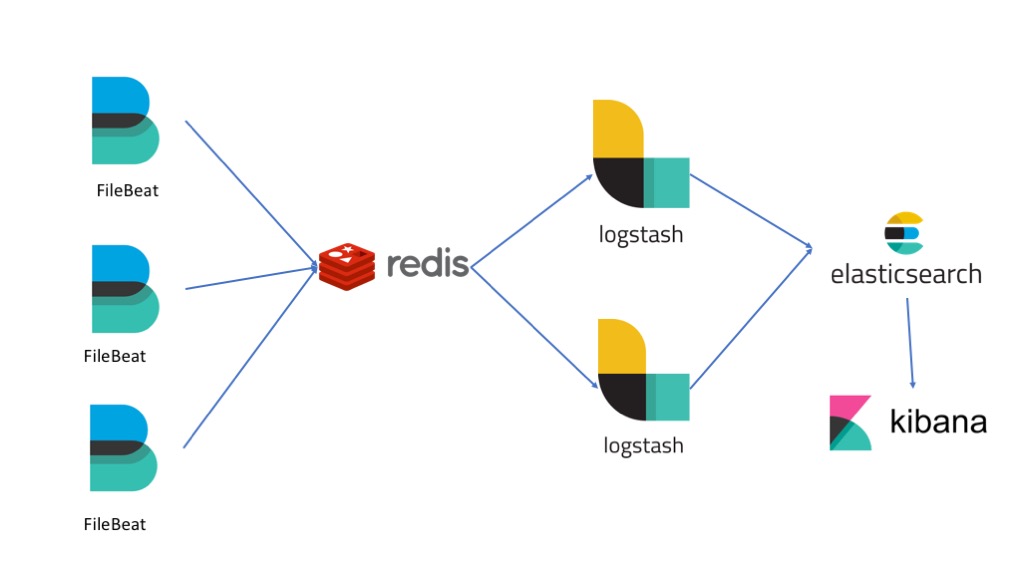
**ELK搭建手册**

2018-2-25



# 系统环境准备 beataudit

## 防火墙端口开启白名单

对指定filebeat客户端开启**17693端口**（用于日志传送）、**80端口**（仅限于公司内网访问ELK服务器）

[root@localhost ~]# firewall-cmd --permanent --new-ipset=elk\_whitelist --type=hash:ip

[root@localhost ~]# firewall-cmd --permanent --new-ipset=web\_whitelist --type=hash:ip

[root@localhost ~]# firewall-cmd --permanent --ipset=web\_whitelist --add-entry=113.61.35.0/24 ##公司内网

[root@localhost ~]# firewall-cmd --permanent --ipset=elk\_whitelist --add-entry=**filebeat客户端IP**

[root@localhost ~]# firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source ipset="elk\_whitelist" port port="17693" protocol="tcp" accept'

[root@localhost ~]# firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source ipset="web\_whitelist" port port="80" protocol="tcp" accept

[root@localhost ~]# systemctl restart firewalld

备注：

后期加filebeat客户端，需要添加17693白名单的时候，直接在elk\_whitelist添加IP即可

## **导入jdk环境变量**

[root@localhost ~]# vim /etc/profile

#######JDK环境变量########################

export JAVA\_HOME=/opt/apps/jdk

export JRE\_HOME=$JAVA\_HOME/jre

export CLASSPATH=$JAVA\_HOME/lib:$JAVA\_HOME/lib/tools.jar

export PATH=$PATH:$JAVA\_HOME/bin:$JAVA\_HOME/jre/bin

#########elk环境变量##########

export PATH=$PATH:/opt/apps/elk/elasticsearch/bin/

export PATH=$PATH:/opt/apps/elk/logstash/bin/

export PATH=$PATH:/opt/apps/elk/kibana/bin/

[root@localhost ~]# source /etc/profile

## **系统优化 ---开集群要配置**

[root@localhost ~]# vim /etc/sysctl.conf

fs.file-max = 262144

vm.max\_map\_count= 262144

[root@localhost ~]# sysctl -p

[root@MyCloudServer]# vim /etc/security/limits.conf

\* soft nproc 262144

\* hard nproc 262144

\* soft nofile 262144

\* hard nofile 262144

[root@localhost ~]# ulimit -n 262144

# **搭建ELK服务器**

## JDK环境搭建 ---需要准备JDK-8.0环境

[swadmin@localhost src]$ cd /opt/src/ && tar -xf jdk-8u121.tar.gz -C /opt/apps

## **下载ELK包到/opt/src并解压安装**

[swadmin@MyCloudServer ~]$ cd /opt/src/

[swadmin@MyCloudServer ~]$ wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.0.0.zip>

[swadmin@MyCloudServer ~]$ wget <https://artifacts.elastic.co/downloads/kibana/kibana-6.0.0-linux-x86_64.tar.gz>

[swadmin@MyCloudServer ~]$ wget <https://artifacts.elastic.co/downloads/logstash/logstash-6.0.0.zip>

[swadmin@MyCloudServer ~]$ cd /opt/src && unzip elasticsearch-6.0.0.zip && unzip logstash-6.0.0.zip

[swadmin@MyCloudServer ~]$ tar -xf kibana-6.0.0-linux-x86\_64.tar.gz

[swadmin@MyCloudServer ~]$ mv elasticsearch-6.0.0 /opt/apps/elk/elasticsearch

[swadmin@MyCloudServer ~]$ mv logstash-6.0.0 /opt/apps/elk/logstash

[swadmin@MyCloudServer ~]$ mv kibana-6.0.0-linux-x86\_64 /opt/apps/elk/kibana

## **给elastic安装geoip模块和x-pack模块**

[swadmin@localhost ~]$ source /etc/profile

[swadmin@localhost ~]$ elasticsearch-plugin install ingest-geoip ##**geoip模块**

[swadmin@localhost ~]$ kibana-plugin install x-pack

[swadmin@localhost ~]$ elasticsearch-plugin install x-pack

[swadmin@localhost ~]$ logstash-plugin install x-pack

[swadmin@localhost ~]$ /opt/apps/elk/elasticsearch/bin/x-pack/setup-passwords interactive

依次设置elasticsearch kibana logstash的密码

[swadmin@MyCloudServer ~]$ vim /opt/apps/elk/kibana/config/kibana.yml

...

server.basePath: "**/elk** ①"

elasticsearch.username: "**elastic**②"

elasticsearch.password: "**Passw0rd**③"

...

备注：

1. /elk为nginx反代的url,如http://103.68.110.223/elk
2. elastic用户名不要写其他
3. 这个密码是前面设置的elasticsearch的x-pack密码

## **破解x-pack**

**6.2.3破解：<https://www.jianshu.com/p/6acfeabb44f8>**

**主要方法：更改LicenseVerifier.class和 XPackBuild.class（6.0版本不需要）**

1. 修改java证书代码 ---- 在Windows本地上操作

Windows需要工具：luyten-0.5.0（java代码编辑器）

/opt/apps/elk/elasticsearch/plugins/x-pack/x-pack-core/**x-pack-core-6.2.3.jar**

将**x-pack-core-6.2.3.jar**包下载到Windows本地，用luyten打开，导出LicenseVerifier.class和 XPackBuild.class分别更改代码

1. LicenseVerifier.class

org.elasticresearch.license----》LicenseVerifier.class : 将此文件另外到桌面（另外后文件名自动为LicenseVerifier.java）

用notepad 编辑LicenseVerifier.java，内容如下：

package org.elasticsearch.license;

import java.nio.\*;

import java.util.\*;

import java.security.\*;

import org.elasticsearch.common.xcontent.\*;

import org.apache.lucene.util.\*;

import org.elasticsearch.common.io.\*;

import java.io.\*;

public class LicenseVerifier

{

public static boolean verifyLicense(final License license, final byte[] encryptedPublicKeyData) {

return true;

}

public static boolean verifyLicense(final License license) {

return true;

}

}

1. org.elasticsearch.xpack.core----》XPackBuild.class： 将此文件另外到桌面（另外后文件名自动为XPackBuild.java）

用notepad 编辑XPackBuild.java，内容如下：

package org.elasticsearch.xpack.core;

import org.elasticsearch.common.io.\*;

import java.net.\*;

import org.elasticsearch.common.\*;

import java.nio.file.\*;

import java.io.\*;

import java.util.jar.\*;

public class XPackBuild

{

public static final XPackBuild CURRENT;

private String shortHash;

private String date;

@SuppressForbidden(reason = "looks up path of xpack.jar directly")

static Path getElasticsearchCodebase() {

final URL url = XPackBuild.class.getProtectionDomain().getCodeSource().getLocation();

try {

return PathUtils.get(url.toURI());

}

catch (URISyntaxException bogus) {

throw new RuntimeException(bogus);

}

}

XPackBuild(final String shortHash, final String date) {

this.shortHash = shortHash;

this.date = date;

}

public String shortHash() {

return this.shortHash;

}

public String date() {

return this.date;

}

static {

final Path path = getElasticsearchCodebase();

String shortHash = null;

String date = null;

Label\_0157: {

shortHash = "Unknown";

date = "Unknown";

}

CURRENT = new XPackBuild(shortHash, date);

}

}

1. 更新java证书代码 ----- 在elk服务器上操作

将刚才在Windows本地修改的LicenseVerifier.java和XPackBuild.java上传到服务器/opt/src/bianyi，然后进行编译，并重新打包jar包

1. 编译LicenseVerifier.java和XPackBuild.java

[swadmin@localhost ~]$ cd /opt/src/bianyi/ && ls

LicenseVerifier.java XPackBuild.java

[swadmin@localhost bianyi]$ javac -cp "/opt/apps/elk/elasticsearch/lib/elasticsearch-6.2.3.jar:/opt/apps/elk/elasticsearch/lib/lucene-core-7.2.1.jar:/opt/apps/elk/elasticsearch/plugins/x-pack/x-pack-core/x-pack-core-6.2.3.jar" LicenseVerifier.java

[swadmin@localhost bianyi]$ javac -cp "/opt/apps/elk/elasticsearch/lib/elasticsearch-core-6.2.3.jar:/opt/apps/elk/elasticsearch/lib/lucene-core-7.2.1.jar:/opt/apps/elk/elasticsearch/plugins/x-pack/x-pack-core/x-pack-core-6.2.3.jar" XPackBuild.jav

1. 重新打包jar包

[swadmin@localhost bianyi]$ mkdir /opt/src/test/ && cd /opt/src/test/

[swadmin@localhost test]$ cp /opt/apps/elk/elasticsearch/plugins/x-pack/x-pack-core/x-pack-core-6.2.3.jar /opt/src/test/

[swadmin@localhost test]$ jar -xvf x-pack-core-6.2.3.jar && rm x-pack-core-6.2.3.jar

[swadmin@localhost test]$ cp /opt/src/bianyi/LicenseVerifier.class org/elasticsearch/license/

[swadmin@localhost test]$ cp /opt/src/bianyi/XPackBuild.class org/elasticsearch/xpack/core/

[swadmin@localhost test]$ jar -cvf x-pack-core-6.2.3.jar ./\*

1. 将重新打包的jar包替换之前的旧x-pack-core-6.2.3.jar包

[swadmin@localhost test]$ cp x-pack-core-6.2.3.jar /opt/apps/elk/elasticsearch/plugins/x-pack/x-pack-core/

1. 重新认证
2. 申请一个免费license

下载链接：<https://license.elastic.co/registration/download/96d3e8ef-49e7-4e6b-930a-47f695440def>

将下载好的文件max-mac-e8e90718-9333-49b6-817a-9098c35c0920-v5.json传至elk服务器/opt/src/bianyi

1. 修改license文件

[swadmin@localhost bianyi]$ cd /opt/src/bianyi/ && vim max-mac-e8e90718-9333-49b6-817a-9098c35c0920-v5.json

"type":"**platinum**"

"expiry\_date\_in\_millis":**2524579200999**

"max\_nodes":**1000**

1. 禁用x-pack 配置license有效期

更新License文件，因为elasticsearch 6.0.0，现在更新license文件时，要么配置SSL\TLS，要么就禁用security。

更新之前先配置elasticsearch.yml，加入：

[swadmin@localhost ~]$ vim /opt/apps/elk/elasticsearch/config/elasticsearch.yml

xpack.security.enabled: false

1. 启动elasticsearch，更新认证

即更新前面编辑的max-mac-e8e90718-9333-49b6-817a-9098c35c0920-v5.json认证文件）

[swadmin@localhost ~]$ elasticsearch -d

[swadmin@localhost test]$ cd /opt/src/bianyi/ && ll

max-mac-e8e90718-9333-49b6-817a-9098c35c0920-v5.json

[swadmin@localhost bianyi]$ curl -XPUT -u elastic 'http://127.0.0.1:9200/\_xpack/license?acknowledge=true' -H "Content-Type: application/json" -d @max-mac-e8e90718-9333-49b6-817a-9098c35c0920-v5.json

**出现acknowledge字符就代表成功**

1. 重启elasticsearch，检查更新

[swadmin@MyCloudServer ~]$ curl -XGET -u elastic "http://127.0.0.1:9200/\_license"

{

"license" : {

"status" : "active",

"uid" : "e8e90718-9333-49b6-817a-9098c35c0920",

"type" : "**platinum**",

"issue\_date" : "2018-02-24T00:00:00.000Z",

"issue\_date\_in\_millis" : 1519430400000,

"expiry\_date" : "**2049-12-31**T16:00:00.999Z",

"expiry\_date\_in\_millis" : 2524579200999,

"max\_nodes" : **1000**,

"issued\_to" : "max mac (SOLAIRE)",

"issuer" : "Web Form",

"start\_date\_in\_millis" : 1519430400000

}

}

## **启动elastic和kibana**

[swadmin@fc88 opt]$ cd /opt/apps/elk/

[swadmin@fc88 elk]$ elasticsearch/bin/elasticsearch &>/dev/null &

[swadmin@fc88 elk]$ kibana/bin/kibana &>/dev/null &

查看下是否启动elastic（9200端口）和kibana（5601端口）

[swadmin@fc88 elk]$ netstat -antpu |egrep "5601|9200"

tcp 0 0 103.68.110.225:**5601** 0.0.0.0:\* LISTEN 30797/../bin/../nod

tcp6 0 0 127.0.0.1:**9200**  :::\* LISTEN 30084/java

**备注：**

前面kibana进行地址重置再重启的话，需要花费好几分钟的时间才能启动成功，属于正常现象

logstash在搭完客户端后再做配置启动

## **安装kibana汉化包**

[swadmin@MyCloudServer ~]$ cd /opt/src/

[swadmin@MyCloudServer src]$ wget <https://github.com/anbai-inc/Kibana_Hanization/archive/master.zip>

swadmin@MyCloudServer src]$ unzip master.zip && mv Kibana\_Hanization-master/ /opt/apps/elk/kibana-china

[swadmin@MyCloudServer src]$ cd /opt/apps/elk/kibana-china/

[swadmin@MyCloudServer kibana-china]$ python main.py "/opt/apps/elk/kibana"

**耐心等待，安装完毕，重启kibana！！！**

## **安装并启动redis 指定端口为17693 ---略**

1. 查看key

127.0.0.1:17693> keys \* ##查看所欲key

127.0.0.1:17693> del 8hcp\_xcp ## del 8hcp\_xcp

## **配置nginx反代**

1. 安装过程 ---- 略
2. 配置

[swadmin@MyCloudServer ~]$ vim /opt/apps/nginx/conf/nginx.conf

server {

listen 80;

server\_name **ELK服务器IP或域名**;

location ^~ **/elk** ①{

rewrite /elk/(.\*)$ /$1 break;

proxy\_pass http://127.0.0.1:5601/ ;

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;

}

}

备注：

1. /elk是前面配置的kibana的url，要保持一致
2. 启动nginx --- 略

# **搭建客户端日志采集器**

## 搭建filebeat客户端

介绍资料：<http://blog.csdn.net/weixin_39077573/article/details/73467712>

### 安装filebeat

[swadmin@MyCloudServer ~]$ cd /opt/src/

[swadmin@MyCloudServer ~]$ wget <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.0.0-linux-x86_64.tar.gz>

[swadmin@MyCloudServer ~]$ tar -xf filebeat-6.0.0-linux-x86\_64.tar.gz

[swadmin@MyCloudServer ~]$ mv filebeat-6.0.0-linux-x86\_64 /opt/apps/filebeat

### **修改配置文件**

[swadmin@MyCloudServer ~]$ cd /opt/apps/filebeat/

[swadmin@MyCloudServer ~]$ cp filebeat.yml filebeat.yml.bak

[swadmin@MyCloudServer ~]$ vim filebeat.yml

filebeat.prospectors:

####nginx #######

- type: log

enabled: true

paths:

- **/opt/bet/logs/nginx/web\_access\*.log**

- **/opt/ylgj2/logs/nginx/web\_access\*.log**

fields:

log\_type: **hbet\_cyl\_nginx\_log**

**ignore\_older: 24h**  ###采集24小时以内的数据

#================================ Outputs =====================================

output.redis:

hosts: ["**103.68.110.223**:**17693**"]

data\_type: "list"

password: "**9tN6GFGK60Jk8BNkBJM611GwA66uDFeG**①"

key: "**hbet\_cyl\_nginx**②"

db: 0 #redis数据库的编号

备注：

1. 为ELK服务器redis密码
2. redis监听的键值，在logstash的input中的key要保持一致

### **启动filebeat**

[swadmin@MyCloudServer ~]$ /opt/apps/filebeat/filebeat -e -c filebeat.yml &>/dev/null &

检查下是否启动成功

[swadmin@MyCloudServer scripts]$ ps -ef |grep filebeat

swadmin **22745** 1 0 15:01 ? 00:00:00 ./**filebeat** -e -c filebeat.yml

# elasticsearch的设置

## setting

通过setting可以更改es配置可以用来修改副本数和分片数

<http://blog.csdn.net/tanga842428/article/details/60953579>

### 通过curl或浏览器查看索引、副本、分片信息

[swadmin@MyCloudServer ~]$ curl -XGET http://127.0.0.1:9200/nginx-2018.03.13/\_settings?pretty -u elastic

{ "nginx-2018.03.13" : {

"settings" : {

"index" : {

"creation\_date" : "1520899209420",

"number\_of\_shards" : "5",

"number\_of\_replicas" : "1",

"uuid" : "tGs5EcupT3W-UX-w38GYFg",

"version" : {

"created" : "6000099"

},

"provided\_name" : "nginx-2018.03.13"

}

}

}

}

备注： shards ---- 分片 replicas -- 索引 provided\_name --索引名

### map查看

<https://www.cnblogs.com/zlslch/p/6474424.html>

[swadmin@vhost-elk]$curl -XGET http://192.168.175.223:9200/java\_log-2018.03.23/\_mappings?pretty -u elastic

# 配置logstash，实现对filebeat客户端的日志管理

## 建立logstash的配置目录和data目录

[swadmin@MyCloudServer ~]$ mkdir /opt/apps/elk/logstash/conf.d/

[swadmin@MyCloudServer ~]$ mkdir /opt/apps/elk/logstash/data/hbet\_cyl\_nginx/

备注：

conf.d目录存放logstash的配置文件

data下面的新建的目录为各个站点的库，用于启动多个logstash

## 编写logstash配置文件，实现对filebeat客户端的日志检索及推送给elasticsearch

### 单个日志文件fliter

[swadmin@MyCloudServer ~]$ vim /opt/apps/elk/logstash/conf.d/hbet\_cyl\_nginx.conf

input {

redis {

data\_type => "list"

password => "9tN6GFGK60Jk8BNkBJM611GwA66uDFeG"

key => "hbet\_cyl\_nginx①"

host => "127.0.0.1"

port => 17693

threads => 5

}

}

filter {

grok {

match => [ "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra\_fields}"]

overwrite => [ "message" ]

}

mutate {

convert => ["response", "integer"]

convert => ["bytes", "integer"]

convert => ["responsetime", "float"]

}

geoip {

source => "clientip"

target => "geoip"

add\_tag => [ "nginx-geoip" ]

}

date {

match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]

remove\_field => [ "timestamp" ]

}

useragent {

source => "agent"

}

}

output {

elasticsearch {

hosts => ["127.0.0.1:9200"]

index => "hbet\_cyl\_test\_nginx②"

user => "elastic"

password => "Passw0rd③"

}

stdout { codec => "rubydebug" }

}

备注：

1. redis与filebeat客户端通信的键值，要与前面配置的一致
2. 后面kibana用来查看日志的index，用令牌码，统一格式，以便对各站点的日志进行区分
3. 前面设置的elastic x-pack的密码，要一致

### 多个日志文件fliter

参考：<https://discuss.elastic.co/t/filter-multiple-different-file-beat-logs-in-logstash/76847/4>

input {

file {

path => "/opt/src/log\_source/8hcp/gameplat\_work.2018-03-23-13.log"

start\_position => "beginning"

type => "8hcp-gameplat\_work-log"

ignore\_older => 0

}

file {

path => "/opt/src/log\_source/8hcp/tomcat\_18001/catalina.out"

start\_position => "beginning"

type => "8hcp-tomcat8001-log"

ignore\_older => 0

}

file {

path => "/opt/src/log\_source/8hcp/nginx/web\_access.log"

start\_position => "beginning"

type => "8hcp-nginx-log"

ignore\_older => 0

}

}

filter {

if ([type] =~ "gameplat" or [type] =~ "tomcat") {

mutate {

"remove\_field" => ["beat", "host", "offset", "@version"]

}

grok {

match => { "message" => "%{COMBINEDAPACHELOG}" }

tag\_on\_failure => []

}

date {

match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]

}

}

else if ([type] =~ "nginx") {

grok {

match => [ "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra\_fields}"]

overwrite => [ "message" ]

}

mutate {

convert => ["response", "integer"]

convert => ["bytes", "integer"]

convert => ["responsetime", "float"]

"remove\_field" => ["beat", "host", "offset", "@version"]

}

geoip {

source => "clientip"

target => "geoip"

database => "/opt/apps/elk/logstash/geoData/GeoLite2-City\_20180306/GeoLite2-City.mmdb"

add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]

add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]

}

date {

match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]

remove\_field => [ "timestamp" ]

}

useragent {

source => "agent"

}

}

}

output {

if ([type] =~ "gameplat") {

elasticsearch {

hosts => ["192.168.175.241:9200"]

index => "gameplat-%{+YYYY.MM.dd}"

user => "elastic"

password => "Passw0rd!\*\*yibo"

}

}

else if ([type] =~ "tomcat") {

elasticsearch {

hosts => ["192.168.175.241:9200"]

index => "tomcat-%{+YYYY.MM.dd}"

user => "elastic"

password => "Passw0rd!\*\*yibo"

}

}

else if ([type] =~ "nginx") {

elasticsearch {

hosts => ["192.168.175.241:9200"]

index => "logstash-nginx-%{+YYYY.MM.dd}"

user => "elastic"

password => "Passw0rd!\*\*yibo"

}

}

stdout {codec => rubydebug}

}

备注：

索引加时间戳： index => "%{type}-%{+YYYY.MM.dd}"

### filter插件用法

参考：<https://www.jianshu.com/p/d469d9271f19>

系统自带语法：HOME{logstash}/vendor/bundle/jruby/2.3.0/gems/logstash-patterns-core-4.1.2/patternsmutate

删除无用字段

mutate {

remove\_field => "message"

remove\_field => "@version"

}

或

mutate {

"remove\_field" => ["beat", "host", "offset", "@version"]

}

加一个字段

mutate {

add\_field => {

"web\_log" => "%{[fields][web\_log]}"

}

## **ELK服务启动logstash**

[swadmin@MyCloudServer ~]$ logstash -f /opt/apps/elk/logstash/conf.d/hbet\_cyl\_nginx.conf --path.data=/opt/apps/elk/logstash/data/hbet\_cyl\_nginx/ &>/dev/null &

稍等片刻检查是否启动成功

[swadmin@MyCloudServer ~]$ ps -ef |grep logstash

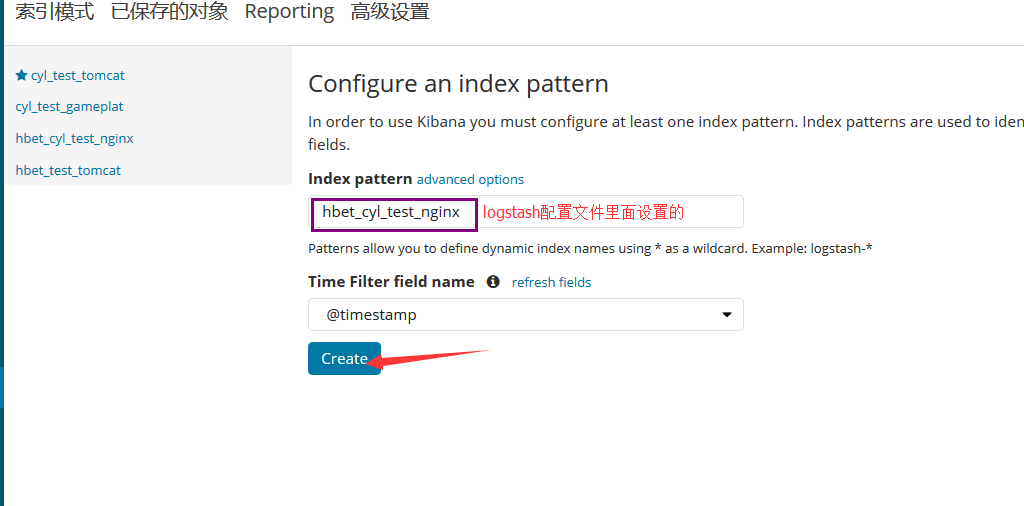
## **登录kibana查看日志信息**

1. 用浏览器登录http://103.68.110.223/elk

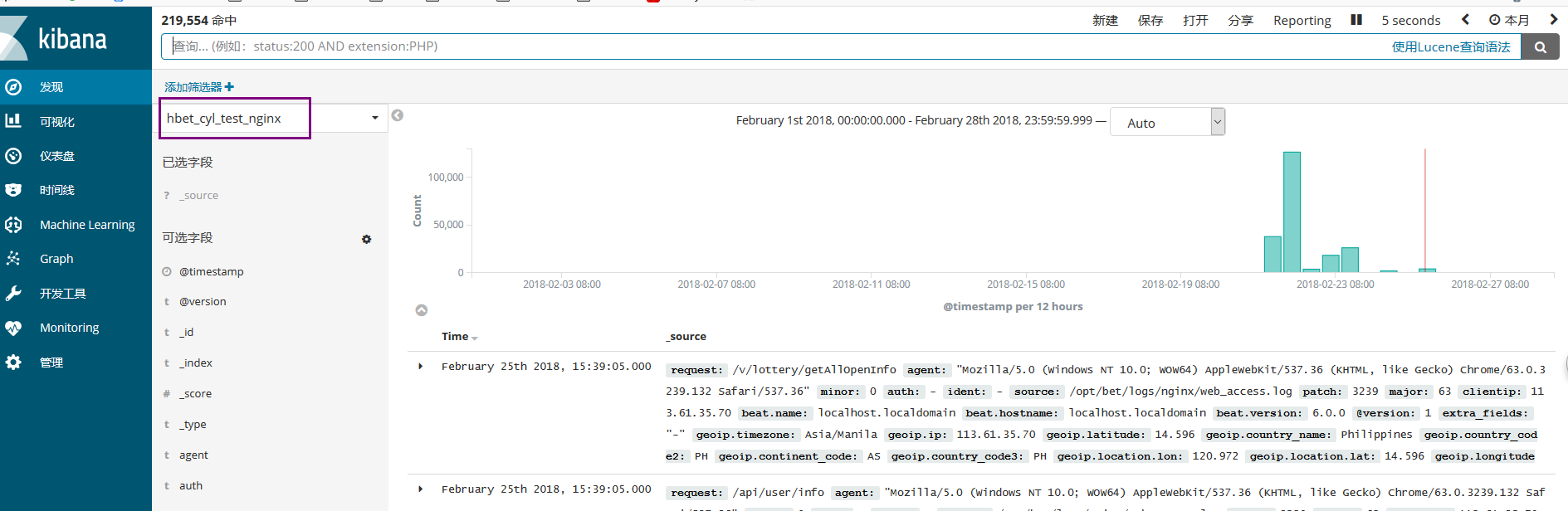
登录用户：elastic 登录密码： 前面设置的

1. 创建index

管理 ---》kibana：索引模式 ---》创建索引模式（如下图）



1. 点击发现查看日志内容



# Elk优化

## 优化指南：

删除时间范围的数据：<https://juejin.im/post/58e5de06ac502e006c254145>

ELK平台性能优化 <http://www.th7.cn/db/nosql/201708/250381.shtml>

<http://blog.csdn.net/jiao_fuyou/article/details/49783861>

Logstash优化 <http://blog.csdn.net/ypc123ypc/article/details/78033142> <https://yq.aliyun.com/articles/413002>

elasticsearch优化 <https://www.jianshu.com/p/29ffce0850af>

安装pv (pipe views） <http://blog.csdn.net/u011478909/article/details/52584935>

优化： <https://zhuanlan.zhihu.com/p/30888923> 有具体参考方法

## elasticsearch优化

1. **索引的curl管理**
2. 查看所有indices

[swadmin@MyCloudServer ~]$ curl -XGET http://127.0.0.1:9200/\_cat/indices -u elastic

1. 删除指定indices

[swadmin@MyCloudServer ~]$ curl -XDELETE "http://127.0.0.1:9200/hbet\_tomcat\_9002" -u elastic

备注：

获取7天前的日期：[swadmin@MyCloudServer ~]$ date +%Y.%m.%d --date="-7 day"

Curator ---删除indices <https://zhuanlan.zhihu.com/p/30888923>

删除索引脚本

#!/bin/bash

valite\_date=$(date +%Y.%m.%d --date="-1 day")

elastic\_ip=192.168.175.241

elastic\_port=9200

elastic\_user=elastic

elastic\_pass=Passw0rd\!\\*\\*yibo

function delete\_index(){

expect << EOF

set timeout 2

spawn curl -XDELETE http://$elastic\_ip:$elastic\_port/$1 -u $elastic\_user ;

expect {

"elastic\'\:" { send "$elastic\_pass\r" }

}

expect eof

EOF

}

##### 删除指定索引

delete\_index gameplat-$valite\_date

delete\_index tomcat-$valite\_date

delete\_index logstash-nginx-$valite\_date

1. 查看threadpool

curl -XGET 'http://localhost:9200/\_nodes/stats?pretty' -u elastic

1. 查看集群信息

curl 'http://127.0.0.1:9200/\_cluster/health?pretty' -u elastic

1. 定期删除索引数据

参考： <https://juejin.im/post/58e5de06ac502e006c254145>

1. **elasticsearch集群搭建**

参考资料：

<https://www.felayman.com/articles/2017/12/12/1513085668561.html>

<http://cwiki.apachecn.org/pages/viewpage.action?pageId=4882617>

<https://www.zybuluo.com/tinadu/note/516453>

节点1 --- master

[swadmin@MyCloudServer ~]$ cd /opt/apps/elk/elasticsearch/

[swadmin@MyCloudServer ~]$ cp config/elasticsearch.yml config/elasticsearch.yml.bak

[swadmin@MyCloudServer elasticsearch]$ grep -v \# config/elasticsearch.yml

cluster.name: my-application

node.name: node-1

path.data: /opt/apps/elk/elasticsearch/data/

path.logs: /opt/apps/elk/elasticsearch/logs/

network.host: 103.68.110.227

http.port: 9200

transport.tcp.port: 9600

node.master: true

discovery.zen.ping.unicast.hosts: ["103.68.110.227:9600", "103.68.110.242:9601"]

discovery.zen.minimum\_master\_nodes: 1

生成x-pack证书

103.68.110.223,103.68.110.225,103.68.110.227,103.68.110.242

参考资料：<https://segmentfault.com/a/1190000012789290>

[swadmin@MyCloudServer es\_crt]$ cd /opt/apps/elk/elasticsearch/config/

[swadmin@MyCloudServer elk]$ /opt/apps/elk/elasticsearch/bin/x-pack/certgen

**依次输入：my\_cluster.zip ---> my\_cluster ---> my\_cluster ---> 103.68.110.242 ---> enter ---> enter**

[swadmin@MyCloudServer config]$ unzip my\_cluster.zip

[swadmin@MyCloudServer ~]$ vim /opt/apps/elk/elasticsearch/config/elasticsearch.yml ##末行追加

################x-pack相关配置

######停用x-pack

##xpack.security.enabled: false

######所有节点进行如下配置，证书秘钥路径一定要正确

xpack.ssl.key: my\_cluster/my\_cluster.key

xpack.ssl.certificate: my\_cluster/my\_cluster.crt

xpack.ssl.certificate\_authorities: ca/ca.crt

xpack.security.transport.ssl.enabled: true

[swadmin@es\_01 config]$ ../bin/x-pack/setup-passwords interactive ###重新配置x-pack密码

节点2

[swadmin@MyCloudServer ~]$ cd /opt/apps/elk/elasticsearch/

[swadmin@MyCloudServer ~]$ cp config/elasticsearch.yml config/elasticsearch.yml.bak

[swadmin@MyCloudServer elasticsearch]$ grep -v \# config/elasticsearch.yml

cluster.name: my-application

node.name: node-2

path.data: /opt/apps/elk/elasticsearch/data/

path.logs: /opt/apps/elk/elasticsearch/logs/

network.host: 103.68.110.242

http.port: 9201

transport.tcp.port: 9601

discovery.zen.ping.unicast.hosts: ["103.68.110.227:9600", "103.68.110.242:9601"]

discovery.zen.minimum\_master\_nodes: 1

从节点1将my\_cluster 和ca目录拉过来放到/opt/apps/elk/elasticsearch/config/下

1. **其他优化**
2. 日志优化

[swadmin@MyCloudServer]$ vim log4j2.properties

logger.index\_search\_slowlog\_rolling.level = info ##默认为trace

1. 启动多个elasticsearch

<https://my.oschina.net/u/3470972/blog/1586637>

<http://knktc.com/2016/06/10/elasticsearch-multiple-instances/>

elasticsearch -Epath.conf=/opt/apps/elk/elasticsearch/config/my\_cluster/ -Ecluster.name=my\_cluster -Enode.name=node\_2

1. 开放elasticsearch给外网

[swadmin@MyCloudServer ~]$ vim /opt/apps/elk/elasticsearch/config/elasticsearch.yml

transport.host: localhost

network.host: 0.0.0.0

[swadmin@MyCloudServer]$ vim /opt/apps/elk/elasticsearch/config/jvm.options

-Xms5g

-Xmx5g

备注：内存分配物理内存1/2或1/4

[swadmin@MyCloudServer]$ vim /opt/apps/elk/elasticsearch/bin/elasticsearch

ES\_JAVA\_OPTS="-Xms6g -Xmx6g"

完整优化

<https://www.cnblogs.com/ningskyer/articles/5788667.html>

1. **禁用x-pack功能 ---有必要的时候**

[swadmin@vhost-elk ~]$ vim /opt/apps/elk/elasticsearch-01/config/elasticsearch.yml

xpack.security.enabled: false

## Logstash优化

1. 利用Pipeline启动多个管道

参考：

<http://blog.csdn.net/ypc123ypc/article/details/78033142>

<http://blog.csdn.net/ypc123ypc/article/details/69945031>

<http://blog.51niux.com/?id=205>

[swadmin@MyCloudServer]$ vim /opt/apps/elk/logstash/config/pipelines.yml

- pipeline.id: tomcat\_log

queue.type: persisted

path.config: "/opt/apps/elk/logstash/conf.d/elk\_tomcat.conf"

pipeline.workers: 6

pipeline.batch.size: 1000

pipeline.batch.delay: 5

- pipeline.id: nginx\_log

path.config: "/opt/apps/elk/logstash/conf.d/elk\_nginx.conf"

pipeline.workers: 4

pipeline.batch.size: 800

pipeline.batch.delay: 5

- pipeline.id: gameplat \_log

queue.type: persisted

path.config: "/opt/apps/elk/logstash/conf.d/elk\_gameplat.conf"

pipeline.batch.size: 1000

pipeline.batch.delay: 5

1. 内存和线程优化

[swadmin@MyCloudServer]$ vim /opt/apps/elk/logstash/config/jvm.options

-Xms6g

-Xmx6g

Logstash参数表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 参数 | 类别 | 说明 |
| 1 | LS\_HEAP\_SIZE | LS | Logstash堆内存大小，默认1g |
| 2 | -w | LS启动 | logstash线程数，默认与cpu数相同 |
| 3 | -b | LS启动 | Batch数，即logstash取多少数据进行一次filter，默认125 |
| 4 | redis.threads | LS input | Redis线程数，默认1 |
| 5 | redis.batch\_count | LS input | Redis每次pop的数量，默认1 |
| 6 | es.workers | LS output | Es提交线程，默认1 |
| 7 | es.flush\_size | LS output | ESbulk提 |
| 8 | -l | LS启动 | 产生日志文件 |

备注：

带pv启动logstash

logstash -f logstash\_dots\_zzm1.conf -l ./logstash\_zzm1.log -b 8000 | pv -abt >/dev/null

#####

再次优化索引

用一个

If ([fields][source] =~ "gameplat")

## x-pack常见参数优化

参考资料：<https://www.felayman.com/articles/2017/12/12/1513085668561.html>

# elk安全告警机制

参考：

<https://xizhibei.github.io/2017/11/19/alerting-with-elastalert/>

<https://github.com/xuyaoqiang/elastalert-dingtalk-plugin> 钉钉报警插件

<http://ksowo.com/2018/02/01/ELK%E6%8E%A5%E6%94%B6paloalto%E6%97%A5%E5%BF%97%E5%B9%B6%E7%94%A8%E9%92%89%E9%92%89%E5%91%8A%E8%AD%A6/>

钉钉添加群---》群设置----》群机器人----》添加机器人---》编辑

创建的钉钉群链接：<https://oapi.dingtalk.com/robot/send?access_token=db5c6b508ee0ffb30dfa9dc88589582f9fe5f0904def7ec8bcb4fb1c597cb436>

sudo pip install setuptools --upgrade

# GeoIP地图库

Logstash下载GeoData

[swadmin@MyCloudServer]$ cd /opt/apps/elk/logstash/ && mkdir geoData/

[swadmin@MyCloudServer logstash]$ cd geoData && wget <http://geolite.maxmind.com/download/geoip/database/GeoLite2-City.tar.gz>

[swadmin@logstash logstash]$ vim /opt/apps/elk/logstash/conf.d/elk\_nginx.conf

.....

geoip {

source => "clientip"

target => "geoip"

database => "/opt/apps/elk/logstash/geoData/GeoLite2-City\_20180306/GeoLite2-City.mmdb"

add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]

add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]

}

....

index => "**logstash-**nginx-%{+YYYY.MM.dd}"

...

备注：index必须以logstash开头

# 常见报错

1. 删掉tags的\_grokparsefailure

grok {

match => { "message" => "%{COMBINEDAPACHELOG}" }

**tag\_on\_failure => []**

}