From Zero to Hero

Easy log centralization with Logstash & Elasticsearch

Rafał Kuć – Sematext Group, Inc.

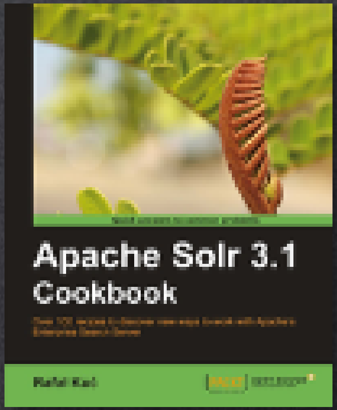
@kucrafal @sematext sematext.com

Kilka słów o mnie…

Sematext consultant & engineer

Solr.pl co-founder

Father and husband ☺



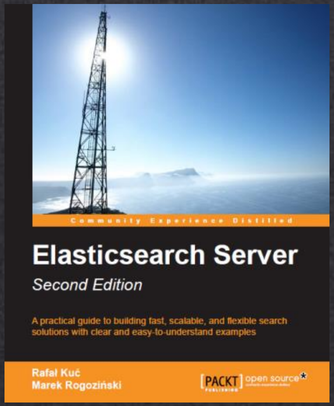
Quick answers to common problems

Apache Solr 3.1 Cookbook

Over 100 recipes to discover new ways to work with Apache's Enterprise Search Server

Rafał Kuć

PACKT open source



Community Experience Distilled

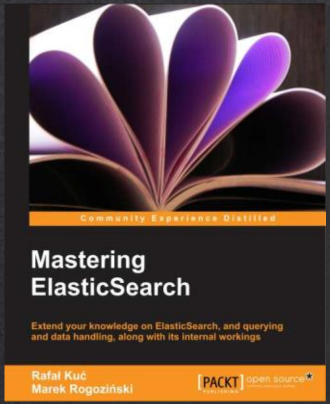
Elasticsearch Server

Second Edition

A practical guide to building fast, scalable, and flexible search solutions with clear and easy-to-understand examples

Rafał Kuć
Marek Rogoziński

PACKT open source



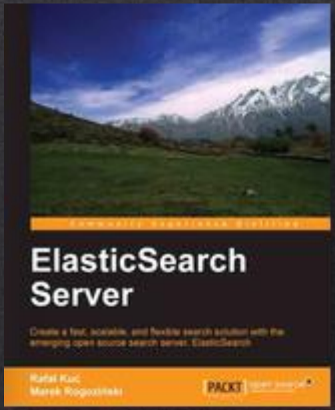
Community Experience Distilled

Mastering ElasticSearch

Extend your knowledge on ElasticSearch, and querying and data handling, along with its internal workings

Rafał Kuć
Marek Rogoziński

PACKT open source



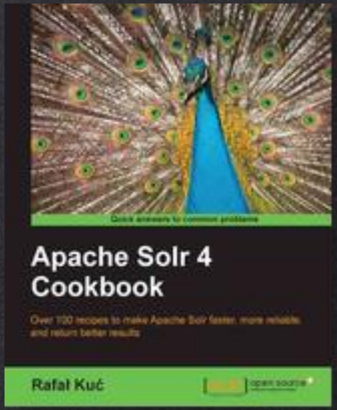
Community Experience Distilled

ElasticSearch Server

Create a fast, scalable, and flexible search solution with the emerging open source search server, ElasticSearch

Rafał Kuć
Marek Rogoziński

PACKT open source



Quick answers to common problems

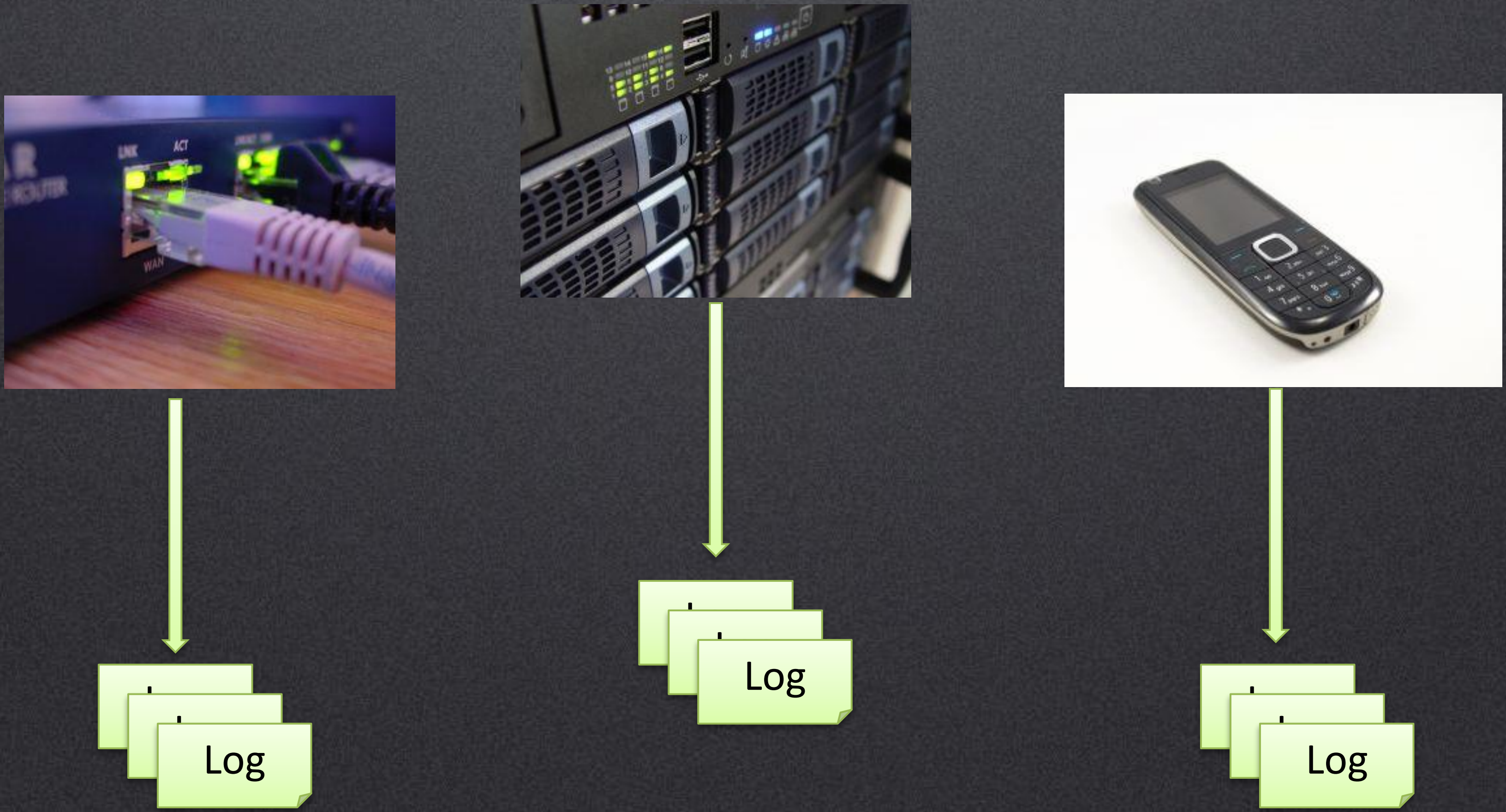
Apache Solr 4 Cookbook

Over 100 recipes to make Apache Solr faster, more reliable, and return better results

Rafał Kuć

PACKT open source

Problem



Log

Log

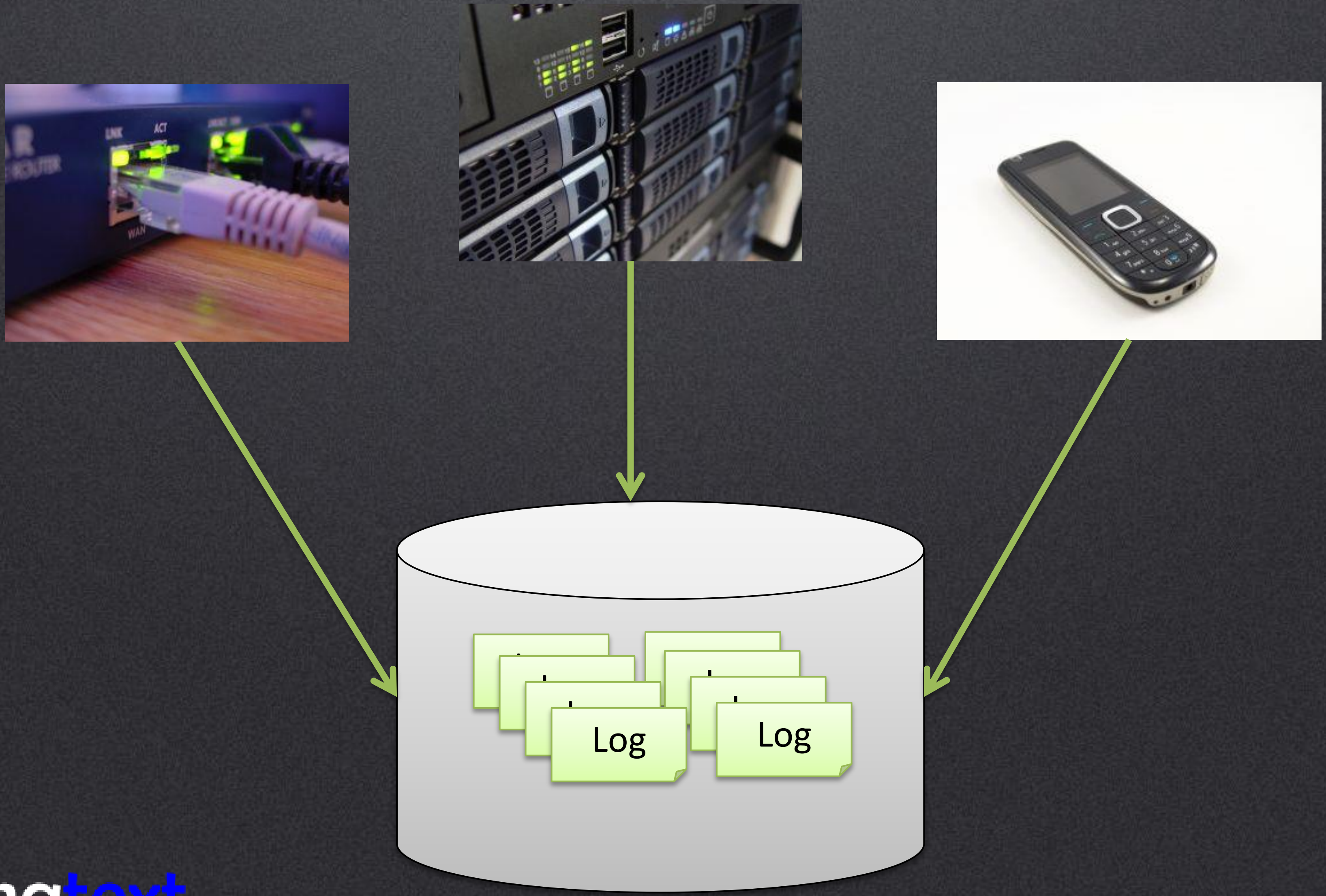
Log

Spróbujmy coś znaleźć

http://www.likesbooks.com/aarafterhours/?p=750

sematext

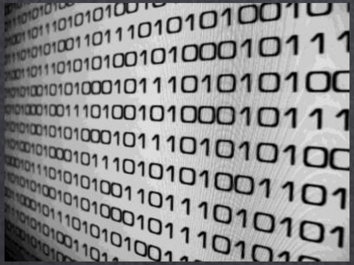
Rozwiązanie



Dostępne narzędzia

...

Dlaczego „search”



Łatwość wyszukiwania danych

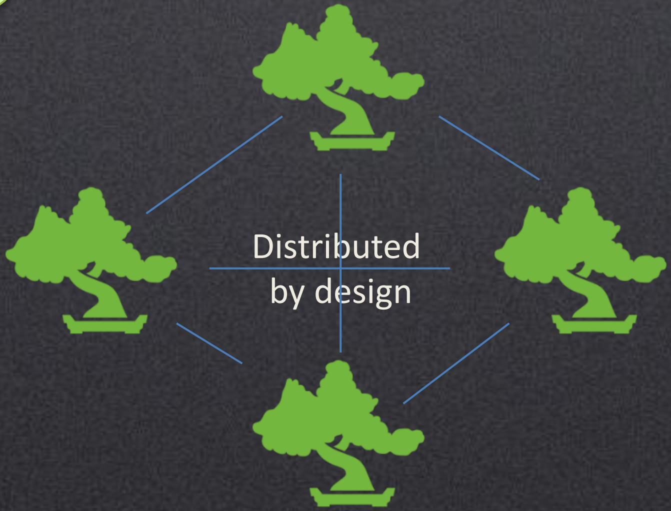
Szybkość i precyzja

Analiza w czasie „prawie” rzeczywistym

Dlaczego Elasticsearch?

Wartości domyślne

{ JSON }



Distributed by design

Lucene

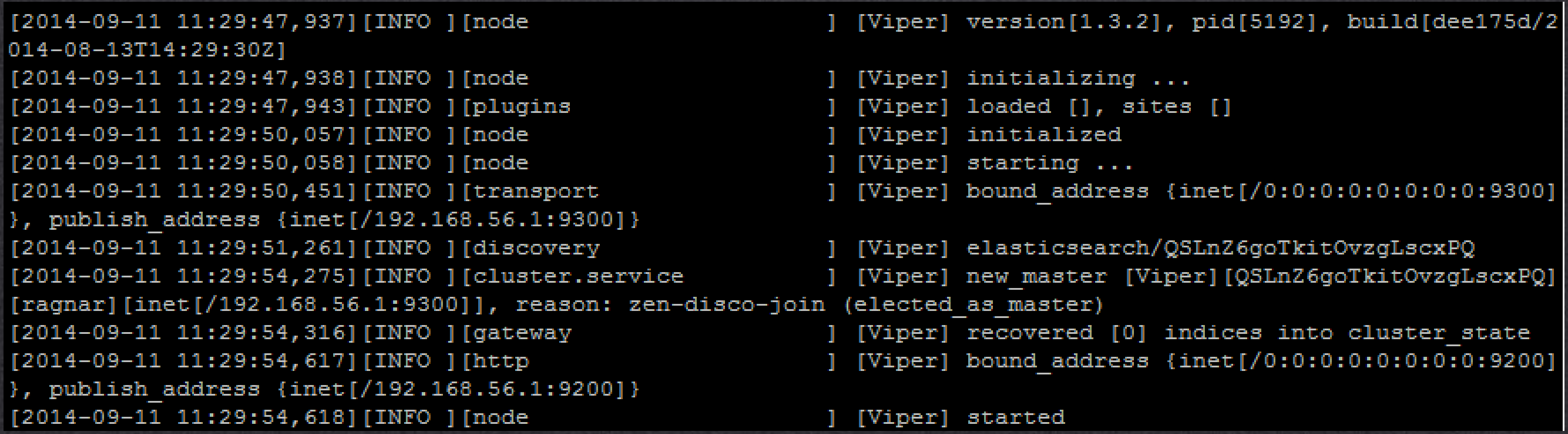
http://www.dailypets.co.uk/2007/06/17/kittens-rest-at-half-time/

sematext

Instalacja

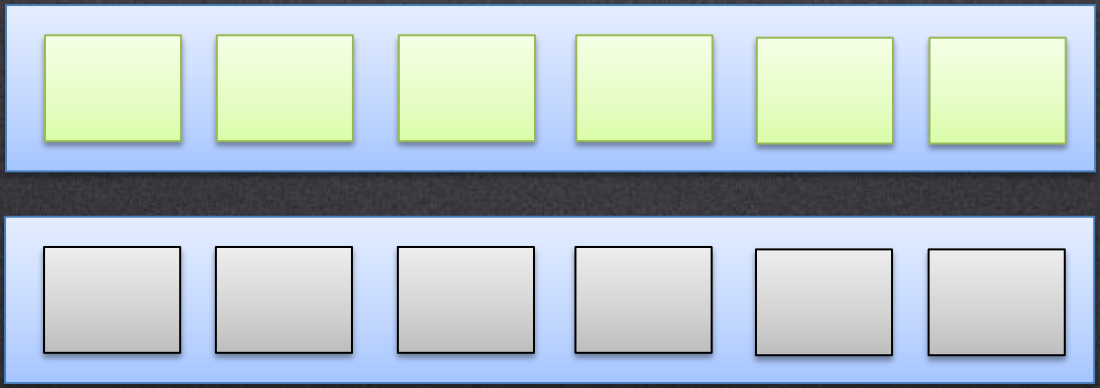
```
$ wget --no-check-certificate
https://download.elasticsearch.org/elasticsearch/elasticsearch/elasticsearch-1.3.2.tar.gz
```

```
$ tar –xvf elasticsearch-1.3.2.tar.gz
$ elasticsearch-1.3.2/bin/elasticsearch
```

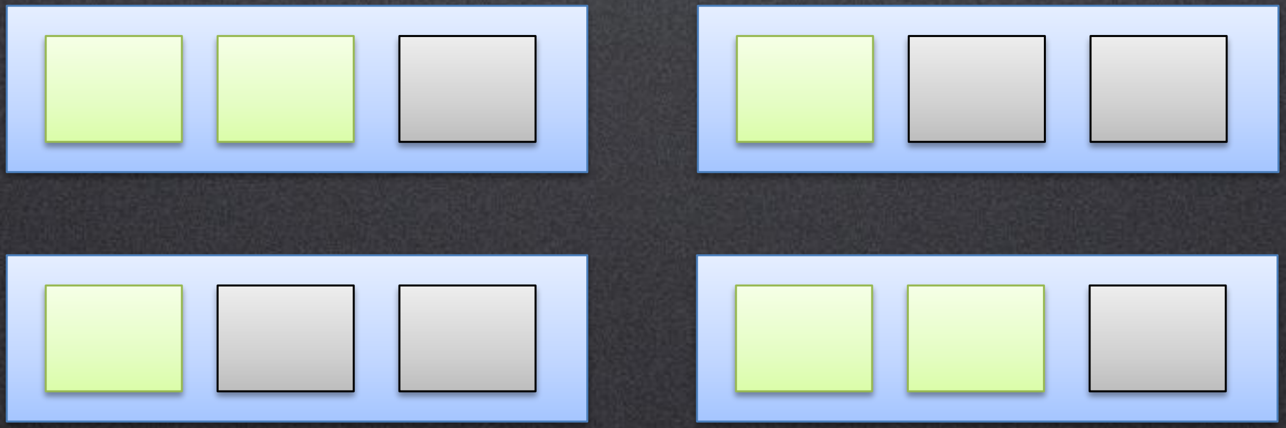


```
[2014-09-11 11:29:47,937][INFO ][node                     ] [Viper] version[1.3.2], pid[5192], build[dee175d/2
014-08-13T14:29:30Z]
[2014-09-11 11:29:47,938][INFO ][node                     ] [Viper] initializing ...
[2014-09-11 11:29:47,943][INFO ][plugins                  ] [Viper] loaded [], sites []
[2014-09-11 11:29:50,057][INFO ][node                     ] [Viper] initialized
[2014-09-11 11:29:50,058][INFO ][node                     ] [Viper] starting ...
[2014-09-11 11:29:50,451][INFO ][transport                ] [Viper] bound_address {inet[/0:0:0:0:0:0:0:0:9300]
}, publish_address {inet[/192.168.56.1:9300]}
[2014-09-11 11:29:51,261][INFO ][discovery                ] [Viper] elasticsearch/QSLnZ6goTkitOvzgLscxPQ
[2014-09-11 11:29:54,275][INFO ][cluster.service          ] [Viper] new_master [Viper][QSLnZ6goTkitOvzgLscxPQ]
[ragnar][inet[/192.168.56.1:9300]], reason: zen-disco-join (elected_as_master)
[2014-09-11 11:29:54,316][INFO ][gateway                  ] [Viper] recovered [0] indices into cluster_state
[2014-09-11 11:29:54,617][INFO ][http                     ] [Viper] bound_address {inet[/0:0:0:0:0:0:0:0:9200]
}, publish_address {inet[/192.168.56.1:9200]}
[2014-09-11 11:29:54,618][INFO ][node                     ] [Viper] started
```

Skalowalność

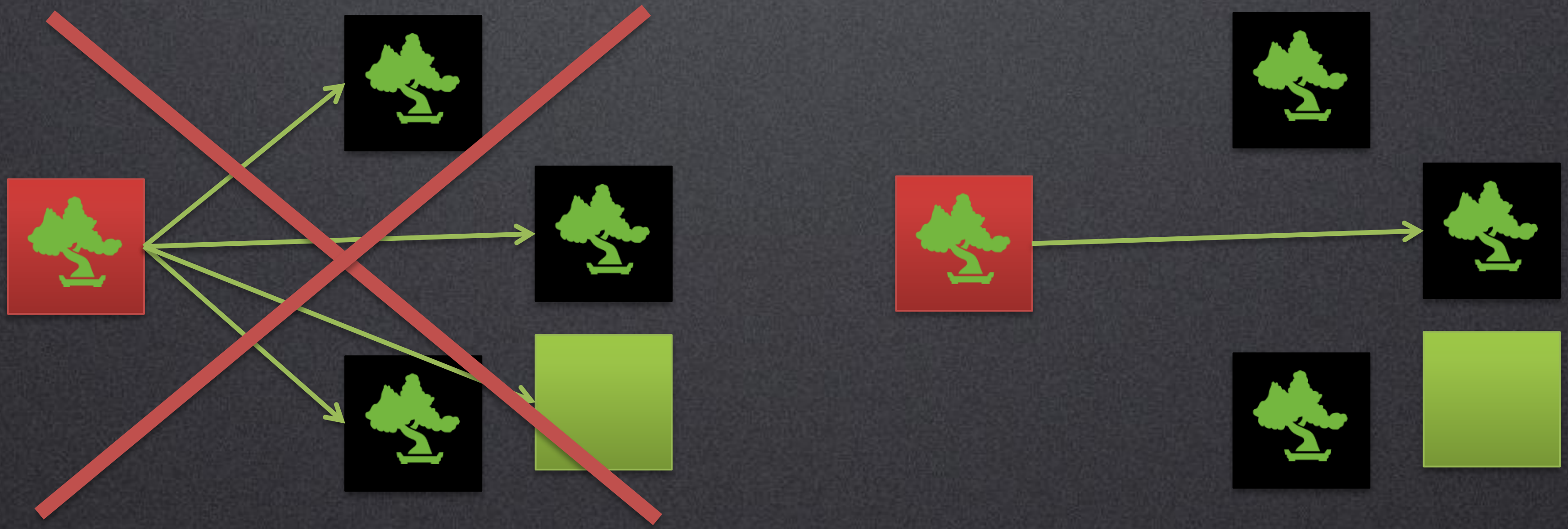


Skalowalność



sematext

Konfiguracja - stabilność



minimum_master_nodes
=
N/2 + 1

Master only	Data only	Data only	
			Client only
Master only	Data only	Data only	
			Client only
Master only	Data only	Data only	

Thread pools

Use fixed

Set size

search

```
threadpool.search.type
threadpool.search.size
threadpool.search.queue_size
```

bulk

```
threadpool.bulk.type
threadpool.bulk.size
threadpool.bulk.queue_size
```

index

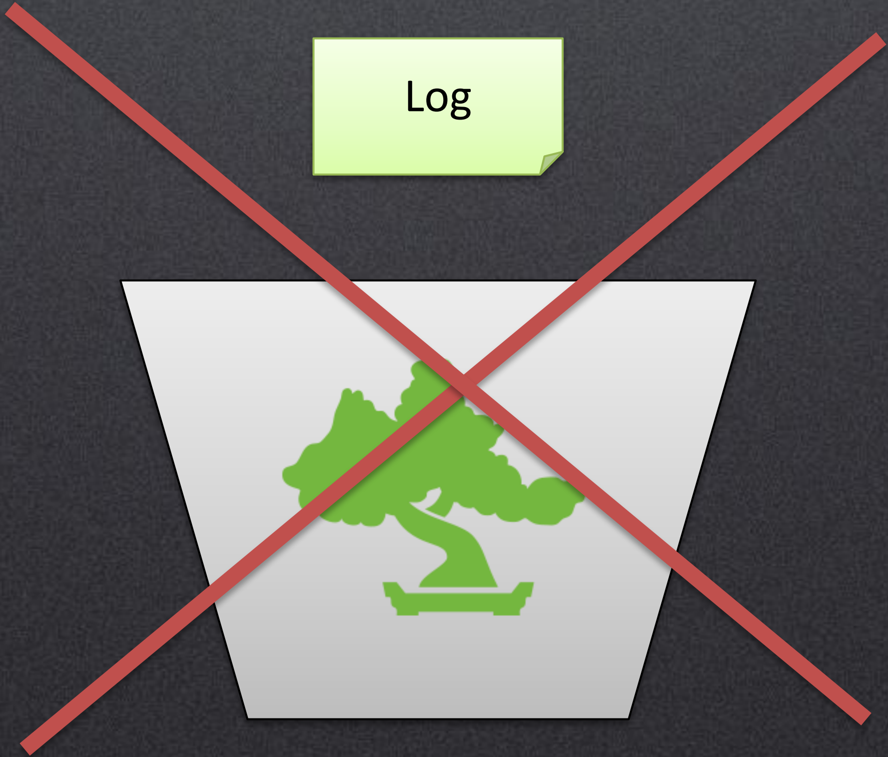
```
threadpool.index.type
threadpool.index.size
threadpool.index.queue_size
```

Set queue

Circuit breakers, caches == brak OOM

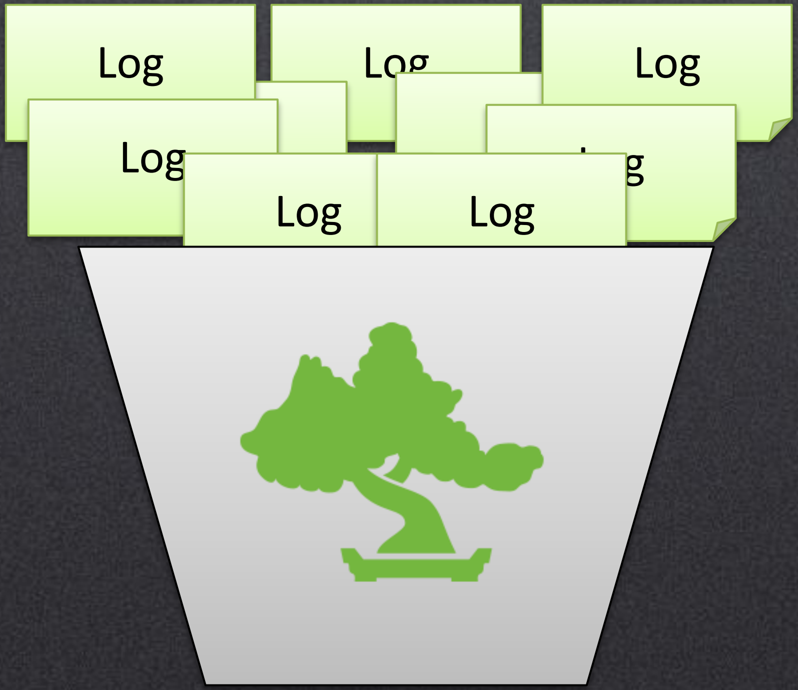
indices.breaker.fielddata.limit indices.breaker.fielddata.overhead	40% Xmx 1
indices.breaker.request.limit indices.breaker.request.overhead	60% Xmx 1.03
indices.breaker.total.limit	70% Xmx
indices.fielddata.cache.size	unbounded
indices.cache.filter.size	10%

Konfiguracja - indeksowanie



Konfiguracja - indeksowanie

Use Bulk!



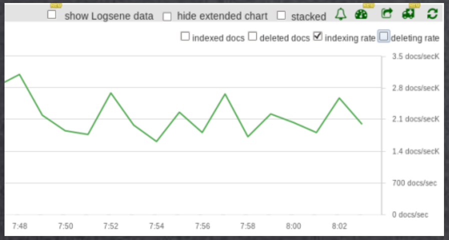
Or UDP Bulk!

```
unlimited
200mb
```

```
index.translog.flush_threshold_ops
index.translog.flush_threshold_size
```

sematext

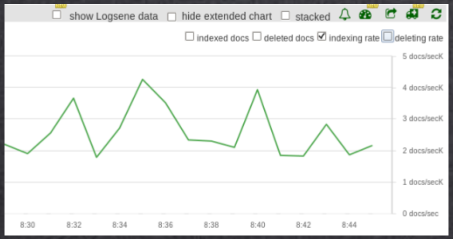
Re-open tylko w razie konieczności



□ show Logsene data □ hide extended chart □ stacked

□ indexed docs □ deleted docs ☑ indexing rate □ deleting rate

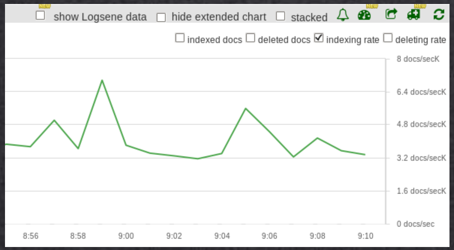
1s refresh -> 2K logs/sec



□ show Logsene data □ hide extended chart □ stacked

□ indexed docs □ deleted docs ☑ indexing rate □ deleting rate

5s refresh -> 2.5K logs/sec



□ show Logsene data □ hide extended chart □ stacked

□ indexed docs □ deleted docs ☑ indexing rate □ deleting rate

30s refresh -> 3.4K logs/sec

http://blog.sematext.com/2013/07/08/elasticsearch-refresh-interval-vs-indexing-performance/

sematext

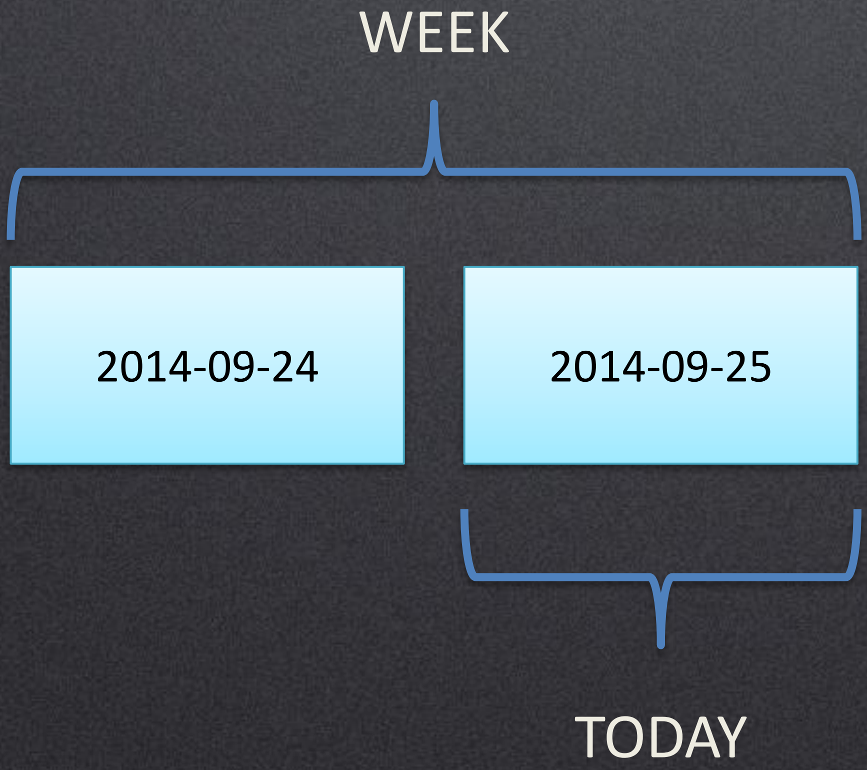
Dane pod kontrolą

WEEK

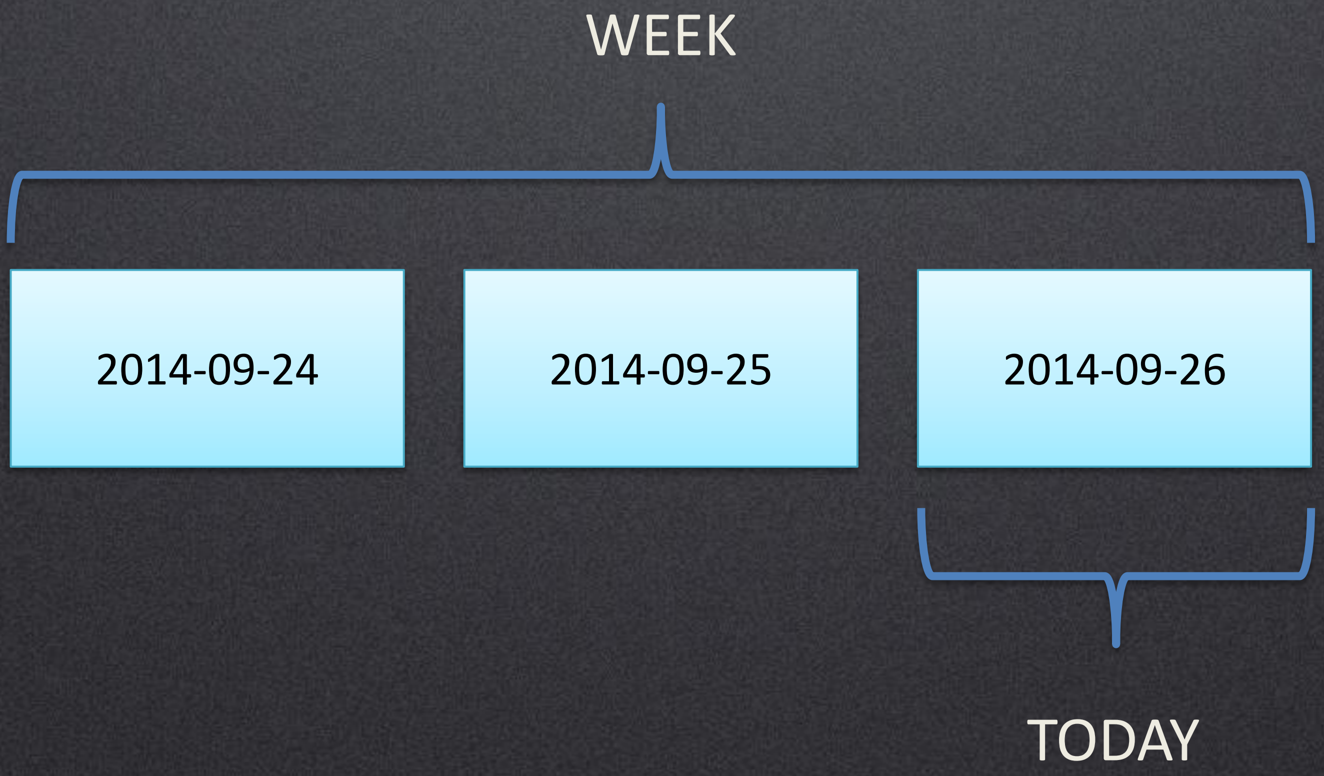
2014-09-24

TODAY

Dane pod kontrolą



Dane pod kontrolą



WEEK

2014-09-24

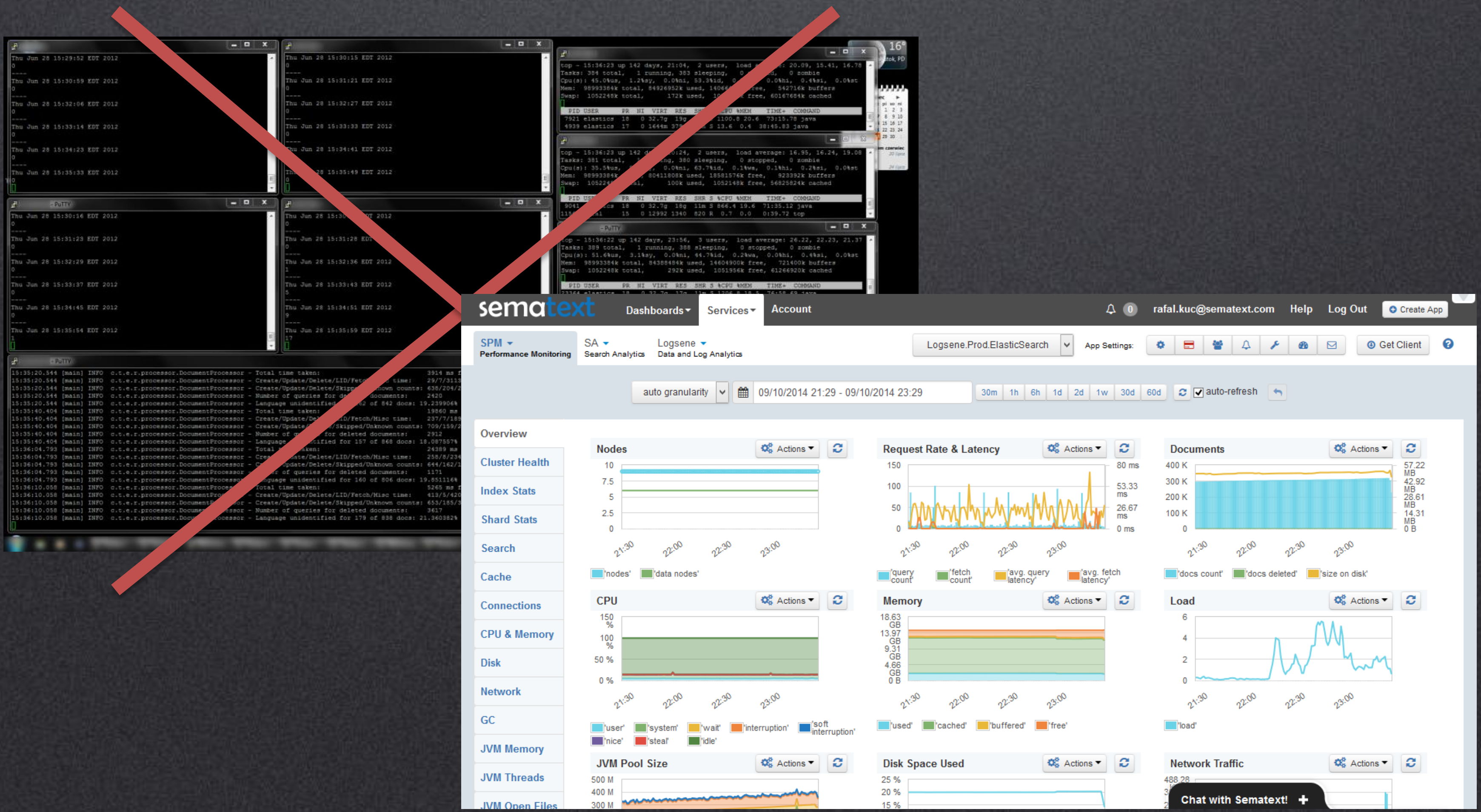
2014-09-25

2014-09-26

TODAY

sematext

Monitoring



```
Thu Jun 28 15:29:52 EDT 2012
0
----
Thu Jun 28 15:30:59 EDT 2012
0
----
Thu Jun 28 15:32:06 EDT 2012
0
----
Thu Jun 28 15:33:14 EDT 2012
0
----
Thu Jun 28 15:34:23 EDT 2012
0
----
Thu Jun 28 15:35:33 EDT 2012
0
```

```
Thu Jun 28 15:30:15 EDT 2012
0
----
Thu Jun 28 15:31:21 EDT 2012
0
----
Thu Jun 28 15:32:27 EDT 2012
0
----
Thu Jun 28 15:33:33 EDT 2012
0
----
Thu Jun 28 15:34:41 EDT 2012
Thu Jun 28 15:35:49 EDT 2012
0
```

```
Thu Jun 28 15:30:16 EDT 2012
0
----
Thu Jun 28 15:31:23 EDT 2012
0
----
Thu Jun 28 15:32:29 EDT 2012
0
----
Thu Jun 28 15:33:37 EDT 2012
0
----
Thu Jun 28 15:34:45 EDT 2012
0
----
Thu Jun 28 15:35:54 EDT 2012
1
```

```
Thu Jun 28 15:30[illegible] EDT 2012
0
----
Thu Jun 28 15:31:28 EDT
0
----
Thu Jun 28 15:32:36 EDT 2012
1
----
Thu Jun 28 15:33:43 EDT 2012
5
----
Thu Jun 28 15:34:51 EDT 2012
9
----
Thu Jun 28 15:35:59 EDT 2012
17
```

```
top - 15:36:23 up 142 days, 21:04,  2 users,  load [illegible]: 20.09, 15.41, 16.78
Tasks: 384 total,   1 running, 383 sleeping,   0 [illegible],   0 zombie
Cpu(s): 45.0%us,  1.2%sy,  0.0%ni, 53.3%id,  0 [illegible]  0.0%hi,  0.4%si,  0.0%st
Mem:  98993384k total, 84926952k used, 14066[illegible] free,   542716k buffers
Swap:  1052248k total,      172k used,  10[illegible] free, 60167684k cached

  PID USER      PR  NI  VIRT  RES  SH[illegible] %MEM    TIME+  COMMAND
 7921 elastics  18   0 32.7g  19g [illegible] 1100.8 20.6  73:15.78 java
 4939 elastics  17   0 1644m 379[illegible] S 13.6  0.4  38:45.83 java
```

```
top - 15:36:23 up 142 d[illegible]0:24,  2 users,  load average: 16.95, 16.24, 19.08
Tasks: 381 total,  [illegible], 380 sleeping,   0 stopped,   0 zombie
Cpu(s): 35.5%us, [illegible],  0.0%ni, 63.7%id,  0.1%wa,  0.1%hi,  0.2%si,  0.0%st
Mem:  98993384k [illegible], 80411808k used, 18581576k free,   923392k buffers
Swap:  105224[illegible], 100k used,  1052148k free, 56825824k cached

  PID US[illegible]  PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 9041 [illegible]  18   0 32.7g  18g  11m S 866.4 19.6  71:35.12 java
115[illegible]  15   0 12992 1340  820 R  0.7  0.0   0:39.72 top
```

```
top - 15:36:22 up 142 days, 23:56,  3 users,  load average: 26.22, 22.23, 21.37
Tasks: 389 total,   1 running, 388 sleeping,   0 stopped,   0 zombie
Cpu(s): 51.6%us,  3.1%sy,  0.0%ni, 44.7%id,  0.2%wa,  0.0%hi,  0.4%si,  0.0%st
Mem:  98993384k total, 84388484k used, 14604900k free,   721400k buffers
Swap:  1052248k total,      292k used,  1051956k free, 61266920k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
```

```
15:35:20.544 [main] INFO  c.t.e.r.processor.DocumentProcessor - Total time taken:                    3914 ms f
15:35:20.544 [main] INFO  c.t.e.r.processor.DocumentProcessor - Create/Update/Delete/LID/Fetc[illegible] time:    29/7/3113
15:35:20.544 [main] INFO  c.t.e.r.processor.DocumentProcessor - Create/Update/Delete/Skipp[illegible]nown counts: 638/204/2
15:35:20.544 [main] INFO  c.t.e.r.processor.DocumentProcessor - Number of queries for de[illegible] documents:     2420
15:35:20.544 [main] INFO  c.t.e.r.processor.DocumentProcessor - Language unidentified [illegible]62 of 842 docs: 19.239906%
15:35:40.404 [main] INFO  c.t.e.r.processor.DocumentProcessor - Total time taken:                    19860 ms
15:35:40.404 [main] INFO  c.t.e.r.processor.DocumentProcessor - Create/Update/De[illegible]ID/Fetch/Misc time:    237/7/189
15:35:40.404 [main] INFO  c.t.e.r.processor.DocumentProcessor - Create/Update/[illegible]/Skipped/Unknown counts: 709/159/2
15:35:40.404 [main] INFO  c.t.e.r.processor.DocumentProcessor - Number of q[illegible] for deleted documents:     2912
15:35:40.404 [main] INFO  c.t.e.r.processor.DocumentProcessor - Language [illegible]ntified for 157 of 868 docs: 18.087557%
15:36:04.793 [main] INFO  c.t.e.r.processor.DocumentProcessor - Total [illegible]aken:                    24389 ms
15:36:04.793 [main] INFO  c.t.e.r.processor.DocumentProcessor - Cre[illegible]date/Delete/LID/Fetch/Misc time:    258/8/234
15:36:04.793 [main] INFO  c.t.e.r.processor.DocumentProcessor - C[illegible]Update/Delete/Skipped/Unknown counts: 644/162/1
15:36:04.793 [main] INFO  c.t.e.r.processor.DocumentProcessor [illegible]r of queries for deleted documents:     1171
15:36:04.793 [main] INFO  c.t.e.r.processor.DocumentProcesso[illegible]nguage unidentified for 160 of 806 docs: 19.851116%
15:36:10.058 [main] INFO  c.t.e.r.processor.DocumentProce[illegible] Total time taken:                    5265 ms f
15:36:10.058 [main] INFO  c.t.e.r.processor.DocumentPro[illegible] - Create/Update/Delete/LID/Fetch/Misc time:    413/5/420
15:36:10.058 [main] INFO  c.t.e.r.processor.DocumentP[illegible]sor - Create/Update/Delete/Skipped/Unknown counts: 653/185/3
15:36:10.058 [main] INFO  c.t.e.r.processor.Documen[illegible]ocessor - Number of queries for deleted documents:     3617
15:36:10.058 [main] INFO  c.t.e.r.processor.Docu[illegible]rocessor - Language unidentified for 179 of 838 docs: 21.360382%
```

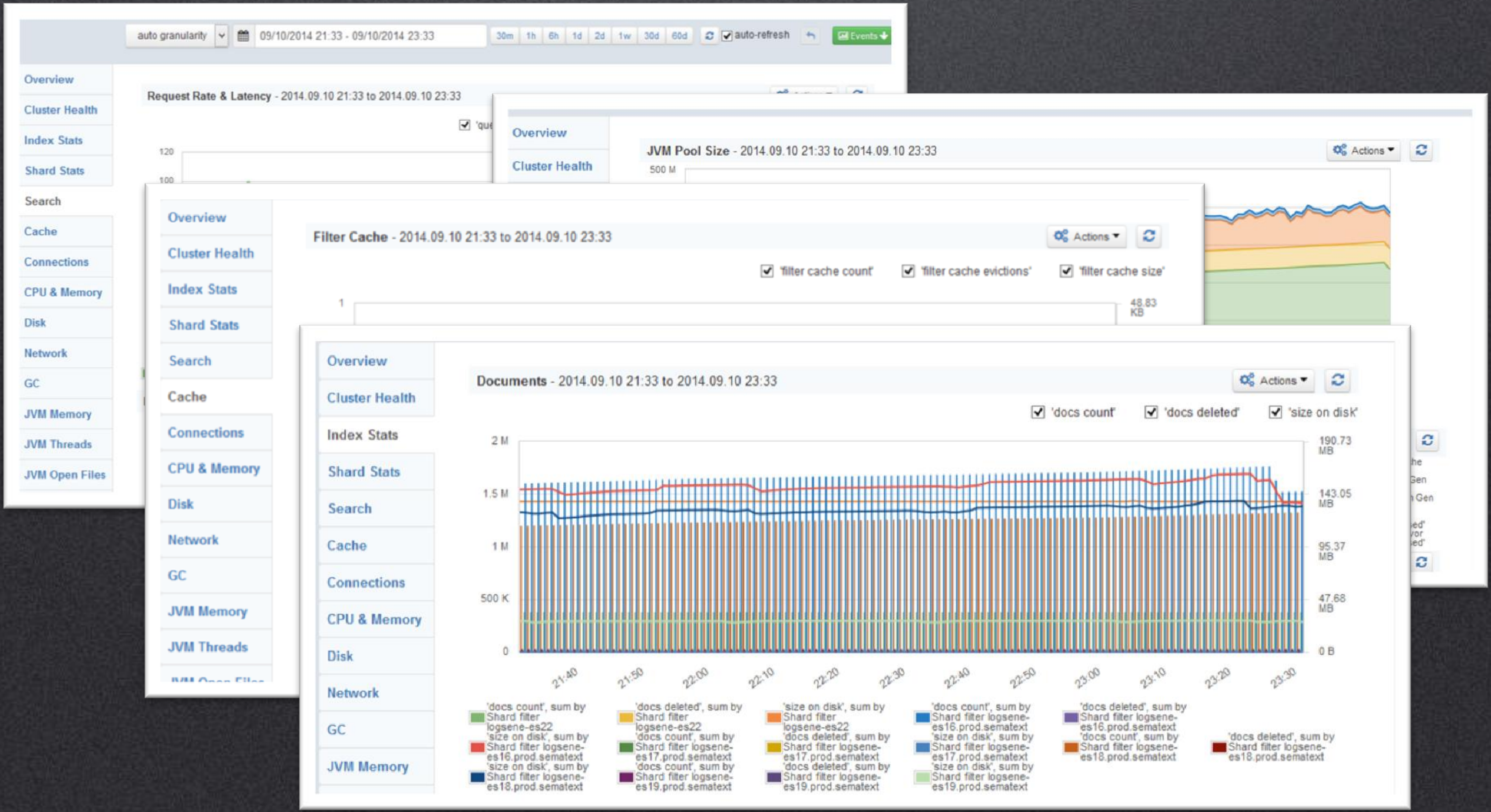
Logsene.Prod.ElasticSearch

auto granularity

09/10/2014 21:29 - 09/10/2014 23:29

☑ auto-refresh

SPM

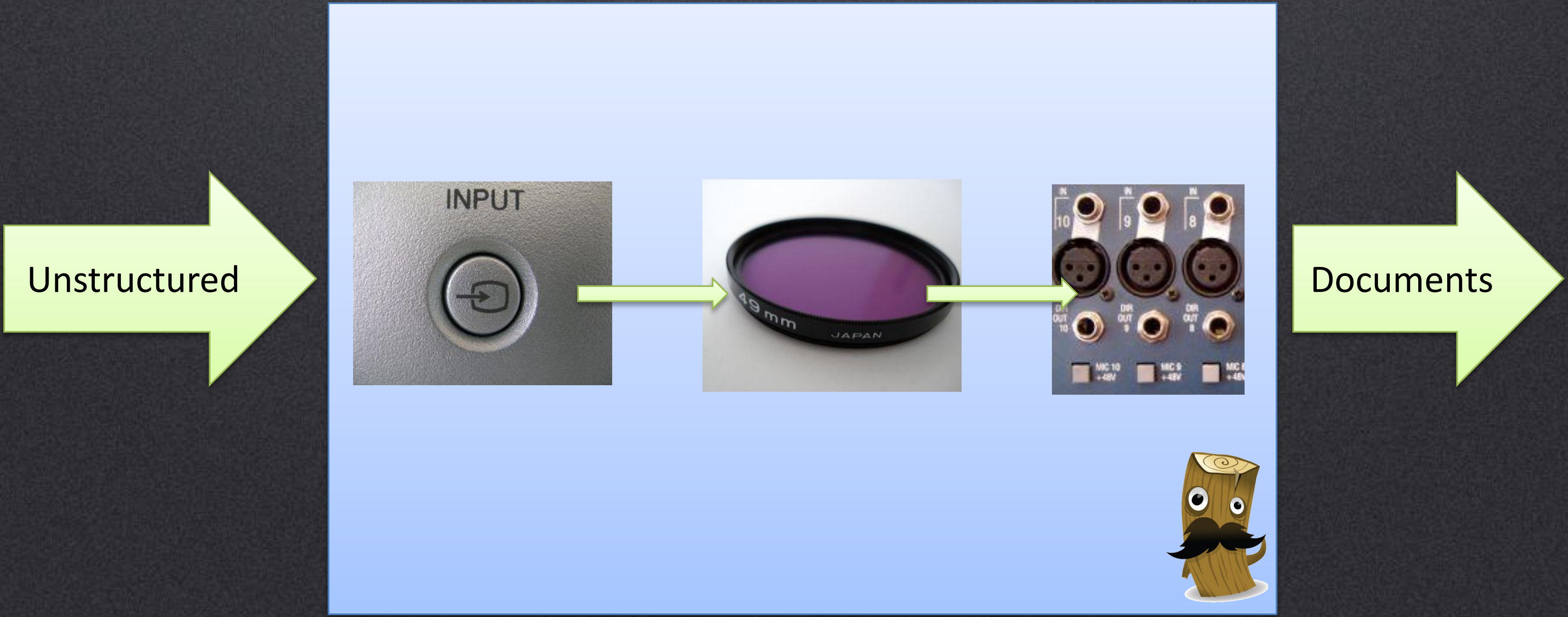


auto granularity
09/10/2014 21:33 - 09/10/2014 23:33
30m 1h 6h 1d 2d 1w 30d 60d
auto-refresh
Events
Overview
Cluster Health
Index Stats
Shard Stats
Search
Cache
Connections
CPU & Memory
Disk
Network
GC
JVM Memory
JVM Threads
JVM Open Files
Request Rate & Latency - 2014.09.10 21:33 to 2014.09.10 23:33
JVM Pool Size - 2014.09.10 21:33 to 2014.09.10 23:33
500 M
Actions
Filter Cache - 2014.09.10 21:33 to 2014.09.10 23:33
☑ 'filter cache count' ☑ 'filter cache evictions' ☑ 'filter cache size'
48.83 KB
Documents - 2014.09.10 21:33 to 2014.09.10 23:33
☑ 'docs count' ☑ 'docs deleted' ☑ 'size on disk'
2 M
1.5 M
1 M
500 K
0
190.73 MB
143.05 MB
95.37 MB
47.68 MB
0 B
21:40 21:50 22:00 22:10 22:20 22:30 22:40 22:50 23:00 23:10 23:20 23:30
'docs count', sum by Shard filter logsene-es22
'docs deleted', sum by Shard filter logsene-es22
'size on disk', sum by Shard filter logsene-es22
'docs count', sum by Shard filter logsene-es16.prod.sematext
'docs deleted', sum by Shard filter logsene-es16.prod.sematext
'size on disk', sum by Shard filter logsene-es16.prod.sematext
'docs count', sum by Shard filter logsene-es17.prod.sematext
'docs deleted', sum by Shard filter logsene-es17.prod.sematext
'size on disk', sum by Shard filter logsene-es17.prod.sematext
'docs count', sum by Shard filter logsene-es18.prod.sematext
'docs deleted', sum by Shard filter logsene-es18.prod.sematext
'size on disk', sum by Shard filter logsene-es18.prod.sematext
'docs count', sum by Shard filter logsene-es19.prod.sematext
'docs deleted', sum by Shard filter logsene-es19.prod.sematext
'size on disk', sum by Shard filter logsene-es19.prod.sematext

http://sematext.com/spm/

sematext

Przychodzi Logstash do lekarza…



Unstructured

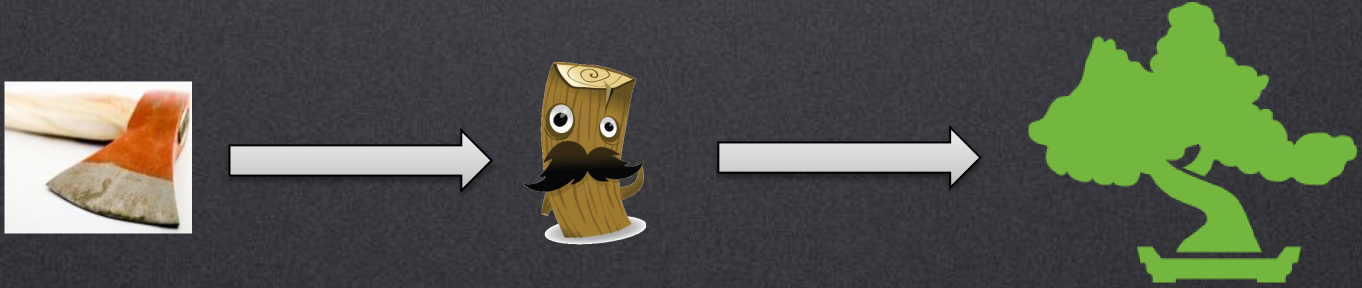
Documents

Przykład

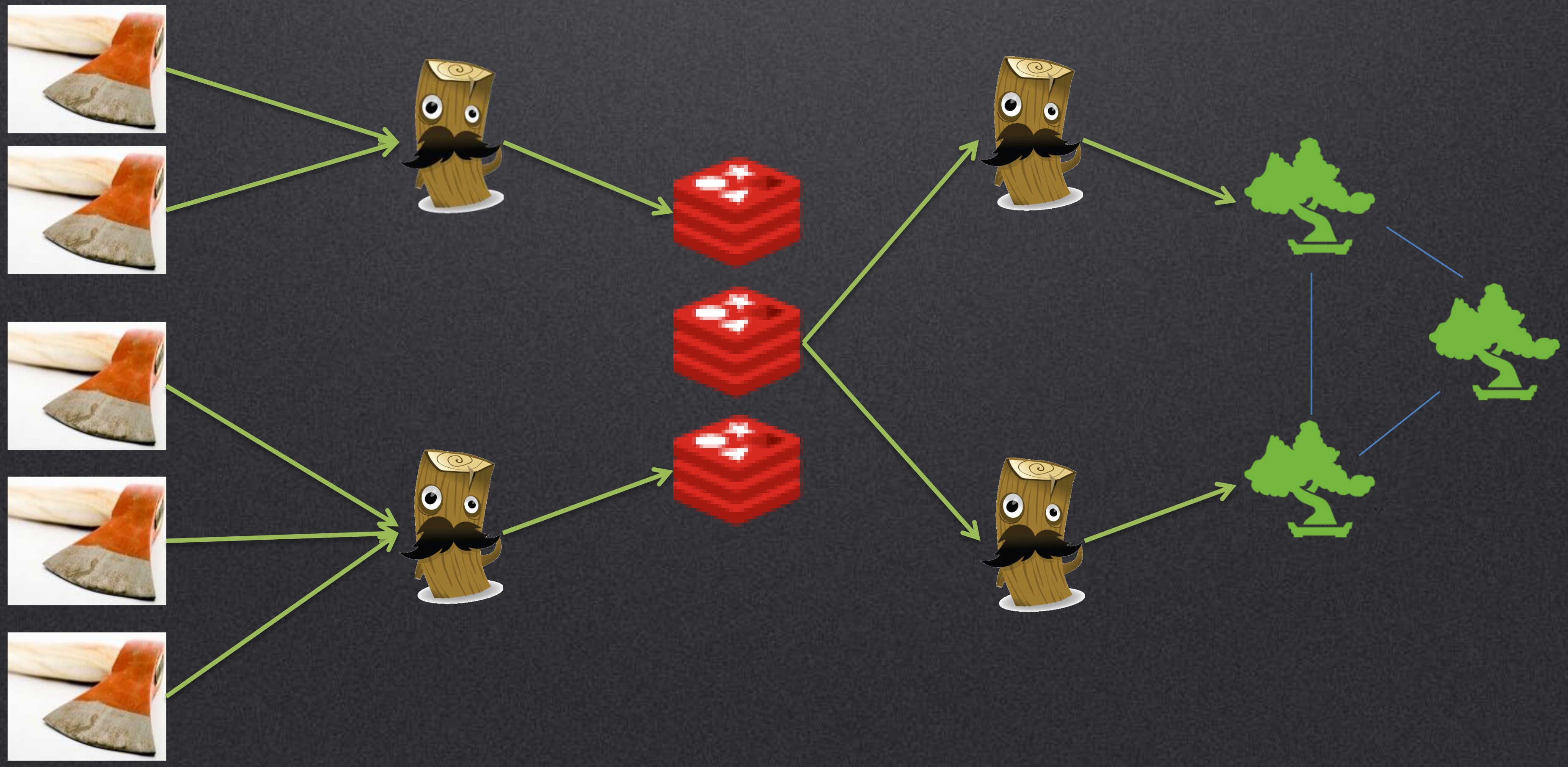
127.0.0.1 - - [05/Feb/2014:17:11:55 +0000] "GET /css/main.css HTTP/1.1" 200 140 "http://www.onet.pl" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1"

```
{
 "host" : "127.0.0.1",
 "@timestamp" : "2014-02-05T17:11:55+0000",
 ...
 "verb" : "GET"
}
```

Jak to wygląda?



To się także skaluje



Logstash input

```
input {
  file {
    path => "/var/log/apache/apache.log"
    type => "access_apache_log"
    start_position => "beginning"
  }
}
```

Grok

```
filter {
  if [type] == "access_apache_log"  {
    grok {
      match => {
        "message" => "%{COMBINEDAPACHELOG}"
      }
    }
  }
}
```

Logstash output

```
output {
  elasticsearch {
    host => "localhost"
    port => 9200
    index => "logs_%{+YYYY.MM.dd}"
    protocol => "http"
    manage_template => true
  }
}
```

Przykładowa konfiguracja Logstash-forwarder

```
{
  "network": {
    "servers": [ "localhost:5043" ],
    "timeout": 15
  },
  "files": [
    {
      "paths": [
        "/var/log/apache/apache*.log"
      ],
      "fields": { "type": "access_apache_log" }
    }
  ]
}
```

```
Logstash side:

input {
  lumberjack {
    port => 5043
    type => "access_apache_log"
  }
}
```

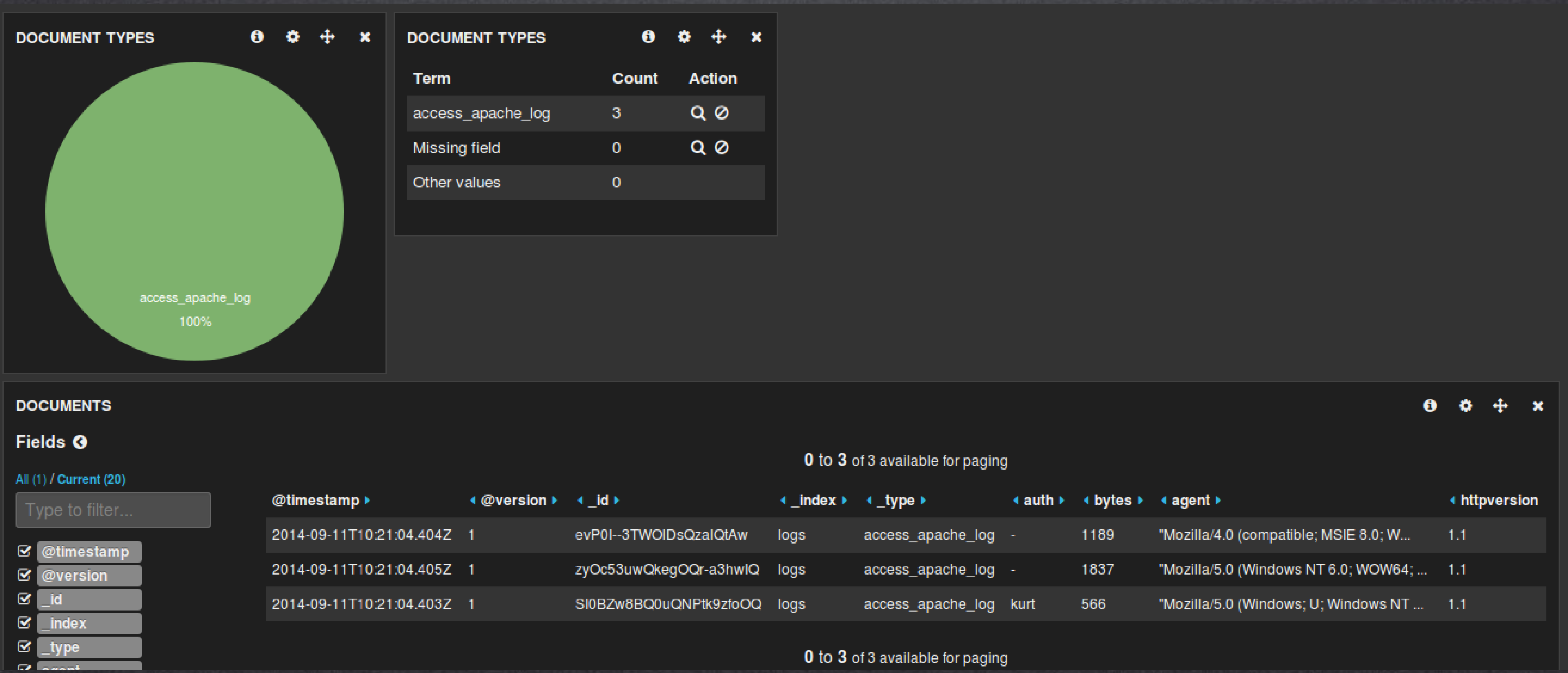
Spróbujmy tak to działa

```
$ bin/logstash –f logstash-filter.conf
```

```
$ curl 'localhost:9200/logs_2014-09-26/_search?pretty'
```

```
{
  "took" : 3,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "failed" : 0
  },
  "hits" : {
    "total" : 3,
    "max_score" : 1.0,
    "hits" : [ {
      "_index" : "logs",
      "_type" : "access_apache_log",
      "_id" : "SI0BZw8BQ0uQNPtk9zfoOQ",
      "_score" : 1.0,
      "_source":{"message":"71.141.244.242 - kurt [18/May/2011:01:48:10 -0700] \"GET /admin HTTP/1.1\" 301 566 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401
Firefox/3.6.3\"","@version":"1","@timestamp":"2014-09-11T10:21:04.403Z","type":"access_apache_log","host":"developer-vb","path":"/home/gro/devops/apache3.log","clientip":"71.141.244.242","ident":"-
","auth":"kurt","timestamp":"18/May/2011:01:48:10 -0700","verb":"GET","request":"/admin","httpversion":"1.1","response":"301","bytes":"566","referrer":"\"-\"","agent":"\"Mozilla/5.0 (Windows; U;
Windows NT 5.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3\""}
    }, {
      "_index" : "logs",
      "_type" : "access_apache_log",
      "_id" : "zyOc53uwQkegOQr-a3hwIQ",
      "_score" : 1.0,
      "_source":{"message":"98.83.179.51 - - [18/May/2011:19:35:08 -0700] \"GET /css/main.css HTTP/1.1\" 200 1837 \"http://www.safesand.com/information.htm\" \"Mozilla/5.0 (Windows NT 6.0; WOW64;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1\"","@version":"1","@timestamp":"2014-09-11T10:21:04.405Z","type":"access_apache_log","host":"developer-
vb","path":"/home/gro/devops/apache3.log","clientip":"98.83.179.51","ident":"-","auth":"-","timestamp":"18/May/2011:19:35:08 -
0700","verb":"GET","request":"/css/main.css","httpversion":"1.1","response":"200","bytes":"1837","referrer":"\"http://www.safesand.com/information.htm\"","agent":"\"Mozilla/5.0 (Windows NT 6.0; WOW64;
rv:2.0.1) Gecko/20100101 Firefox/4.0.1\""}
    }, {
      "_index" : "logs",
      "_type" : "access_apache_log",
      "_id" : "evP0I--3TWOlDsQzalQtAw",
      "_score" : 1.0,
      "_source":{"message":"134.39.72.245 - - [18/May/2011:12:40:18 -0700] \"GET /favicon.ico HTTP/1.1\" 200 1189 \"-\" \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2; .NET4.0C; .NET4.0E)\"","@version":"1","@timestamp":"2014-09-11T10:21:04.404Z","type":"access_apache_log","host":"developer-
vb","path":"/home/gro/devops/apache3.log","clientip":"134.39.72.245","ident":"-","auth":"-","timestamp":"18/May/2011:12:40:18 -
0700","verb":"GET","request":"/favicon.ico","httpversion":"1.1","response":"200","bytes":"1189","referrer":"\"-\"","agent":"\"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2; .NET4.0C; .NET4.0E)\""}
    } ]
  }
}
```

Czas na wizualizację



DOCUMENT TYPES

Term	Count	Action
access_apache_log	3	🔍 ⊘
Missing field	0	🔍 ⊘
Other values	0	

DOCUMENTS

Fields

All (1) / Current (20)

Type to filter...

☑ @timestamp
☑ @version
☑ _id
☑ _index
☑ _type
☑ agent

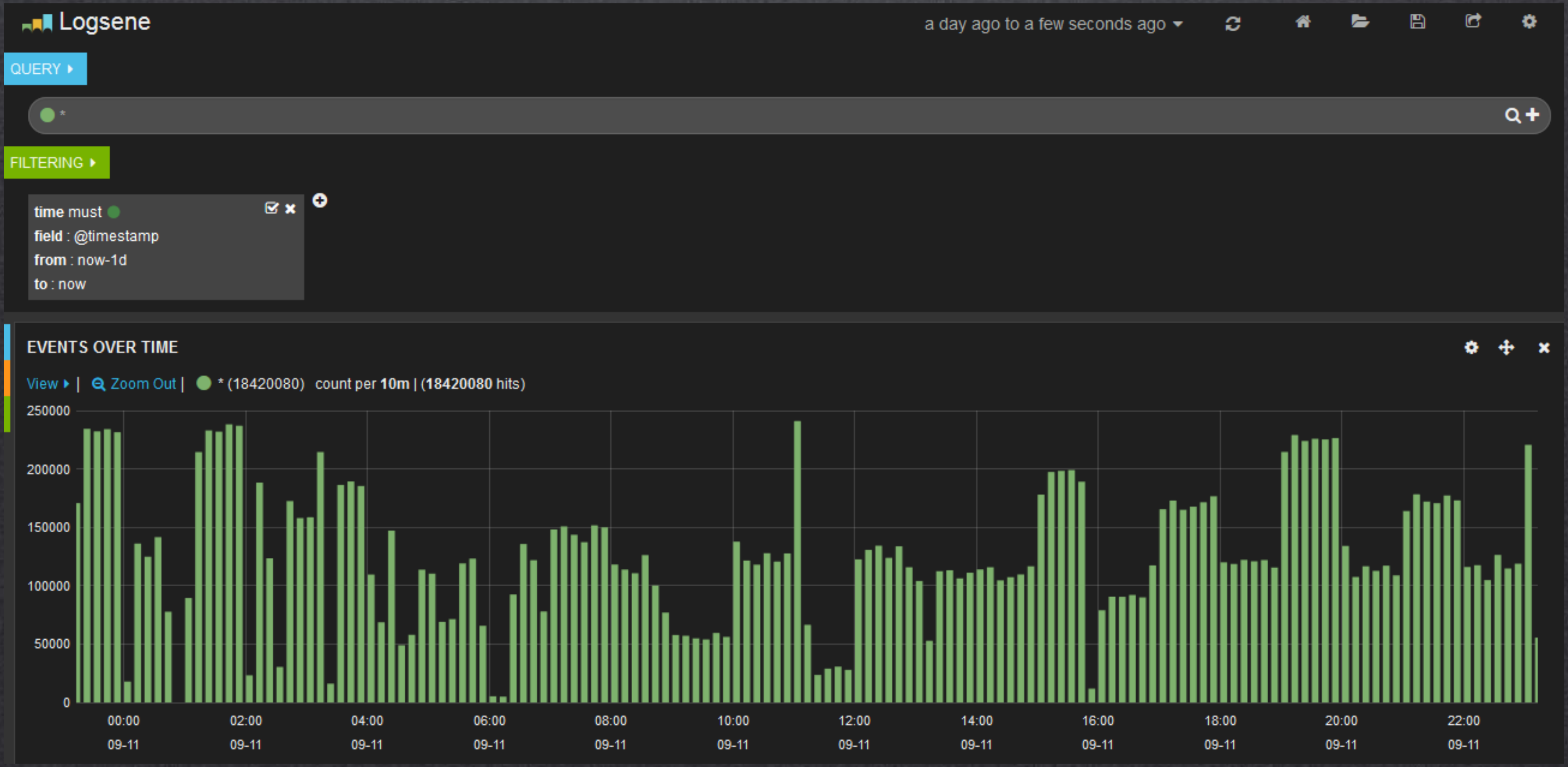
0 to **3** of 3 available for paging

@timestamp	@version	_id	_index	_type	auth	bytes	agent	httpversion
2014-09-11T10:21:04.404Z	1	evP0I--3TWOIDsQzaIQtAw	logs	access_apache_log	-	1189	"Mozilla/4.0 (compatible; MSIE 8.0; W...	1.1
2014-09-11T10:21:04.405Z	1	zyOc53uwQkegOQr-a3hwIQ	logs	access_apache_log	-	1837	"Mozilla/5.0 (Windows NT 6.0; WOW64; ...	1.1
2014-09-11T10:21:04.403Z	1	SI0BZw8BQ0uQNPtk9zfoOQ	logs	access_apache_log	kurt	566	"Mozilla/5.0 (Windows; U; Windows NT ...	1.1

0 to **3** of 3 available for paging

sematext

SaaS == Logsene



time must ●
field : @timestamp
from : now-1d
to : now

● * (18420080) count per 10m | (18420080 hits)

sematext

http://sematext.com/logsene

Logstash + Logsene w akcji

```
output {
  elasticsearch {
    host => "logsene-receiver.sematext.com"
    port => 80
    index => "YOUR_TOKEN"
    protocol => "http"
    manage_template => false
  }
}
```

Krótkie podsumowanie

sematext

http://www.soothetube.com/2013/12/29/thats-all-folks/

Ktoś szuka pracy?

Dig Search ?

Dig Analytics ?

Dig Big Data ?

Dig Performance ?

Dig Logging ?

Dig working with and in open – source ?

We’re hiring world – wide !

http://sematext.com/about/jobs.html

sematext

Dziękuję :)

Rafał Kuć

@kucrafal

rafal.kuc@sematext.com

Sematext

@sematext

http://sematext.com

http://blog.sematext.com

sematext