

NSX-T Data Center 管理指南

修改日期：2022 年 5 月 06 日
VMware NSX-T Data Center 2.5

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 © 2022 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 13

1 NSX Manager 概觀 14

2 第 0 層閘道 17

- 新增第 0 層閘道 17
- 建立 IP 首碼清單 20
- 建立社群清單 21
- 設定靜態路由 22
- 建立路由對應 23
- 在新增路由對應時使用規則運算式來比對社群清單 25
- 設定 BGP 25
- 設定 BFD 28
- 設定 IPv6 第 3 層轉送 29
- 建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔 29

3 第 1 層閘道 31

- 新增第 1 層閘道 31

4 區段 34

- 區段設定檔 34
 - 瞭解 QoS 區段設定檔 35
 - 瞭解 IP 探索區段設定檔 37
 - 瞭解 SpoofGuard 區段設定檔 38
 - 瞭解區段安全性區段設定檔 40
 - 瞭解 MAC 探索區段設定檔 41
- 新增區段 42

5 虛擬私人網路 (VPN) 44

- 瞭解 IPsec VPN 45
 - 使用以原則為基礎的 IPsec VPN 45
 - 使用以路由為基礎的 IPsec VPN 46
- 瞭解第 2 層 VPN 47
- 新增 VPN 服務 48
 - 新增 IPsec VPN 服務 50
 - 新增 L2 VPN 服務 51
- 新增 IPsec VPN 工作階段 53

新增以原則為基礎的 IPSec 工作階段	53
新增路由型 IPSec 工作階段	56
關於支援的合規性套件	59
瞭解 TCP MSS 鉗制	60
新增 L2 VPN 工作階段	60
新增 L2 VPN 伺服器工作階段	60
新增 L2 VPN 用戶端工作階段	62
下載遠端 L2 VPN 組態檔	63
新增本機端點	64
新增設定檔	65
新增 IKE 設定檔	65
新增 IPSec 設定檔	68
新增 DPD 設定檔	70
新增自發 Edge 作為 L2 VPN 用戶端	70
檢查 IPSec VPN 工作階段的實現狀態	73
監控和疑難排解 VPN 工作階段	75

6 網路位址轉譯 77

在閘道上設定 NAT	77
------------	----

7 負載平衡 79

主要負載平衡器概念	79
調整負載平衡器資源	80
支援的負載平衡器功能	81
負載平衡器拓撲	82
設定負載平衡器元件	84
新增負載平衡器	84
新增主動監視器	86
新增被動監視器	89
新增伺服器集區	90
設定虛擬伺服器元件	93
針對伺服器集區和虛擬伺服器建立的群組	113

8 轉送原則 114

新增或編輯轉送原則	115
-----------	-----

9 IP 位址管理 (IPAM) 116

新增 DNS 區域	116
新增 DNS 轉寄站服務	117
新增 DHCP 伺服器	118
設定第 0 層或第 1 層閘道的 DHCP 轉送伺服器	119

新增 IP 位址集區 120

新增 IP 位址區塊 120

10 安全性 122

安全性組態概觀 122

安全性術語 123

身分識別防火牆 123

身分識別防火牆工作流程 124

第 7 層內容設定檔 126

第 7 層防火牆規則工作流程 127

屬性 127

分散式防火牆 131

防火牆草稿 131

新增分散式防火牆 133

分散式防火牆封包記錄 136

選取預設的連線策略 138

管理防火牆排除清單 138

篩選特定網域 (FQDN/URL) 139

將安全性原則延伸至實體工作負載 140

共用位址集 146

東西向網路安全性 - 鏈結第三方服務 147

東西向網路保護的主要概念 147

東西向流量的 NSX-T Data Center 需求 148

東西向網路安全性的高階工作 148

部署用於執行東西向流量自我檢查的服務 148

新增服務設定檔 150

新增服務鏈結 150

新增東西向流量的重新導向規則 151

設定閘道防火牆 153

新增閘道防火牆原則和規則 153

南北向網路安全性 - 插入第三方服務 155

南北向網路安全性的高階工作 155

部署用於執行南北向流量自我檢查的服務 156

設定流量重新導向 158

針對南北向流量新增重新導向規則 159

監控流量重新導向 160

端點保護 160

瞭解端點保護 160

設定端點保護 164

管理端點保護 178

安全性設定檔 187

- 建立工作階段計時器 187
- 洪泛保護 189
- 設定 DNS 安全性 191
- 管理群組與設定檔的優先順序 192

11 詳細目錄 194

- 新增服務 194
- 新增群組 195
- 新增內容設定檔 196

12 監控 198

- 新增防火牆 IPFIX 設定檔 198
- 新增交換器 IPFIX 設定檔 199
- 新增 IPFIX 收集器 200
- 新增連接埠鏡像設定檔 200
- 簡易網路管理通訊協定 (SNMP) 201
- 使用 vRealize Log Insight 進行系統監控 202
- 使用 vRealize Operations Manager 進行系統監控 203
- 使用 vRealize Network Insight Cloud 進行系統監控 205
- 進階監控工具 214
 - 檢視連接埠連線資訊 214
 - Traceflow 215
 - 監控連接埠鏡像工作階段 217
 - 為連接埠鏡像工作階段設定篩選器 220
 - 設定 IPFIX 221
 - 監控邏輯交換器連接埠活動 395

13 邏輯交換器 397

- 瞭解 BUM 框架複寫模式 398
- 建立邏輯交換器 399
- 將虛擬機器連線到邏輯交換器 400
 - 將 vCenter Server 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器 400
 - 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 402
 - 將 KVM 上裝載的虛擬機器連結至 NSX-T Data Center 邏輯交換器 407
- 建立邏輯交換器連接埠 408
- 測試第 2 層連線 408
- 為 NSX Edge 上行建立 VLAN 邏輯交換器 411
- 邏輯交換器和邏輯連接埠的交換設定檔 413
 - 瞭解 QoS 交換設定檔 414
 - 瞭解連接埠鏡像交換設定檔 416
 - 瞭解 IP 探索交換設定檔 418

瞭解 SpoofGuard	419
瞭解交換器安全性交換設定檔	421
瞭解 MAC 管理交換設定檔	423
建立自訂設定檔與邏輯交換器之間的關聯	424
建立自訂設定檔與邏輯連接埠之間的關聯	425
進階網路堆疊	426
自動指派 ENS 邏輯核心	426
設定客體 VLAN 間路由	427
第 2 層橋接	428
建立 Edge 橋接器設定檔	429
設定以 Edge 為基礎的橋接	429
建立第 2 層橋接器備份邏輯交換器	432

14 邏輯路由器 434

第 1 層邏輯路由器	434
建立第 1 層邏輯路由器	435
在第 1 層邏輯路由器上新增下行連接埠	437
在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠	438
在第 1 層邏輯路由器上設定路由通告	438
設定第 1 層邏輯路由器靜態路由	440
建立獨立的第 1 層邏輯路由器	442
第 0 層邏輯路由器	443
建立第 0 層邏輯路由器	445
連結第 0 層和第 1 層	446
針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器	448
新增回送路由器連接埠	451
在第 0 層或第 1 層邏輯路由器上新增 VLAN 連接埠	451
設定靜態路由	452
BGP 組態選項	456
在第 0 層邏輯路由器上設定 BFD	461
啟用第 0 層邏輯路由器上的路由重新分配	462
瞭解 ECMP 路由	465
建立 IP 首碼清單	468
建立社群清單	469
建立路由對應	470
設定轉送累計計時器	471

15 進階 NAT 472

網路位址轉譯	472
第 1 層 NAT	474
第 0 層 NAT	480

自反 NAT 481

16 進階群組物件 484

- 建立 IP 集合 484
- 建立 IP 集區 485
- 建立 MAC 集合 485
- 建立 NSGroup 486
- 設定服務和服務群組 487
 - 建立 NSService 488
- 管理虛擬機器的標記 488

17 進階 DHCP 490

- DHCP 490
 - 建立 DHCP 伺服器設定檔 490
 - 建立 DHCP 伺服器 491
 - 將 DHCP 伺服器連結至邏輯交換器 492
 - 從邏輯交換器中斷連結 DHCP 伺服器 492
 - 建立 DHCP 轉送設定檔 492
 - 建立 DHCP 轉送服務 493
 - 將 DHCP 轉送服務新增至邏輯路由器連接埠 493
 - 刪除 DHCP 租用 493
- 中繼資料 Proxy 494
 - 新增中繼資料 Proxy 伺服器 494
 - 將中繼資料 Proxy 伺服器連結至邏輯交換器 495
 - 將中繼資料 Proxy 伺服器與邏輯交換器中斷連結 495

18 進階 IP 位址管理 496

- 管理 IP 區塊 496
- 管理 IP 區塊的子網路 497

19 進階負載平衡 498

- 主要負載平衡器概念 499
- 設定負載平衡器元件 499
 - 建立負載平衡器 500
 - 設定主動健全狀況監視器 501
 - 設定被動健全狀況監視器 504
 - 新增用於負載平衡的伺服器集區 505
 - 設定虛擬伺服器元件 508

20 進階防火牆 527

- 新增或刪除邏輯路由器的防火牆規則 527

為邏輯交換器橋接器連接埠設定防火牆	528
防火牆區段和防火牆規則	528
啟用和停用 Distributed Firewall	529
新增防火牆規則區段	529
刪除防火牆規則區段	530
啟用和停用區段規則	530
啟用和停用區段記錄	531
設定防火牆排除清單	531
關於防火牆規則	531
新增防火牆規則	532
刪除防火牆規則	534
編輯預設 Distributed Firewall 規則	535
變更防火牆規則的順序	535
篩選防火牆規則	536

21 作業和管理 537

檢視監控儀表板	538
檢視物件類別的使用量和容量	540
查看組態變更的實現狀態	541
搜尋物件	545
依物件屬性篩選	546
新增計算管理程式	547
新增 Active Directory	548
新增 LDAP 伺服器	549
同步 Active Directory	550
管理使用者帳戶和角色型存取控制	551
變更使用者的密碼	551
重設應用裝置的密碼	552
驗證原則設定	553
從 vIDM 主機取得憑證指紋	554
設定 VMware Identity Manager 整合	555
驗證 VMware Identity Manager 功能	557
NSX Manager、vIDM 和相關元件之間的時間同步	558
角色型存取控制	559
新增角色指派或主體身分識別	567
備份和還原 NSX Manager	569
設定備份	569
移除舊備份	571
列出可用的備份	571
還原備份	572
升級期間的備份和還原	574

從 vCenter Server 移除 NSX-T Data Center 延伸	574
管理 NSX Manager 叢集	575
檢視 NSX Manager 叢集的組態和狀態	575
關閉 NSX Manager 叢集及開啟其電源	578
將 NSX Manager 重新開機	578
變更 NSX Manager 的 IP 位址	579
調整 NSX Manager 節點的大小	580
將 ESXi 主機傳輸節點新增至 vCenter Server 和從中移除	581
取代 NSX Edge 叢集中的 NSX Edge 傳輸節點	582
使用 NSX Manager UI 取代 NSX Edge 傳輸節點	582
使用 API 取代 NSX Edge 傳輸節點	582
在 vCenter Server 遺失且無法復原時，復原 NSX-T。	584
NSX-T Data Center 的多站台部署	585
設定應用裝置	593
新增授權金鑰並產生授權使用率報告	593
設定憑證	594
匯入憑證	595
建立憑證簽署要求檔案	595
匯入 CA 憑證	596
建立自我簽署的憑證	597
取代 NSX Manager 節點的憑證或 NSX Manager 叢集虛擬 IP	598
匯入憑證撤銷清單	598
設定 NSX Manager 以擷取憑證撤銷清單	599
匯入 CSR 的憑證	600
公用憑證和私密金鑰的儲存區	600
符合性組態	601
檢視符合性狀態報告	601
符合性狀態報告代碼	602
設定負載平衡器的全域 FIPS 符合性模式	604
收集支援服務包	606
記錄訊息和錯誤碼	607
設定遠端記錄	609
記錄訊息識別碼	616
對 Syslog 問題進行疑難排解	617
在應用裝置虛擬機器上設定序列記錄	618
客戶經驗改進計劃	618
編輯客戶經驗改進計劃組態	618
將標籤新增至物件	619
尋找遠端伺服器的 SSH 指紋	620
檢視在虛擬機器上執行之應用程式的相關資料	621
設定外部負載平衡器	621

22 使用 NSX Cloud 623

- Cloud Service Manager 的快速導覽 623
 - 雲端 623
 - 系統 630
- 使用 NSX Cloud 隔離原則的威脅偵測 632
 - NSX 強制執行模式 中的隔離原則 633
 - 原生雲端強制執行模式 中的隔離原則 637
 - 將虛擬機器加入白名單 638
- NSX 強制執行模式 639
 - 目前支援工作負載虛擬機器的作業系統 639
 - 在 NSX 強制執行模式 中讓虛擬機器上線 640
 - 在 NSX 強制執行模式 中管理虛擬機器 647
- 原生雲端強制執行模式 649
 - 在 原生雲端強制執行模式 中管理虛擬機器 649
- NSX-T Data Center 功能支援 NSX Cloud 652
 - 使用 NSX-T Data Center 和公有雲標記分組虛擬機器 653
 - 使用原生雲端服務 656
 - 針對公有雲的服務插入 657
 - 在 NSX 管理的虛擬機器上啟用 NAT 663
 - 啟用 Syslog 轉送 664
 - 在 NSX 強制執行模式中設定 VPN 664
- 常見問題集 (FAQ) 669

23 使用 NSX Intelligence 672

- 開始使用 NSX Intelligence 672
 - NSX Intelligence 首頁的導覽 672
 - 請熟悉 NSX Intelligence 圖形元素 674
- 瞭解 NSX Intelligence 視圖和流量 676
 - 使用群組視圖 676
 - 使用虛擬機器視圖 680
 - 使用流量 682
- 使用 NSX Intelligence 建議 684
 - 了解 NSX Intelligence 建議 684
 - 產生新的 NSX Intelligence 建議 684
 - 檢閱並發佈產生的建議 686
- 備份和還原 NSX Intelligence 687
 - 設定 NSX Intelligence 備份 688
 - 備份 NSX Intelligence 688
 - 還原 NSX Intelligence 備份 689
- 疑難排解 NSX Intelligence 問題 690

[檢查 NSX Intelligence 應用裝置的狀態](#) 690

[收集 NSX Intelligence 支援服務包](#) 695

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，則在多數情況下，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"> ■ 轉送累計計時器 ■ 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 ■ 草稿 	<p>僅在進階介面中可用的安全性功能：</p> <ul style="list-style-type: none"> ■ CPU 和記憶體臨界值 ■ 橋接防火牆 ■ 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 	<p>進階網路與安全性索引標籤</p>
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，原則型使用者界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 [NSX-T Data Center 功能支援 NSX Cloud](#) 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](#)
- [在新增路由對應時使用規則運算式來比對社群清單](#)
- [設定 BGP](#)
- [設定 BFD](#)
- [設定 IPv6 第 3 層轉送](#)
- [建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔](#)

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-主動式或主動備用。下列服務僅在主動備用模式中受到支援：

- 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。

如果您為第 0 層閘道設定路由重新分配，則有兩個來源群組可供選取：第 0 層子網路和通告的第 1 層子網路。第 0 層子網路群組中的來源為：

來源類型	說明
已連線的介面與區段	其中包括連線至第 0 層閘道的外部介面子網路、服務介面子網路和區段子網路。
靜態路由	您已在第 0 層閘道上設定的靜態路由。
NAT IP	第 0 層閘道所擁有，且從第 0 層閘道上所設定 NAT 規則探索而來 NAT IP 位址。
IPSec 本機 IP	用來建立 VPN 工作階段的本機 IPSEC 端點 IP 位址。
DNS 轉寄站 IP	負責處理來自用戶端的 DNS 查詢，同時作為來源 IP 用來將 DNS 查詢轉送至上游 DNS 伺服器的接聽程式 IP。

通告的第 1 層子網路群組中的來源為：

來源類型	說明
已連線的介面與區段	其中包括連線至第 1 層閘道的區段子網路，和第 1 層閘道上所設定的服務介面子網路。
靜態路由	您已在第 1 層閘道上設定的靜態路由。
NAT IP	第 1 層閘道所擁有，並從第 1 層閘道上所設定的 NAT 規則探索到的 NAT IP 位址。
LB VIP	負載平衡虛擬伺服器的 IP 位址。
LB SNAT IP	由負載平衡器用於來源 NAT 的 IP 位址或 IP 位址範圍。
DNS 轉寄站 IP	負責處理來自用戶端的 DNS 查詢，同時作為來源 IP 用來將 DNS 查詢轉送至上游 DNS 伺服器的接聽程式 IP。
IPSec 本機端點	IPSec 本機端點的 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 > 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 選取 HA (高可用性) 模式。

預設模式為主動-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 (選擇性) 選取 NSX Edge 叢集。

8 (選擇性) 新增一或多個標籤。

9 (選擇性) 按一下 **其他設定**。

a 在 **內部傳送子網路** 欄位中，輸入子網路。

這是用於在此閘道內元件之間通訊的子網路。預設值為 169.254.0.0/28。

b 在 **T0-T1 傳送子網路** 欄位中，輸入一或多個子網路。

這些子網路用於此閘道和與其連結的所有第 1 層閘道之間的通訊。建立此閘道並將第 1 層閘道與其連結後，您會看到指派給第 0 層閘道端和第 1 層閘道端上連結的實際 IP 位址。位址會顯示在第 0 層閘道頁面和第 1 層閘道頁面上的 **其他設定 > 路由器連結**。預設值為 100.64.0.0/16。

c 選取 IPv6 位址組態的 **ND 設定檔** 和 **DAD 設定檔**。

這些設定檔可用來設定 IPv6 位址的無狀態位址自動組態 (SLAAC) 和重複位址偵測 (DAD)。系統會建立預設設定檔。

10 按一下 **儲存**。

11 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 IP**、**IPSec 本機 IP**、**DNS 轉寄站 IP**、**已連線的介面與區段**。

在 **已連線的介面與區段** 下，您可以選取下列一或多項：**服務介面子網路**、**外部介面子網路**、**回送介面子網路**、**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**、**NAT IP**、**LB SNAT IP**、**IPSec 本機端點**、**已連線的介面與區段**。

在 **已連線的介面與區段** 下，您可以選取 **服務介面子網路** 和/或 **已連線的區段**。

12 若要設定介面，請按一下**介面和設定**。

- a 按一下**新增介面**。
- b 輸入名稱。
- c 選取類型。

如果 HA 模式為主動備用，則選項為**外部**、**服務**和**回送**。如果 HA 模式為主動-主動式，則選項為**外部**和**回送**。

- d 以 CIDR 格式輸入 IP 位址。
- e 選取區段。
- f 如果介面類型不是**服務**，請選取 NSX Edge 節點。
- g (選擇性) 如果介面類型不是**回送**，請輸入 MTU 值。
- h (選擇性) 新增標籤，然後選取 ND 設定檔。

13 (選擇性) 如果 HA 模式為主動備用，請按一下 **HA VIP 組態**旁的**設定**，以設定 HA VIP。

已設定 HA VIP 時，即使一個上行已關閉，第 0 層閘道仍可運作。實體路由器只會與 HA VIP 互動。HA VIP 旨在與靜態路由 (而非 BGP) 搭配使用。

- a 按一下**新增 HA VIP 組態**。
- b 輸入 IP 位址和子網路遮罩。

HA VIP 子網路必須與其繫結之介面的子網路相同。

- c 選取來自兩個不同 Edge 節點的兩個介面。

14 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。

15 按一下 **BGP** 以設定 BGP。

16 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。

- a 若要設定第 3 層轉送模式，請按一下**全域組態**索引標籤。
- b 按一下**編輯**。
- c 選取 **IPv4** 或 **IPv4 和 IPv6**。

預設值為僅限 IPv4。不支援僅限 IPv6。若要啟用 IPv6，請選取 **IPv4 和 IPv6**。

- d 按一下**儲存**。

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。

社群清單是使用者定義的社群屬性值清單。這些清單可用來比對或管理 BGP 更新訊息中的社群屬性。

BGP 社群屬性 (RFC 1997) 和 BGP 大型社群屬性 (RFC 8092) 均受支援。BGP 社群屬性是分割為兩個 16 位元值的 32 位元值。BGP 大型社群屬性有 3 個元件，其長度分別為 4 個八位元資料組。

在路由對應中，我們可以比對或設定 BGP 社群或大型社群屬性。使用此功能時，網路營運人員可根據 BGP 社群屬性來實作網路原則。

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**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 指定社群清單。對於一般社群請使用 `aa:nn` 格式，例如 `300:500`。對於大型社群請使用 `aa:bb:cc` 格式，例如 `11:22:33`。請注意，清單不可同時包含一般社群和大型社群。它必須僅包含一般社群，或僅包含大型社群。

此外，您可以選取一或多個下列一般社群。請注意，如果清單包含大型社群，則不可新增一般社群。

- `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](#)。
- 如需關於使用規則運算式為社群清單定義路由對應符合準則的詳細資訊，請參閱[在新增路由對應時使用規則運算式來比對社群清單](#)。

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**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。
- **符合社群 REGEX** - 如果所有與 NRLI 相關聯的一般社群都符合規則運算式，則會在路由對應中執行設定動作。
- **符合大型社群 REGEX** - 如果所有與 NRLI 相關聯的大型社群都符合規則運算式，則會在路由對應中執行設定動作。

您應使用符合準則 MATCH_COMMUNITY_REGEX 來比對標準社群的路由，並使用符合準則 MATCH_LARGE_COMMUNITY_REGEX 來比對大型社群的路由。如果您想要允許包含標準社群或大型社群值的路由，則必須建立兩個符合準則。如果在相同的符合準則中提供比對運算式，則僅允許同時包含標準和大型社群的路由。

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会有相符項目。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	指定社群清單。對於一般社群請使用 aa:nn 格式，例如 300:500。對於大型社群請使用 aa:bb:cc 格式，例如 11:22:33。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**。

在新增路由對應時使用規則運算式來比對社群清單

您可以使用規則運算式來定義社群清單的路由對應符合準則。BGP 規則運算式以 POSIX 1003.2 規則運算式為基礎。

下列運算式是 POSIX 規則運算式的子集。

運算式	說明
.	比對任何單一字元。
*	比對 0 個或更多出現的模式。
+	比對 1 個或更多出現的模式。
?	比對 0 或 1 個出現的模式。
^	比對行首。
\$	比對行尾。
—	此字元在 BGP 規則運算式中具有特殊意義。它會比對空格、逗號、AS 設定分隔符號 { 和 } 以及聯邦分隔符號 (和)。它也會比對行首和行尾。因此，此字元可用於 AS 值界限比對。此字元在技術上會評估為 (^ [,{}() \$)。

以下是在路由對應中使用規則運算式的一些範例：

運算式	說明
^101	比對路由，具有開頭為 101 的社群屬性。
^[0-9]+	比對具有開頭為 0-9 之間數字的社群屬性，且含有一或多個此類數字之執行個體的路由。
.	比對含有或不含社群屬性的路由。
+	比對含有任何社群值的路由。
^\$	比對不含社群值/含有 Null 社群值的路由。

設定 BGP

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 層閘道與您實體基礎結構中的路由器之間的外部或內部 BGP (eBGP 或 iBGP) 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。您也必須設定遠端 AS 數目。EBGP 芳鄰必須直接連線，且位於與第 0 層上行相同的子網路中。如果它們不在相同的子網路中，則應使用 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。

NSX Edge 上的 ECMP 實作是以通訊協定號碼、來源和目的地位址，以及來源和目的地連接埠的 5 元組為基礎。

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。

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。

在主動-主動式模式中，系統會預先填入預設的 ASN 值 65000。在主動備用模式中，沒有預設的 ASN 值。

b 按一下 **BGP** 切換按鈕以啟用或停用 BGP。

在主動-主動式模式中，依預設會啟用 **BGP**。在主動備用模式中，依預設會停用 **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。依預設為啟用。

如果閘道處於主動備用模式中，此功能將無法使用。

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 在**正常重新啟動**欄位中，選取**停用**、**僅限協助程式**或**正常重新啟動和協助程式**。

您可以選擇性地變更**正常重新啟動計時器**和**正常重新啟動失效計時器**。

依預設，[正常重新啟動] 模式會設定為**僅限協助程式**。協助程式模式對於排除和/或減少與路由相關聯的流量中斷很有用，該路由是從能夠 [正常重新啟動] 的芳鄰學習得到。芳鄰必須能夠在進行重新啟動的同時保留其轉送表。

不建議在第 0 層閘道上啟用 [正常重新啟動] 功能，因為來自所有閘道的 BGP 對等一律會是作用中。在容錯移轉時，[正常重新啟動] 功能會增加遠端芳鄰選取替代的第 0 層閘道所花費的時間。這將會延遲以 BFD 為基礎的聚合。

附註：除非由芳鄰特定的組態覆寫，否則會將第 0 層組態套用至所有 BGP 芳鄰。

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 按一下儲存。

您必須先儲存全域 BGP 組態，才能設定 BGP 芳鄰。

7 設定 BGP 芳鄰。

- a 輸入芳鄰的 IP 位址。
- b 啟用或停用 BFD。
- c 輸入**遠端 AS 數目**的值。

對於 iBGP，請輸入與步驟 4a 中相同的 AS 數目。對於 eBGP，請輸入實體路由器的 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 在**來源位址**欄位中，您可以選取來源位址，以使用此特定來源位址建立芳鄰的對等工作階段。若未選取任何位址，閘道將會自動選擇一個。
- h 在 **IP 位址家族**欄位中，選取 **IPv4**、**IPv6** 或**已停用**。
- i 輸入**躍點數目上限**的值。

- j 在**正常重新啟動**欄位中，您可以選擇性地選取**停用**、**僅限協助程式**或**正常重新啟動和協助程式**。

選項	說明
未選取任何項目	此芳鄰的正常重新啟動會遵循第 0 層閘道 BGP 組態。
停用	<ul style="list-style-type: none"> 如果第 0 層閘道 BGP 已設定為停用，將對此芳鄰停用 [正常重新啟動]。 如果第 0 層閘道 BGP 已設定為僅限協助程式，將為此芳鄰停用 [正常重新啟動]。 如果第 0 層閘道 BGP 已設定為正常重新啟動和協助程式，將為此芳鄰停用 [正常重新啟動]。
僅限協助程式	<ul style="list-style-type: none"> 如果第 0 層閘道 BGP 已設定為停用，將為此芳鄰將 [正常重新啟動] 設定為 [僅限協助程式]。 如果第 0 層閘道 BGP 已設定為僅限協助程式，將為此芳鄰將 [正常重新啟動] 設定為 [僅限協助程式]。 如果第 0 層閘道 BGP 已設定為正常重新啟動和協助程式，將為此芳鄰將 [正常重新啟動] 設定為 [僅限協助程式]。
正常重新啟動和協助程式	<ul style="list-style-type: none"> 如果第 0 層閘道 BGP 已設定為停用，將為此芳鄰將 [正常重新啟動] 設定為 [正常重新啟動和協助程式]。 如果第 0 層閘道 BGP 已設定為僅限協助程式，將為此芳鄰將 [正常重新啟動] 設定為 [正常重新啟動和協助程式]。 如果第 0 層閘道 BGP 已設定為正常重新啟動和協助程式，將為此芳鄰將 [正常重新啟動] 設定為 [正常重新啟動和協助程式]。

- k 按一下**計時器與密碼**。

- l 輸入 **BFD 時間間隔**的值。

單位為毫秒。在虛擬機器中執行的 Edge 節點，最小值為 1000。裸機 Edge 節點的最小值為 300。

- m 輸入 **BFD 乘數**的值。

- n 輸入**保持關閉時間**的值。

- o 輸入**保持運作時間**的值。

- p 輸入密碼。

如果您在 BGP 對等之間設定 MD5 驗證，則此為必填。

- 8 按一下**儲存**。

設定 BFD

BFD (雙向轉送偵測) 是可偵測轉送路徑故障的通訊協定。

程序

- 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 選取**網路 > 第 0 層閘道**。
- 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**進階組態**。

這會將您導向至**進階網路與安全性 > 路由器**頁面。閘道會顯示為其中一個邏輯路由器。請依照在**第 0 層邏輯路由器上設定 BFD** 中的指示操作。

設定 IPv6 第 3 層轉送

依預設會啟用 IPv4 第 3 層轉送。您也可以設定 IPv6 第 3 層轉送。

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 按一下功能表圖示 (三個點) 並選取**編輯**，以編輯第 0 層閘道。
- 4 按一下**進階組態**。
這會將您導向至**進階網路與安全性 > 路由器**頁面。閘道會顯示為其中一個邏輯路由器。
- 5 按一下**全域組態索引標籤**。
- 6 在**第 3 層轉送模式**欄位中，選取 **IPv4 和 IPv6**。
不支援僅限 IPv6。
- 7 移至**網路索引標籤**以重新編輯閘道。
- 8 移至**其他設定**。
 - a **內部傳送子網路**沒有可設定的 IPv6 位址。系統會自動使用 IPv6 連結本機位址。
 - b 輸入 IPv6 子網路作為 **T0-T1 傳輸子網路**。
- 9 移至**介面**，然後新增 IPv6 的介面。

建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔

在邏輯路由器介面上使用 IPv6 時，您可以為 IP 位址的指派設定無狀態位址自動組態 (SLAAC)。SLAAC 可用來根據從本機網路路由器通告的網路首碼，透過路由器通告對主機進行定址。重複位址偵測 (DAD) 可確保 IP 位址的唯一性。

必要條件

導覽至**進階網路與安全性 > 路由器 > 全域組態**，然後選取 **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 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**其他設定**。

- 5 若要建立 **ND 設定檔** (SLAAC 設定檔)，請按一下功能表圖示 (三個點)，然後選取**建立新的**。
 - a 輸入設定檔的名稱。
 - b 選取模式。
 - **已停用** - 停用路由器通告訊息。
 - **透過 RA 取得 DNS 的 SLAAC** - 透過路由器通告訊息產生位址和 DNS 資訊。
 - **透過 DHCP 取得 DNS 的 SLAAC** - 透過路由器通告訊息產生位址，並由 DHCP 伺服器產生 DNS 資訊。
 - **透過 DHCP 取得位址和 DNS 的 DHCP** - 由 DHCP 伺服器產生位址和 DNS 資訊。
 - **透過 DHCP 取得位址和 DNS 的 SLAAC** - 由 DHCP 伺服器產生位址和 DNS 資訊。只有 NSX Edge 支援此選項，而 KVM 主機或 ESXi 主機不支援。
 - c 輸入路由器通告訊息的可連線時間和重新傳輸間隔。
 - d 輸入網域名稱，並指定網域名稱的存留時間。僅在使用**透過 RA 取得 DNS 的 SLAAC**模式時，才需要輸入這些值。
 - e 輸入 DNS 伺服器，並指定 DNS 伺服器的存留時間。僅在使用**透過 RA 取得 DNS 的 SLAAC**模式時，才需要輸入這些值。
 - f 輸入路由器通告的值：
 - **RA 時間間隔** - 傳輸連續路由器通告訊息之間的時間間隔。
 - **躍點限制** - 通告路由的存留時間。
 - **路由器存留時間** - 路由器的存留時間。
 - **首碼存留時間** - 首碼的存留時間 (以秒為單位)。
 - **首碼的慣用時間** - 有效位址慣用的時間。
- 6 若要建立 **DAD 設定檔**，請按一下功能表圖示 (三個點)，然後選取**建立新的**。
 - a 輸入設定檔的名稱。
 - b 選取模式。
 - **寬鬆** - 系統會接收重複位址通知，但在偵測到重複位址時不會採取任何動作。
 - **嚴格** - 系統會接收重複位址通知，且不再使用重複的位址。
 - c 輸入**等待時間 (秒)**以指定 NS 封包之間的時間間隔。
 - d 輸入**NS 重試計數**，以指定要依**等待時間 (秒)**中所定義間隔偵測重複位址的 NS 封包數目

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。
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。這是預設的選項。

- 7 (選擇性) 如果您想要讓這個第 1 層閘道主控的可設定狀態服務 (NAT、負載平衡器或防火牆)，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 (選擇性) 按一下 **啟用待命重新放置** 切換按鈕，以啟用或停用待命重新放置。

待命重新放置表示，如果作用中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 節點執行作用中邏輯路由器，原始的待命邏輯路由器會變成作用中邏輯路由器，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。

- 10 按一下 **儲存**。

- 11 (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
- 所有 IPSec 本機端點

在 **設定路由通告規則** 欄位中按一下 **設定**，以新增路由通告規則。

- 12 (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 在 **MTU** 欄位中，輸入介於 64 與 9000 之間的值。

e 在 **ND 設定檔欄位** 中，選取設定檔。

f 按一下 **儲存**。

13 (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。以覆蓋為基礎的邏輯連接埠上支援信任模式。預設值為 0。</p> <p>以覆蓋為基礎及以 VLAN 為基礎的邏輯連接埠上支援未受信任模式。針對以覆蓋為基礎的邏輯連接埠，輸出 IP 標頭的 DSCP 值會設為與邏輯連接埠內部封包類型無關的設定值。針對以 VLAN 為基礎的邏輯連接埠，IP/IPv6 封包的 DSCP 值會設為設定值。未受信任模式的 DSCP 值範圍介於 0 至 63 之間。</p> <p>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。</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>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。

備註 IPv6 的 IP 探索方法會在預設的 IP 探索區段設定檔中停用。若要為區段啟用 IPv6 的 IP 探索，您必須在啟用 IPv6 選項的情況下建立 IP 探索設定檔，並將設定檔連結至區段。此外，請確定分散式防火牆允許所有工作負載之間的 IPv6 芳鄰探索封包 (依預設為允許)。

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 和分散式防火牆 (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。如果藉由將已實現繫結清單上的 IP 新增至略過繫結清單或停用窺探來移除此 IP，則具有最舊時間戳記的重複 IP 將會移至已實現繫結清單中。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 與 SpoofGuard 不同，它不會以 SpoofGuard 使用的相同方式封鎖流量。如需詳細資訊，請參閱[瞭解 SpoofGuard 區段設定檔](#)。

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>。

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。導覽至**進階網路與安全性 > 交換 > 連接埠**並選取連接埠，即可將探索到的繫結新增至略過繫結清單。您也可以將目前探索到的繫結或實現的繫結複製到**略過繫結**，以刪除該繫結。

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 竊探	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。允許的最小值為 1 (預設值)，上限為 256。
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 竊探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP V6 竊探	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。
芳鄰探索竊探	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 竊探。
重複的 IP 偵測	適用於所有竊探方法及 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。

請注意，預設區段安全性設定檔會啟用 **Server Block** 和 **Server Block - IPv6 DHCP** 設定。這表示使用預設區段安全性設定檔的區段會封鎖從 DHCP 伺服器到 DHCP 用戶端的流量。如果您想要允許 DHCP 伺服器流量的區段，則必須為區段建立自訂區段安全性設定檔。

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	<p>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。</p>
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 伺服器封鎖 - IPv6 按鈕及 用戶端封鎖 - IPv6 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>

選項	說明
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	<p>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。</p>
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。
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 **新增區段**。
- 4 輸入區段的名稱。
- 5 選取已連線的閘道。

您可以選取現有的第 0 層或第 1 層閘道，或選取 **無**。預設值為 **無**，這表示區段只是邏輯交換器。在設定子網路後，它將可連結至第 0 層或第 1 層閘道。

- 6 如果已連線的閘道是第 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 若要指定子網路，請按一下 **設定子網路**。

- 8 選取傳輸區域，可以是覆疊或 VLAN。
- 9 如果傳輸區域的類型是 VLAN，請指定 VLAN 識別碼的清單。
- 10 如果您想要使用第 2 層 VPN 來延伸區段，請按一下 **L2 VPN** 文字方塊，然後選取 L2 VPN 伺服器或用戶端工作階段。

您可以選取多個項目。

- 11 在 **VPN 通道識別碼** 中，輸入用來識別區段的唯一值。
- 12 按一下 **儲存**。
- 13 若要新增區段連接埠，請在出現提示時按一下 **是** (如果您要繼續設定區段)。

- a 按一下 **連接埠和設定**。
- b 按一下 **新增區段連接埠**。
- c 輸入連接埠名稱。
- d 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。
- e 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，請將此文字方塊保留為空白。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**。

- f 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。

- g 輸入流量標籤。

輸入容器和其他使用案例中的 VLAN 識別碼。

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

- i 指定標籤。

- j 針對要套用位址繫結的邏輯連接埠指定其 IP (IPv4 位址、IPv6 位址或 IPv6 子網路) 和 MAC 位址，以套用位址繫結。例如，針對 IPv6，2001::/64 是 IPv6 子網路，2001::1 是主機 IP，而 2001::1/64 是無效的輸入。您也可以指定 VLAN 識別碼。

如果指定了手動位址繫結，此繫結將會覆寫自動探索到的位址繫結。

- k 選取此連接埠的區段設定檔。

- 14 若要選取區段設定檔，請按一下 **區段設定檔**。

- 15 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 Limited Export 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 層或第 1 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 層或第 1 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
- 新增自發 Edge 作為 L2 VPN 用戶端
- 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 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。

NSX Edge 支援原則型或路由型的 IPsec VPN。

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](#)。從 NSX-T Data Center 2.5 開始，第 1 層閘道也支援 IPsec VPN。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，以支援高可用性服務。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

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。

備註 在設定了以原則為基礎之 IPsec VPN 的第 1 層閘道上不支援 DNAT。

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 根據靜態路由或透過特殊介面 (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。

備註

- 透過 IPSec VPN 通道的路由不支援 OSPF 動態路由。
- 根據第 1 層開道的 VPN 不支援 VTI 的動態路由。

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

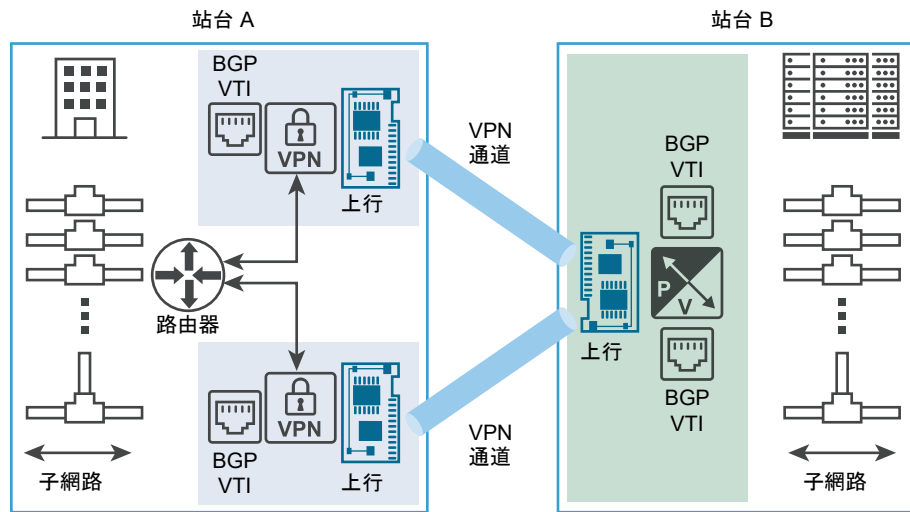
您可以使用在第 0 層開道上設定的路由型 IPSec VPN 工作階段，來設定 VPN 通道備援。透過通道備援，可在兩個站台之間設定多個通道，其中一個通道會用作主要通道，並在主要通道變得無法使用時容錯移轉至其他通道。此功能在站台有多個連線選項時最有用，例如使用不同的 ISP 來連結備援。

重要

- 在 NSX-T Data Center 中，僅在使用 BGP 時支援 IPSec VPN 通道備援。
- 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 開道，並且 NSX-T Data Center 管理站台 B 中的 Edge 開道虛擬應用裝置。

圖 5-1. 路由型 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](#)。

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 (VNI 或 VLAN)。此連線受 L2 VPN 伺服器 and L2 VPN 用戶端之間的路由型 IPSec 通道保護。

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。

延伸的網路是具有單一廣播網域的單一子網路，因此虛擬機器在站台之間移動時，仍保留在相同的子網路上，並且其 IP 位址不會變更。因此，企業可以在網路站台之間無縫地移轉虛擬機器。虛擬機器可以在 VNI 型網路或 VLAN 型網路上執行。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。

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 L2 區段。

在 NSX-T Data Center 中，只有第 0 層閘道支援 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。

從 NSX-T Data Center 2.5 版開始，可使用在 NSX-T Data Center 環境中管理的 NSX Edge 上的 L2 VPN 服務來延伸 VLAN 型的區段。此支援允許將 L2 網路從 VLAN 延伸至 VNI、將 VLAN 延伸至 VLAN，以及將 VNI 延伸至 VNI。

此外，也支援使用以 ESX NSX 管理的虛擬分散式交換器 (N-VDS) 的 VLAN 主幹。如果計算和 I/O 資源允許，VLAN 主幹允許一個 NSX Edge 叢集透過單一介面延伸多個 VLAN 網路。

在下列情況下提供 L2 VPN 服務支援。

- 在 NSX Data Center for vSphere 環境中管理的 NSX Edge 上主控的 NSX-T Data Center L2 VPN 伺服器 and L2 VPN 用戶端之間。受管理的 L2 VPN 用戶端同時支援 VLAN 和 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 用戶端僅支援 VLAN。
- 在自發 NSX Edge 上主控的 NSX-T Data Center L2 VPN 伺服器 and L2 VPN 用戶端之間。自發 L2 VPN 用戶端僅支援 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 and 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

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相關資訊。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 層或第 1 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](#)以建立在 NSX Edge 上主控的 VPN 伺服器。
- 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](#)。指定要用於通道的本機與對等子網路。使用工作階段中定義的通道，可保護從本機子網路到對等子網路的流量。

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 層或第 1 層閘道設定並啟用 IPSec VPN 服務。請參閱[新增 IPSec VPN 服務](#)。
- 2 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](#)。
- 3 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。
- 4 如果您不想使用預設的 DPD 設定檔，請建立 DPD 設定檔。請參閱[新增 DPD 設定檔](#)。
- 5 使用[新增本機端點](#)新增本機端點。
- 6 設定路由型 IPSec VPN 工作階段、套用設定檔，然後將本機端點連結至工作階段。在組態中提供 VTI IP，並使用相同的 IP 來設定路由。路由可以是靜態或動態 (使用 BGP)。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。您也必須使用 L2 VPN 伺服器所產生的對等代碼來設定 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 組態檔](#)取得 L2 VPN 伺服器服務工作階段的對等代碼，它必須套用於遠端站台，且會用於自動設定 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 層或第 1 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 Limited Export 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 層或第 1 層閘道，並可供使用。請參閱[新增第 0 層閘道](#)或[新增第 1 層閘道](#)以取得詳細資訊。

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 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**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 層或第 1 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 層或第 1 層閘道上已啟用 IPsec VPN 服務。
- 7 設定 **IKE 記錄層級**的值。
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**文字方塊中，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

您可以在第 0 層閘道上設定 L2 VPN 服務。若要啟用 L2 VPN 服務，您必須先在第 0 層閘道上建立 IPsec VPN 服務 (如果尚不存在)。然後設定 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 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

在設定 L2 VPN 伺服器服務之後，請在另一個 NSX Edge 執行個體上的用戶端模式中設定 L2 VPN 服務。

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。

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 (選擇性) 如果 IPsec VPN 服務尚不存在於您想要設定為 L2 VPN 伺服器的第 0 層閘道上，請使用下列步驟建立服務。
 - 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

在設定 L2 VPN 伺服器服務之後，請在另一個 NSX Edge 執行個體上的用戶端模式中設定 L2 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 (選擇性) 如果尚不存在，請使用下列步驟為 L2 VPN 用戶端服務建立 IPSec VPN 服務。
 - 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 選擇性地設定**說明**和**標籤**的值。

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 (選擇性) 從**合規性套件**下拉式功能表中，選取安全性合規性套件。

備註 提供以 NSX-T Data Center 2.5 為開頭的合規性套件支援。如需詳細資訊，請參閱[關於支援的合規性套件](#)。

所選取預設值為 `None`。如果您選取合規性套件，則會將**驗證模式**設定為 `Certificate`，並在**進階內容**區段中，**IKE 設定檔**和**IPsec 設定檔**的值設定為所選安全性合規性套件的系統定義設定檔。您無法編輯這些系統定義的設定檔。

- 11 如果**合規性套件**設定為 `None`，請從**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。
- 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 如果**驗證模式**設定為 `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。

14 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。以下為範例。

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

15 若要變更設定檔、起始模式、TCP MSS 鉗制模式和以原則為基礎的 IPsec VPN 工作階段所使用的標籤，請按一下進階內容。

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](#)。

- 如果已啟用 **IKE 設定檔** 下拉式功能表，請選取 IKE 設定檔。
- 如果未停用 **IPsec 設定檔** 下拉式功能表，請選取 IPsec 通道設定檔。
- 如果已啟用 **DPD 設定檔** 下拉式功能表，請選取慣用的 DPD 設定檔。
- 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，並回應來自對等端點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。

- 如果您想要減少 IPsec 連線期間 TCP 工作階段的最大區段大小 (MSS) 裝載，請啟用 **TCP MSS 鉗制**，然後選取 **TCP MSS 方向值**，並選擇性地設定 **TCP MSS 值**。

如需詳細資訊，請參閱[瞭解 TCP MSS 鉗制](#)。

- 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。

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 (選擇性) 從**合規性套件**下拉式功能表中，選取安全性合規性套件。

備註 提供以 NSX-T Data Center 2.5 為開頭的合規性套件支援。如需詳細資訊，請參閱[關於支援的合規性套件](#)。

預設值會設定為 `None`。如果您選取合規性套件，則會將**驗證模式**設定為 `Certificate`，並在**進階內容**區段中，**IKE 設定檔**和 **IPsec 設定檔**的值設定為所選合規性套件的系統定義設定檔。您無法編輯這些系統定義的設定檔。

- 11 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。

- 12 如果**合規性套件**設定為 `None`，請從**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。

- 13 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。

14 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。以下為範例。

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

15 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。

16 若要變更設定檔、起始模式、TCP MSS 鉗制模式和以路由為基礎的 IPsec VPN 工作階段所使用的標籤，請按一下進階內容。

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](#)。

- 如果已啟用 **IKE 設定檔** 下拉式功能表，請選取 IKE 設定檔。
- 如果未停用 **IPsec 設定檔** 下拉式功能表，請選取 IPsec 通道設定檔。
- 如果已啟用 **DPD 設定檔** 下拉式功能表，請選取慣用的 DPD 設定檔。
- 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，並回應來自對等端點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。

17 如果您想要減少 IPsec 連線期間 TCP 工作階段的最大區段大小 (MSS) 裝載，請啟用 **TCP MSS 鉗制**，然後選取 **TCP MSS 方向值**，並選擇性地設定 **TCP MSS 值**。[]

如需詳細資訊，請參閱[瞭解 TCP MSS 鉗制](#)。

18 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。

19 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。

關於支援的合規性套件

從 NSX-T Data Center 2.5 開始，您可以指定要用來設定用於 IPsec VPN 工作階段的安全性設定檔的安全性合規性套件。

安全性合規性套件具有預先定義的值，用於不同的安全性參數，且無法加以修改。選取合規性套件時，預先定義的值會自動用於您要設定的 IPsec VPN 工作階段的安全性設定檔。

下表列出 NSX-T Data Center 中支援 IKE 設定檔的合規性套件，以及針對每個設定檔預先定義的值。

合規性套件名稱	IKE 版本	加密演算法	摘要演算法	Diffie Hellman 群組
CNSA	IKEv2	AES 256	SHA2 384	群組 15，群組 20
FIPS	IKE-Flex	AES 128	SHA2 256	群組 20
基礎	IKEv1	AES 128	SHA2 256	群組 14
PRIME	IKEv2	AES GCM 128	未設定	群組 19
Suite-B-GCM-128	IKEv2	AES 128	SHA2 256	群組 19
Suite-B-GCM-256	IKEv2	AES 256	SHA2 384	群組 20

下表列出 NSX-T Data Center 中支援 IPsec 設定檔的合規性套件，以及針對每個設定檔預先定義的值。

合規性套件名稱	加密演算法	摘要演算法	PFS 群組	Diffie-Hellman 群組
CNSA	AES 256	SHA2 384	已啟用	群組 15，群組 20
FIPS	AES GCM 128	未設定	已啟用	群組 20
基礎	AES 128	SHA2 256	已啟用	群組 14
PRIME	AES GCM 128	未設定	已啟用	群組 19

合規性套件名稱	加密演算法	摘要演算法	PFS 群組	Diffie-Hellman 群組
Suite-B-GCM-128	AES GCM 128	未設定	已啟用	群組 19
Suite-B-GCM-256	AES GCM 256	未設定	已啟用	群組 20

瞭解 TCP MSS 鉗制

TCP MSS 鉗制可讓您減少在透過 IPsec 通道建立連線期間 TCP 工作階段所使用的最大區段大小 (MSS) 值。從 NSX-T Data Center 2.5 開始支援這個功能。

TCP MSS 是主機在單一 TCP 區段中能夠接受的最大資料量 (以位元組為單位)。TCP 連線的每一端皆會在三向信號交換期間將其需要的 MSS 值傳送至其對等端，其中 MSS 是 TCP SYN 封包中使用的其中一個 TCP 標頭選項。TCP MSS 是根據傳送者主機出口介面的傳輸單元最大值 (MTU) 來計算。

當 TCP 流量流過 IPsec VPN 或任何類型的 VPN 通道時，會將額外標頭新增至原始封包來保持安全。針對 IPsec 通道模式，所使用的額外標頭是 IP、ESP 和選擇性的 UDP (如果網路中出現連接埠轉譯)。由於這些額外標頭，封裝式封包的大小超過 VPN 介面的 MTU。封包可能會根據 DF 原則來分段或捨棄。

若要避免封包分段或捨棄，您可以啟用 TCP MSS 鉗制功能來調整 IPsec 工作階段的 MSS 值。**導覽至網路 > VPN > IPsec 工作階段**。當您要新增 IPsec 工作階段或編輯現有的 IPsec 工作階段時，請展開**進階內容**區段，然後啟用 **TCP MSS 鉗制**。

您可以設定 **TCP MSS 方向**及 **TCP MSS 值**，設定適用於 IPsec 工作階段的預先計算 MSS 值。所設定的 MSS 值是用於 MSS 鉗制。您可以設定 **TCP MSS 方向**並將 **TCP MSS 值**保留空白，來選擇使用動態 MSS 計算。當 MSS 值已決定時決定時，會根據 VPN 介面 MTU、VPN 額外負荷和路徑 MTU (PMTU) 自動計算 MSS 值。有效的 MSS 會在每個 TCP 信號交換期間重新計算，以動態處理 MTU 或 PMTU 變更。

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，因為它是屬於敏感資訊。

- 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 L2 VPN 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 VNI 型或 VLAN 型區段。
- d 在 **VPN 通道識別碼**中輸入唯一值，用於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 L2 VPN 伺服器組態期間所產生的對等代碼。請參閱[下載遠端 L2 VPN 組態檔](#)。
- 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 用戶端工作階段所用 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。
- 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 用戶端工作階段的 VNI 型或 VLAN 型區段。
 - d 在**VPN 通道識別碼**中輸入唯一值，用於識別您所選取的區段。
 - 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 組態檔

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，這視為敏感資訊。

例如，L2VPNSession_L2VPNServer_config.txt 包含下列組態。

```
[
  {
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-policyconnectivity-693/ipsec-vpn-services/IpsecService1/sessions/Routebase1",
    "peer_code":
      "MCw3ZjBjYzdzLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXBJcCI6IjE2OS4yNTQuNjQuMSIsImImlrZU9wdG1vbiI6ImlrZXlyIiwic2l0ZW5jYXBQcm90byI6ImdyZS9pcHNIYyIsImRoR3JvdXAiOiJkaDE0Iiwic2l0ZW5jcnlwdEFuZERPZ2VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI6IlZNd2FyZTEyMyIsInRlbn5lbHMI0lt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlcklkIjoiaWNTAuNTAuNTAuMSIsImxvY2FsVnRpSXAiOiIxNjkuMi4yLjMvMzEifV19"
  }
]
```

5 複製對等代碼，用於設定 L2 VPN 用戶端服務和工作階段。

使用前面的組態檔範例，以下為您複製以與 L2 VPN 用戶端組態搭配使用的對等代碼。

MCw3ZjBjYzdjLHsic2l0ZU5hbWUoiOiJsb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB
JcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXxyIiwiZW5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwiZW5jcnldEFuZERpZ2
VzdCI6ImFlcylnY20vc2hhLTI1NiIsInBzayI
6IlZNd2FyZTEyMyIsInRlbm5lbHMiOlt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlcklkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnRwSXAiOiIxNjkuMi4yLjMvMzEifV19

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建立關聯的 IPsec VPN 用戶端服務。

5 輸入本機端點的 IP 位址。

對於在第 0 層閘道上執行的 IPsec VPN 服務，本機端點 IP 位址必須與第 0 層閘道的上行介面 IP 位址不同。您提供的本機端點 IP 位址與第 0 層閘道的回送介面相關聯，也已發佈為上行介面上的可路由 IP 位址。對於在第 1 層閘道上執行的 IPsec VPN 服務，為了使本機端點 IP 位址可路由，必須在第 1 層閘道組態中啟用 IPsec 本機端點的路由通告。如需詳細資訊，請參閱 [新增第 1 層閘道](#)。

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 (選擇性) 選擇性地在 **說明** 中新增說明。

8 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。

9 從 **受信任的 CA 憑證和憑證撤銷清單** 下拉式功能表中，選取本機端點所需的適當憑證。

10 指定標籤 (如有需要)。

11 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

國際網路金鑰交換 (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。

從 NSX-T Data Center 2.5 開始，除了所使用的預設 IKE 設定檔，您也可以選取其中一個支援的合規性套件。如需詳細資訊，請參閱[關於支援的合規性套件](#)。

如果您決定不使用提供的預設 IKE 設定檔或合規性套件，可以使用下列步驟自行設定 IKE 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 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。且在摘要演算法文字方塊中指定 SHA1，則會在 IKE SA 協商期間使用 PRF-HMAC-SHA1 演算法。也必須在對等閘道中進行設定。</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 IPsec 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。

從 NSX-T Data Center 2.5 開始，除了預設的 IPsec 設定檔，您也可以選取其中一個支援的合規性套件。如需詳細資訊，請參閱[關於支援的合規性套件](#)。

如果您決定不使用提供的預設 IPsec 設定檔或合規性套件，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。

表 5-8. 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 GCM 128 (預設值) ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ 無加密驗證 AES GMAC 128 ■ 無加密驗證 AES GMAC 192 ■ 無加密驗證 AES GMAC 256 ■ 無加密 	在網際網路通訊協定安全性 (IPSec) 交涉期間使用的加密演算法。
摘要	<ul style="list-style-type: none"> ■ SHA1 ■ SHA2 256 ■ SHA2 384 ■ SHA2 512 	要在 IPSec 交涉期間使用的安全雜湊演算法。
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 	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。

- 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 5-9. 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，這是在您設定 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。

新增自發 Edge 作為 L2 VPN 用戶端

您可以使用 L2 VPN 將第 2 層網路延伸至未受 NSX-T Data Center 管理的站台。自發 NSX Edge 部署可在站台上以作為 L2 VPN 用戶端。自發 NSX Edge 易於部署、易於進行程式設計，且可提供高效能 VPN。自發 NSX Edge 可使用 OVF 檔案部署在未受 NSX-T Data Center 管理的主機上。您也可以部署主要和次要自發 L2 VPN Edge 用戶端，為 VPN 備援啟用 HA。

必要條件

- 建立連接埠群組，並將其繫結至主機上的 vSwitch。
- 為您的內部 L2 延伸連接埠建立連接埠群組。
- 取得本機 IP 與遠端 IP 的 IP 位址，以與您要新增的 L2 VPN 用戶端工作階段搭配使用。
- 取得 L2 VPN 伺服器組態期間所產生的對等代碼。

程序

- 1 使用 vSphere Web Client 登入管理非 NSX 環境的 vCenter Server。
- 2 選取**主機和叢集**，然後展開叢集以顯示可用的主機。
- 3 以滑鼠右鍵按一下要安裝自發 NSX Edge 的主機，然後選取**部署 OVF 範本**。
- 4 輸入 URL 以從網際網路下載並安裝 OVF 檔案，或按一下**瀏覽**，以找出您的電腦上包含自發 NSX Edge OVF 檔案的資料夾，然後按**下一步**。
- 5 在**選取名稱和資料夾**頁面上，輸入自發 NSX Edge 的名稱，然後選取要用來部署的資料夾或資料中心。然後，按**下一步**。
- 6 在**選取計算資源**頁面上，選取計算資源的目的地。
- 7 在 [OVF 範本詳細資料] 頁面上檢閱範本詳細資料，然後按**下一步**。
- 8 在**組態**頁面上，選取部署組態選項。
- 9 在**選取儲存區**頁面上，選取用來儲存組態檔案或磁碟檔案的位置。
- 10 在**選取網路**頁面上，設定已部署的範本必須使用的網路。選取您為上行介面建立的連接埠群組、您為 L2 延伸連接埠建立的連接埠群組，然後輸入 HA 介面。按**下一步**。
- 11 在**自訂範本**頁面上輸入下列值，然後按**下一步**。
 - a 輸入兩次 CLI 管理員密碼。
 - b 輸入兩次 CLI 啟用密碼。
 - c 輸入兩次 CLI 根密碼。
 - d 輸入管理網路的 IPv4 位址。
 - e 輸入 VLAN 識別碼、結束介面、IP 位址和 IP 首碼長度等**外部連接埠**詳細資料，讓結束介面對應至具有您上行介面之連接埠群組的網路。

如果結束介面連線至主幹連接埠群組，請指定 VLAN 識別碼。例如 **20,eth2,192.168.5.1,24**。您也可以使用 VLAN 識別碼來設定連接埠群組，並以 VLAN 0 作為**外部連接埠**。
 - f (選擇性) 若要設定高可用性，請輸入將結束介面對應至適當 HA 網路的**HA 連接埠**詳細資料。
 - g (選擇性) 將自發 NSX Edge 部署為 HA 的次要節點時，請選取**將此自發 Edge 部署為次要節點**。

使用與主要節點相同的 OVF 檔案，並輸入主要節點的 IP 位址、使用者名稱、密碼和指紋。

若要擷取主要節點的指紋，請登入主要節點，並執行下列命令：

```
get certificate api thumbprint
```

請確定主要和次要節點的 VTEP IP 位址位於相同的子網路中，且其連線至相同的連接埠群組。當您完成部署並啟動次要 Edge 時，它會連線至主要節點以形成 Edge 叢集。

12 在**即將完成**頁面上檢閱自發 Edge 設定，然後按一下**完成**。

備註 如果在部署期間發生錯誤，在 CLI 上會顯示當日訊息。您也可以使用 API 呼叫來檢查錯誤：

```
GET https://<nsx-mgr>/api/v1/node/status
```

錯誤分類為軟體錯誤和硬體錯誤。請視需要使用 API 呼叫解決軟體錯誤。您可以使用 API 呼叫來清除當日訊息：

```
POST /api/v1/node/status?action=clear_bootup_error
```

13 開啟自發 NSX Edge 應用裝置的電源。

14 登入自發 NSX Edge 用戶端。

15 選取 **L2 VPN > 新增工作階段**，然後輸入下列值：

- a 輸入工作階段名稱。
- b 輸入本機 IP 位址和遠端 IP 位址。
- c 輸入來自 L2VPN 伺服器的對等代碼。如需取得對等代碼的詳細資訊，請參閱[下載遠端 L2 VPN 組態檔](#)。

16 按一下**儲存**。

17 選取**連接埠 > 新增連接埠**以建立 L2 延伸連接埠。

18 輸入名稱、VLAN，然後選取結束介面。

19 按一下**儲存**。

20 選取 **L2 VPN > 連結連接埠**，然後輸入下列值：

- a 選取您建立的 L2 VPN 工作階段。
- b 選取您建立的 L2 延伸連接埠。
- c 輸入通道識別碼。

21 按一下**連結**。

如果需要延伸多個 L2 網路，您可以建立其他 L2 延伸連接埠，並將其連結至工作階段。

22 使用瀏覽器登入自發 NSX Edge，或使用 API 呼叫來檢視 L2VPN 工作階段的狀態。

備註 如果 L2VPN 伺服器組態有所變更，請務必再次下載對等代碼，並使用新的對等代碼來更新工作階段。

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 (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 層閘道是以作用中/作用中式模式執行，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 層閘道是以作用中/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。

備註 在設定了以原則為基礎之 IPSec VPN 的第 1 層閘道上不支援 DNAT。

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**。

對於以作用中/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**。

對於以作用中/作用中式模式執行的第 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。
 - 對於 SNAT，外部位址是執行 NAT 之後轉譯的來源位址。
 - 對於 DNAT，外部位址是執行 NAT 之前的原始目的地位址。
 - 在「自反」方面，對於出口流量，防火牆會套用至執行 NAT 之後轉譯的來源位址。對於入口流量，防火牆會套用至執行 NAT 之前的原始目的地位址。
- **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。
 - 對於 SNAT，內部位址是執行 NAT 之前的原始來源位址。
 - 對於 DNAT，內部位址是執行 NAT 之後轉譯的目的地位址。
 - 在「自反」方面，對於出口流量，防火牆會套用至執行 NAT 之前的原始來源位址。對於入口流量，防火牆會套用至執行 NAT 之後轉譯的目的地位址。
- **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。

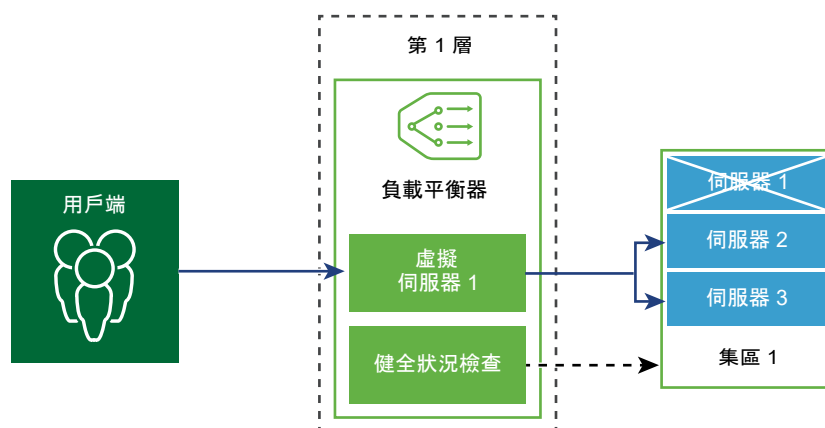
較低的值表示較高的優先順序。預設值為 100。

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 層閘道支援邏輯負載平衡器。一個負載平衡器只能連結至第 1 層閘道。

本章節討論下列主題：

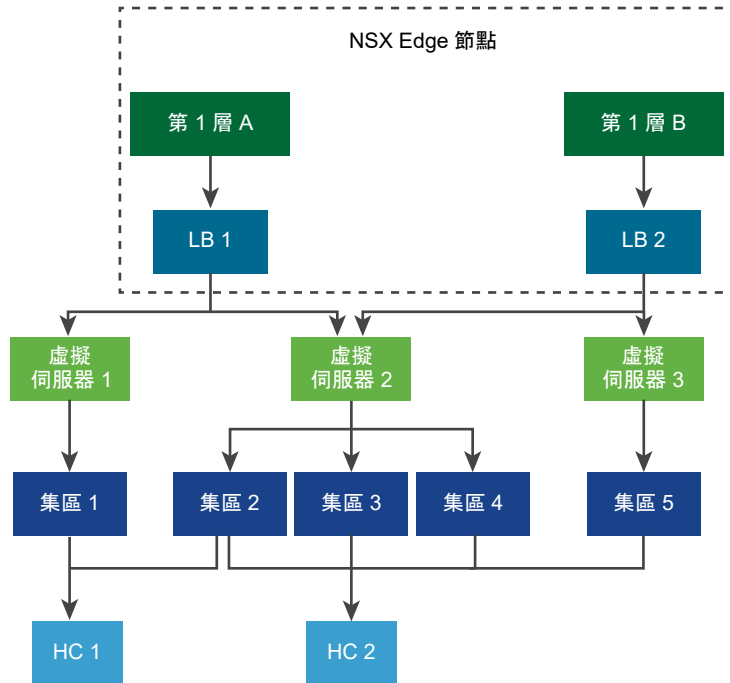
- [主要負載平衡器概念](#)
- [設定負載平衡器元件](#)
- [針對伺服器集區和虛擬伺服器建立的群組](#)

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

您可以在設定負載平衡器時指定大小 (小型、中型或大型)。大小會決定負載平衡器可支援的虛擬伺服器、伺服器集區和集區成員數目。

負載平衡器會在第 1 層閘道上執行，因此必須處於主動備用模式。閘道會在 NSX Edge 節點上執行。NSX Edge 節點的機器尺寸 (裸機、小型、中型或大型) 會決定 NSX Edge 節點可支援的負載平衡器數目。請注意，在**進階網路與安全性**索引標籤中，邏輯路由器一詞是指閘道。

如需不同負載平衡大小和 NSX Edge 機器尺寸所能支援大小的詳細資訊，請參閱 <https://configmax.vmware.com>。

請注意，不建議在生產環境中使用小型 NSX Edge 節點來執行小型負載平衡器。

您可以呼叫 API 來取得 NSX Edge 節點的負載平衡器使用情況資訊。如果您使用**網路**索引標籤來設定負載平衡，請執行下列命令：

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

如果您使用**進階網路與安全性**索引標籤來設定負載平衡，請執行下列命令：

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

使用量資訊包括節點上設定的負載平衡器物件 (例如負載平衡器服務、虛擬伺服器、伺服器集區，以及集區成員) 的數目。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。

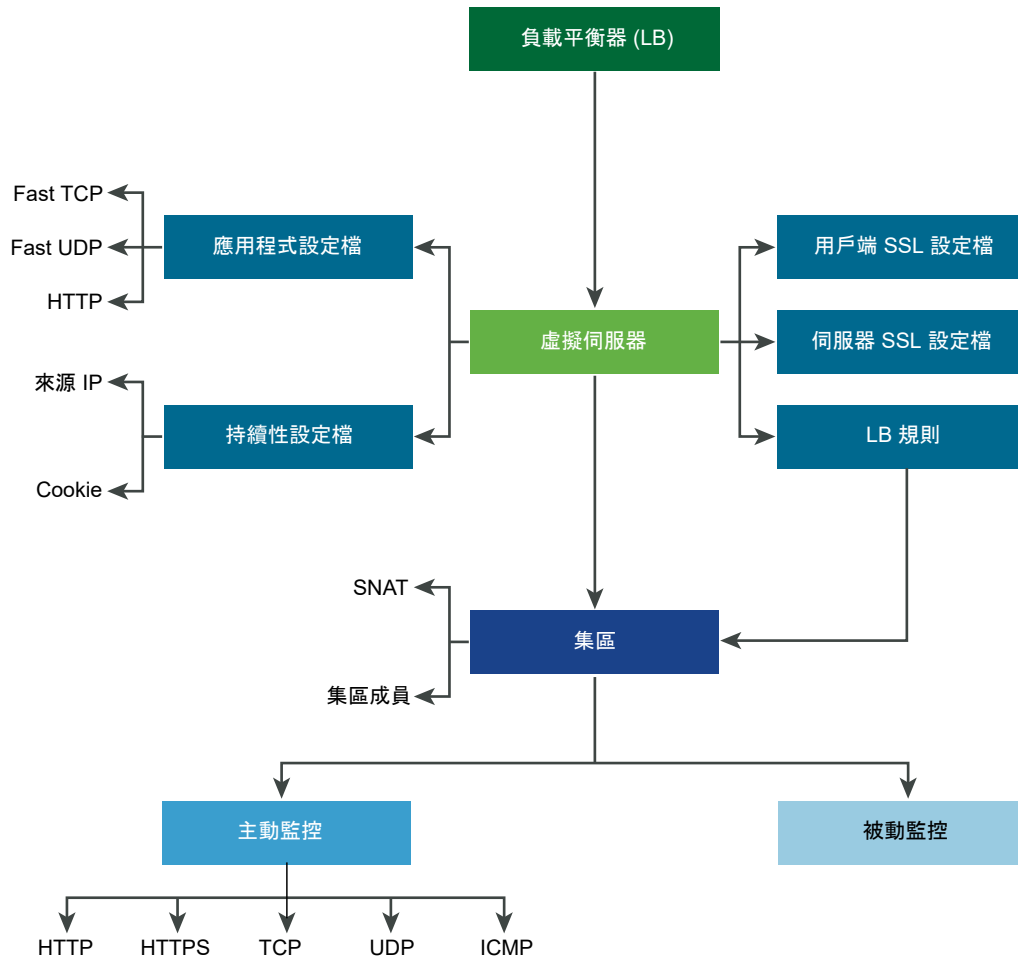
支援的負載平衡器功能

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。

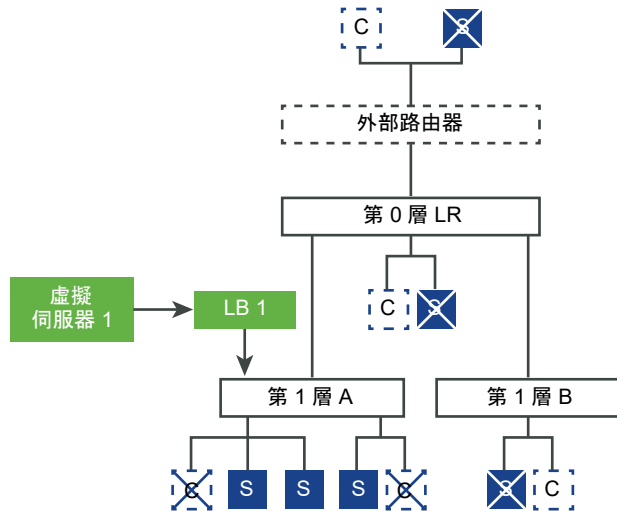


負載平衡器拓撲

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

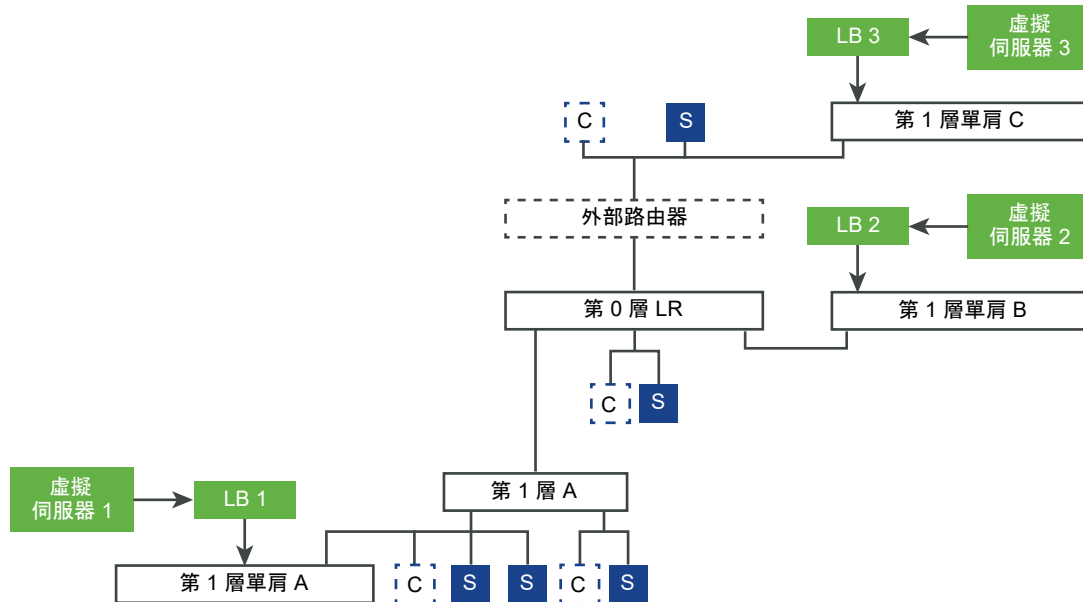
在內嵌模式下，負載平衡器位於用戶端與伺服器之間的流量路徑中。如果不想在負載平衡器上有 SNAT，用戶端和伺服器不應連線到相同第 1 層邏輯路由器上的覆疊區段。如果用戶端和伺服器連線至相同第 1 層邏輯路由器上的覆疊區段，則需要 SNAT。



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

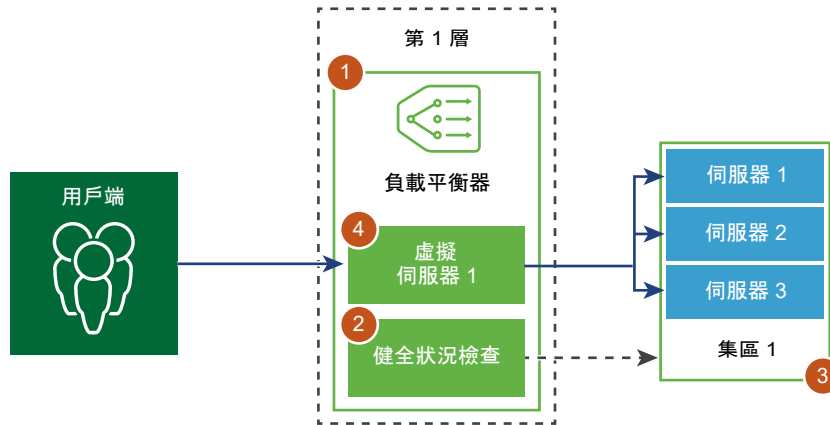
負載平衡器 - 防火牆 - SNAT

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。



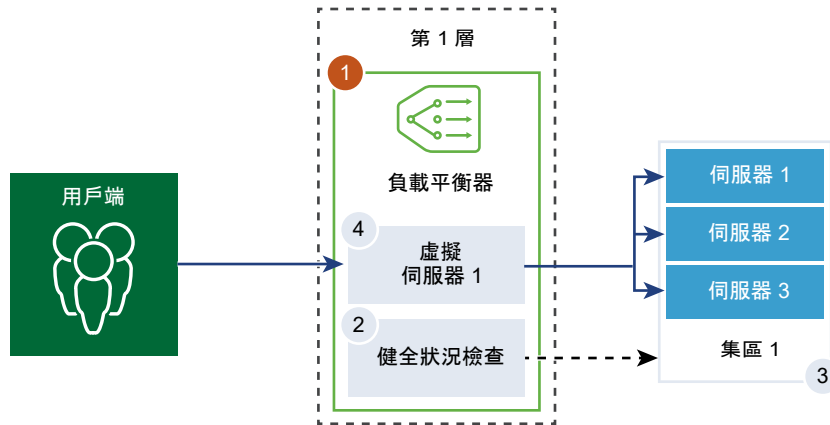
新增負載平衡器

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 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。

- 9 (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

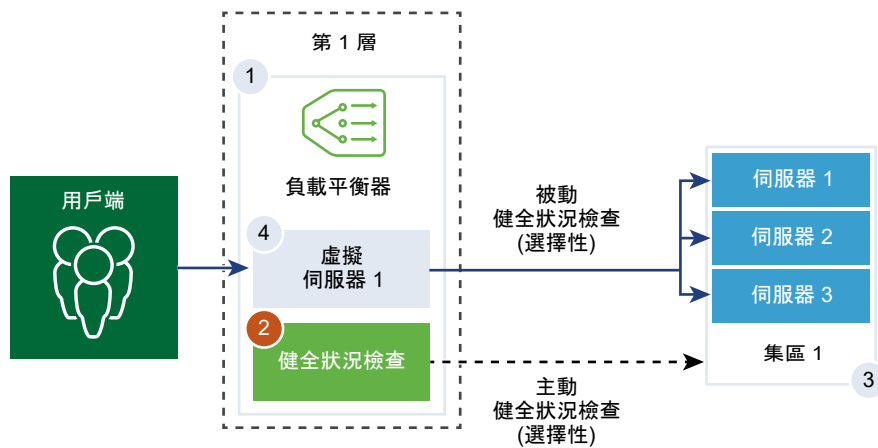
主動健全狀況監視器可用來測試伺服器是否可用。主動健全狀況監視器使用數種類型的測試，例如傳送基本 Ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

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。

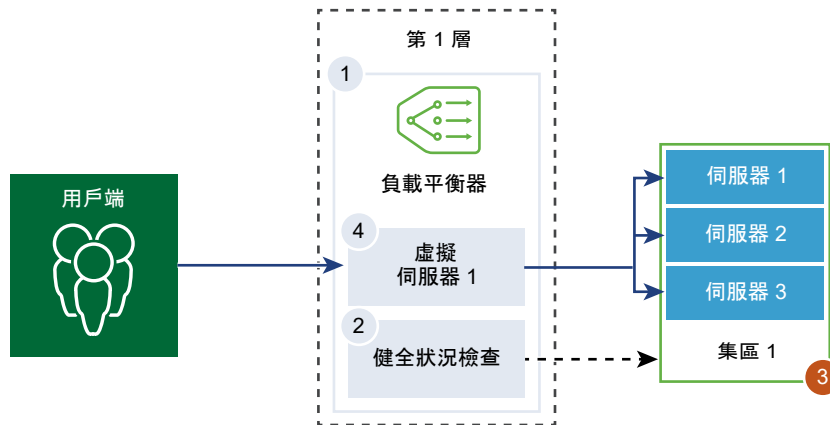
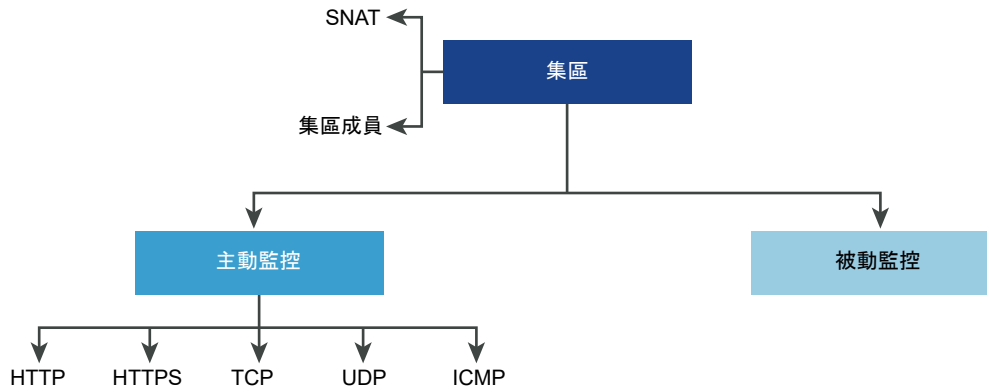


圖 7-1. 伺服器集區參數組態



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>輸入群組名稱和選用說明。</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。

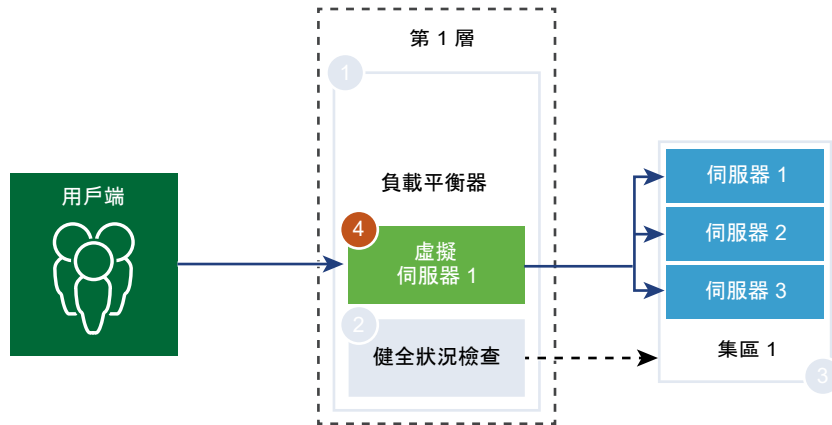
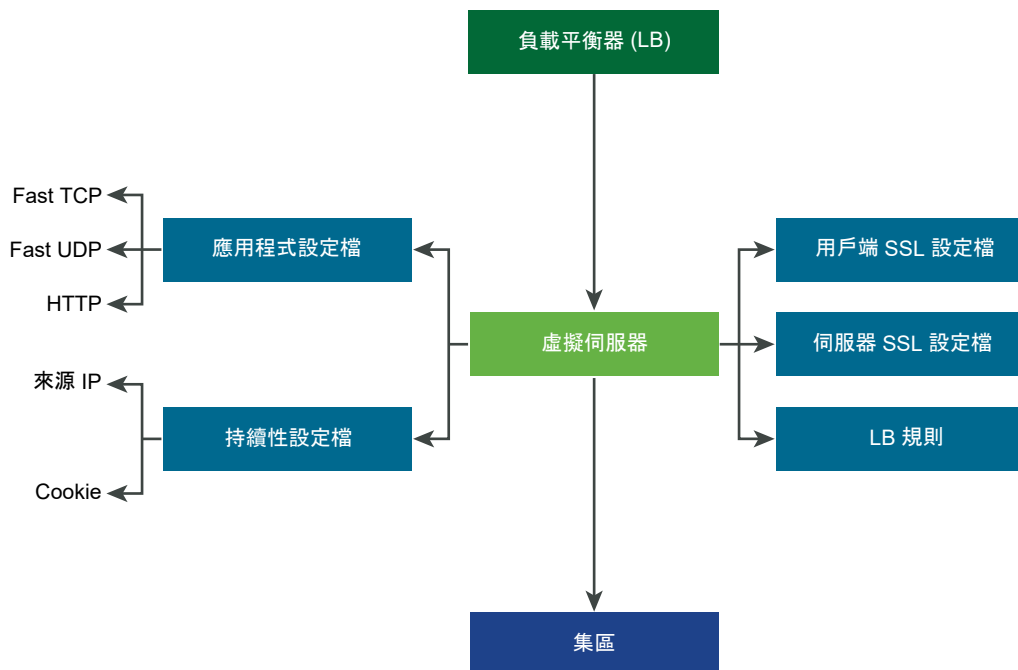


圖 7-2. 虛擬伺服器元件



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

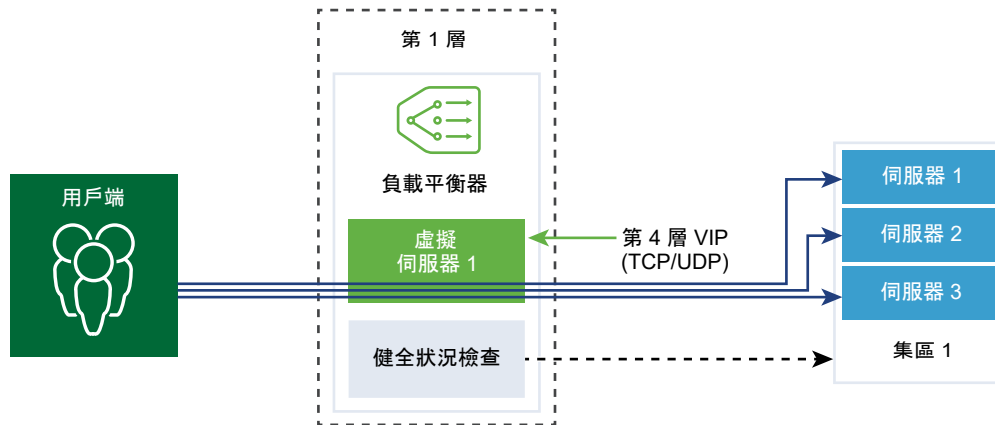
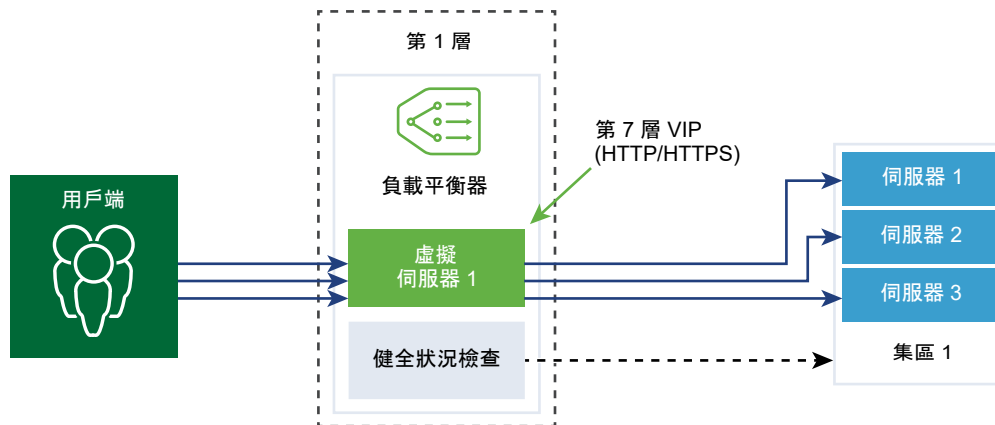


圖 7-4. 第 7 層 HTTPS 應用程式設定檔



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

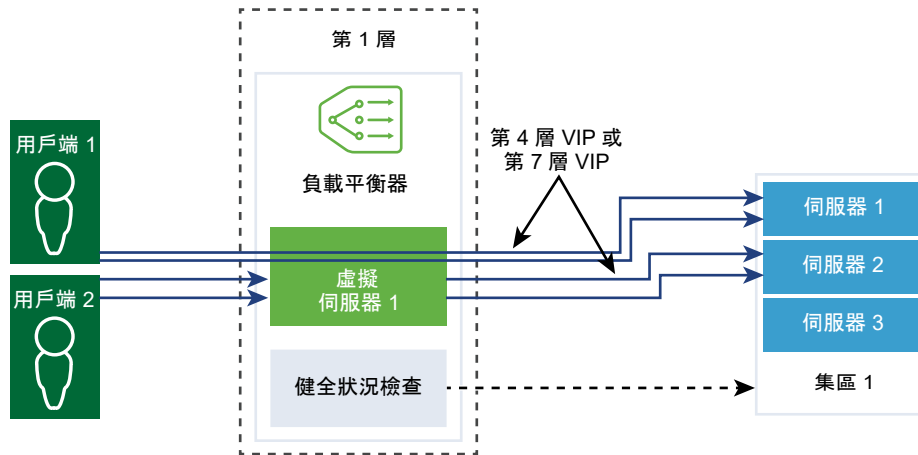
若要確保可設定狀態的應用程式的穩定性，負載平衡器會實作將所有相關連線導向至相同伺服器的持續性。支援不同類型的持續性以因應不同類型的應用程式需求。

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。請注意，不支援 Cookie 名稱中存在空格。

一般持續性設定檔會根據 HTTP 標頭、Cookie 或 HTTP 要求中的 URL 來支援持續性。因此，如果工作階段識別碼是 URL 的一部分，此設定檔就會支援應用程式工作階段持續性。此設定檔不會直接與虛擬伺服器相關聯。您可以在設定要求轉送和回應重寫的負載平衡器規則時指定此設定檔。



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> <p>針對來自新用戶端 IP 的第一個連線，系統會根據負載平衡演算法，將其負載平衡至集區成員。NSX 會將該持續性項目儲存在 LB 持續性資料表上，該資料表可透過 CLI 命令在主控 T1-LB 主動的 Edge 節點上進行檢視：<code>get load-balancer <LB-UUID> persistence-tables</code>。</p> <ul style="list-style-type: none"> ■ 從該用戶端連至 VIP 的連線存在時，系統會保留持續性項目。 ■ 從該用戶端至 VIP 之間沒有更多連線時，持續性項目會開始「持續性項目逾時」值中指定的計時器倒數。如果在計時器到期之前並未進行從該用戶端至 VIP 的新連線，則該用戶端 IP 的持續性項目即會刪除。如果該用戶端在項目刪除之後返回，則系統會根據負載平衡演算法再次將其重新平衡至集區成員。

選項	說明
填滿時清除項目	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。啟用此選項時，系統會刪除最舊的項目以接受最新項目。 停用此選項時，如果來源 IP 持續性資料表已滿，則會拒絕新的用戶端連線。
HA 持續性鏡像	切換按鈕，將持續性項目同步至 HA 對等項。啟用 HA 持續性鏡像時，在發生負載平衡器容錯移轉的情形下用戶端 IP 持續性會保持不變。
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。 ■ 首碼 - 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。不支援 Cookie 名稱中存在空格。
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。

5 選取一般以新增一般持續性設定檔，然後輸入設定檔詳細資料。

選項	說明
名稱與說明	輸入來源 IP 持續性設定檔的名稱和說明。
共用持續性	切換按鈕以在虛擬伺服器之間共用設定檔。
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> <p>針對來自新用戶端 IP 的第一個連線，系統會根據負載平衡演算法，將其負載平衡至集區成員。NSX 會將該持續性項目儲存在 LB 持續性資料表上，該資料表可透過 CLI 命令在主控 T1-LB 主動的 Edge 節點上進行檢視：<code>get load-balancer <LB-UUID> persistence-tables</code>。</p> <ul style="list-style-type: none"> ■ 從該用戶端連至 VIP 的連線存在時，系統會保留持續性項目。 ■ 從該用戶端至 VIP 之間沒有更多連線時，持續性項目會開始「持續性項目逾時」值中指定的計時器倒數。如果在計時器到期之前並未進行從該用戶端至 VIP 的新連線，則該用戶端 IP 的持續性項目即會刪除。如果該用戶端在項目刪除之後返回，則系統會根據負載平衡演算法再次將其重新平衡至集區成員。
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	<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 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

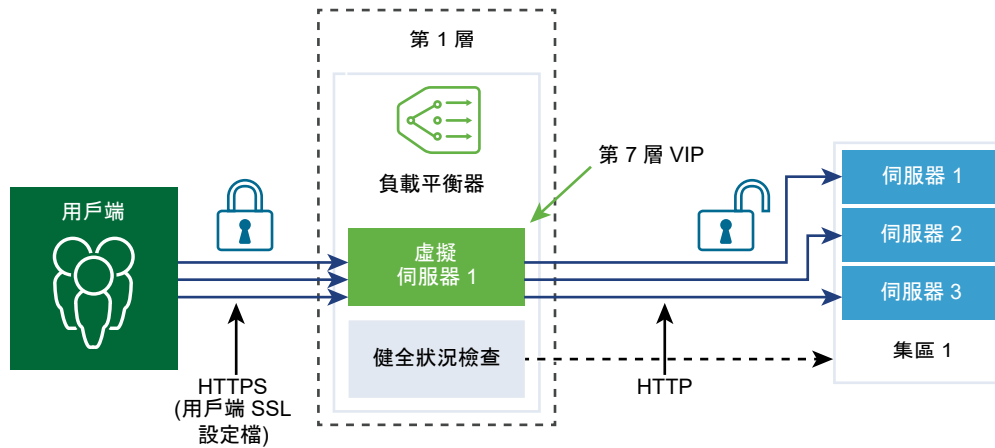
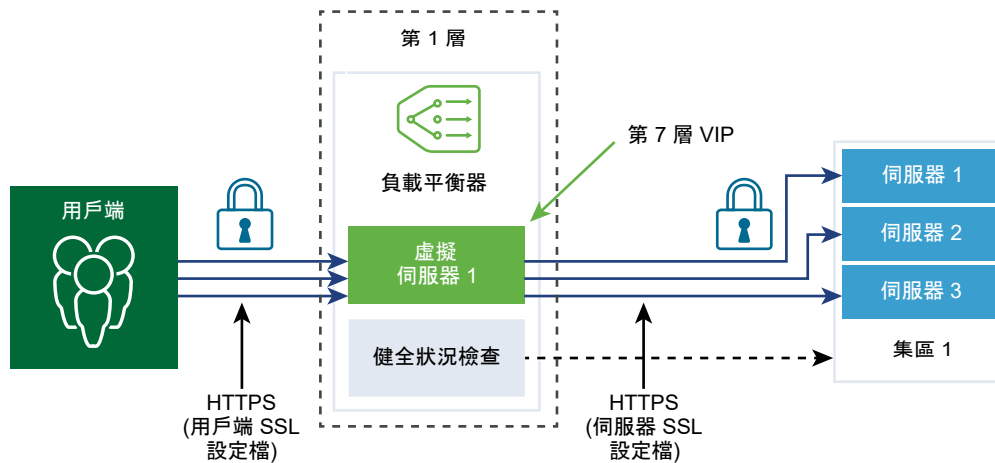


圖 7-6. 端對端 SSL



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。

選項	說明
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。

選項	說明
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。
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。

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

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。

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	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 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。

8 按一下儲存。

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:s)ensitive`」，改為使用「`Case ((?i:s)ensitive)`」。
- 不支援前置處理作業 `\l`、`\u`、`\L` 及 `\U`。其中，`\l` - 可將下一個字元轉成小寫 `\u` - 可將下一個字元轉成大寫 `\L` - 可將 `\E` 之前的字元轉成小寫 `\U` - 可將 `\E` 之前的字元轉成大寫。
- 不支援 `(?(condition)X)`、`(? {code})`、`(??{Code})` 及 `(?#comment)`。
- 不支援預先定義的 Unicode 字元類別 `\X`。
- 不支援將具名字元建構用於 Unicode 字元。例如，請勿使用 `\N{name}`，改為使用 `\u2018`。

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

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

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

備註 對於具名擷取群組，名稱不能以 `_` 字元開頭。

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

- `$_args` - 來自要求的引數
- `$_arg_<name>` - 要求行中的引數 `<name>`
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_upstream_cookie_<name>` - 具有指定名稱且由上游伺服器在「設定 Cookie」回應標頭欄位中傳送的 Cookie
- `$_upstream_http_<name>` - 任意回應標頭欄位，`<name>` 是轉換為小寫、且將虛線取代為底線的欄位名稱
- `$_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
- `$_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」
- (僅限 NSX-T Data Center 2.5.0) `$_ssl_client_cert` - 以 PEM 格式傳回已建立 SSL 連線的用戶端憑證，除第一行外，每一行的前面都會加上定位字元。
- (NSX-T Data Center 2.5.1 及更新版本) `$_ssl_client_escaped_cert` - 針對已建立的 SSL 連線，傳回 PEM 格式的用戶端憑證。
- `$_ssl_server_name` - 傳回透過 SNI 要求的伺服器名稱
- `$_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 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 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
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

動作	說明
變數持續性檢測	<p>選取一般持續性設定檔，並輸入變數名稱。</p> <p>您也可以啟用雜湊變數。如果變數值很長，對變數進行雜湊可確保變數會正確地儲存在持續性資料表中。如果雜湊變數未啟用，則在變數值很長的情況下，只有變數值的固定首碼部分會儲存在持續性資料表中。因此，具有長變數值的兩個不同要求在應分派至不同的後端伺服器時，可能會分派至相同的後端伺服器，因為其變數值具有相同的首碼部分。</p>
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	<p>比對任何 HTTP 回應標頭。</p> <p>http_response.header_name - 要比對的標頭名稱</p> <p>http_response.header_value - 要比對的值</p>
HTTP 回應方法	<p>比對 HTTP 回應方法。</p> <p>http_response.method - 要比對的值</p>
HTTP 回應 URI	<p>比對 HTTP 回應 URI。</p> <p>http_response.uri - 要比對的值</p>
HTTP 回應 URI 引數	<p>比對 HTTP 回應 URI 引數。</p> <p>http_response.uri_args - 要比對的值</p>
HTTP 回應版本	<p>比對 HTTP 回應版本。</p> <p>http_response.version - 要比對的值</p>
HTTP 回應 Cookie	<p>比對任何 HTTP 回應 Cookie。</p> <p>http_response.cookie_value - 要比對的值</p>
用戶端 SSL	<p>比對用戶端 SSL 設定檔識別碼。</p> <p>ssl_profile_id - 要比對的值</p>
TCP 標頭連接埠	<p>比對 TCP 來源或目的地連接埠。</p> <p>tcp_header.source_port - 要比對的來源連接埠</p> <p>tcp_header.destination_port - 要比對的目的地連接埠</p>
IP 標頭來源	<p>比對 IP 來源或目的地位址。</p> <p>ip_header.source_address - 要比對的來源位址</p> <p>ip_header.destination_address - 要比對的目的地位址</p>

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 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
變數持續性學習	選取一般持續性設定檔，並輸入變數名稱。 您也可以啟用 雜湊變數 。如果變數值很長，對變數進行雜湊可確保變數會正確地儲存在持續性資料表中。如果 雜湊變數 未啟用，則在變數值很長的情況下，只有變數值的固定首碼部分會儲存在持續性資料表中。因此，具有長變數值的兩個不同要求在應分派至不同的後端伺服器時，可能會分派至相同的後端伺服器，因為其變數值具有相同的首碼部分。

針對伺服器集區和虛擬伺服器建立的群組

NSX Manager 會自動為負載平衡器伺服器集區和 VIP 連接埠建立群組。

負載平衡器建立的群組會顯示在**詳細目錄 > 群組**下。

伺服器集區群組會使用名稱 NLB.PoolLB.*Pool_Name* LB_Name 建立，並指派群組成員 IP 位址：

- 設定集區但不使用 LB-SNAT (透明)：0.0.0.0/0
- 設定集區但不使用 LB-SNAT 自動對應：T1-Uplink IP 100.64.x.y 和 T1-ServiceInterface IP
- 設定集區但不使用 LB-SNAT IP-Pool：LB-SNAT IP-Pool

使用名稱 NLB.VIP 建立 VIP 群組。**虛擬伺服器名稱**和 VIP 群組成員的 IP 位址為 VIP IP@。

針對伺服器集區群組，您可以從負載平衡器建立允許流量分散式防火牆規則 (NLB.PoolLB.*Pool_Name* LB_Name)。針對第 1 層閘道防火牆，您可以建立允許從用戶端到 LB VIP NLB.VIP 的流量。**虛擬伺服器名稱**。

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 如需關於如何使用 NSX-T Data Center 來管理公有雲工作負載虛擬機器的詳細資訊，請參閱第 22 章 使用 NSX Cloud。

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 一個**至底層的路由**，用於定址在傳送/計算 VPC/VNet 內的所有流量
- 2 另一個**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 一個**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分散式防火牆 (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。

支援的轉送原則和常見的使用案例

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
- 來自底層的路由
- 至覆疊的路由

以下是轉送原則可發揮效用的常見案例：

- **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 按一下**子網路**資料行中的**設定**，以新增子網路。
- 6 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**自動指派閘道**切換按鈕，以啟用或停用自動閘道 IP 指派。
 - d 按一下**新增**。
- 7 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**。
- 8 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
- 分散式防火牆
- 東西向網路安全性 - 鏈結第三方服務
- 設定閘道防火牆
- 南北向網路安全性 - 插入第三方服務
- 端點保護
- 安全性設定檔

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
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定義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

透過身分識別防火牆 (IDFW) 功能，NSX 管理員可建立以 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 會控制已啟用 IDFW 之來源虛擬機器 (VM) 對目的地伺服器的存取。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。

IDFW 也可用於具有受支援作業系統的虛擬機器。請參閱[身分識別防火牆支援的組態](#)。

IDFW 組態工作流程的高階概觀是從準備基礎結構開始。準備工作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 使用者所登入的桌面平台，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，然後將其傳送至內容引擎。此資訊可用於分散式防火牆的強制執行。

IDFW 只會處理在分散式防火牆規則中位於來源的使用者身分識別。以身分識別為基礎的群組無法作為 DFW 規則中的目的地。

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 NSX Guest Introspection 精簡型代理程式所提供。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精簡型代理程式。已登入的使用者不應擁有移除或停止代理程式的權限。

如需支援的 IDFW 組態，請參閱[身分識別防火牆支援的組態](#)。

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。

以身分識別為基礎的防火牆規則由 Active Directory (AD) 群組成員資格中的成員資格所決定。請參閱[身分識別防火牆支援的組態](#)。

IDFW 只會處理在分散式防火牆規則中位於來源的使用者身分識別。以身分識別為基礎的群組無法作為 IDFW 規則中的目的地。

備註 在強制執行身分識別防火牆規則時，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。

必要條件

如果已在虛擬機器上啟用 Windows 自動登入，請移至**本機電腦原則 > 電腦設定 > 系統管理範本 > 系統 > 登入**，並啟用**永遠在電腦啟動及登入時等待網路啟動**。

如需支援的 IDFW 組態，請參閱[身分識別防火牆支援的組態](#)。

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：[啟用身分識別防火牆](#)。
- 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](#)。

啟用身分識別防火牆

必須啟用身分識別防火牆，IDFW 防火牆規則才會生效。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 2 在左側按一下**動作 > 一般設定**。
- 3 切換狀態按鈕以啟用 IDFW。

此外也必須啟用分散式防火牆，IDFW 才能運作。

- 4 若要在獨立主機或叢集上啟用 IDFW，請選取**身分識別防火牆設定索引標籤**。
- 5 切換**啟用**列，然後選取獨立主機，或選取必須啟用 IDFW 主機的叢集。
- 6 按一下**儲存**。

身分識別防火牆最佳做法

下列最佳做法有助於讓身分識別防火牆規則發揮最大效益。

- IDFW 支援下列通訊協定：
 - 單一使用者 (VDI 或非 RDSH 伺服器) 使用案例支援 - TCP、UDP、ICMP
 - 多使用者 (RDSH) 使用案例支援 - TCP、UDP
- 以單一識別碼為基礎的群組在分散式防火牆規則內僅能用作來源。如果需要來源使用以 IP 和識別碼為基礎的群組，請分別建立兩個防火牆規則。
- 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。
- 對於本機網域控制站，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。

身分識別防火牆支援的組態

虛擬機器 (VM) 上的 IDFW 支援下列組態。不支援實體裝置的 IDFW。

客體作業系統	強制執行類型
Windows 8	桌面平台 - 支援桌面平台使用者使用案例
Windows 10	桌面平台 - 支援桌面平台使用者使用案例
Windows 2012	伺服器 - 支援伺服器使用者使用案例
Windows 2012R2	伺服器 - 支援伺服器使用者使用案例
Windows 2016	伺服器 - 支援伺服器使用者使用案例
Windows 2012R2	RDSH - 支援遠端桌面工作階段主機
Windows 2016	RDSH - 支援遠端桌面工作階段主機

Active Directory 網域控制站：

- Windows Server 2012

- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

主機作業系統：ESXi

VMware Tools - 版本 11

- VMCI 驅動程式
- NSX File Introspection 驅動程式
- NSX Network Introspection 驅動程式

第 7 層內容設定檔

第 7 層應用程式識別碼會設定於內容設定檔中。

內容設定檔可以指定一或多個**屬性**，也可包含子屬性，用於分散式防火牆 (DFW) 規則和閘道防火牆規則中。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。除了屬性以外，DFW 也支援可在內容設定檔中指定的完整網域名稱 (FQDN) 或 URL，以用於 FQDN 白名單或黑名單功能。目前，支援預先定義的網域清單。FQDN 可與屬性一起設定於內容設定檔中，也可分別設定在不同的內容設定檔中。內容設定檔一經定義，即可套用至一或多個分散式防火牆規則。

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。您也可以透過執行 API 呼叫 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 以查看 FQDN 的清單。

備註

- 閘道防火牆規則不支援在內容設定檔中使用 FQDN 屬性或其他子屬性。
- 第 0 層閘道防火牆原則不支援內容設定檔。閘道防火牆規則不支援使用 FQDN 屬性或其他子屬性。

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也包含第 7 層內容設定檔，則該封包會重新導向至名為 vDPI 引擎的使用者空間元件。每次的流量都會有少數後續封包被踢給該 vDPI 引擎，待其確認應用程式識別碼後，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再次與規則資料表進行比較，並與 5 元組和第 7 層應用程式識別碼進行比對。系統會採取完全相符的規則中所定義的適當動作，而如果有「允許」規則，則流量的所有後續封包都會在核心內進行處理，並與連線資料表進行比對。對於完全相符的「捨棄」規則，系統會產生拒絕封包。如果該流量被踢給 DPI，防火牆所產生的記錄就會包含第 7 層應用程式識別碼和適用的 URL。

傳入封包的規則處理：

- 1 進入 DFW 或閘道篩選器後，會在流量資料表中根據 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 引擎會確認應用程式識別碼。
- 5 確認應用程式識別碼後，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 進行中」旗標將會移除，且流量不再被踢給 DPI 引擎。
- 6 流量 (現在含應用程式識別碼) 會根據符合應用程式識別碼的所有規則進行重新評估，從根據 5 元組進行比對的原始規則開始，並提取第一個完全相符的 L4/L7 規則。系統會採取適當的動作 (允許/拒絕/回絕)，然後據以更新流量資料表項目。

第 7 層防火牆規則工作流程

第 7 層應用程式識別碼會用來建立內容設定檔，而這些設定檔會用於分散式防火牆規則或閘道防火牆規則中。基於屬性的規則強制執行，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屬性。應用程式識別碼包括版本 (SSL/TLS 及 CIFS/SMB) 和加密套件 (SSL/TLS)。對於分散式防火牆，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 白名單和黑名单結合使用。ESXi 和 KVM 主機均支援應用程式識別碼。

備註

- 閘道防火牆規則不支援在內容設定檔中使用 FQDN 屬性或其他子屬性。
- 第 0 層閘道防火牆原則不支援內容設定檔。閘道防火牆規則不支援使用 FQDN 屬性或其他子屬性。

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。

請注意，如果您使用第 7 層和 ICMP 的組合，或使用任何其他通訊協定，則需要將第 7 層防火牆規則放置於最後。第 7 層「任何/任何」規則以上的任何規則都將不會執行。

程序

- 1 建立自訂內容設定檔：[新增內容設定檔](#)。
- 2 在分散式防火牆規則或閘道防火牆規則中使用內容設定檔：[新增分散式防火牆](#) 或 [新增閘道防火牆原則和規則](#)。

在服務設定為任何的防火牆規則中，可以使用多個應用程式識別碼內容設定檔。對於 ALG 設定檔 (FTP、ORACLE、DCERPC、TFTP)，每個規則可支援一個內容設定檔。

屬性

第 7 層屬性 (應用程式識別碼) 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。

基於應用程式識別碼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。vDPI 可用來對已定義的模式 (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。

第 7 層應用程式識別碼用於分散式防火牆和閘道防火牆規則中的內容設定檔，且在 ESXi 和 KVM 主機上受到支援。

備註 NFS 第 4 版並非支援的屬性。

備註

- 閘道防火牆規則不支援在內容設定檔中使用 FQDN 屬性或其他子屬性。
- 第 0 層閘道防火牆原則不支援內容設定檔。閘道防火牆規則不支援使用 FQDN 屬性或其他子屬性。

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。

屬性 (應用程式識別碼)	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
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

屬性 (應用程式識別碼)	說明	類型
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。	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
CTRXCOTO	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
CTRICA	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
DHCP	動態主機設定通訊協定是用來對網路內 IP 位址分配進行管理的通訊協定	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
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
MCAFREE	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
備註 NFS 第 4 版並非支援的屬性。		

屬性 (應用程式識別碼)	說明	類型
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
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
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 流程提供頻外控制資訊。	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
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
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
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
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	SYSLOG 是一種通訊協定，可讓網路裝置將事件訊息傳送至記錄伺服器。	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

屬性 (應用程式識別碼)	說明	類型
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及服務。	網路

分散式防火牆

分散式防火牆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。

表 10-2. 分散式防火牆規則類別

類別	說明
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

防火牆草稿

草稿是具備原則區段和規則的完整分散式防火牆組態。草稿可以是自動儲存或手動儲存，並可立即發佈或儲存以在日後發佈。

若要儲存手動草稿防火牆組態，請移至分散式防火牆畫面的右上方，然後按一下**動作 > 儲存**。儲存之後，可以選取**動作 > 檢視**來檢視組態。依預設會啟用自動草稿。若要停用自動草稿，請移至**動作 > 一般設定**。當自動草稿啟用時，對防火牆組態所做的任何變更都會導致系統產生自動草稿。最多可儲存 100 份自動草稿和 10 份手動草稿。您可以編輯自動草稿並將其另存為手動草稿，以供立即發佈或稍後發佈。若要防止多個使用者開啟並編輯草稿，可以鎖定手動草稿。發佈草稿時，草稿中的組態會取代目前的組態。

儲存或檢視防火牆草稿

草稿是已發佈或已儲存供日後發行的分散式防火牆組態。草稿可自動和手動建立。

手動草稿可供編輯和儲存。自動草稿可以複製並儲存為手動草稿，然後進行編輯。可以儲存的草稿數目上限為 100 個自動草稿和 10 個手動草稿。

程序

- 1 按一下**安全性 > 分散式防火牆**。

- 若要手動儲存防火牆組態，請移至**動作 > 儲存**。

手動草稿可直接儲存，或在進行編輯後儲存。儲存後，您可以還原為原始組態。

- 為組態命名。
- 若要可防止多個使用者開啟並編輯手動草稿，請**鎖定**組態，並新增註解。
- 按一下**儲存**。
- 若要檢視已儲存的組態，請按一下**動作 > 視圖**。

系統會開啟一個顯示所有已儲存組態的時間表。若要查看詳細資料，例如草稿名稱、日期、時間以及儲存者，請指向任何草稿的點圖示或星號圖示。已儲存的組態可依照時間篩選，顯示在前 1 天、1 週、30 天或前 3 個月的所有草稿。這些組態可依自動草稿和我已儲存進行篩選。也可以使用右上方的搜尋工具依名稱篩選。

- 將游標暫留在草稿上可檢視所儲存組態的名稱、日期和時間詳細資料。按一下名稱可檢視草稿詳細資料。

詳細的草稿視圖會顯示為了與此草稿同步，應該對目前的防火牆組態進行的必要變更。如果已發佈此草稿，則此視圖中顯示的所有變更將套用至目前的組態。

按一下向下箭頭可展開每個區段，並顯示每個區段中新增、修改和刪除的變更。比較會在新增的規則的方塊左側顯示綠色列、修改的元素 (例如名稱變更) 有黃色列，而已刪除的元素則有紅色列。

- 若要編輯所選草稿的名稱或說明，請從**檢視草稿詳細資料**視窗中，按一下功能表圖示 (三個點)，並選取**編輯**。

手動草稿可以鎖定。如果鎖定，則必須提供草稿的註解。

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](#)。

- 自動草稿和手動草稿也可透過按一下**複製**來加以複製和儲存。

在 [已儲存的組態] 視窗中，可以接受預設名稱，或進行編輯。您也可以鎖定組態。如果鎖定，則必須提供草稿的註解。

- 若要儲存草稿組態的複製版本，請按一下**儲存**。草稿現在已出現在 [已儲存的組態] 區段中。

後續步驟

檢視草稿之後，您可以載入草稿並將其發佈。然後它會成為作用中防火牆組態。

發佈或還原防火牆草稿

自動草稿和已儲存的手動草稿都可以載入並發佈以成為作用中組態。

在發佈期間，系統會建立新的自動草稿。此自動草稿可以發佈以還原為先前的組態。

程序

- 若要檢視已儲存的組態，請按一下**動作 > 視圖**。

系統會開啟一個顯示所有已儲存組態的時間表。若要查看詳細資料，例如草稿名稱、日期、時間以及儲存者，請指向任何草稿的點圖示。已儲存的組態會依照時間篩選，顯示在 1 天、1 週、30 天或過去 3 個月建立的所有草稿。

- 2 按一下草稿名稱，接著會顯示 [檢視草稿詳細資料] 視窗。
- 3 按一下**載入**。新的防火牆組態會出現在主視窗中。

備註 如果正在使用防火牆篩選器，或是目前組態中有未儲存的變更，將無法載入草稿。

- 4 若要認可草稿組態，並使其成為作用中，請按一下**發佈**。若要回復為先前的已發佈組態，請按一下**還原**。
發佈之後，草稿中的變更將會顯示在作用中組態。
- 5 若要在發佈之前編輯所選草稿的內容，在按一下**載入**之後，請編輯組態。
- 6 若要儲存草稿組態的編輯版本，請按一下**動作 > 儲存**。
手動草稿可以儲存為新的組態或現有組態的更新。自動草稿僅可以儲存為新的組態。
- 7 輸入**名稱**和選用的**說明**。您也可以**鎖定**草稿。如果鎖定，則必須提供草稿的註解。
- 8 按一下**儲存**。
- 9 若要認可草稿組態並使其成為作用中，請按一下**發佈**，若要返回先前的已發佈組態，請按一下**還原**。

新增分散式防火牆

分散式防火牆 (DFW) 會監控虛擬機器上的所有東西向流量。

必要條件

要受 DFW 保護的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 在強制執行身分識別防火牆規則時，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。

請注意，如果您使用第 7 層和 ICMP 的組合，或使用任何其他通訊協定，則需要將第 7 層防火牆規則放置於最後。第 7 層「任何/任何」規則以上的任何規則都將不會執行。

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 選取導覽面板中的**安全性 > Distributed Firewall**。
- 3 選取**動作 > 一般設定**，並切換分散式防火牆狀態，以啟用分散式防火牆。按一下**儲存**。
- 4 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[分散式防火牆](#)。
- 5 為新的原則區段輸入**名稱**。

6 (選擇性) 若要設定下列原則設定，請按一下齒輪圖示：

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 (DFW) 可能看不到特定流量的三向信號交換 (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>為特定 DFW 原則啟用 TCP 嚴格模式，且使用預設的「任何-任何」封鎖規則時，系統會捨棄未完成三向信號交換連線要求，且符合此區段中以 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。</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，並使用這項資訊決定允許通過防火牆的封包。
已鎖定	<p>您可以鎖定原則，以防止多個使用者編輯相同的區段。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。可在 IDFW 規則的來源欄位中使用含有 Active Directory 成員的群組。如需詳細資訊，請參閱[新增群組](#)。

支援 IPv4、IPv6 和多點傳播位址。

附註：IPv6 防火牆必須在已連線的區段上為 IPv6 啟用 IP 探索。如需詳細資訊，請參閱[瞭解 IP 探索區段設定檔](#)。

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，則會使用符合任何條件的目的地。如需詳細資訊，請參閱[新增群組](#)。支援 IPv4、IPv6 和多點傳播位址。

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 將規則新增至「乙太網路」類別時，**設定檔**資料行無法使用。針對所有其他規則類別，請在**設定檔**資料行中按一下編輯圖示，然後選取內容設定檔，或是按一下**新增內容設定檔**。請參閱[新增內容設定檔](#)。

內容設定檔會使用在分散式防火牆規則和閘道防火牆規則中使用的第 7 層應用程式識別碼屬性。在服務設定為**任何**的防火牆規則中，可以使用多個應用程式識別碼內容設定檔。對於 ALG 設定檔 (FTP 和 TFTP)，每個規則可支援一個內容設定檔。

14 按一下**套用**，將內容設定檔套用至規則。

- 15 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。

- 16 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。

- 17 按一下狀態切換按鈕以啟用或停用規則。

- 18 (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/dfwpklogs.log 檔案。
方向	是指從目的地物件的角度而言的流量方向。「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。
記錄標籤	啟用記錄時，記錄標籤會在防火牆記錄中延續使用。

- 19 按一下**發佈**。可以新增多個規則，然後一同發佈。

- 20 在每個規則上，按一下**資訊**圖示以檢視規則識別碼，及其強制執行的位置。

在您發佈規則之前，此圖示會呈現灰色。您也可以在按一下篩選器圖示時指定規則識別碼，而僅顯示符合篩選準則的原則和規則。

- 21 實現狀態 API 已在安全性原則層級上獲得增強，以提供其他實現狀態資訊。若要達到此目的，可指定查詢參數 `include_enforced_status=true` 與 `intent_path`。進行下列 API 呼叫。

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

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 mainrs/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 mainrs/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，而無需修改個別規則。若要設定預設連線策略，請移至 **分散式防火牆**。在頁面頂端按一下連線狀態以選取其他選項。

必須已建立防火牆原則和規則，才能變更預設選取的連線策略並使其立即生效。如果未建立任何原則或規則，則系統會維持使用預設的連線策略，直到有建立原則和規則為止。

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已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，包括 DHCP 流量在內。
- **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。

管理防火牆排除清單

防火牆排除清單由可以根據群組成員資格從防火牆規則中排除的群組組成。

群組可以從防火牆規則中排除，且清單中最多可以有 100 個群組。用於防火牆排除清單的群組中無法包含 IP 集合、MAC 集合和 AD 群組作為成員。

備註 NSX-T Data Center 會自動將 NSX Manager 和 NSX Edge 節點虛擬機器新增至防火牆排除清單。

程序

- 1 導覽至**安全性 > 分散式防火牆 > 動作 > 排除清單**。
畫面中會有一個視窗列出可用的群組。
- 2 若要將群組新增至排除清單，請按一下任何群組旁的核取方塊。然後，按一下**套用**。
- 3 若要建立群組，請按一下**新增群組**。請參閱**新增群組**。
- 4 若要編輯群組，請按一下群組旁的三個點功能表，然後選取**編輯**。

- 5 若要刪除群組，請按一下三個點功能表，然後選取**刪除**。
- 6 若要顯示群組詳細資料，請按一下**全部展開**。

篩選特定網域 (FQDN/URL)

設定分散式防火牆規則，以篩選使用 FQDN/URL 識別的特定網域，例如 *.office365.com。

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。您也可以透過執行 API 呼叫 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 以查看 FQDN 的清單。

您必須先設定 DNS 規則，然後在其下設定 FQDN 允許清單或封鎖清單規則。NSX-T Data Center 使用 DNS 回應 (DNS 伺服器發給虛擬機器的回應) 中的存留時間 (TTL)，來保留虛擬機器 (VM) 的 DNS 至 IP 對應快取項目。若要使用 DNS 安全性設定檔來覆寫 DNS TTL，請參閱[設定 DNS 安全性](#)。若要使 FQDN 篩選生效，虛擬機器需要使用 DNS 伺服器進行網域解析 (沒有靜態 DNS 項目)，並且還需要採用在 DNS 回應中收到的 TTL。NSX-T Data Center 會使用 DNS 窺探來取得 IP 位址與 FQDN 之間的對應。您應針對所有邏輯連接埠上的交換器啟用 SpoofGuard，以防範 DNS 詐騙攻擊的風險。DNS 詐騙攻擊是指惡意虛擬機器可插入偽造的 DNS 回應，以將流量重新導向至惡意端點或略過防火牆。如需 SpoofGuard 的詳細資訊，請參閱[瞭解 SpoofGuard 區段設定檔](#)。

此功能適用於第 7 層，未涵蓋 ICMP。如果使用者針對 example.com 上的所有服務建立了拒絕清單規則，當 Ping example.com 有回應，但 curl example.com 沒有回應時，該功能便會如預期般運作。

選取萬用字元 FQDN 是最佳做法，因為其中包含子網域。例如，選取 *example.com 將會包含 americas.example.com 和 emea.example.com 之類的子網域。使用 example.com 則不會包含任何子網域。

為 ESXi 主機執行 vMotion 期間會保留以 FQDN 為基礎的規則。

備註 支援 ESXi 和 KVM 主機。KVM 主機僅支援 FQDN 允許清單。FQDN 篩選僅適用於 TCP 和 UDP 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 導覽至**安全性 > 分散式防火牆**。
- 3 依照[新增分散式防火牆](#)中的步驟，新增防火牆原則區段。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**)，並提供下列詳細資料：

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。

選項	說明
套用至	視需要選取群組。
動作	選取允許。

- 6 再次按一下**新增規則**，以設定 FQDN 允許清單或封鎖清單規則。
- 7 為規則適當命名，例如 **FQDN/URL 允許清單**。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、捨棄或拒絕 。

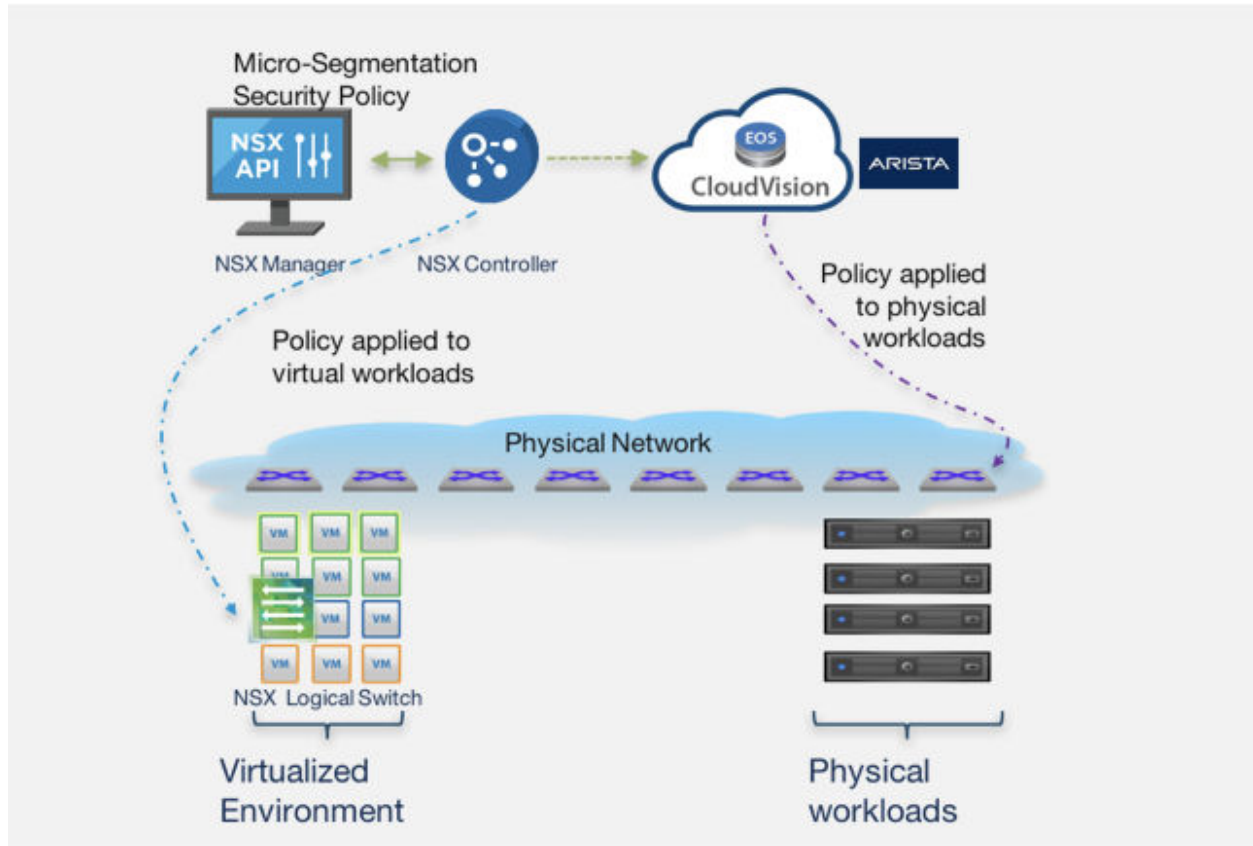
- 9 按一下**發佈**。

將安全性原則延伸至實體工作負載

NSX-T Data Center 可同時作為虛擬和實體工作負載的單一管理點。

從 NSX-T Data Center 2.5.1 開始，支援與 Arista CloudVision eXchange (CVX) 整合。此整合可協助網路與安全性服務獨立於應用程式架構或實體網路基礎結構之外，在虛擬和實體工作負載之間維持一致。NSX-T Data Center 不會直接編程實體網路交換器或路由器，而是會在實體 SDN 控制器層級進行整合，從而讓安全管理員和實體網路管理員保有自主性。

從 NSX-T Data Center 2.5.1 開始，支援與 Arista EOS 4.22.1FX-PCS 及更新版本整合。



限制

- 必須先有 ARP 流量存在，Arista 交換器才能將防火牆規則套用至與 Arista 交換器連線的端點主機。因此，封包會先通過交換器，然後再設定防火牆規則來封鎖流量。
- 當交換器當機或重新載入時，之前允許的流量將不會繼續。您必須在交換器啟動後再次填入 ARP 資料表，然後才能在交換器上強制執行防火牆規則。
- 針對連線至與 Arista 實體交換器連線之 FTP 伺服器的 FTP 被動用戶端，Arista 實體交換器上無法套用防火牆規則。
- 在為 CVX 叢集使用虛擬 IP 的 CVX HA 設定中，CVX 虛擬機器的 DVPF 混合模式和偽造的傳輸必須設定為接受。如果將其設定為預設值 (拒絕)，便無法從 NSX Manager 連線到 CVX HA 虛擬 IP。

設定 Arista CVX 以使其與 NSX-T Manager 互動

在設定 NSX-T Data Center 後，請於 Arista CloudVision eXchange (CVX) 上完成組態設定程序，以便讓 CVX 與 NSX-T Data Center 互動。

必要條件

NSX-T Data Center 已將 CVX 登錄為強制執行點。

程序

- 1 以 root 使用者身分登入 NSX Manager，然後執行下列命令來為 CVX 建立指紋，以便與 NSX Manager 通訊：

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

輸出範例：

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 從 CVX CLI 執行下列命令：

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 從 CVX CLI 執行下列命令以檢查組態：

```
show running-config
```

輸出範例：

```
cvx
    no shutdown
    source-interface Management1
    !
    service hsc
        no shutdown
    !
    service pcs
        no shutdown
        controller 192.168.2.80
        username admin
```

```
password 7 046D26110E33491F482F2800131909556B
enforcement-point cvx-default-ep
pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- 4 在連線到實體伺服器的實體交換器乙太網路介面上設定標籤。在由 CVX 管理的實體交換器上執行下列命令。

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- 5 執行下列命令以驗證交換器的標籤組態：

```
show running-config section tag
```

輸出範例：

```
interface Ethernet4
  description connected-to-7150s-3
  switchport trunk allowed vlan 1-4093
  switchport mode trunk
  tag sx4_app_server
```

在已標記的介面上使用 ARP 學習的 IP 位址會與 NSX-T Data Center 共用。

- 6 登入 NSX Manager 以針對 CVX 所管理的實體工作負載建立和發佈防火牆規則。如需如何建立規則的詳細資訊，請參閱第 10 章 安全性。例如：

	名稱	來源	目的地	服務	設定檔	套用於	動作	
+	Firewall_Services (2)	套用於	DFW				● 開啟	
+	vm_to_phy_server	vm	phy_server	任何	無	DFW	● 允許	
+	phy_server_to_vm	phy_server	vm	任何	無	DFW	● 允許	

在 NSX-T Data Center 中發佈的 NSX-T Data Center 原則和規則，會在由 CVX 管理的實體交換器上顯示為動態 ACL。

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
  10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
  10 permit ip host 27.1.1.11 host 71.1.1.3
```

如需詳細資訊，請參閱 [CVX HA 設定](#)、[CVX HA 虛擬 IP 設定](#) 以及 [實體交換器 Mlag 設定](#)

設定 NSX-T Data Center 以使其與 Arista CVX 互動

在 NSX-T Data Center 上完成組態設定程序，以便可將 CVX 新增為 NSX-T Data Center 中的強制執行點，使 NSX-T Data Center 可與 CVX 互動。

必要條件

取得 Arista CVX 叢集的虛擬 IP 位址。

程序

- 1 以 root 使用者身分登入 NSX Manager，然後執行下列命令以擷取 CVX 的指紋：

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

輸出範例：

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 編輯所擷取的指紋，使其僅使用小寫字元，並在指紋中排除任何冒號。

編輯後的 CVX 指紋範例：

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 呼叫 PATCH /policy/api/v1/infra/sites/default/enforcement-points API，然後使用 CVX 指紋來為 CVX 建立強制執行端點。例如：

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 呼叫 GET /policy/api/v1/infra/sites/default/enforcement-points API 以擷取端點資訊。例如：

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
```

```

"auto_enforce": "false",
"connection_info": {
"enforcement_point_address": "<IP address of CVX>",
"resource_type": "CvxConnectionInfo",
"username": "admin",
"password": "1q2w3e4rT",
"thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
}
}

```

輸出範例：

```

{
"connection_info": {
"thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
"enforcement_point_address": "192.168.2.198",
"resource_type": "CvxConnectionInfo"
},
"auto_enforce": false,
"resource_type": "EnforcementPoint",
"id": "cvx-default-ep",
"display_name": "cvx-default-ep",
"path": "/infra/sites/default/enforcement-points/cvx-default-ep",
"relative_path": "cvx-default-ep",
"parent_path": "/infra/sites/default",
"marked_for_delete": false,
"_system_owned": false,
"_create_user": "admin",
"_create_time": 1564036461953,
"_last_modified_user": "admin",
"_last_modified_time": 1564036461953,
"_protection": "NOT_PROTECTED",
"_revision": 0
}

```

5 呼叫 POST /api/v1/notification-watchers/ API，然後使用 CVX 指紋來建立通知識別碼。例如：

```

POST https://<nsx-manager>/api/v1/notification-watchers/
{
"server": "<virtual IP address of CVX cluster>",
"method": "POST",
"uri": "/pcs/v1/nsgroup/notification",
"use_https": true,
"certificate_sha256_thumbprint":
"35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
"authentication_scheme": {
"scheme_name": "BASIC_AUTH",
"username": "cvpadmin",
"password": "1q2w3e4rT"
}
}

```

6 呼叫 GET /api/v1/notification-watchers/ 以擷取通知識別碼。

輸出範例：

```
{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

7 呼叫 PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap API 以建立 CVX 網域部署對應。例如：

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-
default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}
```

8 呼叫 GET /policy/api/v1/infra/domains/default/domain-deployment-maps API 以擷取部署對應資訊。

共用位址集

您可以在分散式防火牆規則的**套用至文字方塊**中，建立及使用以動態或邏輯物件為基礎的安全群組。

由於位址集是根據虛擬機器名稱或標籤動態填入，且必須在每個篩選器上更新，因此為了儲存 DFW 規則和 IP 位址集，可能會耗盡主機上可用的堆積記憶體數量。

在 NSX-T Data Center 2.5 版及更新版本中，名為全域或共用位址集的功能可讓您在所有篩選器之間共用位址集。雖然每個篩選器可以有不同的規則，但根據**套用至**，位址集成員在所有篩選器間會維持不變。依預設會啟用此功能，以減少堆積記憶體使用量。此功能無法停用。

在 NSX-T Data Center 2.4 及更早版本中，系統會停用全域或共用位址集，且分散式防火牆規則較多的環境可能會發生 VSIP 堆積耗盡的情況。

東西向網路安全性 - 鏈結第三方服務

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。

必要條件

- 合作夥伴必須向 NSX-T Data Center 登錄服務。
- 必須使用傳輸節點設定檔，做好將 ESXi 主機作為 NSX-T Data Center 傳輸節點的準備。

備註

- 服務虛擬機器僅在 ESXi 主機上受支援，而在 KVM 主機上不受支援。
- NSX-T Data Center 僅保護在 ESXi 主機上執行的客體虛擬機器。
- NSX-T Data Center 不會保護在 KVM 主機上執行的客體虛擬機器。

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向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。服務平面可管理服務連結。

- **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)。

東西向流量的 NSX-T Data Center 需求

在 NSX-T Data Center 部署中，您必須確保存在覆疊傳輸區域和支援覆疊的邏輯交換器。

東西向服務插入會套用至整個 NSX-T 部署。您無法在叢集層級或主機層級部署服務。

所有傳輸節點的類型都必須是「覆疊」，因為服務會在 GENEVE 或支援覆疊的邏輯交換器上傳送流量。支援覆疊 (支援 GENEVE) 的邏輯交換器會在內部佈建，且不會顯示在使用者介面上。

即使您計劃使用僅支援 VLAN 的邏輯交換器的部署，東西向流量仍會透過覆疊傳輸區域和支援覆疊的邏輯交換器傳遞。因此，請確保您建立覆疊傳輸區域和支援 GENEVE 的邏輯交換器。若沒有這些需求，在 vMotion 期間，主機上的 guestVM 將無法移轉到其他傳輸節點。guestVM 會進入中斷連線狀態，導致東西向服務中發生組態錯誤。

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 10-3. 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
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

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，身為管理員，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。
- 合作夥伴服務必須已向 NSX-T Data Center 登錄，且已可進行部署。
- 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。
- 以主機為基礎的服務部署：在每個主機上部署服務虛擬機器之前，請藉由套用傳輸節點設定檔以使用 NSX-T Data Center 設定叢集的每個主機。

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 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，選取要部署服務的 vCenter Server。
- 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**，然後選擇 DHCP 或靜態 IP 位址類型和資料網路，以進入 [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。連線至服務區段的客體虛擬機器會受到東西向網路流量保護。
- 10 在 [部署類型] 欄位中，選取下列其中一個部署選項。根據合作夥伴所登錄的服務，可將多項服務部署為單一服務虛擬機器的一部分。
 - 已叢集化：在主機服務虛擬機器專用叢集中包含的一或多個主機上部署服務。
 - 以主機為基礎：在叢集內的所有主機上部署服務。
- 11 在 [部署範本] 欄位中選取範本，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 (僅適用於以叢集為基礎的部署) 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[新增服務設定檔](#)。

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。

備註 您可以為單一廠商建立多個服務設定檔。例如，為正向路徑設定的服務設定檔提供 IDS 保護，而為反向路徑設定的服務設定檔則支援 IPS 保護。不過，您也可以為正向和反向路徑設定單一服務設定檔。

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 **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 [重新導向動作] 欄位會繼承廠商範本中的功能。例如，如果「複製」是廠商範本提供的功能，則您建立服務設定檔時依預設重新導向動作即為「複製」。
- 6 (選用) 定義任何要篩選出的標籤，並管理服務設定檔。
- 7 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。服務區段是連接覆蓋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**，以使用您為正向路徑設定的服務設定檔。
- 10 若要為反向路徑設定新的服務設定檔，請按一下**設定反向路徑**，然後新增服務設定檔。
- 11 按一下**儲存**以完成為服務鏈結新增反向路徑的作業。
- 12 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。
- 13 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-T Data Center 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 選取服務鏈結。
- 4 若要新增原則，請按一下**發佈**。
- 5 按一下區段上的垂直省略符號 (⋮)，然後按一下**新增規則**。
- 6 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。
 - a 使用下列其中一個實體定義成員資格準則：
 - 虛擬機器
 - 邏輯交換器
 - 邏輯連接埠
 - IP 集合
 - b 使用下列其中一個實體定義靜態成員清單：
 - 群組
 - 區段
 - 區段連接埠
 - 虛擬網路介面
 - 虛擬機器
- 7 按一下**儲存**。
- 8 若要新增目的地群組，請編輯**目的地**欄位。
- 9 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。
- 10 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。
- 11 按一下**發佈**。
- 12 若要還原已發佈的規則，請選取規則，然後按一下**還原**。
- 13 若要新增原則，請按一下 **+** **新增原則**。
- 14 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。
- 15 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**。
- 16 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 10-4. 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**。
- 3 若要啟用閘道防火牆，請選取 **動作 > 一般設定**，然後切換狀態按鈕。按一下 **儲存**。
- 4 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](#)。
- 5 為新的原則區段輸入 **名稱**。
- 6 選取原則 **目的地**。

7 按一下齒輪圖示以進行下列原則設定：

設定	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 嚴格可以就個別區段啟用，以關閉中間工作階段提取，並強制要求三向信號交換。為特定防火牆原則啟用 TCP 嚴格模式，且使用預設的「任何-任何」封鎖規則時，系統會捨棄未完成三向信號交換連線要求，且符合此原則區段中以 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，並使用這項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。

8 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。

9 選取原則區段，然後按一下**新增規則**。

10 輸入規則的名稱。支援 IPv4、IPv6 和多點傳播位址。

11 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](#)。

12 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](#)。

13 在**服務**資料行中按一下鉛筆圖示，然後選取服務。若未定義，則代表不分服務。

14 在**設定檔**資料行中按一下編輯圖示，然後選取內容設定檔，或是按一下**新增內容設定檔**。請參閱[新增內容設定檔](#)。

- 第 0 層閘道防火牆原則不支援內容設定檔。
- 閘道防火牆規則不支援具有 FQDN 屬性或其他子屬性的內容設定檔。

內容設定檔會使用在分散式防火牆規則和閘道防火牆規則中使用的第 7 層應用程式識別碼屬性。在服務設定為**任何**的防火牆規則中，可以使用多個應用程式識別碼內容設定檔。對於 ALG 設定檔 (FTP 和 TFTP)，每個規則可支援一個內容設定檔。

15 按一下**套用**。

16 **套用至**資料行會定義每個規則的強制執行範圍，並允許使用者選擇性地將規則套用至一或多個上行介面或服務介面。依預設，閘道防火牆規則會套用至所選閘道上的所有可用上行和服務介面。

17 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。
拒絕	拒絕具有指定來源、目的地和通訊協定的封包。拒絕封包時，系統會將「無法連線到目的地」訊息傳送給寄件者。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。經過一次嘗試而無法建立連線後，傳送方應用程式會收到通知。

18 按一下狀態切換按鈕以啟用或停用規則。

19 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 Edge 的 /var/log/syslog 上。
方向	選項為傳入、傳出及傳入/傳出。預設為傳入/傳出。此欄位是指從目的地物件的角度而言的流量方向。傳入表示僅會檢查流向物件的流量，傳出表示僅會檢查來自物件的流量，而傳入/傳出則表示會檢查這兩個方向的流量。
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。

20 按一下發佈。可以新增多個規則，然後一同發佈。

21 在每個原則區段中，按一下資訊圖示以檢視推送至 Edge 節點的 Edge 防火牆規則目前的狀態。此外也會顯示規則推送至 Edge 節點時所產生的任何警示。

22 若要檢視套用至 Edge 節點之原則規則的整併狀態，請執行 API 呼叫。

```
GET https://<policy-mgr>/policy/api/v1/infra/realized-state/status?
intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

南北向網路安全性 - 插入第三方服務

NSX-T Data Center 提供在資料中心的第 0 層或第 1 層路由器上插入第三方服務的功能，以將流量重新導向至第三方服務進行自我檢查。僅支援 ESXi 主機部署南北向服務虛擬機器。不支援 KVM 主機。

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 管理員可存取合作夥伴服務。
- 邏輯路由器的高可用性模式必須處於主動備用模式。
- 開啟 Distributed Resource Scheduler 公用程式。

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 > 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。

表 10-6. 合作夥伴服務詳細資料 (續)

欄位	說明
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。
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 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。
- 4 若要新增原則，請按一下**發佈**。
- 5 按一下區段上的垂直省略符號 (⋮)，然後按一下**新增規則**。
- 6 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。
- 7 按一下**儲存**。
- 8 若要新增目的地群組，請編輯**目的地**欄位。
- 9 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。
- 10 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。
- 11 按一下**發佈**。
- 12 若要還原已發佈的規則，請選取規則，然後按一下**還原**。
- 13 若要新增原則，請按一下 **+** **新增原則**。
- 14 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。
- 15 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**。
- 16 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。

端點保護

NSX-T Data Center 可讓您插入第三方合作夥伴服務作為個別的服務虛擬機器，以提供端點保護服務。合作夥伴服務虛擬機器會根據 NSX-T Data Center 管理員所套用的端點保護原則規則，處理來自客體虛擬機器的檔案、程序和登錄事件。

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

在虛擬環境中，使用 Guest Introspection 平台為客體虛擬機器提供防毒和防惡意程式碼保護。

身為 NSX 管理員，您可以實作部署為服務虛擬機器 (SVM) 的防毒和防惡意程式碼解決方案，以監控客體虛擬機器上的檔案、網路或程序活動。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，服務虛擬機器會決定如何回應事件。例如，檢查檔案中是否有病毒特徵碼。

- 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，它會要求客體虛擬機器上的精簡型代理程式執行下列其中一個動作：
 - 刪除受感染的檔案或拒絕對該檔案的存取。
 - NSX 可為受感染的虛擬機器指派標籤。此外，您也可以定義一個規則，將這種已標記的客體虛擬機器自動移至安全群組，以隔離受感染的虛擬機器，然後進一步的掃描並從網路隔離，直到完全移除感染為止。

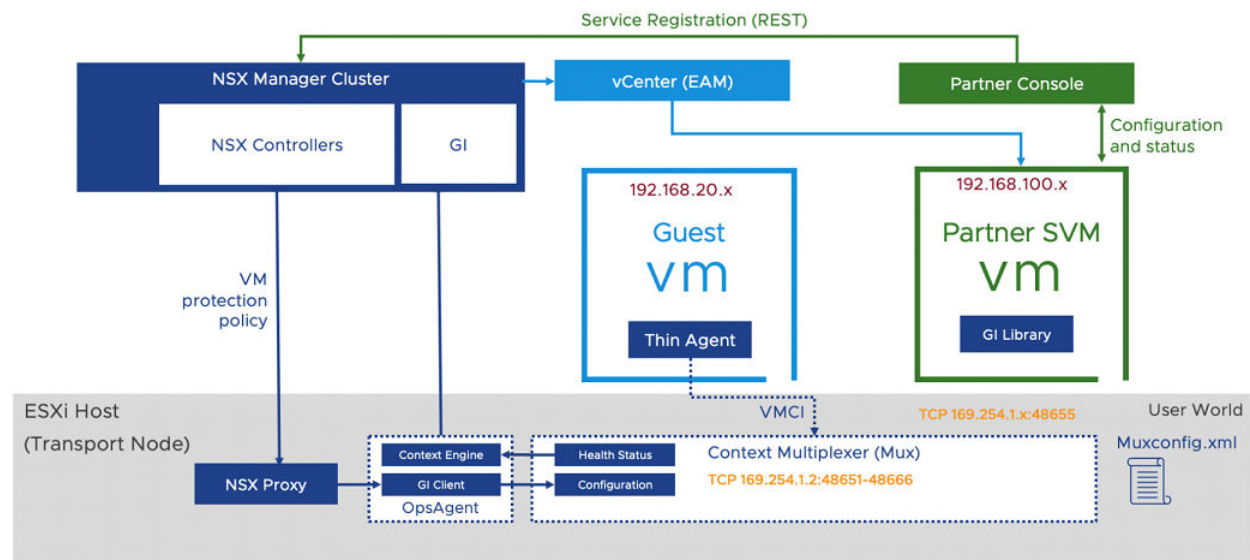
使用 Guest Introspection 平台保護客體虛擬機器端點的好處如下：

- 減少計算資源的耗用量：Guest Introspection 會將主機上每個端點的病毒特徵碼和安全性掃描邏輯卸載至主機上的第三方合作夥伴服務虛擬機器。由於病毒掃描只會在服務虛擬機器上執行，因此不需要在客體虛擬機器上耗費計算資源執行病毒掃描。
- 更好的管理：當病毒掃描卸載至服務虛擬機器時，病毒特徵碼只需更新至每個主機的一個物件。此類機制的運作效果優於以代理程式為基礎的解決方案，後者必須將相同的病毒特徵碼更新至所有客體虛擬機器上。
- 持續的防毒和防惡意程式碼保護：當服務虛擬機器持續執行時，客體虛擬機器不需要執行最新的病毒特徵碼。例如，快照虛擬機器可能會執行某些較舊版本的病毒特徵碼，而使其在傳統的端點保護方式中容易受到攻擊。透過 Guest Introspection 平台，服務虛擬機器會持續執行最新的病毒和惡意軟體特徵碼，從而確保任何新增的虛擬機器也會透過最新的病毒特徵碼受到保護。
- 將病毒特徵碼卸載至服務虛擬機器：病毒資料庫生命週期獨立於客體虛擬機器生命週期以外，因此服務虛擬機器不會受到客體虛擬機器中斷的影響。

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 10-1. Guest Introspection 架構



主要概念：

- 合作夥伴主控台：這是安全廠商所提供的 Web 應用程式，可與 Guest Introspection 平台搭配使用。
- NSX Manager：這是 NSX 的管理平面應用裝置，可為客戶和合作夥伴提供 API 和圖形使用者介面，用於網路和安全性原則的組態。對於 Guest Introspection，NSX Manager 也提供用來部署及管理合作夥伴應用裝置的 API 和 GUI。
- Guest Introspection SDK：VMware 提供給安全廠商使用的程式庫。

- **服務虛擬機器**：是安全廠商提供的虛擬機器，會使用 VMware 提供的 Guest Introspection SDK。它包含掃描檔案或程序事件的邏輯，用以偵測客體上的病毒或惡意軟體。在掃描要求後，它會針對客體虛擬機器對要求採取的動作傳回相關判定或通知。
- **Guest Introspection 主機代理程式 (內容多工器)**：它會處理端點保護原則的組態。它也會對來自受保護虛擬機器的訊息進行多工處理，並將其轉送至服務虛擬機器。它會報告 Guest Introspection 平台的健全狀況狀態，並在 `muxconfig.xml` 檔案中維護服務虛擬機器組態的記錄。
- **Ops Agent (內容引擎和 Guest Introspection Client)**：它會將 Guest Introspection 組態轉送至 Guest Introspection 主機代理程式 (內容多工器)。它也會將解決方案的健全狀況狀態轉送至 NSX Manager。
- **EAM**：NSX Manager 會使用 ESXi Agent Manager 在叢集上每個設定為要保護的主機上部署合作夥伴服務虛擬機器。
- **精簡型代理程式**：這是在客體虛擬機器中執行的檔案或網路自我檢查代理程式。它也會攔截透過主機代理程式轉送至服務虛擬機器的檔案和網路活動。此代理程式是 VMware Tools 的一部分。它會取代由防毒或防惡意軟體安全廠商所提供的傳統代理程式。這是一般的輕量型代理程式，可讓要掃描的檔案和程序更快速地卸載至廠商所提供的服務虛擬機器。

端點保護的重要概念

端點保護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**：合作夥伴會使用下列屬性來定義服務：名稱、說明、支援的構成要素、包含網路介面的部署屬性，以及 SVM 所要使用的應用裝置 OVF 套件位置。
- **服務插入**：NSX 會提供服務插入架構，讓合作夥伴可將網路與安全性解決方案與 NSX 平台整合。Guest Introspection 解決方案就是這種形式的服務插入之一。
- **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。例如，保護層級可以是「金級」、「銀級」或「白金級」。服務設定檔可從廠商範本建立，這可讓 NSX 管理員根據其喜好設定為廠商範本命名。對於 Guest Introspection 以外的服務，服務設定檔允許使用屬性進行進一步的自訂。然後，服務設定檔可在端點保護原則規則中用來為 NSX 中定義的虛擬機器群組設定保護。身為管理員，您可以根據虛擬機器名稱、標籤或識別碼來建立群組。您可以選擇性地從單一廠商範本建立多個服務設定檔。
- **端點保護原則**：原則是規則的集合。當您擁有多個原則時，請依序排列這些原則加以執行。原則內定義的規則也是如此。例如，假設原則 A 有三個規則，而原則 B 有四個規則，這些原則以原則 A 優先於原則 B 的順序排列。當 Guest Introspection 開始執行原則時，將會先執行原則 A 中的規則，再執行原則 B 中的規則。
- **端點保護規則**：身為 NSX 管理員，您可以建立規則以指定要保護的虛擬機器群組，並藉由指定每個規則的服務設定檔來選擇這些群組的保護層級。

- **服務執行個體**：是指主機上的服務虛擬機器。vCenter 會將服務虛擬機器視為特殊虛擬機器，這些虛擬機器會在任何客體虛擬機器開啟電源之前啟動，並在所有客體虛擬機器關閉電源之後停止。每個主機的每項服務都有一個服務執行個體。

重要 服務執行個體的數目等於服務執行所在主機的數目。例如，如果一個叢集中有八個主機，而合作夥伴服務部署在兩個叢集上，則執行中的服務執行個體總數將是 16 個 SVM。

- **服務部署**：身為 admin，您可以透過 NSX-T 在個別的叢集上部署合作夥伴服務虛擬機器。部署會在叢集層級受到管理，因此當任何主機新增至叢集時，EAM 就會自動在其上部署服務虛擬機器。

自動部署 SVM 是很重要的，因為如果 vCenter 叢集上設定了 Distributed Resource Scheduler (DRS) 服務，vCenter 即可在 SVM 部署於新主機並啟動後，將現有的虛擬機器重新平衡或分配到任何已新增至叢集的新主機。由於合作夥伴服務虛擬機器需使用 NSX-T 平台為客體虛擬機器提供安全性，因此主機必須做好成為傳輸節點的準備。

重要 一個服務部署是指 vCenter Server 上的一個叢集，而此叢集會受到管理以部署和設定一個合作夥伴服務。

- **檔案自我檢查驅動程式**：安裝在客體虛擬機器上，用來攔截客體虛擬機器上的檔案活動。
- **網路自我檢查驅動程式**：安裝在客體虛擬機器上，用來攔截客體虛擬機器上的網路流量、程序和使用者的活動。

端點保護的高階工作

包含安全性掃描邏輯的第三方合作夥伴服務會登錄至 NSX-T Data Center，以進行客體虛擬機器保護。當 NSX 管理員部署已登錄的服務，並將端點保護原則套用至客體虛擬機器群組時，即會強制執行合作夥伴服務。

端點保護使用案例的 Guest Introspection 工作流程如下所示：

圖 10-2. 端點保護工作流程

工作流程工作	角色/人物	實作
將服務登錄至 NSX-T Data Center	合作夥伴管理員	合作夥伴主控台
將服務登錄至 NSX-T Data Center	合作夥伴管理員	合作夥伴主控台
將服務登錄至 NSX-T Data Center	合作夥伴管理員	合作夥伴主控台
部署服務	NSX 管理員	API 和 NSX Manager 使用者介面
檢視服務執行個體詳細資料	NSX 管理員	API 和 NSX Manager 使用者介面
啟動服務執行個體	NSX 管理員	API 和 NSX Manager 使用者介面
新增服務設定檔	NSX 管理員	API 和 NSX Manager 使用者介面
耗用 Guest Introspection 原則	NSX 管理員	API 和 NSX Manager 使用者介面
新增及發佈端點保護規則	NSX 管理員	API 和 NSX Manager 使用者介面
監控端點保護狀態	NSX 管理員	API 和 NSX Manager 使用者介面

設定端點保護

使用第三方合作夥伴安全性服務保護在 NSX-T Data Center 環境中執行的客體虛擬機器。

設定端點保護原則的高階步驟：

- 1 在客體虛擬機器上設定端點保護之前，請先確定您符合[設定端點保護的必要條件](#)。
- 2 支援的軟體。請參閱[支援的軟體](#)。
- 3 安裝適用於 Linux 虛擬機器的檔案自我檢查驅動程式。請參閱在[Linux 虛擬機器上安裝 Guest Introspection 精簡型代理程式](#)。
- 4 安裝適用於 Windows 虛擬機器的檔案自我檢查驅動程式。請參閱在[Linux 虛擬機器上安裝 Guest Introspection 精簡型代理程式](#)。
- 5 安裝適用於 Linux 虛擬機器的網路自我檢查驅動程式。請參閱[安裝 Linux 精簡型代理程式以進行網路自我檢查](#)。
- 6 建立具有 Guest Introspection 合作夥伴管理員角色的使用者。請參閱[建立具有 Guest Introspection 合作夥伴管理員角色的使用者](#)。
- 7 將合作夥伴服務登錄至 NSX-T Data Center。請參閱[合作夥伴說明文件](#)。
- 8 部署服務。請參閱[部署服務](#)。
- 9 耗用 Guest Introspection 原則。請參閱[耗用 Guest Introspection 原則](#)。
- 10 新增及發佈端點保護規則。請參閱[新增及發佈端點保護規則](#)。
- 11 監控端點保護規則。請參閱[監控端點保護狀態](#)。

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 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
```

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)
- Windows Server 2016
- Windows Server 2019

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。

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

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA
- Ubuntu 16.04.5 LTS (64 位元)
- SLES 12 GA

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

升級合作夥伴服務虛擬機器。

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 從 [合作夥伴服務] 下拉式清單中，選取要部署的服務。
- 4 按一下**部署**，然後按一下**部署服務**。
- 5 輸入服務部署名稱。
- 6 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。
- 7 在 [叢集] 欄位中，選取必須部署服務的叢集。
- 8 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**已在主機上指定**。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。

若要瞭解如何設定 EAM，請參閱 vSphere 說明文件。

- 9 在 [網路] 資料行中按一下**設定**。
- 10 將 [管理網路] 介面設定為**已在主機上指定**或 **DVPG**。
- 11 將網路類型設定為 DHCP 或靜態 IP 集區。如果將網路類型設定為靜態 IP 集區，請從可用的 IP 集區清單中選取。

- 12 在 [部署規格] 欄位中，選取以主機為基礎的部署，以在所有主機上部署服務。根據合作夥伴所登錄的服務，可將多項服務部署為單一服務虛擬機器的一部分。
- 13 在 [部署範本] 欄位中，選取已登錄的部署範本。
- 14 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	您在部署服務時輸入的名稱。
已部署至	主機的 IP 位址或 FQDN
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	<p>服務執行個體部署後，健全狀況狀態會是就緒。若要讓健全狀況狀態從就緒變成開啟，請進行必要的組態變更。請參閱啟動服務執行個體。</p> <p>當 NSX-T Data Center 成功實現下列參數後，健全狀況狀態就會從就緒變更為開啟。</p> <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 ■ 健全狀況狀態接收時間：<天、日期、時間>

後續步驟

啟動服務執行個體。請參閱[啟動服務執行個體](#)。

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狀態顯示為就緒。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[新增服務設定檔](#)。

新增服務設定檔

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 > Endpoint Protection 規則 > 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 admin 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端點保護原則。請參閱[耗用 Guest Introspection 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。將規則套用至虛擬機器群組後，保護功能便會立即開始運作。

端點保護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。

若要在虛擬機器群組上執行安全服務，您必須：

程序

- 1 定義原則和規則。
- 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。

新增及發佈端點保護規則

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 在新規則中，輸入規則名稱。
- 4 在 [選取群組] 欄位中，按一下 [編輯] 圖示。

- 5 在 [設定群組] 視窗中，從現有群組清單中選取群組，或新增群組。
 - a 若要新增群組，請按一下**新增群組**，輸入詳細資料，然後按一下**儲存**。
請參閱[新增群組](#)。
- 6 在 [群組] 資料行中，選取虛擬機器群組。
- 7 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。
 - a 若要新增服務設定檔，請按一下**新增服務設定檔**，接著輸入詳細資料，然後按一下**儲存**。
請參閱[新增服務設定檔](#)。
- 8 按一下**發佈**。

結果

端點保護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 如何執行端點保護原則](#)

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。

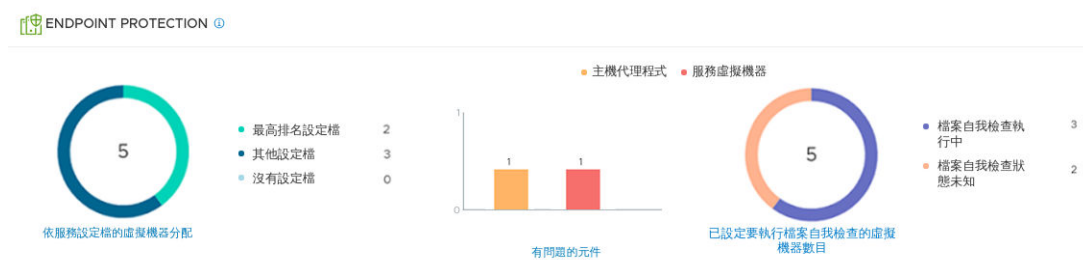
檢視端點保護的組態狀態

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[解決合作夥伴服務問題](#)。

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)	警告警告	嚴重警告
Distributed Firewall 規則	100,000	2	0%	70% 100%
系統組防火牆區段	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。

管理端點保護

解決原則衝突、服務虛擬機器的健全狀況問題，並瞭解端點保護原則的運作方式。

解決合作夥伴服務問題

合作夥伴服務虛擬機器必須正常運作，客體虛擬機器才能防範惡意程式碼。

在每台主機上，確認下列服務或程序已啟動並執行中：

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

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

確認 ESXi Agency Manager 處於線上狀態。

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

- SVM 的連接埠群組不可刪除，因為必須要有這些連接埠群組，才能確保 SVM 可繼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，然後確認 **vmervice-vshield-pg** 是否列出。
- 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。
- NSX-T Data Center 用來與合作夥伴服務主控台通訊的管理介面必須已啟動。
- 在 MUX 與 SVM 之間啟用通訊的控制介面必須已啟動。必須已建立將 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 10-10. ESXi Agency Manager 問題

問題	類別	說明	解決方案
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。這可能是因為提供 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。	ESXi Agency Manager (EAM) 服務會重試 OVF 下載作業。請查看合作夥伴管理主控台狀態。按一下 解決 。
主機版本不相容	未部署虛擬機器	代理程式虛擬機器預期會部署在主機上。但由於相容性問題，代理程式未部署在主機上。	請升級主機或解決方案，使代理程式與主機相容。檢查 SVM 的相容性。按一下 解決 。
資源不足	未部署虛擬機器	代理程式虛擬機器預期會部署在主機上。但是，ESXi Agency Manager (EAM) 服務並未部署代理程式虛擬機器，因為主機的 CPU 或記憶體資源不足。	ESXi Agency Manager (EAM) 服務會嘗試重新部署虛擬機器。請確定有 CPU 和記憶體資源可供使用。檢查主機並釋出部分資源。按一下 解決 。
空間不足	未部署虛擬機器	代理程式虛擬機器預期會部署在主機上。但是，代理程式虛擬機器並未部署，因為主機上的代理程式資料存放區沒有足夠的可用空間。	ESXi Agency Manager (EAM) 服務會嘗試重新部署虛擬機器。在資料存放區上釋出部分空間。按一下 解決 。

表 10-10. ESXi Agency Manager 問題 (續)

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。	將 customAgentVmNetwork 中列出的其中一個網路新增至主機。此問題會在資料存放區可供使用後自動解決。
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。	ESXi Agency Manager (EAM) 服務會嘗試重新部署 SVM。請查看合作夥伴解決方案說明文件或升級合作夥伴解決方案，以取得有效的 OVF 套件。按一下 解決 。
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。	定義虛擬機器網路上的 IP 位址。按一下 解決 。
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。	將 customAgentVmDatastore 中列出的其中一個資料存放區新增至主機。此問題會在資料存放區可供使用後自動解決。
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。	將主機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。此問題會在自訂虛擬機器網路可供使用後自動解決。
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。	將主機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。此問題會自動解決。
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。	將解決方案登錄至 vCenter Server。
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便會發生此情況。	按一下 解決 。ESXi Agency Manager (EAM) 服務會在代理機構組態更新之前嘗試連線主機。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將虛擬機器置於其所屬的詳細目錄中。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試重新設定正確的 OVF 內容。
虛擬機器已損毀	虛擬機器問題	代理程式虛擬機器已損毀。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試修復虛擬機器。

表 10-10. ESXi Agency Manager 問題 (續)

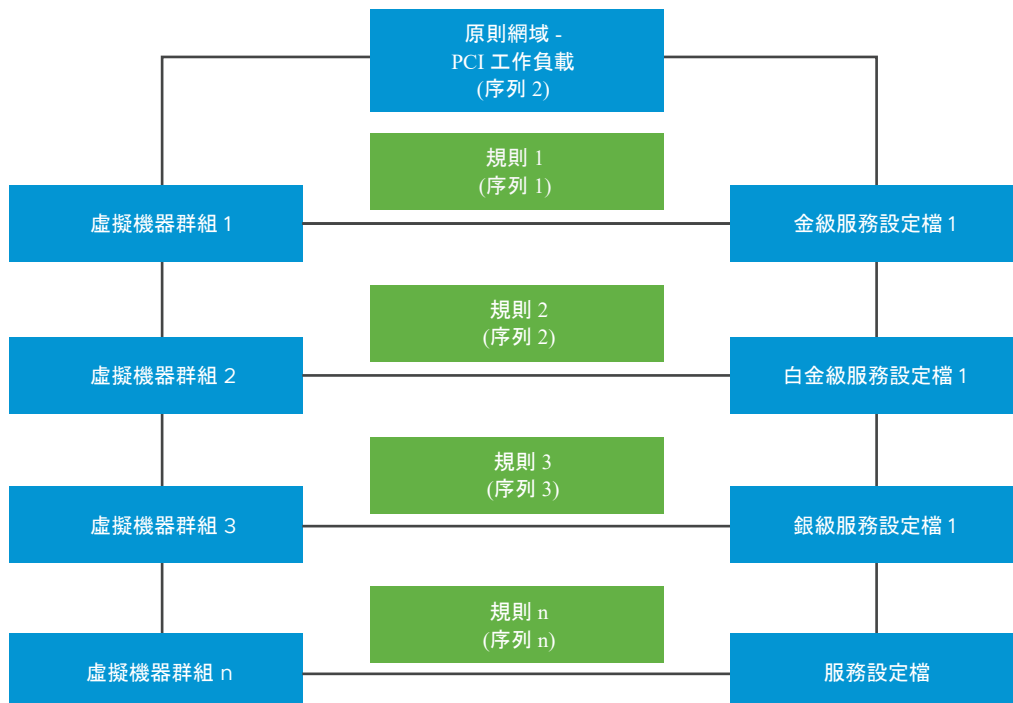
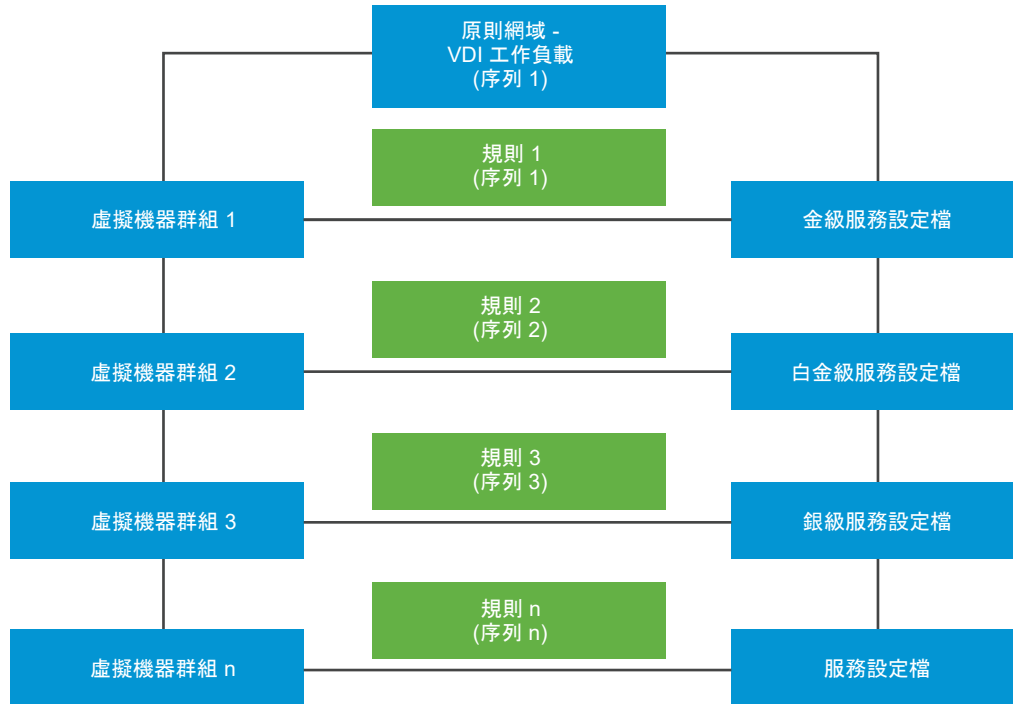
虛擬機器已孤立	虛擬機器問題	主機上存在代理程式虛擬機器，但主機不再屬於代理機構的範圍。當主機因為代理機構組態變更而中斷連線時，就會發生此情況。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將主機重新連線至代理機構組態。
虛擬機器已部署	虛擬機器問題	代理程式虛擬機器應從主機中移除，但代理程式虛擬機器尚未移除。vSphere ESX Agent Manager 無法移除代理程式虛擬機器的特定原因包括：主機處於維護模式、已關閉電源或處於待命模式。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試從主機中移除代理程式虛擬機器。
虛擬機器已關閉電源	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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試開啟虛擬機器的電源。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試關閉虛擬機器的電源。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試開啟虛擬機器的電源。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將代理程式虛擬機器置於指定的資料夾中。
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。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將代理程式虛擬機器置於指定的資源集區中。
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。	按一下 解決 以部署代理程式虛擬機器。

接著，為虛擬機器群組設定端點保護。請參閱[端點保護](#)。

Guest Introspection 如何執行端點保護原則

端點保護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。

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 10-11. 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。	<pre>GET /api/v1/service-configs</pre> <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。	<pre>POST /api/v1/service-configs</pre> <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。	<pre>DELETE /api/v1/service-configs/<config-set-id></pre> <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。	<pre>GET /api/v1/service-configs/<config-set-id></pre> <p>取得特定組態的詳細資料</p>
更新服務組態。	<pre>PUT /api/v1/service-configs/<config-set-id></pre> <p>更新服務組態。</p>
取得有效設定檔。	<pre>GET /api/v1/service-configs/effective-profiles?resource_id=<resource-id>&resource_type=<resource-type></pre> <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。

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 admin，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。

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	預期的端點保護流量	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 端點保護原則會在虛擬機器 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，端點保護不會在第二個虛擬機器群組上執行規則。	端點保護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 admin，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 解決合作夥伴服務問題。 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 解決合作夥伴服務問題。 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 解決合作夥伴服務問題。 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》。

安全性設定檔

本節包含可微調防火牆作業的設定檔：工作階段計時器、洪泛保護和 DNS 安全性

建立工作階段計時器

工作階段計時器可定義工作階段在閒置後可在防火牆上保留多久的時間。

當通訊協定的工作階段逾時到期後，工作階段即會關閉。在防火牆上，可以為 TCP、UDP 和 ICMP 工作階段指定數個逾時，以套用至使用者定義的群組或是第 0 層或第 1 層閘道。預設工作階段值可根據您的網路需求進行修改。請注意，將值設定得太低可能會導致頻繁的逾時，而將值設得太高則可能會延遲失敗偵測。

程序

- 1 導覽到 **安全性 > 設定 > 安全性設定檔 > 工作階段計時器**。
- 2 按一下**新增設定檔**。
設定檔畫面會隨即出現，並填入預設值。
- 3 輸入計時器設定檔的**名稱和說明** (選用)。
- 4 按一下**設定**，以選取要套用計時器設定檔的第 0 層或第 1 層閘道或群組。
- 5 選取通訊協定。接受預設值或輸入您自己的值。

TCP 變數	說明
First Packet	已傳送第一個封包後的連線逾時值。預設為 120 秒。
Opening	已傳輸第二個封包後的連線逾時值。預設為 30 秒。
Established	連線完全建立後的連線逾時值。
CLOSING	已傳送第一個 FIN 後的連線逾時值。預設為 120 秒。
FIN WAIT	兩個 FIN 均已交換且連線關閉後的連線逾時值。預設為 45 秒。
CLOSED	一個端點傳送 RST 後的連線逾時值。預設為 20 秒。

UDP 變數	說明
First Packet	傳送第一個封包後的連線逾時值。這是新 UDP 流量的初始逾時。預設為 60 秒。
SINGLE	在來源主機傳送了多個封包後，目的地主機未傳回封包時的連線逾時值。預設為 30 秒。
MULTIPLE	兩個主機均已傳送封包時的連線逾時值。預設為 60 秒。

ICMP 變數	說明
First Packet	傳送第一個封包後的連線逾時值。這是新 ICMP 流程的初始逾時。預設為 20 秒。
Error Reply	傳回 ICMP 錯誤以回應 ICMP 封包後的連線逾時值。預設為 10 秒。

- 6 按一下**儲存**。

後續步驟

儲存後，按一下[管理群組與設定檔的優先順序](#)以管理群組與設定檔的繫結優先順序。

預設工作階段計時器值

工作階段計時器設定檔會將逾時值套用至第 0 層或第 1 層路由器介面或包含區段的群組。逾時值會決定通訊協定工作階段在工作階段關閉後仍維持作用中狀態的時間長度。

工作階段計時器值

- API 和 UI 顯示的預設計時器設定檔僅適用於分散式防火牆 (DFW)。
- 閘道防火牆 (GFW) 預設工作階段計時器與使用 API 和 UI 時顯示的預設設定檔計時器不同。GFW 預設工作階段計時器已針對南北向流量進行最佳化，且依預設的值較低。
- 您可以使用 API 和 UI 變更 DFW 和 GFW 的 FW 工作階段計時器。

- 如有需要，相同的非預設計時器設定檔可以套用至 DFW 與 GFW。

若未自訂計時器值，閘道將會採用預設值。閘道防火牆預設計時器值：

計時器內容	Edge 預設值 (秒)	最小值 (秒)	最大值 (秒)
ICMP Error Reply	6	10	4320000
ICMP First Packet	6	10	4320000
TCP Closed	2	10	4320000
TCP Closing	900	10	4320000
TCP Established	7200	120	4320000
TCP Fin-wait	4	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	30	10	4320000
UDP Multiple	30	10	4320000
UDP Single	30	10	4320000

分散式防火牆預設工作階段計時器值：

計時器內容	DFW 預設值 (秒)	最小值 (秒)	最大值 (秒)
ICMP Error Reply	10	10	4320000
ICMP First Packet	20	10	4320000
TCP Closed	20	10	4320000
TCP Closing	120	10	4320000
TCP Established	43200	120	4320000
TCP Fin-wait	45	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	60	10	4320000
UDP Multiple	60	10	4320000
UDP Single	30	10	4320000

洪泛保護

洪泛保護有助於防範拒絕服務 (DDoS) 攻擊。

DDoS 攻擊的目的是藉由耗用掉所有可用的伺服器資源，而導致伺服器無法篩選出合法的流量 - 也就是會有大量要求湧入伺服器。建立洪泛保護設定檔，可對 ICMP、UDP 和半開 TCP 流量施加作用中工作階段限制。分散式防火牆可快取處於 SYN_SENT 和 SYN_RECEIVED 狀態的流量項目，並在收到來自啟動器的 ACK 後將每個項目升階為 TCP 狀態，而完成三向信號交換。

程序

- 1 導覽至安全性 > 安全性設定檔 > 洪泛保護。
- 2 按一下**新增設定檔**，然後選取**新增 Edge 閘道設定檔**或**新增防火牆設定檔**。
- 3 填入洪泛保護設定檔參數：

表 10-15. 防火牆和 Edge 閘道設定檔的參數

參數	最小值和最大值	預設值	
TCP 半開連線限制 - 藉由限制防火牆所允許作用中且未完整建立的 TCP 流量數目，以防止 TCP SYN 洪泛攻擊。	1-1,000,000	防火牆 - 無 Edge 閘道 - 1,000,000	設定此文字方塊可限制作用中的 TCP 半開連線數目。如果此文字方塊空白，則會在 ESX 節點上停用此限制，並設定為 Edge 閘道的預設值。
UDP 作用中流量限制 - 藉由限制防火牆所允許作用中 UDP 流量的數目，以防止 UDP 洪泛攻擊。在達到設定的 UDP 流量限制後，系統就會捨棄後續可能建立新流量的 UDP 封包。	1-1,000,000	防火牆 - 無 Edge 閘道 - 1,000,000	設定此文字方塊可限制作用中的 UDP 連線數目。如果此文字方塊空白，則會在 ESX 節點上停用此限制，並設定為 Edge 閘道的預設值。
ICMP 作用中流量限制 - 藉由限制防火牆所允許作用中 ICMP 流量的數目，防止 ICMP 洪泛攻擊。在達到設定的流量限制後，系統就會捨棄後續可能建立新流量的 ICMP 封包。	1-1,000,000	防火牆 - 無 Edge 閘道 - 10,000	設定此文字方塊可限制作用中的 ICMP 開放連線數目。如果此文字方塊空白，則會在 ESX 節點上停用此限制，並設定為 Edge 閘道的預設值。
其他作用中連線限制	1-1,000,000	防火牆 - 無 Edge 閘道 - 10,000	設定此文字方塊，可限制 ICMP、TCP 和 UDP 半開連線以外的作用中連線數目。如果此文字方塊空白，則會在 ESX 節點上停用此限制，並設定為 Edge 閘道的預設值。

表 10-15. 防火牆和 Edge 閘道設定檔的參數 (續)

參數	最小值和最大值	預設值	
SYN 快取 - 同時設定了 TCP 半開連線限制時，系統會使用 SYN 快取。系統會維護未完整建立之 TCP 工作階段的 SYN 快取，以強制執行作用中的半開連線數目。此快取會保留處於 SYN_SENT 和 SYN_RECEIVED 狀態的流量項目。收到來自啟動器的 ACK 之後，每個 SYN 快取項目都會升階為完整 TCP 狀態項目，而完成三向信號交換。		僅適用於防火牆設定檔。	切換為開啟和關閉。只有在設定了 TCP 半開連線限制時，啟用 SYN 快取才有效用。
RST 詐騙 - 從 SYN 快取清除半開狀態時，對伺服器產生詐騙的 RST。允許伺服器清理與 SYN 洪泛 (半開) 相關的狀態。		僅適用於防火牆設定檔。	切換為開啟和關閉。必須選取 SYN 快取才能使用此選項

4 若要將設定檔套用至 Edge 閘道和防火牆群組，請按一下**設定**。

5 按一下**儲存**。

後續步驟

儲存後，按一下[管理群組與設定檔的優先順序](#)以管理群組與設定檔的繫結優先順序。

設定 DNS 安全性

建立 DNS 安全性設定檔有助於防止與 DNS 有關的攻擊。

在設定 DNS 安全性設定檔後，您可以執行下列動作：

- 窺探傳輸節點上的虛擬機器或虛擬機器群組的 DNS 回應，讓 FQDN 與 IP 位址產生關聯。
- 新增全域和預設的 DNS 伺服器資訊，並將其套用至所有使用 DFW 規則的虛擬機器。
- 為選取的虛擬機器指定所選的 DNS 伺服器資訊。
- 將 DNS 設定檔套用至群組。

備註 目前的版本僅支援 ESXi。

程序

- 1 導覽到 **安全性 > 設定 > 安全性設定檔 > DNS 安全性**。
- 2 按一下**新增設定檔**。

3 輸入下列值：

選項	說明
設定檔名稱	提供設定檔名稱。
TTL	<p>此欄位會在數秒內擷取 DNS 快取項目的存留時間。您有下列選項：</p> <p>TTL 0 - 快取的項目永不到期。</p> <p>TTL 1 至 3599 - 無效</p> <p>TTL 3600 到 864000 - 有效</p> <p>TTL 保留為空白 - 自動 TTL，從 DNS 回應封包設定。</p> <p>備註 DNS 安全性設定檔的預設 DNS 快取逾時為 24 小時。</p>
套用至	<p>您可以根據任何準則來選取要套用 DNS 安全性設定檔的群組。</p> <p>備註 僅一個 DNS 伺服器設定檔會套用到虛擬機器。</p>
標籤	<p>選擇性。將標籤和範圍指派給 DNS 設定檔，使其易於搜尋。如需詳細資訊，請參閱 將標籤新增至物件。</p>

4 按一下儲存。

後續步驟

儲存後，按一下[管理群組與設定檔的優先順序](#)以管理群組與設定檔的繫結優先順序。

管理群組與設定檔的優先順序

您可以將多個群組繫結至一個安全性設定檔。NSX-T Data Center 會將安全性設定檔套用至優先順序最高的群組。

如果您將安全性設定檔繫結至多個群組，NSX-T Data Center 會將最高優先順序指派給該清單中最新的群組。但您可以變更群組的優先順序層級。

若要將優先順序指派給群組：

必要條件

- 工作階段計時器群組必須僅包含區段、區段連接埠和虛擬機器作為成員。其他類別類型不受支援。
- DNS 安全群組必須僅包含虛擬機器作為成員。其他類別類型不受支援。

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 **安全性 > 安全性設定檔**。
- 3 按一下 **管理群組與設定檔的優先順序**。
- 4 若要為群組指派最高層級的優先順序，請將其移至清單頂端。
- 5 按一下 **關閉**。

結果

安全性設定檔會套用至優先順序層級最高的群組。

您可以為 NSX-T Data Center 詳細目錄設定服務、群組、內容設定檔和虛擬機器。

當您按一下**詳細目錄**索引標籤時會出現詳細目錄物件的概觀，其中顯示詳細目錄中群組、服務、虛擬機器和內容設定檔的數目。此外也會顯示下列關於群組的資訊：

- 原則中使用的群組數目
- 原則中未使用的群組數目
- 具有成員的群組數目
- 沒有成員的群組數目
- 身分識別群組的數目
- 原則中使用的身分識別群組數目
- 原則中未使用的身分識別群組數目

本章節討論下列主題：

- **新增服務**
- **新增群組**
- **新增內容設定檔**

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，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**。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) 新增一或多個標籤。

9 (選擇性) 輸入說明。

10 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的不同物件，可以作為防火牆規則的來源和目的地。

群組可設定為包含虛擬機器、IP 集合、MAC 集合、區段連接埠、區段交換器、AD 使用者群組以及其他群組的組合。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。您無法在分散式防火牆規則的套用至欄位中使用以動態或邏輯物件為基礎的群組。

NSX 中的標籤區分大小寫，但以標籤為基礎的群組則「不區分大小寫」。例如，如果動態群組成員資格準則為 `VM Tag Equals 'quarantine'`，則該群組中會納入包含「quarantine」或「QUARANTINE」標籤的所有虛擬機器。

群組也可以從防火牆規則中排除，且清單中最多可以有 100 個群組。用於防火牆排除清單的群組中無法包含 IP 集合、MAC 集合和 AD 群組作為成員。如需詳細資訊，請參閱[管理防火牆排除清單](#)。

NSX Cloud 注意事項 如果使用 NSX Cloud，請參閱[使用 NSX-T Data Center 和公有雲標記分組虛擬機器](#)，以取得如何使用公有雲標籤在 NSX Manager 中將工作負載虛擬機器分組的資訊。

以單一識別碼為基礎的群組在分散式防火牆規則內僅能用作來源。如果需要在來源使用以 IP 和識別碼為基礎的群組，請分別建立兩個防火牆規則。

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有所變更時，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 (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：

- **區段連接埠** - 可指定標籤和選用範圍。
- **區段** - 可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。
- **IP 集合** - 可指定標籤和選用範圍。

5 (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**

6 (選擇性) 按一下**IP/MAC 位址**以新增 IP 位址和 MAC 位址做為群組成員。

支援 IPv4、IPv6 和多點傳播位址。

7 (選擇性) 按一下**AD 群組**以新增 Active Directory 群組。在身分識別防火牆的分散式防火牆規則的來源欄位中，可使用含有 Active Directory 成員的群組。群組可同時包含 AD 和計算成員。

8 (選擇性) 輸入說明和標籤。

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

內容設定檔可用來建立屬性金鑰值配對，例如第 7 層應用程式識別碼與網域名稱。內容設定檔定義完成後，即可在一或多個 Distributed Firewall 規則和閘道防火牆規則中使用。

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」。選取「應用程式識別碼」時可以有一或多個子屬性，例如 TLS_Version 和 CIPHER_SUITE。在單一內容設定檔中可同時使用應用程式識別碼和網域名稱。在同一個設定檔中可使用多個應用程式識別碼。可以使用一個具有多個子屬性的應用程式識別碼，但若是在單一設定檔中使用多個應用程式識別碼屬性，則會清除子屬性。

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。您也可以透過執行 API 呼叫 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME` 以查看 FQDN 的清單。

備註

- 閘道防火牆規則不支援在內容設定檔中使用 FQDN 屬性或其他子屬性。
- 第 0 層閘道防火牆原則不支援內容設定檔。閘道防火牆規則不支援使用 FQDN 屬性或其他子屬性。

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至第 7 層 Distributed Firewall 規則 (適用於第 7 層或網域名稱) 或閘道防火牆規則 (適用於第 7 層)。

有多個方式可監控 NSX-T 環境以及網路流量。

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
- 簡易網路管理通訊協定 (SNMP)
- 使用 vRealize Log Insight 進行系統監控
- 使用 vRealize Operations Manager 進行系統監控
- 使用 vRealize Network Insight Cloud 進行系統監控
- 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**計劃和疑難排解** > **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。
收集器組態	從下拉式功能表中選取收集器。
套用至	按一下 設定 ，然後選取要套用篩選器的群組，或建立新的群組。
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 **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。

流程式網路監控可讓網路管理員瞭解周遊網路的流量。

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 **計劃和疑難排解 > 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 輸入下列詳細資料：

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，流量仍會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%，會讓效能影響保持輕微的狀態。

設定	說明
收集器組態	從下拉式功能表中選取收集器。
套用至	選取類別：區段、區段連接埠或群組。IPFIX 設定檔會套用到選取的物件。
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。
匯出覆蓋流程	此參數將定義是否在上行和通道連接埠上進行取樣並匯出覆蓋流程。取樣中會同時包含 vNIC 流程和覆蓋流程。預設值為 已啟用 。停用時，僅會對 vNIC 流程進行取樣和匯出。
標籤	輸入標籤使搜尋更輕鬆。

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**計劃和疑難排解 > 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 僅支援覆蓋區段，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**計劃和疑難排解 > 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**來源**資料行中的**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**。

- 7 按一下**目的地**資料行中的**設定**以設定目的地。
- 8 按一下**儲存**。

簡易網路管理通訊協定 (SNMP)

您可以使用簡易網路管理通訊協定 (SNMP) 來監控您的 NSX-T Data Center 元件。安裝後，依預設不會啟動 SNMP 服務。

程序

- 1 登入 NSX Manager CLI 或 NSX Edge CLI。
- 2 執行下列命令

- 針對 SNMPv1/SNMPv2：

```
set snmp community <community-string>
start service snmp
```

community-string 的字元數上限為 64 個。

- 針對 SNMPv3

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

user_name 的字元數上限為 32 個。請確定您的密碼符合 PAM 限制。如果您想要變更預設引擎識別碼，請使用下列命令：

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

v3-engine-id 是一個長度介於 10 到 64 個字元的十六進位字串。

NSX-T Data Center 支援以 SHA1 和 AES128 作為驗證和隱私通訊協定。您也可以使用 API 呼叫來設定 SNMPv3。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。

範例：

使用 vRealize Log Insight 進行系統監控

您可以使用 Log Insight NSX-T 內容套件監控 NSX-T Data Center 環境。

此內容套件具有下列警示：

警示名稱	說明
SysCpuUsage	CPU 使用率高於 95% 且超過 10 分鐘。
SysMemUsage	記憶體使用量高於 95% 且超過 10 分鐘。
SysDiskUsage	一或多個磁碟分割的磁碟使用量高於 89% 且超過 10 分鐘。
PasswordExpiry	應用裝置使用者帳戶的密碼即將到期或已到期。
CertificateExpiry	一或多個 CA 簽署的憑證已到期。
ClusterNodeStatus	本機 Edge 叢集節點已關閉。
BackupFailure	NSX 排程的備份作業失敗。
VipLeadership	NSX 管理叢集 VIP 已關閉。
ApiRateLimit	用戶端 API 已達到設定的臨界值。
CorfuQuorumLost	叢集中的兩個節點已關閉，且遺失 corfu 仲裁。
DfwHeapMem	DFW 堆積記憶體已超過設定的臨界值。
ProcessStatus	重要處理程序狀態已變更。
ClusterFailoverStatus	SR 高可用性狀態已變更或作用中/待命服務容錯移轉。
DhcpPoolUsageOverloadedEvent	DHCP 集區已達到設定的使用量臨界值。
FabricCryptoStatus	Edge 加密 mux 驅動程式已針對失敗的 Known_Answer_Tests (KAT) 關閉。
VpnTunnelState	VPN 通道已關閉。
BfdTunnelStatus	BFD 通道狀態已變更。
RoutingBgpNeighborStatus	BGP 芳鄰狀態為關閉。
VpnL2SessionStatus	L2 VPN 工作階段已關閉。
VpnIkeSessionStatus	IKE 工作階段已關閉。

警告名稱	說明
RoutingStatus	路由 (BGP/BFD) 已關閉。
DnsForwarderStatus	DNS 轉寄站執行狀態為關閉。
TnConnDown_15min	對控制器/管理程式的傳輸節點連線已關閉，且已持續至少 15 分鐘。
TnConnDown_5min	對控制器/管理程式的傳輸節點連線已關閉，且已持續至少 5 分鐘。
ServiceDown	一或多個服務已關閉。
IpNotAvailableInPool	集區中沒有可用的 IP 或已達到設定的臨界值。
LoadBalancerError	NSX 負載平衡器服務狀態為錯誤。
LoadBalancerDown	NSX 負載平衡器服務狀態為關閉。
LoadBalancerVsDown	VS 狀態：所有集區成員已關閉。
LoadBalancerPoolDown	集區狀態：所有集區成員已關閉。
ProcessCrash	在資料路徑或其他 LB 處理程序 (如發送器等) 中，處理程序或精靈當機。

使用 vRealize Operations Manager 進行系統監控

您可以使用 vRealize Operations Manager 來監控 NSX-T Data Center 環境。

表 12-1. Management Pack for NSX-T 中的警告

警告	說明	建議
NSX-T 管理服務已失敗	在 NSX-T Data Center 主機上的管理服務未執行時觸發。	請登入 NSX-T Manager，並重新啟動失敗的管理服務。
邏輯交換器的管理狀態為未啟動	在邏輯交換器上的管理狀態為已停用時觸發。	如有需要，請登入 NSX-T 並啟用管理狀態。
Edge 節點控制器/管理程式連線未啟動	在 NSX-T Data Center 中的 Edge 節點連線狀態為關閉時觸發。	請檢查 Edge 節點與控制器叢集和管理員叢集的連線狀態，並修正中斷的連線。
Edge 主機節點處於失敗/錯誤狀態	在 NSX-T Data Center 中的主機節點因下列其中一個原因而處於錯誤或失敗狀態時觸發： <ul style="list-style-type: none"> ■ Edge 組態錯誤 ■ 安裝失敗 ■ 解除安裝失敗 ■ 升級失敗 ■ 虛擬機器部署失敗 ■ 虛擬機器關閉電源失敗 ■ 虛擬機器開啟電源失敗 ■ 虛擬機器取消部署失敗 	Edge 主機節點處於失敗/錯誤狀態，請檢查主機節點狀態並修正此問題。
BFD 服務已停用	在邏輯路由器上未啟用 BFD 服務時觸發。	即使已設定芳鄰，第 0 層路由器的 BFD 服務仍未啟用。如有需要，請啟用 BFD 服務。
未設定 NAT 規則	在邏輯路由器上的 NAT 規則未設定時觸發。	請登入 NSX-T Manager，並新增邏輯路由器的 NAT 規則。

表 12-1. Management Pack for NSX-T 中的警示 (續)

警示	說明	建議
靜態路由未設定	未設定邏輯路由器上的靜態路由時觸發。	如有必要，請登入 NSX-T Manager 並新增邏輯路由器的靜態路由。
路由通告服務已停用	在邏輯路由器上未啟用路由通告服務時觸發。	即使已設定路由通告，第 1 層路由器的路由通告服務仍未啟用。請登入 NSX-T Manager 並啟用服務。
路由重新分配服務已停用	在邏輯路由器上未啟用路由重新分配服務時觸發。	即使已設定路由重新分配規則，第 0 層路由器的路由重新分配服務仍未啟用。請登入 NSX-T Manager 並啟用服務。
邏輯路由器的 ECMP 服務已停用	在邏輯路由器上未啟用 ECMP 服務時觸發。	即使已設定芳鄰，第 0 層路由器的 BGP ECMP 服務仍未啟用，請登入 NSX-T Manager 並啟用服務。
控制器節點連線中斷	在 NSX-T Data Center 中的控制器節點連線狀態為關閉時觸發	請登入 NSX-T Manager，並檢查控制器節點與管理節點和控制器叢集的連線，然後解決中斷連線的狀態。
部署的控制器節點數少於 3 個	在 NSX-T Data Center 伺服器的控制器節點數少於 3 個時觸發。	在叢集中部署至少 3 個控制器節點。
控制器叢集狀態不穩定	在 NSX-T Data Center 中的所有控制器節點為關閉時觸發。	請檢查控制器叢集的狀態。
管理狀態不穩定	在管理叢集上任何節點的狀態為關閉時觸發。	請檢查管理叢集的狀態。
檔案系統使用量超過 85%	在控制器虛擬機器的客體檔案系統使用量超過 85% 時觸發。	檔案系統使用量超過 85，請檢查並清理檔案系統以提供更多空間。
檔案系統使用量超過 75%	在控制器虛擬機器的客體檔案系統使用量超過 75% 時觸發。	檔案系統使用量超過 75，請檢查並清理檔案系統以提供更多空間。
檔案系統使用量高於 70%	在控制器虛擬機器的客體檔案系統使用量超過 70% 時觸發。	檔案系統使用量超過 70，請檢查並清理檔案系統以提供更多空間。
Edge 叢集狀態為關閉	Edge 叢集狀態為關閉時觸發。	請檢查 Edge 叢集狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
邏輯交換器狀態為失敗	在邏輯交換器的狀態為失敗時觸發。	請檢查邏輯交換器狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
負載平衡器服務運作狀態已關閉	在負載平衡器服務的運作狀態為關閉時觸發。	請檢查負載平衡器服務的運作狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。

表 12-1. Management Pack for NSX-T 中的警示 (續)

警示	說明	建議
負載平衡器服務運作狀態錯誤	負載平衡器服務的運作狀態包含錯誤時觸發。	請檢查負載平衡器服務的運作狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
負載平衡器虛擬伺服器運作狀態為關閉	在負載平衡器虛擬伺服器的運作狀態為關閉時觸發。	請檢查負載平衡器虛擬伺服器的運作狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
負載平衡器虛擬伺服器運作狀態為中斷連結	在負載平衡器虛擬伺服器運作狀態為中斷連結時觸發。	請檢查負載平衡器虛擬伺服器的運作狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
Edge 節點組態狀態為失敗	在 Edge 節點的組態狀態為失敗時觸發。	請檢查 Edge 節點的組態狀態，並視需要遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
管理服務監控執行階段狀態為失敗	在管理服務的監控執行階段狀態為停止執行時觸發。	請登入 NSX-T Manager VA，並將失敗的管理服務重新啟動。
管理叢集的管理狀態不穩定	在管理叢集的管理狀態不穩定時觸發。	請檢查管理叢集的狀態。
部署的管理程式節點數少於 3 個	在 NSX-T 伺服器部署的管理程式節點數少於 3 個時觸發。	在叢集中部署至少 3 個管理程式節點。
管理程式節點連線中斷	在管理程式節點的管理程式連線狀態為關閉時觸發。	請登入 NSX-T Manager，並檢查管理程式節點的管理程式連線，然後遵循 NSX-T 說明文件和 VMware 說明文件建議的標準疑難排解步驟。
管理程式節點的檔案系統使用量超過 85%	在管理程式節點的客體檔案系統使用量超過 85% 時觸發。	檔案系統使用量超過 85，請檢查並清理檔案系統以提供更多空間。
管理程式節點的檔案系統使用量超過 75%	在管理程式節點的客體檔案系統使用量超過 75% 時觸發。	檔案系統使用量超過 75，請檢查並清理檔案系統以提供更多空間。
管理程式節點的檔案系統使用量超過 70%	在管理程式節點的客體檔案系統使用量超過 70% 時觸發。	檔案系統使用量超過 70，請檢查並清理檔案系統以提供更多空間。

使用 vRealize Network Insight Cloud 進行系統監控

您可以使用 vRealize Network Insight Cloud 來監控 NSX-T Data Center 環境。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	NSX-T 第 1 層邏輯路由器中斷連線事件	NSX-T 第 1 層邏輯路由器已與第 0 層路由器中斷連線。無法從外部連線至此路由器下方的網路，反之亦然。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	路由通告已停用	已為 NSX-T 第 1 層邏輯路由器停用路由通告。無法從外部連線至此路由器下方的網路。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有管理程式連線	NSX-T Edge 節點已失去管理程式連線。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge 節點的控制器連線已降級	NSX-T Edge 節點無法與一或多個控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有控制器連線	NSX-T Edge 節點無法與任何控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtuMismatchEvent	警告	NSX-T 第 0 層與上行交換器/路由器之間的 MTU 不相符	在第 0 層邏輯路由器介面設定的 MTU 與來自相同 L2 網路之上行交換器/路由器的介面不相符。這可能會影響網路效能。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	資訊	已從 NSX-T DFW 防火牆中排除一或多台虛擬機器。	一或多台虛擬機器未受 NSX-T DFW 防火牆保護。vRealize Network Insight 將不會收到這些虛擬機器的 IPFIX 流量。
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	警告	上行 VLAN 組態錯誤	通訊中斷，因為第 0 層路由器上行連接埠上的 VLAN 與外部網路上的 VLAN 不同。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	沒有任何傳輸區域已連結至傳輸節點。	沒有任何傳輸區域已連結至傳輸節點。由於此原因，虛擬機器可能會失去連線。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	傳輸節點上沒有任何可用的 VTEP。	已從傳輸節點中刪除所有 VTEP。由於此原因，虛擬機器可能會失去連線。
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	嚴重	NSX-T 控制器節點沒有控制叢集連線	NSX-T 控制器節點已失去控制叢集連線。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	嚴重	NSX-T 控制器節點沒有管理平面連線	NSX-T 控制器節點已失去管理平面連線。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	嚴重	NSX-T 管理節點沒有管理叢集連線	NSX-T 管理節點已失去管理叢集連線。
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T 主機節點沒有管理程式連線	NSX Manager 的連線狀態與主機傳輸節點之間不同步
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlrConnectivityStatusUnknownEvent	嚴重	NSX-T Edge 節點的控制器連線未知。	NSX-T Edge 節點控制器連線未知。
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlrConnectivityStatusDownEvent	警告	NSX-T 主機節點沒有控制器連線	NSX-T 主機節點無法與任何控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlrConnectivityStatusDegradedEvent	警告	NSX-T 主機節點的控制器連線已降級	NSX-T 主機節點無法與一或多個控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlrConnectivityStatusUnknownEvent	警告	NSX-T 主機節點的控制器連線未知。	NSX-T 主機節點控制器連線未知。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T 主機傳輸節點 PNIC 狀態為「關閉」。	NSX-T 主機傳輸節點 PNIC 狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T 主機傳輸節點 PNIC 狀態為「已降級」	NSX-T 主機傳輸節點 PNIC 狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T 主機傳輸節點 PNIC 狀態為「未知」。	NSX-T 主機傳輸節點 PNIC 狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	嚴重	NSX-T Edge 傳輸節點 PNIC 狀態為「關閉」。	NSX-T Edge 傳輸節點 PNIC 狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	嚴重	NSX-T Edge 傳輸節點 PNIC 狀態為「已降級」。	NSX-T Edge 傳輸節點 PNIC 狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點 PNIC 狀態為「未知」。	NSX-T Edge 傳輸節點 PNIC 狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	警告	NSX-T 主機傳輸節點通道狀態為「關閉」。	NSX-T 主機傳輸節點通道狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	警告	NSX-T 主機傳輸節點通道狀態為「已降級」。	NSX-T 主機傳輸節點通道狀態為「已降級」。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	警告	NSX-T 主機傳輸節點通道狀態為「未知」。	NSX-T 主機傳輸節點通道狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	嚴重	NSX-T Edge 傳輸節點通道狀態為「關閉」。	NSX-T Edge 傳輸節點通道狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradeEvent	嚴重	NSX-T Edge 傳輸節點通道狀態為「已降級」。	NSX-T Edge 傳輸節點通道狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點通道狀態為「未知」。	NSX-T Edge 傳輸節點通道狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	警告	NSX-T 主機傳輸節點狀態為「關閉」。	NSX-T 主機傳輸節點狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	警告	NSX-T 主機傳輸節點狀態為「已降級」。	NSX-T 主機傳輸節點狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	警告	NSX-T 主機傳輸節點狀態為「未知」。	NSX-T 主機傳輸節點狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「關閉」。	NSX-T Edge 傳輸節點狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	嚴重	NSX-T Edge 傳輸節點狀態為「已降級」。	NSX-T Edge 傳輸節點狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「未知」。	NSX-T Edge 傳輸節點狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 邏輯交換器管理狀態為「關閉」	NSX-T 邏輯交換器管理狀態為「關閉」
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	嚴重	NSX-T 邏輯連接埠運作狀態為「關閉」	NSX-T 邏輯連接埠運作狀態為「關閉」。這可能會導致連線至相同邏輯交換器的兩個虛擬介面 (VIF) 之間發生通訊失敗，例如，您無法從一台虛擬機器對另一台虛擬機器執行 Ping 動作。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	警告	NSX-T 邏輯連接埠運作狀態為「未知」	NSX-T 邏輯連接埠運作狀態為「未知」。這可能會導致連線至相同邏輯交換器的兩個虛擬介面 (VIF) 之間發生通訊失敗，例如，您無法從一台虛擬機器對另一台虛擬機器執行 Ping 動作。
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	警告	NSX-T 計算管理程式連線狀態為未啟動	NSX-T 計算管理程式連線狀態為未啟動
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackUpDisabledEvent	警告	NSX-T Manager 備份未排程。	NSX-T Manager 備份未排程
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	嚴重	NSX-T DFW 防火牆已停用。	分散式防火牆已在 NSX-T Manager 中停用
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	正在捨棄 NSX-T 邏輯連接埠收到的封包。	收到的封包已在 NSX-T 邏輯連接埠上捨棄，並且相關聯的實體可能會受到影響
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	正在捨棄 NSX-T 邏輯連接埠傳輸的封包。	傳輸的封包已在 NSX-T 邏輯連接埠上捨棄，並且相關聯的實體可能會受到影響
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	警告	正在捨棄 NSX-T 邏輯交換器收到的封包	收到的封包已在 NSX-T 邏輯交換器上捨棄，並且相關聯的實體可能會受到影響
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	警告	正在捨棄 NSX-T 邏輯交換器傳輸的封包。	傳輸的封包已在 NSX-T 邏輯交換器上捨棄，並且相關聯的實體可能會受到影響
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	正在 NSX-T 管理節點的網路介面上捨棄收到的封包	正在 NSX-T 管理節點的網路介面上捨棄收到的封包。這可能會影響與 NSX-T 管理叢集相關的網路流量。
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	嚴重	正在 NSX-T Edge 節點的網路介面上捨棄收到的封包	正在 NSX-T Edge 節點的網路介面上捨棄收到的封包。這可能會影響 Edge 叢集的網路流量。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	警告	正在 NSX-T 主機節點的網路介面上捨棄收到的封包	正在 NSX-T 主機節點的網路介面上捨棄收到的封包。這可能會影響 ESXi 主機上的網路流量。
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	警告	正在 NSX-T 管理節點的網路介面上捨棄傳輸的封包	正在 NSX-T 管理節點的網路介面上捨棄傳輸的封包。這可能會影響與 NSX-T 管理叢集相關的網路流量。
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	嚴重	正在 NSX-T Edge 節點的網路介面上捨棄傳輸的封包	正在 NSX-T Edge 節點的網路介面上捨棄傳輸的封包。這可能會影響 Edge 叢集的網路流量。
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	正在 NSX-T 主機節點的網路介面上捨棄傳輸的封包	正在 NSX-T 主機節點的網路介面上捨棄傳輸的封包。這可能會影響 ESXi 主機上的網路流量。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	警告	CM 詳細目錄服務已停止執行	CM 詳細目錄服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	警告	控制器服務已停止執行。	控制器服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	警告	資料存放區服務已停止執行。	資料存放區服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	警告	HTTP 服務已停止執行。	HTTP 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	警告	安裝升級服務已停止執行。	安裝升級服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent 服務已停止執行。	Liagent 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	警告	管理程式服務已停止執行。	管理程式服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理平面服務已停止執行。	管理服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	警告	移轉協調器服務已停止執行。	移轉協調器服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	警告	節點管理服務已停止執行。	節點管理服務狀態已轉變為已停止。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	警告	節點統計資料服務已停止執行。	節點統計資料服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	警告	訊息匯流排服務已停止執行。	訊息匯流排用戶端服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	警告	平台用戶端服務已停止執行。	平台用戶端服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	警告	升級代理程式服務已停止執行。	升級服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	警告	NTP 服務已停止執行。	NTP 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	警告	原則服務已停止執行。	原則服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	警告	搜尋服務已停止執行。	搜尋服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP 服務已停止執行。	SNMP 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	警告	SSH 服務已停止執行。	SSH 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	警告	Syslog 服務已停止執行。	Syslog 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	遙測服務已停止執行。	遙測服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	警告	UI 服務已停止執行。	UI 服務狀態已轉變為已停止。
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	嚴重	CM 詳細目錄服務已停止	NSX-T 管理節點的其中一個服務，即 CM 詳細目錄服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	嚴重	控制器服務已停止	NSX-T 管理節點的其中一個服務，即控制器服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	嚴重	資料存放區服務已停止	NSX-T 管理節點的其中一個服務，即資料存放區服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	嚴重	HTTP 服務已停止	NSX-T 管理節點的其中一個服務，即 HTTP 服務已停止執行。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	警告	安裝升級服務已停止	NSX-T 管理節點的其中一個服務，即安裝升級服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	警告	Liagent 服務已停止	NSX-T 管理節點的其中一個服務，即 LI 代理程式服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	嚴重	管理程式服務已停止	NSX-T 管理節點的其中一個服務，即管理程式服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	警告	管理平面服務已停止	NSX-T 管理節點的其中一個服務，即管理平面匯流排服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	警告	移轉協調器服務已停止	NSX-T 管理節點的其中一個服務，即移轉協調器服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEve nt	嚴重	節點管理服務已停止	NSX-T 管理節點的其中一個服務，即節點管理服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEven t	嚴重	節點統計資料服務已停止	NSX-T 管理節點的其中一個服務，即節點統計資料已停止執行。
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStat usEvent	警告	訊息匯流排服務已停止	NSX-T 管理節點的其中一個服務，即訊息匯流排服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientSta tusEvent	嚴重	平台用戶端服務已停止	NSX-T 管理節點的其中一個服務，即平台用戶端服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentSt atusEvent	警告	升級代理程式服務已停止	NSX-T 管理節點的其中一個服務，即升級代理程式服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	嚴重	NTP 服務已停止	NSX-T 管理節點的其中一個服務，即 NTP 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	嚴重	原則服務已停止	NSX-T 管理節點的其中一個服務，即原則服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	嚴重	搜尋服務已停止	NSX-T 管理節點的其中一個服務，即搜尋服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP 服務已停止	NSX-T 管理節點的其中一個服務，即 SNMP 服務已停止執行。

表 12-2. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	UI 名稱	說明
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	嚴重	SSH 服務已停止	NSX-T 管理節點的其中一個服務，即 SSH 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	嚴重	Syslog 服務已停止	NSX-T 管理節點的其中一個服務，即 Syslog 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	警告	遙測服務已停止	NSX-T 管理節點的其中一個服務，即遙測服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	嚴重	UI 服務已停止	NSX-T 管理節點的其中一個服務，即 UI 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	嚴重	叢集管理程式服務已停止	NSX-T 管理節點的其中一個服務，即叢集管理程式服務已停止執行。

NSX-T 系統事件

以下是 vRealize Network Insight 中所支援 NSX-T 2.2 至 2.5 事件的清單。所有這些 NSX-T 系統事件的物件識別碼 (OID) 為 1.3.6.1.4.1.6876.100.1.0.80203。

表 12-3. NSX-T 系統事件

事件名稱	說明
vmwNSXPlatformSysCpuUsage	管理程式和 Edge 應用裝置上的 CPU 使用率 (NSX-T 2.2)。
vmwNSXPlatformSysDiskUsage	管理程式和 Edge 應用裝置上用於 /var/log 磁碟分割的磁碟空間使用量 (NSX-T 2.2)。
vmwNSXPlatformSysMemUsage	管理程式和 Edge 應用裝置上的記憶體使用量 (NSX-T 2.2)。
vmwNSXPlatformSysConfigDiskUsage	管理程式和 Edge 應用裝置用於 /config 磁碟分割的磁碟使用量 (NSX-T 2.4)。
vmwNSXPlatformSysVarDumpDiskUsage	管理程式和 Edge 應用裝置用於 /var/dump 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysRepositoryDiskUsage	管理程式和 Edge 應用裝置用於 /repository 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysRootDiskUsage	管理程式和 Edge 應用裝置用於根磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysTmpDiskUsage	管理程式和 Edge 應用裝置用於 tmp 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysImageDiskUsage	管理程式和 Edge 應用裝置用於 /image 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP 集區超載/正常 (NSX-T 2.5)。

表 12-3. NSX-T 系統事件 (續)

事件名稱	說明
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP 集區租用配置失敗/成功 (NSX-T 2.5)。
vmwNSXPlatformPasswordExpiryStatus	管理程式的密碼到期 (NSX-T 2.4)。
vmwNSXPlatformCertificateExpiryStatus	管理程式的憑證到期 (NSX-T 2.4)。
vmwNSXRoutingBgpNeighborStatus	BGP 芳鄰狀態 (NSX-T 2.2)。
vmwNSXVpnTunnelState	VPN 通道開啟/關閉 (NSX-T 2.2)。
vmwNSXVpnL2TunnelStatus	L2 VPN 工作階段開啟/關閉 (NSX-T 2.2)。
vmwNSXVpnIkeSessionStatus	IKE 工作階段開啟/關閉 (NSX-T 2.2)。
vmwNSXDnsForwarderStatus	DNS 轉寄站狀態 (NSX-T 2.4)。
vmwNSXClusterNodeStatus	叢集節點狀態 (NSX-T 2.4)。
vmwNSXFabricCryptoStatus	Edge 加密 mux 驅動程式失敗/通過 Known_Answer_Tests (KAT) (NSX-T 2.4)。
管理程式磁碟使用率不正常	
BGP 芳鄰已關閉	BGP 芳鄰關閉時需要警示。
BGP 芳鄰已啟動	芳鄰啟動時清除警示。
儲存區使用量超過 X	儲存區超過 X 的警示 - 事件會針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機) 引發。
記憶體使用量超過 X	記憶體超過 X 的警示 - 事件會針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機) 引發。
CPU 使用率超過 X	CPU 超過 X 的警示 - 事件會針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機) 引發。

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蓋網路時加以觀察，且每個封包在通過覆蓋網路時都會受到監控，直到它抵達目的地客體虛擬機器或 Edge 上行。請注意，插入的已標記封包永遠不會真正傳送至目的地客體虛擬機器。

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。

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 覆蓋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。

如果已設定 NSX 橋接，則目的地 MAC 位址不明的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。

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蓋，但不會顯示至連結至邏輯交換器的介面。換句話說，實際上系統不會傳送封包給測試封包的預期收件者。

程序

- 1 從瀏覽器以管理員權限登入 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]。

附註：在 VMware Cloud (VMC) 環境不支援多點傳送和廣播。

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	參數
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。
ICMPv6	指定 ICMP 識別碼和序列。
ICMP	指定 ICMP 識別碼和序列。
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 僅支援覆蓋邏輯交換器，而非 VLAN 邏輯交換器。

NSX Cloud 附註 若使用 NSX Cloud，請參閱 [NSX-T Data Center 功能支援 NSX Cloud](#) 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。
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 [NSX-T Data Center 功能支援 NSX Cloud](#) 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。
匯出覆蓋流程	控制範例結果是否包含覆蓋流程資訊的設定。
取樣機率 (%)	將會取樣的封包百分比 (近似值)。增加此設定可能會影響 Hypervisor 和收集器的效能。如果所有 Hypervisor 正在傳送更多 IPFIX 封包給收集器，則收集器可能無法收集所有封包。將機率設定為預設值 0.1%，將會讓效能影響保持輕微的狀態。
觀察網域識別碼	觀察網域識別碼可識別網路流量源自哪個觀察網域。輸入 0 表示沒有特定觀察網域。
收集器設定檔	選取您在上一個步驟中所設定的交換器 IPFIX 收集器。
優先順序	此參數可解決套用多個設定檔時產生的衝突。IPFIX 匯出工具僅會使用具有最高優先順序的設定檔。較低的值表示較高的優先順序。

5 按一下**新增**。

設定防火牆 IPFIX 收集器

您可以設定防火牆的 IPFIX 收集器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 工具 > IPFIX**
- 3 按一下**防火牆 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**進階網路與安全性 > 工具 > IPFIX**。
- 3 按一下**防火牆 IPFIX 設定檔索引標籤**。
- 4 按一下**新增**以新增設定檔。

設定	說明
名稱與說明	輸入名稱和 (選用) 說明。 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

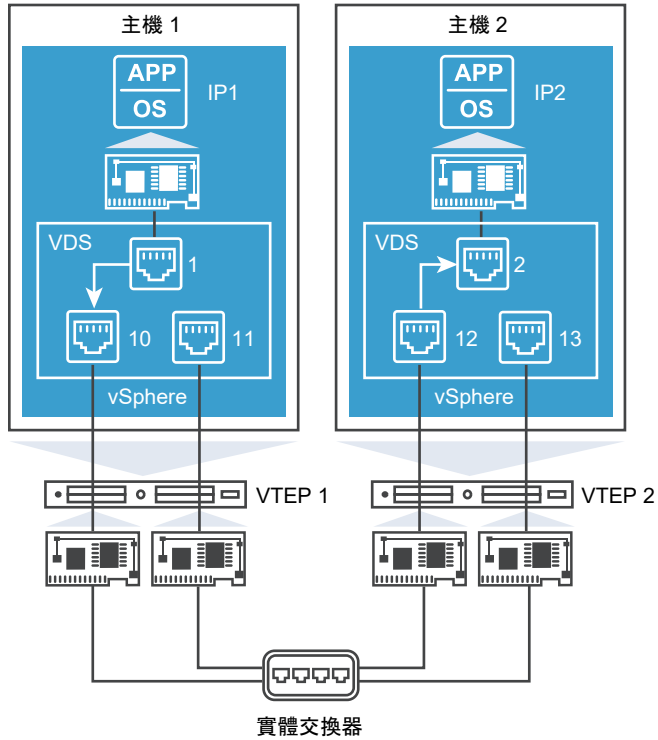
下表列出分散式防火牆 IPFIX 封包中的 VMware 特定元素。

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
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

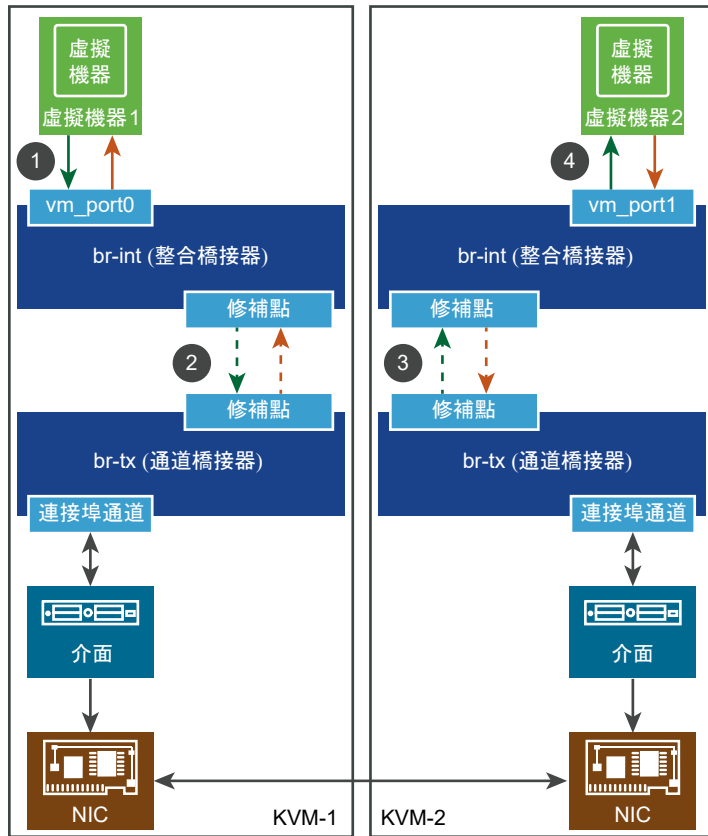
一個 KVM 主機傳輸節點支援 88 個 IPFIX 流程範本和一個選項範本。

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

元素識別碼	參數名稱	資料類型	單位
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](#)。

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。

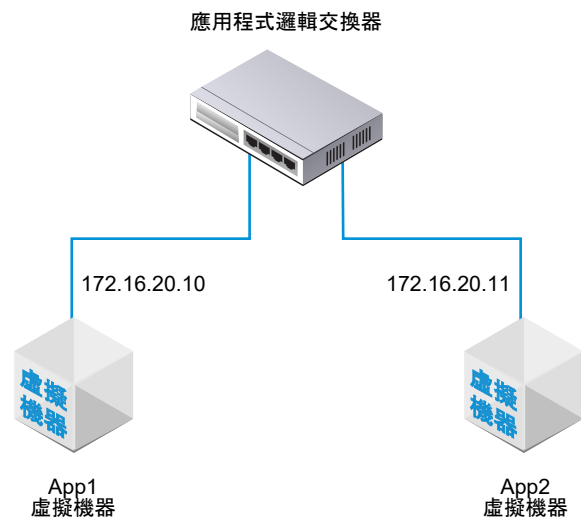
備註 如果您使用**進階網路與安全性**使用者介面來修改在原則介面中建立的物件，則某些設定可能會變為無法設定的狀態。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 **NSX Manager 概觀**。

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要建置的拓撲。

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 [NSX-T Data Center 功能支援 NSX Cloud](#) 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](#)
- [進階網路堆疊](#)
- [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

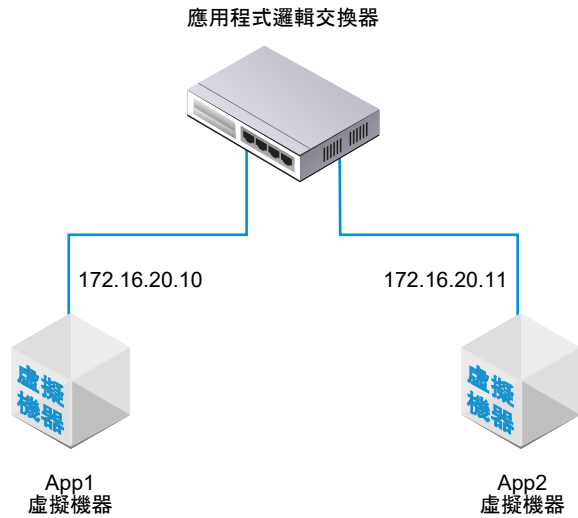
視主機而定，用來將虛擬機器連線到邏輯交換器的組態可能會有所不同。

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和 VIF 連結識別碼。

使用 GET `https://<mgr-ip>/api/v1/logical-ports/` API 呼叫來檢視對應的 VIF 連結識別碼的連接埠詳細資料和管理狀態。若要檢視運作狀態，請搭配適當的邏輯連接埠識別碼使用 `https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status` API 呼叫。

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〉。

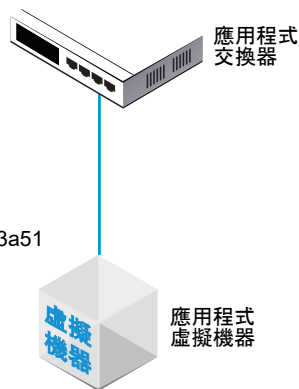
將裝載在獨立 ESXi 上的虛擬機器連結到 NSX-T Data Center 邏輯交換器

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": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fe7-08c5-5bf7-ea26a4c6b18d"
  ],
}
```

```

    "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "type": "REGULAR",
    "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
    "local_id_on_host": "5"
  }

```

3 關閉虛擬機器的電源並從主機解除登錄虛擬機器。

您可以使用虛擬機器管理工具或 ESXi CLI，如此處所示。

```

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

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

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

```

4 從 NSX Manager UI 取得邏輯交換器識別碼。

例如：

app-switch

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

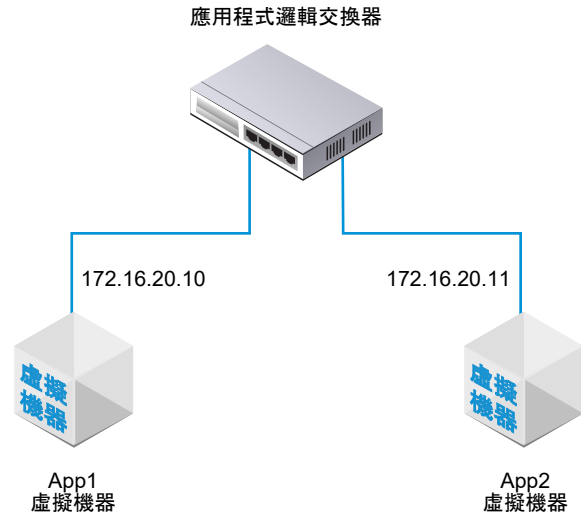
新增邏輯路由器。

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。

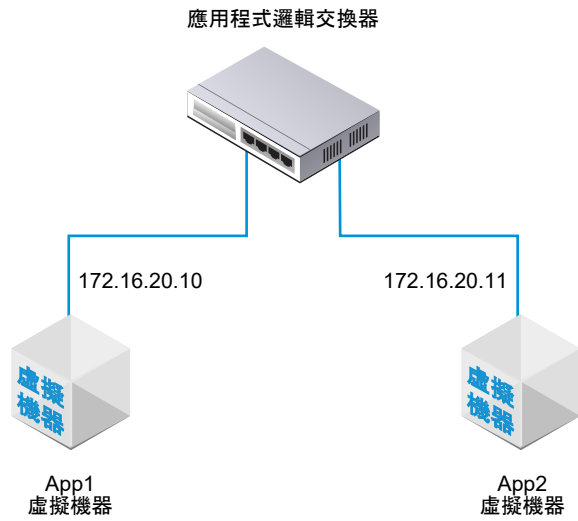
- 4 (選擇性) 在**交換設定檔索引標籤**中，選取交換設定檔。
- 5 按一下**儲存**。

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
<code>get logical-switch <vni-or-uuid> arp-table</code>	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>
<code>get logical-switch <vni-or-uuid> connection-table</code>	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>
<code>get logical-switch <vni-or-uuid> mac-table</code>	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>
<code>get logical-switch <vni-or-uuid> stats</code>	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>
<code>get logical-switch <vni-or-uuid> stats-sample</code>	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>
<pre>get logical-switch <vni-or-uuid> vtep</pre>	<p>顯示與指定邏輯交換器相關的所有虛擬通道端點。</p> <p>輸出範例。</p> <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>

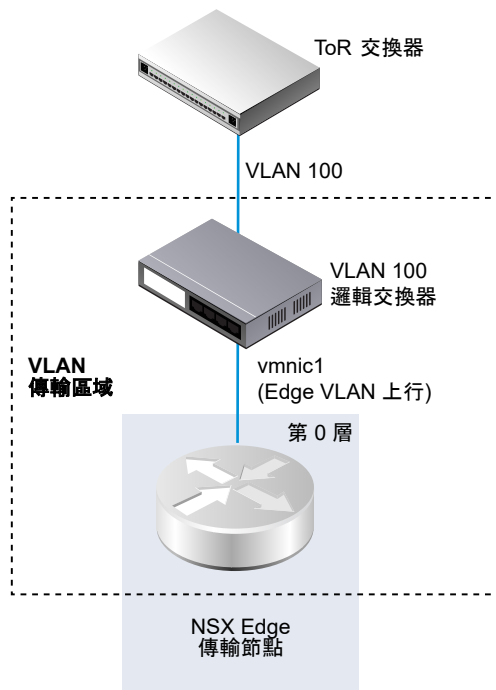
結果

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。以覆蓋為基礎的邏輯連接埠上支援信任模式。預設值為 0。</p> <p>以覆蓋為基礎及以 VLAN 為基礎的邏輯連接埠上支援未受信任模式。針對以覆蓋為基礎的邏輯連接埠，輸出 IP 標頭的 DSCP 值會設為與邏輯連接埠內部封包類型無關的設定值。針對以 VLAN 為基礎的邏輯連接埠，IP/IPv6 封包的 DSCP 值會設為設定值。未受信任模式的 DSCP 值範圍介於 0 至 63 之間。</p> <p>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。

建議僅將連接埠鏡像用於疑難排解。

備註 不建議將連接埠鏡像用於監控，因為長時間使用會影響效能。

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。
封包截斷	選擇性。範圍是 60 - 65535。

選項	說明
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。如果藉由將已實現繫結清單上的 IP 新增至略過繫結清單或停用窺探來移除此 IP，則具有最舊時間戳記的重複 IP 將會移至已實現繫結清單中。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。

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。導覽至**進階網路與安全性 > 交換 > 連接埠**並選取連接埠，即可將探索到的繫結新增至略過繫結清單。您也可以將目前探索到的繫結或實現的繫結複製到**略過繫結**，以刪除該繫結。

備註 TOFU 與 SpoofGuard 不同，它不會以 SpoofGuard 使用的相同方式封鎖流量。如需詳細資訊，請參閱[瞭解 SpoofGuard 區段設定檔](#)。

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 竊探	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。允許的最小值為 1 (預設值)，上限為 256。
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 竊探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP V6 竊探	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。
芳鄰探索竊探	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 竊探。
重複的 IP 偵測	適用於所有竊探方法及 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，可用來防止環境中虛擬機器更改其現有的 IP 位址。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 鄰探 (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 允許清單。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 允許清單。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 > 手動繫結**。
- 4 按一下**新增**。
[新增位址繫結] 對話方塊隨即顯示。

- 5 指定要套用位址繫結之邏輯連接埠的 IP (IPv4 位址、IPv6 位址或 IPv6 子網路) 和 MAC 位址。以 IPv6 為例，2001::/64 是 IPv6 子網路，2001::1 是主機 IP，而 2001::1/64 是無效輸入。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〉。

進階網路堆疊

增強型資料路徑是網路堆疊模式，一旦設定，便可提供卓越的網路效能。它主要針對 NFV 工作負載，這需要此模式提供的效能優勢。

只能在 ESXi 主機上以增強型資料路徑模式設定 N-VDS 交換器。ENS 還支援流經 Edge 虛擬機器的流量。在增強型資料路徑模式中，您可以設定覆疊流量和 VLAN 流量。

自動指派 ENS 邏輯核心

自動將邏輯核心指派給 vNIC，讓專用邏輯核心管理 vNIC 的傳入流量與傳出流量。

在增強型資料路徑模式中設定 N-VDS 交換器時，如果單一邏輯核心與 vNIC 相關聯，該邏輯核心就會處理進出於 vNIC 的雙向流量。設定了多個邏輯核心時，主機會自動判斷必須由哪個邏輯核心來處理 vNIC 的流量。

請根據其中一個參數將邏輯核心指派給 vNIC。

- vNIC 計數：主機會假設在傳輸一個 vNIC 方向的傳入或傳出流量時，所需的 CPU 資源數量是相同的。系統會根據邏輯核心的可用集區，為每個邏輯核心指派相同數目的 vNIC。這是預設模式。vNIC 計數模式很可靠，但對非對稱流量而言並非最佳選項。
- CPU 使用率：主機會預測 CPU 使用率，以使用內部統計資料傳輸每個 vNIC 方向的傳入或傳出流量。根據 CPU 的使用率來傳輸流量時，主機會變更邏輯核心指派，以平衡邏輯核心之間的負載。CPU 使用率模式比 vNIC 計數更理想，但流量不穩定時並不可靠。

在 CPU 使用率模式中，如果傳輸的流量經常變更，則預期的所需 CPU 資源和 vNIC 指派也可能經常變更。太過頻繁的指派變更可能會導致封包遭到捨棄。

如果 vNIC 之間的流量模式是對稱式，則 vNIC 計數選項將可提供可靠的行為，表示較不會頻繁變更。但是，如果流量模式是非對稱，則 vNIC 計數可能會導致封包遭到捨棄，因為它不會區分 vNIC 之間的流量差異。

在 vNIC 計數模式中，建議您設定適當數目的邏輯核心，以將每個邏輯核心指派給相同數目的 vNIC。如果與每個邏輯核心相關聯的 vNIC 數目不同，則會有 CPU 指派不公平，且效能不確定的狀況。

當 vNIC 連線或中斷連線，或在新增或移除邏輯核心時，主機會自動偵測變更並重新平衡。

程序

- ◆ 若要從一種模式切換到另一種模式，請執行下列命令。

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

其中，*<ens-lc-mode>* 可以設定為 **vNIC-count** 或 **cpu-usage** 模式。

vNIC 計數是以 vNIC/方向計數為基礎的邏輯核心指派。

cpu-usage 則是以 CPU 使用率為基礎的邏輯核心指派。

設定客體 VLAN 間路由

在覆疊網路上，NSX-T 支援在 L3 網域上路由 VLAN 間流量。在路由期間，虛擬分散式路由器 (VDR) 會使用 VLAN 識別碼來路由 VLAN 子網路之間的封包。

VLAN 間路由克服了每個虛擬機器只能使用 10 個 vNIC 的限制。NSX-T 支援 VLAN 間路由，可確保能夠在 vNIC 上建立多個 VLAN 子介面，並且用於不同的網路服務。例如，虛擬機器的一個 vNIC 可分割為多個子介面。每個子介面分別屬於一個子網路，可主控 SNMP 或 DHCP 等網路服務。例如，使用 VLAN 間路由時，VLAN-10 上的子介面可連線到 VLAN-10 或任何其他 VLAN 上的子介面。

虛擬機器上的每個 vNIC 都會透過負責管理未標記封包的父系邏輯連接埠連線至 N-VDS。

若要建立子介面，請在增強型 N-VDS 交換器上，使用 API 與相關聯的 VIF 透過程序中說明的 API 呼叫來建立子系連接埠。以 VLAN 識別碼標記的子介面會與新的邏輯交換器相關聯，例如，VLAN10 會連結至邏輯交換器 LS-VLAN-10。VLAN10 的所有子介面都必須連結至 LS-VLAN-10。子介面的 VLAN 識別碼及其相關聯的邏輯交換器之間的這種 1 對 1 對應，是一項重要的必要條件。例如，若將 VLAN20 的子系連接埠新增至對應於 VLAN-10 的邏輯交換器 LS-VLAN-10，將會使 VLAN 之間的封包路由無法運作。這類組態錯誤會導致 VLAN 間路由無法運作。

必要條件

- 將 VLAN 子介面關聯至邏輯交換器之前，請確定邏輯交換器與其他 VLAN 子介面之間沒有任何其他關聯。如果有不相符的狀況，覆疊網路上的 VLAN 間路由可能無法運作。
- 確定主機執行 ESXi v 6.7 U2 或更新版本。

程序

- 1 若要為 vNIC 建立子介面，請確定 vNIC 已更新至父系連接埠。請進行下列 REST API 呼叫。

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
```

```

"context" : {
  "resource_type" : "VifAttachmentContext",
  "vif_type": "PARENT"
},
"id" : "<Attachment UUID of the vNIC>"
},
"admin_state" : "UP",
"logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
"_revision" : 0
}

```

- 2 若要在與虛擬機器上的子介面相關聯的 N-VDS 上建立父系 vNIC 連接埠的子連接埠，請進行 API 呼叫。在進行 API 呼叫前，請先確認有邏輯交換器存在，以將子連接埠與虛擬機器上的子介面連線。

```

POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be
unique.
      "vif_type" : "CHILD"
    },
    "id" : "<ID of the CHILD port>"
  },

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}

```

結果

NSX-T Data Center 會在虛擬機器上建立子介面。

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 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。

建立 Edge 橋接器設定檔時，如果您將容錯移轉模式設定為先佔式並發生容錯移轉，待命節點會變成作用中節點。復原失敗的節點後，它會再次變成作用中節點。如果您將容錯移轉模式設定為非先佔式並發生容錯移轉，待命節點會變成作用中節點。復原失敗的節點後，它會變成待命節點。您可以透過在待命 Edge 節點上執行 CLI 命令 `set l2bridge-port <uuid> state active`，手動將待命 Edge 節點設定為作用中節點。該命令僅能在非先佔式模式下套用。否則會出現錯誤。在非先佔式模式中，在待命節點上套用時，此命令將觸發 HA 容錯移轉，在作用中節點上套用時將遭忽略。如需詳細資訊，請參閱《NSX-T Data Center 命令列介面參考》。

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

- 針對您要設定為接收連接埠的主幹 vNIC，擷取連接埠號碼。
 - 登入 vSphere Web Client，然後導覽至首頁 > 網路。
 - 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。
- 擷取 vSphere Distributed Switch 的 dvsUuid 值。
 - 在 <https://<vc-ip>/mob> 上登入 vCenter Mob UI。
 - 按一下**內容**。
 - 按一下與 **rootFolder** 相關聯的連結 (例如：*group-d1 (Datacenters)*)。
 - 按一下與 **childEntity** 相關聯的連結 (例如：*datacenter-1*)。
 - 按一下與 **networkFolder** 相關聯的連結 (例如：*group-n6*)。
 - 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)*)。
 - 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。
- 確認用來指定連接埠的不透明資料是否存在。
 - 移至 <https://<vc-ip>/mob/?moid=DVSManager&vmodl=1>。
 - 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=DVSManager&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="vmobl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=</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
```

[illegible]

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="vmobl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    </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，您可以設定橋接器支援的邏輯交換器，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

- 確認您有 Edge 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。
- 覆蓋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** > **Edge 橋接器設定檔**。
- 5 按一下**連結**。

6 若要連結至 Edge 橋接器設定檔：

- a 選取 Edge 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**。

7 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 Edge 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：

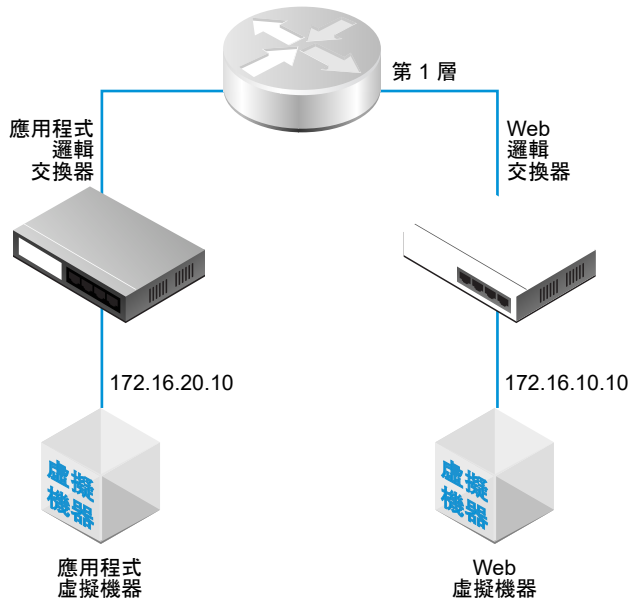
- [第 1 層邏輯路由器](#)
- [第 0 層邏輯路由器](#)

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)。您必須在處於作用中/待命模式的第 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 在處於作用中/待命模式的第 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。

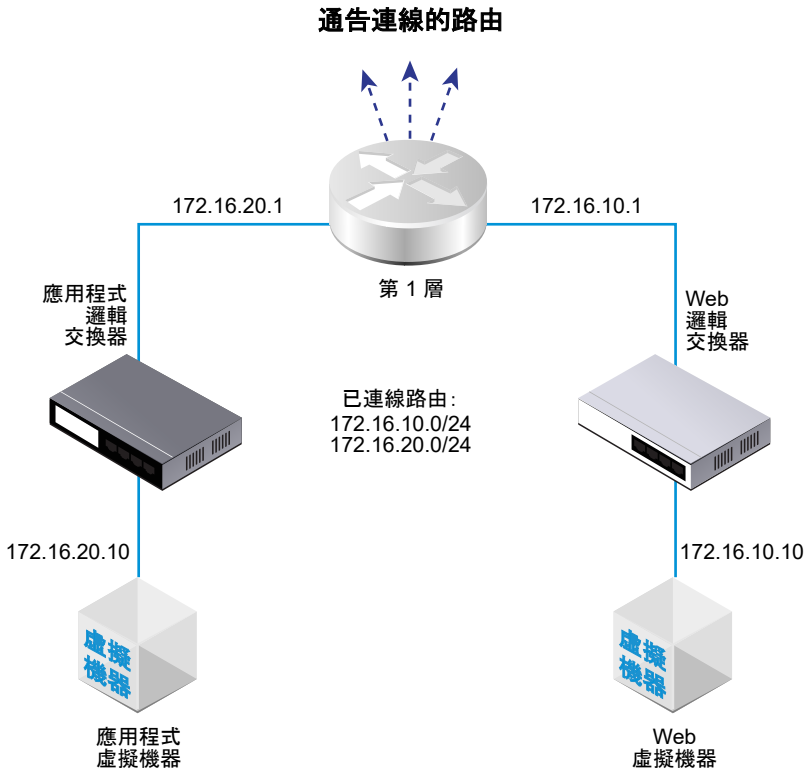
程序

- 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](#)。

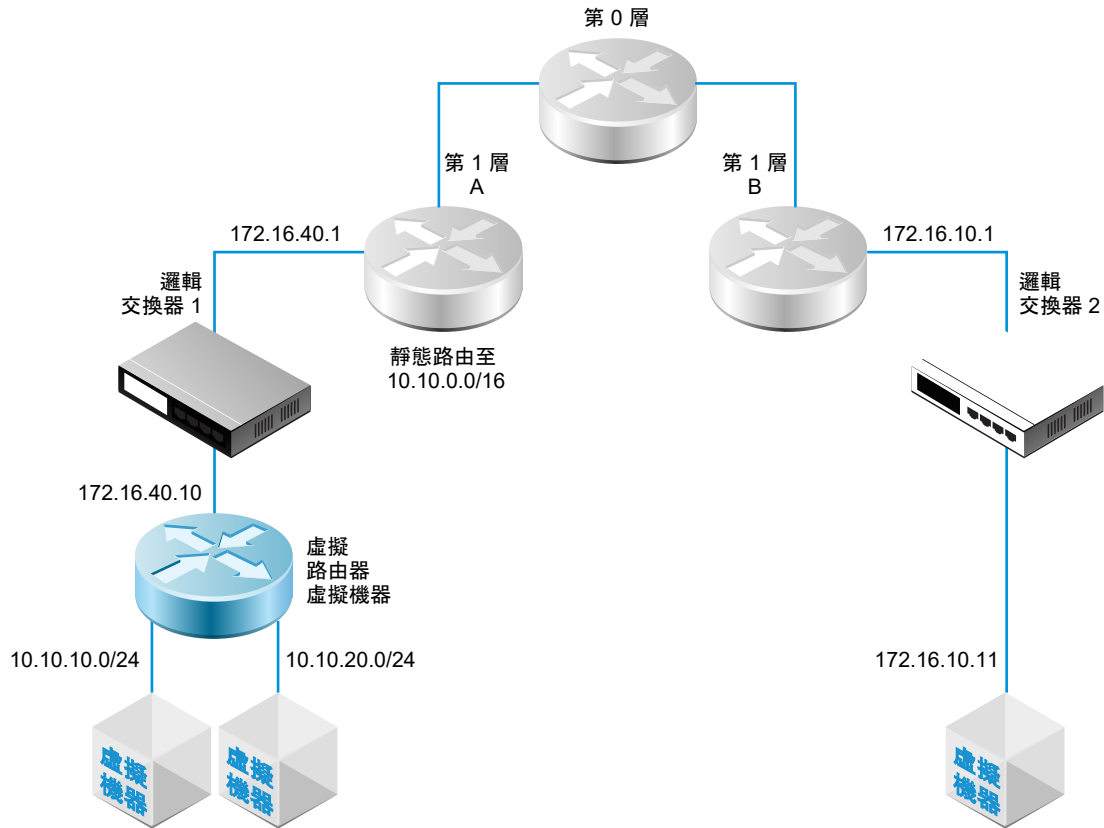
如果您已經有連線至第 1 層邏輯路由器的第 0 層邏輯路由器，則可以確認第 0 層路由器學習連線第 1 層路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

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 覆蓋進行傳播。

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)。
- 可以連線至覆蓋邏輯交換器或 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

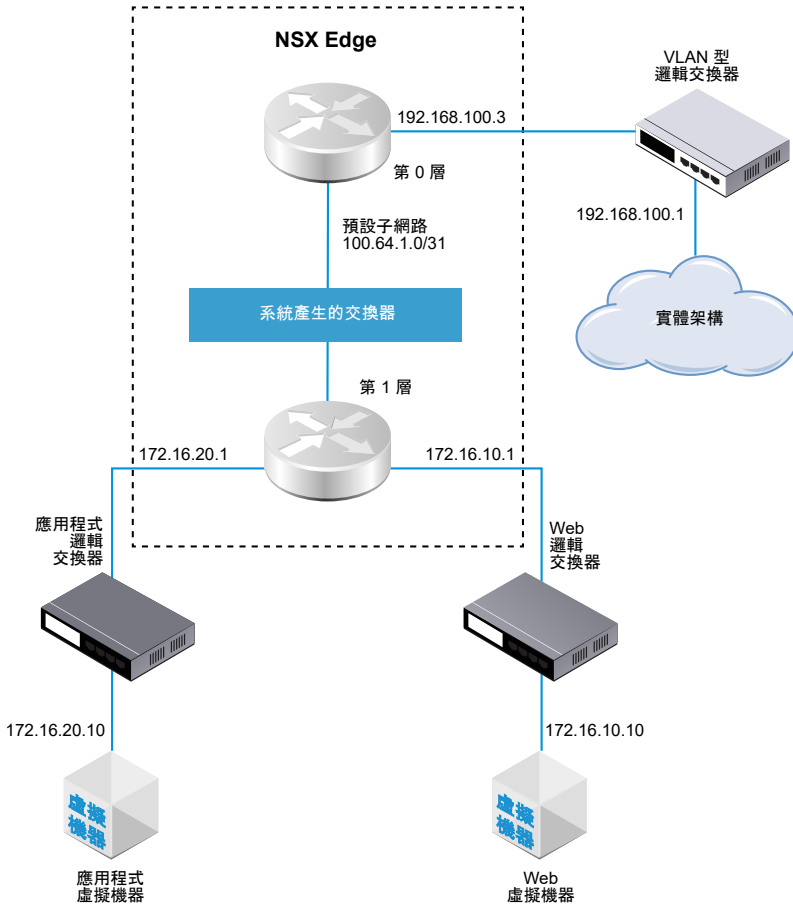
第 0 層邏輯路由器會在邏輯和實體網路之間提供閘道服務。

NSX Cloud 附註 若使用 NSX Cloud，請參閱 [NSX-T Data Center 功能支援 NSX Cloud](#) 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)。您必須在處於作用中/待命模式的第 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 在處於作用中/待命模式的第 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。

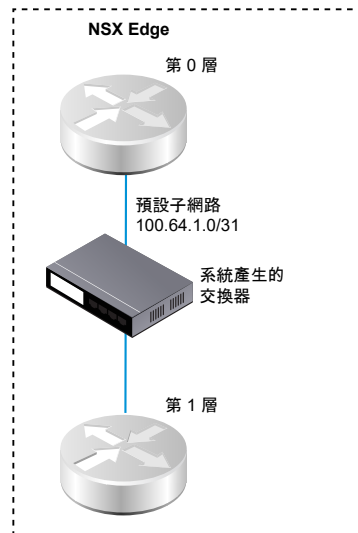
設定第 0 層邏輯路由器，將其連線至 VLAN 邏輯交換器以建立對外部網路的上行連接埠。請參閱[針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器](#)。

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

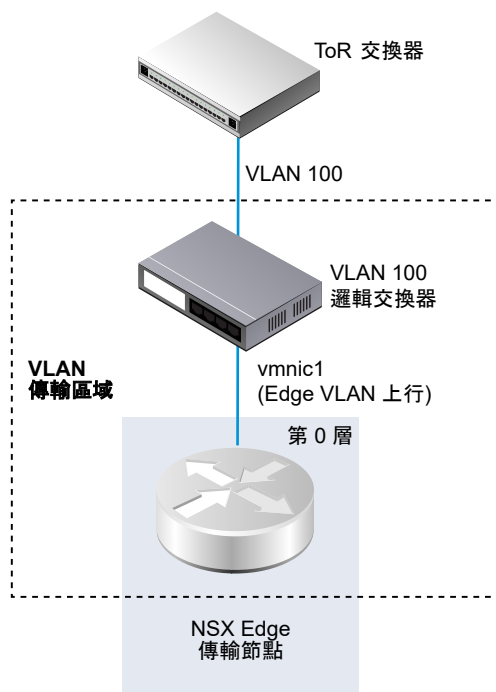
Total number of routes: 7

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[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 BGP](#)。

新增回送路由器連接埠

您可以將回送連接埠新增至第 0 層邏輯路由器。

回送連接埠可用於下列目的：

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

程序

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

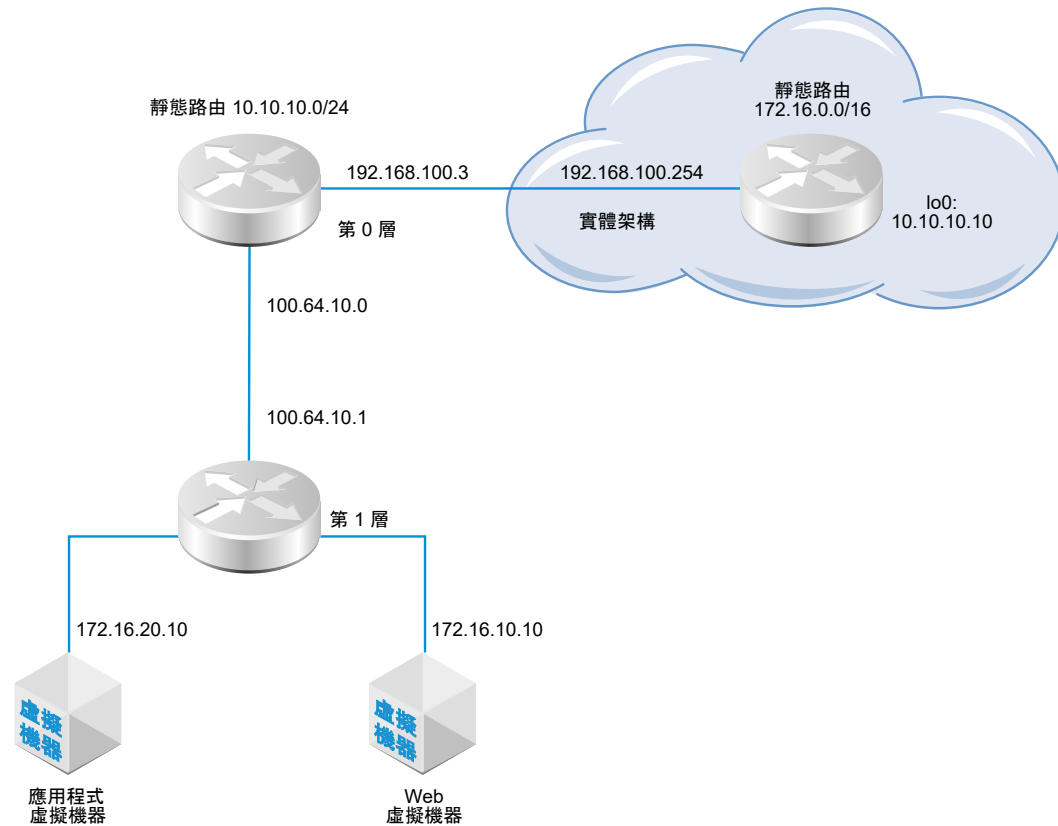
- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**進階網路與安全性 > 網路 > 路由器**。
- 3 按一下路由器的名稱。
- 4 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 5 按一下**新增**。
- 6 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 7 在**類型**欄位中，選取**集中式**。
- 8 對於 **URPF 模式**，請選取**嚴格或無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- 9 (必要) 選取邏輯交換器。
- 10 選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。

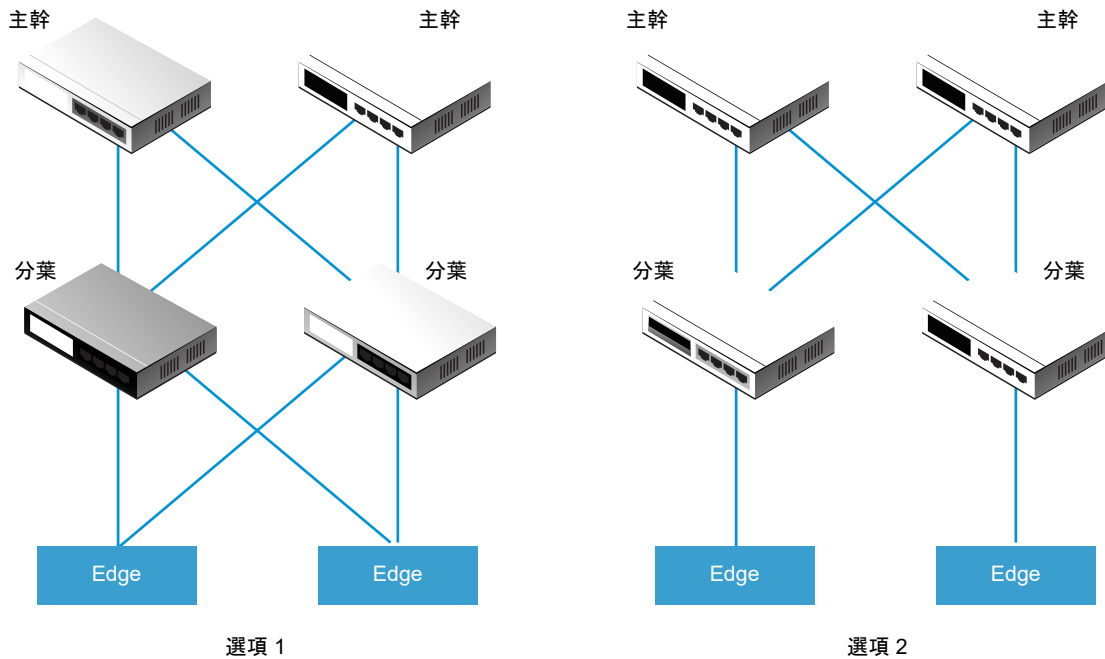
```
ping 10.10.10.10
```

```
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 BGP

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。

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。

當您在設定 BGP 時，必須設定第 0 層邏輯路由器的本機自發系統 (AS) 數目。例如，下列拓撲顯示本機 AS 數目為 64510。您也必須設定遠端 AS 數目。EBGP 芳鄰必須直接連線，且位於與第 0 層上行相同的子網路中。如果它們不在相同的子網路中，則應使用 BGP 多重躍點。

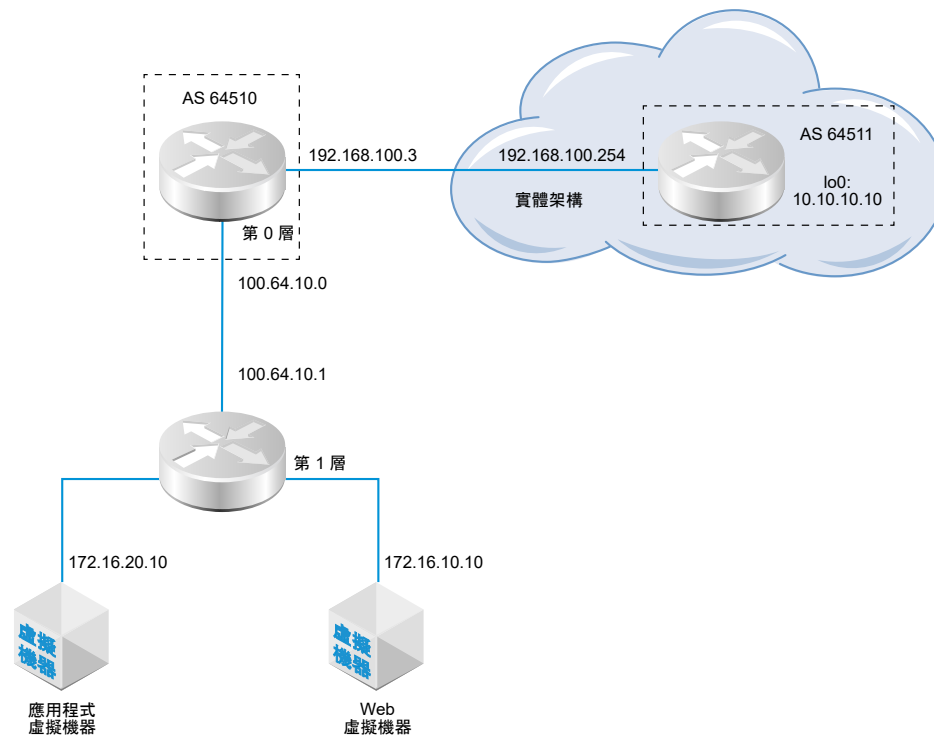
雙主動模式的第 0 層邏輯路由器支援 SR (服務路由器) 間的路由。在雙主動叢集中，如果 1 號路由器無法與南北向實體路由器進行通訊，流量就會重新路由至 2 號路由器。如果 2 號路由器能夠與該實體路由器進行通訊，則 1 號路由器與實體路由器之間的流量不受影響。

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 (eBGP 芳鄰) 或 64510 (iBGP 芳鄰)。

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](#)。

確認來自第 0 層服務路由器的 BGP 連線

從第 0 層服務路由器中使用 CLI 來確認 BGP 已連線通往芳鄰。

必要條件

確認已設定 BGP。請參閱[在第 0 層邏輯路由器上設定 BGP](#)。

程序

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

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbfeb2786666
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 BGP](#)。
- 確認 NSX-T Data Center 靜態路由已針對重新分配進行設定。請參閱[啟用第 0 層邏輯路由器上的路由重新分配](#)。

程序

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

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

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

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

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

a 列出 BGP 路由。

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

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

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

```
ping 172.16.10.10
```

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

c 檢查經過 NSX-T Data Center 覆疊的路徑。

```
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

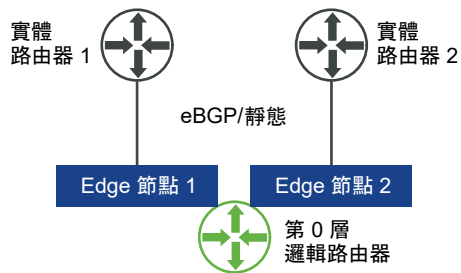
設定其他路由功能，例如 ECMP。

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作用中/作用中模式，ECMP 才可供使用。最多支援八個 ECMP 路徑。NSX Edge 上的 ECMP 實作是以通訊協定號碼、來源位址、目的地位址、來源連接埠與目的地連接埠的 5 元組為基礎。用於在 ECMP 路徑之間散佈資料的演算法不是循環配置資源。因此，某些路徑可能會比其他路徑傳送更多的流量。請注意，如果通訊協定為 IPv6 且 IPv6 標頭有多個延伸標頭，則 ECMP 將僅以來源和目的地位址為基礎。

圖 14-6. ECMP 路由拓撲



例如，上方的拓撲顯示處於作用中/作用中模式、在雙節點 NSX Edge 叢集上執行的單一第 0 層邏輯路由器。設定了兩個上行連接埠，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

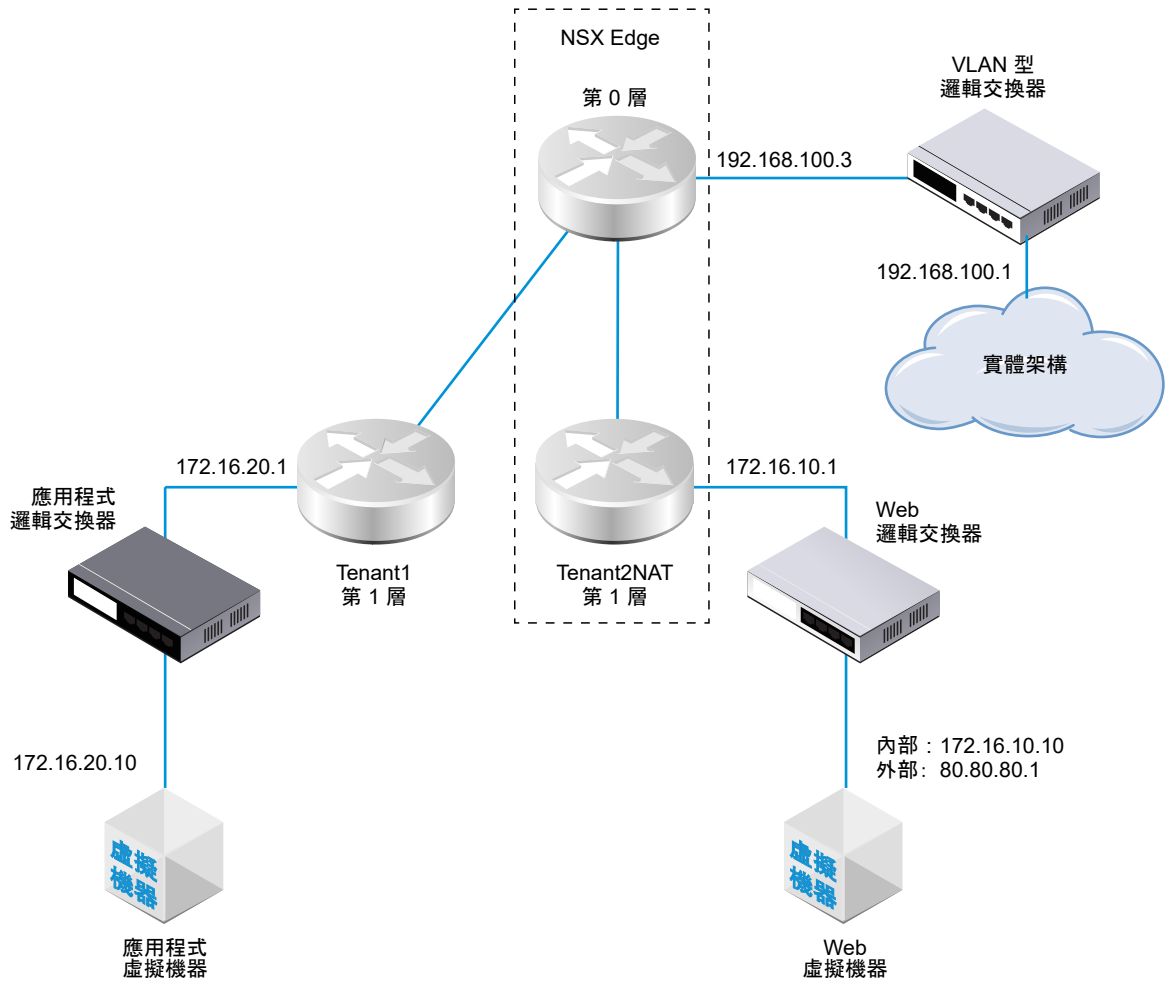
NSX-T Data Center 中的網路位址轉譯 (NAT) 可在第 0 層和第 1 層邏輯路由器中設定。

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。

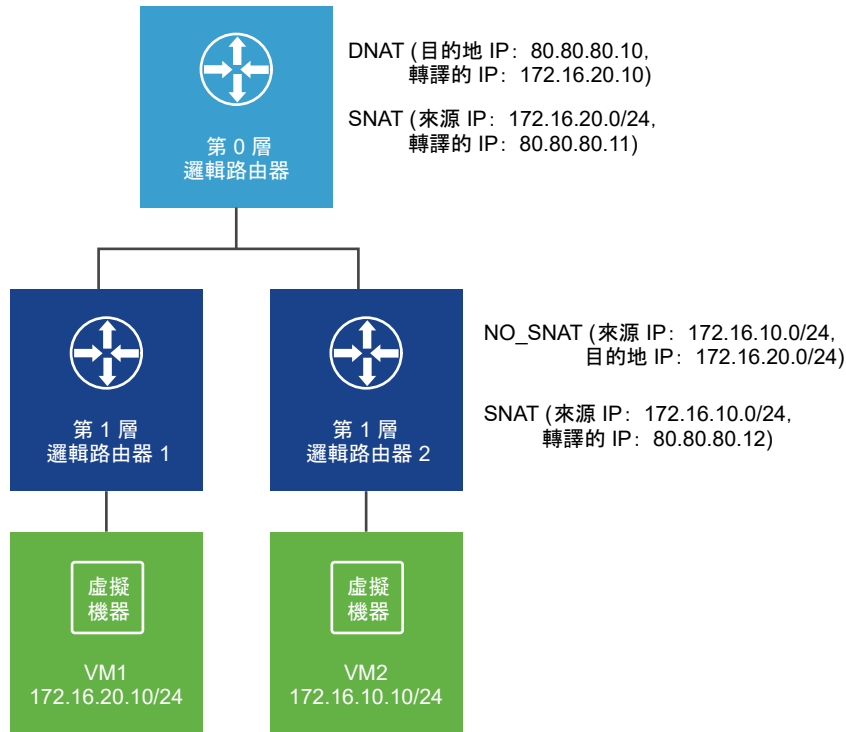
NAT 會在 Tenant2NAT 邏輯路由器對第 0 層邏輯路由器的連線上行強制執行。

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



附註：在下列情況下，NAT 迴轉傳輸不受支援。第 0 層邏輯路由器已設定 DNAT 和 SNAT。第 1 層邏輯路由器 2 已設定 NO_SNAT 和 SNAT。VM2 將無法使用 VM1 的外部位址 80.80.80.10 存取 VM1。



以下幾節說明如何使用管理程式 UI 建立 NAT 規則。您也可以進行 API 呼叫 (POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple) 以同時建立多個 NAT 規則。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。

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 BGP](#) 和 [啟用第 0 層邏輯路由器上的路由重新分配](#)。
- 第 1 層路由器必須各自設定連往第 0 層路由器的上行。Tenant2NAT 必須受 NSX Edge 叢集支援。請參閱[連結第 0 層和第 1 層](#)。

- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱[在第 1 層邏輯路由器上新增下行連接埠與在第 1 層邏輯路由器上設定路由通告](#)。
- 虛擬機器必須連結至正確的邏輯交換器。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**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**套用到**，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		
優先順序: 1024									
1036	SNAT	任何	172.16.10.10	任何	任何	任何	80.80.80.1	任何	

後續步驟

設定第 1 層路由器以通告 NAT 路由器。

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

在第 1 層路由器上設定目的地 NAT

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

您可以建立規則來啟用或停用目的地 NAT。

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

必要條件

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

程序

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

作用中/待命模式下的第 0 層邏輯路由器支援來源 NAT (SNAT)、目的地 NAT (DNAT) 和自反 NAT。作用中/作用中式模式下的第 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**套用到**，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。

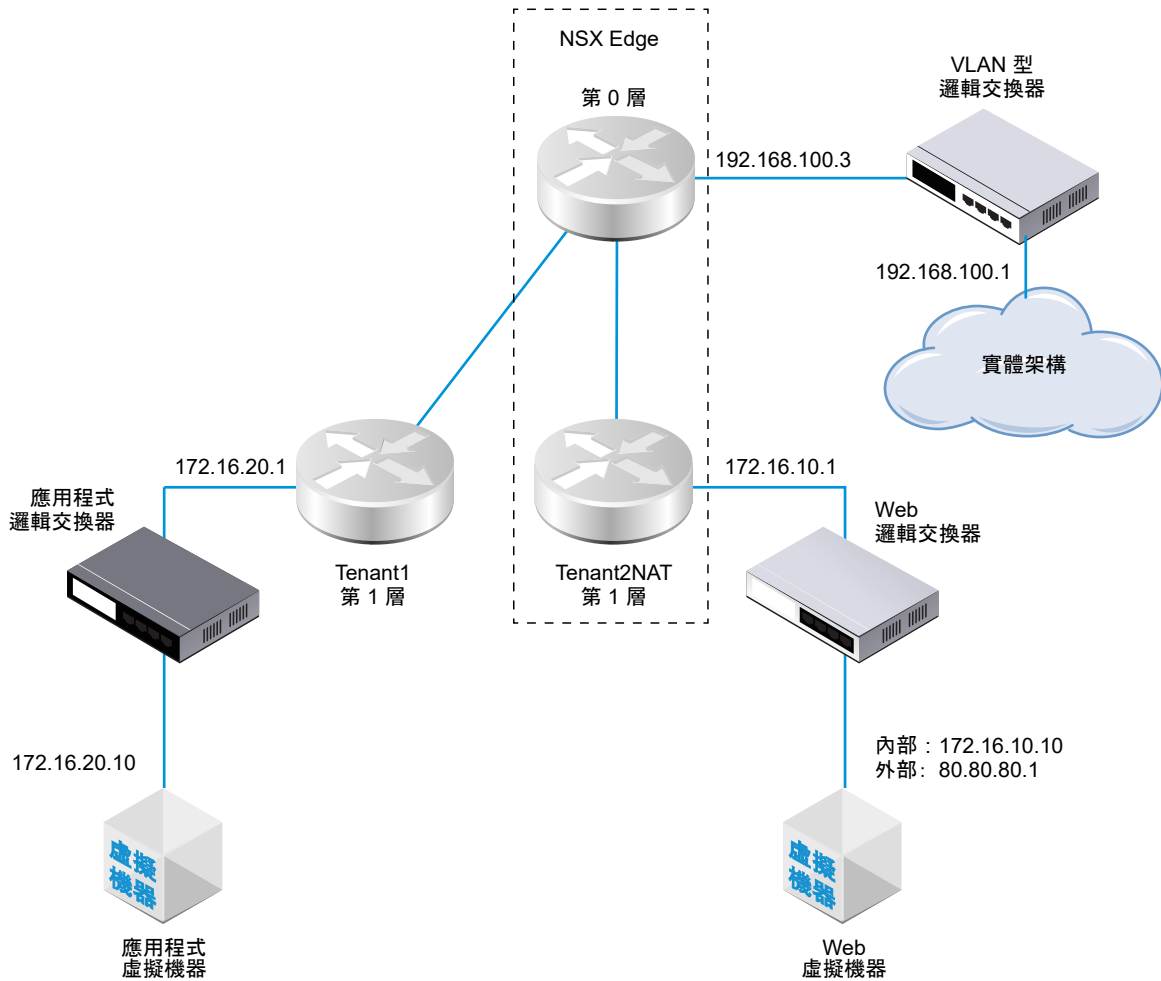
16 (選擇性) 變更防火牆略過設定。

此設定預設為啟用。

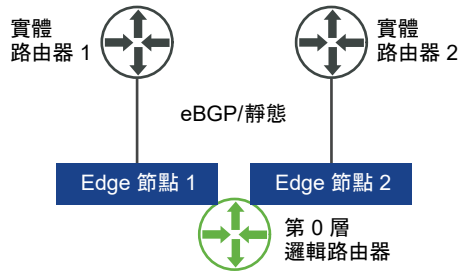
自反 NAT

當第 0 層邏輯路由器在作用中/作用中式模式中執行時，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。對於作用中/作用中式路由器，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。



涉及兩個作用中/作用中式第 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) 輸入閘道。
- 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。您也可以防火牆規則的 **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，作為來源和目的地。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 [NSX-T Data Center 功能支援 NSX Cloud](#) 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。
- **IP 集合** - 可指定標籤和選用範圍。

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

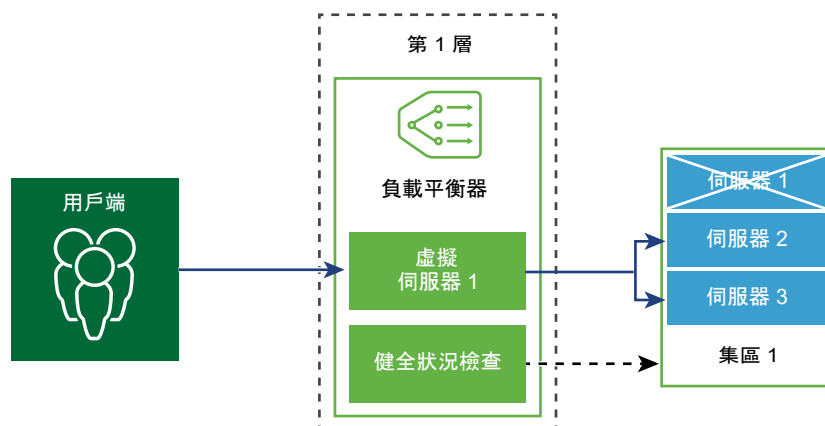
- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取**進階網路與安全性 > 網路 > IPAM**。
- 3 按一下 IP 區塊的名稱。
- 4 按一下**子網路**索引標籤。
- 5 若要新增子網路，請按一下**新增**。
 - a 輸入名稱和 (選用) 說明。
 - b 輸入子網路的大小。
- 6 若要刪除一或多個子網路，請選取子網路。
 - a 按一下**刪除**。

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**

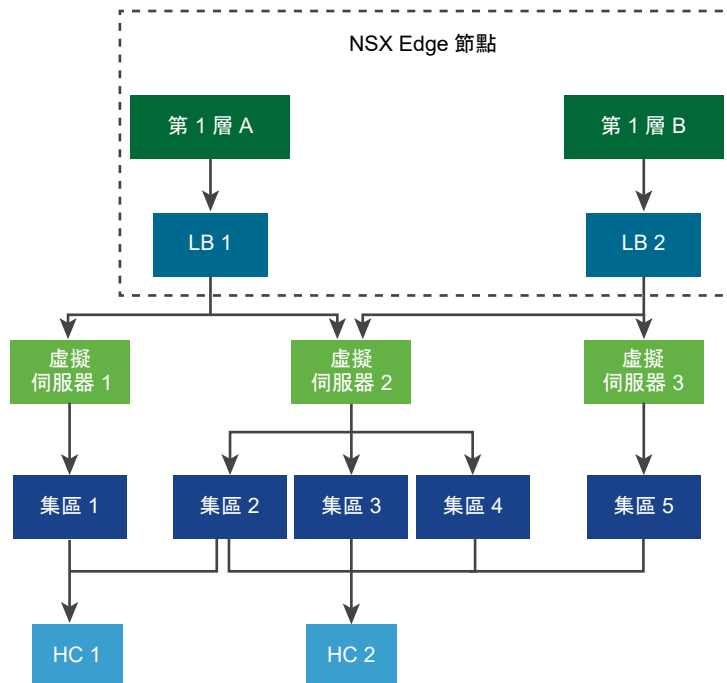
■ 設定負載平衡器元件

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。

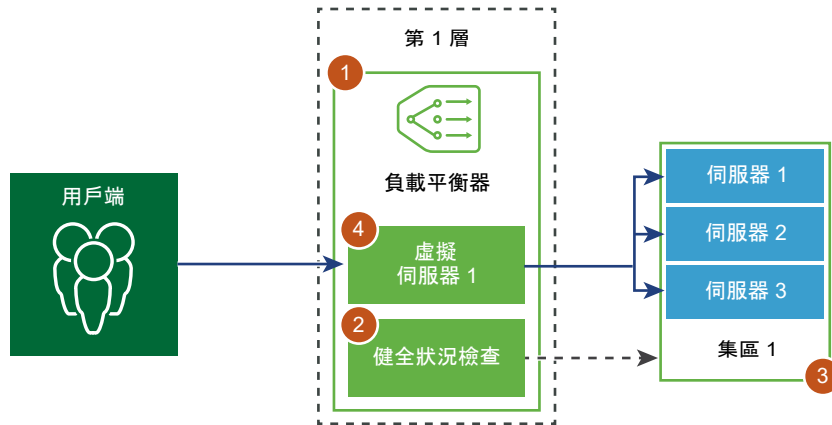
若要測試每個伺服器是否正確執行應用程式，您可以新增用於檢查伺服器健全狀況狀態的健全狀況檢查監視器。



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。

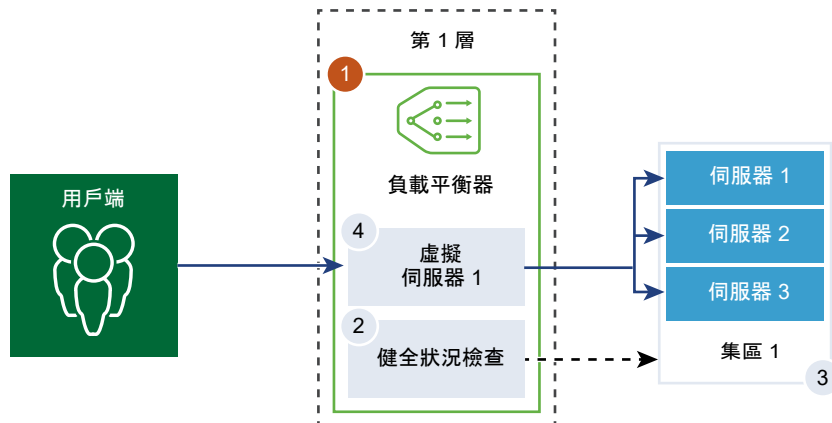


建立負載平衡器

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

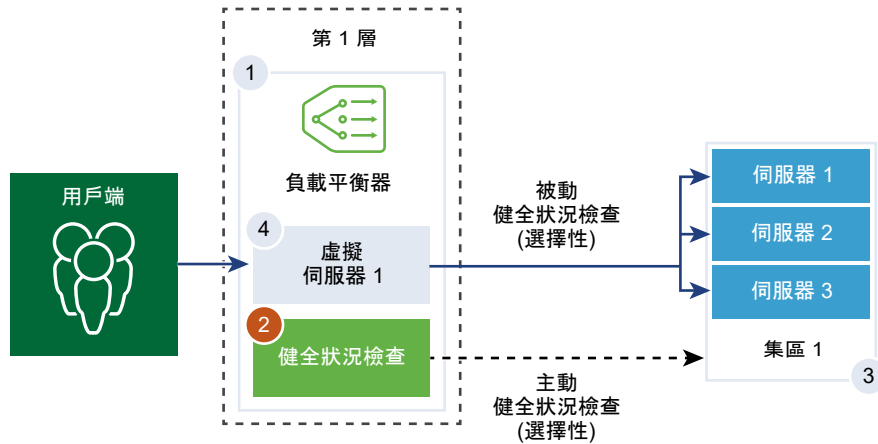
主動健全狀況監視器可用來測試伺服器是否可用。主動健全狀況監視器使用數種類型的測試，例如傳送基本 Ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

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 > 監控 > 主動健全狀況監控 > 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 > 監控 > 被動健全狀況監控 > 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。

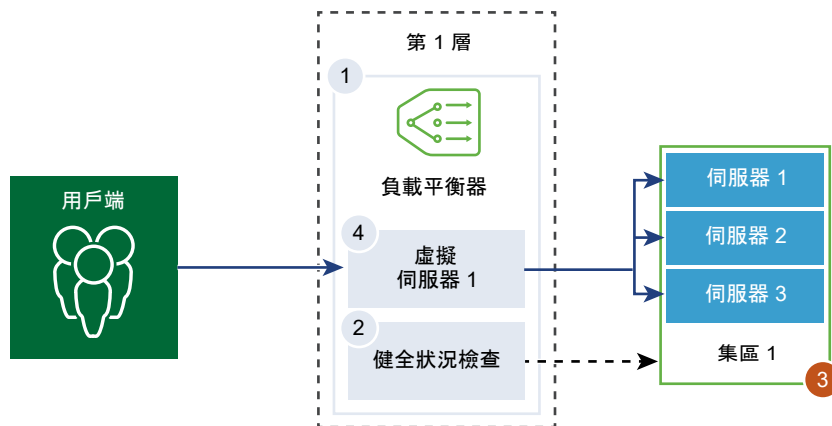
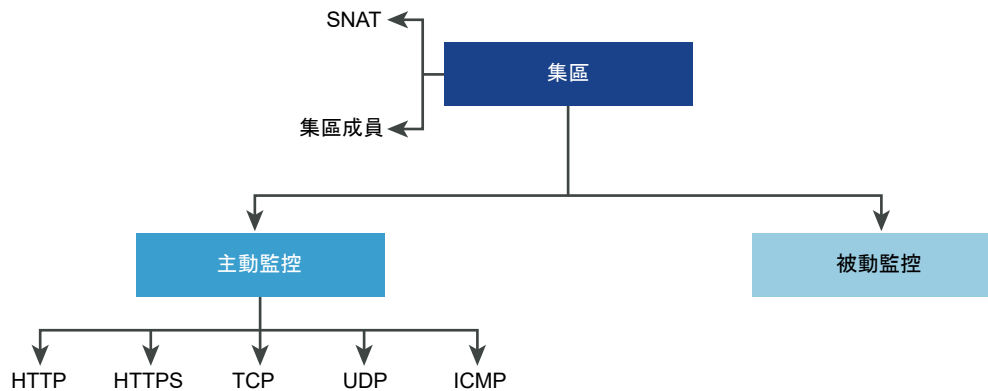


圖 19-1. 伺服器集區參數組態



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。

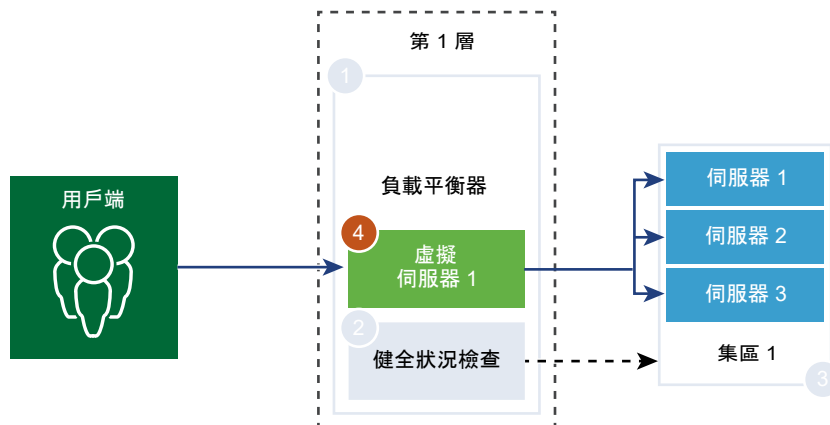
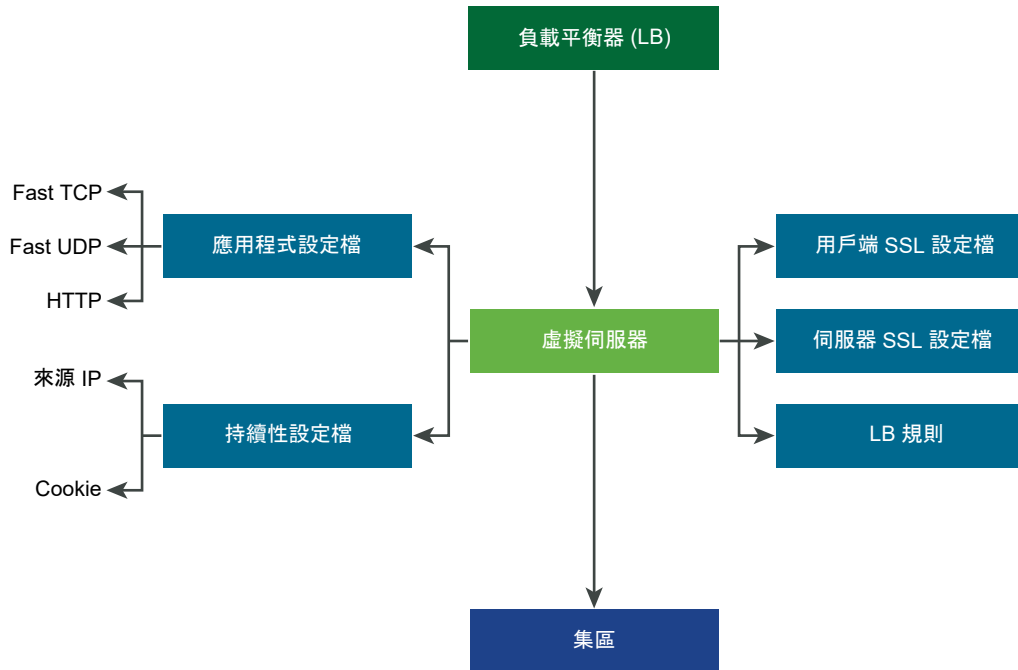


圖 19-2. 虛擬伺服器元件



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

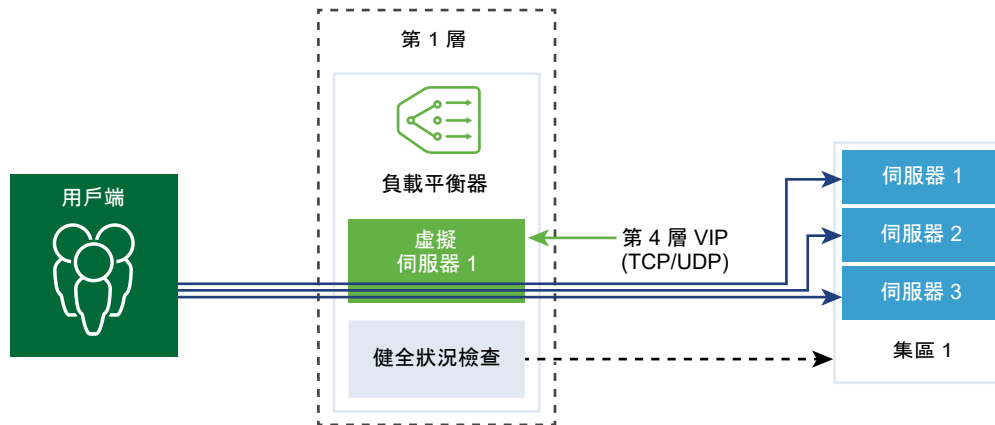
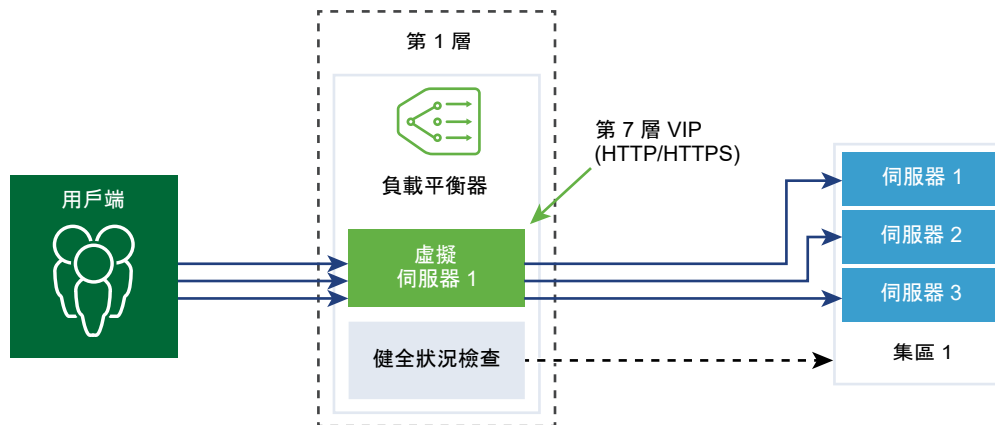


圖 19-4. 第 7 層 HTTPS 應用程式設定檔



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。

- a 從下拉式功能表中選取**新增 > 快速 UDP 設定檔**。
- b 輸入快速 UDP 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
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。

- a 從下拉式功能表中選取**新增 > 快速 HTTP 設定檔**。
- b 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 連線上接收的所有 HTTP 要求會透過單一 TCP 連線傳送到相同的伺服器，以確保不需要重新授權。</p>

d 按一下確定。

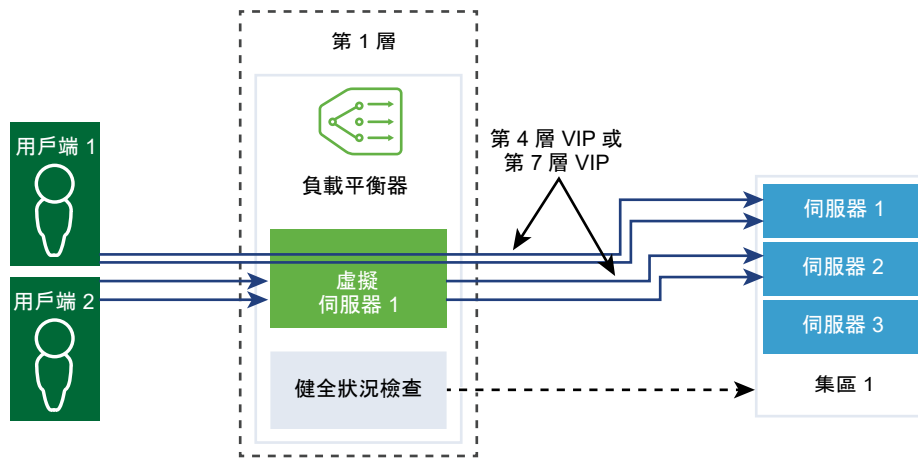
設定持續性設定檔

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

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

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

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



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。

- a 從下拉式功能表中選取**新增 > Cookie 持續性**。
- b 輸入 Cookie 持續性設定檔的名稱和說明。
- c 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。 ■ 首碼 - 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。請注意， 不支援 Cookie 名稱中存在空格。
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

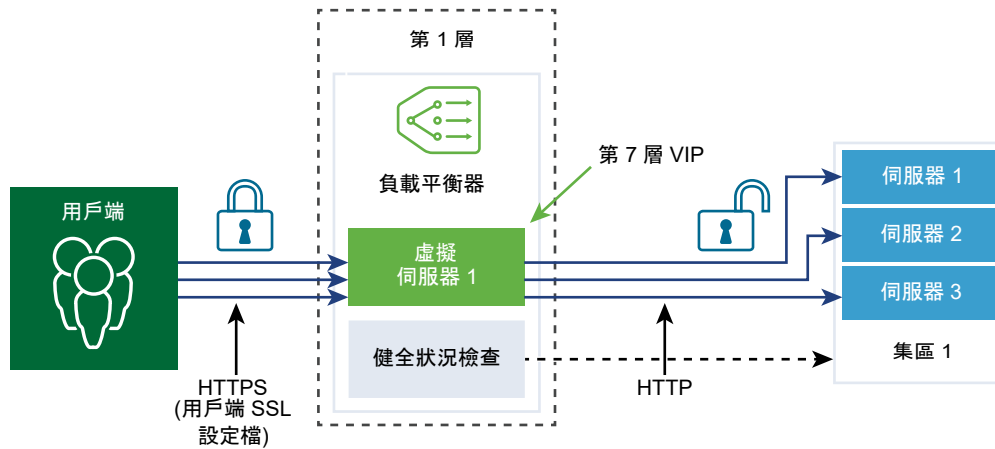
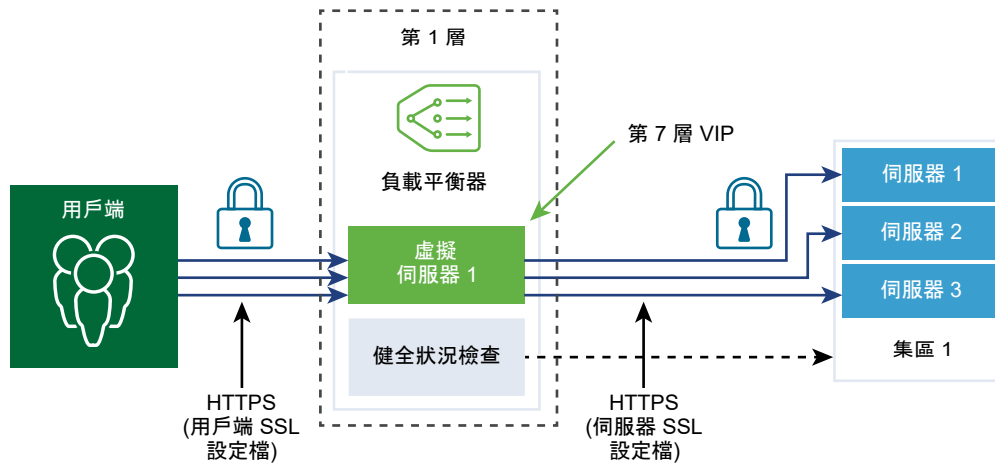


圖 19-6. 端對端 SSL



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[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](#)。
- 確認用戶端與服务器的 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 層虛擬服务器的名稱和說明。
- 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 層虛擬服务器的記錄。
- 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	如果未定義虛擬服务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。

- `$_args` - 來自要求的引數
- `$_arg_<name>` - 要求行中的引數 `<name>`
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_upstream_cookie_<name>` - 具有指定名稱且由上游伺服器在「設定 Cookie」回應標頭欄位中傳送的 Cookie
- `$_upstream_http_<name>` - 任意回應標頭欄位，`<name>` 是轉換為小寫、且將虛線取代為底線的欄位名稱
- `$_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
- `$_http_<name>` - 任意要求標頭欄位，`<name>` 為轉換為小寫且虛線以底線取代的欄位名稱
- `$_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。 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

支援的比對條件	說明
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
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：

- **新增或刪除邏輯路由器的防火牆規則**
- **為邏輯交換器橋接器連接埠設定防火牆**
- **防火牆區段和防火牆規則**
- **關於防火牆規則**

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。

- 若要新增規則，請按一下功能表列上的**新增規則**，然後選取**新增以上規則**或**新增以下規則**，或按一下規則第一個資料行中的功能表圖示，然後選取**新增以上規則**或**新增以下規則**，並指定規則參數。

[套用至] 欄位不會顯示，因為此規則僅會套用至邏輯路由器。

- 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。

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

- 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 > 安全性 > 橋接防火牆**。
- 選取邏輯交換器。
交換器必須已連結至橋接器設定檔。
- 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。

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。

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。對於 TCP 和 UDP 流量，在第一個封包之後，如果防火牆結果是 ALLOW，則會為任一方向的流量元組建立和維護快取。這表示流量不再需要檢查防火牆規則，如此可降低延遲。因此，無狀態防火牆在較大流量負載下通常較快且效能更佳。

可設定狀態防火牆可以從端對端監控流量串流。系統一律會針對每個封包來諮詢防火牆，以驗證狀態和序號。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/dfwpktlogs.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**。

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。

備註 NSX-T Data Center 會自動將 NSX Manager 和 NSX Edge 節點虛擬機器新增至防火牆排除清單。

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**。

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/dfwpktlogs.log` 檔案中。啟用記錄可能會影響效能。

- 13 在**動作資料行**中，選取動作。

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

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

- 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。

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：

- 檢視監控儀表板
- 檢視物件類別的使用量和容量
- 查看組態變更的實現狀態
- 搜尋物件
- 依物件屬性篩選
- 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
- 取代 NSX Edge 叢集中的 NSX Edge 傳輸節點
- 在 vCenter Server 遺失且無法復原時，復原 NSX-T。
- 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
- 符合性組態

- [收集支援服務包](#)
- [記錄訊息和錯誤碼](#)
- [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](#)
- [設定外部負載平衡器](#)

檢視監控儀表板

NSX Manager 介面提供多個監控儀表板，其中顯示有關於系統狀態、網路與安全性以及符合性報告的詳細資料。這些資訊可從 NSX Manager 介面中的不同位置檢視或存取，但可在[首頁 > 監控儀表板](#)頁面中一併存取。

您可以從 NSX Manager 介面的首頁存取監控儀表板。在這些儀表板中，您可以點選進入並存取從中提取儀表板資料的來源頁面。

程序

- 1 以管理員身分登入 NSX Manager 介面。
- 2 如果您還不在首頁上，請按一下[首頁](#)。
- 3 按一下 [監控儀表板]，然後從下拉式功能表中選取所需的儀表板類別。

頁面會顯示所選類別的儀表板。儀表板圖形會經過色彩編碼，而色彩代碼索引鍵會直接顯示在儀表板上。

- 4 若要存取更深入的詳細資料層級，請按一下儀表板的標題或儀表板的其中一個元素 (如果已啟用)。

下表說明預設儀表板及其來源。

表 21-1. 系統儀表板

儀表板	來源	說明
系統	系統 > 應用裝置 > 概觀	顯示 NSX Manager 叢集和資源 (CPU、記憶體、磁碟) 耗用量的狀態。
網狀架構	系統 > 網狀架構 > 節點 系統 > 網狀架構 > 傳輸區域 系統 > 網狀架構 > 計算管理程式	顯示 NSX-T 網狀架構的狀態，包括主機和 Edge 傳輸節點、傳輸區域和計算管理程式的狀態。
備份	系統 > 備份與還原	顯示 NSX-T 備份的狀態 (如果已設定)。強烈建議您設定遠端儲存至 SFTP 站台的排程備份。
Endpoint Protection	系統 > 服務部署	顯示 Endpoint Protection 部署的狀態。

表 21-2. 網路與安全性儀表板

儀表板	來源	說明
安全性	詳細目錄 > 群組 安全性 > Distributed Firewall	顯示群組和安全性原則的狀態。群組是工作負載、區段、區段連接埠和 IP 位址的集合，其中可能會套用安全性原則，包括東西向防火牆規則。
閘道	網路 > 第 0 層閘道 網路 > 第 1 層閘道	顯示第 0 層和第 1 層閘道的狀態。
區段	網路 > 區段	顯示網路區段的狀態。
負載平衡器	網路 > 負載平衡	顯示負載平衡器虛擬機器的狀態。
VPN	網路 > VPN	顯示虛擬私人網路的狀態。

表 21-3. 進階網路與安全性儀表板

儀表板	來源	說明
負載平衡器	進階網路與安全性 > 負載平衡器	顯示負載平衡器服務、負載平衡器虛擬伺服器 and 負載平衡器伺服器集區的狀態。負載平衡器可主控一或多部虛擬伺服器。虛擬伺服器會繫結至包含主控應用程式之成員的伺服器集區。
防火牆	進階網路與安全性 > 安全性 > Distributed Firewall 進階網路與安全性 > 安全性 > 橋接防火牆 進階網路與安全性 > 網路 > 路由器	指出是否已啟用防火牆，並顯示原則、規則和排除清單成員的數目。 備註 此儀表板中顯示的每個詳細項目，皆來自引用來源頁面中的特定子索引標籤。
VPN	不適用。	顯示虛擬私人網路的狀態，以及開啟的 IPSec 和 L2 VPN 工作階段數目。
交換	進階網路與安全性 > 交換	顯示邏輯交換器和邏輯連接埠 (包括虛擬機器和容器連接埠) 的狀態。

表 21-4. 符合性報告儀表板

資料行	說明
非符合性代碼	顯示特定的非符合性代碼。
說明	非符合性狀態的特定原因。
資源名稱	非符合性中的 NSX-T 資源 (節點、交換器和設定檔)。
資源類型	原因的資源類型。
受影響的資源	受影響的資源數目。按一下數值可檢視清單。

如需有關每個符合性報告代碼的詳細資訊，請參閱[符合性狀態報告代碼](#)。

檢視物件類別的使用量和容量

您可以檢視 NSX-T Data Center 環境中各種物件類別的使用量和容量。您也可以設定警示以讓您輕鬆查看何時達到使用量中的特定臨界值。

若要查看不同物件類別的使用量和容量，請按一下下列其中一個索引標籤：

- **網路 > 網路概觀 > 容量**
- **安全性 > 安全性概觀 > 容量**
- **詳細目錄 > 詳細目錄概觀 > 容量**
- **系統 > 系統概觀 > 容量**

您也可以導覽至**計劃和疑難排解 > 整併容量**，以在一個頁面上查看所有物件類別。

在每個容量頁面上，針對每個物件類別，會顯示下列資訊：

- 容量上限 - 此值是以大型應用裝置的容量為基礎。
- 目前的詳細目錄 (已實現) - 已成功建立或設定的物件數目。此數目會反映**進階網路與安全性**索引標籤中顯示的 NSX Manager 物件。這些物件可能包括您在**網路**、**安全性**、**詳細目錄**或**系統**索引標籤中建立的部分物件。顯示以色彩編碼的長條，以指出使用量百分比。如果使用量低於警告警示層級，則色彩為綠色。如果使用量處於或高於警告警示層級，但低於嚴重警示層級，則色彩為橙色。如果使用量處於或高於嚴重警示層級，則色彩為紅色。
- 警告警示 - 這是上述所提及的使用量長條將顯示為橙色的使用量層級。您可以變更此值。
- 嚴重警示 - 這是上述所提及的使用量長條將顯示為紅色的使用量層級。您可以變更此值。

變更警告警示或嚴重警示值時，您可以按一下**還原**，回到上次儲存的值。您可以按一下**重設值**以還原所有物件類別的預設值。

網路容量頁面會顯示下列物件類別：

- 第 0 層邏輯路由器
- 第 1 層邏輯路由器
- 首碼清單
- 全系統 NAT 規則
- DHCP 伺服器執行個體
- 全系統 DHCP 範圍和集區
- 已啟用 NAT 的第 1 層邏輯路由器
- 邏輯交換器
- 全系統邏輯交換器連接埠

安全性容量頁面會顯示下列物件類別：

- 已啟用全系統 Endpoint Protection 的主機
- 已啟用全系統 Endpoint Protection 的虛擬機器

- Active Directory 群組
- Active Directory 網域
- Distributed Firewall 規則
- 全系統防火牆規則
- 全系統防火牆區段
- Distributed Firewall 區段

詳細目錄容量頁面會顯示下列物件類別：

- 網路與安全群組
- IP 集合
- 以 IP 集合為基礎的群組
- vCenter 叢集
- Hypervisor 主機

系統容量頁面會顯示下列物件類別：

- 全系統虛擬介面
- Edge 叢集
- 全系統 Edge 節點

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/mps
```

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>
```

IPSecVPNDPDProfile

```
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>
```

```

DhcpServer
  POST /dhcp/servers
  PUT /dhcp/servers/<server-id>
  DELETE /dhcp/servers/<server-id>

DhcpStaticBinding
  POST /dhcp/servers/static-bindings
  PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
  DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

DhcpIpPool
  POST /dhcp/servers/ip-pools
  PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
  DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

DnsForwarder
  POST /dns/forwarders
  PUT /dns/forwarders/<forwarder-id>
  DELETE /dns/forwarders/<forwarder-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 Entities - 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.

```

```
DhcpServer
Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpStaticBinding
Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?
request_id=<request-id>
Response - An instance of ConfigurationState.

DhcpIpPool
Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.

DnsForwarder
Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>
Response - An instance of ConfigurationState.
```

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。

依物件屬性篩選

在 NSX Manager 中檢視物件時，您可以依照一或多個屬性來篩選物件。例如，檢視第 0 層閘道的詳細資料時，您可以選擇依**狀態**篩選並僅檢視**關閉**的閘道。


可供使用的篩選器類型如下：

- 預先定義的篩選器 – 您可以套用到物件的常用篩選器清單。
- 文字型篩選器 – 根據您輸入之屬性值的篩選器。此篩選器僅適用於物件的**名稱**、**標籤**、**路徑**和**說明**屬性。
- 屬性值配對 – 您可以用來指定篩選屬性值配對的屬性下拉式功能表。

您可以使用一個物件的多個屬性或單一屬性的多個值來篩選物件。選取多個屬性時會套用 AND 運算子，而指定單一屬性的多個值時會套用 OR 運算子。

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 導覽至顯示您想要檢視之物件的索引標籤。
- 3 指定您想要用於篩選物件的屬性。

- 按一下 ，然後從預先定義的篩選器清單中選取。
 - 輸入**名稱**、**標籤**、**路徑**或**說明**屬性的值。
 - 從下拉式功能表中選取屬性並指定其值。例如，**狀態**：**關閉**
- 系統會顯示滿足篩選器準則的物件。

- 4 (選擇性) 按一下**清除**可重設您的篩選器。

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收集來自 vCenter Server 的叢集資訊。

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。

在成功登錄 vCenter Server 後，請勿直接關閉虛擬機器的電源並刪除 NSX Manager 虛擬機器，而不先刪除計算管理程式。否則，當您部署新的 NSX Manager 時，將無法再次登錄相同的 vCenter Server。您將會收到 vCenter Server 已登錄至其他 NSX Manager 的錯誤。

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，以及它們之間的關聯性。NSX Manager 還會擷取 Active Directory (AD) 認證。

在 Active Directory 同步至 NSX Manager 後，您即可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 在強制執行身分識別防火牆規則時，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**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**。

若要擷取網域的 NetBIOS 名稱，請在屬於網域的 Windows Workstation 上或網域控制站上，在命令視窗中輸入 `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。

需要基本辨別名稱 (基本 DN) 才能新增 Active Directory 網域。基本 DN 是在 Active Directory 網域內搜尋使用者驗證時，LDAP 伺服器所使用的起點。例如，如果您的網域名稱為 `corp.local`，則 Active Directory 基本 DN 的 DN 將會是「`DC=corp,DC=local`」。

- 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。

必要條件

網域帳戶必須對網域樹狀結構中的所有物件具有 AD 讀取權限。事件記錄讀取者帳戶必須具有安全性事件記錄的讀取權限。

在有 NSX Manager 叢集的情況下，所有節點都必須能夠連線至 LDAP 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 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 如果選取了 LDAPS，請選取由 NSX Manager 建議的 SHA-256 指紋，或輸入 SHA-256 指紋。
- 9 輸入 LDAP 伺服器的 **連接埠號碼**。
對於本機網域控制站，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。
- 10 輸入 Active Directory 帳戶的 **使用者名稱和密碼**，該帳戶至少具有 Active Directory 網域的唯一讀取權。
- 11 按一下 **儲存**。
- 12 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。

如果您使用 API 來手動結束已開始進行的完整同步，則同步統計資料將不會正確更新。

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。

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：

功能表項目	說明
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 NSX Manager 和 NSX Edge 應用裝置都有三個本機帳戶，即管理員、稽核和根帳戶。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，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。

依預設，使用者密碼會在 90 天後到期。您可以變更或停用每個使用者的密碼到期功能。

當 NSX Manager 上的本機使用者的密碼將在 30 天內到期時，NSX Manager Web 介面會顯示密碼到期通知。如果您將本機使用者的密碼到期時間設為 30 天或更短的時間，則會一律顯示通知。

從 NSX-T Data Center 2.5.1 開始，通知會包含「變更密碼」連結。按一下此連結，可從 Web 介面變更本機使用者的密碼。

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 admin 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 admin 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 admin password-expiration
nsx>
```

重設應用裝置的密碼

下列程序適用於 NSX Manager、NSX Edge 和 Cloud Service Manager 應用裝置。

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。請注意，密碼同步可能需要幾分鐘或更長的時間。

如果您已將使用者重新命名為 `admin` 或 `audit`，請在下列程序中使用新名稱。

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。下列程序要求您已將 GRUB 設定為會顯示 GRUB 開機功能表。如需設定 GRUB 和變更 GRUB `root` 密碼的詳細資訊，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〉。

如果您執行的是 NSX-T Data Center 2.5.2 或更新版本，並且知道 `root` 的密碼，但忘了 `admin` 或 `audit` 的密碼，您可以使用下列程序進行重設：

- 1 以 `root` 身分登入應用裝置。
- 2 對於 NSX Edge，請執行命令 `/etc/init.d/nsx-edge-api-server stop`。否則，請執行命令 `/etc/init.d/nsx-mp-api-server stop`。
- 3 若要重設 `admin` 的密碼，請執行命令 `passwd admin`。
- 4 若要重設 `audit` 的密碼，請執行命令 `passwd audit`。
- 5 執行命令 `touch /var/vmware/nsx/reset_cluster_credentials`。
- 6 對於 NSX Edge，請執行命令 `/etc/init.d/nsx-edge-api-server start`。否則，請執行命令 `/etc/init.d/nsx-mp-api-server start`。

如果您忘記了 `root` 使用者的密碼，則可以使用下列程序來重設密碼。如果您執行的是 NSX-T Data Center 2.5.0 或 2.5.1，且想要重設 `admin` 和 `audit` 的密碼，請一併使用下列程序。如果您執行的是 NSX-T Data Center 2.5.2 或更新版本，則可以在重設 `root` 的密碼後，使用上述程序重設 `admin` 或 `audit` 的密碼。

程序

- 1 連線至應用裝置的主控台。
- 2 將系統重新開機。
- 3 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。

4 按 **e** 編輯功能表。

輸入使用者名稱 (`root`) 和 `root` 的 GRUB 密碼 (與應用裝置的使用者 `root` 不同)。

5 將游標保持在 Ubuntu 選取項目上。

6 按 **e** 編輯選取的選項。

7 搜尋開頭為 `linux` 的行。

8 如果您執行的是 NSX-T Data Center 2.5.0 或 2.5.1，請執行下列步驟：

a 移除 `root=UUID=<ID number>` 後面的所有選項，並將在 UUID 後面新增 `rw single init=/bin/bash`。

b 按 **Ctrl-x** 進行開機。

c 停止記錄訊息時，請按 Enter 鍵。

您會看到提示 `root@(none):/#`。

d 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。

e 輸入新密碼，然後再次輸入加以確認。

f 如果您要重設 NSX Manager 上的密碼，請執行命令 `touch /var/vmware/nsx/reset_cluster_credentials`。

g 執行命令 `sync`。

h 執行命令 `reboot -f`。

9 如果您執行的是 NSX-T Data Center 2.5.2 或更新版本，請執行下列步驟：

a 將 `systemd.wants=PasswordRecovery.service` 新增至行尾。

b 按 **Ctrl-x** 進行開機。

c 輸入 `root` 的新密碼，然後再次輸入加以確認。

開機程序完成後，您可以用 `root` 的身分使用新密碼登入，以確認密碼變更。

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，openssl 命令執行較舊的 OpenSSL 版本，因此您必須在 vIDM 主機中使用 openssl1 命令。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 在 vIDM 主機的主控台或以使用者 **sshuser** 的身分使用 SSH 登入到 vIDM 主機，或者登入到可以對 vIDM 主機執行 ping 動作的任何伺服器。
- 2 執行下列其中一個命令來取得 vIDM 主機的指紋。
 - 如果已登入到 vIDM 主機，請執行 openssl1 命令來取得指紋：

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl
x509 -sha256 -fingerprint -noout -in /dev/stdin
```

如果在執行命令時發生錯誤，您可能需要使用 openssl1 命令 (即 sudo) 來執行 sudo openssl1 ...。

- 如果已登入到可以對 vIDM 主機執行 ping 動作的伺服器，請執行 openssl 命令來取得指紋：

```
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 部署可以是獨立 vIDM 主機或 vIDM 叢集。

vIDM 主機或所有 vIDM 叢集元件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。

如果需要存取 NSX-T API，下列其中一個組態必須成立：

- vIDM 具有已知的 CA 簽署憑證。
- vIDM 在 vIDM 服務端上具有受信任的連接器 CA 憑證。
- vIDM 使用輸出連接器模式。

備註 NSX Manager 和 vIDM 必須位於相同的時區。建議的方式是使用 UTC。

如果您未使用虛擬 IP 或外部負載平衡器，則必須將 DNS 伺服器設定為具有 PTR 記錄 (這表示，管理程式會使用節點的實體 IP 或 FQDN 進行設定)。

如果將 vIDM 設定為與外部負載平衡器整合，則必須在負載平衡器上啟用工作階段持續性，以避免發生頁面未載入或使用者非預期登出之類的問題。

如果 vIDM 部署是 vIDM 叢集，則必須針對 SSL 終止和重新加密設定 vIDM 負載平衡器。

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://<csn-ip-address>/login.jsp?local=true` 個別登入 CSM。

必要條件

- 根據 vIDM 部署的類型 (獨立 vIDM 主機或 vIDM 叢集)，確認您擁有 vIDM 主機或 vIDM 負載平衡器的憑證指紋。兩種情況下用來取得指紋的命令皆相同。請參閱 [從 vIDM 主機取得憑證指紋](#)。

- 確認已向 vIDM 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-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html> 的 VMware Identity Manager 說明文件。建立用戶端時，您僅需要執行下列操作：
 - 將**存取類型**設定為**服務用戶端 Token**。
 - 指定用戶端識別碼。
 - 展開**進階**欄位，然後按一下**產生共用密碼**。
 - 按一下**新增**。

NSX Cloud 附註 如果使用 NSX Cloud，也請確認已向 vIDM 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	根據 vIDM 部署的類型 (獨立 vIDM 主機或 vIDM 叢集)，vIDM 主機或 vIDM 負載平衡器的完整網域名稱 (FQDN)。
OAuth 用戶端識別碼	向 vIDM 登錄 NSX Manager 時所建立的識別碼。
OAuth 用戶端密碼	向 vIDM 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。

驗證 VMware Identity Manager 功能

設定 VMware Identity Manager 之後，請驗證其功能。除非已正確設定並驗證 VMware Identity Manager，否則某些使用者在嘗試登入時，可能會收到「未獲授權」(錯誤碼 98) 訊息。

除非已正確設定並驗證 VMware Identity Manager，否則某些使用者在嘗試登入時，可能會收到「未獲授權」(錯誤碼 98) 訊息。

程序

- 1 建立使用者名稱和密碼的 Base64 編碼。

執行下列命令取得編碼，並移除尾端的「\n」字元。例如：

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZGlpbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

- 2 確認每個使用者都可對每個節點執行 API 呼叫。

使用遠端授權 curl 命令：`curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy`。例如：

```
curl -k -H 'Authorization: Remote c2ZhZGlpbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

這會傳回授權原則設定，例如：

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

如果命令未傳回錯誤，表示 VMware Identity Manager 正常運作。不需要再執行其他步驟。如果 curl 命令傳回錯誤，表示使用者可能會遭到鎖定。

備註 帳戶鎖定原則可在個別節點上設定並強制執行。叢集中的一個節點鎖定使用者時，不代表其他節點也會鎖定。

3 若要重設節點上的使用者鎖定：

- a 使用本機 NSX Manager admin 使用者身分擷取授權原則：

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b 將輸出儲存至目前工作目錄中的 JSON 檔案。
c 修改檔案以變更鎖定期間設定。

例如，假設有許多預設設定套用 900 秒的鎖定和重設期間。請變更這些值以啟用立即重設，例如：

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d 將變更套用至受影響的節點。

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (選擇性) 將授權原則設定檔案回復為其先前的設定。

這樣應該可以解決鎖定問題。如果您仍可執行遠端授權 API 呼叫，但仍無法透過瀏覽器登入，表示瀏覽器可能儲存了無效的快取或 Cookie。請清除快取和 Cookie，然後再試一次。

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 time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 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
- 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 21-5. 角色和權限和表 21-6. 進階網路與安全性的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
- 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 21-5. 角色和權限

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Ad m	LB Au d	VPN Adm	GI Adm	NI Adm
網路 > 第 0 層 闢道	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 網路介面	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 網路靜態 路由	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 地區設定 服務	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 靜態 ARP 組 態	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 區段	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > 區段 > 區段設定 檔	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
網路 > IP 位址 集區	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
網路轉送 原則	FA	R	FA	R	FA	R	FA	R	無	無	無	無	無
網路 > DNS	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
網路 > 負載平衡	FA	R	無	無	R	無	FA	R	FA	R	無	無	無
網路 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	無	無	無
網路 > VPN	FA	R	FA	R	FA	R	FA	R	無	無	FA	無	無
網路 > IPv6 設 定檔													
安全性 > Distribu ted Firewall	FA	R	R	R	FA	R	FA	R	R	R	R	R	R

表 21-5. 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
安全性 > 閘道防火牆	FA	R	R	R	FA	R	FA	R	無	無	無	無	FA
安全性 > 網路自我 檢查	FA	R	R	R	R	R	FA	R	無	無	無	無	FA
安全性 > Endpoint Protection 規則	FA	R	R	R	R	R	FA	R	無	無	無	FA	無
詳細目錄 > 內容設 定檔	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
計劃和疑 難排解 > 連接埠鏡 像	FA	R	FA	R	R	R	FA	R	無	無	無	無	無
計劃和疑 難排解 > 連接埠鏡 像繫結	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
計劃和疑 難排解 > 監控設定 檔繫結	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
計劃和疑 難排解 > 防火牆 IPFIX 設 定檔	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
計劃和疑 難排解 > 交換器 IPFIX 設 定檔	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
系統 > 網狀架構 > 節點 > 主機	FA	R	R	R	R	R	R	R	無	無	無	無	無

表 21-5. 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
系統 > 網狀架構 > 節點 > 節點	FA	R	FA	R	FA	R	R	R	R	R	無	無	無
系統 > 網狀架構 > 節點 > Edge	FA	R	FA	R	R	R	R	R	無	無	無	無	無
系統 > 網狀架構 > 節點 > Edge 叢 集	FA	R	FA	R	R	R	R	R	無	無	無	無	無
系統 > 網狀架構 > 節點 > 橋接器	FA	R	FA	R	R	R	無	無	R	R	無	無	無
系統 > 網狀架構 > 節點 > 傳輸節點	FA	R	R	R	R	R	R	R	R	R	無	無	無
系統 > 網狀架構 > 節點 > 通道	R	R	R	R	R	R	R	R	R	R	無	無	無
系統 > 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
系統 > 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
系統 > 網狀架構 > 設定檔 > 組態	FA	R	無	無	無	無	R	R	無	無	無	無	無
系統 > 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

表 21-5. 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
系統 > 網狀架構 > 傳輸區 域 > 傳 輸區域設 定檔	FA	R	R	R	R	R	R	R	無	無	無	無	無
系統 > 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 > 憑證	FA	R	無	無	FA	R	無	無	FA	R	FA	無	無
系統 > 服務部署 > 服務執 行個體	FA	R	R	R	FA	R	FA	R	無	無	無	FA	FA
系統 > 公用程式 > 支援服 務包	FA	R	無	無	無	無	無	無	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 > Active Director y	FA	R	FA	R	FA	FA	R	R	R	R	R	R	R
系統 > 使用者 > 組態	FA	R	無	無	無	無	無	無	無	無	無	無	無
系統 > 授權	FA	R	R	R	R	R	無	無	無	無	無	無	無
系統 > 系統管理	FA	R	R	R	R	R	R	R	無	無	無	無	無

表 21-5. 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
自訂儀表板組態	FA	R	R	R	R	R	FA	R	R	R	R	R	R
系統 > 生命週期 管理 > 移轉	FA	無	無	無	無	無	無	無	無	無	無	無	無

表 21-6. 進階網路與安全性的角色和權限

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 > 連接埠連 線	E	R	E	E	E	E	E	R	E	E	無	無	無
工具 > Traceflo w	E	R	E	E	E	E	E	R	E	E	無	無	無
工具 > 連接埠鏡 像	FA	R	FA	R	R	R	FA	R	無	無	無	無	無
工具 > IPFIX	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
防火牆 > Distribu ted Firewall > 一般	FA	R	R	R	FA	R	FA	R	無	無	無	無	R
防火牆 > Distribu ted Firewall > 組態	FA	R	R	R	FA	R	FA	R	無	無	無	無	無
防火牆 > Edge 防 火牆	FA	R	R	R	FA	R	FA	R	無	無	無	無	FA
路由 > 路由器	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R
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	無	無	FA	R	無	無	無	無	無

表 21-6. 進階網路與安全性的角色和權限 (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
DHCP > 伺服器	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
DHCP > 轉送設定 檔	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
DHCP > 轉送服務	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
DHCP > 中繼資料 Proxy	FA	R	FA	R	無	無	無	無	無	無	無	無	無
IPAM	FA	R	FA	FA	R	R	無	無	R	R	無	無	無
交換 > 交換器	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R
交換 > 連接埠	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R
交換 > 交換設定 檔	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
網路 > 負載平衡 器	FA	R	無	無	R	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
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	無	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

表 21-6. 進階網路與安全性的角色和權限 (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
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 > 設 定標籤	FA	無	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 啟用**偵測 NSX 組態變更**，會在偵測到任何執行階段或非組態相關變更，或使用者組態中的任何變更時，觸發未排程的完整組態備份。
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。

備註 此選項可能會產生大量備份。請謹慎使用。

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)。

您必須將備份還原至新的 NSX Manager 應用裝置。

如果在建立備份時已有 NSX Manager 叢集，則您還應該還原至 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。

重要 如果 NSX Manager 叢集中的任何節點仍可供使用，則必須在開始還原之前關閉其電源。

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。
- 遵循 [列出可用的備份](#) 中的程序來識別要還原的備份。記下取得備份之 NSX Manager 節點的 IP 或 FQDN。
- 如果您設定 NSX Manager 節點以發佈其 FQDN，則必須為 DNS 伺服器上的 NSX Manager 節點設定正向和反向查閱項目。

程序

- 1 關閉要還原的 NSX Manager 叢集中所有節點的電源。

2 安裝一個新的 NSX Manager 節點，以在其上還原備份。

- 如果要還原之備份的備份清單包含 IP 位址，您必須使用相同的 IP 位址部署新的 NSX Manager 節點。請勿將 NSX Manager 節點設定為發佈其 FQDN。

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- 如果您要還原之備份的備份清單包含 FQDN，則必須使用此 FQDN 設定新的 NSX Manager 節點 (請參閱《NSX-T Data Center 安裝指南》中的「NSX Manager 安裝」主題的〈發佈 NSX Manager 的 FQDN〉一節，以取得詳細資訊)。此外，如果新 NSX Manager 節點的 IP 位址與原本的不同，則您必須使用新的 IP 位址更新 NSX Manager 節點的 DNS 伺服器正向和反向查閱項目。

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

在新的 NSX Manager 節點執行並上線後，您可以繼續進行還原。

- 3 在瀏覽器中，以管理員權限登入新的 NSX Manager。
- 4 選取**系統 > 備份與還原**。
- 5 按一下**還原索引**標籤。
- 6 若要設定備份檔案伺服器，請按一下**編輯**。
- 7 輸入 IP 位址或主機名稱。
- 8 視需要變更連接埠號碼。
預設值為 22。
- 9 若要登入伺服器，請輸入使用者名稱和密碼。
- 10 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。
- 11 輸入用來加密備份資料的複雜密碼。
- 12 輸入儲存備份之伺服器的 SSH 指紋。
- 13 按一下**儲存**。
- 14 選取備份。
- 15 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，**還原完成**畫面會顯示還原的結果、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。

您也可以檢查記錄檔，以確認是否有叢集還原或節點還原失敗。執行 `get log-file syslog` 以檢視系統記錄檔，並搜尋字串 `Cluster restore failed` 和 `Node restore failed`。

若要將管理程式重新啟動，請執行 `restart service manager` 命令。

若要將管理程式重新開機，請執行 `reboot` 命令。

- 16 如果您僅部署一個節點，則在還原的 NSX Manager 節點已啟動且正常運作後，您可以部署其他節點以形成 NSX Manager 叢集。

如需指示，請參閱《NSX-T Data Center 安裝指南》。

- 17 部署新的 NSX Manager 叢集後，請刪除您在步驟 1 中關閉的原始 NSX Manager 叢集虛擬機器。

您也必須取代叢集中第二個和第三個節點上的憑證。

結果

如果您在備份後新增了計算管理程式，並且嘗試在還原後再次新增計算管理程式，您會收到一則錯誤訊息，指出登錄失敗。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](#)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。

升級期間的備份和還原

在升級程序進行期間，管理平面會停止回應，且您需要還原在升級進行中時所建立的備份。

問題

升級協調器已升級，但管理平面停止回應。您的備份是在升級進行中時建立的。

解決方案

- 1 使用先前用來建立備份的相同 IP 位址來部署您的管理平面節點。
- 2 上傳您在升級程序開始時所使用的升級服務包。
- 3 對升級協調器進行升級。
- 4 還原在升級程序中建立的備份。
- 5 上傳新的升級服務包 (如有必要)。
- 6 繼續進行升級程序。

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

- 1 經由 `https://<vCenter Server 主機名稱或 IP 位址>/mob` 登入 MOB。
- 2 按一下 **內容連結**，此為內容資料表中 **內容屬性** 的值。
- 3 按一下 **ExtensionManager 連結**，此為內容資料表中 **extensionManager** 內容的值。
- 4 按一下方法資料表中的 **UnregisterExtension** 連結。
- 5 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 admin 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	UUID	IP
ADDRESS	PORT	FQDN
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-afeb-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      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: CONTROLLER
Group Status: STABLE

Members:
  UUID                                FQDN
IP      STATUS
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      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: POLICY
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: 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

```

關閉 NSX Manager 叢集及開啟其電源

如果您需要關閉 NSX Manager 叢集，請使用下列程序。

程序

- 若要關閉 NSX Manager 叢集，請逐一關閉各個管理程式節點。您可用 `admin` 的身分登入管理程式節點的命令列介面 (CLI)，並執行命令 `shutdown`，或從 vCenter Server 關閉管理程式節點虛擬機器。請確定 vCenter Server 中的虛擬機器已關閉電源，再繼續處理下一個虛擬機器。
- 若要開啟 NSX Manager 叢集的電源，請逐一開啟 vCenter Server 中各個管理程式節點虛擬機器的電源。請確定節點已啟動且正在執行，再繼續處理下一個節點。

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 在**系統索引標籤**上，按一下 **NSX 管理節點**。
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。

將 ESXi 主機傳輸節點新增至 vCenter Server 和從中移除

您可以將 ESXi 主機傳輸節點從一個 vCenter Server (VC) 移至另一個，也可以從一個 NSX Manager 叢集移至另一個。

案例 1：VC1 已連線至 NSX Manager 叢集 1，以及 VC2 已連線至 NSX Manager 叢集 2

假設 ESX1 (ESXi 主機傳輸節點) 位於 VC1 中，您可以透過執行下列步驟，將其移至 VC2：

- 1 從 ESX1 解除安裝 NSX。
- 2 將 ESX1 移至 VC2。
- 3 將傳輸節點設定檔套用至 ESX1。

案例 2：VC1 和 VC2 均已連線至 NSX Manager 叢集

假設 ESX1 (ESXi 主機傳輸節點) 位於 VC1 中，您可以透過執行下列步驟，將其移至 VC2：

- 1 從 ESX1 解除安裝 NSX。
- 2 將 ESX1 移至 VC2。
- 3 將傳輸節點設定檔套用至 ESX1。

案例 3：VC1 已連線至 NSX Manager 叢集 1

假設 ESX1 (ESXi 主機傳輸節點) 位於 VC1 中，您可以透過執行下列步驟，將其移至 NSX Manager 叢集 2 作為獨立主機：

- 1 從 ESX1 解除安裝 NSX。

- 2 將 ESX1 新增至 NSX Manager 叢集 2。

取代 NSX Edge 叢集中的 NSX Edge 傳輸節點

您可以使用 NSX Manager UI 或 API 取代 NSX Edge 叢集中的 NSX Edge 傳輸節點。

使用 NSX Manager UI 取代 NSX Edge 傳輸節點

下列程序說明使用 NSX Manager UI 取代 NSX Edge 叢集中的 NSX Edge 傳輸節點。您可以取代 Edge 傳輸節點，無論其是否正在執行。

如果要取代的 Edge 節點不在執行中，則新的 Edge 節點可以具有相同的管理 IP 位址和 TEP IP 位址。如果要取代的 Edge 節點正在執行中，則新的 Edge 節點必須具有不同的管理 IP 位址和 TEP IP 位址。

必要條件

自行熟悉安裝 NSX Edge 節點、使用管理平面加入 Edge 節點，以及建立 NSX Edge 傳輸節點的程序。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》。

程序

- 1 如果您想要新的 Edge 傳輸節點具有與所要取代 Edge 傳輸節點相同的組態，請執行下列 API 呼叫以尋找組態：

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 依照《NSX-T Data Center 安裝指南》中的程序來安裝和設定 Edge 傳輸節點。

如果您想要此 Edge 傳輸節點具有與所要取代 Edge 傳輸節點相同的組態，請使用在步驟 1 中取得的組態。

- 3 在 NSX Manager 中，選取**系統 > 網狀架構 > 節點 > Edge 叢集**。

- 4 按一下第一個資料行中的核取方塊，以選取 Edge 叢集。

- 5 按一下**動作 > 取代 Edge 叢集成員**。

建議您將要取代的傳輸節點置於維護模式。如果傳輸節點不在執行中，則可以放心地忽略此建議。

- 6 從下拉式清單中選取要取代的節點。

- 7 從下拉式清單中選取取代節點。

- 8 按一下**儲存**。

使用 API 取代 NSX Edge 傳輸節點

下列程序說明使用 NSX-T API 取代 NSX Edge 叢集中的 NSX Edge 傳輸節點。您可以取代 Edge 傳輸節點，無論其是否正在執行。

如果要取代的 Edge 節點不在執行中，則新的 Edge 節點可以具有相同的管理 IP 位址和 TEP IP 位址。如果要取代的 Edge 節點正在執行中，則新的 Edge 節點必須具有不同的管理 IP 位址和 TEP IP 位址。

必要條件

自行熟悉安裝 NSX Edge 節點、使用管理平面加入 Edge 節點，以及建立 NSX Edge 傳輸節點的程序。如需詳細資訊，請參閱《NSX-T Data Center 安裝指南》。

程序

- 1 如果您想要新的 Edge 傳輸節點具有與所要取代 Edge 傳輸節點相同的組態，請執行下列 API 呼叫以尋找組態：

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 依照《NSX-T Data Center 安裝指南》中的程序來安裝和設定 Edge 傳輸節點。

如果您想要此 Edge 傳輸節點具有與所要取代 Edge 傳輸節點相同的組態，請使用在步驟 1 中取得的組態。

- 3 進行 API 呼叫以取得新的傳輸節點識別碼，以及要取代的傳輸節點。id 欄位包含傳輸節點識別碼。例如，

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

- 4 進行 API 呼叫以取得 NSX Edge 叢集的識別碼。id 欄位包含 NSX Edge 叢集識別碼。從 members 陣列取得 NSX Edge 叢集的成員。例如，

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

```

```

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

```

- 5 建立 API 以取代 NSX Edge 叢集中的傳輸節點。member_index 必須符合所要取代傳輸節點的索引。

例如，傳輸節點 TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) 已失敗，且取代為 NSX Edge 叢集 Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78) 中的傳輸節點 TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3)。

```

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

```

在 vCenter Server 遺失且無法復原時，復原 NSX-T。

如果 vCenter Server (VC) 遺失且無法復原 (可能因為沒有備份或備份已損壞)，請在重新部署 VC 之後，使用以下下列來復原 NSX-T 環境。

新的 VC 必須與原始 VC 具有相同的 FQDN 和 IP 位址。此外，它還必須具有包含相同主機的相同叢集。當主機的虛擬機器電源已開啟，將這些主機新增至 VC 時，請務必小心。請確定這些主機是新增到正確的叢集，而非新增到 VC 資料中心。

計算管理程式

在 NSX Manager 中，刪除舊計算管理程式。然後，將新的 VC 新增為計算管理程式。

主機傳輸節點

在 NSX Manager 中，主機將顯示在正確的 VC 叢集中。無需執行任何動作。

Edge 節點

您必須更換從 NSX Manager UI 部署的 Edge 節點。

- 1 請遵循[使用 NSX Manager UI 取代 NSX Edge 傳輸節點](#)中所述的程序來更換 Edge 節點。
- 2 確認已在新的 Edge 虛擬機器上設定閘道 (或邏輯路由器) 和通道。
- 3 移至**系統 > 網狀架構 > Edge 傳輸節點**，以刪除舊 Edge 節點。選取 Edge 節點，然後按一下**動作 > 刪除**。可以忽略諸如「關閉電源失敗」之類的錯誤。
- 4 在 VC 中，關閉舊 Edge 虛擬機器的電源，並將其刪除。
- 5 針對每個 Edge 節點，重複上述步驟。

NSX Manager

您必須更換從 NSX Manager UI 部署的 NSX Manager。通常，第二個和第三個 NSX Manager 是以這種方式部署的。

- 1 登入第一個 NSX Manager 的 UI。
- 2 移至**系統 > 應用裝置**，然後選取第三個 NSX Manager。按一下**動作 > 刪除**。這會因無法關閉 Manager 虛擬機器的電源而失敗。現在有強制刪除選項可用。選取**動作 > 強制刪除**。
- 3 如果強制刪除選項不起作用，請執行下列動作：
 - a 登入第一個 NSX Manager 的 CLI。
 - b 執行 `get cluster status` 命令，以取得第三個 NSX Manager 的 UID。
 - c 執行 `detach node <node-uid>` 命令，使第三個 NSX Manager 脫離叢集。
 - d 執行下列 API 呼叫，以強制刪除第三個 NSX Manager：

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 在 VC 中，關閉第三個 NSX Manager 的電源，並將其刪除。
- 5 部署與第三個 NSX Manager 具有相同組態的新 NSX Manager。
- 6 重複上述步驟，以刪除第二個 NSX Manager。
- 7 部署兩個新的 NSX Manager。

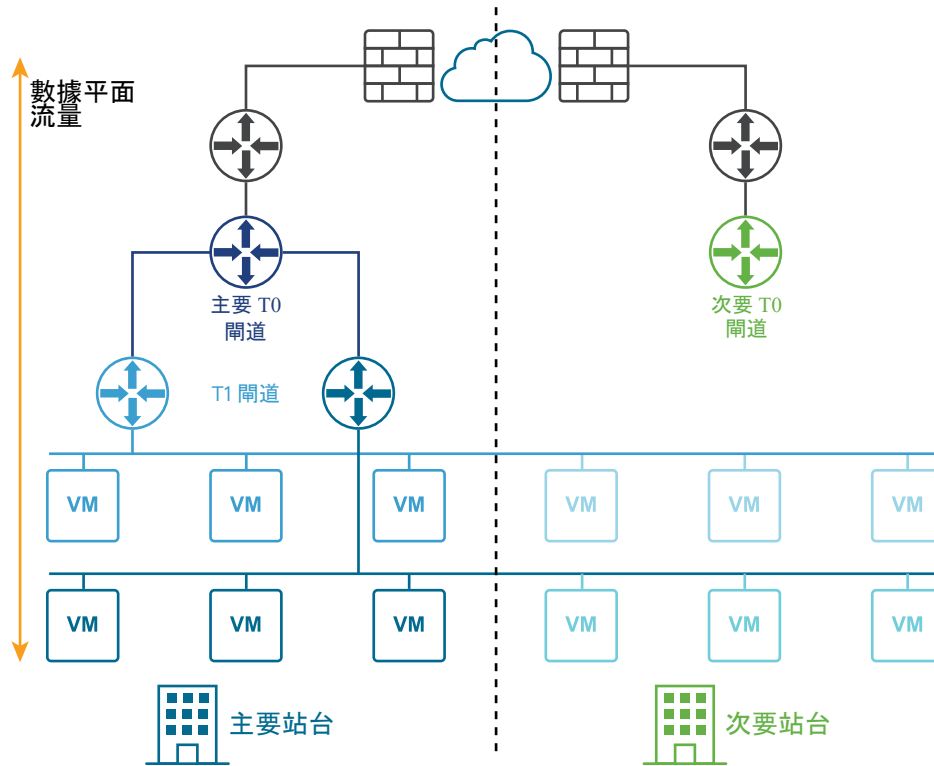
NSX-T Data Center 的多站台部署

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：

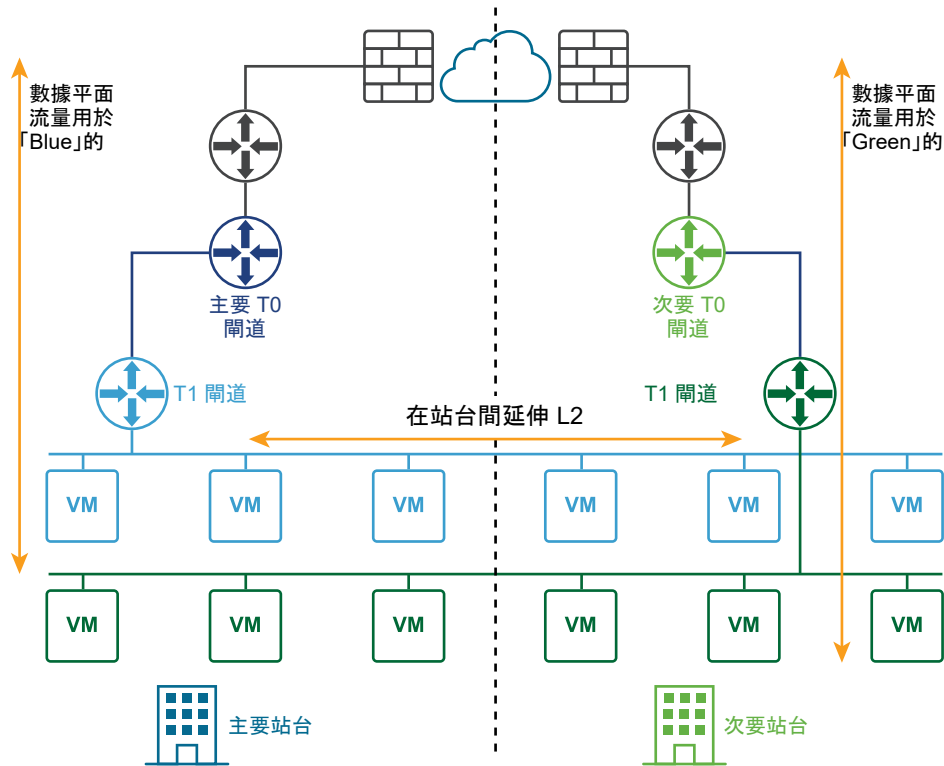
- 災害復原
- 雙主動

下圖說明災害復原部署。



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。



您可以為管理平面和資料平面部署自動或手動/指令碼式復原的兩個站台。

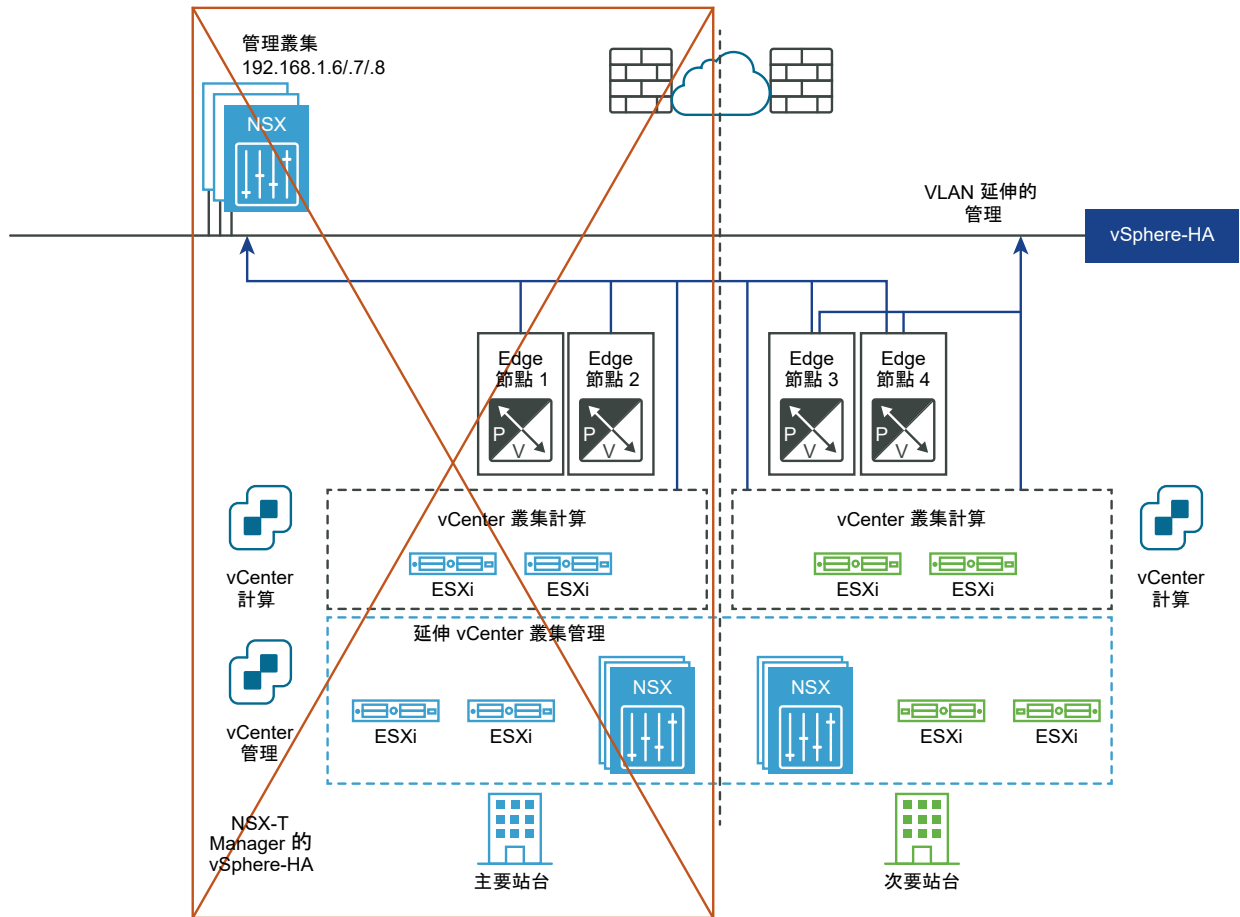
管理平面的自動復原

需求：

- 在設定的站台間具有 HA 的延伸 vCenter 叢集。
- 延伸的管理 VLAN。

NSX Manager 叢集會部署在管理 VLAN 上，並且實際位於主要站台中。如果主要站台故障，vSphere HA 將會重新啟動次要站台中的 NSX Manager。所有傳輸節點會自動重新連線至重新啟動的 NSX Manager。此程序需要大約 10 分鐘。在此期間，管理平面無法使用，但資料平面不會受到影響。

下圖說明管理平面的自動復原。



資料平面的自動復原

需求：

- Edge 節點之間的最大延遲時間為 10 毫秒。
- 第 0 層閘道的 HA 模式必須為主動-待命模式，且容錯移轉模式必須為先佔式。

附註：第 1 層閘道的容錯移轉模式可以是先佔式，也可以是非先佔式。

組態步驟：

- 使用 API 建立兩個站台的失敗網域，例如 FD1A-Preferred_Site1 和 FD2A-Preferred_Site1。將參數 preferred_active_edge_services 設定為主要站台的 true，並將其設定為次要站台的 false。

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Site1",
  "preferred_active_edge_services": "true"
}

POST /api/v1/failure-domains
```



```
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- 使用 API，設定延伸到兩個站台的 Edge 叢集。例如，叢集在主要站台中有 Edge 節點 EdgeNode1A 和 EdgeNode1B，而在次要站台中有 Edge 節點 EdgeNode2A 和 EdgeNode2B。作用中的第 0 層和第 1 層閘道將在 EdgeNode1A 和 EdgeNode1B 上執行。待命第 0 層和第 1 層閘道將在 EdgeNode2A 和 EdgeNode2B 上執行。
- 使用 API，將每個 Edge 節點與該站台的失敗網域建立關聯。先呼叫 GET /api/v1/transport-nodes/<transport-node-id> API 以取得有關 Edge 節點的資料。使用 GET API 的結果作為 PUT /api/v1/transport-nodes/<transport-node-id> API 的輸入，並適當地設定其他內容 failure_domain_id。例如，

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- 使用 API 設定 Edge 叢集，以根據失敗網域配置節點。先呼叫 GET /api/v1/edge-clusters/<edge-cluster-id> API 以取得有關 Edge 叢集的資料。使用 GET API 的結果作為 PUT /api/v1/edge-clusters/<edge-cluster-id> API 的輸入，並適當地設定其他內容 allocation_rules。例如，

```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}

PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}
```

```

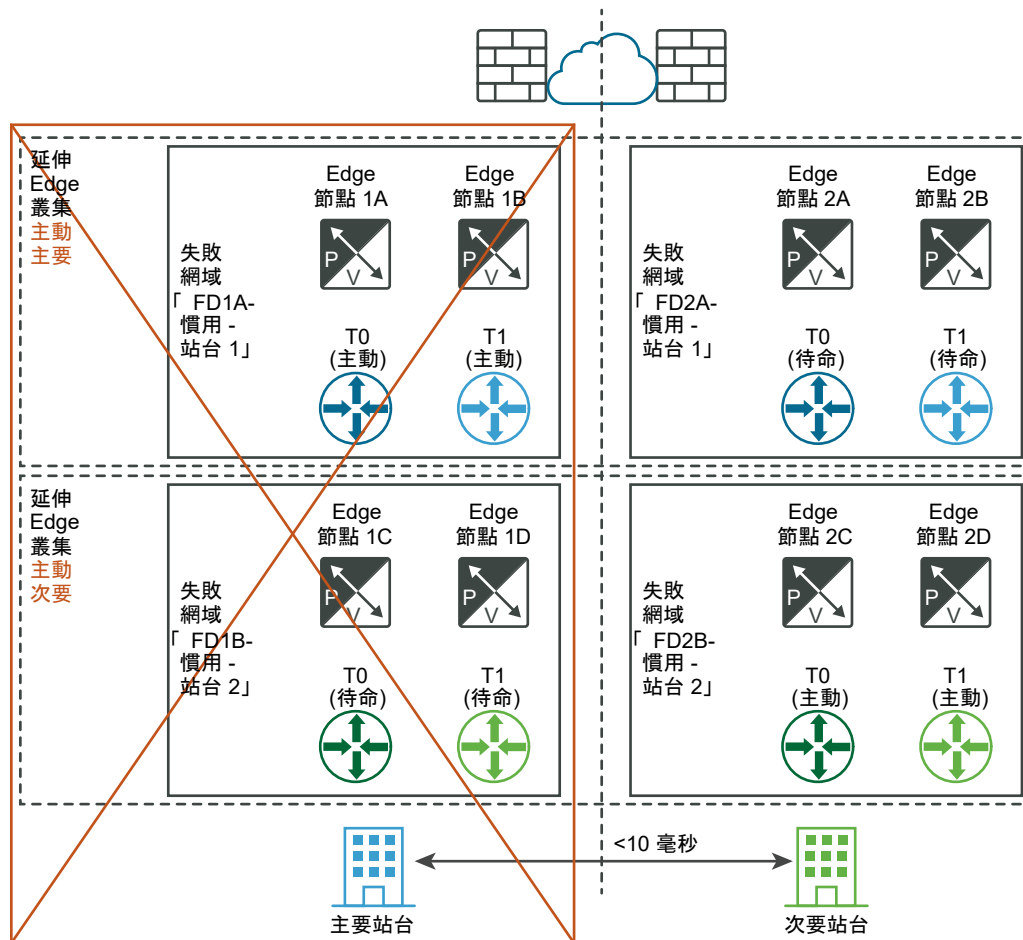
"allocation_rules": [
  {
    "action": {
      "enabled": true,
      "action_type": "AllocationBasedOnFailureDomain"
    }
  },
],
}

```

- 使用 API 或 NSX Manager UI 建立第 0 層和第 1 層閘道。

當主要站台中的 Edge 節點故障時，該節點上主控的第 0 層和第 1 層閘道將會遷移到次要站台中的 Edge 節點。

下圖說明資料平面的自動復原。



管理平面的手動/指令碼式復原

需求：

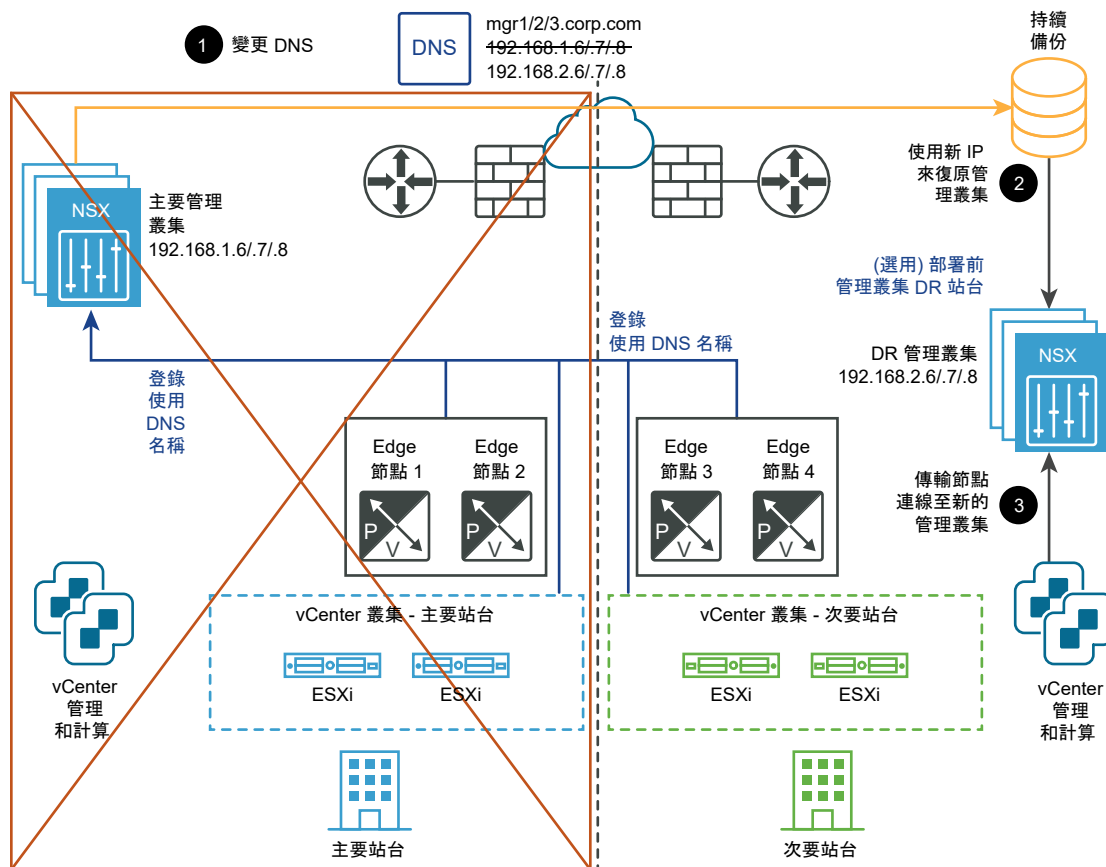
- NSX Manager 的 DNS 具有短 TTL (例如，5 分鐘)。
- 持續備份。

不需要 vSphere HA 和延伸的管理 VLAN。NSX-T Manager 必須與具有短 TTL 的 DNS 名稱相關聯。所有傳輸節點 (Edge 節點和 Hypervisor) 必須使用其 DNS 名稱連線至 NSX Manager。若要節省時間，您可以選擇性地在次要站台中預先安裝 NSX Manager 叢集。

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。

下圖說明管理平面的手動/指令碼式復原。



資料平面的手動/指令碼式復原

需求：

- Edge 節點之間的最大延遲時間為 150 毫秒。

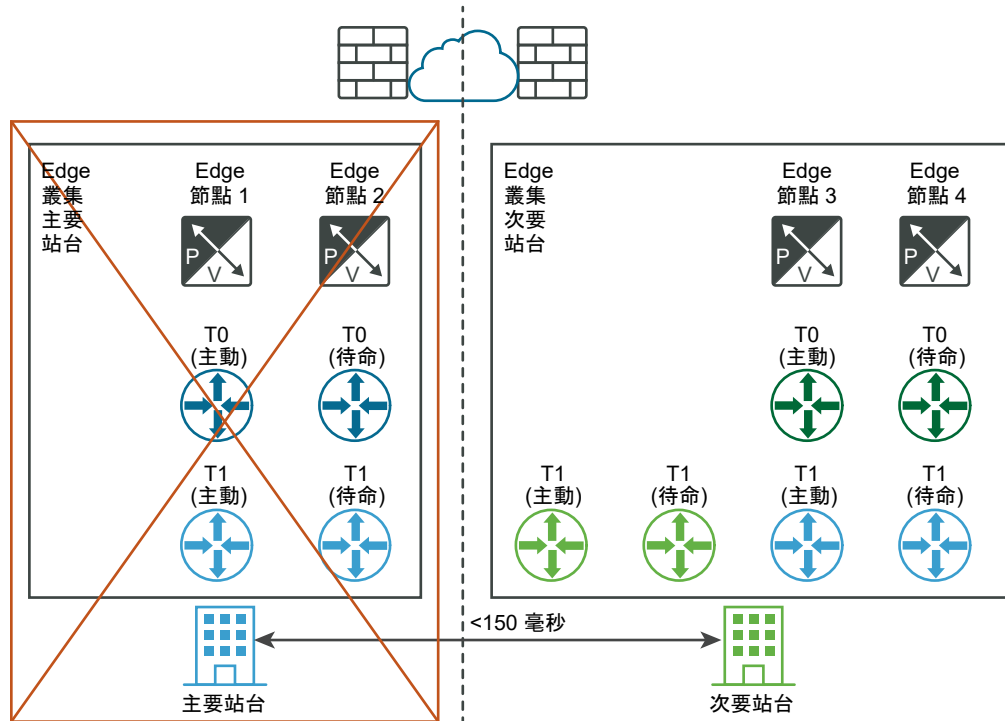
Edge 節點可以是虛擬機器或裸機。第 0 層閘道可以是主動-待命或雙主動。Edge 節點虛擬機器可以安裝在不同的 vCenter Server 中。不需要 vSphere HA。

復原步驟如下：

- 1 在災害復原 (DR) 站台中的現有 Edge 叢集上建立待命第 0 層閘道。

- 2 使用 API，將連線至第 0 層閘道的第 1 層閘道移至 DR 站台中的第 0 層閘道。
- 3 使用 API 將獨立的第 1 層閘道移至 DR 站台。
- 4 使用 API 將第 2 層橋接器移至 DR 站台。

下圖說明資料平面的手動/指令碼式復原。



來自 Edge 叢集主要站台針對所有 T1 (藍色) 所執行的指令碼或手動動作：

- 傳輸到 Edge 叢集次要站台
- 連線至 T0 - 次要 (綠色)

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。
- 第 0 層閘道的 HA 模式必須為主動-待命模式，且容錯移轉模式必須為先佔式。

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。
- 計算災害復原軟體必須支援 NSX-T Data Center，例如 VMware SRM 8.1.2 或更新版本。

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 21-7. 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	<code>set timezone <timezone></code>	PUT <a href="https://<nsx-mgr>/api/v1/node">https://<nsx-mgr>/api/v1/node
設定 NTP 伺服器	<code>set ntp-server <ntp-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/services/ntp">https://<nsx-mgr>/api/v1/node/services/ntp
設定 DNS 伺服器	<code>set name-servers <dns-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/name-servers">https://<nsx-mgr>/api/v1/node/network/name-servers
設定 DNS 搜尋網域	<code>set search-domains <domain></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/search-domains">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：

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced (可從 NSX-T Data Center 2.5.1 取得)
- NSX Enterprise (可從 NSX-T Data Center 2.5.1 取得)

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。擁有預設評估授權時，您可以指派新的評估授權。新的評估授權會覆寫預設評估授權。您也可以取消指派非預設評估授權。在此情況下，預設評估授權將會還原。

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。

如果您的授權將在 60 天內到期或已到期，則您登入 NSX Manager 後，將會出現通知視窗對您告知該情況。您也可以按一下視窗右上角的通知圖示來查看通知。

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 報告會列出下列功能的虛擬機器、CPU、唯一的並行使用者、vCPU 和核心使用率數量：

- 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

備註 Limited Export 版本已停用下列功能：

- IPSec VPN
 - 以 HTTPS 為基礎的負載平衡器
-

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。
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。

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 若要取代理管理節點的憑證，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
```

附註：憑證鏈結必須採用「憑證 - 中繼 - 根」的業界標準順序。

如需 API 的詳細資訊，請參閱《NSX-T Data Center API 參考》。

5 若要取代理管理程式叢集 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
```

附註：憑證鏈結必須採用「憑證 - 中繼 - 根」的業界標準順序。

如需 API 的詳細資訊，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----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTZEMMAoGA1 UECBMD UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbmBkG A1UEAxMSU1NMZW5IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA OGCSqG SIB3DQEBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyySOtYscz8o07avwBxTiMpDEQg== -----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。

符合性組態

可將 NSX-T Data Center 設定為使用 FIPS 140-2 驗證的密碼編譯模組，以在 FIPS 相容模式中執行。模組會根據 NIST 密碼編譯模組驗證方案 (CMVP) 的 FIPS 140-2 標準進行驗證。

FIPS 符合性的所有例外狀況都可使用符合性報告來擷取。如需詳細資訊，請參閱[檢視符合性狀態報告](#)。

NSX-T Data Center 2.5 中使用下列驗證模組：

- VMware OpenSSL FIPS 物件模組版本 2.0.9：憑證 #2839
- VMware OpenSSL FIPS 物件模組版本 2.0.20-vmw：憑證 #3550
- BC-FJA (Bouncy Castle FIPS Java API) 版本 1.0.1：憑證 #3152
- VMware 的 IKE 密碼編譯模組版本 1.1.0：憑證 #3435
- VMware 的 VPN 密碼編譯模組版本 1.0：憑證 #3542

您可以在這裡找到有關 VMware 對 FIPS 140-2 標準完成驗證的密碼編譯模組詳細資訊：<https://www.vmware.com/security/certifications/fips.html>。

依預設，負載平衡器使用已關閉 FIPS 模式的模組。您可以為負載平衡器所使用的模組啟用 FIPS 模式。如需詳細資訊，請參閱[設定負載平衡器的全域 FIPS 符合性模式](#)。

檢視符合性狀態報告

您可以檢視 NSX-T Data Center 功能的符合性報告。您可以使用報告來設定您的 NSX-T Data Center 環境，以符合您的 IT 原則和產業標準。

符合性報告包含每個不相容組態的相關資訊。

表 21-8. 符合性報告資訊

符合性報告欄	說明	範例
非符合性代碼	用於識別非符合性類型的代碼。	72301
說明	非符合性類型的說明。	憑證未經過 CA 簽署。
資源名稱	受影響資源的名稱或識別碼。	nsx-manager-1
資源類型	受影響的資源類型。	CertificateComplianceReporter
受影響的資源	受影響的資源數目。如果存在不相容的組態但未使用此功能，則此數字可以為 0。	1

您也可以使用 API 來擷取報告：GET /policy/api/v1/compliance/status。

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 從首頁頁面，按一下[監控儀表板 > 符合性報告](#)。

符合性狀態報告代碼

您可以找到有關符合性狀態報告之意義的詳細資訊。

表 21-9. 符合性報告代碼

代碼	說明	符合性狀態來源	修復
72001	加密已停用。	如果 VPN IPSec 設定檔組態包含 NO_ENCRYPTION、NO_ENCRYPTION_AUTH_AES_GMAC_128、NO_ENCRYPTION_AUTH_AES_GMAC_192 或 NO_ENCRYPTION_AUTH_AES_GMAC_256 encryption_algorithms，則會報告此狀態。 此狀態會影響使用所報告不相容組態的 IPSec VPN 工作階段組態。	若要修復此狀態，請新增使用相容加密演算法的 VPN IPSec 設定檔，並在所有 VPN 組態中使用該設定檔。請參閱 新增 IPSec 設定檔 。
72011	具有芳鄰略過完整性檢查的 BGP 訊息。未定義訊息驗證。	如果未對 BGP 芳鄰設定密碼，則會報告此狀態。 此狀態會影響 BGP 芳鄰組態。	若要修復此狀態，請在 BGP 芳鄰上設定密碼，並將第 0 層間道組態更新為使用該密碼。請參閱 設定 BGP 。
72012	與 BGP 芳鄰的通訊使用弱式完整性檢查。MD5 用於訊息驗證。	如果對 BGP 芳鄰密碼使用 MD5 驗證，則會報告此狀態。 此狀態會影響 BGP 芳鄰組態。	沒有可用的修復，因為 NSX-T Data Center 僅支援 BGP 的 MD5 驗證。
72021	使用了 SSL 第 3 版來建立安全通訊端連線。建議執行 TLSv 1.1 或更高版本，並完全停用具有通訊協定弱點的 SSLv3。	如果已在負載平衡器用戶端 SSL 設定檔、負載平衡器伺服器 SSL 設定檔，或負載平衡器 HTTPS 監視器中設定 SSL 第 3 版，則會報告此狀態。 此狀態會影響下列組態： <ul style="list-style-type: none"> ■ 與 HTTPS 監視器相關聯的負載平衡器集區。 ■ 與負載平衡器用戶端 SSL 設定檔或伺服器 SSL 設定檔相關聯的負載平衡器虛擬伺服器。 	若要修復此狀態，請設定使用 TLS 1.1 或更新版本的 SSL 設定檔，並在所有負載平衡器組態中使用此設定檔。請參閱 新增 SSL 設定檔 。

表 21-9. 符合性報告代碼 (續)

代碼	說明	符合性狀態來源	修復
72022	使用了 TLS 第 1.0 版來建立安全通訊端連線。建議執行 TLSv 1.1 或更高版本，並完全停用具有通訊協定弱點的 TLSv1.0。	如果已在負載平衡器用戶端 SSL 設定檔、負載平衡器伺服器 SSL 設定檔，或負載平衡器 HTTPS 監視器中設定 TLSv1.0，則會報告此狀態。 此狀態會影響下列組態： <ul style="list-style-type: none"> ■ 與 HTTPS 監視器相關聯的負載平衡器集區。 ■ 與負載平衡器用戶端 SSL 設定檔或伺服器 SSL 設定檔相關聯的負載平衡器虛擬伺服器。 	若要修復此狀態，請設定使用 TLS 1.1 或更新版本的 SSL 設定檔，並在所有負載平衡器組態中使用此設定檔。請參閱 新增 SSL 設定檔 。
72023	使用了弱式 Diffie-Hellman 群組。	如果 VPN IPSec 設定檔或 VPN IKE 設定檔組態包含下列 Diffie-Hellman 群組：2、5、14、15 或 16，則會報告此錯誤。群組 2 和 5 是弱式 Diffie-Hellman 群組。群組 14、15 和 16 不是弱式群組，但並非 FIPS 相容。 此狀態會影響使用所報告不相容組態的 IPSec VPN 工作階段組態。	若要修復此狀態，請將 VPN 設定檔設定為使用 Diffie-Hellman 群組 19、20 或 21。請參閱 新增設定檔 。
72024	負載平衡器 FIPS 全域設定已停用。	如果已停用負載平衡器 FIPS 全域設定，則會報告此錯誤。此狀態會影響所有負載平衡器服務。	若要修復此狀態，請針對負載平衡器啟用 FIPS。請參閱 設定負載平衡器的全域 FIPS 符合性模式 。
72200	沒有足夠的真實熵可用。	使用偽隨機數字產生器來產生熵，而非依賴硬體產生的熵時，會報告此狀態。 不使用硬體產生的熵，因為 NSX Manager 節點沒有所需的硬體加速支援，無法建立足夠的真實熵。	若要修復此狀態，您可能需要使用較新的硬體來執行 NSX Manager 節點。最新的硬體支援此功能。 備註 如果基礎結構是虛擬的，您將無法取得真實熵。
72201	熵來源未知。	當沒有任何熵狀態可用於指示的節點時，會報告此狀態。	若要修復此狀態，請確認指示的節點正確運作。
72301	憑證未經過 CA 簽署。	當其中一個 NSX Manager 憑證未經過 CA 簽署時，會報告此狀態。NSX Manager 使用下列憑證： <ul style="list-style-type: none"> ■ Syslog 憑證。 ■ 個別 NSX Manager 節點的 API 憑證。 ■ 用於 NSX Manager VIP 的叢集憑證。 	若要修復此狀態，請安裝 CA 簽署的憑證。請參閱 設定憑證 。

設定負載平衡器的全域 FIPS 符合性模式

負載平衡器的 FIPS 符合性具有全域設定。依預設，此設定會關閉以提升效能。

變更負載平衡器 FIPS 符合性的全域組態會影響新的負載平衡器執行個體，但不會影響任何現有負載平衡器執行個體。

如果負載平衡器 FIPS 的全域設定 (lb_fips_enabled) 設定為 *true*，新的執行個體負載平衡器會使用符合 FIPS 140-2 的模組。現有負載平衡器執行個體可能會使用不符合的模組。

若要让變更在現有負載平衡器上生效，您必須從第 1 層閘道中斷連結，然後重新連結負載平衡器。

您可以使用 `GET /policy/api/v1/compliance/status` 檢查負載平衡器的全域 FIPS 符合性狀態。

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
    "is_valid": true
  },
  "affected_resources": [
    {
      "path": "/infra/lb-services/LB_Service",
      "target_id": "/infra/lb-services/LB_Service",
      "target_display_name": "LB_1",
      "target_type": "LBService",
      "is_valid": true
    }
  ]
},
...
```

備註 符合性報告會顯示負載平衡器 FIPS 符合性的全域設定。任何指定的負載平衡器執行個體都可以有不同於全域設定的 FIPS 符合性狀態。

程序

1 擷取負載平衡器的全域 FIPS 設定。

GET `https://nsx-mgr1/policy/api/v1/infra/global-config`

回應本文範例：

```
{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
}
```



```

    "path": "/infra/global-config",
    "relative_path": "global-config",
    "marked_for_delete": false,
    "_create_user": "system",
    "_create_time": 1561225479619,
    "_last_modified_user": "admin",
    "_last_modified_time": 1561937915337,
    "_system_owned": true,
    "_protection": "NOT_PROTECTED",
    "_revision": 2
  }

```

2 變更負載平衡器的全域 FIPS 設定。

當您建立新的負載平衡器執行個體時，會使用全域設定。變更此設定不會影響現有的負載平衡器執行個體。

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

要求本文範例：

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}

```

回應本文範例：

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}

```

- 如果您想讓任何現有負載平衡器執行個體使用此全域設定，您必須從第 1 層閘道中斷連結，然後重新連結負載平衡器。

注意 從第 1 層閘道中斷連結負載平衡器會導致負載平衡器執行個體的流量中斷。

- 導覽到 **網路 > 負載平衡**。
- 在您想要中斷連結的負載平衡器上，按一下三點功能表 (⋮)，然後按一下 **編輯**。
- 按一下 (⊗)，然後按一下 **儲存** 以從第 1 層閘道中斷連結負載平衡器。

名稱	大小	第 1 層閘道
LB_1	小	TLR1_LR

- 按一下三點功能表 (⋮)，然後按一下 **編輯**。
- 從 **第 1 層閘道** 下拉式功能表中，選取正確的閘道，然後按一下 **儲存** 將負載平衡器重新連結至第 1 層閘道。

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

- 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 > 支援服務包**。
- 選取目標節點。
可用的節點類型包含 **管理節點**、**Edge**、**主機** 和 **公有雲端閘道**。
- (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。
- (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。

- (選擇性) 選取將服務包上傳至遠端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 若未設定將服務包傳送至遠端檔案伺服器的選項，請按一下**下載**以下載服務包。

如果磁碟空間不足，則管理程式節點的服務包收集可能會失敗。如果您遇到錯誤，請檢查失敗節點上是否存在較舊的支援服務包。使用失敗管理程式節點的 IP 位址登入至其 NSX Manager UI，然後從該節點起始服務包收集。當 NSX Manager 提示時，請下載舊版服務包或將其刪除。

記錄訊息和錯誤碼

NSX-T Data Center 元件會寫入目錄 `/var/log` 中的記錄檔。在 NSX-T 應用裝置和 KVM 主機上，NSX Syslog 訊息會符合 RFC 5424。在 ESXi 主機上，Syslog 訊息會符合 RFC 3164。

檢視記錄

在 NSX-T 應用裝置上，Syslog 訊息位於 `/var/log/syslog` 中。在 KVM 主機上，Syslog 訊息位於 `/var/log/vmware/nsx-syslog` 中。

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

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

這些記錄檔包括：

名稱	說明
auth.log	授權記錄
controller	控制器記錄
controller-error	控制器錯誤記錄
http.log	HTTP 服務記錄
kern.log	核心記錄
manager.log	Manager 服務記錄
node-mgmt.log	節點管理記錄
policy.log	原則服務記錄
Syslog	系統記錄

在 Hypervisor 中，您可以使用 `tac`、`tail`、`grep` 和 `more` 等 Linux 命令來檢視記錄。

每個 Syslog 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。

此稽核記錄是 Syslog 的一部分。您可以利用 structured-data 欄位中的字串 audit="true" 來識別稽核記錄訊息。例如：

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

每個 API 呼叫都會產生一個稽核記錄訊息。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 和 RFC 3164 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。

記錄訊息格式

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.
```

錯誤碼

如需錯誤代碼的清單，請參閱知識庫文章 [71077 NSX-T Data Center 2.x Error Codes \(NSX-T Data Center 2.x 錯誤碼\)](#)。

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

- 請自行熟悉 CLI 命令 `set logging-server`。如需詳細資訊，請參閱《NSX-T CLI 參考》。
- 如果您在 NSX CLI 中使用 TLS 或 LI-TLS 通訊協定來設定記錄伺服器的安全連線，則伺服器和用戶端憑證必須儲存在每個 NSX-T Data Center 應用裝置上的 `/image/vmware/nsx/file-store` 中。請注意，只有在使用 CLI NSX 設定匯出工具時，才需要檔案存放區中的憑證。如果您使用 API，則不需要使用檔案存放區。完成 Syslog 匯出工具設定後，您必須從這個位置刪除所有的憑證和金鑰，以免產生潛在的安全性漏洞。
- 若要設定記錄伺服器的安全連線，請確認已為伺服器設定 CA 簽署的憑證。例如，如果您使用 Log Insight 伺服器 `vrli.prome.local` 作為記錄伺服器，則可以從用戶端執行下列命令，以查看伺服器上的憑證鏈結：

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

程序

- 1 若要在 NSX-T Data Center 應用裝置上設定遠端記錄，請執行下列命令，以設定記錄伺服器 and 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>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

您可以執行此命令多次，以新增多個組態。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
```

若要僅將稽核記錄轉送至遠端伺服器，請在 structured-data 參數中指定 audit="true"。例如：

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 若要使用 LI-TLS 通訊協定設定安全遠端記錄，請指定 proto li-tls 參數。例如：

```
set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt
```

如果設定成功，您將會收到不含任何文字的提示。若要查看伺服器憑證鏈結的內容 (中繼後面是根)，請以 root 的身分登入，並執行下列命令：

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-
chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
```

```

SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

成功和失敗情況的記錄均位於 `/var/log/loginsight-agent/liagent_2020-MM-DD-<file-num>.log` 中。如果設定成功，您可以使用下列命令來檢視 Log Insight 的組態：

```

root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
;
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" )}

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no

```

3 若要使用 TLS 通訊協定設定安全遠端記錄，請指定 `proto tls` 參數。例如：

```

set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem

```

請注意下列事項：

- `serverCA` 參數只需要根憑證，而不需要完整鏈結。
- 如果 `clientCA` 與 `serverCA` 不同，則只需要根憑證。
- 憑證應保留 NSX Manager 的完整鏈結 (應符合 NDcPP 標準 - EKU、BASIC 和 CDP (CDP - 可忽略此檢查))

您可以檢查每個憑證的內容。例如：

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1:  DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5:  36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1:  D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5:  94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
    SHA1:  42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
    SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1:  DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
```



```

SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

/var/log/syslog 中的成功記錄範例：

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514

```

在 /var/log/syslog 中記錄失敗的範例：

```

<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"] Certificate trust
check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied

```

```
key', 'status': 'ERROR'})
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"] Failed to create
certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

您可以使用下列命令檢查憑證與私密金鑰是否相符。如果相符，則輸出將為 writing RSA key。若是任何其他輸出，皆表示兩者不相符。例如：

```
root@cserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

私密金鑰已損毀的範例：

```
root@cserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIICIJANBgqhkiG9w0BAQEFAAOCAg8AMIICGgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCwd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Z1OUtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEGICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZYlly
```

```
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwk2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----
```

私密金鑰和憑證皆有效，但兩者不相符的範例：

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthtUP8khCWd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Zl0Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICLl76crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZYlly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwk2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX2l6u5Jl4/X/pUDI/YHmIf06bsZlr/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DffYUH1L
> W0NUN9ydn+fAl2Uf02liuDqVy9V8AH3ON6fu+QCA8nt7lzkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe0Oe
> HCdxGMLrUtMqxIItJahEsqvMufyqNYecVscYXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwvYnssmgE13Af0nScmfM96k9h5joHVEkWK608v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDFWxxKyTy6GBRPP+8F+Jq9lyGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHawcCAwEAAQ==
```

4 若要檢視記錄組態，請執行 `get logging-server` 命令。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
```

5 若要清除遠端記錄組態，請執行下列命令：

```
nsx> clear logging-servers
```

6 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
```

7 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 21-10. 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
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

表 21-10. 記錄訊息識別碼 (續)

訊息識別碼	範例
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
MONITORING	SNMP 連接埠連線 Traceflow
-	所有其他記錄訊息。

對 Syslog 問題進行疑難排解

如果遠端記錄伺服器未收到記錄，請執行下列步驟。

- 確認遠端記錄伺服器的 IP 位址。
- 確認 `level` 參數已正確設定。
- 確認 `facility` 參數已正確設定。
- 如果通訊協定為 TLS，請將通訊協定設定為 UDP，以查看是否憑證不相符。
- 如果通訊協定為 TLS，請確認已在兩端開啟連接埠 6514。
- 移除訊息識別碼篩選器，並查看伺服器是否收到記錄。
- 使用命令 `restart service rsyslogd` 重新啟動 rsyslog 服務。

在應用裝置虛擬機器上設定序列記錄

您可以在應用裝置虛擬機器上設定序列記錄，以在虛擬機器當機時擷取記錄訊息。

程序

- 1 以 root 身分登入虛擬機器。
- 2 編輯 /etc/default/grub。
- 3 尋找參數 GRUB_CMDLINE_LINUX_DEFAULT 並附加 console=ttyS0 console=tty0。
- 4 執行命令 update-grub2。
- 5 確認 /boot/grub/grub.cfg 檔案是否已在步驟 3 中進行變更。
- 6 關閉虛擬機器的電源。
- 7 編輯虛擬機器的組態 (.vmx) 檔案，並新增下列幾行：

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 開啟虛擬機器電源。

結果

如果虛擬機器中發生核心異常，您可以在與 .vmx 檔案相同的位置找到包含記錄訊息的 serial.out 檔案。

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 [客戶經驗改進計畫] 區段中的**編輯**。
- 4 在 [編輯客戶經驗計畫] 對話方塊中，選取**加入 VMware 客戶經驗改進計畫**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。指定標記時，您也可以指定範圍。

NSX Cloud 附註 若使用 NSX Cloud，請參閱 [NSX-T Data Center 功能支援 NSX Cloud](#) 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。

多數的物件最多可以有 30 個標籤。下列物件的最大值較低，因為有些標籤是在內部建立和使用的。

表 21-11. 使用 [進階網路與安全性] 索引標籤建立之物件的標籤數目上限

物件	標籤數目上限
虛擬機器	25
邏輯連接埠	29

表 21-12. 使用 [網路]、[安全性] 或 [詳細目錄] 索引標籤建立之物件的標籤數目上限

物件	標籤數目上限
群組	29
區段	27
區段連接埠	29
邏輯路由器連接埠	30 - 標籤數目
NAT 規則	27
IPSec VPN 工作階段	29

表 21-13. Cloud Service Manager 物件的標籤數目上限

物件	標籤數目上限
BFD 健全狀況監控設定檔、傳輸區域、上行主機交換器設定檔、傳輸節點、Edge 叢集	23

表 21-14. 公有雲管理程式物件的標籤數目上限

物件	標籤數目上限
BFD 健全狀況監控設定檔、傳輸區域、邏輯交換器、節點、傳輸節點、Edge 叢集、邏輯路由器、邏輯路由器上行連接埠、靜態路由、DHCP 設定檔、NSGroup、防火牆區段規則清單	23
NAT 規則	20
IP 集合、NSGroup	22

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。標記的長度上限為 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 21-15. 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**進階網路與安全性 > 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。

設定外部負載平衡器

您可以設定外部負載平衡器，以將流量散佈到管理程式叢集中的 NSX Manager。

NSX Manager 叢集不需要外部負載平衡器。在管理程式節點失敗的情況下，NSX Manager 虛擬 IP (VIP) 可提供復原能力，但具有下列限制：

- VIP 不會在整個 NSX Manager 中執行負載平衡。
- VIP 要求所有 NSX Manager 都位於相同的子網路中。
- 在管理程式節點失敗的情況中，VIP 復原需要大約 1 - 3 分鐘的時間。

外部負載平衡器可提供下列優點：

- 在整個 NSX Manager 間的負載平衡。
- NSX Manager 可以位於不同的子網路中。
- 管理程式節點失敗時的快速復原時間。

請注意，外部負載平衡器將無法與 NSX Manager VIP 搭配使用。如果您使用外部負載平衡器，則請勿設定 NSX Manager VIP。

透過外部負載平衡器從瀏覽器存取 NSX Manager 時，必須在負載平衡器上啟用工作階段持續性。

透過外部負載平衡器從 API 用戶端存取 NSX Manager 時，有四個驗證方法可供使用 (如需詳細資訊，請參閱《NSX-T Data Center API 指南》)：

- HTTP 基本驗證 - 負載平衡器工作階段持續性不是必要的。
- 用戶端憑證驗證 - 負載平衡器工作階段持續性不是必要的。
- 向 vIDM 進行驗證 - 負載平衡器工作階段持續性不是必要的。
- 以工作階段為基礎的驗證 - 負載平衡器工作階段持續性為必要。

建議：

- 在外部負載平衡器上針對浏览器和 API 存取設定單一 IP。負載平衡器必須啟用工作階段持續性。

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 的快速導覽](#)
- [使用 NSX Cloud 隔離原則的威脅偵測](#)
- [NSX 強制執行模式](#)
- [原生雲端強制執行模式](#)
- [NSX-T Data Center 功能支援 NSX Cloud](#)
- [常見問題集 \(FAQ\)](#)

Cloud Service Manager 的快速導覽

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 (針於 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 使用 NSX Cloud 隔離原則的威脅偵測 。
在網絡視圖和卡視圖間切換	卡顯示詳細目錄的概觀。網絡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 VPC/VNet 數目。
- 您可以檢視每個 VPC/VNet 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。

每張卡片各代表您從 [雲端] 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。每個區域都有 VPC/VNet 和執行個體。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**閘道**。

雲端 > {公有雲} > VPC 或 VNet

VPC 或 VNet 區段會顯示您的公有雲詳細目錄。

您可以依帳戶和區域來篩選詳細目錄。

- 每張卡片各代表一個 VPC/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 中的覆蓋區段。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)：
 - 在 NSX 強制執行模式中啟用或停用隔離原則。
 - 提供在使用 NSX 強制執行模式時，從 NSX Cloud 讓 VPC/VNet 離線時所需的後援安全群組。請參閱[停用時的隔離原則影響](#)。
 - 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 閘道**：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 公用雲端閘道**〉。

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。

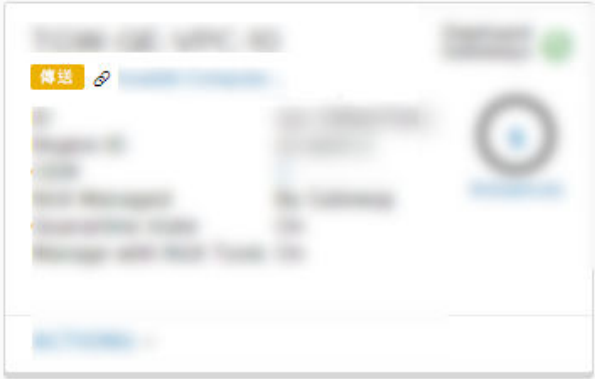
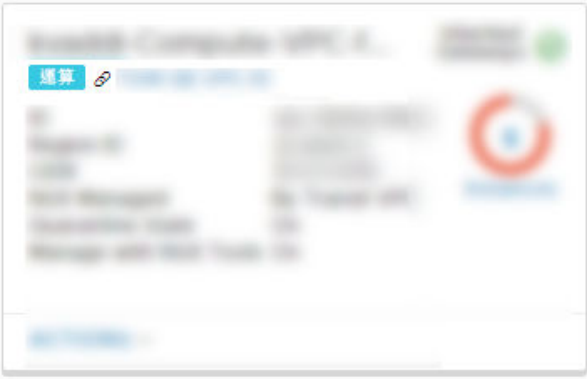
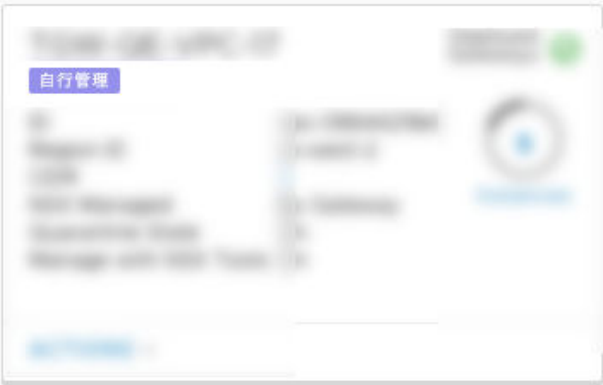
您可以在 CSM 白名單中新增或移除執行個體。如需詳細資料，請參閱[將虛擬機器加入白名單](#)。

CSM 圖示

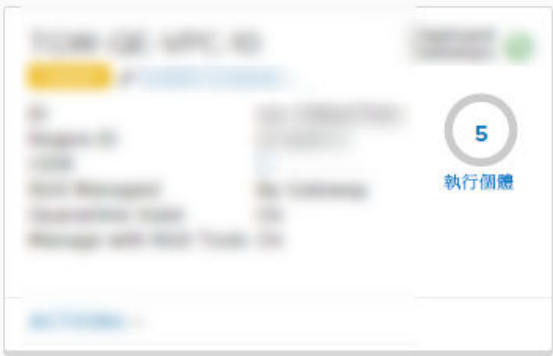
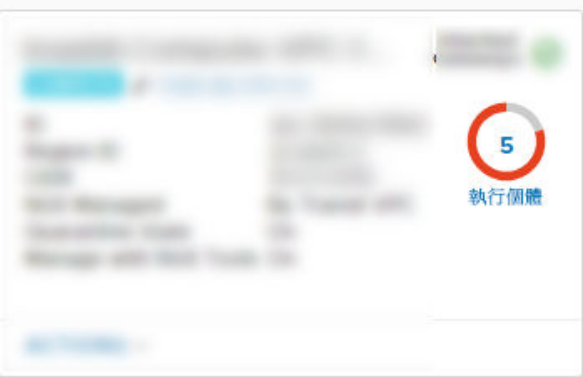
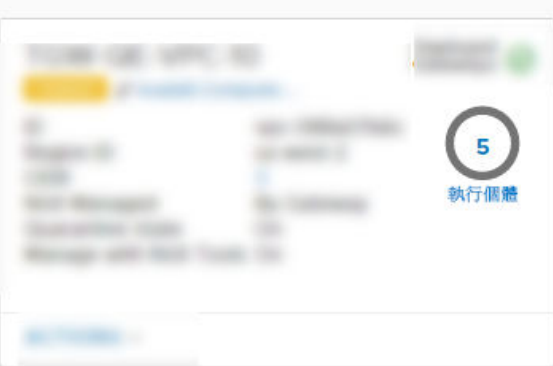
CSM 會使用說明性圖示來顯示公有雲建構的狀態和健全狀況。


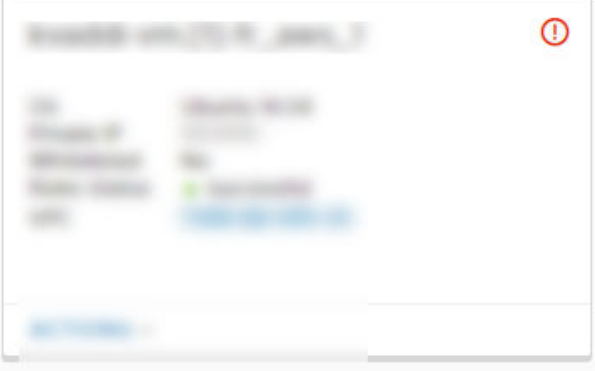
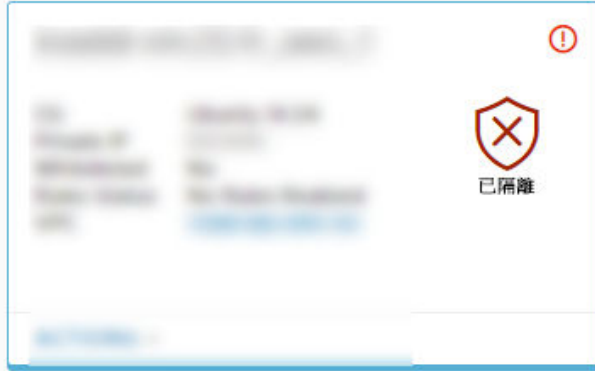
備註 在原生雲端強制執行模式中：一律會啟用隔離原則，且所有虛擬機器一律受 NSX 管理。在此模式中，僅會套用為 NSX 管理的虛擬機器啟用隔離原則的狀態。

在 NSX 強制執行模式中：可停用隔離原則，且在 VPC/VNet 中可以具有未受管理的虛擬機器。所有相關狀態均適用於此模式。

CSM 區段和圖示	說明
VPC/VNet	
	傳送 VPC/VNet
	計算 VPC/VNet
	自行管理 VPC/VNet

CSM 區段和圖示	說明
	VPC/VNet 顯示狀況良好的 PCG
	VPC/VNet 顯示處於錯誤狀態的 PCG
	VPC/VNet 顯示一個 PCG 處於錯誤狀態，另一個狀況良好。
	VPC/VNet 顯示 NSX 管理的虛擬機器。

CSM 區段和圖示	說明
	VPC/VNet 顯示未受管理的虛擬機器。
	VPC/VNet 顯示發生錯誤的虛擬機器。
	VPC/VNet 顯示已關閉電源的虛擬機器。
執行個體	

CSM 區段和圖示	說明
	NSX 管理的虛擬機器沒有錯誤。
	NSX 管理的虛擬機器發生錯誤，且隔離原則已停用。
	NSX 管理的虛擬機器發生錯誤，且隔離原則已啟用。

CSM 區段和圖示	說明
	<p>未受管理的虛擬機器已加入白名單。</p>
	<p>未受管理的虛擬機器已隔離。</p>

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。

選項	說明
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](#)。

使用 NSX Cloud 隔離原則的威脅偵測

NSX Cloud 中的隔離原則功能可為 NSX 管理的工作負載虛擬機器提供威脅偵測機制。

在兩個虛擬機器管理模式中，隔離原則會以不同的方式實作。

表 22-1. NSX 強制執行模式 和 原生雲端強制執行模式 中的隔離原則實作方式

隔離原則的相關組態	在 NSX 強制執行模式 中	在 原生雲端強制執行模式 中
預設狀態	使用 NSX Tools 部署 PCG 時會停用。您可以在 PCG 部署畫面中加以啟用，或稍後再啟用。請參閱 如何啟用或停用隔離原則 。	一律啟用。無法停用。
自動建立各個模式的唯一安全群組	為所有狀況良好、由 NSX 管理的虛擬機器指派 <code>vm-underlay-sg</code> 安全群組。	對於由 NSX 管理，且與 NSX Manager 中 Distributed Firewall 原則相符的工作負載虛擬機器，系統會建立並套用 <code>nsx-<NSX GUID></code> 安全群組。
自動建立兩種模式通用的公有雲安全群組：	<p>在 AWS 和 Microsoft Azure 中，分別將 gw 安全群組套用到各自的 PCG 介面。</p> <ul style="list-style-type: none"> ■ <code>gw-mgmt-sg</code> ■ <code>gw-uplink-sg</code> ■ <code>gw-vtep-sg</code> <p>vm 安全群組會根據其目前狀態以及隔離原則為啟用或停用，套用到由 NSX 管理的虛擬機器：</p> <ul style="list-style-type: none"> ■ Microsoft Azure 中的 <code>vm-quarantine-sg</code> 和 AWS 中的 <code>default</code>。 <p>備註 在 AWS 中，<code>default</code> 安全群組已存在。它不是由 NSX Cloud 建立的。</p>	

NSX 強制執行模式 的一般建議：

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。

NSX 強制執行模式 中的隔離原則

在 NSX 強制執行模式 中，啟用隔離原則為選用。

如何啟用或停用隔離原則

在 NSX 強制執行模式 中，您可以透過兩種方式選擇啟用隔離原則。

在傳送 VPC/VNet 上部署 PCG，或將計算 VPC/VNet 連結至傳送 VPC/VNet 時，即為第一次啟用隔離原則的可能時機。將**相關聯的 VPC/VNet 上的隔離原則**的滑桿從預設的**已停用**狀態移至**已啟用**。請參閱《NSX-T Data Center 安裝指南》中的**部署 PCG**。

您也可稍後再依照以下步驟來啟用隔離原則。

必要條件

如果您在部署或連結至 PCG 之後啟用隔離原則，則必須有一或多個傳送或計算 VPC/VNet 已在 NSX 強制執行模式 中上線 (即您選擇使用 NSX Tools 來管理工作負載虛擬機器的模式)。

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**。

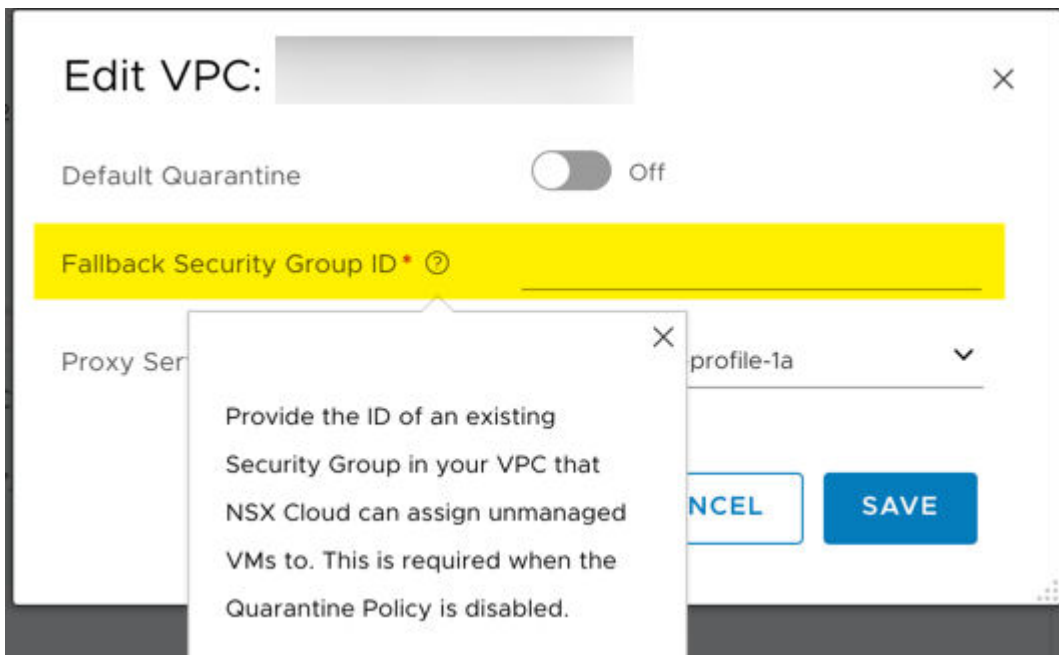


- ◆ 如果您是在 VPC 或 VNet 的頁面中，請按一下 [動作] 圖示，移至**編輯組態**。



- 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。



- 此 VPC 或 VNet 中所有未受管理的虛擬機器，都會在停用隔離原則時被指派後援安全群組。
- 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

隔離原則停用時，NSX Cloud 不會對未標記的虛擬機器管理公有雲安全群組。

但對於在公有雲中使用 `nsx.network=default` 標記的虛擬機器，NSX Cloud 會根據虛擬機器的狀態指派適當的安全群組。此行為與隔離原則啟用時相似，但隔離安全群組 `vm-quarantine-sg` (Microsoft Azure) 和 `default` (AWS) 中的規則限制較少。對已標記的虛擬機器進行安全群組的任何手動變更後，變更都將在兩分鐘內還原為 NSX Cloud 指派的安全群組。

備註 如果您不想要讓 NSX Cloud 將安全群組指派給由 NSX 管理的虛擬機器 (已標記)，請在 CSM 中將其加入白名單。請參閱[將虛擬機器加入白名單](#)。

下表顯示在隔離原則停用時，NSX Cloud 將如何管理工作負載虛擬機器的公有雲安全群組。

表 22-2. NSX Cloud 在隔離原則停用時指派公有雲安全群組的方式

虛擬機器在公有雲中是否標記了 <i>nsx.network=default</i> ?	虛擬機器是否加入白名單中？	虛擬機器在隔離原則停用時的公有雲安全群組及相關說明
已標記	未加入白名單	<ul style="list-style-type: none"> 如果虛擬機器沒有威脅：<code>vm-underlay-sg</code> 如果虛擬機器有潛在威脅 (請參閱附註)：Microsoft Azure 中的 <code>vm-quarantine-sg</code>；AWS 中的 <code>default</code> <p>備註 公有雲安全群組的指派會在 <code>nsx.network=default</code> 標籤套用至工作負載虛擬機器後的 90 秒內觸發。您仍然需要安裝 NSX Tools，虛擬機器才會由 NSX 管理。在安裝 NSX Tools 之前，已標記的工作負載虛擬機器會遭到隔離。</p>
未標記	未加入白名單	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未標記的虛擬機器採取動作。
已標記	已加入白名單	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未加入白名單的虛擬機器採取任何動作。
未標記		

下表說明如果先前啟用了隔離原則，而現在已停用，並且設定了後援安全群組來處理此 VPC/VNet 的安全群組指派時，NSX Cloud 將如何管理虛擬機器的公有雲安全群組。

表 22-3. NSX Cloud 在隔離原則從原先的啟用狀態改為停用時指派公有雲安全群組的方式

虛擬機器在公有雲中是否標記了 <i>nsx.network=default</i> ?	虛擬機器是否加入白名單中？	虛擬機器在隔離原則啟用時的現有公有雲安全群組	虛擬機器在隔離原則停用並提供了後援安全群組後的公有雲安全群組
未標記	未加入白名單	vm-quarantine-sg (Microsoft Azure) 或 default (AWS)	此虛擬機器會被指派您在停用隔離原則時所提供的後援安全群組，因為此虛擬機器未加上標籤而不會被視為由 NSX 管理，因此 NSX Cloud 會在您停用隔離原則時還原為此虛擬機器指派的安全群組。
已標記	未加入白名單	vm-underlay-sg 或 vm-quarantine-sg (Microsoft Azure) 或 default (AWS)	保留 NSX Cloud 指派的安全群組，因為在啟用或停用隔離的模式下，已標記的虛擬機器具有一致的安全群組。
已標記	已加入白名單	任何現有的公有雲安全群組	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未加入白名單的虛擬機器採取任何動作。 備註 如果您在任何 NSX Cloud 指派的安全群組中有加入白名單的虛擬機器，則必須手動將其移至指定的後援安全群組。
未標記			

啟用時的隔離原則影響

隔離原則啟用時，NSX Cloud 會管理此 VPC/VNet 中所有工作負載虛擬機器的公有雲安全群組。

對安全群組所做的任何手動變更，都將在兩分鐘內還原為 NSX Cloud 指派的安全群組。如果您不想要讓 NSX Cloud 將安全群組指派給您的虛擬機器，請在 CSM 中將虛擬機器加入白名單。請參閱[將虛擬機器加入白名單](#)。

備註 將虛擬機器從白名單中移除會導致虛擬機器還原為 NSX Cloud 指派的安全群組。

表 22-4. NSX Cloud 在隔離原則啟用時指派公有雲安全群組的方式

虛擬機器在公有雲中是否標記了 <i>nsx.network=default</i> ?	虛擬機器是否加入白名單中？	虛擬機器在隔離原則啟用時的公有雲安全群組及相關說明
已標記	未加入白名單	<ul style="list-style-type: none"> 如果虛擬機器沒有威脅：vm-underlay-sg 如果虛擬機器有潛在威脅（請參閱附註）：Microsoft Azure 中的 vm-quarantine-sg；AWS 中的 default <p>備註 公有雲安全群組的指派會在 <i>nsx.network=default</i> 標籤套用至工作負載虛擬機器後的 90 秒內觸發。您仍然需要安裝 NSX Tools，虛擬機器才會由 NSX 管理。在安裝 NSX Tools 之前，已標記的工作負載虛擬機器會遭到隔離。</p>
未標記	未加入白名單	Microsoft Azure 中的 vm-quarantine-sg；AWS 中的 default。未標記的虛擬機器會視為未受管理，因此遭到 NSX Cloud 隔離。
已標記	已加入白名單	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未加入白名單的虛擬機器採取動作。
未標記		

下表說明隔離原則從原先的停用改為啟用時，對安全群組指派有何影響：

表 22-5. NSX Cloud 在隔離原則從原先的停用狀態改為啟用時指派公有雲安全群組的方式

虛擬機器在公有雲中是否標記了 <i>nsx.network=default</i> ?	虛擬機器是否加入白名單中？	虛擬機器在隔離原則停用時的現有公有雲安全群組	虛擬機器在隔離原則啟用後的公有雲安全群組
未標記	未加入白名單	任何現有的公有雲安全群組	vm-quarantine-sg (Microsoft Azure) 或 default (AWS)
已標記	未加入白名單	vm-underlay-sg 或 vm-quarantine-sg (Microsoft Azure) 或 default (AWS)	保留 NSX Cloud 指派的安全群組，其在啟用或停用隔離的模式下，已標記的虛擬機器具有一致的安全群組。
已標記	已加入白名單	任何現有的公有雲安全群組。	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未加入白名單的虛擬機器採取任何動作。
未標記			

原生雲端強制執行模式 中的隔離原則

在 原生雲端強制執行模式 中一律會啟用隔離原則。

表 22-6. 原生雲端強制執行模式 中的公有雲安全群組指派

虛擬機器是否為有效 NSX-T 安全性原則的一部分？	虛擬機器是否加入白名單中？	虛擬機器的公有雲安全群組及相關說明
是，虛擬機器與有效的 NSX-T 安全性原則相符	未加入白名單	NSX Cloud 建立的公有雲安全群組名為 <code>nsx-{NSX-GUID}</code> ，這是 NSX-T 安全性原則的對應公有雲安全群組。
否，虛擬機器沒有有效的 NSX-T 防火牆原則	未加入白名單	Microsoft Azure 中的 <code>vm-quarantine-sg</code> 或 AWS 中的 <code>default</code> ，因為這是 NSX Cloud 的威脅偵測行為。在 原生雲端強制執行模式 中，NSX Cloud 建立的安全群組 <code>vm-quarantine-sg</code> (Microsoft Azure) 或 <code>default</code> (AWS) 會模擬預設公有雲安全性原則。 備註 在 CSM 中，虛擬機器會顯示錯誤狀態。
是，虛擬機器具有有效的 NSX-T 安全性原則	已加入白名單	保留現有的公有雲安全群組，因為 NSX Cloud 不會對未加入白名單的虛擬機器採取任何動作。
否，虛擬機器沒有有效的 NSX-T 安全性原則		

將虛擬機器加入白名單

白名單是 CSM 中的可用選項之一，適用於公有雲詳細目錄中的所有工作負載虛擬機器。

白名單在兩種虛擬機器管理模式下皆可正常運作：NSX 強制執行模式 和 原生雲端強制執行模式。

為何要將虛擬機器加入白名單？

- 在 NSX 強制執行模式 中：如果您已啟用隔離原則，並且需要使用虛擬機器上現有的應用程式來驗證任何特定的 DFW 原則，請先將這類虛擬機器加入白名單，然後再使用 NSX Cloud 將其上線。
- 在 NSX 強制執行模式 或 原生雲端強制執行模式 中：
 - 如果虛擬機器發生錯誤，而您想加以存取以解決錯誤，請將這類虛擬機器加入白名單，以便使其脫離隔離狀態，並視需要使用偵錯工具。
 - 將公有雲詳細目錄中不要由 NSX-T 管理的虛擬機器加入白名單，例如 DNS 轉寄站與 Proxy 伺服器。

如何將虛擬機器加入白名單中或從白名單中移除

請依照下列指示，將虛擬機器新增至白名單或將其移除。

必要條件

您必須有一或多個已新增至 CSM 的公有雲帳戶。

程序

- 1 使用企業管理員帳戶登入 CSM，然後移至您的公有雲帳戶。
 - a 如果使用 AWS，請移至雲端 > AWS > VPC > 執行個體。
 - b 如果使用 Microsoft Azure，請移至雲端 > Azure > VNet > 執行個體。
- 2 如果處於 [動態磚] 模式，請按一下執行個體視圖右上角的模式選取器，以切換至 [網格] 模式。

- 3 選取要加入白名單或從白名單中移除的虛擬機器 (執行個體)。
- 4 按一下 **動作**，然後選取**新增至白名單**或 **從白名單中移除**。
- 5 返回 [帳戶] 索引標籤並選取帳戶動態磚，然後按一下 **動作** > **重新同步帳戶**。

結果

每個新增至白名單的虛擬機器仍會保留在它加入白名單之前受指派的安全群組中。此時您可以視需要將任何其他安全群組套用至虛擬機器。無論隔離原則的狀態為何，NSX Cloud 都會忽略已加入白名單的虛擬機器。

如果您在 原生雲端強制執行模式 下從白名單中移除虛擬機器，或在 NSX 強制執行模式 下從白名單中移除 NSX 管理的虛擬機器，則 NSX Cloud 會根據該虛擬機器的狀態開始為其指派安全群組。

NSX 強制執行模式

在 NSX 強制執行模式 中 (也就是使用 NSX Tools 時)，您必須先在公有雲中標記虛擬機器並為其安裝 NSX Tools，讓虛擬機器上線，再使用 NSX-T Data Center 開始管理這些虛擬機器。

目前支援工作負載虛擬機器的作業系統

這是 NSX Cloud 目前針對您在 NSX 強制執行模式 中工作負載虛擬機器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。針對支援的作業系統，我們假設您使用的是標準 Linux 核心版本。具有自訂核心 (例如，修改過來源的上游 Linux 核心) 的公有雲市集映像不受支援。

- Red Hat Enterprise Linux (RHEL) 7.2、7.3、7.4、7.5、7.6
- CentOS 7.2、7.3、7.4、7.5、7.6

備註 不支援 RHEL 和 CentOS 中的 RHEL 延伸更新支援 (EUS) 核心。

備註 NSX Cloud 僅支援其發行版本與預期次要核心版本相符的 CentOS 市集映像。例如，發行版版本及其對應的核心版本應如下所示：

RHEL 版本	核心版本
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04、16.04、18.04

- Microsoft Windows Server 2016 - 服務型版本、桌面體驗 (1709、1803、1809)
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 版本 1809、1803、1709 (僅在目前 NSX Cloud 版本的 Microsoft Azure 中受到支援)

在 NSX 強制執行模式 中讓虛擬機器上線

請參閱此工作流程，以大致瞭解在 NSX 強制執行模式 中從公有雲將工作負載虛擬機器上線並進行管理的步驟。

表 22-7. 將工作負載虛擬機器在 NSX Cloud 中上線的 N 天工作流程

工作	指示
 使用索引鍵-值 <code>nsx.network=default</code> 標記工作負載虛擬機器。	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。
 在您的 Windows 與 Linux 工作負載虛擬機器上安裝 NSX Tools。	請參閱 安裝 NSX Tools
備註 如果在 Microsoft Azure VNet 的 CSM 中啟用了 自動安裝 NSX Tools ，則會自動安裝 NSX Tools。	
 (選用) 在 CSM 中，從白名單中移除所有要置於 NSX 管理下的虛擬機器。	請參閱 如何將虛擬機器加入白名單中或從白名單中移除 。
備註 加入白名單是一個手動步驟，建議您在 CSM 中新增公有雲詳細目錄後，隨即在 0 天工作流程中進行此步驟。如果未將任何虛擬機器新增至白名單，則不需要從白名單中移除虛擬機器。	

標記公有雲中的虛擬機器

將 `nsx.network=default` 標籤套用至要使用 NSX-T Data Center 來管理的虛擬機器。

程序

- 1 登入您的公有雲帳戶，並移至要由 NSX-T Data Center 管理工作負載虛擬機器的 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籤詳細資料，並儲存變更。

```
Key: nsx.network
Value: default
```

備註 在虛擬機器層級上套用此標籤。

結果

您可能已上線將 `nsx.network=default` 標籤套用至工作負載虛擬機器的 VPC/VNet。您也可以先套用標籤後將這些 VPC/VNet 上線。VPC/VNet 成功上線後，工作負載虛擬機器將會視為由 NSX 管理。

後續步驟

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

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

安裝 NSX Tools

在工作負載虛擬機器上安裝 NSX Tools

NSX Tools 有數個可用的安裝選項：

- 在個別工作負載虛擬機器中下載並安裝 NSX Tools。Linux 和 Windows 虛擬機器具有一些差異。
- 利用您的公有雲支援的方法，使用已安裝 NSX Tools 的可複寫映像，例如在 AWS 中建立 AMI，或在 Microsoft Azure 中建立受管理的映像。
- 僅限 AWS：在啟動虛擬機器時，在[使用者資料](#)中提供 NSX Tools 下載位置和安裝命令。
- 僅限 Microsoft Azure：在 Microsoft Azure VNet 中部署 PCG 時或在連結至傳送 VNet 時啟用 NSX Tools 的自動安裝，或藉由編輯傳送/計算 VNet 的組態來啟用此功能。

備註 如果您已將需要安裝 NSX Tools 的工作負載虛擬機器加入白名單，請確定下列連接埠在您指派給此類虛擬機器的安全群組中已開啟：

- 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 Tools 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。
-

在 Linux 虛擬機器上安裝 NSX Tools

若要在 Linux 工作負載虛擬機器上安裝 NSX Tools，請依照下列指示。

如需目前支援的 Linux 散發清單，請參閱[目前支援工作負載虛擬機器的作業系統](#)。

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 Tools 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 執行個體。

- 2 從畫面的 **NSX Tools 下載和安裝**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 時所選取的 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，請移至 **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。若要安裝 NSX Tools，請停用 SELinux。

- 6 NSX Tools 安裝開始後，與 Linux 虛擬機器的連線會中斷。畫面上會顯示如下的訊息：
Installation completed!!! Starting NSX Agent service. SSH connection will now be lost.。若要完成上線程序，請再次登入您的虛擬機器。

結果

您的工作負載虛擬機器上已安裝 NSX Tools。

備註

- NSX Tools 成功安裝後，工作負載虛擬機器上的連接埠 8888 會顯示為開啟，但對於底層模式下的虛擬機器會封鎖此連接埠，因此只有在進階疑難排解需要時，才必須使用此連接埠。如果 jumphost 同時位於與您要存取之工作負載虛擬機器相同的 VPC 中，則可以使用 jumphost 透過連接埠 8888 來存取工作負載虛擬機器。
- 指令碼會將 `eth0` 用作預設介面。

後續步驟

在 NSX 強制執行模式中管理虛擬機器

在 Windows 虛擬機器上安裝 NSX Tools

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

如需目前支援的 Microsoft Windows 版本的清單，請參閱[目前支援工作負載虛擬機器的作業系統](#)。

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：

- 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下傳送 VPC 或計算 VPC。
- 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。

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 **NSX Tools 下載和安裝**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，指出 NSX Tools 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

在 NSX 強制執行模式 中管理虛擬機器

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 Tools](#)

- 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。

自動安裝 NSX Tools

目前僅 Microsoft Azure 支援。

在 Microsoft Azure 中符合下列準則時，即會自動安裝 NSX Tools：

- 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。
- 對 Microsoft Azure 中的虛擬機器套用的安全群組時，必須允許安裝 NSX Tools 的存取。如果已啟用隔離原則，您可以在安裝前使用 CSM 將虛擬機器加入白名單，等到安裝後再將其從白名單中移除。
- 已使用索引鍵 `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 CSM 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。



- 如果您在 [VNet] 索引標籤中，請按一下 [動作] 圖示以移至編輯組態。



- 4 將自動安裝 NSX Tools 旁的滑桿移至 [開啟] 位置。

備註 如果 NSX Tools 安裝失敗，請執行下列動作：

- 1 登入 Microsoft Azure 入口網站，然後導覽至 NSX Tools 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=default 標籤。
- 4 在此虛擬機器上再次新增 nsx.network=default 標籤。

約在三分鐘內，NSX Tools 即會安裝在此虛擬機器上。

在 AWS 中以使用者資料安裝 NSX Tools

在 AWS VPC 中啟動新的工作負載虛擬機器時，您可以藉由在 [使用者資料] 欄位中提供 NSX Tools 下載和安裝指示來安裝 NSX Tools。

從 CSM 複製 NSX Tools 的下載和安裝指示，並在啟動新的工作負載虛擬機器時將其貼到 [使用者資料] 中。

程序

- 1 登入 AWS 主控台，並開始進行啟動新工作負載虛擬機器的程序。
- 2 在另一個瀏覽器視窗中，登入 CSM。
 - a 移至雲端 > AWS > VPC

備註 傳送 VPC/VNet 是一個或一對 PCG 部署並執行所在的位置。計算 VPC/VNet 會連結到傳送 VPC/VNet，並且可以使用其中部署的 PCG。

- b 按一下傳送 VPC 或計算 VPC。
 - c 從畫面的 **NSX Tools 下載和安裝** 區段中，根據您要用於工作負載虛擬機器的作業系統，複製 **Linux** 或 **Windows** 下方的 **下載位置與安裝命令**。
- 3 在 AWS 中，在啟動新的工作負載虛擬機器執行個體的步驟中，將下載位置和安裝命令以文字形式貼到 [進階詳細資料] 區段中 [使用者資料] 中。

結果

工作負載虛擬機器即會啟動，並在其中自動安裝 NSX Tools。

解除安裝 NSX Tools

請使用下列作業系統專用命令來解除安裝 NSX Tools。

從 Windows 虛擬機器解除安裝 NSX Tools

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
```

從 Linux 虛擬機器解除安裝 NSX Tools

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
```

在 NSX 強制執行模式中上線後的安全群組

下列安全群組組態會自動執行：

隔離原則啟用時：

- 由 NSX 管理且狀況良好的虛擬機器會移至公有雲中的 `vm-underlay-sg`。
- 未受管理的虛擬機器，或由 NSX 管理但發生錯誤的虛擬機器會移至 `default` 安全群組 (AWS) 和 `vm-quarantine-sg` 網路安全群組 (Microsoft Azure)。
- 加入白名單的虛擬機器不受影響。

隔離原則停用時：

- 由 NSX 管理且狀況良好的虛擬機器會移至公有雲中的 `vm-underlay-sg`。
- 由 NSX 管理但發生錯誤的虛擬機器會移至 `default` 安全群組 (AWS) 和 `vm-quarantine-sg` 網路安全群組 (Microsoft Azure)。
- 未受管理的虛擬機器和加入白名單的虛擬機器不受影響。

在 NSX 強制執行模式中管理虛擬機器

請依照下列步驟，開始在 NSX 強制執行模式中管理成功上線的虛擬機器。

表 22-8. NSX 管理的工作負載虛擬機器在 NSX 強制執行模式下的微分割工作流程

工作	指示
<input type="checkbox"/> 若要允許對工作負載虛擬機器的輸入存取，請視需要建立分散式防火牆 (DFW) 規則。	請參閱 NSX 強制執行模式中 NSX 管理的工作負載虛擬機器的預設連線策略 。
<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，並設定微分割。	請參閱在 NSX 強制執行模式中針對工作負載虛擬機器設定微分割 。 另請參閱： 使用 NSX-T Data Center 和公有雲標記分組虛擬機器

NSX 強制執行模式中 NSX 管理的工作負載虛擬機器的預設連線策略

當您在傳送 VPC/VNet 上部署 PCG，或將計算 VPC/VNet 連結至傳送 VPC/VNet 時，NSX Cloud 會為 NSX 管理的工作負載虛擬機器建立預設安全性原則和其中的 DFW 規則。

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](#)。

在 NSX 強制執行模式中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。

原生雲端強制執行模式

在 原生雲端強制執行模式 中，您所有的工作負載虛擬機器都會自動由 NSX 管理。請依照此處概述的工作流程，開始使用 NSX-T Data Center 來管理這些虛擬機器。

備註 所有作業系統均支援您處於 原生雲端強制執行模式 的工作負載虛擬機器。

在 原生雲端強制執行模式 中管理虛擬機器

在 原生雲端強制執行模式 中，NSX Cloud 會使用 NSX-T Data Center 群組和分散式防火牆規則，在 Microsoft Azure 中建立對應的應用程式安全群組和網路安全群組，並在 AWS 中建立安全群組。

VPC/VNet 中所有以 原生雲端強制執行模式 上線的工作負載虛擬機器都會由 NSX 管理。

請依照下列工作流程操作：

表 22-9. 工作負載虛擬機器在 原生雲端強制執行模式 下的微分割工作流程

工作	指示
<input type="checkbox"/> 在 NSX Manager 中建立一或多個群組，以納入公有雲中的工作負載虛擬機器。	請參閱在 原生雲端強制執行模式 中針對工作負載虛擬機器設定微分割 另請參閱： 使用 NSX-T Data Center 和 公有雲標記分組虛擬機器
<input type="checkbox"/> 在 NSX Manager 中建立一或多個安全性原則，並套用至您為公有雲工作負載虛擬機器建立的群組。	
<input type="checkbox"/> 使用 CSM 從白名單中移除工作負載虛擬機器 (如果您要讓 NSX-T 安全性原則加以管理)。	
<input type="checkbox"/> 在 CSM 中重新同步您的公有雲帳戶。	
<input type="checkbox"/> 從您的 VPC/VNet 切換至 CSM 中的詳細資料視圖，以對安全性原則進行疑難排解 (如果發生了任何錯誤)。	請參閱 目前的限制和常見錯誤

在 原生雲端強制執行模式 中針對工作負載虛擬機器設定微分割

請參閱此工作流程，以瞭解如何在未將 NSX Tools 安裝於工作負載虛擬機器上的情況下，在 NSX Manager 中為處於 原生雲端強制執行模式 的工作負載虛擬機器設定安全性原則。

必要條件

您必須有處於 原生雲端強制執行模式 的傳送或計算 VPC/VNet。

程序

- 1 在 NSX Manager 中，編輯或建立工作負載虛擬機器的群組，例如以 web、app、db 開頭的虛擬機器名稱可能是三個單獨的群組。如需指示，請參閱[新增群組](#)。另請參閱[使用 NSX-T Data Center 和公有雲標記分組虛擬機器](#)，以取得關於使用公有雲標籤為工作負載虛擬機器建立群組的資訊。

符合準則的工作負載虛擬機器會新增至群組。不符合任何群組準則的虛擬機器會放置在 default 安全群組中 (AWS) 以及 vm-quarantine-sg 網路安全群組中 (Microsoft Azure)。

備註 您無法使用由 NSX Cloud 自動建立的群組。

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 在 NSX Manager 中，輸入來源、目的地或套用至欄位中的群組，以建立 Distributed Firewall (DFW) 規則。如需指示，請參閱[新增分散式防火牆](#)。

備註 公有雲工作負載虛擬機器僅支援可設定狀態的原則。無狀態原則可在 NSX Manager 中建立，但不會與任何包含公有雲工作負載虛擬機器的群組進行比對。

- 3 在 CSM 中，從白名單中移除要置於 NSX 管理下的虛擬機器。如需指示，請參閱[如何將虛擬機器加入白名單中或從白名單中移除](#)。

備註 加入白名單是一個手動步驟，強烈建議您在 CSM 中新增公有雲詳細目錄後，隨即在 0 天工作流程中進行此步驟。如果您尚未將任何虛擬機器加入白名單，則不需要將其從白名單中移除。

- 4 對於在公有雲中找到相符項目的群組和 DFW 規則，系統會自動執行下列動作：

- a 在 AWS 中，NSX Cloud 會建立名稱類似於 nsx-`<NSX GUID>` 的新安全群組。
- b 在 Microsoft Azure 中，NSX Cloud 會建立與在 NSX Manager 中所建立群組相對應的應用程式安全群組 (ASG)，以及與分組工作負載虛擬機器相符之 DFW 規則對應的網路安全群組 (NSG)。

備註 NSX Cloud 每 30 秒會執行一次 NSX Manager 與公有雲群組和 DFW 規則的同步。

- 5 在 CSM 中重新同步您的公有雲帳戶：

- a 登入 CSM 並移至您的公有雲帳戶。
- b 從公有雲帳戶中，按一下動作 > **重新同步帳戶**。等待重新同步完成。
- c 移至 VPC/VNet，然後按一下紅色的錯誤指示器。這會將您導向至執行個體視圖。
- d 如果在 [網格] 中檢視，請將視圖切換至 [詳細資料]，並按一下 [規則實現] 資料行中的失敗，以檢視錯誤 (若有的話)。

後續步驟

請參閱[目前的限制和常見錯誤](#)。

目前的限制和常見錯誤

請參閱下列已知的限制和常見錯誤，以疑難排解您在 原生雲端強制執行模式 中管理公有雲工作負載虛擬機器時遇到的問題。

備註 下列限制由您的公有雲所設定：

- 可套用至工作負載虛擬機器的安全群組數目。
- 可針對工作負載虛擬機器實現的規則數目。
- 每一安全群組可實現的規則數目。
- 安全群組指派的範圍，例如，Microsoft Azure 中網路安全群組 (NSG) 的範圍限制為該區域，而 AWS 中的安全群組 (SG) 的範圍則限制為該 VPC。

如需關於這些限制的詳細資訊，請參閱公有雲說明文件。

目前的限制

目前的版本對於工作負載虛擬機器的 DFW 規則具有下列限制：

- 不支援巢狀群組。
- 不支援未以虛擬機器和/或 IP 位址作為成員的群組，例如，不支援以區段或邏輯連接埠為基礎的準則。
- 不支援將來源和目的地設為以 IP 位址或 CIDR 為基礎的群組。
- 不支援將來源和目的地皆設為「任何」。
- **Applied_To** 群組只能是來源、目的地或「來源 + 目的地」群組。不支援其他選項。
- 僅支援本機 VPC/VNet 規則強制執行。您可以在 NSX Manager 中建立跨 VPC/VNet 的群組。但是，此類規則的實現僅適用於 VPC/VNet 內。跨 VPC/VNet DFW 的規則無法實現。
- 僅支援 TCP 和 UDP。

備註 僅適用於 AWS 中：

為 AWS VPC 中工作負載虛擬機器建立的拒絕規則不會在 AWS 上實現，因為在 AWS 中，依預設會將所有項目加入黑名單。這會在 NSX-T Data Center 中導致下列結果：

- 如果 VM1 和 VM2 之間有拒絕規則，則會因為預設的 AWS 行為而不允許 VM1 與 VM2 之間的流量，而非因為拒絕規則。拒絕規則在 AWS 中無法實現。
- 假設在 NSX Manager 中為相同的虛擬機器建立了下列兩個規則，規則 1 的優先順序高於規則 2：
 - a 拒絕 VM1 至 VM2 的 SSH
 - b 允許 VM1 至 VM2 的 SSH

拒絕規則會被忽略，因為它未在 AWS 中實現，因此會實現允許 SSH 規則。這與預期相反，因為這是預設 AWS 行為所造成的限制。

常見錯誤及其解決方法

錯誤：未將任何 NSX 原則套用至虛擬機器。

如果您看到此錯誤，表示沒有任何 DFW 規則套用至特定虛擬機器。請在 NSX Manager 中編輯規則或群組，以納入此虛擬機器。

錯誤：不支援無狀態 NSX 規則。

如果您看到此錯誤，表示您已在無狀態安全性原則中新增公有雲工作負載虛擬機器的 DFW 規則。此動作不受支援。請在可設定狀態的模式中建立新的或使用現有的安全性原則。

NSX-T Data Center 功能支援 NSX Cloud

NSX Cloud 會透過在 NSX-T Data Center 中產生邏輯網路實體，來為您的公有雲 VPC 或 VNet 建立網路拓撲。

使用此清單作為參考，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。

表 22-10.

NSX-T Data Center 功能	詳細資料	NSX Cloud 附註
區段或邏輯交換器	請參閱第 4 章 區段	區段將針對每個受管理虛擬機器所連結的公有雲子網路來建立。這是混合區段。
閘道或邏輯路由器	請參閱第 2 章 第 0 層閘道與第 3 章 第 1 層閘道。	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
IPFIX	請參閱設定 IPFIX。	<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。

表 22-10. (續)

NSX-T Data Center 功能	詳細資料	NSX Cloud 附註
連接埠鏡像	請參閱 監控連接埠鏡像工作階段 。	只有目前版本中的 AWS 支援連接埠鏡像。 <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。
閘道防火牆	請參閱 設定閘道防火牆 。	僅在第 0 層閘道上受支援。

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 22-11. 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:subscript ion_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 22-12.

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

表 22-12. (續)

工作負載虛擬機器的公有雲標籤	由 NSX Cloud 探索到？	工作負載虛擬機器的對等 NSX Manager 標籤
Abcdefghijklmnopqrstuvwxyz=value2	否 (金鑰超過 20 個字元)	無
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgjgjuytreswqacvbcdefghijklmnopqrstuvwxyz	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[新增群組](#)。
- 請參閱在 [NSX 強制執行模式](#) 中針對工作負載虛擬機器設定微分割。

使用原生雲端服務

在 NSX Manager 內，支援將下列原生雲端服務與您的公有雲工作負載虛擬機器搭配使用。

部署 PCG 時，將會在 NSX Manager 中為每個支援的原生服務建立一個群組。

針對目前支援的公有雲服務，系統會建立下列群組：

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

若要使用這些原生雲端服務，請視需要在規則的來源或目的地欄位中，建立包含原生雲端服務群組的 DFW 原則。

DFW 規則會在虛擬機器上強制執行，而非在原生雲端服務上強制執行。

備註 在 NSX 強制執行模式中，也就是在使用 NSX Tools 管理工作負載時，目前並不支援 Microsoft Azure 的原生雲端服務。

目前的限制

端點			以服務作為目的地的 DFW 規則		以服務作為來源的 DFW 規則	
公有雲	服務	範圍	在虛擬機器上強制執行？	在服務上強制執行？	在服務上強制執行？	在虛擬機器上強制執行？
Microsoft Azure	BLOB 儲存區	全域	是	否	否	是
	Cosmos DB					
	SQL					
	負載平衡器					
AWS	S3	VPC 本機	是	否	否	是
	Dynamo DB					
	RDS					
	ELB					

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 22-13. 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

表 22-13. 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 (續)

頻率？	工作	指示
	設定 PCG 與服務應用裝置之間的 BGP，並從服務應用裝置通告 VSIP，以及從 PCG 通告預設路由 (0.0.0.0/0)。	請參閱 設定 BGP 和路由重新分配
	備註 在目前的版本中，服務插入僅支援南北向流量。	
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

- 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 層開道	選取為傳送 VPC/VNet 自動建立的第 0 層開道。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。

程序

- 1 導覽至網路 > 第 0 層閘道。
- 2 為傳送 VPC/VNet (例如，名為 cloud-t0-vpc-6bcd2c13) 選取自動建立的第 0 層閘道，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。
路由篩選器	設定輸出篩選器，將預設路由 (0.0.0.0/0) 從 PCG 通告至服務應用裝置。

- 5 從路由重新分配區段中，啟用第 0 層閘道上的靜態路由。



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
名稱：	提供原則的描述性名稱，例如， Azure 虛擬機器 的南北向服務插入。
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 。
套用至：	選取 PCG 的第 0 層間道。

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 。

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 22-14.

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。

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>
```

在 NSX 強制執行模式中設定 VPN

您可以使用在內部部署 NSX-T Data Center 部署中顯示為自動建立第 0 層閘道的 PCG 來設定 VPN。這些指示僅適用於在 NSX 強制執行模式中受到管理的工作負載虛擬機器。

依照此處說明的其他步驟，以您在 NSX Manager 中使用第 0 層閘道的相同方式使用 PCG，進行 VPN 的設定。您可以在部署於相同公有雲、不同公有雲，或使用內部部署閘道或路由器的 PCG 之間，建立 VPN 通道。請參閱[第 5 章 虛擬私人網路 \(VPN\)](#)，以進一步瞭解 NSX-T Data Center 中的 VPN 支援。

必要條件

- 確認您已在 VPC/VNet 中部署一個 PCG 或 PCG 的 HA 配對。
- 確認遠端對等支援以路由為基礎的 VPN 和 BGP。

程序

- 1 在您的公有雲中，找出 NSX 為 PCG 指派的本機端點，並視需要指派公用 IP 位址：
 - a 移至公有雲中的 PCG 執行個體，然後導覽至 [標籤]。
 - b 記下標籤之值欄位中的 IP 位址 `nsx.local_endpoint_ip`。

- c (選擇性) 如果您的 VPN 通道需要公用 IP，例如，如果您想要設定其他公有雲或內部部署 NSX-T Data Center 部署的 VPN：
 - 1 導覽至 PCG 執行個體的上行介面。
 - 2 將公用 IP 位址連結至您在步驟 **b** 中記下的 `nsx.local_endpoint_ip` IP 位址。
- d (選擇性) 如果您有 PCG 執行個體的 HA 配對，請重複步驟 **a** 和 **b**，並視需要連結公用 IP 位址，如步驟 **c** 中所述。

- 2 在 NSX Manager 中，為顯示為第 0 層閘道 (名稱類似於 `cloud-t0-vpc/vnet-<vpc/vnet-id>`) 的 PCG 啟用 IPsec VPN，並在這個第 0 層閘道的端點與所需 VPN 對等的遠端 IP 位址之間建立以路由為基礎的 IPsec 工作階段。如需其他詳細資料，請參閱[新增 IPsec VPN 服務](#)。

- a 移至**網路 > VPN > VPN 服務 > 新增服務 > IPsec**。提供下列詳細資料：

選項	敘述
名稱	輸入 VPN 服務的描述性名稱，例如 <code><VPC-ID>-AWS_VPN</code> 或 <code><VNet-ID>-AZURE_VPN</code> 。
第 0 層/第 1 層閘道	為公有雲中的 PCG 選取第 0 層閘道。

- b 移至**網路 > VPN > 本機端點 > 新增本機端點**。提供下列資訊，並參閱[新增本機端點](#)以取得其他詳細資料：

備註 如果您有 PCG 執行個體的 HA 配對，請為每個執行個體建立本機端點；方法是使用其在公有雲中連結的對應本機端點 IP 位址。

選項	敘述
名稱	輸入本機端點的描述性名稱，例如 <code><VPC-ID>-PCG-preferred-LE</code> 或 <code><VNET-ID>-PCG-preferred-LE</code>
VPN 服務	選取您在步驟 2a 中所建立 PCG 第 0 層閘道的 VPN 服務。
IP 位址	輸入您在步驟 1b 中記下的 PCG 本機端點 IP 位址值。

- c 移至**網路 > VPN > IPsec 工作階段 > 新增 IPsec 工作階段 > 以路由為基礎的**。提供下列資訊，並參閱[新增路由型 IPsec 工作階段](#)以取得其他詳細資料：

備註 如果您要在部署於 VPC 中的 PCG 與部署於 VNet 中的 PCG 之間建立 VPN 通道，您必須為 VPC 中每個 PCG 的本機端點以及 VNet 中 PCG 的遠端 IP 位址建立通道，並且反向地從 VNet 中的 PCG 到 VPC 中 PCG 的遠端 IP 位址建立通道。您必須為主動和備用 PCG 建立個別的通道。這會使兩個公有雲之間具有完整網格的 IPsec 工作階段。

選項	敘述
名稱	輸入 IPsec 工作階段的描述性名稱，例如 <code><VPC-ID>-PCG1-to-remote_edge</code>
VPN 服務	選取您在步驟 2a 中建立的 VPN 服務。
本機端點	選取您在步驟 2b 中建立的本機端點。
遠端 IP	輸入您要用來建立 VPN 通道之遠端對等的公用 IP 位址。 備註 如果您可以連線到私人 IP 位址 (例如，使用 DirectConnect 或 ExpressRoute)，則遠端 IP 可以是私人 IP 位址。
通道介面	輸入 CIDR 格式的通道介面。必須將相同的子網路用於遠端對等，才能建立 IPsec 工作階段。

步驟 2a.

VPN 服務

名稱	服務類型	第 0 層/第 1 層間連	工作階段	狀態
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	成功
說明	VPN service on AWS Transit VPC ID vpc-073617880a9622d93	管理狀態	已啟用	
IKE 記錄器埠	資訊	標籤	0	
工作階段同步	已啟用			

步驟 2b.

VPN 服務

名稱	VPN 服務	IP 位址	站點間連	工作階段	狀態
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	未設定	1	成功
說明	未設定	本機識別碼	10.99.3.35		
受信任的 CA 憑證	未設定	憑證檢索清單	未設定		
標籤	0				

步驟 2c.

IPSec 工作階段

名稱	類型	VPN 服務	本機端點	遠端 IP	狀態	警告
<VPC-ID>-PCG1-to-remote_edge	以路由為基礎	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	關閉	0
說明	未設定	管理狀態	已啟用	檢視統計資料		
合規性套件	無	過繼介面	192.168.50.10/24	下載組態		
驗證模式	PSK	遠端識別碼	172.0.3.145			
預先共用的金鑰					
連階內容						
IKE 設定檔	nsx-default-l3vpn-ike-profile	連線初始模式	啟動器			
IPSec 設定檔	nsx-default-l3vpn-tunnel-profile	TCP MSS 限制	已停用			

VPN 對等的 IP 位址

3 在您於步驟 2 中建立的 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](#)。

- 導覽至網路 > 第 0 層閘道
- 選取您建立 IPsec 工作階段所在的自動建立第 0 層閘道，然後按一下編輯。
- 按一下 BGP 區段下方 BGP 芳鄰旁邊的數字或圖示，並提供下列詳細資料：

選項	敘述
IP 位址	使用在 VPN 對等的 IPsec 工作階段中，於通道介面上設定之遠端 VTI 的 IP 位址。
遠端 AS 數目	此數目必須與遠端對等的 AS 數目相符。

 第 0 層閘道

新增閘道 ▾ 全部展開 依名稱

	第 0 層閘道名稱	HA 模式	連結的第 1 層閘道	連結區段
>	多點傳播			
▼	BGP			
	本機 AS	1000	SR 間 iBGP	● 開啟
	BGP	● 開啟	ECMP	● 開啟
	正常重新啟動	僅限協助程式	多重路徑放鬆	● 開啟
	正常重新啟動計時器	180 秒	正常重新啟動失效計時器	600 秒
	路由彙總	0	BGP 芳鄰	

步驟 3.

BGP 芳鄰

第 0 層閘道 cloud-to-415... #芳鄰 1

	IP 位址	BFD	遠端 AS 數目
⋮ ▼	192.168.50.11	已停用	1000
	來源位址	未設定	
	躍點數目上限	1	

- 4 使用重新分配設定檔通告您要用於 VPN 的首碼。在 NSX 強制執行模式中，在重新分配設定檔中連線已啟用第 1 層的路由。

第 0 層閘道

新增閘道

全部展開 依名稱、路徑和其他項目

第 0 層閘道名稱	HA 模式	連結的第 1 層閘道	連結區段	狀態
BGP				
路由重新分配				
路由重新分配	雙主動	0	0	成功

路由重新分配

第 0 層閘道 cloud-t0-vpc... #選取的來源

第 0 層子網路

通告的第 1 層子網路

- 已連線的介面與區段
- 服務介面子網路
- 已連線的區段

常見問題集 (FAQ)

本主題列出一些常見問題。

如何確認我的 NSX Cloud 元件已安裝且正在執行？

- 1 若要確認您工作負載虛擬機器上的 NSX Tools 已連線至 PCG，請執行以下作業：

- 輸入 `nsxcli` 命令以開啟 NSX CLI。
- 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
```

- 2 工作負載虛擬機器必須具有正確的標籤才能連線至 PCG：

- 登入 AWS 主控台或 Microsoft Azure 入口網站。
- 驗證虛擬機器的 `eth0` 或介面標籤。

`nsx.network` 金鑰必須具有值 `default`。

我使用 cloud-init 啟動的虛擬機器遭到隔離，且不允許安裝第三方工具。我該怎麼辦？

啟用隔離原則後，使用具有下列規格的 cloud-init 指令碼啟動虛擬機器時，您的虛擬機器會在啟動時遭到隔離，且您無法在其上安裝自訂應用程式或工具：

- 標記為 `nsx.network=default`
- 在虛擬機器開啟電源時自動安裝或執行啟動程序的自訂服務

解決方案：

在安裝自訂或第三方應用程式時，視需要更新 `default` (AWS) 或 `default-vnet-<vnet-ID>-sg` (Microsoft Azure) 安全群組以新增輸入/輸出連接埠。

我已正確標記虛擬機器且安裝了 NSX Tools，但虛擬機器仍遭到隔離。我該怎麼辦？

如果您遇到此問題，請嘗試下列作業：

- 檢查 NSX Cloud 標籤 `nsx.network` 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？

從公有雲 (AWS 或 Microsoft Azure)：

- 1 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[使用 NSX Cloud 隔離原則的威脅偵測](#)。
 - NSX-T Data Center DFW 規則。如需詳細資料，請參閱[NSX 強制執行模式中 NSX 管理的工作負載虛擬機器的預設連線策略](#)。
 - Linux 上的 Windows 防火牆或 IPTables。
- 2 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。
 - 3 您可以將已鎖定的虛擬機器重新開機。
 - 4 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。

即使在 原生雲端強制執行模式 中仍需要 PCG 嗎？

是。

在 CSM 中將我的公有雲帳戶上線後，可以變更 PCG 的 IAM 角色嗎？

是。您可以重新執行適用於公有雲的 NSX Cloud 指令碼，以重新產生 PCG 角色。重新產生 PCG 角色後，在 CSM 中使用新的使用者名稱編輯您的公有雲帳戶。在公有雲帳戶中部署的任何新 PCG 執行個體將使用新角色。

請注意，現有的 PCG 執行個體會繼續使用舊的 PCG 角色。如果您想要更新現有 PCG 執行個體的 IAM 角色，請移至公有雲，並手動變更該 PCG 執行個體的角色。

我是否可將 NSX-T Data Center 內部部署授權用於 NSX Cloud？

是，只要您的 ELA 有其相關條款即可。

VMware NSX® Intelligence™ 提供內部部署 NSX-T Data Center 環境的安全性狀況視覺化。視覺化是根據特定期間內匯總的網路流量。NSX Intelligence 也會透過根據安全性原則強制執行的分析提供建議以協助您處理微分割規劃。

重要 您必須具有企業管理員角色，才有權限可安裝、設定和使用 NSX Intelligence。

您必須先安裝並設定 NSX Intelligence 應用裝置，才能開始使用 NSX Intelligence 功能。請參閱《NSX-T Data Center 安裝指南》中的〈安裝和設定 NSX Intelligence 應用裝置〉。

本章節討論下列主題：

- [開始使用 NSX Intelligence](#)
- [瞭解 NSX Intelligence 視圖和流量](#)
- [使用 NSX Intelligence 建議](#)
- [備份和還原 NSX Intelligence](#)
- [疑難排解 NSX Intelligence 問題](#)

開始使用 NSX Intelligence

若要開始使用 NSX Intelligence 功能，請自行熟悉 NSX Intelligence 圖形化使用者介面。

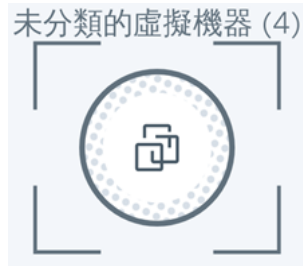
安裝並設定 NSX Intelligence 應用裝置之後，即會啟用 NSX Manager UI 之**計劃和疑難排解**索引標籤中的 NSX Intelligence 功能。在**探索和計劃**區段中，您可以使用**探索和採取動作**來虛擬化您的 NSX-T Data Center 實體，以及使用**建議**來取得微分割規劃的建議。

NSX Intelligence 首頁的導覽

您可以透過按一下 NSX Manager 使用者介面中的**計劃和疑難排解** > **探索和採取動作**來存取 NSX Intelligence 首頁。

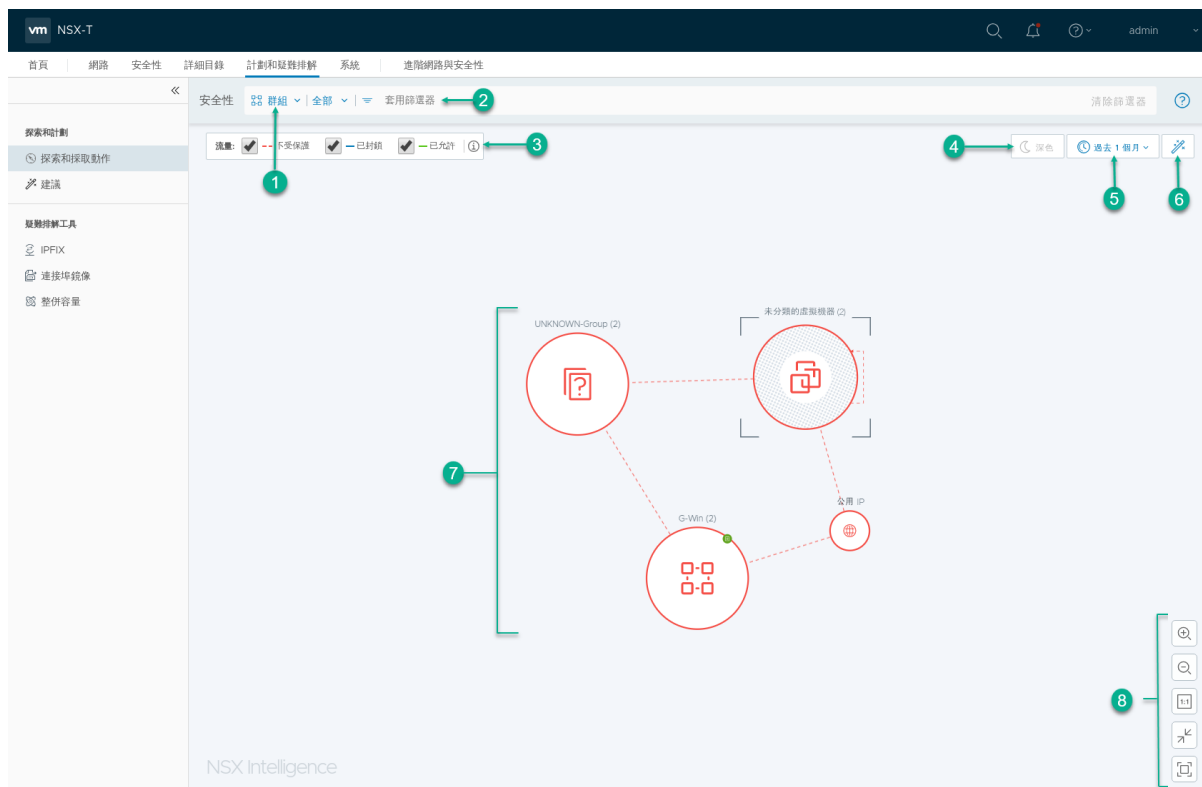
第一次安裝並設定 NSX Intelligence 之後，當您按一下**探索和採取動作**時，您可能會看到這個訊息：找不到任何資料。您可能需要修改上方的篩選器。訊息隨即顯示，因為 NSX Intelligence 尚未接收到可用來建立視覺效果的網路流量資料。已從 NSX Manager 接收到部分網路流量資料之後，NSX Intelligence 便可以開始呈現部分視覺效果。

依預設，當您按一下**探索和採取動作**時，您會看到具有過去 24 小時內群組虛擬機器成員之間不受保護流量之內部部署 NSX-T Data Center 中所有群組的安全性狀態視覺化。不受保護的網路流量是未執行任何微分割的虛擬機器之間的流量。如果尚未定義任何群組，則不會顯示任何群組。如果有虛擬機器，但不屬於任何群組，您會看到未分類虛擬機器群組的下列圖示。



如果您已定義群組，且已擷取流量資料，您可能會看到類似於下列螢幕擷取畫面的視覺效果。後續表格說明螢幕擷取畫面中編號的區段。

備註 NSX Intelligence 將屬於下列其中一個 CIDR 標記法的 IP 位址分類為私人 IP 位址：192.168.0.0/16、172.16.0.0/12 和 10.0.0.0/8。任何不屬於任何 CIDR 標記法的 IP 位址都會分類為公用 IP 位址。如果您的虛擬機器的 IP 位址不屬於其中一個 CIDR 標記法，請考慮使用《NSX-T Data Center API 指南》中的 PATCH /api/v1/intelligence/host-config API 來新增 CIDR 標記法。



區段	說明
1	<p>安全性視圖選取區域可供您選取要顯示的安全性視覺化類型。可用的安全性視圖有兩種類型：群組和虛擬機器。當您按一下探索和採取動作時，顯示的預設安全性視圖即為您 NSX-T Data Center 中過去 24 小時內包含不受保護流量的群組物件的群組視圖。</p> <ul style="list-style-type: none"> ■ 若要選取虛擬機器視圖，請按一下群組旁的向下箭頭，然後選取虛擬機器。 ■ 若要選取要包含在視圖中的特定群組或虛擬機器，請按一下全部旁的向下箭頭，然後從清單中選取。 ■ 若要清除選取項目篩選器，請按一下畫面右上方的清除篩選器。當您在虛擬機器視圖中按一下清除篩選器時，會清除選取項目篩選器，並將您置於群組視圖中。 <p>如需關於如何使用兩個視圖類型的詳細資訊，請參閱使用群組視圖和使用虛擬機器視圖。</p>
2	<p>使用套用篩選器，您可以縮小用於視覺化的準則。您可以從下拉式清單中選取要用於視覺化的準則。您可以選取虛擬機器成員、標籤、流量類型、來源 IP、目的地 IP、規則識別碼或名稱。您可以透過再次按一下套用篩選器，以定義多個要套用的篩選器。</p>
3	<p>使用此流量區段，您可以選取所選期間內要包含在視覺效果中的流量類型。此區段也會顯示視覺效果中用於流量類型的色彩。</p> <ul style="list-style-type: none"> ■ 不受保護流量的紅色調虛線 ■ 已封鎖流量的藍色調實線 ■ 已允許流量的綠色調實線 <p>依預設，已為目前的 NSX Intelligence 視覺化選取不受保護流量類型。如需詳細資訊，請參閱使用流量。</p>
4	<p>顯示模式區段會定義要用於視覺化的主題。淺色佈景主題為預設使用的模式。</p> <ul style="list-style-type: none"> ■ 若要使用深色主題模式，請按一下深色圖示。僅當您以全螢幕模式查看視覺化效果時，才能使用「深色」主題。 ■ 若要進入全螢幕模式，請按一下檢視控制區段中的 。
5	<p>在此區段中，您需要選取要用於判斷哪些網路流量資料將用於產生所需視覺效果與建議的期間。您選擇將決定用於群組或虛擬機器視圖中的歷史資料。期間相對於目前時間，而部分期間在過去。</p> <p>過去 24 小時內為預設使用的時間範圍。若要變更選取的期間，請按一下目前所選的期間，然後選取過去 1 小時、過去 12 小時、過去 24 小時、過去 1 週或過去 1 個月。</p>
6	<p>當您按一下這個「建議棒」  圖示時，[建議] 對話方塊會顯示目前視圖的詳細目錄摘要。如果您是在虛擬機器視圖中，可以透過按一下啟動新的建議來產生 NSX Intelligence 建議。請參閱使用 NSX Intelligence 建議。</p>
7	<p>此區段是內部部署 NSX-T Data Center 中群組或虛擬機器的安全性狀態的視覺效果。它也包含在所選期間內發生之網路流量的視覺效果。在此區段中，您可以指向特定節點或流量箭頭，以取得關於該特定實體的詳細資料。</p> <p>如需詳細資訊，請參閱請熟悉 NSX Intelligence 圖形元素和瞭解 NSX Intelligence 視圖和流量。</p>
8	<p>本節包含放大、縮小、套用 1:1 外觀比例、調整大小以符合視圖，以及進入或退出全螢幕檢視模式的檢視控制項。您也可以使用鍵盤快速鍵來管理檢視控制項。若要顯示在「鍵盤快速鍵說明」視窗，請按 Shift+?。</p> <p>若要導覽至先前檢視的視覺效果，請使用網頁瀏覽器的上一頁按鈕。當您在全螢幕模式中，請按上一步 (位於畫面的左上角) 以執行相同的上一步按鈕導覽。</p>

請熟悉 NSX Intelligence 圖形元素

NSX Intelligence 使用者介面提供數個圖形元件，以協助理資料中心實體、流量，以及 NSX-T Data Center 環境中特定活動的視覺效果。

下表列出您可能會在 NSX Intelligence 視覺效果中看到的 NSX-T Data Center 圖形元素詞彙表。

圖形元素	說明
	此圖示代表一個群組，也就是一組虛擬機器，其中可以套用安全性原則，包括東西向防火牆規則。請參閱 使用群組視圖 。
	此圖示代表屬於您 NSX-T Data Center 的虛擬機器 (VM)。虛擬機器可以屬於多個群組。請參閱 使用虛擬機器視圖 。
	此圖示代表網際網路中的公用 IP。如果您的 NSX-T Data Center 環境中至少有一個虛擬機器在選取的期間內與公用 IP 通訊，則該流量會包含在目前的視覺化中。
	在所選期間內參與網路流量活動的 IP 位址，例如單點傳播、廣播或多點傳送 IP。
未分類的虛擬機器 (4) 	此圖示用於不屬於群組的虛擬機器群組。
	箭頭代表所選期間內兩個虛擬機器之間所發生的網路流量。有三種不同類型的箭頭：紅色虛線箭頭表示不受保護流量、藍色實線箭頭表示已封鎖流量，以及綠色實線箭頭表示已允許流量。請參閱 使用流量 。
	已選取為目前焦點所在節點的節點會以虛線的圓圈括住。它是選取模式期間釘選的節點，而系統會顯示目前的視圖。
	如果在所選期間內已在 NSX-T Data Center 詳細目錄中新增群組，則此圖示會顯示在群組節點的邊緣上。如果 NSX-T Data Center 在所選期間內探索到虛擬機器，則圖示會顯示在該虛擬機器節點的邊緣上。
	如果所選期間內已刪除群組而虛擬機器成員未刪除，則此圖示會顯示在群組節點的邊緣上。在虛擬機器節點的邊緣上，此圖示表示所選期間內已刪除的虛擬機器。雖然虛擬機器或群組已刪除，但它仍會顯示在目前的視覺效果中，以針對所選期間內已移除之虛擬機器或群組提供歷史視圖。
	只要同時看到群組和虛擬機器，就會顯示此圖示。例如，在深入瞭解群組視圖或群組的相關虛擬機器中。 在下列情況下，圖示會顯示在虛擬機器節點的邊緣上。 <ul style="list-style-type: none"> ■ 如果在所選期間內已將虛擬機器移出目前已查看的群組 ■ 如果在所選期間內的某個時間點，虛擬機器是您目前正在檢視的群組的一部分，但不再是相同群組的成員

瞭解 NSX Intelligence 視圖和流量

NSX Intelligence 視覺效果包含群組或虛擬機器，以及所選期間內使用那些群組或虛擬機器所發生的網路流量。

重要 針對特定期間顯示的視覺效果代表所有網路流量和活動，例如在該期間內您 NSX-T Data Center 中所發生虛擬機器和群組的新增、刪除或移動。虛擬機器可能在視覺效果中出現一次以上。例如，如果虛擬機器已連結到最初未受管理的 ESXi 主機，且該主機在所選期間內變得受 VMware vCenter Server™ 所管理，則虛擬機器會在虛擬機器視圖中出現兩次。同樣地，如果 ESXi 主機從 vCenter Server 中斷連線，然後在相同的所選期間內新增回來，則連結至主機的虛擬機器會在所選期間內同時顯示為刪除與新增的部分。在群組視圖中，如果虛擬機器位於未分類的群組中，且在相同的所選期間內新增至群組中，則虛擬機器會同時顯示在未分類的群組及其新的群組中。

NSX Intelligence 僅支援具有虛擬機器成員類型的群組。如果您的群組包含任何其他類型的成員，則群組視圖可能會顯示虛擬機器成員類型的群組之間的相關流量，而不是安全性規則中的實際群組。

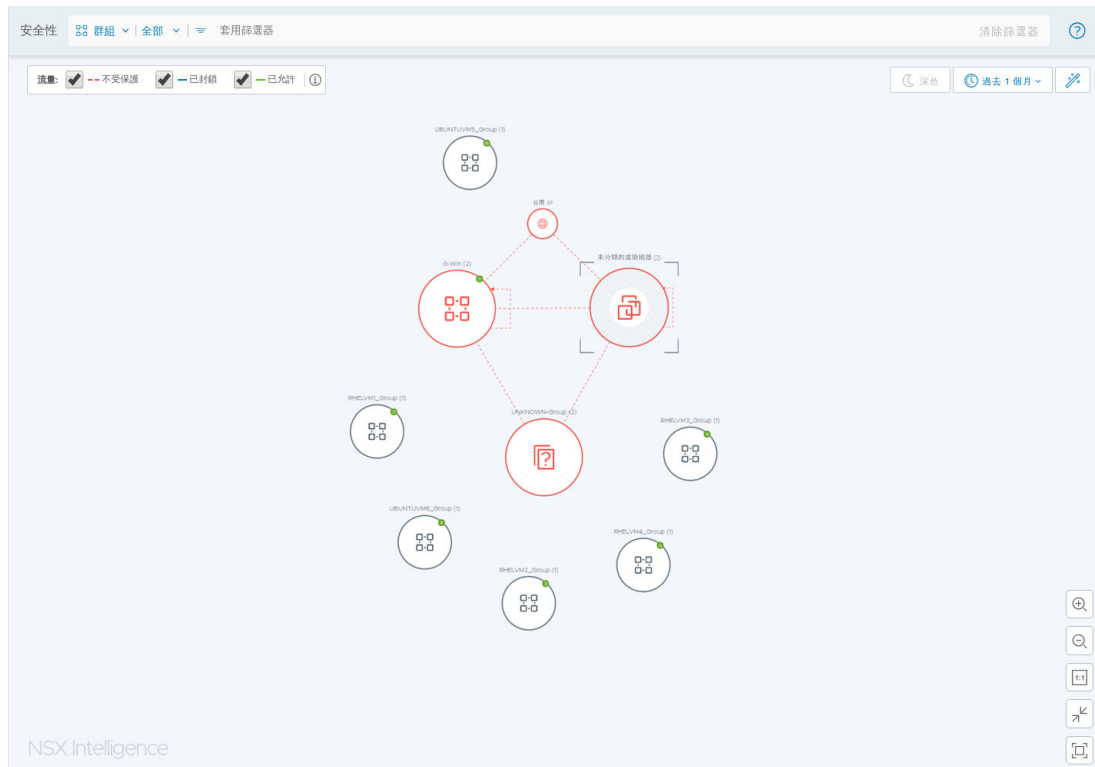
使用此區段中的資訊以深入瞭解關於使用群組視圖、虛擬機器視圖，以及不同流量。

使用群組視圖

NSX Intelligence 首頁中顯示的預設視圖為 [群組] 視圖。此群組視圖會進行篩選，以顯示在過去 24 小時內有未受保護流量的所有群組。

群組視圖中的節點和箭頭

群組視圖中的節點表示 NSX-T Data Center 環境中的 NSX 物件，例如虛擬機器、IP 集合等。下列螢幕擷取畫面是群組視圖的範例。



下表列出您可能會在群組視圖中看到的群組節點類型。

群組節點的類型	圖示	說明
一般群組		NSX Intelligence 中的「一般群組」節點代表您 NSX-T Data Center 環境中的任何 NSX 物件集合。在此版本中，這些 NSX 物件都只是虛擬機器，因此 NSX Intelligence 支援僅具有虛擬機器成員類型的一般群組。NSX 物件可以屬於多個群組，因此虛擬機器可以出現在多個群組節點中。
未分類群組		未分類的群組節點代表不屬於任何群組的虛擬機器集合。
未知群組		「未知群組」節點代表在 NSX-T Data Center 詳細目錄中找不到的一組其他物件。但是，這些物件會與您 NSX-T Data Center 環境中的一或多個 NSX 物件通訊。
公用 IP 群組		公用 IP 群組節點代表正在與您 NSX-T Data Center 中的 NSX 物件通訊的公用 IP 位址 (IPv4 或 IPv6) 的集合。

群組視圖中的節點大小是以屬於該群組的 NSX 物件 (例如虛擬機器) 數目為基礎。例如，群組的節點越大，則有越多虛擬機器屬於該群組。群組的名稱和其成員虛擬機器總數會顯示在節點上方。

群組節點之間的箭頭，代表那些已連線群組節點中的虛擬機器之間在所選期間內發生的流量。群組節點上的自我參考箭頭表示至少有一個虛擬機器正在與同一群組內的另一個虛擬機器進行通訊。如需詳細資訊，請參閱[使用流量](#)。

具有紅色邊緣的節點，表示無論在所選期間內偵測到多少已封鎖或已允許的流量，群組中的虛擬機器至少有一個未受保護的流量。節點上的藍色邊緣表示未偵測到任何不受保護流量，但偵測到至少一個已封鎖流量，無論在選取的期間內偵測到多少已允許流量。具有綠色邊緣的節點表示在所選期間內沒有偵測到不受保護或已封鎖流量，且至少偵測到一個已允許流量。具有灰色邊緣的節點表示在所選期間內，沒有偵測到屬於該群組的虛擬機器流量。

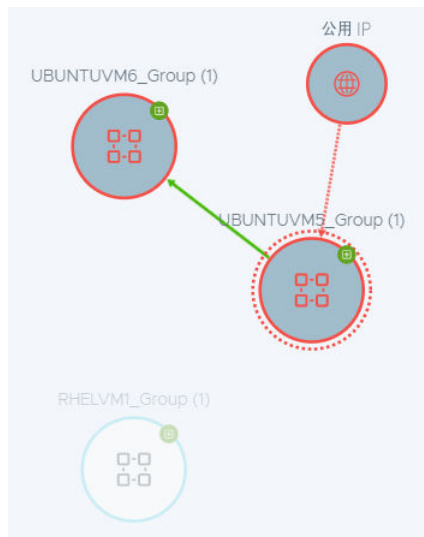
如果您沒有看到群組視圖，請按一下安全性視圖選取區域中**虛擬機器**旁的向下箭頭，然後選取**群組**。在顯示的選取項目下拉式清單中，您可以從清單中選取**所有群組**或特定群組，然後按一下**套用**。使用**搜尋**文字方塊來篩選選取項目清單。如果您在未選取任何選取項目的情況下按一下選取項目下拉式清單，或者如果您在下拉式清單中選取**所有群組**，則會將**所有群組**選取項目套用至群組視圖。

群組視圖中的節點選取項目

當您指向群組的節點時，系統會顯示該群組的相關資訊，如下列範例中針對群組 G-Win 所顯示的內容。系統會列出所選期間內也偵測到的流量數目和類型。如果群組在所選期間內新增，則系統也會顯示新的徽章圖示和群組建立時間的詳細資料。



當您按一下群組的節點時，虛線的圓形會將選取項目標示為釘選的群組節點。已連線至所選群組節點的其他群組也會在視圖中更為顯著。所有其他節點會變暗。例如，在下列螢幕擷取畫面中，會選定 UBUNTUVM5_Group 節點，而所選期間內使用 UBUNTUVM5_Group 共用流量的其他群組也會反白顯示。未與 UBUNTUVM5_Group 通訊的所有其他群組在視圖中會淡出。



若要清除釘選的選取項目，請按一下群組視圖的任何空白區域。

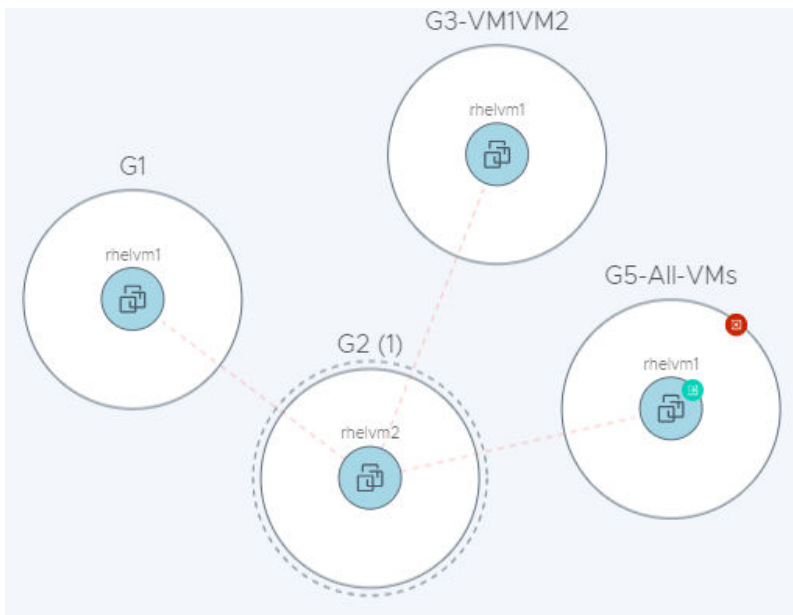
如果您縮小群組視圖，則節點上的詳細資料不會再次顯示，而會指向節點的任何顯示部分並顯示其詳細資料。

群組視圖中的可用動作

當您以滑鼠右鍵按一下群組的節點時，即會顯示可用動作的內容功能表，如下列影像所示。



- 選取**深入探究: *Group_Name*** 會圍繞所選群組的節點，並以虛線圓形將其標記為釘選的群組節點或作為焦點的目前群組。屬於該群組的虛擬機器會顯示在群組節點的內部。具有所選期間內使用釘選群組中虛擬機器之流量的所有群組也會放置於群組視圖中。在下列範例中，群組 G2 是固定群組，而其他群組位於視圖中，是因為其虛擬機器成員在選取的期間內具有群組 G2 中的 rhelvm2 流量。



- 當您選取**篩選依據**時，目前的群組會新增至用於目前群組視圖的視覺效果篩選器。
- 選取**虛擬機器**會顯示所選期間內屬於目前群組之所有虛擬機器的資料表。在該檢視虛擬機器資料表中，您可以查看屬於所選群組的虛擬機器相關詳細資料，以及每個虛擬機器也所屬的其他群組。若要將虛擬機器新增至目前的視覺化篩選器，請按一下篩選器圖示。
- 當您選取**流量詳細資料**時，會顯示目前所選群組的 [流量詳細資料] 資料表，如下列螢幕擷取畫面所示。它會顯示關於所選期間內屬於目前群組的虛擬機器已發生且目前處於作用中狀態的流量詳細資料。詳細資料包括流量類型、流量的來源和目的地群組、流量的開始和結束時間，以及所使用的服務。您可以按一下部分詳細資料來取得詳細資訊。如需詳細資訊，請參閱[使用流量](#)。

流量詳細資料

過去 24 小時



顯示 未分類的虛擬機器 的流量詳細資料

已完成的流量

作用中流量

搜尋

來源	來源群組	目的地	目的地群組	服務	結束時間	最新的流量
ubuntu12.04.1-2G-L...	G5	ubuntu12.04-...	UNCATEGORIZED	SSH... 及其他 2 個	2019/11/6 上午8:...	● 不受保護
ubuntu12.04.1-2G-L...	G1	ubuntu12.04-...	UNCATEGORIZED	SSH... 及其他 2 個	2019/11/6 上午8:...	● 不受保護

重新整理

1 - 2 of 2 流量

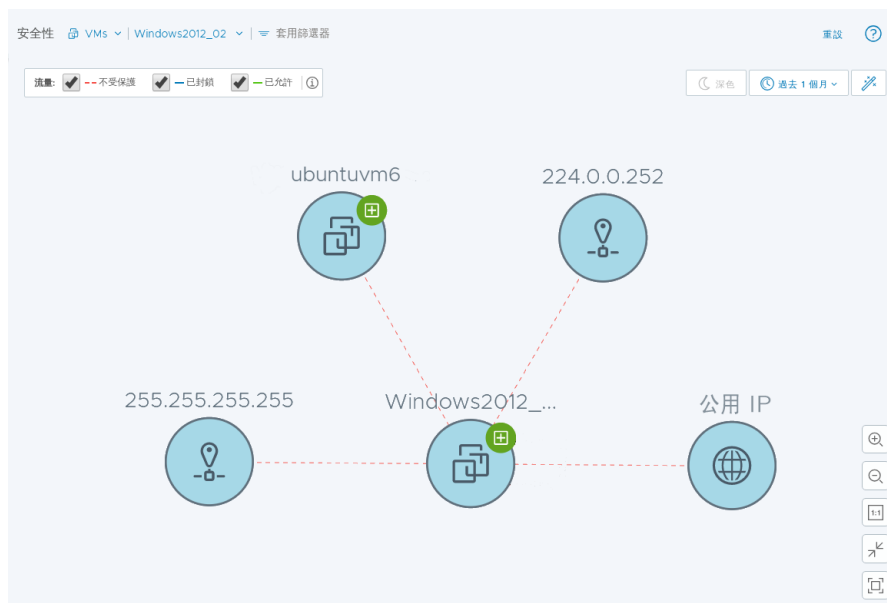
關閉

使用虛擬機器視圖

虛擬機器視圖中的節點代表您內部部署 NSX-T Data Center 環境中的虛擬機器 (VM)。

虛擬機器視圖中的節點和箭頭

當您在虛擬機器視圖中時，看不到群組界限。與 NSX-T Data Center 環境中的其中一個虛擬機器進行通訊但未識別為屬於 NSX-T Data Center 詳細目錄中的任何節點，也會在虛擬機器視圖中表示。下列說明簡易的虛擬機器視圖。



下表列出您可能會在視圖中看到的虛擬機器節點類型。

虛擬機器節點的類型	圖示	說明
一般虛擬機器		一般虛擬機器節點代表屬於 NSX-T Data Center 環境的虛擬機器 (VM)。虛擬機器可以屬於多個群組。
公用 IP		公用 IP 節點代表與您 NSX-T Data Center 環境進行通訊的公用 IP 位址 (IPv4 或 IPv6)。
IP		IP 節點代表在所選期間內參與網路流量活動的 IP 位址。IP 位址可以是單點傳播、廣播或多點傳送 IP。

如果您沒有看到虛擬機器視圖，請按一下安全性視圖選取區域中**群組**旁的向下箭頭，然後選取**虛擬機器**。在顯示的選取項目下拉式清單中，您可以從清單中選取**所有虛擬機器**或特定虛擬機器，然後按一下**套用**。使用**搜尋**文字方塊來篩選選取項目清單。如果您在未選取任何選取項目的情況下按一下選取項目下拉式清單，或者如果您在下拉式清單中選取**所有虛擬機器**，則會將**所有虛擬機器**選項套用至虛擬機器視圖。

虛擬機器節點之間的箭頭代表所選期間內虛擬機器之間已發生的流量。如需詳細資訊，請參閱[使用流量](#)。

虛擬機器視圖中的節點選取項目

當您指向虛擬機器節點時，系統會顯示節點的相關資訊，如下列範例所示。系統會列出所選期間內也偵測到的虛擬機器流量數目和類型。如果群組在所選期間內新增，則系統也會顯示新的徽章圖示和虛擬機器新增時間的詳細資料。



當您按一下虛擬機器的節點時，虛線的圓形會將選取項目標示為釘選的虛擬機器節點。具有使用該釘選虛擬機器節點之流量的其他虛擬機器節點也會在虛擬機器視圖中更為顯著。所有其他節點會變暗，使其較不可見。若要清除釘選的選取項目，請按一下虛擬機器視圖的任何空白區域。

當您縮小虛擬機器視圖時，虛擬機器中的詳細資料不會再次顯示，而會指向虛擬機器節點的任何顯示部分並顯示其詳細資料。

虛擬機器視圖中的可用動作

當您以滑鼠右鍵按一下虛擬機器的節點時，即會顯示可用動作的內容功能表，如下列影像所示。






選取項目	說明
篩選依據	虛擬機器會新增至用於目前虛擬機器視圖的視覺效果篩選器。
虛擬機器資訊	隨即顯示所選期間內虛擬機器的詳細資料。
相關群組	群組表格，其中包含虛擬機器在所選期間內所屬群組的相關資訊。
流量詳細資料	<p>會顯示關於所選期間內虛擬機器已發生且目前處於作用中狀態的流量詳細資料。詳細資料包括以下內容。</p> <ul style="list-style-type: none"> ■ 流量類型 ■ 流量的來源和目的地群組 ■ 流量的開始和結束時間 ■ 所使用的服務 <p>您可以按一下部分詳細資料來取得詳細資訊。如需詳細資訊，請參閱使用流量。</p>
啟動建議	顯示啟動新的建議精靈。如需更多詳細資料，請參閱 使用 NSX Intelligence 建議 。

使用流量

群組或虛擬機器節點之間的箭頭代表所選期間內虛擬機器之間已發生的網路流量。

網路流量會以適當的 L3 Distributed Firewall (DFW) 規則，以及所選期間內發生的流量為基礎。視覺化和流量詳細資料中包含與可設定狀態的 L3 DFW 規則搭配使用 IPv4 或 IPv6 及 TCP、UDP、GRE、ESP 和 SCTP 通訊協定的所有網路流量。TCP 和 UDP 流量具有 IP 和連接埠層級詳細資料，而其他的則僅具有 IP 層級詳細資料。

流量分類為下列類型。

流量類型	圖形	說明
不受保護		紅色虛線箭頭表示系統偵測到流量遭遇規則 (來源：任何 目的地：任何 動作：允許或拒絕或捨棄)，且需要更細微的安全性原則。此規則可以是您的預設規則，也可以位於東西向 Distributed Firewall 中的任何位置。
已封鎖		藍色實線箭頭表示系統偵測到流量遭遇「拒絕」或「捨棄」規則，而這些規則比「不受保護」流量定義中說明的規則更細微。
已允許		綠色實線箭頭表示系統偵測到流量遭遇「已允許」規則，而這些規則比「不受保護」流量定義中說明的規則更細微。

若僅要聚焦於特定類型流量的物件，請使用安全性視圖選取區域來選取視圖類型，然後使用「流量類型」篩選器屬性來縮小選取範圍。

如果取消選取流量類型，則該流量類型的流量資料將在顯示的圖形中隱藏。除非篩選器作用中排除特定物件，否則所有群組或虛擬機器物件會保持顯示，無論這些物件在所選期間內發生的流量類型為何。例如，如果您取消選取「已允許」流量類型，則所有的「已允許」流量資料皆會在圖形中隱藏。但是，所有物件仍會顯示，即使是在所選期間內僅具有「已允許」流量的物件。

流量箭頭的方向表示偵測到流量的來源和目的地。在群組視圖中，群組節點上的自我參考箭頭表示至少有一個虛擬機器正在與同一群組內的另一個虛擬機器進行通訊。在虛擬機器視圖中，自我參考箭頭指示虛擬機器中的 NSX 物件與相同虛擬機器中的另一個 NSX 物件通訊。

當您指向流量箭頭時，系統會涉及群組或虛擬機器之流量的相關資訊，如下列範例中針對群組 G2 所顯示的內容。



當您按一下流量箭頭時，會顯示 [流量詳細資料] 對話方塊。其中顯示所選期間內發生之已完成和作用中流量的相關詳細資料。若要取得流量的來源、目的地、服務類型，以及流量類型的詳細資訊，請按一下資料表中的連結，以查看詳細資料。

使用 NSX Intelligence 建議

NSX Intelligence 可以提供在所選期間內，在 NSX-T Data Center 環境中的虛擬機器之間發生的流量模式的微分割建議。

了解 NSX Intelligence 建議

NSX Intelligence 產生的建議包含安全性原則、原則安全群組和應用程式的服務。

建議是以 vCenter Server 管理的 ESXi 主機上虛擬機器工作負載之間的網路流量模式為基礎。它們可以藉由關聯 NSX-T Data Center 環境中所發生通訊的流量模式，協助您強制執行較動態的安全性原則。

安全性原則建議是應用程式類別的東西向 Distributed Firewall 安全性原則。安全群組建議包含在時間期間內進行分析之網路流量中所看到的虛擬機器清單，以及您已指定的虛擬機器界限。服務建議是服務物件，由您指定的虛擬機器中的應用程式在某些連接埠中使用，但服務尚未在 NSX-T Data Center 詳細目錄中定義。

有多種方式可要求建議，但最簡潔的方法是使用**計劃和疑難排解 > 建議索引**標籤並按一下**啟動新的建議**。您需要提供包含應用程式界限的虛擬機器 (VM)，以及要用來針對那些特定虛擬機器分析網路流量的時間範圍。建議分析完成之後，您可以檢視建議的詳細資料，並在發佈之前視需要進行修改。如需詳細資訊，請參閱[產生新的 NSX Intelligence 建議](#)。

產生新的 NSX Intelligence 建議

NSX Intelligence 建議功能可以提供建議，協助您微分割您的應用程式。

產生 NSX Intelligence 建議包括安全性原則、原則安全群組和應用程式服務的建議。建議是根據 NSX-T Data Center 中虛擬機器之間的通訊流量模式而產生。有多種方式可以使用 NSX Intelligence UI 來產生建議。下列程序說明三個可用的方法。

必要條件

安裝 NSX Intelligence。請參閱《NSX-T Data Center 安裝指南》中的〈安裝和設定 NSX Intelligence〉。

程序

- 1 從瀏覽器以企業管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 開始產生新建議。

使用下表來決定使用三種可用方法中的哪一種。

方法	步驟
選取 計劃和疑難排解 > 建議 。	按一下 啟動新的建議 。
在虛擬機器視圖中，選取虛擬機器，並按一下滑鼠右鍵。	從關聯式功能表中，選取 啟動新的建議 。
選取 計劃和疑難排解 > 探索和採取動作 。	<ol style="list-style-type: none"> 1 在 [安全性狀態] 篩選器中按一下向下箭頭，然後選取虛擬機器。 2 選取包含應用程式界限的虛擬機器，然後套用。 3 按一下建議棒圖示 。 4 在 [建議] 對話方塊中，按一下啟動新的建議。

3 在 [啟動新的建議] 精靈中，選擇性地變更**建議名稱**的預設值。

4 定義或修改用作安全性原則建議之界限的虛擬機器。

a 按一下**選取虛擬機器**或已選取的**虛擬機器**數目。

b 在 [選取虛擬機器] 對話方塊中，選取要用作分析界限的虛擬機器並取消選取不想包含的虛擬機器。

您最多可以選取 100 台虛擬機器用於建議界限。您也可以開始在選取項目列中輸入名稱來篩選要選取的虛擬機器。

c 按一下**儲存**。

已選取的虛擬機器數目會顯示在 [探索新的建議] 對話方塊中。

5 展開**更多選項**以變更說明和用於建議分析之**時間範圍**的預設值。預設的**時間範圍**值為 [過去 1 個月]，這表示建議分析期間將使用過去一個月中所選取虛擬機器之間發生的網路流量。

6 按一下**開始探索**。

建議會以連續方式處理。平均而言，可能需要 3 到 4 分鐘的時間來完成每個建議，取決於是否有擱置中待處理的其他建議。如果必須分析的虛擬機器之間有多個流量，則產生建議可能會花費 10–15 分鐘的時間。您可在**建議**索引標籤中追蹤狀態。狀態會從等待中進展到分析中，最終進入已可發佈。下列螢幕擷取畫面顯示所產生建議的三種不同狀態。

建議					
啟動新的建議		依名稱、路徑或其他項目篩選			
	名稱	狀態	虛擬機器	建立時間	上次修改時間
⋮ >	REC 20191107 10:09:19	沒有可用的建議	6	2019/11/7 上午2:09	2019/11/7 上午2:09
⋮ >	REC 20191106 16:39:30	沒有可用的建議	1	2019/11/6 上午8:39	2019/11/6 上午8:39
⋮ >	REC 20191106 16:15:53	沒有可用的建議	1	2019/11/6 上午8:16	2019/11/6 上午8:16

成功發佈建議之後，狀態會變更為 [已發佈]。

後續步驟

檢閱產生的建議，並決定是否將其發佈。請參閱[檢閱並發佈產生的建議](#)。

檢閱並發佈產生的建議

產生的 NSX Intelligence 建議達到 [已可發佈] 狀態之後，您可以檢閱建議、視需要修改，並決定是否將其發佈。

必要條件

產生新的建議。請參閱[產生新的 NSX Intelligence 建議](#)。

程序

- 1 從瀏覽器以企業管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 按一下 **計劃和疑難排解 > 建議**。
- 3 若要協助縮小所顯示的建議清單，請按一下畫面右上方的**依名稱、路徑或其他項目篩選**，並指定要使用的篩選準則。
- 4 如果您決定不使用建議，請按一下三點功能表圖示，然後選取**刪除**。
- 5 若要檢視建議的摘要，請按一下建議名稱旁邊的箭頭以展開資料列。

您會看到產生的規則數目，以及會受到影響的群組數目。

- 6 檢閱和管理建議的詳細資料。

- a 按一下建議的名稱。

建議精靈隨即顯示，類似於下列影像。

Recommendations

1 Review Recommendations

2 Place rules in FW context

3 Enforcement Summary

REC 20190719 15:59:02

Showing discovered recommendations. Review, Edit and Proceed with your selections to place the rules in the existing Firewall context.

Recommended FW Rules Recommended Groups Recommended Services

Category: Application Recommended Rules: 6 Recommended Groups: 3 Recommended Services: 0

Name	Sources	Destinations	Services	Profiles	Applied To	Action	
Policy-1 (REC 20190719 15:59:02)	(6)						
Rule-1 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	Win - RPC, DCOM, EP...	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-2 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBDG-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-3 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCP-Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-4 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCPv6 Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-5 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBNB-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-6 (REC 20190719 15:59:02)	Group-2 (REC 20190719 15:59:02)	Group-3 (REC 20190719 15:59:02)	SSH	None	Group-2 (REC 20190719 15:59:02)	Allow	<input checked="" type="checkbox"/>

1 of 1 Policy

CANCEL CONTINUE LATER NEXT

- b 在**建議的韌體規則索引標籤**中，檢閱防火牆規則詳細資料。若要修改任何詳細資料，請按一下適當資料行中的值，然後選取**編輯 (鉛筆)** 圖示。
- c 若要定義封包的處理方式，請選取**動作**資料行中的**允許、捨棄或拒絕**。
- d 切換右側按鈕來啟用或停用規則。產生的規則在發佈時依預設會設定為啟用，如上一個步驟中的影像所示。
- e 按一下**建議的群組**。

- f 按一下**成員**資料行中的連結，檢閱針對群組建議所設定之虛擬機器和 IP 的詳細資料。
 - g 按一下群組名稱旁的功能表圖示 (三個點)，然後選取**編輯**來修改群組建議。
 - h 按一下**建議的服務**，並檢閱詳細資料。
 - i 按一下服務名稱旁的功能表圖示 (三個點)，然後選取**編輯**來修改名稱或說明。刪除服務之前，請確保沒有使用該服務的規則。
 - j 按下一步。
- 7 在**韌體內容**中的**放置規則**窗格中，您可以變更套用至現有防火牆規則的規則建議順序。拖曳反白顯示的區段，或按一下三點功能表圖示並選取**移至選取的區段上方**或**移至選取的區段下方**。
 - 8 按一下**發佈**。
 - 9 在**發佈建議**對話方塊中，按一下**是**。
 - 10 在 [強制執行摘要] 頁面中，確認已成功發佈安全性原則，然後按一下**關閉**。
- 建議資料表中的建議 [狀態] 欄會變更為 [已發佈]。

結果

安全性原則建議成功發佈之後，在**計劃和疑難排解 > 建議**索引標籤中會處於唯讀模式。若要檢視並管理已發佈的規則建議，請前往**安全性 > Distributed Firewall**。

重要 發佈規則建議後，視覺化會繼續在虛擬機器之間將受影響的流量顯示為橙色箭頭 (不受保護流量)，直到在受影響的虛擬機器之間產生新流量為止。此視覺化僅會根據流量在主機上發生的時間來報告流量，而不會反映在發生這些流量後發佈的規則集。在發佈規則集並產生新的流量後，新的流量會顯示為綠色箭頭 (已允許流量)。

備份和還原 NSX Intelligence

當目前 NSX Intelligence 組態變得無法運作，或是您想要還原至先前的狀態時，您可以從備份還原組態。備份和還原工作流程僅支援使用 NSX Intelligence CLI。

執行備份時，NSX Intelligence 只會備份包含 NSX Intelligence 應用裝置的所有服務所使用的組態檔。備份中不包含任何視覺化資料。

如果 NSX Intelligence 中發生資料遺失或損毀，則相關流量和建議的所有現有資料也會遺失。重新安裝 NSX Intelligence 會重新開始收集網路流量資料，而這些已收集資料的視覺化將在此點以後提供。

完成備份組態之後，您可隨時在 NSX Intelligence 應用裝置上手動執行備份命令。備份會經過加密、壓縮並儲存在備份組態期間定義的遠端伺服器。當您建立備份時，建立備份的日期和時間將附加到備份檔案名稱，以便唯一識別每個備份檔案。例如，`config-backup-2019-06-21T21_06_07UTC.tar.gz`。

當您還原 NSX Intelligence 備份時，系統會還原擷取備份時的組態狀態。您必須將備份還原至建立備份檔案時正在執行相同 NSX Intelligence 應用裝置版本的 NSX Intelligence 應用裝置。您可以還原至現有 NSX Intelligence 應用裝置或還原至全新安裝的 NSX Intelligence 應用裝置，但它們必須與您備份的 NSX Intelligence 應用裝置版本相同。

設定 NSX Intelligence 備份

建立 NSX Intelligence 組態的備份之前，您必須先設定備份檔案伺服器。備份檔案伺服器設定好之後，您可以在任何時候建立 NSX Intelligence 的備份。

必要條件

- 確認您擁有 NSX Intelligence CLI 的 CLI 管理員認證。
- 請確定您擁有遠端伺服器的使用者名稱和密碼。
- 取得在遠端伺服器中儲存備份檔案的檔案路徑。

程序

- 1 從命令列提示字元中，以管理員權限登入 NSX Intelligence CLI 主機。

```
$ ssh admin@cli-ip-address
admin@cli-ip-address's password:
```

- 2 設定備份檔案伺服器。

命令語法為

```
set backup remote-host remote_host_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase pass_phrase
```

其中 `remote_host_address` 是備份檔案伺服器的遠端主機 IP 或 FQDN 位址，而 `remote_host_username` 帳戶必須擁有在 `remote_folder_path` 中建立備份檔案的必要權限。您必須為 `passphrase` 參數提供強式值。長度必須至少為八個字元，且至少有一個大寫字元、一個小寫字元和一個特殊字元。例如，

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

- 3 確認組態。

```
get configuration
```

在輸出中，確認 `set backup` 行正確無誤。以上一個步驟的範例為例，輸出必須包含下列行。

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

備份 NSX Intelligence

您可以使用 CLI 命令來備份 NSX Intelligence 應用裝置組態檔。

必要條件

- 確保您擁有 NSX Intelligence CLI 的管理員存取權。
- 設定備份檔案伺服器。請參閱[設定 NSX Intelligence 備份](#)。

程序

- 1 以管理員權限登入 NSX Intelligence CLI。
- 2 建立備份。

```
backup intelligence configuration
```

如果備份成功，您會看到類似以下的訊息。

```
Backup Complete. Archived at: backup_file_server-IP_address:/root/backup_archives/
intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 您可以使用另一個 CLI 工作階段來檢視備份進度。
 - a 登入另一個 NSX Intelligence CLI 工作階段。
 - b 輸入以下命令。

```
get log-file node-mgmt.log follow
```

還原 NSX Intelligence 備份

還原備份時，您會將 NSX Intelligence 組態的狀態還原至建立備份的時間。您可以使用 CLI 命令來還原 NSX Intelligence 備份。

您必須將備份還原到與要還原之備份相同版本的 NSX Intelligence 應用裝置安裝上。依預設，還原的備份檔案是最新產生的備份。如果您要還原備份至新安裝的 NSX Intelligence 應用裝置，在還原備份之前，請先設定封存檔名稱。

必要條件

- 確認您擁有備份檔案伺服器的管理員登入認證和主機資訊。
- 確保您擁有 NSX Intelligence CLI 的管理員存取權。

程序

- 1 以管理員權限登入新的 NSX Intelligence CLI 伺服器。
- 2 設定備份所在的遠端伺服器。

命令語法為

```
set restore remote-host backup_server_IP_address remote-path remote_folder_path remote-
host-username remote_host_username remote-host-password remote_host_password passphrase
pass_phrase
```

其中 `backup_server_IP_address` 是備份檔案伺服器的遠端主機 IP 或 FQDN 位址，`remote_host_username` 帳戶必須擁有存取 `remote_folder_path` 中備份檔案的必要權限。例如，

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

3 確認還原組態。

```
get configuration
```

在輸出中，確認 `set restore` 行正確無誤。以上一個步驟的範例為例，輸出必須包含下列行。

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

4 使用以下命令還原備份。

```
restore intelligence configuration
```

如果還原作業成功，您會看到類似下列的訊息。

```
NSX Intelligence Restore Complete.
```

5 您可以使用另一個 CLI 工作階段來檢視備份還原進度。

- a 登入另一個 NSX Intelligence CLI 工作階段。
- b 輸入以下命令。

```
get log-file node-mgmt.log follow
```

疑難排解 NSX Intelligence 問題

如果 NSX Intelligence 應用裝置變得無回應，或您需要有關使用應用裝置時所收到錯誤訊息的詳細資料，您可以執行特定命令來取得 NSX Intelligence 服務的狀態。

您也可以收集支援服務包，以協助您和 VMware 支援人員解決您可能遇到的問題。

檢查 NSX Intelligence 應用裝置的狀態

如果 NSX Intelligence 應用裝置沒有回應，請檢查 NSX Intelligence 服務的狀態。

問題

NSX Intelligence 應用裝置沒有回應，或者您收到錯誤訊息，指出應用裝置未如預期運作。

原因

一或多個基礎 NSX Intelligence 服務可能已停止或未處於健全狀態。

解決方案

- 1 使用具有企業管理員角色的帳戶登入 NSX Intelligence 應用裝置 CLI 主機。
- 2 使用 `get services` 命令檢查 NSX Intelligence 服務的狀態。

如果所有 NSX Intelligence 服務皆正常運作，您會看到類似下列範例的輸出。

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
Session timeout:       1800
Connection timeout:    30
Redirect host:         (not configured)
Client API rate limit: 100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:          kafka
Service state:         running
Service health:        good

Service name:          liagent
Service state:         stopped

Service name:          mgmt-plane-bus
Service state:         stopped

Service name:          node-mgmt
Service state:         running

Service name:          nsx-config
Service state:         running

Service name:          nsx-message-bus
Service state:         stopped

Service name:          nsx-upgrade-agent
Service state:         running

Service name:          ntp
Service state:         running
Start on boot:         True

Service name:          pace-server
Service state:         running
```

```

Service name:      postgres
Service state:     running
Service health:    good

Service name:      processing
Service state:     running

Service name:      snmp
Service state:     stopped
Start on boot:     False

Service name:      spark
Service state:     running
Service health:    good

Service name:      spark-job-scheduler
Service state:     running

Service name:      ssh
Service state:     running
Start on boot:     True

Service name:      syslog
Service state:     running

Service name:      ui-service
Service state:     running

Service name:      zookeeper
Service state:     running
Service health:    good

my_nsx-intel>

```

服務狀態可能是執行或已停止。服務健全狀況可能是良好或已降級。

- 您也可以檢視 `syslog` 檔案，並搜尋 `pace-monitor.sh` 健全狀況檢查指令碼的輸出，該指令碼會將 NSX Intelligence 服務的健全狀況記錄到 `syslog` 檔案。

如果所有服務皆如預期運作，則在執行 `get log-file syslog | find pace-monitor` 命令後，您會看到類似下列範例輸出的輸出。

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - -      "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -      "href": "/"
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -      "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - -      "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - -      "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",

```



```

<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - - "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - - "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - - "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - - ],

```

```

<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - - "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - - ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED -
Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - - }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor

```

如果其中一個服務發生問題，當您執行 `get log-file syslog | grep pace-monitor` 時，可能會看到下列行。

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

4 如果遇到下列其中一個輸出，請使用 `restart service service-name` 命令重新啟動服務。

- 執行 `get services` 命令後，其中一個服務會顯示服務狀態：已停止或服務健全狀況：已降級。
- 執行 `get log-file syslog | grep pace-monitor` 命令後，輸出會顯示如下的訊息：
PACE 健全狀況為「已降級」。傳回碼並非 HTTP OK。訊息。

例如，如果 postgres 服務的狀態顯示為已停止，或者其狀態為執行中，但其狀態為已降級服務健全狀況，請執行下列命令。

```
restart service postgres
```

重要 您必須使用 `restart service service-name` 命令重新啟動 NSX Intelligence 服務。如果您決定改用 `stop service service-name` 和 `start service service-name` 命令，您也必須手動重新啟動每個依存於 `service-name` 的服務。下列清單顯示必須重新啟動 NSX Intelligence 服務的相依性順序。

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-server
```

例如，如果在 nsx-config 服務停止後使用 `stop|start service service-name` 命令加以啟動，您也必須使用 `restart service service-name` 命令重新啟動 processing 和 pace-server 服務。

此外，如果您使用 `restart service service-name` 命令在 spark-job-scheduler 服務之前重新啟動相依性順序清單中顯示的任何服務，您也必須使用 `restart service spark-job-scheduler` 命令手動重新啟動 spark-job-scheduler 服務。若未執行此動作，將會導致 spark-job-scheduler 服務進入錯誤狀態。

收集 NSX Intelligence 支援服務包

您可以使用 NSX Intelligence CLI 收集支援服務包。

支援服務包檔案內容未包含資料。它包含下列目錄中的檔案。

- /opt/vmware/*
- /var/log/*
- /etc/*
- 使用 journalctl 和 systemctl 的系統狀態

必要條件

確定您具有 NSX Intelligence CLI 的企業管理員存取權。

程序

- 1 使用具有企業管理員角色權限的帳戶登入 NSX Intelligence CLI。
- 2 產生支援服務包。

命令語法如下所示，其中您需要為 support_filename.tgz 提供值。

```
get support-bundle file support_filename.tgz
```

例如，

```
get support-bundle file support_bundle123.tgz
```

當服務包檔案已成功建立時，您會收到類似下列範例的訊息。

```
support_bundle123.tgz 已建立，請使用下列命令來傳輸檔案：copy file support_bundle123.tgz url  
<url> 在傳輸 support_bundle123.tgz 之後，請使用 tar xvf support_bundle123.tgz 來擷取它
```

3 使用下列命令確認支援服務包存在。

```
get files
```

您會收到類似下列內容的輸出。

```
Directory of filestore:/  
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```