Splunk® Supported Add-ons
Splunk Add-on for HAProxy released

Generated: 11/24/2022 10:19 am

Table of Contents

Overview

About the Splunk Add-on for HAProxy

Version	2.0.0
Vendor Products	HAProxy 1.7, 1.8, 2.0, 2.1, 2.2

The Splunk Add-on for HAProxy enables a Splunk software administrator to collect HAProxy logs in syslog format. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on. This add-on provides the **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security.

Download the Splunk Add-on for HAProxy from Splunkbase at http://splunkbase.splunk.com/app/3135.

Discuss the Splunk Add-on for HAProxy on Splunk Answers at Questions related to Splunk Add-on for HAProxy.

Source types for the Splunk Add-on for HAProxy

The Splunk Add-on for HAProxy supports the following data sources using the following collection methods and provides the following source types, event types, and **CIM** mapping.

Data source	Collection method	Source type	Event type	CIM data models	ITSI data models
HAProxy logs, Custom format	File monitor or network (TCP/UDP)	`haproxy:splunk:http`	`haproxy_splunk_http`	Web	N/A
HAProxy logs, TCP format	File monitor or network (TCP/UDP)	`haproxy:tcp`	`haproxy_tcp`	N/A	Load Balancer
HAProxy logs, HTTP format	File monitor or network (TCP/UDP)	`haproxy:http`	`haproxy_http`	N/A	Load Balancer
HAProxy logs, CLF HTTP format	File monitor or network (TCP/UDP)	`haproxy:clf:http`	`haproxy_clf_http`	N/A	N/A
HAProxy logs, default format	File monitor or network (TCP/UDP)	`haproxy:default`	`haproxy_default`	N/A	N/A

Release notes for the Splunk Add-on for HAProxy

Version 2.0 of the Splunk Add-on for HAProxy was released on November 23, 2020.

Compatibility

Version 2.0.0 of the Splunk Add-on for HAProxy is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.2.x, 7.3.x, 8.0.x, 8.1.0
CIM	4.17
Platforms	Platform independent
Vendor Products	HAProxy 1.7, 1.8, 2.0, 2.1, 2.2

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

- Support for HAProxy versions 1.7, 1.8, 2.0, 2.1, 2.2.
- Support for the latest Common Information Model (CIM) version 4.17.
- Support for CLF HTTP log and Custom HTTP log

Fixed Issues

Version 2.0.0 of the Splunk Add-on for HAProxy has the following fixed issues:

If no issues appear, no issues were currently fixed for this release.

Known issues

Version 2.0.0 of the Splunk Add-on for HAProxy contains no known issues.

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for HAProxy does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for HAProxy

Latest release

The latest version of the Splunk Add-on for HAProxy is version 2.0.0. See Release notes for the Splunk Add-on for HAProxy for the release notes of this latest version.

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for HAProxy was released on April 21, 2016.

Compatibility

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.x
CIM	4.11
Platforms	Platform independent
Vendor Products	HAProxy 1.4+

New features

Version 1.0.0 of the Splunk Add-on for HAProxy has the following new features.

Date	Issue number	Description
2015-09-14	ADDON-5529	Create a new add-on for HAProxy.
2016-02-10	ADDON-7756	Add mapping to ITSI Load Balancer module to support integration with ITSI.

Known issues

Version 1.0.0 of the Splunk Add-on for HAProxy contains no known issues.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for HAProxy does not incorporate any third-party software or libraries.

Installation and Configuration

Hardware and software requirements for the Splunk Add-on for HAProxy

HAProxy requirements

There are no requirements for the HAProxy platform.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements: see System Requirements in the Splunk Enterprise *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

Installation overview for the Splunk Add-on for HAProxy

Complete the following steps to install and configure this add-on on your supported platform.

1. Download the Splunk Add-on for HAProxy.

2. Install the Splunk Add-on for HAProxy.

3. Configure HAProxy to send syslog data to the Splunk Add-on for HAProxy.

4. Configure inputs for the Splunk Add-on for HAProxy.

Download the Splunk Add-on for HAProxy

Download the add-on from Spunkbase here: https://splunkbase.splunk.com/app/3135.

Install the Splunk Add-on for HAProxy

Installation instructions

See Installing add-ons in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

- single-instance Splunk Enterprise
- distributed Splunk Enterprise
- Splunk Cloud

Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise.

Where to install this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise.

Splunk instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where HAProxy knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. Required if you use universal forwarders to collect data.
Heavy Forwarders	Yes	No	Forwarder needs to be installed directly on the HAProxy server for file monitoring*. If listening over a network port, forwarder does not need to be installed directly on the HAProxy server.
Universal Forwarders	Yes	No	This add-on needs to be installed on indexers if you use a universal forwarder rather than a heavy forwarder for data collection. Forwarder needs to be installed directly on the HAProxy server for file monitoring*. If listening over a network port, forwarder does not need to be installed directly on the HAProxy server.

*When using a file monitor input, the syslog file can be copied to the machine where the forwarder is installed as an alternative to installing the forwarder on the HAProxy server.

Distributed deployment feature compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying the configured add-on.

Configure HAProxy to send syslog data

To configure HAProxy to log in syslog, edit the HAProxy server configuration file (`/etc/haproxy/haproxy.cfg`) and include the following lines:

```
global
log 127.0.0.1 local0
```

You need to configure HAProxy to send events to the Splunk platform through syslog and use one of the supported formats.

Custom log format

The **Splunk HTTP format** is a custom log format for the Splunk Add-on for HAProxy. This is the only format which provides CIM compliance. You can configure this format by using the following `defaults` and `frontend` config sections for

the HAProxy server configuration file found in the following location: `/etc/haproxy/haproxy.cfg`. Do not change the order of the configuration. You can only add additional configurations at the end of all the capture statements specified in the configuration below.

```
defaults
   option httplog
   log-format "%{+Q}o client_ip=%ci client_port=%cp datetime_of_request=[%tr] frontend_name_transport=%ft
backend_name=%b server_name=%s time_to_receive_full_request=%TR Tw=%Tw Tc=%Tc response_time=%Tr
active_time_of_request=%Ta status_code=%ST bytes_read=%B captured_request_cookie=%CC
captured_response_cookie=%CS termination_state_with_cookie_status=%tsc actconn=%ac feconn=%fc beconn=%bc
srv_conn=%sc retries=%rc srv_queue=%sq backend_queue=%bq captured_request_headers_default_style=%hr
captured_response_headers_default_style=%hs server_ip=%si server_port=%sp frontend_name=%f http_method=%HM
http_request_uri_without_query=%HP http_request_query_string=%HQ http_request_uri=%HU bytes_uploaded=%U
ssl_ciphers=%sslc ssl_version=%sslv"
```

```
frontend frontend_name
   capture request header Host len <len>
   capture request header Content-Type len <len>
   capture request header User-Agent len <len>
   capture request header Referer len <len>
   capture request header X-Forwarded-For len <len>
   capture response header Content-Type len <len>
   capture cookie Cookie_2 len <len>
```

TCP format

For **TCP format**; Set `option tcplog` on the frontend to enable this format.

HTTP format

HTTP format; Set `option httplog` on the frontend to enable this format.

CLF HTTP format

The **CLF HTTP format** is equivalent to the HTTP format, but with the fields arranged in CLF form. Set `option httplog clf` on the frontend to enable this format.

Default format

The **default format** only provides basic information about the incoming connection and therefore it is not recommended.

Override character limit

By default, HAProxy will truncate log lines with more than `1024` characters before being sent. To overcome this limit you need to override the default value by using the following config in the global settings: `log <address> len <length>`.

For the `<length>`, specify a value between 80 to 65535. You must specify a large enough value to avoid truncation.

For more information about configuring logging in HAProxy, see http://cbonte.github.io/haproxy-dconv/2.2/configuration.html#8.

Next, configure your data collection node to receive data from HAProxy as described in Configure inputs for the Splunk Add-on for HAProxy.

Configure inputs for the Splunk Add-on for HAProxy

There are two ways to capture the syslog data from HAProxy.

1. Create a file monitor input to monitor the syslog file generated by the HAProxy server or to monitor the files on a syslog aggregator.

2. Create a TCP or UDP input to capture the data sent on the port you have configured in HAProxy.

Note: For information about timestamp processing options for syslog events, see Syslog and timestamps in *Splunk Add-ons.*

Monitor input

To configure the Splunk platform to monitor the syslog file generated by the HAProxy server, you can use either Splunk Web to create the monitor input or configure `inputs.conf` directly. If you use a syslog aggregator, you can create a file monitor input to monitor the files generated by the aggregator.

Configure Monitoring through Splunk Web

Configure a file monitoring input on your data collection node for the HAProxy syslog file.

1. Log into Splunk Web.
2. Select **Settings** > **Data inputs** > **Files & directories**.
3. Click **New**.
4. Click **Browse** next to the **File or Directory** field.
5. Navigate to the syslog file generated by the HAProxy server (for example, `/var/log/haproxy.log`) and click **Next**.
6. On the Input Settings page, next to Source type, click **Select**. In the Select Source Type dropdown, select **Network & Security**, then one of the following depending on your HAProxy syslog configuration:

- **haproxy:splunk:http**
- **haproxy:http**
- **haproxy:tcp**
- **haproxy:clf:http**
- **haproxy:default**

1. Click **Review**.
2. After you review the information, click **Submit**.

Configure inputs.conf

You can create an `inputs.conf` file and configure the monitor input in this file instead of using Splunk Web.

1. Using a text editor, create a file named `inputs.conf` in the local folder of the add-on:
   - `$SPLUNK_HOME/etc/apps/Splunk_TA_haproxy/local` on Unix based systems.
   - `%SPLUNK_HOME%\etc\apps\Splunk_TA_haproxy\local` on Windows systems.

2. Add the following stanza and lines, replacing `<path>` with the actual path to the syslog file (for example, `/var/log/haproxy.log`) and replacing `<log format>` with the format you specified in the HAProxy configuration, either `splunk:http`, `tcp`, `http`, `clf:http` or `default`.

   ```
   [monitor://<path>]
   sourcetype=haproxy:<log format>
   disabled = 0
   ```
3. Save the file.
4. Restart the Splunk platform in order for the new input to take effect.

TCP/UDP input

In the Splunk platform node handling data collection, configure the TCP/UDP input to match your configurations in HAProxy and set your source type to `haproxy:splunk:http`, `haproxy:tcp`, `haproxy:http`, `haproxy:clf:http` or `haproxy:default`, depending upon your HAProxy syslog configuration. The CIM mapping and dashboard panels are dependent on this source type.

For information on how to configure a Splunk forwarder or single-instance to receive a syslog input, see Get data from TCP and UDP ports in the *Getting Data In* manual.

Validate data collection

After you configure the input, run this search to check that you are ingesting the expected data:

```
sourcetype=haproxy:*
```

Reference

Lookups for the Splunk Add-on for HAProxy

The Splunk Add-on for HAProxy has one **lookup**. The lookup file maps a field from the HAProxy system to CIM-compliant values in the Splunk platform. The lookup file is located in `$SPLUNK_HOME/etc/apps/Splunk_TA_haproxy/lookups`.

Filename	Description
`haproxy_httpstatus.csv`	Maps HTTP `status` codes to `status_description` and `status_type`.

Troubleshooting

Troubleshoot the Splunk Add-on for HAProxy

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.