Kibana

Kibana是什么:

数据可视化平台工具

默认安装在: /opt/kibana

配置文件: /opt/kibana/config/kibana.yml

服务名: kibana

端口: 5601

部署

**1.配置**

配置ip: 192.168.1.56

配置yum源: elk

配置主机名(es所有和自己)

**2.直接安装kibana**

1. **修改配置文件**

]# vim /opt/kibana/config/kibana.yml

2 server.port: 5601

//若把端口改为80，可以成功启动kibana，但ss时没有端口，没有监听80端口，

服务里面写死了，不能用80端口，只能是5601这个端口

5 server.host: "0.0.0.0" //服务器监听地址

15 elasticsearch.url: http://192.168.1.51:9200

//声明地址，从哪里查，集群里面随便选一个

23 kibana.index: ".kibana" //kibana自己创建的索引

26 kibana.defaultAppId: "discover" //打开kibana页面时，默认打开的页面discover

53 elasticsearch.pingTimeout: 1500 //ping检测超时时间

57 elasticsearch.requestTimeout: 30000 //请求超时

64 elasticsearch.startupTimeout: 5000 //启动超时

**4.开机自启,查看端口**

**用的head插件**

**添加数据**

**“\*”: 为所有**

1.上方第四4大项--->输入E的索引名

2.第1大项--->左上kibana大标题下选索引名(名末尾有小下拉箭头),右上角添加时间

**做饼**

第2大项

##################################################################################

Logstash

Java

作用:

所有类型数据的集中处理

本次作用:

搜集数据,把数据处理为json格式,发送elasticsearch数据

Logstash会从filebash读取数据,经过grok的过滤筛选最总数据会写到elasticsearch

没有配置文件,没有例子,需自己写

要求: 2cpu 4g内存

分析数据占用内存很大,不是2cpu会报错

配置文件: /etc/logstash/logstash.conf

启动程序: /put/logstash/bin/logstash -f 配置文件

查看插件: /opt/logstash/bin/logstash-plugin list

端口: 5044 (需手动配置端口)

记录文件位置:

默认记录文件在用户家目录下的**.**sincedb\_e9......,一般不用

配置文件书写:

各种插件:

input codec filter output

插件名字: logstash-能使用的区域-功能

codec: 在数据中指定数据的编码格式及其类型,所有区域

11.20

]# /opt/logstash/bin/logstash-plugin list //查看插件

##############################################

Logstash安装

要求: 2cpu 4g内存 分析数据占用内存很大,不是2cpu会报错

1. 安装java-1.8.0-openjdk
2. 直接安装logstash
3. 写配置文件
4. 启动

]# /opt/logstash/bin/logstash -f 配置文件路径

会有点慢,出现两行为成功,可输入东西

调试

##############################################

基本的配置文件书写

input-stdin插件 -->标准输入插件

output-stdout插件 -->标准输出插件

codec-rubydebug插件

input{

stdin{

codec => "json" //输入设置为编码json,输入解析为json

}

}

filter{} //过滤器,数据过滤加工处理

output{

stdout{

codec => "rubydebug" //输出设置为rubydebug,把json输出竖着显示

}

}

###############################################

配置logstash实现数据读取,过滤,并发送到elasticsearch

1.input插件**文件**获取数据

input-file插件

Input-beats插件

input{

beats {

port => 5044 //使用5044端口,让web从此端口传进数据

}

file{

start\_position => "beginning" //第一次读取文件从什么地方开始

sincedb\_path => "/var/lib/logstash/sincedb-access" //读取记录文件位置

path => ["/tmp/a.log","/var/tmp/b.log"] //读取的文件位置

type => 'filelog' //打标签

}

}

默认记录文件在用户家目录下的**.**sincedb\_e9......,一般不用

###############################################

1. filter插件过滤处理收据

filter-grok插件

-- 解析各种非结构化的日志数据插件

filter{

grok {

match => {"message" => "%{COMBINEDAPACHELOG}"}

} //匹配 //输出内容的”message” //宏或正则表达式

}

宏:人家写好的正则表达式

位置:

/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns/grok-patterns

直接调用即可

格式: %{宏名}

###############################################

3.output将数据发送给elasticsearch

logstash-output-elasticsearch插件

output{

stdout{

codec => rubydebug

}

if [type] == "apache\_log" { //分类,也是E的类型(表),若数据类型为”..”

的执行下面(索引在下面)

elasticsearch {

hosts => ["es1:9200","es2:9200","es3:9200"] //随机连接某一台,写多台防

单点故障

index => "weblog" //在elasticsearch上创建的索引名,默认按照时间日期创建

flush\_size => 2000 //满2000字节数据发给elasticsearch

idle\_flush\_time => 10 //空闲10秒,回写硬盘

}}

}

启动logstash查看端口是否开启成功

###############################################################################

Web服务器

Filebeat

通过filebeat把日志传给logstash

配置文件: /etc/filebeat/filebeat.yml

服务名: filebeat

1. 安装filebeat

]# yum -y install filebeat

1. 修改配置文件

vim/etc/filebeat/filebeat.yml

paths:

- /var/log/httpd/access\_log //日志的路径，短横线加空格代表yml格式

document\_type: apachelog //文档类型(打标签)

#elasticsearch: //加上注释,因为把数据直接发给E是不识别的

#hosts: ["localhost:9200"] //加上注释

logstash: //去掉注释

hosts: ["192.168.1.57:5044"] //添加logstash的ip:端口

1. 重启

这样,三大组件都会打通

注意:

清空elasticsearch数据会把”**.**kibana”库给删掉,

需重启kibana即可生成库