Time modifiers for search

http://docs.splunk.com/Documentation/Splunk/6.0.2/SearchReference/SearchTimeModifiers

Use time modifiers to customize the time range of a search or change the format of the timestamps in the search results.

_time and _indextime fields

When an event is processed by the Splunk software, its timestamp is saved as the default field `_time`. This timestamp, which is the time when the event occurred, is saved in epoch notation. Searching with relative time modifiers, `earliest` or `latest`, finds every event with a timestamp beginning, ending, or between the specified timestamps. For example, when you search for `earliest=@d`, the search finds every event with a `_time` value since midnight.

You also have the option of searching for events based on when they were indexed. This epoch timestamp is saved in the default field `_indextime`. Similar to `earliest` and `latest` for `_time`, use the relative time modifiers `_index_earliest` and `_index_latest` to search for events based on `_index_time`. For example, if you wanted to search for events indexed in the previous hour, use: `_index_earliest=-h@h _index_latest=@h`.

Note: When using index-time based modifiers such as `index_earliest` and `index_latest`, your search must **also**have an event-time window which will retrieve the events. In other words, chunks of events might be ruled out based on the non index-time window as well as the index-time window. To be certain of retrieving every event based on index-time, you must run your search using **All Time**.

List of time modifiers

Use the `earliest` and/or `latest` modifiers to specify custom and relative time ranges. Also, when specifying relative time, you can use the `now` modifier to refer to the current time.

Modifier	Syntax	Description
earliest	`earliest=[+|-]<time_integer><time_unit>@<time_unit>`	Specify the earliest _time for the time range of your search.
_index_earliest	`_index_earliest=[+|-]<time_integer><time_unit>@<time_unit>`	Specify the earliest _indextime for the time range of your search.
_index_latest	`_index_latest=[+|-]<time_integer><time_unit>@<time_unit>`	Specify the latest _indextime for the time range of your search.
latest	`latest=[+|-]<time_integer><time_unit>@<time_unit>`	Specify the latest time for the _time range of your search.
now	`now()`	Refers to the current time. If set to earliest, now() is the start of the search.
time	`time()`	In real-time searches, time() is the current machine time.

For more information about customizing your search window, see Specify real-time time range windows in your searchin the *Search Manual*.

How to specify relative time modifiers

You can define the relative time in your search with a string of characters that indicate time amount (integer and unit). You can also specify a "snap to" time unit, which is specified with the @ symbol followed by a time unit. For example:

```
[+|-]<time_integer><time_unit>@<time_unit>
```

1. Begin your string with a plus (+) or minus (-) to indicate the offset from the current time.

2. Define your time amount with a number and a unit. The supported time units are:

- second: s, sec, secs, second, seconds
- minute: m, min, minute, minutes
- hour: h, hr, hrs, hour, hours
- day: d, day, days
- week: w, week, weeks
- month: mon, month, months
- quarter: q, qtr, qtrs, quarter, quarters
- year: y, yr, yrs, year, years

Note: For Sunday, you can specify w0 and w7.

For example, to start your search an hour ago use either of the following time modifiers.

```
earliest=-h
```

or

```
earliest=-60m
```

When specifying single time amounts, the number one is implied. An 's' is the same as '1s', 'm' is the same as '1m', 'h' is the same as '1h', and so forth.

3. You can specify a "snap to" time unit. The time unit indicates the nearest or latest time to which your time amount rounds down. Separate the time amount from the "snap to" time unit with an "@" character.

- You can use any of time units listed in Step 2. For example, @w, @week, and @w0 for Sunday; @month for the beginning of the month; and @q, @qtr, or @quarter for the beginning of the most recent

quarter (Jan 1, Apr 1, Jul 1, or Oct 1). You can use the following for specific days of the week: w0 (Sunday), w1, w2, w3, w4, w5 and w6 (Saturday).

- You can also specify **offsets from the snap-to-time** or "chain" together the time modifiers for more specific relative time definitions. For example, `@d-2h` snaps to the beginning of today (12:00 AM) and subtracts 2 hours from that time.
- When snapping to the nearest or latest time, Splunk Enterprise always **snaps backwards** or rounds down to the latest time not after the specified time. For example, if it is 11:59:00 and you "snap to" hours, you will snap to 11:00 not 12:00.
- If you do not specify a time offset before the "snap to" amount, Splunk Enterprise interprets the time as "current time snapped to" the specified amount. For example, if it is currently 11:59 PM on Friday and you use `@w6` to "snap to Saturday", the resulting time is the *previous* Saturday at 12:01 AM.

Example 1: To search events from the beginning of the current week:

```
earliest=@w0
```

Example 2: To search events from the last full business week:

```
earliest=-5d@w1 latest=@w6
```

Example 3: To search with an exact date as boundary, such as from November 5 at 8 PM to November 12 at 8 PM, use the timeformat: `%m/%d/%Y:%H:%M:%S`

```
earliest="11/5/2015:20:00:00" latest="11/12/2015:20:00:00"
```

More time modifiers

These search time modifiers are still valid, but might be removed and their function no longer supported in a future release.

Modifier	Syntax	Description
daysago	`daysago=<int>`	Search events within the last **integer** number of days.
enddaysago	`enddaysago=<int>`	Set an end time for an integer number of days before now.
endhoursago	`endhoursago=<int>`	Set an end time for an integer number of hours before now.
endminutesago	`endminutesago=<int>`	Set an end time for an integer number of minutes before now.
endmonthsago	`endmonthsago=<int>`	Set an end time for an integer number of months before now.
endtime	`endtime=<string>`	Search for events before the specified time (exclusive of the specified time). Use **timeformat** to specify how the timestamp is formatted.
endtimeu	`endtimeu=<int>`	Search for events before the specific epoch time (Unix time). .
hoursago	`hoursago=<int>`	Search events within the last **integer** number of hours.
minutesago	`minutesago=<int>`	Search events within the last **integer** number of minutes.

monthsago	`monthsago=<int>`	Search events within the last **integer** number of months.
searchtimespandays	`searchtimespandays=<int>`	Search within a specified range of days (expressed as an integer).
searchtimespanhours	`searchtimespanhours=<int>`	Search within a specified range of hours (expressed as an integer).
searchtimespanminutes	`searchtimespanminutes=<int>`	Search within a specified range of minutes (expressed as an integer).
searchtimespanmonths	`searchtimespanmonths=<int>`	Search within a specified range of months (expressed as an integer).
startdaysago	`startdaysago=<int>`	Search the specified number of days before the present time.
starthoursago	`starthoursago=<int>`	Search the specified number of hours before the present time.
startminutesago	`startminutesago=<int>`	Search the specified number of minutes before the present time.
startmonthsago	`startmonthsago=<int>`	Search the specified number of months before the present time.
starttime	`starttime=<timestamp>`	Search from the specified date and time to the present (inclusive of the specified time).
starttimeu	`starttimeu=<int>`	Search from the specific epoch (Unix time).
timeformat	`timeformat=<string>`	Set the timeformat for the **starttime** and **endtime**modifiers. By

		default: `timeformat=%m/%d/%Y:%H:%M:%S`