一，安装jdk:

add-apt-repository ppa:openjdk-r/ppa

apt-get update

apt-get install -y openjdk-8-jdk unzip

java -version #检查版本

```
root@iZj6c9eouywbpysvh29mdqZ:~# java -version
openjdk version "1.8.0_242"
OpenJDK Runtime Environment (build 1.8.0_242-8u242-b08-0
OpenJDK 64-Bit Server VM (build 25.242-b08, mixed mode)
root@iZj6c9eouywbpysvh29mdqZ:~#
```

vi /etc/security/limits.conf #底部增加，如果已有65535要改为65536

```
* soft nofile 65536
* hard nofile 131072
* soft nproc 65535
* hard nproc 65535
```

向系统打印max_map_count值：

echo "vm.max_map_count = 655360" >>/etc/sysctl.conf

立即生效：

sysctl -p

重启系统或重新连接服务器。

二，安装及配置elasticsearch

wget http://mirror.xrk.org/elk/elasticsearch-6.3.2.tar.gz

tar zxvf elasticsearch-6.3.2.tar.gz && mkdir /data

mv elasticsearch-6.3.2 elasticsearch && mv elasticsearch /data/

useradd elastic && mkdir /home/elastic

passwd elastic

```
root@iZj6c9eouywbpysvh29mdqZ:/data/elasticsearch# passwd elastic
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

vi /data/elasticsearch/config/elasticsearch.yml #修改以下配置

path.data: /path/to/data #数据存放路径，默认软件目录下data

path.logs: /path/to/logs #日志存放路径，默认软件目录下logs

network.host: 0.0.0.0

http.port: 9200

vi /data/elasticsearch/config/jvm.options #配置启动内存，两个值建议设置一样（不改默认1G）

-Xms3g

-Xmx3g

授权

chown -R elastic:elastic /data/elasticsearch/

启动：

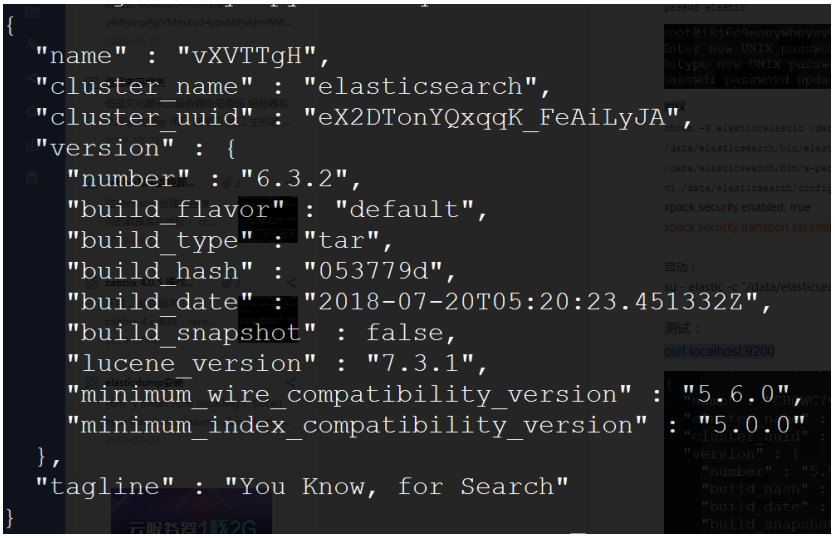
su - elastic -c "/data/elasticsearch/bin/elasticsearch -d"

日志查看：

tail -f /data/elasticsearch/logs/elasticsearch.log

测试：

curl localhost:9200



三，kibana管理工具：

wget http://mirror.cnop.net/elk/kibana-6.3.2-linux-x86_64.tar.gz

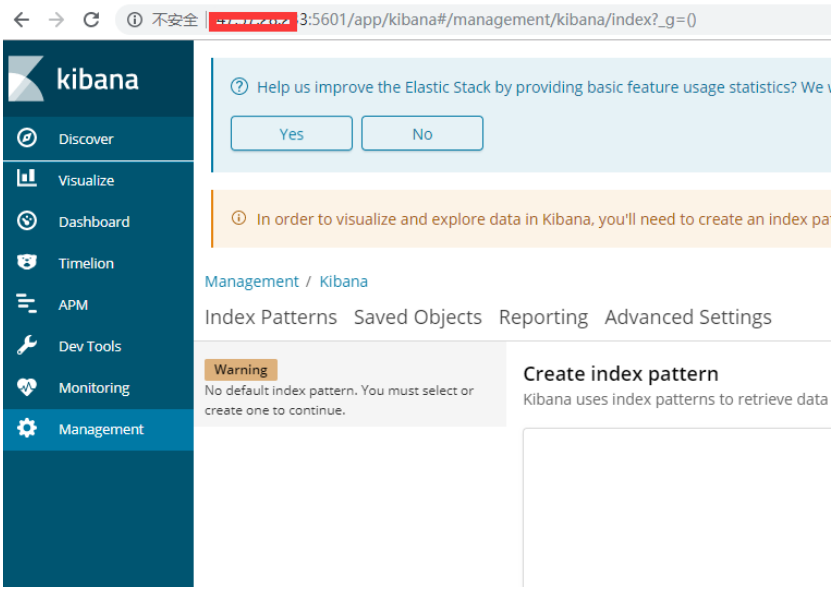
```
tar zxvf kibana-6.3.2-linux-x86_64.tar.gz
mv kibana-6.3.2-linux-x86_64 /data/kibana
vi /data/kibana/config/kibana.yml #去除下面注释

server.port: 5601 #监听的端口
server.host: "0.0.0.0" #监听的地址
elasticsearch.url: "http://localhost:9200"  #elasticsearch访问的URL地址
```

启动：

```
chown -R elastic:elastic /data/kibana
```

su - elastic -c " `/data/kibana/bin/kibana &`"

访问 http://ip:5601



四，加入密码验证：

elasticsearch6.3版本之后x-pack是默认安装好的

```
vi /data/elasticsearch/config/elasticsearch.yml #尾部加入以下
xpack.security.enabled: false #关闭x-pack

cd /data/elasticsearch/modules/x-pack/x-pack-core/
rm -rf x-pack-core-6.3.2.jar #删除原包，并用我们破解后的包进行替换
wget http://mirror.xrk.org/elk/x-pack-core-6.3.2.jar
```

vi license.json #新建json文件

{"license":{"uid":"72ee62fb-865a-4887-9c87-168fe12a1265","type":"platinum","issue_date_in_millis":1530230400000,"expiry_date_in_millis":4102329600000,"max_nodes":100,"issued_to":"jin king (ccn)","issuer":"Web Form","signature":"AAAAAwAAAA02Dgj8/hUDfzKEQ2nrAAABmC9ZN0hjZDBGYnVyRXpCOW5Bb3FjZDAxOWpSbTVoMVZwUzRxVk1PSmkxaktJRVl5Ml

重启下es：

su - elastic -c "/data/elasticsearch/bin/elasticsearch -d"

上传到服务器，命令如下（密码 change）：

curl -XPUT -u elastic 'http://localhost:9200/_xpack/license' -H "Content-Type: application/json" -d @license.json

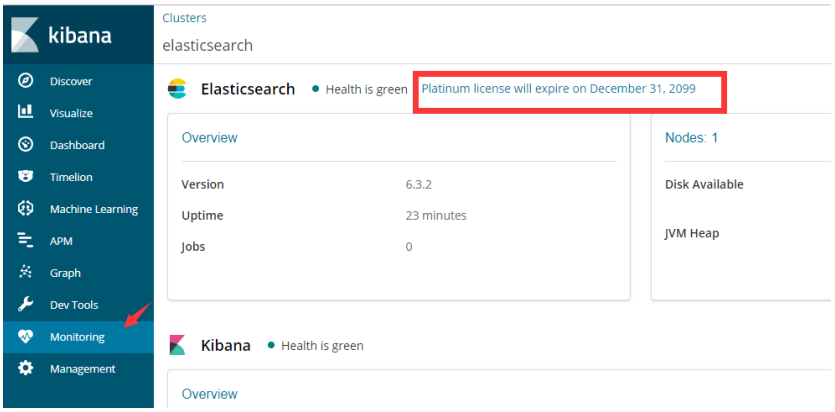
```
Enter host password for user 'elastic':
{"acknowledged":true,"license_status":"valid"}
root@iZj6c9eouywbpysvh29mdqZ:~#
```

```
vi /data/elasticsearch/config/elasticsearch.yml  #尾部
#xpack.security.enabled: false
xpack.security.transport.ssl.enabled: true
```

重新启动：

su - elastic -c "/data/elasticsearch/bin/elasticsearch -d"

访问kibana http://ip:5601 ,查看license，这时时间已经变长：



/data/elasticsearch/bin/elasticsearch-setup-passwords auto #生成密码

```
root@iZj6c9eouywbpysvh29mdqZ:~# /data/elasticsearch/bin/elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic,kibana,logstash_system,beats_system.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y

Changed password for user kibana
PASSWORD kibana = 8OStjU6EOwGt5IfI0TOY

Changed password for user logstash_system
PASSWORD logstash_system = eeukJVPaIJ5eIWKaRlbr

Changed password for user beats_system
PASSWORD beats_system = dd6df7p25RIgyFMQ3s7q

Changed password for user elastic
PASSWORD elastic = aGFf5WYVqd5juGxvgjDP
```

Changed password for user kibana
PASSWORD kibana = 8OStjU6EOwGt5IfI0TOY

Changed password for user logstash_system
PASSWORD logstash_system = eeukJVPaIJ5eIWKaRlbr

Changed password for user beats_system
PASSWORD beats_system = dd6df7p25RIgyFMQ3s7q

Changed password for user elastic
PASSWORD elastic = aGFf5WYVqd5juGxvgjDP

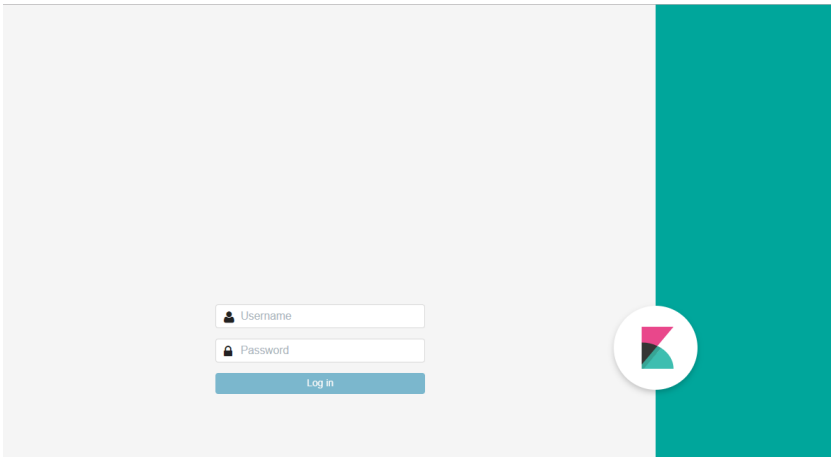
vi /data/kibana/config/kibana.yml　#把上面密码 aGFf5WYVqd5juGxvgjDP 加入kibana.yml
找到：

```
#elasticsearch.username: "user"
#elasticsearch.password: "pass"
```

替换成：

```
elasticsearch.username: "elastic"
elasticsearch.password: "aGFf5WYVqd5juGxvgjDP"    #就是上一步生成的elastic的账号和密码
```

重启下：
su - elastic -c " /data/kibana/bin/kibana &"
访问 http://ip:5601 ，输入密码信息即可。



其他：
GET _cat/indices　#查看所有索引

创建一个默认索引,添加数据：
POST /indextest/_doc

{
"field1": "indextest this test field1",
"field2": "indextest this test field2"
}

yellow
GET /_cat/shards?h=index,shard,prirep,state,unassigned.reason| grep UNASSIGNED

PUT _settings
{
"number_of_replicas":0
}

说明：**x-pack的内置用户**

username	role	权限
elastic	superuser	内置的elasticsearch超级管理员，拥有所有权限
kibana	kibana_system	用户kibana用来连接elasticsearch并与之通信。Kibana服务器以该用户身份提交请求以访问集群监视API和 .kibana索引。不能访问index
logstash_system	logstash_system	用户Logstash在Elasticsearch中存储监控信息时使用
beats_system	beats_system	用户beats在Elasticsearch中存储监控信息时使用

五，开机启动

Ubuntu18.04 不能像16.04 那样可以直接使用 /etc/rc.local 文件，需要设置

vi /etc/systemd/system/rc-local.service

[Unit]
Description=/etc/rc.local Compatibility
ConditionPathExists=/etc/rc.local

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99

[Install]
WantedBy=multi-user.target

vi /etc/rc.local

#!/bin/sh -e
#
rc.local
#
This script is executed at the end of each multiuser runlevel.
Make sure that the script will "exit 0" on success or any other
value on error.
#
In order to enable or disable this script just change the execution

```
# bits.
#
# By default this script does nothing.
su - elastic -c "/data/elasticsearch/bin/elasticsearch -d"
su - elastic -c "/data/kibana/bin/kibana &"
exit 0
```

```
chmod 755 /etc/rc.local && systemctl enable rc-local && systemctl start rc-local.service
```

```
reboot   #重启下系统，查看是否开机启动。
```

参考

https://www.cnblogs.com/panwenbin-logs/p/9674845.html

https://blog.csdn.net/time_future/article/details/85805298