Splunk® Enterprise Search Manual 7.2.5

About the search language

Generated: 11/27/2019 7:28 pm

About the search language

The Splunk **Search Processing Language** (SPL) encompasses all the search commands and their functions, arguments and clauses. Search commands tell Splunk software what to do to the events you retrieved from the indexes. For example, you need to use a command to filter unwanted information, extract more information, evaluate new fields, calculate statistics, reorder your results, or create a chart.

Some search commands have functions and arguments associated with them. Use these functions and their arguments to specify how the commands act on your results and which fields they act on. For example, you can use functions to format the data in a chart, describe what kind of statistics to calculate, and specify what fields to evaluate. Some commands also use clauses to specify how to group your search results.

To get familiar with SPL, read these topics in this manual:

- Types of searches
- Types of commands
- Using Splunk Search

For more details on SPL syntax, see Understanding SPL syntax, in the *Search Reference*.

For information about functions, see

- Evaluation functions in the *Search Reference*
- Statistical and charting functions in the *Search Reference*