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: - Build-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 service, Docker) - Node.js API

Build-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
- Replacement 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

The architecture of Logagent is modular and each input or output module is implemented as a plugin for the Logagent framework. Plugins are loaded on demand depending on the configuration.

Plugin	Type	Description
stdin (default)	input	Reads from standard input
files	input	Watching and tailing files
logagent-input-windows-events	input	Collect Windows Events. Available as separate npm package
logagent-input-elasticsearch-stas	input	Monitoring of Elasticsearch metrics. Available as separate npm package
syslog	input	Receive Syslog messages via UDP
input-tcp	input	Receive data via TCP
heroku	input	Receive logs from Heroku log drains (HTTP)
cloudfoundry	input	Receive logs from Cloud Foundry log drains (HTTP)
command	input	Receive logs from the output of a command, which could run once or periodically
mysql-query	input	Receive results from SQL queries, which could run once or periodically
mssql-query	input	Receive results from SQL queries, which could run once or periodically
postgresql-query	input	Receive results from SQL queries, which could run once or periodically
elasticsearch-query	input	Receive results from Elasticsearch queries, which could run once or periodically

Plugin	Type	Description
input-kafka	input	Receiver messages from Apache Kafka topics
grep	Processor / input filter	Filters text with regular expressions before parsing
sql	Processor / output filter	Transforms and aggregates parsed messages with SQL statements
access-watch	Processor / output filter	Enriches web server logs with robot detection and traffic intelligence
stdout (default)	output	Prints parsed messages to standard output. Supported formats: YAML, JSON, Line delimited JSON (default).
elasticsearch	output	Stores parsed messages in Elasticsearch
rtail	output	Sends parsed messages to rtail servers for real-time view of logs in a web browser
output-kafka	output	Sends parsed messages to Apache Kafka topics
slack-webhook	output	Sends parsed messages to Slack chat. Should be combined with SQL filter plugin or filter function to define alert criterias.
[@sematext/logagent-nodejs-monitor](https://www.npmjs.com/package/@sematext/logagent-nodejs-monitor)	output	Monitors server and nodejs metrics of the Logagent process using spm-agent-nodejs

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 and io.js applications
- Custom Metrics - Custom Metrics for SPM
- Winston-Logsene - Logging for Node.js - Winston transport layer for Logsene