

# vRealize Log Insight 8.4 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，以及使用現代的 Web 介面提供企業範圍的可見度。

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

以下是 vRealize Log Insight 8.4 的一些關鍵特色，可協助您更快速地、精確地且有效地利用記錄資料：

- **記錄來源：**現在，您可以將 Fluentd 設定為從各種來源 (例如 Docker、Kubernetes、Tanzu Kubernetes Grid 和 OpenShift) 收集記錄，然後將這些記錄轉送至 vRealize Log Insight。Fluentd 是開放原始碼記錄處理器和轉送站，可讓您從不同的來源收集記錄資料，並透過篩選器充分利用這些資料。它是適用於 Kubernetes 等容器化環境的偏好選擇。您可以在 vRealize Log Insight 使用者介面內找到 Fluentd 記錄來源的組態步驟。
- **記錄遮罩：**您的記錄資料包含可能會視為敏感的資訊。特定的記錄訊息可能包括使用者名稱、電子郵件地址、URL 參數，以及其他您不想揭露的資訊。記錄遮罩可讓您對處理您認為敏感資訊的組態進行修改，藉此對任何資訊進行遮罩處理。
- **記錄捨棄：**有時，您的基礎結構會產生許多太大或具有明顯波動的記錄事件。在這種情況下，您可能需要選擇要傳送至記錄管理解決方案的記錄，以及要捨棄的記錄。記錄捨棄可讓您藉由修改適當的組態來刪除某些記錄。
- **自訂 Webhook：**vRealize Log Insight Webhook 連線現在可用於將通知從警示傳送至 Slack 和 PagerDuty。您也可以藉由定義適當的裝載，將通知傳送到自訂 Webhook。
- **根據磁碟分割進行封存：**資料封存可保留因儲存區限制而可能會從 vRealize Log Insight 虛擬應用裝置中移除的舊記錄。vRealize Log Insight 可以儲存封存資料，以在 NFS 掛接中進行資料磁碟分割。
- **警示管理：**您可以使用升級後的警示管理，在一個環境中查看您組織範圍內的警示完整清單。警示現在是以組織為中心，而非以使用者為中心的模式，可為控制組織警示提供更多彈性。已更新用於管理以查

詢為基礎的警示權限。使用者目前需要「互動式分析」權限，才能檢視警示，以及需要「編輯共用內容」權限，才能建立和管理警示。

- **使用新的大小調整計算器簡化的大小調整：**正確調整 vRealize Log Insight 叢集大小對於在搜尋及分析記錄時達成最佳效能，並確保一個叢集具有所需的資源至關重要。大小調整計算器會根據伺服器及裝置記錄的類型、預期的擷取速率，以及記錄保留需求，來判斷所需的節點大小。
- **NSX Data Center 版本：**vRealize Log Insight 現在隨附於下列新的 NSX Data Center 版本。如需詳細資訊，請參閱 [VMware NSX Data Center 資料工作表](#)。
  - NSX Firewall
  - 具有 Advanced Threat Prevention 的 NSX Firewall
- **內容套件更新：**下列內容套件已更新。
  - VMware NSX-v 4.2.1 (與欄位擷取相關的更新)
  - VMware NSX-t v4.0.1 (新增儀表板支援「整合安全性流量記錄」)
  - VMware vRA 8.3+ (支援 vRA 8.3+ 產品線)
  - Microsoft IIS v3.4 (〈設定指示〉一節中的改進，說明如何從記錄中擷取自訂欄位。)
  - VMware Horizon v4.0.1
  - vSphere 8.4
  - vRops v4.2
  - vSAN (支援 vSAN 70u2)
  - 已驗證的其他內容套件：
    - NPE 伺服器 v1.1.1
    - Mongo DB v2.4
    - Solarwinds v1.1
    - Oracle DB v1.1
    - NPE Nimble v1.1

## 相容性

vRealize Log Insight 8.4 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。在 FIPS 模式中，vRealize Log Insight 可整合 VMware vCenter Server 6.0 U1 或更新版本。
- 您可以整合 vRealize Log Insight 8.4 與 vRealize Operations Manager 8.0.1 或更新版本。

## 瀏覽器支援

vRealize Log Insight 8.4 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 72.0 及更高版本
- Google Chrome 78.0 及更高版本
- Safari 11.1 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 8.4 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、RHEL 7 和 RHEL 8
- 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 8.4 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 使用者介面的部分。
- 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。
- 新增資料磁碟分割或刪除現有資料磁碟分割時，需要重新啟動叢集 (逐一重新啟動叢集節點) 才能使新的組態生效。但是，現有資料磁碟分割之路由篩選器、已啟用狀態和保留期間的變更則會立即套用 (不需要重新啟動叢集)。
- FIPS 模式啟用後將無法停用。

## 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 8.3 或 8.2 升級至 vRealize Log Insight 8.4。

### 重要升級通知

- 若要升級至 vRealize Log Insight 8.4，您必須是執行 vRealize Log Insight 8.3 或 8.2。
- 從命令列執行手動升級時，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。
- 從使用者介面將主節點升級為 vRealize Log Insight 8.4 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。
- 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。

# 國際化支援

vRealize Log Insight 8.4 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。

## 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 vRealize Log Insight 服務或叢集升級之後，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，針對有四個節點之叢集上的 80 個 VC，延遲時間將為一小時。
- **設定雙向信任時，vRealize 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。

- **Internet Explorer 11.0 中的版面配置問題**

在 Internet Explorer 11.0 中，標頭和圖表圖例清單顯示 (位於儀表板和互動式分析索引標籤上) 的使用者圖示有版面配置問題。

**因應措施：**如需因應措施，請參閱 <https://kb.vmware.com/s/article/78592>。

- **REST API 呼叫「POST/api/v1/sessions」失敗**

當您使用從 4.8 或更早版本升級的舊叢集在 vRealize Log Insight 8.2 或 8.3 中加入新部署的節點時，REST API 會無法將「POST/api/v1/sessions」呼叫至新的工作節點，並引發下列錯誤：

*Error: write EPROTO 1319245176:error:100000f7:SSL routines:OPENSSL\_internal:WRONG\_VERSION\_NUMBER:../third\_party/boringssl/src/ssl/tls\_record.cc:242:*

您可以在 REST 用戶端中找到相關記錄。由於此錯誤，您無法取得節點的工作階段。

**因應措施：**在受影響的節點上執行「service loginsight restart」命令，藉此重新啟動 vRealize Log Insight 服務。

- **在 FIPS 模式下測試使用 STARTTLS 設定的自訂 SMTP 伺服器會引發憑證錯誤**

在 FIPS 模式中透過 STARTTLS 選項來設定自訂 SMTP 伺服器時，當按一下傳送測試電子郵件時，系統會顯示一個接受自我簽署憑證的快顯視窗。當您接受憑證時，系統會顯示下列錯誤：

*找不到要求目標的有效憑證路徑*

**因應措施：**透過執行「service loginsight restart」命令重新啟動 vRealize Log Insight 服務。

- **vRealize Log Insight 使用會沒有信任憑證的自訂 SMTP 伺服器來傳送電子郵件通知**

藉由自訂 SMTP 伺服器，vRealize Log Insight 會透過電子郵件傳送警示和系統通知，即使不接受自訂憑證也一樣。

**因應措施：**無。

- **在 FIPS 模式中部署的 vRealize Log Insight 8.3 全新設定升級失敗**

啟用 FIPS 模式進行部署時，vRealize Log Insight 8.3 全新設定升級失敗。

**因應措施：**部署後啟用 FIPS 模式。請參閱 <https://kb.vmware.com/s/article/83360>。

- **即使升級成功時，vRealize Log Insight 仍會顯示「升級未獲確認」訊息**  
升級至 vRealize Log Insight 8.4 時，可能會出現指出升級狀態未獲確認的訊息。此訊息不會影響整體升級狀態，因此升級最終會成功。

**因應措施：**無。

- **雙重堆疊或 IPv6 設定的升級失敗**  
將雙堆疊或 IPv6 設定升級至 vRealize Log Insight 8.4 失敗。

**因應措施：**無。