### parse

入力データに特定のパーサーを指定するか、またはパースルールを指定して出力します。

#### 構文

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

必須パラメーター

**PARSER**

パーサー名。利用可能なパーサー名はWebコンソールで確認できます。

1. (STD, ENT) **システム設定 > パーサー/トランスフォーマー > パーサー**の「名前」フィールドを参照
2. (MAE, SNR) **収集 > 元ログパーサー、正規化パーサー**の「パーサー識別子」フィールドを参照

パーサーを指定した場合、パーサーが出力するフィールドはすでに定義されているため、field=TARGET\_FIELDオプションは併用できません。

**PARSING\_RULE, ...**

ユーザー定義パースルールのリスト。区切り文字はカンマ（,）です。パースルールの形式は "START\_ANCHOR\*STOP\_ANCHOR" as FIELD\_NAME です。

1. START\_ANCHOR\*STOP\_ANCHOR: パースアンカー
2. as FIELD\_NAME: フィールド名として使用するラベル

開始文字列（START\_ANCHOR）と終了文字列（STOP\_ANCHOR）を認識して文字列をパースし、as句で指定したラベルをフィールド名として使用します。

オプションパラメーター

**overlay=BOOL**

元データの出力オプション（デフォルト: f）。

1. t: パースされたデータを各フィールドに出力し、元データは**line**フィールドに出力
2. f: パースされたデータのみを各フィールドに出力

**field=TARGET\_FIELD**

入力データストリームからパース対象となる値が格納されているフィールド名（デフォルト: line）。このオプションはパーサー（PARSER）と併用できません。

#### 使用例

opensshパーサーを利用してssh\_logテーブルに保存されたログをパース

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

ログから開始および終了テキストを指定してフィールドを抽出（以下の内容を 'sample.txt' として保存して使用）

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

下記のコマンドで、上記の元データから**session**、**proto**、**policy**、**rule**、**end\_time**フィールドを抽出できます。

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