

vRealize Log Insight 8.0 版本說明

版本說明的內容

本說明涵蓋下列主題：

- [關於 vRealize Log Insight](#)
- [新增功能](#)
- [相容性](#)
- [限制](#)
- [從舊版升級](#)
- [國際化支援](#)
- [已解決的問題](#)
- [已知問題](#)

關於 vRealize Log Insight

vRealize Log Insight 特別為 VMware 環境提供最佳的即時和封存記錄管理。以機器學習為基礎的智慧型分組以及高效能搜尋，可加快實體、虛擬和雲端環境中的疑難排解作業。vRealize Log Insight 可以分析數 TB 的記錄、探索非結構化資料中的結構，並使用現代的 Web 介面提供全企業的可見度。

如需詳細資訊，請參閱 vRealize Log Insight 產品說明文件，網址：<https://docs.vmware.com/tw/vRealize-Log-Insight/index.html>。

新增功能

vRealize Log Insight 伺服器功能

- 支援在 Photon OS 上安裝 vRealize Log Insight 伺服器。這包括全新安裝或從 4.8 升級。
- 憑證管理
 - 憑證的新管理頁面
 - 列出所有受信任的憑證
 - 從受信任的存放區中移除個別或選取的憑證
 - 根據指紋、憑證提供者資訊 (提供者類型或主機名稱) 和到期狀態進行篩選
- 支援 IPv6 環境 (單純 IPv6 或雙重堆疊)
- 增強的記錄匯出，可匯出 NFS 共用位置中超過 2 萬筆的記錄行
- 適用於 vSphere 的 REST API 和授權使用量

- 稽核記錄增強功能
 - 單一稽核記錄位置
 - 組態變更的記錄
 - 類似儀表板的內容變更記錄
- 可設定的警示取消期間
- vSphere、vSAN、NSX-T、vRealize Operations Manager、VMware Identity Manager、vRealize Automation 和 Linux 內容套件的增強功能

vRealize Log Insight 代理程式功能

- vRealize Log Insight 代理程式現在為開放原始碼。當您開啟工具 SDK 下載頁面時，您可以在[驅動程式與工具](#)下的 vRealize Log Insight 下載頁面來下載代理程式和匯入工具。
- 平台支援：
 - Windows Server 2019
 - Ubuntu 18.04
 - Photon v3

相容性

vRealize Log Insight 8.0 支援以下 VMware 產品和版本：

- vRealize Log Insight 可以從 VMware vCenter Server 6.0 或更新版本提取事件、工作和警示資料。
- 您可以整合 vRealize Log Insight 8.0 與 vRealize Operations Manager 7.0 版或更新版本。

瀏覽器支援

vRealize Log Insight 8.0 支援下列瀏覽器版本。更新版本的瀏覽器也適用於 vRealize Log Insight，但尚未經過驗證。

- Mozilla Firefox 45.0 及更高版本
- Google Chrome 51.0 及更高版本
- Safari 9.1 及更高版本
- Internet Explorer 11.0 及更高版本

備註：Internet Explorer 文件模式必須在**標準模式**下使用。不支援其他模式。不支援 [相容性檢視] 瀏覽器模式。

支援的最小瀏覽器解析度為 1280x800 像素。

重要事項：您的瀏覽器中必須啟用 Cookie。

vRealize Log Insight Windows 代理程式支援

vRealize Log Insight 8.0 Windows 代理程式支援下列版本：

- Windows 7、Windows 8、Windows 8.1 和 Windows 10
- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019

vRealize Log Insight Linux 代理程式支援

vRealize Log Insight Linux 代理程式支援下列發行版：

- RHEL 5、RHEL 6 和 RHEL 7
- SUSE Enterprise Linux (SLES 11 SP3) 和 SLES 12 SP1
- Ubuntu 14.04 LTS、Ubuntu 16.04 LTS 和 Ubuntu 18.04
- VMware Photon (第 1 版，修訂 2 版)、第 2 版和第 3 版

限制

vRealize Log Insight 8.0 具有以下限制：

一般

- vRealize Log Insight 無法正確處理不可列印的 ASCII 字元。
- vRealize Log Insight 不支援列印。不過，您可以使用瀏覽器的 [列印] 選項。列印結果可能視您使用的瀏覽器而有所不同。建議您使用 Internet Explorer 或 Firefox 列印 vRealize Log Insight 使用者界面的部分。
- 主機資料表可能多次顯示裝置，每次都採取不同格式，包括 IP 位址、主機名稱和 FQDN 的一些組合。例如，名為 foo.bar.com 的裝置可能同時以 foo 和 foo.bar.com 兩種格式出現。主機資料表使用 syslog RFC 中定義的 hostname 欄位。如果裝置透過 syslog 通訊協定傳送的事件沒有主機名稱，則 vRealize Log Insight 會使用來源做為主機名稱。這可能會導致多次列出裝置，因為 vRealize Log Insight 無法判斷這兩種格式是否指向同一個裝置。

vRealize Log Insight Windows 和 Linux 代理程式

- 當 vRealize Log Insight Windows 和 Linux 代理程式以 syslog 模式執行時，無法正確傳遞 hostname 和 source 欄位中的非 ASCII 字元。

vRealize Log Insight Windows 代理程式

- vRealize Log Insight Windows 代理程式是 32 位元應用程式，其所有從 C:\Windows\System32 子目錄開啟檔案的要求，均會由 WOW64 重新導向至 C:\Windows\SysWOW64。不過，您可以將 vRealize Log Insight Windows 代理程式設定為使用特殊別名 C:\Windows\Sysnative 從 C:\Windows\System32 進行收集。例如，若要從 MS DHCP 伺服器的記錄預設位置收集記錄，請將下列一行新增到 vRealize Log Insight Windows 代理程式組態檔中的對應區段：=C:\Windows\Sysnative\dhcp。

vRealize Log Insight Linux 代理程式

- 由於作業系統限制，當 vRealize Log Insight Linux 代理程式設定為透過 syslog 傳送事件時，將無法偵測網路中斷。
- vRealize Log Insight Linux 代理程式不支援在欄位或標籤名稱中使用非英文 (UTF-8) 符號。
- vRealize Log Insight Linux 代理程式預設會收集隱藏的檔案與目錄。若要防止此情況發生，您必須在每個組態區段新增 `exclude=.*` 選項。`exclude` 選項中所用的全域模式 `.*` 代表隱藏的檔案格式。
- 使用標準輸出重新導向至檔案以產生記錄時，vRealize Log Insight 代理程式可能無法正確辨識在這類記錄檔中的事件界限。

vRealize Log Insight 整合

當 vRealize Operations 執行個體看不到虛擬機器的 IP 位址，且該位址未由 vCenter 顯示在虛擬機器上的**虛擬機器摘要索引標籤**時，包括透過 vRealize Log Insight 和 vRealize Operations 的「在環境定義中啟動」針對虛擬機器可能無法正常運作。因為缺乏 vmware-tools 公用程式，IP 位址可能無法使用。較舊、不受支援的版本或故障的 vmware-tools 也會導致 IP 位址變得無法使用。

請確保虛擬機器上已安裝適當的 VMware Tools 版本，且 vCenter 的**虛擬機器摘要索引標籤**顯示了虛擬機器的 IP 位址。

從舊版 vRealize Log Insight 升級

升級至此版本的 vRealize Log Insight 時，請記住下列考量。

升級路徑

您可以從 4.8 直接升級至 vRealize Log Insight 8.0。如果您正在執行舊版的 vRealize Log Insight，您必須先將安裝逐步升級至 4.8。

重要升級通知

- 若要升級至 vRealize Log Insight 8.0，您執行的必須是 vRealize Log Insight 4.8。
- 在執行手動升級時，您必須一次升級一個工作。同時升級多個工作會使升級失敗。將主節點升級為 vRealize Log Insight 8.0 時，除非特別停用漸進式升級，否則會進行漸進式升級。
- 升級必須透過主節點的 FQDN 完成。不支援以整合式負載平衡器 IP 位址進行升級。
- vRealize Log Insight 不支援雙節點叢集。先新增與現有的兩個節點相同版本的第三個 vRealize Log Insight 節點後，再執行升級。
- 如果 vRealize Log Insight 升級 (.pak 檔案) 具有新版的 JRE，則在升級後，使用者在 vRealize Log Insight 設定 (例如針對事件轉送) 中安裝的憑證會變為不可見。
- 如果整合目的地為 SSL 連線提供了不受信任的憑證，則在升級後，與 vRealize Log Insight 的整合將無法正常運作，因為這些憑證未新增至信任存放區。這些整合目的地包括 vSphere、vRealize Operations Manager、事件轉送站、Active Directory 和 SMTP。因應措施是，在每個整合組態頁面中，測試連線並接受不受信任的 SSL 憑證 (如果出現顯示憑證詳細資料的對話方塊)。接受憑證會將其新增至信任存放區。
- Photon OS 已改善安全性原則，而可能會要求您在成功升級至 Photon OS 之後必須變更根密碼。只有在 SLES 中的根密碼到期時才需要變更密碼，但不同於 Photon OS，SLES OS 不會強制執行更新。
- 當您將 SLES 式的 vRealize Log Insight 4.8 升級至最新的 Photon 式 vRealize Log Insight 時，sshd 自訂服務組態 (/etc/ssh/sshd_config) 會重設為其預設值。因應措施是，在升級之前儲存

/etc/ssh/sshd_config 組態，然後在升級後手動重新設定。

- Photon OS 對於同時 ssh 連線數目具有嚴格的規則。由於 /etc/ssh/sshd_config 檔案中的 MaxAuthtries 值依預設為 2，在有多個連線時，使用 ssh 連線至 vRealize Log Insight 虛擬應用裝置可能會失敗，並顯示下列訊息：「從 xx.xx.xx.xxx 連接埠 22:2 收到中斷連線：驗證失敗次數太多」。針對此問題，您可以使用下列任何因應措施：
 - 透過 ssh 連線時，請使用 IdentitiesOnly=yes 選項：`#ssh -o IdentitiesOnly=yes user@ip`
 - 更新 ~/.ssh/config 檔案以新增：`Host* IdentitiesOnly yes`
 - 修改 /etc/ssh/sshd_config 檔案並重新啟動 sshd 服務，以變更 MaxAuthtries 值。
- 開始從 vRealize Log Insight 4.8 叢集升級至 8.0 之前，請確認每個節點在根磁碟分割中有足夠的可用空間。如需詳細資訊，請參閱 <https://kb.vmware.com/s/article/76282>。
- 使用靜態 IP 時 (相對於透過 DHCP 取得的 IP)，請確保對應的 SLES 網路組態檔包含所有叢集節點上的閘道項目，然後再升級至 vRealize Log Insight 8.0。如需詳細資訊，請參閱 <https://kb.vmware.com/s/article/76067>。

國際化支援

vRealize Log Insight 8.0 包括以下當地語系化功能。

- vRealize Log Insight 伺服器 Web 使用者介面現有日文、法文、西班牙文、德文、簡體中文、繁體中文和韓文等當地語系化版本。
- vRealize Log Insight 伺服器 Web 使用者介面支援 Unicode 資料，包括機器學習功能。
- vRealize Log Insight 代理程式可在非英文的原生 Windows 上運作。

限制

- 代理程式安裝程式和內容套件並無當地語系化版本。vRealize Log Insight 伺服器 Web 使用者介面有些地方仍可能會顯示未經當地語系化的字串並有版面配置問題。
- vRealize Log Insight 可與當地語系化版本的 vCenter Server 和 vRealize Operations Manager 互通。不過，內容套件則視未經當地語系化的相符記錄訊息而定。擷取 vCenter Server 事件時，會採用預設地區設定 (應已設為 en_US)。如需詳細資訊，請參閱 <http://kb.vmware.com/kb/2121646>。
- 若使用者名稱含非 ASCII 字元，則不支援與 Active Directory、vSphere 與 vRealize Operations Manager 進行整合。
- 不支援當地語系化的事件記錄。事件記錄僅支援 UTF-8 和 UTF-16 字元編碼。
- vRealize Log Insight 8.0 的全新部署僅顯示英文版的使用者授權合約 (EULA)。

已解決的問題

此版本中沒有已解決的問題。

已知問題

在此版本中出現下列已知問題。

- 虛擬中心 (VC) 事件收集已延遲

重新啟動 Log Insight 服務或 Log Insight 叢集升級之後，如果整合了大量 VC，則可能會延遲虛擬中心 (VC) 的事件收集。

因應措施：在收集到足夠的一段時間之後，事件即會自動還原。時間長度取決於您的環境。例如，針對 4 節點叢集上的 80 個 VC，延遲時間將為一小時。

- **刪除 vRealize Operations 整合失敗**

如果 Log Insight 先前已與 vRealize Operations 執行個體整合，但整合已變得無法連線，則其無法強制移除整合。

因應措施：重新整理並嘗試再次移除整合。

- **設定雙向信任時，Log Insight 無法從第二個受信任的 Active Directory 驗證使用者和群組**

當 Active Directory 設定為搭配其他 Active Directory 使用雙向信任時，vRealize Log Insight 無法驗證第二個受信任 Active Directory 的使用者和群組。

因應措施：使用與這兩個 Active Directory 直接整合的 vIDM。

- **從某些目錄進行收集時，如果這些目錄是在代理程式啟動或重新設定事件之前建立的，則無法執行收集。**

如果在重新設定之後建立新目錄，則不會執行新建目錄的代理程式收集。

因應措施：若要開始監控目錄，請重新啟動服務，或透過 liagent.ini 檔案或 [伺服器管理員代理程式] 頁面更新代理程式組態。

- **Photon OS 上的 vRealize Log Insight 代理程式不會自動升級**

您無法對 Photon OS 上的 vRealize Log Insight 代理程式執行自動升級，因為 Photon OS 不支援 gpg 命令。

因應措施：執行手動升級。

- **SMTP 組態可能不適用於透過 IPv6 的公用郵件伺服器**

SMTP 組態可能不適用於 Google 和 Yahoo 之類的公用電子郵件服務，因為這些服務可能會對 IPv6 利用更嚴格的限制原則。

因應措施：使用替代郵件伺服器 (例如您的公司郵件伺服器)，或啟動專用伺服器。

- **透過 IPv4 整合 VMware Identity Manager 與 vRealize Log Insight，會將重新導向 URL 主機變更為 IPv6 位址**

如果您在部署 vRealize Log Insight 虛擬應用裝置時選取了優先使用 IPv6 位址的選項，則在與不支援 IPv6 的 VMware Identity Manager 整合時，重新導向 URL 主機清單中會填入 IPv6 節點位址。

因應措施：建立備用 IPv4 VIP 以整合 vRealize Log Insight 與 VMware Identity Manager。