Splunk® Light References 6.6.3

Generated: 9/13/2017 2:25 pm

Table of Contents

Search Reference

List of search commands

The search commands that make up the Splunk Light search processing language are a subset of the Splunk Enterprise search commands. The table below lists all of the commands that make up the Splunk Light search processing language sorted alphabetically

This topic links to the Splunk Enterprise Search Reference for each search command.

Command	Description	See also
`abstract`	Produces a summary of each search result.	`highlight`
`accum`	Keeps a running total of the specified numeric field.	`autoregress`, `delta`, `trendline`, `streamstats`
`addcoltotals`	Computes an event that contains sum of all numeric fields for previous events.	`addtotals`, `stats`
`addinfo`	Add fields that contain common information about the current search.	`search`
`addtotals`	Computes the sum of all numeric fields for each result.	`addcoltotals`, `stats`
`analyzefields`	Analyze numerical fields for their ability to predict another discrete field.	`anomalousvalue`
`anomalies`	Computes an "unexpectedness" score for an event.	`anomalousvalue`, `cluster`, `kmeans`, `outlier`
`anomalousvalue`	Finds and summarizes irregular, or uncommon, search results.	`analyzefields`, `anomalies`, `cluster`, `kmeans`, `outlier`
`append`	Appends subsearch results to current results.	`appendcols`, `appendcsv`, `join`, `set`
`appendcols`		

	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.	append, appendcsv, join, set
appendpipe	Appends the result of the subpipeline applied to the current result set to results.	append, appendcols, join, set
arules	Finds association rules between field values.	associate, correlate
associate	Identifies correlations between fields.	correlate, contingency
audit	Returns audit trail information that is stored in the local audit index.	
autoregress	Sets up data for calculating the moving average.	accum, autoregress, delta, trendline, streamstats
bin, discretize	Puts continuous numerical values into discrete sets.	chart, timechart
bucketdir	Replaces a field value with higher-level grouping, such as replacing filenames with directories.	cluster, dedup
chart	Returns results in a tabular output for charting. See Functions for stats, chart, and timechart in the Splunk Enterprise *Search Reference*.	timechart
cluster	Clusters similar events together.	anomalies, anomalousvalue, cluster, kmeans, outlier
concurrency	Uses a duration field to find the number of "concurrent" events for each event.	timechart
contingency, counttable, ctable	Builds a contingency table for two fields.	associate, correlate
convert	Converts field values into numerical values.	eval

correlate	Calculates the correlation between different fields.	associate, contingency
crawl	Crawls the filesystem for new sources to index.	
dbinspect	Returns information about the specified index.	
dedup	Removes subsequent results that match a specified criteria.	uniq
delta	Computes the difference in field value between nearby results.	accum, autoregress, trendline, streamstats
diff	Returns the difference between two search results.	
erex	Allows you to specify example or counter example values to automatically extract fields that have similar values.	extract, kvform, multikv, regex, rex, xmlkv
eval	Calculates an expression and puts the value into a field. See Functions for eval and where in the Splunk Enterprise *Search Reference.*	where
eventcount	Returns the number of events in an index.	dbinspect
eventstats	Adds summary statistics to all search results.	stats
extract, kv	Extracts field-value pairs from search results.	kvform, multikv, xmlkv, rex
fieldformat	Expresses how to render a field at output time without changing the underlying value.	eval, where
fields	Removes fields from search results.	
fieldsummary	Generates summary information for all or a subset of the fields.	af, anomalies, anomalousvalue, stats
filldown	Replaces NULL values with the last non-NULL value.	fillnull

fillnull	Replaces null values with a specified value.	
findtypes	Generates a list of suggested event types.	typer
foreach	Run a templatized streaming subsearch for each field in a wildcarded field list.	eval
format	Takes the results of a subsearch and formats them into a single result.	
gauge	Transforms results into a format suitable for display by the Gauge chart types.	
gentimes	Generates time-range results.	
geostats	Generate statistics which are clustered into geographical bins to be rendered on a world map.	stats, xyseries
head	Returns the first number n of specified results.	reverse, tail
highlight	Causes Splunk Web to highlight specified terms.	
history	Returns a history of searches formatted as an events list or as a table.	search
input	Adds sources to Splunk or disables sources from being processed by Splunk.	
inputcsv	Loads search results from the specified CSV file.	loadjob, outputcsv
iplocation	Extracts location information from IP addresses.	
join	SQL-like joining of results from the main results pipeline with the results from the subpipeline.	selfjoin, appendcols
kmeans	Performs k-means clustering on selected fields.	anomalies, anomalousvalue, cluster, outlier

kvform	Extracts values from search results, using a form template.	extract, kvform, multikv, xmlkv, rex
loadjob	Loads events or results of a previously completed search job.	inputcsv
localize	Returns a list of the time ranges in which the search results were found.	map, transaction
makecontinuous	Makes a field that is supposed to be the x-axis continuous (invoked by chart/timechart)	chart, timechart
makemv	Change a specified field into a multivalued field during a search.	mvcombine, mvexpand, nomv
map	A looping operator, performs a search over each search result.	
metadata	Returns a list of source, sourcetypes, or hosts from a specified index or distributed search peer.	dbinspect
metasearch	Retrieves event metadata from indexes based on terms in the logical expression.	metadata, search
multikv	Extracts field-values from table-formatted events.	
multisearch	Run multiple **streaming searches** at the same time.	append, join
mvcombine	Combines events in search results that have a single differing field value into one result with a multivalue field of the differing field.	mvexpand, makemv, nomv
mvexpand	Expands the values of a multivalue field into separate events for each value of the multivalue field.	mvcombine, makemv, nomv
nomv	Changes a specified multivalued field into a single-value field at search time.	makemv, mvcombine, mvexpand
outlier	Removes outlying numerical values.	anomalies, anomalousvalue, cluster, kmeans

outputcsv	Outputs search results to a specified CSV file.	inputcsv, outputtext
outputtext	Ouputs the raw text field (_raw) of results into the _xml field.	outputtext
predict	Enables you to use time series algorithms to predict future values of fields.	x11
rangemap	Sets RANGE field to the name of the ranges that match.	
rare	Displays the least common values of a field.	stats, top
regex	Removes results that do not match the specified regular expression.	rex, search
relevancy	Calculates how well the event matches the query.	
reltime	Converts the difference between 'now' and '_time' to a human-readable value and adds adds this value to the field, 'reltime', in your search results.	convert
rename	Renames a specified field; wildcards can be used to specify multiple fields.	
replace	Replaces values of specified fields with a specified new value.	
rest	Access a REST endpoint and display the returned entities as search results.	
return	Specify the values to return from a subsearch.	format, search
reverse	Reverses the order of the results.	head, sort, tail
rex	Specify a Perl regular expression named groups to extract fields while you search.	extract, kvform, multikv, xmlkv, regex
rtorder	Buffers events from real-time search to emit them in ascending time order when possible.	

savedsearch	Returns the search results of a saved search.	
script, run	Runs an external Perl or Python script as part of your search.	
scrub	Anonymizes the search results.	
search	Searches Splunk indexes for matching events.	
searchtxn	Finds transaction events within specified search constraints.	transaction
selfjoin	Joins results with itself.	join
sendemail	Emails search results to a specified email address.	
set	Performs set operations (union, diff, intersect) on subsearches.	append, appendcols, join, diff
setfields	Sets the field values for all results to a common value.	eval, fillnull, rename
sort	Sorts search results by the specified fields.	reverse
spath	Provides a straightforward means for extracting fields from structured data formats, XML and JSON.	xpath
stats	Provides statistics, grouped optionally by fields. See Functions for stats, chart, and timechart in the Splunk Enterprise *Search Reference*.	eventstats, top, rare
strcat	Concatenates string values.	
streamstats	Adds summary statistics to all search results in a streaming manner.	eventstats, stats
table	Creates a table using the specified fields.	fields
tags	Annotates specified fields in your search results with tags.	eval
tail	Returns the last number n of specified results.	head, reverse

`timechart`	Create a time series chart and corresponding table of statistics. See Functions for stats, chart, and timechart in the Splunk Enterprise *Search Reference*.	`chart, bucket`
`top`	Displays the most common values of a field.	`rare, stats`
`transaction`	Groups search results into transactions.	
`transpose`	Reformats rows of search results as columns.	
`trendline`	Computes moving averages of fields.	`timechart`
`typeahead`	Returns typeahead information on a specified prefix.	
`typer`	Calculates the eventtypes for the search results.	`typelearner`
`uniq`	Removes any search that is an exact duplicate with a previous result.	`dedup`
`untable`	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.	
`where`	Performs arbitrary filtering on your data. See Functions for eval and where in the Splunk Enterprise *Search Reference*.	`eval`
`x11`	Enables you to determine the trend in your data by removing the seasonal pattern.	`predict`
`xmlkv`	Extracts XML key-value pairs.	`extract, kvform, multikv, rex`
`xmlunescape`	Unescapes XML.	
`xpath`	Redefines the XML path.	
`xyseries`	Converts results into a format suitable for graphing.	

Search commands by category

The search commands that make up the Splunk Light search processing language are a subset of the Splunk Enterprise search commands. The tables below list the commands that make up the Splunk Light search processing language and is categorized by their usage. Some commands fit into more than one category based on the options that you specify.

This topic links to the Splunk Enterprise Search Reference for each search command.

Correlation

These commands can be used to build correlation searches.

Command	Description
`append`	Appends subsearch results to current results.
`appendcols`	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.
`appendpipe`	Appends the result of the subpipeline applied to the current result set to results.
`arules`	Finds association rules between field values.
`associate`	Identifies correlations between fields.
`contingency`, `counttable`, `ctable`	Builds a contingency table for two fields.
`correlate`	Calculates the correlation between different fields.
`diff`	Returns the difference between two search results.
`join`	SQL-like joining of results from the main results pipeline with the results from the subpipeline.
`selfjoin`	Joins results with itself.
`set`	Performs set operations (union, diff, intersect) on subsearches.
`stats`	Provides statistics, grouped optionally by fields. See Functions for stats, chart, and timechart in the Splunk Enterprise *Search Reference*.
`transaction`	Groups search results into transactions.

Data and indexes

These commands can be used to learn more about your data and manager your data sources.

View data

These commands return information about the data you have in your indexes. They do not modify your data or indexes in any way.

Command	Description
`audit`	Returns audit trail information that is stored in the local audit index.
`dbinspect`	Returns information about the specified index.
`eventcount`	Returns the number of events in an index.
`metadata`	Returns a list of source, sourcetypes, or hosts from a specified index or distributed search peer.
`typeahead`	Returns typeahead information on a specified prefix.

Manage data

These are some commands you can use to add data sources to or delete specific data from your indexes.

Command	Description
`crawl`	Crawls the filesystem for new sources to add to an index.
`delete`	Delete specific events or search results.
`input`	Adds sources to Splunk or disables sources from being processed by Splunk.

Fields

These are commands you can use to add, extract, and modify fields or field values. The most useful command for manipulating fields is `eval` and its functions.

Add fields

Use these commands to add new fields.

Command	Description
`accum`	Keeps a running total of the specified numeric field.
`addinfo`	Add fields that contain common information about the current search.
`addtotals`	Computes the sum of all numeric fields for each result.
`delta`	Computes the difference in field value between nearby results.
`eval`	Calculates an expression and puts the value into a field. See Functions for eval and where in the Splunk Enterprise *Search Reference*.
`iplocation`	Adds location information, such as city, country, latitude, longitude, and so on, based on IP addresses.
`multikv`	Extracts field-values from table-formatted events.
`rangemap`	Sets RANGE field to the name of the ranges that match.
`relevancy`	Adds a relevancy field, which indicates how well the event matches the query.
`strcat`	Concatenates string values and saves the result to a specified field.

Extract fields

These commands provide different ways to extract new fields from search results.

Command	Description
`erex`	Allows you to specify example or counter example values to automatically extract fields that have similar values.
`extract, kv`	Extracts field-value pairs from search results.
`kvform`	Extracts values from search results, using a form template.
`rex`	Specify a Perl regular expression named groups to extract fields while you search.
`spath`	Provides a straightforward means for extracting fields from structured data formats, XML and JSON.
`xmlkv`	Extracts XML key-value pairs.

Modify fields and field values

Use these commands to modify fields or their values.

Command	Description
`convert`	Converts field values into numerical values.
`filldown`	Replaces NULL values with the last non-NULL value.
`fillnull`	Replaces null values with a specified value.
`makemv`	Change a specified field into a multivalued field during a search.
`nomv`	Changes a specified multivalued field into a single-value field at search time.
`reltime`	Converts the difference between 'now' and '_time' to a human-readable value and adds adds this value to the field, 'reltime', in your search results.
`rename`	Renames a specified field; wildcards can be used to specify multiple fields.
`replace`	Replaces values of specified fields with a specified new value.

Find anomalies

These commands are used to find anomalies in your data. Either search for uncommon or outlying events and fields or cluster similar events together.

Command	Description
`analyzefields, af`	Analyze numerical fields for their ability to predict another discrete field.
`anomalies`	Computes an "unexpectedness" score for an event.
`anomalousvalue`	Finds and summarizes irregular, or uncommon, search results.
`cluster`	Clusters similar events together.
`kmeans`	Performs k-means clustering on selected fields.
`outlier`	Removes outlying numerical values.
`rare`	Displays the least common values of a field.

Geoip and location

These commands add geographical information to your search results.

Command	Description
`iplocation`	Returns location information, such as city, country, latitude, longitude, and so on, based on IP addresses.
`geostats`	Generate statistics which are clustered into geographical bins to be rendered on a world map.

Prediction and trending

These commands predict future values and calculate trendlines that can be used to create visualizations.

Command	Description
`predict`	Enables you to use time series algorithms to predict future values of fields.
`trendline`	Computes moving averages of fields.
`x11`	Enables you to determine the trend in your data by removing the seasonal pattern.

Reports

These commands are used to build **transforming searches**. These commands return statistical data tables required for charts and other kinds of data visualizations.

Command	Description
`addtotals`	Computes the sum of all numeric fields for each result.
`bin, discretize`	Puts continuous numerical values into discrete sets.
`chart`	Returns results in a tabular output for charting. See Statistical and charting functions in the Splunk Enterprise *Search Reference*.
`contingency, counttable, ctable`	Builds a contingency table for two fields.
`correlate`	Calculates the correlation between different fields.
`eventcount`	Returns the number of events in an index.

`eventstats`	Adds summary statistics to all search results.
`gauge`	Transforms results into a format suitable for display by the Gauge chart types.
`makecontinuous`	Makes a field that is supposed to be the x-axis continuous (invoked by chart/timechart)
`outlier`	Removes outlying numerical values.
`rare`	Displays the least common values of a field.
`stats`	Provides statistics, grouped optionally by fields. See Statistical and charting functions in the Splunk Enterprise *Search Reference*.
`streamstats`	Adds summary statistics to all search results in a streaming manner.
`timechart`	Create a time series chart and corresponding table of statistics. See Statistical and charting functions in the Splunk Enterprise *Search Reference*.
`top`	Displays the most common values of a field.
`trendline`	Computes moving averages of fields.
`untable`	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.
`xyseries`	Converts results into a format suitable for graphing.

Results

These commands can be used to manage search results. For example, you can append one set of results with another, filter more events from the results, reformat the results, and so on.

Alerting

Use this command to email the results of a search.

Command	Description
`sendemail`	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Append

Use these commands to append one set of results with another set or to itself.

Command	Description
`append`	Appends subsearch results to current results.
`appendcols`	Appends the fields of the subsearch results to current results, first results to first result, second to second, and so on.
`join`	SQL-like joining of results from the main results pipeline with the results from the subpipeline.
`selfjoin`	Joins results with itself.

Filter

Use these commands to remove more events or fields from your current results.

Command	Description
`dedup`	Removes subsequent results that match a specified criteria.
`fields`	Removes fields from search results.
`mvcombine`	Combines events in search results that have a single differing field value into one result with a multivalue field of the differing field.
`regex`	Removes results that do not match the specified regular expression.
`searchtxn`	Finds transaction events within specified search constraints.
`table`	Creates a table using the specified fields.
`uniq`	Removes any search that is an exact duplicate with a previous result.
`where`	Performs arbitrary filtering on your data. See Evaluation functions in the Splunk Enterprise *Search Reference*.

Format

Use these commands to reformat your current results.

Command	Description
`untable`	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.

xyseries	Converts results into a format suitable for graphing.

Generate

Use these commands to generate or return events.

Command	Description
gentimes	Returns results that match a time-range.
loadjob	Loads events or results of a previously completed search job.
mvexpand	Expands the values of a multivalue field into separate events for each value of the multivalue field.
savedsearch	Returns the search results of a saved search.
search	Searches Splunk indexes for matching events. This command is implicit at the start of every search pipeline that does not begin with another generating command.

Group

Use these commands to group or classify the current results.

Command	Description
cluster	Clusters similar events together.
kmeans	Performs k-means clustering on selected fields.
mvexpand	Expands the values of a multivalue field into separate events for each value of the multivalue field.
transaction	Groups search results into transactions.
typer	Calculates the eventtypes for the search results.

Reorder

Use these commands to change the order of the current search results.

Command	Description
head	Returns the first number n of specified results.
reverse	Reverses the order of the results.
sort	Sorts search results by the specified fields.
tail	Returns the last number N of specified results

Read

Use these commands to read in results from external files or previous searches.

Command	Description
`inputcsv`	Loads search results from the specified CSV file.
`loadjob`	Loads events or results of a previously completed search job.

Write

Use these commands to define how to output current search results.

Command	Description
`outputcsv`	Outputs search results to a specified CSV file.
`outputtext`	Ouputs the raw text field (`_raw`) of results into the `_xml` field.
`sendemail`	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Search

Command	Description
`map`	A looping operator, performs a search over each search result.
`search`	Searches Splunk indexes for matching events. This command is implicit at the start of every search pipeline that does not begin with another generating command.
`sendemail`	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Subsearch

These are commands that you can use with **subsearches**.

Command	Description
`append`	Appends subsearch results to current results.
`appendcols`	Appends the fields of the subsearch results to current results, first results to first result, second to second, and so on.

`appendpipe`	Appends the result of the subpipeline applied to the current result set to results.
`format`	Takes the results of a subsearch and formats them into a single result.
`join`	SQL-like joining of results from the main results pipeline with the results from the subpipeline.
`return`	Specify the values to return from a subsearch.
`set`	Performs set operations (union, diff, intersect) on subsearches.

Time

Use these commands to search based on time ranges or add time information to your events.

Command	Description
`gentimes`	Returns results that match a time-range.
`localize`	Returns a list of the time ranges in which the search results were found.
`reltime`	Converts the difference between 'now' and '_time' to a human-readable value and adds adds this value to the field, 'reltime', in your search results.

Visualization Reference

About data visualizations

Splunk Light provides a number of options for search result visualization. You can see event data presented as event listings, tables, and charts (such as column, line, area, and pie charts.) You can choose from a variety of gauge and single value displays for searches that return a single, discrete, numerical value. You can also plot geographic coordinates as interactive markers on a world map.

This topic discusses how you can access the visualization features and briefly describes the visualization options.

Accessing visualization features

Splunk Light provides tools to modify and create visualizations in the Search and Dashboard pages.

Visualizations from Search

You can modify how search results display in the **Search** page. The search must be a reporting search that returns results that can be formatted as a visualization.

After running a search, select the **Visualization** tab, then select the type of visualization to display. You can specify formatting options for the selected visualization.

Dashboard panel visualizations

When you base a new dashboard panel on search results you can choose the visualization that best represents the data returned by the search. You can then use the Visualization Editor to fine-tune the way the panel visualization displays.

To create a dashboard panel from search results, after you run the search click **Save As > Dashboard Panel**. You can also create the panel directly from the **Dashboard** page.

Visualization options and data structures

The following table lists the different types of visualizations you can choose with

Splunk Light.

Visualization Type	Description
Event visualizations	Event visualizations are essentially raw lists of events.
Tables	You can generate table visualizations from just about any search. Searches that include transform operations, such as `stats`, `chart`, and `timechart`, generate more interesting tables. You can also configure table visualizations to display sparklines.
Charts	Chart visualizations include column, line, area, scatter, and pie charts. These visualizations require transforming searches whose reults involve one or more series. All chart visualizations can display single-series searches. However the bar, column, line, and pie chart visualizations usually display the data best. Pie charts can only display data from single series searches. If a search produces multiple series, bar, column, line, area, and scatter chart visualizations display the data best.
Single-value visualizations	Single-value visualizations display the results of a transforming search that returns a single value. For example, a search that returns the total count of events for a specific set of search criteria.
Gauges	Gauge visualizations map a single numerical value against a range of colors that may have a particular business meaning or logic. Gauges use range maps to define color ranges. You can choose from three types of gauge visualizations: radial, filler, and marker.
Maps	The map visualization lets you plot geographic coordinates as interactive markers on a world map. Searches for map visualizations typically use the geostats search command to plot markers on a map.

The visualization you can choose depends on the data structure your search returns. If you find the visualization you want is unavailable when you try to create a new panel, then perhaps your underlying search does not return the data that works for that visualization.

For example, most chart visualizations require search results that are structured as tables with at least two columns. The first column provides x-axis values. The subsequent columns provide y-axis values for each series represented in the chart.

For more information, see Data visualization library in the *References* manual.

Data visualization library

This topic is a quick reference for the data visualizations available in Splunk Light.

Events

Event visualizations are a list of raw events. You get event visualizations from any search that does not include a transform operation. For example, a search for a set of terms and field values returns a list of events.

```
error OR failed OR severe OR ( sourcetype=access_* ( 404 OR 500 OR 503
) )
```

With event visualizations, you can:

- Determine the number of events listed.
- Determine whether numbers appear to the left of each panel.
- Have event text wrap to fit within the dashboard panel.

If you add a transforming command, such as `stats`, `chart`, `timechart`, or `top`, you get statistical results that you can present either as a table or a chart.

Tables

You can generate table visualizations from just about any search. However, searches that include transform operations such as `stats`, `chart`, and `timechart`, generate more interesting tables.

For table visualizations you can do the following:

- Set the number of table rows to display.
- Display row numbers.
- Add data overlays that provide additional visual information, such as heat maps or high/low value indicators.

Sparklines in tables

You can configure table visualizations to display sparklines. Sparklines show hidden patterns in data that might otherwise be hard to identify in table results. They can increase the usefulness and overall information density of tables in reports and dashboards.

To use sparklines, the underlying search has to use the `stats` or `chart` transforming commands. You add the `sparklines` function to those commands to add a sparkline column to the table.

Charts

You can choose from a variety of chart visualizations, such as column, line, area, scatter, and pie charts. These visualizations require transforming searches whose results involve one or more **series**.

A series is a sequence of related data points that can be plotted on a chart. For example, each line plotted on a line chart represents an individual series. You can design transforming searches that produce a single series, or you can set them up so the results provide data for multiple series.

Consider a table that a transforming search generates. Each column in the table after the first column represents a different series. A "single series" search produces a table with only two columns, while a "multiple series" search produces a table with three or more columns.

All chart visualizations can display single-series searches. However the bar, column, line, and pie chart visualizations usually display the data best. Pie charts can only display data from single series searches.

If a search produces multiple series, bar, column, line, area, and scatter chart visualizations display the data best.

Column and bar charts

Use a column chart or bar chart to compare the frequency of values of fields in your data. In a column chart, the x-axis values are typically field values. If the search uses the timechart transforming command, the x-axis represents time. The y-axis can be any other field value, count of values, or statistical calculation of a field value. Column charts and bar charts represent data similarly, except that the x-axis and y-axis values are reversed.

Line and area charts

Use line and area charts to show data trends over time. You can use the x-axis to represent any field value other than time. If you chart includes more than one series, a different color represents each line or area. Shaded areas in area charts help emphasize quantities.

Stacked charts

When a base searches involves more than one data series, you can use stacked column and stacked bar charts to compare the frequency of field values in your data. Stacked line and area charts are useful when charting several series, making it easier to see how each data series relates to the entire set of data as a whole.

Unstacked charts

In an unstacked column chart, the columns for different series appear alongside each other. An unstacked column chart is useful for relatively simple search results.

Stacked charts

A stacked column chart displays all the series columns for a single data point as segments of a single column. The total value of the column is the sum of the segments. You can use a stacked column or bar chart to highlight the relative weight, or importance, of the different types of data that make up a specific data

set.

100 per cent stacked charts

You can use 100% stacked charts to compare data distributions within a column or bar chart by percentage of the column or bar size. Each segment of data in the column or bar represents the percentage of all the data available.

Stacked 100% is useful to better see data distributions between segments in a column or bar chart that contains a mix of very small and very large segments.

Pie chart

Use a pie chart to show the relationship of parts of your data to the entire set of data as a whole. The size of a slice in a pie graph shows the value of the data represented by the slice as a percentage of the sum of all values.

Scatter chart

Use a scatter chart, also known as scatter plot, to show trends in the relationships between discrete values of data. A scatter plot shows discrete values that do not occur at regular intervals or belong to a series. This differs from a line graph, which plots a regular series of points.

Bubble chart

A bubble chart provides a visual way to view a three dimensional series. Each point, or bubble, plots against two dimensions on the X and Y axes of the chart. The size of the bubble represents the value for the third dimension

Single value visualizations

Single value displays and gauges display the results of a transforming search that returns a single value. For example, a search that returns the total count of events for a specific set of search criteria. There are various ways to make searches return a single values. One example is to combine the top command with head=1.

Single value display

The single value visualization displays the result of a search that returns a single numerical value. If you base the visualization on a real-time search that returns a single value, the number displayed changes as the search interprets incoming

data.

```
index=_internal source="*splunkd.log" log_level="error" | stats count
as errors | rangemap field=errors low=0-3 elevated=4-20 default=severe
```

You can configure a single value display visualization to change color depending on where the returned value falls within a defined range. Use the `rangemap` search command to define the range in the underlying search. You can also configure the range map for a single value visualization with the Panel Editor. By default, a single value visualization uses the following range map configuration:

- low: green
- elevated: yellow
- severe: red

Gauges

Gauge visualizations map a single numerical value against a range of colors that may have particular business meaning or logic. Gauges use range maps, as described in the single value visualization], to define color ranges. As a value changes over time, the gauge marker changes position within this range.

Gauges provide a dynamic visualization for **real-time searches**, where the value returned fluctuates as events are returned, causing the gauge marker to visibly bounce back and forth within the range.

You can choose from three types of gauge visualizations: radial, filler, and marker. The gauge examples below use the same base search:

```
index=_internal source="*splunkd.log" log_level="error" | stats count
as errors
```

Radial gauge

The radial gauge type looks like a speedometer or pressure valve gauge. It has an arced range scale and a rotating needle. Use a range map, as described for a single value visualization, to define color ranges for the radial gauge.

The current value of the needle displays at the bottom of the gauge. In the example below, the value is 17. If the value falls below or above the specified

minimum or maximum range, the needle "flutters" at the upper or lower boundary, as if it is straining to move past the limits of the range.

The following examples shows the "shiny" and "minimal" version of the radial gauge:

Filler gauge

The filler gauge is similar to a thermometer, with a filler indicator that changes color as it rises and passes gauge range boundaries. Use a range map, as described for a single value visualization, to define color ranges for the filler gauge.

The following examples shows the "shiny" and "minimal" version of the filler gauge:

Marker gauge

The marker gauge is a linear version of the filler gauge. A gauge marker rests at the value returned by the search. Use a range map, as described for a single value visualization, to define color ranges for the marker gauge.

If the gauge displays the results of a real-time search, the marker can appear to slide back and forth across the range as the returned value fluctuates over time. If the returned value falls outside of the upper or lower ranges of the marker gauge, the marker appears to vibrate at the upper or lower boundary, as if it is straining to move past the limits of the range.

Marker gauges have display issues with numbers exceeding 3 digits in length. To manage this, you can set up a search that divides a large number by a factor that reduces it to a smaller number. For example, if the value returned is typically in the tens of thousands, set your search so the result is divided by 1000. Then a result of 19,100 becomes 19.1.

You can also deal with large numbers by setting the chart configuration options to return the range as a percentage.

use the gauge command to set the ranges

You can use the `gauge` command to set custom ranges for a gauge visualization.

The `gauge` command lets you set the gauge ranges using default colors. The default three colors, in order of the ranges, are green, yellow, and red. With `gauge`, you indicate the field to track with the gauge. Then add "range values" to the search string to indicate the beginning and end of the range as well as the relative sizes of the color bands within it.

For example, to set up a gauge that tracks a `hitcount` field value with the ranges 100-119, 120-139, 140-159, 160-179, and 180-200, add this to your search string:

```
...| gauge hitcount 100 120 140 160 180 200
```

If you do not include the `gauge` command in your search or include it but fail to specify range values, the range values default to these values: `0 30 70 100`.

Maps

Splunk Enterprise provides a map visualization that lets you plot geographic coordinates as interactive markers on a world map. Searches for map visualizations typically use the `geostats` search command to plot markers on a map. The `geostats` command is similar to the `stats` command, but provides options for zoom levels and cells for mapping. The `geostats` command generates events that include latitude and longitude coordinates for markers.