15、logstash案例实战之读取日志输出到elasticsearch

简介：从日志文件中读取日志，输出到elasticsearch集群中

logstash配置文件

配置三 test3\_es.conf

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

input {

file {

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

type => "elasticsearch"

start\_position => "beginning" #从文件开始处读写

}

}

output{

elasticsearch{

hosts=>["127.0.0.1:9201"]

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

}

stdout{codec => rubydebug}

}

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

验证

查看索引列表 http://localhost:9201/\_cat/indices?v

查看数据 http://localhost:9201/es-message-2018.02.26/\_search