# 1简介

ELF是由Elasticsearch、Logstash、Filebeat这3个软件的缩写。

Elasticsearch是一个分布式搜索分析引擎，稳定、可水平扩展、易于管理是它的主要设计初衷

Logstash是一个灵活的数据收集、加工和传输的管道软件

filebeat替代以前旧版本的logstash-agent，用于安装在各个主机，收集各个主机上的日志

# 2安装前的准备

## 2.1运行环境

1. JDK1.8
2. CentOS 6.8

## 2.2所需软件

elasticsearch-2.4.4.tar.gz

logstash-5.6.4.tar.gz

filebeat-5.6.4.tar.gz

### 2.2.2 elasticsearch安装

3台机器

172.20.7.49

172.20.7.50

172.20.7.51

新建/usr/lib/es

解压 tar -xzvf elasticsearch-2.4.4.tar.gz 到/usr/lib/es

新建用户组

groupadd  elk

useradd -g elk elk

chown -R elk:elk /usr/lib/es

su elsearch

cd /usr/lib/es/config

修改配置文件

修改一下参数

cluster.name: es

node.name: node-1

path.data: /tmp/es/data

path.logs: /tmp/es/logs

http.port: 9200

node.master: true

node.data: true

discovery.zen.ping.unicast.hosts: ["172.20.7.49"]

discovery.zen.minimum\_master\_nodes: 1

http.cors.enabled: true

http.cors.allow-origin: "\*"

172.20.7.50 修改一下参数

cluster.name: es

node.name: node-2

path.data: /tmp/es/data

path.logs: /tmp/es/logs

http.port: 9200

node.master: false

node.data: true

discovery.zen.ping.unicast.hosts: ["172.20.7.50"]

discovery.zen.minimum\_master\_nodes: 1

http.cors.enabled: true

http.cors.allow-origin: "\*"

172.20.7.51修改一下参数

cluster.name: es

node.name: node-3

path.data: /tmp/es/data

path.logs: /tmp/es/logs

http.port: 9200

node.master: false

node.data: true

discovery.zen.ping.unicast.hosts: ["172.20.7.51"]

discovery.zen.minimum\_master\_nodes: 1

http.cors.enabled: true

http.cors.allow-origin: "\*"

cd ../bin

nohup ./elasticsearch & 启动

浏览器打开 172.20.7.49:9200 验证是否启动成功



172.20.7.50 172.20.7.51也是如此

# 3 安装logstach

解压logstach

tar -xzvf logstash-5.6.4.tar.gz

cd logstash-5.6.4/config

新建配置文件

touch all.conf

input {

beats {

port => 5044

}

}

filter {

grok {

match => { "message" => "%{TIMESTAMP\_ISO8601:time} %{WORD:level} %{IP:client} %{GREEDYDATA:data}"}

remove\_field => ["message"]

}

date {

match => ["time", "yyyy-MM-dd HH:mm:ss"]

target => "@timestamp"

}

}

output {

elasticsearch {

hosts => ["172.20.7.49:9200","172.20.7.50:9200","172.20.7.51:9200"]

index => "log"

template => "/root/logstash-5.6.4/log.json"

template\_name => "log"

template\_overwrite => true

}

}

新建log.json

{

"template" : "log",

"order":1,

"settings" : { "index.refresh\_interval" : "5s" },

"mappings" : {

"\_default\_" : {

"\_all" : { "enabled" : false },

"dynamic\_templates" : [{

"message\_field" : {

"match" : "message",

"match\_mapping\_type" : "string",

"mapping" : { "type" : "string", "index" : "not\_analyzed" }

}

}, {

"string\_fields" : {

"match" : "\*",

"match\_mapping\_type" : "string",

"mapping" : { "type" : "string", "index" : "not\_analyzed" }

}

}],

"properties" : {

"host": {"type": "string","index": "not\_analyzed"},

"index": {"type": "string","index": "not\_analyzed"},

"type": {"type": "string","index": "not\_analyzed"},

"@timestamp" : { "type" : "date"},

"@version" : { "type" : "integer", "index" : "not\_analyzed" },

"level": {"type": "string","index": "not\_analyzed"},

"client": {"type": "string","index": "not\_analyzed"},

"data": {"type": "string","analyzer": "english"},

"time":{"type":"date","format": "yyy-MM-dd HH:mm:ss||yyyy-MM-dd||epoch\_millis"}

}

}

}

}

cd ../bin

nohup ./logstash & -f ../config/all.conf

# 4 安装filebeat

解压filebeat-5.6.4-linux-x86\_64.tar.gz

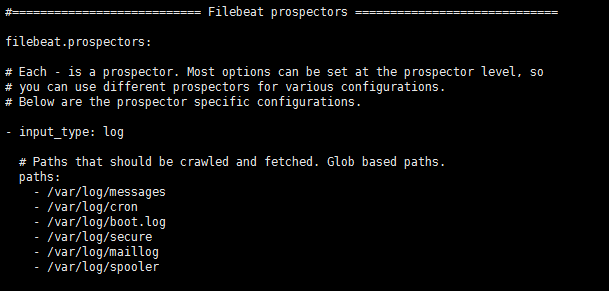
tar -xzvf filebeat-5.6.4-linux-x86\_64.tar.gz

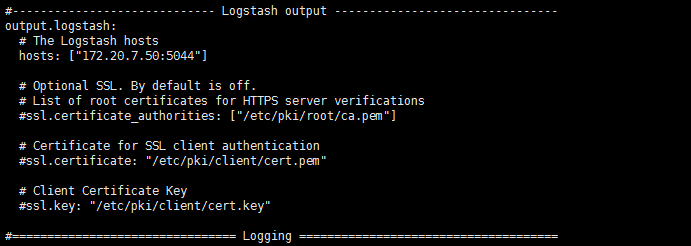
cd filebeat-5.6.4-linux-x86\_64

修改配置文件

vi filebeat.ym

配置监控改动的日志文件

发到logstach



启动

./filebeat -e -c filebeat.yml -d "publish"

至此efl完成

# 5配置syslog

Centos自带rsyslog

修改配置文件

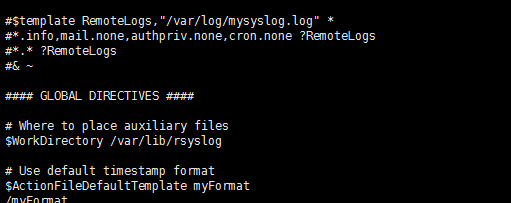
vi /etc/rsyslog.conf

自定义格式

$template myFormat,"%$NOW% %TIMESTAMP:8:15% %syslogseverity-text% %fromhost-ip% %msg%\n"

#$ActionFileDefaultTemplate myFormat

注释原有模板 使用myFormat



客户端需要开启syslog服务器地址



Rsyslog可以设置日志级别

重启syslog

service rsyslog restart