

安裝 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

關於 vRealize Network Insight 安裝指南 5

1 準備安裝 6

- 系統建議和需求 6
 - 權限 9
 - 系統連接埠 10
 - 網路通訊連接埠 14
- 支援的產品和版本 15

2 安裝 vRealize Network Insight 19

- 安裝工作流程 19
- 部署 vRealize Network Insight 平台 OVA 21
 - 使用 vSphere Web Client 進行部署 21
 - 使用 vSphere Windows 原生用戶端進行部署 23
- 啟用授權 24
- 產生共用密碼 24
- 設定 Network Insight 收集器 (OVA) 25
 - 使用 vSphere Web Client 進行部署 25
 - 使用 vSphere Windows 原生用戶端進行部署 26
- 在 AWS 中針對 VMware SD-WAN 設定 Network Insight 收集器 (AMI) 27
- 將其他收集器部署至現有設定 29

3 使用評估授權來存取 vRealize Network Insight 30

- 新增 vCenter Server 30
- 分析流量 31
- 產生報告 32

4 部署垂直擴充規劃 33

- 平台叢集垂直擴充規劃 33
- 收集器垂直擴充規劃 34
- 增加設定的區塊大小 35

5 升級 vRealize Network Insight 36

- 線上升級 37
- 單鍵離線升級 39
- CLI 升級 41

6 解除安裝 vRealize Network Insight 44

在 vCenter 中啟用 Netflow 時移除收集器 IP 44

在 NSX 中啟用 Netflow 時移除收集器 IP 45

關於 vRealize Network Insight 安裝指南

《vRealize Network Insight 安裝指南》適用於負責安裝 vRealize Network Insight 的管理員或專家。

適合對象

此資訊適用於負責安裝 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。

準備安裝

1

安裝 vRealize Network Insight 前，請準備部署環境以符合系統需求。

本章節討論下列主題：

- 系統建議和需求
- 支援的產品和版本

系統建議和需求

為獲得最佳效能，必須符合最低部署建議。

平台部署建議

表 1-1. 平台區塊大小的規格

區塊大小	2.6 GHz CPU 所需的核心數	2.6 GHz CPU 所需的核心數	2.6 GHz CPU 所需的核心數	RAM	磁碟
中型	10	9	8	32 GB	1 TB
大型	15	14	12	48 GB	1 TB
超大型	20	18	16	64 GB	2 TB

備註

- 針對每個節點的 CPU 速度和 RAM 保留必須為上述指定值的 100%。
- 若要使設定符合所有規格，您可能需要新增資源 (RAM、磁碟、CPU)。請參閱 <https://kb.vmware.com/s/article/53550> 和 [增加設定的區塊大小](#)。

表 1-2. 非叢集部署 - 容量上限

區塊大小	虛擬機器數目 (以千為單位)	每日流量數 (以百萬為單位)	流量總計 (以百萬為單位)	流量規劃 (以百萬為單位)
中型	4K	1M	4M	2M
大型	6K	2M	8M	4M

表 1-3. 非叢集部署 - VMware SD-WAN 的容量上限

區塊大小	Edge 數目 (以千為單位)	每日流量數 (以百萬為單位)	流量總計 (以百萬為單位)
中型	2K	1M	4M
大型	2K	2M	8M

備註

- 虛擬機器計數中也包含 vCenter 上的範本。
- 流量總計是指系統可為保留期間儲存的最大流量計數。
- 流量規劃是指系統可對其執行安全性計劃的流量總計。

表 1-4. 叢集部署 - 容量上限

區塊大小	叢集大小	虛擬機器數目 (以千為單位)	每日流量數 (以百萬為單位)	流量總計 (以百萬為單位)	流量規劃 (以百萬為單位)	VMware SD-WAN 的 Edge 數目 (以千為單位)
大型	3	10K	2M	8M	4M	4K
超大型	3	18K	6M	24M	4M	6K
超大型	5	30K	10M	40M	4M	10K
超大型	10	100K	15M	55M	4M	10K

備註

- 虛擬機器計數中也包含 vCenter 上的範本。
- 叢集大小是指叢集中的節點總數。
- 流量總計是指系統中針對保留期間的流量計數。
- 用於判定流量總計的查詢為 `count of flows in last 31 days`，假設保留期間為 31 天。
- 流量規劃是指系統可對其執行安全性計劃的流量總計。

收集器部署建議

表 1-5. 收集器區塊大小的規格

區塊大小	2.1 GHz CPU 所需 的核心數	2.3 GHz CPU 所 需的核心數	2.6 GHz CPU 所 需的核心數	RAM	磁碟
中型	5	5	4	12 GB	200 GB
大型	10	9	8	16 GB	200 GB
超大型	10	9	8	24 GB	200 GB

備註 針對每個節點的 CPU 速度和 RAM 保留必須為上述指定值的 100%。

表 1-6. 收集器部署 - 容量上限

收集器大小	虛擬機器數目 (以千為單位)	每日流量數 (以百萬為單位)	4 天內的流量計數 (以百萬為單位)	VMware SD-WAN 的 Edge 數目 (以千為單位)
中型	4K	2.5M	3.25M	4K
大型	10K	5M	6.5M	6K
超大型	20K	10M	13M	10K

備註

- 虛擬機器計數中也包含 vCenter 上的範本。
- 對於具有多個收集器的單一部署，跨收集器的總流量限制視平台容量而定。

其他需求和考量事項

- 平台節點之間的最大時間誤差必須小於 30 秒。
- NTP 服務的可用性對系統作業至關重要。請確保在 NTP 服務不可用時，不要將平台節點或收集器節點重新開機。
- 當現有計算資源被平台上的其他程序用盡時，vRealize Network Insight 會當機並且不會自動復原。如果服務無法復原，則將平台節點重新開機。
- 如果平台節點與升級伺服器之間的網路延遲超過 500 毫秒，則 vRealize Network Insight 升級可能會發生錯誤。因此，網路延遲必須小於 500 毫秒。
- 為獲得最佳效能，建議磁碟延遲最多為 5 毫秒。如果磁碟延遲超過 5 毫秒，則系統效能會降低。
- 建議的磁碟 IOPS 為 7500。

支援的網頁瀏覽器

- Google Chrome：最新的兩個版本。
- Mozilla Firefox：最新的兩個版本。

支援高可用性的建議

您可以自訂 vSphere HA 選項以啟用 vSphere High Availability。

- 主機故障 - 重新啟動虛擬機器
- 主機隔離 - 已停用
- 客體未產生活動訊號 - 已停用

權限

資料來源所需的權限

- 設定和使用 IPFIX 所需的權限
 - 具有權限的 vCenter Server 認證：
 - Distributed Switch：修改
 - dvPort 群組：修改
 - 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

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。

- NSX Manager 資料提供者所需的權限
 - NSX Manager 資料提供者需要企業角色。
 - 如果已啟用 Central CLI，則 NSX Manager 資料提供者需要具有 `system admin` 認證。
- 在 Cisco 交換器上收集度量所需的使用者權限
 - vRealize Network Insight 能夠透過 SNMP 從 Cisco 交換器收集度量資料，以及透過 SSH 收集組態。Cisco 交換器 UCS 平台需要使用 SSH 和 API 進行收集。

表 1-7.

資料類型	使用者權限
組態資料	唯讀
度量資料	SNMP 唯讀

表 1-7. (續)

資料類型	使用者權限
	SNMPv2 唯讀 SNMP 社群
	SNMPv3 唯讀

系統連接埠

以下是 vRealize Network Insight 輸入通訊所需的連接埠清單：

平台叢集設定的連接埠

表 1-8.

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
SSH 用戶端	平台	22	SSH	CLI 或主機存取	否	是	使用者/密碼或以 SSH 金鑰為基礎的驗證
用戶端網頁瀏覽器 和 vRNI 收集器	平台	443	HTTPS	使用者介面/API 存取 以及與 vRNI 收集器的通訊	是	是	使用以 2048b RSA 金鑰為基礎的 SHA2 憑證 (或使用者設定的自訂憑證) 加密的 SSL 通道。對於此通道上收集器至平台的訊息，還需要使用 HMAC 進一步加密。
平台	平台	2181	HTTP	其他節點上的 zookeeper 伺服器之間的通訊 (若為叢集)。儲存中繼資料資訊 (znode 資料)	否	否	
平台	平台	2888	HTTP	用於連線到 zookeeper 主節點	否	否	
平台	平台	3000	HTTP	用於電子郵件通知	是	否	
平台	平台	3888	HTTP	用於 zookeeper 主節點選擇	是	否	

表 1-8. (續)

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
平台	平台	5432	jdbc	儲存虛擬機器組態資料和基礎結構中繼資料	是	否	
平台	平台	8020	TCP/RPC	在其他名稱節點和資料節點之間進行通訊	是	否	
平台	平台	8025	HTTP	節點管理程式使用此連接埠連線至資源管理程式	否	否	
平台	平台	8030	HTTP	由資源管理程式用來排程工作	否	否	
平台	平台	8032	HTTP	RM 中應用程式管理程式介面的位址	否	否	
平台	平台	8033	HTTP	RM 管理介面的位址	否	否	
平台	平台	8042	HTTP	節點管理程式 Web 應用程式位址	否	否	
平台	平台	8080	HTTP	處理使用者介面要求	是	否	
平台	平台	8088	HTTP	資源管理程式 Web 應用程式的 HTTP 位址	否	否	
平台	平台	8480	TCP/RPC	JournalNode HTTP 伺服器	否	否	
平台	平台	8485	TCP/RPC	HDFS 共用編輯資料目錄	否	否	
平台	平台	9090	HTTP	處理收集器的要求，並將命令傳送到收集器	是	是 (透過 nginx 保護)	
平台	平台	9092	Binary over TCP	其他代理進行通訊所在的連接埠	是	否	

表 1-8. (續)

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
平台	平台	9200-9300	HTTP	處理搜尋要求。ES 使用連接埠範圍進行接聽，如果 9200 已使用，則使用下一個可用的連接埠。	是	否	
平台	平台	9300	HTTP	處理搜尋要求。ES 使用連接埠範圍進行接聽，如果 9200 已使用，則使用下一個可用的連接埠。	是	否	
平台	平台	30000:65535	TCP	由各種程序用來與其他程序進行 TCP 連線的暫時連接埠範圍	否	否	
平台	平台	60000	IPC	用於其他 hbase 主要節點與區域伺服器之間的通訊	是	否	
平台	平台	60010	HTTP	用於 hbase Web 使用者介面	否	否	
平台	平台	60020	IPC	hbase 主要節點與區域伺服器之間的通訊	是	否	
平台	平台	4500-4510	TCP	在不同平台上執行的 Foundation 資料庫伺服器之間的通訊	是	否	

用於單一平台設定的連接埠

表 1-9.

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
SSH 用戶端	平台	22	SSH	CLI 或主機存取	否	是	使用者/密碼或以 SSH 金鑰為基礎的驗證
用戶端網頁瀏覽器 和 vRNI 收集器	平台	443	HTTPS	使用者介面/API 存取 以及與 vRNI 收集器的通訊	是	是	使用以 2048b RSA 金鑰為基礎的 SHA2 憑證 (或使用者設定的自訂憑證) 加密的 SSL 通道。對於此通道上收集器至平台的訊息，還需要使用 HMAC 進一步加密。

用於收集器伺服器的連接埠

表 1-10.

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
SSH 用戶端	收集器	22	SSH	CLI 或主機存取	否	是	使用者/密碼或以 SSH 金鑰為基礎的驗證
vRNI 收集器	平台	443	HTTPS	與平台的主要通訊通道	是	是	使用以 2048b RSA 金鑰為基礎的 SHA2 憑證 (或使用者設定的自訂憑證) 加密的 SSL 通道。對於此通道上收集器至平台的訊息，還需要使用 HMAC 進一步加密。
流量轉寄站	收集器	UDP 2055	NetFlow/ IPFIX	來自目標的流量將推送到此連接埠	是	否	

表 1-10. (續)

來源	目標	連接埠	通訊協定	用途	敏感	SSL	驗證
流量轉寄站	收集器	UDP 6343	sFlow	來自目標的流量將推送到此連接埠	是	否	
ESXi 主機	收集器	1991	TCP	收集虛擬基礎結構的延遲測量，例如： vNIC 至 pNIC、 VTEP 至 VTEP、TEP 至 TEP 等之間的延遲。	否	否	
Dell OS10	收集器	50000	GRPC	從 Dell OS10 裝置接收緩衝區統計資料遙測資訊	否	否	

網路通訊連接埠

下表列出了 vRealize Network Insight 中用於網路通訊的連接埠和通訊協定。

還可以透過 <https://ports.vmware.com/home/vRealize-Network-Insight> 查看連接埠清單。

表 1-11.

用途	從	至	連接埠	通訊協定
vRealize Network Insight 的虛擬機器之間的通訊	收集器	平台 備註 必須為所有平台啟用連接埠。	443	HTTPS
需要存取網際網路的服務	平台和收集器	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS
設定的其他服務的通訊	平台	LDAP 伺服器	389、636	LDAP 和 LDAPS
		SNMP 伺服器	可設定	SNMP
	平台和收集器	DNS 伺服器	53	UDP
		Syslog 伺服器	可設定	
	ESXi 主機	收集器	2055	
	ESXi 主機	收集器	1991	TCP
與做為資料來源的 AWS 進行通訊	收集器	AWS (* .amazonaws.com)	443	HTTPS

表 1-11. (續)

用途	從	至	連接埠	通訊協定
與遙測服務通訊	瀏覽器	遙測 URL https://vcsa.vmware.com	433	HTTPS
與資料中心內的其他資料來源進行通訊	收集器	Arista 交換器	161 和 22	SNMP 和 SSH
		Azure	443	HTTPS
		Brocade 交換器	161 和 22	SNMP 和 SSH
		Check Point 防火牆	443	HTTPS
		Cisco Nexus	161 和 22	SNMP 和 SSH
		Cisco UCS (統一運算系統)	161、22 和 443	SNMP、SSH 和 HTTPS
		Cisco Catalyst 交換器	161 和 22	SNMP 和 SSH
		Cisco ACI 交換器	161	SNMP
		Cisco APIC 控制器	161 和 443	HTTPS 和 SNMP
		Dell 交換器	161 和 22	SNMP 和 SSH
		Dell OS10	50000	TCP
		VeloCloud	443、2055	HTTPS
		HP	22	SSH
		Juniper 交換器	161 和 22	SNMP 和 SSH
		Palo Alto 網路	443	HTTPS
		VMware vSphere	443	HTTPS
		VMware NSX - V (所有元件)	22 和 443	SSH 和 HTTPS
		NSX-T Manager	443	TCP
		VMware PKS API 伺服器	8443 和 9021	TCP
		Kubernetes API 伺服器	8443	TCP
		vRealize Log Insight	443	HTTPS
		Fortinet FortiManager	443	HTTPS

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 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
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

資料來源	版本/型號	連線通訊協定	權限/特殊權限
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 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權限： <ul style="list-style-type: none"> ■ 雲端管理員：新增資料來源並啟用 IPFIX。
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。

資料來源	版本/型號	連線通訊協定	權限/特殊權限
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。

安裝 vRealize Network Insight

2

您可以使用 vSphere Web Client 或 vSphere Windows 原生用戶端部署 vRealize Network Insight。

備註 成功部署 vRealize Network Insight 平台 OVA 之後，確認是否已在 vCenter Server 上設定指定的靜態 IP。

您可以使用 vRealize Suite Lifecycle Manager，將單一虛擬管理介面內的安裝、組態、升級、修補、組態管理、漂移修復及健全狀況自動化。如果您是新的使用者，請按一下這裡以安裝 [vRealize Suite Lifecycle Manager](#)。這麼做可以提供 IT Managers of Cloud 管理資源，讓您專注於業務關鍵解決方案，同時提升實現價值時間 (TTV)、可靠性和一致性。

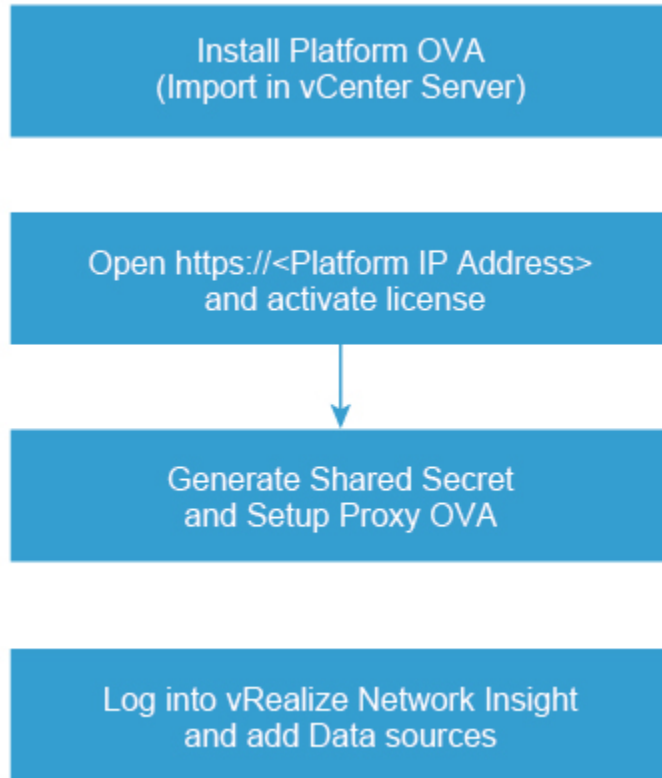
您也可以使用 vRealize Suite Lifecycle Manager 來安裝和升級 vRealize Network Insight。如需詳細資訊，請參閱《[vRealize Suite Lifecycle Manager 安裝、升級和管理指南](#)》。

本章節討論下列主題：

- [安裝工作流程](#)
- [部署 vRealize Network Insight 平台 OVA](#)
- [啟用授權](#)
- [產生共用密碼](#)
- [設定 Network Insight 收集器 \(OVA\)](#)
- [在 AWS 中針對 VMware SD-WAN 設定 Network Insight 收集器 \(AMI\)](#)
- [將其他收集器部署至現有設定](#)

安裝工作流程

若要安裝 vRealize Network Insight，您可以安裝平台 OVA，啟用授權，產生共用密碼，並設定收集器 OVA。



vRealize Network Insight 的簡化部署圖如下所示：



部署 vRealize Network Insight 平台 OVA

您可以將 vRealize Network Insight 平台 OVA 匯入至 vCenter Server。

備註 不支援在 VMC SDDC 上部署 vRealize Network Insight 平台 OVA。

使用 vSphere Web Client 進行部署

您可以使用 vSphere Web Client 部署 vRealize Network Insight。

程序

- 1 在您要安裝應用裝置的**資料中心**上按一下滑鼠右鍵，然後選取**部署 OVF 範本**。
- 2 輸入 URL 以下載 OVA 套件並安裝，或瀏覽以選取 OVA 套件的來源位置。
- 3 輸入 OVA 名稱。選取目的地資料夾用於部署。

- 4 選取要執行已部署範本的主機、叢集或資源集區。
- 5 驗證 OVF 範本詳細資料。
- 6 閱讀終端使用者授權合約並按一下**接受**。
- 7 選取部署組態。按一下**下一步**。
- 8 選取已部署範本之檔案的儲存位置。選取**精簡佈建**做為虛擬磁碟格式。選取用於儲存檔案的資料存放區或資料存放區叢集。按一下**下一步**。
- 9 選取已部署範本將使用的網路。
選取的網路應允許應用裝置連線至網際網路以取得支援和升級。
- 10 若要自訂用於部署的範本，您必須使用虛擬機器主控台手動設定應用裝置。按一下**下一步**。
- 11 驗證組態詳細資料並按一下**完成**。
- 12 增加設定的**區塊大小**，以符合系統建議和需求。
- 13 安裝平台後，啟動虛擬機器並啟動主控台。
- 14 使用您在畫面上看到的主控台認證登入，然後執行 `setup` 命令。
- 15 為 `support` 登入建立密碼，並為 `consoleuser` 變更密碼。

備註

- 密碼必須至少包含 6 個字元。不允許使用單引號 (')。
 - 您必須定期變更 `support` 和 `consoleuser` 密碼以符合組織原則。
-

- 16 輸入下列詳細資料以設定網路：
 - a IPv4 位址：第二個保留的靜態 IP 位址
 - b 網路遮罩：上一個靜態 IP 的子網路遮罩
 - c 預設閘道：網路的預設閘道
 - d DNS：環境的 DNS 伺服器

備註 對於多個 DNS 伺服器，請確保以空格將其分隔。

- e 網域搜尋清單：需要為 DNS 查閱附加的網域
 - f 輸入 `y` 以儲存組態。
- 17 輸入 NTP 伺服器，並確保可以從虛擬機器進行存取。如果 NTP 時間不同步，則服務無法啟動。

備註 對於多個 NTP 伺服器，請確保以逗號將其分隔。

- 18 (選擇性) 若要設定 Web Proxy，請輸入 `y`。
- 19 驗證所有服務。
- 20 根據您的設定需求新增額外的磁碟空間。請參閱 <https://kb.vmware.com/s/article/53550>。

使用 vSphere Windows 原生用戶端進行部署

您可以使用 vSphere Windows 原生用戶端部署 vRealize Network Insight。

備註 vRealize Network Insight 5.2 是支援使用 vSphere Windows 原生用戶端部署 OVA 的最後一個版本。從 5.3 版開始，您可以繼續使用 vSphere Web Client 部署 vRealize Network Insight OVA。

程序

- 1 按一下**檔案 > 部署 OVF 範本**。
- 2 輸入 URL 以便從網際網路下載 OVA 套件並安裝，或瀏覽以選取電腦上 OVA 套件的來源位置。
- 3 按**下一步**並驗證 OVF 範本詳細資料。
- 4 閱讀使用者授權合約並按一下**接受**。
- 5 為已部署的範本提供名稱和指定位置。按**下一步**。
- 6 選取**部署組態**。
- 7 選取要執行已部署範本的**主機/叢集**。
- 8 選取您要在其中部署此範本的**資源集區**。
- 9 選取虛擬機器檔案的目的地儲存區。按**下一步**。
- 10 指定儲存虛擬磁碟要採用的格式。選取**精簡佈建**做為虛擬磁碟格式。按**下一步**。
- 11 指定已部署範本應使用的網路。將網路從 OVA 對應到詳細目錄。
- 12 為部署自訂範本。提供在上線頁面上所產生的共用密碼。您必須使用虛擬機器主控台手動設定應用裝置。按**下一步**。
- 13 驗證所有組態資料。勾選**部署後開啟電源**。按一下**完成**。
- 14 **增加設定的區塊大小**以滿足**系統建議和需求**。
- 15 安裝收集器 OVA 後，啟動虛擬機器並啟動主控台。
- 16 使用您在畫面上看到的主控台認證登入，然後執行 `setup` 命令。
- 17 為 `support` 登入建立密碼，並為 `consoleuser` 變更密碼。

備註

- 密碼必須至少包含 6 個字元。不允許使用單引號 (')。
- 您必須定期變更 `support` 和 `consoleuser` 密碼以符合組織原則。

- 18 輸入下列詳細資料以設定網路：
 - a **IPv4 位址**：第二個保留的靜態 IP 位址
 - b **網路遮罩**：上一個靜態 IP 的子網路遮罩
 - c **預設閘道**：網路的預設閘道

d **DNS**：環境的 DNS 伺服器

備註 對於多個 DNS 伺服器，請確保以空格將其分隔。

e **網域搜尋清單**：需要為 `dns lookup` 附加的網域。

f 輸入 `y` 以儲存組態。

19 輸入 NTP 伺服器，並確保可以從虛擬機器進行存取。如果 NTP 時間不同步，則服務無法啟動。

備註 對於多個 NTP 伺服器，請確保以逗號將其分隔。

20 (選擇性) 若要設定 Web Proxy，請輸入 `y`。

21 驗證所有服務。

22 根據您的設定需求新增額外的磁碟空間。請參閱 <https://kb.vmware.com/s/article/53550>。

啟用授權

安裝 vRealize Network Insight 平台 OVA 後，在 Chrome 網頁瀏覽器中開啟 <https://<vRealize Network Insight 平台 IP 位址>>。

程序

- 1 輸入在歡迎電子郵件中收到的授權金鑰。
- 2 對於使用者介面管理員 (`admin@local`) 的使用者名稱，設定密碼。

備註 您的密碼必須為英數字元，且至少包含 8 個字元，最多包含 100 個字元。字元之間不允許使用空格。

- 3 按一下**啟動**。
- 4 啟用授權後新增 vRealize Network Insight 收集器。

產生共用密碼

您可以產生並匯入 vRealize Network Insight 收集器虛擬應用裝置。

產生共用密碼，並匯入 vRealize Network Insight 收集器虛擬應用裝置：

程序

- 1 登入 vRealize Network Insight 使用者介面。
- 2 展開**基礎結構和支援**，然後按一下**概觀和更新**。
- 3 向下捲動，然後按一下**新增 Proxy 虛擬機器**。

隨即顯示**新增 Network Insight 資料收集器虛擬應用裝置**。

- 4 按一下**複製**，從對話方塊複製共用密碼，然後按一下**完成**。

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

設定 Network Insight 收集器 (OVA)

您可以透過將 OVA 匯入至 vCenter Server，以設定 vRealize Network Insight 收集器。

請遵循下列步驟將 vRealize Network Insight 收集器 OVA 匯入至 vCenter Server。

使用 vSphere Web Client 進行部署

您可以使用 vSphere Web Client 匯入 vRealize Network Insight 收集器 OVA。

程序

- 1 在您要安裝應用裝置的**資料中心**上按一下滑鼠右鍵，然後選取**部署 OVF 範本**。
- 2 輸入 URL 以便從網際網路下載 OVA 套件並安裝，或瀏覽以從電腦中選取 OVA 的來源位置。
- 3 為已部署的範本提供名稱和指定位置。按**下一步**。
- 4 選取要執行已部署範本的資源 (主機或叢集)。按**下一步**。
- 5 驗證範本的所有詳細資料。按**下一步**。
- 6 閱讀使用者授權合約並按一下**接受**。按**下一步**。
- 7 選取部署組態。按**下一步**。
- 8 選取要儲存已部署範本之檔案的位置。指定儲存虛擬磁碟要採用的格式。選取**精簡佈建**做為虛擬磁碟格式。選取要在其中安裝檔案的資料存放區。按**下一步**。
- 9 為來源網路指定目的地網路。按**下一步**。
- 10 為部署自訂範本。提供從 UI 產生的共用密碼。您必須使用虛擬機器主控台手動設定應用裝置。按**下一步**。
- 11 驗證所有組態資料。按一下**完成**。
- 12 安裝收集器 OVA 後，啟動虛擬機器並啟動主控台。
- 13 使用您在畫面上看到的主控台認證登入，然後執行 `setup` 命令。
- 14 為 `support` 登入建立密碼，並為 `consoleuser` 變更密碼。

備註

- 密碼必須至少包含 6 個字元。不允許使用單引號 (')。
 - 您必須定期變更 `support` 和 `consoleuser` 密碼以符合組織原則。
-

- 15 輸入下列詳細資料以設定網路：

- a **IPv4 位址**：第二個保留的靜態 IP 位址
- b **網路遮罩**：上一個靜態 IP 的子網路遮罩

- c **預設閘道**：網路的預設閘道
- d **DNS**：環境的 DNS 伺服器

備註 對於多個 DNS 伺服器，請確保以空格將其分隔。

- e **網域搜尋清單**：需要為 DNS 查閱附加的網域
- f 輸入 `y` 以儲存組態。

- 16 輸入 NTP 伺服器，並確保可以從虛擬機器進行存取。如果 NTP 時間不同步，則服務無法啟動。

備註 對於多個 NTP 伺服器，請確保以逗號將其分隔。

- 17 (選擇性) 設定 Web Proxy：

- a 輸入 `y`。
- b 提供 Web Proxy 詳細資料。

- 18 進行檢查以查看是否已設定共用密碼。收集器與對應的平台進行配對。此作業可能需要幾分鐘時間。

- 19 驗證所有服務。

- 20 上線頁面上顯示偵測到 Proxy! 訊息後，按一下**完成**。將重新導向至登入頁面。

使用 vSphere Windows 原生用戶端進行部署

您可以使用 vSphere Windows 原生用戶端匯入 vRealize Network Insight 收集器 OVA。

備註 vRealize Network Insight 5.2 是支援使用 vSphere Windows 原生用戶端部署 OVA 的最後一個版本。從 5.3 版開始，您可以繼續使用 vSphere Web Client 部署 vRealize Network Insight OVA。

程序

- 1 按一下**檔案 > 部署 OVF 範本**。
- 2 輸入 URL 以便從網際網路下載 OVA 套件並安裝，或瀏覽以選取電腦上 OVA 套件的來源位置。
- 3 驗證 OVF 範本詳細資料。按一下**下一步**。
- 4 閱讀使用者授權合約並按一下**接受**。按一下**下一步**。
- 5 為已部署的範本提供名稱和指定位置。按一下**下一步**。
- 6 選取**部署組態**。按一下**下一步**。
- 7 選取要執行已部署範本的**主機/叢集**。按一下**下一步**。
- 8 選取您要在其中部署此範本的**資源集區**。按一下**下一步**。
- 9 選取虛擬機器檔案的目的地儲存區。按一下**下一步**。
- 10 指定儲存虛擬磁碟要採用的格式。選取**精簡佈建**做為虛擬磁碟格式。按一下**下一步**。
- 11 指定已部署範本應使用的網路。將網路從 OVA 對應到詳細目錄。

- 12 為部署自訂範本。提供在上線頁面上所產生的共用密碼。您必須使用虛擬機器主控台手動設定應用裝置。按下一步。
 - 13 驗證所有組態資料。勾選**部署後開啟電源**。按一下**完成**。
 - 14 安裝收集器 OVA 後，啟動虛擬機器並啟動主控台。
 - 15 使用指定的主控台認證登入。執行 `setup` 命令。
 - 16 為 `support` 登入建立密碼。為 `consoleuser` 變更密碼。
 - 17 輸入下列詳細資料以設定網路：
 - a **IPv4 位址**：第二個保留的靜態 IP 位址
 - b **網路遮罩**：上一個靜態 IP 的子網路遮罩
 - c **預設閘道**：網路的預設閘道
 - d **DNS**：環境的 DNS 伺服器

備註 對於多個 DNS 伺服器，請確保以空格將其分隔。

 - e **網域搜尋清單**：需要為 `dns lookup` 附加的網域。
 - f 輸入 `y` 以儲存組態。
 - 18 輸入 NTP 伺服器，並確保可以從虛擬機器進行存取。如果 NTP 時間不同步，則服務無法啟動。
-
- 備註** 對於多個 NTP 伺服器，請確保以逗號將其分隔。
-
- 19 (選擇性) 設定 Web Proxy：
 - a 輸入 `y`。
 - b 提供 Web Proxy 詳細資料。
 - 20 進行檢查以查看是否已設定共用密碼。收集器與對應的平台進行配對。此作業可能需要幾分鐘時間。
 - 21 驗證所有服務。
 - 22 上線頁面上顯示偵測到 Proxy! 訊息後，按一下**完成**。將重新導向至登入頁面。

在 AWS 中針對 VMware SD-WAN 設定 Network Insight 收集器 (AMI)

您可以透過將 Amazon Machine Image (AMI) 匯入至 AWS 環境來為 AWS 設定 vRealize Network Insight 收集器。

如果環境中沒有 vCenter Server，而您想要在雲端環境中部署收集器，可在 AWS 中部署收集器。

備註 目前，vRealize Network Insight 僅支援針對 VMware SD-WAN 使用 AMI 在 AWS 中部署收集器。

與 EC2 執行個體相關的程序和工作記錄在 <https://docs.aws.amazon.com/efs/index.html> 中。

程序

- 1 在 Amazon EC2 主控台中使用 VMware 提供的 AMI 來啟動 EC2 執行個體。如需程序詳細資料，請參閱 Amazon Elastic File System 說明文件中的〈建立 EC2 資源並啟動 EC2 執行個體〉主題。

備註 當您在 AWS 中啟動 EC2 執行個體時，必須選取下列選項：

選項	動作
執行個體類型	m4.xlarge (中等區塊)
網路	選取適當的網路和子網路。
儲存區	預設儲存區。
標籤	根據客戶原則。
安全群組	對於連接埠 443，允許 0.0.0.0/0 的輸出流量 (或者對於限制的規則，針對連接埠 443 允許 NI SaaS Prod FQDN 的輸出流量)。
金鑰	選取適當的金鑰 (已針對 AMI 啟用 SSH 登入)。

- 2 當您的 EC2 執行個體處於執行中狀態時，請登入您的 EC2 執行個體。
- 3 使用指定的主控台認證登入。執行 `setup` 命令。
- 4 為 `support` 登入建立密碼。為 `consoleuser` 變更密碼。

備註 變更密碼後，系統會在設定 CLI 期間略過網路選項。

Proxy AMI 不支援下列項目：

- IP 變更
- IPv6
- Web Proxy 組態。

- 5 輸入 NTP 伺服器，並確保可以從虛擬機器進行存取。如果 NTP 時間不同步，則服務無法啟動。

備註 對於多個 NTP 伺服器，請確保以逗號將其分隔。

- 6 進行檢查以查看是否已設定共用密碼。收集器與對應的平台進行配對。此程序可能需要花費幾分鐘時間。
- 7 驗證所有服務。

後續步驟

啟用從 Edge 到您在 AWS 中部署的收集器的流量收集。若要啟用流量收集，請執行下列操作：

- 將您在 AWS 中部署的收集器設為非 VeloCloud 站台。如需詳細資料，請聯絡 VMware 支援。

將其他收集器部署至現有設定

您可以將其他 vRealize Network Insight 收集器新增至現有設定。

程序

- 1 登入 vRealize Network Insight 使用者介面。
- 2 展開**基礎結構和支援**，然後按一下**概觀和更新**。
- 3 向下捲動，然後按一下**新增 Proxy 虛擬機器**。
隨即顯示**新增 Network Insight 資料收集器虛擬應用裝置**。
- 4 按一下**複製**，從對話方塊複製共用密碼，然後按一下**完成**。
- 5 請遵循步驟 3 中**設定 Network Insight 收集器 (OVA)**一節中的步驟。

使用評估授權來存取 vRealize Network Insight

3

當您使用評估授權時，vRealize Network Insight 會在 NSX 評估模式下啟動。

您可以將資料來源新增至 vRealize Network Insight，請分析流量，並產生報告。

備註 若要切換到完整產品模式，請按一下位於右下角的切換到完整產品評估。

本章節討論下列主題：

- [新增 vCenter Server](#)
- [分析流量](#)
- [產生報告](#)

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
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。

分析流量

您可以使用 vRealize Network Insight 分析資料中心的流量。

必要條件

在開始流量分析之前，必須至少進行兩個小時的資料收集。

程序

- 1 指定分析的範圍。例如，如果您想要分析叢集中所有虛擬機器的流量，請從下拉式功能表中選取叢集。或者，您可以選取連線至 VLAN 或 VXLAN 的所有虛擬機器。

- 2 選取要為其分析流量的實體名稱。
- 3 選取持續時間，然後按一下**分析**。

產生報告

您可以產生流量評估的報告。

必要條件

分析資料中心內的流量。對於完整報告，請在分析之前收集 24 小時的資料。

程序

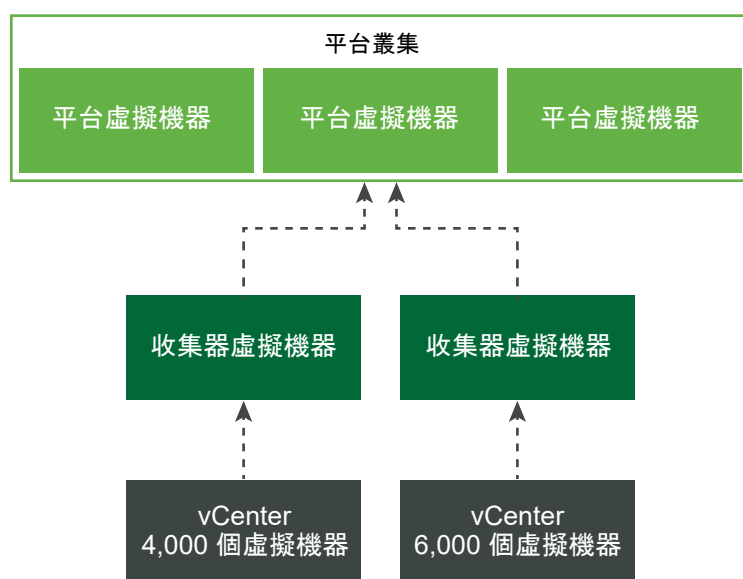
- 1 在 **EVAL NSX 評估模式** 中，按一下 [分析流量] 頁面中的**產生報告**。
- 2 在非 **EVAL 模式** 中，在**微分割**頁面上按一下**流量分佈 > 更多選項 > 評估報告**。

部署垂直擴充規劃

4

如果設定中的虛擬機器計數或作用中流量數目較高或預計會增長，則可以增加平台或收集器的大小。

您可以使用下列架構，更好地瞭解平台和收集器分佈：



本章節討論下列主題：

- [平台叢集垂直擴充規劃](#)
- [收集器垂直擴充規劃](#)
- [增加設定的區塊大小](#)

平台叢集垂直擴充規劃

您可以垂直擴充平台叢集，以符合增加的負載。根據負載，您可以透過增加區塊大小、建立或擴充平台叢集進行垂直擴充。三個 `LARGE` 平台區塊可以連線在一起，以形成平台叢集。如果平台的區塊大小為 `LARGE` 或 `EXTRA LARGE`，則必須透過建立平台叢集進行垂直擴充。

若要決定平台區塊大小和平台區塊數目，請參閱[系統建議和需求](#)。

備註 平台叢集不支援高可用性組態。為了讓叢集以最佳效能水平運作，所有平台節點都必須啟動並執行。

平台叢集垂直擴充案例

- 案例 1：平台執行 5000 個虛擬機器和 150 萬個作用中流量
將平台從 MEDIUM 轉換為 LARGE。請參閱[增加設定的區塊大小](#)。
- 案例 2：平台執行單一 LARGE 節點，該節點具有 9000 個虛擬機器和 200 萬個作用中流量
再新增兩個 LARGE 區塊節點以轉換為 3 節點的 LARGE 區塊叢集。請參閱《vRealize Network Insight 使用者指南》中的〈擴充叢集〉。
- 案例 3：平台執行 3 節點的 LARGE 叢集，該叢集具有一或多個收集器、15000 個虛擬機器和 400 萬個作用中流量。
將現有的平台節點從 LARGE 轉換為 EXTRA-LARGE。請參閱[增加設定的區塊大小](#)。
- 案例 4：平台執行 3 節點的 EXTRA-LARGE 叢集，該叢集具有一或多個收集器、25000 個虛擬機器和 800 萬個作用中流量。
再新增兩個 EXTRA-LARGE 區塊節點以轉換為 5 節點的 Extra-LARGE 叢集。請參閱《vRealize Network Insight 使用者指南》中的〈擴充叢集〉。

收集器垂直擴充規劃

收集器容量是以區塊大小為基礎。您可以新增至收集器的資料來源取決於收集器 (虛擬機器和流量) 的容量。

請參閱表 1-6. [收集器部署 - 容量上限](#)。收集器的區塊大小為 LARGE 後，您必須新增多個收集器。您可以將每個收集器垂直擴充至 EXTRA-LARGE 大小。

您可以根據支援的收集器容量將多個資料來源新增至收集器。但是，無法將同一個資料來源新增至多個收集器。

收集器垂直擴充案例

- 案例 1：vCenter 中有 2000 個虛擬機器。
安裝一個中型收集器虛擬機器。將 vCenter 新增到此收集器。請參閱[新增 vCenter Server](#)。
- 案例 2：vCenter1 中有 1000 個虛擬機器，vCenter2 中有 2000 個虛擬機器 (它們都在一個資料中心內)
安裝一個中型收集器虛擬機器。將兩個 vCenter 新增到此收集器。請參閱[新增 vCenter Server](#)。
- 案例 3：vCenter1 中有 1000 個虛擬機器 (資料中心 1)，vCenter2 中有 2000 個虛擬機器 (資料中心 2)。
在每個資料中心內安裝一個中型收集器虛擬機器。將 vCenter1 新增至同一個資料中心內的收集器虛擬機器，並將 vCenter2 新增至其資料中心內的收集器虛擬機器。請參閱[新增 vCenter Server](#)。
- 案例 4：虛擬機器計數超過 4000，作用中流量超出 250 萬。
將收集器虛擬機器從 MEDIUM 轉換為 LARGE。請參閱[增加設定的區塊大小](#)。

- 案例 5：vCenter1 中有 9,000 個不含流量的虛擬機器 (資料中心 1)。

安裝一個大型收集器虛擬機器。將此 vCenter 新增至收集器。請參閱[新增 vCenter Server](#)。

- 案例 6：虛擬機器計數小於或等於 10000，但作用中流量超過 500 萬。

將收集器虛擬機器從 `LARGE` 轉換為 `EXTRA-LARGE`。請參閱[增加設定的區塊大小](#)。

- 案例 8：兩個 vCenter，vCenter1 有 10000 個虛擬機器和 900 萬個作用中流量，vCenter2 有 10000 個虛擬機器和 400 萬個作用中流量。

安裝一個 `EXTRA-LARGE` 和一個 `LARGE Proxy`。新增 vCenter1 至 `EXTRA-LARGE Proxy`，並將 vCenter2 新增至 `LARGE Proxy`。

- 案例 9：一個 vCenter，執行 10000 個虛擬機器和 900 萬個作用中流量。

安裝一個 `EXTRA-LARGE Proxy` 並將 vCenter 新增至 `Proxy`。

增加設定的區塊大小

若要符合您的需求，可以將平台或收集器應用裝置的區塊大小從 `MEDIUM` 變更為 `LARGE`，或從 `LARGE` 變更為 `EXTRA-LARGE`。

程序

- ◆ 執行與您的設定相關的步驟。

選項	敘述
對於單一節點平台或全新獨立 OVA	<ol style="list-style-type: none"> 登入 vCenter。 關閉平台虛擬機器。 將虛擬機器的磁碟、RAM、vCPU 總計和對應的保留區增加到與目標區塊大小相符。如需詳細資訊，請參閱 [系統建議和需求] 頁面。 重新啟動平台虛擬機器。
對於叢集平台	<ol style="list-style-type: none"> 登入 vCenter。 以反向時間順序關閉平台虛擬機器。例如：按從節點 3 到節點 1 的順序關閉。 增加磁碟、RAM、vCPU 總計和對應的保留區。如需詳細資訊，請參閱 [系統建議和需求]。 以時間順序重新啟動平台虛擬機器。例如：按從節點 1 到節點 3 的順序重新啟動。
對於收集器	<ol style="list-style-type: none"> 登入 vCenter。 關閉收集器虛擬機器。 將虛擬機器的磁碟、RAM、vCPU 總計和對應的保留區增加到與目標區塊大小相符。如需詳細資訊，請參閱 [系統建議和需求] 頁面。 重新啟動收集器虛擬機器。

升級 vRealize Network Insight

5

您可將目前的 vRealize Network Insight 環境升級至最新版本。

升級前的重要考慮事項：

- 升級後，vRealize Network Insight 大約需要 12 到 24 小時的時間來處理在升級作業期間位於管線中的資料，並反映在使用者介面上。
- vRealize Network Insight 不支援回復或產品降級。您必須建立備份後再繼續升級。如需有關備份和還原程序的詳細資訊，請參閱 <https://kb.vmware.com/s/article/55829> 知識庫文章。
- 在叢集環境中，您必須僅在平台 1 節點上執行升級作業。
- 升級至 vRealize Network Insight 5.1 後，某些防火牆規則識別碼可能會變更為 VMware Cloud on AWS 1.9 API 傳回的新識別碼。如果存在任何連結至流量的 VMware Cloud on AWS 1.8 防火牆規則：
 - 針對所有作用中流量升級後，會立即連結正確或相應的 VMware Cloud on AWS 1.9 防火牆規則。
 - 在將 1.8 升級至 1.9 版之前，針對閒置期間超過 24 小時的流量，防火牆規則將參考不存在的規則。

備註 如果在執行集中式升級時出現上傳失敗或使用使用者介面故障等問題，請連絡 VMware 支援。

移轉至 Foundation 資料庫

若要在叢集中的資料存放區之間散佈組態資料，vRealize Network Insight 5.1 會將 PostgreSQL 取代為 Foundation 資料庫，以儲存組態資料。這可讓 vRealize Network Insight：

- 減少平台 1 節點上的負載
- 避免單一故障點
- 改善復原能力
- 增強效能
- 在叢集節點之間統一共用磁碟

移轉程序會自動執行以下動作：

- 關閉所有服務

- 開始從 PostgreSQL 到 Foundation 資料庫的資料表到資料表移轉
- 在平台 1 使用者介面上顯示動態移轉進度資訊

將資料從 PostgreSQL 移到 Foundation 資料庫的移轉時間取決於磁碟速度和節點計數 (節點越多，提供的 Foundation 資料庫寫入輸送量就越大)

完成移轉程序所需的時間取決於資料庫的大小。

設定大小	資料大小	節點計數	一般移轉時間
小型	20 GB 至 40 GB	1 個節點	1 至 2 小時
中型	60 GB 至 100 GB	3 個節點	7 至 10 小時
一個大型雲端設定	500 GB	10 個節點的叢集	15 至 20 小時
XL (超大型)	1 TB	10 個節點的叢集	35 至 40 小時

請注意，將在 vRealize Network Insight 升級程序中進行移轉。因此，升級時間可能會較長，可在程序執行期間於畫面上查看。

vRealize Network Insight 提供不同的升級模式。

本章節討論下列主題：

- [線上升級](#)
- [單鍵離線升級](#)
- [CLI 升級](#)

線上升級

每當有新版本的 vRealize Network Insight 可用時，您都會收到通知。

必要條件

- 如果 /tmp 目錄中沒有足夠的空間，升級步驟可能會失敗。確認是否符合平台和收集器伺服器的以下磁碟空間需求：
 - /tmp - 6 GB
 - /home - 2 GB
- 確認是否符合平台伺服器的以下磁碟空間需求：
 - / - 6 GB (僅適用於平台 1 節點)
 - /var - 40 GB
- 確認您具有 500 KB/s 的最低頻寬需求，以從伺服器下載升級服務包。如果下載頻寬不足，安裝和支援頁面會擲回錯誤。
- 確保所有節點都處於線上狀態。如果任何節點均為非作用中狀態，則不允許觸發升級。
- 取得虛擬機器的快照。

■ 請注意，在移轉後要驗證下列值：

- 虛擬機器計數
- 快照計數大於 0 的虛擬機器
- 防火牆規則計數
- 安全群組計數
- NSX 防火牆計數

程序

1 當有更新可用時，您會看到**更新可用**訊息通知。

備註

- 如果更新通知不可用，請確認 vRealize Network Insight 平台和收集器虛擬機器可以透過執行 `show-connectivity-status` 命令來連線到連接埠 443 上的 `svc.ni.vmware.com` 和連接埠 443 上的 `reg.ni.vmware.com`。如果此連線需要 http proxy，請使用 `set-web-proxy` 命令在每個虛擬機器上進行設定。請確保輸出包含的升級連線狀態為 `Passed`。
- 提交支援票證，並提供產品使用者介面中的服務標籤。服務標籤會顯示在**設定 > 關於**下方。
- 登入應用裝置並執行 `show-connectivity-status` 命令。提供每個 vRealize Network Insight 平台和收集器虛擬機器的命令輸出的螢幕擷取畫面。

2 在更新可用訊息通知中，按一下**檢視詳細資料**以檢視更新的詳細資料。

[vRealize Network Insight 升級] 畫面隨即顯示。

3 閱讀**繼續操作之前**指示，並按一下**繼續**。

4 等待預先檢查完成，這會驗證：

- 磁碟空間，包括移轉所需的空間
- 版本
- NTP 同步狀態
- 頻寬

您可以在安裝程式上看到完成升級程序所需的大概時間 (包括移轉持續時間)。

5 按一下**立即安裝**。

6 升級程序開始後，[vRealize Network Insight 升級] 畫面會提供升級程序的狀態。

備註

- 如果某個節點變成非作用中狀態，則升級程序不會繼續。節點再次變為作用中狀態之後，升級才會繼續。
- 平台 1 成為升級伺服器。如果平台 1 處於離線狀態，則不會升級其他節點。
- 平台升級後，您可以繼續執行一般 vRealize Network Insight 作業，即使仍在執行收集器升級。如果升級程序未全部完成，[安裝與支援] 頁面中會顯示 Node Version Mismatch detected 訊息。

- 升級服務後，Nginx 會重新啟動以顯示移轉程序。因此，您可能在短時間（一至兩分鐘）內無法存取使用者介面。
- vRealize Network Insight 開始將資料移轉至 Foundation 資料庫。在 [資料移轉狀態] 畫面上，您會看到：
 - 整體狀態
 - 已耗用時間
 - 按資料表狀態列出的資料表
 - 已移轉的記錄數

如有任何問題，您可以使用匯出移轉記錄選項與 VMware 支援團隊分享。

- 在升級程序過程中，收集器上的 PostgreSQL 資料也會移轉至 Foundation 資料庫。但是，收集器的移轉狀態不會顯示在使用者介面上。

7 完成升級程序後，您會看到確認訊息。

所有平台和收集器節點均已升級。

後續步驟

- 登入 vRealize Network Insight 並執行您的工作。
- 在兩到三天後，刪除快照以節省磁碟空間。

單鍵離線升級

vRealize Network Insight 支援從 3.7 版及更新版本的產品執行單鍵離線升級。

必要條件

- 如果 /tmp 目錄中沒有足夠的空間，升級步驟可能會失敗。確認是否符合平台和收集器伺服器的以下磁碟空間需求：
 - /tmp - 6 GB
 - /home - 2 GB

- 確認是否符合平台伺服器的以下磁碟空間需求：
 - /-12 GB (僅適用於平台 1 節點)
 - /var - 40 GB

備註 如果 /tmp 目錄中沒有足夠的空間，則服務包上傳和後續升級步驟可能會失敗。

- 若要避免使用者介面工作階段逾時，請移至**設定 > 系統組態 > 使用者工作階段逾時**，並將**使用者工作階段逾時**增加到至少 2 小時。變更工作階段逾時持續期間後，您必須再次登入系統。
- 確保所有節點都處於線上狀態。如果任何節點均為非作用中狀態，則不允許觸發升級。
- 取得虛擬機器的快照。
- 請注意，在移轉後要驗證下列值：
 - 虛擬機器計數
 - 快照計數大於 0 的虛擬機器
 - 防火牆規則計數
 - 安全群組計數
 - NSX 防火牆計數

程序

- 1 從 [My VMware](#) 下載必要的升級服務包檔案並將更新套件儲存在本機磁碟。
- 2 檢查並確認已下載服務包的 MD5SUM 值與 VMware 網站中指定 MD5SUM 值相符。
- 3 在**安裝與支援**頁面的**軟體版本**下，選取**按一下這裡**。
- 4 按一下**瀏覽**以選取檔案並按一下**上傳**。

上傳完成後，vRealize Network Insight 會在 2 到 3 分鐘內顯示服務包上傳完成訊息通知，並且在背景中執行服務包處理。

備註

- 如果未上傳套件，請確保工作階段未關閉。如果工作階段結束，您必須重新啟動上傳程序。
 - 在看到更新可用訊息通知之前，請不要在服務包上傳後重新整理頁面。
-

- 5 在更新可用訊息通知中，按一下**檢視詳細資料**。
[vRealize Network Insight 升級] 畫面隨即顯示。
- 6 讀取**繼續操作之前指令**，並按一下**繼續**。
- 7 等待預先檢查完成，這會驗證：
 - 磁碟空間，包括移轉所需的空間
 - 版本
 - NTP 同步狀態

- 服務包

8 按一下**立即安裝**。

您可以在安裝程式上看到完成升級程序所需的大概時間。

9 升級程序開始後，[vRealize Network Insight 升級] 畫面會提供升級程序的狀態。

備註

- 如果某個節點變成非作用中狀態，則升級程序不會繼續。節點再次變為作用中之後，升級才會復原。
 - 平台 1 成為升級伺服器。如果平台 1 處於離線狀態，則不會升級其他節點。
 - 平台升級後，您可以繼續執行一般 vRealize Network Insight 作業，即使仍在執行收集器升級。如果升級程序未全部完成，[安裝與支援] 頁面中會顯示 `Node Version Mismatch detected` 訊息。
-
- 升級服務後，Nginx 會重新啟動以顯示移轉程序。因此，您可能在短時間 (一至兩分鐘) 內無法存取使用者介面。
 - vRealize Network Insight 開始將資料移轉至 Foundation 資料庫。在 [資料移轉狀態] 畫面上，您會看到：
 - 整體狀態
 - 已耗用時間
 - 按資料表狀態列出的資料表
 - 已移轉的記錄數
- 如有任何問題，您可以使用**匯出移轉記錄**選項與 VMware 支援團隊分享。
- 在升級程序過程中，收集器上的 PostgreSQL 資料也會移轉至 Foundation 資料庫。但是，收集器的移轉狀態不會顯示在使用者介面上。

10 完成升級程序後，您會看到確認訊息。

所有平台和收集器節點均已升級。

後續步驟

- 登入 vRealize Network Insight 並執行您的工作。
- 在兩到三天後，刪除快照以節省磁碟空間。

CLI 升級

僅當線上升級或單鍵離線升級都不起作用時，才考慮進行 CLI 升級。必須先升級平台虛擬機器，再升級收集器虛擬機器。但是，在使用 CLI 啟動離線升級之前，必須先連絡 VMware 支援。

在叢集環境中，您必須僅從平台 1 (P1) 節點執行升級作業，叢集中的其他平台節點會自動升級。但是，您必須單獨升級每個收集器。

必要條件

- 如果 /tmp 目錄中沒有足夠的空間，升級步驟可能會失敗。確認是否符合平台和收集器伺服器的以下磁碟空間需求：
 - /tmp - 6 GB
 - /home - 2 GB
 - /var - 40 GB
- 確保所有節點都處於線上狀態。如果任何節點均為非作用中狀態，則不允許觸發升級。
- 取得虛擬機器的快照。
- 請注意，在移轉後要驗證下列值：
 - 虛擬機器計數
 - 快照計數大於 0 的虛擬機器
 - 防火牆規則計數
 - 安全群組計數
 - NSX 防火牆計數

程序

- 1 從 [My VMware](#) 下載必要的升級服務包檔案。
- 2 檢查並確認已下載服務包的 MD5SUM 值與 VMware 網站中指定的 MD5SUM 值相符。
- 3 將升級服務包複製到 vRealize Network Insight 平台 1 虛擬機器和所有收集器虛擬機器。
 - 若要將檔案從 Linux 虛擬機器複製到 vRealize Network Insight 虛擬機器，請執行命令 `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/`。
 - 若要將檔案從 Windows 虛擬機器複製到 vRealize Network Insight 虛擬機器，請執行命令 `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/`。

備註 使用 <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe> 中的 pscp 公用程式。

- 4 透過 CLI 使用 `consoleuser` 登入 vRealize Network Insight 平台 1，然後執行下列命令：
 - `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
 - `package-installer upgrade --name <filename>.upgrade.bundle`

備註 您必須先執行平台升級，然後再啟動收集器更新。

- 5 在作業系統升級過程中將安裝程式重新開機後再次執行 `package-installer upgrade` 命令。

重要 如果出現 SSH 工作階段逾時錯誤，您必須檢查 `/var/log/arkin/centralized_upgrade.log` 以瞭解是否已進行重新開機。如果重新開機成功，您必須再次執行 `package-installer upgrade` 命令。

- 6 透過 CLI 登入每個收集器節點，並使用用於平台升級的相同命令執行升級。

備註 您可以同時升級所有收集器。

- 7 使用 `show-version` 命令驗證已升級的版本。

解除安裝 vRealize Network Insight

6

您必須透過 vSphere Web Client 解除安裝 vRealize Network Insight。

程序

1 如果您可以存取 vRealize Network Insight Web 入口網站，請執行下列操作：

- a 登入 vRealize Network Insight Web 入口網站。
- b 移至**設定 > 帳戶和資料來源**。
- c 關閉並刪除所有資料來源。

刪除 vCenter 資料來源會移除 VDS 上的 IPFIX 設定 (如果已設定)。同樣，刪除 NSX Manager 資料來源會從 NSX 流量監視器中移除 IPFIX 設定。

2 如果您無法存取 vRealize Network Insight Web 入口網站，請執行下列操作：

- a 如果 vCenter 上已啟用 Netflow (IPFIX)，請從 VDS/DVPG IPFIX 設定中移除 vRealize Network Insight 收集器 IP。請參閱在 [vCenter 中啟用 Netflow 時移除收集器 IP](#)。
- b 如果 NSX 上已啟用 IPFIX，則移除 vRealize Network Insight 收集器 IP 流量監控設定。請參閱在 [NSX 中啟用 Netflow 時移除收集器 IP](#)。
- c 如果在實體交換器上設定 Netflow 以將 Netflow 傳送至 vRealize Network Insight Netflow 收集器，則修改交換器中的組態以停止傳送 NetFlow 資訊。

3 如果建立了任何特定防火牆或路由規則以允許或路由進出 vRealize Network Insight 虛擬機器的流量，則移除這些防火牆/路由規則。

4 基於安全考量，清理用於在 vRealize Network Insight 中設定資料來源的存取認證。

5 關閉並刪除所有 vRealize Network Insight 收集器和平台虛擬機器。

在 vCenter 中啟用 Netflow 時移除收集器 IP

如果在 vCenter 中已啟用 Netflow (IPFIX)，則使用此程序從虛擬專用伺服器 (VDS)/分散式虛擬連接埠群組 (DVPG) IPFIX 設定移除 vRealize Network Insight 收集器 IP。

程序

- 1 登入 vSphere Web Client。
- 2 移至**首頁 > 網路**。

- 3 在左窗格中，選取 **VDS**，然後按一下**設定 > 編輯**。
- 4 在**收集器 IP 位址**欄位中，移除 vRealize Network Insight 收集器 IP 詳細資料。
- 5 在**收集器連接埠**欄位中，移除連接埠詳細資料。
- 6 按一下**確定**。
必須等待約兩分鐘之後，才能移至下一步。
- 7 選取此 VDS 的 DVPG，然後按一下**設定 > 原則 > 編輯**。
- 8 在 **Netflow** 欄位中，從下拉式功能表選取**停用**。
- 9 驗證設定，然後按一下**套用**。

後續步驟

針對已啟用 IPFIX 的每個 VDS 及其 DVPG 再次執行步驟以移除 vRealize Network Insight 收集器 IP。

在 NSX 中啟用 Netflow 時移除收集器 IP

如果在 NSX 中啟用 Netflow (IPFIX)，則使用此程序移除 vRealize Network Insight (vRealize Network Insight) 收集器 IP 流量監控設定。

程序

- 1 登入 vSphere Web Client。
- 2 按一下**首頁 > 網路與安全性 > 工具 > 流量監控 > 組態**。
- 3 在**全域流量收集狀態**中，按一下**停用**。
- 4 若要停用流量連線，請按一下 **IPFIX**。
- 5 在 **IPFIX** 索引標籤中，選取**收集器 IP**，然後按一下**刪除**。
- 6 如果已經沒有其餘的 IP，則按一下**編輯**並清除**啟用 IPFIX 組態**核取方塊。
- 7 按一下**儲存**。