

NSX-T Data Center 管理指南

修改日期：2023 年 2 月 14 日
VMware NSX-T Data Center 3.0

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 © 2017-2023 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 14

檢視監控儀表板 17

2 第 0 層閘道 19

新增第 0 層閘道 20

建立 IP 首碼清單 23

建立社群清單 24

設定靜態路由 25

建立路由對應 26

在新增路由對應時使用規則運算式來比對社群清單 28

設定 BGP 28

設定 BFD 31

設定多點傳播 32

設定 IPv6 第 3 層轉送 32

建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔 33

變更第 0 層閘道的 HA 模式 34

新增 VRF 閘道 35

設定 EVPN 36

3 第 1 層閘道 38

新增第 1 層閘道 38

4 區段 41

區段設定檔 41

瞭解 QoS 區段設定檔 42

瞭解 IP 探索區段設定檔 44

瞭解 SpoofGuard 區段設定檔 46

瞭解區段安全性區段設定檔 47

瞭解 MAC 探索區段設定檔 48

新增區段 50

區段上 DHCP 的類型 52

在區段上設定 DHCP 53

在區段上設定 DHCP 靜態繫結 57

第 2 層橋接 61

建立 Edge 橋接器設定檔 61

- 設定以 Edge 為基礎的橋接 62
- 建立第 2 層橋接器備份區段 64
- 新增中繼資料 Proxy 伺服器 64

5 主機交換器 66

- 在 vSphere Distributed Switch 上管理 NSX-T 66
 - 設定 vSphere Distributed Switch 67
 - 管理 NSX 分散式虛擬連接埠群組 69
 - 使用 VDS 準備的 NSX-T 叢集 70
 - 用來在 NSX-T Data Center 上設定 vSphere Distributed Switch 的 API 71
 - vSphere Distributed Switch 中已啟用以支援 NSX-T Data Center 的功能支援 73
- 進階網路堆疊 76
 - 自動指派 ENS 邏輯核心 76
 - 設定客體 VLAN 間路由 77
- 將主機交換器移轉到 vSphere Distributed Switch 78
- NSX 虛擬分散式交換器 84

6 虛擬私人網路 (VPN) 86

- 瞭解 IPsec VPN 87
 - 使用以原則為基礎的 IPsec VPN 87
 - 使用以路由為基礎的 IPsec VPN 88
- 瞭解第 2 層 VPN 89
 - 啟用和停用 L2 VPN 路徑 MTU 探索 90
- 新增 VPN 服務 91
 - 新增 IPsec VPN 服務 92
 - 新增 L2 VPN 服務 94
- 新增 IPsec VPN 工作階段 96
 - 新增以原則為基礎的 IPsec 工作階段 96
 - 新增路由型 IPsec 工作階段 99
 - 關於支援的合規性套件 102
 - 瞭解 TCP MSS 鉗制 103
- 新增 L2 VPN 工作階段 103
 - 新增 L2 VPN 伺服器工作階段 103
 - 新增 L2 VPN 用戶端工作階段 105
 - 下載遠端 L2 VPN 組態檔 106
- 新增本機端點 107
- 新增設定檔 109
 - 新增 IKE 設定檔 109
 - 新增 IPsec 設定檔 112
 - 新增 DPD 設定檔 114
- 新增自發 Edge 作為 L2 VPN 用戶端 115

檢查 IPSec VPN 工作階段的實現狀態 117

監控和疑難排解 VPN 工作階段 120

7 網路位址轉譯 (NAT) 121

在閘道上設定 NAT 122

8 負載平衡 125

主要負載平衡器概念 125

調整負載平衡器資源 126

支援的負載平衡器功能 127

負載平衡器拓撲 128

設定負載平衡器元件 129

新增負載平衡器 130

新增主動監視器 131

新增被動監視器 134

新增伺服器集區 135

設定虛擬伺服器元件 138

針對伺服器集區和虛擬伺服器建立的群組 165

9 分散式負載平衡器 166

瞭解分散式負載平衡器的流量 167

建立和連結分散式負載平衡器執行個體 168

建立分散式負載平衡器的伺服器集區 169

使用 Fast TCP 或 UDP 設定檔建立虛擬伺服器 171

在 ESXi 主機上驗證分散式負載平衡器組態 172

監控分散式負載平衡器統計資料 173

10 轉送原則 175

新增或編輯轉送原則 176

11 IP 位址管理 (IPAM) 177

新增 DNS 區域 177

新增 DNS 轉寄站服務 178

新增 DHCP 設定檔 179

新增 DHCP 伺服器設定檔 179

新增 DHCP 轉送設定檔 181

將 DHCP 設定檔連結至第 0 層或第 1 層閘道 182

案例：為 DHCP 服務選取 Edge 叢集 183

案例：在 DHCP 上變更區段連線的影響 188

新增 IP 位址集區 190

新增 IP 位址區塊 191

12 網路設定 192

- 設定多點傳播 192
 - 建立 IGMP 設定檔 193
 - 建立 PIM 設定檔 194
- 新增 VNI 集區 194
- 設定閘道設定 195
- 新增閘道 QoS 設定檔 195
- 新增 BFD 設定檔 196

13 安全性 197

- 安全性組態概觀 197
- 安全性概觀 198
- 安全性術語 199
- 身分識別防火牆 199
 - 身分識別防火牆工作流程 200
- 第 7 層內容設定檔 202
 - 第 7 層防火牆規則工作流程 203
 - 屬性 204
- 分散式防火牆 207
 - 防火牆草稿 208
 - 新增分散式防火牆 209
 - 分散式防火牆封包記錄 212
 - 管理防火牆排除清單 215
 - 篩選特定網域 (FQDN/URL) 215
 - 將安全性原則延伸至實體工作負載 217
 - 共用位址集 223
- 分散式 IDS 223
 - 分散式 IDS 設定和簽章 223
 - 分散式 IDS 設定檔 226
 - 分散式 IDS 規則 229
 - 分散式 IDS 事件 230
 - 驗證主機上的分散式 IDS 狀態 232
- 東西向網路安全性 - 鏈結第三方服務 233
 - 東西向網路保護的主要概念 233
 - 東西向流量的 NSX-T Data Center 需求 234
 - 東西向網路安全性的高階工作 234
 - 部署用於執行東西向流量自我檢查的服務 235
 - 新增東西向流量的重新導向規則 236
 - 解除安裝東西向流量自我檢查服務 238
- 閘道防火牆 238

- 新增閘道防火牆原則和規則 239
- URL 分析工作流程 241
- 閘道防火牆封包記錄 243
- 南北向網路安全性 - 插入第三方服務 245
 - 南北向網路安全性的高階工作 245
 - 部署用於執行南北向流量自我檢查的服務 245
 - 針對南北向流量新增重新導向規則 247
 - 解除安裝南北向流量自我檢查服務 248
- 端點保護 248
 - 瞭解端點保護 248
 - 設定端點保護 252
 - 管理端點保護 268
- 安全性設定檔 277
 - 建立工作階段計時器 277
 - 洪泛保護 280
 - 設定 DNS 安全性 281
 - 管理群組與設定檔的優先順序 282
- 以時間為基礎的防火牆原則 283
- 網路自我檢查設定 284
 - 新增服務區段 284
 - 新增服務設定檔 284
 - 新增服務鏈結 285
- 對防火牆進行疑難排解 286
 - 在 NSX Manager 上監控防火牆及進行疑難排解 286
 - 對 ESX 主機上的分散式防火牆進行疑難排解 286
 - 對 KVM 主機上的分散式防火牆進行疑難排解 296
 - 對閘道防火牆進行疑難排解 299
 - 查看規則實現狀態 303
 - 分散式防火牆封包記錄 305
- 裸機伺服器安全性 307

14 詳細目錄 309

- 新增服務 309
- 新增群組 310
- 新增內容設定檔 312
- 容器 313
- 公有雲服務 315
- 實體伺服器 316
- 標籤 316
 - 將標籤新增至物件 319
 - 將標籤新增至多個物件 319

- 從物件取消指派標籤 321
- 從多個物件中取消指派標籤 321

15 多站台和聯盟 322

- NSX-T Data Center 多站台 322
 - 使用 VMware Site Recovery Manager 333
- NSX 聯盟 333
 - NSX 聯盟 概觀 334
 - NSX 聯盟 中的網路 342
 - NSX 聯盟中的安全性 354
 - 在 NSX 聯盟中備份和還原 367

16 系統監控 369

- 監控 NSX Edge 節點 369
- 使用事件和警示 371
 - 關於事件和警示 371
 - 檢視警示資訊 400
 - 檢視警示定義 401
 - 設定警示定義設定 403
 - 管理警示狀態 403
- 使用 vRealize Log Insight 進行系統監控 404
- 使用 vRealize Operations Manager 進行系統監控 405
- 使用 vRealize Network Insight Cloud 進行系統監控 408

17 網路監控 416

- 新增 IPFIX 收集器 416
- 新增防火牆 IPFIX 設定檔 417
- 新增交換器 IPFIX 設定檔 417
- vSphere Distributed Switch 上的 IPFIX 監控 418
- 新增連接埠鏡像設定檔 419
- vSphere Distributed Switch 上的連接埠鏡像 420
- 執行 Traceflow 420
- 簡易網路管理通訊協定 (SNMP) 423
- 監控網狀架構節點 423
- 網路延遲統計資料 424
 - 測量網路延遲統計資料 428
 - 匯出網路延遲統計資料 429
- 管理程式模式中的監控工具 430
 - 在管理程式模式中檢視連接埠連線資訊 430
 - Traceflow 431
 - 在管理程式模式中監控連接埠鏡像工作階段 434

- 為連接埠鏡像工作階段設定篩選器 437
- 在管理程式模式中設定 IPFIX 438
- 在管理程式模式中監控邏輯交換器連接埠活動 612

18 驗證和授權 614

- 本機使用者帳戶 614
 - 管理使用者的密碼或名稱 615
 - 重設應用裝置的密碼 616
 - 驗證原則設定 617
- 與 VMware Identity Manager/Workspace ONE Access 整合 618
 - NSX Manager、vIDM 和相關元件之間的時間同步 618
 - 從 vIDM 主機取得憑證指紋 619
 - 設定 VMware Identity Manager/Workspace ONE Access 整合 620
 - 驗證 VMware Identity Manager 功能 622
- 與 LDAP 整合 623
 - LDAP 身分識別來源 624
- 新增角色指派或主體身分識別 625
- 同時設定 vIDM 和 LDAP 或從 vIDM 轉換至 LDAP 627
- 角色型存取控制 628
- 記錄使用者帳戶變更 636

19 憑證 638

- 憑證類型 638
- NSX 聯盟的憑證 639
- 建立憑證簽署要求檔案 641
- 建立自我簽署憑證 642
 - 建立自我簽署的憑證 642
 - 匯入 CSR 的憑證 643
- 匯入並取代憑證 644
 - 匯入自我簽署的憑證或 CA 簽署的憑證 644
 - 匯入 CA 憑證 644
 - 設定憑證匯入檢查 645
 - 取代憑證 646
- 匯入和擷取 CRL 647
 - 匯入憑證撤銷清單 647
 - 設定 NSX Manager 以擷取憑證撤銷清單 648
- 用於負載平衡器或 VPN 服務的公用憑證和私密金鑰的儲存區 649
- 憑證到期的警示通知 649

20 在管理程式模式中設定 NSX-T Data Center 650

- 管理程式模式中的邏輯交換器 650

- 瞭解 BUM 框架複寫模式 651
- 在管理程式模式中建立邏輯交換器 652
- 在管理程式模式中將虛擬機器連線到邏輯交換器 653
- 在管理程式模式中建立邏輯交換器連接埠 661
- 在管理程式模式中測試第 2 層連線 661
- 在管理程式模式中為 NSX Edge 上行建立 VLAN 邏輯交換器 664
- 邏輯交換器和邏輯連接埠的交換設定檔 666
- 管理程式模式中的第 2 層橋接 680
- 管理程式模式中的邏輯路由器 685
 - 第 1 層邏輯路由器 685
 - 第 0 層邏輯路由器 694
- 管理程式模式中的 NAT 724
 - 網路位址轉譯 724
- 在管理程式模式中群組物件 736
 - 在管理程式模式中建立 IP 集合 736
 - 在管理程式模式中建立 IP 集區 736
 - 在管理程式模式中建立 MAC 集合 737
 - 在管理程式模式中建立 NSGroup 737
 - 設定服務和服務群組 739
 - 在管理程式模式中管理虛擬機器的標籤 740
- 管理程式模式中的 DHCP 741
 - DHCP 741
 - 中繼資料 Proxy 746
- 管理程式模式中的 IP 位址管理 748
 - 在管理程式模式中管理 IP 區塊 748
 - 在管理程式模式中管理 IP 區塊的子網路 748
- 管理程式模式中的負載平衡 749
 - 主要負載平衡器概念 750
 - 設定負載平衡器元件 750
- 管理程式模式中的防火牆 778
 - 在管理程式模式中新增或刪除邏輯路由器的防火牆規則 778
 - 在管理程式模式中為邏輯交換器橋接器連接埠設定防火牆 779
 - 防火牆區段和防火牆規則 779
 - 關於防火牆規則 783

21 備份和還原 NSX Manager 789

- 設定備份 789
- 移除舊備份 792
- 還原備份 792
 - 列出可用的備份 795
- 還原後的憑證管理 796

22 作業和管理 798

- 檢視物件類別的使用量和容量 799
- 設定使用者介面設定 800
- 設定節點設定檔 801
- 查看組態變更的實現狀態 802
- 檢視網路拓撲 806
- 搜尋物件 807
- 依物件屬性篩選 808
- 新增計算管理程式 808
- 新增 Active Directory 811
- 新增 LDAP 伺服器 812
- 同步 Active Directory 813
- 從 vCenter Server 移除 NSX-T Data Center 延伸 814
- 管理 NSX Manager 叢集 814
 - 檢視 NSX Manager 叢集的組態和狀態 814
 - 更新 NSX Manager 叢集的 API 服務組態 817
 - 關閉 NSX Manager 叢集及開啟其電源 818
 - 將 NSX Manager 重新開機 818
 - 變更 NSX Manager 的 IP 位址 819
 - 調整 NSX Manager 節點的大小 820
- 取代 NSX Edge 叢集中的 NSX Edge 傳輸節點 821
 - 使用 NSX Manager UI 取代 NSX Edge 傳輸節點 821
 - 使用 API 取代 NSX Edge 傳輸節點 822
- 管理 Edge 虛擬機器應用裝置的資源保留 823
 - 調整 NSX Edge 應用裝置的資源保留 825
- 將 ESXi 主機傳輸節點新增至 vCenter Server 和從中移除 825
- 變更分散式路由器介面的 MAC 位址 826
- 設定應用裝置 827
- 新增授權金鑰並產生授權使用率報告 828
- 符合性組態 831
 - 檢視符合性狀態報告 831
 - 符合性狀態報告代碼 832
 - 設定負載平衡器的全域 FIPS 符合性模式 834
- 收集支援服務包 836
- 記錄訊息和錯誤碼 837
 - 設定遠端記錄 841
 - 記錄訊息識別碼 848
 - 對 Syslog 問題進行疑難排解 849
 - 在應用裝置虛擬機器上設定序列記錄 850
 - 防火牆稽核記錄訊息 850

- 客戶經驗改進計劃 866
 - 編輯客戶經驗改進計劃組態 866
- 尋找遠端伺服器的 SSH 指紋 867
- 設定外部負載平衡器 868
- 進行 Proxy 設定 870
- 檢視容器相關的資訊 870

23 使用 NSX Cloud 871

- Cloud Service Manager : UI 逐步解說 871
 - 雲端 871
 - 系統 878
- 使用 NSX Cloud 隔離原則的威脅偵測 882
 - NSX 強制執行模式 中的隔離原則 883
 - 原生雲端強制執行模式 中的隔離原則 887
 - 虛擬機器的使用者管理清單 888
- NSX 強制執行模式 889
 - 目前支援工作負載虛擬機器的作業系統 889
 - 在 NSX 強制執行模式 中讓虛擬機器上線 890
 - 在 NSX 強制執行模式 中管理虛擬機器 898
- 原生雲端強制執行模式 899
 - 在 原生雲端強制執行模式 中管理虛擬機器 900
- NSX-T Data Center 功能支援 NSX Cloud 903
 - 使用 NSX-T Data Center 和公有雲標記分組虛擬機器 904
 - 使用原生雲端服務 907
 - 工作負載虛擬機器在 NSX 強制執行模式 下的服務插入 908
 - 在 NSX 管理的虛擬機器上啟用 NAT 916
 - 啟用 Syslog 轉送 916
 - 在原生雲端強制執行模式中設定 VPN 917
 - 在 NSX 強制執行模式中設定 VPN 924
- NSX Cloud 常見問題和疑難排解 929

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>。

相關說明文件

您可以在 <https://docs.vmware.com/tw/VMware-NSX-Intelligence/index.html> 取得 VMware NSX® Intelligence™ 說明文件。NSX Intelligence 1.0 內容最初包含在 NSX-T Data Center 2.5 說明文件集中，並與之一起發佈。

NSX Manager

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 介面提供了兩種設定資源的模式：

- 原則模式
- 管理程式模式

存取原則模式和管理程式模式

如果存在，您可以使用**原則**和**管理程式**按鈕，在原則和管理程式模式之間切換。切換模式可控制哪些功能表項目可供您使用。



- 依預設，如果您的環境僅包含透過原則模式建立的物件，則您的使用者介面會處於原則模式，且您不會看到**原則**和**管理程式**按鈕。
- 依預設，如果您的環境包含透過管理程式模式建立的任何物件，您會在右上角看到**原則**和**管理程式**按鈕。

可透過修改使用者介面設定來變更這些預設值。如需詳細資訊，請參閱[設定使用者介面設定](#)。

原則和管理程式介面中使用相同的**系統**索引標籤。如果您修改 Edge 節點、Edge 叢集或傳輸區域，則那些變更可能需要 5 分鐘的時間，才會在原則模式中顯示。您可以使用 `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload` 立即同步。

使用原則模式或管理程式模式的時機

您使用的模式應保持一致性。您會基於幾種原因而選擇使用其中一個模式。

- 如果您要部署新的 NSX-T Data Center 環境，則在多數情況下，最好的選擇是使用**原則**模式來建立和管理環境。
 - 某些功能在原則模式中無法使用。如果您需要這些功能，請對所有組態使用**管理程式**模式。

- 如果您計劃使用 NSX 聯盟，請使用**原則模式**建立所有物件。全域管理程式僅支援原則模式。
- 如果您要從舊版 NSX-T Data Center 進行升級，且已使用 [進階網路與安全性] 索引標籤建立組態，請使用**管理程式模式**。

您可在 [進階網路與安全性] 索引標籤下找到的功能表項目和組態，可在 NSX-T Data Center 3.0 的**管理程式模式**中取得。

重要 如果您決定使用原則模式，請使用它來建立所有物件。請勿使用管理程式模式來建立物件。

同樣地，如果您需要使用管理程式模式，請使用它來建立所有物件。請勿使用原則模式來建立物件。

表 1-1. 使用原則模式或管理程式模式的時機

原則模式	管理程式模式
多數新的部署應使用原則模式。 聯盟僅支援原則模式。如果您想要使用聯盟，或者將來可能使用聯盟，請使用原則模式。	以前使用進階介面所建立的部署，例如，從原則模式出現之前的版本升級。
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。
僅在原則模式中可用的網路功能： <ul style="list-style-type: none"> ■ DNS 服務和 DNS 區域 ■ VPN ■ NSX Cloud 的轉送原則 	僅在管理程式模式中可用的網路功能： <ul style="list-style-type: none"> ■ 轉送累計計時器
僅在原則模式中可用的安全性功能： <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 	僅在管理程式模式中可用的安全性功能： <ul style="list-style-type: none"> ■ 橋接防火牆

在原則模式和管理程式模式中建立的物件名稱

取決於用來建立物件的介面，您建立的物件會有不同的名稱。

表 1-2. 物件名稱

使用原則模式建立的物件	使用管理程式模式建立的物件
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

表 1-2. 物件名稱 (續)

使用原則模式建立的物件	使用管理程式模式建立的物件
安全性原則	防火牆區段
閘道防火牆	Edge 防火牆

原則和管理程式 API

NSX Manager 提供兩個 API：原則和管理程式。

- 原則 API 包含以 /policy/api 開頭的 URI。
- 管理程式 API 包含以 /api 開頭的 URI。

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

安全性

NSX Manager 具有下列安全性功能：

- NSX Manager 具有稱為 admin 的內建使用者帳戶，該帳戶具有所有資源的存取權限，但沒有作業系統安裝軟體的權限。NSX-T 升級檔案是唯一允許安裝的檔案。您無法編輯 admin 使用者的權限或將該權限刪除。請注意，您可以變更使用者名稱 admin。
- NSX Manager 支援工作階段逾時和自動使用者登出。NSX Manager 不支援工作階段鎖定。啟動工作階段鎖定可能是用來存取 NSX Manager 之工作站作業系統的函數。當工作階段終止或使用者登出時，系統會將使用者重新導向至登入頁面。
- 在 NSX-T 上實作的驗證機制會遵循安全性最佳做法，並可抵禦重新執行攻擊。安全做法會進行系統化部署。例如，NSX Manager 上每個工作階段的工作階段識別碼和 Token 都是唯一的，且在使用者登出後或在閒置一段時間後到期。此外，每個工作階段都有時間記錄，且工作階段通訊會進行加密，以避免工作階段遭到劫持。

您可以使用下列 CLI 命令來檢視和變更工作階段逾時值：

- 命令 `get service http` 會顯示值的清單，其中包括工作階段逾時。
- 若要變更工作階段逾時值，請執行下列命令：

```
set service http session-timeout <timeout-value-in-seconds>
restart service ui-service
```

本章節討論下列主題：

- [檢視監控儀表板](#)

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 1-3. 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。
端點保護	系統 > 服務部署	顯示端點保護部署的狀態。

表 1-4. 原則模式中的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 > 分散式防火牆	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 1-5. 管理程式模式中的網路與安全性儀表板

儀表板	來源	說明
負載平衡器	網路 > 負載平衡	顯示負載平衡器服務、負載平衡器虛擬伺服器與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	安全性 > 分散式防火牆 安全性 > 橋接防火牆 網路 > 第 0 層邏輯路由器和網路 > 第 1 層邏輯路由器	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	網路 > 邏輯交換器	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 1-6. 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](#)。

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 將第 0 層上行與來自 Cisco 的多機箱連接埠通道拓撲 (例如 vPC (虛擬 PortChannel) 或 VSS (虛擬交換器系統)) 或來自 Arista 的 MLAG (多機箱鏈路聚合) 連線時，請務必諮詢網路提供者，以瞭解將拓撲用於傳送路由時的限制。

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](#)
- [設定多點傳播](#)
- [設定 IPv6 第 3 層轉送](#)
- [建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔](#)
- [變更第 0 層閘道的 HA 模式](#)
- [新增 VRF 閘道](#)
- [設定 EVPN](#)

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。

如果您在 NSX 聯盟從全域管理程式新增第 0 層閘道，請參閱[從全域管理程式新增第 0 層閘道](#)。

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

備註 從 NSX-T Data Center 3.0.1 中開始，支援主動備用第 0 層閘道。

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 或雙重堆疊定址，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。

您可以設定第 0 層閘道，以支援 EVPN (乙太網路 VPN) Type-5 路由。如需有關設定 EVPN 的詳細資訊，請參閱[設定 EVPN](#)。

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。
EVPN TEIP IP	這用於在第 0 層閘道上重新分配 EVPN 本機端點子網路。

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。

來源類型	說明
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。

在第 0 層閘道上，Proxy ARP 會處理外部和服務介面 IP 的 ARP 查詢。從 NSX-T Data Center 3.0.2 開始，Proxy ARP 還會處理位於 IP 首碼清單中且使用 Permit 動作設定之服務 IP 的 ARP 查詢。

必要條件

如果您計劃設定多點傳播，請參閱[設定多點傳播](#)。

程序

- 1 從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。

- 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) 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 169.254.0.0/24。

- 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。

- 9 按一下 **VRF 閘道的路由辨別碼**，以設定路由辨別碼管理員位址。
僅 EVPN 和自動路由辨別碼使用案例才需要進行此設定。
- 10 (選擇性) 新增一或多個標籤。
- 11 按一下 **儲存**。
- 12 對於 IPv6，在**其他設定**下，您可以選取或建立 **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)。
- 13 (選擇性) 按一下 **EVPN 設定**以設定 EVPN。
 - a 選取 VNI 集區。
您可以按一下功能表圖示 (3 個點) 來建立 VNI 集區 (如果先前尚未建立)。
 - b 在 **EVPN 通道端點**欄位中，按一下**設定**以新增 EVPN 本機通道端點。
對於通道端點，選取 Edge 節點並指定 IP 位址。
您可以選擇性地指定 MTU。

備註 確保已在您為 EVPN 通道端點選取的 NSX Edge 節點上已設定上行介面。

- 14 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**、**EVPN TEP 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**。
- 15 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) 如果介面類型為**外部**，您可以透過將 **PIM** (通訊協定獨立多點傳播) 設定為**已啟用**來啟用多點傳播。
PIM 僅能在單一上行介面上啟用。
附註：如果您之後在此介面上停用 **PIM**，則將在包括此閘道上的下行的所有介面上停用多點傳播。
 - i (選擇性) 新增標籤，然後選取 ND 設定檔。
 - j (選擇性) 如果介面類型為**外部**，則對於 **URPF 模式**，您可以選取**嚴格或無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
 - k 建立介面之後，您可以透過按一下介面的功能表圖示 (三個點)，然後選取**下載 ARP 資料表**來下載 ARP 資料表。
- 16 (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。
- 17 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。
- 18 按一下**多點傳播**以設定多點傳播路由。
- 19 按一下 **BGP** 以設定 BGP。
- 20 (選擇性) 若要下載路由表或轉送表，請按一下功能表圖示 (三個點)，然後選取下載選項。視需要輸入**傳輸節點、網路和來源**的值，然後儲存 .CSV 檔案。

後續步驟

新增第 0 層閘道後，您可以選擇性地在閘道上啟用動態 IP 管理，方法是選取 DHCP 伺服器設定檔或 DHCP 轉送設定檔。如需詳細資訊，請參閱將 [DHCP 設定檔連結至第 0 層或第 1 層閘道](#)。

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[在管理程式模式中建立第 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，或選取 **NULL**。
如果選取 **NULL**，則路由會稱為裝置路由。
- 11 指定管理距離。
- 12 從下拉式清單中選取範圍。範圍可以是介面、閘道、IPSec 工作階段或區段。

13 按一下**新增**。

後續步驟

請確認已正確設定靜態路由。請參閱[確認第 0 層路由器上的靜態路由](#)。

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[在管理程式模式中建立 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。

對於 EVPN，僅支援**僅限協助程式**模式。

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。在容錯轉移時，[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 在**路由篩選器**下方，按一下**設定**以新增一或多個路由篩選器。

對於 **IP 位址家族**，您可以選取 **IPv4**、**IPv6** 或 **L2VPN EVPN**。您最多可以擁有兩個路由篩選器，其中一個位址家族為 **IPv4**，而另一個為 **L2VPN EVPN**。不允許任何其他組合 (**IPv4** 和 **IPv6**、**IPv6** 和 **L2VPN EVPN**)。

對於**路由數目上限**，您可以指定一個介於 1 和 1,000,000 之間的值。這是閘道將從 BGP 芳鄰接受的 BGP 路由數目上限。

附註：如果您將一個 BGP 芳鄰設定為使用某個位址家族，例如 **L2VPN EVPN**，然後稍後再新增第二個位址家族，則系統將會重設建立的 BGP 連線。

- e 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。

- f 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。
- g 輸入**躍點數目上限**的值。

- h 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]。

附註：對於 EVPN，僅支援**僅限協助程式**模式。

- i 按一下**計時器與密碼**。

- j 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 500。裸機 Edge 節點的最小值為 50。

- k 輸入 **BFD 乘數** 的值。

- l 輸入**保持關閉時間**和**保持運作時間**的值 (以秒為單位)。

保持運作時間會指定傳送 KEEPALIVE 訊息的頻率。值可以介於 0 至 65535 之間。零表示將不會傳送任何 KEEPALIVE 訊息。

保持關閉時間會指定閘道在認為芳鄰無作用之前，等待來自芳鄰的 KEEPALIVE 訊息所需的時間。值可以介於 0 或介於 3 至 65535 之間。零表示 BGP 芳鄰之間未傳送任何 KEEPALIVE 訊息，且一律不會將芳鄰視為無法連線。

保持關閉時間必須至少為**保持運作時間**值的三倍。

- m 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

- 1 從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 針對**靜態路由 BFD 對等**，按一下**路由和設定**。
- 5 按一下**新增靜態路由 BFD 對等**。
- 6 選取 **BFD 設定檔**。請參閱**新增 BFD 設定檔**。
- 7 輸入對等 IP 位址，並選擇性地輸入來源位址。
- 8 按一下**儲存**。

設定多點傳播

IP 多點傳播路由可讓主機 (來源) 將資料的單一複本傳送至單一多點傳播位址。然後，資料會透過特殊格式的 IP 位址 (名為 IP 多點傳播群組位址) 散佈至收件者群組。您可以在 IPv4 網路的第 0 層閘道上設定多點傳播，以啟用多點傳播路由。

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**多點傳播**切換按鈕，以啟用多點傳播。
- 5 在**複寫多點傳播範圍**欄位中，輸入 CIDR 格式的位址範圍。

複寫多點傳播範圍是在底層中用來複寫工作負載/承租人多點傳播群組位址之多點傳播群組位址 (GENEVE 外部目的地 IP) 的範圍。建議複寫多點傳播範圍與工作負載/承租人多點傳播群組位址之間不應有任何重疊。

- 6 在 **IGMP 設定檔** 下拉式清單中，選取 IGMP 設定檔。
- 7 在 **PIM 設定檔** 下拉式清單中，選取 PIM 設定檔。

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 > 網路設定**。
- 3 按一下**全域網路組態**索引標籤。

- 4 編輯全域閘道組態，然後針對第 3 層轉送模式選取 IPv4 和 IPv6。
不支援僅限 IPv6。
- 5 按一下儲存。
- 6 選取網路 > 第 0 層閘道。
- 7 按一下功能表圖示 (三個點) 並選取編輯，以編輯第 0 層閘道。
- 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

導覽至網路 > 網路設定，按一下全域閘道組態索引標籤，然後選取 IPv4 和 IPv6 作為第 3 層轉送模式

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

變更第 0 層閘道的 HA 模式

在特定情況下，您可以變更第 0 層閘道的高可用性 (HA) 模式。

僅當閘道上有多個服務路由器正在執行時，才允許變更 HA 模式。這表示您不可在多個 Edge 傳輸節點上有上行。但您可以在相同 Edge 傳輸節點上有多個上行。

將 HA 模式從作用中/作用中式設定為作用中/待命之後，您可以設定容錯移轉模式。預設值為非先佔式。

如果已設定下列服務或功能，則不允許變更 HA 模式。

- DNS 轉寄站
- IPSec VPN
- L2 VPN
- HA VIP
- 可設定狀態的防火牆
- SNAT、DNAT、NO_SNAT 或 NO_DNAT
- 套用在介面上的自反 NAT
- 服務插入

- VRF
- 集中式服務連接埠

新增 VRF 閘道

虛擬路由和轉送 (VRF) 閘道可讓路由資料表的多個執行個體同時存在同一閘道中。VRF 是 VLAN 的第 3 層同等項目。VRF 閘道必須連結至第 0 層閘道。從第 0 層閘道，VRF 閘道會繼承容錯移轉模式、Edge 叢集、內部傳送子網路、TO-T1 傳輸子網路和 BGP 路由組態。

必要條件

對於 EVPN 上的 VRF 閘道，請確保為要連結的第 0 層閘道設定 EVPN 設定。僅支援 EVPN 時需要這些設定：

- 在第 0 層閘道上指定 VNI 集區。
- 在第 0 層閘道上設定 EVPN 本機通道端點。

如需詳細資訊，請參閱[設定 EVPN](#)。

程序

- 1 從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**新增閘道 > VRF**。
- 4 輸入閘道的名稱。
- 5 選取第 0 層閘道。
- 6 按一下**VRF 設定**。

僅支援 EVPN 時需要這些設定。

- a 指定**路由辨別碼**。

如果已連線的第 0 層閘道已設定 **RD 管理員位址**，則系統會自動填入**路由辨別碼**。如果想要覆寫指派的路由辨別碼，請輸入新的值。

- b 指定**EVPN 傳送 VNI**。

VNI 必須是唯一的，並且屬於連結的第 0 層閘道上設定的 VNI 集區。

- c 在**路由目標**欄位中，按一下**設定**以新增路由目標。

針對每個路由目標，選取模式，可為**自動**或**手動**。指定一或多個**匯入路由目標**。指定一或多個**匯出路由目標**。

- 7 依序按一下**儲存**和**是**以繼續進行 VRF 閘道的設定。

- 8 對於 VRF-lite，請在 VRF 閘道上使用**存取 VLAN 識別碼**設定一或多個外部介面，並連線至 VLAN 區段。對於 EVPN，請在 VRF 閘道上使用存取 VLAN 識別碼設定一或多個服務介面，並連線至覆疊區段。請參閱**新增區段**。VRF 介面需要將連結的第 0 層閘道上的現有外部介面對應至每個 Edge 節點。連線至存取介面的區段需要有以範圍或清單格式設定的 VLAN 識別碼。
- 9 按一下 **BGP** 以設定 **BGP**、**ECMP**、**路由彙總** 和 **BGP 芳鄰**。您可以新增具有 IPv4/IPv6 位址家族的路由篩選器。請參閱**新增第 0 層閘道**。
- 10 按一下**路由**並完成路由組態。若要支援 VRF 閘道和連結的第 0 層閘道/對等 VRF 閘道之間的路由洩漏，您可以新增靜態路由，然後選取下一個躍點範圍作為連結的第 0 層閘道，或作為是其中一個現有的對等 VRF 閘道。請參閱**新增第 0 層閘道**。

設定 EVPN

EVPN (乙太網路 VPN) 是一種以標準為基礎的 BGP 控制平面，可在不同資料中心之間延伸第 2 層和第 3 層連線。

EVPN 功能具有下列功能與限制：

- NSX Edge 與實體路由器之間的多重通訊協定 BGP (MP-BGP) EVPN。
- VXLAN 用作 MP-BGP EVPN 的覆疊。
- 使用 VRF 執行個體在 MP-BGP EVPN 中的多租戶。
- 僅支援 EVPN Type-5 路由。
- NSX-T 為 EVPN 網域中的每個 NSX Edge VTEP 產生唯一的路由器 MAC。但是，網路中可能有其他節點未由 NSX-T 管理，例如，實體路由器。您必須確定路由器 MAC 在 EVPN 網域中的所有 EVPN 之間是唯一的。
- EVPN 功能支援 NSX Edge 做為 EVPN 虛擬通道端點的入口或出口。如果 NSX Edge 節點從其 eBGP 對等收到需要重新分配給另一個 eBGP 對等的 EVPN Type-5 首碼，則會重新通告路由，而不會對 NextHop 進行任何變更。
- 在多路徑網路拓撲中，建議您不要在已設定 EVPN 的閘道上啟用 ECMP。

組態必要條件

- 在 VMware ESXi Hypervisor 上部署的虛擬路由器 (vRouter)。
- 支援 EVPN Type-5 路由的對等實體路由器。

組態步驟

- 建立 VNI 集區。請參閱**新增 VNI 集區**。
- 設定 VLAN 區段。請參閱**新增區段**。
- 設定覆疊區段，並指定一或多個 VLAN 範圍。請參閱**新增區段**。
- 設定第 0 層閘道以支援 EVPN。請參閱**新增第 0 層閘道**。
- 在 [EVPN 設定] 下，選取 VNI 集區，然後建立 EVPN 通道端點。

- 在 [VRF 閘道的路由辨別碼] 下，針對自動路由辨別碼使用案例設定 RD 管理員位址。
- 在第 0 層閘道上設定一或多個外部介面，並連線至 VLAN 區段。
- 使用對等實體路由器設定 BGP 芳鄰。新增具有 IPv4 和 L2VPN EVPN 位址家族的路由篩選器。
- 設定路由重新分配。在第 0 層子網路下選取 EVPN TEP IP，以及其他來源。
- 設定 VRF 以支援 EVPN。請參閱[新增 VRF 閘道](#)。
- 在 [VRF 設定] 下，指定 EVPN 傳送 VNI。
- 指定用於手動路由辨別碼的路由辨別碼。
- 指定手動路由目標的匯入/匯出路由目標。
- 在 VRF 上為每個 Edge 節點新增服務介面，並連線至覆疊區段。指定每個服務介面的存取 VLAN 識別碼。
- 使用對等 vRouter 設定每個 VRF BGP 芳鄰。透過 VRF BGP 工作階段已知的路由，將由 NSX Edge 透過 MP-BGP EVPN 工作階段向對等實體路由器重新分配。

第 1 層閘道

第 1 層閘道具有區段的下行連線以及第 0 層閘道的上行連線。

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。

如果要從 NSX 聯盟中的全域管理程式新增第 1 層閘道，請參閱[從全域管理程式新增第 1 層閘道](#)。

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 (選擇性) 如果您想要讓這個第 1 層閘道主控可設定狀態服務，例如 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。

- 7 (選擇性) 在 Edge 欄位中，按一下**設定**以選取 **NSX Edge 節點**。

- 8 如果您選取了 NSX Edge 叢集，請選取容錯移轉模式或接受預設值。

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。

- 9 如果您計劃在此閘道上設定負載平衡器，請根據負載平衡器的大小，選取 **Edge 集區配置大小設定**。

選項為**路由**、**LB 小型**、**LB 中型**、**LB 大型**以及 **LB 特大**。預設值為**路由**，並且適用於此閘道上沒有設定任何負載平衡器的情況。此參數可讓 NSX Manager 以更智慧的方式將第 1 層閘道置於 Edge 節點上。透過此設定，即可將每個節點上的負載平衡和路由功能的數目納入考量。請注意，在建立閘道後，如果尚未設定負載平衡器，您可以變更此設定。

- 10 (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。

- 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

- 12 按一下**儲存**。

- 13 (選擇性) 按一下**路由通告**。

- a 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。

- 14 (選擇性) 按一下**其他設定**。

- a 對於 IPv6，您可以選取或建立 **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)。

- b 選取入口 **QoS 設定檔**和出口 **QoS 設定檔**以瞭解流量限制。

這些設定檔可用來設定允許流量的資訊速率和高載大小。如需如何建立 QoS 設定檔的詳細資訊，請參閱**新增閘道 QoS 設定檔**。

如果此閘道連結至第 0 層閘道，則**路由器連結**欄位會顯示連結位址。

- 15 (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 對於 **URPF 模式**，您可以選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
 - f 新增一或多個標籤。
 - g 在 **ND 設定檔**欄位中，選取或建立設定檔。
 - h 按一下**儲存**。
- 16 (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**。

後續步驟

新增第 1 層閘道後，您可以選擇性地在閘道上啟用動態 IP 管理，方法是選取 DHCP 伺服器設定檔或 DHCP 轉送設定檔。如需詳細資訊，請參閱將 [DHCP 設定檔連結至第 0 層或第 1 層閘道](#)。

在 NSX-T Data Center 中，區段是虛擬第 2 層網域。區段先前稱為邏輯交換器。

NSX-T Data Center 中有兩個類型的區段：

- VLAN 支援的區段
- 覆疊支援的區段

VLAN 支援的區段是在實體基礎結構中作為傳統 VLAN 執行的第 2 層廣播網域。這表示兩部連結至相同 VLAN 支援區段不同主機上兩部虛擬機器之間的流量，會透過 VLAN 在兩部主機之間延續。產生的限制是，您必須在實體基礎結構中佈建適當的 VLAN，這兩部位虛擬機器才能透過 VLAN 支援的區段在第 2 層進行通訊。

在覆疊支援的區段中，兩個連結至相同覆疊區段之不同主機上兩部虛擬機器之間的流量，其第 2 層流量會由主機之間的通道延續。NSX-T Data Center 會具現化並維護此 IP 通道，而不需要實體基礎結構中的任何區段特定組態。因此，虛擬網路基礎結構會與實體網路基礎結構分離。這表示您可以動態建立區段，而不需任何實體網路基礎結構的組態。

在支援覆疊的區段上學習的 MAC 位址數目預設為 2048 個。每個區段的預設 MAC 限制可透過 `MacLearningSpec` 中的 API 欄位 `remote_overlay_mac_limit` 進行變更。如需詳細資訊，請參閱《NSX-T Data Center API 指南》中的 `MacSwitchingProfile`。

本章節討論下列主題：

- [區段設定檔](#)
- [新增區段](#)
- [區段上 DHCP 的類型](#)
- [在區段上設定 DHCP](#)
- [在區段上設定 DHCP 靜態繫結](#)
- [第 2 層橋接](#)
- [新增中繼資料 Proxy 伺服器](#)

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 值會套用到 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>

選項	說明
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，請確保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。任何指定連接埠之 ARP/ND 隱藏快取中的 IP 數目，會由連接埠之 IP 探索設定檔中的設定來決定。相關設定包括 ARP 繫結限制、ND 窺探限制、重複的 IP 偵測、ARP ND 繫結限制逾時，以及首次使用時信任 (TOFU)。

SpoofGuard 和分散式防火牆 (DFW) 元件也會使用這些探索到的 MAC 和 IP 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。如果您在**管理程式**模式中導覽至**網路 > 邏輯交換器 > 連接埠**，然後選取連接埠，則可以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 探索區段設定檔。您也可以另外建立 IP 探索交換設定檔。

必要條件

請自行熟悉 IP 探索區段設定檔概念。請參閱[瞭解 IP 探索區段設定檔](#)。

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 探索區段設定檔詳細資料。

選項	說明
名稱	輸入名稱。
ARP 窺探	適用於 IPv4 環境。適用於具有靜態 IP 位址的虛擬機器。

選項	說明
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，上限為 256。預設值為 1。
ARP ND 繫結限制逾時	在 TOFU 已停用的情況下，ARP/ND 繫結資料表中 IP 位址的逾時值 (以分鐘為單位)。如果位址逾時，新探索到的位址會將其取代。
DHCP 窺探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP 窺探 - IPv6	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。
VM Tools - IPv6	僅適用於裝載 ESXi 的虛擬機器。
ND 窺探	適用於 IPv6 環境。適用於具有靜態 IP 位址的虛擬機器。
ND 窺探限制	可繫結至連接埠的 IPv6 位址數目上限。
首次使用時信任	適用於 ARP 和 ND 窺探。
重複的 IP 偵測	適用於所有窺探方法及 IPv4 和 IPv6 環境。

5 按一下儲存。

瞭解 SpoofGuard 區段設定檔

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

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

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

NSX-T Data Center SpoofGuard 組態涵蓋下列項目：

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

在連接埠層級中，系統會透過連接埠的位址繫結內容提供允許的 MAC/VLAN/IP 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 允許清單。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>
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 探索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。在預設 MAC 探索區段設定檔中，此內容預設為啟用。

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

您可以新增兩種區段：支援覆疊的區段和支援 VLAN 的區段。

區段會建立為傳輸區域的一部分。傳輸區域有兩種類型：VLAN 傳輸區域和覆疊傳輸區域。在 VLAN 傳輸區域中建立的區段是支援 VLAN 的區段，在覆疊傳輸區域中建立的區段為支援覆疊的區段。

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 > 區段**。
- 3 按一下**新增區段**。
- 4 輸入區段的名稱。
- 5 選取區段的連線類型。

連線	說明
無	當您不想要將區段連線至任何上游閘道 (第 0 層或第 1 層) 時，請選取此選項。您通常會在下列情況下新增獨立區段： <ul style="list-style-type: none"> ■ 想要為在相同子網路上執行工作負載的使用者建立本機測試環境時。 ■ 不需要與其他子網路上的使用者進行東西向連線時。 ■ 不需要與資料中心外部的使用者進行南北向連線時。 ■ 當您想要設定第 2 層橋接或客體 VLAN 標記時。
第 1 層	當您想要將區段連線至第 1 層閘道時，請選取此選項。
第 0 層	當您想要將區段連線至第 0 層閘道時，請選取此選項。

備註 您可以將閘道連線的區段從一個閘道變更為另一個閘道 (相同或不同閘道類型)。此外，您還可以將區段的連線從「無」變更為第 0 層或第 1 層閘道。僅當閘道和連線的區段位於相同的傳輸區域時，才會允許區段連線變更。但是，如果區段上設定了 DHCP，則變更區段連線時適用某些限制和注意事項。如需詳細資訊，請參閱[案例：在 DHCP 上變更區段連線的影響](#)。

- 6 輸入 CIDR 格式的子網路閘道 IP 位址。區段可包含 IPv4 子網路或 IPv6 子網路，或兩者。
 - 如果區段未連線至閘道，則子網路為選用。
 - 如果區段已連線至第 1 層或第 0 層閘道，則需要子網路。

某個區段的子網路不得與您網路中其他區段的子網路重疊。區段一律會與單一虛擬網路識別碼 (VNI) 相關聯，無論其是否已設定一個子網路、兩個子網路或無子網路。

- 7 選取傳輸區域，可以是覆疊或 VLAN。

若要建立支援 VLAN 的區段，請在 VLAN 傳輸區域中新增區段。同樣地，若要建立支援覆疊的區段，請在覆疊傳輸區域中新增區段。

- 8 (選擇性) 若要在區段上設定 DHCP，請按一下**設定 DHCP 組態**。

如需設定 DHCP 設定和 DHCP 選項的詳細步驟，請參閱[在區段上設定 DHCP](#)。

- 9 如果傳輸區域的類型是 VLAN，請指定 VLAN 識別碼的清單。如果傳輸區域的類型是「覆疊」，且您想要支援第 2 層橋接或客體 VLAN 標記，請指定 VLAN 識別碼的清單或 VLAN 範圍
- 10 (選擇性) 選取區段的上行整併原則。

如果您已將其新增至 VLAN 傳輸區域，則此下拉式功能表會顯示具名整併原則。如果未選取任何上行整併原則，則會使用預設整併原則。

- 具名整併原則不適用於覆疊區段。覆疊區段一律遵循預設整併原則。
- 對於支援 VLAN 的區段，您有彈性可使用所選的具名整併原則來覆寫預設整併原則。系統提供此功能，因此您可以將主機的基礎結構流量導向至 VLAN 傳輸區域中的特定 VLAN 區段。在新增 VLAN 區段之前，請確保在 VLAN 傳輸區域中新增具名整併原則名稱。

- 11 (選擇性) 輸入完整網域名稱。

區段上的 DHCPv4 伺服器和 DHCPv4 靜態繫結會自動從區段組態繼承網域名稱，作為網域名稱選項。

- 12 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。

- 13 在 **VPN 通道識別碼** 中，輸入用來識別區段的唯一值。

- 14 (選擇性) 在 **中繼資料 Proxy** 欄位中，按一下 **設定**，以將中繼資料 Proxy 連結至此區段或與其中斷連結。

若要連結中繼資料 Proxy，請選取現有的中繼資料 Proxy。若要中斷連結中繼資料 Proxy，請取消選取所選取的中繼資料 Proxy。

- 15 按一下 **儲存**。

- 16 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：**子系**或**靜態**。

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**。如果此連接埠用於裸機容器或伺服器，請選取**靜態**。

- 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**靜態**，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。
- 17 若要選取區段設定檔，請按一下 **區段設定檔**。
- 18 (選擇性) 若要將靜態 IP 位址繫結至區段上虛擬機器的 MAC 位址，請展開 **DHCP 靜態繫結**，然後按一下 **設定**。
同時支援用於 IPv4 的 DHCP 和用於 IPv6 的 DHCP 的靜態繫結。如需有關設定靜態繫結設定的詳細步驟，請參閱在 [區段上設定 DHCP 靜態繫結](#)。
- 19 按一下 **儲存**。

區段上 DHCP 的類型

NSX-T Data Center 在區段上支援三個類型的 DHCP：DHCP 本機伺服器、閘道 DHCP 和 DHCP 轉送。

DHCP 本機伺服器

顧名思義，它是區段的本機 DHCP 伺服器，並且無法用於網路中的其他區段。本機 DHCP 伺服器僅為連結至區段的虛擬機器提供動態 IP 指派服務。本機 DHCP 伺服器的 IP 位址必須位於區段上設定的子網路中。

閘道 DHCP

類似於中央 DHCP 服務，可在連線至閘道和使用閘道 DHCP 的所有區段上，動態地將 IP 和其他網路組態指派給虛擬機器。根據您連結至閘道的 DHCP 設定檔類型，您可以在區段上設定閘道 DHCP 伺服器或閘道 DHCP 轉送。依預設，連線至第 1 層或第 0 層閘道的區段會使用閘道 DHCP。閘道 DHCP 伺服器的 IP 位址可以與區段中設定的子網路不同。

DHCP 轉送

它是區段的本機 DHCP 轉送服務，且無法用於網路中的其他區段。DHCP 轉送服務會將連結至區段之虛擬機器的 DHCP 要求轉送至遠端 DHCP 伺服器。遠端 DHCP 伺服器可位於 SDDC 外部的任何子網路或實體網路中。

無論區段是否連線至閘道，您都可以在每個區段上設定 DHCP。同時支援用於 IPv4 (DHCPv4) 的 DHCP 和用於 IPv6 (DHCPv6) 的 DHCP 伺服器。

對於閘道連線的區段，支援所有三個類型的 DHCP。但是，僅在區段的 IPv4 子網路中支援閘道 DHCP。

對於未連線至閘道的獨立區段，僅支援本機 DHCP 伺服器。

以下限制適用於 IPv6 子網路上的 DHCPv6 伺服器組態：

- 設定了 IPv6 子網路的區段可以有本機 DHCPv6 伺服器或 DHCPv6 轉送。不支援閘道 DHCPv6。

- 不支援 DHCPv6 選項 (無類別靜態路由和一般選項)。

在區段上設定 DHCP

無論區段是否連線至閘道，您都可以在每個區段上設定 DHCP。同時支援用於 IPv4 (DHCPv4) 的 DHCP 和用於 IPv6 (DHCPv6) 的 DHCP 伺服器。

對於閘道連線的區段，支援所有下列類型的 DHCP：

- DHCP 本機伺服器
- DHCP 轉送
- 閘道 DHCP (僅支援區段中的 IPv4 子網路)

對於未連線至閘道的獨立區段，僅支援本機 DHCP 伺服器。

以下限制適用於 IPv6 子網路上的 DHCPv6 伺服器組態：

- 設定了 IPv6 子網路的區段可以有本機 DHCPv6 伺服器或 DHCPv6 轉送。不支援閘道 DHCPv6。
- 不支援 DHCPv6 選項 (無類別靜態路由和一般選項)。

必要條件

- 已在網路中新增 DHCP 設定檔。
- 如果您要在區段上設定閘道 DHCP，則必須將 DHCP 設定檔連結至直接連線的第 1 層或第 0 層閘道。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nsx-manager-ip-address>>。
- 2 選取 **網路 > 區段**。
- 3 新增或編輯一個區段。
 - 若要設定新區段，請按一下 **新增區段**。
 - 若要修改現有區段的內容，請按一下現有區段名稱旁邊的垂直省略符號，然後按一下 **編輯**。
- 4 如果要新增區段，請確保指定下列區段內容：
 - 區段名稱
 - 連線
 - 傳輸區域
 - 子網路 (閘道連線的區段為必要，對於獨立區段則為選用)

如果您正在編輯現有區段，請直接移至下一個步驟。

- 5 按一下 **設定 DHCP 組態**。

6 在 DHCP 類型下拉式功能表中，選取下列任何其中一個類型。

在區段中，IPv6 和 IPv4 子網路一律會使用相同的 DHCP 類型。不支援混合組態。

DHCP 類型	說明
DHCP 本機伺服器	<p>選取此選項可建立在區段上具有 IP 位址的本機 DHCP 伺服器。</p> <p>顧名思義，它是區段的本機 DHCP 伺服器，並且無法用於網路中的其他區段。本機 DHCP 伺服器僅為連結至區段的虛擬機器提供動態 IP 指派服務。</p> <p>您可以在區段上設定所有 DHCP 設定，包括 DHCP 範圍、DHCP 選項和靜態繫結。</p> <p>對於獨立區段，依預設會選取此類型。</p>
DHCP 轉送	<p>選取此選項，可將 DHCP 用戶端要求轉送至外部 DHCP 伺服器。外部 DHCP 伺服器可位於 SDDC 外部的任何子網路或實體網路中。</p> <p>區段的本機 DHCP 轉送服務，且無法用於網路中的其他區段。</p> <p>當您在區段上使用 DHCP 轉送時，您無法設定 DHCP 設定 和 DHCP 選項。UI 不會防止您設定 DHCP 靜態繫結。但是，在 NSX-T Data Center 3.0 中，使用 DHCP 轉送的靜態繫結是不支援的組態。</p>
閘道 DHCP	<p>此 DHCP 類型類似於中央 DHCP 服務，可在連線至閘道和使用閘道 DHCP 的所有區段上，動態地將 IP 和其他網路組態指派給虛擬機器。根據您連結至閘道的 DHCP 設定檔類型，您可以在區段上設定閘道 DHCP 伺服器或閘道 DHCP 轉送。</p> <p>依預設，連線至第 1 層或第 0 層閘道的區段會使用閘道 DHCP。如有需要，您可以選擇在區段上設定 DHCP 本機伺服器或 DHCP 轉送。</p> <p>若要在區段上設定閘道 DHCP，則必須將 DHCP 設定檔連結至閘道。</p> <p>如果 IPv4 子網路使用閘道 DHCP，則無法在相同區段的 IPv6 子網路中設定 DHCPv6，因為不支援閘道 DHCPv6。在此情況下，IPv6 子網路無法支援任何 DHCPv6 伺服器組態，包括 IPv6 靜態繫結。</p>

備註 在 NSX-T Data Center 3.0 和 3.0.1 中，建立區段之後且 DHCP 服務正在使用時，您無法變更閘道連線區段的 DHCP 類型。從 3.0.2 版開始，您可以變更閘道連線區段的 DHCP 類型。

7 在 DHCP 設定檔下拉式功能表中，選取 DHCP 伺服器設定檔或 DHCP 轉送設定檔的名稱。

- 如果區段連線至閘道，則依預設會選取閘道 DHCP 伺服器。系統會自動選取連結至閘道的 DHCP 設定檔。名稱和伺服器 IP 位址會從該 DHCP 設定檔自動擷取，並以唯讀模式顯示。

當區段使用閘道 DHCP 伺服器時，請確保已在閘道或 DHCP 伺服器設定檔 (或兩者) 中選取 Edge 叢集。如果 Edge 叢集在設定檔或閘道中無法使用，則儲存區段時會顯示錯誤訊息。
- 如果要在區段上設定本機 DHCP 伺服器或 DHCP 轉送，則必須從下拉式功能表中選取 DHCP 設定檔。如果下拉式功能表中沒有可用的設定檔，請按一下垂直省略符號圖示，然後建立 DHCP 設定檔。建立設定檔後，它會自動連結到區段。

當區段使用本機 DHCP 伺服器時，請確保 DHCP 伺服器設定檔包含 Edge 叢集。如果 Edge 叢集在設定檔中無法使用，則儲存區段時會顯示錯誤訊息。

備註 在 NSX-T Data Center 3.0 和 3.0.1 中，建立區段之後且 DHCP 服務正在使用時，您無法變更區段的 DHCP 設定檔。從 3.0.2 版開始，您可以變更使用 DHCP 本機伺服器或 DHCP 轉送之區段的 DHCP 設定檔。

8 按一下 IPv4 伺服器或 IPv6 伺服器索引標籤。

如果區段包含 IPv4 子網路和 IPv6 子網路，則您可以在區段上設定 DHCPv4 和 DHCPv6 伺服器。

9 設定 DHCP 設定。

a 按一下 **DHCP 組態** 切換按鈕，以啟用子網路上的 DHCP 組態設定。

b 在 **DHCP 伺服器位址** 文字方塊中，輸入 IP 位址。

- 如果您要設定 DHCP 本機伺服器，則需要伺服器 IP 位址。最多支援兩個伺服器 IP 位址。一個 IPv4 位址和一個 IPv6 位址。對於 IPv4 位址，首碼長度必須 ≤ 30 ，而對於 IPv6 位址，首碼長度必須 ≤ 126 。伺服器 IP 位址必須屬於您在此區段中指定的子網路。DHCP 伺服器 IP 位址不得與 DHCP 範圍和 DHCP 靜態繫結中的 IP 位址重疊。DHCP 伺服器設定檔可能包含伺服器 IP 位址，但是當您在區段上設定本機 DHCP 伺服器時，系統會忽略這些 IP 位址。

建立本機 DHCP 伺服器後，您可以在 **設定 DHCP 組態** 頁面上編輯伺服器 IP 位址。但是，新的 IP 位址必須屬於在區段中設定的相同子網路。

- 如果您要設定 DHCP 轉送，則此步驟不適用。伺服器 IP 位址會從 DHCP 轉送設定檔自動擷取，並顯示在設定檔名稱下方。
- 如果您要設定閘道 DHCP 伺服器，則此文字方塊無法編輯。伺服器 IP 位址會從連結至已連線閘道的 DHCP 設定檔中自動擷取。

請記住，DHCP 伺服器設定檔中的閘道 DHCP 伺服器 IP 位址可以與區段中設定的子網路不同。在此情況下，閘道 DHCP 伺服器會透過在建立閘道 DHCP 伺服器時自動建立的內部轉送服務，與區段的 IPv4 子網路連線。內部轉送服務會使用來自閘道 DHCP 伺服器 IP 位址子網路中的任何一個 IP 位址。內部轉送服務所使用的 IP 位址將用作閘道 DHCP 伺服器上的預設閘道，以與區段的 IPv4 子網路進行通訊。

建立閘道 DHCP 伺服器後，您可以在閘道的 DHCP 設定檔中編輯伺服器 IP 位址。但是，您無法變更已連結至閘道的 DHCP 設定檔。

- c (選擇性) 在 **DHCP 範圍** 文字方塊中，輸入一或多個 IP 位址範圍。

同時允許 IP 範圍和 IP 位址。IPv4 位址必須採用 CIDR /32 格式，且 IPv6 位址必須採用 CIDR /128 格式。您也可以透過在範圍的開頭和結尾輸入相同的 IP 位址，以輸入 IP 位址作為範圍。例如，172.16.10.10-172.16.10.10。

確保您的 DHCP 範圍符合以下需求：

- DHCP 範圍中的 IP 位址必須屬於在區段上設定的子網路。也就是說，DHCP 範圍不能包含來自多個子網路的 IP 位址。
- IP 範圍不得與 DHCP 伺服器 IP 位址和 DHCP 靜態繫結 IP 位址重疊。
- DHCP IP 集區中的 IP 範圍不得彼此重疊。
- 任何 DHCP 範圍中的 IP 位址數目不得超過 65536。

備註 在 DHCP 的 IPv6 範圍中不允許使用下列類型的 IPv6 位址：

- 連結本機單點傳播位址 (FE80::/64)
- 多點傳播位址 (FF00::/8)
- 未指定的位址 (0:0:0:0:0:0:0:0)
- 全為 F (F:F:F:F:F:F:F:F) 的位址

注意 建立 DHCP 伺服器後，您可以更新現有範圍、附加新的 IP 範圍或刪除現有範圍。但是，最佳做法是避免刪除、縮小或擴充現有的 IP 範圍。例如，不要嘗試合併多個較小的 IP 範圍以建立單一大型 IP 範圍。您可能會意外遺漏包含 IP 位址，這些位址已租用給來自較大 IP 範圍的 DHCP 用戶端。因此，當您在 DHCP 服務執行後修改現有範圍時，可能會導致 DHCP 用戶端中斷網路連線，並導致暫時的流量中斷。

- d (選擇性) (僅適用於 DHCPv6)：在 **排除的範圍** 文字方塊中，輸入您想要針對 DHCPv6 用戶端之動態 IP 指派排除的 IPv6 位址或 IPv6 位址範圍。

在 IPv6 網路中，DHCP 範圍可能很大。有時，您可能想要針對靜態繫結保留特定 IPv6 位址，或來自大型 DHCP 範圍的多個小型 IPv6 位址範圍。在這種情況下，您可以指定排除的範圍。

- e (選擇性) 編輯租用時間 (以秒為單位)。

預設值為 86400。值的有效範圍為 60-4294967295。在 DHCP 伺服器組態中設定的租用時間會優先於您在 DHCP 設定檔中指定的租用時間。

- f (選擇性) (僅適用於 DHCPv6)：輸入慣用時間 (以秒為單位)。

慣用時間是慣用之有效 IP 位址的時間長度。當慣用時間到期時，IP 位址將變為過時。如果未輸入任何值，則慣用時間將自動計算為 (租用時間 * 0.8)。

租用時間必須大於慣用時間。

值的有效範圍為 60-4294967295。預設值為 69120。

g (選擇性) 輸入要用於名稱解析之網域名稱伺服器 (DNS) 的 IP 位址。最多允許兩個 DNS 伺服器。
未指定時，系統不會為 DHCP 用戶端指派 DNS。DNS 伺服器 IP 位址必須與子網路的閘道 IP 位址屬於相同的子網路。

h (選擇性) (僅適用於 DHCPv6)：輸入一或多個網域名稱。
DHCPv4 組態會自動擷取您在區段組態中指定的網域名稱。

i (選擇性) (僅適用於 DHCPv6)：輸入簡易網路時間通訊協定 (SNTP) 伺服器的 IP 位址。最多允許兩個 SNTP 伺服器。

在 NSX-T Data Center 3.0 中，DHCPv6 伺服器不支援 NTP。

DHCPv4 伺服器僅支援 NTP。若要新增 NTP 伺服器，請按一下**選項**，然後新增一般選項 (代碼 42 - NTP 伺服器)。

10 (選擇性) 按一下**選項**，然後指定無類別靜態路由 (選項 121) 和一般選項。

在 NSX-T Data Center 3.0 中，不支援 IPv6 的 DHCP 選項。

- IPv4 的 DHCP 中的每個無類別靜態路由選項可以有具有相同目的地的多個路由。每個路由都包含目的地子網路、子網路遮罩和下一個躍點路由器。如需 DHCPv4 中無類別靜態路由的相關資訊，請參閱 RFC 3442 規格。您可以在 DHCPv4 伺服器上新增最多 127 個無類別靜態路由。
- 若要新增一般選項，請選取選項的代碼，然後輸入選項的值。對於二進位值，值必須為 base-64 編碼格式。

11 按一下**套用**以儲存 DHCP 組態，然後按一下**儲存**以儲存區段組態。

後續步驟

- 在區段上設定了 DHCP 之後，某些限制和須知適用於變更區段連線。如需詳細資訊，請參閱[案例：在 DHCP 上變更區段連線的影響](#)。
- 當 DHCP 伺服器設定檔連結至使用 DHCP 本機伺服器的區段時，系統會在您於 DHCP 設定檔中指定的 Edge 叢集中建立 DHCP 服務。但是，如果區段使用閘道 DHCP 伺服器，則在其中建立 DHCP 服務的 Edge 叢集將取決於多個因素的組合。如需如何為 DHCP 服務選取 Edge 叢集的詳細資訊，請參閱[案例：為 DHCP 服務選取 Edge 叢集](#)。

在區段上設定 DHCP 靜態繫結

您可以同時針對 IPv4 的 DHCP 和 IPv6 的 DHCP 伺服器設定靜態繫結。

在一般網路環境中，您擁有執行服務的虛擬機器，例如 FTP、電子郵件伺服器或應用程式伺服器。您可能不希望這些虛擬機器的 IP 位址在您的網路中變更。在此情況下，您可以將靜態 IP 位址繫結到每部虛擬機器的 MAC 位址 (DHCP 用戶端)。靜態 IP 位址不得與 DHCP IP 範圍和 DHCP 伺服器 IP 位址重疊。

當您在區段上設定本機 DHCP 伺服器或閘道 DHCP 伺服器時，系統會允許 DHCP 靜態繫結。當區段使用 DHCP 轉送時，UI 不會防止您設定 DHCP 靜態繫結。但是，在 NSX-T Data Center 3.0 中，使用 DHCP 轉送的靜態繫結是不支援的組態。

必要條件

您要設定 DHCP 靜態繫結的區段必須已在網路中儲存。

程序

- 1 從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 在您要編輯的區段旁邊，按一下垂直省略符號，然後按一下 **編輯**。
- 4 展開 **DHCP 靜態繫結區段**，然後在 **DHCP 靜態繫結** 旁，按一下 **設定**。

依預設，此時會顯示 **IPv4 靜態繫結** 頁面。若要繫結 IPv6 位址，請確保先按一下 **IPv6 靜態繫結索引** 標籤，然後繼續進行下一個步驟。

5 按一下新增靜態繫結。

a 指定 DHCP 靜態繫結選項。

下表說明 IPv4 的 DHCP 和 IPv6 的 DHCP 伺服器通用的靜態繫結選項。

選項	說明
名稱	輸入可識別每個靜態繫結的唯一顯示名稱。名稱長度必須受限於 255 個字元。
IP 位址	<ul style="list-style-type: none"> ■ IPv4 靜態繫結為必要。輸入要繫結到用戶端 MAC 位址的單一 IPv4 位址。 ■ IPv6 靜態繫結為選用。輸入要繫結到用戶端 MAC 位址的單一全域單點傳播 IPv6 位址。 <p>未指定靜態繫結的 IPv6 位址時，無狀態位址自動組態 (SLAAC) 會用來自動將 IPv6 位址指派給 DHCPv6 用戶端。此外，您也可以使用無狀態 DHCP 將其他 DHCP 組態選項 (如 DNS、網域名稱等) 指派給 DHCPv6 用戶端。</p> <p>如需有關 IPv6 無狀態 DHCP 的詳細資訊，請參閱 RFC 3376 規格。</p> <p>IPv6 靜態繫結中不允許使用下列類型的 IPv6 位址：</p> <ul style="list-style-type: none"> ■ 連結本機單點傳播位址 (FE80::/64) ■ 多點傳播 IPv6 位址 (FF00::/8) ■ 未指定的位址 (0:0:0:0:0:0:0:0) ■ 全為 F (F:F:F:F:F:F:F:F) 的位址 <p>靜態 IP 位址必須屬於在區段上設定的子網路 (如有)。</p>
MAC 位址	<p>必要。輸入您要繫結靜態 IP 位址之 DHCP 用戶端的 MAC 位址。</p> <p>下列驗證適用於靜態繫結中的 MAC 位址：</p> <ul style="list-style-type: none"> ■ MAC 位址在使用本機 DHCP 伺服器區段上的所有靜態繫結中必須是唯一的。 ■ MAC 位址在所有連線至閘道且使用閘道 DHCP 伺服器之所有區段的靜態繫結中，都必須是唯一的。 <p>例如，假設您有 10 個區段連線至第 1 層閘道。您將一個閘道 DHCP 伺服器用於四個區段 (Segment1 至 Segment4)，以及將一個本機 DHCP 伺服器用於剩餘六個區段 (Segment5 至 Segment10)。假設您在使用閘道 DHCP 伺服器的所有四個區段 (Segment1 到 Segment4) 之間總計有 20 個靜態繫結。此外，使用本機 DHCP 伺服器的其他六個區段 (Segment5 到 Segment10) 中的每個都有五個靜態繫結。在此範例中：</p> <ul style="list-style-type: none"> ■ 20 個靜態繫結中的每個 MAC 位址，在使用閘道 DHCP 伺服器的所有區段 (Segment1 到 Segment4) 之間必須是唯一的。 ■ 五個靜態繫結中的 MAC 位址，在使用本機 DHCP 伺服器的每個區段 (Segment5 到 Segment10) 上必須是唯一的。
租用時間	<p>選擇性。輸入 IP 位址繫結至 DHCP 用戶端的時間長度 (以秒為單位)。租用時間到期時，IP 位址會變為無效，且 DHCP 伺服器可以將該位址指派給區段上的其他 DHCP 用戶端。</p> <p>值的有效範圍為 60-4294967295。預設值為 86400。</p>
說明	選擇性。輸入靜態繫結的說明。
標籤	<p>選擇性。新增標籤以標記靜態繫結，以便您可以快速搜尋或篩選繫結、疑難排解和追蹤繫結相關問題，或執行其他工作。</p> <p>如需有關為標記物件新增標籤和使用案例的詳細資訊，請參閱 標籤。</p>

下表說明僅在 IPv4 之 DHCP 伺服器中提供的靜態繫結選項。

IPv4 的 DHCP 選項	說明
閘道位址	輸入 IPv4 的 DHCP 伺服器必須提供給 DHCP 用戶端的預設閘道 IP 位址。
主機名稱	<p>輸入 IPv4 的 DHCP 用戶端的主機名稱，以便 DHCPv4 伺服器一律可將用戶端 (主機) 繫結為相同的 IPv4 位址。</p> <p>主機名稱長度必須受限於 63 個字元。</p> <p>下列驗證適用於靜態繫結中的主機名稱：</p> <ul style="list-style-type: none"> ■ 主機名稱在使用本機 DHCP 伺服器的區段上的所有靜態繫結中必須是唯一的。 ■ 主機名稱在所有連線至閘道且使用閘道 DHCP 伺服器的所有區段的靜態繫結中，都必須是唯一的。 <p>例如，假設您有 10 個區段連線至第 1 層閘道。您將一個閘道 DHCP 伺服器用於四個區段 (Segment1 至 Segment4)，以及將一個本機 DHCP 伺服器用於剩餘六個區段 (Segment5 至 Segment10)。假設您在使用閘道 DHCP 伺服器的所有四個區段 (Segment1 到 Segment4) 之間總計有 20 個靜態繫結。此外，使用本機 DHCP 伺服器的其他六個區段 (Segment5 到 Segment10) 中的每個都有五個靜態繫結。在此範例中：</p> <ul style="list-style-type: none"> ■ 20 個靜態繫結中的每個主機名稱，在使用閘道 DHCP 伺服器的所有區段 (Segment1 到 Segment4) 之間必須是唯一的。 ■ 五個靜態繫結中的主機名稱，在使用本機 DHCP 伺服器的每個區段 (Segment5 到 Segment10) 上必須是唯一的。
DHCP 選項	選擇性。按一下 設定 ，為 IPv4 無類別靜態路由和其他一般選項設定 DHCP。

DHCPv4 靜態繫結的一些其他附註：

- IPv4 靜態繫結會自動繼承您在區段上設定的網域名稱。
- 若要在靜態繫結組態中指定 DNS 伺服器，請新增一般選項 (代碼 6 - DNS 伺服器)。
- 若要在具有 DHCPv4 伺服器的 DHCPv4 用戶端上同步系統時間，請使用 NTP。IPv4 的 DHCP 伺服器不支援 SNTP。
- 如果未在靜態繫結中指定 DHCP 選項，則來自區段上 DHCPv4 伺服器的 DHCP 選項會自動在靜態繫結中繼承。但是，如果您在靜態繫結中明確新增了一或多個 DHCP 選項，則這些 DHCP 選項將不會從區段上的 DHCPv4 伺服器自動繼承。

下表說明僅在 IPv6 的 DHCP 伺服器中提供的靜態繫結選項。

IPv6 的 DHCP 選項	說明
DNS 伺服器	選擇性。輸入最多兩個要用於名稱解析的網域名稱伺服器。 未指定時，系統不會為 DHCP 用戶端指派 DNS。
SNTP 伺服器	選擇性。輸入最多兩個簡易網路時間通訊協定 (SNTP) 伺服器。用戶端會使用這些 SNTP 伺服器，將其系統時間同步為標準時間伺服器的時間。
慣用時間	選擇性。輸入慣用的有效 IP 位址的時間長度。當慣用時間到期時，IP 位址將變為過時。如果未輸入任何值，則慣用時間將自動計算為 (租用時間 * 0.8)。租用時間必須大於慣用時間。

IPv6 的 DHCP 選項	說明
	值的有效範圍為 60-4294967295。預設值為 69120。
網域名稱	選擇性。輸入要提供給 DHCPv6 用戶端的網域名稱。IPv6 靜態繫結中支援多個網域名稱。 未指定時，系統不會為 DHCP 用戶端指派網域名稱。

DHCPv6 靜態繫結的一些其他附註：

- 閘道 IP 位址組態在 IPv6 靜態繫結中無法使用。IPv6 用戶端會從 ICMPv6 路由器通告 (RA) 訊息學習第一個躍點路由器。
- DHCPv6 靜態繫結中不支援 NTP。

b 設定每個靜態繫結後，按一下 **儲存**。

第 2 層橋接

使用第 2 層橋接，您可以連線至支援 VLAN 的連接埠群組或位於 NSX-T Data Center 部署外部的裝置 (例如閘道)。第 2 層橋接器在移轉案例中也很有用，因為您需要在實體和虛擬工作負載間分割子網路。

第 2 層橋接器需要 Edge 叢集和 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。設定區段時，您可以指定 Edge 橋接器設定檔，以啟用第 2 層橋接。

建立 Edge 橋接器設定檔

Edge 橋接器設定檔使 NSX Edge 叢集能夠為區段提供第 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 從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 > Edge 橋接器設定檔**。
- 3 按一下 **新增 Edge 橋接器設定檔**。
- 4 輸入 Edge 橋接器設定檔的名稱，並選擇性地輸入說明。
- 5 選取 NSX Edge 叢集。

- 6 選取主要節點。
- 7 選取備份節點。
- 8 選取容錯移轉模式。

選項為先佔式和非先佔式。

- 9 按一下 **儲存**。

後續步驟

設定以 Edge 為基礎的橋接。請參閱[設定以 Edge 為基礎的橋接](#)。

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 橋接器設定檔之後，需要為在虛擬機器中執行的 Edge 節點進行一些額外的組態設定。

請注意，不支援在相同的 Edge 節點上橋接同一區段兩次。但是，您可以將兩個 VLAN 橋接至兩個不同 Edge 節點上的相同區段。

根據您的環境選擇下列其中一個選項。

備註 如果您要將區段橋接至 VLAN 0，並在此區段上使用分散式路由器，則在使用 MAC 學習時，閘道可能不會路由 VLAN 0 流量。在此案例中，您應避免使用選項 3 (如果 Edge 虛擬機器連結至為 NSX for vSphere 準備的 VDS 連接埠群組，甚至應避免使用選項 2a)。

選項 1：Edge 虛擬機器位於 VSS 連接埠群組上

此選項適用於 Edge 虛擬機器連線至 VSS (vSphere 標準交換器) 時。您必須啟用混合模式和偽造的傳輸。

- 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。
- 作用中和待命 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 2a：Edge 虛擬機器位於 VDS 6.6.0 (或更新版本) 連接埠群組上

此選項適用於 Edge 虛擬機器連線至 VDS (vSphere Distributed Switch) 時。您必須執行 ESXi 6.7 或更新版本以及 VDS 6.6.0 或更新版本。

- 透過使用 VIM API `DVSMacLearningPolicy` 並將 `allowUnicastFlooding` 設定為 `true`，以在連接埠群組上啟用 MAC 學習並使用選項「允許單點傳播洪泛」。

選項 2b：Edge 虛擬機器位於 VDS 6.5.0 (或更新版本) 連接埠群組上

此選項適用於 Edge 虛擬機器連線至 VDS (vSphere Distributed Switch) 時。您需要啟用混合模式和偽造的傳輸。

- 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。
- 作用中和待命 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 3：Edge 虛擬機器已連線至 NSX-T 區段

如果 Edge 部署在已安裝 NSX-T 的主機上，則它可以連線至 VLAN 區段並使用 MAC 學習，而這是慣用的組態選項。

- 若要建立新的 MAC 探索區段設定檔，請導覽至 **網路 > 區段 > 區段設定檔**。
 - 按一下 **新增區段設定檔 > MAC 探索 >**。
 - 啟用 **MAC 學習**。這也將會啟用 **未知單點傳播洪泛**。保持洪泛選項處於啟用狀態，以便在所有案例下均可正常橋接。
- 若要編輯 Edge 所使用的區段，請導覽至 **網路 > 區段**。
 - 按一下功能表圖示 (3 個點)，並選取 **編輯** 以編輯區段。
 - 在 **區段設定檔** 區段中，將 **MAC 探索** 設定檔設定為以上所建立的設定檔。

後續步驟

將區段與橋接器設定檔建立關聯。請參閱 [建立第 2 層橋接器備份區段](#)。

建立第 2 層橋接器備份區段

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區段，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。
- 設定下列其中一個選項：混合模式、MAC 學習或接收連接埠。請參閱設定以 Edge 為基礎的橋接。
- 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，且符合橋接器支援區段的 VLAN 識別碼。
- 覆疊傳輸區域中的一個區段會用作橋接器支援的區段。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取 **網路 > 區段**
- 3 按一下您想要設定第 2 層橋接所在的覆疊區段的功能表圖示 (三個點)，然後選取 **編輯**。
- 4 在 **Edge 橋接器** 欄位中，按一下 **設定**。
- 5 按一下 **新增 Edge 橋接器**。
您可以新增一或多個 Edge 橋接器設定檔。
- 6 選取 Edge 橋接器設定檔。
- 7 選取傳輸區域。
- 8 輸入 VLAN 識別碼或 VLAN 主幹規格 (指定 VLAN 範圍，而非個別 VLAN)。
- 9 (選擇性) 選取整併原則。
- 10 按一下 **新增**。

結果

您可以測試橋接器的功能，方法是將 ping 動作從連結至區段的虛擬機器傳送到 NSX-T 部署外部的裝置。

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。

程序

- 1 從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 > 中繼資料 Proxy**。

- 3 按一下**新增中繼資料 Proxy**。
- 4 輸入中繼資料 Proxy 伺服器的名稱。
- 5 在**伺服器位址欄位**中，輸入 Nova 伺服器的 URL 和連接埠。

有效的連接埠範圍為 3000 - 9000。

- 6 選取 Edge 叢集。
- 7 (選擇性) 選取 Edge 節點。

如果您選取任何 Edge 節點，則無法在下一個步驟中啟用**待命重新放置**。

- 8 (選擇性) 啟用**待命重新放置**。

待命重新放置表示，如果執行中繼資料 Proxy 的 Edge 節點失敗，中繼資料 Proxy 將在待命 Edge 節點上執行。如果您未選取任何 Edge 節點，則只能啟用待命重新放置。

- 9 在**共用簽章密碼欄位**中，輸入中繼資料 Proxy 將用來存取 Nova 伺服器的密碼。

- 10 (選擇性) 選取用於與 Nova 伺服器進行加密通訊的憑證。

- 11 (選擇性) 選取密碼編譯通訊協定。

選項包括 TLSv1、TLSv1.1 和 TLSv1.2。依預設會支援 TLSv1.1 和 TLSv1.2。

主機交換器

5

主機交換器管理的物件是為網路中的各種主機提供網路服務的虛擬網路交換器。它會在參與 NSX-T 網路的每台主機上具現化

NSX-T 中支援下列主機交換器：

- NSX-T 虛擬分散式交換器：NSX-T 推出了主機交換器，可將各種運算網域之間的連線標準化，包括多個 VMware vCenter Server 執行個體、KVM、容器，以及其他的外部部署或雲端實作。

可根據環境中所需的效能設定 NSX-T 虛擬分散式交換器：

- 標準：針對一般工作負載進行設定，其中的工作負載預期有正常的流量輸送量。
- 增強型：針對電信工作負載進行設定，其中的工作負載預期有高流量輸送量。
- vSphere Distributed Virtual Switch：為與 vCenter Server 環境中的交換器相關聯的所有主機的網路組態提供集中式管理和監控。

本章節討論下列主題：

- [在 vSphere Distributed Switch 上管理 NSX-T](#)
- [進階網路堆疊](#)
- [將主機交換器移轉到 vSphere Distributed Switch](#)
- [NSX 虛擬分散式交換器](#)

在 vSphere Distributed Switch 上管理 NSX-T

您可以在 vSphere Distributed Switch (VDS) 交換器上設定和執行 NSX-T。

在 NSX-T 3.0 中，可以透過在 VDS 交換器上安裝 NSX-T 來準備主機傳輸節點。若要準備將 NSX Edge 虛擬機器作為傳輸節點，您僅能使用 N-VDS 交換器。但是，您可以根據網路中的拓撲，將 NSX Edge 虛擬機器連線至任何支援的交換器 (VSS、VDS 或 N-VDS)。

準備使用 VDS 作為主機交換器的傳輸節點主機叢集後，您可以執行下列操作：

- 在 VDS 交換器上管理 NSX-T 傳輸節點。
- 將在 NSX-T 中建立的區段實現為 vCenter Server 中的 NSX 分散式虛擬連接埠群組。
- 在 vSphere 分散式虛擬連接埠群組與 NSX 分散式虛擬連接埠群組之間移轉虛擬機器。
- 傳送在這兩個類型的連接埠群組上執行的虛擬機器流量。

設定 vSphere Distributed Switch

在 VDS 主機交換器上設定傳輸節點時，部分網路參數僅可在 vCenter Server 中設定。

若要在 VDS 主機交換器上安裝 NSX-T，必須符合下列需求：

- vCenter Server 7.0 或更新版本
- ESXi 7.0 或更新版本

已建立的 VDS 交換器可設定為集中管理 NSX-T 主機的網路。

若要為 NSX-T 網路設定 VDS 交換器，需要在 NSX-T 和 vCenter Server 中設定物件。

- 在 vSphere 中：
 - 建立 VDS 交換器。
 - 將 MTU 設定為至少 1600
 - 將 ESXi 主機新增至交換器。這些主機稍後會準備做為 NSX-T 傳輸節點。
 - 將上行指派給實體 NIC。
- 在 NSX-T 中：
 - 設定傳輸節點時，將在 NSX-T 上行設定檔中建立的上行與 VDS 中的上行對應。

如需在 VDS 交換器上準備主機傳輸節點的更多詳細資料，請參閱《NSX-T Data Center 安裝指南》。

下列參數僅可在 VDS 支援的主機交換器上的 vCenter Server 中設定：

組態	VDS	NSX-T	說明
MTU	<p>在 vCenter Server 中，於交換器上設定 MTU 值。</p> <p>備註 VDS 交換器必須具有 1600 或更高的 MTU。</p> <p>在 vCenter Server 中，選取 VDS，按一下 動作 → 設定 → 編輯設定。</p>	<p>隨即會覆寫 NSX-T 上行設定檔中設定的任何 MTU 值。</p>	<p>做為使用 VDS 準備做為主機交換器的主機傳輸節點，需要在 vCenter Server 中的 VDS 交換器上設定 MTU 值。</p>
上行/LAG	<p>在 vCenter Server 中，於 VDS 交換器上設定上行/LAG。</p> <p>在 vCenter Server 中，選取 VDS，按一下 動作 → 設定 → 編輯設定。</p>	<p>傳輸節點備妥時，NSX-T 上的整併原則會與 VDS 交換器上設定的上行/LAG 對應。</p> <p>備註 N-VDS 交換器上會備妥傳輸節點，整併原則會對應至實體 NIC。</p>	<p>做為使用 VDS 準備做為主機交換器的主機傳輸節點，會在 VDS 交換器上設定上行或 LAG。在組態期間，NSX-T 需要為傳輸節點設定整併原則。此整併原則會對應至 VDS 交換器上設定的上行/LAG。</p>
NIOC	<p>在 vCenter Server 中設定。</p> <p>在 vCenter Server 中，選取 VDS，按一下 動作 → 設定 → 編輯設定。</p>	<p>使用 VDS 交換器準備主機傳輸節點時，無法使用 NIOC 組態。</p>	<p>做為使用 VDS 準備做為主機交換器的主機傳輸節點，只能在 vCenter Server 中設定 NIOC 設定檔。</p>

組態	VDS	NSX-T	說明
連結層探索通訊協定 (LLDP)	在 vCenter Server 中設定。 在 vCenter Server 中，選取 VDS，按一下 動作 → 設定 → 編輯設定 。	使用 VDS 交換器準備主機傳輸節點時，無法使用 LLDP 組態。	做為使用 VDS 準備做為主機交換器的主機傳輸節點，只能在 vCenter Server 中設定 LLDP 設定檔。
新增或管理主機	在 vCenter Server 中管理。 在 vCenter Server 中，前往 網路 → VDS 交換器 → 新增和管理主機 。	準備做為 NSX-T 中的傳輸節點。	使用 VDS 交換器準備傳輸節點之前，必須將該節點新增至 vCenter Server 中的 VDS 交換器。

備註 這些虛擬機器的 NIOC 設定檔、連結層探索通訊協定 (LLDP) 設定檔和連結彙總群組 (LAG) 是由 VDS 交換器管理，而不是由 NSX-T 管理。身為 vSphere 管理員，請從 vCenter Server UI 或透過呼叫 VDS API 命令來設定這些參數。

使用 VDS 準備主機傳輸節點做為主機交換器後，主機交換器類型會將 VDS 顯示為主機交換器。它會在 NSX-T 和相關聯的傳輸區域中顯示已設定的上行設定檔。

The screenshot shows the vCenter Server interface for configuring a VDS switch. On the left, there is a list of hosts under the '主機傳輸節點' (Host Transport Nodes) tab. The selected host is '2-cluster-606 (1)'. A configuration window is open for the VDS switch '2-switch-780'. The window shows the following details:

名稱	類型	上行設定檔	傳輸區域
2-switch-780	VDS	b372767d-94e2-4...	3-transportzone-164 4-transportzone-6...

在 vCenter Server 中，用於準備 NSX-T 主機 VDS 交換器會建立為 NSX 交換器。


The screenshot shows the vCenter Server interface for configuring a virtual switch. On the left, there is a list of storage devices under the '儲存區' (Storage) tab. The selected storage device is 'NSX 交換器: DSwitch'. A configuration window is open for the virtual switch 'NSX 交換器: DSwitch'. The window shows the switch name and the management view icon.

管理 NSX 分散式虛擬連接埠群組

使用 VDS 準備做為主機交換器的傳輸節點，可確保在 NSX-T 中建立的區段會在 VDS 交換器和 NSX-T 中的區段上實現為 NSX 分散式虛擬連接埠群組。

在舊版 NSX-T Data Center 中，於 NSX-T 中建立的區段會呈現為 vCenter Server 中的不透明網路。在 VDS 交換器上執行 NSX-T 時，區段會呈現為 NSX 分散式虛擬連接埠群組。

在 vCenter Server 中，對 NSX-T 網路上的區段所做的任何變更都會同步。

在 vCenter Server 中，NSX 分散式虛擬連接埠群組會呈現為 。



在 NSX-T 中建立的任何 NSX-T 區段會在 vCenter Server 中實現為 NSX-T 物件。vCenter Server 會顯示與 NSX-T 區段相關的下列詳細資料：

- NSX Manager
- 區段的虛擬網路識別碼
- 傳輸區域
- 連結的虛擬機器

區段的連接埠繫結依預設會設定為**暫時**。在 NSX-T 中設定之交換器的切換參數無法在 vCenter Server 中編輯，反之亦然。

重要 在 vCenter Server 中，NSX 分散式虛擬連接埠群組的實現不需要唯一的名稱，即可將其與 VDS 交換器上的其他連接埠群組區分。因此，多個 NSX 分散式虛擬連接埠群組可以具有相同名稱。使用連接埠群組名稱的任何 vSphere 自動化都可能會導致錯誤。

在 vCenter Server 中，您可以對 NSX 分散式虛擬連接埠群組執行下列動作：

- 新增 VMkernel 介面卡。
- 將虛擬機器移轉至其他網路。

但是，與 NSX 分散式虛擬連接埠群組相關的 NSX-T 物件只能在 NSX Manager 中進行編輯。您可以編輯這些區段內容：

- 區段的複寫模式
- 區段使用的 VLAN 主幹識別碼

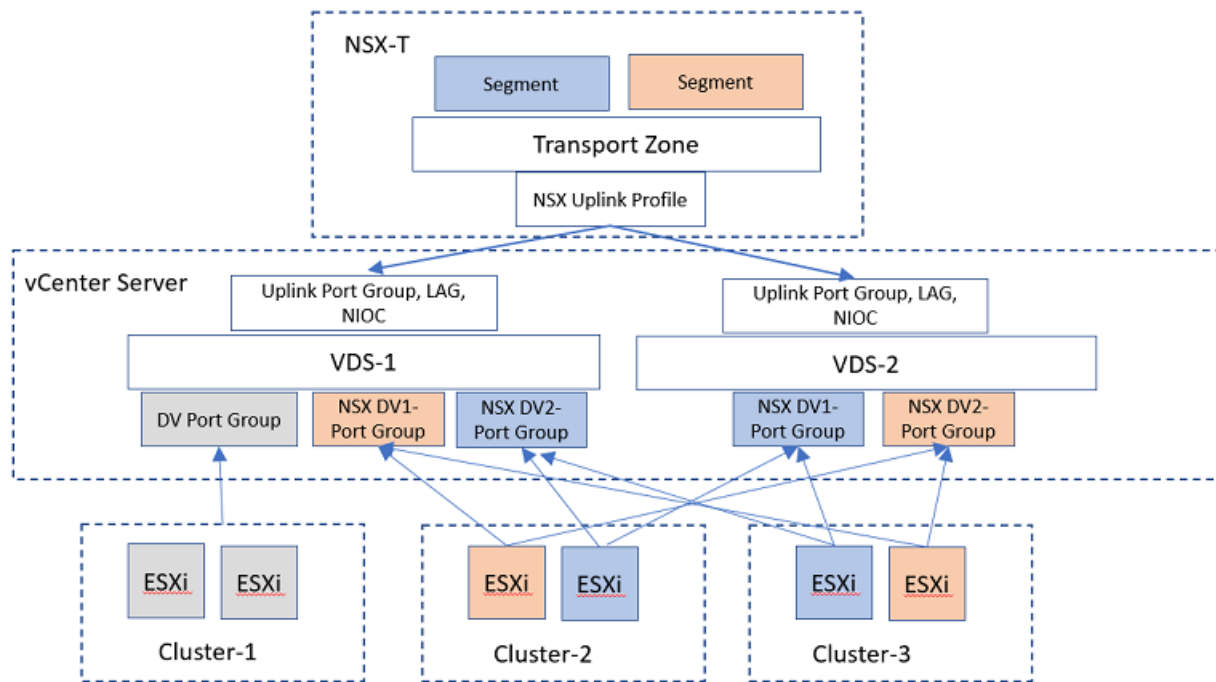
- 交換設定檔 (例如連接埠鏡像)
- 在區段上建立的連接埠

選擇交換器	識別碼	管理狀態	邏輯連接埠	流量類型	組態狀態	傳輸區域
3-switch-1533	e303...c391	開啟	0	覆蓋: 67586	成功	nsx-overlay-transportzone
4-switch-351	356e...d0e4	開啟	0	VLAN: 21	成功	VXLANTZ

如需如何設定 vSphere 分散式虛擬連接埠群組的詳細資料，請參閱《vSphere 網路指南》。

使用 VDS 準備的 NSX-T 叢集

使用 VDS 準備為主機交換器的 NSX-T 叢集的範例。



在範例拓撲圖中，設定了兩個 VDS 交換器來管理 NSX-T 流量和 vSphere 流量。

VDS-1 和 VDS-2 設定為管理來自 Cluster-1、Cluster-2 和 Cluster-3 ESXi 主機的網路。Cluster-1 已備妥僅執行 vSphere 流量，而 Cluster-2 和 Cluster-3 則準備做為這些 VDS 交換器的主機傳輸節點。

在 vCenter Server 中，VDS 交換器上的上行連接埠群組會獲指派實體 NIC。在拓撲中，VDS-1 和 VDS-2 的上行會被指派給實體 NIC。視 ESXi 主機的硬體組態而定，您可能想要規劃要指派給交換器的實體 NIC 數目。除了將上行指派給 VDS 交換器，還會在 VDS 交換器上設定 MTU、NIOC、LLDP、LAG 設定檔。

設定 VDS 交換器後，在 NSX-T 中新增上行設定檔。

透過套用傳輸節點設定檔 (在 VDS 交換器上) 來準備叢集時，來自傳輸節點設定檔的上行會對應至 VDS 上行。相反地，在 N-VDS 交換器上準備叢集時，來自傳輸節點設定檔的上行會直接對應至實體 NIC。

準備叢集後，在 Cluster-2 和 Cluster-3 上的 ESXi 主機管理 NSX-T 流量，而 Cluster-1 會管理 vSphere 流量。

用來在 NSX-T Data Center 上設定 vSphere Distributed Switch 的 API

這些 NSX-T Data Center API 命令用來支援 NSX-T Data Center 上的 vSphere Distributed Switch。

針對 vSphere Distributed Switch 的 API 變更

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

備註 使用 API 命令完成的組態也可以從 vCenter Server 使用者介面完成。如需有關使用 vSphere Distributed Switch 建立 NSX-T Data Center 傳輸節點做為主機交換器的詳細資訊，請參閱《NSX-T Data Center 安裝指南》中的〈設定受管理的主機傳輸節點〉主題。

API

在 vSphere Distributed Switch (VDS) 上的 NSX-T

針對探索到的節點建立傳輸節點。

/api/v1/fabric/discovered-nodes/<external-id/discovered-node-id?>action=cr

```
{
  "node_id":
    "d7ef478b-752c-400a-b5f0-207c04567e5d", "host_switch_spec": {
    "host_switches": [
      {
        "host_switch_name": "vds-1",
        "host_switch_id":
          "50 2b 92 54 e0 80 d8 d1-ee ab 8d a6 7b fd f9 4b",
        "host_switch_type": "VDS",
        "host_switch_mode": "STANDARD",
        "host_switch_profile_ids": [
          {
            "key": "UplinkHostSwitchProfile",
            "value":
              "159353ae-c572-4aca-9469-9582480a7467"
          }
        ],
        "pnics": [],
        "uplinks": [
          {
            "vds_uplink_name": "Uplink 2",
            "uplink_name": "nsxuplink1"
          }
        ],
        "is_migrate_pnics": false,
        "ip_assignment_spec": {
          "resource_type": "AssignedByDhcp"
        },
        "cpu_config": [],
        "transport_zone_endpoints": [
          {
            "transport_zone_id":
              "06ba5326-67ac-4f2c-9953-a8c5d326b51e",
            "transport_zone_profile_ids": [
              {
                "resource_type": "BfdHealthMonitoringProfile",
                "profile_id":
                  "52035bb3-ab02-4a08-9884-18631312e50a"
              }
            ]
          }
        ],
        "vmk_install_migration": [],
        "pnics_uninstall_migration": [],
        "vmk_uninstall_migration": [],
        "not_ready": false
      }
    ],
    "resource_type": "StandardHostSwitchSpec"
  },
  "transport_zone_endpoints": [],
  "maintenance_mode": "DISABLED",
  "is_overridden": false,
  "resource_type": "TransportNode",
  "display_name": "TestTN",
}
```

虛擬機器組態

vim.vm.device.VirtualEthernetCard.DistributedVirtualPortBackingInfo

API	在 vSphere Distributed Switch (VDS) 上的 NSX-T
VMkernel NIC	<code>vim.dvs.DistributedVirtualPort</code>
實體 NIC 與上行的對應	API : <code>vim.host.NetworkSystem:networkSystem.updateNetworkConfig</code> 內容 : <code>vim.host.NetworkConfig.proxySwitch</code>
MTU	API : <code>vim.dvs.VmwareDistributedVirtualSwitch.reconfigure</code> 內容 : <code>VmwareDistributedVirtualSwitch.ConfigSpec.maxMtu</code>
LAG	API : <code>vim.dvs.VmwareDistributedVirtualSwitch.updateLacpGroupConfig</code> 內容 : <code>vim.dvs.VmwareDistributedVirtualSwitch.LacpGroupSpec</code>
NIOC	API : <code>vim.dvs.VmwareDistributedVirtualSwitch.reconfigure</code> 內容 : <code>vim.dvs.VmwareDistributedVirtualSwitch.ConfigSpec.infrastructureTraffic</code>
LLDP	API : <code>vim.dvs.VmwareDistributedVirtualSwitch.reconfigure</code> 內容 : <code>vim.dvs.VmwareDistributedVirtualSwitch.ConfigSpec.linkDiscoveryProtocol</code>

vSphere Distributed Switch 中已啟用以支援 NSX-T Data Center 的功能支援

早於 7.0 和 VDS 版本 7.0 或更新版本的 VDS 交換器版本 (已啟用 NSX-T Data Center) 所支援功能的比較。

IPFIX 和連接埠鏡像

使用 VDS 交換器準備的 NSX-T 傳輸節點支援 IPFIX、連接埠鏡像。

請參閱 [vSphere Distributed Switch 上的連接埠鏡像](#)。

請參閱 [vSphere Distributed Switch 上的 IPFIX 監控](#)。

SR-IOV 支援

SR-IOV 在 vSphere Distributed Switch 上受到支援，但不支援 NSX 虛擬分散式交換器。

功能	NSX 虛擬分散式交換器	vSphere Distributed Switch
SR-IOV	否	是 (vSphere 7.0 及更新版本)

無狀態叢集主機設定檔支援

功能	NSX 虛擬分散式交換器	vSphere Distributed Switch
主機設定檔無狀態	是	是 (vSphere 7.0 及更新版本) 否 (當 VMkernel 介面卡連線至 vSphere Distributed Switch 上的 NSX-T 連接埠群組時。)

Distributed Resource Scheduler 支援

來源主機	目的地主機	DRS (已設定 NIOC)	vSphere
vSphere Distributed Switch-A	vSphere Distributed Switch-B	否	否
不透明網路 (N-VDS-A)	不透明網路 (N-VDS-B)	是	6.7
vSphere Distributed Switch	不透明網路 (N-VDS)	是	7.0
vSphere Distributed Switch-A	vSphere Distributed Switch-A	是	7.0
不透明網路 (N-VDS)	vSphere Distributed Switch	否	否

vMotion 支援

來源 vSphere Distributed Switch 和目的地 vSphere Distributed Switch 之間的 vMotion。這兩個 VDS 交換器都已啟用，以支援 NSX-T Data Center。

來源/VDS	目的地/VDS	計算 vMotion	Storage vMotion
vSphere Distributed Switch-A (vCenter Server-A)	vSphere Distributed Switch-A (vCenter Server-A)	是	是
vSphere Distributed Switch-A (vCenter Server-A)	vSphere Distributed Switch-B (vCenter Server-A)	是	是
vSphere Distributed Switch-A (vCenter Server-A)	vSphere Distributed Switch-B (vCenter Server-B)	是	是
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-A)	否	否
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-B)	否	否
Transport Zone-A	Transport Zone-B	否	否
NSX-T Data Center-A	NSX-T Data Center-B	否	否

vSphere Distributed Switch (已啟用 NSX-T Data Center) 和 NSX Virtual Distributed Switch 之間的 vMotion

來源/VDS	目的地/NSX 虛擬分散式交換器	計算 vMotion	Storage vMotion
vCenter Server-A	vCenter Server-A	是	是
vCenter Server-A	vCenter Server-B	是	是
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-A)	否	否
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-B)	否	否
Transport Zone-A	Transport Zone-B	否	否
NSX-T Data Center-A	NSX-T Data Center-B	否	否

vSphere Distributed Switch (已啟用 NSX-T Data Center) 和 vSphere 標準交換器或 vSphere Distributed Switch 之間的 vMotion

來源/VDS	目的地/NSX 虛擬分散式交換器	計算 vMotion	Storage vMotion
vCenter Server-A	vCenter Server-A	是	是
vCenter Server-A	vCenter Server-B	是	是
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-A)	否	否
Segment-A (vCenter Server-A)	Segment-B (vCenter Server-B)	否	否
Transport Zone-A	Transport Zone-B	否	否
NSX-T Data Center-A	NSX-T Data Center-B	否	否

進階網路堆疊

VDS 和 NSX 虛擬分散式交換器都支援增強型網路堆疊的所有功能。

LACP

- VDS 不支援處於作用中模式的 LACP。
- NSX Virtual Distributed Switch 在作用中模式中支援 LACP。

vSphere 7.0 中支援的規模

參數	NSX 虛擬分散式交換器
邏輯交換器	<ul style="list-style-type: none"> ■ NSX 分散式虛擬連接埠群組 (在 vCenter Server 中) 支援 10000 X N，其中，N 是 vCenter Server 中 VDS 交換器的數目。 ■ NSX-T Data Center 支援 10000 個區段。

NSX 分散式虛擬連接埠群組與主機上的 Hostd 記憶體之間的關聯性。

NSX 分散式虛擬連接埠群組	Hostd 記憶體下限	支援的虛擬機器
5000	600 MB	191
10000	1000 MB	409
15000	1500 MB	682

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，您可以設定覆蓋流量和 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-ic-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。

將主機交換器移轉到 vSphere Distributed Switch

使用 N-VDS 做為主機交換器時，NSX-T 會在 vCenter Server 中表示為不透明網路。N-VDS 在傳輸節點上擁有一或多個實體介面 (pNIC)，並從 NSX-T Data Center 執行連接埠組態。您可以將主機交換器移轉至 vSphere Distributed Switch (VDS) 7.0，以取得最佳 pNIC 使用率，並從 vCenter Server 管理 NSX-T 主機的網路。在 VDS 交換器上執行 NSX-T 時，區段會呈現為 NSX 分散式虛擬連接埠群組。在 vCenter Server 中，對 NSX-T 網路上的區段所做的任何變更都會同步。請注意，在 NSX-T Data Center 3.0 中，N-VDS 型折疊叢集環境不支援從 N-VDS 到 VDS 的移轉。此外，移轉不支援具名整併原則。

若要垂直擴充移轉，您可以透過 vSphere Update Manager 以平行方式移轉主機，或透過 API 進行手動移轉。依預設，在每個管理程式的執行緒集區大小為 22 的叢集中，每個叢集有 64 個主機可在平行模式下進行移轉。透過 vSphere Update Manager 進行移轉時，系統會針對任何正在等待可用執行緒的主機顯示「佇列中」狀態。透過 API 進行移轉時，系統會拒絕任何超過 64 個作用中主機的移轉要求。您可以透過 `PARALLEL_HOST_MIGRATION_COUNT` 欄位在內容檔案中設定執行緒計數。依預設會將其設定為 64。

備註 只會對跨 7.0.2 (X.Y.Z-U.P) 版本的 ESX 升級觸發 N-VDS 到 VDS 上 NSX-T 的移轉。對於任何「U.P」(更新修補程式) 升級，將不會觸發移轉。指定的 ESX 版本格式為 X.Y.Z-U.P，其中，

- X = 主版本
- Y = 次版本
- Z = 維護
- U = 更新
- P = 修補

必要條件

請聯絡 VMware 支援，以評估移轉到 VDS 7.0 的影響。

必須符合下列需求，才能移轉到 VDS 7.0 主機交換器：

- vCenter Server 7.0 或更新版本
- ESXi 7.0 或更新版本
- 移轉後，NSX-T 不再表示為不透明網路。您可能需要更新指令碼，以便管理 NSX-T 主機的移轉後表示。

程序

1 請使用 API 呼叫來移轉主機交換器，或執行命令以從 CLI 進行移轉。您也可以從 NSX Manager 使用者介面起始移轉。

- 進行下列 API 呼叫以執行移轉：
 - a 若要確認主機是否已準備好進行移轉，請執行下列 API 呼叫並執行預先檢查：

```
POST https://<nsx-mgr>/api/v1/nvds-urt/precheck
```

從 NSX-T 3.1.1 開始，您也可以移轉將為每個叢集產生個別 VDS 的主機交換器。在此使用案例中，您必須呼叫下列 API，而非 `POST https://<nsx-mgr>/api/v1/nvds-urt/precheck`。

```
POST https://<nsx-mgr>/api/v1/nvds-urt/precheck-by-cluster
```

兩個 API 呼叫的範例回應：

```
{ "precheck_id": "166959af-7f4b-4d49-b294-907000eef889" }
```

- b 解決任何組態不一致問題，然後再次執行預先檢查。

- c 驗證預先檢查的狀態。

```
POST https://<nsx-mgr>/api/v1/nvds-urt/status-summary/<precheck-id>
```

範例回應：

```
{
  "precheck_id": "166959af-7f4b-4d49-b294-907000eef889",
  "precheck_status": "PENDING_TOPOLOGY"
}
```

- d 對於無狀態主機，請將其中一個主機指定為來源主機，然後起始移轉。

- e 若要擷取建議的拓撲，請執行下列 API 呼叫：

```
GET https://<nsx-mgr>/api/v1/nvds-urt/topology/<precheck-id>
```

範例回應：

```
{
  "topology": [
    {
      "nvds_id": "21d4fd9b-7214-46b7-ab16-c4e7138f011f",
      "nvds_name": "nsxvswitch",
      "compute_manager_topology": [
        {
          "compute_manager_id": "fa1421d9-54a7-418e-9e18-7d0ff0d2f771",
          "dvswitch": [
            {
              "data_center_id": "datacenter-3",
              "vds_name": "VDS-nsxvswitch-datacenter-3",
              "vmknic": [
                "vmk1"
              ],
              "transport_node_id": [
                "4a6161af-7eec-4780-8faf-0e0610c33c2e",
                "5a78981a-03a6-40c0-8a77-28522bbf07a9",
                "f9c6314d-9b99-48aa-bfc8-1b3a582162bb"
              ]
            }
          ]
        }
      ]
    }
  ]
}
```

- f 進行下列 API 呼叫以使用建議的拓撲建立 VDS：

```
POST https://<nsx-mgr>/api/v1/nvds-urt/topology?action=apply
```

請注意，您只能將 N-VDS 取代為新的 VDS，而不能使用現有的 VDS。

輸入範例：

```
{
  "topology": [
    {
      "nvds_id": "c8ff4053-502a-4636-8a38-4413c2a2d52f",
      "nvds_name": "nsxvswitch",
      "compute_manager_topology": [
        {
          "compute_manager_id": "fa1421d9-54a7-418e-9e18-7d0ff0d2f771",
          "dvswitch": [
            {
              "data_center_id": "datacenter-3",
              "vds_name": "test-dvs",
              "transport_node_id": [
                "65592db5-adad-47a7-8502-1ab548c63c6d",
                "e57234ee-1d0d-425e-b6dd-7dbc5f6e6527",
                "70f55855-6f81-45a8-bd40-d8b60ae45b82"
              ]
            }
          ]
        }
      ]
    }
  ]
}
```

- g 若要追蹤移轉狀態，請執行下列 API 呼叫：

```
POST https://<nsx-mgr>/api/v1/nvds-urt/status-summary/<precheck-id>
```

當主機準備好進行移轉時，precheck_status 會從 APPLYING _TOPOLOGY 變更為 UPGRADE_READY。

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

- h 從 vCenter 將 ESXi 主機置於維護模式。
i 若要起始 N-VDS 至 VDS 的移轉，請執行下列 API 呼叫：

```
POST https://<nsx-mgr>/api/v1/transport-nodes/<tn-id>?action=migrate_to_vds
```

主機會以非同步方式進行移轉。您可以透過呼叫所需主機組的 API，平行升級多個傳輸節點。在執行移轉期間，DRS 之類的服務會繼續如預期般執行。

- j 進行下列 API 呼叫以追蹤移轉狀態：

```
POST https://<nsx-mgr>/api/v1/nvds-urt/status-summary/<precheck-id>
```

成功移轉後，host migration_state 會從 UPGRADE_IN_PROGRESS 變更為 SUCCESS。

範例回應：

```
{
  "precheck_id": "c306e279-8b75-4160-919c-6c40030fb3d0",
  "precheck_status": "READY",
  "migration_state": [
    {
      "host": "65592db5-adad-47a7-8502-1ab548c63c6d",
      "overall_state": "UPGRADE_READY"
    },
    {
      "host": "e57234ee-1d0d-425e-b6dd-7dbc5f6e6527",
      "overall_state": "UPGRADE_READY"
    },
    {
      "host": "70f55855-6f81-45a8-bd40-d8b60ae45b82",
      "overall_state": "SUCCESS"
    }
  ]
}
```

如果發生失敗，`overall_state` 會變更為 `FAILED`，指出移轉失敗的原因。執行 `migrate_to_vds` 動作以再次執行移轉工作。

k 對於無狀態主機：

- 1 從已移轉主機擷取新的主機設定檔，並將其連結至叢集。
- 2 將叢集中的剩餘主機重新開機。

■ 從 NSX Manager CLI 執行移轉。

a 若要確認主機是否已準備好進行移轉，請執行下列命令並執行預先檢查：

```
vds-migrate precheck
```

輸出範例：

```
Precheck Id: 0a26d126-7116-11e5-9d70-feff819cdc9f
```

- b 解決任何組態不一致問題，然後再次執行預先檢查。
- c 若要擷取建議的拓撲，請執行下列命令：

```
vds-migrate show-topology
```

輸出範例：

```
Precheck Id: 137d2a87-0544-4914-829d-d8b7e33b13f2
NVDS: nvds1(19cca902-9455-4316-92e2-65f4f5b4b138)
Compute Manager Topology:
[
  {
    "compute_manager_id": "fd37ed6e-0eae-4d65-b29a-d40eee1d5d47",
    "dvswitch": [
```

```

        {
            "transport_node_id": [
                "4d011ade-a010-4eea-b45a-b2569c0bb9ad"
            ],
            "data_center_id": "datacenter-3",
            "vmknic": [],
            "vds_name": "VDS-nvds1-datacenter-3"
        }
    ]
}
]

```

- d 執行下列命令以使用建議的拓撲建立 VDS：

```
vds-migrate apply-topology
```

- e 登入 vCenter Server，並確認 VDS 已建立。

- f 若要起始 N-VDS 至 VDS 的移轉，請執行下列命令：

```
vds-migrate esxi-cluster-name <cluster-name>
```

輸出範例：

```

VDS Migration Done:
  3 Transport-Nodes Migrate Successfully
  0 Transport-Nodes Migrate Failed

```

您也可以使用傳輸節點識別碼來起始移轉：

```
vds-migrate tn-list <file-path>
```

其中 <file-path> 包含傳輸節點識別碼。

輸出範例：

```

nsx-manager-1> vds-migrate tn-list /opt/tnid
VDS Migration Done:
  3 Transport-Nodes Migrate Successfully
  0 Transport-Nodes Migrate Failed

```

- 從 NSX-T Data Center 3.1.1 開始，您可以使用 NSX Manager 進行主機的移轉準備，然後在主機作業系統升級的過程中使用 vSphere Update Manager 移轉至 VDS。

若要在主機作業系統升級過程中使用 vSphere Update Manager 來移轉主機交換器，您需要 vCenter Server 7.0. U2。

備註 必須在不同 ESXi 更新版本之間升級 ESXi 主機，才能觸發此移轉。例如，

- 從 ESXi 7.0 升級到 ESXi 7.0 U2 - 可以觸發交換器移轉。
 - 從 ESXi 7.0 U2 升級到 ESXi 7.0 U2a - 無法觸發交換器移轉，因為是在相同的 ESXi 更新版本中進行升級。
-
- a 以本機 admin 使用者身分登入 NSX Manager，網址為 <https://nsx-manager-ip-address/login.jsp?local=true>。
 - b 選取**系統 > 快速入門**。
 - c 按一下**開始使用**，將主機準備好從 N-VDS 移轉至 VDS。
 - d 按一下**預先檢查**，以確認主機是否已做好移轉準備。
 - e 解決任何組態不一致問題，然後再次執行預先檢查。
 - f 檢閱建議的網路拓撲。
 - g 按一下**建立**，在 vCenter Server 中建立對應的 VDS 交換器，為選取的主機做好移轉準備。
 - h 登入 vCenter Server，並使用 vSphere Update Manager 升級您的 ESXi 主機。主機作業系統升級完成後，即會完成交換器移轉。
 - i 從 [監控] 索引標籤監控移轉進度。
- 2 將已移轉主機移出維護模式。在主機升級過程中使用 vSphere Update Manager 移轉主機交換器時，不需執行此步驟。

NSX 虛擬分散式交換器

傳輸節點的數據平面中所涉及的主要元件是 NSX 虛擬分散式交換器 (N-VDS)。在 ESXi Hypervisor 上，N-VDS 實作是從 VMware vSphere® Distributed Switch™ (VDS) 衍生而來。使用 KVM Hypervisor，N-VDS 實作會衍生自 Open vSwitch (OVS)。

NSX-T 覆疊和支援 VLAN 的網路上需要 N-VDS。

NVDS 會在這些項目之間轉送流量：

- 在傳輸節點上執行的元件 (例如，在虛擬機器之間)。
- 內部元件和實體網路。

如果將 N-VDS 用於在內部元件和實體網路之間轉送流量，則 NVDS 必須在傳輸節點上擁有一或多個實體介面 (pNIC)。與其他虛擬交換器一樣，N-VDS 無法與另一個 N-VDS 共用實體介面，在使用一組不同的 pNIC 時，它可能與另一個 N-VDS (或其他 vSwitch) 共存。雖然實現連線的 N-VDS 行為完全相同，與實作方式無關；不過，數據平面實現和強制執行功能會根據計算管理程式和相關聯的 Hypervisor 功能而有所不同。

依預設，在 ESXi 主機上設定的 N-VDS 上會啟用 IGMP 窺探 (IGMPv1/v2/v3、MLDv1/v2)。

若要變更 N-VDS 交換器上的 IGMP 窺探設定，請執行下列 CLI 命令。

```
get host-switch nvds mcast-filter
```

```
set host-switch nvds mcast-filter
  legacy mcast filter mode: {legacy|snooping}
  snooping mcast filter mode: {legacy|snooping}
```

若要在每個連接埠層級變更設定，請執行下列 CLI 命令。

```
get host-switch <host-switch-name> dvport <dvport-id> mcast-filter
```

```
get host-switch <host-switch-name> dvport <dvport-id> mcast-filter <entry-
mode> <entry-group>
```

如需更多詳細資料，請參閱《NSX-T Data Center Command-Line 介面參考》。

虛擬私人網路 (VPN)

6

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。

裸機伺服器上的 Intel QuickAssist 技術 (QAT) 功能支援 IPsec VPN 大量密碼編譯。此功能的支援從 NSX-T Data Center 3.0 開始。如需在裸機伺服器上支援 QAT 功能的詳細資訊，請參閱《NSX-T Data Center 安裝指南》。

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。

從 NSX-T Data Center 2.5 開始，第 0 層和第 1 層閘道皆支援 IPsec VPN 服務。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。第 0 層或第 1 層閘道在用於 IPsec VPN 服務時，必須處於 `Active-standby` 高可用性模式。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，以在 VPN 服務層級支援高可用性服務。通道是在容錯移轉時重新建立的，並且會同步 VPN 組態資料。在 NSX-T Data Center 3.0 版本之前，重新建立通道時，IPsec VPN 狀態不會同步。從 NSX-T Data Center 3.0 版本開始，IPsec VPN 狀態會在目前作用中的 NSX Edge 節點失敗時同步至待命 NSX Edge 節點，且原始待命 NSX Edge 節點會成為新的作用中 NSX Edge 節點，而不需重新交涉通道。原則型和路由型 IPsec VPN 服務皆支援此功能。

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。

IPSec VPN 可在內部部署網路與您雲端軟體定義的資料中心 (SDDC) 中的網路之間提供安全通道。對於原則型 IPSec VPN，必須在這兩個端點上以對稱方式設定在工作階段中提供的本機和對等網路。例如，如果雲端 SDDC 將本機網路設定為 **x**、**y**、**z** 子網路，並將對等網路設定為 **a**，則內部部署 VPN 組態必須以 **a** 作為本機網路，並以 **x**、**y**、**z** 作為對等網路。即使 **a** 設定為任何 (0.0.0.0/0)，仍是如此。例如，如果雲端 SDDC 原則型 VPN 工作階段將本機網路設定為 10.1.1.0/24，並將對等網路設定為 0.0.0.0/0，則在內部部署 VPN 端點上，VPN 組態必須以 0.0.0.0/0 作為本機網路，並以 10.1.1.0/24 作為對等網路。如果設定錯誤，則 IPSec VPN 通道交涉可能會失敗。

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 6-1. 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 層閘道的 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

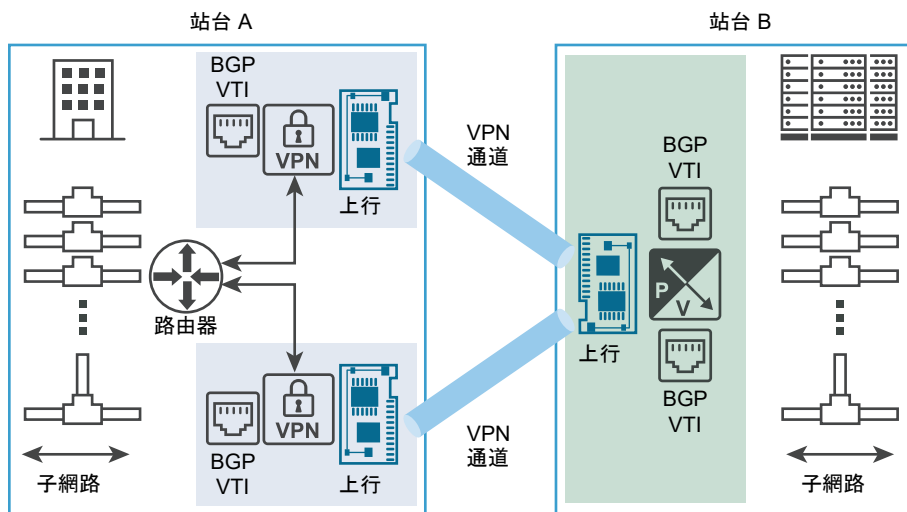
您可以使用在第 0 層閘道上設定的路由型 IPsec VPN 工作階段，來設定 VPN 通道備援。透過通道備援，可在兩個站台之間設定多個通道，其中一個通道會用作主要通道，並在主要通道變得無法使用時容錯移轉至其他通道。此功能在站台有多個連線選項時最有用，例如使用不同的 ISP 來連結備援。

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 閘道，並且 NSX-T Data Center 管理站台 B 中的 Edge 閘道虛擬應用裝置。

圖 6-1. 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，這表示在不同的網站之間移動虛擬機器時，這些虛擬機器會保持在相同的子網路中。虛擬機器的 IP 位址在移動時不會變更。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。

第 0 層和第 1 層閘道皆支援 L2 VPN 服務。第 0 層或第 1 層閘道皆僅能設定一個 L2 VPN 服務 (用戶端或伺服器)。

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。

VLAN 型 和 VNI 型的區段可透過使用在 NSX-T Data Center 環境中受管理之 NSX Edge 節點上的 L2 VPN 服務來延伸。您可以將 L2 網路從 VLAN 延伸至 VNI、將 VLAN 延伸至 VLAN，以及將 VNI 延伸至 VNI。

區段可連線至第 0 層或第 1 層閘道，並使用 L2 VPN 服務。

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。如果有足夠的計算和 I/O 資源，NSX Edge 叢集可以使用 VLAN 主幹透過單一介面延伸多個 VLAN 網路。

從 NSX-T Data Center 3.0 開始，依預設會啟用 L2 VPN 路徑 MTU 探索 (PMTUD) 功能。啟用 PMTUD 之後，來源主機透過 L2 VPN 通道學習目的地主機的路徑 MTU 值，並將傳出 IP 封包的長度限制為學習到的值。此功能可協助避免通道內的 IP 分段和重組，因此改善了 L2 VPN 的效能。

L2 VPN PMTUD 功能不適用於非 IP、非單點傳播以及已清除 DF (不分段) 旗標的單點傳播封包。全域 PMTU 快取計時器每 10 分鐘便會到期。若要停用或啟用 L2 VPN PMTUD 功能，請參閱[啟用和停用 L2 VPN 路徑 MTU 探索](#)。

在下列部署情況中提供 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 伺服器和 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 伺服器和 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 伺服器和 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 伺服器和 NSX-T Data Center L2 VPN 用戶端之間。在此案例中，您可以在兩個內部部署軟體定義資料中心 (SDDC) 之間延伸邏輯 L2 區段。

啟用和停用 L2 VPN 路徑 MTU 探索

您可以使用 CLI 命令來啟用或停用 L2 VPN 路徑 MTU (PMTU) 探索功能。依預設會啟用 L2 VPN PMTU 探索。

必要條件

您必須擁有 admin 帳戶的使用者名稱和密碼才能登入 NSX Edge 節點。

程序

- 1 使用 admin 權限登入 NSX Edge 節點的 CLI。
- 2 若要檢查 L2 VPN PMTU 探索功能的狀態，請使用下列命令。

```
Nsxedg> get dataplane l2vpn-pmtu config
```

如果已啟用此功能，您會看到下列輸出：l2vpn_pmtu_enabled : True。

如果停用此功能，您會看到下列輸出：l2vpn_pmtu_enabled : False。

- 3 若要停用 L2 VPN PMTU 探索功能，請使用下列命令。

```
nsxedg> set dataplane l2vpn-pmtu disabled
```

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 層或第 1 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 層或第 1 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 層或第 1 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**第 0 層/第 1 層閘道**下拉式功能表中，選取要與此 IPSec VPN 服務建立關聯的第 0 層或第 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 若要啟用或停用可設定狀態的 VPN 工作階段同步化，請切換**工作階段同步**。
依預設，此值設為 `Enabled`。
- 10 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，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。
如果啟用這些規則，即使已在 IPSec 工作階段規則中指定了 IP 位址，系統仍會在指定的本機和遠端 IP 網站之間交換資料封包。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。
- 11 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 層或第 1 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 層或第 1 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](#)。

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 層或第 1 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/第 1 層閘道** 下拉式功能表中，選取要與 L2 VPN 伺服器搭配使用的閘道。
 - 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/第 1 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 層或第 1 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 IPsec VPN 服務尚不存在於您想要設定為 L2 VPN 用戶端的第 0 層或第 1 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/第 1 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 層或第 1 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/第 1 層閘道**下拉式功能表中，選取您與不久前所建立的路由型 IPsec 通道搭配使用的同一個第 0 層或第 1 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**第 19 章憑證**。
- 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。

- a 如果已啟用 IKE 設定檔下拉式功能表，請選取 IKE 設定檔。
- b 如果未停用 IPsec 設定檔下拉式功能表，請選取 IPsec 通道設定檔。
- c 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。
- d 從連線初始模式下拉式功能表中，選取慣用模式。

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

表 6-2. 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。

- e 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。

- f 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[第 19 章憑證](#)。
- 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](#)。

- a 如果已啟用 **IKE 設定檔** 下拉式功能表，請選取 IKE 設定檔。
- b 如果未停用 **IPsec 設定檔** 下拉式功能表，請選取 IPsec 通道設定檔。
- c 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。
- d 從**連線初始模式** 下拉式功能表中，選取慣用模式。

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

表 6-3. 連線初始模式

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

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

備註 AES 128 和 AES 256 演算法使用 CBC 作業模式。

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

備註 AES 128 和 AES 256 演算法使用 CBC 作業模式。

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 在 **本機出口閘道 IP** 文字方塊中，輸入區段上您的工作負載虛擬機器用作其預設閘道的本機閘道的 IP 位址。可在延伸區段的遠端站台中設定相同的 IP 位址。
- f 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":
    "MCw3ZjBjYzdjLHsic2l0ZU5hbWUOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
BJcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXlyIiwic2l0ZU5hbWUOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
VzdCI6ImFlcy1nY20vc2hhLTI1NiIsInBzayI
6l1ZN2FyZTEyMyIsInR1bm5lbHMlOlt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVLcklkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnRpsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX"
  }
]
```

- 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。

```
MCw3ZjBjYzdjLHsic2l0ZU5hbWUOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
BJcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1
vbiI6ImlrZXlyIiwic2l0ZU5hbWUOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
VzdCI6ImFlcy1nY20vc2hhLTI1NiIsInBzayI
6l1ZN2FyZTEyMyIsInR1bm5lbHMlOlt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVLcklkIjoINTAuNTAuNTAuMS
IsImxvY2FsVnRpsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYX
```

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。
- 確保您已設定要與此本機端點建立關聯的 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。對於使用憑證式驗證並與本機端點相關聯的 IPsec VPN 工作階段，**本機識別碼**衍生自與本機端點相關聯的驗證。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。

例如，如果憑證不包含任何主體別名 (SAN) 欄位，且其 DN 字串為：

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123
```

則會以 DN 字串作為本機識別碼。此本機識別碼是遠端站台上的對等識別碼。

- 如果在憑證中找到 X509v3 延伸 x509v3 Subject Alternative Name，則會使用其中一個 SAN 欄位作為本機識別碼值。

如果憑證有多個 SAN 欄位，會依以下順序選取本機識別碼。

順序	SAN 欄位
1	IP 位址
2	DNS
3	電子郵件地址

例如，如果所設定的站台憑證有以下 SAN 欄位：

```
x509v3 Subject Alternative Name:
DNS:Site123.vmware.com, email:user@company.com, IP Address:1.1.1.1
```

則會以 IP 位址 1.1.1.1 作為本機識別碼。如果 IP 位址無法使用，則會使用 DNS 字串。如果 IP 位址和 DNS 無法使用，則會使用電子郵件地址。

若要查看用於 IPsec VPN 工作階段的本機識別碼，請執行下列操作：

- a 導覽至網路 > VPN，然後按一下 IPsec 工作階段索引標籤。
- b 展開 IPsec VPN 工作階段。
- c 按一下下載組態以下載包含本機識別碼的組態檔。

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 (選擇性) 指定標籤。

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 設定檔提供多次探查之間等待秒數的相關資訊，以偵測 IPsec 對等站台是否處於運作中狀態。

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設定您自己的設定檔。

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 6-4. 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 CBC 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 CBC 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 選取 **網路 > VPN**，然後按一下 **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 6-5. 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 6-6. 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>在國際網路金鑰交換 (IKE) 交涉期間使用的加密演算法。</p> <p>AES 128 和 AES 256 演算法使用 CBC 作業模式。</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了 SHA1，則在 IKE SA 交涉期間會使用 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 (使用 CBC 模式) 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，請按一下三個點功能表 (⋮)，然後從可用動作清單中進行選取。

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 6-7. 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 選取 **網路 > VPN**，然後按一下 **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 6-8. 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 	<p>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。</p> <p>AES 128 和 AES 256 演算法使用 CBC 作業模式。</p>
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 6-9. 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，請按一下三個點功能表 (⋮)，然後從可用動作清單中進行選取。

新增 DPD 設定檔

DPD (無作用對等偵測) 設定檔提供偵測 IPSec 對等站台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，這是您在設定 IPSec VPN 服務時由系統預設指派的 DPD 設定檔。此預設 DPD 設定檔為定期 DPD 探查模式。

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 從**選取設定檔類型**下拉式功能表中選取 **DPD 設定檔**，然後按一下**新增 DPD 設定檔**。
- 4 輸入 DPD 設定檔的名稱。
- 5 從 **DPD 探查模式**下拉式功能表中，選取**定期**或**隨選**模式。

對於定期 DPD 探查模式，每次達到指定的 DPD 探查間隔時間時，就會傳送 DPD 探查。

對於隨選 DPD 探查模式，如果在閒置一段時間後沒有從對等站台接收到 IPSec 封包，就會傳送 DPD 探查。DPD 探查時間間隔中的值會決定所使用的閒置期間。

- 6 在 **DPD 探查時間間隔**文字方塊中，輸入您想要 NSX Edge 節點等候的秒數，在此段時間過後才傳送下一個 DPD 探查。

對於定期 DPD 探查模式，有效值介於 3 到 360 秒之間。預設值為 60 秒。

對於隨選探查模式，有效值介於 1 到 10 秒之間。預設值為 3 秒。

設定定期 DPD 探查模式時，NSX Edge 上執行的 IKE 精靈會定期傳送 DPD 探查。如果對等站台在半秒內回應，則會在達到所設定的 DPD 探查間隔時間後傳送下一個 DPD 探查。如果對等站台沒有回應，則在等待半秒後再次傳送 DPD 探查。如果遠端對等站台持續無回應，則 IKE 精靈會再次重新傳送 DPD 探查，直到收到回應或達到重試計數為止。IKE 精靈會重新傳送 DPD 探查直到**重試計數**內容中指定的次數上限，之後會將對等站台宣告為無作用。對等站台被宣告為無作用後，NSX Edge 節點隨後會將無作用對等連結上的安全性關聯 (SA) 移除。

設定隨選 DPD 模式時，僅在達到所設定的 DPD 探查間隔時間後仍未從對等站台接收到 IPSec 流量時，系統才會傳送 DPD 探查。

- 7 在 **重試計數**文字方塊中，輸入允許的重試次數。
有效值介於 1 到 100 之間。預設重試計數為 5。
- 8 視需要提供說明並新增標籤。

- 若要啟用或停用 DPD 設定檔，請按一下**管理狀態**切換按鈕。

依預設，此值設為**已啟用**。啟用 DPD 設定檔時，DPD 設定檔會用於使用 DPD 設定檔之 IPsec VPN 服務中的所有 IPsec 工作階段。

- 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。您也可以透過部署主要和次要自發 Edge L2 VPN 用戶端，為 VPN 備援啟用高可用性 (HA)。

必要條件

- 建立連接埠群組，並將其繫結至主機上的 vSwitch。確保此連接埠群組接受混合模式和來自連接埠群組安全設定的偽造傳輸。
- 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 admin 密碼。
- b 輸入兩次 CLI 啟用密碼。
- c 輸入兩次 CLI root 密碼。
- d 輸入管理網路的 IPv4 位址。
- e 啟用部署自發 Edge 的選項。
- f 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。

- g (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。
- h (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)

7

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。

除了 NAT64 之外，還支援下列類型的 NAT：

- 來源 NAT (SNAT) - 轉譯輸出封包的來源 IP 位址，讓封包顯示為源自不同的網路。支援在作用中/待命模式中執行的第 0 層/第 1 層閘道。對於一對一 SNAT，SNAT 轉譯的 IP 位址不會設定在回送連接埠上，且不會有轉送項目具有與首碼相同的 SNAT 轉譯 IP。對於多對一 SNAT，SNAT 轉譯的 IP 位址會設定在回送連接埠上，且使用者會看到具有 SNAT 轉譯 IP 位址首碼的轉送項目。
- 目的地 NAT (DNAT - 轉譯輸入封包的目的地 IP 位址，讓封包傳遞至目標位址以進入另一個網路。支援在作用中/待命模式中執行的第 0 層/第 1 層閘道。
- 自反 NAT - (有時稱為無狀態 NAT) 會轉譯通過路由裝置的位址。輸入封包會經過目的地位址重新寫入，而輸出封包會經過來源位址重新寫入。不會保留工作階段，因為它為無狀態。支援在作用中/作用中式模式中執行的第 0 層閘道。在作用中/作用中式模式中不支援可設定狀態的 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。

備註 NAT 會在第 0 層/第 1 層閘道的上行中設定，並處理通過此介面的流量。這隱含表示第 0 層閘道 NAT 規則將不會在連線至第 0 層的兩個第 1 層閘道之間套用。

NAT64 是一種將 IPv6 封包轉譯為 IPv4 封包 (反之亦然) 的機制。NAT 64 允許僅 IPv6 用戶端使用單點傳播 UDP 或 TCP 來聯繫 IPv4 伺服器。NAT64 只允許僅 IPv6 用戶端啟動與僅 IPv4 伺服器的通訊。為了執行 IPv6-IPv4 轉譯，系統需要儲存繫結和工作階段資訊。NAT64 為可設定狀態。

- NAT64 僅支援透過 NSX-T Edge 上行傳入至覆蓋中 IPv4 伺服器的外部 IPv6 流量。
- NAT64 支援 TCP 和 UDP，將捨棄所有其他通訊協定類型的封包。NAT64 不支援：具有延伸標頭的 ICMP、片段和 IPV6 封包。

備註 在相同 Edge 節點上設定 NAT64 規則和內嵌負載平衡器時，不支援使用 NAT64 規則將 IPv6 封包導向 IPv4 內嵌負載平衡器。

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 NAT 和 NAT 64 規則。

備註 如果在此 NAT 規則中設定了服務，則 translated_port 將在 NSX Manager 上實現為 destination_port。這表示服務將會是轉譯的連接埠，而轉譯的連接埠會用來將流量比對為目的地連接埠。如果未設定任何服務，則將忽略該連接埠

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 **網路 > NAT**。
- 3 選取閘道。
- 4 在視圖旁邊，選取 **NAT** 或 **NAT64**。
- 5 按一下 **新增 NAT 規則** 或 **新增 NAT 64 規則**。
- 6 輸入名稱。
- 7 如果您正在設定 NAT，請選取動作。針對 **NAT 64**，動作為 NAT64。

NAT 選項	說明
第 1 層閘道	可用動作包括 SNAT、DNAT、自反、無 SNAT 以及無 DNAT。
作用中/待命模式中的第 0 層閘道	可用動作包括 SNAT、DNAT、無 SNAT 以及無 DNAT。
作用中/作用中式模式中的第 0 層閘道	可用動作為自反。

- 8 輸入來源。如果將此文字方塊保留空白，則 NAT 規則會套用至本機子網路外部的所有來源。

選項	說明
NAT	以 CIDR 格式指定 IP 位址或 IP 位址範圍。對於 SNAT、NO_SNAT 和 REFLEXIVE 規則，這是必要文字方塊，代表離開網路之封包的來源網路。
NAT64	輸入 IPv6 位址或 IPv6 CIDR。

- 9 (必要) 輸入目的地。

選項	說明
NAT	以 CIDR 格式指定 IP 位址或 IP 位址範圍。
NAT64	以 CIDR 格式加上首碼 /96 輸入 IPv6 位址或 IPv6 位址範圍。支援首碼 /96，因為目的地 IPv4 IP 內嵌於 IPv6 位址中的最後 4 個位元組

10 輸入轉譯的 IP 的值。

選項	說明
NAT	以 CIDR 格式指定 IPv4 位址或 IP 位址範圍。
NAT64	指定 IPv4 位址、以逗點分隔的 IPv4 位址清單，或 IPv4 位址範圍。不支援 IPV4 CIDR。

11 切換**啟用**以啟用規則。

12 在**服務**資料行中，按一下**設定**以選取服務。如需詳細資訊，請參閱[新增服務](#)。對於 NAT 64，選取預先定義的服務，或使用 TCP 或 UDP 建立使用者定義的服務，其中來源/目的地連接埠為**任何**或特定連接埠。

13 對於**套用至**，按一下**設定**並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**。

備註 如果您使用 NSX 聯盟 並從 全域管理程式 應用裝置建立 NAT 規則，則可以為 NAT 選取網站特定的 IP 位址。您可以將 NAT 規則套用至下列任一位置範圍：

- 如果您想要使用將 NAT 規則套用至所有位置的預設選項，請勿按一下**設定**。
- 按一下**設定**。在**套用至**對話方塊中，選取要將規則套用至其實體的位置，然後選取將 **NAT 規則套用至所有實體**。
- 按一下**設定**。在**套用至**對話方塊中，選取位置，然後從**類別**下拉式功能表中選取**介面**。您可以選取要套用 NAT 規則的特定介面。

如需更多詳細資料，請參閱 [聯盟中支援的功能和組態](#)。

14 輸入轉譯的**連接埠**的值。

15 選取防火牆設定。

選項	說明
NAT	可用設定包括： <ul style="list-style-type: none"> ■ 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。 <ul style="list-style-type: none"> ■ 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。 <ul style="list-style-type: none"> ■ 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。
NAT64	可用設定為 略過 - 封包會略過防火牆規則。

16 (選擇性) 切換記錄按鈕以啟用記錄。

17 指定優先順序值。

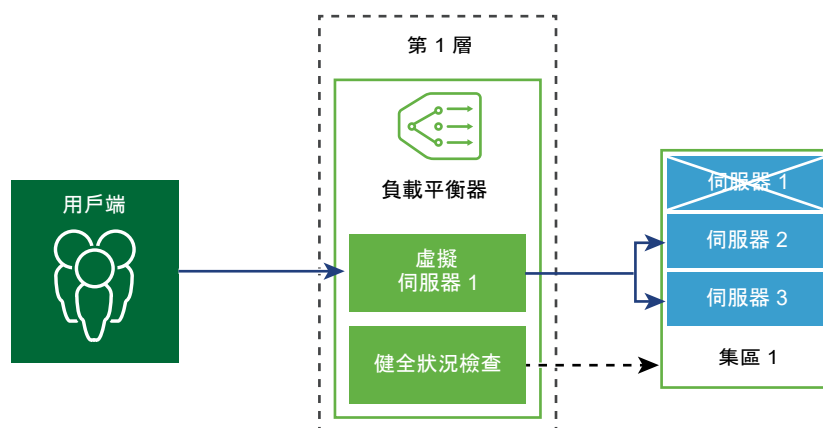
較低的值表示較高的優先順序。預設值為 0。

18 按一下**儲存**。

負載平衡

8

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：

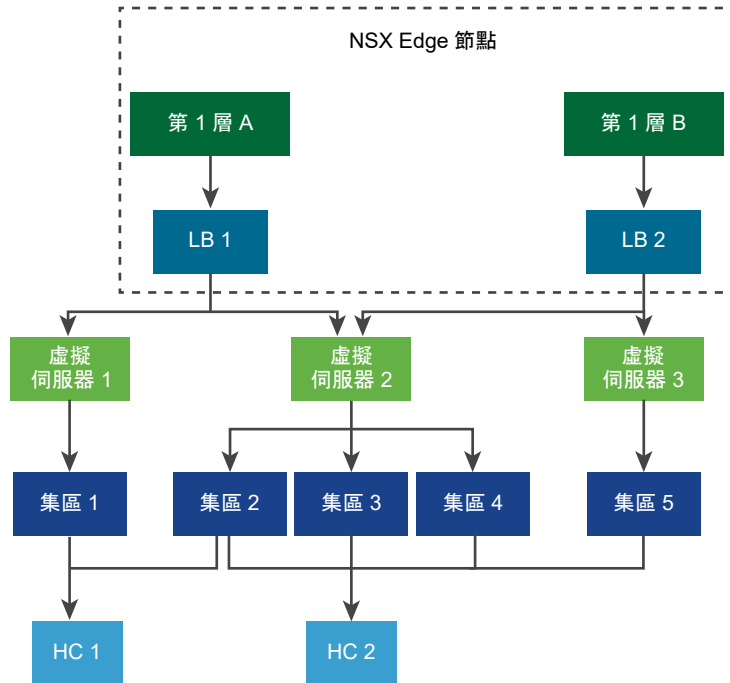
- [主要負載平衡器概念](#)
- [設定負載平衡器元件](#)
- [針對伺服器集區和虛擬伺服器建立的群組](#)

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、中、大或超大)。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，因此必須處於作用中/待命模式。閘道會在 NSX Edge 節點上執行。NSX Edge 節點的機器尺寸 (裸機、小、中、大或超大) 會決定 NSX Edge 節點可支援的負載平衡器數目。請注意，在管理程式模式中，您會建立邏輯路由器，它具有與閘道類似的功能。請參閱第 1 章 [NSX Manager](#)。

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。如果您使用原則模式來設定負載平衡，請執行下列命令：

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

如果您使用管理程式模式來設定負載平衡，請執行下列命令：

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

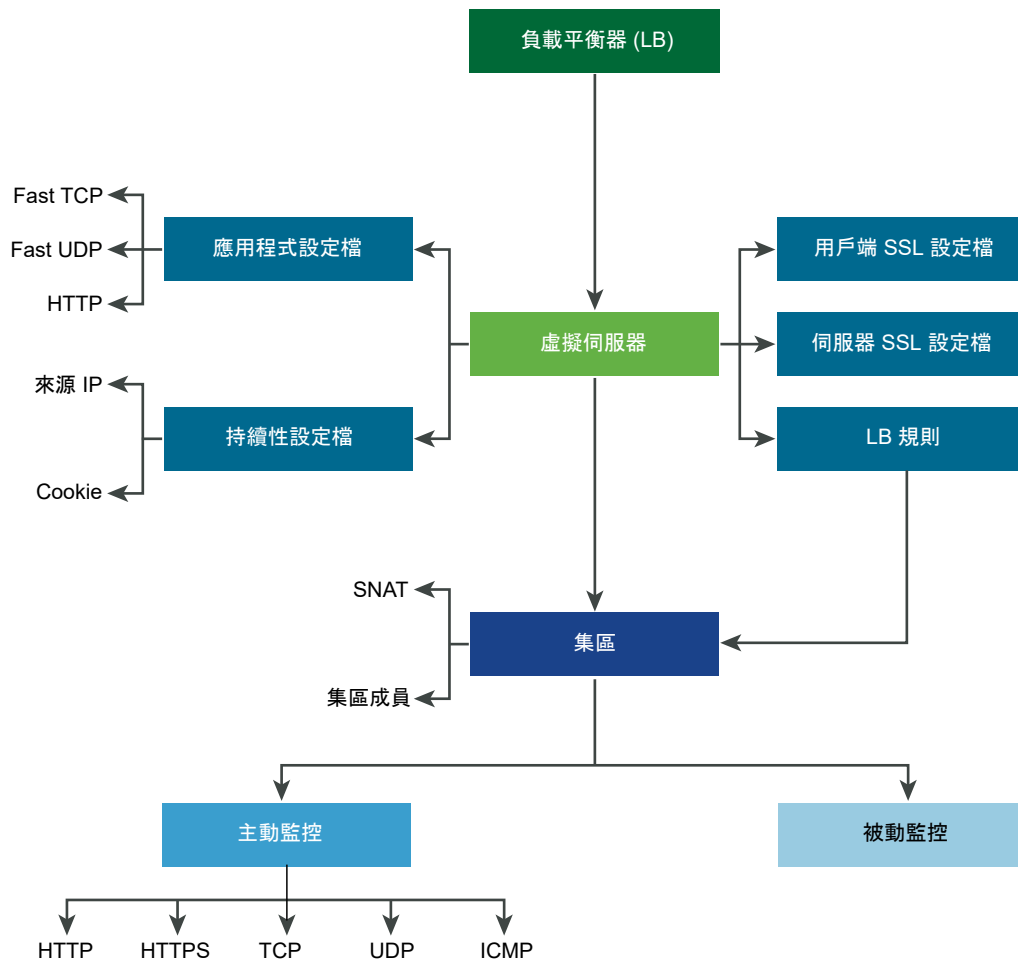
使用量資訊包括節點上設定的負載平衡器物件 (例如負載平衡器服務、虛擬伺服器、伺服器集區，以及集區成員) 的數目。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。

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 - 主動監視器 (包括 HTTP、HTTPS、TCP、UDP 和 ICMP) 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。

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

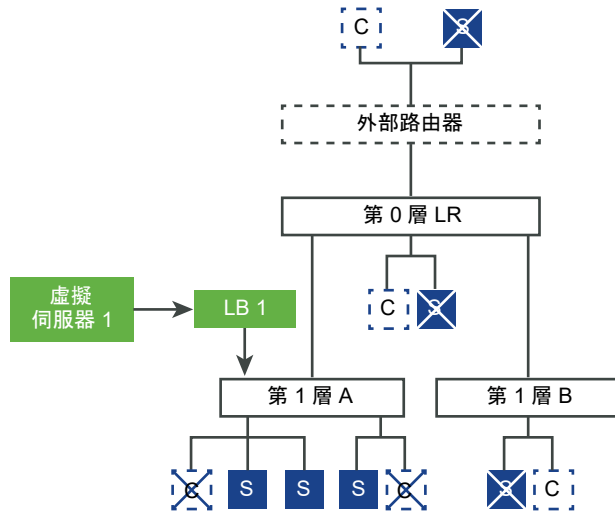


負載平衡器拓撲

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

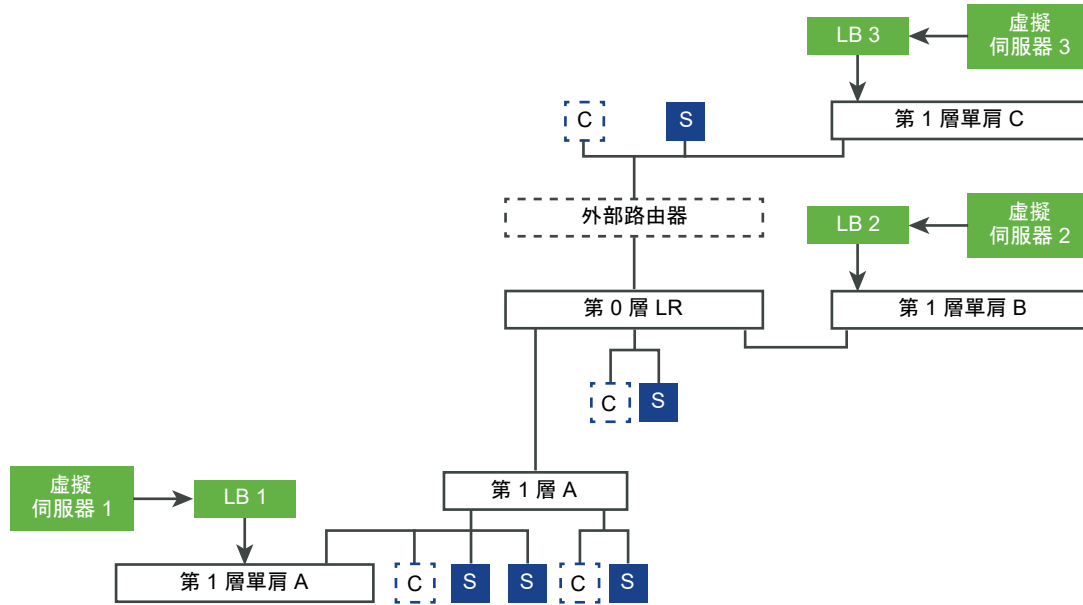
在內嵌模式下，負載平衡器位於用戶端與伺服器之間的流量路徑中。如果不想在負載平衡器上有 SNAT，用戶端和伺服器不應連線到相同第 1 層邏輯路由器上的覆蓋區段。如果用戶端和伺服器連線至相同第 1 層邏輯路由器上的覆蓋區段，則需要 SNAT。



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。



特殊使用案例 如果未使用覆疊且所有內容均為 VLAN，仍必須在裝載第 1 層單臂負載平衡器的 Edge 節點上設定覆疊。這是因為 Edge 節點必須至少有一個通道端點已開啟，才能在 Edge 節點之間實現高可用性。通道開啟後，它們將同意哪個 Edge 節點將執行每個第 0 層和第 1 層閘道的作用中或待命角色。

第 1 層服務鏈結

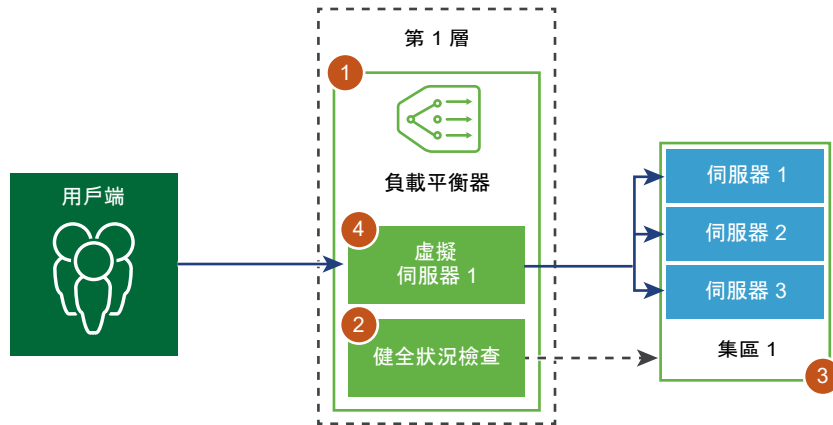
如果第 1 層閘道或邏輯路由器主控不同的服務 (例如 NAT、防火牆和負載平衡器)，則會依下列順序套用服務：

- 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。

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。

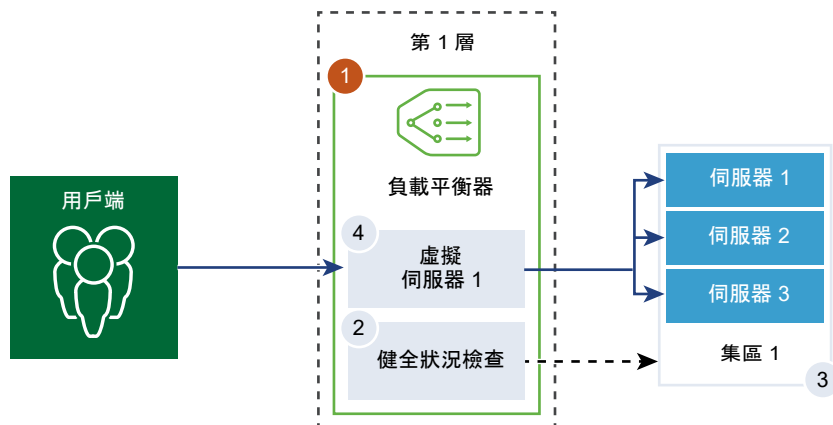


新增負載平衡器

負載平衡器將會建立並連結至第 1 層閘道。

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 根據您的虛擬伺服器和集區成員以及可用資源的需求，選取負載平衡器大小。
- 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。

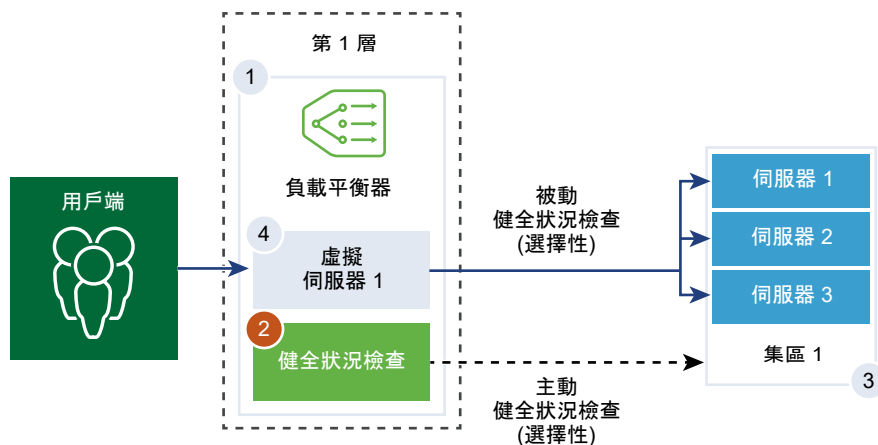
新增主動監視器

主動健全狀況監控可用來測試伺服器是否可用。主動健全狀況監控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為使用多台主動健全狀況監控。



程序

1 從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控值。

選項	說明
名稱與說明	輸入主動健全狀況監控的名稱和說明。
監控連接埠	設定監控連接埠的值。
監控時間間隔	設定監控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	設定在將集區成員監控視為失敗之前，負載平衡器等待其回應的時間。
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	設定在將集區成員狀態從「關閉」變更為「啟動」之前，需達到的連續成功監控次數。
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，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 若要設定 HTTP 要求，請按一下**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。 在要求 URL 中不允許 ASCII 控制字元 (退格鍵、垂直 Tab 鍵、水平 Tab 鍵、換行字元等)、不安全的字元 (例如 space、\、<、>、{、}) 以及 ASCII 字元集以外的任何字元，且都應進行編碼。例如，以加號 (+) 或 %20 取代空格。
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 要求標頭	按一下 新增 ，然後輸入 HTTP 要求標頭名稱和相對應的值。
HTTP 要求本文	輸入要求本文。 適用於 POST 和 PUT 方法。

選項	說明
HTTP 回應代碼	輸入監控預期與 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 按一下**儲存**。
- 9 從下拉式清單中選取 **HTTPS 通訊協定**。
- 10 完成步驟 5。
- 11 按一下**設定**。
- 12 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控的名稱和說明。
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。 在要求 URL 中不允許 ASCII 控制字元 (退格鍵、垂直 Tab 鍵、水平 Tab 鍵、換行字元等)、不安全的字元 (例如 space、\、<、>、{、}) 以及 ASCII 字元集以外的任何字元，且都應進行編碼。例如，以加號 (+) 或 %20 取代空格。
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 要求標頭	按一下 新增 ，然後輸入 HTTP 要求標頭名稱和相對應的值。
HTTP 要求本文	輸入要求本文。 適用於 POST 和 PUT 方法。
HTTP 回應代碼	輸入監控預期與 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。

選項	說明
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。

13 選取 ICMP 通訊協定。

14 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)。

15 選取 TCP 通訊協定。

16 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。

17 選取 UDP 通訊協定。

18 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

將主動健全狀況監控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控。

程序

- 1 從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控的名稱和說明。
- 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控值。

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

將被動健全狀況監控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。

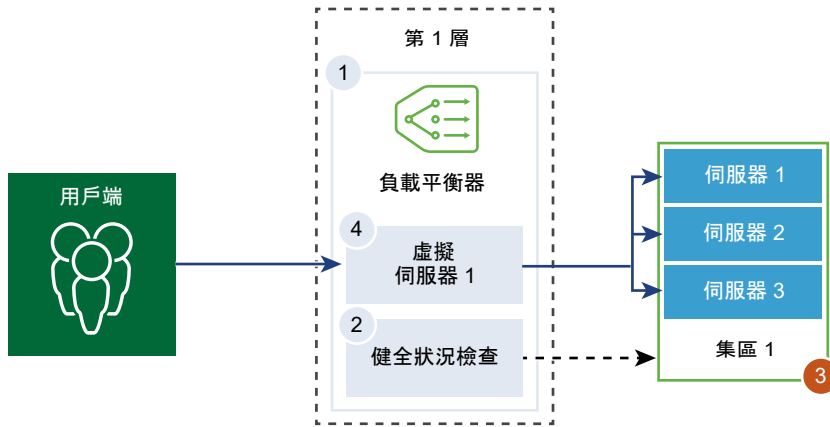
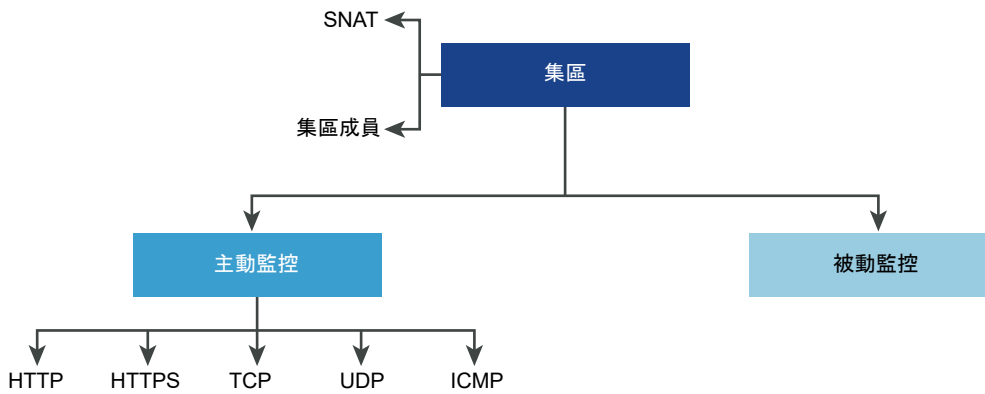


圖 8-1. 伺服器集區參數組態



必要條件

- 如果您使用動態集區成員，則必須設定 NSGroup。請參閱在管理程式模式中建立 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)。
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 按一下 **選取成員**, 然後選擇伺服器集區成員。

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、IPv4 或 IPv6 位址和連接埠。IP 位址可以是 IPv4 或 IPv6。不支援混合定址。請注意, 集區成員的 IP 版本必須符合 VIP IP 版本。例如, VIP-IPv4 與 Pool-IPv4, 以及 IPv6 與 Pool-IPv6。</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 位址與 MAC 位址新增為群組成員, 以及新增 Active Directory 群組。IP 位址可以是 IPv4 或 IPv6。不支援混合定址。身分識別成員會與計算成員相交, 以定義群組的成員資格。從下拉式功能表中選取標籤。</p> <p>您可以選擇性地定義最大群組 IP 位址清單。</p>

- 6 按一下**設定監視器**，然後為伺服器選取一或多個作用中健全狀況檢查監視器。按一下**套用**。

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。每個伺服器集區可設定一個以上的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	<p>停用 SNAT 轉譯模式。</p>
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 IPv4 或 IPv6 位址範圍，例如，1.1.1.1-1.1.1.10。IP 位址可以是 IPv4 或 IPv6。不支援混合定址。</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 按一下**其他內容**，然後切換按鈕以啟用 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 設定每個伺服器保持運作的 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 從下拉式功能表中選取標籤。

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。

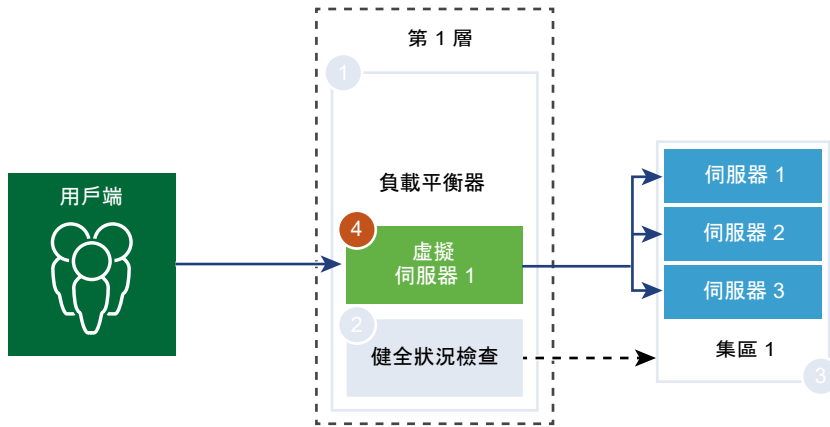
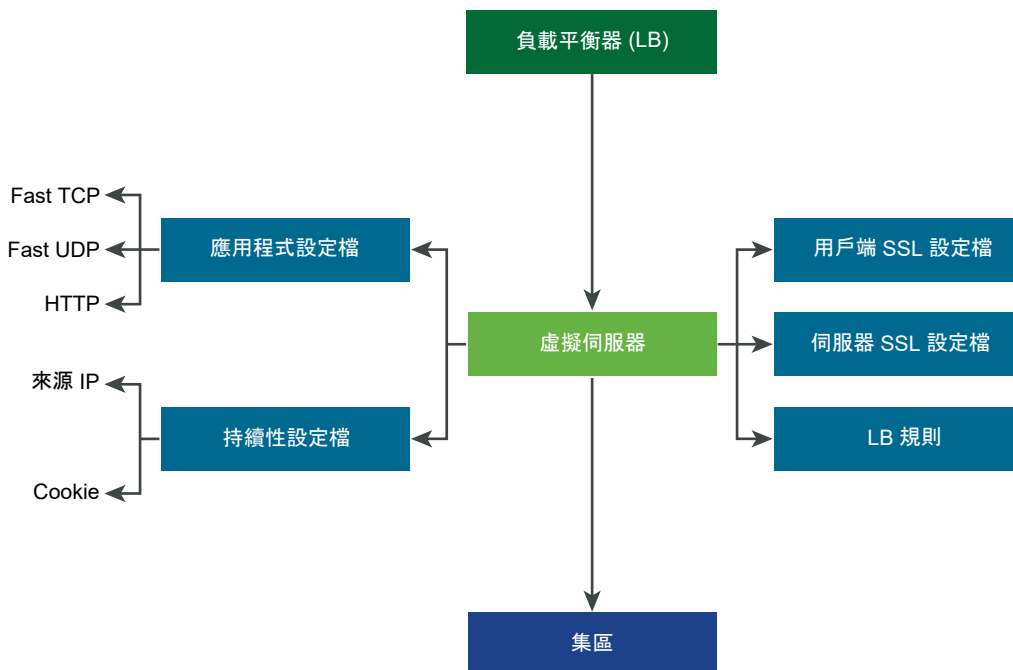


圖 8-2. 虛擬伺服器元件



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 8-3. 第 4 層 TCP 和 UDP 應用程式設定檔

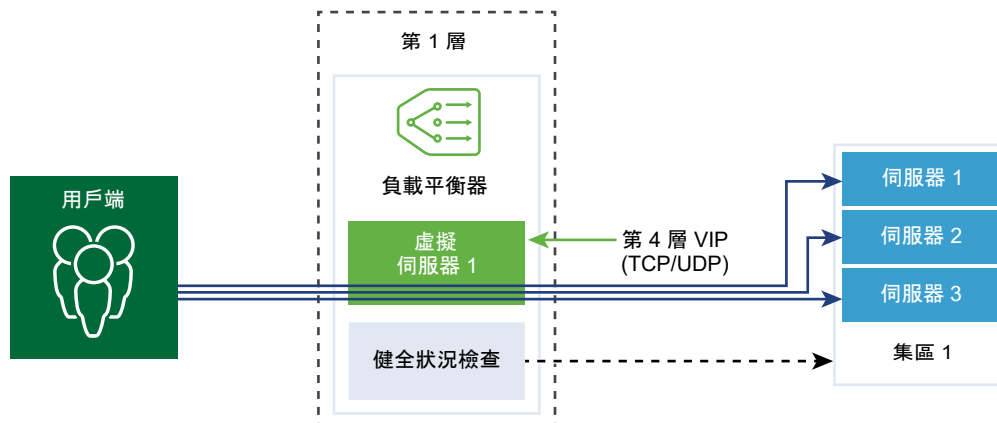
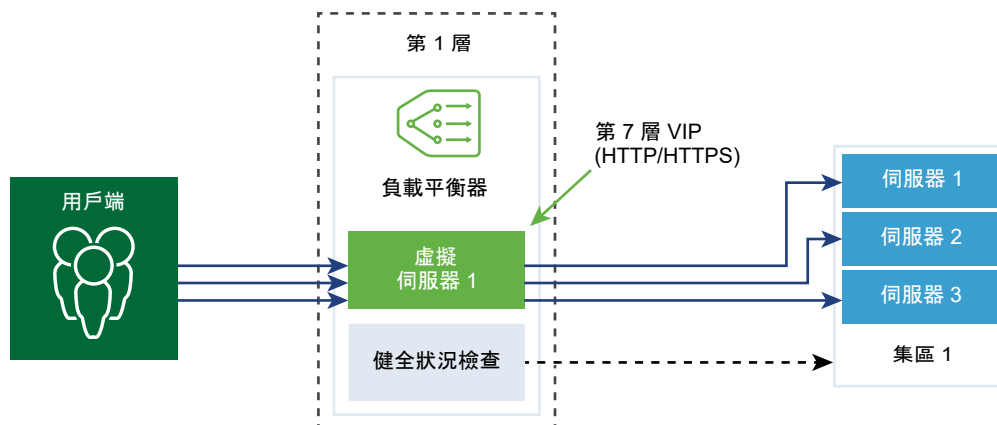


圖 8-4. 第 7 層 HTTPS 應用程式設定檔



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)。
回應標頭大小	指定用來儲存 HTTP 回應標頭的最大緩衝區大小 (以位元組為單位)。預設值為 4096，上限為 65536。
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。

選項	說明
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。
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

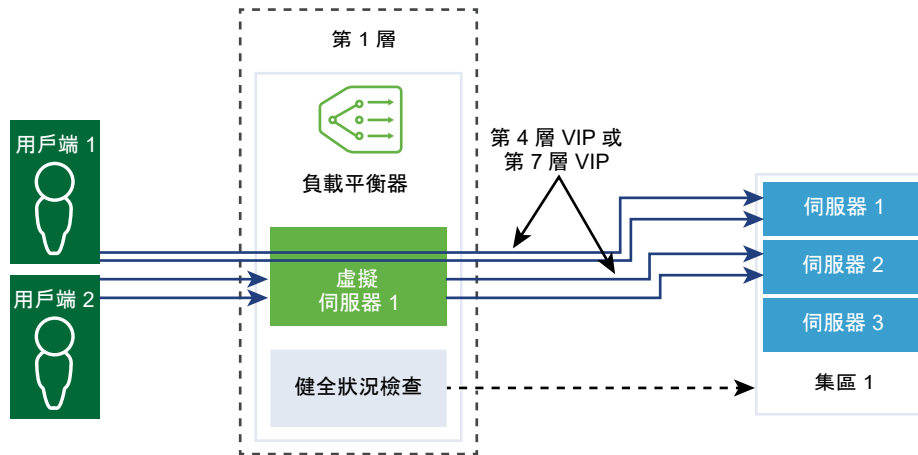
若要確保可設定狀態的應用程式的穩定性，負載平衡器會實作將所有相關連線導向至相同伺服器的持續性。支援不同類型的持續性以因應不同類型的應用程式需求。

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。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 8-5. SSL 卸載

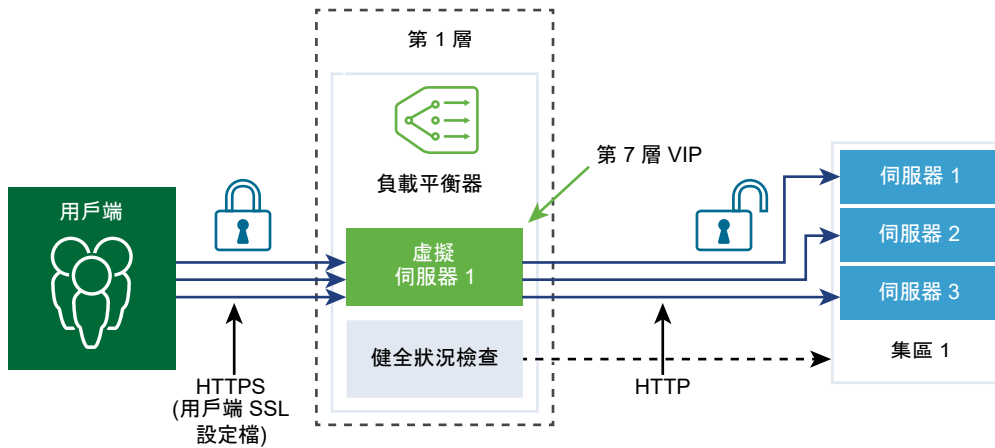
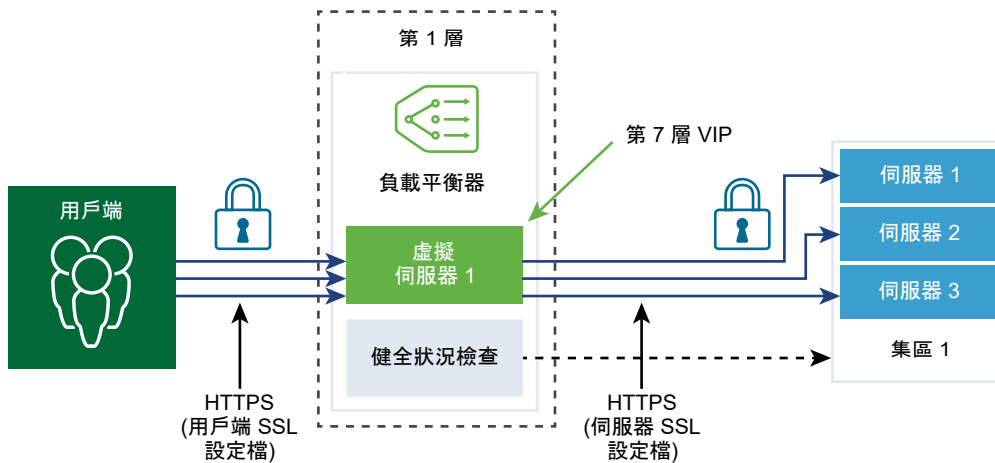


圖 8-6. 端對端 SSL



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** 或 **L4 UDP** 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。

L4 TCP 選項	L4 TCP 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。支援 IPv4 和 IPv6 位址。請注意，集區成員的 IP 版本必須符合 VIP IP 版本。例如，VIP-IPv4 與 Pool-IPv4，以及 IPv6 與 Pool-IPv6。
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。 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。
存取清單控制項	啟用存取清單控制項 (ACL) 時，會使用 ACL 陳述式比較流經負載平衡器的所有流量，進而捨棄或允許流量。 依預設會停用 ACL。若要啟用，請按一下 設定 ，然後選取 已啟用 。 選取動作： <ul style="list-style-type: none"> ■ 允許 - 允許符合所選群組的連線。捨棄所有其他連線。 ■ 捨棄 - 允許不符合所選群組的連線。如果已啟用存取記錄，則捨棄的連線會產生記錄項目。 選取 群組 。此群組中包含已由 ACL 捨棄或允許的 IP 位址。
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。

L4 TCP 選項	L4 TCP 說明
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	<p>從下拉式功能表中選取現有 sorry 伺服器集區。</p> <p>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。</p> <p>您可以按一下垂直省略符號來建立伺服器集區。</p>
預設集區成員連接埠	<p>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。</p> <p>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。</p>
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	<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>
L4 UDP 選項	L4 UDP 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。支援 IPv4 和 IPv6 位址。請注意，集區成員的 IP 版本必須符合 VIP IP 版本。例如，VIP-IPv4 與 Pool-IPv4，以及 IPv6 與 Pool-IPv6。
連接埠	輸入虛擬伺服器的連接埠號碼。
負載平衡器	從下拉式功能表中選取要連結至此第 4 層虛擬伺服器的現有負載平衡器。
伺服器集區	<p>從下拉式功能表中選取現有的伺服器集區。</p> <p>伺服器集區由一或多個以相同方式設定且執行相同應用程式的伺服器 (亦稱為集區成員) 組成。</p> <p>您可以按一下垂直省略符號來建立伺服器集區。</p>
應用程式設定檔	<p>根據通訊協定類型，現有應用程式設定檔會自動填入。</p> <p>您可以按一下垂直省略符號來建立應用程式設定檔。</p>
持續性	<p>從下拉式功能表中選取現有的持續性設定檔。</p> <p>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。</p>
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。
存取清單控制項	<p>啟用存取清單控制項 (ACL) 時，會使用 ACL 陳述式比較流經負載平衡器的所有流量，進而捨棄或允許流量。</p> <p>依預設會停用 ACL。若要啟用，請按一下設定，然後勾選已啟用。</p> <p>選取動作：</p> <ul style="list-style-type: none"> ■ 允許 - 允許符合所選群組的連線。捨棄所有其他連線 ■ 捨棄 - 允許不符合所選群組的連線。如果已啟用存取記錄，則捨棄的連線會產生記錄項目。 <p>選取群組。此群組中包含已由 ACL 捨棄或允許的 IP 位址。</p>
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。

L4 UDP 選項	L4 UDP 說明
Sorry Server 集區	<p>從下拉式功能表中選取現有 sorry 伺服器集區。</p> <p>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。</p> <p>您可以按一下垂直省略符號來建立伺服器集區。</p>
預設集區成員連接埠	<p>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。</p> <p>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。</p>
管理狀態	<p>切換按鈕以停用第 4 層虛擬伺服器的管理狀態。</p>
存取記錄	<p>切換按鈕以啟用第 4 層虛擬伺服器的記錄。</p>
僅記錄重大事件	<p>僅在存取記錄已啟用的情況下，才能設定此欄位。無法傳送至集區成員的連線會被視為重大事件，例如「最大連線限制」或「存取控制捨棄」。</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。

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 從下拉式清單中選取 **L7 HTTP**，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。支援 IPv4 和 IPv6 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 按一下其他內容以設定其他第 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。
僅記錄重大事件	僅在存取記錄已啟用的情況下，才能設定此欄位。HTTP 回應狀態為 ≥ 400 的請求會被視為重大事件。
標籤	從下拉式清單中選取標籤。 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。

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。

每個負載平衡器規則將在下列負載平衡處理的特定階段實作：傳輸、HTTP 存取、要求重寫、要求轉送和回應重寫。並非所有比對條件和動作均適用於每個階段。

如果 LbService 中已設定 `skip_scale_validation` 旗標，則可使用 API 設定最多 4,000 個負載平衡器規則。請注意，您可以透過 API 設定旗標。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。透過使用者介面可設定最多 512 個負載平衡器規則。

對於比對類型，負載平衡器規則支援 REGEX。如需詳細資訊，請參閱[負載平衡器規則中的規則運算式](#)。

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](#)。

■ 設定傳輸階段負載平衡器規則

傳輸階段是用戶端 HTTP 請求的第一個階段。

■ 設定 HTTP 存取負載平衡器規則

JSON Web Token (JWT) 是一種標準化、選用的驗證和/或加密格式，用於保護在兩方之間傳輸的資訊。

■ 設定請求重寫負載平衡器規則

HTTP 請求重寫會套用至來自用戶端的 HTTP 請求。

■ 設定請求轉送負載平衡器規則

請求轉送會將 URL 或主機重新導向至特定伺服器集區。

■ 設定回應重寫負載平衡器規則

HTTP 回應重寫會套用至從伺服器到用戶端的 HTTP 回應。

■ 負載平衡器規則中的規則運算式

規則運算式 (REGEX) 用於負載平衡器規則的相符條件。

設定傳輸階段負載平衡器規則

傳輸階段是用戶端 HTTP 請求的第一個階段。

您可以在 **SSL 組態** 下找到負載平衡器虛擬伺服器 SSL 組態。有兩種可行的組態。在這兩種模式中，負載平衡器會看到流量，並根據用戶端 HTTP 流量套用負載平衡器規則。

- **SSL 卸載**，僅設定 SSL 用戶端。在此模式中，用戶端至 VIP 流量會加密 (HTTPS)，而負載平衡器會對其解密。VIP 至集區成員流量為明文 (HTTP)。
- **SSL 端對端**，同時設定用戶端 SSL 和伺服器 SSL。在此模式中，用戶端至 VIP 流量會加密 (HTTPS)，而負載平衡器會對其解密，然後重新加密。VIP 至集區成員流量為加密 (HTTPS)。

當虛擬伺服器收到用戶端 SSL hello 訊息時，傳輸階段即完成。這會在 SSL 結束之前以及 HTTP 流量之前發生。

傳輸階段可讓管理員根據用戶端 SSL hello 訊息，選取 SSL 模式以及特定伺服器集區。虛擬伺服器 SSL 模式有三個選項：

- SSL 卸載
- 端對端
- SSL 傳遞 (負載平衡器不會結束 SSL)

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。請參閱[負載平衡器規則中的規則運算式](#)。

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，於 [傳輸階段] 旁，按一下 **設定 > 新增規則**，以針對傳輸階段設定負載平衡器規則。
- 3 SSL SNI 是唯一支援的相符條件。相符條件會用於比對透過負載平衡器傳遞的應用程式流量。
- 4 從下拉式清單中，選取**相符類型**：開頭為、結尾為、等於、包含、符合 RegEx。
- 5 輸入 **SNI 名稱**。
- 6 切換**區分大小寫**按鈕，以設定用於 HTTP 標頭值比較的區分大小寫旗標。
- 7 切換**否定**按鈕以進行啟用。
- 8 從下拉式清單中，選取**符合策略**：

符合策略	說明
任何	若主機或路徑任一符合，即可將此規則視為相符。
全部	主機和路徑均必須符合，才將此規則視為相符。

9 從下拉式功能表中，選取 SSL 模式選取項目。

SSL 模式	說明
SSL 傳遞	SSL 傳遞會將 HTTP 流量傳遞至後端伺服器，而不會在負載平衡器上解密流量。資料會在通過負載平衡器時保持加密狀態。 如果已選取 [SSL 傳遞]，則可以選取伺服器集區。請參閱在管理程式模式中新增用於負載平衡的伺服器集區。
SSL 卸載	SSL 卸載會在負載平衡器上解密所有 HTTP 流量。SSL 卸載允許在負載平衡器和伺服器之間傳遞資料時加以檢查。如果未設定 NTLM 和多工，負載平衡器會針對每個 HTTP 請求建立與所選後端伺服器的新連線。
SSL 端對端	收到 HTTP 請求之後，負載平衡器會連線到所選的後端伺服器，並使用 HTTPS 通訊。如果未設定 NTLM 和多工，負載平衡器會針對每個 HTTP 請求建立與所選後端伺服器的新連線。

10 按一下儲存和套用。

設定 HTTP 存取負載平衡器規則

JSON Web Token (JWT) 是一種標準化、選用的驗證和/或加密格式，用於保護在兩方之間傳輸的資訊。

在 HTTP 存取階段中，使用者可以定義用來驗證來自用戶端 JWT 的動作，並將 JWT 傳遞至後端伺服器或將其移除。

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。請參閱負載平衡器規則中的規則運算式。

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，於 [HTTP 存取階段] 旁，按一下設定 > 新增規則，以針對 HTTP 請求重寫階段設定負載平衡器規則。
- 3 從下拉式功能表中，選取相符條件。相符條件會用於比對透過負載平衡器傳遞的應用程式流量。可在一個負載平衡器規則中指定多個相符條件。每個相符條件均定義應用程式流量的準則。

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

支援的比對條件	說明
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
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 HTTP 訊息中 IP 標頭文字方塊。來源類型必須是單一 IP 位址、IP 位址範圍或群組。請參閱 新增群組 。 <ul style="list-style-type: none"> ■ 如果選取了 [IP 標頭來源] 並具有 [IP 位址] 來源類型，則 HTTP 訊息的來源 IP 位址應符合群組中設定的 IP 位址。支援 IPv4 和 IPv6 位址。 ■ 如果選取了 [IP 標頭來源] 並具有 [群組] 來源類型，請從下拉式功能表中選取群組。 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。
用戶端 SSL	比對用戶端 SSL 設定檔識別碼。 ssl_profile_id - 要比對的值
區分大小寫	設定區分大小寫的旗標以用於 HTTP 標頭值比較。如果為 true，則比較 HTTP 本文值時大小寫很重要。

- 4 從下拉式清單中，選取**相符類型**：開頭為、結尾為、等於、包含、符合 Regex。
- 5 如有需要，請輸入 URI。
- 6 從下拉式清單中，選取**符合策略**：

符合策略	說明
任何	若主機或路徑任一符合，即可將此規則視為相符。
全部	主機和路徑均必須符合，才將此規則視為相符。

7 從下拉式功能表，選取動作：

動作	說明
JWT 驗證	<p>JSON Web Token (JWT) 是開放式標準，其定義一種精簡且獨立的方式，用來在各方之間以 JSON 物件形式安全地傳輸資訊。因為此資訊經過數位簽署，因此可驗證且受信任。</p> <ul style="list-style-type: none"> ■ 領域 - 受保護區域的說明。如果未指定領域，用戶端通常會顯示格式化的主機名稱。當用戶端請求遭拒絕，而出現 401 HTTP 狀態時，會傳回已設定的領域。回應為：「WWW-Authentication: Bearer realm=<realm>」。 ■ Token - 此參數為選用。負載平衡器會逐一搜尋每個指定的 Token 是否有 JWT 訊息，直到找到為止。如果找不到，或如果未設定此文字方塊，則負載平衡器依預設會在 HTTP 請求「Authorization: Bearer <token>」中搜尋 Bearer 標頭 ■ 金鑰類型 - 對稱金鑰或非對稱公開金鑰 (certificate-id) ■ 保留 JWT - 此旗標用來保留 JWT 並將其傳遞給後端伺服器。如果停用，則會移除後端伺服器的 JWT 金鑰。
連線捨棄	如果啟用了否定，則在設定 [連線捨棄] 時，會捨棄不符合指定相符條件的所有請求。允許符合指定相符條件的請求。
變數指派	允許使用者透過以下方式，將值指派給 HTTP 存取階段中的變數：可將結果用作為其他負載平衡器規則階段中的條件。

8 按一下儲存和套用。

設定請求重寫負載平衡器規則

HTTP 請求重寫會套用至來自用戶端的 HTTP 請求。

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](#)。

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。請參閱[負載平衡器規則中的規則運算式](#)。

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，於 [請求重寫階段] 旁，按一下**設定 > 新增規則**，以針對 HTTP 請求重寫階段設定負載平衡器規則。
- 3 從下拉式清單中選取相符條件。相符條件會用於比對透過負載平衡器傳遞的應用程式流量。可在一個負載平衡器規則中指定多個相符條件。每個相符條件均定義應用程式流量的準則。

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

支援的比對條件	說明
HTTP 要求 URI 引數	用於比對 URI 引數 (也稱為 HTTP 請求訊息的查詢字串), 例如, 在 URI http://example.com?foo=1&bar=2 中, 「foo=1&bar=2」是包含 URI 引數的查詢字串。在 URI 配置中, 查詢字串是由第一個問號 (「?」) 字元指出, 且結尾為井字號 (「#」) 字元或 URI 結尾。 http_request.uri_arguments - 要比對的值
HTTP 要求版本	用於比對 HTTP 請求訊息的 HTTP 通訊協定版本 http_request.version - 要比對的值
HTTP 要求標頭	用於依 HTTP 標頭欄位比對 HTTP 請求訊息。HTTP 標頭欄位是 HTTP 請求和回應訊息的標頭區段元件。它們定義 HTTP 交易的作業參數。 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	用於依屬於 HTTP 標頭特定類型的 Cookie 比對 HTTP 請求訊息。match_type 和 case_sensitive 會定義比較 cookie 值的方式。 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 HTTP 訊息中的 IP 標頭欄位。來源類型必須是單一 IP 位址、IP 位址範圍或群組。請參閱 新增群組 。 <ul style="list-style-type: none"> ■ 如果選取了 [IP 標頭來源] 並具有 [IP 位址] 來源類型, 則 HTTP 訊息的來源 IP 位址應符合群組中設定的 IP 位址。支援 IPv4 和 IPv6 位址 ■ 如果選取了 [IP 標頭來源] 並具有 [群組] 來源類型, 請從下拉式清單中選取群組。 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。如果為 true, 則比較 HTTP 本文值時大小寫很重要。

- 4 從下拉式功能表中, 選取**相符類型**: 開頭為、結尾為、等於、包含、或符合 Regex。相符類型用於將條件與指定動作比對。

相符類型	說明
開頭為	如果相符條件的開頭為指定值, 則條件會相符。
結尾為	如果相符條件的結尾為指定值, 則條件會相符。
等於	如果相符條件與指定值相同, 則條件會相符。
包含	如果相符條件包含指定的值, 則條件會相符。
符合 Regex	如果相符條件符合指定的值, 則條件會相符。

- 5 指定 URI。
- 6 從下拉式功能表中，選取**符合策略**：

符合策略	說明
任何	指出將符合此規則的主機或路徑視為相符。
全部	指出主機和路徑均必須符合，才將此規則視為相符。

- 7 從下拉式功能表中選取動作：

動作	說明
HTTP 要求 URI 重寫	此動作用於在符合的 HTTP 請求訊息中重寫 URI。指定要在此情況下將相符的 HTTP 請求訊息的 URI 和 URI 引數重寫至新值的 URI 和 URI 引數。HTTP 訊息的完整 URI 配置有如下語法：Scheme://[user[:password]@]host[:port]][/path][?query][#fragment] 此動作的 URI 欄位用於重寫上述配置中的 /path 部分。[URI 引數] 欄位用於重寫查詢部分。擷取的變數和內建變數可用於 URI 和 URI 引數欄位。 <ol style="list-style-type: none"> a 輸入 HTTP 請求的 URI b 輸入 URI 的查詢字串，通常包含索引鍵值配對，例如： foo1=bar1&foo2=bar2。
HTTP 要求標頭重寫	此動作用於將符合 HTTP 請求訊息的標頭欄位重寫為指定的新值。 <ol style="list-style-type: none"> a 輸入標頭文字方塊 HTTP 請求訊息的名稱。 b 輸入標頭值。
HTTP 要求標頭刪除	此動作用於在 HTTP_REQUEST_REWRITE 階段刪除 HTTP 請求訊息的標頭欄位。一個動作可用於刪除具有相同標頭名稱的所有標頭。若要刪除具有不同標頭名稱的標頭，必須定義多個動作。 <ul style="list-style-type: none"> ■ 輸入 HTTP 請求訊息標頭欄位的名稱。
變數指派	建立變數並為其指定名稱和值。

- 8 切換**區分大小寫**按鈕，以設定用於 HTTP 標頭值比較的區分大小寫旗標。
- 9 切換**否定**按鈕以進行啟用。
- 10 按一下**儲存**和**套用**。

設定請求轉送負載平衡器規則

請求轉送會將 URL 或主機重新導向至特定伺服器集區。

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](#)。

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。請參閱[負載平衡器規則中的規則運算式](#)。

程序

- 1 開啟第 7 層 HTTP 虛擬伺服器。
- 2 按一下**請求轉送 > 新增規則**，以針對 HTTP 請求轉送設定負載平衡器規則。

- 3 從下拉式清單中選取相符條件。相符條件會用於比對透過負載平衡器傳遞的應用程式流量。可在一個負載平衡器規則中指定多個相符條件。每個相符條件均定義應用程式流量的準則。

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	用於比對 URI 引數 (也稱為 HTTP 請求訊息的查詢字串)，例如，在 URI http://example.com?foo=1&bar=2 中，「foo=1&bar=2」是包含 URI 引數的查詢字串。在 URI 配置中，查詢字串是由第一個問號 (「?」) 字元指出，且結尾為井字號 (「#」) 字元或 URI 結尾。 http_request.uri_arguments - 要比對的值
HTTP 要求版本	用於比對 HTTP 請求訊息的 HTTP 通訊協定版本 http_request.version - 要比對的值
HTTP 要求標頭	用於依 HTTP 標頭欄位比對 HTTP 請求訊息。HTTP 標頭欄位是 HTTP 請求和回應訊息的標頭區段元件。它們定義 HTTP 交易的作業參數。 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	用於依屬於 HTTP 標頭特定類型的 Cookie 比對 HTTP 請求訊息。match_type 和 case_sensitive 會定義比較 cookie 值的方式。 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 HTTP 訊息中的 IP 標頭欄位。來源類型必須是單一 IP 位址、IP 位址範圍或群組。請參閱 新增群組 。 <ul style="list-style-type: none"> ■ 如果選取了 [IP 標頭來源] 並具有 [IP 位址] 來源類型，則 HTTP 訊息的來源 IP 位址應符合群組中設定的 IP 位址。支援 IPv4 和 IPv6 位址 ■ 如果選取了 [IP 標頭來源] 並具有 [群組] 來源類型，請從下拉式清單中選取群組。 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。如果為 true，則比較 HTTP 本文值時大小寫很重要。

4 選取動作：

動作	說明
HTTP 拒絕	用於拒絕 HTTP 請求訊息。指定的 reply_status 值將用作對應 HTTP 回應訊息的狀態碼。回應訊息會傳送回到用戶端 (通常是瀏覽器)，指出遭到拒絕的原因。 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	用於將 HTTP 請求訊息重新導向至新的 URL。用於重新導向的 HTTP 狀態碼為 3xx，例如，301、302、303、307 等。redirect_url 是將 HTTP 請求訊息重新導向至其中的新 URL。 http_forward.redirect_status - 用於重新導向 http_forward.redirect_url 的 HTTP 狀態碼 - 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。相符的 HTTP 請求訊息會轉送到指定的集區。 如果啟用了 HTTP 保持運作，並在負載平衡器中設定了轉送規則，則會優先採用伺服器保持運作設定。因此，會將 HTTP 要求傳送到已連線且保持運作的伺服器。 在符合負載平衡器規則條件的情況下，如果您始終希望優先使用轉送規則，請停用保持運作設定。 請注意，持續性設定優先於保持運作設定。 執行程序時，其優先順序如下：持續性 > 保持運作 > 負載平衡器規則 http_forward.select_pool - 伺服器集區 UUID
變數持續性檢測	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請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。
連線捨棄	如果在條件中啟用了否定，則在設定 [連線捨棄] 時，會捨棄不符合條件的所有請求。允許符合條件的請求。
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。

5 按一下儲存和套用。

設定回應重寫負載平衡器規則

HTTP 回應重寫會套用至從伺服器到用戶端的 HTTP 回應。

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](#)。

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。請參閱[負載平衡器規則中的規則運算式](#)。

程序

- 1 開啟第 7 層 HTTP 虛擬伺服器。

2 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	此情況用於依 HTTP 標頭欄位，比對來自後端伺服器的 HTTP 回應訊息。 http_response.header_name - 要比對的標頭名稱 http_response.header_value - 要比對的值
HTTP 回應方法	比對 HTTP 回應方法。 http_response.method - 要比對的值
HTTP 回應 URI	比對 HTTP 回應 URI。 http_response.uri - 要比對的值
HTTP 回應 URI 引數	比對 HTTP 回應 URI 引數。 http_response.uri_args - 要比對的值
HTTP 回應版本	比對 HTTP 回應版本。 http_response.version - 要比對的值
HTTP 回應 Cookie	比對任何 HTTP 回應 Cookie。 http_response.cookie_value - 要比對的值
用戶端 SSL	比對用戶端 SSL 設定檔識別碼。 ssl_profile_id - 要比對的值
TCP 標頭連接埠	比對 TCP 來源或目的地連接埠。 tcp_header.source_port - 要比對的來源連接埠 tcp_header.destination_port - 要比對的目的地連接埠
IP 標頭來源	比對 HTTP 訊息中的 IP 標頭欄位。來源類型必須是單一 IP 位址、IP 位址範圍或群組。請參閱 新增群組 。 HTTP 訊息的來源 IP 位址應符合群組中設定的 IP 位址。支援 IPv4 和 IPv6 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。

3 選取動作：

動作	說明
HTTP 回應標頭重寫	此動作用於將 HTTP 回應訊息的標頭欄位重寫為指定的新值。 http_response.header_name - 標頭名稱 http_response.header_value - 要寫入的值
HTTP 回應標頭刪除	此動作用於刪除 HTTP 回應訊息的標頭欄位。 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。

4 按一下儲存和套用。

負載平衡器規則中的規則運算式

規則運算式 (REGEX) 用於負載平衡器規則的相符條件。

支援 Perl 相容規則運算式 (PCRE) 樣式 REGEX 模式，但對進階使用案例有一些限制。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_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「.」

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, 且使用 LB-SNAT 自動對應 : T1-Uplink IP 100.64.x.y 和 T1-ServiceInterface IP
- 設定集區, 且使用 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*。

分散式負載平衡器

9

在 NSX-T Data Center 中設定的分散式負載平衡器可協助您有效地負載平衡東西向流量和縮放流量，因為流量會在每個 ESXi 主機上執行。

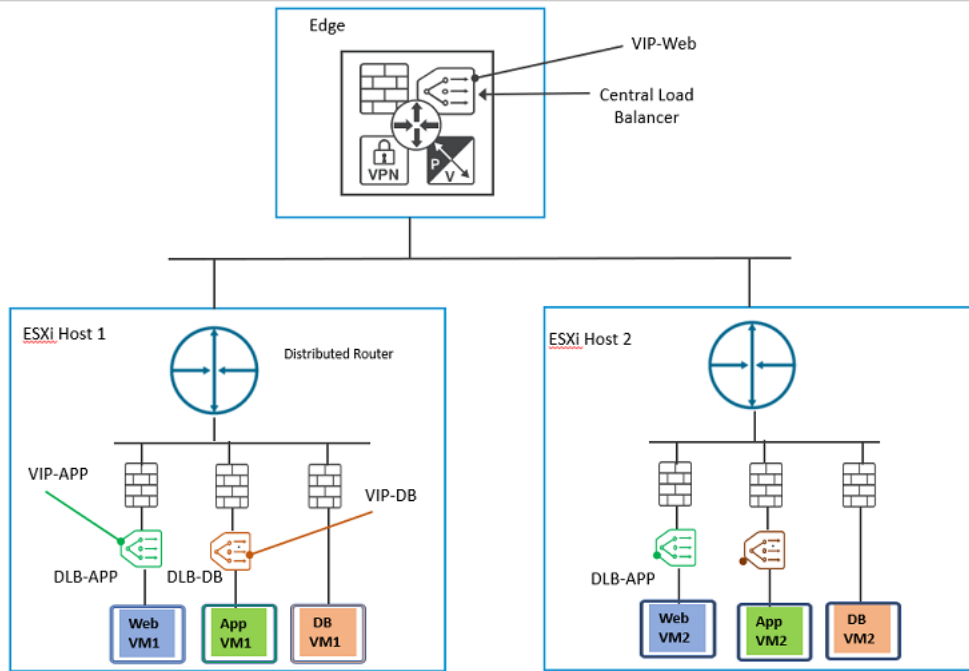
重要 分散式負載平衡器僅支援由 vSphere with Kubernetes 管理的 Kubernetes (K8s) 叢集 IP。任何其他工作負載類型均不支援分散式負載平衡器。身為管理員，您無法使用 NSX Manager GUI，來建立或修改分散式負載平衡器物件。這些物件是在 vCenter Server 中建立 K8 叢集 IP 時由 vCenter Server 透過 NSX-T API 推送。

備註 請勿在使用分散式負載平衡器的環境中啟用分散式入侵偵測服務 (IDS)。NSX-T Data Center 不支援搭配分散式負載平衡器使用 IDS。

在傳統網路中，部署在 NSX Edge 節點上的中央負載平衡器，已設定為可散佈由負載平衡器上設定的虛擬伺服器所管理的流量負載。

如果您使用的是中央平衡器，增加負載平衡器集區中的虛擬伺服器數目，可能不一定總能滿足多層分散式應用程式的規模或效能準則。分散式負載平衡器會在負載平衡工作負載 (例如用戶端和伺服器) 部署所在的每個 Hypervisor 上實現，以確保流量的負載平衡會以散佈的方式在每個 Hypervisor 上進行。

分散式負載平衡器可在 NSX-T Data Center 網路上以及中央負載平衡器上設定。



在此圖中，分散式負載平衡器的執行個體已連結至虛擬機器群組。當虛擬機器下行到分散式邏輯路由器時，分散式負載平衡器僅會對東西向流量進行負載平衡。相反地，中央負載平衡器會管理南北向流量。

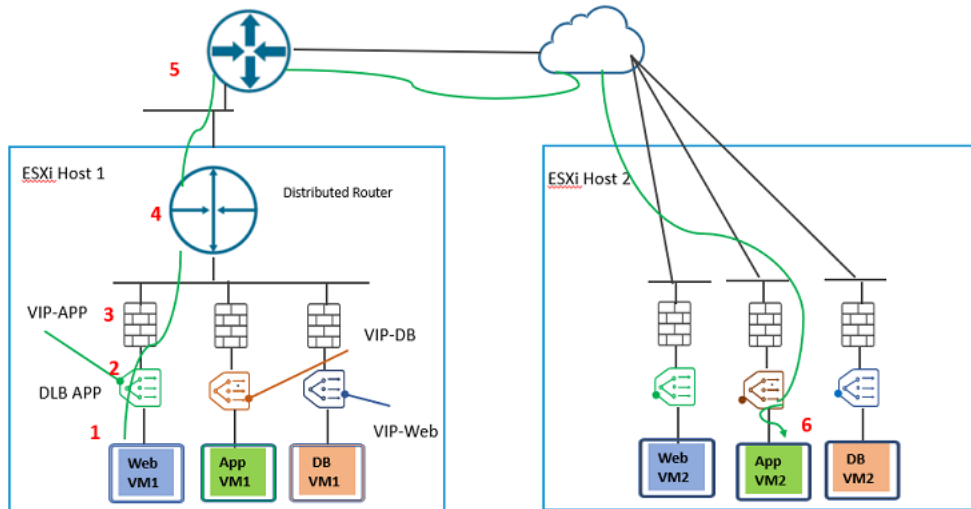
若要迎合應用程式的每個元件或模組的負載平衡需求，可將分散式負載平衡器連結至應用程式的每個階層。例如，若要為使用者請求提供服務，應用程式前端必須向外與中間模組連線以取得資料。但是，中間層的部署可能不會提供最終資料給使用者，因此需要向外與後端層連線以取得其他資料。對於複雜的應用程式，許多模組可能需要彼此互動才能取得資訊。除了複雜性，當使用者要求的數目以指數型增加時，分散式負載平衡器可有效地滿足使用者需求，而不會造成效能衝擊。在每台主機上設定分散式負載平衡器，可有效達成規模和封包傳輸效率的問題。

本章節討論下列主題：

- 瞭解分散式負載平衡器的流量
- 建立和連結分散式負載平衡器執行個體
- 建立分散式負載平衡器的伺服器集區
- 使用 Fast TCP 或 UDP 設定檔建立虛擬伺服器
- 在 ESXi 主機上驗證分散式負載平衡器組態
- 監控分散式負載平衡器統計資料

瞭解分散式負載平衡器的流量

瞭解連線至分散式負載平衡器 (DLB) 執行個體的虛擬機器之間的流量。



身為管理員，請確保：

- 連線至 DLB 執行個體的虛擬 IP 位址和集區成員必須具有唯一的 IP 位址，流量才能正確路由。

Web VM1 和 APP VM2 之間的流量。

- 1 當 Web VM1 送出封包至應用程式 VM2 時，VIP-APP 會接收該封包。

DLB APP 會連結至由 Web 層虛擬機器組成的原則群組。同樣地，主控 VIP-DB 的 DLB 應用程式必須連結至由應用程式層虛擬機器組成的原則群組。

- 2 DLB APP 上主控的 VIP-APP 會接收來自 Web VM1 的請求。
- 3 在到達目的地虛擬機器群組之前，會使用分散式防火牆規則篩選封包。
- 4 根據防火牆規則篩選封包後，會將其傳送至第 1 層路由器。
- 5 然後進一步將它路由至實體路由器。
- 6 當封包傳送到目的地 App VM2 群組時，路由即完成。

由於 DLB VIP 只能從連線至第 0 層或第 1 層邏輯路由器的下行虛擬機器存取，因此，DLB 會對東西向流量提供負載平衡服務。

DLB 執行個體可與 DFW 的執行個體並存。在 Hypervisor 的虛擬介面上啟用 DLB 和 DFW 時，首先會根據 DLB 中的組態對流量進行負載平衡，然後將 DFW 規則套用至從虛擬機器到 Hypervisor 的流量。DLB 規則會套用至源自第 0 層或第 1 層邏輯路由器的下行，並前往目的地 Hypervisor 的流量。DLB 規則不能套用至相反方向的流量，即源自主機外部，前往目的地虛擬機器的流量。

例如，如果 DLB 執行個體是從 Web-VM 到 App-VM 的負載平衡流量，那麼，若要允許此類流量通過 DFW，請確保 DFW 規則已設定為值「Source=Web-VMs, Destination=App-VMs, Action=Allow」。

建立和連結分散式負載平衡器執行個體

與中央負載平衡器不同，分散式負載平衡器 (DLB) 執行個體會連結至虛擬機器群組的虛擬介面。

在程序結束時，DLB 執行個體會連結至虛擬機器群組的虛擬介面。

只能透過 API 命令建立和連結 DLB 執行個體。

必要條件

- 新增由虛擬機器組成的原則群組。例如，此類虛擬機器群組可與從 Web 層的虛擬機器接收請求的應用程式層相關聯。

程序

- ◆ 執行 `Put /policy/api/v1/infra/lb-services/<mydlb>`。

```
{
  "connectivity_path" : "/infra/domains/default/groups/<clientVMGroup>",
  "enabled" : true,
  "size" : "DLB",
  "error_log_level" : "INFO",
  "access_log_enabled" : false,
  "resource_type" : "LBService",
  "display_name" : "mydlb"
}
```

其中，

- `connectivity_path` :
 - 如果連線路徑設為空值或空白，則不會將 DLB 執行個體套用至任何傳輸節點。
 - 如果連線路徑設為 ALL，則所有傳輸節點的所有虛擬介面都將繫結至 DLB 執行個體。一個 DLB 執行個體會套用至原則群組的所有虛擬介面。
- `size` : 設為 DLB 值。由於每個應用程式或虛擬介面會取得 DLB 的一個執行個體，因此 DLB 執行個體僅有單一大小機器尺寸。
- `enabled` : 依預設會啟用建立的 DLB 執行個體。

建立一個 DLB 執行個體，並將其連結至虛擬機器群組。在 Web 層上建立的 DLB 執行個體會連結至應用程式層虛擬機器群組的所有虛擬介面。

後續步驟

建立 DLB 執行個體後，登入 NSX Manager，移至 **網路 -> 負載平衡 -> 負載平衡器**。檢視 DLB 執行個體的詳細資料。

下一步，[建立分散式負載平衡器的伺服器集區](#)。

建立分散式負載平衡器的伺服器集區

建立負載平衡器集區，以包含耗用 DLB 服務的虛擬機器。

此工作可以透過 NSX-T UI 和 NSX-T API 進行。

用來建立 DLB 集區的 API 命令為 PUT `https://<NSXManager_IPAddress>/policy/api/v1/infra/lb-pools/<lb-pool-id>`

必要條件

- 建立耗用 DLB 服務的虛擬機器群組。
- 建立 DLB 執行個體，並將其連結至虛擬機器群組。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 移至網路 → 負載平衡 → 伺服器集區。
- 3 按一下**新增伺服器集區**。
- 4 在這些欄位中輸入值。

欄位	說明
名稱	輸入 DLB 集區的名稱。
演算法	分散式負載平衡器僅支援 ROUND_ROBIN。
成員	<p>按一下選取成員，然後將個別成員新增到群組。</p> <p>新增個別成員時，僅在下列文字方塊中輸入值：</p> <ul style="list-style-type: none"> ■ 名稱 ■ IP 位址 ■ 連接埠 <p>備註 此清單包含只支援將成員新增至 DLB 集區的欄位。</p>
成員群組	<p>按一下選取成員，然後新增成員群組。</p> <p>新增個別成員時，在下列欄位中輸入值：</p> <ul style="list-style-type: none"> ■ 名稱 ■ 計算成員：按一下設定成員，以新增包含所有集區成員的群組。 ■ IP 修訂篩選器：僅支援 IPv4。 ■ 連接埠：所有動態集區成員的預設連接埠。 <p>備註 此清單包含只支援將成員新增至 DLB 集區的欄位。</p>
SNAT 轉譯模式	將此欄位設定為 已停用 狀態。分散式負載平衡器中不支援 SNAT 轉譯。

- 5 按一下**儲存**。

結果

已為分散式負載平衡器新增伺服器集區成員。

後續步驟

請參閱[使用 Fast TCP 或 UDP 設定檔建立虛擬伺服器](#)。

使用 Fast TCP 或 UDP 設定檔建立虛擬伺服器

建立虛擬伺服器，並將其繫結到分散式負載平衡器服務。

此工作可以透過 NSX-T UI 和 NSX-T API 執行。

用來建立虛擬伺服器的 API 命令為 `PUT https://<NSXManager_IPAddress>/policy/api/v1/infra/lb-virtual-servers/<lb-virtual-server-id>`。

必要條件

- 建立用於分散式負載平衡器的伺服器集區。

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 移至網路 → 負載平衡器 → 虛擬伺服器。
- 3 按一下**新增虛擬伺服器 -> L4 TCP**。
- 4 若要設定分散式負載平衡器的虛擬伺服器，僅支援下列欄位。

欄位	說明
名稱	輸入虛擬伺服器的名稱。
IP 位址	分散式負載平衡器虛擬伺服器的 IP 位址。設定分散式負載平衡器虛擬伺服器的 IP 位址，在其中接收所有用戶端連線，並在後端伺服器之間散佈。
連接埠	虛擬伺服器連接埠號碼。 分散式負載平衡器的虛擬伺服器不支援多個連接埠或連接埠範圍。
負載平衡器	連結與虛擬伺服器相關聯的分散式負載平衡器執行個體。然後，虛擬伺服器會知道負載平衡器所服務的原則群組。
伺服器集區	選取伺服器集區。伺服器集區包含後端伺服器。伺服器集區由一或多個已具有類似設定且執行相同應用程式的伺服器組成。也稱為集區成員。
應用程式設定檔	選取虛擬伺服器的應用程式設定檔。 應用程式設定檔會定義應用程式通訊協定的特性。它用於影響負載平衡的執行方式。支援的應用程式設定檔包括： <ul style="list-style-type: none"> ■ 負載平衡器 Fast TCP 設定檔 ■ 負載平衡器 Fast UDP 設定檔
預設集區成員連接埠	選擇性欄位。 輸入一個要在未定義成員連接埠時使用的連接埠號碼。分散式負載平衡器的虛擬伺服器不支援使用多個連接埠或連接埠範圍來作為預設集區成員連接埠。
持續性	選擇性欄位。 選取來源 IP 或已停用。

分散式負載平衡器組態已完成。

結果

確認 DLB 是否根據組態中定義的演算法，將流量散佈到集區中的所有伺服器。如果您選擇 Round_Robin 演算法，則 DLB 必須能夠以循環配置資源方式，從集區選擇伺服器。

在 ESXi 主機中，確認 DLB 組態是否完成。

後續步驟

請參閱在 [ESXi 主機上驗證分散式負載平衡器組態](#)。

在 ESXi 主機上驗證分散式負載平衡器組態

驗證是否已在 ESXi 主機上完整設定分散式負載平衡器。

安全地連線至 ESXi 主機後，請執行 `/opt/vmware/nsx-nestdb/bin/nestdb-cli`。從 `nestdb-cli` 提示，執行下列命令。

命令	回應範例
若要檢視已設定的 DLB 服務，請執行 <code>get LbServiceMsg</code> 。	<pre>{'id': {'left': 13946864992859343551, 'right': 10845263561610880178}, 'virtual_server_id': [{'left': 13384746951958284821, 'right': 11316502527836868364}], 'display_name': 'mydlb', 'size': 'DLB', 'enabled': True, 'access_log_enabled': False, 'log_level': 'LB_LOG_LEVEL_INFO', 'applied_to': {'type': 'CONTAINER', 'attachment_id': {'left': 2826732686997341216, 'right': 10792930437485655035}}}</pre>
若要檢視為 DLB 設定的虛擬伺服器，請執行 <code>get LbVirtualServerMsg</code> 。	<pre>{'port': '80', 'revision': 0, 'display_name': 'mytcpvip', 'pool_id': {'left': 4370937730160476541, 'right': 13181758910457427118}, 'enabled': True, 'access_log_enabled': False, 'id': {'left': 13384746951958284821, 'right': 11316502527836868364}, 'ip_protocol': 'TCP', 'ip_address': {'ipv4': 2071690107}, 'application_profile_id': {'left': 1527034089224553657, 'right': 10785436903467108397}}}</pre>

命令	回應範例
若要檢視 DLB 集區成員的組態，請執行 <code>get LbPoolMsg</code> 。	<pre>{'tcp_multiplexing_number': 6, 'display_name': 'mylbpool', 'tcp_multiplexing_enabled': False, 'member': [{'port': '80', 'weight': 1, 'display_name': 'Member_VM30', 'admin_state': 'ENABLED', 'ip_address': {'ipv4': 3232261280}, 'backup_member': False}, {'port': '80', 'weight': 1, 'display_name': 'Member_VM31', 'admin_state': 'ENABLED', 'ip_address': {'ipv4': 3232261281}, 'backup_member': False}, {'port': '80', 'weight': 1, 'display_name': 'Member_VM32', 'admin_state': 'ENABLED', 'ip_address': {'ipv4': 3232261282}, 'backup_member': False}], 'id': {'left': 4370937730160476541, 'right': 13181758910457427118}, 'min_active_members': 1, 'algorithm': 'ROUND_ROBIN'}</pre>
若要檢視推送至 ESXi 主機的 NSX Controller 組態，請執行 <code>get ContainerMsg</code> 。	<pre>{'container_type': 'CONTAINER', 'id': {'left': 2826732686997341216, 'right': 10792930437485655035}, 'vif': ['cd2e482b-2998-480f- beba-65fbd7able62', 'f8aa2a58-5662-4c6b-8090- d1bd19174205', '83a1f709-e675-4e42-b677- ff501fd0f4ec', 'b8366b39-4c81-41fc-b89e- de7716462b2f'], 'name': 'default.clientVMGroup', 'mac_address': [{'mac': 52237218275}, {'mac': 52243694681}, {'mac': 52233233291}, {'mac': 52239463383}], 'ip_address': [{'ipv4': 16844388}, {'ipv4': 16844644}, {'ipv4': 16844132}, {'ipv4': 3232261283}, {'ipv4': 16844298}, {'ipv4': 16844554}, {'ipv4': 16844042}]}</pre>
若要在 ESXi 主機上檢視應用程式設定檔組態，請執行 <code>get LbApplicationProfileMsg</code> 。	<pre>{'display_name': 'default-tcp-lb-app-profile', 'id': {'left': 1527034089224553657, 'right': 10785436903467108397}, 'application_type': 'FAST_TCP', 'fast_tcp_profile': {'close_timeout': 8, 'flow_mirroring_enabled': False, 'idle_timeout': 1800}}</pre>

監控分散式負載平衡器統計資料

用於監控分散式負載平衡器執行個體統計資料的 NSX-T Data Center CLI 命令。

動作	命令
顯示所有負載平衡器。	<code>get load-balancers</code>
顯示特定負載平衡器。	<code>get load-balancer <UUID_LoadBalancer></code>
顯示負載平衡器虛擬伺服器組態。	<code>get load-balancer <UUID_LoadBalancer> virtual-servers</code>

動作	命令
顯示指定負載平衡器所有集區的統計資料	<code>get load-balancer <UUID_LoadBalancer> pools stats</code>
顯示指定負載平衡器和集區的統計資料	<code>get load-balancer <UUID_LoadBalancer> pool <UUID_Pool> stats</code>
顯示持續性資料表項目	<code>get load-balancer <UUID_LoadBalancer> persistence- tables</code>
顯示負載平衡器集區組態	<code>get load-balancer <UUID_LoadBalancer> pools</code>
顯示指定負載平衡器的所有虛擬伺服器的統計資料	<code>get load-balancer <UUID_LoadBalancer> virtual- servers stats</code>
顯示指定負載平衡器和虛擬伺服器的統計資料	<code>get load-balancer <UUID_LoadBalancer> virtual- server <UUID_VirtualServer> stat</code>
清除指定負載平衡器和集區的統計資料	<code>clear load-balancer <UUID_LoadBalancer> pool <UUID_Pool> stats</code>
清除指定負載平衡器所有集區的統計資料	<code>clear load-balancer <UUID_LoadBalancer> pools stats</code>
清除指定負載平衡器的統計資料	<code>clear load-balancer <UUID_LoadBalancer> stats</code>
清除指定負載平衡器和虛擬伺服器的統計資料	<code>clear load-balancer <UUID_LoadBalancer> virtual- server <UUID_VirtualServer> stats</code>
清除指定負載平衡器所有虛擬伺服器的統計資料	<code>clear load-balancer <UUID_LoadBalancer> virtual- servers stats</code>

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 23 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)

11

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 設定檔
- 將 DHCP 設定檔連結至第 0 層或第 1 層閘道
- 案例：為 DHCP 服務選取 Edge 叢集
- 案例：在 DHCP 上變更區段連線的影響
- 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 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 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 設定檔

您必須先在網路中新增 DHCP 設定檔，之後才能於區段上設定 DHCP。您可以建立兩種類型的 DHCP 設定檔：DHCP 伺服器設定檔和 DHCP 轉送設定檔。

DHCP 設定檔可以同時供您網路中的多個區段和閘道使用。將 DHCP 設定檔連結至區段或閘道時，適用以下條件：

- 在第 0 層或第 1 層閘道或閘道連線的區段中，您可以連結 DHCP 伺服器設定檔或 DHCP 轉送設定檔。
- 在未連線至閘道的獨立區段上，您只能連結 DHCP 伺服器設定檔。獨立區段僅支援本機 DHCP 伺服器。
- **新增 DHCP 伺服器設定檔**
您可以在網路中新增多個 DHCP 伺服器設定檔。此外，您可以將單一 DHCP 伺服器設定檔連結至多個 DHCP 伺服器。
- **新增 DHCP 轉送設定檔**
您可以新增 DHCP 轉送設定檔以將 DHCP 流量轉送至遠端 DHCP 伺服器。遠端或外部 DHCP 伺服器可位於 SDDC 之外的任何覆蓋區段或實體網路中。

新增 DHCP 伺服器設定檔

您可以在網路中新增多個 DHCP 伺服器設定檔。此外，您可以將單一 DHCP 伺服器設定檔連結至多個 DHCP 伺服器。

必要條件

- 已在網路中部署 Edge 節點。
- 已在網路中新增 Edge 叢集。

程序

- 1 從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 管理 > DHCP**。
- 3 按一下 **新增 DHCP 設定檔**。
- 4 輸入可識別 DHCP 伺服器設定檔的唯一名稱。
- 5 在 **設定檔類型** 下拉式功能表中，選取 **DHCP 伺服器**。
- 6 (選擇性) 以 CIDR 格式輸入 DHCP 伺服器的 IP 位址。

備註 最多支援兩個 DHCP 伺服器 IP 位址。您可以輸入一個 IPv4 位址和一個 IPv6 位址。對於 IPv4 位址，首碼長度必須 ≤ 30 ，而對於 IPv6 位址，首碼長度必須 ≤ 126 。DHCP 伺服器 IP 位址不得與 DHCP 範圍和 DHCP 靜態繫結中使用的位址重疊。

如果未指定任何伺服器 IP 位址，則系統會將 100.96.0.1/30 自動指派給 DHCP 伺服器。

伺服器 IP 位址不可為下列任何項目：

- 多點傳播 IP 位址
- 廣播 IP 位址
- 回送 IP 位址
- 未指定的 IP 位址 (全為零的位址)

7 (選擇性) 編輯租用時間 (以秒為單位)。預設值為 86400。

值的有效範圍為 60-4294967295。

8 選取 Edge 叢集。

請遵循下列準則：

- 如果您在區段上使用本機 DHCP 伺服器，則必須在 DHCP 伺服器設定檔中選取 Edge 叢集。如果 Edge 叢集在設定檔中無法使用，則儲存區段時會顯示錯誤訊息。
- 如果您在區段上使用閘道 DHCP 伺服器，請在閘道或 DHCP 伺服器設定檔 (或兩者) 中選取 Edge 叢集。如果 Edge 叢集在設定檔或閘道中無法使用，則儲存區段時會顯示錯誤訊息。

注意 建立 DHCP 伺服器後，您可以在設定檔中變更 Edge 叢集。但是，此動作會導致指派給 DHCP 用戶端的所有現有 DHCP 租用遺失。

當 DHCP 伺服器設定檔連結至使用 DHCP 本機伺服器的區段時，系統會在您於 DHCP 設定檔中指定的 Edge 叢集中建立 DHCP 服務。但是，如果區段使用閘道 DHCP 伺服器，則在其中建立 DHCP 服務的 Edge 叢集將取決於多個因素的組合。如需如何為 DHCP 服務選取 Edge 叢集的詳細資訊，請參閱 [案例：為 DHCP 服務選取 Edge 叢集](#)。

9 (選擇性) 在 Edge 旁，按一下 **設定**，並選取要在其中執行 DHCP 服務的慣用 Edge 節點。

若要選取慣用 Edge 節點，則必須選取 Edge 叢集。您最多可以選取兩個慣用 Edge 節點。下表說明設定 DHCP HA 時的案例。

案例	DHCP HA
未從 Edge 叢集中選取任何慣用 Edge 節點。	已設定 DHCP HA。系統會從 Edge 叢集中的可用節點自動選取一組作用中和待命 Edge 節點。
僅從 Edge 叢集中選取了一個慣用 Edge 節點。	DHCP 伺服器在沒有 HA 支援的情況下執行。
從 Edge 叢集選取了兩個慣用 Edge 節點。	已設定 DHCP HA。您新增的第一個 Edge 節點會成為作用中 Edge，而第二個 Edge 節點則成為待命 Edge。 作用中 Edge 以序號 1 表示，待命 Edge 則以序號 2 表示。 您可以交換作用中和待命 Edge。例如，若要將目前的作用中 Edge 變更為待命，請選取作用中 Edge，然後按一下向下箭頭。或者，您可以選取被動 Edge，然後按一下向上箭頭使其成為作用中。在這兩個情況下，序號會相反。

建立 DHCP 伺服器後，您可以變更 DHCP 伺服器設定檔中的慣用 Edge 節點。但是，此彈性包括特定須知。

例如，假設 DHCP 設定檔中的 Edge 叢集有四個 Edge 節點 N1、N2、N3 和 N4，且您已將 N1 和 N2 設為慣用 Edge 節點。N1 是作用中 Edge，N2 是待命 Edge。DHCP 服務正在作用中的 Edge 節點 N1 上執行，且 DHCP 伺服器已開始將租用指派給區段上的 DHCP 用戶端。

案例	對 DHCP 服務的影響
刪除現有的慣用 Edge 節點 N1 和 N2，並將 N3 和 N4 新增為新的慣用 Edge 節點。	將顯示一則警告訊息，通知您目前的 DHCP 租用將因取代現有的慣用 Edge 而遺失。此動作會導致網路連線中斷。 您可以一次取代一個 Edge 節點，以防止連線中斷。
刪除現有的慣用 Edge N1 和 N2，並將慣用 Edge 節點清單保持空白。	DHCP 伺服器將維持在 Edge 節點 N1 和 N2 上。DHCP 租用會保留下來，且 DHCP 用戶端不會遺失網路連線。
刪除任何一個慣用 Edge，即 N1 或 N2。	刪除任何一個慣用 Edge N1 或 N2 時，另一個 Edge 會繼續為 DHCP 用戶端提供 IP 位址。DHCP 租用會保留下來，且 DHCP 用戶端不會發生網路連線遺失。但會失去 DHCP HA 支援。 若要保留 DHCP HA，您必須將已刪除的 Edge 以 Edge 叢集中的另一個 Edge 節點 (即 N3 或 N4) 取代。

10 (選擇性) 在**標籤**下拉式功能表中，輸入標籤名稱。完成後，按一下**新增項目**。

標籤名稱的長度上限為 256 個字元。

如果詳細目錄中存在標籤，則**標籤**下拉式功能表會顯示所有可用標籤及其範圍的清單。可用標籤的清單包含使用者定義的標籤、系統定義的標籤，以及探索到的標籤。您可以從下拉式功能表中選取現有標籤，並將其新增至 DHCP 設定檔。

11 按一下**儲存**。

後續步驟

將 DHCP 伺服器設定檔連結至區段或閘道，並在每個區段層級設定 DHCP 伺服器設定。

- 將 DHCP 設定檔連結至第 0 層或第 1 層閘道。
- 在區段上設定 DHCP。

新增 DHCP 轉送設定檔

您可以新增 DHCP 轉送設定檔以將 DHCP 流量轉送至遠端 DHCP 伺服器。遠端或外部 DHCP 伺服器可位於 SDDC 之外的任何覆疊區段或實體網路中。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網路 > IP 管理 > DHCP**。
- 3 按一下**新增 DHCP 設定檔**。
- 4 輸入可識別轉送設定檔的唯一名稱。
- 5 在**設定檔類型**下拉式功能表中，選取**DHCP 轉送**。

6 (必要) 輸入遠端 DHCP 伺服器的 IP 位址。

同時支援 DHCPv4 和 DHCPv6 伺服器。您可以輸入多個 IP 位址。遠端 DHCP 伺服器的伺服器 IP 位址不得與 DHCP 範圍和 DHCP 靜態繫結中使用的位址重疊。

伺服器 IP 位址不可為下列任何項目：

- 多點傳播 IP 位址
- 廣播 IP 位址
- 回送 IP 位址
- 未指定的 IP 位址 (全為零的位址)

7 (選擇性) 在**標籤**下拉式功能表中，輸入標籤名稱。完成後，按一下**新增項目**。

標籤名稱的長度上限為 256 個字元。

如果詳細目錄中存在標籤，則**標籤**下拉式功能表會顯示所有可用標籤及其範圍的清單。可用標籤的清單包含使用者定義的標籤、系統定義的標籤，以及探索到的標籤。您可以從下拉式功能表中選取現有標籤，並將其新增至 DHCP 設定檔。

8 按一下**儲存**。

後續步驟

將 DHCP 轉送設定檔連結至閘道，或使用設定檔在區段上設定本機 DHCP 轉送。

- 將 DHCP 設定檔連結至第 0 層或第 1 層閘道。
- 在區段上設定 DHCP。

將 DHCP 設定檔連結至第 0 層或第 1 層閘道

若要使用閘道 DHCP 以進行動態 IP 指派，您必須將 DHCP 伺服器設定檔連結至第 0 層或第 1 層閘道。

僅當連線至該閘道的區段上未設定本機 DHCP 伺服器或 DHCP 轉送時，您才可以將 DHCP 設定檔連結至閘道。如果區段上存在本機 DHCP 伺服器或 DHCP 轉送，則當您嘗試將 DHCP 設定檔連結至閘道時，UI 會擲回錯誤。您必須將區段與閘道中斷連線，然後將 DHCP 設定檔連結至閘道。

必要條件

已在網路中新增 DHCP 伺服器設定檔。

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 移至**網路 > 第 0 層閘道**或**網路 > 第 1 層閘道**。
- 3 編輯適當的閘道。
- 4 視您使用的 NSX-T Data Center 版本而定，執行下列其中一項：
 - 在 3.0.2 版中，按一下 **DHCP** 旁的**設定 DHCP 組態**。

- 在 3.0 和 3.0.1 版中，按一下 **IP 位址管理** 旁的 **無動態 IP 配置**。
- 5 在 **類型** 下拉式功能表中，選取 **DHCP 伺服器** 或 **DHCP 轉送**。

備註 如果您將設定檔類型選取為 DHCP 轉送，則組態不會產生任何作用。您必須將 DHCP 轉送設定檔指派給連線至閘道的區段。將 DHCP 轉送設定檔連結至閘道是一種冗餘組態。此功能行為是已知問題。如需將 DHCP 轉送設定檔指派給區段的相關資訊，請按一下此主題〈後續步驟〉一節中的「在區段上設定 DHCP」連結。

- 6 選取要連結至此閘道的 DHCP 伺服器設定檔。
- 7 按一下 **儲存**。

後續步驟

導覽至 **網路 > 區段**。在連線至此閘道的每個區段上，設定 DHCP 設定、靜態繫結和其他 DHCP 選項。

如需詳細步驟，請參閱：

- [在區段上設定 DHCP](#)。
- [在區段上設定 DHCP 靜態繫結](#)。

在閘道 DHCP 伺服器使用中之後，您可以在閘道上檢視 DHCP 伺服器統計資料。在閘道上的 **DHCP** 或 **IP 位址管理** 旁，按一下「**伺服器**」連結。在 **設定 DHCP 組態** 頁面上，按一下 **統計資料**。

閘道 DHCP 伺服器統計資料會顯示在快顯視窗中。

備註 如果您已在閘道連線的區段上設定本機 DHCP 伺服器，則 **設定 DHCP 組態** 頁面上的 **統計資料** 連結不會顯示本機 DHCP 伺服器統計資料。此頁面上僅會顯示閘道 DHCP 統計資料。

案例：為 DHCP 服務選取 Edge 叢集

DHCP 伺服器在 NSX Edge 叢集中的 Edge 節點中以服務 (服務路由器) 形式執行。

未連線至閘道的獨立區段只能使用 DHCP 本機伺服器。連線至閘道的區段可以使用 DHCP 本機伺服器、DHCP 轉送或閘道 DHCP 伺服器。

無論區段是使用 DHCP 本機伺服器或閘道 DHCP 伺服器，DHCP 伺服器一律會在 Edge 叢集的 Edge 傳輸節點中以服務路由器的形式執行。如果區段使用 DHCP 本機伺服器，會在您於 DHCP 設定檔中指定的 Edge 叢集中建立 DHCP 服務。但是，如果區段使用閘道 DHCP 伺服器，則在其中建立 DHCP 服務的 Edge 叢集將取決於下列因素的組合：

- 閘道中是否已指定 Edge 叢集？
- Edge 叢集是否在閘道的 DHCP 設定檔中指定？
- 閘道中和 DHCP 設定檔中的 Edge 叢集相同或不同？
- 第 1 層路由區段是否連線至第 0 層閘道？

下列案例說明如何選取 Edge 叢集來建立 DHCP 服務。

案例 1：獨立區段使用 DHCP 本機伺服器

案例說明：

- 建立了一個 Edge 叢集 (Cluster1)，且具有四個 Edge 節點：N1、N2、N3、N4。
- 在覆疊傳輸區域中新增使用 [無] 連線的區段。
- 區段依預設會使用 DHCP 本機伺服器。

DHCP 伺服器設定檔組態如下所示：

- 設定檔類型：**DHCP 伺服器**
- Edge 叢集：**Cluster1**
- 慣用 Edge：**無**

在此案例中，來自 Cluster1 的任兩個 Edge 節點均會自動配置以建立 DHCP 服務，且會自動設定 DHCP 高可用性 (HA)。Cluster1 中的其中一個 Edge 節點會在主動模式中執行，而另一個 Edge 則在被動模式中執行。

備註

- 如果您在 DHCP 設定檔中選取兩個慣用 Edge 節點，則先新增的 Edge 節點會成為作用中的 Edge。第二個 Edge 節點則採用被動角色。
- 如果您在 DHCP 設定檔中僅選取一個慣用 Edge 節點，則系統不會設定 DHCP HA。

案例 2：第 1 層路由區段在閘道和 DHCP 設定檔中使用閘道 DHCP 和不同的 Edge 叢集

假設您的網路中有兩個 Edge 叢集 (Cluster1 和 Cluster2)。兩個叢集各有四個 Edge 節點：

- Cluster1 Edge 節點：N1、N2、N3、N4
- Cluster2 Edge 節點：N5、N6、N7、N8

案例說明：

- 區段已連線至第 1 層閘道。
- 第 1 層閘道未連線至第 0 層閘道。
- 第 1 層閘道中的 DHCP 伺服器設定檔使用 Cluster1。
- 第 1 層閘道使用 Cluster2。
- 區段已設定為使用閘道 DHCP 伺服器。

第 1 層閘道中的 DHCP 伺服器設定檔具有以下組態：

- 設定檔類型：**DHCP 伺服器**
- Edge 叢集：**Cluster1**
- 慣用 Edge：**N1、N2 (以指定順序新增)**

第 1 層閘道組態如下所示：

- Edge 叢集：**Cluster2**
- 慣用 Edge：**N5、N6** (以指定順序新增)

在此案例中，DHCP 服務會在 Cluster2 的 Edge 節點上執行。由於 Cluster2 包含多個 Edge 節點，因此系統會自動設定 DHCP HA。但是，系統會針對 DHCP HA 忽略閘道上的慣用 Edge N5 和 N6。系統會針對 DHCP HA 隨機自動配置來自 Cluster2 的任兩個節點。

當區段直接連線至第 0 層閘道，且您的網路拓撲中沒有第 1 層閘道時，也適用此案例。

注意 從 NSX-T Data Center 3.0.2 開始，您可以在建立 DHCP 伺服器後，變更閘道 DHCP 伺服器上的 Edge 叢集。但是，此動作會導致指派給 DHCP 用戶端的所有現有 DHCP 租用遺失。

總之，此案例的重點如下所示：

- 當您使用閘道 DHCP 伺服器並在閘道 DHCP 設定檔和第 1 層閘道上設定不同的 Edge 叢集時，系統一律會在閘道的 Edge 叢集中建立 DHCP 服務。
- 系統會針對 DHCP HA 組態隨機配置來自第 1 層閘道 Edge 節點的 Edge 叢集。
- 如果未在第 1 層閘道上指定任何 Edge 叢集，則系統會使用第 1 層閘道 (Cluster1) DHCP 設定檔中的 Edge 叢集來建立 DHCP 服務。

案例 3：第 1 層路由區段在閘道和 DHCP 設定檔中使用本機 DHCP 伺服器和不同的 Edge 叢集

在此案例中，區段會連線至第 1 層閘道，但您在區段上使用本機 DHCP 伺服器。假設您的網路中有三個 Edge 叢集 (Cluster1、Cluster2、Cluster3)。每個叢集各有兩個 Edge 節點。

- Cluster1 Edge 節點：N1、N2
- Cluster2 Edge 節點：N3、N4
- Cluster3 Edge 節點：N5、N6

案例說明：

- 區段已連線至第 1 層閘道。
- 第 1 層閘道已連線至第 0 層閘道 (選用)。
- 閘道上的 DHCP 設定檔會使用 Cluster1。
- 閘道使用 Cluster2。
- 區段已設定為使用 DHCP 本機伺服器。
- 本機 DHCP 伺服器設定檔使用 Cluster3。

閘道上的 DHCP 伺服器設定檔如下所示：

- 設定檔名稱：**ProfileX**
- 設定檔類型：**DHCP 伺服器**

- Edge 叢集：**Cluster1**
- 慣用 Edge：**N1、N2** (以指定順序新增)

第 1 層閘道組態如下所示：

- Edge 叢集：**Cluster2**
- 慣用 Edge：**N3、N4** (以指定順序新增)

本機 DHCP 伺服器的設定檔如下所示：

- 設定檔名稱：**ProfileY**
- 設定檔類型：**DHCP 伺服器**
- Edge 叢集：**Cluster3**
- 慣用 Edge：**N5、N6** (以指定順序新增)

在此案例中，由於區段已設定為使用本機 DHCP 伺服器，因此會忽略已連線的第 1 層閘道中的 Edge 叢集 (Cluster2) 以建立 DHCP 服務。DHCP 服務會在 Cluster3 (N5、N6) 的 Edge 節點中執行。系統也會設定 DHCP HA。N5 成為作用中的 Edge 節點，N6 成為待命 Edge。

如果未在 Cluster3 中設定任何慣用節點，則系統會針對建立 DHCP 服務和設定 DHCP HA，自動配置來自此叢集的任兩個節點。其中一個 Edge 節點會成為作用中 Edge，而另一個節點則成為待命 Edge。如果在 Cluster3 中僅設定一個慣用 Edge 節點，則系統不會設定 DHCP HA。

當區段直接連線至第 0 層閘道，且您的網路拓撲中沒有第 1 層閘道時，也適用此案例。

案例 4：第 1 層路由區段在閘道和 DHCP 設定檔中使用閘道 DHCP 和相同的 Edge 叢集

考慮您的網路中有單一 Edge 叢集 (Cluster1)，具有四個 Edge 節點：N1、N2、N3、N4。

案例說明：

- 區段已連線至第 1 層閘道。
- 第 1 層閘道已連線至第 0 層閘道 (選用)
- 閘道上的閘道和 DHCP 設定檔使用相同的 Edge 叢集 (Cluster1)。
- 區段已設定為使用閘道 DHCP 伺服器。

閘道上的 DHCP 伺服器設定檔如下所示：

- 設定檔類型：**DHCP 伺服器**
- Edge 叢集：**Cluster1**
- 慣用 Edge：**N1、N2** (以指定順序新增)

第 1 層閘道組態如下所示：

- Edge 叢集：**Cluster1**

- 慣用 Edge : N3、N4 (以指定順序新增)

在此案例中，當閘道 DHCP 設定檔和閘道使用類似的 Edge 叢集(Cluster1) 時，則會在閘道 DHCP 設定檔的慣用 Edge 節點 N1 和 N2 中建立 DHCP 服務。針對建立 DHCP 服務，系統會忽略您在已連線的第 1 層閘道中指定的慣用 Edge 節點 N3 和 N4。

如果未在 DHCP 設定檔中設定任何慣用 Edge，則會針對建立 DHCP 服務和設定 DHCP HA，自動配置來自 Cluster1 的任兩個節點。其中一個 Edge 節點會成為作用中 Edge，而另一個 Edge 則成為待命 Edge。

總之，此案例的重點如下所示：

- 當您使用閘道 DHCP 伺服器並在 DHCP 設定檔和連線的閘道上指定類似的 Edge 叢集時，則會在 DHCP 設定檔的慣用 Edge 節點中建立 DHCP 服務。
- 系統將忽略已連線閘道中指定的慣用 Edge 節點。

案例 5：第 1 層路由區段已連線至第 0 層閘道，且未在第 1 層閘道上設定 Edge 叢集

在此案例中，區段會連線至第 1 層閘道，而第 1 層閘道會連線至第 0 層閘道。假設您的網路中有三個 Edge 叢集 (Cluster1、Cluster2、Cluster3)。每個叢集各有兩個 Edge 節點。

- Cluster1 Edge 節點：N1、N2
- Cluster2 Edge 節點：N3、N4
- Cluster3 Edge 節點：N5、N6

案例說明：

- 區段已直接連線至第 1 層閘道。
- 第 1 層閘道已連線至第 0 層閘道。
- 已在第 1 層和第 0 層閘道上指定 DHCP 伺服器設定檔。
- 第 1 層閘道上的 DHCP 設定檔使用 Cluster1。
- 第 0 層閘道上的 DHCP 設定檔使用 Cluster2。
- 在第 1 層閘道上未選取任何 Edge 叢集。
- 第 0 層閘道使用 Cluster3。
- 區段已設定為使用閘道 DHCP 伺服器。

在此案例中，由於第 1 層閘道未指定任何 Edge 叢集，因此 NSX-T Data Center 會回復為已連線第 0 層閘道的 Edge 叢集。DHCP 服務會在第 0 層閘道 (Cluster3) 的 Edge 叢集中建立。針對建立 DHCP 服務和設定 DHCP HA，系統會自動配置來自此 Edge 叢集的任兩個 Edge 節點。

總之，此案例的重點如下所示：

- 當第 1 層閘道未指定任何 Edge 叢集，因此 NSX-T Data Center 會回復至已連線第 0 層閘道的 Edge 叢集，以建立 DHCP 服務。

- 如果在第 0 層閘道上未偵測到 Edge 叢集，則會在第 1 層閘道 DHCP 設定檔的 Edge 叢集中建立 DHCP 服務。

案例：在 DHCP 上變更區段連線的影響

儲存使用 DHCP 組態的區段之後，您必須小心變更區段的連線。

僅當區段和閘道屬於相同的傳輸區域時，才允許區段連線變更。

下列案例說明允許或不允許的區段連線變更，以及 DHCP 是否在這些情況下受到影響。

案例 1：將使用閘道 DHCP 伺服器的路由區段移至不同的閘道

假設您已新增一個區段，並將其連線至第 0 層或第 1 層閘道。您已在此區段上設定閘道 DHCP 伺服器、儲存區段，以及連線到此區段的工作負載。DHCP 服務現在已由此區段上的工作負載使用。

之後，您決定將此區段的連線變更為位於相同傳輸區域中的另一個第 0 層或第 1 層閘道。

- 從 NSX-T Data Center 3.0.2 開始，允許此變更。不過，當您儲存區段時會出現資訊訊息警示，指出您變更閘道連線會影響已指派給工作負載的現有 DHCP 租用。
- 在 NSX-T Data Center 3.0 和 3.0.1 中，當區段使用閘道 DHCP 伺服器時，您無法將區段的連線從一個閘道變更為另一個閘道。請在因應措施中使用下列步驟：

因應措施 (僅適用於 3.0 和 3.0.1 版)：

- 1 暫時將現有區段將閘道中斷連線，或刪除區段。只有使用 API 才支援暫時中斷區段的連線。遵循下列步驟：

- a 透過執行下列 GET API 來擷取區段詳細資料：

```
GET https://{NSXManager_IP}/policy/api/v1/infra/segments/{segment-id}
```

將 *segment-id* 取代為您想要與閘道中斷連線之區段的實際識別碼。

- b 請注意，API 輸出中的 `advanced_config` 區段顯示 `connectivity:"ON"`。
- c 將 GET API 的輸出複製到文字檔中，然後將 `connectivity` 編輯為 OFF。在下列 PATCH API 的要求內文中貼上完整的 API 輸出：

```
PATCH https://{NSXManager_IP}/policy/api/v1/infra/segments/{segment-id}
```

- d 執行 PATCH API 以中斷區段的連線。

- 2 新增區段。

- 3 將這個新的區段連線至您選擇的閘道。

案例 2：將使用本機 DHCP 伺服器的路由區段移至或轉送至不同的閘道

假設您已新增一個區段，並將其連線至第 0 層或第 1 層閘道。您已在此區段上設定地區設定本機 DHCP 伺服器或 DHCP 轉送、儲存區段，以及連線到此區段的工作負載。DHCP 服務現在已由此區段上的工作負載使用。

之後，您決定將此區段的連線變更為位於相同傳輸區域中的另一個第 0 層或第 1 層閘道。此變更是受允許的。由於 DHCP 伺服器是區段的本機，因此 DHCP 組態設定，包括範圍、靜態繫結和 DHCP 選項，將保留在區段上。工作負載的 DHCP 租用會保留，且不會中斷網路連線。

將區段移至新的閘道後，您可以繼續更新 DHCP 組態設定和其他區段內容。

- 如果您使用的是 NSX-T Data Center 3.0 或 3.0.1，則在將區段移至不同閘道後，您無法變更路由區段的 DHCP 類型和 DHCP 設定檔。例如，您無法將 DHCP 類型從本機 DHCP 伺服器或 DHCP 轉送變更為閘道 DHCP 伺服器。此外，您無法在區段中選取不同的 DHCP 伺服器設定檔或轉送設定檔。但您可以視需要編輯 DHCP 設定檔的內容。
- 從 3.0.2 版開始，在將區段移至不同閘道後，您可以變更路由區段的 DHCP 類型和 DHCP 設定檔。

案例 3：將使用本機 DHCP 伺服器的獨立區段移至第 0 層或第 1 層閘道

假設您已在網路中新增使用 [無] 連線的區段。您已在此區段上設定本機 DHCP 伺服器、儲存區段，以及連線到此區段的工作負載。DHCP 服務現在已由此區段上的工作負載使用。

之後，您決定將此區段連線到位於相同傳輸區域的第 0 層或第 1 層閘道。此變更是受允許的。由於區段上存在本機 DHCP 伺服器，因此 DHCP 組態設定，包括範圍、靜態繫結和 DHCP 選項，將保留在區段上。工作負載的 DHCP 租用會保留，且不會中斷網路連線。

將區段連線至閘道後，您可以繼續更新 DHCP 組態設定和其他區段內容。但您無法在區段中選取不同的 DHCP 類型和 DHCP 設定檔。例如，您無法將 DHCP 類型從本機 DHCP 伺服器變更為閘道 DHCP 伺服器或 DHCP 轉送。此外，您無法在區段中變更 DHCP 伺服器設定檔。但您可以視需要編輯 DHCP 設定檔的內容。

案例 4：將不使用 DHCP 組態的獨立區段移至第 0 層或第 1 層閘道

假設您已在網路中新增使用 [無] 連線的區段。您尚未在此區段上未設定 DHCP、儲存區段，以及連線到此區段的工作負載。

之後，您決定將此區段連線到位於相同傳輸區域的第 0 層或第 1 層閘道。此變更是受允許的。由於區段上不存在 DHCP 組態，因此在連線至閘道後，區段會自動使用閘道 DHCP 伺服器。連結至此閘道的 DHCP 設定檔會在區段中自動選取。

現在，您可以在區段上指定 DHCP 組態設定，包括範圍、靜態繫結和 DHCP 選項。如有必要，您也可以編輯其他區段內容。但是，您無法將 DHCP 類型從閘道 DHCP 伺服器變更為本機 DHCP 伺服器或 DHCP 轉送。

請記住，您只能在區段上設定閘道 DHCPv4 伺服器。在 NSX-T Data Center 3.0 中，不支援閘道 DHCPv6 伺服器。

案例 5：使用第 0 層或第 1 層連線的區段移至無連線

假設您已在網路中新增對第 0 層或第 1 層閘道的區段。您已在此區段上設定閘道 DHCP 伺服器或 DHCP 轉送、儲存區段，以及連線到此區段的工作負載。DHCP 服務現在已由此區段上的工作負載使用。

之後，您決定將此區段的連線變更為無。此變更是不可允許的。

在此案例中，以下因應措施可協助您：

- 1 暫時將現有區段將閘道中斷連線或刪除區段。
如需暫時將區段從閘道中斷連線的相關資訊，請參閱案例 1。
- 2 新增使用 [無] 連線的新區段。
- 3 請視需要在此獨立區段上設定本機 DHCP 伺服器。

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 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**。

附註：新增 IP 位址集區並從該集區中配置 IP 位址後，就無法刪除該集區。如果您要擴充集區，必須新增新的 IP 範圍。例如，如果現有範圍是 192.168.1.11 - 192.168.1.20，且要擴充成 192.168.1.10 - 192.168.1.30，請新增以下兩個範圍：

- 192.168.1.10 - 192.168.1.10
- 192.168.1.21 - 192.168.1.30

新增 IP 位址區塊

您可以設定 IP 位址區塊供其他元件使用。

程序

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

您可以為 IPv6、VNI (虛擬網路識別碼) 集區、閘道、多點傳播和 BFD (雙向轉送偵測) 設定網路設定。

本章節討論下列主題：

- 設定多點傳播
- 新增 VNI 集區
- 設定閘道設定
- 新增閘道 QoS 設定檔
- 新增 BFD 設定檔

設定多點傳播

您可以在 IPv4 網路的第 0 層閘道上設定多點傳播，以將相同的多點傳播資料傳送至收件者群組。在多點傳播環境中，任何主機 (無論是否為群組的成員) 都可以傳送至群組。但是，只有群組的成員才會收到傳送至該群組的封包。

多點傳播功能具有下列功能與限制：

- 使用 IGMPv2 的 PIM 疏鬆模式。
- NSX-T 上沒有集合點 (RP) 或啟動程序路由器 (BSR) 功能，但可以透過 PIM 啟動程序訊息 (BSM) 學習 RP 資訊。此外，也可以設定靜態 RP。
設定靜態 RP 時，它將充當所有多點傳播群組的 RP (224/4)。如果從 BSM 得知的候選 RP 向候選項通告相同的群組範圍，請優先使用靜態 RP。但是，如果候選的 RP 向候選項通告特定群組或群組範圍，則優先使用它們做為這些群組的 RP。
- 檢查所有多點傳播特定 IP (資料流量的傳送端、BSR、RP) 的反向路徑轉送 (RPF)，會要求存在這些項目的路由。在 NSX-T Data Center 3.0.0 中，不支援透過預設路由的連線。從 NSX-T Data Center 3.0.1 開始，也支援透過預設路由連線。
- RPF 檢查需要使用 IP 位址作為下一個躍點之每個多點傳播特定 IP 的路由。當下一個躍點為介面索引時，不支援透過裝置路由進行連線。
- 僅限第 0 層閘道。
- 僅支援第 0 層閘道上的一個上行。
- 僅支援主動冷備用。

- NSX Edge 叢集可以處於主動-主動式或主動-待命模式。當叢集處於主動-主動式模式時，兩個叢集成員將在主動冷備用模式中執行多點傳播。您可以在每個 Edge 上執行 CLI 命令 `get mcast high-availability role`，以識別參與多點傳播的兩個節點。另請注意，由於主動-主動式叢集對 NSX-T 的單點傳播連線是透過 ECMP 執行的，因此北向 PIM 路由器必須選取符合 PIM 芳鄰的 ECMP 路徑，將 PIM 加入/剪除訊息傳送至 NSX-T。依此方式，它將會選取執行 PIM 的作用中 Edge。
- 東西向多點傳播複寫：最多 4 個 VTEP 區段，以達到最大複寫效率。
- 僅限 ESXi 主機和 NSX Edge (不支援 KVM)。
- 不支援連結至下行區段的第 2 層橋接器。
- 多點傳播不支援 Edge 防火牆服務。
- 不支援多站台 (聯盟)。
- 不支援多 VRF。

多點傳播設定的必要條件

底層網路組態：

- 從您的網路管理員取得多點傳播位址範圍。當您在第 0 層閘道上設定多點傳播時，將使用這項資訊來設定多點傳播複寫範圍 (請參閱[設定多點傳播](#))。
- 在 GENEVE 參與主機連結到的第 2 層交換器上啟用 IGMP 窺探。如果在第 2 層上啟用了 IGMP 窺探，則必須在路由器或第 3 層交換器上啟用 IGMP 查詢器，且必須能夠連線至已啟用多點傳播的網路。

多點傳播設定步驟

- 1 建立 IGMP 設定檔。請參閱[建立 IGMP 設定檔](#)。
- 2 選擇性地建立 PIM 設定檔，以設定靜態集合點 (RP)。請參閱[建立 PIM 設定檔](#)。
- 3 設定第 0 層閘道以支援多點傳播。請參閱[新增第 0 層閘道](#)和[設定多點傳播](#)

建立 IGMP 設定檔

網際網路群組管理通訊協定 (IGMP) 是 IPv4 網路中使用的多點傳播通訊協定。

請注意，報告的 IGMP 窺探逾時是一般查詢逾時的 2 倍。依預設，IGMP 窺探逾時值為 120 秒。在 ESXi 上，預設 IGMP 窺探逾時值為 60 秒。

程序

- 1 從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 > 網路設定**。
- 3 按一下 **多點傳播設定檔索引標籤**。
- 4 按一下 **新增 IGMP 設定檔**。

5 輸入設定檔名稱和下列設定檔詳細資料。

選項	說明
查詢間隔 (秒)	一般查詢訊息之間的時間。值越大，會造成傳送 IGMP 查詢的頻率較低。預設值：30。範圍：1 到 1800。
查詢回應時間上限 (秒)	對成員資格查詢訊息傳送回應前允許的時間上限。預設值：10。範圍：1 到 25。
上次成員查詢間隔 (秒)	群組特定查詢訊息之間的時間上限，包括為了回應離開群組訊息而傳送的那些時間。預設值：10。範圍：1 到 25。
加強性變數	已傳送的 IGMP 查詢訊息數。這有助於減輕繁忙網路中的封包遺失風險。在流量高的網路中，建議使用較大的數字。預設值：2。範圍：1 到 255。

建立 PIM 設定檔

通訊協定獨立多點傳播 (PIM) 是 IP 網路的多點傳播路由通訊協定的集合。它不相依於特定的單點傳播路由通訊協定，並且可以利用任何單點傳播路由通訊協定來填入單點傳播路由表。

此步驟是可選的。僅當您想要設定靜態集合點 (RP) 時才需要此功能。集合點是多點傳播網路網域中的路由器，充當多點傳播共用樹狀結構的共用根目錄。如果已設定靜態 RP，則它優先於從選擇的執行啟動程序路由器 (BSR) 已知的 RP。

程序

- 1 從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 > 網路設定**。
- 3 按一下 **多點傳播設定檔索引** 標籤。
- 4 在 **選取設定檔類型** 下拉式功能表中，選取 **PIM 設定檔**。
- 5 按一下 **新增 PIM 設定檔索引** 標籤。
- 6 輸入設定檔名稱。
- 7 輸入靜態集合點 (RP) 位址

新增 VNI 集區

您可以建立在為第 0 層閘道設定 EVPN 時要使用的 VNI 集區。VNI 集區的值不能重疊。

程序

- 1 從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 > 網路設定**。
- 3 按一下 **VNI 集區索引** 標籤。
- 4 按一下 **新增 VNI 集區**。
- 5 輸入集區的名稱。

- 6 輸入起始值。
值必須介於 75001 和 16777215 之間。
- 7 輸入結束值。
值必須介於 75001 和 16777215 之間。
- 8 按一下 **儲存**。

設定閘道設定

為第 3 層轉送模式和傳輸單元最大值 (MTU) 設定全域組態。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 > 網路設定**。
- 3 按一下 **全域網路組態** 索引標籤。
- 4 按一下 **全域閘道組態** 旁的 **編輯**。
 - a 輸入 **閘道介面 MTU** 的值。
預設值為 1500。
 - b 選取第 3 層轉送模式。
- 5 按一下 **儲存**。

新增閘道 QoS 設定檔

建立第 1 層閘道的 QoS 設定檔，以定義流量速率的限制。您可以指定允許的資訊速率和高載大小，以設定限制。不符合 QoS 原則的任何流量都會被捨棄。您可以針對入口和出口流量以及針對所有流量類型 (單點傳播、BUM、IPv4/IPv6) 設定 QoS 設定檔。您可以選擇為每個第 1 層閘道建立不同的設定檔。

備註 只有在第 1 層閘道上才支援閘道 QoS 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 > 網路設定**。
- 3 按一下 **閘道 QoS 設定檔** 索引標籤。
- 4 按一下 **新增閘道 QoS 設定檔**。
- 5 輸入設定檔的名稱。
- 6 輸入您想要為流量設定的認可頻寬限制。

7 輸入高載大小。對於高載大小，使用下列指導方針。

- B 是高載大小 (以位元組為單位)。
- R 是已認可的速率 (或頻寬) (以 Mbps 為單位)。
- I 是時間間隔 (以毫秒為單位)，用於從 Token 值區重新填入或撤回 Token (以位元組為單位)。使用 NSX Edge CLI 中的 `get dataplane` 命令來擷取時間間隔，`Qos_wakeup_interval_ms`。`Qos_wakeup_interval_ms` 的預設值為 50 毫秒。但是，資料平面會根據 QoS 組態自動調整此值。

高載大小的限制為：

- $B \geq R * 1000,000 * I / 1000 / 8$ ，因為高載大小是每個時間間隔中可重新填入的 Token 數量上限。
- $B \geq R * 1000,000 * 1 / 1000 / 8$ ，因為 I 的最小值為 1 毫秒，請考慮其他限制中資料平面的 CPU 使用率。
- $B \geq \text{MTU of SR port}$ ，因為至少需要在 Token 值區中有 MTU 大小數量的 Token，MTU 大小封包才能傳遞速率限制檢查。

由於高載大小需要滿足所有三個限制，因此，高載大小的設定值將為：

```
Max (R * 1000,000 * I / 1000 / 8, R * 1000,000 * 1 / 1000 / 8, MTU)
```

例如，如果 $R = 100$ Mbps， $I = 50$ 毫秒以及 $MTU = 1500$ ，則

```
B >= max (100 * 1000,000 * 50 / 1000 / 8, 100 * 1000,000 * 1 / 1000 / 8, 1500) = 625000 in bytes
```

8 按一下儲存。

新增 BFD 設定檔

BFD (雙向轉送偵測) 是可偵測轉送路徑故障的通訊協定。您可以為第 0 層靜態路由建立 BFD 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 > 網路設定**。
- 3 按一下 **BFD 設定檔** 索引標籤。
- 4 按一下 **新增 BFD 設定檔**。
- 5 輸入設定檔的名稱。
- 6 輸入活動訊號間隔和宣告無作用倍數的值。
- 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
- 分散式 IDS
- 東西向網路安全性 - 鏈結第三方服務
- 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
- 以時間為基礎的防火牆原則
- 網路自我檢查設定
- 對防火牆進行疑難排解
- 裸機伺服器安全性

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一般的規則之前予以強制執行。

東西向或南北向防火牆是否會在失敗時容錯關閉或容錯開啟取決於防火牆中的最後一個規則。若要確保防火牆在失敗時容錯關閉，請將最後一個規則設定為拒絕或捨棄所有封包。

安全性概觀

安全性概觀儀表板有三個索引標籤：見解、組態和容量。

見解索引標籤會顯示以下項目的詳細資料：

- URL 分析：
 - 已啟用 URL 篩選的閘道數目。
 - 連線到雲端服務的閘道數目，以及與雲端服務的連線是否已啟動。
 - 雲端服務上提供的最新簽章套件，以及哪些閘道是最新的。
 - 前五個 URL 類別的資訊，以及在每個類別中存取的 URL。
- 入侵偵測摘要：

項目	說明
入侵事件總計	將入侵事件的總數顯示為可點按的連結，以及每個嚴重性類別中的數目。如需詳細資訊，請參閱 分散式 IDS 事件 。
依嚴重性的趨勢	顯示依時間的入侵事件數目圖表。
依入侵事件或漏洞嚴重性的前幾大虛擬機器	按一下箭頭以選取顯示的資料。

- 分散式防火牆規則使用率：
 - 身分識別防火牆規則的數目。
 - 第 7 層規則的數目。
 - 運算規則的數目。
 - 結合第 7 層和 IDFW 的規則數目。
- 虛擬機器端點保護的組態摘要。您可以檢視有問題的元件，以及依服務設定檔的虛擬機器分佈。

組態索引標籤具有的可點按連結包含下列數目：

- 分散式韌體原則
- 閘道原則

- 端點原則
- 網路自我檢查 EW 原則
- 網路自我檢查 NS 原則
- 分散式 IDS 原則

您也可以檢視分散式防火牆原則的詳細資料，以及每個類別的計數。

容量索引標籤在 [原則] 視圖中無法使用。

安全性術語

以下詞彙將在整個分散式防火牆中使用。

表 13-1. 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，並套用 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 IDFW 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規則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 在右側按一下**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。
- 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。

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

。

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 - 如需支援的 VMware Tools 版本，請參閱 [VMware 產品互通性對照表](#)。

- 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 允許清單或拒絕清單。如需詳細資訊，請參閱[篩選特定網域 \(FQDN/URL\)](#)。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。

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。

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。之後，每個流量的後續封包都將會傳送到 vDPI 引擎。決定應用程式識別碼後，該資訊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。如果該流量已傳送至 vDPI 引擎，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 允許清單和拒絕清單結合使用。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。

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 上所指定的 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」規則之後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。

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 上所指定的 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

屬性 (應用程式識別碼)	說明	類型
AMQP	進階訊息佇列通訊協定是支援應用程式或組織之間的業務訊息通訊的應用程式層通訊協定	網路
AVAST	透過瀏覽 Avast! Antivirus 下載的 Avast.com 官方網站所產生的流量	Web 服務
AVG	AVG 防毒/安全性軟體下載和更新	檔案傳輸
AVIRA	Avira 防毒/安全性軟體下載和更新	檔案傳輸
BLAST	一種遠端存取通訊協定，將在資料中心壓縮、加密和編碼運算體驗並在 VMware Horizon 桌面平台的任何標準 IP 網路之間進行傳輸。	遠端存取
BDEFENDER	BitDefender 防毒/安全性軟體下載和更新	檔案傳輸
CA_CERT	憑證授權單位 (CA) 核發數位憑證，這些憑證可認證用於訊息加密的公開金鑰的擁有權	網路
CIFS	CIFS (Common Internet File System) 可用來提供對網路上的目錄、檔案、印表機、序列埠和節點之間的其他通訊的共用存取	檔案傳輸
CLDAP	不需連線的輕量型目錄存取通訊協定是一種應用程式通訊協定，用於使用 UDP 透過網際網路通訊協定 (IP) 網路存取和維護分散式目錄資訊服務。	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

屬性 (應用程式識別碼)	說明	類型
KASPRSKY	Kaspersky 防毒/安全性軟體下載和更新	檔案傳輸
KERBEROS	Kerberos 是一種網路驗證通訊協定，旨在透過使用秘密金鑰密碼編譯為用戶端/伺服器應用程式提供強式驗證	網路
LDAP	LDAP (輕量型目錄存取通訊協定) 是用於讀取和編輯 IP 網路上的目錄的通訊協定	資料庫
MAXDB	對 MaxDB SQL Server 進行的 SQL 連線和查詢	資料庫
MCAFEE	McAfee 防毒/安全性軟體下載和更新	檔案傳輸
MSSQL	Microsoft SQL Server 是一個關聯式資料庫。	資料庫
NFS	允許用戶端電腦上的使用者以類似於存取本機儲存區的方式存取網路上的檔案。 備註 NFS 第 4 版並非支援的屬性。	檔案傳輸
NNTP	網際網路應用程式通訊協定，用於在新聞伺服器之間傳輸 Usenet 新聞文章 (netnews) 以及透過終端使用者用戶端應用程式讀取並發佈文章。	檔案傳輸
NTBIOSNS	NetBIOS 名稱服務。若要啟動工作階段或散佈資料包，應用程式必須使用名稱服務登錄其 NetBIOS 名稱	網路
NTP	NTP (網路時間通訊協定) 可用於透過網路同步電腦系統的時鐘	網路
OCSP	OCSP 回應程式，用於確認使用者的私密金鑰尚未破解或撤銷	網路
ORACLE	由 Oracle 公司產生並行銷的物件關聯式資料庫管理系統 (ORDBMS)。	資料庫
PANDA	Panda 安全性防毒/安全性軟體下載和更新。	檔案傳輸
PCOIP	遠端存取通訊協定，將在資料中心壓縮、加密和編碼運算體驗並在任何標準 IP 網路之間進行傳輸。	遠端存取
POP2	POP (郵局通訊協定) 是本機電子郵件用戶端用來從遠端伺服器擷取電子郵件的通訊協定。	郵件
POP3	Microsoft 的 NetBIOS 名稱服務 (NBNS) 實作，是 NetBIOS 電腦名稱的名稱伺服器服務。	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 流程提供額外控制資訊。	串流媒體
RTP	RTP (即時傳輸通訊協定) 主要用來提供即時音訊和視訊	串流媒體
RTSP	RTSP (即時資料流通訊協定) 可用於在端點之間建立和控制媒體工作階段	串流媒體
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

屬性 (應用程式識別碼)	說明	類型
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、防毒特徵碼檔案以及軟體更新。	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
TFTP	TFTP (簡單式檔案傳輸通訊協定) 可用來使用用戶端 (例如 WinAgents TFTP 用戶端) 列出、下載及上傳檔案到 TFTP 伺服器 (例如 SolarWinds TFTP 伺服器)。	檔案傳輸
VNC	用於虛擬網路運算的流量。	遠端存取
WINS	Microsoft 的 NetBIOS 名稱服務 (NBNS) 實作，是 NetBIOS 電腦名稱的名稱伺服器和服務。	網路

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。您可以使用類別來組織安全性原則。

系統會以由左到右 (乙太網路 > 緊急 > 基礎結構 > 環境 > 應用程式) 的順序評估類別，並以由上到下的順序評估類別內的分散式防火牆規則。

表 13-2. 分散式防火牆規則類別

乙太網路	緊急	基礎結構	環境	應用程式
建議在此類別中包含第 2 層規則	建議在此類別中包含隔離和允許規則	建議包含會定義共用服務存取權的規則。例如： <ul style="list-style-type: none"> ■ AD ■ DNS ■ NTP ■ DHCP ■ 備份 ■ 管理伺服器 	建議包含區域之間的規則。例如： <ul style="list-style-type: none"> ■ 生產與開發 ■ PCI 與非 PCI ■ 業務單位間規則 	建議包含以下項目之間的規則： <ul style="list-style-type: none"> ■ 應用程式 ■ 應用程式層 ■ 微服務

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**。

2 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。

3 為組態**命名**。

4 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。

5 按一下**儲存**。

6 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。

7 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。

8 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](#)。

- 9 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。

- 10 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

- 1 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

分散式防火牆會監控虛擬機器上的所有東西向流量。

必要條件

若要受到 DFW 保護，虛擬機器必須將其 vNIC 連線至 NSX 覆疊或 VLAN 區段。

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。若要檢視 IDFW 支援的通訊協定，請參閱[身分識別防火牆支援的組態](#)。

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」規則之後的任何規則都將不會執行。

如需分散式防火牆原則與規則建立的聯盟專屬詳細資料，請參閱[從全域管理程式建立 DFW 原則和規則](#)。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取導覽面板中的**安全性 > 分散式防火牆**。
- 3 確定您是位於正確的預先定義類別，然後按一下**新增原則**。如需類別的詳細資訊，請參閱[分散式防火牆](#)。
- 4 為新的原則區段輸入名稱。
- 5 (選擇性) 使用**套用至**，將原則內的規則套用至選取的群組。依預設，原則的**套用至**欄位會設定為 DFW，而原則規則會套用至所有工作負載。原則層級的**套用至**優先於規則層級的**套用至**。

備註 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。

套用至定義了每個原則的強制執行範圍，主要用於 ESXi 與 KVM 主機上的資源最佳化。這有助於為特定的區域、承租人或應用程式定義針對性的原則，卻不干擾為其他應用程式、承租人與區域定義的其他原則。

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 選取原則區段並按一下**新增規則**，然後輸入規則名稱。9 在**來源**資料行中按一下**編輯圖示**，然後選取規則來源。含有 Active Directory 成員的群組可在 IDFW 規則的來源文字方塊中使用。如需詳細資訊，請參閱[新增群組](#)。

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](#)。

10 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](#)。

支援 IPv4、IPv6 和多點傳播位址。

11 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。12 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 或 TFTP)，每個規則可支援一個內容設定檔。

建立 IDS 規則時不支援內容設定檔。

- 13 按一下**套用**，將內容設定檔套用至規則。
- 14 使用**套用至**，將規則套用至選取的群組。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。如果原則及其包含的規則都對群組設定了**套用至**，則原則層級的**套用至**會優先於規則層級的**套用至**。

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

- 15 在**動作**資料行中，選取動作。

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

- 16 按一下狀態切換按鈕以啟用或停用規則。
- 17 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 <code>/var/log/dfwptlogs.log</code> 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。

- 18 按一下**發佈**。可以新增多個規則，然後一同發佈。
- 19 原則的資料路徑實現狀態與傳輸節點詳細資料會顯示在原則資料表右側。

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/dfwptlogs.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->ff02:0:0:0:0:0:1:2/547
```

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 #) - 對於 TCP 連線，系統會在下列 IP 位址後面指出連線終止的實際原因
- 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 - S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
- 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 #) - 對於 TCP 連線，系統會在下列 IP 位址後面指出連線終止的實際原因
- 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 - S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
- APP_XXX 是探索到的應用程式

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 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。
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 。

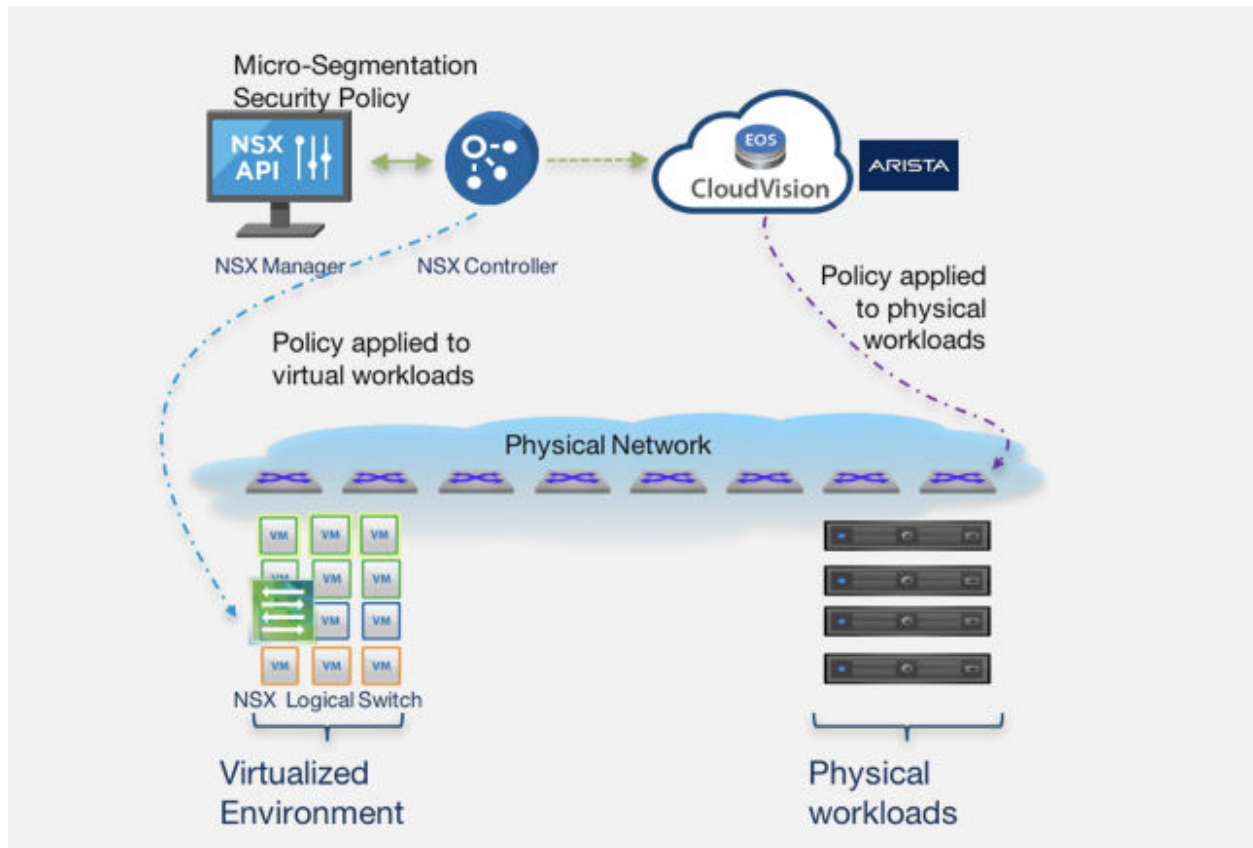
9 按一下發佈。

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。

NSX-T Data Center 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，從而讓安全性管理員和實體網路管理員保有自主性。

NSX-T Data Center 支援與 Arista EOS 4.22.1FX-PCS 和更新版本進行整合。



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 DVPG 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 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。

設定 Arista CVX，使其與 NSX-T Data Center 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 13 章 安全性。例如：

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

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](#)

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。

分散式 IDS

分散式入侵偵測服務 (IDS) 會監控主機上的網路流量是否存在可疑活動。

IDS 會根據已知的惡意指令序列偵測入侵嘗試。IDS 中偵測到的模式稱為簽章。您可以從入侵偵測中排除特定簽章。

備註 請勿在使用分散式負載平衡器的環境中啟用分散式入侵偵測服務 (IDS)。NSX-T Data Center 不支援搭配分散式負載平衡器使用 IDS。

分散式 IDS 組態：

- 1 在主機上啟用 IDS、下載最新的簽章集，以及設定簽章設定。[分散式 IDS 設定和簽章](#)
- 2 建立 IDS 設定檔。[分散式 IDS 設定檔](#)
- 3 建立 IDS 規則。[分散式 IDS 規則](#)
- 4 確認主機上的 IDS 狀態。[驗證主機上的分散式 IDS 狀態](#)

分散式 IDS 設定和簽章

NSX-T 可以透過檢查我們的雲端式服務，自動將簽章套用至您的主機，並更新入侵偵測簽章。

必須啟用分散式防火牆 (DFW)，IDS 才能運作。如果流量由 DFW 規則封鎖，則 IDS 將不會看到流量。

透過切換**已啟用**列，即可在獨立主機上啟用入侵偵測。如果偵測到 VC 叢集，則也可以透過選取叢集並按一下**啟用**，以叢集為基礎啟用 IDS。

簽章

簽章會透過設定檔套用至 IDS 規則。系統會將單一設定檔套用至相符的流量。依預設，NSX Manager 會每日檢查一次新的簽章。新的簽章更新版本會每兩週發佈一次 (含額外的非排程 0 天更新)。有新的更新可用時，頁面上會顯示一個橫幅，其中含有**立即更新**連結。

如果選取**自動更新新的版本**，則在從雲端下載簽章後，會自動將簽章套用至您的主機。如果自動更新已停用，則簽章會停止在所列的版本。除了預設值以外，若要新增另一個版本，請按一下**檢視和變更版本**。目前會維護兩個版本的特徵碼。每當版本認可識別號碼有所變更時，即會下載新版本。

如果已針對 NSX Manager 設定 Proxy 伺服器以存取網際網路，請按一下 **Proxy 設定** 並完成組態。

離線下載和上傳簽章

若要在 NSX Manager 沒有網際網路存取權時，下載並上傳簽章服務包：

- 1 此 API 是在與雲端服務的任何通訊開始之前要呼叫的第一個 API。它會使用用戶端的授權金鑰登錄用戶端，並產生要讓用戶端使用的認證。傳送所有授權，系統將提供必要的權限給您。client_id 是使用者指定的名稱。系統會產生 client_secret，並將其用作驗證 API 的要求。如果用戶端先前已登錄，但沒有 client_id 和 client_secret 的存取權，則用戶端必須使用相同的 API 重新登錄。

```
POST https://api.nsx-sec-prod.com/1.0/auth/register
```

本文：

```
{
  "license_keys":["xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx"],
  "device_type":"NSX-Idps-Offline-Download",
  "client_id": "client_username"
}
```

回應：

```
{"client_id":"client_username",
  "client_secret": "Y54+V/
rCpEm50x5HAUIzH6aXtTq7s97wCA2QqZ8VyrFQjrJih7h0a1ItDQn02T46EJVnSMZWTseragTFScrtIwsiPSX7APQI
C7MxAyZ0BoAWvW2akMxyZKyzbYzjeROb/C2QchehC8GFIFNpwqiAcQjrQHwHGdtX4zTQ="
}
```

- 2 此 API 呼叫會使用 client_id 和 client_secret 來驗證用戶端，並產生要在對 IDS 簽章 API 的請求標頭中使用的授權 Token。Token 在 60 分鐘內有效。如果 Token 到期，則用戶端必須使用 client_id 和 client_secret 進行重新驗證。

```
POST https://api.nsx-sec-prod.com/1.0/auth/authenticate
```

本文：

```
{"client_id":"client_username",
  "client_secret": "Y54+V/
rCpEm50x5HAUIzH6aXtTq7s97wCA2QqZ8VyrFQjrJih7h0a1ItDQn02T46EJVnSMZWTseragTFScrtIwsiPSX7APQI
C7MxAyZ0BoAWvW2akMxyZKyzbYzjeROb/C2QchehC8GFIFNpwqiAcQjrQHwHGdtX4zTQ="
}
```


- 4 導覽至安全性 > 分散式 IDS > 設定。按一下右上角的**上傳 IDS 簽章**。導覽至儲存的簽章 ZIP 檔案，然後上傳檔案。您也可以使用 API 呼叫來上傳簽章 ZIP：

```
POST https://<mgr-ip>/policy/api/v1/infra/settings/firewall/security/intrusion-services/signatures?action=upload_signatures
```

分散式 IDS 設定檔

IDS 設定檔可用來分組簽章，然後可將其套用至選取的應用程式。除了預設設定檔之外，您還可以建立四個自訂設定檔。

簽章可根據簽章的嚴重性分級啟用。分數越高表示與入侵事件相關聯的風險增加。嚴重性取決於下列項目：

- 簽章本身指定的嚴重性
- 簽章中指定的 CVSS (常見漏洞分數系統) 分數
- 與分類類型相關聯的類型-分級

排除項目是根據嚴重性層級設定，並用於停用簽章，從而降低雜訊並提高效能。排除項目用於停用下列情況的簽章：

- 導致誤報
- 有雜訊
- 與受保護的工作負載無關

預設的 IDS 設定檔包含重大嚴重性，因此無法編輯。

程序

- 1 導覽至安全性 > 分散式 IDS > 設定檔。
- 2 輸入設定檔名稱與說明。
- 3 按一下您要包含的一或多個嚴重性。
如需詳細資訊，請參閱 [IDS 嚴重性分級](#)。
- 4 若要排除嚴重性，請按一下**要排除的簽章**下的**選取**。您現在可以檢視和排除該嚴重性層級中包含的簽章。按一下**新增**，以將簽章新增至排除清單。針對每個簽章，會提供下列資訊：

變數	說明
簽章識別碼	參考個別簽章的識別號碼。
詳細資料	描述威脅。
受影響的產品	說明什麼產品容易受到入侵。
攻擊目標	攻擊的目標。
IDS 嚴重性	指示簽章的嚴重性。如需更多詳細資料，請參閱 IDS 嚴重性分級 。

變數	說明
CVSS (常見漏洞分數系統)	CVSS 是一項架構，用於對軟體中安全性漏洞的嚴重性進行評分。0.0-3.9 的 CVSS 基本分數被視為低嚴重性。4.0-6.9 的 CVSS 基本分數為中嚴重性。7.0-10.0 的 CVSS 基本分數為高嚴重性。
CVE (常見漏洞列舉)	常見漏洞列舉 (CVE) 是一種公開已知的資訊安全性漏洞和披露的字典。
類別	攻擊的類型。

5 按一下儲存。

後續步驟

建立 IDS 規則。

IDS 嚴重性分級

簽章嚴重性可協助安全性團隊排列事件優先順序。

分數越高表示與入侵事件相關聯的風險增加。

NSX IDS 嚴重性層級	分類類型 - 分級	分類類型
嚴重	1	<ul style="list-style-type: none"> ■ 嘗試取得使用者權限 ■ 取得使用者權限不成功 ■ 取得使用者權限成功 ■ 嘗試取得管理員權限 ■ 取得管理員權限成功 ■ 偵測到可執行程式碼 ■ 偵測到網路特洛伊木馬程式 ■ Web 應用程式攻擊 ■ 偵測到不當的內容 ■ 潛在的公司隱私權違規 ■ 偵測到鎖定的惡意活動 ■ 偵測到入侵工具組活動 ■ 偵測到觀察到用於 C2 的網域 ■ 偵測到認證竊取成功 ■ 來自 SpiderLabs Research 的新興威脅警示 ■ 來自 SpiderLabs Research 的 RedAlert
高	2	<ul style="list-style-type: none"> ■ 潛在的不良流量 ■ 資訊洩漏 ■ 大規模資訊洩漏 ■ 嘗試拒絕服務 ■ RPC 查詢的解碼 ■ 偵測到可疑檔案名稱 ■ 嘗試使用可疑使用者名稱登入 ■ 偵測到系統呼叫 ■ 使用異常連接埠的用戶端 ■ 拒絕服務攻擊的偵測 ■ 非標準通訊協定或事件的偵測 ■ 存取潛在易受攻擊的 Web 應用程式攻擊 ■ 嘗試以預設使用者名稱和密碼登入 ■ 偵測到裝置正在擷取外部 IP 位址 ■ 偵測到可能有害的程式 ■ 嘗試可能的社交工程 ■ 偵測到加密貨幣採礦活動

NSX IDS 嚴重性層級	分類類型 - 分級	分類類型
中	3	<ul style="list-style-type: none"> ■ 不是可疑流量 ■ 未知的流量 ■ 偵測到可疑的字串 ■ 網路掃描的偵測 ■ 一般通訊協定命令解碼 ■ 其他活動 ■ 一般 ICMP 事件
低	4-9	<ul style="list-style-type: none"> ■ 偵測到 TCP 連線 ■ 非特定的潛在攻擊 ■ 嘗試利用用戶端 Web 應用程式漏洞 ■ 非特定的潛在 Web 應用程式攻擊 ■ 可能是不良想法或錯誤組態的流量 ■ 嘗試入侵管理層級漏洞 ■ 嘗試入侵使用者層級漏洞 ■ 來自 SpiderLabs Research 的以 IP 為基礎警示 ■ 成功入侵根層級漏洞 ■ 作用中後門通道的指示 ■ 蠕蟲傳播 ■ 偵測到特定病毒

分散式 IDS 規則

IDS 規則可用來套用先前建立的設定檔，以選取應用程式和流量。

IDS 規則的建立方式與分散式防火牆 (DFW) 規則相同。首先會建立 IDS 原則或區段，然後建立規則。必須啟用 DFW，並且 DFW 必須允許流量，流量才能傳遞至 IDS 規則。

IDS 規則必須：

- 每個規則指定一個 IDS 設定檔
- 可設定狀態
- 不支援使用第 7 層屬性 (應用程式識別碼)

必須建立具有規則的一或多個原則區段，因為沒有預設規則。建立規則之前，請先建立需要類似規則原則的群組。請參閱[新增群組](#)。

- 1 導覽至[安全性 > IDS > 規則](#)。
- 2 按一下[新增原則](#)以建立原則區段，並為區段指定名稱。

3 按一下齒輪圖示以設定下列原則區段選項：

選項	說明
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	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。 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 。

- 按一下**新增規則**以新增規則，並為規則指定名稱。
- 設定來源/目的地/服務，以用來判定需要 IDS 檢查的流量。IDS 支援任何類型的群組做為來源和目的地。
- 選取要用於比對流量的 **IDS 設定檔**。如需詳細資訊，請參閱[分散式 IDS 設定檔](#)。
- 設定**套用至**，以限制規則的範圍。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。
- 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 和 KVM 主機上的 /var/log/dfwptlogs.log 檔案中。
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。 「傳入/傳出」表示會檢查兩個方向的流量。
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。

- 按一下**發佈**。可以新增多個規則，然後一同發佈。
如需有關建立原則區段和規則的詳細資訊，請參閱[新增分散式防火牆](#)。

分散式 IDS 事件

事件視窗包含過去 14 天的資料。

導覽至[安全性 > 分散式 IDS > 事件](#)以檢視時間入侵事件。

ESXi 主機上的 /var/log/nsx-idps 資料夾中有三個事件記錄檔：

- fast log - 包含 nsx-idps 程序事件的內部記錄，其中包含有限的資訊，且僅用於偵錯用途
- nsx-idps-log - 包含一般的 nsx-idps 程序記錄，其中包含基本資訊和有關程序工作流程的錯誤
- nsx-idps-events.log - 包含有關事件 (所有警示/捨棄/拒絕) 的詳細資訊，並具有 NSX 中繼資料

彩色點表示入侵事件的獨特類型，按一下即可取得詳細資料。點的大小表示出現的入侵事件次數。閃爍點表示攻擊正在進行中。指向某個點可查看攻擊名稱、嘗試次數、第一次發生時間和其他詳細資料。

- 紅色點 - 代表重大嚴重性簽章事件。

- 橙色點 - 代表高嚴重性簽章事件。
- 黃色點 - 代表中嚴重性簽章事件。
- 灰色點 - 代表低嚴重性簽章事件。

特定簽章的所有入侵嘗試都會在其第一次發生時進行分組和繪製。

- 按一下右上角的箭頭，選取時間表。時間表可以介於 24 小時到 14 天之間。
- 依下列各項篩選事件：

篩選準則	說明
攻擊目標	攻擊的目標。
攻擊類型	攻擊的類型，例如特洛伊木馬程式或拒絕服務 (DoS)。
CVSS (常見漏洞分數)	常見的漏洞分數 (根據高於所設定臨界值的分數篩選)。
受影響的產品	有漏洞的產品或 (版本)，即 Windows XP 或 Web_Browsers
虛擬機器名稱	虛擬機器 (以邏輯連接埠為基礎)，其中的入侵流量來自該虛擬機器或由其接收到。

- 按一下事件旁邊的箭頭以檢視詳細資料。

詳細資料	說明
上次偵測時間	這是上次觸發簽章的時間。
詳細資料	觸發的簽章名稱。
受影響的產品	說明什麼產品容易受到入侵。
受影響的虛擬機器	入侵嘗試中涉及的虛擬機器清單。
漏洞詳細資料	如果可用，則會顯示與該漏洞相關聯的 CVE 和 CVSS 分數的連結。
來源	攻擊者的 IP 位址和使用的來源連接埠。
目的地	受害者的 IP 位址和使用的目的地連接埠。
攻擊方向	用戶端-伺服器或伺服器-用戶端。
相關聯的 IDS 規則	已設定 IDS 規則的可點選連結，導致發生此事件。
修訂版本	IDS 簽章的修訂版本編號。
活動	顯示觸發此特定 IDS 簽章的總次數、最近發生的時間和第一次發生的時間。

- 若要檢視入侵歷程記錄，請按一下事件旁邊的箭頭，然後按一下 **檢視入侵歷程記錄**。隨即會開啟一個視窗，其中提供下列詳細資料：

詳細資料	說明
來源 IP	攻擊者的 IP 位址。
來源連接埠	攻擊中使用的來源連接埠。
目的地 IP	受害者的 IP 位址。
目的地連接埠	攻擊中使用的目的地連接埠。

詳細資料	說明
通訊協定	偵測到入侵的流量通訊協定。
偵測到的時間	這是上次觸發簽章的時間。

- 圖表下方顯示的圖形代表在所選時間範圍內發生的事件。您可以放大此圖形上的特定時間範圍，以檢視在該時間範圍內發生的相關事件的簽章詳細資料。

驗證主機上的分散式 IDS 狀態

若要使用 NSX 虛擬應用裝置 CLI，您必須具有 NSX 虛擬應用裝置的 SSH 存取權。每個 NSX 虛擬應用裝置都包含命令列介面 (CLI)。

CLI 中的可檢視模式會根據指派給使用者的角色和權限而有所不同。如果您無法存取介面模式或發出特定命令，請洽詢您的 NSX 管理員。

程序

- 1 對執行先前已部署工作負載所在的計算主機開啟 SSH 工作階段。以 root 身分登入。
- 2 輸入 `nsxcli` 命令以開啟 NSX-T Data Center CLI。
- 3 若要確認此主機上已啟用 IDS，請執行命令：`get ids status`。

輸出範例：

```
localhost> get ids status
NSX IDS Status
-----
status: enabled
uptime: 793756 (9 days 04:29:16)
```

- 4 若要確認這兩個 IDS 設定檔已套用到此主機，請執行命令 `get ids profile`。

```
localhost> get ids profiles
NSX IDS Profiles
-----
Profile count: 2
1. 31c1f26d-1f26-46db-b5ff-e6d3451efd71
2. 65776dba-9906-4207-9eb1-8e7d7fdf3de
```

- 5 若要檢閱 IDS 設定檔 (引擎) 統計資料，包括已載入的規則數目，以及評估的封包和工作階段數目，請執行命令 `get ids engine stats`。

輸出是以每個設定檔為基礎，並顯示為每個設定檔載入的簽章數目，以及評估的封包數。

```
localhost> get ids engine stats
NSX IDS Engine Statistics
-----
uptime: 18 (0 days 00:00:18)

app_layer:
-----
flow:
```



```

http: 10713
tx:
http: 25911
detect:
-----
engines:
alerts: 11129
id: 3
last_reload: 2020-03-17T21:29:39.387087+0000
packets_incoming: 572083
packets_outgoing: 571066
prof-uuid: 53ef4dba-0291-4ea3-96ef-d01259dca2fe
rules_failed: 0
rules_loaded: 11906

tcp:
---
memuse: 20872880
overlap: 50006
reassembly_memuse: 155439408
rst: 23797
sessions: 58811
syn: 89615
synack: 41635

```

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。針對服務產生通知時，NSX-T Data Center 會在 30 秒的時間間隔後通知合作夥伴。
- 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 13-3. 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。
若要建立服務區段：
 - a 按一下 [服務區段] 欄位旁的 + 圖示。
 - b 在 [服務區段] 對話方塊中，按一下**新增服務區段**。
 - c 輸入名稱，從下拉式功能表中選取傳輸區域覆疊，並且如果適用，選取 [套用至閘道] 下的閘道。
 - d 按一下**儲存**。
- 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 將流量分類為必須自我檢查時，它會將流量轉送至一般分散式防火牆，然後再轉送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 確認 NSX Manager 處於**原則**模式。
- 3 選取**安全性 > 東西向安全性 > 網路自我檢查 (E-W) > 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。
- 4 選取服務鏈結。
- 5 若要新增原則，請按一下**發佈**。
- 6 按一下區段上的垂直省略符號 ，然後按一下**新增規則**。
- 7 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](#)。
支援 IPv4、IPv6 和多點傳播位址。
- 8 按一下**儲存**。
- 9 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](#)。
支援 IPv4、IPv6 和多點傳播位址。
- 10 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。
- 11 在 [動作] 文字方塊中，選取**重新導向**以將流量重新導向至服務鏈結，或是選取**不重新導向**，不對流量實施網路自我檢查。
- 12 按一下**發佈**。
- 13 若要還原已發佈的規則，請選取規則，然後按一下**還原**。
- 14 若要新增原則，請按一下 **+** **新增原則**。
- 15 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。
- 16 若要啟用規則，請啟用 [啟用/停用] 圖示，或從功能表中選取規則，然後按一下**啟用 > 啟用規則**。
- 17 啟用或停用規則之後，請按一下**發佈**以強制執行規則。

結果

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

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

解除安裝東西向流量自我檢查服務

解除安裝東西向流量自我檢查服務。

在解除安裝東西向服務的過程中，您需要刪除東西向原則、已部署的合作夥伴服務、服務鏈結、服務設定檔和服務區段。

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 確認 NSX Manager 處於**原則**模式。
- 3 若要刪除原則，請選取**安全性** → **東西向安全性** → **網路自我檢查 (E-W)**。
- 4 選取東西向原則，按一下垂直省略符號，然後按一下**刪除原則**。
- 5 按一下**發佈**。
- 6 若要刪除合作夥伴服務，請選取**系統** → **服務部署**。
- 7 選取合作夥伴服務，按一下垂直省略符號，然後按一下**刪除**。
- 8 按一下**刪除**以完成程序。
- 9 若要刪除東西向服務鏈結，請選取**安全性** → **設定** → **網路自我檢查設定** → **服務鏈結**。
- 10 選取服務鏈結，按一下垂直省略符號，然後按一下**刪除**。
- 11 若要刪除東西向服務設定檔，請選取**安全性** → **設定** → **網路自我檢查設定** → **服務設定檔**。
- 12 選取服務設定檔，按一下垂直省略符號，然後按一下**刪除**。
- 13 若要刪除東西向服務區段，請選取**安全性** → **設定** → **網路自我檢查設定** → **服務區段**。
- 14 選取服務區段，按一下垂直省略符號，然後按一下**刪除**。

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 13-4. 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。

表 13-4. 閘道防火牆規則的類別 (續)

規則類別	用途
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 [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到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到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 通訊協定與註解。

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。

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
```

URL 分析工作流程

URL 分析可讓管理員深入瞭解組織內所存取網站的類型，並瞭解所存取網站的信譽和風險。

- 閘道防火牆上可使用 URL 分析。
- Edge 節點的管理介面 IP 必須具有網際網路連線。
- 必須在 Edge 節點上設定 DNS 伺服器。
- 啟用 URL 分析後，請檢查連線是否已**開啟**，且 URL 資料庫非 0.0.0.0。

設定 URL 分析並分析外部網站的流量：

- 1 確保已在 Edge 節點上設定 DNS。請參閱《NSX-T Data Center 安裝指南》中的〈建立 NSX Edge 傳輸節點〉。
- 2 啟用 URL 分析。[URL 設定](#)
- 3 (選擇性) 設定自訂 URL 分析設定檔。[新增內容設定檔](#)
- 4 [建立第 7 層 DNS 規則](#)
- 5 產生外部網站的流量。
- 6 檢閱 URL 分析儀表板。[URL 分析儀表板](#)

URL 分析儀表板

URL 分析會將網站分類為類別，並根據其網域指派信譽分數。

有超過 80 個預先定義的 URL 類別。網站或網域可以屬於多個類別。例如，www.vmware.com 同時屬於**商業和經濟**類別以及**電腦和網際網路資訊**類別。無法根據 URL 分析自動捨棄或允許流量。

[URL 分析] 儀表板會顯示所有分析 URL 的摘要，依信譽分數和類別分類。僅會分析從第 1 層閘道起始的流量。根據其信譽分數，URL 可分類為下列嚴重性：

嚴重性層級	說明
高風險 (1-20) 為紅色	網站包含惡意連結或裝載的機率很高。
可疑 (21-40) 為橙色	網站包含惡意連結或裝載的機率超過平均。
中等風險 (41-60) 為黃色	通常為良性的網站，展現出一些特性，暗示了安全性風險。
低風險 (61-80) 為灰色	良性的網站，很少展現出使用者面臨安全性風險的特性。
可信網站 (81-100) 為綠色	具有強大安全性做法的知名網站。

左側是 URL 的分佈圖。在頁面底部，有其他有關每個 URI 的詳細資料，包括信譽分數、URL、類別和工作階段計數。

URL 設定

您可以在 NSX Edge 叢集層級啟用 URL 分析。

- 1 導覽至**安全性 > URL 分析 > 設定**。
- 2 在您要開始 URL 分析的 Edge 叢集上切換**啟用**列。NSX Edge 需要存取網際網路，以下載類別和信譽定義。
- 3 按一下**設定**以新增內容設定檔，其中包含 **URL 類別**屬性。URL 分析設定檔可指定要分析的流量類別。如果未建立任何設定檔，則會分析所有流量。如需更多詳細資料，請參閱 [新增內容設定檔](#)。
- 4 針對 DNS 流量設定第 7 層閘道防火牆規則，以便 URL 分析可以分析網域資訊。請參閱 [建立第 7 層 DNS 規則](#)。
- 5 啟用後，您可以針對每個 NSX Edge 節點檢查雲端服務的連線狀態。您也可以確認使用的 URL 資料版本。

備註 如果已在您的環境中啟用 Proxy 伺服器，則不支援擷取 URL 資料版本。NSX Edge 必須與雲端提供者建立具有直接連線，才能擷取 URL 資料版本。

建立第 7 層 DNS 規則

URL 分析依賴第 7 層規則的組態，來擷取周遊 NSX Edge 叢集的 DNS 流量。

必須在所有的第 1 層閘道上 (由您想要分析流量的 NSX Edge 叢集支援) 上設定第 7 層規則。DNS 流量會經過分析，以從 DNS 封包擷取主機名稱和 IP 資訊。接著會使用擷取的資訊來分類和為流量計分。

必要條件

中型 Edge 節點 (或更大型)，或實體機器尺寸 Edge。

程序

- 1 導覽至**安全性 > 閘道防火牆**，並確認您位於**所有共用的規則索引**標籤上。
- 2 按一下**新增原則**以建立原則區段，並為區段指定名稱。
- 3 選取原則旁的核取方塊，然後按一下**新增規則**。
- 4 設定下列選項：

選項	說明
名稱	規則的名稱。
來源	任何
目的地	任何
服務	<ul style="list-style-type: none"> ■ DNS-UDP ■ DNS
設定檔	DNS

選項	說明
套用至	選取已啟用 URL 分析所在的 NSX Edge 叢集支援的所有第 1 層閘道。
動作	允許

5 按一下發佈。

閘道防火牆封包記錄

如果已針對閘道防火牆啟用記錄，則會記錄閘道防火牆封包。

記錄檔為 `/var/log/syslog`。每個記錄訊息都符合 Syslog 格式，且由 Syslog 標頭和防火牆特定的資訊組成。如需 Syslog 的詳細資訊，請參閱[記錄訊息和錯誤碼](#)。

記錄訊息的防火牆特定部分具有下列欄位：

欄位	備註
<VRF ID 和介面 UUID>	您可以透過執行 CLI 命令來取得關於介面的此資訊。例如： <pre>edge-1> get firewall interfaces Interface : 55f1af2f-4875-44e9-b0e0-59132ad7753d Type : UPLINK Sync enabled : true Name : Uplink_40_1 VRF ID : 1 ...</pre>
位址家族	可能的值：INET、INET6
原因	可能的值： <ul style="list-style-type: none"> ■ match：封包符合規則。 ■ fragment：位於第一個片段之後的片段。 ■ short：封包太短 (例如，沒有 IP 標頭或 TCP/UDP 標頭)。 ■ normalize：沒有正確標頭或裝載的格式錯誤封包。 ■ memory：資料路徑記憶體不足。 ■ ip-option：存在無效的 IP 選項。 ■ TERM：已終止連線。
動作	可能的值： <ul style="list-style-type: none"> ■ PASS：接受封包。 ■ DROP：捨棄封包。 ■ NAT：SNAT ■ RDR：DNAT ■ PBR：服務插入。 ■ LB：負載平衡器。
規則識別碼	防火牆規則識別碼。
方向	可能的值：IN、OUT
封包長度	以位址為單位的長度。
通訊協定	可能的值：TCP、UDP 或 PROTO (通訊協定號碼)

欄位	備註
來源 IP 位址和連接埠	對於 SNAT，這是轉譯之前的位址。
目的地 IP 位址和連接埠	對於 DNAT，這是轉譯之前的位址。

TCP 的閘道防火牆記錄訊息範例：

```
<181>1 2020-09-21T22:14:12.080427+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match PASS 1005 OUT 60 TCP 1.1.1.10/45120-
>91.189.92.38/443 S

<181>1 2020-09-21T22:14:19.963758+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET TERM PASS 1005 OUT TCP 1.1.1.10/45120-
>91.189.92.38/443
```

UDP 的閘道防火牆記錄訊息範例：

```
<181>1 2020-09-21T22:05:05.686346+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match PASS 1005 IN 328 UDP 40.40.40.10/60613-
>1.1.1.10/42917

<181>1 2020-09-21T22:05:48.301116+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET TERM PASS 1005 IN UDP 40.40.40.10/60613-
>1.1.1.10/42917
```

PROTO 的閘道防火牆記錄訊息範例：

```
<181>1 2020-09-21T21:54:38.047682+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match PASS 1005 IN 84 PROTO 1 40.40.40.10-
>1.1.1.10

<181>1 2020-09-21T21:54:45.036957+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET TERM PASS 1005 IN PROTO 1 40.40.40.10->1.1.1.10
```

SNAT 的閘道防火牆記錄訊息範例：

```
<181>1 2020-09-21T22:57:24.203037+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match PASS 1005 OUT 60 TCP 1.1.2.10/49974-
>40.40.40.10/22 S

<181>1 2020-09-21T22:57:24.203615+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match NAT 536870914 OUT 60 TCP 2.2.2.10/37305-
OR 1.1.2.10/49974->40.40.40.10/22 S
```

```
<181>1 2020-09-21T22:57:32.125757+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET TERM NAT 536870914 OUT TCP 2.2.2.10/37305-OR
40.40.40.10/22->1.1.2.10/49974
```

DNAT 的閘道防火牆記錄訊息範例：

```
<181>1 2020-09-21T22:49:00.978192+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET reason-match RDR 536870913 IN 60 TCP
40.40.40.10/40082->10.10.10.1/22-OR 1.1.1.10/22 S
```

```
<181>1 2020-09-21T22:50:01.915154+00:00 lur-svc.nsxedge-ob-16404613-1-gdefw NSX 2802 FIREWALL
[nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallpkt" level="INFO"] <1
55f1af2f487544e9:b0e059132ad7753d> INET TERM RDR 536870913 IN TCP 40.40.40.10/40082-
>10.10.10.1/22-OR 1.1.1.10/22
```

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 13-5. 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-T Data Center 使用者介面
針對南北向流量新增重新導向規則	管理員	API 和 NSX-T Data Center 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，您必須在 NSX-T 傳輸節點上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**系統 > 服務部署 > 部署**。
- 3 從 [合作夥伴服務] 下拉式功能表中，選取必須部署的服務。
- 4 按一下**部署服務**。輸入詳細資料以部署服務。

表 13-6. 合作夥伴服務詳細資料

欄位	說明
服務部署名稱	輸入用於識別服務執行個體的名稱。
部署規格	選取要部署的機器尺寸。
連結點	選取必須部署服務執行個體的第 0 層或第 1 層邏輯路由器。
故障原則	選取 允許 或 封鎖 。
網路	對於 主動備用 類型的部署，請將值設為下列欄位： <ul style="list-style-type: none"> ■ 主要介面網路：要由已部署服務使用的介面。 ■ 主要介面 IP：輸入服務執行個體所用的 IP 位址。 ■ 主要閘道位址：輸入閘道位址。 ■ 主要子網路遮罩：輸入子網路遮罩。 ■ 次要介面網路：主要介面無法使用時，要使用的待命介面。 ■ 次要介面 IP：輸入主要 IP 無法使用時，要使用的待命 IP 的 IP 位址。 ■ 次要閘道位址：輸入主要閘道無法使用時，要使用的待命閘道位址。 ■ 次要子網路遮罩：輸入主要子網路遮罩無法使用時，要使用的待命子網路遮罩。 對於類型為 獨立 的部署，請將值設定為主要介面。
計算管理程式	選取已登錄的 vCenter Server。
資料存放區	選取儲存服務執行個體資料的存放庫。
部署模式	選取 獨立 以在第 0 層或第 1 層邏輯路由器上部署單一服務執行個體。 選取 主動備用 以在第 0 層或第 1 層邏輯路由器上，以主動-待命模式部署幾個服務執行個體。
部署範本	選取要在部署服務執行個體時使用的範本。

- 5 按一下**儲存**。

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 層或第 1 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

針對南北向流量新增重新導向規則。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

設定重新導向規則，以將流量傳送至在第 0 層或第 1 層路由器中插入的第三方服務。

必要條件

- 在 NSX-T 上登錄並部署第三方服務。
- 設定第 0 層或第 1 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**安全性 > 南北向安全性 > 網路自我檢查 (N-S) > 新增原則**。
[原則] 區段類似於 [防火牆] 區段，您可以在其中定義規則來判定流量的流動方式。
- 3 將服務執行個體或服務鏈結的**重新導向至**欄位設為第 0 層或第 1 層邏輯路由器，以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：
 - 對於在第 0 層邏輯路由器插入的服務，選取第 0 層路由器的上行。
 - 對於在第 1 層邏輯路由器插入的服務，您不需要選取任何上行。
- 10 每項規則可以個別啟用。啟用後的規則將會套用以符合規則的流量。
- 11 按一下**進階設定**，以設定流量方向並啟用記錄。
- 12 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。

- 13 按一下**發佈**。
- 14 若要還原已發佈的規則，請選取規則，然後按一下**還原**。
- 15 若要新增原則，請按一下 **+ 新增原則**。
- 16 若要複製原則或規則，請選取原則或規則，然後按一下**複製**。
- 17 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**。
- 18 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。

解除安裝南北向流量自我檢查服務

解除安裝南北向流量自我檢查服務。

刪除針對南北向自我檢查服務部署的原則和合作夥伴服務。

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 確認 NSX Manager 處於**原則**模式。
- 3 若要刪除原則，請選取**安全性** → **南北向安全性** → **網路自我檢查 (N-S)**。
- 4 選取原則，按一下垂直省略符號，然後按一下**刪除原則**。
- 5 按一下**發佈**。
- 6 若要刪除合作夥伴服務，請選取**系統** → **服務部署**。
- 7 選取服務，按一下垂直省略符號，然後按一下**刪除**。

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。

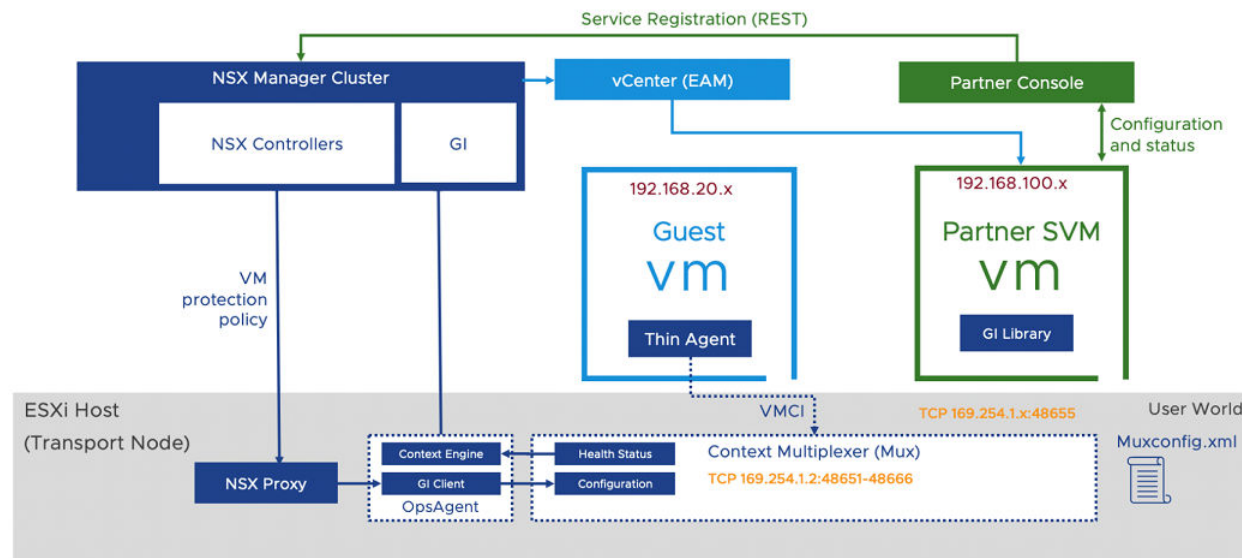
使用 Guest Introspection 平台保護客體虛擬機器端點的好處如下：

- 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。

端點保護架構

瞭解 NSX-T Data Center 中的服務插入與端點保護元件 (Guest Introspection) 架構。

圖 13-1. 端點保護架構



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 13-2. 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 Windows 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 root 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/rhel/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

- d 安裝套件。

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

3 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
```

4 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/centos/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

- d 安裝套件。

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

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/
ubuntu xenial main
```

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 安裝用來自我檢查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 13-7.

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。

表 13-7. (續)

欄位	說明
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 > 端點保護 > 端點保護規則 > 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。將規則套用於虛擬機器群組後，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。將規則套用於虛擬機器群組後，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 EPOSec 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。

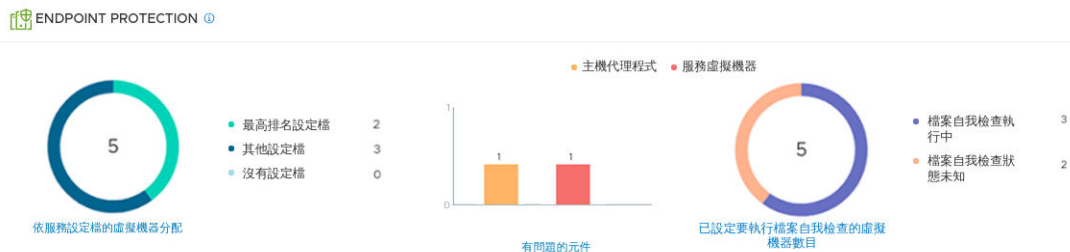
檢視端點保護的組態狀態

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)	警告警示	嚴重警示
Distributed Firewall 規則	100,000	2	0%	70% 100%
系統相關防火牆規則	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。

變更第三方服務虛擬機器

NSX-T Data Center 管理員可以變更或部署服務虛擬機器 (SVM) 的新機器尺寸或版本。

此工作可以透過 UI 或 API 進行。

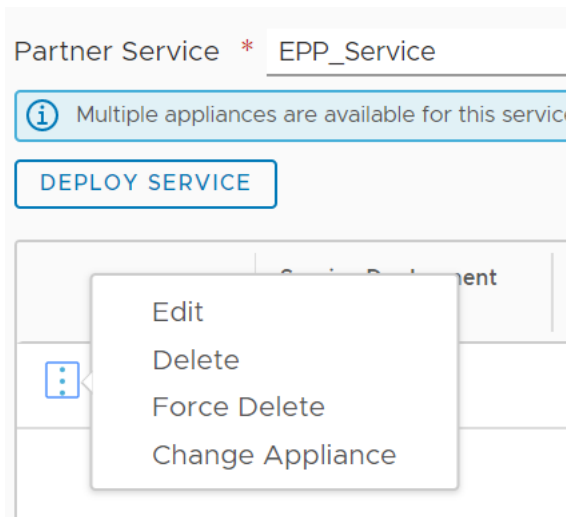
用來變更或升級 SVM 的 API 命令為 /POST https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/{service_id}/service-deployments /<service-deployment-id>?action=upgrade。

必要條件

- 確保合作夥伴已登錄依版本和機器尺寸 (磁碟、vCPU 或 RAM) 區分的多個服務虛擬機器。
- 變更應用裝置之前，請確保 SVM 部署狀態為部署成功。如果 SVM 處於不同的狀態，請移至首頁 → 警示，然後搜尋事件類型 EAM 的任何未處理的警示。嘗試變更為較新的 SVM 之前，請先解決這些項目。
- 在繼續變更應用裝置之前，請確保已滿足部署端點服務或組合作業夥伴服務 (例如，端點保護服務和網路閘道防火牆) 所需的所有必要條件。
- 使用新 SVM 變更現有 SVM 之前，請確保儲存區可供使用。
- 如果存在由現有 SVM 保護的工作負載，請先執行 vMotion 來移轉工作負載，然後變更或部署新的 SVM。

程序

- 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 → 服務部署 → 部署。
- 3 移至服務部署，然後按一下**變更應用裝置**。



- 4 在**變更應用裝置**視窗中，選取您要部署的 SVM 規格，然後按一下**更新**。
- 5 如果部署的服務為「升級失敗」，若無法自動解決此問題，請按一下**解決**。
- 6 按一下**全部解決**。

新 SVM 隨即會部署在 NSX-T 中。

結果

範例：

後續步驟

若要瞭解組合作夥伴服務的執行階段狀態、端點保護服務的健全狀況狀態或部署狀態，請移至**服務執行個體索引標籤**。

將現有 SVM 變更為新 SVM 後，請啟用要保護的客體虛擬機器。

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 13-8. 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 。
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。

表 13-8. ESXi Agency Manager 問題 (續)

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。
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。

表 13-8. ESXi Agency Manager 問題 (續)

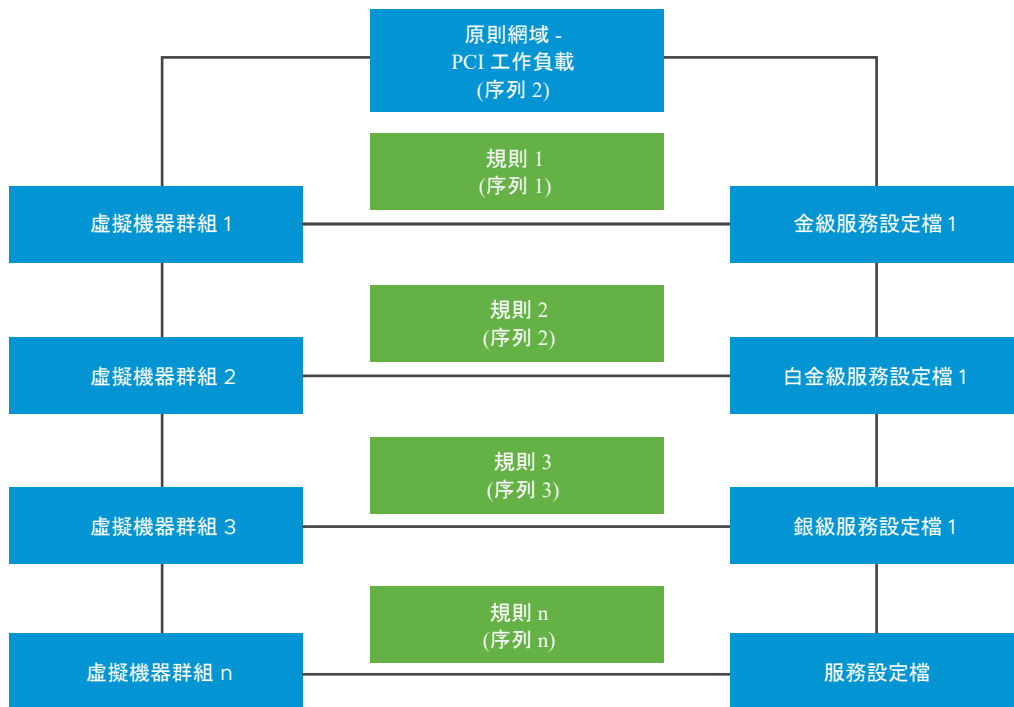
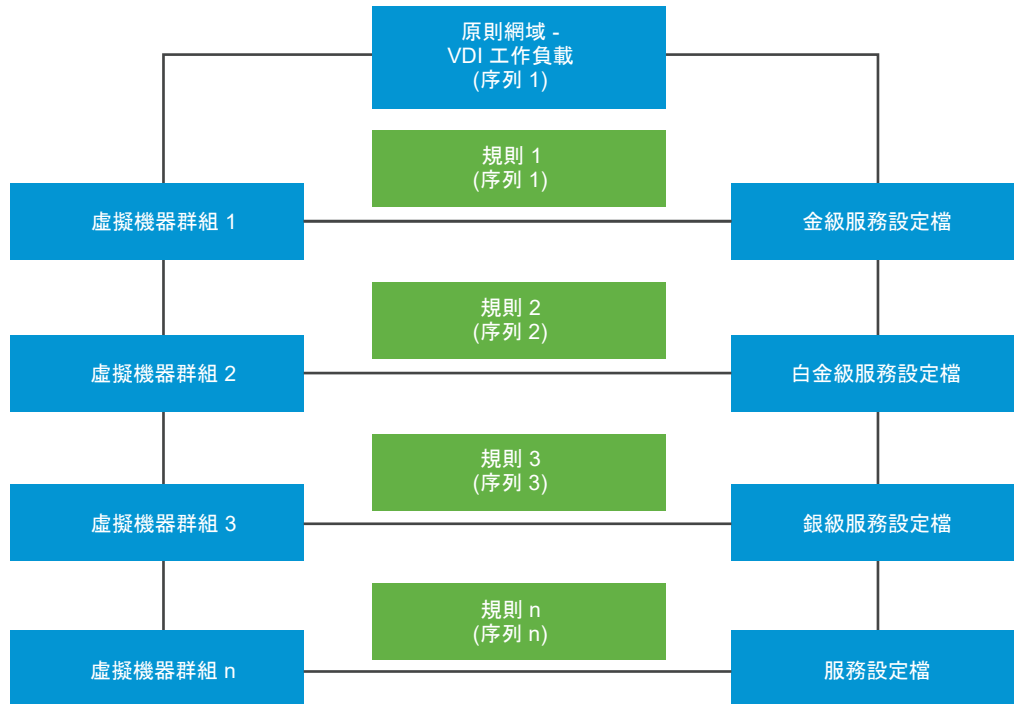
虛擬機器位於錯誤的資料夾中	虛擬機器問題	代理程式虛擬機器應位於指定的代理程式虛擬機器資料夾中，但卻在不同的資料夾中找到。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將代理程式虛擬機器置於指定的資料夾中。
虛擬機器位於錯誤的資源集區中	虛擬機器問題	代理程式虛擬機器應位於指定的代理程式虛擬機器資源集區中，但卻在不同的資源集區中找到。	按一下 解決 。ESXi Agency Manager (EAM) 服務會嘗試將代理程式虛擬機器置於指定的資源集區中。
未部署虛擬機器	代理程式問題	代理程式虛擬機器應部署在主機上，但尚未部署代理程式虛擬機器。ESXi Agent 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 Data Center Policy Manager UI 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 13-9. 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 13-10. 解決原則衝突

案例	預期的端點保護流量	解決方案
<p>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。</p> <p>預期的保護未套用至虛擬機器。</p>	<p>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。</p> <p>將虛擬機器 1 視為屬於群組 1 和群組 2。</p> <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 <p>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。</p>	<p>變更規則 2 的順序編號，使其先於規則 1 執行。</p> <ul style="list-style-type: none"> 在 NSX-T Data Center Policy Manager UI 上，於規則清單中將規則 2 拖曳到規則 1 之前。 使用 NSX-T Data Center Policy Manager API，手動為規則 2 新增較高的順序編號。
<p>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。</p>	<p>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。</p> <p>將虛擬機器 1 視為屬於群組 1 和群組 2。</p> <p>規則 1：群組 1 (按作業系統名稱) 套用金級服務設定檔</p> <p>規則 2：群組 2 (按標籤) 套用金級服務設定檔</p>	<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

- 1 從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 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 13-11. 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 13-12. 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"> 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。 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。 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。 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"> 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。 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。 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。 如果上述步驟均未解決此問題，請連絡 VMware 支援。

表 13-12. 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。如需詳細資訊，請參閱 [預設工作階段計時器值](#)。

ESXi 和 KVM 主機均支援工作階段計時器。

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。預設值為 30 秒。僅限 ESXi 主機。KVM 主機使用 UDP First Packet。
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。僅限 ESXi 主機。KVM 主機使用 ICMP First Packet。

- 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下列項目的群組：區段、區段連接埠、標籤或任何其他以非 IP 為基礎的群組。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 時顯示的預設計時器設定檔不同。對於南北向流量，GFW 預設工作階段計時器會最佳化，依預設，某些計時器值小於可設定的最小值。
- 您可以使用 API 和 UI 變更 DFW 和 GFW 的防火牆工作階段計時器。
- 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 13-13. 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 13-13. 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 快取消除半開狀態時，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	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： TTL 0 - 快取的項目永不到期。 TTL 1 至 3599 - 無效 TTL 3600 到 864000 - 有效 TTL 保留為空白 - 自動 TTL，從 DNS 回應封包設定。 備註 DNS 安全性設定檔的預設 DNS 快取逾時為 24 小時。
套用至	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。 備註 僅一個 DNS 伺服器設定檔會套用至虛擬機器。
標籤	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 。

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。

以時間為基礎的防火牆原則

安全管理員可以使用時間範圍，以針對特定期間限制來自某個來源或前往某個目的地的流量。

時間範圍適用於防火牆原則區段，以及其中的所有規則。每個防火牆原則區段可以有一個時間範圍。可以對多個原則區段套用相同的時間範圍。如果您想要在不同的日期或不同的時間針對不同的網站套用相同的規則，您必須建立多個原則區段。以時間為基礎的規則適用於分散式和閘道防火牆。

必要條件

使用以時間為基礎的規則發佈時，必須在每個傳輸節點上執行網路時間通訊協定 (NTP) 服務。請參閱[設定應用裝置](#)。

部署節點之後，如果 Edge 傳輸節點上的時區發生變更，請重新載入 Edge 節點或重新啟動資料平面，讓以時間為基礎的閘道防火牆原則生效。

建立防火牆原則。

程序

- 1 按一下要有時間範圍之防火牆原則上的時鐘圖示。
時間範圍隨即出現。
- 2 按一下**新增新的時間範圍**，然後輸入**名稱**。
- 3 選取時區：UTC (國際標準時間) 或傳輸節點的本機時間。已啟用 NTP 服務的分散式防火牆僅支援 UTC，在 ESXi 主機上不支援時區組態的變更。
- 4 選取時間範圍的頻率：**每週**或**一次**。
- 5 選取時間範圍生效為星期幾。
當本機時區的整個時間範圍與 UTC 時區在同一天內時，NSX-T Data Center 支援為本機時區設定每週 UTC 時間範圍。例如，您無法以 UTC 設定 PDT 上午 7 點至下午 7 點的時間範圍，這會對應至 UTC 的下午 2 點至隔天上午 2 點。
- 6 選取時間範圍的開始和結束日期，以及該範圍將生效的時間。
- 7 按一下**儲存**。
- 8 按一下要有時間範圍的原則區段旁的核取方塊。然後按一下時鐘圖示。
- 9 選取您要套用的時間範圍，然後按一下**套用**。
- 10 按一下**發佈**。該區段的時鐘圖示會變成綠色。
對於以時間為基礎規則的第一次發佈，會需要時間，而規則強制執行會在 2 分鐘內開始。部署規則後，每次時間範圍的強制執行會瞬間完成。

網路自我檢查設定

本節包含設定網路自我檢查的設定。

新增服務區段

設定東西向網路自我檢查，或想要將封包從 NSX Edge 的上行重新導向至服務鏈結時，請建立服務區段。

必要條件

- 如果要設定東西向服務鏈結，以將封包從 NSX Edge 的上行重新導向至服務鏈結，請建立第 0 層和第 1 層閘道。之後會將區段連線至第 0 層和第 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 按一下 **安全性 > 設定 > 網路自我檢查設定 > 服務區段 > 新增服務區段**。
- 3 按一下 **新增服務區段**。
- 4 在 **名稱** 欄位中，輸入區段的名稱。
- 5 在 **傳輸區域 (覆疊)** 欄位中，選取與區段相關聯的覆疊傳輸區域。
- 6 在 **已連線至** 欄位中，執行下列其中一項作業：
 - 如果要設定東西向網路自我檢查，讓第三方安全性廠商保護客體虛擬機器，請將此欄位保留空白。
 - 如果要設定東西向服務鏈結，以將封包從 NSX Edge 的上行重新導向至服務鏈結，請選取第 0 層或第 1 層閘道。
- 7 按一下 **儲存**。

結果

狀態資料行會顯示服務區段的狀態。

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 > 網路自我檢查設定 > 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 確認 NSX Manager 處於**原則**模式。
- 3 選取**安全性 > 網路自我檢查設定 > 服務鏈結 > 新增鏈結**。
- 4 輸入服務鏈結名稱。
- 5 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。

- 6 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**。
- 7 新增服務鏈結中的第一個設定檔，然後按一下**新增**。
- 8 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。
- 9 按一下**儲存**以完成為服務鏈結新增正向路徑的作業。
- 10 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。
- 11 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。
- 12 按一下**儲存**以完成為服務鏈結新增反向路徑的作業。
- 13 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。

14 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](#)。

對防火牆進行疑難排解

本節提供對防火牆問題進行疑難排解的相關資訊。

在 NSX Manager 上監控防火牆及進行疑難排解

對防火牆進行疑難排解時，需執行幾個步驟。

- 1 檢查防火牆原則實現狀態。請參閱[查看規則實現狀態](#)。
- 2 導覽至**安全性 > 分散式防火牆**或**安全性 > > 閘道防火牆**，然後按一下圖形圖示，以檢查規則叫用統計資料。每 15 分鐘會從所有傳輸節點彙總一次規則層級統計資料。您可以從三個點功能表圖示使用**重設所有規則統計資料**，來重設規則統計資料。
- 3 檢查容量儀表板，以確定組態在 NSX-T Data Center 支援的限制範圍內。容量儀表板可從**安全性 > 安全性概觀 > 容量**存取，請參閱[檢視物件類別的使用量和容量](#)。
- 4 查看**組態限制**，以檢查指定版本支援的組態上限。
- 5 導覽至**邏輯交換器 > 連接埠 > 相關防火牆規則**，以在管理程式模式中查看已推送至資料路徑的個別虛擬機器層級防火牆規則。

您也可以使用 github 中的下列 NSX DFW 協助程式指令碼，取得已設定的防火牆規則和個別虛擬機器防火牆規則的總計。<https://github.com/vmware-samples/nsx-t/blob/master/helper-scripts/DFW/nsx-get-dfw-rules-per-vm.py>

對 ESX 主機上的分散式防火牆進行疑難排解

在 ESX 主機上，請依照下列步驟對 NSX 分散式防火牆 (DFW) 資料路徑問題進行疑難排解。

取得 ESXi 主機上的虛擬機器清單和相關聯的篩選器名稱

這會列出此 ESXi 主機上的所有虛擬機器。請記下「名稱」欄位的值，並在後續命令中使用該值，以取得指定虛擬機器的相關輸出。

```
[root@esxcomp-2a:~] summarize-dvfilter | grep -A 3 vmm
world 1371516 vmm0:PROD-MRS-DB-01 vcUuid:'50 20 92 e1 11 b7 10 d3-56 c5 e0 da 46 87 b5 d2'
  port 67108881 PROD-MRS-DB-01.eth0
  vNic slot 2
    name: nic-1371516-eth0-vmware-sfw.2
--
world 1622816 vmm0:DEV-MRS-DB-01 vcUuid:'50 2d f3 a3 96 a4 f4 94-6e 55 84 85 c1 bd 05 2c'
  port 67108883 DEV-MRS-DB-01.eth0
```

```

vNic slot 2
  name: nic-1622816-eth0-vmware-sfw.2
--
world 7014985 vmm0:PROD-MRS-APP-01 vcUuid:'50 20 9b 5f cd b7 43 de-ab bb 8d 0e f5 bb ca 99'
port 67108895 PROD-MRS-APP-01.eth0
  vNic slot 2
    name: nic-7014985-eth0-vmware-sfw.2
--
world 7022287 vmm0:PROD-MRS-APP-02 vcUuid:'50 20 4a 44 17 fb 21 cf-fb 62 1e a3 d0 3c 7d cf'
port 67108896 PROD-MRS-APP-02.eth0
  vNic slot 2
    name: nic-7022287-eth0-vmware-sfw.2
[root@esxcomp-2a:~]

```

取得套用至虛擬機器的防火牆規則

使用與上方輸出中的虛擬機器相關聯的篩選器名稱，以取得套用至該虛擬機器之 vNIC 的所有防火牆規則

```

[root@esxcomp-2a:~] vsipioctl getrules -f nic-7014985-eth0-vmware-sfw.2
ruleset mainrs {
  # generation number: 0
  # realization time : 2020-12-16T23:41:30
  # PRE_FILTER rules
  rule 5134 at 1 inout protocol any from addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 to
  addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 accept with log tag 'ipv6-app-allow';
  rule 5133 at 2 inout protocol any from any to any accept with log tag 'ipv6-app-deny-
  default';
  rule 5132 at 3 inout inet protocol icmp from any to addrset
  9b14a216-4318-4bb1-94b0-56dfedec6f24 accept with log tag 'icmp-test';
  rule 5132 at 4 inout inet protocol tcp strict from any to addrset
  9b14a216-4318-4bb1-94b0-56dfedec6f24 port 22 accept with log tag 'icmp-test';
  rule 5132 at 5 inout inet protocol ipv6-icmp from any to addrset
  9b14a216-4318-4bb1-94b0-56dfedec6f24 accept with log tag 'icmp-test';
  rule 5130 at 6 inout inet protocol icmp from any to addrset rdst5130 accept with log tag
  'icmp-test-gb-default';
  rule 5130 at 7 inout inet protocol ipv6-icmp from any to addrset rdst5130 accept with log
  tag 'icmp-test-gb-default';
  # FILTER (APP Category) rules
  rule 5102 at 1 inout protocol any from addrset rsrc5102 to addrset d19f38e1-c13e-4fbb-9d6b-
  b6971f251e2d accept;
  rule 5126 at 2 in protocol any from addrset rsrc5127 to addrset d19f38e1-c13e-4fbb-9d6b-
  b6971f251e2d accept;
  rule 5127 at 3 out protocol any from addrset rsrc5127 to addrset d19f38e1-c13e-4fbb-9d6b-
  b6971f251e2d accept;
  rule 5128 at 4 out protocol any from addrset rsrc5128 to addrset rdst5128 accept;
  rule 5129 at 5 in protocol any from addrset rsrc5128 to addrset
  98abd76f-351b-4a4a-857f-1d91416b0798 accept;
  rule 5103 at 6 in protocol any from addrset rsrc5128 to addrset bled4d3d-ab4c-4bab-999b-
  a50642cad495 accept;
  rule 5135 at 7 inout protocol any from any to any with attribute profile
  acf76e7d-400b-438b-966f-8d5c10bebbda accept;
  rule 5135 at 8 inout protocol any from any to any with attribute profile 88dc6bf0-808e-49f6-
  a692-dd0e5cee6ab3 accept;
  rule 5124 at 9 inout protocol any from any to any with attribute profile 8774c654-0f9e-43ad-
  a803-4aa720e590cf accept;

```

```

    rule 5123 at 10 inout protocol any from any to any with attribute profile 13e599b5-
dd2d-420f-8473-9d45f0d324ac accept;
    rule 5125 at 11 inout protocol any from any to any with attribute profile e4be8d7e-
e4ab-4466-8f2e-998445ead95d accept;
    rule 2 at 12 inout protocol any from any to any drop with log tag 'icmp-default-rule';
}

ruleset mainrs_L2 {
  # generation number: 0
  # realization time : 2020-12-16T23:41:30
  # FILTER rules
  rule 1 at 1 inout ethertype any stateless from any to any accept;
}

[root@esxcomp-2a:~]

```

取得每個虛擬機器 VNIC 個別 FW 規則的統計資料

使用上述命令搭配「-s」，以取得與虛擬機器防火牆規則相關聯的防火牆統計資料。

```

[root@esxcomp-2a:~] vsipioctl getrules -f nic-7014985-eth0-vmware-sfw.2 -s
ruleset mainrs {
  # PRE_FILTER rules
rule 5134 at 1, 68 evals, 68 hits, 68 sessions, in 1120 out 1120 pkts, in 113952 out 114184
bytes
rule 5133 at 2, 24 evals, 24 hits, 24 sessions, in 16 out 8 pkts, in 896 out 768 bytes
rule 5132 at 3, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5132 at 4, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5132 at 5, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5130 at 6, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5130 at 7, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
  # FILTER (APP Category) rules
rule 5102 at 1, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5126 at 2, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5127 at 3, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5128 at 4, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5129 at 5, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5103 at 6, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5135 at 7, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5135 at 8, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5124 at 9, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5123 at 10, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 5125 at 11, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
rule 2 at 12, 92 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
}

ruleset mainrs_L2 {
  # FILTER rules
rule 1 at 1, 0 evals, 0 hits, 0 sessions, in 0 out 0 pkts, in 0 out 0 bytes
}

[root@esxcomp-2a:~]

```


取得虛擬機器的防火牆規則中使用的 addrset/群組

防火牆規則會使用來源或目的地中的群組/addrset。此輸出會根據群組組態取得規則中使用的所有 addrset。

```
[root@esxcomp-2a:~] vsipioctl getaddrset -f nic-1371516-eth0-vmware-sfw.2
addrset is shared for this filter
global addrset
addrset 98abd76f-351b-4a4a-857f-1d91416b0798 {
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset 9b14a216-4318-4bb1-94b0-56dfedec6f24 {
ip 10.1.0.0,
ip 10.2.0.2,
ip 10.114.217.26,
ip 172.16.202.2,
ip 172.16.202.22,
ip 192.168.202.2,
ip 2001::172:16:202:2,
ip 2001::172:16:202:22,
mac 00:50:56:a0:0e:25,
mac 00:50:56:a0:26:dc,
mac 00:50:56:a0:2d:c0,
mac 00:50:56:a0:8d:90,
}
addrset b1ed4d3d-ab4c-4bab-999b-a50642cad495 {
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset d19f38e1-c13e-4fbb-9d6b-b6971f251e2d {
ip 3.3.3.3,
ip 4.4.4.4,
}
addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 {
ip 172.16.202.2,
ip 172.16.202.22,
ip 2001::172:16:202:2,
ip 2001::172:16:202:22,
mac 00:50:56:a0:26:dc,
mac 00:50:56:a0:8d:90,
}
addrset rdst5128 {
ip 3.3.3.3,
ip 4.4.4.4,
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset rdst5130 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 100.100.100.100,
}
addrset rsrc5102 {
ip 1.1.1.1,
```

```

ip 1.1.1.2,
}
addrset rsrc5127 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 3.3.3.3,
ip 4.4.4.4,
}
addrset rsrc5128 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 3.3.3.3,
ip 4.4.4.4,
ip 7.7.7.7,
ip 8.8.8.8,
}
local addrset
No address sets.
[root@esxcomp-2a:~]

```

取得每個虛擬機器的作用中防火牆流量

NSX DFW 會維護每個 VNIC 的作用中流量。此輸出會取得通過該 VNIC 的所有作用中流量。

```

[root@esxcomp-2a:~] vsipioctl getflows -f nic-7014985-eth0-vmware-sfw.2
Count retrieved from kernel active=6, inactive=0, drop=0
ecbd448200000001 Active ipv6-icmp 86dd IN 5134 0 0 2001::172:16:202:22 ->
2001::172:16:202:2 128 0 1039376 1039376 9994 9994 tmo 9
ecbd44820000000b9 Active tcp 0800 OUT 5134* 0 0 (est) 172.16.202.2:Unknown(39914) ->
172.16.202.22:ssh(22) 305 EST:EST rtt 21020 retrans 0/0 4409 3725 23 25 tmo 43195
ecbd44820000000ba Active ipv6-icmp 86dd OUT 5134* 0 0 fe80::250:56ff:fea0:8d90 ->
2001::172:16:202:22 135 0 64 72 1 1
ecbd44820000000bb Active igmp 0800 IN 5133* 0 0 (D) 0.0.0.0 -> 224.0.0.1 36 0 1 0 tmo 51
ecbd44820000000bc Active ipv6-icmp 86dd IN 5133* 0 0 (D) fe80::ffff:ffff:ffff:ffff ->
ff02::1 130 0 76 0 1 0 tmo 11
ecbd44820000000bd Active ipv6-icmp 86dd OUT 5133* 0 0 (D) fe80::250:56ff:fea0:8d90 ->
ff02::16 143 0 0 96 0 1 tmo 11
[root@esxcomp-2a:~]

```

取得每個虛擬機器的作用中完整防火牆組態

此輸出會提供每個 VNIC 的完整防火牆組態 - 使用的規則、Addrset 和設定檔。

```

[root@esxcomp-2a:~] vsipioctl getfwconfig -f nic-7014985-eth0-vmware-sfw.2
ruleset mainrs {
# generation number: 0
# realization time : 2020-12-16T23:41:30
# PRE_FILTER rules
rule 5134 at 1 inout protocol any from addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 to
addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 accept with log tag 'ipv6-app-allow';
rule 5133 at 2 inout protocol any from any to any accept with log tag 'ipv6-app-deny-
default';
rule 5132 at 3 inout inet protocol icmp from any to addrset
9b14a216-4318-4bb1-94b0-56dfedec6f24 accept with log tag 'icmp-test';

```

```

rule 5132 at 4 inout inet protocol tcp strict from any to addrset
9b14a216-4318-4bb1-94b0-56dfedec6f24 port 22 accept with log tag 'icmp-test';
rule 5132 at 5 inout inet protocol ipv6-icmp from any to addrset
9b14a216-4318-4bb1-94b0-56dfedec6f24 accept with log tag 'icmp-test';
rule 5130 at 6 inout inet protocol icmp from any to addrset rdst5130 accept with log tag
'icmp-test-gb-default';
rule 5130 at 7 inout inet protocol ipv6-icmp from any to addrset rdst5130 accept with log
tag 'icmp-test-gb-default';
# FILTER (APP Category) rules
rule 5102 at 1 inout protocol any from addrset rsrc5102 to addrset d19f38e1-c13e-4fbb-9d6b-
b6971f251e2d accept;
rule 5126 at 2 in protocol any from addrset rsrc5127 to addrset d19f38e1-c13e-4fbb-9d6b-
b6971f251e2d accept;
rule 5127 at 3 out protocol any from addrset rsrc5127 to addrset d19f38e1-c13e-4fbb-9d6b-
b6971f251e2d accept;
rule 5128 at 4 out protocol any from addrset rsrc5128 to addrset rdst5128 accept;
rule 5129 at 5 in protocol any from addrset rsrc5128 to addrset
98abd76f-351b-4a4a-857f-1d91416b0798 accept;
rule 5103 at 6 in protocol any from addrset rsrc5128 to addrset bled4d3d-ab4c-4bab-999b-
a50642cad495 accept;
rule 5135 at 7 inout protocol any from any to any with attribute profile
acf76e7d-400b-438b-966f-8d5c10bebbda accept;
rule 5135 at 8 inout protocol any from any to any with attribute profile 88dc6bf0-808e-49f6-
a692-dd0e5cee6ab3 accept;
rule 5124 at 9 inout protocol any from any to any with attribute profile 8774c654-0f9e-43ad-
a803-4aa720e590cf accept;
rule 5123 at 10 inout protocol any from any to any with attribute profile 13e599b5-
dd2d-420f-8473-9d45f0d324ac accept;
rule 5125 at 11 inout protocol any from any to any with attribute profile e4be8d7e-
e4ab-4466-8f2e-998445ead95d accept;
rule 2 at 12 inout protocol any from any to any drop with log tag 'icmp-default-rule';
}

ruleset mainrs_L2 {
# generation number: 0
# realization time : 2020-12-16T23:41:30
# FILTER rules
rule 1 at 1 inout ethertype any stateless from any to any accept;
}

addrset is shared for this filter
global addrset
addrset 98abd76f-351b-4a4a-857f-1d91416b0798 {
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset 9b14a216-4318-4bb1-94b0-56dfedec6f24 {
ip 10.1.0.0,
ip 10.2.0.2,
ip 10.114.217.26,
ip 172.16.202.2,
ip 172.16.202.22,
ip 192.168.202.2,
ip 2001::172:16:202:2,
ip 2001::172:16:202:22,

```

```

ip fe80::250:56ff:fea0:26dc,
ip fe80::250:56ff:fea0:8d90,
mac 00:50:56:a0:0e:25,
mac 00:50:56:a0:26:dc,
mac 00:50:56:a0:2d:c0,
mac 00:50:56:a0:8d:90,
}
addrset b1ed4d3d-ab4c-4bab-999b-a50642cad495 {
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset d19f38e1-c13e-4fbb-9d6b-b6971f251e2d {
ip 3.3.3.3,
ip 4.4.4.4,
}
addrset d8e7adac-af3b-4f22-9785-0cc30f0e81b1 {
ip 172.16.202.2,
ip 172.16.202.22,
ip 2001::172:16:202:2,
ip 2001::172:16:202:22,
ip fe80::250:56ff:fea0:26dc,
ip fe80::250:56ff:fea0:8d90,
mac 00:50:56:a0:26:dc,
mac 00:50:56:a0:8d:90,
}
addrset rdst5128 {
ip 3.3.3.3,
ip 4.4.4.4,
ip 7.7.7.7,
ip 8.8.8.8,
}
addrset rdst5130 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 100.100.100.100,
}
addrset rsrc5102 {
ip 1.1.1.1,
ip 1.1.1.2,
}
addrset rsrc5127 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 3.3.3.3,
ip 4.4.4.4,
}
addrset rsrc5128 {
ip 1.1.1.1,
ip 1.1.1.2,
ip 3.3.3.3,
ip 4.4.4.4,
ip 7.7.7.7,
ip 8.8.8.8,
}
local addrset

```

```

No address sets.
containers are shared for this filter
global containers
container 13e599b5-dd2d-420f-8473-9d45f0d324ac {
# generation number: 21208
# realization time : 2020-12-16T23:41:30
FQDN : login\.microsoft\.com(3940c0d7-cbfc-abbb-35b4-786fc4199684),
}
container 8774c654-0f9e-43ad-a803-4aa720e590cf {
# generation number: 21208
# realization time : 2020-12-16T23:41:30
FQDN : outlook\.office365\.com(6e465c1d-7d81-9672-00e1-76ddfc280b8b),
}

container 88dc6bf0-808e-49f6-a692-dd0e5cee6ab3 {
# generation number: 21208
# realization time : 2020-12-16T23:41:30
APP_ID : APP_360ANTIV,
}

container acf76e7d-400b-438b-966f-8d5c10bebbda {
# generation number: 21208
# realization time : 2020-12-16T23:41:30
APP_ID : APP_ACTIVDIR,
}

container e4be8d7e-e4ab-4466-8f2e-998445ead95d {
# generation number: 21208
# realization time : 2020-12-16T23:41:30
FQDN : play\.google\.com(c44ef0fc-a922-eb1b-f155-4f0625271198),
}
local containers
No containers.
[root@esxcomp-2a:~]

```

用於防火牆疑難排解的其他輸出

除了上述命令選項以外，NSX 也允許以其他選項對 ESX 上的 NSX 防火牆資料路徑進行偵錯。請使用下方的說明功能表。

```

[root@esxcomp-2a:~] vsipioctl -h
Usage: help <cmd> <options>
below is a list of available cmd:
  getfilters      : get list of filters
  getfwconfig    : get rules, addrsets and containers of a filter
  getrules       : get rules of a filter
  getaddrsets    : get addrsets of a filter
  getcontainers  : get containers of a filter
  getspoofguard  : get spoofguard setting of a filter
  getflows       : get flows of a filter
  getconncount   : get active connection count
  getconnections : get active connections
  getsismstats   : get service insertion service VM stats
  getsisvctable  : dump service insertion service table

```

```

getsinshtable    : display service insertion nsh table
getsiproxytable  : display service insertion proxy table
getsifailedspis  : get service insertion failed spi table
getsiflowprogtable : get service insertion flow programming table
getsislotid      : get service insertion slot id
getsilbenablestatus: get service insertion load balance enable status
getmeminfo       : get meminfo data
initvsiplogging  : init vsip logger
getfqdnentries   : get fqdn entries
getdnsconfigprofile : get dns config profile for a filter
getfilterstat    : get statistics of a filter
gettimeout       : get connection timeout setting of a filter
getfloodstat     : get flood protection status
getsidcache      : get sid cache of a filter
help             : this help message
run `vsipioctl <cmd> -h' to find out available options of a cmd.
[root@esxcomp-2a:~]

```

用於防火牆疑難排解的 NSX CLI

在 ESXi 上，`nsxcli` 選項可用作 ESX cli 的替代選項 (方法是輸入「`nsxcli`」)，且使用者可使用「`get firewall`」命令樹取得類似上方的輸出。

```

[root@esxcomp-2a:~] nsxcli
esxcomp-2a.dg.vsphere.local>
esxcomp-2a.dg.vsphere.local> get firewall
% Command not found: get firewall

Possible alternatives:
  get firewall <vifuuid> addrsets
  get firewall <vifuuid> profile
  get firewall <vifuuid> ruleset rules
  get firewall exclusion
  get firewall ipfix-containers
  get firewall ipfix-filters
  get firewall ipfix-profiles
  get firewall ipfix-stats
  get firewall packetlog
  get firewall packetlog last <lines>
  get firewall rule-stats
  get firewall rule-stats total
  get firewall status
  get firewall thresholds
  get firewall vifs

esxcomp-2a.dg.vsphere.local> get firewall packetlog last 10
Wed Dec 16 2020 UTC 23:53:55.693
2020-12-16T23:53:23.878Z fd2e9266 INET6 match PASS 5134 OUT 72 ICMP fe80::250:56ff:fea0:8d90-
>fe80::250:56ff:fea0:26dc ipv6-app-allow
2020-12-16T23:53:23.878Z 5f46e9b1 INET6 match PASS 5134 IN 72 ICMP fe80::250:56ff:fea0:8d90-
>fe80::250:56ff:fea0:26dc ipv6-app-allow
2020-12-16T23:53:29.234Z fd2e9266 INET6 TERM 5134 OUT ICMP 135 0 fe80::250:56ff:fea0:8d90-
>2001::172:16:202:22 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:29.234Z 5f46e9b1 INET6 TERM 5134 IN ICMP 135 0 fe80::250:56ff:fea0:8d90-

```

```
>2001::172:16:202:22 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:30.234Z fd2e9266 INET6 TERM 5134 IN ICMP 135 0 fe80::250:56ff:fea0:26dc-
>fe80::250:56ff:fea0:8d90 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:30.234Z 5f46e9b1 INET6 TERM 5134 OUT ICMP 135 0 fe80::250:56ff:fea0:26dc-
>fe80::250:56ff:fea0:8d90 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:35.239Z fd2e9266 INET6 TERM 5134 OUT ICMP 135 0 fe80::250:56ff:fea0:8d90-
>fe80::250:56ff:fea0:26dc 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:35.241Z 5f46e9b1 INET6 TERM 5134 IN ICMP 135 0 fe80::250:56ff:fea0:8d90-
>fe80::250:56ff:fea0:26dc 1/1 72/64 ipv6-app-allow
2020-12-16T23:53:51.876Z fd2e9266 INET6 match PASS 5134 OUT 72 ICMP fe80::250:56ff:fea0:8d90-
>2001::172:16:202:22 ipv6-app-allow
2020-12-16T23:53:51.876Z 5f46e9b1 INET6 match PASS 5134 IN 72 ICMP fe80::250:56ff:fea0:8d90-
>2001::172:16:202:22 ipv6-app-allow
```

```
esxcomp-2a.dg.vsphere.local> get firewall exclusion
```

```
Wed Dec 16 2020 UTC 23:53:57.731
```

```
Firewall Exclusion
```

```
-----
Exclusion count: 7
```

```
00894e3c-8948-4b6b-a4cd-acd3a2c21205
15f077e9-4492-4391-9f63-a99b6c978003
2936443e-128c-4b6d-9fcf-3b2fad778b08
3602f84a-8333-44f3-a3c2-e04fbf5e848f
8149b7ec-553d-48e1-af04-1ee2f5ae266e
d615679c-092e-4bfe-8c17-803fe8b3315d
da619e9d-48a0-4c82-a831-bf580d3bec05
```

```
esxcomp-2a.dg.vsphere.local> get firewall thresholds
```

```
Wed Dec 16 2020 UTC 23:53:59.905
```

```
Firewall Threshold Monitors
```

```
-----
#      Name      Raised  Threshold  CurrValue  CurrSize  MaxSize  PeakEver  EverTime (ago)
1      dfw-cpu      False   60         0          --        --        0         ---:---:--
2      vsip-attr    False   60         3          4 MB     128 MB   3         4d 23:35:06
3      vsip-flow    False   60         0          0 MB     312 MB   0         ---:---:--
4      vsip-fprules False   60         0          0 MB     128 MB   0         ---:---:--
5      vsip-fqdn    False   60         0          0 MB     128 MB   0         ---:---:--
6      vsip-module  False   60         15         153 MB   1024 MB  15        4d 23:35:06
7      vsip-rules   False   60         0          0 MB     512 MB   0         ---:---:--
8      vsip-si      False   60         0          0 MB     128 MB   0         ---:---:--
9      vsip-state   False   60         0          0 MB     384 MB   0         ---:---:--
```

```
esxcomp-2a.dg.vsphere.local>
```

DFW L2 規則顯示未知的 MAC 位址

設定第 2 層防火牆規則並將其中一個 MAC 設定為來源，以及將另一個 MAC 設定為目的地之後，主機上的 `getrules` 命令將目的地 MAC 集合顯示為 `01:00:00:00:00:00/01:00:00:00:00:00`。例如，

```
[root@host1:~] vsipioctl getrules -f nic-1000052822-eth1-vmware-sfw.2
ruleset mainrs {
  # generation number: 0
  # realization time : 2018-07-26T12:42:28
  rule 1039 at 1 inout protocol tcp from any to any port 1521 accept as oracle;
  # internal # rule 1039 at 2 inout protocol tcp from any to any port 1521 accept;
  rule 1039 at 3 inout protocol icmp from any to any accept;
  rule 2 at 4 inout protocol any from any to any accept with log;
}

ruleset mainrs_L2 {
  # generation number: 0
  # realization time : 2018-07-26T12:42:28
  rule 1040 at 1 inout ethertype any stateless from addrset
d83a1523-0d07-4b18-8a5b-77a634540b57 to addrset 9ad9c6ef-c7dd-4682-833d-57097b415e41 accept;
  # internal # rule 1040 at 2 in ethertype any stateless from addrset
d83a1523-0d07-4b18-8a5b-77a634540b57 to addrset 9ad9c6ef-c7dd-4682-833d-57097b415e41 accept;
  # internal # rule 1040 at 3 out ethertype any stateless from addrset
d83a1523-0d07-4b18-8a5b-77a634540b57 to mac 01:00:00:00:00:00/01:00:00:00:00:00 accept;
  rule 1 at 4 inout ethertype any stateless from any to any accept;
}
```

The internal OUT rule with the address `01:00:00:00:00:00/01:00:00:00:00:00` is created by design to handle outbound broadcasting packets and does not indicate a problem.防火牆規則可依照設定運作。

對 KVM 主機上的分散式防火牆進行疑難排解

若要疑難排解 KVM 主機的防火牆問題，您可以查看主機上套用的防火牆規則。

取得 KVM 主機上的 VIF 清單

```
localhost.localdomain> get firewall vifs
***sample output***

                          Firewall VIFs
-----VIF count: 3
1   239140cf-6c6c-464f-96eb-dfb13203171e
2   eb277d27-0d28-4fb0-82ce-f59d86ea5bee
3   afb2aa98-85ee-4bb4-8318-d699fa84c7f0
```

探索套用至特定 VIF 的防火牆規則

依 UUID 指定 VIF (在此範例中為 `239140cf-6c6c-464f-96eb-dfb13203171e`)。

```
localhost.localdomain> get firewall 239140cf-6c6c-464f-96eb-dfb13203171e ruleset rules
***sample output***

                          Firewall Rules
-----
```



```
VIF UUID : 239140cf-6c6c-464f-96eb-dfb13203171e
Ruleset UUID : 7c5838e5-ab75-427d-b4dd-9452e5607805
Rule count : 5345
rule 3073 inout protocol any from any to any profile fbb4b84f-f6c1-40c5-a509-f7c6f81fe7d9
accept with log tag dns;
rule 3072 inout protocol any from any to any profile 6bc09f62-a188-4e36-9708-291af7237039
accept with log tag youtube.com;
rule 3072 inout protocol any from any to any profile 27b9a15b-8071-4d09-a7e8-71eecfca0779
accept with log tag youtube.com;
rule 3075 inout protocol tcp from addrset 81d95211-ab77-4f2d-beaf-3e15b045fb5e to addrset
3d41a802-a899-4464-ba2b-da9240598552 port 5000 accept with log tag portlist1;
rule 3075 inout protocol tcp from addrset 81d95211-ab77-4f2d-beaf-3e15b045fb5e to addrset
3d41a802-a899-4464-ba2b-da9240598552 port 4992/0xffff8 accept with log tag portlist1;
rule 3075 inout protocol tcp from addrset 81d95211-ab77-4f2d-beaf-3e15b045fb5e to addrset
3d41a802-a899-4464-ba2b-da9240598552 port 4864/0xff80 accept with log tag portlist1;
```

取得特定 VIF 中使用的位址集清單

依 UUID 指定 VIF (在此範例中為 239140cf-6c6c-464f-96eb-dfb13203171e)。

```
localhost.localdomain> get firewall 239140cf-6c6c-464f-96eb-dfb13203171e addrsets
***sample output***

                          Firewall Address Sets
-----
Address set count : 11
  UUID : 09f6da50-bcf2-4347-91a7-df00dca003a6
  Address count : 7
    mac 00:50:56:81:9b:2e
    mac 00:0c:29:03:4d:0d
    mac 00:0c:29:03:4d:03
    ip 10.172.177.231
    ip 10.172.177.111
    ip 192.168.1.11
    ip 192.168.2.11
```

取得特定 VIF 中使用的 APPID 和 FQDN 清單

若要檢查 Hypervisor 上的 FQDN 設定檔，請執行命令 `localhost.localdomain> get firewall <vif-id> profile`

尋找在原則 UI 上設定的 URL。

依 UUID 指定 VIF (在此範例中為 239140cf-6c6c-464f-96eb-dfb13203171e)。

```
localhost.localdomain> get firewall 239140cf-6c6c-464f-96eb-dfb13203171e profile
***sample output***

                          Firewall Profiles
-----
Profiles count : 9
  UUID : 87de2b6b-bdf5-49b6-bae2-824f455a21a4
  Attribute count : 2
    FQDN : www\.youtube\.com
    FQDN : .*\.microsoft\.com
```

```

UUID : 68dc8321-5cb5-4cd4-b1d1-14961d71c05e
Attribute count : 1
APP_ID : APP_SSL

```

取得特定 VIF 中使用的 APPID 和 FQDN 清單

依 UUID 指定 VIF (在此範例中為 239140cf-6c6c-464f-96eb-dfb13203171e)。

```

localhost.localdomain> get firewall 239140cf-6c6c-464f-96eb-dfb13203171e profile
***sample output***

                          Firewall Profiles
-----

Profiles count : 9
  UUID : 87de2b6b-bdf5-49b6-bae2-824f455a21a4
  Attribute count : 2
    FQDN : www\.youtube\.com
    FQDN : .*\.microsoft\.com

  UUID : 68dc8321-5cb5-4cd4-b1d1-14961d71c05e
  Attribute count : 1
  APP_ID : APP_SSL

```

探索特定 VIF 的 FQDN

```

localhost.localdomain> get firewall 239140cf-6c6c-464f-96eb-dfb13203171e fqdn
                          Firewall Profile FQDN
-----

Profiles count : 3
  Profile UUID : 87de2b6b-bdf5-49b6-bae2-824f455a21a4
  FQDN count : 2
    FQDN UUID : 37efd4dd-961c-4756-afdd-ec04f44b6c10
    Value : www\.youtube\.com
    IP set : 172.217.6.46

```

透過 Linux Contrack 模組檢查連線。

在此範例中，尋找兩個特定 IP 位址之間經過的流量。

```

ovs-appctl dpctl/dump-contrack -m | grep 192.168.1.15 | grep 192.168.1.16
icmp,orig=(src=192.168.1.15,dst=192.168.1.16,id=7972,type=8,code=0),
reply=(src=192.168.1.16,dst=192.168.1.15,id=7972,type=0,code=0),
id=2901517888,zone=61437,status=SEEN_REPLY|CONFIRMED,mark=2083,labels=0x1f

```

檢查 KVM 主機上的 FQDN 角色和設定檔

您可以建立防火牆規則，以使用 FQDN/URL 篩選特定網域。若要檢查 Hypervisor 上的 FQDN 設定檔，請執行命令 `localhost.localdomain> get firewall <vif-id> profile`。尋找在原則 UI 上設定的 URL。

具有 APP_ID 和 FQDN 項目之已發佈內容設定檔的範例 nsxcli 輸出：

```
localhost.localdomain> get firewall 989bdcf6-c6fc-47cd-86a3-367e552dba32 profile
Firewall Profiles
-----
Profiles count : 3
  UUID : b34b868e-f113-4463-84a6-14736e50168e
  Attribute count : 1
  APP_ID : APP_HTTP
  UUID : c4689750-d5e1-41f5-ba2c-0bfc846ed494
  Attribute count : 1
  FQDN : www\.youtube\.com
  UUID : 77a599db-b2d3-4510-bbff-fa2bb31aceae
  Attribute count : 1
  APP_ID : APP_DNS
localhost.localdomain> get firewall 989bdcf6-c6fc-47cd-86a3-367e552dba32 fqdn
Firewall Profile FQDN
-----
Profiles count : 1
Profile UUID : c4689750-d5e1-41f5-ba2c-0bfc846ed494
FQDN count : 1
FQDN UUID : 1c9d612c-c398-409e-b6f0-f1ec49b778fe
Value : www\.youtube\.com
IP set : 172.217.6.46, 172.217.164.110, 172.217.5.110, 216.58.194.206, 172.217.6.78,
172.217.0.46, 216.58.195.78, 216.58.194.174
```

對閘道防火牆進行疑難排解

利用使用者介面和 API 對閘道防火牆進行疑難排解。

使用 NSX Manager UI 和 API 檢查下列事項：

- 指定的閘道已啟用閘道防火牆。
- 查看指定閘道防火牆原則的實現狀態。UI 會在「防火牆原則」標頭右上方的旁邊顯示實現狀態。
- 查看規則統計資料，以確認是否有任何流量叫用了防火牆原則。
- 啟用規則的記錄，以對原則進行疑難排解。

閘道防火牆會在 NSX Edge 傳輸節點上實作。在下一個步驟中，請在 NSX Edge 節點命令提示字元上使用 nsxcli 命令，進行如下的資料路徑疑難排解。

取得已啟用防火牆之閘道的 UUID

```
EDGE-VM-A01> get logical-router
Logical Router
-----
UUID                                VRF    LR-ID  Name
Type                                Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666  0      0
TUNNEL                                4
8ccc0151-82bd-43d3-a2dd-6a31bf0cd29b  1      1      DR-DC-Tier-0-GW
DISTRIBUTED_ROUTER_TIER0             5
```

```

5a914d04-305f-402e-9d59-e443482c0e15  2      1025  SR-DC-Tier-0-GW
SERVICE_ROUTER_TIER0                    7
495f69d7-c46e-4044-8b40-b053a86d157b  4      2050  SR-PROD-Tier-1
SERVICE_ROUTER_TIER1                    5

```

使用 UUID 取得所有閘道介面

閘道防火牆會根據閘道的上行介面實作。請識別上行介面，並從以下輸出中取得介面識別碼。

```

dc02-nsx-edgevm-1> get logical-router 16f04a64-ef71-4c03-bb5c-253a61752222 interfaces
Wed Dec 16 2020 PST 17:24:13.134
Logical Router
UUID                                VRF      LR-ID  Name                                     Type
16f04a64-ef71-4c03-bb5c-253a61752222  5        2059  SR-PROD-ZONE-GW
SERVICE_ROUTER_TIER1
Interfaces (IPv6 DAD Status A-DAD_Success, F-DAD_Duplicate, T-DAD_Tentative, U-
DAD_Unavailable)
  Interface      : 748d1f17-34d0-555e-8984-3ef9f9367a6c
  Ifuid          : 274
  Mode           : cpu
  Port-type      : cpu

  Interface      : 1bd7ef7f-4f3e-517a-adf0-846d7dff4e24
  Ifuid          : 275
  Mode           : blackhole
  Port-type      : blackhole

  Interface      : 2403a3a4-1bc8-4c9f-bfb0-c16c0b37680f
  Ifuid          : 300
  Mode           : loopback
  Port-type      : loopback
  IP/Mask        : 127.0.0.1/8;::1/128 (NA)

  Interface      : 16cea0ab-c977-4ceb-b00f-3772436ad972          <<<<<<<<<< INTERFACE ID
  Ifuid          : 289
  Name           : DC-02-Tier0-A-DC-02-PROD-Tier-1-t1_lrp
  Fwd-mode       : IPV4_ONLY
  Mode           : lif
  Port-type      : uplink          <<<<<<<<<< Port-type Uplink
Interface
  IP/Mask        :
100.64.96.1/31;fe80::50:56ff:fe56:4455/64 (NA);fc9f:aea3:1afb:d800::2/64 (NA)
  MAC           : 02:50:56:56:44:55
  VNI           : 69633
  Access-VLAN    : untagged
  LS port       : be42fb2e-b10b-499e-a6a9-221da47a4bcc
  Uprf-mode      : NONE
  DAD-mode       : LOOSE
  RA-mode        : SLAAC_DNS_TRHOUGH_RA (M=0, O=0)
  Admin          : up
  Op_state       : up
  MTU            : 1500
  arp_proxy      :

```

取得 GW 介面上的閘道防火牆規則

使用介面識別碼取得在閘道介面上設定的防火牆規則。

```
dc02-nsx-edgevm-2> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972 ruleset rules
Wed Dec 16 2020 PST 17:43:53.047
DNAT rule count: 0

SNAT rule count: 0

Firewall rule count: 6
  Rule ID   : 5137
  Rule      : inout protocol tcp from any to any port {22, 443} accept with log

  Rule ID   : 3113
  Rule      : inout protocol icmp from any to any accept with log

  Rule ID   : 3113
  Rule      : inout protocol ipv6-icmp from any to any accept with log

  Rule ID   : 5136
  Rule      : inout protocol any from any to any accept with log

  Rule ID   : 1002
  Rule      : inout protocol any from any to any accept

  Rule ID   : 1002
  Rule      : inout protocol any stateless from any to any accept

dc02-nsx-edgevm-2>
```

檢查閘道防火牆同步狀態

閘道防火牆會同步 Edge 節點之間的流量狀態，以實現高可用性。閘道防火牆同步組態可使用以下輸出來顯示。

```
dc02-nsx-edgevm-1> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972 sync config
Wed Dec 16 2020 PST 17:30:55.686
HA mode           : secondary-active
Firewall enabled  : true
Sync pending      : false
Bulk sync pending : true           Last status: ok
Failover mode     : non-preemptive
Local VTEP IP     : 172.16.213.125
Peer VTEP IP      : 172.16.213.123
Local context     : 16f04a64-ef71-4c03-bb5c-253a61752222
Peer context      : 16f04a64-ef71-4c03-bb5c-253a61752222

dc02-nsx-edgevm-1>

dc02-nsx-edgevm-2> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972 sync config
Wed Dec 16 2020 PST 17:47:43.683
```

```

HA mode           : primary-passive
Firewall enabled  : true
Sync pending      : false
Bulk sync pending : true           Last status: ok
Failover mode     : non-preemptive
Local VTEP IP     : 172.16.213.123
Peer VTEP IP      : 172.16.213.125
Local context     : 16f04a64-ef71-4c03-bb5c-253a61752222
Peer context      : 16f04a64-ef71-4c03-bb5c-253a61752222

dc02-nsx-edgevm-2>

```

檢查閘道防火牆的作用中流量

閘道防火牆的作用中流量可使用以下命令來顯示。流量狀態會在該閘道的作用中和待命 Edge 節點之間進行同步。以下範例顯示 Edge 節點 1 和 Edge 節點 2 的輸出。

```

dc02-nsx-edgevm-2> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972 connection
Wed Dec 16 2020 PST 17:45:55.889
Connection count: 2
0x0000000330000598: 10.166.130.107:57113 -> 10.114.217.26:22  dir in protocol tcp state
ESTABLISHED:ESTABLISHED fn 5137:0
0x040000033000058f1: 10.166.130.107 -> 10.114.217.26  dir in protocol icmp  fn 5136:0

dc02-nsx-edgevm-2>

dc02-nsx-edgevm-1> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972 connection
Wed Dec 16 2020 PST 17:47:09.980
Connection count: 2
0x0000000330000598: 10.166.130.107:57113 -> 10.114.217.26:22  dir in protocol tcp state
ESTABLISHED:ESTABLISHED fn 5137:0
0x040000033000058f1: 10.166.130.107 -> 10.114.217.26  dir in protocol icmp  fn 3113:0

dc02-nsx-edgevm-1>

```

檢查閘道防火牆記錄

閘道防火牆記錄會提供閘道 VRF 和 GW 介面資訊，以及流量詳細資料。閘道防火牆記錄可從 Edge 存取，也可傳送至 Syslog 伺服器。防火牆記錄會提供邏輯路由器 VRF、防火牆介面識別碼、防火牆規則識別碼，以及流量詳細資料。

```

dc02-nsx-edgevm-1> get log-file syslog | find datapathd.firewallpkt

<181>1 2020-08-04T21:18:25.633996+00:00 dc02-nsx-edgevm-1 NSX 26581 FIREWALL [nsx@6876
comp="nsx-edge" subcomp="datapathd.firewallpkt"
level="INFO"] <8 16cea0abc9774ceb:b00f3772436ad972> INET reason-match PASS 3061 OUT 48 TCP
10.114.217.26/33646->10.114.208.136/22 S

<181>1 2020-08-04T21:18:41.182424+00:00 dc02-nsx-edgevm-1 NSX 26581 FIREWALL [nsx@6876
comp="nsx-edge" subcomp="datapathd.firewallpkt"
level="INFO"] <2 460b362ce1254ebd:98498057bc3b18df> INET TERM PASS 3053 IN TCP
10.166.56.254/60291->10.114.217.26/22

dc02-nsx-edgevm-1>

```

用來偵錯閘道防火牆的其他命令列選項

```
dc02-nsx-edgevm-2> get firewall 16cea0ab-c977-4ceb-b00f-3772436ad972

Possible alternatives:
  get firewall <uuid> addrset name <string>
  get firewall <uuid> addrset sets
  get firewall <uuid> attrset name <string>
  get firewall <uuid> attrset sets
  get firewall <uuid> connection
  get firewall <uuid> connection count
  get firewall <uuid> connection raw
  get firewall <uuid> connection state
  get firewall <uuid> ike policy [<rule-id>]
  get firewall <uuid> interface stats
  get firewall <uuid> ruleset [type <rule-type>] rules [<ruleset-detail>]
  get firewall <uuid> ruleset [type <rule-type>] stats
  get firewall <uuid> sync config
  get firewall <uuid> sync stats
  get firewall <uuid> timeouts
  get firewall [logical-switch <uuid>] interfaces
  get firewall interfaces sync

dc02-nsx-edgevm-2>
```

查看規則實現狀態

您可以使用 UI 和 API 來建立、更新和刪除 DFW 規則。

UI 上的規則實現狀態

您可以導覽至 **安全性 > 分散式防火牆** 或 **安全性閘道防火牆**，然後檢查傳輸節點所報告的規則實現狀態，以確認 DFW 和閘道防火牆原則的規則實現狀態。

規則實現狀態有四個可能的值：

- 成功
- 錯誤
- 進行中
- 未知

透過 API 的規則實現狀態

如果已在相關節點上建立並強制執行規則，您可以透過下列原則管理員 API 來檢查實現狀態。

若要對所有在原則管理員中建立的實體檢查實現狀態，請執行下列命令：GET: `https://<Policy Appliance IP>/policy/api/v1/infra/realized-state/realized-entities`。物件的實現狀態應為「已實現」，而「runtime_status」應為「成功」

例如，在原則管理員層級用來對安全性原則的 <e2d4c010-96c8-11e9-8c0a-f7581ab92530> 檢查實現狀態的查詢為 <f96f27c0-92b8-11e9-96af-b5e746a259e7> is GET https://10.172.121.219/policy/api/v1/infra/realized-state/realized-entities?intent_path=/infra/domains/default/security-policies/f96f27c0-92b8-11e9-96af-b5e746a259e7/rules/e2d4c010-96c8-11e9-8c0a-f7581ab92530

```
{
  "results": [
    {
      "extended_attributes": [],
      "entity_type": "RealizedFirewallRule",
      "intent_paths": [
        "/infra/domains/default/security-policies/1-communication-560"
      ],
      "resource_type": "GenericPolicyRealizedResource",
      "id": "default.1-communication-560.3-communication-110",
      "display_name": "default.1-communication-560.3-communication-110",
      "description": "default.1-communication-560.3-communication-110",
      "path": "/infra/realized-state/enforcement-points/default/firewalls/firewall-sections/default.1-communication-560/firewall-rules/default.1-communication-560.3-communication-110",
      "relative_path": "default.1-communication-560.3-communication-110",
      "parent_path": "/infra/realized-state/enforcement-points/default/firewalls/firewall-sections/default.1-communication-560",
      "intent_reference": [],
      "realization_specific_identifier": "1028",
      "state": "REALIZED",
      "alarms": [],
      "runtime_status": "IN_PROGRESS",
      "_create_user": "system",
      "_create_time": 1561673625030,
      "_last_modified_user": "system",
      "_last_modified_time": 1561674044534,
      "_system_owned": false,
      "_protection": "NOT_PROTECTED",
      "_revision": 6
    }
  ],
  "result_count": 1
}
```

若要檢查 Hypervisor 上的區段中每個規則區段的整體實現狀態，請執行命令：GET https://<policy-mgr>/policy/api/v1/infra/realized-state/status?include_enforced_status=true&intent_path=<Security_policy_path>。

整併狀態有四個可能的值：

- 成功
- 錯誤
- 進行中
- 未知

表 13-14. 整併狀態

傳輸節點 1 整體狀態	傳輸節點 2 整體狀態	整併狀態
錯誤	錯誤	錯誤
錯誤	IN_PROGRESS	錯誤
錯誤	未知	錯誤
IN_PROGRESS	IN_PROGRESS	IN_PROGRESS
IN_PROGRESS	未知	IN_PROGRESS
成功	成功	成功
成功	錯誤	錯誤
成功	IN_PROGRESS	IN_PROGRESS
成功	未知	未知
未知	未知	未知

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 #) - 對於 TCP 連線，系統會在下列 IP 位址後面指出連線終止的實際原因
- 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 - S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
- 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 #) - 對於 TCP 連線，系統會在下列 IP 位址後面指出連線終止的實際原因
- 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 - S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
- APP_XXX 是探索到的應用程式

裸機伺服器安全性

保護在 Windows Server 2016 裸機伺服器上執行的工作負載。

您可以為介於下列項目之間的應用程式或工作負載提供連線和安全性：

- 實體工作負載 (裸機伺服器) 和虛擬工作負載
- 虛擬工作負載和實體工作負載 (裸機伺服器)

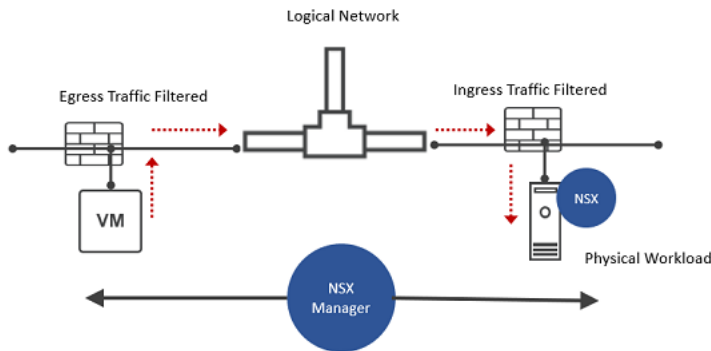
■ 實體工作負載 (裸機伺服器) 和實體工作負載 (裸機伺服器)

工作負載可以位於支援覆蓋或支援 VLAN 的網路上，而工作負載不得在 Windows Server 2016 裸機伺服器的周邊之外。NSX Agent 會隨著組態程序安裝在裸機主機上。在套用 DFW 規則以保護工作負載之前，必須建立 Windows 裸機伺服器、NSX Agent 和 NSX Manager 之應用程式 IP 位址之間的網路連線。

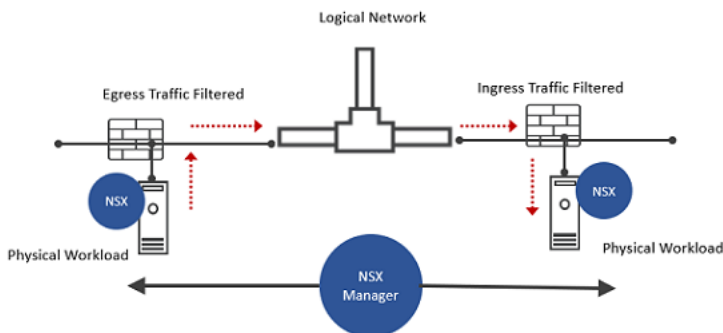
套用 DFW 規則，以在 Windows Server 2016 裸機伺服器和虛擬或實體工作負載上的工作負載之間，保護流經 L2 和 L3 網路的入口和出口流量。

在 Windows 裸機伺服器上篩選入口和出口流量的幾個使用案例。

虛擬和實體裸機工作負載之間的流量



實體裸機工作負載之間的流量



將 DFW 規則套用至 Windows 裸機工作負載之前，請在 Windows Server 上使用 Ansible 指令碼整合 NSX-T。若要在 Windows 裸機伺服器上安裝和整合 NSX-T，請參閱《NSX-T Data Center 安裝指南》中的〈保護在 Windows Server 2016 裸機伺服器上的工作負載〉主題。

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](#)
- [容器](#)
- [公有雲服務](#)
- [實體伺服器](#)
- [標籤](#)

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**。
- 6 選取類型。
選擇包括**第 2 層**和**第 3 層及以上**。
- 7 在**連接埠-通訊協定**中，按一下**新增服務項目**，以新增一或多個服務項目。
對於第 2 層，唯一可用的服務類型為**乙太**。
對於第 3 層及以上版本，可用的服務類型包括 **IP**、**IGMP**、**ICMPv4**、**ICMPv6**、**ALG**、**TCP** 和 **UDP**。
- 8 按一下**服務索引標籤**，以新增一或多個服務。
您新增的任何服務會被視為巢狀服務，因為它包含在您要建立的服務中。建議的最大巢狀層級為 3。三個巢狀層級的範例：服務 A 包含服務 B，服務 B 包含服務 C，而服務 C 包含服務 D。此外，不允許使用循環巢狀。在上述範例中，服務 C 不能包含服務 A 或 B。
- 9 按一下**套用**。
- 10 (選擇性) 新增一或多個標籤。
- 11 (選擇性) 輸入說明。
- 12 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。

備註 如果您使用以 LogicalPort 為基礎的準則在 API 中建立群組，則無法在使用者介面中於 SegmentPort 準則之間使用 AND 運算子來編輯群組。

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](#)。

單一 IP 或 AD 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 IP 和 AD 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。

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。

如果您使用的是 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。

必要條件

如果您使用聯盟，請參閱[NSX 聯盟中的安全性](#)以取得有關組態選項的詳細資料。

備註 如果您使用 NSX 聯盟，則無法從全域管理程式建立群組來包含 AD 使用者群組。

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 如果您要從聯盟的全域管理程式新增群組，請接受預設區域選項，或從下拉式功能表中選取區域。建立含有區域的群組後，即無法編輯區域選取項目。但您可以透過對區域新增或移除位置，來變更區域本身的範圍。您可以先建立自訂區域，然後再建立群組。請參閱[從全域管理程式建立區域](#)。

備註 對於從聯盟環境中全域管理程式新增的群組，選取區域是必要的。如果您未使用全域管理程式，則無法使用此文字方塊。

- 5 (選擇性) 按一下**設定成員**。

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

- **區段連接埠** - 指定標籤、範圍或兩者。
- **區段** - 指定標籤、範圍或兩者。
- **虛擬機器** - 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** - 指定標籤、範圍或兩者。

6 (選擇性) 按一下 **成員** 以選取成員。

可用成員類型為：

- **群組**

備註 如果您使用聯盟，則可以將群組新增為具有較您為從全域管理程式建立之群組選取的區域相同或較小範圍的成員，請參閱 [NSX 聯盟中的安全性](#)。

- **區段**

備註 IP 位址已指派給閘道介面，而 NSX 負載平衡器虛擬 IP 位址不會納入為區段群組成員。

- **區段連接埠**

- **VIF**

- **虛擬機器**

- **實體伺服器**

- **雲端原生服務執行個體**

7 (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 位址、IPv6 位址和多點傳播位址。

按一下 **動作 > 匯入**，從包含以逗號分隔之 IP/MAC 值的 .TXT 檔案或 .CSV 檔案匯入 IP/MAC 位址。

8 (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文字方塊中，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。

如果您使用 NSX 聯盟，則無法從全域管理程式建立群組來包含 AD 群組。

9 (選擇性) 輸入說明和標籤。

10 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，即可在一或多個分散式防火牆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。

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、URL 類別或網域 (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 層分散式防火牆規則 (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)。

容器

您可以導覽至**詳細目錄 > 容器**，以檢視容器相關物件的詳細目錄。

容器相關物件是透過 NSX Container Plugin (NCP) 進行設定。如需 NCP 說明文件，請移至 <https://docs.vmware.com/tw/VMware-NSX-T-Data-Center/index.html>。

命名空間索引標籤會顯示您已設定的命名空間。會顯示下列資訊：

- 命名空間
- 類型
- 叢集
- IP 位址

- 網繭
- 服務
- 網路
- 網路狀態

您可以展開每個資料列以查看更多詳細資料，例如入口規則、標籤、網路和安全性原則。

您可以按一下**網繭**、**服務**和**網路**欄位中的值，以取得詳細資訊。

叢集索引標籤會顯示您已設定的叢集。會顯示下列資訊：

- 容器叢集名稱
- 基礎結構類型
- 節點
- 命名空間
- 網繭
- 服務
- 網路
- 網路狀態

您可以按一下**節點**、**命名空間**、**網繭**、**服務**和**網路**欄位中的值，以取得詳細資訊。

網繭畫面會顯示下列資訊：

- 網繭名稱
- 容器節點
- 傳輸節點
- IP 位址 (僅會顯示來自網繭對應區段連接埠的 IP 位址。對於未連結至區段的網繭網路介面，不會顯示其 IP 位址。)
- 區段
- 區段連接埠
- 服務
- 標籤
- 狀態
- 網路狀態

服務畫面會顯示下列資訊：

- 服務名稱
- 命名空間
- 網路

- 標籤
- 狀態
- 網路狀態

網路畫面會顯示下列資訊：

- 實體名稱
- 實體類型
- 連線
- 標籤
- 狀態

節點畫面會顯示下列資訊：

- 節點名稱
- 外部識別碼
- IP 位址
- 標籤
- 網路狀態

公有雲服務

您可以查看適用於公有雲工作負載虛擬機器的公有雲服務清單。

您可以使用 NSX Cloud，以使用雲端原生安全性建構保護的公有雲服務上線。

備註 在目前版本中，僅支援下列 AWS 服務：

- RDS
 - 應用程式 ELB (不支援網路 ELB)
-

如何使用 NSX Cloud 來將公有雲服務上線

您可以按照在 原生雲端強制執行模式 中將工作負載虛擬機器上線的相同方式，將公有雲服務上線。

上線後，公有雲服務可從 [詳細目錄 > 公有雲服務](#) 取得。

您可以按照對工作負載虛擬機器相同的方式建立這些服務的防火牆規則。

請參閱 [在 原生雲端強制執行模式 中管理虛擬機器](#)。

備註 您必須在 NSX Manager 的防火牆規則中，啟用這些服務所使用的連接埠，例如，用於 ELB 的連接埠 80。

實體伺服器

您可以導覽至**詳細目錄 > 實體伺服器**，以檢視實體伺服器的詳細目錄。這些是在裸機伺服器上執行的傳輸節點。

針對每個實體伺服器，系統會顯示下列資訊：

- 名稱
- 作業系統類型
- IP 位址
- 標籤

標籤

標籤可協助您標記 NSX-T Data Center 物件，讓您快速搜尋或篩選物件、疑難排解和追蹤，以及執行其他相關工作。

您可以使用 UI 和 API 建立標籤。每個標籤都有下列兩個屬性：

- 標籤 (表示標籤名稱。這是必要項目，且必須是唯一的且區分大小寫。)
- 範圍 (選用)

標籤範圍類似於索引鍵，而標籤名稱類似於值。例如，假設您想要根據虛擬機器的作業系統 (Windows、Mac、Linux) 來標記所有虛擬機器。您可以建立三個標籤，例如 Windows、Linux 和 Mac，然後將每個標籤的範圍設定為作業系統。其他標籤範圍的範例包含承租人、擁有者、名稱等。

儲存標籤後，您便無法更新名稱和範圍。但是，您可以從物件取消指派或移除標籤。

如需 NSX-T Data Center 物件中支援的標籤數量上限的相關資訊，請參閱「VMware 組態上限」工具，網址為 <https://configmax.vmware.com/home>。

以下是一些您可以使用標籤執行的作業：

- 對物件指派或取消指派標籤。
- 同時對多個物件指派或取消指派單一標籤 (僅支援虛擬機器)。
- 在詳細目錄中檢視所有標籤的清單。
- 依標籤名稱、標籤來源和標籤範圍篩選標籤清單。
- 檢視已指派特定標籤的物件清單。

標籤的使用案例

下表說明使用標籤的某些使用案例。

使用案例	說明
管理能力	<ul style="list-style-type: none"> ■ 簡化大型詳細目錄管理中的物件搜尋。 ■ 提供更多資訊以區分共用類似或不明名稱的物件。
第三方共用和內容共用	<ul style="list-style-type: none"> ■ 使用自訂資訊為物件加上註解。 ■ 允許第三方非 NSX 系統以自動方式新增中繼資料資訊。例如，來自合作夥伴、雲端管理提供者、容器平台等的中繼資料。 ■ 使用 NSX 探索代理程式、詳細目錄收集、公有雲代理程式、Guest Introspection 與 VM Tools 等來擷取學習到的屬性或內容和關聯性。
安全性	<ul style="list-style-type: none"> ■ 建立分組成員資格準則。 ■ 指定防火牆來源和目的地。
疑難排解 (可追蹤性)	<ul style="list-style-type: none"> ■ 在記錄中追蹤防火牆規則 (規則標籤) ■ 追蹤物件，並將其關聯回 OpenStack 網路。

系統標籤

系統標籤是系統定義的標籤，您無法新增、編輯或刪除這些標籤。

表 14-1. 公有雲管理程式物件中的系統標籤

物件	系統標籤
邏輯交換器	■ CrossCloud
節點	■ CloudType
邏輯路由器	■ CloudScope
邏輯路由器上行連接埠	■ CloudRegion
靜態路由	■ CloudVpId
DHCP 設定檔	■ PcId
防火牆區段規則清單	■ EntityType
NAT 規則	<ul style="list-style-type: none"> ■ CrossCloud ■ CloudType ■ CloudScope ■ CloudRegion ■ CloudVpId ■ PcId ■ EntityType ■ DefaultSnatRule ■ DefaultLinkLocalSNatRule/Cloud-Public-IP ■ DefaultSiNatRule

表 14-2. Cloud Service Manager (CSM) 物件中的系統標籤

物件	系統標籤
BFD 健全狀況監控設定檔	■ CrossCloud
傳輸區域	■ CloudType
上行主機交換器設定檔	■ CloudScope
傳輸節點	■ CloudRegion
Edge 叢集	■ CloudVpclid
	■ Pcmlid
	■ EntityType

表 14-3. NSX Cloud 虛擬機器中的系統標籤

標籤來源	系統標籤
Amazon	<ul style="list-style-type: none"> ■ aws:account ■ aws:availabilityzone ■ aws:region ■ aws:vpc ■ aws:subnet ■ aws:transit_vpc
Microsoft Azure	<ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ azure:transit_vnet_name ■ azure:transit_vnet_rg

表 14-4. 其他 NSX-T Data Center 物件中的系統標籤

物件	系統標籤
群組	<ul style="list-style-type: none"> ■ autoPlumbing ■ abstractionPath ■ NLB-VIP_ID ■ NLB-Lb-ID ■ NLB-Pool_ID
區段	■ subnet-cidr
IP 位址集區	■ abstractionPath
IP 位址區塊	

探索到的標籤

NSX-T Data Center 可以探索 Amazon 和 Microsoft Azure 中的標籤，並進行同步化。

探索到的標籤是您新增至公有雲中虛擬機器的標籤，且由 NSX Cloud 自動探索而來。探索到的標籤會針對您在 NSX Manager 詳細目錄中的工作負載虛擬機器顯示。您無法在 UI 中編輯這些標籤。

探索到 AWS 標籤的首碼為「dis:aws」，而探索到 Azure 標籤的首碼為「dis:azure」。當您對公有雲中的標籤進行變更時，這些變更會反映在 NSX Manager 中。依預設會啟用此功能。

您可以在新增 AWS 帳戶時啟用或停用 AWS 標籤的探索。同樣地，您可以在新增 Microsoft Azure 訂閱時啟用或停用 Microsoft Azure 標籤。

將標籤新增至物件

您可以選取 NSX-T Data Center 詳細目錄中可用的現有標籤，或是建立新標籤以新增至物件。

下列程序說明將標籤新增至單一物件的步驟。在此程序中，考慮使用的是虛擬機器物件。將標籤新增至其他物件的步驟保持不變。您可以導覽至特定物件頁面，並遵循類似步驟以將標籤新增至該物件。

如需 NSX-T Data Center 物件中支援的標籤數量上限的相關資訊，請參閱「VMware 組態上限」工具，網址為 <https://configmax.vmware.com/home>。

程序

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，按一下**詳細目錄 > 虛擬機器**。在您要編輯的虛擬機器旁邊，按一下垂直省略符號，然後按一下**編輯**。

3 在**標籤**下拉式功能表中，輸入標籤名稱。完成後，按一下**新增項目**。

標籤名稱的長度上限為 256 個字元。

如果詳細目錄中存在標籤，則**標籤**下拉式功能表會顯示所有可用標籤及其範圍的清單。可用標籤的清單包含使用者定義的標籤、系統定義的標籤，以及探索到的標籤。您可以從下拉式功能表中選取現有標籤，並將其新增至虛擬機器。

4 (選擇性) 輸入標籤範圍。

例如，假設您想要根據虛擬機器的作業系統 (Windows、Mac、Linux) 來標記虛擬機器。請建立三個標籤，例如 Windows、Linux 和 Mac，然後將每個標籤的範圍設定為作業系統。

範圍的長度上限為 128 個字元。

如果已從詳細目錄中選取現有標籤，則會自動套用所選標籤的範圍。否則，您可以為要建立的新標籤輸入範圍。

5 按一下 **+** 圖示。

標籤即會新增至虛擬機器。

6 (選擇性) 重複步驟 3-5 以將更多標籤新增至虛擬機器。

7 按一下**儲存**。

將標籤新增至多個物件

從 NSX-T Data Center 3.0 開始，您可以同時將標籤新增至多個物件。但是，在 v3.0 中，此功能僅適用於虛擬機器物件。

程序

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

2 按一下 **詳細目錄 > 標籤**。

3 按一下 **新增標籤**。

4 輸入標籤名稱。

標籤名稱的長度上限為 256 個字元。

5 (選擇性) 輸入標籤範圍。

例如，假設您想要根據虛擬機器的作業系統 (Windows、Mac、Linux) 來標記虛擬機器。請建立三個標籤，例如 Windows、Linux 和 Mac，然後將每個標籤的範圍設定為作業系統。

範圍的長度上限為 128 個字元。

6 在已指派到中，按一下 **設定虛擬機器**。

7 (必要) 選取一或多個要指派標籤的虛擬機器，然後按一下 **套用**。

您必須先將標籤指派給至少一個虛擬機器，然後才能儲存標籤。

備註 您一次可以在最多 1000 個虛擬機器上執行大量標籤指派。

8 按一下 **儲存**。

結果

- 如果要將標籤指派到多個虛擬機器，則指派可能需要一些時間。當指派進行中時，**上次指派狀態**會顯示執行中。將標籤成功指派給所有選取的虛擬機器後，**上次指派狀態**資料行會變更為成功。
- 如果發生部分指派，NSX-T Data Center 不會從已套用標籤的虛擬機器復原標籤指派。例如，假設您選取了 100 個虛擬機器進行大量標籤指派，而其中 10 個虛擬機器的指派失敗。在剩餘 90 個虛擬機器上指派的標籤將不會復原。

在此類部分指派的情況下，請執行下列 API 以擷取標籤作業的狀態：

```
GET /api/v1/infra/tags/tag-operations/<tag-operation-id>/status
```

您也可以使用下列 API 來擷取標籤作業的實現狀態：

```
GET /api/v1/infra/realized-state/realized-entities?intent_path=/infra/
tags/tag-operations/<operation-id>
```

如需這些 API 的詳細資料，請參閱《NSX-T Data Center API 指南》。

後續步驟

如果詳細目錄中有較長的標籤清單，您可以篩選或搜尋標籤，以快速找到您所感興趣的標籤。您可以篩選來源、範圍和標籤 (標籤的名稱)。您也可以在 UI 中排序標籤。但是，由於標籤區分大小寫，因此標籤僅依詞彙順序排序。

以下限制會套用至搜尋或篩選標籤：

- 您無法同時依照來源和範圍屬性篩選標籤，因為這兩者都屬於標籤的範圍屬性。

- API 不支援使用特殊字元 (例如 *、&、/、\ 等) 篩選標籤。但是，您可以在 UI 中使用特殊字元篩選標籤。

從物件取消指派標籤

您可以移除先前指派給物件的標籤。

下列程序說明從單一 NSX-T Data Center 物件取消指派標籤的步驟。在此程序中，考慮使用的是虛擬機器物件。從其他物件取消指派標籤的步驟保持不變。您可以導覽至特定物件頁面，並遵循類似步驟從該物件取消指派標籤。

程序

- 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，按一下 **詳細目錄 > 虛擬機器**。在您要編輯的虛擬機器旁邊，按一下垂直省略符號，然後按一下 **編輯**。
- 3 針對要從虛擬機器取消指派的每個標籤，按一下 **X** 圖示。
- 4 按一下 **儲存**。

從多個物件中取消指派標籤

從 NSX-T Data Center 3.0 開始，您可以同時從多個物件取消指派標籤。但是，在 v 3.0 中，此功能僅適用於虛擬機器。

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 按一下 **詳細目錄 > 標籤**。
- 3 在要編輯的標籤旁邊，按一下垂直省略符號，然後按一下 **編輯**。
- 4 在 **已指派到** 資料行中，按一下已指派此標籤之虛擬機器的數目。
- 5 針對每個要取消指派此標籤的虛擬機器，按一下 **X** 圖示。

備註

- 您一次可以在最多 1000 部虛擬機器上執行大量標籤取消指派。
 - 從所有物件取消指派標籤時，系統會在五天後自動從詳細目錄中刪除該標籤。
-

- 6 按一下 **套用**，然後按一下 **儲存**。

有兩個選項可用於跨多個位置管理 NSX-T Data Center。

表 15-1. 多網站和聯盟的比較

	多站台	聯盟
可用性	NSX-T Data Center 2.3	NSX-T Data Center 3.0
環境	中小型企業	大型企業
環境設定檔	<ul style="list-style-type: none"> ■ 中小型規模部署 ■ 無特定網站管理或原則需求 	<ul style="list-style-type: none"> ■ 大規模部署 ■ 特定網站管理或原則需求
NSX Manager 叢集數目	1	每個位置 1 個
VMware Site Recovery Manager 支援管理平面的災難復原	從 NSX-T Data Center 3.0.2 開始完整支援。	從 NSX-T Data Center 3.0.2 開始，完全支援全域管理程式和本機管理程式應用裝置的復原。
VMware Site Recovery Manager 支援計算虛擬機器的災難復原	從 NSX-T Data Center 3.0.2 開始完整支援。	不支援。
vSphere 高可用性 (vSphere HA) 支援管理平面的災難復原	完全支援。	從 NSX-T Data Center 3.0.2 開始，完全支援全域管理程式和本機管理程式應用裝置的復原。

本章節討論下列主題：

- [NSX-T Data Center 多站台](#)
- [NSX 聯盟](#)

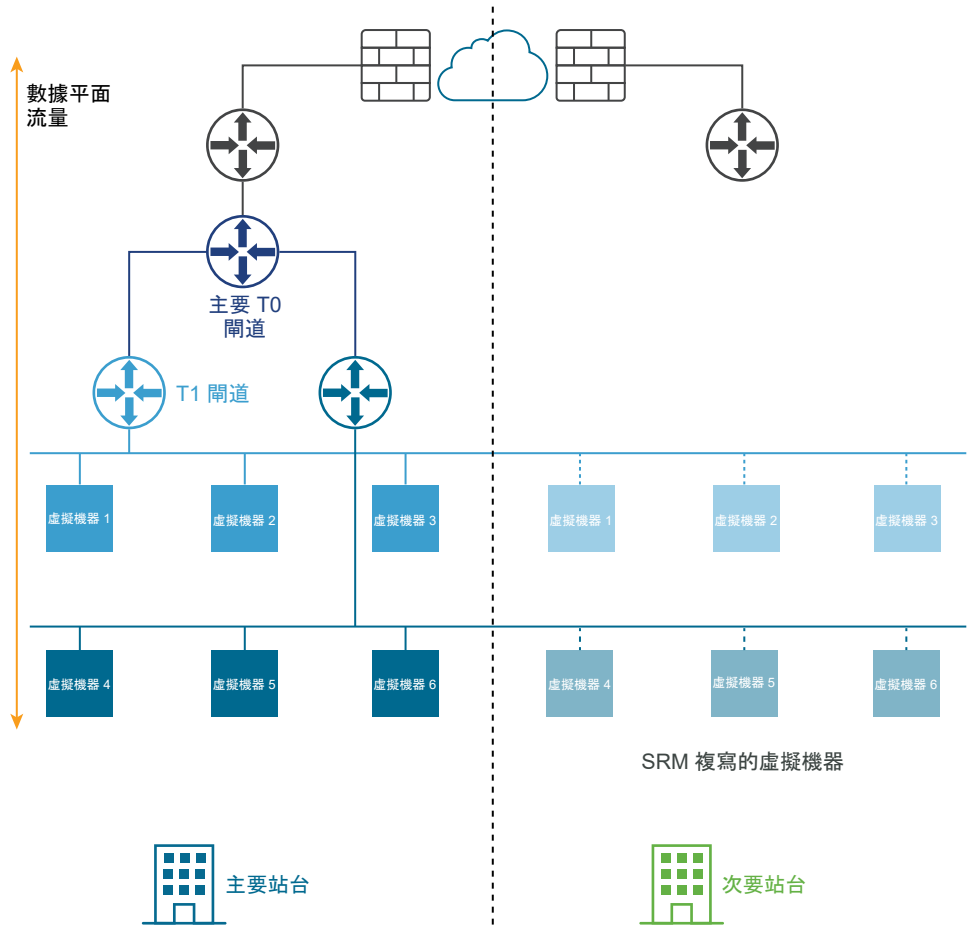
NSX-T Data Center 多站台

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：

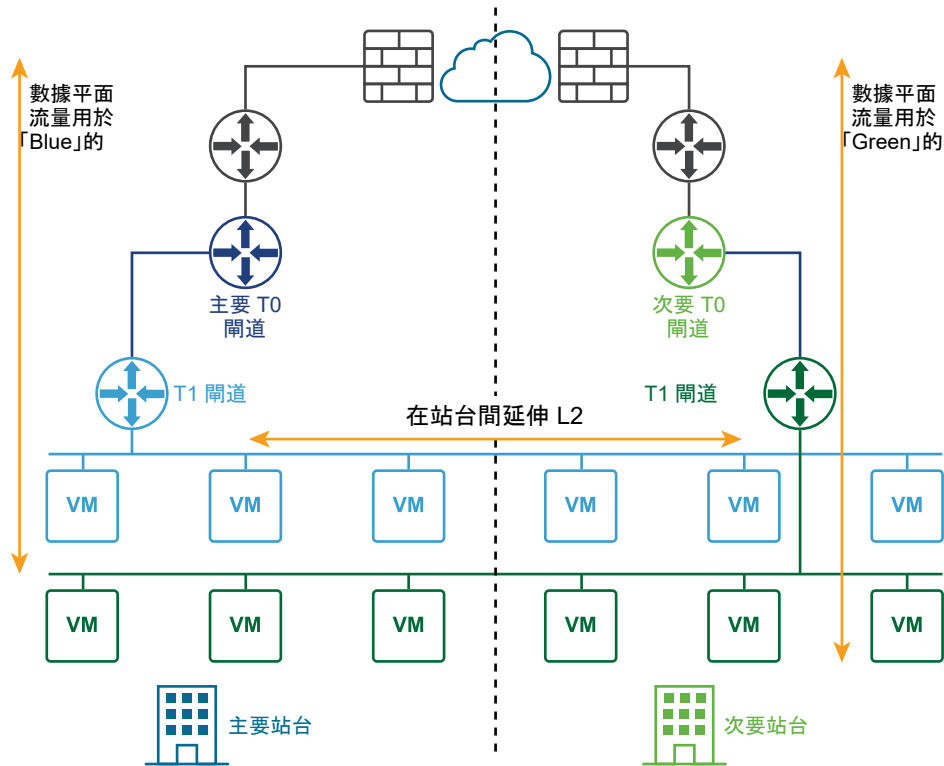
- 災難復原
- 作用中/作用中

下圖說明災難復原部署。



在作用中/作用中部署中，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。在災難復原部署中，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。

下圖說明作用中/作用中部署。



您可以為管理平面和數據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

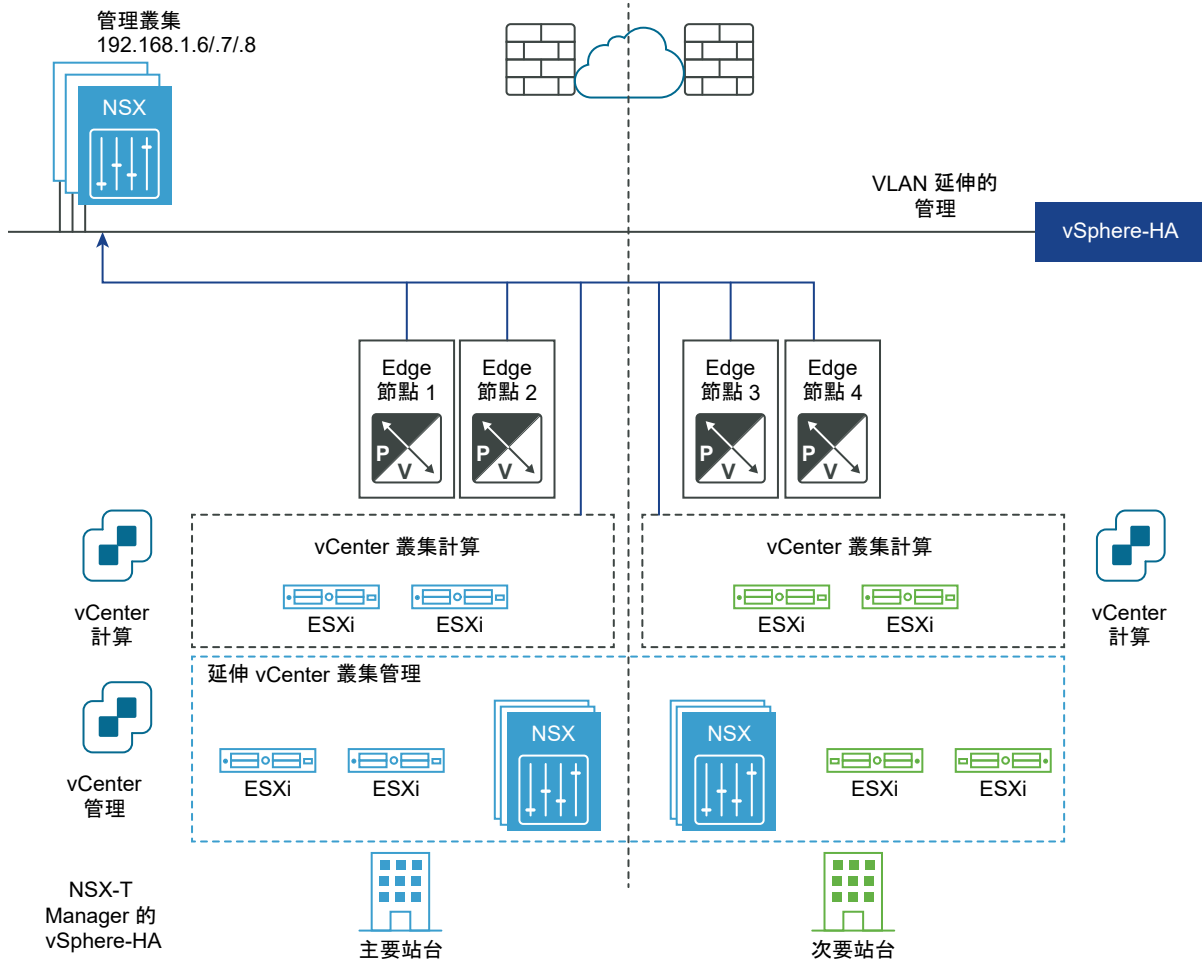
需求：

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

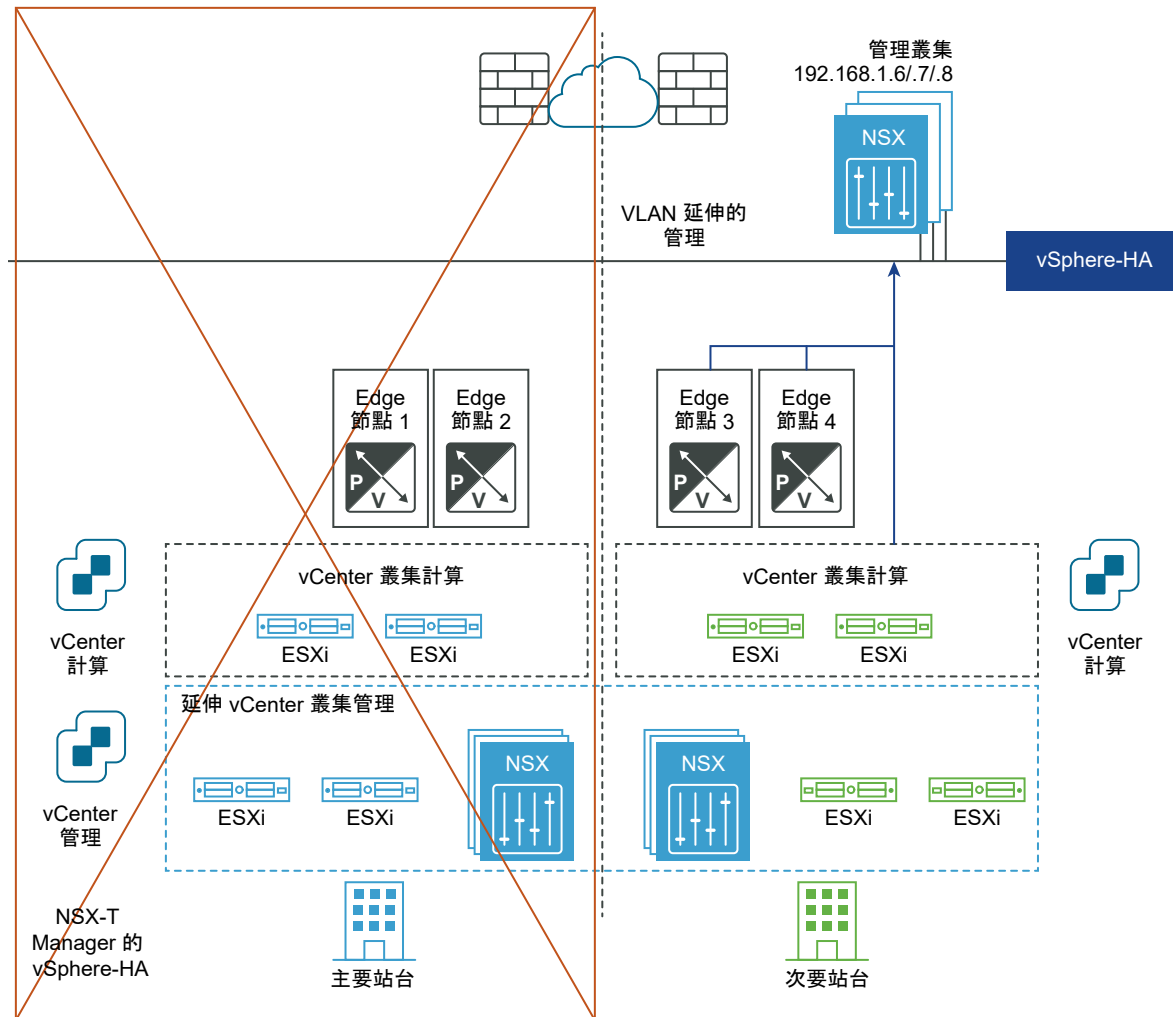
NSX Manager 叢集會部署在管理 VLAN 上，並且實際位於主要站台中。如果主要站台故障，vSphere HA 將會重新啟動次要站台中的 NSX Manager。所有傳輸節點會自動重新連線至重新啟動的 NSX Manager。此程序需要大約 10 分鐘。在此期間，管理平面無法使用，但數據平面不會受到影響。

下圖說明管理平面的自動復原。

災難之前：



災難復原之後：



數據平面的自動復原

您可以為 Edge 節點設定失敗網域，以實現數據平面的自動復原。您可以將 Edge 叢集內的 Edge 節點分組在不同的失敗網域中。NSX Manager 會自動將任何新的作用中第 1 層閘道置於慣用的失敗網域，以及將待命第 1 層閘道置於另一個網域。

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 模式必須為作用中/待命模式，且容錯移轉模式必須為先佔式。
- 如果可以進行非對稱路由 (例如，兩個位置是兩棟建築物，它們之間沒有任何實體防火牆)，則第 0 層閘道的 HA 模式可以是作用中/作用中。

附註：第 1 層閘道的容錯移轉模式可以是先佔式和非先佔式，但建議設定為先佔式，以確保第 0 層和第 1 層閘道位於同一位置。

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"
      }
    }
  ],
}

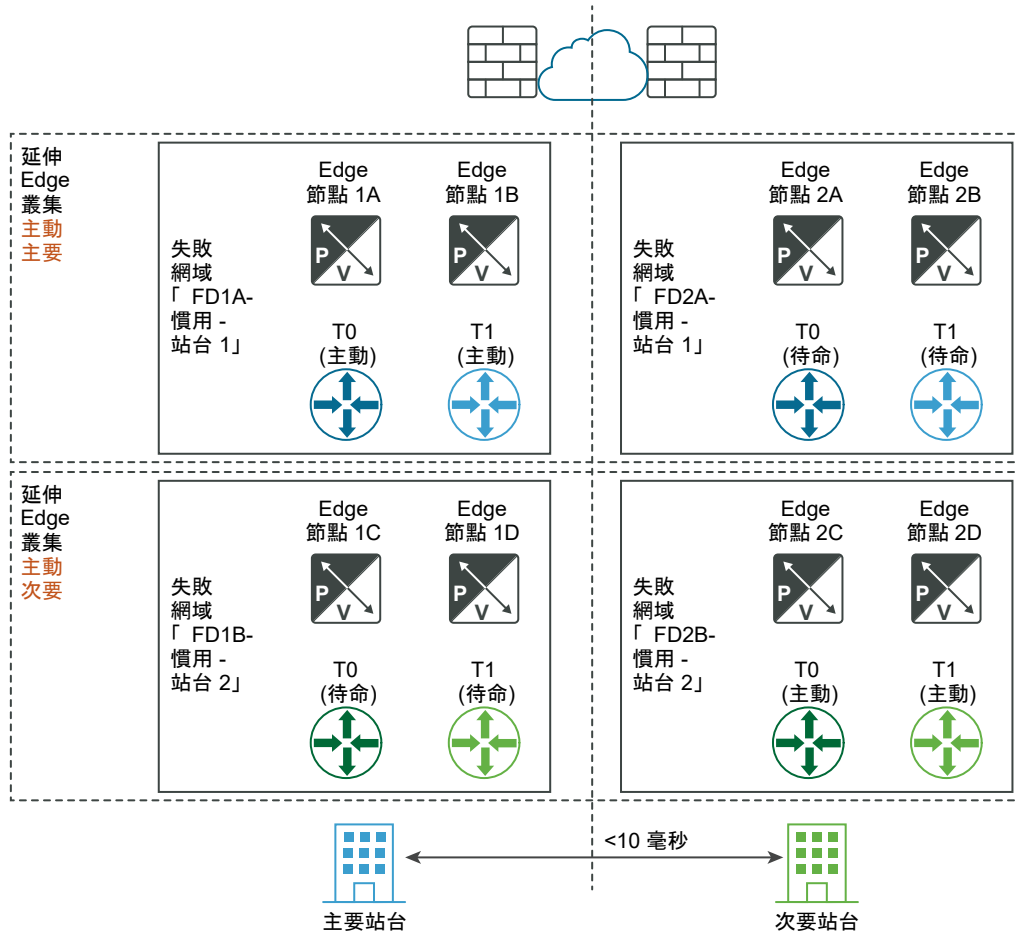
```

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

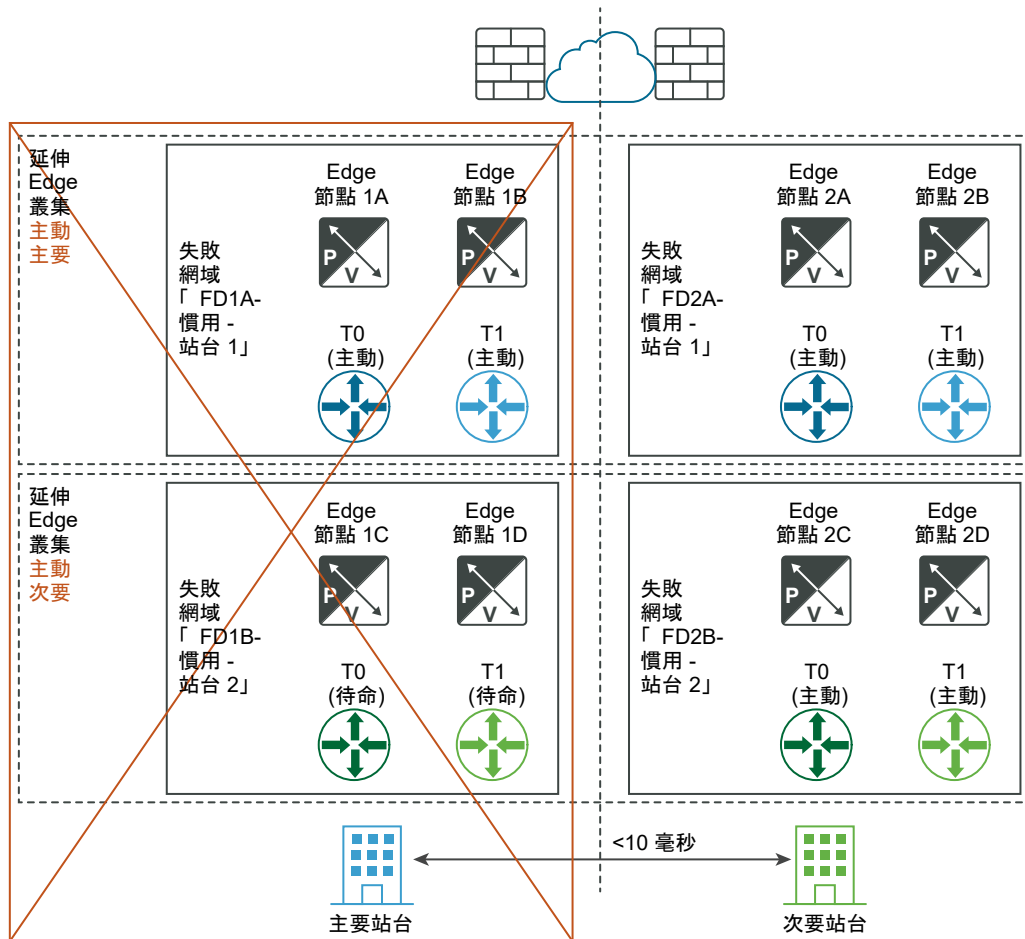
如果整個主要站台失敗，則次要站台中的第 0 層待命和第 1 層待命會自動接管並成為新的作用中閘道。如果主要站台中的其中一個 Edge 節點失敗，則會套用相同的原則。例如，在下圖中，假設 Edge 節點 1B 主控 Tier-O-Test 和 Tier-1-Test，Edge 節點 2A 主控 Tier-O-Test 待命，以及 Edge 節點 2B 主控 Tier-1-Test 待命。如果 Edge 節點 1B 失敗，則在 Edge 節點 2B 上的待命 Tier-O-Test 和 Edge 節點 2A 上的待命 Tier-1-Test 會接管並成為新的作用中閘道。

下圖說明數據平面的自動復原。

災難之前：



災難復原之後：



管理平面的手動/指令碼式復原

需求：

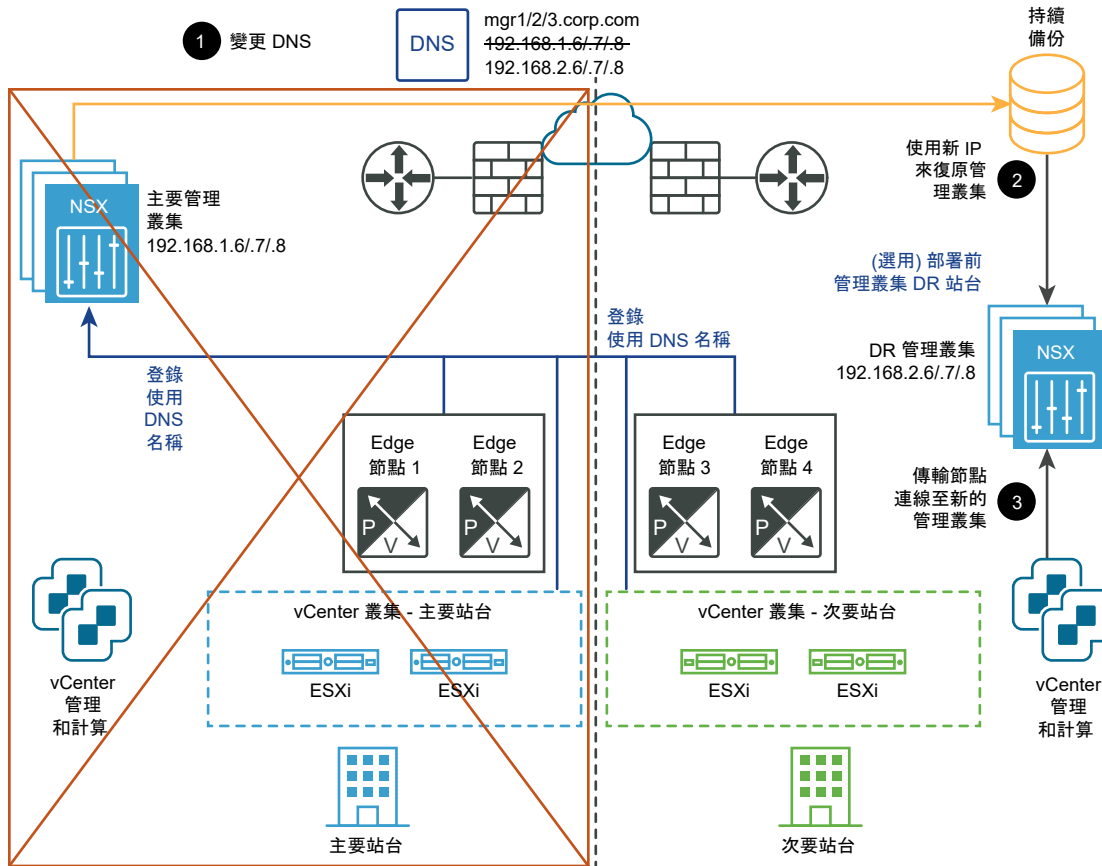
- NSX Manager 的 DNS 具有短 TTL (例如，5 分鐘)。
- 持續備份。

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。



數據平面的手動/指令碼式復原

需求：

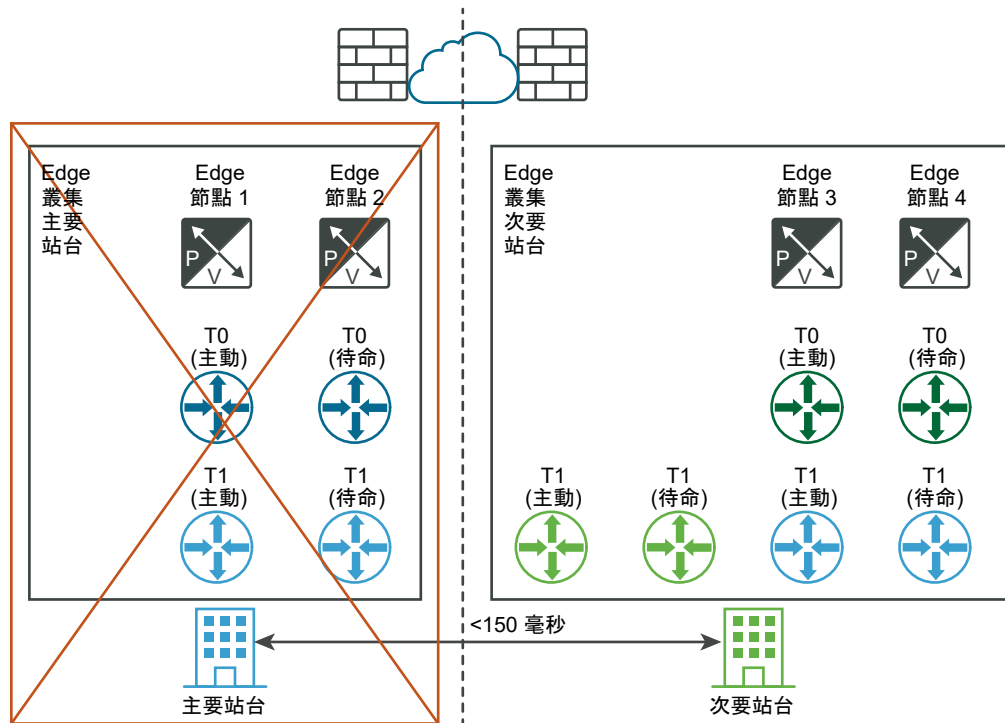
- Edge 節點之間的最大延遲時間為 150 毫秒。

Edge 節點可以是虛擬機器或裸機。每個位置中的第 0 層閘道可以是作用中/待命或作用中/作用中。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 使用 API 將連接至主要第 0 層閘道的第 1 層閘道 (下圖中藍色部分) 移至次要第 0 層閘道 (綠色)。
- 2 使用 API 將獨立的第 1 層閘道移至次要站台。
- 3 使用 API 將第 2 層橋接器移至次要站台。

下圖說明數據平面的手動/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

- 對於管理平面自動復原
 - 在站台之間延伸 VLAN 管理。
 - vSphere HA 跨 NSX Manager 虛擬機器站台。
- 對於管理平面的手動/指令碼式復原
 - 持續備份。
 - NSX Manager 必須設為使用 FQDN。

數據平面

- 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。
- 對於管理平面自動復原
 - 位置之間的最大延遲為 10 毫秒。

- 第 0 層閘道的 HA 模式必須為作用中/待命，且容錯移轉模式必須為先佔式，以確保沒有非對稱路由。
- 如果可接受非對稱路由 (例如，都會區域中的不同建築物)，則第 0 層閘道的 HA 模式可以是作用中/作用中。
- 對於管理平面的手動/指令碼式復原
 - 位置之間的最大延遲為 150 毫秒。

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

使用 VMware Site Recovery Manager

從 NSX-T Data Center 3.0.2 開始，您可以將 VMware Site Recovery Manager 與 NSX-T Data Center 多站台搭配使用。

如需有關使用 VMware Site Recovery Manager 的詳細指示，請參閱：[VMware Site Recovery Manager 說明文件](#)。

下列 Site Recovery Manager 工作流程支援 NSX-T Data Center 多站台：

- NSX-T Data Center 管理虛擬機器：
 - 完整復原以及測試復原管理虛擬機器。
 - 使用 VIP 復原管理叢集。
 - 使用個別節點 IP 位址而非 VIP 來復原管理叢集。
- 計算虛擬機器：
 - 完整復原以及測試復原計算虛擬機器。
 - 復原計算虛擬機器的網路服務。
 - 復原虛擬機器標籤、安全群組和防火牆規則。

NSX 聯盟

透過 NSX 聯盟，您可以使用單一虛擬管理介面來管理多個 NSX-T Data Center 環境、建立跨越一或多個位置的閘道和區段，以及在各位置之間一致地設定和強制執行防火牆規則。

安裝全域管理程式並新增位置後，即可從全域管理程式設定網路與安全性。

如需初始 NSX 聯盟組態 (包括安裝全域管理程式和新增位置) 的相關資訊，請參閱《NSX-T Data Center 安裝指南》中的〈開始使用聯盟〉。

NSX 聯盟 概觀

在設定您的 NSX 聯盟環境之前，請瞭解支援哪些功能、NSX 聯盟跨位置共用資訊的方式，以及使用者介面的運作方式。

聯盟重要概念

NSX 聯盟 推出了一些新的詞彙與概念，例如遠端通道端點 (RTEP)、範圍和區域。

聯盟系統：全域管理程式和本機管理程式

聯盟環境包括兩個類型的管理系統：

- 全域管理程式：類似於 NSX Manager 的系統，會同盟多個本機管理程式。
- 本機管理程式：NSX Manager 系統，負責位置的網路和安全性服務。

聯盟範圍：本機和延伸

當您從 全域管理程式 建立網路物件時，它會跨越一或多個位置。

- 本機：物件僅跨越一個位置。
- 延伸：物件跨越一個以上的位置。

您不會直接設定區段的範圍。區段與其連結的閘道具有相同的範圍。

聯盟區域

安全性物件具有一個區域。區域可能為下列其中一項：

- 位置：系統將針對每個位置自動建立的區域。此區域具有該位置的範圍。
- 全域：範圍為所有可用位置的區域。
- 自訂區域：您可以建立包含可用位置子集的區域。

聯盟通道端點

在聯盟環境中，有兩個類型的通道端點。

- 通道端點 (TEP)：在位置內用於 Geneve 封裝的傳輸節點 (Edge 節點或主機) 的 IP 位址。
- 遠端通道端點 (RTEP)：傳輸節點 (僅限 Edge 節點) 的 IP 位址，用於跨位置的 Geneve 封裝。

聯盟中支援的功能和組態

從全域管理程式所做的所有組態都是在原則模式中進行。聯盟中無法使用管理程式模式。

如需關於兩個模式的詳細資訊，請參閱第 1 章 [NSX Manager](#)。

組態上限

聯盟環境具有以下組態上限：

- 對於多數組態，本機管理程式叢集的組態上限與 NSX Manager 叢集相同。移至 [VMware 組態上限工具](#)，然後選取 NSX-T Data Center。

在 VMware 組態上限工具中，對於 NSX-T Data Center 選取聯盟類別作為例外狀況和其他聯盟特定的值。

- 對於指定的位置，下列組態會導致組態上限：
 - 在本機管理程式上建立的物件。
 - 在全域管理程式上建立並將位置包含在其範圍中的物件。

您可以在每個本機管理程式上檢視容量和使用量。請參閱[檢視物件類別的使用量和容量](#)。

功能支援

表 15-2. 聯盟中支援的功能

功能	詳細資料	相關連結
第 0 層閘道	<ul style="list-style-type: none"> ■ 3.0.1 及更新版本：雙主動和主動備用 ■ 3.0.0：僅限雙主動 	從全域管理程式新增第 0 層閘道
第 1 層閘道		從全域管理程式新增第 1 層閘道
區段	不支援第 2 層橋接器。	從全域管理程式新增區段
群組	一些限制。請參閱 NSX 聯盟中的安全性 。	從全域管理程式建立群組
分散式防火牆		從全域管理程式建立 DFW 原則和規則
閘道防火牆		從全域管理程式建立閘道原則和規則
網路位址轉譯 (NAT)	<p>第 0 層閘道：</p> <ul style="list-style-type: none"> ■ 雙主動：您只能設定無狀態 NAT，也就是動作類型為自反。 ■ 主動備用：您可以建立可設定狀態或無狀態的 NAT 規則。 <p>第 1 層閘道：</p> <ul style="list-style-type: none"> ■ 您可以建立可設定狀態或無狀態的 NAT 規則。 <p>無狀態 NAT 規則會推送至閘道範圍中的所有位置，除非明確地將範圍限制在一或多個位置。</p> <p>可設定狀態的 NAT 規則也會推送至閘道範圍中的所有位置或所選的特定位置。但是，可設定狀態的 NAT 規則僅會在主要位置上實現並強制執行。</p>	在閘道上設定 NAT
DNS		請參閱新增 DNS 轉寄站服務

表 15-2. 聯盟中支援的功能 (續)

功能	詳細資料	相關連結
DHCP 和 SLAAC	<ul style="list-style-type: none"> ■ 區段和閘道上支援 DHCP 轉送。 ■ 在區段上已設定 DHCP 靜態繫結的閘道上，支援 DHCPv4 伺服器。 ■ IPv6 位址可使用透過 RA 取得 DNS 的 SLAAC 來指派 (DAD 僅會偵測位置內的重複項目)。 	<ul style="list-style-type: none"> ■ DHCP 轉送：新增 DHCP 轉送設定檔 ■ DHCP 伺服器 (僅在閘道上支援)： <ul style="list-style-type: none"> ■ 新增 DHCP 伺服器設定檔 ■ 將 DHCP 設定檔連結至第 0 層或第 1 層閘道 ■ 在區段上設定 DHCP 靜態繫結 ■ IPv6 位址指派：建立 IPv6 位址指派的 SLAAC 和 DAD 設定檔
在本機管理程式組態中使用在全域管理程式上建立的物件	<p>支援多數組態。例如：</p> <ul style="list-style-type: none"> ■ 將本機管理程式第 1 層閘道連線至全域管理程式第 0 層閘道。 ■ 在本機管理程式分散式防火牆規則中使用全域管理程式群組。 <p>不支援這些組態：</p> <ul style="list-style-type: none"> ■ 將本機管理程式區段連接至全域管理程式第 0 層或第 1 層閘道。 ■ 將負載平衡器連接至全域管理程式第 1 層閘道。 	
備份和還原	<ul style="list-style-type: none"> ■ 3.0.1 及更新版本：支援使用 FQDN 或 IP 進行備份。 ■ 3.0.0：不支援使用 FQDN 進行備份。 	在 NSX 聯盟中備份和還原
位置之間的 vMotion	不支援在位置之間進行冷移轉。	

瞭解聯盟

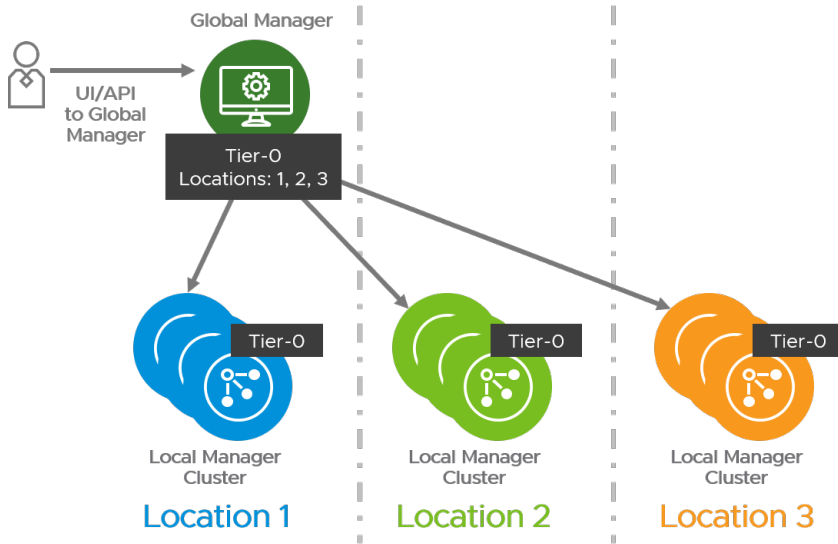
在聯盟中，您可以在全域管理程式上進行組態變更。變更會與相關的本機管理程式同步。本機管理程式也會彼此同步某些資訊。

在全域管理程式上進行變更

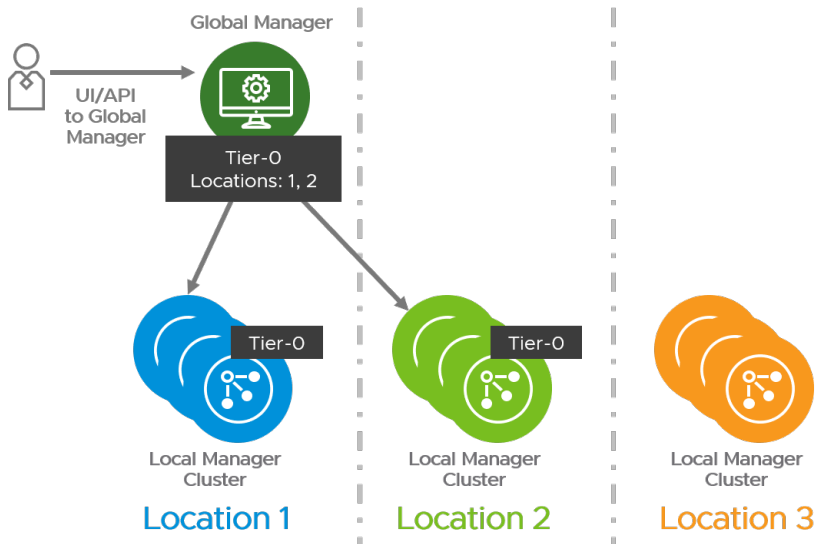
全域管理程式提供類似於 NSX Manager 介面的使用者介面。

在全域管理程式上建立的組態在本機管理程式上為唯讀。本機管理程式上的組態不會與全域管理程式同步。

只有在組態與該位置相關時，全域管理程式才會將組態與本機管理程式同步。例如，如果您建立第 0 層閘道，並將其新增至位置 1、位置 2 和位置 3，則系統會將組態與這三個本機管理程式同步。

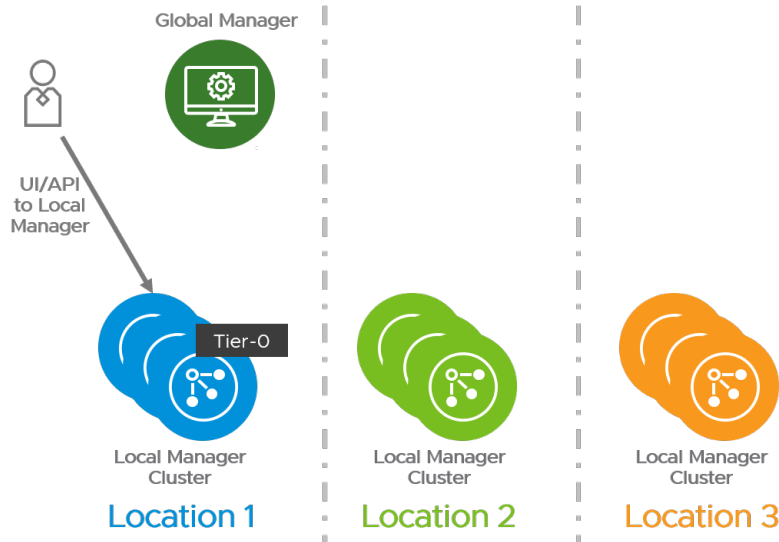


如果第 0 層閘道僅新增至位置 1 和位置 2，則組態不會與位置 3 同步。



在本機管理程式上進行變更

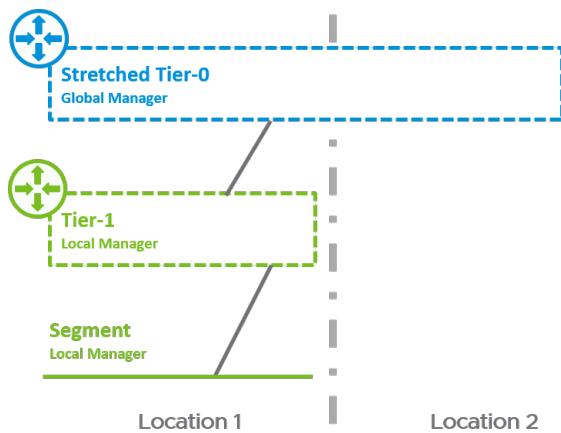
您可以使用本機管理程式在該特定本機管理程式上建立物件。這些物件不會與全域管理程式或任何其他本機管理程式同步。



在本機管理程式上實現全域管理程式變更

全域管理程式僅會對照全域管理程式組態驗證變更。當本機管理程式從全域管理程式接收到組態時，即會在該本機管理程式的網狀架構節點中實現組態。在此實現期間，可能會偵測到錯誤或衝突。

例如，您可以從全域管理程式建立第 0 層閘道，然後可以從本機管理程式建立第 1 層閘道並將其連結至第 0 層閘道。



由於本機管理程式不會將其組態同步至全域管理程式，因此從全域管理程式內容中，第 0 層閘道似乎不會連線至任何閘道。您可以從全域管理程式刪除第 0 層閘道，而此變更會同步至本機管理程式。當每個位置實現變更時，即會發生下列情況：

- 可以從位置 2 的本機管理程式刪除第 0 層閘道。
- 無法從位置 1 的本機管理程式刪除第 0 層閘道。
- 在全域管理程式上將第 0 層閘道標示為待刪除。

當第 0 層與位置 1 中的第 1 層中斷連線時，即會從全域管理程式中刪除第 0 層。

多數問題會顯示在使用者介面上。其他問題則可以使用這些 API 呼叫來顯示。

- 在全域管理程式上：

```
GET /global-manager/api/v1/global-infra/realized-state/alarms
```

- 在本機管理程式上：

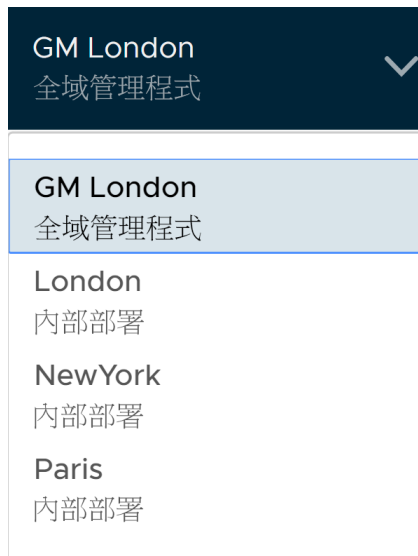
```
GET /policy/api/v1/infra/realized-state/alarms
```

使用全域和本機管理程式 Web 介面

您可以使用全域管理程式來建立僅限於一個位置或跨多個位置的物件。

全域管理程式上的位置下拉式功能表


登入全域管理程式 Web 介面時，您會在頂端導覽列中看到 [位置] 下拉式功能表。您可以使用此功能表在全域管理程式和任何相關聯的本機管理程式之間進行切換。





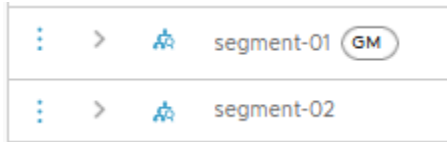
本機和全域物件

在本機管理程式上建立的物件是本機物件。它們為該本機管理程式特定，且無法從全域管理程式 Web 介面進行檢視。

從全域管理程式建立的物件是全域物件，但其範圍可能不包含所有可用的位置。

在本機管理程式上，您可以看到本機物件，以及適用於該位置的任何全域物件。全域物件旁邊有一個圖示：。

來自本機管理程式 Web 介面的此螢幕擷取畫面顯示兩個區段。區段 `segment-01` 旁有  圖示，表示它是在全域管理程式上建立的。區段 `segment-02` 沒有  圖示，表示它是在本機管理程式上建立的。



因為全域管理程式上的所有物件都是全域的，當您登入全域管理程式時，不會顯示任何圖示。

本機和全域物件的狀態

本機管理程式會顯示全域和本機物件的狀態。

全域管理程式僅顯示全域物件，但不會自動接收物件的狀態。


若要從本機管理程式擷取最新狀態，請針對物件按一下**檢查狀態**。若要重新整理狀態，請按一下**重新整理**圖示。



在本機管理程式上覆寫全域管理程式組態

當您從全域管理程式建立物件時，系統會將相同的組態傳播至所有相關的位置。從 NSX-T Data Center 3.0.1 開始，您可以在本機管理程式上覆寫某些全域管理程式組態。

若要覆寫組態，請按一下該組態旁邊的三個點功能表 (⋮)，然後按一下**編輯**。如果**編輯**功能表項目顯示為灰色，則無法覆寫此組態。

如果已覆寫組態，您會在全域管理程式和本機管理程式的狀態資料行中看到此圖示：

若要移除覆寫，請按一下組態旁邊的三個點功能表 (⋮)，然後按一下**還原**。即會還原來自全域管理程式的組態。

如果您覆寫來自本機管理程式上全域管理程式的組態，然後從全域管理程式刪除組態，則該組態仍會保留在本機管理程式上。還原該組態時，系統會從本機管理程式刪除組態。

您可以取得已覆寫所有組態的清單。對全域管理程式進行此 API 要求：`GET https://<global-mgr>/global-manager/api/v1/global-infra/overridden-resources`。

閘道組態

閘道組態可在**網路 > 第 0 層閘道**和**網路 > 第 1 層閘道**中找到。

您可以修改下列閘道組態：

- 第 0 層閘道 BGP 組態
- 第 0 層閘道介面

設定檔組態

全域管理程式上的設定檔組態會用於所有本機管理程式。設定檔組態沒有範圍設定。

您可以覆寫來自本機管理程式的下列全域設定檔組態：

- 區段設定檔：**網路 > 區段 > 區段設定檔**
 - IP 探索設定檔
 - MAC 探索設定檔
 - 區段安全性設定檔
 - SpoofGuard 設定檔
- 網路設定檔：**網路 > 網路設定**
 - IPv6 DAD 設定檔
 - IPv6 ND 設定檔
 - 閘道 QoS 設定檔
 - BFD 設定檔
- 內容設定檔：**詳細目錄 > 內容設定檔**
- 安全性設定檔：**安全性 > 安全性設定檔**
 - 防火牆工作階段計時器設定檔
 - Edge 閘道洪泛保護設定檔
 - 防火牆洪泛保護設定檔
 - DNS 安全性設定檔
 - CPU 和記憶體臨界值設定檔僅適用於 API：
 - 使用 PUT/PATCH <https://<local-manager>/policy/api/v1/global-infra/settings/firewall/cpu-mem-thresholds-profiles/<id>?action=override> 覆寫。
 - 使用 DELETE <https://<local-manager>/policy/api/v1/global-infra/settings/firewall/cpu-mem-thresholds-profiles/<id>> 還原。
- 疑難排解設定檔：**計劃和疑難排解**
 - 防火牆 IPFIX 設定檔
 - 交換器 IPFIX 設定檔

- IPFIX 防火牆收集器
- IPFIX 交換器收集器
- 遠端 L3 SPAN 連接埠鏡像設定檔
- 邏輯 SPAN 連接埠鏡像設定檔
- QoS 設定檔

NSX 聯盟 中的網路

第 0 層閘道、第 1 層閘道和區段可跨越 NSX 聯盟 環境中的一或多個位置。

規劃網路拓撲時，請記住下列需求：

- 第 0 層和第 1 層閘道可以有一或多個位置的範圍。
- 第 1 層閘道的範圍必須等於或其連結至第 0 層閘道的範圍子集。
- 區段的範圍與其連結的第 0 層或第 1 層閘道的範圍相同。隔離的區段在連線至閘道之前不會實現。
- 針對第 0 層和第 1 層閘道全域管理程式上所選取 Edge 叢集中的 NSX Edge 節點，必須設定為使用預設 TZ 覆疊。

您可以建立不同的拓撲以達成不同的目標。

- 您可以建立指定位置特定的區段和閘道。每個網站都有自己的組態，但您可以從全域管理程式介面管理各個項目。
- 您可以建立跨越位置的區段和閘道。這些延伸網路會跨網站提供一致的網路。

NSX 聯盟中的第 0 層閘道組態

透過 NSX 聯盟，您可以部署限制於單一位置的第 0 層閘道，也可以將其延伸至多個位置。

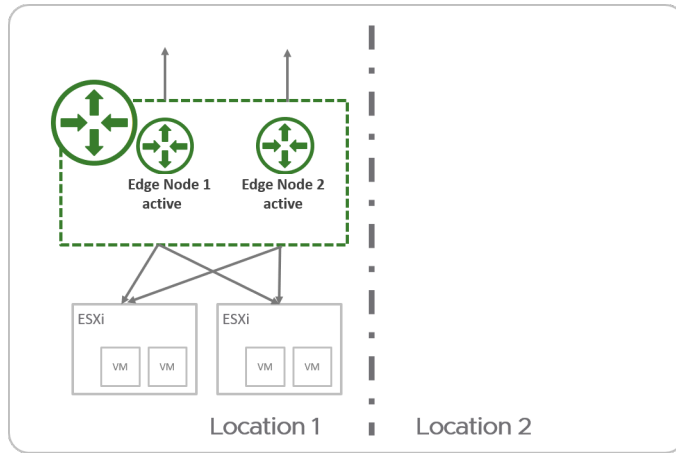
第 0 層閘道可以具有下列其中一項組態：

- 非延伸的第 0 層閘道。
- 具有主要和次要位置的延伸雙主動。
- 具有所有主要位置的延伸雙主動。
- 具有主要和次要位置的延伸主動備用。

備註 從 NSX-T Data Center 3.0.1 中開始，支援主動備用第 0 層閘道。

非延伸的第 0 層閘道

您可以從全域管理程式建立僅跨越一個位置的第 0 層閘道。這與直接在本機管理程式上建立第 0 層閘道類似，但其優點在於您可以從全域管理程式進行管理。



具有主要和次要位置的延伸雙主動第 0 層閘道

在具有主要和次要位置的雙主動第 0 層閘道中，適用於下列情況：

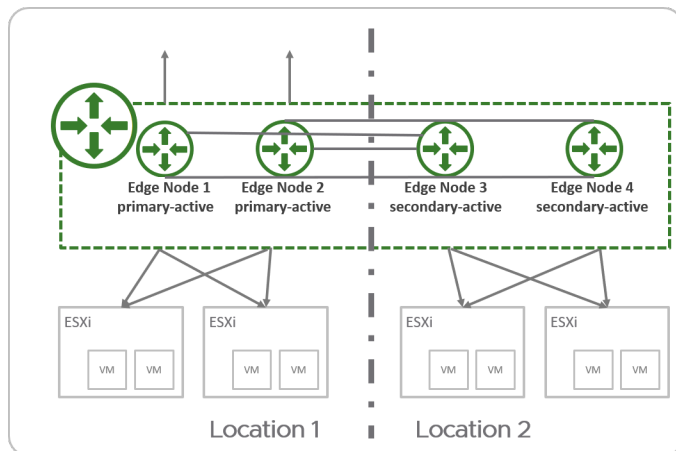
- 所有 Edge 節點會同時作用中，因此第 0 層無法執行可設定狀態的服務。
- 所有流量會透過主要位置的 Edge 節點進入和離開。

如果第 0 層閘道和連結的第 1 層閘道都有主要和次要位置，請將這兩個閘道的相同位置設定為主要，以減少跨位置流量。

重要 在此拓撲中，NSX-T Data Center 可確保所有出口流量都透過主要位置離開。

如果您的環境在實體網路上具有可設定狀態的服務 (例如外部防火牆)，則必須確保傳回流量透過主要位置進入。例如，您可以在次要位置的 BGP 對等上新增 AS 路徑附加。

如果您在實體網路上沒有可設定狀態的服務，且您選擇具有非對稱路由，則必須在所有外部第 0 層介面上停用單點傳播反向路徑轉送 (uRPF)。



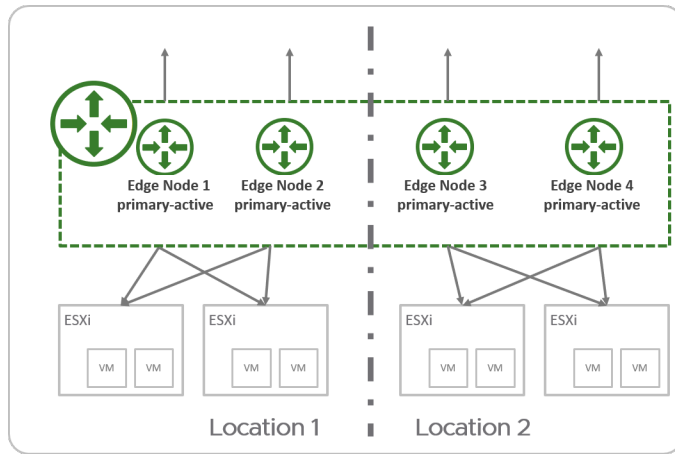
具有所有主要位置的延伸雙主動第 0 層閘道

在具有所有主要位置的雙主動第 0 層閘道中，適用於下列情況：

- 所有 Edge 節點會同時作用中，因此第 0 層無法執行可設定狀態的服務。

- 所有流量會透過與工作負載相同位置中的 Edge 節點進入和離開。

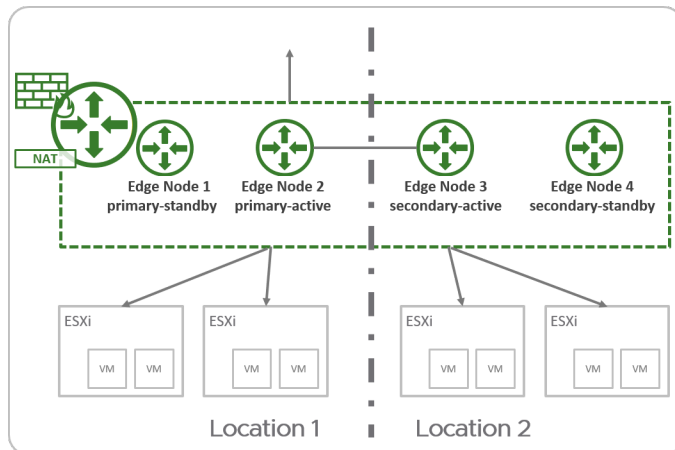
重要 此拓撲會允許流量從每個位置本機出口。您必須確保傳回流量進入相同位置，以允許可設定狀態的服務，例如防火牆。例如，您可以設定位置特定的 NAT IP，讓傳回流量一律會路由回其離開的相同位置。



具有主要和次要位置的延伸主動備用第 0 層閘道

在具有主要和次要位置的延伸主動備用第 0 層閘道中，適用下列項目：

- 一次僅有一個 Edge 節點為作用中，因此第 0 層可以執行可設定狀態的服務。
- 所有流量會透過主要位置的作用中 Edge 節點進入和離開。



對於主動備用第 0 層閘道，支援下列服務：

- 網路位址轉譯 (NAT)
- 閘道防火牆
- DNS
- DHCP

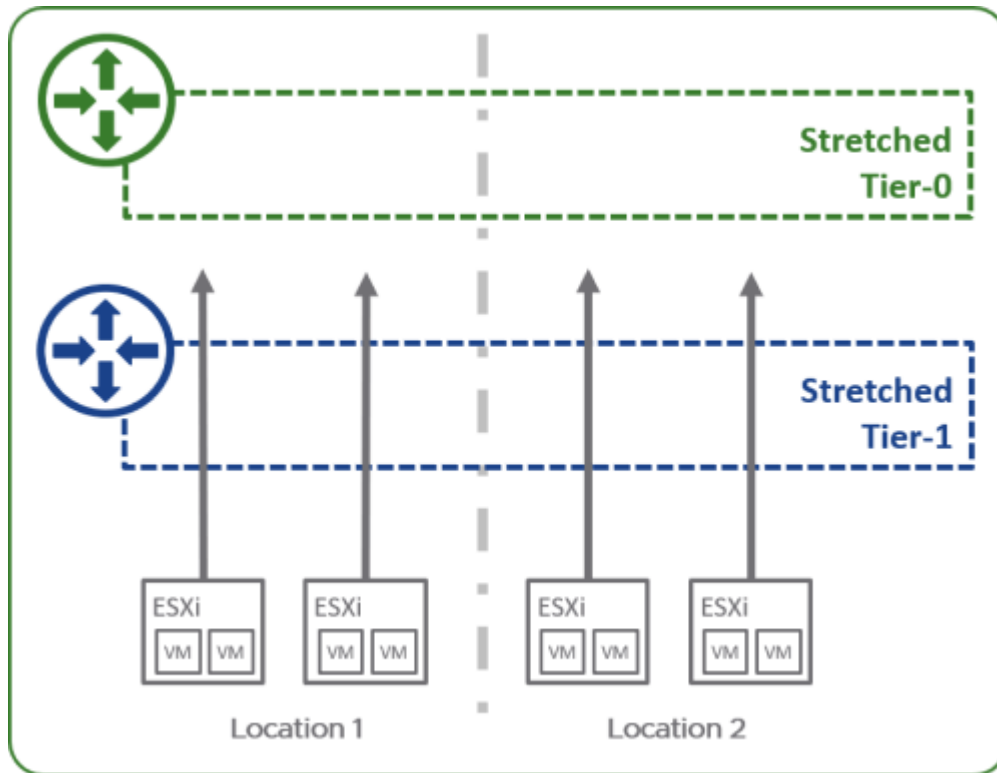
如需詳細資訊，請參閱[聯盟中支援的功能和組態](#)。

聯盟中的第 1 層閘道組態

透過 NSX 聯盟，您可以部署第 1 層閘道以僅提供分散式路由，也可以在其上設定服務。

僅適用分散式路由的第 1 層閘道

您可以在聯盟中建立僅適用分散式路由的第 1 層閘道。此閘道的範圍與其連結的第 0 層閘道相同。第 1 層不使用 Edge 節點進行路由。所有流量會從主機傳輸節點路由到第 0 層閘道。但是，若要啟用跨位置傳送，第 1 層會從連結的第 0 層上設定的 Edge 叢集配置兩個 Edge 節點，以用於該流量。



具有服務或自訂範圍的第 1 層閘道

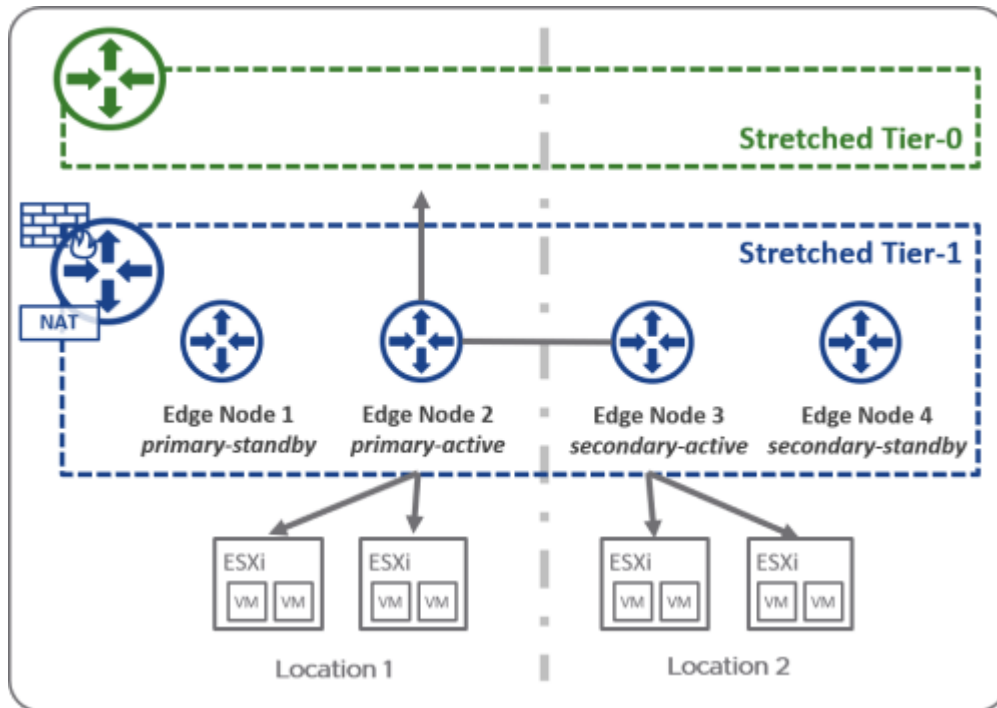
如果您需要下列其中一種組態，您可以設定第 1 層閘道搭配 Edge 叢集：

- 您想要在第 1 層閘道上執行服務。
- 您想要部署的第 1 層閘道的範圍與連結的第 0 層閘道不同。

您可以移除位置，但無法新增尚未包含在第 0 層閘道範圍內的位置。

您可以選取其中一個位置做為主要位置。所有其他位置均為次要。第 1 層閘道的 HA 模式為主動備用。透過此第 1 層閘道傳遞的所有流量，都將透過主要位置中的作用中 Edge 節點進行傳遞。

如果第 1 層閘道和連結的第 0 層閘道都有主要和次要位置，請將這兩個閘道的相同位置設定為主要，以減少跨位置流量。



設定延伸網路的 Edge 節點

如果您想要建立跨越多個位置的閘道和區段，您必須在每個位置的 Edge 節點上設定遠端通道端點 (RTEP)，以處理跨位置流量。

設定 RTEP 時，請以 Edge 叢集為基礎設定。叢集中的所有 Edge 節點必須已設定 RTEP。您不需要使用 RTEP 設定所有 Edge 叢集。僅當 Edge 叢集用於設定跨越多個位置的閘道時，才需要 RTEP。

您可以設定 TEP 和 RTEP，以使用 Edge 節點上的相同實體 NIC，或使用不同的實體 NIC。

您也可以從每個本機管理程式設定 RTEP。選取**系統 > 開始使用 > 設定遠端通道端點**。

您可以在 Edge 節點上編輯 RTEP。登入本機管理程式，然後選取**系統 > 網狀架構 > 網狀節點 > Edge 傳輸節點**。選取 Edge 節點，然後按一下**通道**。如果已設定 RTEP，則會顯示在**遠端通道端點**區段中。按一下**編輯**以修改 RTEP 組態。

必要條件

- 確認參與延伸網路的每個位置都至少有一個 Edge 叢集。
- 判定要用於 RTEP 網路的第 3 層網路和 VLAN。
 - 內部位置通道端點 (TEP) 和位置間通道端點 (RTEP) 必須使用不同的 VLAN 和第 3 層子網路。
- 確認在指定的聯盟環境中使用的所有 RTEP 網路彼此有 IP 連線。
- 確認外部防火牆允許跨位置 RTEP 通道，以及 Edge 之間的 BGP 工作階段。請參閱 VMware 連接埠和通訊協定，網址是 <https://ports.vmware.com/home/NSX-T-Data-Center>。
- 在每個本機管理程式上設定 RTEP 的 MTU。預設值為 1500。將 RTEP MTU 的值設定為與實體網路支援的值一樣高。在每個本機管理程式上，選取**系統 > 網狀架構 > 設定**。按一下**遠端通道端點**旁的**編輯**。

程序

- 1 從瀏覽器以管理員權限登入主動全域管理程式，網址為 <https://<global-manager-ip-address>>。
- 2 移至**系統 > 位置管理程式**，然後按一下您要設定延伸網路之位置的**網路**。
- 3 按一下您要為其設定 RTEP 的 Edge 叢集旁的**設定**。

本機管理程式中會開啟**設定延伸網路的 Edge 節點**畫面，並且該 Edge 叢集已選取。

- 4 您可以選取此叢集中的所有 Edge 節點，也可以一次選取一個節點。針對 RTEP 組態提供下列詳細資料：

選項	說明
主機交換器	從下拉式功能表中選取主機交換器。
整併原則	如果已設定一個整併原則，請選取該整併原則。
RTEP VLAN	輸入 RTEP 網路的 VLAN 識別碼。有效值介於 1 到 4094 之間。
所有節點的 IP 集區	選取此 Edge 叢集中所有節點的 IP 集區。如果您想要將 IP 位址指派給個別節點，可以稍後編輯 RTEP 組態。
位置間 MTU	預設值為 1500。

- 5 按一下**儲存**。

您可以按一下標記為「已設定」的每個 Edge 節點，以查看 Edge 節點的組態詳細資料。選取**通道索引**標籤，以檢視和編輯 RTEP 組態。

從全域管理程式新增第 0 層閘道

您可以從全域管理程式新增第 0 層閘道。此閘道可以有一或多個位置的範圍。此範圍會影響第 1 層閘道和與它連結區段的範圍。

如需有關 NSX 聯盟中第 0 層閘道組態的詳細資料，請參閱 [NSX 聯盟中的第 0 層閘道組態](#)。

下列設定必須在位置之間保持一致。如果您從全域管理程式 Web 介面變更這些設定，則這些變更會自動套用到所有位置。但是，如果您使用 API 變更這些設定，則必須在每個位置手動進行相同的變更。

- 本機 AS
- ECMP 設定
- 多重路徑放鬆設定
- 正常重新啟動

重要 從全域管理程式建立第 0 層閘道時，您必須在第 0 層延伸到的每個位置中設定外部介面。每個外部介面必須與從全域管理程式建立的區段連線，**連線**設定為無，且**流量類型**設定為 VLAN。請參閱[從全域管理程式新增區段](#)。使用這些外部介面設定的 Edge 節點會用於位置間通訊，即使不需要北向通訊也是如此。

必要條件

- 如果要建立跨越多個位置的第 0 層閘道，請確認每個位置都有 Edge 節點設定為使用 RTEP 進行延伸網路。請參閱[設定延伸網路的 Edge 節點](#)。

程序

- 1 從瀏覽器以管理員權限登入主動全域管理程式，網址為 <https://<global-manager-ip-address>>。
- 2 選取 **網路 > 第 0 層閘道**。
- 3 輸入閘道的名稱。
- 4 選取要在每個位置內設定的 HA (高可用性) 模式。

預設模式為雙主動。在雙主動模式中，流量會在所有位置中的 Edge 節點間進行負載平衡。在主動備用模式中，選擇的 Edge 節點會處理每個位置中的流量。如果作用中節點失敗，則待命節點會變成作用中。

備註 從 NSX-T Data Center 3.0.1 中開始，支援主動備用第 0 層閘道。

- 5 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。

- 6 透過為每個位置提供下列詳細資料，以指定此第 0 層閘道的範圍。若要新增其他位置，請按一下 **新增位置**。

選項	說明
位置	從下拉式功能表中選取位置。
Edge 叢集	從此位置選取 Edge 叢集。 如果您正在設定延伸的第 0 層，則必須選取包含已設定 RTEP 之 Edge 節點的 Edge 叢集。
模式	第 0 層閘道的每個位置可以具有 主要 或 次要 模式。 <ul style="list-style-type: none"> ■ 如果 HA 模式為雙主動，則可以設定第 0 層閘道，將所有位置模式設定為主要。 <ol style="list-style-type: none"> 1 選取將所有位置標記為主要切換，以將所有位置標記為主要。 ■ 如果 HA 模式為雙主動或主動備用，則可以設定第 0 層閘道，並將其中一個位置設為主要，然後將所有其他位置設為次要。 <ol style="list-style-type: none"> 1 對於一個位置選取主要模式。在所有其他位置中，將模式設為次要。 2 對於次要位置，您必須選取一個後援喜好設定。

7 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 169.254.0.0/24。

- b 在**TO-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 在**站台間傳送子網路**欄位中，輸入子網路。這是閘道元件之間的跨位置通訊所使用的子網路。預設值為 169.254.32.0/20。

8 按一下**儲存**。

- 9 若要設定介面，請按一下**介面和設定**。為第 0 層閘道跨越的每個位置設定一個外部介面。

- a 按一下**新增介面**。

- b 輸入名稱。

- c 選取位置。

- d 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**。

僅跨越一個位置的閘道上才支援服務介面。如果已延伸閘道，則不支援服務介面。

- e 以 CIDR 格式輸入 IP 位址。

- f 選取區段。

區段的建立必須透過全域管理程式，**連線**設定為無，且**流量類型**設定為 VLAN。請參閱[從全域管理程式新增區段](#)。

- g 如果介面類型不是**服務**，請選取 NSX Edge 節點。

- h (選擇性) 如果介面類型不是**回送**，請輸入 MTU 值。

- i 略過 **PIM** 組態。

聯盟中不支援多點傳播。

- j (選擇性) 新增標籤，然後選取 ND 設定檔。

- k (選擇性) 如果介面類型為**外部**，則對於 **URPF 模式**，您可以選取**嚴格**或**無**。

URPF (單點傳播反向路徑轉送) 是一項安全功能。

- l 建立介面之後，您可以透過按一下介面的功能表圖示 (三個點)，然後選取**下載 ARP 資料表**來下載 ARP 資料表。

10 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。

當您在第 0 層閘道上新增靜態路由時，預設行為是將靜態路由推送至閘道上設定的所有位置。但是，路由僅會在主要位置上啟用。這可確保在次要位置上，從主要位置學習的路由為慣用。

如果想要變更此行為，可以使用**已在次要位置上啟用設定**和**範圍**設定。

如果選取**已在次要位置上啟用**，則在次要位置上也會啟用靜態路由。

新增靜態路由的下一個躍點時，您可以設定**範圍**。範圍可以是介面、閘道或區段。在從全域管理程式建立的第 0 層閘道上，範圍也可以是位置。您可以使用範圍設定為每個位置設定不同的下一個躍點。

11 按一下**BGP**以設定 BGP。

當您從全域管理程式設定第 0 層閘道上的 BGP 時，多數設定會套用至所有位置。

BGP 組態中的部分設定 (例如**路由彙總**和**BGP 芳鄰**) 會提示您為每個位置提供不同的值。

如需設定 BGP 的詳細資訊，請參閱**設定 BGP**。

12 若要設定路由重新分配，請按一下**路由重新分配**，並針對每個位置按一下**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**、**EVPN TEP 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**。

後續步驟

從全域管理程式設定第 1 層閘道。

從全域管理程式新增第 1 層閘道

您可在一或多個位置中設定閘道。這些位置是閘道的範圍。第 1 層閘道的範圍不能大於其連線到的第 0 層閘道。

如需有關 NSX 聯盟中第 1 層閘道組態選項的詳細資料，請參閱**聯盟中的第 1 層閘道組態**。

必要條件

確認您已設定第 0 層閘道。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<global-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。
 - 如果您選取第 0 層閘道，則位置組態會填入在第 0 層上設定的相同位置。如有需要，您可以在 [位置] 區段中修改位置組態。
 - 如果您未選取第 0 層閘道，則可以選取位置。但是，如果您稍後將第 1 層閘道連線至第 0 層閘道，您可能需要更新位置，才能建立有效的組態。
- 6 在位置中，您可以變更為服務或自訂範圍啟用 Edge 叢集設定。此設定依預設為停用。
 - 如果您想要第 1 層閘道具有與第 0 層閘道相同的範圍，且不需在第 1 層閘道上啟用服務，請將為服務或自訂範圍啟用 Edge 叢集保持為已停用。第 1 層閘道將僅執行分散式路由。
 - 如果您想要為第 1 層閘道選擇位置子集，或如果您想要在第 1 層閘道上啟用服務，請啟用為服務或自訂範圍啟用 Edge 叢集。

如果您啟用為服務或自訂範圍啟用 Edge 叢集，請輸入位置、叢集和模式資訊。

- a 從下拉式功能表中選取位置。如果您將此第 1 層閘道連結至第 0 層閘道，則會自動列出該第 0 層閘道的位置。如有需要，您可以刪除位置。
 - b 選取每個位置的 NSX Edge 叢集。如果第 1 層閘道跨越多個位置，則必須已針對其每個 Edge 節點設定使用 RTEP 的 Edge 叢集。
 - c (選擇性) 若要選取特定的 Edge 節點，請按一下 Edge 叢集旁的設定。
如果未選取 Edge 節點，則會自動配置 Edge 節點。
 - d 選取每個位置的模式。模式可以是主要或次要。
僅可將一個位置設定為主要模式。來自此第 1 層閘道的所有北向流量都會透過此位置傳送。
- 7 如果您啟用了 Edge 叢集，請選取容錯移轉模式。

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。

- 8 略過從 Edge 集區配置大小下拉式功能表中選取大小。
- 9 如果已啟用 Edge 叢集，請選取啟用待命重新放置設定。

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 (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

11 按一下**儲存**。12 (選擇性) 按一下**路由通告**。

- a 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。

13 (選擇性) 按一下**其他設定**。

- a 對於 IPv6，您可以選取或建立 **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)。

- b 選取入口 **QoS 設定檔**和出口 **QoS 設定檔**以瞭解流量限制。

這些設定檔可用來設定允許流量的資訊速率和高載大小。如需如何建立 QoS 設定檔的詳細資訊，請參閱[新增閘道 QoS 設定檔](#)。

如果此閘道連結至第 0 層閘道，則**路由器連結**欄位會顯示連結位址。

14 (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。

僅跨越一個位置的閘道上才支援服務介面。如果已延伸閘道，則不支援服務介面。

- 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 對於 **URPF 模式**，您可以選取**嚴格**或**無**。
URPF (單點傳播反向路徑轉送) 是一項安全功能。
- f 新增一或多個標籤。
- g 在 **ND 設定檔**欄位中，選取或建立設定檔。
- h 按一下**儲存**。

15 (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**。

從全域管理程式新增區段

您可以新增兩種區段：支援覆疊的區段和支援 VLAN 的區段。從全域管理程式建立區段時，僅支援覆疊的區段可跨多個位置。

您可以從全域管理程式檢視區段連接埠，但無法建立或修改這些連接埠。如果您需要建立或修改區段連接埠，則必須從本機管理程式進行。

重要 請勿變更聯盟中區段的閘道連線。變更閘道會影響區段的範圍。如果範圍以排除位置的方式變更，則會在排除的位置刪除該區段。您必須先中斷所有虛擬機器的連線，然後再縮小區段的範圍。

必要條件

確認每個位置均已設定預設的覆疊傳輸區域。預設覆疊傳輸區域會用於建立全域覆疊區段。從每個本機管理程式，選取**系統 > 網狀架構 > 傳輸區域**。選取覆疊傳輸區域，然後按一下**動作 > 設定為預設傳輸區域**。

程序

- 1 從瀏覽器以管理員權限登入全域管理程式，網址為 <https://<global-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 選取此區段的連線、流量類型和位置。

表 15-3. 區段組態

連線	流量類型	位置和傳輸區域	詳細資料
全域第 0 層或第 1 層閘道	覆疊	位置區段會填入下列組態： <ul style="list-style-type: none"> ■ 在連結的閘道上設定的相同位置。 ■ 每個位置的預設覆疊傳輸區域。 	使用此組態來建立連線至所選全域閘道的支援全域覆疊區段。
無	VLAN	您必須為此區段選取一個位置。您也必須從該位置選取一個傳輸區域。	使用此組態來建立全域支援 VLAN 的區段，以用於第 0 層外部介面。
無	覆疊	無法選取位置或傳輸區域。	此區段是在全域管理程式上建立，但未在任何本機管理程式中實現。您可以稍後將其連結至閘道。

不支援建立連結至閘道的支援 VLAN 區段。

6 輸入 CIDR 格式的子網路閘道 IP 位址。區段可包含 IPv4 子網路或 IPv6 子網路，或兩者。

- 如果區段未連線至閘道，則子網路為選用。
- 如果區段已連線至第 1 層或第 0 層閘道，則需要子網路。

某個區段的子網路不得與您網路中其他區段的子網路重疊。區段一律會與單一虛擬網路識別碼 (VNI) 相關聯，無論其是否已設定一個子網路、兩個子網路或無子網路。

7 略過設定 DHCP 組態。

在從全域管理程式建立的區段上僅支援靜態繫結。請參閱[聯盟中支援的功能和組態](#)。

8 如果傳輸區域的類型是 VLAN，請指定 VLAN 識別碼的清單。如果傳輸區域的類型是「覆疊」，且您想要支援第 2 層橋接或客體 VLAN 標記，請指定 VLAN 識別碼的清單或 VLAN 範圍

9 (選擇性) 選取區段的上行整併原則。

如果您已將其新增至 VLAN 傳輸區域，則此下拉式功能表會顯示具名整併原則。如果未選取任何上行整併原則，則會使用預設整併原則。

- 具名整併原則不適用於覆疊區段。覆疊區段一律遵循預設整併原則。
- 對於支援 VLAN 的區段，您有彈性可使用所選的具名整併原則來覆寫預設整併原則。系統提供此功能，因此您可以將主機的基礎結構流量導向至 VLAN 傳輸區域中的特定 VLAN 區段。在新增 VLAN 區段之前，請確保在 VLAN 傳輸區域中新增具名整併原則名稱。

10 按一下**儲存**。

11 若要繼續設定區段，請在出現提示時按一下**是**。


12 若要選取區段設定檔，請按一下**區段設定檔**。

13 若要將靜態 IP 位址繫結至區段上虛擬機器的 MAC 位址，請展開**DHCP 靜態繫結**，然後按一下**設定**。

14 按一下**儲存**。

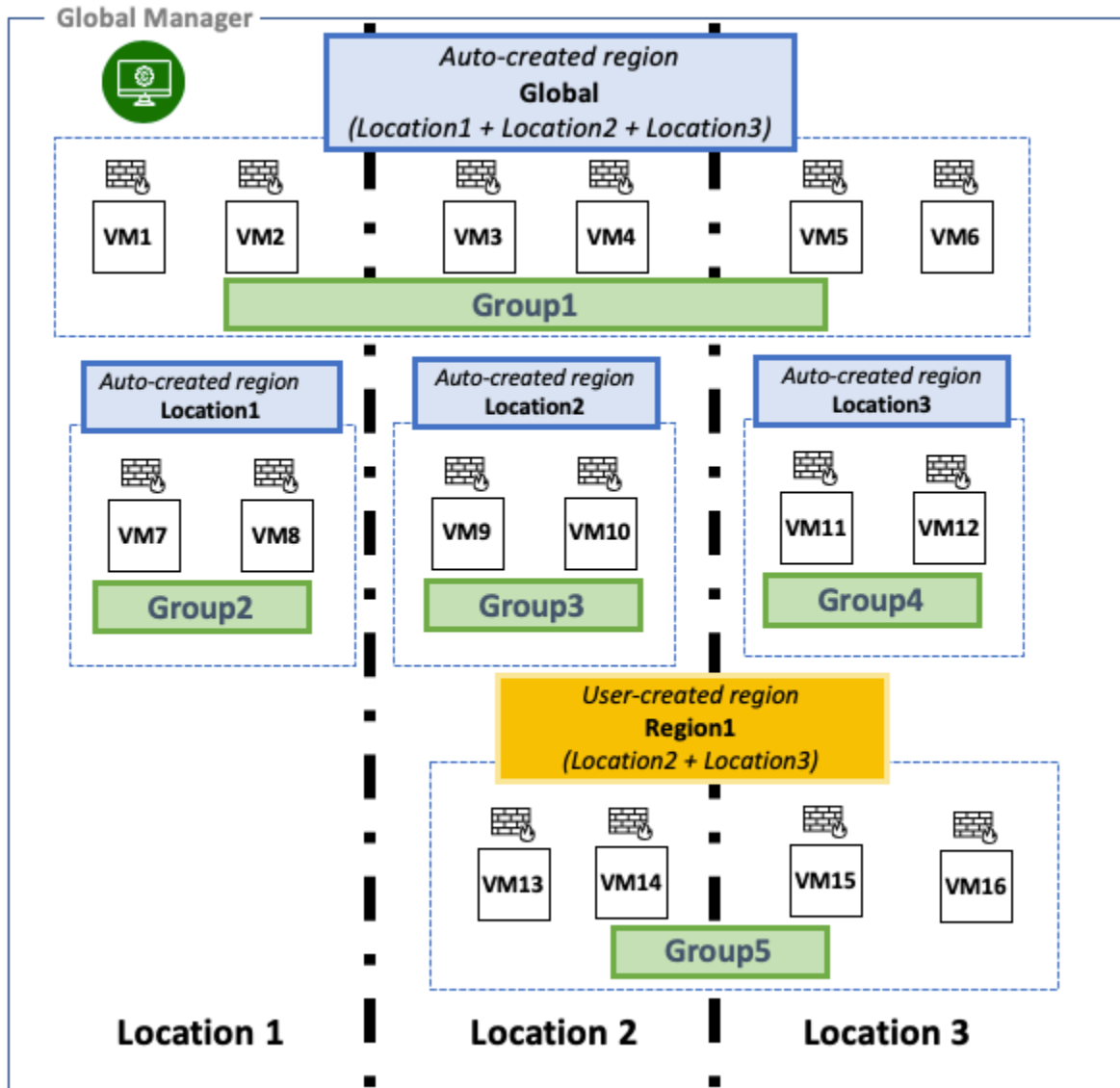
NSX 聯盟中的安全性

您可以從具有全域、區域或本機範圍的全域管理程式建立分散式和閘道防火牆規則。

從全域管理程式建立的分散式和閘道防火牆原則和規則，會同步至本機管理程式並顯示在具有  圖示的本機管理程式中。您只能從全域管理程式編輯從全域管理程式建立的規則。無法從本機管理程式進行編輯。

分散式防火牆 (DFW) 原則和規則的聯盟

使用此範例來瞭解支援的防火牆工作流程：



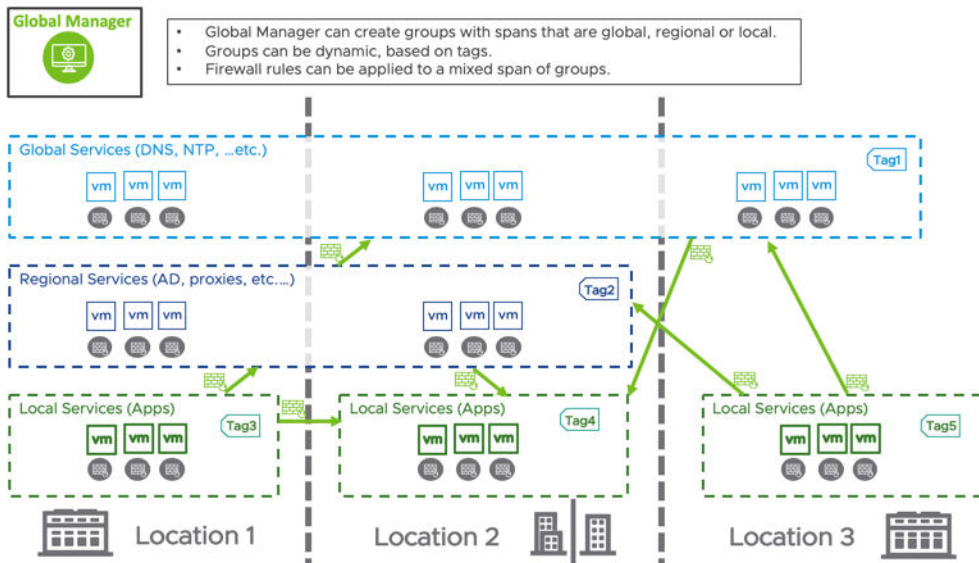
- 在此範例中，全域管理程式有已向其登錄的三個本機管理程式，名為：*Location1*、*Location2* 和 *Location3*。
- 全域管理程式會自動建立下列區域：
 - 全域
 - *Location1*
 - *Location2*
 - *Location3*
- 您可以建立名為 **Region1** 的自訂區域，其中包含名為 *Location2* 和 *Location3* 的本機管理程式。
- 您可以建立下列群組：
 - **Group1**：區域 *Global*。

- Group2 : 區域 Location1。
- Group3 : 區域 Location2。
- Group4 : 區域 Location3。
- Group5 : 區域 Region1。

NSX-T Data Center 3.0.1 中的 DFW 原則和規則

支援下列使用案例：

- **群組範圍**：您可以在具有全域、本機或區域範圍的全域管理程式中建立群組。請參閱[從全域管理程式建立群組](#)。
- **動態群組**：您可以根據動態準則 (例如標籤) 建立群組。
- **DFW 原則範圍**：DFW 原則可套用至全域、區域或本機範圍。
- **DFW 規則的來源和目的地群組**：來源欄位中的所有群組或目的地欄位中的所有群組都必須符合 DFW 原則的範圍。系統會在原則範圍以外的位置自動建立群組。



請參閱資料表以取得 DFW 規則中有效和無效來源和目的地群組的範例：

表 15-4. 3.0.1 中基於 DFW 原則範圍的 DFW 規則的有效來源和目的地

DFW 原則範圍 (適用於)	3.0.1 版 DFW 規則中支援的案例。
<p><i>全域</i></p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group1 	<p>對於具有全域區域範圍的 DFW 原則，DFW 規則的來源和目的地中允許所有群組。以下是一些支援的典型示例，使用我們的範例：</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group3 ■ 來源：Group3；目的地：Group4 ■ 來源：Group4；目的地：Any ■ 來源：Group1；目的地：Group2。
<p><i>Location1</i>：在位置 1 中，為本機管理程式自動建立的區域。</p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group2 	<p>對於具有單一位置範圍的 DFW 原則：此範例中的 <i>Location1</i>，無論是 DFW 規則的來源或目的地群組，皆必須屬於 <i>Location1</i>。</p> <p>支援下列示例：</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group2 ■ 來源：Group3；目的地：Group2。 ■ 來源：Group2；目的地：Group4。 ■ 來源：Group1；目的地：Group2。 <p>以下是此原則範圍不支援群組選取項目的範例。來源和目的地群組均不在原則的範圍內：</p> <ul style="list-style-type: none"> ■ 來源：Group5；目的地：Group3。 ■ 來源：Group1；目的地：Group3。
<p><i>Region1</i>：使用者建立的區域，跨越 <i>Location2</i> 和 <i>Location3</i>。</p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group5 	<p>對於具有使用者所建立區域範圍的 DFW 原則：此範例中的 <i>Region1</i>，無論是 DFW 規則的來源或目的地群組，皆必須包含屬於 <i>Region1</i> 的位置。</p> <p>支援下列示例：</p> <ul style="list-style-type: none"> ■ 來源：Group5；目的地：Group2。 ■ 來源：Group2；目的地：Group5。 ■ 來源：Group2；目的地：Group3。 ■ 來源：Group3；目的地：Group4。 ■ 來源：Any；目的地：Group5 ■ 來源：Group4；目的地：Any <p>以下是此原則範圍不支援群組選取項目的範例。來源和目的地群組均不在原則的範圍內：</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group2。 ■ 來源：Group1；目的地：Group2。 ■ 來源：Group1；目的地：Group1。

- 如果群組包含區段，則 DFW 原則的範圍必須大於或等於區段的範圍。例如，如果群組包含範圍為 *Location1* 的區段，則無法將 DFW 原則套用至區域 *Region1*，因為它僅包含 *Location2* 和 *Location3*。

NSX-T Data Center 3.0.0 中的 DFW 原則和規則

- **群組範圍**：您可以在具有全域、本機或區域範圍的全域管理程式中建立群組。請參閱[從全域管理程式建立群組](#)。
- **動態群組**：您可以根據動態準則 (例如標籤) 建立群組。
- **DFW 原則範圍**：DFW 原則也可套用至全域、區域或本機範圍。
- **DFW 規則的來源和目的地群組**：來源欄位中的所有群組和目的地欄位中的所有群組都必須符合 DFW 原則的範圍。

請參閱資料表，瞭解原則範圍如何判定 DFW 規則中的來源和目的地群組是否有效。

表 15-5. 3.0.0 中基於 DFW 原則範圍的 DFW 規則的有效來源和目的地

DFW 原則範圍 (適用於)	3.0.0 版 DFW 規則中支援的來源和目的地群組。
<p>全域。</p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group1 	<p>對於跨越至全域區域的 DFW 原則，您可以在 DFW 規則的來源和目的地中選取關鍵字 Any 或 Global 群組：</p> <p>例如，</p> <ul style="list-style-type: none"> ■ 來源：Group1；目的地：Group1。 ■ 來源：Group1；目的地：Any ■ 來源：Any；目的地：Group1。 ■ 來源：Any；目的地：Any <p>注意 可以建立但不支援的其他規則組態，例如： .</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group3 ■ 來源：Group4；目的地：Group1
<p>Location1：在位置 1 中，為本機管理程式自動建立的區域。</p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group2 	<p>對於跨越一個位置區域的 DFW 原則：此範例中的 Location1，來源和目的地群組都必須屬於此區域。</p> <p>例如，支援下列規則：</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group2 <p>注意 可以建立但不支援的其他規則組態，例如： .</p> <ul style="list-style-type: none"> ■ 來源：Group2；目的地：Group3 ■ 來源：Group4；目的地：Group2
<p>Region1：跨越 Location2 和 Location3 的自訂區域。</p> <p>從此範例，此區域包含下列群組：</p> <ul style="list-style-type: none"> ■ Group5 	<p>對於跨越至自訂區域的 DFW 原則：此範例中的 Region1，來源和目的地群組都必須屬於此區域。</p> <p>例如，支援下列規則：</p> <ul style="list-style-type: none"> ■ 來源：Group5；目的地：Group5。 ■ 來源：Group5；目的地：Any。 ■ 來源：Any；目的地：Group5。 <p>注意 可以建立但不支援的其他規則組態，例如： .</p> <ul style="list-style-type: none"> ■ 來源：Group2 和目的地：Group3 ■ 來源：Group2；目的地：Group4 ■ 來源：Group3；目的地：Group2 ■ 來源：Group4；目的地：Group2

- 如果群組包含區段，則 DFW 原則的範圍必須大於或等於區段的範圍。例如，如果群組包含範圍為 *Location1* 的區段，則無法將 DFW 原則套用至區域 **Region1**，因為它僅包含 *Location2* 和 *Location3*。

閘道防火牆原則和規則的聯盟

閘道防火牆規則可套用至閘道範圍內包含的所有位置、特定位置的所有介面，或一或多個位置的特定介面。

備註 閘道防火牆規則的來源和目的地群組範圍，必須與您要在其上建立規則的閘道範圍的子集相同。

表 15-6. 閘道防火牆規則的範圍選項

閘道防火牆規則的範圍 (適用於)	套用至
將規則套用至閘道	此規則會套用至此閘道延伸的所有位置中，連結至此閘道的所有介面。
選取位置，然後選取 [將規則套用至所有實體]。	此規則僅會套用至選取的位置。
選取位置，然後選取來自該位置的介面。針對其他位置重複上述步驟，選取要套用規則的每個位置的介面。	此規則僅會套用至選取的介面。

從全域管理程式建立區域

新增至全域管理程式的每個位置會自動成為區域。您也可以建立自訂區域。

使用區域來建立安全性和網路原則的重點群組。在全域管理程式中將位置上線後，部分區域會自動建立。您可以視需要新增更多區域。

備註 每個位置只能是一個自訂區域的一部分。

依預設會新增下列區域：

- 全域區域，包括新增至全域管理程式的所有位置。
- 新增至全域管理程式的每個位置都有一個區域。

對於現有區域，您可以檢視下列資訊：

- 區域的名稱。
- 區域中包含的位置。
- 區域所屬的群組。
- 區域所屬的安全性/網路原則。

必要條件

請參閱 [NSX 聯盟中的安全性](#)，以取得有關區域和群組的範圍在建立和維護安全性原則與規則方面的含義詳細資料。

程序

- 1 選取 **詳細目錄 > 區域**。

- 2 按一下**新增區域**。
- 3 請提供下列資訊：

選項	說明
名稱	提供區域的名稱，例如，EMEA 或 APAC。
位置	選取要包含在此區域中的位置。

- 4 按一下**儲存**。

具有指定位置的區域將會建立。

後續步驟

[從全域管理程式建立群組](#)。

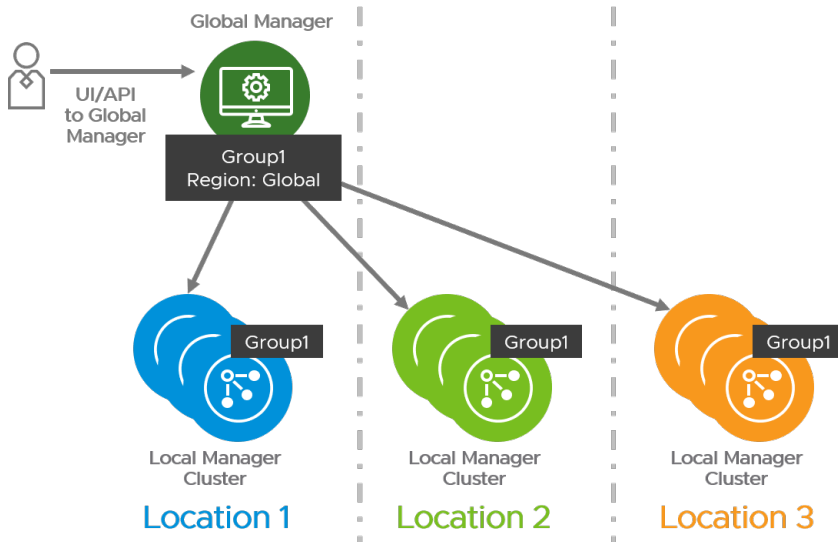
從全域管理程式建立群組

從全域管理程式建立可在 NSX-T Data Center 部署中全域套用或涵蓋所選位置或區域的群組。

群組範圍

當您從全域管理程式建立群組時，您可以為該群組選取一個區域。群組會與該區域中的所有位置同步。全域區域會包含所有位置，而已新增至全域管理程式之每個位置的區域，皆會自動成為您可為群組範圍選取的區域。您可以先建立自訂區域，然後再建立群組。請參閱[從全域管理程式建立區域](#)。

在此範例中，系統將在全域區域中建立 **Group1**，因此會與所有本機管理程式同步。



動態群組

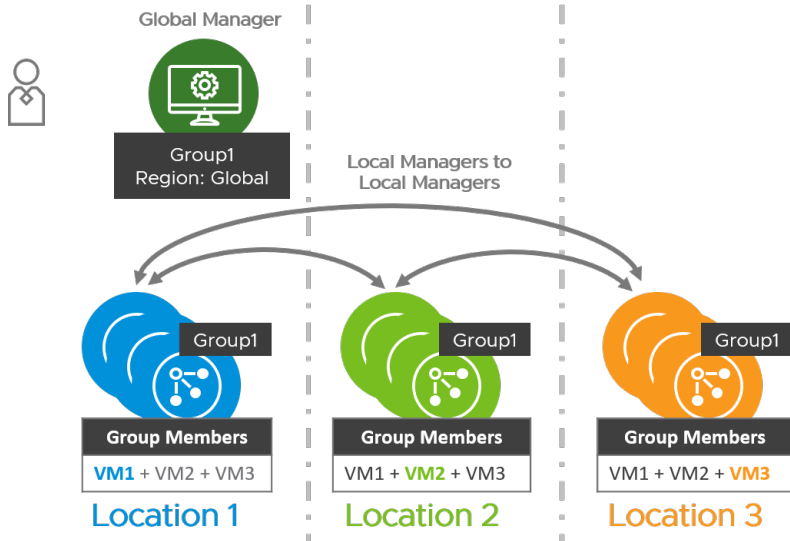
如果跨越多個位置的群組具有動態成員資格，則您需要來自每個位置的資訊，才能列出群組成員資格。

在此範例中，**Group1** 具有下列成員：

- *Location1* 中的 **VM1**

- *Location2* 中的 VM2
- *Location3* 中的 VM3

每個本機管理程式會將其動態群組成員資格與其他本機管理程式同步。因此，每個本機管理程式都有完整的群組成員清單。



巢狀群組

對於從全域管理程式建立的群組，如果範圍等於或小於群組的區域，則可以新增另一個群組作為成員。

備註 如果您使用 NSX-T Data Center 版本 3.0.0，則僅在這兩個群組的範圍完全一致時，才能將群組新增為另一個群組的成員。

使用包含 *Location2* 和 *Location3* 的 **Region1** 來延伸範例時，請注意下列其他組態：

工作	效果
從全域管理程式，建立具有區域 <i>Location2</i> 的 Group-Loc2 。	<ul style="list-style-type: none"> ■ 在全域管理程式中建立 Group-Loc2。 ■ 在本機管理程式 <i>Location2</i> 中建立 Group-Loc2。
從全域管理程式，建立具有區域 Region1 的群組 Group-Region1 。將 Group-Loc2 新增為成員。這是一個巢狀群組。	<ul style="list-style-type: none"> ■ 在全域管理程式中建立 Group-Region1。 ■ 在 <i>Location2</i> 和 <i>Location3</i> 中建立 Group-Region1。 ■ 在本機管理程式 <i>Location3</i> 中建立 Group-Loc2。
在全域管理程式中，導覽至詳細目錄 > 區域並編輯 Region1 ，以移除 <i>Location2</i> 。	因為巢狀群組 Group-Region1 而不允許此動作。

如需建立群組的詳細步驟，請參閱[新增群組](#)。

從全域管理程式建立 DFW 原則和規則

您可以建立安全性原則和 DFW 規則，將其套用至向全域管理程式登錄的多個位置。

必要條件

確定您已建立要用於防火牆規則的任何自訂區域。請參閱[從全域管理程式建立區域](#)。

程序

- 1 從瀏覽器以企業管理員或安全管理員權限登入全域管理程式，網址為 <https://<global-manager-ip-address>>。
- 2 選取**安全性 > 分散式防火牆**
- 3 確定您是位於正確的預先定義類別，然後按一下**新增原則**。如需類別的詳細資訊，請參閱[分散式防火牆](#)。

備註 全域管理程式 不支援乙太網路、緊急類別和預設原則。

- 4 按一下**新增原則**。
- 5 為新的原則區段輸入**名稱**。
- 6 按一下**套用至**旁的鉛筆圖示，以設定此原則的範圍。
- 7 在設定 **[套用至]** 對話方塊中，您可以進行下列選取項目：
 - **區域**：選取要套用原則的本機管理程式。每個本機管理程式會自動新增為區域。您也可以建立自訂區域。請參閱[從全域管理程式建立區域](#)。
 - **選取 [套用至]**：依預設，原則會套用至 **DFW**，也就是說，原則會根據為此原則選取的區域套用到本機管理程式上的所有工作負載。您也可以將原則套用到選取的群組。「**套用至**」會定義每個原則的強制執行範圍，主要用於 ESXi 與 KVM 主機上的資源最佳化。這有助於為特定的區域、承租人和應用程式定義針對性的原則，卻不干擾為其他承租人、區域和應用程式定義的其他原則。

請參閱 [NSX-T Data Center 3.0.1 中的 DFW 原則和規則](#)，瞭解原則範圍如何判斷您的 DFW 規則是否有效或無效。

8 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>

9 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。

10 選取原則區段，然後按一下**新增規則**。

11 輸入規則的名稱。

12 來源和目的地會根據 DFW 原則的範圍進行驗證。如需詳細資訊，請參閱 [NSX-T Data Center 3.0.1 中的 DFW 原則和規則](#)。

- 如果將 DFW 原則套用至某個位置 (例如 `Loc1`)，則來源或目的地可以是關鍵字 **ANY** 或屬於 `Loc1` 的群組。
- 如果將 DFW 原則套用至使用者建立的區域 (例如 `Region1`)，則來源或目的地可以是關鍵字 **ANY**，或範圍與 `Region1` 相同或跨越 `Region1` 內位置的群組。
- 如果將 DFW 原則套用至**全域**，則來源或目的地可以是任何項目。

備註 NSX 聯盟不支援 Active Directory 和 IDFW，也就是說，您無法從全域管理程式使用這些功能。

a 在**來源**資料行中按一下鉛筆圖示，然後選取規則的來源。

b 在**目的地**資料行中按一下鉛筆圖示，然後選取規則的目的地。若未定義，則代表不分目的地。

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**。
- 15 按一下**套用**，將內容設定檔套用至規則。
- 16 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 主機上的資源最佳化。這有助於為特定的區域、承租人和應用程式定義針對性的原則，卻不干擾為其他承租人、區域和應用程式定義的其他原則。

備註 在**套用至**中，您無法選取下列類型的群組：

- 具有 IP 或 MAC 位址的群組
- Active Directory 使用者群組

- 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 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。

- 18 按一下**切換**按鈕以啟用或停用規則。
- 19 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 <code>/var/log/dfwpktlogs.log</code> 中。
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，防火牆記錄中會出現記錄標籤。

- 20 按一下**發佈**。可以新增多個規則，然後一同發佈。
- 21 在每個原則上，按一下**檢查狀態**，以根據每個位置檢視其包含的規則狀態。您可以按一下**成功**或**失敗**以開啟原則狀態視窗。
- 22 按一下**檢查狀態**，以檢查對不同位置上的傳輸節點套用之原則的實現狀態。

從全域管理程式建立閘道原則和規則

您可以從全域管理程式建立要套用至多個位置或特定位置所選介面的閘道防火牆原則和規則。

從全域管理程式建立的第 0 層或第 1 層閘道會涵蓋所有或一組位置。套用從全域管理程式建立的閘道防火牆規則時，您有幾個選項：閘道防火牆規則可套用至閘道範圍內包含的所有位置、特定位置的所有介面，或一或多個位置的特定介面。

在本機管理程式上，規則依下列順序強制執行：

- 1 您從全域管理程式建立的任何可在本機管理程式上成功實現的規則，會優先強制執行。
- 2 接著會強制執行從本機管理程式建立的任何規則。
- 3 上次強制執行的規則是預設的閘道防火牆規則。這是適用於所有位置和所有工作負載的全部允許或全部拒絕規則。您可以從全域管理程式編輯此預設規則的行為。

程序

- 1 從瀏覽器以企業管理員或安全管理員權限登入全域管理程式，網址為 `https://<global-manager-ip-address>`。
- 2 選取**安全性 > 閘道防火牆**。
- 3 確保您處於正確的預先定義類別。全域管理程式上僅支援**預先定義的規則、本機閘道和預設類別**。若要在**本機閘道**類別下定義原則，請按一下**所有共用的規則索引標籤**的類別名稱，或直接按一下**閘道特定規則索引標籤**。

從**閘道**旁的下拉式功能表中，選取第 0 層或第 1 層閘道。您選取的第 0 層或第 1 層閘道的範圍將成為閘道防火牆原則和規則的預設範圍。您可以減少範圍，但不能將其擴大。

- 4 按一下**新增原則**。
- 5 為新的原則區段輸入**名稱**。
- 6 (選擇性) 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。

- 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。來源群組必須具有閘道的相同範圍或其子集。
- 11 在**目的地**資料行中按一下**編輯圖示**，然後選取規則的目的地。若未定義，則代表不分目的地。目的地群組必須具有閘道的相同範圍或其子集。
- 12 在**服務**資料行中按一下**鉛筆圖示**，然後選取服務。若未定義，則服務會比對任何項目。按一下**套用**以儲存。
- 13 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](#)。

備註 第 0 層閘道不支援內容設定檔。您可以將 L7 內容設定檔套用至第 1 層閘道。

- 14 按一下**套用至**資料行中的**鉛筆圖示**。在**套用至**對話方塊中：

套用至選取項目	結果
選取將規則套用至閘道	閘道防火牆規則會套用至閘道範圍涵蓋的所有位置。如果將其他位置新增至閘道，則此閘道防火牆規則會自動套用至位置。
選取位置，然後選取將規則套用至所有實體	將此規則套用至所選位置中的所有介面。
選取位置，然後選取該位置的介面	僅將規則套用至一或多個位置中的所選介面。

備註 套用至沒有預設的選取項目。您必須進行選擇才能發佈此規則。

- 15 在**動作**資料行中，選取動作。

選項	說明
允許	允許具有指定來源、目的地和通訊協定的所有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。

- 16 按一下**狀態切換**按鈕以啟用或停用規則。

17 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	<p>可關閉或開啟記錄。您可以在 NSX Edge 上使用下列 NSX CLI 命令來存取記錄：</p> <pre>get log-file syslog find datapathd.firewallpkt</pre> <p>也可以將記錄傳送到外部 Syslog 伺服器。</p>
方向	<p>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。</p>
IP 通訊協定	<p>選項為IPv4、IPv6及IPv4_IPv6。預設為IPv4_IPv6。</p>
記錄標籤	<p>已新增至規則的記錄標籤。</p>

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。

18 按一下**發佈**。可以新增多個規則，然後一同發佈。

19 按一下**檢查狀態**來檢視透過不同位置的 Edge 節點，套用至閘道的原則實現狀態。您可以按一下**成功**或**失敗**以開啟原則狀態視窗。

在 NSX 聯盟中備份和還原

您可以從全域管理程式內為全域管理程式和每個本機管理程式設定和開始備份。

重要 從 NSX-T Data Center 3.0.1 開始，支援將全域管理程式還原為 FQDN。如果您使用 NSX-T Data Center 3.0.0，請勿將 FQDN 用於全域管理程式。僅 NSX-T Data Center 3.0.0 中的全域管理程式應用裝置支援 IP 位址備份。

- 登入作用中全域管理程式，然後選取**系統 > 備份與還原**。環境中的每個全域管理程式和本機管理程式隨即列出。如需指示，請參閱**設定備份**。
- 您無法從全域管理程式內還原本機管理程式。若要還原本機管理程式備份，請登入要還原的本機管理程式。如需指示，請參閱**還原備份**。
- 系統會將備份和還原作業視為每個應用裝置特定，無論您要備份或還原的是全域管理程式還是本機管理程式。全域管理程式的備份僅包含該應用裝置資料庫的備份。本機管理程式僅包含該應用裝置資料庫和詳細目錄的備份。
- 如果您要還原全域管理程式和本機管理程式，請盡可能選取每個應用裝置接近彼此的備份時間戳記。
- 每個應用裝置還原後，`async replicator` 服務會還原全域管理程式與每個本機管理程式之間的通訊。

聯盟中的還原案例

案例	還原工作流程
遺失全域管理程式。	還原 全域管理程式。還原後，全域管理程式會將組態推送至向其登錄的本機管理程式。
遺失本機管理程式。	還原 本機管理程式。還原時，來自全域管理程式的組態會與本機管理程式同步。
全域管理程式和本機管理程式都遺失。	<p>如果您要還原全域管理程式和本機管理程式，請使用每個應用裝置的最新備份。還原全域管理程式和本機管理程式時，全域管理程式會將組態推送至本機管理程式。</p> <p>您必須手動解決本機管理程式與全域管理程式之間的詳細目錄和網狀架構相關變更的任何差異。</p>

您可以監控 NSX-T Data Center 環境的健全狀況和效能。

本章節討論下列主題：

- [監控 NSX Edge 節點](#)
- [使用事件和警示](#)
- [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](#)

監控 NSX Edge 節點

您可以監控 NSX Edge 節點的資源使用量 (例如 CPU、記憶體和儲存區)。

從 NSX-T Data Center 3.0.1 開始，系統會顯示下列的額外資訊：

- 警示
 - Edge 節點 - 整體警示計數
 - CPU - 資料路徑 CPU 和服務 CPU 的警示
 - 磁碟 - 整體磁碟警示和每個磁碟分割的警示
 - 記憶體 - 整體記憶體警示和每個記憶體集區的警示
- CPU
 - 資料路徑 CPU - 資料路徑 CPU 核心數目及其使用量詳細資料，其中包括所有核心的平均使用量和核心之間的最高使用量。
 - 服務 CPU - 服務 CPU 核心數目及其使用量詳細資料，其中包括所有核心的平均使用量和核心之間的最高使用量。
- 磁碟
 - 所有 ext4 磁碟分割的磁碟使用量總計以及 RAM 磁碟和磁碟分割的清單。即每個磁碟分割的可用空間。

■ 記憶體

- 資料路徑記憶體 - 包含堆積記憶體、記憶體集區和常駐記憶體。
- 記憶體集區 - 所有記憶體集區及其說明和使用量值的清單，除了其使用量總是大約 100% 的 QAT 記憶體集區（屬於裸機 Edge）。記憶體集區為：

名稱	說明
jumbo_mbuf_pool	IPSec 加密裝置所使用 Jumbo 框架的封包集區
common_mbuf_pool	資料路徑通用封包集區
sp_pktmbuf_pool	資料路徑 Slowpath 封包集區
fw_mon_msg	可設定狀態的服務同步訊息集區
vxstt4_frag_q	用於重組的 VXSTT 分段集區
pfstatepl3	可設定狀態的服務狀態集區
pffqdnippl	IP 對應集區的可設定狀態的服務 FQDN
pffqdnsyncpl	可設定狀態的服務 FQDN 同步集區
pffqdnpl	可設定狀態的服務 FQDN 內部集區
pfdnsdpl	可設定狀態的服務 FQDN 內部集區
pfpktpl3	可設定狀態的服務分段封包集區
pfsyncmbufpl3	可設定狀態的服務同步集區
pf_fp_rule_node	可設定狀態的服務規則節點集區
pf_fp_root_rule_node	可設定狀態的服務根規則節點集區
pf_tb_root_rule_node	可設定狀態的服務快速路徑根資料表節點集區
pfa_intattr_pl3	可設定狀態的服務整數屬性集區
pfa_attrconn_pl3	可設定狀態的服務屬性連線集區
pfa_ctx_pl3	可設定狀態的服務內容集區
pfa_key_ace_pl3	可設定狀態的服務整數屬性索引鍵集區
pfa_value_ace_pl3	可設定狀態的服務整數屬性值集區
lb_pkt_pl3	負載平衡器暫時封包快取集區

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**系統 > 網狀架構 > 節點**。
- 3 按一下 **Edge 傳輸節點**索引標籤。
- 4 按一下 Edge 節點的名稱。
- 5 按一下**監控**索引標籤。

隨即顯示 CPU、記憶體和磁碟的使用量資訊，以及節點狀態、網路介面和 NAT 規則統計資料。

使用事件和警示

NSX-T Data Center 提供警示，以讓您注意可能會影響效能和系統作業的事件。警示會提供詳細的事件資訊，例如受影響的元件、事件種類，然後建議採取更正動作。

例如，其中一個 NSX Edge 節點可能會遇到 CPU 使用率異常高或磁碟空間不足的情況。

備註 警示是嚴重性層級大於低的系統事件。

如果引發了某個警示 (例如，憑證即將到期)，之後又針對相同的問題引發了較高嚴重性的警示 (例如，憑證已到期)，則系統將不會自動解決嚴重性較低的警示。您必須採取建議的動作來解決警示。

警示資訊會在 NSX Manager 介面中的多個位置顯示。

關於事件和警示

所有警示是嚴重性層級大於低的事件。但是，它們會以不同方式處理和報告。本節說明這些差異。

事件目錄

下表說明觸發警示的事件，包括警示訊息和用來解決問題的建議動作。嚴重性大於低的任何事件都會觸發警示。

警示管理事件

警示管理事件是由 NSX Manager 和全域管理程式節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
警示服務已超載	嚴重	<p>警示服務已超載。</p> <p>偵測到事件時：「由於報告的警示數量過大，警示服務發生暫時超載的狀況。NSX UI 和 GET /api/v1/alarm NSX API 已停止報告新的警示。但 Syslog 項目和 SNMP 設陷 (如果已啟用) 仍會持續發出報告基礎事件詳細資料。當造成大量警示的基礎問題獲得解決後，警示服務就會重新開始報告新的警示。」</p> <p>解決事件時：「目前已無大量警示，並已重新開始報告新的警示。」</p>	<p>請使用 NSX UI 中的 [警示] 頁面檢閱所有作用中的警示，或使用 GET /api/v1/alarms?status=OPEN,ACKNOWLEDGED,SUPPRESSED NSX API 來檢閱。對於每個作用中的警示，請透過依據建議的警示動作調查其根本原因。解決夠多的警示後，警示服務就會重新開始報告新的警示。</p>
大量警示	嚴重	<p>偵測到大量的特定警示類型。</p> <p>偵測到事件時：「由於 {event_id} 警示數量過大，警示服務已暫時停止報告此類型的警示。NSX UI 和 GET /api/v1/alarms NSX API 不會報告這些警示的新執行個體。但 Syslog 項目和 SNMP 設陷 (如果已啟用) 仍會持續發出報告基礎事件詳細資料。當造成大量 {event_id} 警示的基礎問題獲得解決後，警示服務就會重新開始在偵測到新問題時，報告新的 {event_id} 警示。」</p> <p>解決事件時：「目前已無大量 {event_id} 警示，並已重新開始報告此類型的新警示。」</p>	<p>請使用 NSX UI 中的 [警示] 頁面檢閱所有作用中的警示，或使用 GET /api/v1/alarms?status=OPEN,ACKNOWLEDGED,SUPPRESSED NSX API 來檢閱。對於每個作用中的警示，請透過依據建議的警示動作調查其根本原因。解決夠多的警示後，警示服務就會重新開始報告新的 {event_id} 警示。</p>

憑證事件

憑證事件是從 NSX Manager 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
憑證已到期	嚴重	憑證已到期。 偵測到事件時：「憑證 {entity-id} 已到期。」 解決事件時：「已到期的憑證 {entity-id} 已移除或不再到期。」	確保目前使用憑證的服務已更新，以使用新的、非已到期憑證。例如，若要將新憑證套用至 HTTP 服務，請叫用下列 API 呼叫： POST /api/v1/node/services/http? action=apply_certificate&certificate_id=<cert-id> 其中，<cert-id> 是 API 呼叫 GET /api/v1/trust-management/certificates 所報告之有效憑證的識別碼。 到期的憑證不再使用後，應使用下列 API 呼叫加以刪除： DELETE /api/v1/trust-management/certificates/{entity_id}
憑證即將到期	高	憑證即將到期。 偵測到事件時：「憑證 {entity-id} 即將到期。」 解決事件時：「過期的憑證 {entity-id} 或不再即將到期。」	確保目前使用憑證的服務已更新，以使用新的、非到期中憑證。例如，若要將新憑證套用至 HTTP 服務，請叫用下列 API 呼叫： POST /api/v1/node/services/http? action=apply_certificate&certificate_id=<cert-id> 其中，<cert-id> 是 API 呼叫 GET /api/v1/trust-management/certificates 所報告之有效憑證的識別碼。 到期中憑證不再使用後，應使用 API 呼叫加以刪除： DELETE /api/v1/trust-management/certificates/{entity_id}
接近憑證到期	中	憑證即將到期。 偵測到事件時：「憑證 {entity-id} 即將到期。」 解決事件時：「到期中憑證 {entity-id} 不再接近到期。」	確保目前使用憑證的服務已更新，以使用新的、非到期中憑證。例如，若要將新憑證套用至 HTTP 服務，請叫用下列 API 呼叫： POST /api/v1/node/services/http? action=apply_certificate&certificate_id=<cert-id> 其中，<cert-id> 是 API 呼叫 GET /api/v1/trust-management/certificates 所報告之有效憑證的識別碼。 到期中憑證不再使用後，應使用 API 呼叫加以刪除： DELETE /api/v1/trust-management/certificates/{entity_id}

CNI 健全狀況事件

CNI 健全狀況事件是從 ESXi 和 KVM 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
Hyperbus 管理程式連線已關閉	中	Hyperbus 無法與管理程式節點通訊。 偵測到事件時：「Hyperbus 無法與管理程式節點通訊。」 解決事件時：「Hyperbus 可以與管理程式節點進行通訊。」	Hyperbus vmkernel 介面 (vmk50) 可能遺失。請參閱 知識庫文章 67432 。

DHCP 事件

DHCP 事件是從 NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
集區租用配置失敗	高	IP 集區中的 IP 位址已用盡。 偵測到事件時：「DHCP 伺服器 {dhcp_server_id} 的 IP 集區 {entity_id} 中的位址已用完。前一次的 DHCP 請求失敗，且未來的請求將會失敗。」 解決事件時：「DHCP 伺服器 {dhcp_server_id} 的 IP 集區 {entity_id} 不再已用盡。已成功將租用配置給上一個 DHCP 請求。」	透過叫用 NSX CLI 命令 <code>get dhcp ip-pool</code> ，在 NSX UI 或執行 DHCP 伺服器所在的 Edge 節點上檢閱 DHCP 集區組態。 同時，透過叫用 NSX CLI 命令 <code>get dhcp lease</code> ，在 Edge 節點上檢閱目前作用中的租用。 將租用與作用中虛擬機器的數目比較。如果虛擬機器的數目相較於作用中租用的數目低，請考慮在 DHCP 伺服器組態上減少租用時間。 同時，請考慮透過造訪 NSX UI 中的 網路 > 區段 > 區段 頁面，來擴充 DHCP 伺服器的集區範圍。
集區已超載	中	IP 集區已超載。 偵測到事件時：「DHCP 伺服器 {dhcp_server_id} IP 集區 {entity_id} 使用率正接近耗盡，已配置 {dhcp_pool_usage}% IP。」 解決事件時：「DHCP 伺服器 {dhcp_server_id} IP 集區 {entity_id} 已低於高使用率臨界值。」	透過叫用 NSX CLI 命令 <code>get dhcp ip-pool</code> ，在 NSX UI 或執行 DHCP 伺服器所在的 Edge 節點上檢閱 DHCP 集區組態。 同時，透過叫用 NSX CLI 命令 <code>get dhcp lease</code> ，在 Edge 節點上檢閱目前作用中的租用。 將租用與作用中虛擬機器的數目比較。如果虛擬機器的數目相較於作用中租用的數目低，請考慮在 DHCP 伺服器組態上減少租用時間。 同時，請考慮透過造訪 NSX UI 中的 網路 > 區段 > 區段 頁面，來擴充 DHCP 伺服器的集區範圍。

分散式防火牆事件

分散式防火牆事件是從 NSX Manager 或 ESXi 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
分散式防火牆 CPU 使用率非常高	嚴重	分散式防火牆 CPU 使用率非常高。 偵測到事件時：「傳輸節點 {entity_id} 上的 DFW CPU 使用率已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「DNS 轉寄站 {entity_id} 再次執行。」	考慮將此主機上的虛擬機器工作負載重新平衡至其他主機。 請檢閱安全性設計以進行最佳化。例如，如果規則不適用於整個資料中心，請使用套用至組態。
分散式防火牆記憶體使用量非常高	嚴重	分散式防火牆記憶體使用量非常高。 偵測到事件時：「傳輸節點 {entity_id} 上的 DFW 記憶體使用量 {heap_type} 已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「傳輸節點 {entity_id} 上的 DFW 記憶體使用量 {heap_type} 已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」	透過在主機上叫用 NSX CLI 命令 <code>get firewall thresholds</code> ，以檢視目前 DFW 的記憶體使用量。 考慮將此主機上的工作負載重新平衡至其他主機。

DNS 事件

DNS 事件是從 NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
轉寄站已關閉	高	DNS 轉寄站已關閉。 偵測到事件時：「DNS 轉寄站 {entity_id} 不在執行中。這會影響目前已啟用所有已設定的 DNS 轉寄站。」 解決事件時：「DNS 轉寄站 {entity_id} 再次執行。」	<ol style="list-style-type: none"> 1 叫用 NSX CLI 命令 <code>get dns-forwarders status</code>，以確認 DNS 轉寄站是否處於關閉狀態。 2 檢查 <code>/var/log/syslog</code> 以查看是否有報告任何錯誤。 3 收集支援服務包並連絡 NSX 支援團隊。
轉寄站已停用	高	DNS 轉寄站已停用。 偵測到事件時：「DNS 轉寄站 {entity_id} 已停用。」 解決事件時：「DNS 轉寄站 {entity_id} 已啟用。」	<ol style="list-style-type: none"> 1 叫用 NSX CLI 命令 <code>get dns-forwarders status</code>，以確認 DNS 轉寄站是否處於已停用狀態。 2 使用 NSX 原則 API 或管理程式 API 來啟用 DNS 轉寄站，它不應處於已停用狀態。

Edge 健全狀況事件

Edge 健全狀況事件是從 NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
Edge CPU 使用率非常高	嚴重	Edge 節點 CPU 使用率非常高。 偵測到事件時：「Edge 節點 {entity-id} 上的 CPU 使用率已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點 {entity-id} 上的 CPU 使用率已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」	請檢閱此 Edge 節點的組態、執行中服務和大小調整。考慮調整 Edge 應用裝置的機器尺寸大小，或將服務重新平衡至適用工作負載的其他 Edge 節點。
Edge CPU 使用率高	中	Edge 節點 CPU 使用率偏高。 偵測到事件時：「Edge 節點 {entity-id} 上的 CPU 使用率已達到 {system_resource_usage}%，這等於或高於高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點 {entity-id} 上的 CPU 使用率已達到 {system_resource_usage}%，這低於高臨界值 {system_usage_threshold}%。」	請檢閱此 Edge 節點的組態、執行中服務和大小調整。考慮調整 Edge 應用裝置的機器尺寸大小，或將服務重新平衡至適用工作負載的其他 Edge 節點。
Edge 資料路徑組態失敗	高	Edge 節點資料路徑組態已失敗。 偵測到事件時：「在三次嘗試後，無法啟用 Edge 節點上的資料路徑。」 解決事件時：「已成功啟用 Edge 節點上的資料路徑。」	確保與管理程式節點的 Edge 節點連線狀況良好。 從 Edge 節點 NSX CLI，叫用命令 <code>get services</code> 以檢查服務的健全狀況。 如果資料平面服務已停止，請叫用命令 <code>start service dataplane</code> 將其重新啟動。
Edge 資料路徑 CPU 使用率非常高	嚴重	Edge 節點資料路徑 CPU 使用率非常高。 偵測到事件時：「Edge 節點 {entity-id} 上的資料路徑 CPU 使用率已達到 {datapath_resource_usage}%，其等於或高於極高臨界值至少兩分鐘。」 解決事件時：「Edge 節點 {entity-id} 上的資料路徑 CPU 使用率已低於最大臨界值。」	透過叫用 NSX CLI 命令 <code>get dataplane cpu stats</code> ，以顯示每個 CPU 核心的封包速率，檢閱 Edge 節點上的 CPU 統計資料。較高的 CPU 使用率預期會有較高的封包速率。 考慮增加 Edge 應用裝置的機器尺寸大小，並將此 Edge 節點上的服務重新平衡至相同叢集中的其他 Edge 節點或其他 Edge 叢集。
Edge 資料路徑 CPU 使用率高	中	Edge 節點資料路徑 CPU 使用率偏高。 偵測到事件時：「Edge 節點 {entity-id} 上的資料路徑 CPU 使用率已達到 {datapath_resource_usage}%，其等於或高於高臨界值至少兩分鐘。」 解決事件時：「Edge 節點 {entity-id} 上的 CPU 使用率已達到低於高臨界值。」	透過叫用 NSX CLI 命令 <code>get dataplane cpu stats</code> ，以顯示每個 CPU 核心的封包速率，檢閱 Edge 節點上的 CPU 統計資料。較高的 CPU 使用率預期會有較高的封包速率。 考慮增加 Edge 應用裝置的機器尺寸大小，並將此 Edge 節點上的服務重新平衡至相同叢集中的其他 Edge 節點或其他 Edge 叢集。

事件名稱	嚴重性	警示訊息	建議的動作
Edge 資料路徑加密驅動程式已關閉	嚴重	Edge 節點資料路徑加密驅動程式已關閉。 偵測到事件時：「Edge 節點加密驅動程式已關閉。」 解決事件時：「Edge 節點加密驅動程式已開啟。」	視需要升級 Edge 節點。
Edge 資料路徑記憶體集區偏高	中	Edge 節點資料路徑記憶體集區偏高。 偵測到事件時：「Edge 節點 {entity-id} 上 {mempool_name} 的資料路徑記憶體集區使用率已達到 {system_resource_usage} %，這等於或高於高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點 {entity-id} 上 {mempool_name} 的資料路徑記憶體集區使用率已達到 {system_resource_usage} %，這低於高臨界值 {system_usage_threshold}%。」	以 root 使用者身分登入，並叫用命令 <code>edge-appctl -t /var/run/vmware/edge/dpdctl mempool/show</code> 和 <code>edge-appctl -t /var/run/vmware/edge/dpdctl memory/show malloc_heap</code> 以檢查 DPDK 記憶體使用量。
Edge 磁碟使用量非常高	嚴重	Edge 節點磁碟使用量非常高。 偵測到事件時：「Edge 節點磁碟分割 {disk_partition_name} 的磁碟使用量目前已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點磁碟分割 {disk_partition_name} 的磁碟使用量已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」	檢查具有高使用量的磁碟分割，並查看是否有任何可移除未預期的大型檔案。
Edge 磁碟使用量高	中	Edge 節點磁碟使用量偏高。 偵測到事件時：「Edge 節點磁碟分割 {disk_partition_name} 的磁碟使用量目前已達到 {system_resource_usage}%，這等於或高於高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點磁碟分割 {disk_partition_name} 的磁碟使用量目前已達到 {system_resource_usage}%，這低於高臨界值 {system_usage_threshold}%。」	檢查具有高使用量的磁碟分割，並查看是否有任何可移除未預期的大型檔案。

事件名稱	嚴重性	警示訊息	建議的動作
Edge 全域 ARP 資料表使用量高	中	Edge 節點全域 ARP 資料表使用率偏高。 偵測到事件時：「Edge 節點 {entity-id} 上的全域 ARP 資料表使用率已達到 {datapath_resource_usage}%，這高於高臨界值超過兩分鐘。」 解決事件時：「Edge 節點 {entity-id} 上的全域 ARP 資料表使用率已達到低於高臨界值。」	增加 ARP 資料表大小： 1 以 root 使用者身分登入。 2 叫用命令 <code>edge-appctl -t /var/run/vmware/edge/dpdctl neigh/show</code> 。 3 檢查 neigh 快取使用量是否正常。 a 如果正常，則叫用命令 <code>edge-appctl -t /var/run/vmware/edge/dpdctl neigh/set_param max_entries</code> ，以增加 ARP 資料表大小。
Edge 記憶體使用量非常高	嚴重	Edge 節點記憶體使用量非常高。 偵測到事件時：「Edge 節點 {entity-id} 上的記憶體使用量已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點 {entity-id} 上的記憶體使用量已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」	請檢閱此 Edge 節點的組態、執行中服務和大小調整。考慮調整 Edge 應用裝置的機器尺寸大小，或將服務重新平衡至適用工作負載的其他 Edge 節點。
Edge 記憶體使用量高	中	Edge 節點記憶體使用量偏高。 偵測到事件時：「Edge 節點 {entity-id} 上的記憶體使用量已達到 {system_resource_usage}%，這等於或高於高臨界值 {system_usage_threshold}%。」 解決事件時：「Edge 節點 {entity-id} 上的記憶體使用量已達到 {system_resource_usage}%，這低於高臨界值 {system_usage_threshold}%。」	請檢閱此 Edge 節點的組態、執行中服務和大小調整。考慮調整 Edge 應用裝置的機器尺寸大小，或將服務重新平衡至適用工作負載的其他 Edge 節點。
Edge NIC 連結狀態關閉	嚴重	Edge 節點 NIC 連結已關閉。 偵測到事件時：「Edge 節點 NIC {edge_nic_name} 連結已關閉。」 偵測到事件時：「Edge 節點 NIC {edge_nic_name} 連結已啟動。」	在 Edge 節點上，透過叫用 NSX CLI 命令 <code>get interfaces</code> ，來確認 NIC 連結是否已實際關閉。 如果已關閉，請確認纜線連線。

事件名稱	嚴重性	警示訊息	建議的動作
Edge NIC 的接收緩衝區不足	嚴重	Edge 節點 NIC 的接收描述元循環緩衝區沒有剩餘空間。 偵測到事件時：「Edge 節點 {entity-id} 上的 Edge NIC {edge_nic_name} 接收循環緩衝區已溢位達 {rx_ring_buffer_overflow_percentage} %，且超過 60 秒。」 解決事件時：「Edge 節點 {entity-id} 上的 Edge NIC {edge_nic_name} 接收循環緩衝區使用率不再溢位。」	叫用 NSX CLI 命令 <code>get dataplane</code> ，並檢查下列項目： 1 如果 PPS 和 CPU 使用率高，則透過 <code>get dataplane find ring-size rx</code> 叫用來檢查 rx 循環大小。 <ul style="list-style-type: none"> 如果 PPS 和 CPU 偏高，且 rx 循環大小偏低，請叫用 <code>set dataplane ring-size rx <ring-size></code>，並將 <code>set <ring-size></code> 設為較高的值以容納傳入封包。 如果不符合上述條件，例如循環大小偏高，且 CPU 使用率也偏高，則可能是由於資料平面處理額外負荷延遲所致。
Edge NIC 的傳輸緩衝區不足	嚴重	Edge 節點 NIC 的傳輸描述元循環緩衝區沒有剩餘空間。 偵測到事件時：「Edge 節點 {entity-id} 上的 Edge 節點 NIC {edge_nic_name} 傳輸循環緩衝區已溢位達 {tx_ring_buffer_overflow_percentage} %，且超過 60 秒。」 解決事件時：「Edge 節點 {entity-id} 上的 Edge 節點 NIC {edge_nic_name} 傳輸循環緩衝區使用率不再溢位。」	叫用 NSX CLI 命令 <code>get dataplane</code> ，並檢查下列項目： 1 如果 PPS 和 CPU 使用率高，則透過 <code>get dataplane find ring-size tx</code> 叫用來檢查 tx 循環大小。 <ul style="list-style-type: none"> 如果 PPS 和 CPU 偏高，且 tx 循環大小偏低，請叫用 <code>set dataplane ring-size tx <ring-size></code>，並將 <code>set <ring-size></code> 設為較高的值以容納傳出封包。 如果不符合上述條件，且循環大小偏高，CPU 使用率偏低或正常，則可能是由於 Hypervisor 的傳輸循環大小設定所致。
儲存區錯誤	嚴重	從 NSX-T Data Center 3.0.1 開始。 Edge 節點上的下列磁碟分割處於唯讀模式：{disk_partition_name}	檢查唯讀磁碟分割，以查看重新開機是否可解決此問題，或是需要更換磁碟。請參閱知識庫文章 https://kb.vmware.com/s/article/2146870 。

端點保護事件

端點保護事件是從 NSX Manager 或 ESXi 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
EAM 狀態已關閉	嚴重	<p>計算管理程式上的 ESX Agent Manager (EAM) 服務已關閉。</p> <p>偵測到事件時：「計算管理程式 {entity_id} 上的 ESX Agent Manager (EAM) 服務已關閉。」</p> <p>解決事件時：「計算管理程式 {entity_id} 上的 ESX Agent Manager (EAM) 服務已啟動或計算管理程式 {entity_id} 已移除。」</p>	<p>重新啟動 ESX Agent Manager (EAM) 服務：</p> <ul style="list-style-type: none"> ■ 透過 SSH 進入 vCenter 節點並執行： <pre>service vmware-eam start</pre>
合作夥伴通道已關閉	嚴重	<p>主機模組和合作夥伴 SVM 連線已關閉。</p> <p>偵測到事件時：「主機模組和合作夥伴 SVM {entity_id} 之間的連線已關閉。」</p> <p>解決事件時：「主機模組和合作夥伴 SVM {entity_id} 之間的連線已開啟。」</p>	<p>請參閱知識庫文章 2148821 Troubleshooting NSX Guest Introspection (疑難排解 NSX Guest Introspection)，並確定 {entity_id} 所識別的合作夥伴 SVM 已重新連線至主機模組。</p>

聯盟事件

聯盟事件是從 NSX Manager、NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
LM 對 LM 的同步錯誤	高	<p>從 NSX-T Data Center 3.0.1 開始。</p> <p><i>{site_name}{site_id}</i> 與 <i>{remote_site_name}{remote_site_id}</i> 之間的同步失敗超過 5 分鐘。</p>	<ol style="list-style-type: none"> 1 叫用 NSX CLI 命令 <code>get site-replicator remote-sites</code>，以取得遠端位置之間的連線狀態。如果遠端位置已連線但未同步，則該位置可能仍處於主機的解析程序中。在此情況下，請等待約 10 秒，然後再次嘗試叫用 CLI，以檢查遠端位置的狀態。如果位置已中斷連線，請嘗試下一個步驟。 2 透過 Ping 偵測，檢查從位置 <i>{site_name}{site_id}</i> 中的本機管理程式 (LM) 到位置 <i>{remote_site_name}{remote_site_id}</i> 中 LM 的連線。如果無法執行 Ping 動作，請檢查 WAN 連線的穩定性。如果沒有實體網路連線問題，請嘗試下一個步驟。 3 檢查位置 <i>{site_name}{site_id}</i> 中觸發警示之本機叢集中管理程式節點上的 <code>/var/log/cloudnet/nsx-ccp.log</code> 檔案，以查看是否有任何跨站台通訊錯誤。此外，也需尋找 <code>/var/log/syslog</code> 內的 <code>nsx-appl-proxy</code> 子元件所記錄的錯誤。
LM 對 LM 的同步警告	中	<p>從 NSX-T Data Center 3.0.1 開始。</p> <p><i>{site_name}{site_id}</i> 與 <i>{remote_site_name}{remote_site_id}</i> 之間的同步失敗。</p>	<ol style="list-style-type: none"> 1 叫用 NSX CLI 命令 <code>get site-replicator remote-sites</code>，以取得遠端位置之間的連線狀態。如果遠端位置已連線但未同步，則該位置可能仍處於主機的解析程序中。在此情況下，請等待約 10 秒，然後再次嘗試叫用 CLI，以檢查遠端位置的狀態。如果位置已中斷連線，請嘗試下一個步驟。 2 透過 Ping 偵測，檢查從位置 <i>{site_name}{site_id}</i> 中的本機管理程式 (LM) 到位置 <i>{remote_site_name}{remote_site_id}</i> 中 LM

事件名稱	嚴重性	警示訊息	建議的動作
			<p>的連線。如果無法執行 Ping 動作，請檢查 WAN 連線的穩定性。如果沒有實體網路連線問題，請嘗試下一個步驟。</p> <p>3 檢查位置 <i>{site_name}</i> <i>{{site_id}}</i> 中觸發警示之本機叢集中管理程式節點上的 <code>/var/log/cloudnet/nsx-ccp.log</code> 檔案，以查看是否有任何跨站台通訊錯誤。此外，也需尋找 <code>/var/log/syslog</code> 內的 <code>nsx-appl-proxy</code> 子元件所記錄的錯誤。</p>
RTEP BGP 關閉	高	<p>從 NSX-T Data Center 3.0.1 開始。</p> <p>從來源 IP <i>{bgp_source_ip}</i> 至遠端位置 <i>{remote_site_name}</i> 芳鄰 IP <i>{bgp_neighbor_ip}</i> 的 RTEP BGP 工作階段已關閉。原因：<i>{failure_reason}</i>。</p>	<ol style="list-style-type: none"> 1 在受影響的 Edge 節點上，叫用 NSX CLI 命令 <code>get logical-routers</code>。 2 切換至 <code>REMOTE_TUNNEL_VRF</code> 內容 3 叫用 NSX CLI 命令 <code>get bgp neighbor</code> 以檢查 BGP 芳鄰。 4 或者，叫用 NSX API <code>GET /api/v1/transport-nodes/<transport-node-id>/inter-site/bgp/summary</code>，以取得 BGP 芳鄰狀態。 5 叫用 NSX CLI 命令 <code>get interfaces</code>，並檢查是否已將正確的 RTEP IP 位址指派給名為 <code>remote-tunnel-endpoint</code> 的介面。 6 檢查在指派的 RTEP IP 位址 <i>{bgp_source_ip}</i> 與遠端位置 <i>{remote_site_name}</i> 芳鄰 IP <i>{bgp_neighbor_ip}</i> 之間的 Ping 偵測是否成功執行。 7 檢查 <code>/var/log/syslog</code> 是否有與 BGP 相關的任何錯誤。 8 叫用 API <code>GET</code> 或 <code>PUT /api/v1/transport-nodes/</code>

事件名稱	嚴重性	警示訊息	建議的動作
			<transport-node-id>, 以取得/更新 Edge 節點上的 remote_tunnel_endpoint 組態。這將更新指派給受影響 Edge 節點的 RTEP IP。

高可用性事件

高可用性事件是從 NSX Edge 和公有雲閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
第 0 層閘道容錯移轉	高	第 0 層閘道已進行容錯移轉。 偵測到事件時：「第 0 層閘道 {entity-id} 從 {previous_gateway_state} 到 {current_gateway_state} 的容錯移轉。」 解決事件時：「第 0 層閘道 {entity-id} 現在已啟動。」	判定已關閉的服務，然後將其重新啟動。 1 透過執行 NSX CLI 命令 get logical-routers 來識別第 0 層 VRF 識別碼。 2 透過執行 vrf <vrf-id> 切換到 VRF 內容。 3 透過執行 get high-availability status 來檢視哪個服務已關閉。
第 1 層閘道容錯移轉	高	第 1 層閘道已進行容錯移轉。 偵測到事件時：「第 1 層閘道 {entity-id} 從 {previous_gateway_state} 到 {current_gateway_state} 的容錯移轉。」 解決事件時：「第 1 層閘道 {entity-id} 現在已啟動。」	判定已關閉的服務，然後將其重新啟動。 1 透過執行 NSX CLI 命令 get logical-routers 來識別第 1 層 VRF 識別碼。 2 透過執行 vrf <vrf-id> 切換到 VRF 內容。 3 透過執行 get high-availability status 來檢視哪個服務已關閉。

基礎結構通訊事件

基礎結構通訊事件是從 NSX Edge、KVM、ESXi 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
Edge 通道已關閉	嚴重	Edge 節點的通道狀態為已關閉。 偵測到事件時：「Edge 節點 {entity_id} 的整體通道狀態已關閉。」 解決事件時：「已還原 Edge 節點 {entity_id} 的通道。」	1 使用 SSH 登入 Edge 節點。 2 取得狀態。 <pre>nsxcli get tunnel-ports</pre> 3 在每個通道上，檢查統計資料是否有任何下降。 <pre>get tunnel-port <UUID> stats</pre> 4 檢查 syslog 檔案中是否有任何通道相關錯誤。

基礎結構服務事件

基礎結構服務事件是從 NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
Edge 服務狀態已關閉	嚴重	Edge 服務已關閉，時間已持續至少一分鐘。 偵測到事件時：「服務 <i>{edge_service_name}</i> 已關閉，時間已持續至少一分鐘。」 解決事件時：「服務 <i>{edge_service_name}</i> 已啟動。」	在 Edge 節點上，透過在 <code>/var/log/core</code> 目錄中尋找核心傾印檔案，確認服務尚未因為錯誤而結束。 若要確認服務是否已停止，請叫用 NSX CLI 命令 <code>get services</code> 。 如果是，請執行 <code>start service <service-name></code> 以重新啟動服務。
Edge 服務狀態已變更	低	Edge 服務狀態已變更。 偵測到事件時：「服務 <i>{edge_service_name}</i> 已從 <i>{previous_service_state}</i> 變更為 <i>{current_service_state}</i> 。」 解決事件時：「服務 <i>{edge_service_name}</i> 已從 <i>{previous_service_state}</i> 變更為 <i>{current_service_state}</i> 。」	在 Edge 節點上，透過在 <code>/var/log/core</code> 目錄中尋找核心傾印檔案，確認服務尚未因為錯誤而結束。 若要確認服務是否已停止，請叫用 NSX CLI 命令 <code>get services</code> 。 如果是，請執行 <code>start service <service-name></code> 以重新啟動服務。

Intelligence 通訊事件

NSX Intelligence 通訊事件是從 NSX Manager 節點、ESXi 節點和 NSX Intelligence 應用裝置產生。

事件名稱	嚴重性	警示訊息	建議的動作
傳輸節點流量匯出工具已中斷連線	高	<p>傳輸節點已與其智慧節點的訊息代理中斷連線。資料收集受到影響。</p> <p>偵測到事件時：「傳輸節點 <i>{entity-id}</i> 上的流量匯出工具已與智慧節點的傳訊代理中斷連線。資料收集受到影響。」</p> <p>解決事件時：「傳輸節點 <i>{entity-id}</i> 上的流量匯出工具已重新連線至智慧節點的傳訊代理。」</p>	<ol style="list-style-type: none"> 1 如果訊息服務未在 NSX Intelligence 節點中執行，請將其重新啟動。 2 解決傳輸節點與 NSX Intelligence 節點之間的網路連線失敗問題。
至傳輸節點的控制通道關閉	嚴重	<p>至傳輸節點的控制通道關閉。</p> <p>偵測到事件時：從控制器服務的觀點來看，控制器服務 <i>central_control_plane_id</i> 與傳輸節點 <i>{entity-id}</i> 的連線已關閉至少三分鐘。</p> <p>解決事件時：控制器服務 <i>central_control_plane_id</i> 會還原與傳輸節點 <i>{entity-id}</i> 的連線。</p>	<ol style="list-style-type: none"> 1 使用 Ping 命令，檢查從控制器服務 <i>central_control_plane_id</i> 到傳輸節點 <i>{entity-id}</i> 介面的連線。如果偵測不到，請檢查網路連線的穩定性。 2 檢查是否已使用 netstat 輸出建立 TCP 連線，以查看控制器服務 <i>{central_control_plane_id}</i> 是否接聽連接埠 1235 上的連線。如果不是，請檢查防火牆 (或) iptables 規則，以查看連接埠 1235 是否封鎖傳輸節點 <i>{entity-id}</i> 連線要求。確保底層中沒有主機防火牆或網路防火牆封鎖管理程式節點和傳輸節點之間所需的 IP 連接埠。這會記錄在我們的連接埠和通訊協定工具中，如下所示： https://ports.vmware.com/。 3 傳輸節點 <i>{entity-id}</i> 可能仍處於維護模式。您可以透過下列 API 檢查傳輸節點是否處於維護模式： <pre>GET https://<nsx-mgr>/api/v1/transport-nodes/<tn-uuid></pre> <p>設定維護模式時，傳輸節點將不會連線至控制器服務。當主機升級進行中時，通常會發生此情況。請等待幾分鐘，然後再次檢查連線。</p> <p>備註 此警示並不嚴重且應該能夠解決。此警示的通知不需要與 GSS 取得聯繫，除非該警示在很長的時間內仍未解決。</p>

事件名稱	嚴重性	警示訊息	建議的動作
至傳輸節點的控制通道關閉時間過長	警告	<p>至傳輸節點的控制通道關閉時間過長。</p> <p>偵測到事件時：從控制器服務的觀點來看，控制器服務 <i>central_control_plane_id</i> 與傳輸節點 <i>{entity-id}</i> 的連線已關閉至少 15 分鐘。</p> <p>解決事件時：控制器服務 <i>central_control_plane_id</i> 會還原與傳輸節點 <i>{entity-id}</i> 的連線。</p>	<ol style="list-style-type: none"> 1 使用 Ping 命令，檢查從控制器服務 <i>central_control_plane_id</i> 到傳輸節點 <i>{entity-id}</i> 介面的連線。如果偵測不到，請檢查網路連線的穩定性。 2 檢查是否已使用 netstat 輸出建立 TCP 連線，以查看控制器服務 <i>{central_control_plane_id}</i> 是否接聽連接埠 1235 上的連線。如果不是，請檢查防火牆 (或) iptables 規則，以查看連接埠 1235 是否封鎖傳輸節點 <i>{entity_id}</i> 連線要求。確保底層中沒有主機防火牆或網路防火牆封鎖管理程式節點和傳輸節點之間所需的 IP 連接埠。這會記錄在我們的連接埠和通訊協定工具中，如下所示： https://ports.vmware.com/。 3 傳輸節點 <i>{entity_id}</i> 可能仍處於維護模式。您可以透過下列 API 檢查傳輸節點是否處於維護模式： GET <a href="https://<nsx-mgr>/api/v1/transport-nodes/<tn-uuid>">https://<nsx-mgr>/api/v1/transport-nodes/<tn-uuid> 設定維護模式時，傳輸節點將不會連線至控制器服務。當主機升級進行中時，通常會發生此情況。請等待幾分鐘，然後再次檢查連線。
傳輸節點的管理通道關閉	嚴重	<p>中斷管理程式節點與傳輸節點的連線。</p> <p>偵測到事件時：</p> <p>解決事件時</p>	<ol style="list-style-type: none"> 1 請確保管理程式節點與傳輸節點 <i>nodename (IP)</i> 之間存在網路連線，且沒有任何防火牆封鎖這些節點之間的流量。 2 叫用下列命令以確保 nsx-proxy 服務正在傳輸節點上執行。 <code>/etc/init.d/nsx-prxy status</code> 如果 nsx-proxy 服務不在執行中，請執行下列命令將其重新啟動。 <code>/etc/init.d/nsx-proxy restart</code>
管理程式控制通道關閉	嚴重	<p>管理程式到控制器的通道已關閉。</p> <p>偵測到事件時：</p> <p>解決事件時：</p>	<p>在管理程式節點 <i>managernode (IP)</i> 上，叫用下列兩個 NSX CLI 命令：</p> <ul style="list-style-type: none"> ■ <code>restart service mgmt-plane-bus</code> ■ <code>restart service manage</code>

Intelligence 健全狀況事件

NSX Intelligence 健全狀況事件是從 NSX Manager 節點和 NSX Intelligence 應用裝置產生。

事件名稱	嚴重性	警示訊息	建議的動作
CPU 使用率非常高	嚴重	智慧節點 CPU 使用率非常高。 偵測到事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的 CPU 使用率高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的 CPU 使用率低於極高臨界值 {system_usage_threshold}%。」	使用 top 命令來檢查哪些程序具有最多記憶體使用量，然後檢查 /var/log/syslog 和這些程序的本機記錄，以查看是否有要解決的任何未完成的錯誤。
CPU 使用率高	中	智慧節點 CPU 使用率偏高。 偵測到事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的 CPU 使用率高於高臨界值 {system_usage_threshold}%。」 解決事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的 CPU 使用率低於高臨界值 {system_usage_threshold}%。」	使用 top 命令來檢查哪些程序具有最多記憶體使用量，然後檢查 /var/log/syslog 和這些程序的本機記錄，以查看是否有要解決的任何未完成的錯誤。
記憶體使用量非常高	嚴重	智慧節點記憶體使用量非常高。 偵測到事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的記憶體使用量高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的記憶體使用量低於極高臨界值 {system_usage_threshold}%。」	使用 top 命令來檢查哪些程序具有最多記憶體使用量，然後檢查 /var/log/syslog 和這些程序的本機記錄，以查看是否有要解決的任何未完成的錯誤。
記憶體使用量高	中	智慧節點記憶體使用量偏高。 偵測到事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的記憶體使用量高於高臨界值 {system_usage_threshold}%。」 解決事件時：「NSX Intelligence 節點 {intelligence_node_id} 上的記憶體使用量低於高臨界值 {system_usage_threshold}%。」	使用 top 命令來檢查哪些程序具有最多記憶體使用量，然後檢查 /var/log/syslog 和這些程序的本機記錄，以查看是否有要解決的任何未完成的錯誤。
磁碟使用量非常高	嚴重	智慧節點磁碟使用量非常高。 偵測到事件時：「NSX Intelligence 節點 {intelligence_node_id} 上磁碟分割 {disk_partition_name} 的磁碟使用率高於極高臨界值 {system_usage_threshold}%。」 解決事件時：「NSX Intelligence 節點 {intelligence_node_id} 上磁碟分割 {disk_partition_name} 的磁碟使用率低於極高臨界值 {system_usage_threshold}%。」	檢查磁碟分割 {disk_partition_name}，並查看是否有任何非預期的大型檔案可移除。

事件名稱	嚴重性	警示訊息	建議的動作
磁碟使用量高	中	<p>智慧節點磁碟使用量偏高。</p> <p>偵測到事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 <i>{disk_partition_name}</i> 的磁碟使用率高於高臨界值 <i>{system_usage_threshold}</i> %。」</p> <p>解決事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 <i>{disk_partition_name}</i> 的磁碟使用率低於高臨界值 <i>{system_usage_threshold}</i> %。」</p>	<p>檢查磁碟分割 <i>{disk_partition_name}</i>，並查看是否有任何非預期的大型檔案可移除。</p>
資料磁碟分割使用量非常高	嚴重	<p>智慧節點資料磁碟分割使用率非常高。</p> <p>偵測到事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 / data 的磁碟使用率高於極高臨界值 <i>{system_usage_threshold}</i>%。」</p> <p>解決事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 / data 的磁碟使用率低於極高臨界值 <i>{system_usage_threshold}</i>%。」</p>	<p>停止 NSX Intelligence 資料收集，直到磁碟使用量低於臨界值。</p> <p>在 NSX UI 中，導覽至系統應用裝置 NSX Intelligence 應用裝置。然後，選取動作 > 停止收集資料。</p>
資料磁碟分割使用量高	中	<p>智慧節點資料磁碟分割使用率偏高。</p> <p>偵測到事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 / data 的磁碟使用率高於高臨界值 <i>{system_usage_threshold}</i>%。」</p> <p>解決事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上磁碟分割 / data 的磁碟使用率低於高臨界值 <i>{system_usage_threshold}</i>%。」</p>	<p>停止 NSX Intelligence 資料收集，直到磁碟使用量低於臨界值。</p> <p>檢查 /data 磁碟分割，並查看是否有可移除的任何未預期的大型檔案。</p>
節點狀態已降級	高	<p>智慧節點狀態為已降級。</p> <p>偵測到事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上的服務 <i>{service_name}</i> 不在執行中。」</p> <p>解決事件時：「NSX Intelligence 節點 <i>{intelligence_node_id}</i> 上的服務 <i>{service_name}</i> 正在正常執行。」</p>	<p>在 NSX Intelligence 節點中，使用 NSX CLI 命令 <code>get services</code> 檢查服務狀態和健全狀況資訊。</p> <p>使用 NSX CLI 命令 <code>restart service <service-name></code> 重新啟動未預期的已停止服務。</p>

授權事件

授權事件是從 NSX Manager 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
授權已到期	嚴重	授權已到期。 偵測到事件時：「類型 <i>{license_edition_type}</i> 的授權已到期。」 解決事件時：「類型 <i>{license_edition_type}</i> 的過期授權已移除、更新或不再到期。」	新增新的、非到期授權： 1 在 NSX UI 中，導覽至 系統 > 授權 。 2 按一下 新增 ，然後指定新授權的金鑰。 3 刪除到期的授權，方法是選取核取方塊，然後按一下 取消指派 。
授權即將到期	中	偵測到事件時：「類型 <i>{license_edition_type}</i> 的授權即將到期。」 解決事件時：「由 <i>{license_edition_type}</i> 識別的到期授權已移除、更新，或不再即將到期。」	新增新的、非到期授權： 1 在 NSX UI 中，導覽至 系統 > 授權 。 2 按一下 新增 ，然後指定新授權的金鑰。 3 刪除到期的授權，方法是選取核取方塊，然後按一下 取消指派 。

負載平衡器事件

負載平衡器事件是從 NSX Edge 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
負載平衡器 CPU 非常高	中	負載平衡器 CPU 使用率非常高。 偵測到事件時：「負載平衡器 <i>{entity_id}</i> 上的 CPU 使用率已達到 <i>{system_resource_usage}</i> %，這高於極高臨界值 <i>{system_usage_threshold}</i> %。」 解決事件時：「負載平衡器 <i>{entity_id}</i> 的 CPU 使用率為 <i>{system_resource_usage}</i> %，這低於極高臨界值 <i>{system_usage_threshold}</i> %。」	如果其負載平衡器 CPU 使用率高於 <i>{system_usage_threshold}</i> %，則工作負載對此負載平衡器來說過高。 將負載平衡器的大小從小變更為中型或從中型變更為大型，以重新調整負載平衡器服務。 如果此負載平衡器的 CPU 使用率仍然很高，請考慮調整 Edge 應用裝置機器尺寸大小，或將負載平衡器服務移至其他 Edge 節點，以獲得適當的工作負載。
負載平衡器狀態關閉	中	負載平衡器服務已關閉。 偵測到事件時：「負載平衡器服務 <i>{entity_id}</i> 已關閉。」 解決事件時：「負載平衡器服務 <i>{entity_id}</i> 已啟動。」	確認 Edge 節點中的負載平衡器服務是否正在執行。 如果負載平衡器服務的狀態為未就緒，請將 Edge 節點移至維護模式，然後結束維護模式。 如果負載平衡器服務的狀態仍未復原，請檢查 <code>syslog</code> 中是否存在任何錯誤記錄。

事件名稱	嚴重性	警示訊息	建議的動作
虛擬伺服器狀態關閉	中	負載平衡器虛擬服務已關閉。 偵測到事件時：「負載平衡器虛擬伺服器 {entity_id} 已關閉。」 解決事件時：「負載平衡器虛擬伺服器 {entity_id} 已啟動。」	請查閱負載平衡器集區，以判定其狀態並確認其組態。 如果設定錯誤，請將其重新設定並從虛擬伺服器移除該負載平衡器集區，然後重新將其新增至虛擬伺服器。
集區狀態關閉	中	偵測到事件時：「負載平衡器集區 {entity_id} 狀態為關閉。」 解決事件時：「負載平衡器集區 {entity_id} 狀態為啟動。」	<ol style="list-style-type: none"> 1 請查閱負載平衡器集區，以判定哪些成員為關閉。 2 檢查從負載平衡器到受影響集區成員的網路連線。 3 驗證每個集區成員的應用程式健全狀況。 4 使用設定的監控來驗證每個集區成員的健全狀況。 <p>當成員的健全狀況建立時，集區成員狀態會根據 Rise Count 更新為狀況良好。</p>

管理程式健全狀況事件

NSX Manager 健全狀況事件是從 NSX Manager 節點叢集產生。

事件名稱	嚴重性	警示訊息	建議的動作
重複的 IP 位址	中	管理程式節點的 IP 位址由其他裝置使用中。 偵測到事件時：「管理程式節點 {entity_id} 的 IP 位址 {duplicate_ip_address} 目前由網路中的其他裝置使用中。」 偵測到事件時：「管理程式節點 {entity_id} 似乎已不再使用 {duplicate_ip_address}。」	<ol style="list-style-type: none"> 1 判定哪個裝置使用管理程式的 IP 位址，並為該裝置指派新的 IP 位址。 備註 不支援將管理程式重新設定為使用新的 IP 位址。 2 確認靜態 IP 位址集區/DHCP 伺服器是否已正確設定。 3 如果已手動指派裝置的 IP 位址，請更正該位址。
管理程式 CPU 使用率非常高	嚴重	管理程式節點 CPU 使用率非常高。 偵測到事件時：「管理程式節點 {entity_id} 上的 CPU 使用率已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}。」 解決事件時：「管理程式節點 {entity_id} 上的 CPU 使用率已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold} %。」	請檢閱此管理程式節點的組態、執行中服務和大小調整。 考慮調整管理程式應用裝置機器尺寸大小。

事件名稱	嚴重性	警示訊息	建議的動作
管理程式 CPU 使用率高	中	<p>從 NSX-T Data Center 3.0.1 開始。</p> <p>管理程式節點 CPU 使用率偏高。</p> <p>偵測到事件時：「管理程式節點 {entity_id} 上的 CPU 使用率已達到 {system_resource_usage}%，這等於或高於高臨界值 {system_usage_threshold}%。」</p> <p>解決事件時：「管理程式節點 {entity_id} 上的 CPU 使用率已達到 {system_resource_usage}%，這低於高臨界值 {system_usage_threshold}%。」</p>	<p>請檢閱此管理程式節點的組態、執行中服務和大小調整。</p> <p>考慮調整管理程式應用裝置機器尺寸大小。</p>
管理程式記憶體使用量非常高	嚴重	<p>從 NSX-T Data Center 3.0.1 開始。</p> <p>管理程式節點記憶體使用量非常高。</p> <p>偵測到事件時：「管理程式節點 {entity_id} 上的記憶體使用量已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」</p> <p>解決事件時：「管理程式節點 {entity_id} 上的記憶體使用量已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」</p>	<p>請檢閱此管理程式節點的組態、執行中服務和大小調整。</p> <p>考慮調整管理程式應用裝置機器尺寸大小。</p>
管理程式記憶體使用量高	中	<p>管理程式節點記憶體使用量偏高。</p> <p>偵測到事件時：「管理程式節點 {entity_id} 上的記憶體使用量已達到 {system_resource_usage}%，這等於或高於高臨界值 {system_usage_threshold}%。」</p> <p>解決事件時：「管理程式節點 {entity_id} 上的記憶體使用量已達到 {system_resource_usage}%，這低於高臨界值 {system_usage_threshold}%。」</p>	<p>請檢閱此管理程式節點的組態、執行中服務和大小調整。</p> <p>考慮調整管理程式應用裝置機器尺寸大小。</p>
管理程式磁碟使用量非常高	嚴重	<p>管理程式節點磁碟使用量非常高。</p> <p>偵測到事件時：「管理程式節點磁碟分割 {disk_partition_name} 的磁碟使用量目前已達到 {system_resource_usage}%，這等於或高於極高臨界值 {system_usage_threshold}%。」</p> <p>解決事件時：「管理程式節點磁碟分割 {disk_partition_name} 的磁碟使用量已達到 {system_resource_usage}%，這低於極高臨界值 {system_usage_threshold}%。」</p>	<p>檢查具有高使用量的磁碟分割，並查看是否有任何可移除未預期的大型檔案。</p>

事件名稱	嚴重性	警示訊息	建議的動作
管理程式磁碟使用量高	中	<p>管理程式節點磁碟使用量偏高。</p> <p>偵測到事件時：「管理程式節點磁碟分割 <i>{disk_partition_name}</i> 的磁碟使用量目前已達到 <i>{system_resource_usage}%</i>，這等於或高於高臨界值 <i>{system_usage_threshold}%</i>。」</p> <p>解決事件時：「管理程式節點磁碟分割 <i>{disk_partition_name}</i> 的磁碟使用量目前已達到 <i>{system_resource_usage}%</i>，這低於高臨界值 <i>{system_usage_threshold}%</i>。」</p>	檢查具有高使用量的磁碟分割，並查看是否有任何可移除未預期的大型檔案。
管理程式組態磁碟使用量非常高	嚴重	<p>管理程式節點組態磁碟使用量非常高。</p> <p>偵測到事件時：「管理程式節點磁碟分割 / <i>config</i> 的磁碟使用量目前已達到 <i>{system_resource_usage}%</i>，這等於或高於極高臨界值 <i>{system_usage_threshold}%</i>。」這可能表示 NSX 資料存放區服務在 /<i>config/corfu</i> 目錄下的磁碟使用量過高。」</p> <p>解決事件時：「管理程式節點磁碟分割 / <i>config</i> 的磁碟使用量已達到 <i>{system_resource_usage}%</i>，這低於極高臨界值 <i>{system_usage_threshold}%</i>。」</p>	檢查 / <i>config</i> 磁碟分割，並查看是否有可移除的任何未預期的大型檔案。
管理程式組態磁碟使用量高	中	<p>管理程式節點組態磁碟使用量偏高。</p> <p>偵測到事件時：「管理程式節點磁碟分割 / <i>config</i> 的磁碟使用量目前已達到 <i>{system_resource_usage}%</i>，這等於或高於高臨界值 <i>{system_usage_threshold}%</i>。這可能表示 NSX 資料存放區服務在 /<i>config/corfu</i> 目錄下的磁碟使用量正在上升。」</p> <p>解決事件時：「管理程式節點磁碟分割 / <i>config</i> 的磁碟使用量已達到 <i>{system_resource_usage}%</i>，這低於高臨界值 <i>{system_usage_threshold}%</i>。」</p>	檢查 / <i>config</i> 磁碟分割，並查看是否有可移除的任何未預期的大型檔案。
作業 DB 磁碟使用量高	中	<p>管理程式節點磁碟分割 /<i>nonconfig</i> 的磁碟使用量已達到 <i>{system_resource_usage}%</i>，這等於或高於高臨界值 <i>{system_usage_threshold}%</i>。這可能表示 NSX 資料存放區服務在 /<i>nonconfig/corfu</i> 目錄下的磁碟使用量正在上升。</p>	如果有回報問題，請執行下列工具，並連結 GSS： <code>/opt/vmware/tools/support/inspect_checkpoint_issues.py --nonconfig</code> 。
作業資料庫磁碟使用量極高	嚴重	<p>管理程式節點磁碟分割 /<i>nonconfig</i> 的磁碟使用量已達到 <i>{system_resource_usage}%</i>，這等於或高於極高臨界值 <i>{system_usage_threshold}%</i>。這可能表示 NSX 資料存放區服務在 /<i>nonconfig/corfu</i> 目錄下的磁碟使用量正在上升。</p>	如果有回報問題，請執行下列工具，並連結 GSS： <code>/opt/vmware/tools/support/inspect_checkpoint_issues.py --nonconfig</code> 。

NCP 事件

NSX Container Plug-in (NCP) 事件是從 ESXi 和 KVM 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
NCP 外掛程式已關閉	嚴重	<p>管理程式節點偵測到 NCP 已關閉或狀況不良。</p> <p>偵測到事件時：「管理程式節點偵測到 NCP 已關閉或狀況不良。」</p> <p>解決事件時：「管理程式節點偵測到 NCP 已再次啟動或狀況良好。」</p>	<p>若要找出有問題的叢集，請叫用 NSX API： GET /api/v1/systemhealth/ container-cluster/ncp/status 來擷取所有叢集狀態，並判定任何報告為關閉或未知的叢集名稱。</p> <p>移至 NSX UI 詳細目錄 > 容器 > 叢集 頁面，找到報告為已關閉或未知狀態的叢集名稱，然後按一下列出所有 Kubernetes 和 PAS 叢集成員的 [節點] 索引標籤。</p> <p>對於 Kubernetes 叢集：</p> <ol style="list-style-type: none"> 1 尋找來自所有叢集成員的 K8s 主節點，並登入主節點，以檢查 NCP 網繭活躍性。 然後叫用 kubectl 命令 <code>kubectl get pods --all-namespaces</code>。如果 NCP 網繭發生問題，請使用 <code>kubectl logs</code> 命令檢查問題並修正錯誤。 2 檢查 NCP 與 Kubernetes API 伺服器之間的連線。 NSX CLI 可在 NCP 網繭中使用，以透過從主要虛擬機器叫用下列命令來檢查此連線狀態。 <pre> kubectl exec -it <NCP-Pod-Name> -n nsx-system bash nsxcli get ncp-k8s-api-server status </pre> <p>如果連線發生問題，請檢查網路和 NCP 組態。</p> 3 檢查 NCP 和 NSX Manager 之間的連線。 NSX CLI 可在 NCP 網繭中使用，以透過從主要虛擬機器叫用下列命令來檢查此連線狀態。 <pre> kubectl exec -it <NCP-Pod-Name> -n nsx-system bash nsxcli get ncp-nsx status </pre> <p>如果連線發生問題，請檢查網路和 NCP 組態。</p> <p>對於 PAS 叢集：</p> <ol style="list-style-type: none"> 1 檢查虛擬機器之間的網路連線，並修正任何網路問題。 2 檢查節點和服務的狀態，並修正已損毀的節點或服務。

事件名稱	嚴重性	警示訊息	建議的動作
			<p>叫用命令 <code>bosh vms</code> 和 <code>bosh instances -p</code>，以檢查節點和服務的狀態。</p>

節點代理程式健全狀況事件

節點代理程式健全狀況事件是從 ESXi 和 KVM 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
節點代理程式已關閉	高	<p>在節點虛擬機器內執行的代理程式似乎已關閉。</p> <p>偵測到事件時：「在節點虛擬機器內執行的代理程式似乎已關閉。」</p> <p>解決事件時：「節點虛擬機器內的代理程式執行中。」</p>	<p>對於 ESX：</p> <ol style="list-style-type: none"> 1 如果遺失 Vmk50，請參閱知識庫文章 67432。 2 如果遺失 Hyperbus 4094：重新啟動 <code>nsx-cfgagent</code> 或重新啟動容器主機虛擬機器可能有幫助。 3 如果已封鎖容器主機 VIF，請檢查控制器的連線，以確保已關閉所有組態。 4 如果 <code>nsx-cfgagent</code> 已停止，請重新啟動 <code>nsx-cfgagent</code>。 <p>對於 KVM：</p> <ol style="list-style-type: none"> 1 如果 Hyperbus 命名空間遺失，重新啟動 <code>nsx-opsagent</code> 可能有助於重新建立命名空間。 2 如果 Hyperbus 命名空間中遺失 Hyperbus 介面，則重新啟動 <code>nsx-opsagent</code> 可能有幫助。 3 如果 <code>nsx-agent</code> 已停止，請重新啟動 <code>nsx-agent</code>。 <p>對於 ESX 和 KVM：</p> <ol style="list-style-type: none"> 1 如果遺失 <code>node-agent</code> 套件：請檢查是否已成功將 <code>node-agent</code> 套件安裝在容器主機虛擬機器中。 2 如果容器主機虛擬機器中 <code>node-agent</code> 的介面已關閉：檢查容器主機虛擬機器內 <code>eth1</code> 介面的狀態。

密碼管理事件

密碼管理事件是從 NSX Manager、NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
密碼已到期	嚴重	使用者密碼已到期。 偵測到事件時：「使用者 {username} 的密碼已到期。」 解決事件時：「使用者 {username} 的密碼已成功變更或不再到期。」	使用者 {username} 的密碼必須立即變更才能存取系統。例如，若要將新密碼套用至使用者，請在要求本文中有效密碼叫用下列 NSX API： <pre>PUT /api/v1/node/users/<userid></pre> 其中 <userid> 是使用者的識別碼。如果 admin 使用者 (使用 <userid> 10000) 密碼已到期，則 admin 必須透過 SSH (如果已啟用) 或主控台登入系統，才能變更密碼。輸入目前的已到期密碼時，系統會提示 admin 輸入新密碼。
密碼即將到期	高	使用者密碼即將到期。 偵測到事件時：「使用者 {username} 的密碼即將在 {password_expiration_days} 天後到期。」 解決事件時：「使用者 {username} 的密碼已成功變更或不再即將到期。」	確定由 {username} 識別的使用者密碼會立即變更。例如，若要將新密碼套用至使用者，請在要求本文中有效密碼叫用下列 NSX API： <pre>PUT /api/v1/node/users/<userid></pre> 其中 <userid> 是使用者的識別碼。
接近密碼到期	中	使用者密碼即將到期。 偵測到事件時：「使用者 {username} 的密碼即將在 {password_expiration_days} 天後到期。」 解決事件時：「使用者 {username} 的密碼已成功變更或不再即將到期。」	由 {username} 識別的使用者的密碼需要盡快變更。例如，若要將新密碼套用至使用者，請在要求本文中有效密碼叫用下列 NSX API： <pre>PUT /api/v1/node/users/<userid></pre> 其中 <userid> 是使用者的識別碼。

路由事件

事件名稱	嚴重性	警示訊息	建議的動作
BGP 已關閉	高	BGP 芳鄰已關閉。 偵測到事件時：「在路由器 {entity_id} 中，BGP 芳鄰 {bgp_neighbor_ip} 已關閉，原因：{failure_reason}。」 解決事件時：「在路由器 {entity_id} 中，BGP 芳鄰 {bgp_neighbor_ip} 已啟動。」	<ol style="list-style-type: none"> 1 使用 SSH 進入 Edge 節點。 2 叫用 NSX CLI 命令：<code>get logical-routers</code> 3 切換至服務路由器 {sr_id}。 4 檢查 /var/log/syslog，以查看是否有與 BGP 連線相關的任何錯誤。
外部介面上的雙向轉送偵測 (BFD) 關閉	高	BFD 工作階段已關閉。 偵測到事件時：「在路由器 {entity_id} 中，對等 {peer_address} 的 BFD 工作階段已關閉。」 解決事件時：「在路由器 {entity_id} 中，對等 {peer_address} 的 BFD 工作階段已啟動。」	<ol style="list-style-type: none"> 1 使用 SSH 進入 Edge 節點。 2 叫用 NSX CLI 命令：<code>get logical-routers</code> 3 切換至服務路由器 {sr_id}。 4 透過叫用 NSX CLI 命令：<code>ping <peer_address></code> 來驗證連線。

事件名稱	嚴重性	警示訊息	建議的動作
路由關閉	高	<p>所有 BGP/BFD 工作階段已關閉。</p> <p>偵測到事件時：「所有 BGP/BFD 工作階段已關閉。」</p> <p>解決事件時：「至少一個 BGP/BFD 工作階段已開啟。」</p>	<ol style="list-style-type: none"> 1 叫用 NSX CLI 命令 <code>get logical-routers</code> 以取得第 0 層服務路由器。 2 切換至第 0 層服務路由器 VRF，然後叫用下列 NSX CLI 命令： <ul style="list-style-type: none"> ■ 驗證連線：<code>ping <BFD peer IP address></code> ■ 檢查 BFD 健全狀況： <pre>get bfd-config get bfd-sessions</pre> ■ 檢查 BGP 健全狀況：<code>get bgp neighbor summary</code> <pre>get bfd neconfig get bfd-sessions</pre> <p>檢查 <code>/var/log/syslog</code>，以查看是否有與 BGP 連線相關的任何錯誤。</p>
靜態路由已移除	高	<p>靜態路由已移除。</p> <p>偵測到事件時：「在路由器 <code>{entity_id}</code> 中，靜態路由 <code>{static_address}</code> 已移除，因為 BFD 已關閉。」</p> <p>解決事件時：「在路由器 <code>{entity_id}</code> 中，靜態路由 <code>{static_address}</code> 已在 BFD 復原時重新新增。」</p>	<ol style="list-style-type: none"> 1 使用 SSH 進入 Edge 節點。 2 叫用 NSX CLI 命令：<code>get logical-routers</code> 3 切換至服務路由器 <code>{sr_id}</code>。 4 透過叫用 NSX CLI 命令來驗證連線： <pre>get bgp neighbor summary</pre> 5 此外，確認 NSX 和 BFD 對等中的組態，以確保計時器尚未變更。

傳輸節點健全狀況

傳輸節點健全狀況事件是從 KVM 和 ESXi 節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
LAG 成員已關閉	中	LACP 報告成員已關閉。 偵測到事件時：「LACP 報告成員已關閉。」 解決事件時：「LACP 報告成員已啟動。」	<p>檢查主機上 LAG 成員的連線狀態。</p> <ol style="list-style-type: none"> 1 在 NSX UI 中，導覽至網狀架構 > 節點 > 傳輸節點 > 主機傳輸節點。 2 在 [主機傳輸節點] 清單中，檢查 [節點狀態] 資料行。 尋找 [節點狀態] 為降級或關閉的傳輸節點。 3 選取<傳輸節點> > 監控。 尋找報告為降級或關閉的繫結 (上行)。 4 透過登入失敗的主機並執行適當的命令，檢查 LACP 成員狀態詳細資料： <ul style="list-style-type: none"> ■ ESXi: <code>esxcli network vswitch dvs vmware lacp status get</code> ■ KVM: <code>ovs-appctl bond/show</code> 和 <code>ovs-appctl lacp/show</code>
N-VDS 上行關閉	中	上行即將關閉。 偵測到事件時：「上行即將關閉。」 解決事件時：「上行即將啟動。」	<p>檢查主機上上行的實體 NIC 狀態。</p> <ol style="list-style-type: none"> 1 在 NSX UI 中，導覽至網狀架構 > 節點 > 傳輸節點 > 主機傳輸節點。 2 在 [主機傳輸節點] 清單中，檢查 [節點狀態] 資料行。 尋找 [節點狀態] 為降級或關閉的傳輸節點。 3 選取<傳輸節點> > 監控。 尋找報告為降級或關閉的繫結 (上行) 的狀態詳細資料。 若要避免發生降級狀態，無論是否正在使用中，請確保上行介面均已連線並開啟。

VPN 事件

VPN 事件是從 NSX Edge 和公用閘道節點產生。

事件名稱	嚴重性	警示訊息	建議的動作
以 IPsec 原則為基礎的工作階段關閉	中	以原則為基礎的 IPsec VPN 工作階段已關閉。 偵測到事件時：「以原則為基礎的 IPsec VPN 工作階段 {entity_id} 已關閉。原因：{session_down_reason}。」 解決事件時：「以原則為基礎的 IPsec VPN 工作階段 {entity_id} 已啟動。」	檢查 IPsec VPN 工作階段組態，並根據工作階段關閉的原因解決錯誤。
以 IPsec 路由為基礎的工作階段關閉	中	以路由為基礎的 IPsec VPN 工作階段已關閉。 偵測到事件時：「以路由為基礎的 IPsec VPN 工作階段 {entity_id} 已關閉。原因：{session_down_reason}。」 解決事件時：「以路由為基礎的 IPsec VPN 工作階段 {entity_id} 已啟動。」	檢查 IPsec VPN 工作階段組態，並根據工作階段關閉的原因解決錯誤。
以 IPsec 原則為基礎的通道關閉	中	以原則為基礎的 IPsec VPN 通道已關閉。 偵測到事件時：「工作階段 {entity_id} 中一或多個以原則為基礎的 IPsec VPN 通道已關閉。」 解決事件時：「工作階段 {entity_id} 中所有以原則為基礎的 IPsec VPN 通道均已啟動。」	檢查 IPsec VPN 工作階段組態，並根據通道關閉的原因解決錯誤。
以 IPsec 路由為基礎的通道已關閉	中	以路由為基礎的 IPsec VPN 通道已關閉。 偵測到事件時：「工作階段 {entity_id} 中一或多個以路由為基礎的 IPsec VPN 通道已關閉。」 解決事件時：「工作階段 {entity_id} 中所有以路由為基礎的 IPsec VPN 通道均已啟動。」	檢查 IPsec VPN 工作階段組態，並根據通道關閉的原因解決錯誤。
L2VPN 工作階段關閉	中	L2VPN 工作階段已關閉。 偵測到事件時：「L2VPN 工作階段 {entity_id} 已關閉。」 解決事件時：「L2VPN 工作階段 {entity_id} 已啟動。」	檢查 IPsec VPN 工作階段組態，並根據原因解決錯誤。

身分識別防火牆事件

事件名稱	嚴重性	警示訊息	建議的動作
與 AD 伺服器的連線	嚴重	與 AD 伺服器的連線中斷。 偵測到事件時：與身分識別防火牆 AD 伺服器的連線已關閉。 偵測到事件時：與身分識別防火牆 AD 伺服器的連線已開啟。	<ol style="list-style-type: none"> AD 伺服器可從 NSX 節點進行連線。 AD 伺服器詳細資料已在 NSX 中已正確設定。 AD 伺服器已正確執行。 沒有防火牆會封鎖 AD 伺服器和 NSX 節點之間的存取。 修正連線問題之後，請使用 LDAP 伺服器 UI 中的「測試連線」來測試與 AD 伺服器的連線。
差異同步期間發生錯誤	嚴重	無法同步 AD 伺服器 <i>錯誤說明</i> 偵測到事件時：在身分識別防火牆 AD 伺服器的選擇性同步期間發生故障： <i>錯誤詳細資料</i> 。 偵測到事件時：已修正身分識別防火牆 AD 伺服器的選擇性同步錯誤。	<ol style="list-style-type: none"> 確認 Edge 節點中的負載平衡器服務是否正在執行。 如果負載平衡器服務的狀態為未就緒，請將 Edge 節點移至維護模式，然後結束維護模式。 如果負載平衡器服務的狀態仍未復原，請檢查 Syslog 中是否存在任何錯誤記錄。

檢視警示資訊

警示資訊會顯示在 NSX Manager 介面中的多個位置。警示和事件資訊也包含在標題列的 [通知] 下拉式功能表的其他通知中。

警示可以是下列其中一種狀態：

狀態	說明
未處理	警示處於作用中、未確認狀態。
已確認	警示已由使用者確認。警示仍保持未處理狀態，但不會再顯示在 NSX Manager 通知中。
已隱藏	針對此警示的狀態報告，已由使用者停用使用者所指定的持續時間。
已解決	<p>警示已解決，無論是由系統或透過使用者動作解決。警示將持續顯示在已解決狀態的警示資料表中最多八天，之後會自動刪除它。(系統可能會提早刪除已解決的警示，以因應資源需求。)</p> <p>備註 如果使用者將警示狀態變更為已解決，但觸發警示的情況並未解決，則系統會具現化新的警示執行個體。此外，事件可能會處於已解決達數分鐘，之後所報告的狀態才會在介面中更新。</p>

備註 下列步驟顯示如何從首頁檢視警示。但是，您也可以從其他頁面 (例如第 0 層、第 1 層和負載平衡頁面，以及其他頁面) 檢視警示。請參閱這些頁面上資料表中的 [警示] 資料行。

程序

- 1 導覽至首頁，然後按一下**警示**。

備註 紅色驚嘆號 (!) 出現在**警示**面板標籤旁邊時，表示至少有一個未解決的警示為「嚴重」層級。

[警示] 面板隨即會顯示，隨著最上方的圖形儀表板顯示，如作用中警示、警示最多的最高排名功能，以及最高排名事件 (依發生次數)。儀表板下方是可排序、可篩選的目前警示清單。下表詳細說明有關每個作用中警示的下列資訊：

- 受影響的功能
- 事件類型
- 節點
- 實體
- 嚴重性 (嚴重、高、中)
- 上次報告時間
- 警示狀態 (未處理、已隱藏、已解決、已確認)

[警示] 資料表中的每個資料列均可展開，以顯示更多詳細資料。

- 2 按一下儀表板右上角的漏斗圖示，以篩選儀表板中顯示的結果。
您可以依過去 24 小時、過去 48 小時或自訂時間範圍或所有未處理的警示進行篩選。
- 3 按一下資料表上方的篩選器文字方塊，以篩選資料表中顯示的結果。
系統會提示您指定篩選：警示狀態、說明、實體名稱、實體類型、事件類型、節點等。

後續步驟

檢視警示後，您可以決定如何回應。請參閱[管理警示狀態](#)。

檢視警示定義

詳細的警示定義會在 [警示] 索引標籤中的個別面板上提供。您可以直接開啟面板，或透過按一下 [警示] 資料表中 [事件類型] 資料行中的值來進入。

警示詳細資料會在 NSX Manager 的數個位置顯示。請參閱[檢視警示資訊](#)。

程序

- 1 從 [警示] 索引標籤。
 - a 導覽至首頁，然後按一下**警示**。
[警示] 面板有兩種模式，如面板頂端所示：**警示**和**警示定義**。
 - b 按一下**警示定義**。
[警示] 索引標籤會重新顯示，以顯示 [警示定義] 資料表。

- 2 從 [第 0 層閘道] 頁面。
 - a 移至**網路 > 連線 > 第 0 層閘道**。
閘道資料表的 [未處理的警示] 資料行會顯示未處理的警示數目。
 - b 按一下 [未處理的警示] 資料行中的數字。
對話方塊隨即開啟，以資料表格式顯示未處理的警示。
 - c 按一下 [事件類型] 資料行中的值。
此動作會將您帶到上述的**首頁 > 警示 > 警示定義**面板。
- 3 從 [負載平衡設定] 頁面。
 - a 前往**網路 > 網路服務 > 負載平衡**。
閘道資料表的 [未處理的警示] 資料行會顯示未處理的警示數目。
 - b 按一下 [未處理的警示] 資料行中的數字。
對話方塊隨即開啟，以資料表格式顯示未處理的警示。
 - c 按一下 [事件類型] 資料行中的值。
此動作會將您帶到上述的**首頁 > 警示 > 警示定義**面板。
- 4 存取**警示定義**後，展開任何定義以檢視詳細資料和使用者可定義的設定。

警示定義詳細資料包括：

資料行	說明
功能	顯示警示的來源元件，例如：傳輸節點。
事件類型	顯示特定類型的錯誤，例如：CPU 使用率高。
嚴重性	顯示警示層級：嚴重、高或中。
已啟用	顯示是否已啟用警示偵測。
建立警示	顯示是否在介面或 API 中報告警示。
建立 SNMP 設陷	顯示在偵測到警示或解決警示時，系統是否會發出 SNMP 設陷。

此面板也會顯示下列項目：

項目	說明
說明	說明觸發警示的條件。
建議的動作	說明可採取以來更正情況的步驟。
事件 true 的 SNMP OID	顯示事件狀態為 true 時的 SNMP 物件識別碼。
事件 false 的 SNMP OID	顯示事件狀態為 false 時的 SNMP 物件識別碼。
臨界值	使用者設定用於觸發警示的臨界值。
敏感度 (%)	使用者設定用於觸發警示的敏感度。

後續步驟

警示定義中的某些欄位可以修改。請參閱[設定警示定義設定](#)。

設定警示定義設定

警示定義中的數個設定可進行自訂。從 [警示定義] 頁面，您可以啟用或停用警示、設定事件 (如果為 true) 是否建立警示、建立 SNMP 設陷、設定警示臨界值，以及設定警示敏感度。從 [警示定義] 頁面，您可以啟用或停用警示偵測、是否在 API/使用者介面中報告警示，以及是否在偵測到警示或解決警示時發出 SNMP 設陷。

您可以設定下列警示定義設定：

設定	控制類型	說明
已啟用	切換	啟用或停用警示偵測。
建立警示	切換	啟用或停用是否在 API/UI 中報告警示。
建立 SNMP 設陷	切換	啟用或停用是否在偵測到警示或解決警示時發出 SNMP 設陷。
臨界值	數值	設定用於觸發事件的臨界值。此值可判斷單一取樣是否為 true，並觸發事件。 <ul style="list-style-type: none"> 對於 CPU、磁碟和記憶體警示，臨界值為百分比使用率值，以指出警示條件。 對於憑證或授權到期警示，這是到期前的天數，包括本機密碼到期。
敏感度 (%)	數值 (百分比)	設定用於觸發警示的敏感度。敏感度可定義觸發警示的條件。(取樣大小是內部定義的，因此無法修改。)如果取樣大小為十且敏感度設為 80%，則取樣十個中發生八次或以上便會引發警示。請參閱 NSX-T Data Center REST API 說明文件 。

程序

- 1 導覽至首頁，然後按一下**警示**。

[警示] 面板有兩種模式，如面板頂端所示：**警示**和**警示定義**。

- 2 按一下**警示定義**。

[警示] 索引標籤會重新顯示，以顯示 [警示定義] 面板。

- 3 在警示最左側資料行的三個垂直點圖示上按一下滑鼠右鍵，然後選取**編輯**。

選取的警示定義會展開以顯示定義詳細資料，並將可設定的設定置於編輯模式。

- 4 視需要修改設定。

- 5 按一下**儲存**。

後續步驟

如需有關警示定義的詳細資訊，請參閱[檢視警示定義](#)。如需 SNMP 設陷的詳細資料，請參閱[簡易網路管理通訊協定 \(SNMP\)](#)。

管理警示狀態

除了更正基礎原因以外，您還可以在警示清單中修改其狀態為已報告來管理警示。

觸發的警示可能為下列其中一個狀態：未處理、已確認、已隱藏或已解決。

程序

- 1 導覽至首頁，然後按一下**警示**。

[警示] 面板有兩種模式，如面板頂端所示：**警示**和**警示定義**。

- 2 如果尚未顯示面板，請按一下**警示**模式。

警示面板會顯示所有警示的清單，包括已解決的警示。

備註 已解決的警示將在其解決後持續列出最多八天。

- 3 在頁面上的資料表中找到警示，然後選取最左側資料行中的核取方塊。

- 4 按一下**動作**，然後選取所需的動作。

- 如果您將警示狀態變更為已確認，這表示您知道並已確認該警示。
- 如果您將警示移到已隱藏狀態，系統會提示您指定持續時間 (以小時為單位)。在指定的持續時間過後，警示狀態會還原為未處理。但是，如果系統判定情況已修正，則警示狀態會變更為已解決。
- 您可以將已確認或已隱藏警示的狀態還原為未處理。
- 您無法變更已解決警示的狀態。

[警示狀態] 資料行中的值會相應地更新。

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。

警示名稱	說明
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。
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 16-1. Management Pack for NSX-T Data Center 中的警示

警示	說明	建議
NSX-T Data Center 管理服務失敗	在 NSX-T Data Center 主機上的管理服務未執行時觸發。	請登入 NSX Manager，然後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 Data Center，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。	檢查 Edge 節點與控制器叢集和管理程式叢集的連線狀態，並修正中斷的連線。

表 16-1. Management Pack for NSX-T Data Center 中的警示 (續)

警示	說明	建議
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。	登入 NSX Manager，然後為邏輯路由器新增 NAT 規則。
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 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 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 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 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	登入 NSX 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。	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。	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。

表 16-1. Management Pack for NSX-T Data Center 中的警示 (續)

警示	說明	建議
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。	檢查 Edge 叢集狀態，並視需要遵循 NSX-T Data Center 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。	檢查邏輯交換器狀態，並視需要遵循 NSX-T Data Center 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。	檢查負載平衡器服務的運作狀態，並視需要遵循 NSX-T Data Center 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錯誤	負載平衡器服務的運作狀態包含錯誤時觸發。	檢查負載平衡器服務的運作狀態，並視需要遵循 NSX-T Data Center 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。	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 Data Center 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。	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 Data Center 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。	檢查 Edge 節點的組態狀態，並視需要遵循 NSX-T Data Center 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。	登入 NSX Manager VA，然後重新啟動失敗的管理服務。
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。	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 Data Center 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。

表 16-1. Management Pack for NSX-T Data Center 中的警示 (續)

警示	說明	建議
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。	登入 NSX Manager，並檢查管理程式節點的管理程式連線，然後遵循 NSX-T Data Center 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 16-2. 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	NSXNoUplinkConnectivityEvent	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	NSXRoutingAdvertisementEvent	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	NSXManagerConnectivityDownEvent	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	NSXControllerConnectivityDegradedEvent	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	NSXControllerConnectivityDownEvent	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	NSXMTuMismatchEvent	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 層邏輯路由器介面上設定的 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。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80211	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 與外部閘道上的 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。
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	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	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	NSXTHostNodeCtrlConnectivityStatusDownEvent	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	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	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	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	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」。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80229	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」。
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	NSXTEdgeNodeTunnelStatusDegradedEvent	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」。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80252	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。
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

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80262	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。
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	NSXTMPNodeServiceCmInventoryStatusEvent	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。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80408	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。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	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	NSXTMPNodeServiceNSXMessageBusStatusEvent	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	NSXTMPNodeServiceNSXPlatformClientStatusEvent	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	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	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	NSXTMPNodeServiceNTPStatusEvent	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	NSXTMPNodeServicePolicyStatusEvent	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	NSXTMPNodeServiceSearchStatusEvent	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	NSXTMPNodeServiceSNMPStatusEvent	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	NSXTMPNodeServiceSSHStatusEvent	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	NSXTMPNodeServiceSyslogStatusEvent	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	NSXTMPNodeServiceTelemetryStatusEvent	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	NSXTMPNodeServiceUIServiceStatusEvent	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	NSXTMPNodeServiceCmInventoryStatusEvent	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。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80403	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。
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 MgmtPlaneBusStatusEvent	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 MigrationCoordinatorStatusEvent	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 NodeMgmtStatusEvent	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 NodeStatsStatusEvent	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 NSXMessageBusStatusEvent	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 NSXPlatformClientStatusEvent	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 NSXUpgradeAgentStatusEvent	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。

表 16-2. 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
1.3.6.1.4.1.6876.100.1.0.80417	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。
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。

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

本章節討論下列主題：

- 新增 IPFIX 收集器
- 新增防火牆 IPFIX 設定檔
- 新增交換器 IPFIX 設定檔
- vSphere Distributed Switch 上的 IPFIX 監控
- 新增連接埠鏡像設定檔
- vSphere Distributed Switch 上的連接埠鏡像
- 執行 Traceflow
- 簡易網路管理通訊協定 (SNMP)
- 監控網狀架構節點
- 網路延遲統計資料
- 管理程式模式中的監控工具

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 <code>Global</code> 。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 <code>Global</code> 。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。
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**。

vSphere Distributed Switch 上的 IPFIX 監控

針對 NSX 分散式虛擬連接埠群組以及已連線至已啟用 VDS 交換器的 vSphere 分散式虛擬連接埠群組設定 IPFIX 監控，以支援 NSX-T 網路。

從 vSphere 中，為分散式虛擬連接埠群組 (vSphere) 啟用 IPFIX，並從 NSX Manager，為在 VDS 交換器上建立的區段 (NSX-T) 啟用 IPFIX。

若要為分散式虛擬連接埠群組啟用 IPFIX 監控，請參閱《vSphere 網路》說明文件。

若要為 NSX-T 連接埠群組啟用 IPFIX 監控，請參閱 [新增交換器 IPFIX 設定檔](#)。

針對 NSX-T 啟用的 VDS 交換器會顯示下列行為：

- 非上行和上行連接埠均支援以下項目的傳入和傳出雙向流量：
 - vSphere 上的連接埠、連接埠群組和虛擬機器。
 - NSX-T 上的區段、區段連接埠和群組
- 當封包來自或前往已啟用 IPFIX 的非上行連接埠時，IPFIX 設定檔會對上行連接埠上的封包取樣。例如，假設 *VM-A* 和 *VM-B* 連線至非上行連接埠 (port-1、port-2)，其中，連線至 *VM-A* 的 port-1 已啟用 IPFIX，並且連線至 *VM-B* 的 port-2 未啟用 IPFIX。當您從 *VM-A* 和 *VM-B* 傳送流量至 port-1 時，僅對來自 *VM-A* 的封包進行取樣，因為僅在 *VM-A* 連線到的連接埠上啟用 IPFIX。IPFIX 不會對來自 port-2、與 *VM-B* 相關聯的封包進行取樣，因為未在該連接埠上啟用 IPFIX。
- 匯出至 IPFIX 收集器的封包計數是以取樣速率 (而非取樣的封包) 為基礎的總計數。例如，IPFIX 會計算封包的總計數，並匯出資訊。對於 100 個傳入封包，IPFIX 可能會取樣 9-11 個封包。它會將 90 或 110 個封包匯出至 IPFIX 收集器。

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。

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。

程序

- 1 從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**。

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

vSphere Distributed Switch 上的連接埠鏡像

您可以針對連接埠群組、虛擬機器的虛擬 NIC 和在 NSX-T 中建立的虛擬機器，以及在連線至 vSphere Distributed Switch (VDS) 交換器的 vSphere 中所建立 vSphere 分散式虛擬連接埠群組設定連接埠鏡像。

在 vCenter Server 中，為 VDS 交換器上的 vSphere 分散式虛擬連接埠群組設定連接埠鏡像。

在 NSX Manager 中，針對 VDS 交換器上的區段 (在 NSX-T 中) 設定連接埠鏡像。

備註 您無法編輯在 vCenter Server 中的 NSX-T 建立之區段的組態。身為 admin，您可以檢視連接埠鏡像工作階段的內容，以得知建立其所在的交換器。

若要在 vSphere 分散式虛擬連接埠群組上啟用連接埠鏡像，請參閱《vSphere 網路》說明文件。

若要同時從 NSX Manager 中的原則和管理程式模式在 NSX-T 中的區段、連接埠、群組上啟用連接埠鏡像，請參閱：

- [新增連接埠鏡像設定檔](#)
- [在管理程式模式中監控連接埠鏡像工作階段](#)

整併和遠端 SPAN 之間的上行衝突

在 vSphere 中，依預設，整併原則中的**遠端 SPAN** 會設為不允許。如果您使用所有可用的實體 NIC 來設定遠端 SPAN，則沒有可用上行可供整併原則使用。任何可用上行的無法使用表示目的地連接埠上不允許上行流量，因此導致組態錯誤。

但是，在 NSX-T 中，依預設，**目的地連接埠上的一般 I/O** 會設為已允許。在 NSX-T 中，針對 N-VDS 交換器上的 NSX 連接埠群組設定的連接埠鏡像會允許在目的地連接埠上進行整併和連接埠鏡像。因此，NSX-T 中不會發生上行組態錯誤。

若要解決設定整併和遠端 SPAN 時的上行衝突：

- 確保有可用上行可供使用。例如，在具有 2 個實體 NIC 的 ESXi 主機上，請勿在遠端 SPAN 連接埠鏡像設定檔中將這兩個上行同時指派為目的地 IP 位址，以避免組態中發生上行衝突。至少必須有一個可在整併設定檔中設定的可用上行。
- 在 vCenter Server 中，編輯連接埠鏡像組態設定檔，並將**目的地連接埠上的一般 I/O** 設為已允許。

執行 Traceflow

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。

備註 VLAN 支援的邏輯交換器或區段不支援 Traceflow。

程序

- 1 從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 > 疑難排解工具 > 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]、[多點傳播] 和 [廣播]。IPv6 位址的流量類型選項為 [單點傳播] 或 [多點傳播]。

附註：在 VMware Cloud (VMC) 環境不支援多點傳播和廣播。

- 5 (選擇性) 選取通訊協定，並提供相關資訊。

通訊協定	參數
DHCP	選取 DHCP OP 代碼： 開機要求 或 開機回覆 。
DHCPv6	選取 DHCP 訊息類型： 請求 、 通告 、 要求 或 回覆 。 備註 只有在為 IP 位址選取了 IPv6 時，才能使用此選項。
DNS	指定位址，然後選取訊息類型： 查詢 或 回應 。
ICMP	指定 ICMP 識別碼和序列。
ICMPv6	指定 ICMP 識別碼和序列。 備註 只有在為 IP 位址選取了 IPv6 時，才能使用此選項。
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。

對於 TCP 通訊協定，請注意下列事項：

- 預設旗標為 SYN。
- SYN 無法與 RST 或 FIN 結合。
- 若未選取 SYN，則必須選取 ACK 或 RST。
- ACK 無法與 FIN、PSH 或 URG 結合。

6 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。
多點傳播	步驟同上。	輸入 IP 位址。必須是來自 224.0.0.0 - 239.255.255.255 的多點傳播位址。
廣播	步驟同上。	輸入子網路首碼長度。

7 (選擇性) 按一下 **進階設定** 以查看進階選項。

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 按一下 **追蹤**。

輸出會包含拓撲的圖形對應，以及列出所觀察封包的表格。列出的第一個封包會具有觀察類型 `Injected`，並顯示在插入點插入的封包。

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。

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。

NSX-T Data Center 中的 SNMP 架構可讓您使用 SNMP 管理程式監控各種系統實體 (例如 NSX Edge 上的磁碟) 和邏輯實體 (例如 NSX Edge VPN 通道)。此架構可讓 NSX-T Data Center 類別和平台定義要監控以及可用於讓其 SNMP 管理程式與 NSX-T Data Center 進行互動的 SNMP MIB 物件。

若要下載 SNMP MIB 檔案，請參閱[知識庫文章 1013445 : SNMP MIB module file download \(SNMP MIB 模組檔案下載\)](#)。下載並使用 **VMWARE-NSX-MIB.mib** 檔。

如需 SNMP 組態，請參閱 VMware vSphere 產品說明文件中的〈為 ESXi 設定 SNMP〉。

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》。

監控網狀架構節點

您可以從 NSX Manager UI 監控網狀架構節點，例如主機、Edge、NSX Edge 叢集、橋接器以及傳輸節點。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取導覽面板中的**系統 > 網狀架構 > 節點**。
- 3 選取下列其中一個索引標籤。
 - 主機
 - Edge
 - Edge 叢集
 - 橋接器
 - 傳輸節點

結果

備註 在 [主機] 畫面中，如果某個主機的 MPA 連線狀態為 [關閉] 或 [未知]，請忽略 LCP 連線狀態，因為此狀態可能不精確。

網路延遲統計資料

在網路中，延遲可能會在資料路徑中的多個端點上累積。身為網路管理員，您需要能夠監控網路的延遲，以診斷網路中的效能瓶頸，並對其進行疑難排解。

您可以測量主機傳輸節點上的下列網路延遲統計資料：

- pNIC 至 vNIC
- vNIC 至 pNIC
- vNIC 至 vNIC
- VTEP 至 VTEP

在 NSX-T Data Center 中，測量延遲統計資料時會受到下列限制：

- 在資料平面中，僅支援對 ESXi 主機傳輸節點測量網路延遲。
- 不支援 KVM 主機和 Edge 傳輸節點。
- 在 VLAN 區段上，只有在兩個 vNIC 屬於相同 ESXi 主機上的虛擬機器時，才會測量網路延遲。
- 當虛擬機器連結至不同的區段時，只有在資料流量透過 ESXi 主機傳輸節點上的分散式路由器 (DR) 執行個體進行路由時，才會測量網路延遲。如果透過 Edge 傳輸節點上的 DR 執行個體路由資料流量，則不會測量網路延遲。
- 增強型網路堆疊 (ENS) 不支援 vNIC 至 pNIC、pNIC 至 vNIC，以及 vNIC 至 vNIC 的延遲。
- 使用合作夥伴服務虛擬機器設定東西向網路流量保護時，不支援延遲測量。在服務虛擬機器 (SVM) 和客體虛擬機器的連接埠上會停用延遲監控。

您可以將延遲資料匯出至外部網路效能監控工具，並對資料執行分析。外部監控工具也稱為收集器。使用收集器，可以達到更高的網路可見度、最佳化網路效能，以及識別資料路徑中會導致網路嚴重延遲的端點。

設定主機以測量網路延遲統計資料後，主機上的網路作業代理程式 (netopa) 會定期輪詢資料平面。有可用的延遲資料後，代理程式會以預先設定的間隔將該資料匯出至外部收集器。

備註

- netopa 代理程式只能將網路延遲統計資料匯出至 vRealize Network Insight (vRNI)。目前不支援其他收集器工具。
- 您可以將 ESXi 主機設定為僅使用 NSX REST API 來測量網路延遲統計資料。

下列支援對照表摘要了各種網路延遲統計資料支援的傳輸節點和收集器。

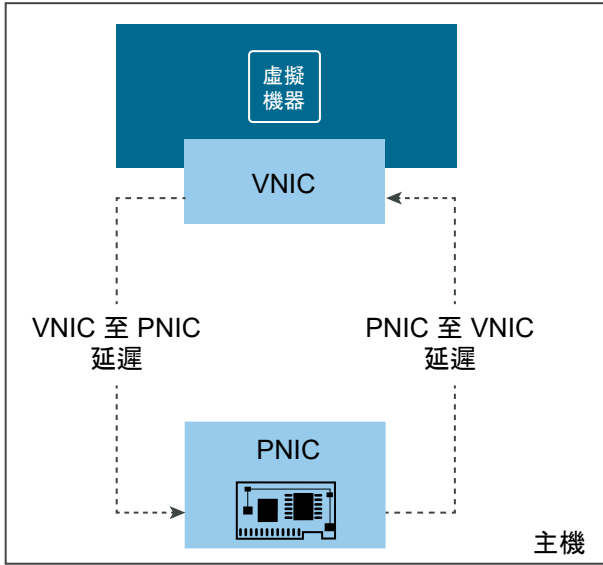
表 17-1. 支援對照表

網路延遲統計資料	起始 NSX-T Data Center 版本	支援的傳輸節點	支援的收集器	註解
VTEP 至 VTEP	2.5	ESXi 主機	vRNI 5.0 或更新版本	
pNIC 至 vNIC vNIC 至 pNIC vNIC 至 vNIC	3.0	ESXi 主機	vRNI 5.3	從 NSX-T Data Center 3.0.2 開始，支援將統計資料匯出至 vRNI 5.3。

您可以測量獨立 ESXi 主機的網路延遲統計資料，也可對屬於 vCenter Server 叢集的 ESXi 主機進行測量。不過，只有 vCenter 管理的 ESXi 主機所產生的網路延遲統計資料可匯出至 vRNI。vRNI 不支援從非由 vCenter Server 管理的獨立 ESXi 主機收集延遲統計資料。

pNIC 至 vNIC 和 vNIC 至 pNIC 的延遲

在主機傳輸節點上啟用 pNIC 延遲測量時，系統會針對主機傳輸節點上的每個 vNIC 計算 vNIC 至 pNIC 的延遲和 pNIC 至 vNIC 的延遲。



pNIC 至 vNIC 和 vNIC 至 pNIC 的延遲統計資料會以下列格式匯出至外部收集器：

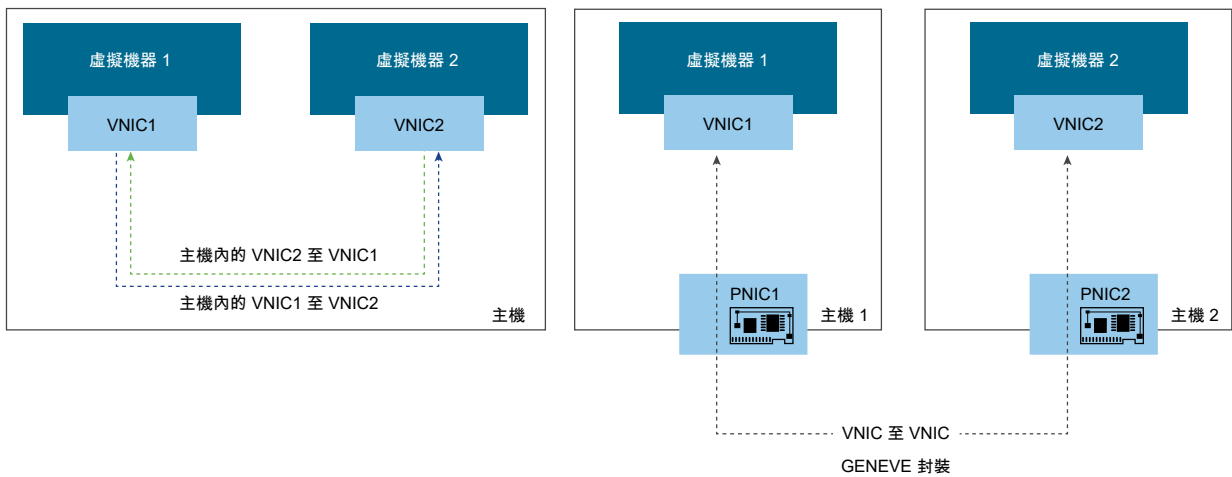
Endpoint1, Endpoint2, Max, Min, Avg

其中：

- *Endpoint1, Endpoint2* 可以是虛擬介面識別碼 (VIF 識別碼)，或是 ESXi 主機 (vmnic) 上實體介面卡的名稱。
- *Max, Min* 和 *Avg* 表示兩個端點之間的最大、最小和平均延遲值 (以微秒為單位)。

vNIC 至 vNIC 的延遲

此延遲表示資料封包從來源 vNIC 傳輸到目的地 vNIC (位於相同 ESXi 主機或不同的 ESXi 主機上) 所花費的時間。如果 vNIC 位於不同的 ESXi 主機上，則主機之間的覆疊通道中僅支援 GENEVE 封裝通訊協定。



vNIC 至 vNIC 網路延遲的計算方式如下：

- 當 VM1 上的來源 vNIC1 和 VM2 上的目的地 vNIC2 位於相同的主機時，將會計算每個行程的單一行程延遲，並匯出至收集器。換句話說，每個 vNIC1 至 vNIC2 行程和 vNIC2 至 vNIC1 行程的延遲會個別計算。
- 當 VM1 上的來源 vNIC1 和 VM2 上的目的地 vNIC2 位於不同的主機時，將會計算來回行程延遲總計，且只會將單一延遲值匯出至收集器。如果沒有從 vNIC2 至 vNIC1 的傳回流量，則不會將任何網路延遲匯出至收集器。

備註 NSX-T Data Center 會使用 GENEVE 封裝封包中的時間戳記，直接計算主機之間從 vNIC 到 vNIC 的延遲。您無須啟用主機上的 pNIC 延遲測量，以及 VTEP 至 VTEP 的延遲。pNIC 至 vNIC、vNIC 至 pNIC，以及 VTEP 至 VTEP 的統計資料，與 vNIC 至 vNIC 的統計資料無關。

vNIC 至 vNIC 的延遲統計資料會以下列格式匯出至外部收集器：

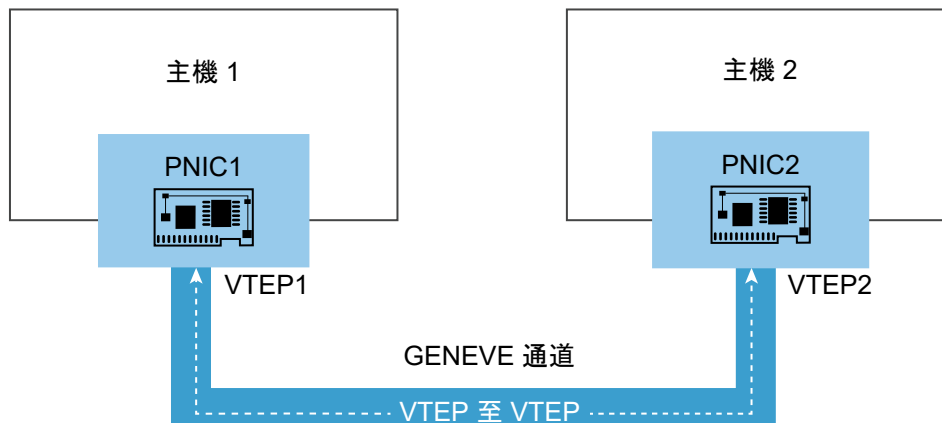
VIF1、*VIF2*、*Max*、*Min*、*Avg*

其中：

- *VIF1*、*VIF2* 代表虛擬介面或 vNIC。
- *Max*、*Min* 和 *Avg* 表示兩個 vNIC 之間的最大、最小和平均延遲值 (以微秒為單位)。

VTEP 至 VTEP 的延遲

此延遲表示資料封包從來源 VTEP 傳輸到目的地 VTEP 所花費的來回行程時間總計。若要測量 VTEP 至 VTEP 的延遲，您必須在傳輸區域設定檔中啟用延遲。



若要計算 ESXi 主機之間的 VTEP 至 VTEP 延遲，請使用雙向流量偵測 (BFD) 通訊協定。NSX-T Data Center 會使用裝載中的時間戳記延伸 BFD 通訊協定，以支援 VTEP 之間的延遲計算。BFD 封包會以固定間隔在主機之間的每個通道中傳輸，以計算 VTEP 至 VTEP 的延遲。

■ 測量網路延遲統計資料

您可以設定網路中的 ESXi 主機，以測量：pNIC 至 vNIC、vNIC 至 pNIC、vNIC 至 vNIC，以及 VTEP 以 VTEP 網路延遲統計資料。

■ 匯出網路延遲統計資料

您可以將網路延遲統計資料匯出至外部收集器，並對資料執行分析。在 ESXi 主機中執行的 netopa 代理程式，只能將網路延遲統計資料匯出至 vRealize Network Insight (vRNI)。目前不支援其他收集器工具。

測量網路延遲統計資料

您可以設定網路中的 ESXi 主機，以測量：pNIC 至 vNIC、vNIC 至 pNIC、vNIC 至 vNIC，以及 VTEP 以 VTEP 網路延遲統計資料。

僅支援使用 NSX REST API 進行設定。下列程序中的步驟會列出您在設定各種網路延遲統計資料的計算時，所必須執行的管理平面 API。如需關於 API 結構描述、範例要求、範例回應，以及所有 API 之錯誤訊息的詳細資訊，您必須閱讀《NSX-T Data Center API 指南》。

必要條件

若要設定以測量網路延遲統計資料的主機 (包括 vCenter 管理的主機和獨立 ESXi 主機)，則必須做好 NSX-T Data Center 的準備。也就是說，必須在您網路中的所有 ESXi 主機上安裝 NSX-T Data Center 元件。

程序

- 1 若要計算 vNIC 至 vNIC、pNIC 至 vNIC，以及 vNIC 至 pNIC 的網路延遲統計資料，請執行下列步驟：

- a 使用下列 POST API 建立延遲設定檔：

```
POST https://<NSX-Manager-IP>/api/v1/latency-profiles
```

依預設，系統會針對主機傳輸節點上的所有 vNIC 測量 vNIC 至 vNIC 的延遲。

在此 API 的要求本文中，設定下列資訊：

- 啟用或停用主機上的 pNIC 延遲。啟用時，系統會針對主機傳輸節點上的每個 vNIC 計算 pNIC 至 vNIC 和 vNIC 至 pNIC 的延遲。
- 指定取樣速率或取樣間隔。

如果同時設定這兩項，將優先適用取樣間隔。

- b 使用下列 POST API，在 NSGroupsSimpleExpression 中建立以傳輸節點作為目標類型的 NSGroup：

```
POST https://<NSX-Manager-IP>/api/v1/ns-groups
```

如果您已在 UI 中啟用**管理程式**模式，則可以使用該 UI 建立 NSGroup，並在成員資格準則中指定傳輸節點。

- c 使用下列 POST API 建立服務組態設定檔：

```
POST https://<NSX-Manager-IP>/api/v1/service-configs
```

此 API 會結合您在先前的步驟中建立的延遲設定檔和 NSGroup。

2 若要測量 VTEP 至 VTEP 的延遲統計資料，請在 BFD 健全狀況監控設定檔中啟用延遲 (這是傳輸區域設定檔中的資源類型)。請執行下列 PUT 或 POST API：

- POST `https://<NSX-Manager-IP>/api/v1/transportzone-profiles`
- PUT `https://<NSX-Manager-IP>/api/v1/transportzone-profiles/<transportzone-profile-id>`

後續步驟

將統計資料匯出至外部收集器，以取得更深入的網路見解，以及對網路特定的延遲問題進行疑難排解。

匯出網路延遲統計資料

您可以將網路延遲統計資料匯出至外部收集器，並對資料執行分析。在 ESXi 主機中執行的 netopa 代理程式，只能將網路延遲統計資料匯出至 vRealize Network Insight (vRNI)。目前不支援其他收集器工具。

在 vRNI 中，您只能從 vCenter 管理的 ESXi 主機收集網路延遲統計資料。vRNI 不支援從非由 vCenter Server 管理的獨立 ESXi 主機收集延遲統計資料。

您可以使用下列其中一種方法來匯出網路延遲統計資料：

- 方法 1：在 NSX-T Data Center 中使用管理平面 API。
- 方法 2：在 vRNI UI 中啟用選用設定，以收集延遲統計資料。

必要條件

- 在 vRNI UI 中，以指定順序完成下列工作：
 - a 將 vCenter Server 新增為資料來源。如果您在 NSX-T Data Center 環境中將多個 vCenter Server 新增為計算管理程式，則可以將所有 vCenter Server 新增為資料來源。
 - b 將 NSX Manager 新增為資料來源。

如需在 vRNI 中新增資料來源的詳細說明，請參閱《使用 vRealize Network Insight》說明文件，網址是 <https://docs.vmware.com/tw/VMware-vRealize-Network-Insight/index.html>。

- 確定已在收集器上開啟連接埠 1991，以便接收來自 ESXi 主機的網路延遲資料。

程序

1 方法 1：使用 NSX-T Data Center REST API。

- a 確定您已設定 ESXi 主機，以測量網路延遲統計資料。

如需詳細步驟，請參閱[測量網路延遲統計資料](#)。

- b 使用下列 PUT API，將網路延遲統計資料匯出至收集器：

```
PUT https://<manager-ip>/api/v1/global-configs/OperationCollectorGlobalConfig
-d '<content>'
```

在此 API 的要求本文中，設定下列資訊：

- 外部收集器的詳細資料，例如收集器 IP 位址與收集器連接埠。
- 控制 netopa 代理程式將統計資料傳送至收集器之頻率的報告間隔。

2 方法 2：在 vRNI UI 中啟用選用設定，以收集延遲統計資料。

當您將 NSX Manager 新增為 vRNI 中的資料來源時，請選取**啟用延遲度量收集**核取方塊。此選項可讓 vRNI 從 ESXi 主機收集延遲統計資料。

如需關於在 vRNI 中將 NSX Manager 新增為資料來源的詳細資訊，請參閱《使用 vRealize Network Insight》說明文件。

結果

vNIC 至 vNIC 的延遲統計資料會以下列格式匯出至外部收集器：

```
VIF1、VIF2、Max、Min、Avg
```

其中：

- *VIF1*、*VIF2* 代表虛擬介面或 vNIC。
- *Max*、*Min* 和 *Avg* 表示兩個 vNIC 之間的最大、最小和平均時間 (以微秒為單位)。

pNIC 至 vNIC 和 vNIC 至 pNIC 的延遲統計資料會以下列格式匯出至外部收集器：

```
Endpoint1、Endpoint2、Max、Min、Avg
```

其中：

- *Endpoint1*、*Endpoint2* 可以是虛擬介面識別碼 (VIF 識別碼)，或是 ESXi 主機 (vmnic) 上實體介面卡的名稱。
- *Max*、*Min* 和 *Avg* 表示兩個端點之間的最大、最小和平均時間 (以微秒為單位)。

管理程式模式中的監控工具

NSX-T 支援在**管理程式**模式中的監控方法，包括檢視連接埠連線、Traceflow、連接埠鏡像和活動監控。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到原則和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取導覽面板中的**計劃和疑難排解 > 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。

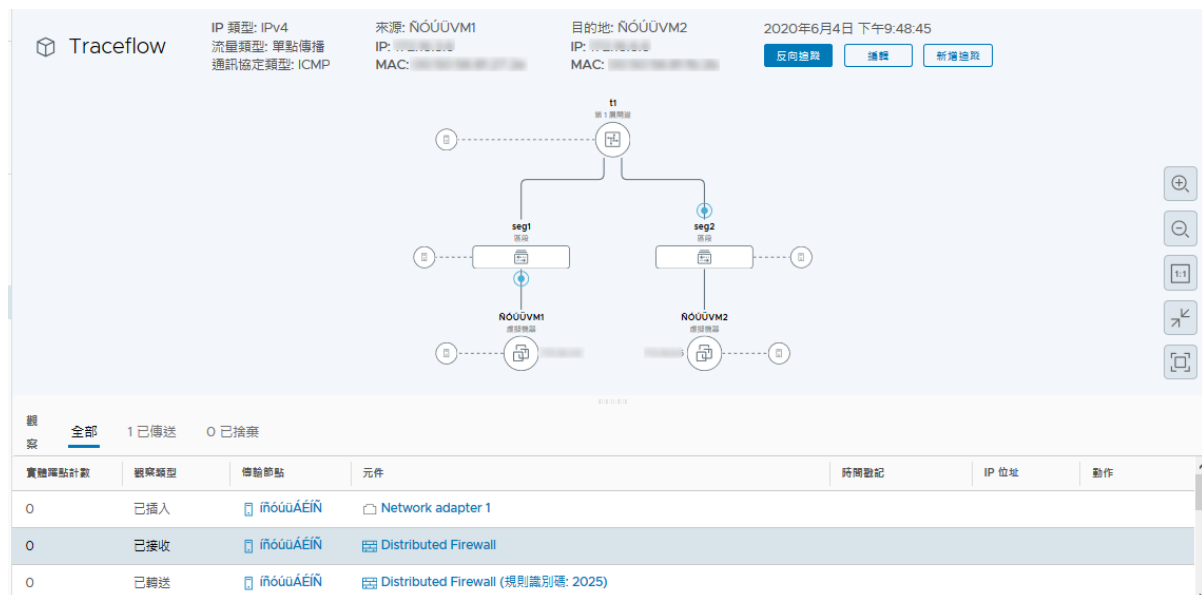
Traceflow

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。

NSX Manager 介面會以圖形方式，根據您所設定的參數 (IP 位址類型、流量類型、來源和目的地) 顯示追蹤路由。此顯示頁面也可讓您編輯參數、反向追蹤 Traceflow，或建立新的參數。

圖 17-1. Traceflow 圖範例



什麼是 Traceflow ？

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。

Traceflow 參數

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-T Data Center 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-T Data Center 分散式邏輯路由器來連線。

如果已設定 NSX-T Data Center 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。

對於單點傳播 Traceflow 封包，您可以觀察封包複寫和/或在 Traceflow 觀察中的洪泛。

- 如果邏輯交換器不知道封包的目的地 TEP，則會複寫 Traceflow 封包。
- 如果 N-VDS 或 VDS 不知道封包的目的地虛擬交換器連接埠，則 Traceflow 封包會有洪泛。

您可以將多點傳播和廣播封包指定為 Traceflow 封包。

- 多點傳播流量的來源為虛擬機器 vNIC 或邏輯連接埠，目的地則為多點傳播 IP 位址。
- 對於廣播流量，來源為虛擬機器 vNIC 或邏輯連接埠，而第 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-T Data Center 計算封包的 IP 網路位址。多點傳播或廣播 Traceflow 封包可傳遞至多個虛擬機器 vNIC 或 Edge 上行，導致產生多個已傳送的觀察。

在管理程式模式中使用 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**計劃和疑難排解** > **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]、[多點傳播] 和 [廣播]。IPv6 位址的流量類型選項為 [單點傳播] 或 [多點傳播]。

附註：在 VMware Cloud (VMC) 環境不支援多點傳播和廣播。

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。
多點傳播	步驟同上。	輸入 IP 位址。必須是來自 224.0.0.0 - 239.255.255.255 的多點傳播位址。
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。

在管理程式模式中監控連接埠鏡像工作階段

您可以監控連接埠鏡像工作階段以用於疑難排解或其他目的。

請注意，邏輯 SPAN 僅支援覆疊邏輯交換器，而非 VLAN 邏輯交換器。

NSX Cloud 附註 若使用 NSX Cloud，請參閱 [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。
- 使用數據平面開發套件 (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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**計劃和疑難排解 > 連接埠鏡像 > 連接埠鏡像工作階段**。
- 3 按一下**新增**，然後選取工作階段類型。
 可用的類型為**本機 SPAN**、**遠端 SPAN**、**遠端 L3 SPAN**，以及**邏輯 SPAN**。
- 4 輸入工作階段名稱，並選擇性地輸入說明。

5 提供其他參數。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 傳輸節點 - 選取傳輸節點。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。
遠端 SPAN	<ul style="list-style-type: none"> ■ 工作階段類型 - 選取 RSPAN 來源工作階段或 RSPAN 目的地工作階段。 ■ 傳輸節點 - 選取傳輸節點。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。 ■ 封裝 VLAN 識別碼 - 指定封裝 VLAN 識別碼。 ■ 保留原始 VLAN - 選取是否要保留原始 VLAN 識別碼。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 封裝 - 選取 GRE、ERSPAN II 或 ERSPAN III。 ■ GRE 機碼 - 如果封裝為 GRE，請指定 GRE 機碼。ERSPAN 識別碼 - 如果封裝為 ERSPAN II 或 ERSPAN III，請指定 ERSPAN 識別碼。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 邏輯交換器 - 選取邏輯交換器。 ■ 方向 - 選取雙向、入口或出口。 ■ 封包截斷 - 選取封包截斷值。

6 按下一步。

7 提供來源資訊。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 選取 N-VDS。 ■ 選取實體介面。 ■ 啟用或停用封裝式封包。 ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。 ■ 選取邏輯交換器。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 選取邏輯連接埠。

8 按下一步。

9 提供目的地資訊。

工作階段類型	參數
本機 SPAN	<ul style="list-style-type: none"> ■ 選取虛擬機器。 ■ 選取虛擬介面。
遠端 SPAN	<ul style="list-style-type: none"> ■ 選取 N-VDS。 ■ 選取實體介面。
遠端 L3 SPAN	<ul style="list-style-type: none"> ■ 指定 IPv4 位址。
邏輯 SPAN	<ul style="list-style-type: none"> ■ 選取邏輯連接埠。

10 按一下儲存。

儲存連接埠鏡像工作階段後，無法變更來源或目的地。

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-ddlee0e10b34"
    ]
  },
  "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。

在管理程式模式中設定 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。

在管理程式模式中設定交換器 IPFIX 收集器

您可以設定交換器的 IPFIX 收集器。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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**計劃和疑難排解 > 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**。

在管理程式模式中設定交換器 IPFIX 設定檔

您可以設定交換器的 IPFIX 設定檔。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 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**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 <code>Global</code> 。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**。

在管理程式模式中設定防火牆 IPFIX 收集器

您可以設定防火牆的 IPFIX 收集器。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**計劃和疑難排解 > 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。

在管理程式模式中設定防火牆 IPFIX 設定檔

您可以設定防火牆的 IPFIX 設定檔。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 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**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 <code>Global</code> 。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

元素識別碼	參數名稱	資料類型	單位
886	tenantSourcePort	unsigned16	2 位元組
887	tenantDestPort	unsigned16	2 位元組
888	egressInterfaceAttr	unsigned16	2 位元組
889	vxlanExportRole	unsigned8	1 位元組
890	ingressInterfaceAttr	unsigned16	2 位元組
898	virtualObsID	字串	變數長度

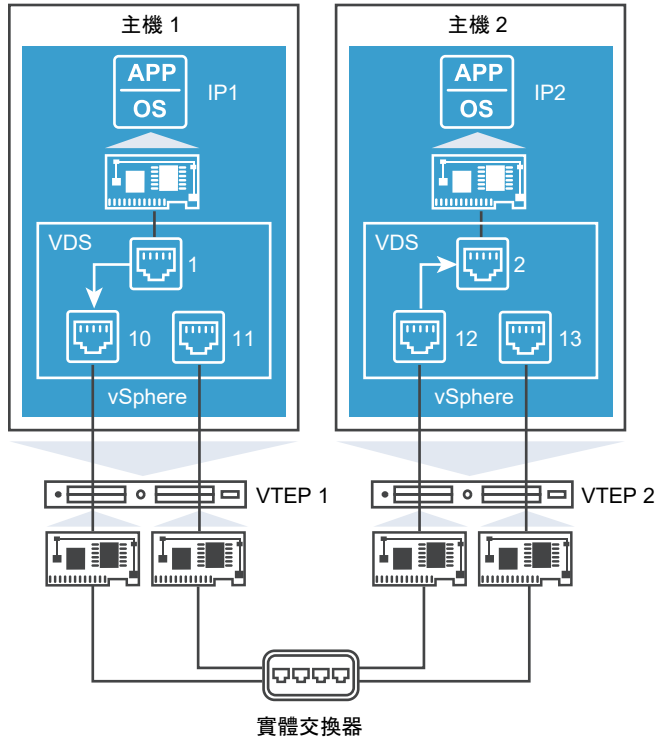
下表列出分散式防火牆 IPFIX 封包中的 VMware 特定元素。

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 封装式範本

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

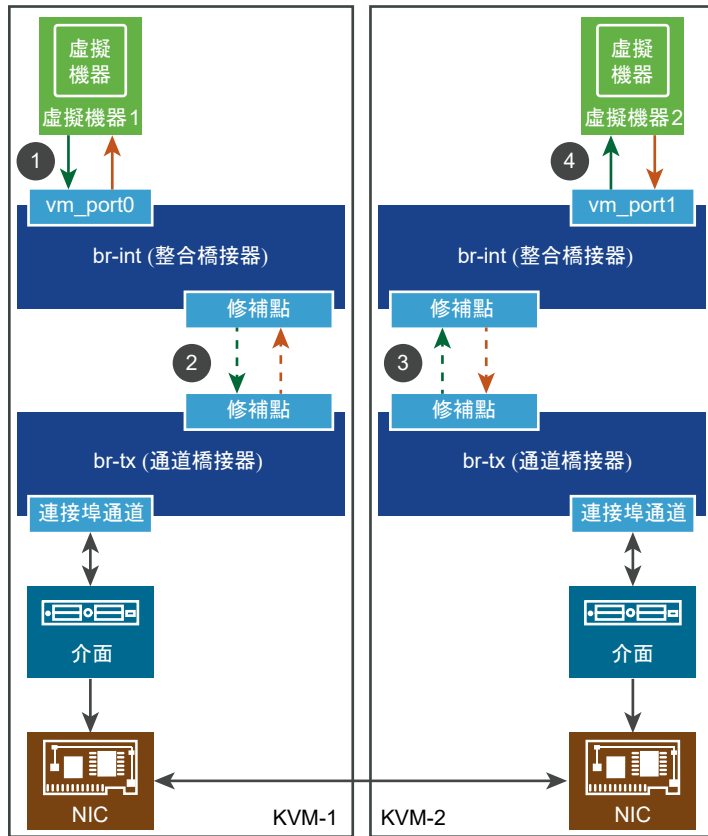
一個 KVM 主機傳輸節點支援 88 個 IPFIX 流程範本和一個選項範本。

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。

在管理程式模式中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[在管理程式模式中將虛擬機器連線到邏輯交換器](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

確認已設定邏輯交換器連接埠。請參閱[在管理程式模式中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**網路 > 邏輯交換器 > 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 若要下載主機已學習 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](#)。

您可以使用本機使用者帳戶、由 VMware Identity Manager (vIDM) 管理的使用者帳戶，或由目錄服務 (例如 Active Directory over LDAP/OpenLDAP) 所管理的使用者帳戶來登入 NSX Manager。您也可以將角色指派給 vIDM 或目錄服務所管理的使用者帳戶，以實作角色型存取控制。

NSX Manager 僅會辨識系統產生的工作階段識別碼，並在管理員登出或其他工作階段終止時，使工作階段識別碼失效。登入成功後，NSX Manager 會使用亂數產生器來建立隨機工作階段識別碼，並將該識別碼儲存在記憶體中。用戶端向 NSX Manager 提出要求時，僅允許用戶端在其呈現的工作階段識別碼與伺服器產生的其中一個識別碼相符時才進行驗證。當任何使用者登出 NSX Manager 時，工作階段識別碼會立即銷毀，且無法重複使用。

透過 UI、API 和 CLI 存取 NSX Manager，會受到驗證和授權的約束。此外，此類存取會產生稽核記錄。此記錄依預設為啟用，且無法停用。工作階段稽核會在系統啟動時啟動。透過在記錄訊息結構化資料部分中的文字 `audit="true"`，可區分稽核記錄訊息。

NSX 應用裝置上的本機使用者密碼可使用在 `/etc/shadow` 中儲存雜湊和 Salt 表示的預設 Linux/PAM 程式庫進行保護。在驗證期間，系統會對使用者輸入的密碼進行模糊處理。其他密碼會使用儲存在本機檔案系統中的隨機金鑰進行加密。

本章節討論下列主題：

- 本機使用者帳戶
- 與 VMware Identity Manager/Workspace ONE Access 整合
- 與 LDAP 整合
- 新增角色指派或主體身分識別
- 同時設定 vIDM 和 LDAP 或從 vIDM 轉換至 LDAP
- 角色型存取控制
- 記錄使用者帳戶變更

本機使用者帳戶

每個 NSX-T 應用裝置都有三個本機帳戶，`admin`、`audit` 和 `root`。若要管理 NSX-T，您必須以管理員身分登入。

root 使用者具有特殊權限。除非基於 VMware 的指引，否則請勿以 root 身分登入並進行本指南中未記錄的變更。root 使用者所做的變更可能會導致災難性失敗。在生產環境中，root 密碼應受到保護，且僅供特殊存取權限存取。

如需有關 NSX Manager 的其他安全性相關資訊，請參閱第 1 章 NSX Manager 中的〈安全性〉一節。

管理使用者的密碼或名稱

您可以透過 NSX-T 應用裝置的 CLI 來管理 admin 和 audit 使用者帳戶。

admin 使用者可以管理密碼和變更 admin 及 audit 使用者的名稱，但無法新增、刪除或停用使用者。對 admin 或 audit 使用者帳戶所做的任何變更將受到稽核。

稽核使用者對 NSX-T 環境具有讀取權限，且依預設為非作用中狀態。若要加以啟用，請以管理員身分登入，然後執行 `set user audit password` 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 admin 或 audit 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。如果您將密碼到期時間設為 30 天或更短的時間，則會一律顯示通知。通知包含變更密碼連結。按一下連結以變更使用者的密碼。

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 以 admin 的身分登入應用裝置的 CLI。
- 2 若要變更密碼，請執行 `set user <username> password` 命令。例如：

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

- 3 若要變更 admin 或 audit 使用者的名稱，請執行 `set user <username> username <new username>` 命令。例如：

```
nsx> set user admin username admin1
nsx>
```

- 4 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>
```

- 5 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>
```

- 6 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、Cloud Service Manager 和 NSX Intelligence 應用裝置。

備註 如果您有 NSX Manager 叢集，在任一 NSX Manager 上重設 `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〉。

如果您知道 `root` 的密碼，但忘記了 `admin` 或 `audit` 的密碼，則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 Intelligence 應用裝置或 Cloud Service Manager，請略過此步驟。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。然後，您可以使用上述程序重設 `admin` 或 `audit` 的密碼。

程序

- 1 連線至應用裝置的主控制台。
- 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，並將 `systemd.wants=PasswordRecovery.service` 新增到行尾。
- 8 按 **Ctrl-X** 進行開機。
- 9 當記錄訊息停止時，請輸入 `root` 的新密碼。
- 10 再次輸入密碼。
開機程序將繼續執行。
- 11 重新開機後，您可以使用 `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
```

與 VMware Identity Manager/Workspace ONE Access 整合

您可以設定 NSX Manager，以使用 VMware Identity Manager (vIDM) 來驗證使用者。

附註：VMware Identity Manager 的新產品名稱為 VMware Workspace ONE Access。

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。

從 vIDM 主機取得憑證指紋

設定 vIDM 與 NSX-T Data Center 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 3.3.2 版或更早版本的 vIDM 主機上，命令 `openssl` 可能執行較舊版本的 OpenSSL。在這種情況下，您必須使用命令 `openssl1`。只有在 vIDM 主機上才能使用此命令。

您可以使用以下命令，來檢查您的 OpenSSL 版本：

```
openssl version
```

在非 vIDM 主機的伺服器中，您可以使用執行 OpenSSL 1.x 版或更新版本的 `openssl` 命令。

程序

- 1 在 vIDM 主機的主控制台或以使用者 `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
```

- 如果您已登入 vIDM 主機，請執行下列一個動作：
 - 如果 OpenSSL 版本為 0.9.x 或更早版本，請執行以下命令：

```
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 OpenSSL 版本為 1.x 或更新版本，請執行以下命令：

```
openssl 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 `openssl` 命令 (即 `sudo`) 來執行 `sudo openssl ...`。

設定 VMware Identity Manager/Workspace ONE Access 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。

附註：VMware Identity Manager 的新產品名稱為 VMware Workspace ONE Access。

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://<csm-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 > 使用者和角色**。
- 3 按一下 **VMware Identity Manager** 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。

參數	說明
SSL 指紋	vIDM 主機的憑證指紋。它必須是 SHA-256 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。

- 按一下儲存。
- 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

- 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'
c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

- 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 c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
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。

與 LDAP 整合

您可以設定 NSX Manager，以使用目錄服務 (例如 Active Directory over LDAP/OpenLDAP) 來驗證使用者。

如果您使用 Active Directory (AD)，且您的 AD 樹系由多個子網域組成，則您應將 NSX-T Data Center 指向 AD 通用類別目錄 (GC)，並每個子網域設定為 NSX 中的替代網域名稱。通用類別目錄服務通常執行於您的主要 AD 網域控制站上，是所有主要和次要網域中最重要資訊的唯讀複本。GC 服務執行於連接埠 3268 (純文字) 和 3269 (透過 TLS 的 LDAP，已加密) 上。

例如，如果您的主要網域是「example.com」，且您有子網域「americas.example.com」和「emea.example.com」，則應：

- 1 將 NSX 設定為在連接埠 3268 上使用 LDAP 通訊協定，或在連接埠 3269 上使用 LDAPS 通訊協定。
- 2 在 NSX LDAP 組態中，新增替代網域名稱「americas.example.com」和「emea.example.com」。其中一個子網域中的使用者必須在其登入名稱中使用適當的網域進行登入。例如，emea.example.com 網域中的使用者「john」必須以使用者名稱「john@emea.example.com」登入。

備註 全域管理程式 (聯盟) 不支援 LDAP 整合。

LDAP 身分識別來源

NSX Manager 可充當 LDAP 用戶端，並與 LDAP 伺服器互動。

可設定三個身分識別來源來進行使用者驗證。當使用者登入 NSX Manager 時，系統會根據使用者網域的適當 LDAP 伺服器來驗證使用者。LDAP 伺服器會使用驗證結果和使用者群組資訊回應。驗證成功後，系統會為使用者指派與其所屬群組對應的角色。

NSX Manager 不支援在負載平衡器後方的多個 LDAP 伺服器，以及 LDAPS 或 StartTLS。如果 LDAP 伺服器位於負載平衡器後方，請將 NSX 設定為直接連線至其中一個 LDAP 伺服器，而非負載平衡器虛擬 IP 位址。

備註 不支援將父系群組對應為 NSX 角色的巢狀 Active Directory 群組。

程序

- 1 導覽至系統 > 使用者和角色 > LDAP。
- 2 按一下**新增身分識別來源**。
- 3 輸入身分識別來源的**名稱**。
- 4 輸入**網域名稱**，此名稱必須對應於 Active Directory 伺服器的網域名稱 (如果使用 Active Directory)。
- 5 選取類型：**Active Directory over LDAP** 或 **Open LDAP** 之一。
- 6 按一下**設定**以設定 LDAP 伺服器。每個網域都支援一個 LDAP 伺服器。

主機名稱/IP	LDAP 伺服器的主機名稱或 IP 位址。
LDAP 通訊協定	選取 通訊協定 ：LDAP (不安全) 或 LDAPS (安全)。
連接埠	將根據選取的通訊協定填入預設連接埠。如果您的 LDAP 伺服器正在非標準連接埠上執行，您可以編輯此文字方塊以提供連接埠號碼。
連線狀態	填寫必要文字方塊 (包括 LDAP 伺服器資訊) 後，您可以按一下此處來測試連線。
使用 StartTLS	如果已選取，則會使用 LDAPv3 StartTLS 延伸來升級要使用加密的連線。若要判定是否應使用此選項，請洽詢您的 LDAP 伺服器管理員。 僅在選取 LDAP 通訊協定時才能使用此選項。

憑證	如果您使用 LDAPS 或 LDAP + StartTLS，則此文字方塊應包含伺服器的 PEM 編碼 x.509 憑證。如果您將此文字方塊保留空白，然後按一下 檢查狀態 連結，則 NSX 會連線至 LDAP 伺服器。接著，NSX 會擷取 LDAP 伺服器的憑證，並詢問您是否要信任該憑證。如果您確認憑證正確無誤，請按一下 確定 ，然後憑證文字方塊將填入已擷取的憑證。
繫結身分識別	格式為 user@domainName，您也可以指定辨別名稱。 對於 Active Directory，您可以使用 userPrincipalName (user@domainName) 或辨別名稱。對於 OpenLDAP，您必須提供辨別名稱。 此文字方塊為必填，除非您的 LDAP 伺服器支援匿名繫結，則此為選用。如果您不確定，請洽詢您的 LDAP 伺服器管理員。
密碼	輸入 LDAP 伺服器的密碼。 此文字方塊為必填，除非您的 LDAP 伺服器支援匿名繫結，則此為選用。請洽詢您的 LDAP 伺服器管理員。

7 按一下 **新增**。

8 輸入 **基本網域**。

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」。

您打算用於控制對 NSX-T Data Center 存取權的所有使用者和群組項目，必須包含在指定基本 DN 根目錄中的 LDAP 目錄樹狀結構內。如果基本 DN 的設定過於特定，例如 LDAP 樹狀結構中較深層的組織單位，則 NSX 可能會找不到尋找使用者並判斷群組成員資格時所需的項目。如果您不確定，最佳做法是選取廣泛的基本 DN。

9 您的 NSX-T Data Center 使用者現在可以使用其登入名稱 (後面接著 @ 和 LDAP 伺服器的網域名稱，例如 user_name@domain_name) 進行登入。

後續步驟

將角色指派給使用者和群組。請參閱 [新增角色指派或主體身分識別](#)。

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，或者如果您使用 LDAP 做為驗證提供者，則可以將角色指派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>
```

對於 LDAP，您可以將使用者群組設定為使用者角色對應資訊；群組會與 Active Directory (AD) 中指定的使用者群組對應。若要授與 NSX 的使用者權限，請將該使用者新增至 AD 中的對應群組。

必要條件

您必須已設定驗證提供者：

- 對於 vIDM 的角色指派，確認 vIDM 主機與 NSX-T 建立關聯。如需詳細資訊，請參閱 [設定 VMware Identity Manager/Workspace ONE Access 整合](#)。
- 對於 LDAP 的角色指派，確認您具有 LDAP 身分識別來源。如需詳細資訊，請參閱 [LDAP 身分識別來源](#)。

程序

- 1 從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 > 使用者和角色**。

- 3 若要指派角色給使用者，請選取**新增 > vIDM 的角色指派**。
 - 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 若要為 LDAP 新增角色指派，請選取**新增 > LDAP 的角色指派**。
 - a 選取網域。
 - b 輸入使用者名稱、登入識別碼或群組名稱的前幾個字元，以搜尋 LDAP 目錄，然後從顯示的清單中選取使用者或群組。
 - c 選取角色。
 - d 按一下**儲存**。
- 6 (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。
- 7 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**匯入自我簽署的憑證或 CA 簽署的憑證**。
 - 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"
}
```

同時設定 vIDM 和 LDAP 或從 vIDM 轉換至 LDAP

如果您已將 vIDM 設定為驗證伺服器，您可以新增 LDAP 作為額外的驗證伺服器。您也可以停用 vIDM，並以獨佔方式使用 LDAP。

若要設定 vIDM 整合，請參閱與 [VMware Identity Manager/Workspace ONE Access 整合](#)。若要設定 LDAP 整合，請參閱與 [LDAP 整合](#)。

如果您已設定 vIDM 和 LDAP 整合，則 vIDM 使用者登入頁面的 URL 將是 `https://<nsx-manager-ip-address>`。系統會將使用者重新導向至 vIDM 登入頁面。LDAP 使用者登入頁面的 URL 為 `https://<nsx-manager-ip-address>/login.jsp?local=true`，且登入名稱的格式必須是 `user_name@domain_name`。

如果您僅設定了 LDAP 整合，則 vIDM 使用者登入頁面的 URL 將是 `https://<nsx-manager-ip-address>`，且登入名稱的格式必須是 `user_name@domain_name`。

如果您已設定 vIDM 整合，且想要轉換為僅使用 LDAP，請先設定 LDAP 整合。AD 伺服器必須與 vIDM 中使用的 AD 伺服器相同。然後，在 vIDM 組態頁面上停用 vIDM。在 vIDM 中建立的角色、使用者和角色指派，都將存在於 LDAP 中。

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 - (建立、讀取、更新和刪除)
- 執行 (讀取、更新)
- 讀取
- 無

完整存取權可為使用者提供所有權限。

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

若要檢視內建角色和相關聯的權限，請導覽至**系統 > 使用者和角色 > 角色**。

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 18-1. 角色和權限和表 18-2. 管理程式模式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 18-1. 角色和權限

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
網路 > 第 0 層 閘道	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
網路 > 第 1 層 閘道	FA	R	FA	R	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

表 18-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
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	R	R	R	FA	R	R	R	R	R	R
網路 > 區段 > 區段設定 檔	FA	R	FA	R	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 > DHCP	FA	R	FA	R	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	FA	R	FA	R	R	R	FA	R	R	R	無	無	無
安全性 > 分散式防 火牆	FA	R	R	R	FA	R	FA	R	R	R	R	R	R
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

表 18-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
安全性 > 端點保護規則	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
詳細目錄 > 虛擬機器 > 建立和指派標籤至虛擬機器	FA	R	R	R	FA	R	FA	R	R	R	R	FA	FA
詳細目錄 > 容器	FA	R	R	R	R	R	無	無	無	無	無	無	無
詳細目錄 > 實體伺服器	FA	R	R	R	R	R	R	R	R	R	無	無	無
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 > IPFIX > 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 > IPFIX > 交換器 IPFIX 設定檔	FA	R	FA	R	R	R	FA	R	R	R	R	R	R

表 18-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
系統 > 網狀架構 > 節點 > 主機	FA	R	R	R	R	R	R	R	無	無	無	無	無
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

表 18-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
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
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 Directory	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

表 18-1. 角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
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
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 18-2. 管理程式模式的角色和權限

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
計劃和疑難排解 > 連接埠連線	E	R	E	E	E	E	E	R	E	E	無	無	無
計劃和疑難排解 > Traceflow	E	R	E	E	E	E	E	R	E	E	無	無	無
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 > IPFIX	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
安全性 > 分散式防火牆 > 一般	FA	R	R	R	FA	R	FA	R	無	無	無	無	R
安全性 > 分散式防火牆 > 組態	FA	R	R	R	FA	R	FA	R	無	無	無	無	無
安全性 > Edge 防火牆	FA	R	R	R	FA	R	FA	R	無	無	無	無	FA
網路 > 路由器	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R

表 18-2. 管理程式模式的角色和權限 (續)

作業	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
網路 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	無	無	無
網路 > DHCP > 伺服器設定檔	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
網路 > DHCP > 伺服器	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
網路 > DHCP > 轉送設定檔	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
網路 > DHCP > 轉送服務	FA	R	FA	R	無	無	FA	R	無	無	無	無	無
網路 > DHCP > 中繼資料 Proxy	FA	R	FA	R	無	無	無	無	無	無	無	無	無
網路 > IPAM	FA	R	FA	FA	R	R	無	無	R	R	無	無	無
網路 > 邏輯交換器 > 交換器	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R
網路 > 邏輯交換器 > 連接埠	FA	R	FA	FA	R	R	FA	R	R	R	R	無	R
網路 > 邏輯交換器 > 交換設定檔	FA	R	FA	FA	R	R	FA	R	R	R	無	無	無
網路 > 負載平衡 > 負載平衡器	FA	R	無	無	R	無	FA	R	FA	R	無	無	無
網路 > 負載平衡 > 設定檔 > SSL 設定檔	FA	R	無	無	FA	R	FA	R	FA	R	無	無	無

表 18-2. 管理程式模式的角色和權限 (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 > 群組	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 群組 > IP 集合	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 群組 > IP 集區	FA	R	FA	R	無	無	無	無	R	R	R	R	R
詳細目錄 > 群組 > MAC 集 合	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 服務	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
詳細目錄 > 虛擬機 器	R	R	R	R	R	R	R	R	R	R	R	R	R
詳細目錄 > 虛擬機 器 > 建 立和指派 標籤至虛 擬機器	FA	R	R	R	FA	R	FA	R	R	R	R	FA	FA
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

記錄使用者帳戶變更

對使用者角色指派所做的變更會自動寫入 Syslog 和稽核記錄。

如需 Syslog 和稽核記錄的詳細資訊，請參閱[記錄訊息](#)和[錯誤碼](#)。

將角色指派給 vIDM 使用者時的記錄訊息範例：

```
2020-09-24T16:05:51.244Z nsxmanager-14663974-1-CertKB-FS NSX 5519 - [nsx@6876 audit="true"
comp="nsx-manager" entId="e3c2af75-9d0f-4020-90cc-f2f00d6af255" level="INFO"
reqId="b27711c6-0590-4b39-b8b6-f0980a0597f0" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="AAA", Operation="CreateRoleBinding", Operation
status="success", New
value=[{"name":"test_AU@idfw.local","type":"remote_user","identity_source_type":"VIDM","roles"
:[{"role":"auditor"}],"id":"bba634c9-cfbd-4806-a831-e63ec195e1f9","_protection":"UNKNOWN"}]
```

更新 vIDM 使用者角色時的記錄訊息範例：

```
2020-09-24T16:12:51.217Z nsxmanager-14663974-1-CertKB-FS NSX 5519 - [nsx@6876 audit="true"
comp="nsx-manager" entId="e3c2af75-9d0f-4020-90cc-f2f00d6af255" level="INFO" reqId="973faed4-
f4b5-443d-bd79-7d995c027183" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="AAA", Operation="UpdateRoleBinding", Operation
status="success", New value=["e3c2af75-9d0f-4020-90cc-f2f00d6af255"
{"name":"test_AU@idfw.local","type":"remote_user","identity_source_type":"VIDM","roles":
[{"role":"security_engineer"}],"_protection":"UNKNOWN"}]
```

將角色指派給 LDAP 使用者時的記錄訊息範例：

```
2020-09-24T16:06:28.663Z nsxmanager-14663974-1-CertKB-FS NSX 5519 - [nsx@6876 audit="true"
comp="nsx-manager" entId="35e45569-6da6-4dcd-b4a1-75747cdd6cf8" level="INFO"
reqId="db27f4ae-25a7-4482-b3f4-49228d12960b" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="AAA", Operation="CreateRoleBinding", Operation
status="success", New
value=[{"name":"skrasner@airius.com","type":"remote_user","identity_source_type":"LDAP","ident
ity_source_id":"ldap","roles":[{"role":"auditor"}],"id":"dd8d3675-
c574-454b-975e-300b65462827","_protection":"UNKNOWN"}]
```

更新 LDAP 使用者角色時的記錄訊息範例：

```
2020-09-24T16:12:37.449Z nsxmanager-14663974-1-CertKB-FS NSX 5519 - [nsx@6876 audit="true"
comp="nsx-manager" entId="35e45569-6da6-4dcd-b4a1-75747cdd6cf8" level="INFO"
reqId="d7cdd3de-75a1-4d29-9fea-27e1dda4b5e2" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="AAA", Operation="UpdateRoleBinding", Operation
status="success", New value=["35e45569-6da6-4dcd-b4a1-75747cdd6cf8"
{"name":"skrasner@airius.com","type":"remote_user","identity_source_type":"LDAP","identity_sou
rce_id":"ldap","roles":[{"role":"network_engineer"}],"_protection":"UNKNOWN"}]
```

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。

如果您使用的是聯盟，則系統會設定其他憑證，以在本機管理程式與全域管理程式之間建立信任。

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)。為提高安全性，建議您將自我簽署的憑證取代為 CA 簽署的憑證。

本章節討論下列主題：

- [憑證類型](#)
- [NSX 聯盟的憑證](#)
- [建立憑證簽署要求檔案](#)
- [建立自我簽署憑證](#)
- [匯入並取代憑證](#)
- [匯入和擷取 CRL](#)
- [用於負載平衡器或 VPN 服務的公用憑證和私密金鑰的儲存區](#)
- [憑證到期的警示通知](#)

憑證類型

NSX-T Data Center 中有三種自我簽署憑證類別。

- [平台憑證](#)
- [NSX Services 憑證](#)
- [主體身分識別憑證](#)

如需每個憑證類別的詳細資料，請參閱下列章節。

平台憑證

安裝 NSX-T Data Center 後，導覽至**系統 > 憑證**，以檢視系統所建立的平台憑證。依預設，這些是自我簽署的 X.509 RSA 2048/SHA256 憑證，用於在 NSX-T Data Center 內進行內部通訊，以及在使用 API 或 UI 存取 NSX Manager 時進行外部驗證。

內部憑證無法檢視或編輯。

表 19-1. NSX-T Data Center 中的平台憑證

NSX Manager 中的命名慣例	用途	可更換？	預設有效性
tomcat	這是一種 API 憑證，用於透過 UI/API 與個別 NSX Manager 節點進行外部通訊。	是。 請參閱 取代憑證	825 天
mp-cluster	這是一種 API 憑證，用於透過 UI/API 與使用叢集 VIP 的 NSX Manager 叢集進行外部通訊。	是。 請參閱 取代憑證	825 天
其他憑證	專用於 NSX 聯盟的憑證。如果您未使用 NSX 聯盟，則不會使用這些憑證。	請參閱 NSX 聯盟的憑證 ，以進一步瞭解為 NSX 聯盟自動設定的自我簽署憑證。	
在 UI 中不可見	用於不同系統元件之間內部通訊的憑證。	否	10 年

NSX Service 憑證

NSX Service 憑證用於負載平衡器和 VPN 等服務。

NSX Service 憑證無法自我簽署。您必須匯入這些憑證。如需指示，請參閱[匯入並取代憑證](#)。

如果憑證簽署要求 (CSR) 是由 CA (本機 CA 或公用 CA，例如 Verisign) 所簽署，則它可作為 NSX Service 憑證。CSR 簽署後，您可以將該簽署的憑證匯入 NSX Manager。CSR 可在 NSX Manager 或 NSX Manager 外部來產生。請注意，NSX Manager 上所產生的 CSR 已停用**服務憑證**旗標。因此，這些已簽署的 CSR 無法用作服務憑證，而只能用作平台憑證。

平台和 NSX Service 憑證會個別儲存在系統內，且匯入為 NSX Service 憑證的憑證無法用於平台或反向。

主體身分識別 (PI) 憑證

PI 憑證可用於服務或平台。

雲端管理平台 (CMP) 的 PI (例如 Openstack) 會使用將 CMP 上線為用戶端時所上傳的 X.509 憑證。如需將角色指派給主體身分識別以及取代 PI 憑證的相關資訊，請參閱[新增角色指派或主體身分識別](#)

NSX 聯盟的 PI 會將 X.509 平台憑證用於本機管理程式和全域管理程式應用裝置。請參閱 [NSX 聯盟的憑證](#)，以進一步瞭解為 NSX 聯盟自動設定的自我簽署憑證。

NSX 聯盟的憑證

系統會建立在 NSX 聯盟應用裝置之間通訊以及外部通訊所需的憑證。

依預設，全域管理程式會使用自我簽署憑證與內部元件和已登錄的本機管理程式進行通訊，以及 NSX Manager UI 或 API 的驗證。

您可以在 NSX Manager 中檢視外部 (UI/API) 和站台間憑證。內部憑證無法檢視或編輯。

全域管理程式和本機管理程式的憑證

將本機管理程式新增至全域管理程式後，所有驗證本機管理程式以進行外部和內部通訊的憑證都會複製到全域管理程式，並在兩個系統之間建立信任。這些憑證也會複製到每個已向全域管理程式登錄的站台。

請參閱下表，以取得針對每個應用裝置使用 NSX 聯盟建立的所有憑證清單，以及這些應用裝置彼此交換的憑證：

表 19-2. 全域管理程式和本機管理程式的憑證

全域管理程式或本機管理程式中的命名慣例	用途	可更換？	預設有效性
下列是每個 NSX 聯盟應用裝置專屬的憑證。			
APH-AR certificate	<ul style="list-style-type: none"> ■ 適用於全域管理程式和每個本機管理程式。 ■ 用於使用 AR 通道 (非同步複製器通道) 的站台間通訊。 	否	10 年
GlobalManager	<ul style="list-style-type: none"> ■ 適用於全域管理程式。 ■ 全域管理程式的 PI 憑證。 	是。請參閱 取代憑證 。	825 天
mp-cluster certificate	<ul style="list-style-type: none"> ■ 適用於全域管理程式和每個本機管理程式。 ■ 用於與全域管理程式或本機管理程式叢集的 VIP 進行 UI/API 通訊。 		
tomcat certificate	<ul style="list-style-type: none"> ■ 適用於全域管理程式和每個本機管理程式。 ■ 用於與個別全域管理程式以及新增至全域管理程式每個位置的本機管理程式節點進行 UI/API 通訊。 		
LocalManager	<ul style="list-style-type: none"> ■ 適用於本機管理程式。 ■ 此特定本機管理程式的 PI 憑證。 		
以下是在 NSX 聯盟應用裝置之間交換的憑證。			
全域管理程式或本機管理程式中的命名慣例	用途	可更換？	預設有效性
雜湊代碼，例如 1729f966-67b7-4c17- bdf5-325affb79f4f	<ul style="list-style-type: none"> ■ 在已向全域管理程式登錄的所有本機管理程式之間交換。 ■ 與本機管理程式交換的全域管理程式 PI 憑證。 ■ 與所有已登錄位置管理程式交換之每個位置的 PI 憑證。 	不適用	
Site certificate CN=<>,O	<ul style="list-style-type: none"> ■ 在所有 NSX 聯盟應用裝置之間交換：所有已登錄的本機管理程式和全域管理程式。 ■ 所有類型的憑證。 		

NSX 聯盟的主體身分識別 (PI) 使用者

在您將本機管理程式新增至全域管理程式後，系統會建立下列具有對應角色的 PI 使用者：

表 19-3. 已針對 NSX 聯盟建立的主體身分識別 (PI) 使用者

NSX 聯盟 應用裝置	PI 使用者名稱	PI 使用者角色
全域管理程式	LocalManagerIdentity 每個向此全域管理程式登錄的本機管理程式各一個。	稽核員
本機管理程式	GlobalManagerIdentity	企業管理員
	LocalManagerIdentity 每個向相同全域管理程式登錄的本機管理程式各一個。使用下列 API 取得所有本機管理程式 PI 使用者的清單，因為這些使用者在 UI 中不可見： <pre>GET https://<local-mgr>/api/v1/trust-management/principal-identities</pre>	稽核員

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。

程序

- 1 從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。

選項	說明
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。
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。其他支援的大小為 3072 和 4096。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，然後按一下動作以選取下列其中一個選項：

- 自我簽署憑證
- 匯入 CSR 的憑證
- 下載 PEM

如果您選取了**下載 CSR PEM**，您可以儲存 CSR PEM 檔案，以用於記錄和 CA 提交。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。對於其他兩個選項，請參閱必要的主題。

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。

建立自我簽署憑證

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。
預設為 825 天。即使您針對先前產生的自我簽署憑證變更此值，每次產生新憑證時仍會顯示預設值。
- 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。

匯入 CSR 的憑證

您可以匯入 NSX-T Data Center 產生的 CSR 的簽署憑證。此頁面提供步驟來匯入 NSX 產生的 CSR 的簽署憑證。

自我簽署憑證可作為憑證以及 CA。不需要從任何外部 CA 來簽署，其中 CSR 是無法用作 CA 且必須由外部 CA 簽署的憑證簽署要求。請注意，自我簽署憑證不支援用於 LB。

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](#)。
- NSX-T Data Center 產生的 CSR 已用作簽署憑證的 CSR。

程序

- 1 從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。

匯入並取代憑證

您可以為平台或服務匯入自我簽署或 CA 簽署的憑證。您可以使用 API 取代部分自我簽署的憑證。

您也可以為服務 (例如負載平衡器) 匯入 CA 憑證。

匯入自我簽署的憑證或 CA 簽署的憑證

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。

您可以使用此程序為平台或服務匯入自我簽署或 CA 簽署的憑證。請注意，在 NSX Manager 上產生的自我簽署 CSR 無法用作服務憑證，例如負載平衡器服務。如果您想要針對負載平衡器服務匯入 CA 憑證，請參閱[匯入 CA 憑證](#)。

必要條件

- 確認可以使用憑證。
- 伺服器憑證必須包含基本限制延伸 `basicConstraints = cA:FALSE`。

程序

- 1 從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。如果匯入的憑證是以 NSX Manager 產生的 CSR 為基礎，則這是選用欄位，因為 NSX Manager 應用裝置上已有私密金鑰存在。
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**。

匯入 CA 憑證

您可以將 CA 憑證從系統外部匯入 NSX-T Data Center 中，例如，搭配負載平衡器服務使用。

如果您想要匯入自我簽署的憑證或 CA 簽署的憑證，請參閱[匯入自我簽署的憑證或 CA 簽署的憑證](#)中的指示。

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。

- 4 按一下**匯入**。

設定憑證匯入檢查

您可以啟用或停用 NSX-T Data Center 在匯入憑證時執行的擴充金鑰使用方法 (EKU) 擴充功能和憑證撤銷清單發佈點 (CDP) 驗證檢查。

附註：如果您具有不含 CDP 的 CA 簽署憑證，則升級後可能會出現問題。若要避免出現此問題，您可以關閉 CRL 檢查或將憑證取代為包含 CDP 的憑證。

若要設定驗證檢查，將下列 API 與裝載搭配使用。如需有關 API 的詳細資訊，請參閱《NSX-T Data Center API 指南》。

```
PUT https://<manager>/api/v1/global-configs/SecurityGlobalConfig
{
  "crl_checking_enabled": false,
  "ca_signed_only": false,
  "eku_checking_enabled": false,
  "resource_type": "SecurityGlobalConfig"
}
```

其中：

- `crl_checking_enabled`：依預設啟用以檢查在匯入的 CA 簽署憑證中指定的 CDP。僅支援包括 HTTP 型 CRL-DP。不支援檔案或 LDAP 型選項。
- `ca_signed_only`：依預設為停用。僅允許由 CA 簽署的檢查。
- `eku_checking_enabled`：依預設為停用。它會在已匯入的憑證中檢查是否有 EKU 擴充功能。
- `revision`：必須包含在要求中之資源的目前修訂版本。若要取得此參數的值，請執行 GET 作業。

取代憑證

您可以發出 API 呼叫，取代理管理程式節點的憑證或管理程式叢集虛擬 IP (VIP)。

安裝 NSX-T Data Center 之後，管理程式節點和叢集會具有自我簽署的憑證。建議您使用 CA 簽署的憑證取代自我簽署憑證，並使用單一通用的 CA 簽署憑證搭配符合所有節點和叢集 VIP 的 SAN (主體替代名稱) 清單。如需系統所設定預設自我簽署憑證的詳細資料，請參閱 [憑證類型](#)。

如果您使用的是聯盟，則可以使用下列 API 取代全域管理程式節點、全域管理程式叢集、本機管理程式節點和本機管理程式叢集憑證。您也可以取代針對全域管理程式和本機管理程式應用裝置自動建立的平台主體身分識別憑證。請參閱 [NSX 聯盟的憑證](#) 以取得自動設定聯盟的自我簽署憑證詳細資料。

必要條件

- 確認 NSX Manager 中可以使用憑證。請參閱 [匯入自我簽署的憑證或 CA 簽署的憑證](#)。
- 伺服器憑證必須包含基本限制延伸 `basicConstraints = cA:FALSE`。
- 透過進行下列 API 呼叫，確認憑證有效：

```
GET https://<nsx-mgr>/api/v1/trust-management/certificates/<certificate-id>?
action=validate
```

程序

- 1 從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 若要取代理管理程式節點的憑證，請使用 `POST /api/v1/node/services/http?action=apply_certificate` API 呼叫。例如，

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

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。

- 6 (選擇性) 若要取代聯盟的主體身分識別憑證，請使用 API 呼叫：POST `https://<nsx-mgr>/api/v1/trust-management/certificates?action=set_pi_certificate_for_federation`。例如：

```
POST https://<nsx-mgr>/api/v1/trust-management/certificates?
action=set_pi_certificate_for_federation
{ "cert_id": "<id>",
  "service_type": "LOCAL_MANAGER" }
```

- 7 (選擇性) 如果您的 NSX Manager 叢集目前已部署 NSX Intelligence 應用裝置，則必須更新 NSX Intelligence 應用裝置上的 NSX Manager 節點 IP、憑證和指紋資訊。如需詳細資訊，請參閱 VMware 知識庫文章 <https://kb.vmware.com/s/article/78505>。

匯入和擷取 CRL

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----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMMAoGA1 UECBMD UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQwMQswCQYDVQLEwJDUz EbmBkG A1UEAxMSU1NMZWZ5IGRlbnw8gc2VydMvYFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwEgIBARcNOTUxMDA5MjMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA 0GCSqG S1B3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFYo/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》。

用於負載平衡器或 VPN 服務的公用憑證和私密金鑰的儲存區

公用憑證和私密金鑰會儲存在用於負載平衡器或 VPN 服務的 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。

憑證到期的警示通知

當憑證即將到期或憑證已到期時，NSX-T Data Center 會產生警示。

NSX-T Data Center 會在下列事件下產生警示：

- 中度嚴重性警示會在憑證到期的 30 天前啟動。
- 高度嚴重性警示會在到期的 7 天前啟動。
- 重大嚴重性警示會在憑證到期後每天啟動。

憑證到期警示包含有關憑證識別碼、嚴重性、節點、第一次/上次報告時間以及建議動作的詳細資料。

作為補救措施，您必須將即將到期的外部平台憑證取代為新的有效憑證，並刪除即將到期的憑證。

在管理程式模式中設定 NSX-T Data Center

20

NSX-T Data Center 具有兩種使用者介面模式：原則模式和管理程式模式。如果您有在管理程式模式中建立的物件，應繼續使用管理程式模式進行變更。

如需關於兩個模式的詳細資訊，請參閱第 1 章 NSX Manager。


如果看不到**原則**和**管理程式**模式按鈕，請參閱設定使用者介面設定。

本章節討論下列主題：

- 管理程式模式中的邏輯交換器
- 管理程式模式中的邏輯路由器
- 管理程式模式中的 NAT
- 在管理程式模式中群組物件
- 管理程式模式中的 DHCP
- 管理程式模式中的 IP 位址管理
- 管理程式模式中的負載平衡
- 管理程式模式中的防火牆

管理程式模式中的邏輯交換器

您可以在**管理程式**模式中設定邏輯交換器和相關物件。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。

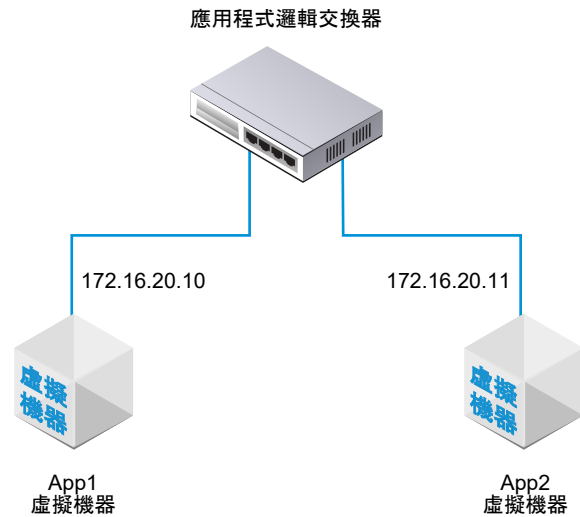
備註 如果您使用**管理程式**模式來修改在**原則**模式中建立的物件，則可能無法進行某些設定。這些唯讀設定的旁邊會顯示此圖示：。如需詳細資訊，請參閱第 1 章 NSX Manager。

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 20-1. 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。

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。

在管理程式模式中建立邏輯交換器

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[管理程式模式中的邏輯交換器與瞭解 BUM 框架複寫模式](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 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[在管理程式模式中將虛擬機器連線到邏輯交換器](#)。

在管理程式模式中將虛擬機器連線到邏輯交換器

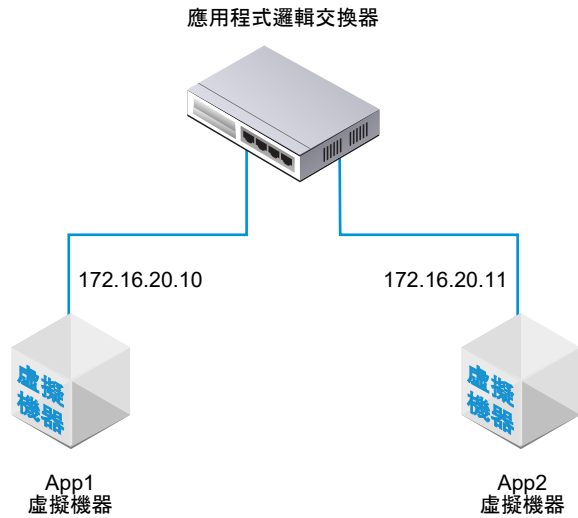
視主機而定，用來將虛擬機器連線到邏輯交換器的組態可能會有所不同。

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。

在管理程式模式中將在 vCenter Server 上主控的虛擬機器連結至邏輯交換器

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，請參閱在管理程式模式中將在獨立 ESXi 上主控的虛擬機器連結至邏輯交換器。

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 UI 上檢視邏輯交換器連接埠和 VIF 連結識別碼。在**管理程式模式**中，選取**網路 > 邏輯交換器 > 連接埠**。

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〉。

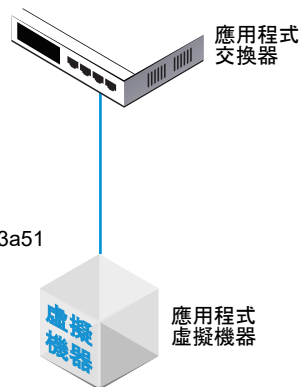
在管理程式模式中將在獨立 ESXi 上主控的虛擬機器連結至邏輯交換器

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

The screenshot shows the 'Virtual Hardware' configuration window. The 'New Network' section is highlighted, showing the following settings:

- 新增網路: VM Network
- 狀態: 開啟電源時連線
- 介面卡類型: VMXNET 3
- DirectPath I/O: 啟用
- MAC 位址: [Empty] 自動

At the bottom, there is a 'New Device' section with a dropdown menu set to 'Network' and a 'New' button.

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

在結果中尋找虛擬機器的 externalId。

例如：

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

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fef7-08c5-5bf7-ea26a4c6b18d"
  ],
}
```



```

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

```

3 關閉虛擬機器的電源並從主機解除登錄虛擬機器。

您可以使用虛擬機器管理工具或 ESXi CLI，如此處所示。

```

[user@host:~] vim-cmd /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：

```

OLD
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"

```

```

ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"

```

NEW

```

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

```

- 6 在 NSX Manager UI 中，新增邏輯交換器連接埠，並使用虛擬機器的 externalId 來連結 VIF。
- 7 重新登錄虛擬機器並開啟其電源。

您可以使用虛擬機器管理工具或 ESXi CLI，如此處所示。

```

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

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

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

```

結果

在 NSX Manager UI 的**管理程式**模式中，選取**網路 > 邏輯交換器 > 連接埠**。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

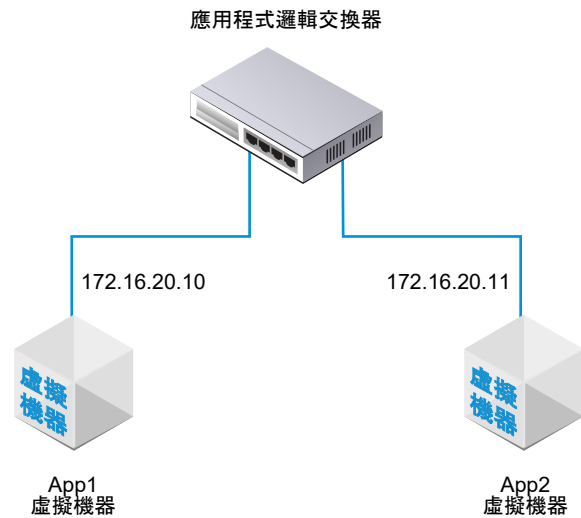
新增邏輯路由器。

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**〉。

在管理程式模式中將 KVM 上主控的虛擬機器連結至邏輯交換器

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 UI 的**管理程式**模式中，選取**網路 > 邏輯交換器 > 連接埠**。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〉。

在管理程式模式中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[在管理程式模式中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 Plugin - 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[在管理程式模式中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[管理程式模式中的邏輯交換器](#)。
- 確認已在 NSX Manager 使用者介面中選取[管理程式模式](#)。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和管理程式模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取 [網路](#) > [邏輯交換器](#) > [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 。如果這是用來連線至虛擬機器的連接埠，請選取 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。

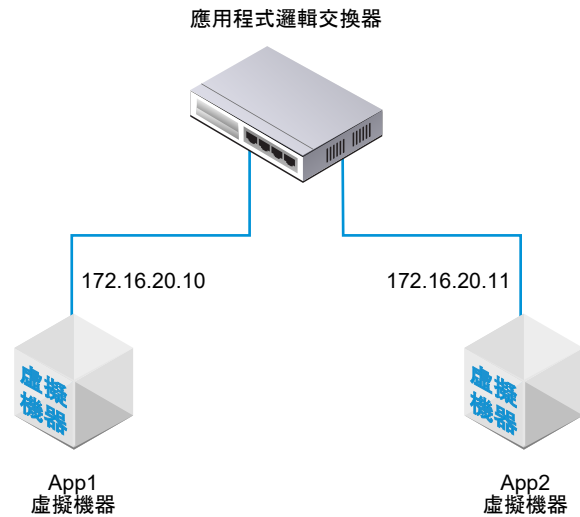
- 4 (選擇性) 在 [交換設定檔](#) 索引標籤中，選取交換設定檔。
- 5 按一下 [儲存](#)。

在管理程式模式中測試第 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 20-2. 邏輯交換器拓撲



必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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**網路 > 邏輯交換器 > 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。 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>

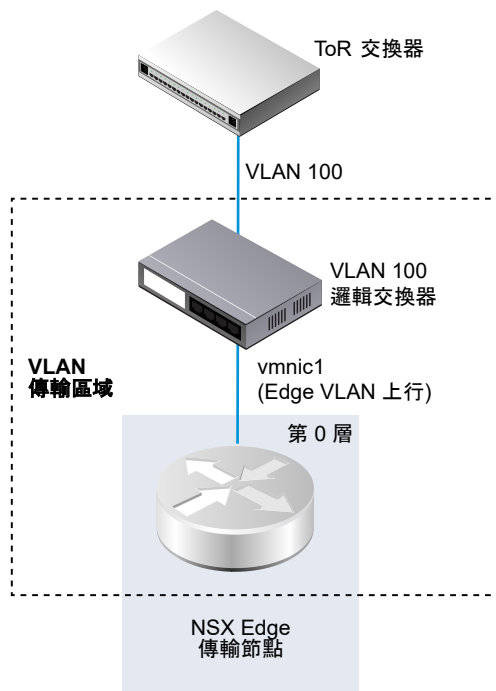
結果

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。

在管理程式模式中為 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》。

- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱**設定使用者介面設定**。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**網路 > 邏輯交換器 > 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。

在管理程式模式中設定自訂 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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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

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。請參閱在管理程式模式中建立自訂設定檔與邏輯交換器之間的關聯或在管理程式模式中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。

在管理程式模式中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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 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。
金鑰	輸入隨機 32 位元值以識別來自邏輯連接埠的鏡像封包。 此「金鑰」值會複製到每個鏡像封包之 GRE 標頭中的 [金鑰] 欄位。如果「金鑰」值設定為 0，則預設定義會複製到 GRE 標頭中的 [金鑰] 欄位。 預設 32 位元值是由下列值所組成。 <ul style="list-style-type: none"> ■ 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	輸入鏡像工作階段的收集器目的地識別碼。 目的地 IP 位址識別碼僅能為網路內的 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。

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[在管理程式模式中建立自訂設定檔與邏輯交換器之間的關聯](#)或在[在管理程式模式中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[在管理程式模式中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[在管理程式模式中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[在管理程式模式中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 窺探會在名稱為「首次使用時信任 (TOFU)」的模式下運作。在 TOFU 模式中，在探索到位址並將其新增至實現的繫結清單時，該繫結會永久保留在實現的清單中。TOFU 會套用至使用 ARP/ND 窺探探索到前「n」個唯一的 <IP、MAC、VLAN> 繫結，其中「n」是您可以設定的繫結限制。您可以針對 ARP/ND 窺探停用 TOFU。隨後，這些方法將會在「每次使用皆信任 (TOEU)」模式中運作。在 TOEU 模式中，在探索到某個位址時，系統即會將其新增至實現的繫結清單中，並在該位址刪除或到期後，將其從實現的繫結清單中移除。DHCP 窺探和 VM Tools 一律會在 TOEU 模式中運作。

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。如果您在**管理程式**模式中導覽至**網路 > 邏輯交換器 > 連接埠**，然後選取連接埠，則可以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>。

在管理程式模式中設定 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**。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱**第 1 章 NSX Manager**。如果看不到**原則和管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 邏輯交換器 > 交換設定檔 > 新增**。
- 3 選取**IP 探索**，然後指定 IP 探索交換設定檔詳細資料。

選項	說明
名稱與說明	輸入名稱和 (選用) 說明。
ARP 窺探	適用於 IPv4 環境。適用於具有靜態 IP 位址的虛擬機器。
ARP 繫結限制	可繫結至連接埠的 IPv4 IP 位址數目上限。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 窺探	適用於 IPv4 環境。適用於具有 IPv4 位址的虛擬機器。
DHCP V6 窺探	適用於 IPv6 環境。適用於具有 IPv6 位址的虛擬機器。
VM Tools	僅適用於裝載 ESXi 的虛擬機器。
IPv6 的 VM Tools	僅適用於裝載 ESXi 的虛擬機器。
芳鄰探索窺探	適用於 IPv6 環境。適用於具有靜態 IP 位址的虛擬機器。
芳鄰探索繫結限制	可繫結至連接埠的 IPv6 位址數目上限。
首次使用時信任	適用於 ARP 和 ND 窺探。
重複的 IP 偵測	適用於所有窺探方法及 IPv4 和 IPv6 環境。

- 4 按一下**新增**。

後續步驟

將此 IP 探索自訂交換設定檔連結至邏輯交換器或邏輯連接埠，讓交換設定檔中已修改的參數可套用至網路流量。請參閱在管理程式模式中建立自訂設定檔與邏輯交換器之間的關聯或在管理程式模式中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 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 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。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 在 NSX Manager 中，選取**網路 > 邏輯交換器 > 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

當您在**管理程式**模式中設定 [SpoofGuard 交換設定檔](#)時使用連接埠位址繫結。

在管理程式模式中設定 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 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。請參閱在管理程式模式中建立自訂設定檔與邏輯交換器之間的關聯或在管理程式模式中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。

在管理程式模式中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。
- 確認已在 NSX Manager 使用者介面中選取管理程式模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取 **網路 > 邏輯交換器**。
- 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。

選項	說明
DHCP 篩選器	<p>切換伺服器封鎖按鈕及用戶端封鎖按鈕以啟用 DHCP 篩選。依預設會停用這兩者。</p> <p>「DHCP 伺服器封鎖」會封鎖 DHCP 伺服器至 DHCP 用戶端的流量。請注意，它不會封鎖 DHCP 伺服器至 DHCP 轉送代理程式的流量。</p> <p>「DHCP 用戶端封鎖」會封鎖 DHCP 要求，以防止虛擬機器取得 DHCP IP 位址。</p>
DHCPv6 篩選器	<p>切換V6 伺服器封鎖按鈕及V6 用戶端封鎖按鈕以啟用 DHCP 篩選。依預設會停用這兩者。</p> <p>「DHCPv6 伺服器封鎖」會封鎖 DHCPv6 伺服器至 DHCPv6 用戶端的流量。請注意，它不會封鎖 DHCP 伺服器至 DHCP 轉送代理程式的流量。將會篩選 UDP 來源連接埠號碼為 547 的封包。</p> <p>「DHCPv6 用戶端封鎖」會封鎖 DHCP 要求，以防止虛擬機器取得 DHCP IP 位址。將會篩選 UDP 來源連接埠號碼為 546 的封包。</p>
封鎖非 IP 流量	<p>切換封鎖非 IP 流量按鈕以僅允許 IPv4、IPv6、ARP 和 BPDU 流量。</p> <p>系統會封鎖剩餘的非 IP 流量。允許的 IPv4、IPv6、ARP、GARP 和 BPDU 流量是根據位址繫結及 SpoofGuard 組態中所設定的其他原則而定。</p> <p>依預設，系統會停用此選項以允許非 IP 流量以一般流量方式處理。</p>
RA 保護	<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>

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。請參閱在管理程式模式中建立自訂設定檔與邏輯交換器之間的關聯或在管理程式模式中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。在預設 MAC 管理交換設定檔中，此內容預設為啟用。

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

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。

在管理程式模式中設定 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](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和管理程式模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取 **網路 > 邏輯交換器 > 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。請參閱在**管理程式模式**中建立自訂設定檔與邏輯交換器之間的關聯或在**管理程式模式**中建立自訂設定檔與邏輯連接埠之間的關聯。

在管理程式模式中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[在管理程式模式中建立邏輯交換器](#)。
- 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](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 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[在管理程式模式中建立自訂設定檔與邏輯連接埠之間的關聯](#)。

在管理程式模式中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[在管理程式模式中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](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 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[在管理程式模式中監控邏輯交換器連接埠活動](#)。

管理程式模式中的第 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。

在管理程式模式中建立 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。
- 確認您處於管理程式模式。

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 > 邏輯交換器 > Edge 橋接器設定檔 > 新增**。
- 3 輸入 Edge 橋接器設定檔的名稱，並選擇性地輸入說明。
- 4 選取 NSX Edge 叢集。
- 5 選取主要節點。
- 6 選取備份節點。
- 7 選取容錯移轉模式。
選項為先佔式和非先佔式。
- 8 按一下 **新增** 按鈕。

後續步驟

設定以 Edge 為基礎的橋接。請參閱 [設定以 Edge 為基礎的橋接](#)。

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。
- 作用中和待命 Edge 虛擬機器應位於不同主機。如果它們位於同一主機，輸送量可能會降低，因為在混合模式中必須將 VLAN 流量同時轉送至這兩個虛擬機器。

選項 2：設定 MAC 學習

如果 Edge 部署在已安裝 NSX-T 的主機上，則可以連線至 VLAN 邏輯交換器或區段。邏輯交換器必須具有已啟用 MAC 學習的 MAC 管理設定檔。同樣地，區段必須具有已啟用 MAC 學習的 MAC 探索設定檔。

選項 3：設定接收連接埠

- 1 針對您要設定為接收連接埠的主幹 vNIC，擷取連接埠號碼。
 - a 登入 vSphere Web Client，然後導覽至首頁 > 網路。
 - b 按一下 NSX Edge 主幹介面所連線的分散式連接埠群組，然後按一下**連接埠**以檢視連接埠和已連線的虛擬機器。記下與主幹介面相關聯的連接埠號碼。在擷取和更新不透明資料時，請使用此連接埠號碼。
- 2 擷取 vSphere Distributed Switch 的 dvsUuid 值。
 - a 在 `https://<vc-ip>/mob` 上登入 vCenter Mob UI。
 - b 按一下**內容**。
 - c 按一下與 `rootFolder` 相關聯的連結 (例如：`group-d1 (Datacenters)`)。

- d 按一下與 **childEntity** 相關聯的連結 (例如：*datacenter-1*)。
 - e 按一下與 **networkFolder** 相關聯的連結 (例如：*group-n6*)。
 - f 按一下與 NSX Edge 相關聯之 vSphere Distributed Switch 的 DVS 名稱連結 (例如：*dvs-1 (Mgmt_VDS)*)。
 - g 複製 UUID 字串的值。在擷取和更新不透明資料時，請使用此 `dvsUuid` 值。
- 3 確認用來指定連接埠的不透明資料是否存在。

- a 移至 `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`。
- b 按一下 **fetchOpaqueDataEx**。
- c 在 **selectionSet** 值方塊中，貼上下列 XML 輸入：

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

使用您為 NSX Edge 主幹介面擷取的連接埠號碼和 `dvsUuid` 值。

- d 將 `isRuntime` 設為 `false`。
 - e 按一下**叫用方法**。如果結果顯示 `vim.dvs.OpaqueData.ConfigInfo` 的值，則表示已有不透明的資料集，而在設定接收連接埠時請使用 `edit` 作業。如果 `vim.dvs.OpaqueData.ConfigInfo` 的值為空白，則在設定接收連接埠時請使用 `add` 作業。
- 4 在 vCenter 受管理物件瀏覽器 (MOB) 中設定接收連接埠。

- a 移至 `https://<vc-ip>/mob/?moid=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="vmodl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```


- NSX-T Data Center 部署外部的虛擬機器或其他終端裝置。此終端裝置必須連結至 VLAN 連接埠，且符合支援橋接器之邏輯交換器的 VLAN 識別碼。
- 覆疊傳輸區域中的一個邏輯交換器會用作橋接器備份邏輯交換器。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式**模式按鈕，請參閱**設定使用者介面設定**。

程序

- 1 從瀏覽器登入 NSX Manager，網址為 `https://<nsx-mgr>`。
- 2 選取**網路 > 邏輯交換器**。
- 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"
}

```

管理程式模式中的邏輯路由器

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。

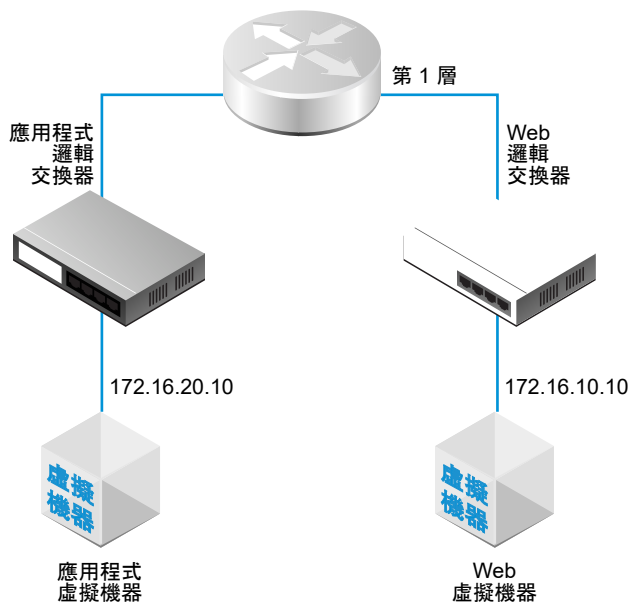
備註 如果您使用管理程式模式來修改在原則模式中建立的物件，則可能無法進行某些設定。這些唯讀設定的旁邊會顯示此圖示：⊖。如需詳細資訊，請參閱第 1 章 NSX Manager。

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 20-3. 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)

在管理程式模式中建立第 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[在管理程式模式中建立邏輯交換器](#)。
- 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](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 1 層邏輯路由器 > 新增**。
- 3 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。

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。請參閱在管理程式模式中的第 1 層邏輯路由器上新增下行連接埠。

在管理程式模式中的第 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[在管理程式模式中建立第 1 層邏輯路由器](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 1 層邏輯路由器**。
- 3 按一下第 1 層路由器的名稱。
- 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 輸入路由器連接埠的 IP 位址和首碼長度。
- 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[在管理程式模式中的第 1 層邏輯路由器上設定路由通告](#)。

在管理程式模式中的第 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

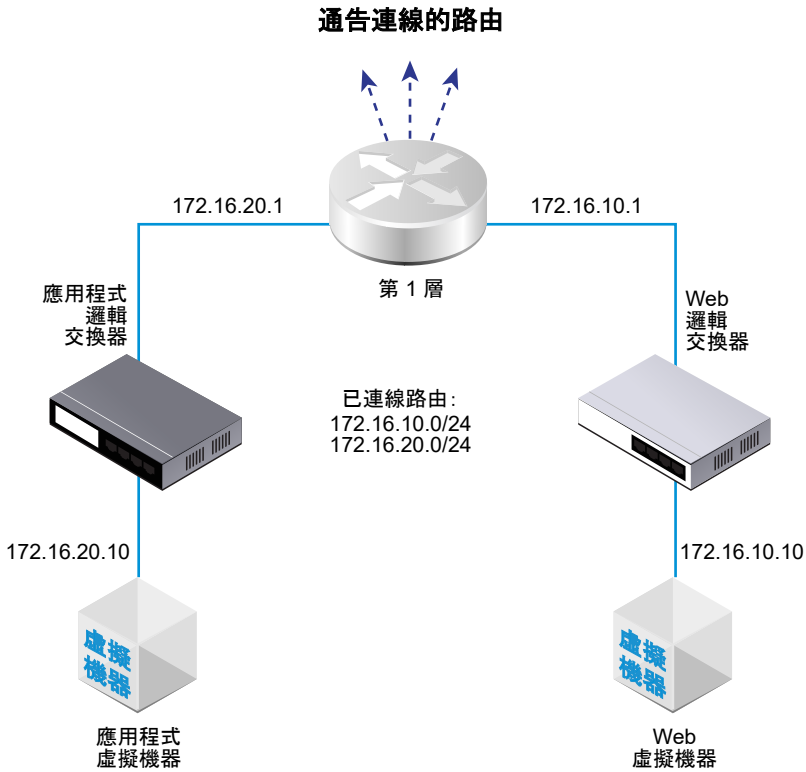
程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 在**網路 > 第 0 層邏輯路由器**或**網路 > 第 1 層邏輯路由器**找到路由器，並加以選取。
- 3 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 4 按一下**新增**。
- 5 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 6 在**類型**欄位中，選取**集中式**。
- 7 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。
- 8 (必要) 選取邏輯交換器。
- 9 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。
- 10 以 CIDR 標記法輸入路由器連接埠 IP 位址。
- 11 按一下**新增**。

在管理程式模式中的第 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[管理程式模式中的邏輯交換器](#)。
- 確認已設定第 1 層邏輯路由器的下行連接埠。請參閱在[管理程式模式中的第 1 層邏輯路由器上新增下行連接埠](#)。
- 確認已在 NSX Manager 使用者介面中選取[管理程式模式](#)。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和管理程式模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取 **網路 > 第 1 層邏輯路由器**。
- 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 (大於或等於) 或 EQ (等於)。

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](#)。

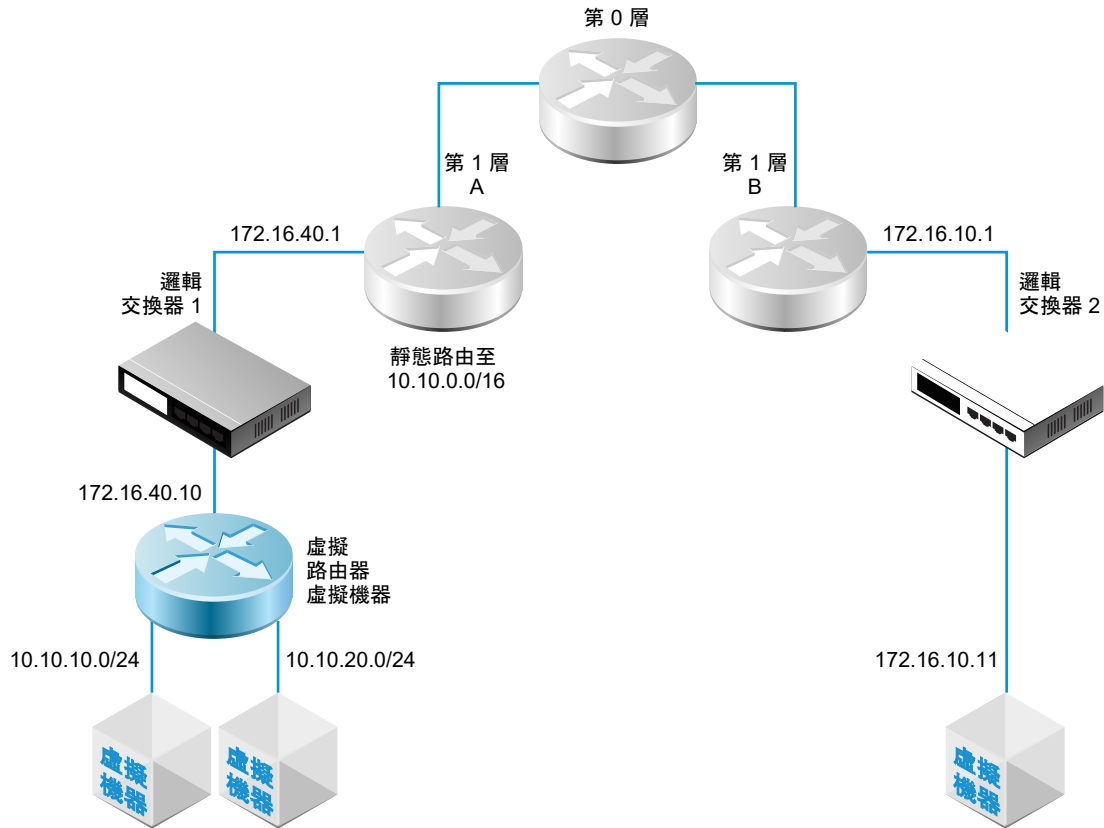
如果您已經有連線至第 1 層邏輯路由器的第 0 層邏輯路由器，則可以確認第 0 層路由器學習連線第 1 層路由器的路由。請參閱[確認第 0 層路由器已從第 1 層路由器學習路由](#)。

在管理程式模式中設定第 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 20-4. 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。請參閱在管理程式模式中的第 1 層邏輯路由器上新增下行連接埠。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱設定使用者介面設定。

確認已設定下行連接埠。請參閱在管理程式模式中的第 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**網路 > 第 1 層邏輯路由器**。
- 3 按一下第 1 層路由器的名稱。
- 4 按一下**路由索引**標籤，然後從下拉式功能表中選取**靜態路由**。
- 5 按一下**新增**。
- 6 以 CIDR 格式輸入網路位址。

支援以 IPv6 為基礎的靜態路由。IPv6 首碼只能有 IPv6 下一個躍點。

例如，10.10.10.0/16 或 IPv6 位址。

- 7 按一下**新增**以新增下一個躍點 IP 位址。

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

- 8 按一下對話方塊底部的**新增**。

新建立的靜態路由網路位址即會顯示在該列中。

- 9 從第 1 層邏輯路由器中，選取**路由 > 路由通告**。

- 10 按一下**編輯**，然後選取**通告所有靜態路由**。

- 11 按一下**儲存**。

靜態路由便會跨越 NSX-T Data Center 覆疊進行傳播。

在管理程式模式中建立獨立的第 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。在作用中/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。
- 如果用來連結負載平衡器 (LB) 服務，則只能有一個集中式服務連接埠 (CSP)。
- 可以連線至覆疊邏輯交換器或 VLAN 邏輯交換器。
- 支援 IPSec、NAT、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 - SNAT - 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取 **網路 > 第 1 層邏輯路由器 > 新增**。
- 3 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

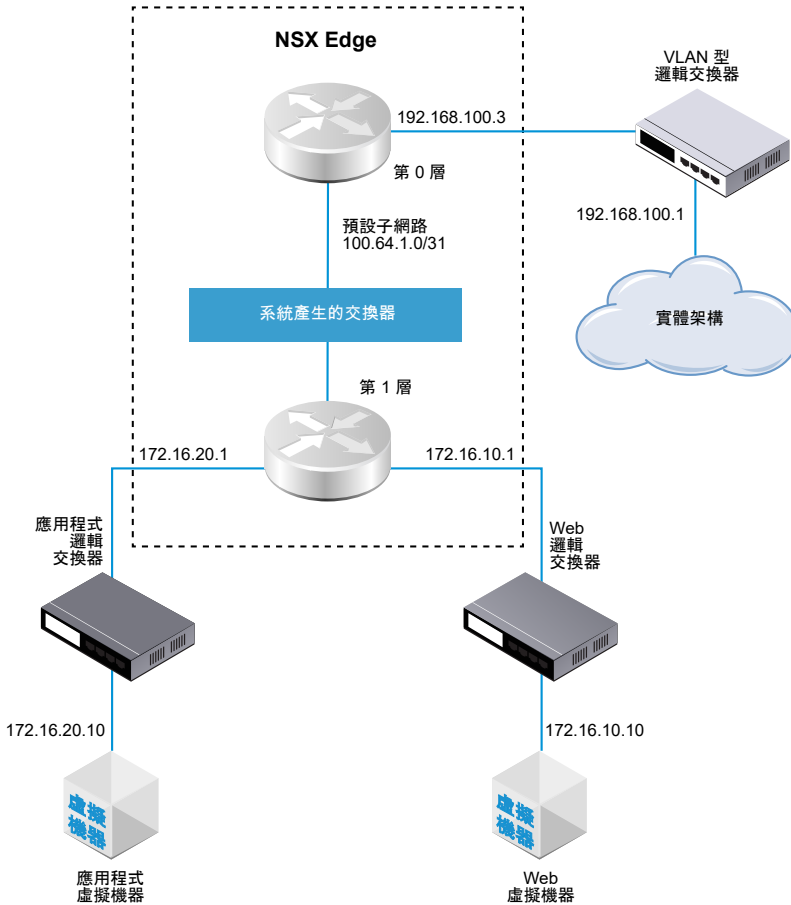
第 0 層邏輯路由器會在邏輯和實體網路之間提供閘道服務。

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 20-5. 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)

在管理程式模式中建立第 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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 第 0 層邏輯路由器 > 新增**。
- 3 輸入第 0 層邏輯路由器的名稱。
- 4 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。
- 5 (選擇性) 選取高可用性模式。

依預設，系統會使用作用中/作用中式模式。在作用中/作用中式模式中，流量會在所有成員間進行負載平衡。在作用中/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。

- 6
- 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。

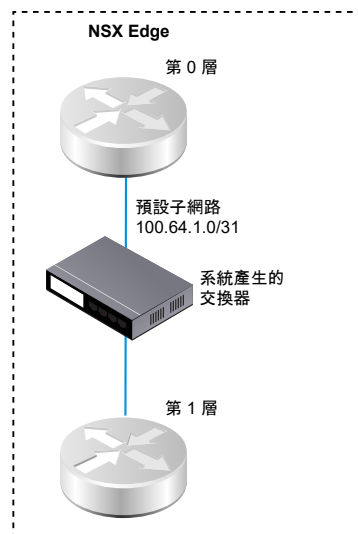
設定第 0 層邏輯路由器，將其連線至 VLAN 邏輯交換器以建立對外部網路的上行連接埠。請參閱在管理程式模式中針對 NSX Edge 上行，將第 0 層邏輯路由器連線至 VLAN 邏輯交換器。

在管理程式模式中將第 1 層路由器連結至第 0 層路由器

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。



必要條件

確認已在 NSX Manager 使用者介面中選取管理程式模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取網路 > 第 1 層邏輯路由器。
- 3 選取第 1 層邏輯路由器。
- 4 在 [第 0 層連線] 區段中，按一下連線。
- 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-edgel(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-edgel(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

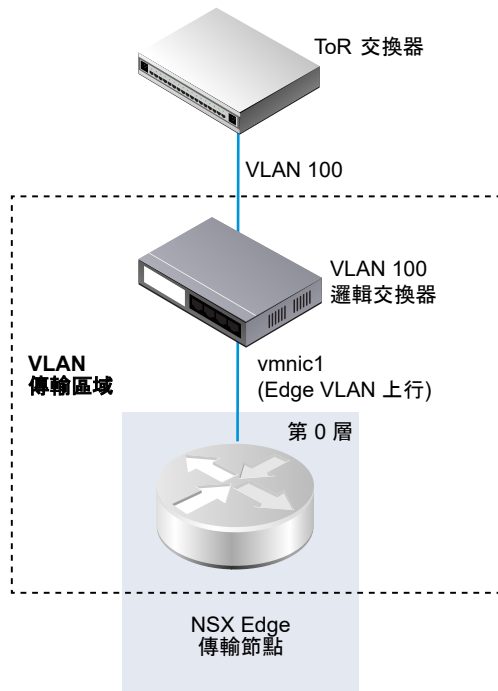
Total number of routes: 7

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
```

在管理程式模式中針對 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。請參閱在管理程式模式中為 NSX Edge 上行建立 VLAN 邏輯交換器。
- 建立第 0 層路由器。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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 選取**連結至新交換器連接埠**或**連結至現有的交換器連接埠**。
如果您選取**連結至新交換器連接埠**，系統將會自動建立連接埠。
- 10 指定與 TOR 交換器上已連線的連接埠位於相同子網路中的 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。請參閱在管理程式模式中針對 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 Edge 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-edgel(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-edgel(tier0_sr)> get route
Flags: t0c - Tier0-Connected, t0s - Tier0-Static, b - BGP,
t0n - Tier0-NAT, t1s - Tier1-Static, t1c - Tier1-Connected,
t1n: Tier1-NAT, t1l: Tier1-LB VIP, t1ls: Tier1-LB SNAT,
t1d: Tier1-DNS FORWARDER, t1lipsec: Tier1-IPSec, isr: Inter-SR,
> - selected route, * - FIB route

Total number of routes: 11

t1c> * 1.1.1.0/25 [3/0] via 100.64.1.1, downlink-282, 08w4d03h
t1c> * 1.1.2.0/24 [3/0] via 100.64.1.1, downlink-282, 08w4d03h
t0c> * 1.1.3.0/24 is directly connected, downlink-275, 08w4d03h
b > * 2.1.4.0/24 [20/0] via 40.40.40.10, uplink-273, 01w0d02h
b > * 10.182.48.0/20 [20/0] via 40.40.40.10, uplink-273, 01w0d02h
t0c> * 40.40.40.0/24 is directly connected, uplink-273, 08w4d03h
t0c> * 100.64.1.0/31 is directly connected, downlink-282, 08w4d03h
t0c> * 169.254.0.0/24 is directly connected, downlink-277, 01w0d02h
b > * 172.17.0.0/16 [20/0] via 40.40.40.10, uplink-273, 01w0d02h
t0c> * fc36:a750:db0d:7800::/64 is directly connected, downlink-282, 08w4d03h
t0c> * fe80::/64 is directly connected, downlink-282, 08w4d03h
```

5 探測 TOR。

```
nsx-edgel(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-edgel>
--- 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[在管理程式模式中設定靜態路由](#)或在[管理程式模式中的第 0 層邏輯路由器上設定 BGP](#)。

在管理程式模式中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

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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。

在管理程式模式中的第 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 在**網路 > 第 0 層邏輯路由器**或**網路 > 第 1 層邏輯路由器**找到路由器，並加以選取。
- 3 按一下**組態索引**標籤，然後選取**路由器連接埠**。
- 4 按一下**新增**。
- 5 輸入路由器連接埠的名稱，並選擇性地輸入說明。
- 6 在**類型**欄位中，選取**集中式**。
- 7 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。
- 8 (必要) 選取邏輯交換器。
- 9 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。
- 10 以 CIDR 標記法輸入路由器連接埠 IP 位址。
- 11 按一下**新增**。

在管理程式模式中設定高可用性 VIP

設定了 HA VIP (高可用性虛擬 IP) 時，即使一個上行已關閉，第 0 層邏輯路由器仍可運作。實體路由器只會與 HA VIP 互動。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

程序

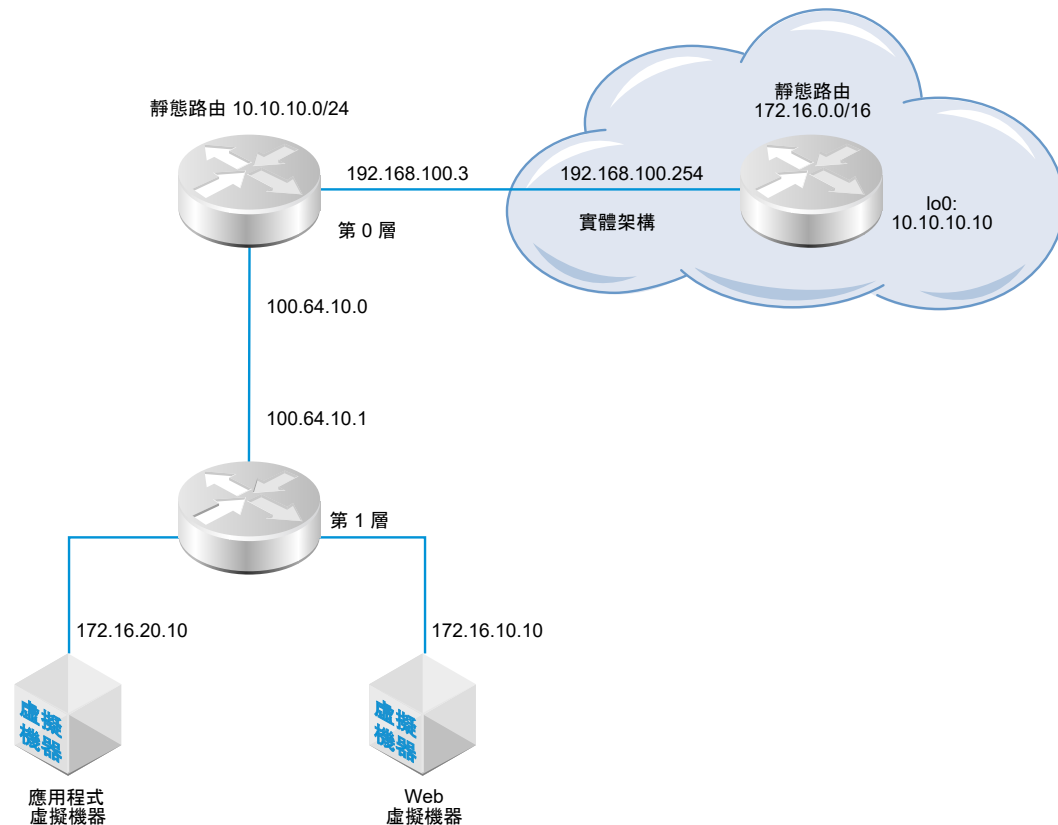
- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取**網路 > 第 0 層邏輯路由器**。
- 3 按一下第 0 層邏輯路由器名稱。
- 4 按一下**組態 > HA VIP**。
- 5 按一下**新增**。
- 6 以 CIDR 格式輸入 IP 位址。
- 7 若要啟用 HA VIP，請將狀態設定為**已啟用**。
- 8 選取正好兩個上行連接埠。
- 9 按一下**新增**。

在管理程式模式中設定靜態路由

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 20-6. 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**在管理程式模式中建立第 1 層邏輯路由器**。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱**第 1 章 NSX Manager**。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 第 0 層邏輯路由器**。

- 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 [確認第 0 層路由器上的靜態路由](#)。

確認第 0 層路由器上的靜態路由

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 [在管理程式模式中設定靜態路由](#)。

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。

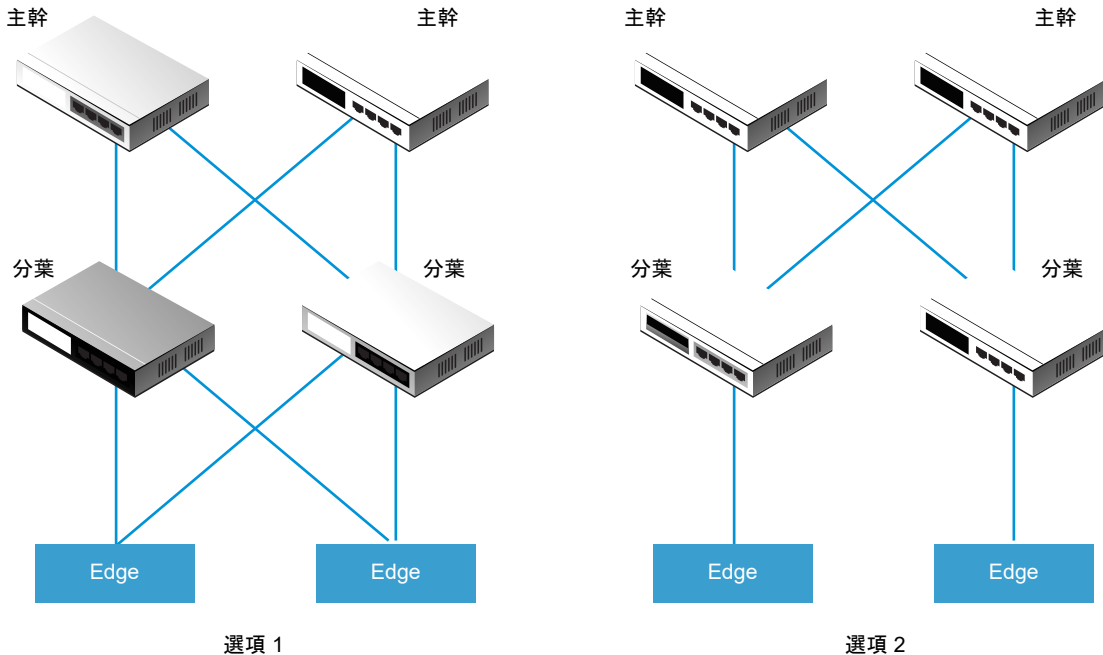
```
ping 10.10.10.10
```

```
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。

在管理程式模式中的第 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。

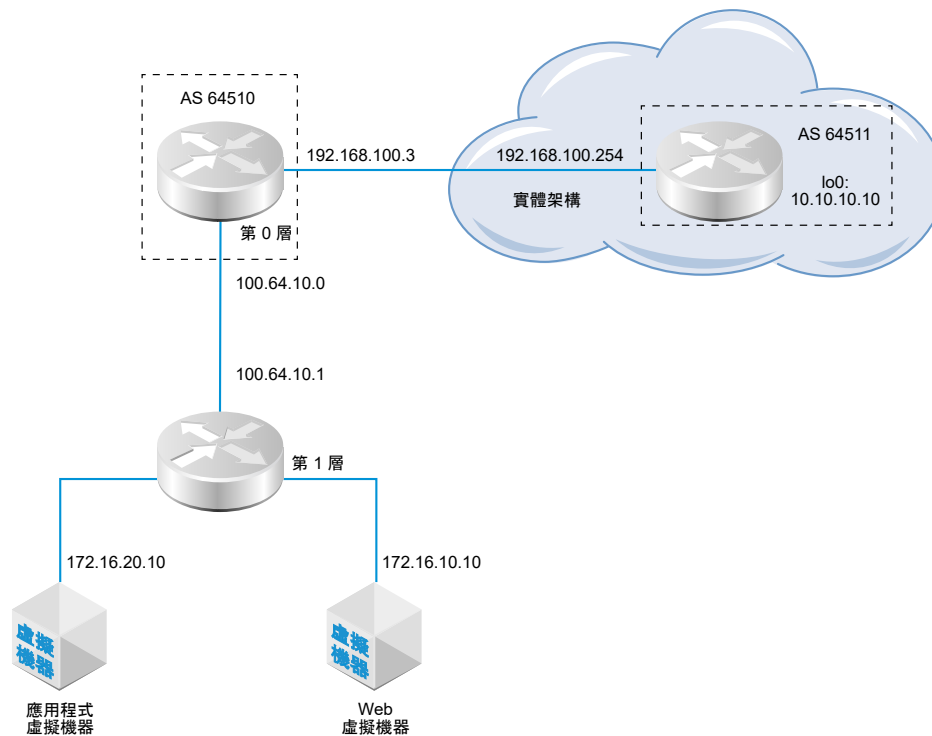
作用中/作用中模式的第 0 層邏輯路由器支援 SR (服務路由器) 間的路由。在作用中/作用中叢集中，如果 1 號路由器無法與南北向實體路由器進行通訊，流量就會重新路由至 2 號路由器。如果 2 號路由器能夠與該實體路由器進行通訊，則 1 號路由器與實體路由器之間的流量不受影響。

在具有的第 0 層邏輯路由器處於作用中/待命模式連結至處於作用中/作用中模式的第 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。作用中/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 對等中學習相同的路由，並在 SR #1 上的靜態路由優先使用所學習的路由，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 20-7. 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。請參閱在管理程式模式中的第 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。請參閱在管理程式模式中建立第 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。
- 確認已在 NSX Manager 使用者介面中選取管理程式模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取網路 > 第 0 層邏輯路由器。
- 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作用中/作用中模式，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[管理程式模式中的第 0 層邏輯路由器上設定 BGP](#)。

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

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

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

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

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



```

type          : SERVICE_ROUTER_TIER1

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

```

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

```

nsx-edge-1> vrf 5
nsx-edgel1(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[確認第 0 層路由器上的南北向連線和路由重新分配](#)。

在管理程式模式中的第 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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**。

在管理程式模式中啟用第 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[在管理程式模式中將第 1 層路由器連結至第 0 層路由器](#)。
- 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[在管理程式模式中建立路由對應](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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。

確認第 0 層路由器上的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。請參閱在管理程式模式中的第 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。請參閱在管理程式模式中啟用第 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-edgel1(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

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

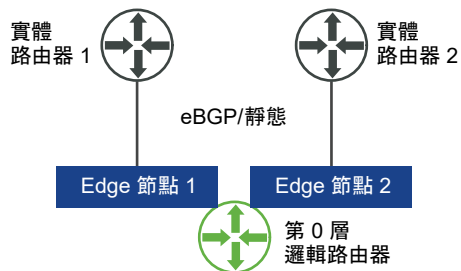
設定其他路由功能，例如 ECMP。

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 20-8. 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。

在管理程式模式中為 ECMP 的第二個 Edge 節點新增上行連接埠

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。請參閱在管理程式模式中為 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。請參閱在管理程式模式中建立第 0 層邏輯路由器。
- 確認已在 NSX Manager 使用者介面中選取管理程式模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取 **網路 > 第 0 層邏輯路由器**。

- 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	uRPF (單點傳播反向路徑轉送) 在外部、內部和服務介面上依預設為啟用。從安全性的觀點而言，最佳做法是在這些介面上保持啟用 uRPF。利用 ECMP 的架構中也建議使用 uRPF。 在具有非對稱路由的複雜路由架構中可以停用 uRPF。
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[在管理程式模式中新增第二個 BGP 芳鄰並啟用 ECMP 路由](#)。

在管理程式模式中新增第二個 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[在管理程式模式中為 ECMP 的第二個 Edge 節點新增上行連接埠](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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[確認第 0 層路由器上的 ECMP 路由連線](#)。

確認第 0 層路由器上的 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。請參閱在[管理程式模式中為 ECMP 的第二個 Edge 節點新增上行連接埠](#)與在[管理程式模式中新增第二個 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。

在管理程式模式中建立 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[在管理程式模式中建立第 0 層邏輯路由器](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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**。

在管理程式模式中建立社群清單

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[在管理程式模式中建立第 0 層邏輯路由器](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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**。

在管理程式模式中建立路由對應

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

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

必要條件

- 確認已設定 IP 首碼清單。請參閱[在管理程式模式中建立 IP 首碼清單](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。

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

- 10 在 [動作] 資料行中，選取允許或拒絕。

您可以允許或拒絕 IP 首碼清單中的 IP 位址通告其位址。

- 11 按一下儲存。

在管理程式模式中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) 之邏輯路由器的作用中/作用中或作用中/待命組態進行容錯移轉，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成正比。計時器在單一 Edge 節點設定時應設為 0。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。


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 選取**網路 > 第 0 層邏輯路由器**。
- 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。

管理程式模式中的 NAT

您可以在**管理程式**模式中設定網路位址轉譯 (NAT)。

備註 如果您使用**管理程式**模式來修改在**原則**模式中建立的物件，則可能無法進行某些設定。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](#)。

網路位址轉譯

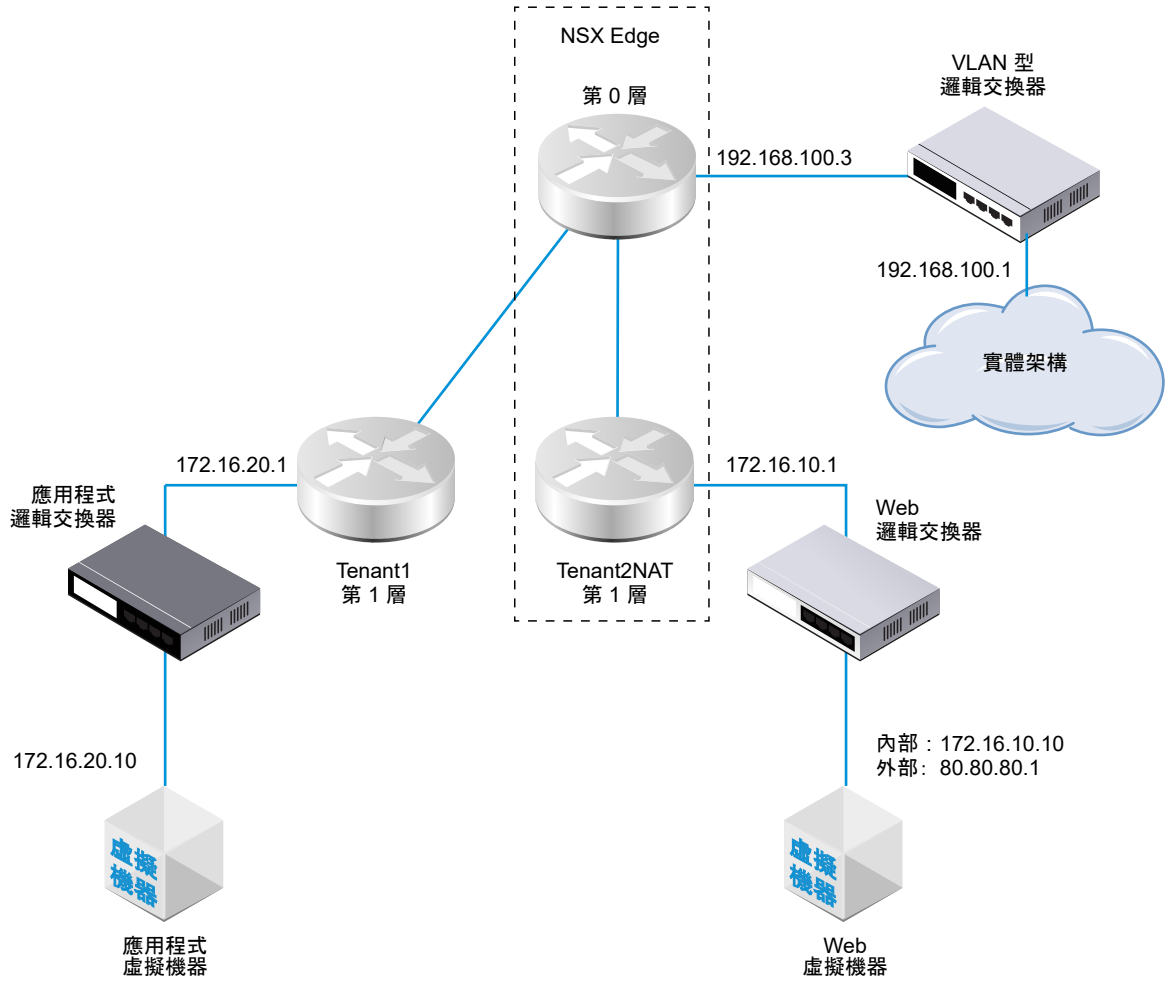
NSX-T Data Center 中的網路位址轉譯 (NAT) 可在第 0 層和第 1 層邏輯路由器中設定。

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。

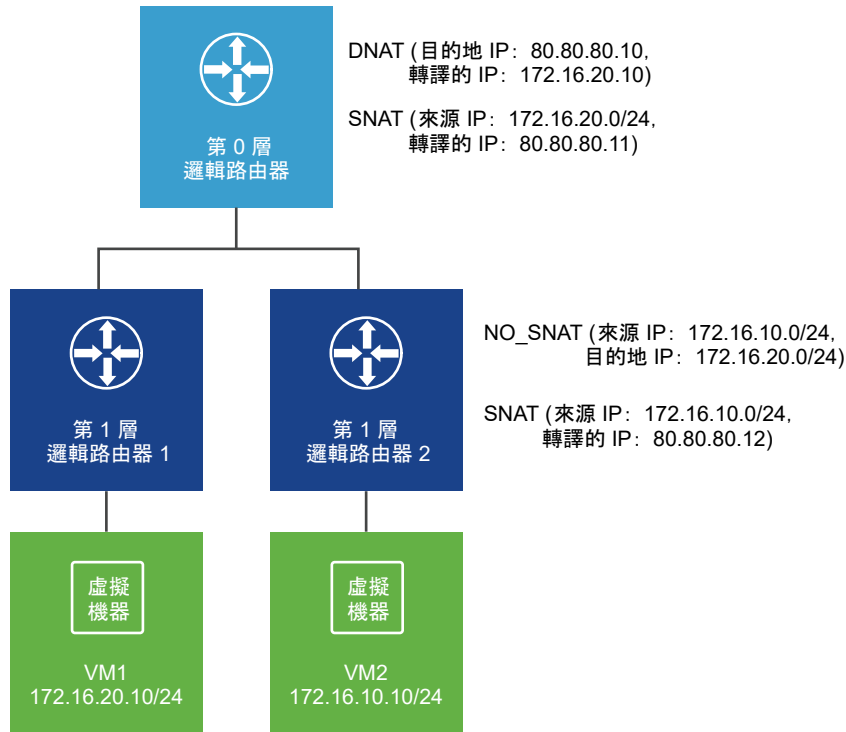
NAT 會在 Tenant2NAT 邏輯路由器對第 0 層邏輯路由器的連線上行強制執行。

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 20-9. 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。

在管理程式模式中於第 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。請參閱在管理程式模式中針對 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。請參閱在管理程式模式中設定靜態路由、在管理程式模式中的第 0 層邏輯路由器上設定 BGP 和在管理程式模式中啟用第 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。請參閱在管理程式模式中將第 1 層路由器連結至第 0 層路由器。

- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱在管理程式模式中的第 1 層邏輯路由器上新增下行連接埠和在管理程式模式中的第 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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 第 0 層邏輯路由器**。
- 3 按一下要在其上設定 NAT 的第 1 層邏輯路由器。
- 4 選取**服務 > NAT**。
- 5 按一下**新增**。
- 6 指定優先順序值。
值越低表示此規則的優先順序越高。
- 7 對於**動作**，請選取 **SNAT** 以啟用來源 NAT，或選取 **NO_SNAT** 以停用來源 NAT。
- 8 選取通訊協定類型。
依預設會選取**任何通訊協定**。
- 9 (選擇性) 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
如果您將此欄位保留空白，則系統會轉譯路由器下行連接埠上的所有來源。在此範例中，來源 IP 位址為 172.16.10.10。
- 10 (選擇性) 對於**目的地 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
如果您將此欄位保留空白，則 NAT 會套用至本機子網路外部的所有目的地。
- 11 如果**動作**為 **SNAT**，則對於**轉譯的 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
在此範例中，已轉譯的 IP 位址為 80.80.80.1。
- 12 (選擇性) 對於**套用至**，請選取路由器連接埠。
- 13 (選擇性) 設定規則的狀態。
此規則預設為啟用。
- 14 (選擇性) 變更記錄狀態。
依預設會停用記錄。
- 15 (選擇性) 變更防火牆略過設定。
此設定預設為啟用。

結果

新規則會在 NAT 下方列出。例如：

Tenant2NAT										
概觀 組態 路由 服務										
NAT 重新整理										
未收集任何統計資料										
+ 新增 編輯 刪除										
識別碼	動作	相符					已轉譯		套用至	統計資料
		通訊協定	來源 IP	來源連接埠	目的地 IP	目的地連接埠	IP	連接埠		
優先順序: 1024										
1036	SNAT	任何	172.16.10.10	任何	任何	任何	80.80.80.1	任何		

後續步驟

設定第 1 層路由器以通告 NAT 路由器。

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

在管理程式模式中於第 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。請參閱在管理程式模式中針對 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。請參閱在管理程式模式中設定靜態路由、在管理程式模式中的第 0 層邏輯路由器上設定 BGP 和在管理程式模式中啟用第 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。請參閱在管理程式模式中將第 1 層路由器連結至第 0 層路由器。
- 第 1 層路由器必須設定下行連接埠和路由通告。請參閱在管理程式模式中的第 1 層邏輯路由器上新增下行連接埠和在管理程式模式中的第 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。
- 確認已在 NSX Manager 使用者介面中選取管理程式模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取網路 > 第 1 層邏輯路由器。

- 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**，請指定 IP 位址或以逗號分隔的 IP 位址清單。
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：

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		
1034	DNAT	任何	任何	任何	80.80.80.1	任何	172.16.10.10	任何	

優先順序: 1024

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。

在管理程式模式中通告第 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 1 層邏輯路由器**。
- 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。

在管理程式模式中通告第 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層編輯路由器**。
- 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 <code>advertise-to-bgp-neighbor</code> 。
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。

管理程式模式中於第 0 層邏輯路由器上設定來源與目的地 NAT

您可以在以作用中/待命模式執行的第 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 規則可套用至一個位址，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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 第 0 層邏輯路由器**。
- 3 按一下第 0 層邏輯路由器。
- 4 選取**服務 > NAT**。
- 5 按一下**新增**以新增 NAT 規則。
- 6 指定優先順序值。

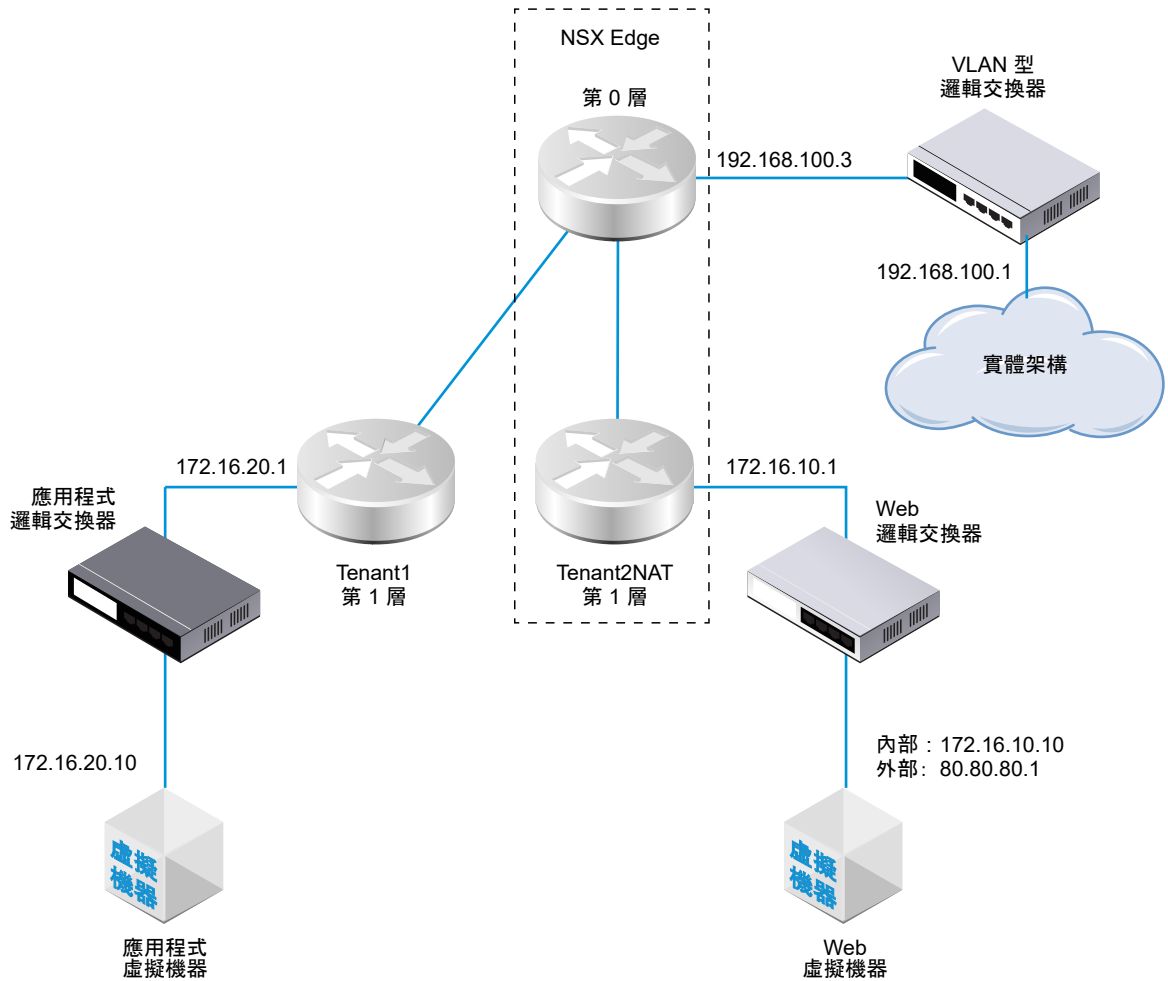
較低的值表示較高的優先順序。

- 7 針對**動作**，選取 **SNAT**、**DNAT**、**Reflexive**、**NO_SNAT** 或 **NO_DNAT**。
- 8 選取**通訊協定類型**。
依預設會選取**任何通訊協定**。
- 9 (必要) 對於**來源 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
如果您將此欄位保留空白，此 NAT 規則會套用至本機子網路外部的所有來源。
- 10 對於**目的地 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
- 11 對於**轉譯的 IP**，請以 CIDR 格式指定 IP 位址或 IP 位址範圍。
- 12 (選擇性) 如果**動作**為 **DNAT**，則對於**轉譯的連接埠**，請指定轉譯的連接埠。
- 13 (選擇性) 對於**套用至**，請選取**路由器連接埠**。
- 14 (選擇性) 設定規則的狀態。
此規則預設為啟用。
- 15 (選擇性) 變更記錄狀態。
依預設會停用記錄。
- 16 (選擇性) 變更防火牆略過設定。
此設定預設為啟用。

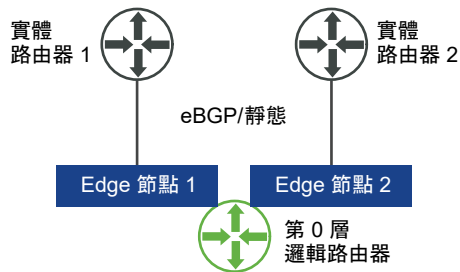
自反 NAT

當第 0 層邏輯路由器在作用中/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。



在管理程式模式中，於第 0 層或第 1 層邏輯路由器上設定自反 NAT

當第 0 層或第 1 層邏輯路由器在作用中/作用中模式下執行時，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。對於作用中/作用中路由器，您可以使用自反 NAT (有時稱為無狀態 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 在**網路 > 第 0 層邏輯路由器**或**網路 > 第 1 層邏輯路由器**中，找到您要修改的邏輯路由器。
- 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		
▼ 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	

在管理程式模式中群組物件

您可以在**管理程式**模式中建立 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**管理程式**模式來修改在**原則**模式中建立的物件，則可能無法進行某些設定。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](#)。

在管理程式模式中建立 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。

備註 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**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**。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > IP 管理 > IP 位址集區**。
- 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**。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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**。

在管理程式模式中建立 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**。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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、標籤、電腦作業系統名稱或電腦名稱。
- **傳輸節點** - 可以指定等於某個 Edge 節點或主機節點的節點類型。
- **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。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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**。

在管理程式模式中管理虛擬機器的標籤

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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取導覽面板中的**詳細目錄 > 虛擬機器**。

虛擬機器的清單會顯示 4 個資料行：虛擬機器、外部識別碼、來源和標籤。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 以指定標籤，並選擇性地指定範圍。
刪除標籤	選取現有的標籤，然後按一下 刪除 。

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**。

管理程式模式中的 DHCP

您可以在**管理程式**模式中設定 DHCPv4。

您無法在**管理程式**模式中設定或修改 DHCPv6 伺服器組態。您必須使用下列任一項目來設定或修改 DHCPv6 伺服器：

- 原則模式
- 原則 API
- 管理程式 API

備註 如果您使用**管理程式**模式來修改在**原則**模式中建立的物件，則可能無法進行某些設定。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](#)。

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。

若要封鎖連接埠 67 和 68 的 DHCP 封包，請透過下列項目設定 DFW 規則：

來源	目的地	服務	規則
任何	任何	任何	封鎖

若要允許 DHCP 封包，請透過下列項目設定 DFW 規則：

來源	目的地	服務	規則
任何	任何	連接埠 67 和 68、TCP	允許

備註 在此版本中，DHCP 伺服器不支援客體 VLAN 標記。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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[在管理程式模式中建立 DHCP 伺服器](#)。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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[在管理程式模式中將 DHCP 伺服器連結至邏輯交換器](#)。

在管理程式模式中將 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱[第 1 章 NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器 > 交換器**。
 - a 選取邏輯交換器。
 - b 按一下**動作 > 連結至 DHCP 伺服器**。
- 3 或者，選取**網路 > DHCP > 伺服器**。
 - a 選取 DHCP 伺服器。
 - b 按一下**動作 > 連結至邏輯交換器**。

在管理程式模式中將 DHCP 伺服器與邏輯交換器中斷連結

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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 邏輯交換器**。
- 3 按一下您想從中斷連結 DHCP 伺服器的邏輯交換器。
- 4 按一下**動作 > 從 DHCP 伺服器中斷連結**。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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。請參閱在**管理程式模式中建立 DHCP 轉送服務**。

在管理程式模式中建立 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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到原則和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**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。請參閱在**管理程式模式中將 DHCP 轉送服務新增至邏輯路由器連接埠**。

在管理程式模式中將 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。請參閱在**管理程式模式中建立 DHCP 轉送服務**。
- 確認路由器連接埠的類型為下行。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 第 0 層邏輯路由器**。
- 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。

在管理程式模式中新增中繼資料 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》。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 **NSX Manager**。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**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。

在管理程式模式中將中繼資料 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，請參閱在管理程式模式中建立邏輯交換器。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**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**網路 > 邏輯交換器 > 交換器**，選取交換器，然後選取功能表選項**動作 > 新增至中繼資料 Proxy**。

在管理程式模式中將中繼資料 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**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

您還可以將中繼資料 Proxy 伺服器與邏輯交換器中斷連結，方法為導覽至**網路 > 邏輯交換器 > 交換器**，選取交換器，然後選取功能表選項**動作 > 從中繼資料 Proxy 中斷連結**。

管理程式模式中的 IP 位址管理

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**管理程式模式**來修改在**原則模式**中建立的物件，則可能無法進行某些設定。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。

在管理程式模式中管理 IP 區塊

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

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則**和**管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > IP 位址集區 > IP 區塊**。
- 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。

在管理程式模式中管理 IP 區塊的子網路

您可以新增或刪除 IP 區塊的子網路

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則**和**管理程式模式**按鈕，請參閱**設定使用者介面設定**。


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 選取 **網路 > IP 位址集區 > IP 區塊**。
- 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**。

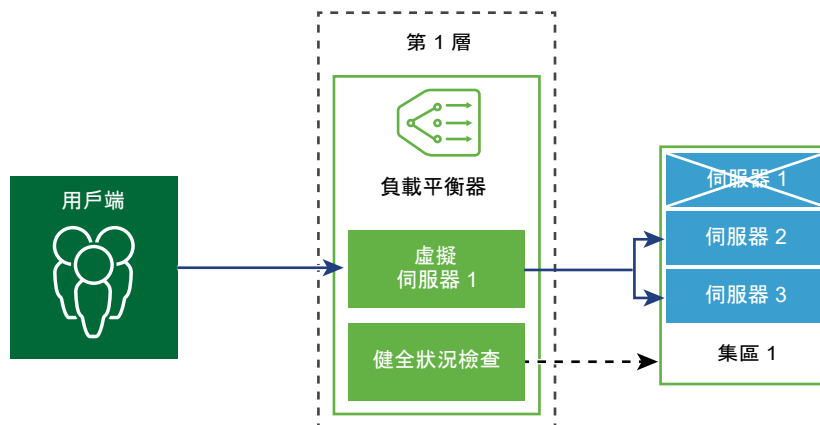
管理程式模式中的負載平衡

此資訊涵蓋管理程式模式中的 NSX-T Data Center 負載平衡組態。

如需 NSX Advanced Load Balancer (Avi 網路) 的相關資訊，請參閱 <https://www.vmware.com/products/nsx-advanced-load-balancer.html>。

備註 如果您使用管理程式模式來修改在原則模式中建立的物件，則可能無法進行某些設定。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。

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。

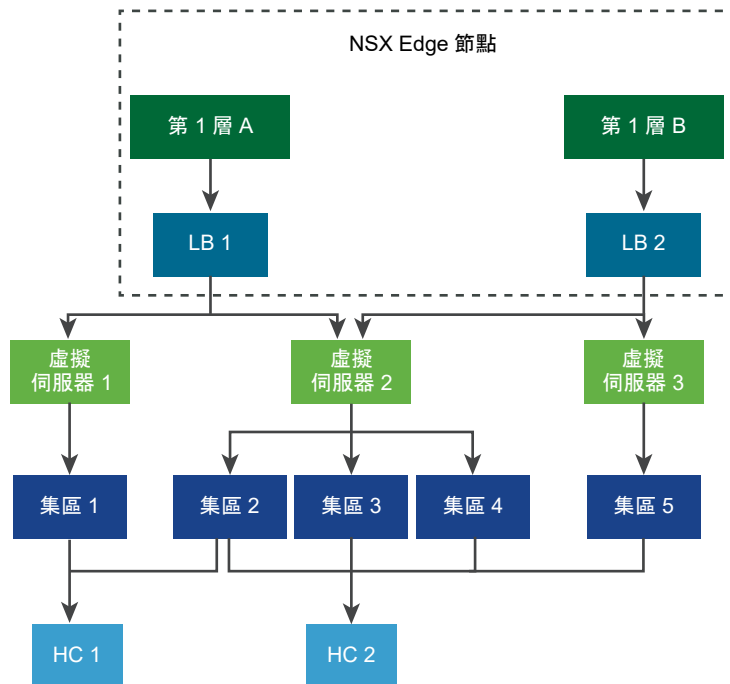
備註 僅第 1 層邏輯路由器支援邏輯負載平衡器。一個負載平衡器只能連結至第 1 層邏輯路由器。

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。

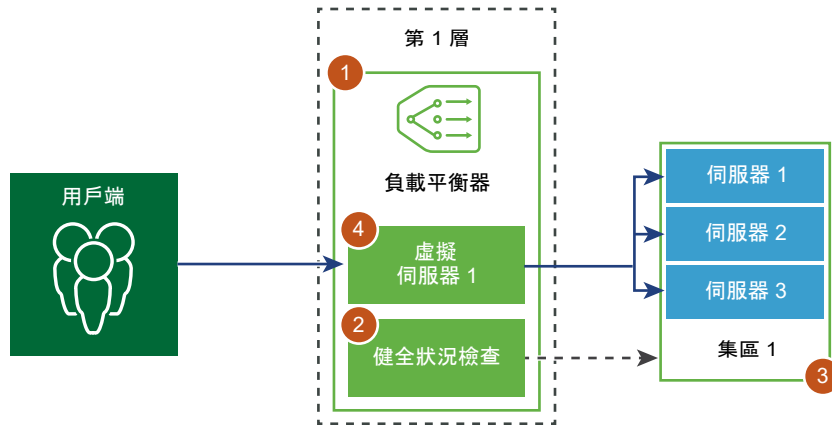
若要測試每個伺服器是否正確執行應用程式，您可以新增用於檢查伺服器健全狀況狀態的健全狀況檢查監視器。



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。

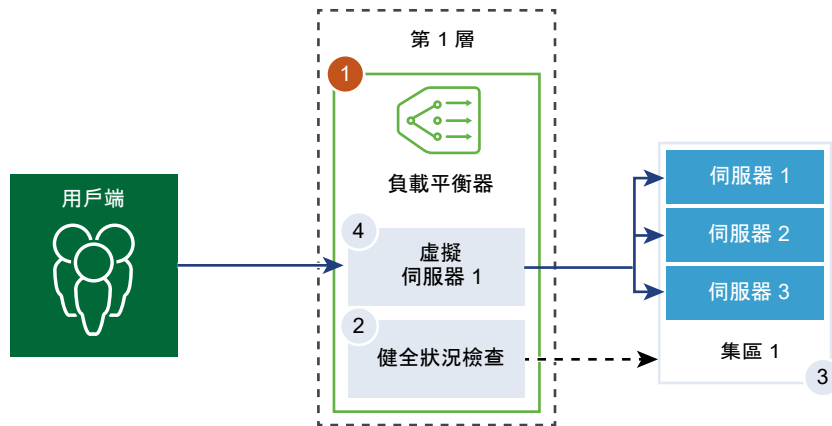


在管理程式模式中建立負載平衡器

負載平衡器將會建立並連結至第 1 層邏輯路由器。

重要 本主題中的資訊為在管理程式模式中管理您的環境所特有。如需有關管理程式模式和原則模式的詳細資訊，請參閱第 1 章 [NSX Manager](#)。如需原則模式中負載平衡器的相關資訊，請參閱第 8 章 [負載平衡](#)。

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。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[在管理程式模式中建立第 1 層邏輯路由器](#)。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則和管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 負載平衡器 > 新增**。
- 3 輸入負載平衡器的名稱和說明。

- 4 根據可用的資源，選取負載平衡器虛擬伺服器的大小和集區成員數目。
- 5 從下拉式功能表中定義錯誤記錄的嚴重性層級。
負載平衡器會將發生的不同嚴重性層級問題的相關資訊收集到錯誤記錄。
- 6 按一下**確定**。
- 7 將新建立的負載平衡器關聯至虛擬伺服器。
 - a 選取負載平衡器，然後按一下**動作 > 連結至虛擬伺服器**。
 - b 從下拉式功能表中選取現有的虛擬伺服器。
 - c 按一下**確定**。
- 8 將新建立的負載平衡器連結至第 1 層邏輯路由器。
 - a 選取負載平衡器，然後按一下**動作 > 連結至邏輯路由器**。
 - b 從下拉式功能表中選取現有的第 1 層邏輯路由器。
第 1 層路由器必須處於作用中/待命模式。
 - 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。

在管理程式模式中設定主動健全狀況監控

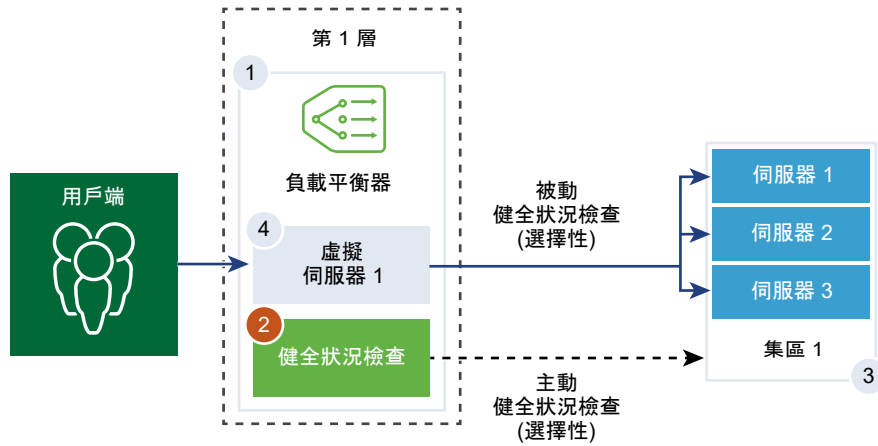
主動健全狀況監控可用來測試伺服器是否可用。主動健全狀況監控使用數種類型的測試，例如傳送基本 Ping 至伺服器或進階 HTTP 要求來監控應用程式健全狀況。

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[在管理程式模式中建立獨立的第 1 層邏輯路由器](#)。

備註 每個伺服器集區可設定為使用多台主動健全狀況監控。



必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 負載平衡 > 監控 > 主動健全狀況監控 > 新增**。
- 3 輸入主動健全狀況監控的名稱和說明。
- 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控值。

選項	說明
監控時間間隔	設定監控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。 在要求 URL 中不允許 ASCII 控制字元 (退格鍵、垂直 Tab 鍵、水平 Tab 鍵、換行字元等)、不安全的字元 (例如 space、\、<、>、{、}) 以及 ASCII 字元集以外的任何字元，且都應進行編碼。例如，以加號 (+) 或 %20 取代空格。
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	輸入監控預期與 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。 在要求 URL 中不允許 ASCII 控制字元 (退格鍵、垂直 Tab 鍵、水平 Tab 鍵、換行字元等)、不安全的字元 (例如 space、\、<、>、{、}) 以及 ASCII 字元集以外的任何字元，且都應進行編碼。例如，以加號 (+) 或 %20 取代空格。
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	輸入監控預期與 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

將主動健全狀況監控與伺服器集區相關聯。請參閱在管理程式模式中新增用於負載平衡的伺服器集區。

在管理程式模式中設定被動健全狀況監控

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控。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 負載平衡 > 監控 > 被動健全狀況監控 > 新增**。
- 3 輸入被動健全狀況監控的名稱和說明。
- 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控值。

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

將被動健全狀況監控與伺服器集區相關聯。請參閱在管理程式模式中新增用於負載平衡的伺服器集區。

在管理程式模式中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。

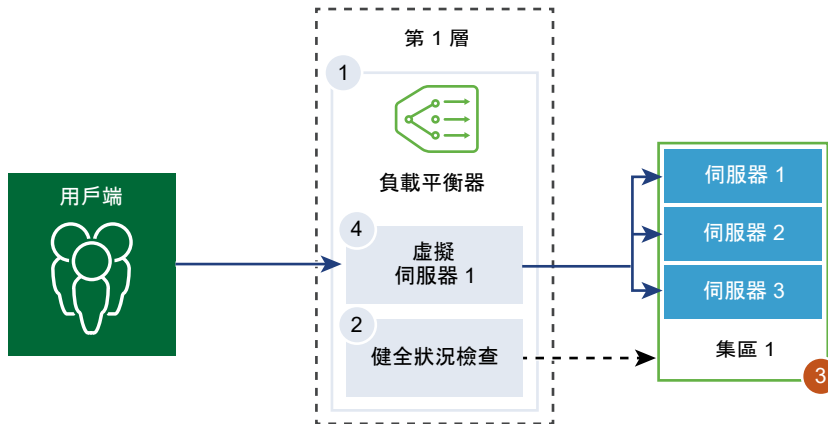
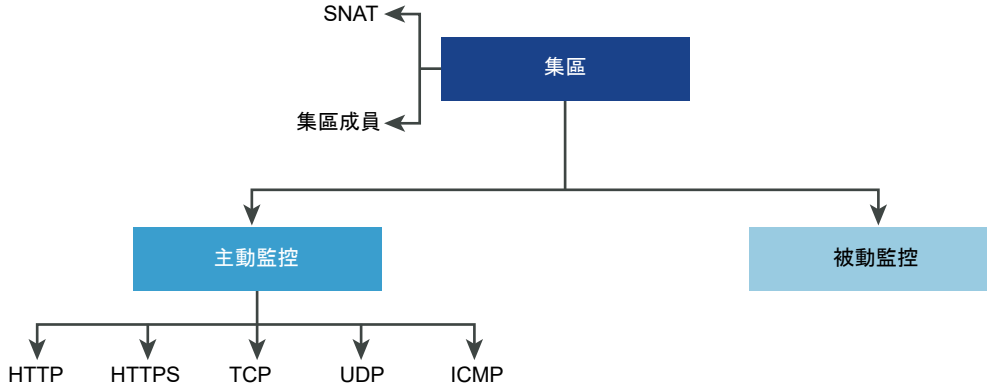


圖 20-10. 伺服器集區參數組態



必要條件

- 如果您使用動態集區成員，則必須設定 NSGroup。請參閱在管理程式模式中建立 NSGroup。
- 根據您使用的監控，請確認主動或被動健全狀況監控已設定。請參閱在管理程式模式中設定主動健全狀況監控或在管理程式模式中設定被動健全狀況監控。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取 **網路 > 負載平衡 > 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)。
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控，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控。

設定伺服器集區的主動和被動健全狀況監控為選用。當您選取主動健全狀況監控，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，請參閱在管理程式模式中建立獨立的第 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。

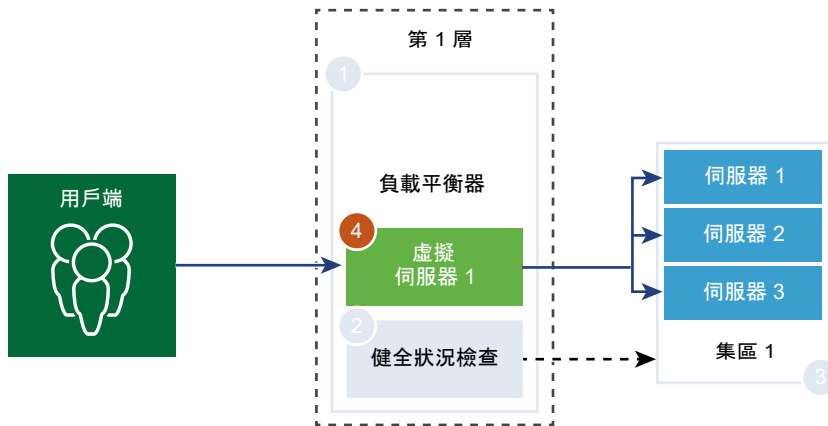
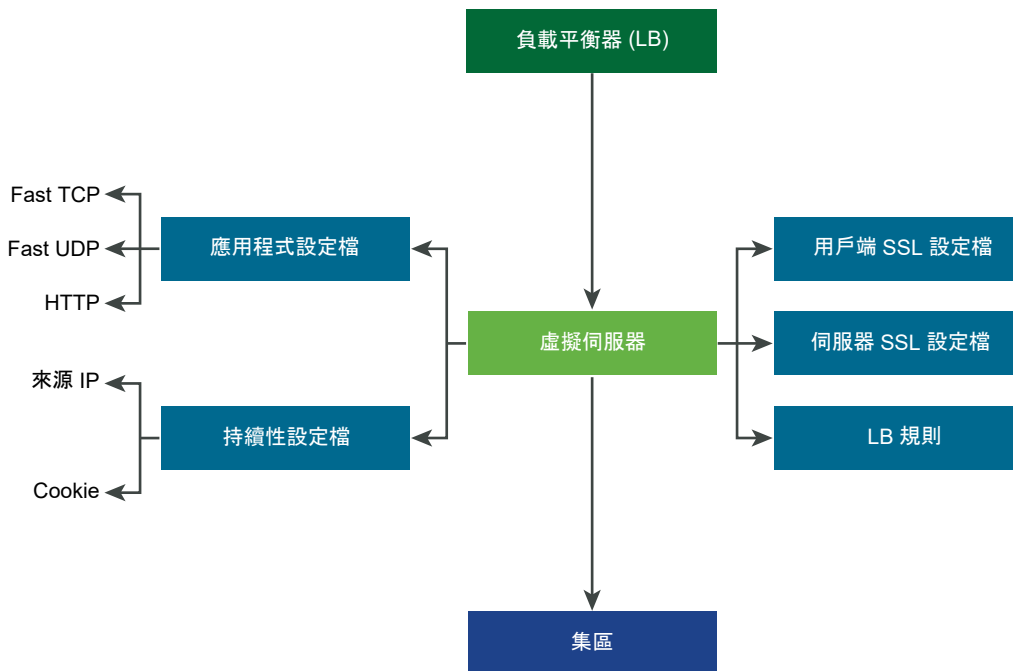


圖 20-11. 虛擬伺服器元件



在管理程式模式中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。Fast TCP、Fast 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 20-12. 第 4 層 TCP 和 UDP 應用程式設定檔

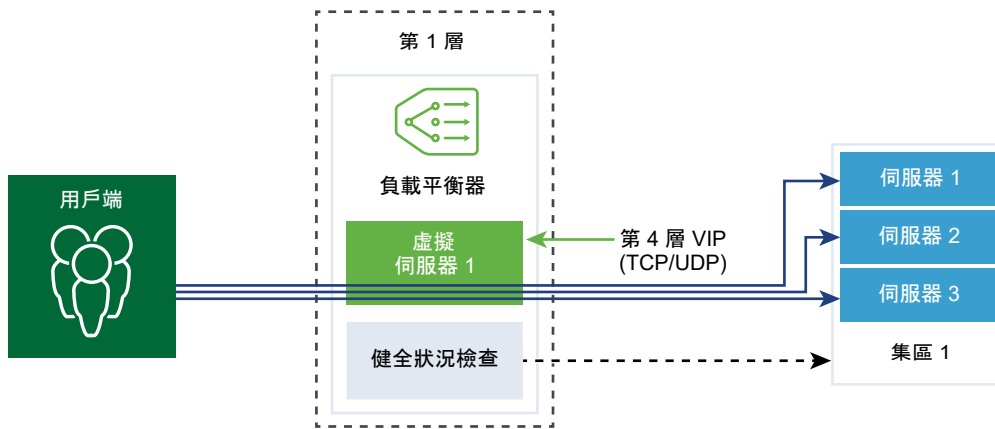
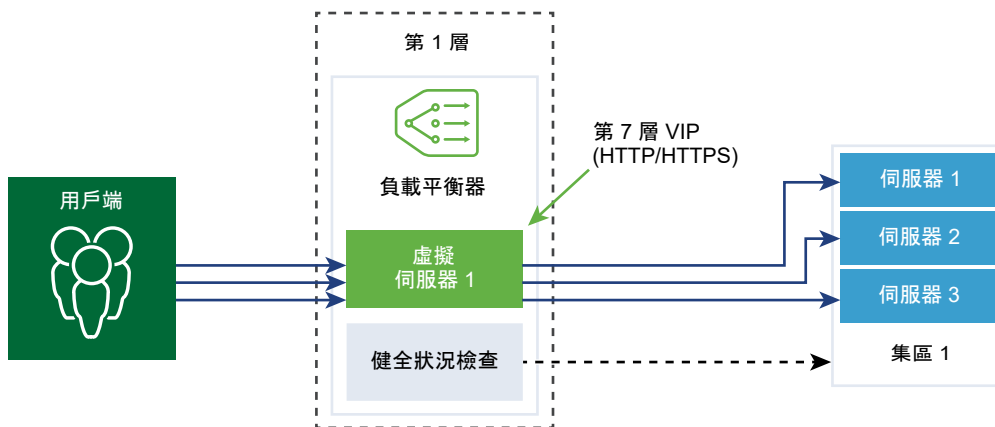


圖 20-13. 第 7 層 HTTPS 應用程式設定檔



必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到原則和管理程式模式按鈕，請參閱設定使用者介面設定。

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 選取 **網路 > 負載平衡 > 設定檔 > 應用程式設定檔**。
- 3 建立 Fast TCP 應用程式設定檔。
 - a 從下拉式功能表中選取 **新增 > Fast TCP 設定檔**。
 - b 輸入 Fast 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 Fast 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 Fast 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 > Fast UDP 設定檔**。
 - b 輸入 Fast 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。

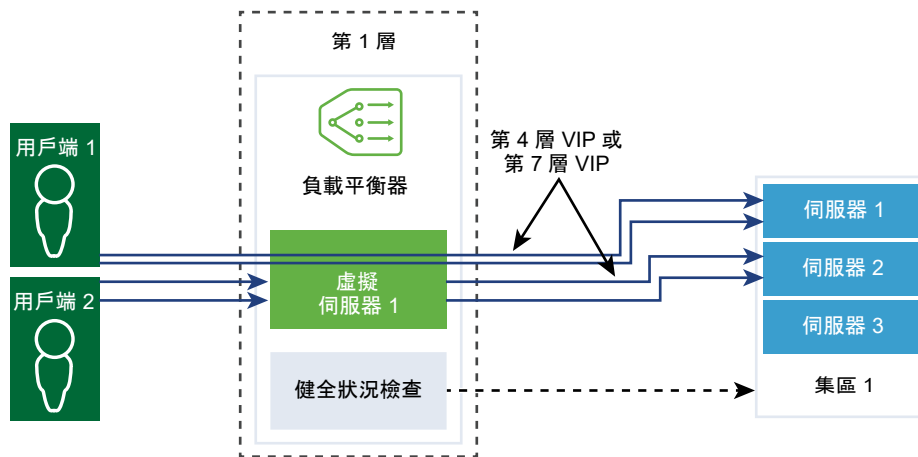
在管理程式模式中設定持續性設定檔

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。



必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式模式**按鈕，請參閱[設定使用者介面設定](#)。

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 選取**網路 > 負載平衡 > 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有持續性資料表。</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有 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。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。

在管理程式模式中設定 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 20-14. SSL 卸載

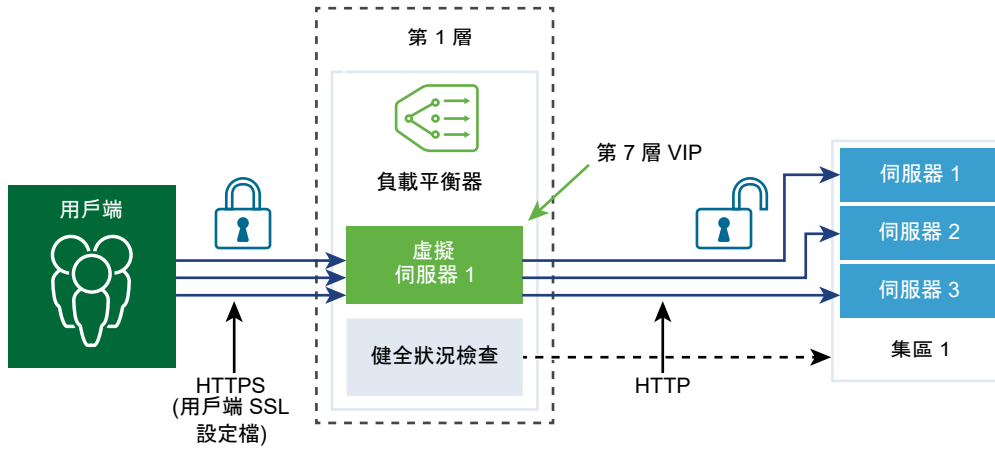
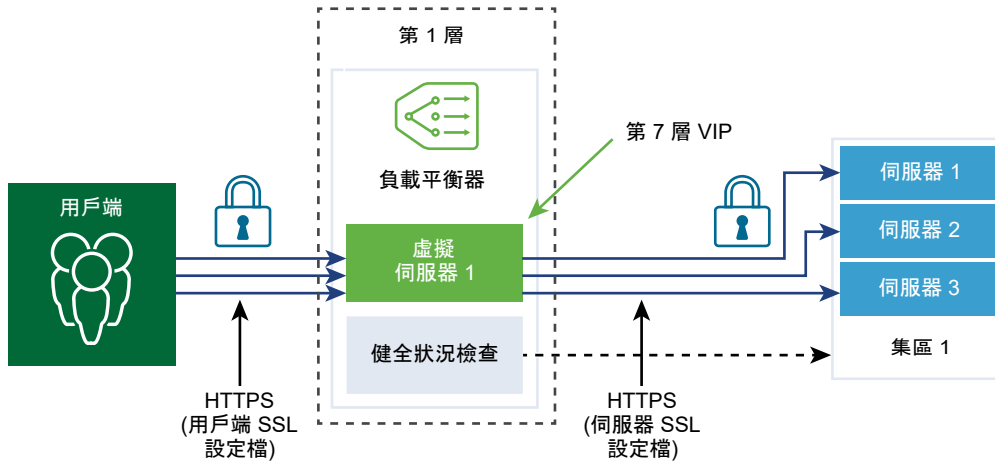


圖 20-15. 端對端 SSL



必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到原則和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 負載平衡 > 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**。

在管理程式模式中設定第 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。請參閱在管理程式模式中設定應用程式設定檔。
- 確認持續性設定檔可供使用。請參閱在管理程式模式中設定持續性設定檔。
- 確認用戶端與服务器的 SSL 設定檔可供使用。請參閱在管理程式模式中設定 SSL 設定檔。
- 確認伺服器集區可供使用。請參閱在管理程式模式中新增用於負載平衡的伺服器集區。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**網路 > 負載平衡 > 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	如果未定義虛擬伺服器的集區成員連接埠，請輸入預設集區成員連接埠。 例如，如果虛擬伺服器所定義的連接埠範圍為 2000–2999，並且預設集區成員連接埠範圍設定為 8000-8999，則到虛擬伺服器連接埠 2500 的傳入用戶端連線會傳送到目的地連接埠設定為 8500 的集區成員。

9 從下拉式功能表中選取現有的伺服器集區。

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

10 從下拉式功能表中選取現有 sorry 伺服器集區。

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

11 按下一步。

12 從下拉式功能表中選取現有持續性設定檔。

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

13 按一下完成。

在管理程式模式中設定第 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[在管理程式模式中設定應用程式設定檔](#)。
- 確認持續性設定檔可供使用。請參閱[在管理程式模式中設定持續性設定檔](#)。
- 確認用戶端與伺服器的 SSL 設定檔可供使用。請參閱[在管理程式模式中設定 SSL 設定檔](#)。

- 確認伺服器集區可供使用。請參閱在管理程式模式中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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 NSX Manager。如果看不到**原則和管理程式**模式按鈕，請參閱設定使用者介面設定。
- **設定第 7 層虛擬伺服器集區和規則**
對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器規則，並使用比對或動作規則自訂負載平衡行為。
- **設定第 7 層虛擬伺服器負載平衡設定檔**
對於第 7 層虛擬伺服器，您可以選擇性地設定負載平衡器持續性、用戶端 SSL 和伺服器端 SSL 設定檔。

程序

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

設定第 7 層虛擬伺服器集區和規則

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

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

REGEX 限制包括：

- 不支援字元聯集和交集。例如，請勿使用 `[a-z[0-9]]` 和 `[a-z&&[aeiou]]`，分別改為使用 `[a-z0-9]` 和 `[aeiou]`。
- 僅支援 9 個反向參考，並且不能使用 `\1` 到 `\9` 來參考它們。
- 使用 `\Odd` 格式來比對八進位字元，而非 `\ddd` 格式。
- 最上層不支援內嵌式旗標，僅群組內支援這些旗標。例如，請勿使用「`Case (?i:s)ensitive`」，改為使用「`Case ((?i:s)ensitive)`」。
- 不支援前置處理作業 `\l`、`\u`、`\L` 及 `\U`。其中，`\l` - 可將下一個字元轉成小寫 `\u` - 可將下一個字元轉成大寫 `\L` - 可將 `\E` 之前的字元轉成小寫 `\U` - 可將 `\E` 之前的字元轉成大寫。

- 不支援 `(?(condition)X)`、`(? {code})`、`(??{Code})` 及 `(?#comment)`。
- 不支援預先定義的 Unicode 字元類別 `\X`。
- 不支援將具名字元建構用於 Unicode 字元。例如，請勿使用 `\N{name}`，改為使用 `\u2018`。

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

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

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

備註 對於具名擷取群組，名稱不能以 `_` 字元開頭。

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

- `$_args` - 來自要求的引數
- `$_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。請參閱在管理程式模式中設定第 7 層虛擬伺服器。

程序

- 1 開啟第 7 層虛擬伺服器。
- 2 跳至 [虛擬伺服器識別碼] 頁面。
- 3 輸入虛擬伺服器 IP 位址和連接埠號碼。

您可以輸入虛擬伺服器連接埠號碼或連接埠範圍。

- 4 完成進階內容詳細資料。

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

- 5 (選擇性) 從下拉式功能表中選取現有的預設伺服器集區。

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

6 按一下新增，針對 HTTP 要求重寫階段設定負載平衡器規則。

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

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

支援的比對條件	說明
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
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。請參閱在管理程式模式中設定第 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。

管理程式模式中的防火牆

您可以在**管理程式模式**中設定分散式防火牆和邏輯路由器防火牆。

備註 如果您使用**管理程式模式**來修改在**原則模式**中建立的物件，則可能無法進行某些設定。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*。

在管理程式模式中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。請參閱在**管理程式模式**中新增防火牆規則。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱第 1 章 *NSX Manager*。如果看不到**原則**和**管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 在**網路 > 第 0 層邏輯路由器**或**網路 > 第 1 層邏輯路由器**中找到路由器。
- 3 按一下邏輯路由器的名稱。
- 4 選取**服務 > Edge 防火牆**。
- 5 按一下現有的區段或規則。
- 6 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。
- 7 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 叢集在作用中/作用中式模式下執行，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 叢集設定為在作用中/待命模式下執行。

在管理程式模式中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**在管理程式模式中建立第 2 層橋接器備份邏輯交換器**。
- 確認已在 NSX Manager 使用者介面中選取**管理程式模式**。請參閱**第 1 章 NSX Manager**。如果看不到**原則和管理程式模式**按鈕，請參閱**設定使用者介面設定**。

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 選取**安全性 > 橋接防火牆**。
- 3 選取邏輯交換器。
交換器必須已連結至橋接器設定檔。
- 4 若要設定第 2 層或第 3 層防火牆，請遵循先前章節中的相同步驟。

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。

在管理程式模式中啟用和停用分散式防火牆

您可以啟用或停用分散式防火牆功能。

如果已停用，則不會在資料平面層級強制執行任何防火牆規則。重新啟動時將強制執行規則。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 導覽到 **安全性 > 分散式防火牆**。
- 2 按一下**設定索引**標籤。
- 3 按一下分散式防火牆 **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**。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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。

- 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。

- 輸入區段名稱。
- 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。

- 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。

- 按一下**確定**。

後續步驟

將防火牆規則新增至區段。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 **NSX Manager**。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

程序

- 選取**安全性 > 分散式防火牆**。
- 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。
- 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。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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**。

在管理程式模式中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/dfwpklogs.log 檔案中。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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**。

在管理程式模式中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 Edge 節點虛擬機器新增至防火牆排除清單。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆 > 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)。先處理第 2 層防火牆規則，然後再處理第 3 層規則，如果第 2 層規則允許，則將由第 3 層規則進行處理。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。

表 20-1. 防火牆規則的內容 (續)

內容	說明
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/dfwpklogs.log 檔案。
動作	規則套用的動作可為 允許 、 捨棄 或 拒絕 。預設為 允許 。
IP 通訊協定	選項為 IPv4、IPv6 及 IPv4_IPv6。預設為 IPv4_IPv6。若要存取此內容，請按一下 進階設定 圖示。
方向	選項為 傳入 、 傳出 及 傳入/傳出 。預設為 傳入/傳出 。此欄位是指從目的地物件的角度而言的流量方向。 傳入 表示僅會檢查流向物件的流量， 傳出 表示僅會檢查來自物件的流量，而 傳入/傳出 則表示會檢查這兩個方向的流量。若要存取此內容，請按一下 進階設定 圖示。
規則標記	已新增至規則的標記。若要存取此內容，請按一下 進階設定 圖示。
流量統計資料	顯示位元組、封包計數和工作階段的唯讀欄位。若要存取此內容，請按一下圖表圖示。

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

在管理程式模式中新增防火牆規則

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。
- 確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 **NSX Manager**。如果看不到**原則**和**管理程式**模式按鈕，請參閱**設定使用者介面設定**。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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**。

在管理程式模式中刪除防火牆規則

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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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**。

在管理程式模式中編輯預設分散式防火牆規則

您可以編輯預設防火牆設定，用來套用至不符合任何使用者定義防火牆規則的流量。

預設防火牆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**，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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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。
- 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**。

在管理程式模式中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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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**。

在管理程式模式中篩選防火牆規則

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。

必要條件

確認已在 NSX Manager 使用者介面中選取**管理程式**模式。請參閱第 1 章 [NSX Manager](#)。如果看不到**原則**和**管理程式**模式按鈕，請參閱[設定使用者介面設定](#)。

程序

- 1 選取**安全性 > 分散式防火牆**。
- 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。

當 NSX Manager 或全域管理程式變得無法運作，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。當應用裝置無法運作時，數據平面不會受到影響，但您無法進行組態變更。

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-T Data Center 版本的新應用裝置。

共有兩種備份方法：

- **週期性**：週期性備份會根據可自訂的排程執行，並確保您有最新的備份。您也可以針對組態變更觸發週期性備份。

當您設定週期性備份時，系統會每隔五分鐘備份詳細目錄。詳細目錄備份可提供最新的詳細目錄更新，例如，將傳輸節點新增或移除至還原。

不會針對全域管理程式收集詳細目錄備份。

- **手動**：您可以隨時手動執行備份。

手動備份不包含詳細目錄備份。

重要 請勿使用快照來備份 NSX-T Data Center 應用裝置。如需詳細資訊和指示，請參閱《NSX-T Data Center 安裝指南》中的[停用 NSX-T Data Center 應用裝置上的快照](#)。

本章節討論下列主題：

- [設定備份](#)
- [移除舊備份](#)
- [還原備份](#)
- [還原後的憑證管理](#)

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，或排程週期性備份。

必要條件

- 確認 SFTP 伺服器執行的是受支援的作業系統和 SFTP 軟體。下表顯示受支援且經過測試可用於備份的軟體，但其他軟體版本或許可以正常運作。

目前支援的作業系統	特別測試的版本	SFTP 軟體版本
CentOS	7.7	OpenSSH_7.4p1
RHEL	7.7	OpenSSH_7.4p1
Ubuntu	18.04	OpenSSH_7.6p1
Windows	Windows Server 2019 Standard	OpenSSH_for_Windows_7.7p1

- 使用下列命令以確認 SFTP 伺服器已準備好可供使用，並且正在執行 SSH 和 SFTP：
 - `$ ssh backup_user@sftp_server`
 - `$ sftp backup_user@sftp_server`
- 確定您要儲存備份的目錄路徑存在。您無法使用根目錄 (/)。
- 如果您有多個 NSX-T Data Center 部署，請務必針對儲存每個部署的備份使用不同的目錄。
- 您可以使用 NSX Manager 或全域管理程式應用裝置的 IP 位址或 FQDN 來進行備份：
 - 如果您使用 IP 位址進行備份和還原，請勿發佈應用裝置的 FQDN。
 - 如果您使用 FQDN 進行備份和還原，則必須在開始備份之前設定和發佈 FQDN。備份和還原僅支援小寫 FQDN。

使用此 API 來發佈 NSX Manager 或全域管理程式 FQDN。

範例要求：

```
PUT https://<nsx-mgr OR global-mgr>/api/v1/configs/management
{
  "publish_fqdns": true,
  "_revision": 0
}
```

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

程序

- 1 從瀏覽器以 admin 權限登入 NSX Manager 或全域管理程式，網址為 `https://<manager-ip-address>`。
- 2 選取 **系統 > 備份與還原**。
- 3 按一下 **SFTP 伺服器** 標籤下的 **編輯**，以設定 SFTP 伺服器。
- 4 輸入備份檔案伺服器的 IP 位址或 FQDN。
- 5 視需要變更預設連接埠。預設連接埠為 22。

6 通訊協定文字方塊已填入。

SFTP 是唯一支援的通訊協定。

7 在目錄路徑文字方塊中，輸入儲存備份的絕對目錄路徑。

該目錄必須已存在，且不可為根目錄 (/)。請避免在目錄名稱中使用路徑磁碟機代號或空格；因為不受支援。如果備份檔案伺服器是 Windows 機器，則您在指定目的地目錄時必須使用正斜線。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。

備份目錄的路徑只能包含下列字元：英數字元 (a-z、A-Z、0-9)、底線 (_)、加號和減號 (+ -)、波狀符號和百分比符號 (~ %)、正斜線 (/) 和句號 (.)。

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>。

8 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 FQDN、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。

9 您可以在稍後的步驟中按一下儲存後，將 SSH 指紋保留空白，並接受或拒絕伺服器提供的指紋。如有必要，您可以使用此 API 來擷取 SSH 指紋：

`POST /api/v1/cluster/backups?action=retrieve_ssh_fingerprint`。請注意，僅接受 SHA256 雜湊 ECDSA (256 位元) 主機金鑰作為指紋。

10 輸入複雜密碼。

重要 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。

11 按一下排程標籤下的編輯。

您可以排程週期性備份。您也可以針對組態變更觸發備份。您可以同時選取兩個選項來進行週期性備份。當您設定週期性備份時，如果詳細目錄中有任何變更，系統即會自動備份詳細目錄，例如新增或移除傳輸節點。此功能不適用於手動備份。

不會針對全域管理程式收集詳細目錄備份。

若要啟用週期性備份：

- a 按一下週期性備份切換。
- b 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時間。
- c 啟用偵測 NSX 組態變更選項，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。對於全域管理程式，如果偵測到資料庫中的任何變更 (例如新增或移除本機管理員或第 0 層閘道或 DFW 原則)，則此設定會觸發備份。

您可以指定用於偵測資料庫組態變更的時間間隔。有效範圍為 5 分鐘到 1,440 分鐘 (24 小時)。此選項可能會產生大量備份。請謹慎使用。

12 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**來手動開始備份。自動備份會依排程執行。

您會看到進行中備份的進度列。

手動或排程備份完成時，它會列在頁面的 [備份歷程記錄] 區段中。**上次備份狀態**標籤指示備份是否成功，並列出已備份應用裝置的時間戳記和節點與叢集詳細資料。如果備份失敗，您會看到錯誤訊息。

如果您需要查看可用備份的清單，但沒有 NSX Manager 或全域管理程式應用裝置的存取權，請參閱[列出可用的備份](#)以取得詳細資料。

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。

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，系統也會還原由 NSX Manager 或全域管理程式應用裝置所維護的組態。對於 NSX Manager，系統會協調在備份建立後對網狀架構所做的任何變更 (例如新增或刪除節點)。

備註 從備份還原時，系統不會保留 DNS 項目 (名稱伺服器和搜尋網域)。

您必須將備份還原至新的 NSX Manager 或全域管理程式應用裝置。

如果在建立備份時擁有 NSX Manager 應用裝置的叢集，則還原程序會先還原一個節點，然後提示您新增其他節點。您可以在還原程序期間或在第一個節點還原後新增另一個節點。

如果您擁有 全域管理程式 應用裝置的叢集，則只能使用還原程序還原一個節點。在第一個節點的還原完成後，您必須建立叢集。

重要 如果應用裝置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 ECDSA (256 位元) 主機金鑰作為指紋。
- 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-T Data Center 應用裝置的 IP 或 FQDN。
- 如果您已在執行備份時在 NSX Manager 上安裝 NSX Intelligence 應用裝置，則在還原備份之前，您必須先在新的 NSX Manager 上，上傳相同版本 NSX Intelligence 應用裝置的 OVA 檔案。如需安裝資訊，請參閱安裝和升級 VMware NSX Intelligence。

程序

- 1 如果應用裝置叢集中有任何您要還原的節點處於線上狀態，請關閉其電源。
- 2 安裝一個新的應用裝置節點，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 或全域管理程式節點。請勿將節點設定為發佈其 FQDN。
 - 如果要還原之備份的備份清單包含 FQDN，則必須使用此 FQDN 設定新的應用裝置節點並發佈此 FQDN。備份和還原僅支援小寫 FQDN。

備註 在設定並發佈 FQDN 之前，系統會在新部署的 NSX Manager 或全域管理程式 UI 中停用備份的還原按鈕。

使用此 API 來發佈 NSX Manager 或全域管理程式 FQDN。

範例要求：

```
PUT https://<nsx-mgr OR global-mgr>/api/v1/configs/management
{
  "publish_fqdns": true,
  "_revision": 0
}
```

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

此外，如果新管理程式節點的 IP 位址與原本的不同，則您必須使用新的 IP 位址更新管理程式節點的 DNS 伺服器正向和反向查閱項目。

在新的管理程式節點執行並上線後，您可以繼續進行還原。

- 3 從瀏覽器以 admin 權限登入 NSX Manager 或全域管理程式，網址為 `https://<manager-ip-address>`。
- 4 選取**系統 > 備份與還原**。
- 5 若要設定備份檔案伺服器，請按一下**編輯**。
如果您要執行還原，請勿設定自動備份。
- 6 輸入 IP 位址或 FQDN。
- 7 視需要變更連接埠號碼。
預設值為 22。
- 8 若要登入伺服器，請輸入使用者名稱和密碼。
- 9 在**目的地目錄**文字方塊中，輸入用來儲存備份的絕對目錄路徑。
備份目錄的路徑只能包含下列字元：英數字元 (a-z、A-Z、0-9)、底線 (_)、加號和減號 (+ -)、波狀符號和百分比符號 (~ %)、正斜線 (/) 和句號 (.)。
請避免在目錄名稱中使用路徑磁碟機代號或空格；因為不受支援。如果備份檔案伺服器是 Windows 機器，則您在指定目的地目錄時必須使用正斜線。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。
- 10 輸入用來加密備份資料的複雜密碼。
- 11 您可以在稍後的步驟中按一下**儲存**後，將 SSH 指紋保留空白，並接受或拒絕伺服器提供的指紋。如有必要，您可以使用此 API 來擷取 SSH 指紋：`POST /api/v1/cluster/backups?action=retrieve_ssh_fingerprint`。
- 12 按一下**儲存**。
- 13 選取備份。
- 14 按一下**還原**。
- 15 還原程序進行時，系統會於必要時提示您採取動作。

備註 如果您要還原 全域管理程式 應用裝置，則不會顯示下列步驟。還原第一個全域管理程式節點後，您必須手動將另一個節點加入以形成叢集。

- a 確認 CM/VC 連線：如果您要還原現有的計算管理程式，請確保它們已向新的 NSX Manager 節點登錄，並在還原程序期間可用。
- b 如果您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。如果在備份後建立了邏輯交換器或區段，則還原後將不會顯示邏輯交換器或區段。
- c 如果備份具有管理程式叢集的相關資訊，則系統會提示您新增其他節點。如果您決定不新增節點，您仍可以繼續進行還原，並在此節點完成還原後手動新增其他節點以形成叢集。
- d 如果有網狀架構節點未探索到新的管理程式節點，則會提供您其清單。

進度列會顯示還原作業的狀態，指出還原程序所在的步驟。在還原程序期間，管理程式應用裝置上的服務會重新啟動，且控制平面會變得無法使用，直到還原完成。

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。備份後所建立的任何區段都無法還原。

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。

您也可以透過選取記錄檔，判定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。

備註 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。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。

如果 vCenter Server 是在備份中使用自訂連接埠登錄，您必須手動開啟已還原管理程式應用裝置上的所有自訂連接埠。

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

如需指示，請參閱《NSX-T Data Center 安裝指南》。

- 17 如果您有其他已在步驟 1 中關閉電源的管理程式叢集虛擬機器，請在部署新的管理程式叢集後將其刪除。

列出可用的備份

備份檔案伺服器會儲存所有 NSX Manager 或全域管理程式節點的備份。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。

可在每個 NSX Manager 或全域管理程式應用裝置上的 `/var/vmware/nsx/file-store/get_backup_timestamps.sh` 中找到此指令碼。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，將此指令碼複製到非 NSX Manager 或全域管理程式的機器，以便在即使所有 NSX Manager 或全域管理程式節點都變得無法存取時，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 或全域管理程式節點，然後在該處執行指令碼。

您可以使用 `admin` 身分登入 NSX Manager 或全域管理程式並執行 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@server1/tmp/
admin@server'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 或全域管理程式節點的 IP 位址或 FQDN (如果 NSX Manager 或全域管理程式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:
10.10.10.20
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.10.10.20's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:13:30 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:01:52 10.10.10.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:00:33 10.10.10.77 35163642-6623-8f6d-7af0-52e03f16faed
```

還原後的憑證管理

在還原您的 NSX Manager 應用裝置後，系統中的憑證會進入不一致的狀態，而您必須更新所有自我簽署或 CA 簽署的憑證。

如需有關在 NSX-T Data Center 中所使用憑證類型的詳細資訊以及更新這些憑證的相關指示，請參閱第 19 章 [憑證](#)。

如果您使用的是 NSX-T Data Center 3.0.1 版或更新版本，則在還原第一個 NSX Manager 節點後，系統會在此還原的節點上套用憑證，不過，這些憑證不會套用至已安裝而形成已還原 NSX Manager 叢集的其他節點。

如果您使用的是 NSX-T Data Center 3.0.0 版，則沒有任何節點會套用原始憑證，您必須為每個節點手動還原憑證。

完成還原程序後，請遵循下列步驟來更新憑證：

- 1 如果您使用的是 NSX-T Data Center 3.0.1 版或更新版本，請在已安裝的兩個節點上更新 Tomcat 憑證，並加入已還原的 NSX Manager 節點，以形成三個節點的叢集。

如果您使用的是 NSX-T Data Center 3.0.0 版，請為所有 NSX Manager 節點 (包括已還原的節點) 更新 Tomcat 憑證。

使用下列 POST 要求，將節點還原為與已備份叢集相同的狀態。

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=<cert-id>
```

憑證識別碼對應於原始設定上所使用 Tomcat 憑證的識別碼。

2 執行下列 GET 要求並確認叢集穩定性以驗證憑證。

```
GET https://<nsx-mgr>/api/v1/trust-management/certificates
```

您可能有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：

- 檢視物件類別的使用量和容量
- 設定使用者介面設定
- 設定節點設定檔
- 查看組態變更的實現狀態
- 檢視網路拓撲
- 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
- 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
- 管理 Edge 虛擬機器應用裝置的資源保留
- 將 ESXi 主機傳輸節點新增至 vCenter Server 和從中移除
- 變更分散式路由器介面的 MAC 位址
- 設定應用裝置
- 新增授權金鑰並產生授權使用率報告
- 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
- 尋找遠端伺服器的 SSH 指紋
- 設定外部負載平衡器
- 進行 Proxy 設定
- 檢視容器相關的資訊

檢視物件類別的使用量和容量

您可以檢視管理程式物件各種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。

此功能僅在管理程式模式中可用。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 > 整合容量**，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。
- 目前詳細目錄 - 已成功建立或設定的物件數目。顯示以色彩編碼的長條，以指出使用量百分比。如果使用量低於容量臨界值下限，則色彩為綠色。如果使用量處於或高於容量臨界值下限，但低於容量臨界值上限，則色彩為橙色。如果使用量處於或高於容量臨界值上限，則色彩為紅色。
- 容量臨界值下限 - 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。預設值為 70%。
- 容量臨界值上限 - 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。預設值為 100%。

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：

- 已啟用全系統端點保護的主機
- 已啟用全系統端點保護的虛擬機器
- Active Directory 群組
- Active Directory 網域
- 分散式防火牆規則
- 全系統防火牆規則
- 全系統防火牆區段
- 分散式防火牆區段

詳細目錄容量頁面會顯示下列物件類別：

- 群組
- IP 集合
- 以 IP 集合為基礎的群組
- vSphere 叢集
- Hypervisor 主機

系統容量頁面會顯示下列物件類別：

- Edge 叢集
- 全系統 Edge 節點

設定使用者介面設定

NSX Manager Web 介面中有兩種可能的模式：原則和管理程式。您可以控制哪個模式為預設值，以及使用者是否可使用使用者介面模式按鈕在其之間切換。

如果存在，您可以使用**原則**和**管理程式**按鈕，在原則和管理程式模式之間切換。切換模式可控制哪些功能表項目可供您使用。



- 依預設，如果您的環境僅包含透過原則模式建立的物件，則您的使用者介面會處於原則模式，且您不會看到**原則**和**管理程式**按鈕。
- 依預設，如果您的環境包含透過管理程式模式建立的任何物件，您會在右上角看到**原則**和**管理程式**按鈕。

您可以使用使用者介面設定來修改這些預設值。

如需模式的相關資訊，請參閱第 1 章 [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 導覽至**系統 > 使用者介面設定**，然後按一下**編輯**。
- 3 修改使用者介面設定：**切換可見度**和**預設模式**。

切換可見度	說明
對所有使用者可見	如果存在管理程式模式物件，則會對所有使用者顯示模式按鈕。
只有具有企業管理員角色的使用者可看見	如果存在管理程式模式物件，則會對具有 企業管理員 角色的使用者顯示模式按鈕。
對所有使用者隱藏	即使存在管理程式模式物件，也對所有使用者隱藏模式按鈕。

預設模式可以設定為**原則**或**管理程式**。

設定節點設定檔

您可以進行時區、NTP 伺服器、SNMP 和 Syslog 伺服器這類設定的設定，以套用至所有 NSX Manager 和 Edge 節點。除了 NSX Manager 和 Edge 節點以外，SNMP 組態會套用至所有 KVM Hypervisor 上的 VMware SNMP 代理程式。

在此版本中，僅支援一個節點設定檔。此設定檔代表時區、NTP 伺服器、SNMP 組態和 Syslog 伺服器的集合。依預設，節點設定檔會套用至所有節點，除非該節點設定為不接受來自 NSX Manager 的此類組態。若要防止節點接受節點設定檔，請在該節點上使用 CLI 命令 `set node central-config disabled`。

程序

- 1 從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 > 設定檔**。
- 3 按一下**節點設定檔**索引標籤。
- 4 在**名稱**資料行中，按一下**所有 NSX 節點**。

- 5 按一下**編輯**來設定時區和 NTP 伺服器。
- 6 在 **Syslog 伺服器** 區段中，按一下**新增**以新增 Syslog 伺服器。
 - a 輸入 Syslog 伺服器的 FQDN 或 IP 位址。
 - b 指定連接埠號碼。
 - c 選取通訊協定。
可用的通訊協定包括 **TCP**、**UDP** 和 **LI** (Log Insight)。
 - d 選取記錄層級。
可用層級包括**緊急**、**警示**、**嚴重**、**錯誤**、**警告**、**通知**、**資訊**和**偵錯**。
- 7 在 **SNMP 輪詢** 區段的 **v2c** 下，按一下**新增**以新增 SNMPv2c 社群。
 - a 輸入社群的名稱。
 - b 輸入**社群字串**值。
此值可用於驗證。
- 8 在 **SNMP 輪詢** 區段的 **v3** 下，按一下**新增**以新增 SNMPv3 使用者。
 - a 輸入使用者名稱。
 - b 輸入驗證密碼。
您可以按一下右側的圖示，以顯示或隱藏密碼。
 - c 輸入私人密碼。
您可以按一下右側的圖示，以顯示或隱藏密碼。
- 9 在 **SNMP 設陷** 區段的 **v2c** 下，按一下**新增**以新增 SNMPv2c 設陷組態。
 - a 輸入 FQDN 或 IP 位址。
 - b 指定連接埠號碼。
 - c 輸入社群的名稱。
 - d 輸入**社群字串**值。
此值可用於驗證。
- 10 在 **SNMP 設陷** 區段的 **v3** 下，按一下**新增**以新增 SNMPv3 設陷組態。
 - a 輸入 FQDN 或 IP 位址。
 - b 指定連接埠號碼。
 - c 輸入使用者名稱。

查看組態變更的實現狀態

進行組態變更後，NSX Manager 通常會傳送要求至其他元件來實作變更。對於某些第 3 層實體，如果您使用 API 進行組態變更，您可以追蹤要求的狀態來查看變更是否成功實作。

您起始的組態變更稱為所需狀態。實作變更的結果稱為實現狀態。如果 NSX Manager 成功實作變更，實現狀態將與所需狀態相同。如果發生錯誤，實現狀態將與所需狀態不同。

對於某些第 3 層實體，當您呼叫 API 來進行組態變更時，回應會包括參數 `request_id`。您可以使用參數 `request_id` 和 `entity_id` 進行 API 呼叫來瞭解要求的狀態。

此功能支援下列實體和 API：

```

EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement

AdvertiseRouteList
  PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

NatRule
  POST /logical-routers/<logical-router-id>/nat/rules
  PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>

```

```
DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>
```

DhcpRelayService

```
POST /dhcp/relays
```

```
PUT /dhcp/relays/<relay-id>
```

```
DELETE /dhcp/relays/<relay-id>
```

DhcpRelayProfile

```
POST /dhcp/relay-profiles
```

```
PUT /dhcp/relay-profiles/<relay-profile-id>
```

```
DELETE /dhcp/relay-profiles/<relay-profile-id>
```

StaticHopBfdPeer

```
POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
```

```
PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

IPPrefixList

```
POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
```

```
PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

RouteMap

```
POST /logical-routers/<logical-router-id>/routing/route-maps
```

```
PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

```
DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

RedistributionConfig

```
PUT /logical-routers/<logical-router-id>/routing/redistribution
```

RedistributionRuleList

```
PUT /logical-routers/<logical-router-id>/routing/redistribution/rules
```

BfdConfig

```
PUT /logical-routers/<logical-router-id>/routing/bfd-config
```

MplsConfig

```
PUT /logical-routers/<logical-router-id>/routing/mpls
```

RoutingGlobalConfig

```
PUT /logical-routers/<logical-router-id>/routing
```

IPSecVPNIKEProfile

```
POST /vpn/ipsec/ike-profiles
```

```
PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
```

```
DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>
```

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 Entites - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of
logical router but if the logical router itself is deleted then the state will be unknown and
it will return the common entity not found error.

```

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API to get the realization state

Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-id>

Response - An instance of LogicalServiceRouterClusterState which will inherit ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile

Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>

Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint / IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession

Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>

Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If the session is deleted then the state will be unknown and it will return the common entity not found error. When IPSecVPNService is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

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》。

檢視網路拓撲

檢視 NSX-T Data Center 環境的網路拓撲，以取得網路中邏輯實體的概觀。驗證網路組態或疑難排解錯誤時，網路拓撲的圖形表示非常有用。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 <https://<nrx-manager-ip-address>>。
- 2 選取**網路 > 網路拓撲**。
- 3 導覽網路拓撲以查看詳細資訊：
 - 放大以檢視更多詳細資料。

- 指向物件即可檢視其在網路中的邏輯路徑。
- 按一下物件以顯示該物件的詳細資料面板。
- 在工具列上按一下**匯出**，將拓撲儲存至 PDF 檔案。
- 套用篩選器以將焦點集中在特定物件上。如需有關篩選器的更多詳細資料，請參閱[依物件屬性篩選](#)。

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 建立角色和使用者並提供此使用者的認證。此角色必須具有下列 vCenter Server 權限：

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Configuration.NetworkConfiguration
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。

- 不支援在 vCenter Server 上使用 HTTP 或 HTTPS 之類的自訂連接埠。

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 **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。
FQDN 或 IP 位址	輸入 vCenter Server 的 FQDN 或 IP 位址。
類型	預設的計算管理程式類型設為 vCenter Server。
反向 Proxy 的 HTTPS 連接埠	預設連接埠為 443。如果使用其他連接埠，請確認已在所有 NSX Manager 應用裝置上開啟該連接埠。 設定反向 Proxy 連接埠，以在 NSX-T 中登錄計算管理程式。
使用者名稱和密碼	輸入 vCenter Server 登入認證。
SHA-256 指紋	輸入 vCenter Server SHA-256 指紋演算法值。
啟用信任	僅在 vCenter Server 7.0 及更新版本上支援。 啟用此欄位來信任計算管理程式以進行驗證。

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。

備註 如果計算管理程式的 FQDN、IP 或指紋在登錄後發生變更，請編輯計算管理程式，並輸入新值。

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 已向另一個 NSX Manager 登錄的錯誤。

備註 成功新增 vCenter Server (VC) 計算管理程式後，如果成功執行下列任一動作，則無法將其移除：

- 傳輸節點是使用相依於 VC 的 VDS 來準備。
- 服務虛擬機器是使用 NSX 服務插入在 VC 中的主機或叢集中部署。
- 您可以使用 NSX Manager UI，在 VC 的主機上或叢集中部署 Edge 虛擬機器、NSX Intelligence 虛擬機器或 NSX Manager 節點。

如果您嘗試執行這些動作中的任何一項，且發生錯誤 (例如，安裝失敗)，則可以在未成功執行以上所列任何動作的情況下移除 VC。

如果您已成功使用相依於 VC 的 VDS 來準備任何傳輸節點或已部署任何虛擬機器，則可以在完成下列作業後移除 VC：

- 取消準備所有傳輸節點。如果解除安裝傳輸節點失敗，您必須強制刪除傳輸節點。
- 取消部署所有服務虛擬機器、任何 NSX Intelligence 虛擬機器、所有 NSX Edge 虛擬機器以及所有 NSX Manager 節點。取消部署必須成功或處於失敗狀態。
- 如果 NSX Manager 叢集包含從 VC (手動方法) 部署的節點以及從 NSX Manager UI 部署的節點，且您必須取消部署手動部署的節點，則無法移除 VC。若要成功移除 VC，請確保從 VC 重新部署 NSX Manager 節點。

此限制適用於 NSX-T Data Center 3.0 的全新安裝和升級。

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。

您可以登錄整個 AD (Active Directory) 網域以供 IDFW (身分識別防火牆) 使用，也可以同步大型網域的子集。登錄網域後，NSX 會同步 IDFW 所需的所有 AD 資料。

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 > 身分識別防火牆 AD > 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。

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 > 身分識別防火牆 AD > 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 網域的唯一讀存取權。

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。

備註 請勿在使用分散式負載平衡器的環境中啟用分散式入侵偵測服務 (IDS)。NSX-T Data Center 不支援搭配分散式負載平衡器使用 IDS。

若要啟用選擇性同步，請使用已啟用選擇性同步的網域建立/更新 API，以及所選組織單位 (OU) 的清單。啟用選擇性同步時，NSX-T 僅會同步位於所選 OU 內的 AD 資料。在選擇性差異同步期間，只會更新位於所選 OU 內且在上次同步後已建立或變更的 Active Directory 資料。如果從選取的 OU 中移除任何目錄群組，則不會在選擇性差異同步期間更新這些群組。這些群組會在所有目錄群組更新時，於完整同步期間進行更新。如需詳細資訊，請參閱《NSX-T Data Center API 指南》。

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 > 身分識別防火牆 AD > 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。

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	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5	5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
CONTROLLER				06fd0574-69c0-432e-a8af-53d140dbef8f	
CLUSTER_BOOT_MANAGER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	da8d535e-7a0c-4dd8-8919-d88bdde006b8	
DATASTORE	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
MANAGER	10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5	eb5e8922-23bd-4c3a-ae22-d13d9195a6bc	
POLICY	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	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	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5	3757f155-8a5d-4b53-828f-d67041d5a210	
CONTROLLER				7b1c9952-8738-4900-b68b-ca862aa4f6a9	
CLUSTER_BOOT_MANAGER	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	b5e12db1-5e0d-4e33-a571-6ba258dceb2e	
DATASTORE	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	bee1f629-4e23-4ab8-8083-9e0f0bb83178	
MANAGER	10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5	45ccd6e3-1497-4334-944c-e6bbcd5c723e	
POLICY	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	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	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5	bce3cc4c-7d60-45e2-aa7b-cdc75e445a14	
CONTROLLER				ced46f5c-9e52-4b31-a1cb-b3dead991c71	
CLUSTER_BOOT_MANAGER	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	88b70d31-3428-4ccc-ab57-55859f45030c	
	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		

			fb4aec3c-cae3-4386-b5b9-c0b99b7d9048
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5	
			82b07440-3ff6-4f67-a1c9-e9327d1686ad
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	
			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

```

更新 NSX Manager 叢集的 API 服務組態

您可以修改 NSX Manager 叢集的 API 服務內容，例如 TLS 通訊協定版本與加密套件等。

下列程序說明執行 NSX API 服務呼叫以停用 TLS 1.1 通訊協定，以及在 API 服務組態中啟用或停用加密套件的工作流程。

如需關於 API 結構描述、範例要求、範例回應，以及 NSX API 服務之錯誤訊息的詳細資訊，您必須閱讀《NSX-T Data Center API 指南》。

程序

- 1 執行下列 GET API 以讀取 NSX API 服務的組態：

```
GET https://<NSX-Manager-IP>/api/v1/cluster/api-service
```

API 回應會包含加密套件和 TLS 通訊協定的清單。

2 停用 TLS 1.1 通訊協定。

- a 將 TLSv1.1 設為 `enabled = false`。
- b 執行下列 PUT API，將變更傳送至 NSX API 伺服器：

```
PUT https://<NSX-Manager-IP>/api/v1/cluster/api-service
```

3 啟用或停用加密套件。

- a 根據您的需求，將一或多個加密名稱設定為 `enabled = false` 或 `enabled = true`。
- b 執行下列 PUT API，將變更傳送至 NSX API 伺服器：

```
PUT https://<NSX-Manager-IP>/api/v1/cluster/api-service
```

結果

每個 NSX Manager 節點上的 API 服務在使用 API 更新後，都會重新啟動。從 API 呼叫完成到新組態生效，最多可能會有一分鐘的延遲。API 服務組態中的變更會套用至 NSX Manager 叢集中的所有節點。

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

- 1 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。
- 2 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。

不建議使用案例 C，因為它會暫時減少 NSX Manager 的數量，且因在 IP 位址變更期間失去兩個作用中管理程式的其中一個，而對 NSX-T Data Center 作業造成影響。在下列情況下就會發生此案例：額外的虛擬 RAM、CPU 和磁碟無法使用，且需要變更 IP 位址。

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。

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。

結果

如果執行的 NSX-T 版本低於 3.1.3，則在取代 NSX Edge 傳輸節點之後，您可能會看到警示：「所有 BGP/BFD 工作階段已關閉。」若要解決此問題，請遵循知識庫文章 <https://kb.vmware.com/s/article/83983> 中的因應措施指示。

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"
}
```

結果

如果執行的 NSX-T 版本低於 3.1.3，則在取代 NSX Edge 傳輸節點之後，您可能會看到警示：「所有 BGP/BFD 工作階段已關閉。」若要解決此問題，請遵循知識庫文章 <https://kb.vmware.com/s/article/83983> 中的因應措施指示。

管理 Edge 虛擬機器應用裝置的資源保留

NSX-T Data Center 使用 vSphere 資源配置來保留 NSX Edge 應用裝置的資源。您可以調整為 NSX Edge 保留的 CPU 和記憶體資源，以確保在 NSX Edge 上資源的使用達到最佳狀況。

若要獲得最佳效能，NSX Edge 虛擬機器應用裝置必須獲指派 100% 的可用資源。如果您自訂配置給 NSX Edge 虛擬機器的資源，請之後將配置改回 100%，以獲得最大效能。

對於自動部署的 NSX Edge 應用裝置，您可以透過 NSX Manager 變更資源配置。但是，如果從 vSphere 部署 NSX Edge 應用裝置，則只能從 vSphere 管理該 NSX Edge 虛擬機器的資源保留。

根據在您的環境中部署的 Edge 虛擬機器的資源需求，有兩個方式可管理保留：

- 指派的預設值會提供 100% 的資源保留。
- 指派的自訂值會提供 0-100% 的資源保留。

預設保留

假設 NSX Edge 設定為高優先順序。優先順序重要性的層級會定義指派給 NSX Edge 的 vCPU 共用和記憶體數目。若要指派自訂值，您可以變更指派給 NSX Edge 的相對優先順序。

設定為一般優先順序的不同機器尺寸的資源限制：

機器尺寸	vCPU 數目	vCPU 共用	RAM (GB)
小	2	2000	4
中	4	4000	8
大	8	8000	32
特大	16	16000	64

您可以透過考慮兩個參數來調整 NSX Edge 應用裝置的保留：

- 指派給虛擬機器的相對優先順序
- 為虛擬機器機器尺寸預先指派的資源限制

自訂保留

為 NSX Edge 應用裝置指派相對優先順序。您可以變更 NSX Edge 應用裝置的相對重要性，以指派下列資源需求：

相對重要性	CPU 共用 (每個 vCPU 的共用)	記憶體 (每 MB 設定的虛擬機器記憶體共用)
超高	4000	40
高	2000	20
一般	1000	10
低	500	5

例如，對部署在中等機器尺寸的 NSX Edge 應用裝置的高相對重要性，會指派下列 vCPU 和記憶體共用：

- $4 \text{ (vCPU)} \times 8000 \text{ (vCPU 共用值)} = 32000 \text{ 個 vCPU 共用}$
- $20 \text{ (GB RAM)} \times 1000 = 20000 \text{ 個記憶體共用}$

備註 以 MHz 指派 CPU 值以保證 NSX Edge 虛擬機器的已配置 CPU 週期之前，請確保相對重要性設為低。如果相對重要性設為一般或高，且自訂 CPU 值以 MHz 為單位，則虛擬機器部署可能會因資源限制而面臨問題。

調整 NSX Edge 應用裝置的資源保留

您可以調整 NSX Edge 虛擬機器應用裝置上的資源保留。依預設，會將 100% 的資源配置給 NSX Edge 虛擬機器。變更資源保留的彈性，可讓您無需將額外的容量新增至 vCenter Server，且不需減少其他非 Edge 虛擬機器上目前的保留。

必要條件

- 確認叢集有足夠的容量來避免失敗。

程序

- 1 從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 > 節點 > Edge 傳輸節點**。
- 3 選取 NSX Edge 傳輸節點。
- 4 按一下 **動作 > 變更 Edge 虛擬機器資源保留**。
- 5 在 **變更 Edge 虛擬機器資源保留** 視窗中，您可以自訂套用至 Edge 傳輸節點的現有資源配置。

動作	說明
CPU 保留優先順序	低 - 2000 個共用 一般 - 4000 個共用 高 - 8000 個共用 超高 - 10000 個共用
記憶體保留 (%)	保留百分比是相對於機器尺寸中預先定義的值。 100 表示為 NSX Edge 虛擬機器保留了 100% 的記憶體。 如果輸入 50，則表示將 50% 的記憶體指派給 Edge 傳輸節點。
CPU 保留 (MHz)	輸入 CPU 保留 (MHz)。 MHz 的數量上限等於 vCPU 的數目乘以實體 CPU 核心的一般 CPU 作業速率。 備註 如果輸入的 MHz 值超過實體 CPU 核心的最大 CPU 容量，即使已接受配置，NSX Edge 虛擬機器也可能無法啟動。

- 6 按一下 **儲存**。

如果對資源保留所做的變更未生效，您可能需要從 vCenter Server 中將 NSX Edge 虛擬機器重新開機。

當 NSX Edge 叢集已關閉 vSphere HA 時，ESXi 主機上自動啟動的 NSX Edge 虛擬機器應用裝置會重新開機。如需 vSphere HA 的詳細資料，請參閱 vSphere 說明文件。

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。

變更分散式路由器介面的 MAC 位址

NSX-T 和 NSX for vSphere 設定中的所有邏輯路由器介面都具有相同的 MAC 位址 (02:50:56:56:44:52)。從 NSX-T Data Center 3.0.2 開始，您可以在 NSX-T 中變更此位址，以避免在將虛擬機器從 NSX for vSphere 設定移轉至 NSX-T 設定時發生問題。

變更 MAC 位址涉及進行兩次 API 呼叫。

如果您尚未建立任何傳輸節點，請進行下列 GET API 呼叫。例如：

```
GET https://10.40.79.126/api/v1/global-configs/RoutingGlobalConfig
```

Response:

```
{
  "l3_forwarding_mode" : "IPV4_ONLY",
  "logical_uplink_mtu" : 1500,
  "vdr_mac" : "02:50:56:56:44:77",
  "vdr_mac_nested" : "02:50:56:56:44:52",
  "allow_changing_vdr_mac_in_use" : true,
  "resource_type" : "RoutingGlobalConfig",
  "id" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "display_name" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "_create_user" : "system",
  "_create_time" : 1595313890595,
```

```

    "_last_modified_user" : "admin",
    "_last_modified_time" : 1595465694142,
    "_system_owned" : false,
    "_protection" : "NOT_PROTECTED",
    "_revision" : 14
  }

```

接受呼叫的回應、變更 `vdr_mac` 值，然後使用它進行下列 PUT API 呼叫。例如：

```

PUT https://10.40.79.126/api/v1/global-configs/RoutingGlobalConfig
{
  "l3_forwarding_mode" : "IPV4_ONLY",
  "logical_uplink_mtu" : 1500,
  "vdr_mac" : "02:50:56:56:44:99",
  "vdr_mac_nested" : "02:50:56:56:44:53",
  "allow_changing_vdr_mac_in_use" : true,
  "resource_type" : "RoutingGlobalConfig",
  "id" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "display_name" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "_create_user" : "system",
  "_create_time" : 1595313890595,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1595465694142,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 14
}

```

Response:

```

{
  "l3_forwarding_mode" : "IPV4_ONLY",
  "logical_uplink_mtu" : 1500,
  "vdr_mac" : "02:50:56:56:44:99",
  "vdr_mac_nested" : "02:50:56:56:44:53",
  "allow_changing_vdr_mac_in_use" : true,
  "resource_type" : "RoutingGlobalConfig",
  "id" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "display_name" : "49b261fe-f4e4-46ad-958c-da9cb4271e32",
  "_create_user" : "system",
  "_create_time" : 1595313890595,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1595466163148,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 15
}

```

如果您已建立傳輸節點，請發出相同的 GET 和 PUT API 呼叫，但對於 PUT 呼叫，請將參數 `allow_changing_vdr_mac_in_use` 設為 `true`。

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 22-1. 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

備註 為所有應用裝置設定 NTP 伺服器的建議方法是設定節點設定檔。請參閱[設定節點設定檔](#)。如果您在應用裝置上個別設定 NTP 伺服器，請確保在所有應用裝置上設定相同的 NTP 伺服器。

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。

以下是可用的一般授權類型：

- 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 Data Center 評估
- NSX for vSphere - Standard
- NSX for vSphere - Advanced
- NSX for vSphere - Enterprise
- NSX for vShield Endpoint

以下是可用的 Limited Export 授權類型：

- 每個處理器的 VMware NSX Enterprise (Limited Export)
- 每個處理器的 NSX Data Center Advanced (適用於 Limited Export)
- NSX Data Center 評估
- NSX for vShield Endpoint

一般和 Limited Export 授權的附加元件授權類型：

- NSX 分散式威脅防護 (包含分散式 IDS)

只有在 NSX Data Center Advanced 或 NSX Data Center Enterprise Plus 授權存在的情況下，才能新增此授權。而且，在刪除此附加程式授權之前，您無法刪除 NSX Data Center Advanced 或 NSX Data Center Enterprise Plus 授權。

附註：對於 Limited Export 發行版本，您僅能在存在每個處理器的 VMware NSX Enterprise (Limited Export) 或每個處理器的 NSX Data Center Advanced (適用於 Limited Export) 授權的情況下新增此授權。而且，在刪除此附加程式授權之前，您無法刪除每個處理器的 VMware NSX Enterprise (Limited Export) 或 NSX Data Center Advanced (適用於 Limited Export) 授權。

安裝 NSX Manager 時，預設授權是 NSX for vShield Endpoint。此授權永遠不會到期，但有某些限制。您無法建立或更新下列物件：

- 第 0 層和第 1 層邏輯路由器
- 第 0 層和第 1 層閘道
- 邏輯交換器
- 第 2 層區段 (附註：您可以建立和更新服務區段。)
- 分散式防火牆
- VPN
- NAT
- 負載平衡器
- 服務插入
- NSX Intelligence

如果是從舊版升級，則預設 vShield Endpoint 授權和先前的預設 NSX Data Center 評估將可供使用。請注意下列事項：

- 您無法刪除預設的 vShield Endpoint 授權金鑰。
- 您可以刪除先前的預設 NSX Data Center 評估授權金鑰。
- 如果您新增新的 vShield Endpoint 授權，則預設 vShield Endpoint 授權將會隱藏。如果您移除新的 vShield Endpoint 授權，則預設 vShield Endpoint 授權將會再次可用。

- 如果您新增 NSX Data Center 評估授權，則預設 NSX Data Center 評估授權 (如果由於升級而存在) 將會永久刪除。如果您移除新的 NSX Data Center 評估授權，則不會有任何評估授權。

備註 關於評估授權：

如果您安裝 NSX Data Center 評估授權，它將在 60 天內有效。

請注意下列事項：

- 您僅有 NSX for vShield Endpoint 授權和 NSX Data Center 評估授權。
 - 如果 NSX Data Center 評估授權有效，將會使用該授權。
 - 如果 NSX Data Center 評估授權已到期，則會使用 NSX for vShield Endpoint 授權。(強制執行將會生效。)
 - 您有 NSX for vShield Endpoint 授權、NSX Data Center 評估授權和其他授權。
 - 如果 NSX Data Center 評估授權有效，則會使用該授權和其他授權。
 - 如果 NSX Data Center 評估授權已到期，則將使用其他授權。
-

如果授權已到期或將在 60 天內到期，則每次登入時都會產生警示。您可以透過前往 **首頁 > 警示** 來檢視警示。

如果您僅有 NSX for vShield Endpoint 授權，則在您登入後，資訊橫幅訊息會告知您授權有某些限制 (請參閱以上)。如果您的授權已到期或即將到期，則在您登入後，會顯示警告橫幅訊息告知您。

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

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 `https://<nsx-manager-ip-address>`。
- 2 選取 **系統 > 授權 > 新增**。
- 3 輸入授權金鑰。
- 4 若要產生授權使用率報告，請選取 **匯出 > 授權使用率報告**。

CSV 報告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
- 分散式防火牆
- 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身分識別防火牆
- 服務插入
- 身分識別防火牆

- 增強型客體自我檢查
- 微分割規劃 (L4) (僅限 CPU、核心、虛擬機器和並行使用者資訊)
- 聯盟 (僅限 CPU、核心、虛擬機器和並行使用者資訊)
- 分散式 IDS (僅限 CPU 資訊)

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
-

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](#)。

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](#)。

與 NSX Controller 之南向和北向連線的相關詳細資料：

- 對於 NSX Manager 應用裝置和其他節點中控制器元件之間的南向連線，X509 憑證型驗證會與 FIPS 140-2 驗證的 OpenSSL 演算法搭配使用。連線支援使用 AES 128 位元、256 位元或 384 位元加密金鑰的 TLS 1.2 型加密套件。
- NSX Manager 應用裝置的控制器功能和管理功能會在相同的節點上執行。因此，NSX Manager 應用裝置的控制器與管理程式元件之間沒有任何北向跨節點通訊。

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 22-2. 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 22-3. 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。

表 22-3. 符合性報告代碼 (續)

代碼	說明	符合性狀態來源	修復
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。	<p>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。</p> <p>此狀態會影響下列組態：</p> <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 。
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。	<p>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。</p> <p>此狀態會影響下列組態：</p> <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。	<p>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。</p> <p>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。</p>	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。	<p>如果已停用負載平衡器 FIPS 全域設定，則會報告此錯誤。</p> <p>此狀態會影響所有負載平衡器服務。</p>	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。	<p>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。</p> <p>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。</p>	<p>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。</p> <p>備註 如果基礎結構是虛擬的，您將無法取得真實熵。</p>

表 22-3. 符合性報告代碼 (續)

代碼	說明	符合性狀態來源	修復
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。請參閱第 19 章憑證。

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。

若要讓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
}

```

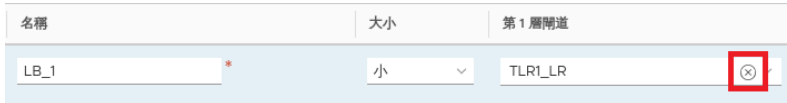
回應本文範例：

```
{
  "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。



- 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

- 1 從瀏覽器以本機 admin 使用者身分登入 NSX Manager，網址為 `https://nsx-manager-ip-address/login.jsp?local=true`。
- 2 選取**系統 > 支援服務包**。
- 3 選取目標節點。
 可用的節點類型包含**管理節點、Edge、主機和公有雲端閘道**。
- 4 (選擇性) 指定記錄存留期 (以天為單位) 以排除超過指定天數的記錄。
- 5 (選擇性) 切換表示要包含或排除核心檔案和稽核記錄的交換器。

備註 核心檔案和稽核記錄可能包含機密資訊，例如密碼或加密金鑰。

- 6 (選擇性) 選取將服務包上傳至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
nsx-audit-write.log	NSX 稽核寫入記錄
nsx-audit.log	NSX 稽核記錄
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 `local16`，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。您可以設定外部記錄伺服器來接收記錄訊息。您也可以使用 `API /api/v1/administration/audit-logs` 來存取稽核記錄。檔案 `nsx-audit.log` 包含 `structured-data` 欄位為 `audit="true"` 的 Syslog 訊息。檔案 `nsx-audit-write.log` 包含 `structured-data` 欄位中具有 `audit="true"` 與 `update="true"` 的 Syslog 訊息。

每個 Syslog 和稽核記錄訊息都包含由 NTP 伺服器 (如果已設定) 或系統時鐘所產生的時間戳記。稽核記錄訊息的範例：

```
<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"
```

API 呼叫可以來自 NSX Manager、原則 API 用戶端或 NSX 節點。所有 API 呼叫會受到驗證和授權的約束，並將產生稽核記錄。此記錄依預設為啟用，且無法停用。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>`。

來自原則或管理程式 API 呼叫的稽核記錄訊息將具有下列其他欄位。請注意，節點 API (NAPI) 和 CLI 稽核記錄將不會有這些欄位。

- `update` 旗標，顯示 API 作業是讀取 (GET) 還是寫入 (PUT/POST/DELETE/...) 運算。
- `operation name` 欄位，會顯示 API 作業名稱。
- `operation status` 欄位，會顯示 API 作業是否成功或失敗。
- `new value` 欄位，會顯示 API 要求的所有參數值。

NSX-T 沒有特殊權限模式的概念。會稽核來自所有來源和使用者的 API 呼叫。

登入和登出 Syslog 訊息的範例，顯示成功的登入、失敗的登入，以及來自 2 個不同裝置的登入 (請注意不同的 IP 位址)：

```
2020-07-07T16:33:20.339Z svc.nsxmanager NSX 1513 SYSTEM [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" subcomp="http"] UserName="admin@10.166.61.56",
ModuleName="ACCESS_CONTROL", Operation="LOGIN", Operation status="success"

2020-07-07T16:33:58.779Z svc.nsxmanager NSX 1513 SYSTEM [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" subcomp="http"] UserName="admin", ModuleName="ACCESS_CONTROL",
Operation="LOGOUT", Operation status="success"

2020-07-07T16:50:21.301Z svc.nsxmanager NSX 1513 SYSTEM [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" subcomp="http"] UserName="admin@10.166.61.80",
ModuleName="ACCESS_CONTROL", Operation="LOGIN", Operation status="success"

2020-07-07T16:43:20.339Z svc.nsxmanager NSX 1513 SYSTEM [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" subcomp="http"] UserName="admin@10.166.61.56",
ModuleName="ACCESS_CONTROL", Operation="LOGIN", Operation status="failure"
```

原則 API 呼叫的 Syslog 訊息範例：

```
<182>1 2020-07-06T18:09:14.210Z svc.nsxmanager NSX 2326 FABRIC [nsx@6876 audit="true"
comp="nsx-manager" entId="68d5a9d0-4691-4c9c-94ed-64fd1c96150f" level="INFO" reqId="4c2335aa-
c973-4f74-983f-331a4f7041ca" subcomp="manager" update="true" username="admin"]
UserName="admin", ModuleName="TransportZone", Operation="CreateTransportZone", Operation
status="success", New
value=[{"transport_type":"OVERLAY","host_switch_name":"nsxvswitch","host_switch_mode":"STANDAR
D","nested_nsx":false,"is_default":false,"display_name":"1-
transportzone-1307","_protection":"UNKNOWN"}]
```

CLI 存取的 Syslog 訊息範例：

```
2020-07-07T16:36:41.783Z svc.nsxmanager NSX 21018 - [nsx@6876 comp="nsx-manager"
subcomp="cli" username="admin" level="INFO"] NSX CLI started (Manager, Policy, Controller)
for user: admin
2020-07-07T16:36:53.469Z svc.nsxmanager NSX 21018 - [nsx@6876 comp="nsx-manager"
subcomp="cli" username="admin" level="INFO"] NSX CLI stopped for user: admin
```

當使用者執行 CLI 命令時，Syslog 訊息的範例 (在此範例中，set user admin password-expiration 100)：

```
<182>1 2020-07-22T20:51:49.017Z manager2 NSX 1864 - [nsx@6876 comp="nsx-manager"
subcomp="cli" username="admin" level="INFO" audit="true"] CMD: set user admin password-
expiration 100 (duration: 2.185s), Operation status: CMD_EXECUTED
```

NAPI 呼叫的 Syslog 訊息範例：

```
<182>1 2020-07-21T21:01:38.803Z manager2 NSX 4690 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] admin 'GET /api/v1/node/
services/syslog/exporters' 200 731 "" "PostmanRuntime/7.26.1" 0.004588
```

CLI 命令的 Syslog 訊息範例：

```
<182>1 2020-07-21T20:54:40.018Z manager2 NSX 16915 - [nsx@6876 comp="nsx-manager"
subcomp="cli" username="admin" level="INFO" audit="true"] CMD: set logging-server 1.1.1.1
proto udp level info (duration: 4.356s), Operation status: CMD_EXECUTED
```

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 and 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@caser:~/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@caser:~/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-----
< MIICIJANBgkqhkiG9w0BAQEFAAOCAg8AMIICGkCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCWd2d2rZ09cUZVl0P9
< kIYBb5RMFC7Z1OUtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHukcWWk3eU6Oy4OiyW6jYuXG7hZYlly

```

```
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV918d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< 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
< EcOKX1FFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthtUP8khCWd2d2r209cUZV10P9
< kIYBb5RMFC7Z10UtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3Pp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf1lDZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV918d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX216u5Jl4/X/pUDI/YHmIf06bsZ1r/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KwVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DdfyUH1L
> W0NUN9YdN+fa12Uf021iuDqVy9V8AH3ON6fu+QCA8nt71ZkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe00e
> HCdxGmlrUtMqxIItJahEsqvMufyqNYecVscyXLHPelizKCsQfy8c08LnznG8Vadc
> YILSn3uYGZap6aF1SgVxsvZicwv1YnssmgE13Af0nScmfM96k9h5joHVEkWK608v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektr8HdMHQit5uvmMRY3S5zow
> FtvfSDfWxxKyTy6GBRrp+8F+Jq9lyGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmVveinDhU35IqWEXHAWcCAwEAAQ==
```

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 22-4. 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 22-4. 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。

防火牆稽核記錄訊息

已稽核防火牆組態變更。以下是與這些變更相關的稽核記錄訊息範例。

原則模式中的分散式防火牆變更

使用規則 (Rule1_1) 新增防火牆區段 (SecurityPolicy-1)：

```
<182>1 2020-08-11T21:58:50.319Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e" splitId="a5mxlu78"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="DfwSecurityPolicy", Operation="PatchSecurityPolicyForDomain", Operation
status="success", Old
value=[{"precedence":10,"category":"Application","resource_type":"CommunicationMap","id":"Secu
rityPolicy-1","display_name":"SecurityPolicy-1","path":"/infra/domains/default/security-
policies/SecurityPolicy-1","relative_path":"SecurityPolicy-1","parent_path":"/infra/domains/
default","unique_id":"895eeac5-641b-4306-be7f-
a43fdd969ee5","marked_for_delete":false,"overridden":false,"_create_user":"admin","_create_tim
e":1597183130247,"_last_modified_user":"admin","_last_modified_time":1597183130247,"_system_ow
ned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["default"
"SecurityPolicy-1"
{"resource_type":"SecurityPolicy","id":"SecurityPolicy-1","display_name":"SecurityPolicy-1","p
```

```

ath":"/infra/domains/default/security-policies/SecurityPolicy-1","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1","path":

<182>1 2020-08-11T21:58:50.320Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e" splitId="a5mXlu78"
splitIndex="2 of 2" subcomp="policy" update="true"] "/infra/domains/default/security-policies/
SecurityPolicy-1/rules/
Rule1_1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_excluded":
false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN
"},"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protectio
n":"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"category":"A
pplication","stateful":true,"locked":false,"scope":["ANY"],"_protection":"UNKNOWN"}]

<182>1 2020-08-11T21:58:50.404Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="Rule1_1" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e"
splitId="E993J2LF" splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="DfwSecurityPolicy", Operation="UpdateSecurityRule", Operation status="success",
Old value={"sequence_number":10,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"Rule1
_1","display_name":"Rule1_1","path":"/infra/domains/default/security-policies/
SecurityPolicy-1/rules/Rule1_1","relative_path":"Rule1_1","parent_path":"/infra/domains/
default/security-policies/
SecurityPolicy-1","unique_id":"2024","marked_for_delete":false,"overridden":false,"_create_use
r":"admin","_create_time":1597183130364,"_last_modified_user":"admin","_last_modified_time":15
97183130364,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}, New
value=["default" "SecurityPolicy-1" "Rule1_1"
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1","path":

<182>1 2020-08-11T21:58:50.404Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="Rule1_1" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e"
splitId="E993J2LF" splitIndex="2 of 2" subcomp="policy" update="true"] "/infra/domains/
default/security-policies/SecurityPolicy-1/rules/
Rule1_1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_excluded":
false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN
"}]

<182>1 2020-08-11T21:58:50.466Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e" splitId="iMHWlshi"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy",
Operation="PatchInfra", Operation status="success", New
value={"enforce_revision_check":true} {"resource_type":"Infra","children":[{"children":
[{"SecurityPolicy":
{"resource_type":"SecurityPolicy","id":"SecurityPolicy-1","display_name":"SecurityPolicy-1","p
ath":"/infra/domains/default/security-policies/SecurityPolicy-1","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1","path":"/
infra/domains/default/security-policies/SecurityPolicy-1/rules/
Rule1_1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_excluded":

```

```

false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN
"},"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protectio
n":"UNKNOWN"}],"marked_for_delete"

<182>1 2020-08-11T21:58:50.466Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="2aff6b4f-3d4f-4d62-a639-61291f7e879e" splitId="iMHWlshi"
splitIndex="2 of 2" subcomp="policy"
update="true"] :false,"overridden":false,"sequence_number":10,"category":"Application","stateful":true,"locked":false,"scope":
["ANY"],"_protection":"UNKNOWN"},"resource_type":"ChildSecurityPolicy","marked_for_delete":fal
se,"mark_for_override":false,"_protection":"UNKNOWN"},"target_type":"Domain","resource_type":
"ChildResourceReference","id":"default","marked_for_delete":false,"mark_for_override":false,"_
protection":"UNKNOWN"},"marked_for_delete":false,"overridden":false,"_protection":"UNKNOWN",
_revision":-1}]

```

在區段 (SecurityPolicy-1) 中更新規則 (從 Rule1_1 至 Rule1_1_updated):

```

<182>1 2020-08-11T22:22:06.303Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa" splitId="mJ7hQGhg"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="DfwSecurityPolicy", Operation="PatchSecurityPolicyForDomain", Operation
status="success", New value=["default" "SecurityPolicy-1"
{"resource_type":"SecurityPolicy","id":"SecurityPolicy-1","display_name":"SecurityPolicy-1","p
ath":"/infra/domains/default/security-policies/
SecurityPolicy-1","unique_id":"895eeac5-641b-4306-be7f-a43fdd969ee5","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1_updated","path
":"/infra/domains/default/security-policies/SecurityPolicy-1/rules/
Rule1_1","unique_id":"2024","marked_for_delete":false,"overridden":false,"rule_id":2024,"seque
nce_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_p
rotection":"UNKNOWN",_revision":0},"resource_type":
<182>1 2020-08-11T22:22:06.303Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa" splitId="mJ7hQGhg"
splitIndex="2 of 2" subcomp="policy" update="true"]
"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"},"mar
ked_for_delete":false,"overridden":false,"sequence_number":10,"internal_sequence_number":13000
010,"category":"Application","stateful":true,"tcp_strict":true,"locked":false,"lock_modified_t
ime":0,"scope":["ANY"],"is_default":false,"_protection":"UNKNOWN",_revision":0}]

<182>1 2020-08-11T22:22:06.324Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="Rule1_1" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa"
splitId="JKVilI6n" splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="DfwSecurityPolicy", Operation="UpdateSecurityRule", Operation status="success",
Old value=[{"sequence_number":10,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"Rule1
_1","display_name":"Rule1_1","path":"/infra/domains/default/security-policies/
SecurityPolicy-1/rules/Rule1_1","relative_path":"Rule1_1","parent_path":"/infra/domains/
default/security-policies/
SecurityPolicy-1","unique_id":"2024","marked_for_delete":false,"overridden":false,"_create_use
r":"admin",_create_time":1597183130364,"_last_modified_user":"admin",_last_modified_time":15

```

```

97183130369,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}}, New
value=["default" "SecurityPolicy-1" "Rule1_1"
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1_updated","path
":

<182>1 2020-08-11T22:22:06.324Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="Rule1_1" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa"
splitId="JKVilI6n" splitIndex="2 of 2" subcomp="policy" update="true"] "/infra/domains/
default/security-policies/SecurityPolicy-1/rules/
Rule1_1","unique_id":"2024","marked_for_delete":false,"overridden":false,"rule_id":2024,"seque
nce_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_p
rotection":"UNKNOWN","_revision":0}}

<182>1 2020-08-11T22:22:06.363Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa" splitId="9MtbEpd8"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy",
Operation="PatchInfra", Operation status="success", New
value=[{"enforce_revision_check":true} {"resource_type":"Infra","children":[{"children":
[{"SecurityPolicy":
{"resource_type":"SecurityPolicy","id":"SecurityPolicy-1","display_name":"SecurityPolicy-1","p
ath":"/infra/domains/default/security-policies/
SecurityPolicy-1","unique_id":"895eeac5-641b-4306-be7f-a43fdd969ee5","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"Rule1_1","display_name":"Rule1_1_updated","path
":"/infra/domains/default/security-policies/SecurityPolicy-1/rules/
Rule1_1","unique_id":"2024","marked_for_delete":false,"overridden":false,"rule_id":2024,"seque
nce_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":
["ANY"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_p
rotection":"UNKNOWN","_revision":
}

<182>1 2020-08-11T22:22:06.363Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="6aadd8de-d157-4479-b84c-8410dd48c2aa" splitId="9MtbEpd8"
splitIndex="2 of 2" subcomp="policy" update="true"]
0),"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protection
":"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"internal_seq
uence_number":13000010,"category":"Application","stateful":true,"tcp_strict":true,"locked":fal
se,"lock_modified_time":0,"scope":
["ANY"],"is_default":false,"_protection":"UNKNOWN","_revision":0},"resource_type":"ChildSecuri
tyPolicy","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"}],"targe
t_type":"Domain","resource_type":"ChildResourceReference","id":"default","marked_for_delete":f
alse,"mark_for_override":false,"_protection":"UNKNOWN"}],"marked_for_delete":false,"overridden
":false,"_protection":"UNKNOWN","_revision":-1}}

```

從區段 (SecurityPolicy-1) 刪除規則 (Rule1_2) :

```

<182>1 2020-08-11T22:12:24.444Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="Rule1_2" level="INFO" reqId="1a58e753-460c-443f-8a28-0d40d8af9b76"
subcomp="policy" update="true" username="admin"] UserName="admin",
ModuleName="DfwSecurityPolicy", Operation="DeleteSecurityRule", Operation status="success",
Old value=[{"sequence_number":20,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":

```

```
[{"ANY"}], "disabled": false, "direction": "IN_OUT", "resource_type": "CommunicationEntry", "id": "Rule1_2", "display_name": "Rule1_2", "path": "/infra/domains/default/security-policies/SecurityPolicy-1/rules/Rule1_2", "relative_path": "Rule1_2", "parent_path": "/infra/domains/default/security-policies/SecurityPolicy-1", "unique_id": "2026", "marked_for_delete": false, "overridden": false, "create_user": "admin", "create_time": 1597183904580, "last_modified_user": "admin", "last_modified_time": 1597183904582, "system_owned": false, "protection": "NOT_PROTECTED", "revision": 0}], New value=["default" "SecurityPolicy-1" "Rule1_2"]
```

```
<182>1 2020-08-11T22:12:24.463Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="1a58e753-460c-443f-8a28-0d40d8af9b76" splitId="hoDI5YJQ" splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="DfwSecurityPolicy", Operation="PatchSecurityPolicyForDomain", Operation status="success", New value=["default" "SecurityPolicy-1" {"resource_type": "SecurityPolicy", "id": "SecurityPolicy-1", "display_name": "SecurityPolicy-1", "path": "/infra/domains/default/security-policies/SecurityPolicy-1", "unique_id": "895eeac5-641b-4306-be7f-a43fdd969ee5", "children": [{"Rule": {"resource_type": "Rule", "id": "Rule1_2", "path": "/infra/domains/default/security-policies/SecurityPolicy-1/rules/Rule1_2", "marked_for_delete": true, "overridden": false, "sources_excluded": false, "destinations_excluded": false, "logged": false, "disabled": false, "direction": "IN_OUT", "protection": "UNKNOWN"}}, {"resource_type": "ChildRule", "marked_for_delete": true, "mark_for_override": false, "protection": "UNKNOWN"}], "marked_for_delete": false, "overridden": false, "sequence_number": 10, "internal_sequence_number": 13000010, "category": "Application", "stateful": true, "tcp_strict": true, "locked": false, "lock_modified_time": 0, "scope":
```

```
<182>1 2020-08-11T22:12:24.463Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="1a58e753-460c-443f-8a28-0d40d8af9b76" splitId="hoDI5YJQ" splitIndex="2 of 2" subcomp="policy" update="true"] [{"ANY}], "is_default": false, "protection": "UNKNOWN", "revision": 0}]
```

```
<182>1 2020-08-11T22:12:24.497Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="1a58e753-460c-443f-8a28-0d40d8af9b76" splitId="mxpzQHfF" splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy", Operation="PatchInfra", Operation status="success", New value=[{"enforce_revision_check": true} {"resource_type": "Infra", "children": [{"children": [{"SecurityPolicy": {"resource_type": "SecurityPolicy", "id": "SecurityPolicy-1", "display_name": "SecurityPolicy-1", "path": "/infra/domains/default/security-policies/SecurityPolicy-1", "unique_id": "895eeac5-641b-4306-be7f-a43fdd969ee5", "children": [{"Rule": {"resource_type": "Rule", "id": "Rule1_2", "path": "/infra/domains/default/security-policies/SecurityPolicy-1/rules/Rule1_2", "marked_for_delete": true, "overridden": false, "sources_excluded": false, "destinations_excluded": false, "logged": false, "disabled": false, "direction": "IN_OUT", "protection": "UNKNOWN"}}, {"resource_type": "ChildRule", "marked_for_delete": true, "mark_for_override": false, "protection": "UNKNOWN"}], "marked_for_delete": false, "overridden": false, "sequence_number": 10, "internal_sequence_number": 13000010, "category": "Application", "stateful": true, "tcp_strict":
```

```
<182>1 2020-08-11T22:12:24.497Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="1a58e753-460c-443f-8a28-0d40d8af9b76" splitId="mxpzQHfF" splitIndex="2 of 2" subcomp="policy" update="true"] true, "locked": false, "lock_modified_time": 0, "scope": [{"ANY}], "is_default": false, "protection": "UNKNOWN", "revision": 0}, {"resource_type": "ChildSecuri
```

```
tyPolicy", "marked_for_delete": false, "mark_for_override": false, "_protection": "UNKNOWN"}], "target_type": "Domain", "resource_type": "ChildResourceReference", "id": "default", "marked_for_delete": false, "mark_for_override": false, "_protection": "UNKNOWN"}], "marked_for_delete": false, "overridden": false, "_protection": "UNKNOWN", "_revision": -1}}
```

刪除包含規則 (Rule1_1) 的區段 (SecurityPolicy-1) :

```
<182>1 2020-08-11T22:24:24.898Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" entId="SecurityPolicy-1" level="INFO" reqId="724b5494-10cd-4124-a431-56ba7d922bbf" splitId="4WIXz9qL" splitIndex="1 of 2" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="DfwSecurityPolicy", Operation="DeleteSecurityPolicyForDomain",
Operation status="success", Old
value=[{"precedence":10,"category":"Application","resource_type":"CommunicationMap","id":"SecurityPolicy-1","display_name":"SecurityPolicy-1","path":"/infra/domains/default/security-policies/SecurityPolicy-1","relative_path":"SecurityPolicy-1","parent_path":"/infra/domains/default","unique_id":"895eeac5-641b-4306-be7f-a43fdd969ee5","marked_for_delete":false,"overridden":false,"_create_user":"admin","_create_time":1597183130247,"_last_modified_user":"admin","_last_modified_time":1597183130251,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}{ "sequence_number":10,"source_groups":["ANY"],"destination_groups":["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":["ANY"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"Rule1_1","display_name":"Rule1_1_updated","path":}
```

```
<182>1 2020-08-11T22:24:24.898Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" entId="SecurityPolicy-1" level="INFO" reqId="724b5494-10cd-4124-a431-56ba7d922bbf" splitId="4WIXz9qL" splitIndex="2 of 2" subcomp="policy" update="true" username="admin"] "/infra/domains/default/security-policies/SecurityPolicy-1/rules/Rule1_1","relative_path":"Rule1_1","parent_path":"/infra/domains/default/security-policies/SecurityPolicy-1","unique_id":"2024","marked_for_delete":false,"overridden":false,"_create_user":"admin","_create_time":1597183130364,"_last_modified_user":"admin","_last_modified_time":1597184526313,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":1}], New value=["default" "SecurityPolicy-1"]
```

```
<182>1 2020-08-11T22:24:24.938Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="724b5494-10cd-4124-a431-56ba7d922bbf" subcomp="policy" update="true"]
UserName="admin", ModuleName="Policy", Operation="PatchInfra", Operation status="success", New value=[{"enforce_revision_check":true}
{"resource_type":"Infra","children":[{"children":[{"SecurityPolicy":
{"resource_type":"SecurityPolicy","id":"SecurityPolicy-1","path":"/infra/domains/default/security-policies/SecurityPolicy-1","marked_for_delete":true,"overridden":false,"locked":false,"_protection":"UNKNOWN"},"resource_type":"ChildSecurityPolicy","marked_for_delete":true,"mark_for_override":false,"_protection":"UNKNOWN"}], "target_type": "Domain", "resource_type": "ChildResourceReference", "id": "default", "marked_for_delete": false, "mark_for_override": false, "_protection": "UNKNOWN"}], "marked_for_delete": false, "overridden": false, "_protection": "UNKNOWN", "_revision": -1}]
```

原則模式中的閘道防火牆變更

請注意，第 0 層閘道和第 1 層閘道的記錄訊息類似。

使用第 1 層閘道 (myT1) 的規則 (myT1_Rule1) 新增區段 (T1-Policies) :

```

<182>1 2020-08-11T22:31:26.800Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="Ta8faYzQ"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="PatchGatewayPolicyForDomain", Operation
status="success", Old
value=[{"precedence":10,"category":"LocalGatewayRules","resource_type":"CommunicationMap","id"
:"T1-Policies","display_name":"T1-Policies","path":"/infra/domains/default/gateway-
policies/T1-Policies","relative_path":"T1-Policies","parent_path":"/infra/domains/
default","unique_id":"a73c1345-6b4e-43e0-
b4ee-9a91c7ba9df6","marked_for_delete":false,"overridden":false,"_create_user":"admin","_creat
e_time":1597185086789,"_last_modified_user":"admin","_last_modified_time":1597185086789,"_syst
em_owned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["default" "T1-
Policies" {"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-
Policies","path":"/infra/domains/default/gateway-policies/T1-Policies","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1","path":

```

```

<182>1 2020-08-11T22:31:26.801Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="Ta8faYzQ"
splitIndex="2 of 2" subcomp="policy" update="true"] "/infra/domains/default/gateway-
policies/T1-Policies/rules/
myT1_Rule1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_exclude
d":false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN"
},"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protection
":"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"category":"Lo
calGatewayRules","stateful":true,"locked":false,"_protection":"UNKNOWN"}]

```

```

<182>1 2020-08-11T22:31:26.878Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="aZfgiFKt"
splitIndex="1 of 2" subcomp="policy" update="true" username="admin"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="PatchGatewayRule", Operation status="success",
Old value=[{"sequence_number":10,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"myT1_R
ule1","display_name":"myT1_Rule1","path":"/infra/domains/default/gateway-policies/T1-Policies/
rules/myT1_Rule1","relative_path":"myT1_Rule1","parent_path":"/infra/domains/default/gateway-
policies/T1-
Policies","unique_id":"2028","marked_for_delete":false,"overridden":false,"_create_user":"admi
n","_create_time":1597185086809,"_last_modified_user":"admin","_last_modified_time":1597185086
809,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["default"
"T1-Policies" "myT1_Rule1"
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1","path":

```

```

<182>1 2020-08-11T22:31:26.878Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="aZfgiFKt"
splitIndex="2 of 2" subcomp="policy" update="true" username="admin"] "/infra/domains/default/
gateway-policies/T1-Policies/rules/
myT1_Rule1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_exclude
d":false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN"
}]

```



```
<182>1 2020-08-11T22:31:26.890Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="0s7tdCjN"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy",
Operation="PatchInfra", Operation status="success", New
value={"enforce_revision_check":true} {"resource_type":"Infra","children":[{"children":
[{"GatewayPolicy":{"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-
Policies","path":"/infra/domains/default/gateway-policies/T1-Policies","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1","path":
"/infra/domains/default/gateway-policies/T1-Policies/rules/
myT1_Rule1","marked_for_delete":false,"overridden":false,"sequence_number":10,"sources_exclude
d":false,"destinations_excluded":false,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"profiles":["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","_protection":"UNKNOWN"
},"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protection
":
};

<182>1 2020-08-11T22:31:26.890Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="c2790fbd-db29-46d3-9a0e-1003455ee9ea" splitId="0s7tdCjN"
splitIndex="2 of 2" subcomp="policy" update="true"]
"UNKNOWN"},"marked_for_delete":false,"overridden":false,"sequence_number":10,"category":"Loca
lGatewayRules","stateful":true,"locked":false,"_protection":"UNKNOWN"},"resource_type":"ChildG
atewayPolicy","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"},"t
arget_type":"Domain","resource_type":"ChildResourceReference","id":"default","marked_for_delet
e":false,"mark_for_override":false,"_protection":"UNKNOWN"},"marked_for_delete":false,"overri
dden":false,"_protection":"UNKNOWN","_revision":-1}]}
```

在區段 (T1-Policies) 中更新規則 (從 myT1_Rule1 至 myT1_Rule1_Updated):

```
<182>1 2020-08-11T22:36:19.410Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="BiHDjsY8"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="PatchGatewayPolicyForDomain", Operation
status="success", New value=["default" "T1-Policies"
{"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-Policies","path":"/
infra/domains/default/gateway-policies/T1-Policies","unique_id":"a73c1345-6b4e-43e0-
b4ee-9a91c7ba9df6","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1_Updated"
,"path":"/infra/domains/default/gateway-policies/T1-Policies/rules/
myT1_Rule1","unique_id":"2028","marked_for_delete":false,"overridden":false,"rule_id":2028,"se
quence_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_pr
otection":"UNKNOWN","_revision":0},"resource_type":

<182>1 2020-08-11T22:36:19.410Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="BiHDjsY8"
splitIndex="2 of 2" subcomp="policy" update="true"]
"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"},"mar
ked_for_delete":false,"overridden":false,"sequence_number":10,"internal_sequence_number":13000
010,"category":"LocalGatewayRules","stateful":true,"tcp_strict":true,"locked":false,"lock_modi
fied_time":0,"is_default":false,"_protection":"UNKNOWN","_revision":0}]

<182>1 2020-08-11T22:36:19.430Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
```

```

manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="HqttDMqz"
splitIndex="1 of 2" subcomp="policy" update="true" username="admin"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="PatchGatewayRule", Operation status="success",
Old value=[{"sequence_number":10,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"myT1_R
ule1","display_name":"myT1_Rule1","path":"/infra/domains/default/gateway-policies/T1-Policies/
rules/myT1_Rule1","relative_path":"myT1_Rule1","parent_path":"/infra/domains/default/gateway-
policies/T1-
Policies","unique_id":"2028","marked_for_delete":false,"overridden":false,"_create_user":"admi
n","_create_time":1597185086809,"_last_modified_user":"admin","_last_modified_time":1597185086
841,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["default"
"T1-Policies" "myT1_Rule1"
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1_Updated"
,"path":

<182>1 2020-08-11T22:36:19.430Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="HqttDMqz"
splitIndex="2 of 2" subcomp="policy" update="true" username="admin"] "/infra/domains/default/
gateway-policies/T1-Policies/rules/
myT1_Rule1","unique_id":"2028","marked_for_delete":false,"overridden":false,"rule_id":2028,"se
quence_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_pr
otection":"UNKNOWN","_revision":0}]

<182>1 2020-08-11T22:36:19.443Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="fMYsYjV5"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy",
Operation="PatchInfra", Operation status="success", New
value=[{"enforce_revision_check":true} {"resource_type":"Infra","children":[{"children":
[{"GatewayPolicy":{"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-
Policies","path":"/infra/domains/default/gateway-policies/T1-
Policies","unique_id":"a73c1345-6b4e-43e0-b4ee-9a91c7ba9df6","children":[{"Rule":
{"action":"ALLOW","resource_type":"Rule","id":"myT1_Rule1","display_name":"myT1_Rule1_Updated"
,"path":"/infra/domains/default/gateway-policies/T1-Policies/rules/
myT1_Rule1","unique_id":"2028","marked_for_delete":false,"overridden":false,"rule_id":2028,"se
quence_number":10,"sources_excluded":false,"destinations_excluded":false,"source_groups":
["ANY"],"destination_groups":["ANY"],"services":["ANY"],"profiles":
["ANY"],"logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_pr
otection":"UNKNOWN","_revision":

<182>1 2020-08-11T22:36:19.443Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="a17fcbdc-1aed-4526-93e9-40a3730eeb7f" splitId="fMYsYjV5"
splitIndex="2 of 2" subcomp="policy" update="true"]
0},"resource_type":"ChildRule","marked_for_delete":false,"mark_for_override":false,"_protectio
n":"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"internal_seq
uence_number":13000010,"category":"LocalGatewayRules","stateful":true,"tcp_strict":true,"locke
d":false,"lock_modified_time":0,"is_default":false,"_protection":"UNKNOWN","_revision":0},"res
ource_type":"ChildGatewayPolicy","marked_for_delete":false,"mark_for_override":false,"_protect
ion":"UNKNOWN"}],"target_type":"Domain","resource_type":"ChildResourceReference","id":"default
","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"}],"marked_for_de
lete":false,"overridden":false,"_protection":"UNKNOWN","_revision":-1}]

```

從區段 (T1-Policies) 刪除規則 (myT1_Rule2) :

```
<182>1 2020-08-11T22:38:03.262Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="myT1_Rule2" level="INFO" reqId="ccb8d0bb-0fe2-415a-9979-ala3a80a7038"
subcomp="policy" update="true" username="admin"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="DeleteGatewayRule", Operation status="success",
Old value=[{"sequence_number":20,"source_groups":["ANY"],"destination_groups":
["ANY"],"services":["ANY"],"action":"ALLOW","logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"myT1_R
ule2","display_name":"myT1_Rule2","path":"/infra/domains/default/gateway-policies/T1-Policies/
rules/myT1_Rule2","relative_path":"myT1_Rule2","parent_path":"/infra/domains/default/gateway-
policies/T1-
Policies","unique_id":"2029","marked_for_delete":false,"overridden":false,"_create_user":"admi
n","_create_time":1597185467310,"_last_modified_user":"admin","_last_modified_time":1597185467
314,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["default"
"T1-Policies" "myT1_Rule2"]
```

```
<182>1 2020-08-11T22:38:03.280Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="ccb8d0bb-0fe2-415a-9979-ala3a80a7038" splitId="G1UhKvqu"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin",
ModuleName="PolicyEdgeFirewall", Operation="PatchGatewayPolicyForDomain", Operation
status="success", New value=["default" "T1-Policies"
{"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-Policies","path":"/
infra/domains/default/gateway-policies/T1-Policies","unique_id":"a73c1345-6b4e-43e0-
b4ee-9a91c7ba9df6","children":[{"Rule":{"resource_type":"Rule","id":"myT1_Rule2","path":"/
infra/domains/default/gateway-policies/T1-Policies/rules/
myT1_Rule2","marked_for_delete":true,"overridden":false,"sources_excluded":false,"destinations
_excluded":false,"logged":false,"disabled":false,"direction":"IN_OUT","_protection":"UNKNOWN"}
,"resource_type":"ChildRule","marked_for_delete":true,"mark_for_override":false,"_protection":
"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"internal_sequen
ce_number":13000010,"category":"LocalGatewayRules","stateful":true,"tcp_strict":true,"locked":
false,"lock_modified_time":0,"is_default":
```

```
<182>1 2020-08-11T22:38:03.280Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="ccb8d0bb-0fe2-415a-9979-ala3a80a7038" splitId="G1UhKvqu"
splitIndex="2 of 2" subcomp="policy" update="true"]
false,"_protection":"UNKNOWN","_revision":0}]
```

```
<182>1 2020-08-11T22:38:03.295Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="ccb8d0bb-0fe2-415a-9979-ala3a80a7038" splitId="xn09T8NE"
splitIndex="1 of 2" subcomp="policy" update="true"] UserName="admin", ModuleName="Policy",
Operation="PatchInfra", Operation status="success", New
value=[{"enforce_revision_check":true} {"resource_type":"Infra","children":[{"children":
[{"GatewayPolicy":{"resource_type":"GatewayPolicy","id":"T1-Policies","display_name":"T1-
Policies","path":"/infra/domains/default/gateway-policies/T1-
Policies","unique_id":"a73c1345-6b4e-43e0-b4ee-9a91c7ba9df6","children":[{"Rule":
{"resource_type":"Rule","id":"myT1_Rule2","path":"/infra/domains/default/gateway-policies/T1-
Policies/rules/
myT1_Rule2","marked_for_delete":true,"overridden":false,"sources_excluded":false,"destinations
_excluded":false,"logged":false,"disabled":false,"direction":"IN_OUT","_protection":"UNKNOWN"}
,"resource_type":"ChildRule","marked_for_delete":true,"mark_for_override":false,"_protection":
"UNKNOWN"}],"marked_for_delete":false,"overridden":false,"sequence_number":10,"internal_sequen
ce_number":13000010,"category":"LocalGatewayRules","stateful":true,"tcp_strict":true,"locked":
```

```
<182>1 2020-08-11T22:38:03.295Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
```

```
manager" level="INFO" reqId="ccb8d0bb-0fe2-415a-9979-ala3a80a7038" splitId="xnO9T8NE"
splitIndex="2 of 2" subcomp="policy" update="true"]
false,"lock_modified_time":0,"is_default":false,"_protection":"UNKNOWN","_revision":0},"resour
ce_type":"ChildGatewayPolicy","marked_for_delete":false,"mark_for_override":false,"_protection
":"UNKNOWN"}],"target_type":"Domain","resource_type":"ChildResourceReference","id":"default","
marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"}],"marked_for_delet
e":false,"overridden":false,"_protection":"UNKNOWN","_revision":-1}]
```

刪除包含規則 (myT1_Rule1_Updated) 的區段 (T1-Policies) :

```
<182>1 2020-08-11T22:41:30.726Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="T1-Policies" level="INFO" reqId="d751343c-32ab-46ee-b176-752b8aelec0d"
splitId="Wzc3oxDG" splitIndex="1 of 2" subcomp="policy" update="true" username="admin"]
UserName="admin", ModuleName="PolicyEdgeFirewall", Operation="DeleteGatewayPolicy", Operation
status="success", Old
value=[{"precedence":10,"category":"LocalGatewayRules","resource_type":"CommunicationMap","id"
:"T1-Policies","display_name":"T1-Policies","path":"/infra/domains/default/gateway-
policies/T1-Policies","relative_path":"T1-Policies","parent_path":"/infra/domains/
default","unique_id":"a73c1345-6b4e-43e0-
b4ee-9a91c7ba9df6","marked_for_delete":false,"overridden":false,"_create_user":"admin","_creat
e_time":1597185086789,"_last_modified_user":"admin","_last_modified_time":1597185086790,"_syst
em_owned":false,"_protection":"NOT_PROTECTED","_revision":0}
{"sequence_number":10,"source_groups":["ANY"],"destination_groups":["ANY"],"services":
["ANY"],"action":"ALLOW","logged":false,"scope":["/infra/tier-1s/
myT1"],"disabled":false,"direction":"IN_OUT","resource_type":"CommunicationEntry","id":"myT1_R
ule1","display_name":"myT1_Rule1_Updated","path":
```

```
<182>1 2020-08-11T22:41:30.726Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" entId="T1-Policies" level="INFO" reqId="d751343c-32ab-46ee-b176-752b8aelec0d"
splitId="Wzc3oxDG" splitIndex="2 of 2" subcomp="policy" update="true" username="admin"] "/
infra/domains/default/gateway-policies/T1-Policies/rules/
myT1_Rule1","relative_path":"myT1_Rule1","parent_path":"/infra/domains/default/gateway-
policies/T1-
Policies","unique_id":"2028","marked_for_delete":false,"overridden":false,"_create_user":"admi
n","_create_time":1597185086809,"_last_modified_user":"admin","_last_modified_time":1597185379
419,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":1}], New value=["default"
"T1-Policies"]
```

```
<182>1 2020-08-11T22:41:30.733Z manager1 NSX 22164 - [nsx@6876 audit="true" comp="nsx-
manager" level="INFO" reqId="d751343c-32ab-46ee-b176-752b8aelec0d" subcomp="policy"
update="true"] UserName="admin", ModuleName="Policy", Operation="PatchInfra", Operation
status="success", New value=[{"enforce_revision_check":true}
{"resource_type":"Infra","children":[{"children":[{"GatewayPolicy":
{"resource_type":"GatewayPolicy","id":"T1-Policies","path":"/infra/domains/default/gateway-
policies/T1-
Policies","marked_for_delete":true,"overridden":false,"locked":false,"_protection":"UNKNOWN"},
"resource_type":"ChildGatewayPolicy","marked_for_delete":true,"mark_for_override":false,"_prot
ection":"UNKNOWN"}],"target_type":"Domain","resource_type":"ChildResourceReference","id":"defa
ult","marked_for_delete":false,"mark_for_override":false,"_protection":"UNKNOWN"}],"marked_for
_delete":false,"overridden":false,"_protection":"UNKNOWN","_revision":-1}]
```

管理程式模式中的分散式防火牆變更

新增防火牆區段 (FirewallSection-2) :

```
<182>1 2020-08-12T00:25:53.300Z manager1 NSX 1503 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="244e8a97-93d4-4047-b817-81b59b94ce13" subcomp="manager" username="admin"] UserName="admin", ModuleName="NSX-Firewall", Operation="CREATE", Operation status="success", New value=[FirewallSectionLock [Id=0ffb0688-9f4e-4096-a19f-2d98ce8cfbeb, sectionId=f5226cab-525b-4e33-a26d-e5053fbba0a1, sectionRevision=0, locked=false, comments=Default section unlock comment, created_by=admin, create_time=1597191953299, last_modified_by=admin, last_modified_time=1597191953299]]
```

```
<182>1 2020-08-12T00:25:53.313Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="244e8a97-93d4-4047-b817-81b59b94ce13" subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall", Operation="AddSection", Operation status="success", New value=[{"operation":"insert_before","id":"ffffffff-8a04-4924-a5b4-54d30e81befe"} {"locked":false,"autoplumbed":false,"tcp_strict":false,"display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"_protection":"UNKNOWN"}]
```

將規則 (mp_Rule1) 新增至區段 (FirewallSection-2) :

```
<182>1 2020-08-12T00:27:21.252Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="3562bb3e-bf18-4aa0-ald-d-abde13e8559c" splitId="ScK9FB8V" splitIndex="1 of 2" subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall", Operation="UpdateSectionWithRules", Operation status="success", Old value=[{"locked":false,"comments":"Default section unlock comment","lock_modified_by":"admin","lock_modified_time":1597191953299,"autoplumbed":false,"enforced_on":"VIF","tcp_strict":false,"category":"Default","resource_type":"FirewallSection","id":"f5226cab-525b-4e33-a26d-e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule_count":0,"is_default":false,"_create_user":"admin","_create_time":1597191953297,"_last_modified_user":"admin","_last_modified_time":1597191953297,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":0}], New value=["f5226cab-525b-4e33-a26d-e5053fbba0a1" {"rules":[{"display_name":"mp_Rule1","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false}], "resource_type":"FirewallSection","id":
<182>1 2020-08-12T00:27:21.252Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="3562bb3e-bf18-4aa0-ald-d-abde13e8559c" splitId="ScK9FB8V" splitIndex="2 of 2" subcomp="manager" update="true" username="admin"] "f5226cab-525b-4e33-a26d-e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule_count":0,"is_default":false,"locked":false,"comments":"Default section unlock comment","lock_modified_by":"admin","lock_modified_time":1597191953299,"autoplumbed":false,"enforced_on":"VIF","tcp_strict":false,"category":"Default","_protection":"UNKNOWN","_revision":0
}]
```

在區段 (FirewallSection-2) 中更新規則 (從 mp_Rule1 至 mp_Rule1_updated) :

```
<182>1 2020-08-12T00:28:54.226Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="37954994-8d59-448e-923d-940813087640" splitId="KcUAlRY1" splitIndex="1 of 2" subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall",
```

```

Operation="UpdateSectionWithRules", Operation status="success", Old
value=[{"section_id":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","resource_type":"FirewallRule","id":"536870917","display_name":"mp_Rule1","sourc
es_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":fa
lse,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false}
{"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597191953299,"autoplumbed":false,"en
forced_on":"VIF","tcp_strict":false,"category":"Default","resource_type":"FirewallSection","id
":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule
_count":1,"is_default":false,"_create_user":"admin","_create_time":1597191953297,"_last_modifi
ed_user":"admin","_last_modified_time":1597192041235,"_system_owned":false,"_protection":"NOT_
PROTECTED","_revision":
<182>1 2020-08-12T00:28:54.226Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO"
reqId="37954994-8d59-448e-923d-940813087640" splitId="KcUALRY1" splitIndex="2 of 2"
subcomp="manager" update="true" username="admin"] 1}], New value=[{"f5226cab-525b-4e33-a26d-
e5053fbba0a1" {"rules":[{"section_id":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","resource_type":"FirewallRule","id":"536870917","display_name":"mp_Rule1_updated
","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"lo
gged":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_revision":1}],
"resource_type":"FirewallSectionRuleList","id":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule
_count":1,"is_default":false,"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597191953299,"autoplumbed":false,"en
forced_on":"VIF","tcp_strict":false,"category":"Default","_protection":"UNKNOWN","_revision":1
}]

```

從區段 (FirewallSection-2) 刪除規則 (mp_Rule2) :

```

<182>1 2020-08-12T00:33:58.355Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO"
reqId="2db867e0-0407-44a2-8a6c-96895ff14a2f" splitId="m9SdpPw2" splitIndex="1 of 3"
subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall",
Operation="UpdateSectionWithRules", Operation status="success", Old
value=[{"section_id":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","resource_type":"FirewallRule","id":"536870918","display_name":"mp_Rule2","sourc
es_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":fa
lse,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false}
{"section_id":"f5226cab-525b-4e33-a26d-
e5053fbba0a1","resource_type":"FirewallRule","id":"536870917","display_name":"mp_Rule1_updated
","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"lo
gged":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false}
{"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597191953299,"autoplumbed":false,"en
forced_on":"VIF","tcp_strict":false,"category":"Default","resource_type":"FirewallSection","id
":
<182>1 2020-08-12T00:33:58.355Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO"
reqId="2db867e0-0407-44a2-8a6c-96895ff14a2f" splitId="m9SdpPw2" splitIndex="2 of 3"
subcomp="manager" update="true" username="admin"] "f5226cab-525b-4e33-a26d-
e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule
_count":2,"is_default":false,"_create_user":"admin","_create_time":1597191953297,"_last_modifi
ed_user":"admin","_last_modified_time":1597192378372,"_system_owned":false,"_protection":"NOT_
PROTECTED","_revision":3}], New value=[{"f5226cab-525b-4e33-a26d-e5053fbba0a1" {"rules":

```

```
[{"section_id":"f5226cab-525b-4e33-a26d-e5053fbba0a1","resource_type":"FirewallRule","id":"536870917","display_name":"mp_Rule1_updated","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false,"_revision":3}],{"resource_type":"FirewallSectionRuleList","id":"f5226cab-525b-4e33-a26d-e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule_count":2,"is_default":false,"locked":false,"comments":"Default section unlock comment","lock_modified_by":<182>1 2020-08-12T00:33:58.355Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="2db867e0-0407-44a2-8a6c-96895ff14a2f" splitId="m9SdpPw2" splitIndex="3 of 3" subcomp="manager" update="true" username="admin"] "admin","lock_modified_time":1597191953299,"autoplumbed":false,"enforced_on":"VIF","tcp_strict":false,"category":"Default","_protection":"UNKNOWN","_revision":3}]
```

刪除包含規則 (mp_Rule1) 的區段 (FirewallSection-2) :

```
<182>1 2020-08-12T00:35:01.304Z manager1 NSX 1503 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="f23e091f-aa6e-47a6-945a-98291cc3f0ba" subcomp="manager" username="admin"] UserName="admin", ModuleName="NSX-Firewall", Operation="DELETE", Operation status="success", Old value=[FirewallSectionLock [Id=0ffb0688-9f4e-4096-a19f-2d98ce8cfbeb, sectionId=f5226cab-525b-4e33-a26d-e5053fbba0a1, sectionRevision=0, locked=false, comments=Default section unlock comment, created_by=admin, create_time=1597191953299, last_modified_by=admin, last_modified_time=1597191953299]]
<182>1 2020-08-12T00:35:01.324Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-manager" entId="f5226cab-525b-4e33-a26d-e5053fbba0a1" level="INFO" reqId="f23e091f-aa6e-47a6-945a-98291cc3f0ba" subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall", Operation="DeleteSection", Operation status="success", Old value=[null{"section_id":"f5226cab-525b-4e33-a26d-e5053fbba0a1","resource_type":"FirewallRule","id":"536870917","display_name":"mp_Rule1_updated","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":false,"direction":"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false} {"locked":false,"autoplumbed":false,"enforced_on":"VIF","tcp_strict":false,"category":"Default","resource_type":"FirewallSection","id":"f5226cab-525b-4e33-a26d-e5053fbba0a1","display_name":"FirewallSection-2","section_type":"LAYER3","stateful":true,"rule_count":1,"is_default":false,"_create_user":"admin","_create_time":1597191953297,"_last_modified_user":"admin","_last_modified_time":1597192438335,"_system_owned":false,"_protection":"NOT_PROTECTED","_revision":4}], New value=[{"f5226cab-525b-4e33-a26d-e5053fbba0a1" {"cascade":true}]
```

管理程式模式中的 Edge 防火牆變更

請注意，第 0 層邏輯路由器和第 1 層邏輯路由器的記錄訊息類似。

為第 1 層邏輯路由器 (myT1_mp) 新增防火牆區段 (FirewallSection-1) :

```
<182>1 2020-08-12T00:09:55.661Z manager1 NSX 1503 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="14af9252-ddc3-4949-8e01-b2c5676ac258" subcomp="manager" username="admin"] UserName="admin", ModuleName="NSX-Firewall", Operation="CREATE", Operation status="success", New value=[FirewallSectionLock [Id=15b61818-2a65-48cf-a98e-7c2f3fccc845, sectionId=9808d1ec-de08-48b3-8173-12f26fb0ae9c, sectionRevision=0, locked=false, comments=Default section unlock comment, created_by=admin, create_time=1597190995659, last_modified_by=admin, last_modified_time=1597190995659]]
```

```
<182>1 2020-08-12T00:09:55.687Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="14af9252-
ddc3-4949-8e01-b2c5676ac258" subcomp="manager" update="true" username="admin"]
UserName="admin", ModuleName="Firewall", Operation="AddSection", Operation status="success",
New value=[{"operation":"insert_before","id":"095b443a-115d-4bf7-b4f7-192305321e95"}
{"locked":false,"autoplumbed":false,"tcp_strict":false,"display_name":"FirewallSection-1","app
lied_tos":
[{"target_id":"6562738e-73b9-4f21-9461-460ead581daf","target_display_name":"myT1_mp","target_t
ype":"LogicalRouter","is_valid":true}],{"section_type":"LAYER3","stateful":true,"is_default":fa
lse,"_system_owned":false,"_protection":"UNKNOWN","_revision":0}]
```

將規則 (myT1_mp_Rule1) 新增至區段 (FirewallSection-1) :

```
<182>1 2020-08-12T00:13:44.092Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO"
reqId="d4e7bdef-0cc6-45e9-8884-061b0f688fec" splitId="snErcGKF" splitIndex="1 of 2"
subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall",
Operation="UpdateSectionWithRules", Operation status="success", Old
value=[{"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597190995659,"autoplumbed":false,"en
forced_on":"LOGICALROUTER","tcp_strict":false,"category":"Default","resource_type":"FirewallSe
ction","id":"9808d1ec-
de08-48b3-8173-12f26fb0ae9c","display_name":"FirewallSection-1","applied_tos":
[{"target_id":"6562738e-73b9-4f21-9461-460ead581daf","target_display_name":"myT1_mp","target_t
ype":"LogicalRouter","is_valid":true}],{"section_type":"LAYER3","stateful":true,"rule_count":0,
"is_default":false,"_create_user":"admin","_create_time":1597190995657,"_last_modified_user":
"admin","_last_modified_time":1597190995657,"_system_owned":false,"_protection":"NOT_PROTECTED"
,"_revision":0}], New value=[{"9808d1ec-de08-48b3-8173-12f26fb0ae9c" {"rules":
[{"display_name":"myT1_mp_Rule1","sources_excluded":false,"destinations_excluded":
```

在區段 (FirewallSection-1) 中更新規則 (從 myT1_mp_Rule1 至 myT1_mp_Rule1_updated) :

```
<182>1 2020-08-12T00:15:31.078Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="eb880eee-5798-42fc-
a8aa-58b70e4aa152" splitId="WviId4ja" splitIndex="1 of 3" subcomp="manager" update="true"
username="admin"] UserName="admin", ModuleName="Firewall",
Operation="UpdateSectionWithRules", Operation status="success", Old
value=[{"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597190995659,"autoplumbed":false,"en
forced_on":"LOGICALROUTER","tcp_strict":false,"category":"Default","resource_type":"FirewallSe
ction","id":"9808d1ec-
de08-48b3-8173-12f26fb0ae9c","display_name":"FirewallSection-1","applied_tos":
[{"target_id":"6562738e-73b9-4f21-9461-460ead581daf","target_display_name":"myT1_mp","target_t
ype":"LogicalRouter","is_valid":true}],{"section_type":"LAYER3","stateful":true,"rule_count":1,
"is_default":false,"_create_user":"admin","_create_time":1597190995657,"_last_modified_user":
"admin","_last_modified_time":1597191224058,"_system_owned":false,"_protection":"NOT_PROTECTED"
,"_revision":1}{"section_id":"9808d1ec-
de08-48b3-8173-12f26fb0ae9c","resource_type":"FirewallRule","id":"536870914","display_name":"m
yT1_mp_Rule1","sources_excluded":
<182>1 2020-08-12T00:15:31.078Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="eb880eee-5798-42fc-
a8aa-58b70e4aa152" splitId="WviId4ja" splitIndex="2 of 3" subcomp="manager" update="true"
username="admin"]
false,"destinations_excluded":false,"action":"ALLOW","disabled":false,"logged":false,"directio
```



```
n": "IN_OUT", "ip_protocol": "IPV4_IPV6", "is_default": false}], New value=[{"9808d1ec-
de08-48b3-8173-12f26fb0ae9c" {"rules": [{"section_id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "resource_type": "FirewallRule", "id": "536870914", "display_name": "m
yT1_mp_Rule1_updated", "sources_excluded": false, "destinations_excluded": false, "action": "ALLOW",
"disabled": false, "logged": false, "direction": "IN_OUT", "ip_protocol": "IPV4_IPV6", "_revision": 1}]
, "resource_type": "FirewallSectionRuleList", "id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "display_name": "FirewallSection-1", "applied_tos":
[{"target_id": "6562738e-73b9-4f21-9461-460ead581daf", "target_display_name": "myT1_mp", "target_t
ype": "LogicalRouter", "is_valid": true}], "section_type": "LAYER3", "stateful": true, "is_default": fa
lse, "locked": false, "comments": "Default section unlock
comment", "lock_modified_by": "admin", "lock_modified_time": 1597190995659, "autoplumbed":
<182>1 2020-08-12T00:15:31.078Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="eb880eee-5798-42fc-
a8aa-58b70e4aa152" splitId="WviLd4ja" splitIndex="3 of 3" subcomp="manager" update="true"
username="admin"]
false, "enforced_on": "LOGICALROUTER", "tcp_strict": false, "category": "Default", "_system_owned": fa
lse, "_protection": "UNKNOWN", "_revision": 1}]}
```

從區段 (FirewallSection-1) 刪除規則 (myT1_mp_Rule2) :

```
<182>1 2020-08-12T00:18:05.341Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="bc95016c-5ec2-4b25-
ab17-0b10b6c5a4f0" splitId="damZHQkr" splitIndex="1 of 3" subcomp="manager" update="true"
username="admin"] UserName="admin", ModuleName="Firewall",
Operation="UpdateSectionWithRules", Operation status="success", Old
value=[{"locked": false, "comments": "Default section unlock
comment", "lock_modified_by": "admin", "lock_modified_time": 1597190995659, "autoplumbed": false, "en
forced_on": "LOGICALROUTER", "tcp_strict": false, "category": "Default", "resource_type": "FirewallSe
ction", "id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "display_name": "FirewallSection-1", "applied_tos":
[{"target_id": "6562738e-73b9-4f21-9461-460ead581daf", "target_display_name": "myT1_mp", "target_t
ype": "LogicalRouter", "is_valid": true}], "section_type": "LAYER3", "stateful": true, "rule_count": 2,
"is_default": false, "_create_user": "admin", "_create_time": 1597190995657, "_last_modified_user":
"admin", "_last_modified_time": 1597191475552, "_system_owned": false, "_protection": "NOT_PROTECTED"
, "_revision": 3} {"section_id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "resource_type": "FirewallRule", "id": "536870914", "display_name":
<182>1 2020-08-12T00:18:05.341Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="bc95016c-5ec2-4b25-
ab17-0b10b6c5a4f0" splitId="damZHQkr" splitIndex="2 of 3" subcomp="manager" update="true"
username="admin"]
"myT1_mp_Rule1_updated", "sources_excluded": false, "destinations_excluded": false, "action": "ALLOW
", "disabled": false, "logged": false, "direction": "IN_OUT", "ip_protocol": "IPV4_IPV6", "is_default":
false} {"section_id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "resource_type": "FirewallRule", "id": "536870915", "display_name": "m
yT1_mp_Rule2", "sources_excluded": false, "destinations_excluded": false, "action": "ALLOW", "disable
d": false, "logged": false, "direction": "IN_OUT", "ip_protocol": "IPV4_IPV6", "is_default": false}],
New value=[{"9808d1ec-de08-48b3-8173-12f26fb0ae9c" {"rules": [{"section_id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "resource_type": "FirewallRule", "id": "536870914", "display_name": "m
yT1_mp_Rule1_updated", "sources_excluded": false, "destinations_excluded": false, "action": "ALLOW",
"disabled": false, "logged": false, "direction": "IN_OUT", "ip_protocol": "IPV4_IPV6", "_revision": 3}]
, "resource_type": "FirewallSectionRuleList", "id": "9808d1ec-
de08-48b3-8173-12f26fb0ae9c", "display_name": "FirewallSection-1", "applied_tos"
<182>1 2020-08-12T00:18:05.341Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808d1ec-de08-48b3-8173-12f26fb0ae9c" level="INFO" reqId="bc95016c-5ec2-4b25-
ab17-0b10b6c5a4f0" splitId="damZHQkr" splitIndex="3 of 3" subcomp="manager" update="true"
```

```
username="admin"] :
[{"target_id":"6562738e-73b9-4f21-9461-460ead581daf","target_display_name":"myT1_mp","target_t
ype":"LogicalRouter","is_valid":true},"section_type":"LAYER3","stateful":true,"is_default":fa
lse,"locked":false,"comments":"Default section unlock
comment","lock_modified_by":"admin","lock_modified_time":1597190995659,"autoplumbed":false,"en
forced_on":"LOGICALROUTER","tcp_strict":false,"category":"Default","_system_owned":false,"_pro
tection":"UNKNOWN","_revision":3}]
```

刪除包含規則 (myT1_mp_Rule2) 的區段 (FirewallSection-1) :

```
<182>1 2020-08-12T00:21:27.646Z manager1 NSX 1503 - [nsx@6876 audit="true" comp="nsx-manager"
level="INFO" reqId="781f43d5-0b4c-494e-89a1-cbc2998fc232" subcomp="manager" username="admin"]
UserName="admin", ModuleName="NSX-Firewall", Operation="DELETE", Operation status="success",
Old value=[FirewallSectionLock [Id=15b61818-2a65-48cf-a98e-7c2f3fcc845, sectionId=9808dlec-
de08-48b3-8173-12f26fb0ae9c, sectionRevision=0, locked=false, comments=Default section unlock
comment, created_by=admin, create_time=1597190995659, last_modified_by=admin,
last_modified_time=1597190995659]]
<182>1 2020-08-12T00:21:27.669Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808dlec-de08-48b3-8173-12f26fb0ae9c" level="INFO"
reqId="781f43d5-0b4c-494e-89a1-cbc2998fc232" splitId="u3AofFMr" splitIndex="1 of 2"
subcomp="manager" update="true" username="admin"] UserName="admin", ModuleName="Firewall",
Operation="DeleteSection", Operation status="success", Old
value=[{"locked":false,"autoplumbed":false,"enforced_on":"LOGICALROUTER","tcp_strict":false,"c
ategory":"Default","resource_type":"FirewallSection","id":"9808dlec-
de08-48b3-8173-12f26fb0ae9c","display_name":"FirewallSection-1","applied_tos":
[{"target_id":"6562738e-73b9-4f21-9461-460ead581daf","target_display_name":"myT1_mp","target_t
ype":"LogicalRouter","is_valid":true},"section_type":"LAYER3","stateful":true,"rule_count":1,
"is_default":false,"_create_user":"admin","_create_time":1597190995657,"_last_modified_user":
"admin","_last_modified_time":1597191671601,"_system_owned":false,"_protection":"NOT_PROTECTED"
,"_revision":6}{ "section_id":"9808dlec-
de08-48b3-8173-12f26fb0ae9c","resource_type":"FirewallRule","id":"536870916","display_name":"m
yT1_mp_Rule1","sources_excluded":false,"destinations_excluded":false,"action":"ALLOW","disable
d":false,"logged":false,"direction":
<182>1 2020-08-12T00:21:27.669Z manager1 NSX 1503 FIREWALL [nsx@6876 audit="true" comp="nsx-
manager" entId="9808dlec-de08-48b3-8173-12f26fb0ae9c" level="INFO"
reqId="781f43d5-0b4c-494e-89a1-cbc2998fc232" splitId="u3AofFMr" splitIndex="2 of 2"
subcomp="manager" update="true" username="admin"]
"IN_OUT","ip_protocol":"IPV4_IPV6","is_default":false>null], New value=["9808dlec-
de08-48b3-8173-12f26fb0ae9c" {"cascade":true}]
```

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-products.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**。

尋找遠端伺服器的 SSH 指紋

在進行某些涉及與遠端伺服器通訊的工作時，您必須提供遠端伺服器的 SSH 指紋。SSH 指紋衍生自遠端伺服器的主機金鑰。

若要使用 SSH 連線，NSX Manager 和遠端伺服器必須具有共同的主機金鑰類型。NSX Manager 支援 ECDSA (256 位元) 金鑰。此金鑰的預設位置為 `/etc/ssh/ssh_host_ecdsa_key.pub`。

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。您可以要求遠端伺服器的管理員提供伺服器的 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。

程序

- 1 以 root 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 找出 ECDSA (256 位元) 金鑰。金鑰的預設位置為 `/etc/ssh/ssh_host_ecdsa_key.pub`。

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

- 3 取得金鑰的指紋。

```
ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub | awk '{print $2}'
```

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。

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。

存取 NSX Manager 時的驗證方法

NSX Manager 支援以下驗證方法。如需有關驗證方法的詳細資訊，請參閱《NSX-T Data Center API 指南》。

- HTTP 基本驗證
- 以工作階段為基礎的驗證
- 使用 X.509 憑證和主體身分識別進行驗證
- VMware Cloud on AWS (VMC) 中的驗證

以工作階段為基礎的驗證方法 (從瀏覽器存取 NSX Manager 時會使用此方法) 需要來源 IP 持續性 (來自用戶端的所有要求都必須前往相同的 NSX Manager)。其他方法則不需要來源 IP 持續性 (來自用戶端的要求可以前往不同的 NSX Manager)。

建議

- 在負載平衡器上建立一個設定了來源 IP 持續性的 VIP，以處理所有驗證方法。
- 如果您的應用程式或指令碼可能會向 NSX Manager 產生大量要求，請為這些應用程式或指令碼建立另一個不具有來源 IP 持續性的 VIP。第一個 VIP 僅用於透過瀏覽器存取 NSX Manager。

VIP 必須具有以下組態：

- 類型：Layer4-TCP
- 連接埠：443
- 集區：NSX Manager 集區
- 持續性：第一個 VIP 的來源 IP 持續性。第二個 VIP (如果存在) 則沒有。

- Header3
 - 名稱：接受
 - 值：應用程式/json

會指出 NSX Manager 正在執行的回應如下：

```
"healthy" : true
```

請注意，回應格式為 "healthy"<space>:<space>true。

如果變更在 Header1 中所指定使用者的密碼，則必須相應地更新 Header1。

進行 Proxy 設定

您可以設定 NSX-T Data Center 環境的 Proxy 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 選取**系統 > Proxy 設定**。
- 3 在**配置資料**行中，選取 HTTP 或 HTTPS。
- 4 在**主機資料**行中，輸入 IP 位址。
- 5 在**連接埠資料**行中，輸入連接埠號碼。
- 6 在**使用者名稱資料**行中，輸入使用者名稱。
- 7 在**密碼資料**行中，輸入密碼。
- 8 按一下**儲存**。

檢視容器相關的資訊

您可以檢視容器相關的資訊，例如 Hyperbus 狀態或 NCP (NSX Container Plug-in) 叢集的狀態。

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 選取導覽面板中的**系統 > 網狀架構 > 節點**。
- 3 若要查看 Hyperbus 和 NSX 節點代理程式狀態，請按一下**主機傳輸節點索引標籤**。
- 4 按一下 NSX 節點代理程式執行所在的節點。
- 5 按一下**監控索引標籤**。

Hyperbus 狀態欄位在頁面底部旁邊。隨即顯示 Hyperbus 狀態和每個節點代理程式 VIFID 的狀態。

- 6 若要檢視 NCP 叢集的相關資訊，請按一下**NCP 叢集索引標籤**。

對於每個叢集，系統會顯示叢集名稱、識別碼、狀態和類型。

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 : UI 逐步解說](#)
- [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](#)
- [NSX Cloud 常見問題和疑難排解](#)

Cloud Service Manager : UI 逐步解說

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：

概觀

可透過按一下**雲端 > 概觀**來存取您的公有雲帳戶。

此頁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。這可讓您在 CSM 中檢視公有雲詳細目錄。它也會顯示由 NSX-T Data Center 管理的虛擬機器數目及其狀態。 如需指示，請參閱《NSX-T Data Center 安裝指南》中的〈新增公有雲帳戶〉。
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。 如需指示，請參閱《NSX-T Data Center 安裝指南》中的〈部署或連結 PCG〉。
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單一虛擬管理介面視圖：

- 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。

帳戶

您可以新增公有雲帳戶，方法是導覽至 CSM 的雲端 > <您的公有雲> > 帳戶區段。您也可以檢視已新增的公有雲帳戶相關資訊。

每張卡片各代表您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

區域

導覽至雲端 > <您的公有雲> > 區域，以查看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**。

如果您在公有雲區域中沒有任何 VPC/VNet，則該區域不會顯示在 CSM 中。

VPC 或 VNet

導覽至雲端 > <您的公有雲> > VPC 或 VNet，以在公有雲帳戶或訂閱中檢視 VPC 或 VNet。

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。

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 Data Center 中的覆疊區段。

備註 NSX Cloud 目前版本中不支援此功能。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。
 - 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 公有雲端閘道**〉。

執行個體

雲端 > <您的公有雲> **執行個體**區段會顯示 VPC 或 VNet 中 NSX 管理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。在其他詳細資料中，您會看到下列內容：
 - **規則實現**：對於在原生雲端強制執行模式中管理的工作負載虛擬機器，您可以查看在 NSX Manager 中建立的 DFW 規則狀態。實現狀態可以是成功或失敗。您可以按一下失敗狀態，以檢視錯誤訊息。如需詳細資料，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](#)。

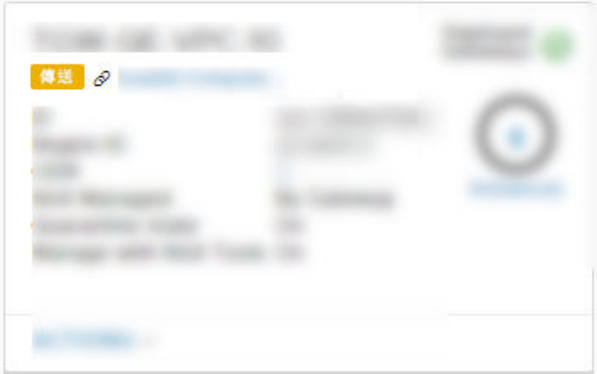
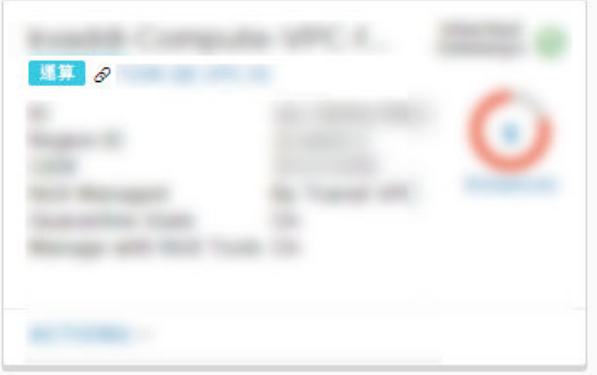
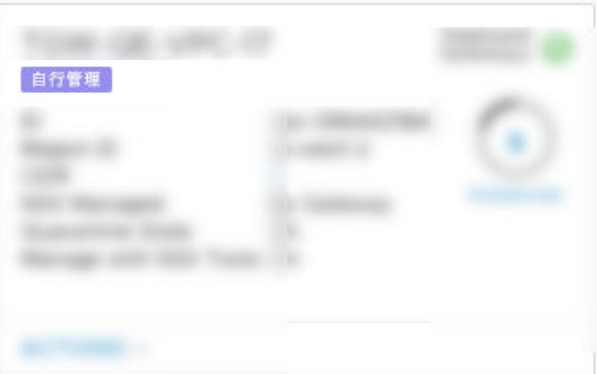
您可以在 CSM 使用者管理的清單中新增或移除執行個體。如需詳細資料，請參閱[虛擬機器的使用者管理清單](#)。

CSM 圖示

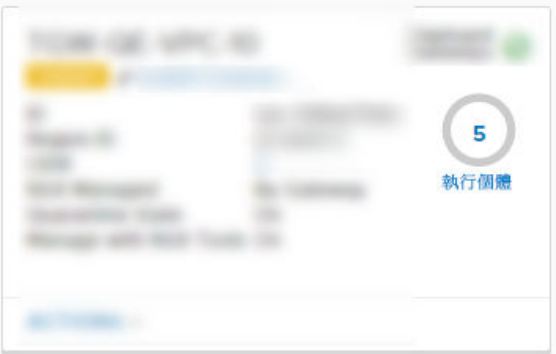
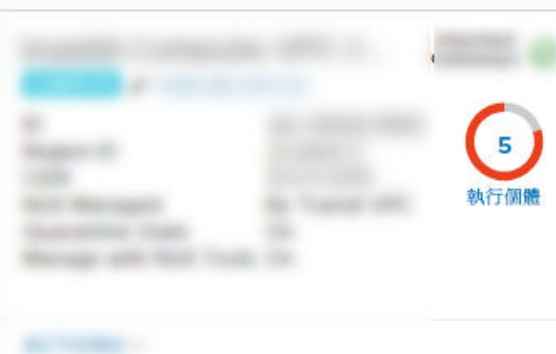
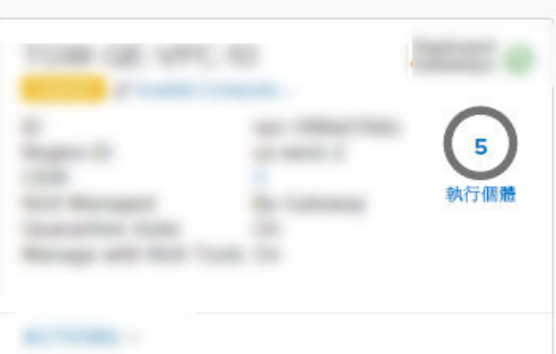
CSM 會使用說明性圖示來顯示公有雲建構的狀態和健全狀況。


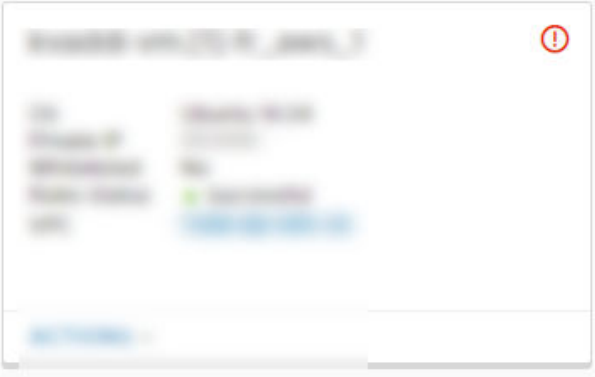
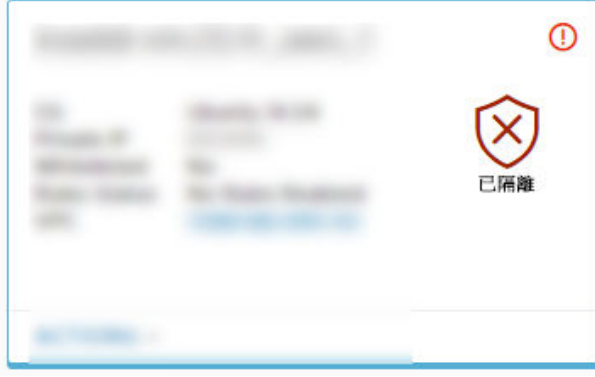
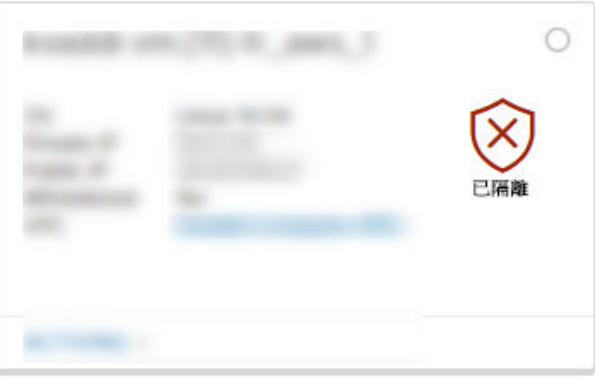
備註 在原生雲端強制執行模式中：一律會啟用隔離原則，且所有虛擬機器一律受 NSX 管理。在此模式中，僅會套用為 NSX 管理的虛擬機器啟用隔離原則的狀態。

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
<p>VPC/VNet</p> 	<p>傳送 VPC/VNet</p>
	<p>計算 VPC/VNet</p>
	<p>自行管理 VPC/VNet</p>

CSM 區段和圖示	說明
	<p>VPC/VNet 顯示狀況良好的 PCG</p>
	<p>VPC/VNet 顯示處於錯誤狀態的 PCG</p>
	<p>VPC/VNet 顯示一個 PCG 處於錯誤狀態，另一個狀況良好。</p>
	<p>VPC/VNet 顯示 NSX 管理的虛擬機器。</p>

CSM 區段和圖示	說明
	<p>VPC/VNet 顯示未受管理的虛擬機器。</p>
	<p>VPC/VNet 顯示發生錯誤的虛擬機器。</p>
	<p>VPC/VNet 顯示已關閉電源的虛擬機器。</p>
<p>執行個體</p>	

CSM 區段和圖示	說明
	<p>NSX 管理的虛擬機器沒有錯誤。</p>
	<p>NSX 管理的虛擬機器發生錯誤，且隔離原則已停用。</p>
	<p>NSX 管理的虛擬機器發生錯誤，且隔離原則已啟用。</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。
- 您必須擁有 NSX Data Center Enterprise Plus 授權。

程序

- 1 在瀏覽器中，登入 CSM。
- 2 當安裝精靈中出現提示時，按一下**開始設定**。
- 3 在 [NSX Manager 認證] 畫面中，輸入下列詳細資料：

選項	說明
NSX Manager 主機名稱	輸入 NSX Manager 的完整網域名稱 (FQDN) (如果有)。您也可以輸入 NSX Manager 的 IP 位址。
管理員認證	輸入 NSX Manager 的企業管理員使用者名稱和密碼。
管理員指紋	(選擇性) 輸入 NSX Manager 的指紋值。如果您將此欄位保留空白，系統會識別指紋，並顯示在下一個畫面中。

- 4 (選擇性) 如果您未提供 NSX Manager 的指紋值，或者值不正確，則會顯示**驗證指紋**畫面。選取核取方塊以接受系統探索到的指紋。
- 5 按一下**連線**。

備註 如果安裝精靈中遺失此設定或您想要變更相關聯的 NSX Manager，請登入 CSM，按一下**系統 > 設定**，然後在標題為**相關聯的 NSX 節點**面板上按一下**設定**。

CSM 會確認 NSX Manager 指紋並建立連線。

- 6 (選擇性) 設定 Proxy 伺服器。請參閱 [\(選用\) 設定 Proxy 伺服器](#) 中的指示。

(選用) 設定 Proxy 伺服器

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

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

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

您可以選擇以下層級的驗證：

- 認證式驗證。
- 適用於 HTTPS 攔截的憑證式驗證。
- 無驗證。

程序

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

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

- 2 在 [設定 Proxy 伺服器] 畫面中，輸入下列詳細資料：

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

系統 > 公用程式

可用公用程式如下。

備份和還原

遵循相同指示以備份和還原 CSM，與 NSX Manager 的方式相同。請參閱 [備份和還原 CSM 應用裝置](#)。

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》。

備份和還原 CSM 應用裝置

您可以備份 CSM 應用裝置，並從備份還原。

目前僅支援 CSM 的 IP 位址備份和還原。

備份 CSM

設定備份伺服器後，您可以手動備份 CSM 應用裝置或設定週期性備份。

您僅能從 IP 位址備份還原 CSM 應用裝置。請勿設定 CSM 應用裝置的 FQDN。

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 金鑰作為指紋。請參閱 [尋找遠端伺服器的 SSH 指紋](#)。
- 確定您要儲存備份的目錄路徑已存在。您無法使用根目錄 (/)。

程序

1 從瀏覽器以 admin 權限登入 CSM，網址為 <https://<csm-ip-address>>。

2 選取 **系統 > 公用程式 > 工具**。

3 在 **備份索引** 標籤上，按一下 **設定**。

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 組態變更選項，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。

您可以指定用於偵測資料庫組態變更的時間間隔。有效範圍為 5 分鐘到 1,440 分鐘 (24 小時)。

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。

如果備份伺服器已滿，請參閱移除備份的指示：[移除舊備份](#)。

從備份還原 CSM

如果您有備份，即可以還原 CSM 應用裝置。

在全新安裝 CSM 時必須還原備份。如果舊 CSM 節點仍然可用，您必須關閉其電源，然後再開始還原程序。

備註 您僅能從 IP 位址備份還原 CSM。CSM 不支援 FQDN 備份。

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

程序

- 1 如果舊 CSM 節點仍然可用，請關閉其電源。
- 2 使用原始 CSM 節點的相同 IP 位址部署新的 CSM 節點。
- 3 在瀏覽器中，以 admin 權限登入新的 CSM 應用裝置。
- 4 選取**系統 > 公用程式 > 工具**。
- 5 按一下**還原索引**標籤。
- 6 按一下**立即還原**。還原精靈隨即開啟。
- 7 選取**必要條件**畫面上的核取方塊。
- 8 提供遠端備份伺服器的詳細資料：
 - a 輸入 IP 位址或主機名稱。
 - b 視需要變更連接埠號碼。
預設值為 22。
 - c 若要登入伺服器，請輸入使用者名稱和密碼。
 - d 在**備份目錄**文字方塊中，輸入用來儲存備份的絕對目錄路徑。

- e 輸入用來加密備份資料的複雜密碼。
- f 輸入儲存備份之伺服器的 SSH 指紋。

9 按下一步。

- 10 選取備份。您也可以透過登入備份檔案伺服器來取得可用備份的清單。請參閱[列出可用的備份](#)。在這些指示中將 NSX Manager 取代為 CSM，例如，當要求您登入 NSX Manager 以執行 CLI 命令時，請改為登入 CSM。

11 按一下還原。

您的連線會中斷，直到還原完成。隨即顯示還原作業的狀態。還原作業完成後會出現 [還原完成] 畫面，其中會顯示還原的結果、備份檔案的時間戳記，以及還原作業的開始和結束時間。如果還原失敗，畫面會顯示發生失敗的步驟。

您也可以透過選取記錄檔，判定還原失敗的原因。執行 `get log-file syslog` 以檢視系統記錄檔。

若要重新啟動 CSM，請執行 `service nsx-cloud-service-manager restart` 命令。

若要將 CSM 節點重新開機，請執行 `reboot` 命令。

- 12 部署新的 CSM 節點後，刪除您在步驟 1 中關閉的原始 CSM 虛擬機器。

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[第 18 章 驗證和授權](#)。

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 23-1. 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 中分散式防火牆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 <code>gw</code> 安全群組套用至各自的 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><code>vm</code> 安全群組會根據其目前狀態以及隔離原則為啟用或停用，套用至由 NSX 管理的虛擬機器：</p> <ul style="list-style-type: none"> ■ Microsoft Azure 中的 <code>default-vnet-<vnet-id>-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**。
- 4 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，但隔離安全群組中的規則：`default-vnet-<vnet-id>-sg` (Microsoft Azure) 和 `default` (AWS) 的設定類似於預設公有雲安全群組，以允許 VPC/VNet 內的所有項目，並拒絕所有其他輸入流量。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)，請將其新增至 CSM 中的「使用者管理」清單。請參閱[虛擬機器的使用者管理清單](#)。

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 23-2. 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 <code>nsx.network=default</code> ?	虛擬機器是否已新增至「使用者管理」清單?	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
虛擬機器可能已標記或未標記	已新增至「使用者管理」清單。	保留現有公有雲安全群組，因為 NSX Cloud 不會對「使用者管理」清單中的虛擬機器採取任何動作。
未標記	未新增至「使用者管理」清單	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	未新增至「使用者管理」清單	<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>default-vnet-<vnet-id>-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仍會保留在預設安全群組中。</p>

下表說明如果先前啟用了隔離原則，而現在已停用，NSX Cloud 將如何管理虛擬機器的公有雲安全群組：

表 23-3. 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 <code>nsx.network=default</code> ?	虛擬機器是否在「使用者管理」清單中？	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後的公有雲安全群組
虛擬機器可能已標記或未標記	是，虛擬機器在「使用者管理」清單中	任何現有的公有雲安全群組	保留現有公有雲安全群組，因為 NSX Cloud 不會對「使用者管理」清單中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位於「使用者管理」清單的虛擬機器，則必須手動將其移至 AWS 中的 default 安全群組，以及 Microsoft Azure 中的 default-vnet- <code><vnet-id>-sg</code> 安全群組。
未標記	未新增至「使用者管理」清單	default-vnet- <code><vnet-id>-sg</code> (Microsoft Azure) 或 default (AWS)	停用隔離原則時會保留在現有的安全群組中，因為其未標記且不會被視為受 NSX 管理。您可以視需要將任何其他安全群組手動指派至此虛擬機器。
已標記	未新增至「使用者管理」清單	vm-underlay-sg 或 default-vnet- <code><vnet-id>-sg</code> (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。

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，請將虛擬機器新增至 CSM 的「使用者管理」清單。請參閱 [虛擬機器的使用者管理清單](#)。

備註 將虛擬機器從使用者管理的清單中移除，會導致虛擬機器還原為 NSX Cloud 指派的安全群組。

表 23-4. 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> ?	虛擬機器是否在「使用者管理」清單中？	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	未新增至「使用者管理」清單	<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 default-vnet-<vnet-ID>-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	未新增至「使用者管理」清單	Microsoft Azure 中的 default-vnet-<vnet-ID>-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	是，虛擬機器在「使用者管理」清單中	保留現有公有雲安全群組，因為 NSX Cloud 不會對「使用者管理」清單中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 23-5. 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> ?	虛擬機器是否在「使用者管理」清單中？	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	未新增至「使用者管理」清單	任何現有的公有雲安全群組	default-vnet-<vnet-ID>-sg (Microsoft Azure) 或 default (AWS)
已標記	未新增至「使用者管理」清單	vm-underlay-sg 或 default-vnet-<vnet-ID>-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	是，虛擬機器在「使用者管理」清單中	任何現有的公有雲安全群組。	保留現有公有雲安全群組，因為 NSX Cloud 不會對「使用者管理」清單中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 23-6. 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？	虛擬機器是否已新增至「使用者管理」清單？	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	未新增至「使用者管理」清單	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	未新增至「使用者管理」清單	Microsoft Azure 中的 <code>default-vnet-<vnet-ID>-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>default-vnet-<vnet-ID>-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	已新增至「使用者管理」清單	保留現有公有雲安全群組，因為 NSX Cloud 不會對新增至「使用者管理」清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		

虛擬機器的使用者管理清單

將虛擬機器新增至**使用者管理**清單，是可供公有雲詳細目錄中所有工作負載虛擬機器從 CSM 使用的選項。您可以在虛擬機器管理模式：NSX 強制執行模式和原生雲端強制執行模式中，將虛擬機器新增至**使用者管理**。

為何要將虛擬機器新增至使用者管理清單？

- 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，請先將此類虛擬機器新增至**使用者管理**清單，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，請將此類虛擬機器新增至**使用者管理**清單，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 管理的虛擬機器新增至**使用者管理**清單，例如 DNS 轉寄站與 Proxy 伺服器。

如何使用使用者管理清單

請依照下列指示，將虛擬機器新增至**使用者管理**清單或將其移除。

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 選取您要從**使用者管理**清單新增或移除的虛擬機器 (執行個體)。
- 4 按一下**動作**，然後選取**新增至使用者管理的清單**或從**使用者管理的清單**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

新增至**使用者管理**清單中的每個虛擬機器仍會在將其新增至**使用者管理**清單之前獲指派的安全群組中。此時您可以視需要將任何其他安全群組套用於虛擬機器。無論隔離原則的狀態為何，NSX Cloud 都會忽略**使用者管理**清單中的虛擬機器。

如果您在原生雲端強制執行模式中從**使用者管理**清單中移除虛擬機器，或在 NSX 強制執行模式中從**使用者管理**清單中移除由 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。

- SUSE Linux Enterprise Server (SLES) 12 SP3
- 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 23-7. 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
<input type="checkbox"/> 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。
<input type="checkbox"/> 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。	
<input type="checkbox"/> (選用) 如果您已將虛擬機器新增至 CSM 中的「使用者管理」清單，請從「使用者管理」清單中移除要置於 NSX 管理下的虛擬機器。	請參閱 如何使用使用者管理清單 。

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。您也可以套用在套用標籤後將這些 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：
 - a 如果使用 AWS，請移至**雲端 > AWS > VPC**。按一下傳送 VPC 或計算 VPC。
 - b 如果使用 Microsoft Azure，請移至**雲端 > Azure > VNet**。按一下已部署且正在執行一個或一對 PCG 的 VNet。

附註： 傳送 VPC/VNet 用於部署並執行一個或一對 PCG。計算 VPC/VNet 會連結到傳送 VPC/VNet，並且可以使用其中部署的 PCG。

- 2 從畫面的 **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 `jumphost` 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，您可以在安裝之前，將虛擬機器新增至 CSM 中的「使用者管理」清單，並在安裝後將其從「使用者管理」清單中移除。
- 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。
- 如果您是在網絡視圖中，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。

當您啟動 AWS EC2 執行個體時，您可以選擇將 `user data` 傳遞至可用來執行一般自動設定工作的執行個體，包括在執行個體啟動後執行指令碼。您可以將兩種類型的使用者資料傳遞至 AWS EC2：Shell 指令碼和 `cloud-init` 指示詞。

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。

必要條件

使用 User Data 安裝 NSX Tools 之前，請確定傳送與計算 VPC 對等。必須符合此條件，才能從啟動的執行個體解析在下載命令中指定的 FQDN (例如 `nsx-gw.vmware.local`)。

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**。您也可以複製並貼上下列 Shell 指令碼：

```
#!/bin/bash
sudo wget http://nsx-gw.vmware.local:8080/factory_default/linux/install_nsx_vm_agent.sh
sudo chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

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 `default-vnet-<vnet-ID>-sg` 網路安全群組 (Microsoft Azure)。
- 「使用者管理」清單中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 `default-vnet-<vnet-ID>-sg` 網路安全群組 (Microsoft Azure)。
- 未受管理的虛擬機器和「使用者管理」清單中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 23-8. 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。

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。

若要對 NSX 所管理的工作負載虛擬機器套用分散式防火牆規則，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](#)。

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

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

- 2 建立東西向分散式防火牆原則與規則，然後套用至您建立的群組。請參閱[新增分散式防火牆](#)。您也可以使用內容設定檔，來建立應用程式識別碼和 FQDN/URL 的特定規則。建立 FQDN/URL 內容設定檔時，可使用預先定義的公有雲 FQDN/URL 清單。如需詳細資料，請參閱[第 7 層內容設定檔](#)。

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 23-9. 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"/> 會從 CSM 的「使用者管理」清單中移除工作負載虛擬機器 (如果您要讓其由 NSX-T 安全性原則管理)。	
<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

您可以針對原生雲端強制執行模式中的工作負載虛擬機器設定 NSX Manager 中的安全性原則。

從 NSX-T Data Center 3.0 開始，您可以從不同帳戶或訂閱，在 VPC/VNet 中建立安全性原則和規則。

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。

必要條件

確認您在原生雲端強制執行模式中有傳送或計算 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 default-vnet-<vnet-ID>-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。

- 2 在 NSX Manager 中，輸入來源、目的地或套用至欄位，建立具有這些群組的分散式防火牆 (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。

原生雲端強制執行模式中工作負載虛擬機器的 DFW 規則不支援 L7 內容設定檔。

- 3 在 CSM 中，從「使用者管理」清單中移除要置於 NSX 管理下的虛擬機器。如需指示，請參閱[如何使用使用者管理清單](#)。

備註 將虛擬機器新增至「使用者管理」清單是一個手動步驟，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新增至「使用者管理」清單，則不需要將其從中移除。

- 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)。
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 TCP、UDP 和 ICMP。

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拒絕的清單。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 23-10.

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	請參閱在管理程式模式中設定 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 23-10. (續)

NSX-T Data Center 功能	詳細資料	NSX Cloud 附註
連接埠鏡像	請參閱在管理程式模式中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 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，請參閱在[管理程式模式中管理虛擬機器的標籤](#)。

表 23-11. 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 23-12.

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 23-12. (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=AbcdefghijklmnopqrstuvwxyzAb23690hgjguytreswqacvbcdefghijklmnopqrstuvwxyz	否 (值超過 65 個字元)	無
nsx.name=Tester	否 (金鑰具有前置詞 nsx)	無

如何在 NSX Manager 中使用標籤

- 請參閱在管理程式模式中管理虛擬機器的標籤。
- 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					

工作負載虛擬機器在 NSX 強制執行模式 下的服務插入

NSX Cloud 支援在公有雲中對 NSX 管理的工作負載虛擬機器 (處於 NSX 強制執行模式下) 使用第三方服務。

NSX Cloud 支援對下列作業使用服務插入：

- 透過傳送 VPC/VNet 中裝載的服務應用裝置，從工作負載虛擬機器傳輸南北向流量。
- 將 PCG 的 VPN 流量傳輸至內部部署 Edge 或閘道。此流量也可透過傳送 VPC/VNet 中的服務應用裝置進行路由。

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之組態的概觀。

表 23-13. 針對 NSX 強制執行模式中 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
如果您想要設定南北向流量的服務插入，請依照下列指示進行初始設定。	最好在傳送 VPC 或 VNet (已在其中部署 PCG) 中設定公有雲中的服務應用裝置。	請參閱第三方服務應用裝置和公有雲的特定指示。
	在 NSX-T Data Center 中登錄第三方服務。	請參閱 建立服務定義和對應的虛擬端點
	使用 /32 虛擬服務 IP 位址 (VSIP) 建立服務的虛擬執行個體端點，以僅供服務應用裝置進行服務插入。VSIP 不應與 VPC 或 VNet 的 CIDR 範圍發生衝突。此 VSIP 透過 BGP 向 PCG 通告。	請參閱 建立服務定義和對應的虛擬端點
	建立服務應用裝置和 PCG 之間的 IPSec VPN 通道。	請參閱 設定 IPSec VPN 工作階段
	設定 PCG 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

表 23-13. 針對 NSX 強制執行模式中 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
依照下列指示，針對公有雲到內部部署的 VPN 流量進行初始設定。	在 PCG 與內部部署 Edge 或閘道之間建立 VPN 通道。	請參閱在 NSX 強制執行模式中設定 VPN。
依照下列指示，在初始設定的過程中設定兩種類型的服務插入。	使用設定為 不重新導向 的動作，建立最低優先順序的預設全部擷取規則。這可確保不會在 PCG 和服務應用裝置的 VTI 介面上重新導向任何封包。	請參閱設定重新導向規則。
根據各種類型之服務插入使用案例的需求，依照這些指示操作。	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。這些規則會套用至 PCG 的上行連接埠以用於南北向服務插入，並套用至 PCG 的 VTI 介面以用於內部部署的流量。	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

您必須在服務插入的初始設定中，設定預設重新導向規則。

建立服務定義和對應的虛擬端點

您必須使用 NSX Manager API，為公有雲中的服務應用裝置建立服務定義和虛擬端點。

必要條件

挑選出 /32 保留的 IP 位址做為公有雲中服務應用裝置的虛擬端點，例如 100.100.100.100/32。這被稱為虛擬服務 IP (VSIP)。

備註 如果在高可用性配對中已部署服務應用裝置，則不會建立另一個服務定義，而是在設定 BGP 期間向 PCG 進行通告時使用相同的 VSIP。

程序

- 1 若要為服務應用裝置建立服務定義，則使用用於授權的 NSX Manager 認證執行下列 API 呼叫：

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

範例要求：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

範例回應：

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
  "_protection": "REQUIRE_OVERRIDE",
}
```

```

    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 若要為服務應用裝置建立虛擬端點，則使用用於授權的 NSX Manager 認證執行下列 API 呼叫：

```

PATCH https://{{NSX Manager-IP}}policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

範例要求：

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  "service_names": [
    "Service_Appliance1"
  ]
}

```

範例回應：

```
200 OK
```

備註 步驟 1 中的 `display_name` 必須與步驟 2 中的 `service_names` 相符。

後續步驟

[設定 IPsec VPN 工作階段](#)

設定 IPsec VPN 工作階段

設定 PCG 和服務應用裝置之間的 IPsec VPN 工作階段。

必要條件

- 一個 PCG 或 PCG 的 HA 配對必須在傳送 VPC/VNet 中部署。
- 必須在公有雲中設定服務應用裝置，最好是在傳送 VPC/VNet 中設定。

程序

1 導覽至網路 > VPN

- 2 新增 IPsec 類型的 **VPN 服務**，並注意特定於 NSX Cloud 的下列組態選項。如需其他詳細資料，請參閱 [新增 IPsec VPN 服務](#)。

選項	說明
名稱	此 VPN 服務的名稱可用來設定本機端點和 IPsec VPN 工作階段。請記下該名稱。
服務類型	確認此值會設為 IPsec。
第 0 層閘道	選取為傳送 VPC/VNet 自動建立的第 0 層閘道。其名稱中包含您的 VPC/VNet 識別碼，例如 cloud-t0-vpc-6bcd2c13。

- 3 為 PCG 新增**本機端點**。本機端點的 IP 位址是傳送 VPC/VNet 中部署的 PCG 的 `nsx:local_endpoint_ip` 標籤的值。登入傳送 VPC/VNet 以取得該值。請注意特定於 NSX Cloud 的下列組態，並參閱 [新增本機端點](#) 以瞭解其他詳細資料。

選項	說明
名稱	本機端點名稱可用來設定 IPsec VPN 工作階段。請記下該名稱。
VPN 服務	選取步驟 2 中新增加的 VPN 服務。
IP 位址	登入 AWS 主控台或 Microsoft Azure 入口網站，以尋找此值。它是套用到 PCG 的上行介面的標籤 <code>nsx:local_endpoint_ip</code> 的值。

- 4 在 PCG 和公有雲中的服務應用裝置 (最好是裝載於傳送 VPC/VNet 中) 之間建立**以路由為基礎的 IPsec 工作階段**。

選項	說明
類型	確認此值會設為 以路由為基礎 。
VPN 服務	選取步驟 2 中新增加的 VPN 服務。
本機端點	選取步驟 3 中建立的本機端點。
遠端 IP	輸入服務應用裝置的私人 IP 位址。 備註 如果可以使用公用 IP 位址存取您的服務應用裝置，請將公用 IP 位址指派給 PCG 上行介面的本機端點 IP (也稱為次要 IP)。
通道介面	此子網路必須與 VPN 通道的服務應用裝置子網路相符。輸入您在 VPN 通道的服務應用裝置中設定的子網路值或記下在此處輸入的值，並確保在服務應用裝置中設定 VPN 通道時使用相同的子網路。 備註 在此通道介面上設定 BGP。請參閱 設定 BGP 和路由重新分配 。
遠端識別碼	輸入公有雲中服務應用裝置的私人 IP 位址。
IKE 設定檔	IPsec VPN 工作階段必須與 IKE 設定檔相關聯。如果已建立設定檔，請從下拉式功能表中選取該設定檔。您也可以使用預設設定檔。

後續步驟

設定 BGP 和路由重新分配

設定 BGP 和路由重新分配

透過 IPsec VPN 通道設定 PCG 和服務應用裝置之間的 BGP。

在 PCG 與服務應用裝置之間建立的 IPsec VPN 通道介面上設定 BGP 芳鄰。如需更多詳細資料，請參閱 [設定 BGP](#)。

您需要以類似方式在服務應用裝置上設定 BGP。如需詳細資料，請參閱公有雲中特定服務的說明文件。

接下來，設定路由重新分配，如下所示：

- PCG 向服務應用裝置通告其預設路由 (0.0.0.0/0)。
- 服務應用裝置向 PCG 通告 VSIP。這是登錄服務時使用的相同 IP 位址。請參閱 [建立服務定義和對應的虛擬端點](#)。

備註 如果您的服務應用裝置在高可用性配對中部署，請從兩個服務應用裝置通告相同的 VSIP。

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 層間道上的靜態路由。



後續步驟

設定重新導向規則

設定重新導向規則

您必須在服務插入的初始設定中，設定預設重新導向規則。

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。

重新導向規則有以下兩種類型：

- 1 在初始服務插入設定的過程中，您必須建立全部擷取規則，以防止 PCG 與服務應用裝置之間的 VPN 通道進行 VTI 介面的流量重新導向。此規則必須盡可能具有最低的優先順序，且對於服務插入的兩種使用案例都必須建立此規則。
- 2 第二個規則會針對服務應用裝置的流量設定特定的重新導向。您可以調整此規則，並視需要新增其他規則。

程序

1 若要新增預設的全部擷取規則以完成一次性設定，請執行下列步驟：

- a 導覽至安全性 > 南北向防火牆 > 網路自我檢查 (N-S)
- b 按一下**新增原則**。

選項	說明
名稱	提供描述性名稱，例如 <code>Default_No-Redirect-Policy</code> 。
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。
套用至：	選取 PCG 的第 0 層閘道。

- c 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	任何
目的地	任何
套用至	選取 PCG 與服務應用裝置之間的 VTI 介面。
動作	選取 不重新導向 。

重要 此規則必須盡可能具有最低的優先順序。

2 對於第二個規則，請執行下列步驟：

- a 導覽至安全性 > 南北向防火牆 > 網路自我檢查 (N-S)
- b 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， AWS 虛擬機器的內部部署服務插入 或 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。
套用至：	選取 PCG 的第 0 層閘道。

- c 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之目的地 IP 位址或服務 (例如 YouTube) 的清單。
套用至	<ul style="list-style-type: none"> ■ 如果您要對公有雲中的服務應用裝置使用南北向服務插入：選取作用中和待命 PCG 的上行連接埠。 ■ 如果您要使用對內部部署的 VPN 流量：選取作用中和待命 PCG 對內部部署服務應用裝置的 VTI 介面。
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 23-14.

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>
```

在原生雲端強制執行模式中設定 VPN

您可以遵循此工作流程，在 PCG 與遠端端點之間建立 VPN 通道。這些指示僅適用於在原生雲端強制執行模式中受到管理的工作負載虛擬機器。

必要條件

- 在 AWS 中：確認您已在原生雲端強制執行模式中部署 VPC。這必須是傳送或自我管理的 VPC。AWS 中的計算 VPC 不支援 VPN。
- 在 Microsoft Azure 中：確認您已在原生雲端強制執行模式中部署 VNet。您可以同時使用傳送和計算 VNet。
- 確認遠端端點已與 PCG 對等，且具有以路由為基礎的 IPsec VPN 和 BGP 功能。

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 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增服務

名稱	服務類型	第 0 層/第 1 層閘道	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 記錄檔	資訊		標籤	0
工作階段同步				已啟用

步驟 2b.

VPN 服務 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增本機端點

名稱	VPN 服務	IP 位址	端點憑證	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		本機端點碼	10.99.3.35	
受信任的 CA 憑證	未設定		憑證檢詢清單	未設定	
標籤					0

步驟 2c.

VPN 服務 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增 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			VPN 對等的 IP 位址	已啟用	檢視統計資料
合規性條件	無			192.168.50.10/24	通過介面	下載檔案
驗證模式	PSK			172.0.3.145	遠端端點碼	
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 控制		已停用	

重新整理

第 1 - 1 個，共 1 個 IPsec 工作階段

3 在您在步驟 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。

- a 導覽至網路 > 第 0 層閘道
- b 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。
- c 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			
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 本機 AS: 1000 BGP: ● 開啟 正常重新啟動: 僅限協助程式 正常重新啟動計時器: 180 秒 路由彙總: 0 		<ul style="list-style-type: none"> SR 間 iBGP: ● 開啟 ECMP: ● 開啟 多重路徑放鬆: ● 開啟 正常重新啟動失效計時器: 600 秒 BGP 芳鄰 	

BGP 芳鄰

第 0 層閘道 cloud-t0-415... #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 **重要** 此步驟僅適用於 NSX-T Data Center 3.0.0。如果您正在使用 NSX-T Data Center 3.0.1，則可以略過。

如果您使用 Microsoft Azure，則在 NSX Manager 中設定 VPN 和 BGP 後，請在 PCG 執行個體的上行介面上**啟用 IP 轉送**。如果您有主動和備用 PCG 執行個體 (用於 HA)，請在兩個 PCG 執行個體上都啟用 IP 轉送。

5 使用重新分配設定檔通告您要用於 VPN 的首碼。執行下列操作：

a

重要 此步驟僅適用於 NSX-T Data Center 3.0.0。如果您正在使用 NSX-T Data Center 3.0.1，則可以略過。

為使用 原生雲端強制執行模式 上線的 VPC/VNet CIDR 新增靜態路由，以指向第 0 層閘道 (即 PCG) 的上行 IP 位址。如需指示，請參閱[設定靜態路由](#)。如果您有用於 HA 的 PCG 配對，請將下一個躍點設定為每個 PCG 的上行 IP 位址。

步驟 5a. ✕

第 0 層閘道 cloud-t0-vpc... #靜態路由 1

Q 搜尋

名稱	網路	下一個躍點	狀態
<VPC/VPN-ID>-NativeCloudMode_C IDR_StaticRoute	14.1.14.128/28	2	● 成功 ↻

↖

下一個躍點 ✕

第 0 層閘道 cloud-t0-vpc... | 靜態路由 <VPC/VPN-I... #下一個躍點 2

Q 搜尋

IP 位址	管理距離	範圍
...	1	...
...	30	...

- b 為使用 原生雲端強制執行模式 上線的 VPC/VNet CIDR 新增首碼清單，並在 BGP 芳鄰組態中將其新增為輸出篩選器。如需指示，請參閱[建立 IP 首碼清單](#)。
- c 啟用靜態路由，並選取您在步驟 b 中為 VPC/VNet CIDR 建立的路由篩選器，以設定路由重新分配設定檔。

設定路由重新分配

步驟 5c.

第 0 層閘道 cloud-t0-vpc... #路由重新分配 2

Q 搜尋

名稱	路由重新分配	路由對應
<VPC/VPN-ID>-NativeClou	設定 *	選取路由對應

選取步驟 5b 中建立的 [路由對應 (Route Map)].

↖

設定路由重新分配 ✕

第 0 層閘道 cloud-t0-vpc... #選取的來源 1

選取下方的來源

第 0 層子網路

靜態路由

IPsec 本機 IP

EVPN TEP IP

已連線的介面與區段

服務介面子網路

回送介面子網路

NAT IP

DNS 轉寄站 IP

外部介面子網路

已連線的區段

6 在您的公用雲端中：

- a 前往您擁有工作負載虛擬機器之子網路的路由表。

備註 請勿使用 PCG 的上行或管理子網路的路由表。

- b 將 `nsx.managed = true` 標籤新增至路由表。

7

重要 此步驟僅適用於 NSX-T Data Center 3.0.0。如果您正在使用 NSX-T Data Center 3.0.1，則可以略過。

NSX Cloud 會為具有來源 `0.0.0.0/0` 和目的地 `Any` 的第 0 層閘道 (PCG) 建立 `default-snat` 規則。基於此規則，使用原生雲端強制執行模式之虛擬機器所產生的所有流量，都會具有 PCG 的上行 IP 位址。如果您想要查看流量的實際來源，請執行下列動作：

- a 移至 **網路 > NAT**，並停用第 0 層閘道 (PCG) 的 `default-snat` 規則。
- b 如果您有使用 NSX 強制執行模式的虛擬機器，請使用下列值建立新的 SNAT 規則，以繼續為此類虛擬機器提供 SNAT：

選項	敘述
來源	NSX 強制執行模式中的 VPC/VNet 的 CIDR。
目的地	任何
已轉譯	在 <code>default-snat</code> 規則中位於已轉譯中的相同 IP 位址。
套用至	選取 PCG 的上行介面。

請勿編輯 `default-snat` 規則。該規則會在容錯移轉時還原。

結果

確認路由是針對遠端端點所通告的所有 IP 首碼在受管理路由表中所建立，且下一個躍點設定為 PCG 的上行 IP 位址。

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 6 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 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增服務

名稱	服務類型	第 0 層/第 1 層閘道	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 記錄檔	資訊		標籤	0
工作階段同步				已啟用

步驟 2b.

VPN 服務 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增本機端點

名稱	VPN 服務	IP 位址	端台憑證	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		憑證檢詢清單	未設定	
標籤	0				

步驟 2c.

VPN 服務 IPSEC 工作階段 L2 VPN 工作階段 本機端點 設定檔

新增 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			VPN 對等的 IP 位址	已啟用	檢視統計資料
合規性條件	無			192.168.50.10/24	通過介面	下載檔案
驗證模式	PSK			172.0.3.145	遠端識別碼	
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 控制		已停用	

重新整理

第 1 - 1 個，共 1 個 IPsec 工作階段

3 在您在步驟 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。

- a 導覽至網路 > 第 0 層閘道
- b 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。
- c 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			
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> 本機 AS BGP 正常重新啟動 正常重新啟動計時器 路由彙總 1000 ● 開啟 僅限協助程式 180 秒 0 <ul style="list-style-type: none"> SR 間 iBGP ECMP 多重路徑放鬆 正常重新啟動失效計時器 BGP 芳鄰 ● 開啟 ● 開啟 ● 開啟 600 秒 			

步驟 3.

BGP 芳鄰

第 0 層閘道 cloud-t0-415... #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	2 步驟 4.	路由重新分配狀態	● 開啟	
VRF TORvf	雙主動	0	0	● 成功

重新整理

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

NSX Cloud 常見問題和疑難排解

本主題涵蓋一些常見問題和疑難排解資訊。

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：

- a 輸入 `nsxcli` 命令以開啟 NSX CLI。
- b 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：

- a 登入 AWS 主控台或 Microsoft Azure 入口網站。
- b 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。

我使用來自 CSM 的 URL 部署 PCG，但因為閘道名稱無法解析而發生錯誤。

當用於安裝 PCG 的 CSM UI 中的 URL 因閘道名稱無法解析而失敗時，請針對工作負載虛擬機器的作業系統在各自的公有雲中執行下列操作：

- 在 Microsoft Azure 中的 Microsoft Windows 工作負載虛擬機器上，執行下列命令，然後使用來自 CSM 的 URL 再次下載安裝指令碼：

```
Add-DnsClientNrptRule -Namespace "nsx-gw.vmware.local" -NameServers "168.63.129.16"
-DnsSecEnable
```

- 在 AWS 中的 Microsoft Windows 工作負載虛擬機器上，執行下列命令，然後使用來自 CSM 的 URL 再次下載安裝指令碼：

```
Add-DnsClientNrptRule -Namespace "nsx-gw.vmware.local" -NameServers "169.254.169.253"
-DnsSecEnable
```

- 在 Microsoft Azure 中的 Linux 工作負載虛擬機器上，執行下列命令以取得 PCG 的 IP 位址，並使用這些 IP 位址與來自 CSM 的 URL 下載安裝指令碼。

```
nslookup nsx-gw.vmware.local 168.63.129.16 | awk '/^Address: / { print $2 }'
```

- 在 AWS 中的 Linux 工作負載虛擬機器上，執行下列命令以取得 PCG 的 IP 位址，並使用這些 IP 位址與來自 CSM 的 URL 下載安裝指令碼。：

```
nslookup nsx-gw.vmware.local 169.254.169.253 | awk '/^Address: / { print $2 }'
```