VMware vRealize Log Insight Developer's Guide

vRealize Log Insight 2.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001660-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

About vRealize Log Insight Developer's Guide

1

The *VMware vRealize Log Insight Developer's Guide* provides information about the Log Insight Ingestion API.

Intended Audience

This information is intended for anyone who wants to use the Log Insight Ingestion API. You must be familiar with REST concepts and with the JSON serialization format.

Using the Log Insight Ingestion API 2

You can interact with the Log Insight Ingestion API to send events to the Log Insight server.

All API request and response bodies are UTF8 encoded JSON strings with `Content-Type: application/json` header field. On success, all calls return HTTP response code 200.

Enforce SSL Only Connections 3

You can use the Log Insight Web UI to configure the Log Insight Agents and the Ingestion API to allow only SSL connections to the server.

NOTE The current version of Log Insight doesn't support syslog SSL connections and works only for Log Insight Ingestion API.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://*log-insight-host*, where *log-insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Click the configuration drop-down menu icon  and select **Administration**.

2 Under Configuration, click **SSL**.

3 Under the API Server SSL, select the **Require SSL Connection** check box.

4 Click **Save**.

Log Insight API allows only SSL connections to the server. Non-SSL connections are refused.

API Services 4

A list of services that the Log Insight Ingestion API provides.

Using the messages/ingest Service

You can use the messages/ingest service to send events to a Log Insight server using HTTP POST requests.

The messages/ingest service uses the following syntax.

Protocol	Value
HTTP	`http://loginsight_host:9000/api/v1/messages/ingest/agentId`
HTTPS	`https://loginsight_host:9543/api/v1/messages/ingest/agentId`

If you enforce SSL from the Web UI you will be able to use only HTTPS. See Chapter 3, "Enforce SSL Only Connections," on page 9.

HTTP Method

`POST`

NOTE The Log Insight Ingestion API has a limit of 100 KB per HTTP POST request.

Parameters

Parameter	Type	Where to pass	Description
`agentId`	String	In URL	The ID of the sending agent should follow the UUID standard. The agent may be an official Log Insight Windows or Linux agent or any client leveraging the Ingestion API.
`Content-Type: application/json`	String	In POST body	The `Content-Type` parameter specifies the nature of the data in the POST body.

`Events array`	Array	In POST body	An array of events. Each event must have the following format.
			`{"messages":`
			`[{`
			`"text": optional, message text as a string,`
			`"timestamp": optional, timestamp encoded as number of milliseconds since Unix epoch,`
			`"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",`
			`},...]`
			`},...]`
			`}`
			NOTE The Log Insight server compares the `"timestamp"` you provide with the local time on the Log Insight server. If you provide a `"timestamp"` outside of the default 10 minutes tolerated drift window, the Log Insight server ignoers your `"timestamp"` and uses its local time. If `"timestamp"` is not present, the Log Insight server uses arrival time.
			NOTE If the `"content"` of a field is not present, then `"startPosition"` and `"length"` must be present and must point to a valid position in the `"text"` field string.

Return HTTP Values

Name	Type	Description
`200 OK`	Integer	Standard HTTP response codes
`400 Bad Request`		
`500 Internal Server Error`		
`503 Service Unavailable`		This response indicates that the server is overloaded. The `Retry-After` response header provides the suggested retry time in seconds.

Example Request

```
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
            }
           ]
}
```

Example Response

```
HTTP/1.1 200 OK

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

Index