Splunk® Supported Add-ons
Splunk Add-on for Apache Web Server released

Generated: 11/05/2022 11:57 am

Table of Contents

Overview

About the Splunk Add-on for Apache Web Server

Version	2.1.0
Vendor Products	Apache 2.4.x

The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. 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 inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Web.

Download the Splunk Add-on for Apache Web Server from Splunkbase at http://splunkbase.splunk.com/app/3186.

Discuss the Splunk Add-on for Apache Web Server on the Splunk Community page.

Hardware and software requirements for the Splunk Add-on for Apache Web Server

Apache Web Server setup requirements

You must have access to the Apache Web Server installation directory so that you can configure Apache Web Server to format log data for the Splunk platform to ingest through file monitoring.

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.

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.

Installation overview for the Splunk Add-on for Apache Web Server

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

1. Download the add-on from Spunkbase.

2. Install the Splunk Add-on for Apache Web Server.

3. Configure Apache Web Server to send logs to Splunk Add-on for Apache Web Server.

4. Configure inputs for the Splunk Add-on for Apache Web Server.

Installation and Configuration

Install the Splunk Add-on for Apache Web Server

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 that require Apache Web Server management.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to monitor Apache Web Server log. Required if you use universal or light forwarders to monitor Apache Web Server log output.
Heavy Forwarders	Yes	No	Use any kind of forwarder.
Universal Forwarders	Yes	No	Use any kind of forwarder.
Light Forwarders	Yes	No	Use any kind of forwarder.

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. Before installing this add-on to a cluster, remove the `eventgen.conf` file and all files in the `Samples` folder.
Indexer Clusters	Yes	You can install this add-on on a indexer cluster for all index-time functionality. Before installing this add-on to a cluster, remove the `eventgen.conf` file and all files in the `Samples` folder.
Deployment Server	Yes	You can use deployment server to deploy the configured add-on to forwarders. Before distributing this add-on to your forwarders, remove the `eventgen.conf` file and all files in the `Samples` folder.

Upgrade the Splunk Add-on for Apache Web Server

No special steps are required to upgrade the Splunk Add-on for Apache Web Server from version 2.0.0. to version 2.1.0. Follow the steps in the Install the Splunk Add-on for Apache Web Server topic in this manual.

Update the apache log formatting configuration to generate logs in the new format by following the Configure log formatting on the Apache Web Server using httpd.conf topic in this manual.

Based on your configuration, perform changes in the Configure monitor inputs for the Splunk Add-on for Apache Web Server topic in this manual.

See Configure enhanced log formatting on the Apache Web Server using httpd.conf for more information.

- Splunk best practice is to use the enhanced Key-Value pair or JSON format. The sourcetypes for apache access logs when using the Key-value pair will be `apache:access:kv` The sourcetype for apache access logs when using the Json format will be `apache:access:json`
- For the default *out-of-the-box* format, the sourcetype for apache access logs will be `apache:access:combined`

Configure enhanced log formatting on the Apache Web Server using httpd.conf

Configure log formatting on the Apache Web Server using httpd.conf. This lets the Splunk Add-on for Apache Web Server monitor your deployment's log files.

To make sure you have all the required fields present in `apache access_log`, Splunk best practice is to use an enhanced custom log format in the apache `httpd.conf` file. For more information, see Configure monitor inputs for the Splunk Add-on for Apache Web Server.

The Splunk Add-on for Apache Web Server now supports the default *out-of-the-box* log format of Apache Web Server; the add-on extracts all possible CIM fields where present and makes them searchable. However, this log format is missing many critical CIM fields (e.g. user, hostname, etc), so note that the add-on does not apply CIM Data Model tags to those events. Splunk best practice is still to use an enhanced custom log format which requires modifications to `httpd.conf`, and use the `apache:access:kv` or `apache:access:json` sourcetypes. To use the default out-of-the-box events, ignore the below steps & proceed with Configure monitor inputs for the Splunk Add-on for Apache Web Server.

1. Open the `httpd.conf` in the Apache Web Server installation folder `$APACHE_HOME/etc/apache/conf/httpd.conf`

   The default location of httpd.conf might be different on different platforms.

2. Look for the statement `<IfModule log_config_module>` and replace the whole block with the following stanza:

```
<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common

 <IfModule logio_module>
```

```
    # You need to enable mod_logio.c to use %I and %O
    LogFormat "time=%{%s}t.%{usec_frac}t, bytes_in=%I, bytes_out=%O, cookie=\"%{Cookie}i\",
server=%v, dest_port=%p, http_content_type=\"%{Content-type}i\", http_method=\"%m\",
http_referrer=\"%{Referer}i\", http_user_agent=\"%{User-agent}i\", ident=\"%l\",
response_time_microseconds=%D, client=%h, status=%>s, uri_path=\"%U\", uri_query=\"%q\",
user=\"%u\"" splunk_kv

    #LogFormat "{\"time\":\"%{%s}t.%{usec_frac}t\", \"bytes_in\":\"%I\", \"bytes_out\":\"%O\",
\"cookie\":\"%{Cookie}i\", \"server\":\"%v\", \"dest_port\":\"%p\",
\"http_content_type\":\"%{Content-type}i\", \"http_method\":\"%m\",
\"http_referrer\":\"%{Referer}i\", \"http_user_agent\":\"%{User-agent}i\", \"ident\":\"%l\",
\"response_time_microseconds\":\"%D\", \"client\":\"%h\", \"status\":\"%>s\", \"uri_path\":\"%U\",
\"uri_query\":\"%q\", \"user\":\"%u\"}" splunk_json

  #LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio

</IfModule>
    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    # CustomLog "logs/access_log" common
    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" splunk_kv
    #CustomLog "logs/access_log" splunk_json
    #CustomLog "logs/access_log" combined
</IfModule>
```

3. Choose either the `splunk_kv` or `splunk_json` format for access logs. Only one format can be enabled at a time. The information provided by either `splunk_kv` and `splunk_json` is the same. The difference is only in formatting. By default, `splunk_kv` is enabled and the `splunk_json` is disabled. To enable the `splunk_json` format:
    1. Comment out the `splunk_kv` definition and log file directives.
    2. Uncomment the `splunk_json` definition and log file directives.

> The KV pair formatting is simpler when compared to JSON formatting. The best practice is to include new custom fields, if required, in KV format. If applied in JSON format, then it must comply with strict JSON formatting.

4. Validate the syntax of the conf file after you make your changes. `sudo apache2ctl configtest`

   or

   `sudo httpd -t` If the output says `syntax ok`, proceed.
5. Restart Apache Web Server. If the log format in Apache Web Server is configured correctly, you receive log files that look like this:
    - For `splunk_kv`

```
time=###TIME###.000000, bytes_in=###BYTES_IN###, bytes_out=###BYTES_OUT###,
cookie="###COOKIE###", server=C6852495051.domain, dest_port=###DEST_PORT###,
http_content_type="###HTTP_CONTENT_TYPE###", http_method="###HTTP_METHOD###",
http_referrer="###HTTP_REFERRER###", http_user_agent="###HTTP_USER_AGENT###", ident="1",
response_time_microseconds=###RESPONSE_TIME_MICROSECONDS###, client=###CLIENT###,
status=###STATUS###, uri_path="###URI_PATH###", uri_query="###URI_QUERY###", user="xyz123"
```

- For `splunk_json`

```
{"time":"###TIME###.000000", "bytes_in":"###BYTES_IN###", "bytes_out":"###BYTES_OUT###",
"cookie":"###COOKIE###", "server":"C6852495051.domain", "dest_port":"###DEST_PORT###",
"http_content_type":"###HTTP_CONTENT_TYPE###", "http_method":"###HTTP_METHOD###",
"http_referrer":"###HTTP_REFERRER###", "http_user_agent":"###HTTP_USER_AGENT###",
"ident":"1", "response_time_microseconds":"###RESPONSE_TIME_MICROSECONDS###",
"client":"###CLIENT###", "status":"###STATUS###", "uri_path":"###URI_PATH###",
"uri_query":"###URI_QUERY###", "user":"xyz123"}
```

The new fields will be auto extracted without making any change in the add-on's field extraction.

Configure monitor inputs for the Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server collects data through file monitoring. After installing the add-on, you need to configure the platform to monitor the access and error log file generated by Apache Web Server. You can user either Splunk Web to create the monitor input or edit the `inputs.conf` directly.

Configure monitoring input through Splunk Web

Configure file monitoring inputs on your data collection node for the Apache Web Server access and error log file.

Configure access log input

Configure file monitoring inputs on your data collection node for the Apache Web Server access log 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 access log file generated by the Apache Web Server and click **Next**.

   The default location of the access log file may vary from different system, The default location of access log usually is /var/log/apache/access.log or /var/log/apache2/access.log, but your path may differ.
6. On the Input Settings page, next to Source type, click **Select**. In the **Select Source Type** drop-down, select **Web**, then `apache:access:kv` or `apache:access:json` or `apache:access:combined`, and `apache:error`, or type these source types in the search field.

   Users can select the apache:access:json formatting option only after completing the apache:access:json formatting configuration steps from the Configure log formatting on the Apache Web Server using httpd.conf topic in this manual.
7. Click **Review**.
8. After you review the information, click **Submit**.

Configure error log inputs

Configure file monitoring inputs on your data collection node for the Apache Web Server error log 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 error log file generated by the Apache Web Server and click **Next**.

   The default location of the error log file may vary from different system, The default location of error log usually is /var/log/apache/error.log or /var/log/apache2/error.log, but your path may differ. And Apache Web Server may have multiple access logs and error logs, you can add an asterisk wildcard at the end of file name to retreive all log data.

6. On the Input Settings page, next to Source type, click **Select**. In the **Select Source Type** drop-down, select **Web**, then `apache:access:kv` or `apache:access:json`, and `apache:error`, or type these source types in the search field.

   Users can select the apache:access:json formatting option only after completing the apache:access:json formatting configuration steps from the Configure log formatting on the Apache Web Server using httpd.conf topic in this manual.

7. Click **Review**.
8. After you review the information, click **Submit**.

Configure monitoring input through 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 `$SPLUNK_HOME/etc/apps/Splunk_TA_apache/local` folder.
2. Add the following stanza and lines, replacing `<path>` with the actual path to access log and error log, and save the file.
   Note: You can add an asterisk wildcard at the end of the file name to retrieve all log data.

   ```
   [monitor://<path>]
   sourcetype=apache:error
   disabled = 0
   [monitor://<path>]
   sourcetype=apache:access:kv
   disabled = 0
   ```

   Users can select the `apache:access:combined` option for the default out-of-the-box events. For the `apache:access:json` formatting option, users can only select this after completing the `apache:access:json` formatting configuration steps in enhanced log formatting on the Apache Web Server using httpd.conf.

3. Restart the Splunk platform for the new input to take effect.

Troubleshoot the Splunk Add-on for Apache Web Server

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*.

Data not coming in

Verify that your source type is set to `apache:access:*` or `apache:error`.

Reference

Source types for the Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server provides the index-time and search-time knowledge for Apache Web Server events, metadata, user and group information, collaboration data, and tasks in the following formats.

Source type	Description	CIM data models
`apache:access`	The server access log records all requests processed by the server, the location and content of the access.	Web
`apache:error`	The server error log sends diagnostic information and records any errors that it encounters in processing requests.	None
`apache:access:kv`	Apache httpd detailed server access log information in KV format.	Web
`apache:access:json`	Apache httpd detailed server access log information in JSON format.	Web
`apache:access:combined`	Apache httpd detailed server access log in Out-of-the-box default format.	None

Lookups for the Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server has one lookup, the http status lookup, which located in `$SPLUNK_HOME/etc/apps/Splunk_TA_apache/lookups/apache_httpstatus.csv`

Filename	Description
`apache_httpstatus.csv`	Maps `http status` to `status_description` and `status_type`

Release Notes

Release notes for Splunk Add-on for Apache Web Server

About this release

Version 2.1.0 of the Splunk Add-on for Apache was released on June 3, 2022. This release is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.1.x, 8.2.x
CIM	5.0.1
Platforms	Platform Independent
Vendor Products	Apache 2.4.x and later

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

Version 2.1.0 of the Splunk Add-on for Apache Web Server contains the following new features.

- Added support for Apache version 2.4.53.
- Added support for the `apache:access:combined` sourcetype, which provides server access log information in an *out-of-the-box* default format.

Splunk best practice is to use the enhanced log format instead and use the apache:access:kv or apache:access:json sourcetypes

- Enhanced CIM mappings and added support for CIM version 5.0.1.
    - Added extraction for new CIM fields **url_length, http_referrer_domain and url_domain** in the `apache:access:kv` and `apache:access:json` sourcetypes.

Field Mapping Changes

Version 2.1.0 of the Splunk Add-on for Apache Web Server introduces field changes to the `apache:access:kv` and `apache:access:json` sourcetypes. See the following table for information in data model changes:

Source-type	Fields added	Fields removed	Fields modified
`apache:access:combined`	status_description, uri_query, http_user_agent, http_version, http_referrer, bytes, client, request, src, url, http_method, status_type, http_user_agent_length, http_referrer_domain, action, bytes_out, uri_path, logname, status, bytes_in, request_bytes, user, vendor_product, timestamp		

Source-type	Fields added	Fields removed	Fields modified
`apache:access:kv`, `apache:access:json`	url_length, http_referrer_domain, url_domain		

Fixed issues

Version 2.1.0 of the Splunk Add-on for Apache Web Server contains no fixed issues.

Known issues

Version 2.1.0 of the Splunk Add-on for Apache Web Server contains no known issues.

Third-party software attributions

Version 2.1.0 of the Splunk Add-on for Apache Web Server does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Apache Web Server

The latest version of the Splunk Add-on for Apache Web Server is version 2.1.0. See Release notes for the Splunk Add-on for Apache Web Server for release notes of this latest version.

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Apache was released on September 23, 2020. This release is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.2.x, 7.3.x, 8.0.x
CIM	4.17
Platforms	Platform Independent
Vendor Products	Apache 2.4.x and later

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

Version 2.0.0 of the Splunk Add-on for Apache Web Server contains the following new features.

- Support for Apache version 2.4.46.
- Support for the following sourcetypes:
  - The `apache:access:kv`, which provides server access log information in KV format.

    - The `apache:access:json`, which provides server access log information in JSON format.
- Increased **Web** CIM data model compatibility

Fixed issues

Version 2.0.0 of the Splunk Add-on for Apache Web Server contains no fixed issues.

Known issues

Version 2.0.0 of the Splunk Add-on for Apache Web Server contains no known issues.

Third-party software attributions

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

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Apache was released on June 7, 2016. This release is compatible with the following software, CIM versions, and platforms.

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	Apache httpd 2.2.x, Apache 2.4.x and later

New features

Version 1.0.0 of the Splunk Add-on for Apache Web Server provides inputs and CIM normalization for Apache Web Server data.

Known issues

Version 1.0.0 of the Splunk Add-on for Apache Web Server contains no known issues.

Third-party software attributions

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