### search

지정된 표현식과 일치하는 입력 데이터를 검색합니다.

#### 문법

search [limit=INT] EXPR

필수 매개변수

**EXPR**

검색 조건 표현식. 예를 들어, "KEY == VALUE" 또는 "KEY != VALUE" 형태의 비교 조건식, 또는 불리언 조건식을 입력할 수 있습니다. and, or 같은 논리 연산자를 이용해 조건식을 연결할 수 있습니다.

EXPR이 참일 때에만 데이터를 다음 쿼리 명령어로 전달합니다.

선택 매개변수

**limit=INT**

반환할 최대 레코드 개수(기본값: 제한 없음)

#### 사용 예

**line** 필드에 game 문자열을 포함하는 로그 (와일드카드 지원)

search line == "\*game\*"

상태 코드가 200이 아닌 로그

search status != 200

src\_ip가 1.2.3.4이고 dst\_port가 22인 경우

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