Plugin: Elasticsearch query

Plugin to receive documents from scheduled Elasticsearch queries. Use cases:

- Alerting. Logagent can report the results of any Elasticsearch query to supported output modules (e.g. Slack channels).

- Re-indexing and transforming documents
- Replicating data to other Elasticsearch clusters
- Storing results of aggregation queries in a new index

Configuration

```
input:
  queryLogs:
    module: elasticsearch-query
    sourceName: errorQuery
    # repeat query every N seconds
    interval: 60
    # tracing settings for elasticsearch-client
    log: 'error'
    url: https://localhost:9200
    query:
      size: 50
      index: logstash-YYYY-MM-DD
      body:
        query:
          bool:
            must:
              - query_string:
                  query: 'status:>399'
            filter:
              - range:
                  '@timestamp':
                    gte: now-1m/m
                    lte: now/m

output:
    stdout: yaml
```

Start Logagent

```
logagent --config myconfig.yml
```