



Adding new test cases can easily be done by creating new yaml files in the test directory. Each file specifies a grok pattern to validate, a sample log line, and a list of expected results.

Also, the example Logstash config file adds some informative tags that aid in finding grok failures and unparsed lines. If you're not interested in those, you can remove all occurrences of `add_tag` and `tag_on_failure` from the config file.

## Contributing

---

I only have access to my own log samples, and my setup does not support or use every feature in postfix. If you miss anything, please open a pull request on github. If you're not very well versed in regular expressions, it's also fine to only submit sample unsupported log lines.

## License

---

Everything in this repository is available under the New (3-clause) BSD license.

## Acknowledgement

---

I use postfix, logstash, elasticsearch and kibana in order to get everything working. For writing the grok patterns I depend heavily on [grokdebug](#), and I looked a lot at [antispin's useful logstash grok patterns](#).

