Statistical and charting functions

The statistical and charting functions with the **chart, stats**, and **timechart** commands.

Command	Supported related commands
chart	sichart
stats	eventstats
	streamstats
	geostats
	sistats
	tstats and mstats
timechart	sitimechart

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

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

Aggregate functions

avg function

Description: Calculates the average of a numeric field.
Syntax: avg(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval avg_value = avg(split(values, ","))
| table values, avg_value
```

Output:

```
| values     | avg_value       |
|------------|-----------------|
| 1,2,3,4,5  | 3               |
```

count function

Description: Counts the number of events or values.
Syntax: count(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval count_value = count(split(values, ","))
| table values, count_value
```

Output:

```
| values     | count_value     |
|------------|-----------------|
```

| 1,2,3,4,5 | 5 |

distinct_count function

Description: Counts the number of unique values in a field.
Syntax: distinct_count(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5,5,5"
| eval distinct_count_value = distinct_count(split(values, ","))
| table values, distinct_count_value
```
Output:
```
| values       | distinct_count_value |
|--------------|----------------------|
| 1,2,3,4,5,5, | 5                    |
```

estdc function

Description: Estimates the distinct count of values in a field.
Syntax: estdc(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5,5,5"
| eval estimated_distinct_count = estdc(split(values, ","))
| table values, estimated_distinct_count
```
Output:
```
| values       | estimated_distinct_count |
|--------------|--------------------------|
| 1,2,3,4,5,5,5 | 5                      |
```

estdc_error function

Description: Calculates the error rate of the estimated distinct count.
Syntax: estdc_error(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5,5,5"
| eval estimated_distinct_count = estdc(split(values, ","))
| eval error_rate = estdc_error(split(values, ","))
| table values, estimated_distinct_count, error_rate
```
Output:
```
| values       | estimated_distinct_count | error_rate |
|--------------|--------------------------|------------|
| 1,2,3,4,5,5,5 | 5                      | 0          |
```

exactperc function

Description: Calculates the exact percentile of a field.
Syntax: exactperc(<field>, <percentile>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval percentile_80 = exactperc(split(values, ","), 80)
| table values, percentile_80
```

Output:

```
| values      | percentile_80    |
|-------------|------------------|
| 1,2,3,4,5   | 4                |
```

max function

Description: Finds the maximum value of a field.
Syntax: max(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval max_value = max(split(values, ","))
| table values, max_value
```

Output:

```
| values      | max_value        |
|-------------|------------------|
| 1,2,3,4,5   | 5                |
```

mean function

Description: Calculates the arithmetic mean of a field.
Syntax: mean(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval mean_value = mean(split(values, ","))
| table values, mean_value
```

Output:

```
| values      | mean_value       |
|-------------|------------------|
| 1,2,3,4,5   | 3                |
```

median function

Description: Calculates the median of a field.
Syntax: median(<field>)

Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval median_value = median(split(values, ","))
| table values, median_value
```

Output:

```
| values      | median_value     |
|-------------|------------------|
| 1,2,3,4,5   | 3                |
```

min function

Description: Finds the minimum value of a field.
Syntax: min(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval min_value = min(split(values, ","))
| table values, min_value
```

Output:

```
| values      | min_value        |
|-------------|------------------|
| 1,2,3,4,5   | 1                |
```

mode function

Description: Finds the mode value(s) of a field.
Syntax: mode(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,2,3,3,3"
| eval mode_value = mode(split(values, ","))
| table values, mode_value
```

Output:

```
| values       | mode_value       |
|--------------|------------------|
| 1,2,2,3,3,3  | 3                |
```

percentile function

Description: Calculates the specified percentile of a field.
Syntax: percentile(<field>, <percentile>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval percentile_75 = percentile(split(values, ","), 75)
```

```
| table values, percentile_75
```
Output:
```
| values      | percentile_75    |
|-------------|------------------|
| 1,2,3,4,5   | 4                |
```

range function

Description: Calculates the range of values in a field.
Syntax: range(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval range_value = range(split(values, ","))
| table values, range_value
```
Output:
```
| values      | range_value      |
|-------------|------------------|
| 1,2,3,4,5   | 4                |
```

stdev function

Description: Calculates the sample standard deviation of a field.
Syntax: stdev(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval stdev_value = stdev(split(values, ","))
| table values, stdev_value
```
Output:
```
| values      | stdev_value      |
|-------------|------------------|
| 1,2,3,4,5   | 1.5811388301     |
```

stdevp function

Description: Calculates the population standard deviation of a field.
Syntax: stdevp(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval stdevp_value = stdevp(split(values, ","))
| table values, stdevp_value
```
Output:
```
| values      | stdevp_value     |
|-------------|------------------|
```

| 1,2,3,4,5 | 1.4142135624 |

sum function

Description: Calculates the sum of values in a field.
Syntax: sum(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval sum_value = sum(split(values, ","))
| table values, sum_value
```
Output:
```
| values      | sum_value       |
|-------------|-----------------|
| 1,2,3,4,5   | 15              |
```

sumsq function

Description: Calculates the sum of squares of values in a field.
Syntax: sumsq(<field>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval sumsq_value = sumsq(split(values, ","))
| table values, sumsq_value
```
Output:
```
| values      | sumsq_value      |
|-------------|------------------|
| 1,2,3,4,5   | 55               |
```

upperperc function

Description: Calculates the upper percentile of a field.
Syntax: upperperc(<field>, <percentile>)
Example Usage:
```
| makeresults
| eval values = "1,2,3,4,5"
| eval upper_percentile_90 = upperperc(split(values, ","), 90)
| table values, upper_percentile_90
```
Output:
```
| values      | upper_percentile_90   |
|-------------|-----------------------|
| 1,2,3,4,5   | 5                     |
```

var function

Description: Calculates the sample variance of a field.
Syntax: var(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval var_value = var(split(values, ","))
| table values, var_value
```

Output:

```
| values      | var_value       |
|-------------|-----------------|
| 1,2,3,4,5   | 2.5             |
```

varp function

Description: Calculates the population variance of a field.
Syntax: varp(<field>)
Example Usage:

```
| makeresults
| eval values = "1,2,3,4,5"
| eval varp_value = varp(split(values, ","))
| table values, varp_value
```

Output:

```
| values      | varp_value      |
|-------------|-----------------|
| 1,2,3,4,5   | 2               |
```

Event order functions

first function

Description: Retrieves the first event in the result set based on the specified field and sorting order.
Syntax: <base search> | head <number of events> <sorting field> <sorting order>
Example Usage:

```
<base search>
| head 1 <sorting field> <sorting order>
```

Output:
The first event based on the specified sorting field and order.

last function

Description: Retrieves the last event in the result set based on the specified field and sorting order.
Syntax: <base search> | tail <number of events> <sorting field> <sorting order>
Example Usage:

```
<base search>
| tail 1 <sorting field> <sorting order>
```

Output:
The last event based on the specified sorting field and order.

Multivalue stats and chart functions

list function

Description: Concatenates multivalue field values into a single string, separated by a specified delimiter.
Syntax: <base search> | stats list(<field>) AS <new field> <other aggregations>
Example Usage:
<base search>
| stats list(<field>) AS <new field> <other aggregations>
Output:
A new field that contains the concatenated values of the specified field.

values function

Description: Extracts the unique multivalue field values as individual events.
Syntax: <base search> | mvexpand <field> | stats values(<field>) AS <new field> <other aggregations>
Example Usage:
<base search>
| mvexpand <field>
| stats values(<field>) AS <new field> <other aggregations>
Output:
Individual events where each event represents a unique value of the specified field.

Time functions

earliest function

Description: Returns the earliest timestamp value in the result set.
Syntax: <base search> | earliest(<timestamp field>) AS <new field>
Example Usage:
<base search>
| earliest(<timestamp field>) AS <new field>
Output:
The earliest timestamp value in the result set.

earliest_time function

Description: Returns the earliest timestamp value as a string in the specified time format.
Syntax: <base search> | eval <new field> = earliest_time(<timestamp field>, <time format>)
Example Usage:
<base search>
| eval <new field> = earliest_time(<timestamp field>, <time format>)
Output:
The earliest timestamp value in the specified time format.

latest function

Description: Returns the latest timestamp value in the result set.
Syntax: <base search> | latest(<timestamp field>) AS <new field>
Example Usage:
<base search>
| latest(<timestamp field>) AS <new field>
Output:
The latest timestamp value in the result set.

latest_time function

Description: Returns the latest timestamp value as a string in the specified time format.
Syntax: <base search> | eval <new field> = latest_time(<timestamp field>, <time format>)
Example Usage:
<base search>
| eval <new field> = latest_time(<timestamp field>, <time format>)
Output:
The latest timestamp value in the specified time format.

per_day function

Description: Aggregates events per day.
Syntax: <base search> | bin <timestamp field> span=1d | stats <aggregations>
Example Usage:
<base search>
| bin <timestamp field> span=1d | stats <aggregations>
Output:
Aggregated statistics per day.

per_hour function

Description: Aggregates events per hour.
Syntax: <base search> | bin <timestamp field> span=1h | stats <aggregations>
Example Usage:
<base search>
| bin <timestamp field> span=1h | stats <aggregations>
Output:
Aggregated statistics per hour.

per_minute function

Description: Aggregates events per minute.
Syntax: <base search> | bin <timestamp field> span=1m | stats <aggregations>
Example Usage:
<base search>
| bin <timestamp field> span=1m | stats <aggregations>

Output:
Aggregated statistics per minute.

per_second function

Description: Aggregates events per second.
Syntax: <base search> | bin <timestamp field> span=1s | stats <aggregations>
Example Usage:
<base search>
| bin <timestamp field> span=1s | stats <aggregations>
Output:
Aggregated statistics per second.

rate function

Description: Calculates the rate of change of a field per second.
Syntax: <base search> | eval <new field> = rate(<field>) AS <new field>
Example Usage:
<base search>
| eval <new field> = rate(<field>) AS <new field>
Output:
The rate of change of the field per second.

rate_avg function

Description: Calculates the average rate of change of a field per second.
Syntax: <base search> | eval <new field> = rate_avg(<field>) AS <new field>
Example Usage:
<base search>
| eval <new field> = rate_avg(<field>) AS <new field>
Output:
The average rate of change of the field per second.

rate_sum function

Description: Calculates the sum of rates of change of a field per second.
Syntax: <base search> | eval <new field> = rate_sum(<field>) AS <new field>
Example Usage:
<base search>
| eval <new field> = rate_sum(<field>) AS <new field>
Output:
The sum of rates of change of the field per second.