SQL output filter

Filter and aggregate parsed logs with SQL.

This filter applies SQL queries on parsed log events. The result of the query is emitted as a new event, while the original events are omitted.

Using SQL it is very easy to aggregate values, e.g. group HTTP requests by status codes. The SQL WHERE statement is used to filter events before they get shipped to Elasticsearch or Logsene.

Configuration

Add the following section 'outputFilter' to the Logagent configuration file. Please note you could use the plugin with multiple configurations for different event sources.

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

outputFilter:
  - module: sql
    config:
      source: !!js/regexp /access.log|httpd/
      interval: 1 # every second
      queries:
        - # calculate average page size for different HTTP methods
          SELECT 'apache_stats' AS _type,
                  AVG(size) AS size_avg,
                  COUNT(method) AS method_count,
                  method as http_method
          FROM ?
          GROUP BY method
        - # log each request to the login page
          SELECT *
          FROM ?
          WHERE path like "/wp-login%"
output:
  elasticsearch:
    module: elasticsearch
    url: http://localhost:9200
    index: mylogs
```

Run Logagent with your config:

```
logagent --config logagent-example-config.yml
```