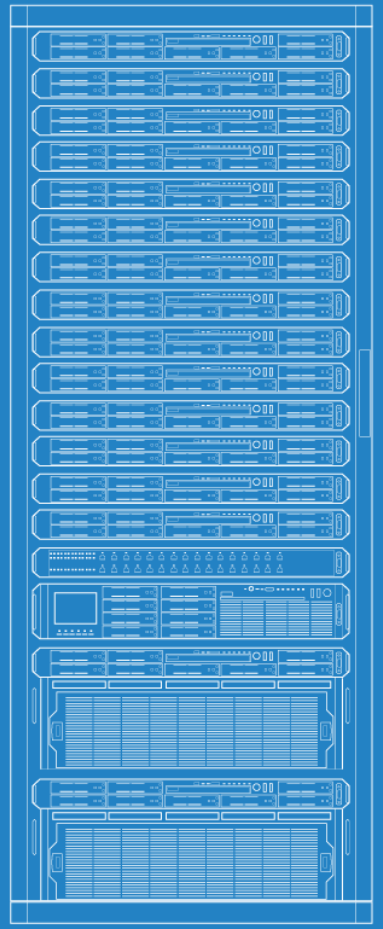
USING SCL TO SIMPLIFY SYSLOG-NG CONFIGURATION



Libre Software Meeting 2017

Peter Czanik / Balabit

BALABIT

SCL

- syslog-ng configuration library
- Reusable configuration blocks
- Hide away complexity of configuration

apache-accesslog-parser()

```
block parser apache-accesslog-parser(prefix(".apache.")) {
    channel {
        parser {
            csv-parser(
                prefix(`prefix`)
                dialect(escape-double-char)
                flags(strip-whitespace)
                delimiters(" ")
                quote-pairs("""[]')
                # field names match of that of Logstash
                columns("clientip", "ident", "auth", "timestamp", "rawrequest", "response", "bytes", "referrer", "agent"));
            csv-parser(
                prefix(`prefix`)
                template("${`prefix`rawrequest}")
                delimiters(" ")
                dialect(escape-none)
                flags(strip-whitespace)
                columns("verb", "request", "httpversion"));
                 date-parser(format("%d/%b/%Y:%H:%M:%S %z")
                        template("${`prefix`timestamp}"));
             };
             rewrite {
                 subst("^HTTP/(.*)$", "$1", value("`prefix`httpversion"));
             };
    };
};
```

Loggly destination

```
block destination loggly(token(TOKEN)
                         tag("tag")
                         host('logs-01.loggly.com')
                         port(514)
                         template("$MSG")) {
    tcp("`host`" port(`port`)
        template("<${PRI}>1 ${ISODATE} ${HOST} ${PROGRAM} ${PID} ${MSGID} [`token`@41058 tag=\"`tag`\"] `template`\n")
template_escape(no)
`__VARARGS__`
    );
};
```

Sending parsed Apache logs to the Cloud

```
source s_apache2 {
  wildcard-file(
    base-dir("/var/log/apache2/")
    recursive(no)
    filename-pattern("*access_log")
    flags(no-parse)
  );
};
parser p_apache2 {
  apache-accesslog-parser(prefix("apache."));
};
destination d_loggly {
  loggly(
    token("TOKEN_FROM_LOGGLY")
    template("$(format-json --scope nv-pairs)")
  );
};
log {
  source(s_apache2);
  parser(p_apache2);
  destination(d_loggly);
};
```

SCL getting started

- /usr/share/syslog-ng/includes/scl (or a similar directory) with the currently available configuration snippets
- an introduction by Bazsi: https://bazsi.blogs.balabit.com/2015/11/the-power-of-scl-integrating-with-loggly/
- documentation: https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html-single/index.html#config-blocks

QUESTIONS?

My blog: http://czanik.blogs.balabit.com/

My e-mail: peter.czanik@balabit.com

Twitter: https://twitter.com/PCzanik