**ELK笔记**

1. curl使用注意点：

在window的cmd窗口下，使用curl时都把单引号（‘）改成用双引号（“），原来的双引号（“）改成用三个双引号（”””）

示例：

错误（按正常教程）:

curl -XPOST "localhost:9200/books/solr/1" -d "{"title":"Apache Solr 4 Cookbook", "published": 2012}"

正确：

curl -XPOST "localhost:9200/books/solr/1" -d "{"""title""":"""Apache Solr 4 Cookbook""", """published""": 2012}"

1. curl中在引号里面如果有空格可能会存在问题，具体原因还不清楚。
2. Kibana自带了类似于curl的工具，我TM之前怎么就没发现呢！这个Kibana自带的工具比curl不知道好用多少倍啊！

启动logstash：cmd-> set JAVA\_HOME = E:/JAVA8 -> logstash -f logstash-jdbc.conf

# Logstash

logstash -f logstash-file-jeesite.conf

要退出logstash必须关闭cmd终端，exit指令关闭无法杀死后台进程！

取message信息，行

codec => line {

format => "%{message}"

}

中文乱码:默认是UTF-8，改成GB2312，UTF-8也可以。

文件的encode最好和charset 相对应。

charset 只对plain 有用。

cmd终端输入的中文字符，可能存在乱码问题，要用codec charset转换字符集。

stdin {

codec => plain {

charset => "GB2312"

}

}

Input的file插件path在windows下必须是”/”，不能是”\”.

示例1：

input { file {

#监听文件的路径

path => ["E:/software/logstash-1.5.4/logstash-1.5.4/data/\*","F:/test.txt"]

#排除不想监听的文件

exclude => "1.log"

#添加自定义的字段

add\_field => {"test"=>"test"}

#增加标签

tags => "tag1"

#设置新事件的标志

delimiter => "\n"

#设置多长时间扫描目录，发现新文件

discover\_interval => 15

#设置多长时间检测文件是否修改

stat\_interval => 1

#监听文件的起始位置，默认是end

start\_position => beginning

#监听文件读取信息记录的位置

sincedb\_path => "E:/software/logstash-1.5.4/logstash-1.5.4/test.txt"

#设置多长时间会写入读取的位置信息

sincedb\_write\_interval => 15

}

}

filter {

}

output {

stdout {}

}

示例2

input {

stdin {

codec => plain {

charset => "GB2312"

}

}

file {

path => "E:/ELK/TestData/TestLog/\*.log"

codec => plain {

charset => "UTF-8"

}

}

}

filter {

}

output {

stdout {

codec => rubydebug

}

file {

path => "E:/ELK/TestData/Result/%{+yyyy-MM-dd}/jeesite2.txt"

}

}

处理分行（以日期分行：2016-01-15 16:54:45,821 [）：

codec => multiline {

pattern => "^\d{4}-\d{2}-\d{2}\s\d{2}\:\d{2}\:\d{2}\,\d{3}\s\["

negate => true

what => "previous"

}

启动Logstash失败：

ERROR logstash.agent - failed to fetch pipeline configuration {:message=>"The following config files contains non-ascii characte rs but are not UTF-8 encoded

reason=>Expected one of #, input, filter, output at line 2, column 1 (byte 2): Logstash

解决方案：logstash.conf 文件需要转为UTF-8无BOM格式！

注意：在logstash启动之后再去log文件夹目录下新增log文件，logstash才会增量的读取数据。

# Kibana

Discover -> Visualize -> Dashboard

Discover :查看es数据

Visualize ：画图

Dashboard：可以将Visualize 画好的图汇总到一起展示