http://comments.gmane.org/gmane.comp.sysutils.logstash.user/3496 //Jruby

http://www.linuxidc.com/Linux/2008-01/10559.htm //Java Update

bin/elasticsearch -Des.insecure.allow.root=true (解决root不能启动)

***Update JDK***

   JAVA\_HOME=/home/ipsp/ELK/jre1.8.0\_74

   PATH=$PATH:/$JAVA\_HOME/bin

   CLASSPATH=.:$JAVA\_HOME/lib

   JRE\_HOME=$JAVA\_HOME/jre

   export JAVA\_HOME PATH CLASSPATH JRE\_HOME

mv  /usr/bin/java   /usr/bin/java.bak

ln -s -f /home/ipsp/ELK/jre1.8.0\_74/bin/java   /usr/bin/java

 ln -s -f /home/ipsp/ELK/jre1.8.0\_74/bin/javac    /usr/bin/javac

***Useful Command:***

curl 'http://localhost:9200/\_search?pretty'

netstat -anp |grep :9200

ps aux |grep elasticsearch|grep -v grep|cut -c 9-15

ps aux |grep logstash|grep -v grep|cut -c 9-15

***Logstash Command:***

logstash -e 'input{file{path => ["/home/ipsp/log/test.log","/home/ipsp/server/\*.log"] start\_position => "beginning"}} output{elasticsearch{hosts => "168.33.130.220:9200"}}'

logstash -e 'input{file{path => "/home/ipsp/log/test.log" start\_position => "beginning"}} output{stdout{}}'

logstash -e 'input{file{path => "/home/ipsp/server/SC0001.log" start\_position => "beginning" tags=>"SC0001" codec => plain{charset => "GB2312"}} file{path => "/home/ipsp/server/SC0002.log" start\_position => "beginning" tags=>"SC0002" codec => plain{charset => "GB2312"}}} output{elasticsearch{hosts => "168.33.130.220:9200" codec => plain{charset => "GB2312"}}}'

***Elastic Command:***

索引查询：

http://168.33.130.221:9200/\_search?pretty

集群状态：

http://168.33.130.221:9200/\_cat/health?v

集群节点：

http://168.33.130.221:9200/\_cat/nodes?v

结群索引：

http://168.33.130.221:9200/\_cat/indices?v

插入索引：

curl -XPUT 'localhost:9200/logstash-2016.03.11?pretty'

删除索引：

curl -XDELETE 'localhost:9200/logstash-2016.03.11?pretty'

更新：

curl -XPOST 'localhost:9200/customer/external/1/\_update?pretty' -d '

删除文档：

curl -XDELETE 'localhost:9200/customer/external/2?pretty'

{

"doc": { "name": "Jane Doe", "age": 20 }

}'

curl -XPOST 'localhost:9200/logstash-2016.03.11/\_search?pretty' -d '

{

"query": { "match\_all": {} }

}'

curl -XGET 'localhost:9200/logstash-2016.03.09/logs/\_search?q=\*&?pretty'

***Plugin installation：***

./plugin --url file:///home/ipsp/ELK/bigdesk-master.zip --install bigdesk

./plugin --url file:///home/ipsp/ELK/head-master.zip --install head

./plugin --url file:///home/ipsp/ELK/marvel-latest.zip --install marvel

***Start Plugins：***

http://168.33.130.220:9200/\_plugin/bigdesk

http://168.33.130.220:9200/\_plugin/marvel

http://168.33.130.220:9200/\_plugin/head/

HEAD:

http://168.33.130.220:9200/logstash-2016.03.14/logs/

/\_search?q=message:接收到

***Elasticsearch restart:***

重启前：

curl -PUT [http://XXX:9200/\_cluster/settings](http://10.10.11.121:9200/_cluster/settings) -d

{  
  "transient": {  
    "cluster.routing.allocation.enable": "none"  
  }  
}

重启后：

{  
                "transient" : {  
                    "cluster.routing.allocation.enable" : "all"  
                }  
 }