Title: Sematext Logagent Log Shipper Description: Logagent is lightweight log shipper, filebeat, fluentd or rsyslog alternative with out of the box and extensible log parsing, on-disk buffering, secure transport, bulk indexing to Elasticsearch, Kafka, and Sematext

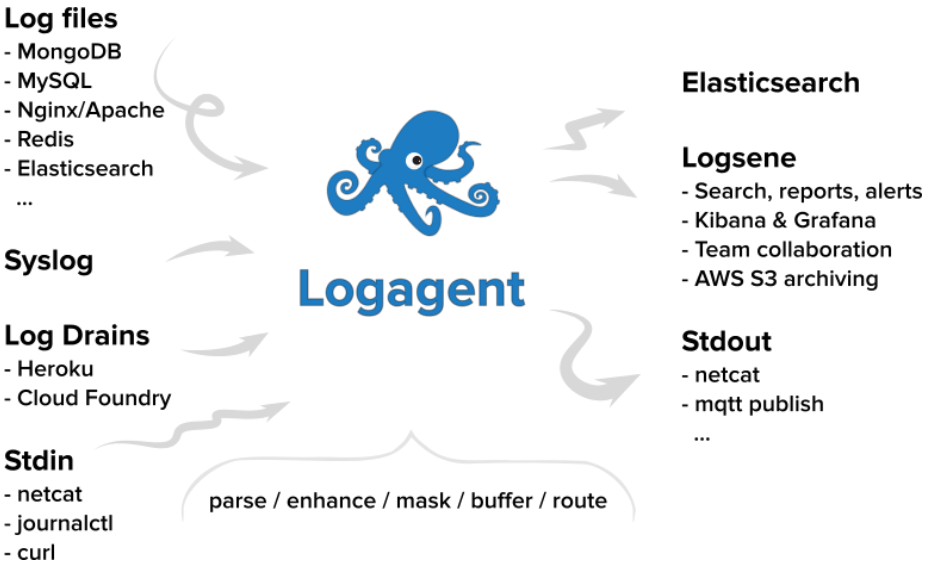

Figure 1: Logagent Logo

What is Logagent?

Logagent is a modern, open-source, lightweight **log shipper** with a low memory footprint and low CPU overhead!

It comes with out of the box and extensible **log parsing**, **on-disk buffering**, **secure transport**, and **log shipping** with **bulk indexing** to any **Elasticsearch endpoint**, including Sematext Logs, Kafka, etc.

If you're eager to get started, here's how you start shipping logs.

```
# Make sure you have Node.js installed
curl -sL https://deb.nodesource.com/setup_12.x | sudo -E bash -
sudo apt-get install -y nodejs

# Install Logagent and run it as a system service
sudo npm i -g @sematext/logagent
sudo logagent-setup -i <LOGS_TOKEN or ES_INDEX>
```

To read more jump to Installation right away.

Features

Logagent contains an installer when you want to use it as a log shipper. Configuration is done via a simple `YAML` configuration file. It has a library that supports **patterns for log parsing**, and it can also be used as a **command line tool**.

- Install Logagent with:
  - Linux Systemd
  - Linux Upstart
  - Windows service
  - Mac OS X Launchd service
  - Docker
  - Docker Swarm
  - Kubernetes
- **Log shipping** with a disk buffer ensures no loss of data
- A simple **YAML configuration file**
- Built-in **data parser** with configurable **patterns**
- **Command-line tool**
- Plugins:
  - Inputs (files, streams, sockets, databases)
  - Input filters (grep/grok filters)
  - Outputs (Elasticsearch, Sematext Cloud, Kafka, etc.)
  - Output filters (SQL aggregation of parsed data, enrichment of data)
- Node.js API

Installation Options

- Install as a system service
- Run as a Docker Container
- Deploy to Heroku as Heroku Log drain
- Deployment to Cloud Foundry as Cloud Foundry Log drain (thus usable with Pivotal, IBM Bluemix, etc.)

Configuration

After installing Logagent, run `logagent-setup` to create a system service and start shipping logs right away. This will also create a simple `YAML` configuration file for you in `/etc/sematext/logagent.conf`.

“‘yaml hl_lines=“18 19 24 25 27 29 30 35” # /etc/sematext/logagent.conf

Global options

options: # print stats every 60 seconds printStats: 60 # don’t write parsed logs to stdout suppress: true # 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 # this is equals to LOGS_TMP_DIR env variable diskBufferDir: /tmp/sematext-logagent

input: # a list of glob patterns to watch files to tail files: - '/var/log/**/*.log'

output: # index logs in Elasticsearch or Sematext Logs sematext: # output a name, e.g., elasticsearch, sematext, etc. module: elasticsearch url: https://logsene-receiver.sematext.com # default Elasticsearch index or Sematext Logs token to use index: # indices for shipping logs to multiple locations indices: : # list of log sources or filenames - syslog.log - access.log - auth.log : # list of RegEx matching a log source or filename - *.wifi.* - *.bluetooth.* "'

Command-line Tool

Logagent can also be **used as a command-line tool**. To use Logagent only as a command-line tool running `logagent-setup` and using the default configuration file is not needed.

- Works with **Unix pipes**, **stdin**, and **stdout**

- **Log parser** and format converter
  - text to JSON
  - line delimited JSON or YAML

    ```
    cat access.log | logagent --yaml
    ```

- **Import files** into Elasticsearch

  ```
  cat access.log | logagent -n nginx -e http://localhost:9200 -i logs
  ```

- **Watch multiple log files** in the terminal

  ```
  logagent -yaml -g '/var/log/**/*.log'
  ```

- **Store logs** in Elasticsearch

  ```
  logagent -e http://localhost:9200 -i logs
  ```

Built-in Log Parser

You can configure custom data patterns for parsing logs.

- Log format detection and intelligent pattern matching
- The pattern library includes a set of popular log formats for databases, web servers, message queues, etc.
- Easy to extend with custom patterns and Javascript transform functions
- Hot reload of changed pattern definitions without service restart
- Auto-detection of date and numeric fields
- Masking of sensitive data with configurable hashing algorithms (SHA-1, SHA-256, SHA-512, …)

- GeoIP lookup with automatic GeoIP DB updates (Maxmind GeoIP-Lite files)

Plugins

A comprehensive collection of plugins for data input, processing, and output are available. See the complete list of Logagent Plugins.

API

Logagent is an npm package and can add log parsing to Node.js applications.

Related Packages

- Logsene-CLI - Enables searching logs in Sematext Logs from the command-line
- Winston-Logsene - Logging for Node.js - Winston transport layer for Sematext Logs