### parse

입력 데이터에 특정 파서를 지정하거나, 파싱 규칙을 지정해 출력합니다.

#### 문법

parse [overlay=t] PARSERparse [overlay=t] [field=TARGET\_FIELD] PARSING\_RULE, ...

필수 매개변수

**PARSER**

파서 이름. 사용할 수 있는 파서의 이름은 웹 콘솔에서 확인할 수 있습니다.

1. (STD, ENT) **시스템 설정 > 파서/트랜스포머 > 파서에서 이름 필드 확인**
2. (MAE, SNR) **수집 > 원본 로그 파서, 정규화 파서**에서 파서 식별자 필드 확인

파서를 지정하면 파서가 출력할 필드가 이미 정의되어 있으므로 field=TARGET\_FIELD 옵션을 함께 사용할 수 없습니다.

**PARSING\_RULE, ...**

사용자 정의 파싱 규칙 목록. 구분자로 쉼표(,)를 사용합니다. 파싱 규칙문의 형식은 "START\_ANCHOR\*STOP\_ANCHOR" as FIELD\_NAME입니다.

1. START\_ANCHOR\*STOP\_ANCHOR: 파싱 앵커
2. as FIELD\_NAME: 필드 이름으로 사용할 레이블

시작 문자열(START\_ANCHOR)과 끝 문자열(STOP\_ANCHOR)을 인식해 문자열을 파싱하고, as 절로 부여된 레이블을 필드 이름으로 사용합니다.

선택 매개변수

**overlay=BOOL**

원본 데이터의 출력 옵션(기본값: f).

1. t: 파싱된 데이터를 필드에 출력하고, 원본 데이터를 **line** 필드에 출력
2. f: 파싱된 데이터만 필드에 출력

**field=TARGET\_FIELD**

입력 데이터 스트림에서 파싱할 값이 있는 필드 이름(기본값: line). 이 옵션을 파서(PARSER)와 함께 사용할 수 없습니다.

#### 사용 예

openssh 파서를 이용해 ssh\_log 테이블에 저장된 로그를 파싱

table from=20200601 to=20200701 ssh\_log | parse openssh

로그에서 시작과 끝 텍스트를 지정하여 필드 추출(다음 내용을 'sample.txt'로 저장해서 사용)

Nov 11 00:00:00 session: Proto:17, Policy:pass, Rule:9000, Type:open, Start\_Time:Nov 11 00:00:00, End\_Time:-

아래 명령으로 위와 같은 원본에서 **session**, **proto**, **policy**, **rule**, **end\_time** 필드를 추출할 수 있습니다.

textfile /opt/logpresso/sample.txt | parse "session:\* " as session, "Proto:\*," as proto, "Policy:\*," as policy, "Rule:\*," as rule, "Start\_Time:\*," as start\_time, "End\_Time:\*" as end\_time