Hangout

一个LOGSTASH INDEXER的替代方案

刘佳@携程

CONTENTS

1.为何开发hangout

2.与logsatsh性能对比

3.支持的input/filter/output

4.设计架构变迁

5. 参数调优

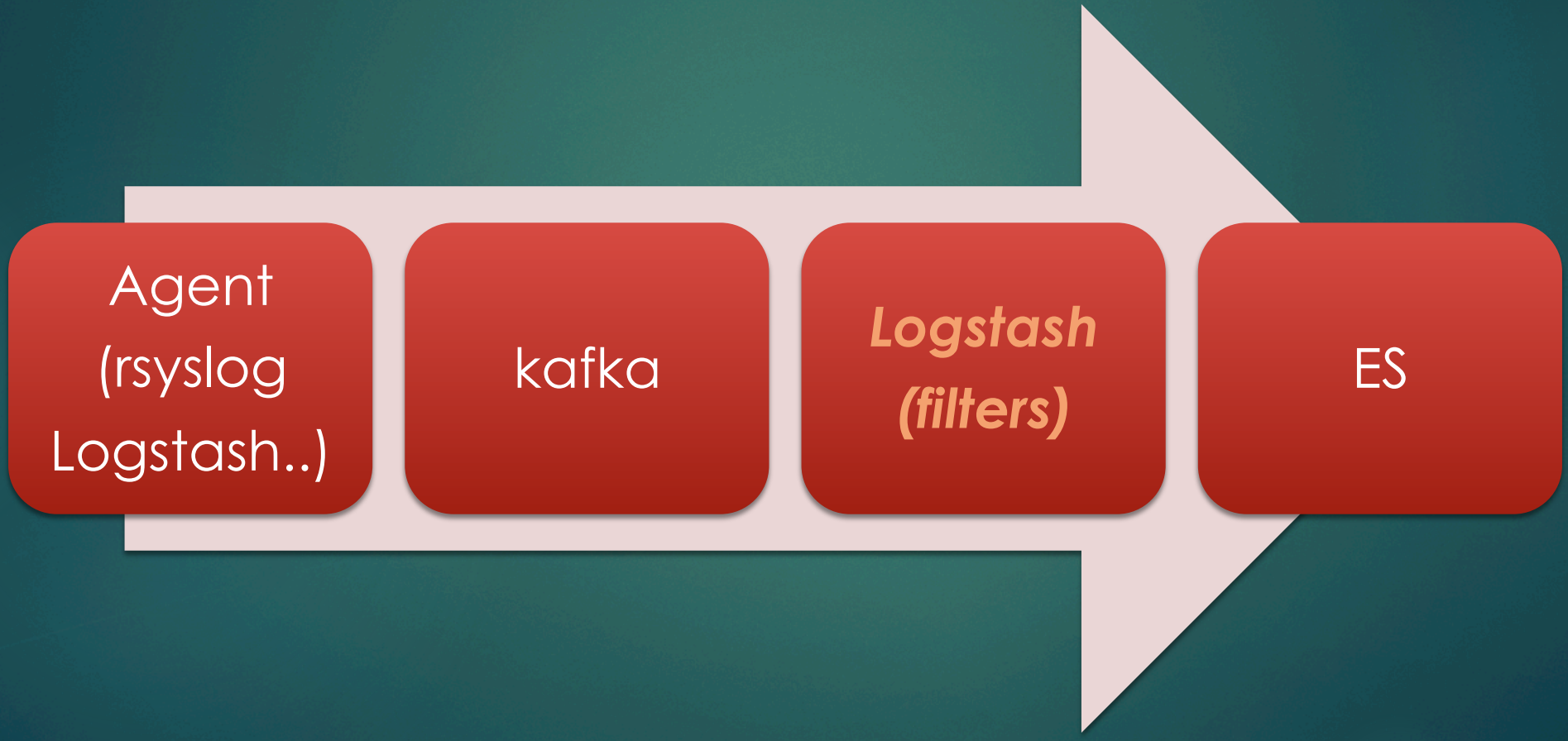
6.找到瓶颈

7. mesos+marathon+gitlba

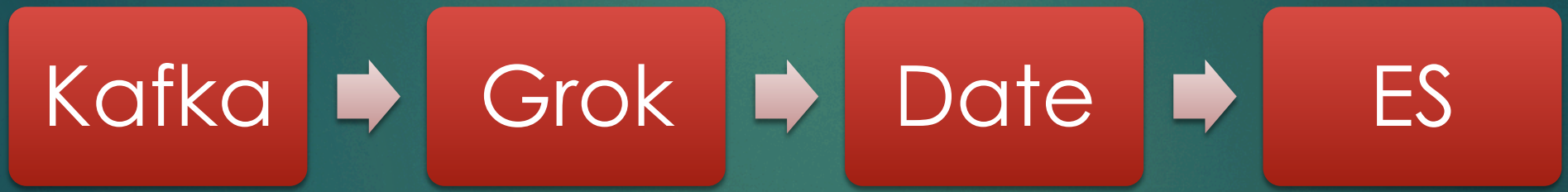
Why Hangout

慢

日志系统框架



性能对比


Kafka
Grok
Date
ES

日志格式

- 03/May/2016:18:11:13 +0800] ws.com vms100001 10.0.0.100 POST /test.php?param=/apiversion=6 80 - 10.1.0.100 110.110.119.123 HTTP/1.1 "Mozilla/5.0 (Linux; Android 5.0.2; HTC M8t Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/37.0.0.0 Mobile Safari/537.36_eb64__Ctrip_CtripWireless_6.15.2" "-" "-" 200 1145 418 0.082 0.082 10.8.177.24:80 200 backend_441

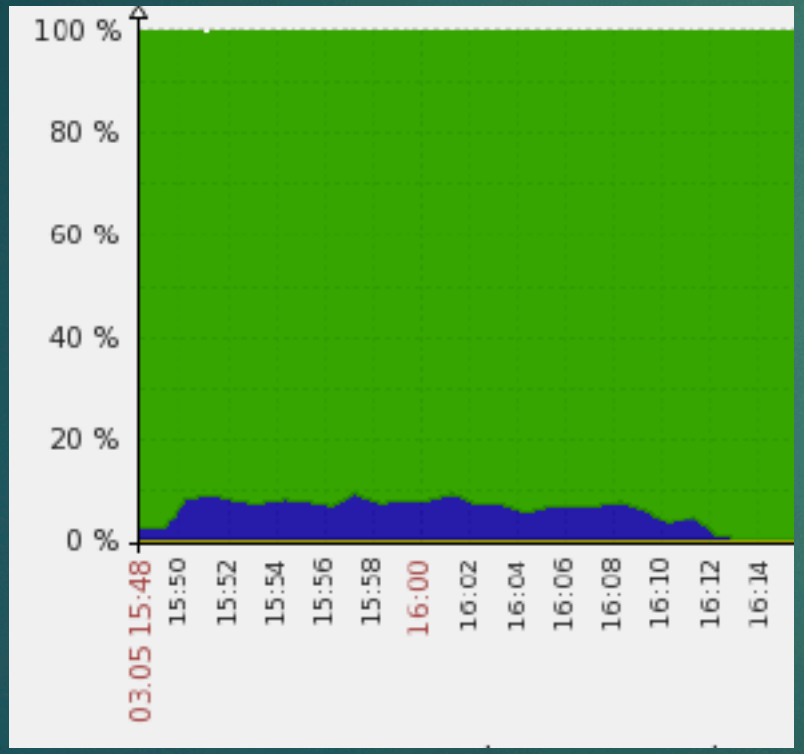
Grok配置

- ^\[%{HTTPDATE:logtime}\] %{HOSTNAME:domain} %{IPORHOST:hostname} %{IP:serverAddr} %{WORD:requestMethod} %{DATA:requestUri} %{NUMBER:serverPort} (-|%{USER:remoteUser}) %{IP:remoteAddr} (-|(?<forwarded>[0-9.]+(, [0-9.]+)*)) %{NOTSPACE:serverProtocol} ("-"|%{QS:UA}) ("-"|%{QS:cookie}) ("-"|%{QS:referer}) %{NUMBER:statusCode} %{NUMBER:requestLength} %{NUMBER:bodyBytesSent} %{NUMBER:request_time} (-|%{NUMBER:upstream_responseTime})(: %{DATA})? (-|%{NOTSPACE:upstreamAddr})(: %{DATA})? (-|%{NUMBER:upstreamStatus})(: %{DATA})? %{DATA:proxy_host}$

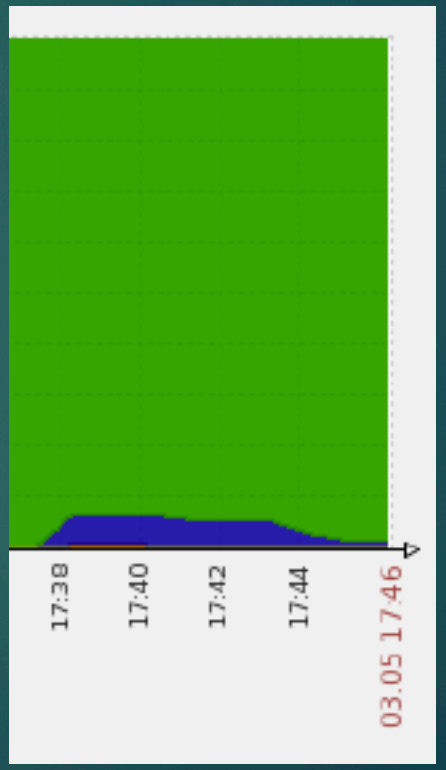
Logstash VS Hangout

- logstash
  - Filters: 32 threads(default)
  - 时钟时间 22m
  - cpu时间 53:22.65
- Hangout
  - Filters: 4 threads
  - 时钟时间 8m
  - Cpu时间 12:30.06

Logstash VS Hangout



L VS H



Plugins


Input
Stdin / Kafka / NewKafka
Filter
Grok / Date / KV / Convert/ GeoIP2 / URLDecode / UA
Output
Stdout / Elasticseach / Kafka

- bin/hangout –f http://10.0.0.100/example.yml

- https://github.com/childe/hangout/blob/master/example.yml

```
inputs:
    - Kafka:
        codec: plain
        encoding: UTF8 # defaut UTF8
        topic:
          app: 2
        consumer_settings:
          group.id: hangout
          zookeeper.connect: 192.168.1.200:2181
          auto.commit.interval.ms: "1000"
    - Kafka:
        codec: json
        topic:
          web: 1
        consumer_settings:
          group.id: hangout
          zookeeper.connect: 192.168.1.201:2181
          auto.commit.interval.ms: "5000"

filters:
    - Grok:
        match:
          - '^(?<logtime>\S+) (?<user>.+) (-|(?<level>\w+)) %{DATA:msg}$'
        remove_fields: ['message']
    - Date:
        src: logtime
        formats:
            - 'ISO8601'
        remove_fields: ['logtime']

outputs:
    - Elasticsearch:
        cluster: hangoutcluster
        hosts:
          - 192.168.1.200
        index: 'hangout-%{user}-%{+YYYY.MM.dd}'
        index_type: logs # default logs
        document_id: ${id} # defautt null, generated by es
        bulk_actions: 20000
        bulk_size: 15
        flush_interval: 10
        concurrent_requests: 0
```

感谢freemarker!

```
    - Add:
        if:
          - '<#if DepartDate?? && LogDateTime??>true</#if>'
        fields:
            Range: '${((DepartDate.getMillis() - LogDateTime.getMillis())/864
00000 + 1)?floor?c}'
```

```
      - Add:
          fields:
            target: '<#assign a=url?split("/")>${a[4]}'
          if:
            - '<#if url??>true</#if>'
            - '<#if url?contains("http://images4.c-ctrip.com/target/")>true<#el
seif url?contains(".c-ctrip.com/images/")>true</#if>'
```

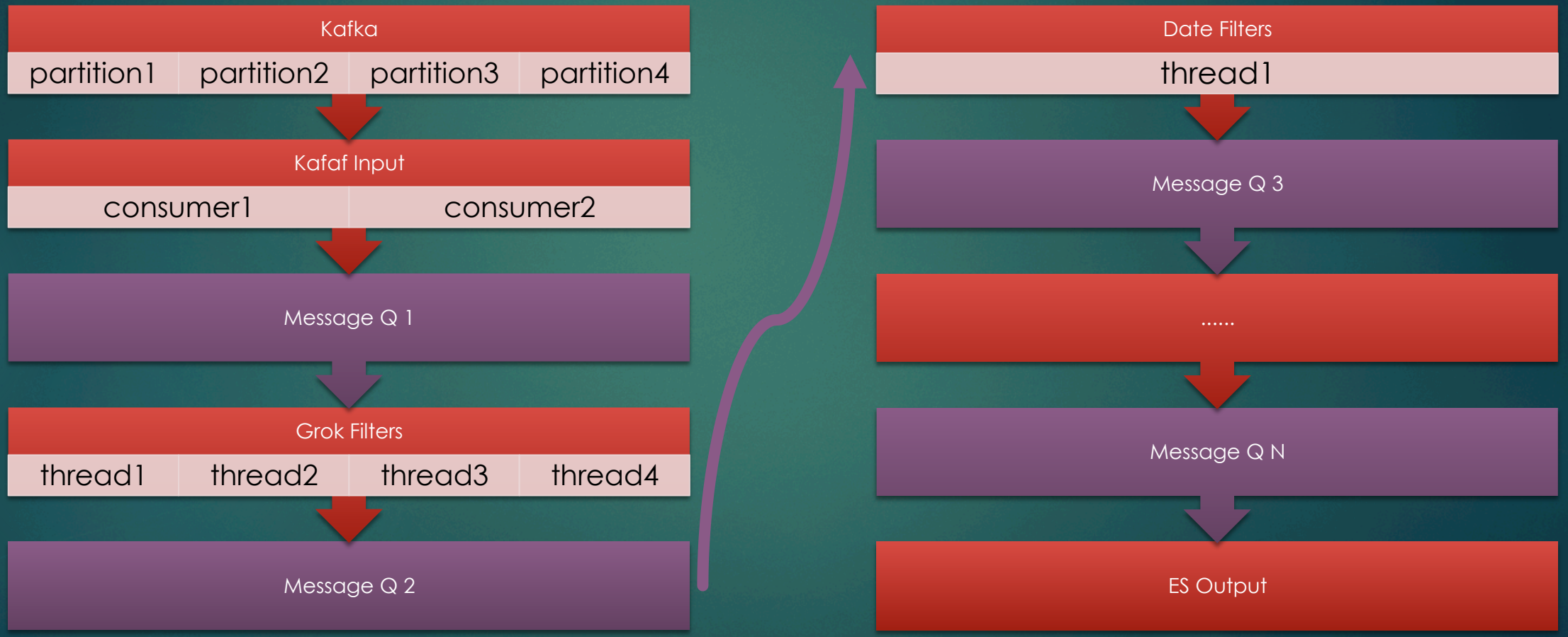
```
      - Add:
          fields:
            message: '${message?join(" ")}'
          if:
              - '<#if message?? && message?is_sequence>true</#if>'
```

架构变迁

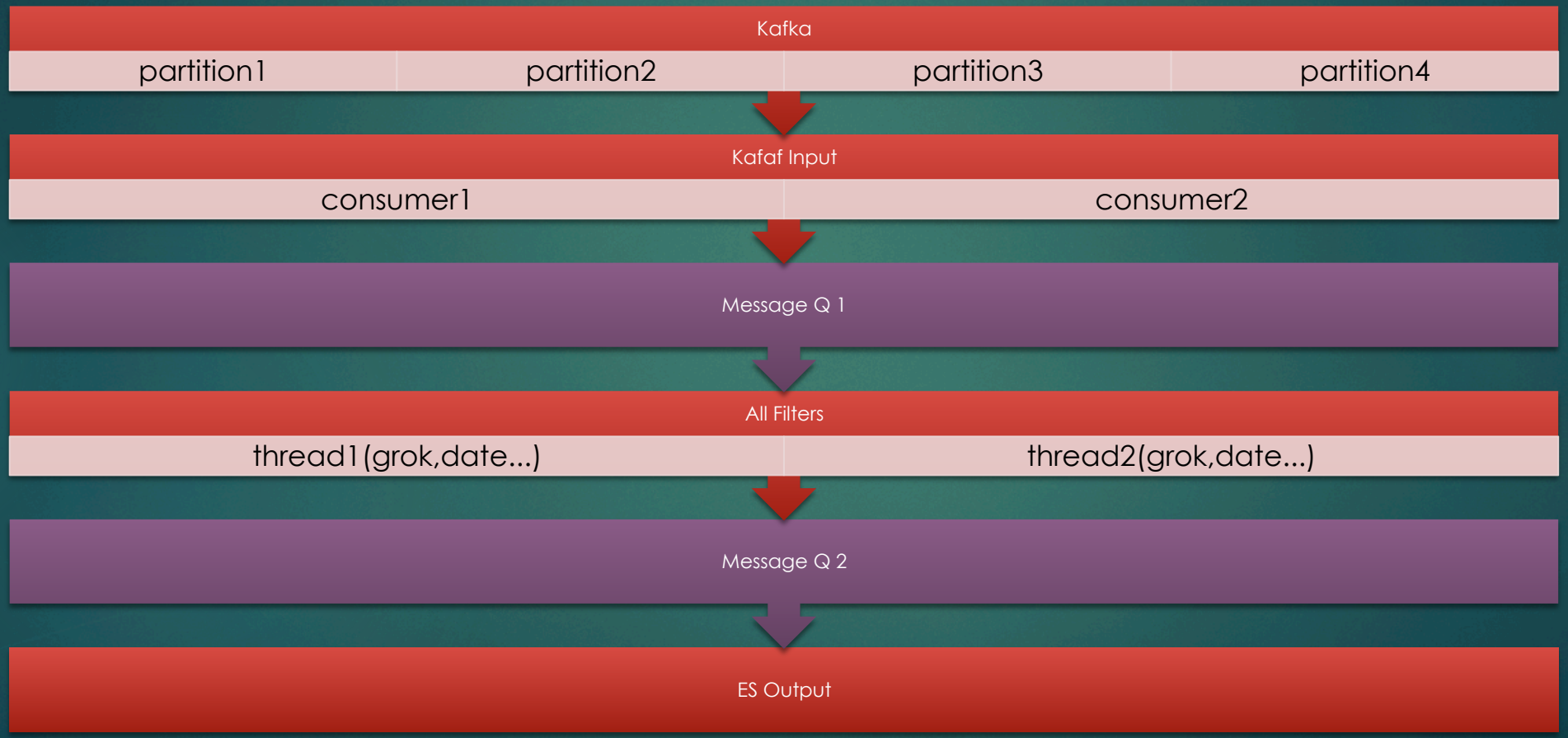
标杆

- **kafka-elasticsearch-standalone-consumer**
- https://github.com/reachkrishnaraj/kafka-elasticsearch-standalone-consumer

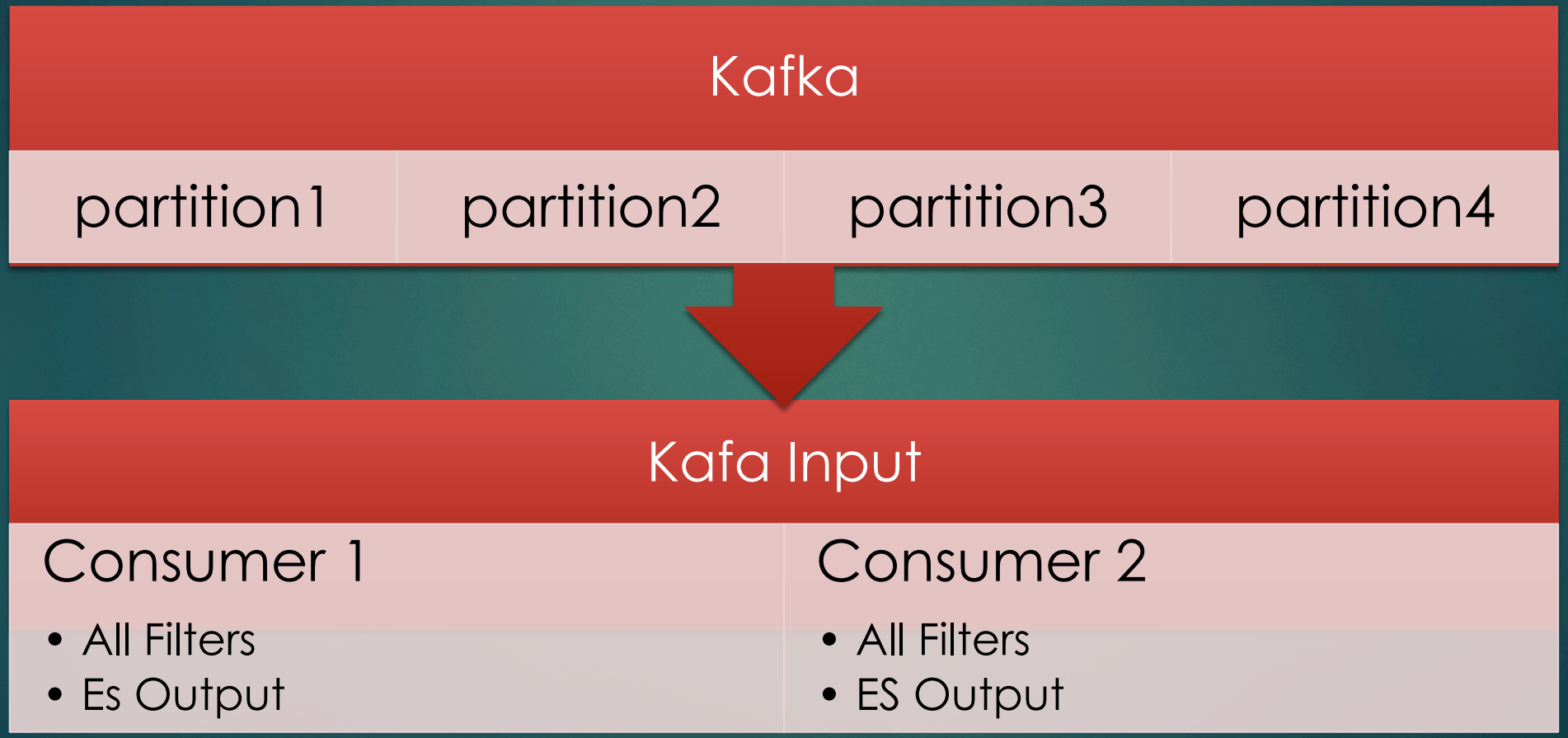
V1


Kafka
partition1
partition2
partition3
partition4
Kafaf Input
consumer1
consumer2
Message Q 1
Grok Filters
thread1
thread2
thread3
thread4
Message Q 2
Date Filters
thread1
Message Q 3
.....
Message Q N
ES Output

V2


Kafka
partition1
partition2
partition3
partition4
Kafaf Input
consumer1
consumer2
Message Q 1
All Filters
thread1(grok,date...)
thread2(grok,date...)
Message Q 2
ES Output

V3


Kafka
partition1
partition2
partition3
partition4
Kafa Input
Consumer 1
• All Filters
• Es Output
Consumer 2
• All Filters
• ES Output

对比测试

测试代码片断

```
for (int i = 0; i < this.messageCount; i++) {
    for (int j = 0; j < this.repeated; j++) {
        s = "172.17.0.2";
        m = p.matcher(s);
        m.matches();
    }
}
```

NO-Q VS Q

- # time java -cp test-java-queue-0.1.jar DirectWriter 1000000 4 20
- real 0m2.511s
- user 0m9.752s
- sys 0m0.236s

- # time java -cp test-java-queue-0.1.jar QueueWriter 1000000 4 20
- real 0m2.948s
- user 0m12.160s
- sys 0m1.144s

Complex Filter

- time java -cp test-java-queue-0.1.jar QueueWriter 1000000 4 1
- real 0m1.309s user 0m2.920s sys 0m1.242s

- time java -cp test-java-queue-0.1.jar QueueWriter 1000000 4 10
- real 0m1.826s user 0m7.321s sys 0m1.006s

- # time java -cp test-java-queue-0.1.jar QueueWriter 1000000 4 100
- real 0m12.176s user 0m49.884s sys 0m1.633s

Extreme Compare

- # time java -cp test-java-queue-0.1.jar DirectWriter 1000000 4 1
- real 0m0.250s
- user 0m0.821s
- sys 0m0.074s

- # time java -cp test-java-queue-0.1.jar QueueWriter 1000000 4 1
- real 0m1.416s
- user 0m3.057s
- sys 0m1.332s

参数调优

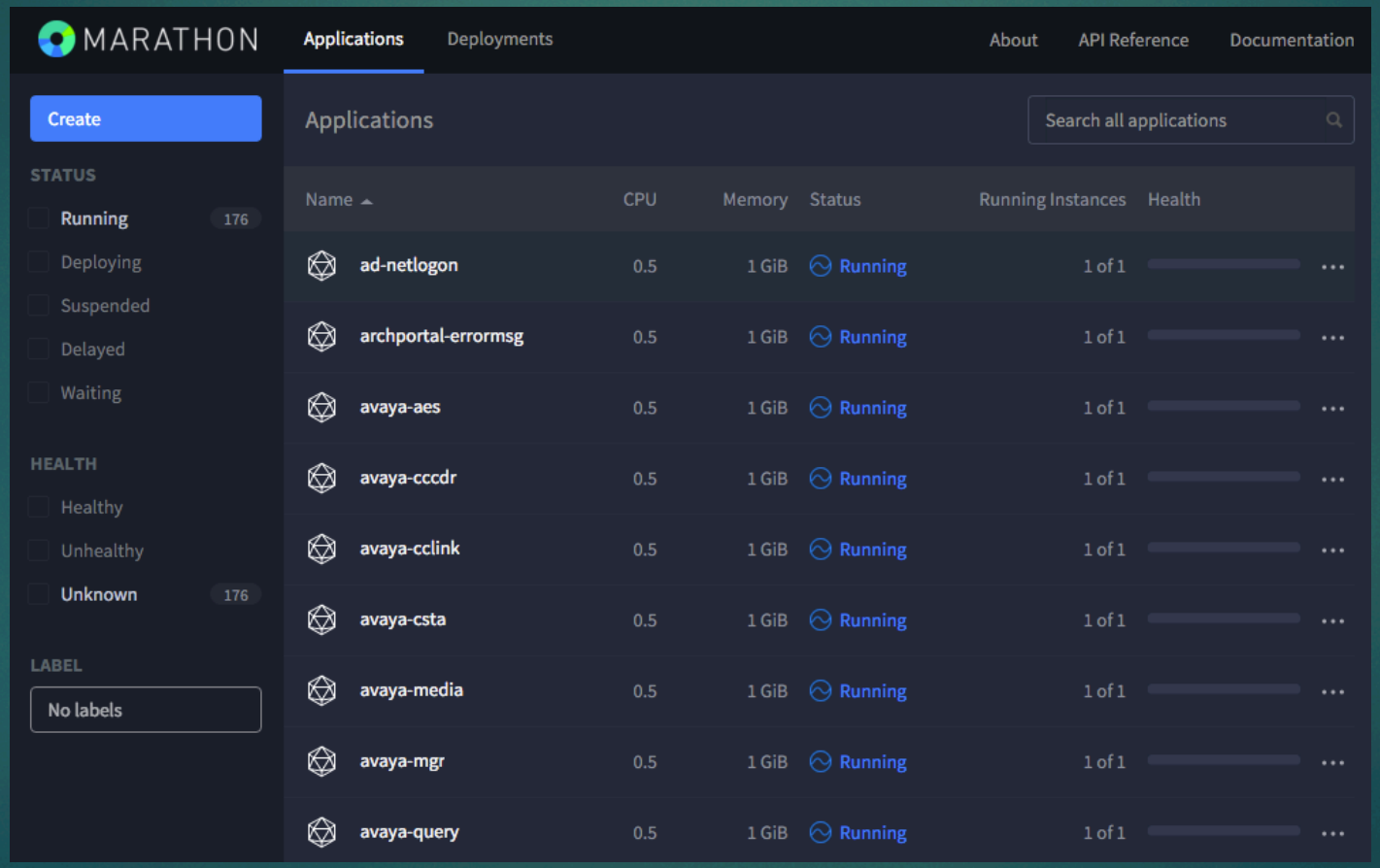
- Input thread
- bulk_actions: 60000
- bulk_size: 50
- flush_interval: 120
- concurrent_requests: 0
- HO_HEAP_SIZE

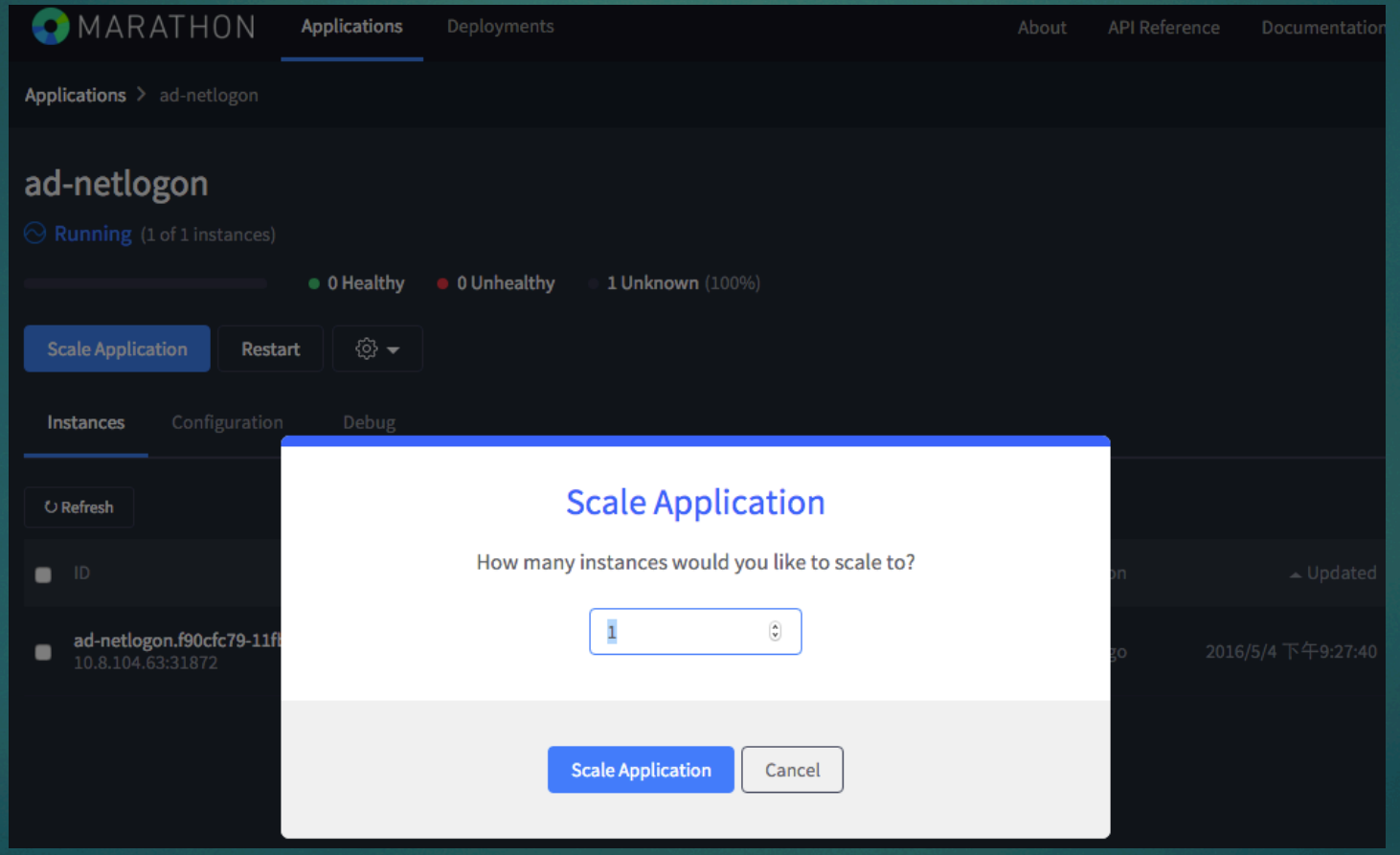
找到瓶颈

- 2016-05-05 03:18:28,138 INFO XXX thread-1 executionId: 37759
- 2016-05-05 03:18:28,138 INFO XXX thread-1 numberOfActions: 60000
- 2016-05-05 03:18:38,326 INFO XXX thread-1 bulk done with executionId: 37759
- 2016-05-05 03:18:46,311 INFO XXX thread-1 executionId: 37760
- 2016-05-05 03:18:46,311 INFO XXX thread-1 numberOfActions: 60000
- 2016-05-05 03:18:52,409 INFO XXX thread-1 bulk done with executionId: 37760

mesos+marathon+gitlab

- 资源分配/隔离
- 增加/减少实例
- 环境和版本一致
- 配置放在远端服务器


MARATHON
Applications
Deployments
About
API Reference
Documentation
Create
STATUS
Running 176
Deploying
Suspended
Delayed
Waiting
HEALTH
Healthy
Unhealthy
Unknown 176
LABEL
No labels
Applications
Search all applications
Name
CPU
Memory
Status
Running Instances
Health
ad-netlogon 0.5 1 GiB Running 1 of 1
archportal-errormsg 0.5 1 GiB Running 1 of 1
avaya-aes 0.5 1 GiB Running 1 of 1
avaya-cccdr 0.5 1 GiB Running 1 of 1
avaya-cclink 0.5 1 GiB Running 1 of 1
avaya-csta 0.5 1 GiB Running 1 of 1
avaya-media 0.5 1 GiB Running 1 of 1
avaya-mgr 0.5 1 GiB Running 1 of 1
avaya-query 0.5 1 GiB Running 1 of 1


MARATHON
Applications
Deployments
About
API Reference
Documentation
Applications > ad-netlogon
ad-netlogon
Running (1 of 1 instances)
0 Healthy
0 Unhealthy
1 Unknown (100%)
Scale Application
Restart
Instances
Configuration
Debug
Refresh
ID
Updated
ad-netlogon.f90cfc79-11f
10.8.104.63:31872
2016/5/4 下午9:27:40
Scale Application
How many instances would you like to scale to?
1
Scale Application
Cancel

/tmp/mesos/slaves/3a872085-2aba-42c2-82d7-55b418011340-S24/frameworks/20160318-041349-4015261706-8081-1-0000/executors/ad-netlog..

[redacted]/static/pailer.html

```
2016-05-06 12:50:48,178 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4278
2016-05-06 12:50:48,704 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4279
2016-05-06 12:50:48,704 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 12:50:50,285 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4279
2016-05-06 12:50:50,851 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4280
2016-05-06 12:50:50,851 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 12:50:52,489 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4280
2016-05-06 12:50:53,091 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4281
2016-05-06 12:50:53,091 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 12:50:54,614 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4281
2016-05-06 12:51:20,286 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 elasticsearch[Marvel Boy][bulk_processor][T#1] ex
2016-05-06 12:51:20,286 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 elasticsearch[Marvel Boy][bulk_processor][T#1] nu
2016-05-06 12:51:21,068 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 elasticsearch[Marvel Boy][bulk_processor][T#1] bu
2016-05-06 13:00:09,022 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4283
2016-05-06 13:00:09,022 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 13:00:11,493 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4283
2016-05-06 13:00:12,035 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4284
2016-05-06 13:00:12,035 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 13:00:13,474 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4284
2016-05-06 13:00:14,043 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4285
2016-05-06 13:00:14,044 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 13:00:15,463 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4285
2016-05-06 13:00:16,000 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4286
2016-05-06 13:00:16,001 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
2016-05-06 13:00:18,660 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 bulk done with executionId: 4286
2016-05-06 13:00:19,205 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 executionId: 4287
2016-05-06 13:00:19,206 INFO com.ctrip.ops.sysdev.outputs.Elasticsearch$1 pool-2-thread-1 numberOfActions: 20000
```

https://github.com/childe/hangout

Thanks!