Config File

Logagent can be configured via config files in YAML format. To use the config file run:

```
logagent --config configFileName.yml
```

When logagent is istalled as system service the default config file is located in

```
/etc/sematext/logagent.conf
```

Section: options

```
# Global options
options:
  # print stats every 60 seconds
  printStats: 60
  # don't write parsed logs to stdout
  suppress: false
  # Enable/disable GeoIP lookups
  # Startup of logagent might be slower, when downloading the GeoIP database
  geoipEnabled: false
  # Directory to store Logagent status and temporary files
  diskBufferDir: ./tmp
```

Section: input

```
input:
  # a list of glob patterns to watch files to tail
  files:
      - '/var/log/**/*.log'
      - '/opt/myapp/logs/*.log'
  # listen to udp syslog protocol
  #syslog:
  #  port: 514
  # listen to http to receive data from Heroku  log drains
  #heroku:
  #  port: 9999
  # listen to http to receive data from Cloud Foundry drains
  #cloudFoundry:
  #  port: 8888
```

Section: parser

In this section defines loading of custom pattern files or inline pattern definitions for the log parser.

```
# optional, if not specified default patterns are used
parser:
  patternFiles:
    # load a list of pattern files to parse logs
    # later files overwrite settings from previous files
   # a 'hot reload' is done as soon one of the listed fiels changes on disk
    - patterns1.yml
    - patterns2.yml
  # inline pattern definitions, to put on top of patterns list
 # loaded from files or default librarary. For inline patterns hot reload is not available.
  patterns:
    - # timestamped messages from /var/log/*.log on Mac OS X
    sourceName: !!js/regexp /\system\.log/ # catch all system.log files
      match:
        -
          type: system_log
       regex: !!js/regexp /([\w|\s]+\s+\d{2}\s[\d|\:]+)\s(.+?)\s(.+?)\s<(.+)>(.*)/
          fields: [ts,host,service,severity,message]
          dateFormat: MMM DD HH:mm:ss
```

Section: output

Logs could be shipped to Elasticsearch or to rtail for realtime log view. The Elasticsearch output supports HTTPS, username/password in the url. In addtion it is possible to route logs from different files to different indicies in Elasticsearch. All logs, which don't match the rules in the indices section are routed to the default index (elasticsearch.index).

```
output:
  # index logs in Elasticsearch or Logsene
  logsene:
    module: elasticsearch
   # URL to Elasticearch server, defaults to Logsene SaaS if not set
    url: https://logsene-receiver.sematext.com

    # Proxy settings behind firewalls
    # httpProxy:  http://localProxy:port
    # httpsProxy: https://localHttpsProxy:port

   # default index to use, for all logs that don't match later in indices section
    # for Logsene use the Logsene App Token here
    index: 0a835c75-9847-4f74-xxxx

    # specific index to use per logSource field of parsed logs
    # logSource is by default the file name of the log file
    # but it can be modified by JS transforms functions in the patterns.yml file
    indices:
      4f70a0c7-9458-43e2-bbc5-xxxx:
      # list of RegEx mathich logSource / filename
    # all logs matching logSource name will be indexed to above index
        - .*wifi.*
        - .*bluetooth.*
      999532c9-18f1-4c4b-8753-xxxx:
        - system\.log
        - access\.log
        - auth\.log
  # print parsed logs in YAML format to stdout (only if options.supress is set to false)
  stdout: yaml # use 'pretty' for pretty json and 'ldjson' for line delimited json (default)

  # forward logs to rtail realtime log viewer
  #rtail:
    # rtail host to send logs to
    #host: localhost
    # rtails port to send logs to
    #udpPort: 3434
    # start rtail Server with given http port and bind to address of hostname
    #webPort: 8080
    #webHost: localhost
```

A collection of example config files are here