# Elasticsearch集群基础安全Xpack设置

## 一、更改ES配置文件

在config目录下对elasticsearch.yml文件进行更改，加入以下内容（最后两个路径也可以写成绝对路径）所有节点都需要加以下配置

xpack.security.enabled: true

xpack.security.http.ssl.enabled: true

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

xpack.security.transport.ssl.client\_authentication: required

xpack.security.transport.ssl.keystore.path: elastic-certificates.p12 #（建议改成绝对路径 如：/home/esuser/elasticsearch-7.10.2/config/elastic-certificates.p12）

xpack.security.transport.ssl.truststore.path: elastic-certificates.p12#（建议改成绝对路径 ）

## 官网地址

## https://www.elastic.co/guide/en/elasticsearch/reference/7.17/security-basic-setup.html

## 二、在一个节点生成节点证书

**1.选择一个节点，在其bin目录下执行以下命令**

./bin/elasticsearch-certutil ca

1. 出现提示时，接受默认文件名，即。此文件包含CA的公共证书和用于为每个节点签署证书的私钥。elastic-stack-ca.p12 （按回车）
2. 输入CA的密码。如果您没有部署到生产环境，则可以选择将密码留空。输入密码（需要提前准备）

**2.在任何单个节点上，为集群中的节点生成证书和私钥。您包括在上一步中生成的输出文件.elastic-stack-ca.p12**

./bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12

1. 输入CA的密码（1-B输入的密码）
2. 出现提示，接受默认文件名及路径（按回车）
3. 出现提示，为elastic-certificates.p12文件生成保护密码（需要提前准备）

会在elasticsearch根目录下生成elastic-certificates.p12文件，将该文件复制到config目录下

1. **①．如果您在创建节点证书时输入了密码，请运行以下命令将密码存储在Elasticsearch密钥库中,（会在config目录下生成****elasticsearch.keystore）：**

**②.如果没有，不需要运行下面两条命令**

./bin/elasticsearch-keystore add xpack.security.transport.ssl.keystore.secure\_password

./bin/elasticsearch-keystore add xpack.security.transport.ssl.truststore.secure\_password

生成后在config目录中可查到对应文件



如果未进行3-②，则没有**elasticsearch.keystore文件**

## 三、设置密码（手动）

手动：./bin/elasticsearch-setup-passwords interactive

手动需要输入密码，需要提前准备好

**密码配置时如下（用户名默认为elastic）：**

**Initiating the setup of passwords for reserved users elastic,apm\_system,kibana,kibana\_system,logstash\_system,beats\_system,remote\_monitoring\_user.**

**You will be prompted to enter passwords as the process progresses.**

**Please confirm that you would like to continue [y/N]y**

**Enter password for [elastic]:**

**Reenter password for [elastic]:**

**Enter password for [apm\_system]:**

**Reenter password for [apm\_system]:**

**Enter password for [kibana\_system]:**

**Reenter password for [kibana\_system]:**

**Enter password for [logstash\_system]:**

**Reenter password for [logstash\_system]:**

**Enter password for [beats\_system]:**

**Reenter password for [beats\_system]:**

**Enter password for [remote\_monitoring\_user]:**

**Reenter password for [remote\_monitoring\_user]:**

**Changed password for user [apm\_system]**

**Changed password for user [kibana\_system]**

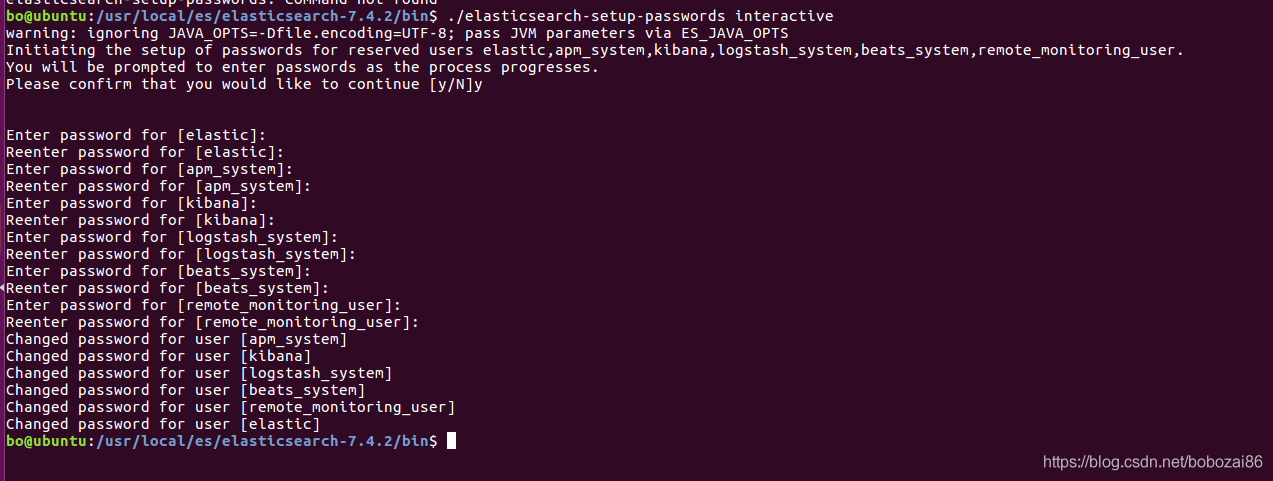
**Changed password for user [kibana]**

**Changed password for user [logstash\_system]**

**Changed password for user [beats\_system]**

**Changed password for user [remote\_monitoring\_user]**

**Changed password for user [elastic]**



## 四、将节点证书发给其余节点

在生成节点的主机内执行以下命令，分别对每个主机发送对应文件

scp elastic-certificates.p12 elasticsearch.keystore username@ip:config

（其中标红部分需要对应修改，ip后面应写绝对路径）

注意：有几个节点就需要分发几次，每个节点都需要

## 五、重启ES节点

对该集群各节点进行杀掉进程并重启

具体步骤如下：

查询进程号：ps aux | grep elastic

杀死进程：kill 00000（对应的进程号）

重启节点：./elasticsearch -d（在bin目录下执行）

## 六、验证

在浏览器中输入节点所在的对应地址ip:9200，出现如下图情况即为成功

