### fulltext

지정된 인덱스에 대해 풀텍스트 검색을 수행합니다.

#### 문법

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], ...]

필수 매개변수

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

테이블(TABLE) 또는 테이블의 특정 인덱스(INDEX)에서 검색할 문자열 또는 표현식. TABLE을 지정하지 않으면 모든 테이블을 검색합니다. TABLE만 지정하면 해당 테이블의 모든 인덱스를 검색합니다. 만약 같은 TABLE이나 INDEX를 여러 번 지정하면, 중복해서 지정한 횟수만큼 출력됩니다.

EXPR은 검색할 데이터를 표현하는 식으로, 다음과 같은 규칙을 만족해야 합니다.

1. 비교연산자를 사용할 수 있습니다. 사용할 수 있는 비교연산자는 다음과 같습니다: ==, !=, >=, >, <, <=
2. 검색할 문자열은 큰 따옴표 쌍(" ")으로 감싸야 하며, 대소문자를 구분하지 않습니다.
3. 논리 연산자인 and, or, not과 괄호 쌍(( ))을 조합해 입력할 수 있습니다.
4. 테이블을 지정하지 않으면 모든 테이블을 검색합니다.
5. 중복 지정된 테이블이나 인덱스가 있으면 중복 횟수만큼 출력됩니다.

EXPR은 표현식에 대괄호 쌍([ ])으로 감싼 서브쿼리를 인식합니다. 인덱스 검색을 수행하기 전에 서브쿼리를 먼저 수행하고, 서브쿼리 결과에 등장하는 모든 용어를 검색합니다. 서브쿼리가 반환하는 검색 대상이 많을수록 인덱스 검색 속도가 느려집니다. 서브쿼리에 [fields](https://docs.logpresso.comnull) 명령어를 사용하여 꼭 필요한 필드만 검색하는 것을 권장합니다.

EXPR에서 사용할 수 있는 전용 함수로 range(), iprange()가 있습니다. 이 두 함수는 다른 명령어에서 사용할 수 없습니다.

range() 함수는 인자로 받은 인덱스에서 지정된 범위에 포함되는 숫자를 검색합니다.

range(MIN\_INT, MAX\_INT)

**MIN\_INT**

검색할 범위의 숫자 중에서 최소값. 이 값은 검색 범위에 포함됩니다.

**MAX\_INT**

검색할 범위의 숫자 중에서 최대값. 이 값은 검색 범위에 포함됩니다.

iprange() 함수는 인덱스에서 지정된 IPv4 또는 IPv6 주소 구간에 포함되는 IP 주소를 검색합니다.

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

**START\_IP\_EXPR**

검색할 IP 주소 구간의 시작 주소 문자열을 반환하는 표현식. 이 값은 검색 범위에 포함됩니다.

**END\_IP\_EXPR**

검색할 IP 주소 구간의 마지막 주소 문자열을 반환하는 표현식. 이 값은 검색 범위에 포함됩니다.

선택 매개변수

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

현재 시각을 기준으로 지정한 시간 이내의 로그만 검색합니다. mon(월), w(주), d(일), h(시), m(분), s(초) 단위로 지정할 수 있습니다. 예를 들어 10s은 현재 시각을 기준으로 "최근 10초"를 의미합니다. 이 옵션은 from, to와 함께 사용할 수 없습니다.

**from=yyyyMMddHHmmss**

검색 대상 기간의 시작 날짜와 시각. yyyyMMddHHmmss 형식으로 입력하며, 입력한 시각도 검색 범위에 포함됩니다. 앞부분만 입력하면 나머지 자리는 0으로 인식합니다. 예를 들어, 20130605를 입력하면 20130605000000(2013년 6월 5일 0시 0분 0초)으로 인식합니다. 이 옵션은 duration과 함께 사용할 수 없습니다.

**to=yyyyMMddHHmmss**

검색 대상 기간의 마지막 날짜와 시각. yyyyMMddHHmmss 형식으로 입력하며, 입력한 시각은 검색 범위에 포함되지 않습니다. 입력 방식은 from과 같습니다. 이 옵션은 duration과 함께 사용할 수 없습니다.

**limit=INT**

검색할 레코드의 최대 개수(기본값: 제한 없음)

**offset=INT**

건너뛸 검색 결과 개수(기본값: 0)

**order={desc|asc}**

인덱스의 검색 순서(기본값: desc)

1. desc: 최근 데이터부터 검색
2. asc: 오래된 데이터부터 검색

**tt=BOOL**

검색 토크나이저의 사용 여부(기본값: f). tt=t일 때, 검색할 문자열을 각 인덱스에 맞는 토크나이저로 분할하여 검색합니다. 또한 EXPR에서 문자열 와일드카드(\*)는 문자열 시작이나 끝에만 넣을 수 있습니다. 예를 들어 EXPR에 "\*asp", "asp\*", "\*asp\*"은 입력 가능하지만 "a\*sp"는 입력할 수 없습니다. 분할된 검색어는 and 논리연산자로 묶여 쿼리문이 재구성됩니다. 예를 들어 fulltext tt=t dst == "10.10.130.235" 쿼리문은 fulltext dst == "10" and dst == "10" and dst == "130" and dst == "235"으로 재구성됩니다.

'duration', 'from'과 'to'를 사용하지 않으면 레코드를 기록한 모든 기간에 대해 검색합니다.

#### 사용 예

전체 테이블에서 2013년 6월 5일 로그 중 1.2.3.4를 포함한 로그 검색

fulltext from=20130605 to=20130606 "1.2.3.4"

iis 테이블에서 cmdshell을 포함한 모든 웹 로그 검색

fulltext "cmdshell" from iis

iis 테이블에서 game을 포함하면서 MSIE 혹은 Firefox 문자열이 포함된 모든 웹 로그 검색

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

iis 테이블에서 400~500 범위의 숫자를 포함한 웹 로그 검색

fulltext range(400, 500) from iis

SSLVPN으로 끝나는 모든 테이블에서 192.0.0.1 ~ 192.0.0.255 사이의 IP 주소 검색

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

iis 테이블에서 블랙리스트 DB의 IP 집합을 검색

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

테이블의 파서가 openssh인 테이블 집합을 대상으로 풀텍스트 검색

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

iis 테이블의 fidx 인덱스 데이터 중 첫 5건은 건너뛴 후 20건 조회

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

"1.2.3.4" 문자열을 fidx 인덱스의 토크나이저를 사용해 분할하여 iis 테이블의 fidx 인덱스에서 검색

fulltext tt=t "1.2.3.4" from iis.fidx