

使用 vRealize Network Insight

VMware vRealize Network Insight 5.2

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

Copyright © 2020 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

1	關於 vRealize Network Insight 使用者指南	10
2	入門	11
	簡介	11
	首頁	13
	導覽	14
	設定	15
3	在 vRealize Network Insight 中新增資料來源	16
	支援的產品和版本	18
	新增 vCenter Server	21
	新增 VMware NSX Manager	22
	新增 VMware NSX-T Manager	24
	新增 VMware SD-WAN	27
	新增 Cisco ASR/ISR 以進行 SD-WAN 評估	28
	新增 VMware Cloud on AWS	30
	為 VMware Cloud on AWS 設定 vRealize Network Insight 收集器	30
	為 vRealize Network Insight 建立 VMware Cloud on AWS 防火牆規則	30
	新增 VMware Cloud on AWS vCenter	32
	新增 VMware Cloud on AWS NSX Manager	33
	新增 Amazon Web Services	34
	新增主要 AWS 帳戶	34
	新增標準 AWS 資料來源	40
	AWS : 地理封鎖支援	43
	新增 Azure 訂閱	44
	啟用 NSG 流量記錄	45
	新增 VMware PKS	45
	新增 Kubernetes	46
	新增 OpenShift	47
	新增 Palo Alto Networks Panorama	48
	新增 Check Point 管理伺服器	49
	新增 Cisco ASA	49
	新增 Fortinet FortiManager	50
	新增 Arista 交換器 SSH	51
	新增 Dell OS10 交換器	52
	在 Dell OS10 交換器上啟用遙測	53
	新增 Huawei 6800/7800/8800 系列	54

- 新增 Cisco ACI 55
- 針對 NetFlow 和 sFlow 新增實體流量收集器 57
- 新增 vRealize Log Insight 57
- 新增 Infoblox 59
- 新增 F5 BIG-IP 60
- 新增 ServiceNow 62
 - 新增 ServiceNow 63
- 新增一般路由器或交換器 78
 - 編輯一般路由器或交換器 79

4 移轉資料來源 80

5 從 vRealize Network Insight 刪除資料來源 82

6 設定 vRealize Network Insight 設定 83

- 檢視系統健全狀況 84
- 設定資料保留間隔 84
- 設定 IP 內容和子網路 85
 - 匯入 DNS 對應檔案 85
 - 設定子網路和 VLAN 之間的對應 85
 - 設定東西向 IP 86
 - 設定南北向 IP 86
- 設定事件及通知 87
 - 系統事件清單 87
 - 檢視和編輯系統事件 123
 - 編輯使用者定義的事件 126
 - 檢視平台健全狀況事件 127
 - NSX-T 事件 128
 - Kubernetes 事件 137
 - 通知 138
- 設定身分識別與存取管理 141
 - 設定使用者管理 141
- 設定記錄 150
 - 檢視和匯出稽核記錄 151
 - 設定 Syslog 組態 151
- 設定郵件伺服器 152
- 設定 SNMP 設陷目的地 152
 - 刪除 SNMP 設陷目的地 153
- 管理授權 153
 - 根據授權版本比較功能 154
 - 新增並變更授權 155

- 設定自動重新整理間隔 156
- 設定使用者工作階段逾時 157
- 新增 Google 地圖 API 金鑰 157
- 設定資料來源憑證驗證 158
 - 手動接受資料來源憑證 158
- 檢視稽核記錄。 159
- 加入或退出客戶經驗改進計劃 160
- 檢視設定的健全狀況 160
- 啟用支援通道 161
- 管理磁碟使用率 161
- 檢視節點詳細資料 162
- 建立支援服務包 162
- 瞭解收集器和平台負載的容量 163

7 vRealize Network Insight 中的 Direct Connect 支援 164

- 檢視 VMC Direct Connect 詳細資料 165
- 檢視透過 Direct Connect 的流量 165
- Direct Connect 搜尋查詢 166

8 vRealize Operations Manager 整合 168

9 建立和擴充叢集 169

- 建立叢集 169
- 擴充叢集 170

10 在 vRealize Network Insight 中設定流量 171

- 啟用 IPFIX 組態 171
 - VDS 和 DVPG 上的 IPFIX 組態 171
 - VMware NSX IPFIX 組態 173
- 針對實體伺服器的流程支援 174
 - 在實體裝置中設定 NetFlow 收集器 175
 - 擴充流程和 IP 端點 179
 - 搜尋實體到實體流程 180
- 檢視已封鎖的流程和受保護的流程 181
- 網路位址轉譯 (NAT) 182
 - NAT 流程支援 - 範例 183
- VMware Cloud on AWS 種流量 185
- 建立 VPC 流量記錄 185
- 將流量記錄從 F5 傳送至 vRealize Network Insight 收集器 186
 - 建立 IPFIX 收集器的集區 187
 - 建立 IPFIX 記錄目的地 187

- 建立記錄發行者 187
- 建立 iRule 188
- 新增 iRule 至虛擬伺服器 193
- 建立路由項目 193

11 Kubernetes 和 VMware PKS 範圍和流量資訊 194

12 檢視實體詳細資料 195

- 檢視 vRealize Network Insight 系統 (NI 系統) 詳細資料 196
- 檢視平台虛擬機器詳細資料 197
- 檢視收集器虛擬機器詳細資料 197
- 檢視 VMware vCenter 資料來源詳細資料 197
- 檢視 PCI 合規性詳細資料 197
 - 匯出為 PDF 198
- 檢視 Kubernetes 詳細資料 199
- 檢視負載平衡器詳細資料 201
- 檢視虛擬機器詳細資料 201
- 檢視 Edge 裝置詳細資料 202
- 檢視 NSX Manager 詳細資料 203
- 檢視 **VMware NSX-T Manager** 詳細資料 204
- 檢視 **NSX-T 管理節點**詳細資料 204
- 檢視 NSX-T 傳輸詳細資料 205
- 檢視虛擬伺服器詳細資料 206
- 檢視集區成員詳細資料 207
- 檢視 Microsoft Azure 詳細資料 208
- 檢視 VeloCloud 企業詳細資料 210
 - 檢視 VeloCloud Edge 詳細資料 211
- 檢視 SD-WAN 和 Edge SD-WAN 應用程式詳細資料 212
- 檢視 **SD-WAN 評估**詳細資料 213
 - 產生評估報告 213
- 檢視 **VeloCloud 連結應用程式**詳細資料 213
- 檢視 **VeloCloud 業務原則**詳細資料 214
- 檢視 VMC SDDC 詳細資料 214
- 檢視 **Arista 硬體閘道**和 **Arista 硬體閘道繫結**詳細資料 214
- 檢視 **Cisco Nexus 裝置**詳細資料 215
- 檢視流量見解詳細資料 215
- 檢視微分割詳細資料 219
- 檢視應用程式詳細資料 220
- 分析 - 極端值偵測 221
 - 如何偵測極端值虛擬機器 221
- 分析：靜態和動態臨界值 223

設定臨界值和警示 223

檢視臨界值組態頁面 224

13 檢視實體拓撲 226

虛擬機器拓撲 226

主機拓撲 226

VXLAN 拓撲 227

VLAN 拓撲 228

NSX Manager 拓撲 228

在 vRealize Network Insight 中檢視 NSX 物件的稽核資訊 229

14 使用釘選項 233

釘選項 233

釘選項類型 233

看板 235

看板的共用和協作 238

將看板設定為首頁 240

複製看板 240

15 vRealize Network Insight 中的負載平衡器支援 242

F5 作為負載平衡器 242

檢視負載平衡器詳細資料 243

檢視虛擬伺服器詳細資料 243

檢視集區成員詳細資料 244

與負載平衡器相關的範例搜尋查詢 245

NSX-V 做為負載平衡器 245

16 網路可見度 247

路徑拓撲 247

AWS 虛擬機器-虛擬機器路徑 248

NSX-T 250

NSX-V Edge 主幹介面虛擬機器-虛擬機器路徑 251

vRealize Network Insight 中的 NAT 支援 251

VMware SD-WAN 虛擬機器-虛擬機器路徑 253

Arista 硬體 VTEP 虛擬機器-虛擬機器路徑 254

VMware Cloud on AWS : 虛擬機器-虛擬機器路徑 255

Cisco ACI 虛擬機器-虛擬機器路徑 256

對 Cisco BGP-EVPN 模式的支援 257

等價多路徑 (ECMP) 路由的支援 258

對 L2 橋接的支援 259

檢視 BGP 芳鄰詳細資料 259

網際網路路徑 260

17 安全性 261

跨 vCenter NSX 261

Palo Alto 網路 262

Cisco ASA 防火牆 265

Check Point 防火牆 267

安全群組 269

以原則為基礎的 VPN 270

NSX 分散式防火牆非作用中規則 271

Fortinet 防火牆 271

18 使用微分割 273

分析應用程式 273

在同心圖視圖中檢視微分割與流量資料 273

在網格視圖中檢視微分割與流量資料 276

手動建立應用程式 277

應用程式探索 279

新增探索到的應用程式 280

VMware Cloud on AWS：規劃和微分割 284

19 建議的防火牆規則 286

匯出規則 288

NSX DFW 一般項目 289

將 CSV 匯出的組態儲存為內容範本 290

匯出並套用 Kubernetes 網路原則 291

20 使用搜尋查詢 294

儲存和刪除搜尋查詢 295

搜尋查詢 295

Azure 搜尋查詢 301

Cisco ACI 實體 302

Fortinet 搜尋查詢 305

使用 Infoblox DNS 資料擴充流程 306

Kubernetes 實體的通用搜尋查詢 306

與負載平衡器相關的範例搜尋查詢 308

NSX 防火牆規則的搜尋查詢 309

VMware SD-WAN 搜尋查詢 309

VMC SDDC 搜尋查詢 311

適用於 AWS 實體的 VMware Cloud on AWS 312

進階查詢 313

時間控制	317
搜尋結果	317
篩選器	318
vCenter 標籤	319

21 規劃 vRealize Network Insight 的災難復原 322

災難復原案例範例	323
----------	-----

22 疑難排解 325

常見資料來源錯誤	325
無法啟用 DFW IPFIX	326

23 使用 vRealize Network Insight 規劃應用程式移轉至 VMware Cloud on AWS 329

如何為 NSX Manager 取得 CSP 重新整理 Token	330
如何取得 vCenter 認證	333
計算閘道防火牆規則	335

關於 vRealize Network Insight 使用者指南

1

《vRealize Network Insight 使用者指南》提供使用 vRealize Network Insight 的相關資訊。

適合對象

此資訊適用於負責使用 vRealize Network Insight 的管理員或專家。該資訊是針對熟悉企業管理應用程式和資料中心作業且富有經驗的虛擬機器管理員而撰寫。

本章節討論下列主題：

- 簡介
- 首頁
- 導覽
- 設定

簡介

vRealize Network Insight 為軟體定義的網路和安全性提供智慧型作業。它可協助客戶跨多雲端環境建置最佳化、高度可用且安全的網路基礎結構。它加速了微分割規劃和部署、實現了跨虛擬和實體網路的可見性，並提供管理和縮放 VMware NSX 部署的運作視圖。

將您的整個資料中心視為由實體及其關聯性組成。例如，虛擬機器是一個實體，並且該虛擬機器是做為另一個實體的主機的一部分。vRealize Network Insight 提供屬於資料中心一部分的大量實體的可見性和資訊。

表 2-1.

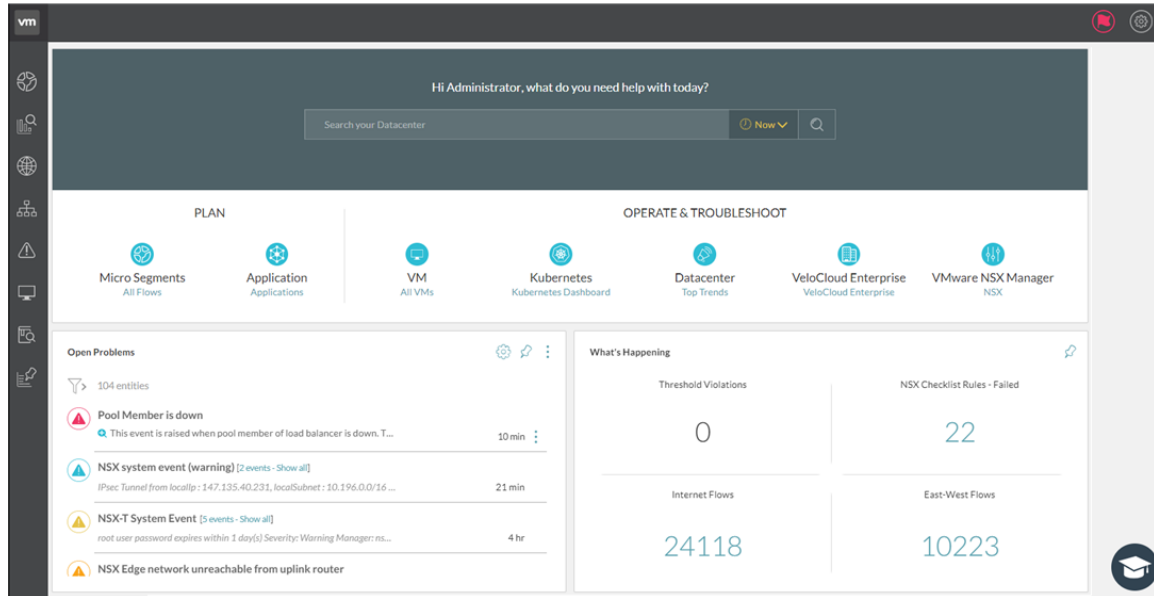
實體	說明
 	主機
 	問題
 	NSX 防火牆
 	虛擬機器
	vSphere Distributed Switch

表 2-1. (續)

實體	說明
	實體交換器
	虛擬連接埠群組
	Cisco Fabric Extender
	邏輯交換器
	資料存放區
	實體網路介面卡
	安全群組
	刀鋒型伺服器
	路由器
	VLAN
	虛擬機器群組
	組態變更
	路由器介面
	疑難排解
	網路存取轉譯 (NAT)
	郵件伺服器

首頁

VMware vRealize Network Insight 首頁提供了整個資料中心的目前狀態的快速摘要。可讓您快速存取資料中心的 vRealize Network Insight 重要元件。



首頁分為以下區段：

搜尋列

透過使用搜尋列，您可以在整個資料中心網路 (及其對應的實體) 之間進行搜尋。您可以使用搜尋列來搜尋資料中心中可用的實體。搜尋列位於首頁頂端。

您可以視需要根據下列時間表選項執行搜尋：

- **預設：**使用此選項，可以針對預設值縮小搜尋結果範圍，例如 last week, last 3 days、last 24 hours、yesterday、today、last 2 hours、last hour，和 now (目前時間)。
- **於：**使用此選項，可以針對特定的日期和時間縮小搜尋結果範圍。
- **介於：**使用此選項，可以在特定的時間間隔之間搜尋資料。

規劃區段

- **微分割：**您可以根據所有虛擬機器之間的流量來規劃網路的微分割。
- **應用程式：**您可以定義應用程式、分析其流量並規劃其安全性。


運作和疑難排解區段

運作和疑難排解區段提供下列元件的可見性、度量和分析：

- 虛擬機器 (VM)
- VLAN 網路

- 資料中心
- NSX 安全群組
- VMware NSX

未解決的問題

未解決的問題區段提供平台在資料中心中找到的重要事件的快速概觀。將對所有這些類似的事件進行分組。使用**全部顯示**以檢視所有事件。若要檢視事件的更多詳細資料，請按一下  (**檢視詳細資料**)。您可以使用 [設定事件] 圖示導覽至 [系統事件] 頁面，並對其進行設定。

此外，如果您針對特定事件按一下**更多選項**下的**設定事件**選項，您可以直接導覽至特定事件的編輯視圖以修改組態。

目前狀態

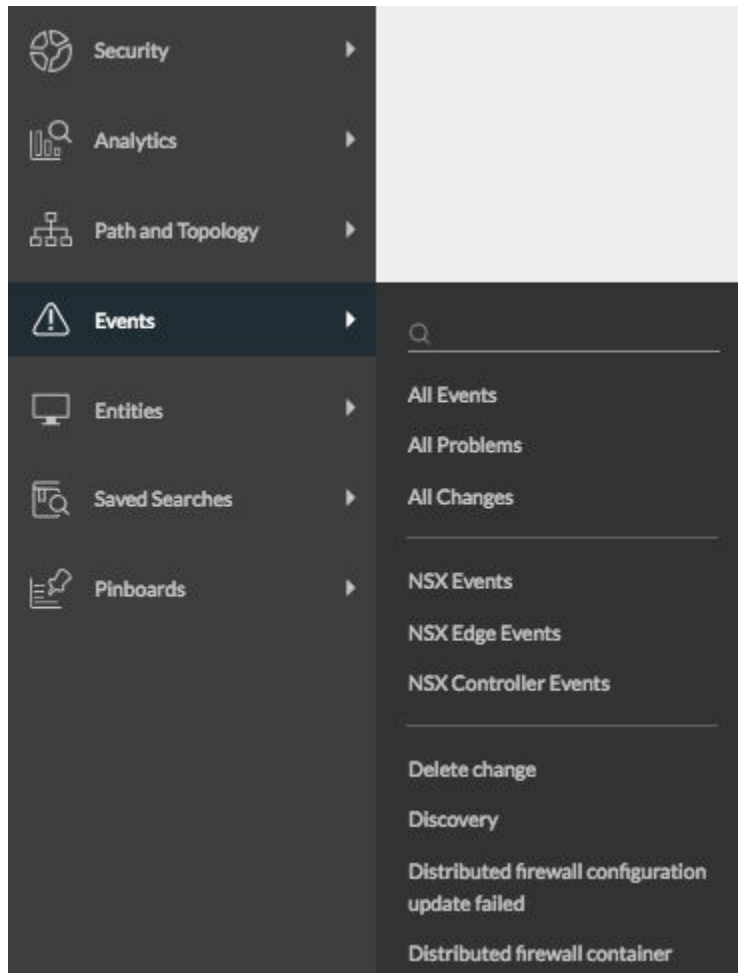
目前狀態區段提供資料中心內較高值內容的快速視圖。若要檢視內容詳細資料，請按一下特定內容的計數。此區段還包含左側的用於篩選事件的篩選器，以及用於檢視事件詳細資料的 [全部展開] 和 [全部收攏] 選項。

導覽

vRealize Network Insight 包含一個左側導覽面板，可協助使用者快速導覽至所需的主要產品功能，例如安全性、拓撲、實體、事件和已儲存的搜尋，而無需輸入任何搜尋查詢。

導覽面板包含下列選項：

- 安全性：為您提供下列選項：
 - 規劃安全性：可讓您分析環境中的流量，且有助於規劃環境內的微分割。您可以選取所有實體或選取特定的實體，然後選取分析所選實體的持續時間。
 - 應用程式：可讓您透過使用自訂搜尋在 vRealize Network Insight 中建立應用程式。一旦建立應用程式，便可相應地進行規劃。
 - PCI 合規性：[PCI 合規性] 儀表板可協助您僅在 NSX 環境中根據 PCI 要求評估合規性。
- 路徑和拓撲：可讓您檢視資料中心的多個實體的任何虛擬機器至虛擬機器路徑或拓撲。
- 事件：可讓您檢視環境中的事件 (變更和問題)。還提供一個事件類型的清單，以便您可以快速檢視特定的事件類型。
- 實體：顯示環境中存在的所有不同類型實體的清單。按一下指定清單中的任何實體類型，以檢視該類型的所有實體的清單。[實體] 清單上方的文字方塊可用來根據輸入的文字縮小清單範圍。
- 已儲存的搜尋：顯示先前儲存的搜尋。



設定

設定頁面會提供用於管理資料提供者、使用者和通知的控制項。

移至設定頁面：

- 1 在首頁的右上角，按一下 [設定檔] 圖示。
- 2 按一下**設定**。此時將顯示**設定**頁面。

在 vRealize Network Insight 中新增資料來源

3

資料來源可讓應用程式能夠從資料中心的某些方面收集資料。其範圍為從 NSX 安裝到實體裝置，例如 Cisco™ 機箱 4500 和 Cisco™ N5K。

若要新增資料來源，請執行下列動作：

- 1 在**安裝和支援**頁面的**設定**下，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 選取帳戶或來源類型。
- 4 在表單上提供所需資訊。
- 5 按一下**驗證**。
- 6 為資料來源輸入暱稱和附註 (如果有)。
- 7 按一下**提交**，將資料來源新增至環境。

對於每個資料來源，您可以檢視以下詳細資料：

內容	說明
類型 (暱稱)	顯示資料來源的名稱。
IP 位址/FQDN	顯示資料來源的 IP 位址或 FQDN 詳細資料。
上次收集時間	顯示上次收集資料的收集時間。
已探索到的虛擬機器數目	顯示已為此資料來源探索到的虛擬機器的數目。 備註 僅在資料來源為 vCenter 或 AWS 來源時，才會填入 [已探索到的虛擬機器數目] 資料行。
收集器虛擬機器	顯示已向其新增資料來源的收集器的名稱。如果所有列出的資料來源已新增至相同的收集器上，則此資料行不可見。僅當資料來源存在於不同的收集器上時，才能檢視此資料行。
已啟用	指示資料來源是否已啟用。
動作	顯示用於編輯和刪除資料來源的選項。

vRealize Network Insight 提供下列功能，以便能夠輕鬆地存取資料來源的資訊。

- 透過使用資料行標頭上方的搜尋列，您可以依名稱、IP 位址或收集器虛擬機器名稱搜尋資料來源。

- 您可以在**類型 (暱稱)** 資料行中按不同的資料來源篩選資訊。
- 您可以在**收集器虛擬機器**資料行中按各種收集器虛擬機器篩選資訊。
- 資料來源按其類型和暱稱的字母順序排序。

對於新增的每個資料來源，您可以檢視以下資訊：

- **全部**：顯示所有可用的資料來源。
- **有問題**：顯示 vRealize Network Insight 發現問題的資料來源。
- **帶有建議**：針對需要其他資訊的資料來源顯示從 vRealize Network Insight 自動產生的建議。
- **已停用**：顯示已停用的資料來源。

本章節討論下列主題：

- [支援的產品和版本](#)
- [新增 vCenter Server](#)
- [新增 VMware NSX Manager](#)
- [新增 VMware NSX-T Manager](#)
- [新增 VMware SD-WAN](#)
- [新增 Cisco ASR/ISR 以進行 SD-WAN 評估](#)
- [新增 VMware Cloud on AWS](#)
- [新增 Amazon Web Services](#)
- [新增 Azure 訂閱](#)
- [新增 VMware PKS](#)
- [新增 Kubernetes](#)
- [新增 OpenShift](#)
- [新增 Palo Alto Networks Panorama](#)
- [新增 Check Point 管理伺服器](#)
- [新增 Cisco ASA](#)
- [新增 Fortinet FortiManager](#)
- [新增 Arista 交換器 SSH](#)
- [新增 Dell OS10 交換器](#)
- [新增 Huawei 6800/7800/8800 系列](#)
- [新增 Cisco ACI](#)
- [針對 NetFlow 和 sFlow 新增實體流量收集器](#)
- [新增 vRealize Log Insight](#)

- 新增 Infoblox
- 新增 F5 BIG-IP
- 新增 ServiceNow
- 新增一般路由器或交換器

支援的產品和版本

vRealize Network Insight 支援多個產品和版本。

資料來源	版本/型號	連線通訊協定	權限/特殊權限
Amazon Web Services (僅限企業授權)	不適用	HTTPS	請參閱使用者指南中的〈新增資料來源〉一節。
Arista 交換器	7050TX、7250QX、7050QX-32S、7280SE-72	SSH、SNMP	請參閱使用者指南中的〈新增資料來源〉一節。
Azure 訂閱	不適用	HTTPS	請參閱使用者指南中的〈新增資料來源〉一節。
Brocade 交換器	VDX 6740、VDX 6940、MLX、MLXe	SSH、SNMP	請參閱使用者指南中的〈新增資料來源〉一節。
Check Point 防火牆	Check Point R80、R80.10、R80.20、R80.30	HTTPS、SSH	請參閱使用者指南中的〈新增資料來源〉一節。
Cisco	ASR 1K、ISR4K、CSR1Kv、ISR1K 備註 僅支援 SD-WAN 評估。	<ul style="list-style-type: none"> ■ 支援的作業系統：Cisco IOS XE Software ■ 作業系統版本：16.07.01 	不支援網路驗證和保證功能 (網路對應和意圖)。
Cisco ACI	3.2	HTTPS (至 APIC 控制器) SNMP (至 APIC 控制器和 ACI 交換器)	請參閱使用者指南中的〈新增資料來源〉一節。
Cisco ASA	具有作業系統 9.4 的 X 系列	SSH、SNMP	請參閱使用者指南中的〈新增資料來源〉一節。
Cisco Catalyst	3000、3750、4500、6000、6500	SSH、SNMP	請參閱使用者指南中的〈新增資料來源〉一節。
Cisco Nexus	3000、5000、6000、7000、9000	SSH、SNMP	唯讀使用者 唯讀 SNMP 使用者
Cisco UCS (統一運算系統)	B 系列刀鋒伺服器，C 系列機架式伺服器、機箱、網狀架構互連	UCS Manager：HTTPS UCS 網狀架構：SSH、SNMP	唯讀使用者 唯讀 SNMP 使用者
Dell 交換器	FORCE10 MXL 10、FORCE10 S6000、S4048、Z9100、S4810、PowerConnect 8024、Dell OS10	SSH、SNMP	唯讀使用者 唯讀 SNMP 使用者

資料來源	版本/型號	連線通訊協定	權限/特殊權限
Fortinet FortiManager	6.0.1	HTTPS	使用者必須具有： <ul style="list-style-type: none"> ■ 至少能夠存取所有 ADOM 和原則套件的受限制的使用者角色。 ■ 已從命令列介面 (CLI) 啟用的 rpc-permit read 存取。
F5 BIG - IP	12.1.2 及更新版本	HTTPS、SSH、SNMP	使用者必須至少具有客體角色。此外，必須啟用 TMSH，並且必須能夠存取所有磁碟分割。F5 BIG-IP 支援路由和負載平衡。
HP	HP Virtual Connect Manager 4.41、HP OneView 3.0	HP OneView 3.0 ? : HTTPS HP Virtual Connect Manager 4.41 : SSH	唯讀使用者
Huawei Cloud Engine	6800、7800、8800	SSH、SNMP	唯讀使用者 唯讀 SNMP 使用者
Infoblox	Infoblox NIOS 版本 8.0、8.1、8.2	HTTPS	具有 API 介面存取權的唯讀使用者 DNS 物件類型的唯讀權限，如下所示： <ul style="list-style-type: none"> ■ 權限類型 - DNS ■ 資源 - A 記錄、DNS 區域、DNS 視圖
Juniper 交換器	EX3300、QFX 51xx 系列 (JunOS v12 和 v15，不含 QFabric)	Netconf、SSH、SNMP	唯讀使用者 唯讀 SNMP 使用者
Kubernetes	<ul style="list-style-type: none"> ■ NSX-T 2.3.1 上的 1.12 ■ NSX-T 2.3.2 上的 1.12 ■ NSX-T 2.3.2 上的 1.13 	HTTPS	使用者必須擁有具有讀取權限的叢集管理員角色。
OpenShift	3.1.1	HTTPS	請參閱使用者指南中的〈新增資料來源〉一節。
Palo Alto 網路	Panorama 7.0.x、7.1、8.x、9.0	HTTPS	使用者必須擁有具有 XML API 存取權的管理員角色。如需詳細資料，請參閱《vRealize Network Insight 使用者指南》中的〈Palo Alto Networks〉一節。
ServiceNow	倫敦	HTTPS	使用者必須具有管理員角色
VMware SD-WAN	VeloCloud Orchestrator 和 Edge 版本 3.3.1 及更新版本	HTTPS	使用者必須擁有具有下列任一權限的 帳戶 角色： <ul style="list-style-type: none"> ■ 超級使用者 ■ 標準管理員 ■ 客戶支援人員
VMC on AWS - vCenter	M8 及更新版本 <u>備註</u> 僅支援以 NSX-T 為基礎的 VMware Cloud on AWS SDDC。	HTTPS	使用者必須具有下列權限： <ul style="list-style-type: none"> ■ 雲端管理員：新增資料來源並啟用 IPFIX。

資料來源	版本/型號	連線通訊協定	權限/特殊權限
VMC on AWS - NSX Manager	M8 及更新版本 備註 僅支援以 NSX-T 為基礎的 VMware Cloud on AWS SDDC。	HTTPS	使用者必須具有下列任一權限： <ul style="list-style-type: none"> ■ 組織成員.管理員：新增資料來源並啟用 IPFIX。 ■ 組織成員.管理員.NSX Cloud 管理員：新增資料來源並啟用 IPFIX。 ■ 組織成員.VMware Cloud on AWS (所有角色)：新增資料來源並啟用 IPFIX。 ■ 組織成員.NSX Cloud 管理員：新增資料來源。
VMware Identity Manager	3.3 及更新版本	HTTPS	使用者必須具有管理員角色。
VMware PKS	支援的版本		使用者必須擁有叢集管理員角色權限 - pks.clusters.admin。
VMware NSX Manager (VMware NSX-V)	支援的版本	SSH、HTTPS	請參閱《vRealize Network Insight 使用者指南》中的〈Edge 資料收集〉一節。
VMware NSX-T Manager	2.4。 對於其他支援的版本，請參閱〈 支援的版本 〉	HTTPS	唯讀使用者
VMware vRealize Log Insight	支援的版本	HTTPS	具有安裝、設定及管理內容套件的權限的 API 使用者
VMware vSphere	支援的版本 對於 IPFIX，需要 VMware ESXi 版本： <ul style="list-style-type: none"> ■ 5.5 Update 2 (組建編號 2068190) 及更高版本 ■ 6.0 Update 1b (組建編號 3380124) 及更高版本 ■ VMware VDS 5.5 及更高版本 備註 應在資料中心的所有虛擬機器上安裝 VMware Tools，才能識別虛擬機器至虛擬機器路徑。	HTTPS	唯讀使用者 設定和使用 IPFIX 所需的權限 具有權限的 vCenter Server 認證： Distributed Switch: Modify dvPort group: Modify vCenter Server 中預先定義的角色必須具有在根層級指派的以下權限，且這些權限需要傳播到子角色： System.Anonymous System.Read System.View global.settings

備註

- Cisco ASA、ACI、Catalyst 和 Nexus 裝置支援的作業系統為 iOS/NX-OS；Cisco UCS 支援的作業系統為 UCSM 版本。
- 支援的 Arista 作業系統為 Arista EOS。

新增 vCenter Server

您可以將 vCenter Server 做為資料來源新增至 vRealize Network Insight。

可以將多個 vCenter Server 新增至 vRealize Network Insight，以開始監控資料。

必要條件

- vCenter Server 中預先定義的角色必須具有在根層級指派的以下權限，且這些權限需要傳播到子角色：
 - System.Anonymous
 - System.Read
 - System.View
 - Global.Settings
- 必須具備下列 vCenter Server 權限才能設定和使用 IPFIX：
 - Distributed Switch：修改和連接埠組態作業
 - dvPort 群組：修改和原則作業

若要深入瞭解 vCenter 中的角色，請參閱《vSphere 安全性》指南中的〈使用角色指派權限〉一節。

程序

- 1 按一下**新增 vCenter**。
- 2 按一下**新增來源**並自訂選項。

選項	動作
收集器虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 vCenter Server 的 IP 位址或完整網域名稱。
使用者名稱	輸入擁有下列權限的使用者名稱： <ul style="list-style-type: none"> ■ Distributed Switch：修改 ■ dvPort 群組：修改
密碼	輸入 vRealize Network Insight 軟體的密碼以存取 vCenter Server 系統。

- 3 按一下**驗證**。

如果探索到的虛擬機器數目超過平台和/或控制器節點的容量，則驗證會失敗。增加平台的區塊大小或建立叢集之後，才能新增資料來源。

每個區塊大小 (含流程和不含流程) 的指定容量如下所示：

區塊大小	虛擬機器	流程狀態
大型	6k	已啟用
大型	10k	已停用

區塊大小	虛擬機器	流程狀態
中型	3k	已啟用
中型	6k	已停用

4 選取在此 vCenter 上啟用 Netflow (IPFIX) 以啟用 IPFIX。

如需有關 IPFIX 的詳細資訊，請參閱使用者指南中的〈在 VDS 和 DVPG 上啟用 IPFIX 組態〉一節。

備註 如果同時在 vCenter 和 VMware NSX Manager 中啟用 IPFIX，則 vRealize Network Insight 會透過停用相關聯的 vCenter 的幾個 DVPG 上的 IPFIX 來自動偵測並移除流量冗餘。

5 將進階資料收集來源新增到您的 vCenter Server 系統。

6 按一下**提交**以新增 vCenter Server 系統。vCenter Server 系統將顯示在首頁上。

新增 VMware NSX Manager

您可以在 vRealize Network Insight 中將 NSX-V 新增為資料來源。

必要條件

確認下列各項：

- 您已將 vCenter 新增為資料來源。
- 企業角色。
- 系統管理員認證 (如果已啟用 Central CLI)。
- 表 3-1。

NSX 版本	使用者
NSX 6.4 和更高版本	<ul style="list-style-type: none"> ■ 若要將 NSX Manager 新增為資料來源，您必須是超級使用者、企業管理員、稽核員或 NSX 安全管理員。 ■ 企業管理員、超級使用者、NSX 安全管理員或稽核員可以執行 vRealize Network Insight 所需的 NSX Central CLI 命令。 <p>備註 NSX 網路管理員無法將 NSX Manager 新增為資料來源。</p>
NSX 6.4 之前的 NSX 6.2 和更高版本	<ul style="list-style-type: none"> ■ 使用者應為管理員才可以啟用 Edge 資料填入。 ■ 稽核員、超級使用者或 NSX 安全管理員可以執行 vRealize Network Insight 所需的 NSX Central CLI 指令。 ■ 將 NSX Manager 新增為資料來源時需要提供的使用者認證必須屬於企業管理員或超級使用者。

程序

1 在設定頁面上，按一下**帳戶和資料來源**。

- 2 按一下**新增來源**。
- 3 在 **VMware Manager** 下，按一下 **VMware NSX Manager**。
- 4 在**新增 VMware NSX Manager 帳戶或來源**頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
主要 VMware vCenter	選取要在 vRealize Network Insight 中新增的 vCenter。 備註 確保 vCenter 和相關聯的 NSX Manager 資料來源已新增到同一個收集器。否則，您將無法看到拒絕的流量 (啟用 NSX IPFIX 時)，並且某些流量中可能沒有已套用的防火牆規則。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 5 按一下**驗證**。
- 6 (選擇性) 如果您想要收集 NSX Controller 資料，則選取**啟用 NSX Controller 資料收集**核取方塊。
如果您選取此選項，vRealize Network Insight 會收集控制器資料，例如，邏輯路由器介面、路由、邏輯交換器 MAC 資料表、VTEP 記錄、控制器叢集狀態和角色。資料收集是由 NSX Central CLI 或 Controller-SSH 工作階段完成的。
- 7 (選擇性) 如果您想要收集 NSX Edge 資料，則選取**啟用 NSX Edge 資料收集**核取方塊。
Edge 資料收集是由 NSX Central CLI 完成的。因此，不會在 NSX Manager 下建立 Edge 資料提供者。啟用 Edge 填入時，會驗證 NSX 使用者權限。
假設使用者在 NSX 6.3 中具有企業管理員權限，並且正在執行目前版本的 vRealize Network Insight，則會在 **VMware NSX Manager** 的**帳戶和資料來源**頁面上顯示 `Insufficient Privileges` 錯誤。顯示此錯誤的原因是，使用者必須是超級使用者才能在 NSX 6.3 中執行 NSX Central CLI 命令。
- 8 (選擇性) 如果您想要收集 IPFIX 流量，請選取**啟用 IPFIX**核取方塊。
如果您選取此選項，則 vRealize Network Insight 會接收來自 NSX-V 的 DFW IPFIX 流量。

備註 如果在 vCenter 和 VMware NSX Manager 中啟用 IPFIX，則 vRealize Network Insight 會透過停用相關聯的 vCenter 的幾個 DVPG 上的 IPFIX 來自動偵測並移除流量冗餘。

如需有關啟用 IPFIX 的詳細資訊，請參閱**啟用 VMware NSX-V IPFIX**。

- 9 在**暱稱**文字方塊中，輸入暱稱。
- 10 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 11 按一下**提交**。

新增 VMware NSX-T Manager

VMware NSX-T 專為處理新興應用程式架構和具有異質端點和技術堆疊的架構而設計。除 vSphere 以外，這些環境可能還包含其他管理程式、容器、裸機和公有雲。vRealize Network Insight 支援虛擬機器由 vCenter 管理的 NSX-T 部署。

考量事項

- vRealize Network Insight 僅支援由 vCenter 管理 ESXi 主機的 NSX-T 設定。
- vRealize Network Insight 支援 NSGroup、NSX-T 防火牆規則、IPSet、NSX-T 邏輯連接埠、NSX-T 邏輯交換器、NSX-T Distributed Firewall IPFIX 流量、區段、群組和以原則為基礎的 VPN。
- vRealize Network Insight 同時支援 NSX-V 和 NSX-T 部署。在查詢中使用 NSX 時，結果將包含 NSX-V 和 NSX-T 實體。NSX Manager 會列出 NSX-V Manager 和 NSX-T Manager。NSX 安全群組會列出 NSX-T 和 NSX-V 安全群組。如果您使用 NSX-V 或 NSX-T 而不是 NSX，則僅會顯示這些實體。此邏輯同樣適用於防火牆規則、IPSet 和邏輯交換器等實體。
- 透過 NSX-T 2.4 版本，vRealize Network Insight 支援 NSX 宣告式原則管理，可透過結果導向的原則聲明簡化並自動化網路與安全性組態。

備註 安全群組的微分割是基於 NSX 原則資料完成的。但是，如果沒有相應的 NSX 原則群組，會將獨立的 NS 群組包含在微分割分析中。如需有關 NS 群組的更多詳細資料，請參閱 [NSX-T 產品說明文件](#)。

將 NSX-T Manager 新增為資料來源

以下是將 NSX-T Manager 新增為資料來源的必要條件：

- 建議將與 NSX-T Manager 相關聯的所有 vCenter 新增為 vRealize Network Insight 中的資料來源。
- 如果在新增 vCenter 前已新增 NSX-T Manager，則 vRealize Network Insight 約需要 4 小時才能穩定。
- 確保在 Distributed Firewall (DFW) 的排除清單中沒有邏輯交換器。如果此清單中有任何邏輯交換器，則不會報告連結至這些邏輯交換器的任何虛擬機器的流程。

新增 NSX-T Manager：

- 1 在設定下的帳戶和資料來源頁面中，按一下新增來源。
- 2 在選取帳戶或資料類型頁面的 VMware Manager 下，選取 VMware NSX-T Manager。

3 提供使用者認證。

備註

- 如果在單一 NSX-T 部署中有多個管理節點，則必須僅新增一個節點做為 vRealize Network Insight 中的資料來源或使用虛擬 IP (VIP) (屬於這些節點)。如果您新增多個管理節點，則 vRealize Network Insight 可能無法正常運作。
- 當您新增 NSX-T 做為資料來源時，建議使用 VIP。如果您新增管理節點 IP 而非 VIP，且在稍後想要新增 VIP 或其他管理節點 IP，則必須刪除現有資料來源，才能新增 VIP 或管理 IP。
- 如果不需要 IPFIX，則使用者必須是具有稽核層級權限的本機使用者。但是，如果需要 IPFIX，則使用者必須具有下列其中一項稽核層級權限：**enterprise_admin**、**network_engineer** 或 **security_engineer**。

- 4 (選擇性) 選取**啟用 DFW IPFIX**以更新 NSX-T 上的 IPFIX 設定。透過選取此選項，vRealize Network Insight 會接收來自 NSX-T 的 DFW IPFIX 流量。如需有關啟用 IPFIX 的詳細資訊，請參閱 [啟用 VMware NSX-T DFW IPFIX](#)。

備註

- DFW IPFIX 在 NSX-T 的標準版本中不受支援。
- vRealize Network Insight 不支援 NSX-T 交換器 IPFIX 流量。

- 5 (選擇性) 如果您想要收集延遲度量資料，則選取**啟用延遲度量收集**核取方塊。如果您選取此選項，則 vRealize Network Insight 會接收來自 NSX-T 的延遲度量 (VTEP - VTEP)。此選項僅適用於 NSX-T 2.5 及更新版本。確保在收集器上開啟連接埠 1991，以接收來自 ESXi 節點的延遲資料。

查詢範例

以下是一些與 NSX-T 相關的查詢範例：

表 3-2. NSX-T 的查詢

查詢	搜尋結果
NSX-T Manager where VC Manager=10.197.53.214	此特定 VC Manager 已新增為計算管理程式的 NSX-T Manager。
NSX-T Logical Switch	列出 vRealize Network Insight 執行個體中存在的所有 NSX-T 邏輯交換器。其中包括它是由系統建立還是使用者建立的交換器的詳細資料。
NSX-T Logical Ports where NSX-T Logical Switch = 'DB-Switch'	列出屬於該特定 NSX-T 邏輯交換器 DB-Switch 的 NSX-T 邏輯連接埠。
VMs where NSX-T Security Group = 'Application-Group' 或 VMs where NSGGroup = 'Application-Group'	列出該特定安全群組 Application-Group 中的所有虛擬機器。
NSX-T Firewall Rule where Action='ALLOW'	列出其動作設為 ALLOW 的所有 NSX-T 防火牆規則。
NSX-T Firewall Rule where Destination Security Group = 'CRM-Group'	列出 CRM-Group 是目的地安全群組的防火牆規則。結果包含直接目的地安全群組和間接目的地安全群組。

表 3-2. NSX-T 的查詢 (續)

查詢	搜尋結果
NSX-T Firewall Rule where Direct Destination Security Group = 'CRM-Group'	列出 CRM-Group 是目的地安全群組的防火牆規則。結果僅包含直接目的地安全群組。
VMs where NSX-T Logical Port = 'App_Port-Id-1'	列出具有該特定 NSX-T 邏輯連接埠的所有虛擬機器。
NSX-T Transport Zone	列出 VLAN 和覆蓋傳輸區域以及與其相關聯的對應詳細資料 (包括傳輸節點的類型)。 備註 vRealize Network Insight 不支援將 KVM 做為資料來源。
NSX-T Router	列出 TIER 1 和 TIER 0 路由器。按一下結果中顯示的路由器，以檢視其相關聯的更多詳細資料，包括 NSX-T Edge 叢集和 HA 模式。

表 3-3. NSX 原則的查詢

NSX Policy Segment	列出 vRealize Network Insight 執行個體中存在的所有 NSX 原則區段。
NSX Policy Manager	列出 vRealize Network Insight 執行個體中存在的所有 NSX Policy Manager。
NSX Policy Group	列出 vRealize Network Insight 執行個體中存在的所有 NSX 原則群組。
NSX Policy Firewall	列出 vRealize Network Insight 執行個體中存在的所有 NSX 原則防火牆。
NSX Policy Firewall Rule	列出 vRealize Network Insight 執行個體中存在的所有 NSX 原則防火牆規則。
NSX Policy Firewall Rule where Action = 'ALLOW'	列出其動作設為 ALLOW 的所有 NSX 原則防火牆規則。
NSX Policy Based VPN	列出 vRealize Network Insight 執行個體中存在的所有以 NSX 原則為基礎的 VPN。

備註 如果將 NSX-T 2.4 和 VMware Cloud on AWS 新增為 vRealize Network Insight 中的資料來源，為了取得 NST-T 實體，您必須在查詢中新增 **SDDC type = ONPREM** 篩選器。例如，
NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'ONPREM'。

NSX-T 度量支援

下表顯示了目前支援 NSX-T 度量的 vRealize Network Insight 實體，以及在對應實體儀表板上顯示這些度量的 Widget。

表 3-4.

實體	實體儀表板上的 Widget	支援的 NSX-T 度量
邏輯交換器	邏輯交換器封包度量 邏輯交換器位元組度量	Multicast and Broadcast Rx
		Multicast and Broadcast Tx
		Unicast Rx
		Unicast Tx
		Dropped Rx
		Dropped Tx
		Rx Packets (Total)
		Tx Packets (Total)
邏輯連接埠	邏輯連接埠封包度量 邏輯連接埠位元組度量	Multicast and Broadcast Rx
		Multicast and Broadcast Tx
		Unicast Rx
		Unicast Tx
		Rx Packets (Total)
		Tx Packets (Total)
路由器介面	路由器介面度量	Rx Packets
		Tx Packets
		Dropped Rx Packets
		Dropped Tx Packets
		Rx Bytes
		Tx Bytes
防火牆規則	防火牆規則度量	Hit Count
		Flow Bytes
		Flow Packets

以下是一些有關 NSX-T 度量的查詢範例：

- `nsx-t logical switch where Rx Packet Drops > 0`
此查詢會列出捨棄的已接收封包計數大於 0 的所有邏輯交換器。
- `nsx-t logical port where Tx Packet Drops > 0`
此查詢會列出捨棄的已傳輸封包計數大於 0 的所有邏輯連接埠。
- `top 10 nsx-t firewall rules order by Connection count`
此查詢根據連線計數 (Hit Count) 列出前 10 個防火牆規則。

新增 VMware SD-WAN

您可以在 vRealize Network Insight 中將 VMware SD-WAN by VeloCloud 新增為資料來源。

必要條件

請確保：

- 您有新增資料來源的正確權限。如需權限的相關資訊，請參閱〈[支援的產品和版本](#)〉。
- 您正在使用 VeloCloud Orchestrator 和 Edge 3.3.1 版或更新版本。
- 您已新增至少一個 VMware SD-WAN 授權。
- 沒有其他 VMware SD-WAN 新增為資料來源。

程序

- 1 在**設定**頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在**SD-WAN**下，按一下**VeloCloud**。
- 4 在**新增 VeloCloud 帳戶或來源**頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
VCO URL	輸入要新增為資料來源的 VCO URL。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 5 按一下**驗證**。
- 6 在**暱稱**文字方塊中，輸入暱稱。
- 7 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 8 按一下**提交**。

後續步驟

您必須在連接埠 2055 上為所有設定檔和 Edge 啟用 NetFlow。若要瞭解如何啟用 NetFlow 收集，請在 VMware SD-WAN 的**編輯資料來源**頁面中，按一下**檢視指示**。

備註 您可以在附註：應為所有設定檔和 Edge 啟用 Netflow 收集中看到**檢視指示**選項。

新增 Cisco ASR/ISR 以進行 SD-WAN 評估

您可以在 vRealize Network Insight 中將 Cisco ASR/ISR 路由器新增為資料來源，其僅會用於 SD-WAN 評估。vRealize Network Insight 不支援將 Cisco ASR/ISR 路由器做為資料來源用於任何其他目的。

vRealize Network Insight 僅支援以下 Cisco ASR/ISR 版本進行 SD-WAN 評估：

版本/型號	支援的作業系統	作業系統版本
ASR 1K、ISR4K、CSR1Kv、ISR1K	Cisco IOS XE Software	16.07.01

程序

- 1 在設定頁面上，按一下帳戶和資料來源。
- 2 按一下新增來源。
- 3 在 WAN 下，按一下 Cisco ASR/ISR (SD-WAN 評估)。
- 4 在新增 Cisco ASR/ISR 帳戶或來源頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址	輸入 IP 位址詳細資料。 備註 無法使用任何 FQDN 來新增此資料來源。您必須輸入 IP 位址詳細資料，才能新增此資料來源。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 5 按一下驗證。
- 6 從 SNMP 版本下拉式功能表中，選取 2C。
- 7 在社群字串文字方塊中，輸入社群字串。
- 8 將每個上行介面對應至 MPLS 或網際網路。若要對應上行介面，請按一下每個介面名稱的下拉式功能表，然後選取適當的選項。

依預設，vRealize Network Insight 會擷取並列出所有上行介面。
- 9 在暱稱文字方塊中，輸入資料來源的暱稱。
- 10 在站台和區域文字方塊中，輸入適當的站台和區域名稱。
- 11 (選擇性) 在附註文字方塊中，您可以視需要新增附註。
- 12 按一下提交。

後續步驟

- 1 針對 NetFlow 和 sFlow 新增實體流量收集器。
- 2 將 Cisco ASR/ISR 設定為將 NetFlow 資訊傳送至 vRealize Network Insight 收集器。如需設定 NetFlow 的相關資訊，請參閱在實體裝置中設定 NetFlow 收集器。

備註 收集足夠的流量資訊進行 SD-WAN 評估需要約四個小時。

- 3 移至 [檢視 SD-WAN 評估詳細資料] 頁面，以取得 SD-WAN 評估詳細資料。

新增 VMware Cloud on AWS

vRealize Network Insight 支援 VMware Cloud on AWS (僅適用於企業授權使用者)。您可以新增 VMware Cloud on AWS (vCenter) 或 VMware Cloud on AWS (NSX Policy Manager) 做為資料來源。

為 VMware Cloud on AWS 設定 vRealize Network Insight 收集器

您必須將 vRealize Network Insight 收集器設定為從 VMware Cloud on AWS 收集資料。

必要條件

在需要新增為資料來源的每個 SDDC 內部署 vRealize Network Insight 收集器。

備註

- 不支援使用在某個 VMware Cloud on AWS SDDC 中部署的 vRealize Network Insight 收集器，從另一個 VMware Cloud on AWS SDDC 收集資料。
- 您必須在原生 VMware Cloud on AWS 區段上部署 vRealize Network Insight 收集器。不支援在延伸區段上部署收集器。

程序

- 1 登入 vRealize Network Insight。
- 2 導覽至設定 > 安裝和支援 > 新增收集器虛擬機器。
- 3 複製共用密碼的內容。

在 vRealize Network Insight 收集器 OVA 部署期間，需要使用此密碼。

- 4 在 VMware Cloud on AWS vCenter 的計算資源集區中部署 vRealize Network Insight 收集器 OVA。

使用您所產生的共用密碼。

備註 對於 VMware Cloud on AWS 中的單一節點 SDDC，Proxy 虛擬機器的 CPU 資源保留區必須至少為 1251 MHz。

- 5 啟動收集器虛擬機器，然後依照精靈將收集器與 vRealize Network Insight 平台配對。
- 6 驗證收集器是否與平台成功配對。

為 vRealize Network Insight 建立 VMware Cloud on AWS 防火牆規則

您必須建立 VMware Cloud on AWS 群組和防火牆規則，才能建立與 vRealize Network Insight 的通訊。

必要條件

- 部署 vRealize Network Insight 平台和收集器 (適用於內部部署) 或取得有效的訂閱 (適用於雲端服務)。
- 您必須具有所需的權限。請參閱 [〈支援的產品和版本〉](#)。

- 使用 NSX-T 網路部署 VMware Cloud on AWS 軟體定義資料中心 (SDDC) 1.8 及更新版本。
- 針對 vRealize Network Insight 平台和收集器之間的通訊設定防火牆規則。
- 如需傳入流量的連接埠需求，請參閱 [系統連接埠] 頁面上 [收集器伺服器] 資料表中的 [連接埠]。
- 針對下列網域的傳出流量開啟 HTTPS 連接埠 443：
 - *.vmwareidentity.com
 - gaz.csp-vidm-prod.com
 - *.vmware.com
 - *.ni-onsaas.com

針對 vRealize Network Insight 平台和收集器之間的通訊設定防火牆規則

在 VMware Cloud on AWS 中設定防火牆規則包括：

- 為 vRealize Network Insight 收集器建立 VMware Cloud on AWS 群組。
 - a 登入 VMware Cloud on AWS，網址為：<https://vmc.vmware.com>。
 - b 在網路與安全性索引標籤上，按一下詳細目錄 > 群組。
 - c 在群組卡上，按一下計算群組，然後按一下新增群組，並為群組指定名稱和選擇性說明。
 - d 按一下設定成員，以開啟選取成員頁面。
 - e 提供 vRealize Network Insight 收集器虛擬機器詳細資料。

您可以在稍後建立的防火牆規則中使用此群組，以允許 VMware Cloud on AWS NSX Manager 和 vRealize Network Insight 之間進行通訊。
- 建立防火牆規則。
 - a 登入 VMC 主控台，網址為：<https://vmc.vmware.com>。
 - b 在網路與安全性索引標籤上，按一下閘道防火牆。
 - c 在閘道防火牆卡上，按一下計算閘道，然後按一下新增規則，並為新規則提供名稱。
 - d 輸入新規則的參數。
 - 來源：輸入包含 vRealize Network Insight 收集器 IP 位址的 VMware Cloud on AWS 群組的名稱。
 - 目的地：選取任何。
 - 服務：選取 HTTPS、DNS、DNS-UDP、NTP、ICMP。
 - 動作：選取允許。
 - 套用至：選取網際網路介面。
 - 記錄：視需要啟用記錄。否則，此欄位保持不變。

新規則預設為啟用。將切換開關向左滑可將其停用。
 - e 按一下發佈。

針對收集器和 NSX Manager 以及收集器和 vCenter 之間的通訊設定防火牆規則

- 1 登入 VMC 主控台，網址為：<https://vmc.vmware.com>。
- 2 在網路與安全性索引標籤上，按一下**閘道防火牆**。
- 3 在**閘道防火牆**卡上，按一下**管理閘道**，然後按一下**新增規則**，並為新規則提供名稱。
- 4 輸入新規則的參數。
 - **來源**：輸入包含 vRealize Network Insight 收集器 IP 位址的 VMware Cloud on AWS 群組的名稱。
 - **目的地**：選取**系統定義的群組**，搜尋 NSX Manager，然後選取 NSX Manager 項目。
 - **服務**：選取 **HTTPS (443)**。
 - **動作**：選取**允許**。
 - **記錄**：視需要啟用記錄。

新規則預設為啟用。滑動切換開關可將其停用。
- 5 按一下**發佈**。
- 6 執行相同的步驟來設定 vCenter Server 的規則。

備註 請確定在步驟 4 中針對 [目的地] 欄位選取 vCenter。

新增 VMware Cloud on AWS vCenter

您可以將 VMware Cloud on AWS - vCenter 新增為資料來源。

必要條件

- 取得用來將 VMware Cloud on AWS - vCenter 新增為資料來源的認證
 - a 登入 VMware Cloud Services 主控台。
 - b 按一下**我的服務**下的 **VMware Cloud on AWS**。
 - c 按一下所需 SDDC 的名稱。
 - d 選取**設定索引標籤**，然後執行下列工作：
 - 展開 **vCenter FQDN** 面板，然後複製或記下 vCenter FQDN。
 - 展開**預設 vCenter 使用者帳戶**面板，然後複製或記下使用者認證。
- 您必須至少具有 VMware Cloud on AWS vCenter 的**唯讀**權限。

程序

- 1 在 vRealize Network Insight 使用者介面中，移至**設定 > 帳戶和資料來源 > 新增來源**。
- 2 在 **VMware Cloud on AWS** 下，按一下 **VMware Cloud on AWS - vCenter**。

3 在新增 VMware Cloud on AWS - VMware vCenter 頁面中，

- 選取收集器虛擬機器。
- 提供已從 VMware Cloud Services 擷取的 vCenter FQDN。
- 提供已從 VMware Cloud Services 擷取的使用者認證。

4 按一下 **驗證**。

5 為資料來源輸入 **暱稱** 和 **附註** (如果有)，然後按一下 **提交**。

6 新增 [VMware Cloud on AWS NSX Manager](#)。

新增 VMware Cloud on AWS NSX Manager

您可以新增 VMware Cloud on AWS - NSX Manager 做為資料來源。

必要條件

- [產生 API Token](#)。
- 若要使用所有可用的 vRealize Network Insight 功能並在 VMware Cloud on AWS Policy Manager 上啟用 DFW IPFIX，您必須擁有 **管理員** 和 **NSX Cloud 管理員** 角色。不過，您可以透過擁有 **NSX Cloud 稽核員** (唯讀) 角色來存取這些功能。如需更多詳細資料，請參閱下表：

組織角色	服務角色	允許的動作
組織成員	管理員	新增資料來源、啟用 IPFIX
組織成員	管理員 和 NSX Cloud 管理員	新增資料來源、啟用 IPFIX
組織成員	VMware Cloud on AWS (所有角色)	新增資料來源、啟用 IPFIX
組織成員	NSX Cloud 稽核員	僅新增資料來源

程序

1 執行下列其中一項：

- 如果您尚未新增 VMware Cloud on AWS - vCenter，
 - a [新增 VMware Cloud on AWS vCenter](#)。
 - b 按一下 **新增 NSX Manager**。
- 如果您已新增 VMware Cloud on AWS - vCenter，
 - a 按一下 **設定 > 帳戶和資料來源 > 新增來源**。
 - b 在 **VMware Cloud on AWS** 下，按一下 **VMware Cloud on AWS - NSX Manager**。

2 在新增 VMC NSX Manager 帳戶頁面中，

- 選取對應的 vCenter。

會根據選取的 vCenter 自動選取收集器。VMware Cloud on AWS。您必須將 NSX Manager 新增到與對應 vCenter 的收集器虛擬機器相同的收集器虛擬機器。

- 提供您所產生的 IP 位址和 API Token。

將在 VMware Cloud on AWS SDDC 的[支援索引標籤](#)中提供 NSX Manager 的 IP。

3 按一下 **驗證**。

4 如果您想要收集 DFW 的 IPFIX 流程，請選取**啟用 DFW IPFIX**。

備註 在下列情況中會彈出錯誤訊息：

- 您沒有 NSX Cloud Admin 權限。
 - 您已將四個收集器新增至 DFW IPFIX 收集器設定檔。另請參閱[無法啟用 DFW IPFIX](#)。
-

5 為資料來源輸入**暱稱**和**附註** (如果有)，然後按一下 **提交**。

新增 Amazon Web Services

您可以在 vRealize Network Insight 中將 Amazon Web Services (AWS) 新增為資料來源。

您可以將下列兩種類型的 AWS 帳戶新增為資料來源。

- 主要和連結 AWS 帳戶
- 標準 AWS 帳戶

主要和連結 AWS 帳戶

主要 AWS 帳戶 (組織帳戶或付款人帳戶) 具有組織層級存取權，可透過 API 呼叫探索和列出組織中所有連結的 AWS 帳戶。

您的組織中所有新增至主要帳戶的 AWS 帳戶稱為連結帳戶。如需詳細資訊，請參閱 [〈ListAccount〉](#)。

主要 AWS 帳戶必須承擔連結 AWS 帳戶的角色，才能存取和控制連結 AWS 帳戶的資源。所有連結的 AWS 帳戶必須透過角色 ARN 信任主要 AWS 帳戶。如需有關角色的詳細資訊，請參閱 [〈AssumeRole〉](#)。

將主要 AWS 帳戶新增為資料來源時，所有連結的 AWS 帳戶將自動新增為資料來源。

標準 AWS 帳戶

標準 AWS 帳戶沒有主要和連結關聯性。

新增主要 AWS 帳戶

透過新增主要 AWS 帳戶，您可以在 vRealize Network Insight 中自動新增組織中的所有連結的 AWS 帳戶。

必要條件

- [針對 AWS API 存取設定防火牆](#)。
- [建立主要和連結帳戶原則](#)。
- [在 AWS 中建立角色](#)。

- 在**主要 AWS 帳戶**中建立使用者。
- 取得您在 AWS 主控台中建立的 Amazon 存取金鑰識別碼。如需更多詳細資料，請參閱 <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>。
- 取得連結 AWS 帳戶的角色 Amazon 資源名稱 (ARN)。請參閱〈[Amazon 資源名稱 \(ARN\) 和 AWS 服務命名空間](#)〉

程序

- 1 登入 vRealize Network Insight。
- 2 移至**設定 > 帳戶和資料來源 > 新增來源**。
- 3 在 [公有雲] 區段下，按一下 **Amazon Web Services**。
- 4 選取收集器 (Proxy) 虛擬機器。
- 5 輸入 Amazon 存取金鑰識別碼及對應的密碼存取金鑰。

vRealize Network Insight 需要 15 到 20 分鐘的時間來收集您的 AWS 帳戶資料。

- 6 按一下**驗證**。

如果探索到的虛擬機器數目超過平台和/或收集器節點的容量，則驗證會失敗。增加平台的區塊大小或建立叢集之後，才能新增資料來源。每個區塊大小 (含流程和不含流程) 的指定容量如下所示：

區塊大小	虛擬機器	流程狀態
大型	6k	已啟用
大型	10k	已停用
中型	3k	已啟用
中型	6k	已停用

- 7 完成 AWS 帳戶驗證後，選取**自動新增連結帳戶**選項。
- 8 在**角色 ARN**中，輸入連結 AWS 帳戶的角色 Amazon 資源名稱以信任主要 AWS 帳戶。
- 9 為資料來源輸入**暱稱**和**附註**。
- 10 按一下**提交**。

vRealize Network Insight 會驗證角色 ARN 並新增帳戶。

建立主要和連結帳戶原則

您必須為主要 Amazon Web Services (AWS) 帳戶建立主要帳戶原則，並為所有連結的 AWS 帳戶建立連結帳戶原則。您可以使用這些原則來管理 AWS 中的存取。

您可以將 AWS 原則附加到 IAM 身分識別，例如使用者或角色。如需詳細資訊，請參閱〈[原則和權限](#)〉。

程序

- 1 在 AWS 主控台中，移至 **IAM > 原則 > 建立原則**。

- 2 在**建立原則**頁面中，按一下 **JSON** 索引標籤。

3 在 JSON 文字方塊中，輸入原則。

選項	敘述
新增主要帳戶原則 備註 您必須在主要 AWS 帳戶中新增主要帳戶原則。	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }, { "Effect": "Allow", "Action": ["organizations:ListAccounts"], "Resource": "*" }, { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<Role ARNs>" }] } </pre>
新增連結帳戶 備註 您必須在主要 AWS 帳戶中新增的所有連結帳戶中新增連結帳戶原則。	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": [</pre>

選項	敘述
	<pre> "ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] }</pre>

4 按一下**檢閱原則**。

5 在**檢閱原則**區段下，輸入原則名稱並按一下**建立原則**。

後續步驟

逐一登入所有連結帳戶，並新增一個角色以信任您要新增至 vRealize Network Insight 的主要 AWS 帳戶，並附加連結帳戶原則。若要建立角色並附加已連結帳戶原則，請參閱在 [AWS 中建立角色](#)。

備註 如果在所有連結帳戶中建立的角色已包含標準原則權限並信任主要帳戶，請略過此步驟。

在 AWS 中建立角色

您可以建立 AWS 角色，以信任您要新增到 vRealize Network Insight 的帳戶。

必要條件

列出您在 [建立主要和連結帳戶原則](#) 中建立的所有連結帳戶原則的清單

程序

- 1 在 AWS 主控台中，移至**服務 > IAM > 角色 > 建立角色**。
- 2 在**建立角色**頁面上，按一下**其他 AWS 帳戶**。
- 3 在**帳戶識別碼**文字方塊中，輸入您要信任的主要帳戶識別碼，然後按**下一步: 權限**。
- 4 搜尋並選取所有連結帳戶原則，然後按**下一步: 標籤**。
- 5 在**檢閱**區段中，輸入**角色名稱**，然後按一下**建立角色**。

後續步驟

在[主要 AWS 帳戶中建立使用者](#)。

在主要 AWS 帳戶中建立使用者

您必須在 AWS 帳戶中建立使用者，以取得 Amazon 存取金鑰識別碼及對應的密碼存取金鑰，以便在 vRealize Network Insight 中新增資料來源時使用。

程序

- 1 登入 AWS 主控台。
- 2 移至**服務 > IAM > 使用者 > 新增使用者**。
- 3 在**新增使用者**頁面上，輸入**使用者名稱**，選取**程式設計存取核取方塊**，然後按一下**下一個權限**。
- 4 在**設定權限群組**下，按一下**已直接附加現有原則**，然後搜尋並選取您先前建立的帳戶原則。
 - 對於主要 AWS 帳戶，選取**主要帳戶原則**。
 - 對於標準 AWS 帳戶，選取**標準帳戶原則**。
- 5 按一下**下一步: 標籤 > 下一步: 檢閱**。
- 6 按一下**建立使用者**。
- 7 請記下**存取金鑰識別碼和密碼存取金鑰**。

後續步驟

- [新增主要 AWS 帳戶](#)。
- [新增標準 AWS 資料來源](#)。

針對 AWS API 存取設定防火牆

收集器虛擬機器需要 URL 清單以存取 AWS。

- AWS 可以在多個區域中部署。存在與不同區域相關聯的單獨 URL。如果您不知道區域或服務，請為 URL 提供萬用字元項目，例如 `*.amazonaws.com`。

備註 此萬用字元項目不適用於中國區域。

如果您想要對單獨 URL 進行更為精細的存取，則有以下 4 個基於區域的服務：

- 除了 GovCloud 和中國以外的區域
 - `ec2.<REGION>.amazonaws.com`
 - `logs.<REGION>.amazonaws.com`
 - `sts.<REGION>.amazonaws.com`
 - `iam.amazonaws.com`

GovCloud 區域

- `ec2.us-gov-west-1.amazonaws.com`
- `logs.us-gov-west-1.amazonaws.com`
- `sts.us-gov-west-1.amazonaws.com`
- `iam.us-gov.amazonaws.com`

中國 (北京) 區域

- `ec2.cn-north-1.amazonaws.cn.cn`
- `logs.cn-north-1.amazonaws.com.cn`
- `sts.cn-north-1.amazonaws.com.cn`
- `iam.cn-north-1.amazonaws.com.cn`

您可以根據 AWS 區域使用 `REGION` 的下列任一值：

區域名稱	區域
美國東部 (俄亥俄州)	<code>us-east-2</code>
美國東部 (北維吉尼亞州)	<code>us-east-1</code>
美國西部 (北加利福尼亞州)	<code>us-west-1</code>
美國西部 (奧勒岡州)	<code>us-west-2</code>
亞太地區 (孟買)	<code>ap-south-1</code>
亞太地區 (首爾)	<code>ap-northeast-2</code>
亞太地區 (新加坡)	<code>ap-southeast-1</code>
亞太地區 (雪梨)	<code>ap-southeast-2</code>
亞太地區 (東京)	<code>ap-northeast-1</code>
加拿大 (中部)	<code>ca-central-1</code>
歐盟 (法蘭克福)	<code>eu-central-1</code>
歐盟 (愛爾蘭)	<code>eu-west-1</code>
歐盟 (倫敦)	<code>eu-west-2</code>
南美洲 (聖保羅)	<code>sa-east-1</code>
Gov Cloud	<code>us-gov-west-1</code>
中國 (北京)	<code>cn-north-1</code>

新增標準 AWS 資料來源

新增 AWS 資料來源：

必要條件

- 針對 AWS API 存取設定組織防火牆。請參閱[針對 AWS API 存取設定防火牆](#)。
- 針對您要在 vRealize Network Insight 中新增的 AWS 帳戶建立標準帳戶原則。若要建立原則，請參閱[建立標準帳戶原則](#)。

- 在標準 AWS 帳戶中建立使用者。若要在 AWS 中建立使用者，請參閱[在主要 AWS 帳戶中建立使用者](#)。

程序

- 1 移至**設定 > 帳戶和資料來源 > 新增來源**。
- 2 在公有雲下，按一下 **Amazon Web Services**。
- 3 選取收集器 (Proxy) 虛擬機器。
- 4 輸入 Amazon 存取金鑰識別碼及對應的密碼存取金鑰。

備註 Amazon 存取金鑰識別碼是一個包含對應的密碼存取金鑰的 20 位字串。如需更多詳細資料，請參閱 <http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html>。

備註 若要將 Gov AWS Cloud 區域新增為資料來源，請透過使用有權存取 Gov Cloud 區域的 AWS 帳戶中的建議原則，以建立 AWS IAM 使用者。使用新建立帳戶的存取金鑰和密碼金鑰，將資料來源新增至 vRealize Network Insight。

此程序可能需要 15-20 分鐘的時間來新增和顯示帳戶資料。

- 5 按一下**驗證**。

如果探索到的虛擬機器數目超過平台和/或 Proxy 節點的容量，則驗證會失敗。增加平台的區塊大小或建立叢集之後，才能新增資料來源。

每個區塊大小 (含流程和不含流程) 的指定容量如下所示：

區塊大小	虛擬機器	流程狀態
大型	6k	已啟用
大型	10k	已停用
中型	3k	已啟用
中型	6k	已停用

- 6 驗證 AWS 帳戶後，您可以選取**啟用流程資料收集**，以取得更深入的見解。

在主要 AWS 帳戶中建立使用者

您必須在 AWS 帳戶中建立使用者，以取得 Amazon 存取金鑰識別碼及對應的密碼存取金鑰，以便在 vRealize Network Insight 中新增資料來源時使用。

程序

- 1 登入 AWS 主控台。
- 2 移至**服務 > IAM > 使用者 > 新增使用者**。
- 3 在**新增使用者**頁面上，輸入**使用者名稱**，選取**程式設計存取核取方塊**，然後按一下**下一個權限**。

- 4 在**設定權限**群組下，按一下**已直接附加現有原則**，然後搜尋並選取您先前建立的帳戶原則。
 - 對於主要 AWS 帳戶，選取**主要帳戶原則**。
 - 對於標準 AWS 帳戶，選取**標準帳戶原則**。
- 5 按一下**下一步: 標籤 > 下一步: 檢閱**。
- 6 按一下**建立使用者**。
- 7 請記下**存取金鑰識別碼**和**密碼存取金鑰**。

後續步驟

- [新增主要 AWS 帳戶](#)。
- [新增標準 AWS 資料來源](#)。

建立標準帳戶原則

您必須為標準 AWS 帳戶建立標準帳戶原則。透過此原則，您可以在 AWS 中管理存取權。

您可以將 AWS 原則附加到 IAM 身分識別，例如使用者或角色。如需詳細資訊，請參閱 [〈原則和權限〉](#)。

程序

- 1 在 AWS 主控台中，移至 **IAM > 原則 > 建立原則**。
- 2 在**建立原則**頁面中，按一下 **JSON 索引標籤**。

3 在 JSON 文字方塊中，輸入下列帳戶原則：

選項	敘述
新增標準帳戶原則 備註 您必須在要新增為資料來源的標準 AWS 帳戶中新增標準帳戶原則。	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListAccountAliases"], "Resource": ["*"] }, { "Effect": "Allow", "Action": ["ec2:Describe*"], "Resource": "*" }, { "Action": ["logs:Describe*", "logs:Get*", "logs:TestMetricFilter", "logs:FilterLogEvents"], "Effect": "Allow", "Resource": "*" }] }</pre>

4 按一下**檢閱原則**。

5 在**檢閱原則**區段下，輸入原則名稱並按一下**建立原則**。

後續步驟

- 在主要 AWS 帳戶中建立使用者。

AWS：地理封鎖支援

由於在公司防火牆上嚴格實作地理封鎖原則，因此，AWS API 呼叫限制為特定的 AWS 區域。vRealize Network Insight 支援 AWS 環境的地理封鎖原則。

在 vRealize Network Insight 中啟用地理封鎖原則：

程序

- 1 在**新增 AWS 資料來源**頁面上，輸入 AWS 存取金鑰和密碼金鑰。按一下**驗證**。
- 2 選取**僅允許存取特定的 AWS 區域**。從清單中選取 **AWS 區域**以啟用從區域自動收集。如果未選取此選項，則不會發生自動收集。

3 按一下提交。

新增 Azure 訂閱

您可以在 vRealize Network Insight 中將 Microsoft Azure 訂閱新增為資料來源。

必須具有下列權限：

- Microsoft.Resources/subscriptions/read
- Microsoft.Compute/virtualMachines/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/applicationSecurityGroups/read
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Network/networkWatchers/queryFlowLogStatus/*
- Microsoft.Network/networkWatchers/read
- Microsoft.Network/publicIPAddresses/read

或者，為了方便使用，您可以新增儲存區帳戶金鑰操作員服務角色、網路參與者和讀者權限。

程序

- 1 在設定頁面上，按一下帳戶和資料來源。
- 2 按一下新增來源。
- 3 在公有雲群組下，按一下 **Microsoft Azure**。
- 4 在新增 Azure 訂閱頁面中，提供所需資訊。

選項	動作
收集器虛擬機器	從下拉式功能表中選取收集器虛擬機器。
承租人識別碼	輸入 Azure Active Directory (AD) 的承租人識別碼。
應用程式識別碼	輸入應用程式識別碼。
應用程式秘密金鑰	輸入應用程式秘密金鑰。
訂閱識別碼	輸入訂閱識別碼。

- 5 按一下驗證。

您必須擁有至少一個虛擬機器、網路安全群組 (NSG)、NIC 和 VNet，才能成功驗證。

- 6 (選擇性) 如果您想要收集 NSG 流量記錄以取得流量的詳細資料見解，請選取**啟用 NSG 流量資料收集**核取方塊。
- 7 在**暱稱**文字方塊中，輸入暱稱。
- 8 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 9 按一下**提交**。

啟用 NSG 流量記錄

若要在 vRealize Network Insight 中啟用網路安全群組 (NSG) 流量資料收集，您必須在 Azure 環境中啟用 NSG 流量記錄。

與 Azure 相關的程序和工作記錄在 <https://docs.microsoft.com/en-us/azure/network-watcher/> 中。

必要條件

確認您有正確的權限。如需權限的相關資訊，請參閱[支援的產品和版本](#)。

程序

- 1 在 Azure 環境中啟用網路監看員。如需更多資訊，請參閱 Azure 的《網路監看員說明文件》中的〈記錄虛擬機器網路流量〉教學課程。
- 2 在 Azure 環境中登錄見解提供者。如需更多資訊，請參閱 Azure 的《網路監看員說明文件》中的〈記錄虛擬機器網路流量〉教學課程。
- 3 在 Azure 環境中啟用 NSG 流量記錄。如需更多資訊，請參閱 Azure 的《網路監看員說明文件》中的〈記錄虛擬機器網路流量〉教學課程。
- 4 在 Microsoft Azure 入口網站中，按一下**儲存區帳戶 > Blob**。
- 5 選取要儲存流量記錄的容器，按一下**變更存取層級**，然後選取**容器 (容器和 Blob 的匿名讀取權限)**。

您必須針對儲存流量記錄的所有容器執行此步驟。

新增 VMware PKS

您可以新增 VMware PKS 作為資料來源，並在 vRealize Network Insight 中擷取 PKS 叢集詳細資料。

必要條件

您必須新增對應的 NSX-T Manager。

程序

- 1 在 [設定] 頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在 [容器] 下，選取 **VMware PKS**。

4 在 [新增資料來源] 頁面上，提供下列詳細資料：

欄位名稱	說明
NSX-T Manager	選取支援 VMware PKS 部署的基礎網路的 NSX-T Manager。
收集器 (Proxy) 虛擬機器	vRealize Network Insight 會自動選取與所選 NSX-T Manager 相關聯的對應收集器虛擬機器。 備註 新增為 NetFlow 收集器的收集器虛擬機器不在清單中。
API 主機名稱 (FQDN)	輸入 PKS API 伺服器的 FQDN 詳細資料。
使用者名稱	輸入有權存取叢集的 PKS 使用者名稱。 備註 使用者必須具有 <code>pks.clusters.admin</code> 權限。
密碼	輸入密碼。 備註 目前不支援包含特殊字元 (例如 <code>&, (,), , <, >, `</code>) 的密碼。

5 按一下 **驗證**。

將會顯示驗證成功訊息。

6 輸入資料來源的暱稱，然後視需要新增任何說明附註。

7 按一下 **提交**。

如果您看到無法從收集器虛擬機器連線到一或多個 Kubernetes 叢集主控主機錯誤訊息，請在收集器虛擬機器上執行下列命令：

a `pks login -a PKS_API_Server - u username -p password -k`

b `pks clusters`

確保叢集狀態為已成功。

c `pks cluster Kubernetes_Cluster_Name`

d `telnet Kubernetes_Master_Host Kubernetes_Master_port`

確認主控主機能夠連線。

e 針對從 step b 探索到的每個 Kubernetes 叢集，重複 step c 和 step d。

新增 Kubernetes

您可以新增 Kubernetes 作為資料來源，並將 Kubernetes 叢集詳細資料擷取到 vRealize Network Insight。

備註 Kubernetes 叢集和對應的 NSX-T Manager 必須新增至相同的收集器虛擬機器。

必要條件

- 在 vRealize Network Insight 中新增 NSX-T Manager。
- 確保 Kubernetes API 伺服器可從收集器虛擬機器進行存取。

程序

- 1 在 [設定] 頁面上，按一下 **帳戶和資料來源**。
- 2 按一下 **新增來源**。
- 3 在 [容器] 下，選取 **Kubernetes**。
- 4 在 [新增資料來源] 頁面上，提供下列詳細資料：

欄位名稱	說明
NSX-T Manager	選取支援 Kubernetes 的基礎網路的 NSX-T Manager。
收集器 (Proxy) 虛擬機器	vRealize Network Insight 會自動選取與所選 NSX-T Manager 相關聯的對應收集器虛擬機器。 備註 新增為 NetFlow 收集器的收集器虛擬機器不在清單中。
Kubeconfig	按一下 瀏覽 ，並上傳包含 Kubernetes 叢集詳細資料的 Kubernetes 組態檔。如需有關 Kubeconfig 組態檔格式的詳細資訊，請參閱 Kubernetes 說明文件 。 備註 Kubeconfig 檔案中設定的使用者必須擁有 列出 和 監視 權限。

- 5 按一下 **驗證**。
將會顯示驗證成功訊息。
- 6 輸入資料來源的暱稱，然後視需要新增任何說明附註。
- 7 按一下 **提交**。

結果

vRealize Network Insight 現在可擷取 Kubernetes 叢集詳細資料。

後續步驟

移至 Kubernetes 儀表板並檢視詳細資料，請參閱 [檢視 Kubernetes 詳細資料](#)。

新增 OpenShift

您可以新增 OpenShift 做為資料來源，並將 OpenShift 詳細資料擷取到 vRealize Network Insight。

備註 OpenShift 和對應的 NSX-T Manager 必須新增至相同的收集器虛擬機器。

必要條件

- 在 vRealize Network Insight 中新增 NSX-T Manager。

程序

- 1 在 [設定] 頁面上，按一下 **帳戶和資料來源**。
- 2 按一下 **新增來源**。
- 3 在 [容器] 下，選取 **OpenShift**。

- 4 在 [新增資料來源] 頁面上，提供下列詳細資料：

欄位名稱	說明
NSX-T Manager	選取支援 OpenShift 的基礎網路的 NSX-T Manager。
收集器 (Proxy) 虛擬機器	vRealize Network Insight 會自動選取與所選 NSX-T Manager 相關聯的對應收集器虛擬機器。 備註 新增為 NetFlow 收集器的收集器虛擬機器不在清單中。
Kubeconfig	按一下 瀏覽 ，並上傳包含 Kubernetes 叢集詳細資料的 Kubernetes 組態檔。如需有關 Kubeconfig 組態檔格式的詳細資訊，請參閱 Kubernetes 說明文件 。 備註 Kubeconfig 檔案中設定的使用者必須擁有 列出 和 監視 權限。

- 5 按一下 **驗證**。

將會顯示驗證成功訊息。

- 6 輸入資料來源的暱稱，然後視需要新增任何說明附註。

- 7 按一下 **提交**。

結果

vRealize Network Insight 現在可擷取 OpenShift 詳細資料。

後續步驟

請參閱[檢視 Kubernetes 詳細資料](#)中的詳細資料。

新增 Palo Alto Networks Panorama

您可以在 vRealize Network Insight 中將 Palo Alto Networks Panorama 新增為資料來源。

必要條件

確保您擁有具有 XML API 存取權的**管理員角色**。如需更多詳細資料，請參閱 [Palo Alto 網路](#)。

備註 vRealize Network Insight 目前不會擷取直接在裝置中定義但未顯示在 Panorama 中的本機 Palo Alto 網路原則。

程序

- 1 在設定頁面上，按一下 **帳戶和資料來源**。
- 2 按一下 **新增來源**。
- 3 在防火牆下，按一下 **Palo Alto Networks Panorama**。
- 4 在 **新增 Palo Alto Networks Panorama 帳戶或來源**頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。

選項	動作
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 按一下 **驗證**。
- 在 **暱稱** 文字方塊中，輸入暱稱。
- (選擇性) 在 **附註** 文字方塊中，您可以視需要新增附註。
- 按一下 **提交**。

新增 Check Point 管理伺服器

vRealize Network Insight 支援 Check Point 安全性管理程式 (SmartCenter) 和 Check Point 多網域安全性 (MDS) 管理伺服器。

必要條件

確保您有正確的權限。如需權限的相關資訊，請參閱 [〈Check Point 防火牆〉](#)。

程序

- 在 **設定** 頁面上，按一下 **帳戶和資料來源**。
- 按一下 **新增來源**。
- 在 **防火牆** 群組下，按一下 **Check Point 管理伺服器**。
- 在 **新增 Check Point 管理伺服器帳戶或來源** 頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。 備註 如果您要新增 Check Point MDS 管理伺服器，則必須提供 MDS 伺服器的 IP。您無法新增 MDS 伺服器的網域管理伺服器 IP 做為個別資料來源。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 按一下 **驗證**。
- 在 **暱稱** 文字方塊中，輸入暱稱。
- (選擇性) 在 **附註** 文字方塊中，您可以視需要新增附註。
- 按一下 **提交**。

新增 Cisco ASA

您可以在 vRealize Network Insight 中將 Cisco ASA 新增為資料來源。

必要條件

您必須具有在啟用模式下進行切換的權限。使用者的密碼必須與用於 Cisco ASA 啟用模式的密碼相同。

程序

- 1 在**設定**頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在**防火牆**群組下，按一下**Cisco ASA**。
- 4 在**新增 Cisco ASA 帳戶或來源**頁面中，提供所需資訊：

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入使用者名稱。 備註 使用者應具有啟用模式權限，以便將終端機長度設為 0 以及切換安全內容。
密碼	輸入密碼。 備註 請確保輸入的密碼與用於 Cisco ASA 的啟用模式的密碼相同。

- 5 (選擇性) 若要實現更豐富的資料收集，請按一下**使用 SNMP (建議用於更豐富的資料收集)**核取方塊。
- 6 按一下**驗證**。
- 7 在**暱稱**文字方塊中，輸入暱稱。
- 8 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 9 按一下**提交**。

新增 Fortinet FortiManager

在 vRealize Network Insight 中，您可以將 Fortinet FortiManager 新增為資料來源：

必要條件

確認下列各項：

- 您使用的是 FortiManager 6.0.1 版。
- 您至少具有**受限制的使用者**角色，能夠存取所有 ADOM 和原則套件。
- 您可以從命令列介面 (CLI) 啟用 **rpc-permit read-write** 存取權。

若要設定 **rpc** 權限，請在 FortiManager CLI 中使用下列命令：

```
config system admin user
edit "<administrator name>"
set rpc-permit [none | read | read-write ]
end
```

程序

- 1 在設定頁面中，按一下**帳戶和資料來源 > 新增來源**。
- 2 在**防火牆區段**下，按一下**Fortinet FortiManager**。
- 3 在**新增 Fortinet FortiManager 帳戶或來源**頁面中，輸入所需資訊：

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入要用於此資料來源的使用者名稱。
密碼	輸入密碼。

- 4 按一下**驗證**。
- 5 在**暱稱**文字方塊中，輸入資料來源的暱稱。
- 6 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 7 按一下**提交**。

新增 Arista 交換器 SSH

您可以在 vRealize Network Insight 中將 Arista 交換器 SSH 新增為資料來源。

必要條件

確保您擁有下列權限：

- 唯讀使用者。
- 唯讀 SNMP 使用者。

程序

- 1 在設定頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在**路由器和交換器**下，按一下**Arista 交換器 SSH**。

4 在新增 Arista 交換器 SSH 帳戶或來源頁面中，提供所需資訊。

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。 備註 您必須輸入您在 VMware NSX Manager 中使用的相同 IP/FQDN，才能設定此交換器。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 按一下 **驗證**。
- (選擇性) 若要實現更豐富的資料收集，請按一下 **使用 SNMP (建議用於更豐富的資料收集)** 核取方塊。
- 在 **暱稱** 文字方塊中，輸入暱稱。
- (選擇性) 在 **附註** 文字方塊中，您可以視需要新增附註。
- 按一下 **提交**。

新增 Dell OS10 交換器

您可以在 vRealize Network Insight 中將 Dell OS10 交換器新增為資料來源。

必要條件

如需支援的 Dell 交換器的相關資訊，請參閱 [〈支援的產品和版本〉](#)。

程序

- 在 **設定** 頁面上，按一下 **帳戶和資料來源**。
- 按一下 **新增來源**。
- 在 **路由器和交換器** 群組下，按一下 **Dell OS10**。
- 在 **新增帳戶或來源** 頁面中，提供所需資訊。

選項	動作
收集器虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入使用者名稱。
密碼	輸入密碼。

- 按一下 **驗證**。
將會顯示驗證成功訊息。
- 若要啟用 SNMP 或資料收集，請選取 **使用 SNMP**。

- 7 在**暱稱**文字方塊中，輸入暱稱。
- 8 在**附註**文字方塊中，您可以視需要新增附註。
- 9 按一下**提交**。

後續步驟

[在 Dell OS10 交換器上啟用遙測](#)

在 Dell OS10 交換器上啟用遙測

您可以在 Dell OS10 交換器上啟用遙測，以整合 Dell 交換器上的緩衝區統計資料和追蹤。

必要條件

新增 Dell OS10 交換器

從交換器接收要求時，vRealize Network Insight 收集器會儲存或緩衝已定義連接埠上的封包。

當緩衝區大小隨著輸入速率的增加 (相較於輸出速率) 而增加時，要求可能會減慢或逾時。Dell OS10 交換器使用 gRPC 來擷取此類度量資訊，您可以在 vRealize Network Insight 上查看此資訊。這可讓您診斷因網路壅塞而可能導致的應用程式效能問題，並主動提供壅塞對應用程式和網路的影響。

程序

- ◆ 在 Dell OS10 交換器上執行下列命令：

```
telemetry
enable
!
destination-group dg03
 destination vRNI Collector IP 50000
!
subscription-profile sp03
 sensor-group bgp
 sensor-group buffer
 sensor-group device
 sensor-group environment
 sensor-group interface
 sensor-group lag
 sensor-group system
 destination-group dg03
 encoding gpb
 transport grpc no-tls
 source-interface ethernet1/1/1
```

結果

vRealize Network Insight 收集器會從 Dell OS10 交換器收集下列遙測資訊。

- per-port egress unicast queues
- per-port egress multicast queues

- per-port egress service pool
- per priority group ingress shared headroom
- per service pool ingress

後續步驟

執行下列任一查詢：

- `show ports where metric > X in time range`
- `show switches where metric > X in time range`
- `port show metrics in time range`
- `switch show metrics in time range`
- `show switches where at least one port metric > X in time range`

您會看到相應的事件已觸發。例如，SwitchPort Buffer Threshold Exceeded Event。

您也可以搜尋介面尖峰緩衝區使用量度量，並找出要求變慢的原因。

新增 Huawei 6800/7800/8800 系列

vRealize Network Insight 支援多個 Huawei 雲端引擎系列。

必要條件

使用者必須至少擁有讀取權限。

程序

- 1 在 [設定] 頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在**路由器和交換器**下，選取 **Huawei 6800/7800/8800 系列**。
- 4 輸入下列資訊：

內容	說明
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取 Proxy 虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
Username	輸入要用於此資料來源的使用者名稱。
Password	輸入密碼。

- 5 按一下**驗證**。
- 6 如果為資料收集啟用 SNMP，請選取 **SNMP 版本**。
 - a 對於 2c，輸入相關聯的社群字串。

b 對於 3，輸入下列項目：

- Username
- Context Name
- Authentication Type

7 視需要提供暱稱和附註。

8 按一下**提交**。

後續步驟

您可以將 vRealize Network Insight 的下列功能與 Huawei 裝置或路由器搭配使用。

- 虛擬機器-虛擬機器路徑
- 虛擬機器基礎拓撲
- Huawei 路由器或交換器儀表板
- 度量：交換器連接埠和路由器介面度量
- 儀表板
 - Huawei 路由器或交換器
 - 路由器介面
 - 連接埠通道
 - 交換器連接埠
 - 路由
- 高可用性：支援 M-LAG (多機箱鏈路聚合) 和 VRRP (虛擬路由器備援通訊協定)
- 搜尋
 - Huawei 的 VRF (虛擬路由和轉送)
 - Huawei 的路由器介面
 - Huawei 的交換器連接埠
 - Huawei 的連接埠通道
 - Huawei 的路由
- Huawei NetStream 資料監控

新增 Cisco ACI

您可以將 Cisco ACI 新增為資料來源。此功能僅適用於企業授權使用者。

必要條件

- 若要透過 HTTPS 連線至 APIC 控制器 REST API，您必須擁有所有承租人的存取權，並具有唯讀權限。
- 對於 SNMP，您必須具有唯讀權限。
- 確保您擁有具有下列權限的本機使用者角色：
 - 安全性網域：全部
 - 角色：管理員
 - 存取權：讀取

如需如何在 Cisco ACI 中建立本機使用者的詳細資料，請參閱《Cisco APIC 安全性組態指南》中的〈存取、驗證和帳戶處理〉一節。

程序

- 1 在設定下的帳戶和資料來源頁面中，按一下**新增來源**。
- 2 在**其他**下，按一下**Cisco ACI**。
- 3 在**新增 Cisco ACI 帳戶或來源**頁面中，提供所需資訊：

選項	動作
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取收集器虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入使用者名稱。 備註 如果使用者為網域使用者，則必須在使用者名稱前新增 apic: 。例如，如果使用者名為 user1 ，且使用者屬於網域 domain1 ，則將使用者名稱指定為 apic:domain1\\user1 。網域名稱區分大小寫。
密碼	輸入密碼。

- 選取收集器虛擬機器。
- 提供叢集中任何 APIC 控制器的 IP 位址。

備註 無需在 ACI 網狀架構中新增個別交換器。

- 提供使用者認證。
- vRealize Network Insight 從個別交換器透過 SNMP 收集度量資料。若要啟用此工作，請選取**使用 SNMP**。

- 4 按一下**驗證**。
- 5 為資料來源輸入**暱稱**和**附註** (如果有)，然後按一下**提交**

針對 NetFlow 和 sFlow 新增實體流量收集器

您可以新增一個實體流量收集器，並設定交換器以將 sFlow 和 NetFlow 記錄推送到收集器。用於 NetFlow 或 sFlow 的收集器虛擬機器是一個專用收集器。它無法用於任何其他資料來源。如果在 Proxy 伺服器上還新增了其他任何資料來源，則它無法用作 sFlow 和 NetFlow 的實體流量收集器。

程序

- 1 在設定頁面中，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在**流量**下，按一下**實體流量收集器 (Netflow、sFlow)**。
僅實體收集器上接受 sFlow。
- 4 視需要輸入**暱稱**和**附註**。
- 5 按一下**提交**。

結果

備註 vRealize Network Insight 收集了 sFlow 的封包範例，因此無法顯示流量的完整度量。

後續步驟

設定交換器以將流量推送到實體流量收集器。

- 定義目的地 (vRealize Network Insight 中新增的收集器 IP 位址)。
- 設定流量收集器的連接埠。
- 指派輪詢間隔。

備註 設定程序取決於您要設定的交換器。如需詳細資訊，請參閱特定的交換器說明文件。

新增 vRealize Log Insight

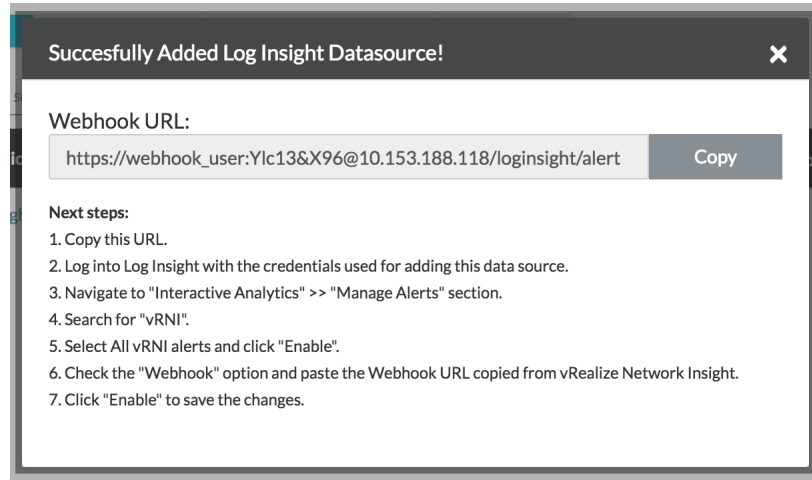
vRealize Log Insight 會在 NSX 事件發生時以動態方式收集 NSX 記錄。但是，vRealize Network Insight 每 10 分鐘從 NSX 收集資料一次。因此，在 vRealize Network Insight 中新增 vRealize Log Insight 可讓您更快地取得事件資訊，而不是只能等待。

在 vRealize Network Insight 和 vRealize Log Insight 整合中，vRealize Log Insight 所產生的警示會由 vRealize Network Insight 使用。只要您建立或修改安全群組，NSX 的記錄便會傳送到 vRealize Log Insight，後者後傳送警示。收到警示後，vRealize Network Insight 輪詢在其上建立安全群組的 NSX Manager，並解壓縮變更安全群組的資料。目前，此整合僅支援與安全群組 CRUD 相關的警示。

如需 vRealize Network Insight 中支援的 vRealize Log Insight 版本清單，請參閱《[VMware 產品互通性對照表](#)》。

程序

- 1 建立或重複使用有權存取 vRealize Log Insight API 的 vRealize Log Insight 使用者。
- 2 在安裝和支援頁面上，按一下帳戶和資料來源。
- 3 按一下新增來源。
- 4 在記錄伺服器下按一下 Log Insight。
- 5 在新增 Log Insight 伺服器帳戶或來源頁面上，按一下頁面標題旁邊的說明。將顯示一個快顯視窗，其中提供了新增 vRealize Log Insight 資料來源的必要條件，以及在 vRealize Log Insight 上啟用



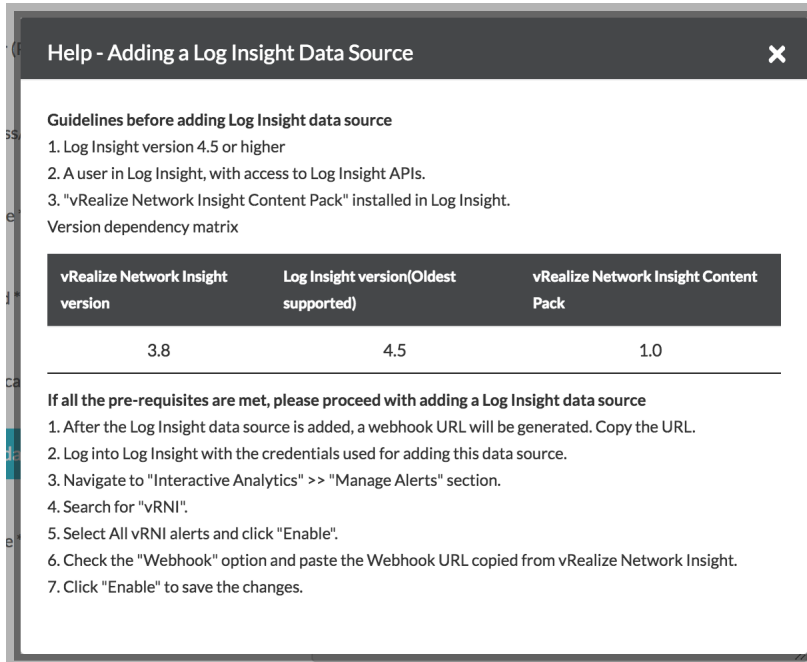
Webhook URL 的說明。

備註 在新增資料來源後產生的 Webhook URL 在 vRealize Log Insight 中使用。

- 6 輸入必要的詳細資料。

名稱	說明
收集器 (Proxy) 虛擬機器	選取為資料收集程序部署的資料收集器的 IP 位址。
IP 位址/FQDN	輸入資料來源的 IP 位址或 FQDN。
使用者名稱	輸入要用於特定資料來源的使用者名稱。
密碼	輸入資料來源的密碼。
驗證提供者	為您提供的認證選取適當的驗證提供者。

- 7 建立資料來源後，會顯示一個快顯視窗，視窗將提供 Webhook URL 以及在 vRealize Log Insight 上啟用此 URL 必須執行的步驟。複製 Webhook URL。使用用於新增此資料來源的認證登入。在 vRealize Log Insight 應用程式中啟用警示，然後設定此 Webhook URL。傳送測試警示，以確保整合成功。



備註 vRealize Network Insight 中 vRealize Log Insight 資料來源上顯示的任何警示會在 1 小時內得到解決。

新增 Infoblox

vRealize Network Insight 允許您將 Infoblox Grid 新增為 DNS 資料提供者。

Infoblox DNS 提供了管理和控制 DNS 的進階解決方案。它使用 Infoblox Grid 來確保 DNS 在整個網路中高度可用。來自 Infoblox 的 DNS 資料僅用於擴充來源或目的地 IP 位址和實體裝置相關聯的流程。

Infoblox DNS 資料與透過使用 CSV 匯入的 DNS 資料共存。

如果在收集器上設定 Infoblox DNS 資料來源，則也可以在相同的收集器上設定其他資料來源。對於 Infoblox，不需要專用的收集器。

考量事項

- 在目前版本中，vRealize Network Insight 僅支援 Infoblox 的單一網格模式。
- 目前版本僅支援 A 記錄。目前不支援共用 A 記錄。
- 在目前版本中，僅標記為實體的 IP 位址支援 DNS 擴充。
- 如果單一實體 IP 位址有多個 FQDN，則會傳回所有 FQDN。

程序

- 1 在設定頁面上，按一下帳戶和資料來源。
- 2 按一下新增來源。
- 3 按一下 DNS 下的 Infoblox。
- 4 提供下列資訊：

表 3-5.

內容	說明
Collector VM	從下拉式功能表中選取收集器虛擬機器。
IP Address/FQDN	輸入 Infoblox Grid 的 IP 位址/FQDN。
Username	輸入要用於特定資料來源的使用者名稱。
Password	輸入密碼。

- 5 按一下驗證。

備註 確定您擁有 API Privilege 以存取 Infoblox API。

- 6 為資料來源輸入暱稱和附註 (如果有)，然後按一下提交將 Infoblox DNS 資料來源新增至環境。

新增 F5 BIG-IP

vRealize Network Insight 支援 F5 BIG-IP 的路由器和負載平衡器功能。支援虛擬機器-虛擬機器路徑、高可用性、VRF、路由、路由器介面、交換器連接埠、連接埠通道、交換器連接埠度量、VRF 儀表板、交換器儀表板和路由器儀表板等功能。若要搜尋 F5 BIG IP 實體，請使用查詢字串 F5 BIG-IP Data Source。vRealize Network Insight 不支援虛擬機器-虛擬機器路徑中的 LLDP 鄰接項目或鄰接裝置。

將 F5 BIG-IP 新增為資料來源：

必要條件

- 使用者必須具有：
 - 可存取所有磁碟分割的 Guest 角色或唯讀權限。
 - 對 REST API 的存取權。
 - 對 TMSH 終端機的存取權。
- 在裝置上啟用 SSH。

為 SSH 啟用 password authentication，如下所示：

備註

- 使用 root 或管理員角色權限可變更 SSHD 組態。
- 在 vRealize Network Insight 中新增 F5 BIG-IP 資料來源時，請勿使用 root 使用者權限。
- Root 使用者沒有 HTTP 存取權。root 使用者權限用於管理目的。

```
[root@bigip:Active] config # tmsh
root@bigip(Active) (/Common) (tmsh) # edit sys sshd

## Adding the following configuration ##

modify sshd {
    include "
        ChallengeResponseAuthentication no
        PasswordAuthentication yes"
    }
#####
Save changes? (y/n/e) y
root@bigip(Active) (/Common) (tmsh) #
root@bigip(Active) (/Common) (tmsh) # save sys config

root@bigip(Active) (/Common) (tmsh) # show running-config sys sshd
sys sshd {
    include "
        ChallengeResponseAuthentication no
        PasswordAuthentication yes"
    }
```

程序

- 1 在 [設定] 頁面上，按一下帳戶和資料來源。
- 2 按一下新增來源。
- 3 在路由器和交換器下，選取 F5 BIG-IP。
- 4 提供下列資訊：

內容	說明
收集器 (Proxy) 虛擬機器	從下拉式功能表中選取 Proxy 虛擬機器。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
Username	輸入要用於此資料來源的使用者名稱。
Password	輸入密碼。

- 5 在文字方塊中輸入資訊後，按一下驗證。

6 如果為資料收集啟用 SNMP，請選取 **SNMP 版本**。

- a 如果您選取 2c，請輸入相關聯的社群字串。
- b 如果您選取 3，請輸入下列內容：

- Username
- Context Name
- Authentication Type

備註 確保在 F5 BIG-IP 使用者介面主控台上設定 SNMP。

- a 登入 F5。
 - b 導覽至**系統 > SNMP**。
 - c 移至 **SNMP > 代理程式 > 存取 (v1,v2c)**。
 - d 輸入社群字串。
 - e 輸入來源 IP 位址。
 - f 選取**唯讀**存取權。
 - g 按一下**已完成**。
-

7 視需要提供**暱稱**和**附註**。按一下**提交**。

新增 ServiceNow

ServiceNow 設定管理資料庫 (CMDB) 可讓您全面瞭解資料中心內的軟體和硬體基礎結構及其之間的關係，這樣可協助您管理詳細目錄。透過 ServiceNow 整合，vRealize Network Insight 可以探索 ServiceNow CMDB 中可用的應用程式，使您可以直接將其新增至 vRealize Network Insight。

CMDB 概念

基本上，CMDB 包含以下項目：

- **組態項目**：系統中的實體或元件。例如，電腦、交換器、服務、應用程式、伺服器或虛擬機器。
- **關聯性**：組態項目之間的通訊的連結或類型。範例：取決於、執行於、交換資料。

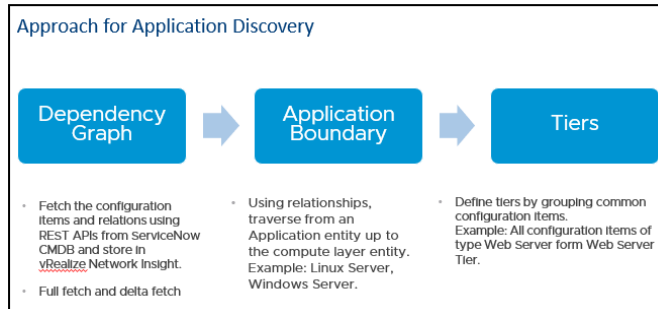
每個組態項目都具有已定義的架構。

- **組態項目類別**：每個組態項目必須與定義其內容的類別相關聯。
- **關聯性類別**：義的組態項目之間的關係類型。

您可以延伸這兩個類別以新增其他內容或自訂內容。

ServiceNow 支援應用程式服務，該服務是一組提供服務的互連應用程式和主機。ServiceNow 允許您透過使用 API 手動建立應用程式服務，也可以透過服務對應自動探索。所有這些應用程式均儲存在 ServiceNow CMDB 中。

當您將 ServiceNow 資料來源新增至 vRealize Network Insight 時，vRealize Network Insight 會從 ServiceNow CMDB 組態檔擷取組態項目和關聯性。



vRealize Network Insight 預設會定期擷取資料。

- 完整資料擷取每 12 小時進行一次，將擷取定義 CMDB 組態之類別的所有記錄。此外，當您新增或更新資料來源時，會執行完整擷取。
- 差異擷取每 2 分鐘進行一次，將擷取 CMDB 組態中所定義類別的所有新增、修改和刪除的記錄。vRealize Network Insight 需要大約 12 分鐘才能在使用者介面上反映這些詳細資料。

備註 vRealize Network Insight 僅在完成擷取期間擷取類別階層和關聯性類型。

限制的預設值

限制名稱	說明	預設值	超出此限制的影響
maxAppsPerDataSource	每個資料來源的最大應用程式數。	5000	資料來源停止擷取資料並在資料來源及事件頁面上顯示錯誤，並且未更新應用程式。
maxTiersPerApp	每個應用程式可儲存的最大層數。	150	在層數減少到滿足限制之前，不會更新應用程式。
maxMembersPerApp	每個應用程式可儲存的最大成員數。	5000	在成員數減少到滿足限制之前，不會更新應用程式。
maxGraphTraversalStackSize	圖形周遊中使用的堆疊的大小上限。	10000	將不會建立應用程式，並擲回 <code>SizeLimitExceededException</code> 。
maxResponseAppCount	可以在 API 回應中傳回的最大應用程式數。	5000	僅傳回滿足限制的應用程式數，並且使用者介面顯示錯誤。

新增 ServiceNow

您可以將 ServiceNow 做為資料來源新增到 vRealize Network Insight 中，並擷取應用程式和層詳細資料。

必要條件

您必須擁有管理員權限，才能新增資料來源。

程序

- 1 在 [設定] 頁面上，按一下 **帳戶和資料來源**。

- 2 按一下**新增來源**。
- 3 在 CMDB 下，選取 **ServiceNow**。
- 4 在 [新增資料來源] 頁面上，提供下列詳細資料：

欄位名稱	說明
收集器 (Proxy) 虛擬機器	ServiceNow 的主機 URL
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。
使用者名稱	輸入要用於此資料來源的使用者名稱。 備註 您計劃新增的使用者必須是 ServiceNow 中的 管理員 或 唯讀管理員 。
密碼	輸入密碼。

- 5 按一下**驗證**。
將會顯示驗證成功訊息。
- 6 新增自訂 CMDB 組態：
 - a 選取**自訂 CMDB 組態**。
 - b 按一下**下載**以下載預設組態檔。
 - c 更新檔案內容。請參閱**自訂 CMDB 組態**。
 - d 在 [新增資料來源] 頁面上，瀏覽並選取已更新的 JSON 檔案。
- 7 輸入資料來源的暱稱，然後新增任何說明附註。
- 8 按一下**提交**。

後續步驟

新增 ServiceNow 資料來源後，vRealize Network Insight 會探索您新增至 vRealize Network Insight 中的 ServiceNow CMDB 中的可用應用程式。如需詳細資訊，請參閱 [新增探索到的應用程式](#)。

預設 CMDB 組態檔

vRealize Network Insight 支援使用 JSON 格式的組態檔自訂 ServiceNow。

```
{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": false,
  "ignoreWorkloadCheck": false,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    }
  ],
}
```

```

{
  "name": "relationshipTypeClasses",
  "value": [
    "*"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadRelationshipTypeClasses",
  "value": [
    "Hosted on::Hosts",
    "Instantiates::Instantiated by",
    "Runs on::Runs",
    "Virtualized by::Virtualizes"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": false
},
{
  "name": "workloadCIClasses",
  "value": [
    "cmdb_ci_computer",
    "cmdb_ci_vm_instance",
    "cmdb_ci_vmware_instance"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "relationClasses",
  "value": [
    "cmdb_rel_ci"
  ],
  "valueType": "CI_CLASS",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredCIClasses",
  "value": [
    "cmdb_ci_vcenter_server_obj"
  ],
  "valueType": "CI_VALUE",
  "systemGenerated": true,
  "expandCIClass": true
},
{
  "name": "ignoredTierCIClasses",
  "value": [
  ],
  "valueType": "CI_VALUE",

```

```

    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "trackedCIClasses",
    "value": [
      "cmdb_ci_appl",
      "cmdb_ci_cluster",
      "cmdb_ci_cluster_node",
      "cmdb_ci_database",
      "cmdb_ci_lb_service",
      "cmdb_ci_spkg",
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint",
      "cmdb_ci_network_adapter",
      "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  }
],
"traversalRule": [
  {
    "fromNode": [
      "applicationClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  },
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 3
  }
],
"traversalStopRule": [
  {
    "fromNode": [
      "trackedCIClasses",

```

```

        "workloadCIClasses"
    ],
    "toNode": [
        "applicationClasses"
    ],
    "relationship": [
        "relationshipTypeClasses"
    ],
    "priority": 5
}
],
"associationRule": [
    {
        "fromNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "toNode": [
            "workloadCIClasses"
        ],
        "relationship": [
            "workloadRelationshipTypeClasses"
        ],
        "priority": 5
    }
]
}

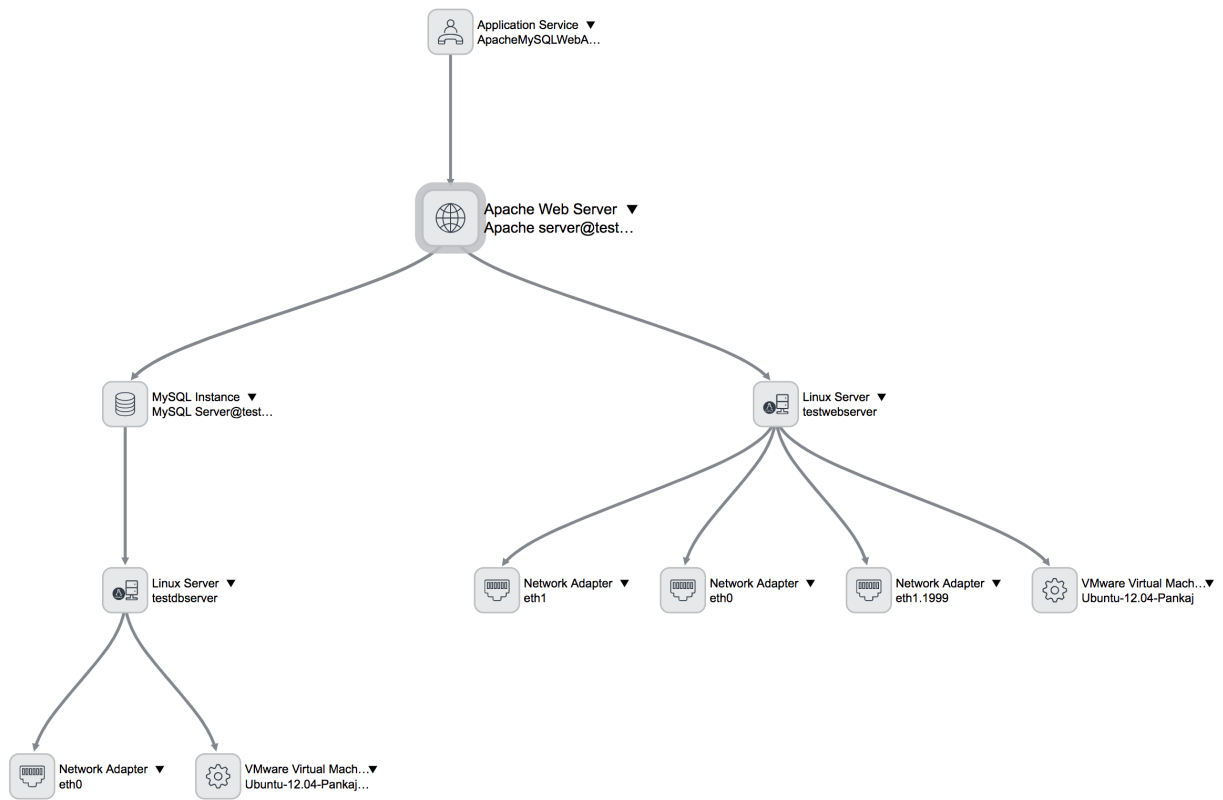
```

vRealize Network Insight 當組態變更時，可能需要 30 分鐘進行完整資料擷取並重新計算所有應用程式。

範例：ServiceMap 和使用預設 CMDB 組態探索到的應用程式的範例

範例：vRealize Network Insight 上用於新增應用程式的已更新頁面

這可讓 vRealize Network Insight 探索 ServiceNow 中的應用程式。



Modify Application

Application Name * ApacheMySQLWebApp

Application Total: 2 VMs | 0 Physical IPs

▼ Tier		Tier Total: 1 VMs 0 Physical IPs
Name *	<u>ApacheMySQLWebApp.apache_web_server</u>	
Virtual Machines / IP Addresses *	VM Names ▼ <u>'Ubuntu-12.04-Pankaj'</u>	1 VMs
Add another Condition		
▼ Tier		Tier Total: 1 VMs 0 Physical IPs
Name *	<u>ApacheMySQLWebApp.db_mysql_instance</u>	
Virtual Machines / IP Addresses *	VM Names ▼ <u>'Ubuntu-12.04-Dark-Pankaj-1'</u>	1 VMs
Add another Condition		

[Add Tier](#)☐ Analyze Flows

Save

Cancel

自訂 CMDB 組態

若要支援不同的自訂，ServiceNow 和 vRealize Network Insight 整合支援一般組態。CMDB 組態必須採用 JSON 格式。

組態包括：

- 組態項目
- 組態項目之間的關係
- 相依性圖形周遊的規則。

您可以根據實作自訂 CMDB 組態。

備註 變更組態時，會完成擷取並重新計算所有應用程式。因此，此程序可能至少需要 30 分鐘才能顯示在 [探索到的應用程式儀表板] 上。

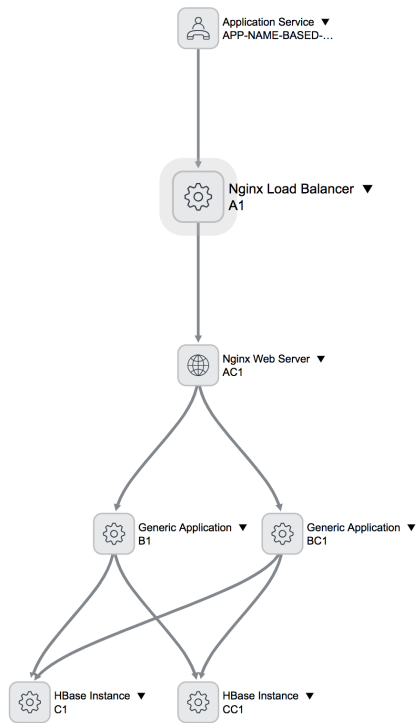
欄位名稱	說明
fetchOnlyApprovedApplications	允許布林值僅從 ServiceNow 擷取核准的應用程式。依預設，該值會設為 False 。
nameBasedSearchForVm	<p>允許布林值指示是否要在 vRealize Network Insight 中不存在 ServiceNow 虛擬機器時使用虛擬機器名稱自訂虛擬機器搜尋準則。如果將值設定為 True，則會建立自訂虛擬機器名稱準則，並且在 vRealize Network Insight 中偵測到對應的虛擬機器時反映計數，而不重新計算應用程式。</p> <p>在不使用服務對應的情況下手動建立相依性圖形或服務對應時，可以使用此項。依預設，該值會設為 False。</p>
ignoreWorkloadCheck	<p>允許布林值指示是否要新增實體至層，即使相關聯的工作負載實體不存在時亦是如此。</p> <p>在不使用服務對應的情況下手動建立相依性圖形或服務對應並且在工作負載層之前未定義關聯性時，可以使用此項。依預設，該值會設為 False。</p>
ciGroup	<p>定義要從中擷取 ServiceNow 的組態項目和關聯性。此欄位允許下列內容：</p> <ul style="list-style-type: none"> ■ Name：組態項目群組的名稱 ■ Value：屬於此群組的 ServiceNow 類別名稱的清單。 ■ ValueType：允許 CI_CLASS (要擷取的類別名稱) 和 CI_VALUE。 <ul style="list-style-type: none"> ■ CI_CLASS - 用於擷取類別。 ■ CI_VALUE <p>備註 vRealize Network Insight 一律會擷取 applicationClasses、workloadCIClasses、trackedCIClasses、workloadCIClasses 和 relationClasses。</p> <ul style="list-style-type: none"> ■ systemGenerated：允許布林值指示該類別為使用者定義的類別還是預設類別。 ■ expandCIClass - 允許布林值欄位指示是否擷取 Value 中列出的組態項目類別的子類別。
Rules for graph traversal	<p>支援三種類型的周遊規則：</p> <ul style="list-style-type: none"> ■ traversalRule：所有允許或有效的周遊。 ■ traversalStopRule：不允許的周遊。 <p>備註 traversalStopRule 中的規則的優先順序高於 traversalRule 中的規則。</p> <ul style="list-style-type: none"> ■ associationRule：與實體相關聯的工作負載所允許的周遊。 <p>規則的內容：</p> <ul style="list-style-type: none"> ■ fromNode：作為周遊來源的 ciGroup 的清單。 ■ toNode：作為周遊目的地的 ciGroup 的清單。 ■ relationship：與周遊類型存在關聯性的 ciGroup 的清單。 ■ priority：如果 ciGroup 符合兩個規則，則 ciGroup 的規則會根據 priority 進行設定。優先順序編號越大，優先順序值越高。
applicationClasses	<p>列出圖形周遊的所有進入點組態項目類別。這些類別代表可用作 CMDB 中的應用程式類別的組態項目類型。</p> <p>預設組態會使用 cmdb_ci_service_discovered 類別。此類別代表由 ServiceNow 的 ServiceMapping 功能所建立的應用程式。</p>

欄位名稱	說明
<code>workloadCiClasses</code>	<p>列出所有主控以軟體為基礎的服務或作業系統 (例如 Linux 伺服器、Windows 伺服器) 的組態項目。例如，虛擬機器、AWS 執行個體、實體伺服器。</p> <p>通常，工作負載組態項目位於相依性圖形的末尾。無法為此群組中所述的組態項目類別建立層。</p> <p>預設組態包含下列組態項目類別：</p> <ul style="list-style-type: none"> ■ <code>cmdb_ci_computer</code>: 代表所有與計算相關的組態項目。這是適用於所有 Linux 和 Windows 伺服器的超級類別。 ■ <code>cmdb_ci_vm_instance</code>: 代表虛擬計算實體，例如，虛擬機器和 AWS 執行個體。 ■ <code>cmdb_ci_vmware_instance</code>: 代表 VMware 虛擬機器。
<code>trackedCiClasses</code>	<p>列出可以是相依性圖形的一部分的所有組態項目，除了 <code>applicationClass</code> 或 <code>workloadCiClass</code> 以外。若要從 <code>applicationClasses</code> 到 <code>workloadCiClasses</code> 完成圖形，此群組中的組態項目是必需的。</p> <p>vRealize Network Insight 會為 <code>trackedCiClasses</code> 中提及的所有類別建立層，除了 <code>ignoredTierCiClasses</code> 下提及的類別以外。</p>
<code>relationshipTypeClasses</code>	<p>列出由關係組態項目類別或關係類型代表的所有相關組態項目。</p> <p>預設組態會使用 * 擷取所有關係類型。</p>
<code>workloadRelationshipTypeClasses</code> :	<p>列出通常表示與工作負載實體的關係的關係類型。以下是 ServiceNow 中預設支援的關係：</p> <ul style="list-style-type: none"> ■ <code>Hosted on::Hosts</code> ■ <code>Instantiates::Instantiated by</code> ■ <code>Runs on::Runs</code> ■ <code>Virtualized by::Virtualizes</code>
<code>ignoredCiClasses</code>	<p>列出 vRealize Network Insight 必須忽略以從 ServiceNow CMDB 擷取的所有組態項目。</p> <p>這在擷取超級類別時非常有用，可以忽略不必要的子類別。</p> <p>依預設，<code>cmdb_ci_vcenter_server_obj</code> 列示在 <code>ignoredCiClasses</code> 下，因為應用程式探索不需要 vCenter Server。</p>
<code>ignoredTierCiClasses</code>	<p>列出不得建立層的所有組態項目。</p>

探索沒有工作負載關係的應用程式的範例

以下是將 `nameBasedSearchForVm` 定義為探索應用程式的自訂 CMDB 組態檔，其中 `cmdb_ci_service_discovered` 類別是進入點，並且未定義工作負載關係。

拓撲



自訂的 CMDB 組態檔

```

{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_service_discovered"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    },
    {
      "name": "relationshipTypeClasses",
      "value": [
        "*"
      ],
      "valueType": "CI_VALUE",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "workloadRelationshipTypeClasses",
      "value": [

```

```

        "Hosted on::Hosts",
        "Instantiates::Instantiated by",
        "Runs on::Runs",
        "Virtualized by::Virtualizes"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": false
},
{
    "name": "workloadCIClasses",
    "value": [
        "cmdb_ci_computer",
        "cmdb_ci_vm_instance",
        "cmdb_ci_vmware_instance"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
},
{
    "name": "relationClasses",
    "value": [
        "cmdb_rel_ci"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
},
{
    "name": "ignoredCIClasses",
    "value": [
        "cmdb_ci_vcenter_server_obj"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
},
{
    "name": "ignoredTierCIClasses",
    "value": [
        "cmdb_ci_qualifier_manual_connection",
        "cmdb_ci_endpoint"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
},
{
    "name": "trackedCIClasses",
    "value": [
        "cmdb_ci_appl",
        "cmdb_ci_cluster",
        "cmdb_ci_cluster_node",
        "cmdb_ci_database",

```

```

        "cmdb_ci_lb_service",
        "cmdb_ci_spkg",
        "cmdb_ci_qualifier_manual_connection",
        "cmdb_ci_endpoint",
        "cmdb_ci_network_adapter",
        "cmdb_ci_translation_rule"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
}
],
"traversalRule": [
    {
        "fromNode": [
            "applicationClasses"
        ],
        "toNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "relationship": [
            "relationshipTypeClasses"
        ],
        "priority": 5
    },
    {
        "fromNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "toNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "relationship": [
            "relationshipTypeClasses"
        ],
        "priority": 3
    }
],
"traversalStopRule": [
    {
        "fromNode": [
            "trackedCIClasses",
            "workloadCIClasses"
        ],
        "toNode": [
            "applicationClasses"
        ],
        "relationship": [
            "relationshipTypeClasses"
        ],
        "priority": 5
    }
]

```

```

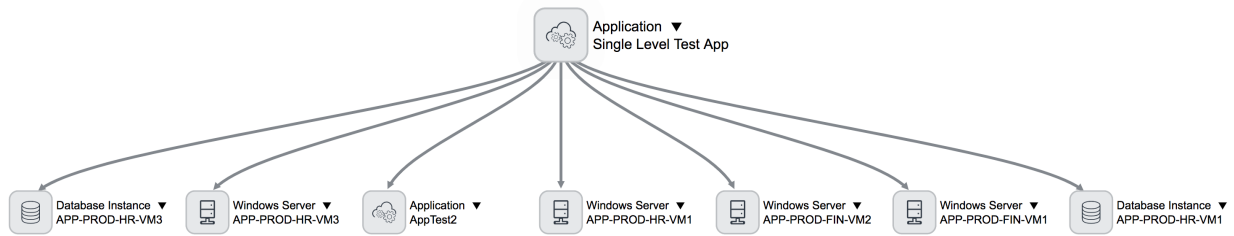
],
"associationRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "workloadCIClasses"
    ],
    "relationship": [
      "workloadRelationshipTypeClasses"
    ],
    "priority": 5
  }
]
}

```

探索單一層級應用程式的範例

以下是將 `nameBasedSearchForVm` 定義為探索單一層級應用程式的自訂 CMDB 組態檔，其中 `cmdb_ci_service_discovered` 類別是進入點，並且未定義工作負載關係。

拓撲



自訂的 CMDB 組態檔

```

{
  "fetchOnlyApprovedApplications": false,
  "nameBasedSearchForVm": true,
  "ignoreWorkloadCheck": true,
  "ciGroup": [
    {
      "name": "applicationClasses",
      "value": [
        "cmdb_ci_appl"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": false
    },
    {
      "name": "relationshipTypeClasses",
      "value": [
        "*"
      ]
    }
  ]
}

```

```

    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": false
  },
  {
    "name": "workloadRelationshipTypeClasses",
    "value": [
      "Hosted on::Hosts",
      "Instantiates::Instantiated by",
      "Runs on::Runs",
      "Virtualized by::Virtualizes"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": false
  },
  {
    "name": "workloadCIClasses",
    "value": [
      "cmdb_ci_computer",
      "cmdb_ci_vm_instance",
      "cmdb_ci_vmware_instance"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "relationClasses",
    "value": [
      "cmdb_rel_ci"
    ],
    "valueType": "CI_CLASS",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredCIClasses",
    "value": [
      "cmdb_ci_vcenter_server_obj"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  },
  {
    "name": "ignoredTierCIClasses",
    "value": [
      "cmdb_ci_qualifier_manual_connection",
      "cmdb_ci_endpoint"
    ],
    "valueType": "CI_VALUE",
    "systemGenerated": true,
    "expandCIClass": true
  }

```



```

    },
    {
      "name": "trackedCIClasses",
      "value": [
        "cmdb_ci_appl",
        "cmdb_ci_cluster",
        "cmdb_ci_cluster_node",
        "cmdb_ci_database",
        "cmdb_ci_lb_service",
        "cmdb_ci_spkg",
        "cmdb_ci_qualifier_manual_connection",
        "cmdb_ci_endpoint",
        "cmdb_ci_network_adapter",
        "cmdb_ci_translation_rule"
      ],
      "valueType": "CI_CLASS",
      "systemGenerated": true,
      "expandCIClass": true
    }
  ],
  "traversalRule": [
    {
      "fromNode": [
        "applicationClasses"
      ],
      "toNode": [
        "trackedCIClasses",
        "workloadCIClasses"
      ],
      "relationship": [
        "relationshipTypeClasses"
      ],
      "priority": 5
    },
    {
      "fromNode": [
        "trackedCIClasses",
        "workloadCIClasses"
      ],
      "toNode": [
        "trackedCIClasses",
        "workloadCIClasses"
      ],
      "relationship": [
        "relationshipTypeClasses"
      ],
      "priority": 3
    }
  ],
  "traversalStopRule": [
    {
      "fromNode": [
        "trackedCIClasses",
        "workloadCIClasses"
      ],

```

```

    "toNode": [
      "applicationClasses"
    ],
    "relationship": [
      "relationshipTypeClasses"
    ],
    "priority": 5
  }
],
"associationRule": [
  {
    "fromNode": [
      "trackedCIClasses",
      "workloadCIClasses"
    ],
    "toNode": [
      "workloadCIClasses"
    ],
    "relationship": [
      "workloadRelationshipTypeClasses"
    ],
    "priority": 5
  }
]
}

```

新增一般路由器或交換器

如果您要新增的路由器或交換器在 vRealize Network Insight 中不受支援，您可以透過上傳裝置組態檔將此不受支援的路由器或交換器新增為一般路由器或交換器。vRealize Network Insight 使用裝置組態檔中的資訊，以提供路由器或交換器的見解。在 vRealize Network Insight 中上傳裝置組態檔後，您無法修改已上傳的裝置組態檔的資訊。

必要條件

使用由 vRealize Network Insight 提供的 SDK，以 .zip 格式建立裝置組態檔。裝置組態檔包含實體的相關資訊，例如，路由器介面、路由、交換器連接埠、VRF、交換器裝置資訊等。若要建立裝置組態檔，請參閱 <https://github.com/vmware/network-insight-sdk-generic-datasources>。

程序

- 1 在 [設定] 頁面上，按一下**帳戶和資料來源**。
- 2 按一下**新增來源**。
- 3 在 [路由器和交換器] 下，按一下**一般路由器和交換器**。

- 4 在**新增一般路由器/交換器**頁面上，修改所需的資訊。

選項	動作
收集器虛擬機器	從下拉式功能表中選取收集器虛擬機器。
裝置組態檔	選取並上傳使用 SDK 建立的組態檔 (.zip)。
IP 位址/FQDN	輸入 IP 位址或 FQDN 詳細資料。

- 5 按一下**驗證**。
- 6 在**暱稱**文字方塊中，輸入您要新增的交換器或路由器的暱稱。
- 7 (選擇性) 在**附註**文字方塊中，您可以視需要新增附註。
- 8 按一下**提交**。

編輯一般路由器或交換器

在 vRealize Network Insight 中，您可以透過上傳新的組態檔來修改現有的一般路由器或交換器的組態。

必要條件

使用由 vRealize Network Insight 提供的 SDK，以 .zip 格式建立裝置組態檔。裝置組態檔包含實體的相關資訊，例如，路由器介面、路由、交換器連接埠、VRF、交換器裝置資訊等。若要建立裝置組態檔，請參閱 <https://github.com/vmware/network-insight-sdk-generic-datasources>。

程序

- 1 在 [設定] 頁面上，按一下**帳戶和資料來源**。
- 2 按一下您要編輯的一般路由器或交換器資料來源旁邊的**編輯資料來源**圖示。
- 3 按一下**取代檔案**並上傳新的裝置組態檔。
- 4 (選擇性) 若要檢視您已上傳的裝置組態檔，請按一下**上傳歷程記錄**。
您可以檢視、下載並刪除最後五個已上傳的裝置組態檔。
- 5 按一下**驗證**。
- 6 (選擇性) 在**暱稱**文字方塊中，變更暱稱。
- 7 按一下**提交**。

移轉資料來源

4

如果 Proxy 虛擬機器已關閉或已刪除，您可以新增 Proxy 虛擬機器，並將資料來源從舊 Proxy 虛擬機器移轉至新的 Proxy 虛擬機器。

移轉資料來源：

程序

- 1 在**安裝和支援**頁面中的**收集器 (Proxy) 虛擬機器**區段下，按一下**編輯圖示**。
如果 Proxy 虛擬機器已關閉，則可以在相同的區段下方看到錯誤訊息，指出 Proxy 虛擬機器無法使用。
- 2 在**編輯收集器 (Proxy) 虛擬機器**頁面中，您可以將暱稱指派給 Proxy 虛擬機器。
- 3 [編輯收集器 (Proxy)] 頁面列出了新增至 Proxy 的所有資料來源。若要移轉資料來源，請針對特定資料來源按一下**移轉**。
- 4 此時將顯示 [編輯帳戶或來源] 頁面。確保填寫下列資訊：

表 4-1.

欄位	說明
收集器 (Proxy) 虛擬機器	必須向其移轉資料來源的新 Proxy 虛擬機器的名稱
IP 位址	資料來源的預先填入的 IP/FQDN 位址
使用者名稱	資料來源的使用者名稱
密碼	資料來源的密碼

- 5 按一下**驗證**。按一下**提交**。然後將在舊 Proxy 虛擬機器中刪除此資料來源，並將其新增至新的 Proxy 虛擬機器。

- 6 移轉成功之後，在**帳戶和資料來源**頁面的**已啟用**資料行中會看到資料來源的新 Proxy 虛擬機器。

備註

- 如果您要將 vCenter 移轉至另一個 Proxy 虛擬機器，請確保將對應的 NSX Manager 也移轉至相同的 Proxy 虛擬機器。
 - 將 NSX Manager 移轉至另一個 Proxy 虛擬機器時，子系資料提供者 (例如 NSX Controller 和 NSX Edge) 也會移轉至新 Proxy 虛擬機器。
-

從 vRealize Network Insight 刪除資料來源

5

如果您不想檢視資料來源中的資料或資料來源未使用，您可以從 vRealize Network Insight 刪除此資料來源。

備註 如果您的環境中不再提供任何資料來源，則必須從 vRealize Network Insight 刪除該資料來源。

程序

- 1 登入 vRealize Network Insight Web 主控台。
- 2 移至 **設定 > 帳戶和資料來源**。
- 3 按一下您要刪除的資料來源旁邊的 **刪除資料來源** 圖示。

vRealize Network Insight 會提示您進行確認。

- 4 按一下 **是**。

備註 從系統移除資料來源後，只能在兩個小時或更長時間後才能再新增同一個資料提供者。

設定 vRealize Network Insight 設定

6

您可以從 vRealize Network Insight 設定頁面設定的各個層面。若要存取設定頁面，請按一下設定檔 > 設定。

本章節討論下列主題：

- 檢視系統健全狀況
- 設定資料保留間隔
- 設定 IP 內容和子網路
- 設定事件及通知
- 設定身分識別與存取管理
- 設定記錄
- 設定郵件伺服器
- 設定 SNMP 設陷目的地
- 管理授權
- 設定自動重新整理間隔
- 設定使用者工作階段逾時
- 新增 Google 地圖 API 金鑰
- 設定資料來源憑證驗證
- 檢視稽核記錄。
- 加入或退出客戶經驗改進計劃
- 檢視設定的健全狀況
- 啟用支援通道
- 管理磁碟使用率
- 檢視節點詳細資料
- 建立支援服務包
- 瞭解收集器和平台負載的容量

檢視系統健全狀況

在 vRealize Network Insight 中，您可以檢視系統的健全狀況狀態。系統的健全狀況由程序延遲、索引子延遲和網格使用率決定。如果所有這些參數均處於綠色狀態，則表示您的系統健全狀況良好。如果這三個參數中的任何一個處於紅色狀態，則表示您的系統健全狀況不佳。

程序

- ◆ 在設定頁面上，按一下**安裝和支援**。

在**安裝和支援**頁面中，您會看到**系統健全狀況**區段。

備註 如果您的系統健全狀況處於錯誤狀態達六小時以上，您必須連絡 vRealize Network Insight 支援。

設定資料保留間隔

在 vRealize Network Insight 中，您可以指定要保留資料的時間。

備註 vRealize Network Insight 僅支援在企業授權上進行可設定的資料管理。在進階授權版本中，資料保留預設為 1 個月。

資料分為以下類別：


表 6-1.

類別	最小值	最大值
事件	1 個月	13 個月
實體和組態資料	1 個月	3 個月
度量	1 個月	13 個月
流程	不適用	1 個月
其他資料	不適用	100 GB 的額外磁碟空間

備註 對於所有類別，最小值為預設值。

可以為每個類別設定和控制不同的原則。您可以根據您的需求設定原則。

設定資料管理：

- 1 在首頁的右上角，按一下 ，然後按一下**設定**。
- 2 在**設定**區段中，按一下**資料管理**。
- 3 首次登入時，此頁面會顯示預設資料。
- 4 如需有關資料如何佔用磁碟的詳細資訊，請按一下資訊圖示。

- 5 按一下**變更原則**以變更各種資料類別的資料保留期間。進行變更後，資訊會記錄在資料庫中。
- 6 按一下**提交**。

備註 低解析度度量的保留期間比高解析度度量的長。

設定 IP 內容和子網路

在 vRealize Network Insight 中，您可以設定不同的 IP 內容以實現更好的安全性規劃和識別。

匯入 DNS 對應檔案

若要為實體裝置之間的流程提供相關資訊，您可以匯入 DNS 對應檔案。DNS 對應檔案支援的格式為 Bind 和 CSV 檔案格式。確保已將這些檔案放置在單一 ZIP 檔案中。

備註 vRealize Network Insight 不支援受密碼保護的 ZIP 檔案。

程序

- 1 在**設定**頁面中，按一下**IP 內容和子網路**。
- 2 按一下**實體 IP 和 DNS 對應**。
- 3 按一下**上傳並取代**以上傳 DNS 對應檔案。選取並上傳檔案後，按一下**驗證**。驗證後，會出現 DNS 記錄數。

上傳並取代作業會移除任何現有的 DNS 對應，並將其取代為即將匯入的對應。DNS 對應檔案包含下列三個欄位：

- 主機名稱
- IP 位址
- 網域名稱

設定子網路和 VLAN 之間的對應

您可以定義子網路與 VLAN 之間的對應。

您可以將此對應用於下列作業：

- 透過新增來源和目的地子網路，以及與流程相關聯的第 2 層網路，擴充從實體到實體流程瞭解的 IP 實體的相關資訊。
- 根據實體位址的子網路和 VLAN 規劃網路拓撲。

程序

- 1 在**設定**頁面中，按一下**IP 內容和子網路**。

- 2 按一下**實體 IP 和 DNS 對應**。
- 3 在**設定**頁面的 **IP 內容和子網路**下，按一下**實體子網路和 VLAN**。
此頁面會列出所有子網路和關聯的 VLAN 識別碼。
- 4 按一下**新增**以新增子網路和 VLAN 資訊。
- 5 定義對應資訊後，您只能編輯與子網路關聯的 VLAN 識別碼。無法變更為與 VLAN 識別碼相關聯的子網路 CIDR。若要編輯與 VLAN 識別碼相關聯的子網路，請刪除您要編輯的子網路，然後使用所需的值建立子網路 VLAN 對應。

更新子網路-VLAN 對應資訊時，將為指定的 VLAN 識別碼建立新的 VLAN，並將子網路資訊與此 VLAN 相關聯。
- 6 若要刪除子網路-VLAN 識別碼對應，請按一下刪除圖示。

備註 建立子網路和 VLAN 對應後，所有 VLAN 建立、更新和刪除作業都不會立即執行。傳播變更以及建立或修改對應的 VLAN 需要一些時間。

設定東西向 IP

在 RFC1918 標準範圍內的 IP 被視為私人 IP。在 RFC1918 之外的 IP 被視為 Internet IP。但是，使用者可以指定他們想要在標記流程和微分割時視為非 Internet IP 的東西向 IP (資料中心公用 IP)，即使在 RFC1918 定義的私人 IP 位址範圍外，也是如此。

指定要視為非 Internet IP 的公用 IP

- 1 在首頁的右上角，按一下**設定檔**圖示，然後按一下**設定**。
- 2 在 [設定] 區段中，按一下**東西向 IP**。
- 3 在 [IP 位址] 方塊中，輸入將被視為非 Internet IP 的特定 IP、IP 範圍或子網路。
- 4 按一下**儲存**。成功儲存後，會立即顯示 [IP 位址已儲存] 確認訊息。

設定南北向 IP

RFC1918 空間中的 IP 分類為南北向 IP。使用者可以在標記和微分割時指定其南北向 IP。

指定南北向 IP：

- 1 在首頁的右上角，按一下 [設定檔] 圖示，然後按一下**設定**。
- 2 在 [設定] 區段中，按一下**南北向 IP**。
- 3 在 [IP 位址] 方塊中，輸入特定的 IP、IP 範圍或子網路。
- 4 按一下**儲存**。成功儲存後，會立即顯示 [IP 位址已儲存] 確認訊息。

設定事件及通知

在 vRealize Network Insight 中，您可以設定各種類型的事件和通知。只要系統符合預設規則，vRealize Network Insight 就會建立一個事件。

在**設定**頁面上，按一下**事件**以檢視各種類型的事件：

- 系統事件
- 使用者定義的事件
- 平台健全狀況事件

系統事件清單

以下是 vRealize Network Insight 中定義的所有系統事件的清單。若要接收有關任何這些系統事件的通知，您必須為該特定事件啟用通知。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.100001	vmwNSXVLatencyNoDataEvent	警告	NSXVLatencyNoDataEvent	網路延遲收集已停止
1.3.6.1.4.1.6876.100.1.0.100051	vmwVMCVMLimitExceededEvent	嚴重	VMCVMLimitExceededEvent	VMC SDDC 中的虛擬機器數目超過限制。
1.3.6.1.4.1.6876.100.1.0.100052	vmwVMCHostLimitExceededEvent	嚴重	VMCHostLimitExceededEvent	VMC SDDC 中的主機數目超過限制。
1.3.6.1.4.1.6876.100.1.0.1510	vmwKubernetesBaseEvent	中等	KubernetesBaseEvent	Kubernetes 叢集報告的事件
1.3.6.1.4.1.6876.100.1.0.20001	vmwEntityDiscoveryChangeEvent	資訊	探索	探索到任何新的實體時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20002	vmwEntityPropertiesChangeEvent	資訊	組態變更	當實體的任何內容變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20003	vmwFirewallNotInstalledOnHostEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20004	vmwHostWithStaleFirewallRulesEvent	警告	主機和 NSX Manager 之間的防火牆規則資料表不相符	主機和 NSX Manager 之間的 Distributed Firewall 規則資料表不同。
1.3.6.1.4.1.6876.100.1.0.20005	vmwIpAddressChangeEvent	資訊	IP 位址變更	當虛擬機器的 IP 位址變更時，會發生此事件

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20006	vmwL2GatewayAnomalyEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20007	vmwL2NetworkAddressAnomalyEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20008	vmwL2NetworkDiameterExceededEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20009	vmwL2NetworkUplinkMissingEvent	資訊	找不到分散式虛擬連接埠群組的上行	VXLAN 不具有指定主機上的上行
1.3.6.1.4.1.6876.100.1.0.20010	vmwL2NetworkWithNoVMsEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20011	vmwLayer2NetworkDiameterChangedEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20012	vmwMTUMismatchEvent	警告	VTEP 與實體交換器連接埠之間的 MTU 不相符	在 VTEP 與其實體交換器連接埠之間的路徑中發現 MTU 不相符
1.3.6.1.4.1.6876.100.1.0.20013	vmwNetworkIsolationEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20014	vmwNoPathEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20015	vmwSpoofguardDisabledEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20018	vmwVMotionEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20019	vmwVMWithDisconnectedVnicsEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20020	vmwVMWithMultipleVnicsOnDifferentVxlansEvent	不適用	不適用	虛擬機器 %s 已連線至多個 vxlan [%s]
1.3.6.1.4.1.6876.100.1.0.20021	vmwVMWithMultipleVnicsOnSameL2Event	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20022	vmwVMWithNoIpAddressEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20023	vmwVTEPMissingEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20024	vmwL2Event	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20025	vmwMembershipChangeEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20026	vmwSecurityGroupMembershipChangeEvent	資訊	安全群組虛擬機器成員資格變更	當安全群組的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20027	vmwFirewallRuleMembershipChangeEvent	資訊	防火牆規則虛擬機器成員資格變更	當防火牆規則的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20028	vmwVlanMembershipChangeEvent	資訊	VLAN 虛擬機器成員資格變更	當 VLAN 的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20029	vmwVxlanMembershipChangeEvent	資訊	VXLAN 虛擬機器成員資格變更	當 VXLAN 的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20030	vmwDeleteChangeEvent	資訊	刪除變更	刪除任何實體時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20031	vmwVtepFailedPingEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20034	vmwEmptySearchStreamChangeEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20035	vmwSearchStreamMembershipChangeEvent	不適用	使用者定義的變更事件	使用者定義的變更事件
1.3.6.1.4.1.6876.100.1.0.20036	vmwEmptySearchStreamProblemEvent	不適用	使用者定義的零結果問題	當搜尋結果為空白時，出現使用者定義的問題
1.3.6.1.4.1.6876.100.1.0.20037	vmwSearchStreamMembershipProblemEvent	不適用	使用者定義的變更問題	當搜尋結果變更時，出現使用者定義的問題
1.3.6.1.4.1.6876.100.1.0.20038	vmwOspfConfigurationMismatchEvent	中等	DLR 和 Edge 路由器之間的 OSPF 區域識別碼不相符	OSPF 區域識別碼在連線的路由器介面上有所不同。
1.3.6.1.4.1.6876.100.1.0.20039	vmwServiceVMNotHealthyEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20040	vmwServiceVMNotPoweredOnEvent	嚴重	NSX 基礎結構虛擬機器未開啟電源	NSX 基礎結構虛擬機器處於已關閉電源的狀態。它提供的服務可能會受到影響。NSX 基礎結構包括控制器叢集
1.3.6.1.4.1.6876.100.1.0.20041	vmwServiceVMHighCPUUsageEvent	警告	針對 NSX 基礎結構虛擬機器報告高 CPU	NSX 基礎結構虛擬機器 CPU 較高。這種情況可能會導致服務中斷。
1.3.6.1.4.1.6876.100.1.0.20042	vmwServiceVMHighMemoryUsageEvent	警告	針對 NSX 基礎結構虛擬機器報告高記憶體使用量	基礎結構虛擬機器記憶體較高。這種情況可能會導致 NSX 服務中斷。
1.3.6.1.4.1.6876.100.1.0.20043	vmwServiceVMHighDiskUsageEvent	警告	針對 NSX 基礎結構虛擬機器報告高磁碟使用量	已耗用為基礎結構虛擬機器配置的大部分磁碟空間。基礎結構虛擬機器可能會變得無法存取或導致服務中斷。
1.3.6.1.4.1.6876.100.1.0.20050	vmwIPSetPropertiesChangeEvent	資訊	IP 集內容變更	當 IPSet 的任何內容變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20051	vmwFirewallRulePropertiesChangeEvent	資訊	防火牆規則內容變更	當防火牆規則的任何內容變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20052	vmwSecurityGroupPropertiesChangeEvent	資訊	安全群組內容變更	當安全群組的任何內容變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20053	vmwIPSetMembershipChangeEvent	資訊	IP 集成員資格變更	當 IPSet 的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20054	vmwFirewallRuleMaskEvent	警告	Distributed Firewall 規則被上述規則遮罩	Distributed Firewall 規則已被一或多個上述規則遮罩。這種情況可能表示組態錯誤
1.3.6.1.4.1.6876.100.1.0.20056	vmwSecurityMembershipChangeEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20057	vmwSecurityTagPropertiesChangeEvent	資訊	安全性標籤內容變更	當安全性標籤的任何內容變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20058	vmwSecurityTagMembershipChangeEvent	資訊	安全性標籤虛擬機器成員資格變更	當安全性標籤的成員資格變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20059	vmwHostDatastoreChangeEvent	資訊	主機的資料存放區已變更	當主機資料存放區變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20060	vmwVMDatasetoreChangeEvent	資訊	虛擬機器的資料存放區已變更	當虛擬機器資料存放區變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20061	vmwVMSnapshotChangeEvent	資訊	虛擬機器的快照已變更	當虛擬機器的快照變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20062	vmwVMVirtualDiskChangeEvent	資訊	虛擬機器的虛擬磁碟已變更	當虛擬機器的虛擬磁碟變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20063	vmwIPSetDefinitionMismatchEvent	資訊	NSX Manager 之間的 IPSet 定義不相符	在兩個 NSX Manager 中定義了名稱相同、範圍不同的 IPSet。這種情況可能表示存在組態錯誤。
1.3.6.1.4.1.6876.100.1.0.20064	vmwSegmentMismatchEvent	資訊	兩個 NSX Manager 之間的區段識別碼範圍重疊	不同 NSX Manager 中定義的 VXLAN 區段識別碼範圍包含重疊的範圍
1.3.6.1.4.1.6876.100.1.0.20065	vmwVtepEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20066	vmwVtepConfigurationFaultEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20067	vmwDLRNetworksNotReachableEvent	嚴重	無法從 NSX Edge 或外部路由器連線到 DLR 網路	無法從 NSX Edge 路由器上的上行介面連線到一或多個 DLR 網路。這種情況表示 Edge 路由器/DLR 上出現 OSPF 組態錯誤或上行路由器上未設定路由。
1.3.6.1.4.1.6876.100.1.0.20068	vmwVtepSubnetMismatchEvent	中等	主機和 NSX 已備妥的叢集之間的 VTEP IP 子網路不相符	一或多個主機 VTEP 的 IP 位址與相同叢集中的其他 VTEP 不在同一個子網路上。這種情況可能會導致網路連線問題
1.3.6.1.4.1.6876.100.1.0.20069	vmwVtepCountMismatchEvent	嚴重	主機的 VTEP 計數與叢集不相符	主機的 VTEP 計數與同一叢集中其他主機的 VTEP 計數不相符。此主機上連線到邏輯交換器的虛擬機器可能無法進行通訊。
1.3.6.1.4.1.6876.100.1.0.20070	vmwEdgeNetworksNotReachableEvent	中等	無法從上行路由器連線到 NSX Edge 網路	無法從上行路由器存取連線至 NSX Edge 路由器的一或多個網路。
1.3.6.1.4.1.6876.100.1.0.20089	vmwNilInfraChangeEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.20090	vmwDataSourceEnabledChangeEvent	資訊	已啟用資料來源	當資料來源啟用時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20091	vmwDataSourceDisabledChangeEvent	資訊	已停用資料來源	當資料來源已停用時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20092	vmwDataSourceCreatedEvent	資訊	已新增資料來源	新增資料來源時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20093	vmwPlatformCpuCoreChangeEvent	資訊	「平台 CPU 核心變更」事件	當平台上的 CPU 核心變更時，會發生此事件

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.20094	vmwPlatformDiskChangeEvent	資訊	「平台磁碟變更」事件	當平台上的磁碟變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20095	vmwPlatformMemoryChangeEvent	資訊	「平台記憶體變更」事件	當平台上的記憶體變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20096	vmwPlatformRebootedEvent	資訊	「平台已重新開機」事件	將平台重新開機時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20097	vmwProxyCpuCoreChangeEvent	資訊	「Proxy CPU 核心變更」事件	當收集器上的 CPU 核心變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20098	vmwProxyDiskChangeEvent	資訊	「Proxy 磁碟變更」事件	當收集器上的磁碟變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20099	vmwProxyMemoryChangeEvent	資訊	「Proxy 記憶體變更」事件	當收集器上的記憶體變更時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20100	vmwProxyRebootedEvent	資訊	「Proxy 已重新開機」事件	將收集器重新開機時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20101	vmwNICClusterChangeEvent	資訊	已擴充叢集	將平台新增至系統時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20102	vmwNISystemProxyChangeEvent	資訊	Proxy 已新增/移除	新增或移除 Proxy 時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.20103	vmwNICClusterCreateEvent	資訊	已建立叢集	建立叢集時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.30001	vmwThresholdExceededEventCpuReady	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30002	vmwThresholdExceededEventCpuCoStop	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30003	vmwThresholdExceededEventDiskCommandAbortRule	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30004	vmwThresholdExceededEventIODeviceLatencyRule	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.30005	vmwThresholdExceededEventIOKernelLatencyRule	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30006	vmwThresholdExceededEventMemorySwapInRule	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30007	vmwThresholdExceededEventMemorySwapOutRule	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30008	vmwThresholdExceededEventNetworkRxDropRule	警告	在主機介面上偵測到接收封包捨棄	在主機介面上偵測到接收端封包捨棄數已超越臨界值。
1.3.6.1.4.1.6876.100.1.0.30009	vmwThresholdExceededEventNetworkTxDropRule	警告	在主機介面上偵測到傳輸封包捨棄	在主機介面上偵測到傳輸端封包捨棄數已超越臨界值。
1.3.6.1.4.1.6876.100.1.0.30010	vmwAWSRegionSGLimitEvent	嚴重	適用於 AWS 區域的 AWS 安全群組。	適用於 AWS 區域的 AWS 安全群組。
1.3.6.1.4.1.6876.100.1.0.30011	vmwAWSVPCSGLimitEvent	嚴重	適用於 AWS VPC 的 AWS 安全群組。	適用於 AWS VPC 的 AWS 安全群組。
1.3.6.1.4.1.6876.100.1.0.30012	vmwAWSSGInboundRuleLimitEvent	嚴重	適用於 AWS 安全群組的輸入規則。	適用於 AWS 安全群組的輸入規則。
1.3.6.1.4.1.6876.100.1.0.30013	vmwAWSSGOutboundRuleLimitEvent	嚴重	適用於 AWS 安全群組的輸出規則。	適用於 AWS 安全群組的輸出規則。
1.3.6.1.4.1.6876.100.1.0.30014	vmwAWSInterfaceSGLimitEvent	嚴重	適用於 AWS 介面的 AWS 安全群組。	適用於 AWS 介面的 AWS 安全群組。
1.3.6.1.4.1.6876.100.1.0.30100	vmwPacketDropEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30101	vmwSwitchPortPacketDropEvent	警告	在交換器連接埠上捨棄封包	在指定的交換器連接埠上偵測到大量封包捨棄
1.3.6.1.4.1.6876.100.1.0.30102	vmwRouterInterfacePacketDropEvent	警告	在 NSX Edge 閘道介面上捨棄封包	在 NSX Edge 閘道的 vNIC 介面上已偵測到超過臨界值的封包捨棄數量。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.30103	vmwVnicPacketDropEvent	警告	在虛擬機器捨棄封包	在虛擬機器介面上偵測到封包捨棄數已超越臨界值。
1.3.6.1.4.1.6876.100.1.0.30104	vmwVTEPUnderlayPacketDropEvent	中等	VTEP 底層封包捨棄	在 VTEP 底層中偵測到封包捨棄計數相當大
1.3.6.1.4.1.6876.100.1.0.30105	vmwPnicUnderlyingSwitchPortPacketDropEvent	警告	在 PNIC 基礎交換器連接埠上捨棄封包	在與指定的實體 NIC 相關聯的交換器連接埠上偵測到封包捨棄數已超越臨界值。
1.3.6.1.4.1.6876.100.1.0.30106	vmwDevicePacketDropEvent	警告	在硬體閘道連接埠上偵測到封包捨棄	在指定的裝置上偵測到封包捨棄數已超越臨界值。
1.3.6.1.4.1.6876.100.1.0.30110	vmwSwitchPortUptimeThresholdRecededEvent	警告	SwitchPortUptimeThresholdRecededEvent	運作時間已縮短
1.3.6.1.4.1.6876.100.1.0.30111	SwitchPortOperationalDownEvent	警告	交換器連接埠已停止運作	交換器連接埠已停止運作。
1.3.6.1.4.1.6876.100.1.0.30112	RouterInterfaceOperationalDownEvent	警告	路由器介面已停止運作	路由器介面已停止運作。
1.3.6.1.4.1.6876.100.1.0.30116	UnderlayDeviceFanMalFunctionEvent	警告	「底層裝置風扇已移除或無法運作」事件。	「底層裝置風扇已移除或無法運作」事件。
1.3.6.1.4.1.6876.100.1.0.30117	UnderlayDeviceTemperatureThresholdExceededEvent	警告	已超過底層裝置溫度臨界值事件	已超過底層裝置溫度臨界值事件。
1.3.6.1.4.1.6876.100.1.0.30118	UnderlayDeviceFexFanMalFunctionEvent	警告	「Fex 風扇已移除或無法運作」事件	「Fex 風扇已移除或無法運作」事件。
1.3.6.1.4.1.6876.100.1.0.30119	UnderlayDeviceFexPsMalFunctionEvent	警告	「Fex 電源供應器已移除或無法運作」事件	「Fex 電源供應器已移除或無法運作」事件。
1.3.6.1.4.1.6876.100.1.0.30120	UnderlayDeviceModuleMalFunctionEvent	警告	「底層裝置模組已移除或無法運作」事件	「底層裝置模組已移除或無法運作」事件。
1.3.6.1.4.1.6876.100.1.0.30121	UnderlayDevicePsMalFunctionEvent	警告	「底層裝置電源供應器已移除或無法運作」事件	「底層裝置電源供應器已移除或無法運作」事件。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.30122	UnderlayDeviceBfdSessionRemovedEvent	警告	「底層裝置 BFD 工作階段已刪除」事件	「底層裝置 BFD 工作階段已刪除」事件。
1.3.6.1.4.1.6876.100.1.0.30123	UnderlayDeviceLldpNeighbourRemovedEvent	警告	「底層裝置 LLDP 芳鄰已移除」事件	「底層裝置 LLDP 芳鄰已移除」事件
1.3.6.1.4.1.6876.100.1.0.30203	vmwThresholdExceededEventDatastoreFreeSpaceWarning	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30204	vmwThresholdExceededEventDatastoreFreeSpaceCritical	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30205	vmwThresholdExceededEventDatastoreReadLatency	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.30206	vmwThresholdExceededEventDatastoreWriteLatency	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35001	vmwDistributedFirewallApplyHostEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35002	vmwDistributedFirewallApplyVMEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35003	vmwNsxEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35004	vmwFeatureImpactedEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35221	vmwNSXComponentEvent	嚴重	NSX 管理服務不在執行中	NSX 管理應用裝置服務已關閉
1.3.6.1.4.1.6876.100.1.0.35222	vmwNSXBackupEvent	資訊	未設定 NSX Manager 備份	未設定 NSX Manager 備份。正確備份所有 NSX 元件對於在出現故障時將系統還原至工作狀態至關重要
1.3.6.1.4.1.6876.100.1.0.35223	vmwNSXBackupAuditLogExcludedEvent	資訊	已從 NSX Manager 備份中排除稽核記錄	目前已從備份中排除稽核記錄

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.35224	vmwNSXUnsecureBackupEvent	資訊	未針對 SFTP 設定 NSX Manager 備份	安全 FTP 目前未用於備份
1.3.6.1.4.1.6876.100.1.0.35225	vmwNSXBackupSystemEventsExcludedEvent	資訊	已從 NSX Manager 備份中排除系統事件	目前已從備份中排除系統事件
1.3.6.1.4.1.6876.100.1.0.35226	vmwNSXBackupNotScheduledEvent	資訊	未啟用排定的 NSX Manager 備份	尚未設定環境的排定備份
1.3.6.1.4.1.6876.100.1.0.35227	vmwNSXBackupNotRecordedEvent	資訊	未記錄 NSX Manager 備份	尚未執行環境備份。正確備份所有 NSX 元件對於在出現故障時將系統還原至工作狀態至關重要
1.3.6.1.4.1.6876.100.1.0.35228	vmwNSXNtpServerEvent	資訊	未針對 NSX Manager 設定 NTP 伺服器	在 NSX Manager 上未設定任何 NTP 伺服器
1.3.6.1.4.1.6876.100.1.0.35229	vmwNSXSyslogServerEvent	資訊	未針對 NSX Manager 設定 Syslog 伺服器	在 NSX Manager 上未設定任何 Syslog 伺服器。Syslog 資料會有助於疑難排解和檢閱在安裝和設定期間記錄的資料
1.3.6.1.4.1.6876.100.1.0.35230	vmwControllerSyslogServerEvent	資訊	未針對 NSX Controller 設定 Syslog 伺服器	沒有為 NSX Controller 設定任何 Syslog 伺服器。Syslog 資料會有助於疑難排解和檢閱在安裝和設定期間記錄的資料
1.3.6.1.4.1.6876.100.1.0.35231	vmwNSXIPv6EnabledEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.35232	vmwNSXospfNeighborDownEvent	警告	無法從 NSX Edge 路由器連線到一或多個 OSPF 芳鄰	連線至 NSX Edge 的一或多個 OSPF 芳鄰已關閉
1.3.6.1.4.1.6876.100.1.0.36022	vmwClusterFeatureVersionMismatchEvent	資訊	NSX 功能版本與 ESXi 叢集版本不相符	已備妥叢集的 NSX 功能版本與 NSX Manager 的 NSX 功能版本不相符。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.36023	vmwHostFeatureVersionMismatchEvent	資訊	主機和叢集之間的 NSX 功能版本不相符	主機的網狀架構狀態資源功能版本與叢集或 NSX Manager 的不同
1.3.6.1.4.1.6876.100.1.0.36024	vmwFeatureVersionMismatchEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.36025	vmwHostFeatureEnabledMismatchEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.36026	vmwHostFeatureInstalledMismatchEvent	資訊	主機和叢集之間的網路網狀架構功能狀態不相符	主機的網路網狀架構功能狀態與叢集中其他主機的狀態不相符。
1.3.6.1.4.1.6876.100.1.0.36027	vmwHostVtepNotFoundEvent	嚴重	在已備妥的主機上找不到 VTEP	叢集中為 NSX 準備的主機遺失至少一個 VTEP。此主機上連線到任何邏輯交換器的虛擬機器可能都無法進行通訊。
1.3.6.1.4.1.6876.100.1.0.36028	vmwHostVtepDisconnectedEvent	警告	主機的 VTEP 以系統管理方式停用	主機的 VTEP 已停用，且處於未連線的狀態。
1.3.6.1.4.1.6876.100.1.0.36029	vmwHostVtepEvent	嚴重	主機 VTEP 已中斷連線	主機 VTEP 已中斷連線
1.3.6.1.4.1.6876.100.1.0.36030	vmwClusterHostsVtepMTUMismatchEvent	警告	主機和 NSX 已備妥的叢集之間的 VTEP MTU 不相符	主機和 NSX 已備妥的叢集之間的 VTEP MTU 不相符。
1.3.6.1.4.1.6876.100.1.0.36031	vmwFeatureUnhealthyEvent	警告	網路網狀架構功能狀態處於錯誤狀態	NSX Manager 報告安裝的 NSX 功能存在某些問題。
1.3.6.1.4.1.6876.100.1.0.36032	vmwEdgeHostNotConfiguredEvent	資訊	NSX Edge 高可用性未啟用	在 NSX Edge 上未啟用高可用性
1.3.6.1.4.1.6876.100.1.0.36033	vmwEdgeInterfacesDownEvent	警告	一或多個 NSX Edge 邏輯路由器介面已關閉	一或多個 NSX Edge 介面已關閉。
1.3.6.1.4.1.6876.100.1.0.36041	vmwModuleUnhealthyEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.36042	vmwModuleNotLoadedEvent	嚴重	在主機上未偵測到 NSX VIB 或主機模組	在主機上未偵測到任何一個 NSX VIB 或主機模組
1.3.6.1.4.1.6876.100.1.0.36043	vmwModuleNetworkConnectionFailureEvent	嚴重	在 NSX Manager 和主機之間未建立訊息匯流排和/或控制平面連線	此主機上的訊息匯流排和/或控制平面代理程式精靈發生 NSX Controller 或 NSX Manager 連線失敗
1.3.6.1.4.1.6876.100.1.0.36044	vmwHostNetworkControlPlaneMismatchEvent	中等	主機和 NSX Controller 之間的邏輯交換器資料表不相符	主要 NSX Controller 與使用邏輯交換器的所有主機之間的邏輯交換器資訊不相符。此事件可能表示分區變更後出現錯誤狀況。
1.3.6.1.4.1.6876.100.1.0.36045	vmwHostNetworkControlPlaneConnectionFailureEvent	嚴重	對於一或多個邏輯交換器，無法建立主機控制平面與控制器的連線	在 NSX 主機上的控制平面代理程式與一或多個邏輯交換器的主要 NSX Controller 之間未建立連線。這種情況會導致主機和 NSX Controller 的相關資訊失效。
1.3.6.1.4.1.6876.100.1.0.36046	vmwHostNetworkControlPlaneNotSyncedEvent	中等	主機和 NSX Controller 之間的邏輯網路不同步	主機上的邏輯交換和路由資訊未與 NSX Controller 資訊同步。若要確認是否發生這種情況
1.3.6.1.4.1.6876.100.1.0.36047	vmwNSXControllerClusterMajorityEvent	中等	沒有 NSX Controller 叢集多數事件	叢集中的部分 NSX Controller 沒有與 NSX Manager 通訊
1.3.6.1.4.1.6876.100.1.0.36048	vmwNSXControllersVMonSameHostEvent	資訊	所有控制器虛擬機器已部署到相同的主機	叢集中的所有 NSX Controller 均部署至相同的主機
1.3.6.1.4.1.6876.100.1.0.36049	vmwVxLanRangeExhaustEvent	警告	VXLAN 區段識別碼範圍達到耗盡	已使用超過 90% 的 VXLAN 區段識別碼

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.36050	vmwNSXFirewallDefaultAllowAllRulesEvent	資訊	依預設，防火牆規則允許所有流量	依預設，Distributed Firewall 設定為允許所有流量
1.3.6.1.4.1.6876.100.1.0.36051	vmwLogicalRouterNoUplinkEvent	資訊	未使用上行介面部署 NSX DLR	NSX DLR 未設定上行介面
1.3.6.1.4.1.6876.100.1.0.36052	vmwEdgeNotHAEvent	資訊	NSX Edge 已設定，但不具高可用性	當兩個 Edge 虛擬機器均已針對 Edge 高可用性設定時
1.3.6.1.4.1.6876.100.1.0.36053	vmwEdgeNotDeployedEvent	資訊	NSX Edge 部署失敗	NSX Edge 無法部署。這種情況可能表示在沒有實際部署的情況下設定了 NSX Edge。
1.3.6.1.4.1.6876.100.1.0.36054	vmwEcmpIsEnabledAndStatefulServicesAreUpEvent	資訊	NSX Edge 設定有 ECMP 和可設定狀態的 Edge 服務	防火牆
1.3.6.1.4.1.6876.100.1.0.36055	vmwLogicalRouterDeployedOnEcmpEdgeHostEvent	資訊	NSX DLR 與一或多個 NSX ECMP Edge 部署到相同的主機	NSX 分散式邏輯路由器控制虛擬機器與一或多個 NSX Edge (針對 ECMP 設定) 部署到相同的主機。
1.3.6.1.4.1.6876.100.1.0.36056	vmwEdgeMissingInterfaceOSPFAreaMappingEvent	資訊	NSX Edge 介面與 OSPF 區域的對應遺失	在 NSX Edge 中已啟用 OSPF
1.3.6.1.4.1.6876.100.1.0.36057	vmwOspfInsecureAuthRouterEvent	資訊	一或多個 OSPF 區域中所使用的驗證不安全	NSX Edge 服務閘道或 DLR 上的一或多個 OSPF 區域未設定為使用 MD5 驗證
1.3.6.1.4.1.6876.100.1.0.36058	vmwNSXControllersDeployedCountEvent	資訊	已部署的 NSX Controller 數目不正確	部署的控制器少於三個
1.3.6.1.4.1.6876.100.1.0.36059	vmwNSXControllerNotActiveCountEvent	中等	少於三個作用中的 NSX Controller	作用中的控制器少於三個
1.3.6.1.4.1.6876.100.1.0.36060	vmwNSXControllerEvent	不適用	不適用	不適用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.36061	vmwNSXEcmpEdgeDownEvent	資訊	ECMP 叢集中的一或多個 NSX Edge 目前已關閉	ECMP 叢集中的一或多個 NSX Edge 目前已關閉
1.3.6.1.4.1.6876.100.1.0.36062	vmwNSXMajorityEcmpEdgesDownEvent	警告	ECMP 叢集中的大多數 NSX Edge 目前已關閉	ECMP 叢集中的大多數 NSX Edge 目前已關閉
1.3.6.1.4.1.6876.100.1.0.36063	vmwNSXAllEcmpEdgesDownEvent	嚴重	ECMP 叢集中的所有 NSX Edge 目前已關閉	ECMP 叢集中的所有 NSX Edge 目前已關閉
1.3.6.1.4.1.6876.100.1.0.36064	vmwNSXEdgeMtuMismatchEvent	資訊	在 Edge 上的一或多個介面上設定的 MTU 與下一個躍點路由器上的 MTU 不相符	在同一個第 2 層網路中 Edge 上的一或多個介面上設定的 MTU 不相符
1.3.6.1.4.1.6876.100.1.0.36065	vmwNSXEdgeSplitBrainEvent	嚴重	兩台 NSX Edge HA 虛擬機器處於作用中狀態	Edge HA 的兩台虛擬機器都處於作用中狀態。最常見的問題是核心分裂
1.3.6.1.4.1.6876.100.1.0.36066	vmwVirtualDistributedRoutingEvent	警告	在主機上找不到用於 VXLAN 路由的 VDR 連接埠	在主機上找不到指定 VXLAN 的 VDR 連接埠
1.3.6.1.4.1.6876.100.1.0.36067	vmwNSXEdgeBGPNeighbourDownEvent	嚴重	一或多個 BGP 芳鄰未處於已建立狀態	一或多個 BGP 芳鄰未處於已建立狀態。
1.3.6.1.4.1.6876.100.1.0.37001	vmwAnalyticsEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.37002	vmwAnalyticsOutlierEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.37003	vmwAnalyticsThresholdEvent	嚴重	「臨界值違規」事件	由於指定的度量超過組態中指定的上限或下限而產生事件
1.3.6.1.4.1.6876.100.1.0.38001	vmwVMCEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.40001	vmwCriticalHostNotAccessibleEvent	嚴重	無法存取具有基礎結構虛擬機器的主機	無法存取具有基礎結構虛擬機器的主機
1.3.6.1.4.1.6876.100.1.0.568	vmwArkinApplicationMemberLimitEvent	資訊	已超過應用程式成員資格限制	應用程式中的成員數目超過支援的限制

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.70000	vmwGenericNSXSystemEvent	中等	NSX 系統事件 (警告)	具有較高或重大嚴重性的 NSX 系統事件
1.3.6.1.4.1.6876.100.1.0.70001	vmwFilterConfigApplyOnHostFailedEvent	警告	主機 vNIC 的 Distributed Firewall 更新無法套用	Distributed Firewall 組態更新無法套用至 NSX 已備妥的主機上的 vNIC。
1.3.6.1.4.1.6876.100.1.0.70002	vmwRulesetLoadOnHostFailedEvent	警告	Distributed Firewall 更新無法套用到主機	Distributed Firewall 規則集未套用到主機。
1.3.6.1.4.1.6876.100.1.0.70003	vmwConfigUpdateOnHostFailedEvent	警告	Distributed Firewall 組態更新失敗	NSX 主機的防火牆組態更新逾時。主機未與最新的防火牆組態版本同步。
1.3.6.1.4.1.6876.100.1.0.70004	vmwSpoofguardConfigUpdateOnHostFailedEvent	資訊	SpoofGuard 組態更新失敗	主機的 SpoofGuard 組態更新失敗。
1.3.6.1.4.1.6876.100.1.0.70005	vmwApplyRuleToVnicFailedEvent	警告	Distributed Firewall 規則未套用到主機 vNIC	Distributed Firewall 規則未套用到主機的 vNIC。
1.3.6.1.4.1.6876.100.1.0.70006	vmwContainerConfigUpdateOnVnicFailedEvent	警告	主機上的 Distributed Firewall 容器更新失敗	無法在 NSX 主機上更新用於 NSX Distributed Firewall 或 Service Composer 的網路和安全性容器資訊。
1.3.6.1.4.1.6876.100.1.0.70007	vmwSpoofguardApplyToVnicFailedEvent	資訊	SpoofGuard 初始設定失敗	SpoofGuard 組態無法套用到主機上指定的 vNIC。
1.3.6.1.4.1.6876.100.1.0.70008	vmwHostMessagingConfigurationFailedEvent	警告	主機傳訊組態更新失敗	透過 NSX 傳訊通道推送至主機的組態更新未完成。
1.3.6.1.4.1.6876.100.1.0.70009	vmwHostMessagingConnectionReconfigurationFailedEvent	警告	主機傳訊連線重新設定失敗	主機傳訊通道上更新的資訊無法傳送到 NSX 主機。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.70010	vmwHostMessagingConfigurationFailedNotificationSkippedEvent	警告	無法重新建立主機和 NSX Manager 之間的主機傳訊通道	當已備妥的主機重新連線到 vCenter Server 時，NSX Manager 嘗試重新建立訊息匯流排通道。此連線再次失敗
1.3.6.1.4.1.6876.100.1.0.70011	vmwHostMessagingInfrastructureDownEvent	警告	主機上的主機傳訊基礎結構已關閉	NSX Manager 和 NSX 主機之間遺失了兩條或更多傳訊通道活動訊號訊息。
1.3.6.1.4.1.6876.100.1.0.70012	vmwEdgeVMNotRespondingEvent	中等	NSX Edge 至 NSX Manager 的活動訊號失敗	NSX Edge 虛擬機器未回應 NSX Manager 的健全狀況檢查
1.3.6.1.4.1.6876.100.1.0.70013	vmwEdgeUnhealthyEvent	嚴重	NSX Edge 虛擬機器未處於作用中/自我狀態	NSX Edge 虛擬機器正在報告有問題的狀態，可能無法正常運作。
1.3.6.1.4.1.6876.100.1.0.70014	vmwEdgeVMMCommunicationFailureEvent	嚴重	NSX Manager 與 Edge 虛擬機器的通訊失敗	偵測到 NSX Manager 和 Edge 虛擬機器之間的通訊失敗。
1.3.6.1.4.1.6876.100.1.0.70015	vmwNSXEdgeEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.71000	vmwOtherCriticalNSXEvent	嚴重	NSX 重要系統事件	嚴重性為嚴重的 NSX 系統事件。
1.3.6.1.4.1.6876.100.1.0.80001	vmwPanNsxNotInRegisteredStateEvent	嚴重	Palo Alto Panorama 未向 NSX Manager 登錄	Panorama 未處於向 NSX Manager 登錄的狀態。
1.3.6.1.4.1.6876.100.1.0.80002	vmwPanNsxDynamicUpdateDelayedEvent	警告	Panorama 動態成員資格定義更新延遲	從 NSX Manager 進行的 Panorama 動態成員資格定義更新已延遲。這種情況可能表示網路連線問題或 NSX Manager 的 NetX 服務發生問題。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80003	vmwPanDeviceInDisconnectedStateEvent	警告	Palo Alto 服務虛擬機器未連線至 Panorama	Palo Alto 網路的服務虛擬機器或裝置未處於與 Panorama 連線的狀態
1.3.6.1.4.1.6876.100.1.0.80004	vmwPanNsxServiceApplianceViewMismatchEvent	嚴重	Panorama 與 NSX Manager 之間的服務虛擬機器狀態不相符	NSX Manager 和 Panorama 之間的服務應用裝置資訊不相符。
1.3.6.1.4.1.6876.100.1.0.80005	vmwPanNsxFabricAgentNotFoundOnHostEvent	嚴重	在主機上找不到 NSX 網狀架構代理程式	NSX 未針對已準備叢集的主機報告安全性網狀架構代理程式
1.3.6.1.4.1.6876.100.1.0.80006	vmwPanNsxServiceVMNotFoundOnHostEvent	嚴重	在主機上找不到 Palo Alto 服務虛擬機器	在 NSX 已備妥叢集中的主機上，找不到 Palo Alto 網路的安全性應用裝置虛擬機器。
1.3.6.1.4.1.6876.100.1.0.80100	vmwCheckpointEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.80102	vmwCheckpointNsxFabricAgentNotFoundOnHostEvent	嚴重	CheckpointNsxFabricAgentNotFoundOnHostEvent	NSX 未針對已準備叢集的主機報告安全性網狀架構代理程式
1.3.6.1.4.1.6876.100.1.0.80103	vmwCheckpointNsxServiceVMNotFoundOnHostEvent	嚴重	CheckpointNsxServiceVMNotFoundOnHostEvent	在 NSX 已備妥叢集中的主機上，找不到 Check Point 的安全性應用裝置虛擬機器。
1.3.6.1.4.1.6876.100.1.0.80104	vmwCheckpointGatewaySicStatusNotCommunicatingEvent	嚴重	CheckpointGatewaySicStatusNotCommunicatingEvent	Check Point 的服務虛擬機器或閘道不具有「通訊中」SIC 狀態
1.3.6.1.4.1.6876.100.1.0.80105	vmwCheckpointNsxServiceApplianceViewMismatchEvent	嚴重	檢查點與 NSX Manager 之間的服務虛擬機器狀態不相符	NSX Manager 和 Check Point 之間的服務應用裝置資訊不相符。
1.3.6.1.4.1.6876.100.1.0.80200	NSXTEvent	不適用	NSX-T 系統事件	NSX-T 平台產生的警示/事件

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80201	NSXTVcNotAddedEvent	警告	一或多個 vCenter Server 未在 vRNI 中新增為資料來源	NSX-T 包含一或多個未在 vRNI 中新增為具有相同 IP 或 FQDN 的資料來源的計算管理程式。
1.3.6.1.4.1.6876.100.1.0.80202	NSXTStandaloneHostsEvent	警告	在 NSX-T 中將一或多個網狀架構節點新增為獨立主機	一或多個網狀架構節點新增做為 NSX-T 中的獨立主機。這些主機上的虛擬機器將不會顯示在 vRNI 中。
1.3.6.1.4.1.6876.100.1.0.80203	vmwNSXTSystemEvent	不適用	不適用	不適用
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	「NSX-T 第 1 層邏輯路由器中斷連線」事件	NSX-T 第 1 層邏輯路由器與第 0 層路由器中斷連線。無法從外部存取此路由器下的網路，反之亦然。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	已停用路由通告	已停用 NSX-T 第 1 層邏輯路由器的路由通告。無法從外部存取此路由器下的網路。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有管理程式連線	NSX-T Edge 節點已中斷管理程式連線。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge 節點的控制器連線已降級	NSX-T Edge 節點無法與一或多個控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有控制器連線	NSX-T Edge 節點無法與任何控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMTUMismatchEvent	警告	NSX-T 第 0 層和上行交換器/路由器之間的 MTU 不相符	在第 0 層邏輯路由器的介面上設定的 MTU 與來自相同 L2 網路的上行交換器/路由器的介面不相符。這可能會影響網路效能。

OID	事件名稱	預設嚴重性	使用者介面名稱	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個虛擬機器。	一或多個虛擬機器不受 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 錯誤組態	由於第 0 層路由器的上行連接埠上的 VLAN 與外部閘道上的 VLAN 不同，通訊將會中斷。
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	沒有傳輸區域連結到傳輸節點。	沒有傳輸區域連結到傳輸節點。虛擬機器可能會因此中斷連線。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	傳輸節點上沒有可用的 VTEP。	已從傳輸節點刪除所有 VTEP。虛擬機器可能會因此中斷連線。
1.3.6.1.4.1.6876.100.1.0.80215	vmwDuplicateL3SwitchEvent	嚴重	「已新增相同的交換器或路由器」事件	新增了具有不同 IP 的相同交換器或路由器。可能不會產生虛擬機器到虛擬機器路徑。
1.3.6.1.4.1.6876.100.1.0.80216	vmwLBPoolMemberDownEvent	嚴重	集區成員已關閉	當負載平衡器的集區成員已關閉時，會發生此事件。若要瞭解已關閉的集區成員，請搜尋「Pool Member where state = DISABLED」
1.3.6.1.4.1.6876.100.1.0.80217	vmwLBPoolDownEvent	嚴重	集區已關閉	當負載平衡器的集區已關閉時，會發生此事件

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80218	vmwLBPoolEmptyEvent	嚴重	集區為空白	當負載平衡器的集區為空白時，會發生此事件。若要瞭解空白的集區，請搜尋「Pool where PoolMembers Count = 0」
1.3.6.1.4.1.6876.100.1.0.80219	vmwLBPoolMemberVMDownEvent	嚴重	集區成員的虛擬機器已關閉	當與負載平衡器集區成員相關聯的虛擬機器關閉時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.80220	vmwLBVirtualServerDisableEvent	嚴重	負載平衡器的虛擬伺服器已停用	當負載平衡器的虛擬伺服器已停用時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.80221	vmwLBServiceNodeIPNotFoundEvent	嚴重	找不到服務節點的 IP	找不到與負載平衡器服務節點的 IP 相關聯的 NIC 時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.80222	vmwLBServiceNodeMultipleNICFoundEvent	嚴重	找到服務節點的多個 NIC	找到與負載平衡器服務節點的 IP 相關聯的多個 NIC 時，會發生此事件
1.3.6.1.4.1.6876.100.1.0.80223	NSXTSwitchIpfixEnabledEvent	警告	NSX-T 交換器 IPFIX 已啟用，它將收集器設定檔指向其中一個 vRNI 收集器。	Network Insight 不支援來自 NSX-T 交換器的 IPFIX 流量資料。它設定為將 IPFIX 資料傳送至其中一個 Network Insight 收集器虛擬機器。它可能已損毀系統中的現有流量資料。
1.3.6.1.4.1.6876.100.1.0.80224	NSXTStandaloneHostsWithoutVcEvent	嚴重	管理 NSX-T 中的一或多個網狀架構節點的 vCenter 未在 vRNI 中新增為資料來源	管理 NSX-T 中的一或多個網狀架構節點的 vCenter 未在 vRNI 中新增為資料來源。這些主機上的虛擬機器將不會顯示在 vRNI 中。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	嚴重	NSX-T 控制器節點不具有控制叢集連線	NSX-T 控制器節點已中斷控制叢集連線。
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	嚴重	NSX-T 控制器節點不具有管理平面連線	NSX-T 控制器節點已中斷管理平面連線。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	嚴重	NSX-T 管理節點不具有管理叢集連線	NSX-T 管理節點已中斷管理叢集連線。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「關閉」。	NSX-T 主機傳輸節點 pNIC 狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「已降級」	NSX-T 主機傳輸節點 pNIC 狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「未知」。	NSX-T 主機傳輸節點 pNIC 狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80231	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」。
1.3.6.1.4.1.6876.100.1.0.80234	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」。
1.3.6.1.4.1.6876.100.1.0.80237	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」。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
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」。
1.3.6.1.4.1.6876.100.1.0.80240	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	NSXTEdgeNodeTunnelStatusDowngradeEvent	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」。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「關閉」。	NSX-T Edge 傳輸節點狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	嚴重	NSX-T Edge 傳輸節點狀態為「已降級」。	NSX-T Edge 傳輸節點狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「未知」。	NSX-T Edge 傳輸節點狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	警告	NSX-T 主機節點沒有管理程式連線	NSX Manager 與主機傳輸節點的連線狀態之間不同步
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	嚴重	NSX-T Edge 節點的控制器連線處於「未知」狀態。	NSX-T Edge 節點控制器連線處於「未知」狀態。
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處於「未知」狀態。	NSX-T 主機節點控制器連線處於「未知」狀態。

OID	事件名稱	預設嚴重性	使用者介面名稱	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) 之間的通訊失敗，例如，您無法從其中一個虛擬機器對另一個虛擬機器執行 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) 之間的通訊失敗，例如，您無法從其中一個虛擬機器對另一個虛擬機器執行 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	未排程 NSX-T Manager 備份。	未排程 NSX-T Manager 備份
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	嚴重	NSX-T DFW 防火牆已停用。	Distributed Firewall 在 NSX-T Manager 中已停用
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	將捨棄 NSX-T 邏輯連接埠接收的封包。	接收的封包將在 NSX-T 邏輯連接埠上捨棄，相關聯的實體可能會受到影響

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	警告	將捨棄 NSX-T 邏輯連接埠傳輸的封包。	傳輸的封包將在 NSX-T 邏輯連接埠上捨棄，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	將捨棄 NSX-T 邏輯交換器接收的封包	接收的封包將在 NSX-T 邏輯交換器上捨棄，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	將捨棄 NSX-T 邏輯交換器傳輸的封包	傳輸的封包將在 NSX-T 邏輯交換器上捨棄，相關聯的實體可能會受到影響
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	接收的封包將在 NSX-T 管理節點的網路介面上捨棄	接收的封包將在 NSX-T 管理節點的網路介面上捨棄。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	接收的封包將在 NSX-T Edge 節點的網路介面上捨棄	接收的封包將在 NSX-T Edge 節點的網路介面上捨棄。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	接收的封包將在 NSX-T 主機節點的網路介面上捨棄	接收的封包將在 NSX-T 主機節點的網路介面上捨棄。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	傳輸的封包將在 NSX-T 管理節點的網路介面上捨棄	傳輸的封包將在 NSX-T 管理節點的網路介面上捨棄。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	傳輸的封包將在 NSX-T Edge 節點的網路介面上捨棄	傳輸的封包將在 NSX-T Edge 節點的網路介面上捨棄。這可能會影響 Edge 叢集的網路流量。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	警告	傳輸的封包將在 NSX-T 主機節點的網路介面上捨棄	傳輸的封包將在 NSX-T 主機節點的網路介面上捨棄。這可能會影響 ESXi 主機上的網路流量。
1.3.6.1.4.1.6876.100.1.0.80301	vmwHardwareVTEPMismatchEvent	嚴重	HardwareVTEPMismatchEvent	硬體開道繫結不相符
1.3.6.1.4.1.6876.100.1.0.80302	vmwHardwareVTEPPortDownEvent	嚴重	HardwareVTEPPortDownEvent	硬體開道連接埠已關閉
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。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	警告	控制器服務已停止執行。	控制器服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	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	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變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	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	NSXTMPNodeServiceHttpStatusEvent	警告	HTTP 服務已停止執行。	HTTP 服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	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	NSXTMPNodeServiceInstallUpgradeEvent	警告	安裝升級服務已停止執行。	安裝升級服務狀態已變為 [已停止]。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	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	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent 服務已停止執行。	Liagent 服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	警告	Liagent 服務已停止	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	NSXTMPNodeServiceManagerStatusEvent	警告	管理程式服務已停止執行。	管理程式服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	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	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	警告	管理平面服務已停止執行。	管理服務狀態已變為 [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	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	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	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	NSXTMPNodeServiceNodeMgmtStatusEvent	警告	節點管理服務已停止執行。	節點管理服務狀態已變為 [已停止]。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	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	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變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	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 (即節點統計資料服務) 已停止執行。
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	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	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變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeServiceNSXPlatformClientStatusEvent	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	NSXTMPNodeServiceNSXUpgradeAgentStatusEvent	警告	升級代理程式服務已停止執行。	升級服務狀態已變為 [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	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	NSXTMPNodeServiceNTPStatusEvent	警告	NTP 服務已停止執行。	NTP 服務狀態已變為 [已停止]。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeServiceNTPStatusEvent	嚴重	NTP 服務已停止	NSX-T 管理節點的其中一個服務，即 NTP 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	警告	原則服務已停止執行。	原則服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	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	NSXTMPNodeServiceSearchStatusEvent	警告	搜尋服務已停止執行。	搜尋服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	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	NSXTMPNodeServiceSNMPStatusEvent	警告	SNMP 服務已停止執行。	SNMP 服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	警告	SNMP 服務已停止	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	NSXTMPNodeServiceSSHStatusEvent	警告	SSH 服務已停止執行。	SSH 服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	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	NSXTMPNodeServiceSyslogStatusEvent	警告	Syslog 服務已停止執行。	Syslog 服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	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	NSXTMPNodeServiceTelemetryStatusEvent	警告	遙測服務已停止執行。	遙測服務狀態已變為 [已停止]。

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	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	NSXTMPNodeServiceUIServiceStatusEvent	警告	使用者介面服務已停止執行。	使用者介面服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	嚴重	使用者介面服務已停止	NSX-T 管理節點的其中一個服務，即使用者介面服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	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。
1.3.6.1.4.1.6876.100.1.0.80501	vmwIndexerLagEvent	嚴重	「索引子延遲」事件	仍在建立最新資料的索引。搜尋結果可能不準確。
1.3.6.1.4.1.6876.100.1.0.80502	vmwIPFIXFlowDPPausedEvent	嚴重	「已暫停 IPFIX 流量資料來源」事件	由於有大量流量，已暫停 IPFIX 流量資料來源。
1.3.6.1.4.1.6876.100.1.0.80503	vmwGridProcessingStoppedEvent	嚴重	「網格處理已停止」事件	網格處理已停止。
1.3.6.1.4.1.6876.100.1.0.80504	vmwUnableToSendEmailsEvent	嚴重	「無法傳送電子郵件」事件	無法傳送電子郵件訊息。
1.3.6.1.4.1.6876.100.1.0.80505	vmwSMTPNotConfiguredEvent	嚴重	「未設定 SMTP」事件	未設定 SMTP
1.3.6.1.4.1.6876.100.1.0.80506	vmwSNMPNotConfiguredEvent	嚴重	「系統健全狀況」事件	未設定 SNMP 目標。
1.3.6.1.4.1.6876.100.1.0.80507	vmwReindexingInProgressEvent	嚴重	「正在重新建立索引」事件	目前正在重新建立資料索引。此移轉活動完成後，搜尋服務將可用。
1.3.6.1.4.1.6876.100.1.0.80508	vmwNodesVersionMismatchEvent	嚴重	「節點版本不相符」事件	偵測到節點版本不相符

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80509	vmwNotAllServicesRunningEvent	嚴重	「並非所有服務都在執行中」事件	一或多個必要服務未執行。
1.3.6.1.4.1.6876.100.1.0.80510	vmwNotAllServicesHealthyEvent	嚴重	「並非所有服務都狀況良好」事件	一或多個必要服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80511	vmwExpandPartitionFailedEvent	嚴重	「擴充磁碟分割失敗」事件	無法擴充磁碟分割。
1.3.6.1.4.1.6876.100.1.0.80512	vmwDiskCleanupFailedEvent	嚴重	「磁碟清理失敗」事件	磁碟清理服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80513	vmwVacuumFailedEvent	嚴重	「Vacuum 失敗」事件	PostgreSQL Vacuum 服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80514	vmwConfigStoreCleanupFailedEvent	嚴重	「組態存放區清理失敗」事件	資料保留 (組態存放區維護) 服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80515	vmwHBaseRetentionToolFailedEvent	嚴重	「HBASE 保留工具失敗」事件	資料保留 (度量保留組態) 服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80516	vmwMetricStoreUpdaterFailedEvent	嚴重	「度量存放區更新程式失敗」事件	資料保留 (度量存放區維護) 服務狀況不良。
1.3.6.1.4.1.6876.100.1.0.80517	vmwCollectorLagEvent	嚴重	「收集器延遲」事件	對收集器的最後一次資料收集為超過臨界值前
1.3.6.1.4.1.6876.100.1.0.80518	vmwCollectionLagEvent	嚴重	「收集延遲」事件	對資料來源的最後一次資料收集為超過臨界值前
1.3.6.1.4.1.6876.100.1.0.80519	vmwGridProcessingLagEvent	嚴重	「網格處理延遲」事件	網格處理延遲超過臨界值
1.3.6.1.4.1.6876.100.1.0.80520	vmwConnectionErrorEvent	嚴重	「連線錯誤」事件	連線至資料來源時發生錯誤 (Error connecting to data source)
1.3.6.1.4.1.6876.100.1.0.80521	vmwNodeNotActiveEvent	嚴重	「節點處於非作用中狀態」事件	節點處於非作用中狀態
1.3.6.1.4.1.6876.100.1.0.80522	vmwHighDiskUtilizationEvent	嚴重	「磁碟使用率較高」事件	磁碟使用率較高
1.3.6.1.4.1.6876.100.1.0.80523	vmwIndexingAbortedEvent	嚴重	「索引處理已中止」事件	索引處理已中止

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80524	vmwUpgradeFailedEvent	嚴重	「升級失敗」事件	升級失敗
1.3.6.1.4.1.6876.100.1.0.80525	vmwFlowProcessingSuspendedEvent	嚴重	「已暫停流量處理」事件	流量處理已暫停
1.3.6.1.4.1.6876.100.1.0.80526	vmwLargeSdmsDroppedEvent	嚴重	資料處理錯誤	捨棄了大型 SDMS
1.3.6.1.4.1.6876.100.1.0.80527	vmwApplianceNotConfiguredEvent	嚴重	「未設定應用裝置」事件	收集器虛擬機器組態不完整。
1.3.6.1.4.1.6876.100.1.0.80531	vmwFdbConfigStoreCleanupFailedEvent		FDB_CONFIG_STORE_CLEANUP_FAILED_EVENT	「FDB 組態存放區清理失敗」事件
1.3.6.1.4.1.6876.100.1.0.80531	vmwDiskAllocationInsufficientEvent	資訊	DISK_ALLOCATION_INSUFFICIENT_EVENT	「未設定磁碟」事件
1.3.6.1.4.1.6876.100.1.0.80601	vmwFailedEvent	嚴重	「資料來源失敗」事件	資料來源失敗
1.3.6.1.4.1.6876.100.1.0.80602	vmwTimeoutEvent	嚴重	「資料來源逾時」事件	資料來源逾時
1.3.6.1.4.1.6876.100.1.0.80603	vmwConnectionRefusedEvent	嚴重	「連線被拒絕」事件	連線被拒絕
1.3.6.1.4.1.6876.100.1.0.80605	vmwIncorrectConnectionStringEvent	嚴重	「連線字串不正確」事件	連線字串不正確
1.3.6.1.4.1.6876.100.1.0.80606	vmwInvalidCredentialsEvent	嚴重	「認證無效」事件	認證無效
1.3.6.1.4.1.6876.100.1.0.80608	vmwUnknownHostEvent	嚴重	「主機不明」事件	主機不明
1.3.6.1.4.1.6876.100.1.0.80609	vmwSNMPConnectionInvalidEvent	嚴重	「SNMP 連線無效」事件	SNMP 連線無效
1.3.6.1.4.1.6876.100.1.0.80610012	vmwPwdAuthModeDisabledAristaEvent	嚴重	「密碼驗證已停用」事件	密碼驗證已停用
1.3.6.1.4.1.6876.100.1.0.806100018	vmwUnsupportedNSXVersionEvent	嚴重	「NSX 版本不受支援」事件	NSX 版本不受支援
1.3.6.1.4.1.6876.100.1.0.80611	vmwFailedCredentialsEncryptEvent	嚴重	「認證加密失敗」事件	認證加密失敗
1.3.6.1.4.1.6876.100.1.0.80612	vmwPwdAuthModeDisabledEvent	嚴重	「密碼驗證模式已停用」事件	密碼驗證模式已停用

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80613	vmwInsufficientPrivilegesEvent	嚴重	「權限不足」事件	權限不足
1.3.6.1.4.1.6876.100.1.0.8061313	vmwFlowCollectionErrorEvent	嚴重	「流量收集錯誤」事件	流量收集錯誤
1.3.6.1.4.1.6876.100.1.0.8061314	vmwAWSThrottlingExceptionEvent	嚴重	「AWS 節流例外狀況」事件	AWS 節流例外狀況
1.3.6.1.4.1.6876.100.1.0.8061315	vmwAWSFlowLogAccessDeniedExceptionEvent	嚴重	「AWS 流量記錄存取遭拒例外狀況」事件	AWS 流量記錄存取遭拒例外狀況。當使用者沒有收集流量記錄的必要權限時，會發生此事件。
1.3.6.1.4.1.6876.100.1.0.80614	vmwNotFoundEvent	嚴重	「找不到」事件	找不到
1.3.6.1.4.1.6876.100.1.0.80616	vmwInvalidConfigEvent	嚴重	「無效的資料來源組態」事件	無效的資料來源組態
1.3.6.1.4.1.6876.100.1.0.80617	vmwWarnConfigEvent	嚴重	「無效的資料來源組態」事件	無效的資料來源組態
1.3.6.1.4.1.6876.100.1.0.80618	vmwUnexpectedDSTypeOrVersionEvent	嚴重	「未預期的資料來源類型或版本」事件	未預期的資料來源類型或版本
1.3.6.1.4.1.6876.100.1.0.80619	vmwNSXControllerNotFoundEvent	嚴重	「找不到 NSX Controller」事件	找不到 NSX Controller
1.3.6.1.4.1.6876.100.1.0.80620	vmwHostNotReachableEvent	嚴重	「無法連線到主機」事件	無法連線到主機
1.3.6.1.4.1.6876.100.1.0.80621	vmwInvalidResponseFromDataSourceEvent	嚴重	「從資料來源的回應無效」事件	從資料來源的回應無效
1.3.6.1.4.1.6876.100.1.0.80622	vmwDataProviderNotRunningEvent	嚴重	「資料來源未執行」事件	資料來源未執行
1.3.6.1.4.1.6876.100.1.0.80623	vmwPrimaryNSXNotAddedEvent	嚴重	「未新增主要 NSX」事件	未新增主要 NSX
1.3.6.1.4.1.6876.100.1.0.80624	vmwHostnameResolutionErrorEvent	嚴重	「主機名稱解析錯誤」事件	主機名稱解析錯誤
1.3.6.1.4.1.6876.100.1.0.80625	vmwNumVMsOrHostsNotFoundEvent	嚴重	「找不到虛擬機器或主機的數目」事件	找不到虛擬機器或主機的數目

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80626	vmwNSXIPFIXStatusMismatchEvent	嚴重	「NSX IPFIX 狀態不相符」事件	NSX IPFIX 狀態不相符
1.3.6.1.4.1.6876.100.1.0.80627	vmwFlowPhysicalNodeEvent	嚴重	「流量實體節點」事件	流量實體節點
1.3.6.1.4.1.6876.100.1.0.80628	vmwNotEmptyNodeEvent	嚴重	「不是空節點」事件	不是空節點
1.3.6.1.4.1.6876.100.1.0.80629	vmwUnsupportedNSXTVersionEvent	嚴重	「NSXT 版本不受支援」事件	NSXT 版本不受支援
1.3.6.1.4.1.6876.100.1.0.80630	vmwComputeManagersNotFoundEvent	嚴重	「找不到計算管理程式」事件	找不到計算管理程式
1.3.6.1.4.1.6876.100.1.0.80631	vmwComputeManagersNotAddedEvent	嚴重	「未新增計算管理程式」事件	未新增計算管理程式
1.3.6.1.4.1.6876.100.1.0.80632	vmwUnsupportedLogInsightVersionEvent	嚴重	「Log Insight 版本不受支援」事件	Log Insight 版本不受支援
1.3.6.1.4.1.6876.100.1.0.80633	vmwUnsupportedVRNICContentPackVersionEvent	嚴重	「vRealize Network Insight 內容套件版本不受支援」事件	vRealize Network Insight 內容套件版本不受支援
1.3.6.1.4.1.6876.100.1.0.80634	vmwVRNICContentPackNotInstalledEvent	嚴重	「在 Log Insight 中找不到 vRealize Network Insight 內容套件」事件	在 Log Insight 中找不到 vRealize Network Insight 內容套件
1.3.6.1.4.1.6876.100.1.0.80635	vmwWebhookNotEnabledOnAlertEvent	嚴重	「在 Network Insight 警示上未啟用 Webhook」事件	未針對 Log Insight 中的一或多個 vRealize Network Insight 內容套件警示啟用 Webhook
1.3.6.1.4.1.6876.100.1.0.80636	vmwIncorrectWebhookConfiguredOnAlertEvent	嚴重	「在 Log Insight 警示上設定的 Webhook URL 不正確」事件	針對 Log Insight 中的一或多個 vRealize Network Insight 內容套件警示找到的 webhook 組態不正確
1.3.6.1.4.1.6876.100.1.0.80637	vmwWebhookNotRunningEvent	嚴重	「Webhook 未在收集器 (Proxy) 虛擬機器上執行」事件	Webhook 未在收集器 (Proxy) 虛擬機器上執行

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80638	vmwInfobloxRecordLimitExceededEvent	嚴重	Infoblox 中的記錄數目超過目前限制	Infoblox 中的記錄數目超過目前限制
1.3.6.1.4.1.6876.100.1.0.80639	vmwIncorrectInfobloxCredentialEvent	嚴重	「Infoblox 認證不正確」事件	Infoblox 認證無效，或使用者不具有存取 Infoblox 資料的「API 權限」
1.3.6.1.4.1.6876.100.1.0.80640	vmwUnsupportedInfobloxVersionEvent	嚴重	「Infoblox 版本不受支援」事件	NIOS 版本不受支援。
1.3.6.1.4.1.6876.100.1.0.80641	vmwUnknownInfobloxVersionEvent	嚴重	「Infoblox 版本未知」事件	無法確定 NIOS 版本。
1.3.6.1.4.1.6876.100.1.0.80642	vmwNoDVSAvailableEvent	嚴重	「無法啟用 IPFIX」事件	由於找不到 DVS，無法啟用 IPFIX
1.3.6.1.4.1.6876.100.1.0.80643	vmwVCNotOnSameProxyEvent	嚴重	「NSX Manager 和 vCenter 資料來源不在同一個收集器虛擬機器上」事件	NSX Manager 和相關聯的 vCenter 資料來源不在同一個收集器虛擬機器上。
1.3.6.1.4.1.6876.100.1.0.80644	vmwNSXTIPFixNoCollectorProfileEvent	嚴重	「NSX-T IPFIX 沒有收集器設定檔」事件	NSXT IPFIX 沒有收集器設定檔
1.3.6.1.4.1.6876.100.1.0.80645	vmwNSXTIPFixNoNewCollectorProfileCanBeAddedEvent	嚴重	「NSX-T IPFIX 無法新增任何收集器設定檔」事件	NSXT IPFIX 無法新增任何收集器設定檔
1.3.6.1.4.1.6876.100.1.0.80646	vmwNSXTIPFixNoIPFixProfileEvent	嚴重	「NSX-T IPFIX 沒有 IPFIX 設定檔」事件	NSXT IPFIX 沒有 IPFIX 設定檔
1.3.6.1.4.1.6876.100.1.0.80647	vmwNSXTIPFixIPFixProfilePriorityNotZeroEvent	嚴重	「NSX-T IPFIX IPFIX 設定檔優先順序不是零」事件	NSXT IPFIX IPFIX 設定檔優先順序不是零
1.3.6.1.4.1.6876.100.1.0.80648	vmwNSXTIPFixCollectorAndIPFixProfileMismatchEvent	嚴重	「NSX-T IPFIX 收集器和 IPFIX 設定檔不相符」事件	NSXT IPFIX 收集器和 IPFIX 設定檔不相符
1.3.6.1.4.1.6876.100.1.0.80649	vmwNSXTIPFixPortIncorrectEvent	嚴重	「NSX-T IPFIX 收集器連接埠不正確」事件	收集器設定檔中的收集器連接埠不正確

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80650	vmwNSXTIPFixDFWStatusNotEnabledEvent	嚴重	「未啟用 NSX-T IPFIX DFW」事件	未啟用 NSX-T IPFIX DFW
1.3.6.1.4.1.6876.100.1.0.80651	vmwPolicyManagerNoDfwIPFixProfile	嚴重	「NSX Policy Manager 上不存在 DFW IPFIX 設定檔」事件。	在 NSX Policy Manager 上找不到 DFW IPFIX 設定檔
1.3.6.1.4.1.6876.100.1.0.80652	vmwPolicyManagerVrniDfwIPFixCollectorAbsent	嚴重	「NSX Policy Manager 上不存在 Network Insight IPFIX 收集器組態」事件。	Network Insight IPFIX 收集器 IP 和連接埠不存在於 NSX Policy Manager 上的 DFW IPFIX 收集器設定檔中。
1.3.6.1.4.1.6876.100.1.0.80653	vmwDataSourceIdentificationChangedEvent	資訊	資料來源的身分識別資訊已變更	憑證或金鑰等資料來源身分識別資訊已變更。
1.3.6.1.4.1.6876.100.1.0.80654	vmwPKSKubernetesUnknownHostEvent	嚴重	「Kubernetes 叢集 API 伺服器無法連線」事件	PKS 中的一或多個 Kubernetes 叢集的 Kube 組態檔無效。
1.3.6.1.4.1.6876.100.1.0.80655	vmwKubernetesInsufficientPrivilegesEvent	嚴重	Kubernetes 叢集服務帳戶沒有足夠的權限	一或多個 Kubernetes 叢集服務帳戶沒有足夠的權限。
1.3.6.1.4.1.6876.100.1.0.80657	vmwUANIFileNotProvidedEvent	嚴重	未提供一般路由器和交換器資料來源所需的檔案	未提供一般路由器和交換器資料來源所需的檔案
1.3.6.1.4.1.6876.100.1.0.80658	vmwUANIFileDoesNotExistEvent	嚴重	一般路由器和交換器資料來源所需的檔案不存在	一般路由器和交換器資料來源所需的檔案不存在
1.3.6.1.4.1.6876.100.1.0.80659	vmwNSXTLatencyNotEnabledEvent	嚴重	NSXT_LATENCY_NOT_ENABLED_EVENT	未啟用 NSX-T 延遲收集
1.3.6.1.4.1.6876.100.1.0.80660	vmwNSXTLatencyMoreBFDProfileEvent		NSXT_LATENCY_MORE_BFD_PROFILE_EVENT	
1.3.6.1.4.1.6876.100.1.0.80662	vmwNSXTLatencyCollectorMismatchEvent	嚴重	NSXT_LATENCY_COLLECTOR_MISMATCH_EVENT	未設定 NSX-T 延遲收集器
1.3.6.1.4.1.6876.100.1.0.80663	vmwBigIpInsufficientShellAccessEvent	嚴重	BIGIP_INSUFFICIENT_SHELL_ACCESS_EVENT	沒有 Shell 存取權

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80664	vmwBigIpInsufficientPartitionAccessEvent	嚴重	BIGIP_INSUFFICIENT_PARTITION_ACCESS_EVENT	磁碟分割存取權不足
1.3.6.1.4.1.6876.100.1.0.80665	vmwBigIpInsufficientRoleEvent	嚴重	BIGIP_INSUFFICIENT_ROLE_EVENT	角色不足
1.3.6.1.4.1.6876.100.1.0.90001	vmwVeloCloudEdgeDownEvent	警告	VeloCloud Edge 狀況不良	VeloCloud Edge 的 Edge 狀態為未連線。
1.3.6.1.4.1.6876.100.1.0.90002	vmwVeloCloudLinkDownEvent	警告	VeloCloud 連結狀況不良	VeloCloud Edge 的連結狀態為未連線。
1.3.6.1.4.1.6876.100.1.0.90005	vmwVeloCloudLinkLostPacketEventTx	嚴重	VeloCloud 連結上游封包遺失超過臨界值。	VeloCloud 連結封包遺失事件 (Tx)。
1.3.6.1.4.1.6876.100.1.0.90007	vmwVeloCloudLinkDegradedVoiceQoeEvent	嚴重	VeloCloud 連結語音 QOE 已降級。	VeloCloud 連結已降級語音 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90008	vmwVeloCloudLinkDegradedVideoQoeEvent	嚴重	VeloCloud 連結視訊 QOE 已降級。	VeloCloud 連結已降級視訊 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90009	vmwVeloCloudLinkDegradedTransQoeEvent	嚴重	VeloCloud 連結交易 QOE 已降級。	VeloCloud 連結已降級交易 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90010	vmwVeloCloudEdgeDegradedVoiceQoeEvent	嚴重	VeloCloud Edge 語音 QOE 已降級。	VeloCloud Edge 已降級語音 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90011	vmwVeloCloudEdgeDegradedVideoQoeEvent	嚴重	VeloCloud Edge 視訊 QOE 已降級。	VeloCloud Edge 已降級視訊 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90012	vmwVeloCloudEdgeDegradedTransQoeEvent	嚴重	VeloCloud Edge 交易 QOE 已降級。	VeloCloud Edge 已降級傳輸 QOE 事件。
1.3.6.1.4.1.6876.100.1.0.90013	vmwVeloCloudLinkLostPacketEventRx	嚴重	VeloCloud 連結下游封包遺失超過臨界值。	VeloCloud 連結封包遺失事件 (Rx)。

檢視和編輯系統事件

事件由系統或使用者定義。系統事件是預先定義的事件。

系統事件在**系統事件**頁面的**設定**下列出。將為每個事件指定下列欄位。可以根據您的需求在除了 [事件] 資料行外的所有下列資料行中篩選資訊。

表 6-2.

資料行	說明
事件	此欄位指定事件的名稱。
嚴重性	此欄位指定事件的嚴重性。您可以將其設定為下列值： <ul style="list-style-type: none"> ■ 嚴重 ■ 中等 ■ 警告 ■ 資訊
類型	此欄位指定事件是表示問題還是變更。 備註 類型為問題的所有事件均會記錄至 Syslog。
實體	此欄位指定將事件設定為包含或排除用於產生事件的實體。依預設，值為 All。
通知	此欄位指定已傳送的通知類型。通知可透過電子郵件和/或 SNMP 設陷傳送。 備註 您必須為定義的所有重要系統事件啟用通知。若要取得所有重要系統事件的清單，請依嚴重性排序系統事件。
已啟用	如果已啟用事件，則選取此選項。

將游標暫留在每個事件上時，您可以查看**更多資訊**。透過按一下此選項，您可以查看該事件的說明、事件標籤和實體類型。

您可以對系統事件執行下列工作：

- 編輯事件
- 執行大量編輯
- 針對特定實體停用事件

編輯系統事件

您可以編輯系統事件，並定義慣用系統事件的通知。

程序

- 1 在特定事件的**已啟用**資料行旁邊，按一下編輯圖示。
- 2 視需要新增或移除事件標籤。
- 3 變更嚴重性。
- 4 如果要為所選實體啟用或停用此事件，請選取 [包含/排除實體]。
 - 建立包含規則：
 - a 選取**包含清單**。
 - b 在**條件**下指定要為事件包含的實體。

- 建立排除規則：
 - a 選取**排除清單**。
 - b 在**條件**下指定要為事件排除的實體。

備註

- 您可以在包含和排除清單中建立多個規則。
- 選取 **NSX Manager** 時，您可以在兩個清單中新增例外狀況。如果您想要包含或排除規則保留特定實體的例外狀況，可以定義例外狀況。
- 也可以透過撰寫自己的查詢以包含或排除實體來指定 **Custom Search**。

- 5 若要設定必須傳送通知的時間，請選取**啟用通知**核取方塊。視您的組態而定，請執行下列操作：

選項	動作
如果您未設定電子郵件伺服器	按一下 設定郵件伺服器 。若要瞭解如何設定郵件伺服器，請參閱 設定郵件伺服器 。
如果您未設定 SNMP 設陷	按一下 設定 SNMP 設陷 。若要瞭解如何設定 SNMP 設陷，請參閱 設定 SNMP 設陷目的地 。
如果您已設定電子郵件伺服器	在 電子郵件頻率 下拉式功能表中指定接收電子郵件的頻率，並在 傳送通知電子郵件到文字方塊 中指定電子郵件地址。
如果您已設定 SNMP 設陷	從 傳送 SNMP 設陷 至下拉式功能表中，選取一或多個 SNMP 設陷目的地。您最多可以選取四個 SNMP 設陷目的地。

- 6 按一下**提交**。

對事件執行大量編輯

- 1 在**系統事件**頁面中，選取多個事件時，**啟用**、**停用**和**編輯**選項將顯示在清單上方。
- 2 按一下**編輯**。
- 3 在**編輯**頁面中，具有下列選項：
 - **覆寫現有值**：在此選項中，僅覆寫您編輯的欄位。
 - **新增至現有**：在此選項中，您可以新增至現有值，例如電子郵件地址和事件標籤。
- 4 按一下**提交**。

停用事件

- 1 您可以在首頁上的**未解決的問題** Widget 中選取事件。也可以在搜尋列中輸入**問題**，然後從清單中選取事件。
- 2 選取特定事件，然後按一下**封存**。
- 3 選取**未來停用此類型的所有事件**，然後選取一個實體或所有實體。

4 按一下儲存。

備註 在嚴重性、標籤或包含/排除規則中所做的變更會反映在未來事件中。現有事件會繼續顯示舊組態。

事件限制

本節提供各種系統定義事件的限制。

Distributed Firewall 規則被上述規則事件限制遮罩

此事件具有下列限制：

- 僅 NSX-V Distributed Firewall 規則支援此事件。不支援其他防火牆廠商。
- 目前支援下列防火牆規則內容用於遮罩計算：
 - 來源
 - 目的地
 - 套用至
 - 服務通訊協定和連接埠範圍
 - 封包類型
 - 第 7 層應用程式識別碼
- 不支援來源或目的地反轉的規則。
- 會忽略已停用的規則。
- 不支援安全群組在「來源」/「目的地」或「套用至」中直接或間接包含已排除成員的規則。
- 「來源」、「目的地」或「套用至」內容的遮罩計算是基於成員 IPSet 的靜態成員資格和 IP 範圍重疊的。不會將安全群組的動態成員資格納入遮罩考量。

編輯使用者定義的事件

使用者定義的事件以搜尋為基礎。

所有使用者定義的事件均在**使用者定義的事件**頁面的**設定**下列出。將為每個事件指定下列欄位。

表 6-3.

欄位	說明
名稱 (搜尋準則)	此欄位指定事件的名稱和事件的搜尋準則。
嚴重性	此欄位指定警示的嚴重性。您可以將其設定為下列值： <ul style="list-style-type: none"> ■ 嚴重 ■ 中等 ■ 警告 ■ 資訊
類型	此欄位指定事件是表示問題還是變更。

表 6-3. (續)

欄位	說明
通知時間	此欄位指定必須傳送通知的時間。
建立者	此欄位指定建立事件的人員。
已啟用	如果已啟用事件，則選取此選項。

您可以編輯或刪除事件。當您進行編輯時，可以指定電子郵件地址和電子郵件通知的頻率。

設定使用者定義的事件

您可以透過搜尋建立使用者定義的事件。

程序

- 1 在搜尋結果視窗中按一下 [建立通知] 圖示。
[設定使用者定義的事件] 頁面隨即開啟。
- 2 為事件輸入唯一名稱。
- 3 選取核取方塊以將事件標記為問題，然後選取嚴重性。
- 4 輸入唯一的搜尋準則。
- 5 選取要接收通知時的條件。
- 6 選取通知頻率為**立即**或**做為每日摘要**。
- 7 指定電子郵件地址。
- 8 若要設定 SNMP 伺服器，請按一下**設定 SNMP 設陷**。
如果您已設定 SNMP 伺服器，則選取**傳送 SNMP 設陷至 IP-address**。
您可以按一下**變更**以修改 SNMP 組態。
- 9 按一下**儲存**。

檢視平台健全狀況事件

[平台健全狀況事件] 頁面是一站式頁面，可檢視提供有關係統整體健全狀況狀態的詳細資料的所有事件。這些事件可能發生在基礎結構中的資料來源或節點上。您也可以透過搜尋檢視這些事件。

表 6-4.

欄位	說明
事件	此欄位指定事件的名稱。
嚴重性	此欄位指定事件的嚴重性。無法變更事件的嚴重性。

表 6-4. (續)

欄位	說明
類型	此欄位指定事件是表示問題還是變更。
通知	此欄位指定已傳送的通知類型。通知可透過電子郵件和/或 SNMP 設陷傳送。

NSX-T 事件

vRealize Network Insight 會引發數個自行計算的 NSX-T 事件。此外，vRealize Network Insight 中還會顯示所有 NSX-T 產生的系統事件 (針對 NSX-T 2.2 到 2.5 版) 以及 NSX-T 警示 (針對 NSX-T 3.0 版及更新版本)。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	警告	「NSX-T 第 1 層邏輯路由器中斷連線」事件	NSX-T 第 1 層邏輯路由器與第 0 層路由器中斷連線。無法從外部存取此路由器下的網路，反之亦然。
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	警告	已停用路由通告	已停用 NSX-T 第 1 層邏輯路由器的路由通告。無法從外部存取此路由器下的網路。
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有管理程式連線	NSX-T Edge 節點已中斷管理程式連線。
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	警告	NSX-T Edge 節點的控制器連線已降級	NSX-T Edge 節點無法與一或多個控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	嚴重	NSX-T Edge 節點沒有控制器連線	NSX-T Edge 節點無法與任何控制器通訊。
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMTuMismatchEvent	警告	NSX-T 第 0 層和上行交換器/路由器之間的 MTU 不相符	在第 0 層邏輯路由器的介面設定的 MTU 與來自相同 L2 網路的上行交換器/路由器的介面不相符。這可能會影響網路效能。
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	資訊	已從 NSX-T DFW 防火牆中排除一或多個虛擬機器。	一或多個虛擬機器不受 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 錯誤組態	由於第 0 層路由器的上行連接埠上的 VLAN 與外部網路上的 VLAN 不同，通訊將會中斷。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	警告	沒有傳輸區域連結到傳輸節點。	沒有傳輸區域連結到傳輸節點。虛擬機器可能會因此中斷連線。
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	警告	傳輸節點上沒有可用的 VTEP。	已從傳輸節點刪除所有 VTEP。虛擬機器可能會因此中斷連線。
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	嚴重	NSX-T 控制器節點不具有控制叢集連線	NSX-T 控制器節點已中斷控制叢集連線。
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	嚴重	NSX-T 控制器節點不具有管理平面連線	NSX-T 控制器節點已中斷管理平面連線。
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	嚴重	NSX-T 管理節點不具有管理叢集連線	NSX-T 管理節點已中斷管理叢集連線。
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 與主機傳輸節點的連線狀態之間不同步
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	嚴重	NSX-T Edge 節點的控制器連線處於「未知」狀態。	NSX-T Edge 節點控制器連線處於「未知」狀態。
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處於「未知」狀態。	NSX-T 主機節點控制器連線處於「未知」狀態。
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「關閉」。	NSX-T 主機傳輸節點 pNIC 狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「已降級」	NSX-T 主機傳輸節點 pNIC 狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	警告	NSX-T 主機傳輸節點 pNIC 狀態為「未知」。	NSX-T 主機傳輸節點 pNIC 狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	嚴重	NSX-T Edge 傳輸節點 pNIC 狀態為「關閉」。	NSX-T Edge 傳輸節點 pNIC 狀態為「關閉」。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
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	NSXTEdgeNodeTunnelStatusDegradeEvent	嚴重	NSX-T Edge 傳輸節點通道狀態為「已降級」。	NSX-T Edge 傳輸節點通道狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點通道狀態為「未知」。	NSX-T Edge 傳輸節點通道狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	警告	NSX-T 主機傳輸節點狀態為「關閉」。	NSX-T 主機傳輸節點狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	警告	NSX-T 主機傳輸節點狀態為「已降級」。	NSX-T 主機傳輸節點狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	警告	NSX-T 主機傳輸節點狀態為「未知」。	NSX-T 主機傳輸節點狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「關閉」。	NSX-T Edge 傳輸節點狀態為「關閉」。
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	嚴重	NSX-T Edge 傳輸節點狀態為「已降級」。	NSX-T Edge 傳輸節點狀態為「已降級」。
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	嚴重	NSX-T Edge 傳輸節點狀態為「未知」。	NSX-T Edge 傳輸節點狀態為「未知」。
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	警告	NSX-T 邏輯交換器管理狀態為「關閉」	NSX-T 邏輯交換器管理狀態為「關閉」

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
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) 之間的通訊失敗，例如，您無法從其中一個虛擬機器對另一個虛擬機器執行 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) 之間的通訊失敗，例如，您無法從其中一個虛擬機器對另一個虛擬機器執行 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	未排程 NSX-T Manager 備份。	未排程 NSX-T Manager 備份
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	嚴重	NSX-T DFW 防火牆已停用。	Distributed Firewall 在 NSX-T Manager 中已停用
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	警告	將捨棄 NSX-T 邏輯連接埠接收的封包。	接收的封包將在 NSX-T 邏輯連接埠上捨棄，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	將捨棄 NSX-T 邏輯連接埠傳輸的封包。	傳輸的封包將在 NSX-T 邏輯連接埠上捨棄，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	將捨棄 NSX-T 邏輯交換器接收的封包	接收的封包將在 NSX-T 邏輯交換器上捨棄，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	將捨棄 NSX-T 邏輯交換器傳輸的封包	傳輸的封包將在 NSX-T 邏輯交換器上捨棄，相關聯的實體可能會受到影響

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	警告	接收的封包將在 NSX-T 管理節點的網路介面上捨棄	接收的封包將在 NSX-T 管理節點的網路介面上捨棄。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	接收的封包將在 NSX-T Edge 節點的網路介面上捨棄	接收的封包將在 NSX-T Edge 節點的網路介面上捨棄。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	接收的封包將在 NSX-T 主機節點的網路介面上捨棄	接收的封包將在 NSX-T 主機節點的網路介面上捨棄。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	傳輸的封包將在 NSX-T 管理節點的網路介面上捨棄	傳輸的封包將在 NSX-T 管理節點的網路介面上捨棄。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	傳輸的封包將在 NSX-T Edge 節點的網路介面上捨棄	傳輸的封包將在 NSX-T Edge 節點的網路介面上捨棄。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	傳輸的封包將在 NSX-T 主機節點的網路介面上捨棄	傳輸的封包將在 NSX-T 主機節點的網路介面上捨棄。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 服務狀態已變為 [已停止]。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	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。	遙測服務狀態已變為 [已停止]。
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	警告	使用者介面服務已停止執行。	使用者介面服務狀態已變為 [已停止]。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	嚴重	CM 詳細目錄服務已停止	NSX-T 管理節點的其中一個服務，即 CM 詳細目錄服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	嚴重	控制器服務已停止	NSX-T 管理節點的其中一個服務，即控制器服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	嚴重	資料存放區服務已停止	NSX-T 管理節點的其中一個服務，即資料存放區服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	嚴重	HTTP 服務已停止	NSX-T 管理節點的其中一個服務，即 HTTP 服務已停止執行。
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 (即節點統計資料服務) 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。

表 6-5. vRealize Network Insight 計算的 NSX-T 事件 (續)

OID	事件名稱	預設嚴重性	使用者介面名稱	說明
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	嚴重	NTP 服務已停止	NSX-T 管理節點的其中一個服務，即 NTP 服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	嚴重	原則服務已停止	NSX-T 管理節點的其中一個服務，即原則服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	嚴重	搜尋服務已停止	NSX-T 管理節點的其中一個服務，即搜尋服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	警告	SNMP 服務已停止	NSX-T 管理節點的其中一個服務，即 SNMP 服務已停止執行。
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	使用者介面服務已停止	NSX-T 管理節點的其中一個服務，即使用者介面服務已停止執行。
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	嚴重	叢集管理程式服務已停止	NSX-T 管理節點的其中一個服務，即叢集管理程式服務已停止執行。

NSX-T 系統事件

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

表 6-6. NSX-T 系統事件

事件名稱	說明
vmwNSXPlatformSysCpuUsage	管理程式和 Edge 應用裝置上的 CPU 使用率 (NSX-T 2.2)。
vmwNSXPlatformSysDiskUsage	管理程式和 Edge 應用裝置上用於 /var/log 磁碟分割的磁碟空間使用量 (NSX-T 2.2)。
vmwNSXPlatformSysMemUsage	管理程式和 Edge 應用裝置上的記憶體使用量 (NSX-T 2.2)。
vmwNSXPlatformSysConfigDiskUsage	管理程式和 Edge 應用裝置上用於 /config 磁碟分割的磁碟使用量 (NSX-T 2.4)。

表 6-6. NSX-T 系統事件 (續)

事件名稱	說明
vmwNSXPlatformSysVarDumpDiskUsage	管理程式和 Edge 應用裝置上用於 /var/dump 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysRepositoryDiskUsage	管理程式和 Edge 應用裝置上用於 /repository 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysRootDiskUsage	管理程式和 Edge 應用裝置上用於根磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysTmpDiskUsage	管理程式和 Edge 應用裝置上用於 tmp 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXPlatformSysImageDiskUsage	管理程式和 Edge 應用裝置上用於 /image 磁碟分割的磁碟使用量 (NSX-T 2.5)。
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP 集區超載/正常 (NSX-T 2.5)。
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP 集區租用配置失敗/成功 (NSX-T 2.5)。
vmwNSXPlatformPasswordExpiryStatus	管理程式的密碼到期 (NSX-T 2.4)。
vmwNSXPlatformCertificateExpiryStatus	管理程式的憑證到期 (NSX-T 2.4)。
vmwNSXRoutingBgpNeighborStatus	BGP 芳鄰狀態 (NSX-T 2.2)。
vmwNSXVpnTunnelState	VPN 通道開啟/關閉 (NSX-T 2.2)。
vmwNSXVpnL2TunnelStatus	L2 VPN 工作階段開啟/關閉 (NSX-T 2.2)。
vmwNSXVpnIkeSessionStatus	IKE 工作階段開啟/關閉 (NSX-T 2.2)。
vmwNSXDnsForwarderStatus	DNS 轉寄站狀態 (NSX-T 2.4)。
vmwNSXClusterNodeStatus	叢集節點狀態 (NSX-T 2.4)。
vmwNSXFabricCryptoStatus	Edge 加密 mux 驅動程式失敗/已通過 Known_Answer_Tests(KAT) (NSX-T 2.4)。
管理程式磁碟使用量不正常	
BGP 芳鄰關閉	當 BGP 芳鄰關閉時需要警示。
BGP 芳鄰開啟	當芳鄰開啟時清除警示。
儲存區使用量超過 X	針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機)，會產生「儲存區超過 X - 事件」警示。
記憶體使用量超過 X	針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機)，會產生「記憶體超過 X - 事件」警示。
CPU 使用量超過 X	針對所有應用裝置虛擬機器 (MP、CCP) 或傳輸節點 (Edge、主機)，會產生「CPU 超過 X - 事件」警示。

NSX-T 系統警示

備註 除了這些事件，所有 NSX-T 3.0 警示還將顯示為 vRealize Network Insight 5.2 及更新版本中的 NSX-T 系統事件。您可以透過以下網址查看 NSX-T 所產生的完整警示清單：https://NSX-T_IP_Address/nsx/#/app/home/alarms/alarm-definitions。

Kubernetes 事件

以下是 vRealize Network Insight 中支援的 Kubernetes 事件的清單。所有 Kubernetes 事件的物件識別碼 (OID) 為 1.3.6.1.4.1.6876.100.1.0.1510。

事件名稱	嚴重性	說明
FailedToCreateContainer	嚴重	無法建立容器
FailedToStartContainer	嚴重	無法啟動容器
PreemptContainer	警告	先佔其他網繭。
BackOffStartContainer	警告	後端停止重新啟動使容器失敗。
ExceededGracePeriod	警告	容器執行階段未在指定的寬限期內停止網繭。
FailedToKillPod	警告	無法停止網繭。
FailedToCreatePodContainer	中等	無法建立網繭容器。
FailedToMakePodDataDirectories	中等	無法建立網繭資料目錄。
NetworkNotReady	警告 嚴重	網路未就緒。
FailedScheduling	嚴重	無法排程網繭
FailedToPullImage	警告 嚴重	無法提取映像。
FailedToInspectImage	警告	無法檢查映像。
ErrImageNeverPullPolicy	警告	違反了映像的 NeverPull 原則。
ImagePullBackOff	嚴重	容器映像提取失敗，kubelet 正在後端停止映像提取
ImageInspectError	警告	無法檢查映像
ErrImagePull	嚴重	映像提取錯誤
ErrImageNeverPull	嚴重	主機上不存在所需的映像，且 PullPolicy 為 NeverPullImage
RegistryUnavailable	嚴重	從登錄提取映像時發生 HTTP 錯誤
InvalidImageName	嚴重	無法剖析映像名稱
KubeletSetupFailed	中等	Kubelet 設定失敗。
FailedAttachVolume	嚴重	無法連結磁碟區。

事件名稱	嚴重性	說明
FailedMountVolume	嚴重	無法掛接磁碟區。
VolumeResizeFailed	警告	無法擴充/縮小磁碟區。
FileSystemResizeFailed	警告	無法擴充/縮小檔案系統。
FailedMapVolume	嚴重	無法對應磁碟區。
WarnAlreadyMountedVolume	警告	已掛接磁碟區。
ContainerGCFailed	警告	容器廢棄項目收集失敗。
ImageGCFailed	警告	映像廢棄項目收集失敗。
FailedNodeAllocatableEnforcement	警告	無法強制執行系統保留的 Cgroup 限制。
FailedCreatePodSandBox	警告	無法建立網繭沙箱。
FailedStatusPodSandBox	警告	失敗的網繭沙箱狀態。
InvalidDiskCapacity	中等	磁碟容量無效。
FreeDiskSpaceFailed	中等	釋放磁碟空間失敗。
ContainerUnhealthy	嚴重	容器狀況不良。
ContainerProbeWarning	警告	容器探查成功，並顯示警告。
FailedSync	警告	網繭同步失敗。
FailedValidation	警告	網繭組態驗證失敗。
FailedPostStartHook	警告	對於網繭啟動，處理常式失敗。
FailedPreStopHook	警告	對於預停止，處理常式失敗。
NodeNotReady	嚴重	節點未就緒。
NodeNotSchedulable	嚴重	節點不可排程。
NodeRebooted	中等	節點已重新開機。

通知

基於搜尋的通知

基於搜尋的通知可分為以下幾類：

- 基於系統的通知
- 使用者定義的通知

基於系統的通知參數是預先定義的，並在啟用通知警示時以郵件形式傳送通知。使用者定義的通知使用者根據其需求進行設定。您可以根據您的搜尋查詢建立電子郵件通知。執行搜尋後，將在結果頁面上顯示**建立通知**選項。對於每個搜尋，您可以：

- 選取要接收通知時的條件。
- 定義要接收通知的頻率。
- 輸入每個通知的電子郵件收件者 (依預設，您的電子郵件識別碼顯示在收件者清單中；您也可以新增多個電子郵件識別碼)。

對於使用者定義的搜尋：

- 必須為基於搜尋的通知指派名稱。
- 必須為標記為問題的搜尋的事件選取嚴重性。
- 使用者定義的事件由搜尋準則唯一識別。
- 您可以將通知頻率指定為**立即**或**做為每日摘要**。

您可以從**設定 > 基於搜尋的通知**頁面管理通知。在**基於搜尋的通知**頁面上，您可以檢視現有的通知，對其進行編輯，將其啟用或停用，也可以刪除不需要的通知。

設定事件通知

通知以電子郵件進行傳送。

若要設定通知，您必須先設定郵件伺服器。若要瞭解如何設定郵件伺服器，請參閱[設定郵件伺服器](#)。

指定要傳送電子郵件通知的事件

使用者可以指定要傳送郵件通知的事件。

指定事件

- 1 在**設定**頁面上，按一下**基於搜尋的通知**，或者僅使用 [搜尋] 方塊來搜尋任何資訊。
- 2 在 [基於搜尋的通知] 頁面上，按一下**建立通知**圖示。會顯示通知對話方塊。
- 3 在**接收通知時間**方塊中，選取要傳送通知的事件。
- 4 在**通知**方塊中，選取傳送通知的頻率。
- 5 如果您不希望發生此事件，請選取**將其標記為問題**核取方塊。
- 6 輸入要接收通知的電子郵件地址，然後按一下**儲存**。

備註 若要確認通知郵件是否已正確設定，請按一下**傳送測試電子郵件**。

事件通知

vRealize Network Insight 包含預先定義的系統事件 (系統問題和系統變更) 清單，您可以每隔四個小時 (該時間可進行修改) 接收一次自動電子郵件通知。

您可以在**設定 > 系統通知**頁面上檢視通知清單。

備註 管理員使用者看不到其他管理員使用者或成員使用者的已訂閱平台和系統事件。

如果您未設定事件的任何電子郵件或 SNMP 通知，則會在首頁上看到提醒並允許您定義通知的警示訊息。您可以按一下警示訊息中的**啟用通知**以直接導覽至 [系統事件] 頁面，並訂閱慣用事件的通知。

若要停用提醒，請選取**不再顯示此訊息**選項。將不會針對此特定使用者顯示警示訊息。若要稍後定義通知，請導覽至**設定 > 事件**。

將問題封存

將問題封存

- 按一下 [全部顯示] 連結 (如果事件有多個執行個體)，以顯示事件的所有執行個體。
- 將游標暫留在要封存的事件執行個體上，以顯示一組圖示，然後按一下 [封存] 圖示。
- 在事件特定的對話方塊中
 - 如果要僅將此事件封存，則從 [即將封存] 清單中選取此事件。
 - 如果要將相同類型的所有事件封存至系統中，則從 [即將封存] 清單中選取此類型的所有事件。
- 按一下**儲存**。

檢視所有已封存的事件

- 在首頁上，在 [搜尋] 方塊中輸入事件，然後按 **Enter**。此時會顯示事件清單。
- 在左側窗格的 [已封存] 面中，選取 True 核取方塊 (在下方的螢幕擷取畫面中反白顯示)。

可以在此處檢視所有已封存的事件。

還原已封存的事件

- 在已封存事件上，按一下 [已封存] 圖示。(請參閱有關檢視已封存事件的上一節，瞭解如何移至 [已封存事件] 頁面)。
- 在事件特定的對話方塊中
 - 如果要僅還原此事件，則從 [即將從封存檔還原] 清單中選取此事件。
 - 如果要還原所有類似類型的事件，則從 [即將從封存檔還原] 清單中選取此類型的所有事件。
 - 按一下 [儲存] 以完成還原。

停用事件

使用者可以選擇性地停用事件以及禁止未來傳送通知。

停用事件通知

方法 1

- 在事件上，按一下**全部顯示**連結 (如果事件有多個執行個體)，以顯示事件的所有執行個體。
- 將游標暫留在要停用其通知的事件的執行個體上。這將會顯示一組圖示，請按一下 [封存] 圖示。

3 在事件特定的對話方塊中，選取**未來停用此類型的所有事件**核取方塊，然後按一下**儲存**。

方法 2

- 1 在**首頁**的右上角，按一下**設定檔**圖示，然後按一下**設定**。
- 2 在**設定區段**中，按一下**事件通知**以查看所有已啟用事件和已停用事件的清單。
- 3 在要停用的已啟用事件上，在**已啟用資料行**中，按一下相應滑桿的左側空白。
- 4 在**確認動作**對話方塊中，按一下**是**。

設定事件通知服務

使用者可以為不同事件啟用客戶通知

設定通知服務

- 1 在 [設定] 上，移至 [事件通知]，然後按一下與要啟用電子郵件通知和 SNMP 的問題相對應的 (編輯) 圖示。
- 2 在 [編輯系統通知] 對話方塊中，輸入要向其傳送電子郵件通知的電子郵件地址。在 [電子郵件頻率] 方塊中，選取要接收通知的時間頻率。
- 3 選取 [為此事件啟用 SNMP 設陷] 核取方塊，以設定 SNMP 通知。
- 4 按一下**儲存**。
- 5 成功啟用後，會顯示相應的郵件和 SNMP 圖示 (在下方的螢幕擷取畫面中反白顯示)。

設定身分識別與存取管理

在 vRealize Network Insight 中，您可以建立使用者，或設定的 LDAP 使用者和 VMware Identity Manager 使用者的存取權。您也可以為使用者指派不同的角色。

設定使用者管理

vRealize Network Insight 支援為使用者指派三種類型的角色。使用者可以根據已指派的角色存取 vRealize Network Insight 功能。

- **管理員**：管理員具有完全存取權。
- **成員**：成員使用者具有有限的存取權。
- **稽核員**：稽核員具有唯讀存取權，無法執行所有建立、新增、編輯或刪除動作。使用者只能檢視狀態。

表 6-7. 每個角色支援的功能

頁面	動作	管理員
[設定] 記錄：稽核記錄	檢視：[稽核記錄] 頁面/索引標籤	允許
	啟用/停用：個人識別資訊	允許
	檢視/篩選：稽核記錄	允許
	匯出為 CSV	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
[設定] 記錄：Syslog 組態	檢視：[Syslog 組態] 頁面/索引標籤	允許
	啟用/停用 Syslog	允許
	新增：Syslog 伺服器	允許
	編輯/刪除：Syslog 伺服器	允許
	檢視：Syslog 伺服器	允許
	檢視：來源伺服器對應	允許
	編輯：來源伺服器對應	允許
[設定] 關於	檢視有關產品的詳細資料 (名稱、版本、服務標籤)	允許
[設定] 系統組態	檢視：[系統組態] 頁面/索引標籤	允許
	檢視：使用者工作階段逾時	允許
	編輯：使用者工作階段逾時	允許
	檢視：資料來源憑證驗證	允許
	編輯：資料來源憑證驗證	允許
	檢視：Google 地圖 API 金鑰	允許
	編輯：Google 地圖 API 金鑰	允許
[設定] 我的喜好設定	檢視/編輯：我的喜好設定	允許
[設定] 授權和使用量	檢視：[授權和使用量] 頁面/索引標籤	允許
	檢視：授權詳細資料	允許
	新增/驗證：授權金鑰	允許
	刪除：授權金鑰	允許
	選項：「想要管理資料來源」	允許
	選項 ([帳戶和資料來源] 頁面的連結)：「將資料來源新增至目前使用量」	允許
[設定] SNMP 設陷目的地	檢視：[SNMP 設陷目的地] 頁面/索引標籤	允許
	檢視：現有 SNMP 目的地 (已設定事件數目) 的清單	允許
	檢視：為每個 SNMP 目的地設定的事件清單	允許
	新增/編輯/刪除/移轉/傳送測試設陷：SNMP 目的地	允許
[設定] 郵件伺服器	檢視：[郵件伺服器] 頁面/索引標籤	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
	檢視：郵件伺服器的現有組態	允許
	新增/編輯/刪除：郵件伺服器組態	允許
	傳送測試電子郵件	允許
[設定] 身分識別與存取管理	檢視：[身分識別與存取管理] 頁面/索引標籤	允許
[設定] 身分識別與存取管理：LDAP	檢視：LDAP 頁面/索引標籤	允許
	檢視：LDAP 現有組態	允許
	新增/編輯/刪除：LDAP 組態	允許
[設定] 身分識別與存取管理：VIDM	檢視：VIDM 頁面/索引標籤	允許
	檢視：VIDM 現有組態	允許
	新增/編輯/刪除：VIDM 組態	允許
	切換：VIDM 組態	允許
[設定] 身分識別與存取管理：使用者管理	檢視：[使用者管理] 頁面/索引標籤	允許
	檢視：本機/LDAP/VIDM 使用者	允許
	新增/編輯/刪除：本機使用者	允許
	新增/編輯/刪除：LDAP 使用者	允許
	新增/編輯/刪除：VIDM 使用者	允許
[設定] 事件	檢視：[事件] 頁面/索引標籤	允許
[設定] 事件：系統事件	檢視：[系統事件] 頁面/索引標籤	允許
	檢視：系統事件清單	允許
	編輯：系統事件	允許
	啟用/停用：系統事件	允許
	大量編輯/啟用/停用：系統事件	允許
[設定] 事件：平台健全狀況事件	檢視：[平台健全狀況事件] 頁面/索引標籤	允許
	檢視：平台健全狀況事件的清單	允許
	編輯：平台健全狀況事件	允許
	大量編輯：平台健全狀況事件	允許
[設定] 事件：使用者定義的事件	檢視：[使用者定義的事件] 頁面/索引標籤	允許
	檢視：使用者定義的事件清單	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
	編輯/刪除：使用者定義的事件	允許
	啟用/停用：使用者定義的事件	允許
[設定] IP 內容和子網路	檢視：[IP 內容和子網路] 頁面/索引標籤	允許
[設定] 實體 IP 和 DNS 對應	檢視：[實體 IP 和 DNS 對應] 頁面/索引標籤	允許
	檢視：上次匯入的實體 IP 和 DNS 對應	允許
	下載：實體 IP 和 DNS 對應檔案	允許
	上傳/取代：實體 IP 和 DNS 對應	允許
	刪除：現有的實體 IP 和 DNS 對應	允許
[設定] 實體子網路和 VLAN	檢視：[實體子網路和 VLAN] 頁面/索引標籤	允許
	檢視：已設定的實體子網路和 VLAN 的現有清單	允許
	新增/編輯/刪除：實體子網路和 VLAN	允許
[設定] 東西向 IP	檢視：[東西向 IP] 頁面/索引標籤	允許
	檢視：現有的東西向 IP 標籤	允許
	新增/更新/刪除：東西向 IP 標籤	允許
[設定] 南北向 IP	檢視：[南北向 IP] 頁面/索引標籤	允許
	檢視：現有的南北向 IP 標籤	允許
	新增/更新/刪除：南北向 IP 標籤	允許
[設定] 帳戶和資料來源	檢視：[帳戶和資料來源] 頁面/索引標籤	允許
	檢視：現有資料來源	允許
	新增/編輯/刪除：資料來源	允許
	啟用/停用：現有資料來源	允許
[設定] 資料管理	檢視：[資料管理] 頁面/索引標籤	允許
	檢視：資料保留間隔詳細資料	允許
	編輯：資料保留間隔詳細資料	允許
[設定] 基礎結構和支援	檢視：[基礎結構和支援] 頁面/索引標籤	允許
[設定] 基礎結構和支援：概觀和更新	檢視：[概觀和更新] 頁面/索引標籤	允許
	檢視：概觀和更新詳細資料	允許
	啟用/停用：線上更新狀態	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
	檢視詳細資料/開始升級：線上更新	允許
	檢視：離線更新	允許
	上傳：離線服務包	允許
	檢視：系統健全狀況	允許
	檢視：平台虛擬機器	允許
	建立叢集	允許
	下載：支援服務包	允許
	檢視：收集器虛擬機器	允許
	新增/編輯/刪除：收集器虛擬機器	允許
[設定] 基礎結構和支援：支援	檢視：[支援] 頁面/索引標籤	允許
	檢視：產品支援詳細資料	允許
	啟用/停用：支援通道	允許
	檢視：客戶經驗改進計劃	允許
	編輯：客戶經驗改進計劃	允許
	建立：支援服務包	允許
	下載：支援服務包	允許
[設定] 範本	檢視：[範本] 頁面/索引標籤	允許
[設定] 範本：內容範本	檢視：[內容範本] 頁面/索引標籤	允許
	檢視：現有內容範本	允許
	複製/編輯/刪除：現有內容範本	允許
[設定] 範本：應用程式探索範本	檢視：[應用程式探索範本] 頁面/索引標籤	允許
	檢視：現有的應用程式探索範本	允許
	複製/編輯/刪除：現有的應用程式探索範本	允許
[儀表板] 計劃與評估	檢視：[計劃與評估] 索引標籤	允許
[儀表板] 計劃與評估：安全性計劃	檢視：[安全性計劃] 頁面 (微分割、流量分佈、依位元組數排序的前幾個連接埠)	允許
	分析：安全性計劃	允許
	釘選 Widget	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
	評估報告	允許
	同心圓/清單視圖：微分割	允許
	匯出為 CSV	允許
[儀表板] 計劃與評估：PCI 合規性	檢視：[PCI 合規性] 頁面/索引標籤	允許
	評估：PCI 合規性	允許
	釘選 Widget/建立通知	允許
	匯出 CSV/PDF	允許
	說明	允許
[儀表板] 計劃與評估：應用程式	檢視：[應用程式] 頁面/索引標籤	允許
	新增：應用程式	允許
	編輯/刪除：現有應用程式	允許
	匯出	允許
應用程式探索	檢視：[探索] 索引標籤	允許
	探索應用程式	允許
[儀表板] 分析	檢視：[分析] 頁面/索引標籤	允許
[儀表板] 分析：極端值	檢視：[極端值] 頁面/索引標籤	允許
	檢視：現有極端值組態	允許
	新增/編輯/刪除：現有極端值組態	允許
	啟用/停用：現有極端值組態	允許
	釘選 Widget	允許
[儀表板] 分析：臨界值	檢視：[臨界值] 頁面/索引標籤	允許
	檢視：現有臨界值組態	允許
	新增/編輯/刪除：現有臨界值組態	允許
	啟用/停用：現有臨界值組態	允許
	釘選 Widget	允許
[儀表板] 分析：Flow Insights	檢視：[Flow Insights] 頁面/索引標籤	允許
	分析：Flow Insights	允許
	釘選 Widget	允許

表 6-7. 每個角色支援的功能 (續)

頁面	動作	管理員
	匯出為 CSV/最大化/說明	允許
已儲存的搜尋	檢視：預設已儲存的搜尋	允許
	新增/刪除：新增已儲存的搜尋	允許

新增本機使用者

vRealize Network Insight 可讓您新增使用者並為每個使用者指派角色。

程序

- 1 在 vRealize Network Insight **設定**頁面中，展開**身分識別與存取管理**。
- 2 按一下**使用者管理**，然後選取 VMware Identity Manager [使用者] 索引標籤。
- 3 按一下**新增使用者**並提供所需的詳細資料。

內容	說明
名稱	輸入使用者的名稱。
電子郵件 (登入識別碼)	輸入電子郵件或登入識別碼 (如果有)。
角色	從下拉式清單中選取角色。
密碼	輸入密碼。
重新輸入新密碼。	重新輸入密碼以進行確認。

- 4 按一下**新增使用者**以儲存使用者資訊。

為 LDAP 使用者指派角色

您可以為任何 LDAP 使用者指派角色，以允許其存取 vRealize Network Insight。

必要條件

設定輕量型目錄存取通訊協定 (LDAP)

程序

- 1 在 vRealize Network Insight **設定**頁面中，展開**身分識別與存取管理**。
- 2 按一下**使用者管理**，然後選取 **LDAP 使用者**索引標籤。
- 3 按一下**新增使用者**。
- 4 提供您要為其指派角色之使用者的登入識別碼。
- 5 從清單中選取角色。如需詳細資料，請參閱**設定使用者管理**。
- 6 按一下**新增使用者**。

設定輕量型目錄存取通訊協定 (LDAP)

若要允許 LDAP 使用者登入 vRealize Network Insight，則必須在 vRealize Network Insight 平台中設定 LDAP 服務。

必要條件

您必須具有**管理員**權限。

程序

- 1 登入 vRealize Network Insight，然後按一下**設定**。
- 2 在**身分識別與存取管理**下，選取 **LDAP**。
- 3 按一下**設定**。
- 4 提供下列資訊。

欄位	說明
網域	輸入網域名稱。這通常是使用者電子郵件地址中「@」符號後的最後一部分。範例：對於以 johndoe@example.com 登入的使用者，則此欄位為 example.com
LDAP 主機 URL	輸入主機名稱。您可以指定多個 LDAP 主機 URL，並以逗號分隔。
以群組為基礎的存取控制	<p>選取此選項可設定群組，並為該群組的成員提供角色。</p> <ol style="list-style-type: none"> a 在基本 DN下，輸入基本 DN，即伺服器開始搜尋使用者的位置。 b 提供搜尋屬性。 c 在群組 DN下，為每個群組選取使用者角色。 <p>如果為特定群組選取管理員角色，則該群組的所有成員都具有管理員權限。同樣地，如果為特定群組選取成員角色，則該群組的所有成員都具有成員權限。如果未選取此選項，則會使用群組設定指派權限。但是，不屬於您所新增群組的其他有效 LDAP 使用者也可以登入產品。</p> <ol style="list-style-type: none"> d 按一下新增更多以在包含清單中新增群組。 e 選取僅限上述群組的成員存取選項，僅允許已新增的 LDAP 群組中的使用者 (直接或繼承的成員資格) 存取。
使用者名稱	具有使用所提供設定進行登入所需權限的使用者。
密碼	使用者的密碼。

- 5 按一下**提交**。

設定之後，將會顯示您已設定的 **LDAP** 詳細資料。

從 VMware Identity Manager 匯入使用者

您可以匯入 VMware Identity Manager 使用者帳戶，以允許他們使用 vRealize Network Insight 並為其指派角色。

必要條件

[設定 VMware Identity Manager](#)。

程序

- 1 在 vRealize Network Insight **設定**頁面中，展開**身分識別與存取管理**。
- 2 按一下**使用者管理**，然後選取 VMware Identity Manager [使用者] 索引標籤。
- 3 按一下**新增使用者**並提供所需的詳細資料。

欄位名稱	說明
網域名稱	輸入要匯入的 VMware Identity Manager 網域名稱。
搜尋使用者/群組	輸入搜尋字串，然後從自動完成清單中選取使用者帳戶。您可以選取單一使用者，也可以選取使用者群組。如果您選取某個群組，則該群組中的所有成員皆可存取 vRealize Network Insight。
角色	為使用者帳戶指派角色。如需詳細資料，請參閱 設定使用者管理 。

- 4 按一下**新增使用者**。

備註

- 如果您已選取某個群組，則該群組中的所有成員會獲得相同的角色。如果您要將不同的角色指派給群組中的特定使用者，則必須單獨新增該使用者，並指派所需的角色。

例如，將**管理員**角色僅指派給 *Mygroup* 中的 *user1*：

- 新增 *Mygroup* 並指派**成員**角色，以及
- 新增 *user1* 並指派**管理員**角色。

指派給使用者的角色會直接覆寫指派給屬於某個群組的使用者的角色。

- 如果使用者屬於多個具有不同角色的群組，則會將最高權限角色指派給該使用者。

例如，如果使用者屬於具有**管理員**角色的群組 *A*，且同時屬於具有**成員**角色的群組 *B* 和群組 *C*，則使用者會繼承**管理員**角色。

結果

現在，此 VMware Identity Manager 使用者或群組成員可以登入 vRealize Network Insight，並根據指派的角色使用功能。

設定 VMware Identity Manager

管理員可以根據使用者的角色為 VMware Identity Manager 使用者提供存取 vRealize Network Insight 功能的授權。

必要條件

向 VMware Identity Manager 主機登錄 vRealize Network Insight 作為 OAuth 用戶端。如需詳細資訊，請參閱 [VMware Workspace ONE Access 說明文件](#)。

程序

- 1 登入 vRealize Network Insight，然後按一下**設定**。
- 2 在 [身分識別與存取管理] 下，選取 VMware Identity Manager。

- 3 按一下**設定**。
- 4 提供下列資訊。

參數	說明
VMware Identity Manager 應用裝置	VMware Identity Manager 主機的完整網域名稱 (FQDN)。
OAuth 用戶端識別碼	向 VMware Identity Manager 主機登錄 vRealize Network Insight 時建立的識別碼。
OAuth 用戶端密碼	向 VMware Identity Manager 主機登錄 vRealize Network Insight 時建立的密碼。
SHA-256 指紋	可視情況選填。VMware Identity Manager 主機的憑證指紋。如需詳細資訊，請參閱 從 VMware Identity Manager 主機取得憑證指紋 。

- 5 按一下**提交**。

設定之後，將會顯示 VMware Identity Manager 應用裝置和您已設定的用戶端詳細資料。

- 6 按一下切換按鈕以啟用或停用 VMware Identity Manager。如果停用，則無法在 vRealize Network Insight 中使用 VMware Identity Manager 驗證。

從 VMware Identity Manager 主機取得憑證指紋

對於 SSL 憑證驗證，您可以從 VMware Identity Manager 主機取得 SHA-256 指紋。

程序

- 1 若要取得 SSL/TLS 憑證，請執行下列命令：

```
openssl s_client -connect <FQDN of vIDM host>:443
```

將伺服器憑證 (從 -----BEGIN CERTIFICATE----- 開始到 -----END CERTIFICATE-----) 複製到名為 cert.pem 的檔案，然後儲存該檔案。

- 2 若要取得指紋，請執行下列命令：

```
openssl x509 -fingerprint -noout -sha256 -in cert.pem
```

結果

將會顯示下列格式的指紋：

SHA256

Fingerprint=3D:E8:4C:CD:19:D6:AD:23:30:86:E4:A1:72:D5:22:08:F9:72:6D:D3:E7:6E:99:32:C8:C7:3D:F8:E2:91:91:AE

後續步驟

複製指紋，並將其貼到 [設定 VMware Identity Manager] 頁面中。

設定記錄

在 vRealize Network Insight 中，您可以檢視和設定不同類型的記錄。

檢視和匯出稽核記錄

稽核記錄擷取在系統中執行的管理動作。它們是一般的 CRUD 作業，以及登入和登出事件。將記錄透過使用者介面、CLI 或 API 執行的管理動作。

稽核記錄從 API、UI 和 CLI 擷取動作。

功能

- 稽核記錄功能永遠處於開啟狀態。
- vRealize Network Insight 在稽核記錄中支援 UTC 格式。
- 稽核記錄會與 Syslog 整合。您可以將 Syslog Collector 設定為收集所有稽核記錄。
- 您可以在 CSV 檔案中匯出所有稽核記錄資料。

設定 Syslog 組態

您可以使用 **Syslog 組態** 頁面為 vRealize Network Insight 設定遠端 syslog 伺服器。

雖然每個 Proxy 伺服器可能具有不同的遠端 syslog 伺服器，但叢集中的所有平台伺服器都使用相同的遠端 syslog 伺服器。

在目前版本中，vRealize Network Insight 問題事件和平台/Proxy 伺服器 Syslog 會傳送到遠端 Syslog 伺服器。

目前，vRealize Network Insight 僅對 vRealize Network Insight 伺服器與遠端 syslog 伺服器之間的通訊支援 UDP。因此，請確保您的遠端 syslog 伺服器設定為接受透過 UDP 的 syslog 流量。

設定 syslog：

- 1 在**設定**頁面中，按一下 **Syslog 組態**。**Syslog 組態** 頁面會列出您組態的 syslog 伺服器及其至虛擬應用裝置的對應。如果您是第一次存取此頁面，則依預設會停用 syslog，且不會此頁面上顯示伺服器清單。
- 2 新增 syslog 伺服器：
 - a 按一下**新增 Syslog 伺服器**。
 - b 輸入伺服器的 IP 位址、暱稱和連接埠號碼。用於 UDP 的標準連接埠號碼為 514。
 - c 若要測試組態，請按一下**傳送測試記錄**。
 - d 按一下**提交**。
 - e 如果這是您新增的第一個伺服器，則在頁面頂端啟用 syslog。
- 3 將伺服器對應至平台和 Proxy：
 - a 按一下**編輯對應**。
 - b 為所有平台和代理程式伺服器選取該 syslog 伺服器。
 - c 如果您不想在任何 Proxy 伺服器或平台上啟用 syslog，請選取**無伺服器**選項。

- d 按一下**提交**。

備註 進行變更後，可能需要幾分鐘才能使這些變更生效。

設定郵件伺服器

在 vRealize Network Insight 中，您可以將郵件伺服器設定為透過郵件接收事件通知。

設定郵件伺服器：

- 1 在首頁的右上角，按一下**設定檔**圖示，然後按一下**設定**。
- 2 按一下**郵件伺服器**。
- 3 選取 [SMTP 伺服器] 核取方塊。
- 4 在方塊中輸入適當的值。

表 6-8.

欄位	說明
寄件者電子郵件	寄件者電子郵件地址。
SMTP 主機名稱/IP 位址	SMTP 伺服器的主機名稱或 IP 位址。
加密	下列加密選項可用：無、TLS 和 SSL。
SMTP 連接埠號碼	SMTP 伺服器的連接埠號碼 (預設值為 25)。

備註 若要將 Gmail 伺服器用作選擇的電子郵件伺服器，則需要 Google 支援上列出的其他組態設定。

(選用) 若要增強安全性，請選取 [驗證] 核取方塊，然後輸入使用者名稱和密碼。

備註 若要確認通知郵件是否已正確設定，請按一下**傳送測試電子郵件**。

- 5 按一下**提交**以完成組態。

設定 SNMP 設陷目的地

在 vRealize Network Insight 中，您可以設定最多四個簡易網路管理通訊協定 (SNMP) 設陷代理程式以接收通知。產品支援 SNMP 的 v2c 和 v3 版本：

- 1 在**設定**頁面中，依序按一下 **SNMP 設陷目的地** > **新增目的地**。
- 2 在**新增 SNMP 設陷目的地**頁面的**版本**下拉式方塊中，選取 **SNMPv2c** 或 **SNMPv3** 通訊協定。

備註 SNMP v2c 通訊協定不需要驗證。SNMP v3 通訊協定支援驗證。

- 3 在**目的地 IP 位址 / FQDN**文字方塊中，輸入 SNMP 代理程式的 IP 位址或完整網域名稱 (FQDN)。
- 4 在**目的地連接埠**文字方塊中，輸入 SNMP 代理程式的連接埠號碼。

- 5 根據您選取的 SNMP 版本，執行下列其中一項：

選項	動作
對於 SNMP v2c	在 社群字串 文字方塊中，輸入社群字串。
對於 SNMP v3	<ol style="list-style-type: none"> 1 在使用者名稱文字方塊中，輸入您在 SNMP 代理程式中建立的使用者的名稱。 2 (選擇性) 選取使用驗證核取方塊。 3 (選擇性) 選取驗證通訊協定，然後輸入 SNMP 代理程式中為特定使用者設定的密碼。 4 (選擇性) 選取使用隱私核取方塊，然後分別選取隱私通訊協定和輸入隱私片語。

- 6 在**暱稱**欄位中，輸入暱稱。
- 7 (選擇性) 若要確認是否已正確設定完成，請按一下**測試 SNMP 設陷**，然後檢查設陷是否已傳送到 SNMP 代理程式。
- 8 按一下**提交**。

刪除 SNMP 設陷目的地

您可以從 vRealize Network Insight 中刪除 SNMP 設陷目的地。如果您有多個 SNMP 設陷目的地，則刪除某個 SNMP 設陷目的地時，可以將與此設陷目的地相關的所有通知移轉到另一個可用的設陷目的地。

程序

- 1 按一下您要刪除的設陷目的地旁邊的**刪除**圖示。
確認動作快顯視窗隨即開啟。
- 2 如果您想要將事件從目前設陷目的地移轉到其他設陷目的地，請按一下**選取多個目的地**下拉式清單，然後選取要將事件移轉到的設陷目的地。
- 3 按一下**確認**。

管理授權

VMware 遵循 vRealize Network Insight 授權的榮譽系統，這意味著出現任何授權計數違規時，都會在使用者介面中顯示警告訊息，但不限制您使用可用的功能。

在下列情況下，您會在使用者介面的所有頁面上看到授權警告訊息：

- 超過了通訊端 (CPU) 授權的授權使用量。
您必須新增額外授權以支援您的需求。
- 混合授權類型
 - 當您同時新增了進階授權和企業授權時。
從進階版本升級至企業版本之後，您必須手動刪除進階授權 (**設定 > 授權和使用量**)。請確保您有足夠數目的企業授權以使用企業功能。

- 當您新增了通訊端授權與核心授權時。
根據您的需求刪除其中一個授權類型。

授權使用量計算

vRealize Network Insight 授權使用量是根據下列比率進行計算的。

物件	說明	每個通訊端授權允許的物件計數
VMware vSphere CPU	內部部署主機的 CPU 通訊端的總數	1
VMware Cloud on AWS 主機	VMware Cloud on AWS 主機總數。	0.5 備註 One VMC host requires two socket licenses.
AWS 或 Azure vCPU	AWS 執行個體或 Azure 的 vCPU 總數	16
非 VMware 端點	出現在專門由非 VMware 流量報告功能 (例如, 來自實體交換器的 NetFlow) 報告的流量中的非網際網路和非 VMware 端點的總數	15

備註 vRealize Network Insight 也會在授權使用量計算期間考量停用的資料來源。如果您希望 vRealize Network Insight 在計算期間忽略它們, 則刪除資料來源。

SD-WAN 授權

若要將 VMware SD-WAN 新增為資料來源, 並在 vRealize Network Insight 中檢視 VMware SD-WAN 部署, 您必須新增 VMware SD-WAN 授權。您可以將 VMware SD-WAN 授權新增為獨立授權, 也可以將其與 Enterprise 授權搭配使用。但是, 您無法將 VMware SD-WAN 授權與進階授權搭配使用。您可以使用多個 VMware SD-WAN 授權金鑰來支援不同頻寬的 Edge。

透過新增至 VMware SD-WAN 資料來源的 VMware SD-WAN 授權, 您也可以新增不含 IPFIX、交換器和路由器以及 Infoblox 的 vCenter。

根據授權版本比較功能

vRealize Network Insight 功能會因您使用的授權而有所不同。

下表顯示了 vRealize Network Insight 所提供的各個授權之間的功能比較：

功能	進階授權	企業授權	雲端服務	SD-WAN 內部部署	SD-WAN SKU (雲端服務)
虛擬流量 (VDS IPFIX、V2V、V2P)	是	是	是	否	否
NSX 防火牆微分割規劃和作業 (NSX IPFIX)	是	是	是	否	否
跨第三方交換器、路由器、防火牆和負載平衡器的可見度	是	是	是	否	否

功能	進階授權	企業授權	雲端服務	SD-WAN 內部部署	SD-WAN SKU (雲端服務)
公用 API	是	是	是	否	否
DNS 對應 (匯入繫結檔案)	是	是	是	否	否
[NSX PCI 合規性] 儀表板	否	是	是	否	否
VMware Cloud on AWS 的安全性計劃與可見度	否	是	是	否	否
AWS 和 Azure 的安全性計劃和可見度	否	是	是	否	否
使用 Infoblox 的 DNS 解析	否	是	是	否	否
實體流量 (NetFlow v7 和 v9 , 以及 sFlow)	否	是	是	否	否
VMware Enterprise PKS、Kubernetes 和 OpenShift 的可見度	否	是	是	否	否
網路與安全性分析 (通訊最多者、異常、極端值偵測等)	否	是	是	否	否
資料的可設定和延長保留期間	否	是	是	否	否
Cisco ACI、BGP-EVPN 底層可見度	否	是	是	否	否
[應用程式探索] 儀表板 (名稱、標籤、RegEx)	是	是	是	否	否
用於應用程式探索的 ServiceNow 整合	否	是	是	否	否
以流量為基礎的應用程式探索	否	否	是	否	否
VMware Cloud on AWS Direct Connect	否	是	是	否	否
VMware SD-WAN by VeloCloud	否	否	否	是	是
vRealize Operations Manager 整合	是	是	是	否	否

新增並變更授權

若要查看授權使用量計數並檢視其詳細資料，請在 [授權和使用量] 頁面上，按一下每個實體計數的相應連結。您也可以透過此頁面新增和變更授權類型。vRealize Network Insight 支援新增多個授權。

新增授權

新增授權：

- 1 在 [授權和使用量] 頁面上，按一下**新增授權**。

- 2 為**新授權金鑰**欄位提供授權金鑰。
- 3 按一下**驗證**。
將會顯示授權類型、授權提供的通訊端或核心計數，以及到期詳細資料。
- 4 按一下**啟動**。
- 5 可以在頁面中看到授權清單。
- 6 您也可以透過按一下 [到期] 資料行旁邊的刪除圖示來刪除授權。如果授權屬於企業版，且這是系統中保留的最後一個企業版，則在刪除該企業授權之前，請確保已刪除 AWS 帳戶。

變更授權

如果評估授權到期，則登入產品時會顯示一則訊息，指出授權已到期，需要更新授權。使用下列步驟來變更授權。

變更授權：

- 1 按一下 [到期] 訊息中包含的連結以前往 [變更授權] 頁面。或者，在**設定**中，按一下**授權和使用量**，然後按一下**變更授權**。
- 2 在**變更授權**頁面的**新授權金鑰**中，輸入從 VMware 收到的新授權金鑰。
- 3 按一下**驗證**。
- 4 按一下**啟動**。

備註 評估授權到期後，將會停用資料提供者，並停止收集資料。更新授權後，必須從使用者介面重新啟用資料提供者才能啟動資料收集。

設定自動重新整理間隔

在 vRealize Network Insight 中，您可以設定實體頁面和看板的自動重新整理間隔。

vRealize Network Insight 提供適用於實體儀表板和看板的自動重新整理功能。此儀表板會以標頭列上指定的每 n 分鐘自動重新整理一次。

您可以指定希望所有儀表板執行自動重新整理的時間間隔。在指定的時間間隔 (n 分鐘) 後，儀表板上所有開啟的 Widget 將會自動重新載入。

備註

- 您無法變更特定儀表板的自動重新整理時間間隔。
 - 如果您在時間表滑桿中選取過去的時間間隔，則會暫停自動重新整理。
-

如果特定的儀表板不需要自動重新整理，則可以將其暫停。在標頭列上，將**暫停**設定為**開啟**。將**暫停**設定為**關閉**後，自動重新整理計數器便會重設。

如果您正在檢視看板，而另一位使用者在對其進行變更，例如變更看板的配置，則自動重新整理功能不僅會更新內容，還會重新整理整個看板。只有在您和其他使用者之間存在共用和協作時才會發生這種情況。

程序

- 1 在**設定**頁面上，按一下**我的喜好設定**。或在相應的儀表板中，按一下標頭列中 [自動重新整理] 旁邊的**修改**。
- 2 按一下**編輯**以變更自動重新整理的時間間隔。從下拉式功能表中選取時間間隔。按一下**儲存**。
- 3 若要停用自動重新整理選項，請從下拉式功能表中選取**已停用**。如果您選取此選項，所有儀表板會自動停用重新整理。

設定使用者工作階段逾時

依預設，使用者工作階段逾時設定為 15 分鐘。您可以根據喜好設定修改此值。

程序

- 1 在**設定**頁面上，按一下**系統組態**。

備註 系統組態索引標籤僅對 admin user 可見。

- 2 按一下**編輯圖示**，以變更使用者工作階段逾時的喜好設定。
- 3 拖曳滑桿列以設定工作階段的逾時值。此值的範圍是從 15 分鐘到 24 小時。
- 4 您也可以在上次**修改欄位**中檢視有關逾時值修改者和時間的詳細資料。
- 5 按一下**提交**。將顯示成功訊息，確認更新的工作階段持續時間將從下次登入時生效。

備註 只有在您先登出再重新登入後，使用者工作階段逾時的新值才會生效。

新增 Google 地圖 API 金鑰

若要取得 SD-WAN 部署的對應視圖，您必須在 vRealize Network Insight 中新增 Google 地圖 API 金鑰。

必要條件

請確保：

- 您是 Google Cloud Platform 的成員，且已在您的帳戶中啟用計費。
- 您有 Google 地圖 API 金鑰。若要取得 API 金鑰，請參閱 Google Maps Platform 說明文件中的「取得 API 金鑰」程序。
- 您已限制 API 金鑰以防止任何誤用情形。若要瞭解詳細資訊，請參閱 Google Maps Platform 說明文件中的「限制 API 金鑰」。

程序

- 1 在**設定**頁面上，按一下**系統組態**。
- 2 在**Google 地圖 API 金鑰**中，輸入 API 金鑰，然後按一下**儲存**。

設定資料來源憑證驗證

當您在 vRealize Network Insight 中新增資料來源時，會自動新增與該資料來源相關的所有憑證 (HTTPS 憑證或 SSH 公開金鑰)，以供第一次使用時信任。在 vRealize Network Insight 中新增資料來源後，每當憑證有任何變更時，系統都會驗證該憑證。

您可以使用兩種方式來設定憑證驗證：**自動接受**和**手動接受**。在**自動接受**中，系統會自動接受所有偵測到的憑證變更，而在**手動接受**中，系統會停止資料來源，並向您顯示手動接受憑證的警示訊息通知。當您接受憑證時，系統會啟動資料來源。

程序

- 1 移至**設定 > 系統組態**。
- 2 從**資料來源憑證驗證**下拉式功能表中，選取其中一個資料來源驗證方法：
 - **自動接受**
 - **手動接受**
- 3 按一下**儲存**。

備註 如果將憑證驗證方法從**手動接受**變更為**自動接受**，您必須手動接受所有可用的憑證變更，然後才能變更憑證驗證方法。

如果您將**資料來源憑證驗證**從**手動接受**變更為**自動接受**，但未接受擱置中偵測到的憑證變更，則必須刪除含有擱置中憑證的所有資料來源，然後再次新增這些資料來源以取得有關這些資料來源的深入資訊。

手動接受資料來源憑證

如果您已將**資料來源憑證驗證**設定為**手動接受**，則必須針對系統偵測到憑證變更的每個資料來源接受新憑證 (HTTPS 憑證或 SSH 公開金鑰)。

如果您已將**資料來源憑證驗證**設定為**手動接受**，則每當 vRealize Network Insight 偵測到憑證中有任何變更時，您都會看到警示訊息通知。您也可以**在帳戶和資料來源頁面中查看憑證變更警示**。使用此程序接受憑證。

程序

- ◆ 在**資料來源憑證更新可用**警示訊息通知中，按一下**檢閱**。

如果可用的憑證更新數目最多為兩個：	a 您會看到 資料來源憑證 視窗中顯示目前憑證和新憑證的詳細資料。 b 檢閱新憑證，然後按一下 接受 。
如果可用的憑證更新數目超過兩個：	a 在 帳戶和資料來源 頁面中，有憑證更新可用的資料來源下會顯示 <div style="background-color: #f2f2f2; padding: 5px; margin: 5px 0;">憑證更新可用。按一下此處以檢閱並接受</div> 訊息。 b 對於要檢閱並接受更新憑證的資料來源，按一下 按一下此處以檢閱並接受 。 c 您會看到 資料來源憑證 視窗中顯示目前憑證和新憑證的詳細資料。 d 檢閱新憑證，然後按一下 接受 。

結果

當您接受新憑證時，將會顯示已成功更新憑證訊息。

檢視稽核記錄。

稽核記錄擷取在系統中執行的管理動作。這些動作是一般的 CRUD 作業，以及登入和登出事件。稽核記錄從 API、UI 和 CLI 擷取動作。

- 稽核記錄功能永遠處於開啟狀態。
- vRealize Network Insight 在稽核記錄中支援 UTC 格式。
- 稽核記錄會與 Syslog 整合。您可以將 Syslog Collector 設定為收集所有稽核記錄。
- 您可以在 CSV 檔案中匯出所有稽核記錄資料。

目前，稽核記錄不會擷取下列管理動作：

- SSH 登入記錄。您可以在 `/var/log/auth.log` 中找到 SSH 記錄。
- [實體 IP 和 DNS 對應] 中的變更。
- [實體子網路和 VLAN] 中的變更。

程序

- 1 在**設定**頁面上，按一下**記錄**下的**稽核記錄**。
- 2 在**稽核記錄**頁面上會顯示下列詳細資料：

資訊	說明
Date & Time	執行實際的動作的時間戳記。
IP Address	從其建立連線的用戶端 (例如 CLI 或瀏覽器) 的 IP 位址。
User Name	正在執行動作的使用者。

資訊	說明
Object Type	正在對其執行動作的物件。
Operation	使用者對物件執行的不同的動作。
Object Identifier	對其執行動作的物件的唯一識別碼。
Response	作業成功或失敗的指示器
Details	已變更的設定的詳細資料，例如暱稱或內容。

- 3 若要在使用者透過瀏覽器或 CLI 登入時允許收集資訊，請啟用**允許收集個人識別資訊**。此選項依預設為停用。

備註 如果停用此選項，則 IP Address 和 User Name 資料行為空白。

- 4 按一下**匯出為 CSV**以 CSV 格式匯出稽核記錄資料。

加入或退出客戶經驗改進計劃

此產品會參與 VMware 客戶經驗改進計劃 (CEIP)。CEIP 為 VMware 提供能讓其改進產品與服務、修正問題的資訊，並就如何以最佳方式部署和使用我們的產品為您提供建議。做為 CEIP 的一部分，VMware 會結合貴組織的 VMware 授權金鑰，定期收集貴組織使用 VMware 產品和服務的相關技術資訊。此類資訊不會單獨識別任何個人身分。

關於透過 CEIP 收集的資料以及 VMware 對資料的使用用途等詳細資訊，將於 Trust & Assurance Center 予以說明，網址為 <https://www.vmware.com/solutions/trustvmware/ceip.html>。

您可以加入或退出 vRealize Network Insight 的客戶經驗改進計劃 (CEIP)。

- 1 在**關於**頁面中的 [客戶經驗改進計劃] 下，按一下**修改**。
- 2 將快顯 CEIP 視窗。若要加入 CEIP，請勾選**啟用**。此動作將會啟動 CEIP，並傳送資料至 <https://vmware.com>。
- 3 若要離開 CEIP，請取消勾選**啟用**。
- 4 按一下**提交**。

檢視設定的健全狀況

健全狀況指示器位於**安裝和支援**頁面上的**概觀**區段中。

如果出現下列任何錯誤事件，**健全狀況**指示器會變成紅色：

- Proxy 停止收集流程資料
- 平台出於任何原因 (例如，磁碟空間不足) 停止處理資料
- 搜尋索引子延遲，導致搜尋結果到期

整體健全狀況指示器顯示異常數目，紅燈亮起。按一下有關整體健全狀況的問題數目時，會列出個別異常及其詳細資料。正常運作時，健全狀況指示器發出綠光。

備註 vRealize Network Insight 有時可能無法偵測到不同步的系統時鐘。如果時鐘未與 NTP 同步，某些服務可能會狀況不良或停止運作。

啟用支援通道

支援通道允許 VMware 在受 SSL 保護的連線上從遠端連線至平台和收集器虛擬機器，以進行進階疑難排解或偵錯。



若要要求進階支援，請切換**安裝與支援**頁面之**概觀**區段中的**支援通道**選項。

備註 請確保允許到連接埠 443 上 support2.ni.vmware.com 的流量。

管理磁碟使用率

如果平台或收集器的磁碟使用率很高，則會觸發事件以警告使用者。此外，還會提供需要額外新增多少磁碟空間的建議。您可以在平台或收集器儀表板中檢視事件。警示也會顯示在**安裝與支援**頁面的相應收集器或平台區段中。

Platform VMs

IP Address (Name)	Last Activity	Status
<div> <div></div> <div>(vrni-platform)</div> <div>  Critical: Disk Utilization is high  </div> </div>		<div> <p>Disk utilization is at 85%. The Platform might run out of disk in 2 days. Add 100 GB more disk space to avoid any service interruption.</p> </div>

您可以透過執行下列步驟將磁碟新增到節點：

備註 請勿擴充現有硬碟。

程序

- 1 使用足夠的權限透過 Web 用戶端登入 vCenter。
- 2 在節點上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 根據警示中提供的建議新增硬碟。

vRealize Network Insight 需要幾分鐘的時間來偵測應用裝置並將其新增至 `/var` 磁碟分割。

檢視節點詳細資料

您可以檢視平台或收集器中每個節點的詳細資料。

程序

- 1 若要檢視特定平台節點的詳細資料，請按一下在**安裝與支援**頁面上**平台虛擬機器**中所列的名稱。
此時將顯示 NI 平台儀表板。
- 2 若要檢視特定收集器節點的詳細資料，請按一下**安裝與支援**頁面上**收集器 (Proxy) 虛擬機器**中所列的名稱。
此時將顯示 NI 收集器儀表板。

建立支援服務包

您可以建立支援服務包以收集診斷資訊，例如，特定於產品的記錄、您的安裝程式的組態檔。當您提高支援請求時，VMware 技術支援將使用此資訊對設定問題進行疑難排解。

程序

- 1 在 [設定] 頁面上，按一下**安裝與支援**。
- 2 按一下**建立支援服務包**。
- 3 選取您要為其建立支援服務包的平台虛擬機器和收集器虛擬機器。
若要選取所有虛擬機器，則按一下平台虛擬機器和收集器虛擬機器資料表的標頭中的核取方塊。
- 4 按一下**建立**。
- 5 按一下**是**以確認建立新的支援服務包。

vRealize Network Insight 需要一些時間來完成建立服務包。

結果

將建立一個顯示日期和時間的新支援服務包。若要啟動支援服務包下載，請按一下相應虛擬機器旁邊的**下載連結**。

備註

- 在中型系統上建立支援服務包可能需要超過 15 分鐘。
 - 在一個指定的時間只能存在兩個支援服務包。因此，在建立新的支援服務包時，如果已有兩個支援服務包，則系統會刪除較舊的支援服務包。
-

後續步驟

將支援服務包連結到 VMware 的服務要求以存取詳細資料。

瞭解收集器和平台負載的容量

vRealize Network Insight 提供了收集器節點和平台的近似容量和負載資訊。基於限制的此資訊可協助您稍後防止效能和體驗問題。

瞭解容量

有以下兩種容量：

- 虛擬機器容量：其定義為節點或設定可以處理的已探索到虛擬機器的數目。
- 流程容量：其定義為節點或設定可以處理的流程數目。

容量定義如下：

- 具有一或多個 Proxy 節點的單一平台：Proxy 節點或平台的容量是它可以處理但不會降低效能的已探索到虛擬機器的數目。
- 叢集設定：叢集設定中平台的容量是所有平台節點的所有容量的彙總，而 Proxy 節點的容量是在個別節點層級上進行考慮。

存取容量資訊

您可以在**安裝與支援**頁面上檢視**虛擬機器容量**和**流程容量**。

針對收集器 (Proxy) 虛擬機器下所列的每個收集器節點，僅提供虛擬機器容量資訊。

備註 當整個部署過程中從資料來源探索到的虛擬機器數目超過系統和/或收集器的容量時，不允許您觸發升級。

檢視資料來源的探索到的虛擬機器：

- 1 在**帳戶和資料來源**頁面中，您可以查看已新增且目前處於作用中狀態的特定資料來源的已探索到虛擬機器的數目。僅在資料來源為 vCenter 或 AWS 來源時，此資料行才有值。

備註 已探索到虛擬機器的計數包含預留位置虛擬機器和範本虛擬機器。因此，它可以不同於產品中的虛擬機器計數。

vRealize Network Insight 中的 Direct Connect 支援

7

Direct Connect 是一種在內部部署位置與公有雲服務之間提供資料傳輸連線的機制。從 5.2 版本開始，vRealize Network Insight 支援 VMware Cloud on AWS 的 Direct Connect 功能。

Direct Connect 支援讓您能夠：

- 識別透過 Direct Connect 在內部部署資料中心與 VMware Cloud on AWS SDDC 之間傳遞的流量。
- 執行流量分析以瞭解流量頻寬和封包速率。
- 檢視透過 Direct Connect 進行通訊的虛擬機器之間的詳細路徑拓撲。
- 檢視有關 Direct Connect 和相關聯事件的詳細資料。

Direct Connect 資料擷取機制

vRealize Network Insight 使用 VMware Cloud on AWS NSX API 擷取 Direct Connect 資訊。因此，您必須新增 VMware Cloud on AWS 相關資料來源 (vCenter 和 NSX Manager)，才能取得 Direct Connect 資訊。

備註 您無須新增 AWS 帳戶或任何其他資料來源，即可支援 Direct Connect。

但是，若要取得路徑拓撲資訊，您必須新增託管路由器，例如 Cisco N9k 和 Cisco ASR 9k (一般路由器)。

Direct Connect 支援收集哪些資料

- VMware Cloud on AWS SDDC 中的 Direct Connect 相關的組態詳細資料。
- Direct Connect 在 SDDC 層級通告和獲知的子網路。
- 與 SDDC 相關聯的 Direct Connect 介面 (VIF) 的組態資訊。

- VMware Cloud on AWS 中的 Distributed Firewall (DFW) 報告的流量。

備註

- 在託管路由器上不需要啟用 NetFlow。
- Direct Connect 不支援以路由為基礎的 VPN。因此，即使您已啟用 [使用 VPN 做為 Direct Connect 的備份] 選項，VPN 備份也會失敗。
- 度量以及通告或獲知的子網路資訊在個別 VIF 層級不可用。

Direct Connect 實體

- VMware Cloud on AWS Direct Connect：這是 vRealize Network Insight 中所有 Direct Connect 實體的父系實體，這會對 VMware Cloud on AWS SDDC 內 Direct Connect 的組態資訊進行建模。
- Direct Connect 介面：這會對 VMware Cloud on AWS 提供的 AWS Direct Connect VIF 資訊進行建模。此實體能夠在 VMware Cloud on AWS 和內部部署資料中心之間交換通告和獲知的路由。

本章節討論下列主題：

- [檢視 VMC Direct Connect 詳細資料](#)
- [檢視透過 Direct Connect 的流量](#)
- [Direct Connect 搜尋查詢](#)

檢視 VMC Direct Connect 詳細資料

您可以根據從 VMware Cloud on AWS 收集的資訊，在 **VMC Direct Connect** 頁面中查看其內容以及與 Direct Connect 相關聯的實體的概觀。

表 7-1. Direct Connect 儀表板

區段	詳細資料
內容	Direct Connect 的主要內容，包括相關聯的 SDDC、本機 ASN、獲知和宣告的路由、失敗的宣告路由。
Direct Connect 介面	與 Direct Connect 相關聯的所有 Direct Connect 虛擬介面的清單
事件	與 Direct Connect 相關聯的事件清單。

檢視透過 Direct Connect 的流量

您可以檢視 Direct Connect 上執行的所有流量的清單，這能夠檢視透過 Direct Connect 的流量。這可協助您分析並瞭解 Direct Connect 的使用率等級。

當您使用 `Flows where connection = Direct Connection_ID` 查詢搜尋時，您會看到透過 Direct Connect 傳遞的流量的清單以及資訊，例如頻寬使用率和特定 Direct Connect 的網路流量速率。更新此行 - 在 [流量類型] 下，您可以查看流量是位於 VPN、Direct Connect 還是混合網路上。

若要僅查看 Direct Connect 流量，您可以執行下列查詢：

```
flows where flow type = Direct Connect group by Connection
```

若要查看每個 Direct Connect 連線上的流量計數及資料量，請執行下列查詢：

```
max(series(sum(Bytes))) of Flows where flow type = Direct Connect and group by Connection
```

若要查看每個 Direct Connect 介面上的流量計數及封包計數，請執行下列查詢：

```
max(series(sum(packets))) of Flows where flow type = Direct Connect and group by Connection
```

如需其他查詢，請參閱 [Direct Connect 搜尋查詢](#)。

Direct Connect 搜尋查詢

您可以在 vRealize Network Insight 中搜尋 VMware Cloud on AWS Direct Connect 和 Direct Connect 介面實體。

表 7-2. 搜尋查詢

說明	查詢
取得可據以篩選資訊的 VMware Cloud on AWS Direct Connect 實體的清單	VMC Direct Connect where
取得 VMware Cloud on AWS Direct Connect 清單視圖	VMC Direct Connect
取得經由 Direct Connect 的資料量上限	max(series(sum(bytes))) of flows where connection = 'Connection-ID' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'
取得經由 Direct Connect 的封包數目上限	max(series(sum(packets))) of flows where connection = 'Connection-ID' and flow type = 'Different Dc' and source vm is set and destination vm is set and flow type = 'Direct Connect'
取得經由 Direct Connect 流向網際網路的封包數目上限	max(series(sum(packets))) of flows where connection = 'Connection-ID' and flow type = 'Destination is internet' and flow type = 'Direct Connect'
取得經由 Direct Connect 流向網際網路的資料量上限	max(series(sum(bytes))) of flows where connection = 'Connection-ID' and flow type = 'Destination is internet' and flow type = 'Direct Connect'

表 7-2. 搜尋查詢 (續)

說明	查詢
取得經由 Direct Connect 的資料中心之間的封包數目上限	<code>max(series(sum(packets))) of flows where connection = 'Connection-ID' and flow type ='Different Dc' and source vm is set and destination vm is set group by Source Dc, Destination Dc and flow type = 'Direct Connect'</code>
取得經由 Direct Connect 的資料中心之間的資料量上限	<code>max(series(sum(bytes))) of flows where connection = '64638-10.63.229.131' and flow type ='Different Dc' and source vm is set and destination vm is set group by Source Dc, Destination Dc and flow type = 'Direct Connect'</code>

vRealize Operations Manager 整合

8

透過 vRealize Operations Manager，您可以查看 vRealize Operations Manager 中的 vRealize Network Insight 警示。此外，您還可以從 vRealize Network Insight 看到 vRealize Operations Manager 中的網路資訊。

vRealize Operations Manager 會使用一組 vRealize Network Insight API，並在 [警示] 儀表板上顯示警示清單。您可以識別警示名稱中含有 `vrni-` 前置詞的 vRealize Network Insight 警示。此外，您還可以查看觸發警示的實體。

如需 vRealize Network Insight API 的清單，請參閱《[vRealize Network Insight API 指南](#)》。

您可以從實體頁面使用在 **VRNI 環境中啟動** 選項，例如虛擬機器、主機、NSX-V 和 NSX-T，您可以檢視特定實體的儀表板。這可讓您查看網路健全狀況和偵錯網路問題。

如需如何將 vRealize Network Insight 與 vRealize Operations Manager 整合的相關資訊，請參閱 [VMware vRealize Operations Management Pack for vRealize Network Insight](#)。如需支援的 vRealize Operations Manager 版本的相關資訊，請參閱《[VMware 產品互通性對照表](#)》。

備註 您必須將 vRealize Operations Manager 使用者新增至 vRealize Network Insight，且使用者必須至少擁有**成員**權限，才能在 vRealize Operations Manager 中使用功能。

建立和擴充叢集

9

本章節討論下列主題：

- [建立叢集](#)
- [擴充叢集](#)

建立叢集

您可以從[安裝與支援](#)頁面建立叢集。

必要條件

需要至少兩個其他平台。應部署其他平台虛擬機器並開啟其電源。

建立叢集

- 1 對於平台虛擬機器，按一下**建立叢集**。
- 2 在**建立叢集**頁面上，輸入下列資訊：
 - **IP 位址**：輸入要新增的平台的 IP 位址。
 - **密碼**：輸入平台虛擬機器的支援使用者密碼。如果尚未變更密碼，請參閱《vRealize Network Insight 安裝指南》中的〈預設登入認證〉一節取得密碼。
- 3 若要繼續新增更多的平台，請按一下**新增更多**，並輸入 IP 位址和支援使用者密碼。
- 4 按一下**提交**。按一下**是**。
- 5 建立叢集後，使用者需要再次登入產品。

備註

- 僅當平台使用大型區塊大小時，才會啟用**建立叢集**選項。所有平台都應採用大型區塊以建立叢集。
 - 在單一節點上啟用遙測功能將會在所有節點上啟用它。
 - 若要擴充叢集，請參閱《vRealize Network Insight 安裝指南》中的〈擴充叢集〉一節。
-

擴充叢集

建立叢集後，您就可以透過新增更多平台節點來擴充叢集。

備註 您必須僅從平台 1 (P1) 節點執行擴充叢集作業。

程序

- 1 在**安裝和支援**頁面上，為**平台虛擬機器**按一下**延伸叢集**。
- 2 在 [延伸叢集] 頁面上已列出屬於叢集一部分的虛擬機器的 IP 位址。若要將一或多個節點新增至現有叢集，請提供節點的 IP 位址和支援使用者密碼。

備註

- 目前，vRealize Network Insight 支援現有叢集中的 10 個節點。達到限制時，就會停用**新增更多**按鈕。
 - 請確保所有新節點皆未佈建且可透過 SSH 進行存取。
 - 在開始擴充叢集之前，請確定已備份現有平台虛擬機器的備份。
-

- 3 按一下**提交**。
將顯示逐步進度。
- 4 叢集延伸連結完成後，會顯示一則指出成功的訊息。
正在進行叢集調整時，應用程式無法用於任何其他動作。

在 vRealize Network Insight 中設定流量

10

本章節討論下列主題：

- 啟用 IPFIX 組態
- 針對實體伺服器的流程支援
- 檢視已封鎖的流程和受保護的流程
- 網路位址轉譯 (NAT)
- VMware Cloud on AWS 種流量
- 建立 VPC 流量記錄
- 將流量記錄從 F5 傳送至 vRealize Network Insight 收集器

啟用 IPFIX 組態

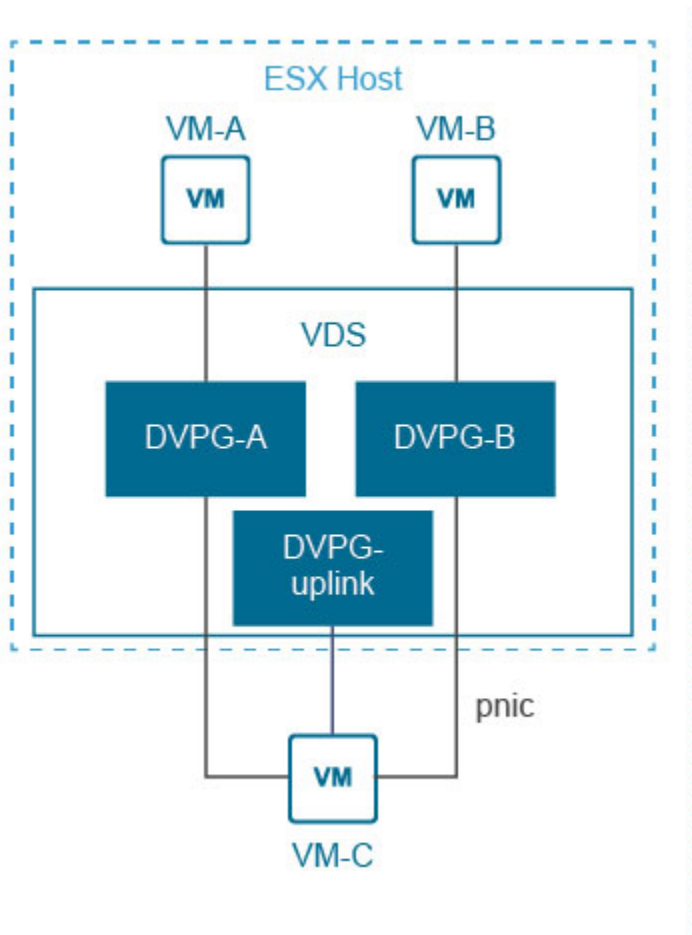
IPFIX 是用於匯出流程資訊的 IETF 通訊協定。

流程定義為在特定期間內傳輸共用相同的 5 元組值 (來源 IP 位址、來源連接埠、目的地 IP 位址、目的地連接埠和通訊協定) 的一組封包。流程資訊可能包含時間戳記、封包/位元組計數、輸入/輸出介面、TCP 徽章、VXLAN 識別碼、封裝的流程資訊等內容。

VDS 和 DVPG 上的 IPFIX 組態

可將 vSphere 環境中的 VDS 設定為使用 IPFIX 匯出流程資訊。必須在連結到 VDS 的所有連接埠群組上啟用流程監控。如果封包到達 VDS 的連接埠 X 並從連接埠 Y 結束，則在連接埠 Y 上啟用流程監控時，便會發出相應的流程記錄。

若要分析任何工作階段的完整資訊，需要這兩個方向的封包的 IPFIX 資料。請參閱下圖，其中 VM-A 連線至 DVPG-A，並與 VM-C 進行通訊。此處 DVPG-A 僅提供有關 C → A 封包的資料，而 DVPG-Uplink 提供有關 A → C 封包的資料。若要取得 A 的完整流量資訊，應在 DVPG-A、DVPG-uplink 上啟用 IPFIX。



vRealize Network Insight Proxy 虛擬機器具有 IPFIX 流程資訊的內建收集器/接收器。您可以在 [vCenter 資料來源] 設定中按不同的粒度層級啟用 IPFIX 資訊收集。

在 VDS 和 DVPG 上啟用 IPFIX 組態

在 vCenter 層級上啟用 IPFIX 資訊：

程序

- 1 在 vRealize Network Insight 中新增 vCenter 時，請選取在此 vCenter 上啟用 NetFlow (IPFIX) 核取方塊。
您會看到所有可用 VDS 的清單。
- 2 從 vCenter 中可用 VDS 的清單中選取要為其啟用 IPFIX 的 VDS。
- 3 對於其中一台主機具有不支援的 ESXi 版本的 VDS，會顯示通知圖示。如果 vRealize Network Insight 偵測到 IPFIX 已為 VDS 設定除 vRealize Network Insight Proxy 虛擬機器以外的其他某個 IP 位址，則會顯示覆寫按鈕。按一下覆寫以檢視該 VDS 下的 DVPG 清單。
- 4 將顯示所選 VDS 的可用 DVPG 清單。依預設會選取所有 DVPG。開啟手動選取來選取要為其啟用 IPFIX 的特定 DVPG。選取所需 DVPG，然後按一下提交。

備註 具有通知圖示的 DVPG 表示它是上行 DVPG，且您必須選取它。

VMware NSX IPFIX 組態

VMware NSX IPFIX 提供與實體裝置所提供類似的網路監控資料，並為管理員提供虛擬網路的明確視圖。

VMware NSX 允許網路管理員將網路與實體硬體中斷連結，從而對網路進行虛擬化。此功能可讓您可以輕鬆地視需要擴充和縮減網路，並使網路對周遊它的應用程式變得透明。

透過在虛擬化網路中使用 NSX IPFIX，網路管理員，您可以檢視虛擬覆蓋。在主機上行上啟用了使用 Netflow 的 VXLAN IPFIX 報告。它提供了封裝封包的 VTEP 的可見度，以及在 NSX 邏輯交換器 (VXLAN) 上產生主機間流量的虛擬機器的詳細資料。

分散式防火牆會實作流程的可設定狀態的追蹤。這些追蹤的流程有群組狀態變更時，IPFIX 可用於匯出如需此流程狀態的資料。

追蹤的事件包括流程建立、流程拒絕、流程更新和流程卸除。已拒絕的事件匯出為 syslog。

啟用 VMware NSX-V IPFIX

在 vRealize Network Insight 中啟用 VMware NSX-V IPFIX：

必要條件

- 確保您具有安全管理員或企業管理員認證。
- 建議在必須從其收集 NSX IPFIX 資料的所有 DVS 和 DVPD 上啟用 VDS IPFIX。您可以從相關聯 vCenter 的詳細資料頁面啟用 VDS IPFIX。

程序

- ◆ 新增或編輯 NSX-V Manager 資料來源時，請選取**啟用 IPFIX**。

啟用 VMware NSX-T DFW IPFIX

在 vRealize Network Insight 中啟用 VMware NSX-T IPFIX：

必要條件

- 確保具有以下權限之一：
 - `enterprise_admin`
 - `network_engineer`
 - `security_engineer`
- 確保分散式防火牆 (DFW) 已啟用。
- 確保優先順序 0 可用於 Network Insight IPFIX 設定檔。如果有另一個優先順序為 0 的 IPFIX 設定檔，必須將其變更為其他值。

程序

- ◆ 新增或編輯 NSX-T Manager 資料來源時，請選取**啟用 IPFIX**。

後續步驟

啟用 IPFIX 時，vRealize Network Insight 會在 NSX-T 上建立自己的 Network Insight 收集器設定檔和 Network Insight IPFIX 設定檔。請確保不要修改任何設定檔。

在 NSX-T 上啟用 IPFIX 後，如果在 vRealize Network Insight 中未看到流程，則可能發生以下事件：

- Network Insight 收集器設定檔未在 NSX-T Manager 中登錄。
- Network Insight IPFIX 設定檔未在 NSX-T Manager 中登錄。
- Network Insight IPFIX 設定檔連接埠號碼已變更。
- Network Insight 收集器設定檔與 NSX-T Manager 中的 Network Insight IPFIX 設定檔不相符。

備註 若要解決所有上述問題，請再次啟用 NSX-T IPFIX。

- Network Insight IPFIX 設定檔的優先順序在 NSX-T Manager 中不為零。
若要解決此問題，請登入 NSX-T Manager，並將 Network Insight IPFIX 設定檔的優先順序設定為零。
- Network Insight 收集器 IP 無法新增至 NSX-T Manager 的現有 Network Insight 收集器設定檔中。
從 NSX-T Manager 中的 Network Insight 收集器設定檔中刪除其中一個收集器，然後從資料來源頁面重新啟用 NSX-T IPFIX。
- 分散式防火牆在 NSX-T Manager 中已停用。
登入 NSX-T Manager 並啟用 DFW 防火牆。

使用 NSX-T 2.4 時，在 NSX-T 上啟用 IPFIX 後，如果在 vRealize Network Insight Network Insight 中未顯示流量，則可能會發生以下事件：

- NSX-T Manager 收集器設定檔中不存在 Network Insight IPFIX 收集器組態。
- NSX-T Manager 中不存在 DFW IPFIX 設定檔。

若要解決這些問題，請再次啟用 DFW IPFIX。

備註 NSX-T 中存在的所有邏輯交換器將在 10-15 分鐘內附加至 IPFIX 設定檔中。

針對實體伺服器的流程支援

vRealize Network Insight 支援傳送版本 v5、v7 和 v9 的 NetFlow 資料的應用裝置。如果提供 DNS 對應和子網路-VLAN 對應資訊，則 vRealize Network Insight 可以使用 DNS 網域、DNS 主機名稱、子網路和第 2 層網路，以擴充 NetFlow 資料。此功能僅適用於企業授權使用者。

在 vRealize Network Insight 中設定 NetFlow：

- 1 針對 NetFlow 和 sFlow 新增實體流量收集器。
- 2 在實體裝置中設定 NetFlow 收集器。
- 3 匯入 DNS 對應檔案。

4 設定子網路和 VLAN 之間的對應。

在實體裝置中設定 NetFlow 收集器

若要將 NetFlow 資訊傳送至 vRealize Network Insight NetFlow 收集器，請手動設定實體裝置。以下是大多數實體裝置中的設定步驟：

1 建立流程記錄。

流程記錄的必填欄位如下所示：

- 將下列欄位標記為 Match。
 - `ipv4 protocol`
 - `ipv4 source address`
 - `ipv4 destination address`
 - `transport source-port`
 - `transport destination-port`
 - `interface input`
- 將下列欄位標記為 Collect。
 - `direction`
 - `counter bytes`
 - `counter packets`
 - `timestamp sys-uptime first`
 - `timestamp sys-uptime last`
- 將下列欄位標記為 Match 或 Collect。否則，將其略過。
 - `transport tcp flags`

2 建立流程匯出工具。

- 提供 vRealize Network Insight NetFlow Proxy IP 和連接埠 2055。

3 設定流程快取，如下所示：

- 作用中逾時：30 秒
- 非作用中逾時：60 秒

4 使用建立的流程記錄和流程匯出工具建立流程監視器。

5 在每個介面上設定監視器。

必要條件

範例

以下幾節提供了設定實體裝置的範例步驟：

- [Cisco 4500](#)
- [Cisco Nexus 1000v](#)
- [Cisco Nexus 9000](#)

備註 這些步驟可能因版本和裝置而有所不同。

Cisco 4500

1 建立流程記錄

```

configure terminal

flow record netflow-original

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface input

collect transport tcp flags

collect counter bytes

collect counter packets

collect timestamp sys-uptime first

collect timestamp sys-uptime last

End

```

2 建立流程匯出工具

```

configure terminal

flow exporter e1

destination <PROXY_IP>

transport udp 2055

end

```

3 建立流程監視器

```

configure terminal

```

```
flow monitor m1  
record netflow-original  
exporter e1  
end
```

4 設定逾時

```
configure terminal  
cache timeout inactive 30  
cache timeout active 60  
end
```

5 在入口模式和出口模式下或至少在入口模式下為每個介面設定流程監視器

```
configure terminal  
interface <INTERFACE_NAME>  
ip flow monitor m1 unicast input  
end
```

Cisco Nexus 1000v

1 設定逾時

```
configure terminal  
Active timeout 60  
Inactive timeout 15  
end
```

2 設定匯出工具

```
configure terminal  
flow exporter <EXPORTER_NAME>  
destination <PROXY_IP>  
transport udp 2055  
source <VSM_IP_OR_SUBNET>  
end
```

3 為每個介面設定流程監視器：

```
configure terminal  
flow monitor <MONITOR_NAME>
```

```
record netflow-original  
exporter <EXPORTER_NAME>  
end
```

4 在入口模式和出口模式下或至少在入口模式下為每個介面設定流程監視器

```
configure terminal  
  
port-profile type vethernet <IF_NAME>  
  
ip flow monitor <MONITOR_NAME> input  
ip flow monitor <MONITOR_NAME> output  
  
.  
.  
end
```

Cisco Nexus 9000

以下是 Cisco Nexus 9000 的一些裝置命令範例：

1 啟用 NetFlow 功能

```
configure terminal  
  
feature netflow  
  
end
```

2 建立流程記錄

```
configure terminal  
  
flow record vrni-record  
  
match ipv4 protocol  
match ipv4 source address  
match ipv4 destination address  
match transport source-port  
match transport destination-port  
match interface input  
  
collect transport tcp flags  
  
collect counter bytes  
collect counter packets  
  
collect timestamp sys-uptime first
```

```
collect timestamp sys-uptime last

End
```

3 建立流程匯出工具

```
configure terminal

flow exporter vrni-exporter

destination <PROXY_IP>

transport udp 2055

version 9

source <INTERFACE_NAME>

end
```

4 為每個介面建立流程監視器

```
configure terminal

flow monitor vrni-monitor

record vrni-record

exporter vrni-exporter

end
```

5 設定逾時

```
configure terminal

cache timeout inactive 30

cache timeout active 60

end
```

6 在入口模式和出口模式下或至少在入口模式下為每個介面設定流程監視器

```
configure terminal

interface <INTERFACE_NAME>

ip flow monitor vrni-monitor input

end
```

擴充流程和 IP 端點

您可以透過 UI 匯入 DNS 對應和子網路-VLAN 對應資訊。

根據 DNS 資料匯入和子網路-VLAN 對應的規格，使用下列類型的相關資訊擴充流程資訊。

- 來源 DNS 網域

- 來源 DNS 主機名稱
- 目的地 DNS 網域
- 目的地 DNS 主機名稱
- 來源 L2 網路
- 來源子網路
- 目的地 L2 網路
- 目的地子網路

根據 DNS 資料匯入和子網路-VLAN 對應的規格，使用下列類型的相關資訊擴充 IP 端點資訊。

- DNS 網域
- DNS 主機名稱
- FQDN
- L2 網路
- 子網路

如需有關透過 DNS 資訊擴充流程的詳細資訊，請參閱[匯入 DNS 對應檔案](#)。

如需有關透過子網路-VLAN 對應擴充流程的詳細資訊，請參閱[設定子網路和 VLAN 之間的對應](#)。

備註

- 僅為實體 IP 增強 DNS 對應和子網路資訊。沒有與任何虛擬 NIC 相關聯的子網路或 DNS 對應資訊。
 - 僅在匯入此資訊後，才會針對已由 vRNI 探索到的流程擴充資訊。
-

搜尋實體到實體流程

您可以根據下列屬性搜尋實體到實體流程：

- 來源 DNS 主機
- 目的地 DNS 主機
- 來源 DNS 網域
- 目的地 DNS 網域
- 來源子網路
- 目的地子網路

您可以根據下列屬性搜尋實體-實體流程。使用擴充的 DNS 和子網路-VLAN 對應資訊進行流程搜尋查詢的幾個範例如下所示：

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Physical-Physical'
```

```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is VM' and  
flow type = 'Destination is Physical'
```



```
bytes,Dns Domain,Dns Host,l2 network of flows where flow type = 'Source is Internet'  
and flow type = 'Destination is Physical'
```

檢視已封鎖的流程和受保護的流程

透過 NSX-IPFIX 整合，您可以查看系統中已封鎖的流程和受保護的流程。

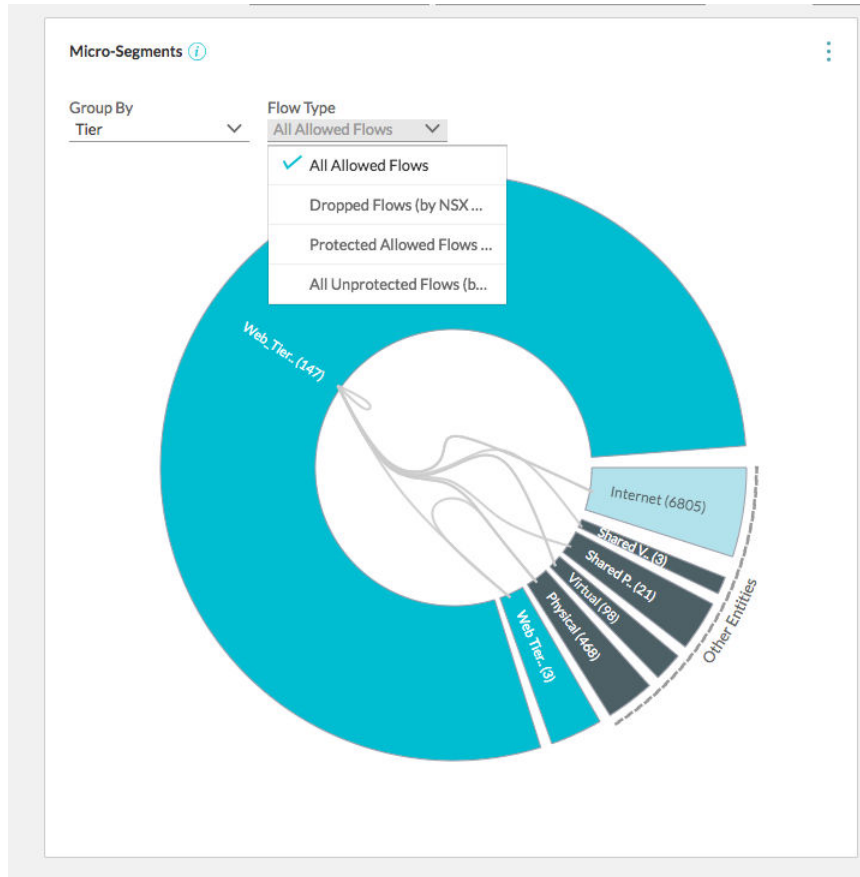
[微分割規劃] 頁面中的基本篩選器如下所示：

- 所有已允許的流程：預設為選取此選項。若要查看防火牆規則中的動作設定為**已允許**的所有流程，請選取此選項。
- 已捨棄的流程：此選項有助於偵測已捨棄的流程，並以更好的方式來規劃安全性。
- 所有受保護的流程：此選項有助於偵測具有與其相關聯的類型不為 `any(source)any(dest)any(service)allow` 的規則的所有流程。此類流程稱為受保護的流程。
- 所有不受保護的流程：此選項有助於偵測具有類型為 `any(source)any(dest)any(service)allow` 的預設規則的所有流程。此類流程稱為不受保護的流程。

防火牆規則僅對已允許的流程和不受保護的流程可見。

例如，如果處於規劃階段，且要查看系統中已允許的流程，請執行下列步驟：

- 1 在 [微分割規劃] 頁面中，針對特定群組，從下拉式功能表中選取**所有已允許的流程**。
- 2 按一下拓撲圖中已捨棄的流程，以查看對應的建議防火牆規則。
- 3 將防火牆規則匯出至 NSX Manager 以對其進行實作。



網路位址轉譯 (NAT)

vRealize Network Insight 支援靜態 NAT (SNAT)、動態 NAT (DNAT)、流程中的反身規則，以及 NSX-V、NSX-T Edge、Fortinet 和 Check Point 的虛擬機器-虛擬機器路徑。

vRealize Network Insight 中的 NAT 流程支援如下所示：

- vRealize Network Insight 支援 NSX for vSphere 和 NSX-T 的嵌套 NAT 階層，對於實體裝置，vRealize Network Insight 僅支援 Fortinet 的單一階層 (DNAT)。
- vRealize Network Insight 支援具有 NAT 定義的上行的 Edge 和層路由器。

備註 不支援 NSX Edge 版本 5.5 或舊版上的 NAT 規則。

- vRealize Network Insight 支援具有範圍的 SNAT 規則。但是，DNAT 必須是目的地和轉譯的 IP 位址之間的一對一對應 (透過 NSX for vSphere 的同位檢查)。
- 對於 Check Point，來源和目的地同時支援使用自動或手動產生的 NAT 規則做為網路、網路群組或位址範圍。

若要檢視 NAT 規則，請使用下列查詢：

- 若要檢視 NSX-T 中的所有 NAT 規則，請使用 NSX-T Edge NAT Rule 查詢。
- 若要檢視 NSX-V 中的所有 NAT 規則，請使用 Edge NAT Rules 查詢。

- 若要檢視 Fortinet 中的所有 NAT 規則，請使用 Fortinet NAT Rule 查詢。
- 若要檢視 Check Point 中的所有 NAT 規則，請使用 Check Point NAT Rule 查詢。
- 若要檢視所有 NAT 規則，請使用 NAT Rule 查詢。

查詢

若要檢視 NAT 規則，請使用下列查詢：

- 若要檢視 NSX-T 中的所有 NAT 規則，請使用 NSX-T Edge NAT Rule 查詢。
- 若要檢視 NSX-V 中的所有 NAT 規則，請使用 Edge NAT Rules 查詢。
- 若要檢視 Fortinet 中的所有 NAT 規則，請使用 Fortinet NAT Rule 查詢。
- 若要檢視 Check Point 中的所有 NAT 規則，請使用 Check Point NAT Rule 查詢。
- 若要檢視所有 NAT 規則，請使用 NAT Rule 查詢。

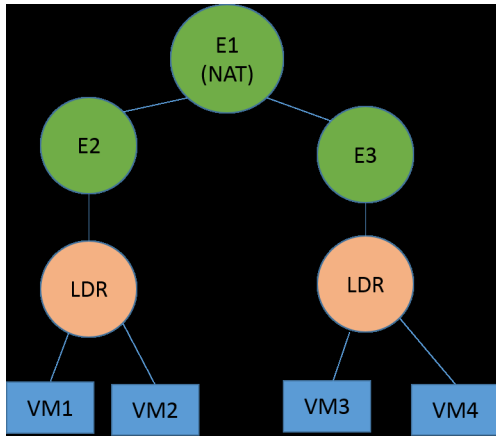
考量事項

- vRealize Network Insight 不支援下列使用案例：
 - 在 NSX-T 中，可以在服務層級上套用 NAT 規則。例如，在 NSX-T 中，L4 連接埠集合是一種服務類型，相關聯的通訊協定可以是 TCP 或 UDP。因此，在虛擬機器-虛擬機器路徑中，不支援服務層級詳細資料。
 - 不支援任何連接埠層級轉譯。
 - 不支援 SNAT 相符目的地位址和 DNAT 相符來源位址。指定 SNAT 規則時，使用 SNAT 相符目的地位址做為目的地 IP 位址。指定 DNAT 規則時，使用 DNAT 相符來源位址做為來源 IP 位址。例如，如果存在 SNAT 規則中所述的目的地 IP 位址，則 vRealize Network Insight 會套用 SNAT 規則，而不管封包是否將目的地位址做為目的地 IP 位址。
 - 在相同的邏輯路由器上使用 NAT 服務啟用時，NSX-T Edge 防火牆對資料路徑。如果流程與 NAT 和 Edge 防火牆均相符，則 NAT 查閱優先於防火牆。因此，防火牆不適用於此流程。如果流程僅與防火牆規則，則此流程接受防火牆查詢結果。
 - 不支援服務轉譯。
 - 不支援 vSEC NAT。

NAT 流程支援 - 範例

本節內容涵蓋 vRealize Network Insight 中支援的 NAT 流程的幾個範例。

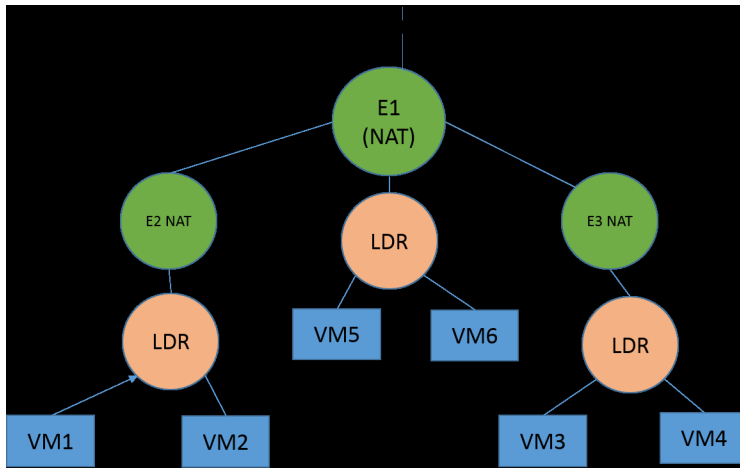
範例 1



在上述拓撲中，E2、E3、LDR、虛擬機器 (VM1、VM2、VM3、VM4) 是 NAT 網域 E1 的一部分。E1 上的任何內容 (例如 E1 的上行) 都是預設 NAT 網域的一部分。以上拓撲包含下列內容：

vRealize Network Insight 中報告了從 VM1 到 VM2 的流程，以及從 VM2 到 VM1 的流程。同樣地，也報告了從 VM3 到 VM4 的流程，以及從 VM4 到 VM3 的流程。

範例 2



以上拓撲包含下列內容：

- VM1 和 VM2 是 E2 網域的一部分。
- VM3 和 VM4 是 E2 網域的一部分。
- E2 和 E3 NAT 網域是 E1 NAT 網域的子網域。
- E1 是預設 NAT 網域的單一子系。
- VM5 和 VM6 是 E1 NAT 網域的一部分。

在上述拓撲中，vRealize Network Insight 中報告了下列流程：

- 從 VM5 到 VM6 的流程

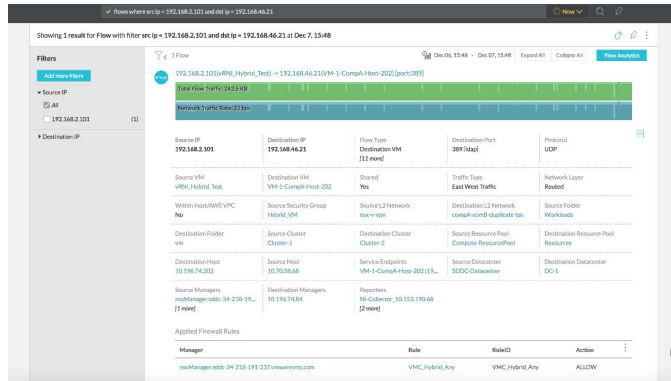
- 從 (VM1, VM2) 到 (VM3, VM4) 的流程

VMware Cloud on AWS 種流量

如果在設定頁面中的資料來源上已啟用 IPFIX 時，您可以檢視流程計數和上次收集時間。

您可以搜尋任何特定流程，並取得與實體相關聯的詳細資料。例如，您可以分別在 Source L2 Network 和 Source Security Group 中檢視原則區段和原則群組資訊。您也可以檢視附加到流程的原則防火牆規則。

vRealize Network Insight 支援透過 VPN 的混合流程。將使用來源實體和目的地實體擴充流程資訊。



備註 如果已將 VMware Cloud on AWS 從 1.8 升級至 1.9 版，您可能會在使用者介面上看到兩次流量。

建立 VPC 流量記錄

透過 Virtual Private Cloud (VPC) 流量記錄，您可以擷取進出 VPC 中網路介面的 IP 流量的相關資訊。

您可以透過 AWS 入口網站建立流量記錄。

程序

- 1 登入 AWS 主控台。
- 2 在尋找服務文字方塊中，輸入並選取 CloudWatch。
- 3 移至記錄 > 動作 > 建立記錄群組。
建立記錄群組視窗隨即出現。
- 4 在建立群組名稱欄位中，輸入群組名稱，然後按一下建立記錄群組。
- 5 在頂端導覽窗格中，按一下服務，然後輸入並選取 VPC。
- 6 在 VPC 儀表板頁面中，按一下您的 VPC。
- 7 選取您要修改的 VPC，然後按一下流量記錄 > 建立流量記錄。

8 在建立流量記錄視窗中，設定流量記錄：

選項	動作
篩選器	選取下列其中一項： 接受 、 拒絕 或 全部 。
目的地	選取 傳送至 CloudWatch 記錄 。
目的地記錄群組	選取您建立的記錄群組。

9 按一下**設定權限**。

系統會開啟 **VPC 流量記錄**正在要求使用您帳戶中的資源的權限頁面。

10 建立 IAM 角色。

- 在 **VPC 流量記錄**正在要求使用您帳戶中的資源的權限頁面的 **IAM 角色**中，選取**建立新的 IAM 角色**。
- 在**角色名稱**文字方塊中，輸入角色名稱。
- 按一下**允許**。

11 在**建立流量記錄**頁面的 **IAM 角色**下拉式功能表中，選取您建立的角色。

12 按一下**建立**

結果

隨即開始在選取的記錄群組上發佈流量記錄。如需有關 VPC 流量記錄的詳細資訊，請參閱 AWS 說明文件，網址為：<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#create-flow-log>。

將流量記錄從 F5 傳送至 vRealize Network Insight 收集器

若要傳送流量記錄，您必須執行下列操作：

SI 編號	工作	連結
1	建立 IPFIX 收集器的集區，以接收來自 BIG-IP 系統的 IPFIX 記錄訊息。	建立 IPFIX 收集器的集區
2	建立記錄目的地以格式化 IPFIX 範本中的記錄。	建立 IPFIX 記錄目的地
3	建立記錄發行者以將記錄傳送到指定的記錄目的地。	建立記錄發行者
4	建立 iRule 以將流量資訊傳送到設定的 vRealize Network Insight 收集器。	建立 iRule
5	新增 iRule 至虛擬伺服器組態，以便 iRule 剖析虛擬伺服器的所有網路流量。	新增 iRule 至虛擬伺服器
6	如果無法從 F5 連線到收集器虛擬機器，您必須為收集器建立路由項目，以便傳送流量記錄。	建立路由項目

建立 IPFIX 收集器的集區

建立 IPFIX 收集器的集區。BIG-IP 系統會將 IPFIX 記錄訊息傳送給此集區。

程序

- 1 登入 F5 主控台。
- 2 按一下**主要 > 本機流量 > 集區 > 集區清單 > 建立**。
新增集區畫面隨即開啟。
- 3 在**名稱**文字方塊中，為集區輸入唯一的名稱。
- 4 在**健全狀況監視器**中，選取 **gateway_icmp** 並將其移至**作用中**方塊。
- 5 在**新增成員**區段中，設定收集器 IP 位址，並按一下**新增**。

選項	動作
節點名稱	輸入收集器 IP 位址。
服務連接埠	2055

- 6 按一下**已完成**。

建立 IPFIX 記錄目的地

建立記錄目的地以格式化 IPFIX 範本中的記錄。格式化之後，這些記錄會傳送至 IPFIX 收集器。

程序

- 1 在 F5 主控台中，按一下**主要 > 系統 > 記錄 > 組態 > 記錄目的地 > 建立**。
記錄目的地畫面隨即顯示。
- 2 在**名稱**文字方塊中，輸入唯一的名稱。
- 3 在**類型**清單中，按一下 **IPFIX**。
- 4 設定 **IPFIX 設定**。

選項	動作
通訊協定	按一下 Netflow V9 。
集區名稱	按一下您在上一個步驟中建立的集區名稱。

- 5 按一下**已完成**。

建立記錄發行者

若要將記錄傳送至指定的記錄目的地，您需要建立記錄發行者。

程序

- 1 在 F5 主控台中，按一下**主要 > 系統 > 記錄 > 組態 > 記錄發行者 > 建立**。
記錄發行者畫面隨即顯示。
- 2 在**名稱**欄位中，輸入唯一的名稱。
- 3 在**目的地**方塊中，選取您先前從**可用**方塊建立的記錄目的地，然後將其移至**已選取**方塊。
- 4 按一下**已完成**。

建立 iRule

若要將流量資訊傳送至已設定的 vRealize Network Insight 收集器，您必須建立 iRule。您必須建立兩個 iRule。一個 iRule 用於 TCP 通訊協定，另一個 iRule 用於 UDP 通訊協定。

程序

- 1 在 F5 主控台中，按一下**主要 > iRule > iRule 清單 > 建立**。
新增 iRule 畫面隨即顯示。
- 2 在**名稱**文字方塊中，輸入唯一的名稱。
- 3 在**定義**文字方塊中，輸入用於 TCP 通訊協定的 TCP 規則和用於 UDP 通訊協定的 UDP 規則。如需角色的相關資訊，請參閱[用於 TCP 和 UDP 通訊協定的 iRule](#)。

確保 iRule 指向先前建立的發行者。
- 4 按一下**已完成**。

用於 TCP 和 UDP 通訊協定的 iRule

使用這些項目為 TCP 和 UDP 通訊協定建立 iRule

TCP 規則

使用以下規則為 TCP 通訊協定建立 iRule：

備註 確保 iRule 指向先前建立的記錄發行者。

```
when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
    set start [clock clicks -milliseconds]
    if { $static::http_rule1_dest == "" } {
        # open the logging destination if it has not been opened yet
        set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
    }
    if { $static::http_rule1_tmplt == "" } {
        # if the template has not been created yet, create the template
```



```

set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
                                                    sourceIPv4Address \
                                                    sourceIPv6Address \
                                                    destinationIPv4Address \
                                                    destinationIPv6Address \
                                                    sourceTransportPort \
                                                    destinationTransportPort \
                                                    protocolIdentifier \
                                                    octetTotalCount \
                                                    packetTotalCount \
                                                    octetDeltaCount \
                                                    packetDeltaCount \
                                                    postNATSourceIPv4Address \
                                                    postNATSourceIPv6Address \
                                                    postNATDestinationIPv4Address \
                                                    postNATDestinationIPv6Address \
                                                    postNAPTSourceTransportPort \
                                                    postNAPTDestinationTransportPort \
                                                    postOctetTotalCount \
                                                    postPacketTotalCount \
                                                    postOctetDeltaCount \
                                                    postPacketDeltaCount \
                                                    flowEndMilliseconds"]

}

}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
    set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
    set client_closed_flag 0
    set server_closed_flag 0
    IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
    IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

    # Clientside
    if { [clientside {IP::version}] equals "4" } {
        # Client IPv4 address
        IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
        # BIG-IP IPv4 VIP address
        IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
    } else {
        # Client IPv6 address
        IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
        # BIG-IP IPv6 VIP address
        IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
    }
    # Client port
    IPFIX::msg set $rule1_msg1 sourceTransportPort [TCP::client_port]
    # BIG-IP VIP port
    IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {TCP::local_port}]

    # Serverside
    if { [serverside {IP::version}] equals "4" } {
        # BIG-IP IPv4 self IP address
        IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
    }
}

```

```

    # Server IPv4 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
} else {
    # BIG-IP IPv6 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
    # Server IPv6 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
}
# BIG-IP self IP port
IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [TCP::local_port]
# Server port
IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [TCP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
    set server_closed_flag 1
    # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
    # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
    if { $client_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes octetDeltaCount
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
    # when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
    # record the client closed time in ms
    IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
    if { $server_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

```

UDP 規則

使用以下規則為 UDP 通訊協定建立 iRule：

備註 確保 iRule 指向先前建立的記錄發行者。

```

when RULE_INIT {
    set static::http_rule1_dest ""
}

```

```

set static::http_rule1_tmplt ""
}

# CLIENT_ACCEPTED event to initiate IPFIX destination and template
when CLIENT_ACCEPTED {
  set start [clock clicks -milliseconds]
  if { $static::http_rule1_dest == "" } {
    # open the logging destination if it has not been opened yet
    set static::http_rule1_dest [IPFIX::destination open -publisher /Common/<Log Publisher>]
  }
  if { $static::http_rule1_tmplt == "" } {
    # if the template has not been created yet, create the template
    set static::http_rule1_tmplt [IPFIX::template create "flowStartMilliseconds \
                                                                sourceIPv4Address \
                                                                sourceIPv6Address \
                                                                destinationIPv4Address \
                                                                destinationIPv6Address \
                                                                sourceTransportPort \
                                                                destinationTransportPort \
                                                                protocolIdentifier \
                                                                octetTotalCount \
                                                                packetTotalCount \
                                                                octetDeltaCount \
                                                                packetDeltaCount \
                                                                postNATSourceIPv4Address \
                                                                postNATSourceIPv6Address \
                                                                postNATDestinationIPv4Address \
                                                                postNATDestinationIPv6Address \
                                                                postNAPTSourceTransportPort \
                                                                postNAPTDestinationTransportPort \
                                                                postOctetTotalCount \
                                                                postPacketTotalCount \
                                                                postOctetDeltaCount \
                                                                postPacketDeltaCount \
                                                                flowEndMilliseconds"]
  }
}

# SERVER_CONNECTED event to initiate flow data to vrni and populate 5 tuples
when SERVER_CONNECTED {
  set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]
  set client_closed_flag 0
  set server_closed_flag 0
  IPFIX::msg set $rule1_msg1 flowStartMilliseconds $start
  IPFIX::msg set $rule1_msg1 protocolIdentifier [IP::protocol]

  # Clientside
  if { [clientside {IP::version}] equals "4" } {
    # Client IPv4 address
    IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
    # BIG-IP IPv4 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv4Address [clientside {IP::local_addr}]
  } else {
    # Client IPv6 address
    IPFIX::msg set $rule1_msg1 sourceIPv6Address [IP::client_addr]
  }
}

```

```

    # BIG-IP IPv6 VIP address
    IPFIX::msg set $rule1_msg1 destinationIPv6Address [clientside {IP::local_addr}]
}
# Client port
IPFIX::msg set $rule1_msg1 sourceTransportPort [UDP::client_port]
# BIG-IP VIP port
IPFIX::msg set $rule1_msg1 destinationTransportPort [clientside {UDP::local_port}]

# Serverside
if { [serverside {IP::version}] equals "4" } {
    # BIG-IP IPv4 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv4Address [IP::local_addr]
    # Server IPv4 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv4Address [IP::server_addr]
} else {
    # BIG-IP IPv6 self IP address
    IPFIX::msg set $rule1_msg1 postNATSourceIPv6Address [IP::local_addr]
    # Server IPv6 IP address
    IPFIX::msg set $rule1_msg1 postNATDestinationIPv6Address [IP::server_addr]
}
# BIG-IP self IP port
IPFIX::msg set $rule1_msg1 postNAPTSourceTransportPort [UDP::local_port]
# Server port
IPFIX::msg set $rule1_msg1 postNAPTDestinationTransportPort [UDP::server_port]
}

# SERVER_CLOSED event to collect IP pkts and bytes count on serverside
when SERVER_CLOSED {
    set server_closed_flag 1
    # when flow is completed, BIG-IP to server REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetTotalCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 packetTotalCount [IP::stats pkts out]
    # when flow is completed, server to BIG-IP RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 octetDeltaCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 packetDeltaCount [IP::stats pkts in]
    if { $client_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

# CLIENT_CLOSED event to collect IP pkts and bytes count on clientside
when CLIENT_CLOSED {
    set client_closed_flag 1
    # when flow is completed, client to BIG-IP REQUEST pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetTotalCount [IP::stats bytes in]
    IPFIX::msg set $rule1_msg1 postPacketTotalCount [IP::stats pkts in]
    # when flow is completed, BIG-IP to client RESPONSE pkts and bytes count
    IPFIX::msg set $rule1_msg1 postOctetDeltaCount [IP::stats bytes out]
    IPFIX::msg set $rule1_msg1 postPacketDeltaCount [IP::stats pkts out]
    # record the client closed time in ms
    IPFIX::msg set $rule1_msg1 flowEndMilliseconds [clock click -milliseconds]
    if { $server_closed_flag == 1 } {
        # send the IPFIX log
        IPFIX::destination send $static::http_rule1_dest $rule1_msg1
    }
}

```

```
}
}
```

新增 iRule 至虛擬伺服器

程序

- 1 在 F5 主控台中，按一下**主要 > 虛擬伺服器 > 虛擬伺服器清單**。
虛擬伺服器清單畫面隨即顯示。
- 2 選取您要新增 iRule 的伺服器。
- 3 按一下**資源索引**標籤，然後在 iRule 區段中按一下**管理**。
- 4 選取您先前建立的 TCP 和 UDP iRule，然後將 iRule 從**可用方塊**移到**啟用方塊**。
- 5 按一下**已完成**。

建立路由項目

收集器虛擬機器必須可從 F5 進行連線。如果無法從 F5 連線到收集器虛擬機器，您必須為收集器建立路由項目。

若要檢查是否可從 F5 連線到收集器虛擬機器，您必須從命令列介面 (CLI) 執行下列命令：`ping <collector-ip> -I <virtual interface>`。如果無法從 F5 連線到收集器，您必須為收集器建立路由項目。

例如，

```
admin@(localhost) (cfg-sync Standalone) (Active) (/Common) (tmsh) # ping 10.153.191.116 -I VLAN301
PING 10.153.191.116 (10.153.191.116) from 10.115.30.50 VLAN301: 56(84) bytes of data.
From 10.115.30.50 icmp_seq=1 Destination Host Unreachable
From 10.115.30.50 icmp_seq=2 Destination Host Unreachable
```

程序

- 1 在 F5 主控台中，按一下**主要 > 網路 > 路由 > 新增**。
新增路由畫面隨即顯示。
- 2 在**內容**區段中，設定路由項目以透過虛擬伺服器將流量記錄從 F5 傳送至 vRealize Network Insight 收集器。

Kubernetes 和 VMware PKS 範圍和流量資訊

11

您可以在 vRealize Network Insight 中執行容器實體範圍並檢視流量資訊。

VMware PKS 和 Kubernetes 流量資訊

vRealize Network Insight 支援 Kubernetes 實體的下列流量類型。

- 虛擬機器至 Kubernetes 網繭
- Kubernetes 網繭至網繭
- 目的地為 Kubernetes 網繭
- 來源為 Kubernetes 網繭

您可以使用這些流量類型來搜尋特定的 Kubernetes 實體。

例如，`flows where flow type = x`，其中 x 是其中一種流量類型

vRealize Network Insight 可提供流量資訊，例如度量、時間序列和所有實體的關係，其中包括容器來源和目的地詳細資料及其實體詳細資料。

此外，還可以在 [流量分析] 儀表板上檢視依 Kubernetes 叢集、命名空間、服務和節點排序的高流量者。

Kubernetes 實體規劃和微分割

您可以透過在 [規劃安全性] 頁面中選取 Kubernetes 叢集、Kubernetes 服務、Kubernetes 命名空間或 Kubernetes 節點做為範圍和微分割，來規劃特定的 Kubernetes 實體類型。此外，您可以規劃或分析應用程式的資料，並根據 Kubernetes 實體定義分組來檢視應用程式流量資訊。

此外，您可以採用 YAML 格式從 [規劃安全性] 頁面中的 [微分割] 匯出與 Kubernetes 實體相關聯的建議防火牆規則。

備註 如果包含虛擬機器或虛擬機器成員，則無法以 YAML 格式匯出應用程式範圍。如果應用程式僅包含容器實體，則可以匯出至 YAML 格式。

檢視實體詳細資料

12

實體頁面提供資料中心內的實體的全面資訊。此資訊涵蓋的範圍可以從顯示與資料中心內其他實體的關係的詳細拓撲到有關特定實體的詳細度量。

每個實體頁面都是 Widget 的集合，且每個 Widget 都顯示與實體相關的特定資訊。同時提供即時資訊與歷史資訊，還提供實體的度量和內容的完整清單。

若要查看有關實體的詳細資訊，則按一下頁面右上角的 **設定檔 > 說明**。

時間表

時間表提供下列資訊：

- 資料中心在過去特定時間的狀態。
- 在所選時間範圍內偵測到的事件的黑鳥瞰視圖。

選取要檢視的時間表的時間範圍。

若要檢視特定時間表，請使用 **時間範圍** 選項來選取時間範圍。

內容 Widget

內容 Widget 在兩個資料行的配置中顯示重要屬性。部分內容釘選項也可能僅顯示單一屬性值。內容釘選項的範例為 **虛擬機器內容** 釘選項。**虛擬機器內容** 釘選項顯示虛擬機器的內容，例如作業系統、IP 位址、預設閘道、邏輯交換器、CPU、記憶體、電源狀態等。

本章節討論下列主題：

- [檢視 vRealize Network Insight 系統 \(NI 系統\) 詳細資料](#)
- [檢視平台虛擬機器詳細資料](#)
- [檢視收集器虛擬機器詳細資料](#)
- [檢視 VMware vCenter 資料來源詳細資料](#)
- [檢視 PCI 合規性詳細資料](#)
- [檢視 Kubernetes 詳細資料](#)
- [檢視負載平衡器詳細資料](#)
- [檢視虛擬機器詳細資料](#)

- [檢視 Edge 裝置詳細資料](#)
- [檢視 NSX Manager 詳細資料](#)
- [檢視 VMware NSX-T Manager 詳細資料](#)
- [檢視 NSX-T 管理節點詳細資料](#)
- [檢視 NSX-T 傳輸詳細資料](#)
- [檢視虛擬伺服器詳細資料](#)
- [檢視集區成員詳細資料](#)
- [檢視 Microsoft Azure 詳細資料](#)
- [檢視 VeloCloud 企業詳細資料](#)
- [檢視 SD-WAN 和 Edge SD-WAN 應用程式詳細資料](#)
- [檢視 SD-WAN 評估詳細資料](#)
- [檢視 VeloCloud 連結應用程式詳細資料](#)
- [檢視 VeloCloud 業務原則詳細資料](#)
- [檢視 VMC SDDC 詳細資料](#)
- [檢視 Arista 硬體閘道和 Arista 硬體閘道繫結詳細資料](#)
- [檢視 Cisco Nexus 裝置詳細資料](#)
- [檢視流量見解詳細資料](#)
- [檢視微分割詳細資料](#)
- [檢視應用程式詳細資料](#)
- [分析 - 極端值偵測](#)
- [分析：靜態和動態臨界值](#)

檢視 vRealize Network Insight 系統 (NI 系統) 詳細資料

[vRealize Network Insight 系統] (NI 系統) 頁面提供與系統相關的所有資訊的快照。存取 [vRealize Network Insight 系統] 頁面：

- 在 **安裝與支援** 頁面上，按一下 **概觀** 旁的 **檢視詳細資料**。此時將顯示 [NI 系統] 頁面。
- 提供 `NI-System` 做為搜尋查詢，以檢視 [vRealize Network Insight 系統] 頁面。

[NI 系統] 頁面分為以下三個區段：

- **概觀**：此區段包含主要內容、資料來源、未解決的問題，以及與系統相關的所有變更和問題的相關資訊。透過按一下每個資料來源，可檢視其詳細資料。
- **事件**：此區段會列出系統、資料來源、平台和收集器中的所有問題和變更。

- 平台和收集器：此區段會列出與系統相關聯的所有平台和收集器。若要檢視有關任何平台或收集器的更多詳細資料，請按一下它。

檢視平台虛擬機器詳細資料

平台**虛擬機器**頁面提供特定平台節點的內容、變更和問題的快照。

在**平台虛擬機器**頁面中，將會顯示：

- 關於所選平台節點的重要資訊，例如名稱、IP 位址、CPU 核心數目、記憶體、上次升級時間和版本。
- 與平台相關聯且未解決的問題。
- 與所選平台節點相關的事件的清單。
- 諸如 CPU 使用率、記憶體使用量和資料磁碟使用量等度量的圖形表示。

檢視收集器虛擬機器詳細資料

收集器**虛擬機器**頁面提供特定收集器節點的內容、變更和問題的快照。

在**收集器虛擬機器**頁面中，將會顯示：

- 關於所選平台節點的重要資訊，例如名稱、IP 位址、CPU 核心數目、記憶體、上次升級時間和版本。
- 與收集器和問題詳細資料相關的未解決問題的數目。
- 與資料來源和問題詳細資料相關的未解決問題的數目。
- 過去七天內在資料來源中發生的變更的清單。
- 資料來源和收集器中可用的 NetFlow 報告器的詳細資料。對於每個 NetFlow 報告器，顯示流程數量。對於資料來源，顯示流程數目，以及探索到的虛擬機器。
- 諸如 CPU 使用率、記憶體使用量和資料磁碟使用量等度量的圖形表示

檢視 VMware vCenter 資料來源詳細資料

VMware vCenter **資料來源**頁面提供特定資料來源的內容、變更和問題的快照。

在 [VMware vCenter 資料來源] 頁面中，將會顯示：

- 關於所選 VMware vCenter 資料來源的重要資訊，例如 IP 位址/FQDN、收集器名稱、已啟用、已探索到的虛擬機器的數目、IPFIX 啟用狀態等。
- 所有與資料來源相關聯的未解決的問題。
- 過去七天在特定資料來源中發生的所有變更和問題。

檢視 PCI 合規性詳細資料

PCI 合規性頁面僅適用於企業授權使用者。

存取 PCI 合規性

- 1 在首頁左側的導覽面板中，選取**安全性 > PCI 合規性**。
- 2 隨即顯示 **PCI 合規性**視窗。選取所需的範圍、適當實體，以及需要資料的持續時間。按一下**評估**。
- 3 隨即顯示 **PCI 合規性**頁面。

PCI 合規性頁面詳細資料

PCI 合規性頁面可協助您僅在 NSX 環境中根據 PCI 要求評估符合性。在儀表板中的第一個釘選項下會顯示這些需求。儀表板中提供用於評估這些需求的資料的其餘釘選項如下所示：

- **網路流程圖**：顯示資料流、防火牆、連線以及與網路相關聯的其他詳細資料。
- **流程**：列出在網路流程圖中檢視的流程。
- **根據目的地連接埠的純文字通訊協定流程**：在特定連接埠上的流量流動採用純文字。此釘選項將根據特定的目的地連接埠顯示純文字通訊協定流程。
- **範圍內的虛擬機器**：顯示在查詢中所選取範圍內的虛擬機器。此釘選項顯示此範圍內的虛擬機器傳出規則、傳入規則和安全群組。
- **虛擬機器的安全群組**：列出虛擬機器的安全群組。
- **虛擬機器計數 (依安全群組)**：按一下此釘選項中的計數，您可以檢視安全群組中的虛擬機器清單。
- **虛擬機器計數 (依安全性標籤)**：按一下此釘選項中的計數，您可以檢視具有安全性標籤的虛擬機器清單。
- **套用至內部流量的防火牆規則**：您可以檢視所選範圍內的虛擬機器之間流量的防火牆規則。
- **套用至傳入流量的防火牆規則**：您可以檢視從範圍以外的虛擬機器傳輸至選取的範圍內的虛擬機器流量的防火牆規則。
- **套用至傳出流量的防火牆規則**：您可以檢視從選取的範圍內的虛擬機器傳輸至範圍外虛擬機器的流量的防火牆規則。
- **安全性標籤成員資格變更**：在此釘選項中顯示與安全性標籤的成員資格相關的變更。
- **安全群組成員資格變更**：在此釘選項中顯示與安全群組成員資格相關的變更。
- **防火牆規則變更**：在此釘選項中列出與任何防火牆規則相關的變更。

備註 如果 NSX 具有巢狀安全群組，則 PCI 合規性的範圍應延伸至安全群組之外。

匯出為 PDF

在 vRealize Network Insight 中，您可以在 [PCI 合規性] 儀表板上建立資訊並匯出為 PDF 報告。

程序

- 1 在 PCI 符合性儀表板中，按一下頁面右上角的**匯出為 PDF**。[匯出為 PDF] 視窗隨即顯示。

- 2 [匯出為 PDF] 視窗列出 PCI 符合性儀表板上可用的所有 Widget 及其相應內容。選取要匯出的 Widget 和內容。

備註

- 必須至少選取一個內容。
 - 您可以選取的內容上限為 20。
 - 清單視圖中可以匯出的項目數目上限為 100。
 - 某些 Widget 不允許選取內容。在這種情況下，請僅指定項目數目。
-

- 3 提供 PDF 報告的標題。

備註

- 標題字元數目上限為 200。
 - 您可以在報告中產生的分頁數目上限為 50。
-

- 4 按一下**預覽**。可查看完整報告的預覽。

- 5 按一下**匯出 PDF**。

檢視 Kubernetes 詳細資料

您可以使用 Kubernetes 儀表板來取得 vRealize Network Insight 中的 Kubernetes 或 VMware PKS 部署的快速概觀。

將會顯示以下詳細資料：

- 前幾個進行通訊的叢集和命名空間 (依據流量)
- Kubernetes 叢集實體的概觀，例如命名空間、網繭、服務和節點的計數
- vRealize Network Insight 中新增的 Kubernetes 叢集
- 在網繭上執行的容器映像的清單和每個容器映像的網繭計數
- 探索到的新網繭的清單以及其計數、命名空間和叢集詳細資料。

此外，您可以按一下儀表板上各個 Kubernetes 實體的計數以查看清單視圖，並移至該特定實體的詳細資料。

表 12-1. Kubernetes 實體儀表板

儀表板	說明
叢集儀表板	<p>您已取得叢集層級的部署詳細資料，其中包括</p> <ul style="list-style-type: none"> ■ 叢集概觀，包含部署中的命名空間、服務、網繭和節點的計數。 ■ 根據流量排列的前幾個命名空間的清單。 ■ 命名空間之間的互動。
命名空間儀表板	<p>您可以取得叢集命名空間詳細資料，例如：</p> <ul style="list-style-type: none"> ■ 命名空間概觀，包括該特定命名空間中的網繭、服務和節點的計數。 ■ 根據流量排列的前幾個通訊服務的清單。 ■ 命名空間中的服務互動。 ■ 依封包數及位元組數的網路流量。
服務儀表板	<p>將會顯示 Kubernetes 服務的詳細資料，例如：</p> <ul style="list-style-type: none"> ■ 包括以下內容計數的服務概觀： <ul style="list-style-type: none"> ■ 24 小時內的開啟事件 ■ 24 小時內的傳入和傳出流量 ■ 網繭 ■ 部署服務所在的節點。 ■ kubernetes 元件與 NSX-T 之間的連線。 ■ 特定期間內作用中節點和網繭的計數。 ■ 命名空間中的服務互動。 ■ 依封包數及位元組數的網路流量。
網繭儀表板	<p>將會顯示相關詳細資料，例如：</p> <ul style="list-style-type: none"> ■ 叢集、命名空間，以及網繭所屬的節點 ■ 根據封包數及位元組數的網繭間的網路流量
節點儀表板	<p>將會顯示相關詳細資料，例如：</p> <ul style="list-style-type: none"> ■ 命名空間詳細資料的清單 ■ 服務的清單 ■ 容器網繭的清單 ■ 根據封包數及位元組數的節點間的網路流量

備註

- vRealize Network Insight 每 10 分鐘從 VMware PKS 收集 Kubernetes 叢集詳細資料一次。
- vRealize Network Insight 每 4 小時從 Kubernetes 叢集收集所有物件 (命名空間、節點、網繭、服務)。但是，如果 Kubernetes 物件有任何變更，vRealize Network Insight 會執行 Watch API 並立即更新變更。
- VMware PKS 不提供關於 Kubernetes 主要節點的詳細資料。
- vRealize Network Insight 提供僅處於成功建立狀態的叢集的詳細資料。

一般事件或錯誤訊息

- `Data Source not reachable` - 從 Proxy 虛擬機器對 VMware PKS 的 IP/FQDN 執行 Ping 動作，以確保 VMware PKS 可供連線。
- `Kubernetes Cluster API Servers not reachable` - 確保所有 Kubernetes 叢集 API 伺服器均可從 Proxy 虛擬機器連線。

檢視負載平衡器詳細資料

[負載平衡器] 頁面概述了在負載平衡器上建立的虛擬伺服器和集區的所有資訊。

將會顯示以下內容：

- 負載平衡器上的虛擬伺服器及其問題的清單
- 負載平衡器上的集區及其相關聯問題的清單
- 與負載平衡器相關聯的事件
- 不同目的地 IP 上的流量、計數及其網路流量的清單。

備註 不會擷取 NSX-V 負載平衡器的流量資訊。

- 提供廠商、類型、序號、虛擬伺服器、集區等資訊的負載平衡器的內容。

檢視虛擬機器詳細資料

您可以使用虛擬機器頁面以取得 vRealize Network Insight 中可用的虛擬機器的詳細概觀。

在 [虛擬機器] 頁面中，將會顯示下列區段：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 虛擬機器詳細資料。 ■ 拓撲資訊。 ■ 各種組態參數。 ■ 與安全性相關的參數。 ■ 虛擬機器至網際網路路徑。
芳鄰	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 相較於芳鄰虛擬機器的各種度量內容的圖形視圖 ■ 屬於相同主機之虛擬機器的清單。
事件	將會顯示與所選虛擬機器相關的事件的清單。

區段	詳細資料
流量	您將看到來自所選虛擬機器的流量清單或嘗試連線至所選虛擬機器 (允許和拒絕其防火牆動作) 的流量清單。
度量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 與所選虛擬機器相關的度量資訊。 ■ ToR 路徑中的連接埠的網路使用量的相關資訊。 ■ 所有度量內容的相關資訊。 ■ 輸入 - 輸出度量資訊。 ■ 虛擬磁碟空間。 ■ 資料存放區效能 <p>備註 如果虛擬機器主控於 vSAN 資料存放區上，則無法查看該虛擬機器的資料存放區度量。</p> <ul style="list-style-type: none"> ■ 虛擬基礎結構延遲詳細資料。 <p>備註 若要查看虛擬基礎結構延遲，必須開啟收集器上的連接埠 1991，以便從 ESXi 主機接收延遲資料。</p>

檢視 Edge 裝置詳細資料

您可以使用 **VMware Edge 裝置** 頁面取得 vRealize Network Insight 中可用的 VMware Edge 裝置的概觀。

若要存取此頁面，請搜尋 **Edge 裝置**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在 **VMware Edge 裝置** 頁面中，將會顯示：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ Edge 裝置的摘要，包括事件圖、位元組、封包、流量和工作階段號碼。 ■ NSX Edge 內容、NSX Edge 服務和 NSX Edge 應用裝置虛擬機器的清單。 ■ 拓撲詳細資料。
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件詳細資料的清單。
流量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種流量分析，例如流經 NSX Edge 的位元組總計、透過 NSX Edge 傳遞的封包總數、流量總計，以及透過 NSX Edge 的工作階段總計。
度量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種度量，例如 NSX Edge 應用裝置虛擬機器的 CPU 使用量、NSX Edge 應用裝置虛擬機器的記憶體使用量、NSX Edge 應用裝置虛擬機器的網路使用量，以及 NSX Edge 的每個 vNIC 的網路使用量。

考量事項

在少數情況下，當以下情況成立時，您可能會在 **VMware Edge 裝置** 頁面中取得錯誤的流量資訊：

- 虛擬機器的 IP 對於 vRealize Network Insight 來說是未知的。
- 虛擬機器中的預設閘道設定不正確。
- 虛擬機器中的南北向流量有兩個以上的 Edge 躍點。
- Edge 屬於 ECMP (相同成本多路徑路由) 叢集。
- Edge 連線至通用邏輯分散式路由器。

檢視 NSX Manager 詳細資料

您可以使用 **NSX Manager** 頁面取得 vRealize Network Insight 中可用的 NSX Manager 的詳細概觀。

如何存取 NSX Manager 頁面

若要存取此頁面，請搜尋 **NSX Manager where SDDC Type = 'VMC'**，然後在搜尋結果清單中，按一下您要檢視的 **NSX Manager** 頁面。

概觀

在 **NSX Manager** 頁面中，將會顯示下列區段：

表 12-2.

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ NSX 原則實體概觀詳細資料。 ■ 過去 24 小時內修改的實體。 ■ 依規則排序的前幾個流量。 ■ 路由器清單。 <p>備註 在 NSX 原則實體概觀 Widget 和 過去 24 小時內的實體數 Widget 中顯示的實體數目可能不同。如果已刪除在過去 24 小時內探索到的某些實體，則 過去 24 小時內的實體數 Widget 中顯示的實體數目可能大於 NSX 原則實體概觀 Widget 中顯示的實體數目。</p>
高流量者	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 您環境中的高流量實體。
網路流量和事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 網路流量和警示概觀詳細資料。 ■ 事件清單。

檢視 VMware NSX-T Manager 詳細資料

您可以使用 **VMware NSX-T Manager** 頁面取得 vRealize Network Insight 中可用的 VMware NSX-T Manager 的概觀。

若要存取此頁面，請搜尋 **NSX-T Manager**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在 NSX Manager 頁面中，將會顯示：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ NSX-T Manager 的摘要，包括事件圖、防火牆規則數目、IPSET、傳輸區域、應用程式和不受保護的流量，以及過去 24 小時內的流量。 ■ 內容清單、依叫用次數的防火牆規則、依規則排序的前幾個流量，以及計算管理程式。 ■ 拓撲詳細資料。拓撲提供實體的內容視圖，還會顯示與實體相關聯的事件。
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件和分析臨界值事件的清單。
流量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種流量分析。
度量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ NSX-T 管理節點健全狀況詳細資料。 <p>備註 NSX-T 管理節點健全狀況詳細資料僅適用於 NSX-T 2.4.0 及更新版本。</p>

檢視 NSX-T 管理節點詳細資料

您可以使用 **NSX-T 管理節點** 頁面，取得 vRealize Network Insight 中可用的 VMware NSX-T 管理節點詳細資料的概觀。

若要存取此頁面，請搜尋 **NSX-T 管理節點**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，您會看到：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ NSX-T 管理節點的摘要，包括內容詳細資料、系統度量和服務狀態。
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件的清單。

區段	詳細資料
介面統計資料	將會顯示以下內容： <ul style="list-style-type: none"> ■ 各種介面統計資料，包括接收的封包數、傳輸的封包數、接收的捨棄封包數、傳輸的捨棄封包數等等。
系統統計資料	將會顯示以下內容： <ul style="list-style-type: none"> ■ 各種系統統計資料，包括系統負載、系統使用量和檔案系統使用量。

檢視 NSX-T 傳輸詳細資料

您可以使用 **NSX-T 傳輸節點** 頁面取得 vRealize Network Insight 中可用的傳輸節點詳細資料的概觀。您可以在 vRealize Network Insight 中檢視主機節點詳細資料和 Edge 節點詳細資料。

節點類型為 [Host] 的 NSX-T 傳輸節點頁面

若要存取此頁面，請搜尋 **NSX-T Transport Node where Node Type = 'HostNode'**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，您會看到：

區段	詳細資料
概觀	將會顯示以下內容： <ul style="list-style-type: none"> ■ 主機傳輸節點的摘要，包括事件圖、傳入流量、傳出流量、內部流量、網路介面數目，以及虛擬機器總數。 ■ 內容詳細資料、傳輸節點狀態、過去 24 小時內的 PNIC 統計資料、過去 24 小時內的 TEP 統計資料，以及過去 24 小時內的系統度量。 <p>備註 系統度量僅適用於 NSX-T 2.4.0 版及更新版本。</p>
事件	將會顯示以下內容： <ul style="list-style-type: none"> ■ 各種事件的清單。
延遲	將會顯示以下內容： <ul style="list-style-type: none"> ■ TEP 至 TEP 延遲詳細資料。
介面統計資料	將會顯示以下內容： <ul style="list-style-type: none"> ■ 各種介面統計資料，包括接收的封包數、傳輸的封包數、接收的捨棄封包數、傳輸的捨棄封包數等等。

區段	詳細資料
系統統計資料	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種系統統計資料，包括系統負載、系統使用量和檔案系統使用量。 <p>備註 系統統計資料僅適用於 NSX-T 2.4.0 版及更新版本。</p>
流量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 依流量排序的前幾台虛擬機器 (過去 24 小時內)，以及依流量排序的前幾個規則 (過去 24 小時內)。

節點類型為 [Edge] 的 NSX-T 傳輸節點頁面

若要存取此頁面，請搜尋 `NSX-T Transport Node where Node Type = 'EdgeNode'`，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，您會看到：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ Edge 傳輸節點的摘要，包括事件圖、網路介面數目、第 0 層服務路由器、第 1 層服務路由器和路由。 ■ 內容詳細資料、傳輸節點狀態、過去 24 小時內的上行統計資料、過去 24 小時內的 TEP 統計資料，以及過去 24 小時內的系統度量
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件的清單。
NAT 統計資料	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種 NAT 統計資料，包括 NAT 規則統計資料、依位元組總計排列的前幾個 NAT 規則、依封包排列的前幾個 NAT 規則，以及依工作階段計數排列的前幾個 NAT 規則。
介面統計資料	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種介面統計資料，包括接收的封包數、傳輸的封包數、接收的捨棄封包數、傳輸的捨棄封包數等等。
系統統計資料	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種系統統計資料，包括系統負載、系統使用量和檔案系統使用量。

檢視虛擬伺服器詳細資料

[虛擬伺服器] 頁面包括虛擬伺服器度量以及問題和變更事件。

將會顯示以下內容：

- 虛擬伺服器中的所有集區成員的清單及其詳細資料，以及任何問題的警示。

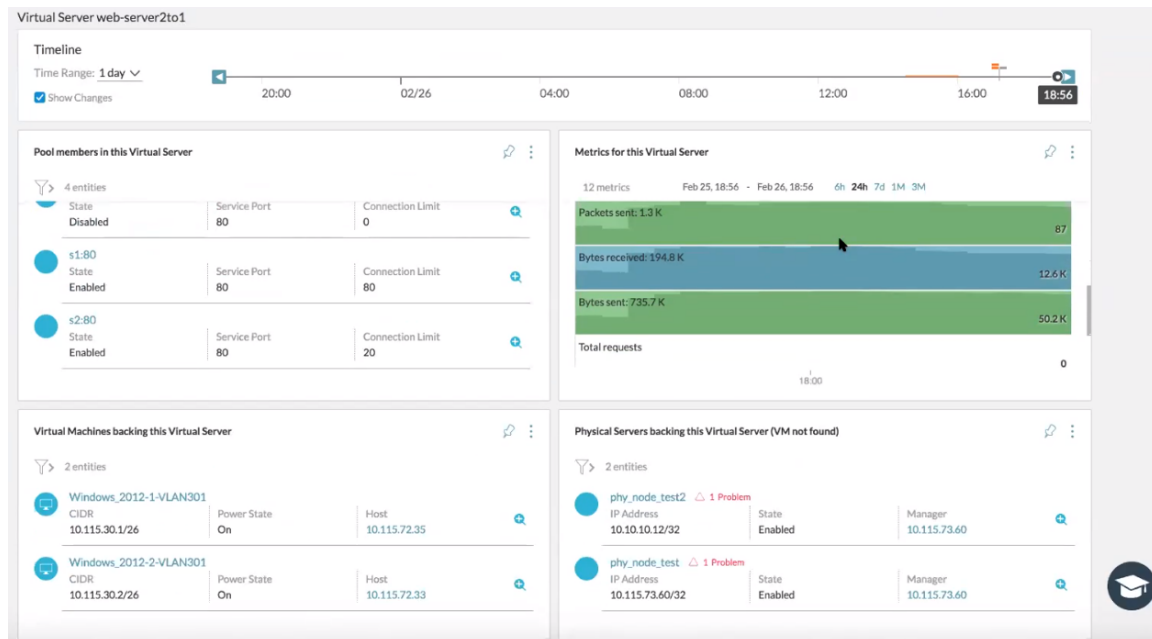
- 虛擬機器的清單
- 實體伺服器的清單
- 與虛擬伺服器相關聯的問題事件的清單
- 與虛擬伺服器相關的度量的清單，例如：
 - 連線 (計數、持續時間)
 - 網路度量 (傳送或接收的封包和位元組數)
 - CPU 使用率

備註 如需受支援的 NSX-V 負載平衡器度量的清單，請參閱[支援的 NSX-V 度量](#)。

- 此虛擬伺服器使用的集區成員的前幾個流量。

備註 不會擷取 NSX-V 負載平衡器的流量資訊。

- 虛擬伺服器內容，提供有關負載平衡器 IP 位址、網路流量、服務連接埠的資訊。



若要檢視與負載平衡器相關聯的拓撲路徑，您可以使用下列查詢：`client VM name to Virtual server IP`。如果不同的服務連接埠上有多個虛擬伺服器，則會在 [選取目的地虛擬機器] 區段下顯示清單。您可以從清單中選取伺服器，然後按一下**顯示路徑**以查看虛擬機器至虛擬伺服器路徑。

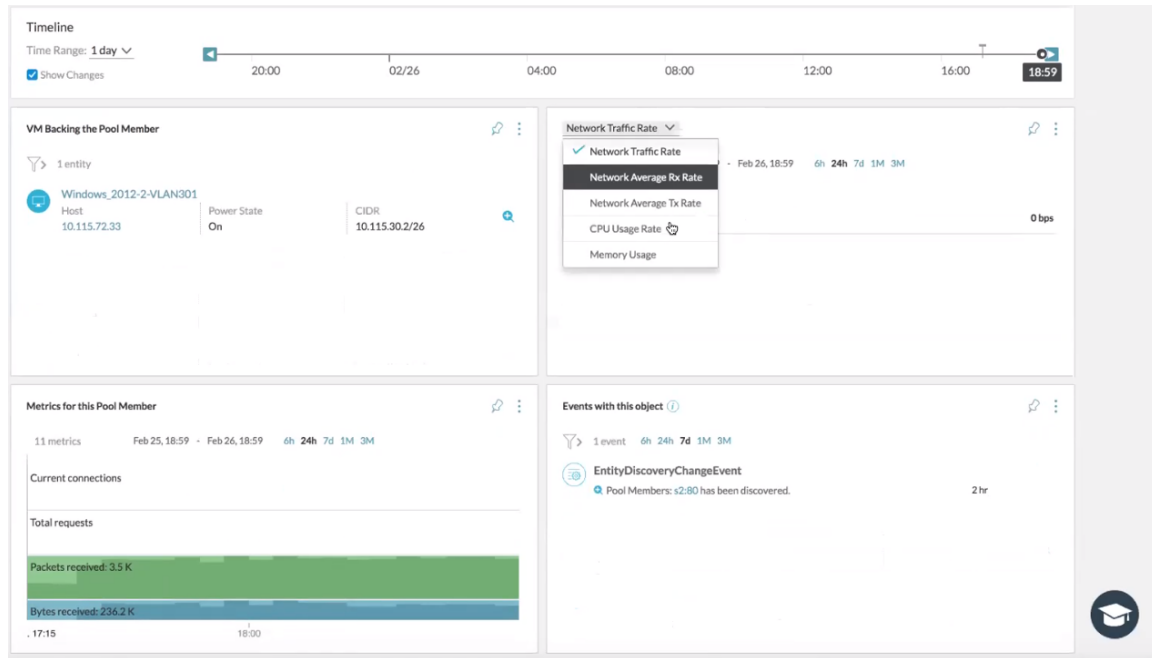
您可以按一下虛擬機器路徑拓撲上的虛擬伺服器，以查看 [虛擬伺服器] 視窗上的一組虛擬機器。按一下**檢視路徑**以查看虛擬伺服器至所選虛擬機器的路徑。

檢視集區成員詳細資料

[集區成員] 頁面會提供有關集區成員、度量以及與集區成員相關聯的事件的見解。

將會顯示以下內容：

- 虛擬機器的清單和虛擬機器的其他詳細資料
- 可讓您將集區成員的度量與虛擬機器的度量進行比較。例如，記憶體和 CPU 使用率、網路流量。
- 與集區成員相關的度量的清單，例如：
 - 連線 (計數、持續時間、存留期)
 - 網路度量 (傳送或接收的封包和位元組數)
 - CPU 使用率
- 提供負載平衡器、節點、狀態、服務連接埠的相關資訊的集區成員內容。



檢視 Microsoft Azure 詳細資料

您可以使用 **Microsoft Azure** 頁面取得 vRealize Network Insight 中 Azure 環境詳細資料的快速概觀。

存取方式

若要存取此頁面，請搜尋 **Azure**。或者，在首頁的**操作和疑難排解**區段中，按一下 **Microsoft Azure** 圖示。

概觀

在此頁面中，您會看到：

- 訂閱清單
- 虛擬機器清單
- 網路介面、虛擬網路、子網路、路由表和路由的清單

- 網路安全群組、應用程式安全群組和 NSG 規則的清單。

您也可以按一下此頁面上的實體，以查看有關特定實體的更詳細的見解。

除了 **Microsoft Azure** 頁面之外，您還可以查看下列 Azure 實體的見解：

表 12-3. Azure 實體詳細資料

實體名稱	說明
Azure 應用程式安全群組	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件、相關聯的虛擬機器和過去 24 小時內的相關聯虛擬機器的清單。 ■ 傳入 NSG 規則和傳出 NSG 規則的清單。 ■ 允許的流量、拒絕的流量、過去 24 小時內的流量的清單。
Azure 資料來源	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件和度量的清單。
Azure NSG 規則	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件和度量的清單。
Azure 網路介面	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件和度量的清單。
Azure 網路安全群組	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件、NIC 和子網路的清單。 ■ 輸出規則和輸入規則的清單。 ■ 允許的流量、拒絕的流量、過去 24 小時內的流量的清單。
Azure 路由	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件和度量的清單。
Azure 路由表	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件和度量的清單。
Azure 子網路	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、事件、虛擬機器、NIC 和自訂路由的清單。 ■ NSG 規則清單。
Azure 訂閱	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容和事件的清單。 ■ 虛擬機器清單。 ■ NIC、虛擬網路和路由表的清單 ■ 網路安全群組、應用程式安全群組和 NSG 規則的清單。

表 12-3. Azure 實體詳細資料 (續)

實體名稱	說明
Azure 虛擬機器	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 內容、事件、NIC、相關聯的應用程式安全群組 (ASG) 的清單。 ■ 傳入 NSG 規則和傳出 NSG 規則的清單。 ■ 允許的流量和拒絕的流量清單。
Azure 虛擬網路	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 內容、事件、虛擬機器、過去 24 小時內建立的虛擬機器、相關聯的 ASG、過去 24 小時內相關聯的 ASG、子網路 and 路由表的清單。 ■ 允許的流量、拒絕的流量、過去 24 小時內的流量的清單。

檢視 VeloCloud 企業詳細資料

您可以檢視 **VeloCloud 企業** 頁面以取得 vRealize Network Insight 中 VMware SD-WAN 部署的快速概觀。

存取 VeloCloud 企業頁面

若要存取此頁面，請搜尋 **VeloCloud 企業**。或者，在首頁的**操作和疑難排解**區段中，按一下 **VeloCloud 企業** 圖示。

概觀

在此頁面中，將會顯示下列區段：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ VMware SD-WAN 部署的摘要，包括事件圖、Edge 數目、集線器、閘道、連結、Edge 到 Edge 的流量、網際網路流量和應用程式。您也會看到這些實體的健全狀況條件。 ■ VMware SD-WAN 部署的對應視圖，以及 Edge 上應用程式的清單。 <p>備註 若要取得對應視圖，您必須在 vRealize Network Insight 中新增 Google 地圖 API 金鑰。如需詳細資訊，請參閱新增 Google 地圖 API 金鑰。如果您未新增 Google 地圖 API 金鑰，則只能看到 Edge 的清單視圖。</p>
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件的清單。
分析	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種流量分佈清單，例如依應用程式的流量分佈、Edge、Edge 配對、流量路徑、流量類型、連結原則和路由類型。

區段	詳細資料
可用性	將會顯示以下內容： <ul style="list-style-type: none"> ■ 可用及無法使用的 Edge/集線器的清單。
度量	將會顯示以下內容： <ul style="list-style-type: none"> ■ 基於 Edge 流量、Edge 封包、Edge QoE、應用程式流量、應用程式封包、連結封包、連結延遲、連結輸送量和連結 QoE 的各種度量。您可以按一下加號 (+) 圖示以取得更多詳細資料。

您也可以按一下此頁面上的實體，以查看有關特定實體的更詳細的見解。

除了 **VeloCloud 企業** 頁面之外，您還可以查看下列 VMware SD-WAN 實體的見解：

表 12-4. VMware SD-WAN 實體詳細資料

實體名稱	說明
VeloCloud 叢集	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容清單。
VeloCloud 資料來源	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容、未解決的問題、過去 7 天內發生的變更和問題的清單。
VeloCloud Edge	將會顯示以下內容： <ul style="list-style-type: none"> ■ 關於 VMware SD-WAN Edge 的詳細資料。如需更多詳細資料，請參閱檢視 VeloCloud Edge 詳細資料。
VeloCloud 閘道	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容和 Edge 的清單。
VeloCloud 第 2 層網路	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容和事件的清單。
VeloCloud 連結	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容和事件的清單。 ■ 有關 QoE、封包、運作時間、延遲和輸送量的度量。
VeloCloud 設定檔	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容和 Edge 的清單。
VeloCloud 區段	將會顯示以下內容： <ul style="list-style-type: none"> ■ 內容清單。

檢視 VeloCloud Edge 詳細資料

您可以使用 **VeloCloud Edge** 頁面取得 vRealize Network Insight 中 VMware SD-WAN Edge 的快速概觀。

若要存取此頁面，請搜尋 **VeloCloud Edge**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，將會顯示下列區段：

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ VMware SD-WAN Edge 的摘要，例如事件圖、原則圖、運作時間詳細資料、應用程式數目、區段、連結、第 2 層網路、LAN 介面、WAN 介面以及通道。 ■ VMware SD-WAN Edge 拓撲。 ■ Edge QoE 和連結 QoE 的清單
事件	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種事件的清單。
流量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 流量清單。
分析	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種流量分佈清單，例如依應用程式和優先順序的流量分佈、流量路徑、流量類型、連結原則和路由類型。
度量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 基於 Edge 流量、Edge 封包、應用程式流量、應用程式封包、連結封包、連結延遲、連結流量和通道流量的各種度量。您可以按一下加號 (+) 圖示以取得更多詳細資料。

您也可以按一下此頁面上的實體，以查看有關特定實體的更詳細的見解。

檢視 SD-WAN 和 Edge SD-WAN 應用程式詳細資料

您可以使用 **SD-WAN 應用程式** 和 **Edge SD-WAN 應用程式** 頁面，取得 vRealize Network Insight 中的 SD-WAN 應用程式和 Edge SD-WAN 應用程式的快速概觀。

概觀

在此頁面中，將會顯示下列區段：

表 12-5. SD-WAN 應用程式

區段	詳細資料
概觀	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ Edge、連結、事件和流量的清單。
流量分佈	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種流量分佈詳細資料，例如依 Edge 的流量和依用戶端的流量。
度量	<p>將會顯示以下內容：</p> <ul style="list-style-type: none"> ■ 各種度量，例如 Edge 流量、Edge 封包、連結流量和連結封包詳細資料。

您也可以按一下此頁面上的實體，以查看有關特定實體的更詳細的見解。

除了 **SD-WAN 應用程式** 頁面之外，您還可以查看下列有關 **Edge SD-WAN 應用程式** 的見解：

- 內容、事件和度量的清單。

備註 vRealize Network Insight 支援每個 VMware SD-WAN Edge 最多 2 個區段，以及最多 20000 個第 3 層網域。

檢視 SD-WAN 評估詳細資料

您可以檢視 **SD-WAN 評估** 頁面，以取得 WAN 部署詳細資料的概觀。您也可以取得 ROI 評估報告，以瞭解流量的性質，並取得 SD-WAN 部署的建議。vRealize Network Insight

如何存取 SD-WAN 評估頁面？

若要存取此頁面，請在左側導覽窗格中，按一下 **計劃與評估 > SD-WAN 評估**。

概觀

在此頁面中，您會看到 SD-WAN 評估報告摘要、出口和入口流量資料，以及出口和入口流量的前幾項服務。

您可以變更評估的範圍和持續時間。若要變更評估的範圍和持續時間，請從 **範圍** 和 **持續時間** 下拉式功能表中，選取您想要使用的範圍和持續時間，然後按一下 **分析**。

您也可以產生 SD-WAN 評估報告。如需詳細資料，請參閱 [產生評估報告](#)。

產生評估報告

在 vRealize Network Insight 中，您可以產生 SD-WAN 評估報告，以取得 VMware SD-WAN 可透過傳統 WAN 設定提供的估計成本節省量。此外，SD-WAN 評估報告也會為每個站台提供 SD-WAN Edge 建議。

程序

- 1 在 **SD-WAN 評估** 頁面中，按一下 **產生報告**。

隨後就會看到 **其他資料** 對話方塊。

- 2 在 **組織名稱** 文字方塊中，輸入您要為其產生報告的組織名稱。
- 3 在 **區域特定輸入** 資料表中，確認區域特定輸入，然後按一下 **產生報告**。

您可以根據需求變更區域特定輸入。您可以按一下 **重設**，以取得區域特定輸入的預設值。

結果

在新的索引標籤中，您可以查看 **SD-WAN 評估報告**。

檢視 VeloCloud 連結應用程式詳細資料

您可以使用 **VeloCloud 連結應用程式** 頁面，取得連結上應用程式的概觀。

若要存取此頁面，請搜尋 **SD-WAN 連結應用程式**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，您會看到下列內容：主要內容、流量詳細資料和流量封包詳細資料的清單。

檢視 VeloCloud 業務原則詳細資料

您可以使用 **VeloCloud 業務原則** 頁面，取得 VeloCloud 業務原則的概觀。

若要存取此頁面，請搜尋 **veloCloud 業務原則**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在此頁面中，您會看到以下內容：定義: 相符、定義: 動作、事件和流量詳細資料。

備註 目前，vRealize Network Insight 不支援下列內容：

- SD-WAN 業務原則，其中來源/目的地為非 VeloCloud 站台。
- SD-WAN 業務原則，其中來源/目的地是物件群組 (IP 群組或連接埠群組)。

檢視 VMC SDDC 詳細資料

您可以使用 **VMC SDDC** 頁面取得 vRealize Network Insight 中 vCenter 和 NSX Manager 的概觀。

如何存取 VMC SDDC 頁面？

若要存取此頁面，請搜尋 **VMC SDDC**，然後在搜尋結果清單中，按一下您要檢視的 **VMC SDDC** 實體。

概觀

在 **VMC SDDC** 頁面中，將會顯示：

區段	詳細資料
概觀	顯示 NSX 原則實體、過去 24 小時內的實體、依規則排序的前幾個流量、路由器清單以及內容詳細資料的概觀。
高流量者	顯示前幾個進行通訊的虛擬機器的圖表。
網路流量和事件	顯示網路流量和清單事件的概觀。

檢視 Arista 硬體閘道和 Arista 硬體閘道繫結詳細資料

您可以檢視 **Arista 硬體閘道** 和 **Arista 硬體閘道繫結** 頁面，以取得 Arista 硬體閘道的概觀。

如何存取 Arista 硬體閘道頁面？

若要存取 Arista 硬體閘道頁面，請搜尋 **Arista 硬體 VTEP**，然後在搜尋結果清單中，按一下您要檢視的實體。

若要存取 Arista 硬體閘道繫結頁面，請搜尋 **Arista 硬體閘道繫結**，然後在搜尋結果清單中，按一下您要檢視的實體。

概觀

在 **Arista 硬體閘道** 頁面中，將會顯示：

- 事件清單
- 主要內容清單
- Arista 硬體閘道繫結的清單。

在 **Arista 硬體閘道繫結** 頁面中，將會顯示：

- 事件清單
- 內容清單。

檢視 Cisco Nexus 裝置詳細資料

您可以使用 **Cisco Nexus 裝置** 頁面取得 vRealize Network Insight 中可用的 Cisco Nexus 裝置的概觀。

概觀

在此頁面中，您會看到：

- 效能監控度量。

備註 若要深入瞭解每個度量，請按一下相應的度量值。

- 事件清單。
- 內容詳細資料。
- 交換器連接埠、交換器連接埠對等以及連線至連接埠的虛擬機器的清單。
- 交換器連接埠度量。

檢視流量見解詳細資料

透過 **流量見解** 頁面，您可以深入瞭解資料中心、裝置和流量。它是以內容為主的頁面，因為該頁面是根據您選取的實體、流量和時間範圍執行分析。

若要存取 [流量見解] 頁面，請執行下列操作：

- 1 在左側導覽窗格中，按一下 **分析 > 流量見解**。
- 2 選取 **範圍** 和 **持續時間**。

3 按一下分析。

或者，您可以搜尋 **Flows**，然後在搜尋結果頁面中按一下**流量見解**。

流程分析儀表板中的各區段如下：

- 高流量者
- 新增功能
- 網路效能
- 極端值

高流量者

此區段可協助您識別哪些實體在您的環境中流量最高。您可以選取不同類型的實體，例如來源-目的地配對、虛擬機器、叢集、L2 網路、子網路。此 Widget 會列出您所選實體類別中的前 10 個高流量者。這可協助客戶規劃網路最佳化。此 Widget 中使用列表示的度量如下所示：

- 按流量：表示流量。
- 按流速：表示流量的速率。
- 按工作階段計數：表示工作階段的數目。
- 按流程計數：表示流程數量



備註

- 如果某虛擬機器在一或多個度量中出現，則在一列中指向該虛擬機器時，虛擬機器也會在其他列中反白顯示。
- 按一下度量列中的虛擬機器時，會顯示傳入此虛擬機器流程的完整清單。
- 在高流量者清單中選取虛擬機器做為實體時，會顯示與此虛擬機器相關的所有流程，無論它是來源還是目的地。如果您在清單中選取來源虛擬機器，則僅考慮傳出此虛擬機器流程。
- 如果您考慮實體流程，則可以選取 [來源 IP] 或 [目的地 IP]。
- 選取來源-目的地配對並指向度量列後，如果您按一下工具提示中的連結，會顯示相應的儀表板。例如，對於來源-目的地配對中的虛擬機器，會顯示虛擬機器-虛擬機器路徑儀表板。
- 對於流程群組視圖、流程實體投影或流程群組查詢，不會顯示**流程分析**按鈕。

新增功能

此區段可協助追蹤所選時間範圍內在資料中心探索到的服務和實體。此區段中的 Widget 如下所示：

- 存取網際網路的新虛擬機器：列出存取網際網路的新虛擬機器。
- 已存取的新網際網路服務：列出在環境中探索到的新網際網路服務。
- 已存取的新內部服務：列出從網際網路端點探索和存取的新內部網路服務。
- 已存取的新內部/E-W 服務：列出資料中心內的機器公開和存取的服務
- 具有已封鎖流程的新服務：列出具有已封鎖流程的服務。僅會針對 IPFIX 填寫此區段。
- 生效的新防火牆規則：列出已生效的新防火牆規則。僅會針對 IPFIX 填寫此區段。

網路效能

在此區段中，您可以根據所選準則針對 TCP 來回行程時間 (RTT) 值的不同範圍尋找並視覺化異常流量。

備註 vRealize Network Insight 僅顯示過去 24 小時內以 5 分鐘為細微度的平均 TCP RTT 度量。

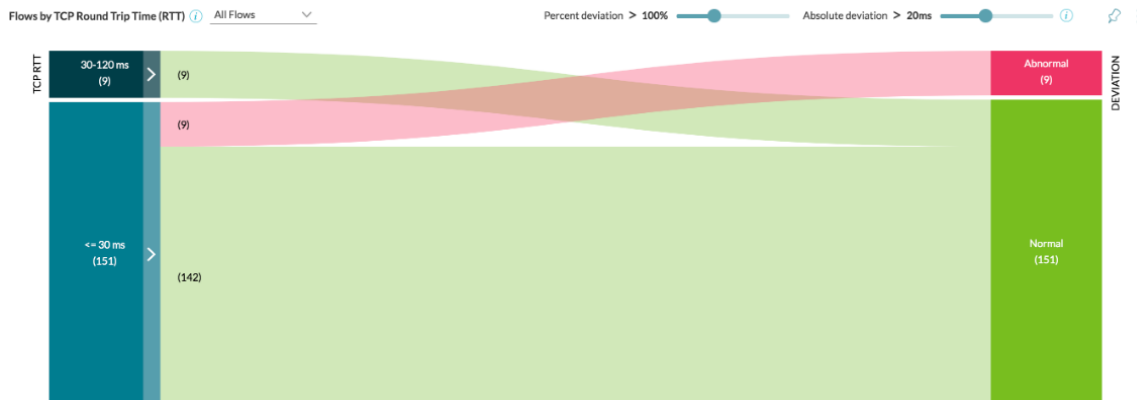
如果流量偏差百分比為 100% 且絕對偏差為 20 毫秒 (ms)，則 vRealize Network Insight 會將該流量視為異常流量。

在視覺化中，左側顯示 TCP RTT 的不同範圍，右側顯示正常與異常偏差範圍。根據偏差百分比和絕對偏差的值，流量會從左側 (TCP RTT) 連線至右側 (DEVIATION)。您可以分析下列類型的流量：

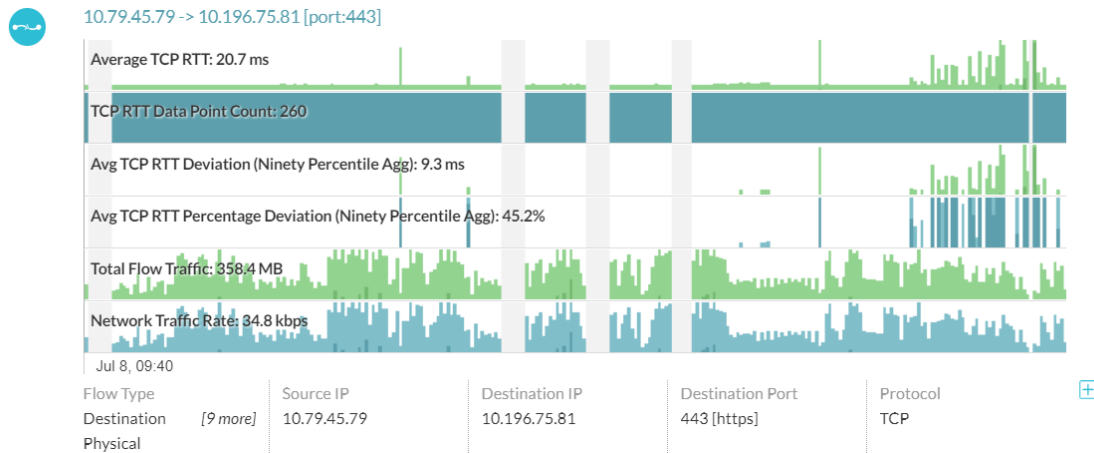
- 主機間
- 主機內部
- 網際網路
- 所有流量

您也可以根據需求變更偏差百分比和絕對偏差。

在下列範例中，有兩個不同的 TCP RTT 範圍，其中一個小於等於 30 毫秒，另一個介於 30 到 120 毫秒之間。您會發現總共有 151 個流量在小於等於 30 毫秒的 TCP RTT 範圍內。在 151 個流量中，9 個流量顯示為異常流量。



若要更深入地瞭解 TCP RTT 分佈資訊和流量計數，請按一下視覺化中的彩色線條。在下列範例中，您可以看到有關 TCP RTT 分佈資訊和流量計數的詳細資料：

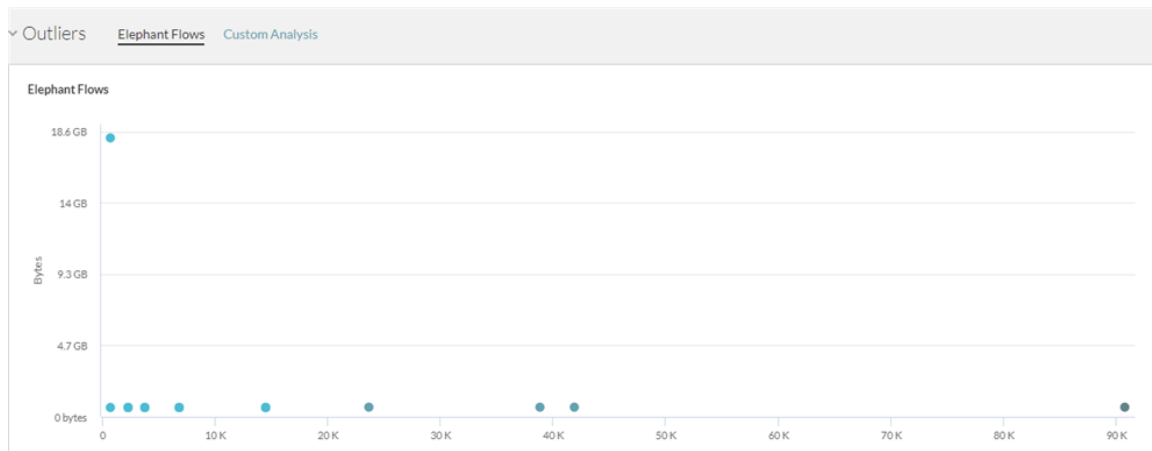


極端值

此區段可協助追蹤和分析相關資料。它包含下列區段：

- **大型流程：**此區段可協助您識別哪些流程的工作階段計數少而輸送量高，哪些流程的工作階段計數多而輸送量小。通常，工作階段計數多而輸送量小的流程也稱為小型流程。分析是以位元組數與工作階段數的比率為基礎。圖形中的每個點表示多個流程。指向一個點時，您會看到流程清單。若要檢視特定流程的詳細資料，請按一下清單中的流程。
- **自訂分析：**在此區段中，您可以在所選的兩個維度上檢視流程資料。這有助於分析資料，以透過多種方式尋找極端值。

備註 此區段中代表的度量是大約值，而不是準確值。



檢視微分割詳細資料

您可以根據 VLAN/VXLAN、安全群組、應用程式、階層、資料夾、子網路、叢集、虛擬機器 (VM)、連接埠、安全性標籤、安全群組和 IPSec 等實體選取相應的範圍並對其進行分割，從而對流程進行分析。

微分割頁面提供了拓撲圖的分析詳細資料。此頁面包含下列區段：

- **微分割：**此 Widget 提供拓撲規劃圖。您可以選取群組和流程的類型。根據輸入內容，您可以檢視對應的拓撲規劃圖。
- **流量分佈：**此 Widget 提供流量分佈的詳細資料 (以位元組為單位)。
- **前幾個連接埠 (依位元組)：**此 Widget 列出記錄最高流量的前 100 個連接埠。提供了流程計數和流量的度量。透過按一下對應至特定連接埠的流程計數，您可以檢視該連接埠的流程。

存取微分割頁面：

程序

- 1 在首頁左側的導覽面板中，按一下**安全性 > 規劃安全性**。

- 2 選取要規劃和分析的範圍、子範圍和持續時間。按一下**分析**。

此時將顯示微分割頁面。

備註 同心圓視圖可以顯示最多 600 個節點和 6000 個 Edge。如果超過限制，將會顯示微分割過多，無法分析。請選取其他實體或微分割準則錯誤。

檢視應用程式詳細資料

應用程式是層的集合。應用程式中的每個層都是基於使用者定義的篩選準則的虛擬機器和實體 IP 的集合。透過這些應用程式，您可以建立一組層，並在同一應用程式的層之間以及在應用程式之間視覺化流量或流程。

您可以透過以下三種方式在 vRealize Network Insight 中建立或新增應用程式：

- [手動建立應用程式](#)
- [公用 API](#)
- [應用程式探索](#)

[應用程式] 頁面會提供 vRealize Network Insight 中單一應用程式的完整可見性。這可讓您對問題進行疑難排解，並檢視分析。

- **概觀**
 - 應用程式拓撲
 - 層概觀
 - 應用程式中的虛擬機器清單
 - 應用程式依賴或使用的實體 IP
 - 共用服務
 - 與此特定應用程式通訊的應用程式
 - 與應用程式相關的事件
 - 應用程式虛擬機器管理程式
- 過去 24 小時的新增內容
 - 傳入和傳出流量計數
 - 捨棄的流量
 - 新的和不受保護的成員
 - 外部存取服務
 - 網際網路存取服務
 - 已使用的應用程式連接埠

- 流量或流量分析
 - 高流量者
 - 依規則排序的前幾名應用程式流量
- 微分割
 - 實體之間的上下文流量，提供了不同流量類型的資料，例如所有允許的流量、捨棄的流量、受保護的流量和不受保護的流量 (依 NSX DFW)。
 - 應用程式的新增內容
- 度量
 - 虛擬機器度量資訊，表示網路速率、CPU、記憶體和磁碟資訊。
 - Kubernetes 度量

分析 - 極端值偵測

vRealize Network Insight 基於與透過虛擬機器和實體 IP 位址定義的流程相關聯的度量提供極端值偵測。這些虛擬機器/IP 應具有類似的流量模式，以便將特定的虛擬機器/IP 分類為極端值是有價值的。例如，屬於應用程式同一層的虛擬機器通常對應用程式執行相同的功能，例如 SQL 資料庫的虛擬機器為 Web 應用程式的要求提供服務。對於這些類型的虛擬機器，接收到的要求數目上限、傳出的流量、工作階段計數等將經歷一系列類似變更。

透過極端值偵測，vRealize Network Insight 允許您偵測特定的虛擬機器，與群組中的其他虛擬機器/IP 相比，它可能會遇到非常不同的流量模式。例如，如果此虛擬機器傳送或接收的流量比群組中其餘虛擬機器的高得多/低得多。可能原因是錯誤地設定了負載平衡器、存在 DDOS 攻擊等。vRealize Network Insight 將此類虛擬機器/IP 分類為極端值。透過查看這些極端值，使用者可以輕鬆地瞭解此未預期的行為，並採取適當動作。

如何偵測極端值虛擬機器

程序

- 1 在側邊列上，按一下**分析**。按一下**極端值**。
- 2 按一下**新增**以新增組態。

3 在分析/設定頁面中，提供組態的下列詳細資料：

表 12-6.

欄位	說明
名稱	組態的名稱
範圍	<p>定義需要對其執行分析的虛擬機器和 IP 之群組的名稱。可以選擇 [應用程式層] 或 [安全群組] 做為範圍。</p> <p>如果您選取 [應用程式層]，請分別提供應用程式和層的名稱。為層定義的虛擬機器和實體 IP 數目顯示在層名稱的旁邊。</p> <p>如果您選取安全群組，則提供安全群組的名稱。</p> <p>備註 目前，一層中的虛擬機器和實體 IP 的數目限制為 200。選取虛擬機器和實體 IP 數目小於此限制的層或安全群組。範圍還應包含至少 3 個虛擬機器/實體 IP。</p> <p>透過按一下檢視微分割，您可以檢視所選組態的微分割。</p>
偵測類型	目前，vRealize Network Insight 支援在系統中偵測極端值。
度量	<p>偵測以此流程度量為基礎。您可以選取下列選項：</p> <ul style="list-style-type: none"> ■ 位元組數 ■ 封包數 ■ 工作階段數 ■ 流速
流量偵測	您可以選取 傳出 、 傳入 或 兩者 做為流量方向。如果您選取 兩者 ，可以在組態預覽中指定傳入或傳出。
流量類型	您可以根據需求選取 網際網路 、 東西向 或 [全部]。
目的地連接埠	<p>您可以選取在所選範圍內探索到的流程上偵測到的所有連接埠，也可以手動輸入您選擇的目的地連接埠。如果您選取所有連接埠，則會顯示目的地連接埠數目。如果您選取手動輸入連接埠，然後在自動完成文字方塊中輸入連接埠，則分析將僅限於這些連接埠。</p> <p>備註 目前，連接埠數目限制為 20。</p>
敏感度	可以度量所需的偵測和報告的敏感度。預設值為 中 。
預覽	此區段會依據您提供的輸入和參數提供特定組態的預覽。如果先前已將流量方向選取為 [兩者]，請指定連接埠和流量方向。您將能夠在圖表中識別極端值虛擬機器。

備註

- 藉由評估過去 24 小時內可用的資料，偵測極端值。
- 您需要連續的 IPFIX 資料流程才能偵測極端值。

4 按一下**提交**以建立分析組態。

5 應用程式建立後，便會出現在 [分析組態] 頁面的應用程式清單視圖中。按一下該特定應用程式，以查看其相關聯的儀表板。

分析：靜態和動態臨界值

透過 vRealize Network Insight，您可以根據實體行為中的偏差來設定臨界值並接收警示。您可以設定下列兩種類型的臨界值：

- **靜態臨界值**：如果特定的度量值高於或低於設定的值，則會產生基於靜態臨界值的警示。
- **動態臨界值**：如果臨界值由系統根據歷史資料分析所決定，則違反此臨界值的情況下會產生警示。產生任何警示之前，對資料進行為期 7 天的分析。建立基準的程序僅限於 21 天的歷史資料，且不會考慮使用較舊的度量值為新度量值建立基準。

違反臨界值後，會立即產生警示。企業授權使用者可以在首頁的**目前狀態**區段中檢視臨界值違規的數目。若要檢視事件詳細資料，請按一下臨界值違規數目。如果系統中不存在臨界值組態，則**目前狀態**區段會顯示 **+ 設定連結**。您可以按一下 **+ 設定連結** 以設定臨界值。

設定臨界值和警示

您可以新增臨界值組態，並取得已設定臨界值的警示。

設定與分析相關聯的臨界值和警示：

程序

- 1 在首頁上的左側導覽面板中，按一下**分析 > 臨界值 > 新增**。

臨界值 - 新增組態頁面隨即開啟。

- 2 在**名稱**文字方塊中，為組態輸入唯一的名稱。

- 3 從**範圍**下拉式功能表中選取範圍，然後在**選取準則**文字方塊中輸入準則。

範圍下拉式功能表由**虛擬機器**、**流量**、**應用程式**、**SD-WAN 連結**、**SD-WAN Edge** 以及 **SD-WAN Edge 應用程式實體**所組成。範圍是以搜尋查詢系統為基礎。您可以根據需求從可用的建議建立查詢。

- 4 在**條件**區段中，設定用於建立警示的條件。

根據您設定的條件，系統會決定是否違反了臨界值。

- 5 預設度量為 `network traffic rate`。選取實體的分組，以及要檢查其臨界值的值。您可以透過彙總一組實體中的資料來設定累積度量的臨界值。

a 若要設定靜態臨界值，請從清單中選取下列任一臨界值條件：

- 超過臨界值
- 低於
- 超出範圍

為 `network traffic rate`、`total traffic` 或任何其他度量輸入 `Upper Bound` 或 `Lower Bound` (如果存在範圍) 時，請確保對該特定文字方塊輸入指定度量中的值。下列轉換值供您參考：

- 1 Kbps = 1000 bps
- 1 Mbps = 1000 kbps
- 1 Gbps = 1000 mbps
- 1 KB = 1024 B
- 1 MB = 1024 KB
- 1 GB = 1024 MB

b 若要設定動態臨界值，請選取與過去行為存在偏差。根據您的報告需求選取敏感度。

Condition ⓘ

For metric `network traffic rate` aggregated over `virtual machine` when any value `deviates from past behavior`

Sensitivity `Medium (2.5 standard deviation)`

- exceeds threshold
- drops below
- is outside range
- ✓ deviates from past behavior

設定臨界值時，您可以檢視頁面頂端的關聯圖形。粉紅列指示違反臨界值的虛擬機器或流程。您可以檢視系統中違反臨界值的實體和臨界值內的實體的清單。

- 6 透過設定下列內容來設定通知或警示：

- 嚴重性
- 電子郵件頻率
- 傳送通知電子郵件到：

備註 如果在系統上已設定 SNMP 設陷，請選取傳送 SNMP 設陷。

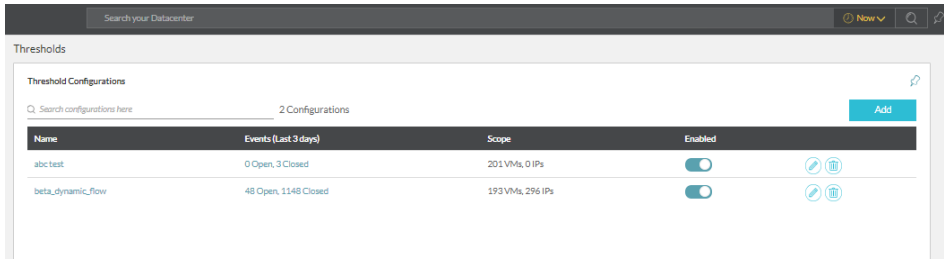
- 7 按一下提交以建立臨界值組態。

檢視臨界值組態頁面

新增臨界值設定，您可以在臨界值組態頁面上檢視其詳細資料。

程序

- 1 在左側導覽面板中，按一下分析。按一下臨界值。

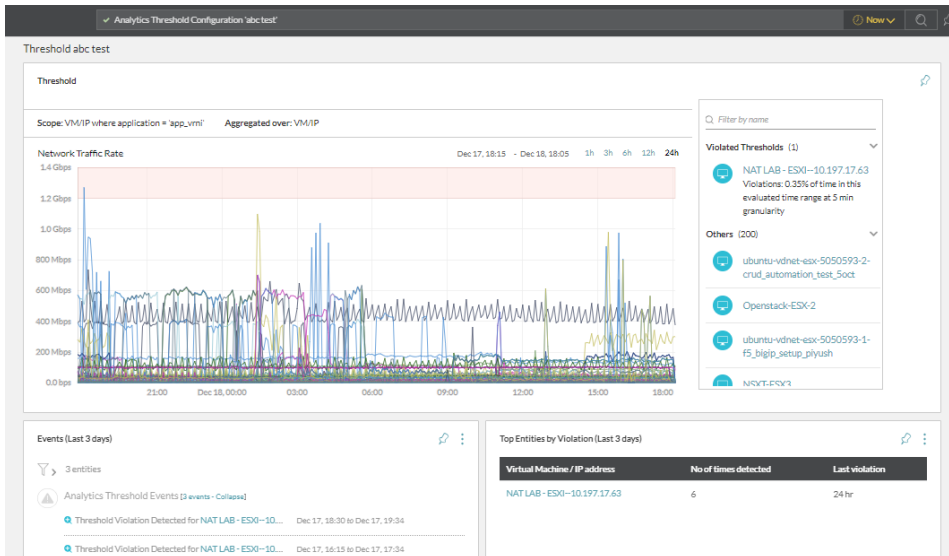


- 2 提供有關臨界值組態的下列詳細資料：

- Name
- Events
- Scope

如果停用此組態，則不會產生違反該特定臨界值的警示。您也可以在此頁面上搜尋任何特定的臨界值組態。

- 3 按一下清單中所需的臨界值組態，以檢視此特定組態的儀表板。



您可以在儀表板上檢視下列 Widget：

- 圖形：臨界值圖可協助您偵測違反臨界值的實體。
- 事件：此 Widget 提供過去三天內為突破臨界值產生的事件清單。
- 前幾名實體 (按違規)：此 Widget 可讓您瞭解在過去三天內影響偏差的前幾名實體。

檢視實體拓撲

13

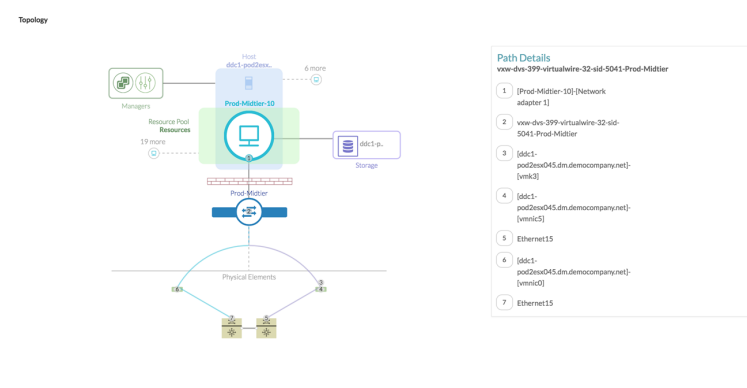
拓撲提供了實體的全面圖形視圖。

本章節討論下列主題：

- 虛擬機器拓撲
- 主機拓撲
- VXLAN 拓撲
- VLAN 拓撲
- NSX Manager 拓撲

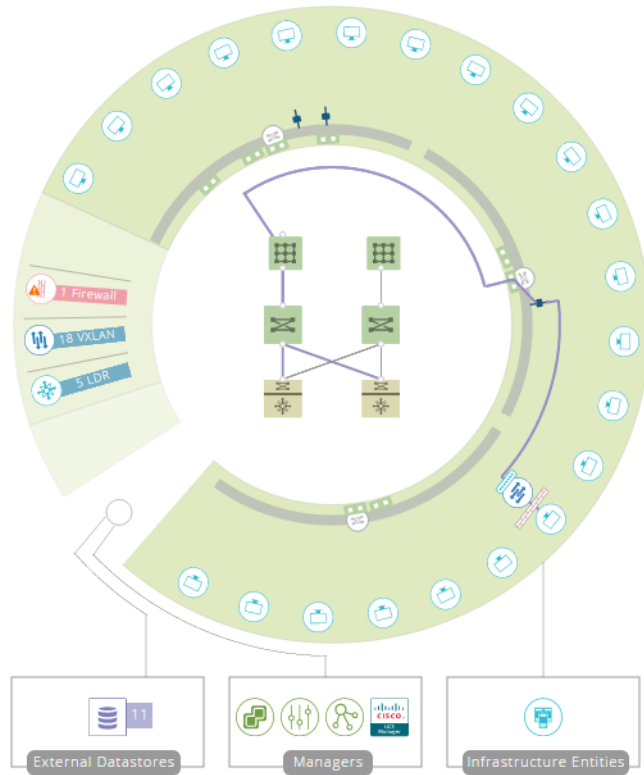
虛擬機器拓撲

虛擬機器拓撲提供了與資料中心其餘部分相關的個別虛擬機器的合併視圖。



主機拓撲

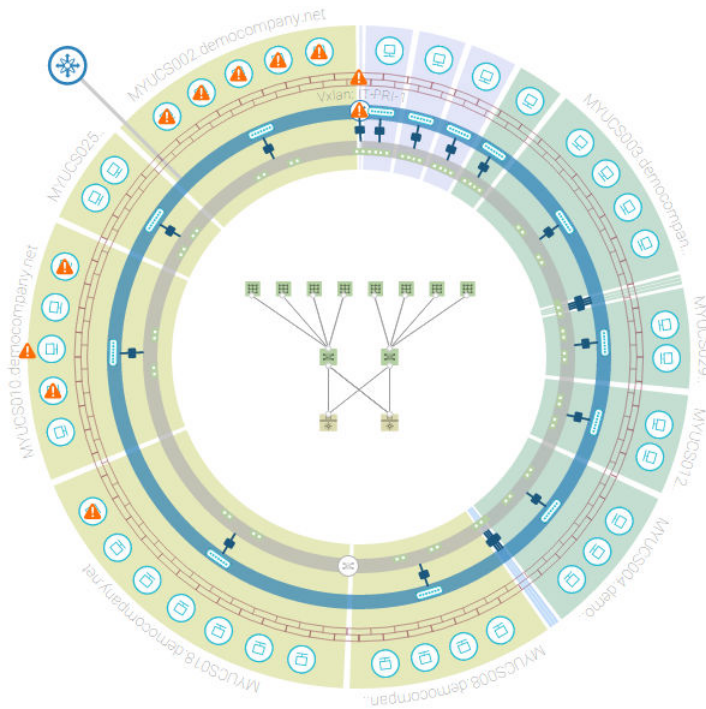
主機拓撲顯示特定主機的虛擬機器如何連線到資料中心的虛擬和實體元件，以及主機本身如何與資料中心連線。



VXLAN 拓撲

虛擬可擴充區域網路 (VXLAN) 覆蓋連線技術是由 VMware 與主要網路連線廠商聯盟開發的產業標準。

VXLAN 拓撲是一種創新的視覺化，可為您提供所選 VXLAN 的概觀。下圖說明組成視覺化的各種元件：



Overview	
VXLAN Network	
Open Problems	4
Configuration Changes	None
Segment ID	5001
Number of VMs	38
Network Address	172.16.151.0/24 172.16.150.0/24
Default Gateway	172.16.150.1
Underlay VLAN ID	218
Underlay Subnet	172.16.69.0/24
Hosts	MYUCS008.democompany.net

備註 虛擬和實體元件都可以透過此方式進行視覺化。

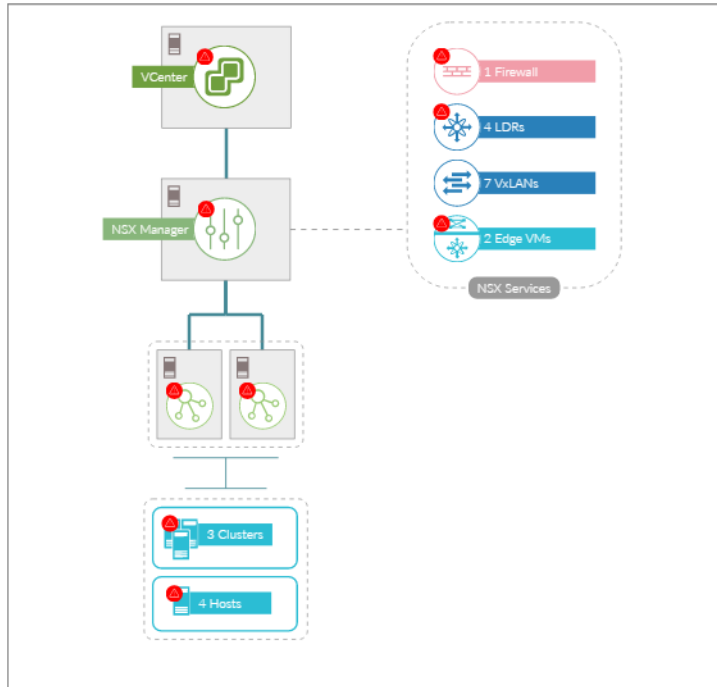
VLAN 拓撲

虛擬 LAN (VLAN) 可讓單一實體 LAN 區段進一步分段，從而使連接埠群組相互隔離，如同位於實際上不同的區段一樣。

VLAN 拓撲的建置方式與 VXLAN 拓撲類似。

NSX Manager 拓撲

NSX Manager 拓撲會顯示與 NSX Manager 相關聯的元件。



在 vRealize Network Insight 中檢視 NSX 物件的稽核資訊

vRealize Network Insight 可從 NSX-T Manager 和 NSX-V Manager 快速擷取 NSX 物件的稽核資訊。此資訊包括建立或修改 NSX 物件的使用者名稱、作業發生時間，以及關於物件的作業詳細資料。

如果您已在 NSX-T Manager 或 NSX-V Manager 中啟用稽核記錄，vRealize Network Insight 可以針對部分 NSX-T 和 NSX-V 物件收集稽核詳細資料。

NSX-V

vRealize Network Insight 在 3 到 5 分鐘內為其收集稽核詳細資料的 NSX-V 物件的清單。

- SecurityGroup
- SecurityGroupTranslation
- FirewallConfiguration
- FirewallStatus
- IPSet
- SecurityTag
- UniversalSecurityGroup
- UniversalSecurityGroupTranslation
- UniversalIPSet

針對探索、內容變更和刪除事件擷取 NSX-V 物件的稽核詳細資料：

- Discovery



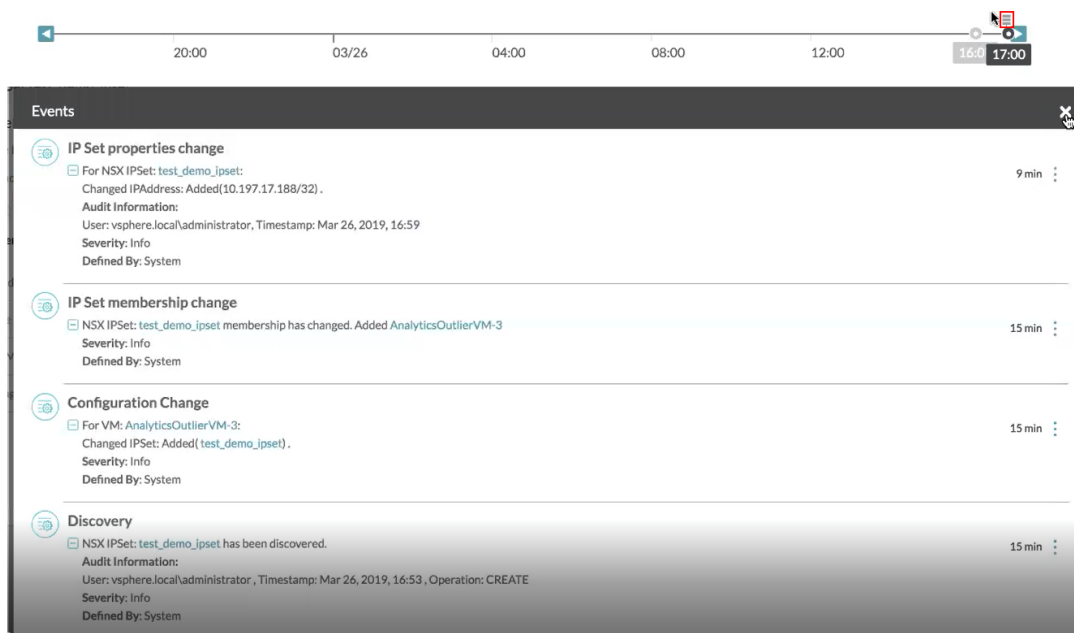
■ Properties Change



■ Delete

<p>NSX IPSet:jagdish_ipset12 deleted.</p> <p>Audit Information: User: vsphere.local\administrator, Timestamp: Feb 13, 2019, 11:23</p> <p>Severity: Info</p> <p>Defined By: System</p>	6 min
<p>NSX Universal IPSet:jagdish_ipset13_universal deleted.</p> <p>Audit Information: User: vsphere.local\administrator, Timestamp: Feb 13, 2019, 11:24</p> <p>Severity: Info</p> <p>Defined By: System</p>	6 min

您也可以在物件的時間表上檢視稽核資訊。



NSX-T

vRealize Network Insight 為其收集稽核詳細資料的 NSX-T 物件的清單。

備註 不提供 VMC 原則實體的稽核資訊。

- NSGroup
- NSService
- NSServiceGroup
- NSFirewallRule

備註 不提供 NSFirewallRule 的刪除事件的稽核資訊。

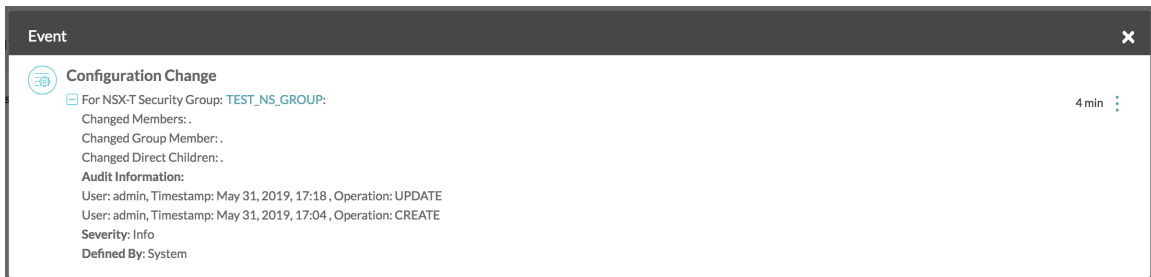
- IPSet
- NSX 原則群組
- NSX 原則防火牆規則

針對探索、內容變更和刪除事件擷取 NSX-T 物件的稽核詳細資料：

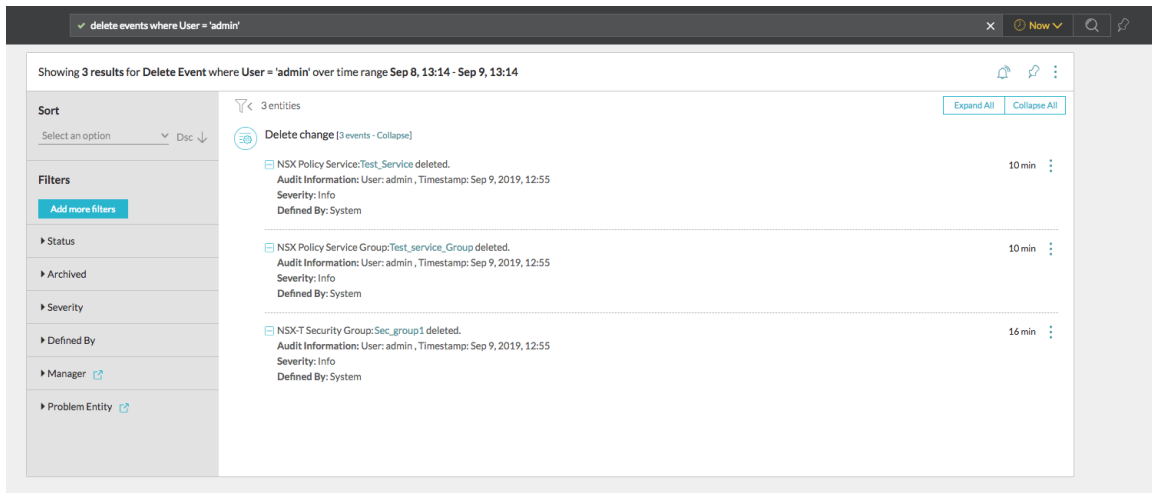
- Discovery



- Properties Change



- Delete



備註 實體儀表板上不顯示刪除事件。但是，您可以搜尋事件以查看稽核資訊。

查看稽核資訊的查詢範例

- `events where user = username`
- `discovery events where user = username`
- `delete events where user = username`
- `change events where user = username`

應用程式的所有部分都表示為釘選項；釘選項是可以儲存和分組的基本單元，用於彙總您認為組合起來可以很有用的資料，以及將其與團隊中的其他成員共用。可以釘選搜尋查詢以及可用於實體的釘選項。

若要新增，請按一下圖釘圖示。所有已儲存的釘選項都顯示在 [看板] 區段中，並可透過按一下標頭中的 [看板] 圖示叫用。

本章節討論下列主題：

- 釘選項
- 看板

釘選項

每個實體頁面上的資訊會分割為多個釘選項。所有實體頁面均由釘選項組成，每個釘選項都包含與實體相關的特定少量資訊。

這些釘選項具有以下功能：

- 您可使用更多選項 () 按鈕最大化任何釘選項視圖，也可以使用**協助**選項檢視釘選項的詳細資料。
- 釘選項也可以包含篩選器，以便您可以深入瞭解釘選項上顯示的資料。
- 許多釘選項還包含匯出為 CSV 選項，以便能以 CSV 格式匯出釘選項中存在的資料。您可以在顯示的對話方塊中選取要匯出的特定內容和 CSV 行數。

備註 選取所有欄位後，對於 180,000 個流量，針對流量資料執行匯出至 CSV 功能需要超過 30 分鐘。

釘選項類型

軟體中可用的大多數釘選項可分為下列類別：

度量釘選項

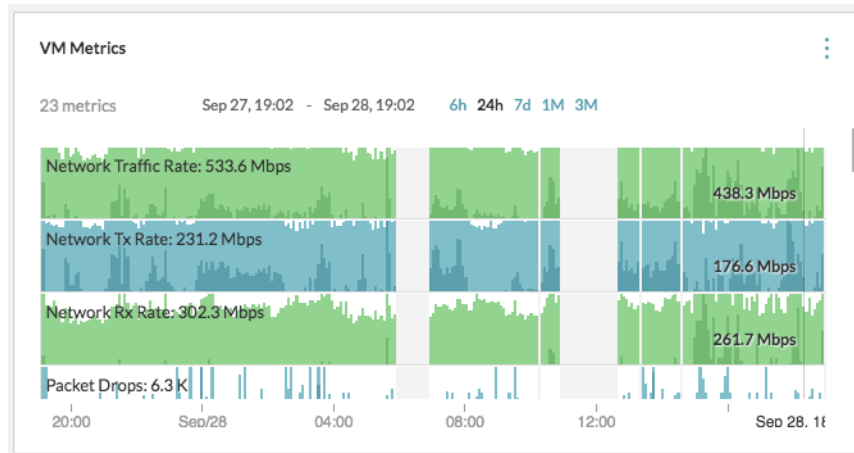
度量釘選項顯示與所選實體相關的重要度量。

度量釘選項使用立體圖形顯示資料，方法是將每個圖形劃分為兩個區段，並將較高的值相互換位。因此，較高的值以較暗的色彩顯示且更容易識別。

您可以從釘選項標頭的下拉式功能表中選取要顯示的特定度量，並變更要顯示的實體選項。

可透過使用範圍預設或輸入自訂日期/時間來修改時間範圍。

度量釘選項的一個範例是虛擬機器度量釘選項。此釘選項顯示虛擬機器的網路流速、網路 Tx 速率、網路 Rx 速率和封包捨棄數。



[實體清單] 視圖釘選項

[實體清單] 視圖釘選項顯示依共同主題分組的實體清單。此清單會顯示每個實體的重要屬性。

透過按一下最右側的放大圖示，您可以查看特定實體的更多屬性。按一下實體名稱會前往實體頁面。

與其他釘選項一樣，篩選器圖示包含可用於篩選清單的各個方面。項目清單視圖釘選項的一個範例是虛擬機器芳鄰釘選項。依預設，此釘選項顯示同一主機上存在的虛擬機器。您也可以按安全群組、VXLAN 和資料存放區篩選虛擬機器。

Metrics			
Key Metrics	Neighbor Benchmark	Neighbor Performance	VM Neighbors
Network Usage of Ports in Path to TOR	All Metrics	I/O Metrics	Virtual Disks
Datastore Performance			

VM Neighbors			
7 entities			Host: ddc1-pod2esx...
Prod-Midtier-14	Def Gateway	Logical Switches	
CIDR 10.17.7.14/24	10.17.7.254	Prod-Midtier	
Lab-Web-19-noip	CPU	Memory (GB)	
Logical Switches Lab-Web	16	16	
Prod-DB-5	Def Gateway	Logical Switches	
CIDR 10.17.8.10/24	10.17.8.254	Prod-DB	

事件視圖清單釘選項

事件清單視圖釘選項依時間順序提供特定實體或實體群組 (可從釘選項標頭的下拉式清單中選取) 的事件清單。

透過使用可用的預設或輸入自訂日期/時間，您可以變更釘選項顯示事件的時間 (離現在) 有多遠。透過按一下篩選器圖示，您可以選取其他篩選器選項，例如事件狀態和事件類型。

在下圖中，將顯示與虛擬機器 Prod-db-vm21 及其相關實體相關的事件。您可以按一下實體名稱，以檢視其他相關實體中的事件。使用篩選器，您可以根據事件的狀態和類型進行篩選。事件可以是與實體相關的變更或問題。

您可以使用事件搜尋查詢來搜尋事件。您可以透過查詢 (如已開啟的事件或已關閉的事件) 來搜尋已開啟或已關閉的事件。您也可以搜尋具有相同修飾詞的問題。

看板

您可以從看板上的任何頁面釘選任何 Widget，以便更輕鬆地存取和共用資料。

建立看板

- 1 按一下要釘選的 Widget 上的圖釘圖示。

- 2 在快顯視窗中按一下**建立新看板**。

備註

- 如果尚未建立任何看板，您可以從**最近修改**清單中選取**預設看板**。

備註 預設看板為首次使用的使用者提供了一般看板的外觀與風格。這可協助使用者熟悉看板的配置和功能。無法共用或刪除預設插接表板。您可以將釘選項從預設看板複製到任何自訂看板。

- 您可以在最近修改清單中看到的項目數目上限為 15。
- 您可以在所有使用者之間建立的最大看板數目為 500。

備註 看板總數包含自訂看板、共用看板和預設看板。

- 每個看板的最大釘選項數目為 20。

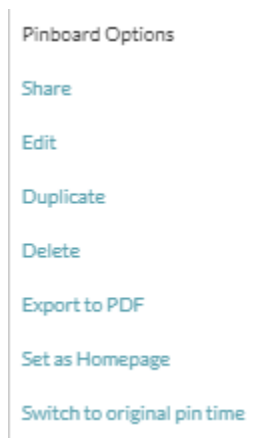
- 3 在**建立看板**視窗中，輸入新看板的名稱和說明。按一下**建立並釘選**。

備註

- 看板的名稱在整個系統中必須是唯一的。
- 看板名稱的允許字元數目上限為 100。在看板的名稱中只能使用字母、數字和空格。

- 4 此時將顯示**已建立看板**訊息。按一下**立即共用**以立即共用看板。
- 5 若要將 Widget 釘選到現有看板，請在**最近修改**下選取看板，然後按一下**釘選**。此時將顯示訊息**您的釘選項已新增**，其中包含指向適當看板的連結。

存取看板選項



按一下看板右上角的**更多選項**，以存取**看板選項**。

備註 僅當您已建立看板或已與具有**檢視**和**編輯**權限的任何其他使用者共用時，才會顯示所有看板選項。任何其他使用者僅可看到**匯出為 PDF**和**移轉至原始釘選時間**選項。

您可以在看板上執行下列動作：

- 可與任何其他現有 vRealize Network Insight 使用者共用看板。

- 您可以編輯看板和看板上釘選項的名稱。
- 您可以重新排列看板上的釘選項。它們的位置保持不變。
- 按一下**刪除**可刪除該特定看板。
- 按一下**匯出為 PDF**可將看板上的資料匯出為 PDF 報告。如需更多詳細資料，請參閱**匯出為 PDF**。
- 若要檢視釘選項在釘選時的資料，請按一下**切換至原始釘選時間**。透過此功能，您可以檢視每個釘選項在建立時的資料。

使用看板的時間表滑桿

vRealize Network Insight 支援看板上的時間表滑桿。若要查看任何所需時間的看板資料，您可以使用時間表滑桿。看板載入時，會載入目前時間 (現在) 的所有釘選項。

檢視看板程式庫

如果您是管理員使用者，您可以在看板程式庫中看見**我的看板**索引標籤和**所有看板**索引標籤，如下圖所示。如果您是成員使用者，您可以在看板程式庫中看到看板清單。

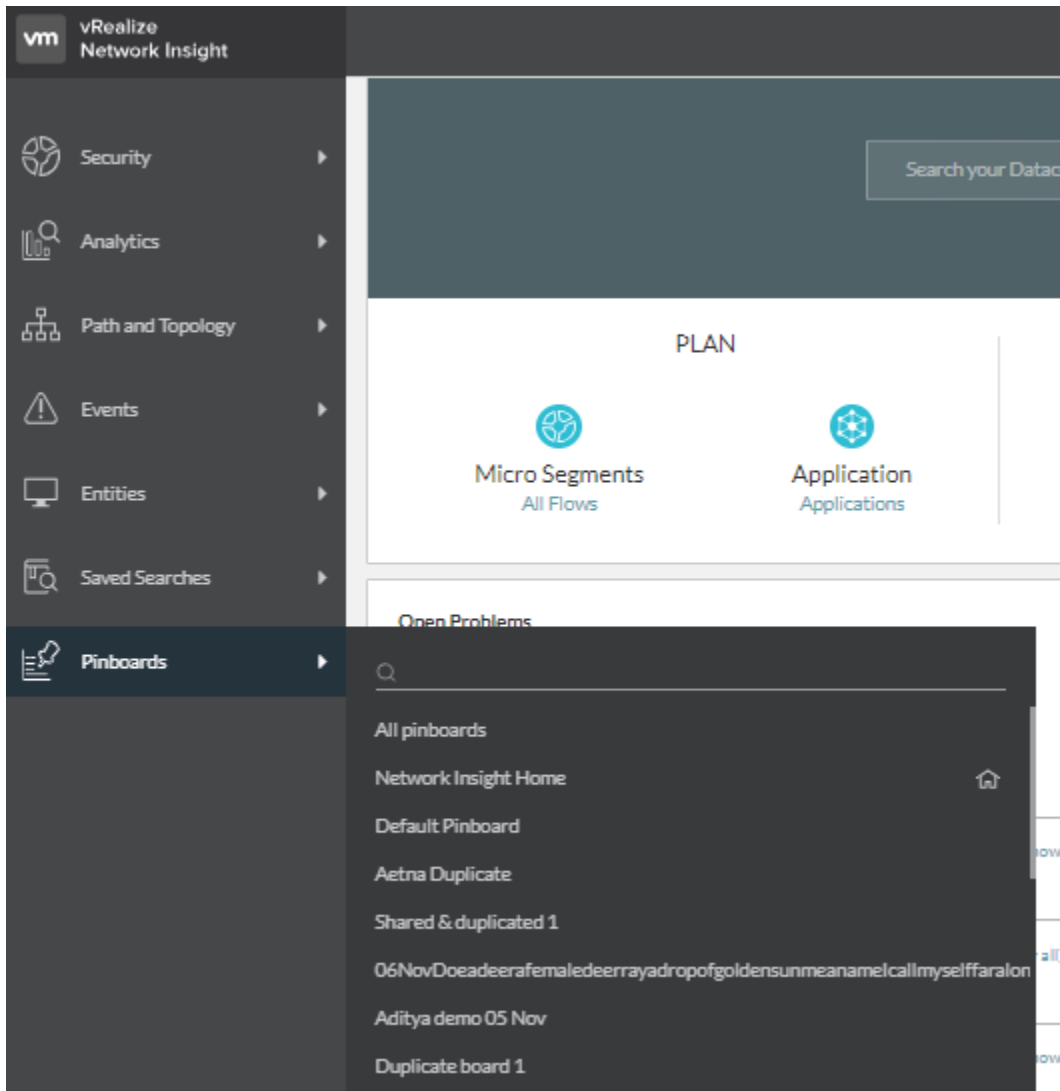
Pinboards

Search for pinboards 17 pinboards

Pinboard name	Last modified	Owner	Shared	Actions
Network Insight Home	--	--	--	
Default Pinboard	81 days	Guest 1	Not shared	
Aetna Duplicate	24 days	Guest 1	Not shared	
Shared & duplicated 1	30 days	Guest 1	5 others	

- 1 在首頁的左導覽列上，按一下**看板**。
- 2 按一下**所有看板**以檢視系統中的所有看板。
- 3 您可以在導覽列中檢視現有看板的清單。此清單具有與看板程式庫中**我的看板**索引標籤相同的項目。上次修改的看板會顯示在清單頂端。按一下您想要檢視的看板。

備註 建立看板後，需要一些時間才會顯示在清單中。



4 您也可以在程式庫中搜尋看板。

複製釘選項

- 1 按一下 Widget 上的圖釘圖示。
- 2 選取您要將釘選項複製到的看板。
- 3 按一下**新增**。

看板的共用和協作

可與其他使用者共用您建立的看板。管理員使用者可以檢視和刪除任何看板。以下是看板的共用和協作功能：

如果您已建立看板，則無論您是管理員或成員使用者，都可以檢視、編輯或刪除。

表 14-1.

看板擁有者	與以下人員共用	權限	可能的動作
管理員	管理員	檢視並編輯	檢視、編輯、刪除
	管理員	僅檢視	檢視、刪除
	成員	檢視並編輯	檢視、編輯
	成員	僅檢視	檢視
成員	管理員	檢視並編輯	檢視、編輯、刪除
	管理員	僅檢視	檢視、刪除
	成員	檢視並編輯	檢視、編輯
	成員	僅檢視	檢視

備註 如果您必須刪除看板，且建立來源的使用者無法使用，則管理員使用者可以刪除它。

Sharing and Collaboration

Link to pinboard

<https://10.197.53.51/#pinboard/10000:10002:76196914460807861> Copy

☒ Allow all users with link access to view

Users with access

Admin (Owner) View & Edit

Invite new users

Select... View only Add

Save Cancel

共用看板：

程序

- 1 在要共用的看板上按一下**更多選項**。
- 2 按一下**共用**。
- 3 您也可以透過按一下**動作**下的共用圖示，從**看板程式庫**共用看板。

- 4 依預設已啟用連結共用。可以與已登入的使用者共用看板的連結。
- 5 您可以新增您想要共用看板的使用者。您可以為特定使用者指定諸如 `view` 和 `view and edit` 之類的權限。

備註 僅擁有檢視權限的使用者無法與任何其他使用者共用看板。

- 6 按一下 **儲存** 以儲存您進行的共用和協作變更。
- 7 您可以使用下列其中一個選項檢視任何看板的共用和協作資訊。
 - 在 **看板程式庫** 中，您可以在特定看板的 **共用資料** 行中檢視共用資訊。
 - 按一下 Widget 上的圖釘圖示。指向 **最近修改** 下列出的任何看板，以檢視有關擁有者以及與其共用其使用者的詳細資料。

將看板設定為首頁

您可以將選取的看板設定為預設首頁。

程序

- 1 導覽到要設定為首頁的所需看板。
- 2 按一下 **看板選項**。按一下 **設定為首頁**。

此特定看板會設定為首頁。

備註 將看板設定為首頁後，就會停用此看板上的 **設定為首頁** 選項。

- 3 在 **我的喜好設定** 頁面的 **設定** 下，您也可以將特定的看板設定為預設首頁。
- 4 如果您要查看之前的首頁，請按一下左側導覽面板中 **看板** 下的 **Network Insight 首頁**。將快顯訊息是 **否要將 Network Insight 首頁設定為首頁?**。如果您要還原為預設首頁，請按一下 **設定首頁**。按一下 **關閉** 以關閉精靈。

備註

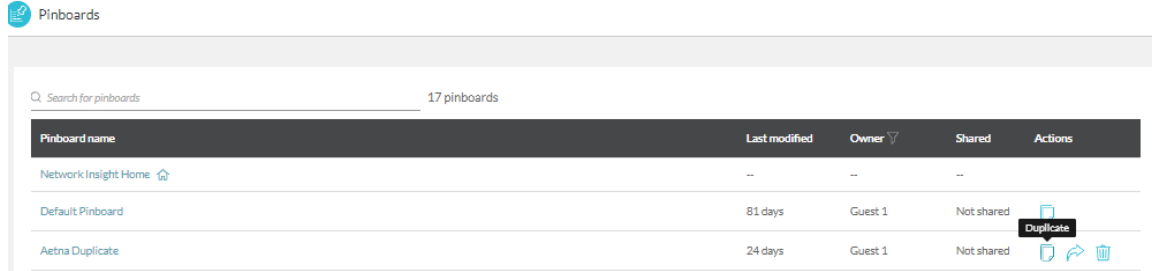
- 如果您刪除已設定為首頁的看板，則預設首頁會重設為 **Network Insight 首頁** 頁面。如果您是要刪除的看板的擁有者，則會快顯一則確認刪除的訊息。
 - 如果另一個使用者已將您建立的看板設定為首頁，則當您刪除時，會為使用者自動將首頁復原為 **Network Insight 首頁**。
-

結果

複製看板

程序

- 1 對於看板程式庫清單中的特定看板，按一下**動作**下的複製圖示。



- 2 此時會出現快顯視窗，您必須在其中輸入看板的名稱。此說明與原始看板的說明相同。按一下**複製**。

備註 看板的名稱為必填。在輸入名稱之前，**複製**按鈕不會啟用。

- 3 如果您嘗試複製已共用的看板，您可以選擇保留來源看板使用者和權限。如果要保留它們，請選取**保留來源看板使用者和權限**。

備註 如果要複製的看板與具有唯讀存取權的您共用，您將無法看到**保留來源看板使用者和權限**選項。

複製看板的使用者將成為新看板的擁有者。

vRealize Network Insight 中的負載平衡器支援

15

透過負載平衡，可以在多個後端目的地 (包括公有雲或私有雲中的部署) 之間散佈輸入應用程式流量。因此，必須具備後端目的地集合的概念。

vRealize Network Insight supports the following load balancing devices.

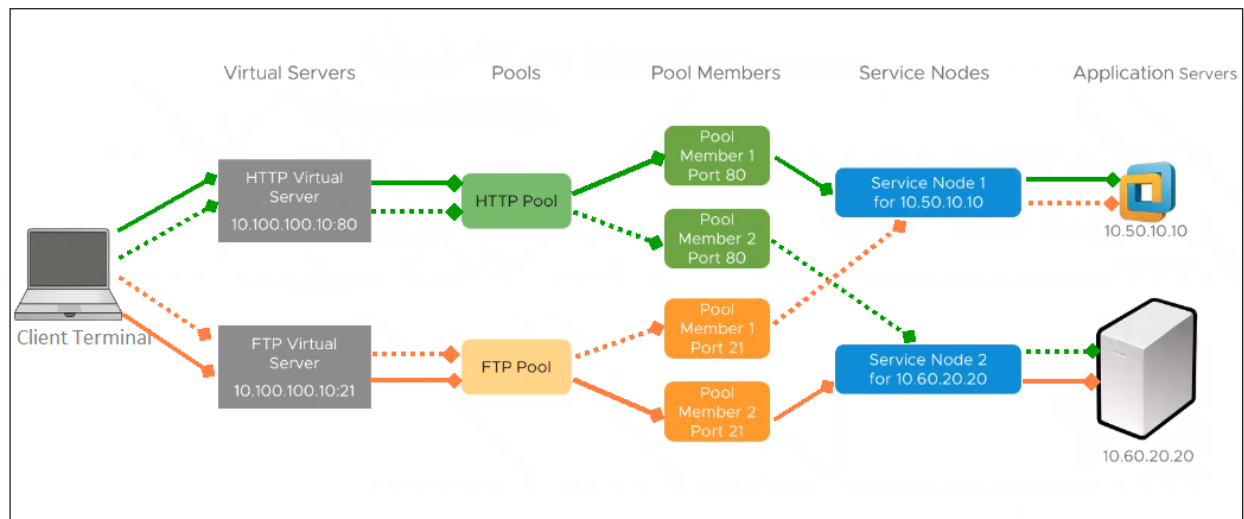
本章節討論下列主題：

- F5 作為負載平衡器
- NSX-V 做為負載平衡器

F5 作為負載平衡器

若要支援並啟用 F5 的負載平衡功能，vRealize Network Insight 新增了所需的元件或實體。

F5 負載平衡器及其元件的概觀



- 應用程式伺服器 - 主控應用程式的機器。例如，如果您有 Web 伺服器，您的伺服器會在應用程式伺服器 (實體或虛擬伺服器) 上執行。
- 服務節點 - F5 代表做為服務節點的應用程式伺服器。因此，服務節點具有與應用程式伺服器相同的 IP 位址或 FQDN。每個服務節點可以有多个應用程式。

- 集區成員 - 邏輯實體。服務節點中的每個應用程式由集區成員表示，它具有服務節點的 IP 位址或 FQDN。若要識別不同的應用程式，集區成員會內嵌含服務節點之 IP 位址的連接埠號碼。
- 集區 - 為一個應用程式提供服務的所有集區成員將分組為集區。
- 虛擬伺服器 - 應用程式的公用 IP 位址。因此，想要使用應用程式的用戶端會連線到虛擬伺服器 IP 位址 (例如，10.100.100.10) 和連接埠號碼 (80 或 21)。
- 用戶端終端機 - 連線從用戶端終端機開始，也就是虛擬機器。

用戶端申請連線到虛擬伺服器，這會根據集區決定集區成員。然後，集區成員將申請轉送到應用程式伺服器 (虛擬機器或實體伺服器)。

備註 單一應用程式伺服器可以處理來自不同連接埠和不同服務節點的多個申請。

vRealize Network Insight 還提供負載平衡功能支援的其他優點：

- 能夠識別應用程式伺服器是實體伺服器還是虛擬機器。
- 可讓您透過深入瞭解應用程式伺服器 (主機或虛擬機器) 資訊，例如組態、效能、流量，輕鬆地偵錯或疑難排解問題。
- 可讓您深入瞭解散佈負載的應用程式中的實體或虛擬網路元件。
- 針對環境中的任何問題引發警示，並且有助於偵測此問題的原因。例如，應用程式沒有回應，因為服務節點虛擬機器已關閉。
- 提供端對端流量可見性。

檢視負載平衡器詳細資料

[負載平衡器] 頁面概述了在負載平衡器上建立的虛擬伺服器和集區的所有資訊。

將會顯示以下內容：

- 負載平衡器上的虛擬伺服器及其問題的清單
- 負載平衡器上的集區及其相關聯問題的清單
- 與負載平衡器相關聯的事件
- 不同目的地 IP 上的流量、計數及其網路流量的清單。

備註 不會擷取 NSX-V 負載平衡器的流量資訊。

- 提供廠商、類型、序號、虛擬伺服器、集區等資訊的負載平衡器的內容。

檢視虛擬伺服器詳細資料

[虛擬伺服器] 頁面包括虛擬伺服器度量以及問題和變更事件。

將會顯示以下內容：

- 虛擬伺服器中的所有集區成員的清單及其詳細資料，以及任何問題的警示。
- 虛擬機器的清單

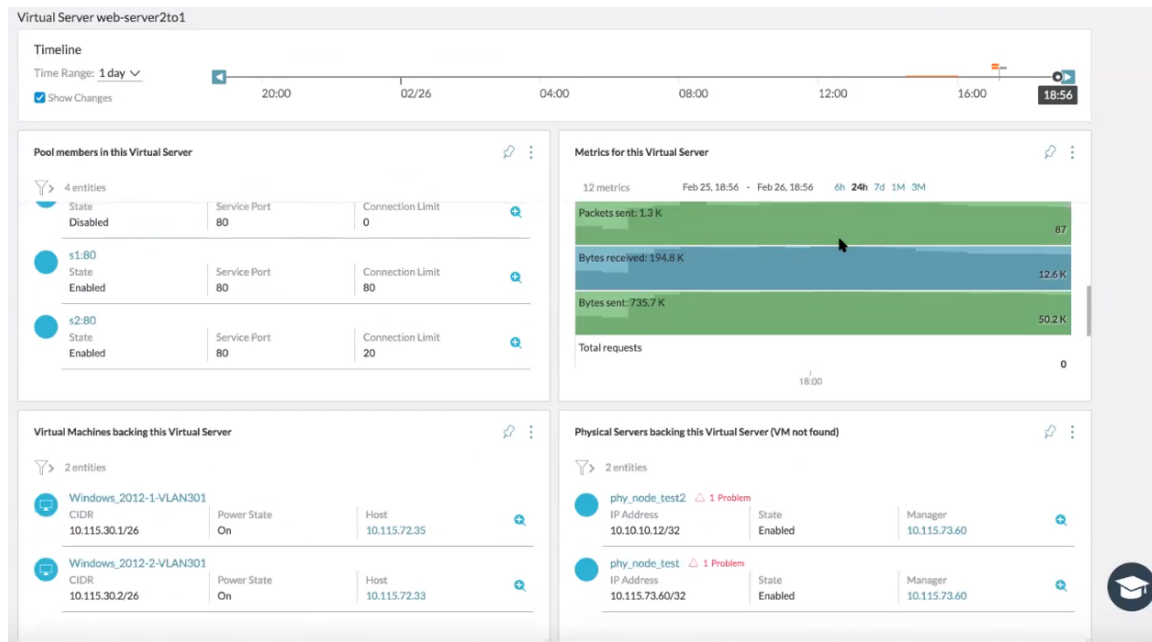
- 實體伺服器的清單
- 與虛擬伺服器相關聯的問題事件的清單
- 與虛擬伺服器相關的度量的清單，例如：
 - 連線 (計數、持續時間)
 - 網路度量 (傳送或接收的封包和位元組數)
 - CPU 使用率

備註 如需受支援的 NSX-V 負載平衡器度量的清單，請參閱[支援的 NSX-V 度量](#)。

- 此虛擬伺服器使用的集區成員的前幾個流量。

備註 不會擷取 NSX-V 負載平衡器的流量資訊。

- 虛擬伺服器內容，提供有關負載平衡器 IP 位址、網路流量、服務連接埠的資訊。



若要檢視與負載平衡器相關聯的拓撲路徑，您可以使用下列查詢：`client VM name to Virtual server IP`。如果不同的服務連接埠上有多個虛擬伺服器，則會在 [選取目的地虛擬機器] 區段下顯示清單。您可以從清單中選取伺服器，然後按一下 **顯示路徑** 以查看虛擬機器至虛擬伺服器路徑。

您可以按一下虛擬機器路徑拓撲上的虛擬伺服器，以查看 [虛擬伺服器] 視窗上的一組虛擬機器。按一下 **檢視路徑** 以查看虛擬伺服器至所選虛擬機器的路徑。

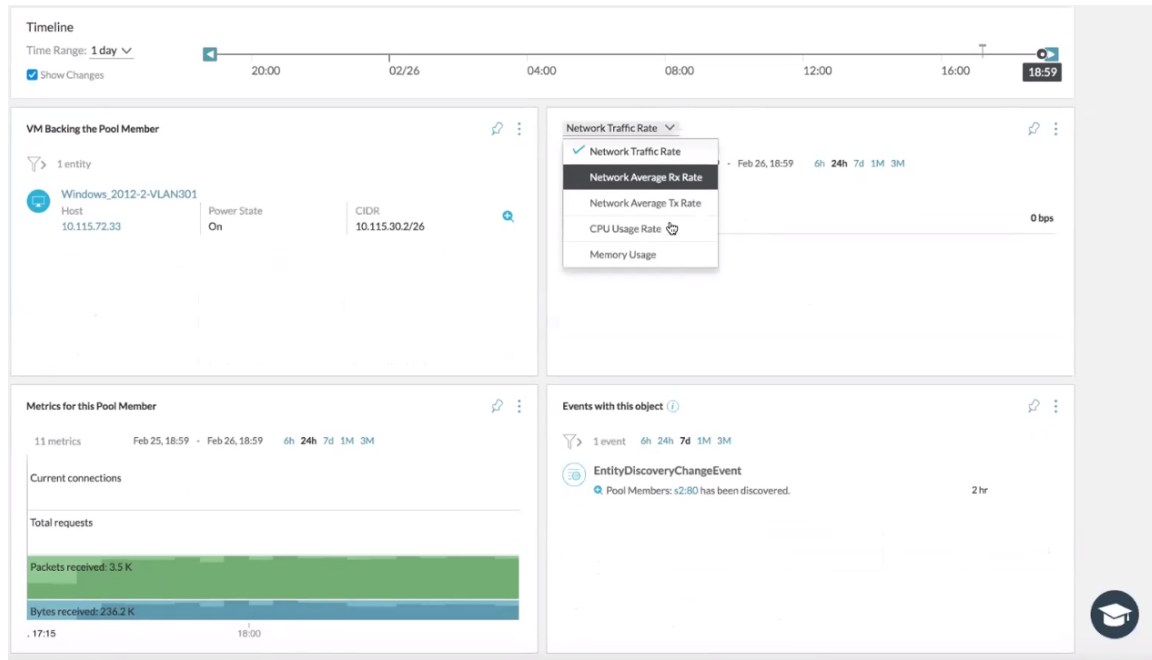
檢視集區成員詳細資料

[集區成員] 頁面會提供有關集區成員、度量以及與集區成員相關聯的事件的見解。

將會顯示以下內容：

- 虛擬機器的清單和虛擬機器的其他詳細資料

- 可讓您將集區成員的度量與虛擬機器的度量進行比較。例如，記憶體和 CPU 使用率、網路流量。
- 與集區成員相關的度量的清單，例如：
 - 連線 (計數、持續時間、存留期)
 - 網路度量 (傳送或接收的封包和位元組數)
 - CPU 使用率
- 提供負載平衡器、節點、狀態、服務連接埠的相關資訊的集區成員內容。



與負載平衡器相關的範例搜尋查詢

您可以使用下列範例查詢篩選或搜尋與負載平衡器相關的資料。

- `vm where lbServiceNodes is set` - 列出主控散佈負載的應用程式的所有虛擬機器。
- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'` - 列出主控負載平衡應用程式，但目前無法正常運作的所有虛擬機器。
- `pool member where state = 'DISABLED'` - 列出所有已停用的集區成員。
- `Count of Pool Memebers where Service Port = '80'` - 提供在連接埠 80 上執行的某種特定服務類型的所有集區成員的計數。
- `service node where virtual machine is not set` - 列出將實體伺服器用作應用程式伺服器的所有服務節點，或 vRealize Network Insight 中未新增主控虛擬機器的 vCenter Server

NSX-V 做為負載平衡器

從 4.2 版本開始，vRealize Network Insight 支援並啟用 NSX-V 的負載平衡功能。

以下是目前支援的度量的清單：

- 虛擬伺服器
 - 傳入的位元組總計
 - 傳出的位元組總計
 - 目前工作階段數
 - 工作階段總計
- 集區
 - 傳入的位元組總計
 - 傳出的位元組總計
 - 目前連線數
 - 連線數上限
 - 連線總數

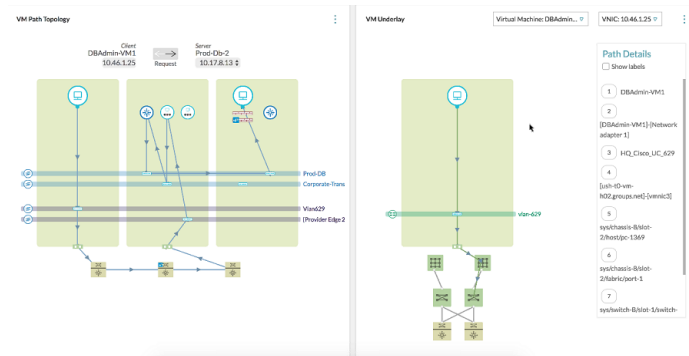
在 vRealize Network Insight 中，目前僅支援將虛擬機器做為集區成員。

本章節討論下列主題：

- 路徑拓撲
- 檢視 BGP 芳鄰詳細資料
- 網際網路路徑

路徑拓撲

路徑拓撲繪製了環境中任何兩個虛擬機器之間存在的詳細連線。



此拓撲涉及第 3 層和第 2 層元件。您可以使用搜尋查詢 `vm_name_1` 至 `vm_name_2` 來檢視此拓撲。如果路徑存在，則虛擬機器-虛擬機器路徑視覺化會繼續填入 `vm_name_1` 至 `vm_name_2` 之間存在的所有元件，也繪製一條動畫路徑。如果路由器是實體路由器，則它們將顯示在邊界外部。

在路徑拓撲中，將會顯示來源和目的地之間的虛擬機器至虛擬機器路徑。如果在虛擬機器之間未設定預設路徑，則會顯示一則錯誤訊息，以通知路徑未定義或找不到路由器介面。

若為 Kubernetes，路徑拓撲會顯示下列案例的路徑：

- Kubernetes 服務至 Kubernetes 服務
- Kubernetes 服務至 Kubernetes 網繭
- Kubernetes 網繭至 Kubernetes 網繭

備註 不支援涉及實體裝置的路徑。

透過負載平衡器的路徑選項會列出在所選來源和目的地虛擬機器的路徑之間使用的所有負載平衡器。若要查看透過特定負載平衡器的虛擬機器之間的路徑，請從清單中選取負載平衡器名稱。如果您將滑鼠暫留在路徑拓撲上的負載平衡器元件上，將會顯示下列詳細資料：

- 虛擬伺服器名稱
- 負載平衡器 IP 位址
- 連接埠號碼
- 負載平衡器演算法
- 已從負載平衡器建立的預設閘道。

您也可以查看路徑拓撲上的路由元件。

如果您將滑鼠暫留在路徑中涉及的任何路由器、Edge 或 LDR 上，則會顯示完整的路由或 NAT 資訊。

位於虛擬機器路徑拓撲右側的 [虛擬機器基礎] 區段會顯示所涉及虛擬機器的基礎資訊，及其與機架交換器頂端和所涉及連接埠的連線。對於 Kubernetes 實體，[虛擬機器基礎] 會顯示網繭所在的虛擬機器或 Kubernetes 節點資訊。

在虛擬機器基礎區段中，如果您選取**路徑詳細資料**下的**顯示標籤**，則對元件進行標記。在此區段中，頂部的下拉式清單會顯示 Edge 上的端點虛擬機器和作用中虛擬機器。對於每個 Edge 虛擬機器，相鄰的下拉式清單會顯示入口和出口介面 IP 位址。根據選取的內容，顯示該特定介面的基礎路徑。

也可以使用拓撲圖頂端的箭頭，反向路徑方向。

透過拓撲圖可讓您更深入地瞭解有關虛擬機器-虛擬機器路徑所涉及連接埠的相關資訊。在**路徑詳細資料**區段中，將會顯示實際連接埠通道的名稱。

備註 在實體正面沒有第 2 層的完整可見性。如果封包從一個交換器周遊到另一個交換器，則可能會涉及多個交換器。但拓撲不會顯示基礎網路中的交換器。

AWS 虛擬機器-虛擬機器路徑

AWS 的虛擬機器-虛擬機器路徑提供內部部署虛擬機器和 AWS EC2 執行個體之間的路徑可見性。

目前，vRealize Network Insight 支援下列案例：

- AWS 內部 VPC 虛擬機器-虛擬機器路徑：此案例涉及特定 VPC 中同一子網路或不同子網路的虛擬機器之間的通訊。
- 透過對等連線的 AWS 內部 VPC 虛擬機器-虛擬機器路徑：此案例涉及一個 VPC 中的虛擬機器與另一個 VPC 中的虛擬機器之間透過對等連線進行的通訊。
- AWS 虛擬機器至網際網路：VPC 中的虛擬機器透過網際網路閘道與網際網路進行通訊。

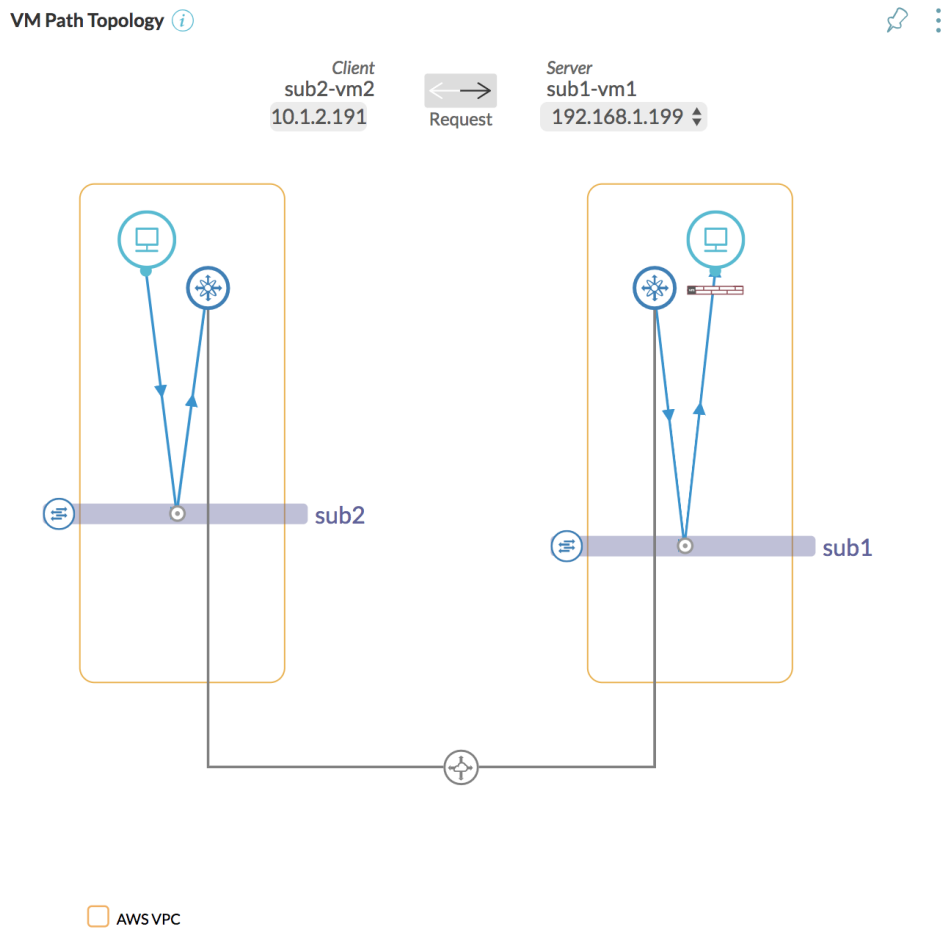
- 透過 AWS VPN 連線的 AWS 虛擬機器到資料中心虛擬機器：在此案例中，VPC 中的虛擬機器透過 AWS VPN 連線與資料中心內的虛擬機器進行通訊。對於此案例，vRealize Network Insight 支援 SDDC、NSX-V 和 NSX-T 資料中心。

備註

- NSX-T 和 NSX-V 資料中心的混合路徑拓撲僅在 NSX-T 和 NSX-V Edge 路由器設定了公用 IP 位址時才有效。
- vRealize Network Insight 不支援 AWS 的虛擬機器基礎拓撲。

備註

透過對等連線的 AWS 內部 VPC 虛擬機器-虛擬機器路徑的 AWS 虛擬機器-虛擬機器路徑範例如下：



您可以透過在虛擬機器-虛擬機器路徑中指向其圖示，來檢視對等連線的內容。

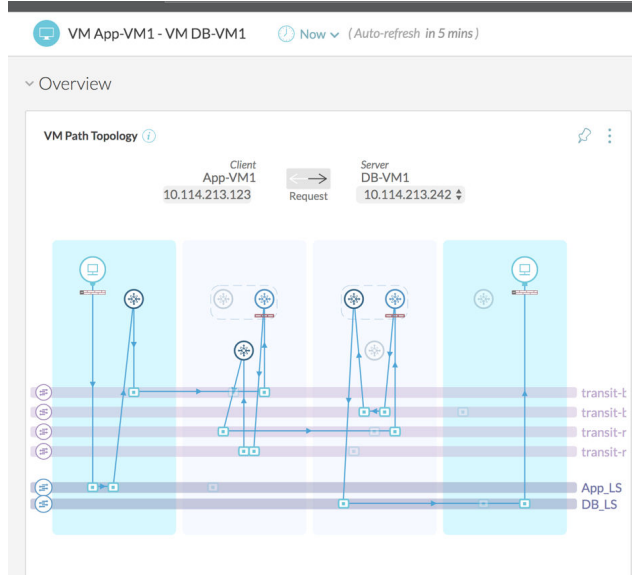
您可以搜尋與 AWS 虛擬機器-虛擬機器路徑相關的下列實體：

- AWS Subnet
- AWS Route Table

- AWS Virtual Private Gateway
- AWS Internet Gateway
- AWS VPN Connection
- AWS VPC Peering Connection

NSX-T

NSX-T 的虛擬機器-虛擬機器路徑範例如下所示：



藍色表示主機節點，灰色代表 edge 節點。畫面右側列出虛擬機器路徑拓撲中使用的圖示，以及路徑詳細資料下的標籤。分散式路由器以相同的色彩顯示，而與其所在的層無關。拓撲圖中服務路由器的色彩會隨相關聯層而變更。所有第 1 層元件均會出現在同一層級，而所有第 0 層元件均會出現在另一個不同的層級。在 NSX-T 中，edge 防火牆用圖進行說明。

若要規劃 NSX-T 網路的安全性，您可以選取 **NSX-T Layer2 網路** 做為範圍，並使用下列查詢：

```
plan NSX-T Layer2 Network '<NAME_OF_NSX_T_LOGICAL_SEGMENT>'
```

您也可以執行下列步驟來達成同樣的目的：

- 從導覽側邊列中選取**安全性**。
- 從下拉式功能表中選取 **NSX-T Layer2 網路** 做為範圍。

備註

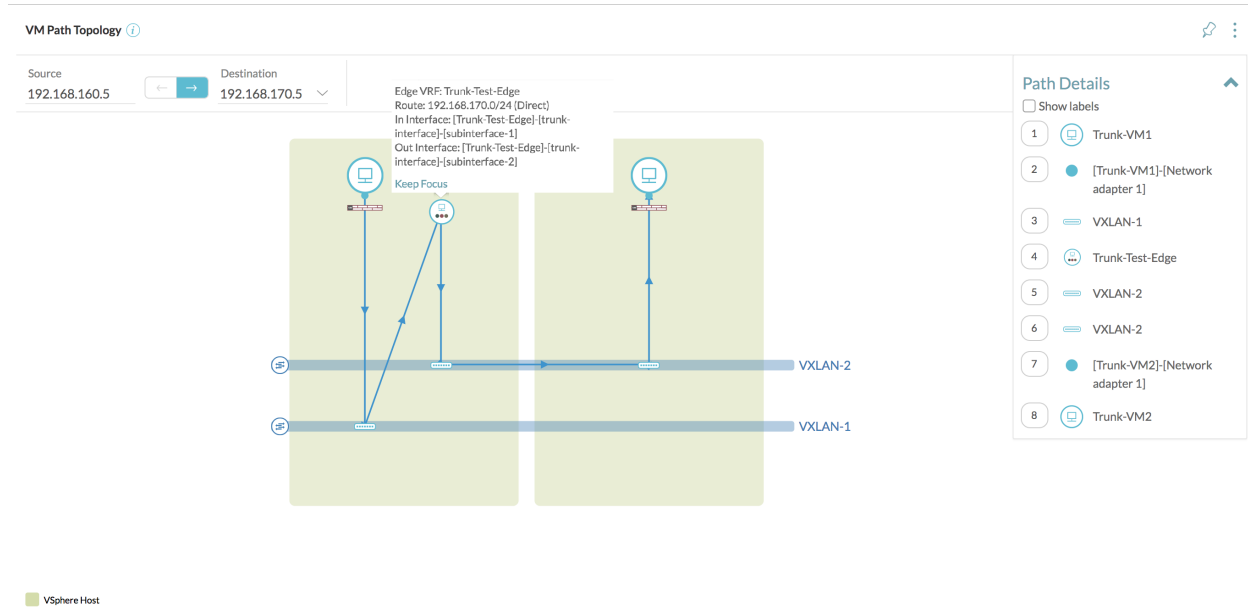
- 範圍中提供了 NSX-T 相關實體，例如 **NSX-T L2 網路** 和**標籤**。您可以在規劃、微分割和應用程式定義中使用這些 NSX-T 相關實體。
- 在**分組依據**下拉式功能表中，**NSX-T 安全群組**是**安全性標籤**的一部分，**邏輯區段**是**VXLAN/VLAN**的一部分。

NSX-V Edge 主幹介面虛擬機器-虛擬機器路徑

在 vRealize Network Insight 中，當 DVPG 連線至 NSX Edge 的主幹 vNIC 並且子介面連線至 VLAN 或 VXLAN 時，您可以檢視虛擬機器-虛擬機器路徑和虛擬機器至網際網路路徑。

以下是透過 NSX Edge 的虛擬機器-虛擬機器路徑的範例：

備註 vRealize Network Insight 不支援 Edge 虛擬機器的主幹介面的基礎資訊。



vRealize Network Insight 中的 NAT 支援

vRealize Network Insight 支援 NSX for vSphere、NSX-T Edge、Fortinet 和 Check Point 的虛擬機器-虛擬機器路徑。

虛擬機器-虛擬機器路徑

採用 NAT 的虛擬機器-虛擬機器路徑範例如下所示：

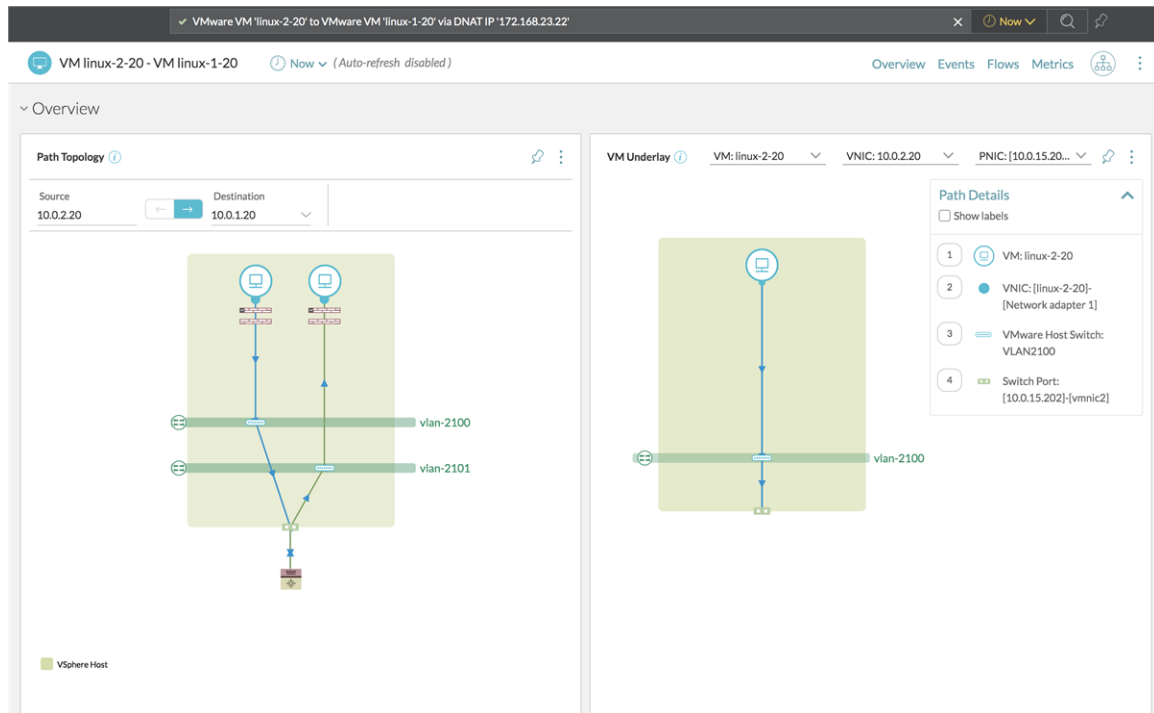
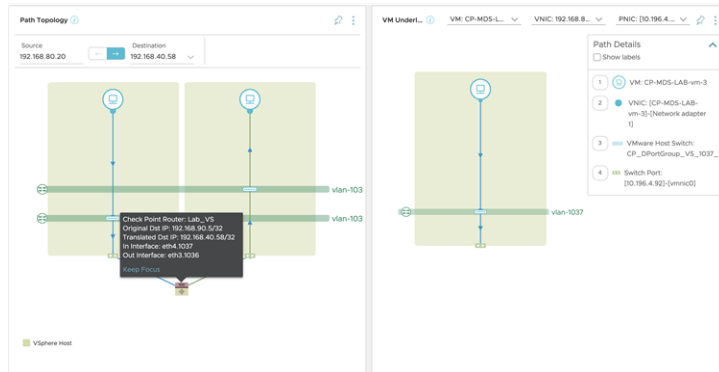


圖 16-1. 透過 Check Point NAT 的虛擬機器-虛擬機器路徑



查詢

若要檢視採用 NAT 的虛擬機器-虛擬機器路徑，請使用下列查詢：

- 如果目的地虛擬機器位於 Fortinet 和 Check Point 路由器後方，且已設定 NAT，請使用 VMware VM '<name of the VM>' to VMware VM '<name of the VM>' via DNAT 查詢。
- 如果目的地虛擬機器位於 NSX for vSphere 或 NSX-T Edge 的後方，且已設定 NAT，請使用 VMware VM '<name of the VM>' to VMware VM '<name of the VM>' 查詢。

考量事項

- 對於具有已啟用 NAT 服務的 NSX-T 邏輯路由器的虛擬機器-虛擬機器路徑，vRealize Network Insight 不會為此類路徑正確顯示 NSX-T Edge 防火牆規則。

VMware SD-WAN 虛擬機器-虛擬機器路徑

在 vRealize Network Insight 中，您可以檢視 VMware SD-WAN 部署的虛擬機器-虛擬機器路徑。

vRealize Network Insight 支援下列案例：

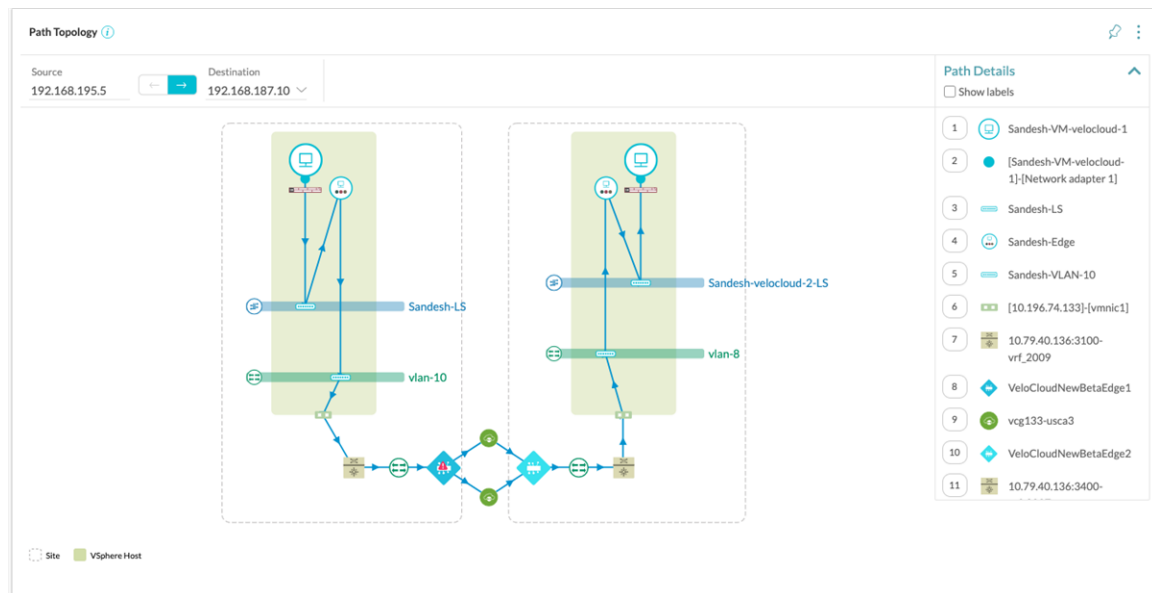
- IP 至 IP 路徑：兩個 IP 都必須直接位於 VMware SD-WAN Edge 後方的 VLAN 上。
- IP 至網際網路/IP 至未知 IP：來源 IP 必須直接位於 VMware SD-WAN Edge 後方的 VLAN 上。

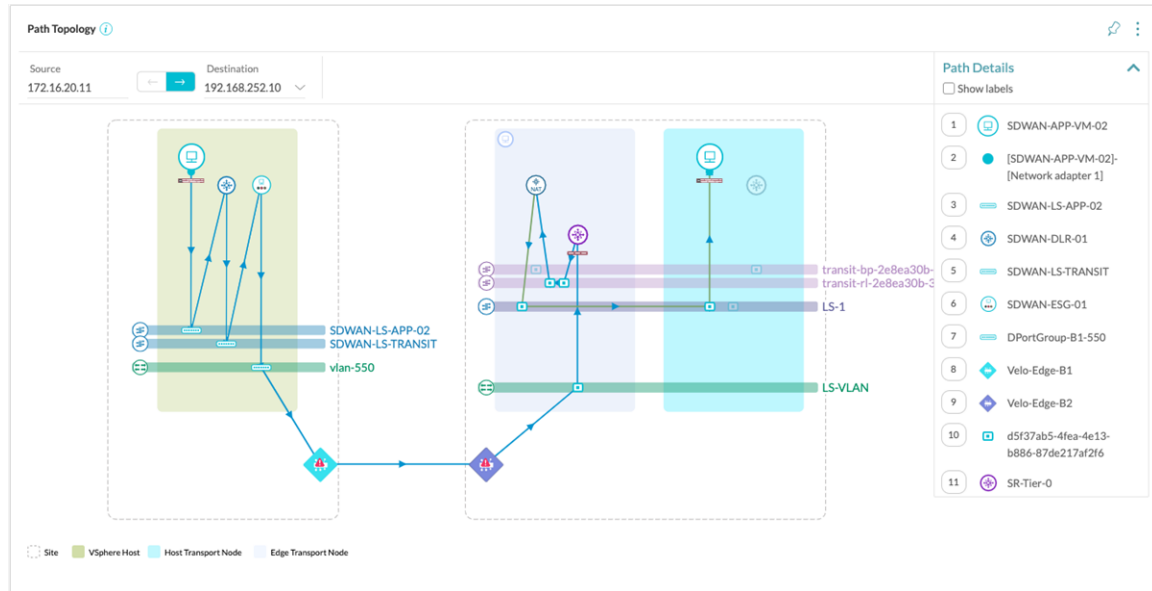
備註 網際網路或未知 IP 是指在 vRealize Network Insight 中未探索到的任何 IP。

- 虛擬機器至 IP、IP 至虛擬機器或虛擬機器至虛擬機器路徑：
 - 僅支援 NSX/NSX-T 資料中心中的虛擬機器。不支援 VMware Cloud on AWS、Amazon Web Services 和 AZURE 中的虛擬機器。
 - VMware SD-WAN Edge 必須透過 VLAN 連線至資料中心內的實體/虛擬路由器。
- **備註** 如果為來源 VMware SD-WAN Edge 和目的地 VMware SD-WAN Edge 設定的 VMware SD-WAN 閘道不相同，則會透過來源 VMware SD-WAN Edge 的閘道顯示路徑。

如果 VMware SD-WAN Edge 之間的分支至分支 VPN 經過 VMware SD-WAN 叢集，則該叢集的所有成員都將顯示在路徑中。

以下是 VMware SD-WAN 虛擬機器-虛擬機器路徑的一些範例：





Arista 硬體 VTEP 虛擬機器-虛擬機器路徑

在 vRealize Network Insight 中，可以在虛擬機器-虛擬機器路徑中檢視硬體 VTEP。

目前，vRealize Network Insight 支援下列案例：

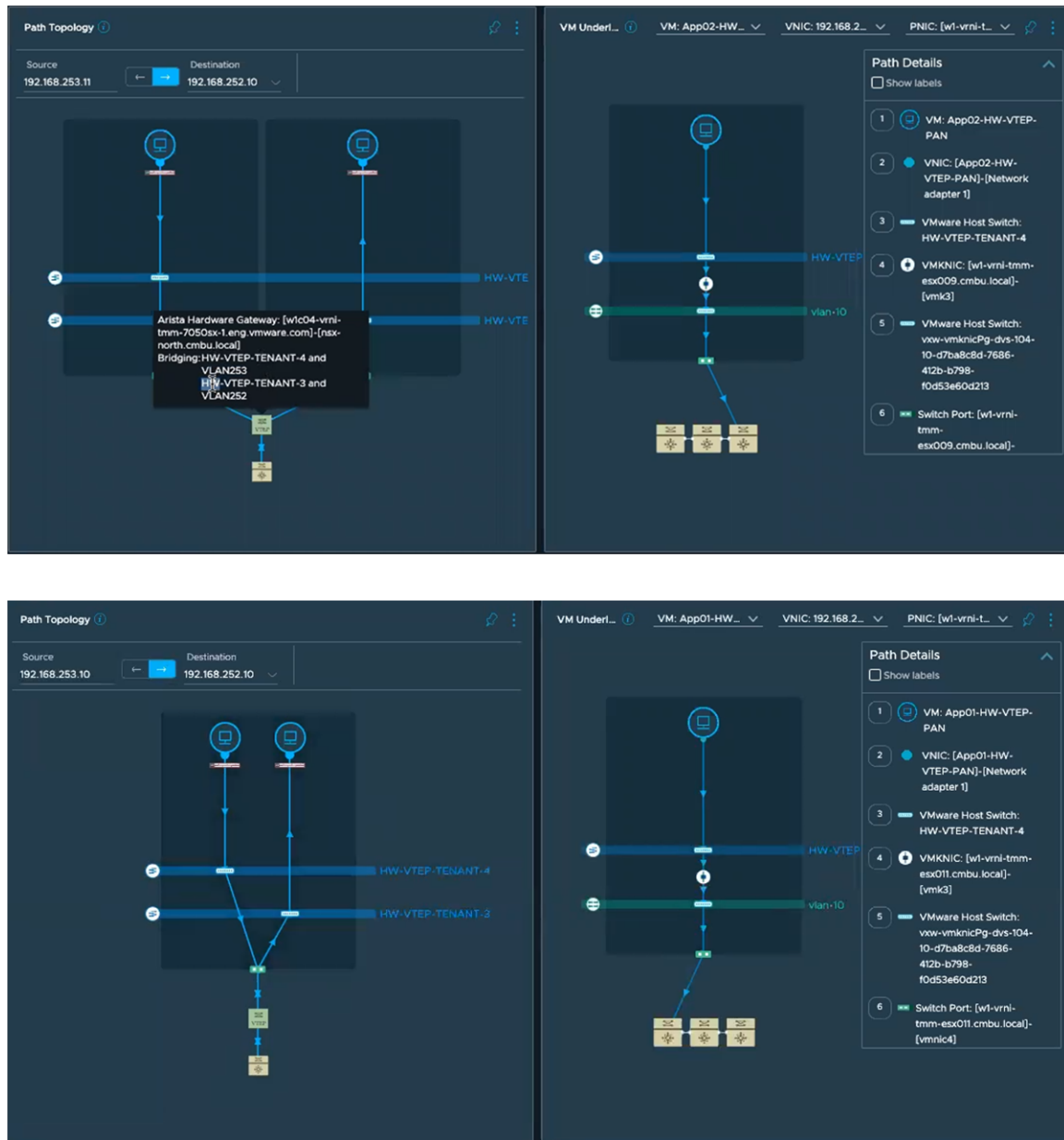
- 當來源和目的地虛擬機器位於不同的 VXLAN 和不同的主機時，採用硬體 VTEP 的虛擬機器-虛擬機器路徑。
- 當來源和目的地虛擬機器位於同一主機但不同的 VXLAN 時，採用硬體 VTEP 的虛擬機器-虛擬機器路徑。
- 當交換器直接連線到主機時，虛擬機器底層拓撲中的硬體 VTEP。

備註 當您在 vRealize Network Insight 中將 Arista 交換器 SSH 新增為資料來源時，必須使用您在 VMware NSX Manager 中用於設定 Arista 交換器 SSH 的同一 IP/FQDN。否則，在虛擬機器-虛擬機器路徑中看不到硬體 VTEP。

如果在虛擬機器與網際網路之間可使用硬體 VTEP，則還可以在虛擬機器拓撲和虛擬機器至網際網路路徑中檢視硬體 VTEP。

當來源和目的地虛擬機器位於同一 VXLAN 時，採用硬體 VTEP 的虛擬機器-虛擬機器路徑不受支援。

以下是採用硬體 VTEP 的虛擬機器-虛擬機器路徑的一些範例：



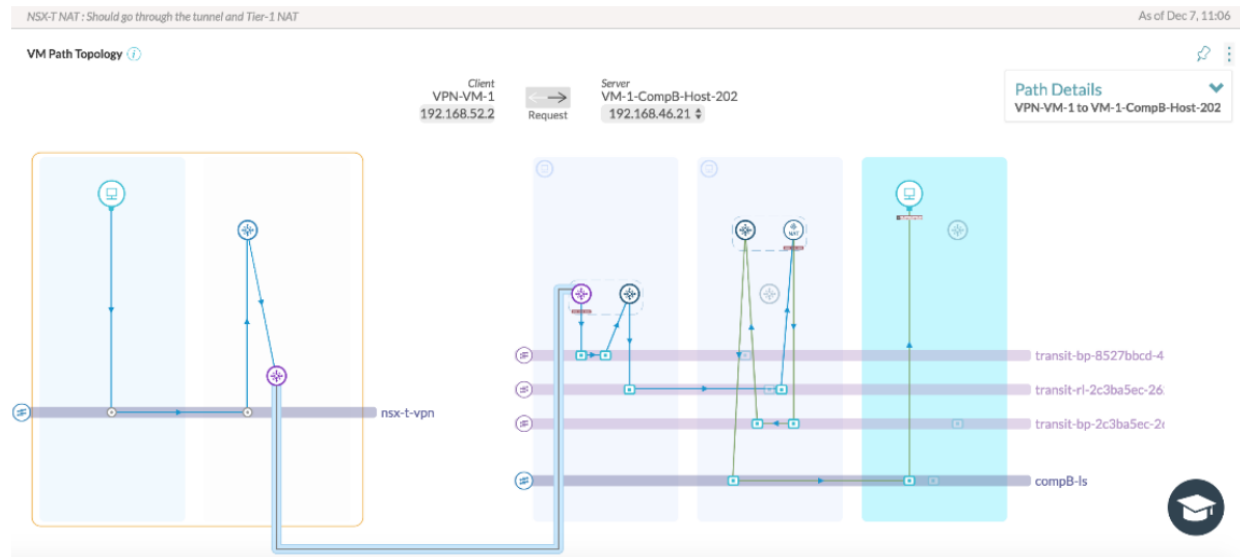
VMware Cloud on AWS：虛擬機器-虛擬機器路徑

vRealize Network Insight 在 VMware Cloud on AWS 中支援下列混合路徑：

- VMware Cloud on AWS 和 VMware Cloud on AWS
- VMware Cloud on AWS 和 NSX-T
- VMware Cloud on AWS 和 NSX-V
- VMware Cloud on AWS 和 AWS
- 內部 VMware Cloud on AWS

對於 VMware Cloud on AWS 中存在的所有虛擬機器，基礎資訊僅顯示到虛擬機器所在的區段，因為網路的基礎實體元素已由 VMware Cloud on AWS 抽出，並且此層級不存在可見性。

VMware Cloud on AWS 和 NSX-T 虛擬機器-虛擬機器路徑的範例如下所示：



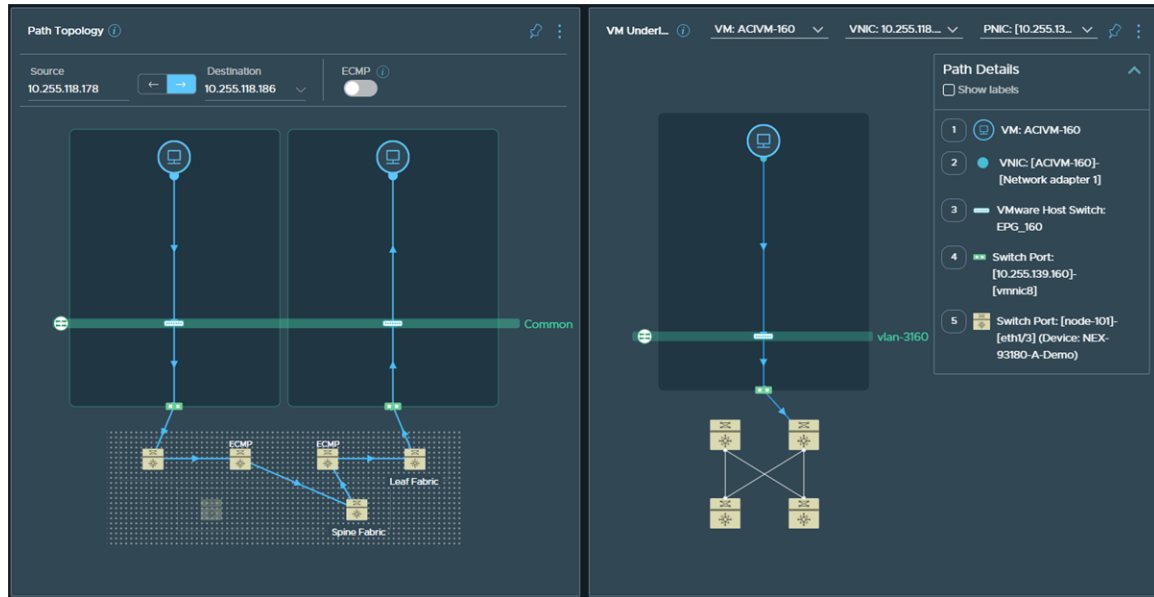
暗藍色線描述通道。

Cisco ACI 虛擬機器-虛擬機器路徑

在 vRealize Network Insight 中，您可以檢視採用 Cisco ACI 的虛擬機器-虛擬機器路徑。

Cisco ACI 的虛擬機器-虛擬機器路徑範例如下所示：

備註 如果 Cisco ACI API 提供交換器層級詳細資料，vRealize Network Insight 會顯示採用分葉和主幹交換器的虛擬機器-虛擬機器路徑。否則，vRealize Network Insight 會顯示適用於整個網狀架構的單一 Cisco ACI VRF，而不是虛擬機器至虛擬機器路徑中的分葉和主幹交換器。

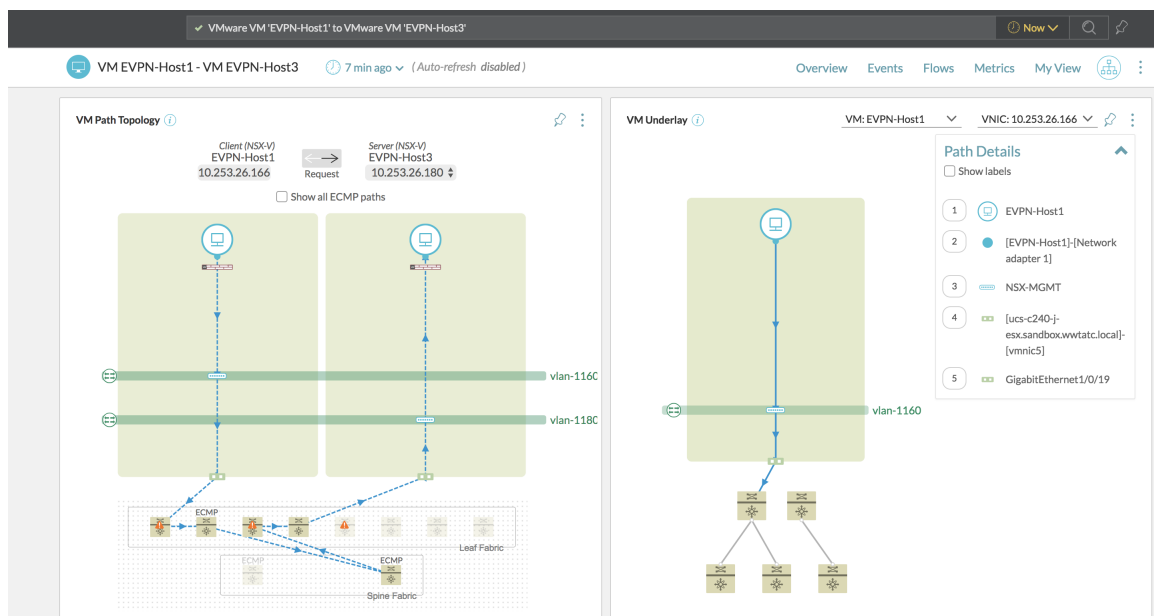


對 Cisco BGP-EVPN 模式的支援

vRealize Network Insight 僅支援在企業版的 Cisco BGP-EVPN 組態模式下設定的 Cisco 9000 交換器的網狀架構。vRealize Network Insight 不支援具有 Cisco BGP-EVPN 組態的 Cisco Nexus 9000 以外的交換器型號。

屬於網狀架構的每個 Cisco Nexus 9000 交換器會被單獨新增為資料來源。若要檢視網狀架構中的所有骨干交換器或分支交換器，請使用 switches where role is set 查詢。

Cisco BGP-EVPN 模式的虛擬機器-虛擬機器路徑的範例如下所示：

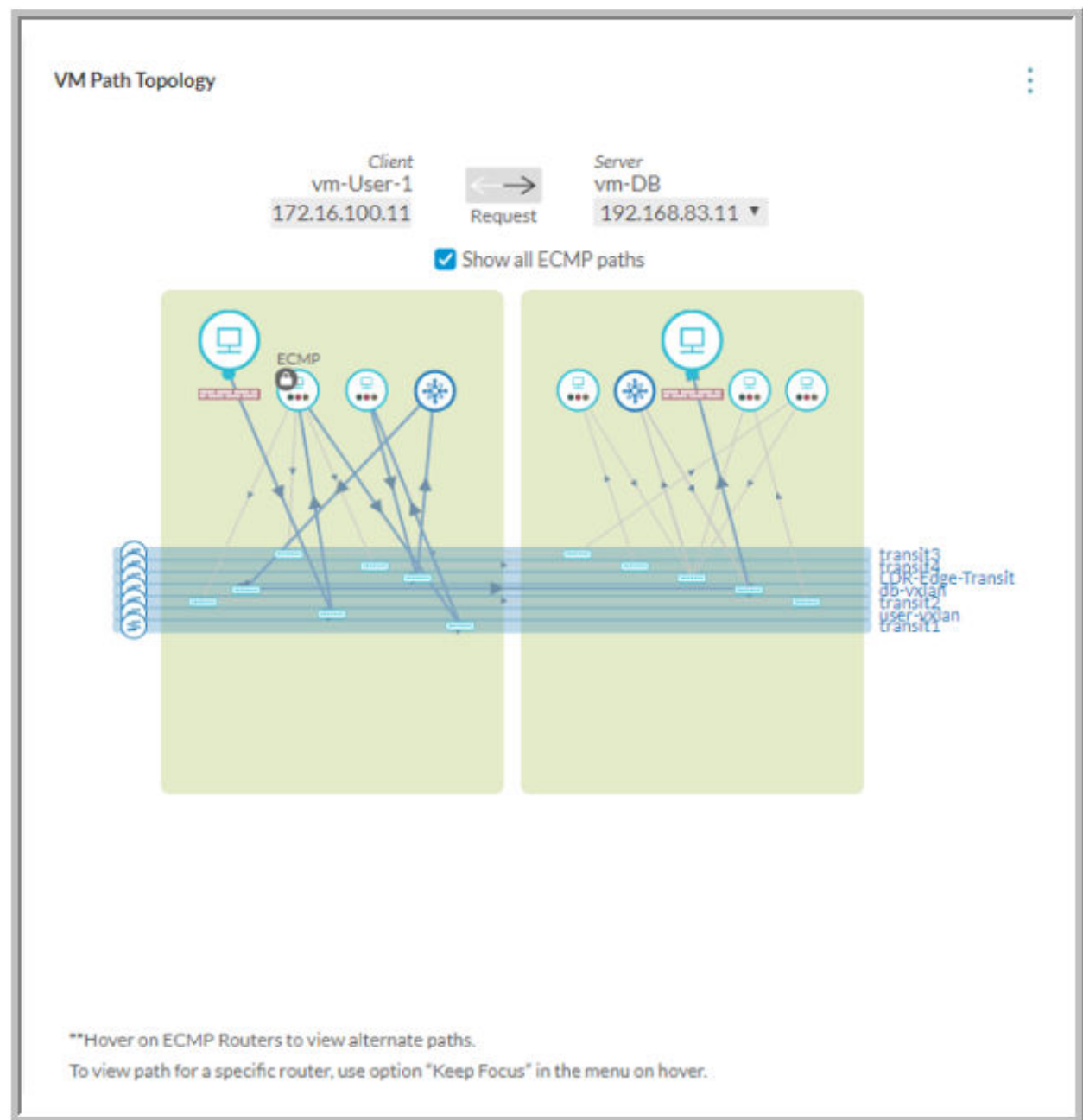


等價多路徑 (ECMP) 路由的支援

vRealize Network Insight 在虛擬機器-虛擬機器路徑中提供 ECMP 支援。

虛擬機器-虛擬機器路徑顯示有關 ECMP 的下列資訊：

- 從來源到目的地的多個 ECMP 路徑
- 實作 ECMP 的路由器
- 指定路由器的可能傳出路徑 (VRF)
- 可能路徑的路由



在上圖中，可以看到已啟用 ECMP 的路由器。如果指向這些路由器，則會顯示其他路徑。此外，也可以視需要選取和鎖定路由器來建立路徑。如果您要檢視兩個虛擬機器之間的所有 ECMP 路徑，請在拓撲圖中顯示所有 ECMP 路徑選項。

如果您要檢視特定路由器的路徑，請指向此路由器，然後按一下**保持焦點**。將顯示特定於此路由器的路徑。

對 L2 橋接的支援

L2 或 VLAN 橋接從多個 VLAN 建立單一廣播網域。在舊版中，如果虛擬機器-虛擬機器路徑涉及兩個或更多個 VLAN 之間的 L2 橋接，則虛擬機器-虛擬機器路徑不起作用。從此版本開始，vRealize Network Insight 支援 L2 橋接。目前僅 Cisco ASA 路由器支援此功能。

檢視 BGP 芳鄰詳細資料

在 vRealize Network Insight 中，您可以查看有關 BGP 芳鄰的各種資訊。您可以檢視 NSX Edge 或邏輯路由器的 BGP 芳鄰。

程序

- 1 在搜尋列中輸入 `Router where bgp= 'Disabled'`，然後按 **Enter**。
- 2 展開清單中的特定路由器以檢視詳細資料。

您可以在 NSX-V 的 BGP 芳鄰下檢視以下資訊：

- IP Address
- Remote AS
- Weight
- Keep Alive Time
- Hold Down Time
- Status

您可以在 NSX-T 的 BGP 芳鄰下檢視以下資訊：

- IP Address
- Remote AS
- Keep Alive Time
- Hold Down Time

■ Status

備註

- 如果未擷取有關芳鄰的相關資訊，則 Status 會顯示為 Unknown。
- 如果 Status 不是 Established.up，則為該 Edge 擲回 One or more BGP neighbours are not in established state 事件。您也可以搜尋 problems 時檢視此事件。

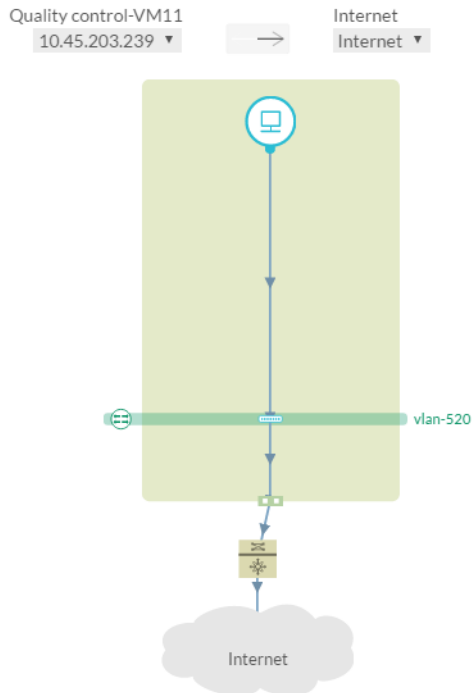
3 (選擇性) 若要查看已停用 BGP 狀態的路由器，請搜尋 Router where bgp= 'Disabled'。

網際網路路徑

對於環境中的每個虛擬機器，vRealize Network Insight 向您顯示如何在網際網路路徑釘選項中使用動畫路徑將虛擬機器連線至網際網路。

該路徑會填入在虛擬機器與網際網路之間存在的所有元件 (虛擬和實體)。它繪製一個依序連線每個元件的動畫路徑。您也可以使用視覺化上方的箭頭，反向路徑方向。

將滑鼠指標指向實體圖示，以取得其可定址名稱。按一下路徑上的圖示，以顯示其主要內容的概觀。您也可以最大化釘選項以檢視路徑詳細資料。



本章節討論下列主題：

- 跨 vCenter NSX
- Palo Alto 網路
- Cisco ASA 防火牆
- Check Point 防火牆
- 安全群組
- 以原則為基礎的 VPN
- NSX 分散式防火牆非作用中規則
- Fortinet 防火牆

跨 vCenter NSX

在跨 vCenter NSX 的環境中，您可以有多個 vCenter Server，每個都必須與其自己的 NSX Manager 配對。

一個 NSX Manager 指派了主要 NSX Manager 角色，而其他 NSX Manager 則指派了次要 NSX Manager 角色。主要 NSX Manager 用於部署通用控制器叢集，該叢集針對跨 vCenter NSX 環境提供控制平面。次要 NSX Manager 不具有其自己的控制器叢集。主要 NSX Manager 可以建立通用物件，例如通用邏輯交換器。這些物件透過 NSX 通用同步服務與次要 NSX Manager 同步。您可以從次要 NSX Manager 檢視這些物件，但無法在其中進行編輯。您必須使用主要 NSX Manager 來管理通用物件。主要 NSX Manager 可用於在環境中設定任何次要 NSX Manager。

支援下列通用物件：

- 通用 LDR
- 通用傳輸區域
- 通用邏輯交換器
- 通用防火牆規則
- 通用安全群組
- 通用 IPSet

- 通用服務
- 通用服務群組
- 通用區段範圍

Palo Alto 網路

vRealize Network Insight 支援 Palo Alto Panorama 防火牆。

備註 vRealize Network Insight 不支援 Palo Alto Panorama 與多個 NSX Manager 整合。

若要在 vRealize Network Insight 中新增 Palo Alto Panorama，Palo Alto 網路使用者必須擁有具有 XML API 存取權的**管理員角色**。在 **Paloalto Networks** 使用者介面中，執行下列步驟為 XML API 新增管理員角色。

- 1 選取 **Panorama > 管理員角色**。
- 2 按一下**新增**以新增管理員角色。
- 3 [管理員角色設定檔] 視窗隨即開啟。
- 4 輸入角色的名稱，然後選取 **Panorama**。
- 5 按一下 **Web 使用者介面**索引標籤，並停用所有項目。
- 6 按一下 **XML API** 索引標籤，然後停用除**組態**和**運作要求**之外的所有項目。
- 7 按一下**確定**以關閉視窗。
新的管理員角色即顯示在清單中。
- 8 按一下**認可**。
- 9 將此角色指派給管理員帳戶，或建立新使用者並將此角色指派給新使用者。

vRealize Network Insight 支援的 Palo Alto 網路功能如下所示：

- Palo Alto 和 NSX 實體的關聯性：Palo Alto 網路的位址和位址群組的虛擬機器成員資格是以 IP 位址到虛擬機器之間的對應進行計算。可以透過下列方式查詢此成員資格資訊：
 - `VM where Address = <>`
 - `Palo Alto address where vm = <>`
 - `VM where Address Group = <>`
 - `Palo Alto address group where vm = <>`

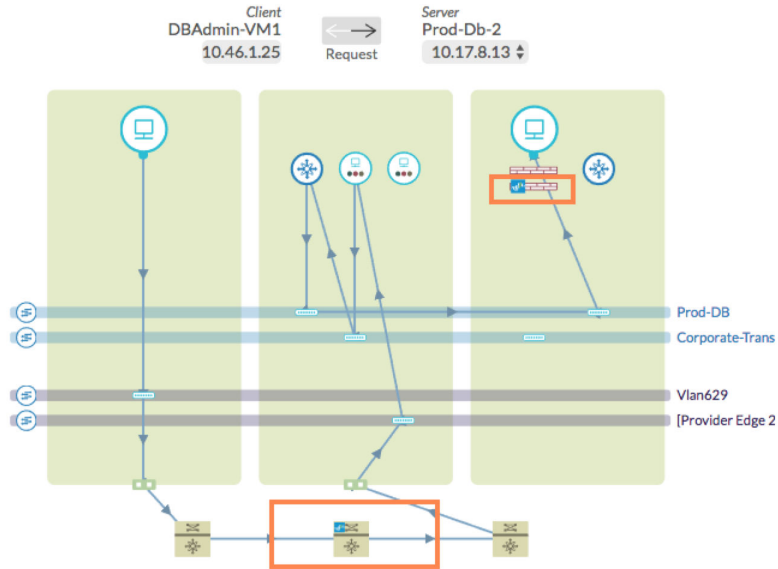
- 查詢：您可以對 vRealize Network Insight 支援的所有 Palo Alto 實體執行查詢。所有實體都以 Palo Alto 為前置詞。一些查詢如下所示：

表 17-1.

實體	查詢
Palo Alto 位址	Palo Alto address where vm = <> VM where Address = <>
Palo Alto 位址群組	Palo Alto address group where Translated VMs = <> VM where address group = <>
Palo Alto 裝置	Palo Alto Device where Version = <> Palo Alto Device where connected = true Palo Alto Device where family = 'PA-5060'
Palo Alto 實體裝置	Palo Alto Physical Device where model = 'PA-5060'
Palo Alto 虛擬機器裝置	Palo Alto VM Device where model = 'PA-VM'
Palo Alto 裝置群組	Palo Alto Device Group where device = <> Palo Alto Device Group where address = <> Palo Alto Device Group where address group = <>
Palo Alto 服務	Palo Alto service where Port = <> Palo Alto service where Protocol = <>
Palo Alto 服務群組	Palo Alto service group where Member = <>
Palo Alto 原則	Palo Alto Policy where Source vm = <> and Destination vm = <> Palo Alto Policy where Source IP = <> and Destination IP = <>
Palo Alto 防火牆	Palo Alto firewall where Rule = <>
Palo Alto 區域	Palo Alto Zone where device = <>
Palo Alto 虛擬系統	Palo Alto Virtual System where Device = <> Palo Alto Virtual System where Device Group = <>

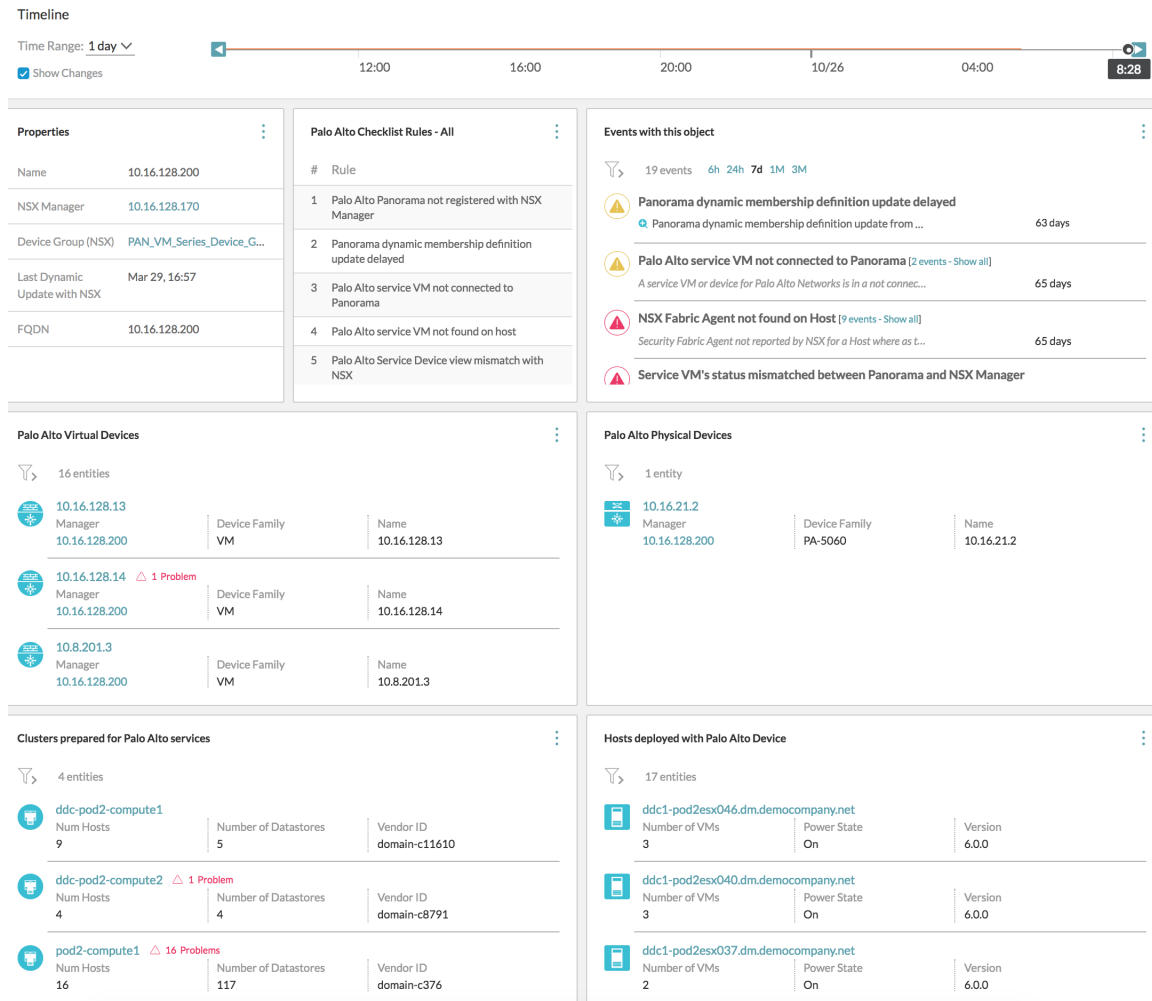
備註 除了查詢之外，也可以使用面來分析搜尋結果。

- 虛擬機器至虛擬機器路徑：做為虛擬機器-虛擬機器拓撲的一部分，vRealize Network Insight 在主機上顯示 Palo Alto 虛擬機器系列防火牆。按一下防火牆圖示時，會顯示適用的規則。如果 Palo Alto 網路的防火牆裝置 (路由裝置) 也存在於路徑中，則也會顯示此裝置。按一下應用裝置圖示時，您會看到基本資訊，例如路由表、介面和包含已套用防火牆規則的資料表。



- 您可以檢視與 Palo Alto 網路的下列案例相關的一些系統事件：
 - Palo Alto 裝置未連線至 Panorama (管理程式)
 - NSX Manager 未在 Panorama 登錄
 - 在 palo alto 裝置的 ESX 上找不到 NSX 網狀架構代理程式
 - 在 NSX 網狀架構代理程式的 Panorama 上找不到 Palo alto 裝置
 - 安全群組成員資格資料不同步
- 您可以使用指定的 NSX manager 在 Panorama 中建立和登錄多個服務定義。如果不同的 ESXi 叢集具有需要虛擬機器系列防火牆以不同方式處理流量的工作負載，則您建立多個服務定義。每個服務定義都有從中選取原則的關聯裝置群組。在 vRealize Network Insight 中顯示虛擬機器-虛擬機器路徑時，應考慮基於虛擬機器叢集資訊的正確原則集。

Palo Alto Manager 儀表板範例

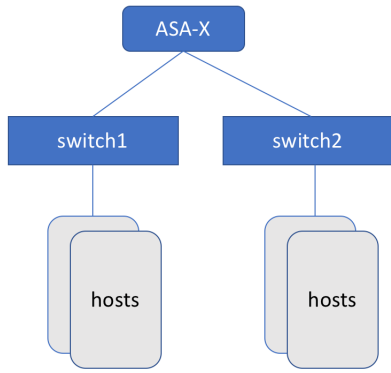


Cisco ASA 防火牆

vRealize Network Insight 支援 Cisco ASA 防火牆。

Cisco ASA 防火牆的功能如下所示：

- vRealize Network Insight 僅支援 Cisco ASA-X 系列。
- vRealize Network Insight 不支援 Firepower 模組。
- 目前，vRealize Network Insight 支援 Cisco ASA 作業系統版本 9.4。
- vRealize Network Insight 不支援 Cisco ASA 的叢集部署。
- vRealize Network Insight 不支援 Cisco ASA 的高可用性。
- 如果 Cisco ASA 直接連線到主機，則不受 vRealize Network Insight 支援。支援類似下列內容的拓撲：



- 僅支援 `Extended` 類型的 Cisco ASA 存取規則。不支援其他存取規則類型，例如 `Standard`、`WebType`、`EtherType` 等。
- 如果在 `Transparent` 模式下設定防火牆，則虛擬機器至虛擬機器路徑中的 Cisco ASA 防火牆不會顯示適當的存取規則。

範例

您可以對 vRealize Network Insight 支援的所有 Cisco ASA 實體執行查詢。

表 17-2.

Cisco ASA 中的實體	關鍵字	範例查詢
安全內容	ASA 防火牆 ASA 安全內容	<code>asa firewall where access group = <></code>
存取規則	ASA 存取規則	<code>asa access rule where source ip = <></code> <code>asa access rule where destination ip = '192.168.2.2'</code> <code>asa access rule where port = <></code> <code>asa access rule where interface = <></code>
存取群組	ASA 存取群組	<code>asa access group where interface = <></code>
網路物件/網路物件群組	ASA 網路物件 ASA 網路物件群組	<code>asa network object where ip address = <></code> <code>asa network object group where ip address = <></code>
服務物件/服務物件群組	ASA 服務物件 ASA 服務物件群組	<code>asa service object where port = <></code> <code>asa service where protocol = <></code> <code>asa service object group</code>

Check Point 防火牆

Check Point 管理伺服器應接受來自收集器 IP 位址的 API 存取。

可以從**管理與設定 > 刀鋒型伺服器 > 管理 API > 進階設定**設定存取權。

如果將 Check Point MDS 新增為資料來源，則 vRealize Network Insight 會從使用者定義的所有網域和全域網域擷取資料。

vRealize Network Insight 使用 Check Point 公用 Web API 從 Check Point 管理伺服器擷取資料。如果 VSX 閘道已連結至管理伺服器，我們會使用以 SSH 為基礎的 CLI 命令擷取 VSX 管理的虛擬系統 VS 路由表，以支援在虛擬機器-虛擬機器路徑中顯示 VS 閘道。

vRealize Network Insight 需要對 Web-API 存取的唯讀權限，以擷取大多數 Check Point 資料。以下是幾個例外狀況：

- 如果非 VSX 實體閘道已連結至管理伺服器，使用者應具有對 Web API 的讀寫存取權限。若要擷取閘道路由以將 `run script` Web API 用於虛擬機器-虛擬機器路徑計算，這一點是必要的。
- 如果 VSX 閘道已連結至管理伺服器，使用者應具有使用相同密碼的 SSH 存取權限。此外，使用者也應具有對 CLI 命令 `vsx_util view_vs_conf` 的存取權限。此指令可用於擷取虛擬機器-虛擬機器路徑計算的 VSX 閘道路由。
- 若要使 MDS 伺服器 IP 做為資料來源，使用者應具有對所有網域 (包括 MDS 網域和全域網域) 的 Web API 存取權限。需要從所有網域中擷取規則、原則套件和其他資料。

您可以對 vRealize Network Insight 支援的所有 Check Point 實體執行查詢。所有實體均以 Check Point 為前置詞。Check Point 的一些查詢如下所示：

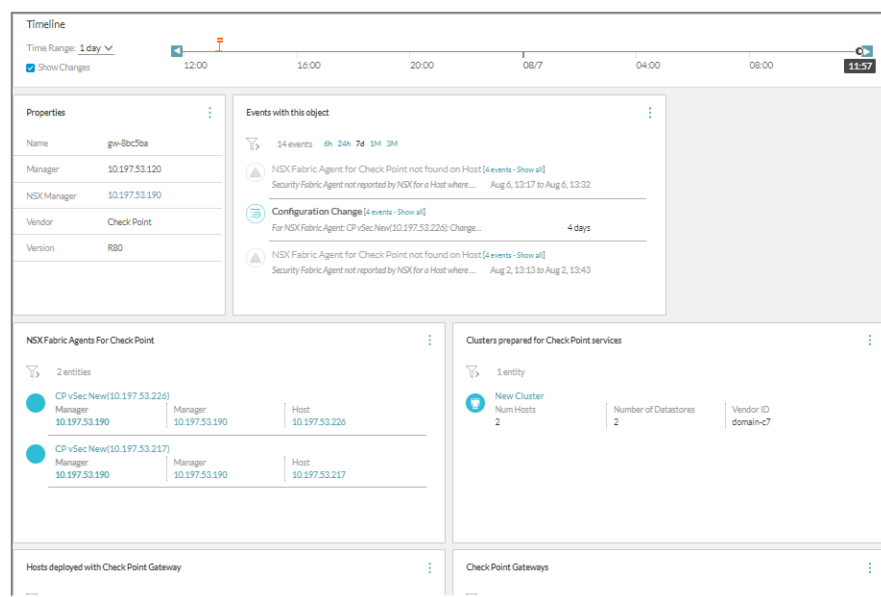
表 17-3.

Check Point 中的實體	關鍵字	查詢
IPset	Check Point Address Range	<code>vm where Address Range = <></code>
	Check Point Network	<code>vm where Address Range = <></code>
		<code>Check Point Address Range where Translated VM = <></code>
群組	Check Point Network Group	<code>Check Point Network Group where Translated VM = <></code>
		<code>vm where Network Group = <></code>
服務/服務群組	Check Point Service	<code>Check point service where Port = <></code>
	Check Point Service Group	<code>Check point service where protocol = <></code>
存取層	Check Point Access Layer	<code>Check Point Policy where Access Layer = <></code>
網域	Check Point Domain	<code>check point domain where ip address = <></code>
		<code>check point policy where domain = <></code>
		<code>check point access layer where domain = <></code>
閘道和閘道叢集	Check Point Gateway	<code>Check Point Gateway Cluster where Policy Package = <></code>
	Check Point Gateway Cluster	

表 17-3. (續)

Check Point 中的實體	關鍵字	查詢
原則套件	Check Point Policy package	Check Point Policy where Policy Package = <> Check Point Policy Package where Rule = <>
原則	Check Point Policy	Check point policy where source ip = <> and Destination IP = <> Rule where source ip = <> and Destination IP = <> (will display other rules- nsx, redirect along with check point policies in the system)

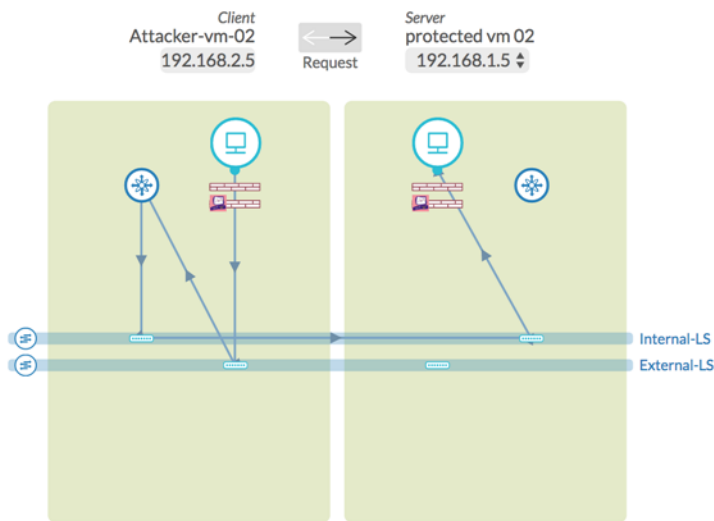
Check Point 管理程式儀表板的範例如下所示：



在虛擬機器-虛擬機器拓撲圖中，您可以查看主機上的 Check Point 服務虛擬機器，以表示特定流量上套用的檢查點規則。VSX 管理的虛擬系統 (VS) 閘道可在虛擬機器-虛擬機器路徑中視為實體閘道。按一下閘道圖示時，會顯示適當 Check Point 原則的清單。

備註 對於虛擬機器-虛擬機器路徑，vRealize Network Insight 不支援包含虛擬交換器和虛擬路由器的 VSX 叢集。

VM Path Topology



以下是針對 Check Point 產生系統事件的一些案例：

- 在 Check Point 閘道的 ESX 上找不到 NSX 網狀架構代理程式。
- 找不到 Check Point 服務虛擬機器。
- Check Point 閘道 `sic` 狀態為未通訊。
- Check Point 實體 (例如位址範圍、網路、原則、群組、原則套件、服務、服務群組等) 的探索與更新事件功能

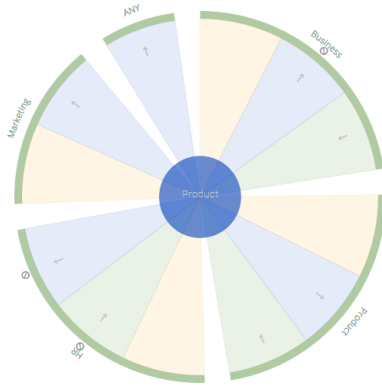
安全群組

安全群組是透過通用權限集進行管理的群組的集合。

安全群組拓撲具有下列兩種視圖：

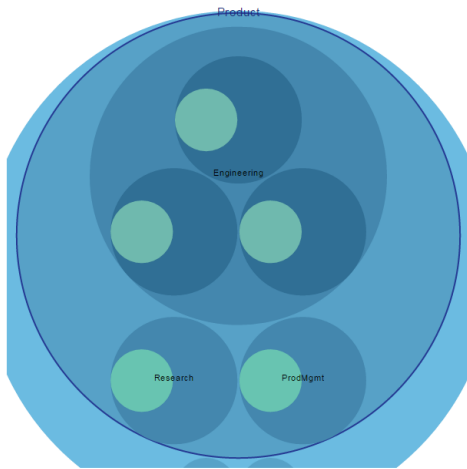
防火牆視圖

安全群組防火牆拓撲透過呈現安全群組之間適用的防火牆規則，以顯示所選安全群組與其他安全群組之間的關係。



容器視圖

安全群組容器拓撲顯示如何相對於其父安全群組或子系 (安全群組或其他實體) 來建構安全群組。



以原則為基礎的 VPN

vRealize Network Insight 在 VMware Cloud on AWS、NSX-T 和 NSX-V 中支援以原則為基礎的 VPN。以原則為基礎的 VPN 支援下列案例：

- VMware Cloud on AWS 公用 IP 位址與 NSX-V/NSX-T/AWS 公用 IP 位址之間的 VPN 通道
- 從 VMware Cloud on AWS 公用 IP 位址和公司防火牆公用 IP 位址至公司防火牆公用 IP 位址與內部 NSX Edge 之間 1:1 NAT 的 VPN 通道

備註 vRealize Network Insight 不支援 VPN 通道來自 VMware Cloud on AWS (結束於公司防火牆)，且未使用內部 NSX Edge 設定 NAT 的案例。

以原則為基礎的 VPN 實體

vRealize Network Insight 為 L3 VPN Session 實體擷取資料，該實體是在資料中心內設定的實際 VPN。

以下是以原則為基礎的 VPN 實體的搜尋詞彙：

表 17-4.

搜尋詞彙	說明
Policy based VPN	VMware Cloud on AWS、NSX-V 和 NSX-T 的所有以原則為基礎的 VPN 工作階段
VMC Policy based VPN	以 VMware Cloud on AWS 原則為基礎的 VPN 工作階段
NSX-T Policy based VPN	NSX-T 以原則為基礎的 VPN 工作階段
NSX Policy based VPN	NSX 以原則為基礎的 VPN 工作階段

NSX 分散式防火牆非作用中規則

vRealize Network Insight 支援在某些時間沒有流程的 NSX 分散式防火牆規則的可見度。這些規則稱為非作用中規則。此類規則使用記憶體堆積，可能會導致安全性問題。為監控這些非作用中規則，vRealize Network Insight 在**安全性**儀表板中提供了下列兩個 Widget：

備註 若要檢視「安全性」儀表板，請在搜尋列中輸入**安全性**。

- 未使用的 NSX 防火牆規則：此 Widget 列出在指定的時間未報告任何流程的所有 NSX 防火牆規則。您也可以使用下列搜尋查詢擷取這些規則：

```
nsx firewall rule where flow is not set
```

備註 請確保您已針對指定的時間的 NSX 分散式防火牆 IPFIX。

Fortinet 防火牆

在 vRealize Network Insight 中，您可以檢視有關 Fortinet 防火牆的見解。

vRealize Network Insight 支援下列 Fortinet 實體 -

- Fortinet 管理程式
- Fortinet ADOM - Fortinet 管理網域詳細資料
- Fortinet VDOM - Fortinet 虛擬網域詳細資料。vRealize Network Insight 僅支援以流量為基礎的篩選。不支援透明模式。
- Fortinet 位址 - ADOM 特定位址的清單。vRealize Network Insight 支援 ipmask、iprange 和 NSX 網狀架構連接器。
- Fortinet 位址群組 - ADOM 特定位址群組的清單
- Fortinet 動態位址 - ADOM 特定動態位址 (VDOM 對應位址) 的清單
- Fortinet 動態位址群組 - ADOM 特定動態位址群組 (VDOM 對應位址群組) 的清單
- Fortinet 動態介面 - ADOM 特定動態介面的清單。
- Fortinet 區域 - ADOM 特定區域的清單。

- Fortinet 服務 - 針對每個 ADOM 手動和自動產生的服務的清單。
- Fortinet 服務群組 - 每個 ADOM 的服務群組的清單。
- Fortinet 原則 - 每個 ADOM 的 Fortinet 原則。我們目前僅支援 IPv4 原則、Fortinet 全域標頭原則和 Fortinet 全域註腳原則。
- Fortinet 原則套件 - 原則套件的清單。原則套件名稱也包含具有套件名稱前置詞的原則套件的路徑。
- Fortinet 裝置 - 與 FortiManager 相關聯的 Fortinet 裝置的清單。
- Fortinet 裝置群組 - 由使用者指定的 Fortinet 裝置群組的清單。

下列內容不受支援：

- NAT 模式下的虛擬機器至虛擬機器路徑。
- 透明模式下實體裝置的虛擬機器至虛擬機器路徑。
- 進階 (不以 IP 為基礎) 原則內容，例如使用者、使用者群組、應用程式和安全性設定檔。

vRealize Network Insight 提供實作微分割安全性的規劃和建議。它可協助使用者快速而自信地管理和延伸 VMware NSX 部署。

本章節討論下列主題：

- [分析應用程式](#)
- [應用程式探索](#)
- [VMware Cloud on AWS：規劃和微分割](#)

分析應用程式

微分割規劃拓撲透過將流程分為多個區段，顯示環境中的所有流程。

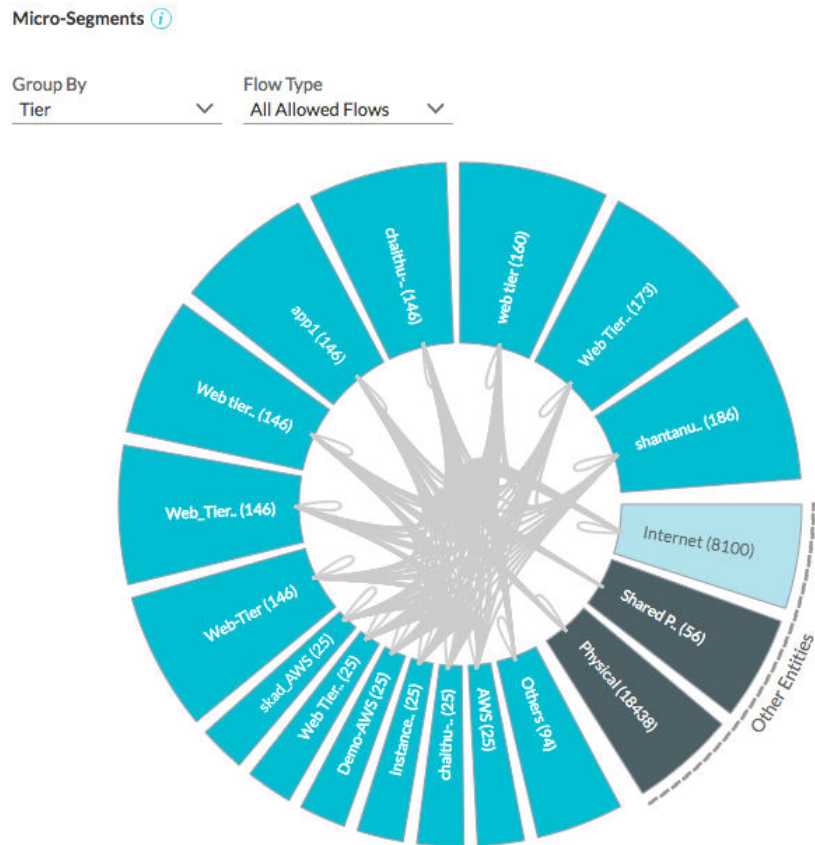
在 vRealize Network Insight 中，流量是一個 4 元組。包括：

- 來源 IP
- 目的地 IP
- 目的地連接埠
- 通訊協定

您可以兩種格式檢視資料：同心圓視圖和網格視圖

在同心圓視圖中檢視微分割與流量資料

在同心圓視圖中，藍線代表傳出流量，綠線代表傳入流量，黃線代表雙向流量。您可以按一下任意區段以檢視其詳細資料。

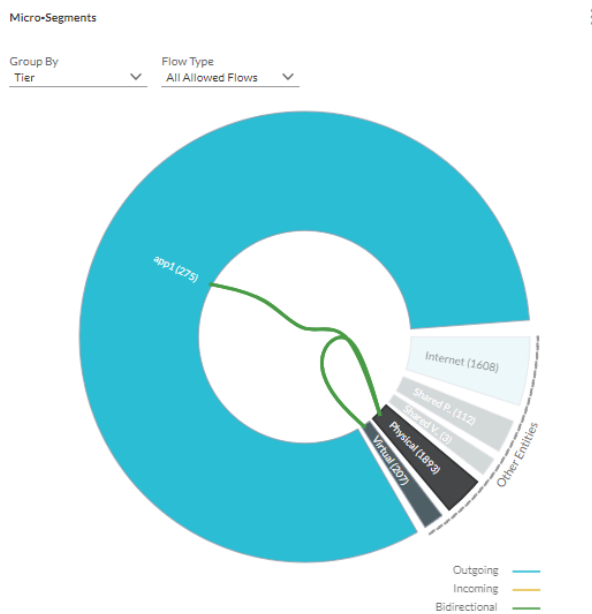


所選範圍之外的虛擬機器在微分割規劃拓撲中分組為**其他實體**。

您也可以透過按實體、其他虛擬和網際網路類別建立子群組來分析流量。

Group By	Also show groups for
VLAN/VXLAN	All
Application	Physical
✓ Tier	Virtual
Subnet	Internet
Folder	✓ None
Cluster	
VM	
Port	
Security Tag	
Security Group	
IPSet	
VPC	

每個群組都展開成一個楔形。在下列拓撲中，您可以看到**實體群組**的楔形。



流程釘選項顯示不同時間間隔的流程 (依連接埠分隔)。您可以檢視所有流程，也可以檢視兩個實體之間的流程。您可以按「已允許」和「已封鎖」流程篩選流程。您可以依 [位元組總計] 或 [允許的工作階段計數] 檢視流程。對於受防火牆保護的流程，會使用「受防火牆保護」符號表示該連接埠中的流程受防火牆保護。

規劃整個資料中心或叢集等範圍時，會選取具有虛擬機器或實體伺服器 (由實體 IP 識別) 做為來源或目的地的流程。

拓撲有兩個不同的區域：

- **內部：**此區域包括範圍內的虛擬機器或 IP 位址。
- **外部：**此區域包含在範圍以外但與內部區域中的虛擬機器或 IP 位址通訊的虛擬機器或 IP 位址。外部區域由下列楔形組成：
 - **DC 虛擬：**包括來源或目的地資料中心內部虛擬機器，這些虛擬機器與內部區域中的虛擬機器或 IP 位址進行通訊，但不主控任何常見共用服務 (如 LDAP、NTP 等)。
 - **共用虛擬：**包括目的地資料中心內部虛擬機器，這些虛擬機器主控常見共用服務 (如 LDAP、NTP 等)，並與內部區域中的虛擬機器或 IP 位址進行通訊。
 - **DC 實體：**包括來源或目的地資料中心內部實體 IP 位址，這些位址與內部區域中的虛擬機器或 IP 位址進行通訊，但不主控任何常見共用服務 (如 LDAP、NTP 等)。
 - **共用實體：**包括目的地資料中心內部實體 IP 位址，這些位址主控常見共用服務 (如 LDAP、NTP 等)，並與內部區域中的虛擬機器或 IP 位址進行通訊。
 - **網際網路：**包括與內部區域中的虛擬機器或 IP 位址通訊的來源或目的地資料中心外部虛擬機器或實體 IP 位址。


備註

- 資料中心內部隱含 RFC 1918 預設指定的 IP + 在 E-W 設定中定義的任何覆寫項目。
- 資料中心外部隱含非 RFC 1918 預設指定的 IP + 在 N-S 設定中定義的任何覆寫項目。

在網格視圖中檢視微分割與流量資料

vRealize Network Insight 可讓您查看表格式視圖或網格視圖中的物件之間的通訊。

程序

- 1 導覽至**安全性 > 規劃安全性**，然後按一下網格視圖  圖示。
- 2 選取**分組依據**選項的值，例如**虛擬機器**、**應用程式**、**安全群組**，以查看表格格式的對應詳細資料。

欄位名稱	說明
來源物件	來源的名稱
目的地物件	目的地的名稱
相關流量	來源與目的地之間的通訊或流量的計數 按一下計數值，以查看相關的流量詳細資料。
位元組總和	所有流量之間的彙總位元組數

欄位名稱	說明
最大流量速率	所有相關流量中觀察到的最大流量速率
工作階段計數	特定流量的作用中工作階段數目

備註

- 您可以按一下每個資料行標頭，以遞增或遞減順序排序資料。
- 您可以從資料表視圖中隱藏欄位，按一下欄位標頭旁邊的更多圖示，然後取消選取欄位名稱。

3 此外，您可以在 [網格視圖] 頁面上執行數個動作。

- 在畫面左側的篩選器窗格中，您可以執行下列動作：
 - 選取個別來源或目的地，以篩選與所選來源或目的地物件相關的流量。
 - 選取防火牆動作，以查看允許的流量或捨棄的流量。
 - 選取保護狀態以查看流量狀態。
- 按一下**新增更多篩選器**以新增其他篩選器。
- 若要以 CSV 格式匯出表格資料，請按一下資料表頂端的更多選項，然後選取**匯出為 CSV**。

手動建立應用程式

您可以在 vRealize Network Insight 使用者介面中手動建立應用程式。

程序

- 1 在 vRealize Network Insight 首頁上，按一下**安全性 > 應用程式**。
- 2 在**應用程式**索引標籤上，按一下**新增應用程式**。
- 3 在**新增應用程式**頁面上的**應用程式名稱**文字方塊中，輸入您要建立的應用程式的名稱。
- 4 在**層/部署**區段中，輸入唯一名稱。

您可以根據需求為虛擬機器、實體機器或服務建立層/部署。

- 5 在**成員**欄位中，

- a 從下拉式功能表中選取建立層的條件。

您可以根據虛擬機器內容、虛擬機器的位置 (應用程式、叢集、資料夾) 定義條件，也可以根據 Kubernetes 服務 (服務名稱、叢集 IP 位址、命名空間，叢集 IP 或服務標籤) 定義條件。

若要在多個叢集中搜尋具有相同名稱、相同 IP 或相同標籤的特定 Kubernetes 服務，請使用自訂搜尋。

- b 輸入或選取您要新增至該層的值。

若要輸入多個值，請在各個值後使用逗號。

若要新增服務做為層的一部分，請選取**服務名稱**並在值中輸入名稱。

根據定義的條件，將會顯示相關聯或相關的虛擬機器計數、實體 IP 計數或服務計數。

- 6 若要新增任何其他條件，請按一下**新增其他條件**。
- 7 (選擇性) 若要在一個應用程式下建立另一層，請按一下**新增層/部署**。

您可以在一個應用程式下建立多個層。

此應用程式會建立所有層，並顯示符合所有條件的虛擬機器、實體 IP 及服務的計數。

- 8 (選擇性) 若要建立動態臨界值組態，請選取**啟用臨界值分析**核取方塊。

系統會在**臨界值組態**頁面中建立臨界值組態。vRealize Network Insight 建立了開頭為 `Sys` 前置詞的臨界值組態名稱。

備註

- 如果在應用程式中新增成員，並選取**啟用臨界值分析**核取方塊，則可能需要大約 20 分鐘才能在 [臨界值組態] 頁面中反映該成員。
 - 您無法刪除系統產生的臨界值組態。當您刪除應用程式或清除**啟用臨界值分析**核取方塊並儲存該應用程式時，將會自動刪除與應用程式相關的系統產生的臨界值組態。
-

- 9 選取 [分析流程] 以在最終新增應用程式之前檢視流程。可以相應地根據虛擬機器或實體位址來查看層。
- 10 按一下**儲存**。

備註 如果您的應用程式沒有任何 VMware 虛擬機器並選取了**啟用臨界值分析**核取方塊，則無法儲存該應用程式。您必須新增 VMware 虛擬機器或清除**啟用臨界值分析**核取方塊才能儲存應用程式。

- 11 (選擇性) 若要預覽流量分析，請按一下**預覽流量**。

將會顯示應用程式的微分割視圖。

後續步驟

您可以在**已儲存的應用程式**下查看應用程式詳細資料。

為實體 IP 建立層

建立應用程式時，您可以從下拉式清單中選取**自訂 IP 搜尋**，以根據擴充的欄位為實體 IP 建立層。如需擴充的欄位的詳細資訊，請參閱**擴充流程和 IP 端點**。

在指定層時，您可以使用擴充的 DNS、子網路、VLAN 相關資訊，如下所示：

- Web

Query: IP Endpoint where Subnet Network = '172.16.101.0/24'

- 應用程式

Query: IP Endpoint where Dns Domain = app.example.com

- 資料庫

Query: IP Endpoint where L2 Network = 'vlan-102'

- 通用服務

Query: IP Endpoint where Dns Domain = svc.example.com

應用程式探索

當您有多個應用程式或應用程式中有多個層時，使用公用 API 或使用者介面建立應用程式會是一個漫長的過程。vRealize Network Insight 自動探索應用程式並自動啟用對這些應用程式及其層的存取，這極大地減少了手動作業。

vRealize Network Insight 可根據以下內容執行應用程式探索：

- 標籤 (vCenter Server 或 AWS 標籤)
- 虛擬機器名稱
- [新增 ServiceNow](#)

範例：應用程式探索建構的範例

假設，

- 您已將 vCenter Server 新增為資料來源
- 您的資料中心內有四個虛擬機器 - VM1、VM2、VM3 和 VM4。
- 您已定義標籤 (索引鍵-值)，用於定義每個虛擬機器所屬的應用程式名稱
- 您已定義標籤 (索引鍵-值)，用於定義每個虛擬機器所屬的層

例如，請參閱資料表：

虛擬機器名稱	索引鍵-值標籤
VM1	<ul style="list-style-type: none"> ■ 應用程式名稱：MyApplication1 ■ 應用程式層：App
VM2	<ul style="list-style-type: none"> ■ 應用程式名稱：MyApplication1 ■ 應用程式層：Web
VM3	<ul style="list-style-type: none"> ■ 應用程式名稱：MyApplication2 ■ 應用程式層：App
VM4	<ul style="list-style-type: none"> ■ 應用程式名稱：MyApplication2 ■ 應用程式層：Web

根據標籤探索應用程式

藉由 vRealize Network Insight，您可以針對這些標籤定義應用程式探索的分組準則。

在此範例中，根據定義的標籤和分組準則，vRealize Network Insight 探索兩個應用程式 (MyApplication1 和 MyApplication2)，它們具有兩個層 (App 和 Web) 及其相關的虛擬機器。

應用程式	層及其虛擬機器
MyApplication1	■ App 和 VM1
	■ Web 和 VM2
MyApplication2	■ App 和 VM3
	■ Web 和 VM4

根據虛擬機器名稱建立應用程式和層

假設虛擬機器名稱以特定的格式定義。ApplicationName : Tier : VMName

```
MyApplication1 : App : VM1
MyApplication1 : Web : VM2
MyApplication2 : App : VM3
MyApplication2 : Web : VM4
```

備註 無法為了應用程式探索對隨機定義的虛擬機器名稱進行分組。

當您使用下列 Regex 時，vRealize Network Insight 探索到兩個應用程式。

- 應用程式 Regex : `(.*)_(.*)_.*-.*`
- 層 Regex : `(.*)_(.*)_(.*)-.*`

應用程式	層及其虛擬機器
MyApplication1	■ App 和 MyApplication1 : App : VM1
	■ Web 和 MyApplication1 : Web : VM2
MyApplication2	■ App 和 MyApplication2 : App : VM3
	■ Web 和 MyApplication2 : Web : VM4

新增探索到的應用程式

您可以探索現有的應用程式，並將其新增至 vRealize Network Insight。

程序

- 1 在 [搜尋] 方塊中，使用 **applications** 字串進行搜尋。
- 2 在 **應用程式索引標籤** 下，執行下列其中一項或全部：
 - 依名稱、層或成員對應用程式排序。
 - 篩選您可以在拓撲中看到的應用程式數目 (例如，前 10 個、前 20 個)。每個六邊形代表一個應用程式。計數越大，六邊形的顏色越深。
 - 依名稱、層或成員搜尋應用程式。
- 3 按一下 **探索索引標籤**。

將會顯示以下用於新增應用程式的索引標籤，其中包括 **標籤**、**ServiceNow**、**名稱** 和 **進階**。

4 選取慣用的索引標籤，然後執行相關步驟。

索引標籤	說明
標籤	<p>a 定義範圍。</p> <ul style="list-style-type: none"> ■ 選取所有虛擬機器以查看 vRealize Network Insight 中新增的所有資料來源提供的所有虛擬機器的清單，或 ■ 選取手動選取，然後根據帳戶、資料中心、管理程式等需求篩選虛擬機器。 <p>b 定義標籤的索引鍵和值。</p> <ul style="list-style-type: none"> ■ 輸入標籤的索引鍵。例如 <i>Automation</i>、<i>Category</i>、<i>CreatedBy</i> 和 <i>Owner</i>。 ■ (選擇性) 輸入相應索引鍵的值。 <p>c 按一下已找到 <i>count</i> 個應用程式連結，以查看應用程式名稱的清單、虛擬機器名稱和符合指定準則的虛擬機器數目。</p> <p>d 按一下未分類的虛擬機器，以查看未遵循指定的名稱模式或標籤模式的虛擬機器清單。您可以編輯虛擬機器以修正名稱或標籤準則。</p> <p>e 選取儲存變更至選項以建立新範本或更新現有範本。</p> <p>備註 如果您是管理員使用者，則可以更新所有範本。如果您是成員使用者，則只能編輯您建立的範本。</p> <p>f 按一下探索。</p>
ServiceNow	您會在 ServiceNow 上看到可用的應用程式。

索引標籤	說明
名稱	<p>a 定義範圍。</p> <ul style="list-style-type: none"> ■ 選取所有虛擬機器以查看 vRealize Network Insight 中新增的所有資料來源提供的所有虛擬機器的清單，或 ■ 選取手動選取，然後根據帳戶、資料中心、管理程式等需求篩選虛擬機器。 <p>b 按一下模式建立器。</p> <p>根據您定義的範圍，vRealize Network Insight 會篩選模式建立器中的虛擬機器清單。</p> <ol style="list-style-type: none"> 1 選取預設虛擬機器名稱或從清單中選取虛擬機器，以根據虛擬機器名稱建置模式或規則運算式 (regex)。 2 按一下位置或群組以建構模式。 <hr/> <p>備註 選取群組之後，如果您選取一個字元或位置，則 vRealize Network Insight 會忽略用於建置模式的群組選取，反之亦然。</p> <hr/> <p>根據您的選取項目，您會看到畫面上出現的模式。此外，將會顯示與模式相符的應用程式清單和相關應用程式中的虛擬機器計數及虛擬機器名稱。</p> <ol style="list-style-type: none"> 3 按一下提交。 <p>c 按一下已找到 count 個應用程式連結，以查看應用程式名稱的清單、虛擬機器名稱和符合 Regex 的虛擬機器數目。</p> <p>d 按一下未分類的虛擬機器，以查看未遵循指定的名稱模式的虛擬機器清單。</p> <p>e 選取儲存變更至選項以建立新範本或更新現有範本。</p> <hr/> <p>備註 如果您是管理員使用者，則可以更新所有範本。如果您是成員使用者，則只能編輯您建立的範本。</p> <hr/> <p>f 按一下探索。</p>
進階	<p>a 定義範圍。</p> <ul style="list-style-type: none"> ■ 選取所有虛擬機器以查看 vRealize Network Insight 中新增的所有資料來源提供的所有虛擬機器的清單，或 ■ 選取手動選取，然後根據帳戶、資料中心、管理程式等需求篩選虛擬機器。 <p>b 按一下模式建立器。</p> <p>根據您定義的範圍，vRealize Network Insight 會篩選模式建立器中的虛擬機器清單。</p> <ol style="list-style-type: none"> 1 選取預設虛擬機器名稱或從清單中選取虛擬機器，以根據虛擬機器名稱建置模式或規則運算式 (regex)。 2 按一下位置或群組以建構模式。 <hr/> <p>備註 選取群組之後，如果您選取一個字元或位置，則 vRealize Network Insight 會忽略用於建置模式的群組選取，反之亦然。</p> <hr/> <p>根據您的選取項目，您會看到畫面上出現的模式。此外，將會顯示與模式相符的應用程式清單和相關應用程式中的虛擬機器計數及虛擬機器名稱。</p> <ol style="list-style-type: none"> 3 按一下提交。 <p>c 按一下已找到 count 個應用程式連結，以查看應用程式名稱的清單、符合 Regex 的虛擬機器數目和虛擬機器名稱。</p> <p>d 按一下未分類的虛擬機器，以查看未遵循指定的名稱模式的虛擬機器清單。</p> <p>e 選取儲存變更至選項以建立新範本或更新現有範本。</p> <hr/> <p>備註 如果您是管理員使用者，則可以更新所有範本。如果您是成員使用者，則只能編輯您建立的範本。</p> <hr/> <p>f 按一下探索。</p>

將會顯示符合準則的所有應用程式的表格式和六邊形地圖視圖。

在地圖視圖中，您可以將滑鼠暫留在六邊形上以查看應用程式名稱、探索到的虛擬機器計數和層計數等資訊。應用程式和網際網路之間的線條代表連線。您可以按一下線條以查看流量詳細資料，例如來源和目的地流量的計數，以及不受保護的來源流量和目的地流量的計數。六邊形上的問號表示 vRealize Network Insight 找不到或無法擷取應用程式的任何流量詳細資料，可能是因為應用程式已超過流量限制或具有不受保護的流量。

在表格式視圖中，您可以查看應用程式詳細資料，其中包括應用程式名稱、無法到達目的地的流量以及因防火牆動作遭拒而被捨棄的流量的計數、層和成員的計數。

地圖和資料表視圖是互動式的。當您按一下表格式視圖中的應用程式時，六邊形會反白顯示或聚焦在地圖視圖上，並且會顯示所有網路連線。

5 (選擇性) 在地圖視圖上執行下列任何動作：

- 放大與縮小，或移動地圖可查看應用程式。
- 查看所有不受保護的應用程式。
- 查看與網際網路通訊的應用程式。
- 查看使用主機共用服務的所有應用程式。
- 查看有問題的應用程式。

6 (選擇性) 在資料表視圖上執行下列任何動作：

- 將滑鼠暫留在 [成員] 資料行中的值上，以查看虛擬機器、實體 IP 和服務的個別計數。
- 按一下應用程式名稱以開啟應用程式儀表板，然後檢視該特定應用程式的詳細資料。
- 按一下表格式視圖中的 + 圖示以展開應用程式詳細資料，例如，準則以及虛擬機器和層計數。

備註 此圖示僅適用於探索到的應用程式。

7 儲存已探索到的應用程式：

- 在地圖視圖中，將滑鼠暫留在六邊形上，然後按一下**儲存應用程式**，或
- 在表格式視圖中，按一下**儲存應用程式**。

備註 您可以透過選取資料表中應用程式的多個核取方塊來執行應用程式的大量儲存，然後按一下**儲存應用程式**。

8 驗證 [新增應用程式] 頁面上的詳細資料，然後按一下提交。

儲存後，您會在應用程式六邊形懸停清單中看到 `application:Saved`，並且在表格式視圖中看到應用程式的刻度標記。如果該應用程式已儲存，您可以將游標暫留在刻度標記上，並按一下**另存新檔**以使用其他名稱儲存應用程式。

備註 如果應用程式在 ServiceNow 中進行修改，則不會在 vRealize Network Insight 中執行自動更新。您必須在 vRealize Network Insight 中手動更新應用程式。

表 18-1. 限制

物件	建議的限制
地圖視圖中的應用程式清單	1000
表格式視圖中的應用程式清單	不適用
已儲存的應用程式	400
所有應用程式之間的層總計	5000
每個應用程式的層數	30
每一層的成員數	不適用
每個應用程式的成員數	1.8K
如果應用程式超過限制，您可能無法在 [應用程式拓撲] 看板中看到流量資訊，或者會看到錯誤訊息。	
每個應用程式的流量	300K

如果您的設定超出每個應用程式建議的層、應用程式和流量限制，您仍可以繼續新增物件，但是效能可能會降低。

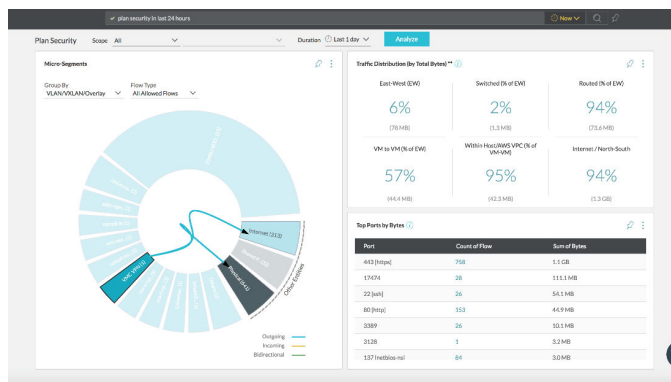
後續步驟

按一下**匯出為 CSV** 將應用程式詳細資料匯出為 .csv 格式。您可以定義應用程式計數以及您要匯出的欄位。將根據成員計數 (每個成員一行) 重複應用程式名稱和層名稱欄位。僅填寫與應用程式相關的欄位，其餘欄位則保留空白。

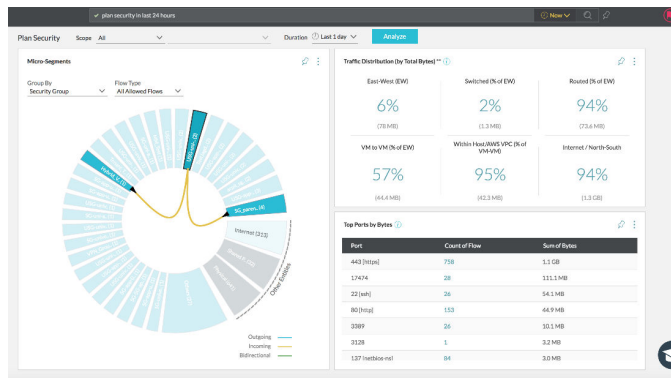
VMware Cloud on AWS：規劃和微分割

您可以透過在**規劃安全性**頁面中選取 **VMC 區段** 做為範圍，來規劃特定的 VMware Cloud on AWS 區段。

對於原則區段，請使用群組中的 `VLAN/VXLAN/Overlay` 子句。



對於原則群組，請使用群組中的 Security Group 子句。

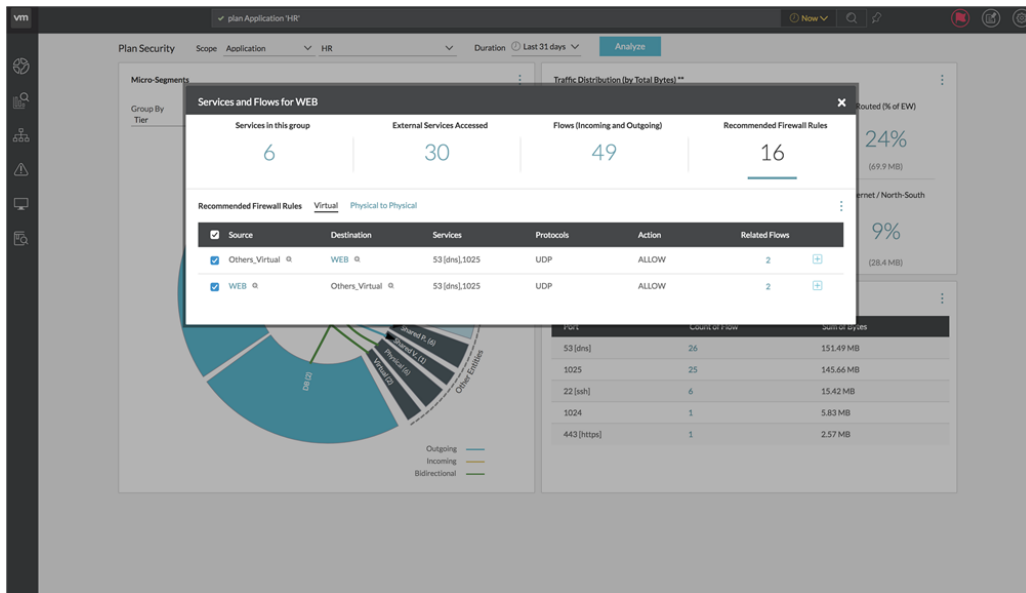


建議的防火牆規則

19

在**規劃安全性**頁面上，按一下拓撲圖中的楔形或 Edge 時，您可以檢視該特定區段的服務和流程清單。按一下**建議的防火牆規則**以檢視在其上定義的規則。來源或目的地的成員在下列規則類型列：

- **實體到實體**：此索引標籤會列出與實體和網際網路 IP 相關聯的所有規則。這些規則可用於實體-實體、實體-網際網路、網際網路-實體或網際網路-網際網路實體。
- **虛擬**：此索引標籤會列出至少一個端點為虛擬機器的所有規則。



對於每個防火牆規則，下列詳細資料可用：

- 顯示群組的成員，方法是按一下實體名稱旁邊的 + 符號以查看群組成員。

Services and Flows for integration.tier2				Flows (Incoming and Outgoing)		Recommended Firewall Rules	
Services in this group	External Services Accessed						
7	22	32	7				

Source	Destination	Services	Protocols	Action	Related Flows
integration.tier2	integration.tier1	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2

備註

- 不會顯示屬於網際網路類別的群組的成員。
 - 如果安全群組同時擁有虛擬和實體 IP，則在該特定群組的成員資格清單中不會顯示實體和網際網路 IP。
 - 成員 Kubernetes 服務會顯示在 **Kubernetes 服務** 索引標籤下。
 - 如果**虛擬機器**、**實體與網際網路 IP** 或 **Kubernetes 服務** 的成員計數或項目為零，則索引標籤不可見。
-
- 來源
 - 目的地
 - 服務
 - 通訊協定
 - 動作
 - 相關流程：按一下相關流程的數字來檢視具有對應流程資訊的流程的清單。
 - 檢視套用的防火牆規則：按一下**相關流程**欄旁邊的 + 符號可檢視與類似流程集相對應的已套用防火牆規則。

Services and Flows for integration.tier2				Flows (Incoming and Outgoing)		Recommended Firewall Rules	
Services in this group	External Services Accessed						
7	22	32	7				

Source	Destination	Services	Protocols	Action	Related Flows
integration.tier2	integration.tier1	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	53 [dns], 1025	UDP	ALLOW	2
integration.tier1	integration.tier2	22 [ssh]	TCP	ALLOW	2

您可以根據您的需求將建議的規則匯出為 XML 或 CSV。

備註 您也可以採用 YAML 格式匯出與 Kubernetes 物件相關的建議規則。

如需這些項目的詳細資訊，請參閱[匯出規則](#)。

保護易受攻擊的作業系統的建議防火牆規則

使用下列程序來取得保護易受攻擊的作業系統的建議防火牆規則：

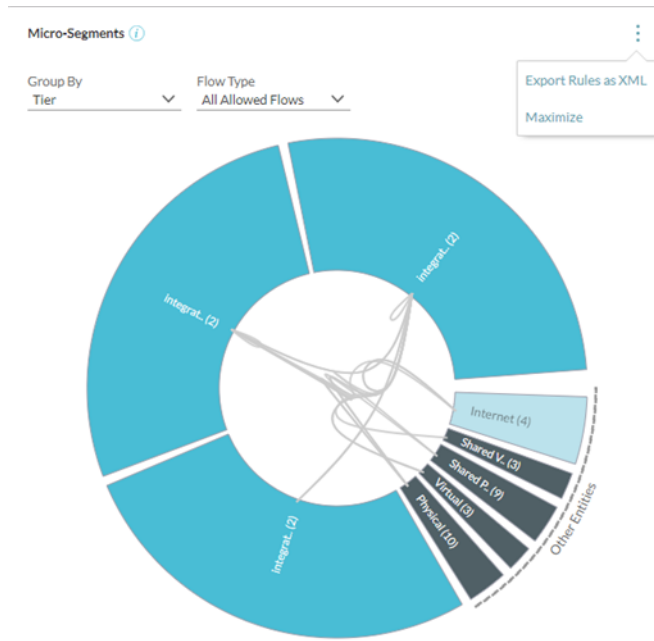
- 1 移至**安全性 > 應用程式 > 建立應用程式**。
- 2 輸入應用程式和層/部署的名稱。
- 3 在**成員**下拉式功能表中，選取自訂**虛擬機器搜尋**，並在文字方塊中新增在**辨識符號**中添加相符準則：作業系統，例如「Microsoft Windows Server 2003」；或作業系統，例如「Microsoft Windows Server 2008」；或作業系統，例如「Red Hat Enterprise Linux 6」；或作業系統，例如「Red Hat Enterprise Linux 5」；或作業系統，例如「SUSE Linux Enterprise 10」條件。
- 4 按一下**儲存**。
- 5 移至**安全性 > 規劃安全性**。
- 6 在**範圍**下拉式功能表中，選取**應用程式**以及您建立的應用程式的名稱。
- 7 在**持續時間**下拉式功能表中，選取**過去 7 天**。
- 8 若要取得建議的防火牆規則，請按一下**分析**

本章節討論下列主題：

- [匯出規則](#)
- [匯出並套用 Kubernetes 網路原則](#)

匯出規則

您可以將所有規則匯出為整個拓撲的 XML。您可以在**微分割規劃**頁面中找到此功能表項目，如下所示：



[匯出為 XML] 選項僅適用於下列實體：

- 安全群組
- 應用程式層

如果規劃範圍僅涉及單一 NSX Manager，則產生的項目會包含與建議的服務和防火牆規則相對應的 XML 檔案。如果規劃範圍涉及多個 NSX Manager，則產生的項目會包含與建議的服務、IPset、安全群組和防火牆規則相對應的 XML 檔案。

以下是安全群組的預留位置項目：

- SG-Others_Internet.xml
- SG-Other.xml

對於拓撲圖中描述的特定楔形或 Edge，您可以將所有規則匯出為 XML 或 CSV。

備註 您也可以採用 YAML 格式匯出與 Kubernetes 物件相關的建議規則。

NSX DFW 一般項目

即可輕鬆地跨各種 vCenter 和 NSX 部署管理通用安全群組中的物件。vRealize Network Insight 僅支援產生和匯入應用程式和層群組的一般項目。使用一般安全群組，在跨 vCenter 案例中輕鬆部署和管理防火牆規則會變得很容易。請確保在主要 NSX manager 上匯入一般項目。您只能透過主要 NSX manager 管理通用安全群組的成員資格。

通用安全群組可包含：

- 其他通用群組
- 一般 IP 集
- 通用安全性標籤

將規則匯出為 XML 時，除了 NSX manager 特定資料夾之外，還會建立一個通用資料夾，其中包含 NSX DFW 一般項目。匯入 NSX DFW 一般項目後，會建立對應的通用安全群組、通用 IP 集合、通用安全性標籤和通用 DFW 防火牆規則。

備註

- 一般安全性標籤僅在主動-待命模式中受支援。
- 一般 IP 集在主動-主動式模式和主動-待命模式下都受支援。

您可以根據需求建立通用 IP 集或一般安全性標籤。如果您要建立通用安全性標記，則可以將應用程式虛擬機器對應到安全性標籤。否則，使用一般 IP 集。

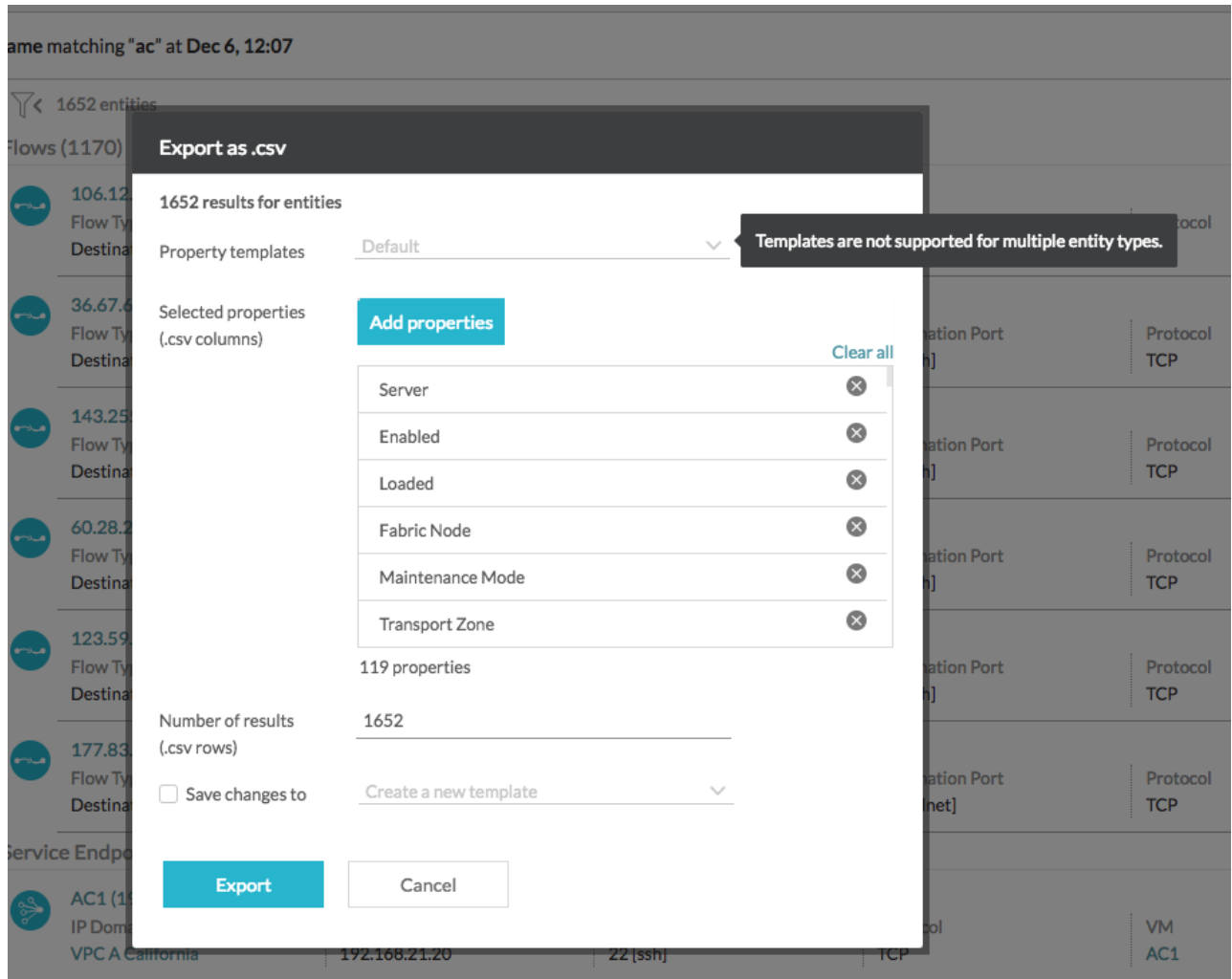
您可以在匯入工具中使用以下徽章：

表 19-1.

徽章名稱	說明
-uni	從通用資料夾匯入項目。
-utag	在一般安全群組的成員資格中匯入具有通用安全性標籤的一般項目。
-log	建立在其上啟用記錄的規則。
	備註 此徽章不特定於一般選項。

將 CSV 匯出的組態儲存為內容範本

以 CSV 檔案從 Widget 匯出資料時，您可以在內容範本中儲存要匯出的內容 (或資料行) 的組合。當結果屬於單一實體類型時，會為 CSV 匯出啟用這些內容範本。如果使用列出多個實體類型的關鍵字進行搜尋，則無法在內容範本中儲存內容的組合。



當您開啟 CSV 匯出強制回應時，將會顯示搜尋結果的預設內容選取項目 (根據實體類型)。您可以變更此所選內容清單，並儲存新組態以供日後參考。或者，您也可以從 CSV 匯出強制回應上的範本區段中載入或開啟儲存前的內容範本。變更該值時，將會顯示所選內容範本的選定內容。

對要匯出的所選內容進行變更後，您可以從 CSV 匯出強制回應建立內容範本或編輯現有的內容範本。此範本與目前搜尋結果的實體類型相同。

您可以透過導覽至**設定 -> 內容範本**頁面，檢視系統中現有內容範本的清單。**內容範本**頁面上的清單會顯示現有範本及詳細資料，例如實體類型、上次更新日期和內容數量。您可以從**內容範本**頁面編輯或刪除內容範本。除了變更內容範本的名稱之外，您還可以編輯內容範本。

匯出並套用 Kubernetes 網路原則

您可以採用 YAML 格式匯出與 Kubernetes 物件相關的建議網路原則規則。vRealize Network Insight 僅支援針對依命名空間分組和依服務拓撲分組匯出至 YAML 格式。

必要條件

- [新增 Kubernetes](#)
- [新增 VMware PKS](#)

程序

- 1 若要將建議的規則匯出至 YAML 格式，請在規劃安全性模型中選取您要為其規劃安全性的 kubernetes 叢集，然後執行其中一個步驟。
 - 在微分割 Widget 中展開更多選項，然後選取以 **YAML 格式匯出規則**，或
 - 在微分割同心圓視圖上選取一個節點，按一下建議的防火牆規則的計數，展開更多選項並選取以 **YAML 格式匯出規則**。

vRealize Network Insight 會下載以 Kubernetes 網路原則命名的 ZIP 檔案以及與其相關聯的時間戳記。當您解壓縮檔案時，將會顯示下列五個 CSV 檔案以及多個資料夾，具體取決叢集數目。每個資料夾將包含叢集的多個 YAML 檔案。

檔案名稱	說明
network-policy-others-ipaddress.csv	包含服務或命名空間與之通訊的實體伺服器 and 虛擬機器的 IP 位址。
recommended-namespace-labels-to-add.csv	包含要附加至與命名空間相關聯的網蔴的標籤。 範例 <ul style="list-style-type: none"> ■ 叢集 - pdk8s ■ 命名空間 - sock-shop ■ 標籤 - sock-shop-pdk8s
recommended-service-labels-to-add.csv	包含要附加至與服務相關聯的網蔴的標籤。 範例 <ul style="list-style-type: none"> ■ 叢集 - pdk8s ■ 命名空間 - sock-shop ■ 服務 - front-end ■ 標籤 - Service:front-sock-shop-pdk8s ■ 叢集 - pdk8s ■ 命名空間 - sock-shop ■ 服務 - user ■ 標籤 - Service:user-sock-shop
recommended-network-policy.csv	包含由 vRealize Network Insight 建議的所有規則。
exported-network-policy-rule-names.csv	列出根據建議的規則匯出的所有網路原則。

2 若要套用服務標籤，請執行下列步驟：

a 執行下列 Kubernetes CLI 命令。

```
kubectl edit deployment service-name -n namespace-name
```

```
kubectl edit deployment redis-master -n guestbook
```

服務的部署檔案隨即開啟。

b 在服務標籤清單中，將 CSV 檔案中建議的標籤附加到服務部署的規格部分中所述的標籤。

3 若要套用命名空間標籤，請執行下列步驟：

a 執行下列 Kubernetes CLI 命令。

```
kubectl edit namespace namespace-name
```

```
kubectl edit namespace guestbook
```

命名空間的部署檔案隨即開啟。

b 在中繼資料中，將 CSV 檔案中建議的標籤附加到命名空間部署的 spec 部分中所述的標籤。

4 執行下列命令來確認標籤是否已套用至網繭。

```
kubectl get pods -n namespace-name--show-labels
```

```
kubectl get pods guestbook--show-labels
```

查看結果視圖中的標籤。

備註 在命名空間上套用時，標籤不會反映在網繭上。

5 若要建立網路原則，請將 YAML 檔案從個別叢集資料夾複製到另一個資料夾，並執行下列任一命令：

- `kubectl apply -f <folder-name>/` - 將所有防火牆規則一起套用。
- `kubectl apply -f <folder-name>/<firewall-rule>.yaml` - 逐一套用防火牆規則

使用搜尋查詢

20

vRealize Network Insight 可對環境中的所有實體執行強大搜尋。

以下是可協助您使用 vRealize Network Insight 中的搜尋功能的部分術語：

- **實體**：資料中心由實體和邏輯建置區塊 (例如主機、虛擬機器、交換器、路由器、NSX Manager 等) 組成。這些區塊的執行個體就是實體。
- **內容**：實體由多個內容組成。內容可以是組態內容，也可以是度量內容。
 - a **組態內容**：實體可以依其組態內容進行說明。組態內容可以是整數或真實值，也可以是字串或布林值。
 - 虛擬機器的名稱、CPU 核心和作業系統
 - 主機的名稱和虛擬機器數目
 - b **度量內容**：度量實體特定特性的任何內容是度量內容。度量內容的值按固定時間間隔進行擷取。虛擬機器的 CPU 使用率、記憶體使用量和網路使用量是度量內容的部分範例。
- **彙總函數**：可以在搜尋查詢中用於運算特定實體類型的執行個體總數或實體的最大值內容。vRealize Network Insight 支援下列彙總函數。
 - a `sum`
 - b `max`
 - c `min`
 - d `avg`

搜尋實體時，軟體會在結果頁面上顯示與搜尋查詢相符的實體。

對於每個搜尋查詢，搜尋列會向您提供建議可讓您縮小搜尋結果範圍的下一個詞彙。例如，輸入**虛擬機器**一詞時，搜尋列會顯示可能的字組，且您可以將其新增至現有的字組，以縮小搜尋結果範圍。搜尋列也會驗證每個搜尋查詢。打勾標記表示有效的搜尋查詢，打叉標記表示無效的搜尋查詢。**說明**頁面會提供目前受支援查詢的範例。

本章節討論下列主題：

- [儲存和刪除搜尋查詢](#)
- [搜尋查詢](#)
- [進階查詢](#)

- [時間控制](#)
- [搜尋結果](#)
- [篩選器](#)
- [vCenter 標籤](#)

儲存和刪除搜尋查詢

vRealize Network Insight 可讓您執行搜尋查詢並儲存查詢以供日後使用。您也可以刪除已儲存的搜尋。

備註

- vRealize Network Insight 提供下列預設已儲存的搜尋：
 - 所有流量
 - 應用程式
 - Azure
 - Kubernetes 儀表板
 - 前幾項趨勢
 - NSX
 - 您無法儲存或刪除預設已儲存的搜尋。
 - 您無法儲存無效的搜尋查詢。
 - 已儲存的搜尋特定於使用者，而預設已儲存的搜尋則可供所有使用者使用。
-

程序

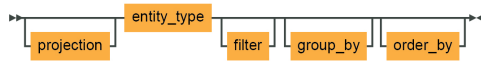
- 1 若要儲存查詢，請執行搜尋，然後按一下搜尋列旁的書籤圖示。
您會看到書籤圖示反白顯示，以確保查詢已儲存。左側導覽列中**已儲存的搜尋**下會列出此搜尋。若要查看所有已儲存的查詢，請按一下**已儲存的搜尋 > 管理已儲存的搜尋**。
- 2 若要刪除已儲存的搜尋，請再次按一下書籤圖示，然後在確認動作對話方塊上按一下**刪除**。
您也可以從**管理已儲存的搜尋**視窗中刪除已儲存的搜尋。
- 3 同時刪除多個已儲存的搜尋查詢：
 - a 展開左側導覽列，按一下**已儲存的搜尋 > 管理已儲存的搜尋**。
 - b 選取要刪除的查詢。
 - c 按一下**刪除**選項。
 - d 確認刪除。

搜尋查詢

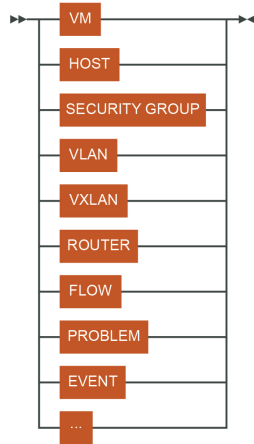
搜尋查詢可以分為以下類別：

1 結構化查詢

結構化查詢包含下列元件：



- **實體類型**：實體類型表示要搜尋的物件類型。可以採用單數形式或複數形式。實體類型在結構化查詢中是必要的。



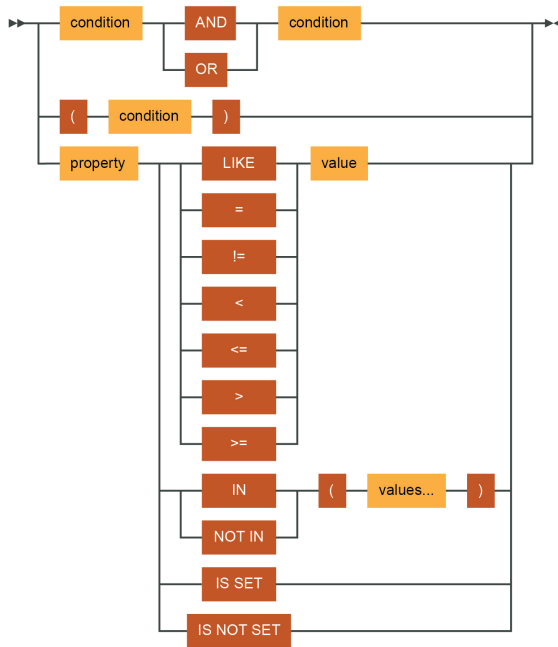
以下是一些範例：

- 1 Virtual machines
- 2 Hosts
- 3 Flows
- 4 MTU Mismatch Events
- 5 Problems

- **篩選器**：篩選器的語法如下所示：



條件的語法如下所示：



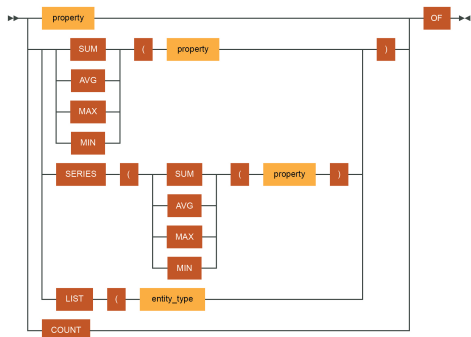
可使用篩選器子句篩選搜尋結果。篩選器子句中的條件包含內容、比較運算子和值。可以將條件與邏輯運算子組合使用以形成複雜條件。以下是您可以使用的運算子清單：

運算子	範例
=	flows where source ip address = '10.16.240.0/24' flows where flow type = 'Source is VM'
!=	vms where ip address != '10.17.0.0/16'
>	vms where memory > 4096 mb
<	vms where cpu usage rate < 70%
>=	vms where memory >= 4096 mb
<=	vms where cpu usage rate <= 70%
like	vms where name like 'app'
not like	vms where name not like 'app'
in	flows where port in (22, 23, 80, 443) vm where ip address in (192.168.91.11, 192.168.91.10)
not in	flows where port not in (22, 23, 80, 443) vm where ip address not in (192.168.91.11, 192.168.91.10)
is set	vms where firewall rule is set
is not set	vms where firewall rule is not set

運算子	範例
()	flows where (src tier = 'App' and destination tier = 'DB') OR (destination tier = 'App' and source tier = 'DB')
and	flows where src tier = 'App' and destinationtier = 'DB'
or	flows where flow type = 'Source is VMKNIC' or flow type = 'Destination is VMKNIC'
相符	vm where name matches '.*' vm where name matches 'a.*' vm where name matches '[a-z]vm-delta[0-9]'
不相符	vm where name not matches '.*' vm where name not matches 'a.*' vm where name not matches '[a-z]vm-delta[0-9]'
巢狀 'in' 運算子	vm where in (vm where name = 'x') vm where in (vm of host where name = 'x') vm where host in (host of vm where name = 'x') vm where name in (name of vm where name = 'x')

- **投影**：查詢中的投影子句確定了必須顯示已篩選實體中的哪些欄位。這是可選子句。如果未指定投影子句，則搜尋結果中會顯示預設欄位集。投影子句可包含下列任何一項：

- 1 內容
- 2 計數
- 3 清單
- 4 彙總
- 5 序列



- 1 **內容**：按實體類型搜尋實體時，搜尋結果中會顯示預設內容集。透過使用投影，您可以選取應在搜尋結果中顯示的欄位。例如，`os of vms` 在搜尋結果中列出具有 `OS property` 的所有虛擬機器。

以下列出了更多此類範例：

- `cpu cores of vms`
- `source ip address of flows`

如果使用度量內容，則會為每個實體顯示一個圖表，其中度量內容做為 y-axis，時間做為 x-axis。

2 計數：計數查詢可用於計算實體類型的物件數目。以下是一些範例：

- `count of vms`
- `count of hosts`
- `count of flows`

3 清單：如果無法在您擷取的實體上套用篩選條件，則清單運算子很有用。

例如：

```
List(host) of vms where memory <= 2gb
```

此查詢擷取主機清單，但在虛擬機器上套用了篩選條件。以下列出了更多此類範例：

- `List(ip address) of vms where cpu cores = 1`

4 彙總函數：彙總函數允許根據數字 `config` 或 `metric` 內容計算單一值。搜尋查詢語言支援下列彙總函數：

- `max`
- `sum`
- `min`
- `avg`

以下是一些範例：

- `sum(memory) of hosts`
- `sum(memory), sum(cpu cores) of vms`
- `sum(bytes) of flows`

5 序列：序列運算子可用來對度量內容執行彙總。例如：

```
series(avg(cpu usage)) of vms where cpu cores = 4
```

此查詢顯示的圖形中包含具有 4 個 CPU 核心的所有虛擬機器的平均 CPU 使用率。以下是一些範例：

- `series(sum(network usage)) of vms where name like 'app'`
- `series(sum(memory usage)) of vms where name like 'db'`
- `series(avg(cpu usage)), series(avg(memory usage)) of vms`

- **排序：**可以使用 `order by` 子句對搜尋結果進行排序。`order by` 子句中僅允許一個欄位。依預設，結果依遞減順序進行排序。



以下是一些範例：

- 1 `vms order by cpu cores`
- 2 `vms order by cpu cores asc`
- 3 `flows order by bytes`

可以使用 `limit` 子句限制結果數目。此子句前面必須有 `order by` 子句。例如：

```
vms order by memory limit 5
```

- **分組：**可以按內容對實體進行分組。按內容對實體分組時，預設會顯示每個群組中的結果數目。透過新增投影，可以計算任何內容的總和/最大值/最小值。新增 `order by` 子句會對結果進行排序。如果查詢中有 `order by` 或 `projection` 子句，則必須存在彙總函數。



```
sum(bytes) of flows group by dest vm
```

此查詢有效，因為查詢在投影子句中具有彙總函數。諸如 `bytes of flows group by dest vm` 之類的查詢無效，因為投影子句中沒有彙總函數。

以下是一些範例：

- 1 `vms group by host`
- 2 `sum (bytes) of flows group by dest vm order by sum(bytes)`

2 實體查詢



- a **按實體類型搜尋：**透過搜尋實體類型，可以列出該實體類型的所有實體。

範例：`vms`、`hosts`、`flows`、`nsx managers`

- b **按實體名稱搜尋**

- **按全名搜尋：**如果您知道實體的全名，則可以透過用單引號括住該名稱對其進行搜尋。

範例：`'prod-68-1'`、`'app1-72-1'`

- **按部分名稱搜尋：**按單一字組或多個字組搜尋會擷取與輸入字組相符的所有實體。

範例：`prod`、`app1`

備註 如果輸入內容包含關鍵字或實體類型，則可能會將其做為搜尋查詢進行處理。

- 按實體類型和名稱搜尋：如果您知道實體的名稱和類型，可以透過一起查詢實體類型和實體名稱來進行搜尋。

範例：搜尋查詢 'vm appl' 會傳回包含 appl 的所有虛擬機器。

3 規劃查詢

這些查詢可用於透過分析流程，以規劃資料中心的安全性。

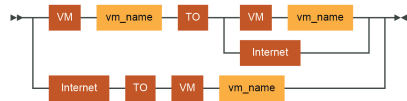


範例：

- plan securitygroup1
- plan host1
- plan security

4 路徑查詢

這些查詢可用於顯示兩個虛擬機器之間的路徑或從虛擬機器至網際網路的路徑。



範例：

- Vm 'vm1' to Vm 'vm2'
- VM 'vm1' to Internet

備註

- 搜尋查詢不區分大小寫。
- 實體類型或組態內容可具有同義詞。例如，實體類型 'virtual machine' 具有同義詞 'vm'。

Azure 搜尋查詢

您可以在 vRealize Network Insight 中搜尋 Azure 實體詳細資料。

以下是一些搜尋查詢範例：

Azure 實體	範例查詢
Microsoft Azure	Azure
Azure 應用程式安全群組	Azure Application Security Group where Azure Virtual Network = 'Test-vnet2'
Azure 資料來源	Azure Data Source
Azure NSG 規則	Azure NSG Rule where Action = 'ALLOW'
Azure 網路介面	Azure Network Interface where Azure Virtual Network = 'Test-vnet2'

Azure 實體	範例查詢
Azure 網路安全群組	Azure Network Security Group where Subscription = 'vRNI-dev'
Azure 路由	Azure Route where Route Table = 'TestRouteTable'
Azure 路由表	Azure Route Table where Azure Virtual Network = 'aks-vnet-28255566'
Azure 子網路	Azure Subnet where Azure Virtual Network = 'vrni-01-vnet'
Azure 訂閱	Azure Subscription
Azure 虛擬機器	Azure Virtual Machine where Azure Application Security Group = 'TestASG'
Azure 虛擬網路	Azure Virtual Network where Azure Peer Virtual Network = 'vrni-01-vnet'

Cisco ACI 實體

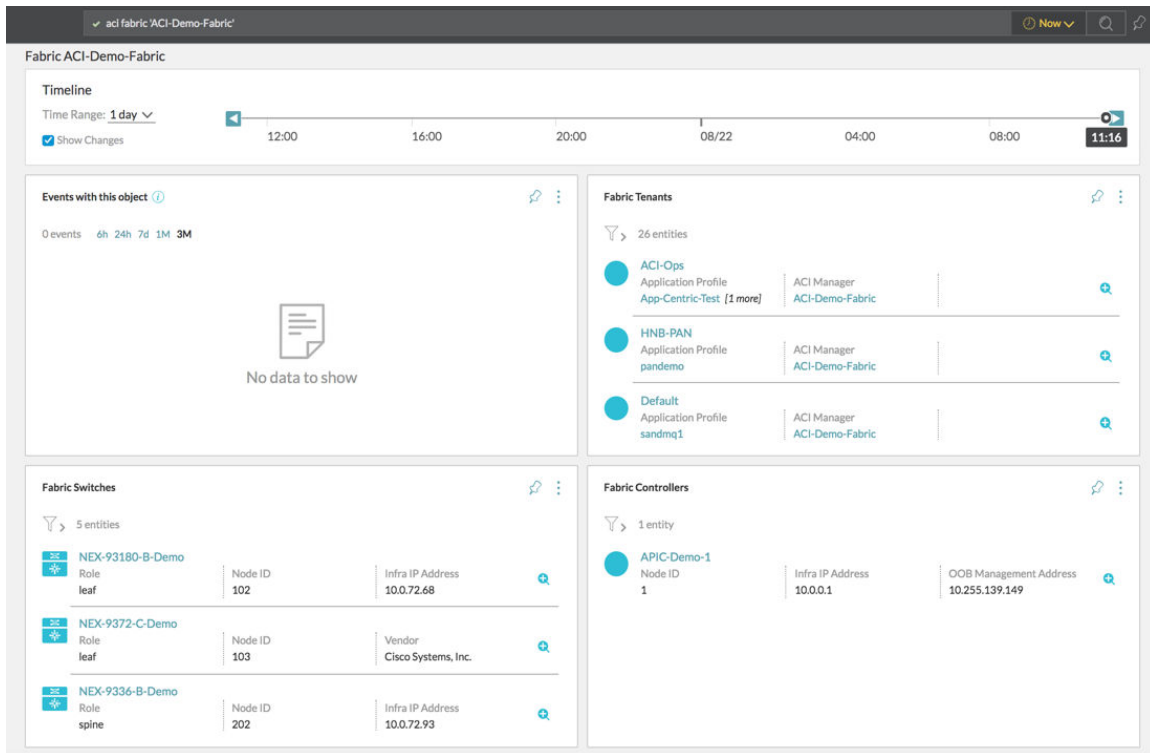
以下是可對其執行搜尋的一些 Cisco ACI 實體的清單：

備註 實體以 `aci` 為前置詞。

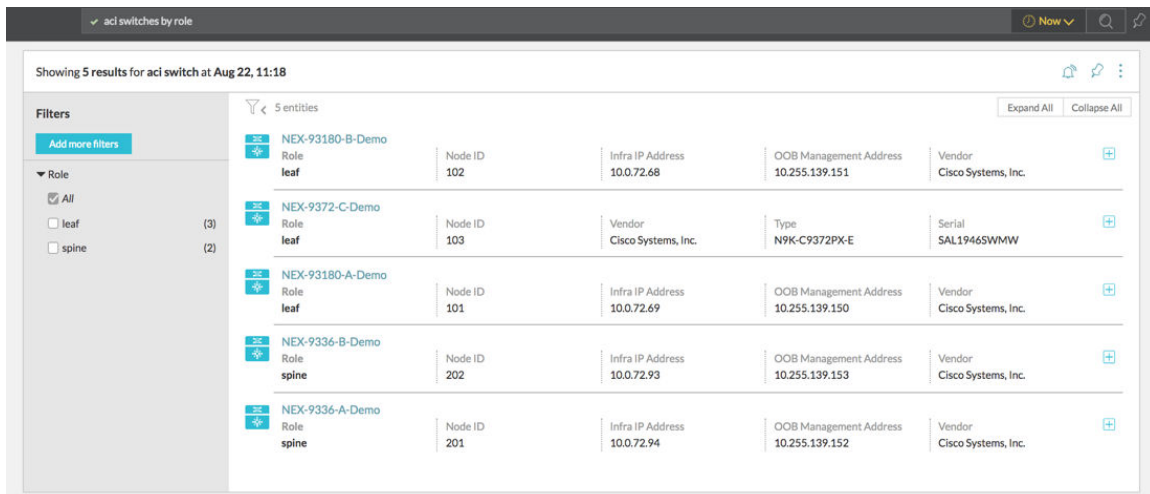
- `aci application profile`
- `aci bridge domain`
- `aci endpoint group`
- `aci fabric`
- `aci switch`
- `aci tenant`

以下是一些搜尋查詢範例：

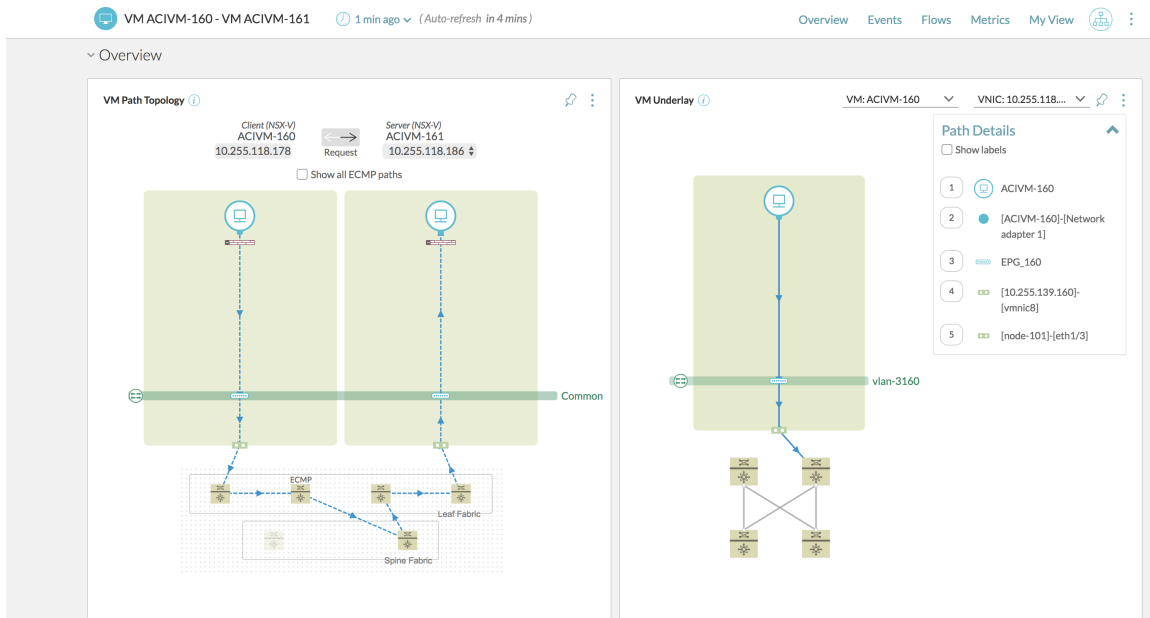
- `aci fabric 'ACI-Demo-Fabric'`：此查詢擷取有關 ACI 網狀架構中承租人、交換器和控制器的資訊。



- aci switches by role : 此查詢擷取有關 ACI 網狀架構中各種分支交換器或主幹式交換器的資訊。從交換器清單中，按一下交換器名稱以取得有關該交換器的更多詳細資料。



- aci endpoint group : 此查詢擷取具有相關聯的虛擬機器、橋接器網域和 VRF 的端點群組的清單。
- aci application profile 'Production' : 此查詢擷取具有包含的端點群組和虛擬機器的生產應用程式設定檔。
- VMware VM 'ACIVM-160' to VMware VM 'ACIVM-161' : 此查詢顯示兩個虛擬機器之間的虛擬機器-虛擬機器路徑。



- 您可以使用 IP 位址進行搜尋，以取得連接埠、端點群組和橋接器網域詳細資料。

10.114.219.158

Showing 2 results for Entities with keywords "10.114.219.158" at Mar 25, 15:10

2 entities

Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 10.114.21... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:B9:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

- 您可以使用 Mac 位址進行搜尋，以取得連接埠、端點群組和橋接器網域詳細資料。

00:0C:29:44:70:D8

Showing 2 results for Entities with keywords "00:0C:29:44:70:d8" at Mar 25, 15:06

2 entities

Endpoint Group (1)

Mgmt-1201	Application Profile NSXInfra	Bridge Domain BD-Mgmt	Encap vlan-1201	Number of VMs 0	Endpoints 00:0C:29:44:70:D8 1... [17 more]
-----------	---------------------------------	--------------------------	--------------------	--------------------	---

Switch Port (1)

[node-104]-[eth1/19]	Operational Status Up	Administrative Status Up	Mac Address 00:D7:8F:85:B9:7B	MTU 9000	Interface speed 10 Gbps
----------------------	--------------------------	-----------------------------	----------------------------------	-------------	----------------------------

Filters

Add more filters

Entity Type

- ☒ All
- ☐ Switch Port
- ☐ Endpoint Group

- 您可以搜尋端點群組，並取得相關聯端點的清單。

✓ aci epg where Endpoint is set

Showing 4 results for aci endpoint group with filter Endpoint is set at Mar 25, 15:11

Filters

Add more filters

▼ Endpoints

☒ All

☐ 00:0C:29:44:70:D8 10.114.219.158 (1)

☐ 00:0C:29:4E:6A:B4 10.114.219.146 (1)

☐ 00:0C:29:BE:EF:D5 10.114.219.147 (1)

☐ 00:1B:21:69:83:88 10.114.219.137 (1)

☐ 00:25:90:E1:6C:52 10.114.219.136 (1)

[20 more]

4 entities

Entity	Endpoints	Application Profile	Bridge Domain	Encap	Number of VMs
Mgmt-1201	00:0C:29:44:70:D8... [17 more]	NSXInfra	BD-Mgmt	vlan-1201	0
IPSt...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:AC:41... [1 more]	NSXInfra	BD-IPStorage	vlan-1204	0
Tran...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:AC:41... [1 more]	NSXInfra	BD-Transport	NSX-VRF	0
Vmo...	00:0C:29:44:70:D8 10.114.219.158 00:0C:29:4E:6A:B4 10.114.219.146 00:0C:29:BE:EF:D5 10.114.219.147 00:1B:21:69:83:88 10.114.219.137 00:25:90:E1:6C:52 10.114.219.136 00:25:90:E1:76:9E 10.114.219.135 00:25:90:E1:CC:B8 10.114.219.134 00:25:90:EB:BA:EE 10.114.219.130 00:25:90:EB:BA:F0 10.114.219.131 00:50:56:BE:16:BF 10.114.219.152 00:50:56:BE:7C:FE 10.114.219.133 00:50:56:BE:84:E5 10.114.219.151 00:50:56:BE:AC:41... [1 more]	NSXInfra	BD-Vmotion	vlan-1203	0

- 您可以搜尋端點。

✓ aci epg where Endpoint like 10.114.219.158

Showing 1 result for aci endpoint group with filter Endpoint like 10.114.219.158 at Mar 25, 15:19

Filters

Add more filters

▼ Endpoints

☒ All

☐ 00:0C:29:44:70:D8 10.114.219.158 (1)

☐ 00:0C:29:4E:6A:B4 10.114.219.146 (1)

☐ 00:0C:29:BE:EF:D5 10.114.219.147 (1)

☐ 00:1B:21:69:83:88 10.114.219.137 (1)

☐ 00:25:90:E1:6C:52 10.114.219.136 (1)

[13 more]

1 entity

Entity	Endpoints	Application Profile	Bridge Domain	Encap	Number of VMs
Mgmt-1201	00:0C:29:44:70:D8... [17 more]	NSXInfra	BD-Mgmt	vlan-1201	0

Fortinet 搜尋查詢

您可以在 vRealize Network Insight 中搜尋 Fortinet 實體詳細資料。

以下是一些搜尋查詢範例：

Fortinet 實體	範例查詢
Fortinet 原則套件	Fortinet Policy Package where Domain Manager = 'ADOM_NAME'
Fortinet 原則	Fortinet Policy where Source IP = '10.0.0.15'
Fortinet 位址	Fortinet Address where Address Type = 'ipmask'
Fortinet 動態位址	Fortinet Dynamic Address where Domain Manager = 'ADOM_NAME'
Fortinet 動態位址群組	Fortinet Dynamic Address Group where Domain Manager = 'ADOM_NAME'
Fortinet 服務	Fortinet Service where port = 5900
Fortinet 服務群組	Fortinet Service Group where Manger = '10.0.15.101'

Fortinet 實體	範例查詢
Fortinet ADOM	Fortinet ADOM where Manager ID = '10.0.15.101'
Fortinet VDOM	Fortinet VDOM where Domain Manager = 'ADOM_NAME'
Fortinet 動態介面	Fortinet Dynamic Interface where Domain Manager = 'ADOM_NAME'

使用 Infoblox DNS 資料擴充流程

vRealize Network Insight 支援下列兩個 DNS 資訊來源：

- 匯入的 CSV 檔案
- Infoblox DNS

備註 如果 Infoblox DNS 與 CSV 檔案之間存在衝突，則來自 Infoblox DNS 的資訊會優先。

您可以使用各種搜尋查詢來找出有關流程中 DNS 項目來源的更多資訊。

表 20-1.

關鍵字	搜尋查詢範例	說明
DNS 提供者	Flows where DNS Provider='Infoblox'	提供從 Infoblox 取得 DNS 資料的流程清單。
DNS 提供者	Flows where DNS Provider='CSV'	提供從 CSV 取得 DNS 資料的流程清單。
來源 DNS 提供者	Flows where Source DNS Provider='Infoblox'	提供來源 IP 位址的 DNS 提供者為 Infoblox 的流程清單。
目的地 DNS 提供者	Flows where Destination DNS provider='Infoblox'	提供目的地 IP 位址的 DNS 提供者為 Infoblox 的流程清單。

Kubernetes 實體的通用搜尋查詢

您可以在 vRealize Network Insight 中搜尋 Kubernetes 實體詳細資料。

通用查詢

- 搜尋流量：`flows where Kubernetes Object = Object name`
範例：其中 **Kubernetes Cluster** = '**Production**' 的流量
- 檢視服務規模：`kubernetes pods group by Kubernetes Services`
- 檢視節點負載：`kubernetes Pods group by Kubernetes Node`
- 檢視節點健全狀況：`MemoryPressure and PIDPressure and DiskPressure and Ready of Kubernetes Node`

- 檢視流量符合性：flows from Kubernetes Object *name of the object* to Kubernetes Object *name of the object*

範例：flows from Kubernetes Namespace '*PCI*' to Kubernetes Namespace '*Non-PCI*'

- 檢視路徑拓撲：
 - Kubernetes 服務 *service name* 至 Kubernetes 服務 *service name*
 - Kubernetes 服務 *service name* 至 Kubernetes 網繭 *pod name*
 - Kubernetes 網繭 *pod name* 至 Kubernetes 網繭 *pod name*

表 20-2. 關於 Kubernetes 物件的查詢

Kubernetes 物件	查詢	說明
命名空間	<ul style="list-style-type: none"> ■ kubernetes namespace where L2 Networks = '<i>a</i>' ■ list(Kubernetes Node) of Kubernetes Pod where Kubernetes Namespace = '<i>a</i>' 	<ul style="list-style-type: none"> ■ 傳回連線至 L2 網路 '<i>a</i>' 的 Kubernetes 命名空間 ■ 傳回 Kubernetes 命名空間為 '<i>a</i>' 的 Kubernetes 節點的清單
網繭	<ul style="list-style-type: none"> ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes nodes) order by Tx Packets desc ■ NSX-T Logical port where connectedto.modelKey in (modelKey of kubernetes pods) and Rx Packet Drops > 0 ■ new kubernetes pod in last 1 hour 	<ul style="list-style-type: none"> ■ 傳回根據按遞減順序傳輸的封包連線至節點的邏輯連接埠的清單 ■ 傳回已連線至 Kubernetes 網繭且 Rx 捨棄封包數 > 0 的邏輯連接埠的清單 ■ 過去 1 小時內探索到的新 Kubernetes 網繭
服務	<ul style="list-style-type: none"> ■ kubernetes pods where kubernetes services is not set ■ kubernetes pods group by Kubernetes Services, Kubernetes Cluster 	<ul style="list-style-type: none"> ■ 不具有服務的 Kubernetes 網繭的清單 ■ 每個服務上執行的網繭數目
節點	<ul style="list-style-type: none"> ■ kubernetes nodes where Ready != 'True' ■ kubernetes node where Virtual Machine = 'vm-a' 	<ul style="list-style-type: none"> ■ 狀況不良的 Kubernetes 節點的清單 ■ 屬於 'vm-a' 虛擬機器的 Kubernetes 節點
流程	<ul style="list-style-type: none"> ■ flows where kubernetes service is set ■ flows where source kubernetes node = '<i>a</i>' 	<ul style="list-style-type: none"> ■ 存在來源或目的地 Kubernetes 服務的流量的清單 ■ 來源 Kubernetes 節點 = '<i>a</i>' 或目的地 Kubernetes 節點 = '<i>a</i>' 的流量的清單

表 20-3. 其他查詢

實體/元件	查詢	說明
具有 Kubernetes 實體的應用程式	application where virtual member = 'service-a'	Kubernetes 服務「service-a」所屬的所有應用程式的清單
	application where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'	Kubernetes 服務「service-a」和 Kubernetes 命名空間「namespace-b」所屬的所有應用程式的清單
	tier where virtual member = 'service-a' and virtual member.Kubernetes Namespace = 'namespace-b'	Kubernetes 服務「service-a」和 Kubernetes 命名空間「namespace-b」所屬的所有層的清單

表 20-3. 其他查詢 (續)

實體/元件	查詢	說明
	count of applications where Virtual Member in (kubernetes services)	成員屬於 Kubernetes 服務類型的應用程式的數目
	count of applications where virtual member in (kubernetes services where Kubernetes Namespace = 'sock-shop')	成員屬於 Kubernetes 命名空間「sock-shop」下的 Kubernetes 服務類型的應用程式數目
	list(virtual member) of applications where Name = 'app-1' and virtual member.Kubernetes Cluster is set	屬於應用程式「app-1」的所有 Kubernetes 服務的清單
度量	nsx-t logical port where (ConnectedTo in (Kubernetes Pods where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo order by max(Rx Packet Drops)	依 Kubernetes 網繭的 Rx 封包捨棄數群組
	nsx-t logical port where (ConnectedTo in (Kubernetes Nodes where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo order by max(Rx Packet Drops)	依 Kubernetes 節點的 Rx 封包捨棄數群組
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:' order by Rx Packet Drops	依 Kubernetes 命名空間的 Rx 封包捨棄數群組
	nsx-t logical switch where Rx Packet Drops > 0 and Tag like 'ncp/project:<namespace name>'	依特定命名空間的封包捨棄數
	nsx-t logical port where (ConnectedTo in (Kubernetes Pods where kubernetes cluster is set)) and Rx Packet Drops > 0 group by ConnectedTo.Kubernetes service order by max(Rx Packet Drops)	依 Kubernetes 服務的封包捨棄數群組
	flows where firewall action = 'DROP' group by Kubernetes Service	依 Kubernetes 服務的捨棄流量群組
	flows where firewall action = 'DROP' group by source Kubernetes Namespace	依 Kubernetes 命名空間的所有已捨棄流量的清單群組
Kubernetes 事件	Kubernetes events where Problem Entity = '<pod/namespace/node Name>'	指定的 Kubernetes 實體的所有 Kubernetes 事件清單。Kubernetes 實體可以是網繭、命名空間或節點
	Kubernetes events where Event code = 'ImagePullBackOff' in last 24 hours	過去 24 小時內類型為「ImagePullBackOff」的 Kubernetes 事件的清單
	Kubernetes events where problem entity.Kubernetes Cluster = '<cluster-a>'	指定的叢集的所有 Kubernetes 事件清單

與負載平衡器相關的範例搜尋查詢

您可以使用下列範例查詢篩選或搜尋與負載平衡器相關的資料。

- `vm where lbServiceNodes is set` - 列出主控散佈負載的應用程式的所有虛擬機器。

- `vm where lbServiceNodes is set and PowerState != 'POWEREDON'` - 列出主控負載平衡應用程式，但目前無法正常運作的所有虛擬機器。
- `pool member where state = 'DISABLED'` - 列出所有已停用的集區成員。
- `Count of Pool Memembers where Service Port = '80'` - 提供在連接埠 80 上執行的某種特定服務類型的所有集區成員的計數。
- `service node where virtual machine is not set` - 列出將實體伺服器用作應用程式伺服器的所有服務節點，或 vRealize Network Insight 中未新增主控虛擬機器的 vCenter Server

NSX 防火牆規則的搜尋查詢

您可以在 vRealize Network Insight 中搜尋 NSX 防火牆規則。

表 20-4. NSX 防火牆規則查詢

搜尋查詢	說明
<code>VM where incoming rules.Source Any</code>	檢視具有任何來源 (可與特定的連接埠結合) 的規則。
<code>Firewall rule where action = allow and service any = true</code>	檢視允許任何連接埠的防火牆規則。
<code>Firewall Rule Masked Event</code>	檢視未使用的防火牆規則的清單。
<code>New firewall rules in last 24 hours</code>	檢視在過去 24 小時內建立的防火牆規則。
<code>New firewall rules in last 7 days</code>	檢視在過去 7 天內建立的防火牆規則。
<code>New firewall rules in last 30 days</code>	檢視在過去 30 天內建立的防火牆規則。
<code>Firewall rule where flow is not set</code>	檢視所有非作用中防火牆規則的清單。
<code>Flow group by firewall rule</code>	檢視叫用每個防火牆規則的流量的計數。
<code>Security group where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	檢視未使用的安全群組。
<code>Ipset where Indirect Incoming Rules is not set and Indirect Outgoing Rules is not set and Direct Incoming Rules is not set and Direct Outgoing Rules is not set</code>	檢視未使用的 IPSet。
<code>Flow where rule id in (1011, 1012, 1013)</code>	叫用特定規則識別碼的流量。
<code>Flow where application = appl</code>	叫用應用程式的流量。

- 未使用的防火牆規則
- 防火牆規則遮罩規則事件

VMware SD-WAN 搜尋查詢

您可以在 vRealize Network Insight 中搜尋 VMware SD-WAN 實體詳細資料。

以下是一些搜尋查詢範例：

VMware SD-WAN 實體	範例查詢
VeloCloud 叢集	VeloCloud Cluster where Description = 'cluster one'
VeloCloud 資料來源	VeloCloud Data Source where Enabled = true
VeloCloud Edge	VeloCloud Edge where Activation State = 'Activated'
VeloCloud 企業	VeloCloud Enterprise where Name = 'VMWare - vRNI'
VeloCloud 閘道	VeloCloud Gateway where City = 'Ashburn'
VeloCloud 第 2 層網路	VeloCloud Layer2 Network where Network = '172.16.40.2/24'
VeloCloud 連結	VeloCloud Link where Link Uptime = 100%
VeloCloud 設定檔	VeloCloud Profile where Name = 'APProfile'

VMware SD-WAN 實體	範例查詢
VeloCloud 區段	<code>VeloCloud Segment where Vendor ID = '1'</code>
VeloCloud 業務原則	<code>VeloCloud Business Policy where Application = 'skype'</code> <code>VeloCloud Business Policy where scope = 'Edge'</code> <code>VeloCloud Business Policy where Source IP = 10.79.46.0</code> <code>VeloCloud Business Policy where OS = 'Linux'</code> <code>VeloCloud Business Policy where Source VLAN ID = '1'</code> <code>VeloCloud Business Policy where Link Policy = 'Fixed'</code> <code>VeloCloud Business Policy where Priority = 'High'</code> <code>VeloCloud Business Policy where Service Class = 'Real Time'</code> <code>VeloCloud Business Policy where Route Policy = 'Gateway'</code> <code>VeloCloud Business Policy where Route Type = 'edge2cloud'</code> <code>flows where Velocloud business policy = 'EdgeToInternet'</code>

VMC SDDC 搜尋查詢

您可以在 vRealize Network Insight 中搜尋 VMC SDDC 實體詳細資料。

以下是一些搜尋查詢範例：

VMC SDDC 實體	範例查詢	說明
NSX Manager	<code>vmc sddc where NSX Manager</code>	顯示與 VMC SDDC 相關聯的 NSX Manager。
NSX Manager FQDN	<code>vmc sddc where NSX Manager Fqdn</code>	顯示 VMC SDDC 的 NSX Manager FQDN。

VMC SDDC 實體	範例查詢	說明
NSX Manager 私人 IP	<code>vmc sddc where NSX Manager Private Ip</code>	顯示 VMC SDDC 的 NSX Manager 私人 IP 位址。
NSX Manager 公用 IP	<code>vmc sddc where NSX Manager Public Ip</code>	顯示 VMC SDDC 的 NSX Manager 公用 IP 位址。
名稱	<code>vmc sddc where Name</code>	顯示 VMC SDDC 的名稱。
組織識別碼	<code>vmc sddc where Org Id</code>	顯示 SDDC 所屬的組織識別碼。
組織名稱	<code>vmc sddc where Org Name</code>	顯示 SDDC 所屬的組織名稱。
區域	<code>vmc sddc where Region</code>	顯示 SDDC 所在的 AWS 區域。
VC FQDN	<code>vmc sddc where VC FQDN</code>	顯示 VMC SDDC 的 vCenter FQDN。
VC Manager	<code>vmc sddc where VC Manager</code>	顯示與 VMC SDDC 相關聯的 vCenter Manager。
VC 私人 IP	<code>vmc sddc where VC Private Ip</code>	顯示 VMC SDDC 的 vCenter 私人 IP 位址。
VC 公用 IP	<code>vmc sddc where VC Public Ip</code>	顯示 VMC SDDC 的 vCenter 公用 IP 位址。
廠商識別碼	<code>vmc sddc where Vendor ID</code>	顯示 SDDC 的識別碼。

適用於 AWS 實體的 VMware Cloud on AWS

以下是與 VMware Cloud on AWS NSX Policy Manager 相關的實體：

- NSX Policy Manager Data Source
- NSX Policy Manager
- NSX Policy Firewall
- NSX Policy Firewall Rule
- NSX Policy Segment
- NSX Policy Based VPN
- NSX Policy Group

備註 如果將 NSX-T 2.4 和 VMware Cloud on AWS 新增為 vRealize Network Insight 中的資料來源，為了取得 VMware Cloud on AWS 實體，您必須在查詢中新增 **SDDC type = VMC** 篩選器。例如，若要針對 VMware Cloud on AWS 列出以原則為基礎的 VPN，則輸入 **NSX Policy Based VPN where Tier0 = '' and SDDC Type = 'VMC'**。

與 VMware Cloud on AWS 實體相關的一些搜尋查詢範例如下：

- `VMs where L2 Network = '' (L2 Network -> NSX Policy Segment)`
- `NSX Policy Based VPN where Tier0 = ''`

- NSX Policy Based VPN where Local Network = '' (Local Network of Policy Based VPN Rule)
- NSX Policy Based VPN where Remote Network = '' (Remote Network of Policy Based VPN Rule)
- NSX Policy Group where Translated VM = ''
- VM where NSX Policy Group = ''

備註

- NSX Policy Manager 不支援子群組或 IPset。因此，將停用類似 NSX Policy firewall rule where Indirect _____ = '' 或 NSX Policy group where Indirect _____ = '' 的所有搜尋。

進階查詢

以下是進階查詢的一些範例：

用於通訊模式的流程查詢

- 跨資料中心或站台的流量總計 (DCI 連結使用)

```
sum(bytes) of flows where ( Dst Manager = 'abc' AND src manager = 'cba') OR ( Dst Manager = 'cba' AND src manager = 'abc')
```

- VTEP 流量總計

- ```
sum(bytes) of flows where Flow Type = 'Src is VTEP' or flow type = 'Dst is VTEP' VTEP traffic grouped by VMKNIC
```

- ```
sum(bytes) of flows where Flow Type = 'Src is VTEP' or Flow Type = 'Dst is VTEP' group by ip
```

- 其他管理流量

```
flows where Flow Type = 'Source is VMKNIC' or Flow Type = 'Destination is VMKNIC'
```

用於彙總和群組的流程查詢

- 網際網路流量總計 (依來源虛擬機器)

```
sum(bytes) of flows where Flow Type = 'Internet' group by src vm
```

- 前幾個連接埠 (依總位元組數)

```
sum(bytes) of flow group by port order by sum(bytes)
```

- 前幾個子網路配對 (依路由的流量)

```
sum(bytes) of flow where Flow Type = 'Routed' group by Source Subnet Network, destination subnet network order by sum(bytes)
```

- 虛擬機器總計 (依配對總位元組數)

```
sum(bytes) of flows group by src vm , dest vm order by sum(bytes)
```

- 前幾個伺服器虛擬機器/連接埠 (依總位元組數)

```
sum(bytes) of flows group by dest vm , port order by sum(bytes)
```

用於容量估計和大小調整的流程查詢

- 由 ESX 分組的所有 vm-internet/internet-vm 流量的總位元組數 (Palo Alto 服務虛擬機器大小調整)

```
sum(bytes) of flows where flow type = 'internet' and (flow type = ' src is vm ' OR  
flow type = 'destination is vm ') group by host order by sum(bytes)
```

- 用於相符流程的彙總流量系列 (Palo Alto 服務虛擬機器大小調整)

```
series( sum(byte rate)) of flows where host = 'ddc1-pod2esx012.dm.democompany.net'  
and (Flow Type = 'Source is VM' OR flow type = 'Destination is VM')
```

應用程式的有用查詢

- 指定應用程式中的虛擬機器

```
VM where application = 'CRM'
```

- 從指定應用程式路由的流程

```
Flows where source application = CRM and Flow Type = 'Routed'
```

- 兩層之間的流程 (單向)

```
Flows where src tier = 'App' and Destination Tier = 'DB'
```

- 兩層之間的流程 (單向)

```
Flows where ( src tier = 'App' and destination Tier = 'DB') OR (destination tier =  
'App' and source tier = 'DB')
```

虛擬機器和 ESX 的有用查詢

- Prod -Midtier-1 虛擬機器的內容 (MAC、IP、主機等)

```
CPU Usage Rate, Network Rate, Memory Usage Rate, mac address, ip , vxlan , host of  
vm 'Quality control-VM26'
```

- 具有最高虛擬機器計數的網路區段

```
vm group by l2 network
```

- 資料存放區具有最高虛擬機器計數

```
vm group by datastore
```

- 主機 (依 vSphere 版本)

```
host group by version
```

- 主機 (依 vSphere 組建版本)

```
host group by OS
```

- 插入特定 UCS 機箱的所有主機/刀鋒型伺服器上的所有虛擬機器 (巢狀查詢)

```
vm where host in (host where Blade like 'sys/chassis-1')
```

有用的查詢：一般容量

- 資料中心數目：

```
count of datacenter
```

- 叢集數目

```
count of cluster
```

- 主機數目

```
count of host
```

- 虛擬機器數目

```
count of vm
```

- 網路數目

```
count of vlan
```

有用的查詢：路由

- VNI (依主要控制器)

```
vxlan group by Primary Controller
```

- 提供者 Edge 3 的路由

```
routes where vrf = 'Provider Edge 3'
```

- DMZ DLR 的路由

```
NextHop Router of routes where VRF = 'LDR-DMZ'
```

- 將指定路由器做為下一個躍點的路由

```
routes where NextHop Router = 'California-Edge'
```

有用的查詢：防火牆規則

- 兩個虛擬機器之間的防火牆規則

```
firewall rules from 'Prod-Midtier-1' to 'Prod-Db-1'
```

- 具有 ANY 來源的規則

```
firewall rules where Service Any = true
```

- 指定規則的虛擬機器

```
vm where Firewall Rule = 'Prod MidTier to Prod DB - DBService '
```

- 允許任何連接埠的防火牆規則

```
firewall rule where action = allow and service any = true
```

- 叫用特定防火牆規則的流程

```
flows where firewall rule = 'Admin to Prod and Lab - SSH'
```

- 系統中已拒絕的流程

```
flows where firewall action = deny
```

- 檢視閘道防火牆

```
Firewall Rule where firewall type = 'GatewayFirewall'
```

- 檢視分散式防火牆

```
Firewall Rule where firewall type = 'Distributed Firewall'
```

有用的查詢：一般流量模式

- 東西向和南北向流量計數、交換的流量計數、路由的流量計數，以及虛擬機器到虛擬機器的流量計數

```
plan security in last 7 days
```

有用的查詢：來自安全鏡頭的流量

- 高流量者虛擬機器詳細資料

```
top 7 vm group by name, Vlan order by sum(Total Network Traffic) in last 7 days
```

- 傳輸最多流量的網路

```
top 7 vlan group by Vlan id, vm count order by sum(Total Network Traffic) in last 7 days
```

- 其中大部分通訊是在 VLAN 內進行的網路 (不跨越實體防火牆或 L3 邊界)

```
top 7 flow where Flow Type = 'Switched' group by Subnet Network order by sum(Bytes) in last 7 days
```

- 其中大部分通訊是跨越 VLAN 進行的網路 (可能會導致實體防火牆出現瓶頸問題)

```
top 7 flow where Flow Type = 'Routed' group by Source Subnet Network, Destination Subnet Network order by sum(Bytes) in last 7 days
```

- 在國家/地區外通訊的虛擬機器

```
top 7 flow where Destination Country != 'United States' group by Source VM, Destination Country order by sum(Bytes) in last 7 days
```

- 發生最大儲存區延遲的資料存放區

```
avg(Read Latency), avg(Write Latency) of top 7 vm group by Datastore, vlan order by avg(Write Latency) in last 7 days
```


有用的查詢：合規性/漏洞

■ 易受攻擊的作業系統詳細資料

```
vm where Operating System like 'Microsoft Windows Server 2003' or Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System like 'SUSE Linux Enterprise 10' group by vlan, Operating System
```

■ 易受攻擊的作業系統計數

```
count of vm where Operating System like 'Microsoft Windows Server 2003' or Operating System like 'Microsoft Windows Server 2008' or Operating System like 'Red Hat Enterprise Linux 6' or Operating System like 'Red Hat Enterprise Linux 5' or Operating System like 'SUSE Linux Enterprise 10'
```

■ 由舊作業系統引起的攻擊面總計

```
vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003', 'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise Linux 5', 'SUSE Linux Enterprise 10')) group by Vlan

count of vm where vlan in (vlan of vm where os in ('Microsoft Windows Server 2003', 'Microsoft Windows Server 2008', 'Red Hat Enterprise Linux 6', 'Red Hat Enterprise Linux 5', 'SUSE Linux Enterprise 10'))
```

備註 若要取得易受攻擊的作業系統的建議防火牆規則，請參閱[保護易受攻擊的作業系統的建議防火牆規則](#)。

時間控制

透過時間控制，您可以在所選時間或時間範圍的環境中執行搜尋查詢。您可以從預設（例如過去 24 小時、最後 3 天等）的清單中選取。也可以使用**處於**選項來指定特定的日期和時間，甚至使用**介於**選項指定範圍。

搜尋結果

搜尋結果頁面會提供與特定搜尋相符的相關實體的詳細清單。此頁面本身提供了大量資訊，包括實體清單、其對應的內容和篩選搜尋結果以縮小搜尋範圍的方面。

也可以展開或摺疊搜尋結果中的每個項目，以檢視有關特定項目的詳細資訊。您也可以為每個搜尋建立通知。

備註 您可以指向搜尋結果以及實體頁面中的特定內容，以檢視包含有關該內容的詳細資訊的工具提示。

下圖顯示了 VXLAN 的搜尋結果，其中 `num vms > 0` 搜尋查詢過去的時間。

vxlan where Num VMs > 0

Showing 12 results for Vxlan with filter Num VMs > 0 at

Filters

Add more filters

▼ VM Count

☒ All (5)

☐ 1 (5)

☐ 2 (2)

☐ 3

► NSX Manager

► Scope

12 entities

Expand All Collapse All

Siteb-Aundh-LS	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
3	10.197.17.114	Global	5006	192.168.23.0/24		
Siteb_P-seattle-vxlan	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
3	10.197.17.229	Global	5000	172.17.1.0/24		
Siteb_P-redmond-vxlan	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5001	172.17.2.0/24		
Siteb-Wagholi-LS	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.114	Global	5005	192.168.26.0/24		
Siteb-pashan-ls-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.114	Global	5002	192.168.24.0/24		
Siteb_P-transit-vxlan-2	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5005	172.17.6.0/24		
Siteb_P-transit-vxlan-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
2	10.197.17.229	Global	5004	172.17.5.0/24		
Siteb-Transit-LS-1	Number of VMs	NSX Manager	Scope	Segment ID	Network Address	
1	10.197.17.114	Global	5003	192.168.21.0/24		

篩選器

Filters

Add more filters

▼ Default Gateway

☒ All

☐ 192.168.23.10 (1)

► NSX Manager

► Scope

► VM Count

取得搜尋結果後，請根據您的需求按一下左窗格上的 [新增更多篩選器]。您可以檢視一系列篩選器類別，可以使用這些類別縮小搜尋結果的範圍。每個類別旁的小方塊中顯示該類別的可用篩選器數目。檢視該類別的可用篩選器 (以及每個篩選器的簡短說明)，然後按一下以套用此篩選器。您也可以使用篩選器搜尋方塊來搜尋特定的篩選器，vRealize Network Insight 將自動顯示與搜尋查詢相符的篩選器，您可以按一下篩選器進行套用。每個篩選器都具有多個用於縮小搜尋結果範圍的內容。從其中一個篩選器選取篩選器內容時，所選內容將在搜尋結果中反白顯示。

vCenter 標籤

vRealize Network Insight 提供用於搜尋和規劃的 vCenter 標籤。

您可以根據 vCenter 標籤和自訂屬性執行虛擬機器搜尋。例如，您可以透過使用標籤來使用下列查詢進行搜尋：

```
vm where tag = '{keyname}:{value}'
```

每個標籤都屬於一個類別。在上述範例中，keyname 是標籤所屬的類別，value 是標籤的名稱。

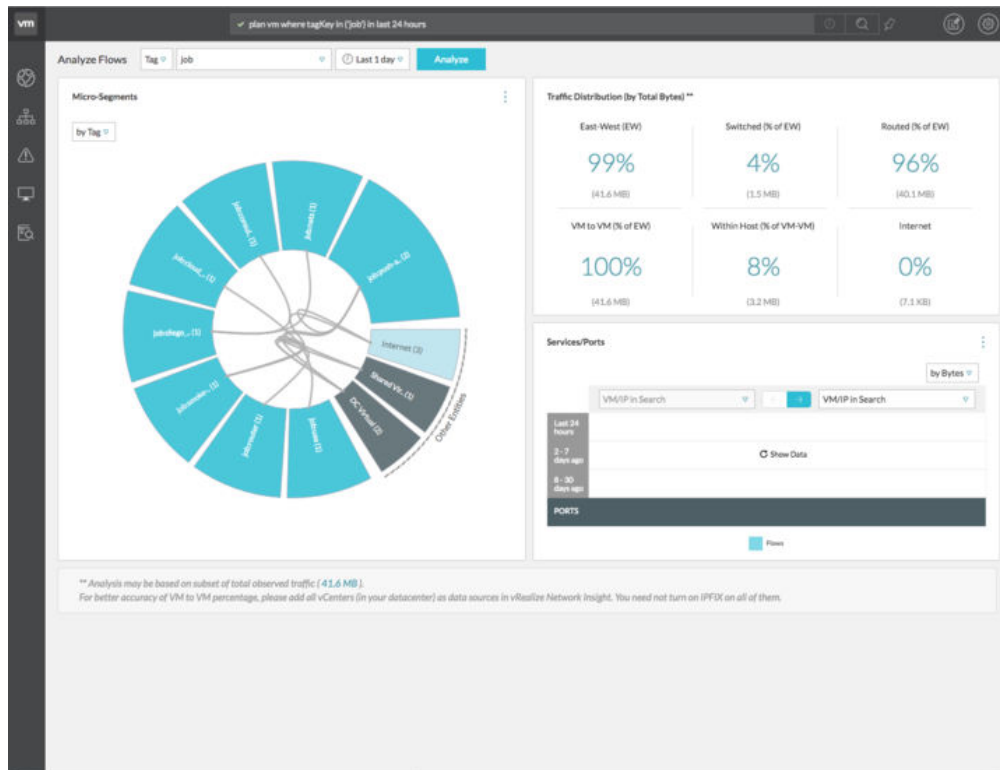
您也可以使用 vCenter 標籤或自訂屬性為虛擬機器提供替代名稱，方法是使用 name 索引鍵。此替代名稱顯示為 other names 內容。也可以使用替代名稱來搜尋並進行路徑查詢。

例如，支援以下查詢：

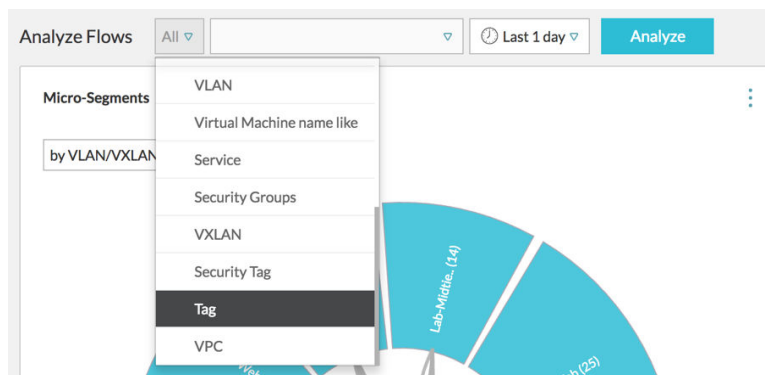
```
vm "other-name-1"
  vm "other-name-1" to vm "other-name-2"
```

在此範例中，other-name-1 和 other-name-2 是自訂屬性，其 name 索引鍵或標籤屬於 name 類別。

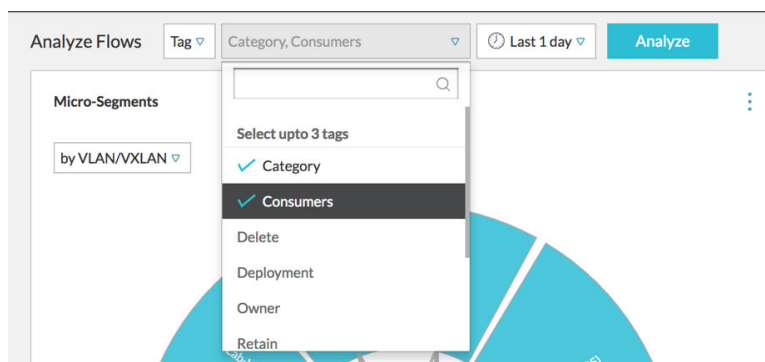
您也可以透過使用 vCenter 標籤來分析網路中的流程，如圖所示。



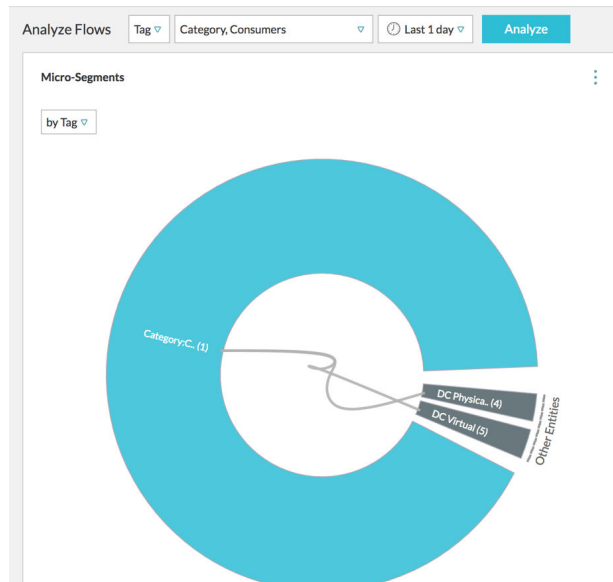
若要使用 vCenter 標籤，請從分析流程下拉式清單中選取標籤選項。



此外，在此層級上最多可以選取三個標籤。選取標籤後，按一下分析。



在按準則分組中，已選取標籤。



規劃 vRealize Network Insight 的災難復原

21

VMware Site Recovery Manager (SRM) 是一個災難復原自動化軟體，可提供以原則為基礎的管理、非破壞性測試和自動協調。vRealize Network Insight 支援 SRM 8.1 及更高版本。為了保護您的 vRealize Network Insight，SRM 會自動執行災難復原計劃的各個方面，以加速復原並消除使用手動程序時所涉及的風險。

如需安裝、升級和設定 SRM 的相關資訊，請參閱 [VMware Site Recovery Manager 說明文件](#)。

針對 vRealize Network Insight 執行災難復原作業的必要條件如下所示：

- 確保您已安裝並設定 vSphere Replication。
- 應同時在受保護和復原站台上設定和部署 SRM。
- 確保已從 SRM 使用者介面內設定正確站台配對，然後再繼續建立復原計劃與其他元件。
- 應在環境中為 vRNI 設定的每個受保護節點啟用 VMware vSphere Replication。啟用 VMware vSphere Replication 時，請考慮到 vRealize Network Insight 節點大小與使用率提供足夠的 RPO，以便在災難期間最小化資料遺失的情況。如需有關複寫的詳細資訊，請參閱 [VMware vSphere Replication 說明文件](#)。
- 確保您已為 vRealize Network Insight 建立獨立保護群組。對於小型和非分散式部署，請確保所有虛擬機器均位於同一個保護群組中。對於分散式部署，建議您將所有平台置於單一保護群組中，以便於復原。您可以將收集器置於不同的保護群組中。
- 建立復原計劃並將包含 vRealize Network Insight 虛擬機器的保護群組新增到此計劃中。確保包含平台節點的保護群組可獲得較高優先順序。在復原計劃中，確保將主要平台節點置於比其他平台節點具有更高優先順序的群組中。
- 目前不支援使用 SRM 自訂任何類型的 IPv4

建議您將 vRealize Network Insight 虛擬機器移轉或復原到相同的網路組態。此外，根據 SRM 建議，您可以定期執行測試，以確保現有計劃適用於基礎結構和設定的 RPO 限制。

- 將 vRealize Network Insight 虛擬機器移轉或復原到相同的網路組態。

如果復原站台設定為與受保護站台具有相同的網路組態並在相同網路之間建立了對應，則將所有複寫的 vRealize Network Insight 虛擬機器設定為使用相同的 IP 啟動，因為這些虛擬機器是受保護的節點。成功完成計劃移轉或災難復原之後，已復原的系統將會處於運作狀態。

- 如果復原站台與受保護站台不具有相同的網路，則不會為復原計劃指定任何 IP 自訂。在此案例中，SRM 將用於復原應用裝置虛擬機器。若要設定復原後的網路，請手動指派網路設定，如下所示：

- 1 在所有平台節點上同時執行 `change-network-settings` 命令。
- 2 連續在 Platform1、Platform2 和 Platform3 中的節點上執行 `update-IP-change` 命令。
- 3 在收集器節點上執行 `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>`。
- 4 檢查服務狀態。如果平台節點上的某些服務不在執行中，請按建議的順序將節點重新開機。

備註 如需有關上述命令的詳細資訊，請參閱《vRealize Network Insight 命令列參考指南》。

本章節討論下列主題：

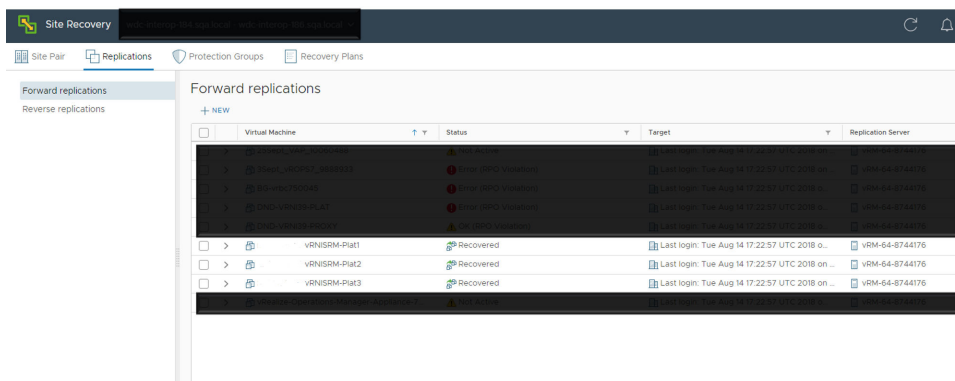
- [災難復原案例範例](#)

災難復原案例範例

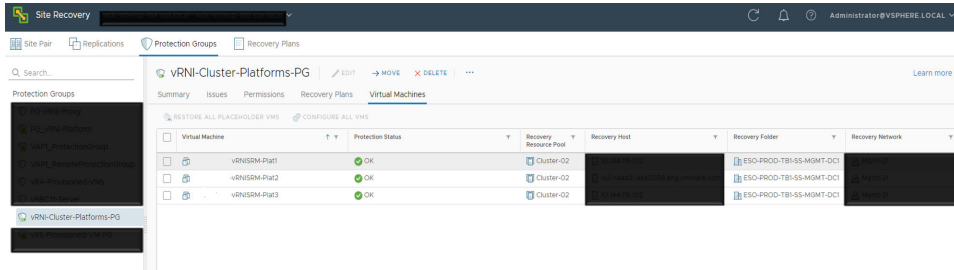
以下是 vRealize Network Insight 災難復原 (DR) 範例案例的步驟：

程序

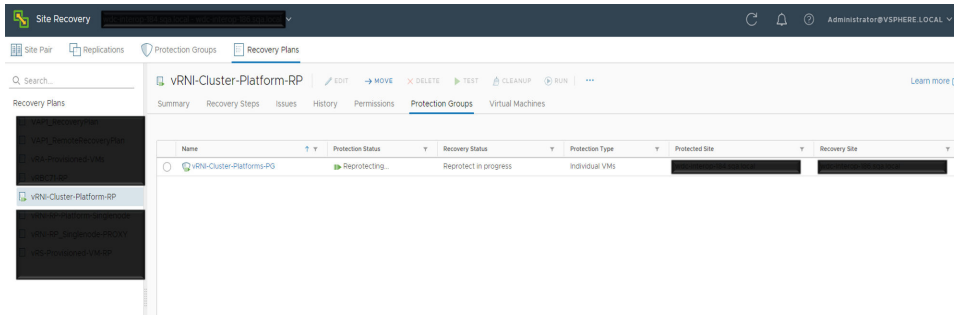
- 1 確認 SRM 在受保護和復原站台中已設定並啟動。
- 2 針對要保護的每個 vRealize Network Insight 節點設定複寫。在設定複寫時，為 vRealize Network Insight 執行個體提供足夠的復原點目標 (RPO) 時間。例如，若是具有單一平台和收集器節點 (中等大小) 的 vRealize Network Insight 部署，則 45 分鐘的 RPO 是合適的。但若是具有含大型區塊的節點的叢集，則應提供足夠的 RPO。快照間隔組態特定於使用者環境和需求。



3 建立保護群組。包括要在特定保護群組下保護的虛擬機器。



4 建立包含個別保護群組的復原計劃。



5 執行測試復原。這是為了確保復原計劃可按預期運作。

6 SRM 會建議使用者定期執行計劃移轉，以驗證現有 DR 計劃的完整性。

7 假設復原站台具有強制 vRealize Network Insight 虛擬機器使用新 IP 的網路組態。使用復原計劃復原 vRealize Network Insight 虛擬機器，該復原計劃假設已復原的虛擬機器沒有網路變更。在 vRealize Network Insight 中報告虛擬機器復原成功後，將新 IP 位址手動指派給 vRealize Network Insight 節點，套用新憑證，並重新初始化叢集。

8 由於目前不支援使用 SRM 自訂 IPv4，因此您可以使用 vRealize Network Insight 執行 DR，前提是沒有任何網路變更。

手動指派網路設定：

- 在所有平台節點上同時執行 `change-network-settings` 命令。
- 連續在 Platform1、Platform2 和 Platform3 中的節點上執行 `update-IP-change` 命令。
- 在收集器節點上執行 `vrni-proxy set-platform --ip-or-fqdn <with-updated-ip-of-Platform1>`。
- 檢查服務狀態。如果平台節點上的某些服務不在執行中，請按建議的順序將節點重新開機。

本章節討論下列主題：

- 常見資料來源錯誤
- 無法啟用 DFW IPFIX

常見資料來源錯誤

新增資料來源時，可能會遇到多個錯誤。此表列出了每個常見錯誤及其原因和解決方案。

表 22-1.

錯誤文字	原因	解決方案
從資料來源的回應無效 (Invalid Response from Data Source)	vRealize Network Insight Proxy 無法處理從資料來源收到的資訊，因為該資訊未採用預期格式。	在部分資料提供者中，此問題會間歇性地出現，並且在下一個輪詢週期中可能會消失。如果持續發生，請連絡支援。
無法從 Proxy 虛擬機器存取資料來源 (Data Source is not reachable from Proxy VM)	SSH/REST (連接埠 22 或 443) 上的資料來源 IP 位址無法從 vRealize Network Insight Proxy 虛擬機器進行存取，或資料來源沒有回應。新增資料來源時，會發生此錯誤。	確認從連接埠 22 或 443 上的 vRealize Network Insight Proxy 虛擬機器到資料來源的連線。確保資料來源已啟動且正在執行，並且防火牆未封鎖從 vRealize Network Insight Proxy 虛擬機器到資料來源的連線。
找不到 NSX Controller (No NSX Controller found)	在 NSX Manager 資料來源頁面中已選取 NSX Controller，但尚未安裝 NSX Controller。	在 NSX Manager 上安裝 NSX Controller，然後在 NSX Manager 資料來源頁面上選取 NSX Controller 核取方塊。
資料來源類型或版本不相符 (Data source type or version mismatch)	提供的資料來源 IP 位址/FQDN 不是所選的資料來源類型。	確認提供的資料來源 IP 位址/FQDN 屬於所選的資料來源類型，並且版本受 vRealize Network Insight 支援
連線至資料來源時發生錯誤 (Error connecting to data source)	vRealize Network Insight Proxy 虛擬機器無法連線到資料來源。新增資料來源後，會發生此錯誤。	確認從連接埠 22 或 443 上的 vRealize Network Insight Proxy 虛擬機器到資料來源的連線。確保資料來源已啟動且正在執行，並且防火牆未封鎖從 vRealize Network Insight Proxy 虛擬機器到資料來源的連線。
找不到 (Not found)	找不到 vRealize Network Insight Proxy 虛擬機器。	確認是否已在 vRealize Network Insight Proxy 虛擬機器和 vRealize Network Insight 平台虛擬機器之間進行配對。

表 22-1. (續)

錯誤文字	原因	解決方案
權限不足，無法啟用 IPFIX (Insufficient privileges to enable IPFix)	嘗試在 vCenter 中啟用 IPFIX 的使用者不具下列權限：DVSwitch.Modify；DVPortgroup.Modify	為使用者提供足夠的權限。
IP/FQDN 無效 (IP/FQDN is invalid)	在資料來源頁面上提供的 IP/FQDN 無效或不存在。	提供有效的 IP/FQDN 位址。
未收到資料 (No data being received)	vRealize Network Insight 平台虛擬機器未收到來自此資料來源的 vRealize Network Insight Proxy 虛擬機器的資料。	連絡支援。
無效的認證 (Invalid credentials)	提供的認證無效。	請提供正確的認證。
連線字串無效 (Connection string is invalid)	在資料來源頁面上提供的 IP/FQDN 未採用正確的格式。	提供有效的 IP/FQDN 位址。
由於處理延遲，最新的資料可能無法使用 (Recent data may not be available, due to processing lag)	vRealize Network Insight 平台虛擬機器超載，在處理時延遲。	連絡支援。
要求逾時，請再試一次 (Request timed out, please try again)	無法在指定的時間內完成要求。	再試一次。如果問題未修正，請連絡支援。
由於未知原因而失敗，請重試或連絡支援 (Failed for unknown reason, please retry or contact support)	由於某個未知原因，要求失敗。	再試一次。如果問題未修正，請連絡支援。
需要在裝置上對 SSH 啟用密碼驗證 (Password authentication for SSH needs to be enabled on device)	在新增的裝置上，停用使用密碼進行 SSH 登入	在新增以監控的應用裝置上對 SSH 啟用密碼驗證。
SNMP 連線錯誤 (SNMP connection error)	連線到 SNMP 連接埠時發生錯誤	確認已在目標裝置上正確設定 SNMP。

無法啟用 DFW IPFIX

vRealize Network Insight 不允許您啟用 DFW IPFIX。

問題

新增 VMware Cloud on AWS 的原則管理程式或來源時，如果您嘗試啟用 DFW IPFIX，則可能會看到下列錯誤訊息：

- 無法新增任何收集器。
- 提供的使用者不具所需角色。僅具有下列角色的使用者可以啟用 IPFIX：雲端管理員。

原因

- VMware Cloud on AWS 僅支援將四個收集器新增至其 DFW IPFIX 收集器設定檔。因此，當現有設定檔中已有四個收集器時，將會顯示

無法新增任何收集器

訊息。

Settings

Install and Support

Accounts and Data Sources

Data Management

IP Properties and Subnets >

Events >

User Management

Logs >

LDAP

Mail Server

SNMP Service

Property Templates

My Preferences

System Configuration

About

Add a New Policy Manager Account or Source of VMware Cloud on AWS

VCenter * [?](#) vcenter.sddc-35-162-64-191.vmwarevmc.com (VC VMC P... ▾)

Collector (Proxy) VM * Ni-Collector_10.153.189.42(Available Capacity: 951 VMs)
Tip: Want to increase capacity of your collector? [Click here](#)

IP Address/FQDN * nsxManager.sddc-35-162-64-191.vmwarevmc.com

CSP Refresh Token * [?](#) 6f60efe1-6d45-448f-b3d5-76e7e15c92bb

Validate ✓ Validation Successful

☐ **Enable DFW IPFIX**
Selecting this option will enable distributed firewall to send IPFIX flow record to the collector

❗ No new collectors can be added.

Nickname *

Notes Optional

Submit Cancel

- 使用者沒有寫入權限。僅具有雲端管理員角色的使用者可以在 VMware Cloud on AWS 原則管理程式上執行寫入作業。

Settings

Install and Support

Accounts and Data Sources

Data Management

IP Properties and Subnets >

Events >

User Management

Logs >

LDAP

Mail Server

SNMP Service

Property Templates

My Preferences

System Configuration

About

Edit Account or Source

VCenter * [?](#) vcenter.sddc-34-218-191-237.vmwarevmc.com (VC VMC ... ▾)

Collector (Proxy) VM * Ni-Collector_10.153.189.42(Available Capacity: 951 VMs)
Tip: Want to increase capacity of your collector? [Click here](#)

IP Address/FQDN * nsxManager.sddc-34-218-191-237.vmwarevmc.com

CSP Refresh Token * [?](#) 232add00-f35e-4d7d-af61-d6c06aa1d9c2

Validate ✓ Validation Successful

☐ **Enable DFW IPFIX**
Selecting this option will enable distributed firewall to send IPFIX flow record to the collector

❗ Provided user does not have the required role. Only users with the following role can enable IPFIX Enterprise Administrator, Cloud Administrator.

Nickname * POLICY VMC.M5P2

Notes Optional

Submit Cancel

解決方案

- ◆ 若要新增收集器，您必須：
 - 刪除現有收集器，或
 - 建立新設定檔，或
- ◆ 若要避免或修正使用者角色問題，請執行下列步驟之一：
 - 將**雲端管理員**角色指派給使用者，或
 - 以具有**雲端管理員**角色的使用者身分登入。

使用 vRealize Network Insight 規劃 應用程式移轉至 VMware Cloud on AWS

23

您可以使用 vRealize Network Insight 評估內部部署環境，以將應用程式移轉至 VMware Cloud on AWS 或 AWS。

步驟	程序	參考
步驟 1	設定您的環境	<ul style="list-style-type: none">■ 接受終端使用者授權合約 (EULA)。<ul style="list-style-type: none">a 建立 VMware 使用者帳戶，或登入 VMware 帳戶。b 更新註冊表單。 新使用者接收電子郵件以啟用其帳戶。c 接受 VMware 條款和終端使用者授權合約。■ 下載 OVA 檔案<ul style="list-style-type: none">a 登入 VMware 產品下載頁面，網址為：https://my.vmware.com/group/vmware/homeb 搜尋 vRealize Network Insight。c 下載最新的 vRealize Network Insight 平台和 Proxy OVA 檔案。■ 安裝準備。<ul style="list-style-type: none">a 驗證系統建議和需求。b 驗證支援的產品和版本。
步驟 2	部署	<ol style="list-style-type: none">1 部署 vRealize Network Insight 平台 OVA 檔案。2 啟用授權。3 產生共用密碼4 部署 vRealize Network Insight Proxy OVA 檔案。5 為 vRealize Network Insight 建立 VMware Cloud on AWS 防火牆規則。
步驟 3	資料來源新增	<ol style="list-style-type: none">1 登入 vRealize Network Insight。2 新增 VMware Cloud on AWS vCenter。3 新增 VMware Cloud on AWS NSX Manager。
步驟 4	模型應用程式	<ul style="list-style-type: none">■ 分析應用程式相依性<ul style="list-style-type: none">a 手動建立應用程式b 為實體 IP 建立層c 分析應用程式d VMware Cloud on AWS：規劃和微分割■ 第 19 章 建議的防火牆規則■ 第 20 章 使用搜尋查詢■ 看板

本章節討論下列主題：

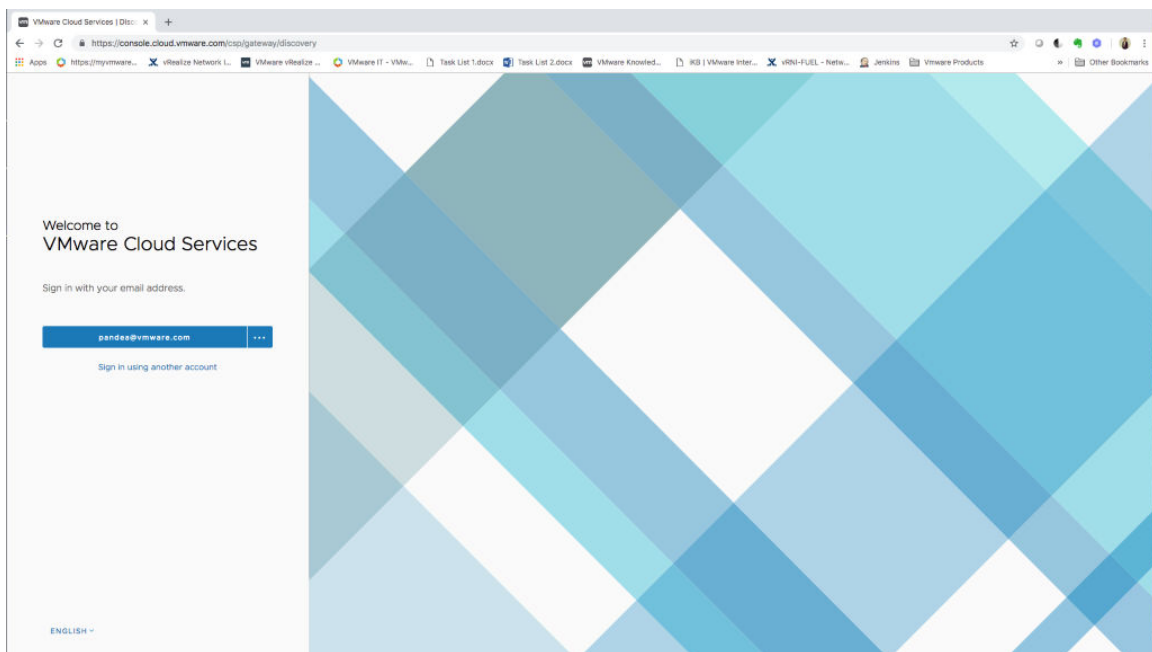
- 如何為 NSX Manager 取得 CSP 重新整理 Token
- 如何取得 vCenter 認證
- 計算閘道防火牆規則

如何為 NSX Manager 取得 CSP 重新整理 Token

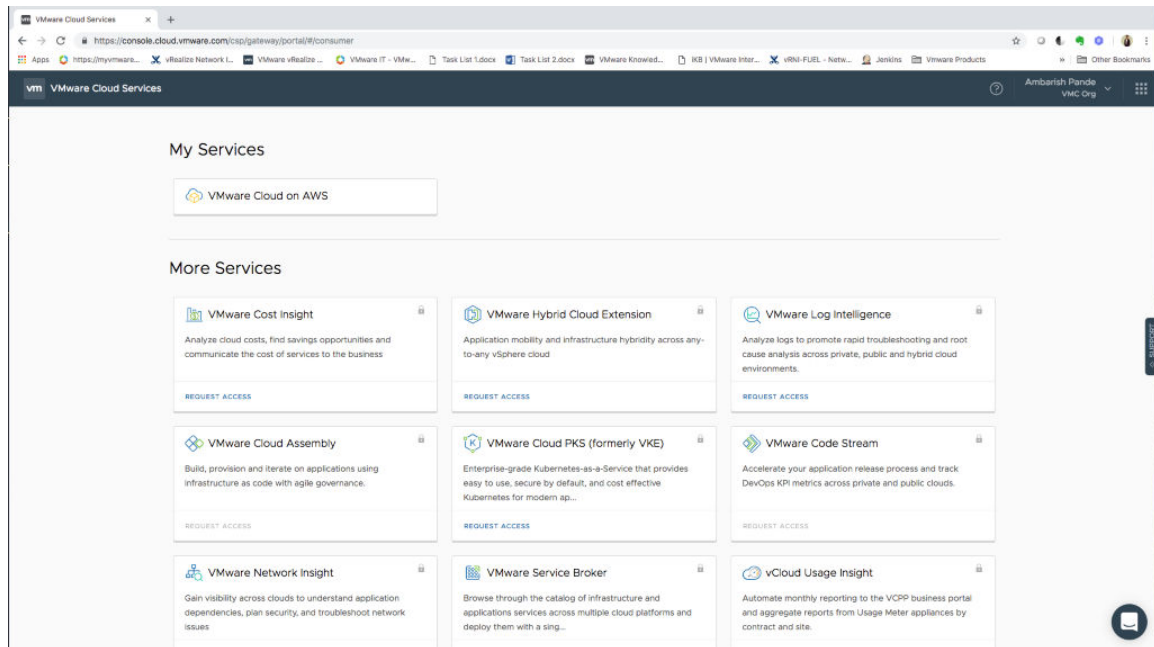
若要將 VMware Cloud on AWS NSX Manager 做為資料來源新增至 vRealize Network Insight，您需要重新整理 Token。

程序

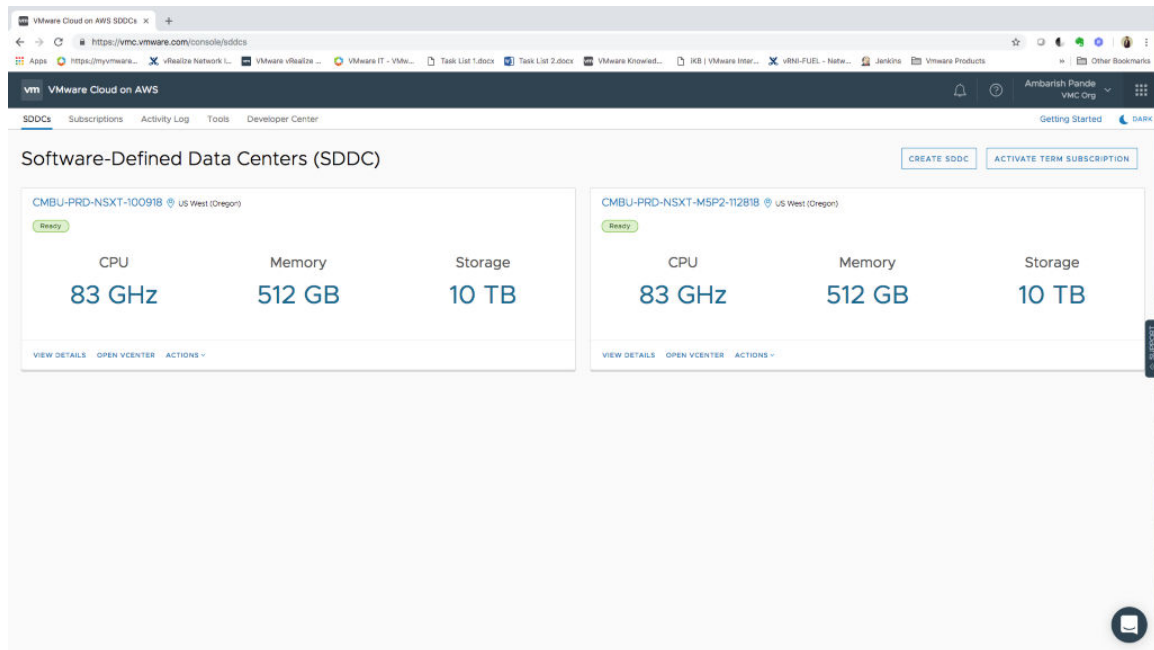
- 1 登入 VMware Cloud 服務主控台。



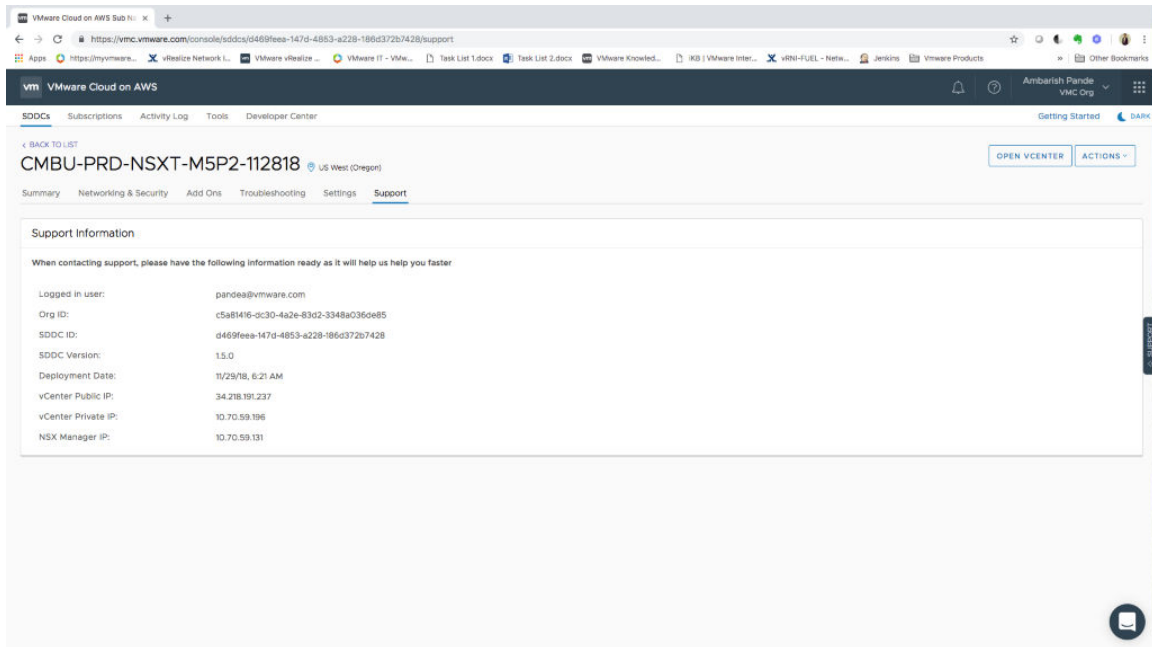
2 在 [我的服務] 下，按一下 VMware Cloud on AWS。



3 選取所需的軟體定義資料中心 (SDDC)。



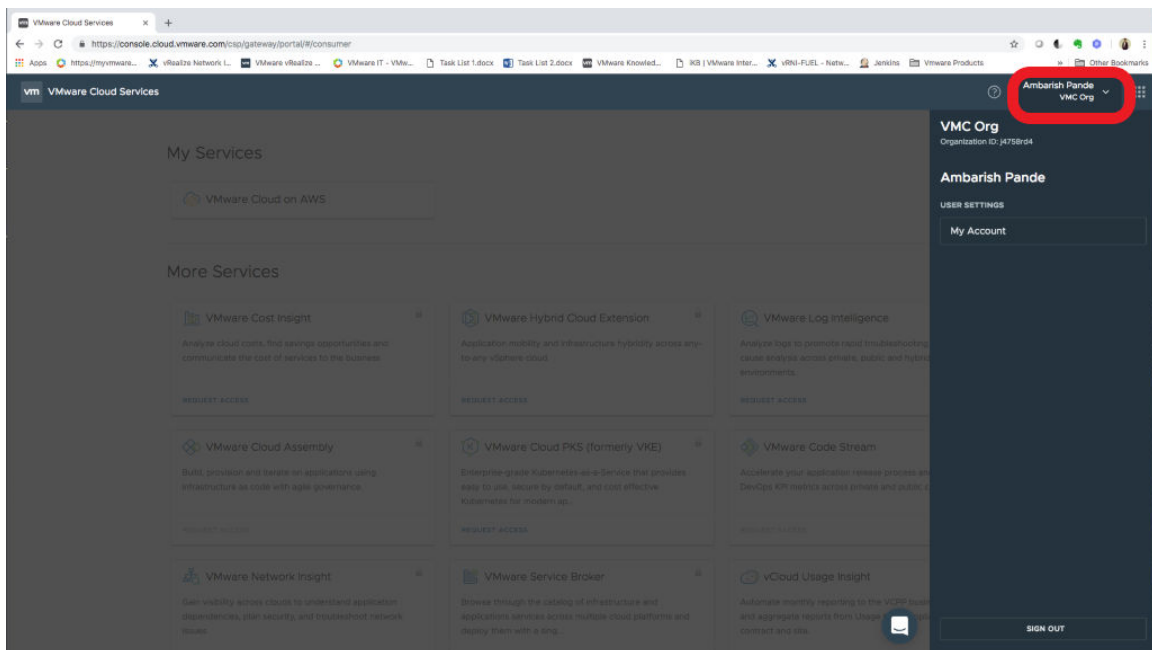
4 按一下支援索引標籤。



5 記下 NSX Manager IP 位址。

6 按一下上方橫幅中的組織名稱。

備註 確保該組織位於所選的 SDDC 中。



7 產生 API Token。

如需相關程序，請參閱〈[產生 API Token](#)〉。

備註 若要產生 API Token，您必須擁有**管理員**和**NSX Cloud 管理員**權限。

結果

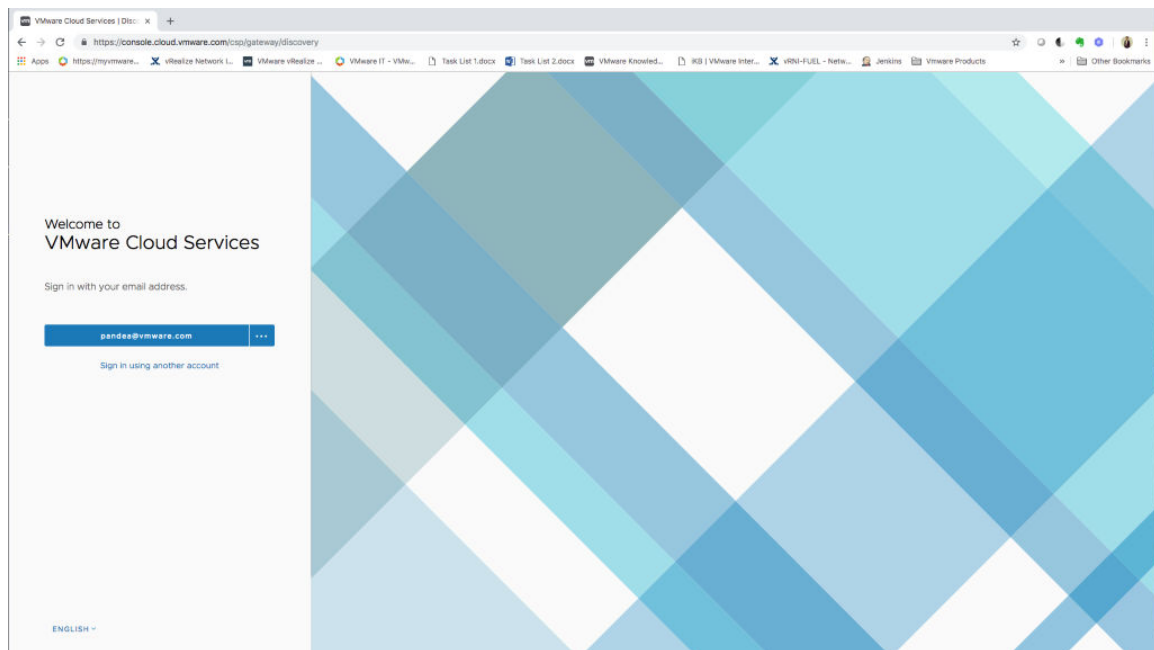
您可以使用此 Token 來驗證組織上的所有 VMware Cloud on AWS SDDC。

如何取得 vCenter 認證

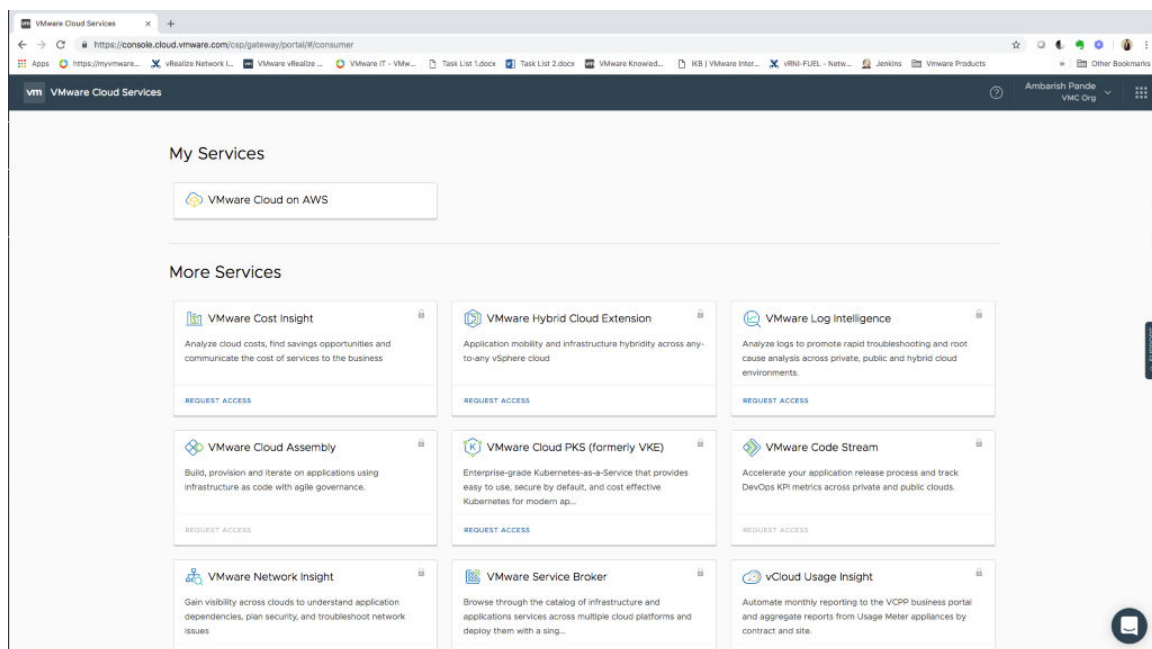
若要將 vCenter 資料來源新增至 vRealize Network Insight，您需要 vCenter 認證。

程序

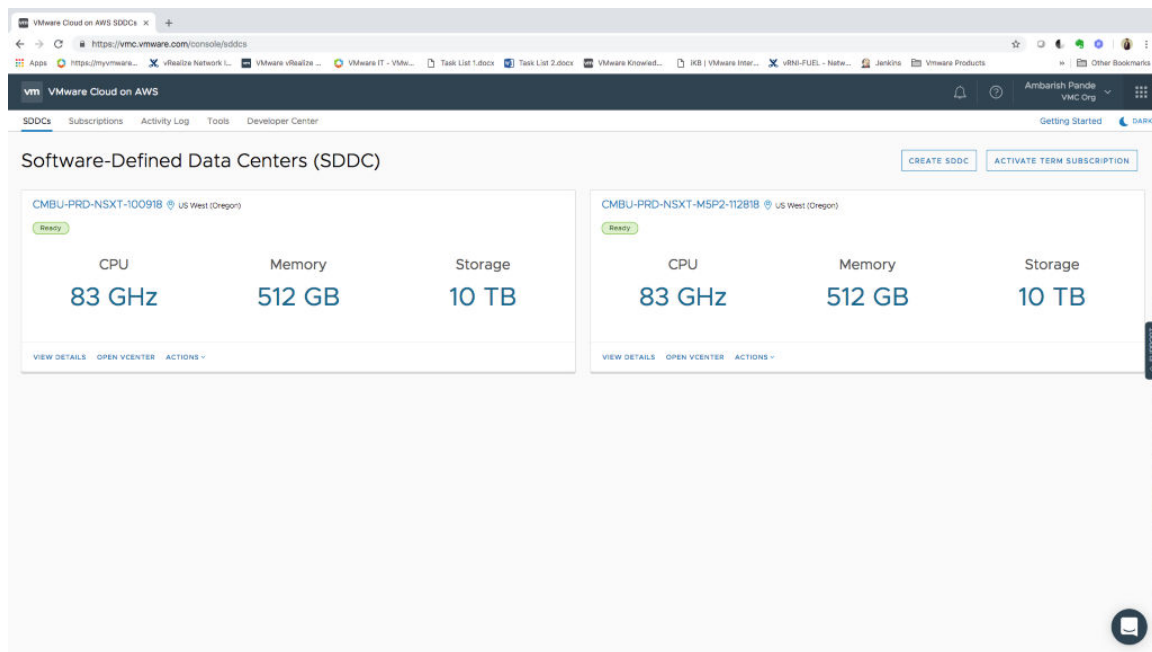
1 登入 VMware Cloud 服務主控台。



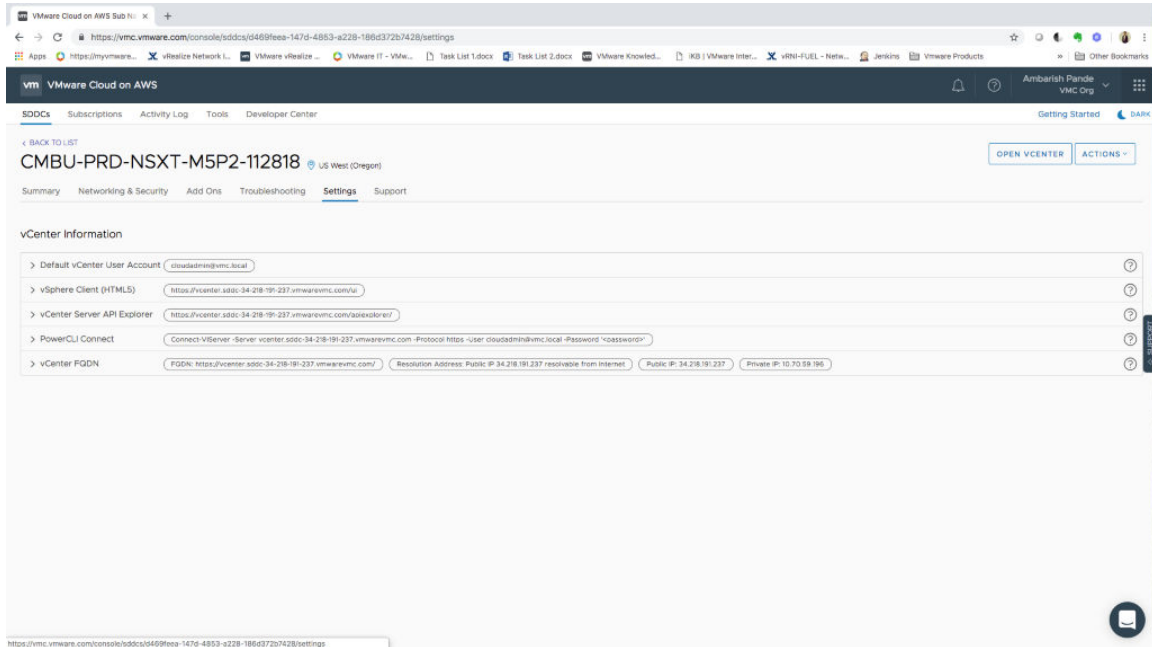
2 在 [我的服務] 下，按一下 VMware Cloud on AWS。



3 選取所需的軟體定義資料中心 (SDDC)。



4 按一下設定索引標籤。

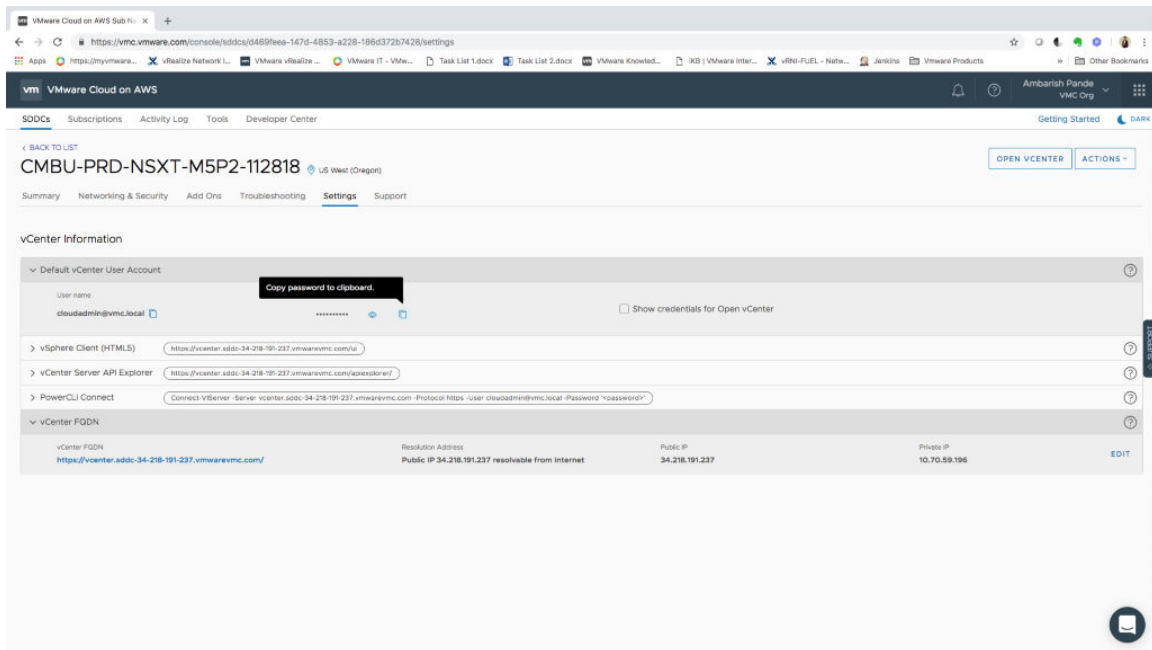


5 展開 vCenter FQDN。

記下 vCenter FQDN 詳細資料。

6 展開預設 vCenter 使用者帳戶，以取得使用者名稱和密碼。

複製密碼，並記下使用者名稱。



計算閘道防火牆規則

與 vRealize Network Insight 平台進行通訊時，收集器要求為傳出流量開啟 HTTPS 連接埠 443。

收集器可透過防火牆存取下列 VMware 主控的 URL：

- *.vmwareidentity.com
- gaz.csp-vidm-prod.com
- *.vmware.com
- *.ni-onsaas.com

此外，為了正常運作 vRealize Network Insight 或 vRealize Network Insight 收集器，應允許 NTP 和 DNS 流量。

使用下列詳細資料建立防火牆規則：

- 名稱：適當的描述性名稱
- 來源：包含收集器 IP 位址的 VMware Cloud on AWS 群組的名稱。
- 目的地：選取任何
- 服務 – 選取 HTTPS、DNS、DNS-UDP、NTP、ICMP
- 動作 – 允許
- 套用至 – 網際網路介面
- 記錄 – 視需要啟用記錄。