logstash实验.md

###### 修改解析规则

* **方式一：在已有的解析规则上修改（简单）**
* 在parse\_rule表中修改H3C交换机对应的解析规则，即name为“华三交换机设备syslog日志解析”，修改其对应filter字段的值
* 复制h3c\_parse\_rule.rb文件的内容，粘贴替换filter字段对应的值
* **方式二：新增一种解析规则**
* 需要修改三张表：
* data\_source
* data\_source\_conf
* parse\_rule
* 修改步骤可参考文件sql\_syslog采集.txt

###### 在页面配置新建syslog采集任务

###### 修改logstash配置文件的参数

* 由于logstash默认jvm堆内存只有1G，规则文件较大会导致溢出，所以需要修改jvm的堆内存(经过实验，logstash6.5.1至少需要5G的堆内存)
* 进入采集任务对应的pod，去/usr/local/logstash-6.5.1/config/jvm.options文件中修改堆内存：
* 把其中的
* -Xms1g
    
  -Xmx1g
* 修改为
* -Xms6g
    
  -Xmx6g

###### 重启pod，使配置生效

* 找到pod对应的容器
* docker ps | grep pod的名字
* 然后重启该容器
* docker restart docker容器名字
* 例如：
* [root@dj ~]# docker ps | grep itoa-task-rc-9d6f5f1b-c866-4f3c-9e19-1c3db951dc30-6gj2t
    
  e536cacca519 matrix-registry.h3c.com:8088/itoa/itoa-task-common "/opt/start\_tasks.sh…" 2 days ago Up 2 days k8s\_itoa-task-rc-9d6f5f1b-c866-4f3c-9e19-1c3db951dc30\_itoa-task-rc-9d6f5f1b-c866-4f3c-9e19-1c3db951dc30-6gj2t\_itoa\_f47d0669-ed15-4aaa-896b-a1b11e9d9809\_0
    
  1088e70ba947 matrix-registry.h3c.com:8088/matrix/pause:3.1 "/pause" 2 days ago Up 2 days k8s\_POD\_itoa-task-rc-9d6f5f1b-c866-4f3c-9e19-1c3db951dc30-6gj2t\_itoa\_f47d0669-ed15-4aaa-896b-a1b11e9d9809\_0
    
  [root@dj ~]# docker restart e536cacca519
    
  e536cacca519

###### 查看pod日志

* kubectl logs -f itoa-task-rc-9d6f5f1b-c866-4f3c-9e19-1c3db951dc30-6gj2t -nitoa
* 看到类似这一行打印信息，表示启动成功:
* [2020-07-24T18:29:20,970][INFO ][logstash.agent ] Successfully started Logstash API endpoint {:port=>9600}
* 从pod的日志中可以查看logstash从启动到启动成功所耗费的时间