ES集群安装

部署ES集群，用于ELK日志分析平台的构建

主机名称	IP地址	角色	规格
es-0001	192.168.1.71	Elasticsearc第一个节点	8CPU16G内存
es-0002	192.168.1.72	Elasticsearc第二个节点	8CPU/16G内存
es-0003	192.168.1.73	Elasticsearc第三个节点	8CPU/16G内存
kibana	192.168.1.74	Kibana	8CPU/16G内存
logstash	192.168.1.75	Logstash	8CPU/16G内存

```
es-0001主机更改/etc/hosts
[root@ es-0001 ~]# vim /etc/hosts
192.168.1.71 es-0001
192.168.1.72 es-0002
192.168.1.73 es-0003
192.168.1.74 kibana
192.168.1.75 logstash

将最新的/etc/hosts配置文件更新到所有的云主机上
[root@es-0001 ~]# for i in 192.168.1.{72..75}; do scp /etc/hosts $i:/etc; done

在跳板机ecs-proxy将ELK相关软件包做好YUM仓库,若之前跳板机已经配置好，则不用再次配置

集群安装配置，安装基础环境软件
es-0001,es-0002,es-0003检查yum源，确定可以使用
[root@es-0001 ~]# cat /etc/yum.repos.d/local.repo
[local_repo]
name=CentOS-$releasever - Localrepo
baseurl=ftp://192.168.1.252/localrepo
enabled=1
gpgcheck=0
[root@es-0001 ~]# for i in 192.168.1.{72..75}; do scp /etc/yum.repos.d/local.repo
$i:/etc/yum.repos.d; done

[root@es-0001 ~]# for i in 192.168.1.{71..75}; do ssh $i yum -y install java-1.8.0-openjdk-
devel; done

#检测JDK环境安装是否成功
[root@es-0001 ~]# java -version
openjdk version "1.8.0_252"
OpenJDK Runtime Environment (build 1.8.0_252-b09)
......

es-0001，es-0002，es-0003安装elasticserach
[root@es-0001 ~]# yum -y install elasticsearch

配置es-0001
[root@es-0001 ~]# vim /etc/elasticsearch/elasticsearch.yml
```

```
17 cluster.name: es                    #集群的名称。
23 node.name: es-0001                  #该节点主机名。
55 network.host: 0.0.0.0          #该节点主机的IP地址。
68 discovery.zen.ping.unicast.hosts: ["es-0001", "es-0002", "es-0003"] #集群节点主机列表
[root@es-0001 ~]# systemctl enable --now elasticsearch
[root@es-0001 ~]# systemctl status elasticsearch
```

配置es-0002和0003

```
[root@es-0001 ~]# scp /etc/elasticsearch/elasticsearch.yml  192.168.1.72:/etc/elasticsearch/
[root@es-0001 ~]# scp /etc/elasticsearch/elasticsearch.yml  192.168.1.73:/etc/elasticsearch/

[root@es-0002 ~]# vim /etc/elasticsearch/elasticsearch.yml
 23 node.name: es-0002
[root@es-0002 ~]# systemctl enable --now elasticsearch

[root@es-0003 ~]# vim /etc/elasticsearch/elasticsearch.yml
 23 node.name: es-0003
[root@es-0003 ~]# systemctl enable --now elasticsearch
```

查看ES集群信息

```
[root@es-0003 ~]# curl -XGET http://192.168.1.71:9200/_cluster/health?pretty
{
"cluster_name" : "es",
"status" : "green",
"timed_out" : false,
"number_of_nodes" : 3,
"number_of_data_nodes" : 3,
"active_primary_shards" : 0,
"active_shards" : 0,
"relocating_shards" : 0,
"initializing_shards" : 0,
"unassigned_shards" : 0,
"delayed_unassigned_shards" : 0,
"number_of_pending_tasks" : 0,
"number_of_in_flight_fetch" : 0,
"task_max_waiting_in_queue_millis" : 0,
"active_shards_percent_as_number" : 100.0
}
```

安装head插件：ES官方没有为ES提供界面管理工具，仅仅提供了后台服务。elasticsearch-head是一个为ES开发的web页面客户端工具

部署插件
由于前后端分离开发，所以会存在跨域问题，需要在服务端做CORS的配置。
(前后端分离：前端所有用到的数据都是后端通过异步接口的方式提供的，前端只管页面的展示及效果。)

在配置文件末尾手动添加以下内容即可

```
[root@es-0001 ~]# vim /etc/elasticsearch/elasticsearch.yml
http.cors.enabled : true
http.cors.allow-origin : "*"
http.cors.allow-methods : OPTIONS, HEAD, GET, POST, PUT, DELETE
http.cors.allow-headers : X-Requested-With,X-Auth-Token,Content-Type,Content-Length
[root@es-0001 ~]# systemctl restart elasticsearch
```

es-0001主机安装head插件，提供访问es的页面

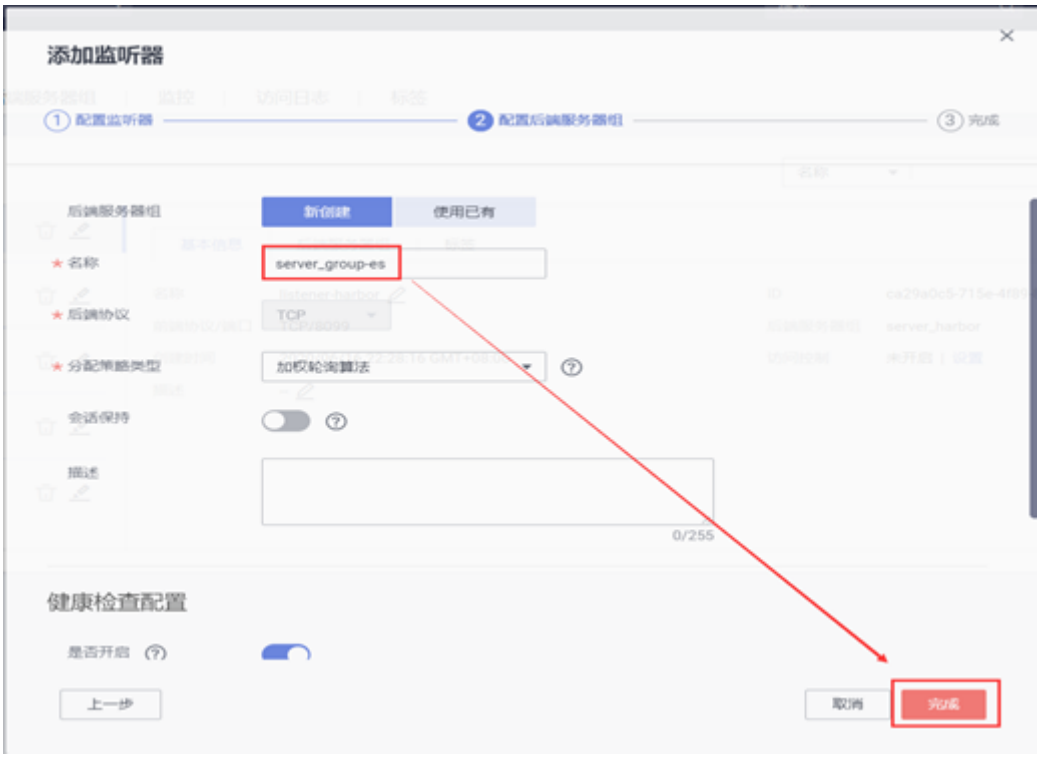
```
[root@es-0001 ~]# yum -y install httpd
[root@es-0001 ~]# scp  192.168.1.252:/root/head.tar.gz   /root
[root@es-0001 ~]# tar -xf head.tar.gz  -C /var/www/html/
[root@es-0001 ~]# cd /var/www/html/
[root@es-0001 html]# mv elasticsearch-head/ head
```

创建监听器（9200），添加后端服务器群组

【服务器列表】—>【弹性负载均衡ELB】—>【(自定义ELB名称)】—>【监听器】—>【添加监听器】

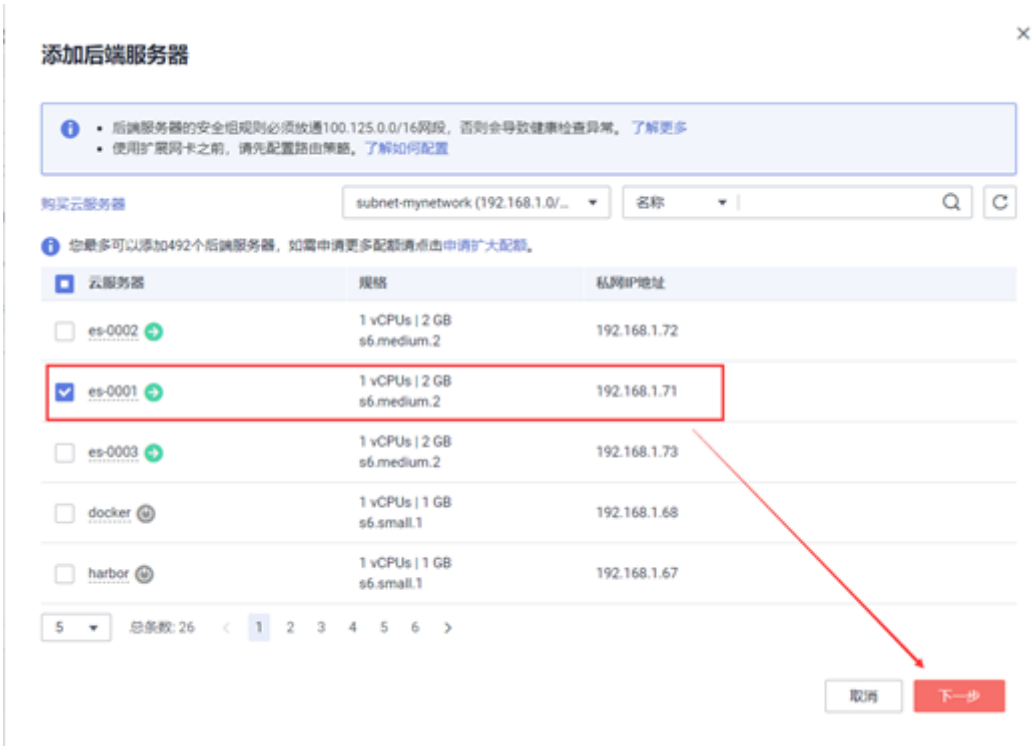
更改监听器名称，并且配置前端协议端口为9200

配置后端服务器组，更改名称，点击完成。如图-3所示



点击【后端服务器群组】，找到我们刚才添加的【server_group-es】，并单击。【添加】后端真实服务器。如图-4所示。

添加es-0001为后端服务器成员，点击下一步。如图-5所示。

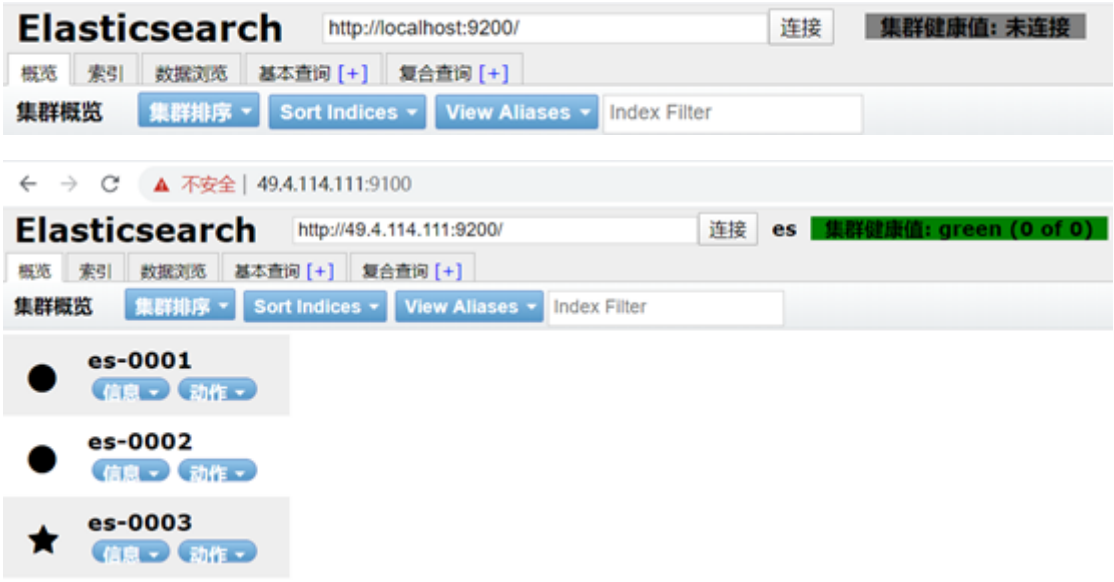


配置后端服务器提供服务的端口9200，点击完成。如图-6所示。

创建监听器（80），添加后端服务器群组，把es-0001上面80端口监听，测试即可

访问head插件：elb的公网ip，http://公网IP/head/

默认打开是未连接状态。将http://localhost:9200/改为http://公网IP:9200，并点击连接。



部署kibana

Kibana是一款开源的数据分析和可视化平台，它是Elastic Stack成员之一。可以使用Kibana对Elasticsearch索引中的数据进行搜索、查看、交互操作。可利用图表、表格等对数据进行多元化的分析和显现。

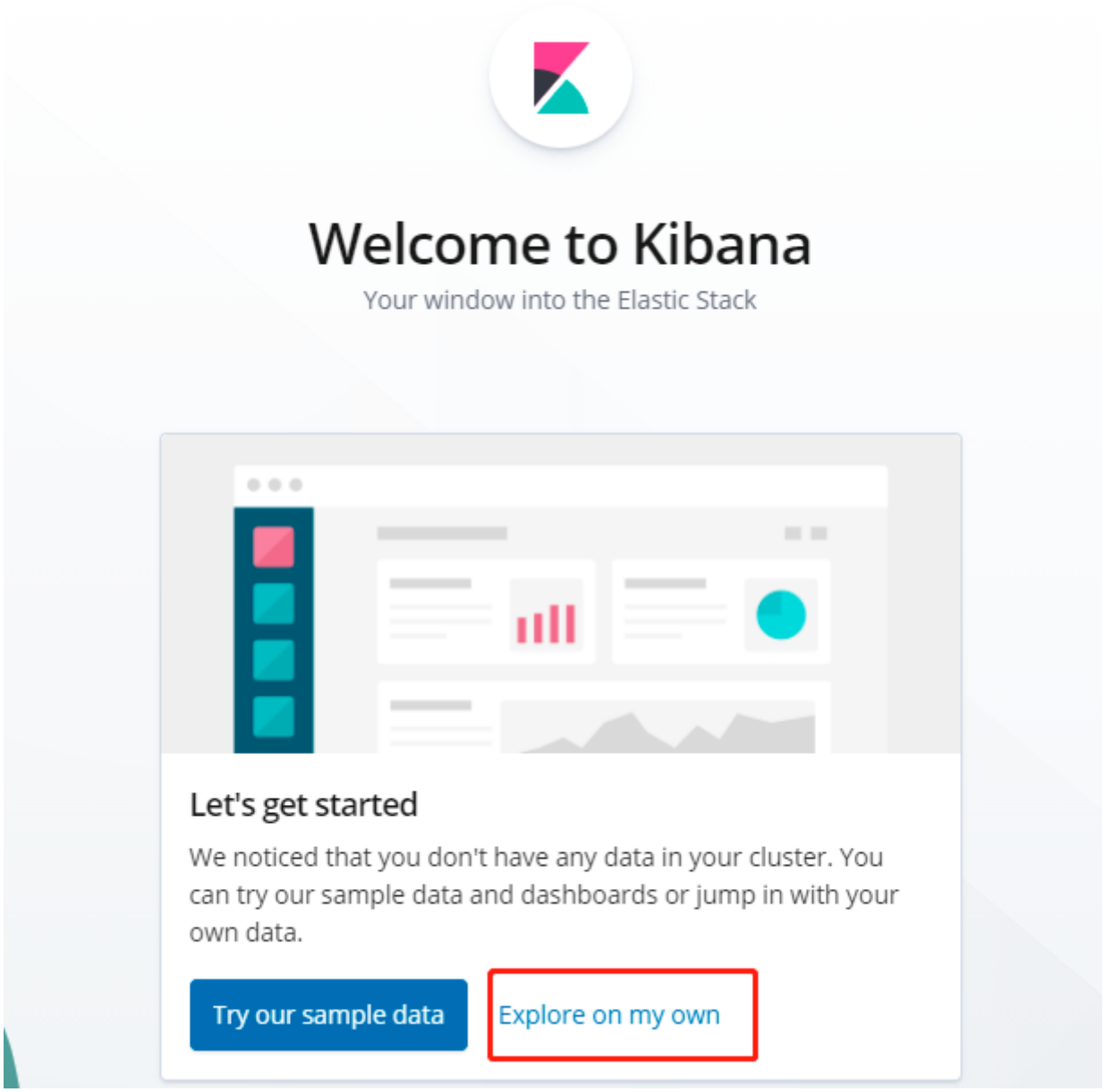
```
安装kibana软件包
[root@kibana ~]# yum -y install kibana
更改kibana服务配置文件
[root@kibana ~]# vim /etc/kibana/kibana.yml
2 server.port: 5601           #提供服务的端口。
7 server.host: "192.168.1.74"       #服务器监听地址。
28 elasticsearch.hosts: ["http://192.168.1.71:9200"]    #用于查询es实例主机地址，集群里面任选一个即可。

启动服务器并查看端口是否启用
[root@kibana ~]# systemctl enable --now kibana
[root@kibana ~]# ss -antpu | grep 5601
```

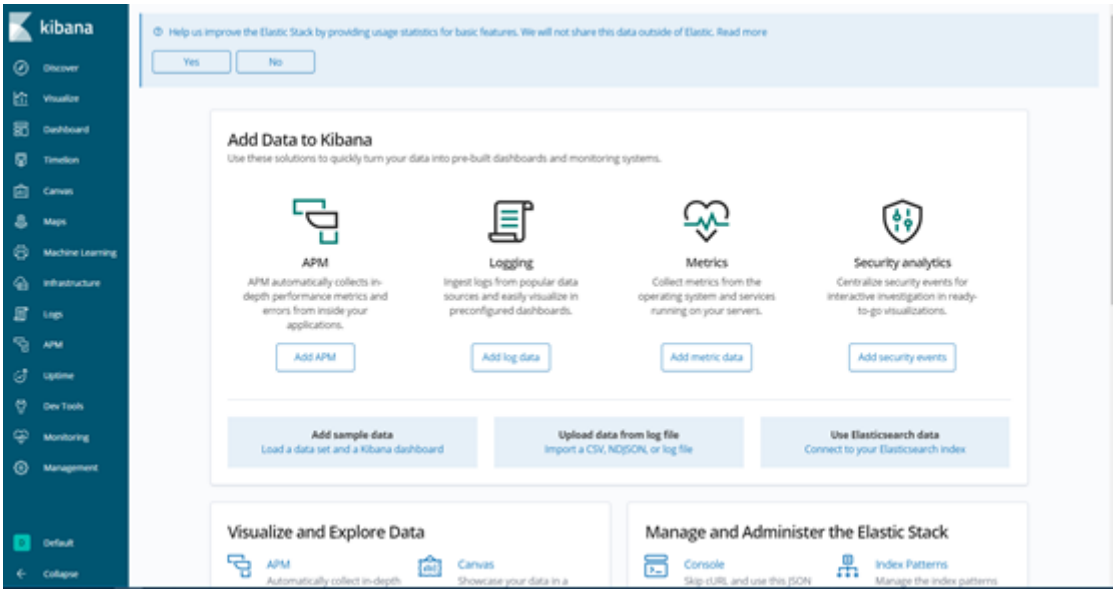
通过浏览器访问kibana，创建监听器，并添加后端服务器。

【服务器列表】—>【弹性负载均衡ELB】—>【(自定义ELB名称)】—>【监听器】—>【添加监听器】

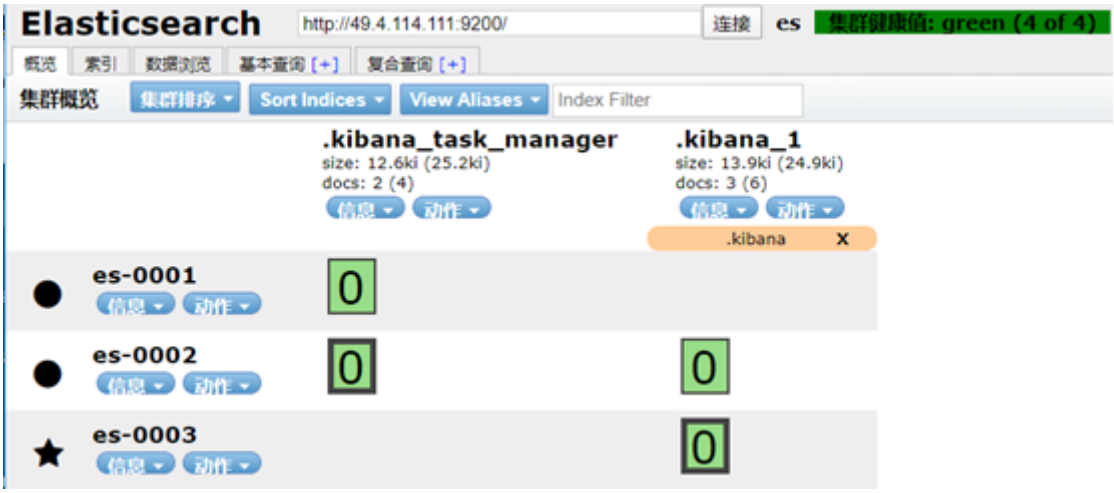
此次监听端口为5601，添加后端服务kibana

访问kibana界面：http://公网IP:5601





用head插件访问es集群，会查看到.kibana的索引信息


Elasticsearch
http://49.4.114.111:9200/
连接
es
集群健康值: green (4 of 4)
概览
索引
数据浏览
基本查询 [+]
复合查询 [+]
集群概览
集群排序
Sort Indices
View Aliases
Index Filter
.kibana_task_manager
size: 12.6ki (25.2ki)
docs: 2 (4)
信息
动作
.kibana_1
size: 13.9ki (24.9ki)
docs: 3 (6)
信息
动作
.kibana
x
es-0001
信息
动作
0
es-0002
信息
动作
0
0
es-0003
信息
动作
0