

1. [案例1：安装Elasticsearch](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case1)
2. [案例2：部署Elasticsearch集群](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case2)
3. [案例3：安装Elasticsearch插件](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case3)
4. [案例4：熟悉Elasticsearch的API调用](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case4)
5. [案例5：安装Kibana](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case5)
6. [案例6：导入日志并绘制图表](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/ARCHITECTURE/DAY01/CASE/01/index.html#case6)

**1 案例1：安装Elasticsearch**

**1.1 问题**

本案例要求：

* 创建虚拟机并安装 elasticsearch
* 最低配置： 1cpu，1G内存，10G硬盘
* 虚拟机：192.168.1.41 es-0001

**1.2 方案**

1）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，ELK分别代表：

Elasticsearch:负责日志检索和储存

Logstash:负责日志的收集和分析、处理

Kibana:负责日志的可视化

2) 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

部署Elasticsearch分布式集群安装，Kibana作为可视化平台，实时总结流量和数据的图表，Logstash用来收集处理日志

**1.3 步骤**

实现此案例需要按照如下步骤进行。

步骤一：先准备一台虚拟机

1）更改主机名，配置IP，搭建第三方yum源

1. [root@localhost ~]# mkdir -p /var/ftp/localrepo/elk
2. [root@localhost ~]# cp /linux-soft/04/elk/\* /var/ftp/localrepo/elk/
3. [[root@localhost](mailto:root@localhost) ~]# createrepo /var/ftp/localrepo/elk/
4. [[root@localhost](mailto:root@localhost) ~]# ssh 192.168.1.41
5. [[root@localhost](mailto:root@localhost) ~]# echo es-0001 > /etc/hostname
6. [[root@localhost](mailto:root@localhost) ~]# eip 41            //配置ip。这是提前写好的脚本
7. [[root@localhost](mailto:root@localhost) ~]# reboot
8. [[root@es-0001](mailto:root@es-0001) ~]# vim /etc/yum.repos.d/local.repo
9. [local\_repo]
10. name=CentOS-$releasever - Base
11. baseurl="<ftp://192.168.1.254/centos-1804>"
12. enabled=1
13. gpgcheck=1
14. [localrepo]
15. name=ELK software
16. baseurl="<ftp://192.168.1.254/localrepo/elk/>"
17. enabled=1
18. gpgcheck=0
19. [[root@es-0001](mailto:root@es-0001) ~]# yum clean all
20. [[root@es-0001](mailto:root@es-0001) ~]# yum repolist
21. 配置主机名解析
22. [[root@es-0001](mailto:root@es-0001) ~]# vim /etc/hosts
23. 192.168.1.41 es-0001

2）安装elasticsearch

1. [root@es-0001 ~]# yum install -y java-1.8.0-openjdk elasticsearch
2. [root@es1 ~]# yum -y install java-1.8.0-openjdk.x86\_64
3. [root@es-0001 ~]# java -version
4. openjdk version "1.8.0\_161"
5. OpenJDK Runtime Environment (build 1.8.0\_161-b14)
6. OpenJDK 64-Bit Server VM (build 25.161-b14, mixed mode)
7. [root@es1 ~]# sestatus //查看selinux状态
8. SELinux status: disabled
9. [root@es1 ~]# yum -y install elasticsearch
10. [root@es-0001 ~]# vim /etc/elasticsearch/elasticsearch.yml
11. network.host: 0.0.0.0
12. [root@es-0001 ~]# systemctl restart elasticsearch.service
13. [root@es-0001 ~]# systemctl enable elasticsearch.service
14. [root@es-0001 ~]# ss -antup | grep 9200
15. tcp LISTEN 0 50 :::9200 :::\* users:(("java",pid=876,fd=109))
16. [root@es-0001 ~]# curl http://es-0001:9200/        //访问验证，返回 json 数据
17. {
18. "name" : "Solo",
19. "cluster\_name" : "elasticsearch",
20. "version" : {
21. "number" : "2.3.4",
22. "build\_hash" : "e455fd0c13dceca8dbbdbb1665d068ae55dabe3f",
23. "build\_timestamp" : "2016-06-30T11:24:31Z",
24. "build\_snapshot" : false,
25. "lucene\_version" : "5.5.0"
26. },
27. "tagline" : "You Know, for Search"
28. }

**2 案例2：部署Elasticsearch集群**

**2.1 问题**

本案例要求：

* 使用5台虚拟机组建 elasticsearch 集群
* 最低配置： 1cpu，1G内存，10G硬盘
* 虚拟机：
* 192.168.1.41 es-0001
* 192.168.1.42 es-0002
* 192.168.1.43 es-0003
* 192.168.1.44 es-0004
* 192.168.1.45 es-0005

**2.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：更改hosts文件，更改配置文件

1）更改hosts文件

1. [root@es-0001 ~]# vim /etc/hosts
2. 192.168.1.41 es-0001
3. 192.168.1.42 es-0002
4. 192.168.1.43 es-0003
5. 192.168.1.44 es-0004
6. 192.168.1.45 es-0005

2）更改配置文件

1. [root@es-0001 ~]# vim /etc/elasticsearch/elasticsearch.yml
2. 17 cluster.name: my-es        //配置集群名字
3. 23 node.name: es-0001        //当前主机名称
4. 54 network.host: 0.0.0.0     // 0.0.0.0（监听所有地址）
5. 68 discovery.zen.ping.unicast.hosts: ["es-0001", "es-0002", "es-0003"]
6. //声明集群里的主机成员有谁，不需要全部写进去
7. [root@es1 ~]# systemctl restart elasticsearch
8. [root@es1 ~]# ss -antup | grep 9200
9. [root@es1 ~]# ss -antup | grep 9300

3） 其他机器（1.42-1.45）一样操作，安装elasticsearch和java-1.8.0-openjdk，同步配置文件在步骤一已经安装了一台elasticsearch，这里只需再准备四台即可

1. 更改对应的主机名、 ip地址以及搭建yum源
2. 安装elasticsearch四台主机同样操作（以es-0002为例子）
3. [root@es-0002 ~]# yum -y install java-1.8.0-openjdk.x86\_64
4. [root@es-0002 ~]# yum -y install elasticsearch

4）同步配置/etc/hosts和/etc/elasticsearch/elasticsearch.yml, 修改node.name字段（以es-0002为例子）

1. [root@es-0001 ~]# for i in {42..45} ; do scp /etc/hosts 192.168.1.$i:/etc/hosts; done
2. [root@es-0001 ~]# for i in {42..45} ; do scp \
3. /etc/elasticsearch/elasticsearch.yml \
4. 192.168.1.$i:/etc/elasticsearch/elasticsearch.yml; done
5. [root@es-0002 ~]# vim /etc/elasticsearch/elasticsearch.yml
6. node.name: es-0002 //另外三台修改为对应es-0003，es-0004，es-0005
7. [root@es-0002 ~]# systemctl restart elasticsearch
8. [root@es-0002 ~]# systemctl enable elasticsearch

4）访问测试，如图-1所示：

可以访问61-65的任意一台主机， 集群的节点都是5台，若先启动的是es4或es5，这两个会自动成为各自的集群，解决办法，先启动集群里的es1或es2或es3其中的一台，或者把es4和es5重启，es4和es5会自动加进去

ES 集群验证：返回字段解析：

”status”: ”green“ 集群状态：绿色为正常、黄色表示有问题但不是很严重、红色表示严重故障

”number\_of\_nodes”： 5, 表示集群中节点的数量

1. firefox http://192.168.1.41:9200/\_cluster/health?pretty



图-1

**3 案例3：安装Elasticsearch插件**

**3.1 问题**

本案例要求：

* 给es-0005安装插件
* 插件：kopf
* 插件：head
* 插件：bigdesk

**3.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：部署插件

插件装在哪一台机器上，只能在哪台机器上使用

1）使用远程 uri 路径可以直接安装

1. [root@es-0005 bin]# cd /usr/share/elasticsearch/bin
2. [root@es-0005 bin]# ./plugin install \
3. ftp://192.168.1.254/localrepo/elk/elasticsearch-head-master.zip
4. //安装head插件
5. [root@es-0005 bin]#./plugin install \
6. ftp://192.168.1.254/localrepo/elk/elasticsearch-kopf-master.zip
7. //安装kopf插件
8. [root@es-0005 bin]#./plugin install \
9. ftp://192.168.1.254/ localrepo/elk/bigdesk-master.zip
10. //安装bigdesk插件
12. [root@es-0005 bin]# ./plugin list            //查看安装的插件
13. Installed plugins in /usr/share/elasticsearch/plugins:
14. - head
15. - kopf
16. - bigdesk

2）访问head插件，如图-2所示：

1. firefox http://192.168.1.45:9200/\_plugin/head

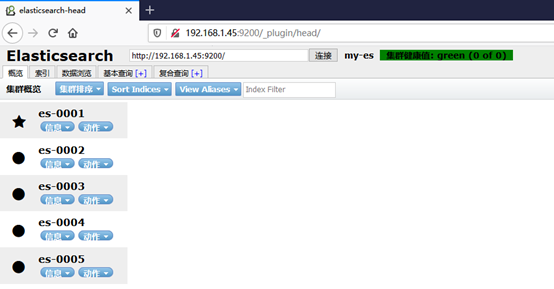


图-2

3）访问kopf插件，如图-3所示：

1. firefox http://192.168.1.45:9200/\_plugin/kopf

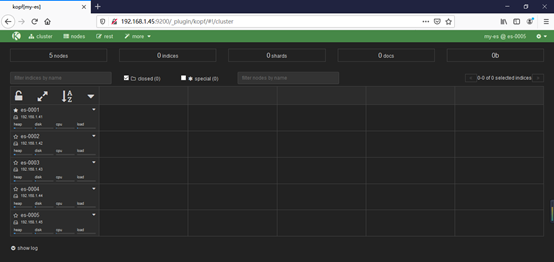


图-3

4）访问bigdesk插件，如图-4所示：

1. firefox http://192.168.1.45:9200/\_plugin/bigdesk

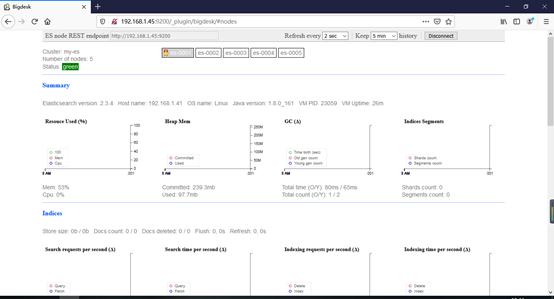


图-4

**4 案例4：熟悉Elasticsearch的API调用**

**4.1 问题**

本案例要求：

* 熟悉Elasticsearch的Api调用
* 增：PUT
* 删：DELETE
* 改：POST
* 查：GET

**4.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：创建 tedu 索引使用 PUT 方式

1. [root@es-0005 bin]# curl -XPUT 'http://es-0001:9200/tedu' -d '{
2. "settings":{
3. "index":{
4. "number\_of\_shards": 5,
5. "number\_of\_replicas": 1
6. }
7. }
8. }'
9. {"acknowledged":true}

步骤二：增加数据

1. [root@es-0005 bin]# curl -XPUT 'http://es-0001:9200/tedu/teacher/1' -d \
2. > '{
3. > "职业": "诗人",
4. > "名字": "李白",
5. > "称号": "诗仙",
6. > "年代": "唐"
7. > }'
8. {"\_index":"tedu","\_type":"teacher","\_id":"1","\_version":1,"\_shards":{"total":2,"successful":2,"failed":0},"created":true}

步骤三：查询数据

1. [root@es-0005 bin]# curl -XGET http://es-0001:9200/tedu/teacher/1?pretty
2. {
3. "\_index" : "tedu",
4. "\_type" : "teacher",
5. "\_id" : "1",
6. "\_version" : 1,
7. "found" : true,
8. "\_source" : {
9. "职业" : "诗人",
10. "名字" : "李白",
11. "称号" : "诗仙",
12. "年代" : "唐"
13. }
14. }

步骤四：修改数据

1. [root@es-0005 bin]# curl -XPOST http://es-0001:9200/tedu/teacher/1/\_update -d \
2. > '{
3. > "doc": {
4. > "年代": "公元701"
5. > }
6. > }'
7. {"\_index":"tedu","\_type":"teacher","\_id":"1","\_version":2,"\_shards":{"total":2,"successful":2,"failed":0}}

步骤五：删除数据

注：删除时候可以是文档，也可以是索引，但不能是类型

1. [root@es-0005 bin]# curl -XDELETE http://es-0001:9200/tedu/teacher/1
2. {"found":true,"\_index":"tedu","\_type":"teacher","\_id":"1","\_version":3,"\_shards":{"total":2,"successful":2,"failed":0}}
3. [root@es-0005 bin]# curl -XDELETE http://es-0001:9200/tedu
4. {"acknowledged":true}[root@es-0005 bin]#
5. [root@es-0005 bin]#
6. [root@es-0005 bin]# curl -XDELETE http://es-0001:9200/\*
7. {"acknowledged":true}

**5 案例5：安装Kibana**

**5.1 问题**

本案例要求批量导入数据：

* 创建虚拟机并安装 kibana
* 最低配置： 1cpu，1G内存，10G硬盘
* 虚拟机IP： 192.168.1.46 kibana

**5.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：安装kibana

1）在另一台主机，配置ip为192.168.1.46，配置yum源，更改主机名

2）安装kibana

1. 更改hosts文件
2. [root@kibana ~]# vim /etc/hosts
3. 192.168.1.41 es-0001
4. 192.168.1.42 es-0002
5. 192.168.1.43 es-0003
6. 192.168.1.44 es-0004
7. 192.168.1.45 es-0005
8. 192.168.1.46 kibana
9. [root@kibana ~]# yum -y install kibana

3）更改配置文件

1. [root@kibana ~]# vim /opt/kibana/config/kibana.yml
2. 2 server.port: 5601
3. 5 server.host: "0.0.0.0"
4. 15 elasticsearch.url: http://es-0001:9200
5. 23 kibana.index: ".kibana"
6. 26 kibana.defaultAppId: "discover"
7. [root@kibana ~]# systemctl start kibana
8. [root@kibana ~]# systemctl enable kibana

步骤二：web 页面访问，如图-5所示：

1. Firefox http://192.168.1.46:5601

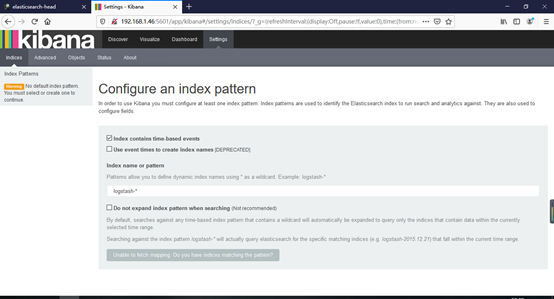


图-5

**6 案例6：导入日志并绘制图表**

**6.1 问题**

本案例要求批量导入数据：

* 导入日志，并绘制图表
* 导入 logs 日志
* 绘制流量图和饼图

**6.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：导入数据

1. [root@localhost ~]# scp /var/ftp/localrepo/elk/\*.gz [root@192.168.1.46](mailto:root@192.168.1.46):/root/
2. [[root@kibana](mailto:root@kibana) ~]# gzip -d logs.jsonl.gz
3. [[root@kibana](mailto:root@kibana) ~]# curl -XPOST <http://es-0001>:9200/\_bulk --data-binary @logs.jsonl

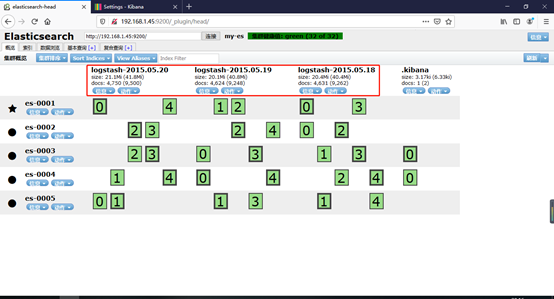


图-6

3）kibana导入数据，如图-7所示：

1. firefox http://192.168.1.46:5601

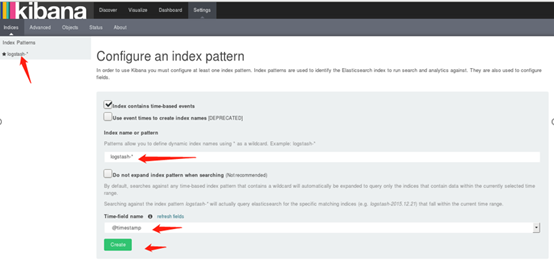


图-7

3）成功创建会有logstash-\*，如图-8所示：



图-8

4）导入成功之后选择Discover，如图-9所示：

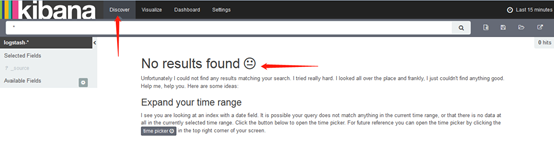


图-9

注意： 这里没有数据的原因是导入日志的时间段不对，默认配置是最近15分钟，在这可以修改一下时间来显示

5）kibana修改时间，选择Lsat 15 miuntes，如图-10所示：

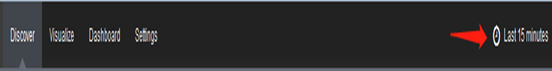


图-10

6）选择Absolute，如图-11所示：

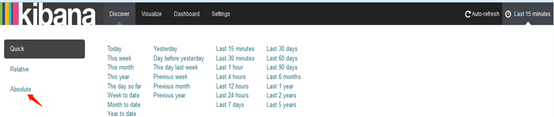


图-11

7）选择时间2015-5-15到2015-5-22，如图-12所示：

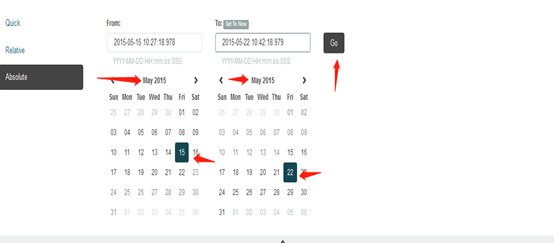


图-12

8）查看结果，如图-13所示：



图-13

9）除了柱状图，Kibana还支持很多种展示方式 ，如图-14所示：

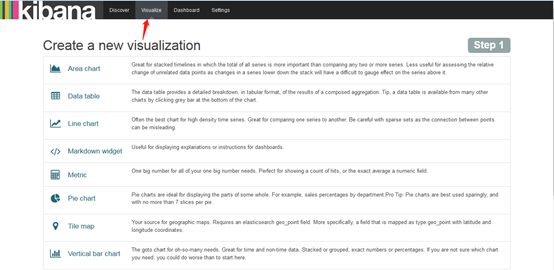


图-14

10）做一个饼图，选择Pie chart，如图-15所示：

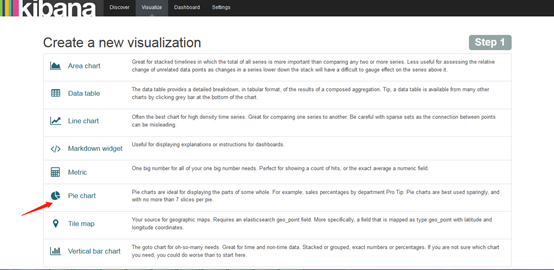


图-15

11）选择from a new serach，如图-16所示：

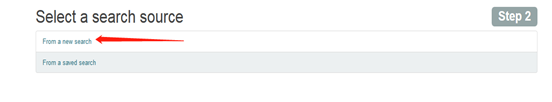


图-16

12）选择Spilt Slices，如图-17所示：

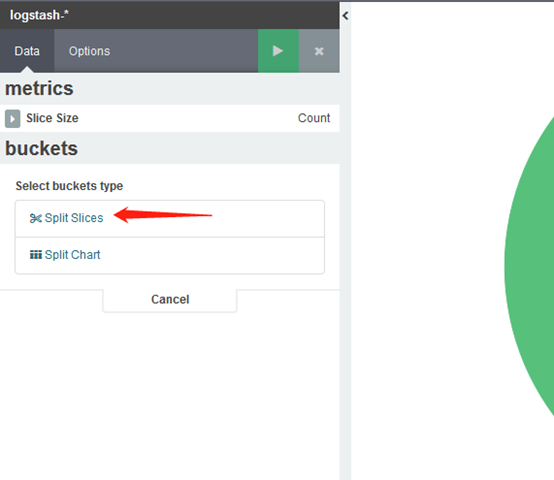


图-17

13）选择Trems,Memary(也可以选择其他的，这个不固定)，如图-18所示：

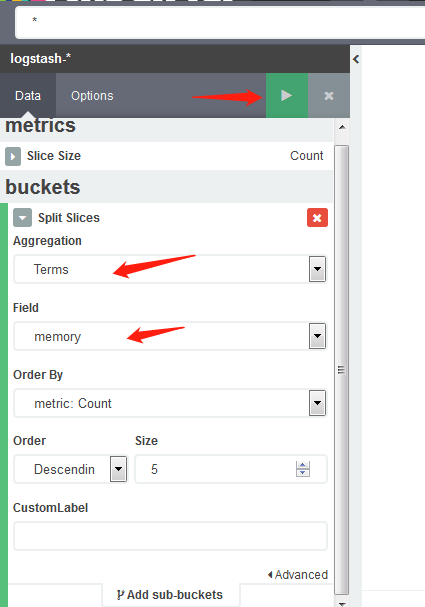


图-18

14）结果，如图-19所示：

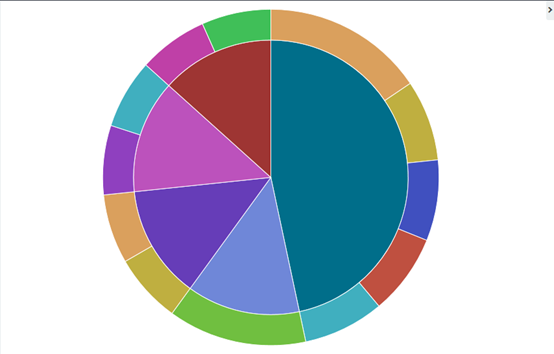


图-19

15）保存后可以在Dashboard查看，如图-20所示：

