Elasticsearch

一、安装elasticsearch-8.4.1

1.准备三台服务器，添加解析

```
# 三台服务器分别执行以下命令
cat >> /etc/hosts << eof
192.168.79.110 superbox
192.168.79.120 superbox2
192.168.79.130 superbox3
eof
```

2.修改

```
# 在最后面添加或修改以下参数
vim /etc/security/limits.conf
* soft nofile 65536
* hard nofile 65536
* soft nproc 8192
* hard nproc 8192
* soft memlock unlimited
* hard memlock unlimited
```

3.三台服务器分别创建数据和日志目录。

```
# 创建数据包存储目录
mkdir -p /data/bao
# 创建数据和日志目录
mkdir -p /data/elk-{log,data}
```

4.三台服务器都下载elasticsearch-8.4.1

```
wget
https://artifacts.elastic.co/downloads/elasticsearch/ela
sticsearch-8.4.1-x86_64.rpm
```

5.分别解压elasticsearch-8.4.1

```
rpm -ivh elasticsearch-8.4.1-x86_64.rpm
```

6.分别修改配置文件

```
# 备份配置文件
cp /etc/elasticsearch/elasticsearch.yml
/etc/elasticsearch/elasticsearch.yml.bak
# 开始修改
vim elasticsearch.yml
```

7.修改cluster模块:

```
# 起一个集群名称，三台服务器要一样
cluster.name: myelk
```

```
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: myelk
#
```

8.修改node模块:

```
# node.name: 自己的主机名
node.name: superbox
```

```
# ------------------------------------ Node ------------------------------------
#
# Use a descriptive name for the node:
#
node.name: superbox
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
```

9.修改Paths模块:

```
# 将 path.data 和 path.logs 更改为开始时创建的文件
path.data: /data/elk-data
path.logs: /data/elk-log
```

```
# ---------------------------------- Paths ------------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /data/elk-data
#
# Path to log files:
#
path.logs: /data/elk-log
#
```

10.修改network模块：

```
# 修改IP和端口号
network.host: 192.168.79.110
http.port: 9200
```

```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 192.168.79.110
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
```

11.修改Discovery模块：

```
# 修改discovery.seed_hosts为三台服务器的主机名或者IP
discovery.seed_hosts: ["superbox", "superbox2", "superbox3"]
cluster.initial_master_nodes: ["superbox", "superbox2", "superbox3"]
```

```
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["superbox", "superbox2", "superbox3"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
cluster.initial_master_nodes: ["superbox", "superbox2", "superbox3"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
```

12.修改xpack.security.enabled：

```
xpack.security.enabled: false
```

```
# Enable security features
xpack.security.enabled: false
```

13.增加参数：

```
http.cors.enabled: true
http.cors.allow-origin: "*"
```

```
# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0
http.cors.enabled: true
http.cors.allow-origin: "*"
# Allow other nodes to join the cluster from anywhere
# Connections are encrypted and mutually authenticated
#transport.host: 0.0.0.0
```

14.启动elasticsearch集群（三台机）

```
# 启动
systemctl start elasticsearch
# 设置开机启动
systemctl enable elasticsearch
```

二、安装elasticsearch-head

1.下载node-10.0.24

```
wget https://nodejs.org/download/release/v10.24.0/node-v10.24.0-linux-x64.tar.gz
```

2.解压node-10.0.24

```
tar -xf node-v10.24.0-linux-x64.tar.gz
```

3.更改node路径

```
mv node-v10.24.0-linux-x64 /usr/local/node
```

4.设置环境变量

```
cat > /etc/profile.d/node << eof
export PATH=/usr/local/node/bin:$PATH
eof
```

5.下载elasticsearch-head

```
wget http://192.168.1.200/220711-note/elasticsearch-head-master.zip
或者
wget https://github.com/mobz/elasticsearch-head/archive/refs/heads/master.zip
```

6.进入elasticsearch-head-master根目录

```
cd elasticsearch-head-master
```

7.更换node源

```
npm config set registry https://registry.npm.taobao.org
```

8.下载

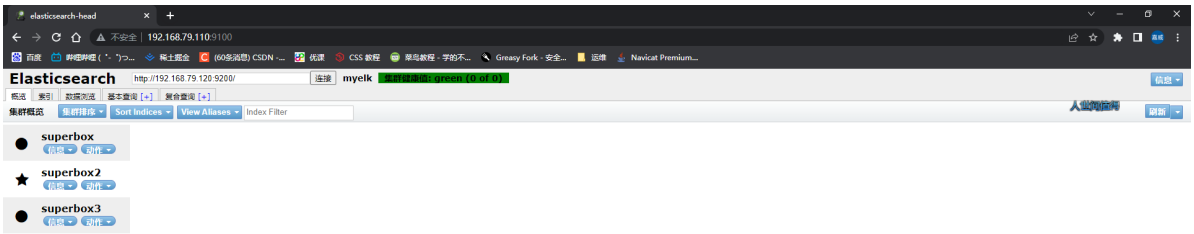
```
npm install
```

9.启动elasticsearch-head

```
npm run start
```

10.网页输入http://localhost:9100

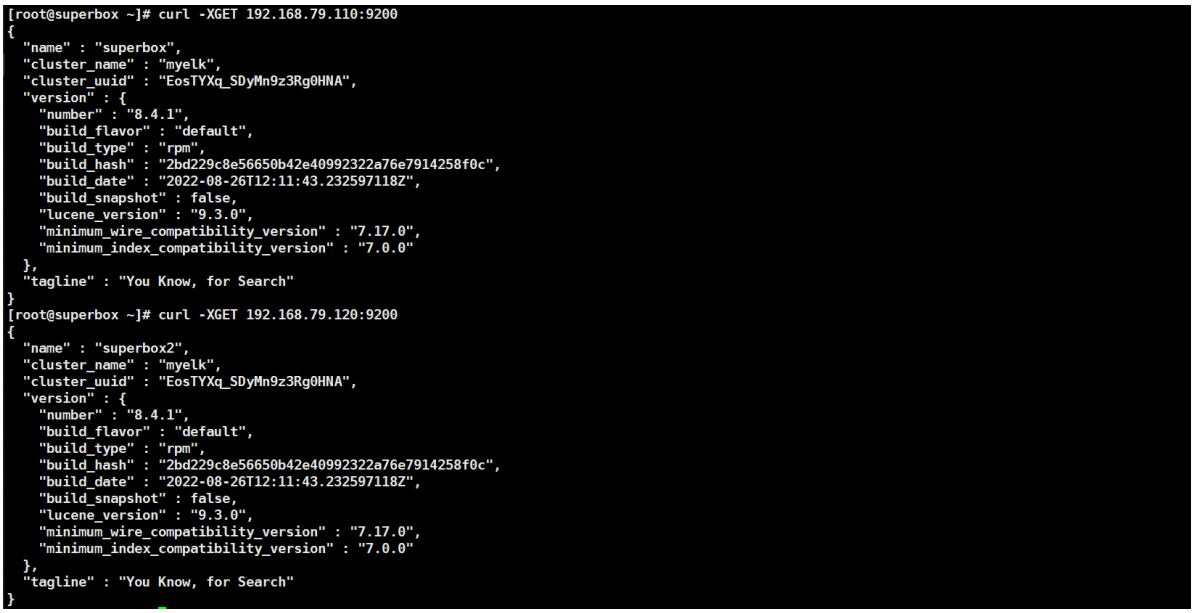
```
# 进入页面后输入http://localhost:9200连接elasticsearch集群
```



三、Elasticsearch基础使用

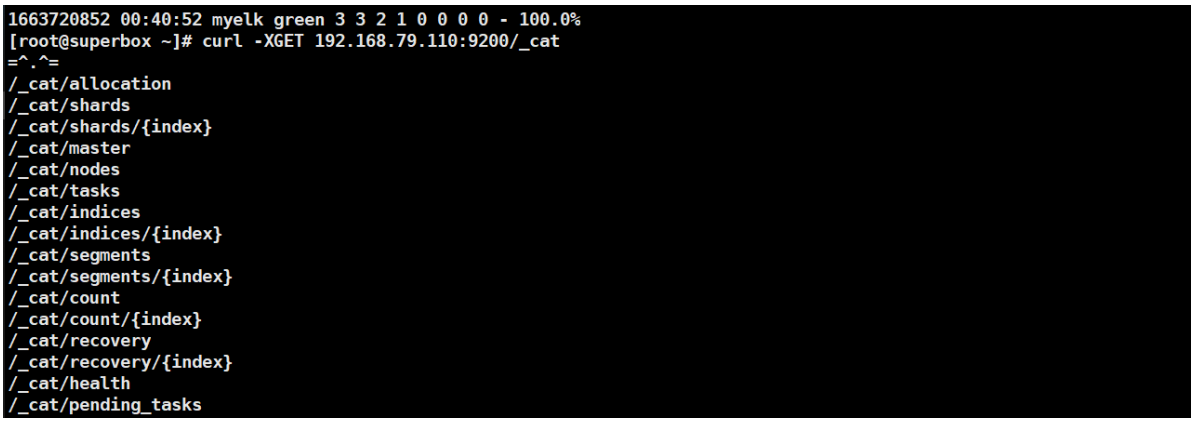
1.查看某个 ES 节点的摘要信息：curl -XGET localhost:9200

```
curl -XGET 192.168.79.110:9200
```



2.获取所有cat系列的操作：curl -XGET localhost:9200/_cat

```
curl -XGET 192.168.79.110:9200/_cat
```



3.查看集群是否健康：curl -XGET localhost:9200/_cat/health

```
curl -XGET 192.168.79.110:9200/_cat/health
# 绿色——最健康的状态，代表所有的主分片shard和副本分片replica都可用。
# 黄色——所有的主分片shard可用，但是部分副本分片replica不可用。
# 红色——部分主分片shard不可用。（此时执行查询部分数据仍然可以查到，遇到这种情况，还是赶快解决比较好）。
```

```
[root@superbox ~]# curl -XGET 192.168.79.110:9200/_cat/health
1663721262 00:47:42 myelk green 3 3 2 1 0 0 0 0 - 100.0%
```

4.获取所有索引信息：curl -XGET localhost:9200/_cat/indices

```
curl -XGET 192.168.79.110:9200/_cat/indices
```

```
[root@superbox ~]# curl -XGET 192.168.79.110:9200/_cat/indices
green open 1       7dwNGMkmSdC4JfoE-LCrxw 1 1 0 0 450b 225b
green open student 2T0m8TS-TDSZJ0MCWQEdlA 1 2 0 0 675b 225b
[root@superbox ~]#
```

5.获取单个索引信息：curl -XGET localhost:9200/student?pretty

```
curl -XGET 192.168.79.110:9200/student?pretty
```

```
[root@superbox ~]# curl -XGET 192.168.79.110:9200/student?pretty
{
  "student" : {
    "aliases" : { },
    "mappings" : { },
    "settings" : {
      "index" : {
        "routing" : {
          "allocation" : {
            "include" : {
              "_tier_preference" : "data_content"
            }
          }
        },
        "number_of_shards" : "1",
        "provided_name" : "student",
        "creation_date" : "1663722138531",
        "number_of_replicas" : "2",
        "uuid" : "2T0m8TS-TDSZJ0MCWQEdlA",
        "version" : {
          "created" : "8040199"
        }
      }
    }
  }
}
```

6.增：添加一个文档，同时索引、类型、文档id也同时生成

```
# 如果id不指定，则ES会自动帮你生成一个id。

```

Kibana

一、安装Kibana

1.下载Kibana的RPM包

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-8.4.2-x86_64.rpm
```

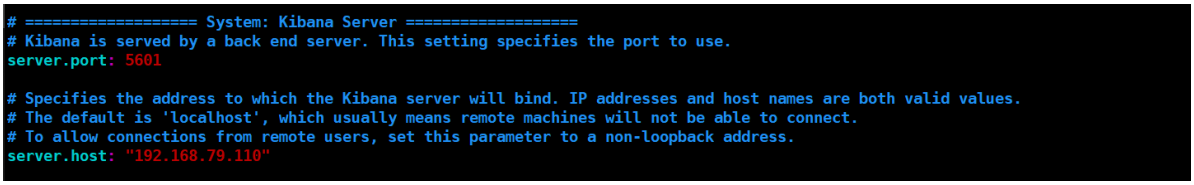
2.解压KibanaRPM包

```
rpm -ivh kibana-8.4.2-x86_64.rpm
```

3.修改配置文件，修改以下信息。

打开port并修改server.host：

```
vim /etc/kibana
server.port: 5601
server.host: "192.168.79.110"
```



打开elasticsearch.hosts：

```
elasticsearch.hosts: ["http://192.168.79.110:9200"]
```

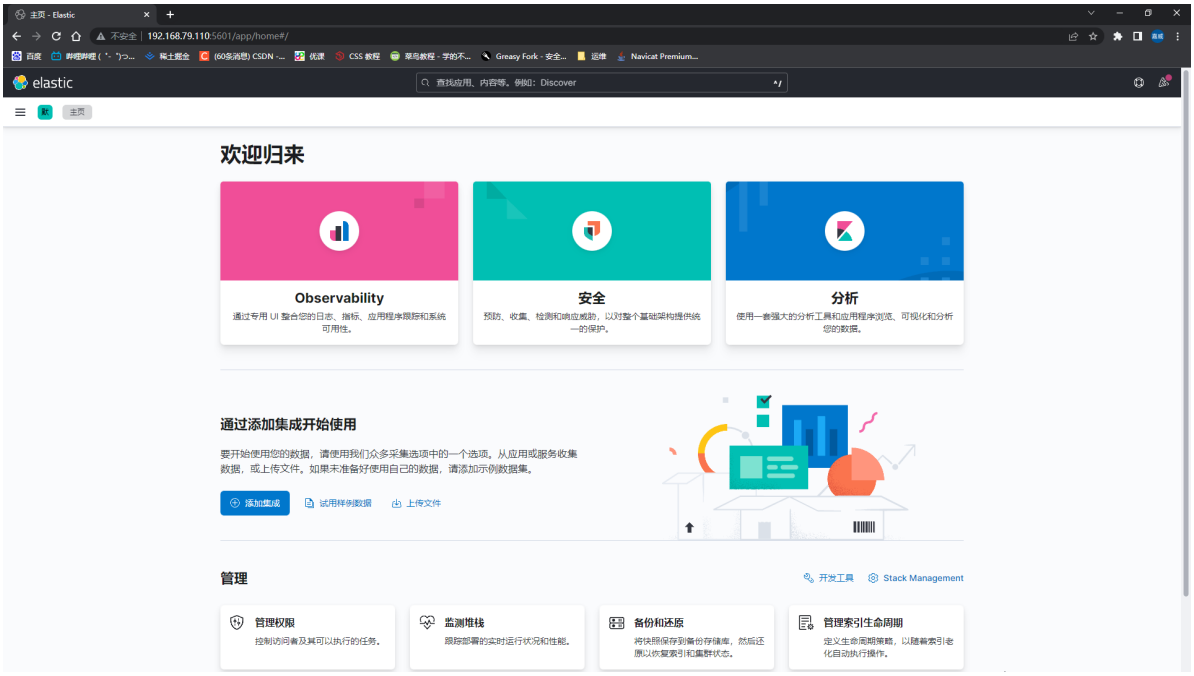
```
# ================== System: Elasticsearch ==================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.79.110:9200"]
```

修改语言：

```
i18n.locale: "zh-CN"
```

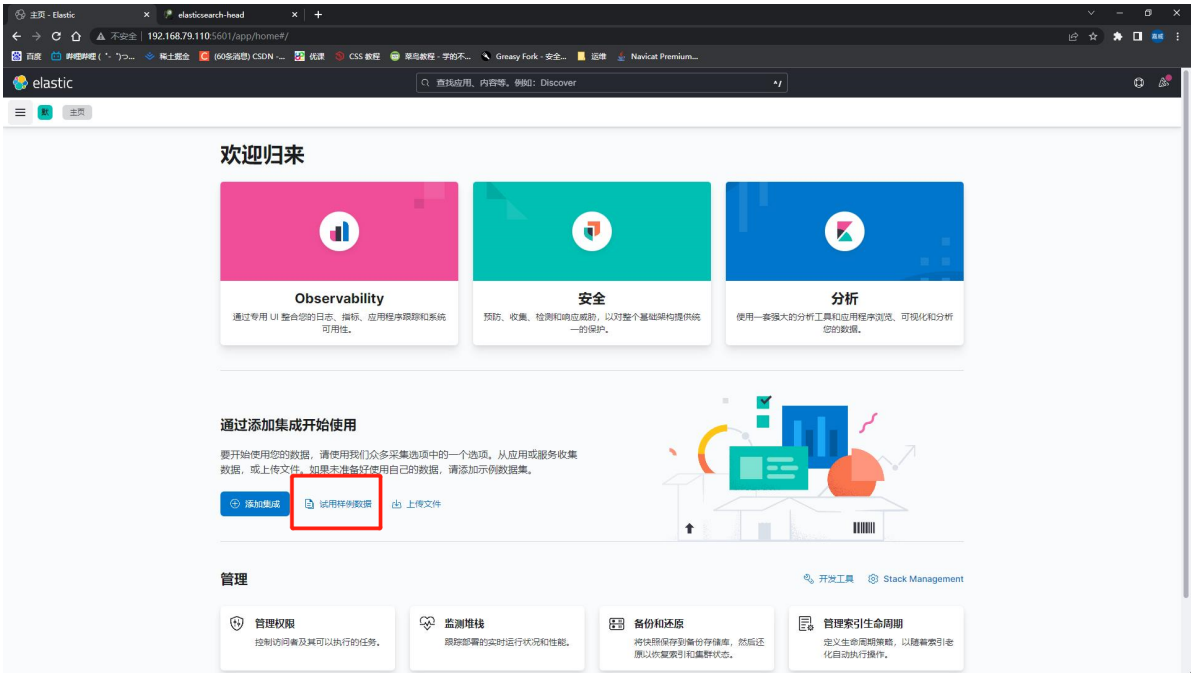
```
# Specifies locale to be used for all localizable strings, dates and number formats.
# Supported languages are the following: English (default) "en", Chinese "zh-CN", Japanese "ja-JP", French "fr-FR".
i18n.locale: "zh-CN"
```

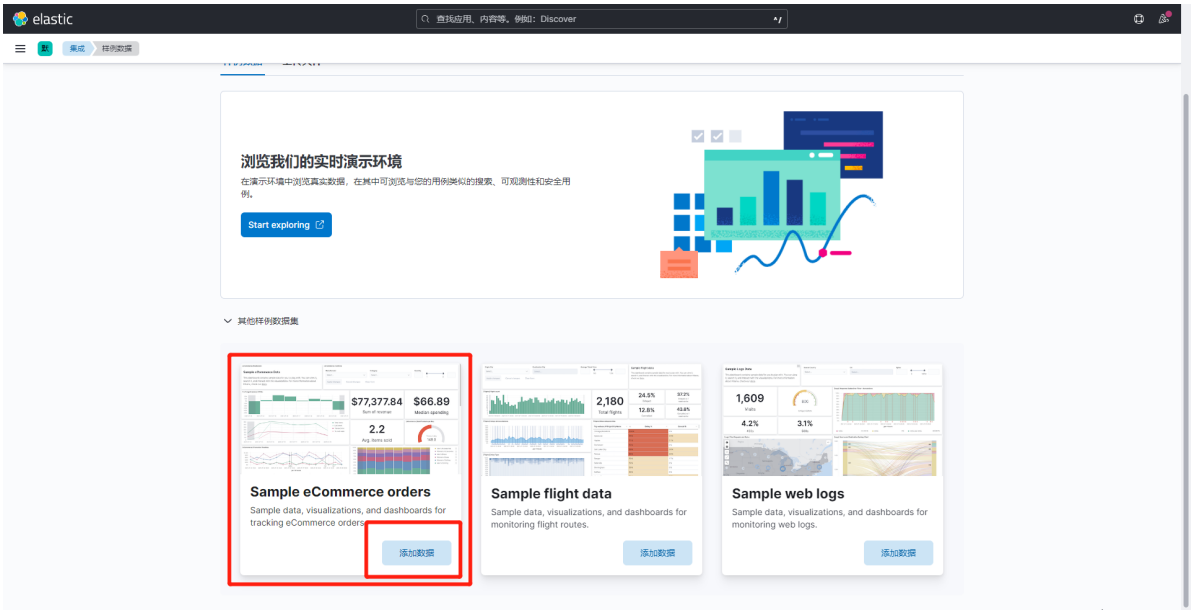
浏览器输入 http://localhost:5601打开面板

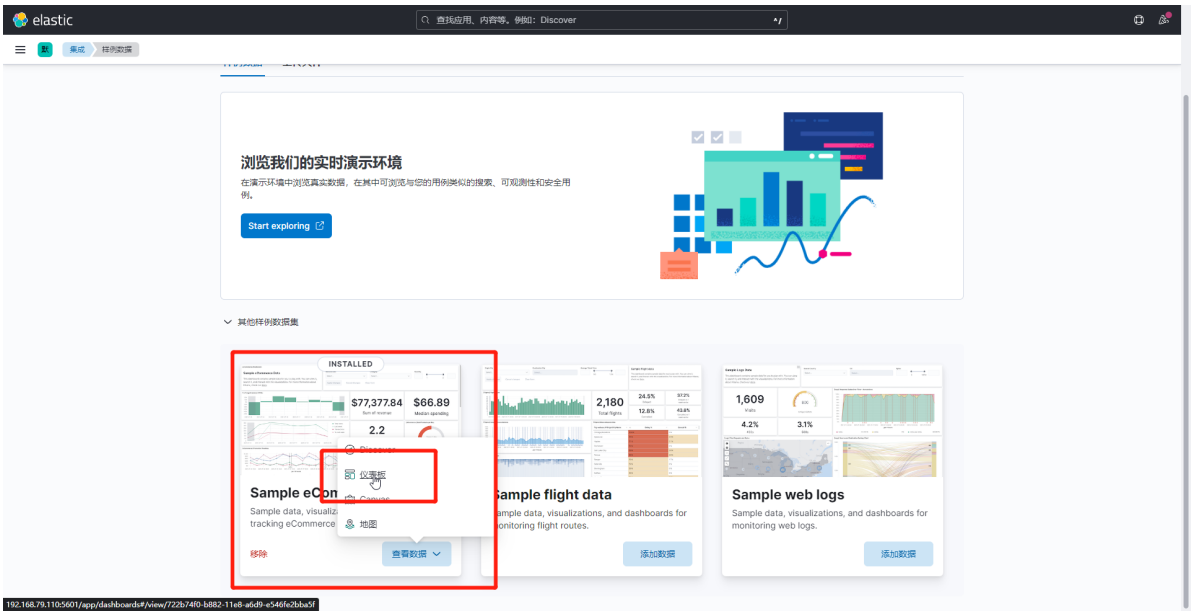


二、kibana基础操作

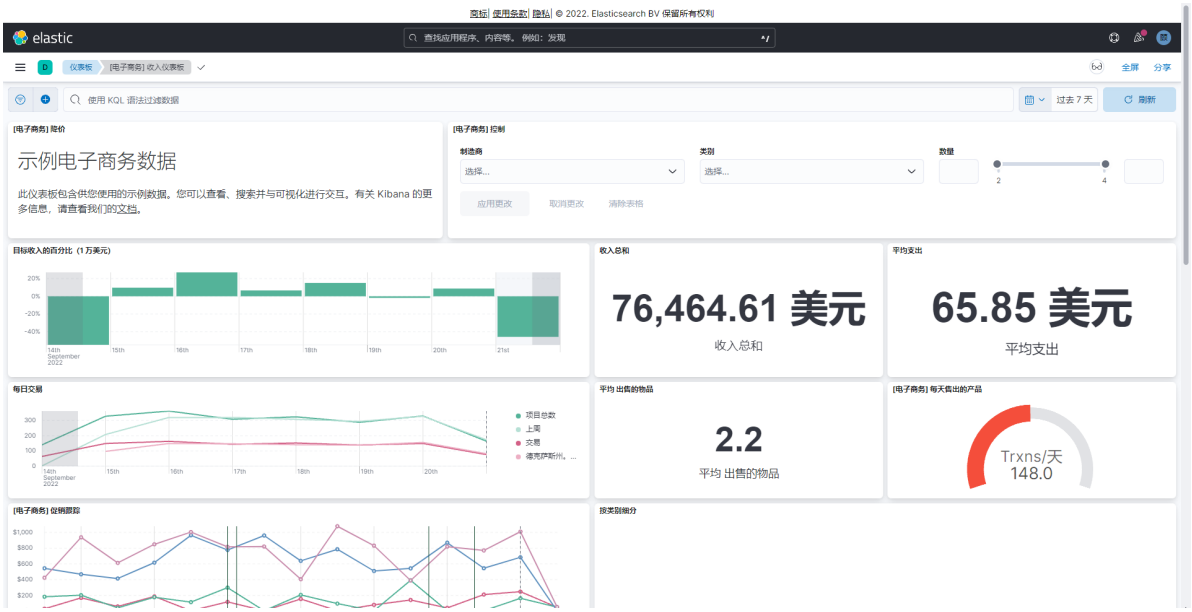
1.添加一个样本数据


elastic
查找应用、内容等。例如：Discover
欢迎归来
Observability
通过专用 UI 整合您的日志、指标、应用程序跟踪和系统可用性。
安全
预防、收集、检测和响应威胁，以对整个基础架构提供统一的保护。
分析
使用一套强大的分析工具和应用程序浏览、可视化和分析您的数据。
通过添加集成开始使用
要开始使用您的数据，请使用我们众多采集选项中的一个选项。从应用或服务收集数据，或上传文件。如果未准备好使用自己的数据，请添加示例数据集。
添加集成
试用样例数据
上传文件
管理
开发工具
Stack Management
管理权限
控制访问者及其可以执行的任务。
监测堆栈
跟踪部署的实时运行状况和性能。
备份和还原
将快照保存到备份存储库，然后还原以恢复索引和集群状态。
管理索引生命周期
定义生命周期策略，以随着索引老化自动执行操作。

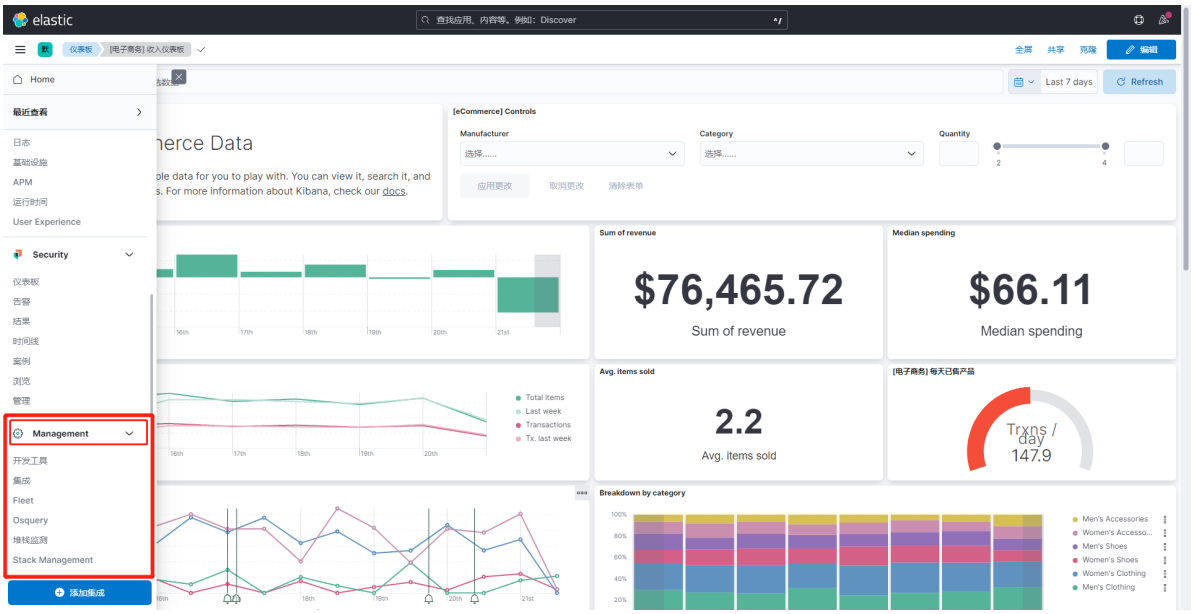

elastic
查找应用、内容等。例如：Discover
浏览我们的实时演示环境
在演示环境中浏览真实数据，在其中可浏览与您的用例类似的搜索、可观测性和安全用例。
Start exploring
其他样例数据集
Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.
添加数据
Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.
添加数据
Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.
添加数据


elastic
查找应用、内容等。例如：Discover
浏览我们的实时演示环境
在演示环境中浏览真实数据，在其中可浏览与您的用例类似的搜索、可观测性和安全用例。
Start exploring
其他样例数据集
INSTALLED
仪表板
地图
查看数据
移除
Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.
添加数据
Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.
添加数据

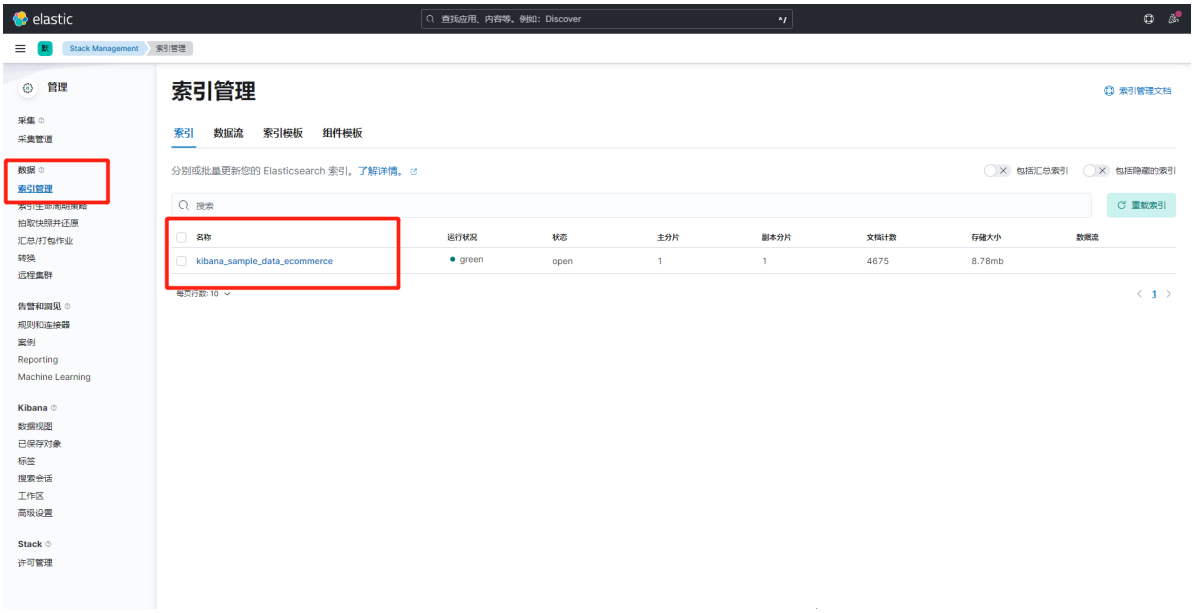
样本数据仪表盘：

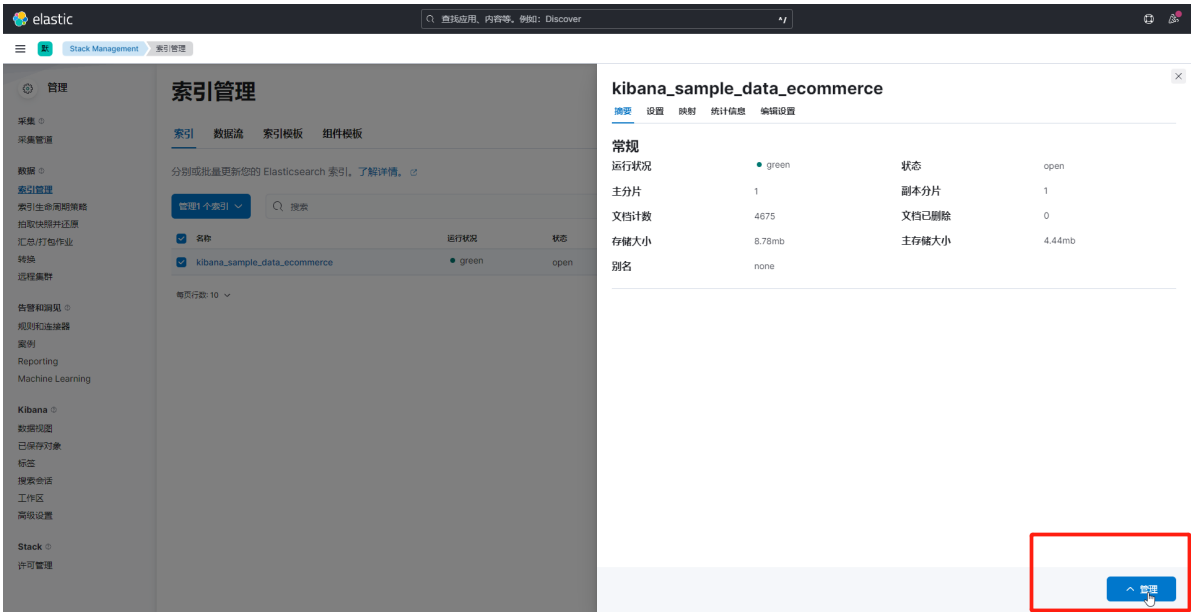


2.在左下角可以进入 ES 的管理界面，可以直接对 ES 中的数据进行管理，比 head 插件功能更加强大。

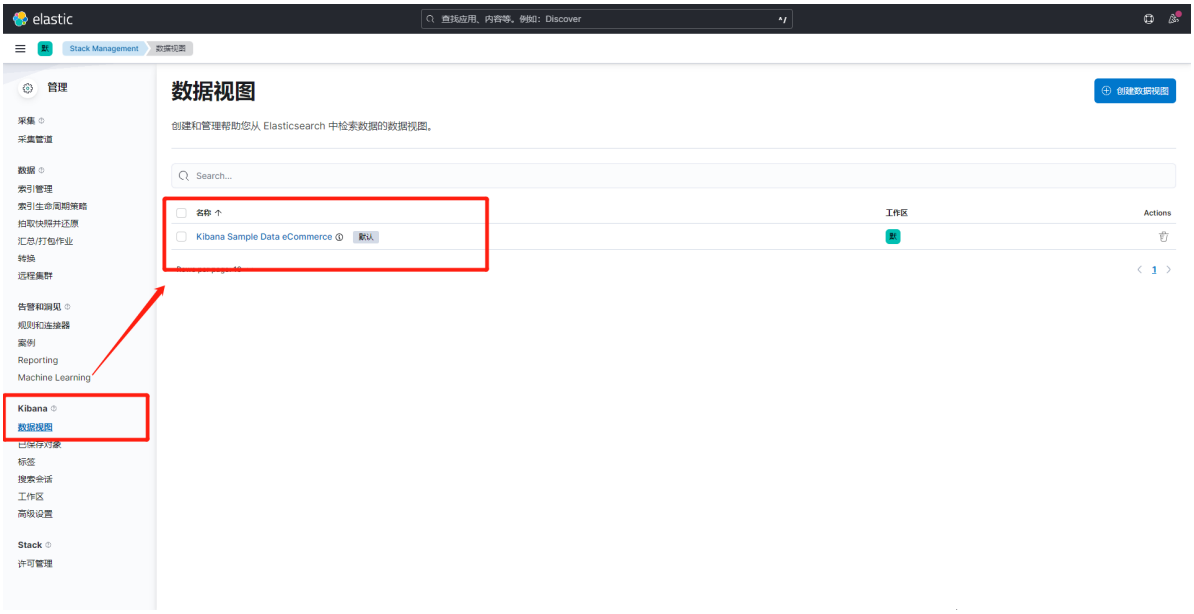


管理索引：





在kibana模块添加视图：



Logstash

一、安装Logstash

在需要采集日志的机器上安装Logstash。

1.下载

```
https://artifacts.elastic.co/downloads/logstash/logstash-8.4.2-x86_64.rpm
```

2.解压

```
rpm -ivh logstash-8.4.2-x86_64.rpm
```

二、使用logstash收集nginx日志

1.修改nginx配置文件。

```
# 在nginx.conf文件中的http模块中将日志文件格式改为json格式。
log_format json '{"@timestamp":"$time_iso8601",'
                            '"@version":"1",'
                            '"client":"$remote_addr",'
                            '"url":"$uri",'
                            '"status":"$status",'
                            '"domain":"$host",'
                            '"host":"$server_addr",'
                            '"size":$body_bytes_sent,'

'"responsetime":$request_time,'
                            '"referer":
"$http_referer",'
                            '"ua": "$http_user_agent"'
                '}';
    access_log /var/log/nginx/access_json.log json;

```

2.配置logstash收集文件

```
vim /etc/logstash/conf.d/nginxlog.conf
input {
  file {
    path =>"/var/log/nginx/access_json.log"
    #第一次从头收集，之后从新添加的日志收集
    start_position => "beginning"
    #日志收集的间隔时间
    stat_interval =>"3"
    type=>"nginx"
  }
}
output {
  if [type] == "nginx" {
    elasticsearch {
      hosts => ["192.168.79.110:9200"]
      index => "nginx-%{+YYYY.MM.dd}"
    }
  }
}
```

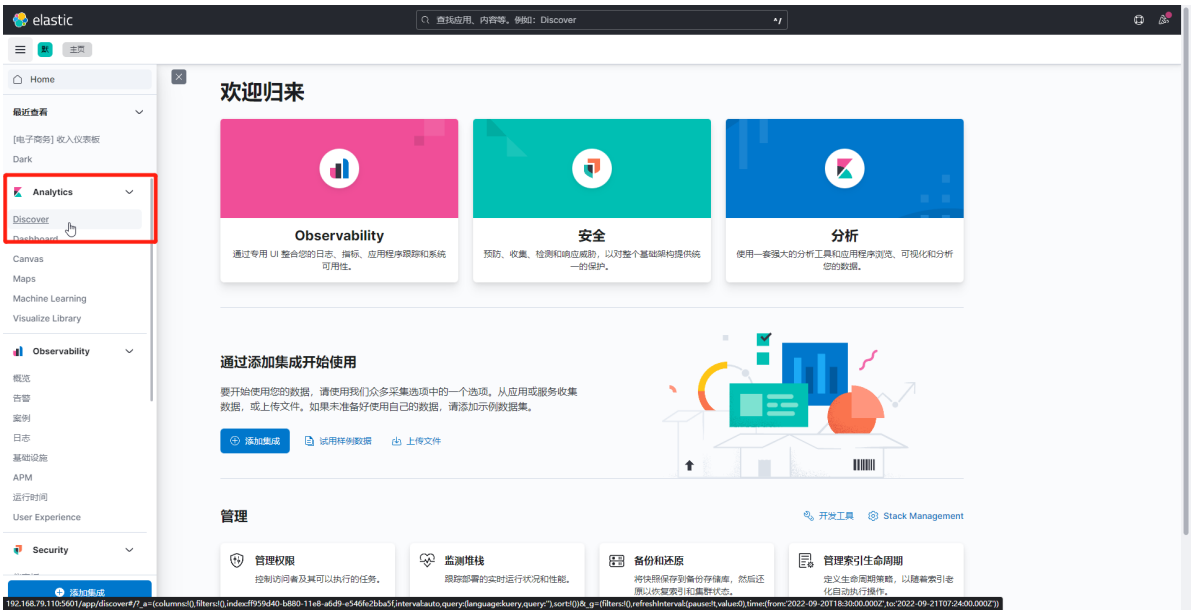
3.重启nginx与logstash

```
# 重启nginx
nginx -t
nginx -c /etc/nginx/nginx.conf
nginx -s reload
# 重启logstash
systemctl restart logstash
```

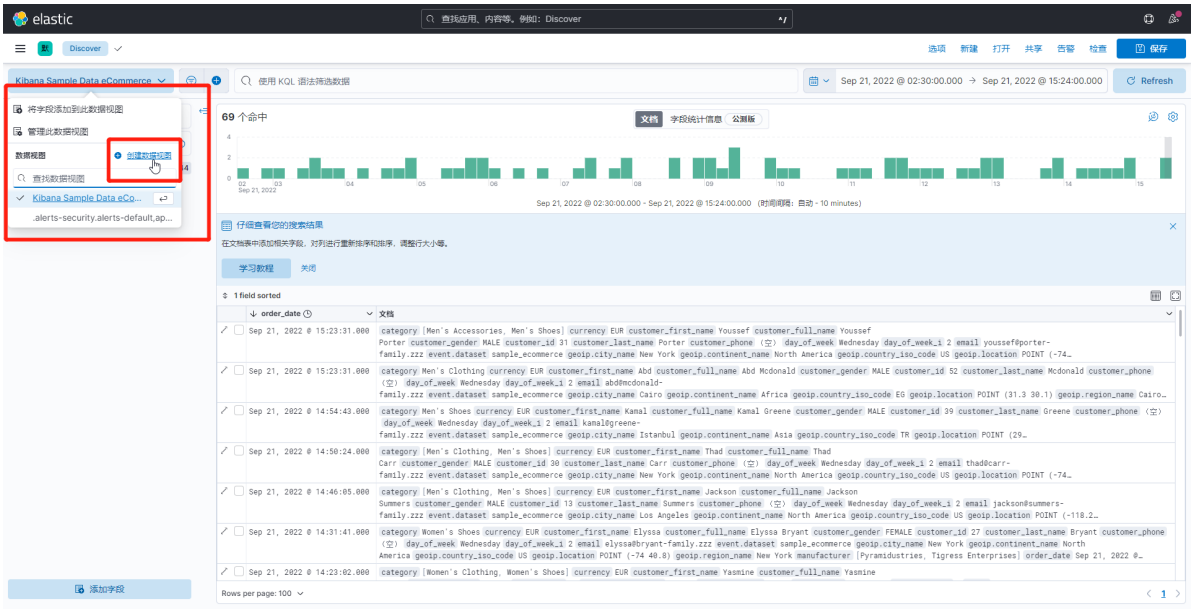
4.打开http://localhost:5601

```
http://192.168.79.110:5601
```

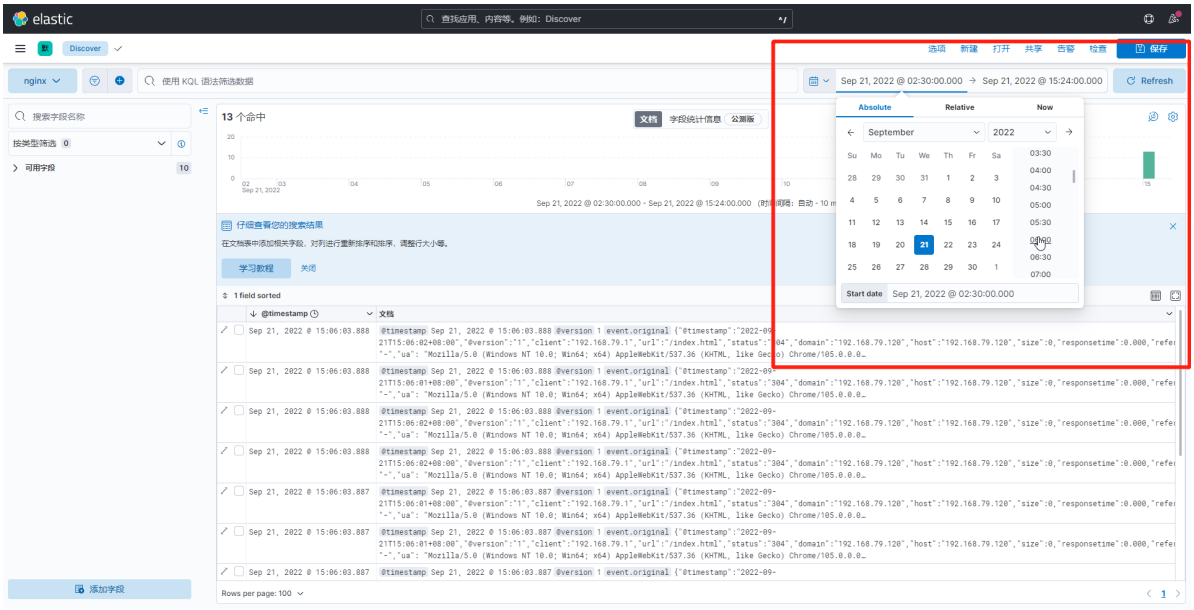
5.打开Analytics下的Discover模块



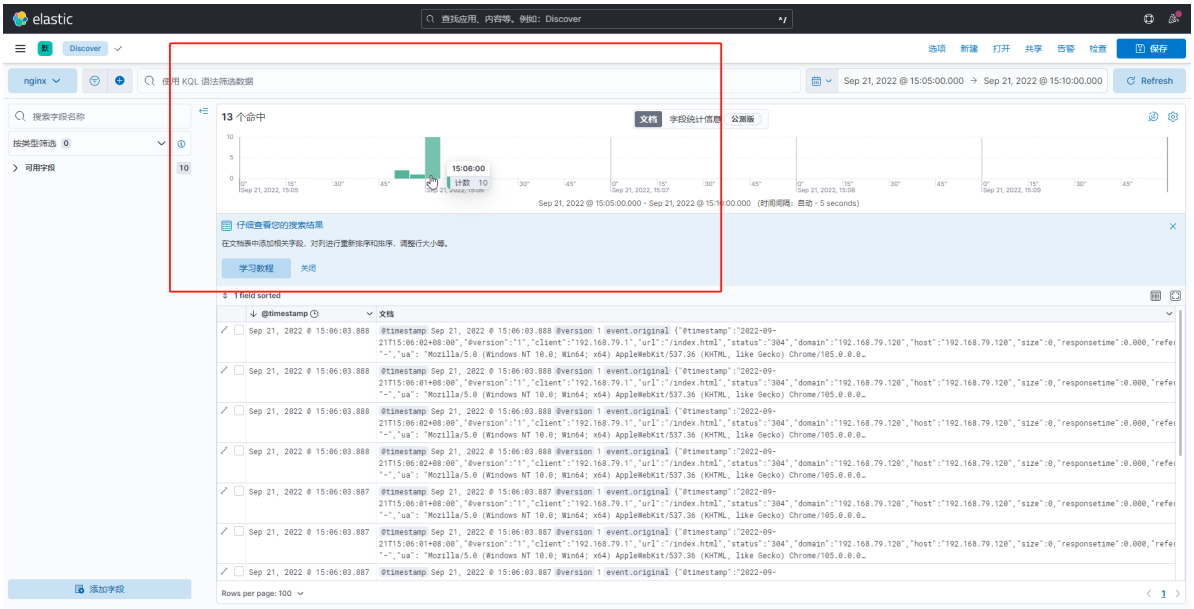
6.选择创建数据视图



7.选择合适的时间显示



8.这样就可以观察了



三、使用logstash收集nginx日志

1.修改tomcat配置文件

```
# 修改日志信息部分，将日志保存形式改为json。
<Valve
className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
   prefix="tomcat_json_log" suffix=".txt"
   pattern="
{clientip:%h,ClientUser:%l,authenticated:%u,AccessTime:%
t,method:%r,status:%s,SendBytes:%b,Query?
string:%q,partner:%{Referer}i,AgentVersion:%{User-
Agent}i}" />
```

2.配置logstash

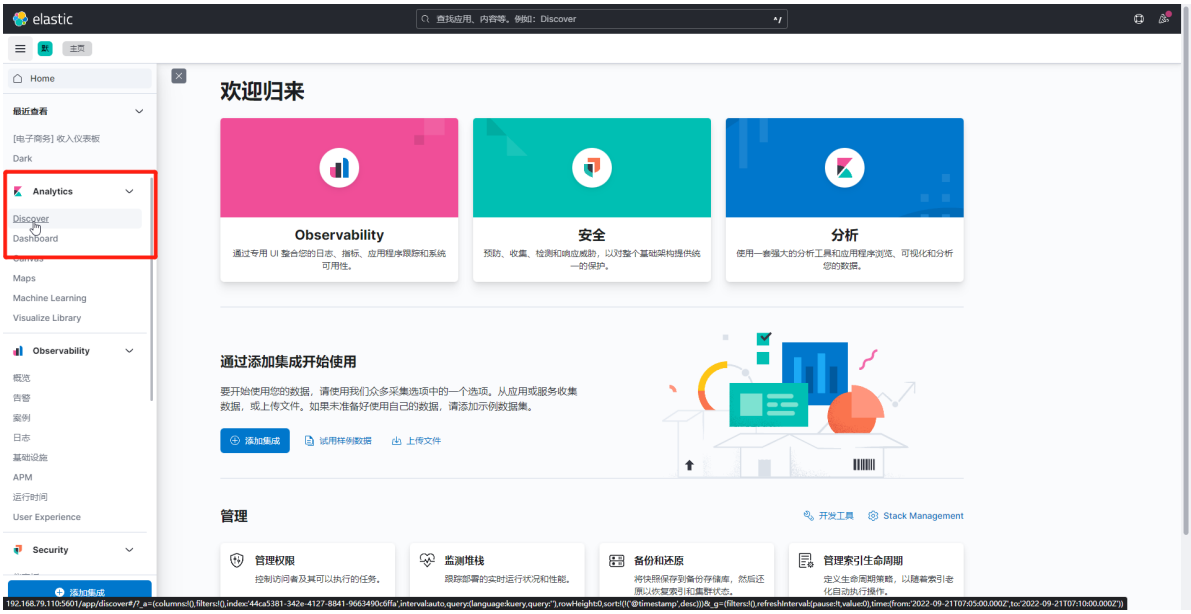
```
cat > /etc/logstash/conf.d/tomcatlog.conf << eof
input{
        file{

 path=>"/usr/local/tomcat/logs/tomcat_json_log.*.txt"
                type=>"tomcat"
                start_position=>"beginning"
                stat_interval=>"5"
        }
}
output{
        elasticsearch{
                hosts=>["192.168.79.120:9200"]
                index=>"tomcatlog-%{+YYYY.MM.dd}"
        }
}
eof
```

3.重启tomcat和logstash

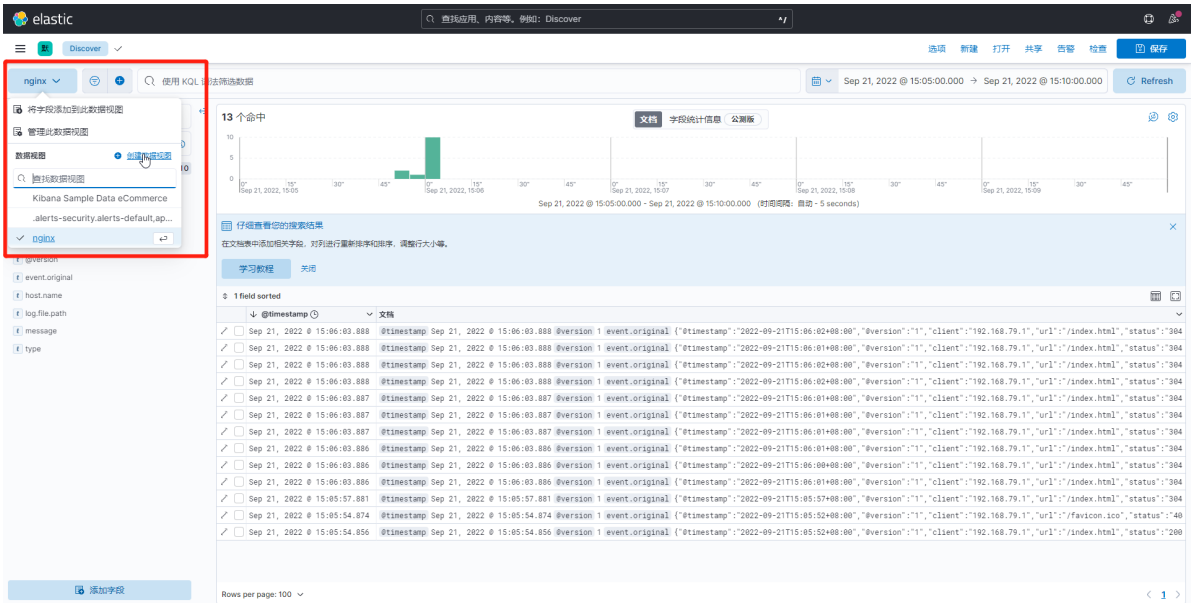
```
# 重启tomcat
/usr/local/tomcat/bin/catalina.sh start
# 启动logstash
/usr/share/logstash/bin/logstash -f
/etc/logstash/conf.d/tomcatlog.conf
```

4.网页进入http://localhost:5601

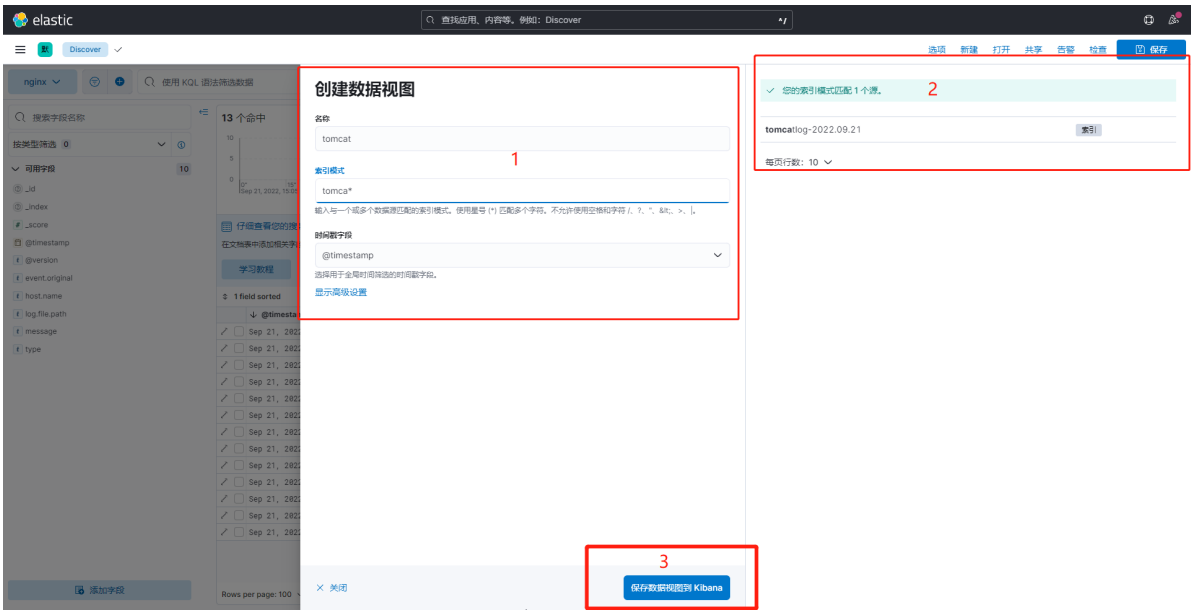
```
192.168.79.120:5601
# 点进去Discover
```



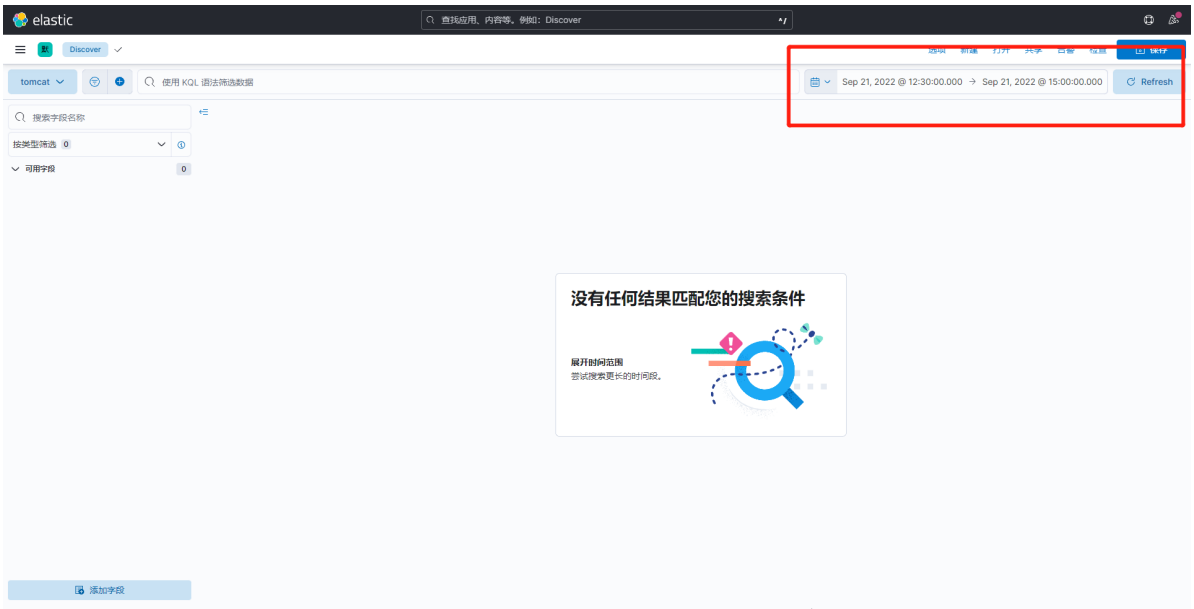
5.点击创建数据视图



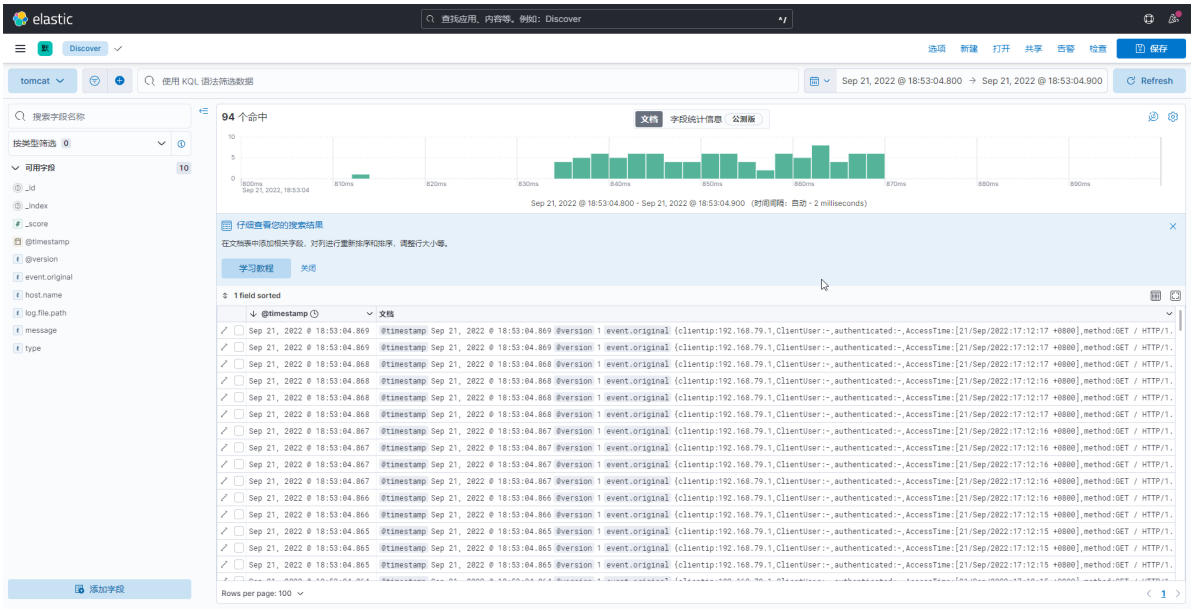
6.创建新的数据视图



7.选择时间段



8.日志数据就出来了


elastic
查找应用、内容等。例如：Discover
Discover
选项
新建
打开
共享
告警
检查
保存
tomcat
使用 KQL 语法筛选数据
Sep 21, 2022 @ 18:53:04.800 → Sep 21, 2022 @ 18:53:04.900
Refresh
搜索字段名称
按类型筛选 0
可用字段 10
_id
_index
_score
@timestamp
@version
event.original
host.name
log.file.path
message
type
添加字段
94 个命中
文档
字段统计信息
公测版
Sep 21, 2022 @ 18:53:04.800 - Sep 21, 2022 @ 18:53:04.900 （时间间隔：自动 - 2 milliseconds）
仔细查看您的搜索结果
在文档表中添加相关字段，对列进行重新排序和排序，调整行大小等。
学习教程
关闭
1 field sorted
@timestamp
文档
Rows per page: 100