Splunk® Enterprise Knowledge Manager Manual 9.0.4

What is Splunk knowledge?

Generated: 2/14/2023 7:29 pm

What is Splunk knowledge?

Splunk software provides a powerful search and analysis engine that helps you to see both the details and the larger patterns in your IT data. When you use Splunk software you do more than look at individual entries in your log files; you leverage the information they hold collectively to find out more about your IT environment.

Splunk software extracts different kinds of knowledge from your IT data (events, fields, timestamps, and so on) to help you harness that information in a better, smarter, more focused way. Some of this information is extracted at index time, as Splunk software indexes your IT data. But the bulk of this information is created at "search time," both by Splunk software and its users. Unlike databases or schema-based analytical tools that decide what information to pull out or analyze beforehand, Splunk software enables you to dynamically extract knowledge from raw data as you need it.

As your organization uses Splunk software, additional categories of Splunk software knowledge objects are created, including event types, tags, lookups, field extractions, workflow actions, and saved searches.

You can think of Splunk software knowledge as a multitool that you use to discover and analyze various aspects of your IT data. For example, event types enable you to quickly and easily classify and group together similar events; you can then use them to perform analytical searches on precisely-defined subgroups of events.

The *Knowledge Manager* manual shows you how to maintain sets of knowledge objects for your organization through Splunk Web and configuration files, and it demonstrates ways that you can use Splunk knowledge to solve your organization's real-world problems.

Splunk software knowledge is grouped into five categories:

- **Data interpretation: Fields and field extractions** - Fields and field extractions make up the first order of Splunk software knowledge. The fields that Splunk software automatically extracts from your IT data help bring meaning to your raw data, clarifying what can at first glance seem incomprehensible. The fields that you extract manually expand and improve upon this layer of meaning.
- **Data classification: Event types and transactions** - You use event types and transactions to group together interesting sets of similar events. Event types group together sets of events discovered through searches, while transactions are collections of conceptually-related events that span time.
- **Data enrichment: Lookups and workflow actions** - Lookups and workflow actions are categories of knowledge objects that extend the usefulness of your data in various ways. Field lookups enable you to add fields to your data from external data sources such as static tables (CSV files) or Python-based commands. Workflow actions enable interactions between fields in your data and other applications or web resources, such as a WHOIS lookup on a field containing an IP address.
- **Data normalization: Tags and aliases** - Tags and aliases are used to manage and normalize sets of field information. You can use tags and aliases to group sets of related field values together, and to give extracted fields tags that reflect different aspects of their identity. For example, you can group events from set of hosts in a particular location (such as a building or city) together--just give each host the same tag. Or maybe you have two different sources using different field names to refer to same data--you can normalize your data by using aliases (by aliasing `clientip` to `ipaddress`, for example).
- **Data models** - Data models are representations of one or more datasets, and they drive the Pivot tool, enabling Pivot users to quickly generate useful tables, complex visualizations, and robust reports without needing to interact with the Splunk software search language. Data models are designed by knowledge managers who fully understand the format and semantics of their indexed data. A typical data model makes use of other knowledge object types discussed in this manual, including lookups, transactions, search-time field extractions, and calculated fields.

The *Knowledge Manager* manual includes information about the following topic:

- **Summary-based report and data model acceleration** - When searches and pivots are slow to complete use Splunk software to speed things up. This chapter discusses report acceleration (for searches), data model acceleration (for pivots) and summary indexing (for special case searches).

For information on why you should manage Splunk knowledge, see Why manage Splunk knowledge?.

Knowledge managers should have a basic understanding of data input setup, event processing, and indexing concepts. For more information, see Prerequisites for knowledge management.