Waf节点

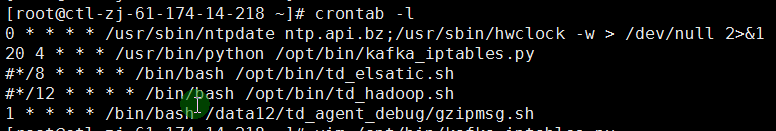
Waf节点生成了日志，有两种方式

一个是

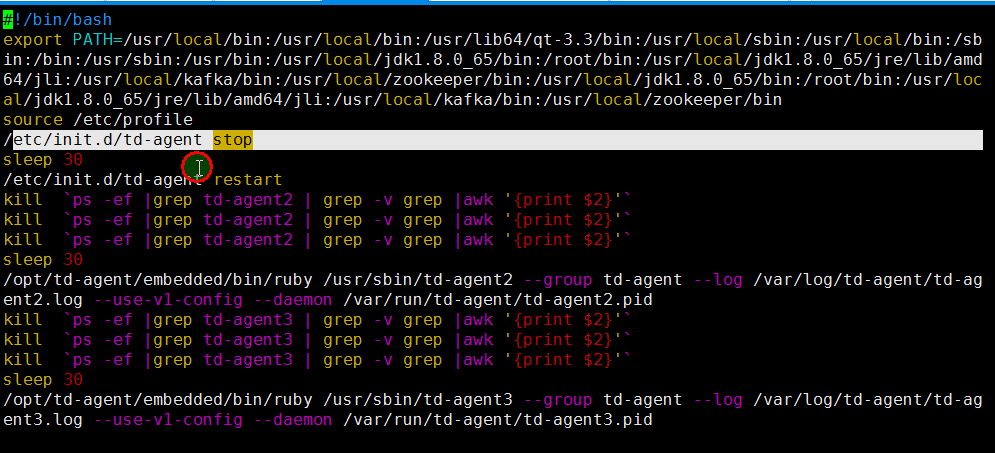
通过Rsyslog传到9.66上面

通过在/usr/local/ndserver/nginx/conf/mod的/etc/rsyslog.conf传到了

kafka里面



/opt/bin/td\_elsatic.sh



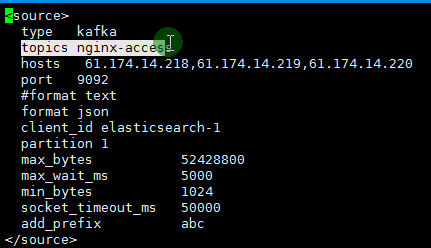
Td\_agent启动后有两个进程

这两个进程一个向td\_elsatic.sh写，一个向td\_hadoop.sh写

为什么会生成3个td\_agent

因为生产的日志速度大于传输的速度，传输的速度又瓶颈，所以要起3个

td\_agent的配置文件在/etc/td-agent/td\_agent

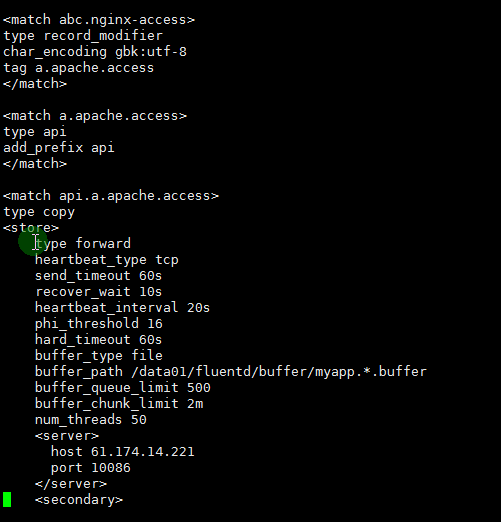


Type模块 使用kafka模块

Hosts从哪里读取kafka日志流

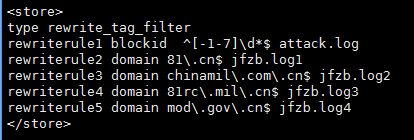
Port端口

add\_prefix 添加前缀abc

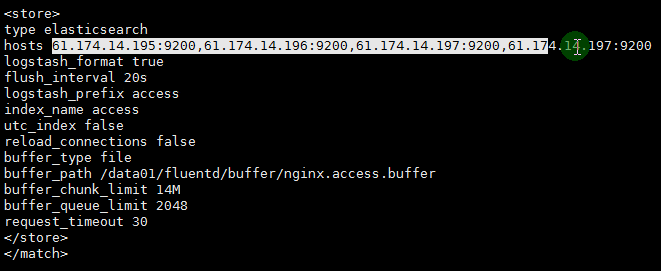


61.174.14.221 写日志的服务器

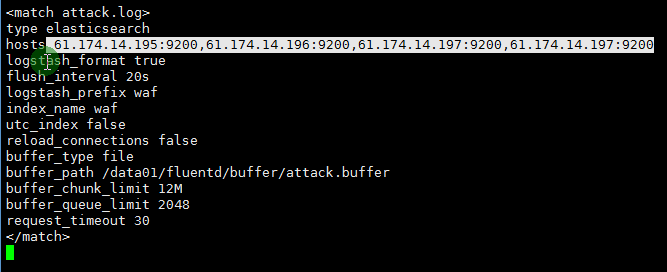
定义攻击日志，和解放军报日志



es日志



定义的攻击日志写入



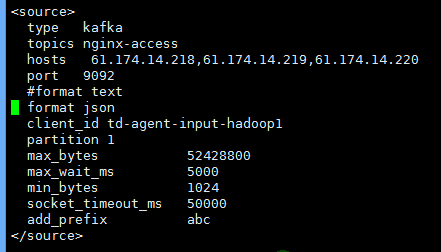
定义的军网日志写入



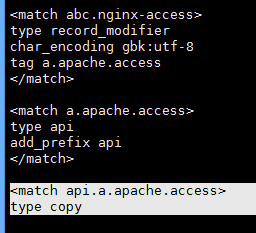
Hadoop

例如61.174.14.218

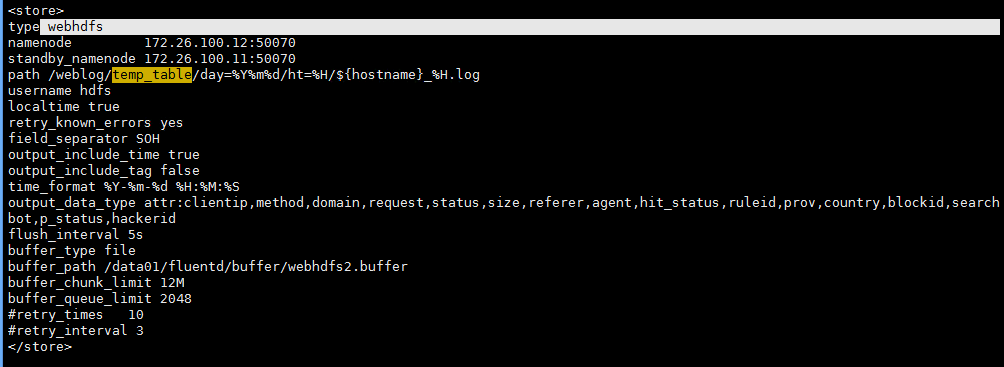
路径:/etc/td\_agent/td-agenthadoop1.conf



预处理



向hadoop里面去写



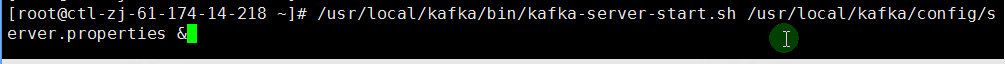
我们的kafka有多少个分区



用这个命令查看nginx-access

Kafka怎么启动的

ll /usr/local/kafka/bin/kafka-server-start.sh 启动脚本



Kafka配置文件/usr/local/kafka/config/consumer.properties

server.properties



14.218, 14.219, 14.220 通过zookeeper.connect搭成集群的

Kafka通过td\_agent传入到es里