## ELK 日志分析系统

The Elastic Stack - 它不是一个软件，而是Elasticsearch，Logstash，Kibana 开源软件的集合，对外是作为一个日志管理系统的开源方案。它可以从任何来源，任何格式进行日志搜索，分析获取数据，并实时进行展示。像盾牌（安全），监护者（警报）和Marvel（监测）一样为产品提供更多的功能。

　　Elasticsearch：搜索，提供分布式全文搜索引擎

　　Logstash: 日志收集，管理，存储

　　Kibana ：日志的过滤web 展示

Filebeat：监控日志文件、转发

服务端安装流程：(服务端是指安装ELK程序的服务器，本文安装环境为Centos7)

安装JDK：yum install java-1.8.0-openjdk -y

准备E、L、K软件包：在此处下载https://www.elastic.co/cn/downloads并安装rpm包

设置自启：systemctl enable elasticsearch

systemctl enable logstash

systemctl enable kibana

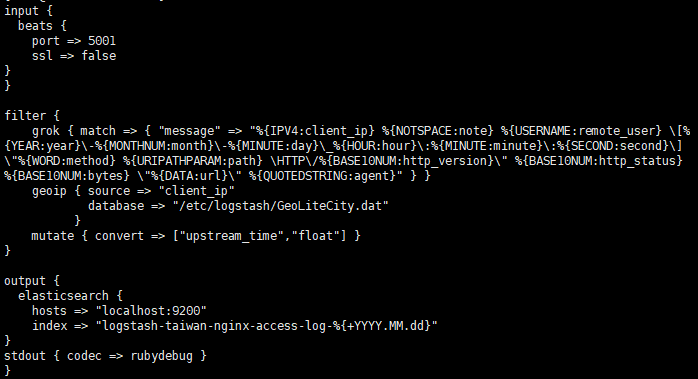
检查服务：netstat -anpt | grep 9200 # es默认端口

netstat -anpt | grep 5601 # kibana默认端口

netstat -anpt | grep 5000

防火墙放行端口：firewall-cmd --add-port=5601/tcp --permanent && firewall-cmd --reload

es不用更改配置，使用默认即可，也可以更改datepath指定数据存储位置，这里我们只需要更改logstash配置：/etc/logstash/logstash.yml



此配置文件分为三部分：

1. input：数据来源，可监听端口接收其他服务器发来的日志，也可指定本地日志
2. filter：日志过滤规则和日志字段设定，以及geoip处理归属地信息

Geoip解析库地址:

<http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz>

正则可用内置规则和自定义规则内置规则请参考我的github：

<https://github.com/aming-note/note/blob/master/Linux_word/logstash-grok.txt>

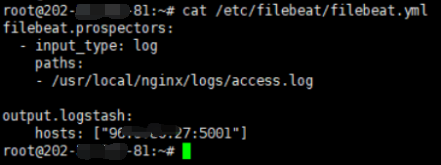
自定义规则格式为: (?<字段名>表达式)，如下例则匹配时间格式YYYY-mm-dd\_HH:MM:ss

(?<logdate>[0-9][0-9][0-9][0-9]-[0-9][0-9]-[0-9][0-9]\_[0-9][0-9]:[0-9][0-9]:[0-9][0-9])

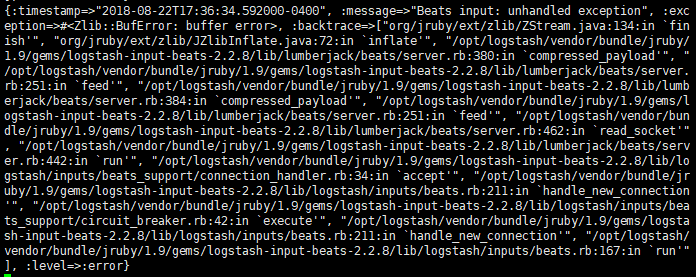
1. output：日志输出至es，指定es的端口和索引

客户端安装流程：(客户端时指存放日志并且需要发送至ELK分析的服务器)

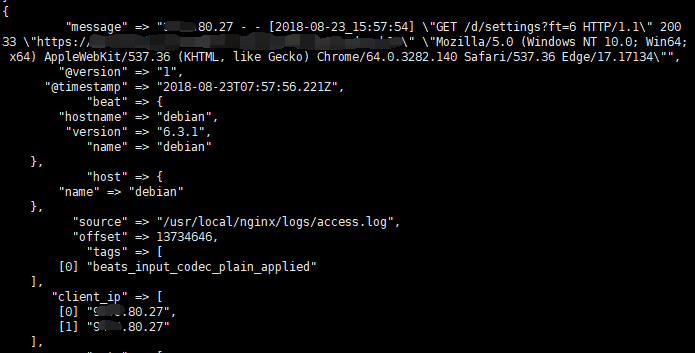
客户端只需安装filebeat，发送本地日志到logstash即可，filebeat也是rpm安装，更改/etc/filebeat/filebeat.yml配置文件:



需要指定本地日志文件的位置和logstash的ip和端口，启动filebeat服务，观察logstash日志：/var/log/logstash/logstash.log

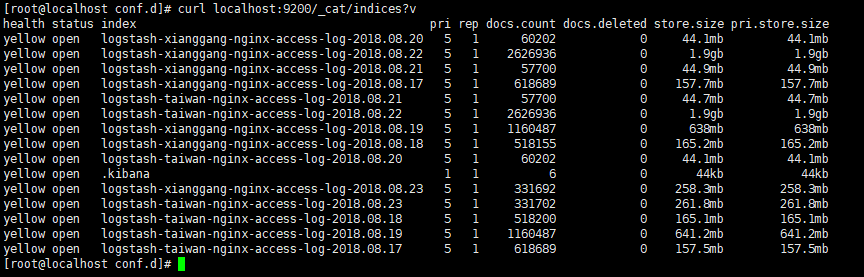


以及logstash输出指es的日志：/var/log/logstash/logstash.stdout



能看到此日志则代表部署成功，否则请检查服务状态和网络情况

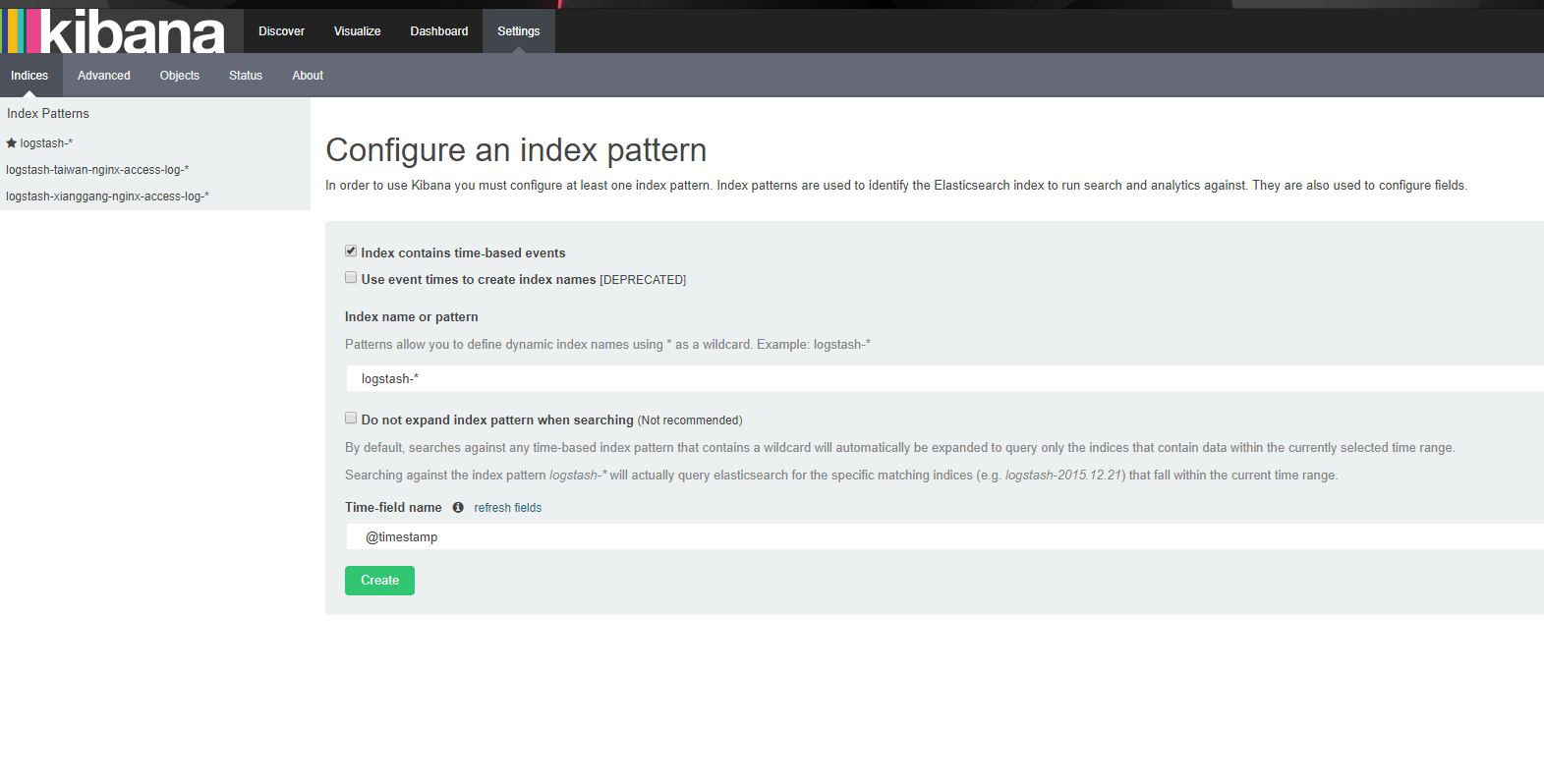
查看es数据：es数据是按照指定的index索引存放的，所以查询时也需要指定响应的索引，可使用curl查看数据导入情况，使用curl localhost:9200/\_cat/indices?v



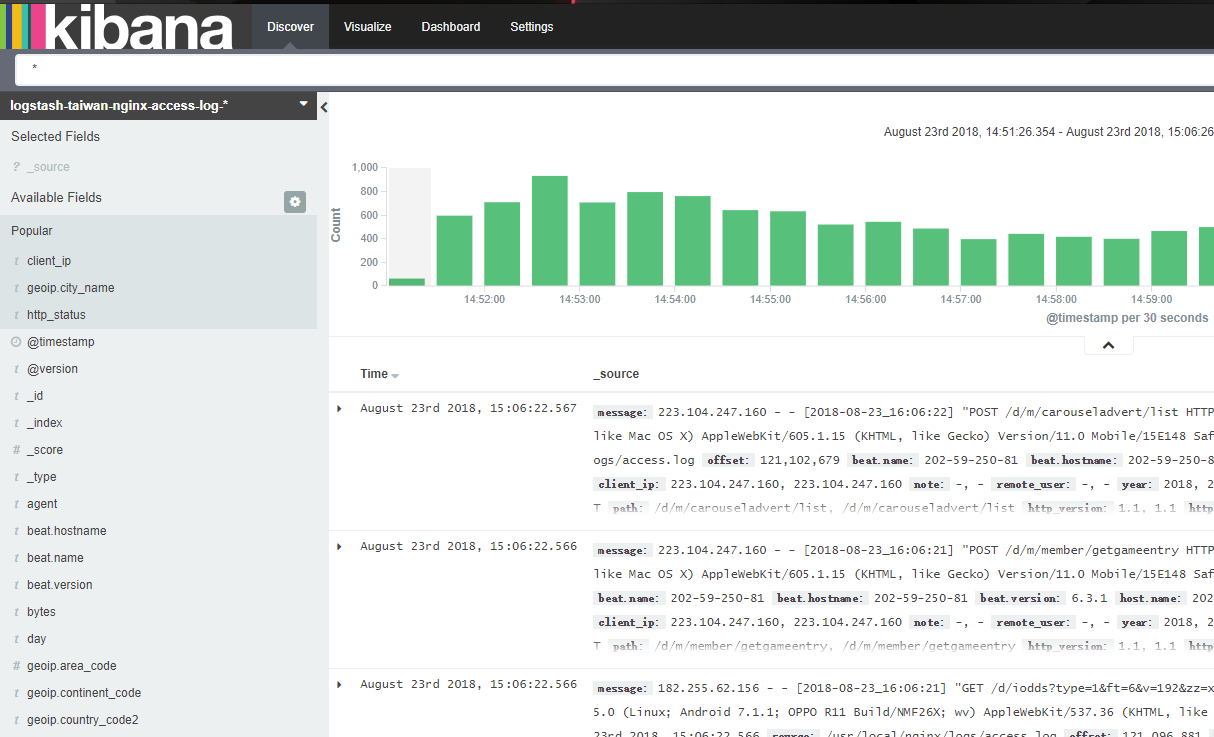
看到上图中所显示的信息就可以在kibana指定索引查看数据了，否则请检查

es服务状态和logstash错误日志

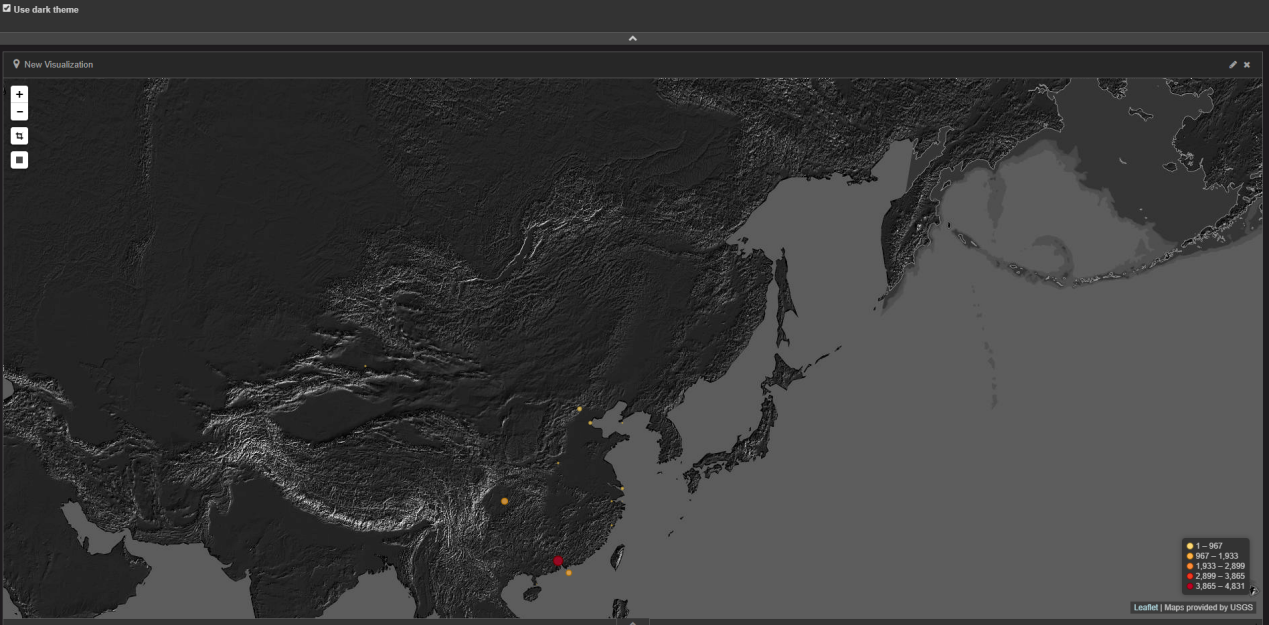
创建kibana索引：



左上方的索引是我已经创建好的，新搭建的系统没有这些，需要在页面指定es中的数据索引来查看响应的日志，索引和日志的对应是我们在logstash中指定的，logstash接收到日志后会将数据提交给es指定的索引中



点击Discover可查看es中的日志数据，也可按照字段或者时间检索日志，既然已经有了geoip库提供的坐标，自然可以以地图的方式显示访问情况



Kibana默认地图为卫星地图，可以更换地图样式，编辑kibana安装目录下的地图文件：

kibana/src/ui/public/vislib/visualizations

//url: 'https://otile{s}-s.mqcdn.com/tiles/1.0.0/map/{z}/{x}/{y}.jpeg',注释此行添加以下行

url: 'http://webrd0{s}.is.autonavi.com/appmaptile?lang=zh\_cn&size=1&scale=1&style=8&x={x}&y={y}&z={z}',

重启kibana服务。

小结：

ELK优势：

针对网络攻击事件时，方便运维人员朔源

日志集中手机存储，方便日后分析

优化业务和系统时做到有据可依

文档写的不怎么好，主要是给自己做备忘用的，搭建过程也是一路坎坷，就不吐槽了，只要会查google 百度，就没有解决不了的问题，更多技术文档请访问我的github：

https://github.com/aming-note/note