下载包

**Elasticsearch：**

wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.4.2-x86_64.rpm>

**Kibana：**

wget <https://artifacts.elastic.co/downloads/kibana/kibana-7.4.2-linux-x86_64.tar.gz>

**Filebeat:**

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.2-x86\_64.rpm

安装elasticsearch

两台机器内存2g （最好3g以上）

yum -y install elasticsearch-7.4.2-x86\_64.rpm

/bin/systemctl daemon-reload #重载所有修改过的配置文件

/bin/systemctl enable elasticsearch

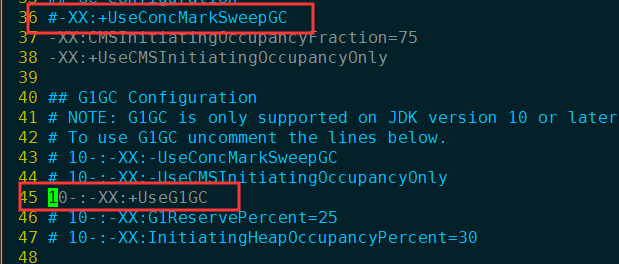
systemctl start elasticsearch

systemctl status elasticsearch



状态中有警告信息（即cms 垃圾收集器在 jdk9 就开始被标注为 @deprecated） 解决方案如下：

vim /etc/elasticsearch/jvm.options



36行加#，45行去掉# 重启elasticsearch

systemctl stop elasticsearch

修改配置文件

vim /etc/elasticsearch/elasticsearch.yml

cluster.name: qian

node.name: node-1

node.master: true

path.data: /var/lib/elasticsearch

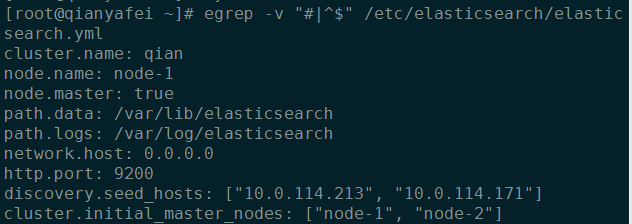
path.logs: /var/log/elasticsearch

network.host: 0.0.0.0

http.port: 9200

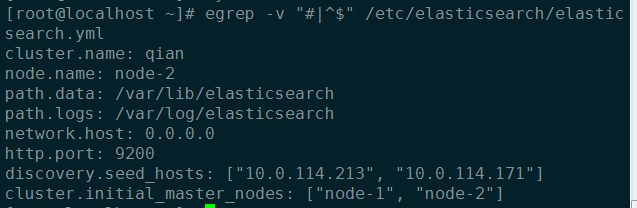
discovery.seed\_hosts: ["10.0.114.213", "10.0.114.171"] #两台es的ip地址

cluster.initial\_master\_nodes: ["node-1", "node-2"]



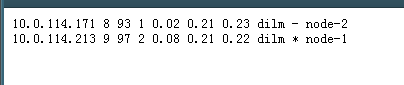
systemctl restart elasticsearch

第二台同理 配置文件如下：



systemctl restart elasticsearch

浏览器访问[http://es机器ip:9200/\_cat/nodes?pretty](http://10.0.114.213:9200/_cat/nodes?pretty)



Es集群搭建完成

安装filebest

yum -y install filebeat-7.4.2-x86\_64.rpm

vim /etc/filebeat/filebeat.yml

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log

filebeat.config.modules:

path: ${path.config}/modules.d/\*.yml

reload.enabled: false

setup.template.settings:

index.number\_of\_shards: 1

setup.kibana:

output.elasticsearch:

hosts: ["10.0.114.213:9200", "10.0.114.171:9200"]

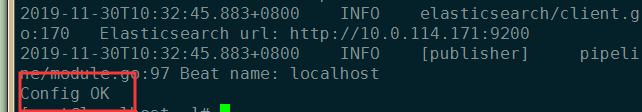
processors:

- add\_host\_metadata: ~

- add\_cloud\_metadata: ~



filebeat test config -e -c /etc/filebeat/filebeat.yml #检测配置文件

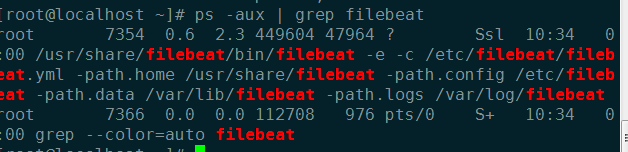


systemctl daemon-reload

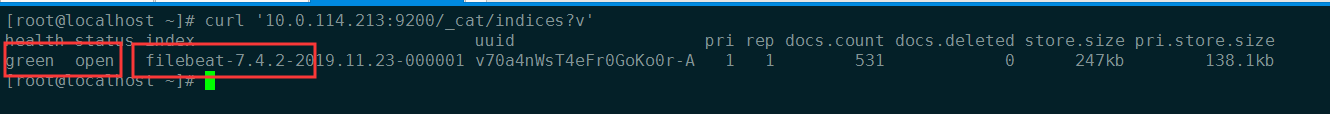
systemctl enable filebeat

systemctl start filebeat

ps -aux | grep filebeat



curl 'es机器ip地址:9200/\_cat/indices?v'



看到一个以filebeat-7.4.2开头的索引，这就代表filesbeat和es能够正常通信了

安装kibana

tar zxfv kibana-7.4.2-linux-x86\_64.tar.gz -C /usr/local/

ln -s /usr/local/kibana-7.4.2-linux-x86\_64/ /usr/local/kibana

vim /usr/local/kibana/config/kibana.yml

server.port: 5601

server.host: "localhost"

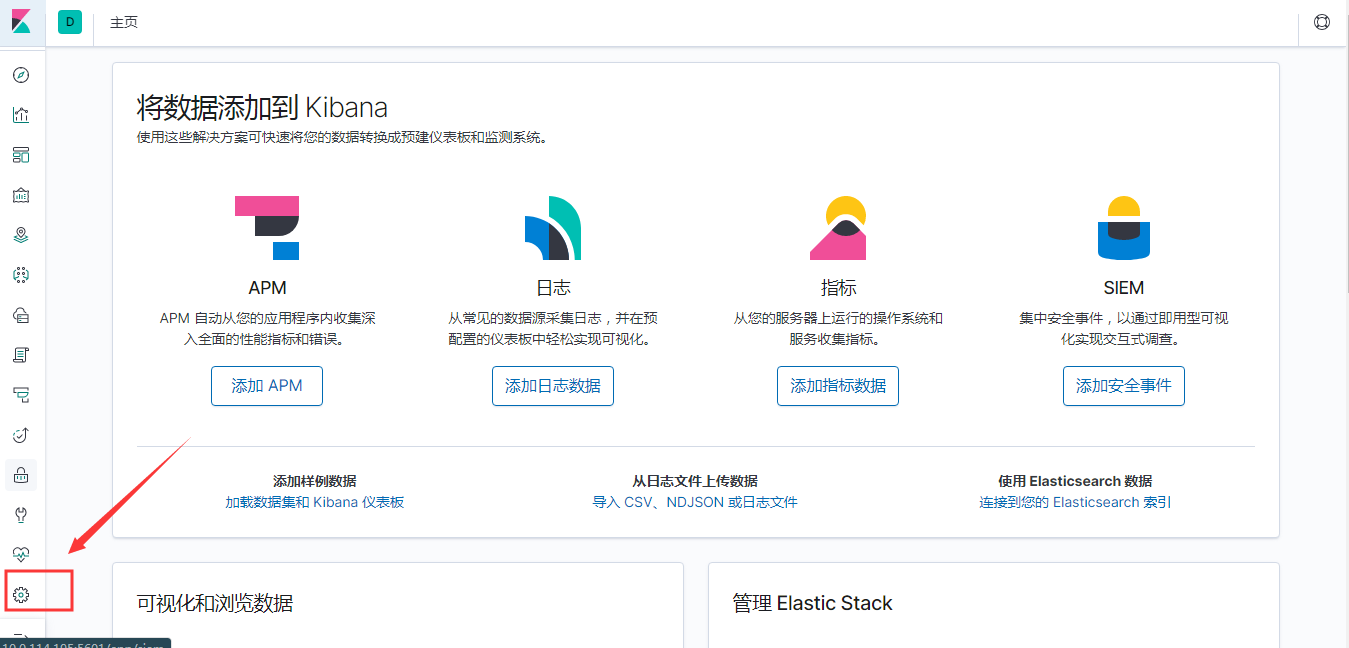
elasticsearch.hosts: ["http://10.0.114.213:9200"]

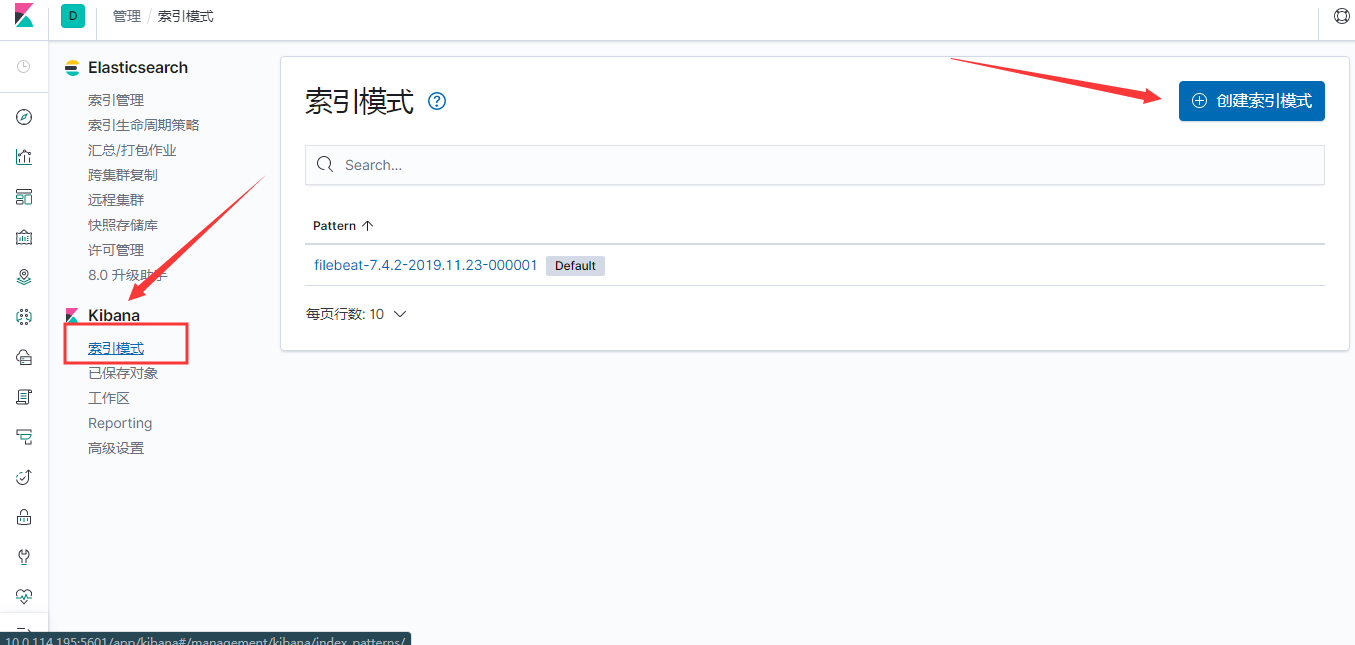
kibana.index: ".kibana"

i18n.locale: "zh-CN"

/usr/local/kibana/bin/kibana --allow-root

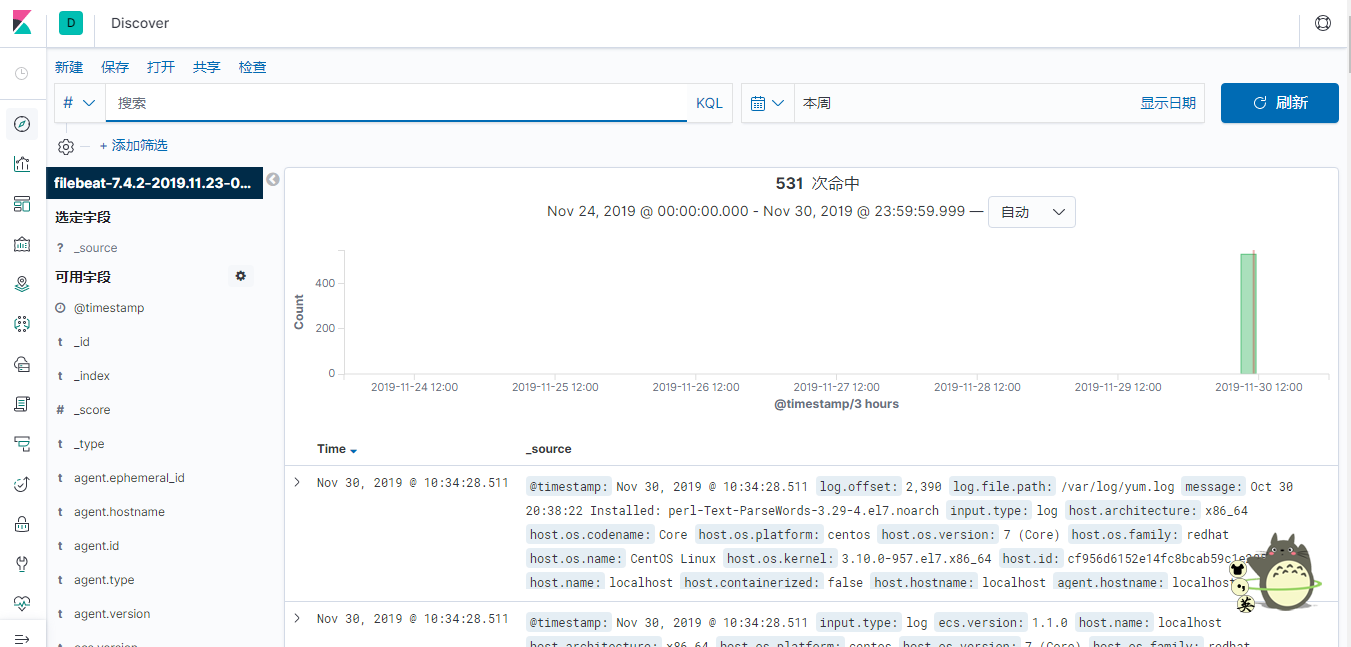
访问浏览器 kibana的ip:5601











也可以点添加日志数据



