Elasticsearch and Kibana

Elasticsearch requires at least Java 8, please check your Java version first by running (and then install/upgrade accordingly if needed):

```
java -version
```

Install Java with brew, to verify which version it will install.

```
brew cask info java
```

Install java

```
brew cask install java
```

Or you can install Java from the homepage
https://www.java.com/en/download/help/download_options.xml

Download and unzip Elasticsearch.

Run

```
bin/elasticsearch
```

in console from the elasticsearch folder.

Download and unzip Kibana.

Open kibana.yml (kibana/config) in an editor and set `elasticsearch.url` (line 28) to point at your Elasticsearch instance.

Run

```
bin/kibana
```

in console from the kibana folder.

Open Kibana on http://localhost:5601.

Add `gem 'logstasher'` to the Gemfile =>

```
bundle install
```

Add to the development.rb and production.rb (or evironment.rb) code below:

```
# Enable the logstasher logs for the current environment
config.logstasher.enabled = true

# Each of the following lines are optional. If you want to selectively disable log
subscribers.
config.logstasher.controller_enabled = true
config.logstasher.mailer_enabled = false
config.logstasher.record_enabled = false
config.logstasher.view_enabled = false
config.logstasher.job_enabled = false

# This line is optional if you do not want to suppress app logs in your
<environment>.log
config.logstasher.suppress_app_log = false

# This line is optional, it allows you to set a custom value for the @source field
of the log event
# config.logstasher.source = 'your.arbitrary.source'

# This line is optional if you do not want to log the backtrace of exceptions
config.logstasher.backtrace = true

# This line is optional, defaults to log/logstasher_<environment>.log
config.logstasher.logger_path = 'log/logstasher.log'

# This line is optional, loaded only if the value is truthy
# config.logstasher.field_renaming = {
#     old_field_name => new_field_name,
# }
```

We use this gem to convert the logs in json objects!

To import the .log in elasticsearch, we must add the index before each log.

Create logstasher.rb in the initializer folder and add code below:

```
if LogStasher.enabled?


  LogStasher::ActiveSupport::LogSubscriber.class_eval do

    alias :original_process_action :process_action

    def process_action(event)
      hash = {index: {_id: event.payload[:request_id]}}
      hash[:log] = event
      logs_for_elastic = Logger.new("#{Rails.root}/log/logstasher.log")
      logs_for_elastic.info(hash.to_json)
    end
```

```
  end

end
```

Change to the folder where the log file is located and type code below:

```
curl -H 'Content-Type: application/x-ndjson' -XPOST
'localhost:9200/log/logs/_bulk?pretty' --data-binary @logstasher.log
```

To check if the index is created:

In the Kibana interface Management => Elasticsearch => Index Management should be the created index `log`.

In Dev Tools => Console add the code `GET /log/logs/_search` and run it with the green arrow

Here are a few different query examples

- Match if the field excption exists:

```
GET /log/_search
{
    "query": {
        "exists" : { "field" : "log.payload.exception" }
    }
}
```

- Match if status: 302

```
GET log/logs/_search
{
  "query": {"match": {
    "log.payload.status": "302"
  }}
}
```

- Shows count of all action keywords

```
GET log/logs/_search
{
  "size": 0,
  "aggs": {
    "status": {
      "terms": {
        "field": "log.payload.params.action.keyword"
      }
    }
  }
}
```

- Match all existing fields in time range

```
GET log/logs/_search
{
  "query": {
    "bool": {
      "must":
        {"exists": {"field": "log.payload.exception"}

        },
        "filter": {
          "range": {
            "log.time": {
              "gte": "2018-11-27T09:48:54-07:00",
              "lte": "2018-11-27T09:50:55-07:00"
            }
          }
        }

    }
  }
}
```