

NSX-T Data Center 管理指南

修改日期：2021 年 3 月 19 日
VMware NSX-T Data Center 2.4

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

Copyright © 2020 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 11

1 NSX Manager 概觀 12

2 第 0 層闡道 15

新增第 0 層闡道 15

建立 IP 首碼清單 17

建立社群清單 18

設定靜態路由 18

建立路由對應 19

設定 BGP 20

3 第 1 層闡道 23

新增第 1 層闡道 23

4 區段 25

區段設定檔 25

瞭解 QoS 區段設定檔 26

瞭解 IP 探索區段設定檔 28

瞭解 SpoofGuard 區段設定檔 29

瞭解區段安全性區段設定檔 30

瞭解 MAC 探索區段設定檔 31

新增區段 33

5 虛擬私人網路 (VPN) 35

瞭解 IPsec VPN 36

使用以原則為基礎的 IPsec VPN 36

使用以路由為基礎的 IPsec VPN 37

瞭解第 2 層 VPN 38

新增 VPN 服務 39

新增 IPsec VPN 服務 40

新增 L2 VPN 服務 41

新增 IPsec VPN 工作階段 44

新增以原則為基礎的 IPsec 工作階段 44

新增路由型 IPsec 工作階段 46

新增 L2 VPN 工作階段 49

新增 L2 VPN 伺服器工作階段 49

新增 L2 VPN 用戶端工作階段	51
下載遠端 L2 VPN 組態	52
新增本機端點	53
新增設定檔	54
新增 IKE 設定檔	54
新增 IPSec 設定檔	57
新增 DPD 設定檔	58
檢查 IPSec VPN 工作階段的實現狀態	59
監控和疑難排解 VPN 工作階段	62
6 網路位址轉譯	63
在閘道上設定 NAT	63
7 負載平衡	65
主要負載平衡器概念	65
調整負載平衡器資源	66
支援的負載平衡器功能	67
負載平衡器拓撲	68
設定負載平衡器元件	70
新增負載平衡器	70
新增主動監視器	72
新增被動監視器	75
新增伺服器集區	76
設定虛擬伺服器元件	79
8 轉送原則	99
新增或編輯轉送原則	100
9 IP 位址管理 (IPAM)	101
新增 DNS 區域	101
新增 DNS 轉寄站服務	102
新增 DHCP 伺服器	103
設定第 0 層或第 1 層閘道的 DHCP 轉送伺服器	104
新增 IP 位址集區	105
新增 IP 位址區塊	105
10 安全性	106
安全性組態概觀	106
安全性術語	107
身分識別防火牆	107
身分識別防火牆工作流程	108

第 7 層內容設定檔	110
第 7 層 Distributed Firewall 規則工作流程	111
應用程式識別 GUID	111
Distributed Firewall	115
新增分散式防火牆	115
新增防火牆規則以將 FQDN/URL 加入白名單	117
分散式防火牆封包記錄	118
選取預設的連線策略	121
設定閘道防火牆	121
新增閘道防火牆原則和規則	121
設定東西向網路自我檢查	123
東西向網路安全性的高階工作	123
東西向網路保護的主要概念	124
部署用於執行東西向流量自我檢查的服務	124
新增服務設定檔	125
新增服務鏈結	126
新增東西向流量的重新導向規則	127
設定南北向網路自我檢查	128
南北向網路安全性的高階工作	128
部署用於執行南北向流量自我檢查的服務	128
設定流量重新導向	130
針對南北向流量新增重新導向規則	131
監控流量重新導向	132
設定 Endpoint Protection	133
瞭解端點保護	133
端點保護工作流程	140
新增網域和虛擬機器群組	154
11 詳細目錄	164
新增網域	164
新增服務	165
新增群組	165
新增內容設定檔	167
12 監控	168
新增防火牆 IPFIX 設定檔	168
新增交換器 IPFIX 設定檔	169
新增 IPFIX 收集器	170
新增連接埠鏡像設定檔	170
進階監控工具	171
檢視連接埠連線資訊	171

Traceflow	171
監控連接埠鏡像工作階段	174
為連接埠鏡像工作階段設定篩選器	177
設定 IPFIX	178
監控邏輯交換器連接埠活動	351
監控網狀架構節點	352

13 邏輯交換器 353

瞭解 BUM 框架複寫模式	354
建立邏輯交換器	355
將虛擬機器連線到邏輯交換器	356
將 vCenter Server 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器	356
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	358
將 KVM 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器	363
建立邏輯交換器連接埠	364
測試第 2 層連線	364
為 NSX Edge 上行建立 VLAN 邏輯交換器	367
邏輯交換器和邏輯連接埠的交換設定檔	369
瞭解 QoS 交換設定檔	370
瞭解連接埠鏡像交換設定檔	372
瞭解 IP 探索交換設定檔	374
瞭解 SpoofGuard	375
瞭解交換器安全性交換設定檔	377
瞭解 MAC 管理交換設定檔	379
建立自訂設定檔與邏輯交換器之間的關聯	380
建立自訂設定檔與邏輯連接埠之間的關聯	381
第 2 層橋接	382
建立 ESXi 橋接器叢集	382
建立 Edge 橋接器設定檔	383
設定以 Edge 為基礎的橋接	383
建立第 2 層橋接器備份邏輯交換器	386

14 邏輯路由器 389

第 1 層邏輯路由器	389
建立第 1 層邏輯路由器	390
在第 1 層邏輯路由器上新增下行連接埠	392
在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠	393
在第 1 層邏輯路由器上設定路由通告	393
設定第 1 層邏輯路由器靜態路由	395
建立獨立的第 1 層邏輯路由器	397
第 0 層邏輯路由器	398

- 建立第 0 層邏輯路由器 400
- 連結第 0 層和第 1 層 401
- 針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器 403
- 新增回送路由器連接埠 406
- 在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠 406
- 設定靜態路由 407
- BGP 組態選項 411
- 在第 0 層邏輯路由器上設定 BFD 418
- 啟用第 0 層邏輯路由器上的路由重新分配 418
- 瞭解 ECMP 路由 421
- 建立 IP 首碼清單 424
- 建立社群清單 425
- 建立路由對應 426
- 設定轉送累計計時器 427

15 進階 NAT 428

- 網路位址轉譯 428
 - 第 1 層 NAT 429
 - 第 0 層 NAT 435
 - 自反 NAT 436

16 進階群組物件 439

- 建立 IP 集合 439
- 建立 IP 集區 440
- 建立 MAC 集合 440
- 建立 NSGroup 441
- 設定服務和服務群組 442
 - 建立 NSService 443
- 管理虛擬機器的標記 443

17 進階 DHCP 445

- DHCP 445
 - 建立 DHCP 伺服器設定檔 445
 - 建立 DHCP 伺服器 446
 - 將 DHCP 伺服器連結至邏輯交換器 447
 - 從邏輯交換器中斷連結 DHCP 伺服器 447
 - 建立 DHCP 轉送設定檔 447
 - 建立 DHCP 轉送服務 448
 - 將 DHCP 轉送服務新增至邏輯路由器連接埠 448
 - 刪除 DHCP 租用 448
- 中繼資料 Proxy 449

- 新增中繼資料 Proxy 伺服器 449
- 將中繼資料 Proxy 伺服器連結至邏輯交換器 450
- 將中繼資料 Proxy 伺服器與邏輯交換器中斷連結 450

18 進階 IP 位址管理 451

- 管理 IP 區塊 451
- 管理 IP 區塊的子網路 452

19 進階負載平衡 453

- 主要負載平衡器概念 454
- 設定負載平衡器元件 454
 - 建立負載平衡器 455
 - 設定主動健全狀況監視器 456
 - 設定被動健全狀況監視器 459
 - 新增用於負載平衡的伺服器集區 460
 - 設定虛擬伺服器元件 463

20 進階防火牆 482

- 防火牆區段和防火牆規則 482
 - 新增防火牆規則區段 482
 - 刪除防火牆規則區段 483
 - 啟用和停用區段規則 483
 - 啟用和停用區段記錄 484
 - 關於防火牆規則 484
 - 新增防火牆規則 485
 - 刪除防火牆規則 487
 - 編輯預設 Distributed Firewall 規則 488
 - 變更防火牆規則的順序 488
 - 篩選防火牆規則 489
 - 為邏輯交換器橋接器連接埠設定防火牆 489
 - 設定防火牆排除清單 490
 - 啟用和停用 Distributed Firewall 490
 - 新增或刪除邏輯路由器的防火牆規則 490
 - 使用 API 的 CPU 和記憶體使用率臨界值 491

21 作業和管理 495

- 查看組態變更的實現狀態 496
- 搜尋物件 499
- 新增計算管理程式 500
- 新增 Active Directory 501
- 新增 LDAP 伺服器 502

同步 Active Directory	503
管理使用者帳戶和角色型存取控制	503
變更使用者的密碼	503
重設應用裝置的密碼	504
驗證原則設定	507
從 vIDM 主機取得憑證指紋	508
設定 VMware Identity Manager 整合	508
NSX Manager、vIDM 和相關元件之間的時間同步	510
角色型存取控制	511
新增角色指派或主體身分識別	516
備份和還原 NSX Manager	518
設定備份	519
移除舊備份	520
列出可用的備份	520
還原備份	521
從 vCenter Server 移除 NSX-T Data Center 延伸	523
管理 NSX Manager 叢集	524
檢視 NSX Manager 叢集的組態和狀態	524
將 NSX Manager 重新開機	527
變更 NSX Manager 的 IP 位址	527
調整 NSX Manager 節點的大小	529
NSX-T Data Center 的多站台部署	529
設定應用裝置	533
新增授權金鑰並產生授權使用率報告	533
設定憑證	534
匯入憑證	534
建立憑證簽署要求檔案	535
匯入 CA 憑證	536
建立自我簽署的憑證	537
取代 NSX Manager 節點的憑證或 NSX Manager 叢集虛擬 IP	537
匯入憑證撤銷清單	538
設定 NSX Manager 以擷取憑證撤銷清單	539
匯入 CSR 的憑證	540
公用憑證和私密金鑰的儲存區	540
收集支援服務包	540
記錄訊息	541
設定遠端記錄	542
記錄訊息識別碼	543
客戶經驗改進計劃	545
編輯客戶經驗改進計劃組態	545
將標籤新增至物件	546

尋找遠端伺服器的 SSH 指紋	546
檢視在虛擬機器上執行之應用程式的相關資料	547

22 使用 NSX Cloud 548

Cloud Service Manager	548
雲端	548
系統	550
管理隔離原則	552
如何啟用或停用隔離原則	553
停用時的隔離原則影響	554
啟用時的隔離原則影響	555
公有雲的 NSX Cloud 安全群組	556
工作負載虛擬機器上線及管理概觀	557
如何將工作負載虛擬機器上線及進行管理	557
工作負載虛擬機器上線	558
支援的作業系統	558
標記公有雲中的虛擬機器	558
安裝 NSX 代理程式	559
自動安裝 NSX 代理程式	562
管理工作負載虛擬機器	563
NSX 管理的工作負載虛擬機器的 DFW 規則	563
使用 NSX-T Data Center 和公有雲標記分組虛擬機器	563
針對工作負載虛擬機器設定微分割	566
如何搭配使用 NSX-T Data Center 功能與公有雲	567
使用進階 NSX Cloud 功能	568
確認 NSX Cloud 元件	568
在 NSX 管理的虛擬機器上啟用 NAT	569
產生可複製的映像	569
針對公有雲的服務插入	570
啟用 Syslog 轉送	576
常見問題集	577
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？	577
如果無法存取我的工作負載虛擬機器，該怎麼辦？	577

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、設定 NAT、防火牆、SpoofGuard、分組和 DHCP。此外也說明如何設定 NSX Cloud。

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 <https://www.vmware.com/topics/glossary>。

NSX Manager 概觀

1

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

NSX Manager Web 介面提供了兩種用來設定資源的方法。

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

原則或進階介面的使用時機

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

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

表 1-1. 原則或進階介面的使用時機


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

表 1-1. 原則或進階介面的使用時機 (續)

原則介面	進階介面
<p>僅在原則介面中可用的網路功能：</p> <ul style="list-style-type: none"> ■ DNS 服務和 DNS 區域 ■ VPN ■ NSX Cloud 的轉送原則 	<p>僅在進階介面中可用的網路功能：</p> <ul style="list-style-type: none"> ■ IPv4 和 IPv6 的第 3 層轉送 ■ 轉送累計計時器 ■ 變更內部傳送網路 IP ■ 第 0 層的 VIP HA 支援 ■ 待命重新放置 ■ 根據第 1 層上的首碼清單的路由通告篩選 ■ 回送建立 ■ BGP MultiHop ■ BGP 來源位址 ■ 以 BFD 和介面作為下一個躍點的靜態路由 ■ 中繼資料 Proxy ■ 連結至隔離區段和靜態繫結的 DHCP 伺服器
<p>僅在原則介面中可用的安全性功能：</p> <ul style="list-style-type: none"> ■ 端點保護 ■ 網路自我檢查 (東西向服務插入) ■ 內容設定檔 <ul style="list-style-type: none"> ■ L7 應用程式 ■ FQDN ■ 新增分散式防火牆和閘道防火牆配置 <ul style="list-style-type: none"> ■ 類別 ■ 自動服務規則 	<p>僅在進階介面中可用的安全性功能：</p> <ul style="list-style-type: none"> ■ 能夠啟用或停用分散式防火牆、身分識別防火牆和閘道防火牆 ■ 分散式防火牆工作階段計時器 ■ 排除清單 ■ CPU 和記憶體臨界值 ■ 無狀態規則的區段 ■ 橋接防火牆 ■ 區段鎖定 ■ 分散式防火牆規則識別碼 ■ 根據來源和目的地中 IP 所建立的分散式防火牆規則

使用原則介面

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

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

哪裡可以找到原則介面和進階介面

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

表 1-2. 原則介面和進階介面

原則介面	進階介面
<ul style="list-style-type: none"> ■ 網路索引標籤 ■ 安全性索引標籤 ■ 詳細目錄索引標籤 ■ 計劃和疑難排解索引標籤 	進階網路與安全性索引標籤
以 /policy/api 開頭的 API URI	以 /api 開頭的 API URI

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

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

在原則介面和進階介面中所建立物件的名稱

您所建立的物件會根據用來建立物件的介面而有不同的名稱。

表 1-3. 物件名稱

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

第 0 層閘道

2

第 0 層閘道會執行第 0 層邏輯路由器的功能。它負責處理邏輯網路和實體網路之間的流量。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

Edge 節點僅支援一個第 0 層閘道或邏輯路由器。在建立第 0 層閘道或邏輯路由器時，請確定您建立的第 0 層閘道或邏輯路由器數目並未超過 NSX Edge 叢集中的 Edge 節點數目。

備註 在[進階網路與安全性](#)索引標籤中，第 0 層邏輯交換器一詞是指第 0 層閘道。

本章節討論下列主題：

- [新增第 0 層閘道](#)
- [建立 IP 首碼清單](#)
- [建立社群清單](#)
- [設定靜態路由](#)
- [建立路由對應](#)
- [設定 BGP](#)

新增第 0 層閘道

第 0 層閘道具有與第 1 層閘道的下行連線和與實體網路的上行連線。

您可以將第 0 層閘道的 HA (高可用性) 模式設定為主動-主動式或主動-待命。下列服務僅在主動-待命模式中受到支援：

- NAT
- 負載平衡
- 可設定狀態的防火牆
- VPN

第 0 層和第 1 層閘道在單一階層和多層拓撲中支援所有介面 (上行、服務連接埠和下行) 的下列定址組態：

- 僅限 IPv4
- 僅限 IPv6
- 雙重堆疊 - IPv4 和 IPv6 兩者

若要使用 IPv6 或雙堆疊定址，請在**網路 > 網路設定 > 全域網路組態**中啟用 **IPv4** 和 **IPv6** 作為第 3 層轉送模式。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網路 > 第 0 層閘道**。
- 3 按一下**新增第 0 層閘道**。
- 4 輸入閘道的名稱。
- 5 (必要) 選取高可用性模式。

預設值為主動-主動式。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。

重要 建立閘道後，HA 模式即無法變更。

- 6 如果 HA 模式為主動-待命，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。
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 選取 NSX Edge 叢集。
- 8 按一下**儲存**。
- 9 若要設定路由重新分配，請按一下**路由重新分配和設定**。

選取一或多個來源：

- 第 0 層子網路：**靜態路由、NAT、IPSec 本機 IP、DNS 轉寄站 IP、服務介面子網路、外部介面子網路、已連線的區段**。
- 通告的第 1 層子網路：**DNS 轉寄站 IP、靜態路由、LB VIP、已連線的子網路、NAT、LB SNAT**。

- 10 若要設定介面，請按一下**介面和設定**。
 - a 按一下**新增介面**。
 - b 以 CIDR 格式輸入名稱和 IP 位址。

- c 選取區段。
 - d 選取 NSX Edge 節點。
 - e (選擇性) 變更 MTU 值，並新增標籤。
- 11 按一下**路由**以新增 IP 首碼清單、社群清單、靜態路由和路由對應。
 - 12 按一下 **BGP** 以設定 BGP。
 - 13 (選擇性) 按一下**進階組態**，移至**進階網路與安全性 > 路由器**頁面，以進行其他設定。

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。您也可以在此 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 層閘道。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**網路 > 第 0 層閘道**。
- 3 若要編輯第 0 層閘道，請按一下功能表圖示 (三個點)，然後選取**編輯**。
- 4 按一下**路由**。
- 5 按一下 **IP 首碼清單**旁的**設定**。
- 6 按一下**新增 IP 首碼清單**。
- 7 輸入 IP 首碼清單的名稱。
- 8 按一下**設定**以新增 IP 首碼。
- 9 按一下**新增首碼**。
 - a 以 CIDR 格式輸入 IP 位址。
例如，192.168.100.3/27。
 - b (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。

- c 從下拉式功能表中選取**拒絕或允許**。
 - d 按一下**新增**。
- 10 重複先前的步驟來指定其他首碼。
- 11 按一下**儲存**。

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。

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 > 第 0 層閘道**。
- 3 若要編輯第 0 層閘道，請按一下功能表圖示 (三個點)，然後選取**編輯**。
- 4 按一下**路由**。
- 5 按一下**社群清單**旁邊的**設定**。
- 6 按一下**新增社群清單**。
- 7 輸入社群清單的名稱。
- 8 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，您可以選取一或多個下列項目：

- 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

- 9 按一下**儲存**。

設定靜態路由

您可以設定第 0 層閘道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 層閘道會自動具有通往其已連線第 0 層閘道的靜態預設路由。

支援遞迴靜態路由。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**網路 > 第 0 層閘道**。
- 3 若要編輯第 0 層閘道，請按一下功能表圖示 (三個點)，然後選取**編輯**。
- 4 按一下**路由**。

- 5 按一下**靜態路由**旁邊的**設定**。
- 6 按一下**新增靜態路由**。
- 7 以 CIDR 格式輸入名稱和網路位址。支援以 IPv6 為基礎的靜態路由。IPv6 首碼只能有 IPv6 下一個躍點。
- 8 按一下**設定下一個躍點**以新增下一個躍點資訊。
- 9 按一下**新增下一個躍點**。
- 10 輸入 IP 位址。
- 11 指定管理距離。
- 12 從下拉式清單中選取介面。
- 13 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](#)。

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。

路由對應可在 BGP 芳鄰層級上和路由重新分配中提供參考。

必要條件

- 確認已設定 IP 首碼清單或社群清單。請參閱[建立 IP 首碼清單](#)或[建立社群清單](#)。

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**網路 > 第 0 層**開道。
- 3 若要編輯第 0 層開道，請按一下功能表圖示 (三個點)，然後選取**編輯**。
- 4 按一下**路由**。
- 5 按一下**路由對應**旁邊的**設定**。
- 6 按一下**新增路由對應**。
- 7 輸入名稱，然後按一下**設定**以新增符合準則。
- 8 按一下**新增符合準則**，以新增一或多個符合準則。

9 針對每個準則選取 IP 首碼或社群清單，然後按一下設定以指定一或多個比對運算式。

- a 如果選取了**社群清單**，請指定配對運算式以定義如何配對社群清單的成員。對於各個社群清單，有下列配對選項可供使用：

- **符合任意項目** - 如果社群清單中有任何社群相符，則會在路由對應中執行設定動作。
- **符合全部項目** - 如果社群清單中的所有社群都相符 (無論順序為何)，則會在路由對應中執行設定動作。
- **完全相符** - 如果社群清單中的所有社群都相符，且順序完全相同，則會在路由對應中執行設定動作。
- **符合 REGEX** - 如果所有與 NRLI 相關聯的社群都符合規則運算式，則會在路由對應中執行設定的動作。

對於任何符合準則，皆應以 **AND** 作業套用比對運算式，這表示必須滿足所有比對運算式才會有相符項目。如果有多個符合準則，則這些準則將會以 **OR** 作業套用，這表示只要滿足任何一個符合準則便會有相符項目。

10 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 格式指定社群清單，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
本機喜好設定	使用此值以選擇輸出外部 BGP 路徑。最好使用具有最高值的路徑。

11 在 [動作] 資料行中，選取允許或拒絕。

您可以允許或拒絕依 IP 首碼清單或社群清單比對的 IP 位址進行通告。

12 按一下儲存。

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 層閘道與實體基礎結構中之路由器之間的外部 BGP (eBGP) 連線。

設定 BGP 時，必須設定第 0 層閘道的本機自發系統 (AS) 數目。支援 BGP 多重躍點。

單一躍點和多重躍點支援 BGPv6。BGPv6 芳鄰僅支援 IPv6 位址。IPv6 首碼支援重新分配、首碼清單和路由對應。

雙主動模式下的第 0 層閘道支援 SR (服務路由器) 間的 iBGP。如果閘道 #1 無法與北向實體路由器通訊，則流量會重新路由至雙主動叢集中的閘道 #2。如果閘道 #2 能夠與實體路由器通訊，則閘道 #1 與實體路由器之間的流量不會受到影響。

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 > 第 0 層閘道**。
- 3 若要編輯第 0 層閘道，請按一下功能表圖示 (三個點)，然後選取**編輯**。
- 4 按一下 **BGP**。
 - a 輸入本機 AS 數目。
 - b 按一下 **BGP** 切換按鈕以啟用或停用 BGP。
 - c 如果此閘道處於雙主動模式，則按一下 **SR 間 iBGP** 切換按鈕以啟用或停用 SR 間 iBGP。
 - d 按一下 **ECMP** 切換按鈕以啟用或停用 ECMP。
 - e 按一下**多重路徑放鬆**切換按鈕以啟用或停用多重路徑 (僅在 AS 路徑屬性值中不同，但具有相同的 AS 路徑長度) 之間的負載共用。

備註 必須啟用 **ECMP**，**多重路徑放鬆**才能運作。

- f 按一下**正常重新啟動**切換按鈕以啟用或停用正常重新啟動。
僅在與第 0 層閘道相關聯的 NSX Edge 叢集只有一個 Edge 節點時才支援正常重新啟動。
- 5 透過新增 IP 位址首碼，設定**路由彙總**。
 - a 按一下**新增首碼**。
 - b 以 CIDR 格式輸入 IP 位址首碼。
 - c 針對選項**僅限摘要**，選取**是或否**。
- 6 設定 **BGP 芳鄰**。
 - a 輸入芳鄰的 IP 位址。
 - b 啟用或停用 BFD。
 - c 請輸入遠端 AS 數目。
 - d 設定輸出篩選器。
 - e 設定輸入篩選器。
 - f 啟用或停用 **Allowas-in** 功能。
依預設會停用此功能。啟用這項功能後，BGP 芳鄰可接收具有相同 AS 的路由，例如，當您具有使用相同服務供應商互連的兩個位置時。此功能適用於所有位址家族，並且無法套用至特定的位址家族。
 - g 按一下**計時器與密碼**。

h 輸入 **BFD 時間間隔** 的值。

i 輸入 **BFD 乘數** 的值。

j 輸入 **保持關閉時間** 的值。

k 輸入 **保持運作時間** 的值。

l 輸入密碼。

如果您在 BGP 對等之間設定 MD5 驗證，則此為必填。

7 按一下**儲存**。

第 1 層閘道

3

第 1 層閘道會執行第 1 層邏輯路由器的功能。它具有區段的下行連線以及第 0 層閘道的上行連線。

備註 在[進階網路與安全性](#)索引標籤中，第 1 層邏輯交換器一詞是指第 1 層閘道。

您可以在第 1 層閘道上設定路由通告和靜態路由。支援遞迴靜態路由。

本章節討論下列主題：

- [新增第 1 層閘道](#)

新增第 1 層閘道

第 1 層閘道通常以北向方向連線至第 0 層閘道，並以南向方向連線至區段。

第 0 層和第 1 層閘道在單一階層和多層拓撲中支援所有介面 (上行、服務連接埠和下行) 的下列定址組態：

- 僅限 IPv4
- 僅限 IPv6
- 雙重堆疊 - IPv4 和 IPv6 兩者

若要使用 IPv6 或雙堆疊定址，請在[網路 > 網路設定 > 全域網路組態](#)中啟用 **IPv4** 和 **IPv6** 作為第 3 層轉送模式。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取[網路 > 第 1 層閘道](#)。
- 3 按一下[新增第 1 層閘道](#)。
- 4 輸入閘道的名稱。
- 5 (選擇性) 選取要連線至這個第 1 層閘道的第 0 層閘道，以建立多層拓撲。

6 選取容錯移轉模式。

選項	說明
先佔式	若偏好的 NSX Edge 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 NSX Edge 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 (選擇性) 如果您想要讓這個第 1 層閘道主控可設定狀態的服務 (NAT、LB、FW)，請選取 **NSX Edge** 叢集。

如果選取 **NSX Edge** 叢集，則一律會建立服務路由器 (即使您未設定可設定狀態的服務)，因而影響南北向流量模式。

8 (選擇性) 選取 **NSX Edge** 節點。

9 按一下**儲存**。

10 (選擇性) 按一下**路由通告**。

選取一或多個下列項目：

- 所有靜態路由
- 所有 **NAT IP** 的
- 所有 **DNS** 轉寄站路由
- 所有 **LB VIP** 路由
- 所有已連線的區段和服務連接埠
- 所有 **LB SNAT IP** 路由

11 (選擇性) 依序按一下**服務介面**和**設定**，以設定區段的連線。在某些拓撲中為必要，例如支援 **VLAN** 的區段或單一裝載負載平衡。

- a 按一下**新增介面**。
- b 以 **CIDR** 格式輸入名稱和 **IP** 位址。
- c 選取區段。
- d 按一下**儲存**。

12 (選擇性) 依序按一下**靜態路由**和**設定**，以設定靜態路由。

- a 按一下**新增靜態路由**。
- b 以 **CIDR** 或 **IPv6 CIDR** 格式輸入名稱和網路位址。
- c 按一下**設定下一個躍點**以新增下一個躍點資訊。
- d 按一下**儲存**。

區段會執行邏輯交換器的功能。

備註 在**進階網路與安全性**索引標籤中，邏輯交換器一詞是指區段。

本章節討論下列主題：

- [區段設定檔](#)
- [新增區段](#)

區段設定檔

區段設定檔包含區段和區段連接埠的第 2 層網路組態詳細資料。NSX Manager 支援數種類型的區段設定檔。

可供使用的區段設定檔類型如下：

- QoS (服務品質)
- IP 探索
- SpoofGuard
- 區段安全性
- MAC 管理

備註 您無法編輯或刪除預設區段設定檔。如果您需要來自預設區段設定檔的其他設定，您可以建立自訂區段設定檔。依預設，所有自訂區段設定檔 (區段安全性設定檔除外) 將繼承適當的預設區段設定檔的設定。例如，依預設，自訂 IP 探索區段設定檔將具有與預設 IP 探索區段設定檔相同的設定。

每個預設或自訂區段設定檔皆有唯一的識別碼。您可以使用此識別碼將區段設定檔與區段或區段連接埠建立關聯。

區段或區段連接埠只能與每種類型的一個區段設定檔建立關聯。例如，您不能將兩個 QoS 區段設定檔關聯至一個區段或區段連接埠。

如果您在建立區段時未關聯區段設定檔，NSX Manager 將關聯對應的預設系統定義區段設定檔。子區段連接埠會繼承父區段交換器的預設系統定義區段設定檔。

在建立或更新區段或區段連接埠時，您可以選擇關聯預設或自訂區段設定檔。當區段設定檔與區段建立關聯或解除關聯時，系統會根據下列準則套用子區段連接埠的區段設定檔。

- 如果父區段具有與其相關聯的設定檔，則子區段連接埠會繼承其父系的區段設定檔。
- 如果父區段沒有與其相關聯的區段設定檔，則系統會對區段指派預設區段設定檔，且區段連接埠會繼承該預設區段設定檔。
- 如果您明確地關聯自訂設定檔與區段連接埠，則此自訂設定檔會覆寫現有的區段設定檔。

備註 如果您已將自訂區段設定檔與區段建立關聯，但想讓其中一個子區段連接埠保留預設區段設定檔，則必須複製預設區段設定檔，並讓此設定檔與特定的區段連接埠建立關聯。

如果自訂區段設定檔關聯到區段或區段連接埠，則無法刪除該設定檔。您可以前往 [摘要] 視圖的 [指派至] 區段，然後按一下列出的區段和區段連接埠，以瞭解是否有任何區段和區段連接埠與自訂區段設定檔建立關聯。

瞭解 QoS 區段設定檔

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區段中緩衝流量時，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 設定或在區段層級修改並設定 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區段所允許的高載流量，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區段並由子區段連接埠繼承。

建立 QoS 區段設定檔

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 **網路 > 區段 > 區段設定檔**。
- 3 按一下 **新增區段設定檔**，然後選取 **QoS**。
- 4 完成 QoS 交換設定檔詳細資料。

選項	說明
名稱	設定檔的名稱。
模式	<p>從 [模式] 下拉式功能表中選取 信任 或 未受信任 選項。</p> <p>當您選取「受信任」模式，內部標頭 DSCP 值會套用至 IP/IPv6 流量的外部 IP 標頭。針對非 IP/IPv6 流量，外部 IP 標頭會採用預設值。以覆疊為基礎的邏輯連接埠上支援信任模式。預設值為 0。</p> <p>以覆疊為基礎及以 VLAN 為基礎的邏輯連接埠上支援未受信任模式。針對以覆疊為基礎的邏輯連接埠，輸出 IP 標頭的 DSCP 值會設為與邏輯連接埠內部封包類型無關的設定值。針對以 VLAN 為基礎的邏輯連接埠，IP/IPv6 封包的 DSCP 值會設為設定值。未受信任模式的 DSCP 值範圍介於 0 至 63 之間。</p> <p>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。</p>
優先順序	<p>設定 CoS 優先順序值。</p> <p>優先順序值範圍從 0 至 63，其中 0 具有最高的優先順序。</p>
服務類別	<p>設定 CoS 值。</p> <p>以 VLAN 為基礎的邏輯連接埠上支援 CoS。CoS 會分組網路中的類似流量類型，且每個流量類型會根據其本身的服務優先順序層級而視為一個類別。較低優先順序的流量會變慢或在某些情況下會捨棄，可提供較佳的輸送量以處理較高優先順序的流量。CoS 也可以使用 0 封包針對 VLAN 識別碼進行設定。</p> <p>CoS 值範圍從 0 至 7，其中 0 是優先順序最低的服務。</p>
入口	<p>設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>您可以使用平均頻寬來降低網路壅塞。尖峰頻寬速率用來支援高載流量，而高載大小會基於使用尖峰頻寬的持續時間。您可以在高載大小設定中設定高載持續時間。您無法保證頻寬。但是，您可以使用平均、尖峰和高載大小設定來限制網路頻寬。例如，如果平均頻寬為 30 Mbps，尖峰頻寬為 60 Mbps，而允許的持續時間為 0.1 秒，則高載大小為 $60 * 1000000 * 0.10/8 = 750000$ 位元組。</p> <p>預設值為 0 會停用入口流量的速率限制。</p>
入口廣播	<p>根據廣播設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>例如，當您將邏輯交換器的平均頻寬設定為 3000 Kbps，尖峰頻寬為 6000 Kbps，而允許的持續期間為 0.1 秒，則高載大小為 $6000 * 1000 * 0.10/8 = 75000$ 位元組。</p> <p>預設值為 0 會停用入口廣播流量的速率限制。</p>
出口	<p>設定從邏輯網路至虛擬機器的輸入網路流量自訂值。</p> <p>預設值為 0 會停用出口流量的速率限制。</p>

如果並未設定入口、入口廣播及出口選項，則會使用預設值。

- 5 按一下 **儲存**。

瞭解 IP 探索區段設定檔

IP 探索使用 DHCP 和 DHCPv6 窺探、ARP (位址解析通訊協定) 窺探、ND (芳鄰探索) 窺探，以及 VM Tools 來學習 MAC 和 IP 位址。

探索到的 MAC 和 IP 位址用於實現 ARP/ND 隱藏，以最大限度地減少連線至相同區段的虛擬機器之間的流量。SpoofGuard 和 Distributed Firewall (DFW) 元件也會使用這些位址。DFW 使用位址繫結來判斷防火牆規則中物件的 IP 位址。

DHCP/DHCPv6 窺探會檢查在 DHCP/DHCPv6 用戶端和伺服器之間交換的 DHCP/DHCPv6 封包，以學習 IP 和 MAC 位址。

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

VM Tools 是一種在 ESXi 主控虛擬機器執行上的軟體，可提供包括 MAC 和 IP 或 IPv6 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。

ND 窺探是 ARP 窺探的對等 IPv6。它會檢查芳鄰請求 (NS) 和芳鄰通告 (無) 訊息，以學習 IP 和 MAC 位址。

重複位址偵測會檢查其他連接埠已實現繫結清單上是否已有新探索到的 IP 位址。會針對同一區段上的連接埠執行此檢查。如果偵測到重複的位址，新探索到的位址就會新增至探索到的清單，但不會新增至實現的繫結清單。所有重複的 IP 都具有相關聯的探索時間戳記。如果藉由將實現繫結清單上的 IP 新增至略過繫結清單或停用窺探來移除此 IP (如下所示)，則具有最舊時間戳記的重複 IP 將會移至實現的繫結清單中。可透過 API 呼叫取得重複位址資訊。

依預設，探索方法 ARP 窺探和 ND 窺探會在名為「首次使用時信任 (TOFU)」的模式下運作。在 TOFU 模式中，在探索到位址並將其新增至實現的繫結清單時，該繫結會永久保留在實現的清單中。TOFU 會套用至使用 ARP/ND 窺探探索到前「n」個唯一的 <IP、MAC、VLAN> 繫結，其中「n」是您設定的繫結限制。您可以針對 ARP/ND 窺探停用 TOFU。隨後，這些方法將會在「每次使用皆信任 (TOEU)」模式中運作。在 TOEU 模式中，在探索到某個位址時，系統即會將其新增至實現的繫結清單中，並在該位址刪除或到期後，將其從實現的繫結清單中移除。DHCP 窺探和 VM Tools 方法一律會在 TOEU 模式中運作。

備註 TOFU 並不同於 SpoofGuard，它不會像 SpoofGuard 一樣封鎖流量。如需 SpoofGuard 的詳細資訊，請參閱[瞭解 SpoofGuard 區段設定檔](#)。

對於每個連接埠，NSX Manager 會維護略過繫結清單，其中包含無法繫結至連接埠的 IP 位址。只能使用 API 更新此清單。您也可以藉由導覽使用此方法以刪除之前針對指定連接埠探索到的 IP。如需詳細資訊，請參閱《NSX-T API 參考》並搜尋 ignore_address_bindings

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>。

建立 IP 探索區段設定檔

NSX-T Data Center 提供多個預設的 IP 探索交換設定檔。您也可以另外建立 IP 探索交換設定檔。

必要條件

自行熟悉 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**網路 > 區段 > 區段設定檔**。
- 3 按一下**新增區段設定檔**，然後選取 **IP 探索**。
- 4 指定 IP 探索交換設定檔詳細資料。

選項	說明
名稱	輸入名稱。
ARP 窺探	適用於 IPv4 環境。適用於具有靜態 IP 位址的虛擬機器。
ARP 繫結限制	可繫結至連接埠的 IPv4 IP 位址數目上限。
ARP ND 繫結限制逾時	在 TOFU 已停用的情況下，ARP/ND 繫結資料表中 IP 位址的逾時值 (以分鐘為單位)。如果位址逾時，新探索到的位址會將其取代。
DHCP 窺探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP V6 窺探	適用於 IPv6 環境。適用於具有 IPv6 位址的虛擬機器。
VM Tools	僅適用於裝載 ESXi 的虛擬機器。
IPv6 的 VM Tools	僅適用於裝載 ESXi 的虛擬機器。
芳鄰探索窺探	適用於 IPv6 環境。適用於具有靜態 IP 位址的虛擬機器。
芳鄰探索繫結限制	可繫結至連接埠的 IPv6 位址數目上限。
首次使用時信任	適用於 ARP 和 ND 窺探。
重複的 IP 偵測	適用於所有窺探方法及 IPv4 和 IPv6 環境。

- 5 按一下**儲存**。

瞭解 SpoofGuard 區段設定檔

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區段位址繫結的 IP 位址，系統即會完全阻止虛擬機器的 vNIC 存取網路。您可以在連接埠或區段層級設定 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。

在區段層級中，系統會透過區段的位址繫結內容提供允許的 MAC/VLAN/IP 白名單。這通常是區段的允許 IP 範圍/子網路，並由區段層級 SpoofGuard 負責處理流量授權。

流量必須獲得連接埠層級和區段層級 SpoofGuard 的允許，才能允許進入區段。連接埠和區段層級 SpoofGuard 的啟用或停用可使用 SpoofGuard 區段設定檔來控制。

建立 SpoofGuard 區段設定檔

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/區段位址繫結使用新的 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**網路 > 區段 > 區段設定檔**。
- 3 按一下**新增區段設定檔**，然後選取 **SpoofGuard**。
- 4 輸入名稱。
- 5 若要啟用連接埠層級 SpoofGuard，請將**連接埠繫結**設為已啟用。
- 6 按一下**儲存**。

瞭解區段安全性區段設定檔

區段安全性可透過檢查區段的入口流量，以及將 IP 位址、MAC 位址和通訊協定與一組允許的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。您可以使用區段安全性，篩除來自網路中虛擬機器的惡意攻擊，藉以保護區段的完整性。

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，來自訂區段上的區段安全性區段設定檔。

建立區段安全性區段設定檔

您可以使用來自允許 BPDU 清單的 MAC 目的地位址，建立自訂區段安全性區段設定檔並設定速率限制。

必要條件

自行熟悉區段安全性區段設定檔概念。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**網路 > 區段 > 區段設定檔**。
- 3 按一下**新增區段設定檔**，然後選取**區段安全性**。
- 4 完成區段安全性設定檔詳細資料。

選項	說明
名稱	設定檔的名稱。
BPDU 篩選器	<p>切換 BPDU 篩選器 按鈕以啟用 BPDU 篩選。依預設為停用狀態。</p> <p>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。</p>
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。您必須啟用 BPDU 篩選器 ，才能從此清單中選取。
DHCP 篩選器	<p>切換伺服器封鎖按鈕及用戶端封鎖按鈕以啟用 DHCP 篩選。依預設會停用這兩者。</p> <p>「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。</p> <p>「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。</p>
DHCPv6 篩選器	<p>切換 V6 伺服器封鎖 按鈕及 V6 用戶端封鎖 按鈕以啟用 DHCP 篩選。依預設會停用這兩者。</p> <p>「DHCPv6 伺服器封鎖」會封鎖 DHCPv6 伺服器至 DHCPv6 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。將會篩選 UDP 來源連接埠號碼為 547 的封包。</p> <p>「DHCPv6 用戶端封鎖」會封鎖 DHCP 要求，以防止虛擬機器取得 DHCP IP 位址。將會篩選 UDP 來源連接埠號碼為 546 的封包。</p>
封鎖非 IP 流量	<p>切換封鎖非 IP 流量 按鈕以僅允許 IPv4、IPv6、ARP 和 BPDU 流量。</p> <p>系統會封鎖剩餘的非 IP 流量。允許的 IPv4、IPv6、ARP、GARP 和 BPDU 流量是根據位址繫結及 SpoofGuard 組態中所設定的其他原則而定。</p> <p>依預設，系統會停用此選項以允許非 IP 流量以一般流量方式處理。</p>
RA 保護	切換 RA 保護 按鈕，以篩選出入口 IPv6 路由器通告。ICMPv6 類型 134 封包將被篩選掉。此選項依預設為啟用。
速率限制	<p>設定廣播及多點傳播流量的速率限制。此選項依預設為啟用。</p> <p>速率限制可用來保護邏輯交換器或虛擬機器免於遭受廣播風暴等事件。</p> <p>若要避免任何連線問題，最低速率限制值必須 ≥ 10 pps。</p>

- 5 按一下**儲存**。

瞭解 MAC 探索區段設定檔

MAC 管理區段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 連線至區段連接埠時，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。此期間不可設定。**MAC 學習使用期限時間**欄位會顯示預先定義的值，即 600。

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

您可以設定可學習的 MAC 位址數目。最大值為 4096，這是預設值。您也可以設定何時達到限制的原則。選項包括：

- **捨棄** - 捨棄來自未知來源 MAC 位址的封包。輸入至此 MAC 位址的封包將視為未知的單點傳播。連接埠只有在已啟用未知單點傳播洪泛時才會接收封包。
- **允許** - 來自未知來源 MAC 位址的封包會進行轉送，但無法學習位址。輸入至此 MAC 位址的封包將視為未知的單點傳播。連接埠只有在已啟用未知單點傳播洪泛時才會接收封包。

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。

建立 MAC 探索區段設定檔

您可以建立 MAC 探索區段設定檔來管理 MAC 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 **網路 > 區段 > 區段設定檔**。
- 3 按一下 **新增區段設定檔**，然後選取 **MAC 探索**。
- 4 完成 MAC 探索設定檔詳細資料。

選項	說明
名稱	設定檔的名稱。
MAC 變更	啟用或停用 MAC 位址變更功能。預設值為已停用。
MAC 學習	啟用或停用 MAC 學習功能。預設值為已停用。
MAC 限制原則	選取 允許 或 捨棄 。預設為 允許 。如果啟用 MAC 學習，則可使用此選項。
未知單點傳播洪泛	啟用或停用未知單點傳播洪泛功能。預設值為已啟用。如果啟用 MAC 學習，則可使用此選項。

選項	說明
MAC 限制	設定 MAC 位址的數目上限。預設值為 4096。如果啟用 MAC 學習，則可使用此選項。
MAC 學習使用期限時間	僅供參考之用。此選項無法設定。預先定義的值為 600。

5 按一下**儲存**。

新增區段

區段可連線至閘道和虛擬機器。區段會執行邏輯交換器的功能。

如需如何尋找虛擬機器之 VIF 識別碼的相關資訊，請參閱[將虛擬機器連線到邏輯交換器](#)。

備註 在增強型資料路徑模式中設定的 N-VDS 交換器支援 IP 探索、SpoofGuard 和 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**網路 > 區段**。

3 按一下**新增**。

4 輸入區段的名稱。

5 選取上行。

您可以選取現有的第 0 層或第 1 層閘道，或選取**無**。如果選取**無**，代表區段只是邏輯交換器。透過設定子網路，其可連結至第 0 層或第 1 層閘道。

6 如果上行是第 1 層閘道，請選取類型：**彈性**或**固定**。

彈性區段可以從閘道取消連結。固定區段可以刪除，但無法從閘道取消連結。

7 按一下**設定子網路**以指定子網路。

8 選取傳輸區域。

9 如果傳輸區域的類型是 VLAN，請指定 VLAN 識別碼的清單。

10 按一下**儲存**。

11 依序按一下**連接埠**和**設定**，以新增區段連接埠。

a 按一下**新增區段連接埠**。

b 輸入連接埠名稱。

c 對於**識別碼**，請輸入虛擬機器的 VIF UUID 或連線至此連接埠的伺服器。

d 選取類型：**父系**、**子系**或**獨立**。

除了像是容器或 VMware HCX 等使用案例外，請將此欄位保留空白。如果此連接埠用於虛擬機器中的容器，請選取**子系**。如果此連接埠用於容器主機虛擬機器，請選取**父系**。如果此連接埠用於裸機容器或伺服器，請選取**獨立**。

e 輸入內容識別碼。

如果**類型**為**子系**，請輸入父系 VIF 識別碼，如果**類型**為**獨立**，則輸入傳輸節點識別碼。

f 輸入流量標籤。

輸入容器和其他使用案例中的 VLAN 識別碼。

g 選取位址配置方法：**IP 集區**、**MAC 集區**、**兩者**或**無**。

h 指定標籤。

i 選取此連接埠的區段設定檔。

12 按一下**區段設定檔**以選取區段設定檔。

13 按一下**儲存**。

虛擬私人網路 (VPN)

5

在 NSX Edge 節點上，NSX-T Data Center 支援 IPsec 虛擬私人網路 (IPsec VPN) 和第 2 層 VPN (L2 VPN)。IPsec VPN 提供 NSX Edge 節點與遠端站台之間的站台間連線。使用 L2 VPN 時，您可以透過允許虛擬機器在跨地理界限保留其網路連線的同時使用相同 IP 位址，來擴充資料中心。

備註 NSX-T Data Center 限制出口版本不支援 IPsec VPN 和 L2 VPN。

您必須具備正常運作的 NSX Edge 節點以及至少一個已設定的第 0 層閘道，才可以設定 VPN 服務。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》中的「NSX Edge 安裝」。

從 NSX-T Data Center 2.4 開始，您還可以使用 NSX Manager 使用者介面設定新的 VPN 服務。在舊版 NSX-T Data Center 中，您只能使用 REST API 呼叫來設定 VPN 服務。

重要 使用 NSX-T Data Center 2.4 或更新版本設定 VPN 服務時，您必須使用新的物件，例如使用 NSX Manager 使用者介面或 NSX-T Data Center 2.4 或更新版本隨附的原則 API 所建立的第 0 層閘道。若要在 NSX-T Data Center 2.4 版本之前設定的現有第 0 層邏輯路由器，您必須繼續使用 API 呼叫來設定 VPN 服務。

具有預先定義的值與設定的系統預設組態設定檔可供您在 VPN 服務設定期間使用。也可以定義具有其他設定的新設定檔，然後在 VPN 服務設定期間選取這些設定檔。

本章節討論下列主題：

- [瞭解 IPsec VPN](#)
- [瞭解第 2 層 VPN](#)
- [新增 VPN 服務](#)
- [新增 IPsec VPN 工作階段](#)
- [新增 L2 VPN 工作階段](#)
- [新增本機端點](#)
- [新增設定檔](#)
- [檢查 IPsec VPN 工作階段的實現狀態](#)
- [監控和疑難排解 VPN 工作階段](#)

瞭解 IPsec VPN

網際網路通訊協定安全性 (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 支援 NSX Edge 節點與遠端站台之間的站台間 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。ESP 會直接在 IP 上運作，並使用 IP 通訊協定號碼 50。

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

在 NSX-T Data Center 中，IPsec VPN 服務僅在必須處於 Active-Standby 高可用性模式下的第 0 層閘道上受支援。如需資訊，請參閱[新增第 0 層閘道](#)。設定 IPsec VPN 服務時，您可以使用連線至第 0 層或第 1 層閘道的區段。

NSX-T Data Center 中的 IPsec VPN 服務會使用閘道層級容錯移轉功能，以支援高可用性。通道是在容錯移轉時重新建立的，並且會同步 VPN 組態資料。重新建立通道時，IPsec VPN 狀態不同步。

在 NSX Edge 節點與遠端 VPN 站台之間，支援預先共用的金鑰模式驗證和 IP 單點傳播流量。此外，從 NSX-T Data Center 2.4 開始，支援憑證驗證。僅支援由下列其中一個簽章雜湊演算法簽署的憑證類型。

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

NSX Edge 支援兩種類型的 IPsec VPN：以原則為基礎的 IPsec VPN 和以路由為基礎的 IPsec VPN。

使用以原則為基礎的 IPsec VPN

以原則為基礎的 IPsec VPN 需要將 VPN 原則套用到封包，以確定哪些流量在通過 VPN 通道之前受到 IPsec 保護。

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，VPN 原則設定也必須一併更新以適應變更。

將以原則為基礎的 IPsec VPN 與 NSX-T Data Center 搭配使用時，您可以使用 IPsec 通道將 NSX Edge 節點後方的一或多個本機子網路與遠端 VPN 站台上的對等子網路進行連線。

您可以在 NAT 裝置後方部署 NSX Edge 節點。在此部署中，NAT 裝置會將 NSX Edge 節點的 VPN 位址轉譯為可公開存取的網際網路對向位址。遠端 VPN 站台會使用此公用位址來存取 NSX Edge 節點。

也可以將遠端 VPN 站台置於 NAT 裝置後方。您必須提供遠端 VPN 站台的公用 IP 位址及其識別碼 (FQDN 或 IP 位址) 來設定 IPsec 通道。在兩端，VPN 位址需要靜態一對一 NAT。

NSX Edge 節點的大小會決定支援的通道數目上限，如下表所示。

表 5-1. 支援的 IPSec 通道數目

Edge 節點大小	每個 VPN 工作階段的 IPSec 通道數目 (以原則為基礎)	每項 VPN 服務的工作階段數目	每項 VPN 服務的 IPSec 通道數目 (每個工作階段 16 個通道)
小	不適用 (僅限 POC/實驗室)	不適用 (僅限 POC/實驗室)	不適用 (僅限 POC/實驗室)
中	128	128	2048
大	128 (軟限制)	256	4096
裸機	128 (軟限制)	512	6000

限制 以原則為基礎的 IPSec VPN 的固有架構會限制您設定 VPN 通道備援。

如需設定以原則為基礎的 IPSec VPN 的相關資訊，請參閱[新增 IPSec VPN 服務](#)。

使用以路由為基礎的 IPSec VPN

以路由為基礎的 IPSec 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 VTI 的所有流量。

以路由為基礎的 IPSec VPN 類似於 Generic Routing Encapsulation (GRE) over IPSec，但在套用 IPSec 處理之前沒有其他封裝新增至封包。

在此 VPN 通道方法中，會在 NSX Edge 節點上建立 VTI。每個 VTI 都與 IPSec 通道相關聯。透過 VTI 介面將加密的流量從一個站台路由到另一個站台。IPSec 處理僅在 VTI 上進行。

VPN 通道備援

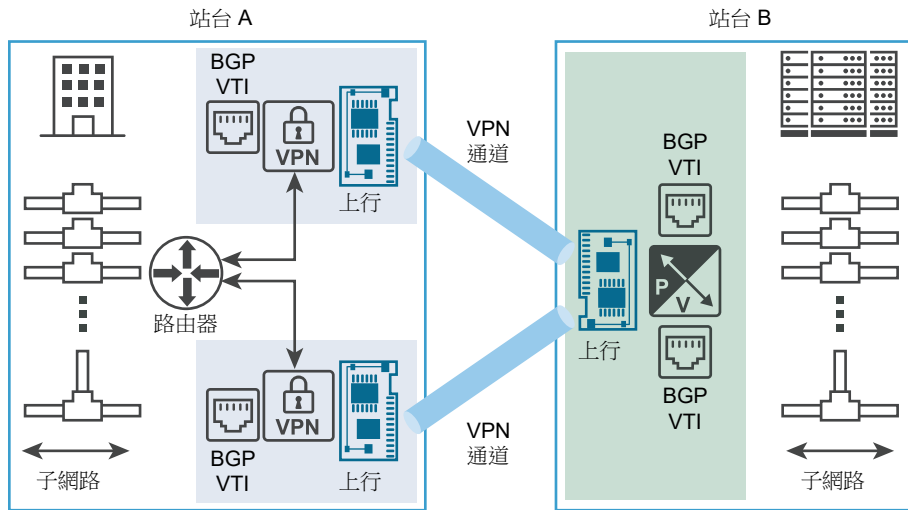
您可以使用以路由為基礎的 IPSec VPN 服務設定 VPN 通道備援。當 ISP 連結失敗或遠端 VPN 閘道失敗時，通道備援可以在兩個站台之間提供不中斷的資料路徑連線。

重要

- 在 NSX-T Data Center 中，僅在使用 BGP 時支援 IPSec VPN 通道備援。透過 IPSec VPN 通道的路由不支援 OSPF 動態路由。
- 不要將靜態路由用於以路由為基礎的 IPSec VPN 通道來實現 VPN 通道備援。

下圖顯示了兩個站台之間的 IPSec VPN 通道備援的邏輯表示。在此圖中，站台 A 和站台 B 代表兩個資料中心。在此範例中，假設 NSX-T Data Center 不管理站台 A 中的 Edge VPN 閘道，並且 NSX-T Data Center 管理站台 B 中的 Edge 閘道虛擬應用裝置。

圖 5-1. 以路由為基礎的 IPSec VPN 通道備援



如圖所示，您可以使用 VTI 來設定兩個獨立的 IPSec VPN 通道。使用 BGP 通訊協定設定動態路由來實現通道備援。如果兩個 IPSec VPN 通道可供使用，它們會保留在服務中。要透過 NSX Edge 節點從站台 A 傳送到站台 B 的所有流量均透過 VTI 進行路由。資料流量經過 IPSec 處理並離開其關聯的 NSX Edge 節點上行介面。從 NSX Edge 節點上行介面上的站台 B VPN 閘道接收的所有傳入 IPSec 流量在解密後轉送到 VTI，然後進行常規路由。

您必須設定 BGP 保持關閉計時器和保持運作計時器值，以便在所需的容錯移轉時間內偵測與對等的連線中斷。請參閱[設定 BGP](#)。

如需設定以原則為基礎的 IPSec VPN 的相關資訊，請參閱[新增 IPSec VPN 服務](#)。

瞭解第 2 層 VPN

透過第 2 層 VPN (L2 VPN)，您可以延伸相同廣播網域上多個站台之間的第 2 層網路 (VLAN 或 VNI)。第 2 層中的虛擬機器 (VM) 可以透過 L2 VPN 順暢地相互通訊，即使其位於不同的資料中心。

透過 L2 VPN 連線，第 2 層網路可以從內部部署資料中心延伸到雲端，例如 VMware Cloud on Amazon (VMC)。此連線受 L2 VPN 用戶端和 L2 VPN 伺服器之間的路由型 IPSec 通道保護。

每個 L2 VPN 工作階段具有一個 Generic Routing Encapsulation (GRE) 通道。不支援通道備援。一個 L2 VPN 工作階段最多可以延伸 4094 個第 2 層網路。

只有第 0 層閘道支援 NSX-T Data Center L2 VPN 服務。區段可連線至第 0 層或第 1 層閘道，並使用 L2 VPN 服務。

備註 此 L2 VPN 功能僅適用於 NSX-T Data Center，且沒有任何第三方互通性。

在下列情況下提供 L2 VPN 服務支援。

- 在 NSX Data Center for vSphere 中管理的 NSX Edge 上主控的 NSX-T Data Center L2 VPN 伺服器和 L2 VPN 用戶端之間。受管理的 L2 VPN 用戶端限制為支援 VNI。

- 在獨立或未受管理的 NSX Edge 上主控的 NSX-T Data Center L2 VPN 伺服器 and L2 VPN 用戶端之間。未受管理的 L2 VPN 用戶端支援 VLAN。
- 從 NSX-T Data Center 2.4 版開始，L2 VPN 服務支援可用於 NSX-T Data Center L2 VPN 伺服器和 NSX-T Data Center L2 VPN 用戶端之間。在此案例中，您可以在兩個內部部署軟體定義資料中心 (SDDC) 之間延伸邏輯 L2 區段。

延伸的網路是具有單一廣播網域的單一子網路，因此虛擬機器 (VM) 在網路站台之間移動時仍保留在相同的子網路上，並且其 IP 位址保持不變。

您可以在不同的實體站台之間移轉工作負載，並且其 IP 位址保持不變。工作負載可以在基於 VXLAN 或基於 VLAN 的網路上執行。L2 VPN 為雲端提供者提供了一個機制，無需修改其工作負載和應用程式使用的現有 IP 位址即可加入承租人。

使用 L2 VPN 延伸的內部部署網路，除了支援資料中心移轉以外，還對災難復原計劃以及動態參與外部部署計算資源以滿足需求的增加非常有用。

新增 VPN 服務

您可以使用 NSX Manager 使用者介面 (UI)，新增 IPsec VPN (以原則為基礎或以路由為基礎) 或 L2 VPN。

以下幾節提供了設定需要的 VPN 服務所需工作流程的高階資訊。這幾節之後的主題則會提供有關如何使用 NSX Manager 使用者介面新增 IPsec VPN 或 L2 VPN 的詳細資料。

以原則為基礎 IPsec VPN 組態工作流程

設定以原則為基礎 IPsec VPN 服務工作流程需要下列高階步驟。

- 1 使用現有第 0 層閘道建立並啟用 IPsec VPN 服務。請參閱[新增 IPsec VPN 服務](#)。
- 2 如果您不想使用系統預設值，則建立 DPD (無作用對等偵測) 設定檔。請參閱[新增 DPD 設定檔](#)。
- 3 若要使用非系統預設的 IKE 設定檔，請定義 IKE (網際網路金鑰交換) 設定檔。請參閱[新增 IKE 設定檔](#)。
- 4 使用[新增 IPsec 設定檔](#)設定 IPsec 設定檔。
- 5 使用[新增本機端點](#)建立本機端點。
- 6 設定以原則為基礎的 IPsec VPN 工作階段、套用設定檔，然後連結本機端點。請參閱[新增以原則為基礎的 IPsec 工作階段](#)。

以路由為基礎的 IPsec VPN 組態工作流程

以路由為基礎的 IPsec VPN 組態工作流程需要下列高階步驟。

- 1 使用現有第 0 層閘道設定並啟用 IPsec VPN 服務。請參閱[新增 IPsec VPN 服務](#)。
- 2 指定要用於通道的本機與對等子網路。
- 3 建立 DPD 設定檔。請參閱[新增 DPD 設定檔](#)。
- 4 如果您不想使用預設的 IKE 設定檔，則定義 IKE 設定檔。請參閱[新增 IKE 設定檔](#)。

- 5 如果您決定不使用系統預設的 IPsec 設定檔，則使用[新增 IPsec 設定檔](#)建立一個設定檔。
- 6 使用[新增本機端點](#)新增本機端點。
- 7 建立以路由為基礎的 IPsec VPN 工作階段。請參閱[新增路由型 IPsec 工作階段](#)。

L2 VPN 組態工作流程

若要設定 L2 VPN，您必須設定一個處於伺服器模式的 L2 VPN 服務，然後再設定一個處於用戶端模式的 L2 VPN 服務。您還必須設定用於 L2 VPN 伺服器和 L2 VPN 用戶端的工作階段。以下是設定 L2 VPN 服務的高階工作流程。

- 1 建立處於伺服器模式的 L2 VPN 服務。
 - a 使用第 0 層閘道設定以路由為基礎的 IPsec VPN 通道，然後使用該以路由為基礎的 IPsec 通道設定 L2 VPN 伺服器服務。請參閱[新增 L2 VPN 伺服器服務](#)。
 - b 設定一個 L2 VPN 伺服器工作階段，以繫結新建立的以路由為基礎的 IPsec VPN 服務和 L2 VPN 伺服器服務，並自動配置 GRE IP 位址。請參閱[新增 L2 VPN 伺服器工作階段](#)。
 - c 對 L2 VPN 伺服器工作階段新增區段。此步驟亦在 [新增 L2 VPN 伺服器工作階段](#)中進行了說明。
 - d 使用[下載遠端 L2 VPN 組態](#)取得 L2 VPN 伺服器服務工作階段的對等代碼，它會用於自動設定 L2 VPN 用戶端工作階段。
- 2 建立處於用戶端模式的 L2 VPN 服務。
 - a 使用其他第 0 層閘道設定另一個以路由為基礎的 IPsec VPN 服務，然後使用剛設定的該第 0 層閘道設定 L2 VPN 用戶端服務。如需資訊，請參閱[新增 L2 VPN 用戶端服務](#)。
 - b 透過匯入 L2 VPN 伺服器服務所產生的對等代碼，定義 L2 VPN 用戶端工作階段。請參閱[新增 L2 VPN 用戶端工作階段](#)。
 - c 新增區段至上個步驟中所定義的 L2 VPN 用戶端工作階段。此步驟在[新增 L2 VPN 用戶端工作階段](#)進行了說明。

新增 IPsec VPN 服務

NSX-T Data Center 支援第 0 層閘道與遠端站台之間的站台間 IPsec VPN 服務。您可以建立以原則為基礎或以路由為基礎的 IPsec VPN 服務。必須先建立 IPsec VPN 服務，才能設定以原則為基礎或以路由為基礎的 IPsec VPN 工作階段。

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

本機端點 IP 位址會通過 IPsec VPN 工作階段設定的相同邏輯路由器中的 NAT 時，不支援 IPsec VPN。

必要條件

- 自行熟悉 IPsec VPN。請參閱[瞭解 IPsec VPN](#)。
- 您必須至少已設定一個第 0 層閘道，並可供使用。如需詳細資訊，請參閱[新增第 0 層閘道](#)。

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 導覽到 **網路 > VPN > VPN 服務**。
- 3 選取**新增服務 > IPSec**。
- 4 輸入 IPSec 服務的名稱。
此名稱為必填。
- 5 從**第 0 層閘道**下拉式功能表中，選取要與此 IPSec VPN 服務建立關聯的第 0 層閘道。
- 6 啟用或停用**管理狀態**。
依預設，此值設為 **Enabled**，表示在設定新的 IPSec VPN 服務後，在第 0 層閘道上已啟用 IPSec VPN 服務。
- 7 設定 **IKE 記錄層級**的值。
網際網路金鑰交換 (IKE) 記錄層級決定了要針對 IPSec VPN 流量收集的資訊量。預設值設為 **Info** 層級。
- 8 如果您想要將此服務加入標籤群組，請輸入**標籤**的值。
- 9 如果您想要允許在指定的本機和遠端 IP 位址之間交換資料封包，而不進行任何 IPSec 保護，且即使已在 IPSec 工作階段規則中指定了 IP 位址亦然，請按一下**全域略過規則**。在**本機網路**和**遠端網路**中，輸入要在其間套用略過規則的本機子網路與遠端子網路清單。
預設值是在本機站台與遠端站台之間交換資料時使用 IPSec 保護。這些規則適用於在此 IPSec VPN 服務內建立的所有 IPSec VPN 工作階段。
- 10 按一下**儲存**。
成功建立新的 IPSec VPN 服務後，系統會詢問您是否要繼續設定其餘的 IPSec VPN 組態。如果您按一下**是**，就會返回 [新增 IPSec VPN 服務] 面板。**工作階段**連結現已啟用，您可以按一下該連結來新增 IPSec VPN 工作階段。

後續步驟

使用**新增 IPSec VPN 工作階段**中的資訊來引導您新增 IPSec VPN 工作階段。您還需提供完成 IPSec VPN 組態所需的設定檔與本機端點的資訊。

新增 L2 VPN 服務

您可以透過先建立路由型 IPSec VPN 通道，來設定 IPSec 通道上的 L2 VPN 服務。然後透過耗用路由型 IPSec VPN 通道，來設定 L2 VPN 伺服器 (目的地閘道) 與 L2 VPN 用戶端 (來源閘道) 之間的 L2 VPN 通道。

若要設定 IPSec 通道上的 L2 VPN 服務，請使用本節中相關主題的資訊。

必要條件

- 自行熟悉 IPsec VPN 和 L2 VPN。請參閱[瞭解 IPSec VPN](#)與[瞭解第 2 層 VPN](#)。

- 您必須至少已設定一個第 0 層閘道，並可供使用。請參閱[新增第 0 層閘道](#)。

程序

1 新增 L2 VPN 伺服器服務

若要設定 L2 VPN 伺服器服務，您必須在 L2 VPN 用戶端要連線到的目的地 NSX Edge 上，於伺服器模式下設定 L2 VPN 服務。

2 新增 L2 VPN 用戶端服務

設定 L2 VPN 伺服器後，請在另一個 Edge 執行個體上的用戶端模式下設定 L2 VPN 服務，該執行個體可以是 NSX 管理的 Edge、獨立 Edge 或 NSX-T 軟體定義資料中心 (SDDC)。

新增 L2 VPN 伺服器服務

若要設定 L2 VPN 伺服器服務，您必須在 L2 VPN 用戶端要連線到的目的地 NSX Edge 上，於伺服器模式下設定 L2 VPN 服務。

設定 L2 VPN 伺服器之前，您必須先建立以路由為基礎的 IPSec VPN 通道。然後，您便可使用此以路由為基礎的 IPSec VPN 通道，建立在兩個站台之間延伸第 2 層網路的 L2 VPN 通道。

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 使用您要設為 L2 VPN 伺服器模式的 NSX Edge，建立以路由為基礎的 IPSec 通道。
 - a 導覽至**網路 > VPN > VPN 服務**索引標籤，然後選取**新增服務 > IPSec**。
 - b 輸入 IPSec VPN 服務的名稱。
 - c 從**第 0 層閘道**下拉式功能表中，選取要與 L2 VPN 伺服器搭配使用的第 0 層閘道。
 - d 如果您想要使用與系統預設值不同的值，請視需要設定 [新增 IPSec 服務] 窗格中的其餘內容。
 - e 按一下**儲存**，然後在出現提示詢問您是否要繼續設定 IPSec VPN 服務時，選取**否**。
- 3 導覽至**網路 > VPN > VPN 服務**索引標籤，然後選取**新增服務 > L2 VPN 伺服器**以建立 L2 VPN 伺服器。
- 4 輸入 L2 VPN 伺服器的名稱。
- 5 從**第 0 層閘道**下拉式功能表中，選取您與不久前所建立的 IPSec 服務搭配使用的同一個第 0 層閘道。
- 6 (選用) 輸入此 L2 VPN 伺服器的說明。
- 7 如果您想要將此服務加入標籤群組，請輸入**標籤**的值。
- 8 啟用或停用**中樞和支點**內容。

依預設，此值設為 **Disabled**，這表示從 L2 VPN 用戶端接收到的流量只會複寫到連線至 L2 VPN 伺服器的區段。如果此內容設為 **Enabled**，來自任何 L2 VPN 用戶端的流量，均會複寫至所有其他 L2 VPN 用戶端。

9 按一下儲存。

成功建立新的 L2 VPN 伺服器後，系統會詢問您是否要繼續設定其餘的 L2 VPN 服務組態。如果您按一下**是**，就會返回 [新增 L2 VPN 伺服器] 窗格，且**工作階段**連結會啟用。您可以使用該連結建立 L2 VPN 伺服器工作階段，也可以使用**網路 > VPN > L2 VPN 工作階段**索引標籤。

後續步驟

使用**新增 L2 VPN 伺服器工作階段**中的資訊做為引導，針對您已設定的 L2 VPN 伺服器設定 L2 VPN 伺服器工作階段。

新增 L2 VPN 用戶端服務

設定 L2 VPN 伺服器後，請在另一個 Edge 執行個體上的用戶端模式下設定 L2 VPN 服務，該執行個體可以是 NSX 管理的 Edge、獨立 Edge 或 NSX-T 軟體定義資料中心 (SDDC)。

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 建立用於 L2 VPN 用戶端服務的路由型 IPSec 通道。
 - a 導覽至**網路 > VPN > VPN 服務**索引標籤，然後選取**新增服務 > IPSec**。
 - b 輸入 IPSec VPN 服務的名稱。
 - c 從**第 0 層閘道**下拉式功能表中，選取要與 L2 VPN 用戶端搭配使用的第 0 層閘道。
 - d 如果您想要使用與系統預設值不同的值，請視需要設定 [新增 IPSec 服務] 窗格中的其餘內容。
 - e 按一下**儲存**，然後在出現提示詢問您是否要繼續設定 IPSec VPN 服務時，選取**否**。
- 3 導覽至**網路 > VPN > VPN 服務**索引標籤，然後選取**新增服務 > L2 VPN 用戶端**。
- 4 輸入 L2 VPN 用戶端服務的名稱。
- 5 從**第 0 層閘道**下拉式功能表中，選取與您剛剛建立的路由型 IPSec 通道搭配使用的同一個第 0 層閘道。
- 6 如果您想要使用系統預設值以外的值，請在 [新增 L2 VPN 用戶端] 窗格上定義其他內容。
- 7 按一下**儲存**。

成功建立新的 L2 VPN 用戶端服務後，系統會詢問您是否要繼續設定其餘的 L2 VPN 用戶端組態。如果您按一下**是**，您將回到 [新增 L2 VPN 用戶端] 窗格，且其中已啟用**工作階段**連結。您可以使用該連結來建立 L2 VPN 用戶端工作階段，或是使用**網路 > VPN > L2 VPN 工作階段**索引標籤。

後續步驟

針對您所設定的 L2 VPN 用戶端服務，設定 L2 VPN 用戶端工作階段。使用**新增 L2 VPN 用戶端工作階段**中的資訊做為操作指南。

新增 IPsec VPN 工作階段

設定 IPsec VPN 服務後，您必須新增以原則為基礎的 IPsec VPN 工作階段或以路由為基礎的 IPsec VPN 工作階段，具體取決於您想要設定的 IPsec VPN 類型。您還需提供要用於完成 IPsec VPN 服務組態之本機端點與設定檔的資訊。

新增以原則為基礎的 IPsec 工作階段

新增以原則為基礎的 IPsec VPN 時，會使用 IPsec 通道將位於 NSX Edge 節點後方的多個本機子網路與位於遠端 VPN 站台上的對等子網路連線。

下列步驟會使用 NSX Manager 使用者介面上的 **IPsec 工作階段** 索引標籤，建立以原則為基礎的 IPsec 工作階段。您也可以新增通道、IKE 和 DPD 設定檔的資訊，然後選取要與以原則為基礎的 IPsec VPN 搭配使用的現有本機端點。

備註 您也可以成功設定 IPsec VPN 服務後立即新增 IPsec VPN 工作階段。當系統提示您繼續 IPsec VPN 服務設定時，按一下**是**，然後選取 [新增 IPsec 服務] 面板上的**工作階段 > 新增工作階段**。以下程序中的前幾個步驟假設您已在系統提示您繼續 IPsec VPN 服務設定時選取**否**。如果您選取了**是**，請繼續前往下列步驟中的步驟 3，將引導您完成其餘的以原則為基礎的 IPsec VPN 工作階段組態。

必要條件

- 您必須已設定 IPsec VPN 服務，才能繼續。請參閱[新增 IPsec VPN 服務](#)。
- 取得本機端點、對等站台 IP 位址、本機網路子網路與遠端網路子網路的資訊，以與您要新增之以原則為基礎的 IPsec VPN 工作階段搭配使用。若要建立本機端點，請參閱[新增本機端點](#)。
- 如果您使用預先共用的金鑰 (PSK) 進行驗證，請取得 PSK 值。
- 如果您使用憑證進行驗證，請確保所需的伺服器憑證以及對應的 CA 簽署憑證已匯入。請參閱[設定憑證](#)。
- 如果您不想使用 NSX-T Data Center 針對 IPsec 通道、IKE 或無作用對等偵測 (DPD) 設定檔提供的預設值，請設定您要改用的設定檔。如需資訊，請參閱[新增設定檔](#)。

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 導覽到 **網路 > VPN > IPsec 工作階段** 索引標籤。
- 3 選取**新增 IPsec 工作階段 > 以原則為基礎**。
- 4 輸入以原則為基礎的 IPsec VPN 工作階段的名稱。
- 5 從 **VPN 服務** 下拉式功能表中，選取要新增此新 IPsec 工作階段的 IPsec VPN 服務。

備註 如果您要從**新增 IPsec 工作階段**對話方塊新增此 IPsec 工作階段，在**新增 IPsec 工作階段**按鈕上方已指示 VPN 服務名稱。

- 6 從下拉式功能表中選取現有的本機端點。

此本機端點值為必填，它會識別本機 NSX Edge 節點。如果您想要建立不同的本機端點，請按一下三個點功能表 (⋮)，然後選取**新增本機端點**。

- 7 在**遠端 IP** 文字方塊中，輸入所需遠端站台的 IP 位址。

此值為必填。

- 8 (選用) 輸入此以原則為基礎的 IPSec VPN 工作階段的說明。

長度上限為 1024 個字元。

- 9 若要啟用或停用 IPSec VPN 工作階段，請按一下**管理狀態**。

依預設，此值設為 **Enabled**，這表示要向 NSX Edge 節點設定 IPSec VPN 工作階段。

- 10 從**驗證模式**下拉式功能表中選取模式。

使用的預設驗證模式為 **PSK**，這表示要將 NSX Edge 與遠端站台之間共用的秘密金鑰用於 IPSec VPN 工作階段。如果您選取 **Certificate**，會將用於設定本機端點的站台憑證用於進行驗證。

- 11 如果您為驗證模式選取 **PSK**，請在**預先共用的金鑰**文字方塊中輸入金鑰值。

此秘密金鑰可以是最大長度為 128 個字元的字串。

注意 共用和儲存 PSK 值時請小心，因為它包含敏感資訊。

- 12 在**本機網路**與**遠端網路**文字方塊中，至少輸入一個要用於此以原則為基礎的 IPSec VPN 工作階段的 IP 子網路位址。

這些子網路必須採用 CIDR 格式。

- 13 若要識別對等站台，請在**遠端識別碼**中輸入值。

對於使用 PSK 驗證的對等站台，此識別碼值必須是對等站台的公用 IP 位址或 FQDN。對於使用憑證驗證的對等站台，此識別碼值必須是對等站台的憑證中使用的一般名稱 (CN) 或辨別名稱 (DN)。

備註 如果對等站台的憑證在 DN 字串中包含電子郵件地址，例如

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

請以下列格式輸入**遠端識別碼**值，作為範例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

如果本機站台的憑證在 DN 字串中包含電子郵件地址，且對等站台使用 **strongSwan IPsec** 實作，請在該對等站台中輸入本機站台的識別碼值，如下列範例所示。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 14 如果您想要在特定群組中包含此工作階段，請在**標籤**中輸入標籤名稱。

15 若要變更原則型 IPsec VPN 工作階段所使用的設定檔和初始模式，請按一下**設定檔和初始模式**。

依預設，會使用系統產生的設定檔。如果您不想使用預設設定檔，請選取另一個可用的設定檔。如果您想要使用尚未設定的設定檔，請按一下三個點功能表 (⋮) 來建立另一個設定檔。請參閱[新增設定檔](#)。

- a 從 **IKE 設定檔** 下拉式功能表中，選取要使用的 IKE 設定檔。
- b 從 **DPD 設定檔** 下拉式功能表中，選取慣用的 DPD 設定檔。
- c 在 **IPsec 設定檔** 中，選取要與 IPsec 工作階段搭配使用的 IPsec 通道設定檔。
- d 從**連線初始模式**下拉式功能表中，選取慣用模式。

連線初始模式定義在通道建立程序中本機端點使用的原則。預設值為 **Initiator**。下表說明可用的不同連線初始模式。

表 5-2. 連線初始模式

連線初始模式	說明
Initiator	預設值。在此模式下，本機端點開始建立 IPsec VPN 通道，並回應來自對等端道的傳入通道設定要求。
On Demand	在此模式下，在接收第一個符合原則規則的封包後，本機端點開始建立 IPsec VPN 通道。它也會回應傳入初始要求。
Respond Only	IPsec VPN 永遠不會起始連線。對等站台永遠會起始連線要求，並且本機端點回應該連線要求。

16 按一下**儲存**。**結果**

新的以原則為基礎的 IPsec VPN 工作階段在設定成功後，便會新增至可用的 IPsec VPN 工作階段清單。處於唯讀模式。

後續步驟

- 確認 IPsec VPN 通道狀態為 [開啟]。如需資訊，請參閱[監控和疑難排解 VPN 工作階段](#)。
- 如有必要，可透過按一下工作階段資料列左側的三個點功能表 (⋮)，來管理 IPsec VPN 工作階段資訊。選取其中一個允許您執行的動作。

新增路由型 IPsec 工作階段

新增路由型 IPsec VPN 時，根據透過虛擬通道介面 (VTI) (使用慣用通訊協定，例如 BGP) 動態學習的路由來提供流量的通道。IPsec 保護流經 VTI 的所有流量。

此主題中所述的步驟使用 **IPSec 工作階段** 索引標籤建立路由型 IPSec 工作階段。您也可以新增通道、IKE 和 DPD 設定檔的資訊，以及選取現有的本機端點，以與路由型 IPSec VPN 搭配使用。

備註 您也可以成功設定 IPSec VPN 服務後立即新增 IPSec VPN 工作階段。當系統提示您繼續 IPSec VPN 服務組態時，按一下**是**，然後選取 [新增 IPsec 服務] 面板上的**工作階段 > 新增工作階段**。以下程序中的前幾個步驟假設您已在系統提示您繼續 IPSec VPN 服務組態時選取**否**。如果您已選取**是**，則繼續進行以下步驟中的步驟 3，以引導您進行路由型 IPSec VPN 工作階段設定的剩餘部分。

必要條件

- 您必須已設定 IPSec VPN 服務，才能繼續。請參閱[新增 IPSec VPN 服務](#)。
- 取得要與新增的路由型 IPSec 工作階段搭配使用的本機端點、對等站台的 IP 位址和通道服務 IP 子網路位址的相關資訊。若要建立本機端點，請參閱[新增本機端點](#)。
- 如果您使用預先共用的金鑰 (PSK) 進行驗證，請取得 PSK 值。
- 如果您使用憑證進行驗證，請確保所需的伺服器憑證以及對應的 CA 簽署憑證已匯入。請參閱[設定憑證](#)。
- 如果您不想使用由 NSX-T Data Center 提供的 IPSec 通道、IKE 或無作用對等偵測 (DPD) 設定檔的預設值，請設定要使用的設定檔。如需資訊，請參閱[新增設定檔](#)。

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 導覽到 **網路 > VPN > IPSec 工作階段**。
- 3 選取**新增 IPSec 工作階段 > 以路由為基礎**。
- 4 輸入路由型 IPSec 工作階段的名稱。
- 5 從 **VPN 服務** 下拉式功能表中，選取要新增此新 IPSec 工作階段的 IPSec VPN 服務。

備註 如果您要從**新增 IPSec 工作階段**對話方塊新增此 IPSec 工作階段，在**新增 IPSec 工作階段**按鈕上方已指示 VPN 服務名稱。

- 6 從下拉式功能表中選取現有的本機端點。
此本機端點值為必填，它會識別本機 NSX Edge 節點。如果您想要建立不同的本機端點，請按一下三個點功能表 (⋮)，然後選取**新增本機端點**。
- 7 在**遠端 IP** 文字方塊中，輸入遠端站台的 IP 位址。
此值為必填。
- 8 輸入此路由型 IPSec VPN 工作階段的選用說明。
長度上限為 1024 個字元。
- 9 若要啟用或停用 IPSec 工作階段，請按一下**管理狀態**。
依預設，此值設為 **Enabled**，這表示要向 NSX Edge 節點設定 IPSec 工作階段。

10 從驗證模式下拉式功能表中選取模式。

使用的預設驗證模式為 **PSK**，這表示要將 **NSX Edge** 與遠端站台之間共用的秘密金鑰用於 **IPSec VPN** 工作階段。如果您選取 **Certificate**，會將用於設定本機端點的站台憑證用於進行驗證。

11 如果您為驗證模式選取 PSK，請在預先共用的金鑰文字方塊中輸入金鑰值。

此秘密金鑰可以是最大長度為 **128** 個字元的字串。

注意 共用和儲存 **PSK** 值時請小心，因為它包含一些敏感資訊。

12 在通道介面中以 CIDR 標記法輸入 IP 子網路位址。

此位址為必填。

13 輸入值遠端識別碼。

對於使用 **PSK** 驗證的對等站台，此識別碼值必須是對等站台的公用 IP 位址或 **FQDN**。對於使用憑證驗證的對等站台，此識別碼值必須是對等站台的憑證中使用的一般名稱 (**CN**) 或辨別名稱 (**DN**)。

備註 如果對等站台的憑證在 **DN** 字串中包含電子郵件地址，例如

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

請以下列格式輸入遠端識別碼值，作為範例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

如果本機站台的憑證在 **DN** 字串中包含電子郵件地址，且對等站台使用 **strongSwan IPsec** 實作，請在該對等站台中輸入本機站台的識別碼值。以下為範例。

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

14 如果您想要將此 IPSec 工作階段包含做為特定群組標籤的一部分，請在標籤中輸入標籤名稱。**15 若要變更路由型 IPSec VPN 工作階段所使用的設定檔和初始模式，請按一下設定檔和初始模式。**

依預設會使用系統產生的設定檔。如果您不想使用預設設定檔，請選取另一個可用的設定檔。如果您想要使用尚未設定的設定檔，請按一下三個點功能表 (⋮) 來建立另一個設定檔。請參閱[新增設定檔](#)。

a 從 **IKE 設定檔** 下拉式功能表中，選取要使用的 **IKE** 設定檔。

b 從 **DPD 設定檔** 下拉式功能表中，選取慣用的 **DPD** 設定檔。

- c 在 **IPSec 設定檔** 中，選取要與 IPSec 工作階段搭配使用的 IPSec 通道設定檔。
- d 從**連線初始模式**下拉式功能表中，選取慣用模式。

連線初始模式定義在通道建立程序中本機端點使用的原則。預設值為 **Initiator**。下表說明可用的不同連線初始模式。

表 5-3. 連線初始模式

連線初始模式	說明
Initiator	預設值。在此模式下，本機端點開始建立 IPSec VPN 通道，並回應來自對等端道的傳入通道設定要求。
On Demand	請勿搭配使用以路由為基礎的 VPN。此模式僅適用以原則為基礎的 VPN。
Respond Only	IPSec VPN 永遠不會起始連線。對等站台永遠會起始連線要求，並且本機端點回應該連線要求。

16 按一下儲存。

結果

已成功設定新的路由型 IPSec VPN 工作階段時，它會新增至可用的 IPsec VPN 工作階段清單。處於唯讀模式。

後續步驟

- 確認 IPSec VPN 通道狀態為 [開啟]。如需資訊，請參閱[監控和疑難排解 VPN 工作階段](#)。
- 使用靜態路由或 BGP 設定路由。請參閱[設定靜態路由](#)或[設定 BGP](#)。
- 如有必要，可透過按一下工作階段資料列左側的三個點功能表 (⋮)，來管理 IPSec VPN 工作階段資訊。選取您可以執行的其中一個動作。

新增 L2 VPN 工作階段

在設定 L2 VPN 伺服器 and L2 VPN 用戶端後，您必須為它們新增 L2 VPN 工作階段，才能完成 L2 VPN 服務組態設定。

新增 L2 VPN 伺服器工作階段

建立 L2 VPN 伺服器服務之後，您必須新增 L2 VPN 工作階段，並將其連結至現有的區段。

下列步驟使用 NSX Manager 使用者介面上的 **L2 VPN 工作階段** 索引標籤，來建立 L2 VPN 伺服器工作階段。您也可以選取現有的本機端點，以及要連結至 L2 VPN 伺服器工作階段的區段。

備註 您也可以成功設定 L2 VPN 伺服器服務後立即新增 L2 VPN 伺服器工作階段。當系統提示您繼續 L2 VPN 伺服器設定時，您按一下**是**，再選取 [新增 L2 VPN 伺服器] 面板上的**工作階段 > 新增工作階段**。以下程序中的前幾個步驟假設您已在系統提示您繼續 L2 VPN 伺服器設定時選取**否**。如果您已選取**是**，則繼續進行以下步驟中的步驟 3，以引導您進行 L2 VPN 伺服器工作階段設定的剩餘部分。

必要條件

- 您必須已設定 L2 VPN 伺服器服務，才能繼續。請參閱[新增 L2 VPN 伺服器服務](#)。
- 取得要與新增的 L2 VPN 伺服器工作階段搭配使用的本機端點及遠端 IP 的相關資訊。若要建立本機端點，請參閱[新增本機端點](#)。
- 取得預先共用的金鑰 (PSK) 和通道介面子網路的值，以與 L2 VPN 伺服器工作階段搭配使用。
- 取得您想要連結至您要建立的 L2 VPN 伺服器工作階段的現有區段名稱。如需資訊，請參閱[新增區段](#)。

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 導覽到 **網路 > VPN > L2 VPN 工作階段** 索引標籤。
- 3 選取**新增 L2 VPN 工作階段 > L2 VPN 伺服器**。
- 4 輸入 L2 VPN 伺服器工作階段的名稱。
- 5 從 **L2 VPN 服務** 下拉式功能表中，選取為其建立 L2 VPN 工作階段的 L2 VPN 伺服器服務。

備註 如果您正從 [設定 L2VPN 伺服器工作階段] 對話方塊新增此 L2 VPN 伺服器工作階段，L2 VPN 伺服器服務已在**新增 L2 工作階段**按鈕上方指出。

- 6 從下拉式功能表中選取現有的本機端點。

如果您想要建立不同的本機端點，請按一下三個點功能表 (⋮)，然後選取**新增本機端點**。

- 7 輸入遠端站台的 IP 位址。
- 8 若要啟用或停用 L2 VPN 伺服器工作階段，請按一下**管理員狀態**。

依預設，此值設為**已啟用**，這表示要向 NSX Edge 節點設定 L2 VPN 伺服器工作階段。

- 9 在**預先共用的金鑰**中輸入秘密金鑰值。

注意 共用和儲存 PSK 值時請小心，因為它包含敏感資訊。

- 10 在**通道介面**中使用 CIDR 標記法輸入 IP 子網路位址。

例如，4.5.6.6/24。此子網路位址為必填。

- 11 在**遠端識別碼**中輸入值。

對於使用憑證驗證的對等站台，此識別碼必須是對等站台的憑證中的一般名稱。對於 PSK 對等，此識別碼可以是任何字串。最好將 VPN 的公用 IP 位址或 VPN 服務的 FQDN 用作 Remote ID。

- 12 如果您想要在特定群組中包含此工作階段，請在**標籤**中輸入標籤名稱。

- 13 按一下**儲存**，然後當系統提示您是否要繼續進行 VPN 服務設定時按一下**是**。

您將返回 [新增 L2VPN 工作階段] 面板，且現已啟用**區段連結**。

14 將現有區段連結至 L2 VPN 伺服器工作階段。

- a 按一下**區段 > 設定區段**。
- b 在**設定區段**對話方塊中，按一下**設定區段**，將現有區段連結至 L2 VPN 伺服器工作階段。
- c 從**區段**下拉式功能表中，選取要連結至工作階段的區段。
- d 在 **VPN 通道識別碼**中輸入值，用於唯一識別您所選取的區段。
- e 按一下**儲存**，然後按一下**關閉**。

在 [設定 L2VPN 工作階段] 窗格或對話方塊中，系統已遞增 L2 VPN 伺服器工作階段的**區段**計數。

15 若要完成 L2 VPN 伺服器工作階段設定，請按一下**關閉編輯**。

結果

在 **VPN 服務**索引標籤中，系統已遞增您設定的 L2 VPN 伺服器服務的工作階段計數。

後續步驟

若要完成 L2 VPN 服務設定，您還必須在用戶端模式下建立 L2 VPN 服務和 L2 VPN 用戶端工作階段。請參閱[新增 L2 VPN 用戶端服務](#)與[新增 L2 VPN 用戶端工作階段](#)。

新增 L2 VPN 用戶端工作階段

建立 L2 VPN 用戶端服務之後，您必須新增 L2 VPN 用戶端工作階段，然後將其連結至現有區段。

下列步驟會使用 NSX Manager 使用者介面上的 **L2 VPN 工作階段**索引標籤建立 L2 VPN 用戶端工作階段。您也可以選取現有本機端點與區段來連結至 L2 VPN 用戶端工作階段。

備註 您也可以成功設定 L2 VPN 用戶端服務後，立即新增 L2 VPN 用戶端工作階段。在出現提示詢問您是否繼續設定 L2 VPN 用戶端時按一下**是**，然後選取 [新增 L2 VPN 用戶端] 面板上的**工作階段 > 新增工作階段**。下列程序的前幾個步驟假設您在出現提示詢問是否繼續設定 L2 VPN 用戶端時選取了**否**。如果您選取了**是**，請繼續前往下列步驟中的步驟 3，以引導您完成其餘的 L2 VPN 用戶端工作階段組態。

必要條件

- 您必須已設定 L2 VPN 用戶端服務才能繼續。請參閱[新增 L2 VPN 用戶端服務](#)。
- 取得本機 IP 與遠端 IP 的 IP 位址資訊，以與您要新增的 L2 VPN 用戶端工作階段搭配使用。
- 取得設定 L2 VPN 伺服器期間所產生的對等代碼。請參閱[下載遠端 L2 VPN 組態](#)。
- 取得您要連結至要建立之 L2 VPN 用戶端工作階段的現有區段的名稱。請參閱[新增區段](#)。

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 > VPN > L2 VPN 工作階段**。
- 3 選取**新增 L2 VPN 工作階段 > L2 VPN 用戶端**。
- 4 輸入 L2 VPN 用戶端工作階段的名稱。

- 5 從 **VPN 服務** 下拉式功能表中，選取要與 L2 VPN 工作階段建立關聯的 L2 VPN 用戶端服務。

備註 如果是從 [設定 L2VPN 用戶端工作階段] 對話方塊新增此 L2 VPN 用戶端工作階段，**新增 L2 工作階段** 按鈕上方已指出 L2 VPN 用戶端服務。

- 6 在 **本機 IP 位址** 文字方塊中，輸入 L2 VPN 用戶端工作階段的 IP 位址。
- 7 輸入 L2 VPN 用戶端服務所用 IPSec 通道的遠端 IP 位址。
- 8 在 **對等組態** 文字方塊中，輸入設定 L2 VPN 伺服器服務時所產生的對等代碼。
 - a 導覽至您使用 **下載遠端 L2 VPN 組態** 已下載 L2VPNSession_<L2VPN-Server-Session>_config.txt 的位置。
 - b 將該檔案的內容複製並貼到 **對等組態** 文字方塊中。
- 9 啟用或停用 **管理狀態**。
依預設，此值設為 **已啟用**，這表示要向 NSX Edge 節點設定 L2 VPN 伺服器工作階段。
- 10 按一下 **儲存**，然後當系統提示您是否要繼續進行 VPN 服務設定時按一下 **是**。
- 11 將現有區段連結至 L2 VPN 用戶端工作階段。
 - a 選取 **區段 > 新增區段**。
 - b 在 **設定區段** 對話方塊中，按一下 **新增區段**。
 - c 從 **區段** 下拉式功能表中，選取要連結至 L2 VPN 伺服器工作階段的區段。
 - d 在 **VPN 通道識別碼** 中輸入值。
 - e 按一下 **關閉**。
- 12 若要完成 L2 VPN 用戶端工作階段組態，請按一下 **關閉編輯**。

結果

在 **VPN 服務** 索引標籤中，針對您設定的 L2 VPN 用戶端服務，工作階段計數會更新。

下載遠端 L2 VPN 組態

若要設定 L2 VPN 用戶端工作階段，必須取得在設定 L2 VPN 伺服器工作階段時產生的對等代碼。

必要條件

- 您必須成功設定 L2 VPN 伺服器服務和工作階段，才能繼續操作。請參閱 **新增 L2 VPN 伺服器服務**。

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 導覽到 **網路 > VPN > L2 VPN 工作階段** 索引標籤。
- 3 在 L2 VPN 工作階段的資料表中，展開您打算用於 L2 VPN 用戶端工作階段組態的 L2 VPN 伺服器工作階段資料列。

- 4 按一下**下載組態**，然後按一下 [警告] 對話方塊上的**是**。

即會下載名為 `L2VPNSession_<name-of-L2-VPN-server-session>.config.txt` 的文字檔。其中包含遠端 L2 VPN 組態的對等代碼。

注意 儲存和共用對等程式碼時請小心，因為它包含 PSK 值，這是敏感資訊。

例如，`L2VPNSession_L2VPNSess1_config.txt` 包含下列組態。

```
[{"transport_tunnel_path":"/infra/tier-0s/T0-gateway-1-AS/locale-services/1f309c00-277f-11e9-8074-a18943ad6b99/ipsec-vpn-services/IPS01-01/sessions/093ad8d0-2fad-11e9-8e5b-15a7211d1582",
"peer_code":"MCxiYTNjZmIwLHsic2l0ZU5hbWUiOiJMMLZQTi1MMLZTZXNzMSIsInNyY1RhclwIjoimTY5LjI1NC42NC4yIiwizHN0VGFWsXAiOiIxNjkuMjU0LjY0LjEiLCJpa2VpcHRpb24iOiJpa2V2MiIsImVuY2FwUHJvdG8iOiJncmUvaXBzZWMiLCJkaEdyb3VwIjoizGgxNCIsImVuY3J5cHRBbmREaWdlc3QiOiJhZXMtZ2NtL3NoYyS0yNTYiLCJwc2siOiIxMTIyMzM0NDU1NjYiLCJ0dW5uZWxzIjpbeyJsbnh2NhbElkIjoINC41LjYuNiIsInBlZXJJZCI6IjEuMS4yLjIiLCJsb2NhbFZ0aUlwIjoINC41LjYuMS8yNCJ9XX0="}]2NhbFZ0aUlwIjoINC41LjYuMS8yNCJ9XX0="}]
```

後續步驟

設定 L2 VPN 用戶端服務和工作階段。請參閱[新增 L2 VPN 用戶端服務](#)與[新增 L2 VPN 用戶端工作階段](#)。

新增本機端點

您必須設定本機端點，以與您要設定的 IPsec VPN 搭配使用。

下列步驟使用 NSX Manager 使用者介面上的**本機端點**索引標籤。您也可以在新增 IPsec VPN 工作階段中，透過按一下三個點功能表 (⋮)，然後選取**新增本機端點**，來建立本機端點。如果您正在設定 IPsec VPN 工作階段，請跳至下列步驟中的步驟 3，以引導您建立新的本機端點。

必要條件

- 如果您正為 IPsec VPN 工作階段 (將使用您要設定的本機端點) 使用憑證式驗證模式，請取得本機端點必須使用的憑證相關資訊。
- 確保您已設定與此本機端點相關聯的 IPsec VPN 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 導覽至 **網路 > VPN > 本機端點**，然後按一下**新增本機端點**。
- 3 輸入本機端點的名稱。
- 4 從 **VPN 服務**下拉式功能表中，選取要與此本機端點相關聯的 IPsec VPN 服務。
- 5 輸入本機端點的 IP 位址。
- 6 如果您正為 IPsec VPN 工作階段使用憑證式驗證模式，請從**站台憑證**下拉式功能表中，選取將由本機端點使用的憑證。

7 輸入用來識別本機 NSX Edge 執行個體的本機識別碼值。

此本機識別碼是遠端站台上的對等識別碼。此本機識別碼必須是遠端站台的公用 IP 位址或 FQDN。對於使用本機端點定義的憑證型 VPN 工作階段，本機識別碼衍生自與本機端點相關聯的憑證。系統將忽略在本機識別碼文字方塊中指定的識別碼。自 VPN 工作階段憑證衍生的本機識別碼取決於憑證中的延伸。

- 如果憑證中不存在 X509v3 延伸 X509v3 Subject Alternative Name，則會使用辨別名稱 (DN) 做為本機識別碼值。
- 如果在憑證中找到 X509v3 延伸 X509v3 Subject Alternative Name，則會使用其中一個主體別名的做為本機識別碼值。

8 從信任 CA 憑證和信任 CLR 憑證下拉式功能表中，選取所需的適當憑證。

9 指定標籤 (如有需要)。

10 按一下儲存。

新增設定檔

NSX-T Data Center 提供了系統產生的 IPsec 通道設定檔和 IKE 設定檔，在您設定 IPsec VPN 或 L2 VPN 服務時，依預設會指派這些設定檔。系統產生的 DPD 設定檔則是針對 IPsec VPN 組態而建立。

IKE 與 IPsec 設定檔提供了用於在網站間驗證、加密及建立共用密碼之演算法的相關資訊。DPD 設定檔提供了兩次探查相間隔之秒數的相關資訊。

如果您決定不使用 NSX-T Data Center 提供的預設設定檔，可以使用本節後續主題中的資訊自行設定。

新增 IKE 設定檔

網際網路金鑰交換 (IKE) 設定檔提供了在建立 IKE 通道時用於在網站間驗證、加密及建立共用密碼之演算法的相關資訊。

NSX-T Data Center 提供了系統產生的 IKE 設定檔，在您設定 IPsec VPN 或 L2 VPN 服務時，依預設會指派這些設定檔。下表列出了所提供的預設設定檔。

表 5-4. 用於 IPsec VPN 或 L2 VPN 服務的預設 IKE 設定檔

預設 IKE 設定檔名稱	說明
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ 用於 L2 VPN 服務組態。 ■ 設定了 IKE V2、AES 128 加密演算法、SHA2 256 演算法，以及 Diffie-Hellman 群組 14 金鑰交換演算法。
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ 用於 IPsec VPN 服務組態。 ■ 設定了 IKE V2、AES 128 加密演算法、SHA2 256 演算法，以及 Diffie-Hellman 群組 14 金鑰交換演算法。

如果您決定不使用提供的預設 IKE 設定檔，可以使用下列步驟自行設定。

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 按一下**網路 > VPN > 設定檔**索引標籤。
- 3 選取 **IKE 設定檔**設定檔類型，然後按一下**新增 IKE 設定檔**。
- 4 輸入 IKE 設定檔的名稱。
- 5 從 **IKE 版本**下拉式功能表中，選取用於設定 IPSec 通訊協定套件中之安全性關聯 (SA) 的 IKE 版本。

表 5-5. IKE 版本

IKE 版本	說明
IKEv1	選取後，IPSec VPN 會起始並僅回應 IKEv1 通訊協定。
IKEv2	此版本為預設值。選取後，IPSec VPN 會起始並僅回應 IKEv2 通訊協定。
IKE-Flex	如果選取此版本，並且使用 IKEv2 通訊協定建立通道失敗，則來源站台不會回復並使用 IKEv1 通訊協定起始連線。不過，如果遠端站台使用 IKEv1 通訊協定起始連線，則系統會接受連線。

- 6 從下拉式功能表中，選取加密、摘要與 Diffie-Hellman 群組演算法。您可以選取多個要套用的演算法，也可以取消選取任何不想套用的已選取演算法。

表 5-6. 使用的演算法

演算法類型	有效值	說明
加密	<ul style="list-style-type: none"> AES 128 (預設值) AES 256 AES GCM 128 AES GCM 192 AES GCM 256 	<p>在網際網路金鑰交換 (IKE) 交涉期間使用的加密演算法。</p> <p>搭配 IKEv2 使用時，會支援 AES-GCM 演算法。搭配 IKEv1 使用時不支援。</p>
摘要	<ul style="list-style-type: none"> SHA2 256 (預設值) SHA1 SHA2 384 SHA2 512 	<p>要在 IKE 交涉期間使用的安全雜湊演算法。</p> <p>根據 RFC 5282 中的第 8 節，如果 AES-GCM 是加密演算法文字方塊中選取的唯一加密演算法，則無法在摘要演算法文字方塊中指定任何雜湊演算法。此外，會隱含選取偽隨機功能 (PRF) 演算法 PRF HMAC-SHA2 256，且用於 IKE 安全性關聯 (SA) 交涉。也必須在對等閘道上設定 PRF HMAC-SHA2 256 演算法，IKE SA 交涉的階段 1 才會成功。</p> <p>如果在加密演算法文字方塊中指定包含 AES-GCM 演算法的多個演算法，則可以在摘要演算法文字方塊中選取一或多個雜湊演算法。此外，會根據設定的雜湊演算法隱含判斷在 IKE SA 交涉中使用的 PRF 演算法。也必須在對等閘道上設定至少一個相符的 PRF 演算法，IKE SA 交涉的第 1 階段才會成功。例如，如果加密演算法文字方塊包含 AES 128 和 AES GCM 128，並且在摘要演算法文字方塊中指定了 SHA1，那麼在 IKE SA 交涉期間會使用 PRF-HMAC-SHA1 演算法，也必須在對等閘道上設定。</p>
Diffie-Hellman 群組	<ul style="list-style-type: none"> 群組 14 (預設值) 群組 2 群組 5 群組 15 群組 16 群組 19 群組 20 群組 21 	<p>對等站台和 NSX Edge 用於在不安全的通訊通道上建立共用密碼的密碼編譯配置。</p>

備註 當您嘗試使用兩種加密演算法或兩種摘要演算法與 GUARD VPN 用戶端 (之前為 QuickSec VPN 用戶端) 來建立 IPSec VPN 通道時，GUARD VPN 用戶端會在建議的交涉清單中新增額外的演算法。例如，如果您在用來建立 IPSec VPN 通道的 IKE 設定檔中，將 AES 128 和 AES 256 指定為要使用的加密演算法，並將 SHA2 256 和 SHA2 512 指定為摘要演算法，則 GUARD VPN 用戶端也會在交涉清單中建議 AES 192 和 SHA2 384。在此情況下，NSX-T Data Center 會使用您在建立 IPSec VPN 通道時所選取的第一種加密演算法。

- 7 如果您不想為安全性關聯 (SA) 存留時間使用預設值 86400 秒 (24 小時)，則輸入想要使用的值 (以秒為單位)。
- 8 視需要提供說明並新增標籤。

9 按一下儲存。

結果

可用的 IKE 設定檔資料表中即會新增一列。若要編輯或刪除非系統建立的設定檔，請按一下三點功能表 (⋮)，然後從可用的動作清單中選取動作。

新增 IPsec 設定檔

網際網路通訊協定安全性 (IPsec) 設定檔提供了在建立 IPsec 通道時用於在網站間驗證、加密及建立共用密碼之演算法的相關資訊。

NSX-T Data Center 提供了系統產生的 IPsec 設定檔，在您設定 IPsec VPN 或 L2 VPN 服務時，依預設會指派這些設定檔。下表列出了所提供的預設設定檔。

表 5-7. 用於 IPsec VPN 或 L2 VPN 服務的預設 IPsec 設定檔

預設 IPsec 設定檔的檔案名稱	說明
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ 用於 L2 VPN。 ■ 設定了 AES GCM 128 加密演算法和 Diffie-Hellman 群組 14 金鑰交換演算法。
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ 用於 IPsec VPN。 ■ 設定了 AES GCM 128 加密演算法和 Diffie-Hellman 群組 14 金鑰交換演算法。

如果您決定不使用提供的預設 IPsec 設定檔，可以使用下列步驟自行設定。

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 導覽到 **網路 > VPN > 設定檔** 索引標籤。
- 3 選取 **IPsec 設定檔** 設定檔類型，然後按一下 **新增 IPsec 設定檔**。
- 4 輸入 IPsec 設定檔的名稱。
- 5 從下拉式功能表中，選取加密、摘要與 Diffie-Hellman 演算法。您可以選取多個要套用的演算法。
取消選取您不想使用的演算法。
- 6 如果您決定不在 VPN 服務中使用 PFS 群組通訊協定，請取消選取 **PFS 群組**。
依預設會選取此選項。
- 7 在 **SA 存留時間** 文字方塊中，修改必須重新建立 IPsec 通道之前所經過的預設秒數。
依預設，使用 24 小時 (86400 秒) 的 SA 存留時間。
- 8 選取要與 IPsec 通道搭配使用的 **DF 位元值**。
此值決定如何處理所收到資料封包中包含的「不分段」(DF) 位元。下表說明可接受的值。

表 5-8. DF 位元值

DF 位元值	說明
COPY	預設值。選取此值後，NSX-T Data Center 會將所收到封包中的 DF 位元值複製到轉送的封包中。此值表示如果所收到的資料封包設定有 DF 位元，加密後，該封包也設定有 DF 位元。
CLEAR	選取此值後，NSX-T Data Center 會忽略所收到資料封包中的 DF 位元值，加密封包中的 DF 位元一律為 0。

9 視需要提供說明並新增標籤。

10 按一下**儲存**。

結果

可用的 IPSec 設定檔資料表中即會新增一列。若要編輯或刪除非系統建立的設定檔，請按一下三點功能表 (⋮)，然後從可用的動作清單中選取動作。

新增 DPD 設定檔

DPD (無作用對等偵測) 設定檔提供偵測 IPSec 對等項是否處於運作中狀態的多次探查之間等待秒數的相關資訊。

NSX-T Data Center 提供由系統產生之名為 `nsx-default-l3vpn-dpd-profile` 的 DPD 設定檔，這是在設定 IPSec VPN 服務時由系統預設指派的 DPD 設定檔。

如果您決定不使用系統提供的預設 DPD 設定檔，可以使用下列步驟設定您自己的 DPD 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 導覽到 **網路 > VPN > 設定檔**。
- 3 選取 **DPD 設定檔** 設定檔類型，然後按一下 **新增 DPD 設定檔**。
- 4 輸入 DPD 設定檔的名稱。
- 5 在 **DPD 探查時間間隔** 文字方塊中，輸入您想要 NSX-T Data Center 等候的秒數，之後才傳送下一個 DPD 探查。預設為 60 秒。

如果 NSX Edge 節點從遠端對等站台收到回應，DPD 探查時間間隔計時器會重新啟動。如果 NSX Edge 節點未在傳送下一個 DPD 探查之後的 0.5 秒內收到對等站台的回應，重新傳輸計時器會設定為 0.5 秒。NSX Edge 節點會在達到重新傳輸計時器之後，重新傳輸下一個 DPD 探查。如果遠端對等站台持續不回應，重新傳輸計時器會大幅增加至 6 秒的上限。每當重新傳輸計時器到期，NSX Edge 節點會繼續重新傳輸 DPD 探查。NSX Edge 節點會重新傳輸最多 30 次，之後才會將對等站台宣告為無作用，並且會將無作用對等連結上的安全性關聯 (SA) 移除。重新傳輸 DPD 探查 30 次所需的時間總計大約為 2 分鐘 45 秒。

6 視需要提供說明並新增標籤。

7 按一下**儲存**。

結果

可用 DPD 設定檔資料表中會新增一列資料列。若要編輯或刪除非系統建立的設定檔，請按一下三點功能表 (⋮)，然後從可用的動作清單中選取動作。

檢查 IPsec VPN 工作階段的實現狀態

在傳送 IPsec VPN 工作階段的組態更新要求後，您可以在傳輸節點上的 NSX-T Data Center 本機控制平面中查看要求的狀態是否已成功處理。

建立 IPsec VPN 工作階段時，會建立多個實體：IKE 設定檔、DPD 設定檔、通道設定檔、本機端點、IPsec VPN 服務，以及 IPsec VPN 工作階段。所有這些實體共用相同的 `IPsecVPNSession` 橫跨範圍，因此您可以使用同一個 GET API 呼叫來取得 IPsec VPN 工作階段之所有實體的實現狀態。您可以僅使用 API 來查看實現狀態。

必要條件

- 自行熟悉 IPsec VPN。請參閱[瞭解 IPsec VPN](#)。
- 確認已成功設定 IPsec VPN。請參閱[新增 IPsec VPN 服務](#)。
- 您必須具有 NSX Manager API 的存取權。

程序

- 1 傳送 POST、PUT 或 DELETE 要求 API 呼叫。

例如：

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPsecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
        {
          "subnet": "1.1.1.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "2.1.4..0/24"
        }
      ]
    }
  ]
}
```

```

        "action": "PROTECT",
        "enabled": true,
        "_revision": 1
    }
]
}

```

- 2 在傳回的回應標頭中找到並複製 `x-nsx-requestid` 的值。

例如：

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 使用下列 GET 呼叫來要求 IPSec VPN 工作階段的實現狀態。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

下列 API 呼叫使用上述步驟所用範例中的 `id` 和 `x-nsx-requestid` 值。

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?
request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

以下是您在實現狀態為 `in_progress` 時收到的回應範例。

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization
is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}

```

以下是您在實現狀態為 `in_sync` 時收到的回應範例。

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ]
}

```

```

    }
  ],
  "state": "in_sync"
}

```

以下是您在實現狀態為 **unknown** 時收到的可能回應範例。

```

{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}

```

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
      "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}

```

在執行實體 **DELETE** 作業之後，您可能會收到 **NOT_FOUND** 狀態，如下列範例所示。

```

{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}

```

如果停用與此工作階段相關聯的 **IPSec VPN** 服務，您會收到 **BAD_REQUEST** 回應，如下列範例所示。

```

{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization status."
}

```

監控和疑難排解 VPN 工作階段

設定 IPsec 或 L2 VPN 工作階段後，您可以監控 VPN 通道狀態，並使用 NSX Manager 使用者介面對任何報告的通道問題進行疑難排解。

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 導覽至 **網路 > VPN > IPsec 工作階段** 或 **網路 > VPN > L2 VPN 工作階段** 索引標籤。
- 3 展開您要監控或疑難排解的 VPN 工作階段的資料列。
- 4 若要檢視 VPN 通道狀態的狀態，請按一下資訊圖示。
[狀態] 對話方塊隨即出現，並顯示可用的狀態。
- 5 若要檢視 VPN 通道流量統計資料，請按一下 [狀態] 資料行中的**檢視統計資料**。
[統計資料] 對話方塊隨即顯示 VPN 通道的流量統計資料。
- 6 若要檢視錯誤統計資料，請按一下 [統計資料] 對話方塊中的**檢視更多連結**。
- 7 若要關閉**統計資料**對話方塊，請按一下**關閉**。

網路位址轉譯

6

網路位址轉譯 (NAT) 會將一個 IP 位址空間對應至另一個。您可以在第 0 層和第 1 層閘道上設定 NAT。

本章節討論下列主題：

- 在閘道上設定 NAT

在閘道上設定 NAT

您可以在第 0 層或第 1 層閘道上設定來源 NAT (SNAT)、目的地 NAT (DNAT) 或自反 NAT。

如果第 0 層閘道是以主動-主動式模式執行，則您無法設定 SNAT 或 DNAT，因為非對稱路徑可能會發生問題。您只能設定自反 NAT (有時稱為無狀態 NAT)。如果第 0 層閘道是以主動-待命模式執行，則您可以設定 SNAT、DNAT 或自反 NAT。

您也可以針對某個 IP 位址或位址範圍停用 SNAT 或 DNAT。如果位址具有多個 NAT 規則，則會套用優先順序最高的規則。

在第 0 層閘道的外部介面上設定的 SNAT 會處理來自第 1 層閘道的流量，以及來自第 0 層閘道上另一個外部介面的流量。

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**網路 > NAT**。
- 3 選取閘道。
- 4 按一下**新增 NAT 規則**。
- 5 選取動作。

對於第 1 層閘道，可用動作包括 **SNAT**、**DNAT**、**自反**、**無 SNAT** 和**無 DNAT**。

對於以主動-待命模式執行的第 0 層閘道，可用動作包括 **SNAT**、**DNAT**、**無 SNAT** 和**無 DNAT**。

對於以主動-主動式模式執行的第 0 層閘道，可用動作是**自反**。

- 6 在**服務**資料行中，按一下**設定**以選取服務。

- 7** (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。

- 8** 對於**目的地 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** 輸入**轉譯的連接埠**的值。

- 11** 從下列選項中選取防火牆設定：

- **符合外部位址** - 封包會根據符合已轉譯的 IP 位址與轉譯的連接埠組合的防火牆規則進行處理。
- **符合內部位址** - 封包會根據符合原始 IP 位址與原始連接埠組合的防火牆規則進行處理。
- **略過** - 封包會略過防火牆規則。

- 12** (必要) 變更記錄狀態。

- 13** (必要) 針對**套用至**，選取要套用此規則的物件。

可用的物件包括**第 0 層閘道**、**介面**、**標籤**、**服務執行個體端點**和**虛擬端點**。

- 14** 指定優先順序值。

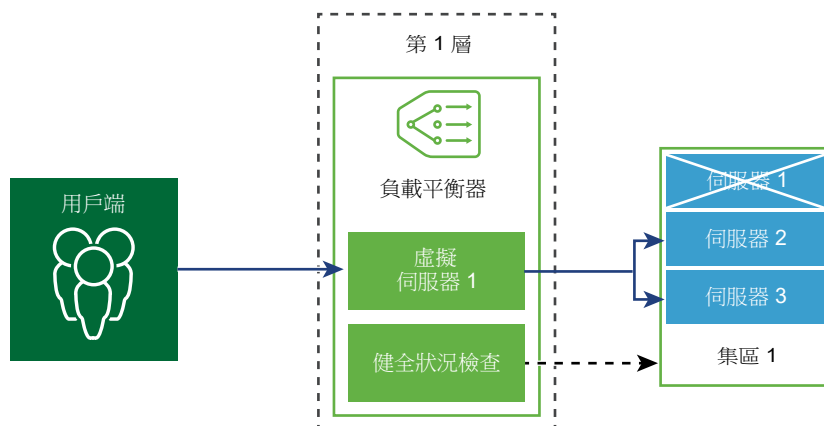
較低的值表示較高的優先順序。預設值為 100。

- 15** 按一下**儲存**。

負載平衡

7

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 層開道支援邏輯負載平衡器。一個負載平衡器只能連結至第 1 層開道。

本章節討論下列主題：

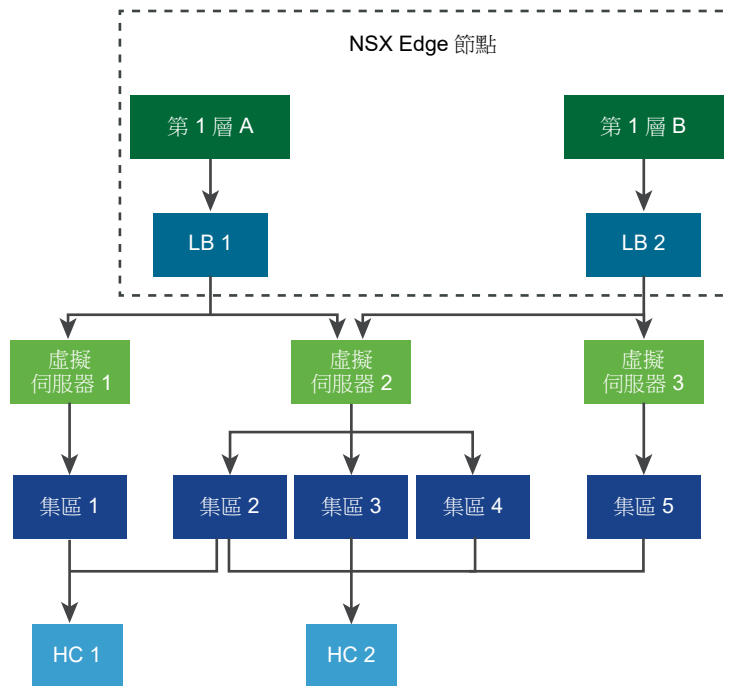
- [主要負載平衡器概念](#)
- [設定負載平衡器元件](#)

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。

備註 在[進階與安全性](#)索引標籤中，第 1 層邏輯路由器一詞用來指第 1 層閘道。

表 7-1. 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	20	100	1000
每個負載平衡器的集區數目	60	300	3000
每個負載平衡器的集區成員數目	300	2000	7500

負載平衡器已連結至一個第 1 層邏輯路由器。這個必須處於主動備用模式的第 1 層邏輯路由器裝載於 NSX Edge 節點上。

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 7-2. 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	300
NSX Edge 虛擬機器 - 大型	40	4	1	7500
NSX Edge 虛擬機器 - 裸機	750	75	18	30,000

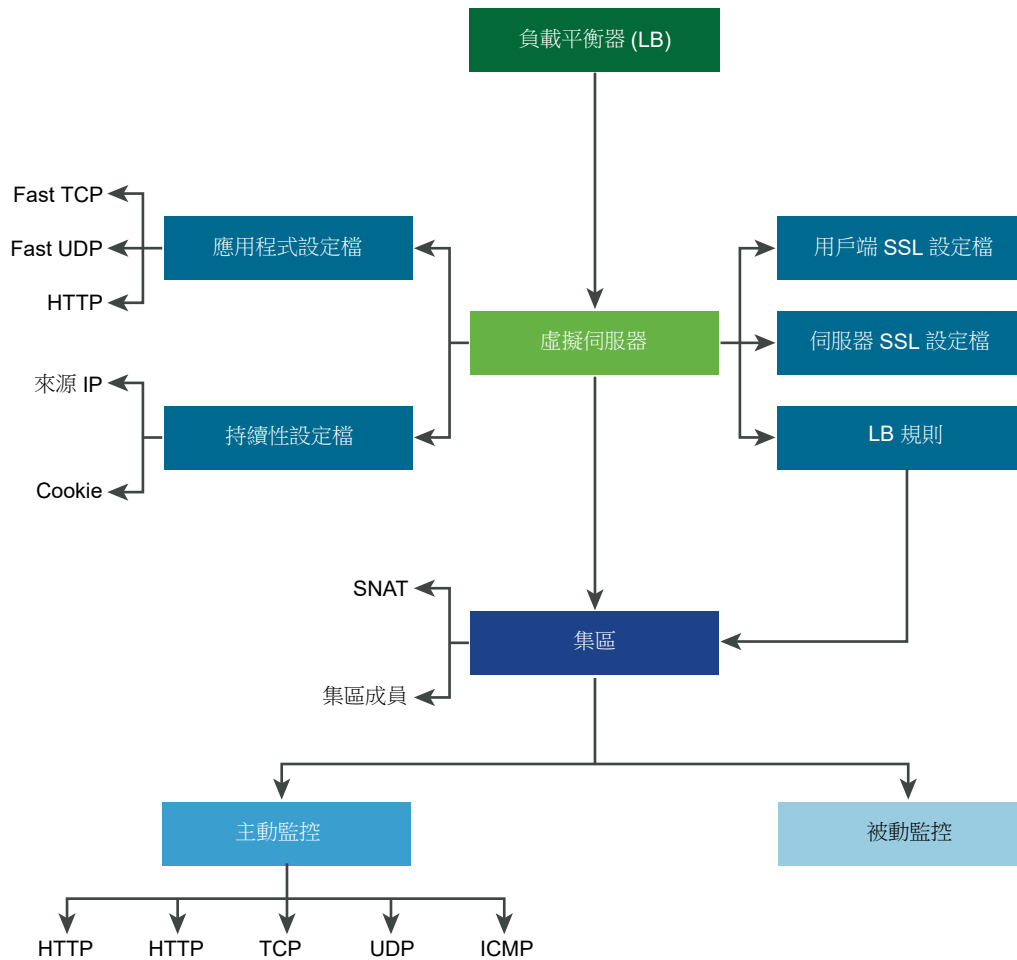
支援的負載平衡器功能

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 Limited Export 版本不支援 SSL 終止模式和 Proxy 模式。

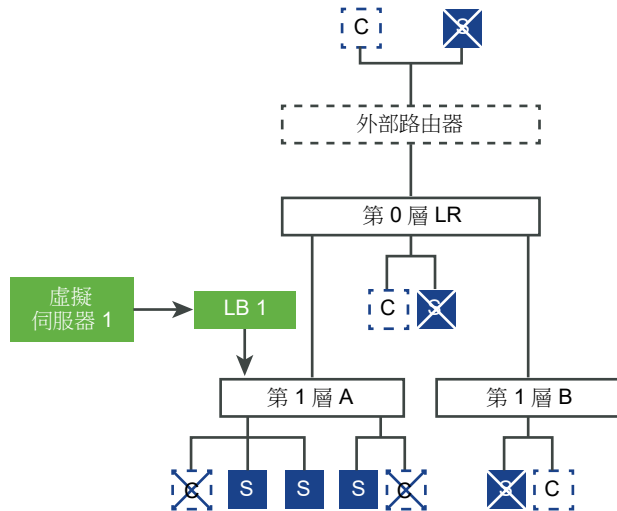


負載平衡器拓撲

負載平衡器通常在內嵌或單一裝載模式下進行部署。單一裝載模式需要虛擬伺服器來源 NAT (SNAT) 組態，而內嵌模式則不需要。

內嵌拓撲

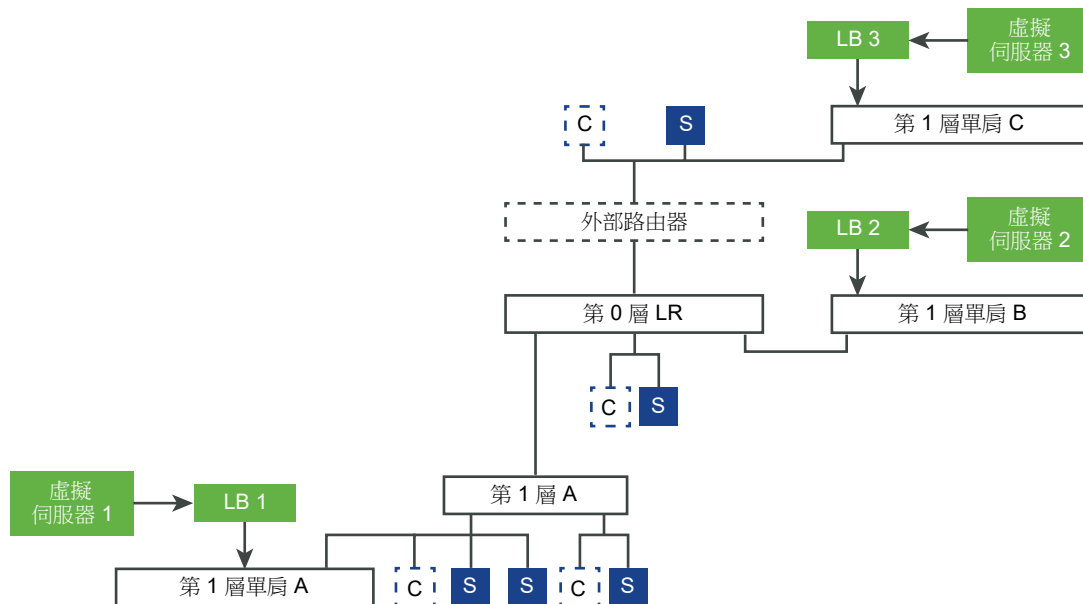
在內嵌模式下，負載平衡器位於用戶端與伺服器之間的流量路徑中。如果不想在負載平衡器上有 **SNAT**，用戶端和伺服器不應連線到相同第 1 層邏輯路由器上的覆疊區段。如果用戶端和伺服器連線至相同第 1 層邏輯路由器上的覆疊區段，則需要 **SNAT**。



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。負載平衡器會將回應轉送至用戶端。



第 1 層服務鏈結

如果第 1 層閘道或邏輯路由器主控不同的服務 (例如 NAT、防火牆和負載平衡器)，則會依下列順序套用服務：

- 入口

DNAT - 防火牆 - 負載平衡器

附註：如果 DNAT 設定了防火牆略過，則會略過防火牆，但不會略過負載平衡器。

■ 出口

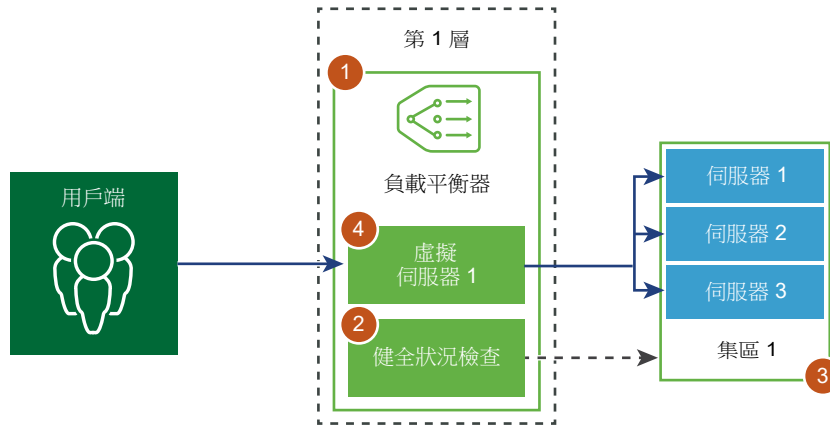
負載平衡器 - 防火牆 - SNAT

設定負載平衡器元件

若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 層閘道進行啟動。

備註 在**進階與安全性**索引標籤中，第 1 層邏輯路由器一詞是指第 1 層閘道。

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，並將新建立的虛擬伺服器連結至負載平衡器。



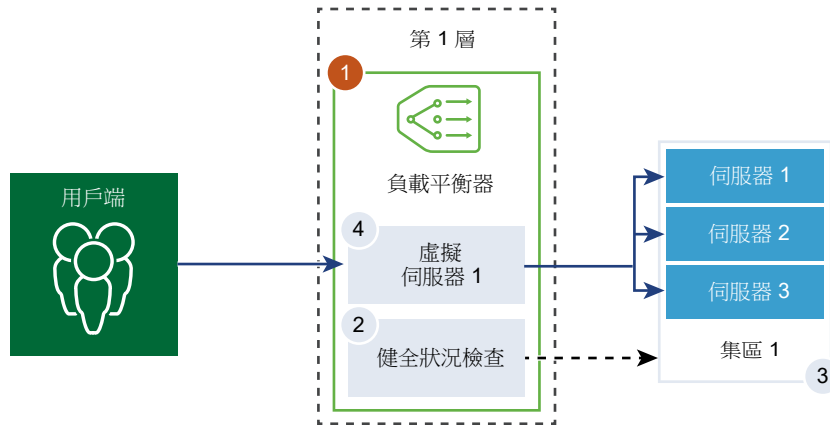
新增負載平衡器

負載平衡器將會建立並連結至第 1 層閘道。

備註 在**進階與安全性**索引標籤中，第 1 層邏輯路由器一詞是指第 1 層閘道。

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 層閘道。請參閱[第 3 章 第 1 層閘道](#)。

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 > 新增負載平衡器**。

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 從下拉式功能表中選取要連結至此負載平衡器的已設定第 1 層閘道。

第 1 層閘道必須處於主動-待命模式。

6 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。

7 (選擇性) 輸入標籤使搜尋更輕鬆。

您可以指定標籤，以設定標籤範圍。

8 切換按鈕，以停用負載平衡器的管理狀態。

9 按一下**儲存**。

建立負載平衡器並將其連結至第 1 層閘道大約需要三分鐘，在這段期間，組態狀態會顯示為綠色和 [啟動]。

如果狀態是 [關閉]，請按一下資訊圖示，然後解決錯誤後再繼續操作。

10 (選擇性) 刪除負載平衡器。

a 從虛擬伺服器和第 1 層閘道中斷連結負載平衡器。

b 選取負載平衡器。

c 按一下垂直省略符號按鈕。

d 選取**刪除**。

新增主動監視器

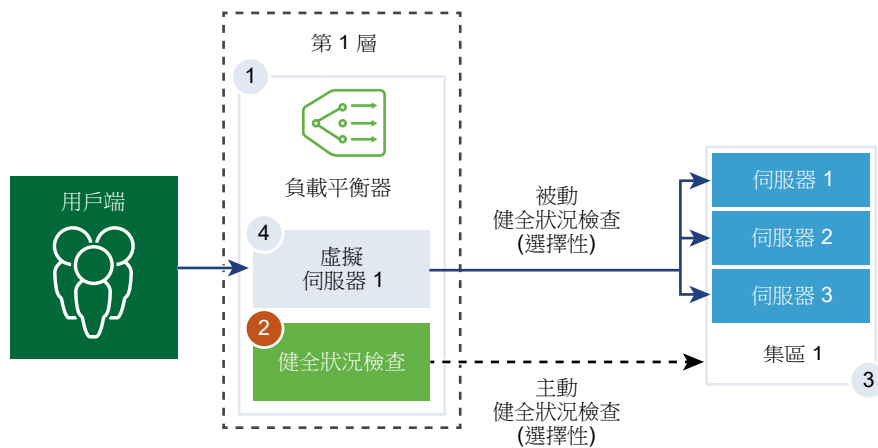
主動健全狀況監視器可用來測試伺服器是否可用。主動健全狀況監視器使用數種類型的測試，例如傳送基本 Ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

備註 在**進階與安全性**索引標籤中，第 1 層邏輯路由器一詞是指第 1 層閘道。

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 層閘道之後，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**網路 > 負載平衡 > 監控 > 主動 > 新增主動監視器**。

3 從下拉式功能表中選取伺服器的通訊協定。

您也可以為 NSX Manager 使用預先定義的通訊協定；HTTP、HTTPS、ICMP、TCP 和 UDP。

4 選取 **HTTP** 通訊協定。

5 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
名稱與說明	輸入主動健全狀況監視器的名稱和說明。
監控連接埠	設定監控連接埠的值。
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)。
逾時期間	設定伺服器被視為 [關閉] 之前所經過的測試次數。
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。

選項	說明
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。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

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]。

- 6 按一下**設定**。
- 7 輸入 HTTP 要求和回應組態詳細資料。

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。
HTTP 回應標頭	按一下 新增 ，然後輸入 HTTP 回應標頭名稱和相對應的值。 預設標頭值為 4000。最大標頭值為 64,000。
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 選取 **HTTPS** 通訊協定。
- 9 完成步驟 5。
- 10 按一下**設定**。
- 11 輸入 HTTP 要求和回應，以及 SSL 組態詳細資料。

選項	說明
名稱與說明	輸入主動健全狀況監視器的名稱和說明。
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。
HTTP 回應標頭	按一下 新增 ，然後輸入 HTTP 回應標頭名稱和相對應的值。 預設標頭值為 4000。最大標頭值為 64,000。

選項	說明
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。
伺服器 SSL	開啟按鈕以啟用 SSL 伺服器。
用戶端憑證	(選用) 如果伺服器未以相同 IP 位址裝載多個主機名稱或用戶端不支援 SNI 延伸，請從下拉式功能表中選取要使用的憑證。
伺服器 SSL 設定檔	(選用) 從下拉式功能表中指派一個預設 SSL 設定檔，其定義可重複使用和獨立於應用程式的用戶端 SSL 內容。 按一下垂直省略符號，然後建立自訂的 SSL 設定檔。
受信任的 CA 憑證	(選用) 您可以要求用戶端具有用於驗證的 CA 憑證。
強制伺服器驗證	(選用) 開啟按鈕以啟用伺服器驗證。
憑證鏈結深度	(選用) 設定用戶端憑證鏈結的驗證深度。
憑證撤銷清單	(選用) 在用戶端 SSL 設定檔中設定憑證撤銷清單 (CRL)，以拒絕已損毀的用戶端憑證。

12 選取 **ICMP** 通訊協定。

13 完成步驟 5，並指派 ICMP 健全狀況檢查封包的資料大小 (以位元組為單位)。

14 選取 **TCP** 通訊協定。

15 完成步驟 5，您可以將 TCP 資料參數留空。

如果未列出傳送及預期資料，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。

如果列出的資料必須是字串，則為預期資料。不支援規則運算式。

16 選取 **UDP** 通訊協定。

17 完成步驟 5，並設定 UDP 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]。

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[新增伺服器集區](#)。

新增被動監視器

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來確認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 > 監控 > 被動 > 新增被動監視器**。
- 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。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

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。

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[新增伺服器集區](#)。

新增伺服器集區

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。

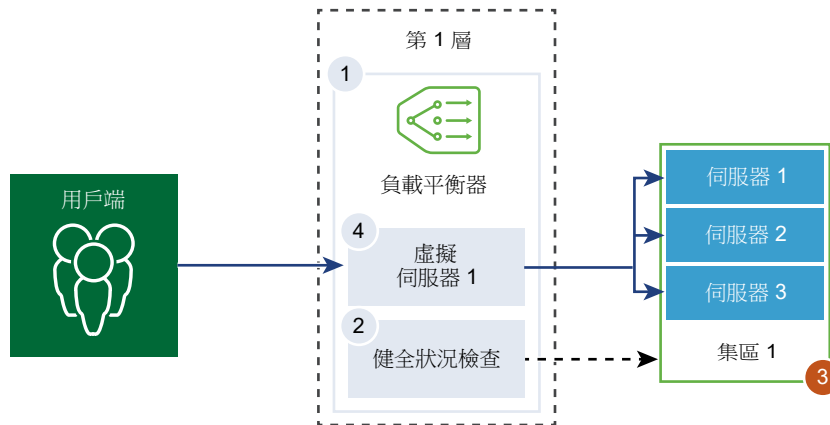
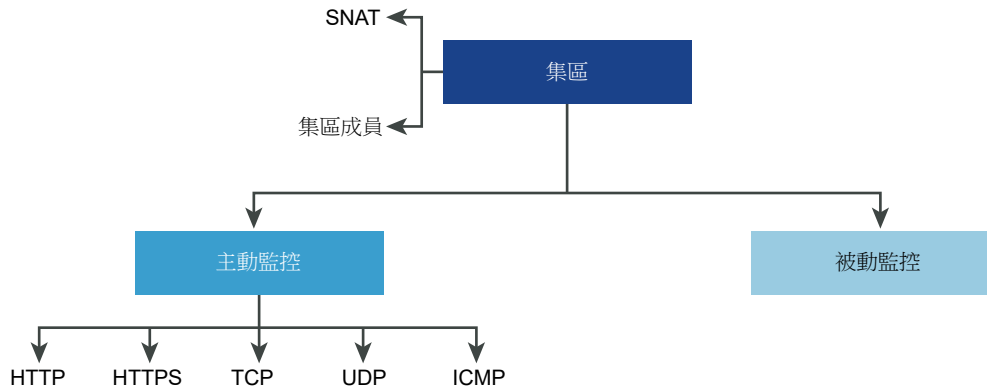


圖 7-1. 伺服器集區參數組態



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](#)。
- 確認您已設定被動健全狀況監視器。請參閱[新增被動監視器](#)。

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 > 伺服器集區 > 新增伺服器集區**。

3 輸入負載平衡器伺服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。

4 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在可用的伺服器資源之間散佈負載。 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 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。

選項	說明
輸入個別成員	<p>輸入集區成員的名稱、IP 位址和連接埠。</p> <p>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。</p> <p>您可以設定伺服器集區管理狀態。依預設，新增伺服器集區成員時，此選項處於啟用狀態。</p> <p>如果停用此選項，會處理作用中連線，且不會針對新連線選取此伺服器集區成員。新連線會指派給集區的其他成員。</p> <p>如果是正常停用，可讓您移除伺服器以進行維護。系統會繼續處理處於此狀態的伺服器集區中成員的現有連線。</p> <p>切換按鈕以將某個集區成員指定為備用成員，以便使用健全狀況監視器提供主動備用狀態。如果作用中成員未通過健全狀況檢查，流量就會容錯移轉給備用成員。系統在選取伺服器期間會略過備用成員。當伺服器集區處於非作用中狀態時，傳入的連線僅會傳送給設有道歉頁面來表示應用程式無法使用的備用成員。</p> <p>[並行連線數目上限] 值會指派連線數目上限，以便伺服器集區成員不會因超載而在選取伺服器期間被略過。若未指定此值，則連線數目無限制。</p>
選取群組	<p>選取預先設定的伺服器集區成員群組。</p> <p>輸入群組的名稱、(選用) 說明以及網域。請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。</p> <p>從現有清單中設定計算成員，或是自行建立。您可以指定成員資格準則、選取群組成員、將 IP 與 MAC 位址新增為群組成員，以及新增 Active Directory 群組。身分識別成員會與計算成員相交，以定義群組的成員資格。</p> <p>輸入標籤使搜尋更輕鬆。您可以指定標籤，以設定標籤範圍。</p> <p>您可以選擇性地定義最大群組 IP 位址清單。</p>

6 從下拉式功能表中，為伺服器集區選取主動健全狀況監視器。

無論資料流量如何，負載平衡器均會定期向伺服器傳送 ICMP Ping 來確認健全狀況。每個伺服器集區只能設定一個主動健全狀況檢查監視器。

7 選取 [來源 NAT] (SNAT) 轉譯模式。

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
自動對應模式	<p>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。</p> <p>需要 SNAT。</p> <p>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。</p> <p>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。</p>
停用	停用 SNAT 轉譯模式。
IP 集區	<p>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。</p> <p>依預設，4000 - 64000 連接埠範圍用於所有設定的 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。</p> <p>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。</p> <p>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。</p>

8 切換按鈕以啟用 TCP 多工處理。

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。

9 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。

10 輸入伺服器集區必須始終擁有的作用中成員的數目下限。

11 從下拉式功能表中，為伺服器集區選取被動健全狀況監視器。

12 輸入標籤使搜尋更輕鬆。

您可以指定標籤，以設定標籤範圍。

設定虛擬伺服器元件

您可以設定第 4 層和第 7 層虛擬伺服器並設定多個虛擬伺服器元件，例如，應用程式設定檔、持續性設定檔和負載平衡器規則。

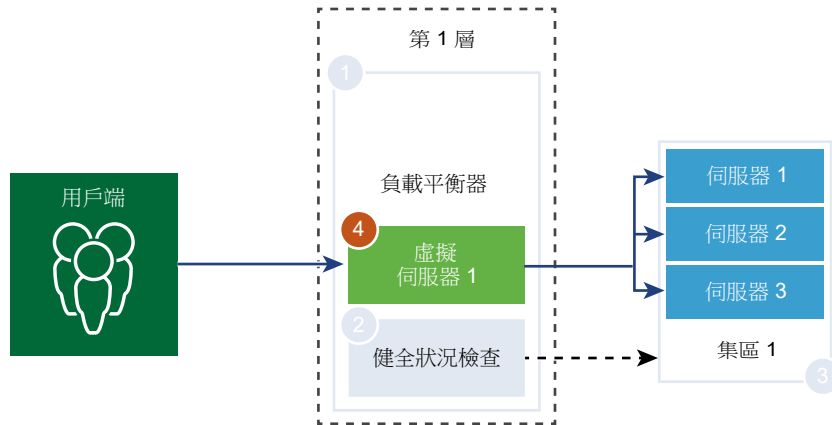
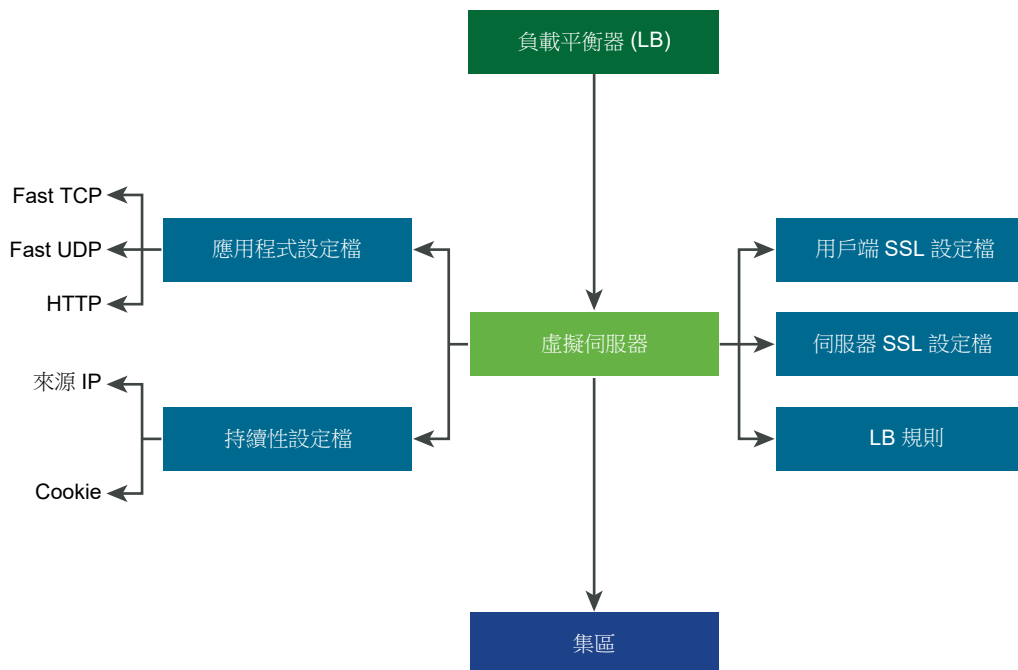


圖 7-2. 虛擬伺服器元件



新增應用程式設定檔

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。

當負載平衡器必須以第 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停止 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停止用戶端 TCP 連線，然後再選取伺服器集區成員。

圖 7-3. 第 4 層 TCP 和 UDP 應用程式設定檔

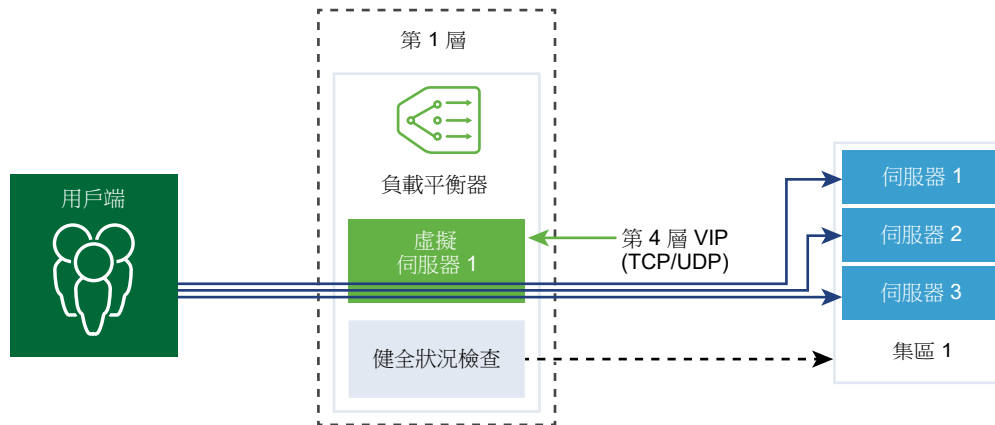
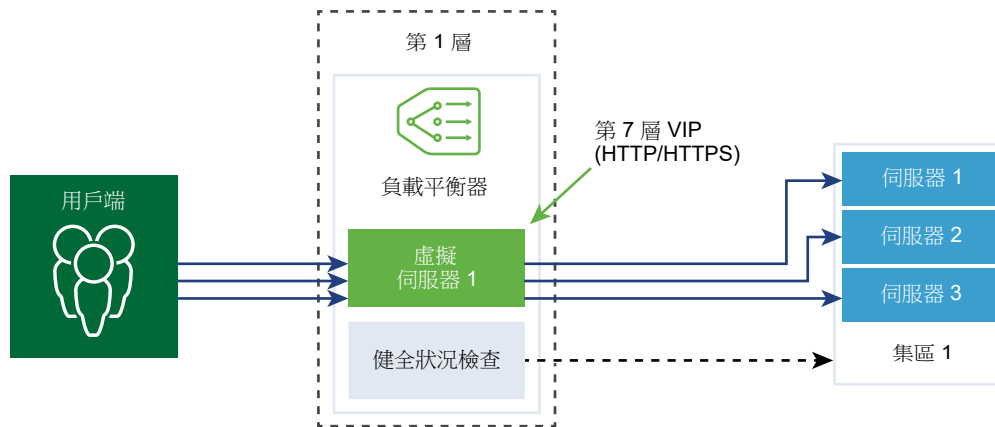


圖 7-4. 第 7 層 HTTPS 應用程式設定檔



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 > 設定檔 > 應用程式 > 新增應用程式設定檔。
- 3 選取**快速 TCP** 應用程式設定檔，並輸入設定檔詳細資料。

也可以接受預設的快速 TCP 設定檔設定。

選項	說明
名稱與說明	輸入快速 TCP 應用程式設定檔的名稱和說明。
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。
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。

選項	說明
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。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

4 選取**快速 UDP** 應用程式設定檔，並輸入設定檔詳細資料。

也可以接受預設的 UDP 設定檔設定。

選項	說明
名稱與說明	輸入快速 UDP 應用程式設定檔的名稱和說明。
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。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

5 選取**HTTP** 應用程式設定檔，並輸入設定檔詳細資料。

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。

選項	說明
名稱與說明	輸入 HTTP 應用程式設定檔的名稱和說明。
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)。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ 插入 - 如果傳入要求中沒有 XFF HTTP 標頭存在，則負載平衡器會插入具有用戶端 IP 位址的新 XFF 標頭。如果傳入要求中有 XFF HTTP 標頭存在，則負載平衡器會附加具有用戶端 IP 位址的 XFF 標頭。 ■ 取代 - 如果傳入要求中有 XFF HTTP 標頭存在，則負載平衡器會取代標頭。 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。
要求本文大小	輸入用於儲存 HTTP 要求本文的緩衝區大小上限值。 如果不指定大小，則要求本文大小無限制。

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。
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>
標籤	<p>輸入標籤使搜尋更輕鬆。</p> <p>您可以指定標籤，以設定標籤範圍。</p>

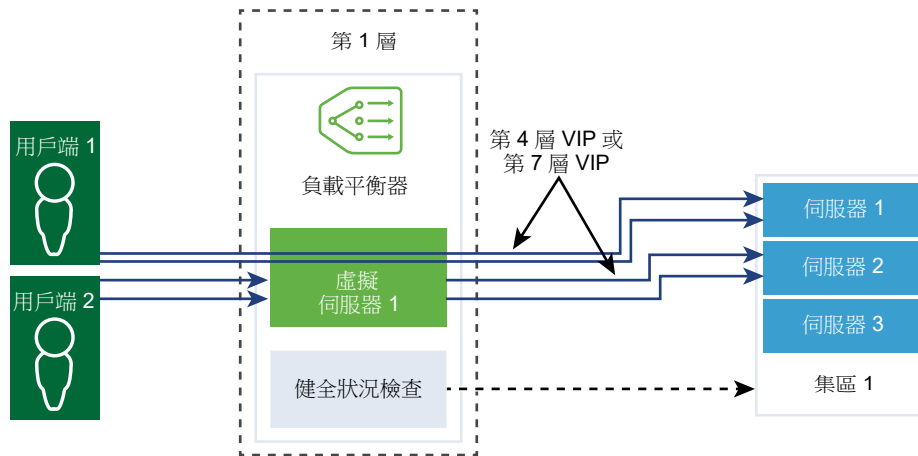
新增持續性設定檔

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 持續性設定檔會根據來源 IP 位址對工作階段進行追蹤。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 持續性設定檔會插入唯一 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來提供 Cookie 持續性。第 7 層虛擬伺服器只能使用 Cookie 持續性設定檔。



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 > 設定檔 > 持續性 > 新增持續性設定檔。
- 3 選取來源 IP 以新增來源 IP 持續性設定檔，然後輸入設定檔詳細資料。

也可以接受預設的來源 IP 設定檔設定。

選項	說明
名稱與說明	輸入來源 IP 持續性設定檔的名稱和說明。
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>
填滿時清除項目	<p>開啟此按鈕以在持續性資料表已滿時清除項目。</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>

選項	說明
HA 持續性鏡像	切換按鈕，將持續性項目同步至 HA 對等項。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

4 選取 **Cookie** 持續性設定檔，然後輸入設定檔詳細資料。

選項	說明
名稱與說明	輸入 Cookie 持續性設定檔的名稱和說明。
共用持續性	開啟按鈕，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 <code><name>.<profile-id>.<pool-id></code> 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有 Cookie 持續性，並由集區成員限定。負載平衡器將以 <code><name>.<virtual_server_id>.<pool_id></code> 格式插入 Cookie。
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 後援	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。 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。
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	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。加密 Cookie 伺服器 IP 位址和連接埠資訊。
Cookie 類型	從下拉式功能表中選取 Cookie 類型。 工作階段 Cookie - 不會儲存。將在瀏覽器關閉後遺失。 持續性 Cookie - 由瀏覽器儲存。不會在瀏覽器關閉後遺失。
閒置時間上限	輸入 Cookie 到期之前 Cookie 類型可閒置的時間 (以秒為單位)。
Cookie 存留期上限	針對工作階段 Cookie 類型，輸入 Cookie 可供使用的時間 (以秒為單位)。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

新增 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 伺服器並停止用戶端 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 7-5. SSL 卸載

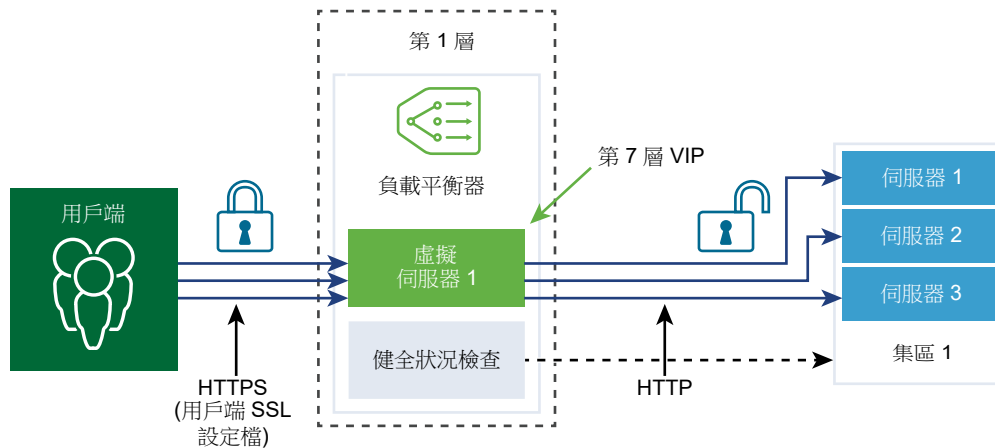
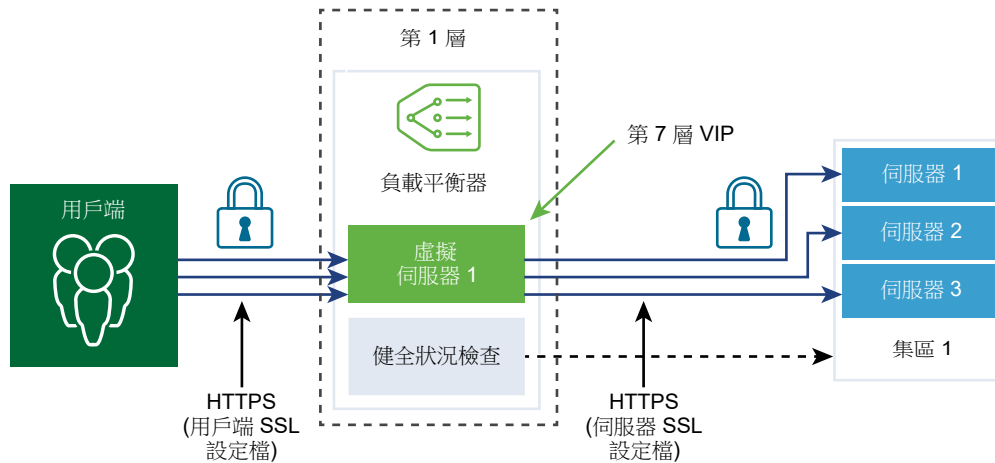


圖 7-6. 端對端 SSL



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 > 設定檔 > SSL 設定檔**。
- 3 選取 **用戶端 SSL 設定檔**，然後輸入設定檔詳細資料。

選項	說明
名稱與說明	輸入用戶端 SSL 設定檔的名稱和說明。
SSL 套件	從下拉式功能表中選取 SSL 加密方式群組，系統會填入要包含在用戶端 SSL 設定檔中的可用 SSL 加密方式和 SSL 通訊協定。 預設是平衡的 SSL 加密方式群組。
工作階段快取	切換按鈕，以允許 SSL 用戶端和伺服器重複使用先前交涉的安全性參數，從而避免 SSL 信號交換期間昂貴的公開金鑰作業。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。
支援的 SSL 加密方式	根據 SSL 套件，此處會填入您所指派之支援的 SSL 加密方式。按一下 檢視更多 以檢視完整清單。 如果您選取 自訂 ，則您必須從下拉式功能表中選取 SSL 加密方式。
支援的 SSL 通訊協定	根據 SSL 套件，此處會填入您所指派之支援的 SSL 通訊協定。按一下 檢視更多 以檢視完整清單。 如果您選取 自訂 ，則您必須從下拉式功能表中選取 SSL 加密方式。
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。

4 選取伺服器 SSL 設定檔，然後輸入設定檔詳細資料。

選項	說明
名稱與說明	輸入伺服器 SSL 設定檔的名稱和說明。
SSL 套件	從下拉式功能表中選取 SSL 加密方式群組，系統會填入要包含在伺服器 SSL 設定檔中的可用 SSL 加密方式和 SSL 通訊協定。 預設是平衡的 SSL 加密方式群組。
工作階段快取	切換按鈕，以允許 SSL 用戶端和伺服器重複使用先前交涉的安全性參數，從而避免 SSL 信號交換期間昂貴的公開金鑰作業。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。
支援的 SSL 加密方式	根據 SSL 套件，此處會填入您所指派之支援的 SSL 加密方式。按一下 檢視更多 以檢視完整清單。 如果您選取 自訂 ，則您必須從下拉式功能表中選取 SSL 加密方式。
支援的 SSL 通訊協定	根據 SSL 套件，此處會填入您所指派之支援的 SSL 通訊協定。按一下 檢視更多 以檢視完整清單。 如果您選取 自訂 ，則您必須從下拉式功能表中選取 SSL 加密方式。
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。

新增第 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，拒絕與虛擬服务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，則與該虛擬服务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[新增應用程式設定檔](#)。
- 確認持續性設定檔可供使用。請參閱[新增持續性設定檔](#)。
- 確認用戶端與伺服器的 SSL 設定檔可供使用。請參閱[新增 SSL 設定檔](#)。
- 確認伺服器集區可供使用。請參閱[新增伺服器集區](#)。
- 確認負載平衡器可供使用。請參閱[新增負載平衡器](#)。

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 > 虛擬伺服器 > 新增虛擬伺服器。

3 選取 **L4 TCP** 通訊協定，然後輸入通訊協定詳細資料。

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。

選項	說明
名稱與說明	輸入第 4 層虛擬伺服器的名稱和說明。
IP 位址	輸入虛擬伺服器的 IP 位址。
連接埠	輸入虛擬伺服器的連接埠號碼。
負載平衡器	從下拉式功能表中選取要連結至此第 4 層虛擬伺服器的現有負載平衡器。
伺服器集區	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。 您可以按一下垂直省略符號來建立伺服器集區。
應用程式設定檔	根據通訊協定類型，現有應用程式設定檔會自動填入。 您可以按一下垂直省略符號來建立應用程式設定檔。
持續性	從下拉式功能表中選取現有的持續性設定檔。 可以在虛擬伺服器上啟用持續性設定檔，讓與來源 IP 相關的用戶端連線均傳送至同一個伺服器。
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。
Sorry Server 集區	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。 您可以按一下垂直省略符號來建立伺服器集區。
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。
管理狀態	切換按鈕以停用第 4 層虛擬伺服器的管理狀態。
存取記錄	切換按鈕以啟用第 4 層虛擬伺服器的記錄。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

4 選取 **L4 UDP** 通訊協定，然後輸入通訊協定詳細資料。

選項	說明
名稱與說明	輸入第 4 層虛擬伺服器的名稱和說明。
IP 位址	輸入虛擬伺服器的 IP 位址。

選項	說明
連接埠	輸入虛擬伺服器的連接埠號碼。
負載平衡器	從下拉式功能表中選取要連結至此第 4 層虛擬伺服器的現有負載平衡器。
伺服器集區	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。 您可以按一下垂直省略符號來建立伺服器集區。
應用程式設定檔	根據通訊協定類型，現有應用程式設定檔會自動填入。 您可以按一下垂直省略符號來建立應用程式設定檔。
持續性	從下拉式功能表中選取現有的持續性設定檔。 可以在虛擬伺服器上啟用持續性設定檔，讓與來源 IP 相關的用戶端連線均傳送至同一個伺服器。
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。
Sorry Server 集區	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。 您可以按一下垂直省略符號來建立伺服器集區。
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。
管理狀態	切換按鈕以停用第 4 層虛擬伺服器的管理狀態。
存取記錄	切換按鈕以啟用第 4 層虛擬伺服器的記錄。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

新增第 7 層 HTTP 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。

備註 NSX-T Data Center 3.0 及更新版本支援第 7 層 SSL 傳遞。

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。

備註 NSX-T Data Center 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 Fast TCP 設定檔。

必要條件

- 確認應用程式設定檔可供使用。請參閱[新增應用程式設定檔](#)。
- 確認持續性設定檔可供使用。請參閱[新增持續性設定檔](#)。
- 確認用戶端與伺服器的 SSL 設定檔可供使用。請參閱[新增 SSL 設定檔](#)。
- 確認伺服器集區可供使用。請參閱[新增伺服器集區](#)。
- 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](#)。
- 確認負載平衡器可供使用。請參閱[新增負載平衡器](#)。

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 > 虛擬伺服器 > 新增虛擬伺服器**。
- 3 選取 **L7 HTTP** 通訊協定，然後輸入通訊協定詳細資料。

第 7 層虛擬伺服器支援 HTTP 和 HTTPS 通訊協定。

選項	說明
名稱與說明	輸入第 7 層虛擬伺服器的名稱和說明。
IP 位址	輸入虛擬伺服器的 IP 位址。
連接埠	輸入虛擬伺服器的連接埠號碼。
負載平衡器	從下拉式功能表中選取要連結至此第 4 層虛擬伺服器的現有負載平衡器。
伺服器集區	<p>從下拉式功能表中選取現有的伺服器集區。</p> <p>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。</p> <p>您可以按一下垂直省略符號來建立伺服器集區。</p>

選項	說明
應用程式設定檔	根據通訊協定類型，現有應用程式設定檔會自動填入。 您可以按一下垂直省略符號來建立應用程式設定檔。
持續性	從下拉式功能表中選取現有的持續性設定檔。 可以在虛擬伺服器上啟用持續性設定檔，讓與來源 IP 和 Cookie 相關的用戶端連線均傳送至同一個伺服器。

4 按一下設定以設定第 7 層虛擬伺服器 SSL。

您可以設定用戶端 SSL 和伺服器 SSL。

5 設定用戶端 SSL。

選項	說明
用戶端 SSL	切換按鈕以啟用設定檔。 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。
預設憑證	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。
用戶端 SSL 設定檔	從下拉式功能表中選取用戶端 SSL 設定檔。
SNI 憑證	從下拉式功能表中選取可用的 SNI 憑證。
受信任的 CA 憑證	選取可用的 CA 憑證。
強制用戶端驗證	切換按鈕以啟用此功能表項目。
憑證鏈結深度	設定憑證鏈結深度，以驗證伺服器憑證鏈結的深度。
憑證撤銷清單	選取可用的 CRL，以便不允許已遭破解的伺服器憑證。

6 設定伺服器 SSL

選項	說明
伺服器 SSL	切換按鈕以啟用設定檔。
用戶端憑證	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，則會使用此憑證。
伺服器 SSL 設定檔	從下拉式功能表中選取伺服器端 SSL 設定檔。
受信任的 CA 憑證	選取可用的 CA 憑證。
強制伺服器驗證	切換按鈕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。
憑證鏈結深度	設定憑證鏈結深度，以驗證伺服器憑證鏈結的深度。
憑證撤銷清單	選取可用的 CRL，以便不允許已遭破解的伺服器憑證。 伺服器端不支援 OCSP 和 OCSP 裝訂。

7 設定其他第 7 層虛擬伺服器內容。

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。
Sorry Server 集區	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。 您可以按一下垂直省略符號來建立伺服器集區。
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。
管理狀態	切換按鈕以停用第 7 層虛擬伺服器的管理狀態。
存取記錄	切換按鈕以啟用第 7 層虛擬伺服器的記錄。
標籤	輸入標籤使搜尋更輕鬆。 您可以指定標籤，以設定標籤範圍。

新增負載平衡器規則

藉由第 7 層 HTTP 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:sensitive)`」，改為使用「`Case ((?i:sensitive))`」。
- 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 HTTP 虛擬伺服器可供使用。請參閱[新增第 7 層 HTTP 虛擬伺服器](#)。

程序

- 1 開啟第 7 層 HTTP 虛擬伺服器。
- 2 在 [負載平衡器規則] 區段中，按一下**設定 > 新增規則**，以針對 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 Cookie	比對任何 HTTP 要求 Cookie。 http_request.cookie_value - 要比對的值
HTTP 要求本文	比對 HTTP 要求的內文內容。 http_request.body_value - 要比對的值
用戶端 SSL	比對用戶端 SSL 設定檔識別碼。 ssl_profile_id - 要比對的值
TCP 標頭連接埠	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 標頭來源	比對 IP 來源或目的地地址。 ip_header.source_address - 要比對的來源地址 ip_header.destination_address - 要比對的目的地址

支援的比對條件	說明
變數	建立一個變數並為該變數指派值。
區分大小寫	設定區分大小寫的旗標以用於 HTTP 標頭值比較。

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
HTTP 要求標頭刪除	刪除 HTTP 標頭。 http_request.header_delete - 標頭名稱 http_request.header_delete - 要寫入的值

- 3 按一下**要求轉送 > 新增規則**，以針對 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 Cookie	比對任何 HTTP 要求 Cookie。 http_request.cookie_value - 要比對的值
HTTP 要求本文	比對 HTTP 要求的內文內容。 http_request.body_value - 要比對的值
用戶端 SSL	比對用戶端 SSL 設定檔識別碼。 ssl_profile_id - 要比對的值
TCP 標頭連接埠	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 標頭來源	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

支援的比對條件	說明
變數	建立一個變數並為該變數指派值。
區分大小寫	設定區分大小寫的旗標以用於 HTTP 標頭值比較。
動作	說明
HTTP 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
HTTP 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
回覆狀態	設定回覆的狀態。
回覆訊息	伺服器以回覆訊息回應，其中含有已確認的位址與組態。

4 按一下回應重寫 > 新增規則，以針對 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
HTTP 回應方法	比對 HTTP 回應方法。 http_response.method - 要比對的值
HTTP 回應 URI	比對 HTTP 回應 URI。 http_response.uri - 要比對的值
HTTP 回應 URI 引數	比對 HTTP 回應 URI 引數。 http_response.uri_args - 要比對的值
HTTP 回應版本	比對 HTTP 回應版本。 http_response.version - 要比對的值
HTTP 回應 Cookie	比對任何 HTTP 回應 Cookie。 http_response.cookie_value - 要比對的值
用戶端 SSL	比對用戶端 SSL 設定檔識別碼。 ssl_profile_id - 要比對的值
TCP 標頭連接埠	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

支援的比對條件	說明
IP 標頭來源	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
變數	建立一個變數並為該變數指派值。
區分大小寫	設定區分大小寫的旗標以用於 HTTP 標頭值比較。
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
HTTP 回應標頭刪除	刪除 HTTP 標頭。 http_request.header_delete - 標頭名稱 http_request.header_delete - 要寫入的值

轉送原則

8

此功能與 NSX Cloud 有關。

轉送原則或以原則為基礎的路由 (PBR) 規則可定義 NSX-T 如何處理 NSX 管理的虛擬機器所傳送的流量。此流量可導向至 NSX-T 覆疊，也可以透過雲端提供者的 (底層) 網路進行路由。

備註 當您在公有雲中為公有雲工作負載虛擬機器加上 `nsx.network=default` 標記，並為其安裝 NSX 代理程式後，這些機器將由 NSX-T 管理。如需詳細資料，請參閱[工作負載虛擬機器上線](#)。

當您在傳送 VPC/VNet 上部署 PCG，或將計算 VPC/VNet 連結至傳送 VPC/VNet 後，系統會自動設定三個預設轉送原則。

- 1 至底層的路由，用於定址在傳送/計算 VPC/VNet 內的所有流量
- 2 至底層的路由，用於以公有雲的中繼資料服務為目標的所有流量。
- 3 至覆疊的路由，用於所有其他流量，例如，傳輸至傳送/計算 VPC/VNet 以外的流量。這些流量會透過 NSX-T 覆疊通道路由至 PCG，繼而路由至目的地。

備註 若是以相同 PCG 所管理的另一個 VPC/VNet 為目標的流量：流量會透過 NSX-T 覆疊通道從來源 NSX 管理的 VPC/VNet 路由至 PCG，然後再路由至目的地 VPC/VNet。

若是以不同 PCG 所管理的另一個 VPC/VNet 為目標的流量：流量會透過 NSX 覆疊通道從一個 NSX 管理的 VPC/VNet 路由至來源 VPC/VNet 的 PCG，然後再轉送至目的地 NSX 管理的 VPC/VNet 的 PCG。

如果流量傳輸至網際網路，則 PCG 會將其路由至網際網路中的目的地。

路由至底層時進行微分割

即使是將流量路由至底層網路的工作負載虛擬機器，也會強制執行微分割。

如果您從 NSX 管理的工作負載虛擬機器直接連線至受管理的 VPC/VNet 外部的目的地，並且想要略過 PCG，請設定轉送原則，以透過底層路由來自此虛擬機器的流量。

透過底層網路來路由流量時，將會略過 PCG，因此流量不會遇到南北向防火牆。不過，您仍需管理東西向或 Distributed Firewall (DFW) 的規則，因為在流量到達 PCG 之前，將會在虛擬機器層級套用這些規則。

目前支援的轉送原則

您可能會在下拉式功能表中看到轉送原則清單，但在此版本中僅支援下列轉送原則：

- **至底層的路由：**從 NSX 管理的虛擬機器存取位於底層的服務。例如，存取 AWS 底層網路上的 AWS S3 服務。
- **來自底層的路由：**從基礎網路存取 NSX 管理的虛擬機器上主控的服務。例如，從 AWS ELB 存取 NSX 管理的虛擬機器。

本章節討論下列主題：

- [新增或編輯轉送原則](#)

新增或編輯轉送原則

您可以編輯自動建立的轉送原則，也可以自行新增。

例如，若要使用公有雲所提供的服務 (例如 AWS 的 S3)，您可以手動建立原則來允許一組 IP 位址透過底層進行路由來存取此服務。

必要條件

您必須具有已部署 PCG 的 VPC 或 VNet。

程序

- 1 按一下**新增區段**。為區段適當命名，例如 **AWS Services**。
- 2 選取區段旁的核取方塊，然後按一下**新增規則**。為規則命名，例如 **S3 Rules**。
- 3 在**來源**索引標籤中，選取您要讓服務存取的工作負載虛擬機器 (例如，AWS VPC) 所在的 VNet 或 VPC。您也可以在此處建立**群組**，以納入符合一或多項準則的多個虛擬機器。
- 4 在**目的地**索引標籤中，選取主控服務的 VPC 或 Vnet，例如含有 AWS S3 服務之 IP 位址的**群組**。
- 5 從**服務**索引標籤的下拉式功能表中選取服務。如果服務不存在，您可以新增服務。您也可以將選取項目保留為**任何**，因為您可以在**目的地**下提供路由詳細資料。
- 6 在**動作**索引標籤中，選取想要的路由方式，例如，如果是針對 AWS S3 服務設定此原則，請選取**至底層的路由**。
- 7 按一下**發佈**完成設定轉送原則。

IP 位址管理 (IPAM)

9

若要管理 IP 位址，您可以設定 DNS (網域名稱系統)、DHCP (動態主機設定通訊協定)、IP 位址集區，以及 IP 位址區塊。

備註 IP 區塊由 NSX Container Plug-in (NCP) 所使用。如需有關 NCP 的詳細資訊，請參閱《適用於 Kubernetes 和 Cloud Foundry 的 NSX Container Plug-in - 安裝和管理指南》。

本章節討論下列主題：

- 新增 DNS 區域
- 新增 DNS 轉寄站服務
- 新增 DHCP 伺服器
- 設定第 0 層或第 1 層閘道的 DHCP 轉送伺服器
- 新增 IP 位址集區
- 新增 IP 位址區塊

新增 DNS 區域

您可以為 DNS 服務設定 DNS 區域。DNS 區域是 DNS 中網域名稱空間的單獨管理單元。

設定 DNS 區域時，您可以指定轉送 DNS 查詢至上游 DNS 伺服器時使用之 DNS 轉寄站的來源 IP。如果未指定來源 IP，DNS 查詢封包的來源 IP 將會是 DNS 轉寄站的接聽程式 IP。如果接聽程式 IP 是從外部上游 DNS 伺服器無法連線到的內部地址，則需要指定來源 IP。若要確保 DNS 回應封包會路由回轉寄站，則需要專用的來源 IP。或者，您也可以設定邏輯路由器上的 SNAT，將接聽程式 IP 轉譯為公用 IP。在此情況下，您不需要指定來源 IP。

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 > IP 位址管理 > DNS**。
- 3 按一下 **DNS 區域**索引標籤。

- 4 若要新增預設區域，請選取**新增 DNS 區域 > 新增預設區域**
 - a 輸入名稱和 (選用) 說明。
 - b 輸入最多三部 DNS 伺服器的 IP 位址。
 - c (選擇性) 在**來源 IP** 欄位中輸入 IP 位址。
- 5 若要新增 FQDN 區域，請選取**新增 DNS 區域 > 新增 FQDN 區域**
 - a 輸入名稱和 (選用) 說明。
 - b 輸入網域的 FQDN。
 - c 輸入最多三部 DNS 伺服器的 IP 位址。
 - d (選擇性) 在**來源 IP** 欄位中輸入 IP 位址。
- 6 按一下**儲存**。

新增 DNS 轉寄站服務

您可以設定 DNS 轉寄站，以將 DNS 查詢轉送至外部 DNS 伺服器。

在設定 DNS 轉寄站之前，您必須先設定預設 DNS 區域。您可以選擇性地設定一或多個 FQDN DNS 區域。每個 DNS 區域最多會與 3 個 DNS 伺服器相關聯。在設定 FQDN DNS 區域時，您可以指定一或多個網域名稱。DNS 轉寄站會與預設 DNS 區域和最多 5 個 FQDN DNS 區域相關聯。收到 DNS 查詢時，DNS 轉寄站會比較查詢中的網域名稱與 FQDN DNS 區域中的網域名稱。如果找到相符的名稱，則會將查詢轉送至 FQDN DNS 區域中指定的 DNS 伺服器。如果找不到相符的名稱，則會將查詢轉送至預設 DNS 區域中指定的 DNS 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**網路 > IP 位址管理 > DNS**。
- 3 按一下**新增 DNS 服務**。
- 4 輸入名稱和 (選用) 說明。
- 5 選取第 0 層或第 1 層閘道。
- 6 輸入 DNS 服務的 IP 位址。
用戶端會將 DNS 查詢傳送至此 IP 位址，這也稱為 DNS 轉寄站的接聽程式 IP。
- 7 選取預設 DNS 區域。
- 8 選取記錄層級。
- 9 選取最多五個 FQDN 區域。
- 10 按一下**管理狀態**切換按鈕，以啟用或停用 DNS 服務。
- 11 按一下**儲存**。

新增 DHCP 伺服器

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。

備註 在 VLAN 支援的區段上，不支援使用此程序建立的 DHCP 伺服器。您必須使用**進階網路與安全性**下的 DHCP 功能，來建立 VLAN 支援的邏輯交換器所支援的 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**網路 > IP 位址管理 > DHCP**。
- 3 按一下**新增伺服器**。
- 4 選取 **DHCP 伺服器**做為伺服器類型。
- 5 輸入伺服器的名稱。
- 6 輸入 CIDR 格式的伺服器 IP 位址。

此步驟會建立兩個邏輯連接埠 (一個用於邏輯介面，另一個用於 DHCP 伺服器本身)，並將 DHCP 伺服器連線至特定的 DHCP 邏輯交換器。此介面會在第 0 層或第 1 層閘道上顯示為已連線的介面，因此請確定您為想要指派 DHCP 伺服器的第 1 層或第 0 層閘道選擇非重疊的子網路。您可以針對此目的指定 `<IP address>/30`。在此處使用的子網路範圍不會向已連線的第 0 層閘道通告，但是會顯示在第 1 層閘道的轉送表中。

- 7 輸入租用時間。
- 8 選取 NSX Edge 叢集。
- 9 按一下**儲存**。
- 10 將 DHCP 伺服器指派給第 0 層或第 1 層閘道：
 - a 導覽至**網路 > 第 0 層閘道**或**網路 > 第 1 層閘道**。
 - b 編輯現有的閘道。
 - c 在 **IP 位址管理**欄位中，按一下**無 IP 配置**。
 - d 從類型下拉式清單選取 **DHCP 本機伺服器**。
 - e 選取 DHCP 伺服器。
 - f 按一下**儲存**。
 - g 按一下**儲存**。
- 11 若要將 DHCP 伺服器指派給一個區段：
 - a 導覽至**網路 > 區段**。
 - b 新增或編輯一個區段。

該區段必須與第 0 層或第 1 層閘道相關聯。

- c 如果您要新增新的區段，請按一下**設定子網路**，或若要新增或修改子網路，請按一下**子網路**下的數字。
- d 輸入適當的 DHCP 範圍。
- e 按一下**套用**。
- f 按一下**儲存**。

設定第 0 層或第 1 層閘道的 DHCP 轉送伺服器

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 轉送伺服器以將 DHCP 流量轉送至外部 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**網路 > IP 位址管理 > DHCP**。
- 3 按一下**新增伺服器**。
- 4 選取 **DHCP 轉送**做為伺服器類型。
- 5 輸入轉送伺服器的名稱。
- 6 輸入伺服器的一或多個 IP 位址。
- 7 按一下**儲存**。
- 8 移至**網路 > 第 0 層閘道**或**網路 > 第 1 層閘道**，以設定閘道的 DHCP 轉送伺服器。
- 9 編輯適當的閘道。
- 10 在 **IP 位址管理**欄位中，針對第 0 層閘道按一下**無 IP 配置**，或針對第 1 層閘道按一下**無 IP 配置集合**。
- 11 在**類型**欄位中，選取 **DHCP 轉送**。
- 12 在 **DHCP 轉送** 欄位中，選取您先前建立的 DHCP 轉送伺服器。
- 13 按一下**儲存**。
- 14 對於連線至將使用此 DHCP 轉送服務之閘道的每個區段，您必須指定 DHCP 範圍才能讓轉送正常運作。
 - a 移至**網路 > 區段**。
 - b 新增或編輯一個區段。
 - c 如果您要新增新的區段，請按一下**設定子網路**，或按一下**子網路**下的數字以修改子網路。
 - d 指定一或多個 DHCP 範圍。
這是必要的，才能讓轉送正常運作。
 - e 按一下**套用**。
 - f 按一下**儲存**。

新增 IP 位址集區

您可以設定元件 (例如 DHCP) 所使用的 IP 位址集區。

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 > IP 位址管理 > IP 位址集區**。
- 3 按一下**新增 IP 位址集區**。
- 4 輸入名稱和 (選用) 說明。
- 5 若要指定位址區塊，請選取**新增子網路 > IP 區塊**。
 - a 選取 IP 區塊。
 - b 指定大小。
 - c 按一下**新增**。
- 6 若要指定 IP 範圍，請選取**新增 Sunet > IP 範圍**。
 - a 輸入 IPv4 或 IPv6 IP 範圍。
 - b 以 CIDR 格式輸入 IP 範圍。
 - c 輸入**閘道 IP** 的位址。
 - d 按一下**新增**。
- 7 按一下**儲存**。

新增 IP 位址區塊

您可以設定 IP 位址區塊供其他元件使用。

備註 您也可以導覽至**進階網路與安全性 > 網路 > IPAM** 來新增 IP 位址區塊。

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**網路 > IP 位址管理 > IP 位址集區**。
- 3 按一下**IP 位址區塊**索引標籤。
- 4 按一下**新增 IP 位址區塊**。
- 5 輸入名稱和 (選用) 說明。
- 6 以 CIDR 格式輸入 IP 區塊。
- 7 按一下**儲存**。

本小節中的主題涵蓋分散式防火牆規則的南北向和東西向安全性、身分識別防火牆、網路自我檢查、閘道防火牆和端點保護原則。

本章節討論下列主題：

- [安全性組態概觀](#)
- [安全性術語](#)
- [身分識別防火牆](#)
- [第 7 層內容設定檔](#)
- [Distributed Firewall](#)
- [設定閘道防火牆](#)
- [設定東西向網路自我檢查](#)
- [設定南北向網路自我檢查](#)
- [設定 Endpoint Protection](#)

安全性組態概觀

為您的環境設定東西向和南北向防火牆原則 (這些原則歸屬於預先定義的類別)。

分散式防火牆 (東西向) 和閘道防火牆 (南北向) 提供按類別區分的多個可設定規則集。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。

安全性原則根據下列方式強制執行：

- 規則會按類別從左到右處理。
- 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。

安全性術語

以下詞彙將在整個分散式防火牆中使用。

表 10-1. 安全性相關的術語

建構	定義
網域	網域表示包含防火牆規則與群組的環境或安全性區域。建立網域是選擇性的。預設網域代表整個 NSX 環境。網域中的規則必須在來源或目的地中至少有一個群組是同一個網域的成員。請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。
原則	安全性原則包含各種安全性元素，包括防火牆規則和服務組態。原則先前稱為防火牆區段。
規則	用於評估流量的一組參數，可定義相符時將採取的動作。規則中包含來源和目的地、服務、內容設定檔、記錄和標籤等參數。
群組	群組中包含靜態和動態新增的不同物件，並且可用作防火牆規則的來源和目的地欄位。群組可設定為包含虛擬機器、IP 集合、MAC 集合、邏輯連接埠、邏輯交換器、AD 使用者群組以及其他巢狀群組的組合。群組的動態納入方式可以根據標籤、機器名稱、作業系統名稱或電腦名稱來進行。 當您建立群組時，您必須包含其所屬的網域，依預設，此網域為預設網域。 群組先前稱為 NSGroup 或安全群組。
服務	定義連接埠和通訊協定的組合。用於根據連接埠和通訊協定將流量分類。預先定義的服務和使用者的服務可在防火牆規則中使用。
內容設定檔	定義內容感知的屬性，包括應用程式識別碼和網域名稱。還包括子屬性，例如應用程式版本或加密集。防火牆規則可以包含內容設定檔，以啟用第 7 層防火牆規則。

身分識別防火牆

身分識別防火牆 (IDFW) 功能可讓 NSX 管理員建立以 Active Directory 使用者為基礎的分散式防火牆 (DFW) 規則。

IDFW 可用於虛擬桌面平台 (VDI) 或遠端桌面平台工作階段 (RDSH 支援)，實現讓多個使用者同時登入、根據需求進行使用者應用程式存取，以及維護獨立使用者環境的能力。VDI 管理系統控制哪些使用者有權存取 VDI 虛擬機器。NSX-T 控制從來源虛擬機器對目的地伺服器的存取。在來源虛擬機器處理 IDFW。使用 RDSH 時，管理員會將 Active Directory (AD) 中的不同使用者建立成安全群組，然後根據這些使用者的角色，允許或拒絕其對應用程式伺服器的存取。例如，人力資源部和工程部可以連線至同一個 RDSH 伺服器，但對該伺服器上的不同應用程式具有存取權。

備註 IDFW 需依賴客體作業系統的安全性和完整性。惡意本機管理員有多種方法可偽造其身分識別以略過防火牆規則。使用者身分識別資訊由客體虛擬機器中的 Guest Introspection Agent 所提供。安全性管理員必須確定已在每個客體虛擬機器中安裝並執行 NSX Guest Introspection Agent。已登入的使用者不應擁有移除或停止代理程式的權限。

不支援 Linux 作業系統。

下列系統可支援 IDFW：

Microsoft Active Directory Windows Server：

- 2008

- 2012
- 2012R2
- 2016
- 2019

VMware Tools 10.3 版或更新版本：NSX File Introspection 驅動程式、NSX Network Introspection 驅動程式、VMCI 驅動程式。

主機作業系統：僅限 ESXi

客體作業系統：

- 桌面平台強制執行：Windows 8、Windows 10
- RDSH 強制執行：Windows 2012R2、Windows 2016

IDFW 組態工作流程的高階概觀是從準備基礎結構開始。這包括管理員在每個受保護的叢集上安裝主機準備元件，然後設定 Active Directory 同步化，讓 NSX 能夠取用 AD 使用者與群組。接著，IDFW 必須知道 Active Directory 使用者是登入哪個桌面平台，以便套用 IDFW 規則。當使用者產生網路事件時，隨 VMware Tools 安裝在虛擬機器上的精簡型代理程式會收集資訊，然後將收集到的資訊轉送給內容引擎。此資訊用於提供對分散式防火牆的強制執行。

IDFW 工作流程：

- 1 使用者登入虛擬機器，然後開啟 Skype 或 Outlook 來啟動網路連線。
- 2 精簡型代理程式會偵測到使用者登入事件，它會收集連線資訊和身分識別資訊，然後將收集到的資訊傳送給內容引擎。
- 3 內容引擎將這些連線資訊和身分識別資訊轉送給分散式防火牆來強制執行任何適用的規則。

身分識別防火牆工作流程

IDFW 可藉由允許基於使用者身分識別的防火牆規則，來增強傳統防火牆的效用。例如，管理員可以使用單一防火牆原則來允許或禁止客戶支援人員存取 HR 資料庫。

以使用者基礎的分散式防火牆規則是由 Active Directory (AD) 群組成員資格中的成員資格決定。身分識別防火牆需要 Thin Agent。

備註 IDFW 需依賴客體作業系統的安全性和完整性。惡意本機管理員有多種方法可偽造其身分識別以略過防火牆規則。使用者身分識別資訊由客體虛擬機器中的 Guest Introspection Agent 所提供。安全管理員必須確定已在每個客體虛擬機器中安裝並執行 NSX Guest Introspection Agent。已登入的使用者不應擁有移除或停止代理程式的權限。

備註 在強制執行 Identity Firewall 規則時，所有使用 Active Directory 的虛擬機器均應**開啟** Windows 時間服務。這可確保 Active Directory 與虛擬機器之間的日期和時間能夠保持同步。此外，AD 群組成員資格變更 (包括啟用和刪除使用者) 並不會對登入的使用者立即生效。若要使變更生效，使用者必須登出後再重新登入。修改群組成員資格後，AD 管理員應強制登出。此行為是一個 Active Directory 限制。

必要條件

Microsoft Active Directory Windows Server:

- 2008
- 2012
- 2012R2
- 2016
- 2019

VMware Tools 10.3 版或更新版本：NSX File Introspection 驅動程式、NSX Network Introspection 驅動程式、VMCI 驅動程式。

主機作業系統：僅限 ESXi

客體作業系統：

- 桌面平台強制執行：Windows 8、Windows 10
- RDSH 強制執行：Windows 2012R2、Windows 2016

程序

- 1 啟用 NSX File Introspection 驅動程式和 NSX Network Introspection 驅動程式。依預設，VMware Tools 完整安裝會新增這些項目。
- 2 在叢集或獨立主機上啟用 IDFW：啟用 [Identity Firewall](#)。
- 3 設定 Active Directory 網域：新增 [Active Directory](#)。
- 4 設定 Active Directory 同步作業：同步 [Active Directory](#)。
- 5 使用 Active Directory 群組成員建立安全群組 (SG)：新增群組。
- 6 將具有 AD 群組成員的 SG 指派給分散式防火牆規則：新增分散式防火牆。

啟用 Identity Firewall

必須啟用 Identity Firewall，IDFW 防火牆規則才會生效。

程序

- 1 選取導覽面板中的**安全性 > Distributed Firewall**。
- 2 按一下橫幅上的**啟用 IDFW**。
- 3 再次按一下橫幅上的**啟用 IDFW**。按一下狀態按鈕以啟用 IDFW。
編輯 Identity Firewall 畫面隨即顯示。
- 4 切換狀態按鈕以啟用 IDFW。
- 5 (選擇性) 切換狀態按鈕以啟用獨立主機上的 IDFW。
- 6 (選擇性) 變更每個可用叢集的狀態，以便在每個叢集上啟用 IDFW。

7 按一下儲存。

Identity Firewall 最佳做法

下列最佳做法有助於讓 Identity Firewall 規則發揮最大效益。

- IDFW 僅支援以 TCP 型的防火牆規則。
- 以單一識別碼為基礎的群組可用於一個防火牆規則中。如果需要在來源使用以 IP 和識別碼為基礎的群組，請建立分別兩個防火牆規則。
- 不支援以 Windows 2008 作為 Active Directory 伺服器或 RDSH 伺服器作業系統。
- 對網域的任何變更 (包含網域名稱變更) 都將觸發與 Active Directory 之間的完整同步。由於完整同步可能需要很長的時間，建議您在離峰時間或非營業時間進行同步。
- 預設 LDAP 連接埠 389 和 LDAPS 連接埠 636 會用於 Active Directory 同步，不應編輯為非預設值。不支援自訂連接埠。

第 7 層內容設定檔

第 7 層應用程式身分識別是在內容設定檔中設定。

內容設定檔可以指定一或多個**應用程式識別 GUID**，同時還可包含子屬性。當定義了諸如 TLS 1.2 版之類的子屬性時，不支援多個應用程式身分識別屬性。內容設定檔中除了能設定 APP-ID，還能設定完整網域名稱 (FQDN) 或 URL 來將 FQDN 加入白名單。可以在一個內容設定檔中同時設定 FQDN 和 APP-ID，也可以在不同的內容設定檔中分別設定這兩項。內容設定檔一經定義，即可套用至一或多個 Distributed Firewall 規則。

當規則中使用了內容設定檔時，凡是從虛擬機器傳入的流量，均會與規則資料表進行 5 元組比對。如果比對流量的規則還包含第 7 層內容設定檔，該封包便會被重新導向至一個稱為深度封包檢查 (DPI) 引擎的使用者空間元件。每次流量都會有少數後續封包被踢給該 DPI 引擎，待其判斷出 APP_ID 後，此資訊就會儲存在核心內的內容資料表中。當流量的下個封包傳入時，內容資料表中的資訊即會與規則資料表進行比較，並與 5 元組和第 7 層 APP-ID 進行比對。系統會採取規則中所定義的適當動作，而如果是 [允許] 規則，則流量的所有後續封包均會在核心內進行處理，並與連線資料表進行比對。如果該流量被踢給 DPI，Distributed Firewall 所產生的記錄就會包含第 7 層 APP_ID。

傳入封包的規則處理：

- 1 進入 DFW 篩選器後，會在流程資料表中根據 5 元組查詢封包。
- 2 如果找不到流量/狀態，就會根據規則資料表對流量進行 5 元組比對，然後在流量資料表中建立一個項目。
- 3 如果流量符合含有第 7 層服務物件的規則，流量資料表狀態會標記為「DPI 進行中」。
- 4 然後，流量便會被踢給 DPI 引擎。DPI 引擎會判斷 APP_ID。
- 5 判斷出 APP_ID 後，DPI 引擎便會將插入此流量之內容資料表的屬性向下傳送。「DPI 中進行」旗標將會移除，且流量不再被踢給 DPI 引擎。

- 6 流量 (現在含 APP-ID) 會根據符合 APP_ID 的所有規則進行重新評估，從進行 5 元組比對的原始規則開始，並確保不以相符的 L4 規則優先。系統會採取適當的動作 (允許/拒絕)，然後據以更新流量資料表項目。

第 7 層 Distributed Firewall 規則工作流程

第 7 層應用程式識別碼用於建立內容設定檔，以及建立 Distributed Firewall 規則。基於應用程式身分識別的規則強制執行可讓使用者允許或拒絕在任何連接埠上執行應用程式。

NSX-T 提供一般基礎結構和企業應用程式的內建 [應用程式識別 GUID](#)。應用程式識別碼包括版本 (SSL/TLS 及 CIFS/SMB) 和加密套件 (SSL/TLS)。應用程式識別碼會透過內容設定檔用於規則中，並且可與 FQDN 白名單和黑名單結合使用。僅在 ESXi 主機上受支援。

支援的應用程式識別碼和 FQDN：

- 對於 FQDN，使用者必須為連接埠 53 上所指定 DNS 伺服器設定 DNS 應用程式識別碼的高優先順序規則。
- ALG 應用程式識別碼 (FTP、ORACLE、DCERPC、TFTP) 需要防火牆規則的對應 ALG 服務。
- 僅在標準連接埠上才會偵測到 SYSLOG 應用程式識別碼。

程序

- 1 建立自訂內容設定檔：[新增內容設定檔](#)。
- 2 在 Distributed Firewall 規則中使用內容設定檔：[新增分散式防火牆](#)。

應用程式識別 GUID

第 7 層應用程式識別會識別特定封包或流量由哪個應用程式產生，與正在使用的連接埠無關。

基於應用程式身分識別的強制執行可讓使用者允許或拒絕要在任何連接埠上執行的應用程式，或強制應用程式在其標準連接埠上執行。深度封包檢查 (DPI) 允許對照定義的模式 (通常稱為簽章) 比對封包裝載。簽章型識別與強制執行讓客戶不僅能比對流量所屬的特定應用程式/通訊協定，還能比對該通訊協定的版本，例如 TLS 1.0 版、TLS 1.2 版或是其他版本的 CIFS 流量。這可讓客戶一窺甚至禁止使用在所有已部署的應用程式中已知具有安全性弱點的通訊協定，以及其在資料中心內的東西向流量。

支援的應用程式識別碼和 FQDN：

- 對於 FQDN，使用者必須為連接埠 53 上所指定 DNS 伺服器設定 DNS 應用程式識別碼的高優先順序規則。
- ALG 應用程式識別碼 (FTP、ORACLE、DCERPC、TFTP) 需要防火牆規則的對應 ALG 服務。
- 僅在標準連接埠上才會偵測到 SYSLOG 應用程式識別碼。

KVM 支援的應用程式識別碼和 FQDN：

- 在 KVM 上不支援子屬性。
- 在 KVM 上支援 FTP 和 TFTP ALG 應用程式識別碼。

第 7 層 APP-ID 會用在分散式防火牆的內容設定檔中使用，且僅在 ESXi 主機上受支援。

GUID	說明	類型
360ANTIV	360 Safeguard 是由位於中國的 IT 公司 Qihoo 360 開發的一個程式	Web 服務
ACTIVDIR	Microsoft Active Directory	網路
AD_BKUP	Microsoft Active Directory 備份服務	網路
AD_NSP	Microsoft Active Directory 服務提供者	網路
AMQP	進階訊息佇列通訊協定是支援應用程式或組織之間的業務訊息通訊的應用程式層通訊協定	網路
AVAST	透過瀏覽 Avast! Antivirus 下載的 Avast.com 官方網站所產生的流量	Web 服務
AVG	AVG 防毒/安全性軟體下載和更新	檔案傳輸
AVIRA	Avira 防毒/安全性軟體下載和更新	檔案傳輸
BLAST	一種遠端存取通訊協定，將在資料中心壓縮、加密和編碼運算體驗並在 VMware Horizon 桌面平台的任何標準 IP 網路之間進行傳輸。	遠端存取
BDEFENDER	BitDefender 防毒/安全性軟體下載和更新	檔案傳輸
CA_CERT	憑證授權單位 (CA) 核發數位憑證，這些憑證可認證用於訊息加密的公開金鑰的擁有權	網路
CIFS	CIFS (Common Internet File System) 可用來提供對網路上的目錄、檔案、印表機、序列埠和節點之間的其他通訊的共用存取	檔案傳輸
CLDAP	不需連線的輕量型目錄存取通訊協定是一種應用程式通訊協定，用於使用 UDP 透過網際網路通訊協定 (IP) 網路存取和維護分散式目錄資訊服務。	
CLRCASE	用於對原始程式碼和其他軟體開發資產進行修訂控制的軟體工具。它是由 IBM 的 Rational Software 部門開發的。ClearCase 構成了許多大中型企業的修訂控制基礎，可以處理涉及數百或數千個開發人員的專案	網路
CTRXCGP	Citrix 通用閘道通訊協定是一種應用程式通訊協定，用於使用 UDP 透過網際網路通訊協定 (IP) 網路存取和維護分散式目錄資訊服務。	資料庫
CTRXGOTO	主控 Citrix GoToMeeting 或以 GoToMeeting 平台為基礎的類似工作階段。包含語音、視訊和有限的群眾管理功能	協作
CTRIXICA	ICA (Independent Computing Architecture) 是由 Citrix 系統設計用於應用程式伺服器系統的專屬通訊協定	遠端存取
DCERPC	分散式運算環境/遠端程序呼叫是針對分散式運算環境 (DCE) 開發的遠端程序呼叫系統	網路
DIAMETER	用於電腦網路的驗證、授權和會計通訊協定	網路
DNS	透過 TCP 或 UDP 查詢 DNS 伺服器	網路
EPIC	Epic EMR 是電子醫療記錄應用程式，可提供病患護理和醫療保健資訊。	用戶端伺服器
ESET	Eset 防毒/安全性軟體下載和更新	檔案傳輸
FPROT	F-Prot 防毒/安全性軟體下載和更新	檔案傳輸

GUID	說明	類型
FTP	FTP (檔案傳輸通訊協定) 可用於將檔案從檔案伺服器傳送到本機機器	檔案傳輸
GITHUB	以 Web 為基礎的 Git 或版本控制存放庫和網際網路主控服務	協作
HTTP	(超文字傳輸通訊協定) World Wide Web 的主體傳輸通訊協定	Web 服務
HTTP2	透過瀏覽支援 HTTP 2.0 通訊協定的網站所產生的流量	Web 服務
IMAP	IMAP (網際網路訊息存取通訊協定) 是一種網際網路標準通訊協定，用於存取遠端伺服器上的電子郵件	郵件
KASPRSKY	Kaspersky 防毒/安全性軟體下載和更新	檔案傳輸
KERBEROS	Kerberos 是一種網路驗證通訊協定，旨在透過使用秘密金鑰密碼編譯為用戶端/伺服器應用程式提供強式驗證	網路
LDAP	LDAP (輕量型目錄存取通訊協定) 是用於讀取和編輯 IP 網路上的目錄的通訊協定	資料庫
MAXDB	對 MaxDB SQL Server 進行的 SQL 連線和查詢	資料庫
MCAFEE	McAfee 防毒/安全性軟體下載和更新	檔案傳輸
MSSQL	Microsoft SQL Server 是一個關聯式資料庫。	資料庫
NFS	允許用戶端電腦上的使用者以類似於存取本機儲存區的方式存取網路上的檔案	檔案傳輸
NNTP	網際網路應用程式通訊協定，用於在新聞伺服器之間傳輸 Usenet 新聞文章 (netnews) 以及透過終端使用者用戶端應用程式讀取並發佈文章。	檔案傳輸
NTBIOSNS	NetBIOS 名稱服務。若要啟動工作階段或散佈資料包，應用程式必須使用名稱服務登錄其 NetBIOS 名稱	網路
NTP	NTP (網路時間通訊協定) 可用於透過網路同步電腦系統的時鐘	網路
OCSP	OCSP 回應程式，用於確認使用者的私密金鑰尚未破解或撤銷	網路
ORACLE	由 Oracle 公司產生並行銷的物件關聯式資料庫管理系統 (ORDBMS)。	資料庫
PANDA	Panda 安全性防毒/安全性軟體下載和更新。	檔案傳輸
PCOIP	遠端存取通訊協定，將在資料中心壓縮、加密和編碼運算體驗並在任何標準 IP 網路之間進行傳輸。	遠端存取
POP2	POP (郵局通訊協定) 是本機電子郵件用戶端用來從遠端伺服器擷取電子郵件的通訊協定。	郵件
POP3	Microsoft 的 NetBIOS 名稱服務 (NBNS) 實作，是 NetBIOS 電腦名稱的名稱伺服器和服務。	郵件
RADIUS	為電腦提供集中式驗證、授權和會計 (AAA) 管理，以連線並使用網路服務	網路
POSTGRES		
RDP	RDP (遠端桌面通訊協定) 為使用者提供另一台電腦的圖形化介面	遠端存取

GUID	說明	類型
RTCP	RTCP (即時傳輸控制通訊協定) 是即時傳輸通訊協定 (RTP) 的姊妹通訊協定。RTCP 為 RTP 流程提供額外控制資訊。	串流媒體
RTP	RTP (即時傳輸通訊協定) 主要用來提供即時音訊和視訊	串流媒體
RTSP	RTSP (即時資料流通訊協定) 可用於在端點之間建立和控制媒體工作階段	串流媒體
RTSPS	一種安全的網路控制通訊協定，專門用於娛樂和通訊系統，以控制串流媒體伺服器。此通訊協定可用於在端點之間建立和控制媒體工作階段。	串流媒體
SAP	與多個 SAP 產品的一般元件的連線，例如 Netweaver、BusinessObjects XI 和 Crystal Enterprise Server。	協作
SIP	SIP (工作階段初始化通訊協定) 是一種通用控制通訊協定，用於設定和控制語音與視訊通話	串流媒體
SKIP	簡單金鑰管理網際網路通訊協定 (SKIP) 是混合的金鑰發佈通訊協定。簡單金鑰管理網際網路通訊協定 (SKIP) 類似於 SSL，不同之處在於其一次建立長期金鑰，然後無需事先通訊即可按照逐個工作階段建立或交換金鑰。	網路
SMTP	SMTP (簡易郵件傳輸通訊協定) 是一個用於跨網際網路通訊協定 (IP) 網路傳輸電子郵件的網際網路標準。	郵件
SNMP	SNMP (簡易網路管理通訊協定) 是一種網際網路標準通訊協定，用於管理 IP 網路上的裝置。	網路監控
SQLNET	允許在程式與 Oracle 資料庫之間或多個 Oracle 資料庫之間進行遠端資料存取的網路軟體。	資料庫
SQLSERV	SQL 服務	資料庫
SSH	SSH (Secure Shell) 是一種網路通訊協定，允許使用兩個網路裝置之間的安全通道交換資料。	遠端存取
SSL	SSL (安全通訊端層) 是一種密碼編譯通訊協定，可透過網際網路提供安全性。	Web 服務
SVN	管理 Subversion 伺服器上的內容。	資料庫
SYMUPDAT	Symantec LiveUpdate 流量，這包括間諜軟體定義、防火牆規則、防毒簽章檔案以及軟體更新。	檔案傳輸
SYSLOG	Symantec LiveUpdate 流量，這包括間諜軟體定義、防火牆規則、防毒簽章檔案以及軟體更新。	網路監控
TELNET	一種用於網際網路或區域網路的網路通訊協定，可使用虛擬終端連線提供雙向互動式文字導向通訊設施。	遠端存取
TFTP	TFTP (簡單式檔案傳輸通訊協定) 可用來使用用戶端 (例如 WinAgents TFTP 用戶端) 列出、下載及上傳檔案到 TFTP 伺服器 (例如 SolarWinds TFTP 伺服器)。	檔案傳輸
VNC	用於虛擬網路運算的流量。	遠端存取
WINS	Microsoft 的 NetBIOS 名稱服務 (NBNS) 實作，是 NetBIOS 電腦名稱的名稱伺服器和服務。	網路

Distributed Firewall

Distributed Firewall 隨附了多種類別的預先定義防火牆規則。規則的評估順序是由上至下、由左至右。可以使用 API 來變更類別名稱。

表 10-2. 類別

乙太網路	用於基於第 2 層的規則
緊急	用於隔離及允許規則
基礎結構	定義對共用服務的存取權。全域規則 - AD、DNS、NTP、DHCP、備份、管理伺服器
環境	生產區域與開發區域間的規則、業務單位間的規則
應用程式	應用程式間的規則、應用程式層間的規則，或微服務間的規則

新增分散式防火牆

分散式防火牆會監控虛擬機器上的所有東西向流量。

必要條件

為了受到 DFW 保護，客體虛擬機器必須將其 vNIC 連線至與傳輸區域相關聯的 N-VDS 邏輯交換器。

若要為身分識別防火牆建立規則，請先建立含有 Active Directory 成員的群組。IDFW 僅支援以 TCP 為基礎的防火牆規則。

備註 在強制執行 Identity Firewall 規則時，所有使用 Active Directory 的虛擬機器均應**開啟** Windows 時間服務。這可確保 Active Directory 與虛擬機器之間的日期和時間能夠保持同步。此外，AD 群組成員資格變更 (包括啟用和刪除使用者) 並不會對登入的使用者立即生效。若要使變更生效，使用者必須登出後再重新登入。修改群組成員資格後，AD 管理員應強制登出。此行為是一個 Active Directory 限制。

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 > Distributed Firewall**。
- 3 確定您是位於正確的預先定義類別，然後按一下**新增原則**。如需類別的詳細資訊，請參閱 [Distributed Firewall](#)。
- 4 為新的原則區段輸入**名稱**。
- 5 選取原則**目的地**網域。保留預設的原則網域，或者新增或建立其他網域。網域是一個邏輯建構，代表一個安全性區域和所有的安全群組與規則。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

6 (選擇性) 按一下齒輪圖示以進行下列原則設定：

功能表選項	說明
TCP 嚴格	<p>TCP 連線會以三向信號交換 (SYN、SYN-ACK、ACK) 開始，並通常以雙向交換 (FIN、ACK) 結束。在某些情況下，分散式防火牆可能看不到特定流量的三向信號交換 (即由於非對稱流量，或流量存在時所啟用的分散式防火牆)。依預設，分散式防火牆不會強制必須看到三向信號交換，且將會提取已建立的工作階段。TCP 嚴格可以每個區段為基礎啟用，以關閉中間工作階段接聽並強制執行三向信號交換的要求。</p> <p>當針對特定分散式防火牆區段啟用 TCP 嚴格模式，且使用預設「任何-任何」封鎖規則時，系統將捨棄並未完成三向信號交換連線要求，且符合中此區段中以 TCP 為基礎之規則的封包。嚴格僅適用於可設定狀態的 TCP 規則，且會在分散式防火牆區段層級上啟用。TCP 嚴格不會針對符合未指定任何 TCP 服務之預設「任何-任何」允許的封包強制執行。</p>
可設定狀態	可設定狀態的防火牆會監控作用中連線的狀態，並使用此資訊決定可通過防火牆的封包。
已鎖定	<p>您可以鎖定原則，以防多位使用者對相同的區段進行變更。鎖定區段時，必須加上註解。</p> <p>某些角色 (如企業管理員) 具有完整存取認證，且無法鎖定。請參閱角色型存取控制。</p>

7 按一下**發佈**。您可以新增多個原則，然後一同發佈。

新的原則即會顯示在畫面上。

8 選取原則區段，然後按一下**新增規則**。

9 輸入規則的名稱。

10 在**來源**資料行中按一下編輯圖示，然後選取規則來源。含有 Active Directory 成員的群組可在 IDFW 規則的來源文字方塊中使用。如需詳細資訊，請參閱[新增群組](#)。

11 在**目的地**資料行中按一下編輯圖示，然後選取規則的目的地。若未定義，則代表不分目的地。如需詳細資訊，請參閱[新增群組](#)。

12 在**服務**資料行中按一下編輯圖示，然後選取服務。若未定義，則服務會比對**任何**項目。

13 向「乙太網路」類別新增規則時，**設定檔**資料行會無法使用。針對所有其他規則類別，在**設定檔**資料行中按一下編輯圖示，然後選取內容設定檔。請參閱[新增內容設定檔](#)。

內容設定檔會使用第 7 層應用程式識別碼屬性，以供在分散式防火牆規則中使用。

14 依預設，**套用至**資料行設定為 [DFW]，而規則會套用至所有工作負載。您也可以將規則或原則套用至選取的群組。**套用至**定義了每個規則的強制執行範圍，主要用於 ESXi 與 KVM 主機上的最佳化或資源。這有助於為特定的區域與承租人定義針對性的原則，卻不干擾為其他承租人與區域所定義的其他原則。

僅由 IP 位址、MAC 位址或 Active Directory 群組組成的群組，無法在**套用至**文字方塊中使用。

15 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。

16 按一下狀態切換按鈕以啟用或停用規則。**17** (選擇性) 按一下齒輪圖示以設定下列規則選項：

選項	說明
記錄	依預設會關閉記錄。記錄會儲存在 ESXi 與 KVM 主機上的 /var/log/dfwptlogs.log 檔案。
方向	此文字方塊會參照就目的地物件的觀點而言的流量方向。「傳入」表示僅檢查傳給物件的流量，「傳出」表示僅檢查物件發出的流量，而「傳入/傳出」則表示檢查這兩個方向的流量。
IP 通訊協定	依 IPv4、IPv6 或 IPv4-IPv6 這兩者強制執行規則。
標籤	標籤可讓搜尋更輕鬆。

18 按一下**發佈**。可以新增多個規則，然後一同發佈。**新增防火牆規則以將 FQDN/URL 加入白名單**

設定 Distributed Firewall 規則，以將前往特定網域 (以 FQDN/URL 識別，例如 *.office365.com) 的特定東西向流量加入白名單。

目前，支援預先定義的網域清單。您在新增屬性類型為 [網域 (FQDN) 名稱] 的內容設定檔時，即可看到 FQDN 清單。

您必須先設定 DNS 規則，然後在其下設定 FQDN 白名單規則。這是因為 NSX-T Data Center 使用 DNS 窺探取得 IP 位址與 FQDN 之間的對應。若要防止發生 DNS 詐騙攻擊的風險 (惡意虛擬機器可能會插入詐騙的 DNS 回應，將流量重新導向至惡意端點或略過 DFW)，則應在所有邏輯連接埠上的交換器啟用 Spoofguard。如需關於 Spoofguard 的詳細資訊，請參閱[瞭解 SpoofGuard 區段設定檔](#)。

執行 vMotion 期間會保留基於 FQDN 的規則。

備註 在目前的版本中，僅支援 ESXi。

必要條件

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**安全性 > Distributed Firewall**。
- 3 依照**新增分散式防火牆**中的步驟，新增防火牆原則區段。或者，您也可以使用現有的防火牆原則區段。
- 4 選取新的或現有的防火牆原則區段，然後按一下**新增規則**，以先建立 DNS 防火牆規則。
- 5 提供防火牆規則的名稱 (例如 **DNS rule**)，然後提供下列詳細資料：

選項	說明
服務	按一下編輯圖示，然後視您環境的需要選取 DNS 或 DNS-UDP 服務。
設定檔	按一下編輯圖示，然後選取 DNS 內容設定檔。這是預先建立的項目，依預設，可在您的部署中使用。
套用至	視需要選取 DFW 或群組。
動作	選取允許。

- 6 再次按一下**新增規則**，以設定 FQDN 白名單規則。
- 7 為規則適當命名，例如 **FQDN/URL Whitelist**。將規則拖曳至此原則區段下的 DNS 規則下。
- 8 提供下列詳細資料：

選項	說明
服務	按一下編輯圖示，然後選取要與此規則建立關聯的服務，例如 HTTP。
設定檔	按一下編輯圖示，然後按一下 新增內容設定檔 。按一下名為 屬性 的資料行，然後選取 網域 (FQDN) 名稱 。從預先定義的清單中選取屬性名稱/值的清單。按一下 新增 。如需詳細資料，請參閱 新增內容設定檔 。
套用至	視需要選取 DFW 或群組。
動作	選取允許。

- 9 按一下**發佈**。

分散式防火牆封包記錄

如果已為防火牆規則啟用記錄，則可以查看防火牆封包記錄來對問題進行疑難排解。

ESXi 和 KVM 主機的記錄檔為 `/var/log/dfwpktlogs.log`。

以下是分散式防火牆規則的一般記錄範例：

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainsrs/1024 IN 52 TCP 192.168.4.3/49627->192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainsrs/1024 OUT 52 TCP 192.168.4.3/49676->192.168.4.4/135 SEW
```

```
2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1
```

```
2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

DFW 記錄檔格式的元素包含下列項目，並以空格分隔：

- 時間戳記：
- 介面 VIF 識別碼的最後 8 位數
- INET 類型 (v4 或 v6)
- 原因 (match)
- 動作 (PASS、DROP、REJECT)
- 規則集名稱/規則識別碼
- 封包方向 (IN/OUT)
- 封包大小
- 通訊協定 (TCP、UDP 或 PROTO #)
- netx 規則叫用的 SVM 方向
- 來源 IP 位址/來源連接埠 > 目的地 IP 位址/目的地連接埠
- TCP 旗標 (SEW)

針對通過的 TCP 封包，系統會在工作階段結束時產生終止記錄：

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

TCP 終止記錄的元素包含下列項目，並以空格分隔：

- 時間戳記：
- 介面 VIF 識別碼的最後 8 位數
- INET 類型 (v4 或 v6)
- 動作 (TERM)
- 規則集名稱/規則識別碼
- 封包方向 (IN/OUT)
- 通訊協定 (TCP、UDP 或 PROTO #)
- TCP RST 旗標
- netx 規則叫用的 SVM 方向
- 來源 IP 位址/來源連接埠 > 目的地 IP 位址/目的地連接埠
- IN 封包計數/OUT 封包計數 (全部累積)

■ IN 封包大小/OUT 封包大小

以下是分散式防火牆規則的 FQDN 記錄檔範例：

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

FQDN 記錄的元素包含下列項目，並以空格分隔：

- 時間戳記：
- 介面 VIF 識別碼的最後 8 位數
- INET 類型 (v4 或 v6)
- 原因 (match)
- 動作 (PASS、DROP、REJECT)
- 規則集名稱/規則識別碼
- 封包方向 (IN/OUT)
- 封包大小
- 通訊協定 (TCP、UDP 或 PROTO #)
- 來源 IP 位址/來源連接埠 > 目的地 IP 位址/目的地連接埠
- 網域名稱/UUID，其中 UUID 是網域名稱的二進位內部表示

以下是分散式防火牆規則的第 7 層記錄檔範例：

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

第 7 層記錄的元素包含下列項目，並以空格分隔：

- 時間戳記：
- 介面 VIF 識別碼的最後 8 位數
- INET 類型 (v4 或 v6)
- 原因 (match)
- 動作 (PASS、DROP、REJECT)
- 規則集名稱/規則識別碼
- 封包方向 (IN/OUT)
- 封包大小
- 通訊協定 (TCP、UDP 或 PROTO #)
- 來源 IP 位址/來源連接埠 > 目的地 IP 位址/目的地連接埠

- APP_XXX 是探索到的應用程式

選取預設的連線策略

您可以選取預設的連線策略來強制執行想要的安全性模型。

預設的連線策略會在您建立的其他防火牆規則之外，再建立全部允許 (黑名單) 或全部拒絕 (白名單) 防火牆原則，讓您無需修改個別規則。

可用的選項如下：

- **黑名單 (使用或不使用記錄功能)：**這是預設選項，會在 DFW 上建立全部允許規則。
- **白名單 (使用或不使用記錄功能)：**建立全部拒絕流量防火牆規則。只允許來自防火牆規則中定義的站台或應用程式的通訊，並對所有其他通訊拒絕存取，這包括 DHCP 流量。
- **無：**選取此選項會停用將防火牆規則加入黑名單或白名單的功能。如果您有一組已用舊版 NSX-T Data Center 設定的規則，此選項會很有用。

設定閘道防火牆

閘道防火牆代表實施於周邊防火牆的規則。

所有共用的規則視圖下方提供預先定義的類別，其中顯示所有閘道的規則。規則的評估順序是由上至下、由左至右。可以使用 API 來變更類別名稱。

表 10-3. 閘道防火牆規則的類別

規則類別	用途
緊急	用於隔離。也可用於允許規則。
系統	這些規則是由 NSX-T Data Center 自動產生，並且專門用於內部控制平面流量，例如 BFD 規則、VPN 規則等。 備註 請勿編輯系統規則。
共用的預先定義的規則	這些規則會全面地跨閘道實施。
本機閘道	這些規則專門用於特定閘道。
自動服務規則	這些是自動探索的規則，適用於資料平面。您可以視需要編輯這些規則。
預設值	這些規則定義預設的閘道防火牆行為。

新增閘道防火牆原則和規則

在屬於預先定義之類別的 [防火牆原則] 區段下新增閘道防火牆規則，即可實作閘道防火牆規則。

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 選取安全性 > 南北向安全性 > 閘道防火牆，並導覽至您要新增原則的類別。

- 3 按一下**新增原則**。如需類別的詳細資訊，請參閱[設定閘道防火牆](#)。
- 4 為新的原則區段輸入**名稱**。
- 5 選取原則**目的地**網域。保留預設的原則網域，或者新增或建立其他網域。網域是一種邏輯結構，代表一個安全性區域以及所有安全群組和規則。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

- 6 按一下齒輪圖示以進行下列原則設定：

功能表選項	說明
TCP 嚴格	TCP 連線會以三向信號交換 (SYN、SYN-ACK、ACK) 開始，並通常以雙向交換 (FIN、ACK) 結束。在某些情況下，防火牆可能看不到特定流量的三向信號交換 (例如由於非對稱流量)。依預設，防火牆不會強制必須看到三向信號交換，且將會提取已建立的工作階段。TCP 嚴格可以每個區段為基礎啟用，以關閉中間工作階段提取，並強制要求三向信號交換。 當針對特定防火牆原則啟用 TCP 嚴格模式，且使用預設「任何-任何」封鎖規則時，系統將捨棄未完成三向信號交換連線要求，且符合中此原則區段中以 TCP 為基礎之規則的封包。嚴格僅適用於可設定狀態的 TCP 規則，且會在閘道防火牆原則層級上啟用。TCP 嚴格不會針對符合未指定任何 TCP 服務之預設「任何-任何」允許的封包強制執行。
可設定狀態	可設定狀態的防火牆會監控作用中連線的狀態，並使用此資訊決定可通過防火牆的封包。
已鎖定	您可以鎖定原則，以防多位使用者對相同的區段進行變更。鎖定區段時，必須加上註解。

- 7 按一下**發佈**。您可以新增多個原則，然後一同發佈。
新的原則即會顯示在畫面上。
- 8 選取原則區段，然後按一下**新增規則**。
- 9 輸入規則的名稱。
- 10 在**來源**資料行中按一下編輯圖示，然後選取規則來源。如需詳細資訊，請參閱[新增群組](#)。
- 11 在**目的地**資料行中按一下編輯圖示，然後選取規則的目的地。若未定義，則目的地會符合任何項目。如需詳細資訊，請參閱[新增群組](#)。
- 12 在**服務**資料行中按一下編輯圖示，然後選取服務。若未定義，則服務會符合任何項目。
- 13 **套用至**資料行定義每個規則的強制執行範圍，並且主要用於最佳化 ESXi 和 KVM 主機上的資源。您可以針對特定區域和承租人定義目標明確的原則，而不會干擾已針對其他承租人和區域定義的原則。在此資料行中，您可以選擇邏輯路由器或路由型 VPN 工作階段上的邏輯路由器 (第 0 層或第 1 層) 或介面。

14 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。

15 按一下狀態切換按鈕以啟用或停用規則。**16** 按一下齒輪圖示，以設定記錄、方向、IP 通訊協定、標籤和說明。

選項	說明
記錄	可關閉或開啟記錄。記錄會儲存在 ESXi 與 KVM 主機上的 /var/log/dfwptlogs.log 檔案。
方向	選項為 輸入 、 輸出 及 輸入/輸出 。預設為 輸入/輸出 。此欄位是指從目的地物件的角度而言的流量方向。 輸入 表示僅會檢查流向物件的流量， 輸出 表示僅會檢查來自物件的流量，而 輸入/輸出 則表示會檢查這兩個方向的流量。
IP 通訊協定	選項為 IPv4 、 IPv6 及 IPv4_IPv6 。預設為 IPv4_IPv6 。
標籤	已新增至規則的標籤。

備註 按一下圖表圖示以檢視防火牆規則的流量統計資料。您可以查看位元組、封包計數和工作階段等資訊。

17 按一下**發佈**。可以新增多個規則，然後一同發佈。

設定東西向網路自我檢查

合作夥伴向 NSX-T Data Center 登錄網路服務 (例如入侵偵測系統或入侵防護系統 (IDS/IPS)) 後，身為管理員的您可以設定網路服務，來自我檢查在內部部署資料中心中虛擬機器之間傳輸的東西向流量。

東西向網路安全性的高階工作

請依照下列步驟設定東西向流量的網路安全性。

表 10-4. 設定東西向網路自我檢查的工作清單

工作流程工作	角色	實作
登錄服務	合作夥伴	僅 API
登錄廠商範本	合作夥伴	僅 API
登錄 Service Manager	合作夥伴	僅 API
部署用於執行東西向流量自我檢查的服務	管理員	API 和 NSX Manager 使用者介面

表 10-4. 設定東西向網路自我檢查的工作清單 (續)

工作流程工作	角色	實作
新增服務設定檔	管理員	API 和 NSX Manager 使用者介面
新增服務鏈結	管理員	API 和 NSX Manager 使用者介面
新增東西向流量的重新導向規則	管理員	API 和 NSX Manager 使用者介面

東西向網路保護的主要概念

內部部署資料中心上的客體虛擬機器之間的流量受到合作夥伴提供的第三方服務保護。本文提供幾個概念，可協助您瞭解工作流程。

- **服務：**合作夥伴向 NSX-T Data Center 登錄服務。服務表示合作夥伴所提供的安全性功能、服務部署詳細資料 (例如服務虛擬機器的 OVF URL)、連結服務的點、服務狀態。
- **廠商範本：**其中包含服務可對網路流量執行的功能。合作夥伴定義廠商範本。例如，廠商範本可提供網路作業服務，例如使用 IPSec 服務建立通道。
- **服務設定檔：**是廠商範本的執行個體。NSX-T Data Center 管理員可以建立將由服務虛擬機器耗用的服務設定檔。
- **客體虛擬機器：**網路中流量的來源或目的地。傳入或傳出流量由服務鏈結進行自我檢查，此服務鏈結是針對執行東西向網路服務的規則而定義的。
- **服務虛擬機器：**執行由服務指定的 OVA 或 OVF 應用裝置的虛擬機器。此虛擬機器透過服務平面連線以接收重新導向的流量。
- **服務執行個體：**是在主機上部署服務時建立的。每個服務執行個體具有對應的服務虛擬機器。
- **服務區段：**與傳輸區域相關聯的服務平面的區段。每個服務連結都與其他服務連結以及 NSX-T 提供的一般 L2 或 L3 網路區段區隔。服務平面可管理服务連結。
- **Service Manager：**是指向一組服務的合作夥伴 Service Manager。
- **服務鏈結：**是由管理員定義的服務設定檔的邏輯序列。服務設定檔會按照服務鏈結中定義的順序對網路流量進行自我檢查。例如，第一個服務設定檔為防火牆，第二個服務設定檔為監視器，依此類推。服務鏈結可以針對不同的流量方向 (出口/入口) 指定不同的服務設定檔序列。
- **重新導向原則：**確保為特定服務鏈結分類的流量重新導向至該服務鏈結。它基於與 NSX-T Data Center 安全群組和服務鏈結相符的流量模式。與模式相符的所有流量都會沿著服務鏈結重新導向。
- **服務路徑：**是實作服務鏈結之服務設定檔的一系列服務虛擬機器。管理員會定義服務鏈結，其中包含預先定義的服務設定檔順序。NSX-T Data Center 會根據客體虛擬機器和服務虛擬機器的數目和位置，從服務鏈結產生多個服務路徑。針對要進行自我檢查的流量選取最佳服務路徑。每個服務路徑由服務路徑索引 (SPI) 識別，並且沿路徑的每個躍點都具有唯一的服務索引 (SI)。

部署用於執行東西向流量自我檢查的服務

合作夥伴登錄服務後，做為管理員，您必須在叢集的成員主機上部署服務的執行個體。

在叢集中的所有 NSX-T Data Center 主機上部署執行合作夥伴安全性引擎的合作夥伴服務虛擬機器。部署 SVM 後，您可以建立 SVM 用來保護客體虛擬機器的原則規則。

必要條件

- 所有主機都由 vCenter Server 管理。
- 合作夥伴服務已向 NSX-T Data Center 登錄，並且已可供部署。
- NSX-T Data Center 管理員可以存取合作夥伴服務和廠商範本。
- 服務虛擬機器與合作夥伴 Service Manager (主控台) 雙方必須能夠在管理網路層級彼此通訊。

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 **系統 > 服務部署 > 部署 > 部署服務**。
- 3 從 [合作夥伴服務] 欄位中，選取合作夥伴服務。
- 4 輸入服務部署名稱。
- 5 在 [計算管理程式] 欄位中，選取要部署服務之 vCenter Server 上的計算資源。
- 6 在 [叢集] 欄位中，選取必須部署服務的叢集。
- 7 在 [資料存放區] 下拉式功能表中，選取資料存放區做為服務虛擬機器的存放庫。
- 8 在 [網路] 資料行中按一下 **設定**，然後透過選擇 DHCP 或靜態 IP 位址類型、控制網路和資料網路來進入 [管理網路] 介面。
- 9 在 [服務區段] 欄位中，從清單中選取服務區段，或按一下 [動作] 圖示來新增或編輯服務區段。服務區段決定與覆疊傳輸區域相關聯的客體虛擬機器會提供東西向網路流量保護。
- 10 在 [部署規格] 欄位中，選取要在叢集主機上部署之服務虛擬機器的服務和構成要素。可以有多個服務可供部署。
- 11 在 [部署範本] 欄位中選取廠商範本，其中包含的屬性可保護您要在客體虛擬機器群組上執行的工作負載。
- 12 在 [叢集部署計數] 中，輸入要在叢集上部署的服務虛擬機器數目。vCenter Server 會決定在哪一台主機上部署服務虛擬機器。
- 13 按一下 **儲存**。

結果

在服務部署完成後，合作夥伴 Service Manager 會收到更新的通知。

後續步驟

瞭解主機上部署之服務執行個體的部署詳細資料和健全狀況狀態。請參閱[檢視服務執行個體詳細資料](#)。

新增服務設定檔

服務設定檔是合作夥伴廠商範本的執行個體。管理員可以自訂廠商範本的屬性來建立範本的執行個體。

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 導覽到 **安全性 > 東西向安全性 > 網路自我檢查 > 服務設定檔**。
- 3 在 [合作夥伴服務] 下拉式欄位中選取服務。您可以為所選的服務建立服務設定檔。
- 4 輸入服務設定檔的名稱，然後選取廠商範本。
- 5 按一下**儲存**。

結果

即為合作夥伴服務建立了新服務設定檔。

後續步驟

新增服務鏈結。請參閱[新增服務鏈結](#)。

新增服務鏈結

服務鏈結是網路管理員所定義的服務設定檔的邏輯序列。

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**安全性 > 東西向安全性 > 網路自我檢查 > 服務鏈結 > 新增鏈結**。
- 3 輸入服務鏈結名稱。
- 4 在 [服務區段] 欄位中，選取您要套用服務鏈結的服務區段。服務區段是連接覆疊傳輸區域的多個服務虛擬機器之服務平面的區段。服務鏈結中的每個服務虛擬機器與 NSX-T Data Center 執行的其他服務虛擬機器及 L2 和 L3 網路區段不同。服務平面控制服務虛擬機器的存取權。
- 5 若要設定正向路徑，請按一下**設定正向路徑**欄位，然後按一下**依序新增設定檔**。
- 6 新增服務鏈結中的第一個設定檔，然後按一下**新增**。
- 7 若要指定下一個服務設定檔，請按一下**依序新增設定檔**，然後輸入詳細資料。您也可以使用向上和向下箭頭圖示來重新排列設定檔的順序。
- 8 按一下**儲存**以完成為服務鏈結新增正向路徑的作業。
- 9 在 [反向路徑] 資料行中，為服務平面選取**反向正向路徑**，來以反向順序使用正向路徑。若要設定新的反向路徑，請按一下**設定反向路徑**，然後新增反向路徑。
- 10 按一下**儲存**以完成為服務鏈結新增反向路徑的作業。
- 11 在 [故障原則] 欄位中，
 - 選取**允許**，在服務虛擬機器發生故障時，將流量傳送至目的地虛擬機器。服務虛擬機器故障與否是由運作情況偵測機制偵測的，而該機制只能由合作夥伴啟用。
 - 選取**封鎖**，在服務虛擬機器發生故障時，不將流量傳送至目的地虛擬機器。

12 按一下儲存。

結果

新增服務鏈結後，合作夥伴 Service Manager 會收到更新的通知。

後續步驟

建立重新導向規則以自我檢查東西向網路流量。請參閱[新增東西向流量的重新導向規則](#)。

新增東西向流量的重新導向規則

新增重新導向東西向流量來進行網路自我檢查的規則。

規則是在原則中定義的。做為概念的原則，類似於防火牆中區段的概念。新增原則時，請選取重新導向流量來由服務鏈結的服務設定檔進行自我檢查的服務鏈結。

規則定義包含流量的來源和目的地、自我檢查服務、要套用規則的 NSX 物件，以及流量重新導向原則。發佈規則後，NSX Manager 會在找不到相符的流量模式時觸發此規則。規則會開始自我檢查流量。例如，當 NSX Manager 將流量歸類為必須自我檢查時，它不會將流量轉送至一般 Distributed Firewall，而是將該流量重新導向至原則中指定的服務鏈結。服務鏈結中定義的服務設定檔會自我檢查合作夥伴提供之網路服務的流量。如果服務設定檔完成自我檢查，並且未在流量中偵測到任何安全性問題，就會將流量轉送至服務鏈結中的下一個服務設定檔。在服務鏈結結束時，流量會轉送至目的地。

所有通知都會傳送給合作夥伴 Service Manager 和 NSX-T Data Center。

必要條件

服務鏈結可用於重新導向流量來進行網路自我檢查。

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 安全性 > 東西向安全性 > 網路自我檢查 > 規則 > 新增原則。
[原則] 區段類似於 [防火牆] 區段，您可在其中定義規則來判定流量的流動方式。
- 3 (選擇性) 按一下預設網域以選取不同的網域。
請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。
- 4 選取服務鏈結。
- 5 若要新增原則，請按一下**發佈**。
- 6 按一下區段上的垂直省略符號 (⋮)，然後按一下**新增規則**。
- 7 編輯**來源**欄位，以透過定義成員資格準則、靜態成員、IP/MAC 位址或 Active Directory 群組來新增群組。可以從下列其中一個類型定義成員資格準則：虛擬機器、邏輯交換器、邏輯連接埠、IP 集合。
您可以從下列其中一個類別選取靜態成員：群組、區段、區段連接埠、虛擬網路介面或虛擬機器。
- 8 按一下**儲存**。
- 9 若要新增目的地群組，請編輯**目的地**欄位。

10 在 [套用至] 欄位中，您可以執行下列其中一項作業：

- 選取 **DFW** 以將規則套用到連結至邏輯交換器的所有虛擬 NIC。
- 選取**虛擬機器群組**以將規則套用到群組之成員虛擬機器的虛擬 NIC。可以從靜態清單或根據動態準則選取成員。支援的 NSX-T Data Center 物件包括：虛擬機器、邏輯交換器、邏輯連接埠、IP 集合等。

11 在 [動作] 欄位中，選取**重新導向**以將流量重新導向至服務鏈結，或是選取**不重新導向**，不對流量實施網路自我檢查。

12 按一下**發佈**。

13 若要還原已發佈的規則，請選取規則，然後按一下**還原**。

14 若要新增原則，請按一下 **+ 新增原則**。

15 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。

16 若要啟用規則，請啟用 [啟用/停用] 圖示，或從功能表中選取規則，然後按一下**啟用 > 啟用規則**。

17 啟用或停用規則之後，請按一下**發佈**以強制執行規則。

結果

流入來源的流量會重新導向至服務鏈結來進行網路自我檢查。鏈結中的服務設定檔對流量進行自我檢查後，會將流量傳送到目的地。

在部署期間，特定原則的虛擬機器群組成員資格有可能變更。NSX-T Data Center 會向合作夥伴 Service Manager 通知這些更新。

設定南北向網路自我檢查

合作夥伴向 NSX-T Data Center 登錄網路服務後，身為管理員的您可以設定網路服務，來自我檢查在資料中心和外部網路中虛擬機器之間傳輸的南北向流量。

南北向網路安全性的高階工作

請依照下列步驟設定南北向流量的網路安全性。

表 10-5. 設定南北向網路自我檢查的工作清單

工作流程工作	角色	實作
將服務登錄至 NSX-T Data Center	合作夥伴	僅 API
部署用於執行南北向流量自我檢查的服務	管理員	API 和 NSX Manager 使用者介面
設定流量重新導向	管理員	API 和 NSX Manager 使用者介面

部署用於執行南北向流量自我檢查的服務

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。

在充當實體環境與 vCenter Server 上邏輯網路之間之閘道的第 0 層或第 1 層邏輯路由器上部署合作夥伴服務虛擬機器。在部署 SVM 做為獨立服務執行個體或主動-待命服務執行個體後，您可以建立重新導向規則，來將流量重新導向至 SVM 進行網路自我檢查。

必要條件

- 所有主機都由 vCenter Server 管理。
- 合作夥伴服務已向 NSX-T Data Center 登錄，並且已可供部署。
- NSX-T Data Center 管理員可以存取合作夥伴服務和廠商範本。

確認邏輯路由器的高可用性模式是主動-待命。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 合作夥伴服務 > 服務執行個體 > 目錄**。
- 3 [目錄] 索引標籤會顯示已登錄的服務。
- 4 選取 OVF 構成要素中顯示的服務，然後按一下**部署**以開始部署服務執行個體。
- 5 在 [合作夥伴服務插入] 視窗中，按一下**繼續**。
- 6 在 [合作夥伴服務] 視窗中，輸入詳細資料。

表 10-6. 合作夥伴服務詳細資料

欄位	說明
執行個體名稱	輸入用於識別服務執行個體的名稱。
說明	關於服務執行個體的說明。
合作夥伴服務	選取已向 NSX-T Data Center 登錄的合作夥伴服務。
部署規格	選取要部署的構成要素。
邏輯路由器	選取必須部署服務執行個體的第 0 層邏輯路由器。

- 7 按**下一步**。
- 8 在 [執行個體組態] 視窗中，輸入詳細資料。

表 10-7. 服務執行個體詳細資料

欄位	說明
部署模式	選取 獨立 以在第 0 層邏輯路由器上部署單一服務執行個體。 選取 高可用性 以在第 0 層邏輯路由器上以主動-待命模式部署幾個服務執行個體。
故障原則	選取 允許 或 封鎖 。
服務執行個體 IP 位址	輸入服務執行個體所用的 IP 位址。

表 10-7. 服務執行個體詳細資料 (續)

欄位	說明
閘道	輸入閘道位址。
子網路遮罩	輸入子網路遮罩。
網路識別碼	輸入要連線管理網路的邏輯交換器的網路識別碼。
計算管理程式	選取已登錄的 vCenter Server。
資源集區	選取提供資源來部署服務執行個體的資源集區。
資料存放區	選取儲存服務執行個體資料的存放庫。

9 按下一步。

10 在 [進階組態] 視窗中，輸入詳細資料。

表 10-8.

欄位	說明
部署範本	選取要在部署服務執行個體時使用的範本。
授權	輸入範本的授權。

11 按一下完成。

結果

[服務執行個體] 索引標籤會顯示部署進度。可能需要幾分鐘時間才能完成部署。確認部署狀態，以確保成功在第 0 層邏輯路由器上部署服務執行個體。

或者，移至 vCenter Server 並確認部署狀態。

後續步驟

設定規則，以將流量重新導向至第 0 層路由器上部署的服務執行個體。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，請設定路由器會重新導向至服務的流量類型。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[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 **進階網路與安全性 > 合作夥伴服務 > 服務執行個體**。
- 3 按一下服務執行個體。

- 4 按一下**流量重新導向**索引標籤。
- 5 若要新增區段，請選取現有的區域，然後按一下**新增區段**。
 - ◆ 從功能表中選取**新增以上區段**或**新增以下區段**。

此時會建立新的區段。要重新導向的流量類型設為 **L3 重新導向**、服務類型為**無狀態**，且**套用至欄位**與主機上設定的第 0 層邏輯路由器相關聯。在定義規則後，會自動填入**規則欄位**。
- 6 按一下**發佈**以保存區段的組態詳細資料。
- 7 若要在該區段中新增規則，請選取該區段，然後按一下**新增規則**。
- 8 在規則列中，輸入下列詳細資料：
 - a 輸入規則名稱。
 - b 輸入 L3 流量的來源和目的地。合作夥伴服務虛擬機器會先對從來源傳入的流量進行自我檢查，然後再將流量重新導向至目的地虛擬機器。
 - c 在**套用至欄位**中，選取第 0 層路由器的上行。
 - d 如果服務虛擬機器需要對流量進行自我檢查，請在**動作欄位**中選取**重新導向**；如果不需要對流量進行南北向自我檢查，請選取**不重新導向**。
- 9 每項規則可以個別啟用。啟用後的規則將會套用至符合規則的流量。
- 10 按一下 [進階設定]，以設定流量方向並啟用記錄。
- 11 在包含規則的區段結束時，按一下**發佈**以保存區段中的規則，或按一下**還原**以取消作業。

結果

流量會傳送到將原則規則套用至流量的網路自我檢查規則。

後續步驟

請參閱[針對南北向流量新增重新導向規則](#)。

針對南北向流量新增重新導向規則

使用**進階網路與安全性**使用者介面來設定南北向重新導向規則。只有在第 0 層路由器上插入的服務，才會發生流量重新導向。

請依照[設定流量重新導向](#)中的指示操作。

必要條件

- 在 NSX-T 上登錄並部署第三方服務。
- 設定第 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 安全性 > 南北向防火牆 > 網路自我檢查 (N-S) > 新增原則。

[原則] 區段類似於 [防火牆] 區段，您可在其中定義規則來判定流量的流動方式。

3 (選擇性) 按一下預設網域以選取不同的網域。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

4 將**重新導向目標**設為已在 NSX-T 中登錄的服務執行個體，方可對在來源與目的地實體之間傳輸的流量執行網路自我檢查。

5 若要新增原則，請按一下**發佈**。

6 按一下區段上的垂直省略符號 (⋮)，然後按一下**新增規則**。

7 編輯**來源**欄位，以透過定義成員資格準則、靜態成員、IP/MAC 位址或 Active Directory 群組來新增群組。可以從下列其中一個類型定義成員資格準則：虛擬機器、邏輯交換器、邏輯連接埠、IP 集合。您可以從下列其中一個類別選取靜態成員：群組、區段、區段連接埠、虛擬網路介面或虛擬機器。

8 按一下**儲存**。

9 若要新增目的地群組，請編輯**目的地**欄位。

10 在 [套用至] 欄位中，您可以執行下列其中一項作業：

- 選取 **DFW** 以將規則套用到連結至邏輯交換器的所有虛擬 NIC。
- 選取**虛擬機器群組**以將規則套用到群組之成員虛擬機器的虛擬 NIC。可以從靜態清單或根據動態準則選取成員。支援的 NSX-T Data Center 物件包括：虛擬機器、邏輯交換器、邏輯連接埠、IP 集合等。

11 在 [動作] 欄位中，選取**重新導向**以將流量重新導向至服務執行個體，或選取**不重新導向**而不對流量套用網路自我檢查。

12 按一下**發佈**。

13 若要還原已發佈的規則，請選取規則，然後按一下**還原**。

14 若要新增原則，請按一下 **+** **新增原則**。

15 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。

16 若要啟用規則，請啟用 [啟用/停用] 圖示，或從功能表中選取規則，然後按一下**啟用 > 啟用規則**。

17 啟用或停用規則之後，請按一下**發佈**以強制執行規則。

結果

根據設定的動作，南北向流量會重新導向至服務執行個體以進行網路自我檢查。

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**進階網路與安全性 > 合作夥伴服務 > 服務執行個體**。
- 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。

設定 Endpoint Protection

在合作夥伴向 NSX-T Data Center 登錄其服務後，Endpoint Protection 原則會套用至客體虛擬機器群組。在為客體虛擬機器設定 Endpoint Protection 之前，您必須部署合作夥伴服務做為服務插入工作流程的一部分。

瞭解端點保護

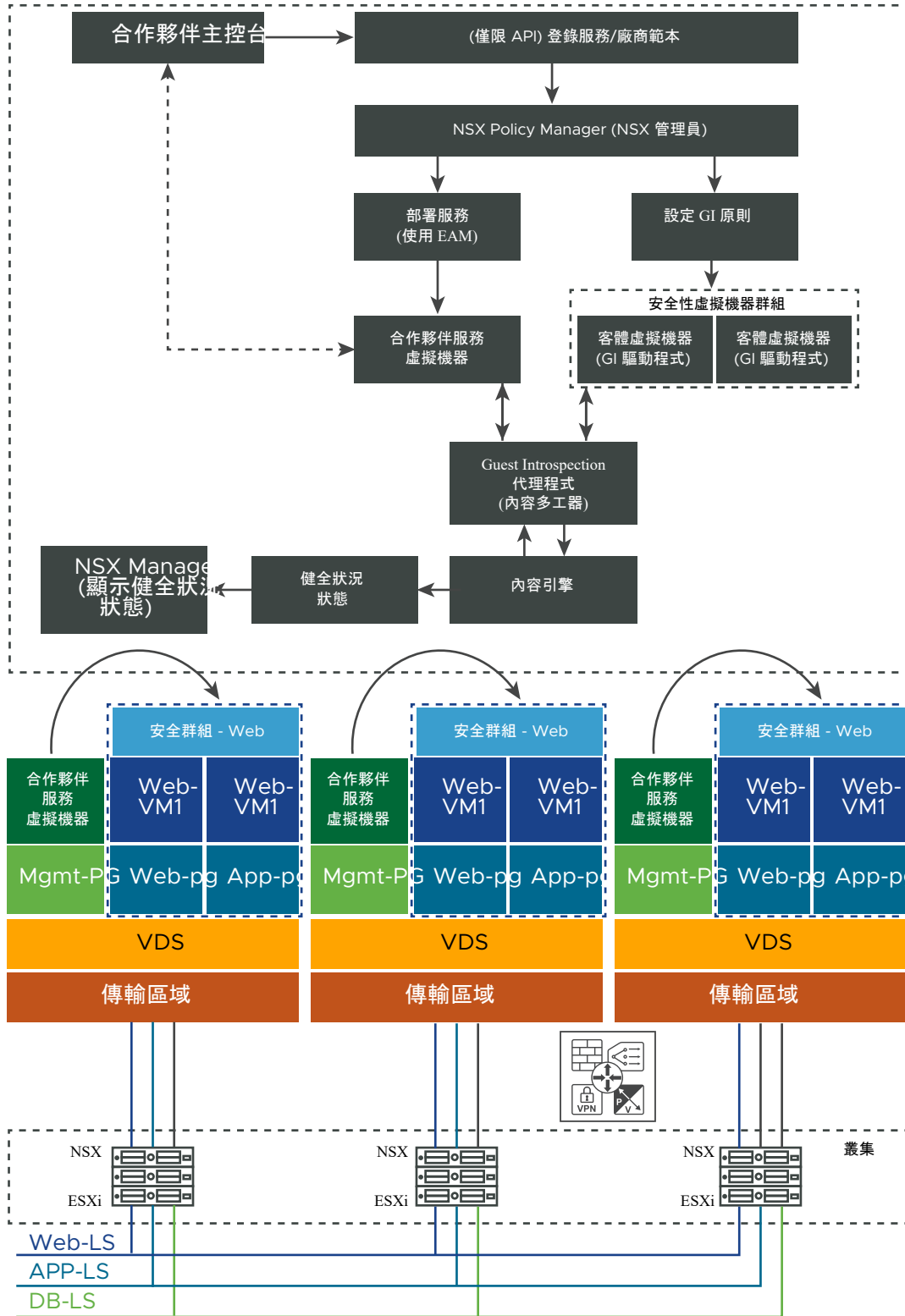
瞭解端點保護的使用案例、工作流程和主要概念。

端點保護使用案例

NSX-T 會為虛擬網路提供 L2 至 L4 可設定狀態的防火牆服務。如果您的環境需要有防惡意程式碼的安全性服務來保護客體虛擬機器，NSX 透過在主機中整合第三方廠商的服務來防範惡意程式碼，提供了強大的方式來自我檢查客體虛擬機器。

在主機節點準備期間，NSX-T 會安裝 Guest Introspection 主機代理程式，做為叢集中的所有主機上主機服務包安裝的一部分。因此，不需要在主機節點上單獨安裝 Guest Introspection 主機代理程式。合作夥伴服務虛擬機器 (SVM) 會安裝在主機節點上做為虛擬應用裝置。SVM 使用 Guest Introspection API 程式庫 (EPSec API 程式庫) 對客體虛擬機器進行自我檢查，並保護其免遭惡意程式碼侵害。

圖 10-1. 端點保護使用案例



身為 NSX 管理員，您可以實作部署為服務虛擬機器 (SVM) 的防惡意程式碼解決方案，以監控客體虛擬機器上的檔案活動。每當存取檔案時，例如嘗試開啟檔案，防惡意程式碼服務虛擬機器就會收到事件通知。然後，服務虛擬機器便會決定要對事件做何回應，例如，檢查檔案中是否有病毒簽章。

- 如果服務虛擬機器判斷檔案不含病毒，就會允許檔案開啟作業繼續執行。
- 如果服務虛擬機器在檔案中偵測到病毒，就會嘗試清理檔案。
 - 如果成功清理檔案，服務虛擬機器就會讓檔案開啟作業繼續執行。
 - 如果服務虛擬機器無法清理該檔案，就會阻止檔案開啟作業，並將檔案 (和虛擬機器) 標記為受到感染。此外，您還可定義規則，以便自動將虛擬機器移至含有受感染虛擬機器的安全群組。

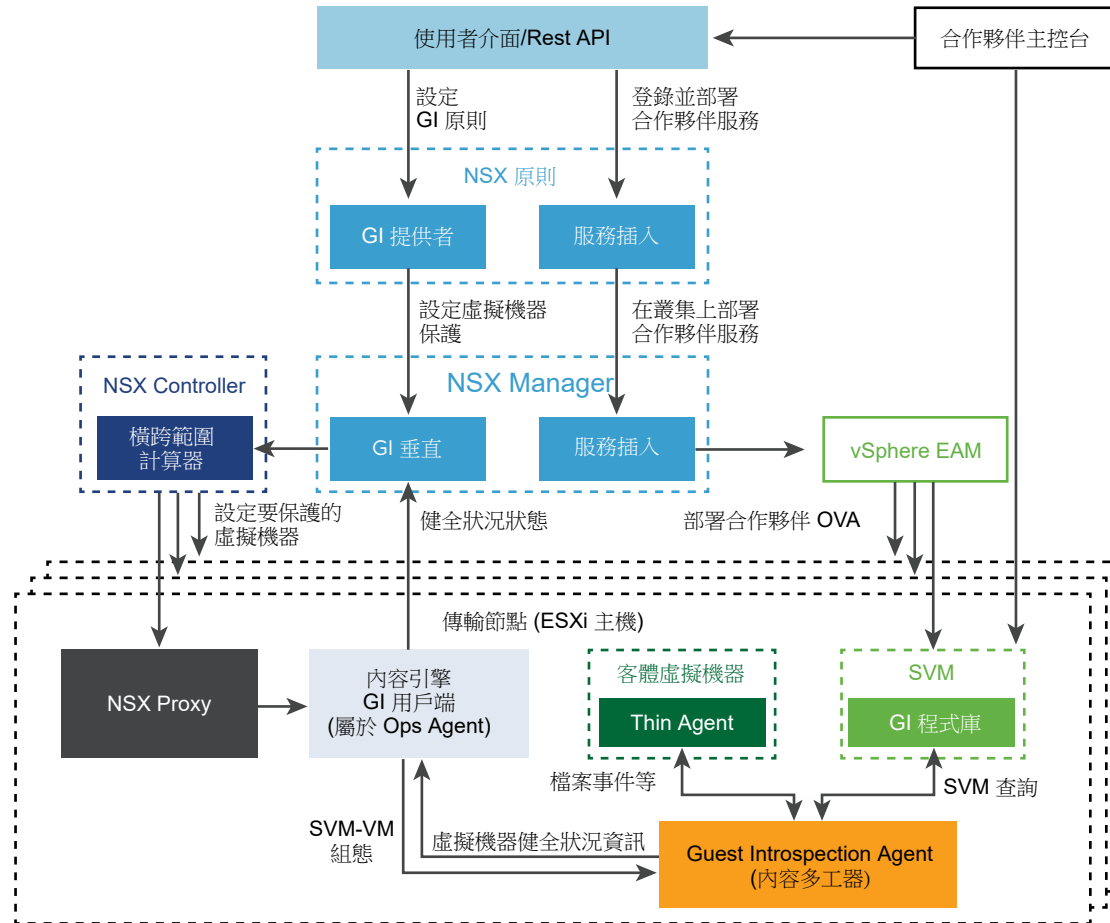
備註 如果客體虛擬機器已中斷連線或無法連線到 ESXi 主機代理程式 (MUX) 或 SVM，則可能會在未經防毒掃描的情況下允許客體上的檔案存取。

不像客體虛擬機器可能會離線，服務虛擬機器會持續執行。因此，服務虛擬機器可持續更新防毒簽章、為主機上的虛擬機器提供不中斷的保護，並且立即為新上線的虛擬機器提供保護。因為 Guest Introspection 可讓服務虛擬機器讀寫客體虛擬機器上的特定檔案，所以，它提供了一種高效的方式來避免資源瓶頸並最佳化記憶體使用。

Guest Introspection 架構

瞭解 NSX-T Data Center 中的服務插入與客體自我檢查元件架構。

圖 10-2. Guest Introspection 架構



合作夥伴登錄：

- 合作夥伴透過叫用由 NSX Manager API 提供的 Guest Introspection Rest API 程式庫，登錄服務。
- 稍後在工作流程中將合作夥伴服務 (服務虛擬機器) 部署到主機上時，合作夥伴主控台會向 SVM 登錄，以接收與維護活動相關的通知以及客體虛擬機器群組上所發生的事件通知。

部署服務：

- 使用服務插入架構在 NSX 準備的主機上部署合作夥伴服務。
- vSphere Enterprise Agency Manager (EAM) 會在 NSX-T 主機上部署合作夥伴服務虛擬機器。
- 叢集中的每個主機都執行該服務的執行個體，即 SVM。

Guest Introspection 驅動程式安裝:

- 讓 SVM 與客體虛擬機器和其他元件進行通訊之前，在客體虛擬機器上安裝 GI 驅動程式。
- 管理員使用 VMTools 在每個客體虛擬機器上安裝精簡型代理程式。
- 精簡型代理程式會執行下列功能。
 - 透過稱為虛擬機器通訊介面 (VMCI) 的快速通道，與稱為 Guest Introspection 代理程式 (MUX) 的元件進行通訊。

- 擷取客體虛擬機器上的檔案存取事件。
- 向合作夥伴的 SVM 通知客體虛擬機器上的事件。
- 在客體虛擬機器上實作保護原則。例如，允許或拒絕檔案存取，或是隔離檔案或虛擬機器。

原則建立：

管理員會建立原則來將虛擬機器群組與服務設定檔建立關聯，藉以保護虛擬機器群組。

- NSX Policy Manager 會撰寫 GI 原則並與 GI 元件 (執行於 NSX Manager) 互動。
- 此 GI 元件負責在虛擬機器群組上設定 GI 原則，以及向控制平面 (特別是 CCP 範圍計算器元件) 傳送此組態。

控制平面管理虛擬機器組態：

- 控制平面會收到有關套用至虛擬機器群組的 GI 原則的組態。它會計算主控特定群組之虛擬機器的傳輸節點範圍。
- CCP 範圍計算器：NSX Manager 會向 CCP 傳送群組 (虛擬機器及其相關原則) 的組態詳細資料。範圍計算器會判斷這些虛擬機器所屬的傳輸節點。然後，它會將虛擬機器識別碼清單連同相關原則，推送至主控這些虛擬機器的傳輸節點。LCP 會接收此資訊並將其儲存在主機上的資料庫。
- 內容引擎會接聽資料庫中發生的任何更新，並更新 Guest Introspection 代理程式 (MUX) 元件。

在 SVM、客體虛擬機器與內容多工器之間建立通訊：

- SVM：合作夥伴服務會在叢集的每個主機上稱為服務虛擬機器 (SVM) 的獨立應用裝置上執行。合作夥伴會提供在登錄服務時用於部署 SVM 的 OVF 位置。SVM 會與下列元件進行通訊：
 - 客體虛擬機器和 Guest Introspection 代理程式會透過 ESXi Hypervisor 上的快速通道 (VMCI) 進行通訊，而客體虛擬機器和 SVM 則會透過 TCP/IP 通道進行通訊。客體虛擬機器內執行的精簡型代理程式會收集作業系統與檔案活動的相關資訊。SVM 會透過 EPSec API 程式庫收集精簡型代理程式所提供的內容。GI 驅動程式會向 SVM 傳送事件。SVM 會判斷檔案是惡意程式碼還是乾淨的檔案。SVM 會讀取 EPSec API 程式庫，以根據所收集的內容來決定要採取的動作。
 - 待叢集的每個主機上都部署了 SVM 後，NSX Manager 中的 Guest Introspection 元件便會將 SVM 組態向下傳送到內容引擎。內容引擎會使用新的 SVM 組態資訊更新 Guest Introspection 代理程式。SVM 會登錄來接收虛擬機器或檔案上所發生的任何事件。

Guest Introspection 代理程式建立與客體自我檢查程式庫的通訊，這會使 SVM 收到虛擬機器開啟電源事件。SVM 現已可接收來自精簡型代理程式的檔案事件。

- Guest Introspection 代理程式：此為 Guest Introspection 主機模組 (內容多工器)，會對來自所有受保護客體虛擬機器的訊息進行多工處理並轉送給 SVM。在 NSX-T 主機上，此模組以 vSphere Installation Bundle (VIB) 形式安裝。在 ESX 主機上，NSX Manager 安裝並設定此模組。主機上的 Guest Introspection 代理程式組態檔 (/var/run/muxconfig.xml) 會指定合作夥伴解決方案的相關組態資訊。VMConfig 檔案會列出受保護的虛擬機器以及對應解決方案。SolutionConfig 檔案則會列出 SVM 詳細資料，例如解決方案識別碼、IP 位址、接聽程式連接埠、UUID。

內容引擎的角色：

- 內容引擎：此元件會向 Guest Introspection 代理程式傳送與虛擬機器相關聯之 SVM 的組態詳細資料。Guest Introspection 代理程式收到組態詳細資料時，會在 `muxconfig.xml` 檔案中記錄 SVM 組態更新。組態資訊還包含服務設定檔標籤，供 SVM 查詢及識別原則。在自我檢查期間，Guest Introspection 代理程式僅會轉送來自與該 SVM 相關聯之虛擬機器的事件。此元件負責向 NSX Manager 中的 GI 垂直元件傳送精簡型代理程式與 Guest Introspection 代理程式的健全狀況狀態。
- 健全狀況狀態：GI 元件 (執行於 NSX Manager) 會定期從內容引擎要求健全狀況資訊。
- 內容引擎會從 Guest Introspection 代理程式收集健全狀況狀態資訊，然後將收集到的資訊傳送給 GI 元件 (執行於 NSX Manager)。健全狀況狀態由下列因素決定：合作夥伴解決方案的狀態、Guest Introspection 代理程式 (內容多工器) 與內容引擎 (Ops Agent) 之間的連線，以及 Guest Introspection 代理程式資訊、SVM 通訊協定資訊在 NSX Manager 中的可用性。

Endpoint Protection 的重要概念

會保護客體虛擬機器抵禦惡意程式碼。Endpoint Protection 工作流程需要合作夥伴向 NSX-T Data Center 登錄其服務，管理員才能使用這些服務。本文提供幾個概念，可協助您瞭解工作流程。

- 服務定義：合作夥伴使用以下屬性定義來定義服務：名稱、說明、支援的構成要素、部署屬性 (例如儲存區、網路儲存區)。
- 服務插入：NSX 提供一種架構，可讓合作夥伴使用服務定義 API 來向 NSX-T 登錄其服務。服務插入用於在主機上部署合作夥伴服務，以便執行 Guest Introspection 來抵禦惡意程式碼。
- 橫跨範圍計算器：對於需要保護的虛擬機器群組，控制平面會查明哪些傳輸節點裝載了屬於此群組的虛擬機器。虛擬機器群組可能具有裝載於不同傳輸節點的虛擬機器。控制平面會計算裝載這些虛擬機器之傳輸節點的橫跨範圍。計算橫跨範圍後，NSX Manager 會將虛擬機器組態 (虛擬機器及其關聯的原則) 推送至每個傳輸節點。這是必要的，因為傳輸節點需要知道與虛擬機器相關聯的原則。控制平面也會將虛擬機器識別碼清單與 SVM 原則一併推送至傳輸節點。
- 服務設定檔和廠商範本：合作夥伴會登錄公開原則之保護層級的廠商範本。保護層級包括「金級」、「銀級」或「白金級」。廠商範本也可能提供合作夥伴專用的部署屬性，例如名稱或授權金鑰等。這些屬性是服務定義的一部分。這些屬性可讓 NSX 管理員自訂廠商範本，以便從單一廠商範本建立許多服務設定檔。如果廠商範本中沒有可供使用的部署屬性，則管理員只能從該廠商範本建立單一服務設定檔。
- Guest Introspection 程式庫和 SVM：Guest Introspection 程式庫 (之前稱為 EPSec) 是在合作夥伴 SVM 上執行的程式庫。它也可以充當合作夥伴 SVM 與 Guest Introspection Thin Agent 之間的介面。
- Guest Introspection Agent (MUX) 和 SVM：此元件負責將 Guest Introspection Thin Agent 事件轉送至所設定的 SVM。它也會將 SVM 要求轉送至 Guest Introspection Thin Agent。
- 內容引擎 GI 用戶端：此元件負責：
 - 將 Thin Agent 和 Guest Introspection Agent (MUX) 的健全狀況狀態傳送至 NSX Manager 中的 GI 元件。
 - 提供 NestDb 組態給 Guest Introspection Agent (MUX)。

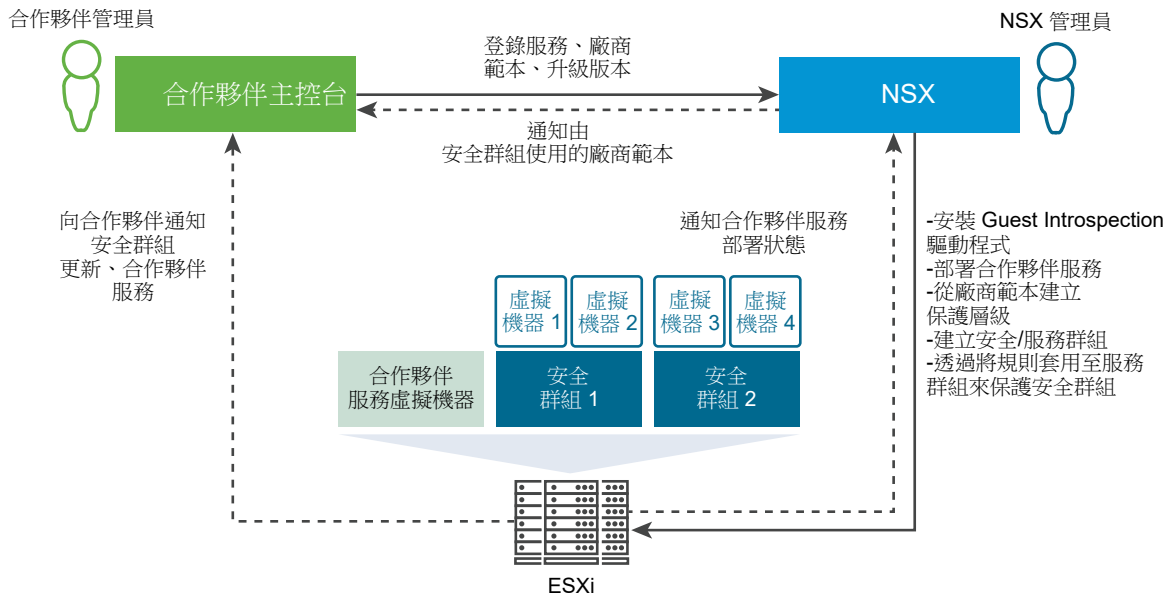
- 健全狀況狀態：內容引擎會將 SVM 的健全狀況狀態、虛擬機器健全狀況、Guest Introspection Agent 健全狀況、Guest Introspection Client 健全狀況傳送至 Guest Introspection (在 NSX Manager 上執行)。
- 網域和虛擬機器群組：網域是裝載虛擬機器群組和原則規則的環境。虛擬機器群組是裝載於單一或多個傳輸節點的虛擬機器的清單。NSX 管理員會先在網域中建立一組虛擬機器，然後再將保護原則套用至該虛擬機器群組。例如，可以為 PCI-DSS 安全性網域 (由必須符合最高安全性標準的不同虛擬機器群組組成) 建立一個網域。請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。
- 順序編號：決定跨多個網域執行規則的順序。如果存在多個網域，而每個網域都有規則，則 Guest Introspection 會對等級較高之網域的規則進行排序，然後對等級較低之網域的規則進行排序，直到對所有規則都進行排序。發佈規則之後，規則會立即套用至需要保護的虛擬機器群組，且 Guest Introspection 會開始執行。可以透過 API 呼叫或透過使用者介面來明確定義順序編號。請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

端點保護工作流程

在此工作流程的第一部分中，合作夥伴會向 NSX-T 登錄服務。在此工作流程的最後一部分中，NSX 管理員會部署已登錄的服務，並將端點保護原則套用至虛擬機器群組。

針對端點保護的客體自我檢查工作流程如下所示：

圖 10-3. 端點保護工作流程



大致而言，合作夥伴服務透過取用 EPSec API (GI) 程式庫，準備服務虛擬機器 (SVM)。服務登錄是透過合作夥伴 Service Manager 主控台叫用 NSX-T 原則 API 來進行。Service Manager 主控台由合作夥伴管理。合作夥伴除了登錄服務，還會登錄廠商範本，其中包含在 NSX-T 中套用客體虛擬機器時用來加以保護的組態。登錄後，NSX 管理員必須將具有特定 IP 位址與連接埠號碼的服務繫結至合作夥伴的 Service Manager。

合作夥伴登錄其服務後，NSX-T 管理員可以在 NSX-T Policy Manager 使用者介面上檢視所有已登錄的合作夥伴服務。管理員會將這些服務部署到叢集上。部署完成時，叢集中的每個主機便會執行 SVM，進而執行安全性引擎。SVM 使用 EPSec API 程式庫與客體虛擬機器進行通訊，藉以攔截事件。為了在客體虛擬機器上套用原則，管理員會指定規則來將虛擬機器群組與服務設定檔 (廠商範本的執行個體) 建立關聯，而服務設定檔定義了何種類型的保護層級套用至客體虛擬機器。

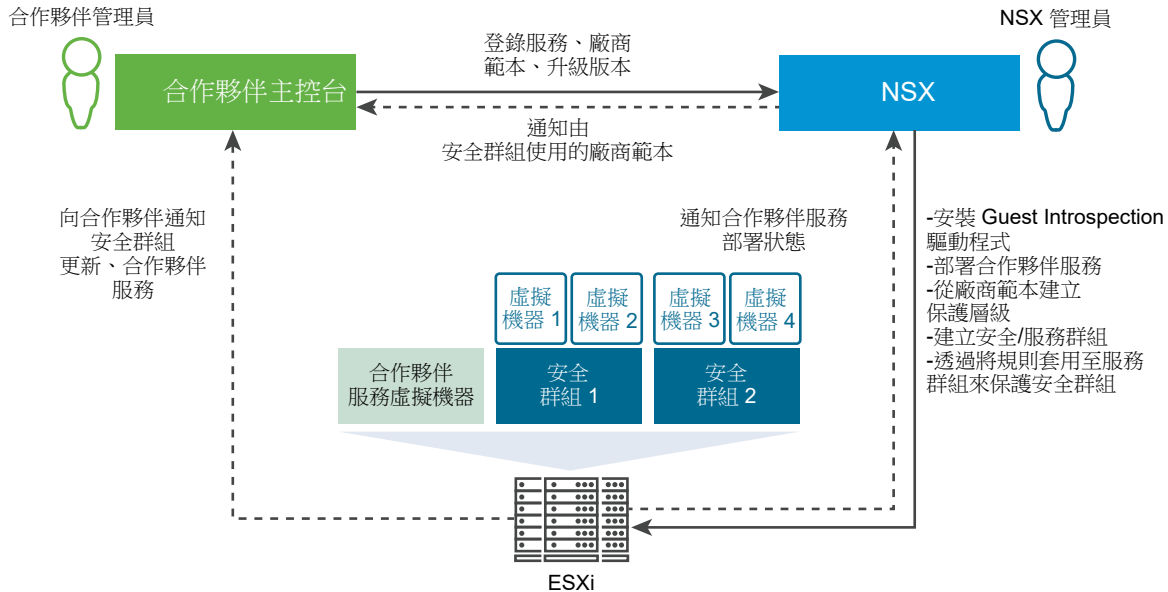
部署並設定客體自我檢查服務後，SVM 便會開始自我檢查客體虛擬機器。當客體虛擬機器上發生事件時，SVM 會攔截事件並加以修復。SVM 還會通知合作夥伴主控台和 NSX-T Manager。

端點保護工作流程

在此工作流程的第一部分中，合作夥伴會向 NSX-T 登錄服務。在此工作流程的最後一部分中，NSX 管理員會部署已登錄的服務，並將端點保護原則套用至虛擬機器群組。

針對端點保護的客體自我檢查工作流程如下所示：

圖 10-4. 端點保護工作流程



大致而言，合作夥伴服務透過取用 EPSec API (GI) 程式庫，準備服務虛擬機器 (SVM)。服務登錄是透過合作夥伴 Service Manager 主控台叫用 NSX-T 原則 API 來進行。Service Manager 主控台由合作夥伴管理。合作夥伴除了登錄服務，還會登錄廠商範本，其中包含在 NSX-T 中套用客體虛擬機器時用來加以保護的組態。登錄後，NSX 管理員必須將具有特定 IP 位址與連接埠號碼的服務繫結至合作夥伴的 Service Manager。

合作夥伴登錄其服務後，NSX-T 管理員可以在 NSX-T Policy Manager 使用者介面上檢視所有已登錄的合作夥伴服務。管理員會將這些服務部署到叢集上。部署完成時，叢集中的每個主機便會執行 SVM，進而執行安全性引擎。SVM 使用 EPSec API 程式庫與客體虛擬機器進行通訊，藉以攔截事件。為了在客體虛擬機器上套用原則，管理員會指定規則來將虛擬機器群組與服務設定檔 (廠商範本的執行個體) 建立關聯，而服務設定檔定義了何種類型的保護層級套用至客體虛擬機器。

部署並設定客體自我檢查服務後，SVM 便會開始自我檢查客體虛擬機器。當客體虛擬機器上發生事件時，SVM 會攔截事件並加以修復。SVM 還會通知合作夥伴主控台和 NSX-T Manager。

設定端點保護的必要條件

在為客體虛擬機器設定端點保護之前，請確定您符合必要條件。

必要條件

- 已在所有主機上安裝 NSX Manager。
- 藉由套用傳輸節點設定檔準備 NSX-T Data Center 叢集，並將其設定為傳輸節點。將主機設定做為傳輸節點後，會安裝 Guest Introspection 元件。請參閱《NSX-T Data Center 安裝指南》。
- 合作夥伴主控台已安裝並設定，以向 NSX-T Data Center 登錄服務。
- 確定客體虛擬機器執行虛擬機器硬體版組態檔案版本 9 或更高版本。
- 設定 VMware Tools 並安裝精簡型代理程式。
 - 請參閱在 [Linux 虛擬機器上安裝 Guest Introspection 精簡型代理程式](#)。
 - 請參閱在 [Windows 虛擬機器上安裝 Guest Introspection 精簡型代理程式](#)。
 - 請參閱[安裝 Linux 精簡型代理程式以進行網路自我檢查](#)。

在 Windows 虛擬機器上安裝 Guest Introspection 精簡型代理程式

若要使用 Guest Introspection 安全性解決方案來保護虛擬機器，您必須在虛擬機器上安裝 Guest Introspection 精簡型代理程式 (也稱為 Guest Introspection 驅動程式)。Guest Introspection 驅動程式隨附於 VMware Tools for Windows，但並非預設安裝的一部分。若要在 Windows 虛擬機器上安裝 Guest Introspection，您必須執行自訂安裝，並選取驅動程式。

已安裝 Guest Introspection 驅動程式的 Windows 虛擬機器在已安裝安全性解決方案的 ESXi 主機上啟動時自動受到保護。受保護的虛擬機器在經過關機並重新啟動後仍會受到安全性保護，甚至在使用 vMotion 移至已安裝安全性解決方案的其他 ESXi 主機後也是如此。

- 如果您使用 vSphere 6.0，請參閱下列有關於安裝 VMware Tools 的指示：[在 Windows 虛擬機器中手動安裝或升級 VMware Tools](#)。
- 如果您使用 vSphere 6.5，請參閱下列有關於安裝 VMware Tools 的指示：<https://www.vmware.com/support/pubs/vmware-tools-pubs.html>。

必要條件

確定客體虛擬機器已安裝支援的 Windows 版本。NSX Guest Introspection 支援下列 Windows 作業系統：

- Windows XP SP3 及更高版本 (32 位元)
- Windows Vista (32 位元)
- Windows 7 (32/64 位元)
- Windows 8 (32/64 位元)

- Windows 8.1 (32/64) (vSphere 6.0 及更新版本)
- Windows 10
- Windows 2003 SP2 及更高版本 (32/64 位元)
- Windows 2003 R2 (32/64 位元)
- Windows 2008 (32/64 位元)
- Windows 2008 R2 (64 位元)
- Win2012 (64)
- Win2012 R2 (64) (vSphere 6.0 及更新版本)

程序

- 1 依照您 vSphere 版本適用的指示，開始進行 VMware Tools 安裝。選取自訂安裝。
- 2 展開 [VMCI 驅動程式] 區段。
可用的選項視 VMware Tools 的版本而有所不同。
- 3 選取要安裝在虛擬機器上的驅動程式。

驅動程式	說明
vShield Endpoint 驅動程式	安裝檔案自我檢查 (vsepflt) 和網路自我檢查 (vnetflt) 驅動程式。
Guest Introspection 驅動程式	安裝檔案自我檢查 (vsepflt) 和網路自我檢查 (vnetflt) 驅動程式。
NSX File Introspection 驅動程式和 NSX Network Introspection 驅動程式	選取 NSX File Introspection 驅動程式以安裝 vsepflt。 選擇性地選取 NSX Network Introspection 驅動程式以安裝 vnetflt (在 Windows 10 或更新版本上為 vnetWFP)。
備註 只有在使用身分識別防火牆或端點監控功能時，才應選取 NSX Network Introspection 驅動程式。	

- 4 在您要新增的驅動程式旁的下拉式功能表中，選取 [此功能安裝在本機硬碟上]。
- 5 請依照程序中的剩餘步驟操作。

後續步驟

以管理權限使用 `fltmc` 命令確認精簡型代理程式正在執行中。輸出中的 [篩選器名稱] 資料行會列出具有 `vsepflt` 項目的精簡型代理程式。

在 Linux 虛擬機器上安裝 Guest Introspection 精簡型代理程式

Guest Introspection 在 Linux 中僅支援將檔案自我檢查用於防毒。若要使用 Guest Introspection 安全性解決方案來保護 Linux 虛擬機器，您必須安裝 Guest Introspection 精簡型代理程式。

Linux 精簡型代理程式可作為作業系統特定套件 (Osp) 的一部分。這些套件由 VMware 套件入口網站主控。企業或安全管理員 (非 NSX 管理員) 可將代理程式安裝在 NSX 以外的客體虛擬機器上。

VMware Tools 不一定要安裝。

請根據您的 Linux 作業系統，使用根權限執行下列步驟：

必要條件

- 確定客體虛擬機器已安裝支援的 Linux 版本。
 - Red Hat Enterprise Linux (RHEL) 7.4 (64 位元) GA
 - SUSE Linux Enterprise Server (SLES) 12 (64 位元) GA
 - Ubuntu 16.04.5 LTS (64 位元) GA
 - CentOS 7.4 GA
- 確認已在 Linux 虛擬機器上安裝 GLib 2.0。

程序**1 針對 Ubuntu 系統**

- a 使用下列命令取得並匯入 VMware 封裝公開金鑰。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 `/etc/apt/sources.list.d` 下，建立名為 `vmware.list` 檔案的新檔案。
- c 以下列內容編輯檔案：

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d 安裝套件。

```
apt-get update
apt-get install vmware-nsx-gi-file
```

2 針對 RHEL7 系統

- a 使用下列命令取得並匯入 VMware 封裝公開金鑰。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 `/etc/yum.repos.d` 下，建立名為 `vmware.repo` 檔案的新檔案。
- c 以下列內容編輯檔案：

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```


3 安裝套件。

```
yum install vmware-nsx-gi-file
```

4 針對 SLES 系統

- a 使用下列命令取得並匯入 VMware 封裝公開金鑰。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 新增下列存放庫：

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c 安裝套件。

```
zypper install vmware-nsx-gi-file
```

5 針對 CentOS 系統

- a 使用下列命令取得並匯入 VMware 封裝公開金鑰。

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 在 /etc/yum.repos.d 下，建立名為 `vmware.repo` 檔案的新檔案。

- c 以下列內容編輯檔案：

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

後續步驟

以管理權限使用服務 `vsepd status` 命令確認精簡型代理程式正在執行中。其狀態必須為執行中。

安裝 Linux 精簡型代理程式以進行網路自我檢查

安裝 Linux 精簡型代理程式以自我檢查網路流量。

重要 若要防範客體虛擬機器遭病毒入侵，您不需要安裝 Linux 精簡型代理程式以進行網路自我檢查。

用來自我檢查網路流量的 Linux 精簡型代理程式驅動程式取決於開放原始碼驅動程式。

必要條件

安裝下列套件：

- glib2
- libnetfilter-contrack3/ libnetfilter-contrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

程序

1 若要安裝 Guest Introspection 所提供的開放原始碼驅動程式。

a 新增下列 URL 作為您作業系統的基底 URL。

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

b 匯入 VMware 封裝金鑰。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

c 更新存放庫並安裝開放原始碼驅動程式。

```
apt-get install Guest-Introspection-for-VMware-NSX
```

2 安裝用來自檢檔案和或網路流量的 Linux 精簡型代理程式。

- 若要安裝檔案和網路自我檢查套件，請在步驟 c 中選取 **vmware-nsx-gi** 套件。

- 若要安裝網路自我檢查套件，請在步驟 c 中選取 **vmware-nsx-gi-net** 套件。

a 新增下列 URL 作為您作業系統的基底 URL。

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

b 匯入 VMware 封裝金鑰。

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

c 安裝其中一個驅動程式。

```
vmware-nsx-gi
vmware-nsx-gi-net
```

支援的軟體

Guest Introspection 可與軟體的特定版本互通。

VMware Tools

支援 VMware Tools 10.3.10 版本。

查看 VMware Tools 與 NSX-T 之間的互通性。請參閱 [VMware 產品互通性對照表](#)。

支援的作業系統

僅支援 Microsoft Windows 作業系統。

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server

支援的主機

對於支援的 ESXi 主機，請參閱 [《VMware 產品互通性對照表》](#)。

建立具有 Guest Introspection 合作夥伴管理員角色的使用者

指派具有在 NSX-T Data Center 中可用之 Guest Introspection 合作夥伴管理員角色的使用者。

附註：建議由與 Guest Introspection 合作夥伴管理員角色相關聯的使用者來登錄合作夥伴服務，以避免發生任何安全性問題。

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 → 使用者 → 角色指派。
- 3 按一下新增。
- 4 選取使用者，並為該使用者指派 **GI 合作夥伴管理員** 角色。

後續步驟

將服務登錄至 NSX-T Data Center。請參閱[將服務登錄至 NSX-T Data Center](#)。

將服務登錄至 NSX-T Data Center

將第三方安全性服務登錄至 NSX-T Data Center。

必要條件

- 確定符合必要條件。請參閱[設定端點保護的必要條件](#)。
- 確定已為 vIDM 使用者指派 GI 合作夥伴管理員角色。此角色會用來向 NSX-T Data Center 登錄服務。

程序

- 1 使用 GI 合作夥伴管理員權限登入合作夥伴主控台。
- 2 使用 NSX-T Data Center 登錄服務、廠商範本，並設定合作夥伴解決方案。請參閱合作夥伴說明文件。

後續步驟

檢視合作夥伴服務的目錄。請參閱[檢視合作夥伴服務目錄](#)。

檢視合作夥伴服務目錄

[目錄] 頁面會顯示向 NSX-T Data Center 登錄的所有合作夥伴和及其服務。

必要條件

- 合作夥伴向 NSX-T Data Center 登錄服務。
- 將在叢集上部署服務。

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**系統 > 服務部署 > 目錄**。
- 3 在服務上按一下**檢視**。[部署] 頁面會顯示有關服務的詳細資料，例如部署狀態、網路詳細資料、叢集詳細資料等。

後續步驟

部署服務。請參閱[部署服務](#)。

部署服務

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。

在叢集中的所有 NSX-T Data Center 主機上部署執行合作夥伴安全性引擎的合作夥伴服務虛擬機器。vSphere ESX Agency Manager (EAM) 服務用於在每台主機上部署合作夥伴服務虛擬機器。部署 SVM 後，您可以建立 SVM 用來保護客體虛擬機器的原則規則。

必要條件

- 所有主機都由 vCenter Server 管理。
- 合作夥伴服務已向 NSX-T Data Center 登錄，並且已可供部署。
- NSX-T Data Center 管理員可以存取合作夥伴服務和廠商範本。
- 服務虛擬機器與合作夥伴 Service Manager (主控台) 雙方必須能夠在管理網路層級彼此通訊。
- 將主機準備好做為 NSX-T Data Center 傳輸節點：
 - 建立傳輸區域。
 - 為通道端點 IP 位址建立 IP 集區。
 - 建立上行設定檔。
 - 新增傳輸節點設定檔，以準備好叢集來自動部署 NSX-T Data Center 傳輸節點。
 - 設定獨立主機或受管理的主機。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 移至**系統索引**標籤，然後按一下**服務部署**。
- 3 按一下**部署**，然後按一下**部署服務**。
- 4 輸入服務部署名稱。
- 5 在 [計算管理程式] 欄位中，選取要部署服務之 vCenter Server 上的計算資源。
- 6 在 [叢集] 欄位中，選取必須部署服務的叢集。
- 7 在 [資料存放區] 下拉式功能表中，您可以：
 - a 選取資料存放區做為服務虛擬機器的存放庫。
 - b 選取**在主機上設定**。這個設定表示您不需要在此精靈中選取資料存放區和連接埠群組。您可以在 vCenter Server 中的 EAM 上直接設定代理程式設定，來指向要用於服務部署的特定資料存放區和連接埠群組。繼續執行步驟 11。

若要瞭解如何設定 EAM，請參閱 vSphere 說明文件。

- 8 在 [網路] 資料行中按一下**設定**，然後透過選取 DHCP 或靜態 IP 位址類型、控制網路和資料網路來進入 [管理網路] 介面。
- 9 在 [部署規格] 欄位中，選取要在叢集主機上部署之服務虛擬機器的服務和構成要素。可以有多個服務可供部署。
- 10 在 [部署範本] 欄位中選取廠商範本，其中包含的屬性可保護您要在客體虛擬機器群組上執行的工作負載。
- 11 按一下**儲存**。

結果

將新主機新增至叢集後，EAM 會自動在新主機上部署服務虛擬機器。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 NSX Manager 使用者介面中檢視狀態。當狀態變為部署成功時，代表已在主機上成功部署服務。

若要從叢集移除主機，請先將其置於維護模式。然後，選取將客體虛擬機器移轉至其他主機的選項，以完成移轉。

後續步驟

瞭解主機上部署之服務執行個體的部署詳細資料和健全狀況狀態。請參閱[檢視服務執行個體詳細資料](#)。

檢視服務執行個體詳細資料

瞭解在叢集的成員主機上部署的服務執行個體的部署詳細資料和健全狀況狀態。

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 **系統 > 服務部署 > 服務執行個體**。
- 3 從 [合作夥伴服務] 下拉式功能表中，選取合作夥伴服務以檢視與服務執行個體相關的詳細資料。

表 10-9.

欄位	說明
服務執行個體名稱	用於識別特定主機上的服務執行個體的唯一識別碼。
服務部署名稱	用於識別服務定義的唯一識別碼
已部署至	主機 IP 位址
部署模式	叢集或獨立
部署狀態	[開啟] 狀態，判定部署成功
健全狀況狀態	透過 NSX-T Data Center 成功實現下列參數時，健全狀況狀態為 [開啟]。 <ul style="list-style-type: none"> ■ 解決方案狀態：開啟 ■ NSX-T Data Center Guest Introspection Agent 和 NSX-T Data Center Ops Agent 之間的連線：開啟 ■ 已定義服務虛擬機器通訊協定 ■ 服務虛擬機器與 NSX-T Data Center Guest Introspection Agent 之間的通訊協定相容性

後續步驟

檢視已登錄服務的目錄。請參閱[檢視合作夥伴服務目錄](#)。

啟動服務執行個體

部署服務執行個體之後，必須在 NSX-T Data Center 中實現特定參數，健全狀況狀態才會顯示為 [開啟]。

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 > 服務部署 > 服務執行個體**。
- 3 從 [合作夥伴服務] 下拉式功能表中，選取合作夥伴服務以檢視與服務執行個體相關的詳細資料。
- 4 [健全狀況狀態] 資料行會將服務執行個體的状态顯示為就緒。這表示服務執行個體已準備就緒，可設定用來保護虛擬機器的端點保護原則規則。
- 5 必須在 NSX-T Data Center 中實現下列參數，健全狀況狀態才會變更為啟動。
 - 主機上必須有可用的客體虛擬機器。
 - 必須開啟客體虛擬機器的電源。
 - 必須將端點保護規則套用至客體虛擬機器。
 - 必須使用支援的 VMtools 版本和檔案自我檢查驅動程式設定客體虛擬機器。

後續步驟

新增服務設定檔。請參閱[新增 Endpoint Protection 服務設定檔](#)。

新增 Endpoint Protection 服務設定檔

僅當服務設定檔在 NSX-T Data Center 中可用時，才能實作 Guest Introspection 原則。服務設定檔是從合作夥伴提供的範本建立的。服務設定檔可供管理員透過選擇廠商提供的廠商範本，來為虛擬機器選擇保護層級（「金級」、「銀級」、「白金級」原則）。

例如，廠商可以提供「金級」、「白金級」和「銀級」原則層級。每個建立的設定檔都可能提供不同的工作負載類型。金級服務設定檔提供適用於 PCI 類型工作負載的完整反惡意程式碼保護，而銀級服務設定檔僅提供適用於一般工作負載的基本反惡意程式碼保護。

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**安全性 > Endpoint Protection > 服務設定檔**。
- 3 從 [合作夥伴服務] 欄位中，選取您要為其建立服務設定檔的服務。
- 4 按一下**新增服務設定檔**。
- 5 輸入服務設定檔的名稱，然後選取廠商範本。（選擇性）新增說明和標籤。
- 6 按一下**儲存**。

用於建立服務設定檔的廠商範本識別碼會傳遞到合作夥伴主控台。合作夥伴會儲存廠商範本識別碼，以追蹤受到這些廠商範本保護之客體虛擬機器的使用情況。

結果

建立服務設定檔後，NSX 管理員會建立規則來將服務設定檔與一組虛擬機器相關聯，然後再發佈原則規則。

後續步驟

對需要抵禦惡意程式碼的客體虛擬機器群組套用 Endpoint Protection 原則。

耗用 Guest Introspection 原則

透過建立將服務設定檔與虛擬機器群組相關聯的規則，可以對虛擬機器群組強制執行原則。將規則套用到至虛擬機器群組後，保護功能便會立即開始運作。

Endpoint Protection 原則是合作夥伴提供的一項保護服務，可透過在客體虛擬機器上實作服務設定檔，來保護客體虛擬機器抵禦惡意程式碼。將規則套用到至虛擬機器群組後，該群組中的所有客體虛擬機器都會受到該服務設定檔的保護。當客體虛擬機器上發生檔案存取事件時，GI Thin Agent（執行於每個客體虛擬機器）會收集檔案的內容（檔案屬性、檔案控點和其他內容詳細資料），並將事件通知 SVM。如果 SVM 想要掃描檔案內容，它會使用 EPSec API 程式庫來請求詳細資料。一旦 SVM 判定檔案安全，GI Thin Agent 會允許使用者存取檔案。如果 SVM 回報檔案受到感染，GI Thin Agent 會拒絕使用者存取檔案。

若要實作 Endpoint Protection 原則，請先建立適合特定類型工作負載的網域。然後，透過將虛擬機器群組與服務設定檔 (其定義用來保護虛擬機器的服務和保護層級) 相關聯來定義 EPP 規則。請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

若要在虛擬機器群組上執行安全服務，您必須：

程序

- 1 定義網域，這是裝載了虛擬機器群組和規則的環境。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

- 2 定義形成虛擬機器群組的成員資格準則。
- 3 定義虛擬機器群組的規則。
- 4 發佈規則。

新增及發佈 Endpoint Protection 規則

將原則規則發佈到虛擬機器群組，表示需要使用特定服務設定檔保護關聯的虛擬機器群組。

程序

- 1 在 [原則] 區段中，選取原則。
- 2 按一下 **新增** -> **新增規則**。
- 3 在 [名稱] 資料行中，輸入規則的名稱。
- 4 在 [群組] 資料行中，選取虛擬機器群組。
- 5 在 [服務設定檔] 資料行中，選取向群組中客體虛擬機器提供所需保護層級的服務設定檔。
- 6 按一下 **發佈**。

結果

Endpoint Protection 原則會保護虛擬機器群組。

後續步驟

您可能想要根據不同虛擬機器群組所需的保護類型，來變更規則的順序。請參閱 [Guest Introspection 如何執行 Endpoint Protection 原則](#)

監控端點保護狀態

監控受保護和未受保護虛擬機器的組態狀態、主機代理程式和服務虛擬機器的问题，以及設定了在 VMtools 安裝過程中安裝的檔案自我檢查驅動程式的虛擬機器。

您可以檢視：

- 檢視服務部署狀態。
- 檢視端點保護的組態狀態。

- 檢視為端點保護設定的容量狀態。

檢視服務部署狀態

在 [監控] 儀表板上檢視服務部署詳細資料。

檢視 EPP 原則的全系統狀態。

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 導覽至 **首頁 > 監控 - 儀表板**。
- 3 從下拉式功能表中，按一下 **監控 - 系統**。
- 4 若要檢視系統中各叢集的部署狀態，請導覽至端點保護 Widget，然後按一下環圈圖以檢視成功或失敗的部署。
[服務部署] 頁面會顯示部署詳細資料。

檢視為端點保護設定的容量狀態

檢視端點保護服務的容量狀態。

檢視 EPP 原則的容量狀態。

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 導覽至 **首頁 > 監控 - 儀表板**。
- 3 從下拉式功能表中，按一下 **監控 - 網路與安全性**。
- 4 若要檢視叢集上的 EPP 狀態，請按一下安全性 Widget。
- 5 在 [安全性概觀] 頁面中，按一下 **容量**，然後檢視下列參數的容量狀態。

限制	容量上限	目前的詳細目錄 (已實現)	警告警示	嚴重警示
Distributed Firewall 規則	100,000	2	0%	70% 100%
系統相關防火牆區段	10,000	5	0.05%	70% 100%

- a **全系統端點保護已啟用的主機**：如果受保護的主機數目達到臨界值限制，則在達到對應的臨界值限制時，NSX Manager 會傳送警告警示或嚴重警示。
- b **全系統端點保護已啟用的虛擬機器**：如果受保護的虛擬機器數目達到臨界值限制，則在達到對應的臨界值限制時，NSX Manager 會傳送警告警示或嚴重警示。

備註 您可以為這些參數設定臨界值限制、檢視狀態，以及在這些參數達到設定的臨界值限制時接收警示。

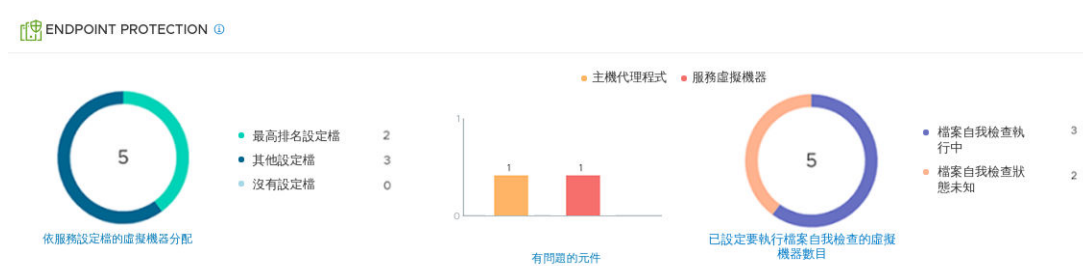
檢視端點保護的組態狀態

檢視端點保護服務的組態狀態。

檢視 EPP 原則的全系統狀態。

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 導覽至 **首頁 > 安全性 > 安全性概觀**。
- 3 若要檢視叢集上的 EPP 狀態，請按一下安全性 Widget。
- 4 在 [安全性概觀] 頁面中，按一下**組態**。



- 5 在 [端點保護] 區段中，檢視：

- a [依服務設定檔的虛擬機器分配] Widget 會顯示：

- 1 最高排名設定檔所保護的虛擬機器數目。最高排名設定檔代表在叢集中保護最多虛擬機器的設定檔。
- 2 受剩餘服務設定檔保護的虛擬機器會分類在 [其他設定檔] 下方。
- 3 未受保護的虛擬機器會分類在 [沒有設定檔] 下方。

[端點保護規則] 頁面會顯示受端點保護原則保護的虛擬機器。

- b [有問題的元件] Widget 會顯示：

- 1 主機：內容多工器的相關問題。
- 2 SVM：服務虛擬機器的相關問題。例如，SVM 狀態為關閉，與客體虛擬機器的 SVM 連線已關閉。

[部署] 頁面上的 [狀態] 資料行會顯示健全狀況問題。

- c [設定要執行檔案自我檢查的虛擬機器數目] Widget 會顯示：

- 1 由檔案自我檢查驅動程式保護的虛擬機器。
- 2 檔案自我檢查驅動程式狀態為未知的虛擬機器。

ESXi Agency Manager (EAM) 會嘗試解決與主機、SVM 和組態錯誤相關的一些問題。請參閱[確保合作夥伴服務在每台主機上正常運作](#)。

新增網域和虛擬機器群組

建立一個網域來代表原則和虛擬機器安全群組所屬的環境。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

程序

- 1 選取**安全性 > Endpoint Protection > 規則**。
- 2 按一下**新增原則**。
- 3 在 [名稱] 資料行中，輸入原則的名稱。
- 4 在 [網域] 欄位中，按一下**預設**來選取網域或建立新網域。
- 5 在 [選取網域] 視窗的底部，按一下**建立新網域**。
- 6 在 [名稱] 資料行中，輸入網域的名稱。
- 7 按一下**儲存**。
- 8 按一下**是**來設定此網域中的群組。
- 9 按一下**新增群組**。
- 10 在 [新增群組] 視窗中，輸入群組的名稱。
- 11 在 [計算成員] 資料行中，選取 [成員]。
- 12 在 [選取成員] 視窗中，設定成員資格準則以便自動選取要加入群組的虛擬機器，或者是手動選取要加入群組的虛擬機器。
- 13 按一下**新增準則**。可以依標籤、作業系統名稱或電腦名稱來定義成員資格準則。
- 14 為虛擬機器加入群組新增所需準則後，請按一下**儲存**，然後按一下**關閉**。
- 15 按一下**儲存**。

後續步驟

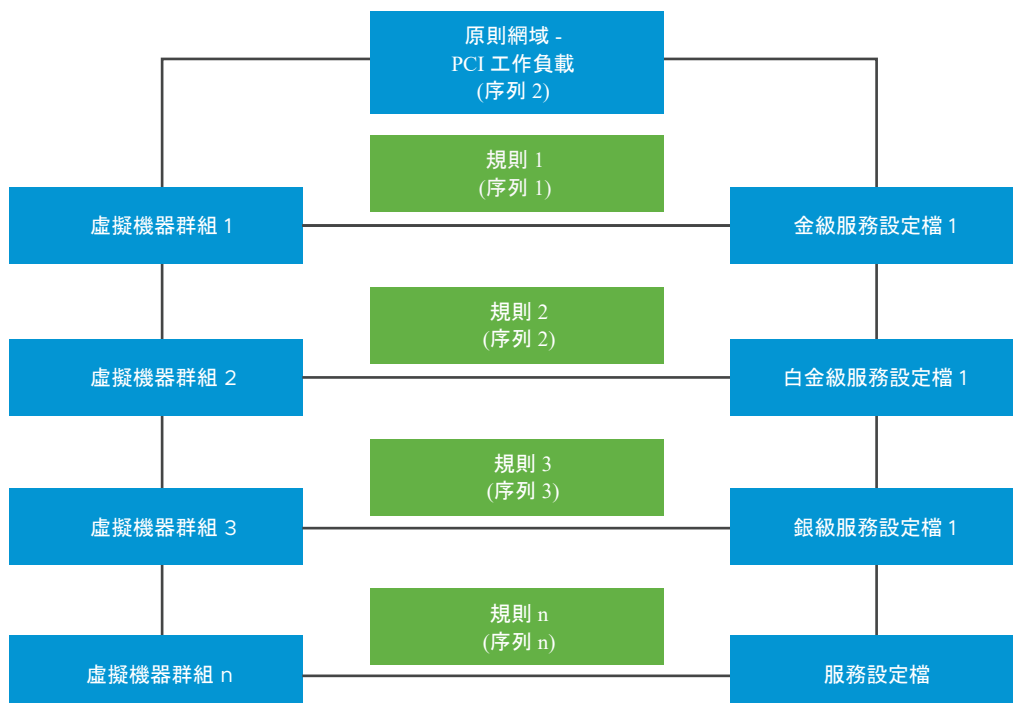
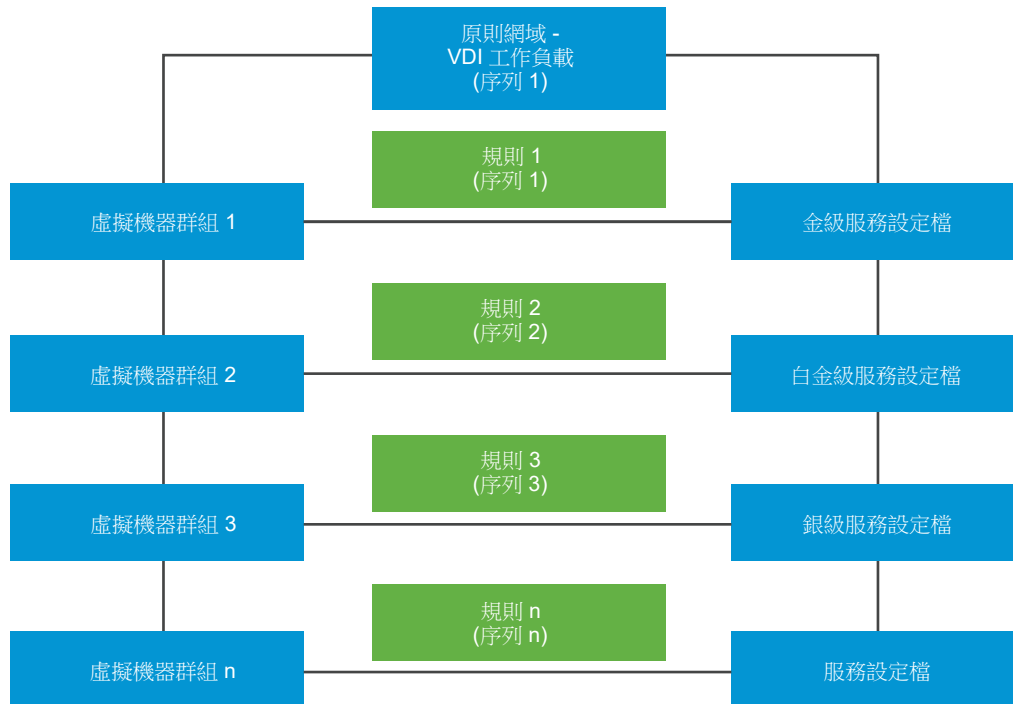
建立並發佈規則。請參閱[新增及發佈 Endpoint Protection 規則](#)。

Guest Introspection 如何執行 Endpoint Protection 原則

Endpoint Protection 原則會以特定順序強制執行。當您設計原則時，請考量與規則及裝載規則之網域相關聯的順序編號。

備註 網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

案例：您的組織會執行許多工作負載，但基於說明目的，我們選擇兩種工作負載，即執行虛擬桌面基礎結構 (VDI) 工作負載的虛擬機器，以及執行支付卡產業資料安全標準 (PCI-DSS) 工作負載的虛擬機器。組織中的一部分員工需要執行遠程桌面存取，虛擬桌面基礎結構 (VDI) 工作負載即由此而來。根據組織所設定的符合性規則，這些 VDI 工作負載可能需要金級保護原則層級，而 PCI-DSS 工作負載需要最高保護層級，也就是白金級層級保護。



由於有兩種工作負載類型，因此會建立兩個原則，分別適用於 VDI 工作負載和伺服器工作負載。在每個原則或區段中，定義網域來反映工作負載類型，並在該區段中定義用於該工作負載的規則。發佈規則以在客體虛擬機器上啟動 GI 服務。GI 內部使用兩個順序編號：原則順序編號及規則順序編號，來決定規則執行的完整順序。每個規則都有兩個目的：決定要保護哪些虛擬機器，以及必須套用哪個保護原則來保護虛擬機器。

若要變更順序，請在 NSX-T Policy Manager 使用者介面中拖曳規則，即可變更其順序。或者，您可以使用 API 來明確指派規則的順序編號。

還可以執行 NSX-T Data Center API 呼叫來手動定義規則，方法是將服務設定檔與虛擬機器群組相關聯，然後宣告規則的順序編號。如需有關 API 和參數的詳細資料，請參閱《NSX-T Data Center API 指南》。執行服務組態 API 呼叫，將設定檔套用至實體，例如虛擬機器群組等。

表 10-10. NSX-T Data Center API 用於定義將服務設定檔套用至虛擬機器群組的規則

API	詳細資料
取得所有服務組態詳細資料。	<p>GET /api/v1/service-configs</p> <p>此服務組態 API 會傳回下列項目的詳細資料：套用至虛擬機器群組的服務設定檔、所保護的虛擬機器群組，以及決定規則優先順序的順序或優先順序編號。</p>
建立服務組態。	<p>POST /api/v1/service-configs</p> <p>此服務組態 API 會取得下列項目的輸入參數：服務設定檔、所保護的虛擬機器群組，以及必須套用至規則的順序或優先順序編號。</p>
刪除服務組態。	<p>DELETE /api/v1/service-configs/<config-set-id></p> <p>此服務組態 API 會刪除套用至虛擬機器群組的組態。</p>
取得特定組態的詳細資料。	<p>GET /api/v1/service-configs/<config-set-id></p> <p>取得特定組態的詳細資料</p>
更新服務組態。	<p>PUT /api/v1/service-configs/<config-set-id></p> <p>更新服務組態。</p>
取得有效設定檔。	<p>GET /api/v1/service-configs/effective-profiles?resource_id=<resource-id>&resource_type=<resource-type></p> <p>此服務組態 API 僅會傳回套用至特定虛擬機器群組的設定檔。</p>

請遵循以下建議來有效率地管理規則：

- 為其規則必須先執行的原則設定較高的順序編號。您可以從使用者介面中拖曳原則來變更其優先順序。
- 同樣地，為每個原則中的規則設定較高的順序編號。

- 根據您需要的規則數量而定，可以將規則以 2、3、4 甚或 10 的倍數來間隔放置。如此，兩個間隔 10 個位次的連續規則，可讓您有更多彈性來重新排列規則的順序，而不用變更所有規則的順序編號。例如，如果您不打算定義許多規則，則您可以選擇將規則以 10 個位次的間隔放置。如此，規則 1 的順序編號為 1，規則 2 的順序編號為 10，規則 3 的順序編號為 20，依此類推。這項建議提供高效管理規則的彈性，讓您無需重新排列所有規則的順序。

在系統內部，Guest Introspection 會以下列方式排列這些原則規則的順序。

Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (1001)
- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (1010)
- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (1020)
- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (1030)

Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1 ↔ Service Profile ↔ Sequence Number 1 (2001)
- Rule 2 : Group 1 ↔ Service Profile ↔ Sequence Number 10 (2010)
- Rule 3 : Group 1 ↔ Service Profile ↔ Sequence Number 20 (2020)
- Rule 4 : Group 1 ↔ Service Profile ↔ Sequence Number 30 (2030)

根據上述順序編號，GI 會先執行原則 1 的規則，然後再執行原則 2 的規則。

但有時會發生預定規則不適用於虛擬機器群組或虛擬機器的情況。此時必須解決這些衝突，才能套用所需的原則保護層級。

確保合作夥伴服務在每台主機上正常運作

合作夥伴服務虛擬機器必須正常運作，才能保護客體虛擬機器抵禦惡意程式碼。

在每台主機上，下列服務或程序必須已啟動並在執行中：

- ESXi Agency Manager (EAM) 服務必須已啟動並在執行中。為了進行確認，必須能夠存取下列 URL。

```
https://<vCenter_Server_IP_Address>/eam/mob
```

執行命令以確認 ESXi Agency Manager 是否處於線上狀態。

```
root> service-control --status vmware-eam
```

- 由 NSX-T Data Center 自動建立之與 SVM 相關的連接埠群組不會遭到刪除，因為系統需要這些連接埠群組來確保 SVM 持續保護客體虛擬機器。

```
https://<vCenter_Server_IP_Address>/ui
```

在 vCenter Server 中，移至虛擬機器，按一下**網路**索引標籤，然後檢查是否有列出 **vm-service-vshield-pg**。

- 內容多工器 (MUX) 服務已啟動並在執行中。檢查主機上的 **nsx-context-mux** VIB 已啟動並在執行中。
- 管理介面：NSX-T Data Center 藉以與合作夥伴服務主控台進行通訊的 SVM 介面。
- 控制介面：促成 MUX 與 SVM 之間通訊的 SVM 介面。已建立將 SVM 與 MUX 連線的連接埠群組。必須有此介面和連接埠群組，合作夥伴服務才能正常運作。

ESXi Agency Manager 問題

此資料表列出可使用 NSX Manager 使用者介面上的 [解決] 按鈕來解決的 ESXi Agency Manager 問題。它會將錯誤詳細資料通知 NSX Manager。

表 10-11. ESXi Agency Manager 問題

問題	類別	說明
無法存取代理程式 OVF	未部署虛擬機器	代理程式虛擬機器應部署在主機上，但無法部署代理程式虛擬機器，因為 ESXi Agent Manager 無法存取代理程式 OVF 套件。這是因為提供 OVF 套件的 Web 伺服器已關閉。Web 伺服器通常是建立代理機構之解決方案的內部元件。
主機版本不相容	未部署虛擬機器	代理程式虛擬機器應部署在主機上，但無法部署代理程式，因為它與主機不相容。
資源不足	未部署虛擬機器	代理程式虛擬機器應部署在主機上，但無法部署代理程式虛擬機器，因為主機沒有足夠的可用 CPU 或記憶體資源。
空間不足	未部署虛擬機器	代理程式虛擬機器應部署在主機上，但無法部署代理程式虛擬機器，因為主機的代理程式資料存放區沒有足夠的可用空間。
沒有代理程式虛擬機器網路	未部署虛擬機器	代理程式虛擬機器應部署在主機上，但無法部署代理程式，因為主機上未設定代理程式網路。
OVF 格式無效	未部署虛擬機器	代理程式虛擬機器應佈建在主機上，但佈建失敗，因為佈建 OVF 套件失敗。必須將提供 OVF 套件的解決方案升級或修補，來為代理程式虛擬機器提供有效的 OVF 套件，佈建才有可能成功。
缺少代理程式 IP 集區	虛擬機器已關閉電源	代理程式虛擬機器應開啟電源，但代理程式虛擬機器已關閉電源，因為代理程式的虛擬機器網路上未定義任何 IP 位址。

表 10-11. ESXi Agency Manager 問題 (續)

沒有代理程式虛擬機器資料存放區	虛擬機器已關閉電源	代理程式虛擬機器應部署在主機上，但無法部署代理程式，因為主機上未設定代理程式資料存放區。
沒有自訂代理程式虛擬機器網路	沒有代理程式虛擬機器網路	代理程式虛擬機器應部署在主機上，但無法部署代理程式，因為主機上未設定代理程式網路。主機必須新增至自訂代理程式虛擬機器網路中列出的其中一個網路。
沒有自訂代理程式虛擬機器資料存放區	沒有代理程式虛擬機器資料存放區	代理程式虛擬機器應部署在主機上，但無法部署代理程式，因為主機上未設定代理程式資料存放區。主機必須新增至自訂代理程式虛擬機器資料存放區中列出的其中一個資料存放區。
孤立的代理機構	代理機構問題	建立代理機構的解決方案不再向 vCenter Server 登錄。
孤立的 DvFilter 交換器	主機問題	主機上存在 dvFilter 交換器，但主機上沒有任何代理程式依賴於 dvFilter。當主機因為代理機構組態變更而中斷連線時，通常會發生此情況。
未知代理程式虛擬機器	主機問題	在 vCenter Server 詳細目錄中找到的代理程式虛擬機器不屬於此 vSphere ESX Agent Manager 伺服器執行個體中的任何代理機構。
OVF 內容無效	虛擬機器問題	代理程式虛擬機器必須開啟電源，但 OVF 內容遺失或具有無效的值。
虛擬機器已損毀	虛擬機器問題	代理程式虛擬機器已損毀。
虛擬機器已孤立	虛擬機器問題	主機上存在代理程式虛擬機器，但主機不再屬於代理機構的範圍。當主機因為代理機構組態變更而中斷連線時，通常會發生此情況。
虛擬機器已部署	虛擬機器問題	代理程式虛擬機器應從主機中移除，但代理程式虛擬機器尚未移除。vSphere ESX Agent Manager 無法移除代理程式虛擬機器的特定原因包括：主機處於維護模式、已關閉電源或處於待命模式。
虛擬機器已關閉電源	虛擬機器問題	代理程式虛擬機器應開啟電源，但代理程式虛擬機器已關閉電源。
虛擬機器已開啟電源	虛擬機器問題	代理程式虛擬機器應關閉電源，但代理程式虛擬機器已開啟電源。
虛擬機器已暫停	虛擬機器問題	代理程式虛擬機器應開啟電源，但代理程式虛擬機器已暫停。
虛擬機器位於錯誤的資料夾中	虛擬機器問題	代理程式虛擬機器應位於指定的代理程式虛擬機器資料夾中，但卻在不同的資料夾中找到。

表 10-11. ESXi Agent Manager 問題 (續)

虛擬機器位於錯誤的資源集區中	虛擬機器問題	代理程式虛擬機器應位於指定的代理程式虛擬機器資源集區中，但卻在不同的資源集區中找到。
未部署虛擬機器	代理程式問題	代理程式虛擬機器應部署在主機上，但尚未部署代理程式虛擬機器。ESXi Agent Manager 無法部署代理程式的特定原因包括：無法存取代理程式的 OVF 套件或缺少主機組態。從主機中明確刪除代理程式虛擬機器時，也可能發生此問題。

接著，為虛擬機器群組設定 Endpoint Protection。請參閱[設定 Endpoint Protection](#)。

端點原則衝突解決

假設有一個案例：有兩個原則網域，每個都包含多個規則。身為管理員，您並非總是能夠確定哪些虛擬機器會取得群組的成員資格，因為虛擬機器群組是根據動態成員資格準則 (例如作業系統名稱、電腦名稱、使用者、標記) 來與群組相關聯。

備註 網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

在下列情況下，將會出現衝突：

- 虛擬機器屬於兩個群組，而每個群組受不同的設定檔保護。
- 一個合作夥伴服務虛擬機器與多個服務設定檔相關聯。
- 客體虛擬機器執行未預期的規則，或規則未在虛擬機器群組上執行。
- 未指派順序編號給原則規則或網域。

表 10-12. 解決原則衝突

案例	預期的 Endpoint Protection 流量	解決方案
當虛擬機器取得多個群組的成員資格時，每個群組受不同類型的服務設定檔保護。 預期的保護未套用至虛擬機器。	使用成員資格準則建立虛擬機器群組，代表虛擬機器會以動態方式新增到群組。在此情況下，同一個虛擬機器可以屬於多個群組。您無法預先決定虛擬機器將屬於哪一個群組，因為成員資格準則會以動態方式將虛擬機器填入群組中。 將虛擬機器 1 視為屬於群組 1 和群組 2。 <ul style="list-style-type: none"> 規則 1: 群組 1 (按作業系統名稱) 套用金級服務設定檔且順序編號為 1 規則 2: 群組 2 (按標籤) 套用白金級服務設定檔且順序編號為 10 Endpoint Protection 原則會在虛擬機器 1 上執行金級服務設定檔，但不會在虛擬機器 1 上執行白金級服務設定檔。	變更規則 2 的順序編號，使其先於規則 1 執行。 <ul style="list-style-type: none"> 在 NSX-T Policy Manager 使用者介面上，於規則清單中將規則 2 拖曳到規則 1 之前。 使用 NSX-T Policy Manager API，手動為規則 2 新增較高的順序編號。
當一個規則關聯同一個服務設定檔來保護兩個虛擬機器群組時，Endpoint Protection 不會在第二個虛擬機器群組上執行規則。	Endpoint Protection 只會在虛擬機器上執行第一個服務設定檔，因為同一個服務設定檔無法再次套用到跨原則或網域的任何其他規則。 將虛擬機器 1 視為屬於群組 1 和群組 2。 規則 1: 群組 1 (按作業系統名稱) 套用金級服務設定檔 規則 2: 群組 2 (按標籤) 套用金級服務設定檔	<ul style="list-style-type: none"> 將群組 2 新增至規則 1。(規則 1: 群組 1 和群組 2 均套用設定檔 1)

隔離虛擬機器

對虛擬機器群組套用規則後，根據合作夥伴所設定的保護層級與標籤，可能會有虛擬機器被識別為受到感染而需要隔離。

合作夥伴會使用 API，透過 `virus_found=true` 標籤來標記受到感染的虛擬機器。受影響的虛擬機器會附加 `virus_found=true` 標籤。

做為管理員，您可以根據值為 `virus_found=true` 的標籤建立預先定義的隔離群組，以便受到感染的虛擬機器被標記時即會填入群組。做為管理員，您可以選擇為隔離群組設定特定的防火牆規則。您可以為隔離群組設定防火牆規則。例如，您可以選擇封鎖所有進出隔離群組的流量。

確認服務執行個體的健全狀況狀態

服務執行個體的健全狀況狀態取決於多種因素：合作夥伴解決方案的狀態、Guest Introspection 代理程式 (內容多工器) 和內容引擎 (Ops Agent) 之間的連線、Guest Introspection 代理程式資訊的可用性、NSX Manager 的 SVM 通訊協定資訊。

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 **系統 > 服務部署 > 服務執行個體**。

- 3 在 [健全狀況狀態] 資料行中，按一下  瞭解服務執行個體的健全狀況。

表 10-13. 第三方服務執行個體的健全狀況狀態

參數	說明
健全狀況狀態接收時間	當 NSX Manager 接收服務執行個體的健全狀況狀態詳細資料時的最新時間戳記。
解決方案狀態	在 SVM 上執行的合作夥伴解決方案的狀態。狀態為 [開啟] 表示合作夥伴解決方案正在正常執行。
NSX-T Data Center Guest Introspection 代理程式和 NSX-T Data Center Ops Agent 之間的連線	當 NSX-T Data Center Guest Introspection 代理程式 (內容多工器) 與 Ops Agent (包括內容引擎) 連線時，狀態為 [開啟]。內容多工器會將 SVM 的健全狀況資訊轉送到內容引擎。他們還會相互共用 SVM-VM 組態以瞭解哪些客體虛擬機器受到 SVM 保護。
服務虛擬機器通訊協定版本	傳輸通訊協定版本供內部使用對問題進行疑難排解。
NSX-T Data Center Guest Introspection 代理程式資訊	代表 NSX-T Data Center Guest Introspection 代理程式與 SVM 之間的通訊協定版本相容性。

- 4 如果健全狀況狀態為開啟 (狀態顯示為綠色)，並且合作夥伴主控台將所有客體虛擬機器顯示為受保護，則服務執行個體的健全狀況狀態為開啟。
- 5 如果健全狀況狀態為開啟 (狀態顯示為綠色)，但合作夥伴主控台顯示客體虛擬機器處於不受保護狀態，則執行下列步驟：
- 請連絡 VMware 支援以解決此問題。服務執行個體的健全狀況狀態可能為 [關閉]，而 NSX Manager 使用者介面無法正確地反映此狀態。
- 6 如果健全狀況狀態為關閉 (狀態顯示為紅色)，則確定服務執行個體健全狀況的一或多個因素會關閉。

表 10-14. 疑難排解健全狀況狀態

健全狀況狀態屬性	解決方案
解決方案狀態為關閉或不適用。	<ol style="list-style-type: none"> 1 確認服務部署狀態為開啟 (綠色)。如果遇到錯誤，請參閱 確保合作夥伴服務在每台主機上正常運作。 2 確保受影響主機中至少有一個客體虛擬機器受端點保護原則保護。 3 從合作夥伴主控台，確認解決方案服務正在主機上的 SVM 上執行。請參閱合作夥伴說明文件以取得更多詳細資料。 4 如果上述步驟均未解決此問題，請連絡 VMware 支援。
NSX-T Data Center Guest Introspection 代理程式和 NSX-T Data Center Ops Agent 之間的連線已關閉。	<ol style="list-style-type: none"> 1 確認服務部署狀態為開啟 (綠色)。如果遇到錯誤，請參閱 確保合作夥伴服務在每台主機上正常運作。 2 確保受影響主機中至少有一個客體虛擬機器受端點保護原則保護。 3 從合作夥伴主控台，確認解決方案服務正在主機上的 SVM 上執行。請參閱合作夥伴說明文件以取得更多詳細資料。 4 如果上述步驟均未解決此問題，請連絡 VMware 支援。

表 10-14. 疑難排解健全狀況狀態 (續)

健全狀況狀態屬性	解決方案
服務虛擬機器通訊協定版本為無法使用。	<ol style="list-style-type: none"> 1 確認服務部署狀態為開啟 (綠色)。如果遇到錯誤，請參閱確保合作夥伴服務在每台主機上正常運作。 2 確保受影響主機中至少有一個客體虛擬機器受端點保護原則保護。 3 從合作夥伴主控台，確認解決方案服務正在主機上的 SVM 上執行。請參閱合作夥伴說明文件以取得更多詳細資料。 4 如果上述步驟均未解決此問題，請連絡 VMware 支援。
NSX-T Data Center Guest Introspection 代理程式資訊為無法使用。	請連絡 VMware 支援。

刪除合作夥伴服務

若要刪除合作夥伴服務，請執行 API 呼叫。在執行 API 呼叫來刪除主機上部署的合作夥伴服務或 SVM 之前，必須先從 NSX Manager 使用者介面執行下列動作。

若要刪除合作夥伴服務：

程序

- 1 移除已套用至主機上執行之虛擬機器群組的 EPP 規則。
- 2 移除已套用至虛擬機器群組的服務設定檔保護。
- 3 若要移除將 SVM 與合作夥伴 Service Manager 繫結的解決方案，請執行下列 API 呼叫。

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/{{service_id}}/solution-configs/<solution-config-id>
```

- 4 若要刪除服務部署，請執行下列 API 呼叫。

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/<service-id>/service-deployments/<service-deployment-id>
```

如需有關 API 參數的詳細資訊，請參閱《NSX-T Data Center API 指南》。

您可以為 NSX-T Data Center 詳細目錄設定服務、群組、網域和內容設定檔。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

本章節討論下列主題：

- [新增網域](#)
- [新增服務](#)
- [新增群組](#)
- [新增內容設定檔](#)

新增網域

網域是具有一般業務目標之工作負載和物件的邏輯集合。透過建立網域，您可以更輕鬆地管理環境中的物件。

備註 網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。

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**詳細目錄 > 網域**。
- 3 按一下**新增網域**。
- 4 輸入名稱和 (選用) 說明。
- 5 按一下**儲存**並繼續設定群組。
- 6 按一下**新增群組**。
- 7 輸入名稱。
- 8 按一下**設定成員**。

您可以使用下列一或多種方法來選取成員：

- 指定成員準則
- 選取成員

- 輸入 IP 位址或 MAC 位址
- 選取 AD 群組

- 9 按一下**新增準則**以透過指定成員資格準則來選取成員。
- 10 按一下**成員索引標籤**以選取物件。
- 11 按一下 **IP/MAC 位址**索引標籤以輸入 IP 位址或 MAC 位址。
- 12 按一下 **AD 群組**索引標籤以選取 AD 群組。
- 13 按一下**儲存**。

新增服務

您可以設定服務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。

您也可以使用服務，在防火牆規則中允許或封鎖特定的流量類型。建立服務後即無法變更類型。某些服務是預先定義的，因此無法修改或刪除。

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**詳細目錄 > 服務**。
- 3 按一下**新增服務**。
- 4 輸入名稱。
- 5 按一下**設定服務項目**。從清單中選取預先定義的服務，或按一下**新增服務項目**。
- 6 針對新服務，請選取服務類型並指定其他內容。
可用類型包括 **IP**、**IGMP**、**ICMPv4**、**ICMPv6**、**ALG**、**TCP**、**UDP** 和**乙太**。
- 7 按一下**儲存**。
- 8 (選擇性) 輸入範圍。
- 9 按一下**儲存**。

新增群組

群組包含以靜態方式和動態方式新增，並且可用做防火牆規則的來源和目的地欄位的不同物件。

群組可設定為包含虛擬機器、IP 集合、MAC 集合、邏輯連接埠、邏輯交換器、AD 使用者群組以及其他巢狀群組的組合。群組的動態納入方式可以根據標籤、機器名稱、作業系統名稱或電腦名稱來進行。

以單一識別碼為基礎的群組可用於一個防火牆規則中。如果需要在來源使用以 IP 和識別碼為基礎的群組，請建立分別兩個防火牆規則。

僅由 IP 位址、MAC 位址或 Active Directory 群組組成的群組，無法在**套用至**文字方塊中使用。

備註 在 vCenter Server 中新增或移除主機時，主機上的虛擬機器的外部識別碼會發生變更。如果虛擬機器是某個群組的靜態成員，當虛擬機器的外部識別碼發生變更時，NSX Manager UI 就不再將虛擬機器顯示為該群組的成員。不過，列出群組的 API 仍會顯示該群組包含虛擬機器，且虛擬機器具有其原始的外部識別碼。如果您將虛擬機器新增為某個群組的靜態成員，當虛擬機器的外部識別碼發生變更時，您必須使用其新的外部識別碼重新新增虛擬機器。您也可以使用動態成員資格準則，以避免發生此問題。

程序

1 選取導覽面板中的**詳細目錄 > 群組**。

2 按一下**新增群組**。

3 輸入群組名稱。

4 (必要) 從下拉式功能表中選擇網域，或使用預設網域。網域是一種邏輯結構，代表一個安全性區域以及所有規則和群組。預設網域代表整個 NSX 環境。

請注意，網域物件是 NSX-T Data Center 2.4 中的實驗性功能，未在 NSX-T Data Center 2.4.1 中提供。在 NSX-T Data Center 2.4.1 中，不需建立任何網域。

5 (選擇性) 按一下**設定成員**。

對於每個成員資格準則，您最多可以指定五個規則，與邏輯 AND 運算子組合使用。可用成員準則可套用至下列項目：

- **邏輯連接埠** - 可以指定標籤和選用範圍。
- **邏輯交換器** - 可以指定標籤和選用範圍。
- **虛擬機器** - 可以指定等於、包含、開頭為、結尾為或不等於某個特定字串的名稱、標籤、電腦作業系統名稱或電腦名稱。
- **傳輸節點** - 可以指定等於某個 Edge 節點或主機節點的節點類型。

6 (選擇性) 按一下**成員**以選取成員。

可用成員類型為：

- **群組**
- **區段**
- **區段連接埠**
- **虛擬網路介面**
- **虛擬機器**

7 按一下 **IP/MAC 位址**以新增 IP 位址和 MAC 位址做為群組成員。

8 按一下 **AD 群組**以新增 Active Directory 群組。具有 Active Directory 成員的群組可以在身分識別防火牆的分散式防火牆規則的來源或目的地欄位中使用，並且必須是群組中的唯一成員。例如，不能有同時將 ADGroup 和 IPSet 做為成員的群組。

9 按一下套用。

隨即列出群組，您可以檢視成員及使用群組的位置。

新增內容設定檔

內容設定檔會使用第 7 層應用程式識別碼屬性，以供在 Distributed Firewall 規則中使用。定義好內容設定檔後，即可在一或多個 Distributed Firewall 規則中使用內容設定檔。

在內容設定檔中會用到兩個屬性：「應用程式識別碼」和「網域 (FQDN) 名稱」。如果選取應用程式識別碼，會一併取得 TLS_Version 和 CIPHER_SUITE 子屬性。可以在單一內容設定檔中同時使用應用程式識別碼和網域名稱。可以在同一個設定檔中使用多個應用程式識別碼。可以使用具有多個子屬性的一個應用程式識別碼，但若是單一定義檔中使用多個應用程式識別碼屬性，則會清除這些子屬性。

程序

- 1 選取**詳細目錄 > 內容設定檔**。
- 2 按一下**新增內容設定檔**。
- 3 輸入**設定檔名稱**。
- 4 在 [屬性] 資料行中按一下**設定**。
- 5 選取某個屬性，或按一下**新增屬性**，然後選取**應用程式識別碼**或**網域 (FQDN) 名稱**。
- 6 選取一或多個屬性。
- 7 (選擇性) 如果您已選取某個具有子屬性 (例如 SSL 或 CIFS) 的屬性，請在 [子屬性/值] 資料行中按一下**設定**。
 - a 按一下**新增子屬性**，然後從下拉式功能表中選取子屬性類別。
 - b 選取一或多個子屬性。
 - c 按一下**新增**。可以透過按一下**新增子屬性**來新增另一個子屬性。
 - d 按一下**套用**。
- 8 按一下**新增**。
- 9 (選擇性) 若要新增其他類型的屬性，請再按一下**新增屬性**。
- 10 按一下**套用**。
- 11 (選擇性) 輸入說明。
- 12 (選擇性) 輸入標籤。
- 13 按一下**儲存**。

後續步驟

將此內容設定檔套用到第 7 層 Distributed Firewall 規則。

本節中的主題顯示如何使用防火牆和交換器的網際網路通訊協定流量資訊匯出 (IPFIX) 的設定檔來設定監控，以及如何設定 IPFIX 收集器。

本章節討論下列主題：

- 新增防火牆 IPFIX 設定檔
- 新增交換器 IPFIX 設定檔
- 新增 IPFIX 收集器
- 新增連接埠鏡像設定檔
- 進階監控工具

新增防火牆 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 選取工具 > 監控設定檔 > IPFIX。
- 3 按一下防火牆 IPFIX 設定檔索引標籤。
- 4 按一下新增防火牆 IPFIX 設定檔。
- 5 完成下列詳細資料。

設定	說明
名稱與說明	輸入名稱和 (選用) 說明。 備註 如果您想要建立全域設定檔，請將設定檔命名為 Global 。全域設定檔無法從使用者介面編輯或刪除，但您可以使用 NSX-T Data Center API 來執行此操作。
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。
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。

設定	說明
收集器組態	從下拉式清單中選取收集器。
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。

6 依序按一下**儲存**和**是**以繼續進行設定檔的設定。

7 按一下**套用至**以將設定檔套用至物件。

選取一或多個物件。

8 按一下**儲存**。

新增交換器 IPFIX 設定檔

您可以為交換器 (也稱為區段) 設定 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**工具 > 監控設定檔 > IPFIX**。
- 3 按一下**交換器 IPFIX 設定檔**索引標籤。
- 4 按一下**新增交換器 IPFIX 設定檔**。
- 5 完成下列詳細資料。

設定	說明
名稱與說明	輸入名稱和 (選用) 說明。 備註 如果您想要建立全域設定檔，請將設定檔命名為 Global 。全域設定檔無法從使用者介面編輯或刪除，但您可以使用 NSX-T Data Center API 來執行此操作。
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。
封包取樣機率 (%)	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。
收集器組態	從下拉式清單中選取收集器。
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。
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。
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。

6 依序按一下**儲存**和**是**以繼續進行設定檔的設定。

- 7 按一下**套用至**以將設定檔套用至物件。
選取一或多個物件。
- 8 按一下**儲存**。

新增 IPFIX 收集器

您可以設定防火牆和交換器的 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**工具 > 監控設定檔 > IPFIX**。
- 3 按一下**收集器**索引標籤。
- 4 選取**新增收集器 > IPFIX 交換器**或**新增收集器 > IPFIX 防火牆**。
- 5 輸入名稱。
- 6 輸入最多四個收集器的 IP 位址和連接埠。支援 IPv4 和 IPv6 位址。
- 7 按一下**儲存**。

新增連接埠鏡像設定檔

您可以設定連接埠鏡像工作階段的連接埠鏡像設定檔。

請注意，邏輯 SPAN 僅支援覆疊區段，而非 VLAN 區段。

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**工具 > 連接埠鏡像**
- 3 選取**新增設定檔 > 遠端 L3 SPAN**或**新增設定檔 > 邏輯 SPAN**。
- 4 輸入名稱和 (選用) 說明。
- 5 填寫下列設定檔詳細資料。

工作階段類型	參數
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 方向 - 選取雙向、入口或出口。 ■ 快照長度 - 指定要從封包擷取的位元組數。 ■ 封裝類型 - 選取 GRE、ERSPAN II 或 ERSPAN III。 ■ GRE 機碼 - 如果封裝類型為 GRE，請指定 GRE 機碼。 ■ ERSPAN 識別碼 - 如果封裝類型為 ERSPAN II 或 ERSPAN III，請指定 ERSPAN 識別碼。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 方向 - 選取雙向、入口或出口。 ■ 快照長度 - 指定要從封包擷取的位元組數。

- 6 按一下**目的地**資料行中的**設定**以設定目的地。
- 7 依序按一下**儲存**和**是**以繼續進行設定檔的設定。
- 8 依序按一下**來源**和**設定**以設定來源。

邏輯 SPAN 的可用來源為**區段連接埠**、**虛擬機器的群組**和**虛擬網路介面的群組**。

遠端 L3 SPAN 的可用來源為**區段**、**區段連接埠**、**虛擬機器的群組**和**虛擬網路介面的群組**。

- 9 按一下**儲存**。

進階監控工具

NSX-T 支援進階監控方法，包括檢視連接埠連線、Traceflow、連接埠鏡像、活動監控等。

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 從導覽面板中選取**進階網路與安全性 > 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。

Traceflow

Traceflow 可讓您在網路中插入封包，並監控封包在網路中的流程。此流程可讓您監控網路，並識別瓶頸或中斷之類的問題。

Traceflow 可讓您識別封包送達其目的地所採用的一或多個路徑，或相反地，識別封包在路徑中遭到捨棄之處。每個實體都會報告輸入和輸出的封包處理，因此您可以確認在接收封包或轉送封包時是否發生問題。

Traceflow 與客體虛擬機器堆疊之間傳輸的 Ping 要求/回應不同。Traceflow 會在標記的封包周遊覆疊網路時加以觀察，且每個封包在通過覆疊網路時都會受到監控，直到它傳送至目的地客體虛擬機器。插入的標記封包實際上絕不會傳送至目的地客體虛擬機器，因此，即使客體虛擬機器已關閉電源，Traceflow 也會成功執行。

Traceflow 可在傳輸節點上使用，且同時支援 IPv4 和 IPv6 通訊協定，包括：ICMP、TCP、UDP、DHCP、DNS 和 ARP/NDP。

Traceflow 支援下列流量類型：

- 第 2 層單點傳播

- 第 3 層單點傳播
- 第 2 層廣播
- 第 2 層多點傳送

您可以使用自訂標頭欄位和封包大小來建構封包。Traceflow 的來源或目的地可以是邏輯交換器連接埠、邏輯路由器上行連接埠、CSP 或 DHCP 連接埠。目的地端點可以是 NSX 覆疊或底層中的任何裝置。不過，您無法選取在 NSX Edge 節點北側的目的地。目的地必須位於相同的子網路上，或必須能夠透過 NSX 分散式邏輯路由器來連線。

如果來源和目的地位於相同的第 2 層網域中，則會將 Traceflow 作業視為第 2 層。在 NSX 中，這表示它們位於同一個 VXLAN 網路識別碼 (VNI 或區段識別碼) 上。例如，當兩個虛擬機器連結至相同的邏輯交換器時，就會發生此情況。

如果已設定 NSX 橋接，則未知的第 2 層封包一律會傳送至橋接器。一般而言，橋接器會將這些封包轉送至 VLAN，並將 Traceflow 封包報告為已傳送。封包報告為已傳送，不一定表示追蹤封包已傳送至指定的目的地。

就第 3 層 Traceflow 單點傳播流量而言，兩個端點會位於不同的邏輯交換器上，且具有連線至分散式邏輯路由器 (DLR) 的不同 VNI。

多點傳送流量的來源為虛擬機器 vNIC 或邏輯連接埠，目的地則為多點傳送群組位址。

Traceflow 觀察可能包含廣播 Traceflow 封包的觀察。ESXi 主機如果不知道目的地主機的 MAC 位址，則會廣播 Traceflow 封包。廣播流量的來源為虛擬機器 vNIC。廣播流量的第 2 層目的地 MAC 位址為 FF:FF:FF:FF:FF:FF。若要建立有效封包以進行防火牆檢測，廣播 Traceflow 作業必須要有子網路首碼長度。子網路遮罩可讓 NSX 計算封包的 IP 網路位址。

使用 Traceflow 追蹤封包的路徑

使用 Traceflow 檢查封包的路徑。Traceflow 可追蹤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 選取**進階網路與安全性 > 工具 > Traceflow**。
- 3 選取 IPv4 或 IPv6 位址類型。
- 4 選取流量類型。

IPv4 位址的流量類型選項為 [單點傳播]、[多點傳送] 和 [廣播]。IPv6 位址的流量類型選項為 [單點傳播] 或 [多點傳送]。

5 根據流量類型指定來源和目的地資訊。

流量類型	來源	目的地
單點傳播	<p>選取虛擬機器或邏輯連接埠。對於虛擬機器：</p> <ul style="list-style-type: none"> ■ 從下拉式清單中選取虛擬機器。 ■ 選取虛擬介面。 ■ 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，請從下拉式清單中選取其中一個。 ■ 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>對於邏輯連接埠：</p> <ul style="list-style-type: none"> ■ 選取連結類型：VIF、DHCP、Edge 上行或 Edge 集中式服務。 ■ 選取連接埠。 	<p>選取虛擬機器、邏輯連接埠或 IP-MAC。對於虛擬機器：</p> <ul style="list-style-type: none"> ■ 從下拉式清單中選取虛擬機器。 ■ 選取虛擬介面。 ■ 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，請從下拉式清單中選取其中一個。 ■ 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>對於邏輯連接埠：</p> <ul style="list-style-type: none"> ■ 選取連結類型：VIF、DHCP、Edge 上行或 Edge 集中式服務。 ■ 選取連接埠。 <p>對於 IP-MAC：</p> <ul style="list-style-type: none"> ■ 選取追蹤類型 (第 2 層或第 3 層)。若為第 2 層，請輸入 IP 位址和 MAC 位址。對於第 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。

6 (選擇性) 按一下**進階**以查看進階選項。

7 (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	預設值為 128。
TTL	預設值為 64。
逾時 (毫秒)	預設值為 10000。
Ethertype	預設值為 2048。
裝載類型	選取 Base64 、十六進位、純文字、二進位或十進位。
裝載資料	根據所選類型的裝載格式。

8 (選擇性) 選取通訊協定，並提供相關資訊。

通訊協定	步驟 1
TCP	指定來源連接埠、目的地連接埠和 TCP 旗標。
UDP	指定來源連接埠和目的地連接埠。
ICMP	指定 ICMP 識別碼和序列。

通訊協定	步驟 1
DHCPv6	選取 DHCP 訊息類型： 請求、通告、要求或回覆 。
DHCP	選取 DHCP OP 代碼： 開機要求或開機回覆 。
DNS	指定位址，然後選取訊息類型： 查詢或回應 。

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。

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。

請注意，邏輯 SPAN 僅支援覆疊邏輯交換器，而非 VLAN 邏輯交換器。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

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。
- 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。
- 對於本機 SPAN 工作階段，鏡像工作階段的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 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 **進階網路與安全性 > 工具 > 連接埠鏡像工作階段**。
- 4 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**。
- 5 輸入工作階段名稱, 並選擇性地輸入說明。
- 6 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。

工作階段類型	參數
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。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。

7 按下一步。

8 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。

9 按下一步。

10 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。

11 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。

為連接埠鏡像工作階段設定篩選器

您可以為連接埠鏡像工作階段設定篩選器，以便限制鏡像的資料量。

這項功能具有下列功能與限制：

- 只支援 ESXi 與 KVM 主機傳輸節點。
- 針對來源和目的地支援 IP 位址、IP 首碼和 IP 範圍。
- 針對來源或目的地不支援 IPSet。
- 不支援 ESXi 或 KVM 的鏡像統計資料。

必須使用 API 設定篩選器。不支援使用 NSX Manager 使用者介面。如需連接埠鏡像 API 和 PortMirroringFilter 架構的詳細資訊，請參閱《NSX-T Data Center API 參考》。

程序

- 1 使用 NSX Manager 使用者介面或 API 設定連接埠鏡像工作階段。
- 2 呼叫 GET /api/v1/mirror-sessions API 以取得連接埠鏡像工作階段的相關資訊。
- 3 呼叫 GET /api/v1/mirror-sessions/<mirror-session-id> API 以新增一或多個篩選器。例如，

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
  "mirror_sources": [
    {
      "resource_type": "LogicalPortMirrorSource",
      "port_ids": [
        "6a361832-43e4-430d-a48a-b84a6cba73c3"
      ]
    }
  ],
  "mirror_destination": {
    "resource_type": "LogicalPortMirrorDestination",
    "port_ids": [
      "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
    ]
  },
  "port_mirroring_filters": [
    {
      "filter_action": "MIRROR",
      "src_ips": {
        "ip-addresses": [
          "192.168.175.250",
          "2001:bd6::c:2957:160:126"
        ]
      }
      "dst_ips": {
        "ip-addresses": [
```

```

        "192.168.160.126",
        "2001:bd6::c:2957:175:250"
    ]
}
}
"session_type": "LogicalPortMirrorSession",
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}

```

- 4 (選擇性) 您可以呼叫 `get mirroring-session <session-number>` CLI 命令以顯示連接埠鏡像工作階段的內容，包括篩選器。

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 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

此功能符合 RFC 7011 及 RFC 7012 中指定的標準。

當您啟用 IPFIX 時，所有已設定的主機傳輸節點會使用連接埠 4739，將 IPFIX 訊息傳送至 IPFIX 收集器。若為 ESXi，則 NSX-T 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。

設定交換器 IPFIX 收集器

您可以設定交換器的 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**進階網路與安全性 > 工具 > IPFIX**。
- 3 按一下**交換器 IPFIX 收集器**索引標籤。
- 4 按一下**新增**以新增收集器。
- 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**新增**。

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**進階網路與安全性 > 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。 備註 如果您想要建立全域設定檔，請將設定檔命名為 Global 。全域設定檔無法從使用者介面編輯或刪除，但您可以使用 NSX-T Data Center API 來執行此操作。
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。

- 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。

- 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

- 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 選取**進階網路與安全性 > 工具 > IPFIX**
- 按一下**防火牆 IPFIX 收集器**索引標籤。
- 按一下**新增**以新增收集器。
- 輸入名稱和 (選用) 說明。
- 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。
- 按一下**新增**。

設定防火牆 IPFIX 設定檔

您可以設定防火牆的 IPFIX 設定檔。

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**進階網路與安全性 > 工具 > IPFIX**
- 按一下**防火牆 IPFIX 設定檔**索引標籤。
- 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。 備註 如果您想要建立全域設定檔，請將設定檔命名為 Global 。全域設定檔無法從使用者介面編輯或刪除，但您可以使用 NSX-T Data Center API 來執行此操作。
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 按一下新增。

ESXi IPFIX 範本

ESXi 主機傳輸節點支援八個邏輯交換器 IPFIX 流量範本，以及兩個分散式防火牆 IPFIX 流量範本。

下表列出邏輯交換器 IPFIX 封包中的 VMware 特定元素。

元素識別碼	參數名稱	資料類型	單位
880	tenantProtocol	unsigned8	1 位元組
881	tenantSourceIPv4	ipv4Address	4 位元組
882	tenantDestIPv4	ipv4Address	4 位元組
883	tenantSourceIPv6	ipv6Address	16 位元組
884	tenantDestIPv6	ipv6Address	16 位元組
886	tenantSourcePort	unsigned16	2 位元組
887	tenantDestPort	unsigned16	2 位元組
888	egressInterfaceAttr	unsigned16	2 位元組
889	vxlانExportRole	unsigned8	1 位元組
890	ingressInterfaceAttr	unsigned16	2 位元組
898	virtualObsID	字串	變數長度

下表列出分散式防火牆 IPFIX 封包中的 VMware 特定元素。

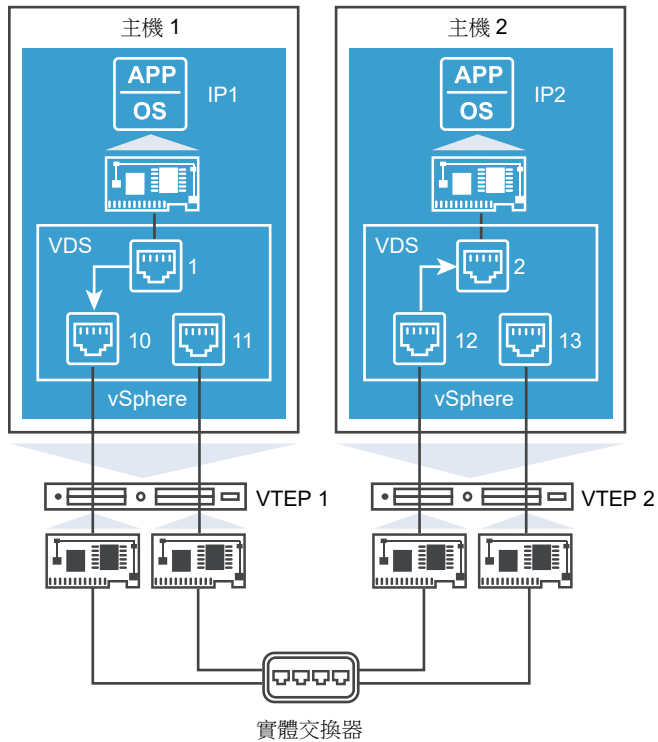
元素識別碼	參數名稱	資料類型	單位
950	ruleId	unsigned32	4 位元組
951	vmUuid	字串	16 位元組
952	vnidIndex	unsigned32	4 位元組
953	sessionFlags	unsigned8	1 位元組
954	flowDirection	unsigned8	1 位元組
955	algControlFlowId	unsigned64	8 位元組
956	algType	unsigned8	1 位元組
957	algFlowType	unsigned8	1 位元組
958	averageLatency	unsigned32	4 位元組
959	retransmissionCount	unsigned32	4 位元組

元素識別碼	參數名稱	資料類型	單位
960	vifUuid	octetArray	16 位元組
961	vifId	字串	變數長度

ESXi 邏輯交換器 IPFIX 範本

ESXi 主機傳輸節點支援八個邏輯交換器 IPFIX 流量範本。

下圖顯示受到 IPFIX 功能監控之 ESXi 主機所連結虛擬機器之間的流量。



IPv4 封裝的範本將具有下列元素：

- 標準元素
- SrcAddr: VTEP1
- DstAddr: VTEP2
- tenantSourceIPv4: IP1
- tenantDestIPv4: IP2
- tenantSourcePort: 10000
- tenantDestPort: 80
- tenantProtocol: TCP
- ingressInterfaceAttr: 0x03 (通道連接埠)

- egressInterfaceAttr: 0x01
- encapExportRole: 01
- virtualObsID: 89fd5032-2dc9-4fc3-993a-9bb4b616de54 (邏輯連接埠識別碼)

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()
```

ESXi 分散式防火牆 IPFIX 範本

ESXi 主機傳輸節點支援兩個分散式防火牆 IPFIX 流量範本。

IPv4 範本

範本識別碼：288

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address,4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address,4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4,1)
```

```

IPFIX_TEMPLATE_FIELD(icmpCodeIPv4,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

IPv6 範本

範本識別碼：289

```

IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

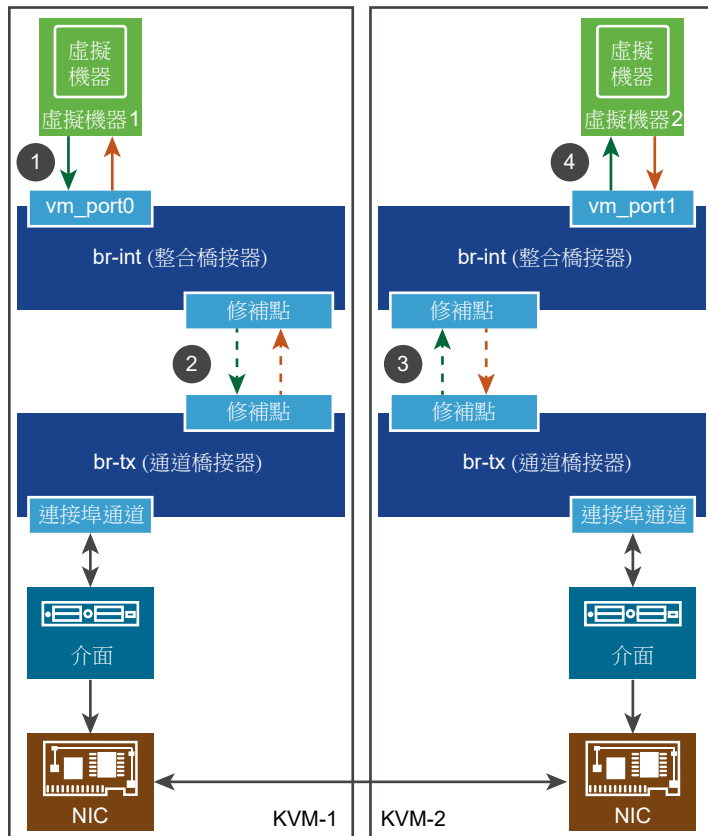
KVM IPFIX 範本

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。

下表列出 KVM IPFIX 封包中的 VMware 特定元素。

元素識別碼	參數名稱	資料類型	單位
891	tunnelType	unsigned8	1 位元組
892	tunnelKey	位元組數	變數長度
893	tunnelSourceIPv4Address	unsigned32	4 位元組
894	tunnelDestinationIPv4Address	unsigned32	4 位元組
895	tunnelProtocolIdentifier	unsigned8	1 位元組
896	tunnelSourceTransportPort	unsigned16	2 位元組
897	tunnelDestinationTransportPort	unsigned16	2 位元組
898	virtualObsID	字串	變數長度

下圖顯示受到 IPFIX 功能監控的 KVM 主機所連結的虛擬機器之間的流量。



KVM IPv4 IPFIX 入口範本將有下列元素：

- 標準元素
- virtualObsID: 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (邏輯連接埠識別碼)

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。

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**進階網路與安全性 > 網路 > 交換 > 連接埠**

3 按一下連接埠的名稱。

4 按一下**監控**索引標籤。

此時會顯示連接埠狀態和統計資料。

5 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**。

6 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。

邏輯交換器

13

您可以從**進階網路與安全性**索引標籤設定邏輯交換器和相關的物件。邏輯交換器可在與基礎硬體分離的虛擬環境中，重現交換功能、廣播、未知單點傳播以及多點傳播 (BUM) 流量。

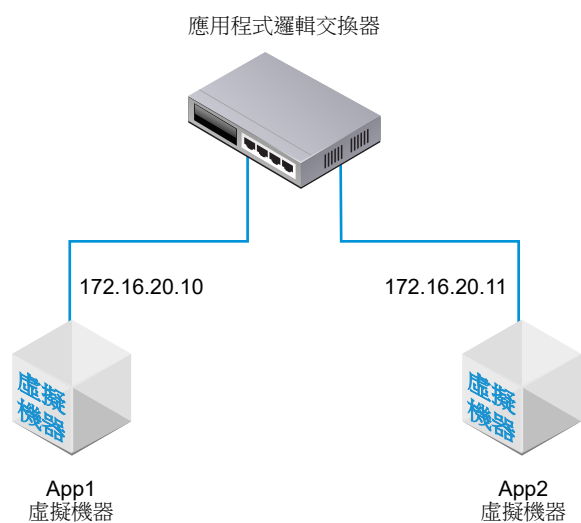
備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

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 13-1. 邏輯交換器拓撲



例如，上方的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。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

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](#)
- [將虛擬機器連線到邏輯交換器](#)
- [建立邏輯交換器連接埠](#)
- [測試第 2 層連線](#)
- [為 NSX Edge 上行建立 VLAN 邏輯交換器](#)
- [邏輯交換器和邏輯連接埠的交換設定檔](#)
- [第 2 層橋接](#)

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 13 章 邏輯交換器與瞭解 BUM 框架複寫模式。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取 **進階網路與安全性 > 網路 > 交換 > 交換器 > 新增**。
- 3 輸入邏輯交換器的名稱，並選擇性地輸入說明。
- 4 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。
- 5 輸入上行整併原則的名稱。
- 6 將**管理狀態**設定為**開啟**或**關閉**。

7 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。

8 (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。

9 (選擇性) 按一下**交換設定檔**索引標籤並選取交換設定檔。

10 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](#)。

將虛擬機器連線到邏輯交換器

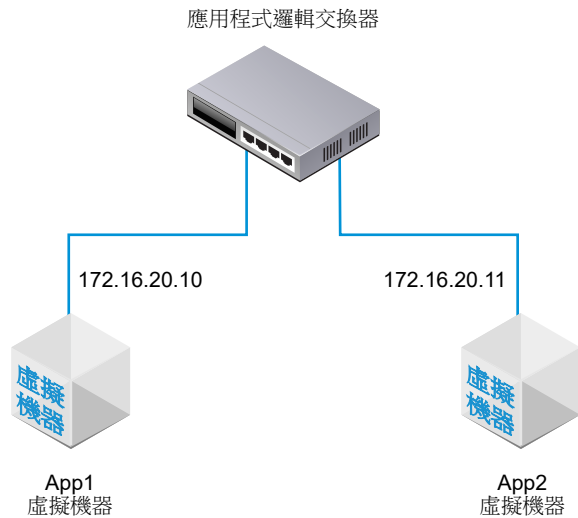
視主機而定，用來將虛擬機器連線到邏輯交換器的組態可能會有所不同。

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 NSX Manager 的 **進階網路與安全性 > 網路 > 交換 > 連接埠** 中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 NSX-T Data Center 使用者介面中，**進階網路與安全性 > 網路 > 交換 > 連接埠** 下的 VIF 連結識別碼會與 API 呼叫中出現的 ExternalID 相符。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〉。

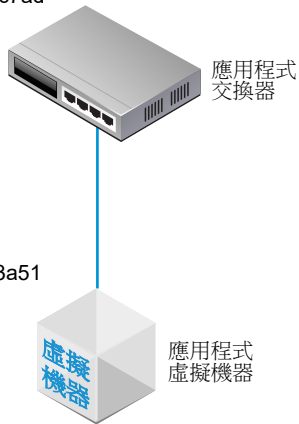
將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T Data Center 邏輯交換器

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 乙太網路介面卡。

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

- 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": [
    "instanceUid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUid: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 使用者介面中的 **進階網路與安全性 > 網路 > 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。

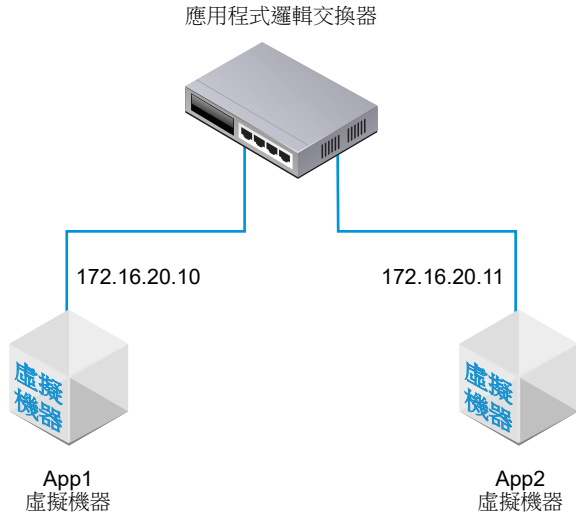
後續步驟

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 NSX Manager 使用者介面中的 **進階網路與安全性 > 網路 > 交換 > 連接埠** 下方，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〉。

建立邏輯交換器連接埠

邏輯交換器具有多個交換器連接埠。邏輯交換器連接埠可讓其他網路元件、虛擬機器或容器連線至邏輯交換器。

如果您將虛擬機器連線至由 vCenter Server 管理之 ESXi 主機上的邏輯交換器，則系統會自動建立邏輯交換器連接埠。如需如何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。

若要監控邏輯交換器連接埠上的活動，請參閱[監控邏輯交換器連接埠活動](#)。

必要條件

確認您已建立邏輯交換器。請參閱[第 13 章 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**進階網路與安全性 > 網路 > 交換 > 連接埠 > 新增**。
- 3 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	從下拉式功能表中選取邏輯交換器。
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。

使用 API，您可以將連結類型設定為其他值 (LOGICALROUTER、BRIDGEENDPOINT、DHCP_SERVICE、METADATA_PROXY、L2VPN_SESSION)。如果連結類型為 DHCP 服務、中繼資料 Proxy 或 L2 VPN 工作階段，連接埠的交換設定檔必須為預設值。您無法使用任何使用者定義的設定檔。

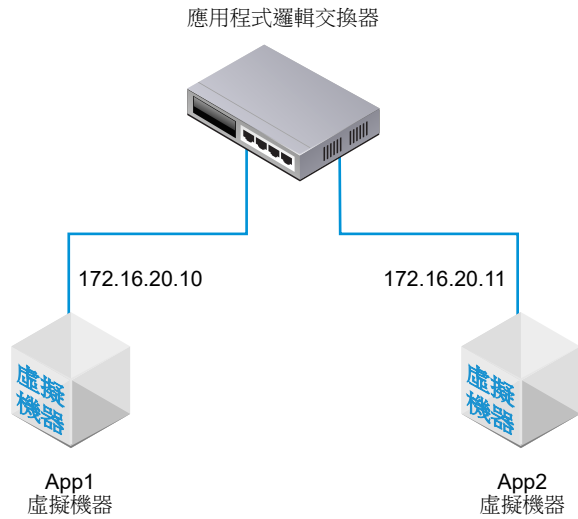
- 4 (選擇性) 在**交換設定檔**索引標籤中，選取交換設定檔。
- 5 按一下**儲存**。

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 13-2. 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 **進階網路與安全性 > 網路 > 交換 > 交換器**。

- e 按一下邏輯交換器並記下 UUID 和 VNI 資訊。
- f 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-manager1> 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-manager1> 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-manager1> 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-manager1> 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-manager1> 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	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。
	<pre>nsx-manager1> 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>

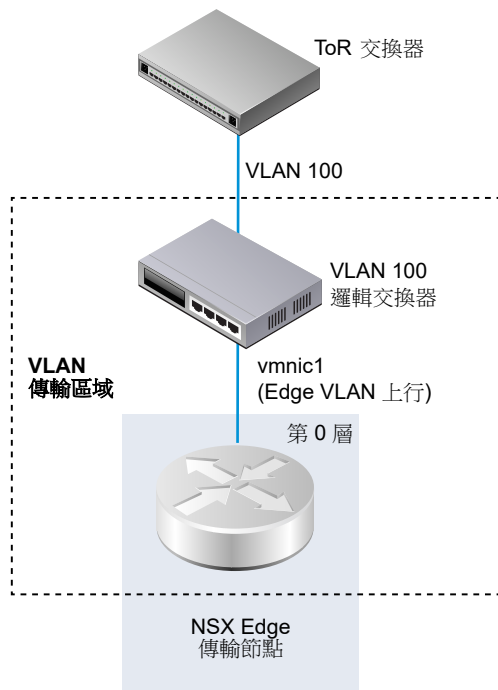
結果

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。

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 **進階網路與安全性 > 網路 > 交換 > 交換器 > 新增**。
- 3 輸入邏輯交換器的名稱。
- 4 選取邏輯交換器的傳輸區域。
- 5 選取上行整併原則。
- 6 對於管理狀態，選取**開啟**或**關閉**。
- 7 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。

- 8 (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。

邏輯交換器和邏輯連接埠的交換設定檔

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

可供使用的交換設定檔類型如下。

- QoS (服務品質)
- 連接埠鏡像
- 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。

使用預設設定檔之前，請確定設定為您所需的設定。建立自訂設定檔時，某些設定具有預設值。不要假設在預設設定檔中，這些設定將具有預設值。

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。

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 **進階網路與安全性 > 網路 > 交換 > 交換設定檔 > 新增**

3 選取 QoS，然後填寫 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	<p>從 [模式] 下拉式功能表中選取信任或未受信任選項。</p> <p>當您選取「受信任」模式，內部標頭 DSCP 值會套用至 IP/IPv6 流量的外部 IP 標頭。針對非 IP/IPv6 流量，外部 IP 標頭會採用預設值。以覆疊為基礎的邏輯連接埠上支援信任模式。預設值為 0。</p> <p>以覆疊為基礎及以 VLAN 為基礎的邏輯連接埠上支援未受信任模式。針對以覆疊為基礎的邏輯連接埠，輸出 IP 標頭的 DSCP 值會設為與邏輯連接埠內部封包類型無關的設定值。針對以 VLAN 為基礎的邏輯連接埠，IP/IPv6 封包的 DSCP 值會設為設定值。未受信任模式的 DSCP 值範圍介於 0 至 63 之間。</p> <p>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。</p>
優先順序	<p>設定 DSCP 值。</p> <p>優先順序值在 0 到 63 之間。</p>
服務類別	<p>設定 CoS 值。</p> <p>以 VLAN 為基礎的邏輯連接埠上支援 CoS。CoS 會分組網路中的類似流量類型，且每個流量類型會根據其本身的服務優先順序層級而視為一個類別。較低優先順序的流量會變慢或在某些情況下會捨棄，可提供較佳的輸送量以處理較高優先順序的流量。CoS 也可以使用 0 封包針對 VLAN 識別碼進行設定。</p> <p>CoS 值範圍從 0 至 7，其中 0 是優先順序最低的服務。</p>
入口	<p>設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>您可以使用平均頻寬來降低網路壅塞。尖峰頻寬速率用來支援高載流量，而高載大小會基於使用尖峰頻寬的持續時間。您可以在高載大小設定中設定高載持續時間。您無法保證頻寬。但是，您可以使用平均、尖峰和高載大小設定來限制網路頻寬。</p> <p>例如，如果平均頻寬為 30 Mbps，尖峰頻寬為 60 Mbps，而允許的持續時間為 0.1 秒，則高載大小為 $60 * 1000000 * 0.10/8 = 750000$ 位元組。</p> <p>預設值為 0 會停用入口流量的速率限制。</p>
入口廣播	<p>根據廣播設定從虛擬機器至邏輯網路的輸出網路流量自訂值。</p> <p>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。例如，當您將邏輯交換器的平均頻寬設定為 3000 Kbps，尖峰頻寬為 6000 Kbps，而允許的持續期間為 0.1 秒，則高載大小為 $6000 * 1000 * 0.10/8 = 75000$ 位元組。</p> <p>預設值為 0 會停用入口廣播流量的速率限制。</p>
出口	<p>設定從邏輯網路至虛擬機器的輸入網路流量自訂值。</p> <p>預設值為 0 會停用出口流量的速率限制。</p>

如果並未設定入口、入口廣播及出口選項，則會使用預設值。

4 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](#)。

瞭解連接埠鏡像交換設定檔

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

連接埠鏡像通常用於下列案例：

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

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

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

設定自訂連接埠鏡像交換設定檔

您可以使用不同的目的地及金鑰值建立自訂連接埠鏡像交換設定檔。

必要條件

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

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 網路 > 交換 > 交換設定檔 > 新增**
- 3 選取**連接埠鏡像**，然後填寫連接埠鏡像交換設定檔詳細資料。

選項	說明
名稱與說明	將名稱指派至自訂連接埠鏡像交換設定檔。 您可以選擇性地描述您修改的設定以自訂此設定檔。
方向	從下拉式功能表中選取選項，將此來源用於入口、出口或雙向流量。 入口是從虛擬機器至邏輯網路的輸出網路流量。 出口是從邏輯網路至虛擬機器的輸入網路流量。 雙向是從虛擬機器至邏輯網路以及從邏輯網路至虛擬機器的雙向流量。這是預設的選項。

選項	說明
封包截斷	選擇性。範圍是 60 - 65535。
金鑰	<p>輸入隨機 32 位元值以識別來自邏輯連接埠的鏡像封包。</p> <p>此「金鑰」值會複製到每個鏡像封包之 GRE 標頭中的 [金鑰] 欄位。如果「金鑰」值設定為 0，則預設定義會複製到 GRE 標頭中的 [金鑰] 欄位。</p> <p>預設 32 位元值是由下列值所組成。</p> <ul style="list-style-type: none"> ■ 第一個 24 位元是 VNI 值。VNI 是封裝式框架 IP 標頭的一部分。 ■ 第 25 個位元表示第一個 24 位元是否為有效的 VNI 值。1 代表有效值，而 0 代表無效值。 ■ 第 26 個位元表示鏡像流量的方向。1 代表入口方向，而 0 代表出口方向。 ■ 其餘的六個位元並未使用。
目的地	<p>輸入鏡像工作階段的收集器目的地識別碼。</p> <p>目的地 IP 位址 ID 僅能為網路內的 IPv4 位址，或非由 NSX-T Data Center 所管理的遠端 IPv4 位址。您可以新增最多三個目的地 IP 位址，並以逗號分隔。</p>

4 按一下儲存。

結果

自訂連接埠鏡像交換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](#)。

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

確認自訂連接埠鏡像交換設定檔

在開始使用自訂連接埠鏡像交換設定檔之前，請先確認自訂項目可以正常運作。

必要條件

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

程序

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

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

- 2 在目的地 IP 位址上執行 tcpdump 命令。

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

例如，目的地 IP 位址是 10.24.123.196。

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

後續步驟

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

瞭解 IP 探索交換設定檔

IP 探索使用 DHCP 和 DHCPv6 窺探、ARP (位址解析通訊協定) 窺探、ND (芳鄰探索) 窺探，以及 VM Tools 來學習 MAC 和 IP 位址。

探索到的 MAC 和 IP 位址可用於實現 ARP/ND 隱藏，以最大限度地減少連線至相同邏輯交換器的虛擬機器之間的流量。SpoofGuard 和 Distributed Firewall (DFW) 元件也會使用這些位址。DFW 使用位址繫結來判斷防火牆規則中物件的 IP 位址。

DHCP/DHCPv6 窺探會檢查在 DHCP/DHCPv6 用戶端和伺服器之間交換的 DHCP/DHCPv6 封包，以學習 IP 和 MAC 位址。

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

VM Tools 是一種在 ESXi 主控虛擬機器執行上的軟體，可提供包括 MAC 和 IP 或 IPv6 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。

ND 窺探是 ARP 窺探的對等 IPv6。它會檢查芳鄰請求 (NS) 和芳鄰通告 (無) 訊息，以學習 IP 和 MAC 位址。

重複位址偵測會檢查其他連接埠已實現繫結清單上是否已有新探索到的 IP 位址。會針對同一邏輯交換器上的連接埠執行此檢查。如果偵測到重複的位址，新探索到的位址不會新增至實現的繫結清單，但會新增至已探索到的清單。所有重複的 IP 都具有相關聯的探索時間戳記。如果藉由將實現繫結清單上的 IP 新增至略過繫結清單或停用窺探來移除此 IP (如下所示)，則具有最舊時間戳記的重複 IP 將會移至實現的繫結清單中。可透過 API 呼叫取得重複位址資訊。

依預設，探索方法 ARP 窺探和 ND 窺探會在名稱為「首次使用時信任 (TOFU)」的模式下運作。在 TOFU 模式中，在探索到位址並將其新增至實現的繫結清單時，該繫結會永久保留在實現的清單中。TOFU 會套用至使用 ARP/ND 窺探探索到前「n」個唯一的 <IP、MAC、VLAN> 繫結，其中「n」是您可以設定的繫結限制。您可以針對 ARP/ND 窺探停用 TOFU。隨後，這些方法將會在「每次使用皆信任 (TOEU)」模式中運作。在 TOEU 模式中，在探索到某個位址時，系統即會將其新增至實現的繫結清單中，並在該位址刪除或到期後，將其從實現的繫結清單中移除。DHCP 窺探和 VM Tools 一律會在 TOEU 模式中運作

備註 TOFU 並不同於 SpoofGuard，它不會像 SpoofGuard 一樣封鎖流量。如需 SpoofGuard 的詳細資訊，請參閱[瞭解 SpoofGuard](#)。

對於每個連接埠，NSX Manager 會維護略過繫結清單，其中包含無法繫結至連接埠的 IP 位址。只能使用 API 更新此清單。也可以使用此方法刪除之前為指定連接埠探索到的 IP。如需詳細資訊，請參閱《NSX-T API 參考》並搜尋 `ignore_address_bindings`。

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

NSX-T Data Center 提供多個預設的 IP 探索交換設定檔。您也可以另外建立 IP 探索交換設定檔。

必要條件

自行熟悉 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 **進階網路與安全性 > 網路 > 交換 > 交換設定檔 > 新增**。
- 3 選取 **IP 探索**，然後指定 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	適用於 IPv4 環境。適用於具有靜態 IP 位址的虛擬機器。
ARP 繫結限制	可繫結至連接埠的 IPv4 IP 位址數目上限。
ARP ND 繫結限制逾時	在 TOFU 已停用的情況下，ARP/ND 繫結資料表中 IP 位址的逾時值 (以分鐘為單位)。如果位址逾時，新探索到的位址會將其取代。
DHCP 窺探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP V6 窺探	適用於 IPv6 環境。適用於具有 IPv6 位址的虛擬機器。
VM Tools	僅適用於裝載 ESXi 的虛擬機器。
IPv6 的 VM Tools	僅適用於裝載 ESXi 的虛擬機器。
芳鄰探索窺探	適用於 IPv6 環境。適用於具有靜態 IP 位址的虛擬機器。
芳鄰探索繫結限制	可繫結至連接埠的 IPv6 位址數目上限。
首次使用時信任	適用於 ARP 和 ND 窺探。
重複的 IP 偵測	適用於所有窺探方法及 IPv4 和 IPv6 環境。

- 4 按一下**新增**。

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，選取**進階網路與安全性 > 網路 > 交換 > 連接埠**。
- 2 按一下您要套用位址繫結的邏輯連接埠。
邏輯連接埠摘要隨即顯示。
- 3 在**概觀**索引標籤中，展開**位址繫結**。
- 4 按一下**新增**。
新增位址繫結對話方塊隨即顯示

- 5 指定您要套用位址繫結之邏輯連接埠的 IP 和 MAC 位址。您也可以指定 VLAN 識別碼。
- 6 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**進階網路與安全性 > 網路 > 交換 > 交換設定檔 > 新增**。
- 3 選取 **SpoofGuard**。
- 4 輸入名稱和 (選用) 說明。
- 5 若要啟用連接埠層級 SpoofGuard，請將**連接埠繫結**設為**已啟用**。
- 6 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**進階網路與安全性 > 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。依預設為停用狀態。 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。您必須啟用 BPDU 篩選器 ，才能從此清單中選取。
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。依預設會停用這兩者。 「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。
DHCPv6 篩選器	切換 V6 伺服器封鎖 按鈕及 V6 用戶端封鎖 按鈕以啟用 DHCP 篩選。依預設會停用這兩者。 「DHCPv6 伺服器封鎖」會封鎖 DHCPv6 伺服器至 DHCPv6 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。將會篩選 UDP 來源連接埠號碼為 547 的封包。 「DHCPv6 用戶端封鎖」會封鎖 DHCP 要求，以防止虛擬機器取得 DHCP IP 位址。將會篩選 UDP 來源連接埠號碼為 546 的封包。
封鎖非 IP 流量	切換 封鎖非 IP 流量 按鈕以僅允許 IPv4、IPv6、ARP 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。
RA 保護	切換 RA 保護 按鈕，以篩選出入口 IPv6 路由器通告。ICMPv6 類型 134 封包將被篩選掉。此選項依預設為啟用。
速率限制	設定廣播及多點傳送流量的速率限制。此選項依預設為啟用。 速率限制可用來保護邏輯交換器或虛擬機器免於遭受廣播風暴等事件。 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，除非是使用 VMware Integrated OpenStack 部署客體虛擬機器，在此情況下，依預設會啟用該內容。

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

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

您可以設定可學習的 MAC 位址數目。最大值為 4096，這是預設值。您也可以設定何時達到限制的原則。選項包括：

- **捨棄** - 捨棄來自未知來源 MAC 位址的封包。輸入至此 MAC 位址的封包將視為未知的單點傳播。連接埠只有在已啟用未知單點傳播洪泛時才會接收封包。
- **允許** - 來自未知來源 MAC 位址的封包會進行轉送，但無法學習位址。輸入至此 MAC 位址的封包將視為未知的單點傳播。連接埠只有在已啟用未知單點傳播洪泛時才會接收封包。

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 **進階網路與安全性 > 網路 > 交換 > 交換設定檔 > 新增**。
- 3 選取 **MAC 管理**，然後填寫 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。預設值為已停用。
狀態	啟用或停用 MAC 學習功能。預設值為已停用。
未知單點傳播洪泛	啟用或停用未知單點傳播洪泛功能。預設值為已啟用。如果啟用 MAC 學習，則可使用此選項。
MAC 限制	設定 MAC 位址的數目上限。預設值為 4096。如果啟用 MAC 學習，則可使用此選項。
MAC 限制原則	選取 允許 或 捨棄 。預設為 允許 。如果啟用 MAC 學習，則可使用此選項。

- 4 按一下 **新增**。

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 [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 **進階網路與安全性 > 網路 > 交換 > 交換器**。
- 3 按一下邏輯交換器以套用自訂交換設定檔。
- 4 按一下 **管理** 索引標籤。
- 5 從下拉式功能表中選取自訂交換設定檔類型。

■ QoS

- 連接埠鏡像
- IP 探索
- SpoofGuard
- 交換器安全性
- MAC 管理

6 按一下**變更**。

7 從下拉式功能表中選取先前建立的自訂交換設定檔。

8 按一下**儲存**。

邏輯交換器現在會與自訂交換設定檔建立關聯。

9 確認**管理**索引標籤下方顯示具有已修改之組態的全新自訂交換設定檔。

10 (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至子邏輯連接埠。

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[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**進階網路與安全性 > 網路 > 交換 > 連接埠**。
- 3 按一下邏輯連接埠以套用自訂交換設定檔。
- 4 按一下**管理**索引標籤。
- 5 從下拉式功能表中選取自訂交換設定檔類型。
 - QoS
 - 連接埠鏡像
 - IP 探索

- **SpoofGuard**
- **交換器安全性**
- **MAC 管理**

- 6 按一下**變更**。
- 7 從下拉式功能表中選取先前建立的自訂交換設定檔。
- 8 按一下**儲存**。

邏輯連接埠現在會與自訂交換設定檔建立關聯。

- 9 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 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。此第 2 層橋接器在移轉案例中特別有用，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 Edge 叢集和 Edge 橋接器設定檔。您可以使用 NSX Edge 傳輸節點來設定第 2 層橋接。若要使用 NSX Edge 傳輸節點進行橋接，您可以建立 Edge 橋接器設定檔。Edge 橋接器設定檔會指定要用於橋接的 Edge 叢集，以及要作為主要和備份橋接器的 Edge 傳輸節點。

Edge 橋接器設定檔會連結至邏輯交換器，而對應會指定在 Edge 上用於橋接的實體上行，以及要與邏輯交換器相關聯的 VLAN 識別碼。邏輯交換器可連結至數個橋接器設定檔。

建立 ESXi 橋接器叢集

ESXi 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 ESXi 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，ESXi 橋接器叢集將在主動-待命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**系統 > 網狀架構 > 節點 > ESXi 橋接器叢集 > 新增**。
- 2 輸入橋接器叢集的名稱，並選擇性地輸入說明。
- 3 選取橋接器叢集的傳輸區域。
- 4 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。
- 5 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 Edge 橋接器設定檔

Edge 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**系統 > 網狀架構 > 設定檔 > Edge 橋接器設定檔 > 新增**。
- 2 輸入 Edge 橋接器設定檔的名稱，並選擇性地輸入說明。
- 3 選取 NSX Edge 叢集。
- 4 選取主要節點。
- 5 選取備份節點。
- 6 選取容錯移轉模式。
選項為**先佔式**和**非先佔式**。
- 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設定檔建立關聯。

設定以 Edge 為基礎的橋接

當您設定以 Edge 為基礎的橋接時，在為 Edge 叢集建立 Edge 橋接器設定檔後，需要進行一些額外的組態。

請注意，不支援在相同的 Edge 節點上橋接邏輯交換器兩次。但是，您可以將兩個 VLAN 橋接至兩個不同 Edge 節點上的相同邏輯交換器。

有三個組態選項可供使用。

選項 1：設定混合模式

- 在連接埠群組上設定混合模式。
- 在連接埠群組上允許偽造的傳輸。
- 執行下列命令，在執行 Edge 虛擬機器的 ESXi 主機上啟用反向篩選：

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

然後，使用下列步驟在連接埠群組上先停用再啟用混合模式：

- 編輯連接埠群組的設定。
- 停用混合模式並儲存設定。
- 再次編輯連接埠群組的設定。
- 啟用混合模式並儲存設定。
- 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，輸送量可能會降低，因為在混合模式中必須將 VLAN 流量同時轉送至這兩個虛擬機器。

選項 2：設定 MAC 學習

如果 Edge 部署在已安裝 NSX-T 的主機上，則可以連線至 VLAN 邏輯交換器或區段。邏輯交換器必須具有已啟用 MAC 學習的 MAC 管理設定檔。同樣地，區段必須具有已啟用 MAC 學習的 MAC 探索設定檔。

選項 3：設定接收連接埠

- 1 針對您要設定為接收連接埠的主幹 vNIC，擷取連接埠號碼。
 - a 登入 vSphere Web Client，然後導覽至 **首頁 > 網路**。
 - b 按一下 NSX Edge 主幹介面所連線的分散式連接埠群組，然後按一下 **連接埠** 以檢視連接埠和已連線的虛擬機器。記下與主幹介面相關聯的連接埠號碼。在擷取和更新不透明資料時，請使用此連接埠號碼。
- 2 擷取 vSphere Distributed Switch 的 dvsUuid 值。
 - a 在 `https://<vc-ip>/mob` 上登入 vCenter Mob UI。
 - b 按一下 **內容**。
 - c 按一下與 **rootFolder** 相關聯的連結 (例如： `group-d1 (Datacenters)`)。
 - d 按一下與 **childEntity** 相關聯的連結 (例如： `datacenter-1`)。
 - e 按一下與 **networkFolder** 相關聯的連結 (例如： `group-n6`)。
 - f 按一下與 NSX Edge 相關聯之 vSphere Distributed Switch 的 DVS 名稱連結 (例如： `dvs-1 (Mgmt_VDS)`)。
 - g 複製 UUID 字串的值。在擷取和更新不透明資料時，請使用此 dvsUuid 值。

3 確認用來指定連接埠的不透明資料是否存在。

- a 移至 `https://<vc-ip>/mob/?moid=DVManager&vmodl=1`。
- b 按一下 **fetchOpaqueDataEx**。
- c 在 **selectionSet** 值方塊中，貼上下列 XML 輸入：

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

使用您為 NSX Edge 主幹介面擷取的連接埠號碼和 dvsUuid 值。

- d 將 **isRuntime** 設為 **false**。
 - e 按一下 **叫用方法**。如果結果顯示 `vim.dvs.OpaqueData.ConfigInfo` 的值，則表示已有不透明的資料集，而在設定接收連接埠時請使用 **edit** 作業。如果 `vim.dvs.OpaqueData.ConfigInfo` 的值為空白，則在設定接收連接埠時請使用 **add** 作業。
- 4 在 vCenter 受管理物件瀏覽器 (MOB) 中設定接收連接埠。

- a 移至 `https://<vc-ip>/mob/?moid=DVManager&vmodl=1`。
- b 按一下 **updateOpaqueDataEx**。
- c 在 **selectionSet** 值方塊中，貼上下列 XML 輸入。例如，

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

使用您從 vCenter MOB 中擷取的 dvsUuid 值。

- d 在 **opaqueDataSpec** 值方塊上，貼上下列其中一個 XML 輸入。

如果不透明資料未設定 (**operation** 設定為 **add**)，請使用此輸入來啟用接收連接埠：

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAA= </opaqueData>
    </opaqueData>
  </opaqueDataSpec>
```

如果不透明資料已設定 (operation 設定為 edit)，請使用此輸入來啟用接收連接埠：

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmwmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA= </opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

請使用此輸入來停用接收連接埠：

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmwmodl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA= </opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

- e 將 isRuntime 設為 false。
- f 按一下叫用方法。

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。

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 **進階網路與安全性 > 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。

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"
}
```

NSX-T Data Center 支援第 2 層路由模型。

最上層是第 0 層邏輯路由器。第 0 層邏輯路由器的北向會連線到一或多個實體路由器或第 3 層交換器，並做為實體基礎結構的閘道。第 0 層邏輯路由器的南向會連線至一或多個第 1 層邏輯路由器或直接連線至一或多個邏輯交換器。

下層是第 1 層邏輯路由器。北向的第 1 層邏輯路由器會連接至第 0 層邏輯路由器。南向則連線至一或多個邏輯交換器。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

本章節討論下列主題：

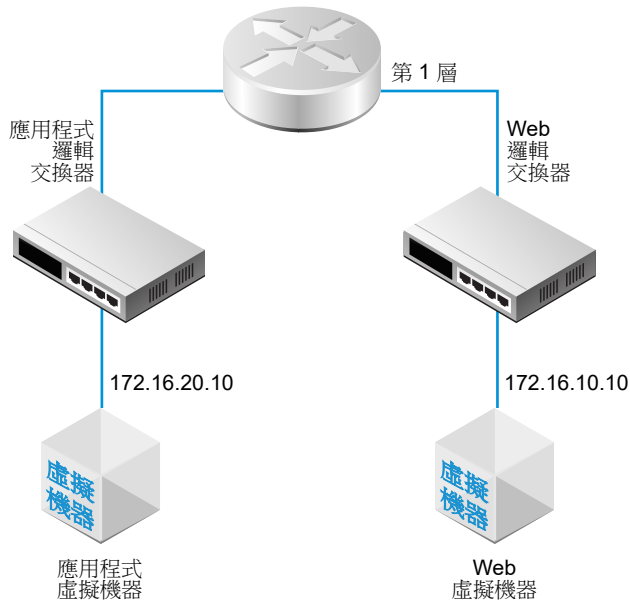
- [第 1 層邏輯路由器](#)
- [第 0 層邏輯路由器](#)

第 1 層邏輯路由器

第 1 層邏輯路由器具有下行連接埠可連線至邏輯交換器，以及上行連接埠可連線至第 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 14-1. 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。

在某些情況下，外部用戶端會針對繫結至 LB VIP 連接埠的 MAC 位址傳送 ARP 查詢。但是，LB VIP 連接埠沒有 MAC 位址且無法處理此類查詢。Proxy ARP 會在第 1 層邏輯路由器的集中式服務連接埠上實作，以代表 LB VIP 連接埠處理 ARP 查詢。

為第 1 層邏輯路由器設定了 DNAT、Edge 防火牆和負載平衡器時，將會依下列順序處理往返於另一個第 1 層邏輯路由器的流量：DNAT、Edge 防火牆和負載平衡器。第 1 層邏輯路由器內的流量先透過 DNAT 進行處理，再以負載平衡器處理。此時會略過 Edge 防火牆處理。

在第 0 層或第 1 層邏輯路由器上，您可以設定不同類型的連接埠。其中一個類型稱為集中式服務連接埠 (CSP)。您必須在處於主動備用模式的第 0 層邏輯路由器上或第 1 層邏輯路由器上設定 CSP，才能連線至 VLAN 支援的邏輯交換器，或建立獨立的第 1 層邏輯路由器。CSP 在處於主動備用模式的第 0 層邏輯路由器上或第 1 層邏輯路由器上支援下列服務：

- NAT
- 負載平衡
- 可設定狀態的防火牆
- VPN (IPsec 和 L2VPN)

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 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**進階網路與安全性 > 路由器 > 路由器 > 新增**。
- 3 選取**第 1 層路由器**，然後輸入邏輯路由器的名稱，並選擇性地輸入說明。
- 4 (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。

- 5 (選擇性) 選取 NSX Edge 叢集。

若要取消選取您所選取的叢集，請按一下 **x** 圖示。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。

- 6 (選擇性) 按一下**待命重新放置**切換按鈕以啟用或停用待命重新放置。

待命重新放置表示，如果主動或待命邏輯路由器執行所在的 Edge 節點失敗，即會在另一個 Edge 節點上建立新的待命邏輯路由器，以維持高可用性。如果失敗的 Edge 節點執行主動邏輯路由器，原始的待命邏輯路由器會變成主動邏輯路由器，並且會建立新的待命邏輯路由器。如果失敗的 Edge 節點執行待命邏輯路由器，新的待命邏輯路由器會加以取代。

- 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**。

結果

建立邏輯路由器之後，如果您想要從路由器的組態移除 Edge 叢集，請執行下列步驟：

- 按一下路由器的名稱來查看組態詳細資料。
- 選取**服務 > Edge 防火牆**。
- 按一下**停用防火牆**。

- 按一下**概觀**索引標籤，然後按一下**編輯**。
- 在 **Edge 叢集** 欄位中，按一下 **x** 圖示。
- 按一下**儲存**。

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**進階網路與安全性 > 網路 > 路由器**。
- 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。

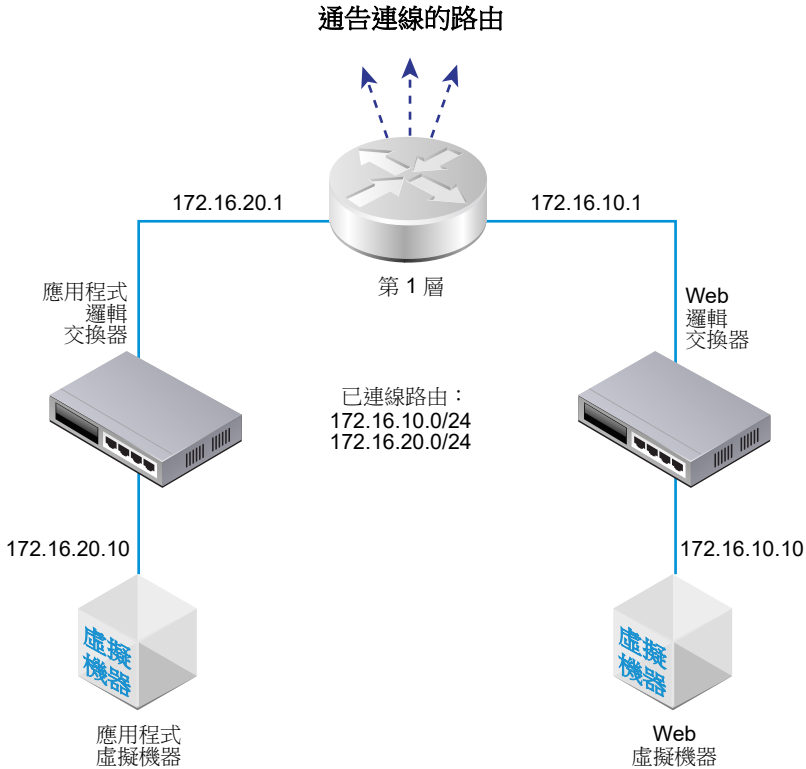
程序

- 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**進階網路與安全性 > 網路 > 路由器**。
- 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 13 章 邏輯交換器。
- 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**進階網路與安全性 > 網路 > 路由器**。
- 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

- 通告所有 DNS 轉寄站路由

- 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 0 層邏輯路由器](#)。

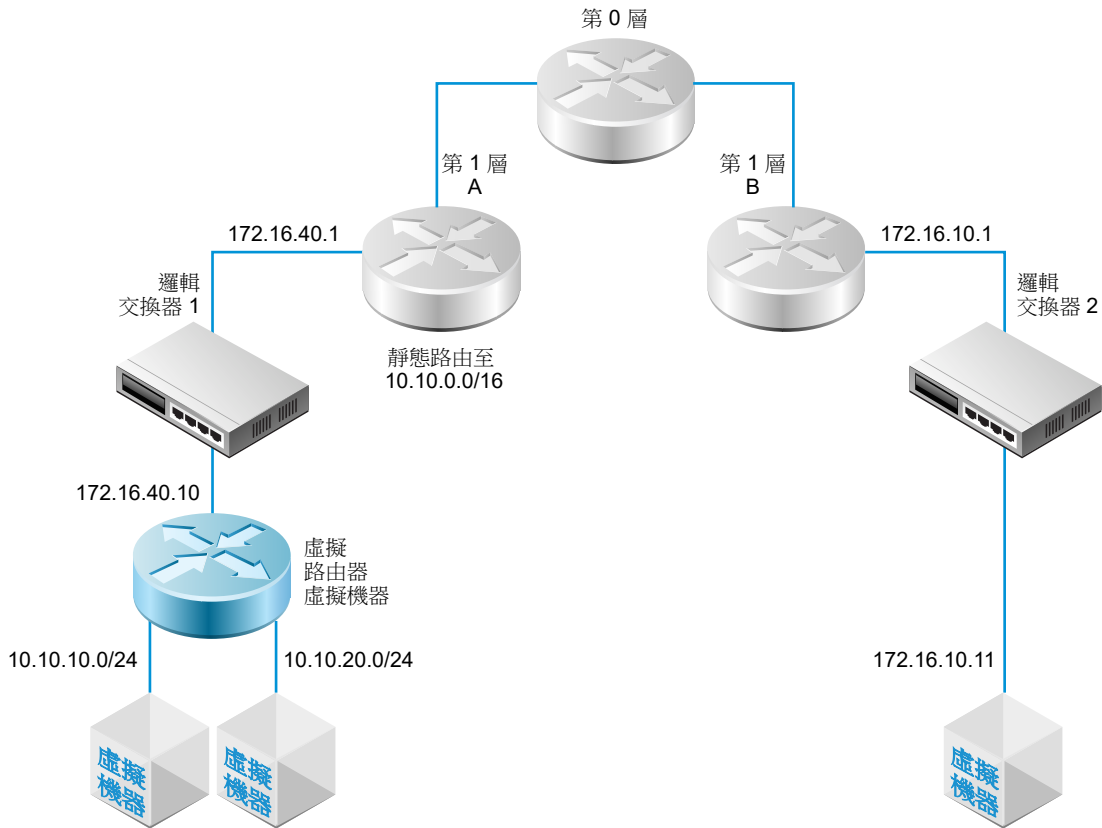
如果您已經有連線至第 1 層邏輯路由器的第 0 層邏輯路由器，則可以確認第 0 層路由器學習連線第 1 層路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

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 14-2. 第 1 層邏輯路由器靜態路由拓撲



支援遞迴靜態路由。

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**進階網路與安全性 > 網路 > 路由器**。
- 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。

支援以 IPv6 為基礎的靜態路由。IPv6 首碼只能有 IPv6 下一個躍點。

例如，10.10.10.0/16 或 IPv6 位址。

- 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。
- 支援 IPSec、DNAT、防火牆、負載平衡器等服務和服務插入的任何組合。對入口的處理順序為：IPSec – DNAT – 防火牆 – 負載平衡器 – 服務插入。對出口的處理順序為：服務插入 – 負載平衡器 – 防火牆 – DNAT – IPSec。

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。

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。
- 支援獨立路由器上的 ARP Proxy。您可以在 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 可以是 1.1.1.2。如果已正確設定路由，使 2.2.2.2 的流量可以到達獨立路由器，則虛擬 IP 也可以是另一個子網路中的 IP (例如 2.2.2.2)。
- 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。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 路由器 > 路由器 > 新增**。
- 3 選取**第 1 層路由器**，然後輸入邏輯路由器的名稱，並選擇性地輸入說明。
- 4 (必要) 選取要連線至這個第 1 層邏輯路由器的 NSX Edge 叢集。

5 (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。

6 按一下**新增**。

7 按一下您剛建立的路由器的名稱。

8 按一下**組態索引標籤**，然後選取**路由器連接埠**。

9 按一下**新增**。

10 輸入路由器連接埠的名稱，並選擇性地輸入說明。

11 在**類型**欄位中，選取**集中式**。

12 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。

13 (必要) 選取邏輯交換器。

14 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。

15 以 CIDR 標記法輸入路由器連接埠 IP 位址。

16 按一下**新增**。

第 0 層邏輯路由器

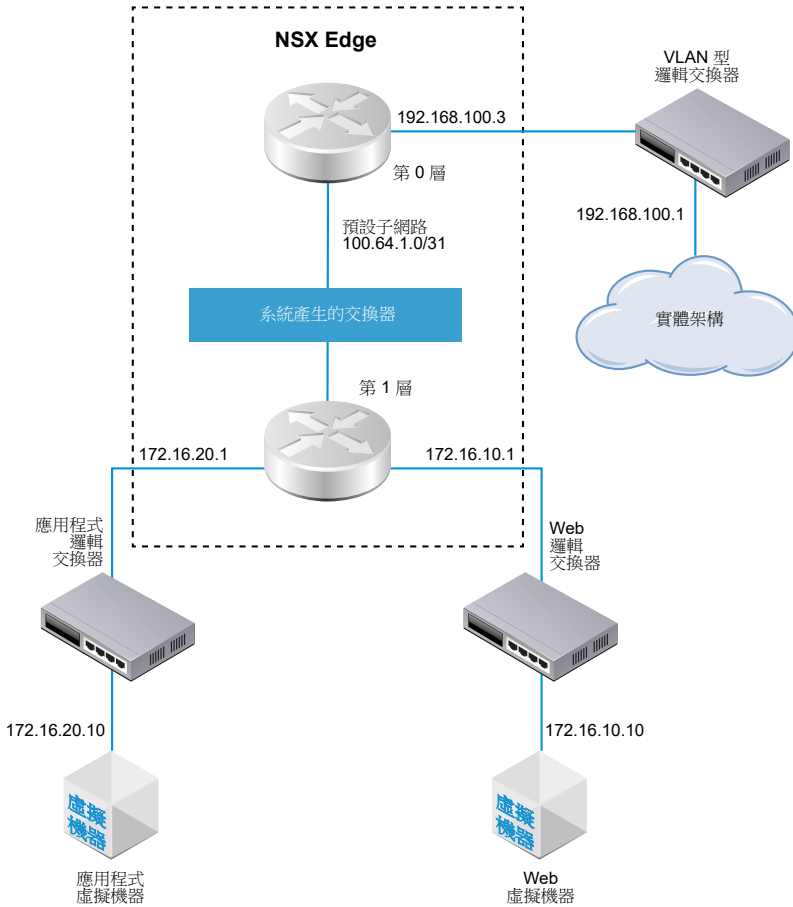
第 0 層邏輯路由器會在邏輯和實體網路之間提供閘道服務。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

Edge 節點僅支援一個第 0 層閘道或邏輯路由器。在建立第 0 層閘道或邏輯路由器時，請確定您建立的第 0 層閘道或邏輯路由器數目並未超過 NSX Edge 叢集中的 Edge 節點數目。

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 14-3. 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。

在某些情況下，外部用戶端會針對繫結至回送或 IKE IP 連接埠的 MAC 位址傳送 ARP 查詢。但是，回送和 IKE IP 連接埠沒有 MAC 位址且無法處理此類查詢。Proxy ARP 會在第 0 層邏輯路由器的上行和集中式服務連接埠上實作，以代表回送和 IKE IP 連接埠處理 ARP 查詢。

為第 0 層邏輯路由器設定了 DNAT、IPsec 和 Edge 防火牆時，將會依下列順序處理流量：IPsec、DNAT 和 Edge 防火牆。

在第 0 層或第 1 層邏輯路由器上，您可以設定不同類型的連接埠。其中一個類型稱為集中式服務連接埠 (CSP)。您必須在處於主動備用模式的第 0 層邏輯路由器上或第 1 層邏輯路由器上設定 CSP，才能連線至 VLAN 支援的邏輯交換器，或建立獨立的第 1 層邏輯路由器。CSP 在處於主動備用模式的第 0 層邏輯路由器上或第 1 層邏輯路由器上支援下列服務：

■ NAT

- 負載平衡
- 可設定狀態的防火牆
- VPN (IPsec 和 L2VPN)

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 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**進階網路與安全性 > 路由器 > 路由器 > 新增**。
- 3 從下拉式功能表中選取**第 0 層路由器**。
- 4 指派名稱給第 0 層邏輯路由器。
- 5 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。
- 6 (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。

- 7 (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。

- 8 (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 100.64.0.0/16。系統會為每個第 0 層至第 1 層的對等連線，提供一個在 100.64.0.0/16 位址空間內的 /31 子網路。

- 9 按一下**儲存**。

新的第 0 層邏輯路由器會顯示為連結。

- 10 (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。

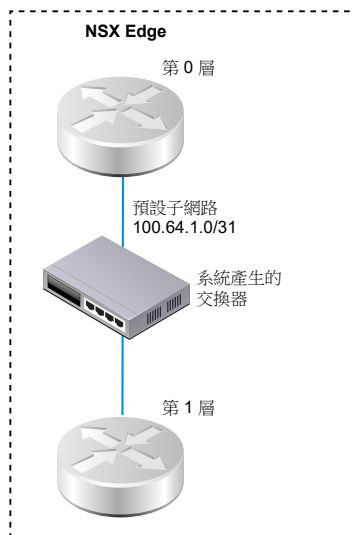
設定第 0 層邏輯路由器，將其連線至 VLAN 邏輯交換器以建立對外部網路的上行連接埠。請參閱[針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。

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 100.64.0.0/16。系統會為每個第 0 層至第 1 層的對等連線，提供一個在 100.64.0.0/16 位址空間內的 /31 子網路。您也可以在第 0 層的[摘要 > 進階](#)組態中選擇性地設定位址空間。

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[進階網路與安全性 > 網路 > 路由器](#)。
- 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

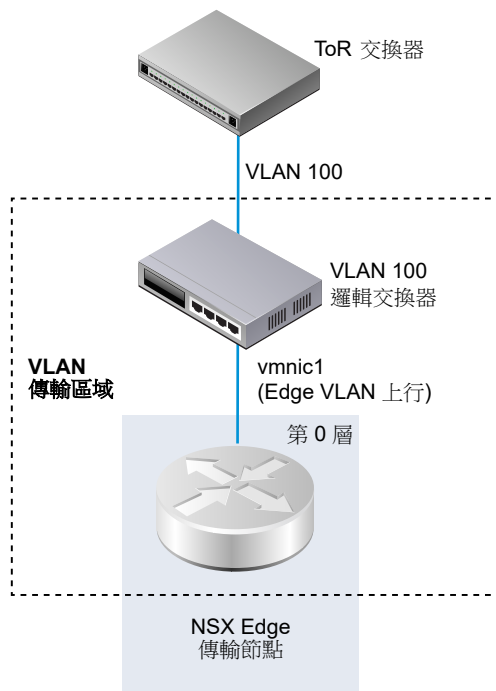
Total number of routes: 7

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**進階網路與安全性 > 網路 > 路由器**。
- 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 eBGP](#)。

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**進階網路與安全性 > 網路 > 路由器**。
- 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

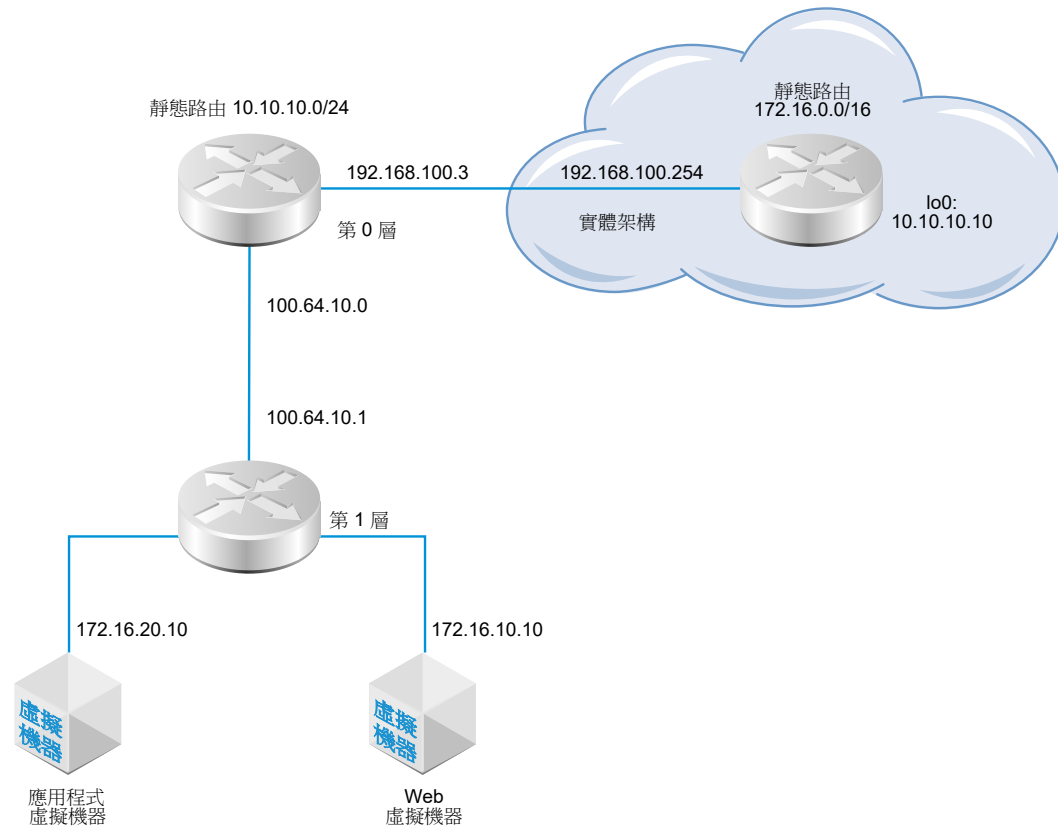
- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**進階網路與安全性 > 網路 > 路由器**。
- 3 按一下路由器的名稱。
- 4 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 5 按一下**新增**。
- 6 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 7 在**類型**欄位中，選取**集中式**。
- 8 對於 **URPF 模式**，請選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 9 (必要) 選取邏輯交換器。
- 10 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 14-4. 靜態路由拓撲



支援遞迴靜態路由。

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 選取進階網路與安全性 > 網路 > 路由器。
- 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 route 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。

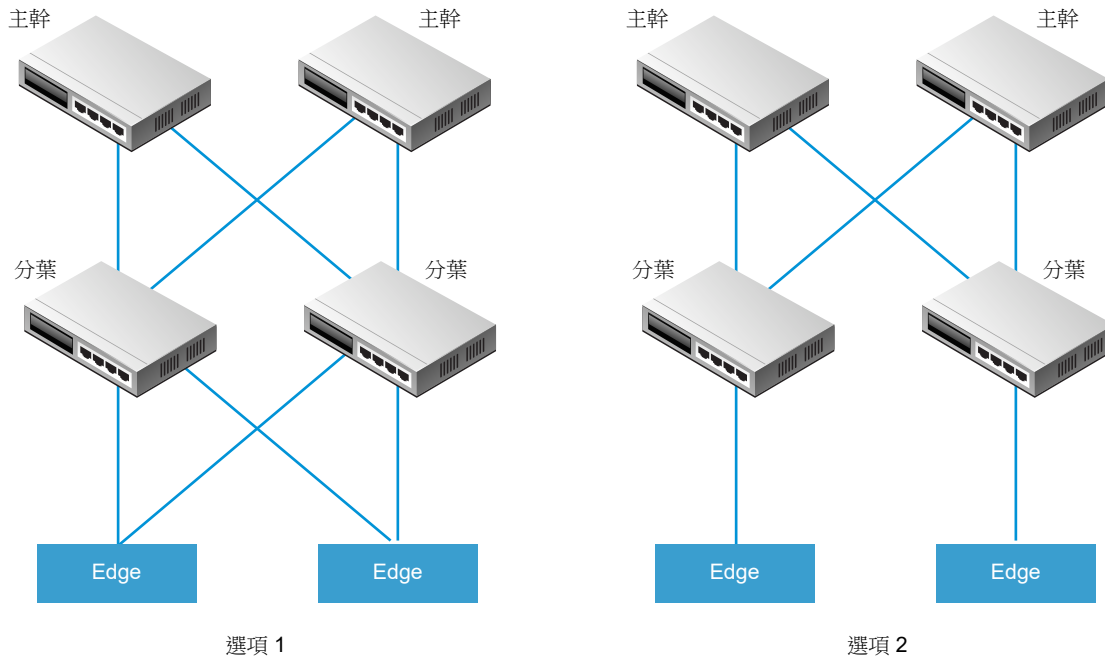
```
ping 10.10.10.10
```

```
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 eBGP

若要啟用虛擬機器與外部環境之間的存取，您可以設定第 0 層邏輯路由器與您實體基礎結構中的路由器之間的外部或內部 BGP (eBGP/iBGP) 連線。

在設定 eBGP 時，您必須設定第 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。

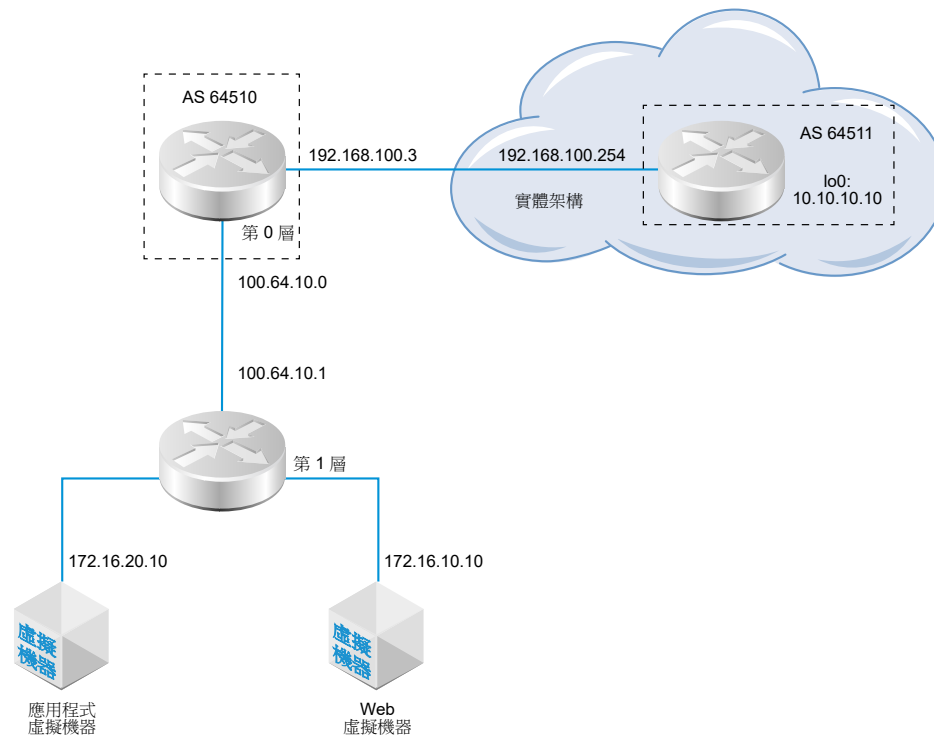
雙主動模式的第 0 層邏輯路由器支援 SR (服務路由器) 間的路由。在雙主動叢集中，如果 1 號路由器無法與南北向實體路由器進行通訊，流量就會重新路由至 2 號路由器。如果 2 號路由器能夠與該實體路由器進行通訊，則 1 號路由器與實體路由器之間的流量不受影響。

在具有的第 0 層邏輯路由器處於主動-待命模式連結至處於雙主動模式的第 1 層邏輯路由器拓撲中，您必須啟用 SR 間路由來處理非對稱路由。主動-待命如果您在其中一個 SR 上設定靜態路由，或如果某個 SR 必須連線到另一個 SR 的上行，則您具有非對稱路由。此外，請注意下列事項：

- 如果在其中一個 SR 上設定靜態路由 (例如，在 Edge 節點 #1 上的 SR #1)，另一個 SR (例如，Edge 節點 #2 上的 SR #2) 可能會從 eBGP 對等記住相同的路由，並在 SR #1 上的靜態路由優先使用記住的路由，此方式可能較有效率。若要確保 SR #2 使用 SR #1 上設定的靜態路由，請在先佔式模式中設定第 1 層邏輯路由器，並將 Edge 節點 #1 設定為慣用節點。
- 如果第 0 層邏輯路由器在 Edge 節點 #1 上有上行連接埠，以及在 Edge 節點 #2 有上另一個上行連接埠，如果這兩個上行位於不同子網路，則從承租人虛擬機器對上行執行 Ping 流量可運作。如果兩個上行位於相同的子網路，Ping 流量將會失敗。

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 14-5. BGP 連線拓撲



請注意，以下是發生 BGP 或 BFD 的相關連線失敗時的不同案例：

- 僅設定了 BGP 時，如果所有 BGP 芳鄰皆關閉，則服務路由器的狀態將是關閉。
- 僅設定了 BFD 時，如果所有 BFD 芳鄰皆關閉，則服務路由器的狀態將是關閉。
- 設定了 BGP 和 BFD 時，如果所有 BGP 和 BFD 芳鄰皆關閉，則服務路由器的狀態將是關閉。

- 設定了 BGP 和靜態路由時，如果所有 BGP 芳鄰皆關閉，則服務路由器的狀態將是關閉。
- 僅設定了靜態路由時，除非節點發生失敗或處於維護模式，否則服務路由器的狀態將一律為開啟。

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**進階網路與安全性 > 網路 > 路由器**。
- 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 輸入本機 AS 數目。
例如，64510。
 - b 按一下**狀態**切換按鈕以啟用或停用 BGP。
 - c 按一下 **ECMP** 切換按鈕以啟用或停用 ECMP。
 - d 按一下**正常重新啟動**切換按鈕以啟用或停用正常重新啟動。
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。
 - e 如果此邏輯路由器處於雙主動模式，請按一下 **SR 間路由**切換按鈕以啟用或停用 SR 間路由。
 - f 設定路由彙總。
 - g 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 指定躍點上限。
預設值為 1。
- 9 請輸入遠端 AS 數目。
例如，64511。
- 10 設定計時器 (保持連線時間及等候時間) 及密碼。

- 11 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 按一下**位址家族**索引標籤可新增位址家族。
- 13 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](#)。

在第 0 層邏輯路由器上設定 iBGP

您可以使用 API，為第 0 層邏輯路由器設定內部 BGP (iBGP)。設定 iBGP 後，第 0 層邏輯路由器可交換路由與連線資訊。

iBGP 功能具有下列功能與限制：

- 支援重新分配、首碼清單和路由對應。
- 不支援路由反映器。
- 不支援 BGP 聯邦。

此版本不支援使用 NSX Manager 使用者介面來設定 iBGP。

程序

- 1 呼叫下列 API 以新增 BGP 芳鄰，其中 `remote_as` 參數設定為與本機 AS 相同的值。例如，

```
POST https://<nsx-mgr>/api/v1/logical-routers/7a62a0c5-1ea1-4b25-9d43-dce1c0fa4b8c/routing/bgp/neighbors
{
  "display_name": "neighbor1",
  "neighbor_address": "2.2.2.2",
  "remote_as_num": "200",
  "maximum_hop_limit": 1,
  "enabled": true,
  "logical_router_id": "c831795d-dc7b-448c-92ce-21b16ec9a7ad",
  "address_families": [
    {
      "type": "IPV4_UNICAST",
      "enabled": true,
    }
  ],
  "remote_as": 200,
  "enable_bfd": false,
}
```

- 2 呼叫下列 API 以新增路由對應，其中 `nexthop_self` 參數設定為 **true**，而 `local_preference` 參數設定為 200。例如，

```
POST https://<nsx-mgr>/api/v1/logical-routers/7a62a0c5-1ea1-4b25-9d43-dce1c0fa4b8c/routing/route-
maps
{
  "description": "Route Map",
  "display_name": "Route Map",
  "logical_router_id": "c831795d-dc7b-448c-92ce-21b16ec9a7ad",
  "sequences": [
    {
      "match_criteria": {
        "match_community_expression": {
          "expression": [
            {
              "match_operator": "MATCH_ALL",
              "community_list_id": "c4b2b171-661b-4059-960c-fc931a612507"
            }
          ],
          "operator": "AND"
        }
      },
      "set_criteria": {
        "as_path_prepend" : "50",
        "weight" : 50,
        "community" : "30:40",
        "multi_exit_discriminator" : 10,
        "nexthop_self" : true,
        "local_preference" : 200
      },
      "action": "PERMIT"
    }
  ]
}
```

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 eBGP](#)。

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**進階網路與安全性 > 網路 > 路由器**。
- 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**進階網路與安全性 > 網路 > 路由器**。
- 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**編輯**以啟用或停用路由重新分配。

6 按一下**新增**以新增一組路由重新分配準則。

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 advertise-to-bgp-neighbor。
來源	選取一或多個下列來源： <ul style="list-style-type: none"> ■ TO 已連線 ■ TO 上行 ■ TO 下行 ■ TO CSP ■ TO 回送 ■ TO 靜態 ■ TO NAT ■ TO DNS 轉寄站 IP ■ TO IPsec 本機 IP ■ T1 已連線 ■ T1 CSP ■ T1 下行 ■ T1 靜態 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 轉寄站 IP
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。

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 eBGP](#)。
- 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。

```
traceroute 172.16.10.10
```

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

4 從內部虛擬機器對外部 IP 位址執行 Ping 偵測。

```
ping 10.10.10.10
```

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

後續步驟

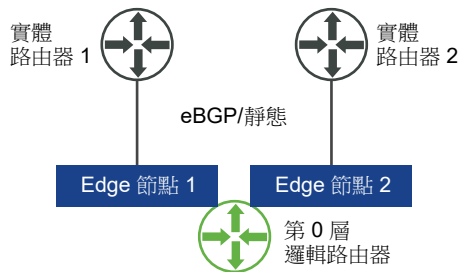
設定其他路由功能，例如 ECMP。

瞭解 ECMP 路由

相同成本多路徑 (ECMP) 路由通訊協定可透過對第 0 層邏輯路由器增加上行連接埠，並在 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。

第 0 層邏輯路由器必須處於雙主動模式，ECMP 才可供使用。最多支援八個 ECMP 路徑。

圖 14-6. ECMP 路由拓撲



例如，上方的拓撲顯示處於雙主動模式、在雙節點 NSX Edge 叢集上執行的單一第 0 層邏輯路由器。設定了一個上行連接埠，每個 Edge 節點上各一個。

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**進階網路與安全性 > 網路 > 路由器**。
- 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。
MTU	如果將此欄位保留為空白，則會使用預設值 1500。
傳輸節點	從下拉式功能表中指派 Edge 傳輸節點。
URPF 模式	單點傳播反向路徑轉送是一項安全功能。如果您有多個處於 ECMP 模式的雙主動 Edge 節點，建議您將其設為 無 。預設值為 嚴格 。
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**進階網路與安全性 > 網路 > 路由器**。
- 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 確認第 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。

- 8 在兩個 Edge 節點上啟動 SSH 工作階段。

- 9 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>
```

- 10 使用可從連線至第 0 層路由器之來源虛擬機器產生到目的地虛擬機器之流量的任何工具。

- 11 觀察兩個 Edge 節點上的流量。

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**進階網路與安全性 > 網路 > 路由器**。
- 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**進階網路與安全性 > 網路 > 路由器**。
- 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**進階網路與安全性 > 網路 > 路由器**。
- 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。

BGP 屬性	說明
加權	設定權重以影響路徑選擇。範圍為 0 - 65535。
社群	<p>以 aa:nn 格式指定社群，例如，300:500。或使用下拉式功能表選取下列其中一項：</p> <ul style="list-style-type: none"> ■ 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**進階網路與安全性 > 網路 > 路由器**。
- 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**。

您可以從**進階網路與安全性**索引標籤設定 NAT。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 [NSX Manager 概觀](#)。

本章節討論下列主題：

- [網路位址轉譯](#)

網路位址轉譯

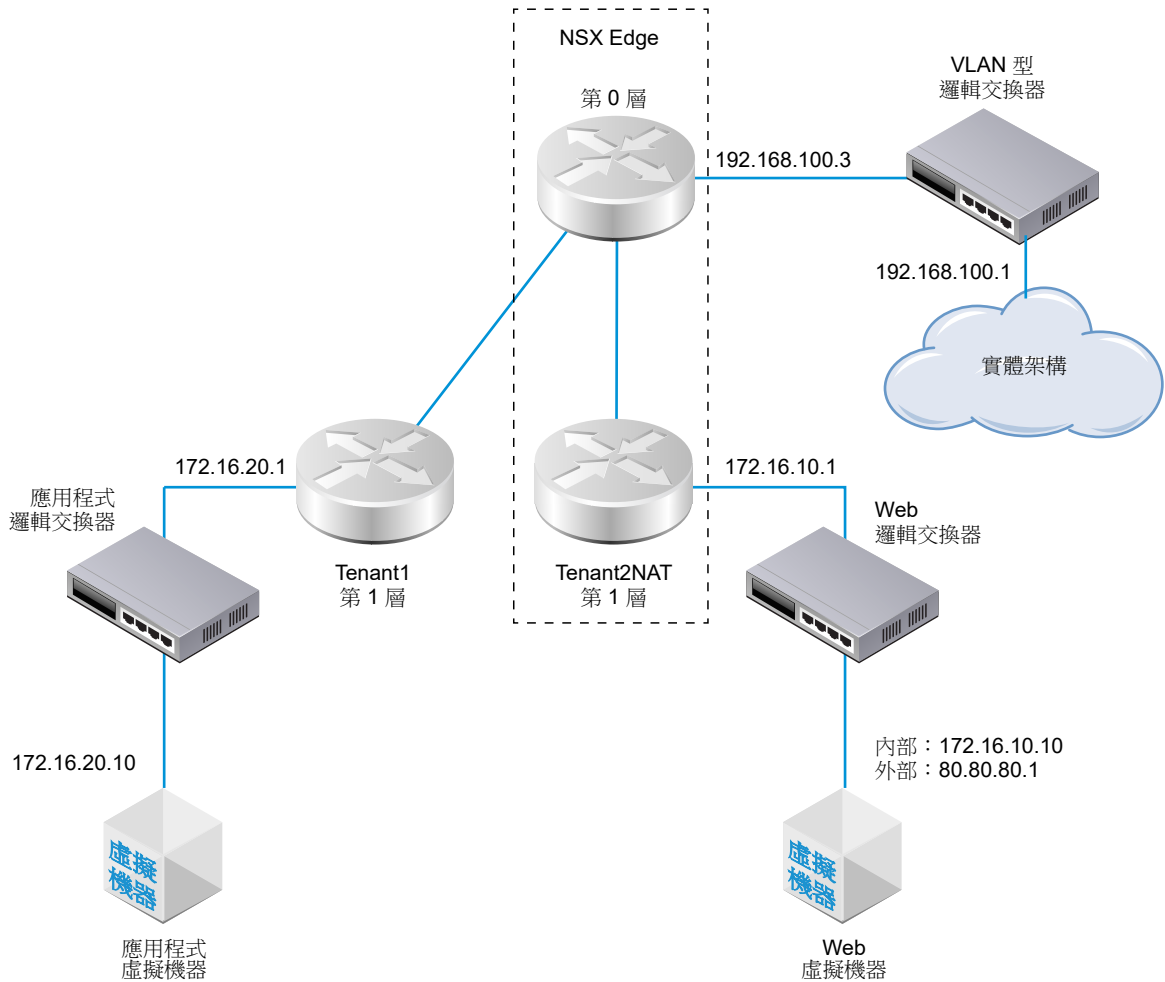
NSX-T Data Center 中的網路位址轉譯 (NAT) 可在第 0 層和第 1 層邏輯路由器中設定。

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 15-1. NAT 拓撲



第 1 層 NAT

第 1 層邏輯路由器支援來源 NAT (SNAT)、目的地 NAT (DNAT) 和自反 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 eBGP](#) 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**進階網路與安全性 > 網路 > 路由器**。
- 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 eBGP](#) 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 **進階網路與安全性 > 網路 > 路由器**。
- 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										
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**進階網路與安全性 > 網路 > 路由器**。
- 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 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
- 通告所有 **DNS** 轉寄站路由

- 6 按一下**儲存**。

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 按一下**編輯**以啟用或停用路由重新分配。

6 按一下**新增**以新增一組路由重新分配準則。

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 advertise-to-bgp-neighbor。
來源	<p>選取一或多個下列來源：</p> <ul style="list-style-type: none"> ■ TO 已連線 ■ TO 上行 ■ TO 下行 ■ TO CSP ■ TO 回送 ■ TO 靜態 ■ TO NAT ■ TO DNS 轉寄站 IP ■ TO IPsec 本機 IP ■ T1 已連線 ■ T1 CSP ■ T1 下行 ■ T1 靜態 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 轉寄站 IP
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。

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

主動備用模式下的第 0 層邏輯路由器支援來源 NAT (SNAT)、目的地 NAT (DNAT) 和自反 NAT。主動-主動式模式下的第 0 層邏輯路由器僅支援自反 NAT。

在第 0 層邏輯路由器上設定來源與目的地 NAT

您可以在以主動備用模式執行的第 0 層邏輯路由器上設定來源與目的地 NAT。

您也可以針對某個 IP 位址或位址範圍停用 SNAT 或 DNAT。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。

在第 0 層邏輯路由器的上行上設定的 SNAT 會處理來自第 1 層邏輯路由器的流量，以及來自該第 0 層邏輯路由器上另一個上行的流量。

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**進階網路與安全性 > 網路 > 路由器**。
- 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 針對**動作**，選取 **SNAT**、**DNAT**、**Reflexive**、**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。

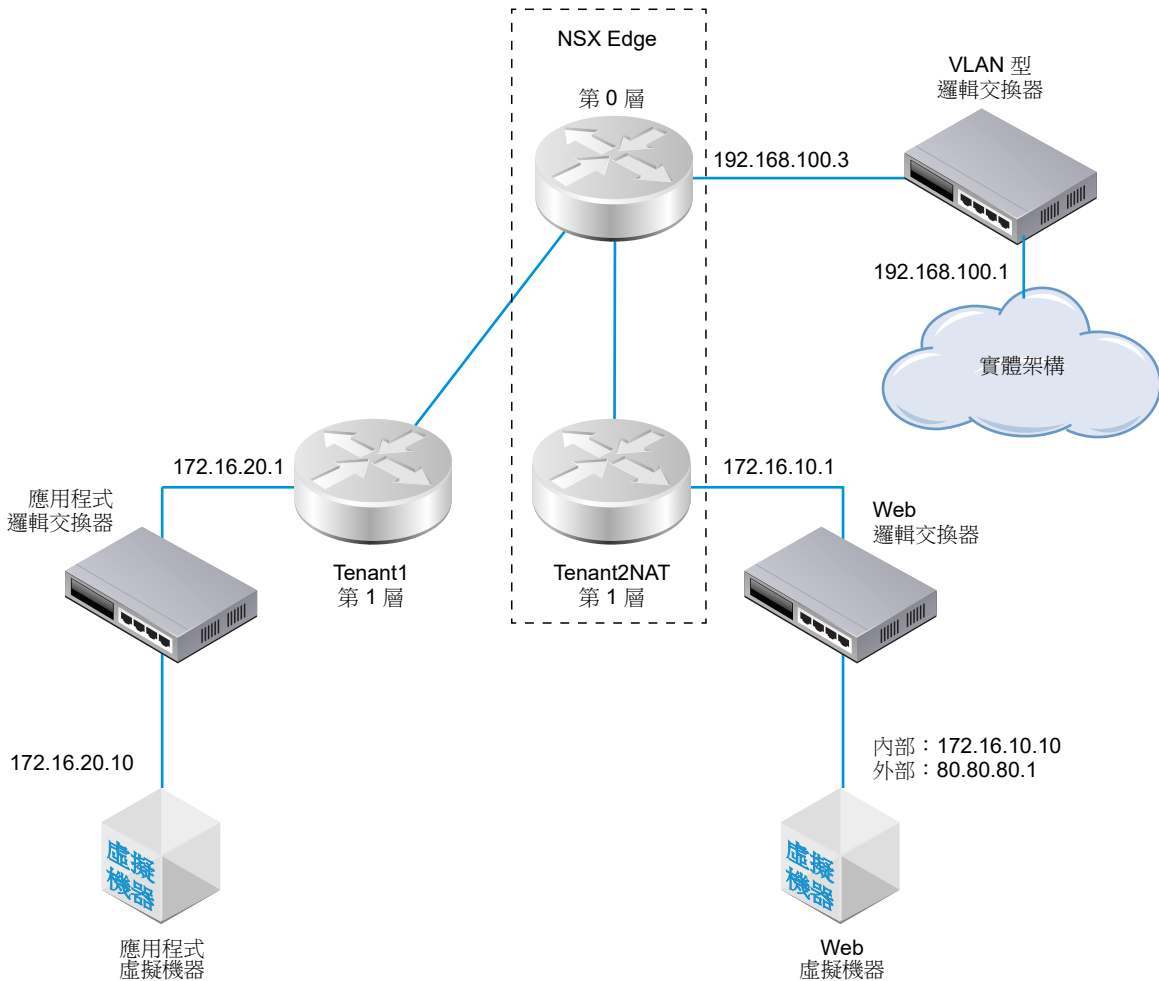
16 (選擇性) 變更防火牆略過設定。

此設定預設為啟用。

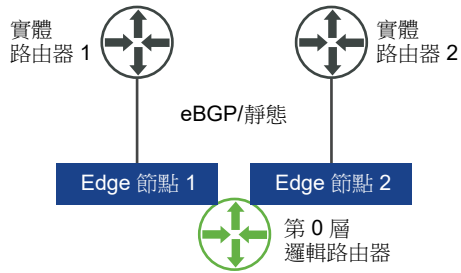
自反 NAT

當第 0 層邏輯路由器在主動-主動式模式中執行時，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。對於主動-主動式路由器，您可以設定自反 NAT (有時稱為無狀態 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。



涉及兩個主動-主動式第 0 層路由器時 (如下所示)，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**進階網路與安全性 > 網路 > 路由器**。
- 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										
✔ 2048	自反	任何	80.80.80.1	任何	任何	任何	172.16.10.10	任何		

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。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 [NSX Manager 概觀](#)。

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，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。此方法所建立的任何 IP 集合將不會在原則模式中顯示。在原則模式中，我們可以透過導覽至**詳細目錄 > 群組 > 設定成員**並指定 IP 或 MAC 位址來建立群組，以及將成員新增為 IP 位址、範圍、網路位址或 MAC 位址。

備註 防火牆規則的來源或目的地範圍支援 IPv4 位址和 IPv6 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**進階網路與安全性 > 詳細目錄 > 群組 > IP 集合 > 新增**。
- 3 輸入名稱。
- 4 (選擇性) 輸入說明。

- 5 在**成員**中，在以逗號分隔的清單中輸入個別 IP 位址、IP 範圍和子網路。
- 6 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**進階網路與安全性 > 詳細目錄 > 群組 > IP 集區 > 新增**。
- 3 輸入新 IP 集區的名稱。
- 4 (選擇性) 輸入說明。
- 5 按一下**新增**。
- 6 按一下 IP 範圍儲存格，然後輸入 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。
- 7 (選擇性) 輸入開道。
- 8 輸入包含尾碼的 CIDR IP 位址。
- 9 (選擇性) 輸入 DNS 伺服器。
- 10 (選擇性) 輸入 DNS 尾碼。
- 11 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**進階網路與安全性 > 詳細目錄 > 群組 > MAC 集合 > 新增**。
- 3 輸入名稱。
- 4 (選擇性) 輸入說明。
- 5 在以逗號分隔的清單中輸入 MAC 位址。
- 6 按一下**新增**。

建立 NSGroup

NSGroup 可設定為包含 IP 集合、MAC 集合、邏輯連接埠、邏輯交換器以及其他 NSGroup。也可以在防火牆規則的 **Applied To** 欄位中指定包含邏輯交換器、邏輯連接埠與虛擬機器的 NSGroup 做為來源及目的地。在分散式防火牆的 **Applied To** 欄位中，將忽略包含 IPset 和 MACSet 的 NSGroup。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

NSGroup 具有下列特性：

- 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，新增 NSGroup-3 並指定 NSGroup-2 做為成員。NSGroup-3 現在具有直接成員 NSGroup-2，以及有效成員 LogicalSwitch-1 和 LogicalSwitch-2。從主要群組資料表中，按一下群組並選取**相關 > NSGroup** 會顯示 NSGroup-1、NSGroup-2 和 NSGroup-3，因此這三個群組都直接或間接地將 LogicalSwitch-1 設為成員。
- 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。NSX Manager 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。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。
 - 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 = ...`。
 - 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:...`。
- 支援的虛擬機器數目上限為 10,000。
- 您最多可以建立 10,000 個 NSGroup。

對於所有可新增至 NSGroup 做為成員的物件，您可以導覽至任何物件的畫面，並選取**相關 > NSGroup**。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**進階網路與安全性 > 詳細目錄 > 群組 > 新增**。
- 3 輸入 NSGroup 的名稱。
- 4 (選擇性) 輸入說明。

5 (選擇性) 按一下**成員資格準則**。

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。可用成員準則可套用至下列項目：

- **邏輯連接埠** - 可以指定標籤和選用範圍。
- **邏輯交換器** - 可以指定標籤和選用範圍。
- **虛擬機器** - 可以指定等於、包含、開頭為、結尾為或不等於某個特定字串的名稱、標記、電腦作業系統名稱或電腦名稱。
- **傳輸節點** - 可以指定等於某個 **Edge** 節點或主機節點的節點類型。

6 (選擇性) 按一下**成員**以選取成員。

可用成員類型為：

- **AD 群組** - 包含 ADGroup 的 NSGroup 只能在分散式防火牆規則的 **extended_source** 欄位中使用，且必須是群組中的唯一成員。例如，不能有同時將 ADGroup 和 IPSet 做為成員的 NSGroup。
- **IP 集合** - 可以同時包含 IPv4 和 IPv6 位址。
- **邏輯連接埠** - 可以同時包含 IPv4 和 IPv6 位址。
- **邏輯交換器** - 可以同時包含 IPv4 和 IPv6 位址。
- **MAC 集合**
- **NSGroup**
- **傳輸節點**
- **VIF**
- **虛擬機器**

7 按一下**新增**。

該群組將新增到群組的資料表。按一下群組名稱來顯示概觀並編輯群組資訊，包括成員資格準則、成員、應用程式以及相關群組。捲動至**概觀**索引標籤的底部以新增和刪除標記。如需詳細資訊，請參閱[將標籤新增至物件](#)。選取**相關 > NSGroup** 會顯示將所選 NSGroup 做為成員的所有 NSGroup。

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**進階網路與安全性 > 詳細目錄 > 服務 > 新增**。
- 3 輸入名稱。
- 4 (選擇性) 輸入說明。
- 5 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。
- 6 對於個別服務，請選取服務類型和通訊協定。
可用類型包括**乙太、IP、IGMP、ICMP、ALG 和 L4 連接埠集合**。
- 7 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**。
- 8 按一下**新增**。

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**進階網路與安全性 > 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]。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 選取導覽面板中的**詳細目錄 > 虛擬機器**。

4 選取虛擬機器。

5 按一下**管理標記**。

6 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 。

可從 NSX Manager 指派給虛擬機器的標籤數目上限為 25。其他所有受管理物件 (例如邏輯交換器或連接埠) 的標籤數目上限為 30。

7 按一下**儲存**。

您可以從**進階網路與安全性**索引標籤設定 DHCP。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

本章節討論下列主題：

- **DHCP**
- **中繼資料 Proxy**

DHCP

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

您可以建立 DHCP 伺服器來處理 DHCP 要求，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。

在此版本中，DHCP 伺服器不支援客體 VLAN 標記。

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**進階網路與安全性 > 網路 > DHCP > 伺服器設定檔 > 新增**。
- 3 輸入名稱和 (選用) 說明。
- 4 從下拉式功能表中選取 NSX Edge 叢集。
- 5 (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**進階網路與安全性 > 網路 > DHCP > 伺服器 > 新增**。
- 3 輸入名稱和 (選用) 說明。
- 4 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`。
- 5 (必要) 從下拉式功能表中選取 DHCP 設定檔。
- 6 (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。
- 7 (選擇性) 輸入無類別靜態路由選項。
- 8 (選擇性) 輸入其他選項。
- 9 按一下**儲存**。
- 10 選取新建立的 DHCP 伺服器。
- 11 展開 [IP 集區] 區段。
- 12 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。
- 13 展開 [靜態繫結] 區段。
- 14 按一下**新增**，以新增 MAC 位址和 IP 位址之間的靜態繫結、預設閘道、主機名稱、租用持續時間、無類別靜態路由選項和其他選項。

後續步驟

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

將 DHCP 伺服器連結至邏輯交換器

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

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 網路 > 交換**。
 - a 按一下邏輯交換器的核取方塊。
 - b 按一下**動作 > 連結 DHCP 伺服器**。
- 3 或者，選取**進階網路與安全性 > DHCP**。
 - a 按一下**伺服器**索引標籤。
 - b 按一下 DHCP 伺服器的核取方塊。
 - c 按一下**動作 > 連結至邏輯交換器**。

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**進階網路與安全性 > 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 或 DHCPv6 伺服器。當您建立 DHCP/DHCPv6 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**進階網路與安全性 > 網路 > DHCP > 轉送設定檔 > 新增**。
- 3 輸入名稱和 (選用) 說明。
- 4 輸入一或多個外部 DHCP/DHCPv6 伺服器位址。

後續步驟

建立 DHCP/DHCPv6 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**進階網路與安全性 > 網路 > DHCP > 轉送服務 > 新增**。
- 3 輸入名稱和 (選用) 說明。
- 4 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 轉送服務新增至邏輯路由器連接埠](#)。

將 DHCP 轉送服務新增至邏輯路由器連接埠

您可以將 DHCP 轉送服務新增至邏輯路由器連接埠。連結至該連接埠之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](#)。
- 確認路由器連接埠的類型為下行。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**進階網路與安全性 > 網路 > 路由器**。
- 3 選取適當的路由器，以顯示更多資訊和組態選項。
- 4 選取**組態 > 路由器連接埠**。
- 5 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**。
- 6 從 **轉送服務** 下拉式清單中選取 DHCP 轉送服務，然後按一下**儲存**。

當您新增邏輯路由器連接埠時，也可以選取 DHCP 轉送服務。

刪除 DHCP 租用

在某些情況下，您可能會想要刪除 DHCP 租用。例如，您想要讓 DHCP 用戶端取得不同的 IP 位址，或是在用戶端未釋放其 IP 位址即關閉的情況下，讓該位址可供其他用戶端使用。

您可以使用下列 API 來刪除 DHCP 租用：

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```


若要確保能夠移除正確的租用，請在 **DELETE API** 之前和之後呼叫下列 API：

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

呼叫 **DELETE API** 之後，請確定 **GET API** 的輸出並未顯示已刪除的租用。

如需詳細資訊，請參閱《NSX-T Data Center API 參考》。

中繼資料 Proxy

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

下列步驟描述中繼資料 Proxy 的運作方式：

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

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

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 **進階網路與安全性 > 網路 > DHCP > 中繼資料 Proxy > 新增**。
- 3 輸入中繼資料 Proxy 伺服器的名稱。
- 4 (選擇性) 輸入說明。
- 5 輸入 Nova 伺服器的 URL 和連接埠。
有效的連接埠範圍為 3000 - 9000。
- 6 輸入密碼的值。
- 7 從下拉式清單中選取 NSX Edge 叢集。
- 8 (選擇性) 選取 NSX Edge 叢集的成員。

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**進階網路與安全性 > 網路 > DHCP > 中繼資料 Proxy**。
- 3 選取中繼資料 Proxy 伺服器。
- 4 選取功能表選項**動作 > 連結至邏輯交換器**
- 5 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**進階網路與安全性 > 網路 > DHCP > 中繼資料 Proxy**。
- 3 選取中繼資料 Proxy 伺服器。
- 4 選取功能表選項**動作 > 從邏輯交換器中斷連結**
- 5 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 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》。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

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 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**進階網路與安全性 > 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**進階網路與安全性 > 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**。

進階負載平衡

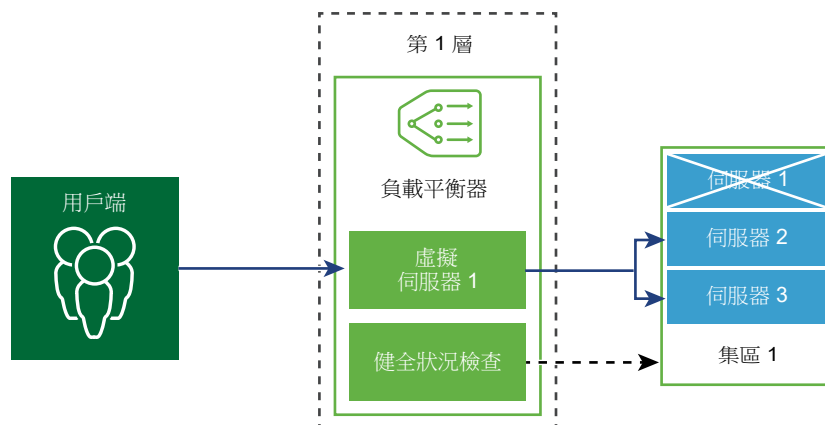
19

本資訊涵蓋可在**進階網路與安全性**索引標籤底下所找到的 NSX-T Data Center 負載平衡組態。

如需 NSX 進階負載平衡器 (Avi 網路) 的相關資訊，請參閱 <https://www.vmware.com/products/nsx-advanced-load-balancer.html>。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

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：

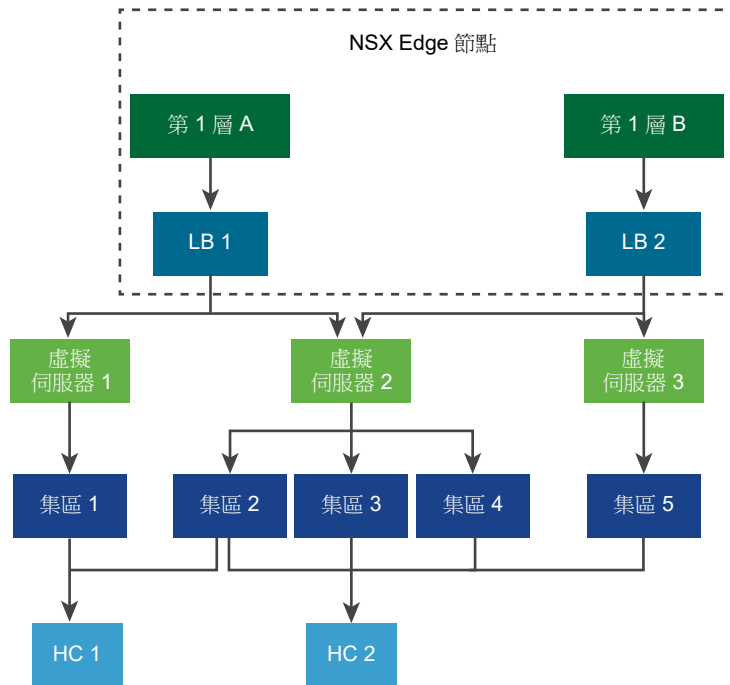
- [主要負載平衡器概念](#)
- [設定負載平衡器元件](#)

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。

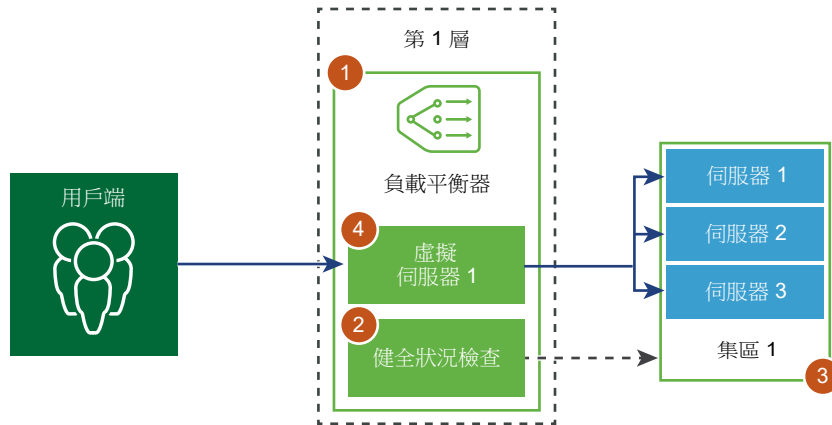
若要測試每個伺服器是否正確執行應用程式，您可以新增用於檢查伺服器健全狀況狀態的健全狀況檢查監視器。



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。

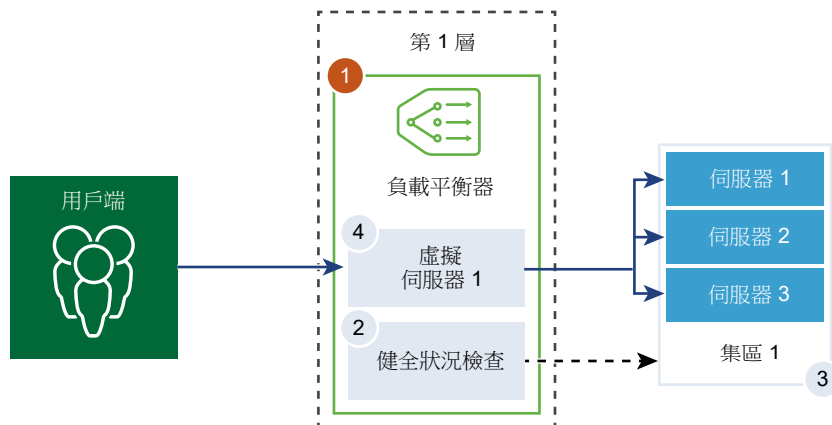


建立負載平衡器

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**進階網路與安全性 > 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

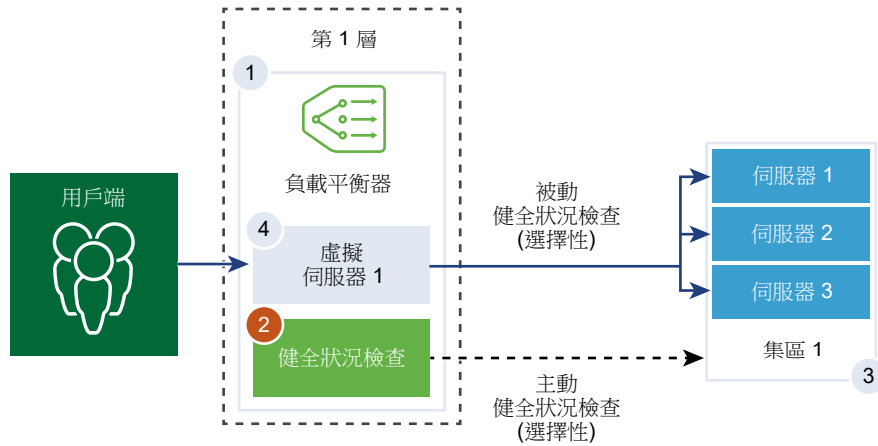
主動健全狀況監視器可用來測試伺服器是否可用。主動健全狀況監視器使用數種類型的測試，例如傳送基本 Ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

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 層閘道 (先前稱為第 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。

如果第 1 層閘道連線至第 0 層閘道，則會建立路由器連結連接埠，且其 IP 位址 (一般為 100.64.x.x 格式) 會用來為負載平衡器服務執行健全狀況檢查。如果第 1 層閘道為獨立 (僅具有一個集中式的服務連接埠並且未連線至第 0 層閘道)，則會使用集中式服務連接埠 IP 位址來為負載平衡器服務執行健全狀況檢查。如需獨立第 1 層閘道的詳細資訊，請參閱[建立獨立的第 1 層邏輯路由器](#)。

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 **進階網路與安全性 > 網路 > 負載平衡器 > 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。

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用於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。

選項	說明
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	從下拉式功能表選取用於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 **進階網路與安全性 > 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。

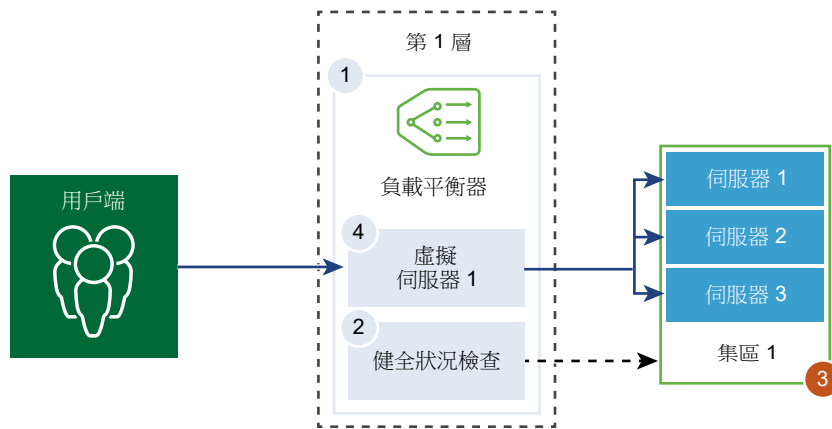
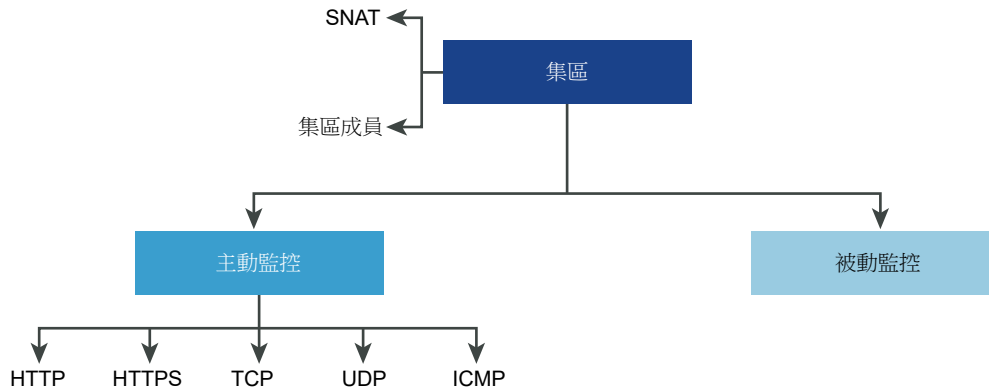


圖 19-1. 伺服器集區參數組態

**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

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 網路 > 負載平衡器 > 伺服器集區 > 新增**。
- 3 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。
- 4 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：

- 管理狀態設為 **DISABLED**。
- 管理狀態設為 **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 **DOWN**。
- 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)。

選項	說明
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在可用的伺服器資源之間公平地散佈負載。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。如果作用中成員未通過健全狀況檢查，流量就會容錯移轉給備用成員。

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。

設定伺服器集區的主動和被動健全狀況監視器為選用。當您選取主動健全狀況監視器，且第 1 層閘道已連線至第 0 層閘道，則會建立路由器連結連接埠。路由器連結連接埠的 IP 位址 (一般為 100.64.x.x 格式) 會用來為負載平衡器服務執行健全狀況檢查。如果第 1 層閘道為獨立 (僅具有一個集中式的服務連接埠並且未連線至第 0 層閘道)，則會使用集中式服務連接埠 IP 位址來為負載平衡器服務執行健全狀況檢查。如需獨立第 1 層閘道的詳細資訊，請參閱[建立獨立的第 1 層邏輯路由器](#)。

新增防火牆規則以允許該 IP 位址要為負載平衡器服務執行健全狀況檢查。

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。

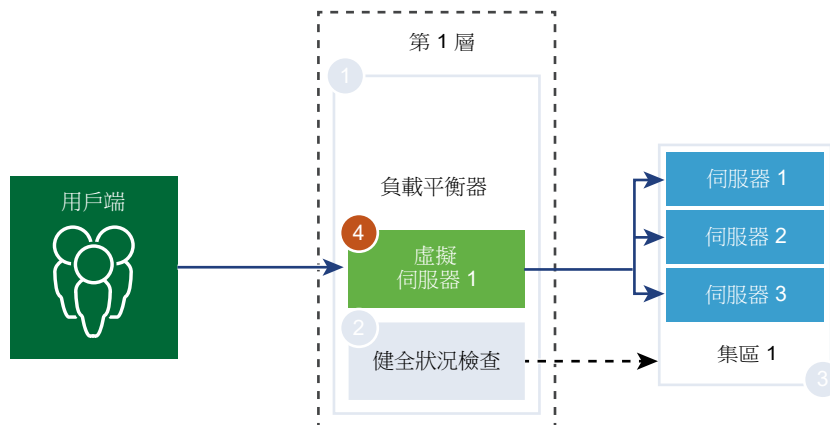
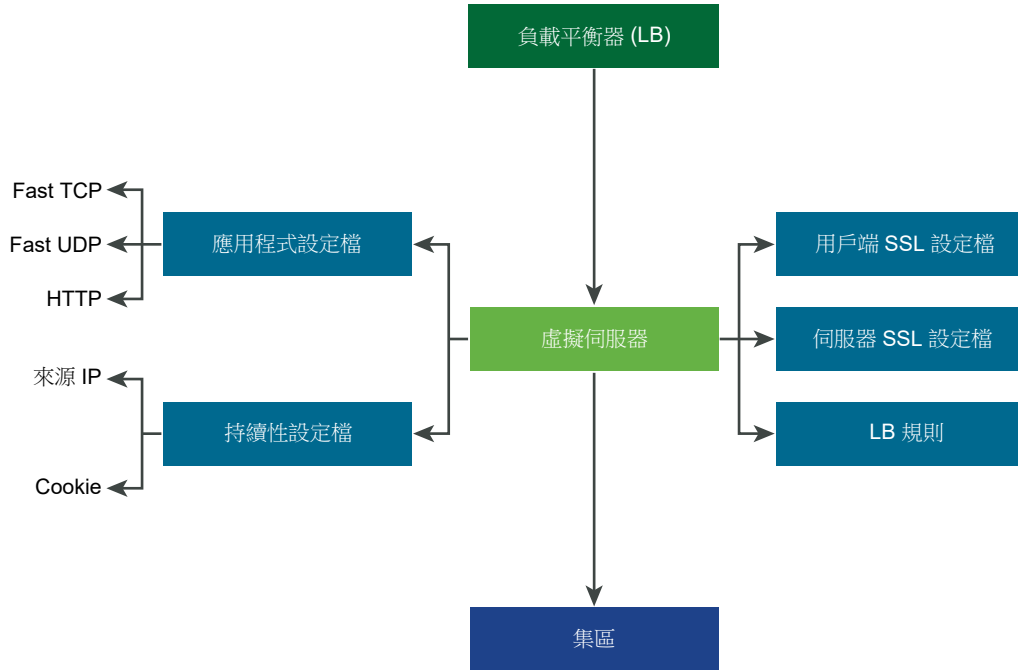


圖 19-2. 虛擬伺服器元件



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 19-3. 第 4 層 TCP 和 UDP 應用程式設定檔

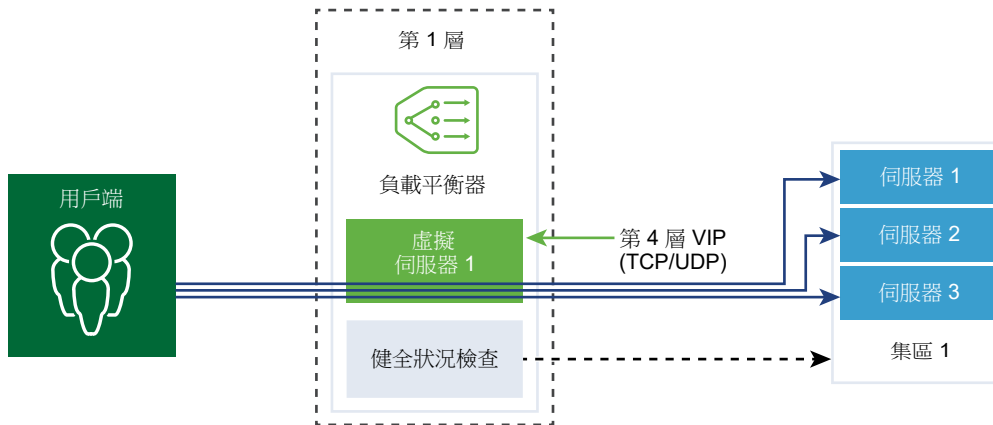
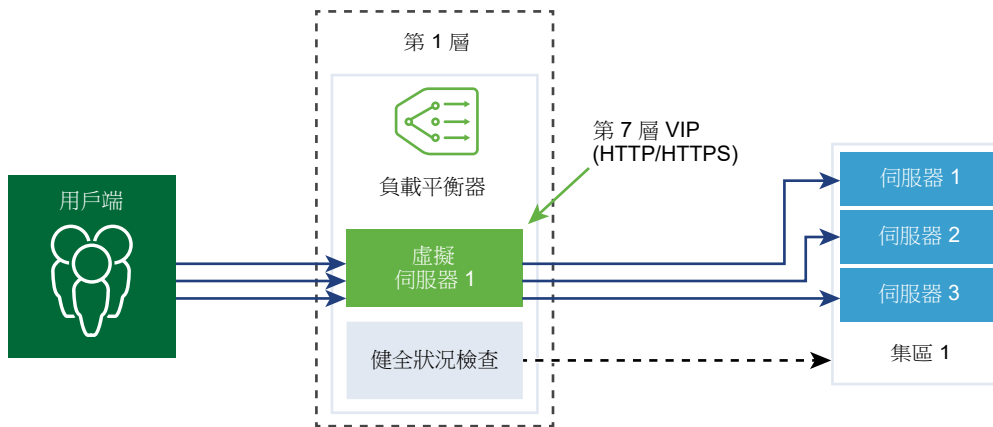


圖 19-4. 第 7 層 HTTPS 應用程式設定檔



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 **進階網路與安全性 > 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 - 如果傳入要求中沒有 XFF HTTP 標頭存在，則負載平衡器會插入具有用戶端 IP 位址的新 XFF 標頭。如果傳入要求中有 XFF HTTP 標頭存在，則負載平衡器會附加具有用戶端 IP 位址的 XFF 標頭。 ■ 取代 - 如果傳入要求中有 XFF HTTP 標頭存在，則負載平衡器會取代標頭。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。

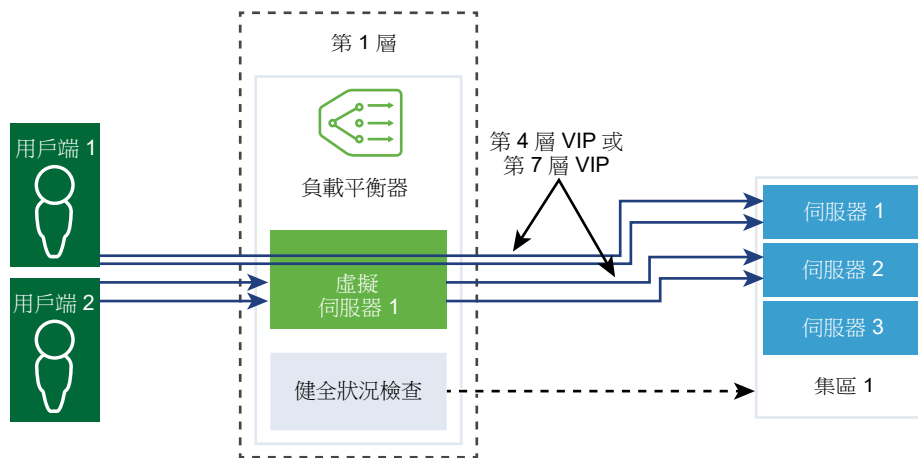
設定持續性設定檔

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 **進階網路與安全性 > 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。 工作階段 Cookie 不會儲存，且將在瀏覽器關閉後遺失。 持續性 Cookie 會儲存在瀏覽器中，且不會在瀏覽器關閉後遺失。
閒置時間上限	輸入 Cookie 在到期之前可閒置的時間 (以秒為單位)。
Cookie 存留期上限	僅適用於 工作階段 Cookie 。輸入 Cookie 可處於作用中狀態的存留期上限 (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 19-5. SSL 卸載

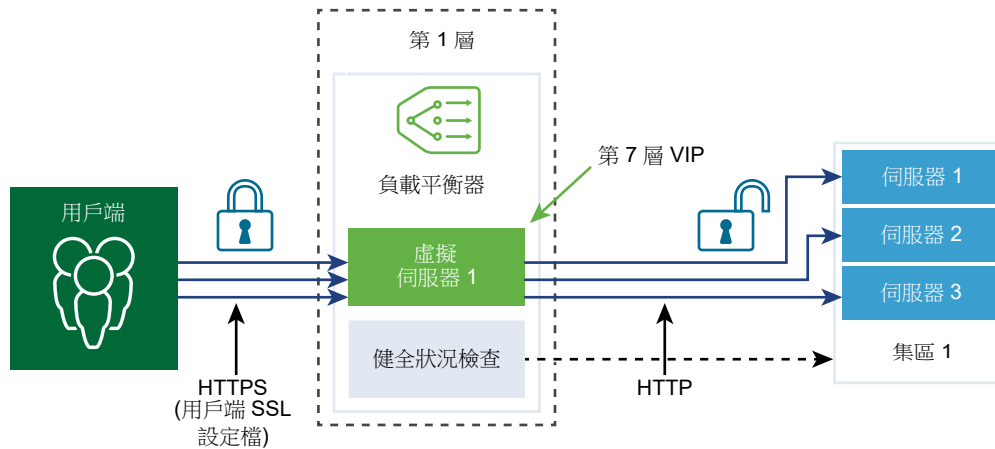
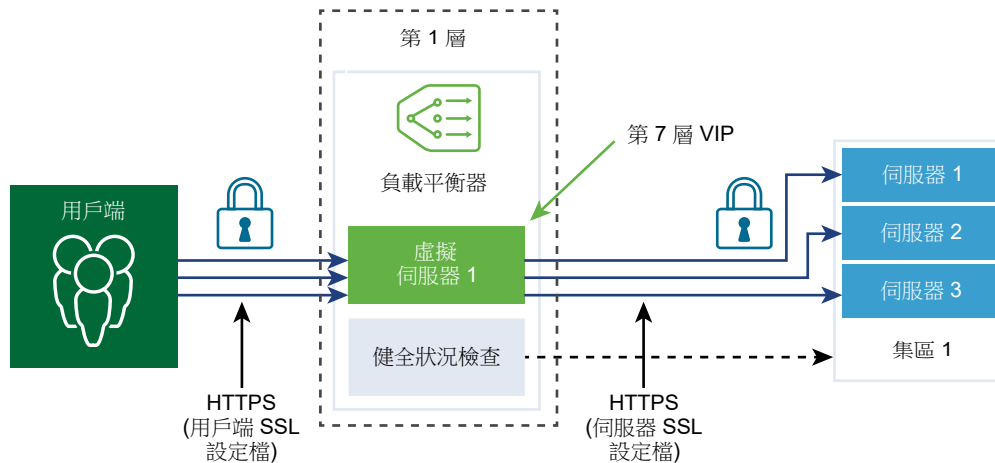


圖 19-6. 端對端 SSL



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**進階網路與安全性 > 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 **進階網路與安全性 > 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**進階網路與安全性 > 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:sensitive)`」，改為使用「`Case ((?i:sensitive))`」。
- 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
- `$_ssl_ciphers` - 傳回用戶端 SSL 加密方式
- `$_ssl_client_i_dn` - 根據 RFC 2253 傳回所建立 SSL 連線用戶端憑證的「簽發者 DN」字串
- `$_ssl_client_s_dn` - 根據 RFC 2253 傳回所建立 SSL 連線用戶端憑證的「主體 DN」字串

- `$_ssl_protocol`: 傳回所建立 SSL 連線的通訊協定
- `$_ssl_session_reused`: 如果重複使用 SSL 工作階段，則傳回「r」，否則傳回「.」

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。 <code>http_request.method</code> - 要比對的值
HTTP 要求 URI	比對不含查詢引數的 HTTP 要求 URI。 <code>http_request.uri</code> - 要比對的值
HTTP 要求 URI 引數	比對 HTTP 要求 URI 查詢引數。 <code>http_request.uri_arguments</code> - 要比對的值
HTTP 要求版本	比對 HTTP 要求版本。 <code>http_request.version</code> - 要比對的值
HTTP 要求標頭	比對任何 HTTP 要求標頭。 <code>http_request.header_name</code> - 要比對的標頭名稱 <code>http_request.header_value</code> - 要比對的值

支援的比對條件	說明
HTTP 要求裝載	比對 HTTP 要求的內文內容。 http_request.body_value - 要比對的值
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 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 Fast 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前往 [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**。

備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

本章節討論下列主題：

- **防火牆區段和防火牆規則**

防火牆區段和防火牆規則

防火牆區段用於群組一組防火牆規則。

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

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

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

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。

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**進階網路與安全性 > 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**進階網路與安全性 > 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**進階網路與安全性 > 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 ESXi 和 KVM 主機上的 /var/log/dfwptlogs.log 檔案中。

程序

- 1 選取**進階網路與安全性 > 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 TCP 嚴格可以每個區段為基礎啟用，以關閉中間工作階段接聽並強制執行三向信號交換的要求。當針對特定分散式防火牆區段啟用 TCP 嚴格模式，且使用預設「任何-任何」封鎖規則時，系統將捨棄並未完成三向信號交換連線要求，且符合中此區段中以 TCP 為基礎之規則的封包。嚴格僅適用於可設定狀態的 TCP 規則，且會在分散式防火牆區段層級上啟用。TCP 嚴格不會針對符合未指定任何 TCP 服務之預設「任何-任何」允許的封包強制執行。

表 20-1. 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。來源或目的地範圍同時支援 IPv4 和 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。來源或目的地範圍同時支援 IPv4 和 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/dfwpktlogs.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 輸入 、 輸出 及 輸入/輸出 。預設為 輸入/輸出 。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**進階網路與安全性 > 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/dfwptlogs.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、規則標籤及註解。

- 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**進階網路與安全性 > 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**進階網路與安全性 > 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**進階網路與安全性 > 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**進階網路與安全性 > 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**進階網路與安全性 > 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**進階網路與安全性 > 安全性 > Distributed Firewall > 排除清單 > 新增**。
- 2 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**。
- 3 按一下**確定**。
- 4 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 Distributed Firewall

您可以啟用或停用 Distributed Firewall 功能。

如果已停用，則不會在數據平面層級強制執行任何防火牆規則。此時，會重新強制執行重新啟用規則。

程序

- 1 導覽到 **進階網路與安全性 > 安全性 > Distributed Firewall**。
- 2 按一下**設定**索引標籤。
- 3 按一下 Distributed Firewall **編輯**。
- 4 在對話方塊中，將防火牆狀態切換為綠色 (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。

Edge 防火牆功能會在上行路由器連接埠上實作，這表示只有在流量抵達 Edge 上的上行路由器連接埠時，才會套用防火牆規則。若要將防火牆規則套用至特定 IP 目的地，您必須設定 /32 網路的群組。如果您提供 /32 以外的子網路，防火牆規則將會套用至整個子網路。

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**進階網路與安全性 > 網路 > 路由器**。
- 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到邏輯路由器。
- 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。

使用 API 的 CPU 和記憶體使用率臨界值

使用服務組態 API，將 CPU 和記憶體使用率臨界值套用到分散式防火牆規則。實作服務組態 API 時，您可以將設定檔組態套用到諸如虛擬機器群組、傳輸節點、邏輯交換器和邏輯連接埠之類的實體。

取得服務組態詳細資料

如需語法和用法詳細資料，請參閱《NSX-T Data Center API》指南。

所有服務組態的清單。

```
GET https://<nsx-mgr>/api/v1/service-configs
```

表 20-2. API 屬性

屬性	詳細資料
設定檔	<p>設定檔是套用到虛擬機器群組的組態。</p> <p>例如，<code>FirewallSessionTimerProfile</code> 是套用到傳輸節點以收集分散式防火牆規則執行時有關傳輸節點之 CPU 使用率的詳細資料的設定檔。</p> <p>備註 服務組態中只能包含一個設定檔。</p>
Applied_To	套用服務設定檔的虛擬機器群組。
優先順序	<p>會依設定檔類型套用優先順序。</p> <p>NSX-T Data Center 決定依遞增的優先順序數字必須套用到虛擬機器群組之設定檔的優先順序。</p> <p>例如，序號為 1 的設定檔的優先順序高於序號為 2 的設定檔。</p>

建立服務組態

建立可以群組設定檔和組態的服務組態。

```
POST https://<nsx-mgr>/api/v1/service-config
{
  "display_name": "testServiceConfig",
  "profiles": [{"profile_type": "FirewallSessionTimerProfile",
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a60"
  }
],
  "precedence": 10,
  "applied_to": [{
    "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type": "NSGroup"
  }]
}
```

Example Response:

```
{
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
  "display_name": "testServiceConfig",
  "profiles": [{"profile_type": "FirewallSessionTimerProfile",
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a60"
  }
],
  "precedence": 10,
  "applied_to": [{
    "target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
    "target_type": "NSGroup"
  }]
  "_create_user": "system",
  "_last_modified_user": "system",
  "_last_modified_time": 1414057732203,
  "_create_time": 1414057732203
}
```

刪除服務組態

刪除指定的服務組態。

```
DELETE https://<nsx-mgr>/api/v1/service-configs/<183e372b-854c-4fcc-a24e-05721ce89a60>
```

取得特定組態的詳細資料

傳回指定的服務組態的相關資訊。

```
GET https://<nsx-mgr>/api/v1/service-configs/<183e372b-854c-4fcc-a24e-05721ce89a60>
```

Example Response:

```
{
  "_revision": 1,
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
```

```

    "display_name": "testServiceConfig1",
    "resource_type": "ServiceConfig",
    "profiles": [{"profile_type": "FirewallSessionTimerProfile",
                  "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45",
                  "is_valid": true
                }],
    "precedence": 10,
    "applied_to": [{"target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
                  "target_type": "LogicalSwitch",
                  "is_valid": true
                }
    ]
    "_create_user": "system",
    "_last_modified_user": "system",
    "_last_modified_time": 1414057732203,
    "_create_time": 1414057732203
}

```

更新服務組態

更新指定的服務組態。

```

PUT https://<nsx-mgr>/api/v1/service-configs/183e372b-854c-4fcc-a24e-05721ce89a60
{
  "id": "183e372b-854c-4fcc-a24e-05721ce89a60",
  "display_name": "testServiceConfig1",
  "resource_type": "ServiceConfig",
  "profiles": [{"profile_type": "FirewallSessionTimerProfile",
                "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45"
              }],
  "precedence": 10,
  "applied_to": [{"target_id": "333e372b-854c-4fcc-a24e-05721ce89b71",
                "target_type": "NSGroup"
              }]
  "_create_user": "system",
  "_last_modified_user": "system",
  "_last_modified_time": 1414057732203,
  "_create_time": 1414057732203,
  "_create_user": "admin",
  "_revision": 0
}

```

取得有效的設定檔

傳回套用到指定資源的有效設定檔。

```

GET https://<nsx-mgr>/api/v1/service-configs/effective-profiles?
resource_id=<144e372b-854c-4fcc-a24e-05721ce89a60>&resource_type=NSGroup

```

Example Response:

```

{
  "cursor": "00012",
  "sort_ascending": true,
  "result_count": 2,

```

```
"results": [  
  { "profile_type": "FirewallSessionTimerProfile",  
    "target_id": "183e372b-854c-4fcc-a24e-05721ce89a45",  
    "target_name": "Firewall Session Timer Profile",  
    "is_valid": true  
  },  
  { "profile_type": "FirewallCpuMemThresholdsProfile",  
    "target_id": "5678372b-854c-4fcc-a24e-05721ce89a45",  
    "target_name": "Firewall CPU Profile",  
    "is_valid": true  
  },  
]  
}
```

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：

- [查看組態變更的實現狀態](#)
- [搜尋物件](#)
- [新增計算管理程式](#)
- [新增 Active Directory](#)
- [新增 LDAP 伺服器](#)
- [同步 Active Directory](#)
- [管理使用者帳戶和角色型存取控制](#)
- [備份和還原 NSX Manager](#)
- [從 vCenter Server 移除 NSX-T Data Center 延伸](#)
- [管理 NSX Manager 叢集](#)
- [NSX-T Data Center 的多站台部署](#)
- [設定應用裝置](#)
- [新增授權金鑰並產生授權使用率報告](#)
- [設定憑證](#)
- [收集支援服務包](#)
- [記錄訊息](#)
- [客戶經驗改進計劃](#)
- [將標籤新增至物件](#)
- [尋找遠端伺服器的 SSH 指紋](#)

■ 檢視在虛擬機器上執行之應用程式的相關資料

查看組態變更的實現狀態

進行組態變更後，NSX Manager 通常會傳送要求至其他元件來實作變更。對於某些第 3 層實體，如果您使用 API 進行組態變更，您可以追蹤要求的狀態來查看變更是否成功實作。

您起始的組態變更稱為所需狀態。實作變更的結果稱為實現狀態。如果 NSX Manager 成功實作變更，實現狀態將與所需狀態相同。如果發生錯誤，實現狀態將與所需狀態不同。

對於某些第 3 層實體，當您呼叫 API 來進行組態變更時，回應會包括參數 `request_id`。您可以使用參數 `request_id` 和 `entity_id` 進行 API 呼叫來瞭解要求的狀態。

此功能支援下列實體和 API：

```
EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement
```


AdvertiseRouteList

PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

NatRule

POST /logical-routers/<logical-router-id>/nat/rules

PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DhcpRelayService

POST /dhcp/relays

PUT /dhcp/relays/<relay-id>

DELETE /dhcp/relays/<relay-id>

DhcpRelayProfile

POST /dhcp/relay-profiles

PUT /dhcp/relay-profiles/<relay-profile-id>

DELETE /dhcp/relay-profiles/<relay-profile-id>

StaticHopBfdPeer

POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers

PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>

DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>

IPPrefixList

POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists

PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>

DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>

RouteMap

POST /logical-routers/<logical-router-id>/routing/route-maps

PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>

DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>

RedistributionConfig

PUT /logical-routers/<logical-router-id>/routing/redistribution

RedistributionRuleList

PUT /logical-routers/<logical-router-id>/routing/redistribution/rules

BfdConfig

PUT /logical-routers/<logical-router-id>/routing/bfd-config

MplsConfig

PUT /logical-routers/<logical-router-id>/routing/mpls

RoutingGlobalConfig

PUT /logical-routers/<logical-router-id>/routing

IPSecVPNIKEProfile

POST /vpn/ipsec/ike-profiles

PUT /vpn/ipsec/ike-profiles/<ike-profile-id>

DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>

IPSecVPNPDProfile

POST /vpn/ipsec/dpd-profiles

```

PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>

IPSecVPNTunnelProfile
POST /vpn/ipsec/tunnel-profiles
PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>

IPSecVPNLocalEndpoint
POST /vpn/ipsec/local-endpoints
PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>

IPSecVPNPeerEndpoint
POST /vpn/ipsec/peer-endpoints
PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>

IPSecVPNService
POST /vpn/ipsec/services
PUT /vpn/ipsec/services/<service-id>
DELETE /vpn/ipsec/services/<service-id>

IPSecVPNSession
POST /vpn/ipsec/sessions
PUT /vpn/ipsec/sessions/<session-id>
DELETE /vpn/ipsec/sessions/<session-id>

```

您可以呼叫下列 API 來取得實現狀態：

```

EdgeCluster
Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the edge
cluster is deleted then the state will be unknown and it will return the common entity not found
error.

LogicalRouter / All L3 Entites - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of logical
router but if the logical router itself is deleted then the state will be unknown and it will return
the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API to get
the realization state
Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-id>
Response - An instance of LogicalServiceRouterClusterState which will inherit ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile
Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /
IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession
Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>

```

Response – An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If the session is deleted then the state will be unknown and it will return the common entity not found error. When IPSecVPNService is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

如需有關 API 的詳細資訊，請參閱《NSX-T Data Center API 參考》。

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。

新增計算管理程式

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

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

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

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

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

必要條件

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

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

程序

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

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

如果您將指紋值保留空白，則系統會提示您接受伺服器提供的指紋。

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

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

- a 選取錯誤訊息，然後按一下**解決**。一個可能的錯誤訊息如下：

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

- b 輸入 vCenter Server 認證，然後按一下**解決**。

現有登錄將被取代 (若有)。

結果

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

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

新增 Active Directory

Active Directory 用於建立以使用者為基礎的身分識別防火牆規則。

不支援以 Windows 2008 作為 Active Directory 伺服器或 RDSH 伺服器作業系統。

您可以向 NSX Manager 登錄一或多個 Windows 網域。NSX Manager 會從登錄的每個網域取得群組和使用者資訊，以及它們之間的關係。NSX Manager 還會擷取 Active Directory (AD) 認證。

一旦 NSX Manager 擷取 AD 認證，您便可以根據使用者的身分識別建立安全群組，以及建立以身分識別為基礎的防火牆規則。

備註 在強制執行 Identity Firewall 規則時，所有使用 Active Directory 的虛擬機器均應**開啟** Windows 時間服務。這可確保 Active Directory 與虛擬機器之間的日期和時間能夠保持同步。此外，AD 群組成員資格變更 (包括啟用和刪除使用者) 並不會對登入的使用者立即生效。若要使變更生效，使用者必須登出後再重新登入。修改群組成員資格後，AD 管理員應強制登出。此行為是一個 Active Directory 限制。

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 導覽到 **系統 > Active Directory**。
- 3 按一下**新增 Active Directory**。
- 4 輸入 Active Directory 的名稱。
- 5 輸入 **NetBIOS 名稱**和**基本辨別名稱**。

若要擷取您網域的 NetBIOS 名稱，請在屬於網域的 Windows Workstation 上或在網域控制站上，於命令視窗中輸入 `nbtstat /n`。在 NetBIOS 本機名稱資料表中，前置詞為 `<00>` 且類型為 [群組] 的項目是 NetBIOS 名稱。

- 6 設定**差異同步間隔** (如有必要)。差異同步會更新自上次同步事件後發生變更的本機 AD 物件。

在 Active Directory 中進行的任何變更不會出現在 NSX Manager 上，直到執行差異或完整同步後。

- 7 按一下**儲存**。

新增 LDAP 伺服器

LDAP (輕量型目錄存取通訊協定) 伺服器組態和功能僅適用搭配使用身分識別防火牆。

LDAP 提供用於驗證的集中位置，這表示當您設定與 LDAP 伺服器的連線時，使用者記錄會儲存在您的外部 LDAP 伺服器中。

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 導覽到 **系統 > Active Directory**。
- 3 選取 **LDAP 伺服器**索引標籤。
- 4 按一下**新增 LDAP 伺服器**。
- 5 輸入 LDAP 伺服器的主機名稱。
- 6 從**已連線至 (目錄)**下拉式功能表中選取 LDAP 伺服器連線到的 Active Directory。
- 7 (選擇性) 選取**通訊協定**: LDAP (不安全) 或 LDAPS (安全)。

- 8 預設 LDAP 連接埠 389 和 LDAPS 連接埠 636 會用於 Active Directory 同步，不應編輯為非預設值。不支援自訂連接埠。
- 9 輸入 Active Directory 帳戶的**使用者名稱**和**密碼**，該帳戶至少具有 Active Directory 網域的唯一讀存取權。
- 10 按一下**儲存**。
- 11 若要確認您可以連線到 LDAP 伺服器，請按一下**測試連線**。

同步 Active Directory

Active Directory 物件可用來建立以使用者身分識別為基礎的安全群組，以及以身分識別為基礎的防火牆規則。

備註 在強制執行 Identity Firewall 規則時，所有使用 Active Directory 的虛擬機器均應**開啟** Windows 時間服務。這可確保 Active Directory 與虛擬機器之間的日期和時間能夠保持同步。對於已登入的使用者，AD 群組成員資格變更 (包括啟用和刪除使用者) 並不會立即生效。若要使變更生效，使用者必須登出後再重新登入。修改群組成員資格後，AD 管理員應強制登出。此行為是一個 Active Directory 限制。

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 導覽到 **系統 > Active Directory**。
- 3 按一下您要同步的 Active Directory 旁的三個按鈕功能表圖示，然後選取下列其中一項：

同步差異	執行差異同步，其中更新了自上次同步以來發生變更的本機 AD 物件。
全部同步	執行完整同步，其中更新了所有 AD 物件的本機狀態。

- 4 按一下**檢視同步狀態**以查看 Active Directory 的目前狀態、先前的同步狀態、同步狀態和上次同步時間。

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。

變更使用者的密碼

每個應用裝置都具有兩個內建使用者 (即管理員和稽核)，可供您用來登入 NSX Manager 或透過 SSH 連線至應用裝置，並執行 CLI 命令。您可以管理這些使用者的密碼，但無法新增或刪除使用者。

依預設，密碼會在 90 天後到期。

依預設，稽核使用者不會處於作用中狀態。若要加以啟用，請以管理員身分登入，然後執行 `set user audit` 命令並提供新密碼。當系統提示您輸入目前密碼時，請按 Enter 鍵。

必要條件

請自行熟悉 NSX Manager 和 NSX Edge 的密碼複雜性需求。請參閱《NSX-T Data Center 安裝指南》中的「NSX Manager 安裝」和「NSX Edge 安裝」。

程序

- 1 登入應用裝置的 CLI。
- 2 若要變更密碼，請執行 `set user` 命令。例如，

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

- 3 若要取得密碼到期資訊，請執行 `get user <username> password-expiration` 命令。例如，

```
nsx> get user audit password-expiration
Password expires 90 days after last change
nsx>
```

- 4 若要設定密碼到期時間 (以天為單位)，請執行 `set user <username> password-expiration <number of days>` 命令。例如，

```
nsx> set user audit password-expiration 120
nsx>
```

- 5 若要停用密碼到期時間，請執行 `clear user <username> password-expiration` 命令。例如，

```
nsx> clear user audit password-expiration
nsx>
```

重設應用裝置的密碼

如果您忘記了 `root`、`admin` 或 `audit` 使用者的密碼，則可以藉由將應用裝置開機至單一使用者模式來重設密碼。

備註 如果您有 NSX Manager 叢集，重設一個 NSX Manager 上的 `root`、`admin` 或 `audit` 使用者的密碼將會自動重設叢集中其他 NSX Manager 的密碼。

重要 當您將應用裝置重新開機時，依預設不會顯示 GRUB 開機功能表。若要進行下列程序，您必須已將應用裝置設定為顯示 GRUB 開機功能表，且您知道 GRUB 根使用者的密碼。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》中的〈設定 NSX-T Data Center 以在開機時顯示 GRUB 功能表〉。

程序

- 1 如果您在 NSX Manager 上重設密碼，請執行下列步驟：
 - a 關閉 NSX Manager。
 - b 從 <http://releases.ubuntu.com/16.04/ubuntu-16.04.6-server-amd64.iso> 下載 Ubuntu 16.04 .iso 檔案。
 - c 啟動 vSphere 或 ESXi 圖形使用者介面 (GUI)。
 - d 將 Ubuntu .iso 檔案匯入至 NSX Manager 虛擬機器適用的資料存放區中。
 - e 編輯 NSX Manager 虛擬機器的設定，並新增 CD ROM 光碟機裝置 (如果不存在)。
 - f 在 **CD ROM 光碟機** 組態中，勾選**開啟電源時連線**核取方塊。
 - g 在 **CD/DVD 媒體** 中按下**瀏覽**，然後從適用的資料存放區中選取 `ubuntu-16.04.6-server-amd64.iso`。
 - h 按一下**儲存**以結束**編輯設定**頁面。
 - i 開啟 NSX Manager 的電源。
- 2 連線至應用裝置的主控台。
- 3 將系統重新開機。
- 4 顯示 GRUB 開機功能表時，請快速按左側的 **SHIFT** 或 **ESC** 鍵。如果等待時間過長且開機順序沒有暫停，必須再次將系統重新開機。
- 5 按 **e** 編輯功能表。
輸入使用者名稱 (**root**) 和密碼。請注意，這是 GRUB 根使用者，與應用裝置的根使用者不同。
- 6 將游標保持在 Ubuntu 選取項目上。
- 7 按 **e** 編輯選取的選項。
- 8 搜尋開頭為 `linux` 的行。
- 9 移除 `root=UUID=` 之後的所有選項。
- 10 新增下列選項。
`rw single init=/bin/bash`
- 11 按 **Ctrl-X** 進行開機。
- 12 停止記錄訊息時，請按 Enter 鍵。
您會看到提示 `root@(none):/#`。
- 13 如果您要重設 `root` 的密碼，請執行命令 `passwd`。
如果您要重設 `admin` 或 `audit` 的密碼，請執行命令 `passwd <admin or audit user ID>`。
您可以多次執行 `passwd` 命令。
- 14 輸入新密碼。

15 再次輸入密碼。

16 執行命令 `sync`。

17 執行命令 `reboot -f`。

重要：如果您在 NSX Manager 上重設密碼，則在執行此命令後，請及時按 **ESC** 鍵，以便執行下一個步驟。如果等待時間過長且開機順序未暫停，則必須再次將系統重新開機。

18 如果您在 NSX Manager 上重設密碼，且已在上一個步驟中成功暫停開機順序，請執行下列步驟：

a 使用向下鍵向下捲動至 **<進入設定>**，然後按 **Enter** 鍵。

b 使用向右鍵導覽至開機功能表選項。

c 使用 **+** 或 **-** 鍵讓 CD-ROM 成為第一個裝置。

d 按 **F10** 以在儲存後結束作業。

e 若要儲存組態變更並結束作業，請針對是選項按 **Enter** 鍵。

此時將會重新開機，並顯示 BIOS 橫幅頁面。請勿按任何鍵。

f 經過幾秒鐘後，Ubuntu 將會從 CD-ROM 光碟機的 `.iso` 檔案啟動。

g 選取語言，然後按 **Enter** 鍵。

您將會看到 Ubuntu 功能表。

h 使用向下鍵選取**救援已損壞的系統**，然後按 **Enter** 鍵。

i 在後續畫面中，選取語言、國家/地區和鍵盤配置，然後按 **Enter** 鍵。

j 輸入暫時的主機名稱，或接受預設值。

k 如有必要，請設定正確的時間和時區。

l 系統會提示您輸入要作為根檔案系統的裝置。使用向下鍵選取**不使用根檔案系統**選項，然後按 **Enter** 鍵。

m 此時，系統會提示您進入救援模式。選取在**安裝程式環境中執行 Shell**，然後按 **Enter** 鍵。

n 選取**繼續**選項以進行確認，然後按 **Enter** 鍵。

o 此時您會進入 Linux Shell。輸入下列 Linux 命令：

```
mount /dev/sda2 /mnt
mount --bind /dev /mnt/dev
chroot /mnt
mount /config
touch /config/vmware/nsx-node-api/reset_cluster_credentials
umount /config
exit
umount /mnt/dev
umount /mnt
sync
exit
```

- p 此時您會再次看到**進入救援模式**畫面，請使用向下鍵選取**將系統重新開機**選項，然後按 **Enter** 鍵。

當您看到 BIOS 橫幅頁面時，請隨即按下 **ESC** 鍵。

- q 使用向下鍵向下捲動至 **<進入設定>**，然後按 **Enter** 鍵。

- r 使用向右鍵導覽至開機功能表選項。

- s 使用向下鍵導覽至**硬碟**選項，然後按 **+** 直到它成為第一個裝置。

- t 按 **F10** 以在儲存後結束作業。

- u 若要儲存組態變更並結束作業，請針對**是**選項按 **Enter** 鍵。系統將會重新開機。

- v 在 GRUB 功能表出現時，選取 Ubuntu 選項，然後按 **Enter** 鍵。

NSX Manager 將啟動並具有新密碼。

- w 如果時間允許，請在 NSX Manager 虛擬機器的 vSphere 或 ESXi GUI 中使用**編輯設定**選項移除 CD ROM 裝置。

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 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。

您必須使用 OpenSSL 1.x 版或更高版本來取得指紋。在 vIDM 主機中，命令 `openssl` 執行較舊的 OpenSSL 版本，因此您必須在 vIDM 主機中使用命令 `openssl1`。此命令僅適用於 vIDM 主機。

在非 vIDM 主機的伺服器中，您可以使用執行 OpenSSL 1.x 版或更高版本的 `openssl` 命令。

程序

- 1 登入 vIDM 主機的主控制台，或使用 SSH，或登入可對 vIDM 主機執行 Ping 動作的任何伺服器。
- 2 使用 OpenSSL 1.x 版或更高版本來取得 vIDM 主機的指紋。

- `openssl1`：如果您已在主控制台或使用 SSH 登入 vIDM 主機，請執行下列命令以取得指紋：

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

- `openssl`：如果您登入的伺服器可對 vIDM 主機執行 Ping 動作，但不是 vIDM 主機，請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
```

設定 VMware Identity Manager 整合

您可以將 NSX-T Data Center 與提供身分識別管理服務的 VMware Identity Manager (vIDM) 整合。

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，請參閱位於 <https://docs.vmware.com/tw/VMware-Identity-Manager/index.html> 的 VMware Identity Manager 說明文件。

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。

備註 NSX Manager 和 vIDM 必須位於相同的時區。建議的方式是使用 UTC。

在啟用 vIDM 的情況下，如果您使用 URL `https://<nsx-manager-ip-address>/login.jsp?local=true`，您仍可使用本機使用者帳戶登入 NSX Manager。

如果您使用 UserPrincipalName (UPN) 登入 vIDM，則對 NSX-T 的驗證可能會失敗。若要避免此問題，請使用不同類型的認證，例如 SAMAccountName。

如果您使用 NSX Cloud，則可以使用 URL `https://<csm-ip-address>/login.jsp?local=true` 個別登入 CSM。

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://docs.vmware.com/tw/VMware-Identity-Manager/index.html> 的 VMware Identity Manager 說明文件。

NSX Cloud 附註 如果使用 NSX Cloud，請確認已在 vIDM 主機上將 CSM 登錄為 OAuth 用戶端。

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 > 使用者**。
- 3 按一下 **組態索引標籤**。
- 4 按一下 **編輯**。
- 5 若要啟用外部負載平衡器整合，請按一下 **外部負載平衡器整合** 切換按鈕。

備註 如果您已設定虛擬 IP (VIP) (檢查 **系統 > 應用裝置 > 虛擬 IP**)，則您無法使用 **外部負載平衡器整合** (即使您已啟用)。這是因為您可以在設定 vIDM 時使用 VIP 或外部負載平衡器，但不能同時使用兩者。如果您想要使用外部負載平衡器，請停用 VIP。如需詳細資料，請參閱《NSX-T Data Center 安裝指南》中的 [設定叢集的虛擬 IP \(VIP\) 位址](#)。

- 6 若要啟用 VMware Identity Manager 整合，請按一下 **VMware Identity Manager 整合** 切換按鈕。
- 7 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 Manager 時所建立的識別碼。

參數	說明
OAuth 用戶端密碼	向 vIDM 主機登錄 NSX Manager 時所建立的密碼。
SSL 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)。如果您使用 NSX Manager 叢集，請使用負載平衡器 FQDN 或叢集 VIP FQDN 或 IP 位址。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。

8 按一下**儲存**。

9 如果您使用 NSX Cloud，請登入 CSM (而非 NSX Manager)，並從 CSM 應用裝置重複步驟 1 至 8。

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>

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

- VPN 管理員
- Guest Introspection 管理員
- 網路自我檢查管理員

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 21-1. 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
- VPN Adm - VPN 管理員
- GI Adm - Guest Introspection 管理員
- NI Adm - 網路自我檢查管理員
- FA - 完整存取權
- E - 執行
- R - 讀取

表 21-1. 角色和權限

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
工具 > 連接埠連線	E	R	E	E	E	E	E	R	E	E	無	無	無
工具 > Traceflow	E	R	E	E	E	E	E	R	E	E	無	無	無

表 21-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
工具 > 連接埠鏡 像	FA	R	FA	FA	FA	FA	FA	R	無	無	無	無	無
工具 > IPFIX	FA	R	FA	R	FA	R	FA	R	無	無	R	R	R
防火牆 > 一般	FA	R	R	R	FA	R	FA	R	無	無	無	無	R
防火牆 > 組態	FA	R	R	R	FA	R	FA	R	無	無	無	無	無
路由 > 路由器	FA	R	FA	R	R	R	FA	R	R	R	無	無	無
路由 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	無	無	無
DHCP > 伺服器設 定檔	FA	R	FA	R	FA	無	FA	R	無	無	無	無	無
DHCP > 伺服器	FA	R	FA	R	FA	無	FA	R	無	無	無	無	無
DHCP > 轉送設定 檔	FA	R	FA	R	FA	無	FA	R	無	無	無	無	無
DHCP > 轉送服務	FA	R	FA	R	FA	無	FA	R	無	無	無	無	無
DHCP > 中繼資料 Proxy	FA	R	FA	R	FA	無	無	無	無	無	無	無	無
IPAM	FA	R	FA	R	FA	無	無	無	無	無	無	無	無
交換 > 交換器	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
交換 > 連接埠	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
交換 > 交換設定 檔	FA	R	FA	FA	FA	FA	FA	R	R	R	無	無	無
原則 > 網路 > 負載平衡 器	FA	R	無	無	無	無	FA	R	FA	R	無	無	無
負載平衡 > 虛擬伺 服器	FA	R	無	無	無	無	FA	R	FA	R	無	無	無

表 21-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
負載平衡 > 設定檔 > 應用程式 設定檔	FA	R	無	無	無	無	FA	R	FA	R	無	無	無
負載平衡 > 設定檔 > 持續性 設定檔	FA	R	無	無	無	無	FA	R	FA	R	無	無	無
負載平衡 > 設定檔 > SSL 設 定檔	FA	R	無	無	FA	R	FA	R	FA	R	無	無	無
負載平衡 > 伺服器 集區	FA	R	無	無	無	無	FA	R	FA	R	無	無	無
負載平衡 > 監視器	FA	R	無	無	無	無	FA	R	FA	R	無	無	無
詳細目錄 > 群組	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > IP 集 合	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > IP 集 區	FA	R	FA	R	無	R	無	無	R	R	R	R	R
詳細目錄 > MAC 集合	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 服務	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 虛擬機 器	R	R	R	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	R	FA	FA
詳細目錄 > 虛擬機 器 > 設 定標籤	FA	無	無	無	FA	無	無	無	無	無	無	無	無

表 21-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
網狀架構 > 節點 > 主機	FA	R	R	R	R	R	R	R	無	無	無	無	無
網狀架構 > 節點 > 節點	FA	R	FA	R	FA	R	R	R	無	無	無	無	無
網狀架構 > 節點 > Edge	FA	R	FA	R	R	R	R	R	無	無	無	無	無
網狀架構 > 節點 > Edge 叢 集	FA	R	FA	R	R	R	R	R	無	無	無	無	無
網狀架構 > 節點 > 橋接器	FA	R	FA	R	R	R	無	無	R	R	無	無	無
網狀架構 > 節點 > 傳輸節點	FA	R	R	R	R	R	R	R	R	R	無	無	無
網狀架構 > 節點 > 通道	R	R	R	R	R	R	R	R	R	R	無	無	無
網狀架構 > 設定檔 > 上行設 定檔	FA	R	R	R	R	R	R	R	R	R	無	無	無
網狀架構 > 設定檔 > Edge 叢集設定 檔	FA	R	FA	R	R	R	R	R	R	R	無	無	無
網狀架構 > 設定檔 > 組態	FA	R	無	無	無	無	R	R	無	無	無	無	無
網狀架構 > 傳輸區 域 > 傳 輸區域	FA	R	R	R	R	R	R	R	R	R	無	無	無
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	無	無	無

表 21-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
網狀架構 > 計算管理程式	FA	R	R	R	R	R	R	R	無	無	無	R	R
系統 > 信任	FA	R	無	無	FA	R	無	無	FA	R	FA	無	無
系統 > 組態	FA	R	無	無	無	無	無	無	無	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	無	無	無
系統 > 公用程式 > 備份	FA	R	無	無	無	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	無	無	無
系統 > 公用程式 > 升級	FA	R	R	R	R	R	無	無	無	無	無	無	無
系統 > 使用者 > 角色指派	FA	R	無	無	無	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	無	無	無

新增角色指派或主體身分識別

如果 VMware Identity Manager 與 NSX-T Data Center 整合，您可以指派角色給使用者或使用者群組。也可以指派角色給主體身分識別。

主體是 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 - 這可以是指派給主體身分識別的任意英數位元值
- 憑證
- 指示此主體存取權的 RBAC 角色

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。

如果主體身分識別使用者的憑證到期，您必須匯入新憑證並進行 API 呼叫，以更新主體身分識別使用者的憑證 (請參閱下列程序)。如需關於 NSX-T Data Center API 的詳細資訊，請存取 <https://docs.vmware.com/tw/VMware-NSX-T-Data-Center> 中的 API 資源連結。

主體身分識別使用者的憑證必須符合下列需求：

- 以 SHA256 為基礎。
- 金鑰大小為 2048 位元或以上的 RSA/DSA 訊息演算法。
- 不可為根憑證。

您可以使用 API 來刪除主體身分識別。不過，刪除主體身分識別不會自動刪除對應的憑證。您必須手動刪除憑證。

刪除主體身分識別及其憑證的步驟：

- 1 取得要刪除之主體身分識別的詳細資料，並記下回應中的 `certificate_id` 值。

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 刪除主體身分識別。

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 使用在步驟 1 中取得的 `certificate_id` 值來刪除憑證。

```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

必要條件

- 如果您想要指派角色給使用者，請確認 vIDM 主機與 NSX-T 相關聯。如需詳細資訊，請參閱[設定 VMware Identity Manager 整合](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**系統 > 使用者**。
- 3 若要指派角色給使用者，請選取**新增 > 角色指派**。
 - a 選取使用者或使用者群組。
 - b 選取角色。
 - c 按一下**儲存**。
- 4 若要新增主體身分識別，請選取**新增 > 具有角色的主體身分識別**。
 - a 輸入主體身分識別的名稱。
 - b 選取角色。
 - c 輸入節點識別碼。

- d 以 PEM 格式輸入憑證。
 - e 按一下**儲存**。
- 5** (選擇性) 如果您使用 NSX Cloud，請登入 CSM 應用裝置 (而非 NSX Manager)，並重複步驟 1 至 4。
- 6** 如果主體身分識別的憑證到期，請執行下列步驟：
- a 匯入新憑證並記下憑證的識別碼。請參閱[匯入憑證](#)。
 - b 呼叫下列 API 以取得主體身分識別的識別碼。

```
GET https://<nsx-mgr>/api/v1/trust-management/principal-identities
```

- c 呼叫下列 API 以更新主體身分識別的憑證。您必須提供已匯入憑證的識別碼和主體身分識別使用者的識別碼。

例如，

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

備份和還原 NSX Manager

當 NSX Manager 叢集變得無法運作，或是您想要將環境還原至先前的狀態時，您可以從備份還原。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。

備份有以下兩種類型：

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。

共有兩種備份方法：

手動

您可以隨時手動執行備份。

自動

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，以確保您擁有最新的備份。

您可以將 NSX-T Data Center 組態還原成任何備份中擷取的狀態。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。

設定備份

在進行備份之前，必須先設定備份檔案伺服器。設定好備份檔案伺服器之後，您可以隨時啟動備份，或設定排程來自動執行備份。

必要條件

確認您擁有備份檔案伺服器的 SSH 指紋。僅接受 SHA256 雜湊的 ECDSA (256 位元) 金鑰作為指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**系統 > 備份與還原**。
- 3 按一下頁面右上方的**編輯**來設定備份。
- 4 輸入備份檔案伺服器的 IP 位址或主機名稱。
- 5 視需要變更預設連接埠。
- 6 通訊協定欄位已填入。請勿變更值。

SFTP 是唯一支援的通訊協定。

- 7 輸入登入備份檔案伺服器所需的使用者名稱和密碼。

第一次設定檔案伺服器時，您必須提供密碼。之後，當您重新設定檔案伺服器時，如果伺服器 IP (或主機名稱)、連接埠及使用者名稱均維持不變，則您不需要再次輸入密碼。

- 8 在**目的地目錄**欄位中，輸入儲存備份的絕對目錄路徑。

該目錄必須已存在，且不可為 /。如果您有多個 NSX-T Data Center 部署，請務必針對每個部署使用不同的目錄。如果備份檔案伺服器是 Windows 機器，則您在指定目的地目錄時仍應使用正斜線。例如，如果 Windows 機器上的備份目錄為 `c:\SFTP_Root\backup`，請指定 `/SFTP_Root/backup` 作為目的地目錄。

備註 備份程序會為備份檔案產生可能很長的名稱。在 Windows Server 上，備份檔案的完整路徑名稱長度可能超過 Windows 設定的限制，並導致備份失敗。若要避免此問題，請參閱知識庫文章 <https://kb.vmware.com/s/article/76528>。

- 9 若要加密備份，請按一下**變更加密複雜密碼**切換按鈕，然後輸入加密複雜密碼。
您需要此複雜密碼才能還原備份。如果您忘記複雜密碼，則無法還原任何備份。
- 10 輸入儲存備份之伺服器的 SSH 指紋。
您可以將此項目保留空白，然後接受或拒絕伺服器提供的指紋。
- 11 按一下**排程**索引標籤。
- 12 若要啟用自動備份，請按一下**自動備份**切換按鈕。
- 13 按一下**每週**並設定備份的日期和時間，或按一下**間隔**並設定備份之間的間隔。

14 若要在網路組態變更時觸發備份，請將**偵測 NSX 組態變更**切換按鈕設為已啟用。

您可以設定由組態變更觸發的備份之間的間隔。預設值為 5 分鐘。

15 按一下**儲存**。

結果

設定備份檔案伺服器之後，您可以隨時按一下**立即備份**來啟動備份。

移除舊備份

備份會在備份檔案伺服器上累積並耗用大量儲存區。您可以執行 NSX-T Data Center 隨附的指令碼以自動刪除舊備份。

您可以在 NSX Manager 上的目錄 `/var/vmware/nsx/file-store` 中找到 Python 指令碼 `nsx_backup_cleaner.py`。您必須以 root 身分登入才能存取此檔案。通常，您可以在備份檔案伺服器上排程工作以定期執行此指令碼來清除舊備份。下列使用資訊說明了如何執行指令碼：

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]

Required parameters:
  -d/--dir: Backup root directory
  -k/--retention-period: Number of days need to retain a backup file

Optional parameters:
  -l/--min-count: Minimum number of backup files to be kept, default value is 100
  -h/--help: Display help message
```

備份存留期由備份時間戳記與指令碼執行時間之差計算而來。如果此值大於保留期間，則當磁碟上的備份數目大於備份數目下限時，會刪除備份。

如需有關將指令碼設定為在 Linux 或 Windows 伺服器上定期執行的詳細資訊，請參閱指令碼開頭的註解。

列出可用的備份

備份檔案伺服器會儲存所有 NSX Manager 的備份。若要取得備份清單來找到想要還原的備份，您必須執行 `get_backup_timestamps.sh` 指令碼。

此指令碼位於 NSX Manager 上。完整路徑名稱為 `/var/vmware/nsx/file-store/get_backup_timestamps.sh`。您可以在任何 Linux 機器或 NSX-T Data Center 應用裝置上執行此指令碼。最佳做法是，安裝 NSX-T Data Center 後，您應該將此指令碼複製到非 NSX Manager 的機器，以便在即使所有 NSX Manager 都變得無法存取時，您也可執行此指令碼。如果您需要還原備份，但無法存取此指令碼，則可以安裝新的 NSX Manager，然後執行其上的指令碼。

您可以使用管理員身分登入 NSX Manager 並執行 CLI 命令，以將指令碼複製到其他機器或備份檔案伺服器。例如：

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

此為互動式指令碼，會提示您輸入在設定備份檔案伺服器時所指定的資訊。您可以指定要顯示的備份數目。系統會列出每個備份，以及時間戳記、NSX Manager 節點的 IP 位址或 FQDN (如果 NSX Manager 節點已設定為發佈其 FQDN)，以及節點識別碼。例如，

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

還原備份

還原備份後，網路將會還原為備份建立時的狀態。此外也會還原由 NSX Manager 維護的組態，並協調在備份建立後對網狀架構所做的任何變更 (例如新增或移除節點)。

您必須在全新安裝 NSX Manager 時還原備份，如以下的第一個步驟中所述。

必要條件

- 確認您擁有備份檔案伺服器的登入認證。
- 確認您擁有備份檔案伺服器的 SSH 指紋。僅接受 SHA256 雜湊的 ECDSA (256 位元) 金鑰作為指紋。請參閱[尋找遠端伺服器的 SSH 指紋](#)。
- 確認您擁有備份檔案的複雜密碼。

程序

- 1 安裝新的 NSX Manager 節點，以在其上還原備份。

如果為原始 NSX Manager 設定了預設設定 "publish_fqdns": false (亦即不發佈其 FQDN)，則必須使用原始 NSX Manager 所使用的相同 IP 位址來安裝新的 NSX Manager。如果原始 NSX Manager

設為會發佈其 FQDN (即 "publish_fqdns": true)，則可以使用不同的 IP 位址來安裝新的 NSX Manager。不過，新的 NSX Manager 必須設定為會發佈其 FQDN。如果在建立備份時已有 NSX Manager 叢集，則您還必須還原至 NSX Manager 叢集。還原程序會先還原一個 NSX Manager 節點，然後提示您新增其他 NSX Manager 節點。

- a 關閉所有 NSX Manager 節點的電源。
- b 使用原始 NSX Manager 節點的相同名稱和 IP 位址來部署新的 NSX Manager 節點。

若要識別原始 NSX Manager 節點，請開啟 NSX Manager 儀表板，並導覽至**系統 > 應用裝置**，以檢視管理叢集。這會顯示 NSX Manager 節點。原始節點即為 [部署類型] 顯示為 [手動] 的節點。

在新的 NSX Manager 節點執行並上線後，您即可繼續進行剩餘程序。

- 2 在瀏覽器中，以管理員權限登入新的 NSX Manager。

此 NSX Manager 節點的 IP 位址或 FQDN 必須與已建立備份之 NSX Manager 的 IP 位址或 FQDN 相同。

- 3 選取**系統 > 備份與還原**。
- 4 按一下**還原**索引標籤。
- 5 若要設定備份檔案伺服器，請按一下**編輯**。
- 6 輸入 IP 位址或主機名稱。
- 7 視需要變更連接埠號碼。

預設值為 22。

- 8 若要登入伺服器，請輸入使用者名稱和密碼。
- 9 在**目的地目錄**文字方塊中，輸入用來儲存備份的絕對目錄路徑。
- 10 輸入用來加密備份資料的複雜密碼。
- 11 輸入儲存備份之伺服器的 SSH 指紋。
- 12 按一下**儲存**。
- 13 選取備份。
- 14 按一下**還原**。

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

如果備份具有 NSX Manager 叢集的相關資訊，則系統會提示您新增 NSX Manager 節點。如果您選擇不新增 NSX Manager 節點，您仍可以繼續進行還原。

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**。您可以將管理程式重新啟動或重新開機，還原作業將繼續執行。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
```

- 第一個 NSX Manager 節點啟動並運作後，請部署兩個額外的節點，以完成 NSX Manager 叢集。

請參閱《NSX-T Data Center 安裝指南》中的〈部署 NSX Manager 節點以從 UI 形成叢集〉。

- 部署新的 NSX Manager 叢集後，請刪除您在此程序的步驟 1a 中關閉電源的原始 NSX Manager 叢集虛擬機器。

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。您可以按一下**解決**按鈕，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 4。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。如果您移除計算管理程式，vCenter Server 中的延伸將會自動移除。如果此延伸因故未移除，您可以使用下列程序手動移除此延伸。

必要條件

依照 <https://kb.vmware.com/s/article/2042554> 中的程序，允許存取 vCenter Server 受管理物件瀏覽器 (MOB)。

程序

- 經由 `https://<vCenter Server 主機名稱或 IP 位址>/mob` 登入 MOB。
- 按一下**內容連結**，此為內容資料表中**內容**屬性的值。
- 按一下 **ExtensionManager** 連結，此為內容資料表中 **extensionManager** 內容的值。
- 按一下方法資料表中的 **UnregisterExtension** 連結。
- 在**值**文字欄位中輸入 `com.vmware.nsx.management.nsx`。

- 6 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。
- 7 若要確定延伸已移除，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**。

管理 NSX Manager 叢集

如果變得無法運作，您可以將 NSX Manager 重新開機。您也可以變更 NSX Manager 的 IP 位址。

在生產環境中，強烈建議 NSX Manager 叢集有三個成員以提供高可用性。如果您刪除 NSX Manager 並重新部署一個，則新的 NSX Manager 可以有相同或不同的 IP 位址。

備註 主要 NSX Manager 節點即為您建立管理程式叢集之前先建立的節點。此節點無法刪除。從主要管理程式節點的 UI 部署兩個以上的管理程式節點來組成叢集之後，僅第二個和第三個管理程式節點具有用來刪除的選項 (透過齒輪圖示)。如需移除和新增管理程式節點相關資訊，請參閱[變更 NSX Manager 的 IP 位址](#)。

檢視 NSX Manager 叢集的組態和狀態

您可以從 NSX Manager 使用者介面檢視 NSX Manager 叢集的組態和狀態。您可以使用 CLI 取得其他資訊。

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**系統 > 概觀**。
隨即顯示 NSX Manager 叢集的狀態。
- 3 若要查看有關組態的其他資訊，請執行下列 CLI 命令：

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
```

ENTITY	PORT	FQDN	UUID	IP
ADDRESS				
HTTPS			5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5		
CONTROLLER			06fd0574-69c0-432e-a8af-53d140dbef8f	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
CLUSTER_BOOT_MANAGER			da8d535e-7a0c-4dd8-8919-d88bdde006b8	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
DATASTORE			3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5		

MANAGER			eb5e8922-23bd-4c3a-ae22-d13d9195a6bc	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
POLICY			f9da1039-08ad-4a20-bacc-5b91c5d67730	
10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5		
Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672				
Node Status: JOINED				
ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			3757f155-8a5d-4b53-828f-d67041d5a210	
10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5		
CONTROLLER			7b1c9952-8738-4900-b68b-ca862aa4f6a9	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
CLUSTER_BOOT_MANAGER			b5e12db1-5e0d-4e33-a571-6ba258dceb2e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
DATASTORE			bee1f629-4e23-4ab8-8083-9e0f0bb83178	
10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5		
MANAGER			45ccd6e3-1497-4334-944c-e6bbcd5c723e	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
POLICY			d5ba5803-b059-4fbc-897c-3aace8cf1219	
10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5		
Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea				
Node Status: JOINED				
ENTITY			UUID	IP
ADDRESS	PORT	FQDN		
HTTPS			bce3cc4c-7d60-45e2-aa7b-cdc75e445a14	
10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5		
CONTROLLER			ced46f5c-9e52-4b31-a1cb-b3dead991c71	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
CLUSTER_BOOT_MANAGER			88b70d31-3428-4ccc-ab57-55859f45030c	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
DATASTORE			fb4aec3c-cae3-4386-b5b9-c0b99b7d9048	
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5		
MANAGER			82b07440-3ff6-4f67-a1c9-e9327d1686ad	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		
POLICY			61f21a78-a56c-4af1-867b-3f24132d53c7	
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		

4 若要查看有關狀態的其他資訊，請執行下列 CLI 命令：

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN
  IP      STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
  10.160.71.225  UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
  10.160.93.240  UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
  10.160.76.33  UP

```

Group Type: CLUSTER_BOOT_MANAGER

Group Status: STABLE

Members:

UUID	FQDN
IP	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: CONTROLLER

Group Status: STABLE

Members:

UUID	FQDN
IP	
7b1c9952-8738-4900-b68b-ca862aa4f6a9	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
ced46f5c-9e52-4b31-a1cb-b3dead991c71	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	
06fd0574-69c0-432e-a8af-53d140dbef8f	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	

Group Type: MANAGER

Group Status: STABLE

Members:

UUID	FQDN
IP	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: POLICY

Group Status: STABLE

Members:

UUID	FQDN
IP	
43cd0642-275c-af1d-fe46-1f5200f9e5f9	ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225 UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672	ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240 UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea	ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33 UP	

Group Type: HTTPS

Group Status: STABLE

Members:		
UUID		FQDN
IP	STATUS	
43cd0642-275c-af1d-fe46-1f5200f9e5f9		ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225	UP	
8ebb0642-201e-6a5f-dd47-a1e38542e672		ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240	UP	
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea		ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33	UP	

將 NSX Manager 重新開機

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

如果您需要將多個 NSX Manager 重新開機，則必須一次重新開機一個。等待重新開機的 NSX Manager 上線，然後將另一個 NSX Manager 重新開機。

程序

- 1 登入 NSX Manager 的 CLI。
- 2 執行下列命令。

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

變更 NSX Manager 的 IP 位址

您可以變更 NSX Manager 叢集中 NSX Manager 的 IP 位址。本小節說明幾種方法。

例如，如果您有包含 Manager A、Manager B 和 Manager C 的叢集，您可以以下列方式變更一或多個管理程式的 IP 位址：

- 案例 A：
 - Manager A 具有 IP 位址 172.16.1.11。
 - Manager B 具有 IP 位址 172.16.1.12。
 - Manager C 具有 IP 位址 172.16.1.13。
 - 使用新的 IP 位址新增 Manager D，例如 192.168.55.11。
 - 移除 Manager A。
 - 使用新的 IP 位址新增 Manager E，例如 192.168.55.12。
 - 移除 Manager B。
 - 使用新的 IP 位址新增 Manager F，例如 192.168.55.13。
 - 移除 Manager C。
- 案例 B：
 - Manager A 具有 IP 位址 172.16.1.11。

- Manager B 具有 IP 位址 172.16.1.12。
 - Manager C 具有 IP 位址 172.16.1.13。
 - 使用新的 IP 位址新增 Manager D，例如 192.168.55.11。
 - 使用新的 IP 位址新增 Manager E，例如 192.168.55.12。
 - 使用新的 IP 位址新增 Manager F，例如 192.168.55.13。
 - 移除 Manager A、Manager B 和 Manager C。
- 案例 C:
- Manager A 具有 IP 位址 172.16.1.11。
 - Manager B 具有 IP 位址 172.16.1.12。
 - Manager C 具有 IP 位址 172.16.1.13。
 - 移除 Manager A。
 - 使用新的 IP 位址新增 Manager D，例如 192.168.55.11。
 - 移除 Manager B。
 - 使用新的 IP 位址新增 Manager E，例如 192.168.55.12。
 - 移除 Manager C。
 - 使用新的 IP 位址新增 Manager F，例如 192.168.55.13。

在此 IP 位址變更期間，前兩個案例需要額外的虛擬 RAM、CPU 和磁碟供額外的 NSX Manager 使用。

不建議案例 C，因為它會暫時減少 NSX Manager 的數目，並且在 IP 位址變更期間兩個作用中管理程式中斷其中一個將會影響 NSX-T 作業。此案例適用於沒有其他虛擬 RAM、CPU 和磁碟可用，且必須變更 IP 位址的情況。

備註 如果您使用叢集 VIP 功能，則必須使用相同子網路做為新 IP 位址，或是在 IP 位址變更期間停用叢集 VIP，因為叢集 VIP 需要所有 NSX Manager 處於相同的子網路。

必要條件

自行熟悉如何將 NSX Manager 部署至叢集。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》。

程序

- 1 如果您想要移除的 NSX Manager 是手動部署的，請執行下列步驟。
 - a 執行下列 CLI 命令，以從叢集中斷連結 NSX Manager。


```
detach node <node-id>
```
 - b 刪除 NSX Manager 虛擬機器。

- 2 如果您想要刪除的 NSX Manager 是透過 NSX Manager 使用者介面自動部署的，請執行下列步驟。
 - a 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://nsx-manager-ip-address>。
此 NSX Manager 不得是您想要刪除的 NSX Manager。
 - b 按一下**系統**索引標籤。
隨即顯示 NSX Manager 叢集的狀態。
 - c 對於您想要刪除的 NSX Manager，按一下齒輪圖示，然後選取**刪除**。
- 3 部署新的 NSX Manager

調整 NSX Manager 節點的大小

您可以隨時變更 NSX Manager 節點的 CPU 核心或記憶體數目。

請注意，在一般作業條件中，三個管理程式節點全都必須有相同數目的 CPU 核心和記憶體。只有從某個大小的 NSX Manager 轉換為不同大小的 NSX Manager 時，NSX 管理叢集中的 NSX Manager 之間才會有不相符的 CPU 或記憶體數目。

如果您已為 vCenter Server 中的 NSX Manager 虛擬機器設定資源配置保留，您可能需要調整保留。如需詳細資訊，請參閱 vSphere 說明文件。

必要條件

- 確認新大小符合管理程式節點的系統需求。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》中的〈NSX Manager 虛擬機器系統需求〉。
- 自行熟悉如何將 NSX Manager 部署至叢集。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》。
- 如需如何從叢集中移除管理程式節點的相關資訊，請參閱[變更 NSX Manager 的 IP 位址](#)。

程序

- 1 以新的大小部署新的管理程式節點。
- 2 將新的管理程式節點新增至叢集。
- 3 移除舊的管理程式節點。
- 4 重複步驟 1 至 3，以取代其他兩個舊的管理程式節點。

NSX-T Data Center 的多站台部署

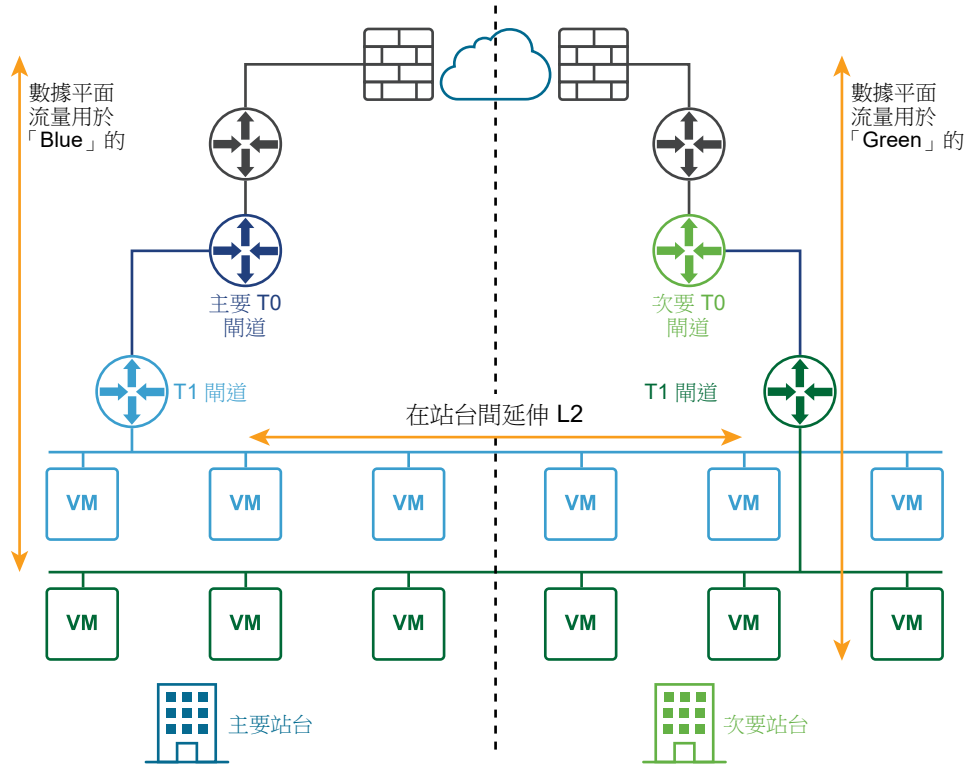
NSX-T Data Center 支援多站台部署，進而您可從一個 NSX Manager 叢集管理所有站台。

支援兩種類型的多站台部署：

- 雙主動
- 災害復原

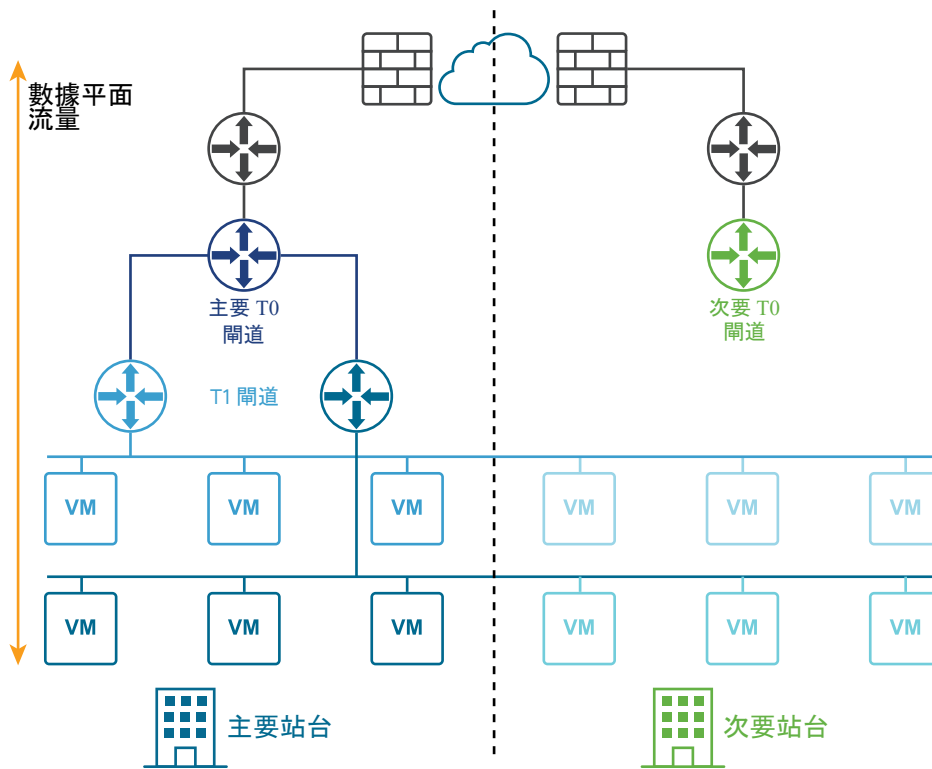
在雙主動部署中，所有站台均處於作用中狀態，且第 2 層流量會跨越站台界限。在災害復原部署中，位於主要站台的 NSX-T Data Center 會處理企業的網路。次要站台則會處於備用狀態，以便在主要站台發生災難性失敗時接手。

下圖說明雙主動部署。

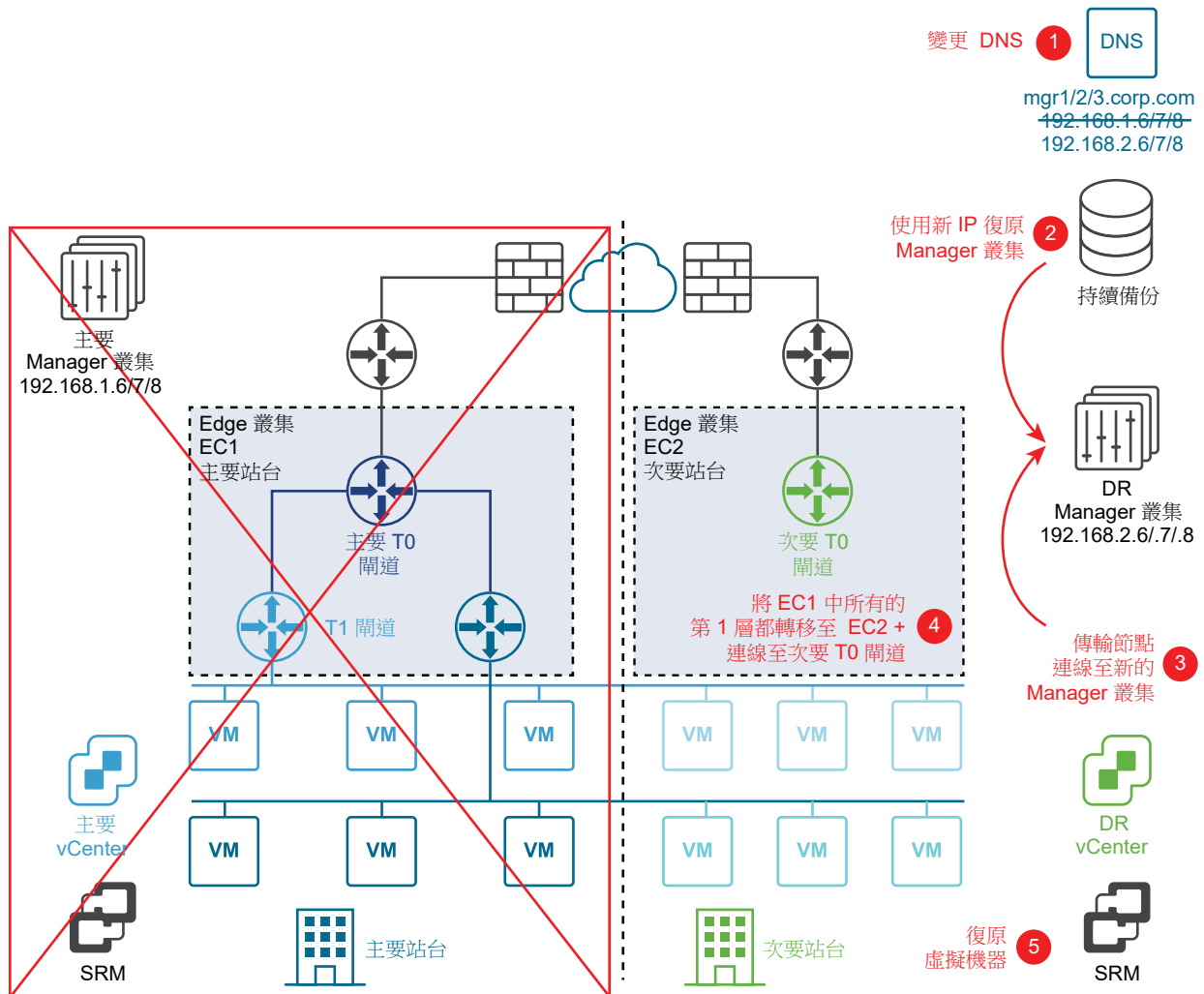


在雙主動部署中，如果主要閘道失敗，它將容錯移轉至次要閘道。如果主要站台失敗，則必須完成下方針對災害復原說明的所有步驟。

下圖說明災害復原部署。



下圖說明災害復原程序。



復原步驟如下：

- 1 變更 DNS 記錄，讓 NSX Manager 叢集具有不同的 IP 位址。
- 2 從備份還原 NSX Manager 叢集。
- 3 讓傳輸節點連線至新的 NSX Manager 叢集。
- 4 將主要站台上 NSX Edge 叢集中的第 1 層閘道轉移到次要站台上的 NSX Edge 叢集中。
- 5 復原虛擬機器。

多站台部署需求

站台間通訊

- 頻寬必須至少有 1 Gbps，且延遲時間 (RTT) 必須少於 150 毫秒。
- MTU 必須至少為 1600。建議使用 9000。

NSX Manager 組態

- 必須啟用在 NSX-T Data Center 組態有所變更時自動備份的功能。

- NSX Manager 必須設為使用 FQDN。

數據平面復原

- 如果公用 IP 位址是透過 NAT 或負載平衡器之類的服務公開，則必須使用相同的網際網路提供者。

雲端管理系統

- 雲端管理系統 (CMS) 必須支援 NSX-T Data Center 外掛程式。在此版本中，VMware Integrated OpenStack (VIO) 和 vRealize Automation (vRA) 可滿足此需求。

限制

- 無本機出口功能。所有南北向流量均必須在一個站台內進行。
- 計算災害復原協調功能必須支援 NSX-T Data Center。

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 21-2. 系統組態命令和 API 要求。

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

新增授權金鑰並產生授權使用率報告

您可以新增授權金鑰，並產生授權使用率報告。使用率報告是 CSV 格式的檔案。

我們提供下列非評估版 NSX-T Data Center 授權類型：

- 標準
- Professional
- 進階
- Enterprise Plus

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**系統 > 授權 > 新增**。
- 3 輸入授權金鑰。
- 4 若要產生授權使用率報告，請選取**匯出 > 授權使用率報告**。

CSV 報告列出下列功能的虛擬機器、CPU、唯一的並行使用者以及 vCPU 使用率數量：

- 交換和路由
- NSX Edge 負載平衡器
- VPN
- DFW
- 內容感知微分割 - 應用程式識別
- 內容感知微分割 - 用於遠端桌面工作階段主機的 Identity Firewall
- 服務插入
- Identity Firewall
- 增強型客體自我檢查

設定憑證

您可以匯入憑證、建立憑證簽署要求 (CSR)、產生自我簽署憑證，以及匯入憑證撤銷清單 (CRL)。

安裝 NSX-T Data Center 之後，管理程式節點和叢集會具有自我簽署的憑證。為提高安全性，強烈建議您將自我簽署的憑證取代為 CA 簽署的憑證。

匯入憑證

啟用後，您可以匯入具有私密金鑰的憑證，以取代預設的自我簽署憑證。

請注意，僅支援 RSA 型憑證。

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 選取系統 > 憑證。

3 選取匯入 > 匯入憑證，然後輸入憑證詳細資料。

選項	說明
名稱	指派名稱給憑證。
憑證內容	瀏覽到電腦上的憑證檔案，然後新增該檔案。憑證必須未加密。如果是 CA 簽署的憑證，請務必以下列順序納入整個鏈結：憑證 - 中繼 - 根。
私密金鑰	瀏覽到電腦上的私密金鑰檔案，然後新增該檔案。
複雜密碼	如果已加密，請新增此憑證的複雜密碼。在此版本中，因為不支援加密的憑證，因此不使用此欄位。
說明	輸入此憑證所含內容的說明。
服務憑證	設為 是 ，可將此憑證用於負載平衡器和 VPN 之類的服務。如果此憑證用於 NSX Manager 節點，請設為 否 。

4 按一下匯入。

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 and 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 選取系統 > 憑證。
- 3 按一下 **CSR** 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。

選項	說明
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)。
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 按一下產生。

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。在匯入並啟用後，NSX-T Data Center 將會信任由該 CA 簽署的憑證。

請注意，僅支援 RSA 型憑證。

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 選取系統 > 憑證。

- 3 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。
服務憑證	設為 是 ，可將此憑證用於負載平衡器和 VPN 之類的服務。如果此憑證用於 NSX Manager 節點，請設為 否 。

- 4 按一下**匯入**。

建立自我簽署的憑證

您可以建立自我簽署的憑證。不過，使用自我簽署的憑證比使用受信任的憑證不安全。

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**系統 > 憑證**。
- 3 按一下 **CSR** 索引標籤。
- 4 選取 CSR。
- 5 選取**動作 > CSR 的自我簽署憑證**。
- 6 輸入自我簽署憑證有效天數。
預設值為 10 年。
- 7 按一下**新增**。

結果

自我簽署的憑證會顯示在**憑證**索引標籤中。

取代 NSX Manager 節點的憑證或 NSX Manager 叢集虛擬 IP

您可以發出 API 呼叫，取代理管理程式節點的憑證或管理程式叢集虛擬 IP (VIP)。

安裝 NSX-T Data Center 之後，管理程式節點和叢集會具有自我簽署的憑證。為提高安全性，強烈建議您將自我簽署的憑證取代為 CA 簽署的憑證，以及對每個節點使用不同的憑證。

在版本 2.4 中，將現有的憑證取代為 CA 簽署的憑證可能會失敗。此問題在 2.4.1 版本中已修正。

必要條件

確認 NSX Manager 中可以使用憑證。請參閱[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**系統 > 憑證**。

3 在識別碼資料行中，按一下所要使用憑證的識別碼，然後複製快顯視窗中的憑證識別碼。

請確保匯入此憑證時，選項**服務憑證**已設定為否。

4 若要取代表管理程式節點的憑證，請使用 `POST /api/v1/node/services/http?action=apply_certificate` API 呼叫。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 Data Center API 參考》。

5 若要取代表管理程式叢集 VIP 的憑證，請使用 `POST /api/v1/cluster/api-certificate?action=set_cluster_certificate` API 呼叫。例如，

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

如需詳細資訊，請參閱《NSX-T Data Center API 參考》。如果您未設定 VIP，則不需要此步驟。

匯入憑證撤銷清單

憑證撤銷清單 (CRL) 是個列出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**系統 > 憑證**。

3 按一下 **CRL** 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	複製 CRL 中的所有項目，並將其貼上至此區段中。 範例 CRL。
	<pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTENMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEbMBk G A1UEAxMSU1NMZW5IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDB a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TFazG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
說明	輸入此 CRL 所含內容的摘要。

5 按一下匯入。

結果

匯入的 CRL 會顯示為連結。

設定 NSX Manager 以擷取憑證撤銷清單

您可以使用 API 來設定 NSX Manager，以擷取憑證撤銷清單 (CRL)。然後，您可以對 NSX Manager 進行 API 呼叫以檢查 CRL，而不是對憑證授權機構進行呼叫。

此功能可提供以下好處：

- 在伺服器 (即 NSX Manager) 上快取 CRL 可以提高效率。
- 用戶端不需要建立對憑證授權機構的任何輸出連線。

與憑證撤銷清單相關的可用 API 如下：

```
GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file
```

您可以管理 CRL 發佈點，以及擷取儲存在 NSX Manager 中的 CRL。如需詳細資訊，請參閱《NSX-T Data Center API 參考》。

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**系統 > 憑證**。
- 3 按一下 **CSR** 索引標籤。
- 4 選取 CSR。
- 5 選取**動作 > 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**新增**。

結果

自我簽署的憑證會顯示在**憑證**索引標籤中。

公用憑證和私密金鑰的儲存區

公開金鑰憑證和私密金鑰會儲存在 NSX Manager 上。當建立的負載平衡器或 VPN 服務需要私密金鑰時，NSX Manager 會傳送一份私密金鑰至執行負載平衡器或 VPN 服務所在的 Edge 節點。

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 **系統 > 支援服務包**。

3 選取目標節點。

可用的節點類型包含 **管理節點**、**Edge**、**主機** 和 **公用雲端閘道**。

4 (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。

5 (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。

6 (選擇性) 選取將服務包上傳至檔案伺服器的核取方塊。

7 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。

8 監控收集程序的狀態。

[狀態] 索引標籤會顯示收集支援服務包的進度。

9 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。

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 會產生種類為 `local6`，具有數值 22 的記錄。每個 API 呼叫會產生一個稽核記錄，其中包含結構化資料欄位中的 `audit="true"`。

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
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 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 21-3. 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
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 升級 (NSX Manager、NSX Edge 和主機套件升級) 實現 標籤

表 21-3. 記錄訊息識別碼 (續)

訊息識別碼	範例
MONITORING	SNMP 連接埠連線 Traceflow
-	所有其他記錄訊息。

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 CEIP 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 > 客戶計畫**。
- 3 按一下 [客戶經驗改進計劃] 區段中的 **編輯**。
- 4 在 [編輯客戶經驗計劃] 對話方塊中，選取 **加入 VMware 客戶經驗改進計劃** 核取方塊。
- 5 切換 **排程** 切換開關，以停用或啟用資料收集。
排程預設為啟用。
- 6 (選擇性) 設定資料收集和上傳週期設定。
- 7 按一下 **儲存**。

將標籤新增至物件

您可以將標記新增至物件使搜尋更為輕鬆。指定標籤時，您也可以指定範圍。

NSX Cloud 附註 若使用 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清單、支援的功能和 NSX Cloud 所需的組態。

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 編輯物件。

例如，移至**區段**索引標籤，然後編輯區段。

3 移至**標籤**欄位，然後新增標籤。

每個標籤都有一個必要的標籤值，和選用的範圍值。一個物件最多可以有 30 個標記。標籤的長度上限為 256 個字元。範圍的長度上限為 128 個字元。

4 按一下**儲存**。

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 21-4. 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
```

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。

使用 NSX Cloud

22

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。

請參閱《NSX-T Data Center 安裝指南》中的[安裝 NSX Cloud 元件](#)以取得 NSX Cloud 部署工作流程。

另請參閱：[公有雲](#)。

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](#)
- [常見問題集](#)

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。

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。
- 您可以在傳送 VPC/VNet 中部署一或兩個 (對於 HA) PCG。
- 您可以將計算 VPC/VNet 連結到傳送 VPC/VNet。
- 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。

備註 在網格視圖中，您可以看到三個索引標籤：**概觀**、**執行個體**以及**區段**。

- **概觀**會列出動作下的選項，如下一個步驟所述。
 - **執行個體**會顯示 VPC/VNet 中的執行個體清單。
 - **區段**會顯示 NSX-T 中的覆疊區段。NSX Cloud 的目前版本不支援此功能。請勿使用此畫面上顯示的標籤來標記 AWS 或 Microsoft Azure 中的工作負載虛擬機器。
-
- 按一下**動作**可存取下列項目：
 - **編輯組態** (僅適用於傳送 VPC/VNet)：
 - 啟用或停用隔離原則。
 - 變更 Proxy 伺服器選擇。
 - **連結至傳送 VPC/VNet**：此選項僅適用於其中未部署任何 PCG 的 VPC/VNet。按一下以選取要連結到的傳送 VPC/VNet。
 - **部署 NSX Cloud 開道**：此選項僅適用於其中未部署 PCG 的 VPC/VNet。按一下此選項，可開始在此 VPC/VNet 中部署 PCG，並使其成為傳送 VPC/VNet 或自行管理的 VPC/VNet。如需詳細指示，請參閱《NSX-T Data Center 安裝指南》中的〈**部署或連結 NSX 公用雲端開道**〉。

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。

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，且您必須擁有管理員帳戶的使用者名稱和密碼，才能登入 NSX Manager。
- 必須安裝 CSM，且您必須擁有 CSM 中指派的企業管理員角色。

程序

- 1 在瀏覽器中，登入 CSM。
- 2 當安裝精靈中出現提示時，按一下**開始設定**。
- 3 在 [NSX Manager 認證] 畫面中，輸入下列詳細資料：

選項	說明
NSX Manager 主機名稱	輸入 NSX Manager 的完整網域名稱 (FQDN) (如果有)。您也可以輸入 NSX Manager 的 IP 位址。
管理員認證	輸入 NSX Manager 的企業管理員使用者名稱和密碼。
管理員指紋	(選擇性) 輸入 NSX Manager 的指紋值。如果您將此欄位保留空白，系統會識別指紋，並顯示在下一個畫面中。

- 4 (選擇性) 如果您未提供 NSX Manager 的指紋值，或者值不正確，則會顯示**驗證指紋**畫面。選取核取方塊以接受系統探索到的指紋。
- 5 按一下**連線**。

備註 如果安裝精靈中遺失此設定或您想要變更相關聯的 NSX Manager，請登入 CSM，按一下**系統 > 設定**，然後在標題為**相關聯的 NSX 節點**面板上按一下**設定**。

CSM 會確認 NSX Manager 指紋並建立連線。

- 6 (選擇性) 設定 Proxy 伺服器。請參閱 [\(選用\) 設定 Proxy 伺服器](#) 中的指示。

(選用) 設定 Proxy 伺服器

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

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

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

您可以選擇以下層級的驗證：

- 認證式驗證。
- 適用於 HTTPS 攔截的憑證式驗證。
- 無驗證。

程序

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

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

- 2 在 [設定 Proxy 伺服器] 畫面中，輸入下列詳細資料：

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

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

在傳送 VPC/VNet 上部署 PCG，或將計算 VPC/VNet 連結到傳送 VPC/VNet 時，您可以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

您的傳送 VPC/VNet 必須已部署且正在執行一個或一對 PCG。

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**。按一下傳送 VPC 或計算 VPC。
 - b 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下傳送 VNet 或計算 VNet。
- 2 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 VPC 或 VNet 旁的核取方塊，然後按一下**動作 > 編輯組態**。

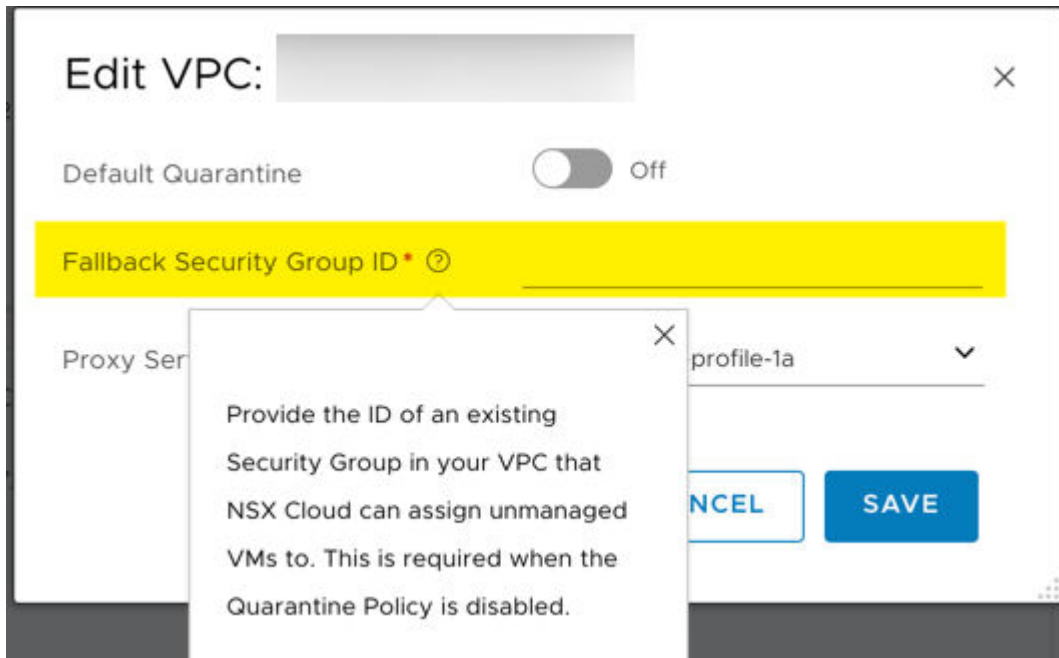


- ◆ 如果您是在 VPC 或 VNet 的頁面中，請按一下 [動作] 圖示，移至**編輯組態**。



- 3 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。
- 確定下列連接埠已開啟：
 - 輸入 UDP 6081：用於覆疊資料封包。對於 (作用中/待命) PCG 的 VTEP IP 位址 (eth1 介面)，應允許使用該連接埠。
 - 輸出 TCP 5555：用於控制封包。對於 (作用中/待命) PCG 的管理 IP 位址 (eth0 介面)，應允許使用該連接埠。
 - TCP 8080：用於 PCG 的管理 IP 位址上的安裝/升級。
 - TCP 80：用來在安裝 NSX 代理程式時下載任何第三方相依性。

- UDP 67、68：用於 DHCP 封包。
- UDP 53：用於 DNS 解析。

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响：

表 22-1. 停用隔離原則對安全群組的影响

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响

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 22-2. 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 22-3. 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 22-4. 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

請參閱檢查清單，以瞭解將工作負載虛擬機器上線並進行管理所涉及的步驟概觀。

如需 0 天工作流程，請參閱《NSX-T Data Center 安裝指南》中的〈[為公有雲安裝和設定 NSX Cloud 元件的概觀](#)〉。

如何將工作負載虛擬機器上線及進行管理

請參閱此工作流程，瞭解從公有雲將工作負載虛擬機器上線並進行管理的步驟概觀。

表 22-5. 將工作負載虛擬機器在 NSX Cloud 中上線的 N 天工作流程

工作	角色	指示
<input type="checkbox"/> 如果啟用了 [隔離原則]，則將虛擬機器置於 vm_underlay_sg 安全群組中。 如果停用了 [隔離原則]，則將虛擬機器置於 vm_override_sg 安全群組中。	公有雲管理員	請依照公有雲說明文件中將工作負載虛擬機器置於特定安全群組的指示操作。
<input type="checkbox"/> 使用索引鍵-值 nsx.network=default 標記工作負載虛擬機器。	公有雲管理員	請依照公有雲說明文件中標記工作負載虛擬機器的指示操作。

表 22-5. 將工作負載虛擬機器在 NSX Cloud 中上線的 N 天工作流程 (續)

工作	角色	指示
<input type="checkbox"/> 在您的 Windows 與 Linux 工作負載虛擬機器上安裝 NSX 代理程式。 備註 如果在 CSM 中已針對 Microsoft Azure 帳戶開啟 自動代理程式安裝 ，則會自動安裝 NSX 代理程式。	公有雲管理員	請參閱 安裝 NSX 代理程式 。
<input type="checkbox"/> 如果啟用了 [隔離原則]，請將虛擬機器置於 預設 安全群組中。	公有雲管理員	請依照公有雲說明文件中將工作負載虛擬機器置於特定安全群組的指示操作。
<input type="checkbox"/> 若要允許對工作負載虛擬機器的輸入存取，請視需要建立 Distributed Firewall (DFW) 規則。	NSX-T Data Center 企業管理員	請參閱 NSX 管理的工作負載虛擬機器的 DFW 規則 。
<input type="checkbox"/> 使用公有雲標籤或 NSX-T Data Center 標籤將工作負載虛擬機器分組，然後設定微分割。	NSX-T Data Center 企業管理員	請參閱 使用 NSX-T Data Center 和公有雲標記分組虛擬機器 。

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。

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
- Ubuntu 14.04、16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Sever 2016
- Microsoft Windows 10

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

如需有關在已安裝 NSX 代理程式的情況下建立 AMI 或受管理映像的指示，請參閱[產生可複製的映像](#)。

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](#)。

備註 若要確認此指令碼的總和檢查碼，請移至 **VMware 下載 > 驅動程式和工具 > NSX Cloud 指令碼**。

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**。按一下傳送 VPC 或計算 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。

附註： 傳送 VPC/VNet 用於部署並執行一個或一對 PCG。計算 VPC/VNet 會連結到傳送 VPC/VNet，並且可以使用其中部署的 PCG。

- 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 對於 VNet，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。對於傳送 VNet，`-dnsServer <dns-server-ip>` 參數是選擇性的。對於計算 VNet，必須提供 DNS 轉寄站 IP 位址，才能完成此命令。

- 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。

備註 若要確認此指令碼的總和檢查碼，請移至 **VMware 下載 > 驅動程式和工具 > NSX Cloud 指令碼**。

附註：

- 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。

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](#)。

備註 若要確認此指令碼的總和檢查碼，請移至 **VMware 下載 > 驅動程式和工具 > NSX Cloud 指令碼**。

必要條件

您需要使用下列命令來執行 NSX 代理程式安裝指令碼：

■ wget

- **nslookup**
- **dmidecode**

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**。按一下傳送 VPC 或計算 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。

附註：傳送 VPC/VNet 用於部署並執行一個或一對 PCG。計算 VPC/VNet 會連結到傳送 VPC/VNet，並且可以使用其中部署的 PCG。

- 2 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 對於 VNet，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。對於傳送 VNet，`-dnsServer <dns-server-ip>` 參數是選擇性的。對於計算 VNet，必須提供 DNS 轉寄站 IP 位址，才能完成此命令。

- 3 使用超級使用者權限登入 Linux 工作負載虛擬機器。
- 4 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。

備註 若要確認此指令碼的總和檢查碼，請前往 **VMware 下載 > 驅動程式和工具 > NSX Cloud 指令碼**。

- 5 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：

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

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。

後續步驟

管理工作負載虛擬機器

解除安裝 NSX 代理程式

使用這些作業系統專屬命令可解除安裝 NSX 代理程式。

從 Windows 虛擬機器解除安裝 NSX 代理程式

備註 若要查看其他適用於安裝指令碼的選項，請使用 `-help`。

- 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
```

解除安裝 Linux 虛擬機器上的 NSX 代理程式

備註 若要查看其他適用於安裝指令碼的選項，請使用 `--help`。

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

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

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。
- 套用到 Microsoft Azure 中的虛擬機器的安全群組必須允許安裝 NSX 代理程式。如果隔離原則已啟用，請將 `vm-override-sg` 套用到工作負載虛擬機器。如果隔離原則已停用，則向其套用 `vm_underlay_sg`。
- 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**。



4 將**自動代理程式安裝**旁的滑桿移至 [開啟] 位置。

備註 如果 NSX 代理程式安裝失敗，請執行下列操作：

- 1 登入 Microsoft Azure 入口網站，然後導覽至 NSX 代理程式安裝失敗的虛擬機器。
- 2 前往虛擬機器的延伸，並解除安裝名為 `VMwareNsxAgentInstallCustomScriptExtension` 的延伸。
- 3 從此虛擬機器移除 `nsx.network` 標籤。
- 4 在此虛擬機器上再次新增 `nsx.network` 標籤。

在大約三分鐘內，NSX 代理程式將會安裝在此虛擬機器上。

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。

NSX 管理的工作負載虛擬機器的 DFW 規則

當您在傳送 VPC/VNet 上部署 PCG，或將計算 VPC/VNet 連結到傳送 VPC/VNet 時，NSX Cloud 會為 NSX 管理的工作負載虛擬機器建立預設 DFW 規則，該規則會封鎖所有連到這些虛擬機器的輸入連線。

兩個無狀態規則適用於 DHCP 存取，並且不會影響對工作負載虛擬機器的存取。

兩個可設定狀態的規則如下：

NSX Cloud 在 [原則] 下建立的 DFW 規則：cloud-stateful-cloud-<VPC/VNet ID>	內容
cloud-<VPC/VNet ID>-managed	允許存取同一 VPC/VNet 內的虛擬機器。
cloud-<VPC/VNet ID>-inbound	禁止從 VPC/VNet 外部的任何位置存取 NSX 管理的虛擬機器。

備註 請勿編輯任何一個預設規則。

您可以建立現有輸入規則的複本，接著調整來源和目的地，然後將規則設定為**允許**。將**允許**規則放置在高於預設**拒絕**規則的位置。您也可以新增原則和規則。如需指示，請參閱**新增分散式防火牆**。

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。

備註 DFW 規則取決於指派給虛擬機器的標籤。由於這些標籤可由具有適當公有雲權限的任何人修改，因此 NSX-T Data Center 會假設此類使用者可信賴，且公有雲網路系統管理員需負責確保和稽核虛擬機器在任何時間都已正確標記。

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
 - azure:transit_vnet_name
 - azure:transit_vnet_rg
 - aws:account
 - aws:availabilityzone
 - aws:region
 - aws:vpc
 - aws:subnet
 - aws:transit_vpc
- **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，而以 **dis:aws** 做為前置詞的標籤則是從 AWS 探索到的。

當您對公有雲中的標籤進行任何變更時，這些變更會在三分鐘內反映在 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 22-6. 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:availability zone 	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 22-7.

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
Abcdefghijklmnopqrstuvwxyz=value2	否 (金鑰超過 20 個字元)	無
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgjguytreswqacvbcdefghijklmnopqrstuvwxyz	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。

若要對 NSX 所管理的工作負載虛擬機器套用 Distributed Firewall 規則，請執行下列動作：

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

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

備註 DFW 規則取決於指派給虛擬機器的標籤。由於這些標籤可由具有適當公有雲權限的任何人修改，因此 NSX-T Data Center 會假設此類使用者可信賴，且公有雲網路系統管理員需負責確保和稽核虛擬機器在任何時間都已正確標記。

- 2 建立東西向 Distributed Firewall 原則與規則，然後套用至您建立的群組。請參閱[新增分散式防火牆](#)。

手動重新同步 CSM 中的詳細目錄後，或是將公有雲中的變更提取到 CSM 後約三分鐘內，此微分割便會生效。

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

如需有關成功部署 PCG 後建立之邏輯實體的詳細資料，請參閱《NSX-T Data Center 安裝指南》中的〈自動建立的 NSX-T 邏輯實體〉。

重要 請勿編輯或刪除任何這些自動建立的實體。

備註 如果您無法存取 Windows 工作負載虛擬機器上的部分功能，請確定您已正確設定 Windows 防火牆設定。

邏輯區段常見問題集

表 22-8.

問題	回答
在哪可以找到邏輯區段的詳細資料？	請參閱第 4 章 區段
在哪可以找到邏輯交換器的詳細資訊？	請參閱第 13 章 邏輯交換器。

邏輯路由器常見問題集

表 22-9.

問題	回答
部署 PCG 時，NSX Cloud 會自動建立邏輯路由器嗎？	是。在傳送 VPC 或 Vnet 上部署 PCG 時，NSX Cloud 會自動建立第 0 層邏輯路由器。每次有計算 VPC/VNet 連結至傳送 VPC/VNet 時，則會針對其建立一個第 1 層路由器。
在哪可以找到邏輯路由器的詳細資訊？	請參閱第 2 章 第 0 層閘道與第 3 章 第 1 層閘道。

IPFIX 常見問題集

表 22-10.

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？	是。 <ul style="list-style-type: none"> NSX Cloud 僅在 UDP 連接埠 4739 上支援 IPFIX。 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 22-11.

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 22-12.

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

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
```

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`。

在 NSX 管理的虛擬機器上啟用 NAT

NSX Cloud 支援在 NSX 管理的虛擬機器上啟用 NAT。

您可以在 NSX 管理的虛擬機器中，使用公有雲標籤啟用虛擬機器的南北向流量。

在您要啟用 NAT 之 NSX 管理的虛擬機器上，套用下列標籤：

表 22-13.

金鑰	值
<code>nsx.publicip</code>	您的公有雲提供的公用 IP 位址，例如 50.1.2.3

備註 您在此處提供的公用 IP 位址必須未被佔用，並且不得已指派給任何虛擬機器，即使是您要為其啟用 NAT 的工作負載虛擬機器亦然。如果您指派的公用 IP 位址先前已與任何其他執行個體或私人 IP 位址相關聯，NAT 將無法運作。在此情況下，請取消指派公用 IP 位址。

在套用此標籤後，工作負載虛擬機器即可存取網際網路流量。

產生可複製的映像

您可以針對已安裝 NSX 代理程式的虛擬機器，在 AWS 中產生 AMI，或在 Microsoft Azure 中產生受管理的映像。

藉由這項功能，您可以啟動其代理程式已設定好並在執行中的多個虛擬機器。

您可以使用下列兩種方式，來為已安裝 NSX 代理程式的虛擬機器產生 AMI/受管理的映像（下文皆稱為「映像」）：

- **使用未設定的 NSX 代理程式產生映像：**您可以從已安裝 NSX 代理程式但未使用 `-noStart` 選項加以設定的虛擬機器產生映像。此選項可讓您擷取並安裝 NSX 代理程式套件，但不會啟動 NSX 服務。此外，不會進行任何 NSX 組態設定，例如產生憑證。
- **移除現有 NSX 代理程式組態後產生映像：**您可以從現有 NSX 管理的虛擬機器移除組態，然後使用該虛擬機器來產生映像。

使用未設定的 NSX 代理程式產生 AMI

您可以在虛擬機器上已安裝 NSX 代理程式但未設定的情況下，產生該虛擬機器的 AMI。

若要使用 **noStart** 選項從安裝了 NSX 代理程式的虛擬機器產生映像，請執行下列操作：

程序

- 1 從 CSM 複製並貼上 NSX 代理程式安裝命令。請參閱相關說明，網址為：[安裝 NSX 代理程式](#)

- a 編輯適用於 Windows 的命令，如下所示：

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

- b 編輯適用於 Linux 的命令，如下所示：

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 在公有雲中移至此虛擬機器並建立映像。

移除現有的 NSX 代理程式組態後產生映像

您可以為具有已設定的 NSX 代理程式的虛擬機器產生映像。

若要從現有的 NSX 管理的虛擬機器移除組態並將其用於產生映像，請執行下列操作：

程序

- 1 從 Windows 或 Linux 虛擬機器移除 NSX 代理程式組態：

- a 最好使用 jump host 登入工作負載虛擬機器。
 - b 開啟 NSX-T CLI：

```
sudo nsxcli
```

- c 輸入下列命令：

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 在公有雲中找到此虛擬機器並建立映像。

針對公有雲的服務插入

NSX Cloud 支援在公有雲中針對 NSX 管理的工作負載虛擬機器使用第三方服務。

若要針對公有雲工作負載虛擬機器使用服務插入，您必須在公有雲中裝載服務應用裝置，而不是在 NSX-T Data Center 中。建議在傳送 VPC/VNet 中裝載服務應用裝置。

您必須在傳送 VPC 或 VNet 中部署 PCG，才能啟用服務插入。

以下是允許針對 NSX 管理的工作負載虛擬機器使用服務插入的一次性組態的概觀。

表 22-14. 針對公有雲中 NSX 管理的工作負載虛擬機器使用服務插入所需的組態的概觀

頻率?	工作	指示
初始設定一次	最好在傳送 VPC 或 VNet (已在其中部署 PCG) 中設定公有雲中的服務應用裝置。	請參閱第三方服務應用裝置和公有雲的特定指示。
	在 NSX-T Data Center 中登錄第三方服務。	請參閱 建立服務定義和對應的虛擬端點
	使用 /32 虛擬服務 IP 位址 (VSIP) 建立服務的虛擬執行個體端點，以僅供服務應用裝置進行服務插入。VSIP 不應與 VPC 或 VNet 的 CIDR 範圍發生衝突。此 VSIP 透過 BGP 向 PCG 通告。	請參閱 建立服務定義和對應的虛擬端點
	建立服務應用裝置和 PCG 之間的 IPSec VPN 通道。	請參閱 設定 IPSec VPN 工作階段
	設定 PCG 和服務應用裝置之間的 BGP。	請參閱 設定 BGP 和路由重新分配
	備註 將服務應用裝置設定為通告 VSIP，而 PCG 設定為通告預設路由 (0.0.0.0/0)。	
在需要時	一次性組態完成後，請設定重新導向規則將 NSX 管理的工作負載虛擬機器中的選擇性流量重新路由到 VSIP。這些規則會套用到 PCG 的上行連接埠。	請參閱 設定重新導向規則 。

程序

1 建立服務定義和對應的虛擬端點

您必須使用 NSX Manager API，為公有雲中的服務應用裝置建立服務定義和虛擬端點。

2 設定 IPSec VPN 工作階段

設定 PCG 和服務應用裝置之間的 IPSec VPN 工作階段。

3 設定 BGP 和路由重新分配

透過 IPSec VPN 通道設定 PCG 和服務應用裝置之間的 BGP。

4 設定重新導向規則

重新導向規則可根據您的需求進行調整。

建立服務定義和對應的虛擬端點

您必須使用 NSX Manager API，為公有雲中的服務應用裝置建立服務定義和虛擬端點。

必要條件

挑選出 /32 保留的 IP 位址做為公有雲中服務應用裝置的虛擬端點，例如 100.100.100.100/32。這被稱為虛擬服務 IP (VSIP)。

備註 如果在高可用性配對中已部署服務應用裝置，則不會建立另一個服務定義，而是在設定 BGP 期間向 PCG 進行通告時使用相同的 VSIP。

程序

- 1 若要為服務應用裝置建立服務定義，則使用用於授權的 NSX Manager 認證執行下列 API 呼叫：

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

範例要求：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

範例回應：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
  "_protection": "REQUIRE_OVERRIDE",
}
```

```

    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 若要為服務應用裝置建立虛擬端點，則使用用於授權的 NSX Manager 認證執行下列 API 呼叫：

```

PATCH https://{NSX Manager-IP}policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-services/
cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

範例要求：

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [ "100.100.100.100"
    ],
      "prefix_length": 32
    }
  ],
  "service_names": [ "Service_Appliance1"
  ]
}

```

範例回應：

```

200 OK

```

備註 步驟 1 中的 `display_name` 必須與步驟 2 中的 `service_names` 相符。

後續步驟

設定 IPsec VPN 工作階段

設定 IPsec VPN 工作階段

設定 PCG 和服務應用裝置之間的 IPsec VPN 工作階段。

必要條件

- 一個 PCG 或 PCG 的 HA 配對必須在傳送 VPC/VNet 中部署。
- 必須在公有雲中設定服務應用裝置，最好是在傳送 VPC/VNet 中設定。

程序

- 1 導覽至 **網路 > VPN**

- 2 新增 IPsec 類型的 **VPN 服務**，並注意特定於 NSX Cloud 的下列組態選項。如需其他詳細資料，請參閱[新增 IPsec VPN 服務](#)。

選項	說明
名稱	此 VPN 服務的名稱可用來設定本機端點和 IPsec VPN 工作階段。請記下該名稱。
服務類型	確認此值會設為 IPsec。
第 0 層閘道	選取為傳送 VPC/VNet 自動建立的第 0 層閘道。其名稱中包含您的 VPC/VNet 識別碼，例如 <code>cloud-t0-vpc-6bcd2c13</code> 。

- 3 為 PCG 新增**本機端點**。本機端點的 IP 位址是傳送 VPC/VNet 中部署的 PCG 的 `nsx:local_endpoint_ip` 標籤的值。登入傳送 VPC/VNet 以取得該值。請注意特定於 NSX Cloud 的下列組態，並參閱[新增本機端點](#)以瞭解其他詳細資料。

選項	說明
名稱	本機端點名稱可用來設定 IPsec VPN 工作階段。請記下該名稱。
VPN 服務	選取步驟 2 中新增加的 VPN 服務。
IP 位址	登入 AWS 主控台或 Microsoft Azure 入口網站，以尋找此值。它是套用到 PCG 的上行介面的標籤 <code>nsx:local_endpoint_ip</code> 的值。

- 4 在 PCG 和公有雲中的服務應用裝置 (最好是裝載於傳送 VPC/VNet 中) 之間建立**以路由為基礎的 IPsec 工作階段**。

選項	說明
類型	確認此值會設為 以路由為基礎 。
VPN 服務	選取步驟 2 中新增加的 VPN 服務。
本機端點	選取步驟 3 中建立的本機端點。
遠端 IP	輸入服務應用裝置的私人 IP 位址。 備註 如果可以使用公用 IP 位址存取您的服務應用裝置，請將公用 IP 位址指派給 PCG 上行介面的本機端點 IP (也稱為次要 IP)。
通道介面	此子網路必須與 VPN 通道的服務應用裝置子網路相符。輸入您在 VPN 通道的服務應用裝置中設定的子網路值或記下在此處輸入的值，並確保在服務應用裝置中設定 VPN 通道時使用相同的子網路。 備註 在此通道介面上設定 BGP。請參閱 設定 BGP 和路由重新分配 。
遠端識別碼	輸入公有雲中服務應用裝置的私人 IP 位址。
IKE 設定檔	IPsec VPN 工作階段必須與 IKE 設定檔相關聯。如果已建立設定檔，請從下拉式功能表中選取該設定檔。您也可以使用預設設定檔。

後續步驟

設定 BGP 和路由重新分配

設定 BGP 和路由重新分配

透過 IPsec VPN 通道設定 PCG 和服務應用裝置之間的 BGP。

在 PCG 與服務應用裝置之間建立的 IPsec VPN 通道介面上設定 BGP 芳鄰。如需更多詳細資料，請參閱[設定 BGP](#)。

您需要以類似方式在服務應用裝置上設定 BGP。如需詳細資料，請參閱公有雲中特定服務的說明文件。

接下來，設定路由重新分配，如下所示：

- PCG 向服務應用裝置通告其預設路由 (0.0.0.0/0)。
- 服務應用裝置向 PCG 通告 VSIP。這是登錄服務時使用的相同 IP 位址。請參閱[建立服務定義和對應的虛擬端點](#)。

備註 如果您的服務應用裝置在高可用性配對中部署，請從兩個服務應用裝置通告相同的 VSIP。

必要條件

程序

- 1 導覽至**網路 > 第 0 層**欄道
- 2 為傳送 VPC/VNet (例如，名為 `cloud-t0-vpc-6bcd2c13`) 選取自動建立的第 0 層欄道，然後按一下**編輯**。
- 3 按一下 **BGP** 區段下 **BGP 芳鄰**旁的數字或圖示。
- 4 請注意下列組態：

選項	說明
IP 位址	將服務應用裝置通道介面上設定的 IP 位址用於 PCG 和服務應用裝置之間的 VPN。
遠端 AS 數目	此數目必須與公有雲中服務應用裝置的 AS 數目相符。

- 5 (必要) 從**靜態路由**區段中，設定 PCG 預設路由 (0.0.0.0/0) 的靜態路由。
- 6 從**路由重新分配**區段中，選取與預設路由相關聯的靜態路由。

後續步驟

設定重新導向規則

設定重新導向規則

重新導向規則可根據您的需求進行調整。

完成初始設定後，您可以根據需要建立和編輯重新導向規則，以便透過服務應用裝置為 NSX 管理的工作負載虛擬機器重新路由不同類型的流量。

必要條件

您必須完成所有服務插入設定，然後才能建立重新導向規則。

程序

- 1 導覽至 **安全性 > 南北向防火牆 > 網路自我檢查 (N-S)**
- 2 按一下 **新增原則**。

選項	說明
網域	NSX-T Data Center 2.4：選取為此傳送 VPC/VNet 的第 0 層閘道自動建立的網域，例如 <code>cloud-vpc-6bcd2c13</code> 。 NSX-T Data Center 2.4.1：網域物件不會在使用者介面中顯示。您不需要執行任何動作。
重新導向至：	選取在登錄服務時為此服務應用裝置建立的虛擬端點的名稱。請參閱 建立服務定義和對應的虛擬端點 。

- 3 選取新原則，然後按一下 **新增規則**。請注意特定於服務插入的下列值：

選項	說明
來源	選取必須重新導向其流量的一組子網路，例如，一組 NSX 管理的工作負載虛擬機器。
目的地	選取要透過服務應用裝置路由的目的地 IP 位址或服務的清單，例如 Google 。
套用至	選取主動和備用 PCG 的上行連接埠。
動作	選取 重新導向 。

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分散式防火牆 (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>
```

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[NSX 管理的工作負載虛擬機器的 DFW 規則](#)。
- 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。