Logsene looks for the following fields in logs and gives them a special treatment:

- host
- source
- facility
- severity
- syslog-tag
- tags
- message
- @timestamp

host is a single-valued field and should contain the ID (typically a hostname) of the device or server sending logs.

source is a single-valued field and should contain the ID or descriptor of where the data is coming from. For example, this could be a file name or even a full path to a filename, or the name of the application or process.

facility is a single-valued field used by syslog to indicate the facility level. Logsene stores the keyword values of these levels (such as *user* or *auth*).

severity ** is a single-valued field and should contain the log level, such as *error* or *info*.

syslog-tag is a single-valued field used by syslog to indicate the name and the PID of the application generating the event (for example, **httpd[215]:**)

tags is a multi-valued array field that can contain zero or more tags. Tags can contain multiple tokens separated by space.

message is a string field that can contain any sort of text (usually the original log line or some other free text)

@timestamp is a date field, on which log retention is based. If it's not present, Logsene will add a timestamp upon event receipt

All of these fields are optional, but their use is strongly encouraged. If found in logs with low-enough cardinality, all distinct values of these fields will be loaded and shown in the UI as filters and thus allowing one to very quickly narrow down the search.