Elasticsearch集群搭建手册

1. 服务器资源
   1. 系统版本

|  |  |
| --- | --- |
| IP | OS Version |
| 192.168.0.201 | Centos 7.6 |
| 192.168.0.202 | Centos 7.6 |
| 192.168.0.203 | Centos 7.6 |

* 1. 软件版本

|  |  |  |
| --- | --- | --- |
| Soft Name | Soft Version | 备注 |
| Elasticsearch | 7.10.2 |  |
| Kibana | 7.10.2 |  |
| Ik-Analysis | 7.10.2 |  |
| Split-Analysis | 7.10.2 | 自定义的切词分词器 |
| Metricbeat | 7.10.2 | 轻量级指标采集器 |

1. 环境优化

参考：

https://www.elastic.co/guide/en/elasticsearch/reference/7.10/system-config.html

* 1. 调整文件句柄数

vim /etc/security/limits.conf,在末尾增加如下内容：

elasticsearch - nofile 65535

elasticsearch为启动ES的用户名，\*表示所有用户

* 1. 调整vm.max\_map\_count大小

vim /etc/sysctl.conf，增加如下内容：

vm.max\_map\_count=655360

添加完后执行sysctl -p

* 1. 禁用Swap
     1. 调整配置

vim /etc/fstab，注释所有包含swap的行，然后重启服务器

* + 1. 验证

通过执行free命令查看，显示结果中的Swap行是否全为0，若为0则成功

1. 搭建ES集群

注：三台服务器都需要执行以下步骤

$ES\_HOME：是指 ES 的安装包 tar 包解压后的文件夹目录

* 1. 解压Ik-Analysis至目录$ES\_HOME/plugins/ik下
  2. 解压Split-Analysis至目录$ES\_HOME/plugins/split下
  3. 修改$ES\_HOME/config/jvm.options中的-Xms和-Xmx为服务器内存的一般但不能超过32G
  4. 修改$ES\_HOME/config/elasticsearch.yml，增加如下内容：

注：cluster.initial\_master\_nodes，集群启动完成后需要删除配置，该项配置的值一定要和node.name保持一致，详细信息见：

<https://www.elastic.co/guide/en/elasticsearch/reference/current/important-settings.html#initial_master_nodes>

https://blog.csdn.net/laoyang360/article/details/111148362

cluster.name: dev

node.name: node01 //节点名称不可重复

path.data: /var/data/elasticsearch

path.logs: /var/log/elasticsearch

network.host: 192.168.0.201 //自行修改IP为要使用的服务器IP

http.port: 9200

discoverty.seed\_hosts: ["192.168.0.201:9300", "192.168.0.202:9300", "192.168.0.203:9300"]

cluster.initial\_master\_nodes: ["node01","node02","node03"]

transport.port: 9300

http.cors.enabled: true

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

xpack.security.enabled: true

xpack.security.transport.ssl.enabled: true

xpack.security.transport.ssl.verification\_mode: certificate

xpack.security.transport.ssl.keystore.path: elastic-certificates.p12

xpack.security.transport.ssl.truststore.path: elastic-certificates.p12

xpack.monitoring.collection.enabled: true

* 1. 生成证书

cd $ES\_HOME

./bin/elasticsearch-certutil ca -out config/elastic-certificates.p12 -pass ""

注：生成后需将证书复制到所有节点

* 1. 进入ES的bin目录

cd $ES\_HOME/bin

* 1. 启动ES，-d：后台启动

注：请不要使用root用户启动

./elasticsearch -d

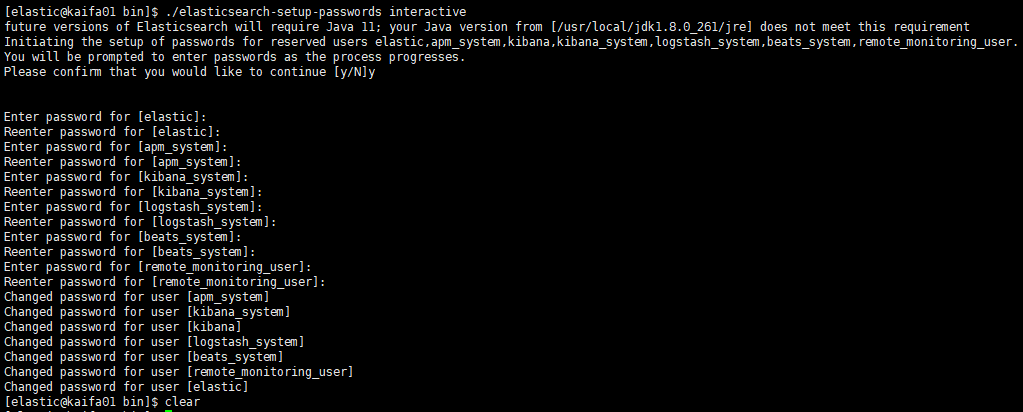
* 1. 配置密码

注：此操作需要在所有节点启动完成后进行

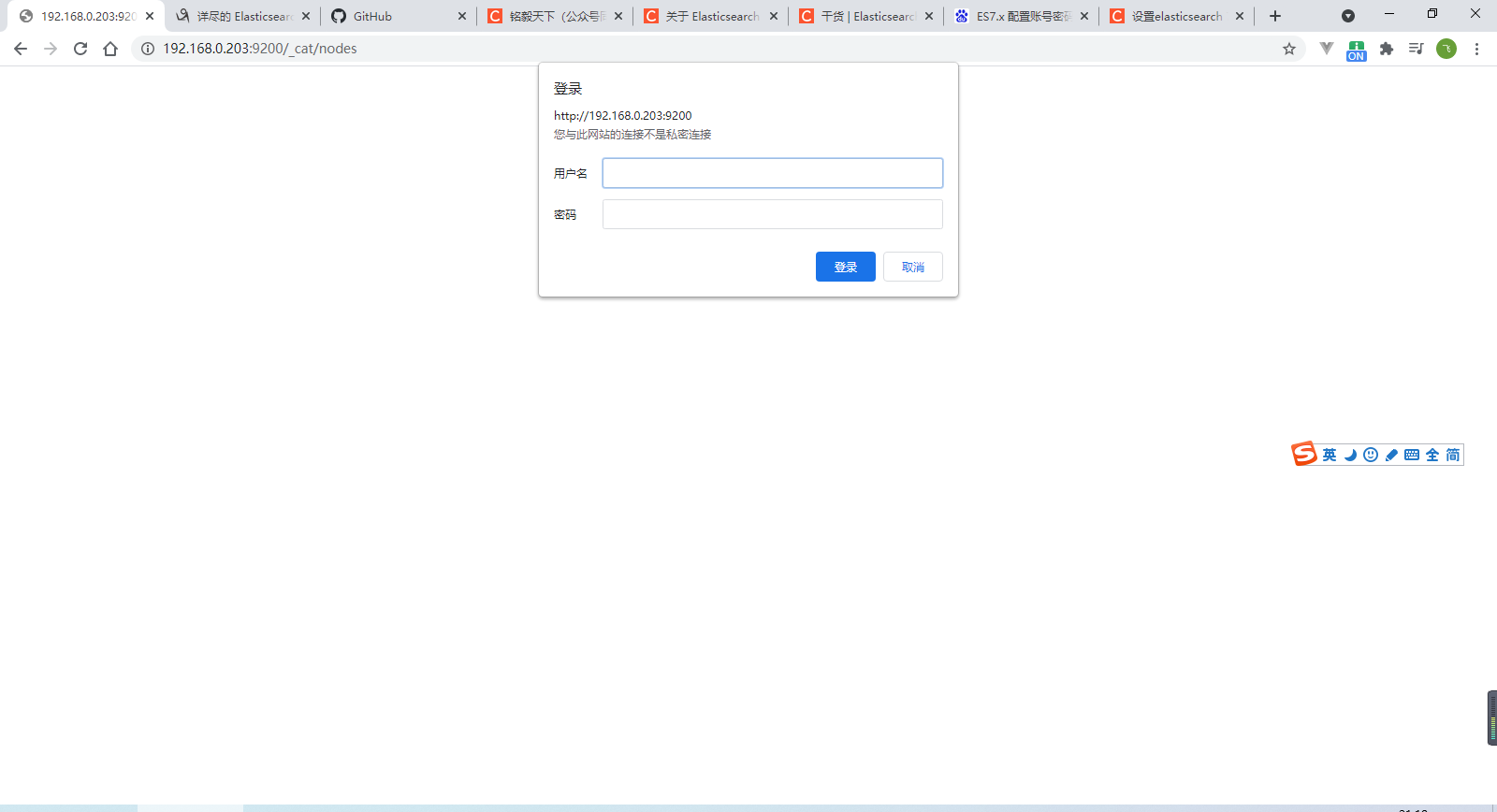
运行./ elasticsearch-setup-passwords [auto| interactive]，如下图所示：

auto：生成随机密码

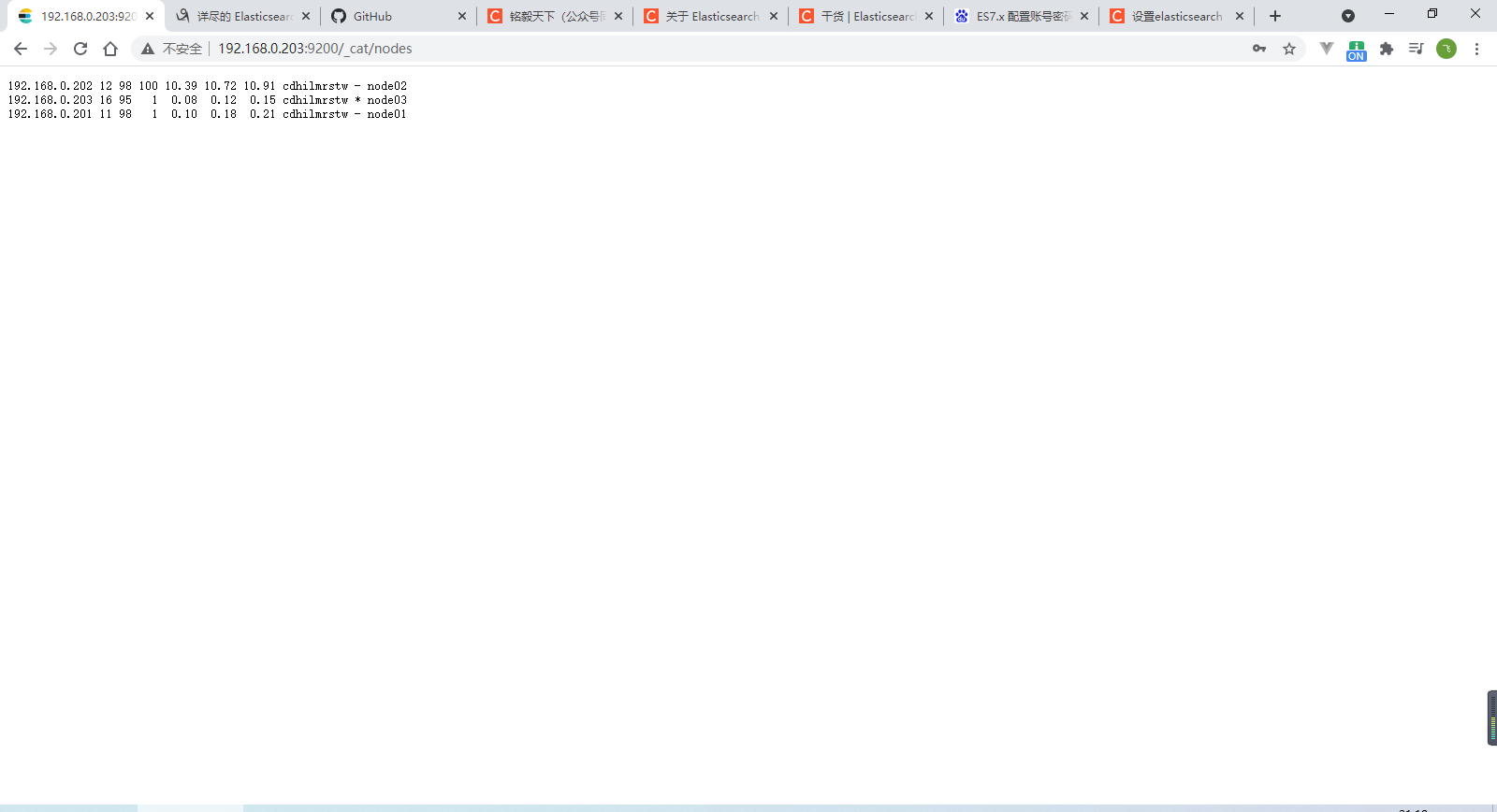
interactive：自定义密码



配置完成后随机访问一台服务器：



输入账号密码：



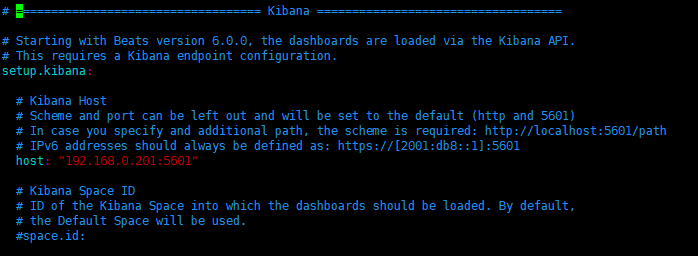
1. 搭建Metricbeat

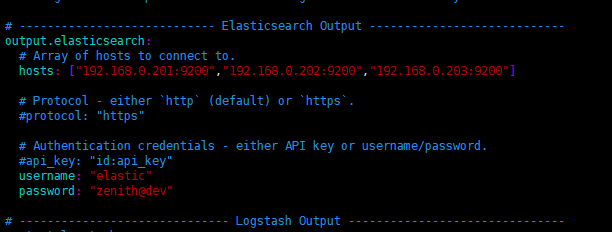
注：以下操作需在所有节点执行，请不要使用root账号启动metricbeat，使用root账号即使是后代运行关闭shell窗口后metricbeat也会退出

$METRICBEAT\_HOME: 指的是解压后目录

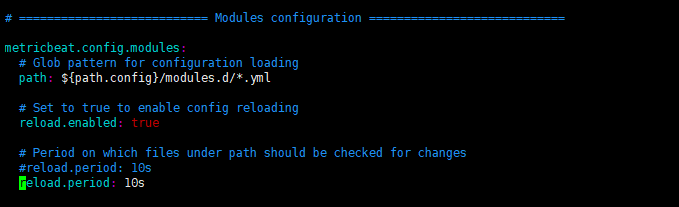
cd $METRICBEAT\_HOME/bin

vim metricbeat.yml，修改kibana和elasticsearch的配置如下：





开启自动加载配置：

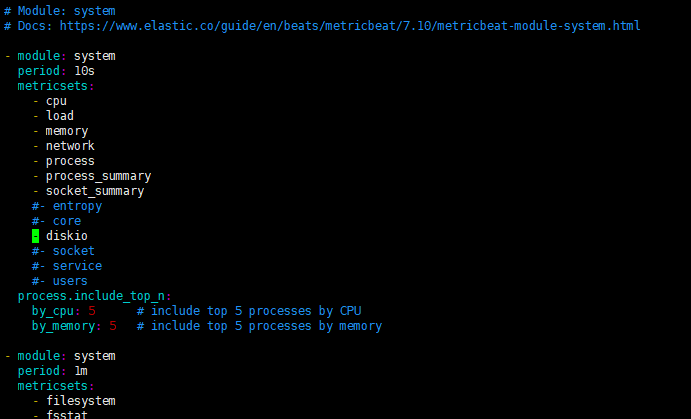


开启磁盘IO采集（非必选）：

注：system模块默认为开启，若不需要则关闭即可

关闭System模块：

./metricbeat modules disable system



启用模块：

./metricbeat modules enable elasticsearch-xpack

启动采集器：

nohup ./metricbeat -e -d “publish”&

1. 搭建Kibana

$KIBANA\_HOME：是指 Kibana 的安装包 tar 包解压后的文件夹目录

* 1. 选择任意一台服务器（此处选择192.168.0.201）进行如下操作

cd $KIBANA\_HOME/config && vim kibana.yml，增加如下内容：

server.port: 5601

server.host: 192.168.0.201

server.name: 192.168.0.201

elasticsearch.hosts:["http://192.168.0.201:9200","http://192.168.0.202:9200", "http://192.168.0.203:9200"]

elasticsearch.username: {ES账号}

elasticsearch.password: {ES密码}

i18n.locale: "zh-CN"

monitoring.kibana.collection.enabled: false

* 1. 配置Metricbeat采集Kibana信息

见：https://www.elastic.co/guide/en/kibana/7.7/monitoring-metricbeat.html

在Kibana所在主机执行：

cd $METRICBEAT\_HOME/bin

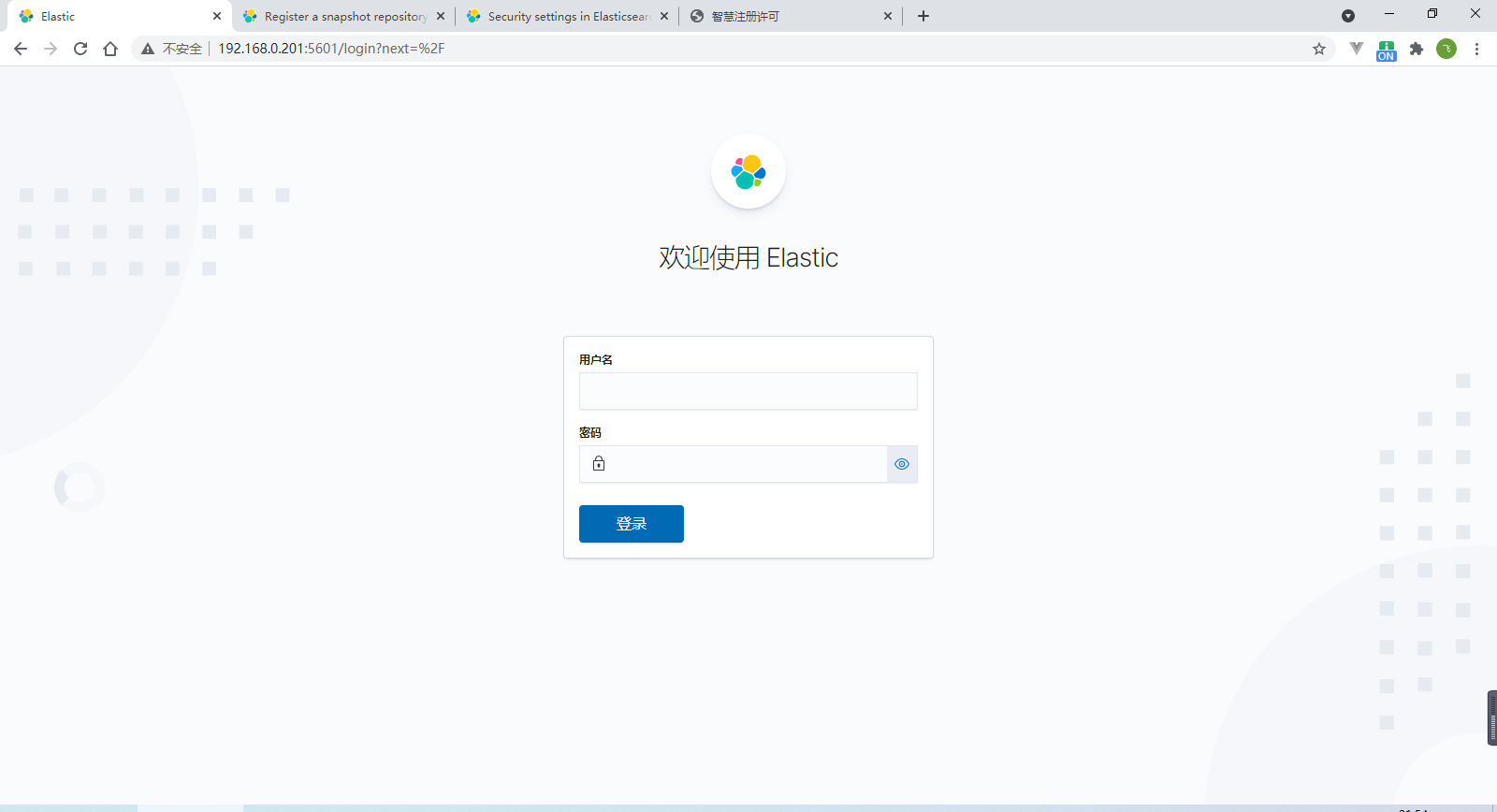
./metricbeat modules enable kibana-xpack

* 1. 启动

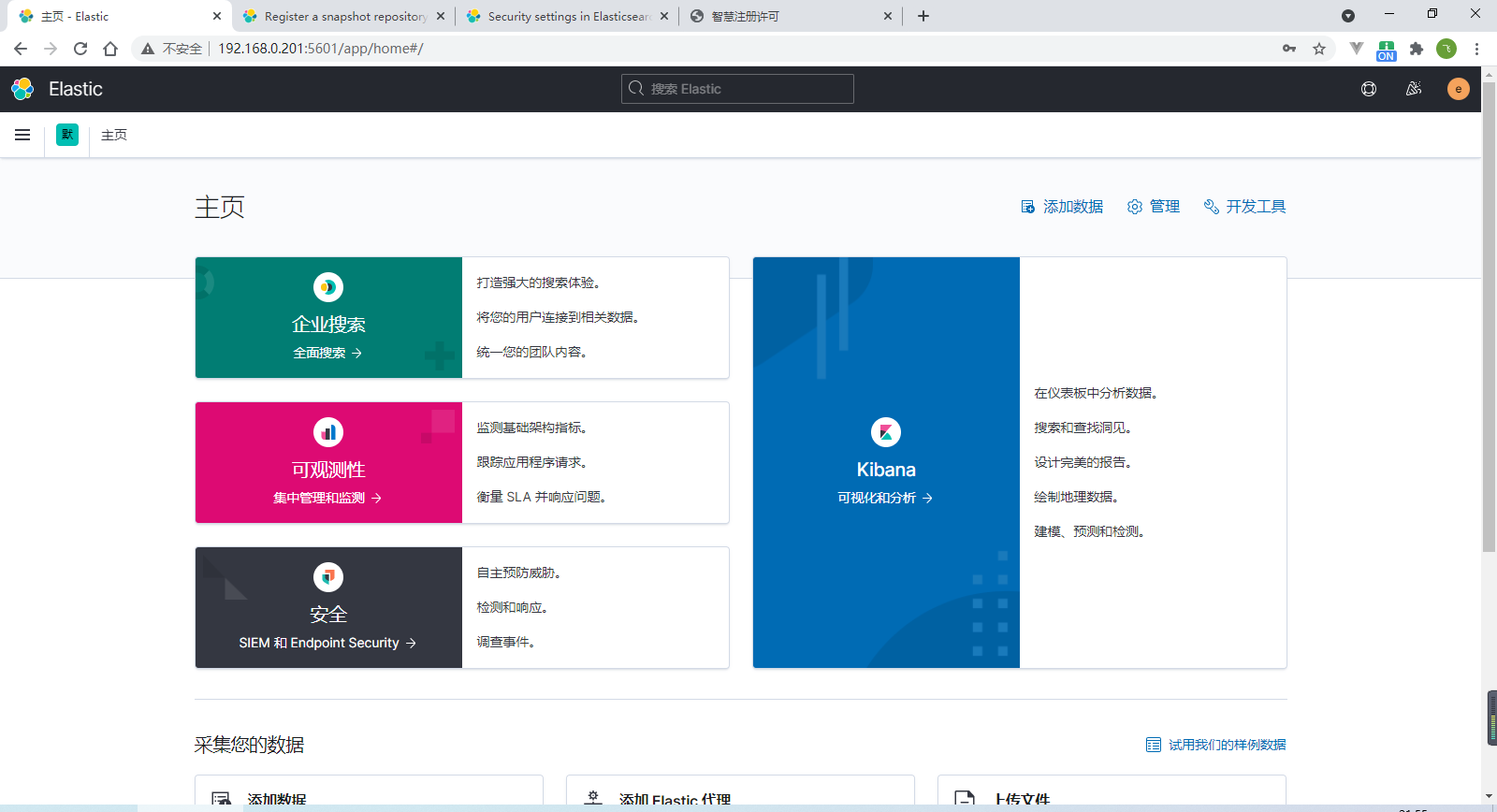
注：请不要使用root用户启动

cd $KIBANA\_HOME/bin && nohup ./kibana &

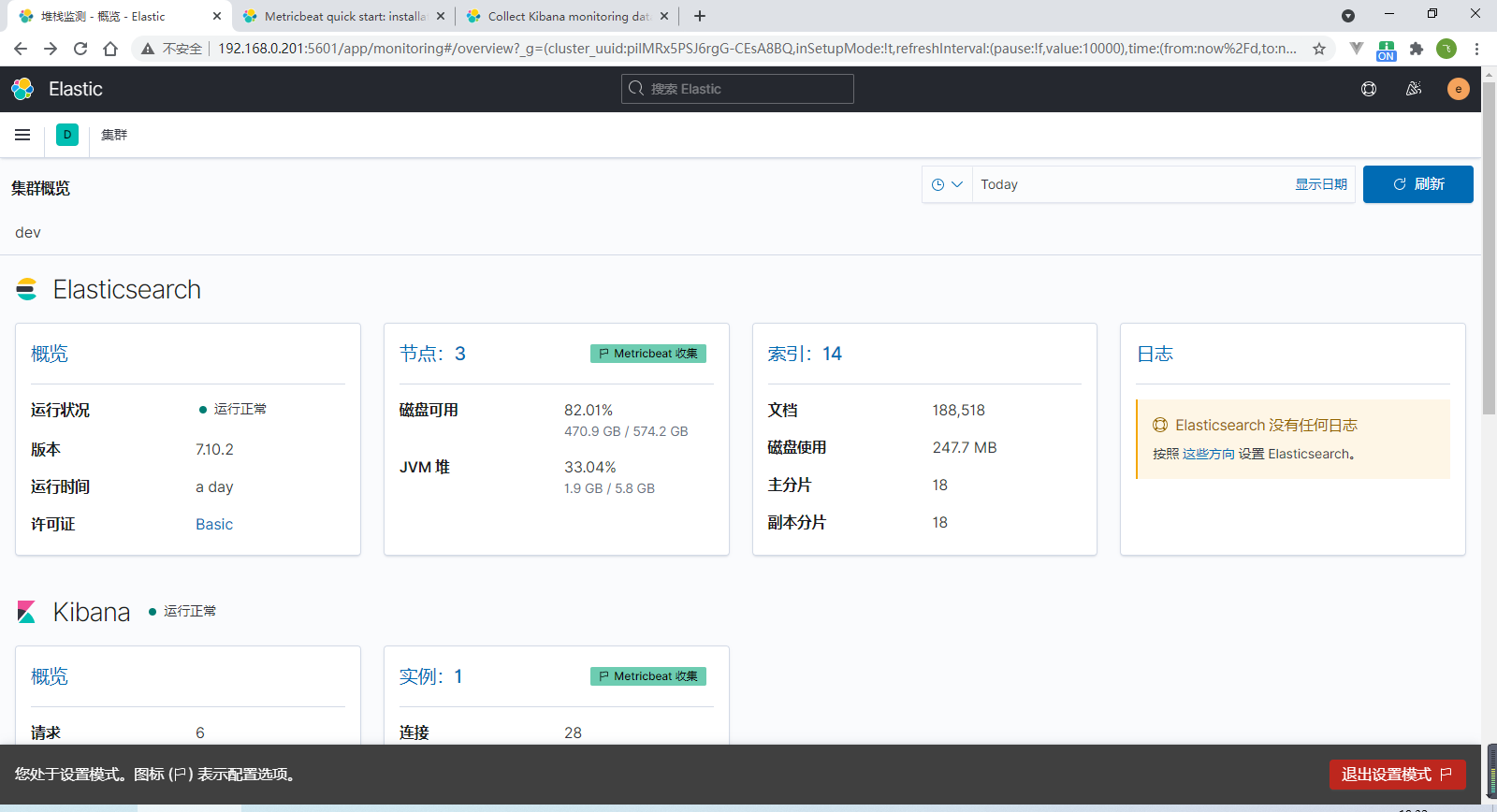
使用浏览器访问：<http://192.168.0.201:5601>



输入账号密码：



进入监控页面点击【进入设置模式】若出现以下信息则表示Metricbeat已经启用成功：



Metricbeat在开启system模块的情况下，点击Kibana->Dashboard，选择[Metricbeat System] Host overview ECS，如下图所示即成功

