Elasticsearch - Tips and Troubleshooting

Tips

Read the basics 🙂

https://www.elastic.co/guide/en/elasticsearch/reference/current/_basic_concepts.html

Show Indexes and status

```
curl localhost:9200/_cat/indices
yellow open filebeat-2016.03.30   5 1      7 0  78.9kb  78.9kb
yellow open logstash-2016.03.28   5 1      1 0  12.7kb  12.7kb
yellow open filebeat-2016.03.31   5 1     10 0 112.2kb 112.2kb
yellow open filebeat-2016.03.21   5 1      1 0  11.9kb  11.9kb
yellow open filebeat-2016.03.22   5 1      1 0  11.9kb  11.9kb
yellow open filebeat-2016.04.01   5 1      6 0  67.6kb  67.6kb
yellow open filebeat-2016.03.23   5 1      1 0  11.9kb  11.9kb
yellow open filebeat-2016.04.02   5 1     15 0 167.5kb 167.5kb
yellow open logstash-2013.12.11   5 1      1 0  11.3kb  11.3kb
yellow open filebeat-2016.03.13   5 1      1 0  11.9kb  11.9kb
yellow open filebeat-2016.04.03   5 1   4718 0     5mb     5mb
yellow open filebeat-2016.03.24   5 1      1 0  12.1kb  12.1kb
yellow open filebeat-2016.03.25   5 1      1 0  11.9kb  11.9kb
yellow open filebeat-2016.03.26   5 1      2 0    23kb    23kb
yellow open packetbeat-2016.04.03 5 1 115546 0  78.3mb  78.3mb
yellow open .kibana               1 1    115 0  86.3kb  86.3kb
yellow open topbeat-2016.04.03    5 1 198026 0  75.9mb  75.9mb
yellow open filebeat-2016.03.27   5 1      2 0    23kb    23kb
yellow open filebeat-2016.03.28   5 1      4 0  45.3kb  45.3kb
yellow open filebeat-2016.03.29   5 1      2 0    23kb    23kb
yellow open filebeat-2016.03.18   5 1      2 0  23.1kb  23.1kb
```

Show Shards and status

```
curl http://localhost:9200/_cat/shards
filebeat-2016.03.30   4 p STARTED         0    160b 77.243.52.155 elkserver
filebeat-2016.03.30   3 p STARTED         2  22.4kb 77.243.52.155 elkserver
filebeat-2016.04.01   3 p STARTED        37  30.9kb 77.243.52.155 elkserver
filebeat-2016.04.01   1 p STARTED        43  98.5kb 77.243.52.155 elkserver
filebeat-2016.03.28   0 p STARTED        21  44.2kb 77.243.52.155 elkserver
topbeat-2016.04.05    4 p STARTED    560941 118.1mb 77.243.52.155 elkserver
topbeat-2016.04.05    3 p STARTED    560573   118mb 77.243.52.155 elkserver
topbeat-2016.04.05    1 p STARTED    561605 118.5mb 77.243.52.155 elkserver
topbeat-2016.04.05    2 p STARTED    560822 117.9mb 77.243.52.155 elkserver
topbeat-2016.04.05    0 p STARTED    561131 118.1mb 77.243.52.155 elkserver
filebeat-2016.03.29   4 p STARTED        25  89.7kb 77.243.52.155 elkserver
filebeat-2016.03.29   0 p STARTED        26 100.6kb 77.243.52.155 elkserver
topbeat-2016.04.06    4 p STARTED    558312 116.5mb 77.243.52.155 elkserver
packetbeat-2016.04.13 0 p STARTED    201328    83mb 77.243.52.155 elkserver
packetbeat-2016.04.13 0 r UNASSIGNED
.kibana               0 p STARTED       126 136.5kb 77.243.52.155 elkserver
filebeat-2016.03.07   4 p STARTED         0    160b 77.243.52.155 elkserver
```

Delete all values in an index

```
curl -XDELETE http://localhost:9200/filebeat*
```

Troubleshooting

Logstash could not deliver data to Elasticsearch that was status "red"

```
curl localhost:9200/_cluster/health?pretty
{
  "cluster_name" : "moselk",
  "status" : "red",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 421,
  "active_shards" : 421,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 25,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 94.39461883408072
}
```

For some reasons, the some "shards" was status "red" and "UNASSIGNED":

```
curl http://localhost:9200/_cat/indices
green  open filebeat-2016.03.30   5 0       5 0  56.9kb  56.9kb
green  open filebeat-2016.03.31   5 0       8 0  90.2kb  90.2kb
green  open filebeat-2016.04.01   5 0     197 0 385.2kb 385.2kb
green  open filebeat-2016.04.02   5 0     196 0 339.3kb 339.3kb
red    open filebeat-2016.04.03   5 0   54394 0  26.6mb  26.6mb
green  open logstash-2013.12.11   5 0       1 0  11.3kb  11.3kb
green  open filebeat-2016.04.04   5 0  119742 0  59.7mb  59.7mb
green  open filebeat-2016.04.05   5 0   53192 0    32mb    32mb
yellow open pinglog-2016.04.13    5 1    1017 0 517.1kb 517.1kb
red    open pinglog-2016.04.10    5 0    1436 0 510.1kb 510.1kb

curl http://localhost:9200/_cat/shards
filebeat-2016.03.30   4 p STARTED         0    160b 77.243.52.155 elkserver
filebeat-2016.03.30   3 p STARTED         2  22.4kb 77.243.52.155 elkserver
pinglog-2016.04.13    4 p STARTED       203 132.3kb 77.243.52.155 elkserver
pinglog-2016.04.13    4 r UNASSIGNED
pinglog-2016.04.13    3 p STARTED       207  64.9kb 77.243.52.155 elkserver
pinglog-2016.04.13    3 r UNASSIGNED
pinglog-2016.04.13    1 p STARTED       207  64.6kb 77.243.52.155 elkserver
pinglog-2016.04.13    1 r UNASSIGNED
pinglog-2016.04.13    2 p STARTED       202   103kb 77.243.52.155 elkserver
pinglog-2016.04.13    2 r UNASSIGNED
pinglog-2016.04.13    0 p STARTED       202  63.1kb 77.243.52.155 elkserver
pinglog-2016.04.13    0 r UNASSIGNED
pinglog-2016.04.10    4 p STARTED       287 120.6kb 77.243.52.155 elkserver
pinglog-2016.04.10    3 p STARTED       294  91.2kb 77.243.52.155 elkserver
pinglog-2016.04.10    1 p STARTED       281 118.5kb 77.243.52.155 elkserver
```

Partly, it seems that a single node Elasticsearch is not optimal, as unassigned shards are reallocated to other servers nomally, but this fixed it:

```
curl -XPUT http://localhost:9200/_settings -d '{ "number_of_replicas" :0 }'


./reassign.sh
```

Where the reassign.sh scripts is like this:

```
NODE="elkserver"
IFS=$'\n'
for line in $(curl -s 'localhost:9200/_cat/shards' | fgrep UNASSIGNED); do
  INDEX=$(echo $line | (awk '{print $1}'))
  SHARD=$(echo $line | (awk '{print $2}'))
  curl -XPOST 'localhost:9200/_cluster/reroute' -d '{
     "commands": [
        {
            "allocate": {
                "index": "'$INDEX'",
                "shard": '$SHARD',
                "node": "'$NODE'",
                "allow_primary": true
          }
        }
    ]
  }'
done
```

Afterwards:

```
curl localhost:9200/_cat/indices
green  open filebeat-2016.03.30   5 1      7 0  78.9kb  78.9kb
green  open logstash-2016.03.28   5 1      1 0  12.7kb  12.7kb
green  open filebeat-2016.03.31   5 1     10 0 112.2kb 112.2kb
green  open filebeat-2016.03.21   5 1      1 0  11.9kb  11.9kb
green  open filebeat-2016.03.22   5 1      1 0  11.9kb  11.9kb
green  open filebeat-2016.04.01   5 1      6 0  67.6kb  67.6kb
green  open filebeat-2016.03.23   5 1      1 0  11.9kb  11.9kb
green  open filebeat-2016.04.02   5 1     15 0 167.5kb 167.5kb
green  open filebeat-2016.03.26   5 1      2 0    23kb    23kb
green  open packetbeat-2016.04.03 5 1 115546 0  78.3mb  78.3mb
green  open .kibana               1 1    115 0  86.3kb  86.3kb
green  open topbeat-2016.04.03    5 1 198026 0  75.9mb  75.9mb
green  open filebeat-2016.03.27   5 1      2 0    23kb    23kb
green  open filebeat-2016.03.28   5 1      4 0  45.3kb  45.3kb
green  open filebeat-2016.03.29   5 1      2 0    23kb    23kb
green  open filebeat-2016.03.18   5 1      2 0  23.1kb  23.1kb
```