

# vRealize Log Insight Importer の使用

2019 年 11 月 28 日

vRealize Log Insight 8.0



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見およびご感想は、[docfeedback@vmware.com](mailto:docfeedback@vmware.com) までお送りください。

VMware, Inc.  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

ヴァイエムウェア株式会社  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2019 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

1	vRealize Log Insight Importer の使用	4
	vRealize Log Insight Importer のインストール	4
	vRealize Log Insight Importer をインストールする前に	5
	vRealize Log Insight Importer のインストール	5
	vRealize Log Insight Importer の実行	6
	vRealize Log Insight Importer のマニフェスト ファイルについて	6
	vRealize Log Insight Importer のマニフェスト ファイルの構成例	7
	vRealize Log Insight Importer の実行	8

# vRealize Log Insight Importer の使用

# 1

vRealize Log Insight Importer は、ローカル マシンの過去データのオフライン ログを vRealize Log Insight サーバにインポートするために使用するコマンドライン ユーティリティです。

過去に収集されたログをインポートする場合は、Importer を使用します。サポート バンドルとアーカイブ ログをインポートし、vRealize Log Insight または VMware 製品から収集したサポート バンドルからのログを分析することができます。

vRealize Log Insight Importer は次の機能を提供します。

- vRealize Log Insight Importer は取り込み API を介してデータを送信します。
- これは再帰的なディレクトリ収集を含むファイル ログ収集をサポートします。
- vRealize Log Insight Importer は、zip、tar、bzip、bzip2、または gz のアーカイブ ファイルからデータを読み取ることができます。7-Zip はサポートされません。
- ネストされた ZIP ファイルなど、ネストされたアーカイブから再帰的にデータを読み取ったり、アーカイブ内のディレクトリからデータを読み取るように指定できます。

この章には、次のトピックが含まれています。

- [vRealize Log Insight Importer のインストール](#)
- [vRealize Log Insight Importer の実行](#)

## vRealize Log Insight Importer のインストール

vRealize Log Insight Importer は、VMware ダウンロード サイトから入手可能なインストール パッケージからインストールします。各インストール パッケージには、Windows 用の MSI インストーラと、Linux 用の POSIX インストール パッケージ (RPM、DEB および BIN) が含まれています。

- [vRealize Log Insight Importer をインストールする前に](#)  
Importer をインストールする前に、要件を確認し、Importer の動作について理解してください。
- [vRealize Log Insight Importer のインストール](#)  
vRealize Log Insight Importer は Windows および Linux にインストールできます。また、vRealize Log Insight Importer を vRealize Log Insight サーバにインストールして、サーバから実行することもできます。

## vRealize Log Insight Importer をインストールする前に

Importer をインストールする前に、要件を確認し、Importer の動作について理解してください。

インストールの前に、アーカイブされたデータが保存される NFS サーバに vRealize Log Insight がアクセスできることを確認します。ネットワーク障害または NFS サーバ上のエラーのために NFS サーバにアクセスできなくなると、アーカイブされたデータのインポートが失敗することがあります。

取り込み中にバンドルからログを抽出する際、ログバンドル名は自動的に決定され、抽出されたすべてのログにバンドルタグとして追加されます。タグ名はログのファイル名、またはディレクトリソースの場合はディレクトリ名です。バンドルタグによって vRealize Log Insight サーバ上のバンドルを差別化します。

このタグは、マニフェストファイルで指定された同じ名前のすべてのタグをオーバーライドします。また、このタグは、同じ名前を使用するコマンドラインタグによってオーバーライドすることができます。

Importer を使用する場合は、次の動作に注意します。

- vRealize Log Insight Importer は vRealize Log Insight 仮想アプライアンス上の利用可能なディスク容量をチェックしません。したがって、仮想アプライアンスのディスク容量が不足しているとアーカイブされたログのインポートは失敗することがあります。
- vRealize Log Insight はログのインポート中に進捗情報を表示しません。アーカイブされたデータのインポートの進行中、コンソールの出力からはインポート終了までの残り時間や、インポート済みのデータの量を知ることができません。

### サポートされているオペレーティングシステム

vRealize Log Insight Importer は、次のオペレーティングシステムでサポートされます。

- Windows 32 ビットおよび 64 ビット
- Linux 32 ビットおよび 64 ビット

Linux バージョンは、Apple の Macintosh システムでは実行されません。

## vRealize Log Insight Importer のインストール

vRealize Log Insight Importer は Windows および Linux にインストールできます。また、vRealize Log Insight Importer を vRealize Log Insight サーバにインストールして、サーバから実行することもできます。

vRealize Log Insight Importer をインストールするときに、いくつかの VMware 製品マニフェストファイルもインストールされます。vRealize Log Insight Importer を実行するときに、これらのファイルを使用するか目的に合わせて変更することができます。これらのマニフェストファイルは、Windows の場合は C:\Program Files (x86)\VMware\Log Insight Importer\Manifests にあり、Linux の場合は /usr/lib/loginsight-importer/manifests にあります。

.bin パッケージをアンインストールした場合は、/usr/bin/loginsight\_importer シンボリックリンクも削除します。

### 前提条件

- [VMware ダウンロード](#) サイトにアクセスして vRealize Log Insight Importer をダウンロードできることを確認します。

## 手順

- 1 [VMware ダウンロード](#) サイトから vRealize Log Insight Importer インストール パッケージをダウンロードします。

各インストール パッケージには、Windows 用の MSI インストーラと、Linux 用の POSIX インストール パッケージ (RPM、DEB および BIN) が含まれています。

- 2 システムにツールをインストールします。

インストール後に、Windows では Importer のインストール ディレクトリが PATH 環境変数に追加され、Linux では `loginsight-importer` 実行ファイルへのシンボリックリンクが `/usr/bin/` に追加されます。このため、パス プリフィックスを指定しなくても、クライアントがシェルから `loginsight-importer` を呼び出すことができます。

vRealize Log Insight Importer ツールは、次の場所にインストールされます。

オペレーティング システム	ファイル名	インストール場所
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

## vRealize Log Insight Importer の実行

インポータを実行するときは、マニフェスト ファイルを含める必要があります。マニフェスト ファイルは、ログの形式、インポートするデータの場所、およびソースとターゲットの情報を提供します。

- [vRealize Log Insight Importer のマニフェスト ファイルについて](#)

vRealize Log Insight Importer は、マニフェスト構成ファイルを使用してログ フォーマットを決定し、インポートするデータの場所を指定します。マニフェスト ファイルは、`liagent.ini` 構成ファイルに似た形式を持ち、その構造も類似しています。

- [vRealize Log Insight Importer のマニフェスト ファイルの構成例](#)

サンプルの vRealize Log Insight Importer マニフェスト ファイルに、パラメータ構成の例を示します。

- [vRealize Log Insight Importer の実行](#)

履歴データのオフライン ログを vRealize Log Insight サーバにインポートするには、vRealize Log Insight Importer を実行します。

## vRealize Log Insight Importer のマニフェスト ファイルについて

vRealize Log Insight Importer は、マニフェスト構成ファイルを使用してログ フォーマットを決定し、インポートするデータの場所を指定します。マニフェスト ファイルは、`liagent.ini` 構成ファイルに似た形式を持ち、その構造も類似しています。

オプションで、任意のログ ファイルをインポートするために、独自のマニフェスト ファイルを作成できます。ファイルを作成することのメリットの 1 つは、データ ファイルへの絶対パスを知る必要がないということです。

マニフェスト ファイルを作成しない場合、vRealize Log Insight Importer では、デフォルトのマニフェスト ファイルが使用されます。デフォルトのマニフェスト ファイルは、すべての `.txt` ファイルと `.log` ファイルを収集し (`include=*.log*;*.txt*`)、抽出されたログに自動パーサ (タイムスタンプとキー/値ペアを抽出) を適用します。

`liagent.ini` 構成ファイルをマニフェスト ファイルとして使用すると、vRealize Log Insight Importer は `[filelog]` セクションのみをマニフェストとして抽出します。`[filelog]` セクションのすべてのオプションが vRealize Log Insight Importer でサポートされます。

`[filelog]` セクションでサポートされているオプションと設定例については、『vRealize Log Insight エージェントの操作』の「ログ ファイルからのイベントの収集」を参照してください。

## マニフェスト ファイルを作成するには

エージェント構成ファイルの内容をコピーして、新しい TXT ファイルに貼り付けることができます。動的パスを識別するには、ディレクトリ パスの先頭の「/」を削除します。

## ディレクトリ パスの指定

`[filelog]` セクションのディレクトリは、ソースに対する相対パスまたは絶対パスとして指定できます。相対パスを指定する場合、Linux では先頭にスラッシュを含めないでください。先頭にスラッシュがあると、そのパスは vRealize Log Insight Importer で絶対パスとして扱われます。

ディレクトリ キーの値での名前のパターンを示すため、`*` 文字と `**` 文字を使用できます。

- `*` は、単一ディレクトリを表すプレースホルダとして使用できます。これは、任意のフォルダ名を持つ 1 つのネスト レベルを示すために使用します。たとえば、`directory = log_folder_*` は、文字列 `log_folder_` で始まる任意のフォルダを示します。
- `**` は、任意のフォルダ名を持つ、任意のネスト レベルを示すために使用します。たとえば、`directory = **/log` は、ソース ディレクトリ内の任意のネスト レベルにある、`log` という名前の任意のフォルダを示します。

## vRealize Log Insight Importer のマニフェスト ファイルの構成例

サンプルの vRealize Log Insight Importer マニフェスト ファイルに、パラメータ構成の例を示します。

ディレクトリ キーの値は、ソースに対する相対パスとして指定するか、絶対パスとして指定する必要があります。次の例は、ソース ディレクトリより 2 つ下のレベルにあり、最終フォルダの名前が文字列 `_log` で終わるディレクトリにある、拡張子が `.log` のファイルからログを収集する方法を示しています。

```
[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
```

次の例は、ソース ディレクトリのすべてのサブフォルダ (ソース自体を含む) から、拡張子が `.log` のすべてのファイルを収集する方法を示しています。

```
[filelog|sbimporter_test_channel]
directory = **
```

```
include = *.log
```

次の例は、ソース ディレクトリ（サブフォルダは対象外）内にあるファイルのうち、拡張子が `.ini` のファイルを除いたすべてのファイルからログを収集する方法を示しています。ここでは、ファイルのエンコーディングを UTF-16LE として解釈します。

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

次の例は、ソース ディレクトリ（サブフォルダは対象外）内にあるファイルのうち、拡張子が `.log` のすべてのファイルからログを収集する方法を示しています。ログ ファイル内のイベントのタイムスタンプは、共通ログフォーマット (CLF) パーサを使用して解析され、抽出された過去のタイムスタンプが適用されます。CLF パーサで解析されるログは、`2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract` の形式になります。

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

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

## vRealize Log Insight Importer の実行

履歴データのオフライン ログを vRealize Log Insight サーバにインポートするには、vRealize Log Insight Importer を実行します。

### 前提条件

- [vRealize Log Insight Importer のマニフェスト ファイルについて](#) を確認して、インポータに使用するマニフェスト ファイルを作成します。詳細については、[vRealize Log Insight Importer のマニフェスト ファイルの構成例](#)を参照してください。
- `honor_timestamp` パラメータを使用する場合は、適切なログイン認証情報があることを確認します。
- サポート バンドルをインポートする場合は、`honor_timestamp` と、ユーザー名およびパスワードを設定します。

## 手順

- 1 次のコマンドをコマンド プロンプトで入力し、vRealize Log Insight Importer ツールを起動します。

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

- 2 プロンプトが表示されたら、マニフェスト ファイル名を入力します。
- 3 構成パラメータを定義して [Enter] キーを押します。

--source および --server パラメータは必須です。

必須パラメータ	説明
--source <path>	サポート バンドル ディレクトリへのパス、または zip、gzip、bzip、bzip2、または tar アーカイブへのパスを指定します。この値は、bundle タグの値としてすべての送信メッセージに追加されます。
--server <hostname>	ターゲット サーバのホスト名または IP アドレスです。

オプション	説明
--port <port>	接続用のポートです。設定されていない場合、SSL 以外の接続にはポート 9000 が使用され、SSL 接続にはポート 9543 が使用されます。
--logdir <path>	ログ ディレクトリへのパスを指定します。設定されていない場合、パスは、Windows では \$(LOCALAPPDATA)\VMware\Log Insight Importer\log になり、Linux では ~/.loginsight-importer/log になります。
--manifest <file-path>	マニフェスト ファイル (.ini 形式) へのパスを指定します。設定されていない場合、ソース ディレクトリ内の importer.ini ファイルが使用されます。importer.ini ファイルがない場合や送信元ディレクトリ内に見つからない場合、vRealize Log Insight Importer は、デフォルトの (ハードコードされた) マニフェストを適用して、すべての .txt ファイルと .log ファイルを収集し (include=*.log*;*.txt*)、自動パーサ (タイムスタンプとキー/値ペアを抽出) を適用します。
--no_ssl	接続に SSL を使用しません。 認証された接続 (--honor_timestamp が使用されている場合など) では、設定しないようにします。
--ssl_ca_path <path>	信頼済みルート証明書バンドル ファイルへのパスです。
--tags <tags>	すべての送信イベントにタグを設定します。例: --tags "{ \"tag1\" : \"value1\", \"tag2\":\"value2\"}"  <b>注:</b> tags オプションでは、タグ名として hostname を指定できます。コマンドラインで指定した hostname タグの値は、vRealize Log Insight Importer で抽出された全イベントの hostname フィールドの値として、送信マシンの FQDN の代わりに使用されます。これは、マニフェスト ファイル内の tags パラメータや、パーサによって抽出されるフィールドとは反対の働きで、これらのパラメータやフィールドでは、hostname フィールドは無視されます。  ファイル名またはディレクトリ名 (ディレクトリ ソースの場合) のログ バンドル名は自動的に決定され、取り込み中にその特定のバンドルから抽出されたすべてのログにバンドルタグとして追加されます。このタグによって、vRealize Log Insight サーバのバンドルを差別化することができます。バンドル タグは、タグをマニフェスト ファイルの同じ名前前でオーバーライドします。ただし、バンドル名のタグがある場合は、コマンドライン タグによってオーバーライドすることができます。
--username <username >	認証用のユーザー名です。--honor_timestamp が設定されている場合は必須です。
--password <password>	認証用のパスワードです。--honor_timestamp が設定されている場合は必須です。ユーザー名とパスワードのペアにより、vRealize Log Insight サーバで許可される時間の誤差が無効になるため、過去のタイムスタンプを持ったデータのインポートが可能になります。

オプション	説明
<code>--honor_timestamp</code>	<p>抽出されたタイムスタンプを適用します。構成済みのパーサはログ エントリからタイムスタンプを抽出し、<code>--honor_timestamp</code> が抽出されたタイムスタンプを適用します。</p> <ul style="list-style-type: none"> <li>■ タイムスタンプが構成済みのパーサを使用して抽出された場合、イベントにはそのタイムスタンプが適用されます。</li> <li>■ 抽出したタイムスタンプを持たないイベントがログ ファイル内にある場合は、同じログ ファイル内で以前のイベントから正常に抽出されたタイムスタンプが適用されます。</li> <li>■ ファイル内にタイムスタンプが見つからないまたは解析されない場合には、ログ ファイルの MTIME がタイムスタンプとして適用されます。</li> </ul> <p><b>注：</b> マニフェスト ファイルが指定されなかった場合、vRealize Log Insight Importer が使用するデフォルトのハードコーディングされたマニフェストで自動ログ パーサーが有効になります。この場合、<code>--honor_timestamp</code> パラメータが使用されていれば vRealize Log Insight Importer はログ エントリからタイムスタンプを抽出します。</p>
<code>--debug_level &lt;1 2&gt;</code>	ログ ファイルの詳細度のレベルを増やします。これは、トラブルシューティングの場合にのみ変更します。通常の運用では、このフラグは使用しないようにします。
<code>--help</code>	ヘルプを表示して終了します。

4 インポートが完了したら、Windows または Linux で [Ctrl+C] を押してツールを終了します。

vRealize Log Insight Importer が、パラメータで指定されたディレクトリからログ エントリを抽出します。処理されたファイル数、抽出されたログ メッセージ数、送信されたログ メッセージ数、および処理時間それぞれの合計が表示されます。

#### 次のステップ

vRealize Log Insight の [インタラクティブ分析] タブで、ビューを更新してインポートされたログ イベントの一覧を表示できます。サポート バンドルをインポートして `honor_timestamp` を使用した場合は、ダッシュボードにも一定期間イベントが表示されるはずです。