1:先安装jdk

### 2：安装安装 Elasticsearch注意事项：

### 不可以使用root权限。Elasticsearch所在文件夹所有者也不能是root。

### 3：kibana查看url：http://192.168.1.251:5601

**4：**Screen创建环境下运行的终端命令（长期运行）：下载screen拆件：yum install screen

### 创建终端logstash\_1：screen -S logstash\_1 进入logstash\_1：screen -r logstash\_1

### 断开环境：Ctrl+A+D 重新接管：再次进入即可。查看screen列表：screen -list

### 杀死screen：进入screen中执行exit。后台运行：nohup+命令+&

5：logstash安装：下载logstash和elasticsearch与kibana版本一致，tar zxvf logstash-5.4.0.tar.gz解压，进入config配置（新建文件）logstashtest.conf

6:启动logstash：在/root/logstash/logstash-5.4.0/下执行.  bin/logstash -f config/logstashtest.conf

问题：Could not find any executable java binary. Please install java in your PATH or set JAVA\_HOME.

解决：配置jdk JAVA\_HOME

logstash 和logstash.lib.sh 里面加上 export JAVACMD=`which java`

插件：查看可用插件：./logstash-plugin list 插件下载：在bin目录下./logstash-plugin install logstash-output-email

input {

#输入

}

filter {

#过滤匹配

}

output {

#输出

}

A:输入插件input：标准输入（指在命令行中输入什么就输出什么）：stdin

文件输入（即从文件中读取并输出）：file 可以指定监听时间discover\_interval:，指定开始读取文件的位置start\_position,默认是结束位置，可以配置编解码：codec

递归子目录写法：path=>[“/path/logs/\*\*/\*.log”.]

B:过滤匹配filter：转换时间格式date；正则捕获grok；获取ip所属信息geoip；json编解码json； Key-value提供去重功能。速率阈值检测metrics监测日志的异常状态码频率。Mutate数据修改：类型装换convert，字符串处理如切割，拼接，合并，去除空格，大小写转换，字段处理如重命名。

C：输出插件：输出到elasticsearch；发送email报警（应该加入判断条件）；保存为文件file；

标准输出stdout；输出到hdfs

D：性能测试：一般11kb/s；

E：心跳监测：heartbeat；

F：读取redis数据：redis；建议使用pattern\_channel作为插件的data\_type设置值。

7：elasticsearch安装：下载.tar文件版本5，执行tar xzvf elasticsearch-5.4.0.tar.gz解压

修改配置vi config/elasticsearch.yml

cluster.name=es\_cluster

node.name=node0

path.data=/tmp/elasticsearch/data

path.logs=/tmp/elasticsearch/logs

#当前hostname或IP，我这里是centos2

network.host=centos2

network.port=9200

启动：进入bin目录执行./elasticsearch ；查看进程：ps -ef | grep elastic后kill进程

集群监控：curl -XGET 127.0.0.1:9200/\_cluster/health?level=indices或curl -XGET 127.0.0.1:9200/\_cluster/health?pretty

查看分片状态：curl -XGET http://127.0.0.1:9200/\_cat/shards?v

监控节点性能：从github上克隆bigdesk：git clone <https://github.com/lukas-vlcek/bigdesk> ;后进入bigdesk目录执行python -mSimpleHTTPServer启动bigdesk服务，之后进入elasticsearch下bin启动elasticsearch，在浏览器打开<http://192.168.1.251:8000>查看你要查看的节点状况。

集群搭建：保证集群中的机器位于同一局域网下，在所有config下的elasticsearch.yml中配置相同的cluster.name ，不同的http.port，network.host都为0.0.0.0即可,子节点需将 node.master 设置为 false

Elasticsearch数据存放在lib/data下

常见问题：警告1：max file descriptors [4096] for elasticsearch process likely too low, increase to at least [65536] 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: liuqing hard nofile 65536

liuqing soft nofile 65536

警告2：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 后重新登录liuqing用户，启动elasticsearch即可

**启动报错：J**ava HotSpot(TM) 64-Bit Server VM warning: INFO: os::commit\_memory(0x0000000085330000, 2060255232, 0) failed; error='Cannot allocate memory' (errno=12) ：因为虚拟机内存最大为1g

1. # vim config/jvm.options
2. -Xms2g
3. -Xmx2g 修改为
4. -Xms512m
5. -Xmx512m

设置elasticsearch内存的大小如上或export ES\_HEAP\_SIZE=10g，一般是机器内存的一半，但不要超过32g。一般当分给elasticsearch的内存小于8g就会有问题。

OpenJDK 64-Bit Server VM warning: If the number of processors is expected to increase from one, then you should configure the number of parallel GC threads appropriately using -XX:ParallelGCThreads=N

Exception in thread "main" ElasticsearchParseException[malformed, expected settings to start with 'object', instead was [VALUE\_STRING]]

at org.elasticsearch.common.settings.loader.XContentSettingsLoader.load(XContentSettingsLoader.java:73)

at org.elasticsearch.common.settings.loader.XContentSettingsLoader.load(XContentSettingsLoader.java:52)

at org.elasticsearch.common.settings.loader.YamlSettingsLoader.load(YamlSettingsLoader.java:50)

at org.elasticsearch.common.settings.Settings$Builder.loadFromStream(Settings.java:1037)

at org.elasticsearch.common.settings.Settings$Builder.loadFromPath(Settings.java:1026)

at org.elasticsearch.node.InternalSettingsPreparer.prepareEnvironment(InternalSettingsPreparer.java:100)

at org.elasticsearch.cli.EnvironmentAwareCommand.createEnv(EnvironmentAwareCommand.java:72)

at org.elasticsearch.cli.EnvironmentAwareCommand.execute(EnvironmentAwareCommand.java:67)

at org.elasticsearch.cli.Command.mainWithoutErrorHandling(Command.java:122)

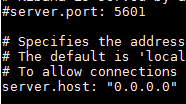
at org.elasticsearch.cli.Command.main(Command.java:88)

at org.elasticsearch.bootstrap.Elasticsearch.main(Elasticsearch.java:91)

at org.elasticsearch.bootstrap.Elasticsearch.main(Elasticsearch.java:84)

配置文件中符号错误或者配置参数时加个空格

8：kibana安装下载.tar文件版本5，执行tar xzvf kibana-5.4.0-linux-x86\_64.tar.gz

解压，进入config目录执行vi kibana.yml，修改server.host即可

启动：先启动elasticsearch，后执行llbin/kibana；在网页查看<http://192.168.1.251:5601>

Logstash简易配置：

[ayue@localhost config]$ vi logstashtest.conf

input {

log4j {

host => "0.0.0.0"

port => 4560

}

}

数据类型强转

filter{

if "com.rhea.ws.game.core.task.CoreTaskHandler" in [path]{

mutate{

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

}

}

}

output {

stdout {

codec => rubydebug

}

if "com.rhea.ws.game.chat.cmd.CreatePostHandler18012" in [path]{

elasticsearch{

hosts => ["localhost:9200"]

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

}

}

else if "com.rhea.ws.game.battle" in [path]{

elasticsearch{

hosts => ["localhost:9200"]

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

}

}

else {

elasticsearch{

hosts => ["localhost:9200"]

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

document\_type => "log4j\_type"

}

}

}

Json格式处理，可以将json的key作为字段展示出来，以达到只查看value的效果（如查看在线玩家）

filter{

json{

source => "message"

#target => "doc"

#remove\_field => ["message"]

}

}

Grok正则捕获：

filter{

if "当前在线人数" in [message]{

grok{

match=>{

"message" =>"(?<online>-?[0-9]\d\*?)"

}

}

mutate{

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

}

}

}

input {

file {

path => "/var/log/messages" start\_position => "beginning"

}

}

文件输入，将start\_position设置为beginning，则会从头读取文件，下次启动如果elasticsearch中已经包含了前面的内容则会从从新文件处开始读取

发邮件配置

if "协议-9017-报错" in [message]{

email{

port => "465"

address => "smtp.qq.com"

username => "1759467285@qq.com"

password =>"rcmmwxlgfhvoccjb"

authentication => "plain"

use\_tls =>false

from => "1759467285@qq.com"

subject=>"aaaaaaaaaaa"

to => "fengyuexiao@rheagame.com"

via=>"smtp"

body=>"bbbbbbbbbbbbbbb"

}

}

1. 查看elasticsearch的索引：curl 'localhost:9200/\_cat/indices?v'

Log4j配置：

Properties配置

### \u8BBE\u7F6E###

log4j.rootLogger = debug,stdout,D,E,logstash

### \u8F93\u51FA\u4FE1\u606F\u5230\u63A7\u5236\u62AC ###

log4j.appender.stdout = org.apache.log4j.ConsoleAppender

log4j.appender.stdout.Target = System.out

log4j.appender.stdout.layout = org.apache.log4j.PatternLayout

log4j.appender.stdout.layout.ConversionPattern = [%-5p] %d{yyyy-MM-dd HH:mm:ss,SSS} method:%l%n%m%n

### \u8F93\u51FADEBUG \u7EA7\u522B\u4EE5\u4E0A\u7684\u65E5\u5FD7\u5230=/Users/bee/Documents/elk/log4j/debug.log###

log4j.appender.D = org.apache.log4j.DailyRollingFileAppender

log4j.appender.D.File = /Users/bee/Documents/elk/log4j/debug.log

log4j.appender.D.Append = true

log4j.appender.D.Threshold = DEBUG

log4j.appender.D.layout = org.apache.log4j.PatternLayout

log4j.appender.D.layout.ConversionPattern = %-d{yyyy-MM-dd HH:mm:ss} [ %t:%r ] - [ %p ] %m%n

### \u8F93\u51FAERROR \u7EA7\u522B\u4EE5\u4E0A\u7684\u65E5\u5FD7\u5230=/Users/bee/Documents/elk/log4j/error.log ###

log4j.appender.E = org.apache.log4j.DailyRollingFileAppender

log4j.appender.E.File =/Users/bee/Documents/elk/log4j/error.log

log4j.appender.E.Append = true

log4j.appender.E.Threshold = ERROR

log4j.appender.E.layout = org.apache.log4j.PatternLayout

log4j.appender.E.layout.ConversionPattern = %-d{yyyy-MM-dd HH:mm:ss} [ %t:%r ] - [ %p ] %m%n

#\u8F93\u51FA\u65E5\u5FD7\u5230logstash

log4j.appender.logstash=org.apache.log4j.net.SocketAppender

log4j.appender.logstash.RemoteHost=192.168.138.128

log4j.appender.logstash.port=4560

log4j.appender.logstash.ReconnectionDelay=60000

log4j.appender.logstash.LocationInfo=true

xml配置

<log4j:configuration xmlns:log4j=" http://jakarta.apache.org/log4j/" >

<appender name="ConsoleAppender" class="org.apache.log4j.ConsoleAppender" >

<layout class="org.apache.log4j.PatternLayout" >

<param name="ConversionPattern" value="%d{yyyy/MM/dd-HH:mm:ss} >> %5p >> %t >> %l >> %m%n" />

</layout>

</appender>

<appender name="socketAppender" class="org.apache.log4j.net.SocketAppender">

<param name="remoteHost" value="localhost" />

<param name="port" value="4560" />

<param name="Threshold" value="INFO" />

<param name="ReconnectionDelay" value="1000" />

<param name="LocationInfo" value="true" />

</appender>

<root>

<priority value="info" />

<appender-ref ref="ConsoleAppender" />

<appender-ref ref="sockethubAppender" />

</root>

</log4j:configuration>

**Logstash启动时报错：**

**[logstash.outputs.elasticsearch] Attempting to install template {:manage\_template=>{"template"=>"logstash-\*", "version"=>50001, "settings"=>{"index.refresh\_interval"=>"5s"}, "mappings"=>{"\_default\_"=>{"\_all"=>{"enabled"=>true, "norms"=>false}, "dynamic\_templates"=>[{"message\_field"=>{"path\_match"=>"message", "match\_mapping\_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}}, {"string\_fields"=>{"match"=>"\*", "match\_mapping\_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"keyword"=>{"type"=>"keyword"}}}}}], "properties"=>{"@timestamp"=>{"type"=>"date", "include\_in\_all"=>false}, "@version"=>{"type"=>"keyword", "include\_in\_all"=>false}, "geoip"=>{"dynamic"=>true, "properties"=>{"ip"=>{"type"=>"ip"}, "location"=>{"type"=>"geo\_point"}, "latitude"=>{"type"=>"half\_float"}, "longitude"=>{"type"=>"half\_float"}}}}}}}}**

**解决：可能是配置文件中含有多余空格，将文件删掉重写，处字符间外不要带空格**

**基本就是符号不正确**

**Elasticsearch存储原理：新文件存到内存buffer中，同时记录到translog日志中，每5秒刷新translog日志到磁盘，之后buffer生成新的segment（断）刷到文件系统缓存中，lucene检索新segment；每隔30分钟或是translog文件大于512M时进行一次flush（吧segment刷到磁盘，translog清空）**

# Logstash处理json格式日志文件的三种方法：

<https://blog.csdn.net/jiao_fuyou/article/details/49174269>

Kibana5数据查询功能

<https://www.cnblogs.com/bugsbunny/p/7248386.html>

Kibana5数据查询语法

<https://blog.csdn.net/gb4215287/article/details/77101328>

[logstash修改字段类型](https://blog.csdn.net/sxf_123456/article/details/77857155)

https://blog.csdn.net/sxf\_123456/article/details/77857155

**"当前在线人数" AND [0 TO 200]**

**elasticsearch删除索引**curl -XDELETE 'http://172.16.1.16:9200/logstash-2013.03.\*'

Elasticseach会有后台线程根据Lucene的合并规则定期进行[segment merging](https://www.elastic.co/guide/en/elasticsearch/guide/current/merge-process.html" \t "_blank)合并操作，一般不需要用户担心或者采取任何行动。

强制Elasticsearch进行segment merging，已释放其占用的大量系统资源。

       curl -XPOST 'http://localhost:9200/searchrecord/\_forcemerge?only\_expunge\_deletes=true'

**centos7**

firewall-cmd --reload #重启firewall

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）

**elasticsearch压测：机器4g内存，es2g：当在短时间内插入10m左右的日志后就开始进行频繁GC导致无法插入但依旧可以查询**

**rcmmwxlgfhvoccjb**