14、Logstash采集输送日志input filter output流程测试

简介：讲解Logstash采集日志和输送日志流程测试,包括input，filter和output元素的测试

bin/logstash -f test1.conf

./logstash -f ../config/test1.conf

codec的使用( Coder/decoder 两个单词首字母缩写）

Codec: 解码编码 数据格式

好处 更方便logstash与支持自定义数据格式的运维产品进行使用

logstash更细化的处理流程

input->decode->filter->encode->output

配置一 test1.conf

========================================

input {

# 从文件读取日志信息 输送到控制台

file {

path => "/Users/jack/Desktop/person/elk/elasticsearch-6.1.1/logs/elasticsearch.log"

#codec => "json" ## 以JSON格式读取日志

type => "elasticsearch"

start\_position => "beginning"

}

}

# filter {

#

# }

output {

# 标准输出

# stdout {}

# 输出进行格式化，采用Ruby库来解析日志

stdout { codec => rubydebug }

}

========================================

filter使用

例子

切割插件mutate，随意输入一串以|分割的字符，比如 "123|000|ttter|sdfds\*=123|dfwe

配置二 test2\_filter.conf

========================================

input {

stdin {}

}

filter {

mutate {

split => ["message", "|"]

}

}

output {

# 标准输出

# stdout {}

# 输出进行格式化，采用Ruby库来解析日志

stdout { codec => rubydebug }

}

========================================