

使用 vRealize Log Insight 导入程序

2020 年 10 月 06 日

vRealize Log Insight 8.2

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

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

**威睿信息技术（中国）有
限公司**
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

1	使用 vRealize Log Insight Importer	4
	安装 vRealize Log Insight Importer	4
	在安装 vRealize Log Insight Importer 之前	5
	安装 vRealize Log Insight Importer	5
	运行 vRealize Log Insight Importer	6
	关于 vRealize Log Insight Importer 清单文件	6
	vRealize Log Insight Importer 清单文件配置示例	7
	运行 vRealize Log Insight Importer	8

使用 vRealize Log Insight Importer

1

《使用 vRealize Log Insight Importer》提供了有关安装和运行 vRealize Log Insight Importer 的信息。

vRealize Log Insight Importer 是一个命令行实用程序，用于将历史数据的脱机日志从本地计算机导入到 vRealize Log Insight 服务器。

如果您希望导入过去收集的日志，可使用该导入程序。您可以导入支持包和存档的日志，并分析从 vRealize Log Insight 或任何 VMware 产品收集的支持包中的日志。

vRealize Log Insight Importer 包含以下特性和功能。

- vRealize Log Insight Importer 通过数据获取 API 发送数据。
- 它支持文件日志收集，包括递归目录收集。
- 导入程序可以从 zip、tar、bzip、bzip2 或 gz 存档文件中读取数据。不支持 7-Zip。
- 您可以指定从嵌套的存档（如嵌套的 ZIP 文件）或者从存档中的目录递归读取数据。

本章讨论了以下主题：

- [安装 vRealize Log Insight Importer](#)
- [运行 vRealize Log Insight Importer](#)

安装 vRealize Log Insight Importer

可以使用从 VMware 下载站点获取的安装软件包安装 vRealize Log Insight 导入程序。安装软件包中包含适用于 Windows 的 MSI 安装程序，以及适用于 Linux 的 POSIX 安装软件包（RPM、DEB 和 BIN）。

- [在安装 vRealize Log Insight Importer 之前](#)

在安装导入程序之前，请先查看要求，并了解导入程序的行为。

- [安装 vRealize Log Insight Importer](#)

可以在 Windows 和 Linux 上安装 vRealize Log Insight Importer。也可以将 vRealize Log Insight Importer 安装在 vRealize Log Insight 服务器上并从服务器上运行。

在安装 vRealize Log Insight Importer 之前

在安装导入程序之前，请先查看要求，并了解导入程序的行为。

在安装之前，必须先确保 vRealize Log Insight 能够访问存储存档数据的 NFS 服务器。如果 NFS 服务器由于网络故障或 NFS 服务器上的错误而变得不可访问，则存档数据的导入可能会失败。

在载入期间从包中提取日志时，将会自动确定日志包名称，并将其作为包标记添加到所有提取的日志中。标记名称是日志的文件名或目录名称（如果来自于目录）。包标记可以区分 vRealize Log Insight 服务器上的包。

此标记会覆盖在清单文件中指定的任何同名标记。该标记会被同名的命令行标记覆盖。

在使用导入程序时，请注意以下行为：

- vRealize Log Insight Importer 不会检查 vRealize Log Insight 虚拟设备上的可用磁盘空间。因此，如果虚拟设备磁盘空间不足，则导入存档的日志可能失败。
- vRealize Log Insight 在日志导入过程中不显示进度。在导入存档数据的过程中，无法根据控制台输出推断距离导入完成还有多长时间或已导入多少数据。

受支持的操作系统

以下操作系统支持 vRealize Log Insight Importer：

- Windows 32 位和 64 位
- Linux 32 位和 64 位

Linux 版本不在 Apple Macintosh 系统上运行。

安装 vRealize Log Insight Importer

可以在 Windows 和 Linux 上安装 vRealize Log Insight Importer。也可以将 vRealize Log Insight Importer 安装在 vRealize Log Insight 服务器上并从服务器上运行。

安装 vRealize Log Insight Importer 时，还会安装若干 VMware 产品清单文件。运行 vRealize Log Insight Importer 时，您可以使用这些文件，也可以根据需要修改它们。对于 Windows，这些清单文件位于 C:\Program Files (x86)\VMware\Log Insight Importer\Manifests；对于 Linux，则位于 /usr/lib/loginsight-importer/manifests。

如果卸载 .bin 软件包，也需删除 /usr/bin/loginsight_importer 符号链接。

前提条件

- 验证您是否能够访问 [VMware 下载](#) 站点下载 vRealize Log Insight Importer。

步骤

- 1 从 [VMware 下载](#) 站点下载 vRealize Log Insight Importer 安装软件包。

安装软件包中包含适用于 Windows 的 MSI 安装程序以及适用于 Linux 的 POSIX 安装软件包（RPM、DEB 和 BIN）。

2 在您的系统上安装此工具。

安装后，导入程序安装目录会添加到 Windows 上的 PATH 环境变量，指向 `loginsight-importer` 可执行文件的符号链接会添加到 Linux 上的 `/usr/bin/`。因此，客户端无需指定一个路径前缀即可从 shell 中调用 `loginsight-importer`。

vRealize Log Insight Importer 工具安装在以下位置。

操作系统	文件名	安装位置
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

运行 vRealize Log Insight Importer

运行导入程序时，必须包含清单文件。清单文件提供了有关日志格式、要导入的数据所在的位置的信息，以及源和目标信息。

- [关于 vRealize Log Insight Importer 清单文件](#)

vRealize Log Insight Importer 使用清单配置文件来确定日志格式并指定要导入的数据的位置。清单文件与 `liagent.ini` 配置文件格式相同、结构相似。

- [vRealize Log Insight Importer 清单文件配置示例](#)

vRealize Log Insight Importer 清单文件示例提供了参数配置的示例。

- [运行 vRealize Log Insight Importer](#)

运行 vRealize Log Insight Importer 以将历史数据的脱机日志导入 vRealize Log Insight 服务器。

关于 vRealize Log Insight Importer 清单文件

vRealize Log Insight Importer 使用清单配置文件来确定日志格式并指定要导入的数据的位置。清单文件与 `liagent.ini` 配置文件格式相同、结构相似。

您可以选择创建自己的清单文件以导入任意日志文件。创建此类文件的一个好处是，您不需要知道数据文件的绝对路径。

如果不创建清单文件，vRealize Log Insight Importer 将使用收集所有 `.txt` 和 `.log` 文件 (`include=*.log*;*.txt*`) 的默认清单，并且会对已提取的日志应用自动分析程序（提取时间戳 + `kvp`）。

如果将 `liagent.ini` 配置文件用作清单文件，vRealize Log Insight Importer 将仅提取 `[filelog]` 部分作为清单。`[filelog]` 部分的所有选项在 vRealize Log Insight Importer 中均受支持。

有关 `[filelog]` 部分中支持的选项以及配置示例的信息，请参见《使用 vRealize Log Insight 代理》中的“从日志文件收集事件”主题。

创建清单文件

您可以将代理配置文件的内容复制并粘贴到新的 TXT 文件中。要确定一个动态路径，请移除目录路径前开头的 “/” 。

指定目录路径

在 [filelog] 部分中指定的目录可与源路径相关或者为绝对路径。要指定相对路径，在 Linux 下，请不要包含开头的斜线，否则，vRealize Log Insight Importer 会将此路径视为绝对路径。

要在目录键的值中表示名称模式，您可以使用 * 和 ** 字符。

- 在单个目录中将 * 用作占位符。使用该字符表示具有一个任意文件夹名称的一级嵌套。例如，使用 `directory = log_folder_*` 表示以字符串 `log_folder_` 开头的任意文件夹。
- 使用 ** 表示具有文件夹名称的任意级别嵌套。例如，可以使用 `directory = **/log` 表示源目录中任意级别嵌套具有 `log` 名称的任意文件夹。

vRealize Log Insight Importer 清单文件配置示例

vRealize Log Insight Importer 清单文件示例提供了参数配置的示例。

目录键的值必须为相对于源的值，或者为绝对值。以下示例说明如何从扩展名为 `.log`（位于源目录以下两级且最后一个文件夹名以 `_log` 字符串结尾）的文件中收集日志。

```
[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
```

以下示例说明如何从源目录的所有子文件夹（包括源本身）中收集扩展名为 `.log` 的所有文件。

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

以下示例说明如何从源目录（不包括子文件夹）中的所有文件（扩展名为 `.ini` 的文件除外）收集日志。在这里文件是指 UTF-16LE 编码文件。

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

以下示例说明如何从源目录（不包括子文件夹）中扩展名为 `.log` 的所有文件收集日志。事件的时间戳在日志文件中使用通用日志格式 (CLF) 分析程序进行分析，且应用了已提取的历史时间戳。由 CLF 分析程序分析的日志格式为 `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
```

运行 vRealize Log Insight Importer

运行 vRealize Log Insight Importer 以将历史数据的脱机日志导入 vRealize Log Insight 服务器。

前提条件

- 查看[关于 vRealize Log Insight Importer 清单文件](#)并创建清单文件以用于导入程序。有关详细信息，请参见[vRealize Log Insight Importer 清单文件配置示例](#)。
- 如果使用 `honor_timestamp` 参数，则验证您是否拥有相应的登录凭据。
- 如果导入一个支持包，需配置 `honor_timestamp` 以及用户名和密码。

步骤

- 1 在命令提示符下输入以下命令以启动 vRealize Log Insight Importer 工具。

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

- 2 在提示符下输入清单文件名。
- 3 定义配置参数并按 **Enter**。

`--source` 和 `--server` 参数是必要参数。

必要参数	描述
<code>--source <path></code>	指定支持包目录的路径或到 zip、gzip、bzip、bzip2 或 tar 存档的路径。该值作为 <code>bundle</code> 标记的值添加到所有已发送的消息。
<code>--server <hostname></code>	目标服务器主机名或 IP 地址。

选项	描述
<code>--port <port></code>	用于连接的端口。如果未设置，则端口 9000 将用于非 SSL 连接，端口 9543 将用于 SSL 连接。
<code>--logdir <path></code>	指定到日志目录的路径。如果未设置，则路径为： <code>\$(LOCALAPPDATA)\VMware\Log Insight Importer\log</code> （适用于 Windows）和 <code>~/loginsight-importer/log</code> （适用于 Linux）。

选项	描述
<code>--manifest <file-path></code>	指定到清单文件的路径（.ini 格式）。如果未设置，则将使用源目录中的 <code>importer.ini</code> 文件。如果 <code>importer.ini</code> 文件不存在或者在源目录中未找到，vRealize Log Insight Importer 将应用默认的（硬编码）清单并收集所有 .txt 和 .log 文件 (<code>include=*.log*;*.txt*</code>)，还会应用自动分析程序（提取时间戳 + kvp）。
<code>--no_ssl</code>	请勿使用 SSL 进行连接。 不应为经过身份验证的连接设置此参数（例如，如果使用了 <code>--honor_timestamp</code> ）。
<code>--ssl_ca_path <path></code>	到信任根证书包文件的路径。
<code>--tags <tags></code>	为所有已发送的事件设置标记。例如， <code>--tags "{ \"tag1\" : \"value1\", \"tag2\" : \"value2\"}"</code> 注 标记选项可接受 <code>hostname</code> 作为一个标记名称。命令行中 <code>hostname</code> 标记的值而非发送计算机的 FQDN 被用作由 vRealize Log Insight Importer 提取的所有事件的 <code>hostname</code> 字段的值。这正好与清单文件中的标记参数和由忽略 <code>hostname</code> 字段的分析程序所提取的字段相反。 将自动确定日志包名称（文件名或目录名 - 如果来自目录），并会作为 <code>bundle</code> 标记添加到在载入过程中从该特定包提取的所有日志。该标记帮助您区分 vRealize Log Insight 服务器上的包。 <code>bundle</code> 标记将覆盖清单文件中的同名标记。但如果具有 <code>bundle</code> 名称的命令行标记，命令行标记可能会覆盖该标记。
<code>--username <username></code>	用于进行身份验证的用户名。如果已设置 <code>--honor_timestamp</code> ，则需设置此参数。
<code>--password <password></code>	用于进行身份验证的密码。如果已设置 <code>--honor_timestamp</code> ，则需设置此参数。用户名/密码对禁用 vRealize Log Insight 服务器上已允许的时间偏移，因此，可以导入带有历史时间戳的数据。
<code>--honor_timestamp</code>	应用提取的时间戳。已配置的分析程序从日志条目提取时间戳，然后 <code>--honor_timestamp</code> 应用提取的时间戳。 <ul style="list-style-type: none">■ 如果使用已配置的分析程序提取时间戳，则事件将使该时间戳得到应用。■ 如果日志文件中存在不带有任何已提取的时间戳的事件，则将应用同一日志文件中从前一个事件成功提取的时间戳。■ 如果文件中未发现或未分析任何时间戳，则将日志文件的 <code>MTIME</code> 作为时间戳应用。 注 如果未提供清单文件，则 vRealize Log Insight Importer 将使用的默认硬编码清单会使自动日志分析程序启用。在这种情况下，如果使用 <code>--honor_timestamp</code> 参数，则 vRealize Log Insight Importer 从日志条目提取时间戳。
<code>--debug_level <1 2></code>	增加日志文件的详细级别。只在进行故障排除时才应更改此参数。正常操作时，不应使用此标记。
<code>--help</code>	显示帮助并退出。

4 在导入完成后，在 Windows 或 Linux 上按 **Ctrl+C** 以退出该工具。

结果

vRealize Log Insight Importer 会从在参数中指定的目录提取日志条目。将显示已处理文件的总数、已提取日志消息的总数、已发送日志消息的总数以及运行时间。

后续步骤

在 vRealize Log Insight “交互式分析”选项卡中，您可以刷新视图以列出已导入的日志事件。如果导入了一个支持包并使用了 `honor_timestamp`，则仪表板也应显示一段时间内的事件。