

## What is Logagent

Logagent is a modern, open-source, light-weight log shipper. It is like Filebeat and Logstash in one, without the JVM memory footprint. It comes with out of the box and extensible log parsing, on-disk buffering, secure transport, and bulk indexing to Elasticsearch, Logsene, and other destinations. Its low memory footprint and low CPU overhead makes it suitable for deploying on edge nodes and devices, while its ability to parse and structure logs makes it a great Logstash alternative.

## Features

This project contains a library and patterns for log parsing, a command line tool and installer to use Logagent as log shipper with the following features:

- Built-in data parser with configurable patterns
- Command line tool
- Plugins
- Inputs (files, streams, sockets, databases)
- Input filters (e.g. grep filter)
- Outputs (Elasticsearch, Sematext Cloud, Kafka, ...)
- Output filters (SQL aggregation of parsed data, enrichment of data)
- Reliable log shipping with disk buffer
- Various deployment options (Systemd, Upstart, Windows service, Mac OS X Launchd service, Docker)
- Node.js API

### Built-in data parser

- Log format detection and intelligent pattern matching
- Pattern library included covering a set of common databases, web servers, message queues, etc.
- Easy to extend with custom patterns and JS 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)

### Command-line tool

Logagent can also be used as a command-line tool.

- Works with Unix pipes (stdin/stdout)

- Log parser and format converter (e.g. 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 and watch them in real-time in the Web browser `logagent -e http://localhost:9200 -i logs --rtailWebPort 8080 --rtailPort 9999 /var/log/*.*log`

## Plugins

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

## Reliable log shipping with disk buffer

Logagent doesn't lose data. It stores parsed logs to a disk buffer if the network connection to the Elasticsearch API fails. Logagent retries shipping logs later, when the network or Elasticsearch is available again.

## Deployment options

- Deployable as a system service: Systemd, Upstart (Linux), or Launchd (Mac OS X)
- Docker Container
- Deployment to Heroku as Heroku Log drain
- Deployment to Cloud Foundry as Cloud Foundry Log drain (thus usable with Pivotal, IBM Bluemix, etc.)

## API

- Node.js module to integrate parsers into Node.js programs
- logagent-js is a part of Sematext Docker Agent for parse container logs

## Related packages

- Sematext Agent for Docker - collects metrics, events and logs from Docker API and CoreOS. Logagent-js is a component of sematext-agent-docker. More Information: Innovative Docker Log Management
- Logsene-CLI - Enables searching Logsene log entries from the command-line.
- SPM Agent for Node.js - collects performance metrics for Node applications

- Custom Metrics - Custom Metrics for SPM
- Winston-Logsen - Logging for Node.js - Winston transport layer for Logsen