sample

```
[2019-06-13T19:32:13,904][INFO ][o.e.m.j.JvmGcMonitorService] [esnode-2] [gc][9271483] overhead, spent [383ms] collecting in the last [1s]
```

grok pattern

```
\[(?<create_time>([0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}[,][0-9]{3}))\](\s*)+\[(?<loglevel>(\S*\s*))\](\s*)+\S*(?<submessage>(.*))
```

Structured Data

```
{
  "create_time": "2019-06-13T19:32:13,904",
  "submessage": " [esnode-2] [gc][9271483] overhead, spent [383ms] collecting in the last [1s]",
  "loglevel": "INFO "
}
```