### search

Filters only the input data that match the specified expression.

#### Syntax

search [limit=INT] EXPR

Required Parameter

**EXPR**

Filter conditions in the form of an expression. For example, you can enter a comparison expression in the form "KEY == VALUE" or "KEY != VALUE" or a boolean expression. You can concatenate conditional expressions using logical operators such as and and or.

Only if the EXPR is true, the data can be passed to the next query command.

Optional Parameter

**limit=INT**

Maximum number of records to return (default: unlimited).

#### Usage

Filter a log containing the game string literal in the **line** field (supports wildcards).

search line == "\*game\*"

Filter a log where the status code is not 200.

search status != 200

Search for the case where src\_ip is 1.2.3.4 and dst\_port is 22.

search src\_ip == ip("1.2.3.4") and dst\_port == 22