Apache: Web Server

There are two types of Apache web server logs:

- Access. Information about requests coming in to the web server, including what pages people are viewing, the success status of requests, and how long the server took to respond.
- Error. Information about errors the web server encountered when processing requests, as well as diagnostic information about the server itself.

In the Common Information Model, Apache Web Server data can be mapped to Web data model in Splunk’s Common Information Model.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud Platform). Refer to the documentation, and note the following:

- Source types:
  - apache:access
  - apache:error
  - apache:access:kv
  - apache:access:json
- Add-on or app: Splunk Add-on for Apache Web Server

Application

When your Splunk deployment is ingesting Apache web server data, you can use the data to achieve the following use cases:

- Managing web server performance
- Detecting web fraud
- Identifying web users by country