# 安全重启集群节点

1. 关闭集群的shard均衡

curl -XPUT http://192.168.1.2:9200/\_cluster/settings -d'

{

"transient" : {

"cluster.routing.allocation.enable" : "none"

}

}'

1. Shutdown节点

curl -XPOST <http://192.168.1.3:9200/_cluster/nodes/_local/_shutdown>

1. 打开集群的shard均衡

curl -XPUT http://192.168.1.2:9200/\_cluster/settings -d'

{

"transient" : {

"cluster.routing.allocation.enable" : "all"

}

}'

# 集群节点配置说明

cluster.name: tsg\_es

node.name: "192.168.239.128"

discovery.zen.ping.unicast.hosts: ["192.168.239.128", "192.168.239.129"]

path.data: /home/elas/data/es/data

path.logs: /home/ elas /data/es/logs

network.host: "192.168.239.128"

# elasticsearch http安全认证

elasticsearch及相关插件都是没有鉴权的，可以随便删除所有数据，因此在公网暴露es主机是不安全。可以采用 elasticsearch-http-basic 进行ip和http鉴权。

# Github [elasticsearch-http-basic](https://github.com/Asquera/elasticsearch-http-basic)

下载对应版本的jar包或者源码进行编译。

在es\_home/plugins/下创建目录http-basic,将jar拷入该目录

修改配置文件

http.basic.enabled true 开关，开启会接管全部HTTP连接

http.basic.user "admin" 账号

http.basic.password "admin\_pw" 密码

http.basic.ipwhitelist ["localhost", "127.0.0.1"] 白名单内的ip访问不需要通过账号和密码，支持ip和主机名，不支持ip区间或正则

http.basic.trusted\_proxy\_chains [] 信任代理列表

http.basic.log false 把无授权的访问事件添加到ES的日志

http.basic.xforward "" 记载代理路径的header字段名