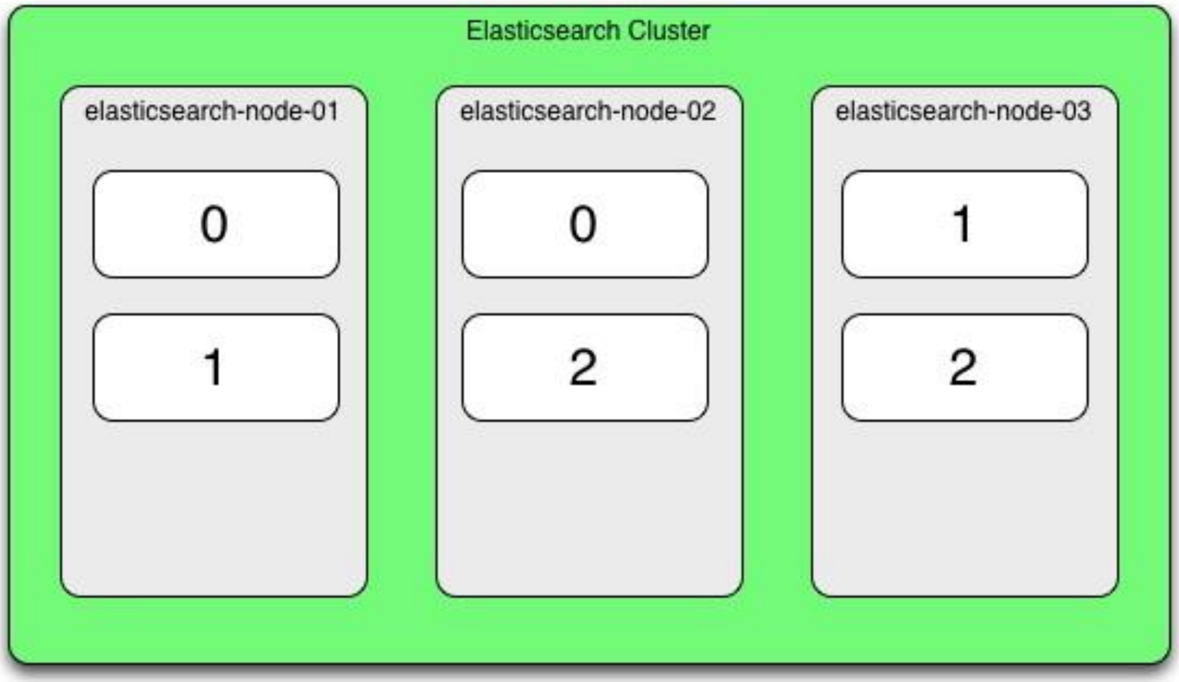
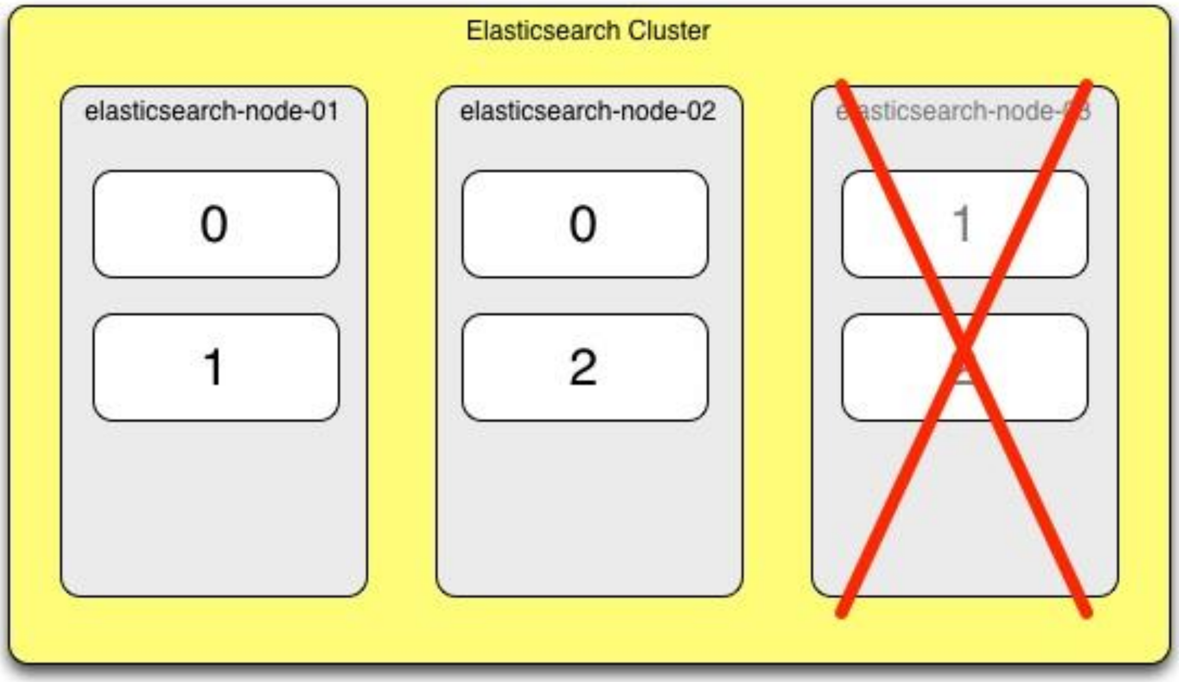
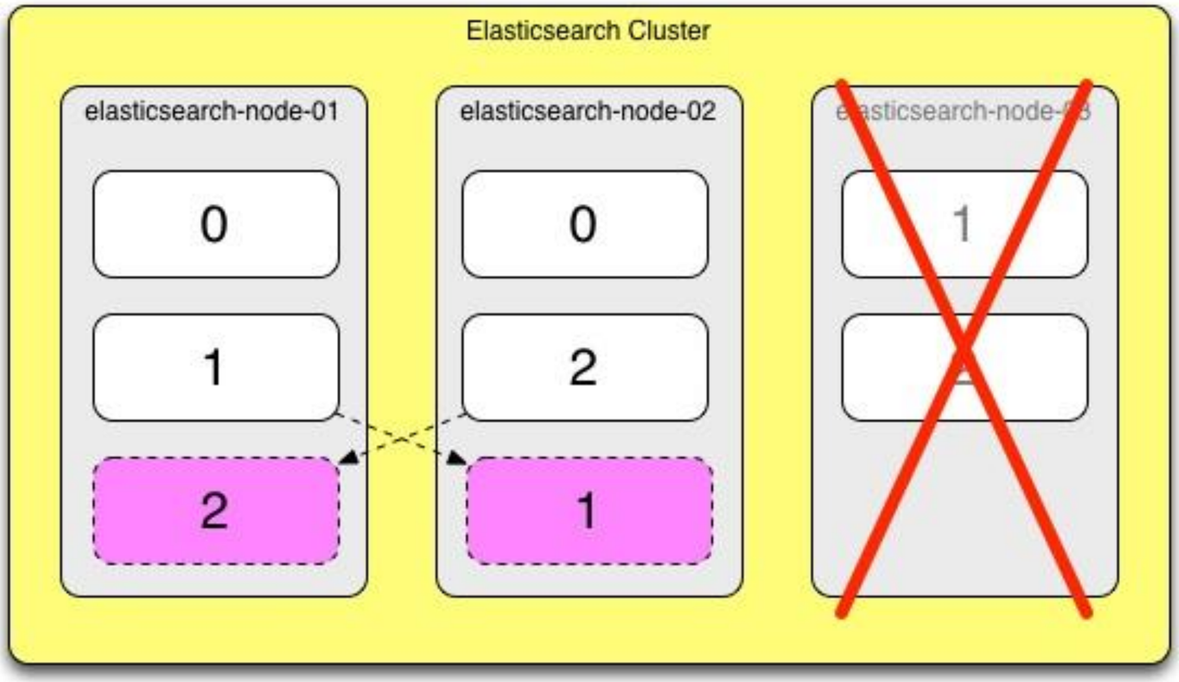
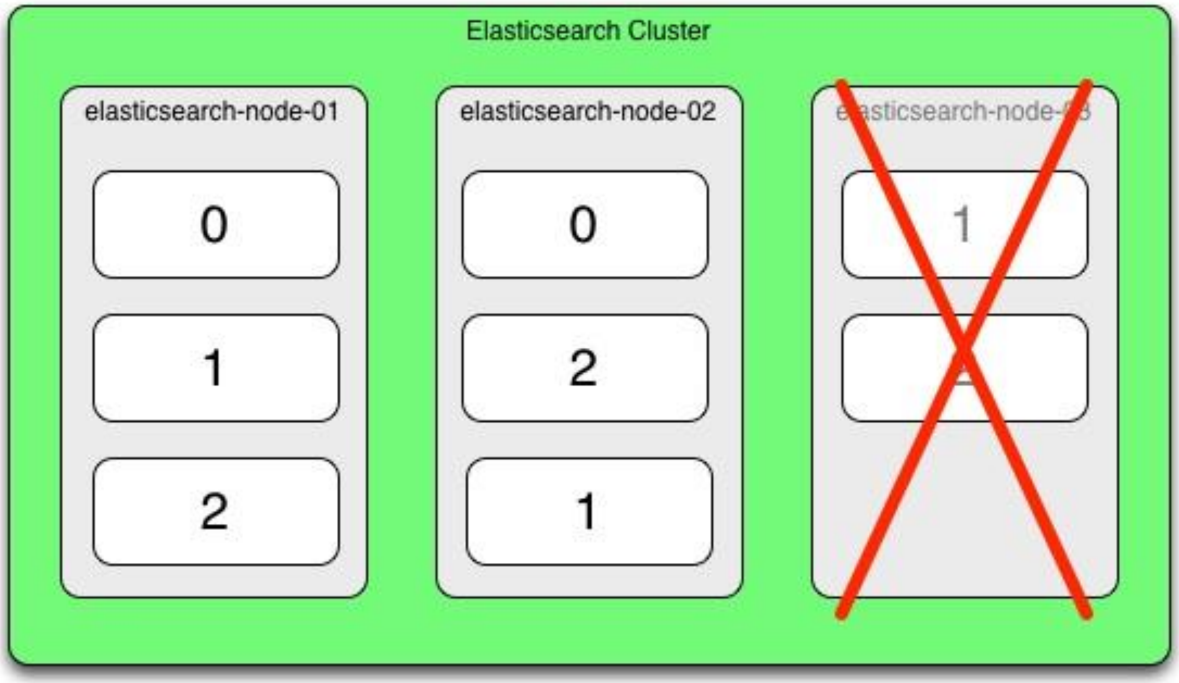
Chapter 1: Introduction to Monitoring Elasticsearch

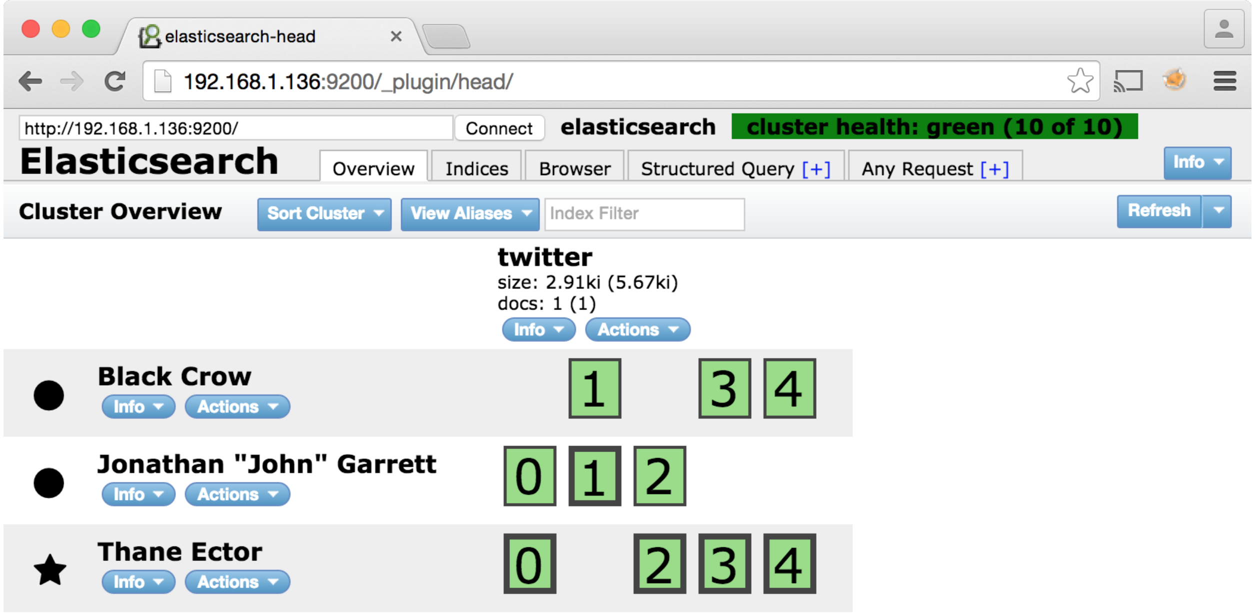





Elasticsearch Cluster
elasticsearch-node-01
0
1
2
elasticsearch-node-02
0
2
1
asticsearch-node-
1


Elasticsearch Cluster
elasticsearch-node-01
0
1
2
elasticsearch-node-02
0
2
1
asticsearch-node-
1

Chapter 2: Installation and the Requirements for Elasticsearch



http://192.168.1.136:9200/

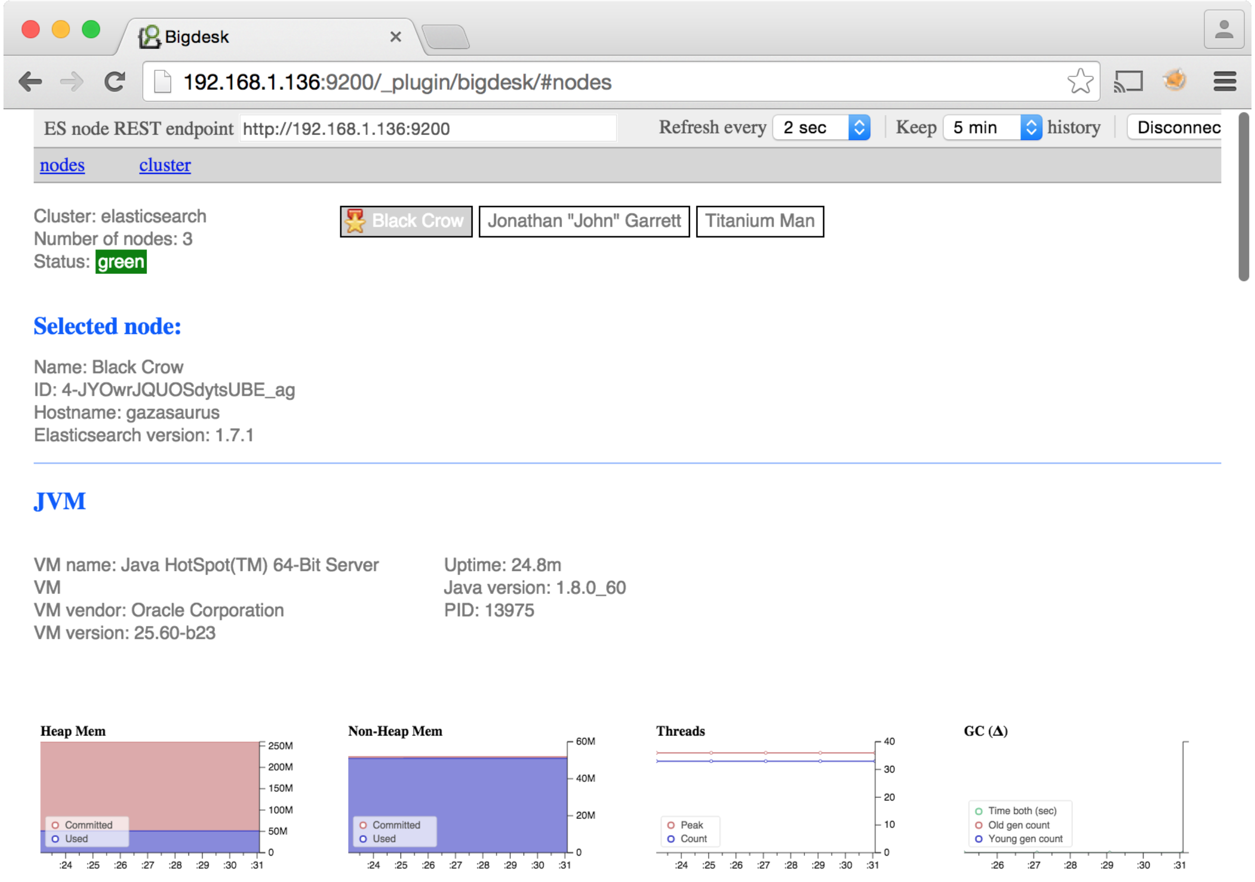
elasticsearch cluster health: green (10 of 10)

twitter
size: 2.91ki (5.67ki)
docs: 1 (1)

● Black Crow 1 3 4

● Jonathan "John" Garrett 0 1 2

★ Thane Ector 0 2 3 4



Bigdesk

192.168.1.136:9200/_plugin/bigdesk/#nodes

ES node REST endpoint http://192.168.1.136:9200 Refresh every 2 sec Keep 5 min history Disconnec

nodes cluster

Cluster: elasticsearch
Number of nodes: 3
Status: green

Black Crow | Jonathan "John" Garrett | Titanium Man

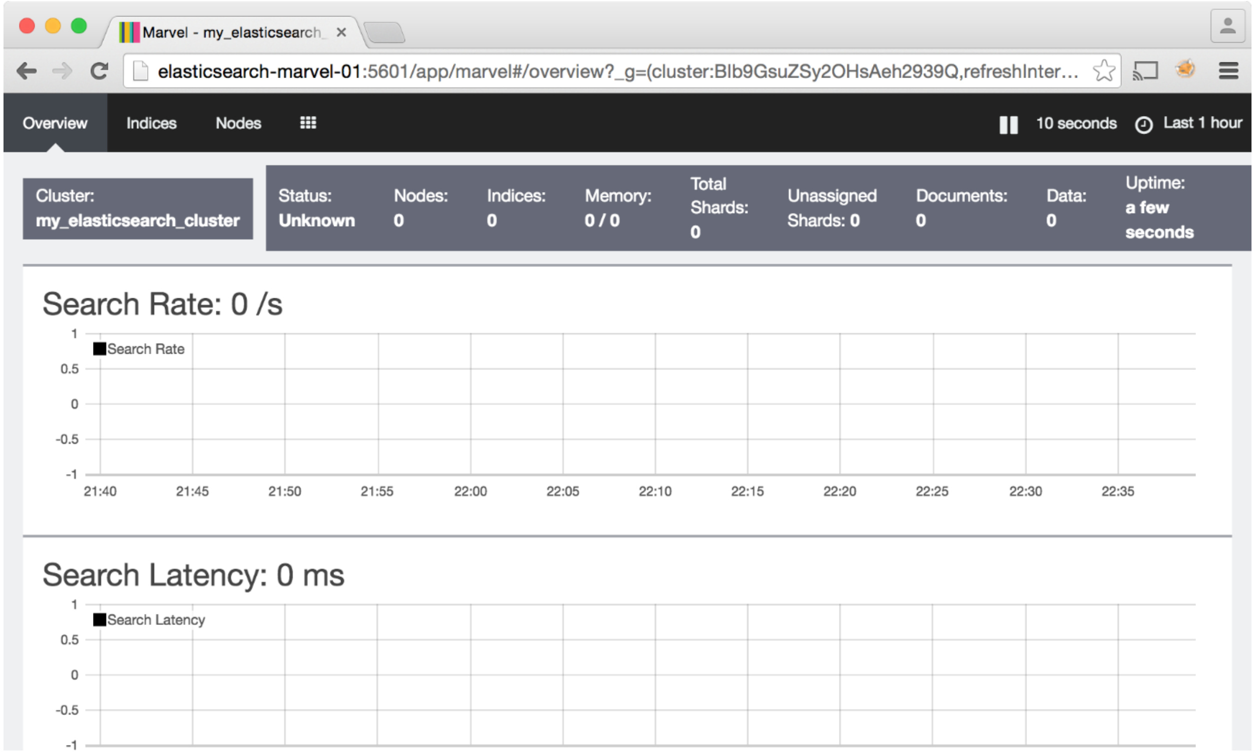
Selected node:

Name: Black Crow
ID: 4-JYOwrJQUOSdytsUBE_ag
Hostname: gazasaurus
Elasticsearch version: 1.7.1

JVM

VM name: Java HotSpot(TM) 64-Bit Server VM
VM vendor: Oracle Corporation
VM version: 25.60-b23

Uptime: 24.8m
Java version: 1.8.0_60
PID: 13975


Marvel - my_elasticsearch_
elasticsearch-marvel-01:5601/app/marvel#/overview?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInter…
Overview
Indices
Nodes
10 seconds
Last 1 hour

Cluster: **my_elasticsearch_cluster**

Status: **Unknown**

Nodes: **0**

Indices: **0**

Memory: **0 / 0**

Total Shards: **0**

Unassigned Shards: **0**

Documents: **0**

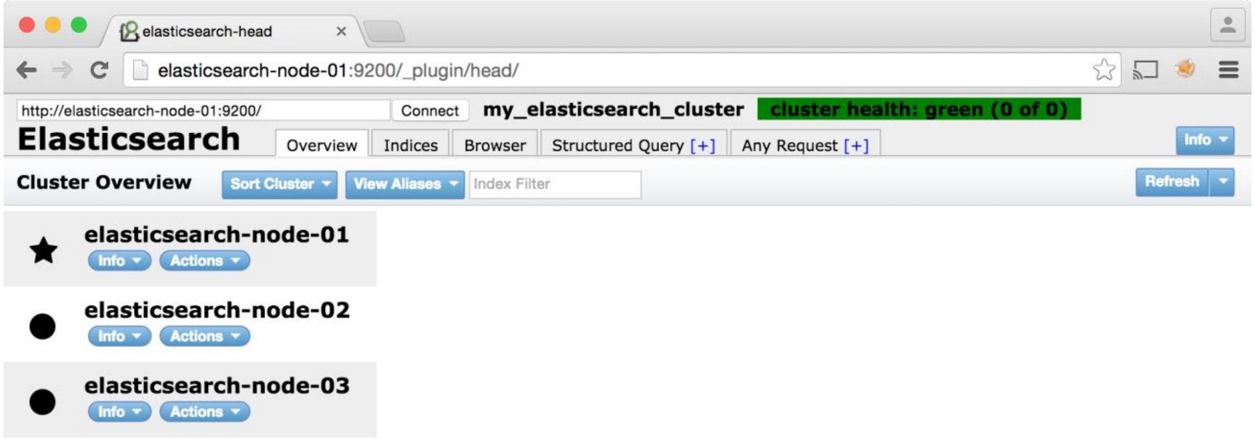
Data: **0**

Uptime: **a few seconds**

Search Rate: 0 /s

Search Latency: 0 ms

Chapter 3: Elasticsearch-head and Bigdesk

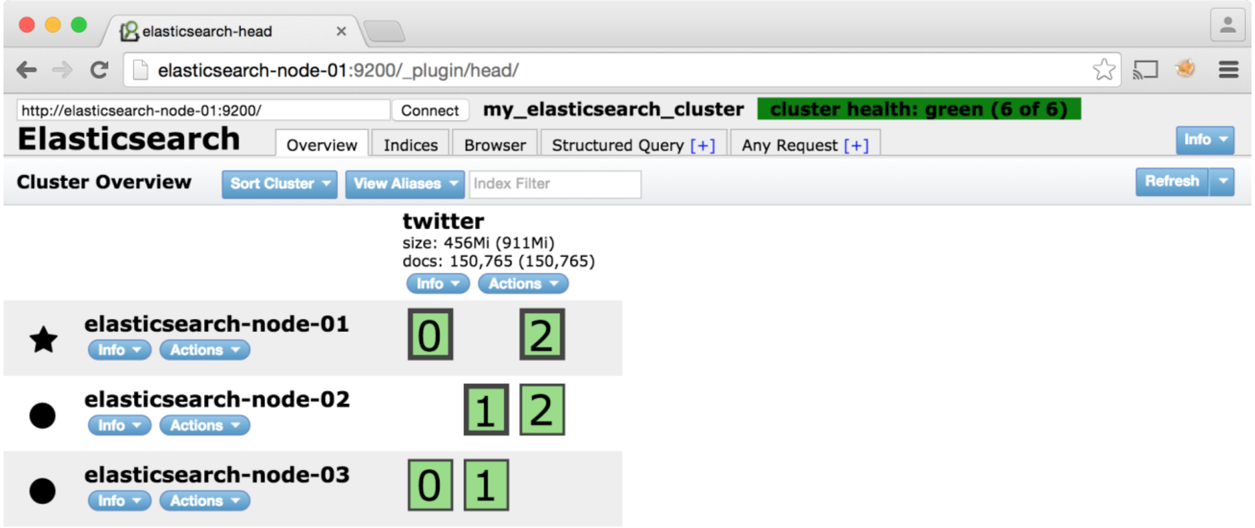


elasticsearch-node-01:9200/_plugin/head/

http://elasticsearch-node-01:9200/

my_elasticsearch_cluster

cluster health: green (0 of 0)



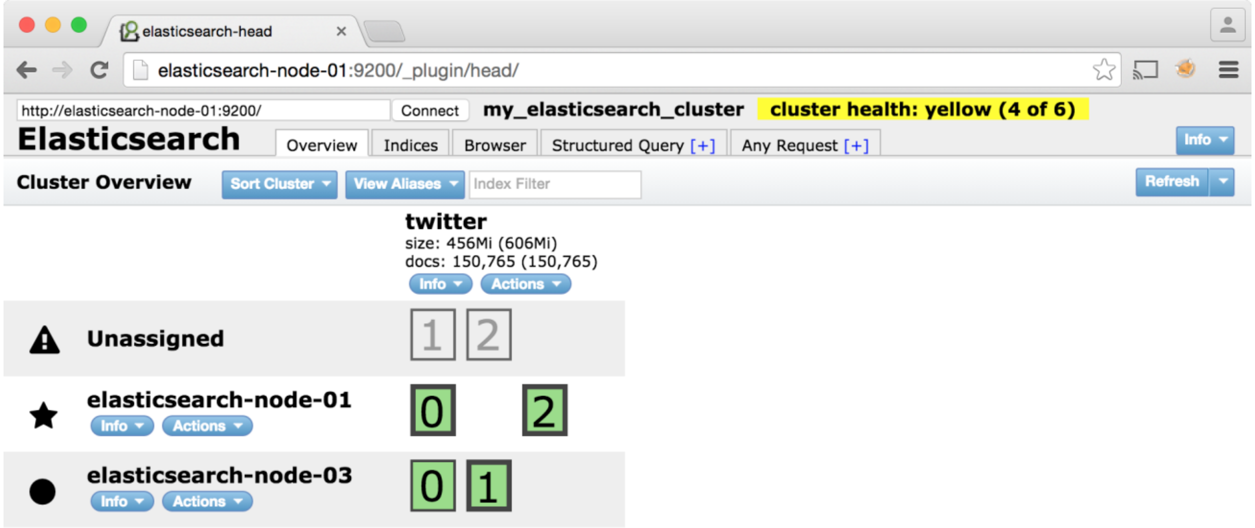
elasticsearch-node-01:9200/_plugin/head/

http://elasticsearch-node-01:9200/

my_elasticsearch_cluster

cluster health: green (6 of 6)

twitter
size: 456Mi (911Mi)
docs: 150,765 (150,765)



elasticsearch-node-01:9200/_plugin/head/

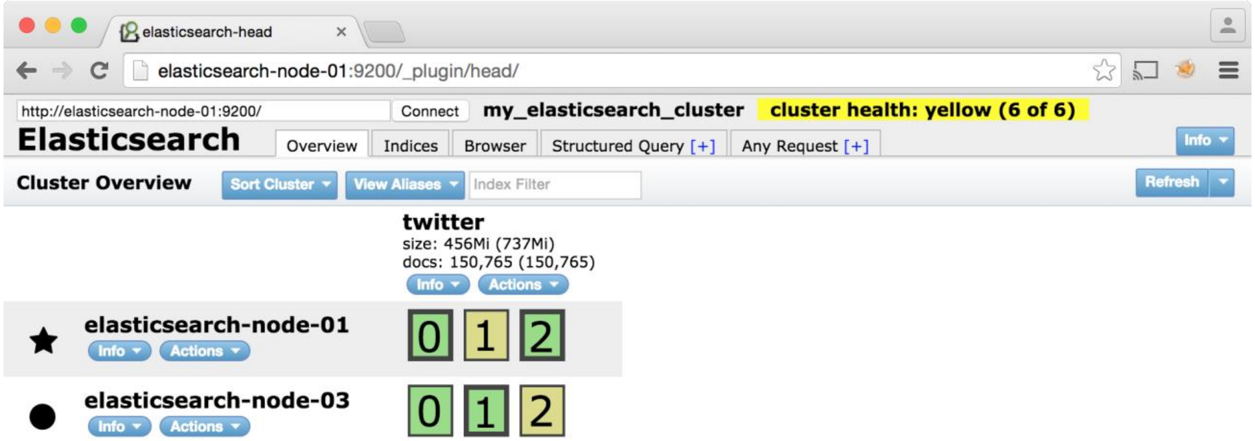
http://elasticsearch-node-01:9200/ Connect my_elasticsearch_cluster cluster health: yellow (4 of 6)

Elasticsearch

Cluster Overview

twitter
size: 456Mi (606Mi)
docs: 150,765 (150,765)

	twitter
Unassigned	1 2
elasticsearch-node-01	0 2
elasticsearch-node-03	0 1



elasticsearch-node-01:9200/_plugin/head/

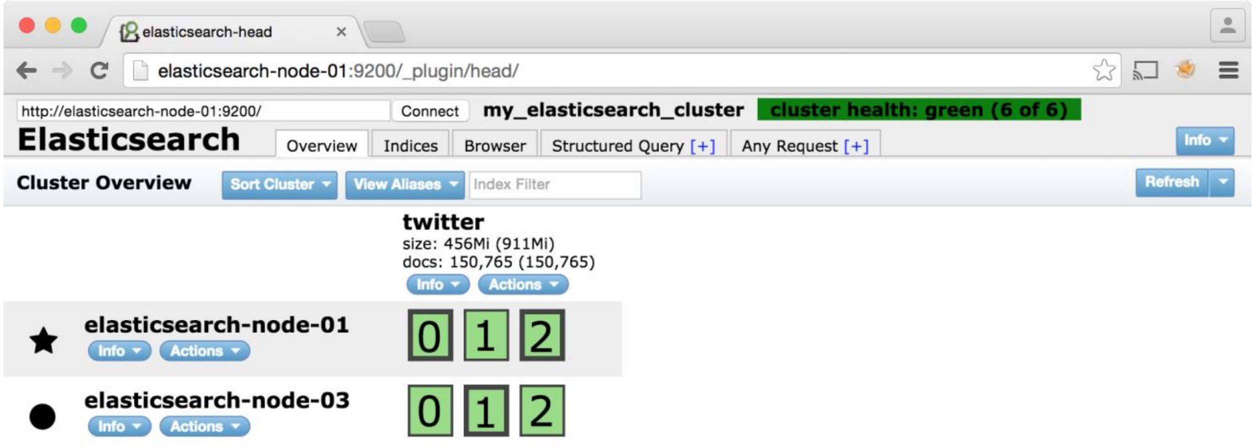
http://elasticsearch-node-01:9200/ Connect my_elasticsearch_cluster cluster health: yellow (6 of 6)

Elasticsearch

Cluster Overview

twitter
size: 456Mi (737Mi)
docs: 150,765 (150,765)

	twitter
elasticsearch-node-01	0 1 2
elasticsearch-node-03	0 1 2



elasticsearch-node-01:9200/_plugin/head/

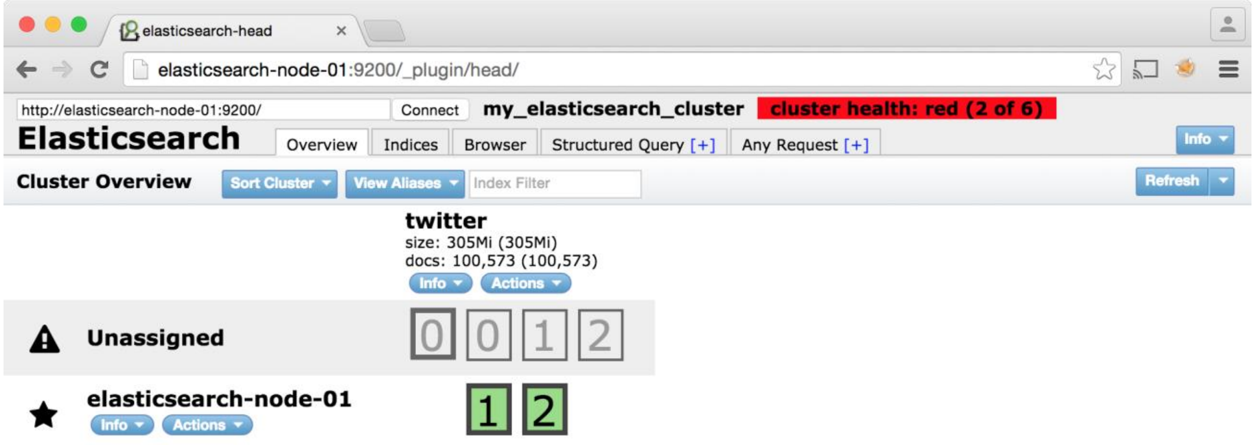
http://elasticsearch-node-01:9200/

my_elasticsearch_cluster cluster health: green (6 of 6)

twitter
size: 456Mi (911Mi)
docs: 150,765 (150,765)

★ elasticsearch-node-01 0 1 2

● elasticsearch-node-03 0 1 2



elasticsearch-node-01:9200/_plugin/head/

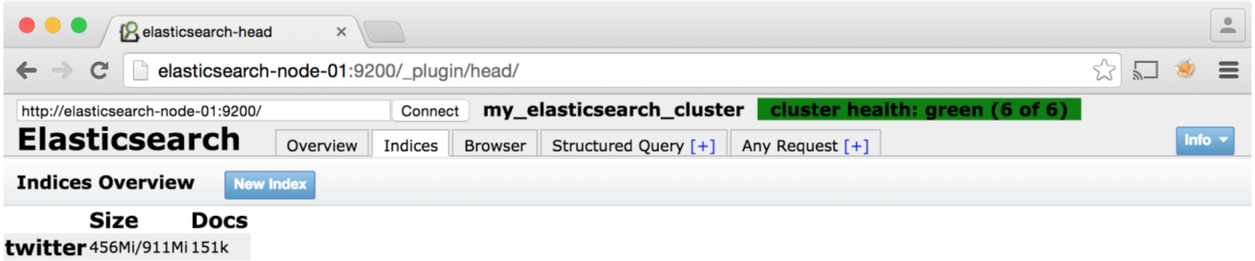
http://elasticsearch-node-01:9200/

my_elasticsearch_cluster cluster health: red (2 of 6)

twitter
size: 305Mi (305Mi)
docs: 100,573 (100,573)

⚠ Unassigned 0 0 1 2

★ elasticsearch-node-01 1 2



elasticsearch-head

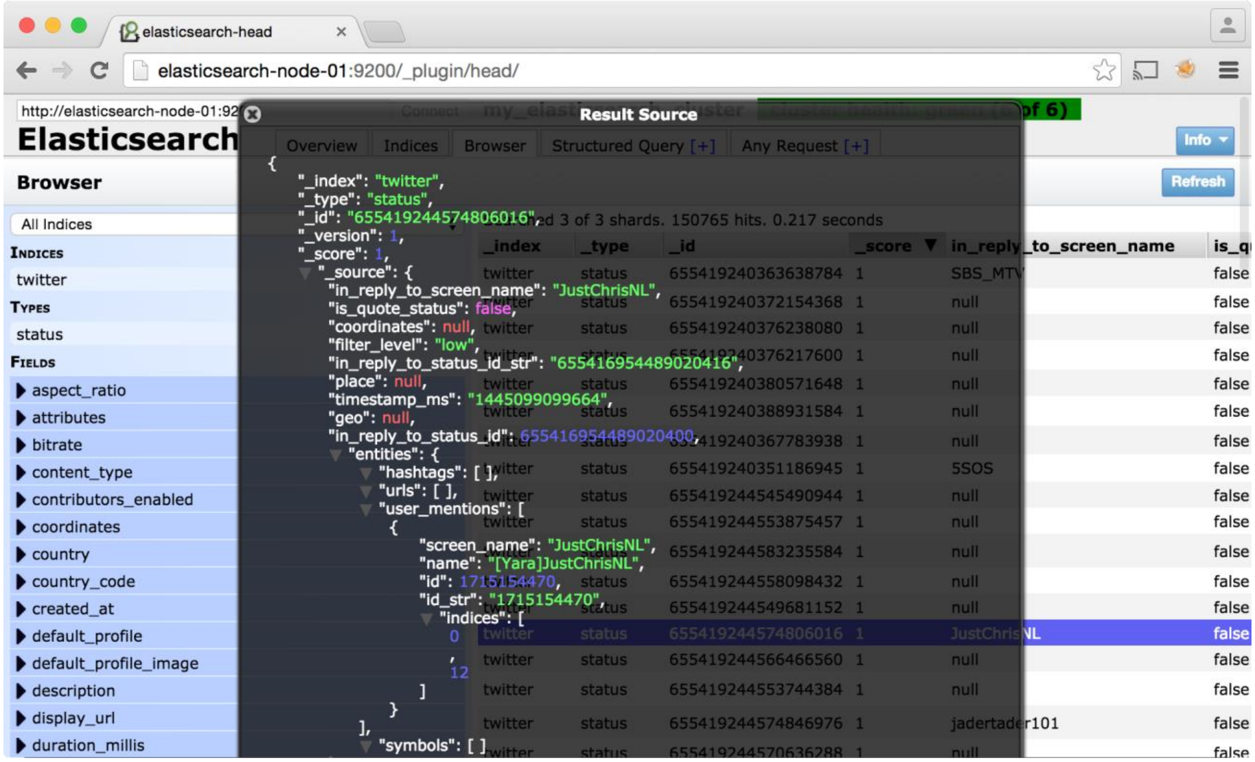
elasticsearch-node-01:9200/_plugin/head/

http://elasticsearch-node-01:9200/ Connect **my_elasticsearch_cluster** cluster health: green (6 of 6)

Elasticsearch

Indices Overview

	Size	Docs
twitter	456Mi/911Mi	151k



elasticsearch-head

elasticsearch-node-01:9200/_plugin/head/

http://elasticsearch-node-01:92

Elasticsearch

Browser

All Indices

Indices

twitter

Types

status

Fields

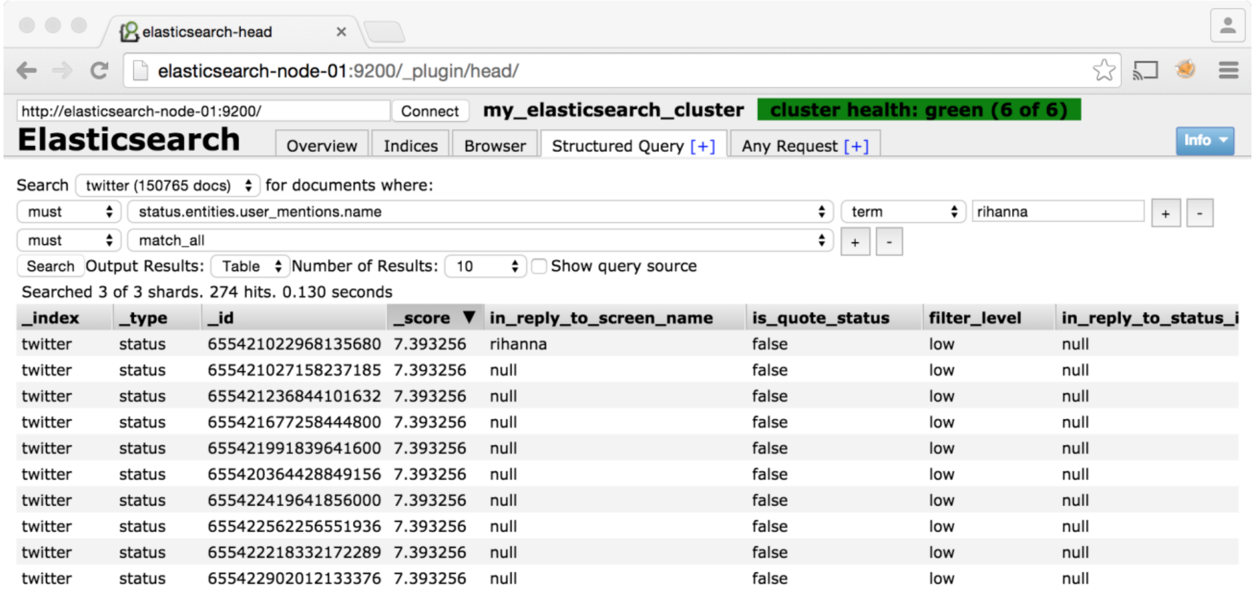
- aspect_ratio
- attributes
- bitrate
- content_type
- contributors_enabled
- coordinates
- country
- country_code
- created_at
- default_profile
- default_profile_image
- description
- display_url
- duration_millis

Result Source

```
{
    "_index": "twitter",
    "_type": "status",
    "_id": "655419244574806016",
    "_version": 1,
    "_score": 1,
    "_source": {
        "in_reply_to_screen_name": "JustChrisNL",
        "is_quote_status": false,
        "coordinates": null,
        "filter_level": "low",
        "in_reply_to_status_id_str": "655416954489020416",
        "place": null,
        "timestamp_ms": "1445099099664",
        "geo": null,
        "in_reply_to_status_id": 655416954489020400,
        "entities": {
            "hashtags": [ ],
            "urls": [ ],
            "user_mentions": [
                {
                    "screen_name": "JustChrisNL",
                    "name": "[Yara]JustChrisNL",
                    "id": 1715154470,
                    "id_str": "1715154470",
                    "indices": [
                        0
                        ,
                        12
                    ]
                }
            ],
            "symbols": [ ]
```

ed 3 of 3 shards. 150765 hits. 0.217 seconds

_index	_type	_id	_score ▼	in_reply_to_screen_name	is_q
twitter	status	655419240363638784	1	SBS_MTV	false
twitter	status	655419240372154368	1	null	false
twitter	status	655419240376238080	1	null	false
twitter	status	655419240376217600	1	null	false
twitter	status	655419240380571648	1	null	false
twitter	status	655419240388931584	1	null	false
twitter	status	655419240367783938	1	null	false
twitter	status	655419240351186945	1	5SOS	false
twitter	status	655419244545490944	1	null	false
twitter	status	655419244553875457	1	null	false
twitter	status	655419244583235584	1	null	false
twitter	status	655419244558098432	1	null	false
twitter	status	655419244549681152	1	null	false
twitter	status	655419244574806016	1	JustChrisNL	false
twitter	status	655419244566466560	1	null	false
twitter	status	655419244553744384	1	null	false
twitter	status	655419244574846976	1	jadertader101	false
twitter	status	655419244570636288	1	null	false



Search twitter (150765 docs) for documents where:

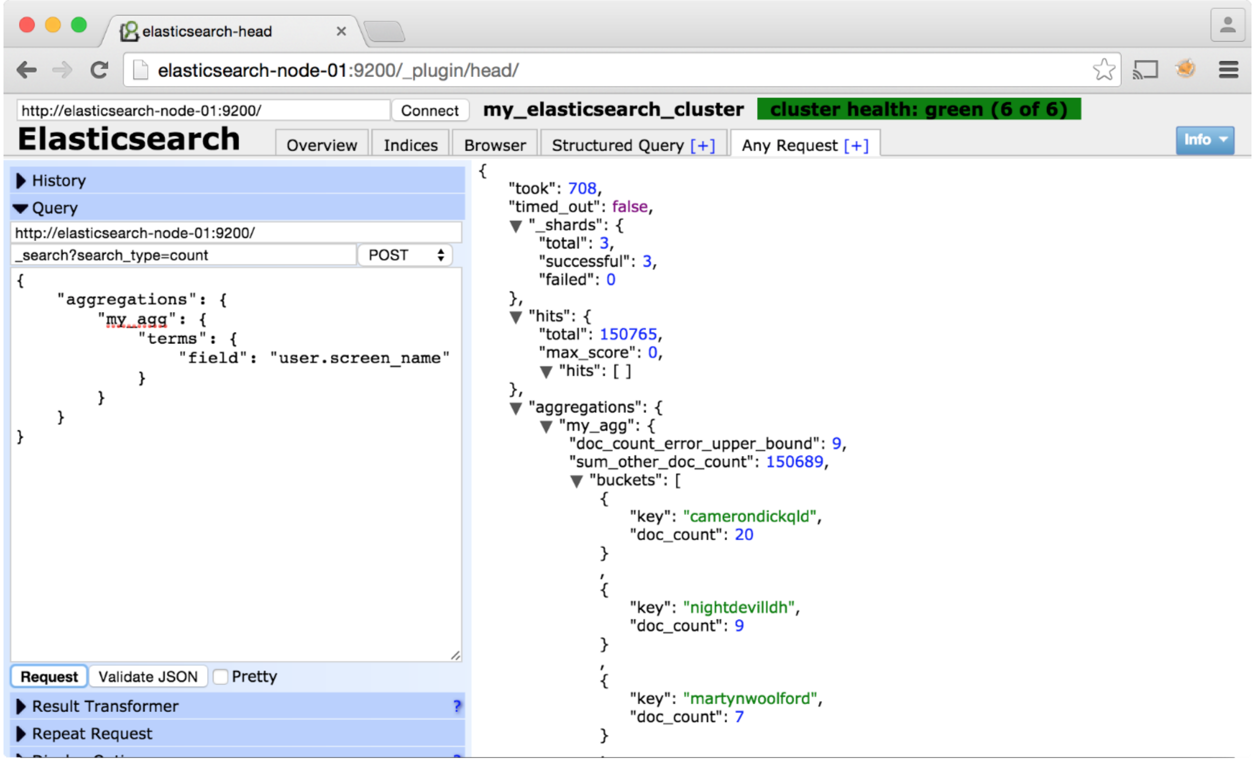
must status.entities.user_mentions.name term rihanna + -

must match_all + -

Search Output Results: Table Number of Results: 10 □ Show query source

Searched 3 of 3 shards. 274 hits. 0.130 seconds

_index	_type	_id	_score ▼	in_reply_to_screen_name	is_quote_status	filter_level	in_reply_to_status_i
twitter	status	655421022968135680	7.393256	rihanna	false	low	null
twitter	status	655421027158237185	7.393256	null	false	low	null
twitter	status	655421236844101632	7.393256	null	false	low	null
twitter	status	655421677258444800	7.393256	null	false	low	null
twitter	status	655421991839641600	7.393256	null	false	low	null
twitter	status	655420364428849156	7.393256	null	false	low	null
twitter	status	655422419641856000	7.393256	null	false	low	null
twitter	status	655422562256551936	7.393256	null	false	low	null
twitter	status	655422218332172289	7.393256	null	false	low	null
twitter	status	655422902012133376	7.393256	null	false	low	null

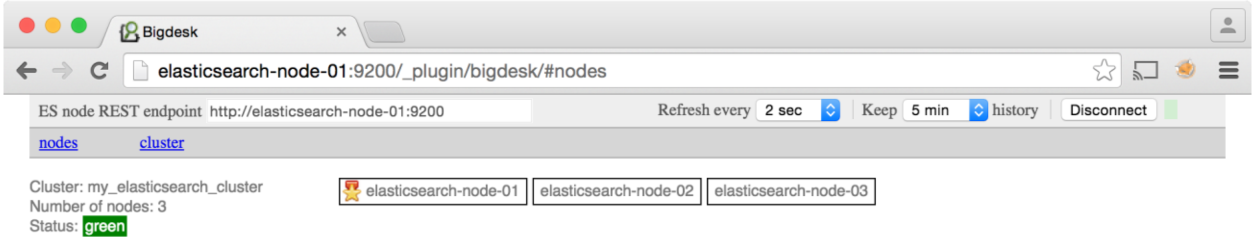


http://elasticsearch-node-01:9200/

_search?search_type=count POST

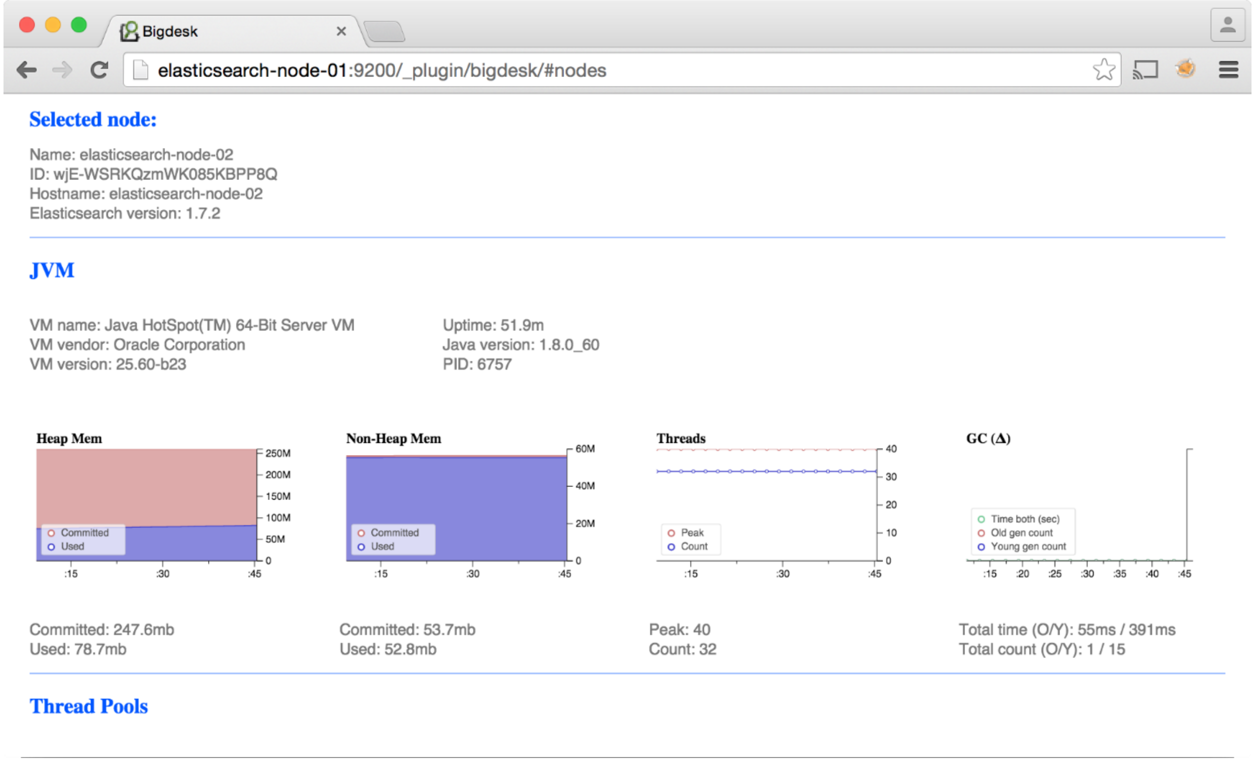
```
{
    "aggregations": {
        "my_agg": {
            "terms": {
                "field": "user.screen_name"
            }
        }
    }
}
```

```
{
  "took": 708,
  "timed_out": false,
▼ "_shards": {
     "total": 3,
     "successful": 3,
     "failed": 0
  },
▼ "hits": {
     "total": 150765,
     "max_score": 0,
   ▼ "hits": [ ]
  },
▼ "aggregations": {
   ▼ "my_agg": {
        "doc_count_error_upper_bound": 9,
        "sum_other_doc_count": 150689,
      ▼ "buckets": [
           {
              "key": "camerondickqld",
              "doc_count": 20
           }
           ,
           {
              "key": "nightdevilldh",
              "doc_count": 9
           }
           ,
           {
              "key": "martynwoolford",
              "doc_count": 7
           }
```



ES node REST endpoint http://elasticsearch-node-01:9200 Refresh every 2 sec Keep 5 min history Disconnect

Cluster: my_elasticsearch_cluster
Number of nodes: 3
Status: green



Selected node:

Name: elasticsearch-node-02
ID: wjE-WSRKQzmWK085KBPP8Q
Hostname: elasticsearch-node-02
Elasticsearch version: 1.7.2

JVM

VM name: Java HotSpot(TM) 64-Bit Server VM
VM vendor: Oracle Corporation
VM version: 25.60-b23

Uptime: 51.9m
Java version: 1.8.0_60
PID: 6757

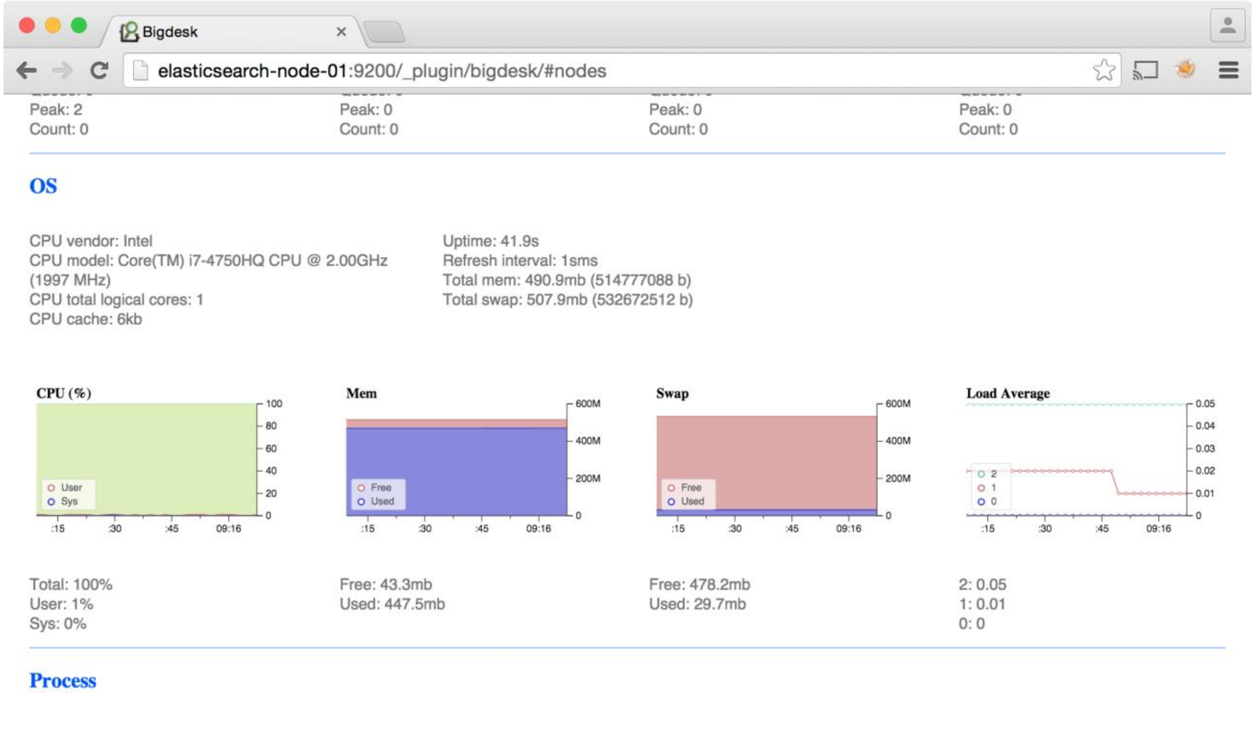
Committed: 247.6mb
Used: 78.7mb

Committed: 53.7mb
Used: 52.8mb

Peak: 40
Count: 32

Total time (O/Y): 55ms / 391ms
Total count (O/Y): 1 / 15

Thread Pools



Peak: 2
Count: 0

Peak: 0
Count: 0

Peak: 0
Count: 0

Peak: 0
Count: 0

OS

CPU vendor: Intel
CPU model: Core(TM) i7-4750HQ CPU @ 2.00GHz (1997 MHz)
CPU total logical cores: 1
CPU cache: 6kb

Uptime: 41.9s
Refresh interval: 1sms
Total mem: 490.9mb (514777088 b)
Total swap: 507.9mb (532672512 b)

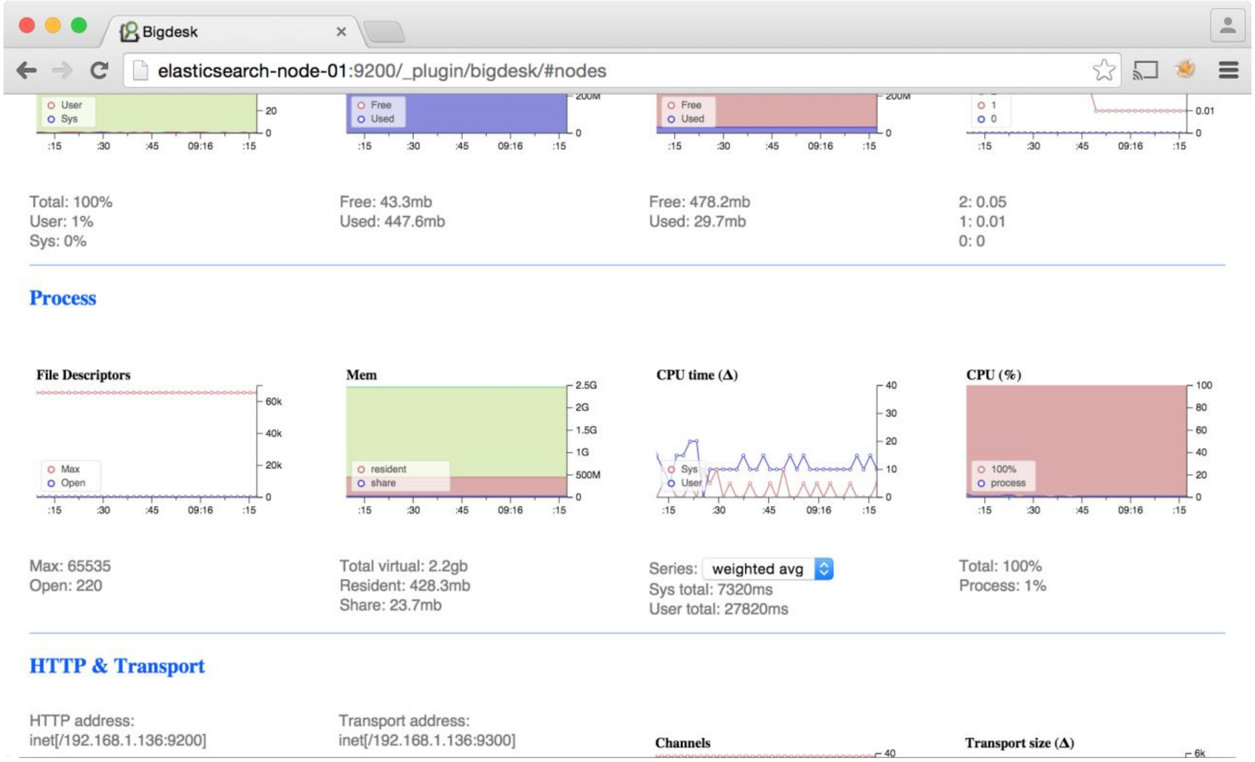
Total: 100%
User: 1%
Sys: 0%

Free: 43.3mb
Used: 447.5mb

Free: 478.2mb
Used: 29.7mb

2: 0.05
1: 0.01
0: 0

Process



Total: 100%
User: 1%
Sys: 0%

Free: 43.3mb
Used: 447.6mb

Free: 478.2mb
Used: 29.7mb

2: 0.05
1: 0.01
0: 0

Process

Max: 65535
Open: 220

Total virtual: 2.2gb
Resident: 428.3mb
Share: 23.7mb

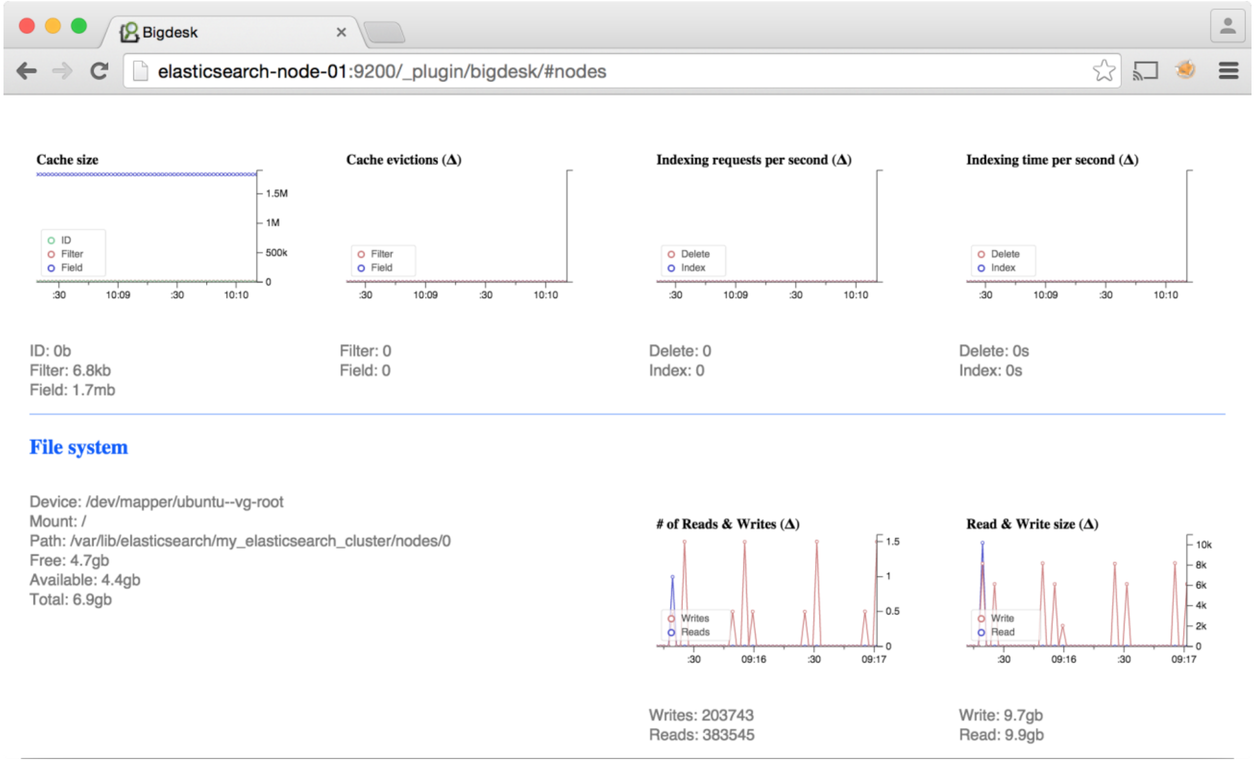
Series: weighted avg
Sys total: 7320ms
User total: 27820ms

Total: 100%
Process: 1%

HTTP & Transport

HTTP address:
inet[/192.168.1.136:9200]

Transport address:
inet[/192.168.1.136:9300]



ID: 0b
Filter: 6.8kb
Field: 1.7mb

Filter: 0
Field: 0

Delete: 0
Index: 0

Delete: 0s
Index: 0s

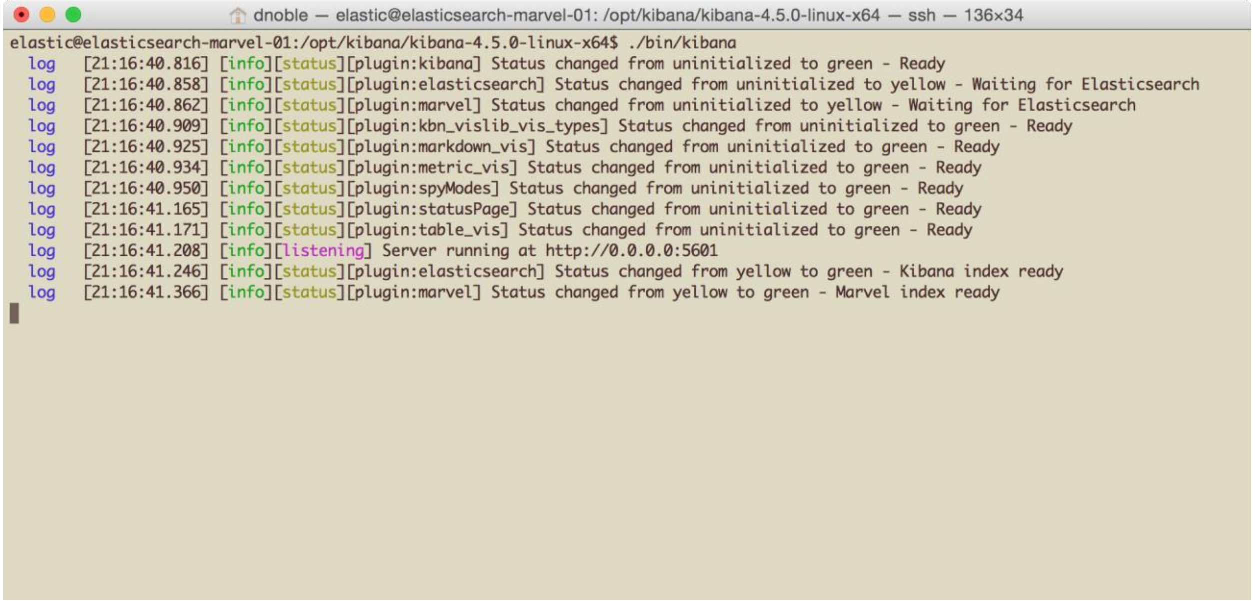
File system

Device: /dev/mapper/ubuntu--vg-root
Mount: /
Path: /var/lib/elasticsearch/my_elasticsearch_cluster/nodes/0
Free: 4.7gb
Available: 4.4gb
Total: 6.9gb

Writes: 203743
Reads: 383545

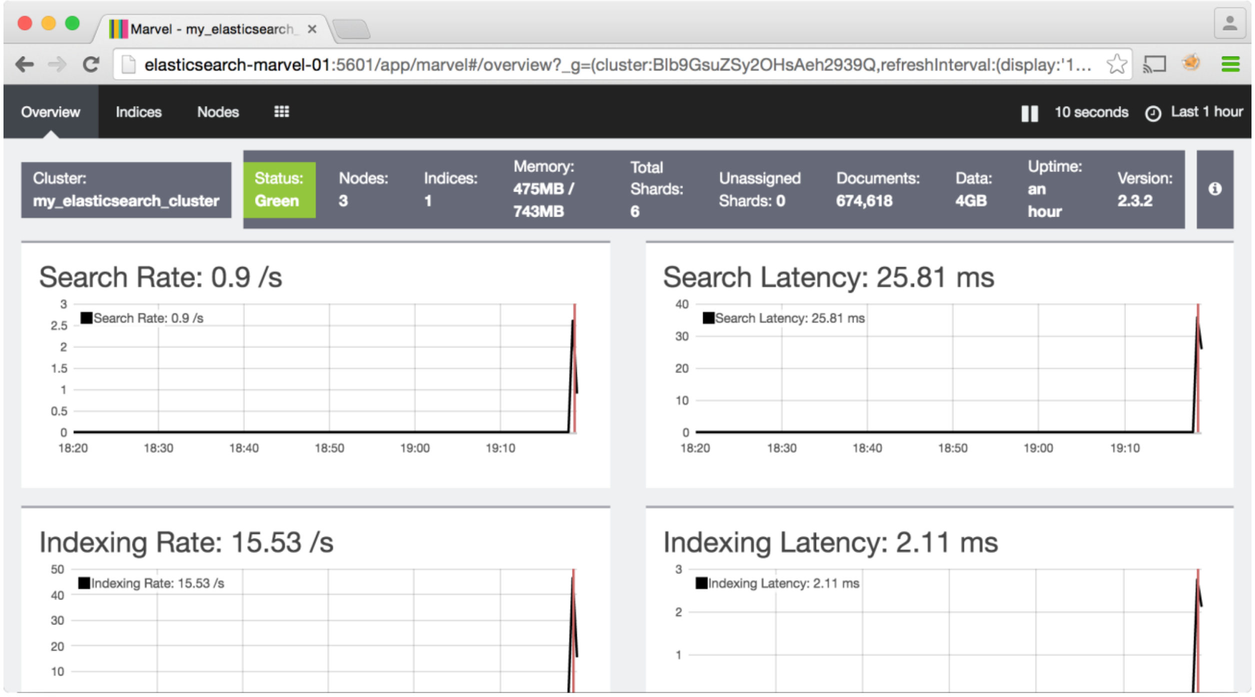
Write: 9.7gb
Read: 9.9gb

Chapter 4: Marvel Dashboard



dnoble — elastic@elasticsearch-marvel-01: /opt/kibana/kibana-4.5.0-linux-x64 — ssh — 136×34

```
elastic@elasticsearch-marvel-01:/opt/kibana/kibana-4.5.0-linux-x64$ ./bin/kibana
  log   [21:16:40.816] [info][status][plugin:kibana] Status changed from uninitialized to green - Ready
  log   [21:16:40.858] [info][status][plugin:elasticsearch] Status changed from uninitialized to yellow - Waiting for Elasticsearch
  log   [21:16:40.862] [info][status][plugin:marvel] Status changed from uninitialized to yellow - Waiting for Elasticsearch
  log   [21:16:40.909] [info][status][plugin:kbn_vislib_vis_types] Status changed from uninitialized to green - Ready
  log   [21:16:40.925] [info][status][plugin:markdown_vis] Status changed from uninitialized to green - Ready
  log   [21:16:40.934] [info][status][plugin:metric_vis] Status changed from uninitialized to green - Ready
  log   [21:16:40.950] [info][status][plugin:spyModes] Status changed from uninitialized to green - Ready
  log   [21:16:41.165] [info][status][plugin:statusPage] Status changed from uninitialized to green - Ready
  log   [21:16:41.171] [info][status][plugin:table_vis] Status changed from uninitialized to green - Ready
  log   [21:16:41.208] [info][listening] Server running at http://0.0.0.0:5601
  log   [21:16:41.246] [info][status][plugin:elasticsearch] Status changed from yellow to green - Kibana index ready
  log   [21:16:41.366] [info][status][plugin:marvel] Status changed from yellow to green - Marvel index ready
```



Marvel - my_elasticsearch_
elasticsearch-marvel-01:5601/app/marvel#/overview?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'1…
Overview
Indices
Nodes
10 seconds
Last 1 hour

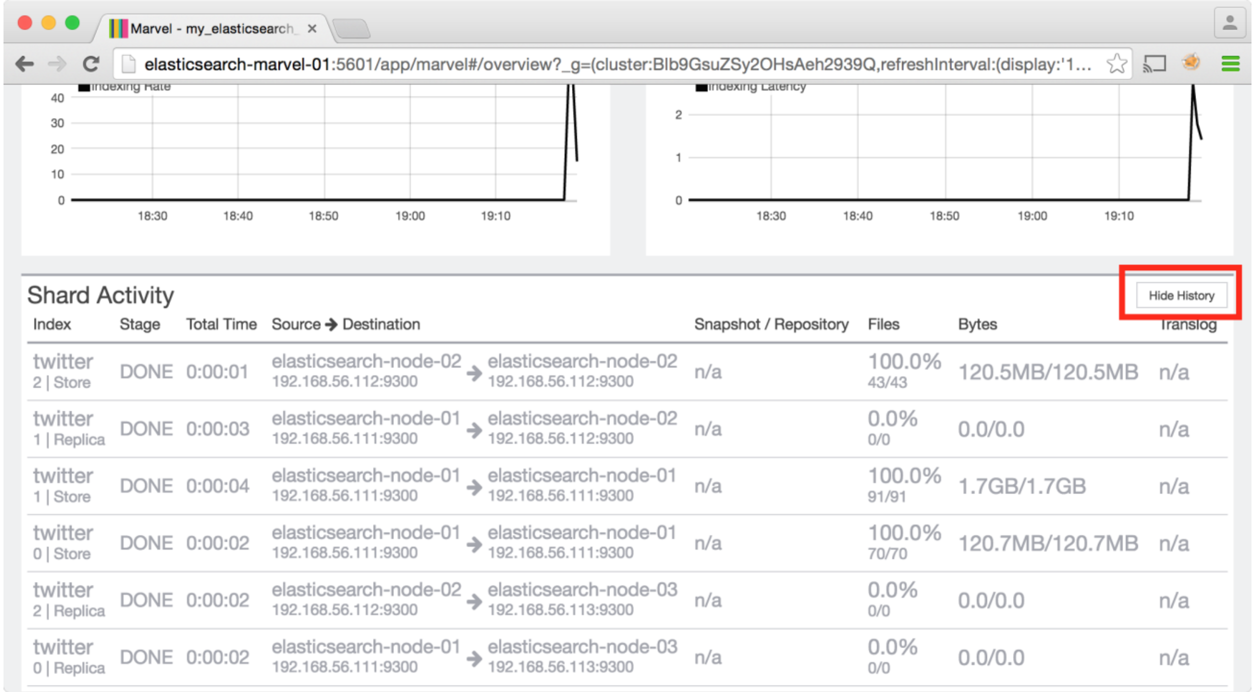
Cluster: my_elasticsearch_cluster | Status: Green | Nodes: 3 | Indices: 1 | Memory: 475MB / 743MB | Total Shards: 6 | Unassigned Shards: 0 | Documents: 674,618 | Data: 4GB | Uptime: an hour | Version: 2.3.2

Search Rate: 0.9 /s

Search Latency: 25.81 ms

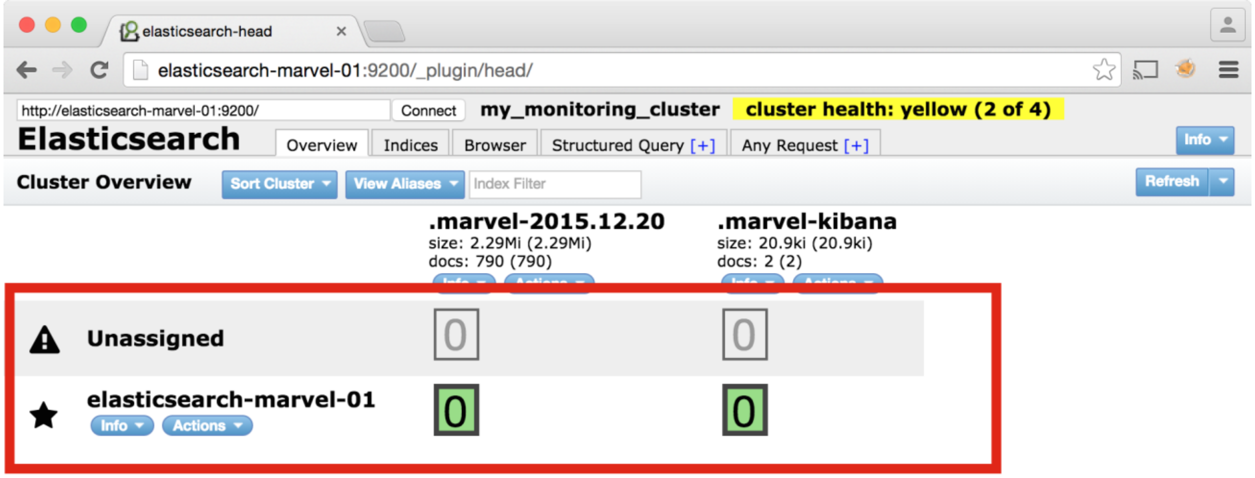
Indexing Rate: 15.53 /s

Indexing Latency: 2.11 ms


Marvel - my_elasticsearch
elasticsearch-marvel-01:5601/app/marvel#/overview?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'1…
Indexing Rate
40
30
20
10
0
18:30
18:40
18:50
19:00
19:10
Indexing Latency
2
1
0
18:30
18:40
18:50
19:00
19:10
Hide History

Shard Activity

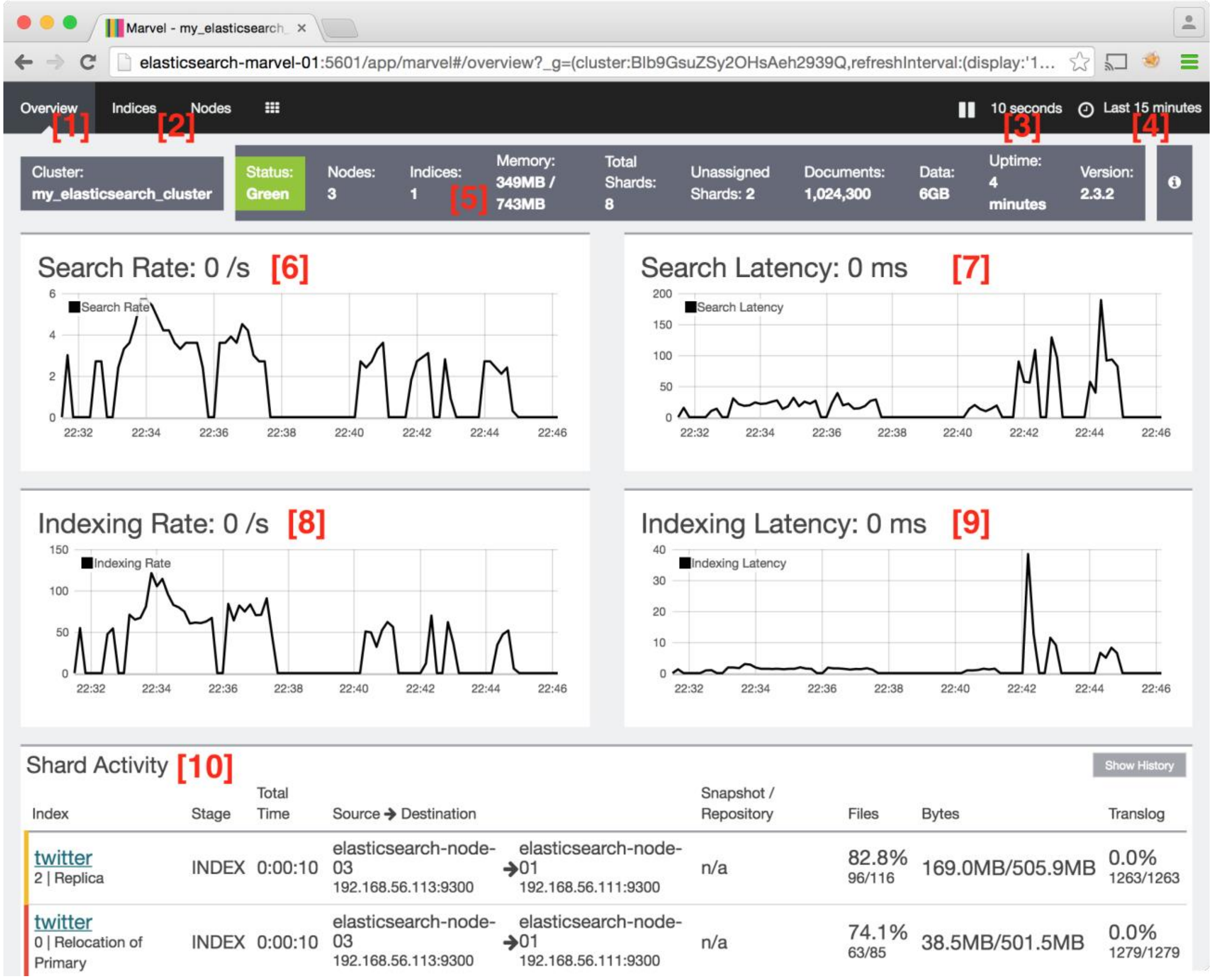
Index	Stage	Total Time	Source → Destination		Snapshot / Repository	Files	Bytes	Translog
twitter 2 | Store	DONE	0:00:01	elasticsearch-node-02 192.168.56.112:9300	elasticsearch-node-02 192.168.56.112:9300	n/a	100.0% 43/43	120.5MB/120.5MB	n/a
twitter 1 | Replica	DONE	0:00:03	elasticsearch-node-01 192.168.56.111:9300	elasticsearch-node-02 192.168.56.112:9300	n/a	0.0% 0/0	0.0/0.0	n/a
twitter 1 | Store	DONE	0:00:04	elasticsearch-node-01 192.168.56.111:9300	elasticsearch-node-01 192.168.56.111:9300	n/a	100.0% 91/91	1.7GB/1.7GB	n/a
twitter 0 | Store	DONE	0:00:02	elasticsearch-node-01 192.168.56.111:9300	elasticsearch-node-01 192.168.56.111:9300	n/a	100.0% 70/70	120.7MB/120.7MB	n/a
twitter 2 | Replica	DONE	0:00:02	elasticsearch-node-02 192.168.56.112:9300	elasticsearch-node-03 192.168.56.113:9300	n/a	0.0% 0/0	0.0/0.0	n/a
twitter 0 | Replica	DONE	0:00:02	elasticsearch-node-01 192.168.56.111:9300	elasticsearch-node-03 192.168.56.113:9300	n/a	0.0% 0/0	0.0/0.0	n/a



http://elasticsearch-marvel-01:9200/

my_monitoring_cluster cluster health: yellow (2 of 4)

	.marvel-2015.12.20 size: 2.29Mi (2.29Mi) docs: 790 (790)	.marvel-kibana size: 20.9ki (20.9ki) docs: 2 (2)
⚠ Unassigned	0	0
★ elasticsearch-marvel-01	0	0



Cluster: my_elasticsearch_cluster

Status: Green | Nodes: 3 | Indices: 1 | Memory: 349MB / 743MB | Total Shards: 8 | Unassigned Shards: 2 | Documents: 1,024,300 | Data: 6GB | Uptime: 4 minutes | Version: 2.3.2

Search Rate: 0 /s

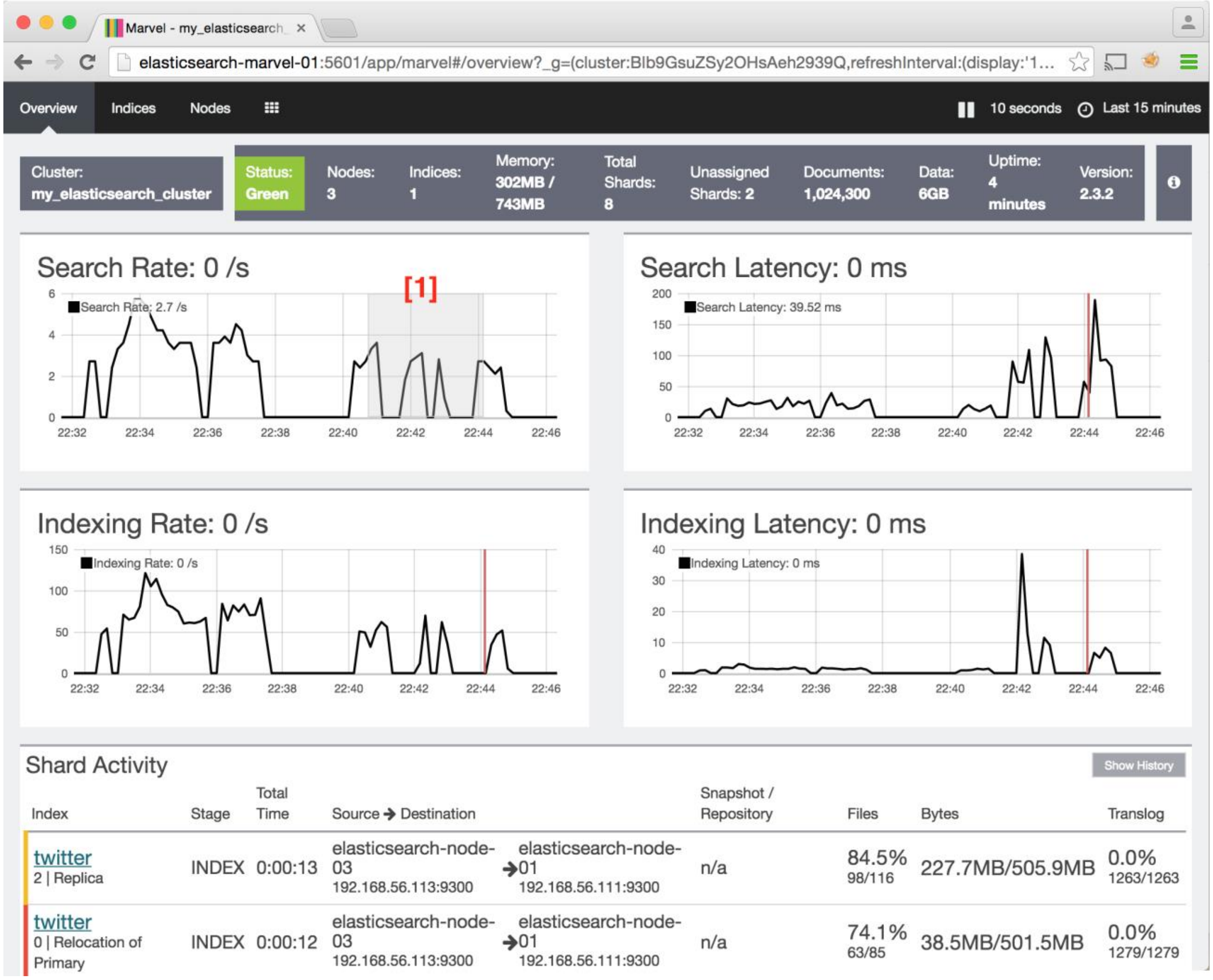
Search Latency: 0 ms

Indexing Rate: 0 /s

Indexing Latency: 0 ms

Shard Activity

Index	Stage	Total Time	Source → Destination		Snapshot / Repository	Files	Bytes	Translog
twitter 2 | Replica	INDEX	0:00:10	elasticsearch-node-03 192.168.56.113:9300	→elasticsearch-node-01 192.168.56.111:9300	n/a	82.8% 96/116	169.0MB/505.9MB	0.0% 1263/1263
twitter 0 | Relocation of Primary	INDEX	0:00:10	elasticsearch-node-03 192.168.56.113:9300	→elasticsearch-node-01 192.168.56.111:9300	n/a	74.1% 63/85	38.5MB/501.5MB	0.0% 1279/1279

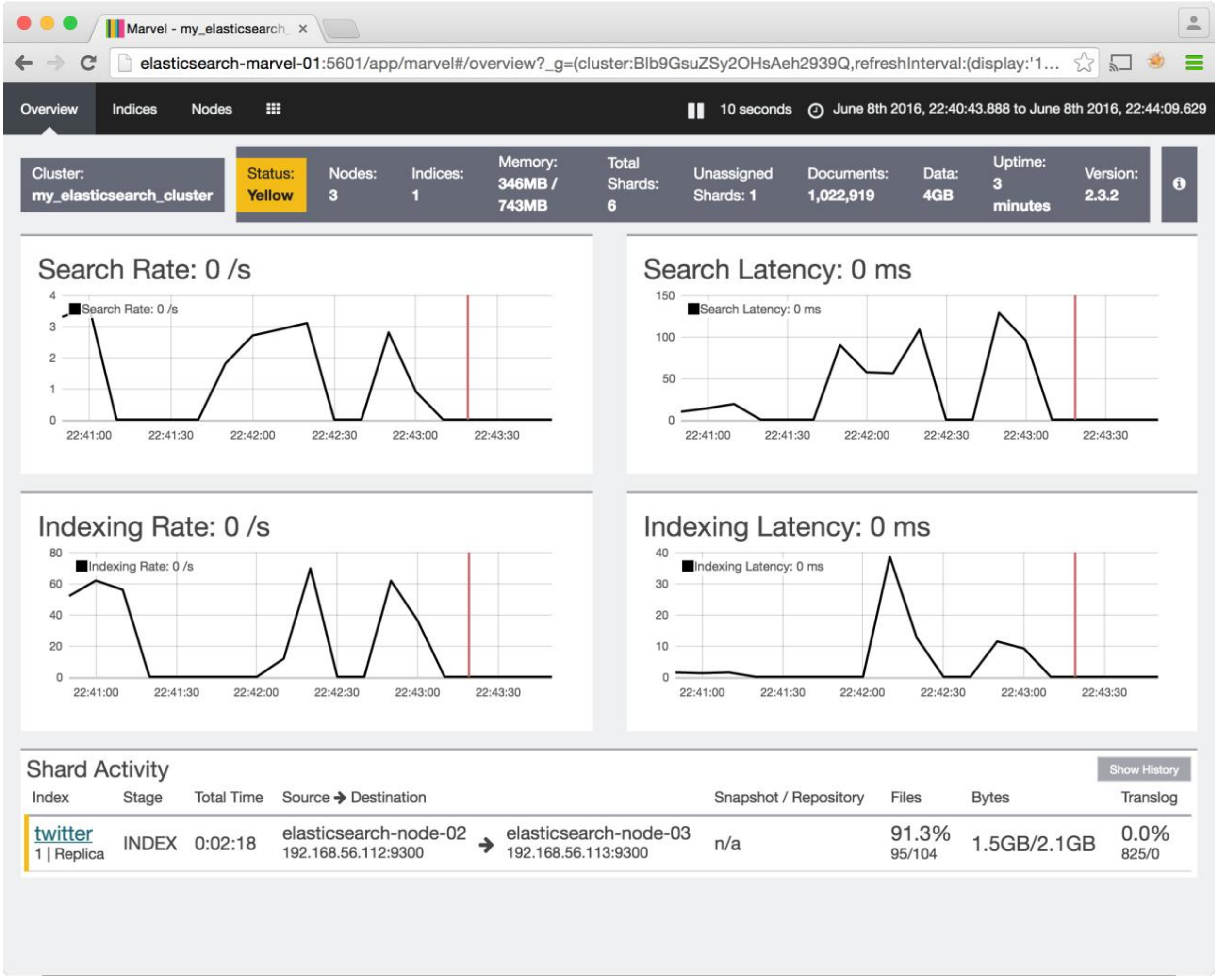


Marvel - my_elasticsearch_
elasticsearch-marvel-01:5601/app/marvel#/overview?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'1…
Overview
Indices
Nodes
10 seconds
Last 15 minutes

Cluster:	Status:	Nodes:	Indices:	Memory:	Total Shards:	Unassigned Shards:	Documents:	Data:	Uptime:	Version:
my_elasticsearch_cluster	Green	3	1	302MB / 743MB	8	2	1,024,300	6GB	4 minutes	2.3.2

Shard Activity

Index	Stage	Total Time	Source → Destination		Snapshot / Repository	Files	Bytes	Translog
twitter 2 | Replica	INDEX	0:00:13	elasticsearch-node-03 192.168.56.113:9300	→ elasticsearch-node-01 192.168.56.111:9300	n/a	84.5% 98/116	227.7MB/505.9MB	0.0% 1263/1263
twitter 0 | Relocation of Primary	INDEX	0:00:12	elasticsearch-node-03 192.168.56.113:9300	→ elasticsearch-node-01 192.168.56.111:9300	n/a	74.1% 63/85	38.5MB/501.5MB	0.0% 1279/1279



Marvel - my_elasticsearch_
elasticsearch-marvel-01:5601/app/marvel#/overview?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'1…
Overview
Indices
Nodes
10 seconds
June 8th 2016, 22:40:43.888 to June 8th 2016, 22:44:09.629

Cluster: my_elasticsearch_cluster

Status: Yellow

Nodes: 3

Indices: 1

Memory: 346MB / 743MB

Total Shards: 6

Unassigned Shards: 1

Documents: 1,022,919

Data: 4GB

Uptime: 3 minutes

Version: 2.3.2

Search Rate: 0 /s

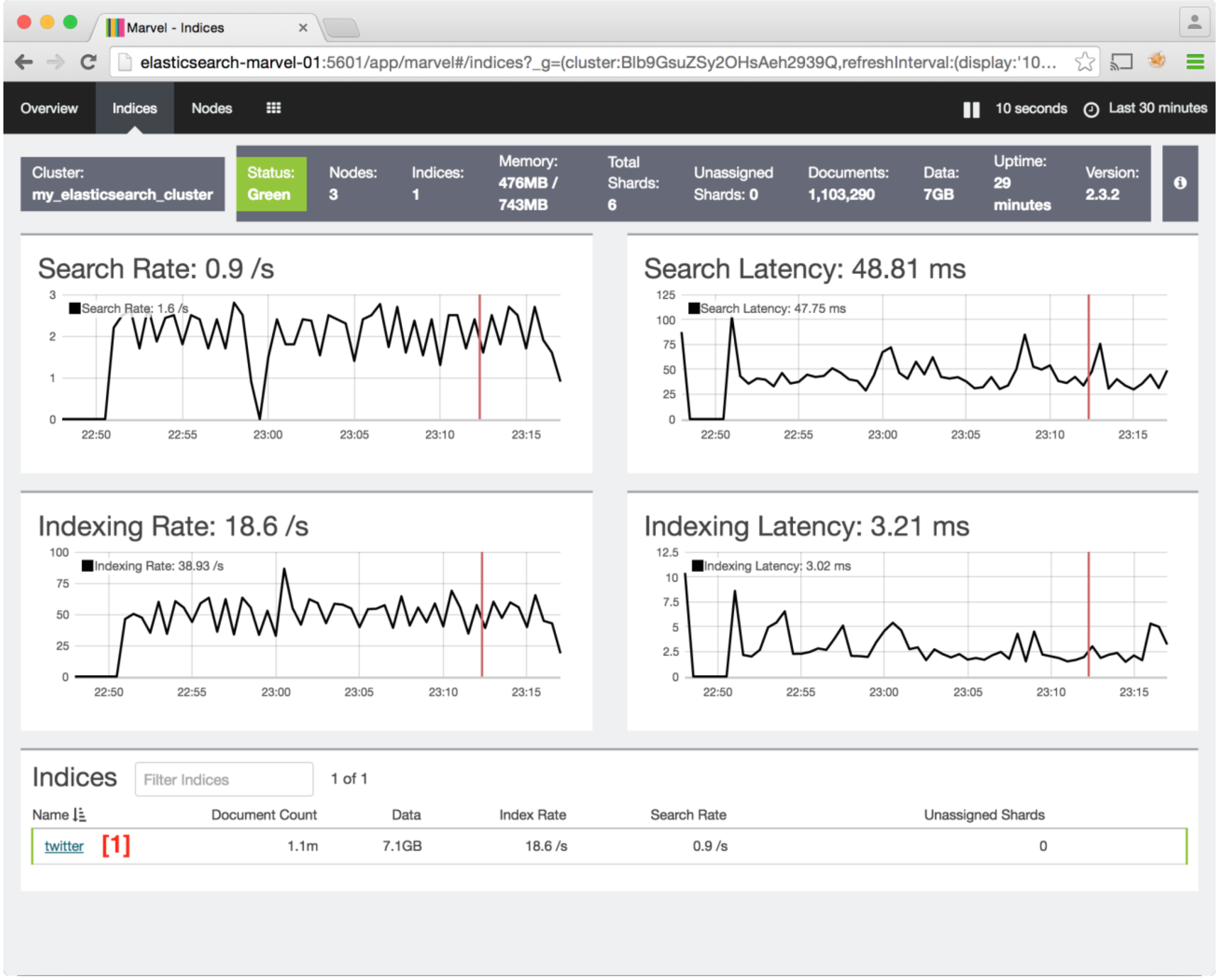
Search Latency: 0 ms

Indexing Rate: 0 /s

Indexing Latency: 0 ms

Shard Activity

Index	Stage	Total Time	Source → Destination		Snapshot / Repository	Files	Bytes	Translog
twitter 1 | Replica	INDEX	0:02:18	elasticsearch-node-02 192.168.56.112:9300 →	elasticsearch-node-03 192.168.56.113:9300	n/a	91.3% 95/104	1.5GB/2.1GB	0.0% 825/0



Marvel - Indices
elasticsearch-marvel-01:5601/app/marvel#/indices?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'10…
Overview
Indices
Nodes
10 seconds
Last 30 minutes

Cluster: my_elasticsearch_cluster

Status: Green

Nodes: 3

Indices: 1

Memory: 476MB / 743MB

Total Shards: 6

Unassigned Shards: 0

Documents: 1,103,290

Data: 7GB

Uptime: 29 minutes

Version: 2.3.2

Search Rate: 0.9 /s

Search Latency: 48.81 ms

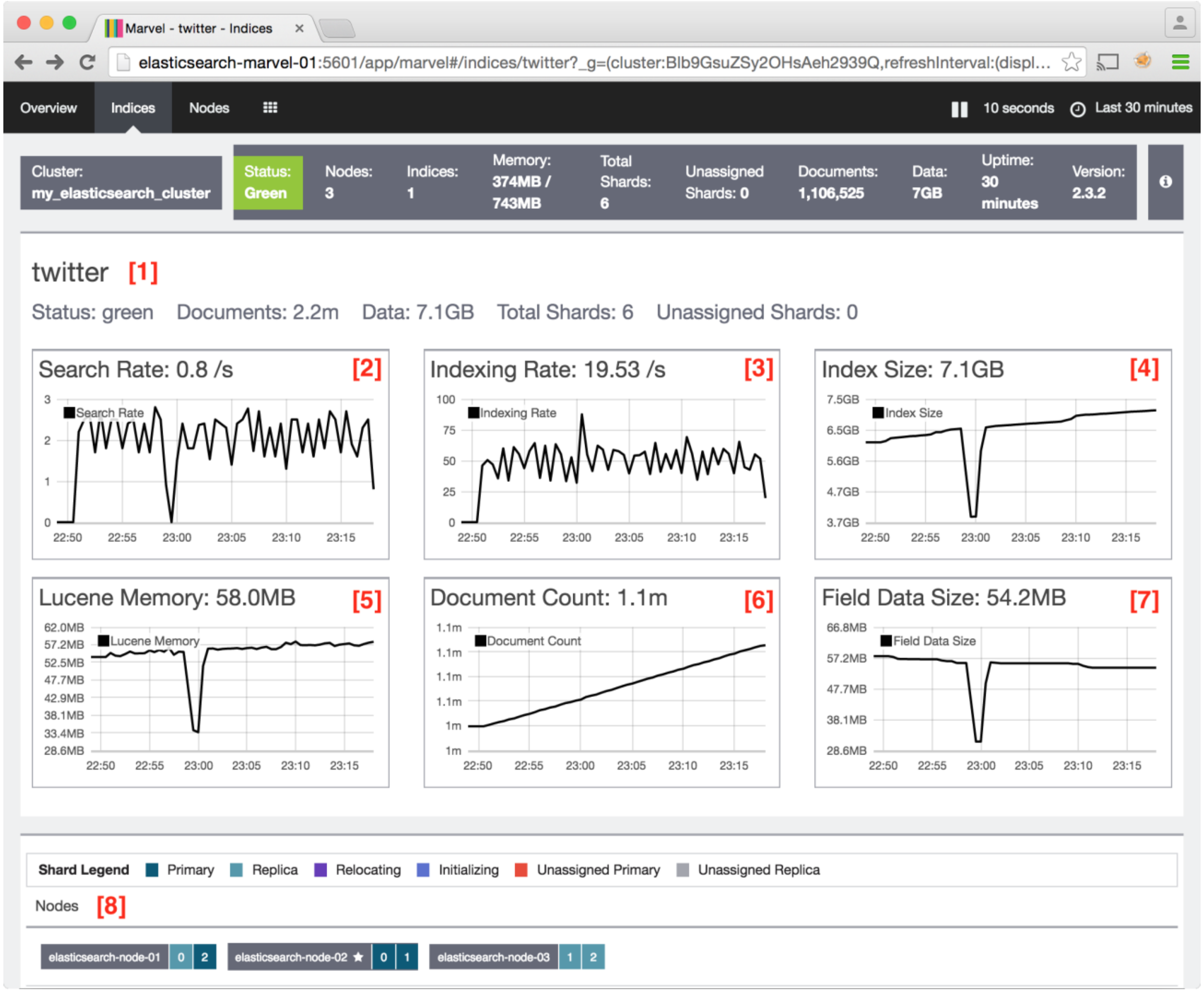
Indexing Rate: 18.6 /s

Indexing Latency: 3.21 ms

Indices

1 of 1

Name	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
twitter [1]	1.1m	7.1GB	18.6 /s	0.9 /s	0



Marvel - twitter - Indices

elasticsearch-marvel-01:5601/app/marvel#/indices/twitter?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(displ…

Overview Indices Nodes

10 seconds Last 30 minutes

Cluster: my_elasticsearch_cluster | Status: Green | Nodes: 3 | Indices: 1 | Memory: 374MB / 743MB | Total Shards: 6 | Unassigned Shards: 0 | Documents: 1,106,525 | Data: 7GB | Uptime: 30 minutes | Version: 2.3.2

twitter [1]

Status: green Documents: 2.2m Data: 7.1GB Total Shards: 6 Unassigned Shards: 0

Search Rate: 0.8 /s [2]

Indexing Rate: 19.53 /s [3]

Index Size: 7.1GB [4]

Lucene Memory: 58.0MB [5]

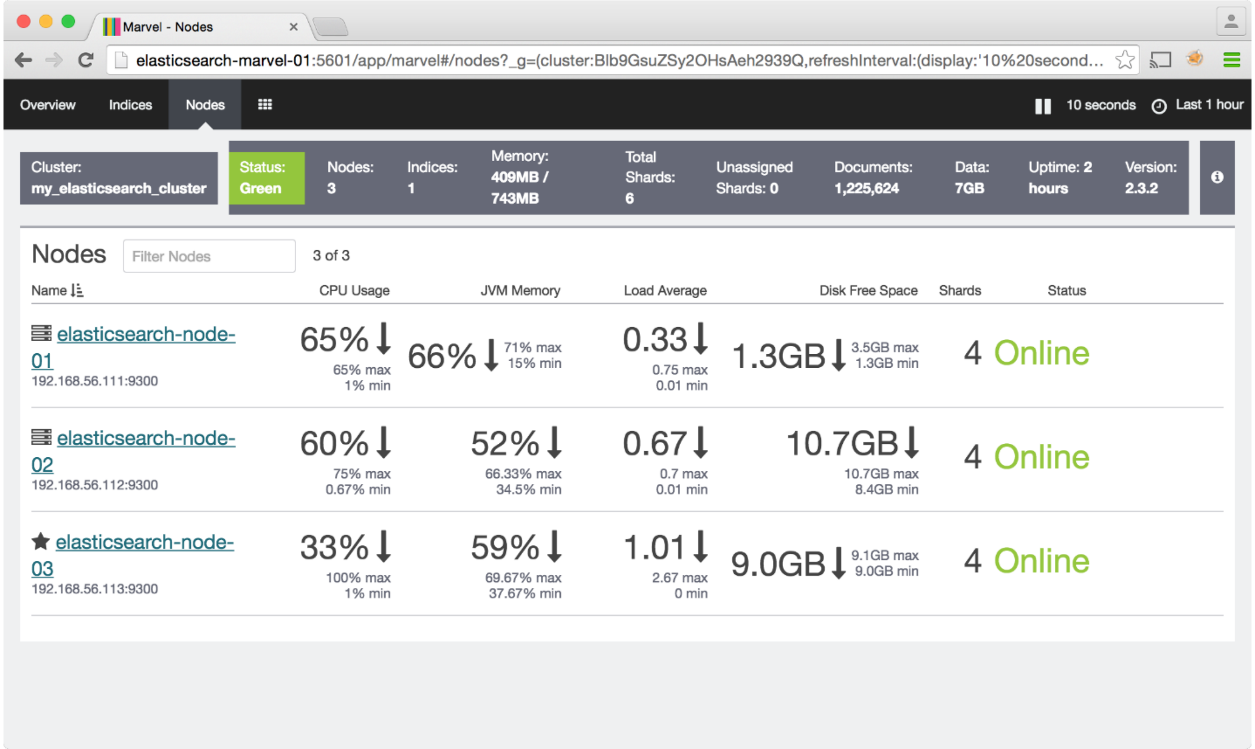
Document Count: 1.1m [6]

Field Data Size: 54.2MB [7]

Shard Legend ■ Primary ■ Replica ■ Relocating ■ Initializing ■ Unassigned Primary ■ Unassigned Replica

Nodes [8]

elasticsearch-node-01 0 2 | elasticsearch-node-02 ★ 0 1 | elasticsearch-node-03 1 2

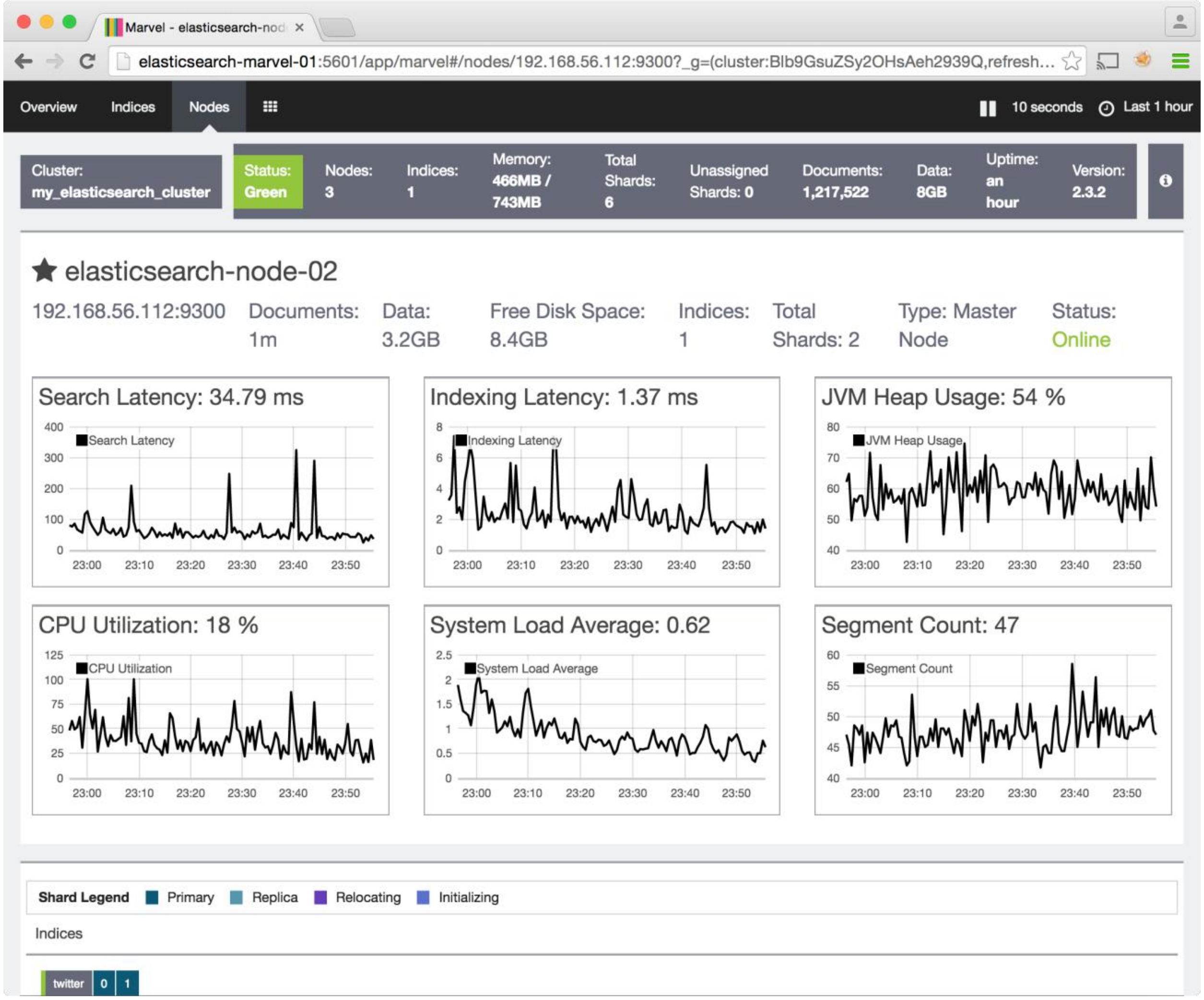


elasticsearch-marvel-01:5601/app/marvel#/nodes?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'10%20second…

Cluster: **my_elasticsearch_cluster** | Status: **Green** | Nodes: **3** | Indices: **1** | Memory: **409MB / 743MB** | Total Shards: **6** | Unassigned Shards: **0** | Documents: **1,225,624** | Data: **7GB** | Uptime: **2 hours** | Version: **2.3.2**

Nodes Filter Nodes 3 of 3

Name	CPU Usage	JVM Memory	Load Average	Disk Free Space	Shards	Status
elasticsearch-node-01 192.168.56.111:9300	65% 65% max 1% min	66% 71% max 15% min	0.33 0.75 max 0.01 min	1.3GB 3.5GB max 1.3GB min	4	Online
elasticsearch-node-02 192.168.56.112:9300	60% 75% max 0.67% min	52% 66.33% max 34.5% min	0.67 0.7 max 0.01 min	10.7GB 10.7GB max 8.4GB min	4	Online
★ elasticsearch-node-03 192.168.56.113:9300	33% 100% max 1% min	59% 69.67% max 37.67% min	1.01 2.67 max 0 min	9.0GB 9.1GB max 9.0GB min	4	Online


Marvel - elasticsearch-nod
elasticsearch-marvel-01:5601/app/marvel#/nodes/192.168.56.112:9300?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refresh…
Overview
Indices
Nodes
10 seconds
Last 1 hour

Cluster: my_elasticsearch_cluster | Status: Green | Nodes: 3 | Indices: 1 | Memory: 466MB / 743MB | Total Shards: 6 | Unassigned Shards: 0 | Documents: 1,217,522 | Data: 8GB | Uptime: an hour | Version: 2.3.2

★ elasticsearch-node-02

192.168.56.112:9300 | Documents: 1m | Data: 3.2GB | Free Disk Space: 8.4GB | Indices: 1 | Total Shards: 2 | Type: Master Node | Status: Online

Search Latency: 34.79 ms

Indexing Latency: 1.37 ms

JVM Heap Usage: 54 %

CPU Utilization: 18 %

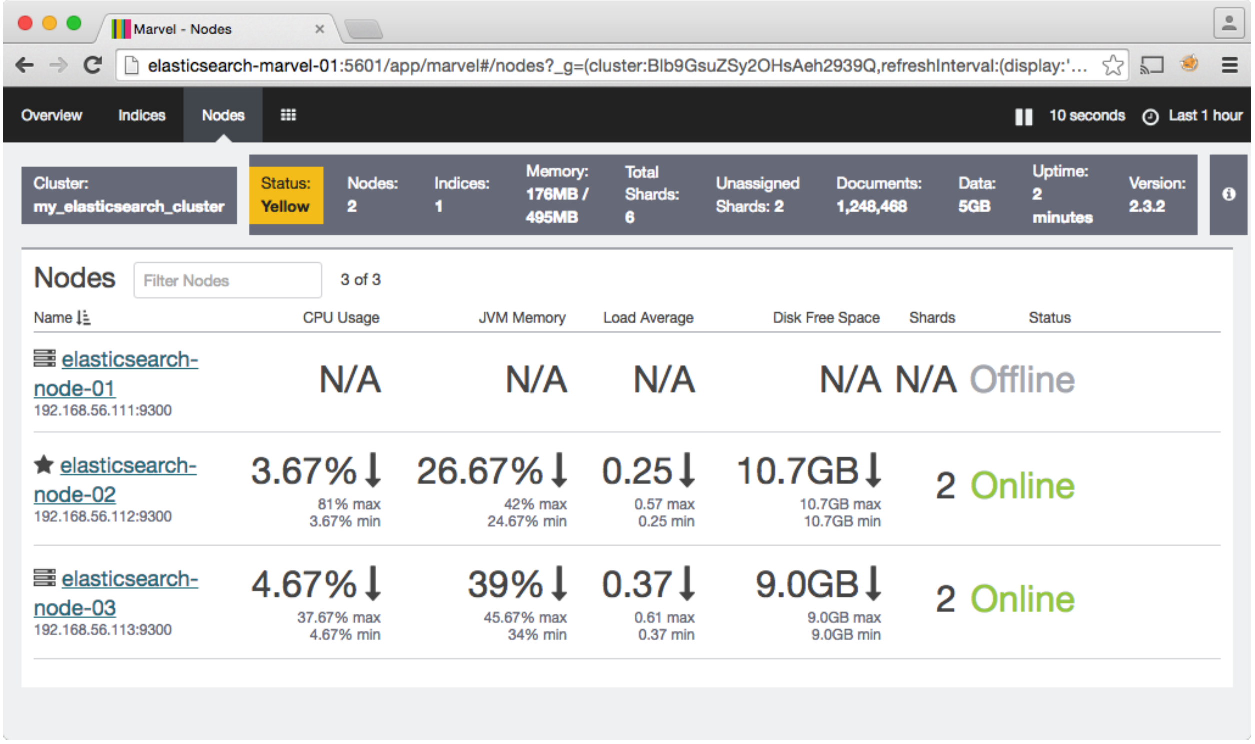
System Load Average: 0.62

Segment Count: 47

Shard Legend 🟦 Primary 🟦 Replica 🟪 Relocating 🟦 Initializing

Indices

twitter 0 1

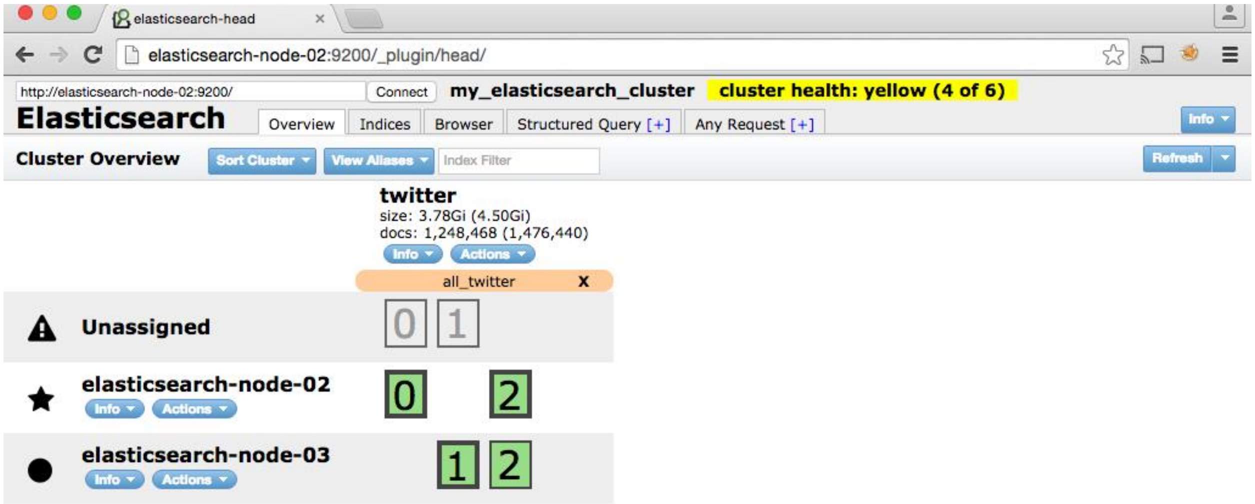


Marvel - Nodes
elasticsearch-marvel-01:5601/app/marvel#/nodes?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(display:'…
Overview
Indices
Nodes
10 seconds
Last 1 hour

Cluster: my_elasticsearch_cluster | Status: Yellow | Nodes: 2 | Indices: 1 | Memory: 176MB / 495MB | Total Shards: 6 | Unassigned Shards: 2 | Documents: 1,248,468 | Data: 5GB | Uptime: 2 minutes | Version: 2.3.2

Nodes | Filter Nodes | 3 of 3

Name	CPU Usage	JVM Memory	Load Average	Disk Free Space	Shards	Status
elasticsearch-node-01 192.168.56.111:9300	N/A	N/A	N/A	N/A	N/A	Offline
★ elasticsearch-node-02 192.168.56.112:9300	3.67% 81% max 3.67% min	26.67% 42% max 24.67% min	0.25 0.57 max 0.25 min	10.7GB 10.7GB max 10.7GB min	2	Online
elasticsearch-node-03 192.168.56.113:9300	4.67% 37.67% max 4.67% min	39% 45.67% max 34% min	0.37 0.61 max 0.37 min	9.0GB 9.0GB max 9.0GB min	2	Online

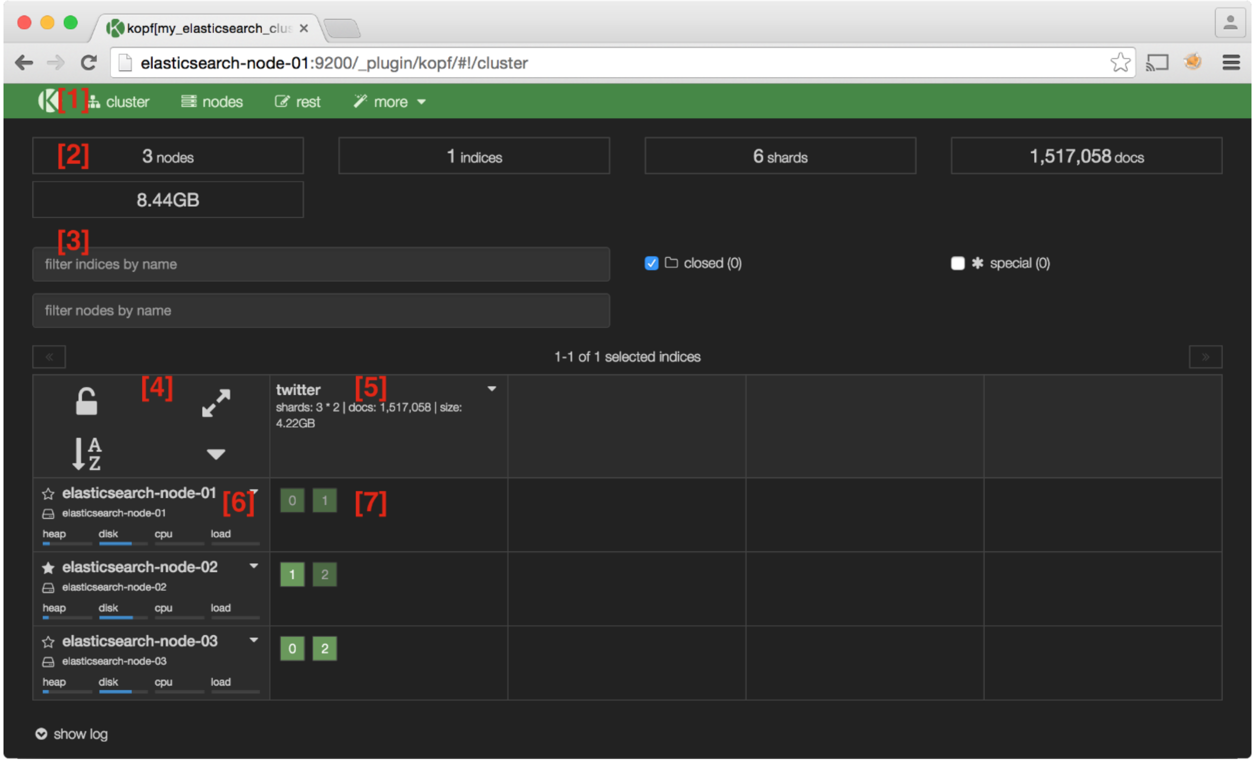


my_elasticsearch_cluster cluster health: yellow (4 of 6)

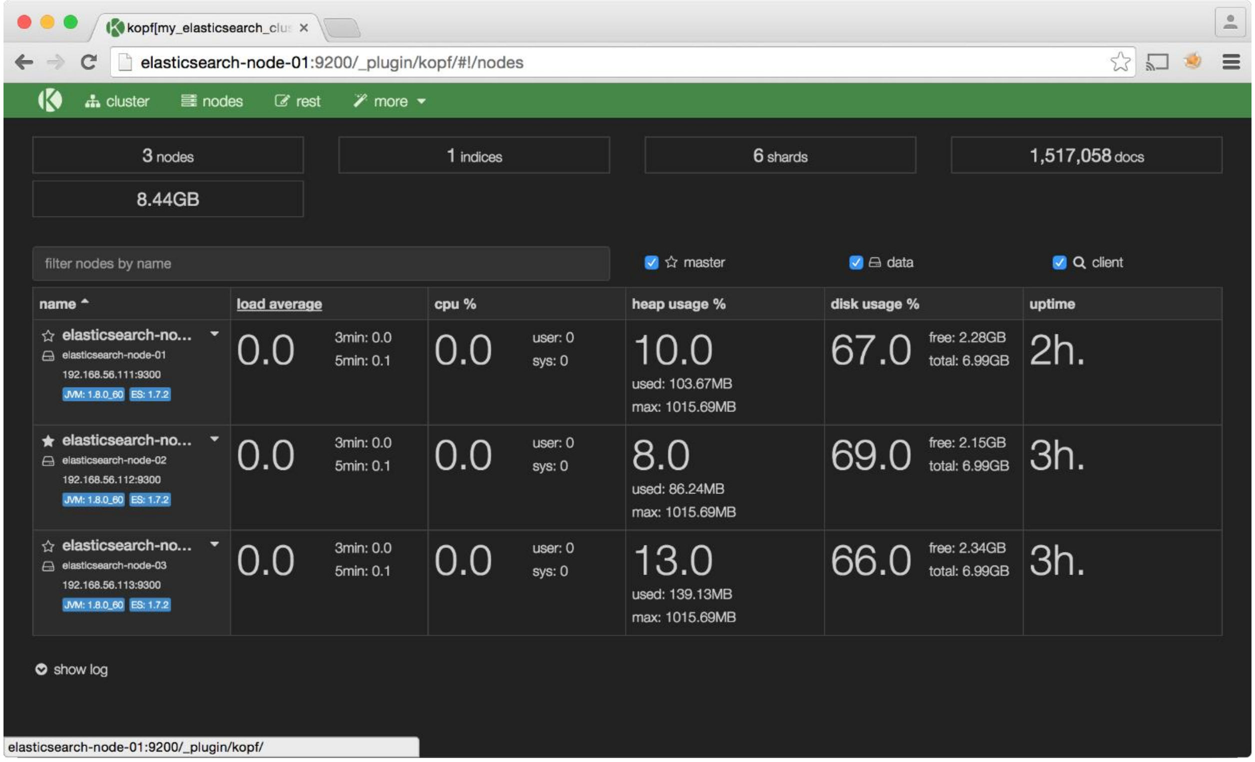
twitter
size: 3.78Gi (4.50Gi)
docs: 1,248,468 (1,476,440)

	twitter
Unassigned	0 1
★ elasticsearch-node-02	0 2
● elasticsearch-node-03	1 2

Chapter 5: System Monitoring



elasticsearch-node-01:9200/_plugin/kopf/#!/cluster



kopf[my_elasticsearch_clus ×
elasticsearch-node-01:9200/_plugin/kopf/#!/nodes
cluster
nodes
rest
more

3 nodes

1 indices

6 shards

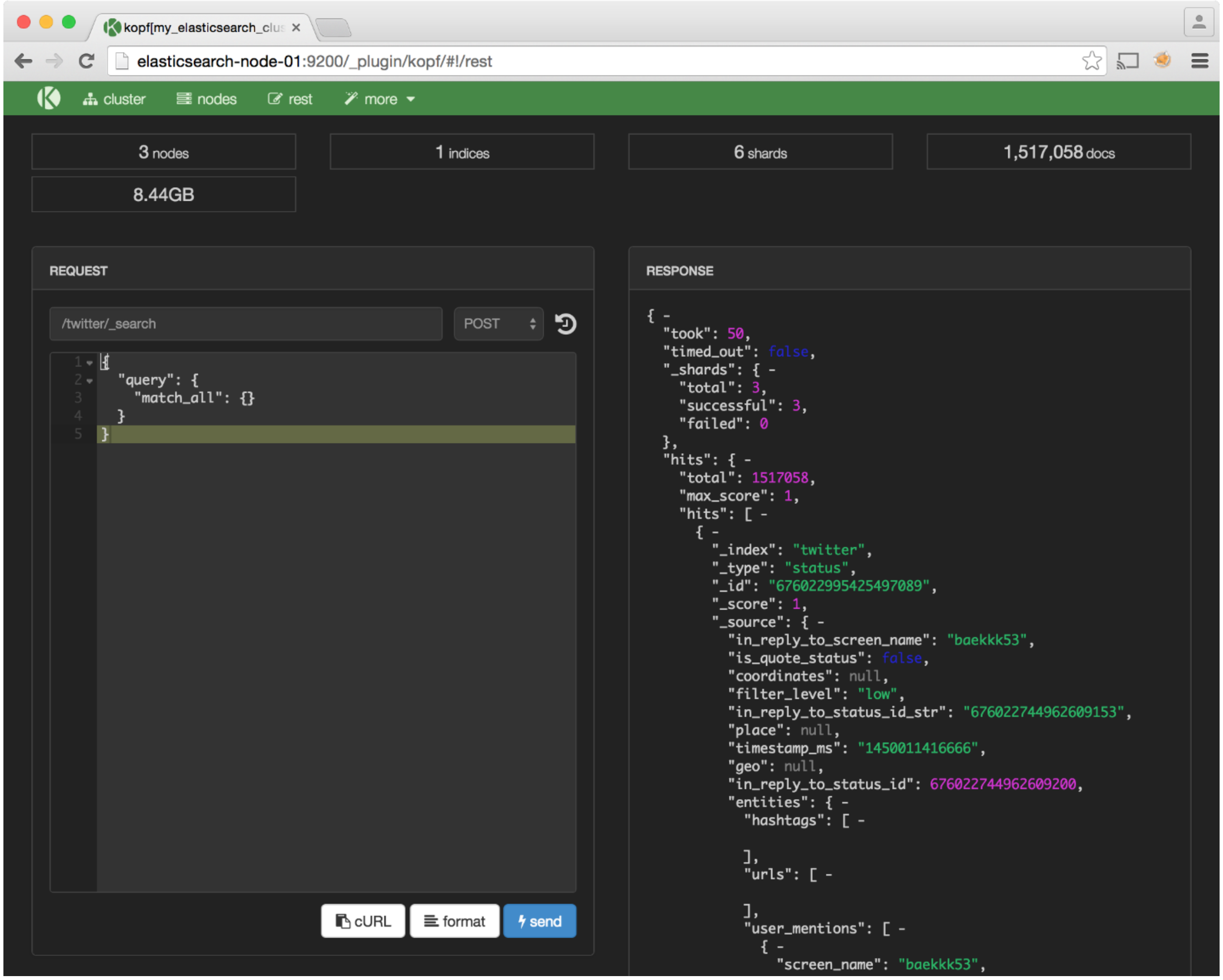
1,517,058 docs

8.44GB

filter nodes by name

☑ ☆ master ☑ data ☑ client

name	load average		cpu %		heap usage %	disk usage %		uptime
☆ elasticsearch-no... elasticsearch-node-01 192.168.56.111:9300 JVM: 1.8.0_60 ES: 1.7.2	0.0	3min: 0.0 5min: 0.1	0.0	user: 0 sys: 0	10.0 used: 103.67MB max: 1015.69MB	67.0	free: 2.28GB total: 6.99GB	2h.
★ elasticsearch-no... elasticsearch-node-02 192.168.56.112:9300 JVM: 1.8.0_60 ES: 1.7.2	0.0	3min: 0.0 5min: 0.1	0.0	user: 0 sys: 0	8.0 used: 86.24MB max: 1015.69MB	69.0	free: 2.15GB total: 6.99GB	3h.
☆ elasticsearch-no... elasticsearch-node-03 192.168.56.113:9300 JVM: 1.8.0_60 ES: 1.7.2	0.0	3min: 0.0 5min: 0.1	0.0	user: 0 sys: 0	13.0 used: 139.13MB max: 1015.69MB	66.0	free: 2.34GB total: 6.99GB	3h.



kopf[my_elasticsearch_clus
elasticsearch-node-01:9200/_plugin/kopf/#!/rest
cluster
nodes
rest
more
cURL
format
send

3 nodes

1 indices

6 shards

1,517,058 docs

8.44GB

REQUEST

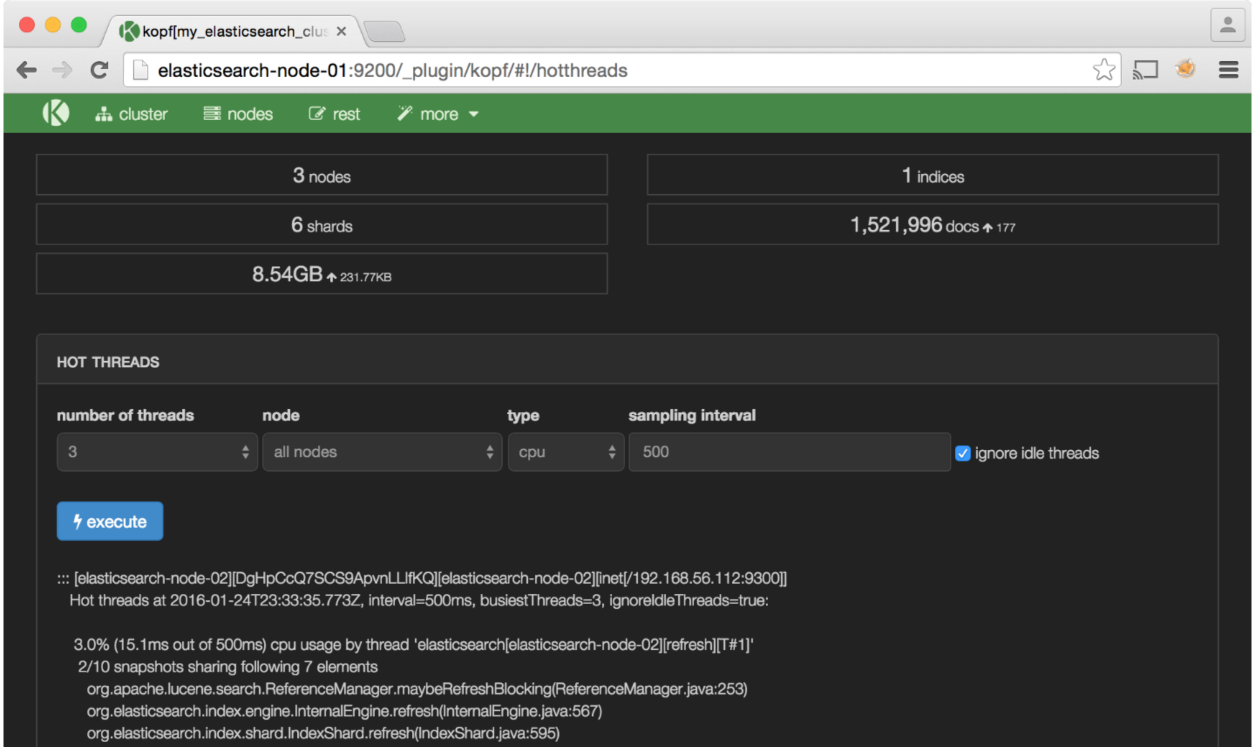
/twitter/_search

POST

```
{
  "query": {
    "match_all": {}
  }
}
```

RESPONSE

```
{ -
  "took": 50,
  "timed_out": false,
  "_shards": { -
    "total": 3,
    "successful": 3,
    "failed": 0
  },
  "hits": { -
    "total": 1517058,
    "max_score": 1,
    "hits": [ -
      { -
        "_index": "twitter",
        "_type": "status",
        "_id": "676022995425497089",
        "_score": 1,
        "_source": { -
          "in_reply_to_screen_name": "baekkk53",
          "is_quote_status": false,
          "coordinates": null,
          "filter_level": "low",
          "in_reply_to_status_id_str": "676022744962609153",
          "place": null,
          "timestamp_ms": "1450011416666",
          "geo": null,
          "in_reply_to_status_id": 676022744962609200,
          "entities": { -
            "hashtags": [ -

            ],
            "urls": [ -

            ],
            "user_mentions": [ -
              { -
                "screen_name": "baekkk53",
```



kopf[my_elasticsearch_clus ×
elasticsearch-node-01:9200/_plugin/kopf/#!/hotthreads
cluster
nodes
rest
more
execute

3 nodes

1 indices

6 shards

1,521,996 docs ↑ 177

8.54GB ↑ 231.77KB

HOT THREADS

number of threads: 3

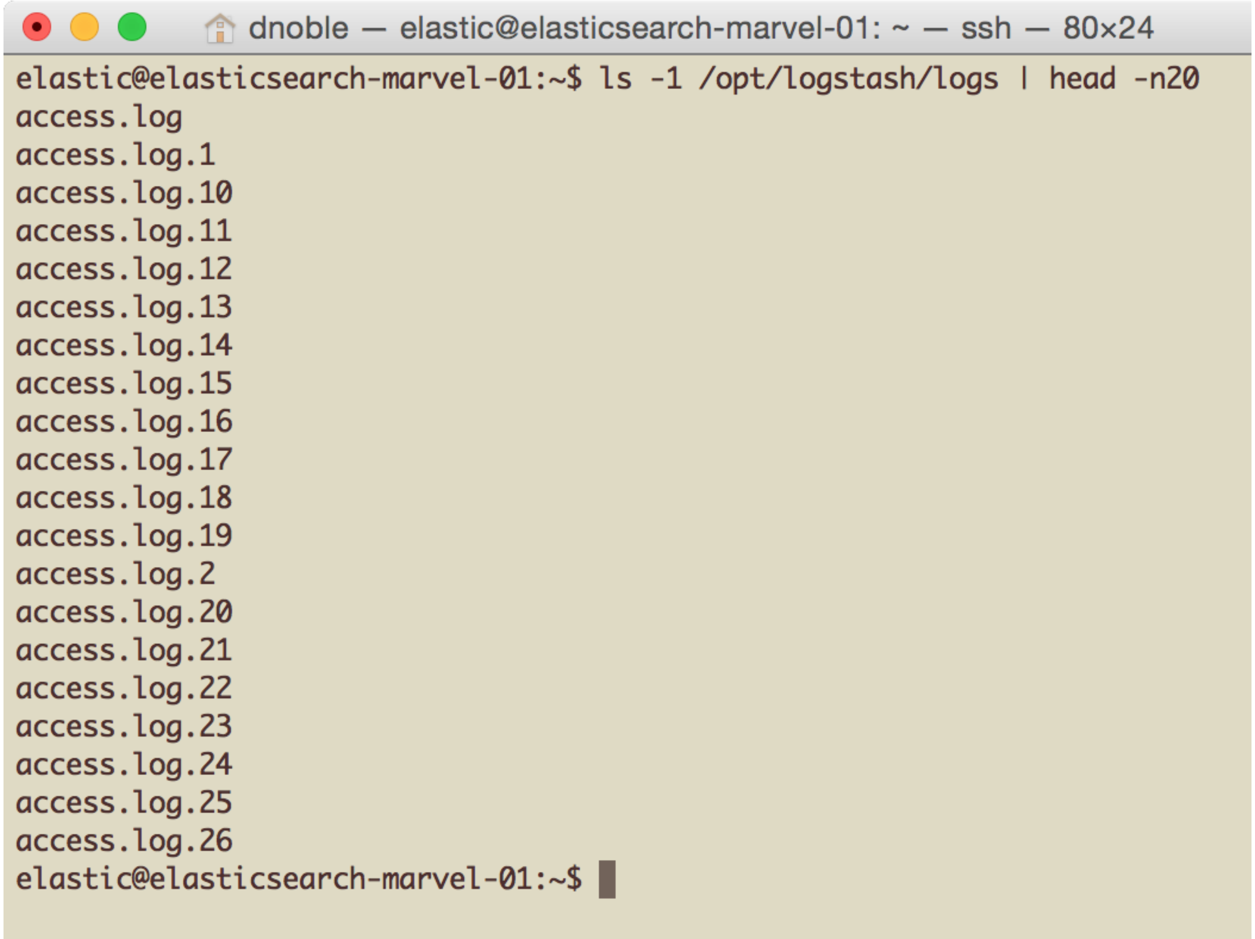
node: all nodes

type: cpu

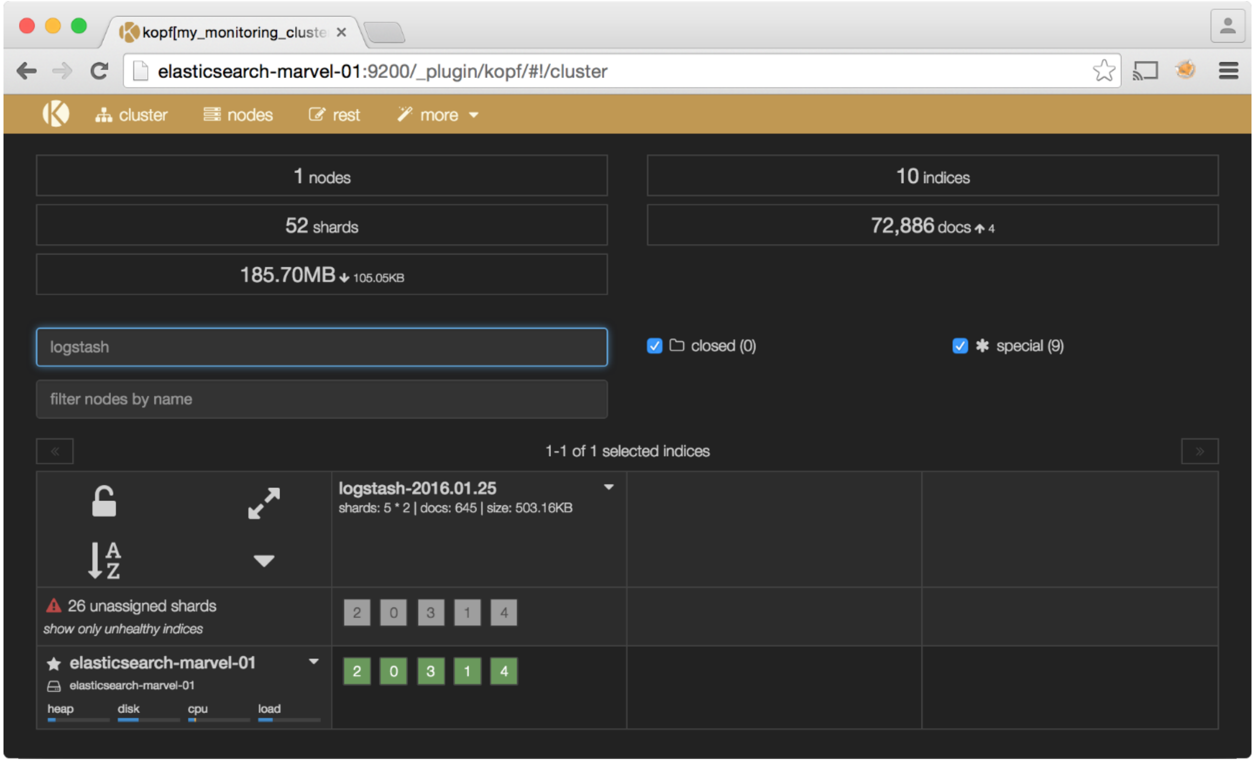
sampling interval: 500

☑ ignore idle threads

```
::: [elasticsearch-node-02][DgHpCcQ7SCS9ApvnLLlfKQ][elasticsearch-node-02][inet[/192.168.56.112:9300]]
   Hot threads at 2016-01-24T23:33:35.773Z, interval=500ms, busiestThreads=3, ignoreIdleThreads=true:

    3.0% (15.1ms out of 500ms) cpu usage by thread 'elasticsearch[elasticsearch-node-02][refresh][T#1]'
     2/10 snapshots sharing following 7 elements
       org.apache.lucene.search.ReferenceManager.maybeRefreshBlocking(ReferenceManager.java:253)
       org.elasticsearch.index.engine.InternalEngine.refresh(InternalEngine.java:567)
       org.elasticsearch.index.shard.IndexShard.refresh(IndexShard.java:595)
```



```
elastic@elasticsearch-marvel-01:~$ ls -1 /opt/logstash/logs | head -n20
access.log
access.log.1
access.log.10
access.log.11
access.log.12
access.log.13
access.log.14
access.log.15
access.log.16
access.log.17
access.log.18
access.log.19
access.log.2
access.log.20
access.log.21
access.log.22
access.log.23
access.log.24
access.log.25
access.log.26
elastic@elasticsearch-marvel-01:~$ 
```



elasticsearch-marvel-01:9200/_plugin/kopf/#!/cluster

1 nodes

10 indices

52 shards

72,886 docs ↑ 4

185.70MB ↓ 105.05KB

logstash

☑ closed (0)

☑ special (9)

filter nodes by name

1-1 of 1 selected indices

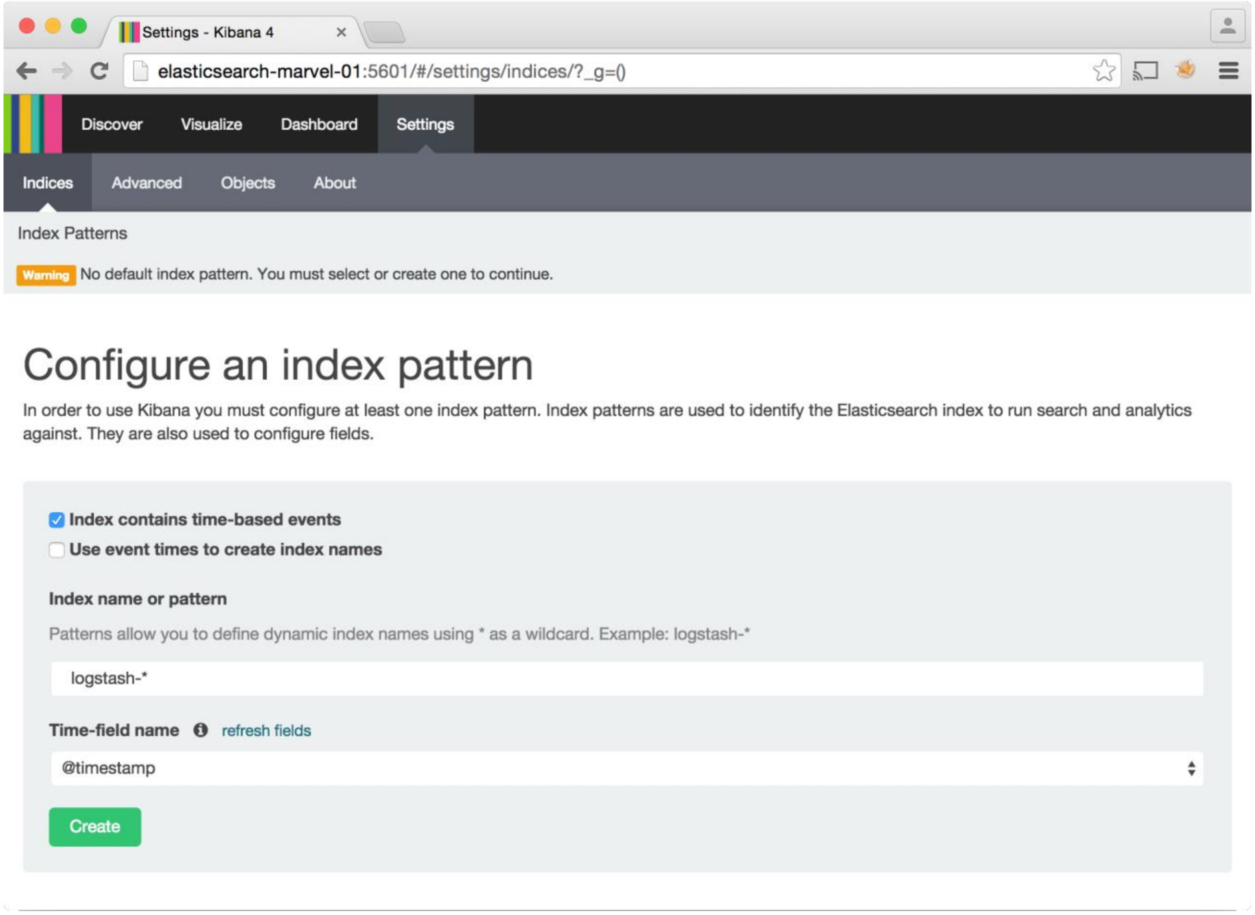
logstash-2016.01.25
shards: 5 * 2 | docs: 645 | size: 503.16KB

26 unassigned shards
show only unhealthy indices

2 0 3 1 4

elasticsearch-marvel-01
elasticsearch-marvel-01

2 0 3 1 4



elasticsearch-marvel-01:5601/#/settings/indices/?_g=()

Index Patterns

Warning No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☑ Index contains time-based events

□ Use event times to create index names

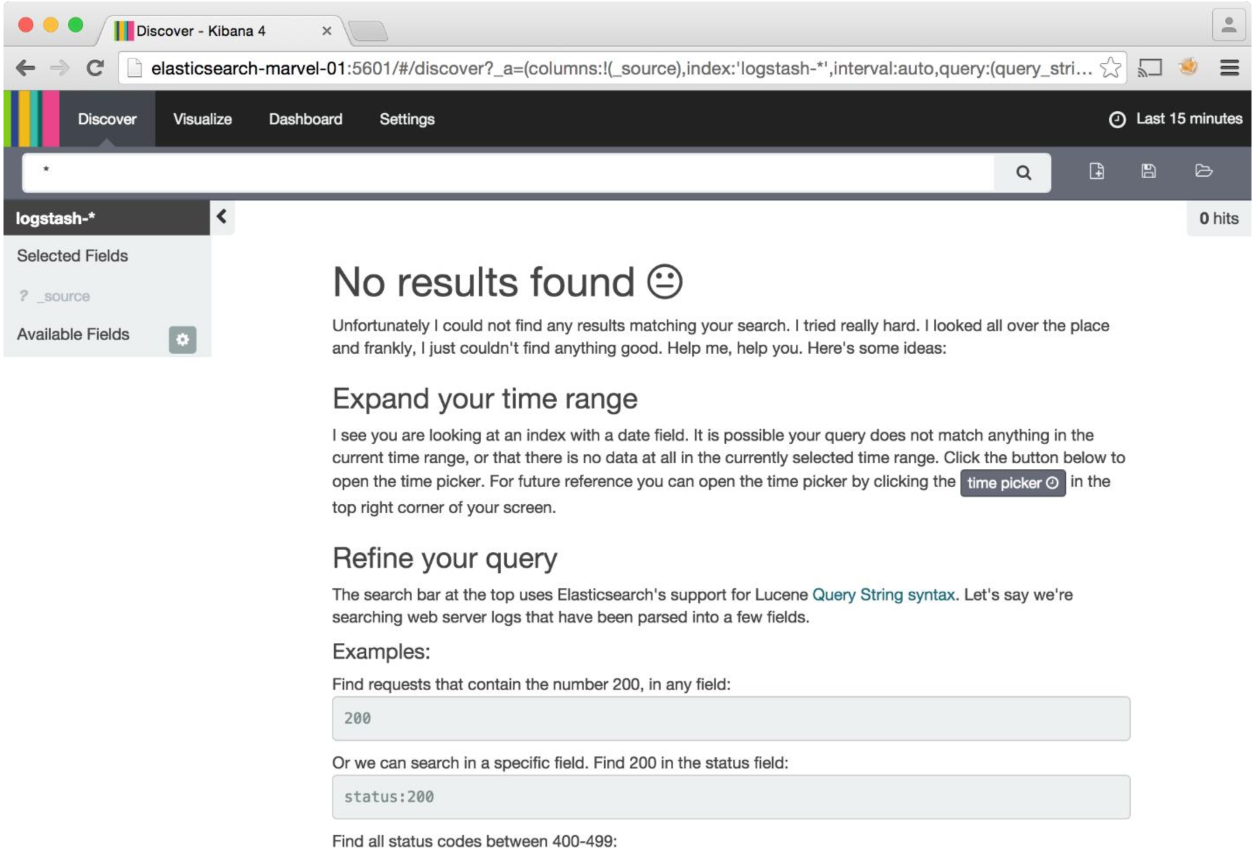
Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

logstash-*

Time-field name

@timestamp



No results found 😐

Unfortunately I could not find any results matching your search. I tried really hard. I looked all over the place and frankly, I just couldn't find anything good. Help me, help you. Here's some ideas:

Expand your time range

I see you are looking at an index with a date field. It is possible your query does not match anything in the current time range, or that there is no data at all in the currently selected time range. Click the button below to open the time picker. For future reference you can open the time picker by clicking the time picker in the top right corner of your screen.

Refine your query

The search bar at the top uses Elasticsearch's support for Lucene Query String syntax. Let's say we're searching web server logs that have been parsed into a few fields.

Examples:

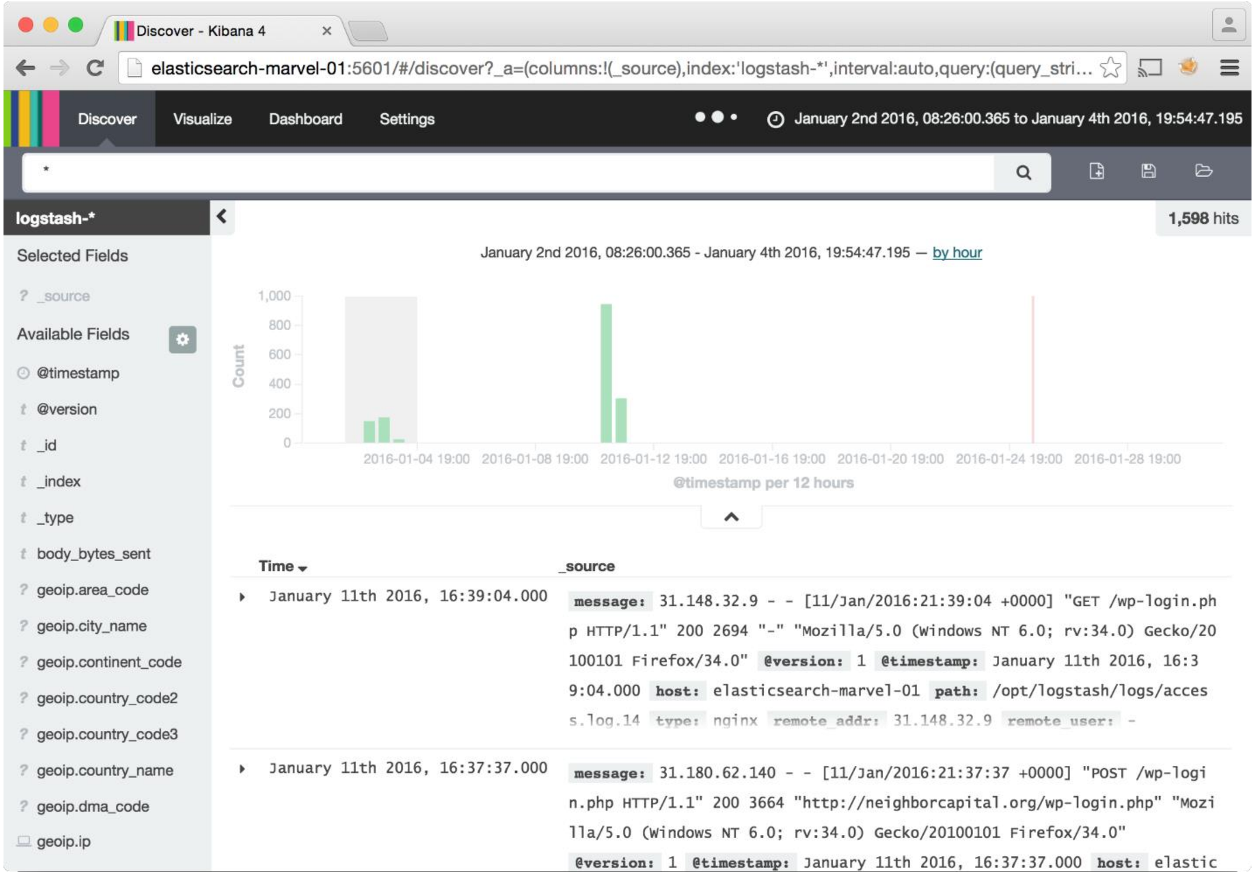
Find requests that contain the number 200, in any field:

```
200
```

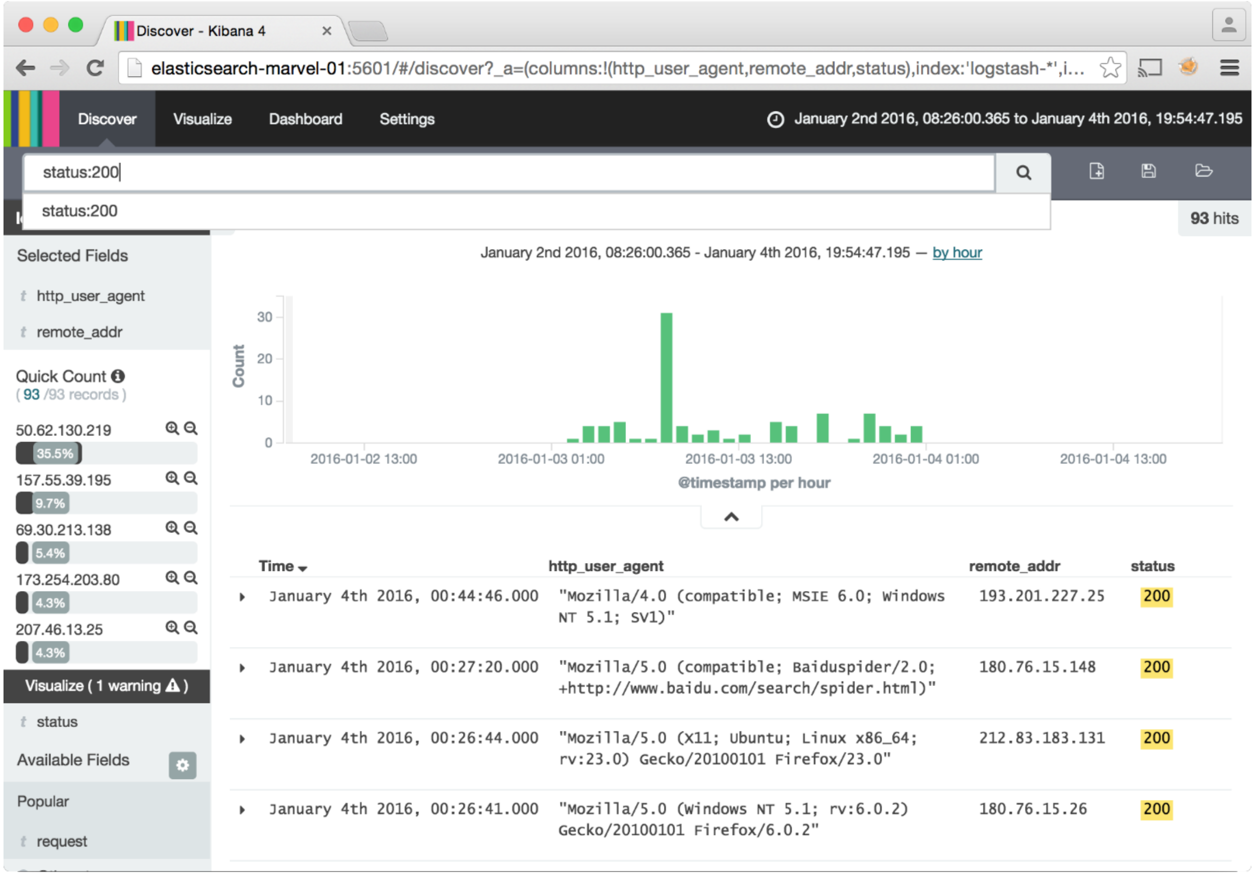
Or we can search in a specific field. Find 200 in the status field:

```
status:200
```

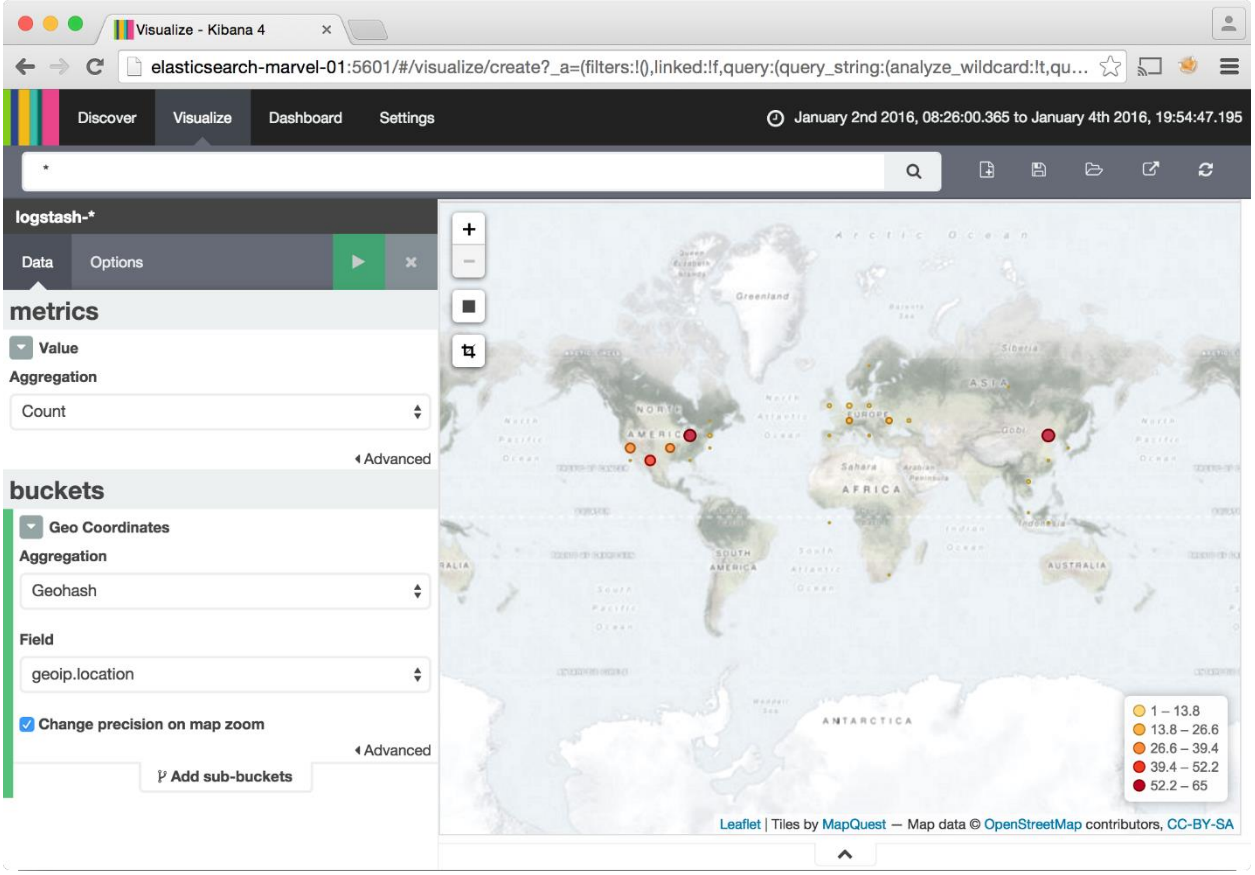
Find all status codes between 400-499:



```
January 11th 2016, 16:39:04.000   message: 31.148.32.9 - - [11/Jan/2016:21:39:04 +0000] "GET /wp-login.php HTTP/1.1" 200 2694 "-" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" @version: 1 @timestamp: January 11th 2016, 16:39:04.000 host: elasticsearch-marvel-01 path: /opt/logstash/logs/access.log.14 type: nginx remote_addr: 31.148.32.9 remote_user: -

January 11th 2016, 16:37:37.000   message: 31.180.62.140 - - [11/Jan/2016:21:37:37 +0000] "POST /wp-login.php HTTP/1.1" 200 3664 "http://neighborcapital.org/wp-login.php" "Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0" @version: 1 @timestamp: January 11th 2016, 16:37:37.000 host: elastic
```



Time	http_user_agent	remote_addr	status
January 4th 2016, 00:44:46.000	"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"	193.201.227.25	200
January 4th 2016, 00:27:20.000	"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"	180.76.15.148	200
January 4th 2016, 00:26:44.000	"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:23.0) Gecko/20100101 Firefox/23.0"	212.83.183.131	200
January 4th 2016, 00:26:41.000	"Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"	180.76.15.26	200



Visualize - Kibana 4

elasticsearch-marvel-01:5601/#/visualize/create?_a=(filters:!(),linked:!f,query:(query_string:(analyze_wildcard:!t,qu…

January 2nd 2016, 08:26:00.365 to January 4th 2016, 19:54:47.195

*

logstash-*

metrics

Value

Aggregation: Count

buckets

Geo Coordinates

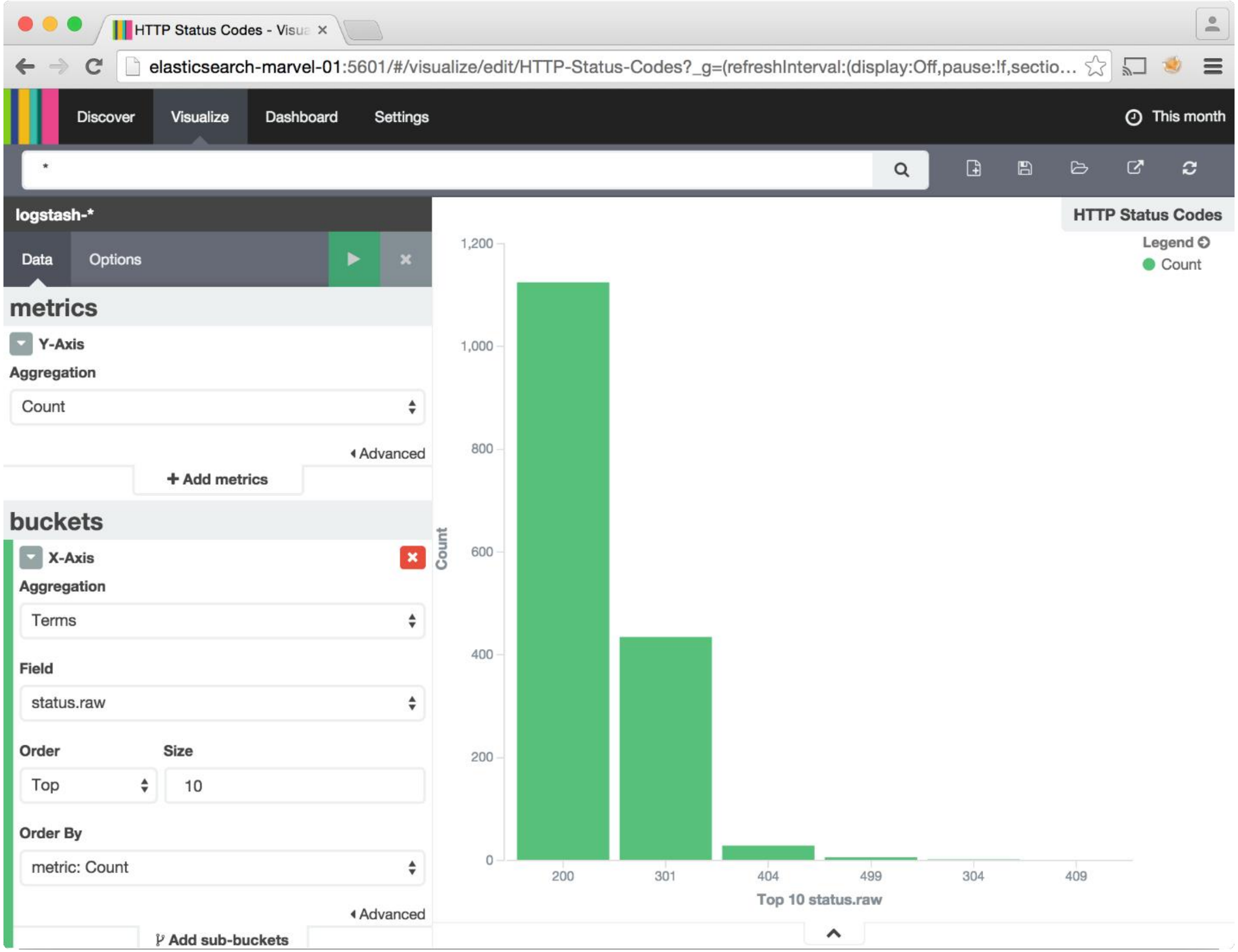
Aggregation: Geohash

Field: geoip.location

☑ Change precision on map zoom

● 1 – 13.8
● 13.8 – 26.6
● 26.6 – 39.4
● 39.4 – 52.2
● 52.2 – 65

Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA



elasticsearch-marvel-01:5601/#/visualize/edit/HTTP-Status-Codes?_g=(refreshInterval:(display:Off,pause:!f,sectio…

logstash-*

metrics

Y-Axis

Aggregation: Count

buckets

X-Axis

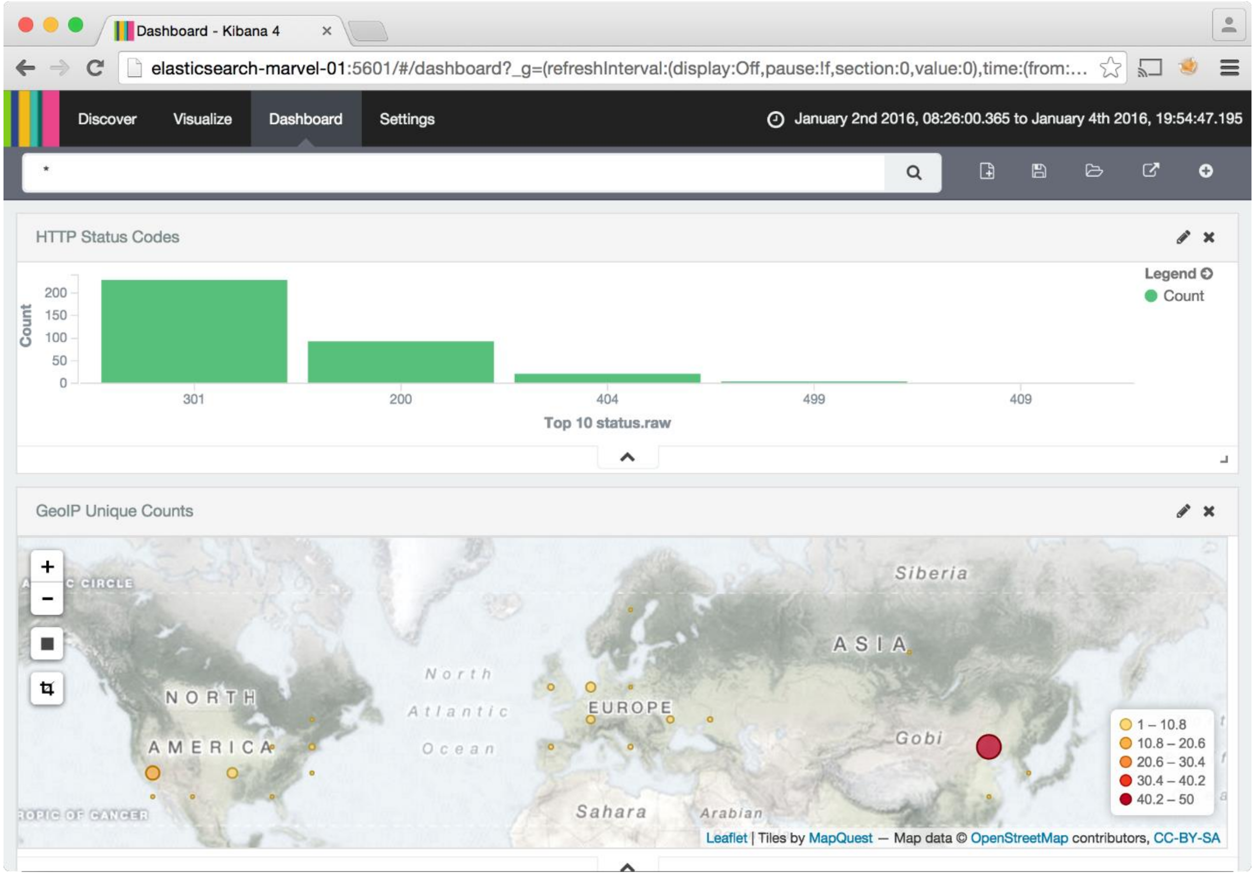
Aggregation: Terms

Field: status.raw

Order: Top

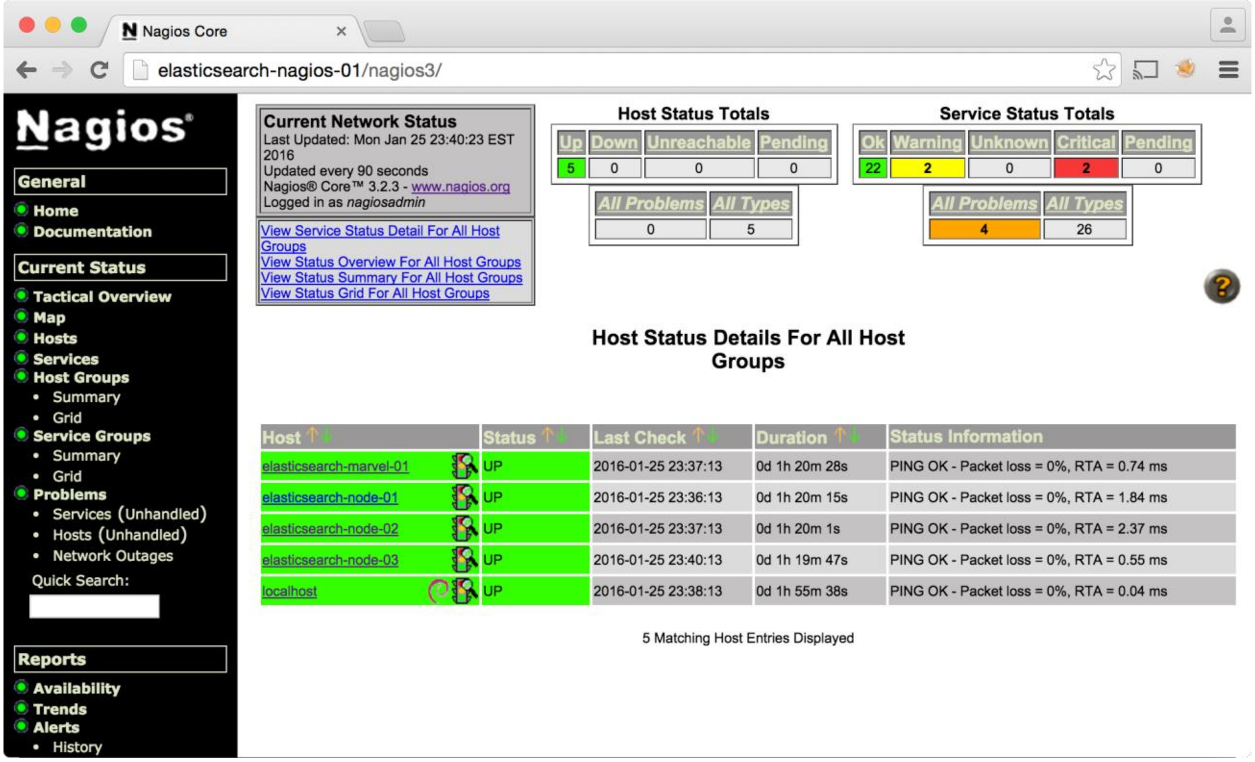
Size: 10

Order By: metric: Count



elasticsearch-marvel-01:5601/#/dashboard?_g=(refreshInterval:(display:Off,pause:!f,section:0,value:0),time:(from:…

January 2nd 2016, 08:26:00.365 to January 4th 2016, 19:54:47.195



elasticsearch-nagios-01/nagios3/

Current Network Status
Last Updated: Mon Jan 25 23:40:23 EST 2016
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as *nagiosadmin*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
5	0	0	0

All Problems	All Types
0	5

Service Status Totals

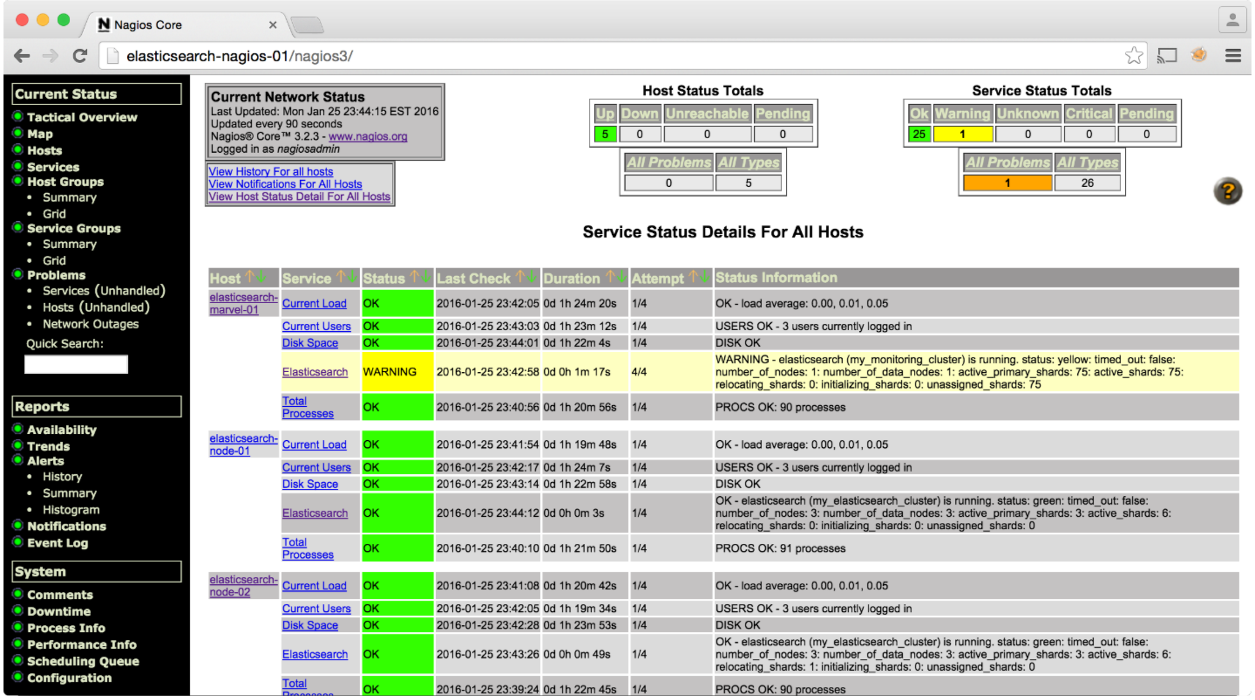
Ok	Warning	Unknown	Critical	Pending
22	2	0	2	0

All Problems	All Types
4	26

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
elasticsearch-marvel-01	UP	2016-01-25 23:37:13	0d 1h 20m 28s	PING OK - Packet loss = 0%, RTA = 0.74 ms
elasticsearch-node-01	UP	2016-01-25 23:36:13	0d 1h 20m 15s	PING OK - Packet loss = 0%, RTA = 1.84 ms
elasticsearch-node-02	UP	2016-01-25 23:37:13	0d 1h 20m 1s	PING OK - Packet loss = 0%, RTA = 2.37 ms
elasticsearch-node-03	UP	2016-01-25 23:40:13	0d 1h 19m 47s	PING OK - Packet loss = 0%, RTA = 0.55 ms
localhost	UP	2016-01-25 23:38:13	0d 1h 55m 38s	PING OK - Packet loss = 0%, RTA = 0.04 ms

5 Matching Host Entries Displayed



Current Network Status
Last Updated: Mon Jan 25 23:44:15 EST 2016
Updated every 90 seconds
Nagios® Core™ 3.2.3 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
5	0	0	0

All Problems	All Types
0	5

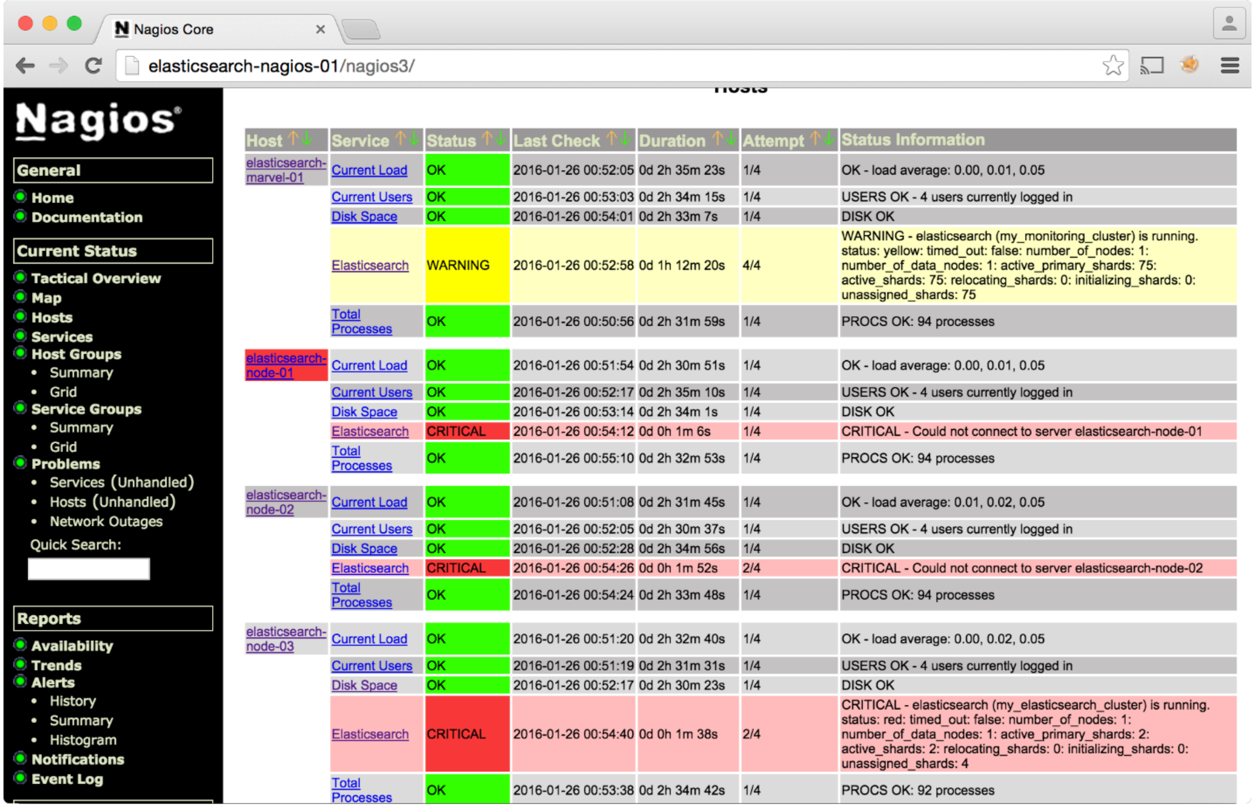
Service Status Totals

Ok	Warning	Unknown	Critical	Pending
25	1	0	0	0

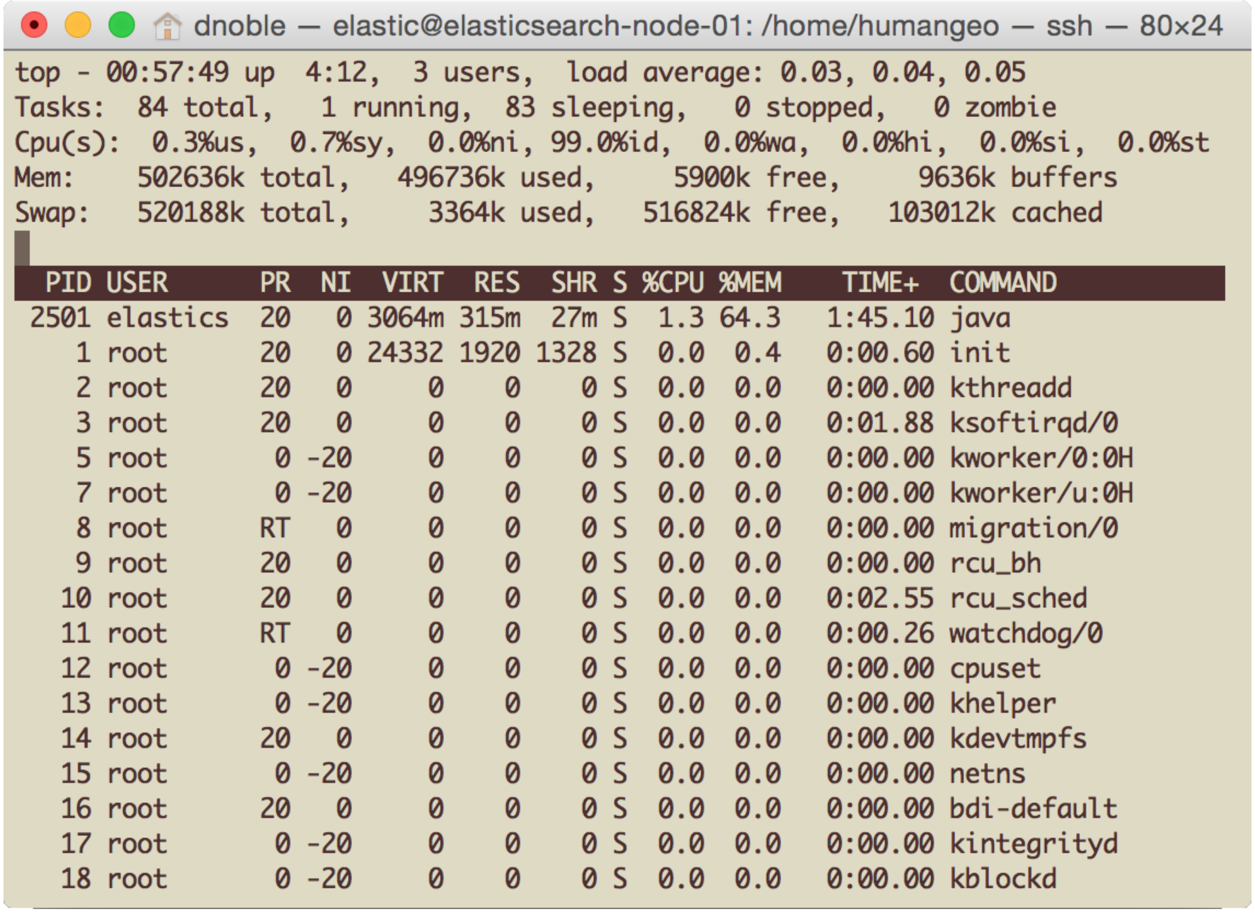
All Problems	All Types
1	26

Service Status Details For All Hosts

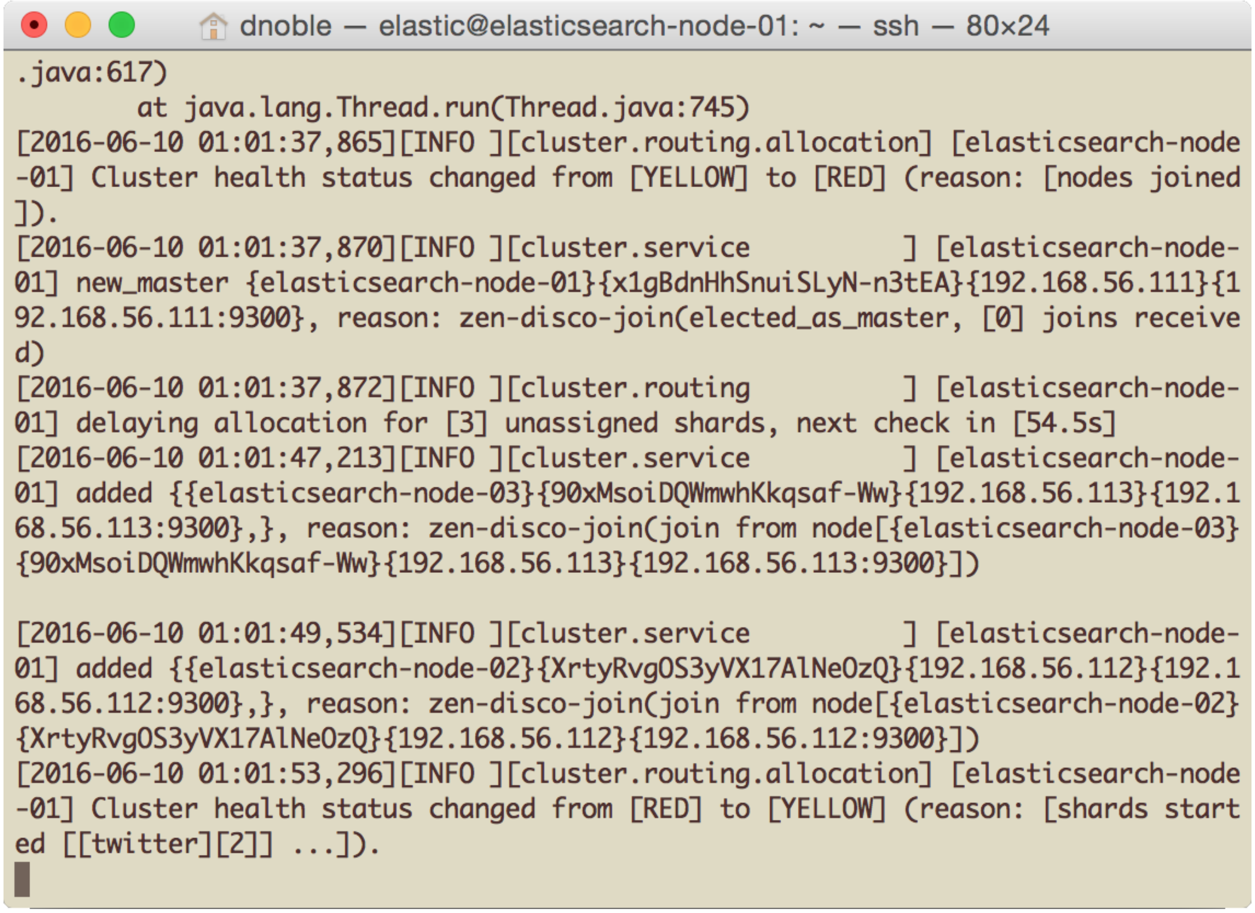
Host	Service	Status	Last Check	Duration	Attempt	Status Information
elasticsearch-marvel-01	Current Load	OK	2016-01-25 23:42:05	0d 1h 24m 20s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2016-01-25 23:43:03	0d 1h 23m 12s	1/4	USERS OK - 3 users currently logged in
	Disk Space	OK	2016-01-25 23:44:01	0d 1h 22m 4s	1/4	DISK OK
	Elasticsearch	WARNING	2016-01-25 23:42:58	0d 0h 1m 17s	4/4	WARNING - elasticsearch (my_monitoring_cluster) is running. status: yellow: timed_out: false: number_of_nodes: 1: number_of_data_nodes: 1: active_primary_shards: 75: active_shards: 75: relocating_shards: 0: initializing_shards: 0: unassigned_shards: 75
	Total Processes	OK	2016-01-25 23:40:56	0d 1h 20m 56s	1/4	PROCS OK: 90 processes
elasticsearch-node-01	Current Load	OK	2016-01-25 23:41:54	0d 1h 19m 48s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2016-01-25 23:42:17	0d 1h 24m 7s	1/4	USERS OK - 3 users currently logged in
	Disk Space	OK	2016-01-25 23:43:14	0d 1h 22m 58s	1/4	DISK OK
	Elasticsearch	OK	2016-01-25 23:44:12	0d 0h 0m 3s	1/4	OK - elasticsearch (my_elasticsearch_cluster) is running. status: green: timed_out: false: number_of_nodes: 3: number_of_data_nodes: 3: active_primary_shards: 3: active_shards: 6: relocating_shards: 0: initializing_shards: 0: unassigned_shards: 0
	Total Processes	OK	2016-01-25 23:40:10	0d 1h 21m 50s	1/4	PROCS OK: 91 processes
elasticsearch-node-02	Current Load	OK	2016-01-25 23:41:08	0d 1h 20m 42s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2016-01-25 23:42:05	0d 1h 19m 34s	1/4	USERS OK - 3 users currently logged in
	Disk Space	OK	2016-01-25 23:42:28	0d 1h 23m 53s	1/4	DISK OK
	Elasticsearch	OK	2016-01-25 23:43:26	0d 0h 0m 49s	1/4	OK - elasticsearch (my_elasticsearch_cluster) is running. status: green: timed_out: false: number_of_nodes: 3: number_of_data_nodes: 3: active_primary_shards: 3: active_shards: 6: relocating_shards: 1: initializing_shards: 0: unassigned_shards: 0
	Total Processes	OK	2016-01-25 23:39:24	0d 1h 22m 45s	1/4	PROCS OK: 90 processes



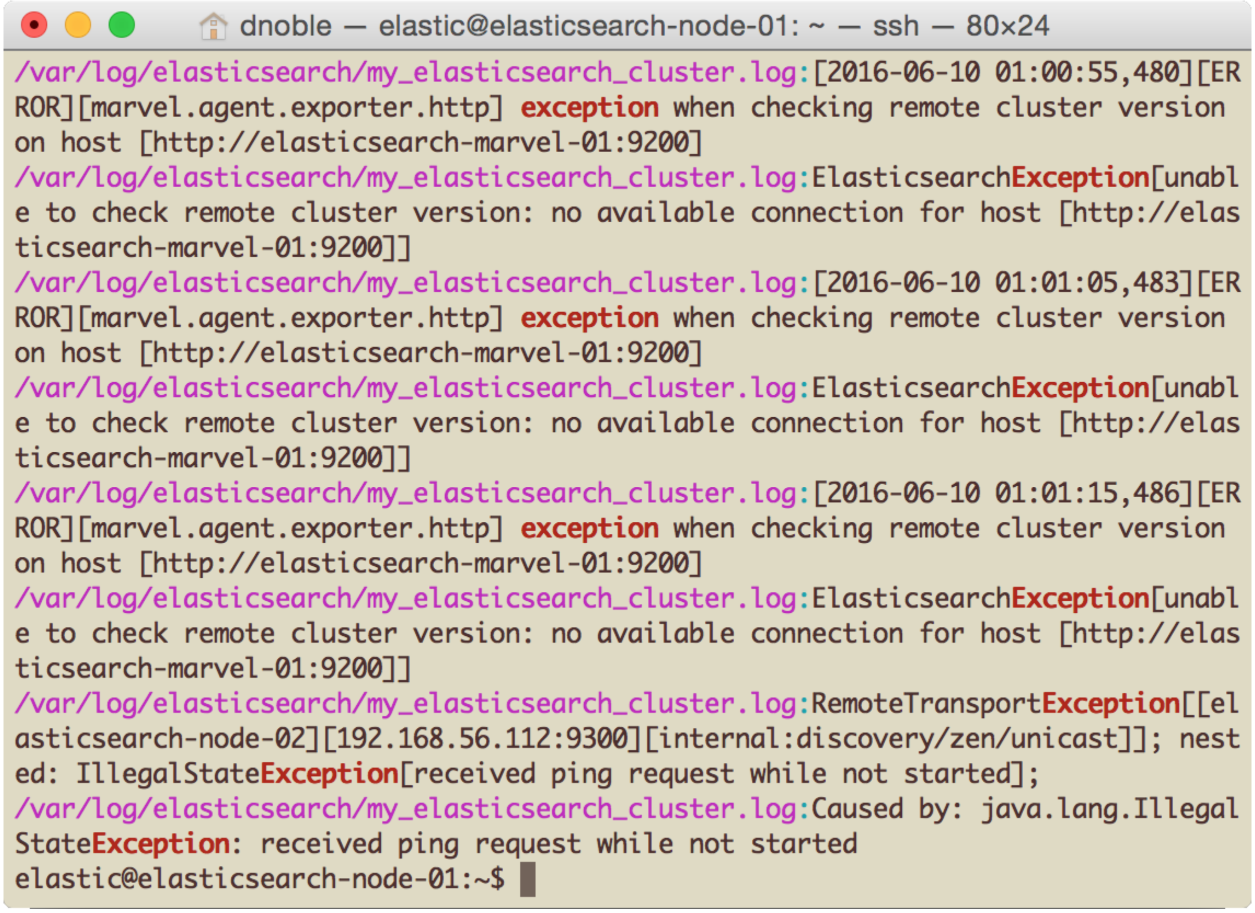
Host	Service	Status	Last Check	Duration	Attempt	Status Information
elasticsearch-marvel-01	Current Load	OK	2016-01-26 00:52:05	0d 2h 35m 23s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2016-01-26 00:53:03	0d 2h 34m 15s	1/4	USERS OK - 4 users currently logged in
	Disk Space	OK	2016-01-26 00:54:01	0d 2h 33m 7s	1/4	DISK OK
	Elasticsearch	WARNING	2016-01-26 00:52:58	0d 1h 12m 20s	4/4	WARNING - elasticsearch (my_monitoring_cluster) is running. status: yellow: timed_out: false: number_of_nodes: 1: number_of_data_nodes: 1: active_primary_shards: 75: active_shards: 75: relocating_shards: 0: initializing_shards: 0: unassigned_shards: 75
	Total Processes	OK	2016-01-26 00:50:56	0d 2h 31m 59s	1/4	PROCS OK: 94 processes
elasticsearch-node-01	Current Load	OK	2016-01-26 00:51:54	0d 2h 30m 51s	1/4	OK - load average: 0.00, 0.01, 0.05
	Current Users	OK	2016-01-26 00:52:17	0d 2h 35m 10s	1/4	USERS OK - 4 users currently logged in
	Disk Space	OK	2016-01-26 00:53:14	0d 2h 34m 1s	1/4	DISK OK
	Elasticsearch	CRITICAL	2016-01-26 00:54:12	0d 0h 1m 6s	1/4	CRITICAL - Could not connect to server elasticsearch-node-01
	Total Processes	OK	2016-01-26 00:55:10	0d 2h 32m 53s	1/4	PROCS OK: 94 processes
elasticsearch-node-02	Current Load	OK	2016-01-26 00:51:08	0d 2h 31m 45s	1/4	OK - load average: 0.01, 0.02, 0.05
	Current Users	OK	2016-01-26 00:52:05	0d 2h 30m 37s	1/4	USERS OK - 4 users currently logged in
	Disk Space	OK	2016-01-26 00:52:28	0d 2h 34m 56s	1/4	DISK OK
	Elasticsearch	CRITICAL	2016-01-26 00:54:26	0d 0h 1m 52s	2/4	CRITICAL - Could not connect to server elasticsearch-node-02
	Total Processes	OK	2016-01-26 00:54:24	0d 2h 33m 48s	1/4	PROCS OK: 94 processes
elasticsearch-node-03	Current Load	OK	2016-01-26 00:51:20	0d 2h 32m 40s	1/4	OK - load average: 0.00, 0.02, 0.05
	Current Users	OK	2016-01-26 00:51:19	0d 2h 31m 31s	1/4	USERS OK - 4 users currently logged in
	Disk Space	OK	2016-01-26 00:52:17	0d 2h 30m 23s	1/4	DISK OK
	Elasticsearch	CRITICAL	2016-01-26 00:54:40	0d 0h 1m 38s	2/4	CRITICAL - elasticsearch (my_elasticsearch_cluster) is running. status: red: timed_out: false: number_of_nodes: 1: number_of_data_nodes: 1: active_primary_shards: 2: active_shards: 2: relocating_shards: 0: initializing_shards: 0: unassigned_shards: 4
	Total Processes	OK	2016-01-26 00:53:38	0d 2h 34m 42s	1/4	PROCS OK: 92 processes


dnoble — elastic@elasticsearch-node-01: /home/humangeo — ssh — 80×24

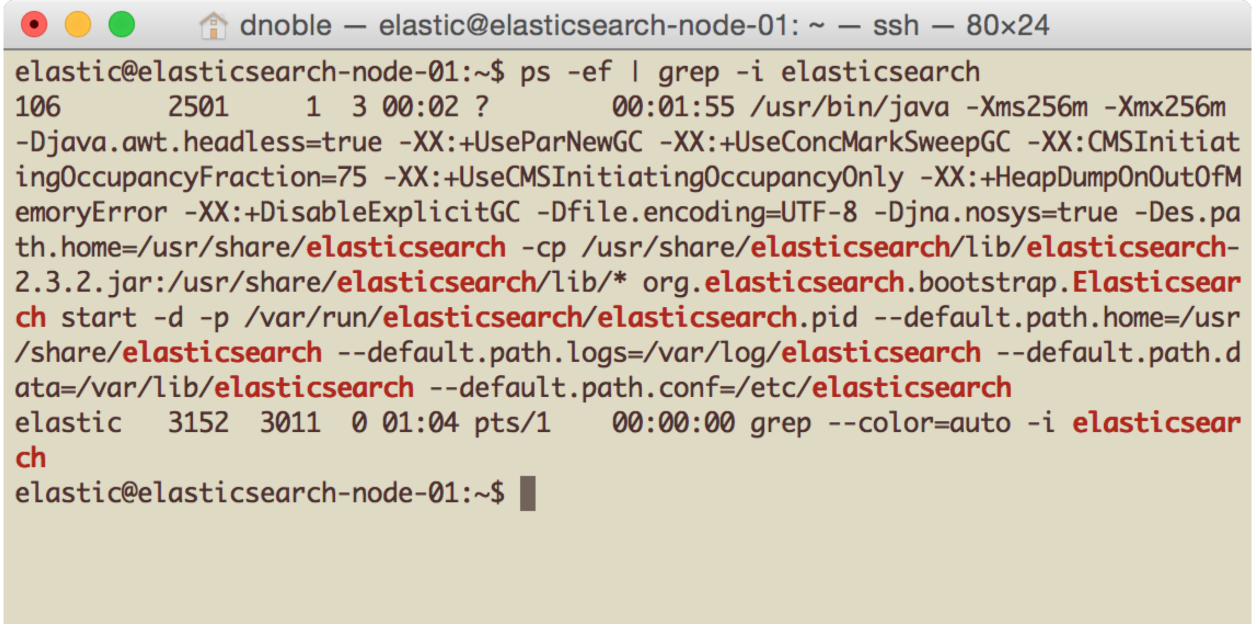
```
top - 00:57:49 up  4:12,  3 users,  load average: 0.03, 0.04, 0.05
Tasks:  84 total,   1 running,  83 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.3%us,  0.7%sy,  0.0%ni, 99.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:    502636k total,   496736k used,     5900k free,     9636k buffers
Swap:   520188k total,     3364k used,   516824k free,   103012k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2501 elastics  20   0 3064m 315m  27m S  1.3 64.3   1:45.10 java
    1 root      20   0 24332 1920 1328 S  0.0  0.4   0:00.60 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S  0.0  0.0   0:01.88 ksoftirqd/0
    5 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kworker/u:0H
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    9 root      20   0     0    0    0 S  0.0  0.0   0:00.00 rcu_bh
   10 root      20   0     0    0    0 S  0.0  0.0   0:02.55 rcu_sched
   11 root      RT   0     0    0    0 S  0.0  0.0   0:00.26 watchdog/0
   12 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 cpuset
   13 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 khelper
   14 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kdevtmpfs
   15 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 netns
   16 root      20   0     0    0    0 S  0.0  0.0   0:00.00 bdi-default
   17 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kintegrityd
   18 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kblockd
```



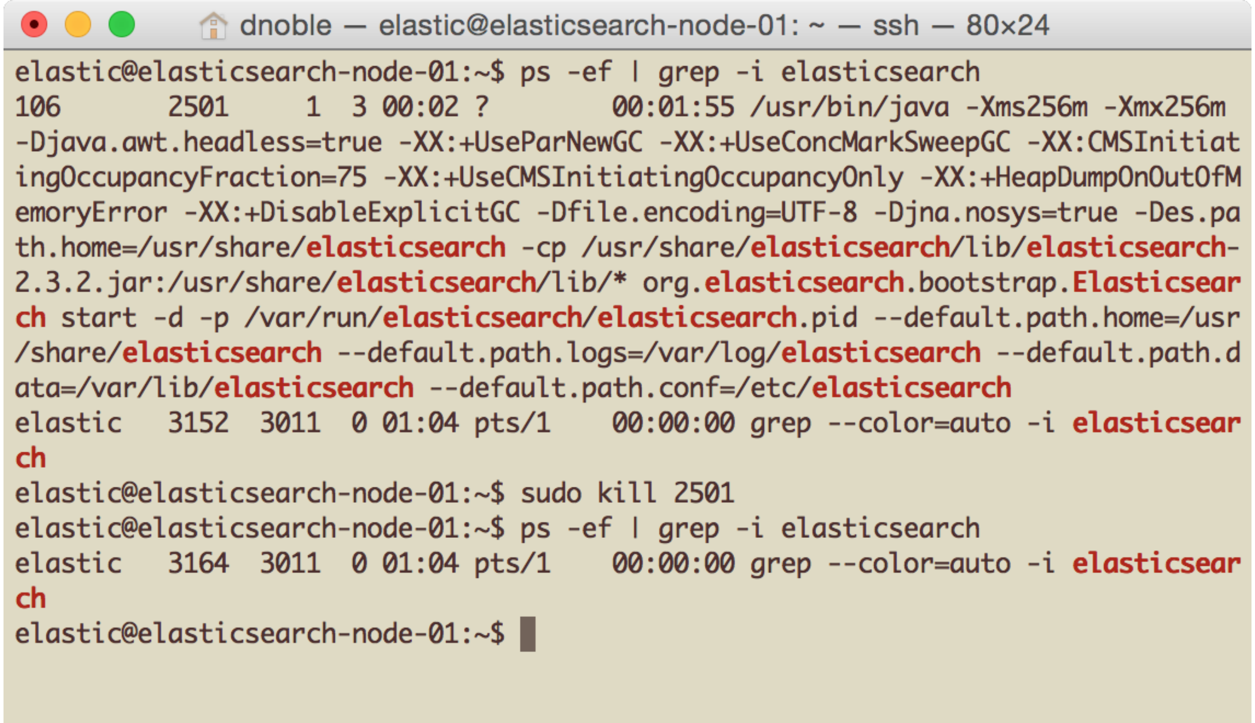
```
.java:617)
        at java.lang.Thread.run(Thread.java:745)
[2016-06-10 01:01:37,865][INFO ][cluster.routing.allocation] [elasticsearch-node
-01] Cluster health status changed from [YELLOW] to [RED] (reason: [nodes joined
]).
[2016-06-10 01:01:37,870][INFO ][cluster.service          ] [elasticsearch-node-
01] new_master {elasticsearch-node-01}{x1gBdnHhSnuiSLyN-n3tEA}{192.168.56.111}{1
92.168.56.111:9300}, reason: zen-disco-join(elected_as_master, [0] joins receive
d)
[2016-06-10 01:01:37,872][INFO ][cluster.routing          ] [elasticsearch-node-
01] delaying allocation for [3] unassigned shards, next check in [54.5s]
[2016-06-10 01:01:47,213][INFO ][cluster.service          ] [elasticsearch-node-
01] added {{elasticsearch-node-03}{90xMsoiDQWmwhKkqsaf-Ww}{192.168.56.113}{192.1
68.56.113:9300},}, reason: zen-disco-join(join from node[{elasticsearch-node-03}
{90xMsoiDQWmwhKkqsaf-Ww}{192.168.56.113}{192.168.56.113:9300}])

[2016-06-10 01:01:49,534][INFO ][cluster.service          ] [elasticsearch-node-
01] added {{elasticsearch-node-02}{XrtyRvgOS3yVX17AlNeOzQ}{192.168.56.112}{192.1
68.56.112:9300},}, reason: zen-disco-join(join from node[{elasticsearch-node-02}
{XrtyRvgOS3yVX17AlNeOzQ}{192.168.56.112}{192.168.56.112:9300}])
[2016-06-10 01:01:53,296][INFO ][cluster.routing.allocation] [elasticsearch-node
-01] Cluster health status changed from [RED] to [YELLOW] (reason: [shards start
ed [[twitter][2]] ...]).
```



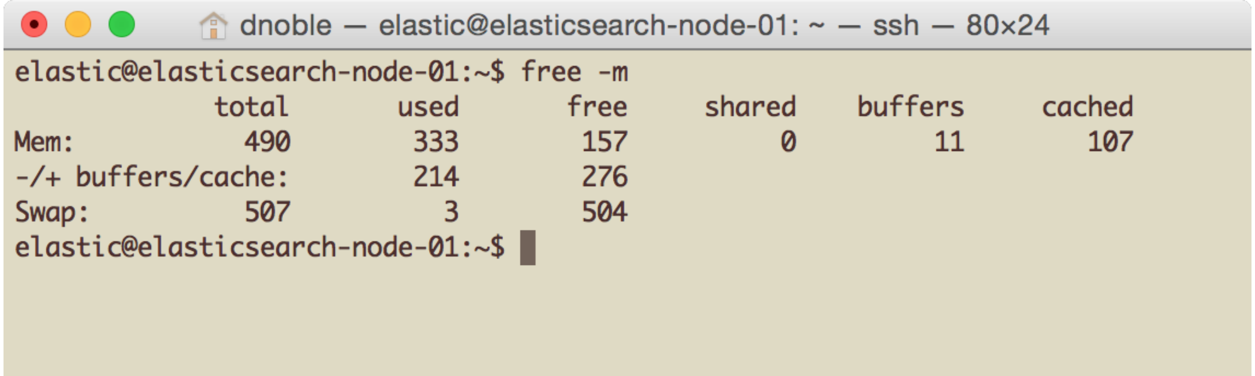
```
/var/log/elasticsearch/my_elasticsearch_cluster.log:[2016-06-10 01:00:55,480][ER
ROR][marvel.agent.exporter.http] exception when checking remote cluster version
on host [http://elasticsearch-marvel-01:9200]
/var/log/elasticsearch/my_elasticsearch_cluster.log:ElasticsearchException[unabl
e to check remote cluster version: no available connection for host [http://elas
ticsearch-marvel-01:9200]]
/var/log/elasticsearch/my_elasticsearch_cluster.log:[2016-06-10 01:01:05,483][ER
ROR][marvel.agent.exporter.http] exception when checking remote cluster version
on host [http://elasticsearch-marvel-01:9200]
/var/log/elasticsearch/my_elasticsearch_cluster.log:ElasticsearchException[unabl
e to check remote cluster version: no available connection for host [http://elas
ticsearch-marvel-01:9200]]
/var/log/elasticsearch/my_elasticsearch_cluster.log:[2016-06-10 01:01:15,486][ER
ROR][marvel.agent.exporter.http] exception when checking remote cluster version
on host [http://elasticsearch-marvel-01:9200]
/var/log/elasticsearch/my_elasticsearch_cluster.log:ElasticsearchException[unabl
e to check remote cluster version: no available connection for host [http://elas
ticsearch-marvel-01:9200]]
/var/log/elasticsearch/my_elasticsearch_cluster.log:RemoteTransportException[[el
asticsearch-node-02][192.168.56.112:9300][internal:discovery/zen/unicast]]; nest
ed: IllegalStateException[received ping request while not started];
/var/log/elasticsearch/my_elasticsearch_cluster.log:Caused by: java.lang.Illegal
StateException: received ping request while not started
elastic@elasticsearch-node-01:~$ 
```



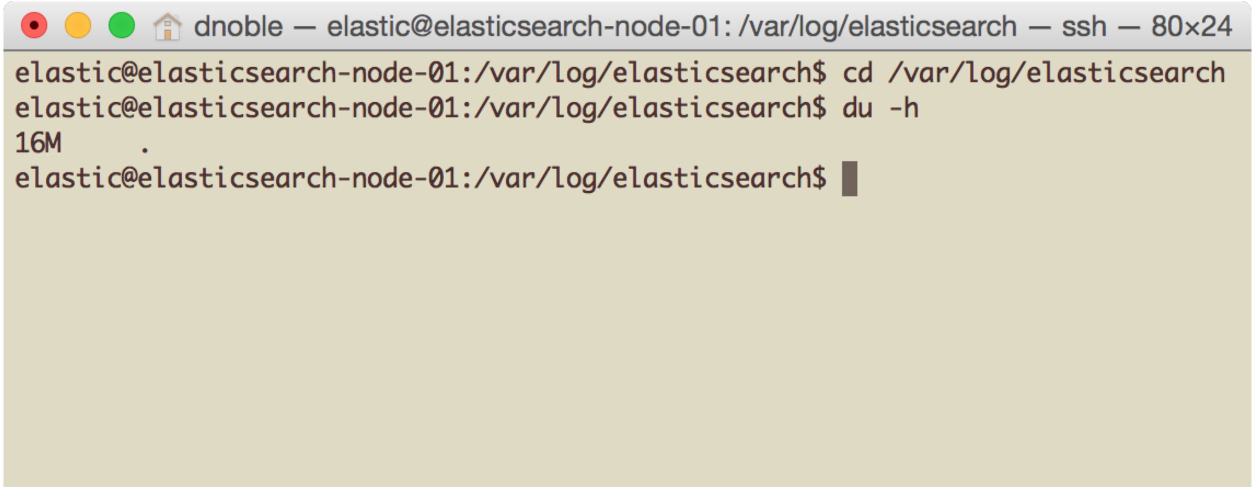
```
elastic@elasticsearch-node-01:~$ ps -ef | grep -i elasticsearch
106       2501     1  3 00:02 ?        00:01:55 /usr/bin/java -Xms256m -Xmx256m
-Djava.awt.headless=true -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CMSInitiat
ingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -XX:+HeapDumpOnOutOfM
emoryError -XX:+DisableExplicitGC -Dfile.encoding=UTF-8 -Djna.nosys=true -Des.pa
th.home=/usr/share/elasticsearch -cp /usr/share/elasticsearch/lib/elasticsearch-
2.3.2.jar:/usr/share/elasticsearch/lib/* org.elasticsearch.bootstrap.Elasticsear
ch start -d -p /var/run/elasticsearch/elasticsearch.pid --default.path.home=/usr
/share/elasticsearch --default.path.logs=/var/log/elasticsearch --default.path.d
ata=/var/lib/elasticsearch --default.path.conf=/etc/elasticsearch
elastic   3152  3011  0 01:04 pts/1    00:00:00 grep --color=auto -i elasticsear
ch
elastic@elasticsearch-node-01:~$ 
```



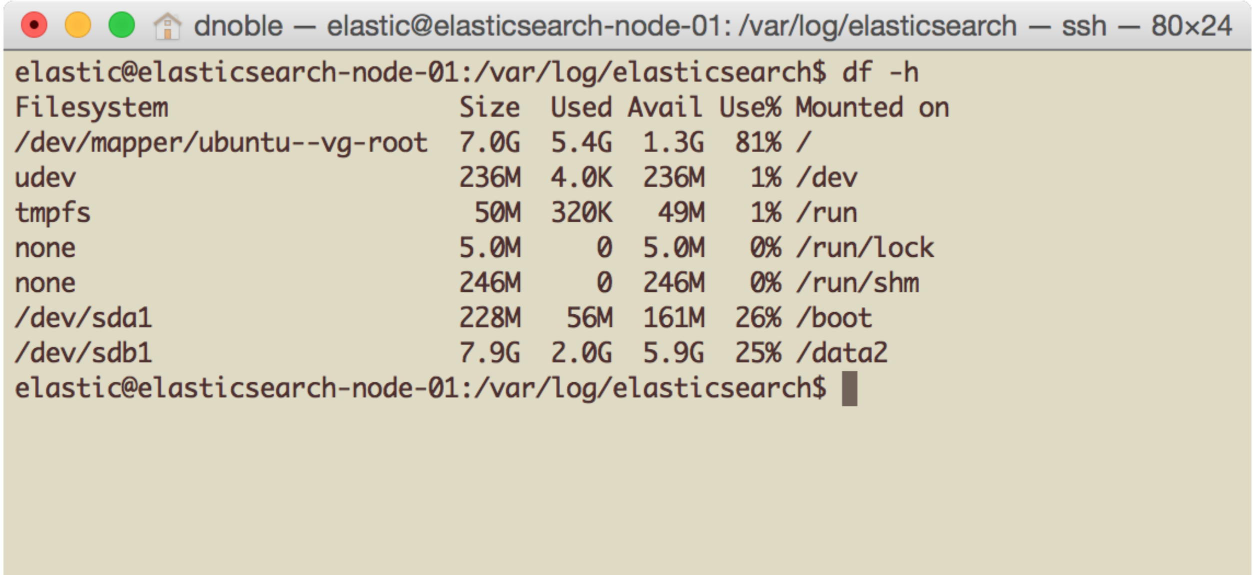
```
elastic@elasticsearch-node-01:~$ ps -ef | grep -i elasticsearch
106       2501     1  3 00:02 ?        00:01:55 /usr/bin/java -Xms256m -Xmx256m
-Djava.awt.headless=true -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CMSInitiat
ingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -XX:+HeapDumpOnOutOfM
emoryError -XX:+DisableExplicitGC -Dfile.encoding=UTF-8 -Djna.nosys=true -Des.pa
th.home=/usr/share/elasticsearch -cp /usr/share/elasticsearch/lib/elasticsearch-
2.3.2.jar:/usr/share/elasticsearch/lib/* org.elasticsearch.bootstrap.Elasticsear
ch start -d -p /var/run/elasticsearch/elasticsearch.pid --default.path.home=/usr
/share/elasticsearch --default.path.logs=/var/log/elasticsearch --default.path.d
ata=/var/lib/elasticsearch --default.path.conf=/etc/elasticsearch
elastic   3152  3011  0 01:04 pts/1    00:00:00 grep --color=auto -i elasticsear
ch
elastic@elasticsearch-node-01:~$ sudo kill 2501
elastic@elasticsearch-node-01:~$ ps -ef | grep -i elasticsearch
elastic   3164  3011  0 01:04 pts/1    00:00:00 grep --color=auto -i elasticsear
ch
elastic@elasticsearch-node-01:~$ 
```



```
elastic@elasticsearch-node-01:~$ free -m
             total       used       free     shared    buffers     cached
Mem:           490        333        157          0         11        107
-/+ buffers/cache:        214        276
Swap:          507          3        504
elastic@elasticsearch-node-01:~$ 
```

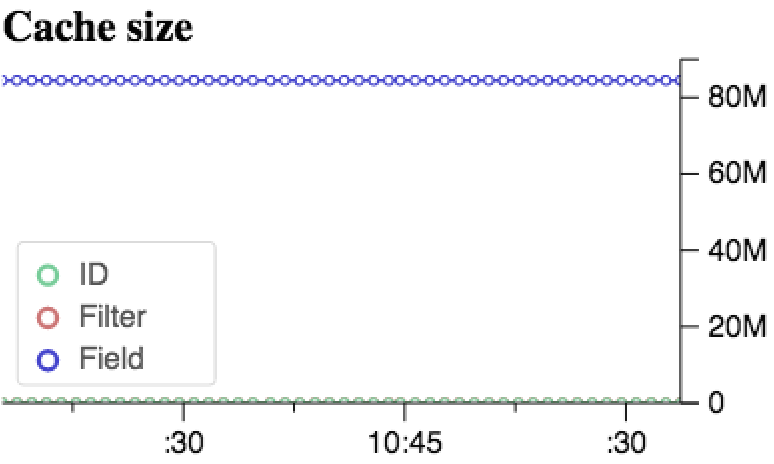

dnoble — elastic@elasticsearch-node-01: /var/log/elasticsearch — ssh — 80×24

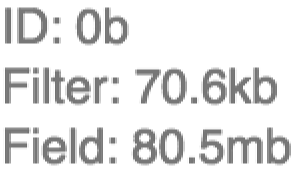
```
elastic@elasticsearch-node-01:/var/log/elasticsearch$ cd /var/log/elasticsearch
elastic@elasticsearch-node-01:/var/log/elasticsearch$ du -h
16M     .
elastic@elasticsearch-node-01:/var/log/elasticsearch$ 
```

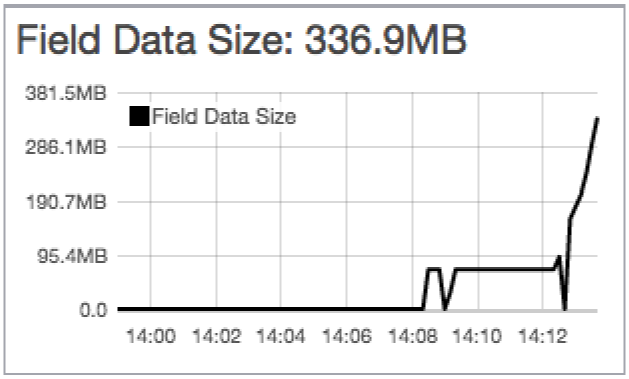

dnoble — elastic@elasticsearch-node-01: /var/log/elasticsearch — ssh — 80×24

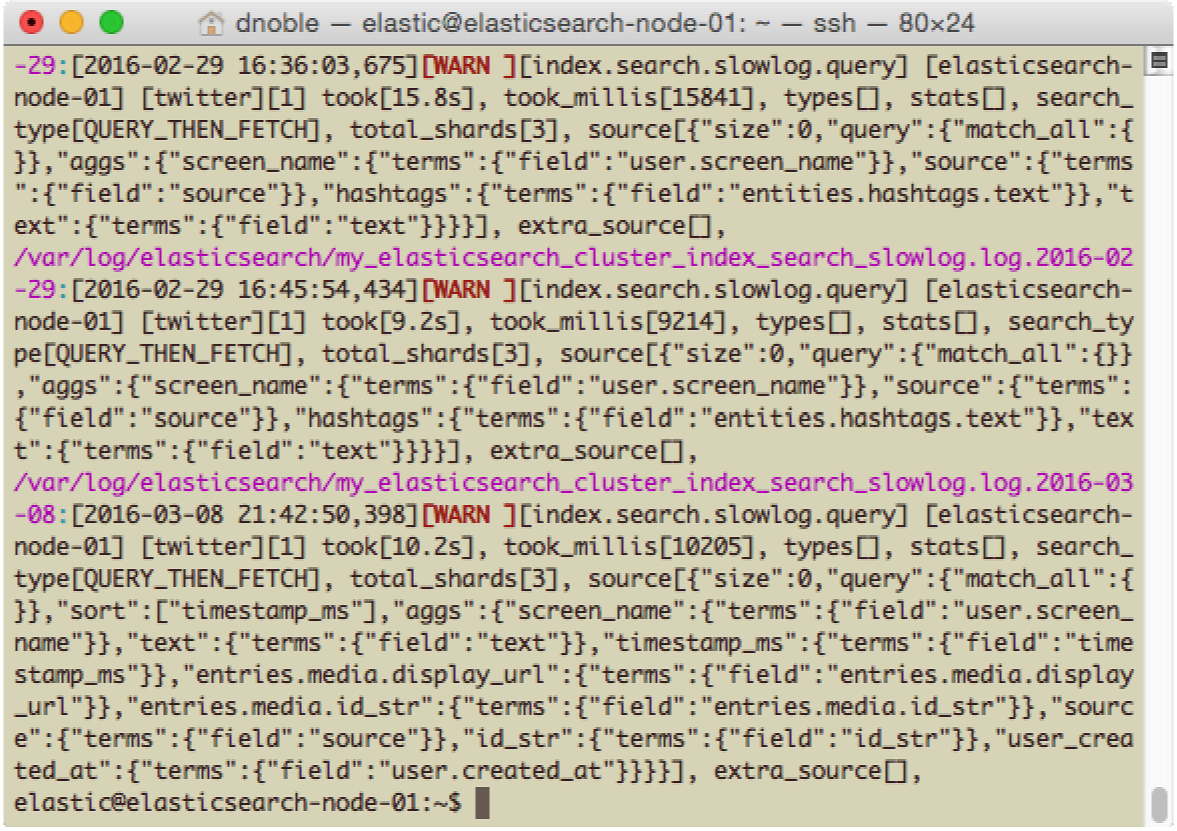
```
elastic@elasticsearch-node-01:/var/log/elasticsearch$ df -h
Filesystem                  Size  Used Avail Use% Mounted on
/dev/mapper/ubuntu--vg-root 7.0G  5.4G  1.3G  81% /
udev                        236M  4.0K  236M   1% /dev
tmpfs                        50M  320K   49M   1% /run
none                        5.0M     0  5.0M   0% /run/lock
none                        246M     0  246M   0% /run/shm
/dev/sda1                   228M   56M  161M  26% /boot
/dev/sdb1                   7.9G  2.0G  5.9G  25% /data2
elastic@elasticsearch-node-01:/var/log/elasticsearch$ 
```

Chapter 6: Troubleshooting and Performance Reliability Issues

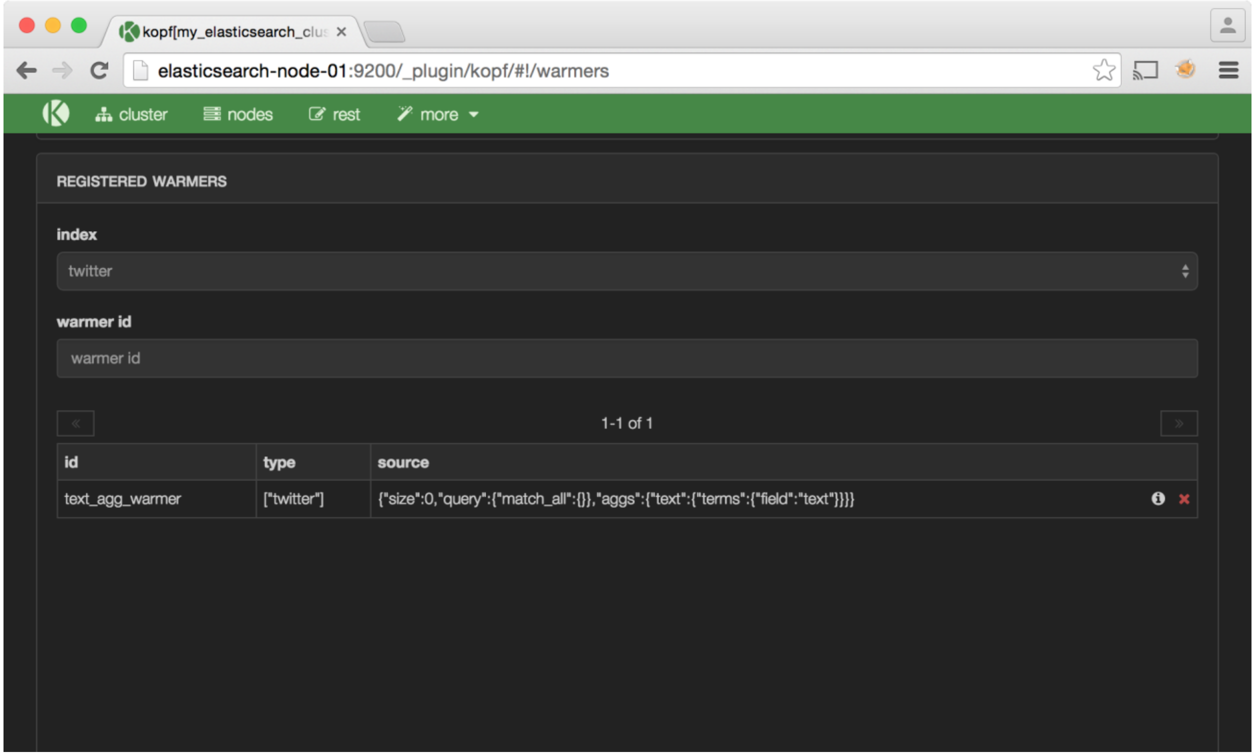



ID: 0b
Filter: 70.6kb
Field: 80.5mb





```
-29:[2016-02-29 16:36:03,675][WARN ][index.search.slowlog.query] [elasticsearch-
node-01] [twitter][1] took[15.8s], took_millis[15841], types[], stats[], search_
type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{
}},"aggs":{"screen_name":{"terms":{"field":"user.screen_name"}},"source":{"terms
":{"field":"source"}},"hashtags":{"terms":{"field":"entities.hashtags.text"}},"t
ext":{"terms":{"field":"text"}}}}], extra_source[],
/var/log/elasticsearch/my_elasticsearch_cluster_index_search_slowlog.log.2016-02
-29:[2016-02-29 16:45:54,434][WARN ][index.search.slowlog.query] [elasticsearch-
node-01] [twitter][1] took[9.2s], took_millis[9214], types[], stats[], search_ty
pe[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{}}
,"aggs":{"screen_name":{"terms":{"field":"user.screen_name"}},"source":{"terms":
{"field":"source"}},"hashtags":{"terms":{"field":"entities.hashtags.text"}},"tex
t":{"terms":{"field":"text"}}}}], extra_source[],
/var/log/elasticsearch/my_elasticsearch_cluster_index_search_slowlog.log.2016-03
-08:[2016-03-08 21:42:50,398][WARN ][index.search.slowlog.query] [elasticsearch-
node-01] [twitter][1] took[10.2s], took_millis[10205], types[], stats[], search_
type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{
}},"sort":["timestamp_ms"],"aggs":{"screen_name":{"terms":{"field":"user.screen_
name"}},"text":{"terms":{"field":"text"}},"timestamp_ms":{"terms":{"field":"time
stamp_ms"}},"entries.media.display_url":{"terms":{"field":"entries.media.display
_url"}},"entries.media.id_str":{"terms":{"field":"entries.media.id_str"}},"sourc
e":{"terms":{"field":"source"}},"id_str":{"terms":{"field":"id_str"}},"user_crea
ted_at":{"terms":{"field":"user.created_at"}}}}], extra_source[],
elastic@elasticsearch-node-01:~$
```


kopf[my_elasticsearch_clu
elasticsearch-node-01:9200/_plugin/kopf/#!/warmers
cluster
nodes
rest
more

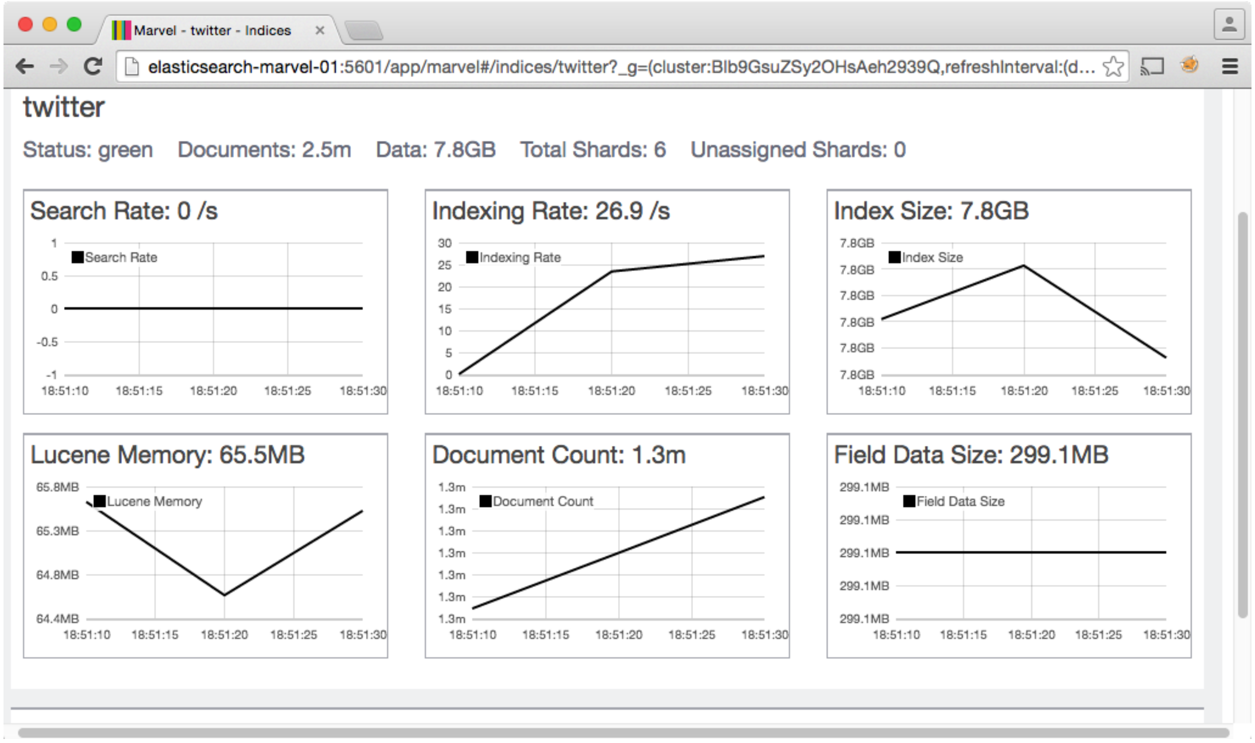
REGISTERED WARMERS

index: twitter

warmer id: warmer id

1-1 of 1

id	type	source
text_agg_warmer	["twitter"]	{"size":0,"query":{"match_all":{}},"aggs":{"text":{"terms":{"field":"text"}}}}



Marvel - twitter - Indices
elasticsearch-marvel-01:5601/app/marvel#/indices/twitter?_g=(cluster:Blb9GsuZSy2OHsAeh2939Q,refreshInterval:(d…

twitter

Status: green Documents: 2.5m Data: 7.8GB Total Shards: 6 Unassigned Shards: 0

Search Rate: 0 /s

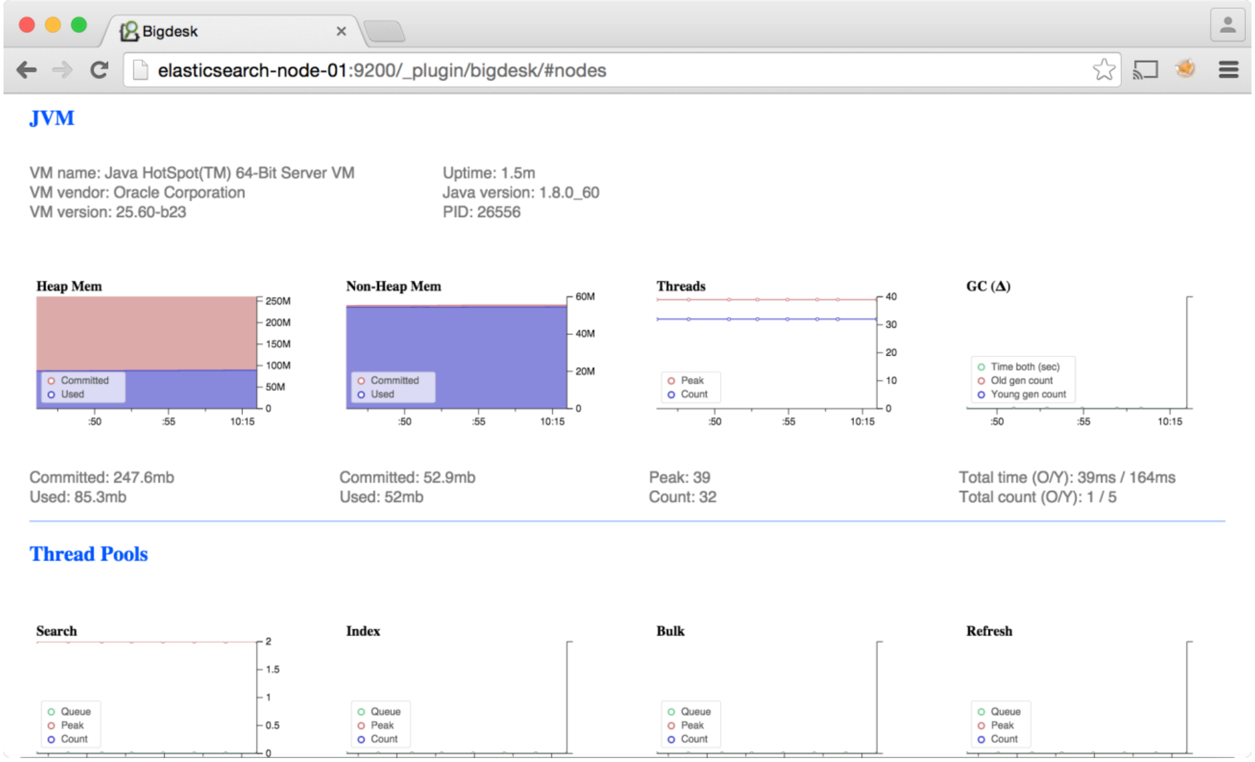
Indexing Rate: 26.9 /s

Index Size: 7.8GB

Lucene Memory: 65.5MB

Document Count: 1.3m

Field Data Size: 299.1MB



JVM

VM name: Java HotSpot(TM) 64-Bit Server VM
VM vendor: Oracle Corporation
VM version: 25.60-b23

Uptime: 1.5m
Java version: 1.8.0_60
PID: 26556

Committed: 247.6mb
Used: 85.3mb

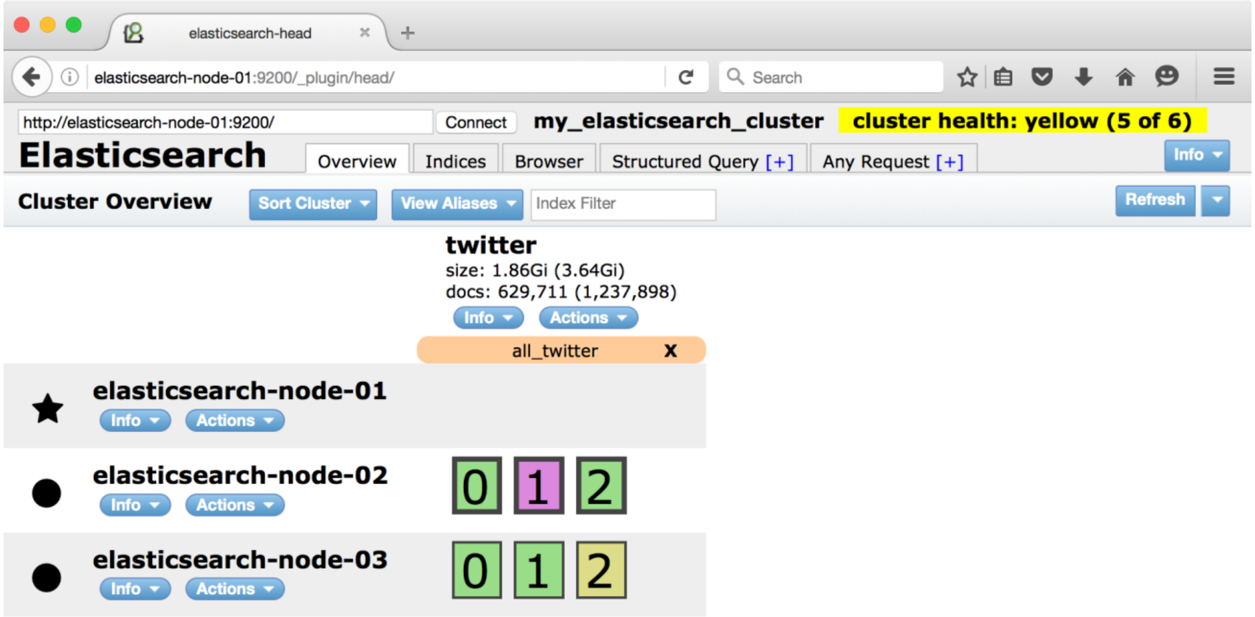
Committed: 52.9mb
Used: 52mb

Peak: 39
Count: 32

Total time (O/Y): 39ms / 164ms
Total count (O/Y): 1 / 5

Thread Pools

Chapter 7: Node Failure and Port-Mortem Analysis



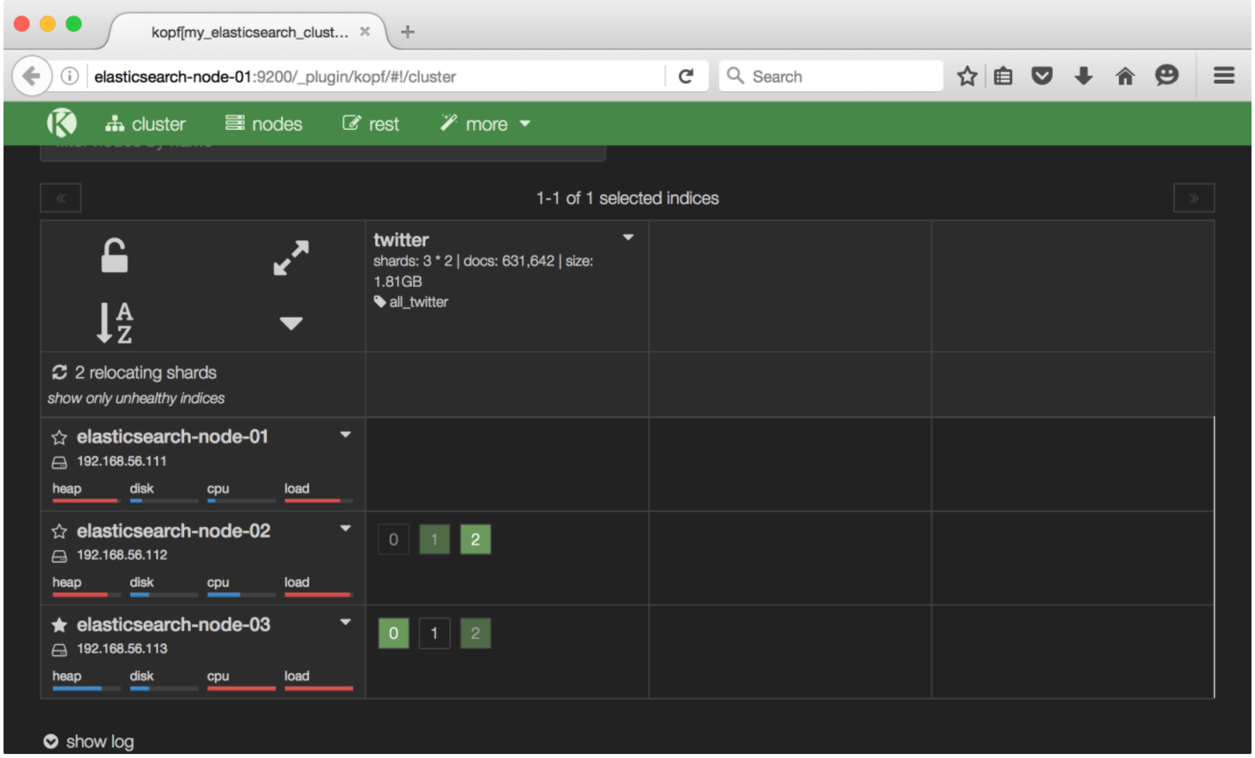
elasticsearch-node-01:9200/_plugin/head/

http://elasticsearch-node-01:9200/

my_elasticsearch_cluster

cluster health: yellow (5 of 6)

twitter
size: 1.86Gi (3.64Gi)
docs: 629,711 (1,237,898)

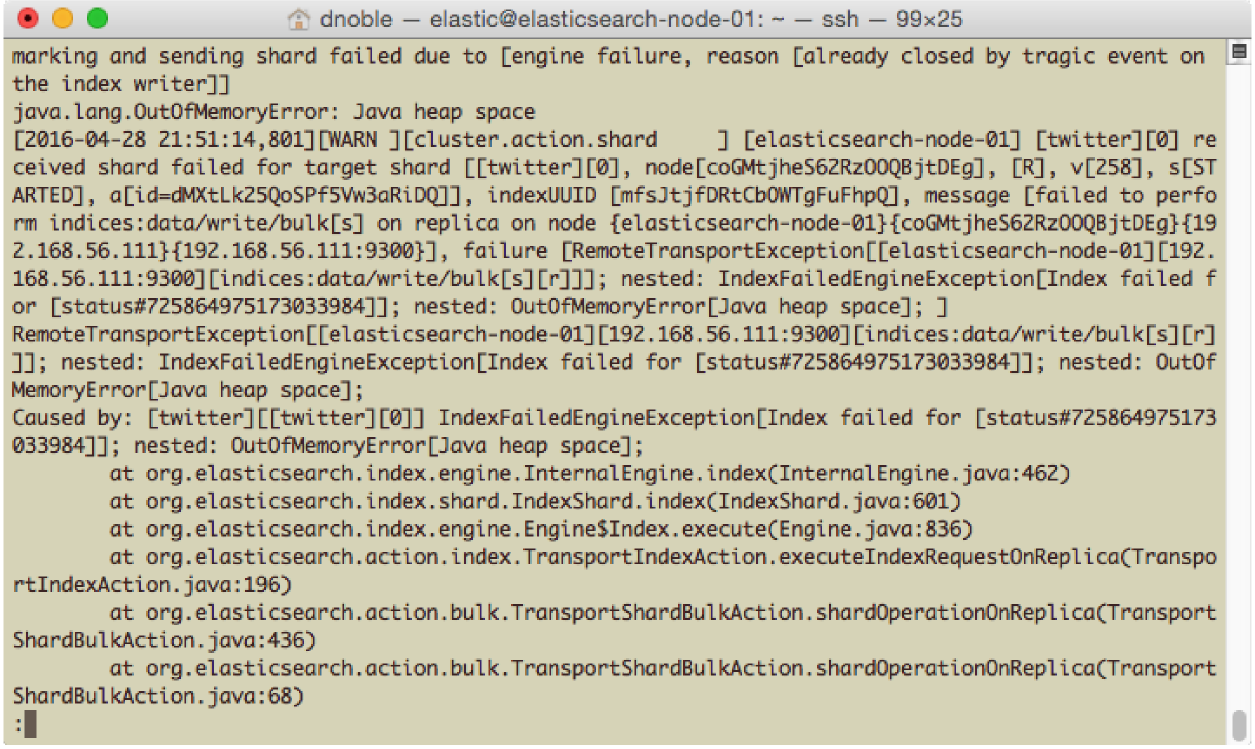

kopf[my_elasticsearch_clust...
elasticsearch-node-01:9200/_plugin/kopf/#!/cluster
Search
cluster
nodes
rest
more
show log

1-1 of 1 selected indices

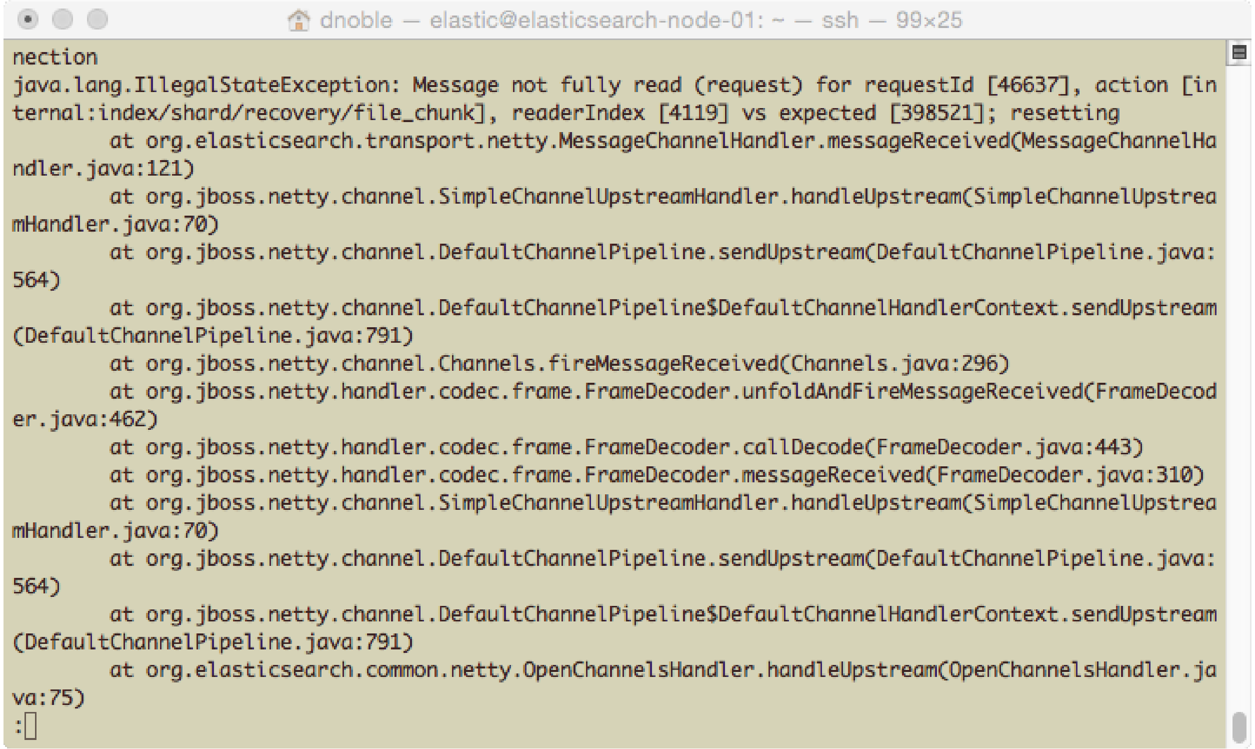
twitter
shards: 3 * 2 | docs: 631,642 | size: 1.81GB
all_twitter

2 relocating shards
show only unhealthy indices

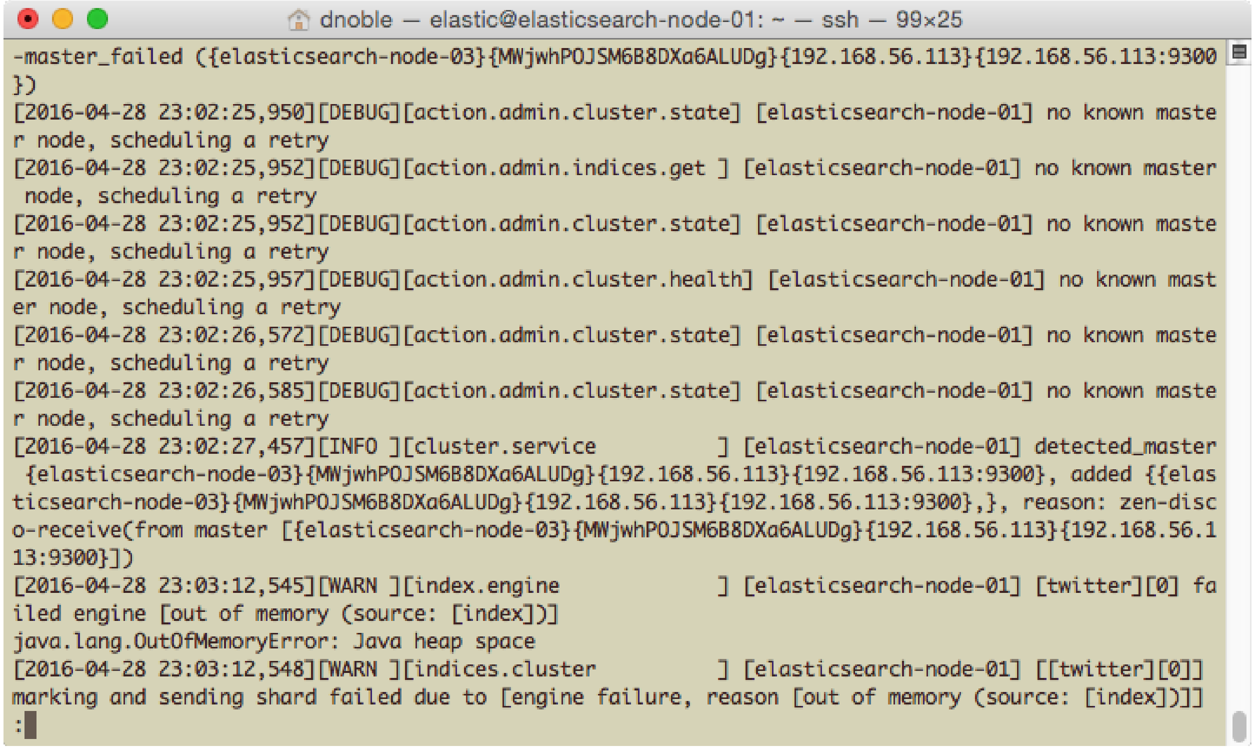
	twitter
elasticsearch-node-01 192.168.56.111 heap disk cpu load	
elasticsearch-node-02 192.168.56.112 heap disk cpu load	0 1 2
elasticsearch-node-03 192.168.56.113 heap disk cpu load	0 1 2



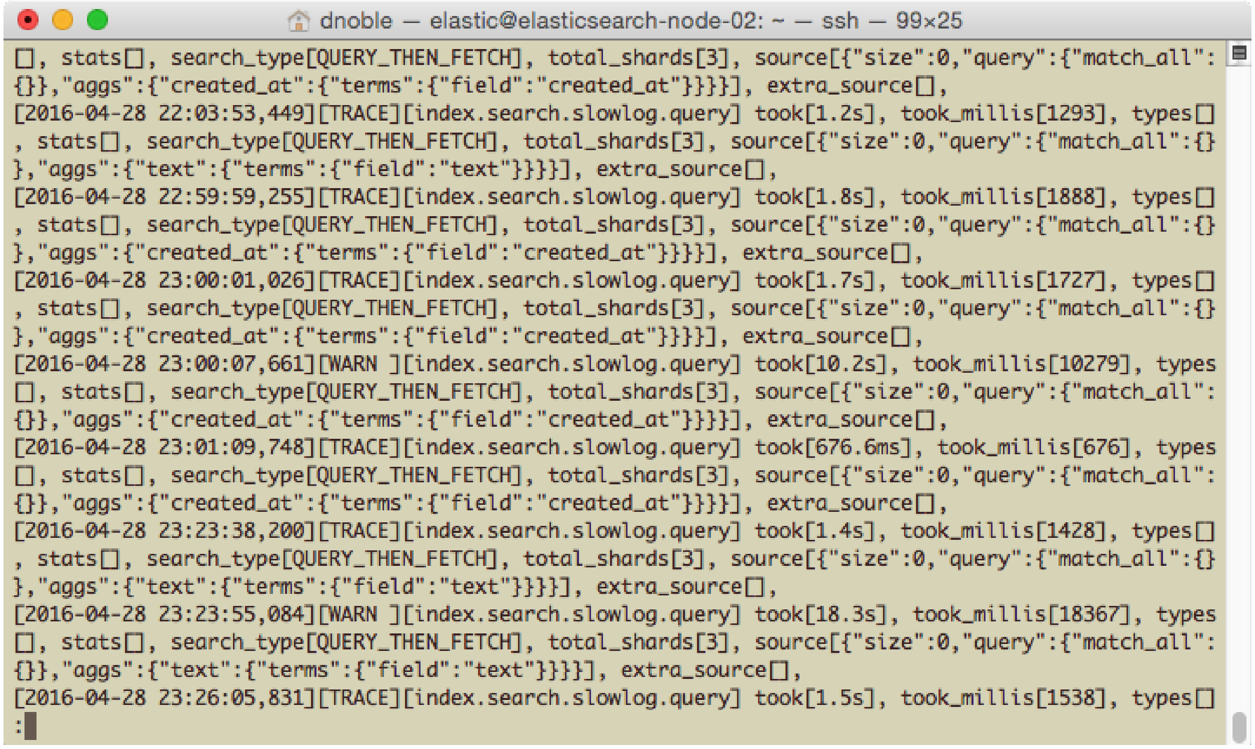
```
marking and sending shard failed due to [engine failure, reason [already closed by tragic event on
the index writer]]
java.lang.OutOfMemoryError: Java heap space
[2016-04-28 21:51:14,801][WARN ][cluster.action.shard     ] [elasticsearch-node-01] [twitter][0] re
ceived shard failed for target shard [[twitter][0], node[coGMtjheS6ZRzO0QBjtDEg], [R], v[258], s[ST
ARTED], a[id=dMXtLk25QoSPf5Vw3aRiDQ]], indexUUID [mfsJtjfDRtCbOWTgFuFhpQ], message [failed to perfo
rm indices:data/write/bulk[s] on replica on node {elasticsearch-node-01}{coGMtjheS6ZRzO0QBjtDEg}{19
2.168.56.111}{192.168.56.111:9300}], failure [RemoteTransportException[[elasticsearch-node-01][192.
168.56.111:9300][indices:data/write/bulk[s][r]]]; nested: IndexFailedEngineException[Index failed f
or [status#7258649751730339841]]; nested: OutOfMemoryError[Java heap space]; ]
RemoteTransportException[[elasticsearch-node-01][192.168.56.111:9300][indices:data/write/bulk[s][r]
]]; nested: IndexFailedEngineException[Index failed for [status#7258649751730339841]]; nested: OutOf
MemoryError[Java heap space];
Caused by: [twitter][[twitter][0]] IndexFailedEngineException[Index failed for [status#725864975173
033984]]; nested: OutOfMemoryError[Java heap space];
        at org.elasticsearch.index.engine.InternalEngine.index(InternalEngine.java:462)
        at org.elasticsearch.index.shard.IndexShard.index(IndexShard.java:601)
        at org.elasticsearch.index.engine.Engine$Index.execute(Engine.java:836)
        at org.elasticsearch.action.index.TransportIndexAction.executeIndexRequestOnReplica(Transpo
rtIndexAction.java:196)
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardOperationOnReplica(Transport
ShardBulkAction.java:436)
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardOperationOnReplica(Transport
ShardBulkAction.java:68)
:
```



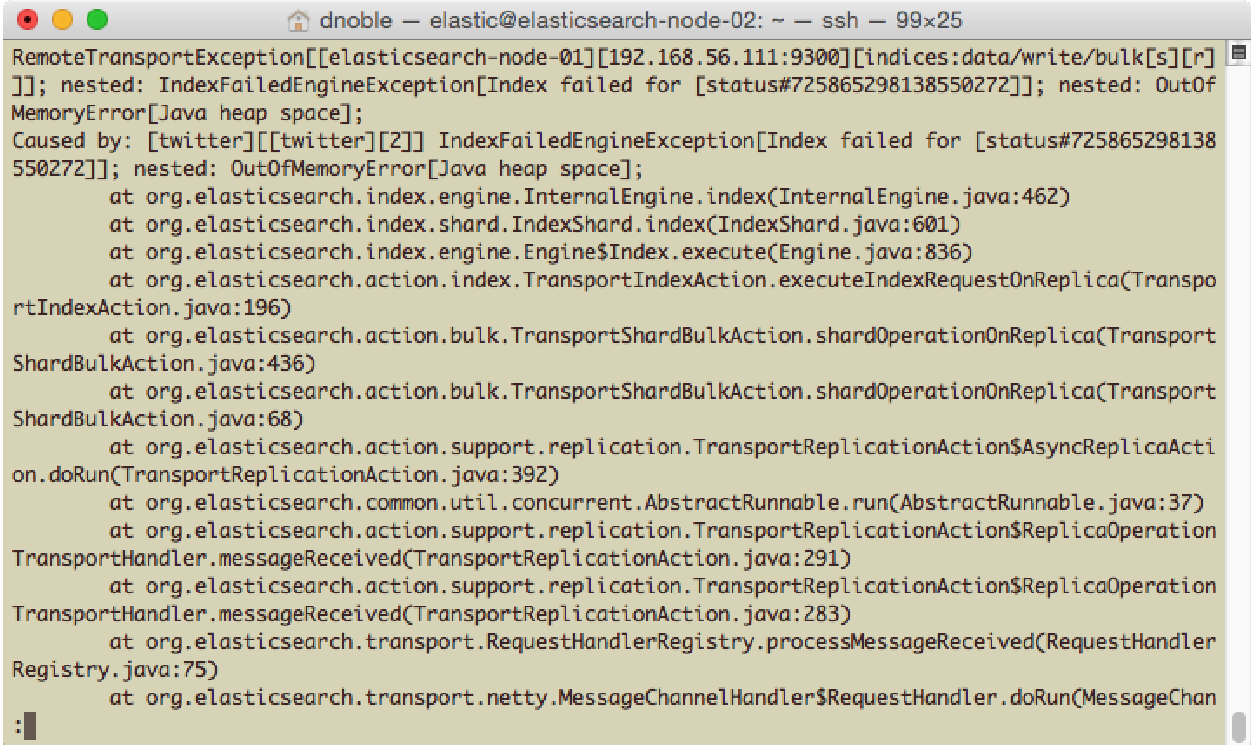
```
nection
java.lang.IllegalStateException: Message not fully read (request) for requestId [46637], action [in
ternal:index/shard/recovery/file_chunk], readerIndex [4119] vs expected [398521]; resetting
        at org.elasticsearch.transport.netty.MessageChannelHandler.messageReceived(MessageChannelHa
ndler.java:121)
        at org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstrea
mHandler.java:70)
        at org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:
564)
        at org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream
(DefaultChannelPipeline.java:791)
        at org.jboss.netty.channel.Channels.fireMessageReceived(Channels.java:296)
        at org.jboss.netty.handler.codec.frame.FrameDecoder.unfoldAndFireMessageReceived(FrameDecod
er.java:462)
        at org.jboss.netty.handler.codec.frame.FrameDecoder.callDecode(FrameDecoder.java:443)
        at org.jboss.netty.handler.codec.frame.FrameDecoder.messageReceived(FrameDecoder.java:310)
        at org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstrea
mHandler.java:70)
        at org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:
564)
        at org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream
(DefaultChannelPipeline.java:791)
        at org.elasticsearch.common.netty.OpenChannelsHandler.handleUpstream(OpenChannelsHandler.ja
va:75)
:
```



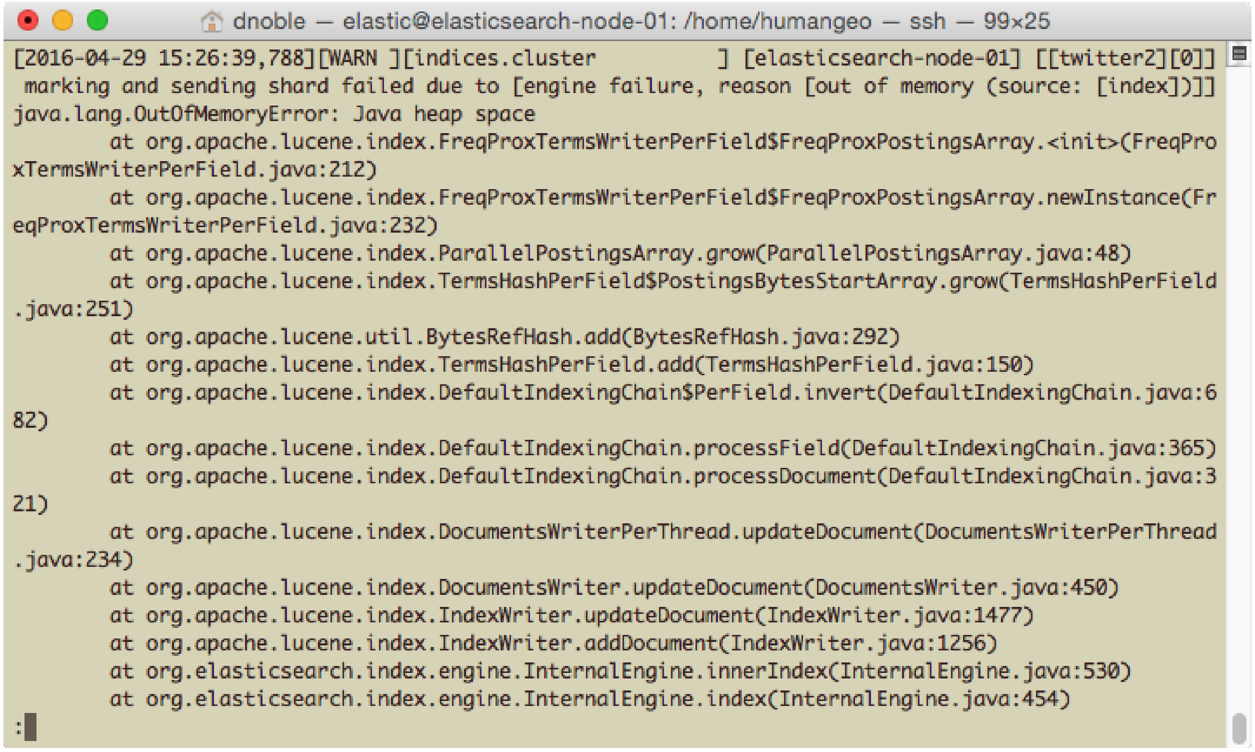
```
-master_failed ({elasticsearch-node-03}{MWjwhPOJSM6B8DXa6ALUDg}{192.168.56.113}{192.168.56.113:9300
})
[2016-04-28 23:02:25,950][DEBUG][action.admin.cluster.state] [elasticsearch-node-01] no known maste
r node, scheduling a retry
[2016-04-28 23:02:25,952][DEBUG][action.admin.indices.get ] [elasticsearch-node-01] no known master
 node, scheduling a retry
[2016-04-28 23:02:25,952][DEBUG][action.admin.cluster.state] [elasticsearch-node-01] no known maste
r node, scheduling a retry
[2016-04-28 23:02:25,957][DEBUG][action.admin.cluster.health] [elasticsearch-node-01] no known mast
er node, scheduling a retry
[2016-04-28 23:02:26,572][DEBUG][action.admin.cluster.state] [elasticsearch-node-01] no known maste
r node, scheduling a retry
[2016-04-28 23:02:26,585][DEBUG][action.admin.cluster.state] [elasticsearch-node-01] no known maste
r node, scheduling a retry
[2016-04-28 23:02:27,457][INFO ][cluster.service          ] [elasticsearch-node-01] detected_master
 {elasticsearch-node-03}{MWjwhPOJSM6B8DXa6ALUDg}{192.168.56.113}{192.168.56.113:9300}, added {{elas
ticsearch-node-03}{MWjwhPOJSM6B8DXa6ALUDg}{192.168.56.113}{192.168.56.113:9300},}, reason: zen-disc
o-receive(from master [{elasticsearch-node-03}{MWjwhPOJSM6B8DXa6ALUDg}{192.168.56.113}{192.168.56.1
13:9300}])
[2016-04-28 23:03:12,545][WARN ][index.engine             ] [elasticsearch-node-01] [twitter][0] fa
iled engine [out of memory (source: [index])]
java.lang.OutOfMemoryError: Java heap space
[2016-04-28 23:03:12,548][WARN ][indices.cluster          ] [elasticsearch-node-01] [[twitter][0]]
marking and sending shard failed due to [engine failure, reason [out of memory (source: [index])]]
:
```



```
[], stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":
{}},"aggs":{"created_at":{"terms":{"field":"created_at"}}}}], extra_source[],
[2016-04-28 22:03:53,449][TRACE][index.search.slowlog.query] took[1.2s], took_millis[1293], types[]
, stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{}
},"aggs":{"text":{"terms":{"field":"text"}}}}], extra_source[],
[2016-04-28 22:59:59,255][TRACE][index.search.slowlog.query] took[1.8s], took_millis[1888], types[]
, stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{}
},"aggs":{"created_at":{"terms":{"field":"created_at"}}}}], extra_source[],
[2016-04-28 23:00:01,026][TRACE][index.search.slowlog.query] took[1.7s], took_millis[1727], types[]
, stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{}
},"aggs":{"created_at":{"terms":{"field":"created_at"}}}}], extra_source[],
[2016-04-28 23:00:07,661][WARN ][index.search.slowlog.query] took[10.2s], took_millis[10279], types
[], stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":
{}},"aggs":{"created_at":{"terms":{"field":"created_at"}}}}], extra_source[],
[2016-04-28 23:01:09,748][TRACE][index.search.slowlog.query] took[676.6ms], took_millis[676], types
[], stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":
{}},"aggs":{"created_at":{"terms":{"field":"created_at"}}}}], extra_source[],
[2016-04-28 23:23:38,200][TRACE][index.search.slowlog.query] took[1.4s], took_millis[1428], types[]
, stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":{}
},"aggs":{"text":{"terms":{"field":"text"}}}}], extra_source[],
[2016-04-28 23:23:55,084][WARN ][index.search.slowlog.query] took[18.3s], took_millis[18367], types
[], stats[], search_type[QUERY_THEN_FETCH], total_shards[3], source[{"size":0,"query":{"match_all":
{}},"aggs":{"text":{"terms":{"field":"text"}}}}], extra_source[],
[2016-04-28 23:26:05,831][TRACE][index.search.slowlog.query] took[1.5s], took_millis[1538], types[]
:
```

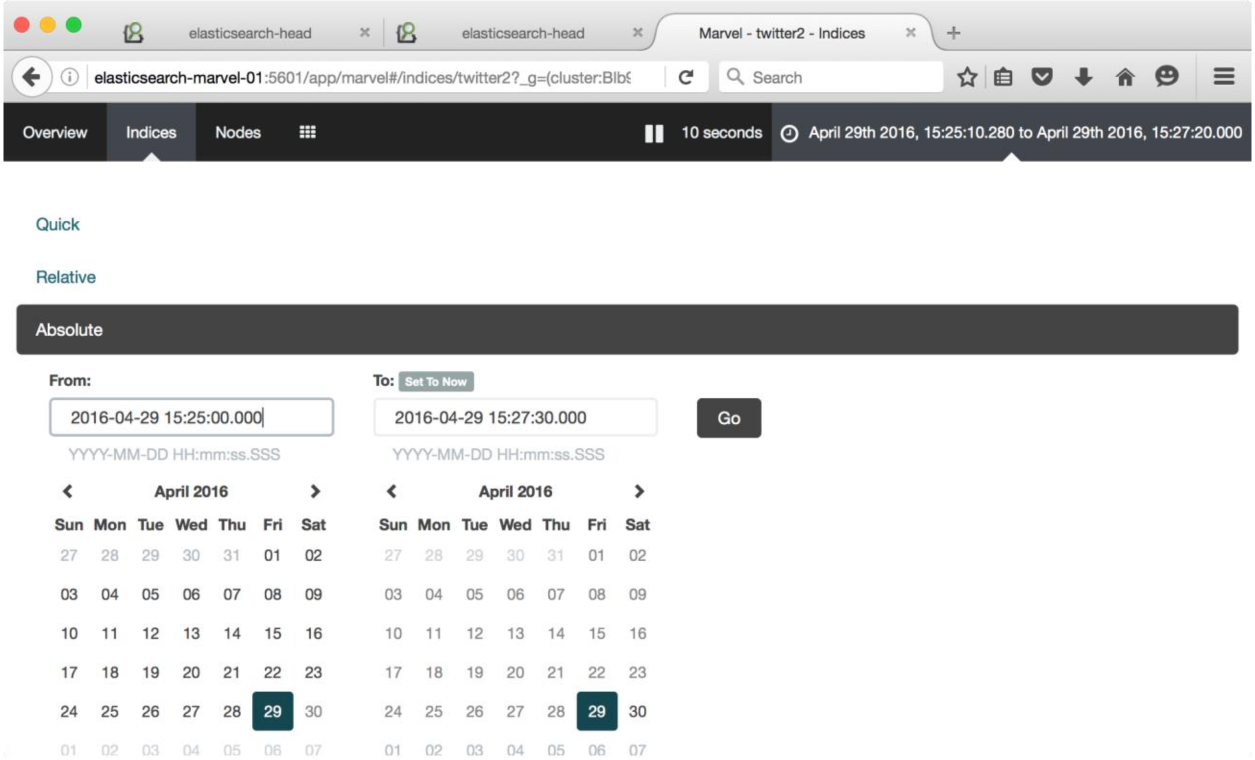


```
RemoteTransportException[[elasticsearch-node-01][192.168.56.111:9300][indices:data/write/bulk[s][r]
]]; nested: IndexFailedEngineException[Index failed for [status#725865298138550272]]; nested: OutOf
MemoryError[Java heap space];
Caused by: [twitter][[twitter][2]] IndexFailedEngineException[Index failed for [status#725865298138
550272]]; nested: OutOfMemoryError[Java heap space];
        at org.elasticsearch.index.engine.InternalEngine.index(InternalEngine.java:462)
        at org.elasticsearch.index.shard.IndexShard.index(IndexShard.java:601)
        at org.elasticsearch.index.engine.Engine$Index.execute(Engine.java:836)
        at org.elasticsearch.action.index.TransportIndexAction.executeIndexRequestOnReplica(Transpo
rtIndexAction.java:196)
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardOperationOnReplica(Transport
ShardBulkAction.java:436)
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardOperationOnReplica(Transport
ShardBulkAction.java:68)
        at org.elasticsearch.action.support.replication.TransportReplicationAction$AsyncReplicaActi
on.doRun(TransportReplicationAction.java:392)
        at org.elasticsearch.common.util.concurrent.AbstractRunnable.run(AbstractRunnable.java:37)
        at org.elasticsearch.action.support.replication.TransportReplicationAction$ReplicaOperation
TransportHandler.messageReceived(TransportReplicationAction.java:291)
        at org.elasticsearch.action.support.replication.TransportReplicationAction$ReplicaOperation
TransportHandler.messageReceived(TransportReplicationAction.java:283)
        at org.elasticsearch.transport.RequestHandlerRegistry.processMessageReceived(RequestHandler
Registry.java:75)
        at org.elasticsearch.transport.netty.MessageChannelHandler$RequestHandler.doRun(MessageChan
:
```



dnoble — elastic@elasticsearch-node-01: /home/humangeo — ssh — 99×25

```
[2016-04-29 15:26:39,788][WARN ][indices.cluster          ] [elasticsearch-node-01] [[twitter2][0]]
 marking and sending shard failed due to [engine failure, reason [out of memory (source: [index])]]
java.lang.OutOfMemoryError: Java heap space
        at org.apache.lucene.index.FreqProxTermsWriterPerField$FreqProxPostingsArray.<init>(FreqPro
xTermsWriterPerField.java:212)
        at org.apache.lucene.index.FreqProxTermsWriterPerField$FreqProxPostingsArray.newInstance(Fr
eqProxTermsWriterPerField.java:232)
        at org.apache.lucene.index.ParallelPostingsArray.grow(ParallelPostingsArray.java:48)
        at org.apache.lucene.index.TermsHashPerField$PostingsBytesStartArray.grow(TermsHashPerField
.java:251)
        at org.apache.lucene.util.BytesRefHash.add(BytesRefHash.java:292)
        at org.apache.lucene.index.TermsHashPerField.add(TermsHashPerField.java:150)
        at org.apache.lucene.index.DefaultIndexingChain$PerField.invert(DefaultIndexingChain.java:6
82)
        at org.apache.lucene.index.DefaultIndexingChain.processField(DefaultIndexingChain.java:365)
        at org.apache.lucene.index.DefaultIndexingChain.processDocument(DefaultIndexingChain.java:3
21)
        at org.apache.lucene.index.DocumentsWriterPerThread.updateDocument(DocumentsWriterPerThread
.java:234)
        at org.apache.lucene.index.DocumentsWriter.updateDocument(DocumentsWriter.java:450)
        at org.apache.lucene.index.IndexWriter.updateDocument(IndexWriter.java:1477)
        at org.apache.lucene.index.IndexWriter.addDocument(IndexWriter.java:1256)
        at org.elasticsearch.index.engine.InternalEngine.innerIndex(InternalEngine.java:530)
        at org.elasticsearch.index.engine.InternalEngine.index(InternalEngine.java:454)
:
```



elasticsearch-head
elasticsearch-head
Marvel - twitter2 - Indices
elasticsearch-marvel-01:5601/app/marvel#/indices/twitter2?_g=(cluster:Blb
Search
Overview
Indices
Nodes
Quick
Relative
Absolute
Set To Now
Go

10 seconds

April 29th 2016, 15:25:10.280 to April 29th 2016, 15:27:20.000

From: 2016-04-29 15:25:00.000

YYYY-MM-DD HH:mm:ss.SSS

To: 2016-04-29 15:27:30.000

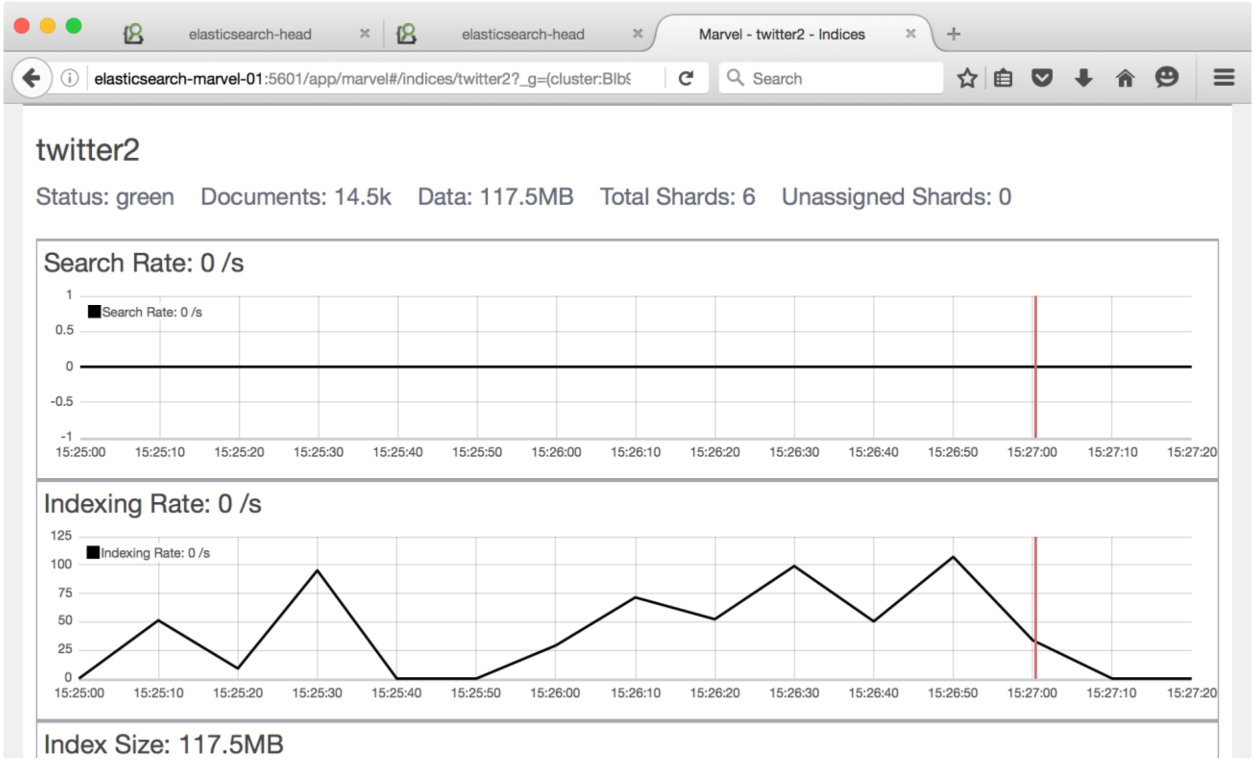
YYYY-MM-DD HH:mm:ss.SSS

April 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
01	02	03	04	05	06	07

April 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
01	02	03	04	05	06	07


elasticsearch-head
elasticsearch-head
Marvel - twitter2 - Indices
elasticsearch-marvel-01:5601/app/marvel#/indices/twitter2?_g=(cluster:Blb!
Search

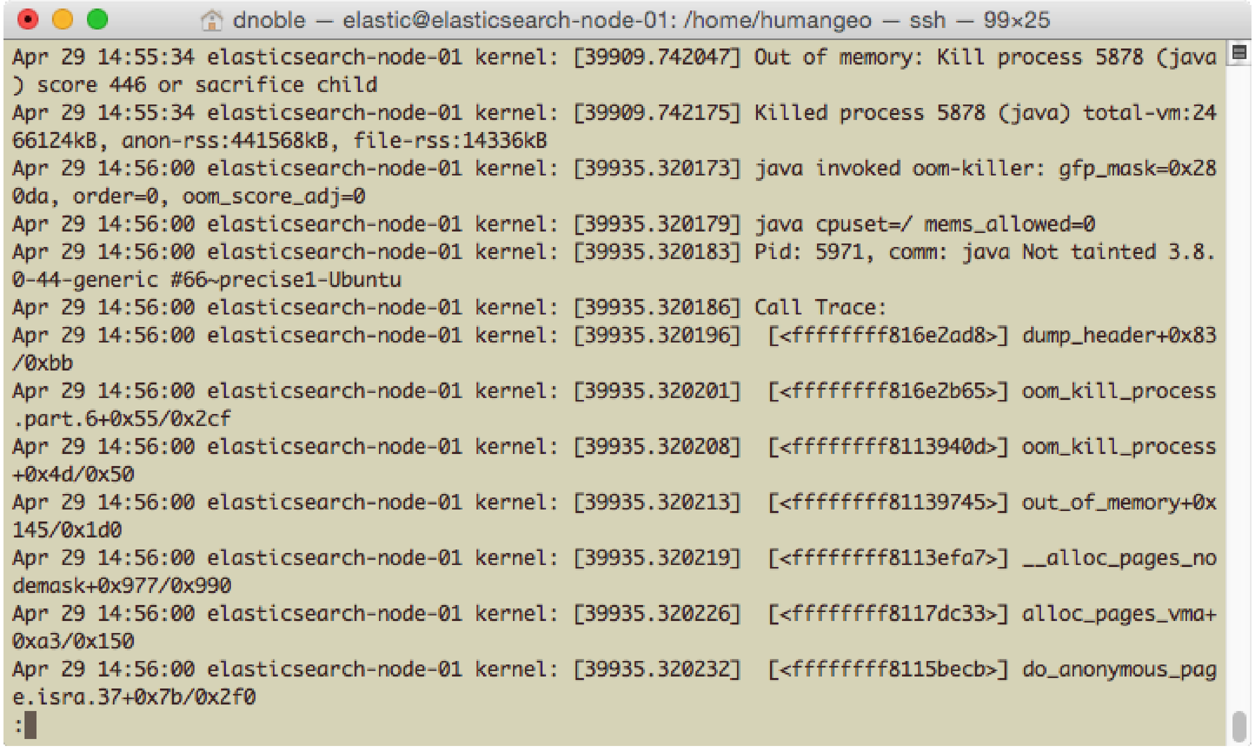
twitter2

Status: green Documents: 14.5k Data: 117.5MB Total Shards: 6 Unassigned Shards: 0

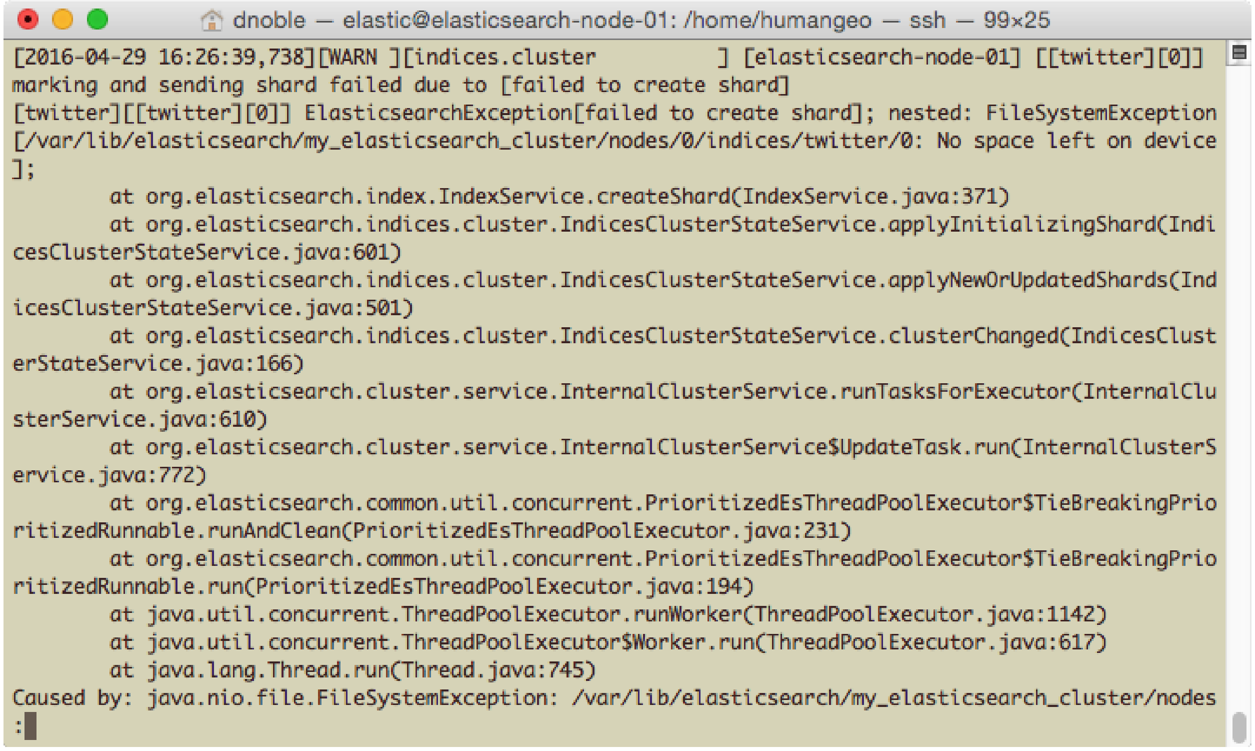
Search Rate: 0 /s

Indexing Rate: 0 /s

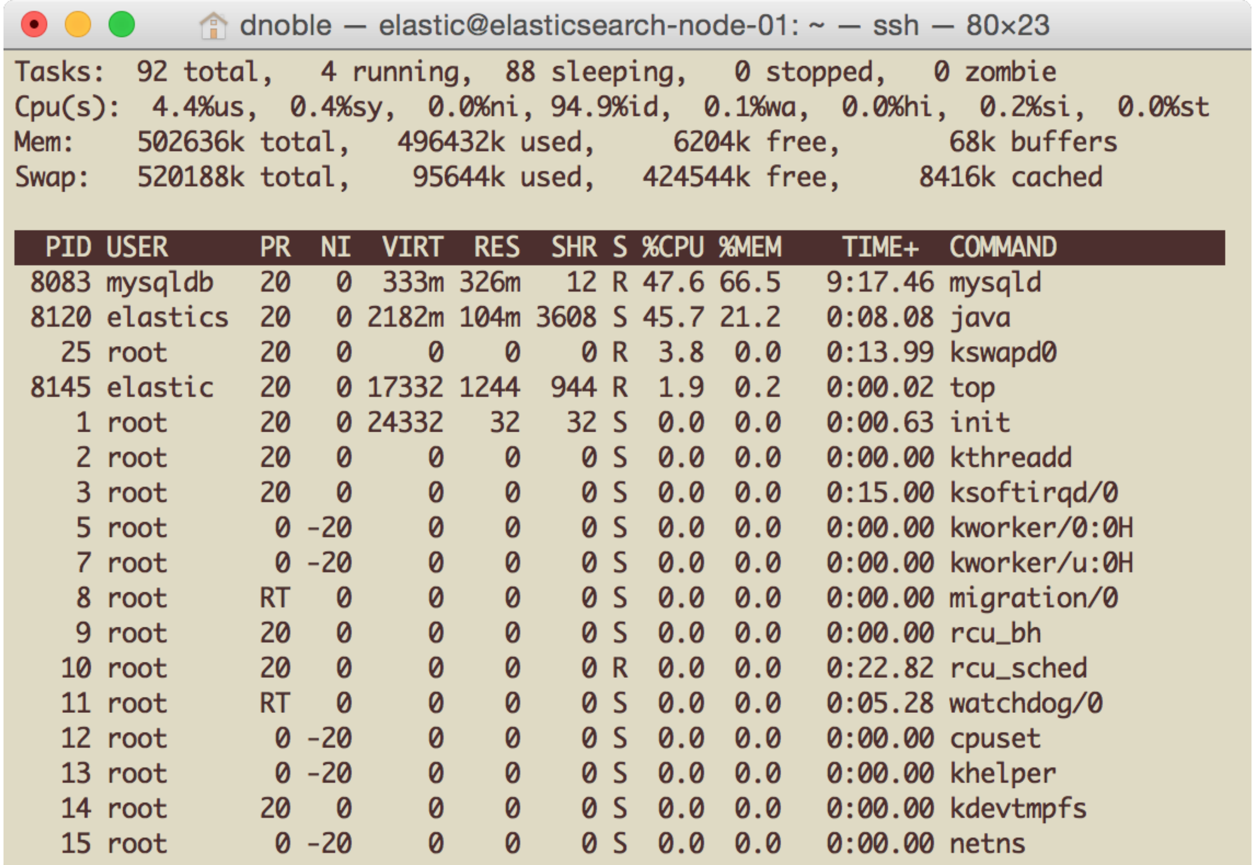
Index Size: 117.5MB


dnoble — elastic@elasticsearch-node-01: /home/humangeo — ssh — 99×25

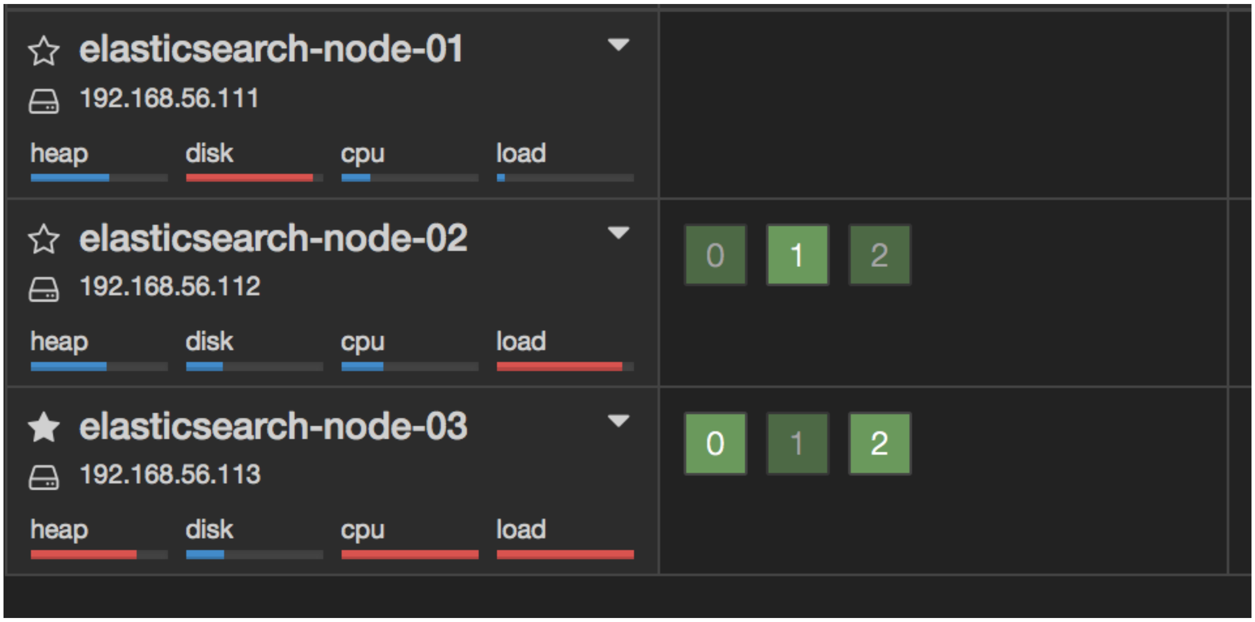
```
Apr 29 14:55:34 elasticsearch-node-01 kernel: [39909.742047] Out of memory: Kill process 5878 (java
) score 446 or sacrifice child
Apr 29 14:55:34 elasticsearch-node-01 kernel: [39909.742175] Killed process 5878 (java) total-vm:24
66124kB, anon-rss:441568kB, file-rss:14336kB
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320173] java invoked oom-killer: gfp_mask=0x28
0da, order=0, oom_score_adj=0
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320179] java cpuset=/ mems_allowed=0
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320183] Pid: 5971, comm: java Not tainted 3.8.
0-44-generic #66~precise1-Ubuntu
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320186] Call Trace:
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320196]  [<ffffffff816e2ad8>] dump_header+0x83
/0xbb
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320201]  [<ffffffff816e2b65>] oom_kill_process
.part.6+0x55/0x2cf
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320208]  [<ffffffff8113940d>] oom_kill_process
+0x4d/0x50
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320213]  [<ffffffff81139745>] out_of_memory+0x
145/0x1d0
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320219]  [<ffffffff8113efa7>] __alloc_pages_no
demask+0x977/0x990
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320226]  [<ffffffff8117dc33>] alloc_pages_vma+
0xa3/0x150
Apr 29 14:56:00 elasticsearch-node-01 kernel: [39935.320232]  [<ffffffff8115becb>] do_anonymous_pag
e.isra.37+0x7b/0x2f0
:
```


dnoble — elastic@elasticsearch-node-01: /home/humangeo — ssh — 99×25

```
[2016-04-29 16:26:39,738][WARN ][indices.cluster          ] [elasticsearch-node-01] [[twitter][0]]
marking and sending shard failed due to [failed to create shard]
[twitter][[twitter][0]] ElasticsearchException[failed to create shard]; nested: FileSystemException
[/var/lib/elasticsearch/my_elasticsearch_cluster/nodes/0/indices/twitter/0: No space left on device
];
        at org.elasticsearch.index.IndexService.createShard(IndexService.java:371)
        at org.elasticsearch.indices.cluster.IndicesClusterStateService.applyInitializingShard(Indi
cesClusterStateService.java:601)
        at org.elasticsearch.indices.cluster.IndicesClusterStateService.applyNewOrUpdatedShards(Ind
icesClusterStateService.java:501)
        at org.elasticsearch.indices.cluster.IndicesClusterStateService.clusterChanged(IndicesClust
erStateService.java:166)
        at org.elasticsearch.cluster.service.InternalClusterService.runTasksForExecutor(InternalClu
sterService.java:610)
        at org.elasticsearch.cluster.service.InternalClusterService$UpdateTask.run(InternalClusterS
ervice.java:772)
        at org.elasticsearch.common.util.concurrent.PrioritizedEsThreadPoolExecutor$TieBreakingPrio
ritizedRunnable.runAndClean(PrioritizedEsThreadPoolExecutor.java:231)
        at org.elasticsearch.common.util.concurrent.PrioritizedEsThreadPoolExecutor$TieBreakingPrio
ritizedRunnable.run(PrioritizedEsThreadPoolExecutor.java:194)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
        at java.lang.Thread.run(Thread.java:745)
Caused by: java.nio.file.FileSystemException: /var/lib/elasticsearch/my_elasticsearch_cluster/nodes
:
```



```
Tasks:  92 total,   4 running,  88 sleeping,   0 stopped,   0 zombie
Cpu(s):  4.4%us,  0.4%sy,  0.0%ni, 94.9%id,  0.1%wa,  0.0%hi,  0.2%si,  0.0%st
Mem:    502636k total,   496432k used,     6204k free,       68k buffers
Swap:   520188k total,    95644k used,   424544k free,     8416k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 8083 mysqldb   20   0  333m 326m   12 R 47.6 66.5   9:17.46 mysqld
 8120 elastics  20   0 2182m 104m 3608 S 45.7 21.2   0:08.08 java
   25 root      20   0     0    0    0 R  3.8  0.0   0:13.99 kswapd0
 8145 elastic   20   0 17332 1244  944 R  1.9  0.2   0:00.02 top
    1 root      20   0 24332   32   32 S  0.0  0.0   0:00.63 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S  0.0  0.0   0:15.00 ksoftirqd/0
    5 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 kworker/u:0H
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    9 root      20   0     0    0    0 S  0.0  0.0   0:00.00 rcu_bh
   10 root      20   0     0    0    0 R  0.0  0.0   0:22.82 rcu_sched
   11 root      RT   0     0    0    0 S  0.0  0.0   0:05.28 watchdog/0
   12 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 cpuset
   13 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 khelper
   14 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kdevtmpfs
   15 root       0 -20     0    0    0 S  0.0  0.0   0:00.00 netns
```

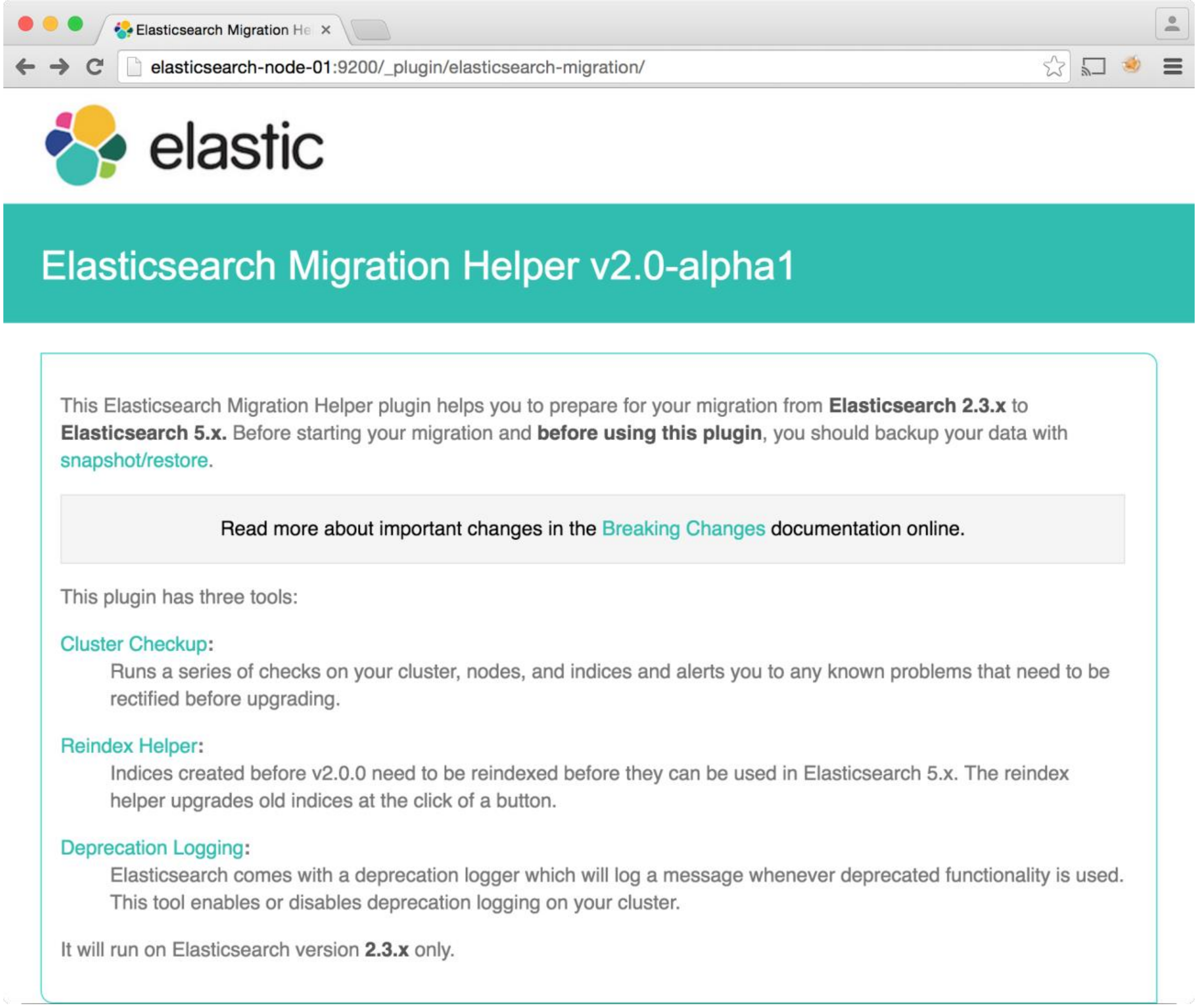


☆ elasticsearch-node-01
192.168.56.111
heap disk cpu load

☆ elasticsearch-node-02
192.168.56.112
heap disk cpu load
0 1 2

★ elasticsearch-node-03
192.168.56.113
heap disk cpu load
0 1 2

Chapter 8: Looking Forward


Elasticsearch Migration He
elasticsearch-node-01:9200/_plugin/elasticsearch-migration/
elastic

Elasticsearch Migration Helper v2.0-alpha1

This Elasticsearch Migration Helper plugin helps you to prepare for your migration from **Elasticsearch 2.3.x** to **Elasticsearch 5.x.** Before starting your migration and **before using this plugin**, you should backup your data with snapshot/restore.

Read more about important changes in the Breaking Changes documentation online.

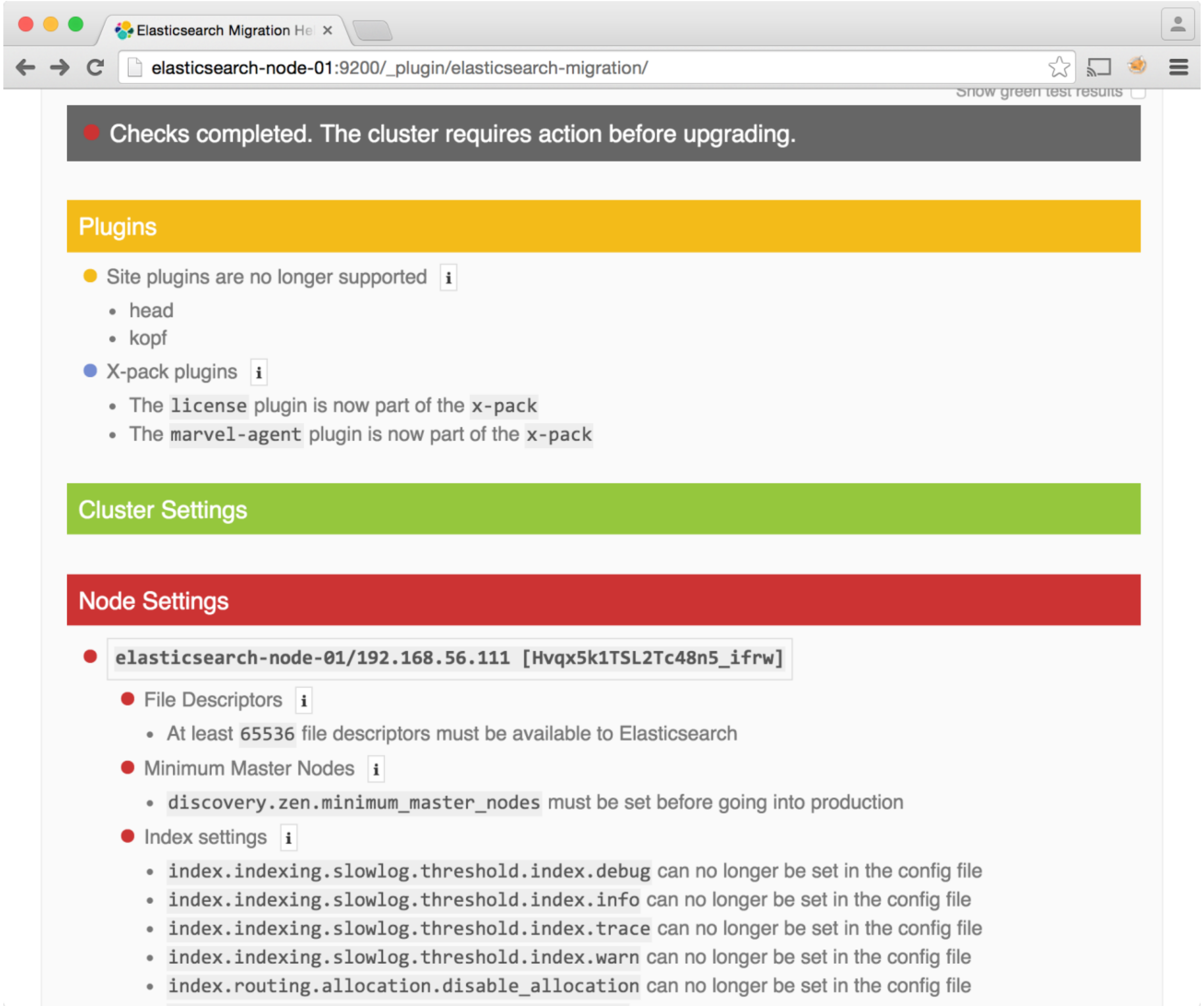
This plugin has three tools:

Cluster Checkup:
Runs a series of checks on your cluster, nodes, and indices and alerts you to any known problems that need to be rectified before upgrading.

Reindex Helper:
Indices created before v2.0.0 need to be reindexed before they can be used in Elasticsearch 5.x. The reindex helper upgrades old indices at the click of a button.

Deprecation Logging:
Elasticsearch comes with a deprecation logger which will log a message whenever deprecated functionality is used. This tool enables or disables deprecation logging on your cluster.

It will run on Elasticsearch version **2.3.x** only.


Elasticsearch Migration He
elasticsearch-node-01:9200/_plugin/elasticsearch-migration/
Show green test results

● Checks completed. The cluster requires action before upgrading.

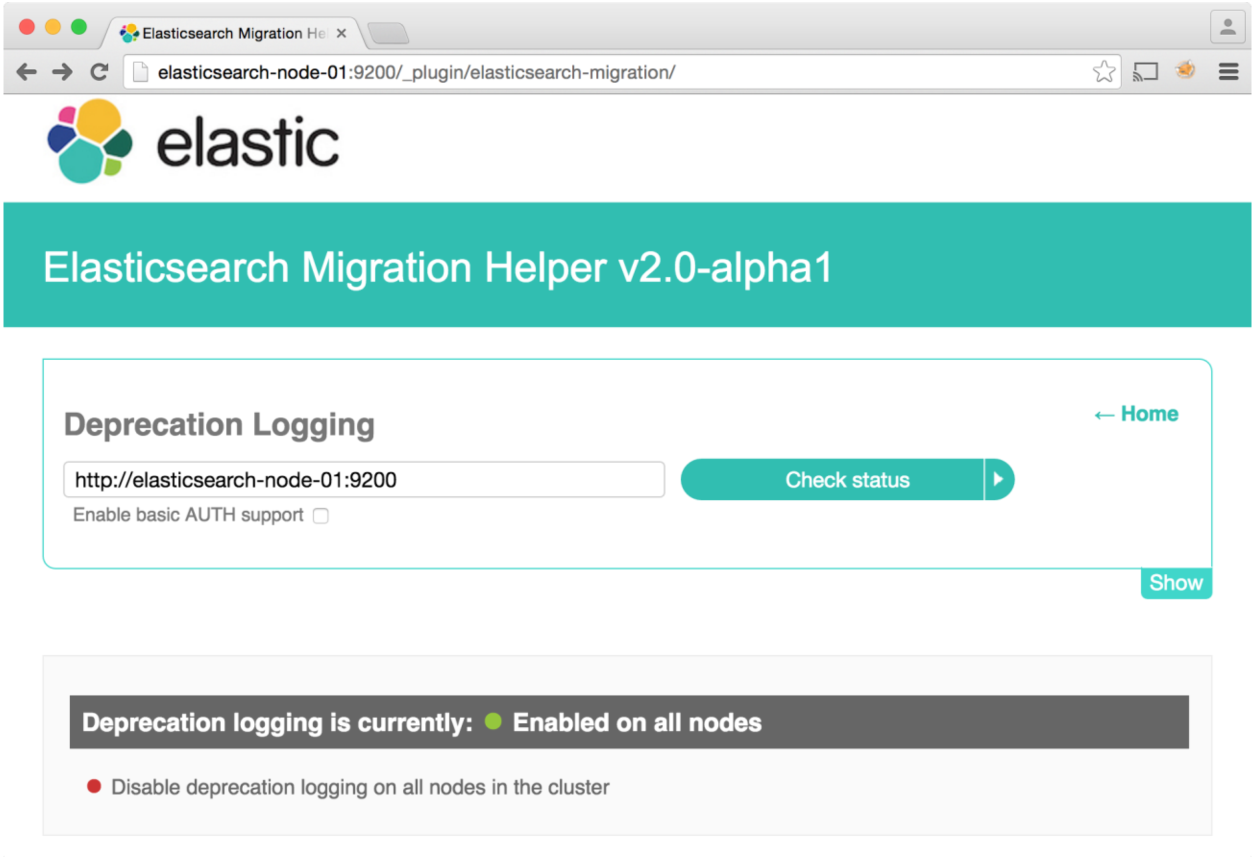
Plugins

- ● Site plugins are no longer supported i
  - head
  - kopf
- ● X-pack plugins i
  - The `license` plugin is now part of the `x-pack`
  - The `marvel-agent` plugin is now part of the `x-pack`

Cluster Settings

Node Settings

- ● `elasticsearch-node-01/192.168.56.111 [Hvqx5k1TSL2Tc48n5_ifrw]`
  - ● File Descriptors i
    - At least `65536` file descriptors must be available to Elasticsearch
  - ● Minimum Master Nodes i
    - `discovery.zen.minimum_master_nodes` must be set before going into production
  - ● Index settings i
    - `index.indexing.slowlog.threshold.index.debug` can no longer be set in the config file
    - `index.indexing.slowlog.threshold.index.info` can no longer be set in the config file
    - `index.indexing.slowlog.threshold.index.trace` can no longer be set in the config file
    - `index.indexing.slowlog.threshold.index.warn` can no longer be set in the config file
    - `index.routing.allocation.disable_allocation` can no longer be set in the config file


Elasticsearch Migration He
elasticsearch-node-01:9200/_plugin/elasticsearch-migration/
elastic

Elasticsearch Migration Helper v2.0-alpha1

Deprecation Logging

← Home

http://elasticsearch-node-01:9200

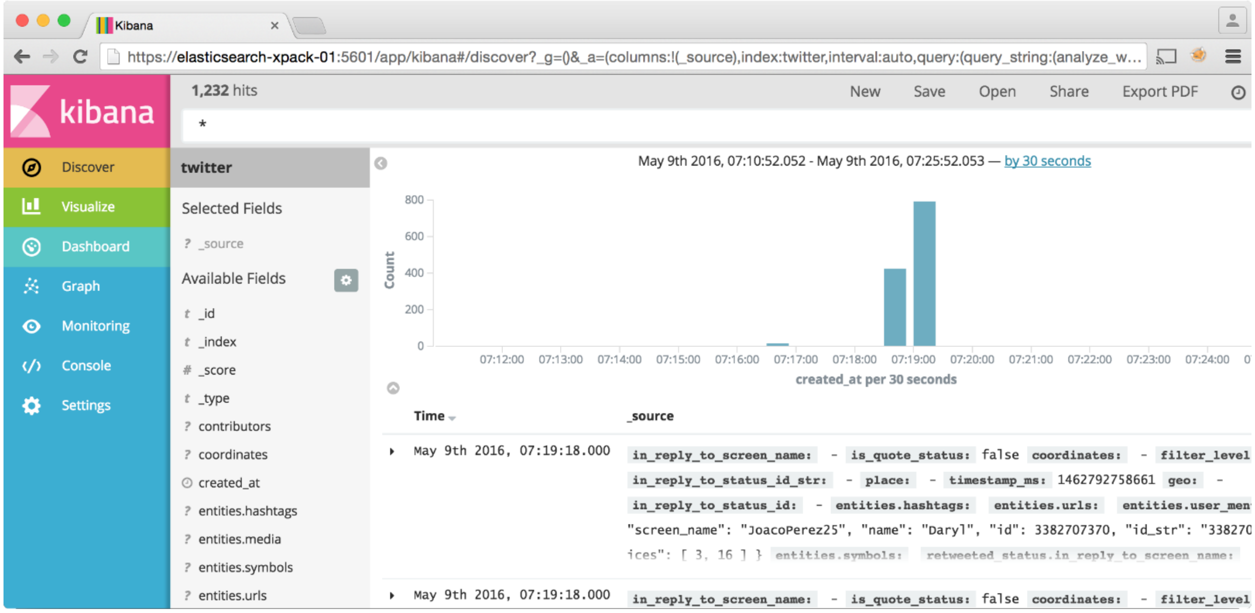
Check status

Enable basic AUTH support □

Show

Deprecation logging is currently: ● Enabled on all nodes

● Disable deprecation logging on all nodes in the cluster



1,232 hits

*

May 9th 2016, 07:10:52.052 - May 9th 2016, 07:25:52.053 — by 30 seconds

twitter

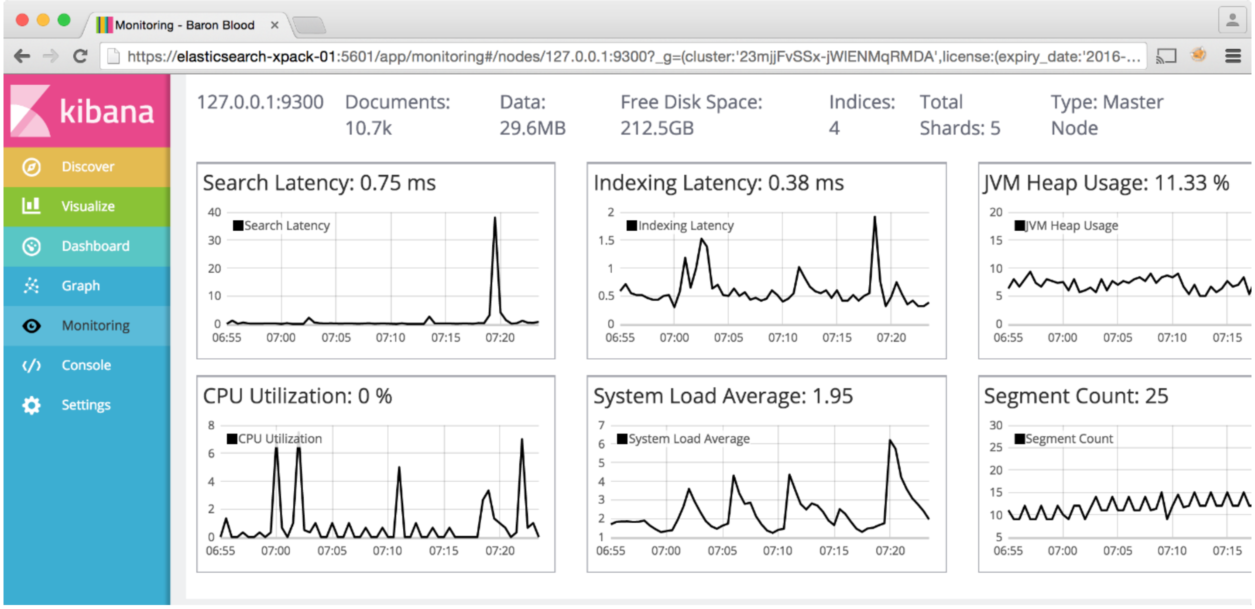
Selected Fields

? _source

Available Fields

t _id
t _index
_score
t _type
? contributors
? coordinates
⏲ created_at
? entities.hashtags
? entities.media
? entities.symbols
? entities.urls

```
Time        _source
May 9th 2016, 07:19:18.000   in_reply_to_screen_name:  -  is_quote_status: false  coordinates:  -  filter_level
                             in_reply_to_status_id_str:  -  place:  -  timestamp_ms: 1462792758661  geo:  -
                             in_reply_to_status_id:  -  entities.hashtags:   entities.urls:   entities.user_men
                             "screen_name": "JoacoPerez25", "name": "Daryl", "id": 3382707370, "id_str": "338270
                             ices": [ 3, 16 ] }  entities.symbols:   retweeted_status.in_reply_to_screen_name:
May 9th 2016, 07:19:18.000   in_reply_to_screen_name:  -  is_quote_status: false  coordinates:  -  filter_level
```



https://elasticsearch-xpack-01:5601/app/monitoring#/nodes/127.0.0.1:9300?_g=(cluster:'23mjjFvSSx-jWIENMqRMDA',license:(expiry_date:'2016-…

127.0.0.1:9300
Documents: 10.7k
Data: 29.6MB
Free Disk Space: 212.5GB
Indices: 4
Total Shards: 5
Type: Master Node

Search Latency: 0.75 ms

Indexing Latency: 0.38 ms

JVM Heap Usage: 11.33 %

CPU Utilization: 0 %

System Load Average: 1.95

Segment Count: 25