ELK 日志集中分析平台
部署手册

hdhuang@cn.ibm.com

2015/05/15

关于本文档

《ELK 日志集中分析部署手册》提供了有关安装 Logstash、Elasticsearch 和 Kibana 的信息。

目标读者

本文适用于要执行以下任务的用户：

1. 安装,升级或使用 ELK
2. 需要分析 Vmware vSphere 平台日志的用户

本文的目标为信息系统工程师，软件开发人员等。

文档反馈

本文作者欢迎您提出宝贵的建议，以便改进我们的文档，如有意见，请将反馈发送到 hdhuang@cn.ibm.com

ELK 安装

ELK 简介

日志的分析和监控在系统开发中占非常重要的地位，系统越复杂，日志的分析和监控就越重要，常见的需求有:

- 根据关键字查询日志详情
- 监控系统的运行状况
- 统计分析，比如接口的调用次数、执行时间、成功率等
- 异常数据自动触发消息通知
- 基于日志的数据挖掘

很多团队在日志方面可能遇到的一些问题有:

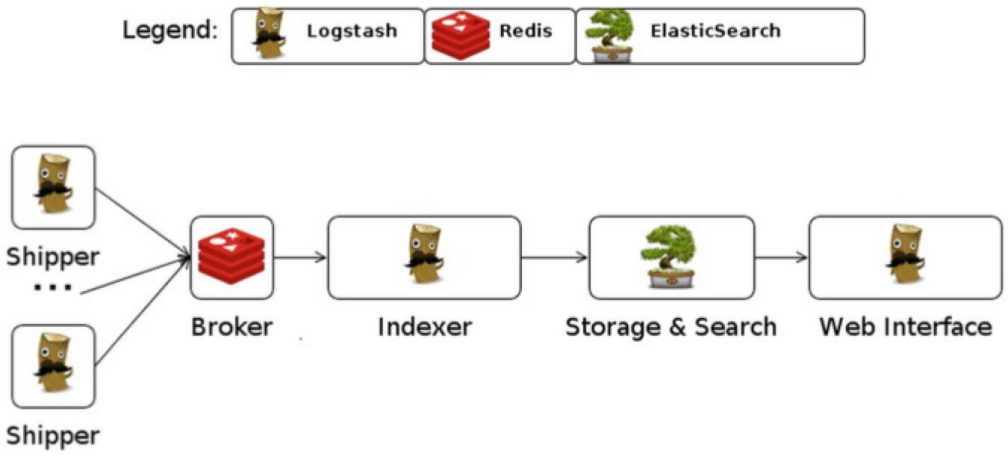
- 开发人员不能登录线上服务器查看详细日志，经过运维周转费时费力
- 日志数据分散在多个系统，难以查找
- 日志数据量大，查询速度慢
- 一个调用会涉及多个系统，难以在这些系统的日志中快速定位数据
- 数据不够实时

logstash+elasticsearch+kibana(elk)组合正是符合了以上需求。

对于日志来说，最常见的需求就是收集、查询、显示，正对应 logstash、elasticsearch、kibana 的功能。

平台架构

采用官方推荐的平台机构，如图所示：



环境规划

IP 地址	系统版本	角色	应用	用户名	密码
9.110.85.240	CentOS 6.5	Shiper	Logstash	root	passw0rd
9.110.85.75	CentOS 6.5	Shiper	Logstash	root	passw0rd
9.110.85.241	CentOS 6.5	Broker	Redis	root	passw0rd
9.110.85.242	CentOS 6.5	Index	logstash	root	passw0rd
9.110.85.73	CentOS 6.5	Index	logstash	root	passw0rd
9.110.85.243	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.244	CentOS 6.5	Web interface	Kibana	root	passw0rd
9.110.85.245	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.246	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.74	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.76	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.90	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.91	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd
9.110.85.92	CentOS 6.5	Storage& search	Elasticsearch	root	passw0rd

安装前准备

需要准备下列软件：

Centos 6.5_64

Logstash 1.4.2

Readis 2.8.17

Elasticsearch 1.4.1

nxlog-ce-2.9.1347

Kibana3.1.2

Elasticsearch 插件：head，kopf，bigdisk

Jdk 1.7

Putty

同时需要在所有的服务器上关闭防火墙，Linux 系统还需要关闭 selinux。

安装 Kibana

1.使用 putty 连接 9.110.85.244，登陆后安装 apache

```
# yum install apache –y
```

2.解压已经上传到服务器的 kibana 安装包,然后将 kibana 解压后的文件移动 apache 网站根目录

```
#tar zxvf kibana-3.1.2.tar.gz
#mv kibana-3.1.2    kibana
```

#mv kibana-3.1.2 /var/www/html/

3. 启动 apache 服务，kibana 完成

service httpd start

安装 Elasticsearch

1．使用 putty 分别登陆 elasticsearch 每个节点服务器，解压已上传的 elasticsearch 安装包

tar elasticsearch-1.4.1.tar.gz

2. 重命名已解压的文件夹移动到/usr/lcoal 目录；

#mv elasticsearch-1.4.1 elasticsearch

#mv elasticsearch /usr/local/

3. 修改配置文件，启动服务，elasticsearch 安装完成

cd /usr/local/elasticsearch/config/

vim elasticsearch.yml

添加以下两行到文件：

http.cors.allow-origin: "/.*/"

http.cors.enabled: true

启动服务

/usr/local/elasticsearch/bin/elasticsearch &

安装 Logstash index

1. 使用 putty 分别登陆 logstash 每个节点服务器，解压已上传的 logstash 安装包

tar zxvf logstash-1.4.2.tar.gz

2. 重命名已解压的文件夹移动到/usr/lcoal 目录

mv logstash-1.4.2 logstash

#mv logstash /usr/local

3. 新建配置文件

cd /usr/local/logstash/bin/

vim logstash.conf

输入以下内容后保存：

```
input {
  redis {
    host => "9.110.85.241"  # redis 服务器地
    port => "6379"  # redis 端口
    data_type => "list"
    key => "logstash"
    codec => "json"
    type => "syslog"
    threads => "10"
  }
}
filter {
        if "vCenter" in [tags]{
```

```
        grok {
        match => [

"message","%{SYSLOGTIMESTAMP:syslogtimestamp} %{HOST:vCenter} %{SYSLOGP
ROG:message_program} %{TIMESTAMP_ISO8601:@timestamp} (?<message-b
    ody>(?<message_system_info>(?:\[%{DATA:message_thread_id}  %{DATA:syslo
g_level} \'%{DATA:message_service}\'\ ?%{DATA:message_opID}])) \[%{DATA:me
    ssage_service_info}]\ (?<message-syslog>(%{GREEDYDATA})))",

"message","%{SYSLOGTIMESTAMP:syslogtimestamp} %{HOST:vCenter} %{SYSLOGP
ROG:message_program} %{TIMESTAMP_ISO8601:@timestamp} (?<message-b
    ody>(?<message_system_info>(?:\[%{DATA:message_thread_id}  %{DATA:syslo
g_level} \'%{DATA:message_service}\'\ ?%{DATA:message_opID}])) (?<message-
    syslog>(%{GREEDYDATA})))",
        "message",
"<%{POSINT:syslog_pri}>%{TIMESTAMP_ISO8601:@timestamp} %{GREEDYDATA:m
essage-syslog}"
      ]
    }

  }
```

```
output {
  elasticsearch {
    cluster => " elasticsearch "     # elasticsearch  集群名称
    port => "9300"
    flush_size => "50000"
    idle_flush_time => "30"
  }
}
```

4. 启动服务，logstash index 安装完成

```
# /usr/local/logstash/logsash –f   logstash.conf &
```

安装 Redis

1. 使用 putty 连接准备安装的 redis 服务器，解压已上传 redis 安装包

```
# tar zxvf redis-2.8.17.tar.gz
```

2. 安装 redis

```
# cd   zxvf redis-2.8.17
# make
```

3.创建配置文件，启动服务，redis 安装完成。

```
# cp redis.conf   /etc/
#redis-server   /etc/redis.conf &
```

安装 Logstash shipper

1. 用 putty 连接准备安装的 logstash 服务器，解压 logstash 已上传的安装包

```
# tar zxvf logstash-1.4.2.tar.gz
```

2. 重命名已解压的文件夹移动到/usr/lcoal 目录

```
# mv logstash-1.4.2  logstash
#mv logstash  /usr/local
```

3. 新建配置文件

```
# cd /usr/local/logstash/bin/
# vim logstash.conf
```

输入以下内容后保存

```
input {
file {
type => "vCenter"
path => [ "/var/log/messages" ]  # syslog 文件
tags => ['vCenter']  # vcenter 标签
}
}
output {
  redis {
    host => "9.110.85.241"    #redis 服务器地址
    data_type => "list"
    key => "logstash"
```

}

}

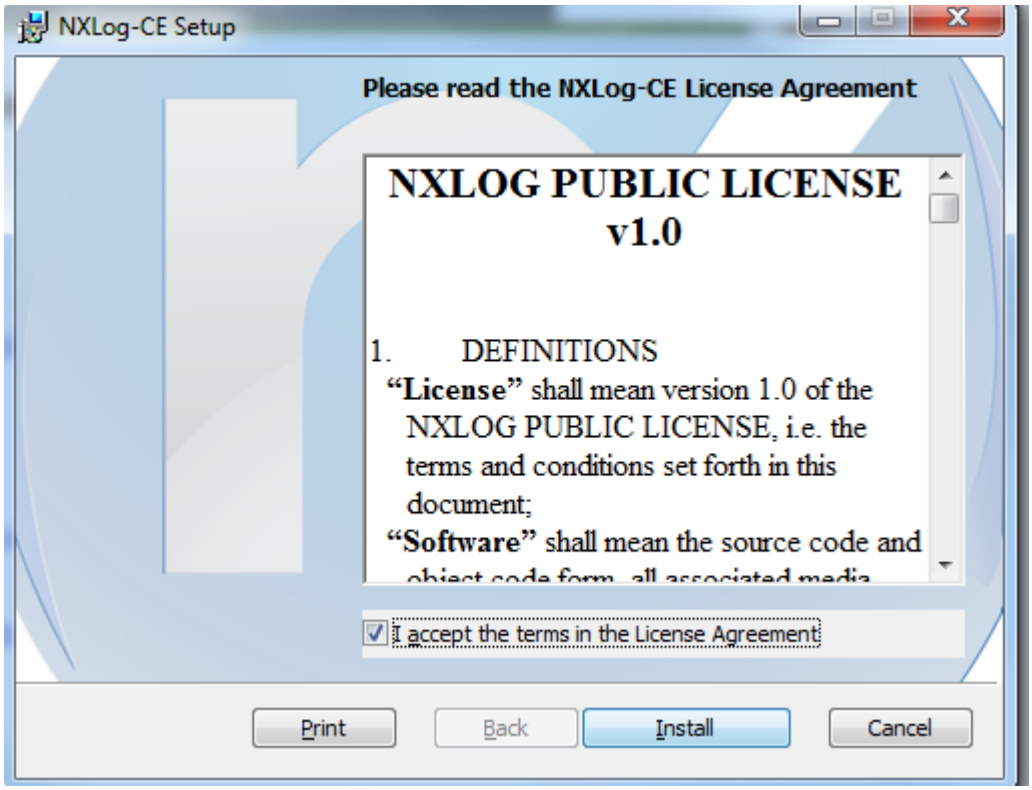
4.启动 syslog 服务，启动 logstash shipper 安装完成,。

service rsyslog start

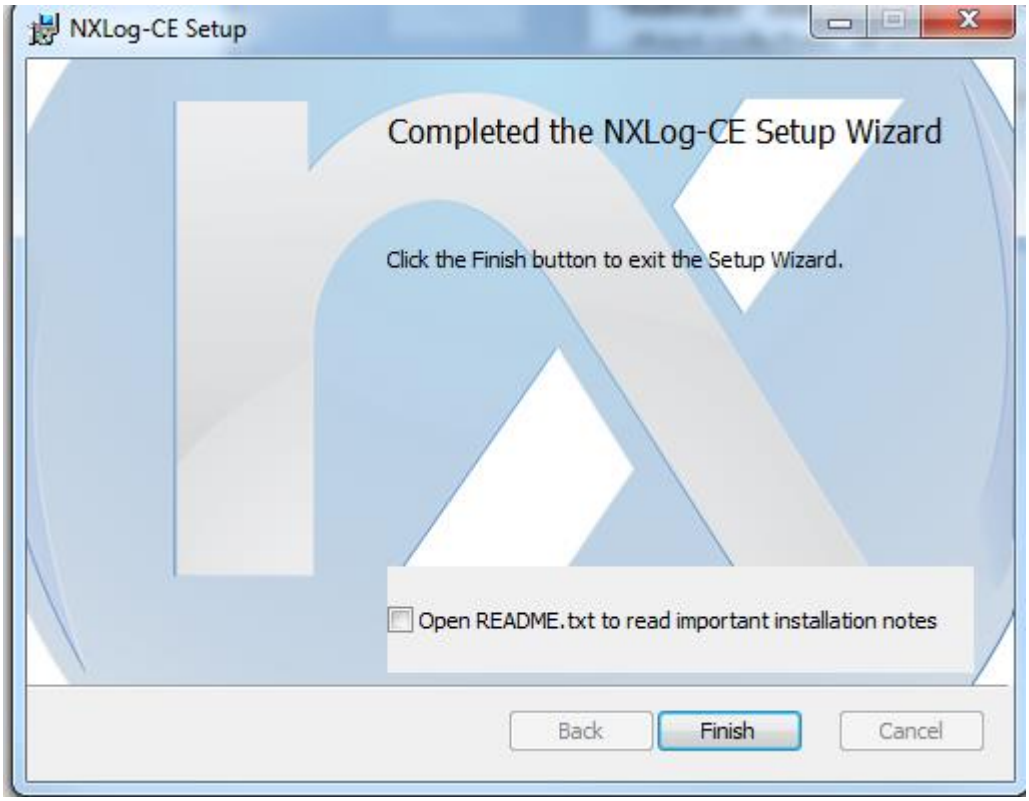
/usr/local/logstash/bin/logstash agent –f logstash.conf &

在 vCenter 上安装 nxlog

1.下载 nxlog-ce-2.9.1347.msi 后上传到 vCenter,双击运行，



2.点击 install，安装完成；



3.打开 C:\Program Files (x86)\nxlog\conf\nxlog.conf,编辑配置文件，输入一下内容：

<Input VPXD>

Module im_file

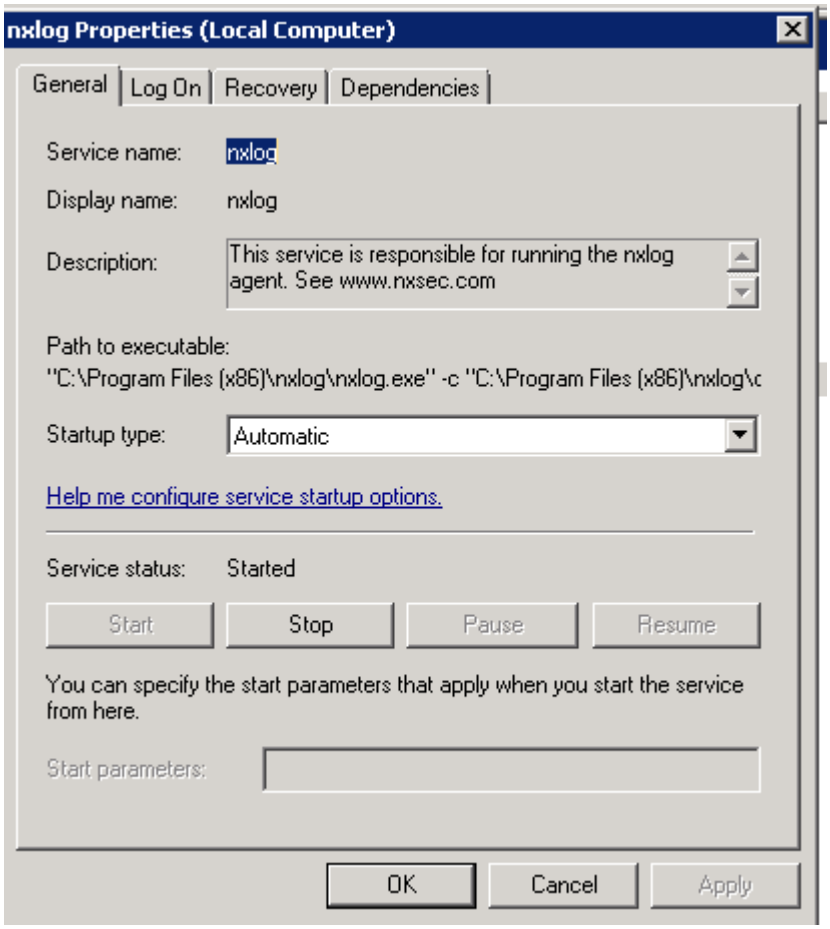
File "C:\\ProgramData\\VMware\\VMware VirtualCenter\\Logs\\vpxd-[0-9]*.log"

SavePos TRUE

</Input>

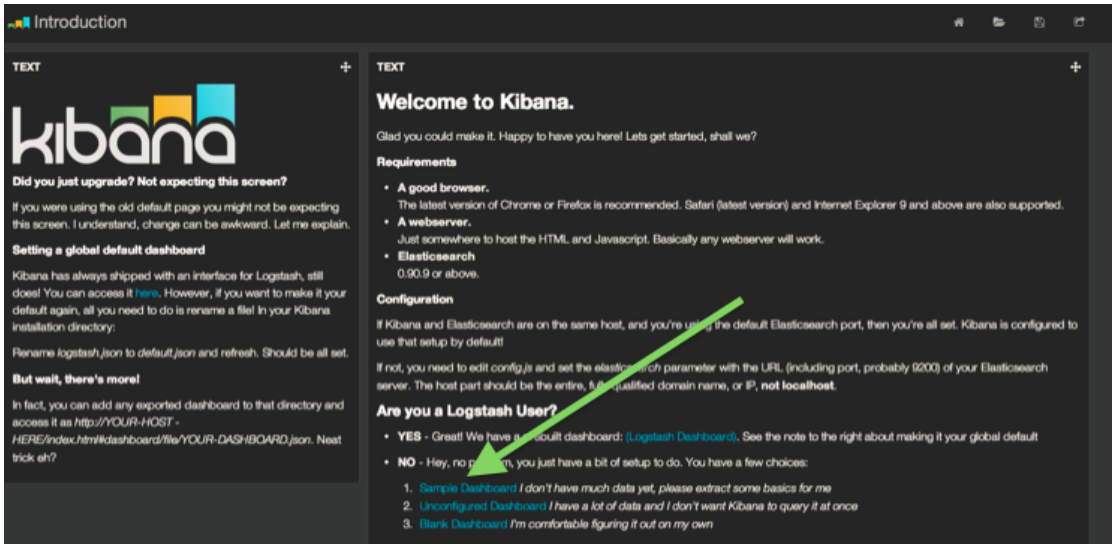
```
<Output out>
    Module          om_tcp
    Host            9.110.85.240    # syslog server 地址
    Port            514
    Exec      to_syslog_bsd();
</Output>

<Route 1>
    Path            VPXD => out
</Route>
```

4. 启动 NXlog 服务，并将该服务设置为自动启动，nxlog 安装完成。

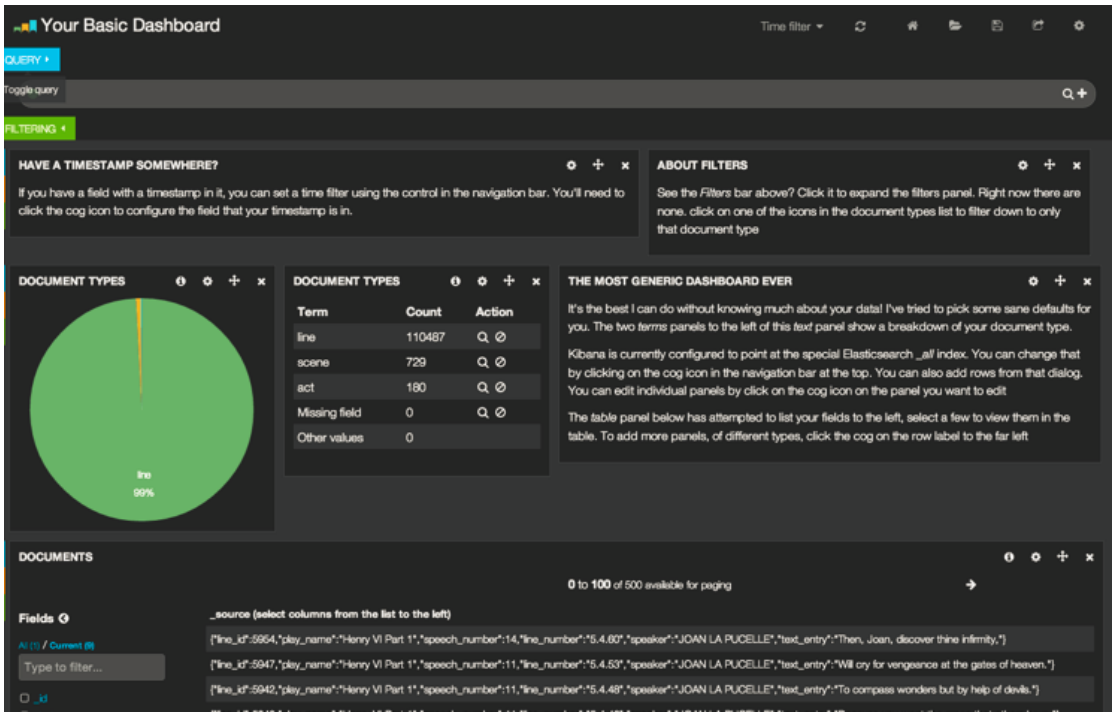


访问 Kibana 界面

1. 打开浏览器，访问已经发布了 Kibana 服务器地址，如果你解压路径无误，就可以看到一下这个页面，点击 Sample Dashboard



2. 现在显示 sample dashboard，ELK 安装完成。



安装 Elasticsearch 插件

1.安装 elasticsearch HEAD 插件

安装 head 插件集群管理工具，下载插件文件，解压缩后移动到 elasticsearch/plugins 目录下

#wget https://github.com/mobz/elasticsearch-head/archive/master.zip

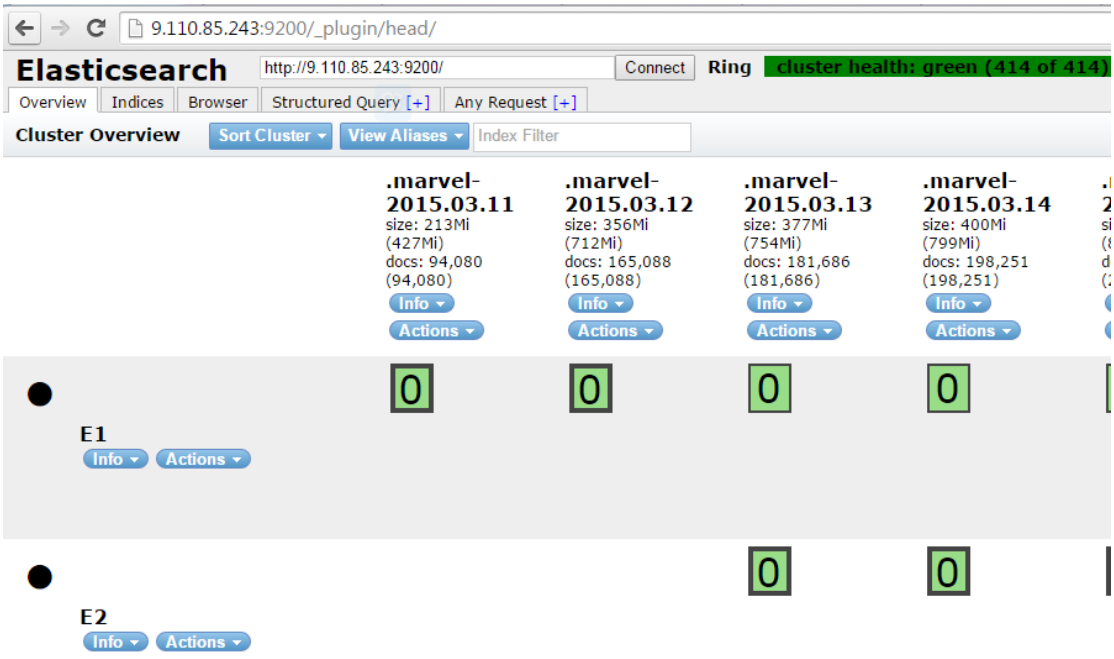
#unzip master.zip

#mkdir –p /usr/local/elasticsearch/plugins/head/_site

#mv elasticsearch-head-master/* /usr/local/elasticsearch/plugins/head/_site

访问http://9.110.85.243:9200/_plugin/head/

可方便查询索引数据及索引大小，如下图所示:



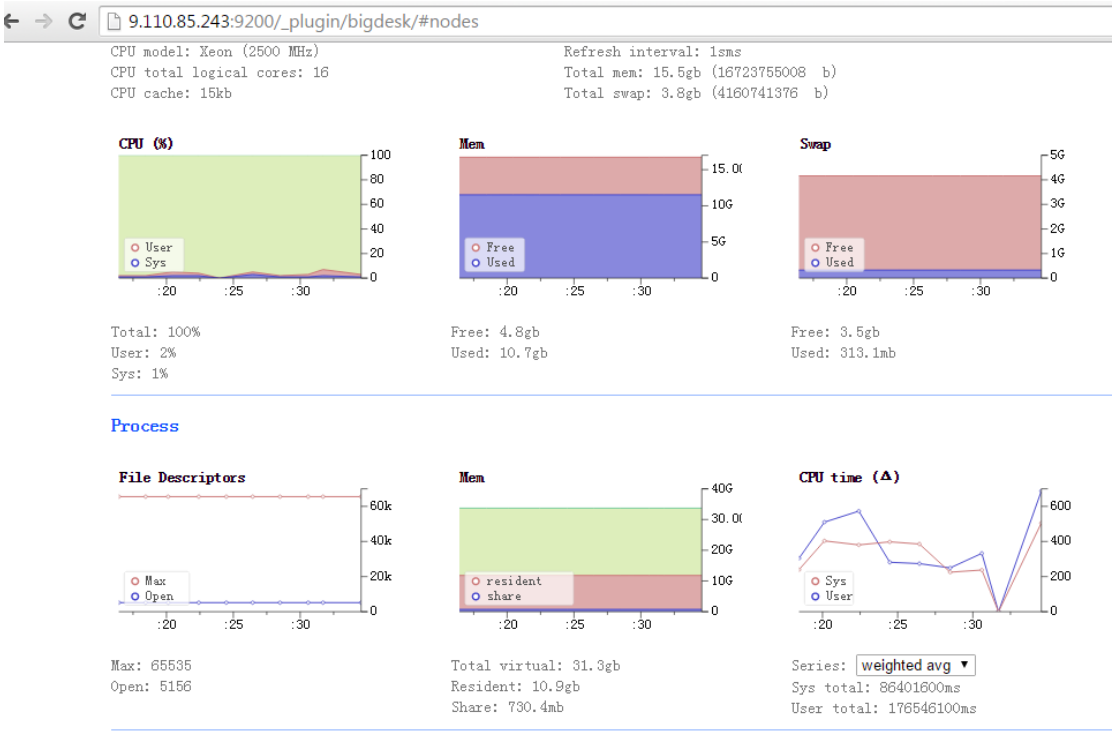
2.安装 bigdesk 插件

Bigdesk 插件可以查看 cpu、内存使用情况，索引数据、搜索情况，http 连接数等

#/usr/local/elstaicsearch/bin/plugin -i lukas-vlcek/bigdesk

访问http://9.110.85.243:9200/_plugin/bigdesk

如下图所示:



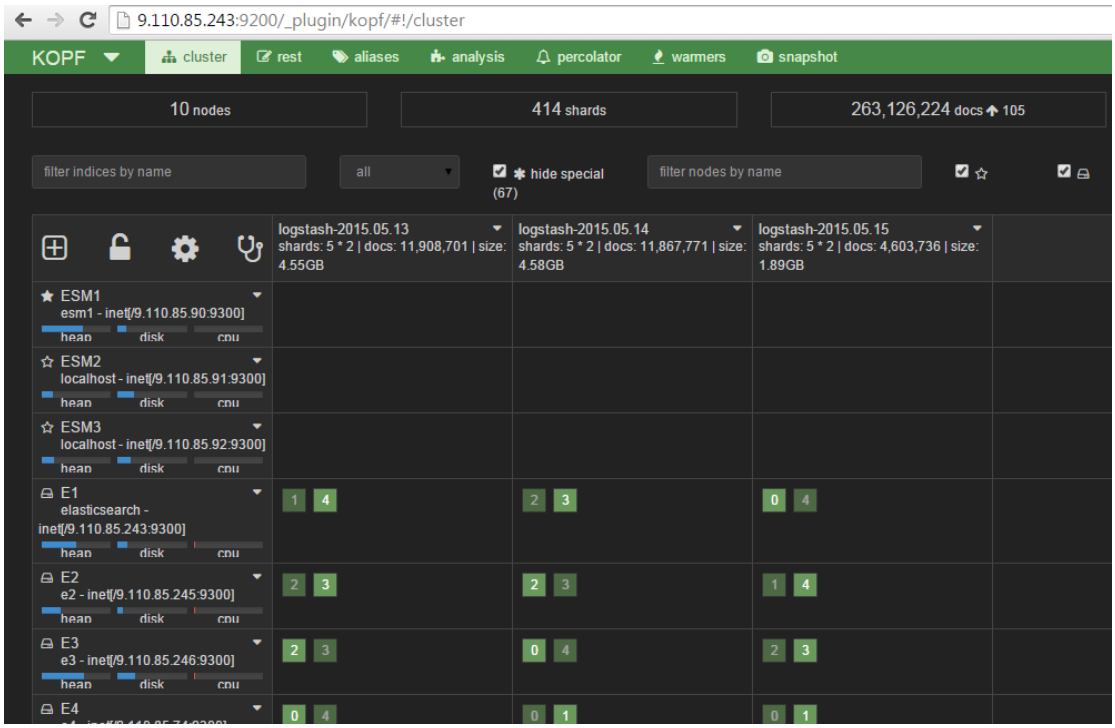
3.安装 elasticsearch KOPF 插件

KOPF 插件可以管理集群，监控查看 cpu、内存使用情况、在线查询/提交 elsticsearch 数据

安装

#/usr/local/elstaicsearch/bin/plugin –I lmenezes/elasticsearch-kopf

访问 http://9.110.85.243:9200/_plugin/kopf


9.110.85.243:9200/_plugin/kopf/#!/cluster
KOPF
cluster
rest
aliases
analysis
percolator
warmers
snapshot
10 nodes
414 shards
263,126,224 docs 105
filter indices by name
all
hide special (67)
filter nodes by name
logstash-2015.05.13
shards: 5 * 2 | docs: 11,908,701 | size: 4.55GB
logstash-2015.05.14
shards: 5 * 2 | docs: 11,867,771 | size: 4.58GB
logstash-2015.05.15
shards: 5 * 2 | docs: 4,603,736 | size: 1.89GB
ESM1
esm1 - inet[/9.110.85.90:9300]
ESM2
localhost - inet[/9.110.85.91:9300]
ESM3
localhost - inet[/9.110.85.92:9300]
E1
elasticsearch - inet[/9.110.85.243:9300]
E2
e2 - inet[/9.110.85.245:9300]
E3
e3 - inet[/9.110.85.246:9300]
E4
heap
disk
cpu