ELK是个经典的配合：ElasticSearch、LogStash、Kibana。E解决了存储和检索、L用于日志收集、K生动的展示了数据的变化趋势、并提供查询能力。

安装elasticsearch及其插件head

安装包准备:

ELK官网下载官网: https://www.elastic.co/downloads

nodejs下载官网:https://nodejs.org/en/download/

从github下载head插件:https://github.com/mobz/elasticsearch-head

开始安装elasticsearch

环境准备

Centos7.4 、jdk1.8

解压安装包 tar -zxvf elasticsearch-6.7.1.tar.gz

进行设置

从5.0开始，ElasticSearch 安全级别提高了，不允许采用root帐号启动，所以我们要添加一个用户

1.添加一个用户elk，并切换至该用户

useradd elk

passwd elk

2.修改ES配置文件:

./elasticsearch-6.7.1/config/elasticsearch.yml

cluster.name: es-cluster # 集群名称(个节点必须一致)

node.name: es-node-1 # 节点名称

node.master: true # 设置为主节点(三个节点:2个true,1个false)

node.data: true # 存储数据

path.data: /data/ELK/elasticsearch-6.7.1/data

path.logs: /data/ELK/elasticsearch-6.7.1/data

bootstrap.memory_lock: false # true:不允许交换内存;false:允许交换内存

bootstrap.system_call_filter: false # 系统调用过滤器,建议禁用该项检查

network.host: 0.0.0.0 # 绑定端口，默认为localhost，建议改为0.0.0.0，否则其他机器无法访问到该机器

http.port: 9200 #默认端口号9200

4.启动环境配置:

配置系统参数:

/etc/security/limits.conf

* hard nofile 65536

* soft nofile 65536

/etc/sysctl.conf

vm.max_map_count=262144

sysctl -p

创建elsearch用户:

adduser elsearch

设置elsearch用户的密码:

passwd elsearch

通过浏览器访问：es安装成功

elasticsearch-head是es可视化界面

1.安装elasticsearch-head插件需要nodejs的支持

安装grunt（如果未安装，head插件的启动使用grunt）

1.1 npm install -g grunt-cli #安装grunt命令行工具grunt-cli

1.2 npm install grunt --save-dev #安装grunt及其插件

1.3 grunt -version #查看安装版本情况

下载并安装elasticsearch-head

git clone git://github.com/mobz/elasticsearch-head.git #git下载

cd elasticsearch-head #进入目录

npm install # 如果npm使用很多错误，尝试使用cnpm

npm install grunt --save #安装grunt到模块中并保存

修改elasticsearch-head下的Gruntfile.js

```
cd ./elasticsearch-head  #(elasticsearch-head源码文件夹)
vim Gruntfile.js
Add hostname
     connect: {
                    server: {
                            options: {
                                    hostname: '0.0.0.0',
                                    port: 9100,
                                    base: '.',
                                    keepalive: true
                            }
                    }
            }
```

启动elasticsearch和head插件

grunt server #执行该命令，启动head插件

在浏览器访问es的head插件页面，http://ip:9100, 9100默认端口号

安装Logbash及其插件

创建目录,新增配置文件

Touch Config/logbash-tcp.conf(文件名称自定义)

配置文件内容如下

```
input {
    tcp {
      port => 8688      //tcp监听port,log4j.appender.logstash.port=8688

       }
}

output {
       elasticsearch {
       hosts => ["192.168.60.251:9200"]  #elasticsearch         的访问地址
       index => "log4j-%{+YYYY.MM.dd}"       #定义es的索引格式
       }
       stdout {
              codec => rubydebug
       }
}
```

执行启动logstash

./logstash -f /conf/logstash.conf (-f:指定加载的文件)

安装kibana

解压安装包

tar -zxvf kibana-6.7.1-linux-x86_64.tar.gz

修改kibana的配置文件

vi /kibana-6.7.1/config/kibana.yml

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

server.host: "0.0.0.0"

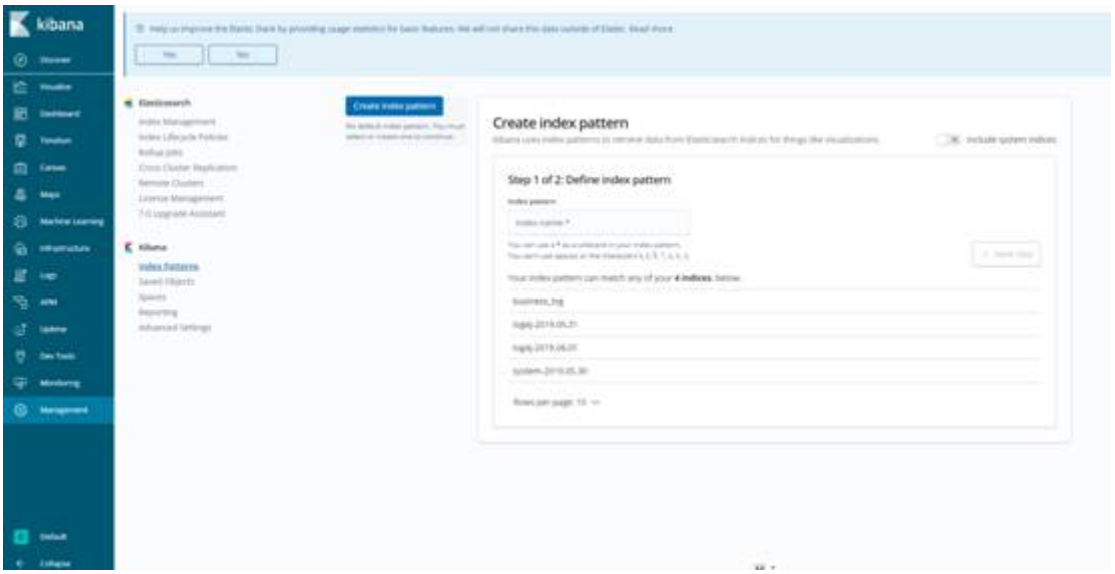
然后访问:http://ip:5601

启动Kibana

cd /kibana-6.7.1/bin

启动：   ./kibana

观察是否启动成功



1. Management:创建kibana的索引
2. Discover: 根据创建的索引，条件式的查看日志
3. Visualize: 为数据创建图形分析图