### event

Retrieves events based on scenarios provided in Logpresso Sonar.

#### Syntax

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

Parameters

If you do not use duration, from or to, all events are searched.

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

Time range to search the previous data based on the current time. You can specify the time in units of mon (month), w (week), d (day), h (hour), m (minute), and s (second). For example, 10s refers to "the last 10 seconds" based on the time the query is executed. This option cannot be used with from or to.

**from=yyyyMMddHHmmss**

Start date and time of the period to search in the form of yyyyMMddHHmmss. The time period for the search includes the specified time point. If you provide only the first part, the remaining digits are recognized as 0. For example, if you provide 20130605, it is recognized as 20130605000000 (June 5, 2013, 00:00:00).to=yyyyMMddHHmmss

**to=yyyyMMddHHmmss**

End date and time of the period to serch in the form of yyyyMMddHHmmss. The time period for the search does NOT include the specified time point.

**order=STR**

Sorting order of the records (default: desc).

* asc: Sorts in ascending order, the oldest at the top.
* desc: Sortes in descending order, the latest records at the top.

**raw=BOOL**

Whether to retrieve the original event log (default: f).

* t: Retrieves event information as the original event log.
* f: Retrieves only normalized event informations.

#### Description

When raw=f, this query command retrieves only normalized event information. When raw=t, it retrieves event information as the original. A single event can be mapped with multiple original event logs so the number of normalized event may differ from the number of the original event log. Event information on the Ticket page is the same of the result of running this query command with raw=t.

The output fields of when running the event query command vary depending on the fields of the original evnet log because each event log has different default fields, or MariaDB database columnm. The **\_time** field of original log is converted to **\_log\_time** field.

#### Usage

Retrieve events occurred from May 23, 2023 00:00:00 to May 23, 2023 23:59:59.

event from=20230523 to=20230524