title: Ingest data in Elasticsearch description: Forwards parsed logs with Elasticsearch output plugin for Logagent, light-weight 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 and Sematext logs management platform

Elasticsearch Output Plugin

The Elasticsearch output plugin forwards parsed logs to Elasticsearch or Sematext Logs.

Features

- log routing by log source to multiple Elasticsearch servers
- log routing by log source to multiple Elasticearch indices (or Sematext Logs Apps)
- SSL/TLS by default, when using Sematext
- Two-way SSL Authentication, also known as Mutual Authentication as part of PKI, secure client authentication with SSL client certificates
- bulk indexing with timeout (1000 docs or 10 second timeout by default)
- disk buffer an re-transmit when connection to Elasticsearch fails
- renaming of invalid field names
- limit field size (240k by default)

Simple config

The following example configuration ships all log files in /var/log (including sub-directories) to one Elasticsearch index.

```
input:
  files:
      - '/var/log/**/*.log'
output:
  my-logs-app:
    module: elasticsearch
    url: https://logsene-receiver.sematext.com
    index: bb308f80-0453-485e-894c-f80c054a0f10
```

Log routing to multiple targets

In some situations, it is required to ship data from different sources to different Elasticsearch servers or clusters. The output section in the Logagent configuration file accepts multiple definitions for the Elasticsearch output module.

Each Elasticsearch output might have a list of indices followed by a list of regular expressions matching the log source (e.g. file name of the log file).

The following example ships logs from wireless devices and authentication log to a local Elasticsearch server and other server logs to multiple Sematext Logs Apps.

```
input:
  files:
      - '/var/log/**/*.log'

output:
  # index logs in Elasticsearch or Sematext
  local-elasticsearch:
    module: elasticsearch
    url: http://localhost:9200
    # default index to use, for all logs that don't match any other configuration
    index: other_logs
    # specific indices to use per logSource field of parsed logs
    indices:
      wireless_logs: # use regex to match log source e.g. /var/log/wifi.log
        - wifi|bluetooth
      security_logs:
        - auth\.log
   sematext:
        module: elasticsearch
        url: https://logsene-receiver.sematext.com
        indices:
          bb308f80-0453-485e-894c-f80c054a0f10:
              - [nginx|httpd]\.log
          a0ca5032-62da-467d-b6d5-e465a7ce45bb
              - mysql|postgres|oracle
          969020b4-f11c-41dd-86e4-24e67759cdb3
              - mongo.*\.log
              - myapp1\/app.log
              - myapp2\/app.log
```

HTTP, HTTPS and authentication options

The Elasticsearch output module accepts http(s) options. Client side certificates and keys are specified with a file name. If you use self-signed certificates, set *rejectUnauthorized* to *false*.

```
output:
  secure-elasticsearch:
    module: elasticsearch
    url: "https://user:password@localhost"  # password characters will have to be urlencode
    index: logs
    httpOptions:
      key: /ssl-keys/client.key
```

```
cert: /ssl-keys/client.crt
ca: /ssl-keys/ca.pem
rejectUnauthorized: true
```