

Verwenden von vRealize Log Insight Importer

14. April 2020

vRealize Log Insight 8.1



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Verwenden von vRealize Log Insight Importer	4
	Installieren von vRealize Log Insight Importer	4
	Vor der Installation von vRealize Log Insight Importer	5
	Installieren von vRealize Log Insight Importer	5
	Ausführen von vRealize Log Insight Importer	6
	Informationen zur vRealize Log Insight Importer-Manifestdatei	7
	Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien	8
	Ausführen von vRealize Log Insight Importer	9

Verwenden von vRealize Log Insight Importer

1

Bei vRealize Log Insight Importer handelt es sich um ein Befehlszeilendienstprogramm, das zum Importieren der Offline-Protokolle von Verlaufsdaten aus lokalen Geräten zum vRealize Log Insight-Server verwendet wird.

Verwenden Sie den Importer, wenn Sie Protokolle importieren möchten, die in der Vergangenheit gesammelt wurden. Sie können Support-Pakete und archivierte Protokolle importieren und Protokolle von Support-Paketen aus vRealize Log Insight oder aus beliebigen VMware-Produkten analysieren.

vRealize Log Insight Importer enthält die im Folgenden aufgeführten Funktionen.

- vRealize Log Insight Importer sendet Daten über die Ingestion-API.
- Die Erfassung der Dateiprotokolle einschließlich der rekursiven Verzeichniserfassung wird unterstützt.
- Importer ist in der Lage, Daten aus ZIP-, TAR-, BZIP-, BZIP2- und GZ-Archivdateien zu lesen. 7-Zip wird nicht unterstützt.
- Sie haben die Möglichkeit, die Daten anzugeben, die rekursiv aus einem verschachtelten Archiv gelesen werden (wie z. B. eine verschachtelte ZIP-Datei) oder ein Verzeichnis in einem Archiv festzulegen.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von vRealize Log Insight Importer](#)
- [Ausführen von vRealize Log Insight Importer](#)

Installieren von vRealize Log Insight Importer

Sie installieren vRealize Log Insight Importer aus einem Installationspaket, das über die VMware-Download-Website erhältlich ist. Das Installationspaket enthält das MSI-Installationsprogramm für Windows und POSIX-Installationspakete (RPM, DEB und BIN) für Linux.

- [Vor der Installation von vRealize Log Insight Importer](#)
Überprüfen Sie die Anforderungen und machen Sie sich mit dem Verhalten von Importer vertraut, bevor Sie mit der Installation beginnen.

■ Installieren von vRealize Log Insight Importer

Sie können vRealize Log Insight Importer auf Windows oder Linux installieren. Sie können den vRealize Log Insight Importer auch auf einem vRealize Log Insight-Server installieren und über den Server ausführen.

Vor der Installation von vRealize Log Insight Importer

Überprüfen Sie die Anforderungen und machen Sie sich mit dem Verhalten von Importer vertraut, bevor Sie mit der Installation beginnen.

Vor der Installation müssen Sie sicherstellen, dass vRealize Log Insight Zugriff auf den NFS-Server hat, auf dem die archivierten Daten gespeichert sind. Wenn aufgrund eines Netzwerkausfalls oder Fehlers auf dem NFS-Server der Zugriff auf den NFS-Server nicht möglich ist, kann der Import von archivierten Daten fehlschlagen.

Wenn im Rahmen der Erfassung Protokolle aus einem Paket extrahiert werden, wird automatisch ein Name für das Protokollpaket festgelegt und als Paket-Tag allen extrahierten Protokollen hinzugefügt. Der Tag-Name ist entweder der Dateiname des Protokolls oder bei Verzeichnisquellen der Name des Verzeichnisses. Paket-Tags unterscheiden Pakete auf einem vRealize Log Insight-Server.

Dieses Tag überschreibt alle Tags mit demselben Namen, die in der Manifestdatei angegeben sind. Das Tag kann von Befehlszeilen-Tags, die denselben Namen verwenden, überschrieben werden.

Bei der Verwendung von Importer ist Folgendes zu beachten:

- vRealize Log Insight Importer überprüft nicht den verfügbaren Festplattenspeicher in der virtuellen vRealize Log Insight-Appliance. Deshalb schlägt der Import von archivierten Protokollen möglicherweise fehl, wenn für die virtuelle Appliance nicht ausreichend Speicherplatz verfügbar ist.
- Beim Import von Protokollen werden von vRealize Log Insight keine Fortschrittsinformationen dargestellt. Während der Import von archivierten Daten durchgeführt wird, können Sie anhand der Konsolenausgabe nicht ableiten, wie viel Zeit übrigbleibt, bis der Importvorgang abgeschlossen wird, oder wie groß die bereits importierte Datenmenge ist.

Unterstützte Betriebssysteme

vRealize Log Insight Importer wird bei folgenden Betriebssystemen unterstützt:

- Windows 32-Bit und 64-Bit
- Linux 32-Bit und 64-Bit

Die Linux-Version kann nicht auf einem Apple Macintosh-System ausgeführt werden.

Installieren von vRealize Log Insight Importer

Sie können vRealize Log Insight Importer auf Windows oder Linux installieren. Sie können den vRealize Log Insight Importer auch auf einem vRealize Log Insight-Server installieren und über den Server ausführen.

Bei der Installation von vRealize Log Insight Importer werden auch eine Reihe von Manifestdateien für VMware-Produkte installiert. Sie können diese Dateien bei der Ausführung von vRealize Log Insight Importer verwenden oder für Ihre Bedürfnisse modifizieren. Die Manifestdateien befinden sich in Windows unter `C:\Program Files (x86)\VMware\Log Insight Importer\Manifests` und in Linux unter `/usr/lib/loginsight-importer/manifests`.

Wenn Sie das Paket `.bin` deinstallieren, löschen Sie auch den symbolischen Link `/usr/bin/loginsight_importer`.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf die [VMware-Download-Website](#) zugreifen können, um den vRealize Log Insight Importer herunterzuladen.

Verfahren

- 1 Laden Sie das vRealize Log Insight Importer-Installationspaket von der [VMware-Download-Website](#) herunter.

Das Installationspaket enthält das MSI-Installationsprogramm für Windows und POSIX-Installationspakete (RPM, DEB und BIN) für Linux.

- 2 Installieren Sie das Tool auf Ihrem System.

Nach der Installation wird auf Windows das Importer-Installationsverzeichnis zur Umgebungsvariable „PATH“ hinzugefügt, und auf Linux wird ein symbolischer Link zur ausführbaren Datei `loginsight-importer` zu `/usr/bin/` hinzugefügt. Dadurch kann der Client `loginsight-importer` von der Shell aus aufrufen, ohne dafür das Präfix eines Pfads angeben zu müssen.

Das vRealize Log Insight Importer-Tool wird an den folgenden Speicherorten installiert:

Betriebssystem	Dateiname	Speicherort der Installation
Windows	<code>loginsight-importer.exe</code>	<code>C:\Programme (x86)\VMware\Log Insight Importer</code>
Linux	<code>loginsight-importer</code>	<code>/usr/lib/loginsight-importer</code>

Ausführen von vRealize Log Insight Importer

Wenn Sie den Importer ausführen, müssen Sie eine Manifestdatei einbeziehen. Die Manifestdatei enthält Informationen über das Protokollformat, den Speicherort der zu importierenden Daten sowie Quell- und Zielinformationen.

- [Informationen zur vRealize Log Insight Importer-Manifestdatei](#)

vRealize Log Insight Importer verwendet eine Manifestkonfigurationsdatei, um das Protokollformat zu bestimmen und den Speicherort der zu importierenden Daten anzugeben. Die Manifestdatei hat dasselbe Format wie die Konfigurationsdatei `liagent.ini` und weist eine ähnliche Struktur auf.

- **Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien**

Die Beispiele für vRealize Log Insight Importer-Manifestdateien dienen als Beispiele für die Konfiguration von Parametern.

- **Ausführen von vRealize Log Insight Importer**

Führen Sie vRealize Log Insight Importer für den Import von Offline-Protokollen von Verlaufsdaten auf den vRealize Log Insight-Server aus.

Informationen zur vRealize Log Insight Importer-Manifestdatei

vRealize Log Insight Importer verwendet eine Manifestkonfigurationsdatei, um das Protokollformat zu bestimmen und den Speicherort der zu importierenden Daten anzugeben. Die Manifestdatei hat dasselbe Format wie die Konfigurationsdatei `liagent.ini` und weist eine ähnliche Struktur auf.

Optional können Sie Ihre eigenen Manifestdateien erstellen, um beliebige Protokolldateien zu importieren. Ein Vorteil der Erstellung einer solchen Datei ist, dass Sie den absoluten Pfad zu den Datendateien nicht kennen müssen.

Wenn Sie keine Manifestdatei erstellen, verwendet vRealize Log Insight Importer das Standardmanifest, das alle Dateien des Formats `.txt` und `.log` (`include=*.log*;*.txt*`) erfasst und den Auto-Parser (extrahiert Zeitstempel und Schlüssel/Wert-Paar) auf die extrahierten Protokolle anwendet.

Wenn die Konfigurationsdatei `liagent.ini` als Manifestdatei verwendet wird, extrahiert vRealize Log Insight Importer nur die Abschnitte `[filelog]` als Manifest. Alle Optionen für den Abschnitt `[filelog]` werden in vRealize Log Insight Importer unterstützt.

Informationen zu den im Abschnitt `[filelog]` unterstützten Optionen und Konfigurationsbeispielen finden Sie im Thema „Erfassen von Ereignissen aus einer Protokolldatei“ im Abschnitt *Arbeiten mit vRealize Log Insight-Agenten*.

Erstellen einer Manifestdatei

Sie können den Inhalt der Agentenkonfigurationsdatei kopieren und in eine neue TXT-Datei einfügen. Entfernen Sie zum Ermitteln eines dynamischen Pfads den Schrägstrich am Anfang vor dem Verzeichnispfad.

Angeben des Verzeichnispfads

Das im Abschnitt `[filelog]` angegebene Verzeichnis kann entweder relativ zur Quelle oder absolut sein. Fügen Sie zum Angeben des relativen Pfads unter Linux nicht den Schrägstrich am Anfang ein, da vRealize Log Insight Importer den Pfad ansonsten als absolut behandelt.

Um Namensmuster im Wert des Verzeichnisschlüssels anzugeben, können Sie die Zeichen `*` und `**` verwenden.

- Verwenden Sie `*` als Platzhalter für ein einzelnes Verzeichnis. Verwenden Sie dieses, um auf eine Verschachtelungsebene mit einem beliebigen Ordner hinzuweisen. Beispielsweise können Sie `directory = log_folder_*` verwenden, um alle mit der Zeichenfolge `log_folder_` beginnende Ordner anzuzeigen.

- Verwenden Sie **, um auf eine beliebige Verschachtelungsebene mit einem Ordner hinzuweisen. Sie können z. B. `directory = **/log` verwenden, um einen Ordner mit dem Namen `log` auf einer beliebigen Verschachtelungsebene innerhalb des Quellverzeichnisses anzugeben.

Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien

Die Beispiele für vRealize Log Insight Importer-Manifestdateien dienen als Beispiele für die Konfiguration von Parametern.

Der Wert des Verzeichnisschlüssels muss entweder relativ zur Quelle oder absolut sein. Im folgenden Beispiel wird dargestellt, wie Protokolle aus Dateien mit einer `.log`-Erweiterung erfasst werden, welche sich zwei Ebenen unter dem Quellverzeichnis befinden, und bei denen der Name des letzten Ordners mit der Zeichenfolge `_log` endet.

```
[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
```

Im folgenden Beispiel wird dargestellt, wie alle Dateien mit der `.log`-Erweiterung aus allen Unterordnern des Quellverzeichnisses einschließlich der Quelle selbst erfasst werden.

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

Im folgenden Beispiel wird dargestellt, wie Protokolle aus allen Dateien im Quellverzeichnis (nicht jedoch aus den Unterordnern) erfasst werden, ausgenommen die Dateien, die über eine `.ini`-Erweiterung verfügen. Dateien werden als UTF-16LE-codiert interpretiert.

```
[filelog|quotes_channel3]
directory=
charset=UTF-16LE
exclude=*.ini
tags={"Provider" : "Apache"}
```

Im folgenden Beispiel wird dargestellt, wie Protokolle aus allen Dateien mit der Erweiterung `.log` im Quellverzeichnis (nicht jedoch aus den Unterordnern) erfasst werden. Der Zeitstempel der Ereignisse wird in der Protokolldatei unter Verwendung des Parser im Common Log Format (CLF-Parser) analysiert, und es wird der extrahierte Verlaufszeitstempel angewendet. Das mit dem CLF-Parser analysierte Protokollformat lautet `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
```

Ausführen von vRealize Log Insight Importer

Führen Sie vRealize Log Insight Importer für den Import von Offline-Protokollen von Verlaufsdaten auf den vRealize Log Insight-Server aus.

Voraussetzungen

- Schlagen Sie unter [Informationen zur vRealize Log Insight Importer-Manifestdatei](#) nach und erstellen Sie eine Manifestdatei, die Sie mit dem Importfunktion-Dienstprogramm verwenden. Weitere Informationen finden Sie unter [Beispiele für die Konfiguration von vRealize Log Insight Importer-Manifestdateien](#).
- Stellen Sie bei der Verwendung des Parameters `honor_timestamp` sicher, dass Sie über die entsprechenden Anmeldedaten verfügen.
- Wenn Sie ein Support-Paket importieren, konfigurieren Sie den Parameter `honor_timestamp` sowie den Benutzernamen und das Kennwort.

Verfahren

- 1 Starten Sie das Tool vRealize Log Insight Importer, indem Sie den folgenden Befehl in eine Eingabeaufforderung eingeben.

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

- 2 Geben Sie an der Eingabeaufforderung den Namen der Manifestdatei ein.
- 3 Legen Sie die Konfigurationsparameter fest und drücken Sie die **Eingabetaste**.

Die Parameter `--source` und `--server` sind erforderlich.

Erforderliche Parameter	Beschreibung
<code>--source <path></code>	Legt den Pfad zu einem Support-Paket-Verzeichnis oder zu Archivdateien im Format ZIP, GZIP, BZIP, BZIP2 oder TAR fest. Der Wert wird zu allen gesendeten Nachrichten als Wert des <code>bundle-</code> Tags hinzugefügt.
<code>--server <hostname></code>	Hostname oder IP-Adresse des Zielservers.

Optionen	Beschreibung
<code>--port <port></code>	Port für die Verbindung. Wenn kein Wert angegeben ist, wird Port 9000 für Verbindungen ohne SSL und Port 9543 für SSL-Verbindungen verwendet.
<code>--logdir <path></code>	Gibt den Pfad zum Protokollverzeichnis an. Wenn dafür kein Wert angegeben ist, lautet der Pfad für Windows <code>\$(LOCALAPPDATA)\VMware\Log Insight Importer\log</code> und für Linux <code>~/.loginsight-importer/log</code> .

Optionen	Beschreibung
<code>--manifest <file-path></code>	Gibt den Pfad zur Manifestdatei an (INI-Format). Wenn dafür kein Wert angegeben ist, wird die Datei <code>importer.ini</code> im Quellverzeichnis verwendet. Wenn die Datei <code>importer.ini</code> im Quellverzeichnis nicht vorhanden ist oder nicht gefunden werden kann, wendet vRealize Log Insight Importer das (hartcodierte) Standardmanifest an und erfasst alle Dateien des Formats <code>.txt</code> und <code>.log</code> (<code>include=*.log;*.txt*</code>), und wendet zudem den Auto-Parser an (extrahiert Zeitstempel und Schlüssel/Wert-Paar).
<code>--no_ssl</code>	Verwenden Sie SSL nicht für Verbindungen. Dieser Wert darf nicht für authentifizierte Verbindungen festgelegt werden (wenn z. B. <code>--honor_timestamp</code> verwendet wird).
<code>--ssl_ca_path <path></code>	Pfad zur Paketdatei der vertrauenswürdigen Stammzertifikate.
<code>--tags <tags></code>	Legen Sie Tags für alle gesendeten Ereignisse fest. Beispiel: <code>--tags "{ \"tag1\" : \"value1\", \"tag2\":\"value2\"}"</code> Hinweis Die Tags-Option kann <code>hostname</code> als Tagname akzeptieren. Als Wert für das <code>hostname</code> -Feld für alle durch vRealize Log Insight Importer extrahierten Ereignisse wird der Wert des <code>hostname</code> -Tags aus der Befehlszeile anstelle des FQDN der sendenden Maschine verwendet. Dies ist das Gegenteil von Tags-Parametern in der Manifestdatei und durch Parser extrahierte Felder, welche das <code>hostname</code> -Feld ignorieren. Der Name eines Protokollpakets, der entweder ein Dateiname oder bei Verzeichnisquellen ein Verzeichnisname ist, wird automatisch festgelegt und während der Aufnahme als Paket-Tag allen Protokollen hinzugefügt, die aus dem jeweiligen Paket extrahiert wurden. Mit diesem Tag können Sie Pakete auf dem VMware vRealize® Log Insight-Server voneinander unterscheiden. Paket-Tags überschreiben Tags mit demselben Namen aus einer Manifestdatei. Sie können jedoch durch Befehlszeilen-Tags überschrieben werden, wenn einer namens Paket vorhanden ist.
<code>--username <username ></code>	Benutzername für die Authentifizierung. Erforderlich, wenn <code>--honor_timestamp</code> festgelegt ist.
<code>--password <password></code>	Kennwort für die Authentifizierung. Erforderlich, wenn <code>--honor_timestamp</code> festgelegt ist. Das Benutzername/Kennwort-Paar deaktiviert die zulässige Zeitabweichung auf dem vRealize Log Insight-Server, um das Importieren von Daten mit einem historischen Zeitstempel zu ermöglichen.
<code>--honor_timestamp</code>	Wendet den extrahierten Zeitstempel an. Die konfigurierten Parser extrahieren den Zeitstempel aus den Protokolleinträgen, und <code>--honor_timestamp</code> wendet den extrahierten Zeitstempel an. <ul style="list-style-type: none"> ■ Wenn der Zeitstempel mithilfe von konfigurierten Parsern extrahiert wird, wird dieser Zeitstempel auf Ereignisse angewendet. ■ Wenn sich in der Protokolldatei ein Ereignis ohne extrahierten Zeitstempel befindet, wird der erfolgreich extrahierte Zeitstempel aus dem vorherigen Ereignis in derselben Protokolldatei angewendet. ■ Wenn in der Datei kein Zeitstempel gefunden oder analysiert wird, wird die MTIME der Protokolldatei als Zeitstempel angewendet. Hinweis Wenn keine Manifestdatei bereitgestellt wurde, ist für das hartcodierte Standard-Manifest, das von vRealize Log Insight Importer verwendet wird, der automatische Protokollparser aktiviert. In diesem Fall extrahiert vRealize Log Insight Importer den Zeitstempel aus den Protokolleinträgen, wenn der Parameter <code>--honor_timestamp</code> verwendet wird.
<code>--debug_level <1 2></code>	Erhöht den Ausführlichkeitsgrad der Protokolldatei. Dies sollte nur im Rahmen einer Fehlerbehebung geändert werden. Im Normalbetrieb sollte dieses Flag nicht verwendet werden.
<code>--help</code>	Zeigen Sie Hilfe an und beenden Sie das Programm.

- 4 Drücken Sie nach Abschluss des Importvorgangs unter Windows oder Linux **Strg + C**, um das Tool zu beenden.

Ergebnisse

vRealize Log Insight Importer extrahiert die Protokolleinträge aus den in den Parametern angegebenen Verzeichnissen. Es werden die Gesamtanzahl der verarbeiteten Dateien, der extrahierten Protokollmeldungen, der gesendeten Protokollmeldungen sowie die Laufzeit angezeigt.

Nächste Schritte

Über die Registerkarte „Interaktive Analyse“ in vRealize Log Insight können Sie die Ansicht für die Auflistung der importierten Protokollereignisse aktualisieren. Wenn Sie ein Support-Paket importiert und den Parameter `honor_timestamp` verwendet haben, sollte das Dashboard auch die Ereignisse im Zeitverlauf anzeigen.