时间：70 分钟

ELK stack 概述

ELK：一款轻量级的实时日志收集，处理，展示系统。

一：介绍 ELK 需求及优缺点

1. 需求

（1）：业务需求，市场的需求
（2）：开发与产品的需求，运维的一种责任
（3）大数据也是当前的一个前景

2. ELK 日志分析系统的优势：

（1）使用方便，直接解决了我们的需求，并且是开源的
（2）相对来说，学习还是配置都是相对简单的。
（3）es 搜索快，基本上是秒级的
（4）架构相对简单，横向扩展方便

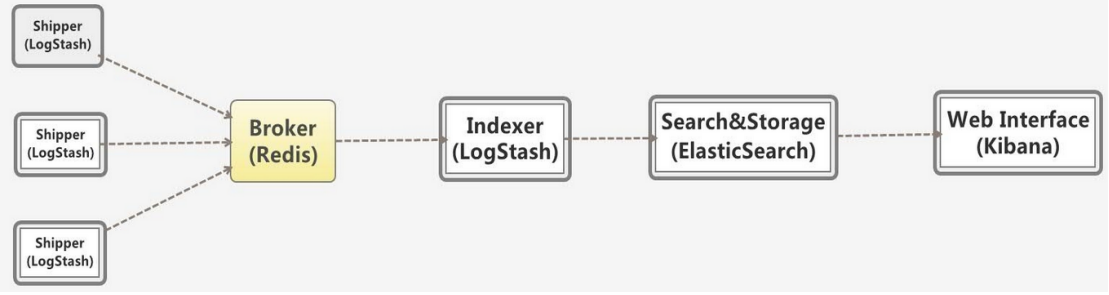
3. ELK 日志分析系统的缺点

（1）Logstash 耗资源较大，运行占用 CPU 和内存高
（2）另外没有消息队列缓存，存在数据丢失隐患

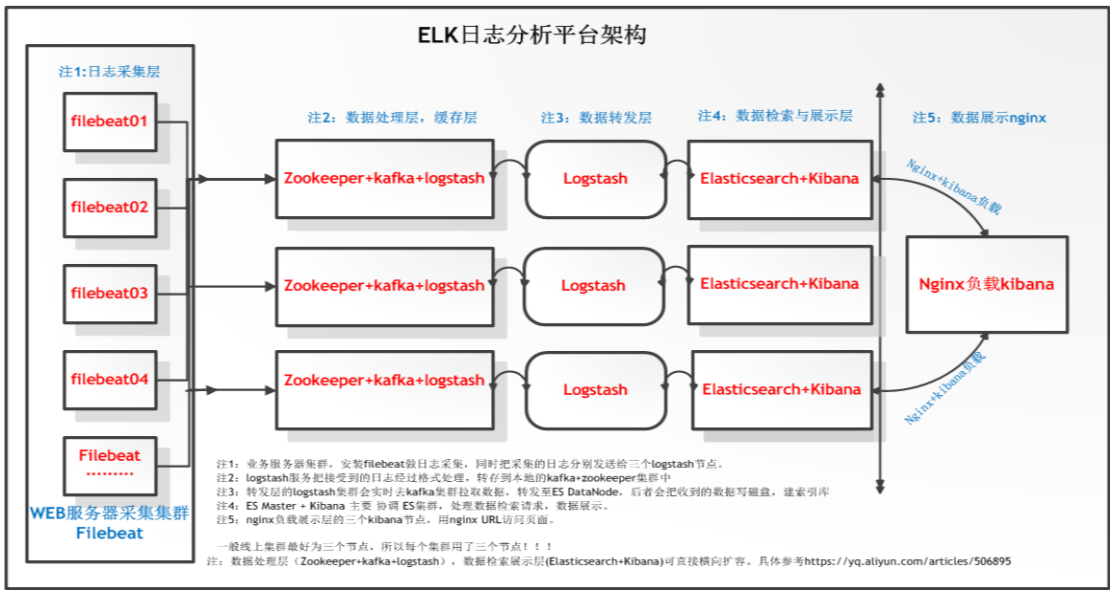
二：公开课程的目标

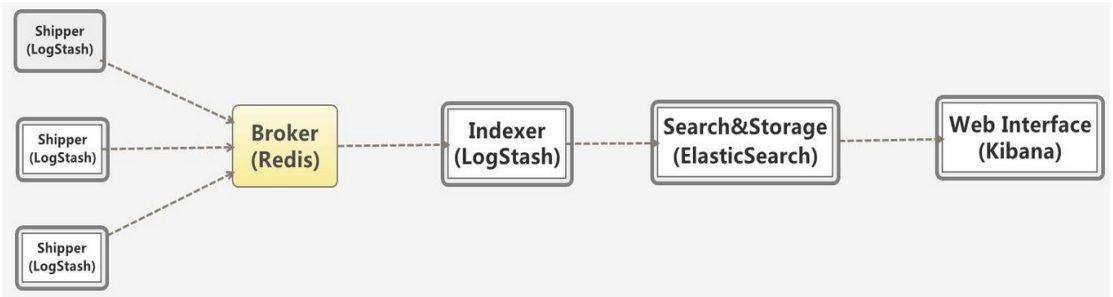
（1）可以收获属于自己的进步
（2）可以自己动手去搭建一下这个系统，去了解一下这个系统

三：介绍 ELK 的组成部分。



集群部署 ELK 拓扑图：





ELK 是 Elasticsearch、Logstash、Kibana 三个开源软件的组合而成，形成一款强大的实时日志收集展示系统。除了相关的 beat 相关采集插件外，基本都是基于这个架构来完成。

（1） 日志采集层， logstash 或 filebeat
（2） 消息代理层， redis 或 kafka。
（3） 管理层， logstash
（4） 搜索引擎层， Elasticsearch
（5） 展示层， kibana

注：Filebeat 隶属于 Beats(社区)。目前 Beats 包含四种工具：

1. Packerbeat (搜集网络流量数据)
2. Topbeat (搜集系统，进程和文件系统级别的 CPU 和内存使用情况等数据)
3. Filebeat(搜集文件数据)
4. Winlogbeat(搜集 windows 事件日志数据)

四：Redis 和 kafka 的作用。

1. 那如果 logstash 和 ES 无法通讯的话，日志是不是会从而丢失？
2. 那如果日志量过大的话，日志是不是会从而丢失？
3. 防止 logstash 直接与 es 操作，产生大量的链接，导致 es 瓶颈

《ELK 企业实战》

基础篇

Elk 分析 nginx 日志

目录

访问及报错日志

NO.1 <<Elasticsearch>> 安装与集群配置

一、软件版本

操作系统：CentOS-6.5-x86_64

ES 版本：5.0

主机：192.168.63.246

主机：192.168.63.242

二、部署环境规划：

1、 需求：jdk 版本：open-jdk.1.8

```
# java -version      （查看 JDK 版本号）
openjdk version "1.8.0_101"
OpenJDK Runtime Environment (build 1.8.0_101-b13)
OpenJDK 64-Bit Server VM (build 25.101-b13, mixed mode)
```

2、 下载解压安装即可：

```
[root@module-kzkt-02 opt]# cd /opt/
[root@module-kzkt-02 opt]# tar zcvf elasticsearch-5.3.1.tar.gz
```

3、 具体配置 elasticsearch：

```
[root@module-kzkt-02 opt]# cd elasticsearch-5.3.1/config/
[root@module-kzkt-02 config]# vim elasticsearch.yml
```

配置解析：

```
cluster.name: es-log                              ####集群名
node.name: node-1                ####节点名称
```

```
path.data: /path/to/data          ####存储数据地址
path.logs: /path/to/logs          ####存储日志地址
bootstrap.memory_lock: true       ###当内存不足时，是否使用交换分区空间
network.host: 10.0.1.7            ####IP 地址
http.port: 9200                   #####通讯端口
discovery.zen.ping.unicast.hosts: ["host1", "host2"]    ####集群地址 IP
discovery.zen.minimum_master_nodes: 3                   ####集群节点个数
```

其他配置解析：

######当消耗完交换分区这么大空间后才会产生 oom 的。

```
vim /etc/sysctl.conf
vm.max_map_count=262144
```

```
sysctl –p
```

系统的打开文件数：

```
vim /etc/security/limits.conf
* soft nofile 655350
* hard nofile 655350
```

修改用户打开的线程数，因为 es 的段要经常打开文件控制索引：

```
vim /etc/security/limits.d/20-nproc.conf
*          soft     nproc      4096
```

切换到普通用户启动：

```
[root@module-kzkt-02 bin]# su - elk
[elk@module-kzkt-02 logs]$ cd /opt/elasticsearch-5.3.1/bin/
[elk@module-kzkt-02 bin]$ ./elasticsearch
```

#####1.要是提示，报一些没有启动的目录，直接创建即可

#####2.但是想写入日志和数据必须是普通用户有写入权限 logs,data

启动之后：测试有如下显示表示已经安装成功。

```
[root@module-kzkt-02 bin]# curl -XGET '10.0.1.7:9200'
{
  "name" : "node-1",
  "cluster_name" : "es-log",
  "cluster_uuid" : "ZKwbyR74RHqKhUMyzFSQ5A",
  "version" : {
    "number" : "5.3.1",
```

```
    "build_hash" : "5f9cf58",
    "build_date" : "2017-04-17T15:52:53.846Z",
    "build_snapshot" : false,
    "lucene_version" : "6.4.2"
  },
  "tagline" : "You Know, for Search"
}
```

扩展：

集群启动设置

假如说只有一个节点，那么 es 就当做自己是一个集群。

一个节点(node)就是一个 Elasticsearch 实例，而一个集群(cluster)由一个或多个节点组成，它们具有相同的 cluster.name，它们协同工作，分享数据和负载。

当加入新的节点或者删除一个节点时，集群就会感知到并平衡数据。

NO.2 <<logstash>>安装与配置

1. **下载解压即可**

```
[root@module-kzkt-02 opt]# cd /opt/
[root@module-kzkt-02 opt]# tar xf logstash-6.2.4.tar.gz
```

2. **配置文件修改**

```
[root@module-kzkt-02 config]# vim config/logstash_to_es.conf
input {
    file {
        type => "log"
        path => "/usr/local/nginx/logs/*.log"
        discover_interval => 10
        start_position => "beginning"
    }
}
filter {
}
output {
    elasticsearch {
    index => "log-%{+YYYY.MM.dd}"
    hosts => ["10.0.1.7:9200"]
    }
    stdout {codec => rubydebug}
```

#####可以加判断：

例如：

```
if [type] ==  "****"{
                elasticsearch {
                      hosts => ["192.168.1.1:9200"]
                      index =>  "system-%{+YYYY.MM.dd}"
                }
        }

        if [type] ==  "****"{
                elasticsearch {
                      hosts => ["192.168.1.160:9200"]
                      index =>  "es-error-%{+YYYY.MM.dd}"
                }
        }
```

我的配置文件如下：

```
input {
    file {
        type => "log"
        path => "/usr/local/nginx/logs/*.log"
        discover_interval => 10
        start_position => "beginning"
    }
}
filter {
}
output {
    elasticsearch {
    index => "log-%{+YYYY.MM.dd}"
    hosts => ["10.0.1.7:9200"]
    }
    stdout {codec => rubydebug}
}
~
```

3. 启动程序

```
[root@module-kzkt-02 bin]# nohup ./bin/logstash -f config/logstash_to_es.conf  &
```

NO.3 <<filebeat>>安装与配置

1. 下载解压即可

```
[root@module-kzkt-02 opt]# cd /opt/
[root@module-kzkt-02 opt]# tar xf filebeat-5.3.1-linux-x86_64
```

2.配置文件修改

```
[root@module-kzkt-02 filebeat-5.3.1-linux-x86_64]# vim filebeat.yml
- input_type: log              ###类型

  paths:
    - /var/log/*.log           ####需要采集的日志路径
    - /**                      ####多个的话直接添加

exclude_files: [".gz$"] :      ###移除这个目录下面相关 gz 结尾的文件

exclude_lines: ["^DBG"]:       ###表示移除什么样的结尾的行。
```

#####这里注意，output 到哪里，其他的就要关掉。这里演示直接打入 eslasticsearch，

```
output 到哪个 elastisearch：
output.elasticsearch:
  # Array of hosts to connect to.
hosts: ["localhost:9200"]
  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

输出到 logstash:
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]

输出到 redis:
output.redis:
hosts: ["localhost"]
password: "my_password"
key: "filebeat"
db: 0
timeout: 5
```

#####这里注意，output 到哪里，其他的就要关掉。这里演示直接打入 eslasticsearch，

NO.4 <<kibana>>安装与配置

1.下载解压即可

```
[root@module-kzkt-02 opt]# cd /opt/
[root@module-kzkt-02 opt]# tar xf kibana-5.3.1-linux-x86_64.tar.gz
```

2.配置文件修改

```
[root@module-kzkt-02 config]# cd /opt/kibana-5.3.1-linux-x86_64/config/
[root@module-kzkt-02 config]# vim kibana.yml
```

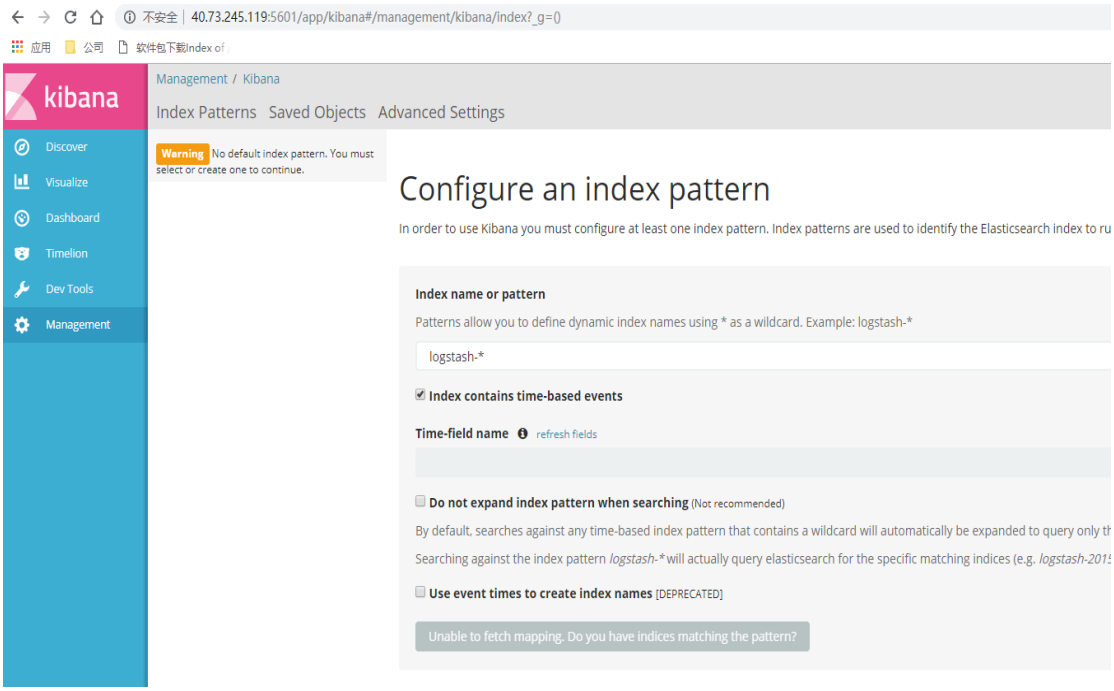
```
server.port: 5601                          ####服务端口
server.host: "10.0.1.7"                    ####服务 IP
elasticsearch.url: http://10.0.1.7:9200    ####连接 es 的地址
#elasticsearch.username: "user"            ####es 用户
#elasticsearch.password: "pass"            ####es 密码
```

3.启动服务

```
[root@module-kzkt-02 bin]# ./kibana
```

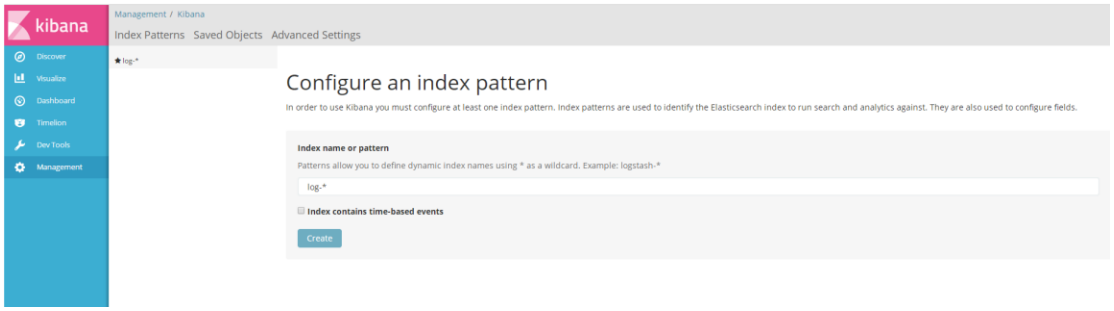
4.直接访问 URL IP:5601

刚开始有个初始化的步骤，可能要等一会。

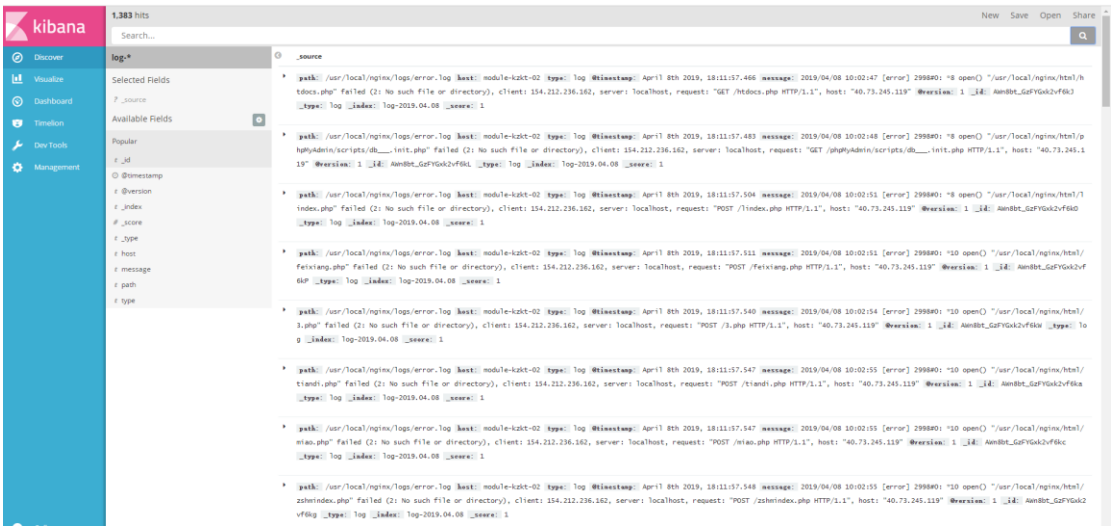


#####要创建一个索引

Management-->>index Partterns-->>Add New

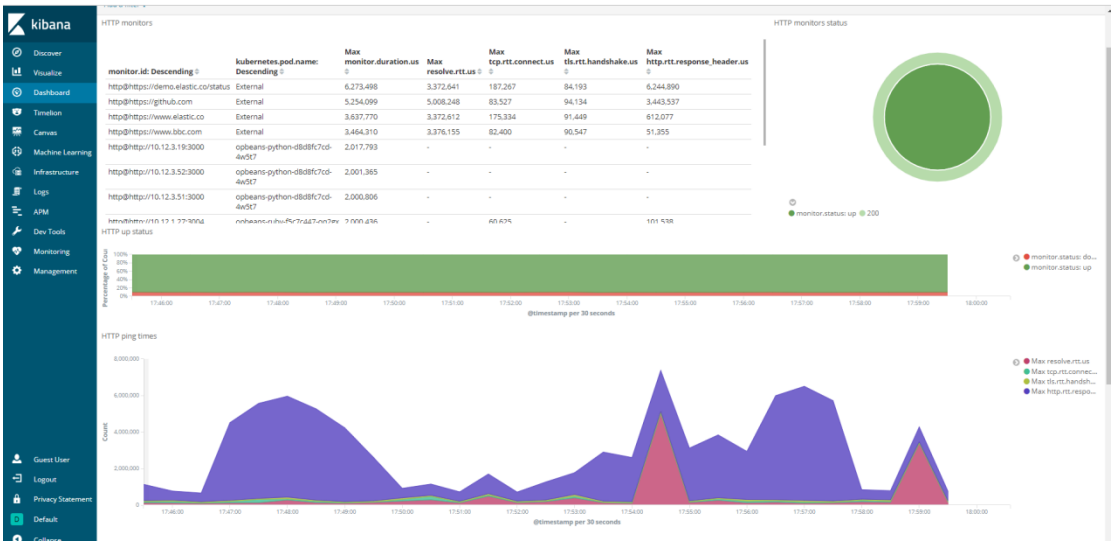


####出图

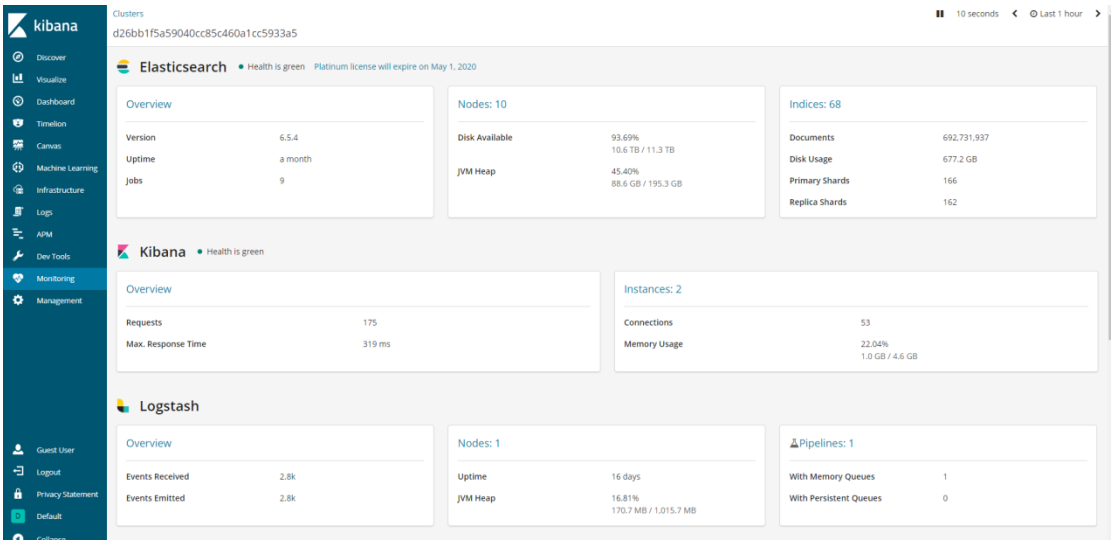


####apache<===>官网总访问量及总字节数

####电商月份总收入额


kibana
HTTP monitors
HTTP monitors status
HTTP up status
HTTP ping times
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Guest User
Logout
Privacy Statement
Default

#####组件的一些监控


kibana
Clusters
d26bb1f5a59040cc85c460a1cc5933a5
Elasticsearch
Health is green
Platinum license will expire on May 1, 2020
Overview
Version 6.5.4
Uptime a month
Jobs 9
Nodes: 10
Disk Available 93.69%
10.6 TB / 11.3 TB
JVM Heap 45.40%
88.6 GB / 195.3 GB
Indices: 68
Documents 692,731,937
Disk Usage 677.2 GB
Primary Shards 166
Replica Shards 162
Kibana
Health is green
Overview
Requests 175
Max. Response Time 319 ms
Instances: 2
Connections 53
Memory Usage 22.04%
1.0 GB / 4.6 GB
Logstash
Overview
Events Received 2.8k
Events Emitted 2.8k
Nodes: 1
Uptime 16 days
JVM Heap 16.81%
170.7 MB / 1,015.7 MB
Pipelines: 1
With Memory Queues 1
With Persistent Queues 0
Guest User
Logout
Privacy Statement
Default