

Logstash grok patterns for postfix logging

A set of grok patterns for parsing postfix logging using grok. Also included is a sample Logstash config file for applying the grok patterns as a filter.

Usage

- Install logstash
- Add 50-filter-postfix.conf to /etc/logstash/conf.d
- Add postfix.grok to /etc/logstash/patterns.d
- Restart logstash

The included Logstash config file requires two input fields to exist in input events:

- program : the name of the program that generated the log line, f.i. postfix/smtpd (named tag in syslog lingo)
- message: the log message payload without additional fields (program, pid, etc), f.i. connect from 1234.static.ctinets.com[45.238.241.123]

This event format is supported by the Logstash syslog input plugin out of the box, but several other plugins produce input that can be adapted fairly easy to produce these fields too. See ALTERNATIVE INPUTS for details.

Tests

build passing

In the test/ directory, there is a test suite that tries to make sure that no previously supported log line will break because of changing common patterns and such. It also returns results a lot faster than doing sudo service logstash restart :-).

The test suite needs the patterns provided by Logstash, you can easily pull these from github by running <code>git submodule</code> update --init . To run the test suite, you also need <code>ruby 2.2</code> or higher, and the <code>jls-grok gem. Then simply execute ruby test/test.rb</code> .

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.

© 2017 GitHub, Inc. Terms Privacy Security Status Help



Contact GitHub API Training Shop Blog About