### timechart

지정된 시간 단위마다 집계 함수의 결과를 계산합니다. by 절을 이용하여 그룹 필드를 지정하는 경우, 그룹 필드 값으로 필드가 생성되면서 필드별 통계 값을 계산합니다.

#### 문법

timechart span=INT{y|mon|w|d|h|m|s} AGGR\_FUNC [as ALIAS], ... [by GRP\_FIELD, ...]

필수 매개변수

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

**\_time** 필드의 시간 단위. y(연), mon(월), w(주), d(일), h(시), m(분), s(초) 단위로 지정할 수 있습니다. 가령, 10m은 10분 단위입니다. 월 단위 mon을 사용하는 경우, 집계가 가능하도록 12의 약수 중에서 1mon, 2mon, 3mon, 4mon, 6mon만 지정할 수 있습니다. 즉, 3mon은 허용되지만 5mon은 허용되지 않습니다. 12mon 대신에 1y를 사용합니다. 단위가 y일 때, 1y만 허용됩니다.

**AGGR\_FUNC [as ALIAS], ...**

실행할 집계 함수(AGGR\_FUNC)를 이용해 표현식을 입력합니다. as 절을 이용해 집계 함수값을 담을 필드에 이름(ALIAS)을 지정할 수 있습니다. 이름을 지정하지 않으면 **count()**, **sum(sent\_pkts)** 등 함수 이름을 필드 이름으로 사용하므로 필드 이름(ALIAS)을 지정하는 것이 좋습니다.

선택 매개변수

**by GRP\_FIELD, ...**

집계에 사용할 그룹 필드 목록. 구분자로 쉼표(,)를 사용합니다.

#### 사용 예

10분 단위 로그 발생량

timechart span=10m count

1분 단위 bytes 변화 추이

timechart span=1m sum(bytes)

각 목적지 포트의 1시간 단위 로그 발생 갯수

timechart span=1h count by dst\_port