### event

ログプレッソ・ソナーにおいて、シナリオベースで検出されたイベント一覧を照会します。

#### 構文

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

パラメータ

duration、from、toなどのオプションで検索期間・範囲を指定しない場合、すべてのデータが検索対象となります。

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

現在時刻を基準に、指定した時間分だけ過去のデータのみを検索します。mon（月）、w（週）、d（日）、h（時）、m（分）、s（秒）単位で指定します。例：10sはクエリ実行時点から「直近10秒間」を意味します。このオプションはfrom、toと同時に使用できません。

**from=yyyyMMddHHmmss**

検索開始日時をyyyyMMddHHmmss形式で指定します。指定した時刻から検索を開始します。先頭部分のみ入力した場合、残りの桁は0として認識されます。例：20130605と入力すると20130605000000（2013年6月5日0時0分0秒）として扱われます。

**to=yyyyMMddHHmmss**

検索終了日時をyyyyMMddHHmmss形式で指定します。指定した時刻は検索範囲に含まれません。

**order=STR**

レコードのソート順（デフォルト：desc）

* asc: 昇順。古いレコードから出力。
* desc: 降順。新しいレコードから出力。

**raw=BOOL**

元イベントの参照可否（デフォルト：f）

* t: イベントを元のまま表示
* f: 正規化されたイベント情報を表示

#### 説明

本コマンドは、raw=fの場合は正規化されたイベント情報を、raw=tの場合はイベントを元の形式で表示します。1つのイベントが複数の元ログにマッピングされる場合があるため、正規化イベントと元イベントでは出力レコード数が異なる場合があります。ログプレッソ・ソナーのチケット画面で証拠資料として利用されるイベントは、raw=tが適用された形式で表示されます。

eventコマンドの出力フィールドは、イベントごとに固有のフィールドやMariaDBのデータベースカラムを含む場合があり、可変的です。ただし、**\_time**フィールドは\*\*\_log\_time\*\*として表示されます。

#### 使用例

2023年5月23日00:00:00から5月23日23:59:59までに発生したイベントを照会

event from=20230523 to=20230524