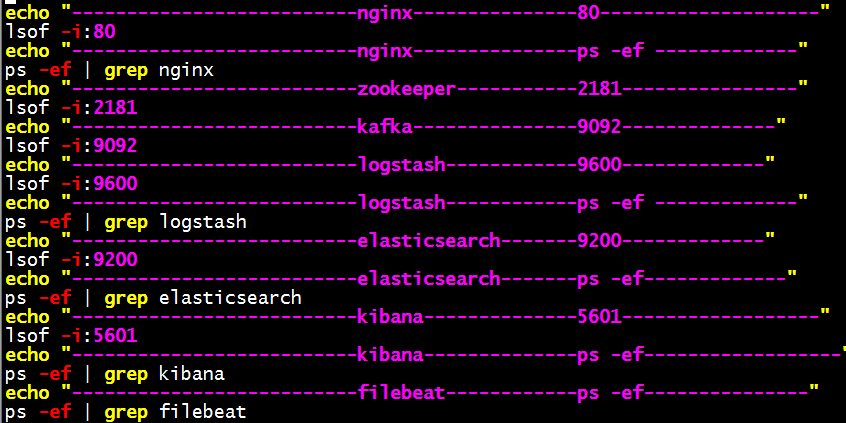
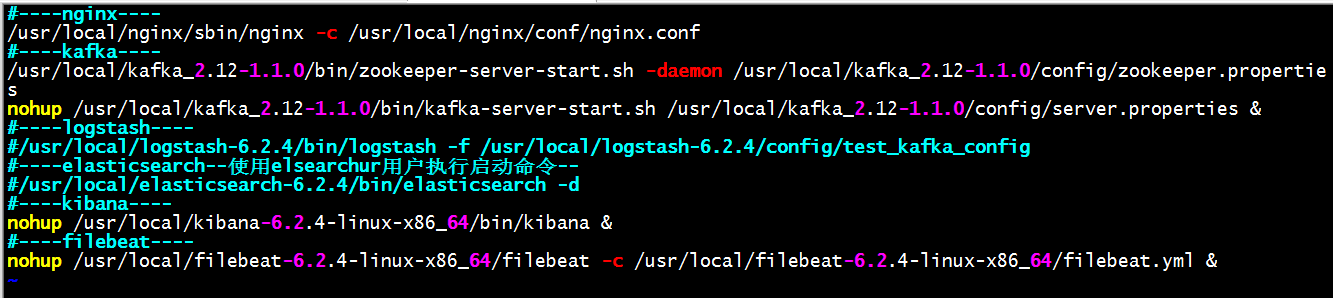


环境说明：Centos6.5 Vmware14

用户密码Ubuntu elk 111111

脚本汇总

****

****

**参考资源：**

<https://blog.csdn.net/qq_36079872/article/details/72772826>

<https://segmentfault.com/a/1190000012730949>

## 一、替换为JDK8

rpm -qa |grep jdk

yum remove java-1.8.0-openjdk-headless-1.8.0.171-3.b10.el6\_9.x86\_64

export JAVA\_HOME=/usr/local/jdk1.8.0\_172

export JRE\_HOME=/usr/local/jdk1.8.0\_172/jre

export CLASSPATH=.:$JAVA\_HOME/lib:$JRE\_HOME/lib

export PATH=$JAVA\_HOME/bin:$PATH

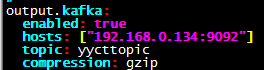
## 二、Filebeat安装

### 修改配置文件

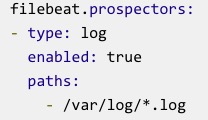
数据源 /usr/local/gogs/log/gogs.log （猜测如需增加源，直接追加行）



参见filebeat.reference.yml ，



注意参见官方，一定要打开探测开关，修改为true



### 启动与重新载入

参见 filebeat –help

测试配置： filebeat test config

启动： nohup filebeat –c filebeat.yml &

重启使用kill -9 pid

## 三、Kafka配置

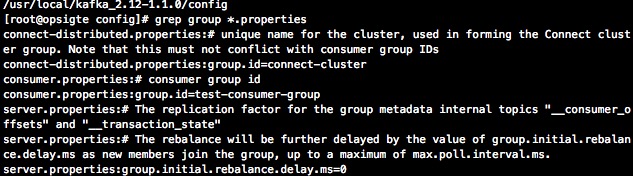
修改配置 kafka的server.properties的 broker.id=1必须是唯一的

**提供** 9092端口 依赖zookeeper，提供端口2181

C:\Users\Administrator\Documents\Tencent Files\917992753\Image\C2C\{55EF3F62-F9BA-CE30-0B03-A57CACDE62F5}.jpg

### 1.启动kafka

注意配置group\_id,topic\_id，服务不要绑定为localhost



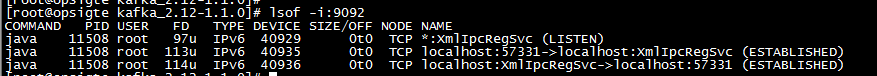
**使用安装包中的脚本启动单节点 Zookeeper 实例：**

bin/zookeeper-server-start.sh -daemon config/zookeeper.properties

zookeeper默认端口2181

nohup bin/kafka-server-start.sh config/server.properties &

kafka默认端口9092



### 2.快速使用kafka,检测topics

<http://kafka.apache.org/quickstart>

配置主题需要单独脚本执行，参见官网

配置a topic 标准方法，一个分区，一个副本：

bin/kafka-topics.sh --create --zookeeper localhost:2181 --replication-factor 1 --partitions 1 --topic test

已经集成脚本内网115ubuntu上**create\_kafka\_topics.sh**

查看当前topics,默认会有一个yycttopic(猜测是filebeat或者logstash连接时产生的)



已经集成脚本内网115ubuntu上**list\_kafka\_topics.sh**

### 3.测试消息的生产与消费

C:\Users\Administrator\Documents\Tencent Files\917992753\Image\C2C\{48E372C4-3876-51BC-8CA6-29040FA2759B}.jpg



详见kafka目录的脚本**consumer\_on\_console.sh producer\_on\_console.sh**

### 4.启动一个多broker的集群

英文原版参见官方：<http://kafka.apache.org/quickstart#quickstart_download>









### 5.Kafka使用的监控工具：KafkaOffsetMonitor

官网下载好jar包，执行startmonitor.sh

java -cp KafkaOffsetMonitor-assembly-0.2.1.jar com.quantifind.kafka.offsetapp.OffsetGetterWeb --zk 192.168.0.155:2181 --port 8881 --refresh 10.seconds --retain 2.days 1>/usr/local/kafkaoffsetmonitor/stdout.log 2>/usr/local/kafkaoffsetmonitor/stderr.log &

## 四、Logstash配置

从kafka端口中，按group\_id,topic\_id取出

安装目录下添加自定义的配置文件

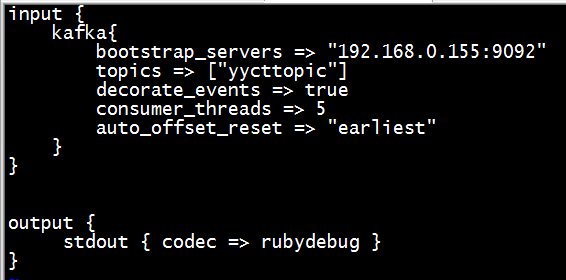
/usr/local/logstash-6.2.4/config/test\_config

测试配置文件bin/logstash -t -f test\_conf

启动 bin/logstash -f test\_conf

重启使用kill -9

### 1.简单解析，对日志不作任何过滤



### 2.解析nginx日志

参考资源：<http://blog.51cto.com/liqingbiao/1927520>

<https://doc.yonyoucloud.com/doc/logstash-best-practice-cn/filter/useragent.html>

index： 为日志创建索引logstash-nginx-access-＊，这里也就是kibana那里添加索引时的名称

#### 1.logstash数据源：直接从文件中读取

统一日志输出格式  
log\_format main1 '$http\_host $remote\_addr - $remote\_user [$time\_local] "$request" '

                      '$status $body\_bytes\_sent "$http\_referer" '

                      '"$http\_user\_agent" "$http\_x\_forwarded\_for" "$upstream\_addr" $request\_time';

Host.access.log日志输出

192.168.0.134 192.168.0.136 - - [05/Jun/2018:06:29:03 +0800] "GET /GME-Web-Admin/gme-web-repository HTTP/1.1" 200 19440 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36" "-" "127.0.0.1:3000" 0.037

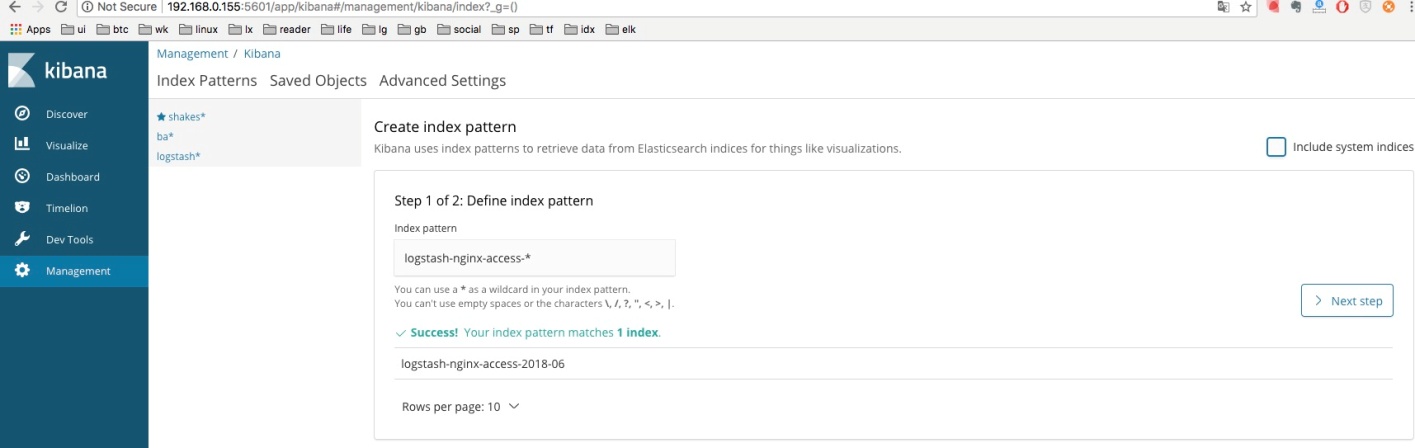
Grok解析表达式

//NGUSERNAME [a-zA-Z\.\@\-\+\_%]+

//NGUSER %{NGUSERNAME}

NGINXACCESS %{IPORHOST:http\_host} %{IPORHOST:clientip} - %{USERNAME:remote\_user} \[%{HTTPDATE:timestamp}\] \"(?:%{WORD:http\_verb} %{NOTSPACE:http\_request}(?: HTTP/%{NUMBER:http\_version})?|%{DATA:raw\_http\_request})\" %{NUMBER:response} (?:%{NUMBER:bytes\_read}|-) %{QS:referrer} %{QS:agent} %{QS:xforwardedfor} %{QS:upstream\_addr} %{NUMBER:request\_time:float}

添加索引，索引key参见配置文件中的index项



#### 2.输入源是kafka(filebeat采集)

消费数据的格式如下：

{"@timestamp":"2018-06-04T09:00:31.995Z","@metadata":{"beat":"filebeat","type":"doc","version":"6.2.4","topic":"yycttopic"},"source":"/usr/local/nginx/logs/host.access.log","offset":516555,"message":"192.168.0.136 - - [31/May/2018:06:35:26 -0700] \"GET /zabbix/jsLoader.php?ver=3.4.9\u0026lang=zh\_CN\u0026showGuiMessaging=1 HTTP/1.1\" 304 0 \"http://192.168.0.155/zabbix/latest.php?fullscreen=0\u0026hostids%5B%5D=10084\u0026application=\u0026select=\u0026show\_without\_data=1\u0026show\_details=1\u0026filter\_set=1\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36\" \"-\"","prospector":{"type":"log"},"beat":{"name":"ubuntu","hostname":"ubuntu","version":"6.2.4"}}

解析ip地理信息？

### 3.解析post json日志？

背景说明：考虑到json已经是格式化文本，不必为每个接口写过滤解析规则，不对json内容作任何加工。

使用正则模板

### 4.Grok 调试grokdebug与构造grokconstructor

<http://grokdebug.herokuapp.com> 官方

<http://grokconstructor.appspot.com>

国内的镜像，方便使用：

<http://grok.elasticsearch.cn/>

如果你的日志每一行都遵循固定格式，你可以考虑使用 dissect filter(<https://www.elastic.co/guide/en/logstash/current/plugins-filters-dissect.html>)，性能更强更简单

## 五、Elasticsearch配置

path.data: /usr/local/elasticsearch-6.2.4/data/elasticsearch

path.logs: /usr/local/elasticsearch-6.2.4/logs/elasticsearch

network.host: 192.168.0.134

http.port: 9200

./elasticsearch –d –Xms512m –Xmx512m 内存参数待定

### 1.问题： centos6.5（内网IP134,155）上添加非root用户,使用elsearchur用户执行启动命令

groupadd elsearchgp  
useradd elsearchur -g elsearchgp -p elsearchpw  
chown -R elsearchur:elsearchgp elasticsearch-6.2.4  
su elsearchur cd elasticsearch-6.2.4/bin  
./elasticsearch -d

### 2.问题： 升级内核：

rpm --import <https://www.elrepo.org/RPM-GPG-KEY-elrepo.org>

yum install -y http://www.elrepo.org/elrepo-release-7.0-2.el7.elrepo.noarch.rpm  //添加源

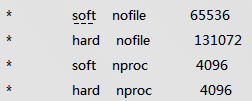
yum --enablerepo=elrepo-kernel install -y kernel-ml  //安装当前最新内核，以后升级内核直接运行这句就可

如果不想折腾升级内核，请使用ubuntu（默认内核版本较新（3.5+））

### 3.问题：修改进程限制

/etc/security/limits.conf

添加配置项：





查看进程 ps –aux | grep elasticsearch

查看端口 netstat –atunlp

http访问查看 curl <http://localhost:9200/?pretty>

curl 'localhost:9200/\_cluster/health?level=indices&pretty'

Elastalert-基于Elasticsearch层面的监控告警框架

### 4.ElasticSearch插件安装---Head ，Kopf,Bigdesk

Elasticsearch-head官网安装方式在ubuntu(全新内核4.4)安装失败（不兼容），使用centos6.5(老内核2.6.32)安装成功

* git clone git://github.com/mobz/elasticsearch-head.git
* cd elasticsearch-head
* npm install
* npm run start
* open <http://localhost:9100/>

ElasticSearch插件安装---Kopf

git://github.com/lmenezes/elasticsearch-kopf.git

ElasticSearch插件安装---Bigdesk

git clone https://github.com/lukas-vlcek/bigdesk.git

最终采用tomcat容器本地运行

## 六、Kibana配置

**elasticsearch.url: "http://localhost:9200"**

参考<http://cwiki.apachecn.org/pages/viewpage.action?pageId=8159438>

vim /usr/local/kibana/config/kibana.yml 添加一个es

elasticsearch.url: "http://10.149.11.226:9200"

server.host: "0.0.0.0"

logging.dest: "/usr/local/kibana/kibana.log"

启动 nohup ../bin/kibana &

杀进程

ps -ef | grep kibana （这个有时候不行）  
ps -ef | grep node  
kill -2 21048

看日志

tail -f /usr/local/kibana/kibana.log 查看实时日志输出

UI配置 <http://192.168.0.155:5601>

### 1.添加测试数据，进行基本操作

旧版本参照（中文）

<http://www.cnblogs.com/yiwangzhibujian/p/7137546.html>

新版本参见官方（英文）

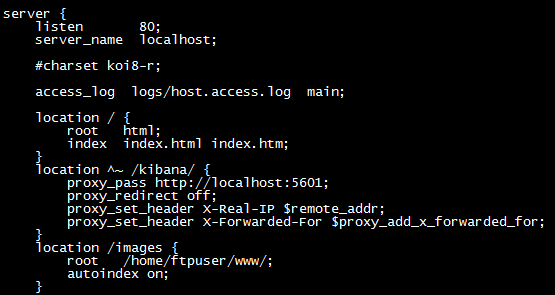
<https://www.elastic.co/guide/en/kibana/current/tutorial-load-dataset.html>

<https://www.elastic.co/guide/en/kibana/current/tutorial-define-index.html>

<https://www.elastic.co/guide/en/kibana/current/tutorial-discovering.html>

## 七、Nginx 配置

**添加反向代理5601接口**

****

sbin/nginx -s reload 修改配置后刷新

sbin/nginx –c conf/nginx.conf 启动服务

lsof –i:80 查看端口服务

ps –ef |grep nginx 查看进程

## 八、SpringBoot整合kafka和storm以及在这过程遇到的一些问题和解决方案

<https://github.com/xuwujing/springBoot-study>

## 九、监控系统

Watcher监控网络，suricata监控网络行为

参见<https://sdk.cn/news/3225>

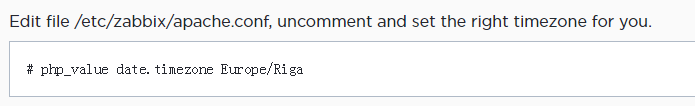
### 1.Zabbix服务端安装

119.29.1.175此服务器nginx软件安装情况说明：nginx按官方方式安装，参见<http://wiki.ubuntu.org.cn/Nginx> ，重启重载等操作方式与源码安装的不同

同样的，192.168.0.155，ubuntu机器按相同的方式配置安装

因为依赖数据库，先选择腾讯云远程服务器（119.29.1.175，mysql5.7.22）安装进行测试使用.安装方法详情参见官方说明：<https://www.zabbix.com/download?zabbix=3.4&os_distribution=ubuntu&os_version=xenial&db=MySQL>

安装过程中注意时区设置



要如下设置，不能设置为Asia/China



安装完毕后，修改默认的80端口，vim /etc/apache2/ports.conf



添加转发规则，



重启nginx方法1: /etc/init.d/nginx restart 方法2：service nginx start

方法3： nginx –c nginx.conf

只有方法3，nignx是最稳定的,不会自动退出进程

安装完毕后，系统生成配置文件/usr/share/zabbix/conf/zabbix.conf.php

Web页面登录，用户名Admin ,密码zabbix

重启服务

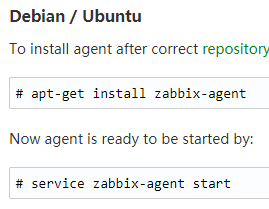
# systemctl restart zabbix-server zabbix-agent apache2  
# systemctl enable zabbix-server zabbix-agent apache2

界面汉化，系统安装语言包apt-get install language-pack-zh-hant language-pack-zh-hans

修改Admin登录密码，与腾讯云系统用户密码一致

### 2.Zabbix Agent安装

参照官网<https://www.zabbix.com/documentation/3.2/manual/installation/install_from_packages/agent_installation>



### 3.Zabbix\_get 安装

命令apt-get install zabbix-get

测试获取系统压力

zabbix\_get -s 172.16.1.61 -p 10050 -k "system.cpu.load[all,avg1]"

日志收集性能检测、防止丢失方法、丢失后续处理方法

防止数据丢失，在kafka数据层多节点。

切换为HTTPS（safe）

添加用户登录（safe）

添加IP绑定限制（safe）

提供tomcat错误日志、调试日志、事件日志、SQL日志、慢日志、nginx等类型日志接入

高级集群配置