# ELK日志分析系统

需要两台服务器，主要看日志

地址需要用到动态网

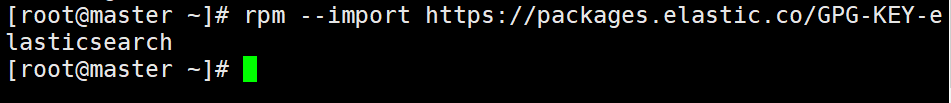
要上网下载软件

Master：192.168.0.100

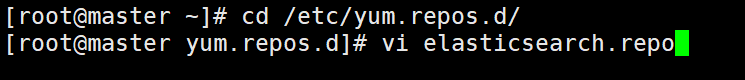
Slave：192.168.0.104

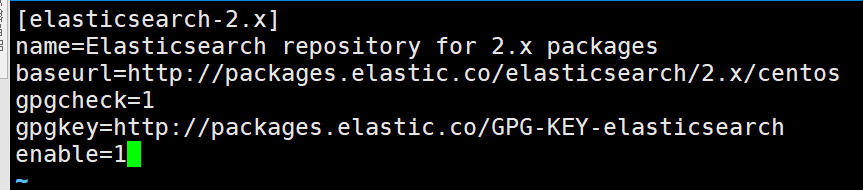
## ES部署

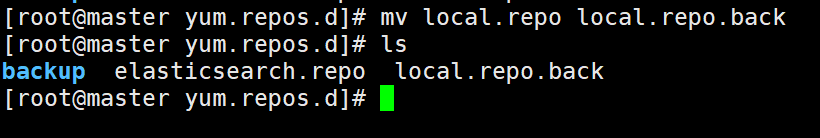
下载密钥



编写一个新的yum仓库







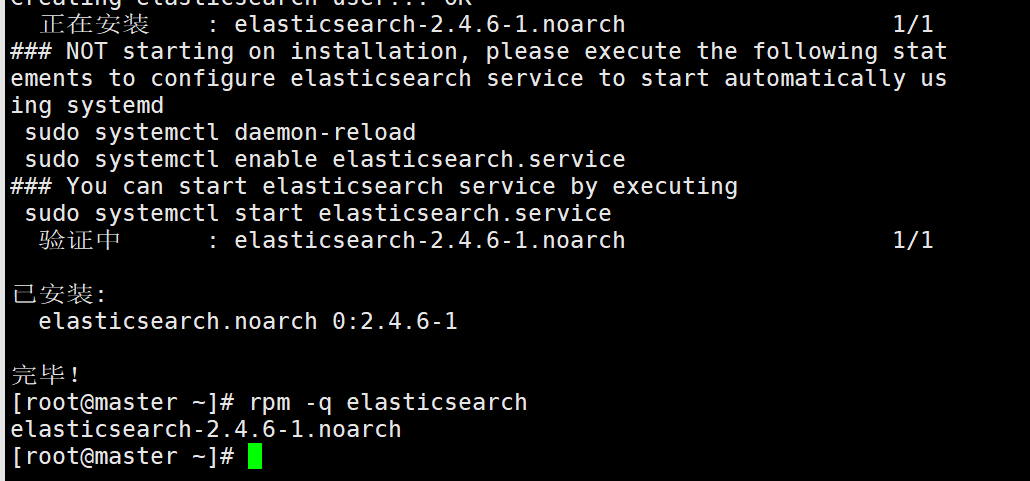
如果安装不了就把原来的yum仓库注释掉

安装list

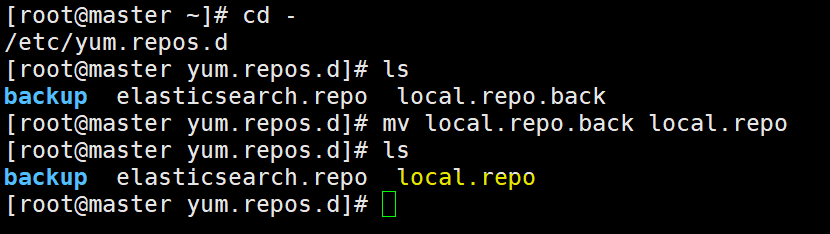


开始安装elasticsearch

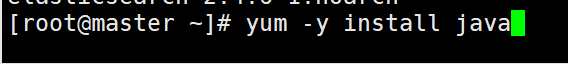


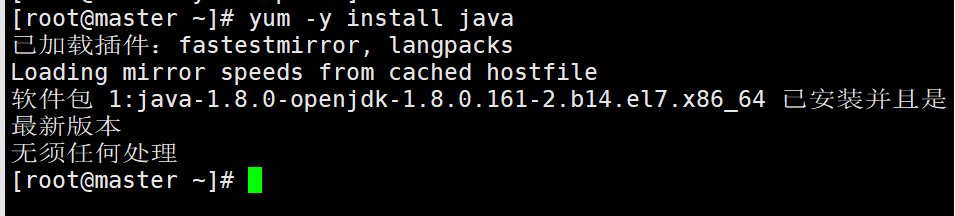


把注释的yum仓库改回来

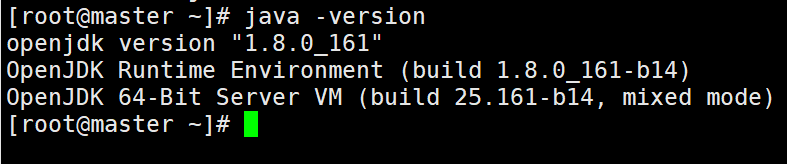


安装java

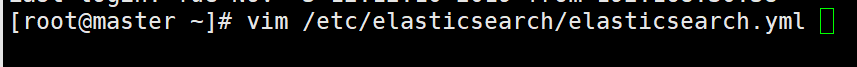




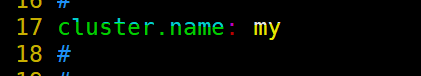
查看一下



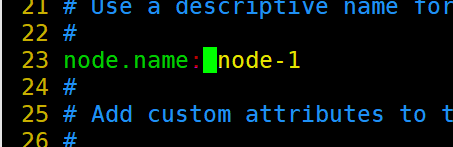
修改配置文件（用vim修改要用wq！退出）



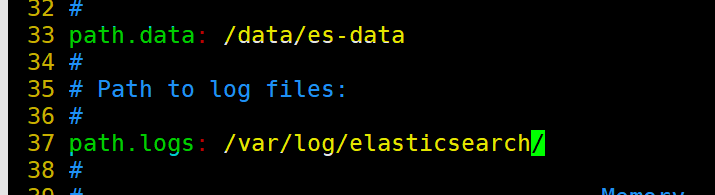
17行 集群名称



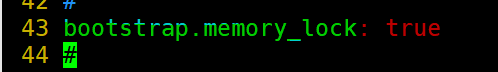
23行 节点名称



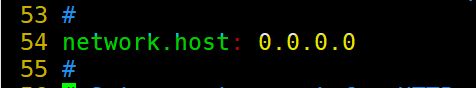
33行 工作目录



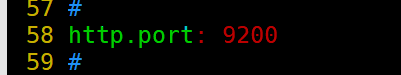
43行 防止交换swap分区



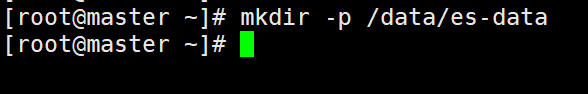
54行 监听网络改成所有的



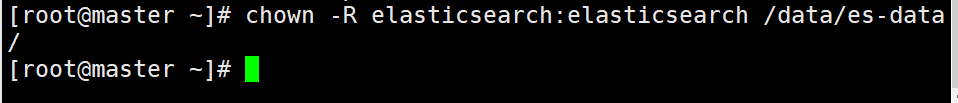
58行 端口



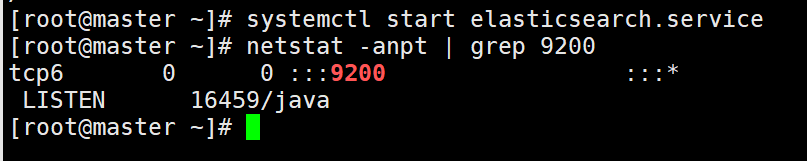
创建一个不存在的文件夹



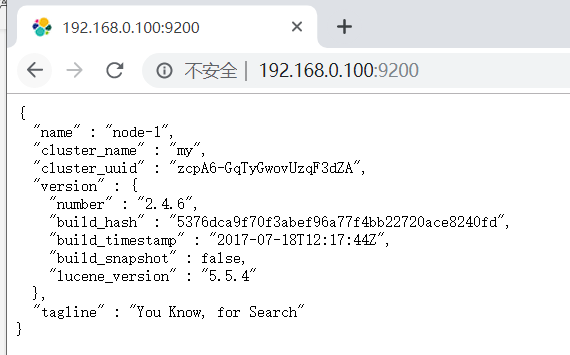
改变属主属组



启动服务加查看端口号

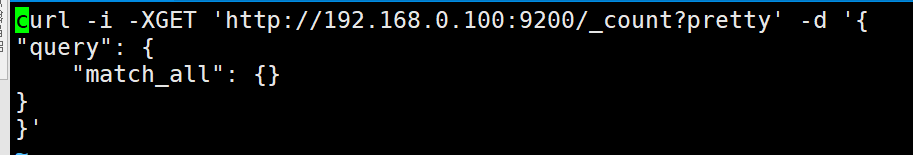


测试

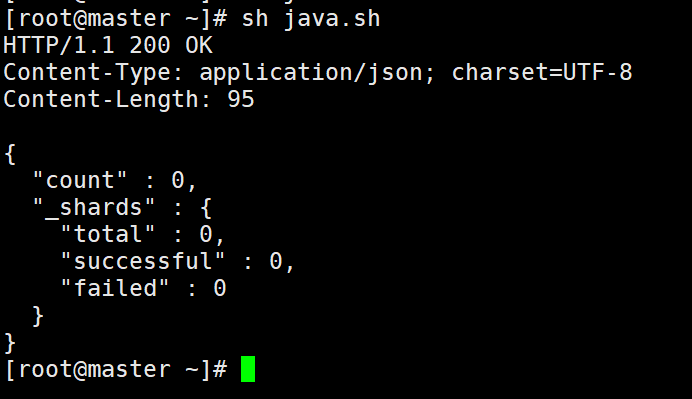


编写一个脚本

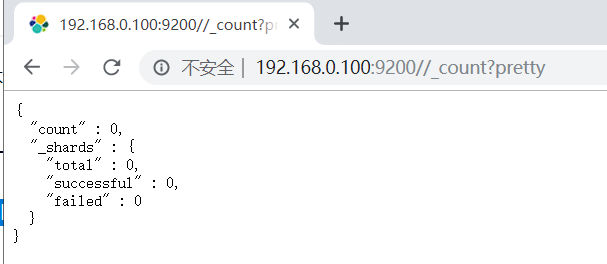




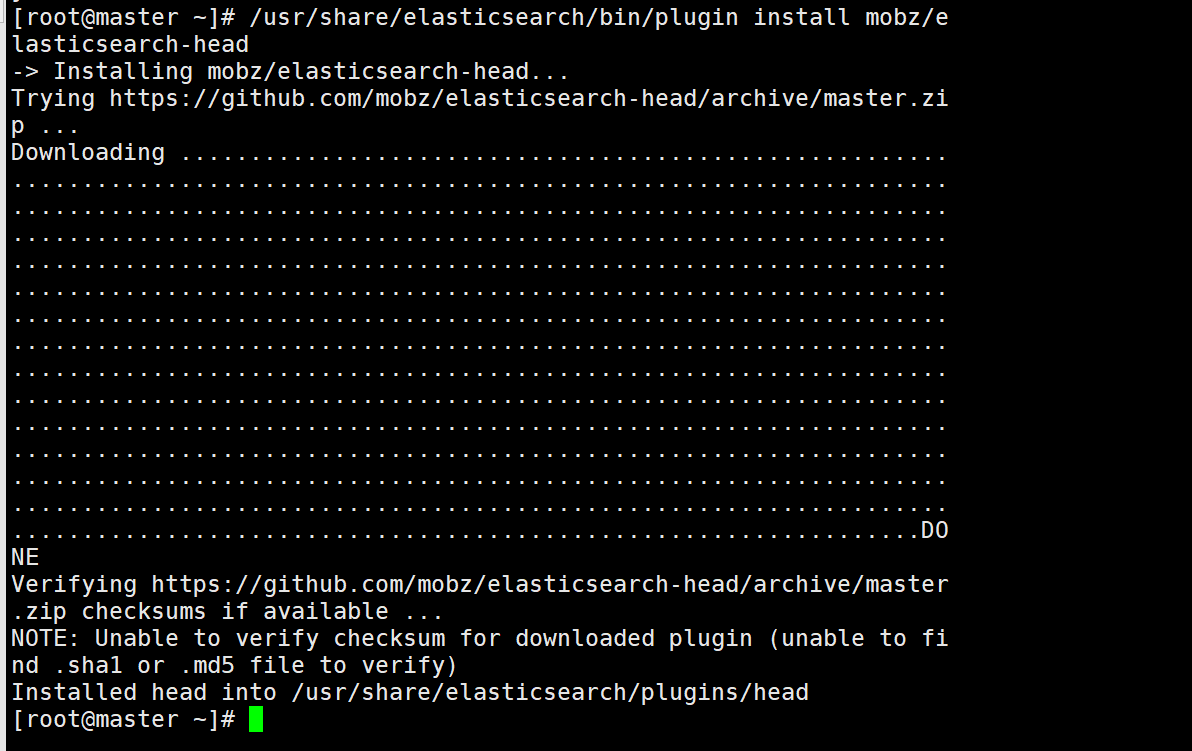
运行脚本



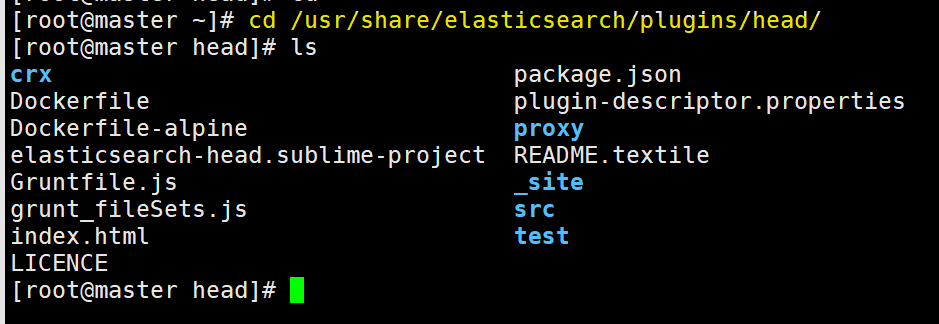
测试



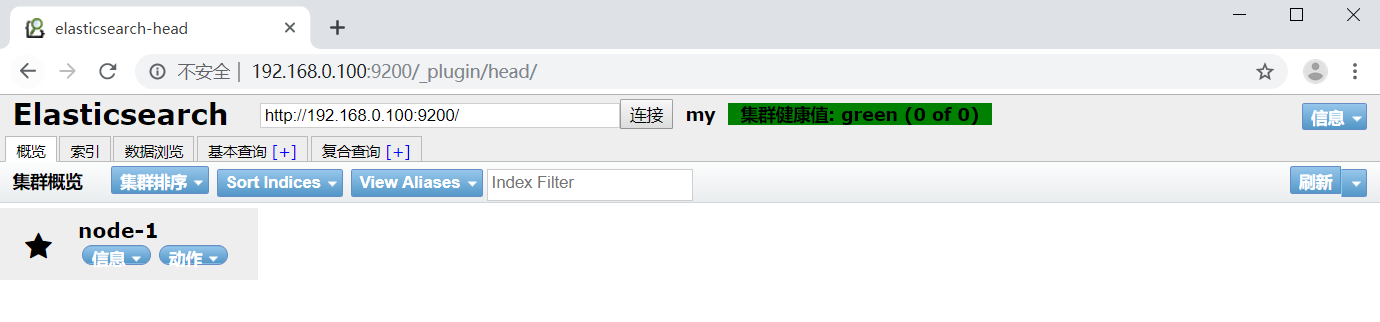
在主的上面安装ES插件



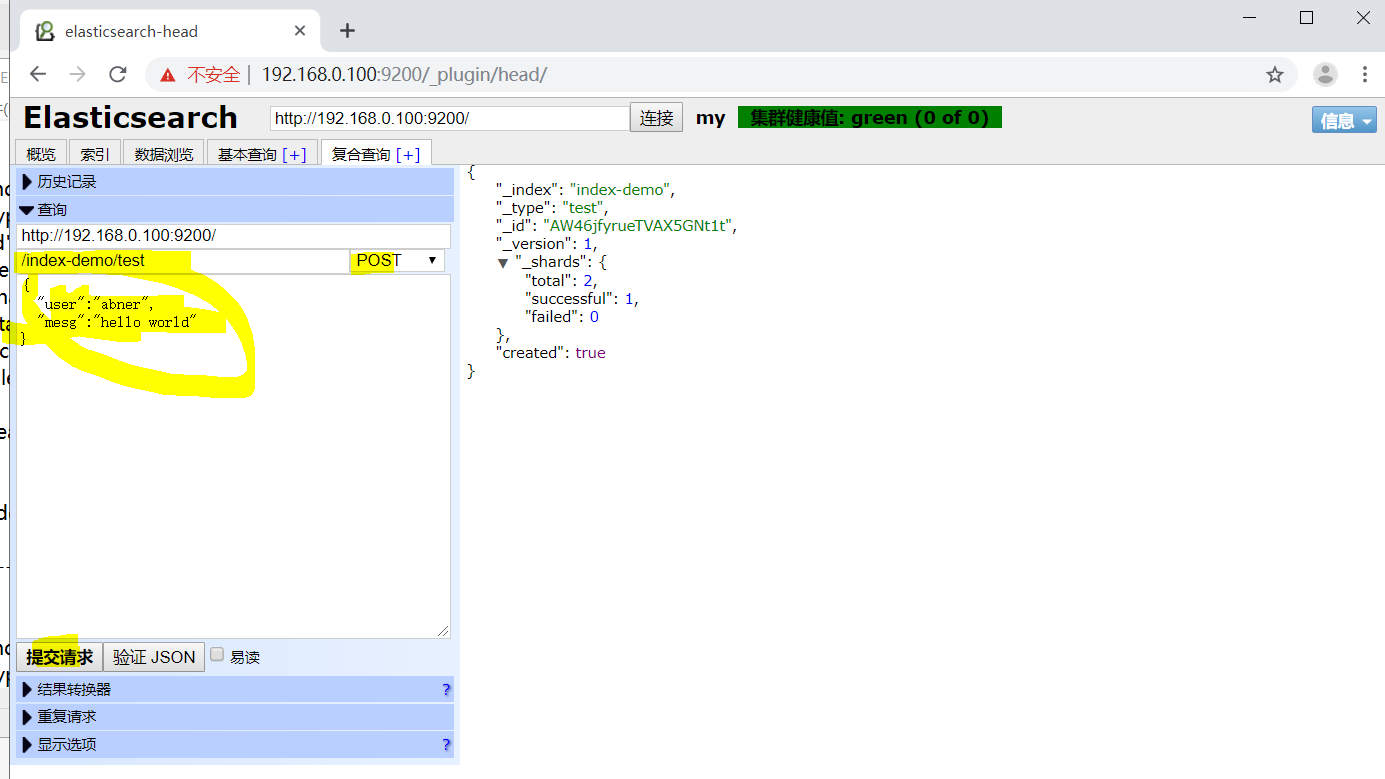
查看安装位置



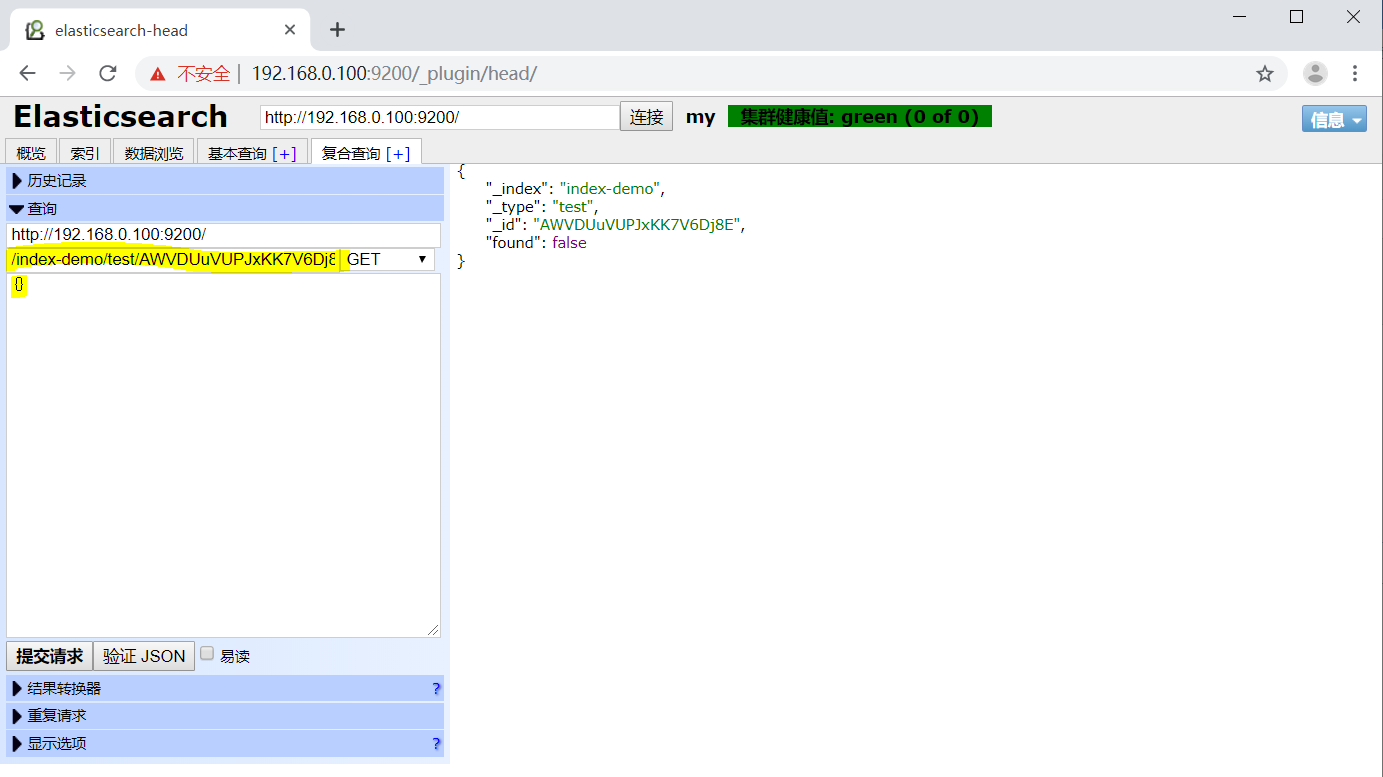
测试



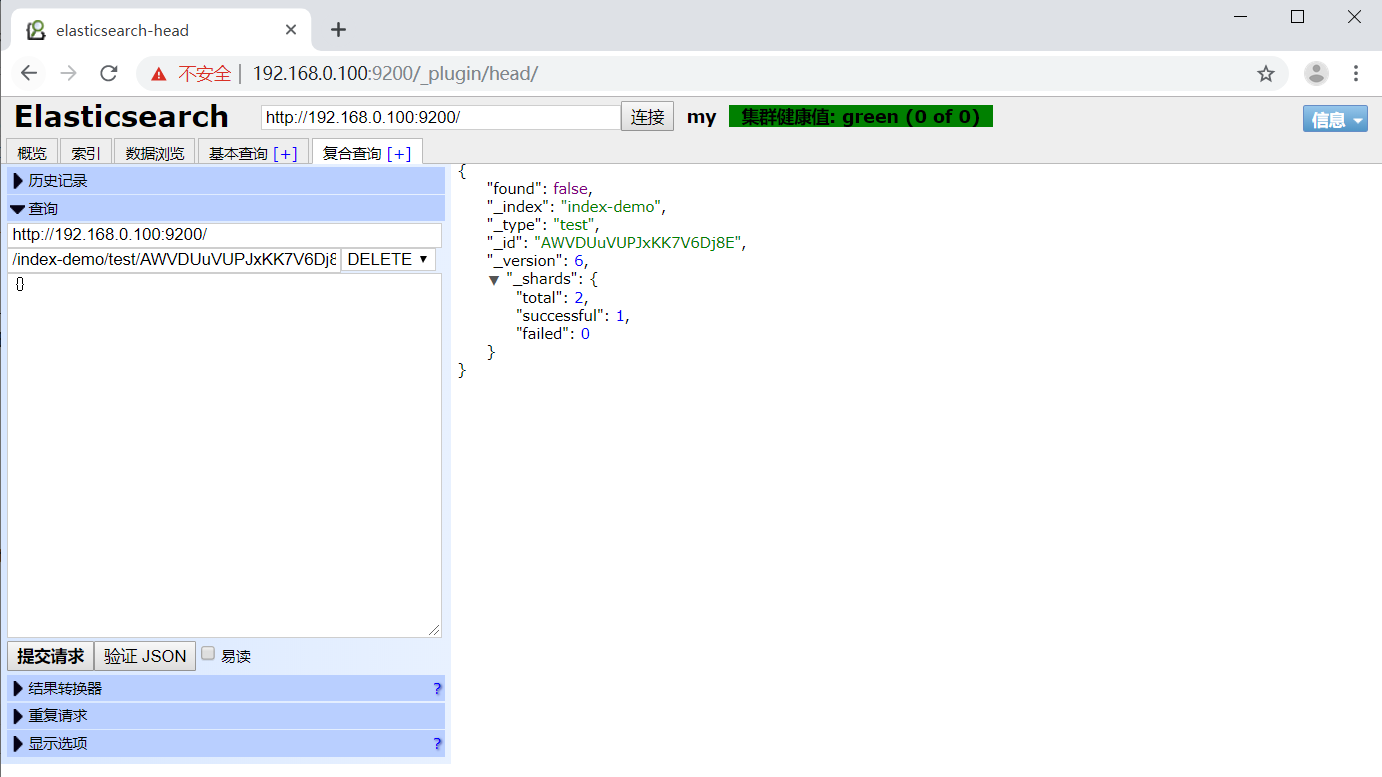
复合查询，之后提交测试



下载



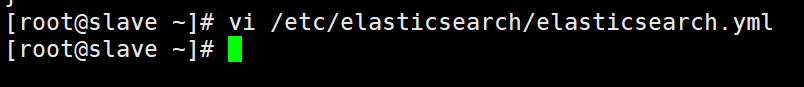
删除

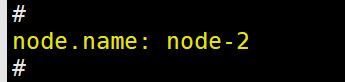


Slave

从的服务器也这样操作（不用安装ES插件）

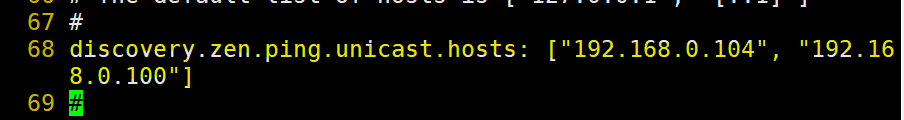
配置和主服务器一样除了节点名称不一样





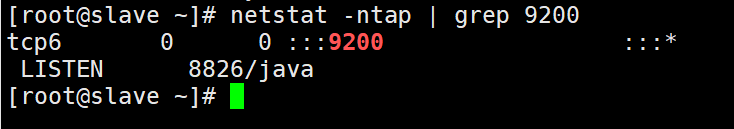
68行 自动发现机制

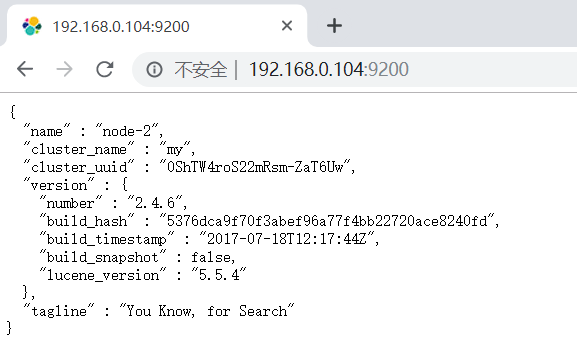
第一个地址填本机的，第二个填主服务器的



启动服务

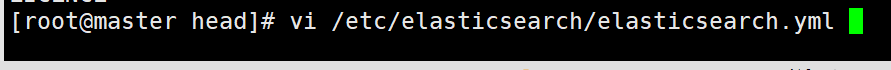


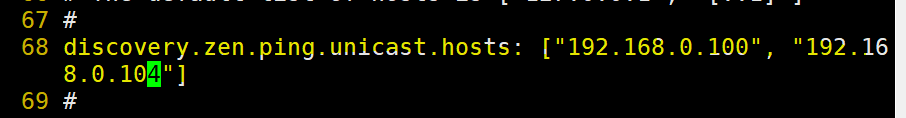




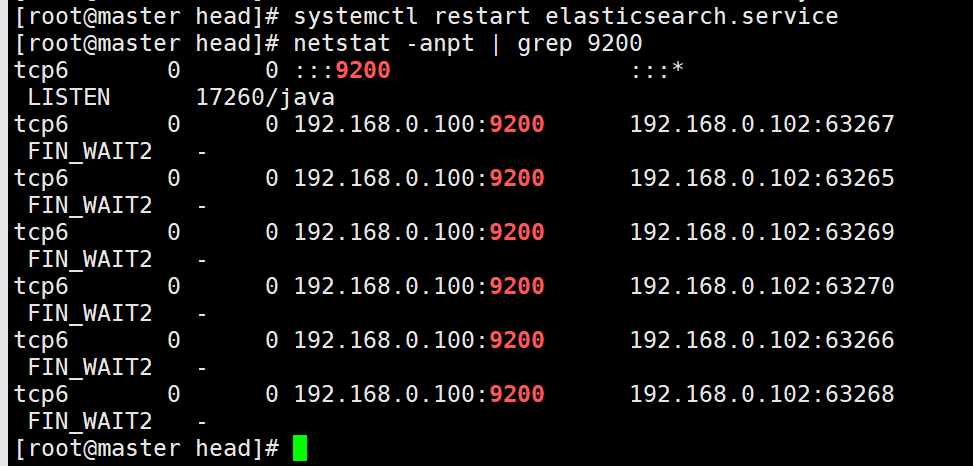
Master

在主服务器里也要修改



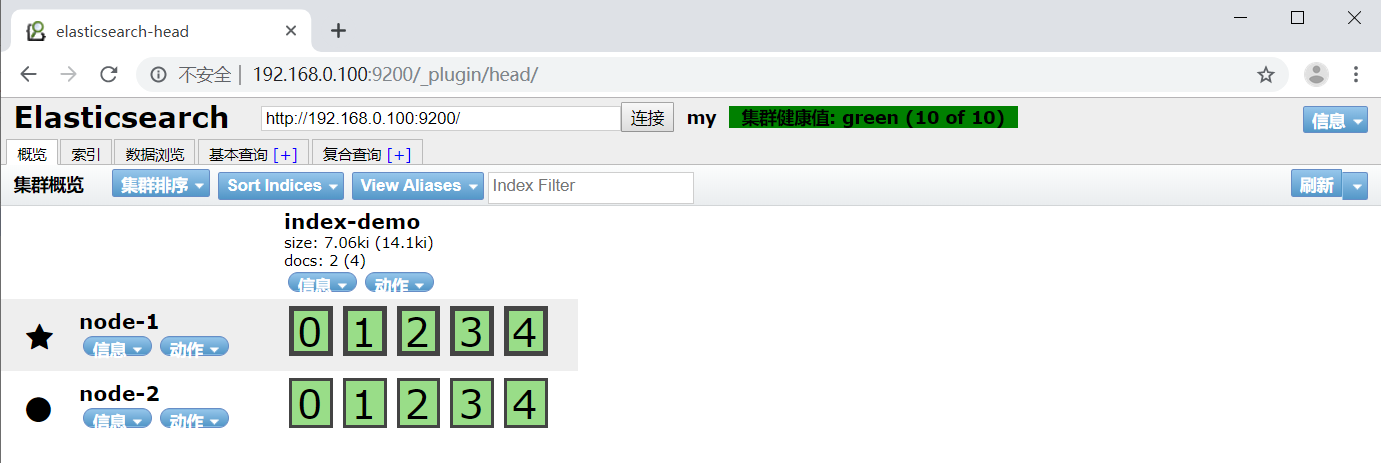


重启服务加查看端口号



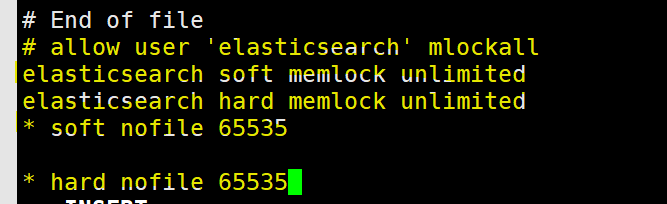
想让主上有星星，就要先重启主服务后再重启从的服务就可以了

测试

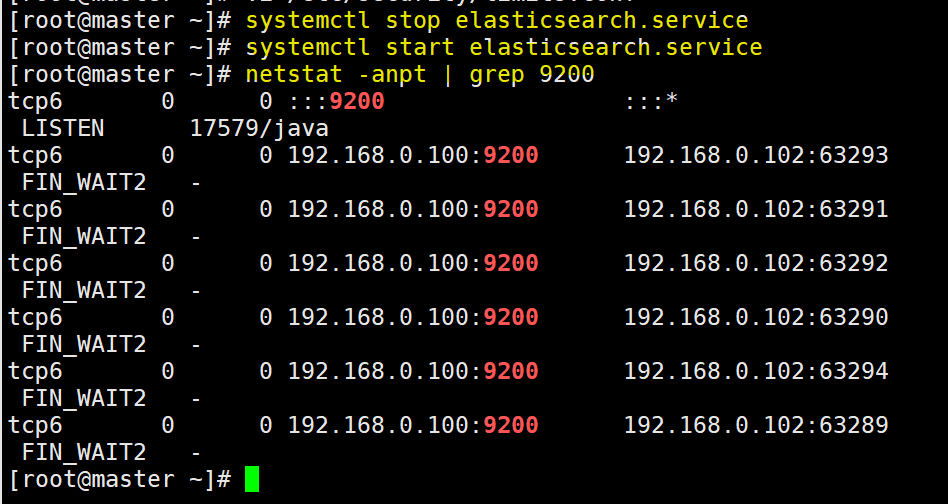


在主服务器里修改配置文件（在末尾添加）

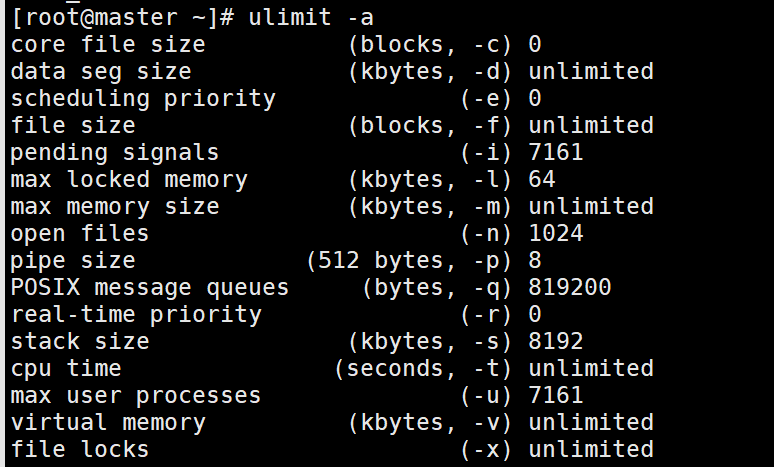




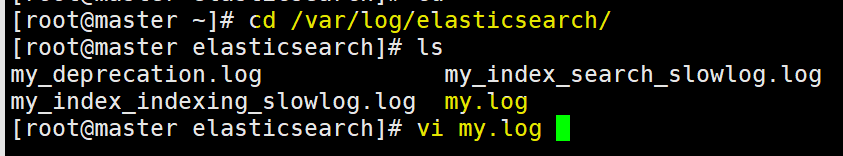
重启服务加查看端口号

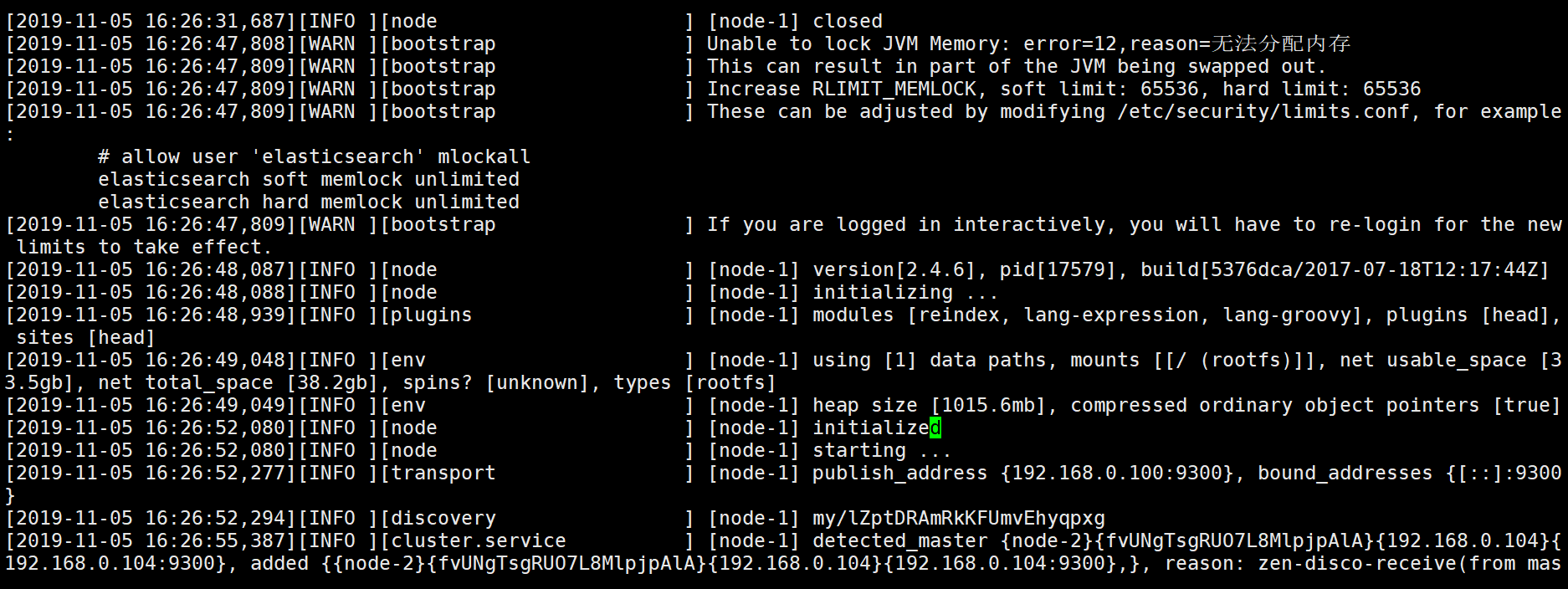


查看一下



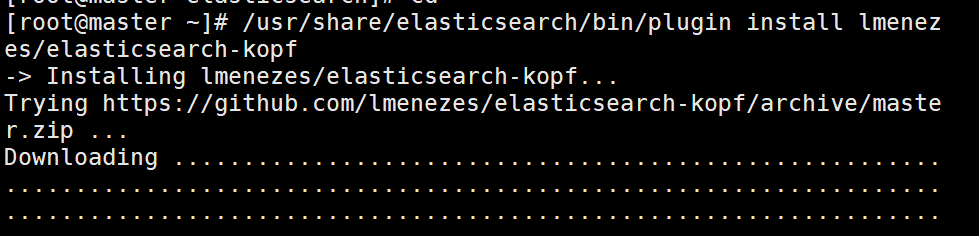
查看日志

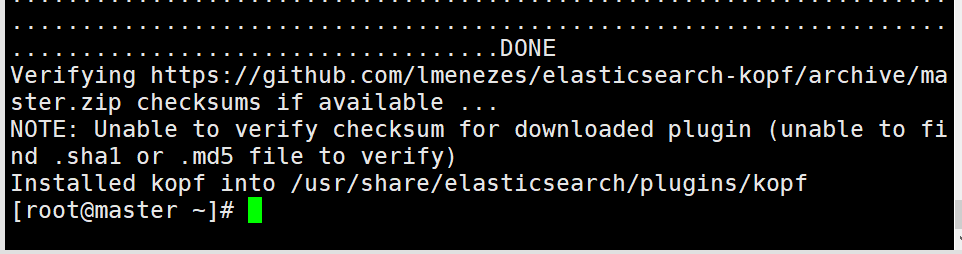




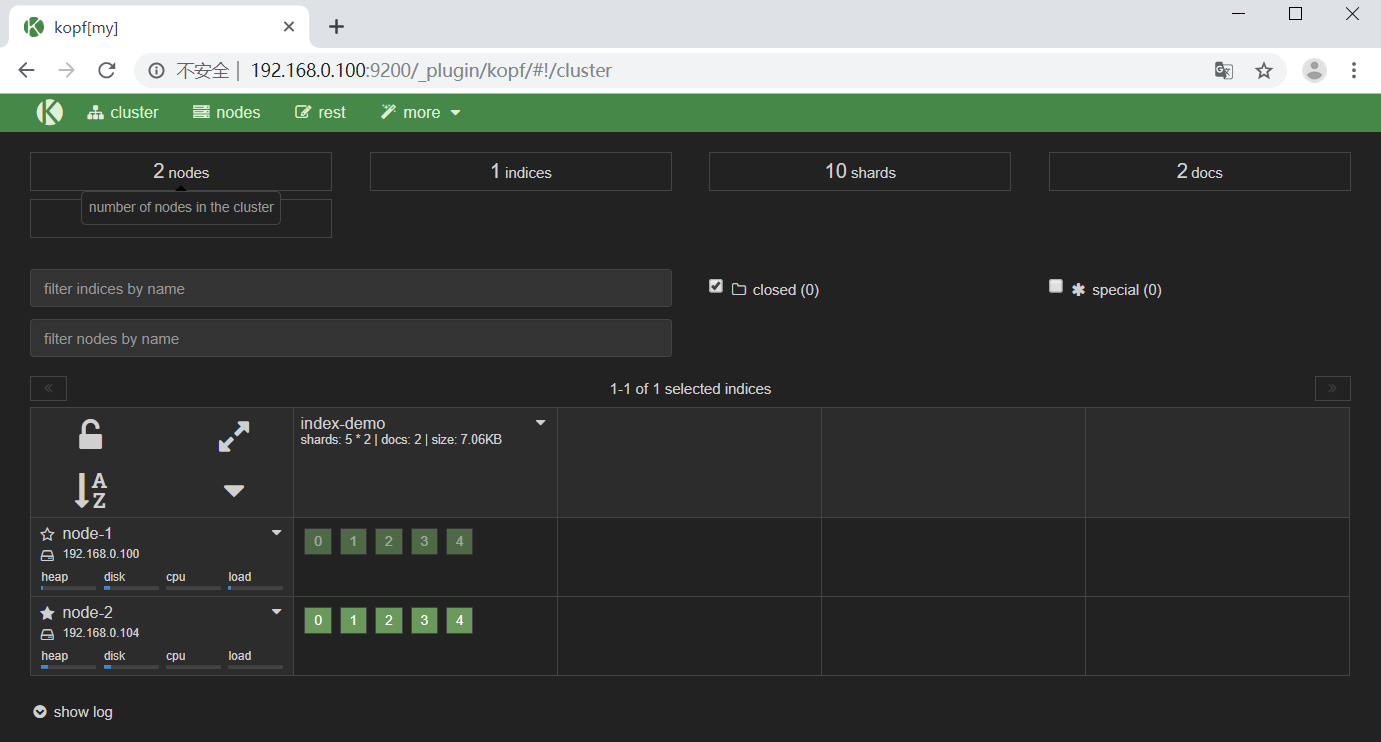
无法分配内存不影响（有其他报错有影响）

安装监控组件

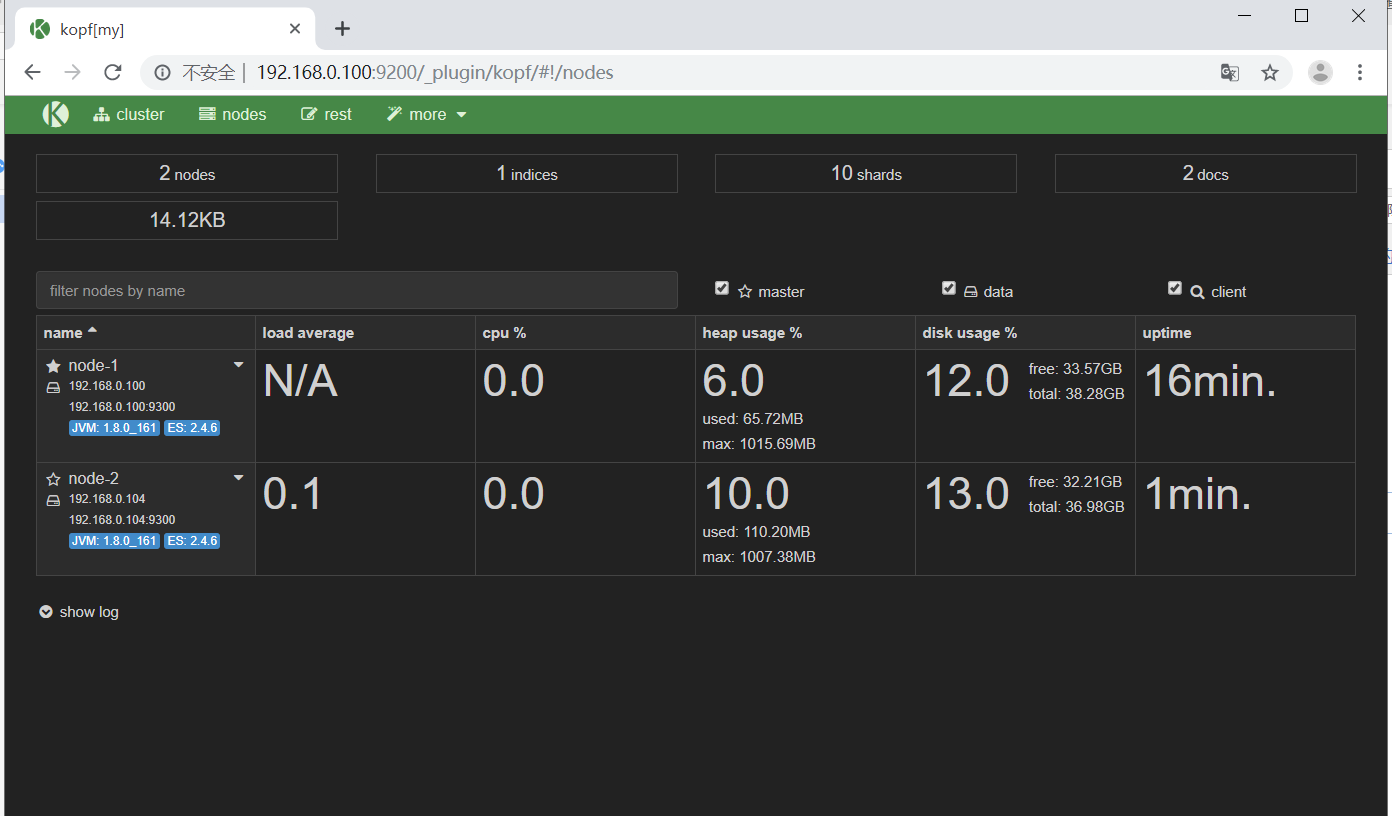




测试

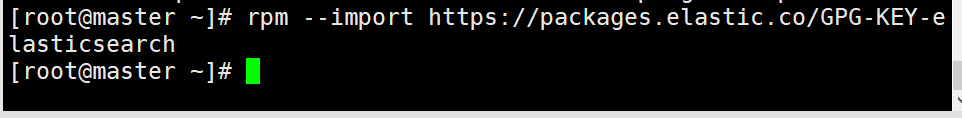


我重启了从服务器的服务，让其主回归node-1

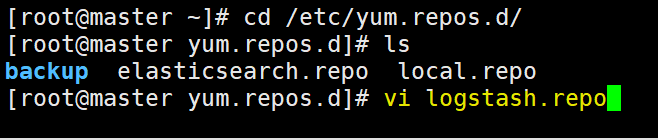


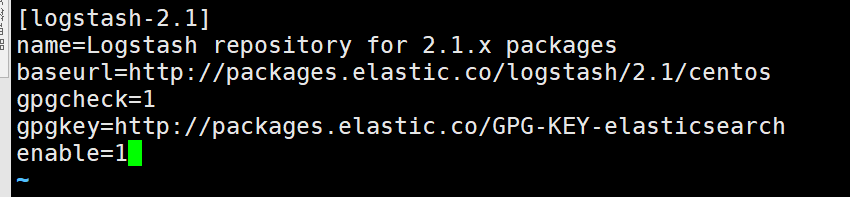
## ES之logstash部署

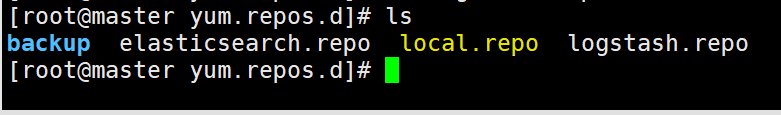
下载密钥



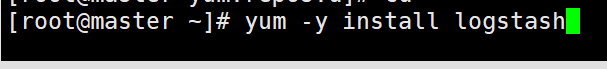
编写一个新的yum仓库

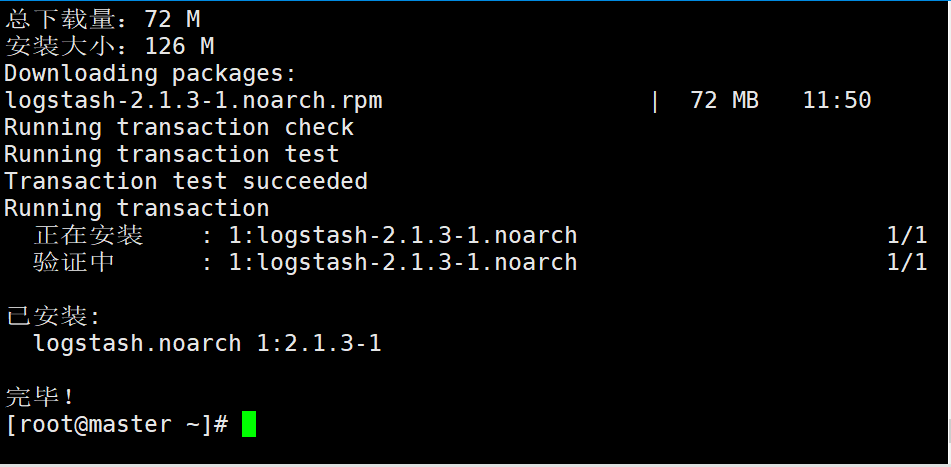




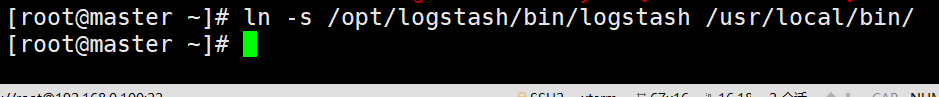


安装日志软件

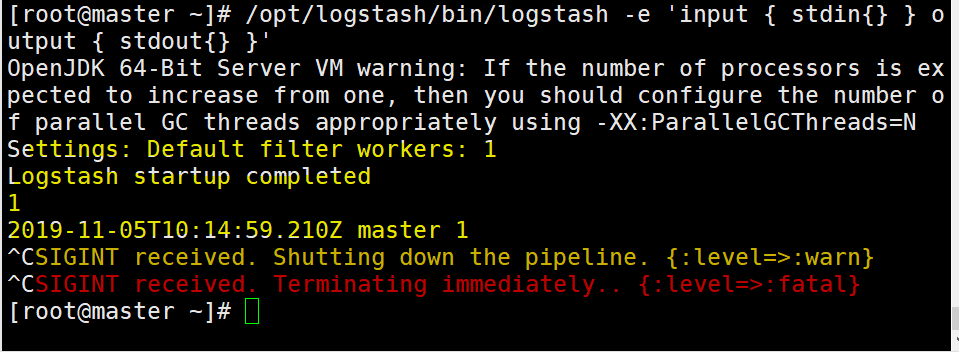




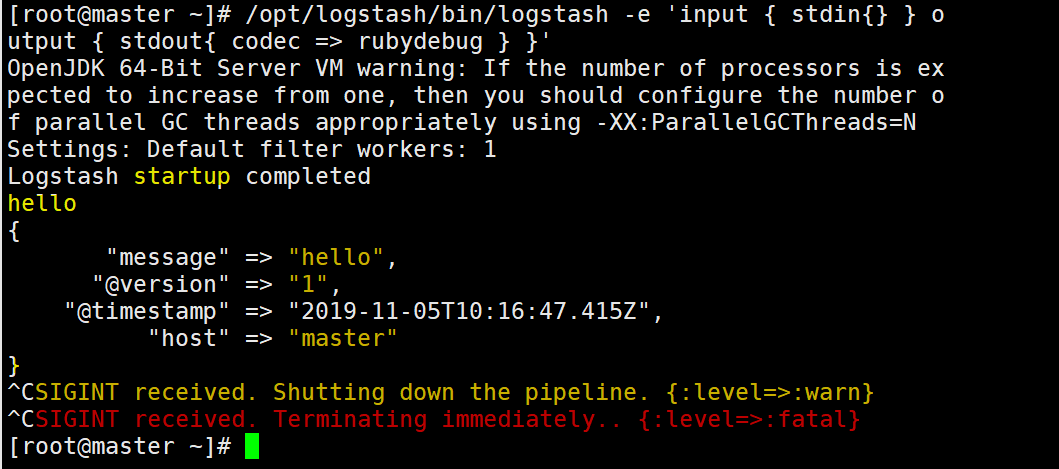
可以做一个软链接（之后就可以就用logstash -e ----）



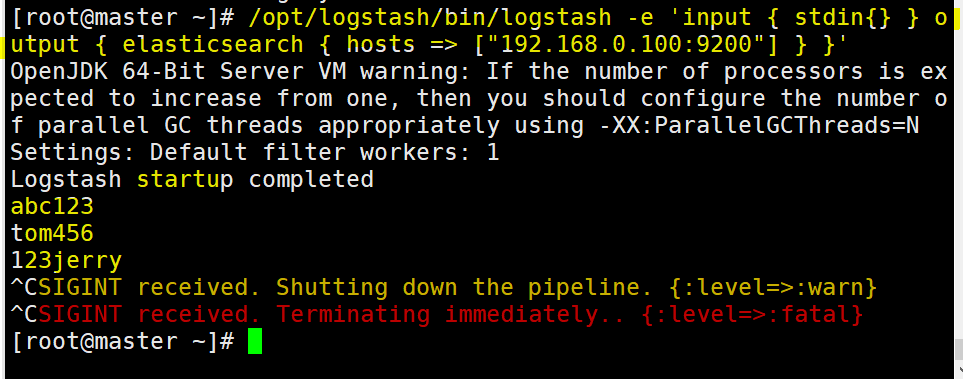
定义输入和输出流，类似管道（先等startup启动，之后开始输入，需要两次ctrl+c才可以退出）



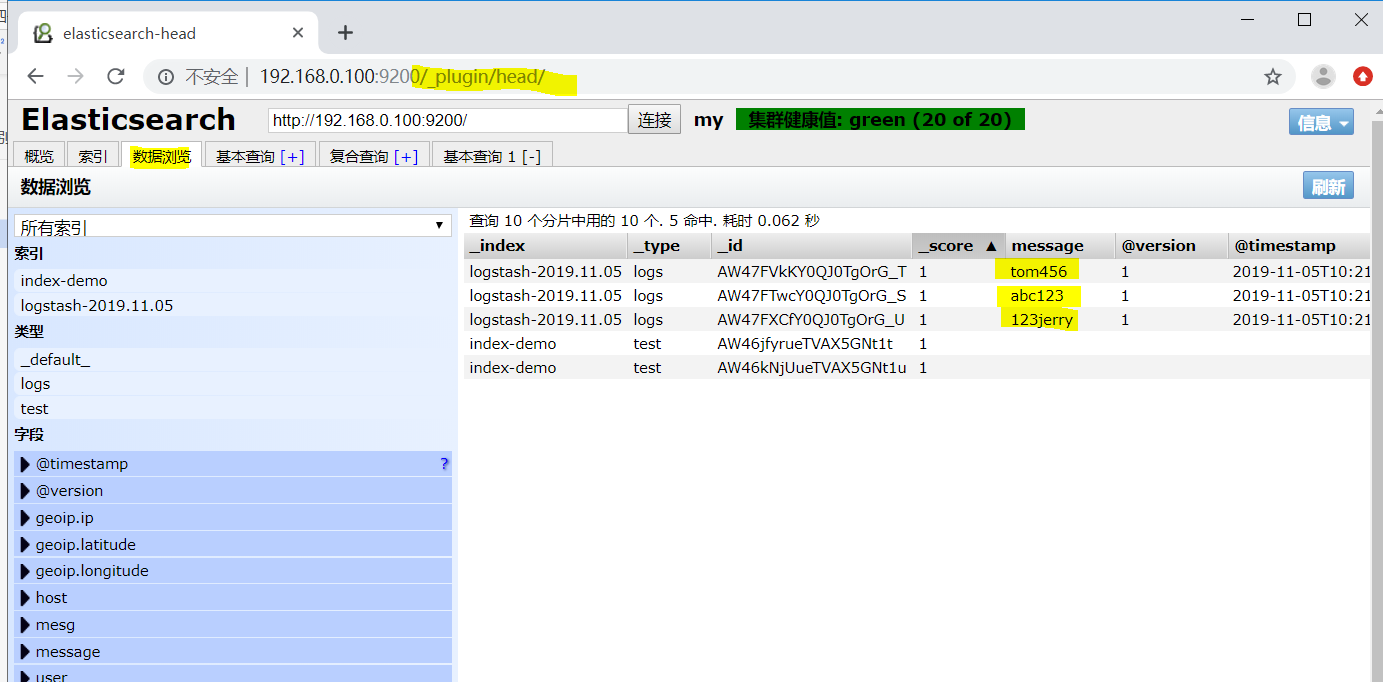
详细格式显示（上面的升级版，格式化了）



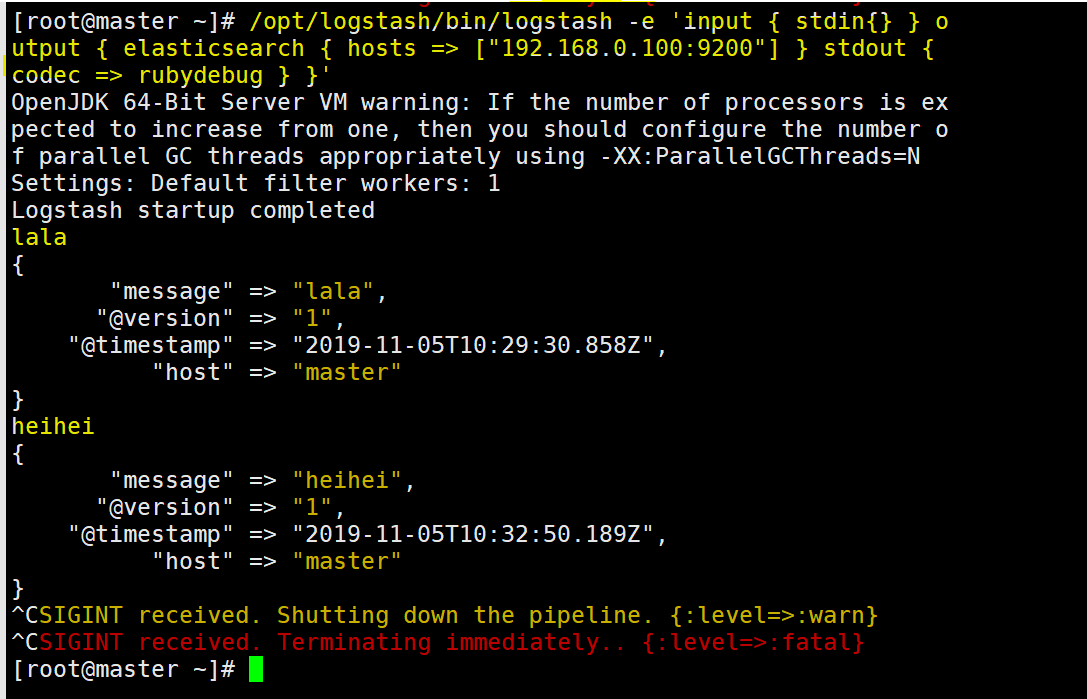
写入到elasticsearch中（把内容写进网页上）



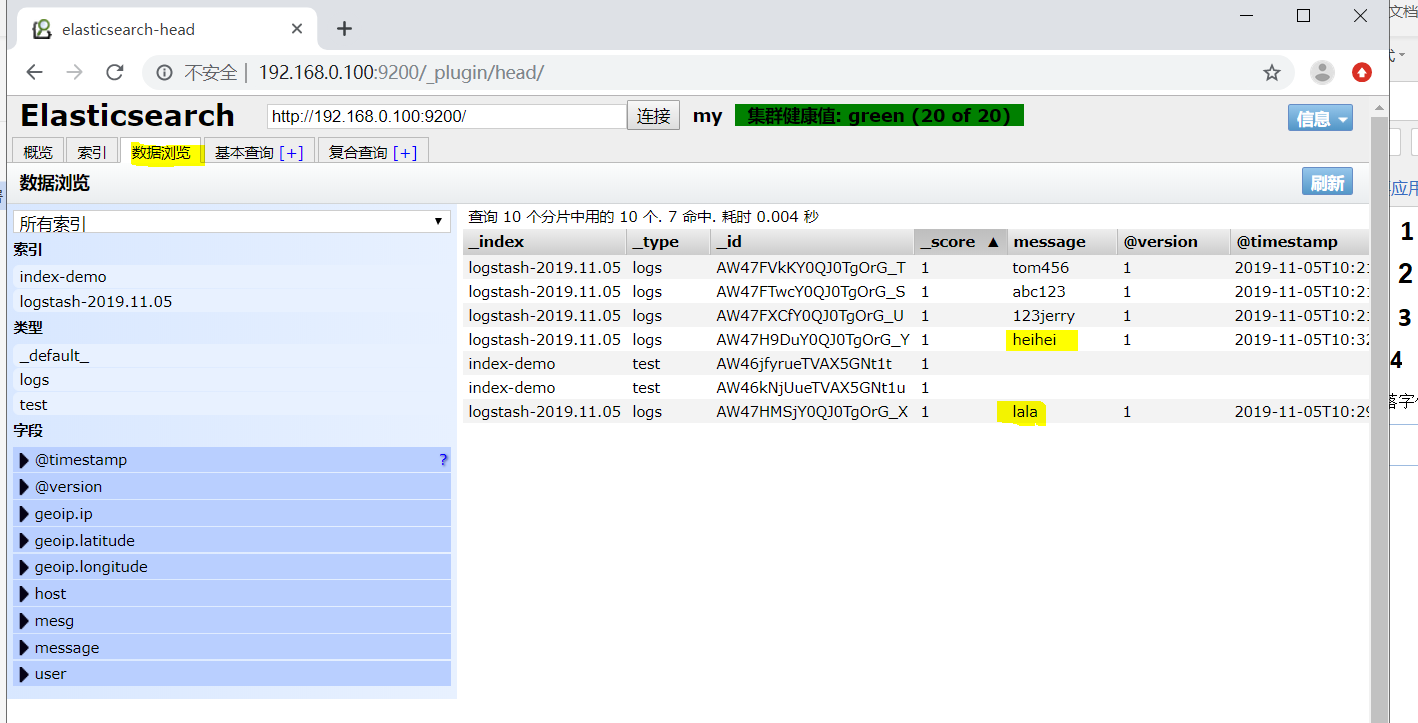
在网页上查看



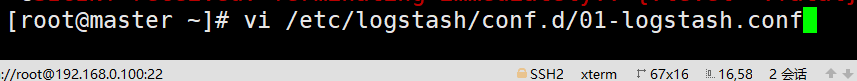
写入ES和同时生成文本（写入网页，也在xshell上生成表格。上面的升级版）

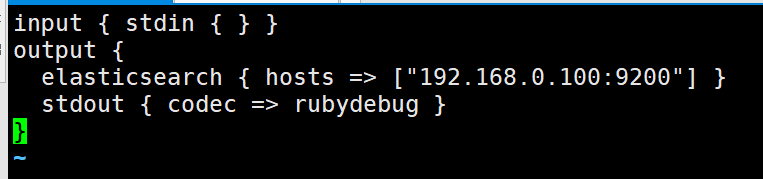


刷新一下网页后

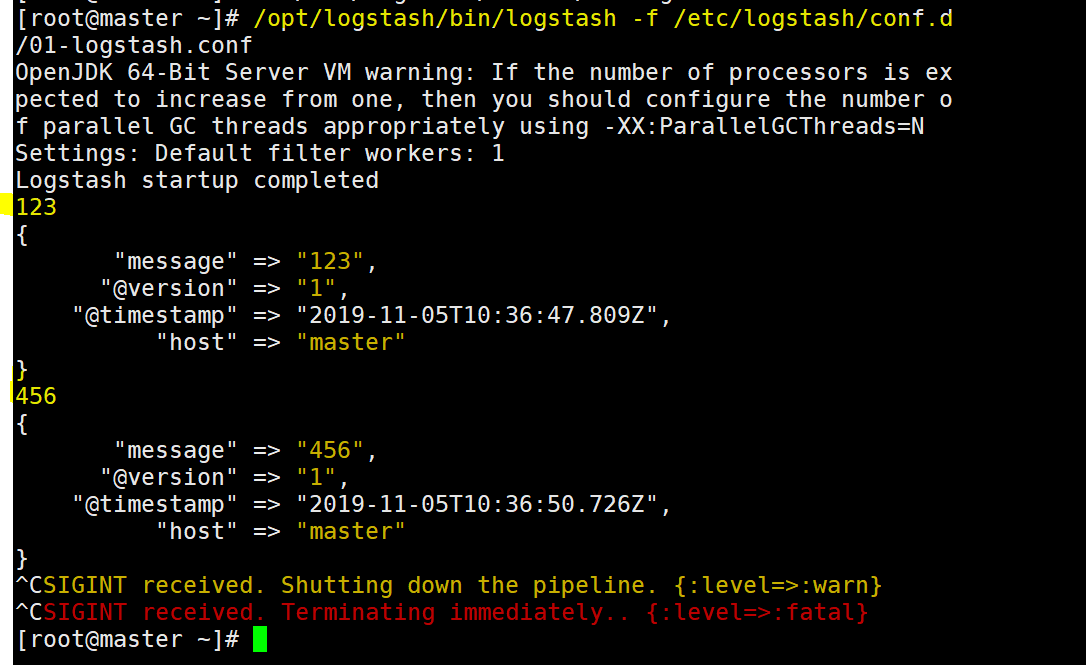


编写一个脚本（写入ES和同时生成文本）

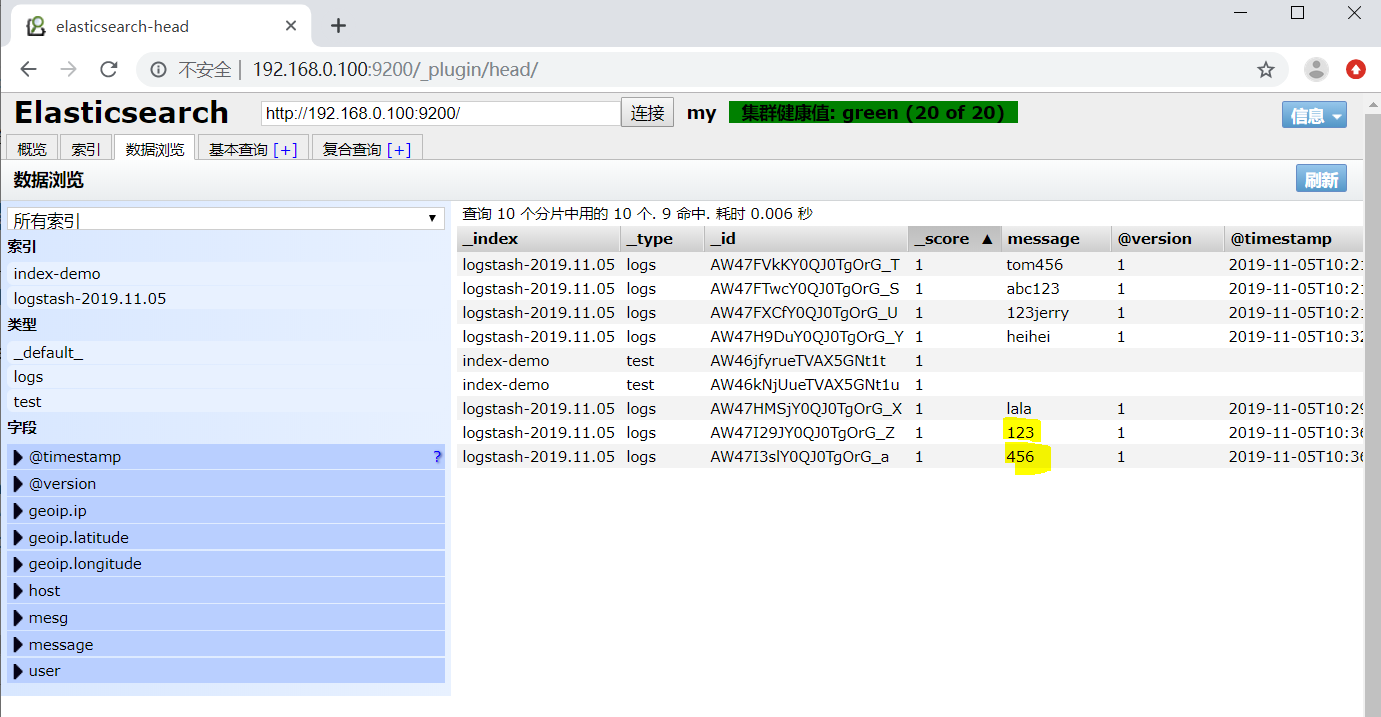




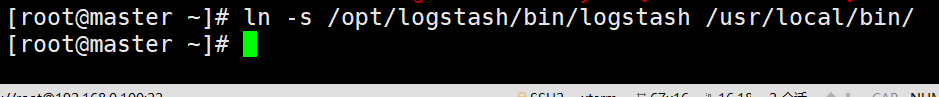
调用刚刚写好的脚本



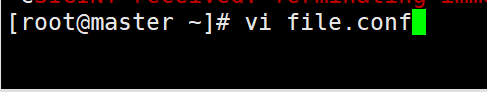
刷新一下网页

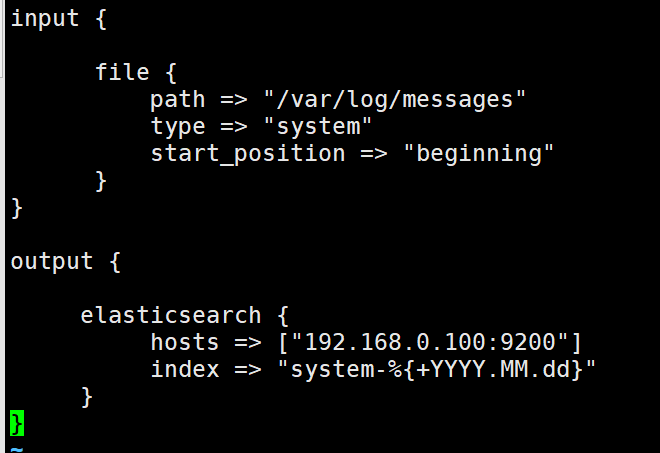


因为先前做过软链接

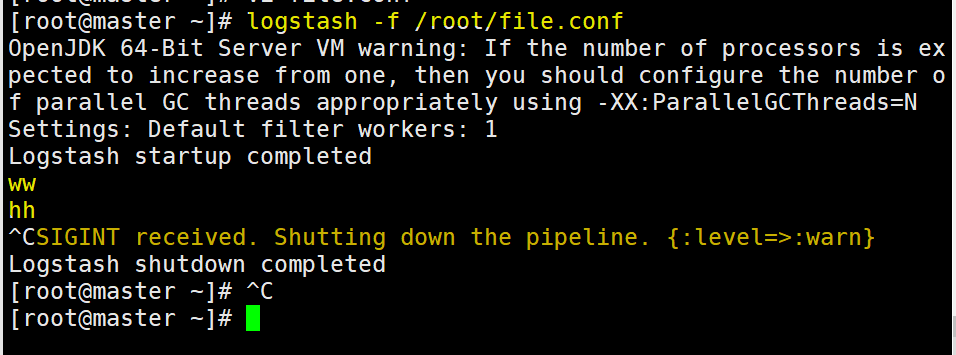


编写一个脚本（logstash收集系统日志）

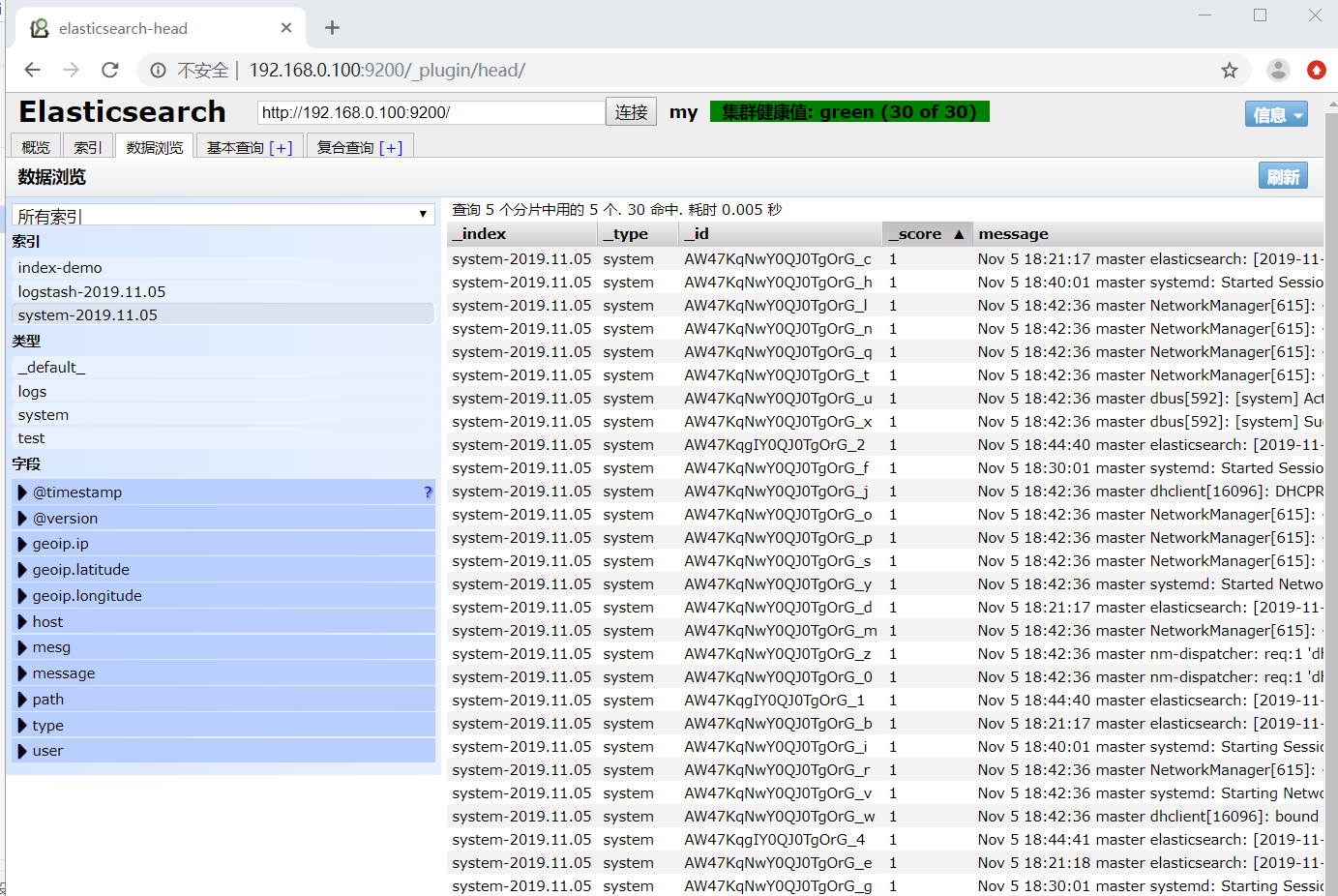




调用刚刚写好的脚本（采集messages日志）



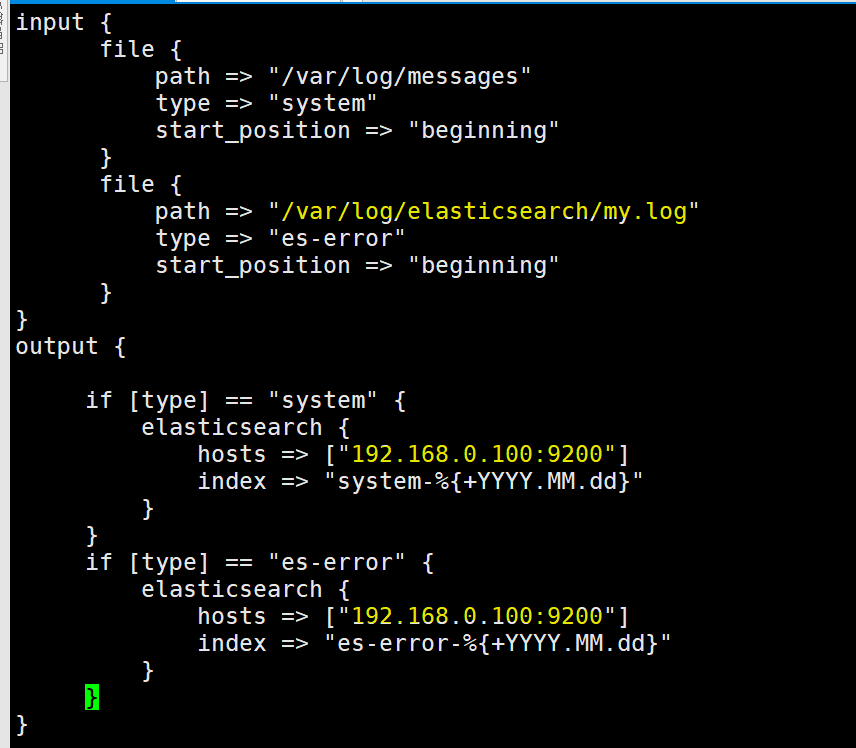
刷新网页看到会有好多内容



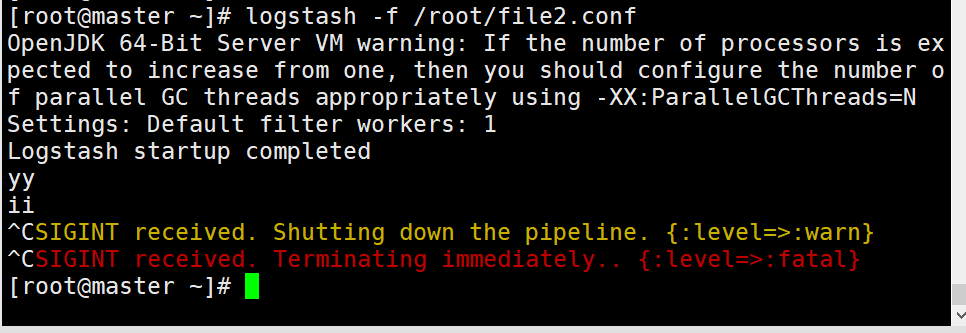
编写一个脚本（监控java系统日志）（收集java异常日志）

日志的路径要对，地址也要对

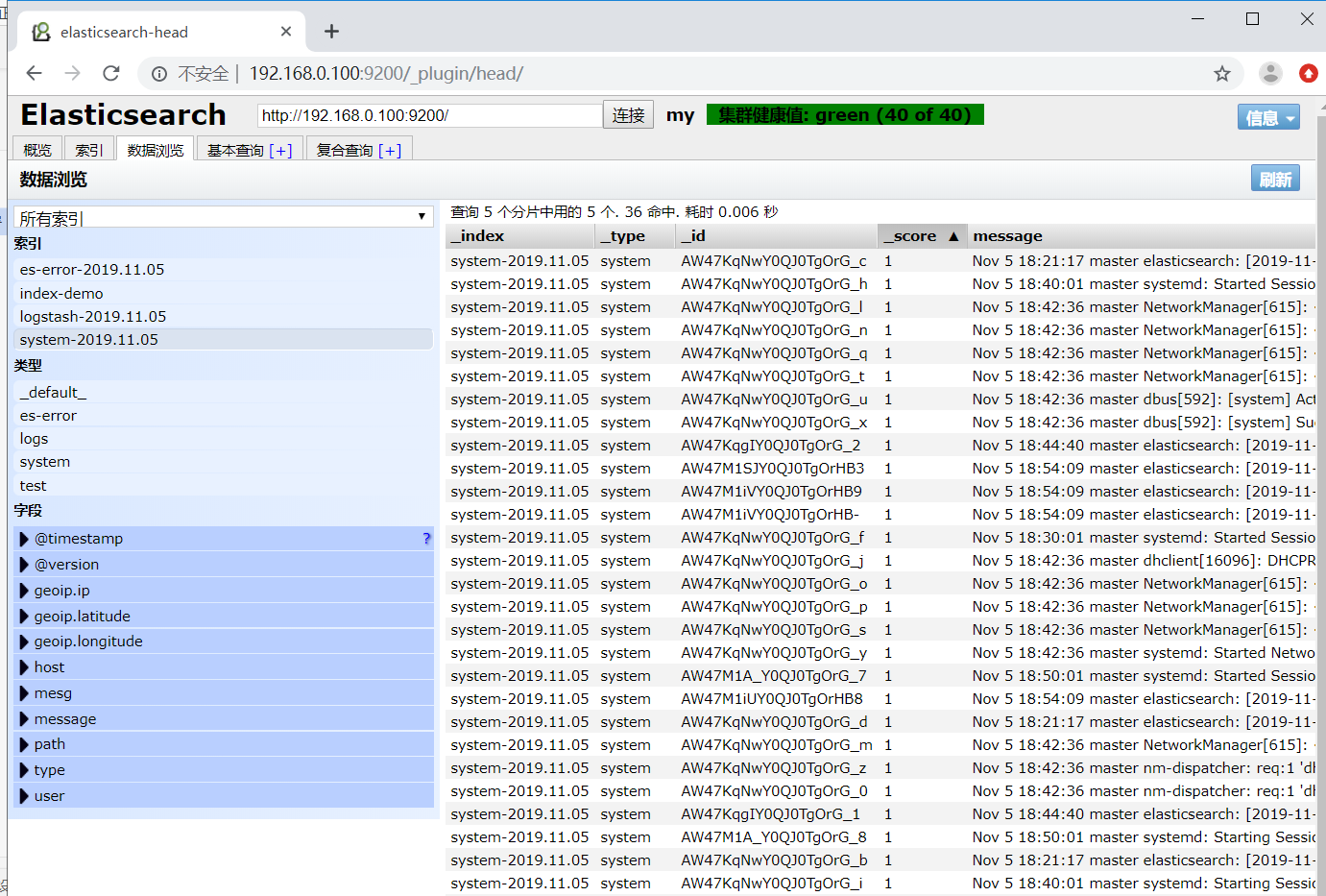




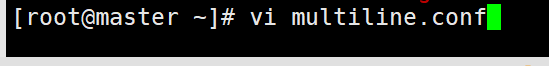
调用编写好的脚本

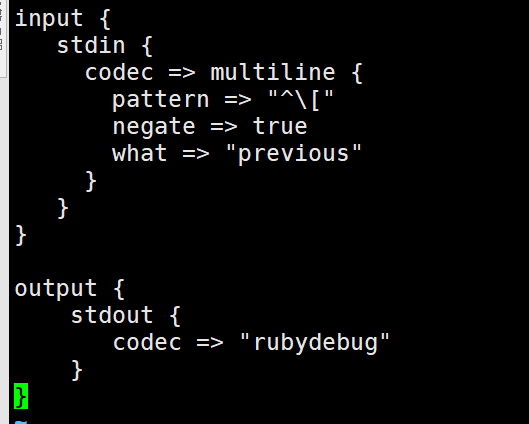


刷新一下网页

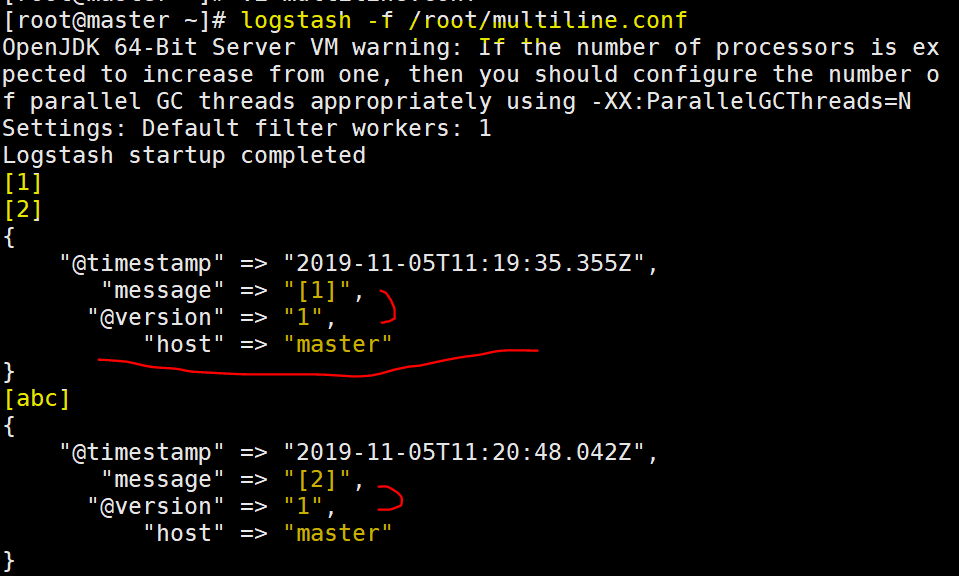


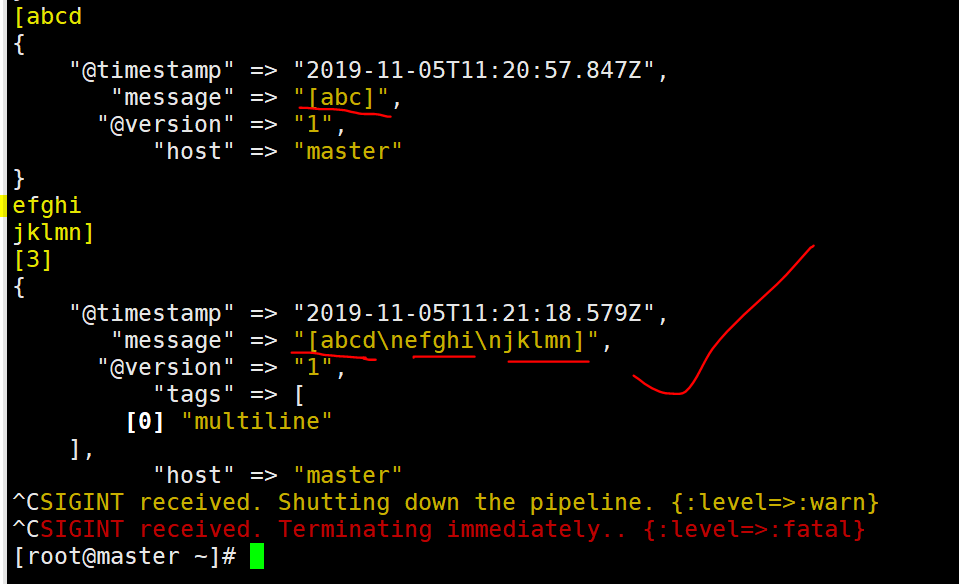
编写一个脚本（事件优化处理，codec插件处理堆栈信息，引用正则表达式）





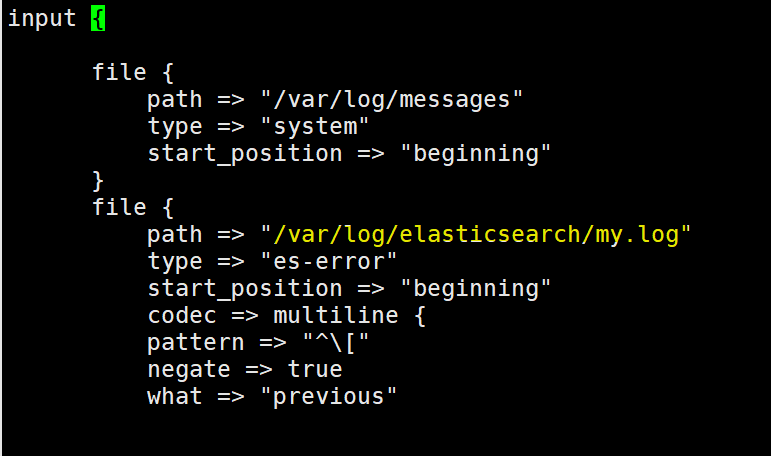
调用刚刚写好的脚本（只出现[]之前的内容）（要一段一段的打）

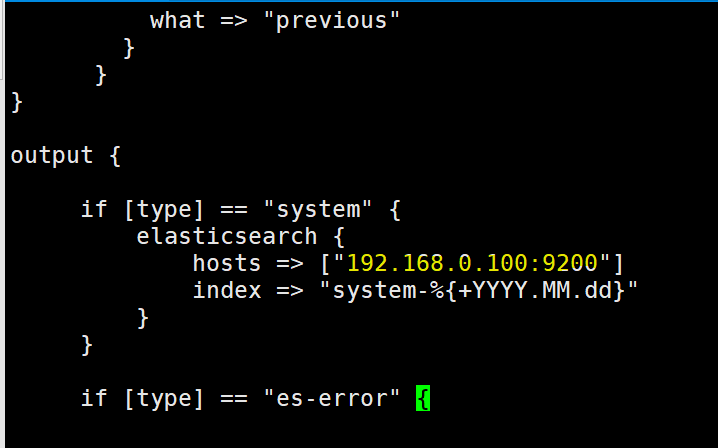


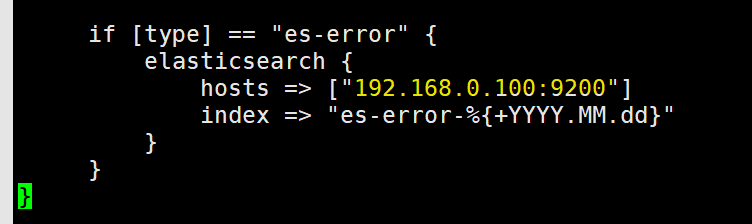


再编写一个脚本（日志要对，还有地址）（重新定义）

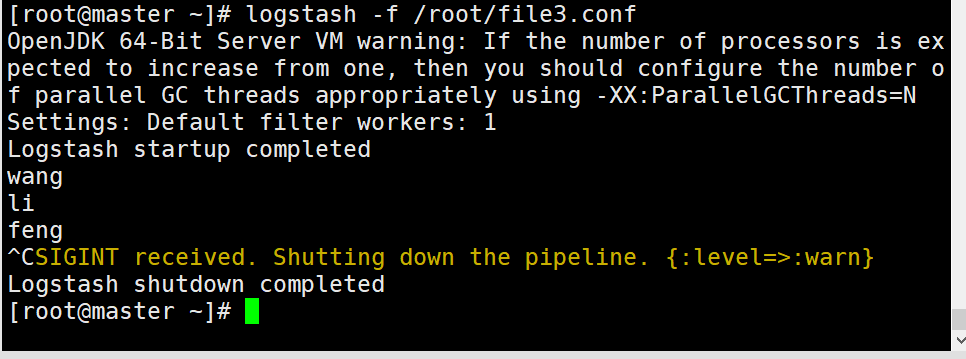




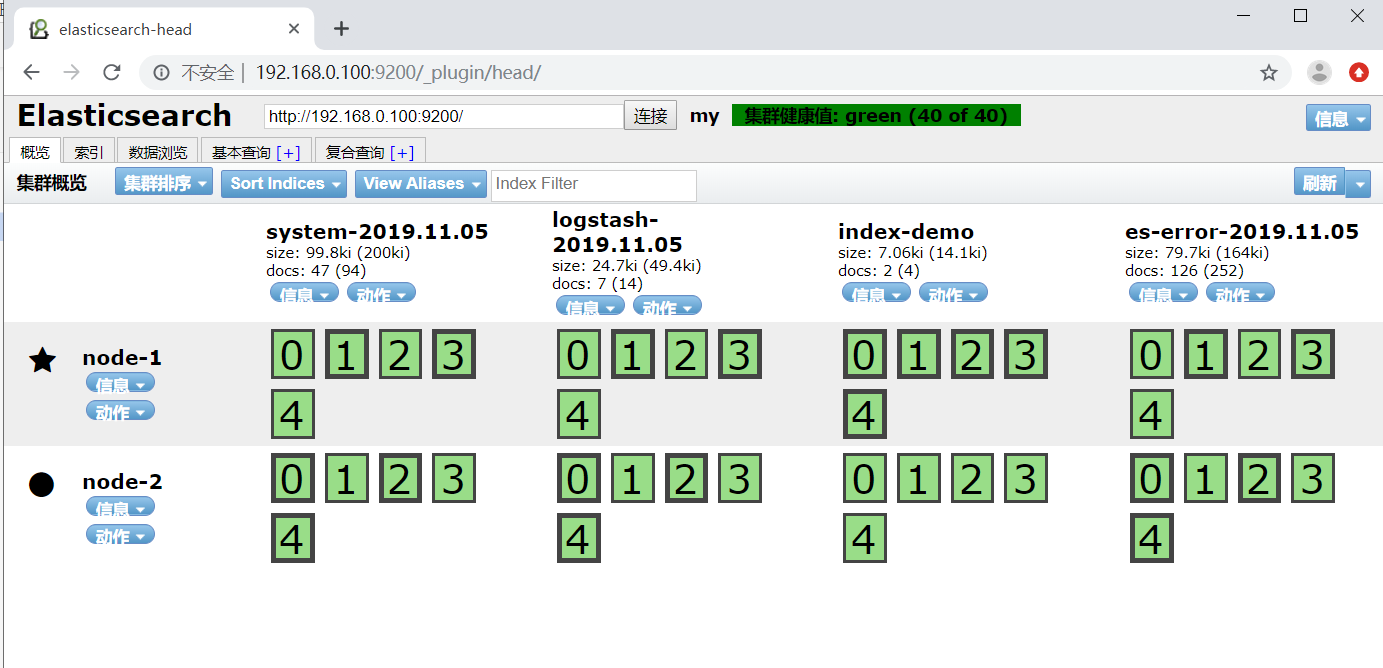


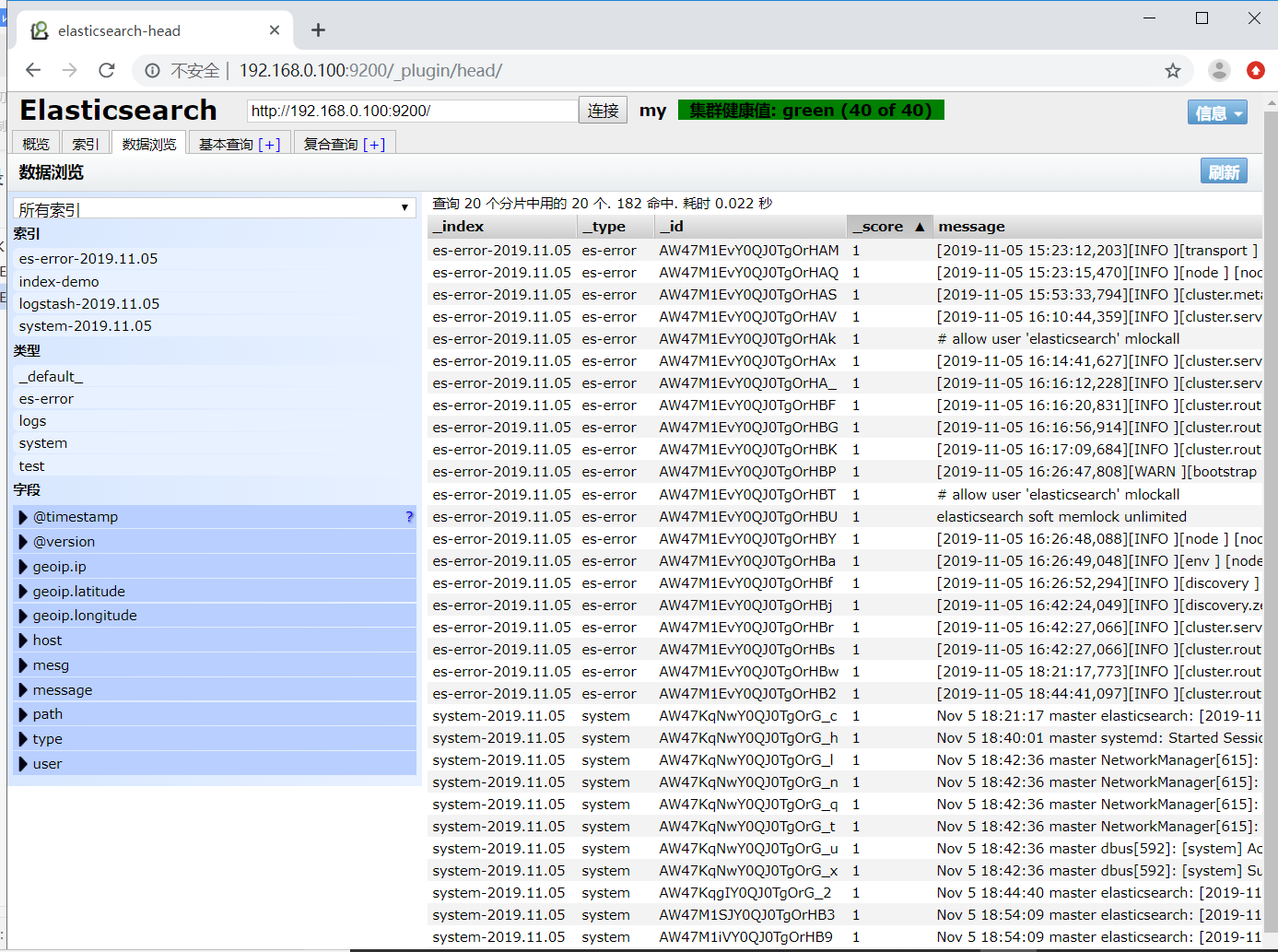


调用刚刚编写好的脚本



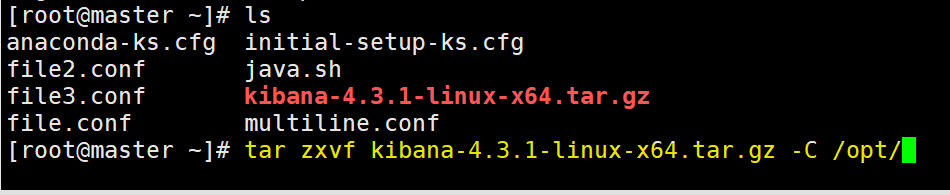
刷新一下网页

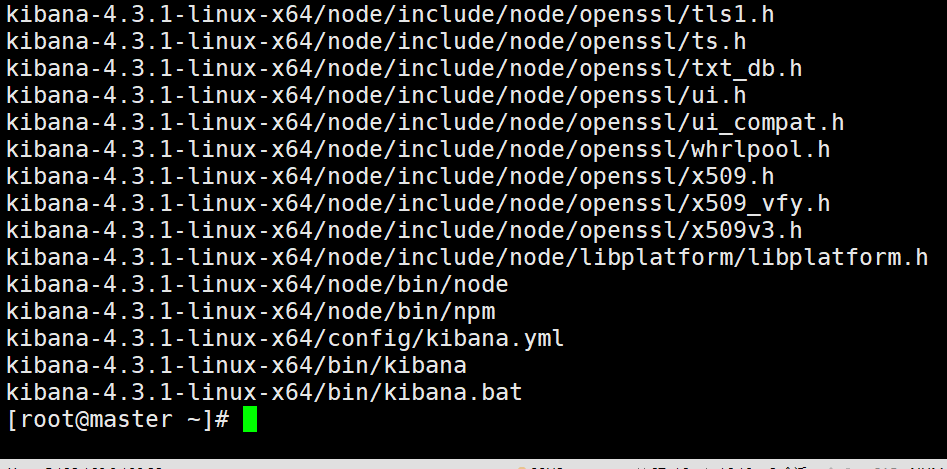




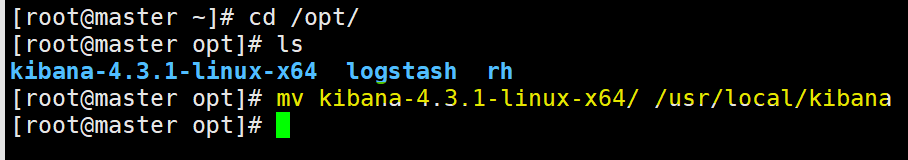
## kibana部署

把文件解压到opt



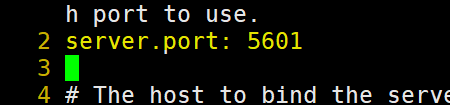


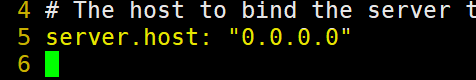
把文件移进系统文件夹里顺便改个名字

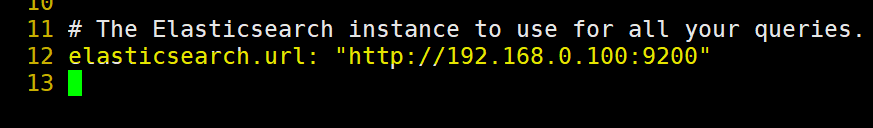


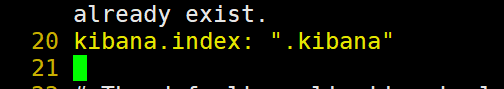
修改配置文件



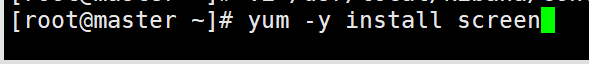


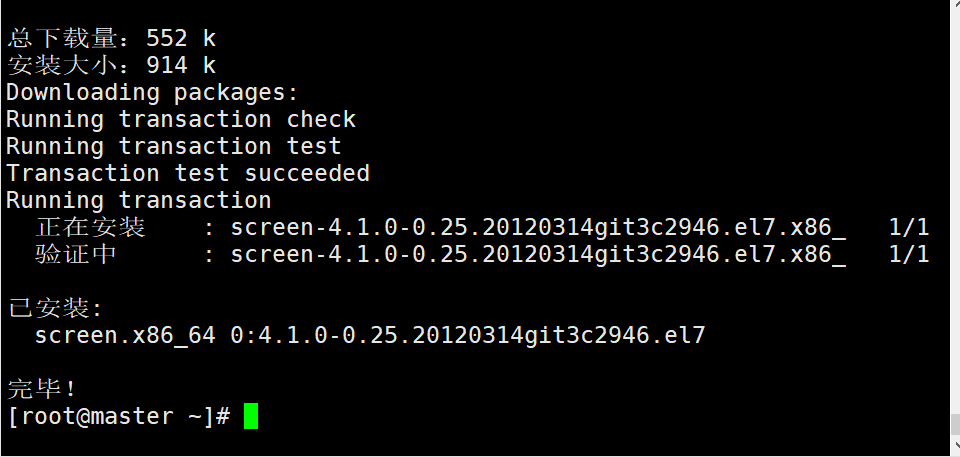




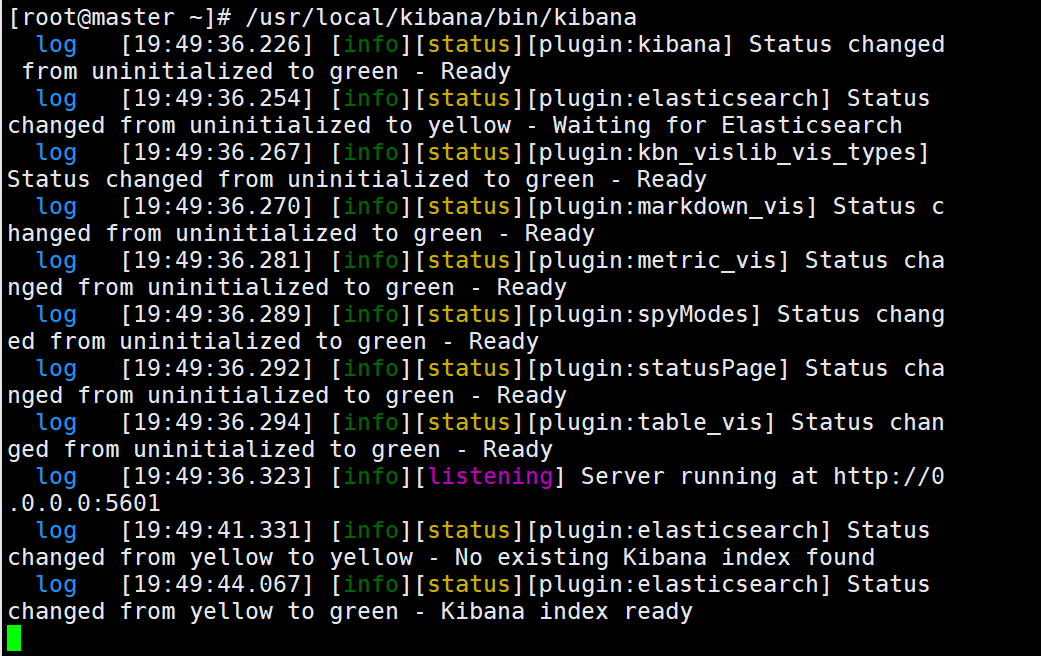


安装分屏软件





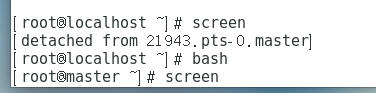
启动监听

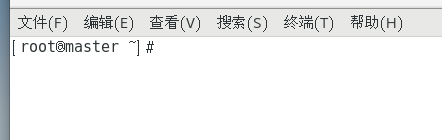


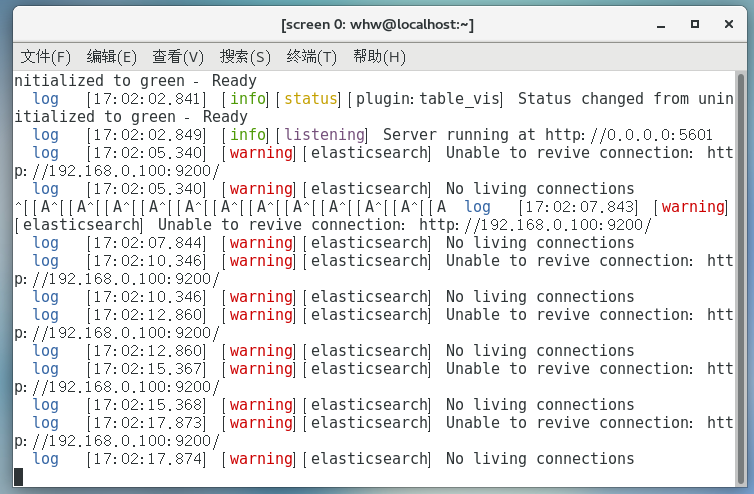
ctrl+a+d 进行丢入后台

丢人后台后就可以不影响其他操作了

先用分屏（到另外一个屏幕里）







之后ctrl+a+d（就可以了）



网页测试

