# ELASTICSEARCH几个问题的解决

* [Elasticsearch几个问题的解决](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html)

* + [大量](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "unassigned-shards" \o "大量unassigned shards)**[unassigned](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "unassigned-shards" \o "大量unassigned shards)****[shards](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "unassigned-shards" \o "大量unassigned shards)**
  + [status: red](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html#status-red)

* + **[fix](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "fix-unassigned-shards" \o "fix unassigned shards)****[unassigned](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "fix-unassigned-shards" \o "fix unassigned shards)****[shards](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html" \l "fix-unassigned-shards" \o "fix unassigned shards)**
  + [“Too many open files”](http://www.wklken.me/posts/2015/05/23/elasticsearch-issues.html#too-many-open-files)

今天惯例看统计报表, 才发现es集群悲剧了......昨天下午到今天早上, 持续报错, 写了1G的错误日志>\_<#(暂无监控....)

当前状态: 单台机器, 单节点(空集群), 200W 数据, 500+shrads, 约3G大小

以下是几个问题的处理过程

### 大量unassigned shards

其实刚搭完运行时就是status: yellow(所有主分片可用，但存在不可用的从分片), 只有一个节点, 主分片启动并运行正常, 可以成功处理请求, 但是存在**unassigned**\_**shards**, 即存在没有被分配到节点的从分片.(只有一个节点.....)

.当时数据量小, 就暂时没关注. 然后, 随着时间推移, 出现了大量**unassigned** **shards**

curl -XGET http://localhost:9200/\_cluster/health\?pretty

{

"cluster\_name" : "elasticsearch",

"status" : "yellow",

"timed\_out" : false,

"number\_of\_nodes" : 2,

"number\_of\_data\_nodes" : 1,

"active\_primary\_**shards**" : 538,

"active\_**shards**" : 538,

"relocating\_**shards**" : 0,

"initializing\_**shards**" : 0,

"**unassigned**\_**shards**" : 558,

"number\_of\_pending\_tasks" : 0

}

处理方式: 找了台内网机器, 部署另一个节点(保证[cluster.name](http://cluster.name/)一致即可, 自动发现, 赞一个). 当然, 如果你资源有限只有一台机器, 使用相同命令再启动一个es实例也行. 再次检查集群健康, 发现**unassigned**\_**shards**减少, active\_**shards**增多.

操作完后, 集群健康从yellow恢复到 green

### status: red

集群健康恶化了......

这次检查发现是status: red(存在不可用的主要分片)

curl -XGET http://localhost:9200/\_cluster/health\?pretty

{

"cluster\_name" : "elasticsearch",

"status" : "red", // missing some primary **shards**

"timed\_out" : false,

"number\_of\_nodes" : 4,

"number\_of\_data\_nodes" : 2,

"active\_primary\_**shards**" : 538,

"active\_**shards**" : 1076,

"relocating\_**shards**" : 0,

"initializing\_**shards**" : 0,

"**unassigned**\_**shards**" : 20, // where your lost primary **shards** are.

"number\_of\_pending\_tasks" : 0

}

### fix unassigned shards

开始着手修复

查看所有分片状态

curl -XGET http://localhost:9200/\_cat/**shards**

找出**UNASSIGNED**分片

curl -s "http://localhost:9200/\_cat/**shards**" | grep **UNASSIGNED**

pv-2015.05.22 3 p **UNASSIGNED**

pv-2015.05.22 3 r **UNASSIGNED**

pv-2015.05.22 1 p **UNASSIGNED**

pv-2015.05.22 1 r **UNASSIGNED**

查询得到master节点的唯一标识

curl 'localhost:9200/\_nodes/process?pretty'

{

"cluster\_name" : "elasticsearch",

"nodes" : {

"AfUyuXmGTESHXpwi4OExxx" : {

"name" : "Master",

....

"attributes" : {

"master" : "true"

},

.....

执行reroute(分多次, 变更shard的值为**UNASSIGNED**查询结果中编号, 上一步查询结果是1和3)

curl -XPOST 'localhost:9200/\_cluster/reroute' -d '{

"commands" : [ {

"allocate" : {

"index" : "pv-2015.05.22",

"shard" : 1,

"node" : "AfUyuXmGTESHXpwi4OExxx",

"allow\_primary" : true

}

}

]

}'

批量处理的脚本(当数量很多的话, 注意替换node的名字)

#!/bin/bash

for index in $(curl -s 'http://localhost:9200/\_cat/**shards**' | grep **UNASSIGNED** | awk '{print $1}' | sort | uniq); do

for shard in $(curl -s 'http://localhost:9200/\_cat/**shards**' | grep **UNASSIGNED** | grep $index | awk '{print $2}' | sort | uniq); do

echo $index $shard

curl -XPOST 'localhost:9200/\_cluster/reroute' -d "{

'commands' : [ {

'allocate' : {

'index' : $index,

'shard' : $shard,

'node' : 'Master',

'allow\_primary' : true

}

}

]

}"

sleep 5

done

done

### “Too many open files”

发现日志中大量出现这个错误

执行

curl http://localhost:9200/\_nodes/process\?pretty

可以看到

"max\_file\_descriptors" : 4096,

官方文档中

Make sure to increase the number of open files descriptors on the machine (or for the user running elasticsearch). Setting it to 32k or even 64k is recommended.

而此时, 可以在系统级做修改, 然后全局生效

最简单的做法, 在bin/elasticsearch文件开始的位置加入

ulimit -n 64000

然后重启es, 再次查询看到

"max\_file\_descriptors" : 64000,

问题解决