vRealize Log Insight Developer Resources

11-SEP-2017

vRealize Log Insight 4.3

vmware®

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

https://docs.vmware.com/

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

vRealize Log Insight Developer Resources

1

vRealize Log Insight Developer Resources provides information about the vRealize Log Insight API.

Intended Audience

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

Enforce SSL-Only Connections

2

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

The vRealize Log Insight API is normally reachable through HTTP on port 9000 and through HTTPS on port 9543. Both ports can be used by the vRealize Log Insight Agent or custom API clients. All authenticated requests require SSL, but unauthenticated requests, including vRealize Log Insight Agent ingestion traffic, can be performed with either. You can force all API request to use SSL connections. This option does not restrict Syslog port 514 traffic and does not affect the vRealize Log Insight user interface, for which HTTP port 80 requests continue redirecting to HTTPS port 443.

Prerequisites

Verify that you are logged in to the vRealize 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 vRealize 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 **Require SSL Connection**.
4. Click **Save**.

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

Using the vRealize Log Insight Ingestion API

3

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

This chapter includes the following topics:

Using the events/ingest Service

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

The events/ingest service uses the following syntax.

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

HTTP Method

POST

Note The vRealize Log Insight Ingestion API has a limit of 4 MB per HTTP POST request. The maximum size of a single `text` field is 16 KB.

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 vRealize 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. `{"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", },...] },...] }` **Note** The vRealize Log Insight server compares the "`timestamp`" you provide with the local time on the vRealize Log Insight server. If you provide a "`timestamp`" outside of the default 10 minutes tolerated drift window, the vRealize Log Insight server ignores your "`timestamp`" and uses its local time. If "`timestamp`" is not present, vRealize Log Insight 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/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
             }
           ]
}
```

Example Response

```
HTTP/1.1 200 OK

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

Using the messages/ingest Service (Deprecated)

You can use the messages/ingest service to send events to a vRealize 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`

HTTP Method

POST

Note The vRealize Log Insight Ingestion API has a limit of 4 MB per HTTP POST request. The maximum size of a single `text` field is 16 KB.

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 vRealize 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 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", },...] },...] }` **Note** The vRealize Log Insight server compares the "`timestamp`" you provide with the local time on the vRealize Log Insight server. If you provide a "`timestamp`" outside of the default 10 minutes tolerated drift window, the vRealize Log Insight server ignores your "`timestamp`" and uses its local time. If "`timestamp`" is not present, vRealize Log Insight 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`		

Name	Type	Description
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}
```

The vRealize Log Insight REST API

The REST API provides programmatic access to vRealize Log Insight and to the data it collects.

You can use the API to insert events into the vRealize Log Insight data store, to query for events and to change product configuration. You can also use the API to install or upgrade vRealize Log Insight.

For more information, see the vRealize Log Insight API reference at https://www.vmware.com/go/loginsight/api.