12、Logstash插件介绍

简介：讲解input,filter和output的插件的基本使用

简单的配置 test.conf

#===================================

input {

# 从文件读取日志信息

file {

path => "/var/log/messages"

type => "system"

start\_position => "beginning"

}

}

filter {

}

output {

#标准输出

elasticsearch {

hosts => ["localhost:9200"]

index => "logstash-test-%{type}-%{host}"

}

}

#===================================

input插件：https://www.elastic.co/guide/en/logstash/current/input-plugins.html

file，http，kafka，rabbitmq等

filter插件：https://www.elastic.co/guide/en/logstash/current/filter-plugins.html

grok(号称将非标准化的日志数据转换成标准化并且可搜索数据最好的方式，常用于处理Niginx，sysLog等日志)

drop(跳过某些日志，不进入output)

geoip(获取地理信息)

output插件：https://www.elastic.co/guide/en/logstash/current/output-plugins.html

elasticSearch,cvs,email,file等