Splunk® Enterprise
Getting Data In 8.0.5

How timestamp assignment works

Generated: 8/18/2020 11:24 am
How timestamp assignment works

Timestamp processing is a key step in event processing. Splunk software uses timestamps to:

- Correlate events by time
- Create the timeline histogram in Splunk Web
- Set time ranges for searches

Splunk software adds timestamps to events at index time. It oftentimes assigns timestamp values automatically by using information that it finds in the raw event data. If there is no explicit timestamp in an event, Splunk software attempts to assign a timestamp value through other means. For some data, you might need to help it learn how to recognize the timestamps.

Splunk software stores timestamp values in the _time field, in Coordinated Universal Time (UTC) format.

For more information on event processing, see the chapter in this manual called Configure event processing.

How Splunk software assigns timestamps

Splunk software uses the following precedence rules to assign timestamps to events:

1. It looks for a time or date in the event itself using an explicit TIME_FORMAT, if provided. You configure the TIME_FORMAT attribute in props.conf.
2. If no TIME_FORMAT was configured for the data, Splunk software attempts to automatically identify a time or date in the event itself. It uses the source type of the event (which includes TIME_FORMAT information) to try to find the timestamp.
3. If an event has a time and date, but not a year, Splunk software determines the year, as described in How Splunk software determines timestamps with no year, and builds the timestamp from that.
4. If no events in a source have a date, Splunk software tries to find a date in the source name or file name. Time of day is not identified in filenames. (This requires that the events have a time, even though they don't have a date.)
5. For file sources, if no date can be identified in the file name, Splunk software uses the file modification time.
6. As a last resort, Splunk software sets the timestamp to the current system time when indexing each event.

Splunk software can extract only dates from a source, not times. If you need to extract a time from a source, use a transform. See Create custom fields at index time.

How Splunk software determines timestamps with no year

If Splunk software discovers a timestamp within an event that does not have a year element, it uses the following logic to determine the year:

1. It identifies the current date by using either the date of the event it last parsed or the current clock time.
2. It then uses the year from that date as a base and runs the year through several tests:
   1. If the date in the new event is December 31 and the current date is January 1, it decrements the base year.
   2. If the date in the new event is January 1 and the current date is December 31, it increments the base year.
   3. If the date in the new event is February 29, it determines if the current date year is a leap year.
   4. If the current date year is a leap year, it uses that year as the base year. If it is not, it uses the previous leap year.
3. If none of the previous tests results in a successful base year determination, the software uses the following procedure to determine the year:
   1. It determines the day of the year of the new event by calculating the number of days from January 1.
   2. If the date information of the previous event is available, and the day of the year of that event is more than the day of the year of the new event plus 4, then it increments the base year.
   3. If the date information of the previous event is not available, and the day of the year of the new event is greater than the current day of the year plus 2, then it decrements the base year.
4. The software then assigns the base year to the timestamp for the event. The timestamp must still pass the time range check for the timestamp to be valid.

**Example 1**

If Splunk software encounters 26 Jun in a new event on May 26, 2017, and it was not able to determine the year in the previous events:

1. Since it was not able to determine the year in the previous event, it sets a base year of 2017 as that is the year of the current date.
2. The December 31 and January 1 tests fail, as the date is neither December 31 nor January 1. The base year remains 2017.
3. The leap year test fails, as the date is not February 29. The base year remains 2017.
4. Splunk software calculates the day of the year for June 26 as Day 177.
5. Since it could not determine the year in the previous event, it adds two to this number to arrive at 179.
6. It then compares 179 to the day of the year of the current date, May 26 (2017) which is Day 147.
7. Since 179 is greater than 147, the software decrements the year from 2017 to 2016.
8. The software then builds the new timestamp: 26 Jun 2016.
9. If the new timestamp falls within the time range that has been set, the software adds the timestamp to the event.

**Example 2**

If Splunk software encounters 10 Apr in a new event on May 26, 2017, and it determined the year 2017 in previous events:

1. Since it determined the year in the previous event, it sets that year as the base year: 2017.
2. The December 31 and January 1 tests fail, as the date is neither December 31 nor January 1. The base year remains 2017.
3. The leap year test fails, as the date is not February 29. The base year remains 2017.
4. Splunk software calculates the day of the year for April 10 as Day 100.
5. Since the year information in the previous event was available, it adds four to this number to arrive at 104.
6. It then compares 104 to the day of the year of the current date, May 26 (2017) which is Day 147.
7. Since 104 is less than 147, the software increments the year from 2017 to 2018.
8. The software then builds the new timestamp: 10 Apr 2018.
9. By default, this new timestamp is not legal, since it falls outside the default MAX_DAYS_HENCE setting which limits valid timestamps to 2 days into the future. The software uses the current date of 26 May 2017 as the timestamp, and applies that timestamp to the event.

**Configure timestamps**

Most events do not require special timestamp handling. Splunk software automatically recognizes and extracts their timestamps. For some sources and distributed deployments, you might need to configure how timestamps are extracted, so that they format properly.

There are two ways to configure timestamp extraction:
• Use the "Set Sourcetype" page in Splunk Web to interactively adjust timestamps on sample data. Once you are happy with the results, save the changes to a new source type and then apply that source type to your data inputs. See The "Set Sourcetypes" page.

• Edit props.conf directly. See Configure timestamp recognition.

You can also configure timestamp extraction to:

• Apply time zone offsets. See Apply time zone offsets.
• Extract the correct timestamp from events with more than one timestamp. See Configure timestamp assignment for events with multiple timestamps.
• Improve indexing performance. See Tune timestamp recognition for better indexing performance.

Considerations when adding data from new inputs

If you index data from a new input and then discover that you need to adjust the timestamp extraction process, you must reindex that data after you make the configuration changes.

Consider previewing your data to prevent the need to reindex. Alternatively, you can test new data inputs in a test Splunk deployment (or in a separate index on the production Splunk instance) before adding data to your production instance. That way, you can delete and reindex until you get the results you want.