链滴

ELK 日志系统环境搭建

作者：zorkelvll

原文链接：https://ld246.com/article/1553062503110

来源网站：链滴

ZERO

    　　持续更新 请关注：https://zorkelvll.cn/blogs/zorkelvll/articles/2019/03/20/1553062484473

背景

    近期由于项目需求，
要建立一套日志聚合系统，采用经典的ELK(logstash =》elasticsearch =》kibana)日志系统架构，
文则是记录相关elasticsearch\logstash\kibana\filebeat等环境的安装过程!

说明：

- 数据流走向：filebeat => logstash => elasticsearch => kibana
- 组件启动顺序：elasticsearch => logstash => kibana (ELK名称的来源？) => filebeat
- elasticsearch-6.6.1 logstash-6.6.2 kibana-6.6.2 filebeat-6.6.2

下载

    在
lk官网下载安装包logstash\elasticsearch\kibana 以及filebeats，其中elasticsearch的下载以及安装程可参见ElasticSearch 环境搭建

cd /usr/local #root用户

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-6.6.2.tar.gz
wget https://artifacts.elastic.co/downloads/kibana/kibana-6.6.2-linux-x86_64.tar.gz
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.6.2-linux-x86_64.tar.gz

tar -zxvf logstash-6.6.2.tar.gz
chown es:es /usr/local/logstash-6.6.2/ -R

tar -zxvf kibana-6.6.2-linux-x86_64.tar.gz
chown es:es /usr/local/kibana-6.6.2-linux-x86_64/ -R

tar -zxvf filebeat-6.6.2-linux-x86_64.tar.gz
chown es:es /usr/local/filebeat-6.6.2-linux-x86_64/ -R
```

配置

elasticserach

  可参见 ElasticSearch 环境搭建

logstash

```
cd /usr/local/logstash-6.6.2 #es用户
vim default.conf #创建default.conf文件并添加内容：

# 监听5044端口作为输入
input {
    beats {
        port => "5044"
    }
}
# 数据过滤
filter {
    grok {
        match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
    geoip { source => "clientip" }
}
# 输出配置为本机的9200端口，这是ElasticSerach服务的监听端口
output {
    elasticsearch {
        hosts => ["127.0.0.1:9200"]
    }
}
```

kibana

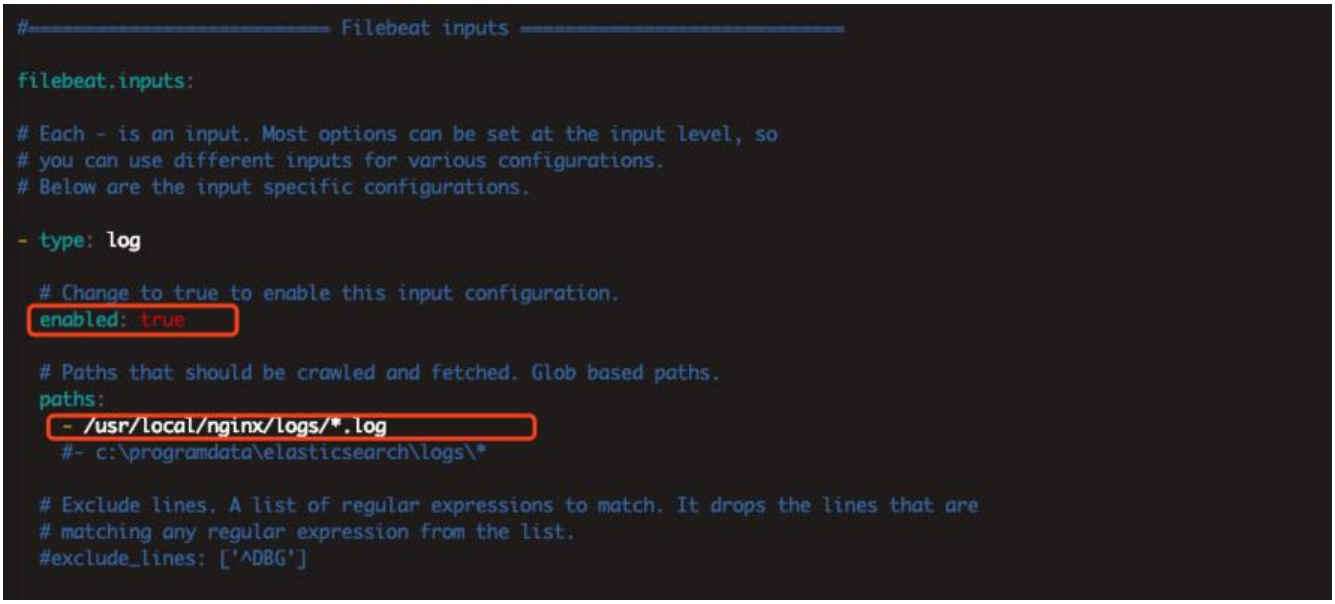
```
cd /usr/local/kibana-6.6.2-linux-x86_64 #es用户
vim config/kibana.yml # 将server.host配置项取消注释并修改(若修改为局域网ip地址则内网访问，处设为0位可外网访问)为server.host:"0.0.0.0"
```

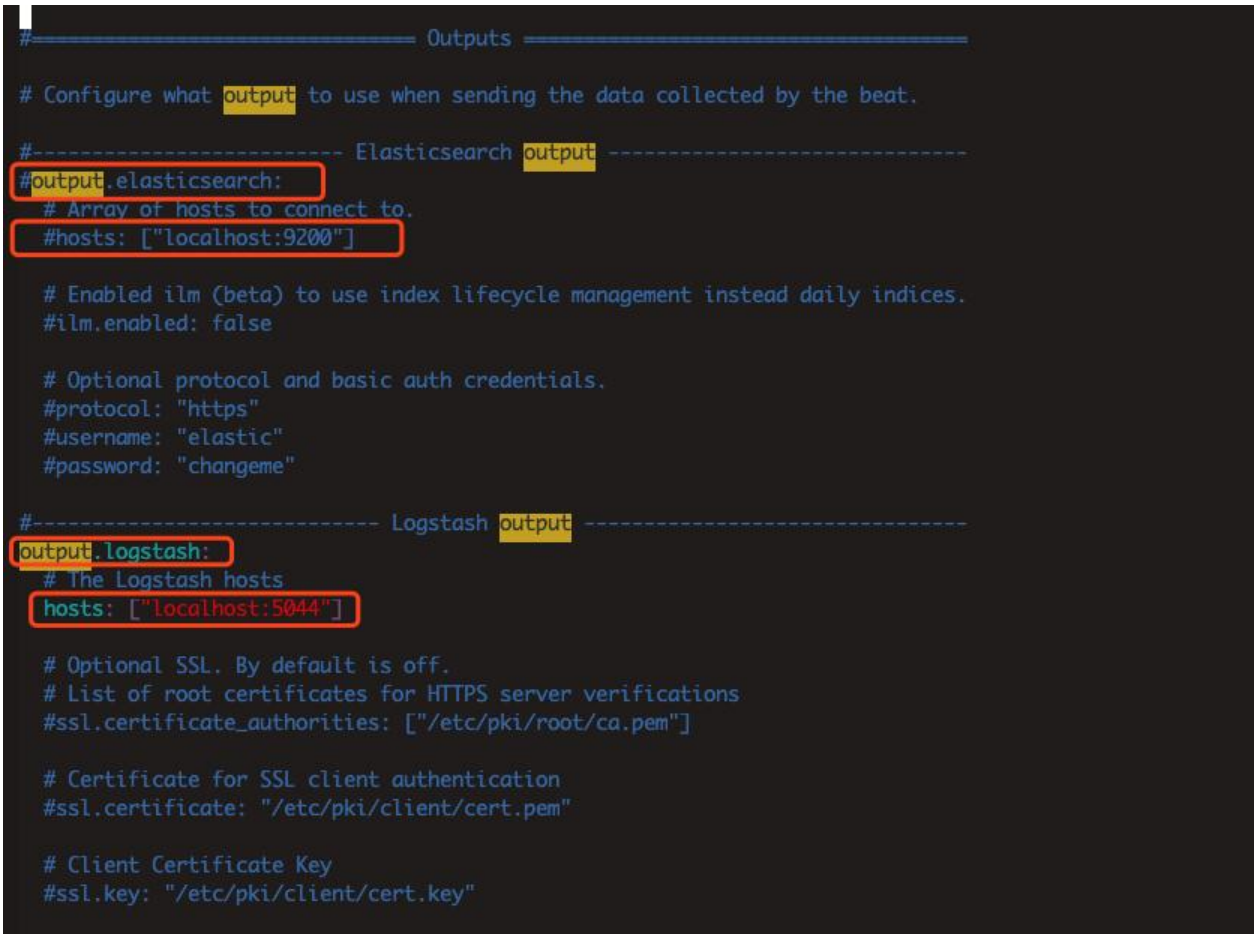
filebeat

cd /usr/local/filebeat-6.6.2-linux-x86_64 #es用户

vim filebeat.yml #配置日志以及日志文件路径（配置如截图，且需要保证es用户具有访问该log目的权限），如nginx日志为例

vim filebeat.yml #配置elasticsearch日志输出地址或者logstash输出地址，在这里我们将采用filebea先收集日志到logstash中，然后由logstash再到elasticsearch中，因此注释掉默认的elasticsearch地并取消默认注释的logstash地址（配置如截图）





启动

elasticserach

  可参见 ElasticSearch 环境搭建

logstash

cd /usr/local/logstash-6.6.2 #es用户
nohup bin/logstash -f default.conf --config.reload.automatic & #以后台进程形式启动logstash
务
tail -f nohup.out #查看启动日志（或者先以bin/logstash -f default.conf -config.reload.automati
命令启动在控台打印启动日志确定可以成功关闭后再以后台形式启动）

kibana

cd /usr/local/kibana-6.6.2-linux-x86_64 #es用户
nohup bin/kibana & #以后台进程形式启动kibana服务
tail -f nohup.out #查看启动日志（或者先以bin/kibana命令启动在控台打印启动日志确定可以成功
闭后再以后台形式启动）
浏览器中访问 http://ip:5601 #可以访问页面成功，则kibana启动成功

kibana关闭：

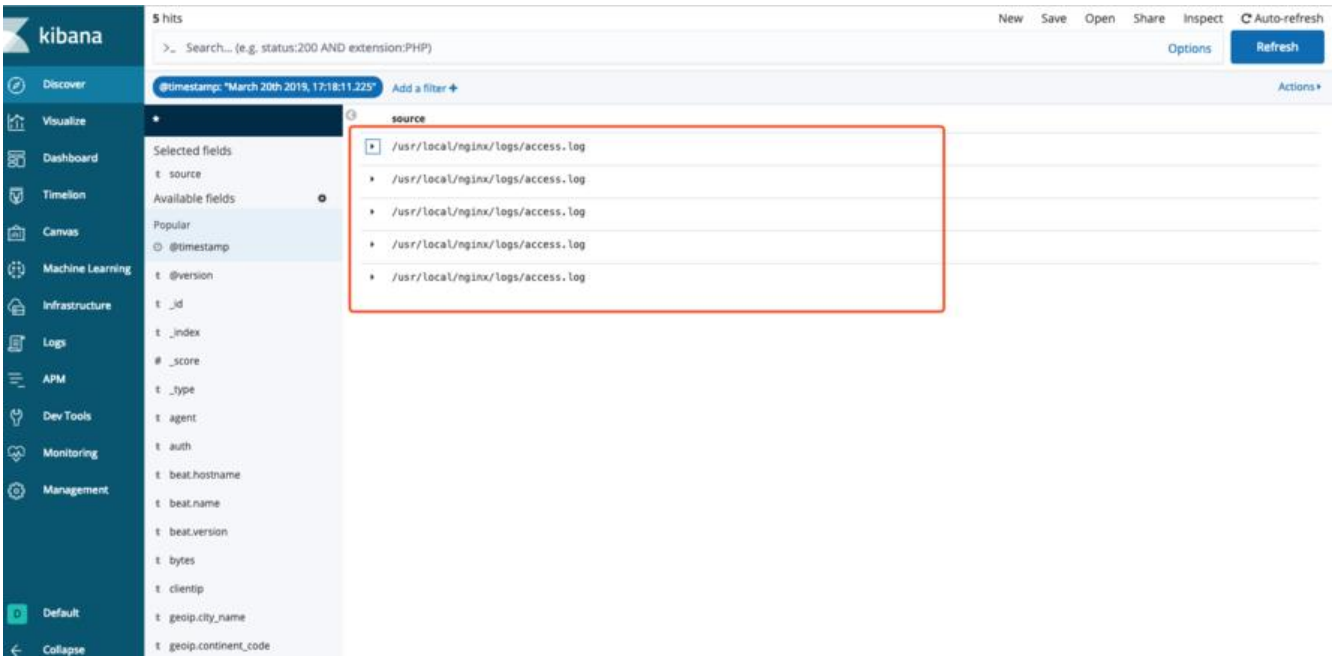
```
[es@aokayTech kibana-6.6.2-linux-x86_64]$ ps -ef | grep node
es         310 32750  0 17:32 pts/4    00:00:00 grep --color=auto node
es       29775     1  1 16:14 ?        00:00:52 bin/../node/bin/node --no-warnings --max-http-header-size=65536 bin/../src/cli
```

filebeat

cd /usr/local/filebeat-6.6.2-linux-x86_64 #es用户
nohup ./filebeat -e -c filebeat.yml -d "publish" & #以后台进程形式启动filebeat服务
tail -f nohup.out #查看启动日志（或者先以./filebeat -e -c filebeat.yml -d "publish"命令启动在台打印启动日志确定可以成功关闭后再以后台形式启动）

确认kibana中是否存在nginx的日志

浏览器中访问 http://ip:5601 #查看kibana中是否有nginx日志存在



TODO:

- Kibana界面汉化

