QCAT - Bug #1093

Server failure: massive requests over API error in elasticsearch

12 Oct 2016 12:02 - Kurt Gerber

Status:	Closed	**Start date:**	12 Oct 2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	QCAT Backlog	**Spent time:**	0.00 hour
Resolution:			

Description

Problem

During the Night between 11.10 and 12.10.2016, before midnight, massive requests to the api have happened which produced errors in elasticsearch.

The requests all came from the following IP address: **81.142.94.122**

I guess it is UNCCD, but I have to ask them...

This request started on 11/Oct/2016:23:39:04:

```
81.142.94.122 - - [11/Oct/2016:23:39:04 +0200] "GET /en/api/v1/questionnaires/?page=5902268 HTTP/1
.1" 500 1345 "-" "Java/1.7.0_55"
81.142.94.122 - - [11/Oct/2016:23:39:04 +0200] "GET /en/api/v1/questionnaires/?page=3882341 HTTP/1
.1" 500 1345 "-" "Java/1.7.0_55"
```

with more than 10 requests per second.

In elasticsearch each request produced this error message:

```
[2016-10-11 23:39:04,441][DEBUG][action.search.type       ] [Peggy Carter] [qcat_wocat_1][0], node
[kv7klLv0RAW7S_yCAHe7Xw], [P], v[16], s[STARTED], a[id=fGjNxJO3TSq6pYGh5XWD1A]: Failed to execute
[org.elasticsearch.action.search.SearchRequest@4418d4ae] lastShard [true]
RemoteTransportException[[Peggy Carter][127.0.0.1:9300][indices:data/read/search[phase/query]]]; n
ested: QueryPhaseExecutionException[Result window is too large, from + size must be less than or e
qual to: [10000] but was [97208550]. See the scroll api for a more efficient way to request large
data sets. This limit can be set by changing the [index.max_result _window] index level parameter.
];
Caused by: QueryPhaseExecutionException[Result window is too large, from + size must be less than
or equal to: [10000] but was [97208550]. See the scroll api for a more efficient way to request la
rge data sets. This limit can be set by changing the [index.max_result_window] index level paramet
er.]
        at org.elasticsearch.search.internal.DefaultSearchContext.preProcess(DefaultSearchContext.
java:200)
        at org.elasticsearch.search.query.QueryPhase.preProcess(QueryPhase.java:103)
        at org.elasticsearch.search.SearchService.createContext(SearchService.java:674)
        at org.elasticsearch.search.SearchService.createAndPutContext(SearchService.java:618)
        at org.elasticsearch.search.SearchService.executeQueryPhase(SearchService.java:369)
        at org.elasticsearch.search.action.SearchServiceTransportAction$SearchQueryTransportHandle
r.messageReceived(SearchServiceTransportAction.java:368)
        at org.elasticsearch.search.action.SearchServiceTransportAction$SearchQueryTransportHandle
r.messageReceived(SearchServiceTransportAction.java:365)
        at org.elasticsearch.transport.TransportService$4.doRun(TransportService.java:350)
        at org.elasticsearch.common.util.concurrent.AbstractRunnable.run(AbstractRunnable.java:37)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
        at java.lang.Thread.run(Thread.java:745)
```

This produced a log file of more than 1 GB per hour.

After 2:00 in the morning of 12.10.2016 /var/log run out of space and the application crashed.

Solution for the moment:

- IP Adresse 81.142.94.122 blocked completely in the firewall

Subtasks:

Task # 1094: fail2ban rule to ban ip adresses spoofing qcat	**Closed**
Task # 1095: More robust behavior of elasticsearch	**Closed**

History

#1 - 05 Dec 2016 08:37 - Kurt Gerber

- Status changed from New to Closed