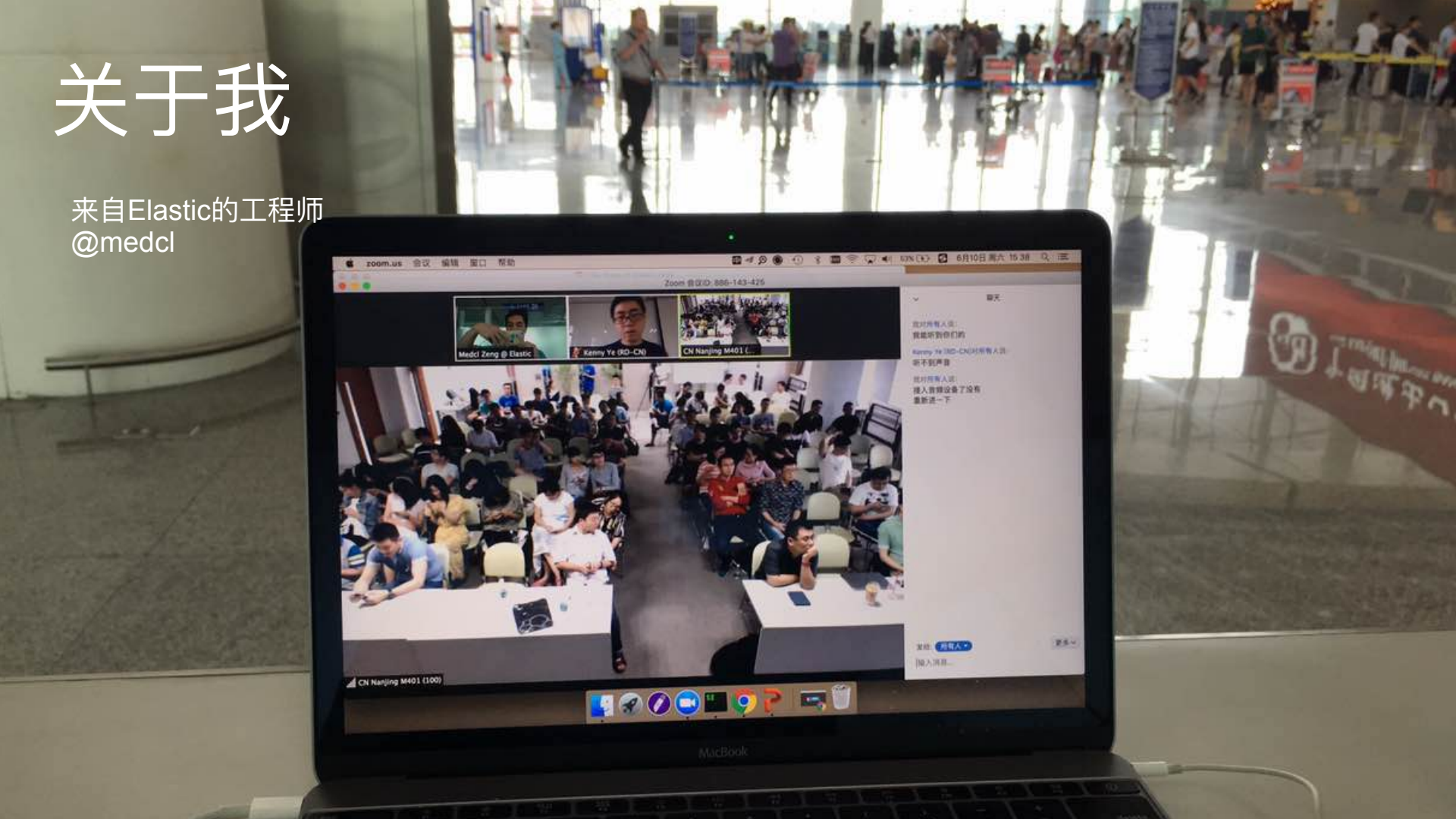


Elastic 探秘之遗落的珍珠

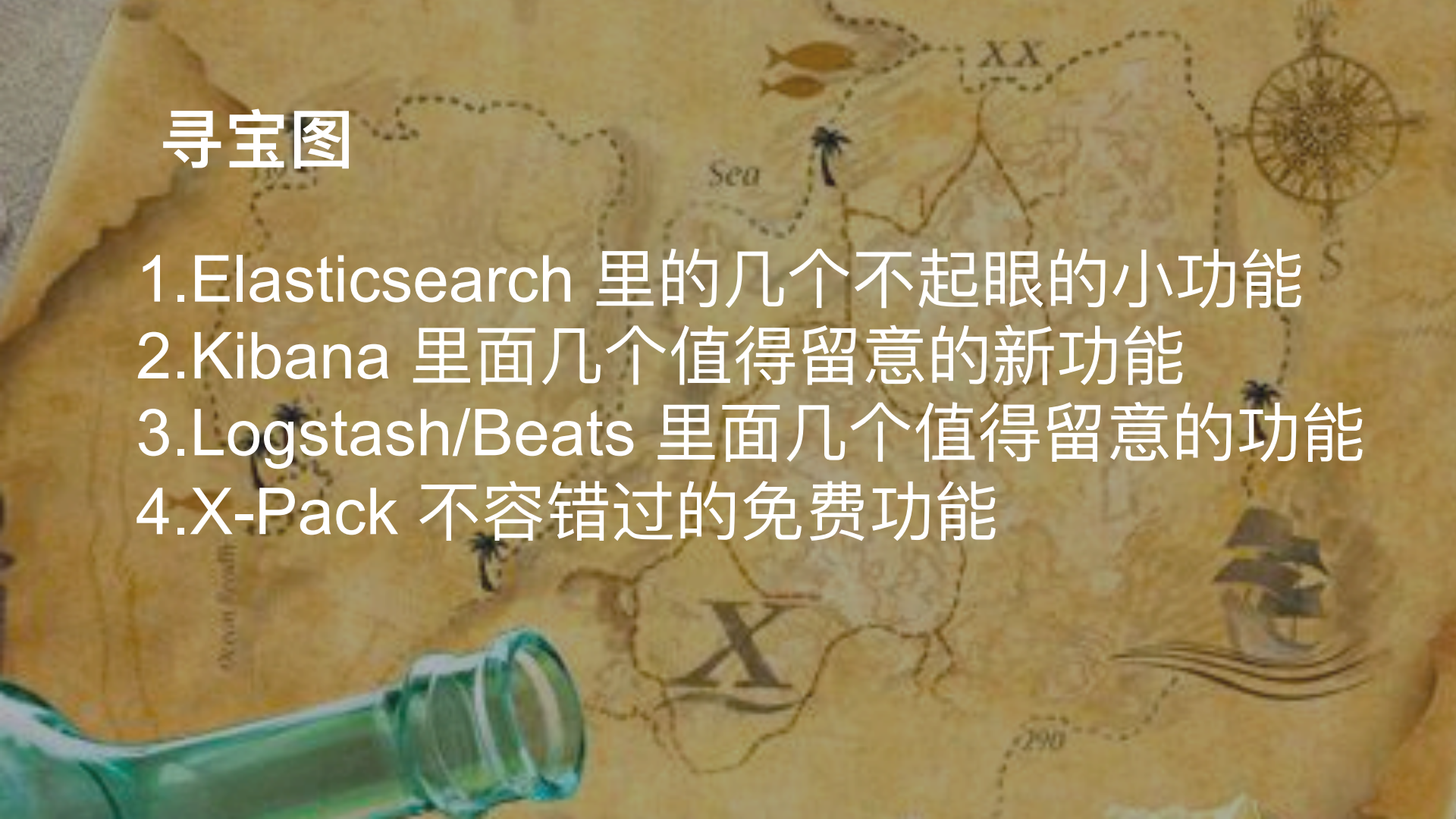

elastic
Elastic 探秘之遗落的功能

关于我

来自Elastic的工程师
@medcl




elastic
世界领先的开源软件提供商
加入我们：http://grnh.se/iup1q61


寻宝图
1.Elasticsearch 里的几个不起眼的小功能
2.Kibana 里面几个值得留意的新功能
3.Logstash/Beats 里面几个值得留意的功能
4.X-Pack 不容错过的免费功能
XX
Sea
X





elasticsearch

Query 1

```
CREATE TABLE `aws_answer` (
  `answer_id` int(11) NOT NULL AUTO_INCREMENT COMMENT '回答id',
  `question_id` int(11) NOT NULL COMMENT '问题id',
  `answer_content` text COMMENT '回答内容',
  `add_time` int(10) DEFAULT '0' COMMENT '添加时间',
  `against_count` int(11) NOT NULL DEFAULT '0' COMMENT '反对人数',
  `agree_count` int(11) NOT NULL DEFAULT '0' COMMENT '支持人数',
  `uid` int(11) DEFAULT '0' COMMENT '发布问题用户ID',
  `comment_count` int(11) DEFAULT '0' COMMENT '评论总数',
  `uninterested_count` int(11) DEFAULT '0' COMMENT '不感兴趣',
  `thanks_count` int(11) DEFAULT '0' COMMENT '感谢数量',
  `category_id` int(11) DEFAULT '0' COMMENT '分类id',
  `has_attach` tinyint(1) DEFAULT '0' COMMENT '是否存在附件',
  `ip` bigint(11) DEFAULT NULL,
  `force_fold` tinyint(1) DEFAULT '0' COMMENT '强制折叠',
  `anonymous` tinyint(1) DEFAULT '0',
  `publish_source` varchar(16) DEFAULT NULL,
  PRIMARY KEY (`answer_id`),
  KEY `publich_source` (`publish_source`)
) ENGINE=InnoDB AUTO_INCREMENT=716 DEFAULT CHARSET=utf8 COMMENT='回答';
```

Meta Field

GET mapping
PUT mapping

```
PUT my_index
{
  "mappings": {
    "doc": {
      "_meta": {
        "database": "localhost",
        "table_name": "aws_answer",
        "comments": {
          "answer_id": "回答id",
          "question_id": "问题id",
          "answer_content": "回答内容"
        },
        "schema_version": {
          "ver": "1.0",
          "date": "2018-06-25"
        },
        "operator": "medcl"
      }
    }
  }
}
```

Index Sorting

提升排序性能
更好的压缩比
更少的磁盘

```
PUT twitter
{
    "settings" : {
        "index" : {
            "sort.field" : "date",
            "sort.order" : "desc"
        }
    },
    "mappings": {⟺}
}
```

Adaptive Replica Selection

```
PUT /_cluster/settings
{
    "transient": {
        "cluster.routing.use_adaptive_replica_selection": true
    }
}
```

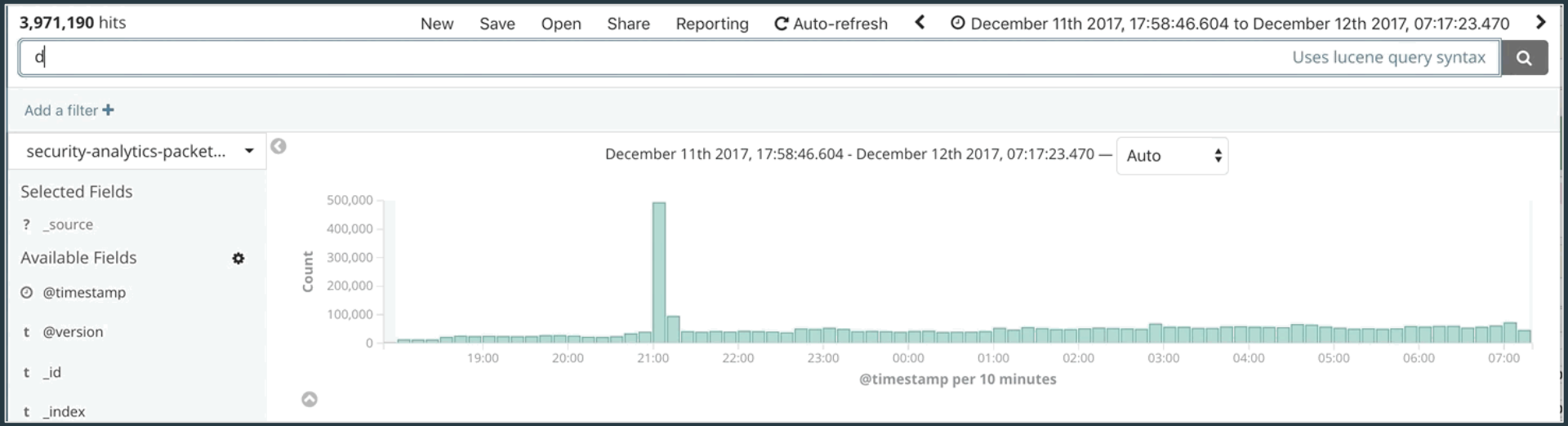
依次轮询 -> 智能的选择副本进行查询





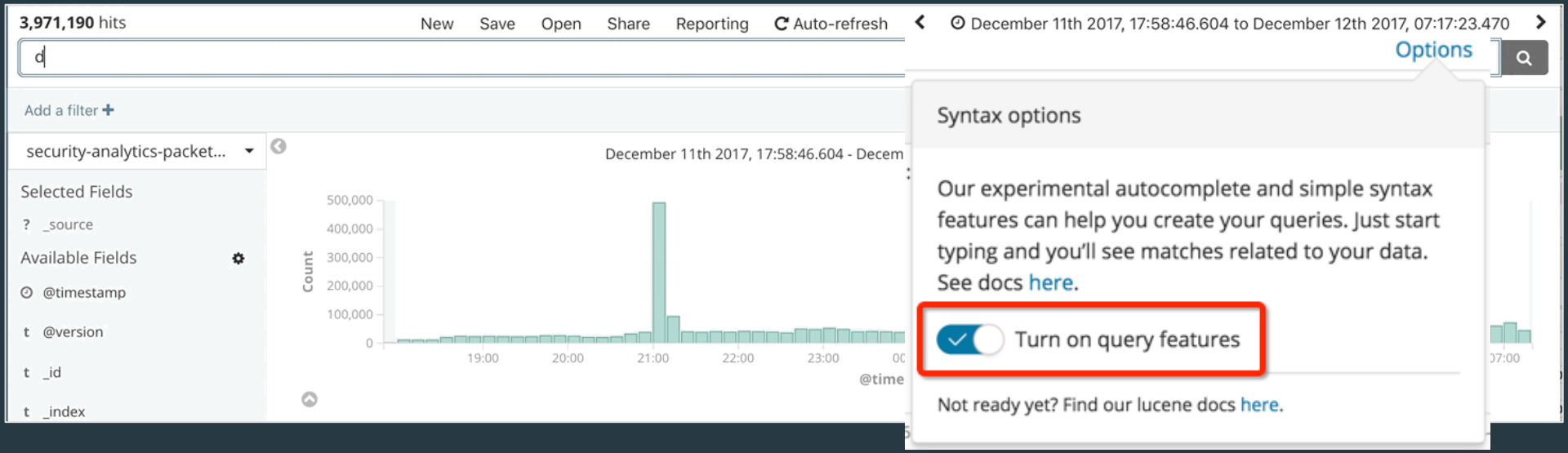
kibana

Kuery + Autocomplete



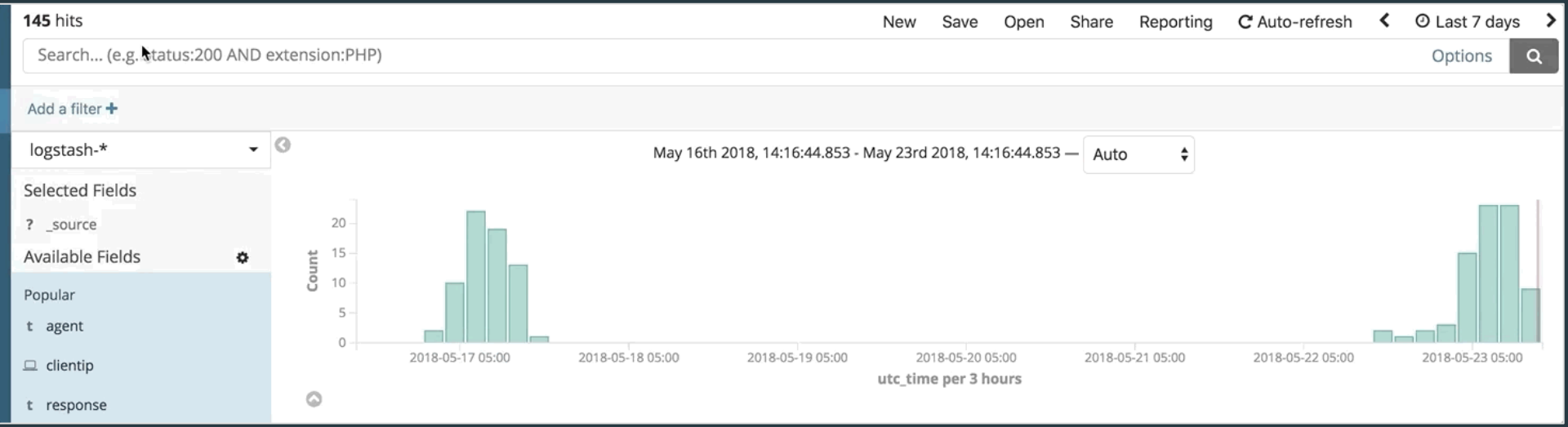
默认

Kuery + Autocomplete



开启

Kuery + Autocomplete

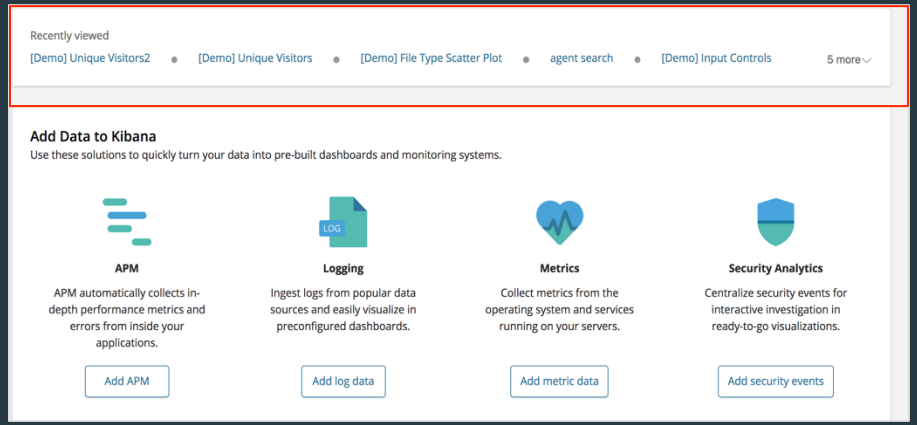


开启后

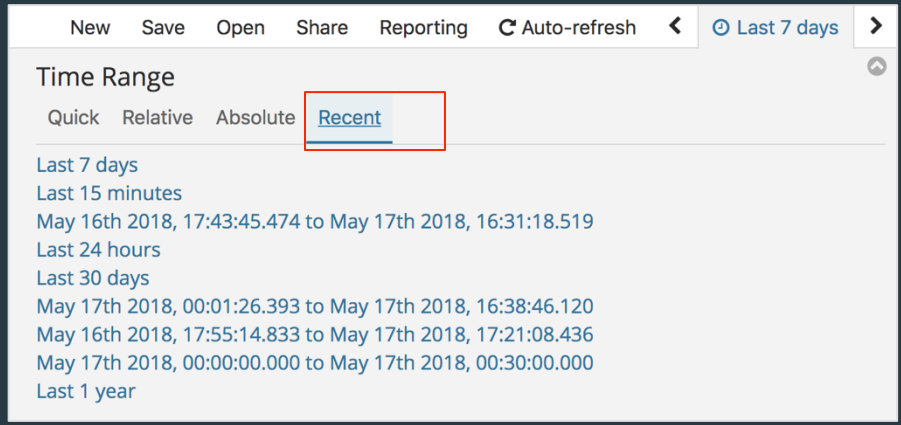
Recently Viewed and Recent Time Range

Where was I...

Recently viewed objects



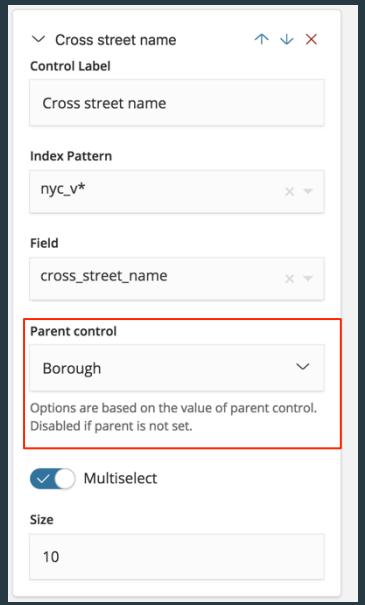
Recently used time range

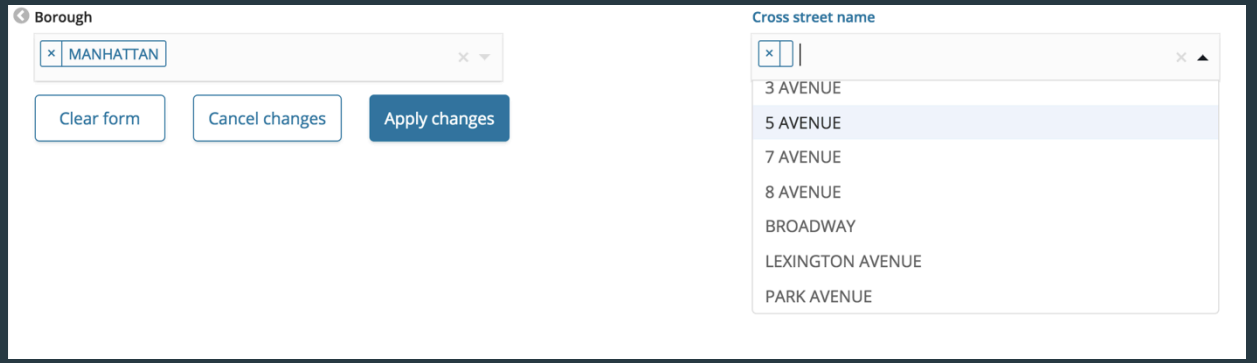


Chained Input Control

Remember Input Control?

- The first input control filters the values for the second input control

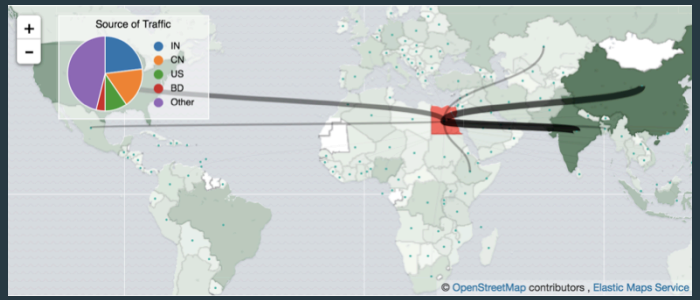




Geo

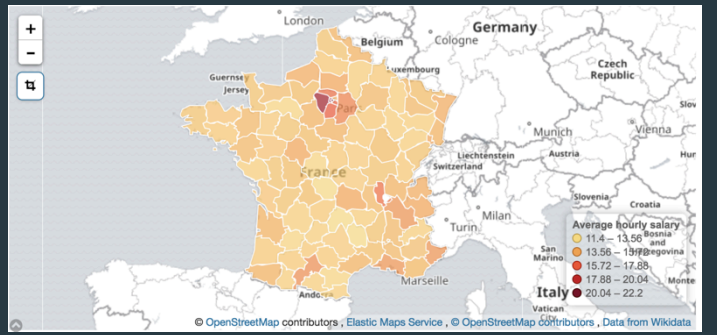
Vega:

- Support for Vega base map
- Create interactive highly customizable maps

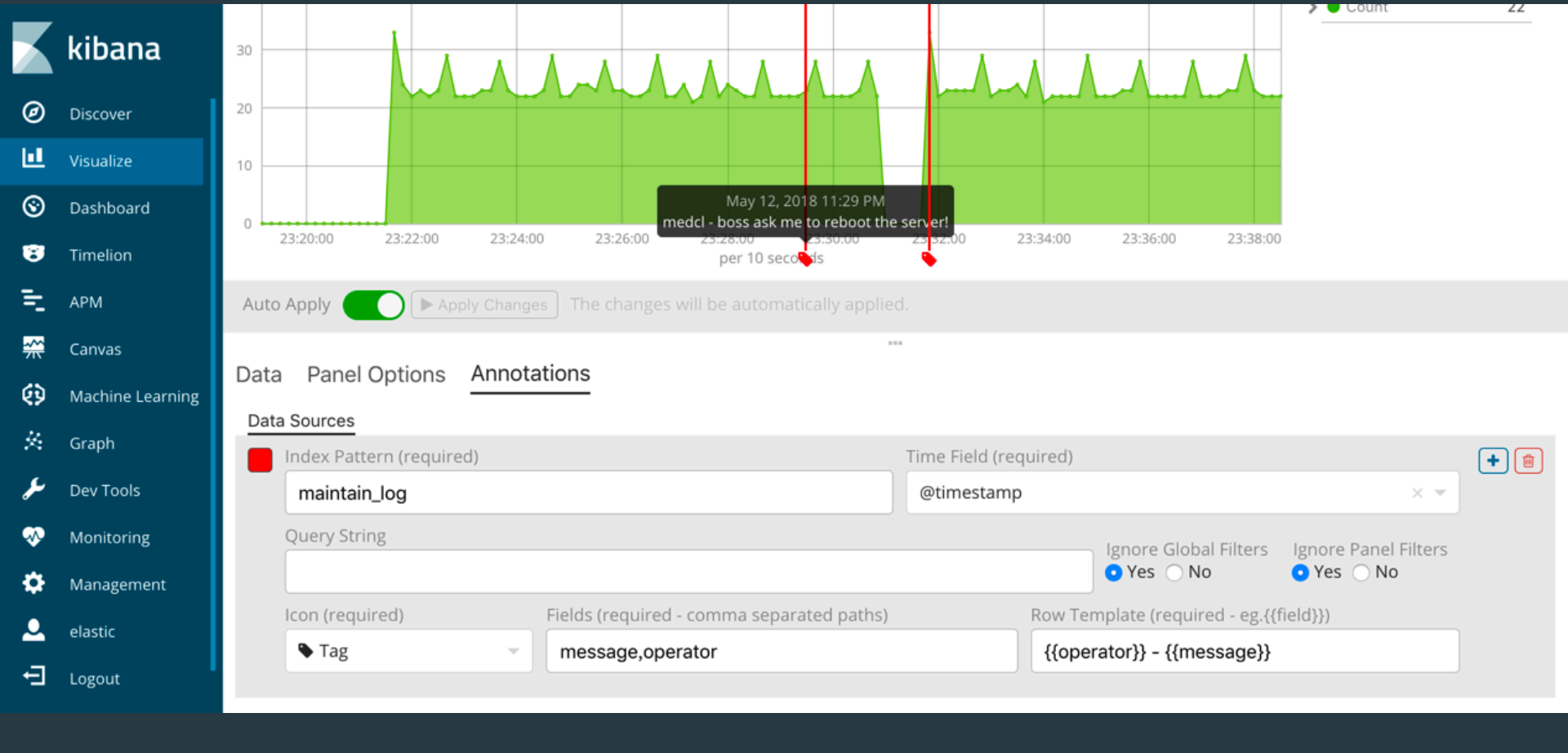


Region maps:

- 2 new vector maps China provinces and France departments



TSVB 注解


kibana
Discover
Visualize
Dashboard
Timelion
APM
Canvas
Machine Learning
Graph
Dev Tools
Monitoring
Management
elastic
Logout
30
20
10
0
23:20:00
23:22:00
23:24:00
23:26:00
23:34:00
23:36:00
23:38:00
May 12, 2018 11:29 PM
medcl - boss ask me to reboot the server!
per 10 seconds
Count
22
Auto Apply
Apply Changes
The changes will be automatically applied.
Data
Panel Options
Annotations
Data Sources
Index Pattern (required)
maintain_log
Time Field (required)
@timestamp
Query String
Ignore Global Filters
Yes
No
Ignore Panel Filters
Yes
No
Icon (required)
Tag
Fields (required - comma separated paths)
message,operator
Row Template (required - eg.{{field}})
{{operator}} - {{message}}

使用 API 来创建 Index Pattern

```
curl -X POST http://localhost:5601/api/
saved_objects/index-pattern/my-pattern  -H 'kbn-xsrf:
true' -H 'Content-Type: application/json' –d’
  {
  "attributes": {
      "title": "my-pattern-*"
  }
}'
```





logstash



beats

Dissect filter

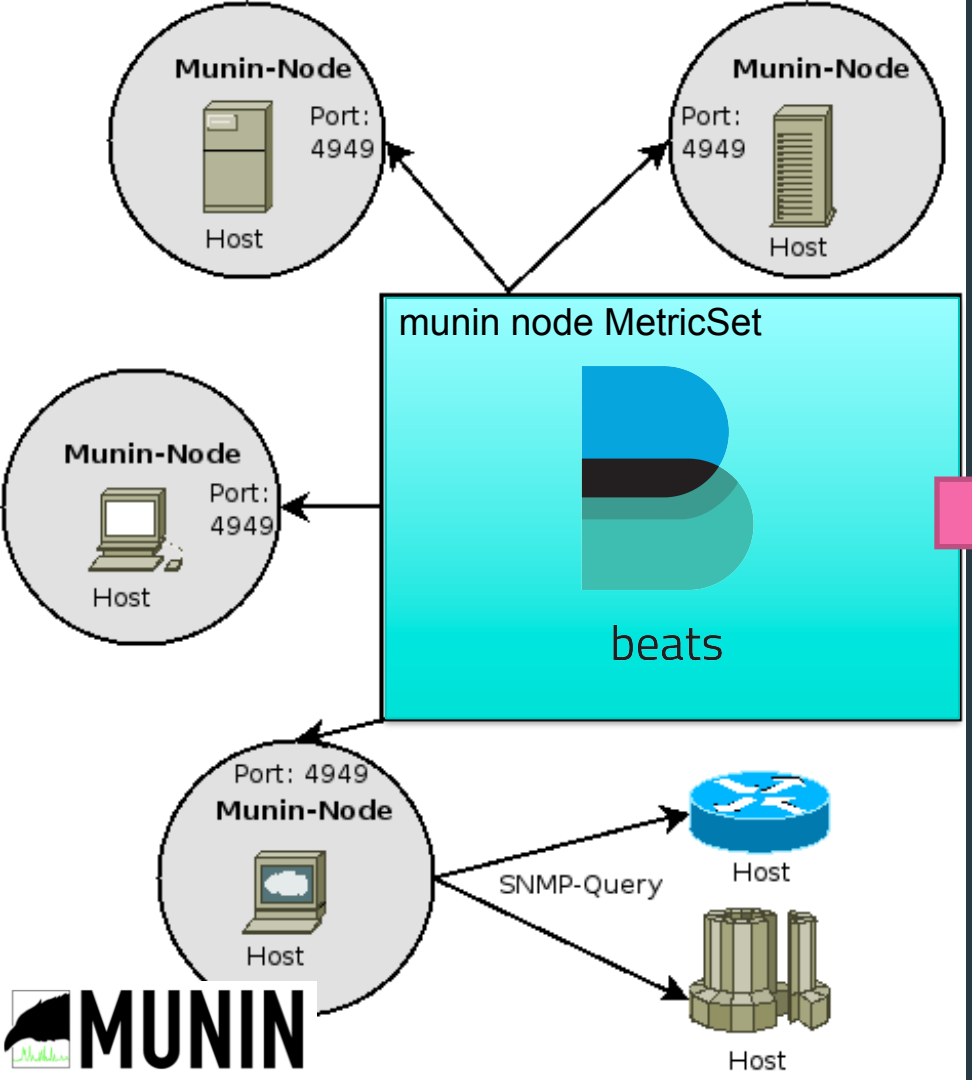
```
filter {
    dissect {
      mapping => {
        "message" => “%{name},%{addr1},%{addr2},%{addr3},%{city},%{zip}"
      }
    }
  }
```

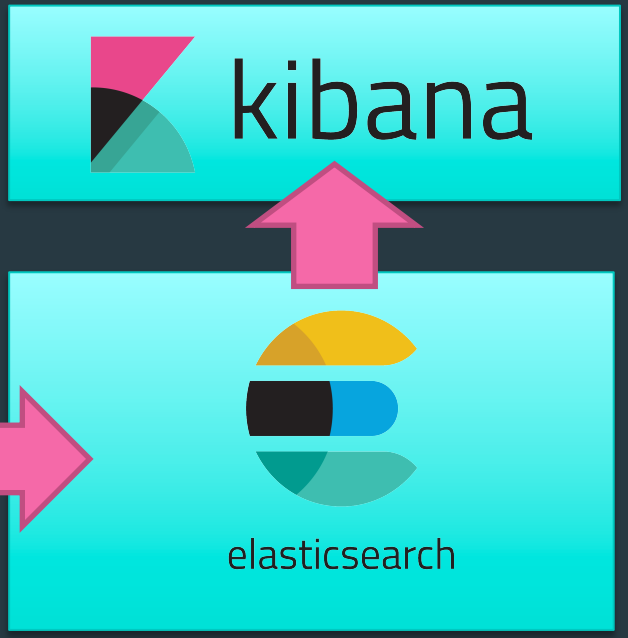
输入：Jane Doe,4321 Fifth Avenue,,,New York,87432

输出：

```
{
          "name": "Jane Doe",
          "addr1": "4321 Fifth Avenue",
          "addr2": "",
          "addr3": "",
          "city": "New York"
          "zip": "87432"
}
```

https://www.elastic.co/guide/en/logstash/current/plugins-filters-dissect.html





历史悠久, started in 2002
跨平台, Perl 编写
插件丰富:

- http://gallery.munin-monitoring.org/index.html
- https://github.com/munin-monitoring/contrib/

Beats - Spooling to Disk (Beta)

- Persistence at the edge
  - Great for ephemeral data
  - Part of libbeat, OSS
- At-least-one delivery
- Spool is an alternative to in-memory queue (either, not both)
- Restarts from where it left off
- Size is max, but likely will use all

```
# ____beat.yml

queue:
  spool:

    file:
      path: "${path.data}/spool.dat"
      permissions: 0600  # One-time
      size: 100MiB       # One-time
      #prealloc: true    # One-time

    write:
      buffer_size: 1MiB
      flush.timeout: 1s
      flush.events: 16384
```





x-pack

Reporting
ine Learni
ger Canva
Monitoring CSV

X-PACK

PAID
FREE

OPEN

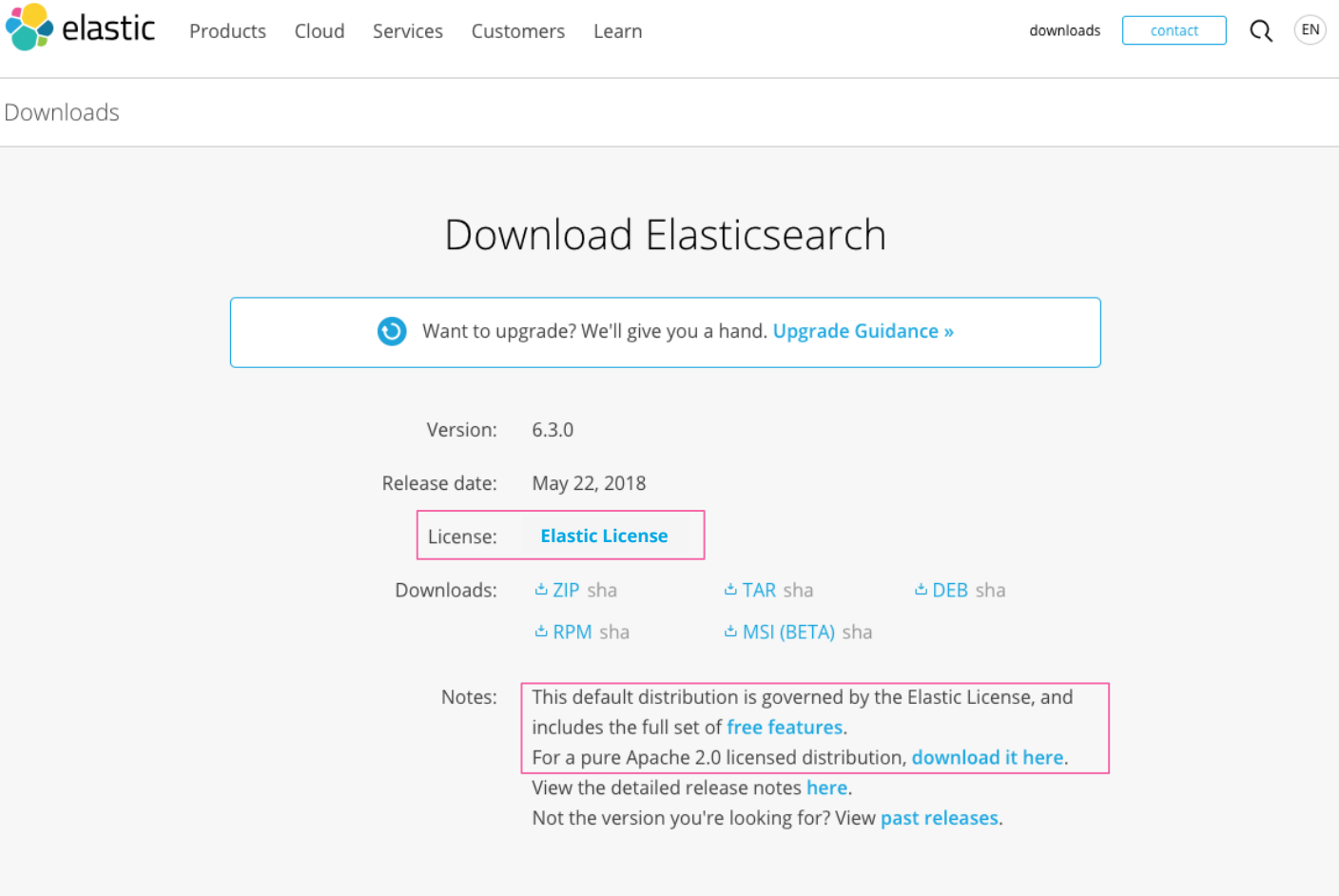
PRODUCT.ZIP

OPT IN
DEFAULT

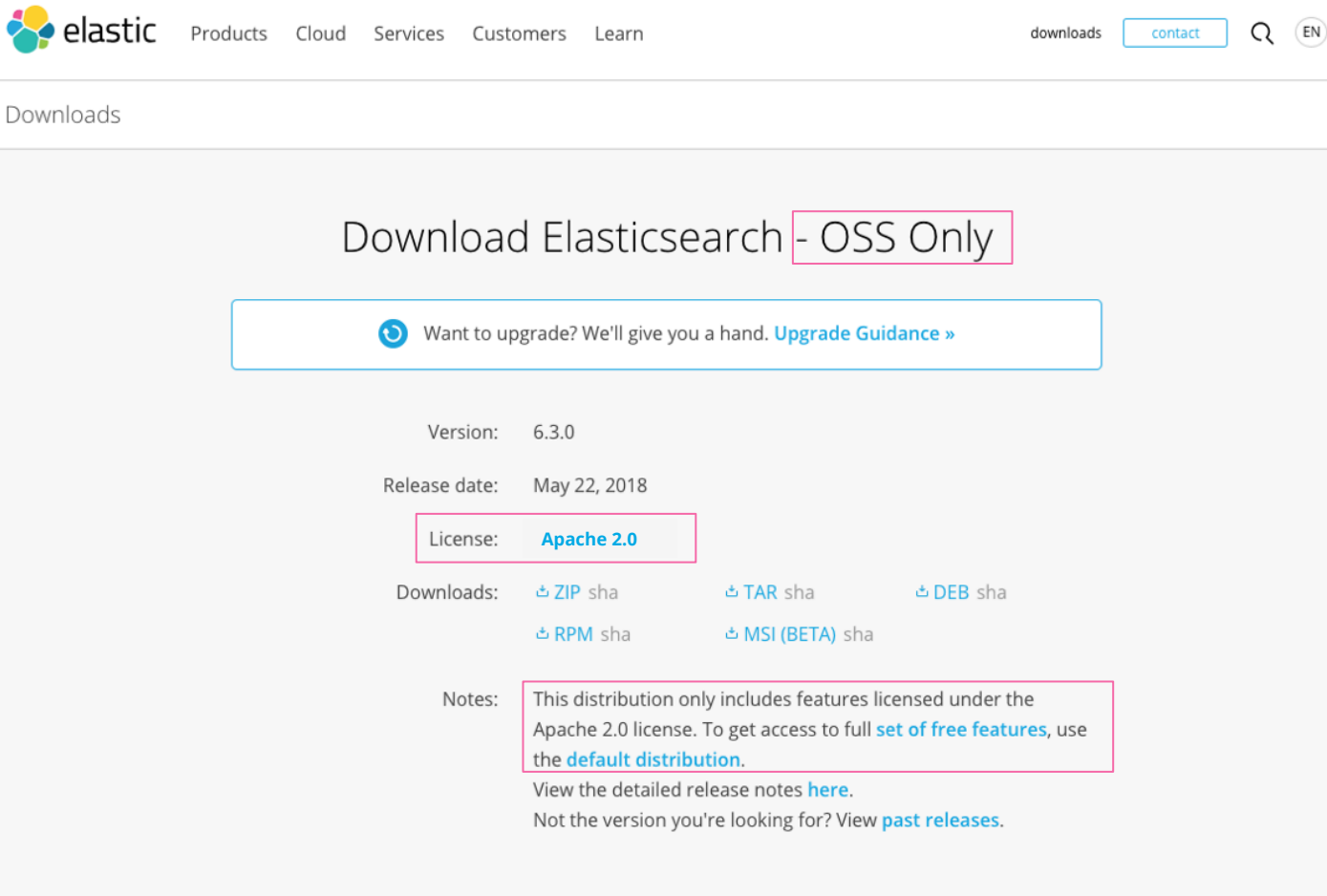
Ingestions
Distributed
Engine
Data Collection
Dashboard
Visualizations
Agents
Edge Collection
estions
Enrichment
Dashboard
ction
Distributed
Search Engine
Data Collection

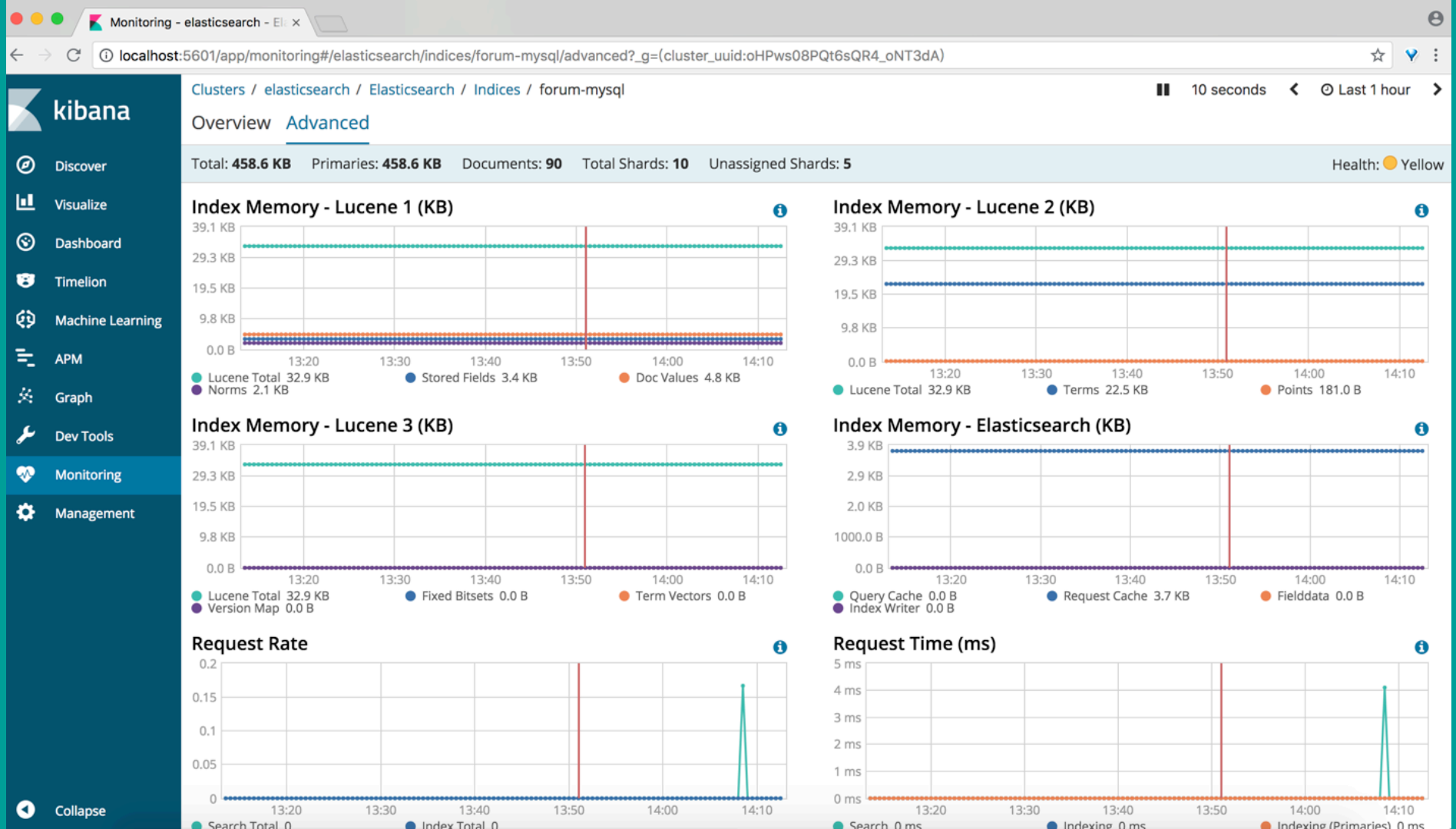
OSS

elastic.co/downloads/elasticsearch



elastic.co/downloads/elasticsearch-oss




Monitoring - elasticsearch - El
localhost:5601/app/monitoring#/elasticsearch/indices/forum-mysql/advanced?_g=(cluster_uuid:oHPws08PQt6sQR4_oNT3dA)
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
Collapse
Clusters / elasticsearch / Elasticsearch / Indices / forum-mysql
10 seconds
Last 1 hour
Overview
Advanced
Total: 458.6 KB
Primaries: 458.6 KB
Documents: 90
Total Shards: 10
Unassigned Shards: 5
Health: Yellow
Index Memory - Lucene 1 (KB)
39.1 KB
29.3 KB
19.5 KB
9.8 KB
0.0 B
13:20
13:30
13:40
13:50
14:00
14:10
Lucene Total 32.9 KB
Stored Fields 3.4 KB
Doc Values 4.8 KB
Norms 2.1 KB
Index Memory - Lucene 2 (KB)
39.1 KB
29.3 KB
19.5 KB
9.8 KB
0.0 B
13:20
13:30
13:40
13:50
14:00
14:10
Lucene Total 32.9 KB
Terms 22.5 KB
Points 181.0 B
Index Memory - Lucene 3 (KB)
39.1 KB
29.3 KB
19.5 KB
9.8 KB
0.0 B
13:20
13:30
13:40
13:50
14:00
14:10
Lucene Total 32.9 KB
Fixed Bitsets 0.0 B
Term Vectors 0.0 B
Version Map 0.0 B
Index Memory - Elasticsearch (KB)
3.9 KB
2.9 KB
2.0 KB
1000.0 B
0.0 B
13:20
13:30
13:40
13:50
14:00
14:10
Query Cache 0.0 B
Request Cache 3.7 KB
Fielddata 0.0 B
Index Writer 0.0 B
Request Rate
0.2
0.15
0.1
0.05
0
13:20
13:30
13:40
13:50
14:00
14:10
Search Total 0
Index Total 0
Request Time (ms)
5 ms
4 ms
3 ms
2 ms
1 ms
0 ms
13:20
13:30
13:40
13:50
14:00
14:10
Search 0 ms
Indexing 0 ms
Indexing (Primaries) 0 ms

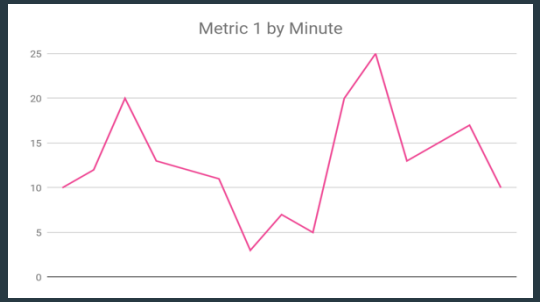
```
sql> SELECT description FROM features
WHERE product = 'elasticsearch' AND version =
'6.3.0';

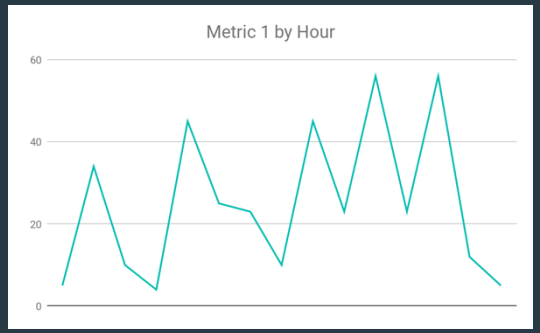
description
---------------
SQL
Data Rollups
Java 10 Support
```

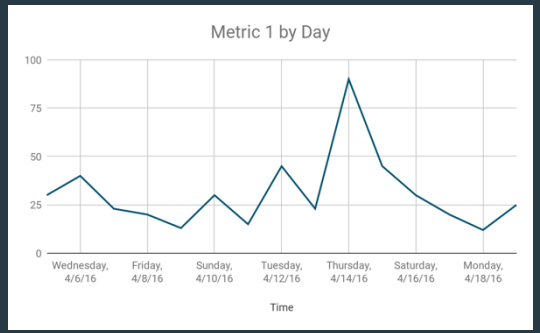
Rolling up Metricbeat data

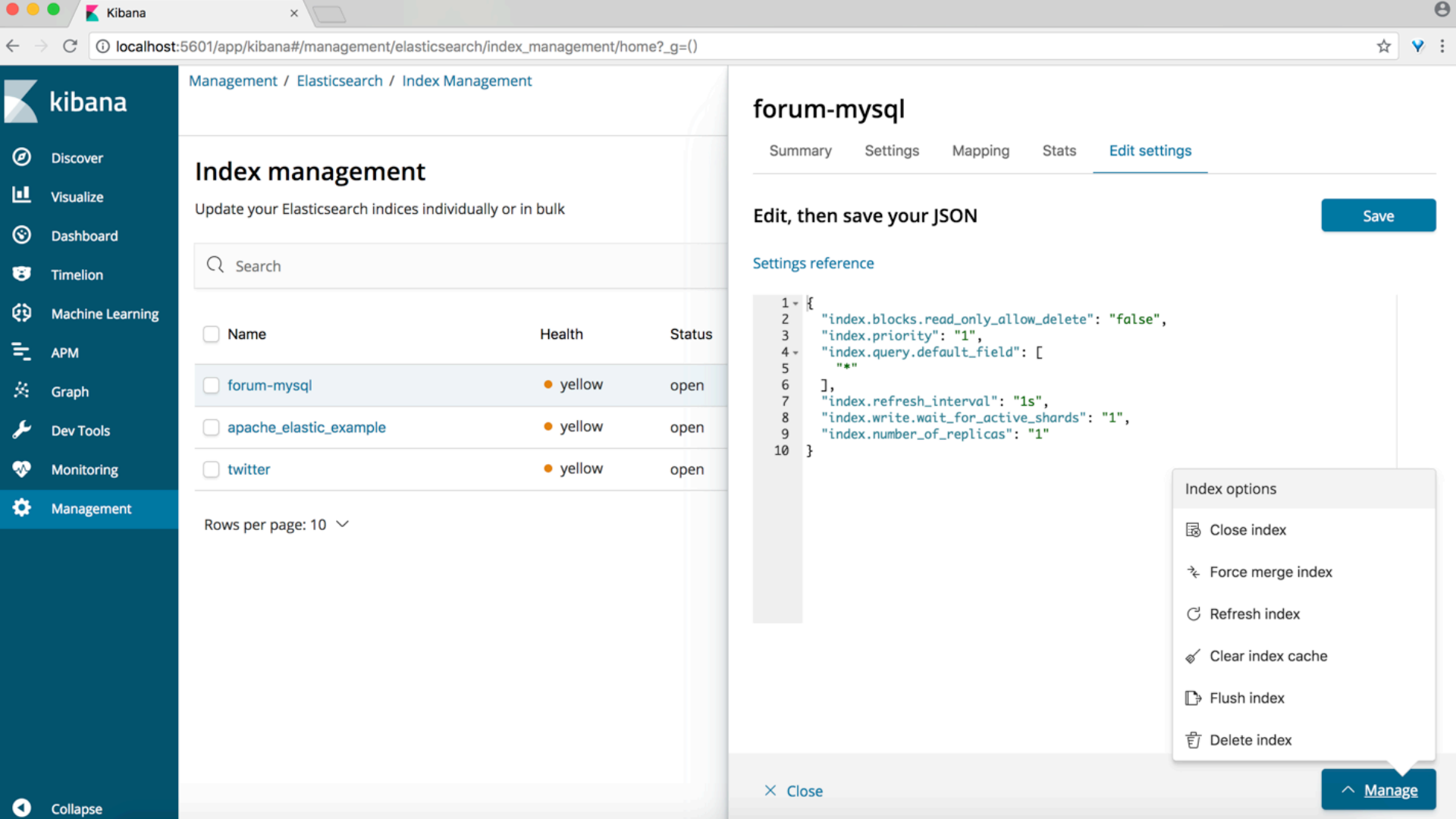
	Raw	Minute	Hour	Day
Docs:	**9,041,000**	**1,448,285**	**49,554**	**8,447**
Size:	**2.23gb**	**1.25gb**	**48.40mb**	**9.10mb**
Docs % change:		**-83.98%**	**-99.45%**	**-99.91%**
Size % change:		**-43.68%**	**-97.84%**	**-99.59%**

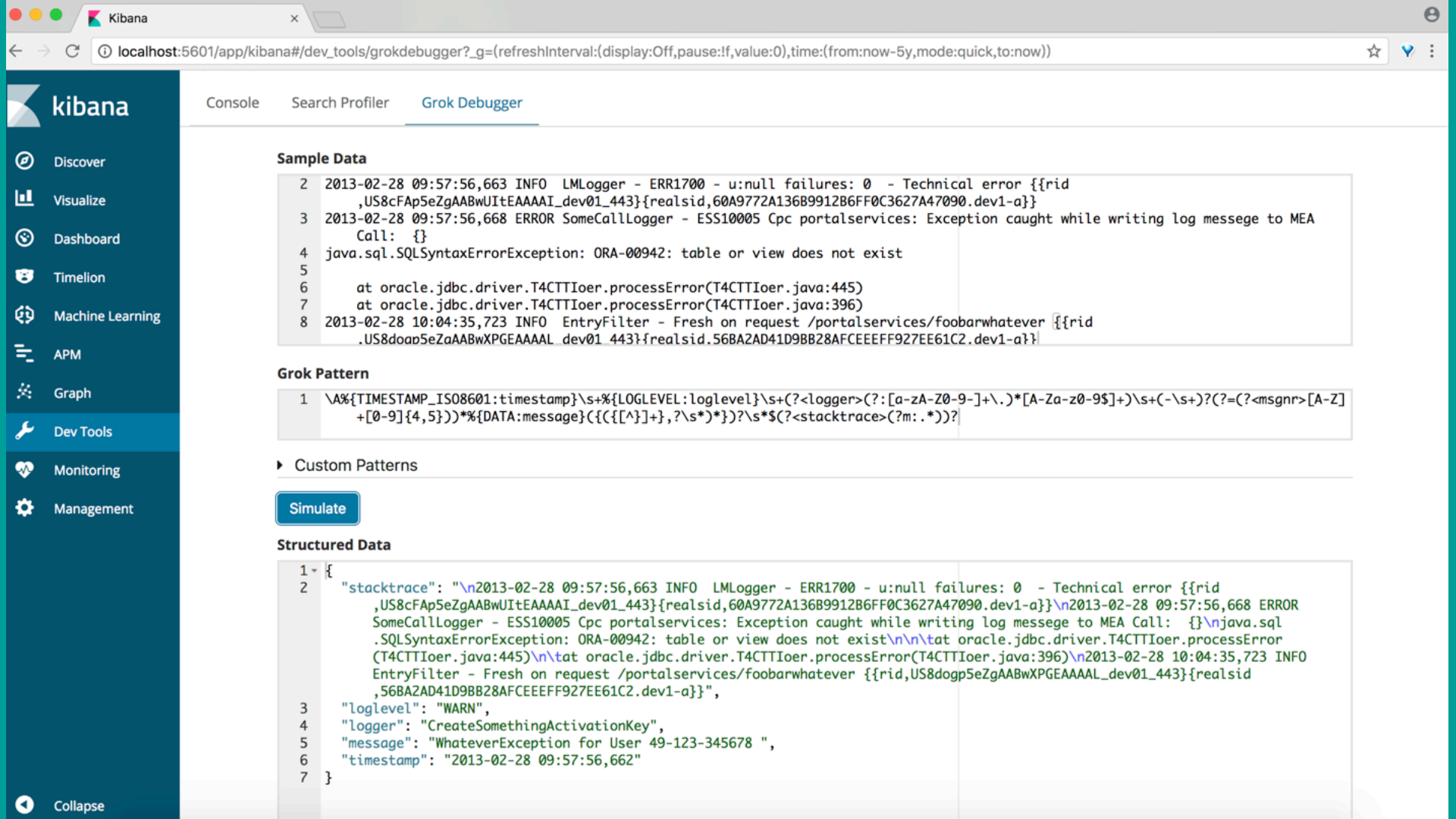
(avg ~200 docs per minute, 32 days of data, single host)
(20 grouping fields, 62 numerics @ min/max/avg == 186 metrics)

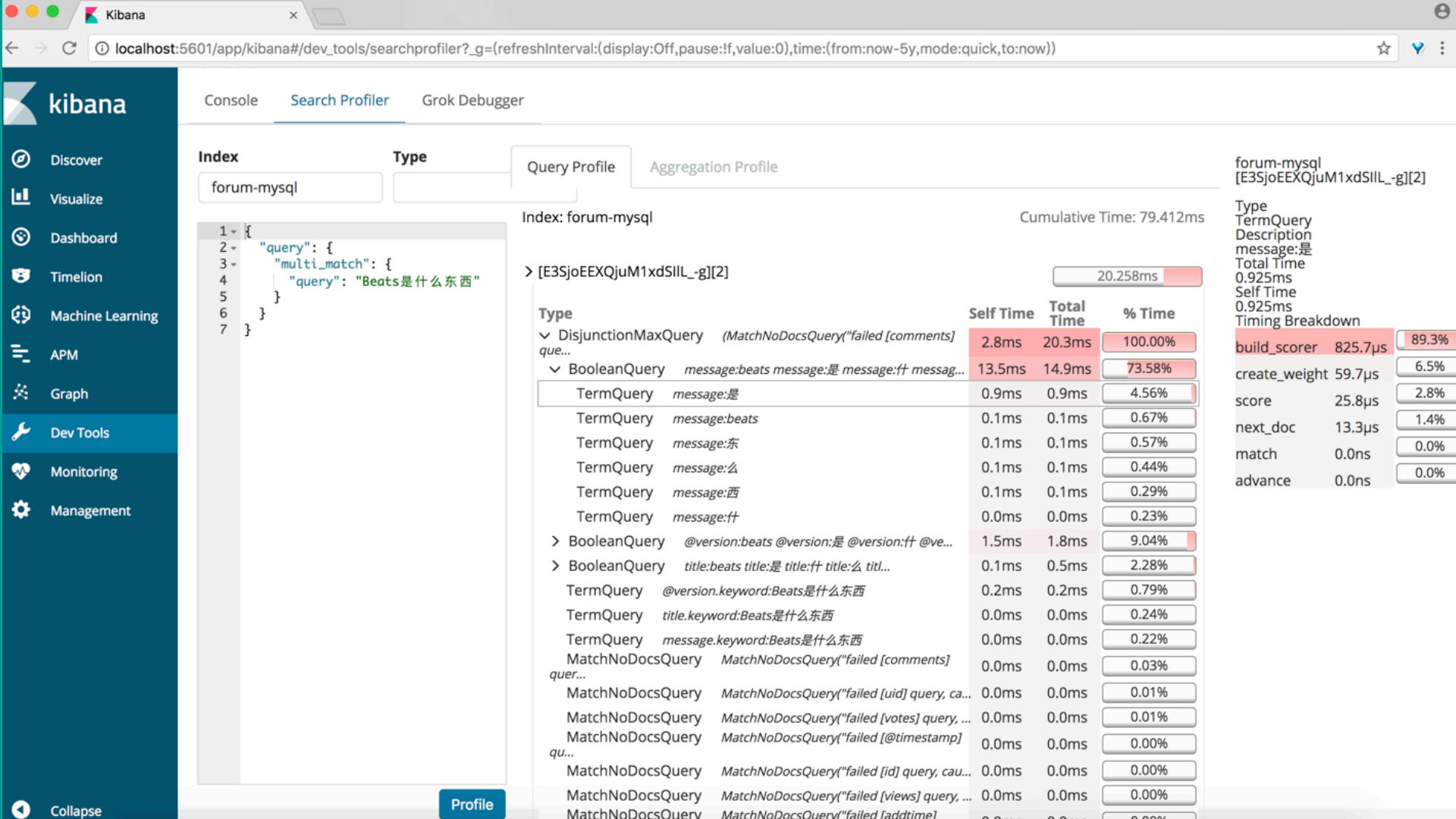


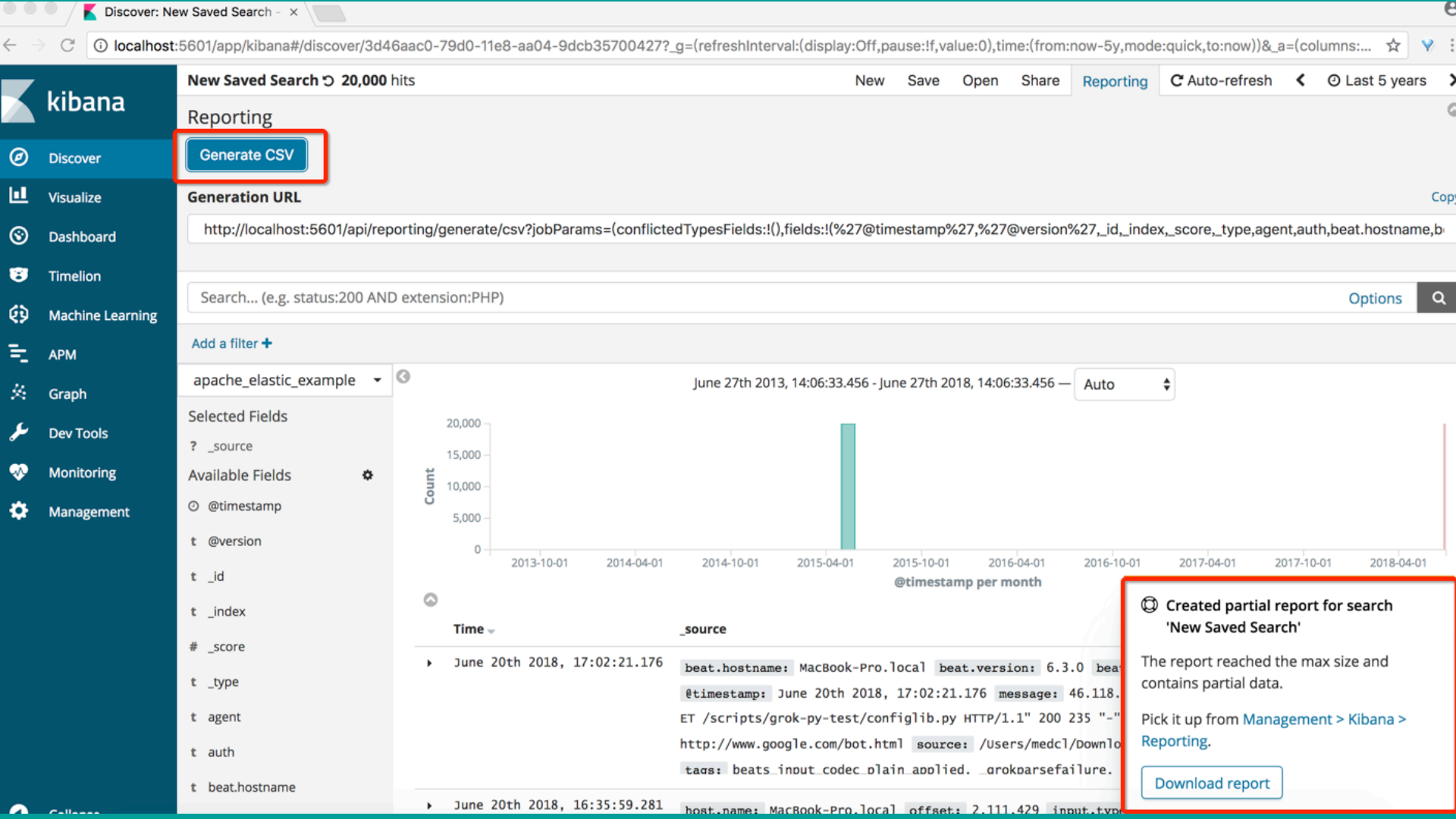





Kibana
localhost:5601/app/kibana#/management/elasticsearch/index_management/home?_g=()
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
Collapse
Management / Elasticsearch / Index Management
Index management
Update your Elasticsearch indices individually or in bulk
Search
Name
Health
Status
forum-mysql
yellow
open
apache_elastic_example
yellow
open
twitter
yellow
open
Rows per page: 10
forum-mysql
Summary
Settings
Mapping
Stats
Edit settings
Edit, then save your JSON
Save
Settings reference
{
"index.blocks.read_only_allow_delete": "false",
"index.priority": "1",
"index.query.default_field": [
"*"
],
"index.refresh_interval": "1s",
"index.write.wait_for_active_shards": "1",
"index.number_of_replicas": "1"
}
Index options
Close index
Force merge index
Refresh index
Clear index cache
Flush index
Delete index
Close
Manage


Kibana
localhost:5601/app/kibana#/dev_tools/grokdebugger?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-5y,mode:quick,to:now))
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
Collapse
Console
Search Profiler
Grok Debugger
Sample Data
2 2013-02-28 09:57:56,663 INFO LMLogger - ERR1700 - u:null failures: 0 - Technical error {{rid
,US8cFAp5eZgAABwUItEAAAAI_dev01_443}{realsid,60A9772A136B9912B6FF0C3627A47090.dev1-a}}
3 2013-02-28 09:57:56,668 ERROR SomeCallLogger - ESS10005 Cpc portalservices: Exception caught while writing log messege to MEA
Call: {}
4 java.sql.SQLSyntaxErrorException: ORA-00942: table or view does not exist
5
6 at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:445)
7 at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:396)
8 2013-02-28 10:04:35,723 INFO EntryFilter - Fresh on request /portalservices/foobarwhatever {{rid
,US8dogp5eZgAABwXPGEAAAAL_dev01_443}{realsid,56BA2AD41D9BB28AFCEEEFF927EE61C2.dev1-a}}
Grok Pattern
1 \A%{TIMESTAMP_ISO8601:timestamp}\s+%{LOGLEVEL:loglevel}\s+(?<logger>(?:[a-zA-Z0-9-]+\.)*[A-Za-z0-9$]+)\s+(-\s+)?(?=(?<msgnr>[A-Z]
+[0-9]{4,5}))*%{DATA:message}({{{[^}]+},?\s*)*})?\s*$(?<stacktrace>(?m:.*))?
Custom Patterns
Simulate
Structured Data
1 {
2 "stacktrace": "\n2013-02-28 09:57:56,663 INFO LMLogger - ERR1700 - u:null failures: 0 - Technical error {{rid
,US8cFAp5eZgAABwUItEAAAAI_dev01_443}{realsid,60A9772A136B9912B6FF0C3627A47090.dev1-a}}\n2013-02-28 09:57:56,668 ERROR
SomeCallLogger - ESS10005 Cpc portalservices: Exception caught while writing log messege to MEA Call: {}\njava.sql
.SQLSyntaxErrorException: ORA-00942: table or view does not exist\n\n\tat oracle.jdbc.driver.T4CTTIoer.processError
(T4CTTIoer.java:445)\n\tat oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:396)\n2013-02-28 10:04:35,723 INFO
EntryFilter - Fresh on request /portalservices/foobarwhatever {{rid,US8dogp5eZgAABwXPGEAAAAL_dev01_443}{realsid
,56BA2AD41D9BB28AFCEEEFF927EE61C2.dev1-a}}",
3 "loglevel": "WARN",
4 "logger": "CreateSomethingActivationKey",
5 "message": "WhateverException for User 49-123-345678 ",
6 "timestamp": "2013-02-28 09:57:56,662"
7 }


Kibana
localhost:5601/app/kibana#/dev_tools/searchprofiler?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-5y,mode:quick,to:now))
kibana
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
Collapse
Console
Search Profiler
Grok Debugger
Index
forum-mysql
Type
{
"query": {
"multi_match": {
"query": "Beats是什么东西"
}
}
}
Profile
Query Profile
Aggregation Profile
Index: forum-mysql
Cumulative Time: 79.412ms
[E3SjoEEXQjuM1xdSIlL_-g][2]
20.258ms
Type
Self Time
Total Time
% Time
DisjunctionMaxQuery (MatchNoDocsQuery("failed [comments] que... 2.8ms 20.3ms 100.00%
BooleanQuery message:beats message:是 message:什 messag... 13.5ms 14.9ms 73.58%
TermQuery message:是 0.9ms 0.9ms 4.56%
TermQuery message:beats 0.1ms 0.1ms 0.67%
TermQuery message:东 0.1ms 0.1ms 0.57%
TermQuery message:么 0.1ms 0.1ms 0.44%
TermQuery message:西 0.1ms 0.1ms 0.29%
TermQuery message:什 0.0ms 0.0ms 0.23%
BooleanQuery @version:beats @version:是 @version:什 @ve... 1.5ms 1.8ms 9.04%
BooleanQuery title:beats title:是 title:什 title:么 titl... 0.1ms 0.5ms 2.28%
TermQuery @version.keyword:Beats是什么东西 0.2ms 0.2ms 0.79%
TermQuery title.keyword:Beats是什么东西 0.0ms 0.0ms 0.24%
TermQuery message.keyword:Beats是什么东西 0.0ms 0.0ms 0.22%
MatchNoDocsQuery MatchNoDocsQuery("failed [comments] quer... 0.0ms 0.0ms 0.03%
MatchNoDocsQuery MatchNoDocsQuery("failed [uid] query, ca... 0.0ms 0.0ms 0.01%
MatchNoDocsQuery MatchNoDocsQuery("failed [votes] query, ... 0.0ms 0.0ms 0.01%
MatchNoDocsQuery MatchNoDocsQuery("failed [@timestamp] qu... 0.0ms 0.0ms 0.00%
MatchNoDocsQuery MatchNoDocsQuery("failed [id] query, cau... 0.0ms 0.0ms 0.00%
MatchNoDocsQuery MatchNoDocsQuery("failed [views] query, ... 0.0ms 0.0ms 0.00%
forum-mysql
[E3SjoEEXQjuM1xdSIlL_-g][2]
Type
TermQuery
Description
message:是
Total Time
0.925ms
Self Time
0.925ms
Timing Breakdown
build_scorer 825.7µs 89.3%
create_weight 59.7µs 6.5%
score 25.8µs 2.8%
next_doc 13.3µs 1.4%
match 0.0ns 0.0%
advance 0.0ns 0.0%


Discover: New Saved Search
localhost:5601/app/kibana#/discover/3d46aac0-79d0-11e8-aa04-9dcb35700427?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-5y,mode:quick,to:now))&_a=(columns:...
kibana
New Saved Search 20,000 hits
New
Save
Open
Share
Reporting
Auto-refresh
Last 5 years
Reporting
Generate CSV
Generation URL
http://localhost:5601/api/reporting/generate/csv?jobParams=(conflictedTypesFields:!(),fields:!(%27@timestamp%27,%27@version%27,_id,_index,_score,_type,agent,auth,beat.hostname,b
Search... (e.g. status:200 AND extension:PHP)
Options
Add a filter +
Discover
Visualize
Dashboard
Timelion
Machine Learning
APM
Graph
Dev Tools
Monitoring
Management
apache_elastic_example
Selected Fields
? _source
Available Fields
@timestamp
t @version
t _id
t _index
_score
t _type
t agent
t auth
t beat.hostname
June 27th 2013, 14:06:33.456 - June 27th 2018, 14:06:33.456 —
Auto
20,000
15,000
10,000
5,000
0
Count
2013-10-01
2014-04-01
2014-10-01
2015-04-01
2015-10-01
2016-04-01
2016-10-01
2017-04-01
2017-10-01
2018-04-01
@timestamp per month
Time
_source
June 20th 2018, 17:02:21.176
beat.hostname: MacBook-Pro.local beat.version: 6.3.0
@timestamp: June 20th 2018, 17:02:21.176 message: 46.118.
ET /scripts/grok-py-test/configlib.py HTTP/1.1" 200 235 "-"
http://www.google.com/bot.html source: /Users/medcl/Downlo
tags: beats_input_codec_plain_applied, _grokparsefailure.
June 20th 2018, 16:35:59.281
host.name: MacBook-Pro.local offset: 2,111,429
Created partial report for search 'New Saved Search'
The report reached the max size and contains partial data.
Pick it up from Management > Kibana > Reporting.
Download report





https://conf.elasticsearch.cn/2018/

ELASTIC CERTIFIED ENGINEER
QUAERERE
INVENIET

https://www.elastic.co/training/certification

elastic
COMMUNITY
RADIO

https://radio.elasticsearch.cn


THANK YOU
medcl@elastic.co
http://www.elastic.co/



elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/