### event

로그프레소 소나에서 시나리오 기반하여 탐지한 이벤트 목록을 조회합니다.

#### 문법

event [duration=INT{mon|w|d|h|m|s}] [from=yyyyMMddHHmmss] [to=yyyyMMddHHmmss] [order=STR] [raw=BOOL]

매개변수

duration, from, to과 같은 옵션으로 검색 기간/범위를 지정하지 않으면 모든 데이터를 검색합니다.

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

현재 시각을 기준으로 지정한 시간만큼 이전 데이터만 검색. mon(월), w(주), d(일), h(시), m(분), s(초) 단위로 입력합니다. 예를 들어 10s은 쿼리 실행 시각을 기준으로 "최근 10초"를 의미합니다. 이 옵션은 from, to와 함께 사용할 수 없습니다.

**from=yyyyMMddHHmmss**

검색할 기간의 시작 날짜를 yyyyMMddHHmmss 형식으로 지정. 입력한 시각부터 검색을 시작합니다. 앞부분만 입력하면 나머지 자리는 0으로 인식합니다. 예를 들어 20130605를 입력하면 20130605000000(2013년 6월 5일 0시 0분 0초)으로 인식합니다.

**to=yyyyMMddHHmmss**

검색할 기간의 끝 날짜를 yyyyMMddHHmmss 형식으로 지정. 입력한 시각은 검색 범위에 포함되지 않습니다.

**order=STR**

레코드의 정렬 순서 (기본값: desc)

* asc: 오름차순 정렬. 오래된 레코드부터 출력.
* desc: 내림차순 정렬. 최근 레코드부터 출력.

**raw=BOOL**

원본 이벤트 조회 여부(기본값: f)

* t: 이벤트를 원본 그대로 조회
* f: 정규화된 이벤트 정보를 조회

#### 설명

이 명령어는raw=f일 때 정규화된 이벤트 정보를, raw=t일 때 이벤트를 원본 형태 그대로 보여줍니다. 하나의 이벤트는 여러 개의 원본 로그에 매핑될 수 있으므로 정규화된 이벤트와 원본은 조회 레코드 개수에 차이가 있을 수 있습니다. 로그프레소 소나의 티켓 화면에서 근거자료로 활용되는 이벤트는 raw=t가 적용된 형태로 보여줍니다.

event의 출력 필드는 이벤트마다 각각 고유한 필드, 또는 마리아 DB의 데이터베이스 컬럼을 포함할 수 있으므로 가변적입니다. 다만, **\_time** 필드는 **\_log\_time**으로 표시합니다.

#### 사용 예

2023년 5월 23일 00:00:00부터 5월 23일 23:59:59까지 발생한 이벤트 조회

event from=20230523 to=20230524