Specify time ranges for real-time searches

Time ranges for historical searches are set at the time the search runs. With real-time searches, the time range boundaries are constantly updating and by default, the results accumulate from the start of the search. You can also specify a range that represent a sliding window of time, for example, the last 30 seconds. When you specify a sliding window, Splunk software uses that amount of time to accumulate data. For example, if your sliding window is 5 minutes, you will not start to see data until after the first 5 minutes have passed. You can override this behavior so that Splunk software backfills the initial window with historical data before running in the normal real-time search mode. See Real-time backfill.

Real-time modifier syntax

To run a search in real time, you can select from predefined Real-time time range windows in the time range range picker list or you can specify a custom real-time window using Custom time... and selecting Real-time.

Time ranges for real-time search follow the same syntax as for historical searches, except that you precede the relative time specifier with "rt", so that it's rt<time_modifier>: rt[+|-]<time_integer><time_unit>@<time_unit>. See Specify time modifiers in your search.

These values are not designed to be used in a search string. If you are a Splunk Enterprise administrator, you can use these values when you edit the times.conf file (to add options to the time range picker), to specify the earliest/latest time ranges in the saved search dialog, or when you use the REST API to access the Splunk search engine.

When you use time range windows with real-time searches, some of the events that occur within the latest second may not be displayed. This is expected behavior and is due to the latency between the timestamps within the events and the time when the event arrives. Because the time range window is with respect to the timestamps within the events and not the time when the event arrives, events that arrive after the time window won't display.

Real-time searches over "all time"

There is a small difference between real-time searches that take place within a set time window (30 seconds, 1 minute, 2 hours) and real-time searches that are set to "all time."

- In "windowed" real-time searches, the events in the search can disappear as they fall outside of the window, and events that are newer than the time the search job was created can appear in the window when they occur.
- In "all-time" real-time searches, the window spans all of your events, so events do not disappear once they appear in the window, but events that are newer than the time the search job was created can appear in the window as they occur.
- In comparison, historical search events never disappear from within the set range of time that you are searching and the latest event is always earlier than the job creation time (with the exception of searches that include events that have future-dated timestamps).

Real-time backfill

For windowed real-time searches, you can backfill the initial window with historical data. This is run as a single search, just in two phases: first, a search on historical data to backfill events; then, a normal real-time search. Real-time backfill ensures that real-time dashboards seeded with data on actual visualizations and statistical metrics over time periods are accurate from the start.

You can enable real-time backfill in the limits.conf file in the [realtime] stanza:
[realtime]

default_backfill = <bool>
* Specifies if windowed real-time searches should backfill events
* Defaults to true

See also

• About real-time searches and reports
• Expected performance and known limitations of real-time searches and reports