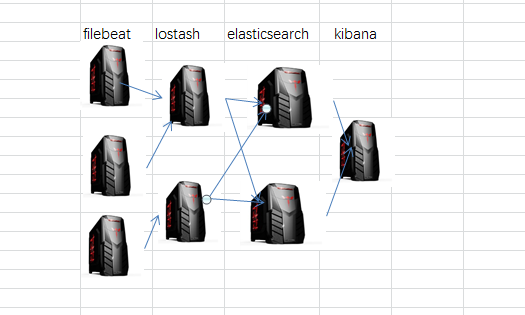
整体架构



一、Elasticsearch 部署

官网下载最新版本

前期系统需求：

解压缩到想要安装的目录一般为/usr/local下 tar -xf elasticsearch.5.x

**问题一：警告提示**

2016-11-06T16:27:21,712][WARN ][o.e.b.JNANatives ] unable to install syscall filter:

java.lang.UnsupportedOperationException: seccomp unavailable: requires kernel 3.5+ with CONFIG\_SECCOMP and CONFIG\_SECCOMP\_FILTER compiled inat org.elasticsearch.bootstrap.Seccomp.linuxImpl(Seccomp.java:349) ~[elasticsearch-5.0.0.jar:5.0.0]

at org.elasticsearch.bootstrap.Seccomp.init(Seccomp.java:630) ~[elasticsearch-5.0.0.jar:5.0.0]

报了一大串错误，其实只是一个警告。

解决：使用心得linux版本，就不会出现此类问题了。

**问题二：ERROR: bootstrap checks failed**

max file descriptors [4096] for elasticsearch process likely too low, increase to at least [65536]  
max number of threads [1024] for user [lishang] likely too low, increase to at least [2048]

**解决：**切换到root用户，编辑limits.conf 添加类似如下内容

vi /etc/security/limits.conf

添加如下内容:

\* soft nofile 65536

\* hard nofile 131072

\* soft nproc 2048

\* hard nproc 4096

**问题三：max number of threads [1024] for user [lish] likely too low, increase to at least [2048]**

**解决**：切换到root用户，进入limits.d目录下修改配置文件。

vi /etc/security/limits.d/90-nproc.conf

修改如下内容：

\* soft nproc 1024

#修改为

\* soft nproc 2048

**问题四：max virtual memory areas vm.max\_map\_count [65530] likely too low, increase to at least [262144]**

**解决**：切换到root用户修改配置sysctl.conf

vi /etc/sysctl.conf

添加下面配置：

vm.max\_map\_count=655360

并执行命令：

sysctl –p

然后，重新启动elasticsearch，即可启动成功

**防火墙配置**：firewall-cmd --zone=public --add-port=9200/tcp –permanent 针对elasticsearch

Firewall-cmd –zone=public –add-port=5601/tcp –permanent 针对kibana

Firewall-cmd –zone=public –add-port=5044/tcp –permanent 针对logstash

Firewall-cmd –zone=public –add-port=80/tcp –permanent 针对nginx

重载防火墙配置firewall-cmd --reload

**配置：配置文件 解压缩位置/elasticsearch/config/elasticsearch.yml 这几个软件的配置文件都是以.yml结尾的**

**需要改动的地方 监听ip 及端口 network.host: 0.0.0.0 http.port: 9200**

**可以直接启动了 elasticsearch/bin/elasticsearch**

**检查安装 curl** [**http://127.0.0.1:9200**](http://127.0.0.1:9200) **默认监听端口是9200和9300**

二、filebeat（beats） 部署

官网下载最新源码包 <https://www.elastic.com>

解压缩到你要安装的位置 tar –xf beats.-version tar.gz

**配置：配置文件 解压缩位置/filebeat/filebeat.yml**

**需要改动的地方**

**paths:**

**- /var/log/\*.log**

**- /var/log/message 这里根据自己需求监控日志：之检测文件夹下的文件，不递归可以配置多个**

**注释掉Elasticsearch output 的相关设置：**

#-------------------------- Elasticsearch output ------------------------------#output.elasticsearch:# Array of hosts to connect to.#hosts: ["localhost:9200"]# Optional protocol and basic auth credentials.#protocol: "https"#username: "elastic"#password: "changeme"

**配置输出到 Logstash：**

#----------------------------- Logstash output -------------------------------- output.logstash: # The Logstash hosts hosts: ["logstash ip:5044"] # Optional SSL. By default is off. # List of root certificates for HTTPS server verifications #ssl.certificate\_authorities: ["/etc/pki/root/ca.pem"] # Certificate for SSL client authentication #ssl.certificate: "/etc/pki/client/cert.pem" # Client Certificate Key #ssl.key: "/etc/pki/client/cert.key"

**启动filebeat 解压缩位置/filebeat/filebeat -e -c filebeat.yml**

**启动后会有数据传输，一般会在后台启动**

三、logstash部署

官网下载最新源码包 <https://www.elastic.com>

解压缩到你要安装的位置 tar –xf logstash.-version tar.gz

**配置：配置文件 解压缩位置/logstash/config/logstash.yml**

**需要改动的地方 mkdir 解压缩位置/logstash/config/config.d touch 解压缩位置/logstash/config/config.d/logstash.conf**

**input { beats { port => 5044 } } output { elasticsearch { hosts => "localhost:9200" manage\_template => false index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}" document\_type => "%{[@metadata][type]}" } }**

**启动 解压缩位置/logstash/bin/logstash -f 解压缩位置/logstash/config/config.d/logstash.conf**

四、kibana部署

官网下载最新源码包 <https://www.elastic.com>

解压缩到你要安装的位置 tar –xf kibana.versin.tar.gz

**配置：配置文件 解压缩位置/kibana/config/** **kibana.yml**

**需要改动的地方**

**server.port 5601 server.host 0.0.0.0**

**启动./ 解压缩位置/kibana/bin/kibana**

**浏览器访问**[**http://kibana的ip:5601**](http://kibana的ip:5601)

五、nginx代理kibana

**安装nginx**

**配置nginx：配置文件 /usr/local/nginx/conf/nginx.conf**

**server { listen 80; server\_name elk; location / { proxy\_pass http://localhost:5601; proxy\_http\_version 1.1; proxy\_set\_header Upgrade $http\_upgrade; proxy\_set\_header Connection 'upgrade'; proxy\_set\_header Host $host; proxy\_cache\_bypass $http\_upgrade; } }**

**启动nginx /usr/local/nginx/sbin/nginx**

**测试： curl** [**http://kibana**](http://kibana)**的ip**

六、页面检索的分类配置

**浏览器打开**[**http://kibana**](http://kibana)**的ip**

