Where do my Splunk® props.conf settings belong?

1. Line Breaking
2. Time Stamping
3. Data Filtering
4. Data Routing
5. Changing meta fields

Extracting Fields

- Are you using TRANSFORMS-*?
  - YES: No further questions
  - NO: Proceed to the next step

- Are you using INDEXED_EXTRACTIONS?
  - YES: Forwarder
  - NO: Proceed to the next step

- Is the data being ingested on a Heavy Forwarder?
  - YES: Heavy Forwarder
  - NO: Proceed to the next step

- Will the data pass through a Heavy Forwarder?
  - YES: Proceed to the next step
  - NO: Proceed to the next step

- Is the data being ingested on a Search Head?
  - YES: Search Head
  - NO: Proceed to the next step

- Are you using JSON?
  - YES: NO
  - NO: Proceed to the next step

- Are you using REPORT-* or EXTRACT-* or KV_MODE?
  - YES: NO
  - NO: Proceed to the next step

- Make sure you set KV_MODE = none for the sourcetype on the search head

Indexer

Sales@aplura.com
https://www.aplura.com

Splunk is a registered trademark of Splunk, Inc.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.