Reducing event delay in Splunk Enterprise

An event in Splunk software is a piece of data that comes from a log or other input. Events can be single line or multiline. An ideal time between the time the data is generated by an application and the time the event becomes searchable is three to five seconds. Longer times degrade search performance.

You can run the following search on a single event to test the time between event generation and searchability.

```
| eval event_delay=_indextime - _time
```

To compute event delay at scale, the following search is more useful.

```
| tstats max(_indextime) as indexed_time count WHERE index=* latest=+1day earliest=-1day _index_latest=-1sec _index_earliest=-2sec
BY index host splunk_server _time span=1s
| eval _time=round(_time), delay=indexed_time-_time, delay_str=tostring(delay,"duration")
| eventstats max(delay) AS max_delay max(_time) AS max_time count AS eps BY host index
| where max_delay = delay
| eval max_time=_time
| sort - delay
```

You can also use this event delay dashboard to find key metrics, such as the average delay per index, the number of events received per index, and the maximum delay per index. Clicking into the charts on the dashboard allows you to select an index to drill down on for more detailed information.

Investigate the causes of event delay

The causes of event delay typically fall into one of three main categories. To reduce event delay, investigate the following:

- **Congestion**
  - Rate limiting: Low default processing rates slow transmission, causing true event delay.
  - Network congestion: A saturated network has the same effect as rate limiting and causes true even delay.
  - Index configuration: Excessive ingestion rates, FS IO problems, inefficient regexes and inefficient line breaking can all cause true event delay.

- **Clock skew**
  - Wrong time zones: When time zones aren’t configured correctly, event delay measurement is shifted into the past or future.
  - Clock drift: Use the Network Time Protocol to align all clocks across your deployment.
  - Parsing issue: Automatic source typing assumes the American date format when it is unknown.

- **Timeliness**
  - Scripted inputs: Lengthy polling frequency delays events coming into the indexer for the same amount of time.
Offline components: When forwarders or other components are offline, restarting them causes a delay.

Historical load: Waiting for historical data to load causes fake event delay.

Next steps

The content in this article comes from a Conf19 Talk, one of the thousands of Splunk resources available to help users succeed.