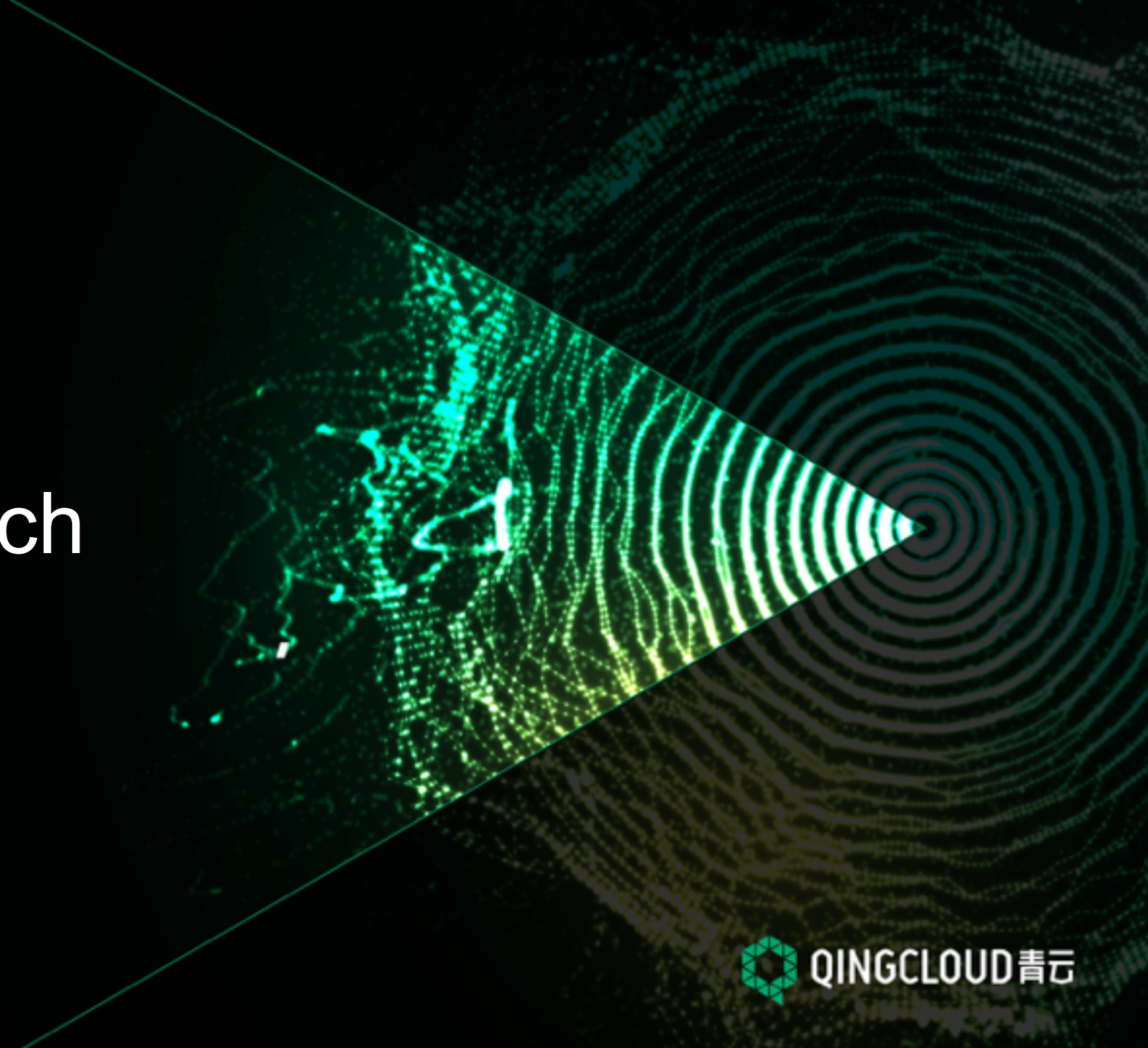
QING CLOUD INSIGHT 2016 科技.洞见未来

2016. 7. 28 北京国际饭店

Elasticsearch

王渊命 @jolestar



QINGCLOUD青云

目录

- Elasticsearch简介
- Elasticsearch核心概念及架构
- Elasticsearch集群搭建与配置
- Elasticsearch集群演示
- Elasticsearch全文检索
- Elasticsearch文档数据库
- Elasticsearch分析引擎
- ELK 使用场景演示

Elasticsearch简介

Elasticsearch is a distributed, open source search and analytics engine, designed for horizontal scalability, reliability, and easy management. It combines the speed of search with the power of analytics via a sophisticated, developer-friendly query language covering structured, unstructured, and time-series data.

Elasticsearch简介-使用场景

- 站内搜索（全文索引）
- 文档数据库（vs mongodb）
- 日志以及时间序列数据（ELK）

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch核心概念

- 集群（Cluster）
- 节点（Node)
- 索引（Index)
- 主分片（Primary shard）
- 副本分片（Replica shard）
- 类型（Type）
- Mapping
- 文档（Document)
- 字段（Field）
- 分配（Allocation）

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch架构-分布式

- 状态共享
  - 服务发现
  - 选主
- 弹性（Elastic）
  - 新增节点
  - 删除节点

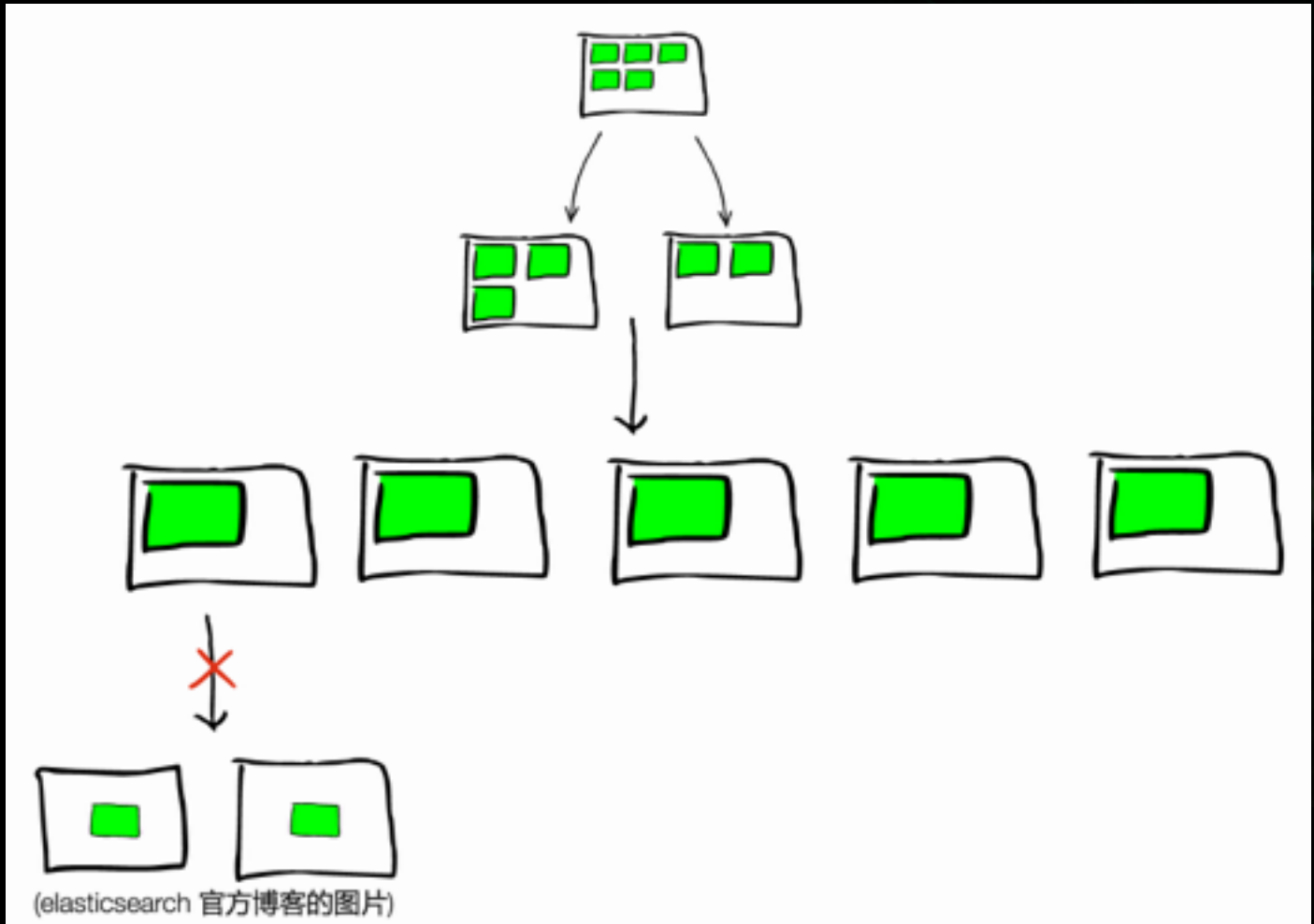
QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch架构-服务发现以及选主

- 节点启动后先ping（这里的ping是 Elasticsearch 的一个RPC命令。）
- Ping的response会包含该节点的基本信息以及该节点认为的master节点。
- 选举开始，先从各节点认为的master中选，规则很简单，按照id的字典序排序，取第一个。
- 如果各节点都没有认为的master，则从所有节点中选择，规则同上。这里有个限制条件就是discovery.zen.minimum_master_nodes，如果节点数达不到最小值的限制，则循环上述过程，直到节点数足够可以开始选举
- 最后选举结果是肯定能选举出一个master，如果只有一个local节点那就选出的是自己。
- 如果当前节点是master，则开始等待节点数达到 minimum_master_nodes，然后提供服务。
- 如果当前节点不是master，则尝试加入master。

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch架构-分片以及副本



QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch架构-恢复与容灾

- 集群中的某个节点丢失网络连接
- master提升该节点上的所有主分片的在其他节点上的副本为主分片
- cluster集群状态变为 yellow ,因为副本数不够
- 等待一个超时设置的时间，如果丢失节点回来就可以立即恢复（默认为1分钟，通过 index.unassigned.node_left.delayed_timeout 设置）。如果该分片已经有写入，则通过 translog进行增量同步数据。
- 否则将副本分配给其他节点，开始同步数据。

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch架构-系统架构

- Guice
- Netty
- Lucene
- ClusterState

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch集群搭建

- java
- 下载 https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/tar/elasticsearch/2.3.5/elasticsearch-2.3.5.tar.gz
- bin/elasticsearch
- config/elasitcsearch.yaml

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch集群搭建-config

```
bootstrap.mlockall: true
cluster.name: elasticsearch
discovery.zen.minimum_master_nodes: 2
discovery.zen.ping.timeout: 5s
discovery.zen.ping.unicast.hosts:
["192.168.229.11", "192.168.229.5"]
gateway.recover_after_nodes: 2
http.port: 9200
network.host: 0.0.0.0
node.name: node-1
path.data: /data/elasticsearch/data
path.logs: /data/elasticsearch/logs
```

```
script.file: false
script.indexed: sandbox
script.inline: sandbox
script.mapping: false
script.update: false
http.cors.enabled: true
http.cors.allow-origin: "*"
index.number_of_shards: 1
index.number_of_replicas: 0
```

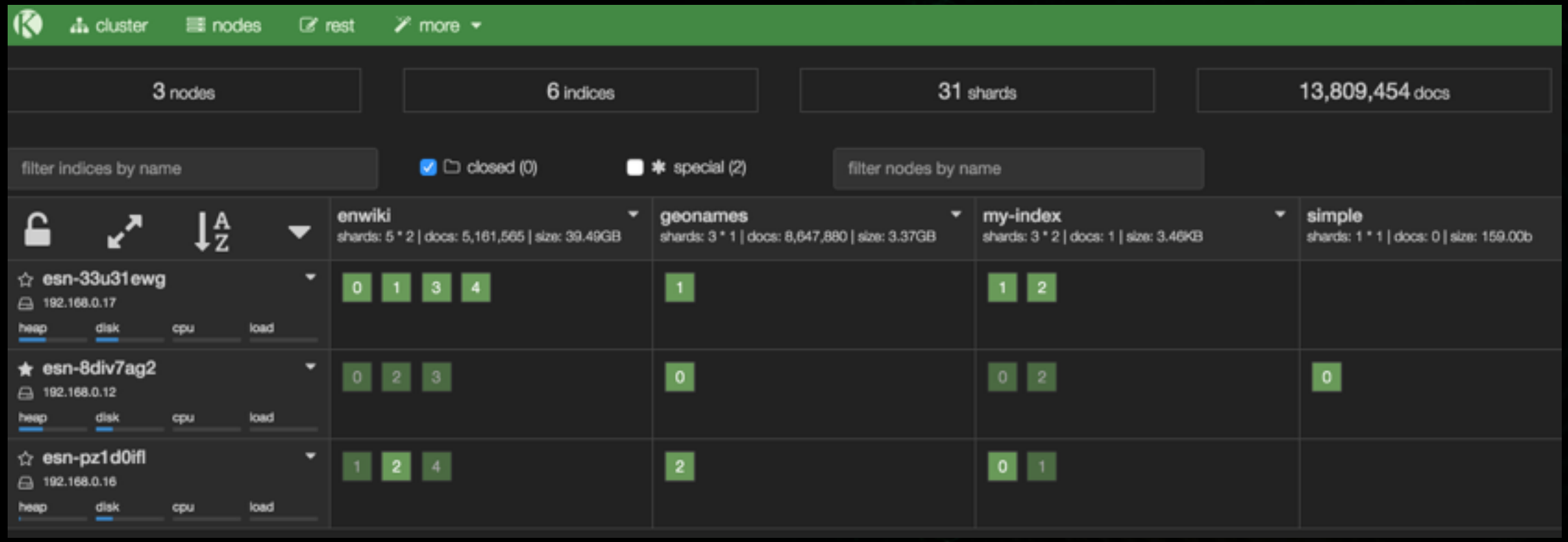
QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch集群搭建-docker

- docker pull elasticsearch:2.3.5
- docker run --name elasticsearch -p 9200:9200 -p 9300:9300 -d elasticsearch:2.3.5 elasticsearch

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch集群演示



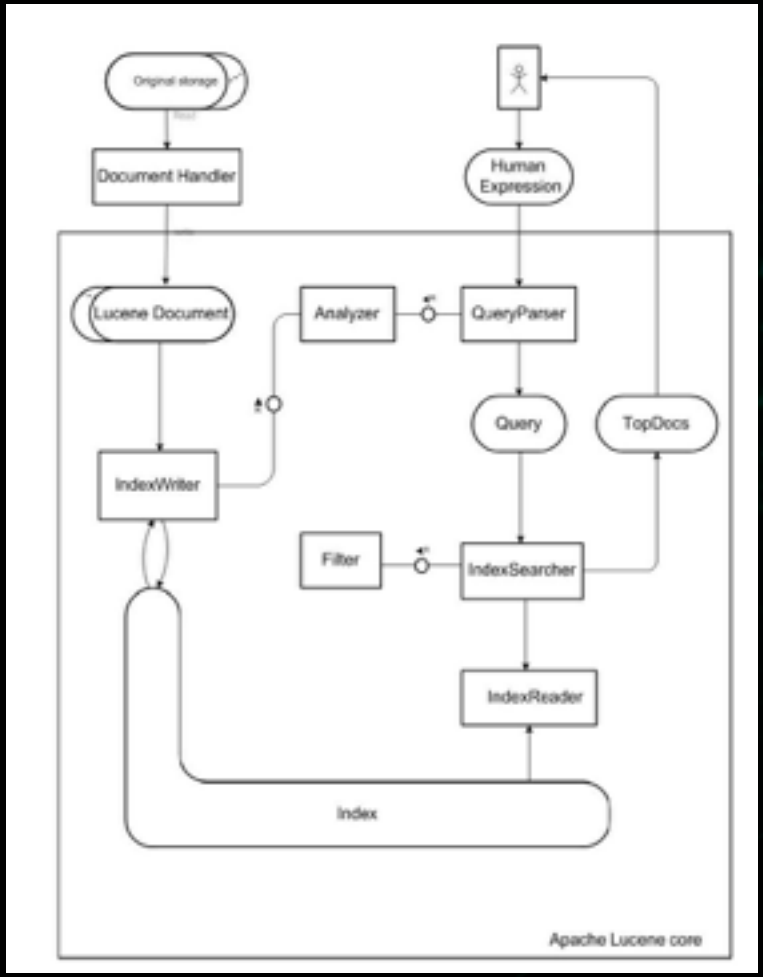
QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch全文检索

- Lucene
- Mapper-attachments
- Analyzer

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch全文检索-lucene



http://www.slideshare.net/gamgoster/architecture-and-implementation-of-apache-lucene-13105167

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch全文检索-lucene

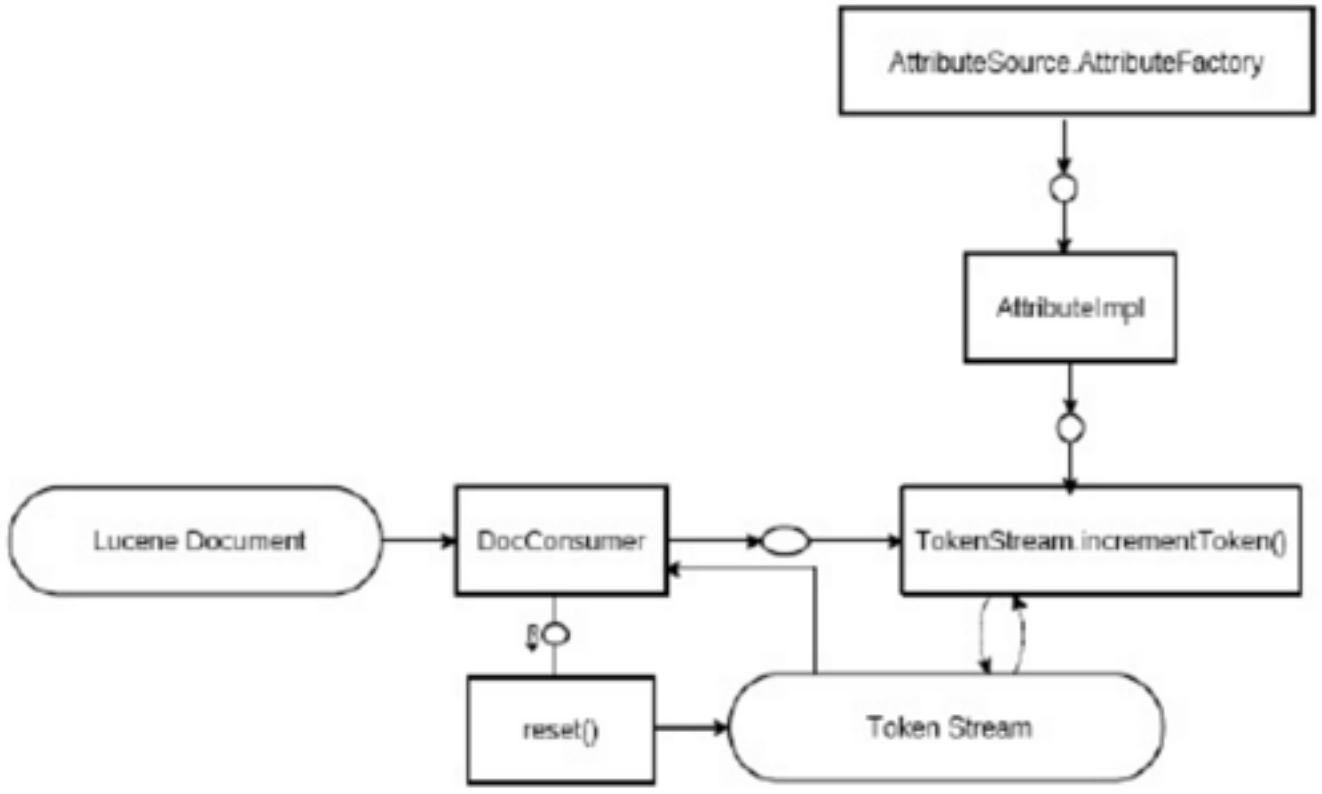


Figure 14: The tokenization process(FMC Notation)

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch全文检索-lucene

Segment

term ordinal	terms dict	postings list
0	data	0,1
1	index	0,1
2	Lucene	0
3	term	0
4	sql	1

doc id	document
0	Lucene in action
1	Databases

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库

- Lucene store field
- Translog
- Dynamic-mapping 以及 schema-free
- QueryDSL

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库-mapping

```
PUT my_index
{
  "mappings": {
    "user": {
      "_all":       { "enabled": false  },
      "properties": {
        "title":    { "type": "string"  },
        "name":     { "type": "string"  },
        "age":      { "type": "integer" }
      }
    },
    "blogpost": {
      "properties": {
        "title":    { "type": "string"  },
        "body":     { "type": "string"  },
        "user_id":  {
          "type":   "string",
          "index":  "not_analyzed"
        },
        "created":  {
          "type":   "date",
          "format": "strict_date_optional_time||epoch_millis"
        }
}}}}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库-datatype

Core datatypes

String datatype

`string`

Numeric datatypes

`long`, `integer`, `short`, `byte`, `double`, `float`

Date datatype

`date`

Boolean datatype

`boolean`

Binary datatype

`binary`

Complex datatypes

Array datatype

Array support does not require a dedicated `type`

Object datatype

`object` for single JSON objects

Nested datatype

`nested` for arrays of JSON objects

Geo datatypes

Geo-point datatype

`geo_point` for lat/lon points

Geo-Shape datatype

`geo_shape` for complex shapes like polygons

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库-QueryDSL

```
SELECT document
FROM   products
WHERE  price = 20
```

```
{
    "term" : {
        "price" : 20
    }
}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库-QueryDSL

```
SELECT product
FROM   products
WHERE  (price = 20 OR productID = "XHDK-A-1293-#fJ3")
  AND  (price != 30)
```

```
{
   "bool" : {
      "must" :     [],
      "should" :   [],
      "must_not" : [],
      "filter":    []
   }
}
```

```
{
            "bool" : {
              "should" : [
                { "term" : {"price" : 20}},
                { "term" : {"productID" : "XHDK-
A-1293-#fJ3"}}
              ],
              "must_not" : {
                "term" : {"price" : 30}
              }
            }
}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch文档数据库-QueryDSL

```
SELECT document
FROM   products
WHERE  price BETWEEN 20 AND 40
```

```
"range" : {
    "price" : {
        "gt" : 20,
        "lt" : 40
    }
}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch分析引擎

- Aggregations
- Kibana

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch分析引擎-Aggregations

- Bucketing
- Metric
- Pipeline

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch分析引擎-Aggregations

```
"aggs" : {
    "<aggregation_name>" : {
        "<aggregation_type>" : {
            <aggregation_body>
        }
        [,"meta" : {  [<meta_data_body>] } ]?
        [,"aggregations" : { [<sub_aggregation>]+ } ]?
    }
    [,"<aggregation_name_2>" : { ... } ]*
}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

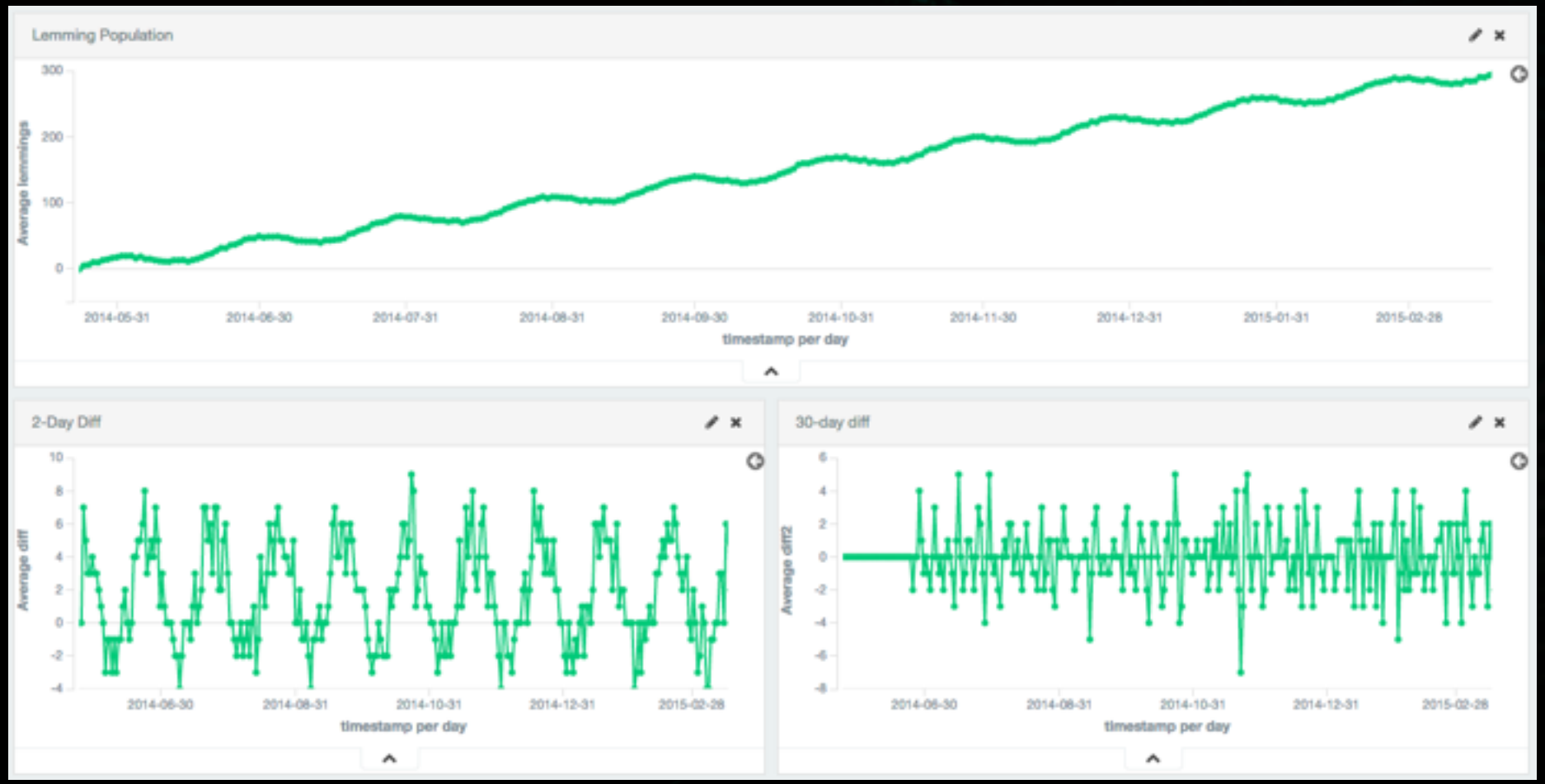
Elasticsearch分析引擎-Aggregations

```
{
    "aggs" : {
        "avg_grade" : { "avg" : { "field" : "grade" } }
    }
}
```

```
{
    "aggs" : {
        "articles_over_time" : {
            "date_histogram" : {
                "field" : "date",
                "interval" : "month"
            }
        }
    }
}
```

QING CLOUD INSIGHT 2016 科技,洞见未来

Elasticsearch分析引擎-Serial Differencing Aggregation



QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch分析引擎-Aggregations

```
{
  "aggs": {
    "my_date_histo": {
      "date_histogram": {
        "field": "timestamp",
        "interval": "day"
      },
      "aggs": {
        "the_sum": {
          "sum": {
            "field": "lemmings"
          }
        },
        "thirtieth_difference": {
          "serial_diff": {
            "buckets_path": "the_sum",
            "lag" : 30
          }
}}}}}
```

QING CLOUD INSIGHT 2016 科技.洞见未来

Elasticsearch分析引擎-Aggregations

Pipeline Aggregations

- Avg Bucket Aggregation
- Derivative Aggregation
- Max Bucket Aggregation
- Min Bucket Aggregation
- Sum Bucket Aggregation
- Stats Bucket Aggregation
- Extended Stats Bucket Aggregation
- Percentiles Bucket Aggregation
- Moving Average Aggregation
- Cumulative Sum Aggregation
- Bucket Script Aggregation
- Bucket Selector Aggregation
- Serial Differencing Aggregation

Bucket Aggregations

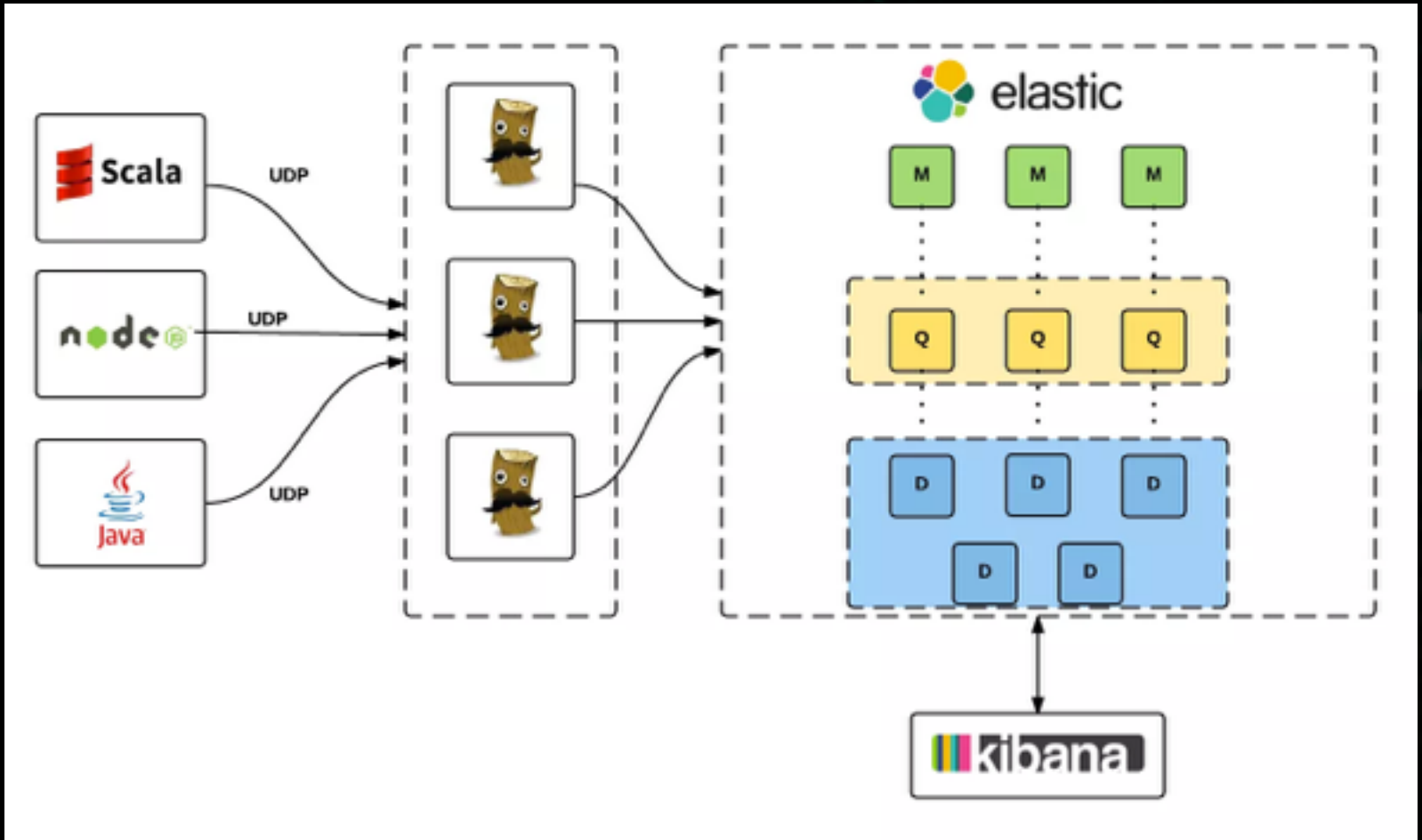
- Children Aggregation
- Date Histogram Aggregation
- Date Range Aggregation
- Filter Aggregation
- Filters Aggregation
- Geo Distance Aggregation
- GeoHash grid Aggregation
- Global Aggregation
- Histogram Aggregation
- IPv4 Range Aggregation
- Missing Aggregation
- Nested Aggregation
- Range Aggregation
- Reverse nested Aggregation
- Sampler Aggregation
- Significant Terms Aggregation
- Terms Aggregation

Metrics Aggregations

- Avg Aggregation
- Cardinality Aggregation
- Extended Stats Aggregation
- Geo Bounds Aggregation
- Geo Centroid Aggregation
- Max Aggregation
- Min Aggregation
- Percentiles Aggregation
- Percentile Ranks Aggregation
- Scripted Metric Aggregation
- Stats Aggregation
- Sum Aggregation
- Top hits Aggregation
- Value Count Aggregation

QING CLOUD INSIGHT 2016 科技.洞见未来

ELK演示



QING CLOUD INSIGHT 2016 科技.洞见未来

午夜咖啡

工具 · 架构 · 成长 · 思考

公众号：jolestar-blog
个人博客：http://jolestar.com

微信扫描关注 午夜咖啡

QING CLOUD INSIGHT 2016 科技.洞见未来

Thank you.

@jolestar