****>客户端****

**1、安装redis**

**2、安装filebeat**

|  |
| --- |
| wget <https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.3.0-x86_64.rpm>  rpm -ivh filebeat-6.3.0-x86\_64.rpm |

**配置filebeat(收集nginx)**

/etc/filebeat/filebeat.yml

|  |
| --- |
| filebeat.prospectors:  - input\_type: log  paths:  - /data/nginx/logs/gateway/access.log  tags: ["pfgw65\_stag\_nginx\_access"]  fields:  service: pfgw65\_stag\_nginx\_access  exclude\_lines: '\.(gif|css|js|ico) HTTP'  tail\_files: true #Filebeat从文件尾开始监控文件新增内容，非从头开始    output.redis:  hosts: ["172.31.131.14:12001"]  db: 0  timeout: 5  key: "default\_list" |

重要参数解释：

input\_type：指定输入的类型是log或者是stdin

paths：慢日志路径，支持正则，比如/data/\*.log

exclude\_lines：过滤掉# Time开头的行

multiline.pattern：匹配多行时指定正则表达式，这里匹配以# Time或者# User开头的行，Time行要先匹配再过滤

multiline.negate：定义上边pattern匹配到的行是否用于多行合并，也就是定义是不是作为日志的一部分

multiline.match：定义如何将皮排行组合成时间，在之前或者之后

tail\_files：定义是从文件开头读取日志还是结尾，这里定义为true，从现在开始收集，之前已存在的不管

name：设置filebeat的名字，如果为空则为服务器的主机名，这里我们定义为服务器IP

output.kafka：配置要接收日志的kafka集群地址可topic名称

**启动filebeat**

|  |
| --- |
| **service filebeat start** |

**查看日志**

|  |
| --- |
| **tail -f /var/log/filebeat/filebeat** |

****>服务端****

**1、安装jdk**

**2、安装ElasticSearch**

**注意：ElasticSearch数据量可能很大，会占用大量磁盘空间，建议另建一个磁盘用以存放ElasticSearch数据。**

**ES启动的时候回占用特别大的资源所以需要修改下系统参数,若不修改资源启动会异常退出**

修改系统参数：

|  |
| --- |
| vim /etc/sysctl.conf  #添加参数  vm.max\_map\_count=655360  sysctl –p |

.修改资源参数：

|  |
| --- |
| vim /etc/security/limits.conf  #修改  \* soft nofile 65536  \* hard nofile 131072  \* soft nproc 65536  \* hard nproc 131072 |

|  |
| --- |
| useradd elk  groupadd elk  useradd elk -g elk  mkdir /home/elk/{data,logs}  wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.3.0.tar.gz  tar xf elasticsearch-6.3.0.tar.gz -C /usr/local/  chown -R elk.elk /home/elk  chown -R elk.elk /usr/local/elasticsearch-6.3.0  vim /usr/local/elasticsearch-6.3.0/config/elasticsearch.yml |
| #这里指定的是集群名称，需要修改为对应的，开启了自发现功能后，ES会按照此集群名称进行集群发现  cluster.name: ht-es  node.name: esnode-1  #目录需要手动创建  path.data: /home/elk/data  path.logs: /home/elk/logs  #ES监听地址任意IP都可访问  network.host: 0.0.0.0  http.port: 9200  #若是集群，可在里面引号中添加，逗号隔开  discovery.zen.ping.unicast.hosts: ["172.60.51.94"]  # enable cors，保证\_site类的插件可以访问es  http.cors.enabled: true #手动添加  http.cors.allow-origin: "\*" #手动添加  # Centos6不支持SecComp，而ES5.2.0默认bootstrap.system\_call\_filter为true进行检测，所以导致检测失败，失败后直接导致ES不能启动  bootstrap.memory\_lock: false #手动添加  bootstrap.system\_call\_filter: false #手动添加 |

**启动es**

|  |
| --- |
| su -elk && cd /usr/local/elasticsearch-6.3.0/bin/  ./elasticsearch -d |

**查看Elasticsearch状态**

|  |
| --- |
| http://172.60.51.94:9200/ |

**查看elasticsearch是否接收到了数据**

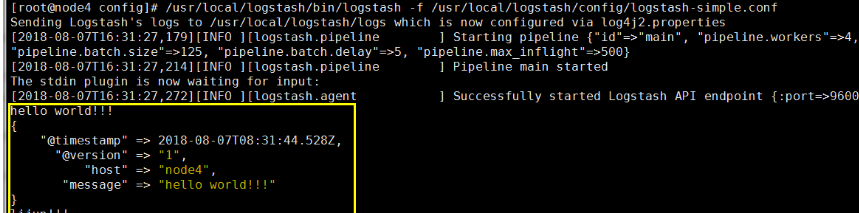
|  |
| --- |
| http://172.60.51.94:9200/\_search?pretty |

****3、安装Logstash****

|  |
| --- |
| wget <https://artifacts.elastic.co/downloads/logstash/logstash-6.3.0.tar.gz>  tar xf logstash-6.3.0.tar.gz -C /usr/local/  在此创建主配文件进行测试：  cat /usr/local/logstash-6.3.0/config/logstash-simple.conf  input { stdin { } }  output {  stdout { codec=> rubydebug }  } |

使用logstash参数-f读取配置文件进行测试：

|  |
| --- |
| /usr/local/logstash-6.3.0/bin/logstash -f /usr/local/logstash-6.3.0/config/logstash-simple.conf |



此时说明我们的logstash是完全没有问题了，可以进行日志收集了

cd /usr/local/logstash-6.3.0 && vim config/logstash.yml

添加一下配置

|  |
| --- |
| path.config: /usr/local/logstash-6.3.0/conf.d  config.reload.automatic: true |

cd /usr/local/logstash-6.3.0/ && mkdir conf.d && cd conf.d

vim ht\_stag\_app.yml

|  |
| --- |
| input {  redis {  host => "192.168.1.12"  port => "12345"  key => "default\_list"  data\_type => "list"  threads => "5"  db => "0"  codec => "json"  }  }  filter {  mutate {  gsub => ["message", "\\x", "\\\x"]  }  json {  source => "message"  remove\_field => "message"  remove\_field => "severity"  remove\_field => "pid"  remove\_field => "logsource"  remove\_field => "timestamp"  remove\_field => "facility\_label"  remove\_field => "type"  remove\_field => "facility"  remove\_field => "@version"  remove\_field => "priority"  remove\_field => "severity\_label"    }  mutate {  convert => [ "status","integer" ]  convert => [ "size","integer" ]  convert => [ "upstreatime","float" ]  convert => ["[geoip][coordinates]", "float"]  remove\_field => "message"  }  date {  match => [ "timestamp" ,"dd/MMM/YYYY:HH:mm:ss Z" ]  }  geoip {  source => "client" ##日志格式里的ip来源，这里是client这个字段（client":"$remote\_addr"）  target => "geoip"  database => "/usr/local/src/GeoLite2-City\_20190827/GeoLite2-City.mmdb" ##### 下载GeoIP库  add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]  add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]  }  mutate {  remove\_field => "timestamp"  }  if "\_geoip\_lookup\_failure" in [tags] { drop { } } ### 如果解析的地址是内网IP geoip解析将会失败，会生成\_geoip\_lookup\_failure字段，这段话的意思是如果内网地址 drop掉这个字段。  }  output {  if [fields][service] == "pfgw65\_stag\_nginx\_access" {  elasticsearch {  hosts => ["127.0.0.1:9200"]  index => "logstash-pfgw176.65-%{+YYYY.MM.dd}"  document\_type => "%{type}"  }  stdout { codec => rubydebug }  }  } |

**软连接**

|  |
| --- |
| ln -s /usr/local/logstash-6.3.0/bin/logstash /usr/local/bin/logstash |

**启动**

Logstash

1. ****安装kibana****

|  |
| --- |
| ># wget https://artifacts.elastic.co/downloads/kibana/kibana-6.3.0-x86\_64.rpm  ># rpm -ivh kibana-6.3.0-x86\_64.rpm  vim /etc/kibana/kibana.yml  #添加以下配置  server.host: "0.0.0.0"  elasticsearch.url: "http://127.0.0.1:9200"  ># service kibana start |

[http://172.60.51.94:5601](http://172.60.51.94:5601/)

1. ****安装grafana****

|  |
| --- |
| wget <https://dl.grafana.com/oss/release/grafana-6.3.5-1.x86_64.rpm>  sudo yum localinstall grafana-6.3.5-1.x86\_64.rpm |

**安装插件**

|  |
| --- |
| grafana-cli plugins install grafana-piechart-panel  grafana-cli plugins install satellogic-3d-globe-panel |

[http://172.60.51.94:3000](http://172.60.51.94:3000/) admin/admin

1. ****参考文档****

<http://www.zhouqishan.cn/2017/11/16/filebeatredislogstashelasticsearchkibana%E6%90%AD%E5%BB%BA%E6%97%A5%E5%BF%97%E7%B3%BB%E7%BB%9F/>

<https://www.centos.bz/2018/08/linux%e6%90%ad%e5%bb%baelk%e6%97%a5%e5%bf%97%e6%94%b6%e9%9b%86%e7%b3%bb%e7%bb%9f%ef%bc%9afilebeatredislogstashelasticse/>