elasticsearch手册

一、日志平台elasticsearch架构

日志平台elasticsearch集群由es-master,es-data,es-data组成。es的master节点为候选主节点，负责创建索引、删除索引、分配分片、追踪集群中的节点状态。es-data节点为数据节点，主要负责数据存储及相关操作。es-balance节点为客户端节点，主要负责数据分发、汇总。日志平台elasticsearch集群架构图如图1

图1



master节点

master节点配置方法将node.master设置成true，node.data设置成false。在配置成候选主节点之后，全部启动后参与选举，最终选举出主节点，其余节点依然为候选主节点，在主节点出现问题时，候选主节点会重新选举。

data节点

data节点配置方法将node.master设置成false，node.data设置成true。数据节点主要负责存储数据，对磁盘要求比较大。多块磁盘配置可在配置文件中加入path.data: 后接挂载点，多个使用逗号分隔。如日志平台配置path.data: /data01/es1, /data02/es1，/data03/es1，/data04/es1，/data05/es1

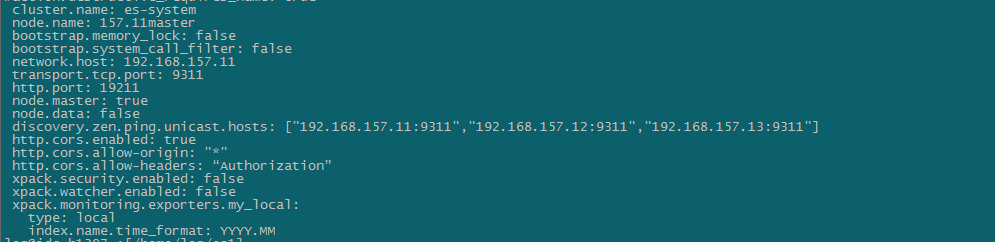
balance节点（客户端节点）

balance节点配置方法node.master设置成false，node.data设置成false。客户端节点主要负责数据分发、汇总。如一个查询balance节点会分发到各data节点查询到结果再汇总成完成的数据返回给用户。

二、配置文件详解

如图2为日志平台es的system集群master节点配置文件

图2



cluster.name: es-system

配置es的集群名称，默认是elasticsearch，可根据cluster.name区分集群，同一网段下相同名字为一个集群。

node.name: 157.11master

配置es节点名称，可根据集群分布自己定义

bootstrap.memory\_lock: false

此配置为5.x版本，5版本之前配置为bootstrap.mlockall: false，设置成false保证使用swap，即允许内存交换。可以设置为true来锁住内存，此时尽量加大es内存配置。

bootstrap.system\_call\_filyter: false

系统调用过滤器，一般设置成false

network.host: 192.168.157.11

配置bind host配置成主机IP地址

transport.tcp.port: 9311

设置节点间交互的tcp端口，默认是9300。

http.port: 19211

设置对外服务的http端口，默认为9200。

node.master: true

设置es节点是否为候选主节点，为候选主节点配置成true，非则配置成false

node.data: false

设置es节点是否为数据节点，为true时可存储数据，为false则为非数据节点

discovery.zen.ping.unicast.hosts: ["192.168.157.11:9311", "192.168.157.12:9311","192.168.157.13:9311"]

提供其他 Elasticsearch 服务节点的单点广播发现功能。配置集群中基于主机 TCP 端口的其他 Elasticsearch 服务的逗号分隔列表。

http.cors.enabled: true

如果启用了 HTTP 端口，那么此属性会指定是否允许跨源 REST 请求。

http.cors.allow-origin "\*"

如果 http.cors.enabled 的值为 true，那么该属性会指定允许 REST 请求来自何处。

http.cors.allow-headers: "Authorization"

跨域允许设置的头信息，默认为X-Requested-With,Content-Type,Content-Length

xpack.security.enabled: false

禁用 xpack的 安全机制

xpack.watcher.enabled: false

禁用观察器

xpack.monitoring.exporters.my\_local:

type: local

index.name.time\_format: YYYY.MM

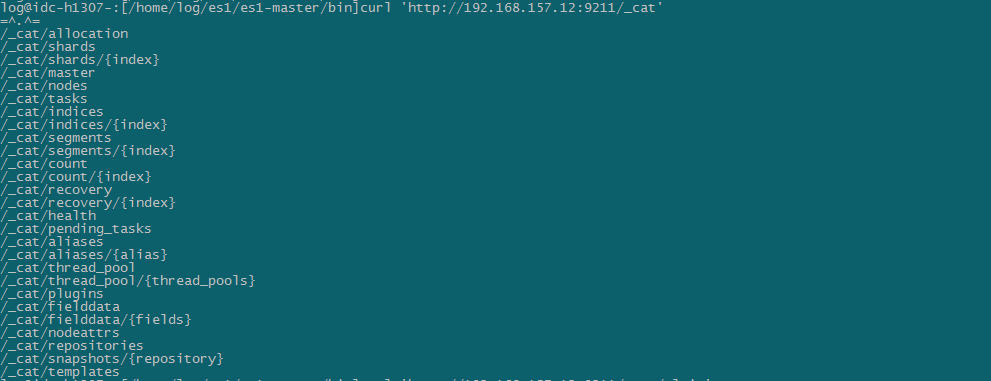
本地导出设置，本地的导出是默认的导出器由Monitoring来使用。

三、常用指令

常用指令以日志平台系统为例

执行curl 'http://192.168.157.12:9211/\_cat'显示cat下的指令，如图3

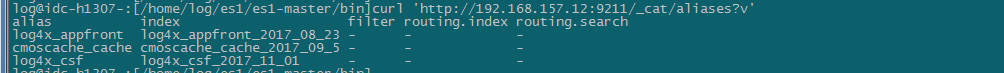
图3



aliases指令

实例中打印alias和index对应的信息如图4

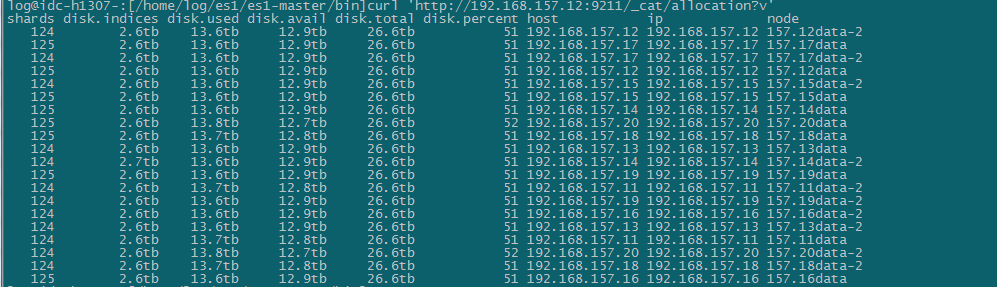
图4



allocation指令

该指令提供一个快照，反映当前节点有多少个分片（shard）以及用了多少磁盘空间（disk）如图5

图5



count指令

该指令可以获取当前集群中有多少个document，类似mysql中有多少条记录，也可以获取指定index的document的数量。如图6

图6



获取单个索引document数量，如图7

图7



health指令

该指令反应当前集群的健康指数信息。如图8

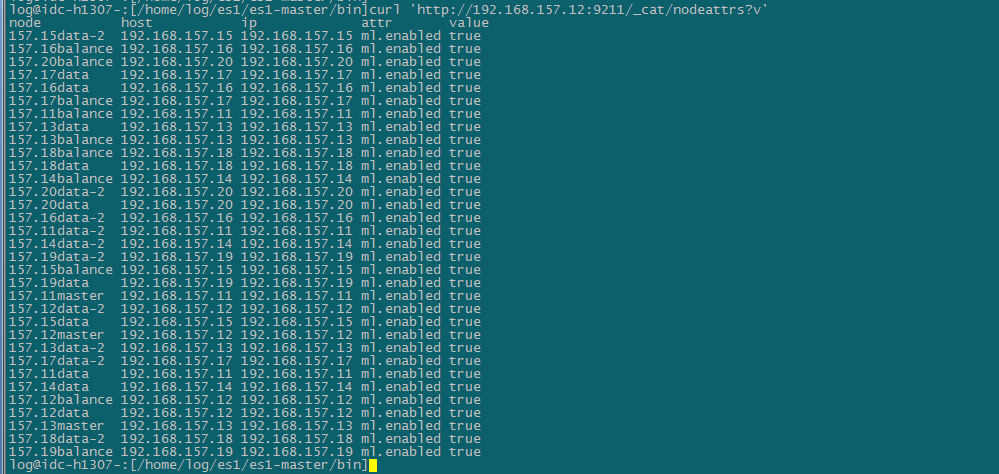
图8



nodeattrs指令

该指令可以反应出当前数据节点的属性信息。如图9

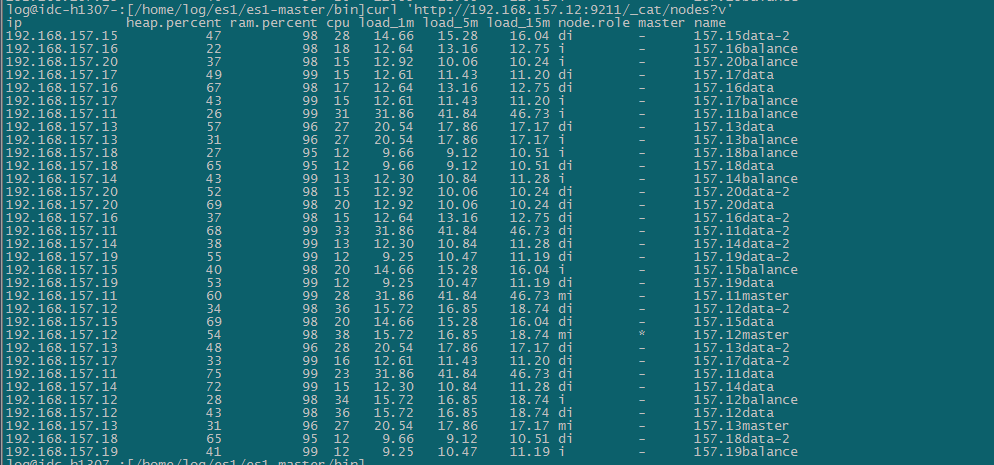
图9



nodes指令

该指令反应出当前集群的拓扑信息。如图10

图10



pending\_tasks指令

该指令反应当前集群有多少任务处在pending状态，与指令/\_cluster/pending\_tasks的效果一样。如图11

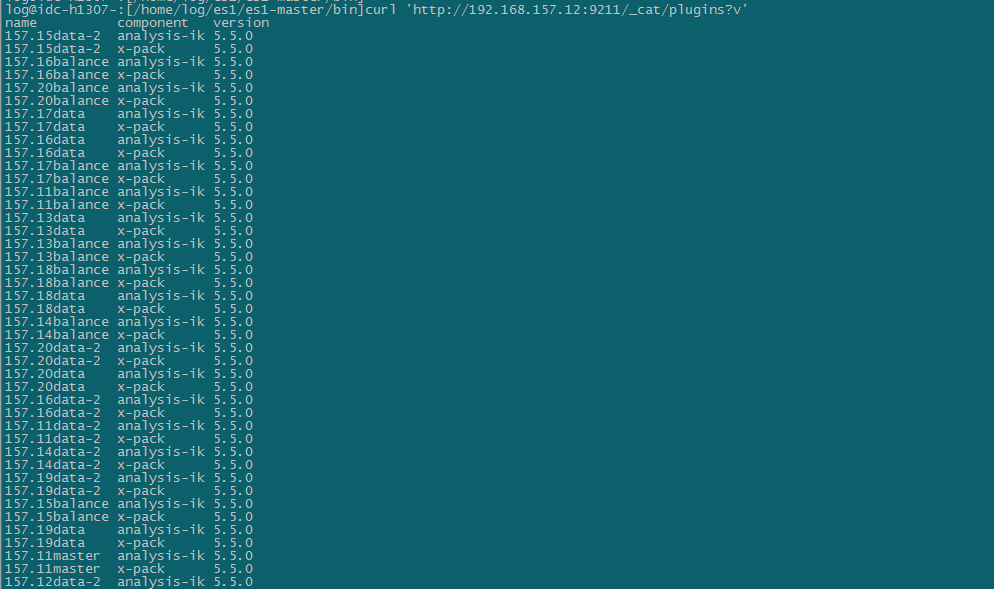
图11



plugins指令

该指令提供一个视图，反应当前节点中处在运行状态的插件及版本。如图12

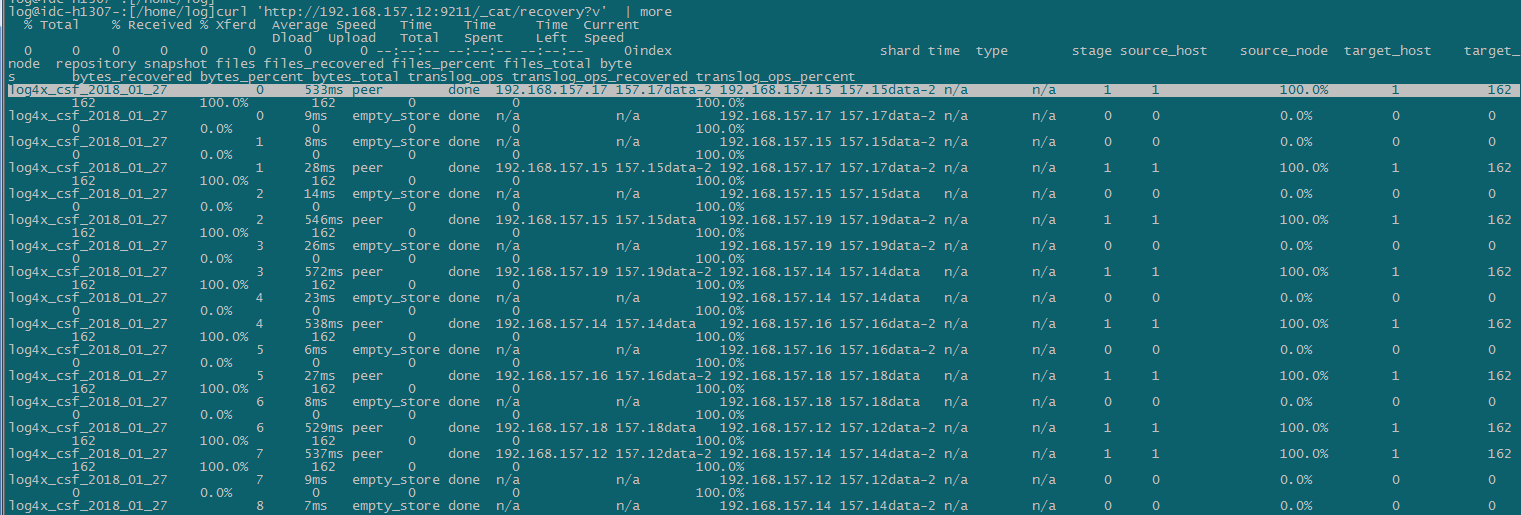
图12



recovery指令

该指令反应当前系统中，索引分片的恢复信息，包括正在进行的以及已经完成了的。恢复，指的是当节点添加或者减少时发生的数据移动造成的。如图13

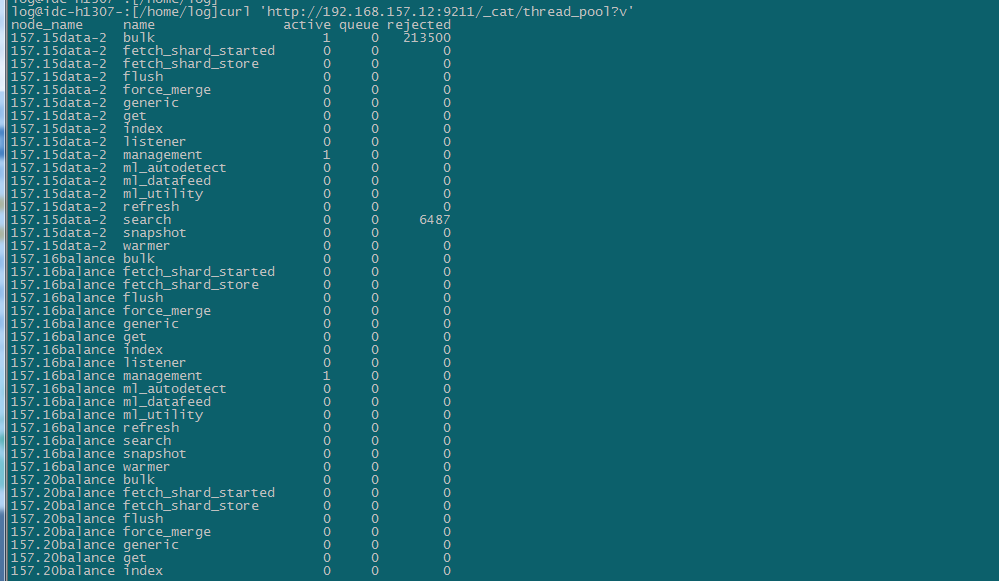
图13



hread\_pool指令

该指令反应当前集群中的thread pool在每一个节点上的统计信息。 “By default the active, queue and rejected statistics are returned for the bulk, index and search thread pools”如图14

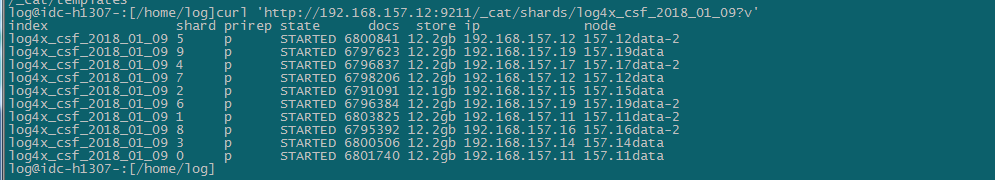
图14



shards指令

该指令，相对比较重要，反应每个节点有那些分片，告诉我们，那些是主分片，那些是从分片，每个分片的document数量，以及在该节点占用的磁盘空间。如图15

图15



三、对索引操作

创建模板

索引可使用预定义的模板进行创建,这个模板称作Index templates，模板设置包括settings和mappings，通过模式匹配的方式使得多个索引重用一个模板，例如：

定义模板：

curl -XPUT 'http://192.168.100.106:9200/\_template/errorlogs\_template?pretty' -H 'Content-Type: application/json' -d '

{

"template" : "errorlogs\_\*",

"settings": {

"index": {

"number\_of\_replicas": "1",

"number\_of\_shards": "6",

"refresh\_interval": "30s"

}

},

"mappings": {

"errorlogs": {

"dynamic": false,

"properties": {

"systemCode": {

"type": "keyword"

},

"appName": {

"type": "keyword"

},

"instanceName": {

"type": "keyword"

},

"hostIp": {

"type": "keyword"

},

"traceId": {

"type": "keyword"

},

"serviceName": {

"type": "keyword"

},

"province": {

"type": "keyword"

},

"errorCode": {

"type": "keyword"

},

"errorMsg": {

"type": "text",

"analyzer": "ik\_max\_word"

},

"errorTime": {

"type": "date",

"format": "yyyyMMddHHmmss"

},

"exceptionStack": {

"type": "text",

"analyzer": "ik\_max\_word"

},

"browserType": {

"type": "keyword"

},

"opId": {

"type": "keyword"

}

}

}

}

}

'

命令注释：

curl命令是一个利用URL规则在命令行下工作的文件传输工具，它支持文件的上传和下载，所以是综合传输工具，但按传统，习惯称curl为下载工具。作为一款强力工具，curl支持包括HTTP、HTTPS、ftp等众多协议，还支持POST、cookies、认证、从指定偏移处下载部分文件、用户代理字符串、限速、文件大小、进度条等特征。

-X //url命令的选项，后指定什么命令

PUT //UT请求

http://192.168.100.106:9200/\_template/errorlogs\_template?pretty //s的URL

-H //头信息

-d //TTP POST方式传送数据

"template" : "errorlogs\_\*" //表示对此模板对errorlogs\_开头的索引有效

"settings": { //settings部分设置索引信息

"index": {

"number\_of\_replicas": "1", //表示一个副本

"number\_of\_shards": "6", //表示6个分片

"refresh\_interval": "30s" //表示30秒合并时间间隔，默认一秒。把写入的数据合并成一个segment，并创建前缀索引 }

},

"mappings": { //模板的具体配置

"errorlogs": {

"dynamic": false,

"properties": { //存放具体每个索引的配置

"systemCode": { //字段，相当于数据库的字段

"type": "keyword" //字段类型

建立别名

curl -XPOST 'http:// 192.168.124.168:9200/\_aliases' -d '

{

"actions": [

{"add": {"index": "test1", "alias": "alias1"}}

]

}'

命令注释：将别名alias1与索引test1建立关联

移除别名

curl -XPOST '192.168.124.168:9200/\_aliases' -d '

{

"actions": [

{"remove": {"index": "ngcct\_contact\_2017\_10\_19", "alias": "ngcct\_contact"}}

]

}

命令注释：将ngcct\_contact\_2017\_10\_19索引的别名ngcct\_contact移除

别名重命名

curl -XPOST 'http:// 192.168.124.168:9200/\_aliases' -d '

{

"actions": [

{"remove": {"index": "test1", "alias": "alias1"}},

{"add": {"index":"test1", "alias": "alias2"}}

]

}'

命令注释：先移除别名再增加别名

多个索引关联一个别名

curl -XPOST '192.168.124.168:9200/\_aliases' -d '

{

"actions": [

{"add": {"index": "test1", "alias":"alias1"}},

{"add": {"index": "test2", "alias":"alias1"}}

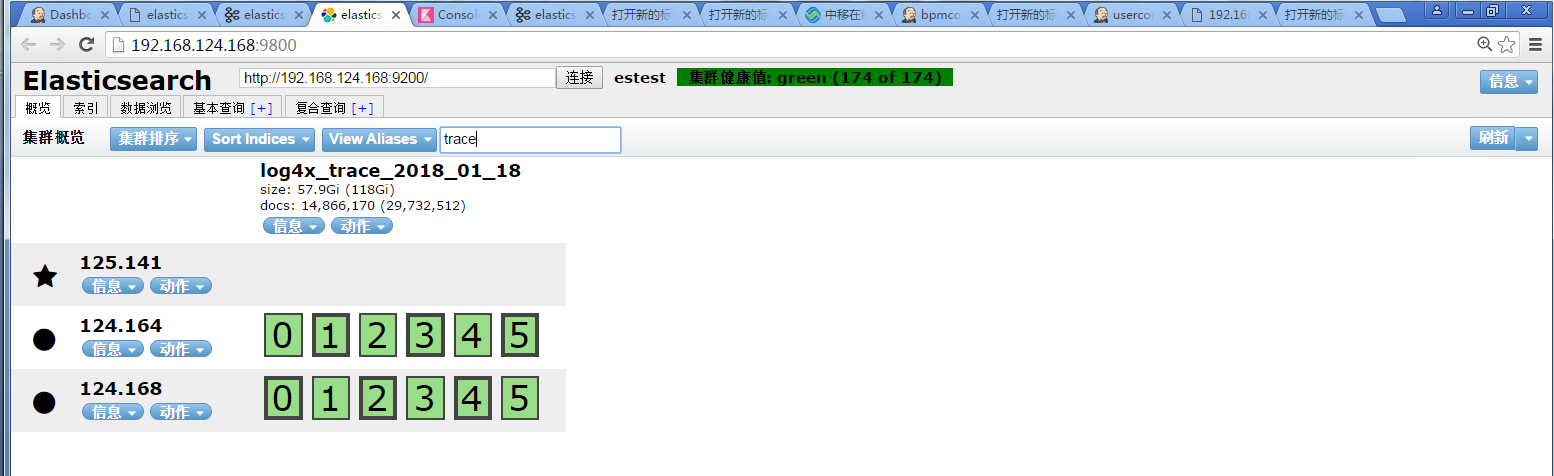
]

}'

命令注释：将别名alias1关联索引test1和test2

elasticsearch页面，如图16为日志平台测试环境

图16



访问地址：

http://192.168.124.168:9800为head页面的地址

http://192.168.124.168:9200为es的节点地址

页面信息：

集群若正常显示集群名，集群健康值:green(num of num)，测试实例集群名estest

概览 索引 数据浏览 基本查询 符合查询

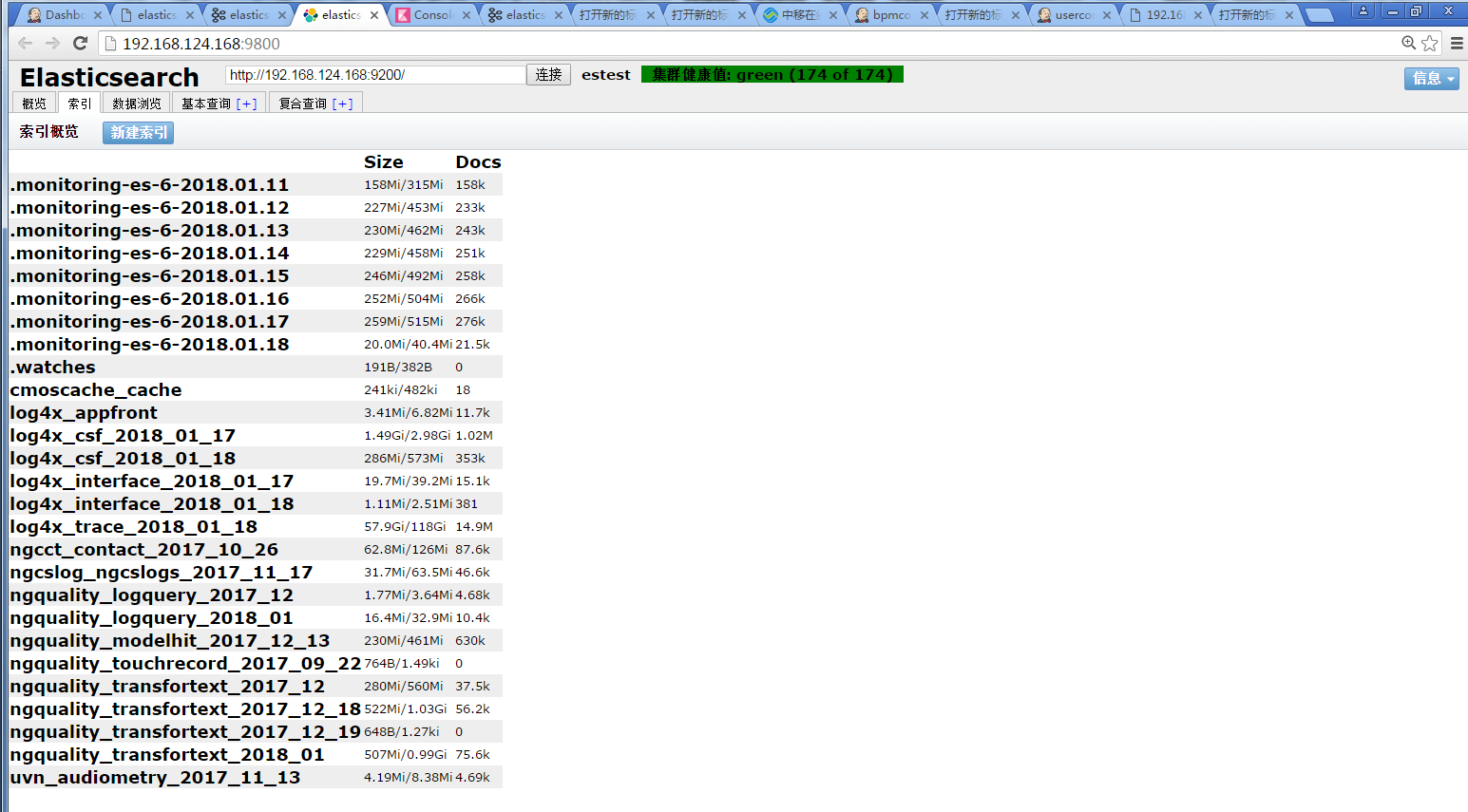
概览页面如上图为索引log4x\_trace\_2018\_01\_18信息包含索引size和文档大小docs

五角星符号表示主节点，圆圈符号表示数据节点

012345表示数据分片，124.164节点和124.168节点各位012345上下相同数据为副本

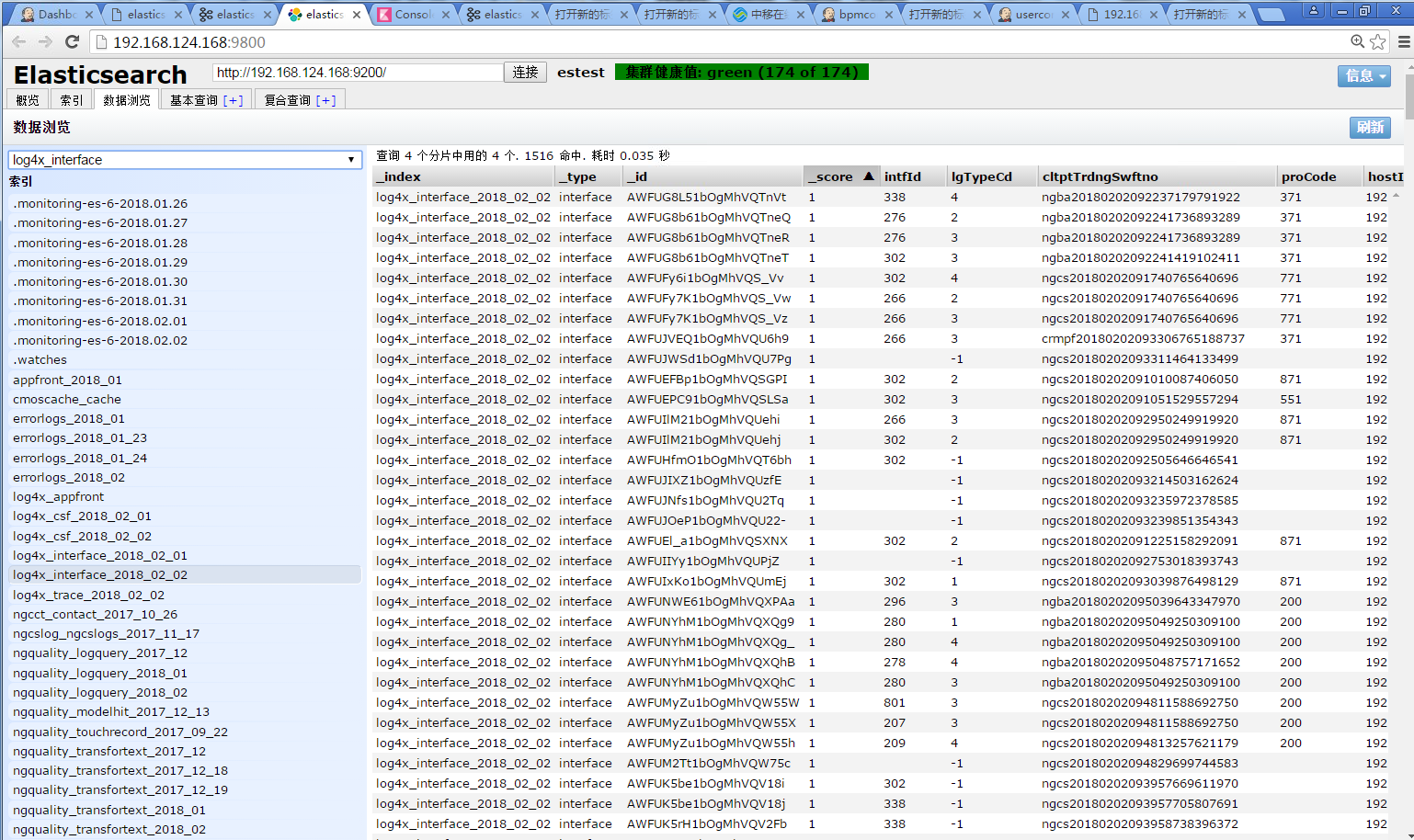
索引页面如图17，包含此集群的所有索引，索引大小，文档大小

图17



数据浏览页面如图18，可查询索引的所有字段数据

图18



基本查询页面如图，可根据索引名，字段，字段模糊匹配查询索引，输出结果有三种格式，tabl, json, csv如图19

图19

