where

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/Where

Description

The `where` command uses `eval` expressions to filter search results. The search keeps only the results for which the evaluation was successful (that is, the Boolean result was true).

The `where` command uses the same expression syntax as `eval`. Also, both commands interpret quoted strings as literals. If the string is not quoted, it is treated as a field. Because of this, you can use `where` to compare two different fields, which you cannot use `search` to do.

Syntax

where <eval-expression>

Required arguments

eval-expression

Syntax: <string>

Description: A combination of values, variables, operators, and functions that represent the value of your destination field.

The syntax of the eval expression is checked before running the search, and an exception will be thrown for an invalid expression.

- The result of an eval statement is not allowed to be boolean. If the expression cannot be successfully evaluated for a particular event at search-time, eval erases the value in the result field.
- If the expression references a **field name** that contains non-alphanumeric characters, it needs to be surrounded by**single quotes**; for example, `new=count+'server-1'`.
- If the expression references **literal strings** that contains non-alphanumeric characters, it needs to be surrounded by **double quotes**; for example, `new="server-"+count`.

Functions

The where command includes the following functions: `abs, case, ceil, ceiling, cidrmatch, coalesce, commands, exact, exp, floor, if, ifnull, isbool, isint, isnotnull, isnull, isnum, isstr, len, like, ln, log, lower, ltrim, match, max, md5, min, mvappend, mvcount, mvindex, mvfilter, mvjoin, mvrange, mvzip, now, null, nullif, pi, pow, random, relative_time, replace, round, rtrim, searchmatch, sha1, sha256, sha512, sigfig, spath, split, sqrt, strftime, strptime, substr, time, tonumber, tostring, trim, typeof, upper, urldecode, validate.`.

For **descriptions and examples** of each function, see "Evaluation functions".

Examples

Example 1: Return "CheckPoint" events that match the IP or is in the specified subnet.

```
host="CheckPoint" | where like(src, "10.9.165.%") OR cidrmatch("10.9.165.0/25", dst)
```

Example 2: Return "physicjobs" events with a speed is greater than 100.

```
sourcetype=physicsjobs | where distance/time > 100
```

See also

eval, search, regex

Answers

Have questions? Visit Splunk Answers and see what questions and answers the Splunk community has using the where command.