

使用 vRealize Log Insight Importer

2020 年 4 月 14 日

vRealize Log Insight 8.1



vmware®

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/>

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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 使用 vRealize Log Insight Importer 4**
 - 安裝 vRealize Log Insight Importer 4
 - 安裝 vRealize Log Insight Importer 之前 4
 - 安裝 vRealize Log Insight Importer 5
 - 執行 vRealize Log Insight Importer 6
 - 關於 vRealize Log Insight Importer 資訊清單檔案 6
 - vRealize Log Insight Importer 資訊清單檔案組態範例 7
 - 執行 vRealize Log Insight Importer 8

使用 vRealize Log Insight Importer

1

vRealize Log Insight Importer 是一種命令列公用程式，用於將歷史資料的離線記錄從本機機器匯入至 vRealize Log Insight 伺服器。

當您想要匯入過去收集的記錄檔時，請使用匯入工具。您可以匯入支援服務包和封存記錄檔，並分析從 vRealize Log Insight 或任何 VMware 產品收集的支援服務包記錄檔。

vRealize Log Insight Importer 包括下列特性和功能。

- vRealize Log Insight Importer 會透過擷取 API 傳送資料。
- 它支援檔案記錄收集，包括遞迴目錄收集。
- Importer 可從 zip、tar、bzip、bzip2 或 gz 封存檔中讀取資料。不支援 7-Zip。
- 您可以規定要從巢狀封存檔 (例如巢狀 ZIP 檔案) 或從封存檔內的目錄中遞迴地讀取資料。

本章節討論下列主題：

- [安裝 vRealize Log Insight Importer](#)
- [執行 vRealize Log Insight Importer](#)

安裝 vRealize Log Insight Importer

您需要從透過 VMware 下載網站取得的安裝套件來安裝 vRealize Log Insight Importer。安裝套件包含適用於 Windows 的 MSI 安裝程式，以及適用於 Linux 的 POSIX 安裝套件 (RPM、DEB 及 BIN)。

- [安裝 vRealize Log Insight Importer 之前](#)
安裝匯入工具之前，請檢查需求並瞭解匯入工具的行為。
- [安裝 vRealize Log Insight Importer](#)
您可以在 Windows 和 Linux 上安裝 vRealize Log Insight Importer。您也可以從 vRealize Log Insight 伺服器上安裝 vRealize Log Insight Importer，並從伺服器加以執行。

安裝 vRealize Log Insight Importer 之前

安裝匯入工具之前，請檢查需求並瞭解匯入工具的行為。

安裝之前，請確保 vRealize Log Insight 可存取儲存封存資料所在的 NFS 伺服器。如果 NFS 伺服器因為網路故障或 NFS 伺服器上的錯誤而變得無法存取，則匯入封存資料可能會失敗。

在擷取期間從服務包中擷取記錄時，將會自動決定記錄服務包名稱，並以服務包標籤的形式將其新增至所有已擷取的記錄。此標籤名稱為記錄的檔案名稱，如果是目錄來源，則為目錄名稱。服務包標籤可區分 vRealize Log Insight 伺服器上的服務包。

此標籤會覆寫資訊清單檔案中所指定的任何同名標籤。使用相同名稱的命令列標籤則會覆寫此標籤。

使用匯入工具時，請留意下列行為：

- vRealize Log Insight Importer 不會檢查 vRealize Log Insight 虛擬應用裝置上的可用磁碟空間。因此，如果虛擬應用裝置的磁碟空間不足，匯入已封存記錄可能會失敗。
- 於記錄匯入期間，vRealize Log Insight 不會顯示進度資訊。當匯入封存資料的作業正在進行中時，您無法根據主控台輸出來推斷匯入作業究竟還剩下多少時間才會完成，或究竟已匯入多少資料。

支援的作業系統

下列作業系統支援 vRealize Log Insight Importer：

- Windows 32 位元和 64 位元
- Linux 32 位元和 64 位元

Linux 版本無法在 Apple Macintosh 系統上執行。

安裝 vRealize Log Insight Importer

您可以在 Windows 和 Linux 上安裝 vRealize Log Insight Importer。您也可以從 vRealize Log Insight 伺服器上安裝 vRealize Log Insight Importer，並從伺服器加以執行。

安裝 vRealize Log Insight Importer 時，系統也會安裝一些 VMware 產品資訊清單檔案。您可以在執行 vRealize Log Insight Importer 時，視需要使用或修改這些檔案。這些資訊清單檔案位於 C:\Program Files (x86)\VMware\Log Insight Importer\Manifests (適用於 Windows) 和 /usr/lib/loginsight-importer/manifests (適用於 Linux)。

如果您解除安裝 .bin 套件，也會刪除 /usr/bin/loginsight_importer 符號連結。

必要條件

- 確認您可以存取 [VMware 下載網站](#)，以下載 vRealize Log Insight Importer。

程序

- 1 從 [VMware 下載網站](#) 下載 vRealize Log Insight Importer 安裝套件。

安裝套件包含適用於 Windows 的 MSI 安裝程式，以及適用於 Linux 的 POSIX 安裝套件 (RPM、DEB 及 BIN)。

2 在您的系統上安裝工具。

安裝之後，在 Windows 上會將匯入工具安裝目錄新增到 PATH 環境變數，在 Linux 上會將指向可執行檔 `loginsight-importer` 的符號連結新增到 `/usr/bin/`。如此用戶端就可以從 Shell 呼叫 `loginsight-importer`，而不必指定路徑首碼。

vRealize Log Insight Importer 工具會安裝在下列位置。

作業系統	檔案名稱	安裝位置
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

執行 vRealize Log Insight Importer

當您執行匯入工具時，您必須包含資訊清單檔案。資訊清單檔案提供記錄檔格式、要匯入資料位置的相關資訊以及來源和目的地資訊。

- [關於 vRealize Log Insight Importer 資訊清單檔案](#)

vRealize Log Insight Importer 使用資訊清單組態檔來判定記錄格式並指定要匯入的資料位置。資訊清單檔案與 `liagent.ini` 組態檔具有相同的格式和相似的結構。

- [vRealize Log Insight Importer 資訊清單檔案組態範例](#)

範例 vRealize Log Insight Importer 資訊清單檔案提供參數組態的範例。

- [執行 vRealize Log Insight Importer](#)

執行 vRealize Log Insight Importer 以將歷史資料的離線記錄匯入至 vRealize Log Insight 伺服器。

關於 vRealize Log Insight Importer 資訊清單檔案

vRealize Log Insight Importer 使用資訊清單組態檔來判定記錄格式並指定要匯入的資料位置。資訊清單檔案與 `liagent.ini` 組態檔具有相同的格式和相似的結構。

您可以選擇性地建立自己的資訊清單檔案來匯入任意記錄檔。建立此類檔案的優點之一是您不需要知道資料檔案的絕對路徑。

如果不建立資訊清單檔案，vRealize Log Insight Importer 會使用收集所有 `.txt` 和 `.log` 檔案 (`include=*.log*;*.txt*`) 的預設資訊清單，並對擷取的記錄套用自動剖析器 (擷取時間戳記 + `kvp`)。

如果將 `liagent.ini` 組態檔用作資訊清單檔案，則 vRealize Log Insight Importer 只會擷取 `[filelog]` 區段做為資訊清單。vRealize Log Insight Importer 支援 `[filelog]` 區段的所有選項。

如需 `[filelog]` 區段中支援的選項和組態範例的相關資訊，請參閱《使用 vRealize Log Insight 代理程式》中的主題〈從記錄檔收集事件〉。

建立資訊清單檔案

您可以複製代理程式組態檔的內容，並將其貼到新的 `TXT` 檔案中。若要識別動態路徑，請移除目錄路徑前面的前置「/」。

指定目錄路徑

[filelog] 區段中指定的目錄可以是來源的相對或絕對路徑。若要指定相對路徑，請勿在 Linux 下包含前置斜線，否則 vRealize Log Insight Importer 會將路徑視為絕對路徑。

若要在目錄索引鍵的值中表示名稱模式，您可以使用 * 和 ** 字元。

- 使用 * 做為單一目錄的預留位置。使用它來表示具有任意資料夾名稱的一個巢狀層級。例如，使用 `directory = log_folder_*` 可表示開頭為字串 `log_folder_` 的任何資料夾。
- 使用 ** 來表示具有任何資料夾名稱的任意巢狀層級。例如，您可以使用 `directory = **/log` 來表示來源目錄內在任意巢狀層級具有名稱 `log` 的資料夾。

vRealize Log Insight Importer 資訊清單檔案組態範例

範例 vRealize Log Insight Importer 資訊清單檔案提供參數組態的範例。

目錄索引鍵的值必須是來源的相對或絕對值。下列範例顯示如何從副檔名為 `.log` 的檔案收集記錄，這些檔案所在位置比來源目錄低兩個層級且最後一個資料夾的名稱以 `_log` 字串結尾。

```
[filelog|importer_test]
directory=*\*_log
include=*.log
event_marker=^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} [A-Z]{4} LOG
```

下列範例顯示如何從來源目錄（包括來源本身）的所有子資料夾收集副檔名為 `.log` 的所有檔案。

```
[filelog|sbimporter_test_channel]
directory = **
include = *.log
```

下列範例顯示如何從來源目錄（但不從子資料夾）中除副檔名為 `.ini` 檔案以外的所有檔案收集記錄檔。我們將檔案解譯為 UTF-16LE 編碼。

```
[filelog|quotes_channe3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

下列範例顯示如何從來源目錄（但不從子資料夾）中副檔名為 `.log` 的所有檔案收集記錄檔。事件的時間戳記在記錄檔中是使用一般記錄格式 (CLF) 剖析器進行剖析，並套用擷取的歷史時間戳記。CLF 剖析器剖析的記錄格式為 `2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract.`

```
[filelog|vcd-container-debug]
directory=
include=*.log
```

```
parser=vcd

[parser|vcd]
base_parser=clf
format=%{Y-%m-%d %H:%M:%S%f}t %M
```

執行 vRealize Log Insight Importer

執行 vRealize Log Insight Importer 以將歷史資料的離線記錄匯入至 vRealize Log Insight 伺服器。

必要條件

- 檢閱關於 [vRealize Log Insight Importer 資訊清單檔案](#)，並建立要與匯入工具搭配使用的資訊清單檔案。如需詳細資訊，請參閱 [vRealize Log Insight Importer 資訊清單檔案組態範例](#)。
- 如果使用 `honor_timestamp` 參數，請確認您具有適當的登入認證。
- 如果匯入支援服務包，請設定 `honor_timestamp` 以及使用者名稱和密碼。

程序

- 1 在命令提示字元中輸入下列命令以啟動 vRealize Log Insight Importer 工具。

```
/usr/bin/loginsight-importer.exe
```

- 2 在提示字元處輸入資訊清單檔案名稱。
- 3 定義組態參數，然後按 **Enter**。

`--source` 和 `--server` 為必要參數。

必要參數	說明
<code>--source <path></code>	指定支援服務包目錄的路徑或 zip、gzip、bzip、bzipped 或 tar 封存的路徑。該值會新增至所有傳送訊息做為 <code>bundle</code> 標籤的值。
<code>--server <hostname></code>	目的地伺服器主機名稱或 IP 位址。

選項	說明
<code>--port <port></code>	用於連線的連接埠。如果未設定，則會針對非 SSL 連線使用連接埠 9000，針對 SSL 連線使用連接埠 9543。
<code>--logdir <path></code>	指定記錄目錄的路徑。如果未設定此值，則在 Windows 上路徑為 <code>\$(LOCALAPPDATA)\VMware\Log Insight Importer\log</code> ，在 Linux 上為 <code>~/.loginsight-importer/log</code> 。
<code>--manifest <file-path></code>	指定資訊清單檔案 (.ini 格式) 的路徑。如果未設定此值，則會使用來源目錄中的 <code>importer.ini</code> 檔案。如果 <code>importer.ini</code> 檔案不存在或不在來源目錄中，vRealize Log Insight Importer 將套用預設 (硬式編碼) 資訊清單並收集所有 .txt 和 .log 檔案 (<code>include=*.log*;*.txt*</code>)，同時套用自動剖析器 (擷取時間戳記 + kvp)。
<code>--no_ssl</code>	不使用 SSL 進行連線。 不應針對已通過驗證的連線 (例如，如果已使用 <code>--honor_timestamp</code>) 設定此值。
<code>--ssl_ca_path <path></code>	受信任之根憑證服務包檔案的路徑。

選項	說明
<code>--tags <tags></code>	<p>為所有傳送事件設定標籤。例如 <code>--tags "{ \"tag1\" : \"value1\", \"tag2\": \"value2\"}"</code></p> <p>備註 標籤選項可以接受 <code>hostname</code> 做為標籤名稱。系統會使用命令列中 <code>hostname</code> 標籤的值 (而非傳送機器的 FQDN)，做為由 vRealize Log Insight Importer 擷取的所有事件之 <code>hostname</code> 欄位的值。這與資訊清單檔案和剖析器所擷取欄位中的標籤參數相反，其會忽略 <code>hostname</code> 欄位。</p> <p>記錄服務包名稱 (檔案名稱，或是目錄來源的目錄名稱) 會自動判定，並以 <code>bundle</code> 標籤的形式，新增至所有在擷取期間擷取自該特定服務包的所有記錄。此標籤可協助您區分 vRealize Log Insight 伺服器上的服務包。<code>bundle</code> 標籤會覆寫資訊清單檔案中具有相同名稱的標籤。但若其中一個標籤具有 <code>bundle</code> 名稱，則命令列標籤可能會覆寫該標籤。</p>
<code>--username <username ></code>	用於驗證的使用者名稱。如果已設定 <code>--honor_timestamp</code> ，則為必要項。
<code>--password <password></code>	用於驗證的密碼。如果已設定 <code>--honor_timestamp</code> ，則為必要項。使用者名稱/密碼配對會停用 vRealize Log Insight 伺服器上允許的時間偏離，從而可以匯入具有歷史時間戳記的資料。
<code>--honor_timestamp</code>	<p>套用擷取的時間戳記。設定的剖析器會從記錄項目擷取時間戳記，<code>--honor_timestamp</code> 會套用擷取的時間戳記。</p> <ul style="list-style-type: none"> ■ 如果使用設定的剖析器擷取時間戳記，則事件將套用該時間戳記。 ■ 如果記錄檔中存在不含所擷取時間戳記的事件，將會套用從同一記錄檔中前一個事件成功擷取的時間戳記。 ■ 如果在檔案中找不到時間戳記或未剖析時間戳記，將會套用記錄檔的 <code>MTIME</code> 做為時間戳記。 <p>備註 如果未提供資訊清單檔案，vRealize Log Insight Importer 使用的預設硬式編碼資訊清單將啟用自動記錄剖析器。在此情況下，如果使用 <code>--honor_timestamp</code> 參數，vRealize Log Insight Importer 會從記錄項目擷取時間戳記。</p>
<code>--debug_level <1 2></code>	增加記錄檔的詳細資訊層級。只應在疑難排解時進行這一變更。在執行一般作業時，不應使用此旗標。
<code>--help</code>	顯示說明並結束。

4 匯入完成後，在 Windows 或 Linux 上按 **Ctrl+C** 以結束工具。

結果

vRealize Log Insight Importer 會從參數中所指定的目錄擷取記錄項目。此時會顯示已處理檔案總數、已擷取的記錄訊息數、已傳送的記錄訊息數以及執行時間。

後續步驟

從 vRealize Log Insight 的 [互動式分析] 索引標籤中，您可以重新整理視圖以列出所匯入的記錄事件。如果您已匯入支援服務包並使用 `honor_timestamp`，則儀表板還應顯示隨時間變化的事件。