

# vRealize Log Insight 에이 전트 작업

업데이트 1

수정일: 2017년 9월 3일

vRealize Log Insight 4.0



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](mailto:docfeedback@vmware.com)

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

Copyright © 2014–2017 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

# 목차

vRealize Log Insight Agent 작업 정보	5
vRealize Log Insight 에이전트 작업에 대해 업데이트된 정보	6
<b>1 vRealize Log Insight 에이전트 개요</b>	<b>7</b>
vRealize Log Insight Windows 에이전트 개요	7
Log Insight Linux Agent 개요	8
<b>2 vRealize Log Insight 에이전트 설치</b>	<b>9</b>
Windows 또는 Linux 에이전트 파일 다운로드	9
기본 구성으로 vRealize Log Insight Windows 에이전트 설치	10
vRealize Log Insight Windows 에이전트 설치, 업데이트 및 구성	11
여러 시스템에 Log Insight Windows Agent 배포	12
변환 .mst 파일을 사용하여 vRealize Log Insight Windows 에이전트 배포	12
vRealize Log Insight Windows 에이전트의 여러 인스턴스 배포	13
vRealize Log Insight Linux 에이전트 RPM 패키지 설치 또는 업데이트	14
vRealize Log Insight Linux 에이전트 DEB 패키지 설치 또는 업데이트	15
Log Insight Linux Agent 이진 패키지 설치	17
<b>3 vRealize Log Insight 에이전트 구성</b>	<b>19</b>
설치 후 Log Insight Windows Agent 구성	19
Log Insight Windows Agent의 기본 구성	20
대상 vRealize Log Insight 서버 설정	21
Windows 이벤트 채널에서 이벤트 수집	23
로그 파일에서 이벤트 수집	27
Log Insight Windows Agent로 이벤트 전달	31
Log Insight Linux Agent 구성	31
vRealize Log Insight Linux Agent의 기본 구성	32
Linux 에이전트 구성에 대해 공통 값 사용	33
대상 vRealize Log Insight 서버 설정	35
로그 파일에서 이벤트 수집	37
vRealize Log Insight 에이전트의 중앙 집중식 구성	41
구성 병합 예	41
로그 구문 분석	43
로그 구문 분석기 구성	43
<b>4 vRealize Log Insight 에이전트 제거</b>	<b>65</b>
Log Insight Windows Agent 제거	65

Log Insight Linux Agent RPM 패키지 제거 65

Log Insight Linux Agent DEB 패키지 제거 66

Log Insight Linux Agent Bin 패키지 제거 66

## 5 vRealize Log Insight 에이전트 문제 해결 68

Log Insight Windows Agent용 지원 번들 생성 68

Log Insight Linux Agent용 지원 번들 생성 69

Log Insight Agents의 로그 세부 정보 수준 정의 69

관리 UI에 Log Insight Agents가 표시되지 않음 70

vRealize Log Insight 에이전트가 이벤트를 보내지 않음 71

Log Insight Windows Agent에 대한 아웃바운드 예외 규칙 추가 72

Windows 방화벽에서 Log Insight Windows Agent의 아웃바운드 연결 허용 73

Log Insight Windows Agent의 대량 배포가 실패함 73

RPM 패키지 업데이트 설치가 실패함 74

Log Insight Agents가 자체 서명된 인증서를 거부함 75

vRealize Log Insight 서버가 암호화되지 않은 트래픽의 연결을 거부함 75

# vRealize Log Insight Agent 작업 정보

“vRealize Log Insight Agent 작업”에서는 vRealize™Log Insight™ Windows 및 Linux 에이전트를 설치하고 구성하는 방법을 설명합니다. 또한 문제 해결 팁도 포함되어 있습니다.

이 정보는 Log Insight Agents를 설치하거나 구성하거나 문제 해결하려는 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

vRealize Log Insight 서버로 에이전트용 구성 클래스를 생성하는 방법에 대해서는 “vRealize Log Insight 관리”를 참조하십시오.

# vRealize Log Insight 에이전트 작업에 대해 업데이트된 정보

“vRealize Log Insight 에이전트 작업”은 제품의 각 릴리스에 따라 또는 필요할 때 업데이트됩니다. 이 표에는 변경 사항이 요약되어 있습니다.

개정	설명
002369 -1	편집 변경 사항.
002369-0	최초 릴리스.

# vRealize Log Insight 에이전트 개요

1

vRealize Log Insight 에이전트는 Linux 및 Windows 시스템의 로그 파일에서 이벤트를 수집하고 이를 vRealize Log Insight 서버에 전달합니다.

본 장은 다음 항목을 포함합니다.

- [vRealize Log Insight Windows 에이전트 개요](#)
- [Log Insight Linux Agent 개요](#)

## vRealize Log Insight Windows 에이전트 개요

vRealize Log Insight Windows 에이전트는 Windows 이벤트 채널 및 로그 파일에서 이벤트를 수집하여 이를 vRealize Log Insight 서버에 전달합니다.

Windows 이벤트 채널은 Windows 시스템의 관련 이벤트를 수집하기 위한 풀입니다.

Windows 시스템에서 애플리케이션은 파일 시스템의 플랫폼 텍스트 파일에 로그 데이터를 저장할 수 있습니다. vRealize Log Insight Windows 에이전트는 디렉토리를 모니터링하고 플랫폼 텍스트 로그 파일에서 이벤트를 수집할 수 있습니다.

vRealize Log Insight Windows 에이전트는 vRealize Log Insight 서버에 보내는 요청이 각각 64KB로 제한됩니다.

vRealize Log Insight Windows 에이전트는 Windows 서비스로 실행되며 설치 직후 시작됩니다. 설치 중이나 설치 이후에 vRealize Log Insight Windows 에이전트에 대해 다음 옵션을 구성할 수 있습니다.

- vRealize Log Insight Windows 에이전트가 이벤트를 전달하는 대상 vRealize Log Insight 서버를 선택합니다.
- vRealize Log Insight Windows 에이전트가 사용하는 통신 프로토콜 및 포트를 선택합니다.
- vRealize Log Insight Windows 에이전트가 이벤트를 수집하는 Windows 이벤트 채널을 더 추가합니다.
- 모니터링할 Windows 디렉토리를 선택하고 수집할 플랫폼 로그 파일을 추가합니다.

vRealize Log Insight Windows 에이전트를 사용하려면 Windows Vista 이상 또는 Windows Server 2008 이상이 필요합니다.

vRealize Log Insight Windows 에이전트 .msi 파일의 복사본이 있는지 확인합니다. [Windows 또는 Linux 에이전트 파일 다운로드](#) 항목을 참조하십시오.

## Log Insight Linux Agent 개요

Log Insight Linux Agent는 Linux 시스템의 로그 파일에서 이벤트를 수집하여 이를 vRealize Log Insight 서버에 전달합니다.

Linux 시스템에서 애플리케이션은 파일 시스템의 플랫폼 텍스트 파일에 로그 데이터를 저장할 수 있습니다. Log Insight Linux Agent는 디렉토리를 모니터링하고 플랫폼 텍스트 로그 파일에서 이벤트를 수집할 수 있습니다.

Log Insight Linux Agent는 대몬으로 실행되며 설치 직후 시작됩니다. 설치 후 다음 옵션을 구성할 수 있습니다.

- Log Insight Linux Agent가 이벤트를 전달하는 대상 vRealize Log Insight 서버를 선택합니다.
- Log Insight Linux Agent로 모니터링할 디렉토리를 구성합니다.

Log Insight Linux Agent는 다음 배포 및 버전을 지원합니다.

- RHEL 5, RHEL 6 및 RHEL 7
- SLES 11 SP3 및 SLES 12 SP1
- Ubuntu 12.04 LTS, 14.04 LTS 및 16.04 LTS

Log Insight Linux Agent는 자체 작업 로그 파일을 `/var/log/loginsight-agent/liagent_*.log`에 기록합니다. 로그 파일은 Log Insight Linux Agent가 다시 시작될 때 그리고 크기가 10MB에 도달할 때 순환됩니다. 순환에서 50MB의 결합된 제한이 유지됩니다.

Log Insight Linux Agent 패키지를 다운로드하려면 vRealize Log Insight 웹 사용자 인터페이스의 관리 페이지로 이동하고 관리 섹션에서 **에이전트**를 클릭한 다음 해당 패키지 링크를 클릭합니다.

사용할 루트 권한이 없는 사용자를 위해 Log Insight Linux Agent의 기본 설치를 구현하는 경우, 기본 구성이 데이터 수집 시 문제를 초래할 수 있습니다. 채널 구독에 실패했다는 경고를 에이전트가 로그하지 않습니다. 그리고 수집의 파일에 읽기 권한이 없습니다. `Inaccessible log file ... will try later` 메시지가 로그에 반복적으로 추가됩니다. 문제를 초래하는 기본 구성을 주석 처리하거나 사용자 사용 권한을 변경할 수 있습니다.

rpm 또는 DEB 패키지를 사용하여 Linux 에이전트를 설치하는 경우 패키지 설치의 일부로 `liagentd`라는 이름의 `init.d` 스크립트가 설치됩니다. `bin` 패키지는 스크립트를 추가하지만 이를 등록하지는 않습니다. 스크립트를 수동으로 등록할 수 있습니다.

`(/sbin/)service liagentd status` 명령을 실행하여 성공적으로 설치되었는지 확인할 수 있습니다.



# vRealize Log Insight 에이전트 설치

## 2

Log Insight Windows Agent 및 Linux Agent는 Windows 및 Linux 시스템에서 이벤트를 수집하여 이를 vRealize Log Insight 서버로 전달합니다. 서버, 포트 및 프로토콜에 대한 매개 변수를 설치 및 구성하거나 기본 설정을 유지하도록 선택할 수 있습니다.

vRealize Log Insight 에이전트를 설치하고 실행하려는 경우 호스트/시스템에서 x86 및 x86\_64 아키텍처와 MMX, SSE, SSE2 및 SSE3 명령 집합을 지원하는 데 필요한 최소 하드웨어 매개 변수가 있습니다.

본 장은 다음 항목을 포함합니다.

- [Windows 또는 Linux 에이전트 파일 다운로드](#)
- [기본 구성으로 vRealize Log Insight Windows 에이전트 설치](#)
- [vRealize Log Insight Windows 에이전트 설치, 업데이트 및 구성](#)
- [여러 시스템에 Log Insight Windows Agent 배포](#)
- [vRealize Log Insight Linux 에이전트 RPM 패키지 설치 또는 업데이트](#)
- [vRealize Log Insight Linux 에이전트 DEB 패키지 설치 또는 업데이트](#)
- [Log Insight Linux Agent 이전 패키지 설치](#)

## Windows 또는 Linux 에이전트 파일 다운로드

vRealize Log Insight 에이전트를 설치하고 구성하기 전에 에이전트 파일을 다운로드해야 합니다.

vRealize Log Insight 서버 에이전트 페이지에서 다운로드하는 모든 패키지에는 대상 호스트 이름이 포함됩니다. 서버 호스트 이름은 MSI, RPM 및 DEB 에이전트의 초기 설치 시 적용됩니다. 구성 파일에 호스트 이름이 이미 있거나, 호스트 이름 매개 변수를 사용하여 패키지를 실행하는 경우에는 포함된 서버 호스트 이름이 무시됩니다.

### 절차

- 1 vRealize Log Insight 웹 사용자 인터페이스의 **관리** 페이지로 이동합니다.
- 2 관리 섹션에서 **에이전트**를 클릭합니다.

### 3 Log Insight 에이전트 다운로드를 클릭하고 다운로드할 에이전트 파일을 선택합니다.

옵션	설명
Windows MSI	Windows MSI(32비트/64비트)
Linux RPM	Linux RPM(32비트/64비트)
Linux DEB	Linux DEB(32비트/64비트)
Linux BIN	Linux BIN(32비트/64비트)

다음에 수행할 작업

다운로드한 파일을 사용하여 vRealize Log Insight 에이전트를 배포합니다.

## 기본 구성으로 vRealize Log Insight Windows 에이전트 설치

명령줄 매개 변수를 구성하지 않고 vRealize Log Insight Windows 에이전트를 설치할 수 있습니다.

사전 요구 사항

- vRealize Log Insight Windows 에이전트 .msi 파일의 복사본이 있는지 확인합니다. [Windows 또는 Linux 에이전트 파일 다운로드](#) 항목을 참조하십시오.
- 설치를 수행할 수 있는 사용 권한이 있으며 Windows 시스템에서 서비스를 시작했는지 확인합니다.

절차

- 1 로그 vRealize Log Insight Windows 에이전트를 설치할 Windows 시스템에 로그인합니다.
- 2 vRealize Log Insight Windows 에이전트 .msi 파일이 있는 디렉토리로 변경합니다.
- 3 vRealize Log Insight Windows 에이전트 .msi 파일을 두 번 클릭하고 라이선스 계약 내용에 동의한 후 **다음**을 클릭합니다.
- 4 vRealize Log Insight 서버의 IP 주소 또는 호스트 이름을 입력하고 **설치**를 클릭합니다.  
vRealize Log Insight Windows 에이전트가 LocalSystem 서비스 계정 아래에 자동 Windows 서비스로 설치됩니다.
- 5 **완료**를 클릭합니다.

다음에 수행할 작업

liagent.ini 파일을 편집하여 vRealize Log Insight Windows 에이전트를 구성합니다. [설치 후 Log Insight Windows Agent 구성](#) 을 참조하십시오.

# vRealize Log Insight Windows 에이전트 설치, 업데이트 및 구성

vRealize Log Insight Windows 에이전트를 설치 또는 업데이트하고, 서비스 계정을 지정하고, 서버, 포트 및 프로토콜에 대한 명령줄 매개 변수를 구성할 수 있습니다.

MSI 명령줄 옵션에 대한 자세한 내용은 MSDN(Microsoft Developer Network) 라이브러리 웹 사이트에서 MSI 명령줄 옵션을 검색하여 참조하십시오.

## 사전 요구 사항

- vRealize Log Insight Windows 에이전트 .msi 파일의 복사본이 있는지 확인합니다. [Windows 또는 Linux 에이전트 파일 다운로드](#) 항목을 참조하십시오.
- 설치를 수행할 수 있는 사용 권한이 있으며 Windows 시스템에서 서비스를 시작했는지 확인합니다.
- 자동 설치 옵션 /quiet 또는 /qn을 사용하는 경우 관리자로 설치 프로그램을 실행하는지 확인하십시오. 관리자가 아닌 사용자가 자동 설치를 실행하는 경우 설치가 관리자 권한을 요청하지 않고 실패합니다. 진단 목적으로 로깅 옵션 및 매개 변수 /!xv\* file\_name을 사용하십시오.

## 절차

- 1 vRealize Log Insight Windows 에이전트를 설치 또는 업데이트할 Windows 시스템에 로그인합니다.
- 2 **명령 프롬프트** 창을 엽니다.
- 3 vRealize Log Insight Windows 에이전트 .msi 파일이 있는 디렉토리로 변경합니다.
- 4 명령을 실행하여 설치 또는 업데이트를 시작하고 *Version-Build\_Number*를 사용자의 버전 및 빌드 번호로 바꿉니다.

```
Drive:\path-to-msi_file>VMware-Log-Insight-Agent-Version-Build_Number.msi
```

```
Drive:\path-to-msi_file>VMware-Log-Insight-Agent-30.msi.
```

- 5 (선택 사항) vRealize Log Insight Windows 에이전트 서비스를 실행할 사용자 서비스 계정을 지정합니다.

```
Drive:\path-to-msi_file>VMware-Log-Insight-Agent-*.msi SERVICEACCOUNT=domain\user
SERVICEPASSWORD=user_password
```

**참고** SERVICEACCOUNT 매개 변수에 제공되는 계정에는 **서비스로 로그인** 권한 및 %ProgramData%\VMware\Log Insight Agent 디렉토리에 대한 전체 쓰기 액세스 권한이 부여됩니다. 지원되는 계정이 없으면 새로 생성됩니다. 사용자 이름은 20자를 초과해서는 안 됩니다. SERVICEACCOUNT 매개 변수를 지정하지 않으면 vRealize Log Insight Windows 에이전트 서비스가 LocalSystem 서비스 계정 아래에 설치 또는 업데이트됩니다.

## 6 (선택 사항) vRealize Log Insight 서버, 포트 및 프로토콜을 입력합니다.

매개 변수	설명
SERVERHOST	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
SERVERPROTO	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 cfapi 및 syslog입니다. 기본 cfapi 설정을 사용하십시오.
SERVERPORT	포트 번호는 SERVERPROTO의 값에 따라 달라집니다. SERVERPORT의 기본값은 9000이며 이는 기본 SERVERPROTO=cfapi과 동일합니다. SERVERPROTO=syslog에는 SERVERPORT=514를 사용하십시오.

명령줄 매개 변수는 liagent.ini 파일의 [server] 섹션에 있는 hostname, proto 및 port에 해당합니다.

## 7 Enter를 누릅니다.

명령이 vRealize Log Insight Windows 에이전트를 Windows 서비스로 설치 또는 업데이트합니다. vRealize Log Insight Windows 에이전트 서비스는 Windows 시스템이 시작될 때 시작됩니다.

다음에 수행할 작업

설정된 명령줄 매개 변수가 liagent.ini 파일에 올바르게 적용되었는지 확인합니다. [설치 후 Log Insight Windows Agent 구성](#) 을 참조하십시오.

## 여러 시스템에 Log Insight Windows Agent 배포

Windows 도메인에 있는 여러 대상 시스템에 Log Insight Windows Agent를 배포할 수 있습니다.

## 변환 .mst 파일을 사용하여 vRealize Log Insight Windows 에이전트 배포

배포 도중 사용할 설치 매개 변수를 지정하려면 .mst 변환 파일을 생성합니다. vRealize Log Insight 서버로 이벤트를 보내고 Log Insight 에이전트 서비스 설치 및 시작에 필요한 통신 프로토콜, 포트 및 사용자 계정을 설정하도록 vRealize Log Insight Windows 에이전트를 구성할 수 있습니다.

사전 요구 사항

- vRealize Log Insight Windows .msi 파일의 복사본이 있는지 확인합니다. [Windows 또는 Linux 에이전트 파일 다운로드](#)를 참조하십시오.
- Orca 데이터베이스 편집기를 다운로드하여 설치합니다. <http://support.microsoft.com/kb/255905>를 참조하십시오.

절차

- 1 Orca 편집기에서 vRealize Log Insight Windows 에이전트 .msi 파일을 열고 **Transform > New Transform**을 선택합니다.

- 2 속성 테이블을 편집하고 사용자 지정된 설치 또는 업그레이드를 위해 필요한 매개 변수 및 값을 추가합니다.

매개 변수	설명
SERVERHOST	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
SERVERPROTO	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 cfapi 및 syslog입니다. 기본 cfapi 설정을 사용하십시오.
SERVERPORT	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 통신 포트입니다. 기본값은 SSL이 사용되는 cfapi의 경우 9543, SSL이 사용되지 않는 cfapi의 경우 9000, SSL이 사용되는 syslog의 경우 6514, SSL이 사용되지 않는 syslog의 경우 514입니다.
SERVICEACCOUNT	Log Insight Windows Agent 서비스를 실행할 사용자 서비스 계정입니다.  <b>참고</b> 설치 관리자가 제대로 실행되려면 SERVICEACCOUNT 매개 변수에 제공된 계정에 <b>서비스로 로그인</b> 권한 및 %ProgramData%\VMware\Log Insight Agent 디렉토리에 대한 쓰기 액세스 권한이 있어야 합니다. SERVICEACCOUNT 매개 변수를 지정하지 않으면 vRealize Log Insight Windows 에이전트 서비스가 LocalSystem 서비스 계정 아래에 설치됩니다.
SERVICEPASSWORD	사용자 서비스 계정의 암호입니다.

- 3 **Transform > Generate Transform**을 선택하고 .mst 파일을 저장합니다.

다음에 수행할 작업

.msi 및 .mst 파일을 사용하여 vRealize Log Insight Windows 에이전트를 배포합니다.

## vRealize Log Insight Windows 에이전트의 여러 인스턴스 배포

vRealize Log Insight Windows 에이전트의 여러 인스턴스를 Windows 도메인 내의 대상 컴퓨터에 배포할 수 있습니다.

클라이언트 시스템을 두 번 재부팅해야 하는 이유에 대해서는 [support.microsoft.com/kb/305293](http://support.microsoft.com/kb/305293)을 참조하십시오.

### 사전 요구 사항

- 도메인 컨트롤러에 대한 관리자 계정 또는 관리 권한이 있는 계정을 보유하고 있는지 확인합니다.
- vRealize Log Insight Windows 에이전트 .msi 파일의 복사본이 있는지 확인합니다. [Windows 또는 Linux 에이전트 파일 다운로드](#)를 참조하십시오.
- <http://support.microsoft.com/kb/887405> 및 <http://support.microsoft.com/kb/816102>에 설명된 절차를 숙지합니다.

### 절차

- 1 관리자 계정 또는 관리 권한이 있는 계정으로 도메인 컨트롤러에 로그인합니다.
- 2 배포 지점을 생성하고 해당 배포 지점에 vRealize Log Insight Windows 에이전트 .msi 파일을 복사합니다.

- 3 그룹 정책 관리 콘솔을 열고 vRealize Log Insight Windows 에이전트 .msi 파일을 배포하기 위한 그룹 정책 개체를 생성합니다.
- 4 소프트웨어 배포용 그룹 정책 개체를 편집하고 패키지를 할당합니다.
- 5 (선택 사항) 배포 전에 .mst 파일을 생성한 경우 **GPO 속성** 창의 **수정** 탭에서 .mst 구성 파일을 선택합니다. 그리고 고급 방법을 사용하여 .msi 패키지를 배포할 그룹 정책 개체를 편집합니다.
- 6 (선택 사항) vRealize Log Insight Windows 에이전트를 업그레이드합니다.
  - a 업그레이드 .msi 파일을 배포 지점에 복사합니다.
  - b 그룹 정책 개체 **속성** 창에서 **업그레이드** 탭을 클릭합니다.
  - c 처음 설치된 버전의 .msi 파일을 업그레이드 대상 섹션에 있는 패키지에 추가합니다.
- 7 도메인 사용자가 포함된 특정 보안 그룹에 vRealize Log Insight Windows 에이전트를 배포합니다.
- 8 도메인 컨트롤러에서 모든 그룹 정책 관리 콘솔 및 그룹 정책 관리 편집기 창을 닫고 클라이언트 시스템을 다시 시작합니다.  
빠른 로그인 최적화가 사용하도록 설정된 경우 클라이언트 시스템을 두 번 재부팅합니다.
- 9 vRealize Log Insight Windows 에이전트가 클라이언트 시스템에 로컬 서비스로 설치되었는지 확인합니다.  
vRealize Log Insight Windows 에이전트의 여러 인스턴스를 배포하기 위해 .mst 파일을 사용하도록 SERVICEACCOUNT 및 SERVICEPASSWORD 매개 변수를 구성한 경우, vRealize Log Insight Windows 에이전트가 지정된 사용자 계정으로 클라이언트 시스템에 설치되었는지 확인합니다.

#### 다음에 수행할 작업

vRealize Log Insight Windows 에이전트의 여러 인스턴스가 제대로 작동하지 않는 경우 [Log Insight Windows Agent의 대량 배포가 실패함](#) 항목을 참조하십시오.

## vRealize Log Insight Linux 에이전트 RPM 패키지 설치 또는 업데이트

vRealize Log Insight Linux 에이전트를 루트 또는 루트가 아닌 사용자로 설치하거나 업데이트할 수 있으며 설치 도중 대상 서버를 설정할 수 있습니다. 설치 후 설치된 버전을 확인할 수 있습니다.

#### 사전 요구 사항

- **루트**로 로그인하거나 **sudo**를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트가 작동하려면 syslog 및 네트워킹 서비스에 대한 액세스 권한이 있어야 합니다. vRealize Log Insight Linux 에이전트를 설치하고 실행 수준 3 및 5에서 실행합니다. vRealize Log Insight Linux 에이전트를 다른 실행 수준에서 작동하려면 시스템을 그에 맞게 구성합니다.

## 절차

- 1 콘솔을 열고 `rpm -i package_name` 명령을 실행하여 vRealize Log Insight Linux 에이전트를 설치합니다.

`package_name`을 적합한 버전으로 바꿉니다.

```
rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

## 참고

```
sudo SERVERHOST=hostname rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

- 2 설치 도중 대상 vRealize Log Insight 서버를 설정하려면 `sudo` 명령을 실행하고 `hostname`을 vRealize Log Insight 서버의 IP 주소 또는 호스트 이름으로 바꿉니다.

```
sudo SERVERHOST=hostname rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

- 3 (선택 사항) vRealize Log Insight Linux 에이전트를 업데이트하려면 `rpm -Uhv` 명령을 실행합니다.

```
rpm -Uhv VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

**참고** vRealize Log Insight Linux 에이전트 RPM 패키지를 설치, 업데이트 또는 제거하는 동안 `-h`, `--hash`, `--version`, `--allfiles` 등의 다른 RPM 명령을 실행할 수 있지만 지원되지 않습니다.

- 4 (선택 사항) **루트가 아닌** 사용자로 vRealize Log Insight Linux 에이전트를 설치하려면 `sudo` 명령을 실행합니다.

```
sudo LIAGENTUSER=liagent rpm -i VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER.rpm
```

지정한 사용자가 없는 경우 vRealize Log Insight Linux 에이전트가 설치 도중 해당 사용자 계정을 생성합니다. 생성된 계정은 Agent를 제거해도 삭제되지 않습니다. `LIAGENTUSER=non_root_user` 매개 변수로 vRealize Log InsightLinux 에이전트를 설치하고 `LIAGENTUSER=non_root_user2`로 업그레이드하려고 하면 `non_root_user2` 사용자에게는 `non_root_user` 사용자의 사용 권한이 없으므로 충돌이 발생하고 경고가 표시됩니다.

- 5 (선택 사항) 적절한 버전의 RPM 패키지를 두 번 클릭하여 vRealize Log InsightLinux 에이전트를 설치 또는 업데이트합니다.
- 6 (선택 사항) `rpm -qa | grep Log-Insight-Agent` 명령을 실행하여 설치된 버전을 확인합니다.

## vRealize Log Insight Linux 에이전트 DEB 패키지 설치 또는 업데이트

vRealize Log Insight Linux 에이전트 DEB 패키지를 설치하거나 업데이트할 때는 설치 도중 대상 서버를 설정하고 `liagent.ini` 구성 파일을 유지하거나 바꿀 수 있습니다. 설치 후 설치된 버전을 확인할 수 있습니다.

## 사전 요구 사항

- **루트**로 로그인하거나 `sudo`를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트에 `syslog` 및 네트워크 서비스에 대한 액세스 권한(에이전트 작동에 필요함)이 있는지 확인합니다. 기본적으로 vRealize Log Insight Linux 에이전트는 실행 수준 2, 3, 4 및 5에서 실행하고 실행 수준 0, 1 및 6에서 중지합니다.

## 절차

- 1 콘솔을 열고 `dpkg -i package_name` 명령을 실행하여 vRealize Log Insight Linux 에이전트를 설치 또는 업데이트합니다.

`package_name`을 적합한 버전으로 바꿉니다.

```
dpkg -i vmware-log-insight-agent-버전-빌드 번호_all.deb
```

- 2 설치 도중 대상 vRealize Log Insight 서버를 설정하려면 `sudo` 명령을 실행하고 `hostname`을 vRealize Log Insight 서버의 IP 주소 또는 호스트 이름으로 바꿉니다.

```
sudo SERVERHOST=hostname dpkg -i vmware-log-insight-agent-버전-빌드 번호_all.deb
```

설치 도중 `--force-confold` 플래그를 사용하도록 설정한 경우 이외에는 새 버전으로 업데이트할 때마다 시스템이 `liagent.ini` 구성 파일을 유지할지 아니면 바꿀지 물어봅니다. 다음의 시스템 메시지가 나타납니다.

```
Configuration file `/var/lib/loginsight-agent/liagent.ini'
==> Modified (by you or by a script) since installation.
==> Package distributor has shipped an updated version.
What would you like to do about it ? Your options are:
  Y or I : install the package maintainer's version
  N or O : keep your currently-installed version
  D      : show the differences between the versions
  Z      : start a shell to examine the situation
The default action is to keep your current version.
*** liagent.ini (Y/I/N/O/D/Z) [default=N] ?
```

- 3 (선택 사항) 기존 구성을 유지하려면 `[default=N]`을 사용하십시오. 명령줄에서 전달된 추가적인 매개 변수는 계속 적용됩니다.
- 4 (선택 사항) **루트가 아닌** 사용자로 vRealize Log Insight Linux 에이전트를 실행하려면 `sudo` 명령을 실행합니다.

```
sudo LIAGENTUSER=liagent dpkg -i vmware-log-insight-agent-버전-빌드 번호_all.deb
```

지정한 사용자가 없는 경우 vRealize Log Insight Linux 에이전트가 설치 도중 해당 사용자 계정을 생성합니다. 생성된 계정은 Agent를 제거해도 삭제되지 않습니다. `LIAGENTUSER=non_root_user` 매개 변수로 vRealize Log Insight Linux 에이전트를 설치하고 `LIAGENTUSER=non_root_user2` 매개 변수로 업그레이드하려고 하면 `non_root_user2` 사용자에게는 `non_root_user` 사용자의 사용 권한이 없으므로 충돌이 발생하고 경고가 표시됩니다.



- 5 (선택 사항) `dpkg -l | grep -i vmware-log-insight-agent` 명령을 실행하여 설치된 버전을 확인합니다.

## Log Insight Linux Agent 이진 패키지 설치

이진 패키지를 설치할 때는 .bin 파일을 실행 파일로 변경한 다음 에이전트를 설치하는 과정이 포함됩니다.

.bin 패키지를 업그레이드하는 것은 공식적으로 지원되지 않습니다. .bin 패키지를 사용하여 기존 Log Insight Linux Agent를 설치한 경우 `/var/lib/loginsight-agent` 디렉토리에 있는 `liagent.ini` 파일의 백업 복사본을 만들어 로컬 구성을 유지하십시오. 백업 복사본을 만든 후 Log Insight Linux Agent를 수동으로 제거합니다. [Log Insight Linux Agent Bin 패키지 제거](#)를 참조하십시오.

.bin 패키지를 사용하여 Linux 에이전트를 설치하는 경우 패키지 설치의 일부로 `liagentd`라는 이름의 `init.d` 스크립트가 설치되지만 패키지는 스크립트를 등록하지 않습니다. 스크립트를 수동으로 등록할 수 있습니다.

`(/sbin/)service liagentd status` 명령을 실행하여 성공적으로 설치되었는지 확인할 수 있습니다.

### 사전 요구 사항

- Log Insight Linux Agent .bin 패키지를 다운로드하여 대상 Linux 시스템에 복사합니다.
- **루트**로 로그인하거나 `sudo`를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent에 `syslog` 및 네트워킹 서비스에 대한 액세스 권한이 있는지 확인합니다.

### 절차

- 1 콘솔을 열고 `chmod` 명령을 실행하여 .bin 파일을 실행 파일로 변경합니다.

*filename-version*을 적합한 버전으로 바꿉니다.

```
chmod +x filename-version.bin
```

- 2 `./filename-version.bin` 명령을 실행하여 에이전트를 설치합니다.

*filename-version*을 적합한 버전으로 바꿉니다.

### 참고

```
sudo SERVERHOST=hostname ./filename-version.bin
```

- 3 설치 도중 대상 vRealize Log Insight 서버를 설정하려면 `sudo SERVERHOST=hostname ./filename-version.bin` 명령을 실행합니다.

*hostname*을 vRealize Log Insight 서버의 IP 주소 또는 호스트 이름으로 바꿉니다.

- 4 (선택 사항) **루트 이외**의 사용자로 Log Insight Linux Agent를 실행하려면 `sudo` 명령을 실행합니다.

```
sudo LIAGENTUSER=liagent ./filename-version.bin
```

지정된 사용자가 없는 경우 Log Insight Linux Agent가 설치 도중 해당 사용자 계정을 생성합니다. 생성된 계정은 Agent를 제거해도 삭제되지 않습니다. `LIAGENTUSER=non_root_user` 매개 변수로 Log Insight Linux Agent를 설치하고 `LIAGENTUSER=non_root_user2` 매개 변수로 업그레이드하려고 하면 `non_root_user2` 사용자에게는 `non_root_user` 사용자의 사용 권한이 없으므로 충돌이 발생하고 경고가 표시됩니다.

# vRealize Log Insight 에이전트 구성

## 3

에이전트를 배포한 후에는 선택한 vRealize Log Insight 서버에 이벤트를 보내도록 구성하고 통신 프로토콜을 지정하는 등의 작업을 할 수 있습니다.

필요에 따라 이 지침을 사용하여 에이전트를 필요에 맞게 구성하십시오.

### ■ 설치 후 Log Insight Windows Agent 구성

설치 이후 Log Insight Windows Agent를 구성할 수 있습니다. 선택한 vRealize Log Insight 서버로 이벤트를 보내고 통신 프로토콜 및 포트를 설정하고 Windows 이벤트 채널을 추가하고 플랫폼 파일 로그 수집을 구성하도록 Log Insight Windows Agent를 구성하려면 `liagent.ini` 파일을 편집해야 합니다.

### ■ Log Insight Linux Agent 구성

Log Insight Linux Agent를 설치한 이후에 구성할 수 있습니다. `liagent.ini` 파일은 `/var/lib/loginsight-agent/`에 위치합니다. 선택한 vRealize Log Insight 서버로 이벤트를 보내고 통신 프로토콜 및 포트를 설정하고 플랫폼 파일 로그 수집을 구성하도록 Log Insight Linux Agent를 구성하려면 이 파일을 편집해야 합니다.

### ■ vRealize Log Insight 에이전트의 중앙 집중식 구성

다수의 Windows 또는 Linux vRealize Log Insight 에이전트를 구성할 수 있습니다.

### ■ 로그 구문 분석

에이전트 측 로그 구문 분석기는 원시 로그에서 구조화된 데이터를 추출하여 vRealize Log Insight 서버에 제공합니다. vRealize Log Insight는 로그 구문 분석기를 사용하여 로그를 분석하고, 여기에서 정보를 추출하고, 해당 결과를 서버에 표시할 수 있습니다. 로그 구문 분석기는 Windows 및 Linux vRealize Log Insight 에이전트 모두에 대해 구성할 수 있습니다.

## 설치 후 Log Insight Windows Agent 구성

설치 이후 Log Insight Windows Agent를 구성할 수 있습니다. 선택한 vRealize Log Insight 서버로 이벤트를 보내고 통신 프로토콜 및 포트를 설정하고 Windows 이벤트 채널을 추가하고 플랫폼 파일 로그 수집을 구성하도록 Log Insight Windows Agent를 구성하려면 `liagent.ini` 파일을 편집해야 합니다.

## Log Insight Windows Agent의 기본 구성

설치를 마치면 liagent.ini 파일에 Log Insight Windows Agent에 대해 미리 구성된 기본 설정이 포함됩니다.

### Log Insight Windows Agent liagent.ini 기본 구성

ASCII가 아닌 이름과 값을 사용하는 경우 구성을 UTF-8로 저장합니다.

최종 구성은 이 파일과 서버의 구성을 결합한 것으로 liagent-effective.ini 파일을 형성합니다.

서버의 에이전트 페이지에서 설정을 구성하는 것이 더 효율적일 수 있습니다.

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
; Example of configuration with trusted CA:
;ssl=yes
;ssl_ca_path=/etc/pki/tls/certs/ca.pem

; Time in minutes to force reconnection to the server.
; This option mitigates imbalances caused by long-lived TCP connections. Default:
;reconnect=30

[logging]
; Logging verbosity: 0 (no debug messages), 1 (essentials), 2 (verbose with more impact on performance).
; This option should always be 0 under normal operating conditions. Default:
;debug_level=0

[storage]
; Max local storage usage limit (data + logs) in MBs. Valid range: 100-2000 MB.
;max_disk_buffer=200

; Uncomment the following sections to collect these channels.
; The recommended way is to enable Windows content pack from LI server.
;[winlog|Application]
;channel=Application

;[winlog|Security]
;channel=Security

;[winlog|System]
```

;channel=System

매개 변수	값	설명
proto	cfapi	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 cfapi 및 syslog입니다. 기본 cfapi 설정을 사용하십시오.
hostname	LOGINSIGHT	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
port	9543, 9000, 6514 및 514	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 통신 포트입니다. 기본값은 SSL이 사용되는 cfapi의 경우 9543, SSL이 사용되지 않는 cfapi의 경우 9000, SSL이 사용되는 syslog의 경우 6514, SSL이 사용되지 않는 syslog의 경우 514입니다.
ssl	yes	SSL을 사용하거나 사용하지 않도록 설정합니다. 기본값은 yes입니다. ssl을 [yes]로 설정하고 포트 값을 설정하지 않은 경우 포트 9543이 자동으로 선택됩니다.
max_disk_buffer	200	Log Insight Windows Agent에서 이벤트 및 자체 로그를 버퍼링하는 데 사용하는 MB 단위의 최대 디스크 공간입니다. 지정된 max_disk_buffer에 도달하면 에이전트를 새로 들어오는 이벤트를 삭제하기 시작합니다.
debug_level	0	로그 세부 정보 수준을 정의합니다. <a href="#">Log Insight Agents의 로그 세부 정보 수준 정의</a> 항목을 참조하십시오.
channel	애플리케이션, 보안, 시스템	애플리케이션, 보안 및 시스템 Windows 이벤트 로그 채널은 기본적으로 주석 처리되며 Log Insight Windows Agent는 이러한 채널의 로그를 수집하지 않습니다. <a href="#">Windows 이벤트 채널에서 이벤트 수집 항목을 참조하십시오.</a>

## 대상 vRealize Log Insight 서버 설정

설치 프로세스 동안 값을 설정하지 않은 경우 vRealize Log Insight Windows 에이전트가 보내는 이벤트를 수신할 대상 vRealize Log Insight 서버를 설정하거나 변경할 수 있습니다.

### 사전 요구 사항

- vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자 자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

- 통합된 로드 밸런서를 사용하는 vRealize Log Insight 클러스터가 있는 경우 사용자 지정 SSL 인증서 관련 요구 사항은 [통합된 로드 밸런서 사용](#)을 참조하십시오.

## 절차

- 1 vRealize Log Insight Windows 에이전트의 프로그램 데이터 폴더로 이동합니다.  
%ProgramData%\VMware\Log Insight Agent
- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.
- 3 다음 매개 변수를 수정하고 환경에 맞게 값을 설정합니다.

매개 변수	설명
proto	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 cfapi 및 syslog입니다. 기본 cfapi 설정을 사용하십시오.
hostname	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다. IPv4 또는 IPv6 주소를 지정할 수 있습니다. IPv6 주소는 대괄호를 사용하거나 사용하지 않고 지정할 수 있습니다. 예:  <pre>hostname = 2001:cdba::3257:9652 or hostname = [2001:cdba::3257:9652]</pre> 호스트가 IPv4 스택과 IPv6 스택 모두를 지원하고 도메인 이름을 호스트 이름으로 지정한 경우, 에이전트는 이름 확인 프로그램이 반환하는 IP 주소에 기반하여 적절한 IP 스택을 사용합니다. 확인 프로그램이 IPv4 주소와 IPv6 주소 둘 모두 반환하면 에이전트는 주어진 순서대로 두 주소에 순차적으로 연결을 시도합니다.
port	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 통신 포트입니다. 기본값은 SSL이 사용되는 cfapi의 경우 9543, SSL이 사용되지 않는 cfapi의 경우 9000, SSL이 사용되는 syslog의 경우 6514, SSL이 사용되지 않는 syslog의 경우 514입니다.
ssl	SSL을 사용하거나 사용하지 않도록 설정합니다. 기본값은 yes입니다. ssl을 [yes]로 설정하고 포트 값을 설정하지 않은 경우 포트 9543이 자동으로 선택됩니다.
reconnect	강제로 서버에 다시 연결하는 시간(분)입니다. 기본값은 30입니다.

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOG/NSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
```

```
;port=9543

; SSL usage. Default:
;ssl=yes
```

4 liagent.ini 파일을 저장한 후 닫습니다.

## 예제: 구성

다음 구성 예에서는 신뢰할 수 있는 CA(인증 기관)를 사용하는 대상 vRealize Log Insight 서버를 설정합니다.

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem
```

다음에 수행할 작업

vRealize Log Insight Windows 에이전트에 대한 추가 SSL 옵션을 구성할 수 있습니다. [서버와 Log Insight Agent 사이의 SSL 연결 구성](#)을 참조하십시오.

## Windows 이벤트 채널에서 이벤트 수집

Windows 이벤트 채널을 Log Insight Windows Agent 구성에 추가할 수 있습니다. 그러면 Log Insight Windows Agent에서 이벤트를 수집하여 vRealize Log Insight 서버로 보냅니다.

필드 이름은 제한됩니다. 다음 필드 이름은 예약된 것이므로 필드 이름으로 사용할 수 없습니다.

- event\_type
- hostname
- source
- text

### 사전 요구 사항

vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

### 절차

- 1 vRealize Log Insight Windows 에이전트의 프로그램 데이터 폴더로 이동합니다.  
%ProgramData%\VMware\Log Insight Agent
- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.

### 3 다음 매개 변수를 추가하고 환경에 맞게 값을 설정합니다.

매개 변수	설명
<code>[winlog  <i>section_name</i> ]</code>	구성 섹션의 고유 이름입니다.
<code>channel</code>	Windows 애플리케이션에 기본 제공되는 이벤트 뷰어에 표시된 이벤트 채널의 전체 이름입니다. 정확한 채널 이름을 복사하려면 이벤트 뷰어에서 채널을 마우스 오른쪽 버튼으로 클릭하고 <b>속성</b> 을 선택한 후 <b>전체 이름</b> 필드의 콘텐츠를 복사합니다.
<code>enabled</code>	구성 섹션을 사용 또는 사용하지 않도록 설정하는 선택적 매개 변수입니다. 가능한 값은 yes 또는 no입니다(대/소문자를 구분하지 않음). 기본값은 yes입니다.
<code>tags</code>	수집된 이벤트의 필드에 사용자 지정 태그를 추가하는 선택적 매개 변수입니다. JSON 표기법을 사용하여 태그를 정의해야 합니다. 태그 이름에는 문자, 숫자 및 밑줄을 포함할 수 있습니다. 태그 이름은 문자 또는 밑줄로만 시작할 수 있으며 64자를 초과할 수 없습니다. 태그 이름은 대/소문자를 구분하지 않습니다. 예를 들어 <code>tags={"tag_name1": "tag value 1", "Tag_Name1": "tag value 2" }</code> 를 사용하면 Tag_Name1은 중복 항목으로 무시됩니다. 태그 이름으로 <code>event_type</code> 및 <code>timestamp</code> 를 사용할 수 없습니다. 동일한 선언 내의 중복 항목은 무시됩니다.  대상이 syslog 서버인 경우 태그는 APP-NAME 필드를 재정의합니다. 예를 들어 <code>tags={"appname": "VROPS"}</code> 일 수 있습니다.
<code>whitelist, blacklist</code>	로그 이벤트를 명시적으로 포함 또는 제외하는 선택적 매개 변수입니다.  <b>참고</b> blacklist 옵션은 필드에만 작동하며 blacklist 텍스트에 사용할 수 없습니다.
<code>exclude_fields</code>	(선택 사항) 수집 대상에서 개별 필드를 제외하는 매개 변수입니다. 여러 값은 세미콜론으로 구분된 목록으로 제공할 수 있습니다. 예를 들면 다음과 같습니다. <code>exclude_fields=EventId; ProviderName</code>

```
[winlog|section_name]
channel=event_channel_name
enabled=yes_or_no
tags={"tag_name1": "Tag value 1", "tag_name2": "tag value 2" }
```

### 4 liagent.ini 파일을 저장한 후 닫습니다.

#### 예제: 구성

다음 [winlog] 구성 예를 참조하십시오.

```
[winlog|Events_Firewall ]
channel=Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
enabled=no
```

```
[winlog|custom]
channel=Custom
tags={"ChannelDescription": "Events testing channel"}
```



## Windows 이벤트 채널에 대한 필터링 설정

Windows 이벤트 채널에 대한 필터를 설정하여 로그 이벤트를 명시적으로 포함하거나 제외할 수 있습니다.

whitelist 및 blacklist 매개 변수를 사용하여 필터 식을 평가할 수 있습니다. 필터 식은 이벤트 필드 및 연산자로 구성된 부울 식입니다.

**참고** blacklist 옵션은 필드에만 작동하며 blacklist 텍스트에 사용할 수 없습니다.

- whitelist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트만 수집합니다. whitelist을 생략하면 값은 암시적으로 1이 됩니다.
- blacklist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트를 제외합니다. 기본값은 0입니다.

Windows 이벤트 필드 및 연산자의 전체 목록은 [이벤트 필드 및 연산자](#) 항목을 참조하십시오.

### 사전 요구 사항

vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

### 절차

- 1 vRealize Log Insight Windows 에이전트의 프로그램 데이터 폴더로 이동합니다.

```
%ProgramData%\VMware\Log Insight Agent
```

- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.

- 3 [winlog] 섹션에 whitelist 또는 blacklist 매개 변수를 추가합니다.

예를 들면 다음과 같습니다.

```
[winlog|unique_section_name]
channel = event_channel_name
blacklist = filter_expression
```

- 4 Windows 이벤트 필드 및 연산자를 기반으로 필터 식을 생성합니다.

예를 들면 다음과 같습니다.

```
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

- 5 liagent.ini 파일을 저장한 후 닫습니다.

### 예제: 필터 구성

다음과 같이 오류 이벤트만 수집하도록 에이전트를 구성할 수 있습니다.

```
[winlog|Security-Error]
channel = Security
whitelist = Level == WINLOG_LEVEL_CRITICAL or Level == WINLOG_LEVEL_ERROR
```

다음과 같이 애플리케이션 채널에서 VMware 네트워크 이벤트만 수집하도록 에이전트를 구성할 수 있습니다.

```
[winlog|VMwareNetwork]
channel = Application
whitelist = ProviderName == "VMnetAdapter" or ProviderName == "VMnetBridge" or ProviderName == "VMnetDHCP"
```

다음과 같이 보안 채널에서 특정 이벤트를 제외한 모든 이벤트를 수집하도록 에이전트를 구성할 수 있습니다.

```
[winlog|Security-Verbose]
channel = Security
blacklist = EventID == 4688 or EventID == 5447
```

## 이벤트 필드 및 연산자

Windows 이벤트 필드 및 연산자를 사용하여 필터 식을 작성할 수 있습니다.

### 필터 식 연산자

연산자	설명
==, !=	같음 및 같지 않음. 숫자 필드 및 문자열 필드 모두에 사용할 수 있습니다.
>=, >, <, <=	크거나 같음, 보다 큼, 보다 작음, 작거나 같음. 숫자 필드에만 사용할 수 있습니다.
&,  , ^, ~	비트 AND, OR, XOR 및 보수 연산자. 숫자 필드에만 사용할 수 있습니다.
and, or	논리 AND 및 OR. 단순 식을 결합하여 복합 식을 작성하는 데 사용합니다.
아님	단항 논리 NOT 연산자. 식의 값을 반전하는 데 사용합니다.
()	연산 순서를 변경하기 위해 논리 식에 괄호를 사용합니다.

### Windows 이벤트 필드

필터 식에 다음 Windows 이벤트 필드를 사용할 수 있습니다.

필드 이름	필드 유형
호스트 이름	문자열
텍스트	문자열
ProviderName	문자열
EventSourceName	문자열
EventID	숫자
EventRecordID	숫자
채널	문자열
UserID	문자열

필드 이름	필드 유형
수준	숫자 다음과 같은 미리 정의된 상수를 사용할 수 있습니다. <ul style="list-style-type: none"> <li>■ WINLOG_LEVEL_SUCCESS = 0</li> <li>■ WINLOG_LEVEL_CRITICAL = 1</li> <li>■ WINLOG_LEVEL_ERROR = 2</li> <li>■ WINLOG_LEVEL_WARNING = 3</li> <li>■ WINLOG_LEVEL_INFO = 4</li> <li>■ WINLOG_LEVEL_VERBOSE = 5</li> </ul>
작업	숫자
OpCode	숫자
키워드	숫자 다음과 같은 미리 정의된 비트 마스크를 사용할 수 있습니다. <ul style="list-style-type: none"> <li>■ WINLOG_KEYWORD_RESPONSETIME = 0x0001000000000000;</li> <li>■ WINLOG_KEYWORD_WDICONTEXT = 0x0002000000000000;</li> <li>■ WINLOG_KEYWORD_WDIDIAGNOSTIC = 0x0004000000000000;</li> <li>■ WINLOG_KEYWORD_SQM = 0x0008000000000000;</li> <li>■ WINLOG_KEYWORD_AUDITFAILURE = 0x0010000000000000;</li> <li>■ WINLOG_KEYWORD_AUDITSUCCESS = 0x0020000000000000;</li> <li>■ WINLOG_KEYWORD_CORRELATIONHINT = 0x0040000000000000;</li> <li>■ WINLOG_KEYWORD_CLASSIC = 0x0080000000000000;</li> </ul>

## 예

다음은 모든 중요, 오류 및 경고 이벤트를 수집합니다.

```
[winlog|app]
channel = Application
whitelist = level > WINLOG_LEVEL_SUCCESS and level < WINLOG_LEVEL_INFO
```

다음은 보안 채널에서 감사 실패 이벤트만 수집합니다.

```
[winlog|security]
channel = Security
whitelist = Keywords & WINLOG_KEYWORD_AUDITFAILURE
```

## 로그 파일에서 이벤트 수집

하나 이상의 로그 파일에서 이벤트를 수집하도록 vRealize Log Insight Windows 에이전트를 구성할 수 있습니다.

암호화된 폴더에서 수집

에이전트는 암호화된 폴더에서 수집할 수 있습니다. 에이전트는 폴더를 암호화한 사용자에게 의해 실행된 경우에만 암호화된 폴더에서 수집합니다.

필드 이름은 제한됩니다. 다음 필드 이름은 예약된 것이므로 필드 이름으로 사용할 수 없습니다.

- event\_type

- hostname
- source
- text

## 사전 요구 사항

vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

## 절차

- 1 vRealize Log Insight Windows 에이전트의 프로그램 데이터 폴더로 이동합니다.  
%ProgramData%\VMware\Log Insight Agent
- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.
- 3 구성 매개 변수를 추가하고 환경에 맞게 값을 설정합니다.

매개 변수	설명
[filelog] <i>section_name</i> ]	구성 섹션의 고유 이름입니다.
directory	<p>로그 파일 디렉토리의 전체 경로입니다.</p> <p>하나 이상의 다른 구성 섹션 아래에서 동일한 디렉토리를 정의하여 동일한 파일에서 여러 번 로그를 수집할 수 있습니다. 이 프로세스를 통해 여러 태그 및 필터를 동일한 이벤트 소스에 적용할 수 있습니다.</p> <p><b>참고</b> 해당 섹션에 대해 정확히 동일한 구성을 사용하는 경우 중복 이벤트가 서버 쪽에서 발견됩니다.</p>
include	<p>(선택 사항) 데이터를 수집할 파일 이름 또는 파일 마스크(glob 패턴)의 이름입니다. 값은 세미콜론으로 구분된 목록으로 제공할 수 있습니다. 기본값은 *이며, 이는 모든 파일이 포함된다는 의미입니다. 매개 변수는 대/소문자를 구분합니다.</p> <p><b>참고</b> 기본적으로 .zip 및 .gz 파일은 수집 대상에서 제외됩니다.</p> <p><b>중요</b> 회전 로그 파일을 수집하는 경우 include 및 exclude 매개 변수를 사용하여 기본 파일 및 회전 파일 모두와 일치하는 glob 패턴을 지정합니다. glob 패턴이 기본 로그 파일과만 일치하면 회전하는 동안 이벤트가 vRealize Log Insight 에이전트에서 누락될 수 있습니다. vRealize Log Insight 에이전트는 회전 파일의 올바른 순서를 자동으로 확인하고 올바른 순서로 이벤트를 vRealize Log Insight 서버로 전송합니다. 예를 들어 기본 로그 파일의 이름이 myapp.log로 지정되고 회전 로그의 이름이 myapp.log.1, myapp.log.2 등으로 지정되는 경우 다음 include 패턴을 사용할 수 있습니다.</p> <p>include= myapp.log;myapp.log.*</p>
exclude	<p>(선택 사항) 수집 대상에서 제외할 파일 이름 또는 파일 마스크(glob 패턴)입니다. 값은 세미콜론으로 구분된 목록으로 제공할 수 있습니다. 기본값은 비워 두는 것이며, 이는 제외할 파일이 없다는 의미입니다.</p>

매개 변수	설명
<b>event_marker</b>	<p>(선택 사항) 로그 파일에서 이벤트의 시작을 나타내는 정규식입니다. 이를 생략하면 새 행이 기본값이 됩니다. 입력하는 식은 Perl 정규식 구문을 사용해야 합니다.</p> <p><b>참고</b> 따옴표(" ") 등의 기호는 정규식의 래퍼로 처리되지 않습니다. 이러한 기호는 패턴의 일부로 처리됩니다.</p> <p>vRealize Log Insight 에이전트는 실시간 수집에 최적화되어 있기 때문에 내부 지연과 함께 작성된 부분 로그 메시지는 여러 이벤트로 분할될 수 있습니다. 확인된 새 event_marker 없이 로그 파일 추가가 200ms 이상 중지되어 있으면 부분 이벤트가 완료, 구문 분석 및 전달된 것으로 처리됩니다. 이 시간 논리는 구성할 수 없으며 event_marker 설정보다 우선시 됩니다. 로그 파일 appender가 전체 이벤트를 플러시해야 합니다.</p>
<b>enabled</b>	<p>(선택 사항) 구성 섹션을 사용 또는 사용하지 않도록 설정하는 매개 변수입니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.</p>
<b>charset</b>	<p>(선택 사항) 에이전트가 모니터링하는 로그 파일의 문자 인코딩입니다. 가능한 값은 UTF-8, UTF-16LE 및 UTF-16BE입니다. 기본값은 UTF-8입니다.</p>
<b>tags</b>	<p>(선택 사항) 수집된 이벤트의 필드에 사용자 지정 태그를 추가하는 매개 변수입니다. JSON 표기법을 사용하여 태그를 정의해야 합니다. 태그 이름에는 문자, 숫자 및 밑줄을 포함할 수 있습니다. 태그 이름은 문자 또는 밑줄로만 시작할 수 있으며 64자를 초과할 수 없습니다. 태그 이름은 대/소문자를 구분하지 않습니다. 예를 들어 tags={"tag_name1": "tag value 1", "Tag_Name1": "tag value 2"}를 사용하면 Tag_Name1은 중복 항목으로 무시됩니다. 태그 이름으로 event_type 및 timestamp를 사용할 수 없습니다. 동일한 선언 내의 중복 항목은 무시됩니다.</p> <p>대상이 syslog 서버인 경우 태그는 APP-NAME 필드를 재정의합니다. 예를 들어 tags={"appname": "VROPS"}일 수 있습니다.</p>
<b>exclude_fields</b>	<p>(선택 사항) 수집 대상에서 개별 필드를 제외하는 매개 변수입니다. 여러 값을 세미콜론 또는 쉼표로 구분된 목록으로 제공할 수 있습니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>■ exclude_fields=hostname; filepath</li> <li>■ exclude_fields=type; size</li> <li>■ exclude_fields=type, size</li> </ul>

```
[filelog|section_name]
directory=path_to_log_directory
include=glob_pattern
```

## 예제: 구성

```
[filelog|vCenterMain]
directory=C:\ProgramData\VMware\VMware VirtualCenter\WLogs
include=vpxd-*.log
exclude=vpxd-alert-*.log;vpxd-profiler-*.log
event_marker=^Wd{4}-Wd{2}-Wd{2}[A-Z]Wd{2}:Wd{2}:Wd{2}W.Wd{3}
```

```
[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
```

```
include=*.log
exclude=*_old.log
tags={"Provider" : "Apache"}
```

```
[filelog|MSSQL]
directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log
charset=UTF-16LE
event_marker=[^Ws]
```

## Windows 로그 파일 채널 필터링 설정

Windows 로그 파일에 대한 필터를 설정하여 로그 이벤트를 명시적으로 포함하거나 제외할 수 있습니다.

whitelist 및 blacklist 매개 변수를 사용하여 필터 식을 평가할 수 있습니다. 필터 식은 이벤트 필드 및 연산자로 구성된 부울 식입니다.

**참고** blacklist 옵션은 필드에만 작동하며 blacklist 텍스트에 사용할 수 없습니다.

- whitelist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트만 수집합니다. whitelist을 생략하면 값은 암시적으로 1이 됩니다.
- blacklist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트를 제외합니다. 기본값은 0입니다.

Windows 이벤트 필드 및 연산자의 전체 목록은 [이벤트 필드 및 연산자](#) 항목을 참조하십시오.

### 사전 요구 사항

vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

### 절차

- 1 vRealize Log Insight Windows 에이전트의 프로그램 데이터 폴더로 이동합니다.  
%ProgramData%\VMware\Log Insight Agent
- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.
- 3 [filelog] 섹션에 whitelist 또는 blacklist 매개 변수를 추가합니다.

예:

```
[filelog|apache]
directory = path_to_log_directory
include = glob_pattern
blacklist = filter_expression
```

- 4 Windows 이벤트 필드 및 연산자를 기반으로 필터 식을 생성합니다.

예를 들면 다음과 같습니다.

```
whitelist = myServer
```

**5** liagent.ini 파일을 저장한 후 닫습니다.

### 예제: 필터 구성

server\_name이 있는 Apache 로그만 수집하도록 에이전트를 구성할 수 있습니다.

```
[filelog|apache]
directory=C:\Program Files\Apache Software Foundation\Apache2.4\logs
include=error.log
parser=clf
whitelist = server_name == "sample.com"
blacklist = remote_host == "127.0.0.1"
```

## Log Insight Windows Agent로 이벤트 전달

Windows 시스템의 이벤트를 Log Insight Windows Agent가 실행 중인 시스템으로 전달할 수 있습니다.

Windows 이벤트 전달을 사용하여 여러 Windows 시스템의 이벤트를 Log Insight Windows Agent가 설치된 단일 시스템으로 전달할 수 있습니다. 그런 다음 전달된 모든 이벤트를 수집하고 vRealize Log Insight 서버에 보내도록 Log Insight Windows Agent를 구성할 수 있습니다.

Windows 이벤트 전달 기능을 숙지합니다. <http://technet.microsoft.com/en-us/library/cc748890.aspx> 및 [http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb870973(v=vs.85).aspx)를 참조하십시오.

### 사전 요구 사항

[Windows 이벤트 채널에서 이벤트 수집](#)을 참조하십시오.

### 절차

- 1 전달된 이벤트를 수신하는 Windows 이벤트 채널로부터 이벤트를 수집하도록 Log Insight Windows Agent 구성에 새 섹션을 추가합니다.

기본 채널 이름은 ForwardedEvents입니다.

- 2 Windows 이벤트 전달을 설정합니다.

### 다음에 수행할 작업

vRealize Log Insight 웹 사용자 인터페이스로 이동하고 전달된 이벤트가 도착했는지 확인합니다.

## Log Insight Linux Agent 구성

Log Insight Linux Agent를 설치한 이후에 구성할 수 있습니다. liagent.ini 파일은 /var/lib/loginsight-agent/에 위치합니다. 선택한 vRealize Log Insight 서버로 이벤트를 보내고 통신 프로토콜 및 포트를 설정하고 플랫폼 파일 로그 수집을 구성하도록 Log Insight Linux Agent를 구성하려면 이 파일을 편집해야 합니다.

## vRealize Log Insight Linux Agent의 기본 구성

설치를 마치면 liagent.ini 파일에는 Log Insight Windows Agent에 대해 미리 구성된 기본 설정이 포함됩니다.

### vRealize Log Insight Linux Agent liagent.ini 기본 구성

ASCII가 아닌 이름과 값을 사용하는 경우 구성을 UTF-8로 저장합니다.

최종 구성은 이 파일과 서버의 구성을 결합한 것으로 liagent-effective.ini 파일을 형성합니다.

서버의 에이전트 페이지에서 설정을 구성하는 것이 더 효율적일 수 있습니다.

```
[server]
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
; Example of configuration with trusted CA:
;ssl=yes
;ssl_ca_path=/etc/pki/tls/certs/ca.pem

; Time in minutes to force reconnection to the server.
; This option mitigates imbalances caused by long-lived TCP connections. Default:
;reconnect=30

[logging]
; Logging verbosity: 0 (no debug messages), 1 (essentials), 2 (verbose with more impact on performance).
; This option should always be 0 under normal operating conditions. Default:
;debug_level=0

[storage]
; Max local storage usage limit (data + logs) in MBs. Valid range: 100-2000 MB.
;max_disk_buffer=200

; Uncomment the appropriate section to collect system logs
; The recommended way is to enable the Linux content pack from LI server
;[filelog|syslog]
;directory=/var/log
;include=messages;messages.?.syslog;syslog.?
```



매개 변수	값	설명
proto	cfapi	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 cfapi 및 syslog입니다. 기본 cfapi 설정을 사용하십시오.
hostname	LOGINSIGHT	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.
port	9543, 9000, 6514 및 514	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 통신 포트입니다. 기본값은 SSL이 사용되는 cfapi의 경우 9543, SSL이 사용되지 않는 cfapi의 경우 9000, SSL이 사용되는 syslog의 경우 6514, SSL이 사용되지 않는 syslog의 경우 514입니다.
ssl	yes	SSL을 사용하거나 사용하지 않도록 설정합니다. 기본값은 yes입니다. ssl을 [yes]로 설정하고 포트 값을 설정하지 않은 경우 포트 9543이 자동으로 선택됩니다.
max_disk_buffer	200	Log Insight Windows Agent에서 이벤트 및 자체 로그를 버퍼링하는 데 사용하는 MB 단위의 최대 디스크 공간입니다. 지정된 max_disk_buffer에 도달하면 에이전트를 새로 들어오는 이벤트를 삭제하기 시작합니다.
debug_level	0	로그 세부 정보 수준을 정의합니다. <a href="#">Log Insight Agents의 로그 세부 정보 수준 정의</a> 항목을 참조하십시오.

## Linux 에이전트 구성에 대해 공통 값 사용

각 에이전트 구성 섹션을 적용하는 공통 매개 변수 값으로 에이전트 구성 파일의 기본값을 재정의할 수 있습니다.

### 공통 옵션

구성 파일의 [common|global] 섹션에 지정된 옵션은 모든 섹션으로 전파되고, [common|filelog] 섹션에 지정된 옵션은 모든 filelog 섹션으로만 전파되고, [common|winlog] 옵션은 모든 winlog 섹션으로만 전파됩니다.

다음 예와 같이 공통 섹션에서 tags, include, exclude, event\_marker, charset, exclude\_fields 및 parser와 같은 매개 변수를 정의할 수 있습니다.

```
[common|global]

tags = {"log_source_vm":"win-2008r2-64"}
exclude_fields = test_tag;some_other_tag
parser = auto
```

```
[common|filelog]
tags = {"collector_type":"filelog"}
exclude = *.trc

[filelog|channel_1]
directory = C:\WappWlog
include = *.log

...
```

이 예에서는 다음 동작을 지정합니다.

- filelog 섹션의 모든 로그는 해당 값에 log\_source\_vm 및 collector\_type 태그를 둘 다 포함합니다.
- test\_tag 및 some\_other\_tag 태그는 전송되는 모든 로그에서 제외됩니다.
- auto 파서는 수집된 모든 로그에 적용됩니다.
- 기본적으로 모든 filelog 수집기는 모니터링에서 \*.trc 파일을 제외합니다.

[common|global]의 옵션은 모든 winlog 섹션에도 적용됩니다.

## 병합 및 재정의 기준

옵션이 둘 이상의 섹션에 정의되면 해당 값은 병합되거나 재정의되고, 더 작은 범위를 갖는 섹션이 병합/재정의 시 더 높은 우선 순위를 갖습니다. 즉, [common|global]의 값은 [common|filelog]의 값으로 병합 또는 재정의된 다음 [filelog|sample\_section]의 값으로 결합 또는 재정의됩니다.

병합 및 재정의 동작은 다음 규칙을 따릅니다.

- 해당 값이 값 목록을 나타내는 옵션(tags, include, exclude 및 exclude\_fields)은 섹션의 해당 옵션 값과 병합될 때 더 높은 우선 순위를 갖습니다. 또한 태그의 경우 앞서 설명한 것처럼 더 높은 우선 순위를 갖는 섹션의 태그 값이 더 낮은 우선 순위를 갖는 섹션의 동일한 태그 값을 재정의합니다.
- 단일 값을 가질 수 있는 옵션(event\_marker, charset 및 parser) 값은 더 높은 우선 순위의 섹션에 있는 해당 옵션의 값으로 재정의됩니다.

즉, [filelog|sample\_section]의 charset=UTF-8 값은 [common|global]의 charset=UTF-16LE 글로벌 값을 재정의합니다.

따라서 예를 들어 [common|filelog]에 tags={"app":"global-test"}가 있고 [filelog|flg\_test\_section]에 tags={"app":"local-test","section":"flg\_test\_section"}이 있는 경우 [filelog|flg\_test\_section] 섹션의 "app" 태그 값은 [common|filelog]의 값을 재정의합니다. 이 filelog 섹션을 통해 수집한 모든 로그는 "local-test" 값을 갖는 "app" 태그와 "flg\_test\_section" 값을 갖는 "section" 태그를 추가적으로 포함합니다. winlog 섹션의 경우 우선 순위 체인은 같습니다. 즉, 모든 [winlog|...] 섹션이 가장 높은 우선 순위를 갖고, [common|global] 섹션이 가장 낮은 우선 순위를 갖습니다.

공통 섹션에 잘못된 값이 지정되면 일반적으로 이러한 값은 건너뛰며, 앞에 나온 해당 filelog/winlog 섹션의 값과 병합되지 않습니다. 태그 또는 `exclude_fields` 옵션에 잘못된 값이 있는 경우 에이전트는 가능한 한 많은 유효한 데이터를 추출하고, 잘못된 데이터가 나오면 파일의 나머지 부분을 건너뜁니다. 모든 이상 징후는 에이전트 로그 파일에 보고됩니다. 예기치 않은 동작이 발생하는 경우 로그 파일을 확인하고 에이전트에서 보고된 모든 오류를 수정하십시오.

에이전트는 filelog 또는 winlog 섹션에서 잘못된 옵션 값을 감지하면 해당 섹션의 옵션 값을 공통 섹션의 옵션 값과 병합하지 않고 해당 섹션을 사용하도록 설정하지 않습니다. 모든 오류는 에이전트 로그 파일에 보고됩니다. 예기치 않은 동작이 발생하는 경우 로그 파일을 확인하고 에이전트에서 보고된 모든 오류를 수정하십시오.

## 대상 vRealize Log Insight 서버 설정

vRealize Log Insight Linux 에이전트가 이벤트를 전달하는 대상 vRealize Log Insight 서버를 설정 또는 변경할 수 있습니다.

### 사전 요구 사항

- **루트**로 로그인하거나 `sudo`를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 `pgrep liagent`를 실행하여 vRealize Log Insight Linux 에이전트가 설치되어 실행 중인지 확인합니다.
- 통합된 로드 밸런서를 사용하는 vRealize Log Insight 클러스터가 있는 경우 사용자 지정 SSL 인증서 관련 요구 사항은 [통합된 로드 밸런서 사용](#)을 참조하십시오.

### 절차

- 1 텍스트 편집기에서 `/var/lib/loginsight-agent/liagent.ini` 파일을 엽니다.
- 2 다음 매개 변수를 수정하고 환경에 맞게 값을 설정합니다.

매개 변수	설명
<code>proto</code>	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 프로토콜입니다. 가능한 값은 <code>cfapi</code> 및 <code>syslog</code> 입니다. 기본 <code>cfapi</code> 설정을 사용하십시오.
<code>hostname</code>	vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다. IPv4 또는 IPv6 주소를 지정할 수 있습니다. IPv6 주소는 대괄호를 사용하거나 사용하지 않고 지정할 수 있습니다. 예: <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>hostname = 2001:cdba::3257:9652 or hostname = [2001:cdba::3257:9652]</pre> </div> 호스트가 IPv4 스택과 IPv6 스택 모두를 지원하고 도메인 이름을 호스트 이름으로 지정한 경우, 에이전트는 이름 확인 프로그램이 반환하는 IP 주소에 기반하여 적절한 IP 스택을 사용합니다. 확인 프로그램이 IPv4 주소와 IPv6 주소 둘 모두 반환하면 에이전트는 주어진 순서대로 두 주소에 순차적으로 연결을 시도합니다.

매개 변수	설명
port	에이전트의 이벤트가 vRealize Log Insight 서버로 전송되는 데 사용되는 통신 포트입니다. 기본값은 SSL이 사용되는 cfapi의 경우 9543, SSL이 사용되지 않는 cfapi의 경우 9000, SSL이 사용되는 syslog의 경우 6514, SSL이 사용되지 않는 syslog의 경우 514입니다.
ssl	SSL을 사용하거나 사용하지 않도록 설정합니다. 기본값은 yes입니다. ssl을 [yes]로 설정하고 포트 값을 설정하지 않은 경우 포트 9543이 자동으로 선택됩니다.
reconnect	강제로 서버에 다시 연결하는 시간(분)입니다. 기본값은 30입니다.

```
[server]
hostname=LOGINSIGHT
; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOG/INSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog. Default:
;proto=cfapi

; Log Insight server port to connect to. Default ports for protocols (all TCP):
; syslog: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
;port=9543

; SSL usage. Default:
;ssl=yes
```

3 liagent.ini 파일을 저장한 후 닫습니다.

## 예제: 구성

다음 구성 예에서는 신뢰할 수 있는 CA(인증 기관)를 사용하는 대상 vRealize Log Insight 서버를 설정합니다.

```
[server]
proto=cfapi
hostname=LOGINSIGHT
port=9543
ssl=yes;
ssl_ca_path=/etc/pki/tls/certs/ca.pem
```

다음에 수행할 작업

vRealize Log Insight Linux 에이전트에 대한 추가 SSL 옵션을 구성할 수 있습니다. [서버와 Log Insight Agent 사이의 SSL 연결 구성](#)을 참조하십시오.

## 로그 파일에서 이벤트 수집

하나 이상의 로그 파일에서 이벤트를 수집하도록 vRealize Log Insight Linux 에이전트를 구성할 수 있습니다.

**참고** 기본적으로 vRealize Log Insight Linux 에이전트는 프로그램 또는 편집기가 생성한 숨겨진 파일을 수집합니다. 숨겨진 파일 이름은 마침표로 시작합니다. 제외 **exclude=.\*** 매개 변수를 추가하여 vRealize Log Insight Linux 에이전트가 숨겨진 파일을 수집하지 않도록 지정할 수 있습니다.

필드 이름은 제한됩니다. 다음 필드 이름은 예약된 것이므로 필드 이름으로 사용할 수 없습니다.

- event\_type
- hostname
- source
- text

### 사전 요구 사항

- **루트**로 로그인하거나 sudo를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 pgrep liagent를 실행하여 vRealize Log Insight Linux 에이전트가 설치되어 실행 중인지 확인합니다.

### 절차

- 1 텍스트 편집기에서 /var/lib/loginsight-agent/liagent.ini 파일을 엽니다.
- 2 구성 매개 변수를 추가하고 환경에 맞게 값을 설정합니다.

매개 변수	설명
[filelog] <i>section_name</i> ]	구성 섹션의 고유 이름입니다.
directory	로그 파일 디렉토리의 전체 경로입니다. 하나 이상의 다른 구성 섹션 아래에서 동일한 디렉토리를 정의하여 동일한 파일에서 여러 번 로그를 수집할 수 있습니다. 이 프로세스를 통해 여러 태그 및 필터를 동일한 이벤트 소스에 적용할 수 있습니다.
<b>참고</b> 해당 섹션에 대해 정확히 동일한 구성을 사용하는 경우 중복 이벤트가 서버 쪽에서 발견됩니다.	

매개 변수	설명
<b>include</b>	<p>(선택 사항) 데이터를 수집할 파일 이름 또는 파일 마스크(glob 패턴)의 이름입니다. 값은 세미콜론으로 구분된 목록으로 제공할 수 있습니다. 기본값은 *이며, 이는 모든 파일이 포함된다는 의미입니다. 매개 변수는 대/소문자를 구분합니다.</p> <p><b>참고</b> 기본적으로 .zip 및 .gz 파일은 수집 대상에서 제외됩니다.</p> <p><b>중요</b> 회전 로그 파일을 수집하는 경우 include 및 exclude 매개 변수를 사용하여 기본 파일 및 회전 파일 모두와 일치하는 glob 패턴을 지정합니다. glob 패턴이 기본 로그 파일과만 일치하면 회전하는 동안 이벤트가 vRealize Log Insight 에이전트에서 누락될 수 있습니다. vRealize Log Insight 에이전트는 회전 파일의 올바른 순서를 자동으로 확인하고 올바른 순서로 이벤트를 vRealize Log Insight 서버로 전송합니다. 예를 들어 기본 로그 파일의 이름이 myapp.log로 지정되고 회전 로그의 이름이 myapp.log.1, myapp.log.2 등으로 지정되는 경우 다음 include 패턴을 사용할 수 있습니다.</p> <pre>include= myapp.log;myapp.log.*</pre>
<b>exclude</b>	<p>(선택 사항) 수집 대상에서 제외할 파일 이름 또는 파일 마스크(glob 패턴)입니다. 값은 세미콜론으로 구분된 목록으로 제공할 수 있습니다. 기본값은 비워 두는 것이며, 이는 제외할 파일이 없다는 의미입니다.</p>
<b>event_marker</b>	<p>(선택 사항) 로그 파일에서 이벤트의 시작을 나타내는 정규식입니다. 이를 생략하면 새 행이 기본값이 됩니다. 입력하는 식은 Perl 정규식 구문을 사용해야 합니다.</p> <p><b>참고</b> 따옴표(" ") 등의 기호는 정규식의 래퍼로 처리되지 않습니다. 이러한 기호는 패턴의 일부로 처리됩니다.</p> <p>vRealize Log Insight 에이전트는 실시간 수집에 최적화되어 있기 때문에 내부 지연과 함께 작성된 부분 로그 메시지는 여러 이벤트로 분할될 수 있습니다. 확인된 새 event_marker 없이 로그 파일 추가가 200ms 이상 중지되어 있으면 부분 이벤트가 완료, 구문 분석 및 전달된 것으로 처리됩니다. 이 시간 논리는 구성할 수 없으며 event_marker 설정보다 우선시 됩니다. 로그 파일 appender가 전체 이벤트를 플러시해야 합니다.</p>
<b>enabled</b>	<p>(선택 사항) 구성 섹션을 사용 또는 사용하지 않도록 설정하는 매개 변수입니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.</p>
<b>charset</b>	<p>(선택 사항) 에이전트가 모니터링하는 로그 파일의 문자 인코딩입니다. 가능한 값은 UTF-8, UTF-16LE 및 UTF-16BE입니다. 기본값은 UTF-8입니다.</p>

매개 변수	설명
<b>tags</b>	<p>(선택 사항) 수집된 이벤트의 필드에 사용자 지정 태그를 추가하는 매개 변수입니다. JSON 표기법을 사용하여 태그를 정의해야 합니다. 태그 이름에는 문자, 숫자 및 밑줄을 포함할 수 있습니다. 태그 이름은 문자 또는 밑줄로만 시작할 수 있으며 64자를 초과할 수 없습니다. 태그 이름은 대/소문자를 구분하지 않습니다. 예를 들어 tags={"tag_name1": "tag value 1", "Tag_Name1": "tag value 2"}를 사용하면 Tag_Name1은 중복 항목으로 무시됩니다. 태그 이름으로 event_type 및 timestamp를 사용할 수 없습니다. 동일한 선언 내의 중복 항목은 무시됩니다.</p> <p>대상이 syslog 서버인 경우 태그는 APP-NAME 필드를 재정의합니다. 예를 들어 tags={"appname": "VROPS"}일 수 있습니다.</p>
<b>exclude_fields</b>	<p>(선택 사항) 수집 대상에서 개별 필드를 제외하는 매개 변수입니다. 여러 값을 세미콜론 또는 쉼표로 구분된 목록으로 제공할 수 있습니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>■ exclude_fields=hostname; filepath</li> <li>■ exclude_fields=type; size</li> <li>■ exclude_fields=type, size</li> </ul>

```
[filelog|section_name]
directory=path_to_log_directory
include=glob_pattern
```

### 3 liagent.ini 파일을 저장한 후 닫습니다.

## 예제: 구성

```
[filelog|messages]
directory=/var/log
include=messages;messages.?[

[filelog|syslog]
directory=/var/log
include=syslog;syslog.?[

[filelog|Apache]
directory=/var/log/apache2
include=*
```

## Linux 로그 파일 채널 필터링 설정

Linux 로그 파일에 대한 필터를 설정하여 로그 이벤트를 명시적으로 포함하거나 제외할 수 있습니다.

**참고** 기본적으로 vRealize Log Insight Linux 에이전트는 프로그램 또는 편집기가 생성한 숨겨진 파일을 수집합니다. 숨겨진 파일 이름은 마침표로 시작합니다. 제외 **exclude=.\*** 매개 변수를 추가하여 vRealize Log Insight Linux 에이전트가 숨겨진 파일을 수집하지 않도록 지정할 수 있습니다.

whitelist 및 blacklist 매개 변수를 사용하여 필터 식을 평가할 수 있습니다. 필터 식은 이벤트 필드 및 연산자로 구성된 부울 식입니다.

**참고** blacklist 옵션은 필드에만 작동하며 blacklist 텍스트에 사용할 수 없습니다.

- whitelist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트만 수집합니다. whitelist을 생각하면 값은 암시적으로 1이 됩니다.
- blacklist는 필터 식이 0 이외의 값으로 평가되는 로그 이벤트를 제외합니다. 기본값은 0입니다.

Linux 이벤트 필드 및 연산자의 전체 목록은 [로그 파일에서 이벤트 수집](#) 항목을 참조하십시오.

#### 사전 요구 사항

- **루트**로 로그인하거나 sudo를 사용하여 콘솔 명령을 실행합니다.
- vRealize Log Insight Linux 에이전트를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 pgrep liagent를 실행하여 vRealize Log Insight Linux 에이전트가 설치되어 실행 중인지 확인합니다.

#### 절차

- 1 텍스트 편집기에서 /var/lib/loginsight-agent/liagent.ini 파일을 엽니다.
- 2 [filelog] 섹션에 whitelist 또는 blacklist 매개 변수를 추가합니다.

예를 들면 다음과 같습니다.

```
[filelog|apache]
directory = path_to_log_directory
include = glob_pattern
blacklist = filter_expression
```

- 3 Linux 이벤트 필드 및 연산자를 기반으로 필터 식을 생성합니다.

예를 들면 다음과 같습니다.

```
whitelist = server_name
```

- 4 liagent.ini 파일을 저장한 후 닫습니다.

#### 예제: 필터 구성

server\_name이 sample.com이고 remote\_host가 127.0.0.1이 아닌 Apache 로그만 수집하도록 에이전트를 구성할 수 있습니다. 예를 들면 다음과 같습니다.

```
[filelog|apache]
directory=/var/log/httpd
include=access_log
parser=clf
whitelist = server_name == "sample.com"
blacklist = remote_host == "127.0.0.1"
```



## vRealize Log Insight 에이전트의 중앙 집중식 구성

다수의 Windows 또는 Linux vRealize Log Insight 에이전트를 구성할 수 있습니다.

각 vRealize Log Insight 에이전트마다 로컬 구성과 서버 측 구성이 있습니다. 로컬 구성은 vRealize Log Insight 에이전트가 설치된 시스템의 `liagent.ini` 파일에 저장되어 있습니다. 서버 측 구성은 액세스 및 편집이 가능합니다. 예를 들어 Windows의 경우 웹 사용자 인터페이스의 **관리 > 에이전트**에서 액세스하고 편집할 수 있습니다. 각 vRealize Log Insight 에이전트의 구성은 섹션과 키로 구성됩니다. 키에는 구성 가능한 값이 있습니다.

vRealize Log Insight 에이전트는 주기적으로 vRealize Log Insight 서버를 폴링하여 서버 측 구성을 수신합니다. 서버 측 구성 및 로컬 구성은 병합되며, 해당 결과가 유효 구성이 됩니다. 각 vRealize Log Insight 에이전트는 유효 구성을 운영 구성으로 사용합니다. 구성은 섹션별 그리고 키별로 병합됩니다. 서버 측 구성의 값은 로컬 구성의 값을 재정의합니다. 병합 규칙은 다음과 같습니다.

- 섹션이 로컬 구성에만 제공되거나 서버 측 구성에만 제공되는 경우 해당 섹션 및 관련 콘텐츠 모두가 유효 구성의 일부가 됩니다.
- 섹션이 로컬 구성 및 서버 측 구성 모두에 제공되는 경우 섹션의 키는 다음 규칙에 따라 병합됩니다.
  - 키가 로컬 구성에만 제공되거나 서버 측 구성에만 제공되는 경우 키 및 관련 값이 유효 구성에서 해당 섹션의 일부가 됩니다.
  - 키가 로컬 구성 및 서버 측 구성 모두에 제공되는 경우 키는 유효 구성에서 해당 섹션의 일부가 되고 서버 측 구성의 값이 사용됩니다.

vRealize Log Insight 관리자는 모든 vRealize Log Insight 에이전트에 중앙 집중식 구성을 적용할 수 있습니다. 예를 들어 Windows에서는 [관리] 페이지로 이동하고 [관리] 섹션에서 **에이전트**를 클릭합니다. **에이전트 구성** 상자에 구성 설정을 입력하고 **모든 에이전트에 대해 구성 저장**을 클릭합니다. 구성은 다음 폴링 주기 동안 연결된 모든 에이전트에 적용됩니다.

---

**참고** 중앙 집중식 구성은 cfapi 프로토콜을 사용하는 vRealize Log Insight 에이전트에만 적용할 수 있습니다.

---

설치 후 [Log Insight Windows Agent 구성](#) 를 참조하십시오.

## 구성 병합 예

다음은 Log Insight Windows Agent의 로컬 구성과 서버 측 구성의 병합 예입니다.

### 로컬 구성

Log Insight Windows Agent의 로컬 구성은 다음과 같을 수 있습니다.

```
[server]
proto=cfapi
hostname=HOST
port=9000

[winlog|Application]
channel=Application
```

```
[winlog|Security]
channel=Security

[winlog|System]
channel=System

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(Wd{1,3}W.){3}Wd{1,3} - -
```

## 서버 측 구성

웹 사용자 인터페이스의 **관리 > 에이전트** 페이지를 사용하여 모든 에이전트에 중앙 집중식 구성을 적용할 수 있습니다. 예를 들어 수집 채널을 제외 및 추가할 수 있고 기본 다시 연결 설정을 변경할 수 있습니다.

```
[server]
reconnect=20

[winlog|Security]
channel=Security
enabled=no

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational
```

## 유효 구성

유효 구성은 로컬 구성 및 서버 측 구성을 병합한 결과입니다. Log Insight Windows Agent는 다음을 수행하도록 구성됩니다.

- vRealize Log Insight 서버에 20분마다 다시 연결
- 애플리케이션 및 시스템 이벤트 채널을 계속 수집
- 보안 이벤트 채널 수집 중지
- Microsoft-Windows-DeviceSetupManager/Operational 이벤트 채널 수집 시작
- ApacheAccessLogs 계속 수집

```
[server]
proto=cfapi
hostname=HOST
port=9000
reconnect=20

[winlog|Application]
channel=Application
```

```
[winlog|Security]
channel=Security
enabled=no

[winlog|System]
channel=System

[winlog|Microsoft-Windows-DeviceSetupManagerOperational]
channel=Microsoft-Windows-DeviceSetupManager/Operational

[filelog|ApacheAccessLogs]
enabled=yes
directory=C:\Program Files (x86)\Apache Software Foundation\Apache2.2\logs
include=*.log
exclude=*_old.log
event_marker=^(Wd{1,3}W.){3}Wd{1,3} --
```

## 로그 구문 분석

에이전트 측 로그 구문 분석기는 원시 로그에서 구조화된 데이터를 추출하여 vRealize Log Insight 서버에 제공합니다. vRealize Log Insight는 로그 구문 분석기를 사용하여 로그를 분석하고, 여기에서 정보를 추출하고, 해당 결과를 서버에 표시할 수 있습니다. 로그 구문 분석기는 Windows 및 Linux vRealize Log Insight 에이전트 모두에 대해 구성할 수 있습니다.

syslog 프로토콜을 사용하는 경우, 구문 분석기를 통해 추출된 필드는 RFC5424에 따라 STRUCTURED-DATA의 일부입니다.

## 로그 구문 분석기 구성

FileLog 및 WinLog 수집기 모두에 대해 구문 분석기를 구성할 수 있습니다.

### 사전 요구 사항

vRealize Log Insight Linux Agent:

- 루트로 로그인하거나 sudo를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 pgrep liagent를 실행하여 Log Insight Linux Agent가 설치되어 실행 중인지 확인합니다.

vRealize Log Insight Windows Agent:

- Log Insight Windows Agent가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 서비스가 설치되었는지 확인합니다.

## 절차

- 1 liagent.ini 파일이 포함된 폴더로 이동합니다.

운영 체제	경로
Linux	/var/lib/loginsight-agent/
Windows	%ProgramData%\VMware\Log Insight Agent

- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.

- 3 특정 구문 분석기를 구성하려면 구문 분석기 섹션을 정의합니다. [parser|myparser]

여기서 myparser는 로그 소스에서 참조할 수 있는 구문 분석기의 임의의 이름입니다. 구문 분석기 섹션은 기본 제공(또는 다른 정의된) 구문 분석기를 참조하고 해당 구문 분석기의 필수 옵션과 필요한 경우 선택적 옵션을 구성해야 합니다.

예를 들어 base\_parser=csv는 myparser 구문 분석기가 기본 제공 구문 분석기 csv에서 파생되었음을 보여줍니다. 이 경우 입력 로그는 세미콜론으로 구분된 두 개의 필드로 구성되어야 합니다.

```
[parser|myparser]

base_parser=csv

fields=field_name1,field_name2

delimiter=";"
```

- 4 myparser를 정의한 후에는 로그 소스 winlog 또는 filelog에서 이 구문 분석기를 참조합니다.

```
[filelog|some_csv_logs]

directory=D:\Logs

include=*.txt;*.txt.*

parser=myparser
```

D:\Logs 디렉토리 및 같은 some\_csv\_logs 소스에서 수집된 로그는 myparser에 의해 구문 분석되며 추출된 이벤트는 서버에서 각각 field\_name1 및 field\_name2로 표시됩니다.

**참고** D:\Logs 디렉토리의 정적 로그는 에이전트가 vRealize Log Insight로 가져오지 않습니다. 하지만 D:\Logs 디렉토리에 생성된 새 파일은 vRealize Log Insight에서 사용할 수 있습니다.

- 5 liagent.ini 파일을 저장한 후 닫습니다.

## 구문 분석기의 공통 옵션

이름 지정된 필드를 생성하는 모든 구문 분석기에 대해 공통 옵션을 구성할 수 있습니다.

필드 이름은 제한됩니다. 다음 필드 이름은 예약된 것이므로 필드 이름으로 사용할 수 없습니다.

- event\_type

- hostname
- source
- text

공통 옵션	설명
base_parser	이 사용자 지정 구문 분석기가 확장하는 기본 구문 분석기의 이름입니다. 기본 제공 구문 분석기 이름이거나 다른 사용자 지정 구문 분석기 이름일 수 있습니다. 이 구성 키는 필수입니다.
field_decoder	중첩된 구문 분석기는 JSON 문자열로 지정됩니다. 이 문자열의 키는 중첩된 구문 분석기가 적용되는 필드의 이름이고, 값은 해당 필드에 사용할 구문 분석기의 이름입니다. 중첩된 구문 분석기 각각은 기본 구문 분석기가 디코딩한 적절한 필드에 적용됩니다. 필드 디코더는 필드의 값이 타임 스탬프와 같은 복잡한 값일 때 유용합니다.
field_rename	추출된 필드의 이름을 바꿉니다. JSON 문자열로서, 키는 필드의 원래 이름이고 값은 필드의 원하는 새 이름입니다. field_decoder는 항상 field_rename 전에 적용됩니다. INI 파일에서 이러한 옵션의 순서는 중요하지 않습니다. 확실히 하기 위해 field_decoder를 먼저 지정하십시오.
next_parser	다음으로 실행할 구문 분석기의 이름입니다. 동일한 입력에 대해 여러 구문 분석기를 순차적으로 실행할 수 있습니다.  <b>참고</b> 구문 분석기는 next_parser 키워드로 정의된 이후의 모든 구문 분석기를 처리하며 이전 구문 분석기에 의해 이미 추출된 필드 값을 바꿀 수 있습니다.
exclude_fields	서버에 제공되기 전에 이벤트에서 제거할 세미콜론으로 구분된 필드 이름 목록입니다. 이 옵션은 이벤트 필터링이 수행되기 전에 적용되므로 구문 분석 도중 제외한 필드를 필터 조건에 사용할 수 없습니다.
debug	특정 구문 분석기의 디버깅을 사용하도록 설정하는 Yes 또는 No 옵션입니다. 디버깅을 사용하도록 설정하면 구문 분석기는 수신되는 입력, 수행한 작업 및 생성한 결과의 상세 로깅을 수행합니다. 옵션은 섹션별로 적용됩니다. 즉, 특정 섹션으로 정의된 구문 분석기에만 적용됩니다. 구문 분석기에 대한 디버깅의 기본 값은 debug=no입니다.

## 쉽게로 구분된 값 로그 구문 분석기

FileLog 및 WinLog 수집기 모두에 대해 CSV(쉽게로 구분된 값) 구문 분석기를 구성할 수 있습니다.

csv 구문 분석기에 대해 사용할 수 있는 옵션은 fields 및 delimiter입니다.

### 쉽게로 구분된 값 구문 분석기 옵션

csv 구문 분석기의 구조에 대한 다음 정보를 참고하십시오.

옵션	설명
fields	<p>fields 옵션은 로그에 있는 필드의 이름을 지정합니다. 나열된 필드 이름의 전체 수는 로그에 있는 샘플로 구분된 필드의 전체 수와 일치해야 합니다.</p> <p>fields 옵션은 CSV 구문 분석기에 필수입니다. 이 옵션을 지정하지 않으면 아무것도 구문 분석되지 않습니다. 필드 내용에 따라 필드 값 앞뒤의 큰따옴표는 선택 사항입니다.</p> <p>필드 이름은 다음과 같이 샘플로 구분되어야 합니다.</p> <pre>fields = field_name1, field_name2, field_name3, field_name4</pre> <p>이 정의는 추출된 필드에 이름 field_name1, field_name2, field_name3 및 field_name4가 순차적으로 할당되는 것으로 가정합니다.</p> <p>CSV 구문 분석기가 일부 필드를 생략해야 하는 경우에는 해당 이름을 목록에서 생략할 수 있습니다. 예를 들면 다음과 같습니다.</p> <pre>fields = field_name1, , field_name3, field_name4</pre> <p>이 경우 구문 분석기는 첫 번째, 세 번째 및 네 번째 필드만 이벤트에서 추출하며 여기에 이름 field_name1, field_name3 및 field_name4를 순차적으로 할당합니다.</p> <p>fields 옵션이 로그의 전체 필드 목록을 지정하지 않으면 구문 분석기는 빈 목록을 반환합니다. 예를 들어 로그 파일에 field1, field2, field3, field4 및 field5가 포함되어 있지만 fields= field1,field2,field3만 지정된 경우 구문 분석기는 빈 필드 목록을 반환합니다.</p> <p>구문 분석기가 빈 필드 목록을 반환하므로 CSV 구문 분석기에 fields=*를 사용할 수 없습니다. 이미 설명한 것처럼 특정 필드를 생략해야 하는 경우 이외에는 전체 필드 목록을 지정해야 합니다.</p>
delimiter	<p>delimiter 옵션은 구문 분석기에서 사용할 구분 기호를 지정합니다. 기본적으로 csv 구문 분석기는 샘플로 구분 기호로 사용하지만, 구분 기호를 세미콜론, 공백 또는 기타 특수 문자로 변경할 수 있습니다. 정의된 구분 기호는 큰따옴표로 묶어야 합니다.</p> <p>예: delimiter="," 및 delimiter=";"</p> <p>csv 구문 분석기의 경우 " " 또는 "asd" 같이 따옴표로 묶은 문자 집합을 구분 기호로 지원합니다. 로그에 사용된 필드 값의 구분 기호는 구분 기호 매개 변수에 정의된 패턴과 정확하게 일치해야 합니다. 구분 기호가 일치하지 않으면 구문 분석기가 실패합니다.</p> <p>공백 또는 탭 같은 특수 문자도 csv 구문 분석기에 사용할 구분 기호로 정의할 수 있지만, 이 경우에는 해당 특수 문자 앞에 이스케이프 문자가 반드시 있어야 합니다(\\, \s, \t). 예를 들어 delimiter="Ws" 또는 delimiter=" "와 같습니다.</p> <p>delimiter 옵션은 선택 사항입니다.</p>

## CSV 로그 구문 분석기 구성

winlog 또는 filelog 소스에서 수집된 로그를 구문 분석하려면 다음 구성을 사용합니다.

```
[filelog|some_csv_logs]
directory=D:\WLogs
include=*.txt;*.txt.*
parser=myparser

[parser|myparser]
base_parser = csv
fields = timestamp,field_name1, field_name2, field_name3
delimiter = ";";
field_decoder={"timestamp": "tsp_parser"}
[parser|tsp_parser]
; timestamp is a built-in parser
base_parser=timestamp
```

```
; "format" is an option of timestamp parser
format=%Y-%m-%d %H:%M:%S
```

이 구성을 사용하면 some\_csv\_logs 소스에서(예: directory=D:\Logs 디렉토리에서) 수집된 로그가 myparser에 의해 구문 분석됩니다. 수집된 로그에 세미콜론으로 구분된 세 개의 값이 포함된 경우, 구문 분석된 이벤트에는 field\_name1, field\_name2 및 field\_name3 이름이 순차적으로 할당됩니다.

다음 CSV 로그를 구문 분석하려면:

```
"United States","USA","North America","High income: OECD","Fiscal year end: September 30; reporting period for national accounts data: CY."
```

CSV 구문 분석기 구성을 정의합니다.

```
[parser|csv_log_parser]
base_parser=csv
fields=country_name, country_code, region, income_group, special_notes
```

CSV 구문 분석기가 다음 필드를 반환합니다.

```
country_name=United States
country_code=USA
region=North America
income_group=High income: OECD
special_notes=Fiscal year end: September 30; reporting period for national accounts data: CY.
```

## CLF(Common Log Format)(Apache) 로그 구문 분석기

FileLog 및 WinLog 수집기 모두에 대해 CLF(Common Log Format) Apache 구문 분석기를 구성할 수 있습니다.

### CLF(Common Log Format)(Apache) 구문 분석기

기본 CLF 구문 분석기는 다음과 같은 순서 및 이름의 필드를 정의합니다.

```
host ident authuser datetime request statuscode bytes
```

구문 분석기 이름: clf

CLF 구문 분석기의 옵션은 format입니다.

#### format 옵션

format 옵션은 Apache 로그 생성에 사용되는 형식을 지정합니다. 이 옵션은 필수 사항이 아닙니다.

형식을 지정하지 않으면 다음의 기본 공통 로그 형식이 사용됩니다.

```
%h %l %u %t W"%rW" %s %b
```

CLF 구문 분석기 형식 문자열은 정규식을 허용하지 않습니다. 예를 들어 식 \s+ 대신 공백을 지정하십시오.

다른 로그 형식을 구문 분석하려면 에이전트의 구성에 해당 형식을 지정하십시오. 구문 분석된 필드는 서버 측에 다음 이름으로 표시됩니다.

**참고** 변수가 필요한 경우 구성에 {VARNAME}이 제공되지 않으면 필드가 무시됩니다.

필드	값
'%a':	"remote_ip"
'%A':	"local_ip"
'%B', '%b':	"response_size"
'%C':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%c':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%D':	"request_time_mcs"
'%E':	"error_status"
'%e':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%F', '%f':	"file_name"
'%h':	"remote_host"
'%H':	"request_protocol"
'%i':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%k':	"keepalive_request_count"
'%l':	"remote_log_name"
'%L':	"request_log_id"
'%M':	"log_message"(이 지정자에 도달한 후에 파서는 입력 로그 구문 분석을 중지함)
'%m':	"request_method"
'%n':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%o':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%p':	"server_port" 추가 형식을 이 지정자와 함께 사용할 수 있습니다. %(format)p. 지원되는 형식은 "canonical", "local" 또는 "remote"입니다. "canonical" 형식이 사용되면 필드 이름은 "server_port"로 유지됩니다. "local" 형식이 사용되면 필드 이름은 "local_server_port"가 되고 "remote" 형식이 사용되면 필드 이름은 "remote_server_port"가 됩니다.
'%P':	"process_id" 추가 형식을 이 지정자와 함께 사용할 수 있습니다. %(format)P. 지원되는 형식은 "pid", "tid" 및 "hextid"입니다. "pid"가 형식으로 사용되면 필드 이름은 "process_id"가 됩니다. 반면에 "tid" 및 "hextid" 형식은 이름이 "thread_id"인 필드를 생성합니다.
'%q':	"query_string"
'%r':	"request"
'%R':	"response_handler"
'%s':	"status_code". 요청의 최종 상태를 생성하는 이 필드도 지원됩니다. 서버에 "status_code"로 나타납니다.



필드	값
'%t':	<p>"timestamp"는 수집 시 이벤트 타임 스탬프로 작동하고, 타임 스탬프 파서를 활용합니다. 타임 스탬프 자동 감지를 재정의하려면 날짜 및 시간 형식을 <code>%{Y-m-d %H:%M:%S}t</code>와 같이 중괄호로 지정할 수 있습니다. 자세한 내용은 <a href="#">타임 스탬프 구문 분석기</a>를 참조하십시오.</p> <p>CLF 파서에 대한 타임 스탬프 형식은 "begin:" 또는 "end:" 접두사로 시작할 수 있습니다. 형식이 begin:으로 시작하면(기본값) 요청 처리가 시작될 때가 시간으로 지정됩니다. end:로 시작될 경우 이 시간은 요청 처리가 끝나는 시간에 가까운, 로그 항목이 기록될 때에 해당합니다. 예를 들어 다음과 같은 형식은 CLF 파서에서 지원됩니다. <code>%h %l %u [%{begin:%d/%b/%Y %T}t.%{msec_frac}t] W"rW" %s %b</code></p> <p>CLF 파서 타임 스탬프 형식 지정자에 대해 다음 형식 토큰도 지원됩니다.</p> <p><b>sec</b> Epoch 이후의 시간(초)입니다. 이 시간은 타임 스탬프 파서의 <code>%s</code> 지정자와 같습니다.</p> <p><b>msec</b> Epoch 이후의 시간(밀리초)입니다.</p> <p><b>usec</b> Epoch 이후의 시간(마이크로초)입니다.</p> <p><b>msec_frac</b> 밀리초 부분(타임 스탬프 파서의 <code>%f</code> 지정자와 같음)</p> <p><b>usec</b> 마이크로초 부분(타임 스탬프 파서의 <code>%f</code> 지정자와 같음)</p> <p>타임 스탬프가 형식 토큰으로 표시되는 로그를 구문 분석하려면 구성에 다음 형식을 사용할 수 있습니다.</p> <pre>format=%h %l %u %{sec}t W"rW" %s %b format=%h %l %u %{msec}t W"rW" %s %b format=%h %l %u %{usec}t W"rW" %s %b</pre> <p>이러한 토큰을 서로 조합하거나 동일한 형식 문자열의 타임 스탬프 파서 형식과 조합할 수 없습니다. 대신 여러 <code>%{format}t</code> 토큰을 사용할 수 있습니다. 예를 들어 타임 스탬프 파서의 <code>%f</code> 지정자를 사용하는 경우를 제외하고 밀리초를 포함하는 타임 스탬프를 사용하려면 다음의 조합된 타임 스탬프를 사용할 수 있습니다. <code>%{d/%b/%Y %T}t.%{msec_frac}t</code>.</p>
'%T':	"request_time_sec"
'%u':	"remote_auth_user"
'%U':	"requested_url"
'%v':	"server_name"
'%V':	"self_referential_server_name"
'%X':	"connection_status"는 형식에 지정된 변수 이름에 따라 좌우됩니다.
'%x':	형식에 지정된 변수 이름에 따라 좌우됩니다.
'%I':	"received_bytes"
'%O':	"sent_bytes"
'%S':	"transferred_size"

예를 들어 winlog 또는 filelog 소스에서 수집된 로그를 CLF 구문 분석기로 구문 분석하려면 다음 구성을 지정합니다.

```
[filelog|cllogs]
directory=D:\Logs
include=*.txt
```

```
parser=myclf

[parser|myclf]
debug=yes ;Note: use this option only while debugging and set it to 'no' when used in production.
base_parser=clf
format=%h %l %u %b %t W"%rW" %s
```

이 구성을 사용하면 clfflogs 소스에서(예: directory=D:\Logs 디렉토리에서) 수집된 로그가 myclf에 의해 구문 분석됩니다. myclf 구문 분석기는 구성에 설명된 형식으로 생성된 로그만 구문 분석합니다. 구문 분석기에 대한 디버그의 기본 값은 debug=no입니다.

## CLF를 사용하여 생성된 로그 구문 분석

CLF를 사용하여 생성된 로그를 구문 분석하려면 구성에서 해당 형식을 정의해야 합니다. 예를 들면 다음과 같습니다.

```
format=%h %l %u %t W"%rW" %>s %b W"%{Referer}iW" W"%{User_Agent}iW"
```

지정자 %{Referer}i 및 %{User\_Agent}i를 사용하는 비어 있지 않은 필드는 vRealize Log Insight 서버에서 각각 referer 및 user\_agent라는 이름으로 표시됩니다.

## 타임 스탬프 구문 분석기와 CLF 구문 분석기 통합

사용자 지정 시간 형식의 Apache 로그를 구문 분석할 수 있습니다.

다음과 같이 사용자 지정 시간 형식을 가진 로그에 액세스합니다.

```
format = %h %l %u %a, %d %b %Y %H:%M:%S)t W"%rW" %>s %b
```

사용자 지정 시간이 지정되지 않은 경우 CLF 구문 분석기는 자동 타임 스탬프 구문 분석기를 실행하여 자동으로 시간 형식을 추론하려고 시도하며, 그렇지 않은 경우에는 사용자 지정 시간 형식이 사용됩니다.

오류 로그에 대해 지원되는 사용자 지정 시간 형식은 다음과 같습니다.

사용자 지정 시간 형식	설명	구성 형식
%{u}t	마이크로초(ms)를 포함한 현재 시간	format=[%{u}t] [%l] [pid %P] [client %a] %M
%{cu}t	마이크로초(ms)를 포함한 컴팩트 ISO 8601 형식 현재 시간	format=[%{cu}t] [%l] [pid %P] [client %a] %M

지원되는 타임 스탬프 지정자의 전체 목록은 [타임 스탬프 구문 분석기](#)를 참조하십시오.

## 예제: Windows에 대한 Apache 기본 액세스 로그 구성

이 예는 Windows에 대한 Apache v2.4 액세스 로그 구성의 형식을 지정하는 방법을 보여줍니다.

```
;ACCESS LOG
;127.0.0.1 - - [13/May/2015:14:44:05 +0400] "GET /xampp/navi.php HTTP/1.1" 200 4023 "http://localhost/xampp/"
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0"
;format=%h %l %u %d/%b/%Y:%H:%M:%S %z)t W"%rW" %>s %b W"%{Referer}iW" W"%{User_agent}iW"
```

```
; Section to collect Apache ACCESS logs
[filelog|clflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*
    parser=clfpaser_apache_access
    enabled=yes

;Parser to parse Apache ACCESS logs
[parser|clfpaser_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u %d/%b/%Y:%H:%M:%S %z}t W"rW" %a %A %e %k %l %L %m %n %T %v %V %>s %b W"%{Referer}iW" W"%{User-agent}iW"
```

엑세스 로그 형식 정의:

1 액세스 로그 형식(httpd.conf)에 대해 Apache를 구성합니다.

```
LogFormat "%h %l %u %d-%b-%Y:%H:%M:%S}t W"rW" %a %A %e %k %l %L %m %n %T %v %V %>s %b W"%{Referer}iW" W"%{User-Agent}iW" combined
```

2 CLF 구문 분석기 구성을 정의합니다.

```
;ACCESS LOG
;127.0.0.1 unknown - 21-May-2015:13:59:35 "GET /xampp/navi.php HTTP/1.1" 127.0.0.1 127.0.0.1 - 0 unknown - GET -
1 localhost localhost 200 4023 "http://localhost/xampp/" "-"
[filelog|clflogs-access]
    directory=C:\xampp\apache\logs
    include=acc*;*myAcc*
    parser=clfpaser_apache_access
    enabled=yes
; Parser to parse Apache ACCESS logs
[parser|clfpaser_apache_access]
    debug=yes
    base_parser=clf
    format=%h %l %u %d-%b-%Y:%H:%M:%S}t W"rW" %a %A %e %k %l %L %m %n %T %v %V %>s %b W"%{Referer}iW" W"%{User-Agent}iW"
```

CLF 구문 분석기가 다음을 반환합니다.

```
remote_host=127.0.0.1
timestamp=2015-05-13T10:44:05
request=GET /xampp/navi.php HTTP/1.1
status_code=200
response_size=4023
referer=http://localhost/xampp/
user_agent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
```

예제: Windows에 대한 Apache 기본 오류 로그 구성

이 예는 Windows에 대한 Apache v2.4 오류 로그 구성의 형식을 지정하는 방법을 보여줍니다.

```
;ERROR LOG
;[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354: Child: Starting 150 worker
```

```

threads.
;[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent: Created child process 3480
;format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %{thread_id}i] %E: %M
;format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M

; Section to collect Apache ERROR logs
[filelog|cllogs-error]
    directory=C:\xampp\apache\logs
    include=err*
    parser=clfpaser_apache_error
    enabled=yes

;Parser to parse Apache ERROR logs
[parser|clfpaser_apache_error]
    debug=yes
    base_parser=clf
    format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %{thread_id}i] %E: %M
    next_parser=clfpaser_apache_error2

;Parser to parse Apache ERROR logs
[parser|clfpaser_apache_error2]
    debug=yes

```

```
base_parser=clf  
format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M
```

**참고** 제공되는 이름은 결합된 로그 형식에 해당합니다. Apache 오류 로그는 Apache 오류 로그 형식이 아니라 위의 형식 지정 키를 사용하여 설명되기도 합니다.

오류 로그 형식 정의:

- 1 오류 로그 형식(httpd.conf)에 대해 Apache를 구성합니다.

```
LogFormat "%h %l %u %{d-%b-%Y:%H:%M:%S}t W\"%rW\" %a %A %e %k %l %L %m %n %T %v %V %>s %b W\"%{Referer}iW\" W\"%{User-Agent}iW\"" combined
```

- 2 CLF 구문 분석기 구성을 정의합니다.

```
;Parser to parse Apache ERROR logs
[parser|clfpaser_apache_error]
  debug=yes
  base_parser=cl f
  format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P] %E: %M
  next_parser=clfpaser_apache_error2

;Parser to parse Apache ERROR logs
[parser|clfpaser_apache_error2]
  debug=yes
  base_parser=cl f
  format=[%{a %b %d %H:%M:%S%f %Y}t] [%m:%{severity}i] [pid %P:tid %t{thread_id}i] %E: %M
```

로그 항목:

```
[Wed May 13 14:37:17.042371 2015] [mpm_winnt:notice] [pid 4488:tid 272] AH00354: Child: Starting 150 worker threads.
```

CLF 구문 분석기가 로그 항목에 대해 다음 필드를 반환합니다(+0400 표준 시간대에서 구문 분석기를 사용 중인 경우).

```
timestamp=2015-05-13T10:37:17.042371
request_method=mpm_winnt
severity=notice
process_id=4488
thread_id=272
error_status=AH00354
log_message=Child: Starting 150 worker threads.
```

로그 항목:

```
[Wed May 13 14:37:27.042371 2015] [mpm_winnt:notice] [pid 5288] AH00418: Parent: Created child process 3480
```

CLF 구문 분석기가 로그 항목에 대해 다음 필드를 반환합니다(+0400 표준 시간대에서 구문 분석기를 사용 중인 경우).

```
timestamp=2015-05-13T10:37:27.042371
request_method=mpm_winnt
severity=notice
process_id=5288
error_status=AH00418
log_message=Parent: Created child process 3480
```

## 키/값 쌍 구문 분석기

FileLog 및 WinLog 수집기 모두에 대해 KVP(키/값 쌍) 구문 분석기를 구성할 수 있습니다.

### KVP(키/값 쌍) 구문 분석기

kvp 구문 분석기는 임의의 로그 메시지 텍스트에서 key=value 일치 항목을 모두 찾아서 추출합니다. 다음 예에서는 kvp 구문 분석기 형식을 보여 줍니다.

```
[parser|kvp_parser]
base_parser=kvp
fields=*
```

예를 들어 키-값 로그는 scope=local; abstract=false; lazyInit=false; autowireMode=0; dependencyCheck=0; 형식일 수 있습니다.

kvp 구문 분석기를 사용할 때는 값을 추출할 필드를 지정해야 합니다. 예를 들어 구성에 정의 fields=name,lastname,country가 있는 경우에는 지정된 키를 가진 값만 구문 분석하여 서버로 보냅니다.

필요한 경우 공백 또는 기타 특수 문자를 정의할 때 키와 값 모두 큰따옴표(“)로 묶을 수 있습니다.

키 또는 값에 대해 큰따옴표를 사용할 경우 백슬래시 문자(“)를 이스케이프 문자로 사용할 수 있습니다. 백슬래시 다음에 나오는 모든 문자는 리터럴 방식으로 정의됩니다(큰따옴표 문자 또는 백슬래시 문자 포함). 예: “\”

다음 고려 사항에 주의하십시오.

- 키/값 쌍의 키 뒤에 등호 기호가 없고 VALUE가 제공되지 않으면 일반 텍스트의 경우처럼 옵션을 건너뜁니다.
- 키는 비워 둘 수 없으며 값은 비워 둘 수 있습니다.
- 등호 기호 뒤에 값이 없으면 일반 텍스트로 취급하여 건너뜁니다.
- 값은 큰따옴표 문자로 묶인 문자열이거나 비어 있을 수 있습니다. 값에 특수 문자가 포함된 경우 백슬래시를 사용하여 이스케이프합니다.

### KVP 구문 분석기 옵션

kvp 구문 분석기의 구조에 대해 다음 정보를 참고하십시오.

옵션	설명
fields	추출하려는 정보이며 데이터 단위로 정의됩니다. 예를 들면 fields=name,lastname,country입니다.
delimiter	<p>선택 사항입니다.</p> <p>기본 구분 기호는 공백 문자, 탭, 줄 바꿈 문자, 쉼표 및 세미콜론 문자입니다.</p> <p>구성에 구분 기호가 지정되지 않은 경우 kvp 구문 분석기는 기본 구분 기호를 구문 분석에 사용합니다.</p> <p>기본 구분 기호를 특정 구분 기호로 변경하려면 해당 구분 기호를 큰따옴표로 묶어야 합니다. 예를 들면 delimiter = "#^ "입니다. 이 정의는 큰따옴표 안에 있는 각 문자가 구분 기호로 사용된다는 것을 의미합니다. kvp 구문 분석기의 경우 모든 문자를 구분 기호로 간주할 수 있습니다. 정의에 포함된 다른 구분 기호와 함께 기본 구분 기호를 포함할 수 있습니다.</p> <p>예를 들어 delimiter = "#^ WtWrWnWs" 문에는 탭, 줄 바꿈 문자 및 공백이 구분 기호로 포함됩니다. 이러한 문자를 사용할 경우 해당 문자 앞에 이스케이프 문자가 나와야 합니다. 예를 들어 공백 문자를 구분 기호로 정의하려면 공백 문자 앞에 이스케이프 문자 "\"를 입력합니다(예: delimiter="Ws").</p>
field_decoder	<p>중첩된 구문 분석기는 JSON 문자열로 지정됩니다. 이 문자열의 키는 중첩된 구문 분석기에 적용할 필드의 이름이고, 값은 해당 필드에 사용할 구문 분석기의 이름입니다.</p> <p>중첩된 구문 분석기 각각은 기본 구문 분석기가 디코딩한 적절한 필드에 적용됩니다.</p> <p>필드 디코더는 키-값 쌍의 값이 타임 스탬프 또는 쉼표로 구분된 목록과 같은 복잡한 값일 때 유용합니다.</p>
debug =	<p>선택 사항입니다. debug = 값은 yes 또는 no일 수 있습니다. 구문 분석기에 대한 디버그의 기본 값은 debug=no입니다.</p> <p>옵션을 yes로 설정하면 liagent_&lt;date&gt;.log에서 구문 분석기 수집의 상세 로그를 볼 수 있습니다.</p>

### 추가적인 키 값 옵션

키	정의
KVP_MESSAGE = *(MESSAGE_ENTRY [WSPR])	선택적인 공백으로 구분된 메시지 항목의 목록입니다.
MESSAGE_ENTRY = KVP / FREE_TEXT	항목은 키/값 쌍이거나 일반 텍스트입니다.
KVP = KEY [ "=" VALUE]	키/값 쌍입니다. KEY 다음에 등호와 VALUE가 나오지 않으면 일반 텍스트처럼 건너뛩니다.
KEY = BARE_KEY / QUOTED_KEY	
FREE_TEXT = "="	단독으로 나오는 등호는 일반 텍스트로 간주되어 건너뛩니다.
BARE_KEY = *1BARE_KEY_CHAR	적어도 한 문자 이상입니다.
BARE_KEY_CHAR = %0x00-08 / %0x10-19 / %0x21-3C / %3E-%FF	등호, 공백 또는 탭을 제외한 모든 문자입니다.
QUOTED_KEY = 0x22 *1(QUOTED_STRING_CHAR / "W" CHAR) 0x22	큰따옴표 문자로 묶은 하나 이상의 문자입니다. 백슬래시를 이스케이프 문자로 사용합니다.
QUOTED_STRING_CHAR = %0x00-21 / %0x23-FF	큰따옴표를 제외한 모든 문자입니다.
VALUE = BARE_VALUE / QUOTED_VALUE	
BARE_VALUE = *BARE_VALUE_CHAR	0개 이상의 문자입니다.



키	정의
BARE_VALUE_CHAR = %0x00-08 / %0x10-19 / %0x21-FF	공백 또는 탭을 제외한 모든 문자입니다.
QUOTED_VALUE = 0x22 *(QUOTED_STRING_CHAR / "W" CHAR) 0x22	큰따옴표 문자로 묶은 문자열입니다. 이 값은 비워 둘 수 있습니다. 백슬래시를 이스케이프 문자로 사용합니다.

## KVP 구문 분석기 구성 예

필요한 경우 fields=\*를 사용하여 모든 필드를 구문 분석할 수 있습니다.

```
[parser|simple_kv]
base_parser =kv
fields=*
```

이 예에서는 필드 디코더를 지정하는 방법을 보여 줍니다.

```
[parser|mykv]
debug=no
base_parser=kvp
delimiter="#^|"
fields=*
;OR fields=scope,abstract,lazyInit,autowireMode,dependencyCheck
field_decoder={"field1":"field1_parser1"}

[parser|field1_parser1]
base_parser=clf
format=[%{value1}i]]
field_decoder={"value1":"field_parser2"}
```

다음 KVP 로그를 구문 분석하려면:

```
Configuring transport... proto = cfapi server_hostname = LOCALHOST ssl = no port = 9000 reconnect = 30
```

KVP 구문 분석기 구성을 정의합니다.

```
[parser|kvp_log_parser]
base_parser=kvp
fields=*
```

KVP 구문 분석기가 다음 필드를 반환합니다.

```
proto=cfapi
server_hostname=LOCALHOST
ssl=no
port=9000
reconnect=30
```

## 예제: 단순한 KVP 구문 분석기 및 복잡한 KVP 구문 분석기의 예

### 단순한 KVP 구문 분석기 예

```
[filelog|MyLog]
directory=C:\W<folder_name>WParser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
```

### 복잡한 KVP 구문 분석기 예

```
[filelog|MyLog]
directory=C:\W<folder_name>WParser_logs
include=*.log
parser=my_KVP_parser

[parser|my_KVP_parser]
base_parser=kvp
fields=*
field_decoder={"field1":" field1_parser1"}

[parser| field1_parser1]
base_parser=clf
format=[%{value1}i]]
field_decoder={"value1":" field1_parser2"}
```

## 타임 스탬프 구문 분석기

timestamp 구문 분석기는 필드를 생성하지는 않지만 대신 문자열의 입력을 내부 타임 스탬프 형식 (UNIX epoch 시작인 1970년 1월 1일(UTC/GMT 자정) 이후의 시간을 밀리초로 표시)으로 변환합니다.

유일하게 지원되는 구성 옵션은 format입니다. 예를 들면 format=%Y-%m-%d %H:%M:%S입니다.

CLF 구문 분석기와 달리 timestamp 구문 분석기는 %A%B%d%H%M%S%Y%Z와 같이 시간 지정자 사이에 구분 기호가 없을 때 시간을 구문 분석할 수 있습니다.

timestamp 구문 분석기가 사용하는 형식 지정자는 다음과 같습니다.

```
'%a':   Abbreviated weekday name, for example: Thu
'%A':   Full weekday name, for example: Thursday
'%b':   Abbreviated month name, for example: Aug
'%B':   Full month name, for example: August
'%d':   Day of the month, zero-padded (01-31), for example: 03
'%e':   Day of the month, space-padded ( 1-31), for example:  3
'%f':   Fractional seconds of time, for example: .036 'f' specifier assumes that '.' or ','
        character should exist before fractional seconds and there is no need to mention
        that character in the format. If none of these characters precedes fractional seconds,
        timestamp wouldn't be parsed.
'%H':   Hour in 24h format (00-23), for example: 14
```

```
'%l':    Hour in 12h format (01-12), for example: 02
'%m':    Month as a decimal number (01-12), for example: 08
'%M':    Minute (00-59), for example: 55
'%p':    AM or PM designation, for example: PM
'%S':    Second (00-61), for example: 02
'%s':    Total number of seconds from the UNIX epoch start, for example 1457940799
          (represents '2016-03-14T07:33:19' timestamp)
'%Y':    Year, for example: 2001
'%z':    ISO 8601 offset from UTC in timezone (1 minute=1, 1 hour=100).., for example: +100
```

추가적인 지정자는 타임 스탬프 구문 분석기에 서 수락되지만 해당 값은 무시되며 구문 분석된 시간에 영향을 미치지 않습니다.

```
'%C':    Year divided by 100 and truncated to integer (00-99), for example: 20
'%g':    Week-based year, last two digits (00-99), for example, 01
'%G':    Week-based year, for example, 2001
'%j':    Day of the year (001-366), for example: 235
'%u':    ISO 8601 weekday as number with Monday as 1 (1-7), for example: 4
'%U':    Week number with the first Sunday as the first day of week one (00-53), for example: 33
'%V':    ISO 8601 week number (00-53), for example: 34
'%w':    Weekday as a decimal number with Sunday as 0 (0-6), for example: 4
'%W':    Week number with the first Monday as the first day of week one (00-53), for example: 34
'%y':    Year, last two digits (00-99), for example: 01
```

format 매개 변수가 정의되지 않은 경우 Timestamp 구문 분석기는 기본 형식을 사용하여 타임 스탬프를 구문 분석합니다.

## 자동 타임 스탬프 구문 분석기

자동 타임 스탬프 구문 분석기는 타임 스탬프 구문 분석기에 대해 정의된 형식이 없는 경우 호출되거나 field\_decoder에서 timestamp를 사용하여 타임 스탬프 구문 분석기 정의 없이 직접 구문 분석기를 호출할 수 있습니다. 예:

```
[parser|mycsv]
base_parser=csv
debug=yes
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "timestamp"}
```

## 예제: 기본 구성을 사용하는 타임 스탬프 구문 분석기

이 예에서는 기본 구성을 사용하는 timestamp 구문 분석기를 보여줍니다.

```
[parser|tsp_parser]
base_parser=timestamp
debug=no
format=%Y-%m-%d %H:%M:%S%f
```

timestamp 구문 분석기를 다른 구문 분석기(예: CSV 구문 분석기)와 통합하려면 다음 구성을 지정하십시오.

```
[parser|mycsv]
base_parser=csv
```

```
fields=timestamp,action,source_id,dest
field_decoder={"timestamp": "tsp_parser"}
```

이 구성이 정의되면 mycsv 구문 분석기는 구성에 지정된 이름의 필드를 추출하고 timestamp 필드의 내용에 대해 tsp\_parser를 실행합니다. tsp\_parser가 유효한 타임 스탬프를 검색하면 서버는 로그 메시지에 해당 타임 스탬프를 사용합니다.

## 자동 로그 구문 분석기

자동 구문 분석기는 행의 첫 200자 내에서 타임 스탬프를 자동으로 감지합니다. 자동 감지된 타임 스탬프의 형식은 timestamp 구문 분석기의 형식과 동일합니다.

자동 구문 분석기에는 옵션이 없습니다. 타임 스탬프의 자동 감지 이외에도, 로그 항목에 대해 키/값 구문 분석기가 실행되어 로그의 기존 키/값 쌍 모두를 자동으로 감지하고 그에 따라 필드를 추출합니다. 예를 들면 다음과 같습니다.

```
[filelog|some_logs]
directory=/var/log
include=*
parser=auto
```

다른 구문 분석기와 마찬가지로 자동 구문 분석기에 대한 별도의 작업을 정의할 수 있습니다.

```
[filelog|kvplogs]
directory=C:\temp_logs\wcsv-itbm
include=*.txt
parser=myauto
[parser|myauto]

base_parser=auto
debug=yes
```

자동 구문 분석기에 대해 debug를 사용하도록 설정한 경우에는 구문 분석에 대한 추가 정보가 인쇄됩니다. 예를 들어 자동 구문 분석기가 실행된 로그 및 로그에서 추출된 필드에 대한 정보가 인쇄됩니다.

구문 분석기에 대한 디버그의 기본 값은 debug=no입니다.

## Syslog 구문 분석기

syslog 구문 분석기는 기본적으로 timestamp 및 app name 필드만 추출합니다.

syslog 구문 분석기에 대해 모든 공통 옵션과 message\_decoder 옵션을 사용할 수 있습니다.

```
[filelog|data_logs]
directory=D:\WLogs
include=*.txt
parser=mysyslog

[parser|mysyslog]
base_parser=syslog
message_decoder=syslog_message_decoder
debug=yes
```

```
[parser|syslog_message_decoder]
base_parser=kvp
fields=*
```

예를 들어 syslog 형식 로그가 다음과 같은 경우,

```
2015-09-09 13:38:31.619407 +0400 smith01 john: Fri Dec 5 08:58:26 2014 [pid 26123] [jsmith.net]
status_code=FAIL
oper_atiion=LOGIN: Client "176.31.17.46"
```

KVP 구문 분석기를 실행하기 위해 message\_decoder 옵션이 적용된 syslog 구문 분석기는 다음을 반환합니다.

```
timestamp=2015-09-09T09:38:31.619407
appname=john
status_code=FAIL
oper_atiion=LOGIN:
```

## 레이블 지정된 탭으로 구분된 값 구문 분석기

LTSV(레이블 지정된 탭으로 구분된 값) 형식은 TSV(탭으로 구분된 값)의 변형입니다.

LTSV 파일의 각 기록은 한 줄에 나타납니다. 각 필드는 <TAB>으로 구분되어 있으며 레이블과 값이 있습니다. 레이블과 값은 :으로 구분되어 있습니다. LTSV 형식을 사용하는 경우 줄을 <TAB>으로 분할 (TSV 형식과 동일)하여 각 줄을 구문 분석하고 특별한 순서 없이 고유한 레이블로 모든 필드를 확장할 수 있습니다. LTSV 정의 및 형식에 대한 자세한 내용은 <http://ltsv.org/>를 참조하십시오.

### 예제: LTSV 구문 분석기 구성

LTSV 구문 분석기에는 특정 구성 옵션이 필요하지 않습니다. LTSV 구문 분석기를 사용하려면 구성에 기본 제공 ltsv 구문 분석기 이름을 지정합니다.

```
[parser|myltsv]
base_parser=ltsv
```

LTSV 파일은 ABNF 형식의 LTSV 프로덕션과 일치하는 바이트 순서여야 합니다.

```
ltsv = *(record NL) [record]
record = [field *(TAB field)]
field = label ":" field-value
label = 1*lbyte
field-value = *fbyte

TAB = %x09
NL = [%x0D] %x0A
lbyte = %x30-39 / %x41-5A / %x61-7A / "_" / "." / "-" ;; [0-9A-Za-z_.-]
fbyte = %x01-08 / %x0B / %x0C / %x0E-FF
```

## 예제: 샘플 LTSV 로그

```
host:127.0.0.1<TAB>ident:--<TAB>user:frank<TAB>time:[10/Oct/2000:13:55:36 -0700]<TAB>req:GET /apache_pb.gif HTTP/1.0<TAB>status:200<TAB>size:2326<TAB>referer:http://www.example.com/start.html<TAB>ua:Mozilla/4.08 [en] (Win98; I ;Nav)
```

샘플 LTSV 구성을 사용하는 경우 로그의 구문 분석은 다음 필드를 반환합니다.

```
host=127.0.0.1
ident=--
user=frank
time=[10/Oct/2000:13:55:36 -0700]
req=GET /apache_pb.gif HTTP/1.0
status=200
size=2326
referer=http://www.example.com/start.html
ua=Mozilla/4.08 [en] (Win98; I ;Nav)
```

## 디버그 구성

LTSV 구문 분석기에 대해 추가 디버깅도 사용할 수 있습니다. 기본적으로 LTSV 디버깅은 사용되지 않도록 설정되어 있습니다. LTSV 디버깅을 사용하도록 설정하려면 `debug=yes`를 입력합니다.

```
[parser|myltsv]
base_parser=ltsv
debug=yes
```

디버깅이 설정되면 LTSV 구문 분석기가 로그에서 모든 올바른 레이블의 값을 추출합니다. LTSV 구문 분석기를 사용하려면 레이블 이름이 영숫자, 밑줄('\_'), 점('.') 및 대시('-')로만 구성되어야 합니다. 잘못된 레이블 이름이 하나라도 있으면 구문 분석이 실패합니다. 레이블 이름이 올바른 경우에도 에이전트가 필드 이름을 확인합니다. 잘못된 이름이 있다면 잘못된 레이블 이름을 올바른 필드 이름으로 수정해야 합니다.

## filelog 섹션에서 LTSV 구문 분석기 구성

filelog 섹션에서 직접 LTSV 구문 분석기를 구성할 수도 있습니다.

```
[filelog|simple_logs]
directory=/var/log
include=*
parser=ltsv
```

## 정규식 구문 분석기

regex 구문 분석기를 사용하면 수집된 데이터에 대해 몇 가지 정규식을 사용할 수 있습니다.

regex 구문 분석기는 명명된 캡처 그룹이 포함된 정규식을 지정하는 방법으로 정의할 수 있습니다. 예: `(?<field_1>Wd{4})[-](?<field_2>Wd{4})[-](?<field_3>Wd{4})[-](?<field_4>Wd{4})`

그룹에 지정된 이름(예: field\_1, field\_2, field\_3 및 field\_4)은 해당하는 추출된 필드의 이름으로 사용됩니다. 이름에 대한 요구 사항은 다음과 같습니다.

- 정규식 패턴에 지정하는 이름은 vRealize Log Insight의 올바른 필드 이름이어야 합니다.

- 이름에는 영숫자와 밑줄("\_") 문자만 포함할 수 있습니다.
- 이름은 숫자로 시작할 수 없습니다.

잘못된 이름을 지정하면 구문 분석기가 구성되지 않습니다.

## 정규식 구문 분석기 옵션

regex 구문 분석기의 유일한 필수 옵션은 format 옵션입니다.

debug 옵션은 추가적인 디버깅 정보가 필요한 경우에 사용할 수 있습니다.

## 구성

regex 구문 분석기를 생성하려면 regex를 base\_parser로 사용하고 format 옵션을 반드시 제공해야 합니다.

## 예제: 정규식 구성 예

다음 예는 1234-5678-9123-4567을 분석하는 데 사용할 수 있습니다.

```
[parser|regex_parser]
base_parser=regex
format=(?<tag1>Wd{4})[-](?<tag2>Wd{4})[-](?<tag3>Wd{4})[-](?<tag4>Wd{4})
[filelog|some_info]
directory=D:WLogs
include=*.txt
parser=regex_parser
```

다음과 같이 결과가 표시됩니다.

```
tag1=1234
tag2=5678
tag3=9123
tag4=4567
```

## 예제: Apache 로그 구문 분석 예

regex 구문 분석기를 사용하여 Apache 로그를 구문 분석하려면 Apache 로그에 사용할 특정 regex 형식을 제공해야 합니다.

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.*)(?<remote_log_name>.*)(?<remote_auth_user>.*)W[(?<log_timestamp>.*)W]"(?<request>.*)"(?<status_code>.*)(?<response_size>.)
```

다음과 같이 결과가 표시됩니다.

```
127.0.0.1 - admin [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
remote_host=127.0.0.1
remote_log_name=-
remote_auth_user=admin
log_timestamp=10/Oct/2000:13:55:36 -0700
request=GET /apache_pb.gif HTTP/1.0
```

```
status_code=200
response_size=2326
```

다음 코드는 Apache 로그를 구문 분석하는 다른 예를 보여 줍니다.

```
[parser|regex_parser]
base_parser=regex
format=(?<remote_host>.* (?<remote_log_name>.*)) (?<remote_auth_user>.*) W[(?<log_timestamp>.*)W] "(?<request>.*
(?<resource>.* (?<protocol>.*))" (?<status_code>.* (?<response_size>.*
127.0.0.1 unknown - [17/Nov/2015:15:17:54 +0400] W"GET /index.php HTTP/1.1W" 200 4868
remote_host=127.0.0.1 unknown
remote_log_name=unknown
remote_auth_user=-
log_timestamp=17/Nov/2015:15:17:54 +0400
request=GET /index.php HTTP/1.1
resource=/index.php
protocol=HTTP/1.1
status_code=200
response_size=4868
```

## 성능 고려 사항

regex 구문 분석기는 CLF 구문 분석기 같은 다른 구문 분석기에 비해 리소스를 더 많이 사용합니다. 다른 구문 분석기를 사용하여 로그를 구문 분석할 수 있는 경우에는 해당 구문 분석기를 regex 구문 분석기 대신 사용하여 성능을 개선하는 방법을 고려해 보십시오.

사용할 수 있는 다른 구문 분석기가 없어 regex 구문 분석기를 사용해야 하는 경우에는 형식을 최대한 명확하게 정의하십시오. 다음 예에서는 더 나은 성능을 제공하는 구성을 보여 줍니다. 이 예에서는 숫자 값이 있는 필드를 지정합니다.

```
(?<remote_host>Wd+.Wd+.Wd+.Wd+) (?<remote_log_name>.*) (?<remote_auth_user>.*) W[(?<log_timestamp>.*)W] "(?
<request>.*" (?<status_code>Wd+) (?<response_size>Wd+)
```



# vRealize Log Insight 에이전트 제거

## 4

vRealize Log Insight 에이전트를 제거해야 하는 경우 설치된 에이전트 패키지에 해당하는 지침을 따르십시오.

본 장은 다음 항목을 포함합니다.

- [Log Insight Windows Agent 제거](#)
- [Log Insight Linux Agent RPM 패키지 제거](#)
- [Log Insight Linux Agent DEB 패키지 제거](#)
- [Log Insight Linux Agent Bin 패키지 제거](#)

## Log Insight Windows Agent 제거

Log Insight Windows Agent를 제거할 수 있습니다.

### 사전 요구 사항

vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자를 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

### 절차

1 **제어판 > 프로그램 및 기능**으로 이동합니다.

2 VMware vRealize Log Insight Windows Agent를 선택하고 **제거**를 클릭합니다.

그러면 VMware vRealize Log Insight Windows Agent 서비스가 중지되고 시스템에서 관련 파일이 제거됩니다.

## Log Insight Linux Agent RPM 패키지 제거

Log Insight Linux Agent RPM 패키지를 제거할 수 있습니다.

### 사전 요구 사항

- **루트**로 로그인하거나 **sudo**를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent를 설치한 Linux 시스템에 로그인하고, 터미널 콘솔을 연 후 **pgrep liagent**를 실행하여 VMware Log Insight Linux Agent가 설치되어 실행 중인지 확인합니다.

## 절차

- ◆ 다음 명령을 실행합니다. 여기서 *VERSION* 및 *BUILD\_NUMBER*를 설치된 에이전트의 버전 및 빌드 번호로 바꿉니다.

```
rpm -e VMware-Log-Insight-Agent-VERSION-BUILD_NUMBER
```

그러면 VMware Log Insight Linux Agent 대몬이 중지되고 시스템에서 자체 로그를 제외한 모든 파일이 제거됩니다.

## Log Insight Linux Agent DEB 패키지 제거

Log Insight Linux Agent DEB 패키지를 제거할 수 있습니다.

### 사전 요구 사항

- **루트**로 로그인하거나 **sudo**를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent를 설치한 Linux 시스템에 로그인하고, 터미널 콘솔을 연 후 **pgrep liagent**를 실행하여 VMware Log Insight Linux Agent가 설치되어 실행 중인지 확인합니다.

## 절차

- ◆ 다음 명령을 실행합니다.

```
dpkg -P vmware-log-insight-agent
```

그러면 VMware Log Insight Linux Agent 대몬이 중지되고 시스템에서 자체 로그를 제외한 모든 파일이 제거됩니다.

## Log Insight Linux Agent Bin 패키지 제거

Log Insight Linux Agent .bin 패키지를 제거할 수 있습니다.

### 사전 요구 사항

- **루트**로 로그인하거나 **sudo**를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent를 설치한 Linux 시스템에 로그인하고, 터미널 콘솔을 연 후 **pgrep liagent**를 실행하여 VMware vRealize Log Insight Linux Agent가 설치되어 실행 중인지 확인합니다.

## 절차

- 1 Log Insight Linux Agent 대몬을 중지합니다. 이는 `sudo service liagentd stop` 명령 또는 이전 버전의 Linux인 경우 `sudo /sbin/service liagentd stop` 명령을 실행하여 중지하면 됩니다.
- 2 Log Insight Linux Agent 파일을 수동으로 제거합니다.
  - `/usr/lib/loginsight-agent` - 대몬 바이너리 및 라이선스 파일 디렉토리입니다.

- `/usr/bin/loginsight-agent-support` - Log Insight Linux Agent에 대한 지원 번들을 생성하는 데 사용됩니다.
- `/var/lib/loginsight-agent` - 구성 파일 및 데이터베이스 스토리지 디렉토리입니다.
- `/var/log/loginsight-agent` - Log Insight Linux Agent의 로그 디렉토리입니다.
- `/var/run/liagent/liagent.pid` - Log Insight Linux Agent PID 파일입니다. 자동으로 삭제되지 않은 파일은 수동으로 제거하십시오.
- `/etc/init.d/liagentd` - Log Insight Linux Agent 데몬의 스크립트 디렉토리입니다.
- `/usr/lib/systemd/system/liagentd.service`

# vRealize Log Insight 에이전트 문제 해결

5

알려진 문제 해결 정보는 vRealize Log Insight 에이전트의 운영과 관련된 문제를 진단하고 수정하는데 도움이 됩니다.

본 장은 다음 항목을 포함합니다.

- Log Insight Windows Agent용 지원 번들 생성
- Log Insight Linux Agent용 지원 번들 생성
- Log Insight Agents의 로그 세부 정보 수준 정의
- 관리 UI에 Log Insight Agents가 표시되지 않음
- vRealize Log Insight 에이전트가 이벤트를 보내지 않음
- Log Insight Windows Agent에 대한 아웃바운드 예외 규칙 추가
- Windows 방화벽에서 Log Insight Windows Agent의 아웃바운드 연결 허용
- Log Insight Windows Agent의 대량 배포가 실패함
- RPM 패키지 업데이트 설치가 실패함
- Log Insight Agents가 자체 서명된 인증서를 거부함
- vRealize Log Insight 서버가 암호화되지 않은 트래픽의 연결을 거부함

## Log Insight Windows Agent용 지원 번들 생성

문제가 발생하여 Log Insight Windows Agent가 예상대로 작동하지 않으면 로그 및 구성 파일의 복사본을 VMware 지원 서비스로 전송할 수 있습니다.

### 절차

- 1 Log Insight Windows Agent가 설치된 대상 시스템에 로그인합니다.
- 2 Windows **시작** 버튼을 클릭한 후 **VMware > Log Insight Agent - Collect** 지원 번들을 클릭합니다.
- 3 (선택 사항) 바로 가기를 사용할 수 없으면 Log Insight Windows Agent의 설치 디렉토리로 이동하고 `loginsight-agent-support.exe`를 두 번 클릭합니다.

---

**참고** 기본 설치 디렉토리는 `C:\Program Files (x86)\VMware\Log Insight Agent`입니다.

---

번들이 생성되어 내 문서에 .zip 파일로 저장됩니다.

#### 다음에 수행할 작업

요청에 따라 지원 번들을 VMware 지원 서비스로 전달합니다.

## Log Insight Linux Agent용 지원 번들 생성

문제가 발생하여 Log Insight Linux Agent가 예상대로 작동하지 않으면 로그 및 구성 파일의 복사본을 VMware 지원 서비스로 전송할 수 있습니다.

#### 절차

- 1 Log Insight Linux Agent가 설치된 대상 시스템에 로그인합니다.
- 2 다음 명령을 실행합니다.

```
/usr/lib/loginsight-agent/bin/loginsight-agent-support
```

번들이 생성되어 현재 디렉토리에 .zip 파일로 저장됩니다.

#### 다음에 수행할 작업

요청에 따라 지원 번들을 VMware 지원 서비스로 전달합니다.

## Log Insight Agents의 로그 세부 정보 수준 정의

vRealize Log Insight Agent의 구성 파일을 편집하여 로깅 수준을 변경할 수 있습니다.

#### 사전 요구 사항

Log Insight Linux Agent의 경우:

- **루트**로 로그인하거나 **sudo**를 사용하여 콘솔 명령을 실행합니다.
- Log Insight Linux Agent를 설치한 Linux 시스템에 로그인하고, 콘솔을 연 후 **pgrep liagent**를 실행하여 VMware vRealize Log Insight Linux Agent가 설치되어 실행 중인지 확인합니다.

Log Insight Windows Agent의 경우:

- vRealize Log Insight Windows 에이전트가 설치된 Windows 시스템에 로그인하고 서비스 관리자 시작하여 vRealize Log Insight 에이전트 서비스가 설치되었는지 확인합니다.

#### 절차

- 1 liagent.ini 파일을 포함하는 폴더로 이동합니다.

운영 체제	경로
<b>Linux</b>	/var/lib/loginsight-agent/
<b>Windows</b>	%ProgramData%\VMware\Log Insight Agent

- 2 텍스트 편집기에서 liagent.ini 파일을 엽니다.

### 3 liagent.ini 파일의 [logging] 섹션에서 로그 디버그 수준을 변경합니다.

**참고** 디버그 수준이 높을수록 vRealize Log Insight Agent에 미치는 영향도 커집니다. 기본값이자 권장 값은 0입니다. 디버그 수준 1은 좀 더 많은 정보를 제공하며 대부분의 문제 해결을 위해 이 수준이 권장됩니다. 디버그 수준 2는 세부 정보를 제공합니다. 수준 1과 수준 2는 VMware 지원팀에서 요청한 경우에만 사용하십시오.

```
[logging]
; The level of debug messages to enable: 0..2
debug_level=1
```

### 4 liagent.ini 파일을 저장한 후 닫습니다.

로그 디버그 수준이 변경됩니다.

## 관리 UI에 Log Insight Agents가 표시되지 않음

Log Insight Agents 인스턴스에 대한 정보가 관리 UI의 에이전트 페이지에 나타나지 않습니다.

### 문제

Log Insight Agents를 설치한 후 관리 UI의 에이전트 페이지에 Log Insight Agents가 표시되지 않습니다.

### 원인

가장 일반적인 원인은 네트워크 연결 문제이거나 liagent.ini 파일에서 잘못된 Log Insight Agents 구성 때문입니다.

### 해결책

- ◆ Log Insight Agents가 설치된 Windows 또는 Linux 시스템이 vRealize Log Insight 서버와 연결되었는지 확인합니다.
- ◆ Log Insight Agents가 cfapi 프로토콜을 사용하는지 확인합니다.  
syslog 프로토콜을 사용하면 UI에 Log Insight Windows Agents가 표시되지 않습니다.
- ◆ 다음 디렉토리에 위치한 Log Insight Agents 로그 파일의 콘텐츠를 봅니다.
  - Windows - %ProgramData%\VMware\Log Insight Agent\log
  - Linux - /var/log/loginsight-agent/

Config transport error: Couldn't resolve host name 및 Resolver failed. No such host is known 구를 포함하는 로그 메시지를 찾습니다.
- ◆ liagent.ini에 대상 vRealize Log Insight 서버에 대한 올바른 구성이 포함되어 있는지 확인합니다. [대상 vRealize Log Insight 서버 설정](#) 및 [대상 vRealize Log Insight 서버 설정](#)을 참조하십시오.

## vRealize Log Insight 에이전트가 이벤트를 보내지 않음

잘못된 구성으로 인해 vRealize Log Insight 에이전트가 vRealize Log Insight 서버로 이벤트를 전달하지 못할 수 있습니다. 플랫폼 파일 수집 채널이 올바르게 구성되지 않은 경우 다음과 같은 메시지를 볼 수 있습니다. "Invalid settings were obtained for channel 'CHANNEL\_NAME'. Channel 'CHANNEL\_NAME' will stay dormant until properly configured."

### 문제

vRealize Log Insight 에이전트 인스턴스가 **관리 > 에이전트** 페이지에 나타나지만 vRealize Log Insight 에이전트 호스트 이름의 대화형 분석 페이지에는 이벤트가 나타나지 않습니다. 플랫폼 파일 수집 채널이 올바르게 구성되지 않았습니다.

### 원인

잘못된 구성으로 인해 vRealize Log Insight 에이전트가 vRealize Log Insight 서버로 이벤트를 전달하지 못할 수 있습니다.

### 해결책

- ◆ 올바른 수집 채널을 정의합니다. 플랫폼 파일 수집 채널이 올바르게 구성되었는지 확인합니다. [장 3 vRealize Log Insight 에이전트 구성](#) 항목을 참조하십시오.
- ◆ vRealize Log Insight Windows 에이전트의 경우 다음을 시도합니다.
  - Windows 채널이 사용되도록 설정된 경우 %ProgramData%\VMware\Log Insight Agent\log에 있는 vRealize Log Insight Windows 에이전트 로그 파일의 콘텐츠를 확인합니다. Subscribed to channel CHANNEL\_NAME 구를 포함하는 채널 구성 관련 로그 메시지를 찾습니다. 일반적으로 사용되는 채널은 ApplicationSystem 및 Security입니다.
  - 채널이 올바르게 구성되지 않은 경우 다음과 유사한 로그 메시지를 볼 수 있습니다. Could not subscribe to channel CHANNEL\_NAME events. Error Code: 15007. The specified channel could not be found. Check channel configuration. 15007 이외의 오류 코드 번호를 볼 수도 있습니다.
  - 플랫폼 파일 수집 채널이 올바르게 구성되지 않은 경우 다음과 같은 메시지를 볼 수 있습니다. Invalid settings were obtained for channel 'CHANNEL\_NAME'. Channel 'CHANNEL\_NAME' will stay dormant until properly configured
- ◆ vRealize Log Insight Windows 에이전트 및 vRealize Log Insight Linux 에이전트의 경우 다음을 시도합니다.
  - ◆ 구성된 플랫폼 파일 수집 채널이 없는 경우 다음과 유사한 메시지를 볼 수 있습니다. Cannot find section 'filelog' in the configuration. The flat file log collector will stay dormant until properly configured

vRealize Log Insight 에이전트 로그 파일의 콘텐츠는 다음 디렉토리에 위치합니다.

- Windows - %ProgramData%\VMware\Log Insight Agent\log
- Linux - /var/log/loginsight-agent/

## 다음에 수행할 작업

vRealize Log Insight 에이전트 구성에 대한 자세한 내용은 [설치 후 Log Insight Windows Agent 구성](#) 및 [Log Insight Linux Agent 구성](#) 항목을 참조하십시오.

## Log Insight Windows Agent에 대한 아웃바운드 예외 규칙 추가

Windows 방화벽에서 Log Insight Windows Agent 차단 해제 예외 규칙을 정의할 수 있습니다.

절차는 Windows Server 2008 R2 이상 및 Windows 7 이상에 적용됩니다.

### 사전 요구 사항

- 관리자 계정 또는 관리 권한이 있는 계정을 보유하고 있는지 확인합니다.

### 절차

- 1 **시작 > 실행**을 선택합니다.
- 2 wf.msc를 입력하고 **확인**을 클릭합니다.
- 3 왼쪽 창에서 **아웃바운드 규칙**을 마우스 오른쪽 버튼으로 클릭하고 **새 규칙**을 클릭합니다.
- 4 **사용자 지정**을 선택하고 마법사에 따라 다음 옵션을 설정합니다.

옵션	설명
프로그램	liwinsvc.exe
서비스	Log Insight Agent 서비스
프로토콜 및 포트	cfapi의 경우 TCP 9000 그리고 syslog의 경우 514

- 5 이 규칙을 적용할 프로파일 지정 페이지에서 적합한 네트워크 유형을 선택합니다.

- 도메인
- 공용
- 전용

**참고** 네트워크 유형에 관계없이 예외 규칙을 활성화 상태로 유지하기 위해 모든 네트워크 유형을 선택할 수 있습니다.



## 다음에 수행할 작업

Log Insight Windows Agent 로그 디렉토리인 %ProgramData%\VMware\Log Insight Agent\log로 이동하고 최신 로그 파일을 엽니다. 최근 이벤트에 Config transport error: Couldn't resolve host name 및 Resolver failed. No such host is known 메시지가 포함되어 있으면 Log Insight Windows Agent 서비스와 Windows 시스템을 다시 시작합니다.

**참고** Log Insight Windows Agent 서비스가 서버에 다시 연결되는 데 최대 5분이 걸릴 수 있습니다.

## Windows 방화벽에서 Log Insight Windows Agent의 아웃바운드 연결 허용

Windows 방화벽 설정을 구성하여 Log Insight Windows Agent에서 vRealize Log Insight 서버로의 아웃바운드 연결을 허용할 수 있습니다.

Log Insight Windows Agent 서비스를 설치하고 시작한 후 Windows 도메인 또는 로컬 방화벽이 대상 vRealize Log Insight 서버로의 연결을 제한할 수도 있습니다.

절차는 Windows Server 2008 R2 이상 및 Windows 7 이상에 적용됩니다.

### 사전 요구 사항

- 관리자 계정 또는 관리 권한이 있는 계정을 보유하고 있는지 확인합니다.

### 절차

- 1 **시작 > 실행**을 선택합니다.
- 2 wf.msc를 입력하고 **확인**을 클릭합니다.
- 3 작업 창에서 **속성**을 클릭합니다.
- 4 **도메인 프로파일** 탭의 **아웃바운드 연결** 드롭다운 메뉴에서 **허용(기본값)**을 선택합니다.

컴퓨터가 도메인에 연결되어 있지 않으면 컴퓨터가 연결된 네트워크 유형에 따라 **개인 프로파일** 또는 **공개 프로파일**을 선택할 수 있습니다.

- 5 **확인**을 클릭합니다.

## 다음에 수행할 작업

Windows 방화벽에서 Log Insight Windows Agent에 대해 차단 해제 예외 규칙을 정의합니다. [Log Insight Windows Agent에 대한 아웃바운드 예외 규칙 추가](#)를 참조하십시오.

## Log Insight Windows Agent의 대량 배포가 실패함

대상 시스템에서 Log Insight Windows Agent의 대량 배포가 실패합니다.

## 문제

GPO(그룹 정책 개체)를 사용하여 Windows 도메인 시스템에서 대량 배포를 수행한 후 Log Insight Windows Agent의 로컬 서비스로의 설치가 실패합니다.

## 원인

그룹 정책 설정으로 인해 Log Insight Windows Agent가 올바르게 설치되지 않을 수 있습니다.

## 해결책

- 1 GPO(그룹 정책 개체) 설정을 편집하고 Log Insight Windows Agent 에이전트를 다시 배포하십시오.
  - a GPO를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭한 후 **컴퓨터 구성 > 정책 > 관리 템플릿 > 시스템 > 로그인**으로 이동합니다.
  - b **컴퓨터 시작 및 로그인 시 네트워크가 초기화될 때까지 항상 대기** 정책을 사용하도록 설정합니다.
  - c **컴퓨터 구성 > 정책 > 관리 템플릿 > 시스템 > 그룹 정책**으로 이동합니다.
  - d **시작 정책 처리 대기 시간**을 사용하도록 설정하고 **대기 시간(초)**을 120으로 설정합니다.
- 2 대상 시스템에서 `gpupdate /force /boot` 명령을 실행합니다.

## RPM 패키지 업데이트 설치가 실패함

Linux GUI를 사용하는 경우 RPM 패키지 업데이트를 설치하려 하면 설치되지 않습니다.

## 문제

RHEL 및 SUSE Linux 배포의 GUI를 사용할 때 Log Insight Linux Agent RPM 패키지의 설치 또는 업데이트가 실패합니다. `PK_TMP_DIR[dir:///var/tmp/TmpDir.MtqOPs] Repository already exists`. 오류 메시지가 표시될 수 있습니다.

## 원인

애플리케이션 설치 후 캐시 및 저장소 목록이 정리되어 있지 않을 수 있습니다.

## 해결책

- 1 Log Insight Linux Agent RPM이 설치된 Linux 시스템에 로그인하고 시스템 콘솔을 엽니다.
- 2 **루트** 사용자로 다음 명령을 실행합니다.

```
sudo zypper rr 2
sudo zypper rr 1
sudo zypper clean -a
sudo zypper ref
```

- 3 업데이트를 설치할 Log Insight Linux Agent RPM 패키지를 두 번 클릭합니다.

## Log Insight Agents가 자체 서명된 인증서를 거부함

Log Insight Agents가 자체 서명된 인증서를 거부합니다.

### 문제

Log Insight Agents가 자체 서명된 인증서를 거부하고 서버와 연결하지 못합니다.

**참고** vRealize Log Insight Agent와의 연결 문제가 있는 경우 Agent의 디버그 수준을 1로 변경하여 세부 로그를 확인할 수 있습니다. [Log Insight Agents의 로그 세부 정보 수준 정의](#)를 참조하십시오.

### 원인

vRealize Log Insight Agent 로그에 표시된 메시지에 관련 원인이 포함되어 있습니다.

메시지	원인
Rejecting peer self-signed certificate. Public key doesn't match previously stored certificate's key.	<ul style="list-style-type: none"> <li>Log Insight 서버 인증서가 바뀐 경우에 이 문제가 발생할 수 있습니다.</li> <li>클러스터 환경에서 사용하도록 설정된 HA가 vRealize Log Insight 노드에서 다른 자체 서명된 인증서로 구성된 경우에 이 문제가 발생할 수 있습니다.</li> </ul>
Rejecting peer self-signed certificate. Have a previously received certificate which is signed by trusted CA.	Agent 측에 CA 서명된 인증서가 저장되어 있습니다.

### 해결책

- 대상 호스트 이름이 신뢰할 수 있는 vRealize Log Insight 인스턴스인지 확인한 후 vRealize Log Insight Agent cert 디렉토리에서 이전 인증서를 수동으로 삭제합니다.
  - Log Insight Windows Agent의 경우 C:\ProgramData\VMware\Log Insight Agent\cert로 이동합니다.
  - Log Insight Linux Agent의 경우 /var/lib/loginsight-agent/cert로 이동합니다.

**참고** 일부 플랫폼은 신뢰할 수 있는 인증서를 저장하는 데 비표준 경로를 사용할 수도 있습니다. Log Insight Agents에는 `ssl_ca_path=<fullpath>` 구성 매개 변수를 설정하여 신뢰할 수 있는 인증서 저장소의 경로를 구성하는 옵션이 있습니다. <fullpath>를 신뢰할 수 있는 루트 인증서 번들 파일의 경로로 바꿉니다. [Log Insight Agent SSL 매개 변수 구성](#)을 참조하십시오.

## vRealize Log Insight 서버가 암호화되지 않은 트래픽의 연결을 거부함

vRealize Log Insight 서버는 사용자가 암호화되지 않은 트래픽을 보내려고 하면 Log Insight Agents와의 연결을 거부합니다.

SSL 이외의 연결을 수락하도록 vRealize Log Insight 서버를 구성하거나, SSL cfapi 프로토콜 연결을 통해 데이터를 보내도록 Log Insight Agents를 구성할 수 있습니다.

## 문제


cfapi를 사용하여 암호화되지 않은 트래픽을 보내려고 하면 vRealize Log Insight 서버가 해당 연결을 거부합니다. Log Insight Agent 로그에 다음 오류 메시지가 나타납니다.

```
403 Forbidden.
```

## 원인

vRealize Log Insight가 SSL 연결만 허용하도록 구성된 반면 Log Insight Agents는 SSL 이외의 연결을 사용하도록 구성되었습니다.

## 해결책

- 1 SSL 이외의 연결을 수락하도록 vRealize Log Insight 서버를 구성합니다.
  - a 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
  - b 구성 아래에서 **SSL**을 클릭합니다.
  - c API 서버 SSL 머리글 아래에서 **SSL 연결 필요**를 선택 취소합니다.
  - d **저장**을 클릭합니다.
- 2 SSL Cfapi 프로토콜 연결을 통해 데이터를 보내도록 Log Insight Agents를 구성합니다.
  - a liagent.ini 파일을 포함하는 폴더로 이동합니다.

운영 체제	경로
<b>Linux</b>	/var/lib/loginsight-agent/
<b>Windows</b>	%ProgramData%\VMware\Log Insight Agent

- b 텍스트 편집기에서 liagent.ini 파일을 엽니다.
- c liagent.ini 파일의 [server] 섹션에서 ssl 키를 yes로 변경하고 프로토콜을 cfapi로 변경합니다.

```
proto=cfapi
ssl=yes
```

- d liagent.ini 파일을 저장한 후 닫습니다.