### fulltext

指定したインデックスに対してフルテキスト検索を実行します。

#### 構文

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], ...]

必須パラメータ

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

テーブル（TABLE）またはテーブル内の特定インデックス（INDEX）に対して検索する文字列または式を指定します。TABLEを指定しない場合、すべてのテーブルが検索対象となります。TABLEのみを指定した場合、そのテーブル内のすべてのインデックスが検索対象となります。同じTABLEやINDEXを複数回指定した場合、指定した回数分だけ出力されます。

EXPRは検索対象データを表現する式であり、以下の規則を満たす必要があります。

1. 比較演算子を使用できます。利用可能な比較演算子は次の通りです：==, !=, >=, >, <, <=
2. 検索する文字列はダブルクォーテーション（" "）で囲みます。大文字・小文字は区別されません。
3. 論理演算子and、or、notおよび丸括弧（( )）を組み合わせて入力できます。
4. テーブルを指定しない場合、すべてのテーブルが検索対象となります。
5. 重複して指定されたテーブルやインデックスがある場合、重複回数分だけ出力されます。

EXPR内では、角括弧（[ ]）で囲んだサブクエリを認識します。インデックス検索を実行する前にサブクエリが先に実行され、サブクエリの結果に含まれるすべての用語が検索されます。サブクエリが返す検索対象が多いほど、インデックス検索の速度は低下します。サブクエリ内では[fields](https://docs.logpresso.comnull)コマンドを使用し、必要なフィールドのみを検索することを推奨します。

EXPRで使用できる専用関数として、range()およびiprange()があります。これら2つの関数は他のコマンドでは使用できません。

range()関数は、指定したインデックスにおいて、引数で与えた範囲に含まれる数値を検索します。

range(MIN\_INT, MAX\_INT)

**MIN\_INT**

検索範囲の最小値。この値は検索範囲に含まれます。

**MAX\_INT**

検索範囲の最大値。この値も検索範囲に含まれます。

iprange()関数は、インデックス内で指定したIPv4またはIPv6アドレス区間に含まれるIPアドレスを検索します。

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

**START\_IP\_EXPR**

検索するIPアドレス区間の開始アドレス文字列を返す式。この値は検索範囲に含まれます。

**END\_IP\_EXPR**

検索するIPアドレス区間の終了アドレス文字列を返す式。この値も検索範囲に含まれます。

オプションパラメータ

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

現在時刻を基準に、指定した期間内のログのみを検索します。mon（月）、w（週）、d（日）、h（時）、m（分）、s（秒）単位で指定できます。例：10sは「現在時刻から直近10秒間」を意味します。このオプションはfrom、toと同時に使用できません。

**from=yyyyMMddHHmmss**

検索対象期間の開始日時をyyyyMMddHHmmss形式で指定します。指定した時刻も検索範囲に含まれます。先頭部分のみ入力した場合、残りの桁は0として扱われます。例：20130605と入力すると20130605000000（2013年6月5日0時0分0秒）と認識されます。このオプションはdurationと同時に使用できません。

**to=yyyyMMddHHmmss**

検索対象期間の終了日時をyyyyMMddHHmmss形式で指定します。指定した時刻は検索範囲に含まれません。入力方法はfromと同様です。このオプションはdurationと同時に使用できません。

**limit=INT**

検索するレコードの最大件数（デフォルト：制限なし）

**offset=INT**

検索結果からスキップする件数（デフォルト：0）

**order={desc|asc}**

インデックスの検索順序（デフォルト：desc）

1. desc：新しいデータから検索
2. asc：古いデータから検索

**tt=BOOL**

検索トークナイザーの使用有無（デフォルト：f）。tt=tの場合、検索文字列を各インデックスに適したトークナイザーで分割して検索します。また、EXPR内でのワイルドカード（\*）は文字列の先頭または末尾のみに使用可能です。例：" \*asp", "asp\*", "\*asp\*"は指定可能ですが、"a\*sp"は指定できません。分割された検索語はand論理演算子で結合され、クエリ文が再構成されます。例：fulltext tt=t dst == "10.10.130.235"は、fulltext dst == "10" and dst == "10" and dst == "130" and dst == "235"として再構成されます。

'duration'、'from'、'to'を指定しない場合、すべての期間のレコードが検索対象となります。

#### 使用例

全テーブルから2013年6月5日のログのうち「1.2.3.4」を含むログを検索

fulltext from=20130605 to=20130606 "1.2.3.4"

iisテーブルから「cmdshell」を含むすべてのWebログを検索

fulltext "cmdshell" from iis

iisテーブルから「game」を含み、かつ「MSIE」または「Firefox」を含むすべてのWebログを検索

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

iisテーブルから400～500の範囲の数値を含むWebログを検索

fulltext range(400, 500) from iis

「SSLVPN」で終わるすべてのテーブルから192.0.0.1～192.0.0.255のIPアドレスを検索

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

iisテーブルからブラックリストDBのIP集合を検索

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

パーサーがopensshであるテーブル集合を対象にフルテキスト検索

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

iisテーブルのfidxインデックスデータから最初の5件をスキップし、20件を取得

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

「1.2.3.4」文字列をfidxインデックスのトークナイザーで分割し、iisテーブルのfidxインデックスで検索

fulltext tt=t "1.2.3.4" from iis.fidx