

# vRealize Log Insight 개발 자 리소스

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

# 목차

- 1** vRealize Log Insight 개발자 리소스 정보 4
- 2** SSL 전용 연결 적용 5
- 3** vRealize Log Insight Ingestion API 사용 6
  - 이벤트/수집 서비스 사용 6
  - 메시지/수집 서비스 사용(더 이상 사용되지 않음) 8
  - vRealize Log Insight REST API 10

# vRealize Log Insight 개발자 리소스 정보

# 1

"vRealize Log Insight 개발자 리소스"에서는 vRealize Log Insight Ingestion API에 대한 정보를 제공합니다.

## 대상 사용자

이 정보는 vRealize Log Insight Ingestion API를 사용하려는 모든 사용자를 대상으로 제공됩니다. REST 개념과 JSON 직렬화 형식에 대해 숙지하고 있어야 합니다.

## SSL 전용 연결 적용


vRealize Log Insight 웹 사용자 인터페이스를 사용하여 vRealize Log Insight Agents 및 Ingestion API가 서버로의 SSL 연결만 허용하도록 구성할 수 있습니다.

vRealize Log Insight API는 일반적으로 포트 9000의 HTTP 및 포트 9543의 HTTPS를 통해 연결할 수 있습니다. 두 포트는 vRealize Log Insight Agent 또는 사용자 지정 API 클라이언트에서 사용될 수 있습니다. 인증된 모든 요청에는 SSL이 필요하지만 vRealize Log Insight Agent 수집 트래픽을 비롯한 인증되지 않은 요청은 두 방법 중 하나를 통해 수행될 수 있습니다. 강제로 모든 API 요청에 SSL 연결이 사용되도록 할 수 있습니다. 이 옵션은 Syslog 포트 514 트래픽을 제한하지 않으며 vRealize Log Insight 사용자 인터페이스에 영향을 미치지 않습니다. 이 인터페이스에서 HTTP 포트 80 요청은 HTTPS 포트 443으로 계속 리디렉션됩니다.

### 사전 요구 사항

vRealize Log Insight 웹 사용자 인터페이스에 **관리자 편집** 권한을 가진 사용자로 로그인했는지 확인합니다. URL 형식은 `https://log-insight-host`이며 여기서 *log-insight-host*는 vRealize Log Insight 가상 장치의 IP 주소 또는 호스트 이름입니다.

### 절차

- 1 구성 드롭다운 메뉴 아이콘 을 클릭하고 **관리**를 선택합니다.
- 2 구성 아래에서 **SSL**을 클릭합니다.
- 3 [API 서버 SSL]에서 **SSL 연결 필요**를 선택합니다.
- 4 **저장**을 클릭합니다.

vRealize Log Insight API는 서버와의 SSL 연결만 허용합니다. SSL 이외의 연결은 거부됩니다.

# vRealize Log Insight Ingestion API 사용

## 3

vRealize Log Insight Ingestion API와 상호 작용하여 vRealize Log Insight 서버에 이벤트를 보낼 수 있습니다.

모든 API 요청 및 응답 본문은 헤더 필드가 Content-Type: application/json인 UTF8 인코딩 JSON 문자열입니다. 성공할 경우 모든 호출은 HTTP 응답 코드 200을 반환합니다.

본 장은 다음 항목을 포함합니다.

- 이벤트/수집 서비스 사용
- 메시지/수집 서비스 사용(더 이상 사용되지 않음)
- vRealize Log Insight REST API

## 이벤트/수집 서비스 사용

이벤트/수집 서비스를 사용하면 HTTP POST 요청을 통해 vRealize Log Insight 서버에 이벤트를 전송할 수 있습니다.

이벤트/수집 서비스에는 다음 구문이 사용됩니다.

프로토콜	값
HTTP	<code>http://loginsight_host:9000/api/v1/events/ingest/agentId</code>
HTTPS	<code>https://loginsight_host:9543/api/v1/events/ingest/agentId</code>

## HTTP 메서드

POST

**참고** vRealize Log Insight Ingestion API는 HTTP POST 요청당 4MB로 제한됩니다. 단일 text 필드의 최대 크기는 16KB입니다.

## 매개 변수

매개 변수	유형	전달 위치	설명
agentId	문자열	URL	전송하는 에이전트의 ID는 UUID 표준을 따라야 합니다. 에이전트는 공식 vRealize Log Insight Windows 또는 Linux 에이전트이거나 Ingestion API를 활용하는 클라이언트일 수 있습니다.
Content-Type: application/json	문자열	POST 본문	Content-Type 매개 변수는 POST 본문의 데이터 특성을 지정합니다.
Events array	어레이	POST 본문	<p>일련의 이벤트. 각 이벤트는 다음 형식이어야 합니다.</p> <pre>{   "events": [     {       "text": optional, message text as a string,       "timestamp": optional, timestamp encoded as number of milliseconds since Unix epoch in UTC,       "fields": optional array of [         {           "name": the name of the field,           "content": optional, the content of the field,           "startPosition": optional, the start position in the "text",           "length": optional, the length of the string in the "text",         }, ... ]       }, ... ]     }   ] }</pre> <p><b>참고</b> vRealize Log Insight 서버는 사용자가 제공한 "timestamp"와 vRealize Log Insight 서버의 현지 시간을 비교합니다. 기본 허용 추이 기간인 10분을 벗어난 "timestamp"를 제공하면 vRealize Log Insight 서버에서 사용자의 "timestamp"가 무시되고 서버의 현지 시간이 사용됩니다. "timestamp"가 제공되지 않는 경우 vRealize Log Insight는 도착 시간을 사용합니다.</p> <p><b>참고</b> 필드의 "content"가 제공되지 않는 경우 "startPosition" 및 "length"가 제공되어 "text" 필드 문자열의 유효한 위치를 가리켜야 합니다.</p>

## HTTP 값 반환

이름	유형	설명
200 OK	정수	표준 HTTP 응답 코드
400 Bad Request		
500 Internal Server Error		
503 Service Unavailable		이 응답은 서버가 오버로드되었음을 나타냅니다. Retry-After 응답 헤더에는 제시된 시간(초)이 제안됩니다.

## 요청 예

```
POST http://loginsight:9000/api/v1/events/ingest/4C4C4544-0037-5910-805A-C4C04F585831
```

```
Host: loginsight:9000
```

```
Connection: keep-alive
```

```
Content-Type: application/json
```

```

charset: utf-8
Content-Length: ??

{"events": [{
  "fields": [
    {"name": "Channel", "content": "Security"},
    {"name": "EventID", "content": "4688"},
    {"name": "EventRecordID", "content": "33311266"},
    {"name": "Keywords", "content": "Audit Success"},
    {"name": "Level", "content": "Information"},
    {"name": "OpCode", "content": "Info"},
    {"name": "ProcessID", "content": "4"},
    {"name": "ProviderName", "content": "Microsoft-Windows-Security-Auditing"},
    {"name": "Task", "content": "Process Creation"},
    {"name": "ThreadID", "content": "64"}
  ],
  "text": "A new process has been created.",
  "timestamp": 1396622879241
}]
}
```

## 응답 예

```
HTTP/1.1 200 OK
```

```
{"status":"ok","message":"events ingested","ingested":18}
```

## 메시지/수집 서비스 사용(더 이상 사용되지 않음)

메시지/수집 서비스를 사용하면 HTTP POST 요청을 통해 vRealize Log Insight 서버에 이벤트를 전송할 수 있습니다.

메시지/수집 서비스에는 다음 구문이 사용됩니다.

프로토콜	값
HTTP	<code>http://loginsight_host:9000/api/v1/messages/ingest/agentId</code>
HTTPS	<code>https://loginsight_host:9543/api/v1/messages/ingest/agentId</code>

## HTTP 메서드

POST

**참고** vRealize Log Insight Ingestion API는 HTTP POST 요청당 4MB로 제한됩니다. 단일 text 필드의 최대 크기는 16KB입니다.



## 매개 변수

매개 변수	유형	전달 위치	설명
agentId	문자열	URL	전송하는 에이전트의 ID는 UUID 표준을 따라야 합니다. 에이전트는 공식 vRealize Log Insight Windows 또는 Linux 에이전트이거나 Ingestion API를 활용하는 클라이언트일 수 있습니다.
Content-Type: application/json	문자열	POST 본문	Content-Type 매개 변수는 POST 본문의 데이터 특성을 지정합니다.
Events array	어레이	POST 본문	<p>일련의 이벤트. 각 이벤트는 다음 형식이어야 합니다.</p> <pre>{   "messages":   [     {       "text": optional, message text as a string,       "timestamp": optional, timestamp encoded as number of milliseconds since Unix epoch in UTC,       "fields": optional array of       [         {           "name": the name of the field,           "content": optional, the content of the field,           "startPosition": optional, the start position in the "text",           "length": optional, the length of the string in the "text",         },...       ],...     },...   ] }</pre> <p><b>참고</b> vRealize Log Insight 서버는 사용자가 제공한 "timestamp"와 vRealize Log Insight 서버의 현지 시간을 비교합니다. 기본 허용 추이 기간인 10분을 벗어난 "timestamp"를 제공하면 vRealize Log Insight 서버에서 사용자의 "timestamp"가 무시되고 서버의 현지 시간이 사용됩니다. "timestamp"가 제공되지 않는 경우 vRealize Log Insight는 도착 시간을 사용합니다.</p> <p><b>참고</b> 필드의 "content"가 제공되지 않는 경우 "startPosition" 및 "length"가 제공되어 "text" 필드 문자열의 유효한 위치를 가리켜야 합니다.</p>

## HTTP 값 반환

이름	유형	설명
200 OK	정수	표준 HTTP 응답 코드
400 Bad Request		
500 Internal Server Error		
503 Service Unavailable		이 응답은 서버가 오버로드되었음을 나타냅니다. Retry-After 응답 헤더에는 제시된 시간(초)이 제안됩니다.

## 요청 예

```
POST http://loginsight:9000/API/v1/messages/ingest/4C4C4544-0037-5910-805A-C4C04F585831
```

```
Host: loginsight:9000
```

```
Connection: keep-alive
```

```
Content-Type: application/json
```

```

charset: utf-8
Content-Length: ??

{"messages": [{
  "fields": [
    {"name": "Channel", "content": "Security"},
    {"name": "EventID", "content": "4688"},
    {"name": "EventRecordID", "content": "33311266"},
    {"name": "Keywords", "content": "Audit Success"},
    {"name": "Level", "content": "Information"},
    {"name": "OpCode", "content": "Info"},
    {"name": "ProcessID", "content": "4"},
    {"name": "ProviderName", "content": "Microsoft-Windows-Security-Auditing"},
    {"name": "Task", "content": "Process Creation"},
    {"name": "ThreadID", "content": "64"}
  ],
  "text": "A new process has been created.",
  "timestamp": 1396622879241
}]
}
```

## 응답 예

```

HTTP/1.1 200 OK

{"status":"ok","message":"messages ingested","ingested":18}
```

## vRealize Log Insight REST API

REST API는 vRealize Log Insight와 여기에서 수집하는 데이터에 대해 프로그래밍 방식으로 액세스할 수 있도록 합니다.

API를 사용하여 vRealize Log Insight 데이터스토어에 이벤트를 삽입하고, 이벤트를 쿼리하고, 제품 구성을 변경할 수 있습니다. 또한 API를 사용하여 vRealize Log Insight를 설치하거나 업그레이드할 수도 있습니다.

자세한 내용은 <https://www.vmware.com/go/loginsight/api>에서 "vRealize Log Insight API 참조"를 참조하십시오.