**中车宝联日志分析系统（ELK）搭建及说明**

1. **环境：**

**JDK1.7以上**

**elasticsearch-2.3.4：搜索节点日志**

**logstash-2.3.4：管理和收集日志和事件的工具**

**kibana-4.5.3-linux-x64：功能强大的数据显示客户端**

**redis-3.2.1：缓存日志**

1. **插件：**

**Kopf；head（功能相同，通过图形化对elasticsearch进行配置）**

1. **IP：**

**192.168.1.17：服务端**

**4、搭建：**

## 安装Elasticsearch

A.解压elasticsearch-2.2.4.tar.gz

B．进入 bin目录，启动./ elasticsearch –d（后台启动）

C.测试验证，curl -X GET <http://192.168.1.17:9200>

{

"status" : 200,

"name" : "test-node1",

"cluster\_name" : "cluster",

"version" : {

"number" : "2.3.4",

"build\_hash" : "544816042d40151d3ce4ba4f95399d7860dc2e92",

"build\_timestamp" : "2015-03-23T14:30:58Z",

"build\_snapshot" : false,

"lucene\_version" : "4.10.4"

},

"tagline" : "You Know, for Search"

}

表示安装配置成功。

注：基本配置介绍../conf/ elasticsearch.yml

cluster.name: zcbl (集群名称)

node.name: node-0 (集群结点名称)

path.data: /tmp （日志目录）

path.logs: /tmp/logs （日志路径）

network.host: 192.168.1.17

http.port: 9200 (对外访问监听IP)

常用基本命令：

查询所有数据：curl <http://localhost:9200/_search?pretty>

集群健康状态：curl -XGET <http://localhost:9200/_cluster/health?pretty>

删除所有数据: curl -XDELETE 'http://localhost:9200/\_all'

删除指定索引：curl -XDELETE 'http://10.21.16.86:9200/索引名称'

## 安装Logstash

A.解压logstash-2.3.4.tar.gz。

B.进入bin目录，./logstash agent –f 配置文件 &即可。

logstash下载即可使用，命令行参数可以参考[logstash flags](http://logstash.net/docs/1.2.1/flags)，主要有

agent #运行Agent模式

-f CONFIGFILE #指定配置文件

## 安装Kibana

A．解压kibana-4.5.3-linux-x64.tar.gz

B.进入bin，启动./kibana即可。

C.登录访问：<http://192.168.1.17:5601>(默认端口为5601)

**注：可以修改kibana.yml配置elasticsearch的地址和索引**

**server.port: 5601（端口）**

**server.host: "192.168.1.17"（kibana IP）**

**elasticsearch.url: "http://192.168.1.17:9200"**

**kibana.index: ".kibana" （索引名称）**

## 安装redis

A．解压redis-3.2.1.tar.gz

B．建立链接 ln -s redis-3.2.1 redis

C．安装gcc yum install gcc

D．安装至/usr/local/下 make PREFIX=/usr/local/redis install

E．启动 /usr/local/redis/bin/redis-server ../redis.conf

注：后台启动修改redis.conf将daemonize no 改为daemonize yes

**5、集成**

首先把redis和elasticsearch都启动起来

在logstash目录下新建一个配置文件

[root@bogon logstash-2.3.4]# cat redis.conf

input {

redis {

host => "127.0.0.1"

port => "6379"

key => "logstash:demo"

data\_type => "list"

codec => "json"

type => "logstash-redis-demo"

tags => ["logstashdemo"]

}

}

output {

elasticsearch {

hosts => "192.168.1.17"

}

}

用这个配置文件启动logstash agent

./logstash agent -f redis.conf &

在redis 加一条数据

/usr/local/ redis/bin/ redis-cli

RPUSH logstash:demo "{\"time\": \"2013-01-01T01:23:55\", \"message\": \"logstash demo message\"}"

通过单独的kibana界面查看http://192.168.1.17:5601

