SPL data types and clauses

http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/ListOfDataTypes#wc-field

Data types

bool

The **<bool>** argument value represents the Boolean data type. The documentation specifies 'true' or 'false'. Other variations of Boolean values are accepted in commands. For example, for 'true' you can also use 't', 'T', 'TRUE', or the number one '1'. For 'false', you can use 'f', 'F', 'FALSE', or the number zero '0'.

int

The **<int>** argument value represents the integer data type.

num

The <num> argument value represents the number data type.

float

The <float> argument value represents the float data type.

Common syntax clauses

bin-span

Syntax: span=(<span-length> | <log-span>)
Description: Sets the size of each bin.
Example: span=2d
Example: span=5m
Example: span=10

by-clause

Syntax: by <field-list>
Description: Fields to group by.
Example: BY addr, port
Example: BY host

eval-function

Syntax: abs | case | cidrmatch | coalesce | exact | exp | floor | if | ifnull | isbool | isint | isnotnull | isnull | isnum | isstr | len|like | ln|log | lower | match | max | md5 | min | mvcount | mvindex | mvfilter | now | null | nullif | pi | pow | random | replace | round | searchmatch | sqrt | substr | tostring | trim | ltrim | rtrim | typeof | upper | urldecode | validate

Description: Function used by eval.

Example: md5(field)

Example: typeof(12) + typeof("string") + typeof(1==2) + typeof(badfield)

Example: searchmatch("foo AND bar")

Example: sqrt(9)

Example: round(3.5)

Example: replace(date, "^(\d{1,2})/(\d{1,2})/", "\2/\1/")

Example: pi()

Example: nullif(fielda, fieldb)

Example: random()

Example: pow(x, y)

Example: mvfilter(match(email, "\.net$") OR match(email, "\.org$"))

Example: mvindex(multifield, 2)

Example: null()

Example: now()

Example: isbool(field)

Example: exp(3)

Example: floor(1.9)

Example: coalesce(null(), "Returned value", null())

Example: exact(3.14 * num)

Example: case(error == 404, "Not found", error == 500, "Internal Server Error", error == 200, "OK")

Example: cidrmatch("123.132.32.0/25", ip)

Example: abs(number)

Example: isnotnull(field)

Example: substr("string", 1, 3) + substr("string", -3)

Example: if(error == 200, "OK", "Error")

Example: len(field)

Example: log(number, 2)

Example: lower(username)

Example: match(field, "^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$")

Example: max(1, 3, 6, 7, "f"^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$")oo", field)

Example: like(field, "foo%")

Example: ln(bytes)

Example: mvcount(multifield)

Example: urldecode("http%3A%2F%2Fwww.splunk.com%2Fdownload%3Fr%3Dheader")

Example: validate(isint(port), "ERROR: Port is not an integer", port >= 1 AND port <= 65535, "ERROR: Port is out of range")

Example: tostring(1==1) + " " + tostring(15, "hex") + " " + tostring(12345.6789, "commas")

Example: trim(" ZZZZabcZZ ", " Z")

evaled-field

Syntax: eval(<eval-expression>)
Description: A dynamically evaled field

field

field-list

regex-expression

Syntax: (\")?<string>(\")?
Description: A Perl Compatible Regular Expression supported by the PCRE library.
Example: ... | regex _raw="(?<!\d)10.\d{1,3}\.\d{1,3}\.\d{1,3}(?!\d)"

single-agg

Syntax: count | stats-func (<field>)
Description: A single aggregation applied to a single field (can be evaled field). No wildcards are allowed. The field must be specified, except when using the special 'count' aggregator that applies to events as a whole.
Example: avg(delay)
Example: sum({date_hour * date_minute})
Example: count

sort-by-clause

Syntax: ("-"|"+")<sort-field> ","
Description: List of fields to sort by and their sort order (ascending or descending)
Example: - time, host
Example: -size, +source
Example: _time, -host

span-length

Syntax: <int:span>(<timescale>)?
Description: Span of each bin. If using a timescale, this is used as a time range. If not, this is an absolute bucket "length."
Example: 2d
Example: 5m
Example: 10

split-by-clause

Syntax: <field> (<tc-option>)* (<where-clause>)?
Description: Specifies a field to split by. If field is numerical, default discretization is applied.

stats-agg

Syntax: <stats-func>("(" (<evaled-field> | <wc-field>)? ")")?
Description: A specifier formed by a aggregation function applied to a field or set of fields. As of 4.0, it can also be an aggregation function applied to a arbitrary eval expression. The eval expression must be wrapped by "{" and "}". If no field is specified in the parenthesis, the aggregation is applied independently to all fields, and is equivalent to calling a field value of * When a numeric aggregator is applied to a not-completely-numeric field no column is generated for that aggregation.
Example: count({sourcetype="splunkd"})
Example: max(size)
Example: stdev(*delay)
Example: avg(kbps)

tc-option

Syntax: <bins-options> | (usenull=<bool>) | (useother=<bool>) | (nullstr=<string>) |(otherstr=<string>)
Description: Options for controlling the behavior of splitting by a field. In addition to the bins-options: usenull controls whether or not a series is created for events that do not contain the split-by field. This series is labeled by the value of the nullstr option, and defaults to NULL. useother specifies if a series should be added for data series not included in the graph because they did not meet the criteria of the <where-clause>. This series is labeled by the value of the otherstr option, and defaults to OTHER.
Example: otherstr=OTHERFIELDS
Example: usenull=f
Example: bins=10

timeformat

Syntax: timeformat=<string>
Description: Set the time format for starttime and endtime terms.
Example: timeformat=%m/%d/%Y:%H:%M:%S

timestamp

Syntax: (MM/DD/YY)?:(HH:MM:SS)?|<int>
Description: None
Example: 10/1/07:12:34:56
Example: -5

where-clause

Syntax: where <single-agg> <where-comp>

Description: Specifies the criteria for including particular data series when a field is given in the tc-by-clause. This optional clause, if omitted, default to "where sum in top10". The aggregation term is applied to each data series and the result of these aggregations is compared to the criteria. The most common use of this option is to select for spikes rather than overall mass of distribution in series selection. The default value finds the top ten series by area under the curve. Alternately one could replace sum with max to find the series with the ten highest spikes.

Example: where max < 10

Example: where count notin bottom10

Example: where avg > 100

Example: where sum in top5

wc-field