### fulltext

Searches for data stored in a table using a full-text index.

#### Syntax

fulltext [duration=INT{mon|w|d|h|m|s}] [from=yyyyMMddHHmmss] [to=yyyyMMddHHmmss] [limit=INT] [offset=INT] [order={desc|asc}] [tt=BOOL] EXPR [from TABLE[.INDEX], ...]

Required Parameter

**EXPR [from TABLE[.INDEX], ...]**

String literal or expression to match records in the table and/or index. If you specify only TABLE, all indexes in the table are retrieved. If you specify the same table or index multiple times, the same search results are duplicated and returned as many time as specified.

EXPR is an expression that expresses the data to be searched and must satisfy the following rules.

1. You can use comparison operators. The comparison operators you can use are: ==, !=, >=, >, <, <=
2. The string to be searched must be enclosed in a pair of double quotes (" ") and is case insensitive.
3. You can provide a combination of the logical operators and, or, not, and a pair of parentheses (( )).
4. This searches all tables unless you specify a table.
5. If there is a table or index specified more than once, it is returned as many times as it is duplicated.

EXPR recognizes the subquery enclosed in a pair of square brackets([ ]) in the expression. This runs the subquery first before running an index search and then searches all terms to be returned in the results of the subquery. The more search targets returned by the subquery, the slower the index search speed. We recommend that you use the ['fields'](https://docs.logpresso.com/en/query/fields-command) command in a subquery to retrieve only the fields that you really need.

range() and iprange() functions are exclusive to EXPR.

range() function returns the values that fall within a specified range in the table index.

range(MIN\_INT, MAX\_INT)

**MIN\_INT**

Starting index value. This value is include in the range.

**MAX\_INT**

Ending index value. This value is include in the range.

iprange() function returns IP addresses that fall within a specified IPv4 or IPv6 address range in the table index.

iprange(START\_IP\_EXPR, END\_IP\_EXPR)

**START\_IP\_EXPR**

Expression to return the starting IP address of the IP address range. This ip address is included in the range.

**END\_IP\_EXPR**

Expression to return the ending IP address of the IP address range. This ip address is included in the range.

Optional Parameter

**duration=INT{mon|w|d|h|m|s}**

Time range to search the previous data based on the current time. You can specify time in units of mon (month), w (week), d (day), h (hour), m (minute), and s (second). For example, 10s refers to "the last 10 seconds" based on the current time. This option cannot be used with from and to.

**from=yyyyMMddHHmmss**

Start date and time of the period to search in the form of yyyyMMddHHmmss. The time period for the search includes the specified time point. If you provide only the first part, the remaining digits are recognized as 0. For example, if you provide 20130605, it is recognized as 20130605000000 (June 5, 2013, 00:00:00). This option cannot be used with duration.

**to=yyyyMMddHHmmss**

Specify the date and time to end the search in the form of yyyyMMddHHmmss. The time period for the search does NOT include the specified time point. The input format is the same as from. This option cannot be used with duration.

**limit=INT**

Maximum number of search results (default: unlimited).

**offset=INT**

Number of search results to skip (default: 0).

**order={desc|asc}**

Search order of the index (default: desc)

1. desc: Searches from the most recent data to the oldest ones.
2. asc: Searches from the oldest data to the most recent ones.

**tt=BOOL**

Boolean option to use the search term tokenizer (default: f).

1. t: Searches the string by splitting it into tokenizers for each index.
2. f: NOT use the search tokenizer

When you use the tt option, the string wildcard (\*) in EXPR can only be placed at the beginning or end of the string. For example, you can enter "\*asp", "asp\*", and "\*asp\*" in the EXPR, but not "a\*sp". Tokens are separated by the and logical operator to reconstruct the query statement. For example, the query statement fulltext tt=t dst == "10.10.130.235" is reconstructed as fulltext dst == "10" and dst == "10" and dst == "130" and dst == "235".

If you do not use 'duration', 'from' or 'to', all logs are searched.

#### Usage

Search for logs dated June 5, 2013 including "1.2.3.4" from the table.

fulltext from=20130605 to=20130606 "1.2.3.4"

Search for all web logs including "cmdshell" from the iis table.

fulltext "cmdshell" from iis

Search for all web logs including "MSIE" or "Firefox" strings while including the word "game" from the "iis" table.

fulltext "game" and ("MSIE" or "Firefox") from iis

Search for web logs including numbers in the range of 400 to 500 from the iis table.

fulltext range(400, 500) from iis

Search for IP addresses that fall within the range from 192.0.0.1 to 192.0.0.255 in the tables with the name pattern \*.\*SSLVPN.

fulltext iprange("192.0.0.1", "192.0.0.255") from \*.\*SSLVPN

Search for the IP set of the blacklist DB from the iis table.

fulltext [ dbquery black select ip from ip\_blacklist ] from iis

Search for full text for a set of tables where the parser of the table is openssh.

fulltext "term" from meta("parser==openssh")

Search for full text for the next 20 fidx index data after skipping the first 5 index data.

fulltext offset=5 limit=20 "\*" from iis.fidx

Split the "1.2.3.4" string using the tokenizer for the fidx index and match them against the fidx index from the iis table

fulltext tt=t "1.2.3.4" from iis.fidx