

# vRealize Network Insight 常見問題集

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](http://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 常見問題集指南 4
- 2 一般 5
- 3 安裝與組態 7
- 4 在 vRealize Network Insight 中新增或設定資料來源 12
- 5 微分割與流量 15
- 6 叢集 17
  - 叢集 - 一般 17
  - 叢集 - 安裝和設定 19
  - 叢集 - 調整 20
  - 叢集 - 部署 21
- 7 資料管理和處理 23
- 8 IPFIX 25

# 關於 vRealize Network Insight 常見問題集指南

1

vRealize Network Insight 常見問題集指南為使用者提供了關於 vRealize Network Insight 的常見問題。

## 適合對象

此資訊適用於使用 vRealize Network Insight 的使用者。

## 如何建立支援服務包？

請參閱《vRealize Network Insight 命令列參考指南》中的〈支援服務包〉一節。

## 如何在 Palo Alto Networks Panorama 中為 XML API 存取建立唯讀管理員角色？

為 XML API 存取新增**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，並開啟 [管理員角色設定檔] 對話方塊
- 3 在 [管理員角色設定檔] 對話方塊中
  - a 為角色指定名稱 (例如，api-only-admin)
  - b 選取**角色**為 **Panorama**
  - c 在 Web 使用者介面索引標籤中停用所有項目
  - d 在 XML API 索引標籤中啟用除**認可**以外的所有項目
  - e 按一下**確定**關閉對話方塊，新的**管理員角色**隨即與名稱一起出現在清單中
  - f 按一下**認可**以認可對 Panorama 進行的變更
- 4 將此**管理員**角色指派給管理員帳戶。

## 何時將服務視為共用？

下列連接埠已設定為共用：

通訊協定	連接埠
DNS	53
Bootpc	68
Kerberos	110

通訊協定	連接埠
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

## 資料來源上顯示事件/錯誤「資料來源身分識別資訊 (例如，憑證或金鑰) 已變更」。這意味著什麼？

vRealize Network Insight 已從資料來源收到新憑證，該憑證與產品中儲存的憑證不同。vRealize Network Insight 自動接受資料來源提供的憑證。在此程序期間，您將在可下載舊憑證和新憑證的資料來源中取得事件。

## 在 vRealize Network Insight 中匯入 DNS 記錄的限制是什麼？

匯入 DNS 記錄的限制如下：

- Infobox DNS 資料來源：您可以從一個資料來源匯入 90 萬筆記錄。
- 手動匯入 DNS 記錄：您可以使用多個 .csv 或繫結檔案 (封裝為一個 zip 檔案) 來匯入 DNS 記錄。您可以匯入的記錄數目沒有限制，但存在上傳限制，如下所示：
  - 單一 zip 檔案中的檔案數目 – 25
  - 單一 zip 檔案的大小上限 – 10 MB。

## vRealize Network Insight 的資源需求是什麼？

如需資源需求，請參閱《vRealize Network Insight 安裝指南》。

## 如果在 vRealize Network Insight Proxy OVA 部署期間輸入錯誤的金鑰，會怎樣？

在 vRealize Network Insight Proxy OVA 部署期間不會驗證秘密金鑰。即使秘密金鑰不正確，仍會完成部署。但是，配對會失敗，且 vRealize Network Insight Proxy 不會在 vRealize Network Insight 使用者介面上顯示為已偵測。

若要更正共用密碼，請登入 vRealize Network Insight Proxy CLI 並執行 `set-proxy-shared-secret` 命令以設定正確的秘密金鑰。此命令會將舊金鑰取代為新金鑰，因此，vRealize Network Insight 平台會偵測到 vRealize Network Insight Proxy 並進行配對。

## 如何在 vRealize Network Insight Proxy OVA 部署後設定 DNS？

登入 vRealize Network Insight Proxy CLI，並執行 `change-network-settings` 命令。此互動式命令將為使用者提供新增或修改 DNS 的選項，之後，將使用新的 DNS 重新設定 vRealize Network Insight Proxy。

如果有任何網路參數未正確設定，可使用 `change-network-settings` 命令修改網路組態參數。

## 如何從使用者介面中找到 vRealize Network Insight Proxy 虛擬機器 IP？

移至 [設定] 頁面並選取 [vRealize Network Insight 基礎結構] 功能表選項。會顯示 vRealize Network Insight 平台和 vRealize Network Insight Proxy 虛擬機器的 IP 位址。

## 如果在部署 vRealize Network Insight Proxy OVA 後的 5 分鐘內未偵測到 vRealize Network Insight Proxy，該怎麼辦？

使用 `consoleuser` 登入 vRealize Network Insight Proxy (請參閱 vRealize Network Insight 命令列介面指南)，並確認下列事項：

- 使用 CLI `show-connectivity-status` 確認 vRealize Network Insight 平台與 vRealize Network Insight Proxy 的配對狀態。
- 如果配對狀態顯示為 `Passed`，請在新的瀏覽器視窗中開啟平台使用者介面並登入以查看狀態。
- 如果配對狀態顯示為 `Failed`，則在 vRealize Network Insight Proxy OVA 部署期間指定的共用秘密金鑰可能有誤。若要修正此問題，請使用 `set-proxy-shared-secret` 命令設定正確的秘密金鑰。此命令會將舊金鑰取代為新金鑰，因此，vRealize Network Insight 平台會偵測到 vRealize Network Insight Proxy。
- 如果 `show-connectivity-status` 顯示與 vRealize Network Insight 平台的網路連線失敗，則使用 `ping` 命令確認是否可以從 vRealize Network Insight Proxy 虛擬機器連線到 vRealize Network Insight 平台。
- 如果無法連線，則使用 `show-config` 命令確認 NTP、DNS、閘道和其他網路參數是否已正確設定。
- 如果有任何網路參數未正確設定，可使用 `setup` 命令修改網路組態參數。

## 如果忘了登入認證，該怎麼辦？

如果您是使用者介面本機使用者：請連絡 vRealize Network Insight 使用者介面管理員以重設認證。

如果您是管理員：自 vRealize Network Insight 3.4 起，可以使用 CLI `modify-password` 變更使用者介面認證。如需詳細資料，請參閱 CLI 指南。如果使用的是 3.4 之前的 vRealize Network Insight 版本，請連絡支援。

## 如何變更登入密碼？

變更登入密碼：

- 1 移至**管理員 > 設定**，然後按一下左窗格中的**我的設定檔**。
- 2 在**變更密碼**頁面中，填寫所需的資訊，然後按一下**儲存**。

## 如果在偵測到 vRealize Network Insight Proxy 虛擬機器之前出現登入畫面，該怎麼辦？

- 如果在偵測到 Proxy 之前重新整理瀏覽器或在新視窗中開啟 URL，則會出現此行為。
- 使用在授權啟用期間為 `admin@local` 使用者名稱設定的認證登入。



## vRealize Network Insight 是否支援多個 vCenter Server/NSX Manager ?

是，vRealize Network Insight 支援多個 vCenter Server 和 NSX Manager。

## vRealize Network Insight 的哪些服務需要存取網際網路？為什麼？

vRealize Network Insight 支援遠端家庭呼叫功能，此功能需要存取網際網路。透過此功能或服務，vRealize Network Insight 團隊可以更深入地瞭解客戶環境並主動疑難排解或修復問題。下列服務需要存取網際網路：

- 自動更新服務 (svc.ni.vmware.com:443)：vRealize Network Insight 會使用此服務聯繫遠端升級主機，並在新釋放的位元套件可用時提取，並且使用者會在更新可用時取得使用者介面通知。此服務預設為啟用，但您可以透過使用者介面或透過 CLI 使用 `online-upgrade` 命令來停用此服務。
- 效能遙測服務 (svc.ni.vmware.com:443)：會定期為 vRealize Network Insight 收集和上傳與 vRealize Network Insight 的關鍵服務和效能相關的某些度量。支援團隊會監控這些度量並識別環境中的任何異常，進而採取行動以免影響任何關鍵服務。此服務預設為停用，但您可以透過 CLI 使用 `telemetry` 命令啟用/停用此服務。如需更多資訊，請造訪 <https://kb.vmware.com/s/article/59242>
- 支援服務 (support2.ni.vmware.com:443)：此服務會建立與 vRealize Network Insight 支援主機的遠端安全通道，以允許授權人員從遠端存取和使用部署。該服務預設為停用，可透過使用者介面以及「support-tunnel」CLI 進行啟用/停用。
- 登錄服務 (reg.ni.vmware.com:443)：用於向所有外部服務登錄應用裝置。它可以在上述提及的服務之間啟用信任通訊。當安裝程式能夠存取網際網路時，會自動進行登錄。在隔離環境中，可使用「offline-registration」CLI (請參閱 CLI 指南以取得詳細資料) 完成此操作。啟用支援通道時需要使用此服務。

**備註** 如果 vRealize Network Insight 平台位於網際網路 Proxy 後面，請將下列網域名稱和連接埠加入白名單：

表 3-1.

服務	URL	連接埠
升級服務/度量服務	svc.ni.vmware.com	443
支援通道服務	support2.ni.vmware.com	443
登錄服務	reg.ni.vmware.com	443

## 如何從應用裝置停用網際網路存取？

下列服務會使用安全的遠端/網際網路服務：

- 自動更新服務
- 效能遙測服務
- 支援服務
- 登錄服務

如需如何啟用或停用這些服務的相關資訊，請參閱 [vRealize Network Insight 的哪些服務需要存取網際網路？為什麼？](#) 常見問題。如果啟用了其中任何一項服務，則 vRealize Network Insight 需要網際網路存取權。

## 什麼是連接埠彙總以及執行彙總的機制是什麼？

已內建連接埠彙總功能，用於彙總暫時連接埠流量 - 例如，動態 FTP、Oracle、MS-RPC 等。這有助於減少系統中的流量數目，並針對本質上用於同一服務的大量流量提供彙總視圖。

執行彙總的機制如下所示：

- 在通知 `destination_ip` 的前三天，我們會將該特定 IP 上的目的地連接埠彙總到 10K 值區中，並開始為該 IP 建置連接埠設定檔（根據目的地 IP 建置連接埠設定檔）。
- 三天過後，已經建置了一個設定檔，我們將開始彙總連接埠密度較高的連接埠範圍（反映暫時連接埠開啟模式）。範圍本身為動態大小（例如 100、1,000、10,000），並且將根據開啟的連接埠數目及其在給定彙總範圍內的廣泛程度來建立。

---

**備註** 會針對每個伺服器的 IP 位址單獨做出此決定。

---

- 這將允許在沒有批次連接埠開啟活動的情況下報告高連接埠流量，但不會進行彙總，此外，還允許在發生此類活動的情況下套用動態彙總。
- 該設定檔會以時間衰減的方式不斷更新，以說明正在開啟新的連接埠或不再使用舊的連接埠。

## 如何在 vRealize Network Insight OVA 部署後變更 IP 位址、閘道或網路遮罩？

若要變更 vRealize Network Insight 平台/Proxy 網路設定，請登入 CLI 並執行 `change-network-settings` 命令。此互動式命令將為使用者提供修改 IP 位址、閘道、網路遮罩等的選項，之後，將使用新的詳細資料重新設定 vRealize Network Insight 應用裝置。

---

**備註**

- 必須使用虛擬機器主控台工作階段完成此工作，因為應用裝置最後會重新開機。
- 如果 vRNI 平台 IP 已修改並與 Proxy 進行配對，則在每個 Proxy 虛擬機器上執行此 CLI 命令：

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

---

## 如何從評估授權變更為永久授權？

請參閱《vRealize Network Insight 使用者指南》中的〈新增和變更授權〉一節。

## vRealize Network Insight 中的授權有哪些特性？

表 3-2.

授權名稱	授權類型	功能
企業	完全/生產：可以是永久的，也可以與時間繫結。	已啟用下列功能： <ul style="list-style-type: none"> <li>■ AWS 做為資料提供者</li> <li>■ 可調整資料保留原則</li> <li>■ Infoblox DNS 資料來源</li> <li>■ 實體 IP 和 DNS 對應</li> <li>■ 分析</li> </ul>
進階	完全/生產：可以是永久的，也可以與時間繫結。	不適用

**備註** 所有授權的容量均按 CPU 通訊端和 CCU (並行使用者) 進行計算。可以透過使用者介面 -> 設定 -> 關於使用更新的金鑰將評估授權更新或轉換為生產。如需詳細資料，請參閱使用者指南。

## 如何為 vRealize Network Insight 中的虛擬機器建立備份？

請參閱《VMware 最佳做法》以建立虛擬機器的備份，例如 VMware VADP/VDP API。建議您先執行備份，再建立或擴充叢集。

# 在 vRealize Network Insight 中新增 或設定資料來源

## 4

### 如果在使用 IP 位址新增 vCenter Server 時收到「要求逾時」訊息，該怎麼辦？

- 確認是否可從 vRealize Network Insight Proxy 虛擬機器連線到 vCenter Server IP 位址。
- 登入 vRealize Network Insight Proxy CLI，並使用 `ping` 確保可連線到 IP，並使用 `telnet` 確保可在連接埠 443 上連線到 vCenter Server。
- 如果可以連線到 vCenter Server，則重試新增。
- 如果無法連線到 IP 位址，則使用命令 `show-config` 確認是否已從 vRealize Network Insight Proxy 虛擬機器正確設定閘道。
- 如果閘道不正確，則使用 `setup` 命令進行更正。

### 如果在新增 vCenter Server 時收到「IP/FQDN 無效」訊息，該怎麼辦？

- 確認針對 vCenter Server 提供的 IP/FQDN 是否正確。
- 確認是否可以使用 `ping` 命令從 vRealize Network Insight Proxy 虛擬機器存取 FQDN。
- 如果無法存取，則使用 `nslookup FQDN` 和 `show-config` 命令確認是否已在 vRealize Network Insight Proxy 虛擬機器上正確設定 DNS。
- 如果 DNS 不正確，則使用 `setup` 命令進行更正。

### vRealize Network Insight 安全和操作平台需要哪些權限？

vRealize Network Insight 需要具有下列權限的 VMware vCenter Server 認證：

- Distributed Switch：修改
- dvPort 群組：修改

## 如果在 vCenter Server 資料來源頁面上啟用 IPFIX 時收到「使用者不具有所需權限」錯誤，該怎麼辦？

vRealize Network Insight 需要具有下列權限的 VMware vCenter Server 認證才能啟用 IPFIX：

- Distributed Switch：修改
- dvPort 群組：修改

請確保所提供的 VMware vCenter Server 使用者對 vCenter Server 的根資料夾及其所有子實體 (例如，所有資料夾和所有資料中心) 具有權限。

## 從環境擷取資料的頻率是多少？

vRealize Network Insight Proxy 每 10 分鐘從環境擷取一次資料。

## 新增 vCenter Server 後多久開始分析資料？

新增 vCenter Server 後將立即開始分析資料。產品使用者介面將在幾分鐘內顯示部分資料圖片，這可能需要兩個小時才能完全顯示。

---

**備註** 流量資料不斷變更，並在其分析中包含至少 24 小時的資料。

---

## 如果刪除了 vRealize Network Insight OVA，該如何清理 vCenter Server 中的 IPFIX 設定？

- 使用 VMware vSphere Web Client：移至首頁 > 網路 > VDS (名稱) > Netflow 設定。從收集器設定中移除 vRealize Network Insight Proxy IP。
- 使用 VMware vSphere Windows 用戶端：移至首頁 > 詳細目錄 > 網路 > VDS (名稱) > 編輯設定。從 Netflow 索引標籤的收集器設定中移除 vRealize Network Insight Proxy IP。對於啟用了 IPFIX 的每個 VDS，都需要執行此步驟。

## 如何清理 vRealize Network Insight 中的 IPFIX 組態？

在 vRealize Network Insight 使用者介面中，移至設定 > 資料來源，刪除 vCenter Server。這會移除 vRealize Network Insight 所執行的 IPFIX 組態。

## 在 vRealize Network Insight 中新增 VMware NSX Manager 後，在虛擬機器-虛擬機器路徑中顯示正確的防火牆規則需要多長時間？

在 vRealize Network Insight 中新增 VMware NSX Manager 後，最多可能需要 24 小時才能計算虛擬機器與防火牆規則的關聯性。

## 在 vRealize Network Insight 中新增 VMware vCenter 後，為何在虛擬機器-虛擬機器路徑中看不到 PNIC？

通常，在 vRealize Network Insight 中將 VMware vCenter 新增為資料來源後，vRealize Network Insight 計算虛擬機器-虛擬機器路徑需要大約 2 小時。但在某些罕見的情況下，在 vRealize Network Insight 中新增 VMware vCenter 後，可能需要大約 8-10 小時才能在虛擬機器-虛擬機器路徑中正確顯示 PNIC。

## 流量分佈釘選項中的數字代表什麼？

百分比提供了基於流量分析的流量分佈概觀。

表 5-1.

流量	說明
東西向 (EW)	東西向流量佔群組總計流量的百分比
已交換 (佔東西向流量的百分比)	交換流量佔東西向流量的百分比
已路由 (佔東西向流量的百分比)	路由流量佔東西向流量的百分比 (%)
在主機內 (佔虛擬機器-虛擬機器流量的百分比)	同一主機上來源和目的地的流量佔虛擬機器至虛擬機器流量的百分比
虛擬機器至虛擬機器 (佔東西向流量的百分比)	虛擬機器至虛擬機器的流量佔東西向流量的百分比
網際網路	網際網路流量佔群組總計流量的百分比

## 如何在流量中彙總連接埠？

已內建連接埠彙總功能，用於彙總暫時連接埠流量 - 例如，動態 FTP、Oracle、MS-RPC 等。這有助於減少系統中的流量數目，並針對本質上用於同一服務的大量流量提供彙總視圖。執行此操作的機制如下所示：

- 在通知 destination\_ip 的前三天，我們會將該 IP 上的目的地連接埠彙總到 10K 值區中，並開始為該 IP 建置連接埠設定檔。
- 三天過後，已經建置了可以放心使用的設定檔，我們將開始彙總連接埠密度較高的連接埠範圍 (換句話說，反映暫時連接埠開啟模式)。範圍本身為動態大小 (100、1,000、10,000)，並且將根據開啟的連接埠數目及其在給定彙總範圍內的廣泛程度進行建立。
- 這將允許在沒有批次連接埠開啟活動的情況下報告高連接埠流量，但不會進行彙總；此外，還允許在發生此類活動的情況下套用動態彙總。
- 該設定檔會以時間衰減的方式不斷更新，以說明正在開啟新的連接埠或不再使用舊的連接埠。

## 240.240.240.240 IP 位址在 vRealize Network Insight 中表示什麼？

240.240.240.240 是 vRealize Network Insight 中的預留位置 IP 位址。如果有大量 IP 位址 (> 5000) 叫用某個特定 IP，則使用此 IP 位址。可以將該服務端點的所有後續傳入網際網路 IP (自第 5001 個起) 取代為此預留位置 IP 240.240.240.240。

這是為了限制系統中的流量數目，因為單獨記錄每個網際網路用戶端的公開服務可能會造成大量流量，從而增加系統負載。

對於已取代為此預留位置 IP 的所有流量，所有度量都彙總在具有此 IP 位址的對應流量中，因此，在彙總層級不會遺失統計資料。

流量視圖中所報告流量的所有目的地 IP 都顯示為來自 240.240.240.240，實際上，這些流量由大量網際網路 IP (> 5000) 叫用。



本章節討論下列主題：

- 叢集 - 一般
- 叢集 - 安裝和設定
- 叢集 - 調整
- 叢集 - 部署

## 叢集 - 一般

是否可以將 Proxy 或收集器虛擬機器叢集化？

否。不支援對收集器/Proxy 虛擬機器進行叢集化。

**vRealize Network Insight 是否需要 vRealize Log Insight 等負載平衡器？**

vRealize Network Insight 叢集化是擴充解決方案，而不是 HA 解決方案。如果主要平台虛擬機器/主節點出現故障，則整個服務無法使用。

**如果遠端 Proxy 與平台之間的連線中斷，會怎樣？**

如果平台與 Proxy 虛擬機器之間的連線已中斷，Proxy 虛擬機器會在本機儲存資料 (取決於磁碟空間)，並在連線恢復時將其傳送。

**vRealize Log Insight 是否與 vRealize Network Insight 整合？**

是，vRealize Log Insight 已與 vRealize Network Insight 3.4 整合。會將警示傳送至 Syslog (可能為 vRealize Log Insight)。

**如果節點重新開機，會怎樣？**

如果節點重新開機，它會自動加入叢集並繼續運作。如果是主要節點，則服務會在節點關閉期間完全遺失。

## 如何變更叢集中任何平台節點或收集器的 IP ？

在叢集中，您可以使用 CLI 命令變更任何收集器或平台節點的 IP。

### 備註

- 執行此作業之前，請連絡 VMware 支援。
  - 應用裝置會在程序結束時重新開機。因此，您必須在虛擬機器主控台上執行這些步驟。
- 
- 若要變更收集器 IP，請執行 `change-network-settings` 命令。
  - 若要變更平台 IP，請執行以下作業：
    - a 執行 `change-network-settings` 命令。
    - b 在所有其他平台上執行 `update-IP-change` 命令，以反映其新 IP。
    - c 對收集器執行 `show-connectivity-status` 命令，並搜尋 **Platform VM IP/URL**，以識別其是否與此平台相關聯。
    - d 執行 `vrni-proxy`，以反映相關聯收集器上的新平台 IP。

使用案例 1：在 3 節點的叢集中，僅變更平台 2 的 IP。沒有任何收集器顯示與其相關聯。

- 1 在平台 2 上執行 `change-network-settings`。
- 2 在平台 1 和平台 3 上執行 `update-IP-change` 以反映平台 2 的新 IP。

使用案例 2：在 3 節點的叢集中，變更平台 1 和平台 2 的 IP。收集器 A 與平台 2 相關聯，其餘收集器與平台 3 相關聯。

- 1 在平台 1 上執行 `change-network-settings`。
- 2 在平台 2 上執行 `change-network-settings`。
- 3 在平台 2 和平台 3 上執行 `update-IP-change platform1-oldIP platform1-newIP`。
- 4 在平台 1 和平台 3 上執行 `update-IP-change platform2-oldIP platform2-newIP`。
- 5 在收集器 A 上執行 `vrni-proxy set-platform --ip-or-fqdn platform2-newIP`。

## 平台 1 上需要多少磁碟空間？

與叢集中的其他節點相比，平台 1 需要更多磁碟空間，因為某些組態資料僅儲存在平台 1 上。

## 如果有任何節點的磁碟空間不足，會怎樣？

當任何特定平台節點上的磁碟空間達到某個臨界值時，使用者介面將開始顯示錯誤訊息。登入 vCenter 以將更多磁碟空間新增至平台節點。

## 將在叢集中複寫多少次資料？

資料複寫機制取決於平台節點中存在的元件。

## 叢集 - 安裝和設定

### 所有平台虛擬機器都必須位於相同的 L2/L3 區段上嗎？

否。但是，最好將所有平台節點置於一個常用網路上，以減少節點之間的延遲。這是因為許多分散式元件會在節點之間複寫資料，且高延遲可能會導致系統效能和穩定性問題。

### 可以使用產品中的升級功能來升級叢集嗎？

在 3.7 之前，叢集不支援線上升級。從 3.8 及後續版本開始，叢集可使用線上升級方式進行升級。

### 如果在叢集建立程序期間出現故障，會怎樣？

最佳做法是在啟動叢集建立程序之前為主要平台和 Proxy 建立快照。如果出現故障，則刪除次要平台節點，然後從快照中復原主要平台和 Proxy 虛擬機器。

### 將單一節點部署擴充至叢集時，現有資料和組態會發生什麼變化？

所有資料和組態會保持不變。建立叢集後，將可存取資料。

### 您可以將平台虛擬機器放在不同的區域中嗎？

否，我們要求平台節點共同置於相同的站台中。Proxy 伺服器可以按地理分佈。

### 平台是否可以主控於 vSAN 延伸叢集 (2 個資料中心)？

是，相同資料中心內或跨資料中心的 vSAN 叢集仍可確保一定的 IO 效能，例如本機儲存區。

### 是否可以將叢集節點主控於不同的 vSAN 叢集？

是，平台叢集的不同節點可主控於不同的基礎資料存放區。

### 是否需要備份平台節點？

是，必須使用 VMware 建議的快照/備份技術來執行備份。

### 如何估計一個區域上的叢集 Proxy 虛擬機器與另一個區域上的平台虛擬機器叢集之間的頻寬？

在某些大型部署中，我們看到此數值的範圍介於 1 mbps 到 20 mbps 之間。將資料傳送至平台虛擬機器之前，在 Proxy 虛擬機器中進行了大量重複資料刪除或壓縮操作。

### 叢集節點之間的網路流量是多少？

流量通常取決於叢集大小與資料中心環境的類型。

對於具有 30-50k 虛擬機器的安裝：

- 在叢集之間：約為 50-400Mbps

- 在 Proxy 與平台之間：約為 100Kbps-15Mbps

## 叢集中節點之間允許的最大延遲是多少？

平台節點必須共同置於相同的站台中。在此類情況下，可達到最小延遲。如果平台節點主控於 vSAN 延伸叢集 (兩個資料中心)，則相同資料中心內或跨資料中心的 vSAN 叢集仍可確保一定的 IO 效能，例如本機儲存區。在資料中心 (例如 vRealize Network Insight) 上執行的應用程式將正常運作。您可以將平台叢集的不同節點主控於不同的基礎資料存放區。但是需要確保叢集中的所有平台虛擬機器共同置於相同的站台。

## 一個區域上的 Proxy 虛擬機器與另一個區域上的平台虛擬機器叢集之間允許的最大延遲是多少？

您的設定中可以有按地理分佈的 Proxy。Proxy 虛擬機器與平台虛擬機器之間存在 HTTPS 連線，因此它可以容許高延遲 (以數秒指定)。vRealize Network Insight 支援一個叢集中最多有 10 個節點 (30,000 個含流量的虛擬機器或 50,000 個不含流量的虛擬機器)。

## Proxy/平台虛擬機器的大小應為多少？

使用大型區塊組態：請參閱安裝指南。

## 叢集 - 調整

### 是否可以延伸已建立的叢集？

是，支援將叢集延伸至最多 10 個節點。

### 如果非主要平台虛擬機器變得無法使用，會怎樣？

內部服務對非主要節點故障的復原能力有限。一般而言，由於節點故障，主機會失去計算能力。

### 支援何種類型的負載平衡？

已修正 Proxy 與平台的對應。一旦任何 Proxy 虛擬機器中的資料到達任何平台虛擬機器，便會在所有平台虛擬機器內部之間對其處理進行負載平衡。

### 建立平台叢集是否會增加頻寬耗用量？

Proxy 或收集器虛擬機器僅繼續與主要或平台虛擬機器進行通訊。平台虛擬機器叢集通訊的頻寬需求最低。因此，頻寬耗用量不會顯著增加。

### Proxy 虛擬機器與平台虛擬機器之間的資料傳輸頻率是多少？

Proxy 虛擬機器會持續將執行重複資料刪除或壓縮的資料傳送至平台虛擬機器。

## 是否在 Proxy 虛擬機器中執行任何資料最佳化？

會在 Proxy 虛擬機器中執行各種重複資料刪除、壓縮、縮減或批次處理步驟。當虛擬機器平台與 Proxy 虛擬機器之間的連線關閉時，Proxy 虛擬機器會在本機儲存資料 (取決於磁碟空間)，並在連線還原時將其傳送。

## 是否對網路頻寬進行了任何最佳化？

是，會在 Proxy 虛擬機器上執行各種重複資料刪除/壓縮/縮減/批次處理步驟。

## 是否可以在 Proxy 伺服器上執行叢集化？

否。無法在 Proxy 伺服器上執行叢集化。

## vCenter 如何將流量傳送至 Proxy 伺服器？

vCenter 不會將流量傳送至 Proxy 伺服器。Proxy 伺服器實際上連線到其指定的 vCenter 以擷取資訊。

## 部署叢集時，vCenter 如何將流量傳送至各個 Proxy 伺服器？

實際上 Proxy 會連線到 vCenter 以擷取資訊。相應的 Proxy 將連線到指定的 vCenter 並擷取資訊。無法在 Proxy 上進行叢集化

## 叢集 - 部署

### 如何在擴充叢集後存取使用者介面？

只能從平台 1 存取使用者介面。

### 什麼是平台 1，為何需要記住此節點？

從中起始叢集建立程序的平台節點被視為平台 1。在叢集的 n 個節點中，只能從此節點存取使用者介面。

### 如果使用者介面存取權僅限於平台 1，如何從叢集中的其他節點擷取資料？

資料中心的資料會散佈在叢集中的所有節點之間。當使用者介面層在平台 1 上申請資料時，平台 1 節點會取得儲存在所有節點上的資料並向使用者介面傳送回應。

### 我可以部署在不同資料中心的平台節點來建立叢集嗎？

叢集中的所有節點會相互交換資料。因此，若要避免延遲問題，建議使用部署在相同資料中心內的平台節點來建立叢集

### 當我擴充平台節點時，現有平台上的資料會發生什麼變化？

現有平台節點上的資料會保留並散佈在叢集中的所有節點之間。

## Proxy 虛擬機器數目對於確定需要所需的平台區塊數是否重要？

否。只有所有 vCenter 中的虛擬機器總數和流量狀態 (已啟用或已停用) 會影響所需的區塊數目。請參閱《vRealize Network Insight 安裝指南》中的區塊模型資料表。

## vCenter 數目、實體裝置 (例如路由器) 數目或任何其他類型的資料來源的數量是否會影響所需的平台區塊數？

否。只有所有 vCenter 中的虛擬機器總數和流量狀態 (已啟用或已停用) 會影響所需的區塊數目。請參閱《vRealize Network Insight 安裝指南》中的區塊模型資料表。

## vRNI 是否支援平台叢集散佈在 2 個資料中心之間以實現 HA？

否。平台叢集不支援散佈在多個資料中心之間。所有平台叢集虛擬機器應位於同一個站台中。平台叢集目前不支援 HA。此功能已列在藍圖中。客戶可以跨 2 個站台使用 SRM 執行災難復原以實現 HA。

## vRNI 是否支援具有超過 6000 個虛擬機器且啟用了流量的單一 vCenter？

在版本 3.5 之前，vRNI Proxy 不支援從具有超過 6000 個含流量的虛擬機器的單一大型 vCenter 收集資料。此功能已列在藍圖中。

## 平台 1 上需要多少磁碟空間？

與叢集中的其他節點相比，平台 1 需要更多磁碟空間，因為某些組態資料僅儲存在平台 1 上。

## 如果有任何節點的磁碟空間不足，會怎樣？

當任何特定平台節點上的磁碟空間達到某個臨界值時，使用者介面將開始顯示錯誤訊息。登入 vCenter 以將更多磁碟空間新增至平台節點。

## 將在叢集中複寫多少次資料？

資料複寫機制取決於平台節點中存在的元件。

## 叢集如何運作？

- 部署中的所有 Proxy 都連線至一個平台 (平台 1)。平台和 Proxy 之間的連線是透過 https 在連接埠 443 上進行的。因此，僅連接埠 443 對平台 1 中的 Proxy 可見。
- 收到來自 Proxy 的申請後，平台 1 節點會以循環配置資源方式將申請負載平衡到叢集中的其他平台節點。
- 平台節點會將資料標準化並放在訊息佇列中，以由計算引擎進行處理。
- 計算引擎使用資料複寫機制將資料散佈在叢集中的所有節點之間。如此一來，如果叢集中的任何節點 (除了平台 1) 出現故障，都不會有任何資料遺失情況。
- 部分組態資料會明確儲存在未複寫的平台 1 節點上。這是高可用性解決方案不受支援的原因。

## 在邊界條件下，例如，平台-Proxy 伺服器通訊中斷時，資料處理管線會如何表現？

- 預設保留期間是多久？

30 天。可以使用企業授權從使用者介面增加天數。附註：增加時，請確保遵循磁碟準則。

- 如何在 Proxy 上處理資料？

Proxy 上的所有資料將在傳送至平台 (包括流量資料) 之前都轉換為 SDM (自描述訊息)。其中包括任何資料來源中的所有組態、詳細目錄和度量資料。如果無法連線到平台或將 SDM 上傳至 Kafka 佇列失敗，則會將其寫入 Proxy 虛擬機器上的磁碟中 (位於 /var/BLOB\_STORE 下)。

- 何時開始清除 Proxy 上的資料？

對於非流量資料：配置了 10 GB 空間用於在磁碟 (BLOB\_STORE) 上儲存 SDM。當此存放區填滿時，收集器會開始刪除較舊的 SDM 並將新的 SDM 新增到磁碟。這取決於從所有資料來源收集的資料大小以及超出此限制的速度。

對於流量資料：配置了 15 GB 空間用於儲存原始流量 (位於 /var/flows/vds/nfcapd 下)。只要耗用此空間，流量處理器就會開始刪除較舊的流量檔案。如果傳入原始流量速率約為 2M/分鐘，則大約需要 10 小時才會開始輪替。

- 清除邏輯是什麼？

首先刪除最舊的 SDM。

- 何時在 Proxy 中停止處理新資料？

只要服務正常執行，就永遠不會停止。

- 假設平台和 Proxy 之間中斷連線並且沒有滿足清除條件，則在重新連線時是否會在平台上協調所有資料？

儲存在磁碟上的所有資料都將傳送至平台。除非平台上存在資料遺失情況 (更多資訊如下)，否則應進行完全協調。

- 在平台上發生資料遺失情況有哪些條件？

平台開始捨棄 Kafka 佇列上的 SDM 超過 6 小時 (若為 3 節點叢集，則為 18 小時)。另一個可能性是佇列處於飽和狀態。當系統中存在滯後且傳入資料速率較高時，可能會發生這種情況。

- 最新的 SDM 是先發佈還是按照該順序中為最早的一個？

首先傳送最舊的 SDM。在 3.9 版本之前存在一個已知問題，該問題會導致部分資料遺失。如需詳細資訊，請連絡 GSS。

- 如果不存在任何通訊問題，是否會將資料儲存在 Proxy 中的磁碟上，然後再將其推送至平台？

如果不存在任何通訊問題，則不會將 SDM 儲存在磁碟上。該資料會自行從記憶體傳送至平台。僅當 Proxy 收到傳送 SDM 出現問題時，才會將資料儲存在磁碟上。

- 如果出現任何問題，Proxy 如何知道哪個是上次處理的流量檔案？

流量處理器會在資料庫中保留上次處理的 nfcapd 檔案的書籤。

- 如果沒有任何問題，則可以處理的 SDM 大小上限為何？使用者如何瞭解是否超出此限制？

SDM 大小限制為 15 MB。從 3.9 版本開始，只要平台捨棄大型 SDM，都會引發事件。



## 什麼是 IPFIX ？

IPFIX 是用於匯出流程資訊的 IETF 通訊協定。流量定義為在特定期間內傳輸且共用 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。流量資訊可能包含時間戳記、封包/位元組計數、輸入/輸出介面、TCP 旗標、VXLAN 識別碼、封裝的流量資訊等內容。這通常稱為 Netflow。但是，IPFIX 是標準的 IETF 通訊協定。

## VDS 匯出哪些流量資訊 ？

可將 vSphere 環境中的 VDS 設定為使用 IPFIX 匯出流程資訊。在附加到 VDS 的所有連接埠群組上啟用流量監控。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 上啟用流量監控時，便會發出相應的流量記錄。每個流量記錄的方向設定為「出口」。

## vRealize Network Insight 如何使用 IPFIX ？

vRealize Network Insight 會使用 VMware VDS IPFIX 收集網路流量資料。每個工作階段具有兩個路徑。例如：工作階段 A↔C 具有 A→C 封包和 C→A 封包。若要分析任何工作階段的完整資訊，需要有關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。

## 如何疑難排解 vRealize Network Insight 流量收集 ？

- 1 請確保特定的 VDS 及其 DVPG 和上行內容已啟用 Netflow 監控，並且收集器 IP 位址是 vRealize Network Insight 收集器的 IP 位址。
- 2 IPFIX Netflow 封包被防火牆 (NSX、虛擬或實體) 捨棄。請確保在 ESXi 主機和 vRealize Network Insight 收集器之間的路由中可能存在的任何防火牆，都允許傳送到 vRealize Network Insight 收集器 IP 上 UDP 連接埠 2055 的 Netflow 封包。
- 3 ESXi 主機已停止傳送 IPFIX Netflow 封包。如果無法連線到 UDP 連接埠 2055，ESXi 主機將在一段時間後停止傳送 Netflow 封包。這可能是由於防火牆捨棄封包所致。

- 4 由於網路路由問題，ESXi 主機無法連線到 vRealize Network Insight 收集器。請確保 ESXi 主機和 vRealize Network Insight 收集器之間存在正確路由。

## 應瞭解哪些與 IPFIX 相關的 VMware 知識庫文章？

VMware ESXi 6.0 Update 1 : [2135956](#)。

## 何時將服務視為共用？

通訊協定	連接埠
DNS	53
Bootpc	68
Kerberos	88
Pop3	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269