

vRealize Log Insight Importer 사용

2019년 6월 25일 수요일

vRealize Log Insight 4.7



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

1	vRealize Log Insight Importer 사용	4
	vRealize Log Insight Importer 설치	4
	vRealize Log Insight Importer를 설치하기 전에	5
	vRealize Log Insight Importer 설치	5
	vRealize Log Insight Importer 실행	6
	vRealize Log Insight Importer 매니페스트 파일 정보	6
	vRealize Log Insight Importer 매니페스트 파일 구성 예	7
	vRealize Log Insight Importer 실행	8

vRealize Log Insight Importer 사용

1

vRealize Log Insight Importer는 로컬 시스템에 있는 기간별 데이터의 오프라인 로그를 vRealize Log Insight 서버에 가져오는 데 사용되는 명령줄 유틸리티입니다.

이전에 수집한 로그를 가져오려는 경우 임пор터를 사용합니다. 지원 번들 및 아카이브된 로그를 가져올 수 있으며 vRealize Log Insight 또는 VMware 제품에서 수집한 지원 번들에서 로그를 분석할 수 있습니다.

vRealize Log Insight Importer에는 다음과 같은 기능이 포함되어 있습니다.

- vRealize Log Insight Importer는 수집 API를 통해 데이터를 전송합니다.
- 재귀 디렉토리 수집을 포함하여 파일 로그 수집을 지원합니다.
- 임пор터는 zip, tar, bzip, bzip2 또는 gz 아카이브 파일에서 데이터를 읽어올 수 있습니다. 7-Zip은 지원되지 않습니다.
- 중첩된 ZIP 파일과 같은 중첩된 아카이브 또는 아카이브 내의 디렉토리에서 재귀적으로 데이터를 읽을 수 있도록 지정할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [vRealize Log Insight Importer 설치](#)
- [vRealize Log Insight Importer 실행](#)

vRealize Log Insight Importer 설치

VMware 다운로드 사이트에서 다운받은 설치 패키지를 통해 vRealize Log Insight Importer를 설치합니다. 설치 패키지에는 Windows용 MSI 설치 관리자 및 Linux용 POSIX 설치 패키지(RPM, DEB 및 BIN)가 포함되어 있습니다.

- [vRealize Log Insight Importer를 설치하기 전에](#)
임пор터를 설치하기 전에 요구 사항을 확인하고 임пор터 동작을 이해합니다.
- [vRealize Log Insight Importer 설치](#)
vRealize Log Insight Importer는 Windows 및 Linux에 설치할 수 있습니다. vRealize Log Insight Importer를 vRealize Log Insight 서버에 설치한 후 서버에서 실행할 수도 있습니다.

vRealize Log Insight Importer를 설치하기 전에

임포터를 설치하기 전에 요구 사항을 확인하고 임포터 동작을 이해합니다.

설치하기 전에 vRealize Log Insight에서 아카이브된 데이터가 저장되어 있는 NFS 서버에 액세스할 수 있는지 확인합니다. 네트워크 장애나 NFS 서버의 오류로 인해 NFS 서버에 액세스할 수 없게 되면 아카이브된 데이터를 가져올 수 없습니다.

수집하는 동안 번들에서 로그가 추출되면 로그 번들 이름이 자동으로 결정되고 추출된 모든 로그에 번들 태그로 추가됩니다. 태그 이름은 로그의 파일 이름이거나 디렉토리 이름(디렉토리 소스의 경우)입니다. 번들 태그는 vRealize Log Insight 서버에서 번들을 구분합니다.

이 태그는 매니페스트 파일에서 지정되는 동일한 이름을 가진 다른 태그에 우선합니다. 이 태그를 동일한 이름을 사용하는 명령줄 태그로 재정의할 수 있습니다.

임포터를 사용하는 경우 다음 동작을 알아두어야 합니다.

- vRealize Log Insight Importer에서는 vRealize Log Insight 가상 장치의 사용 가능한 디스크 공간을 확인하지 않습니다. 따라서 가상 장치의 디스크 공간이 부족하면 아카이브된 로그 가져오기에 실패할 수 있습니다.
- vRealize Log Insight에서는 로그 가져오기 동안 진행률 정보를 표시하지 않습니다. 아카이브된 데이터 가져오기가 진행 중일 경우에는 가져오기가 완료될 때까지 남은 시간 또는 이미 가져온 데이터의 양을 콘솔 출력에서 참조할 수 없습니다.

지원되는 운영 체제

vRealize Log Insight Importer는 다음과 같은 운영 체제에서 지원됩니다.

- Windows 32비트 및 64비트
- Linux 32비트 및 64비트

Linux 버전은 Apple Macintosh 시스템에서는 실행되지 않습니다.

vRealize Log Insight Importer 설치

vRealize Log Insight Importer는 Windows 및 Linux에 설치할 수 있습니다. vRealize Log Insight Importer를 vRealize Log Insight 서버에 설치한 후 서버에서 실행할 수도 있습니다.

vRealize Log Insight Importer를 설치하면 VMware 제품의 여러 매니페스트 파일도 설치됩니다. vRealize Log Insight Importer를 실행할 때 필요에 따라 이러한 파일을 사용하거나 수정할 수 있습니다. 이러한 매니페스트 파일은 Windows의 경우 C:\Program Files (x86)\VMware\Log Insight Importer\Manifests에, Linux의 경우 /usr/lib/loginsight-importer/manifests에 있습니다.

.bin 패키지를 제거하면 /usr/bin/loginsight_importer 심볼 링크도 함께 삭제됩니다.

사전 요구 사항

- [VMware 다운로드](#) 사이트에 액세스하여 vRealize Log Insight Importer를 다운로드할 수 있는지 확인합니다.

절차

- 1 [VMware 다운로드](#) 사이트에서 vRealize Log Insight Importer 설치 패키지를 다운로드합니다.

설치 패키지에는 Windows용 MSI 설치 관리자 및 Linux용 POSIX 설치 패키지(RPM, DEB 및 BIN)가 포함되어 있습니다.

- 2 시스템에 도구를 설치합니다.

설치를 완료하면 Windows에서는 PATH 환경 변수에 임포터 설치 디렉토리가 추가되고, Linux에서는 `loginsight-importer` 실행 파일에 대한 심볼 링크가 `/usr/bin/`에 추가됩니다. 그러면 클라이언트에서 경로 접두사를 지정하지 않고 셸에서 `loginsight-importer`를 호출할 수 있습니다.

vRealize Log Insight Importer 도구는 다음 위치에 설치됩니다.

운영 체제	파일 이름	설치 위치
Windows	loginsight-importer.exe	C:\Program Files (x86)\VMware\Log Insight Importer
Linux	loginsight-importer	/usr/lib/loginsight-importer

vRealize Log Insight Importer 실행

임포터를 실행하는 경우에는 매니페스트 파일을 포함해야 합니다. 매니페스트 파일은 로그 형식, 가져올 데이터 위치에 대한 정보와 소스 및 대상 정보를 제공합니다.

- [vRealize Log Insight Importer 매니페스트 파일 정보](#)

vRealize Log Insight Importer는 매니페스트 구성 파일을 사용하여 로그 형식을 결정하고, 가져올 데이터의 위치를 지정합니다. 매니페스트 파일은 `liagent.ini` 구성 파일과 형식이 동일하며 구조도 유사합니다.

- [vRealize Log Insight Importer 매니페스트 파일 구성 예](#)

샘플 vRealize Log Insight Importer 매니페스트 파일에서는 매개 변수 구성의 예를 제공합니다.

- [vRealize Log Insight Importer 실행](#)

vRealize Log Insight Importer를 실행하여 기록 데이터의 오프라인 로그를 vRealize Log Insight 서버로 가져옵니다.

vRealize Log Insight Importer 매니페스트 파일 정보

vRealize Log Insight Importer는 매니페스트 구성 파일을 사용하여 로그 형식을 결정하고, 가져올 데이터의 위치를 지정합니다. 매니페스트 파일은 `liagent.ini` 구성 파일과 형식이 동일하며 구조도 유사합니다.

사용자 자신의 매니페스트 파일을 생성하여 임의의 로그 파일을 가져올 수 있습니다. 매니페스트 파일 생성 여부는 선택 사항이지만 매니페스트 파일을 사용하면 데이터 파일의 절대 경로를 알고 있을 필요가 없습니다.

매니페스트 파일을 생성하지 않으면 vRealize Log Insight Importer는 모든 기본 매니페스트를 사용하여 .txt 및 .log 파일(include=*.log*;*.txt*)을 수집하고, 추출된 로그에 자동 구문 분석기(타임 스탬프 + kvp 추출)를 적용합니다.

liagent.ini 구성 파일을 매니페스트 파일로 사용하면 vRealize Log Insight Importer는 [filelog] 섹션만 매니페스트로 추출합니다. vRealize Log Insight Importer에서는 [filelog] 섹션에 대한 모든 옵션이 지원됩니다.

[filelog] 섹션에 대해 지원되는 추가적인 옵션 및 구성 예를 보려면 "vRealize Log Insight Agent 관리 가이드"에서 vRealize Log Insight 에이전트 설명서를 참조하십시오.

매니페스트 파일을 생성하려면

에이전트 구성 파일의 콘텐츠를 복사하여 새 .txt 파일에 붙여 넣을 수 있습니다. 동적 경로를 나타내려면 디렉토리 경로에서 선행 "/"를 제거합니다.

디렉토리 경로 지정

[filelog] 섹션에 지정된 디렉토리는 소스에 대해 상대적인 디렉토리이거나 절대적인 디렉토리일 수 있습니다. 상대 경로를 지정하려면 Linux의 경우 선행 슬래시를 포함하지 마십시오. 선행 슬래시를 포함하면 vRealize Log Insight Importer에서 경로를 절대 경로로 처리합니다.

* 및 ** 문자를 사용하여 디렉토리 키의 값에 이름 패턴을 나타낼 수 있습니다.

- 단일 디렉토리의 경우 *를 자리 표시자로 사용합니다. 이 자리 표시자는 임의의 폴더 이름 및 중첩 수준 하나를 나타내는 데 사용합니다. 예를 들어 log_folder_로 시작하는 임의의 폴더를 나타내려면 directory = log_folder_*를 사용합니다.
- 임의의 폴더 이름과 임의의 중첩 수준을 나타내려면 **를 사용합니다. 예를 들어 소스 디렉토리 내에서 임의의 중첩 수준에 있고 이름이 log인 모든 폴더를 나타내려면 directory = **/log를 사용합니다.

vRealize Log Insight Importer 매니페스트 파일 구성 예

샘플 vRealize Log Insight Importer 매니페스트 파일에서는 매개 변수 구성의 예를 제공합니다.

디렉토리 키는 소스에 대해 상대적인 값이거나 절대값이어야 합니다. 다음 예에서는 소스 디렉토리보다 두 수준 아래에 있고 마지막 폴더의 이름이 _log 문자열로 끝나는 폴더에서 .log 확장명을 가진 파일로부터 로그를 수집하는 방법을 보여 줍니다.

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

다음 예에서는 소스 자체를 포함한 소스 디렉토리의 모든 하위 폴더에서 .log 확장명을 가진 모든 파일을 수집하는 방법을 보여 줍니다.

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

```
include = *.log
```

다음 예에서는 소스 디렉토리(하위 폴더는 제외)에서 .ini 확장명을 사용하는 파일을 제외한 모든 파일에서 로그를 수집하는 방법을 보여 줍니다. 파일은 UTF-16LE 인코딩된 파일로 해석됩니다.

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

다음 예에서는 소스 디렉토리(하위 폴더 제외)에서 .log 확장명을 가진 모든 파일에서 로그를 수집하는 방법을 보여 줍니다. 이벤트의 타임 스탬프는 CLF(일반 로그 형식) 구문 분석기를 사용하여 로그 파일에 구문 분석되며, 추출된 시간별 타임 스탬프가 적용됩니다. CLF 구문 분석기가 구문 분석한 로그 형식은 2015-03-25 22:11:46,786 | DEBUG | pool-jetty-76 | AuthorizationMethodInterceptor | Authorizing method: public abstract입니다.

```
[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 실행

vRealize Log Insight Importer를 실행하여 기록 데이터의 오프라인 로그를 vRealize Log Insight 서버로 가져옵니다.

사전 요구 사항

- [vRealize Log Insight Importer 매니페스트 파일 정보](#)를 검토하고 임пор터에서 사용할 매니페스트 파일을 생성합니다. 자세한 내용은 [vRealize Log Insight Importer 매니페스트 파일 구성 예](#) 항목을 참조하십시오.
- honor_timestamp 매개 변수를 사용하는 경우에는 적절한 로그인 자격 증명이 있는지 확인합니다.
- 지원 번들을 가져오는 경우에는 honor_timestamp 및 사용자 이름과 암호를 구성합니다.

절차

- 1 명령 프롬프트에 다음 명령을 입력하여 vRealize Log Insight Importer 도구를 시작합니다.

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

- 2 프롬프트에서 매니페스트 파일 이름을 입력합니다.

3 구성 매개 변수를 정의하고 **Enter** 키를 누릅니다.

--source 및 --server 매개 변수가 필요합니다.

필수 매개 변수	설명
--source <path>	지원 번들 디렉토리의 경로 또는 zip, gzip, bzip, bzip2, tar 아카이브의 경로를 지정합니다. 이 값은 모든 보내기 메시지에 bundle 태그 값으로 추가됩니다.
--server <hostname>	대상 서버 호스트 이름 또는 IP 주소입니다.

옵션	설명
--port <port>	연결 포트입니다. 값을 설정하지 않으면 SSL 이외의 연결에는 포트 9000이 사용되고 SSL 연결에는 포트 9543이 사용됩니다.
--logdir <path>	로그 디렉토리의 경로를 지정합니다. 값을 설정하지 않으면 경로는 \$(LOCALAPPDATA)\VMware\Log Insight Importer\log(Windows) 및 ~/.loginsight-importer/log(Linux)가 됩니다.
--manifest <file-path>	매니페스트 파일(.ini 형식)의 경로를 지정합니다. 값을 설정하지 않으면 소스 디렉토리의 importer.ini 파일이 사용됩니다. importer.ini 파일이 존재하지 않거나 이 파일을 소스 디렉토리에서 찾을 수 없으면 vRealize Log Insight Importer는 하드 코딩된 기본 매니페스트를 적용하여 모든 .txt 및 .log 파일(include=*.log*;*.txt*)을 수집하며, 자동 구문 분석기(타임 스탬프 + kvp 추출)도 적용합니다.
--no-ssl	연결에 SSL을 사용하지 않습니다. 인증된 연결(예: --honor_timestamp를 사용하는 경우)에는 이 매개 변수를 설정하면 안 됩니다.
--ssl_ca_path <path>	신뢰할 수 있는 루트 인증서 번들 파일의 경로입니다.
--tags <tags>	보낸 모든 이벤트에 대해 태그를 설정합니다. 예: --tags "{ W"tag1W" : W"value1W", W>tag2W":W"value2W"}" 참고 tags 옵션에는 hostname을 태그 이름으로 사용할 수 있습니다. vRealize Log Insight Importer가 추출하는 모든 이벤트의 hostname 필드에는 보내는 시스템의 FQDN이 아니라 명령줄에서 가져온 hostname 태그의 값이 대신 사용됩니다. 이는 hostname 필드를 무시하는 매니페스트 파일의 tags 매개 변수 및 구문 분석기로 추출된 필드와는 반대입니다. 로그 번들 이름(파일 이름 또는 디렉토리 소스의 경우에는 디렉토리 이름)이 자동으로 결정된 후 수집 중에 특정 번들에서 추출된 모든 로그에 bundle 태그로 추가됩니다. 이 태그는 vRealize Log Insight Server에서 번들을 구분하는 데 도움이 됩니다. bundle 태그는 매니페스트 파일의 동일한 이름으로 태그를 재정의합니다. 하지만 bundle 이름의 명령줄 태그가 있는 경우 이러한 태그로 재정의될 수 있습니다.
--username <username>	인증에 사용하는 사용자 이름입니다. --honor_timestamp를 설정한 경우에는 필수 매개 변수입니다.
--password <password>	인증에 사용하는 암호입니다. --honor_timestamp를 설정한 경우에는 필수 매개 변수입니다. 사용자 이름/암호 쌍은 vRealize Log Insight 서버에서 허용되는 시간 경과를 사용하지 않도록 설정하기 때문에 기간별 타임 스탬프가 포함된 데이터를 가져올 수 있습니다.

옵션	설명
--honor_timestamp	<p>추출된 타임 스탬프를 적용합니다. 구성된 구문 분석기가 로그 항목에서 타임 스탬프를 추출하고 --honor_timestamp가 추출된 타임 스탬프를 적용합니다.</p> <ul style="list-style-type: none"> ■ 구성된 구문 분석기를 사용하여 타임 스탬프를 추출하면 이벤트에 해당 타임 스탬프가 적용됩니다. ■ 타임 스탬프가 추출되지 않은 이벤트가 로그 파일에 있으면 같은 로그 파일의 이전 이벤트에서 성공적으로 추출된 타임 스탬프가 적용됩니다. ■ 파일에 타임 스탬프가 없거나 타임 스탬프가 구문 분석되지 않은 경우에는 로그 파일의 MTIME 이 타임 스탬프로 적용됩니다. <p>참고 매니페스트 파일이 제공되지 않은 경우, vRealize Log Insight Importer에서 사용할 기본 하드 코딩된 매니페스트에 자동 로그 구문 분석기가 사용하도록 설정됩니다. 이 경우, --honor_timestamp 매개 변수를 사용하면 vRealize Log Insight Importer가 로그 항목에서 타임 스탬프를 추출합니다.</p>
--debug_level <1 2>	로그 파일의 세부 정보 표시 수준을 높입니다. 이 매개 변수는 문제를 해결하는 경우에만 변경해야 합니다. 일반적인 작업을 수행할 때는 이 플래그를 사용하면 안 됩니다.
--help	도움말을 표시하고 도움말을 종료합니다.

4 가져오기가 완료된 후에 Windows 또는 Linux에서 **Ctrl+C**를 눌러 도구를 종료합니다.

vRealize Log Insight Importer가 매개 변수에 지정된 디렉토리에서 로그 항목을 추출합니다. 처리된 총 파일 수, 추출된 로그 메시지, 보낸 로그 메시지 및 실행 시간이 표시됩니다.

다음에 수행할 작업

vRealize Log Insight 대화형 분석 탭에서 보기를 새로 고치면 가져온 로그 이벤트 목록을 볼 수 있습니다. 지원 번들을 가져오고 honor_timestamp를 사용한 경우에는 시간 경과에 따른 이벤트도 대시보드에 표시되어야 합니다.