ELK

对日志进行处理的

简介:

***ELK是日志分析平台，不是一款软件***,***而是一整套解决方案***,是三个软件产品的首字母缩写,就像LNMP,并不是一款软件,是一个组合

ELK分别代表：

–E: Elasticsearch负责日志检索和储存(**非关系型数据库,java开发的, 重要级:1**)

–L: Logstash负责日志的收集和分析、处理(**重要级:2**)

–K: Kibana负责日志的可视化(**把数据做成网页,重要级:3**)

作用:

ELK组件在海量日志系统的运维中,可用于解决分布式日志数据集中式查询和管理系统监控等，故障排查，安全信息和事件管理，报表功能

工作流程:

Web日志、通过filebeat发送数据--->Logstash格式化数据----->E(elastic...)储存数据<------>Kibana从E读取数据、把数据做成页面

Logstash ---> Elasticsearch --> Kibana

Elasticsearch要做成高可用集群,数据很重要

先搭建Elasticsearch,不然搭到最后出问题了不好找,不知道三大组件哪个出问题了

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

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

Elasticsearch

Java开发、非关系型数据库,、至少需要java 7

通过http协议对数据库增.删.改.查

可以分片:

每台机器存的数据都不一样

浅框: 备份数据

深框: 源数据

Elasticsearch:

–DB -> Databases -> Tables -> Rows -> Columns

–关系型 数据库 表 行 列

–ES -> Indices -> Types -> Documents -> Fields

–ES -> 索引 类型 文档 域(字段)

端口: 9200 9300

服务名: elasticsearch

配置文件: /etc/elasticsearch/elasticsearch.yml

相关概念

Node: 装有一个ES服务器的节点

Cluster: 有多个Node组成的集群

Index: 拥有相似特征的文档的集合(等同于mysql库)

Type: 一个索引中可以定义一种或多种类型(表)

Document: 文档、一个可被搜索的基础信息单元(行)

Filed: 是ES的最小单位,数据的某一列 (字段)

Shards: 索引的分片, 每一个分片就是一个Shard

易拉色吃的index和mysql的index完全不一样

部署

192.168.1.51--56 --> es1 -- es5

部署yum源

1. 安装 java-1.8.0-openjdk.x86\_64

2.配置主机名/etc/hosts //要求互相ping通,所以配置

3.安装elasticsearch

Yum直接安装

4.修改文件

(/etc/elasticsearch/elasticsearch.yml)

17 cluster.name: myelk //配置集群名字,(一致,靠名称识别是否为一个集群)

23 node.name: es1 //当前主机名称

54 network.host: 0.0.0.0 // 0.0.0.0（监听所有地址）

68 discovery.zen.ping.unicast.hosts: ["es1", "es2", "es3"]

//集群成员,不需要全部添加,最好为3个

1. 启动

]# systemctl restart elasticsearch

插件:

Head

Kopf

Bigdesk

./plugin install 插件

remove

分片

每台机器存的数据都不一样

浅框: 备份数据

深框: 源数据

绿色,

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

http请求由三部分组成:

请求行 , 消息报头 , 请求正文

ES常用:

PUT 增

DELETE 删

POST 改

GET 查

ip:9200/\_plugin/head/ //访问elasticsearch主页

Ip:9200/\_cat/nodes //

Ip:9200/\_cat/nodes?v

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

RESTful API调用

curl命令操作

-A 修改请求agent

-X设置请求方法

-i 显示返回头信息

总命令:

curl -X大写字母 http://IP:9200/索引[/类型/文档号] -d '

json格式'

字母:

GET

PUT

POST

DELETE

创建索引

curl -XPUT http://es2:9200/tedu -d '

{"settings": {

"index": {

"number\_of\_shards": 5, //分片数

"number\_of\_replicas": 1 //备份数

}

}

}'

添加文档

curl -XPUT http://es2:9200/tedu/teacher/**1** -d '

{ //tedu库下teacher表第一行

"姓名":"nn",

"爱好":"ss",

"年龄":"80"

}'

查询

- json格式输出

curl -XGET 'http://es2:9200/tedu/teacher/1'

修改文档

curl -XPOST http://es2:9200/tedu/teacher/1/\_update -d '

{"doc":{"年龄":18}}'

删除

- 能删索引,文档,但不能删类型

curl -XDELETE 'http://es2:9200/tedu/teacher/1' //删行

curl -XDELETE 'http://es2:9200/tedu' //删索引

curl -XDELETE http://es2:9200/\* //删除所有索引

导入数据

-- 日志内容以json格式导入

1. 文件里有指定索引,类型,id

curl -XPOST http//es3:9200/\_bulk --data-binary @文件名

2.文件里没有指定

curl -XPOST http://es3:9200/mysy/sss/\_bulk --data-binary @文件名