ELK日志平台搭建

安装环境centos7.0　单点搭建
一，准备工作
rpm包安装elk
jdk环境：jdk-8u65-linux-x64.rpm（用于es和kibana） jdk-8u91-linux-x64.gz（用于logstash）
elk安装包：elasticsearch-5.3.0.rpm ；kibana-5.3.0-x86_64.rpm； logstash-5.3.0.rpm
elasticsearch head插件需要的node包 node-v6.10.2-linux-x64.tar.xz
包放在 /usr/loacl/src/
EShead插件所需要的包elasticsearch-head.tar phantomjs.tar

关闭防火墙
systemctl stop firewalld.service #停止firewall
systemctl disable firewalld.service #禁止firewall开机启动
firewall-cmd --state #查看默认防火墙状态（关闭后显示notrunning，开启后显示running）

修改hostname
hostname #查看主机名
hostnamectl set-hostname elk_zabbix ##修改主机名
hostnamectl status ##查看主机名状态

修改hosts
[root@elk_zabbix ~]# vim /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
110.24.166.104 elk_zabbix

首先安装jdk包
[root@elk_zabbix src]# yum localinstall -y jdk-8u65-linux-x64.rpm

查看jdk版本
[root@elk_zabbix src]# java -version
java version "1.8.0_65"
Java(TM) SE Runtime Environment (build 1.8.0_65-b17)
Java HotSpot(TM) 64-Bit Server VM (build 25.65-b01, mixed mode)

1.安装elasticsearch
下载并安装GPG key
rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

[root@elk_zabbix src]# yum localinstall -y elasticsearch-5.3.0.rpm

配置文件
【如果 ES 是单节点】
[root@elk_zabbix etc]# grep ^[^#] /etc/elasticsearch/elasticsearch.yml
cluster.name: elk
node.name: elk_zabbix #节点的名称
path.data: /data/elasticsearch #日志存储目录
path.logs: /var/log/elasticsearch #elasticsearch启动日志路径
network.host: 10.24.166.104

【如果 elasticsearch 是集群】
[root@elk_zabbix etc]# grep ^[^#] /etc/elasticsearch/elasticsearch.yml
cluster.name: elk

node.name: elk01
path.data: /data/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 10.50.200.220
discovery.zen.ping.unicast.hosts: ["10.50.200.218", "10.50.200.219", "10.50.200.220"]
discovery.zen.minimum_master_nodes: 3
其他节点类似

#以下两项设置es5.x版本的head插件可以访问es
http.cors.enabled: true #开启跨域访问支持，默认为false
http.cors.allow-origin: "*" #跨域访问允许的域名地址，使用正则表达式

创建日志存贮目录和elasticsearch启动日志路径
mkdir -pv /data/elasticsearch
设置权限 /data/elasticsearch（不设置权限启动不起来）
chown -R elasticsearch:elasticsearch /data/elasticsearch

启动elasticsearch
systemctl daemon-reload
systemctl start elasticsearch.service
systemctl enable elasticsearch.service

安装部署head
第一步，安装git
需要从github上面下载代码，因此先要安装git
[root@elk_zabbix ~]# yum -y install git

第二步，安装node
由于head插件本质上还是一个nodejs的工程，因此需要安装node，使用npm来安装依赖的包。
jar包是xz格式的，一般的linux可能不识别，还需要安装xz.
yum install -y xz
然后解压nodejs的安装包:
[root@elk_zabbix ~]# cd /usr/local/src
[root@elk_zabbix src]# xz -d node-v6.10.2-linux-x64.tar.xz
[root@elk_zabbix src]# tar -xvf node-v6.10.2-linux-x64.tar -C /usr/loca/src
解压完node的安装文件后
[root@elk_zabbix src]# cd
[root@elk_zabbix ~]# ln -s /usr/local/node-v6.10.2-linux-x64/bin/npm /usr/bin/npm
[root@elk_zabbix ~]# ln -s /usr/local/node-v6.10.2-linux-x64/bin/node /usr/bin/node
这个时候可以测试一下node是否生效：
[r[root@elk_zabbix ~]# node -v
v6.9.1
[root@elk_zabbix ~]# npm -v
3.10.10
第三步，安装grunt
grunt是一个很方便的构建工具，可以进行打包压缩、测试、执行等等的工作，5.0里的head插件就是通过grunt启动的。因此需要安装一下grunt：
[root@elk_zabbix ~]# npm install grunt-cli
[root@elk_zabbix ~]# ln -s /usr/local/node-v6.10.2-linux-x64/lib/node_modules/grunt-cli/bin/grunt /usr/bin/grunt
安装完成后检查一下：
[root@elk_zabbix ~]# grunt -version
第四步，安装head插件
进入elasticsearch的安装目录
[root@elk_zabbix ~]# cd /var/lib/elasticsearch/
[root@elk_zabbix elasticsearch]# git clone git://github.com/mobz/elasticsearch-head.git
[root@elk_zabbix elasticsearch]# chown -R elasticsearch:elasticsearch elasticsearch-head/

由于head的代码还是2.6版本的，直接执行有很多限制，比如无法跨机器访问。因此需要用户修改两个地方：
修改服务器监听地址
[root@elk_zabbix elasticsearch]# cd elasticsearch-head
[root@elk_zabbix elasticsearch]# vim Gruntfile.js +94
```
connect: {
    server: {
        options: {
            port: 9100,
            hostname: '*',
            base: '.',
            keepalive: true
        }
    }
}
```
增加hostname属性，设置为*
修改连接地址：
[root@elk_zabbix elasticsearch]# vim _site/app.js +4329
修改head的连接地址:
this.base_uri = this.config.base_uri || this.prefs.get("app-base_uri") || "http://localhost:9200";
把localhost修改成你es的服务器地址，如:
this.base_uri = this.config.base_uri || this.prefs.get("app-base_uri") || "http://10.24.166.10:9200";
第五步，运行head
首先开启5.0 ES。
然后在head目录中，执行npm install 下载以来的包：
npm install
#安装完成后可能有一些报错,解决方法如下：
(1) 查看报错信息”Error: Cannot find module '/var/lib/elasticsearch/elasticsearch-head/node_modules/phantomjs-prebuilt/install.js'” ，未找到” phantomjs-prebuilt/install.js”文件；
(2) 采取比较土的办法，将完整的”phantomjs-prebuilt/”目录上传到相应位置，重新执行”npm install” ，无报错。
由于无法上传附件，附上下载git地址：git clone https://github.com/ariya/phantomjs.git
#同时有3个警告信息，忽略即可，其中“npm WARN elasticsearch-head@0.0.0 license should be a valid SPDX license expression”警告信息可做如下处理
即修改”./ elasticsearch-head”目录下“package.json”文件第17行的”"Apache2" ”为"Apache-2.0"，涉及到开源软件与其他合作类软件的使用声明。
#如果没有全局安装grunt二进制程序，可在”elasticsearch-head”目录下执行”npm install grunt --save“或” npm install grunt-cli “。
#启动head插件，需要到head目录下
#可以采用screen放在后台运行，不然退出ssh后grunt进程就关闭了。
grunt server &
访问:10.24.166.104:9100
这个时候，访问http://10.24.166.104:9100就可以访问head插件
[root@elk_zabbix elasticsearch]# curl -I 10.24.166.104:9100
```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 03 May 2017 06:21:28 GMT
ETag: W/"440-15bccf87a40"
Content-Type: text/html; charset=UTF-8
Content-Length: 1088
Date: Fri, 05 May 2017 08:27:41 GMT
Connection: keep-alive
```

2.安装kibana
[root@elk_zabbix src]# yum localinstall -y kibana-5.3.0-x86_64.rpm

配置文件
[root@elk_zabbix src]# grep ^[^#] /etc/kibana/kibana.yml
server.port: 5601 #默认端口
server.host: "0.0.0.0" #允许访问的ip
elasticsearch.url: "http://10.24.166.104:9200" #es地址与端口

启动kibana
systemctl daemon-reload
systemctl enable kibana.service
systemctl start kibana.service

3.安装logstash
logstash要安装到需要去收集日志的服务器上
首先要看需要收集复制日志服务的jdk版本 5.x版本的logstash必须匹配jdk1.8版本以上
tar -zxvf jdk-8u91-linux-x64.gz -C /usr/local/
配置环境变量
tar -cvf jdk1.7.0_79.tar jdk1.7.0_79
vim /etc/profile.d/java.sh 或者 vim /etc/profile
添加环境变量
export JAVA_HOME=/usr/local/jdk1.8.0_91
export JAVA_BIN=/usr/local/jdk1.8.0_91/bin
export PATH=$PATH:$JAVA_HOME/bin
export CLASSPATH=.:JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib/tools.jar
export JAVA_HOME JAVA_BIN PATH CLASSPATH

cd /usr/bin/
rm -f java
rm -f javac
ln -s /usr/local/jdk1.8.0_91/bin/java /usr/bin/java
ln -s /usr/local/jdk1.8.0_91/bin/javac /usr/bin/javac
source /etc/profile.d/java.sh 或者 source /etc/profile
java -version
java version "1.8.0_91"
Java(TM) SE Runtime Environment (build 1.8.0_91-b14)
Java HotSpot(TM) 64-Bit Server VM (build 25.91-b14, mixed mode)

cd /usr/local/src/

yum localinstall -y logstash-5.3.0.rpm
安装后看是否有缺少环境变量的报错 (若有报错remove掉解决报错后重新装)

配置文件
grep ^[^#] /etc/logstash/logstash.yml
path.data: /var/lib/logstash　　#数据路径
path.config: /etc/logstash/conf.d　　#配置文件路径
path.logs: /var/log/logstash　　#日志路径

配置文件 必须要以”.conf“以尾缀
默认配置已经明确数据，日志，logstash pipeline实例文件的存储位置，保持默认即可；
根据默认配置，pipeline实例文件默认应放置于/etc/logstash/conf.d目录，此时目录下无实例文件，可根据实际情况新建实例，
cat /etc/logstash/conf.d/log.conf
```
input {
 file {
   type => 'api'
   path => "/data/logs/qiyu/api/api.log"
   start_position => "beginning"
 }
}
filter {
   grok {
      match => ["message" ,"%{TIMESTAMP_ISO8601:time}"]
 }
}
output {
   if [type] == 'api' {
      elasticsearch {
         action => "index"
         hosts => ["10.24.166.104:9200"]
         index => "logstash-testapi-%{+YYYY.MM.dd}"
       }
    }
}
```
注：api文件的配置文件（其他文件按这个来filter不动 需要增加input和output） iindex必须按照logstash*-%{+YYYY.MM.dd}的格式
chown -R logstash:logstash /etc/logstash/conf.d/
#配置实例文件以”input“，”output“，”filter”等区域组成，前两者为必选项；
#”input”与”output”利用插件进行数据输入与输出，如这里”file”即输入插件，“elasticseach”与“stdout”即输出插件；
#在各插件内再具体定义行为，如”input”定义了数据源，“elasticseach”定义了输出节点与数据输出的索引与格式；
#请注意权限，这里数据源必须要求有“读“的权限
启动测试
cd /usr/share/logstash/
 bin/logstash -e 'input { stdin { } } output { stdout {} }'
这样将logstash日志输出在屏幕上显示输出输入 会有告警用如下方法解决：
在“$LS_HOME”下建立“config”目录，并将”/etc/logstash/”下的文件建软链接到“config”目录，
mkdir -p /usr/share/logstash/config/
ln -s /etc/logstash/* /usr/share/logstash/config
chown -R logstash:logstash /usr/share/logstash/config/

配置文件实例启动测试并查看配置文件是否正确
cd /usr/share/logstash/
/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/log.conf -t
```
[root@iZwz9jdh2ap4dnsqf1alh6Z logstash]# /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/log.conf -t
Sending Logstash's logs to /var/log/logstash which is now configured via log4j2.properties
Configuration OK
```
若提示
Configuration OK
则表明配置文件正确（但具体情况要具体分析 有些根据生产环境情况配置）

/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/log.conf & 后台启动 -f 选定配置文件
jobs可以查看程序进程
ps aux |grep logstash 查看是否有进程