Splunk® Enterprise
Search Reference 9.0.4

Statistical and charting functions

Generated: 2/15/2023 3:49 am

Statistical and charting functions

You can use the statistical and charting functions with the `chart`, `stats`, and `timechart` commands.

Support for related commands

The functions can also be used with related statistical and charting commands. The following table lists the commands supported by the statistical and charting functions and the related command that can also use these functions.

Command	Supported related commands
`chart`	• `sichart`
`stats`	• `eventstats` • `streamstats` • `geostats` • `sistats` • For the `tstats` and the `mstats` commands, see the documentation for each command for a list of the supported functions.
`timechart`	• `sitimechart`

Functions that you can use to create sparkline charts are noted in the documentation for each function. Sparkline is a function that applies to only the `chart` and `stats` commands, and allows you to call other functions. For more information, see Add sparklines to search results in the *Search Manual*.

How field values are processed

Most of the statistical and charting functions expect the field values to be numbers. All of the values are processed as numbers, and any non-numeric values are ignored.

The following functions process the field values as literal string values, even though the values are numbers.

• `count` • `distinct_count` • `earliest`	• `estdc` • `estdc_error` • `first`	• `latest` • `last` • `list`	• `max` • `min` • `mode` • `values`

For example, you use the `distinct_count` function and the field contains values such as "1", "1.0", and "01". Each value is considered a distinct string value.

The only exceptions are the `max` and `min` functions. These functions process values as numbers if possible. For example, the values "1", "1.0", and "01" are processed as the same numeric value.

Supported functions and syntax

There are two ways that you can see information about the supported statistical and charting functions:

- Function list by category
- Alphabetical list of functions

Function list by category

The following table is a quick reference of the supported statistical and charting functions, organized by category. This table provides a brief description for each functions. Use the links in the table to learn more about each function and to see examples.

Type of function	Supported functions and syntax	Description
Aggregate functions	`avg(X)`	Returns the average of the values in the field X.
	`count(X)`	Returns the number of occurrences where the field that you specify contains any value (is not empty. You can also count the occurrences of a specific value in the field by using the `eval` command with the `count` function. For example: `count eval(field_name="value")`.
	`distinct_count(X)`	Returns the count of distinct values in the field X.
	`estdc(X)`	Returns the estimated count of the distinct values in the field X.
	`estdc_error(X)`	Returns the theoretical error of the estimated count of the distinct values in the field X. The error represents a ratio of the `absolute_value(estimate_distinct_count - real_distinct_count)/real_distinct_count`.
	`max(X)`	Returns the maximum value of the field X. If the values of X are non-numeric, the maximum value is found using lexicographical ordering. This function processes field values as numbers if possible, otherwise processes field values as strings.
	`mean(X)`	Returns the arithmetic mean of the field X.
	`median(X)`	Returns the middle-most value of the field X.
	`min(X)`	Returns the minimum value of the field X. If the values of X are non-numeric, the minimum value is found using lexicographical ordering.
	`mode(X)`	Returns the most frequent value of the field X.
	`percentile<X>(Y)`	Returns the X-th percentile value of the numeric field Y. Valid values of X are integers from 1 to 99. Additional percentile functions are `upperperc<X>(Y)` and `exactperc<X>(Y)`.
	`range(X)`	Returns the difference between the maximum and minimum values of the field X ONLY IF the values of X are numeric.
	`stdev(X)`	Returns the sample standard deviation of the field X.
	`stdevp(X)`	Returns the population standard deviation of the field X.
	`sum(X)`	Returns the sum of the values of the field X.
	`sumsq(X)`	Returns the sum of the squares of the values of the field X.
	`var(X)`	Returns the sample variance of the field X.
	`varp(X)`	Returns the population variance of the field X.
Event order functions	`first(X)`	Returns the first seen value of the field X. In general, the first seen value of the field is the most recent instance of this field, relative to the input order of events into the stats command.
	`last(X)`	Returns the last seen value of the field X. In general, the last seen value of the field is the oldest instance of this field relative to the input order of events into the stats command.

Type of function	Supported functions and syntax	Description
Multivalue stats and chart functions	`list(X)`	Returns a list of up to 100 values of the field X as a multivalue entry. The order of the values reflects the order of input events.
	`values(X)`	Returns the list of all distinct values of the field X as a multivalue entry. The order of the values is lexicographical.
Time functions	`earliest(X)`	Returns the chronologically earliest (oldest) seen occurrence of a value of a field X.
	`earliest_time(X)`	Returns the UNIX time of the earliest (oldest) occurrence of a value of the field. Used in conjunction with `earliest(x)`, `latest(x)`, and `latest_time(x)` to calculate the rate of increase for an accumulating counter.
	`latest(X)`	Returns the chronologically latest (most recent) seen occurrence of a value of a field X.
	`latest_time(X)`	Returns the UNIX time of the latest (most recent) occurrence of a value of the field. Used in conjunction with `earliest(x)`, `earliest_time(x)`, and `latest(x)` to calculate the rate of increase for an accumulating counter.
	`per_day(X)`	Returns the values of field X, or eval expression X, for each day.
	`per_hour(X)`	Returns the values of field X, or eval expression X, for each hour.
	`per_minute(X)`	Returns the values of field X, or eval expression X, for each minute.
	`per_second(X)`	Returns the values of field X, or eval expression X, for each second.
	`rate(X)`	Returns the per-second rate change of the value of the field. Represents `(latest(X) - earliest(X)) / (latest_time(X) - earliest_time(X))` Requires the `earliest(X)` and `latest(X)` values of the field to be numerical, and the `earliest_time(X)` and `latest_time(X)` values to be different.
	`rate_avg(X)`	Returns the average rates for the time series associated with a specified accumulating counter metric.
	`rate_sum(X)`	Returns the summed rates for the time series associated with a specified accumulating counter metric.

Alphabetical list of functions

The following table is a quick reference of the supported statistical and charting functions, organized alphabetically. This table provides a brief description for each function. Use the links in the table to learn more about each function and to see examples.

Supported functions and syntax	Description	Type of function
`avg(X)`	Returns the average of the values in the field X.	Aggregate functions
`count(X)`	Returns the number of occurrences where the field that you specify contains any value (is not empty. You can also count the occurrences of a specific value in the field by using the `eval` command with the `count` function. For example: `count eval(field_name="value")`.	Aggregate functions
`distinct_count(X)`	Returns the count of distinct values in the field X.	Aggregate functions
`earliest(X)`	Returns the chronologically earliest (oldest) seen occurrence of a value of a field X.	Time functions
`earliest_time(X)`		Time functions

Supported functions and syntax	Description	Type of function
	Returns the UNIX time of the earliest (oldest) occurrence of a value of the field. Used in conjunction with `earliest(x)`, `latest(x)`, and `latest_time(x)` to calculate the rate of increase for an accumulating counter.	
`estdc(X)`	Returns the estimated count of the distinct values in the field X.	Aggregate functions
`estdc_error(X)`	Returns the theoretical error of the estimated count of the distinct values in the field X. The error represents a ratio of the `absolute_value(estimate_distinct_count - real_distinct_count)/real_distinct_count`.	Aggregate functions
`first(X)`	Returns the first seen value of the field X. In general, the first seen value of the field is the most recent instance of this field, relative to the input order of events into the stats command.	Event order functions
`last(X)`	Returns the last seen value of the field X. In general, the last seen value of the field is the oldest instance of this field relative to the input order of events into the stats command.	Event order functions
`latest(X)`	Returns the chronologically latest (most recent) seen occurrence of a value of a field X.	Time functions
`latest_time(X)`	Returns the UNIX time of the latest (most recent) occurrence of a value of the field. Used in conjunction with `earliest(x)`, `earliest_time(x)`, and `latest(x)` to calculate the rate of increase for an accumulating counter.	Time functions
`list(X)`	Returns a list of up to 100 values of the field X as a multivalue entry. The order of the values reflects the order of input events.	Multivalue stats and chart functions
`max(X)`	Returns the maximum value of the field X. If the values of X are non-numeric, the maximum value is found using lexicographical ordering. This function processes field values as numbers if possible, otherwise processes field values as strings.	Aggregate functions
`mean(X)`	Returns the arithmetic mean of the field X.	Aggregate functions
`median(X)`	Returns the middle-most value of the field X.	Aggregate functions
`min(X)`	Returns the minimum value of the field X. If the values of X are non-numeric, the minimum value is found using lexicographical ordering.	Aggregate functions
`mode(X)`	Returns the most frequent value of the field X.	Aggregate functions
`percentile<X>(Y)`	Returns the X-th percentile value of the numeric field Y. Valid values of X are integers from 1 to 99. Additional percentile functions are `upperperc<X>(Y)` and `exactperc<X>(Y)`.	Aggregate functions
`per_day(X)`	Returns the values of field X, or eval expression X, for each day.	Time functions
`per_hour(X)`	Returns the values of field X, or eval expression X, for each hour.	Time functions
`per_minute(X)`	Returns the values of field X, or eval expression X, for each minute.	Time functions
`per_second(X)`	Returns the values of field X, or eval expression X, for each second.	Time functions
`range(X)`	Returns the difference between the maximum and minimum values of the field X ONLY IF the values of X are numeric.	Aggregate functions
`rate(X)`		Time functions

Supported functions and syntax	Description	Type of function
	Returns the per-second rate change of the value of the field. Represents `(latest(X) - earliest(X)) / (latest_time(X) - earliest_time(X))` Requires the `earliest(X)` and `latest(X)` values of the field to be numerical, and the `earliest_time(X)` and `latest_time(X)` values to be different.	
`rate_avg(X)`	Returns the average rates for the time series associated with a specified accumulating counter metric.	Time functions
`rate_sum(X)`	Returns the summed rates for the time series associated with a specified accumulating counter metric.	Time functions
`stdev(X)`	Returns the sample standard deviation of the field X.	Aggregate functions
`stdevp(X)`	Returns the population standard deviation of the field X.	Aggregate functions
`sum(X)`	Returns the sum of the values of the field X.	Aggregate functions
`sumsq(X)`	Returns the sum of the squares of the values of the field X.	Aggregate functions
`values(X)`	Returns the list of all distinct values of the field X as a multivalue entry. The order of the values is lexicographical.	Multivalue stats and chart functions
`var(X)`	Returns the sample variance of the field X.	Aggregate functions
`varp(X)`	Returns the population variance of the field X.	Aggregate functions

See also

Commands

- chart
- geostats
- eventstats
- stats
- streamstats
- timechart

Functions

- Evaluation functions

Answers

Have questions? Visit Splunk Answers and search for a specific function or command.