (長度: 8)
- 未知(354) (長度: 8)
- 未知(355) (長度: 8)
- 未知(356) (長度: 8)
- 未知(357) (長度: 8)
- 未知(358) (長度: 8)
- MUL_DPKTS (長度: 8)
- postMCastPacketTotalCount (長度: 8)
- 未知(352) (長度: 8)
- 未知(353) (長度: 8)
- flowEndReason (長度: 1)
- DROPPED_BYTES (長度: 8)
- DROPPED_BYTES_TOTAL (長度: 8)
- BYTES (長度: 8)
- BYTES_TOTAL (長度: 8)
- BYTES_SQUARED (長度: 8)
- BYTES_SQUARED_PERMANENT (長度: 8)
- IP LENGTH MINIMUM (長度: 8)

- IP LENGTH MAXIMUM (長度: 8)
- MUL_DOCTETS (長度: 8)
- postMCastOctetTotalCount (長度: 8)

KVM 選項 IPFIX 範本

存在一個 KVM 選項範本，以 IETF RFC 7011 的第 3.4.2 節為基礎。

選項範本

範本識別碼: 462。範圍計數: 1。資料計數: 1。

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疊，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 從瀏覽器以管理員權限登入 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 > Traceflow**。
 - 選取導覽面板中的**交換**、按一下**連接埠**索引標籤，接著選取連結 VIF 的連接埠，然後按一下**動作 > 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 VMtools，或虛擬機器是透過 OpenStack 外掛程式來進行部署 (在此情況下，將使用位址繫結)，將顯示 IP 位址和 MAC 位址。如果虛擬機器具有一個以上的 IP 位址，請從下拉式功能表中選取其中一個。</p> <p>如果未顯示 IP 位址和 MAC 位址，請在文字方塊中輸入 IP 位址和 MAC 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"> ■ 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 IP 位址和 MAC 位址 ■ 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 IP 位址和 MAC 位址。如果追蹤類型是第 3 層，請輸入 IP 位址。
多點傳送	步驟同上。	輸入 IP 位址。必須是來自 224.0.0.0 - 239.255.255.255 的多點傳送位址。
廣播	步驟同上。	輸入子網路首碼長度。

- 5 (選擇性) 按一下**進階**以查看進階選項。
- 6 (選擇性) 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 (Base64、十六進位、純文字、二進位或十進位)

- 7 (選擇性) 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 (選擇性) 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 TCP 旗標。
UDP	輸入來源連接埠。	輸入目的地連接埠。	不適用
ICMP	輸入 ICMP ID。	輸入序列值。	不適用

- 9 按一下**追蹤**。

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**、**已傳送**、**已捨棄**)。如果有已捨棄的觀察結果，依預設會套用**已捨棄**篩選器。否則則會套用**全部**篩選器。圖形對應會顯示後擋板和路由器連結。請注意，不會顯示橋接資訊。

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**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

必要條件

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網路 > 交換**。
- 3 按一下**連接埠**索引標籤。
- 4 按一下連接埠的名稱。
- 5 按一下**監控**索引標籤。
此時會顯示連接埠狀態和統計資料。
- 6 若要下載主機已知的 MAC 位址的 CSV 檔案，請按一下**下載 MAC 資料表**。
- 7 若要監控連接埠上的活動，請按一下**開始追蹤**。

[連接埠追蹤] 頁面隨即開啟。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。

結果

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。

NSX Cloud 附註 如果使用 NSX Cloud，請參閱[如何搭配使用 NSX-T Data Center 功能與公有雲](#)以取得自動產生的邏輯實體、支援功能和 NSX Cloud 所需組態的清單。

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 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的 **工具 > 連接埠鏡像工作階段**。
- 3 按一下 **新增**，然後選取工作階段類型。
 可用的類型為 **本機 SPAN**、**遠端 SPAN**、**遠端 L3 SPAN**，以及 **邏輯 SPAN**。
- 4 輸入工作階段名稱，並選擇性地輸入說明。

5 提供其他參數。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 傳輸節點 - 選取傳輸節點。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。
遠端 SPAN	<ul style="list-style-type: none"> ■ 工作階段類型 - 選取 RSPAN 來源工作階段或 RSPAN 目的地工作階段。 ■ 傳輸節點 - 選取傳輸節點。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。 ■ 封裝 VLAN 識別碼 - 指定封裝 VLAN 識別碼。 ■ 保留原始 VLAN - 選取是否要保留原始 VLAN 識別碼。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 封裝 - 選取 GRE、ERSPAN II 或 ERSPAN III。 ■ GRE 機碼 - 如果封裝為 GRE，請指定 GRE 機碼。 ■ 傳輸節點 - 如果封裝為 ERSPAN II 或 ERSPAN III，請指定傳輸節點。 ■ ERSPAN 識別碼 - 如果封裝為 ERSPAN II 或 ERSPAN III，請指定 ERSPAN 識別碼。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 邏輯交換器 - 選取邏輯交換器。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。

6 按下一步。

7 提供來源資訊。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 選取 N-VDS。 ■ 選取實體介面。 ■ 啟用或停用封裝式封包。 ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。 ■ 選取邏輯交換器。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 選取邏輯連接埠。

8 按下一步。

9 提供目的地資訊。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 SPAN	<ul style="list-style-type: none"> ■ 選取 N-VDS。 ■ 選取實體介面。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 指定 IPv4 位址。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 選取邏輯連接埠。

10 按一下儲存。

儲存連接埠鏡像工作階段後，無法變更來源或目的地。

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、NSX Edge 叢集、橋接器以及傳輸節點。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**網狀架構 > 節點**。
- 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

結果

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。

檢視在虛擬機器上執行之應用程式的相關資料

您可以針對在 NSGroup 成員之虛擬機器上執行的應用程式檢視其相關資訊。此為技術預覽功能。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取導覽面板中的**詳細目錄 > 群組**。

- 3 按一下 NSGroup 的名稱。
- 4 按一下**應用程式索引**標籤。
- 5 按一下**收集應用程式資料**。

此處理程序可能需要幾分鐘時間。處理程序完成時會顯示下列資訊。

- 處理程序的總數。
- 代表各種不同階層的圓圈，例如 **Web** 層、資料庫層和應用程式層。此外也會顯示各階層中的處理程序數目。

- 6 按一下圓圈以查看該階層中處理程序的相關詳細資訊。

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。

NSX Cloud 附註 如果您想要收集 CSM 的支援服務包，請登入 CSM，移至**系統 > 公用程式 > 支援服務包**，然後按一下**下載**。可以使用下列指示從 NSX Manager 取得 PCG 的支援服務包。PCG 的支援服務包還包含所有工作負載虛擬機器的記錄。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 *https://nsx-manager-ip-address*。
- 2 選取導覽面板中的**系統 > 公用程式**。
- 3 按一下**支援服務包索引**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、主機和公用雲端閘道。

- 5 (選擇性) 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 (選擇性) 切換表示要包含或排除核心檔案和稽核記錄的交換器。

備註 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 (選擇性) 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**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**以下載服務包。

客戶經驗改進計劃

NSX-T Data Center 參與了 VMware 的客戶經驗改進計劃 (CEIP)。

如需有關透過 CEIP 收集之資料以及 VMware 使用此資料之目的的詳細資料，請參閱信任與保障中心，網址為：<https://www.vmware.com/solutions/trustvmware/ceip.html>。

若要加入或退出 NSX-T Data Center 的 CEIP，或要編輯計劃設定，請參閱[編輯客戶經驗改進計劃組態](#)。

編輯客戶經驗改進計劃組態

安裝或升級 NSX Manager 時，您可以決定加入 CEIP 並設定資料收集設定。

您也可以編輯現有的 CEIP 組態來加入或退出此計劃、定義收集資訊的頻率和天數，以及 Proxy 伺服器組態。

必要條件

- 確認 NSX Manager 已連線並且可與您的 Hypervisor 進行同步。
- 確認 NSX-T Data Center 已連線至公用網路以上傳資料。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
- 2 選取**系統 > 組態 > 內容**。
- 3 按一下 [狀態和統計資料] 區段中的**編輯**。
- 4 切換**資料收集**功能表項目。
- 5 按一下 [客戶經驗改進計劃] 區段中的**編輯**。
- 6 切換加入 **VMware 客戶經驗改進計劃**功能表項目。
- 7 (選擇性) 設定資料收集和上傳週期設定。
- 8 (選擇性) 按一下 **Proxy** 索引標籤。
- 9 切換 **Proxy** 功能表項目，設定 Proxy 伺服器設定以傳送資料。

選項	說明
主機名稱	輸入 Proxy 伺服器 FQDN 或 IP 位址。
連接埠	輸入 Proxy 伺服器連接埠。
使用者名稱	(選擇性) 輸入透過 Proxy 伺服器進行驗證所使用的使用者名稱。
密碼	(選擇性) 輸入透過 Proxy 伺服器進行驗證所使用的密碼。
配置	透過下拉式功能表設定 Proxy 伺服器接受的 HTTP 或 HTTPS 配置。

- 10 按一下**儲存**。