|  |
| --- |
|  |

|  |
| --- |
| **永达ELK安装实施手册** |
|  |
|  |
|  |
|  |
|  |

目录

[一、软件版本 3](#_Toc68784251)

[二、 安装前准备工作 4](#_Toc68784252)

[2.1系统资源表 4](#_Toc68784253)

[2.2 服务器磁盘分区 4](#_Toc68784254)

[2.3 网络信息表 4](#_Toc68784255)

[三、ELK环境准备 5](#_Toc68784256)

[3.1.操作系统环境 5](#_Toc68784257)

[3.1.1系统磁盘划分 5](#_Toc68784258)

[3.1.2系统内存信息 5](#_Toc68784259)

[3.1.3系统网络信息 5](#_Toc68784260)

[3.2安装配置elasticsearch服务 6](#_Toc68784261)

[3.2.1安装elasticsearch 6](#_Toc68784262)

[3.2.2修改elasticsearch配置文件 6](#_Toc68784263)

[3.2.3添加开机自启，启动elasticsearch，查看端口和服务是否启动 6](#_Toc68784264)

[3.2.4设置权限管理账户密码 6](#_Toc68784265)

[3.2.5检查服务状态信息 7](#_Toc68784266)

[3.3安装配置logstash服务 7](#_Toc68784267)

[3.3.1解压安装文件到/usr/local/logstash目录 7](#_Toc68784268)

[3.3.2修改文件pipelines.yml，添加以下内容: 7](#_Toc68784269)

[3.3.3编辑采集日志配置文件 8](#_Toc68784270)

[3.3.4添加开机自启动服务 9](#_Toc68784271)

[3.4安装配置kibana服务 10](#_Toc68784272)

[3.4.1安装kibana包 10](#_Toc68784273)

[3.4.2配置kibana.yml文件 10](#_Toc68784274)

[3.4.3添加开机自启动kibana服务 10](#_Toc68784275)

[3.5安装配置winlogbeat服务 11](#_Toc68784276)

[3.5.1安装winlogbeat 11](#_Toc68784277)

[3.5.2配置winlogbeat.yml,设置主机地址和账户密码 11](#_Toc68784278)

[3.5.3启动winlogbeat服务 11](#_Toc68784279)

[3.6监控权限配置设置 12](#_Toc68784280)

[3.6.1登录kibana 12](#_Toc68784281)

[3.6.2选择manage 12](#_Toc68784282)

[3.6.3选择创建用户或者角色 12](#_Toc68784283)

[3.6.4创建只读用户 15](#_Toc68784284)

[3.6.5填写用户信息角色 16](#_Toc68784285)

[3.7创建索引信息 17](#_Toc68784286)

[3.7.1选择kibana下面的index patterns 17](#_Toc68784287)

[3.7.2创建index pattern 18](#_Toc68784288)

[3.7.3添加index pattern name 18](#_Toc68784289)

[3.7.4查看日志 19](#_Toc68784290)

[3.7.5选择查看日志类型 20](#_Toc68784291)

[3.7.6定期删除索引 21](#_Toc68784292)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **标题** | 永达ELK日志系统 | | | |
| **项目名称** | ELK日志系统 | | | |
| **类别** | 管理文档□ 设计方案□ 实施文档 X  配置文档□ 测试文档□ 其他□ | | | |
| **摘要** |  | | | |
| **当前版本** | v1.0 | | | |
| **创建日期** | 2021.03.03 | | | |
| **文档作者** | 贺元明 | | | |
| **文件名称** |  | | | |
| **版本号** | **日期** | **修改人** | **审阅人** | **摘要** |
| v1.0 | 2021.03 | 贺元明 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 一、软件版本

**A:ELK主机信息：**

操作系统：centos 7.9\_x86 (64 bit)

软件版本：Elasticsearch：elasticsearch-7.10.1-x86\_64.rpm

logstash：logstash-7.10.1-x86\_64.rpm

logstash-7.11.1-linux-x86\_64.tar.gz

logstash-7.11.1-windows-x86\_64.zip

kinaba：kibana-7.10.1-x86\_64.rpm

Java：java-1.8.0-openjdk-1.8.0.212.b04-0.el7\_6.x86\_64

**B:监控系统信息：**

操作系统：SLES12 for SAP SP2

Centos6.5\_x86\_64

Centos7.6\_x86\_64

Windows Server 2012 R2

数据库软件：MySQL：Server version: 5.7.20-log MySQL Community Server (GPL)

# 二、 安装前准备工作

## 2.1系统资源表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 系统 | CPU | 内存 | 系统盘 | 数据盘 |
| velkprd | Centos7.6 x64 | 2 | 16G | 100G | 500G |
|  |  |  |  |  |  |

## 2.2 服务器磁盘分区

a.系统磁盘分区

|  |  |  |  |
| --- | --- | --- | --- |
| 文件系统 | 容量 | 文件类型 | 挂载点 |
| /dev/sda1 | 1000M | xfs | /boot |
| /dev/mapper/centos-root | 544G | xfs | / |
| /dev/mapper/centos-swap | 16G | SWAP |  |

## 2.3 网络信息表

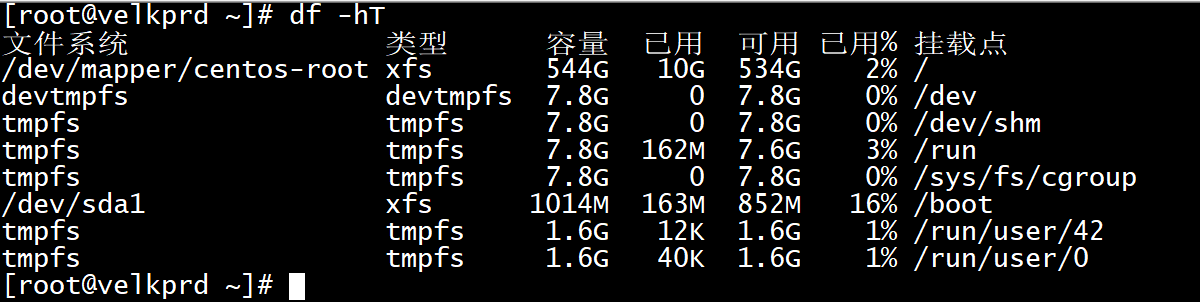
A.资产中间件主机名、IP地址信息：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | IP Address | gateway | netmask | Interface |
| velkprd | 192.168.20.68 | 192.168.20.1 | 255.255.255.0 | ens192 |
|  |  |  |  |  |

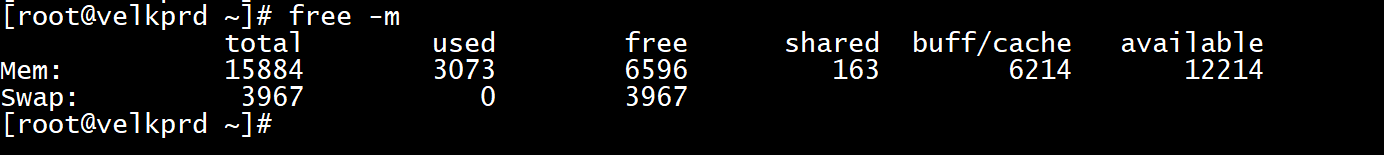
# 三、ELK环境准备

## 3.1.操作系统环境

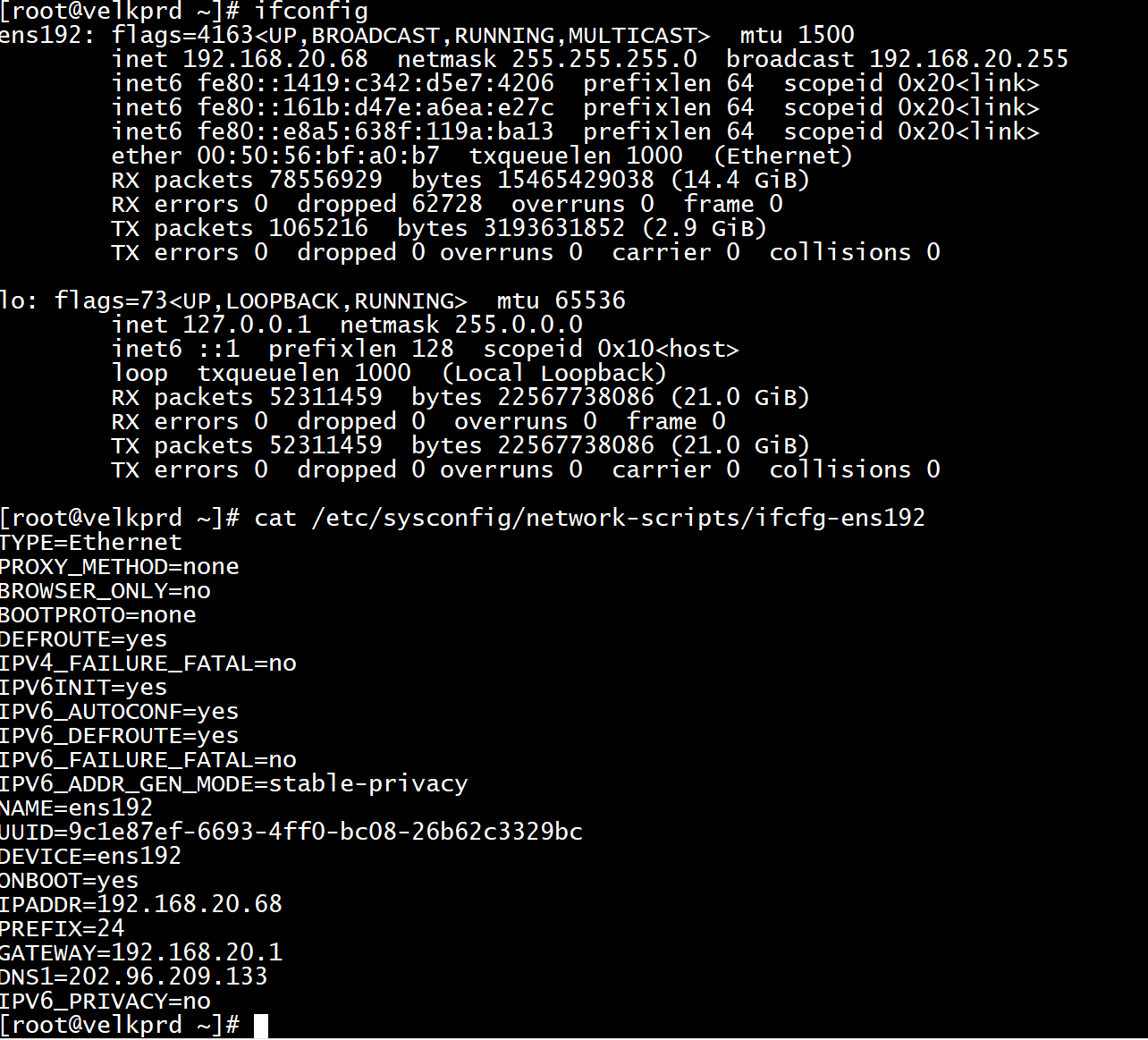
### 3.1.1系统磁盘划分



### 3.1.2系统内存信息

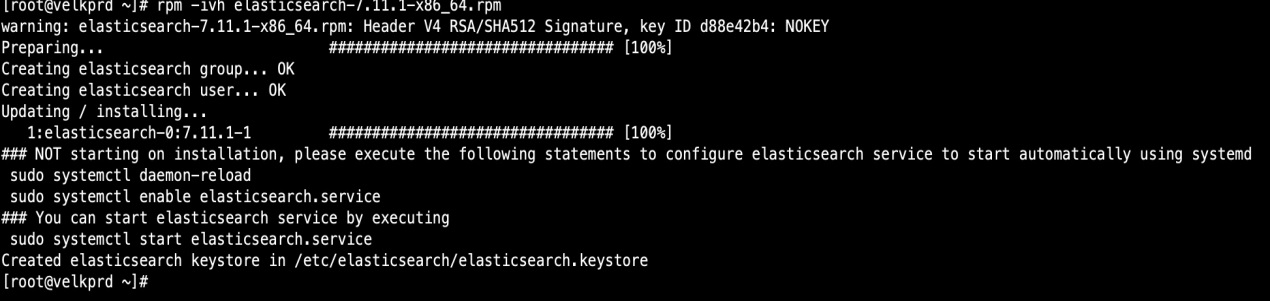


### 3.1.3系统网络信息

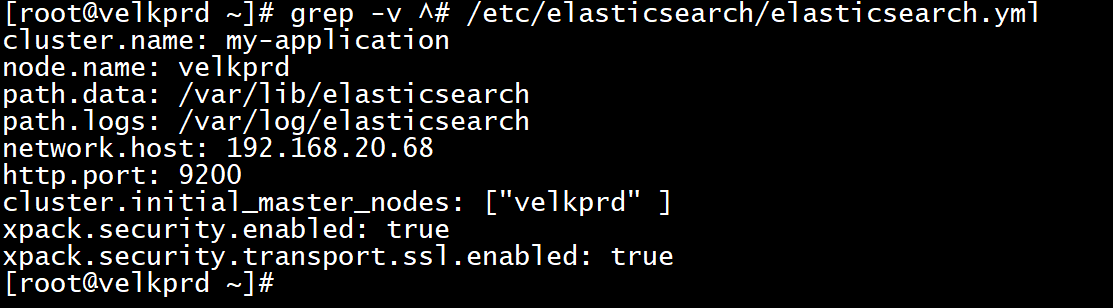


## 3.2安装配置elasticsearch服务

### 3.2.1安装elasticsearch



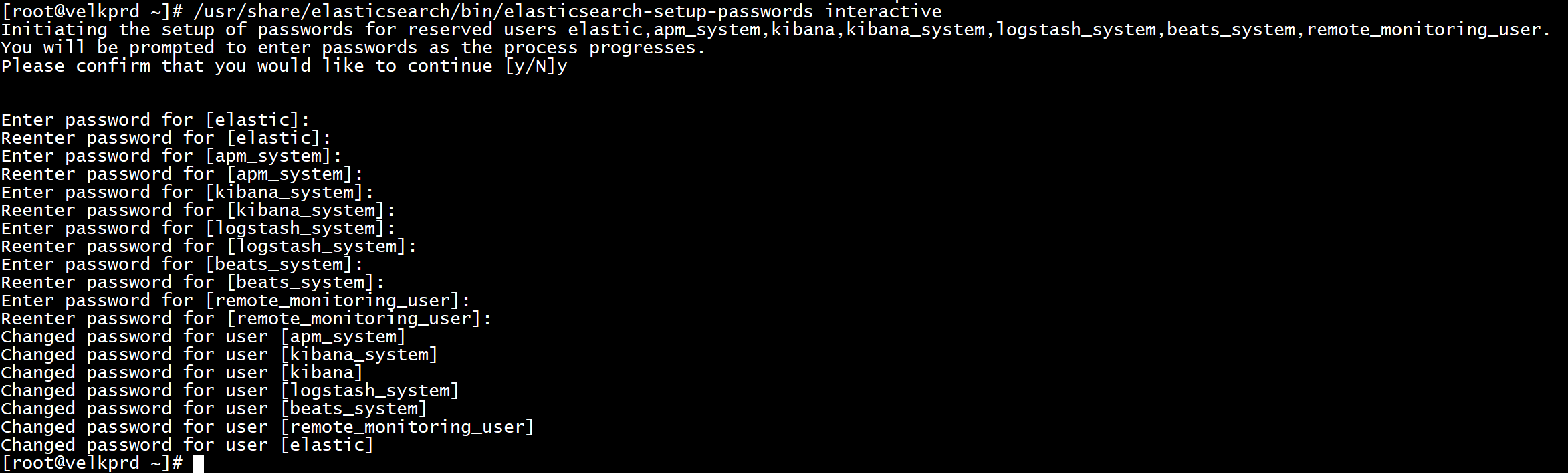
### 3.2.2修改elasticsearch配置文件



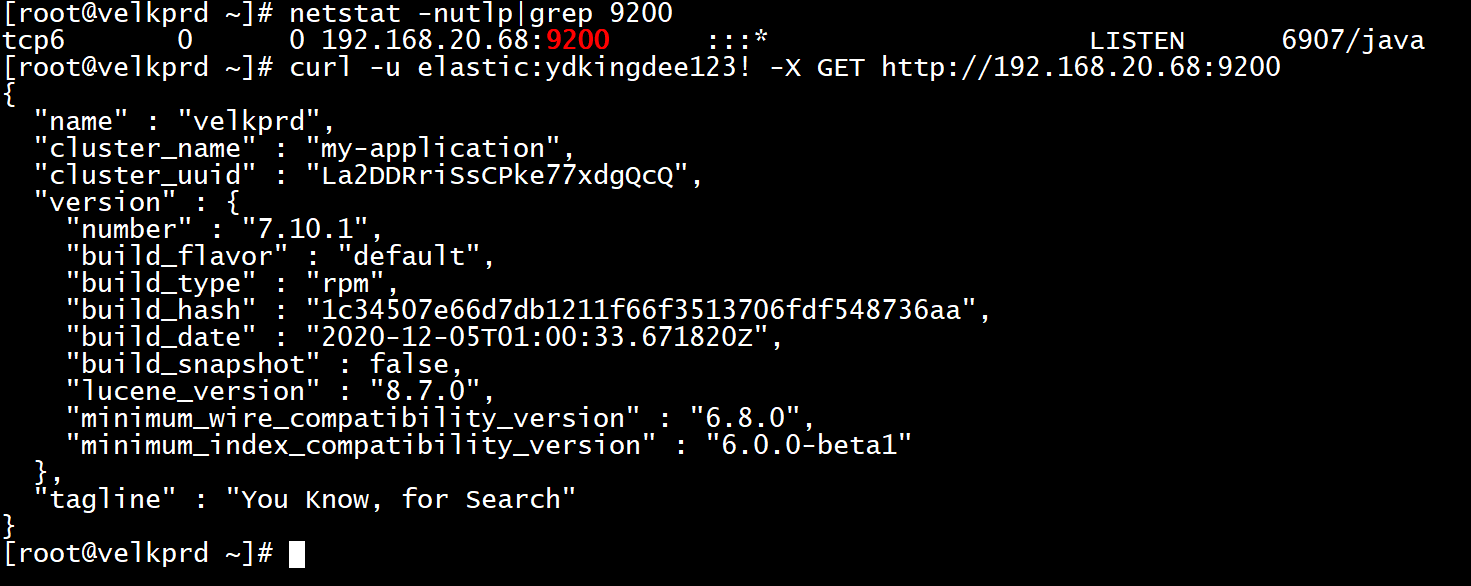
### 3.2.3添加开机自启，启动elasticsearch，查看端口和服务是否启动



### 3.2.4设置权限管理账户密码

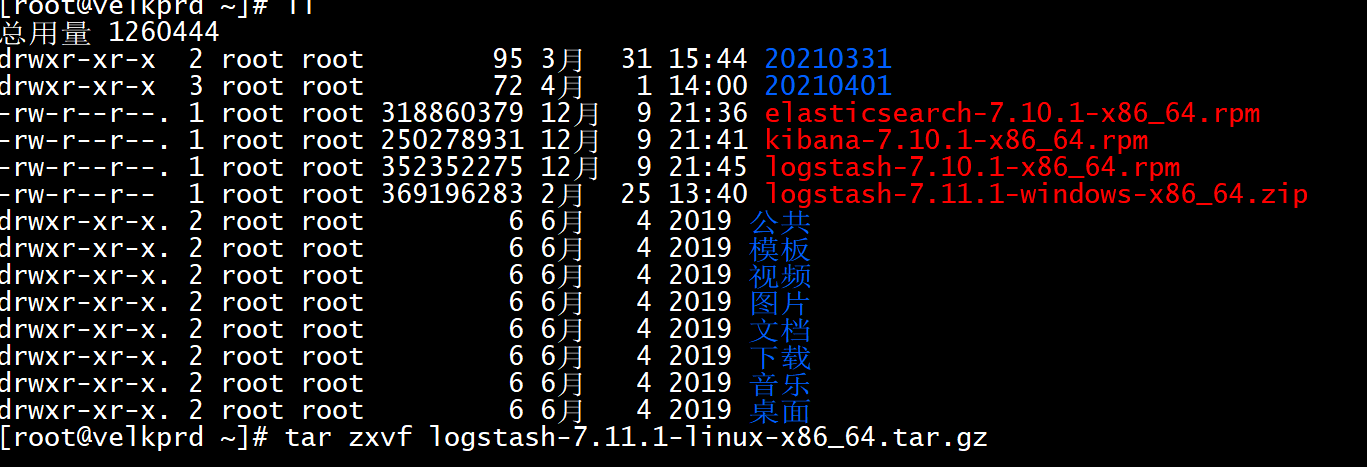


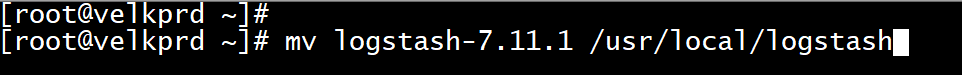
### 3.2.5检查服务状态信息



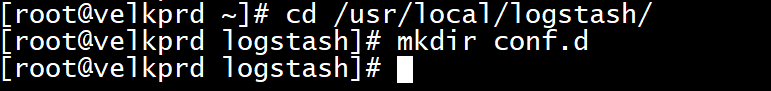
## 3.3安装配置logstash服务

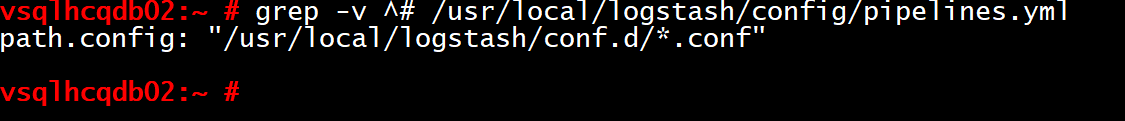
### 3.3.1解压安装文件到/usr/local/logstash目录



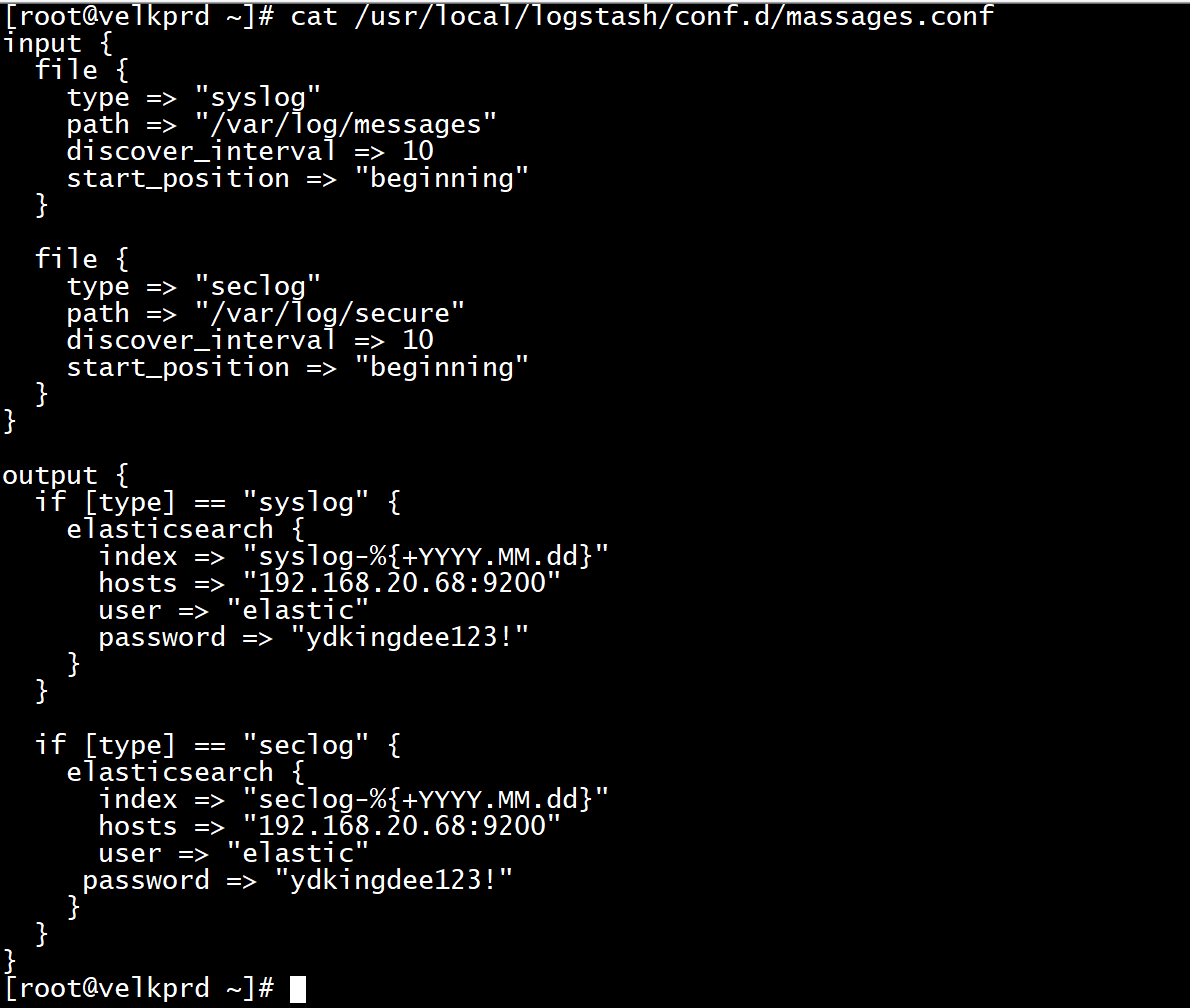


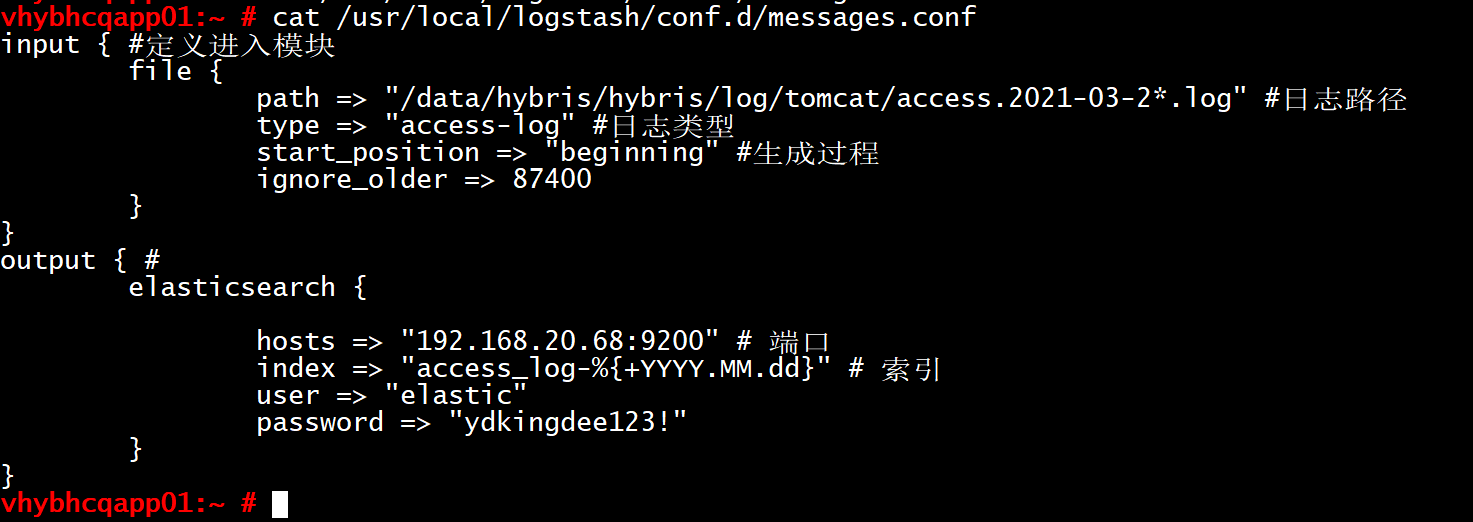
### 3.3.2修改文件pipelines.yml，添加以下内容:



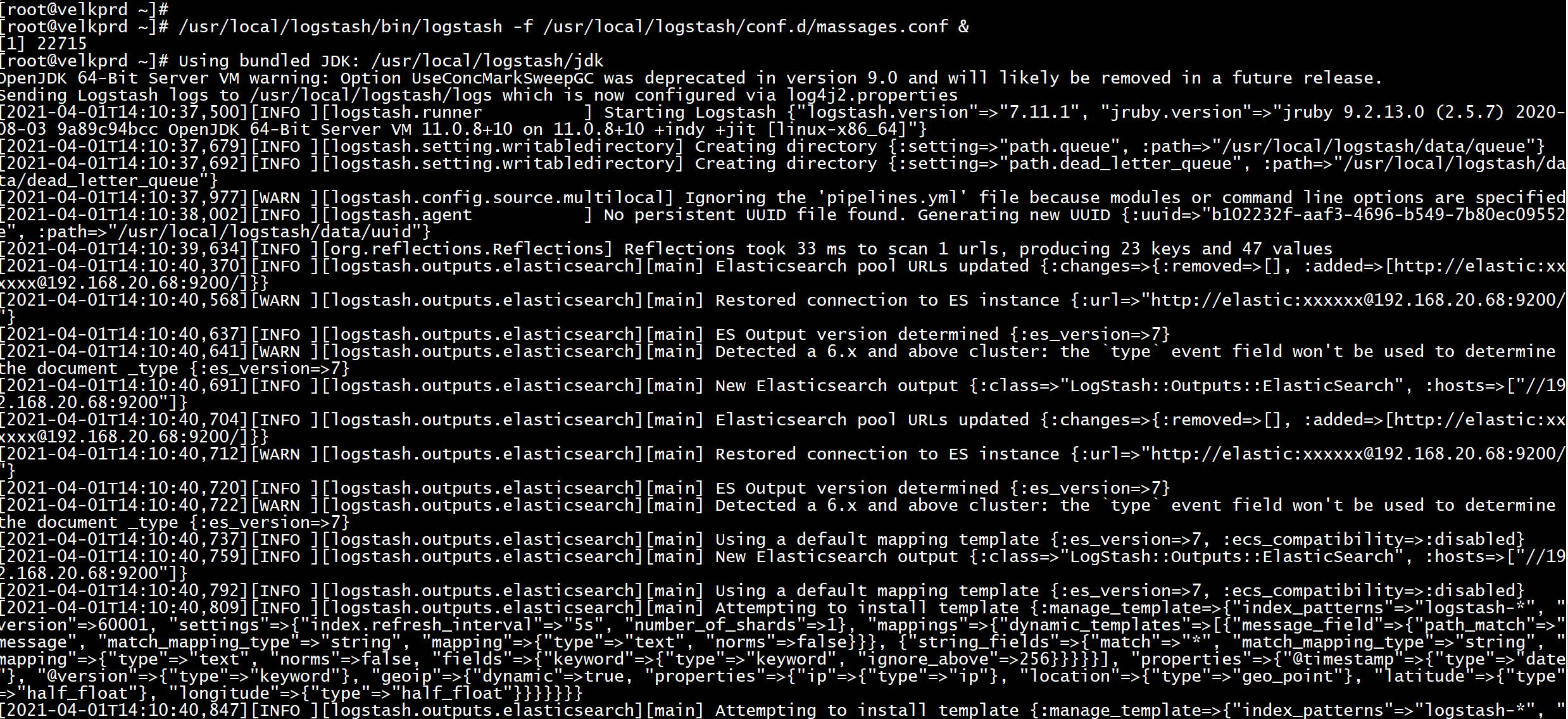


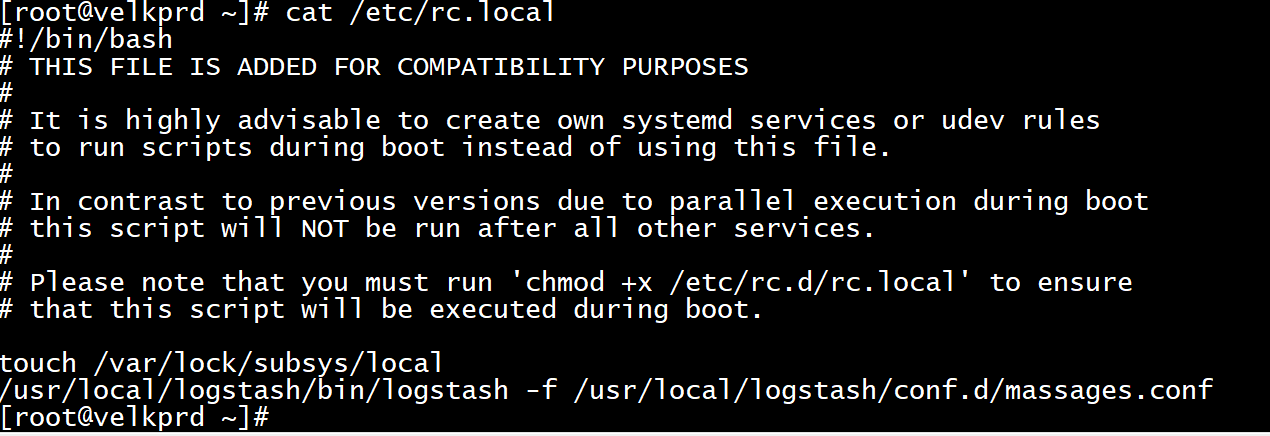
### 3.3.3编辑采集日志配置文件

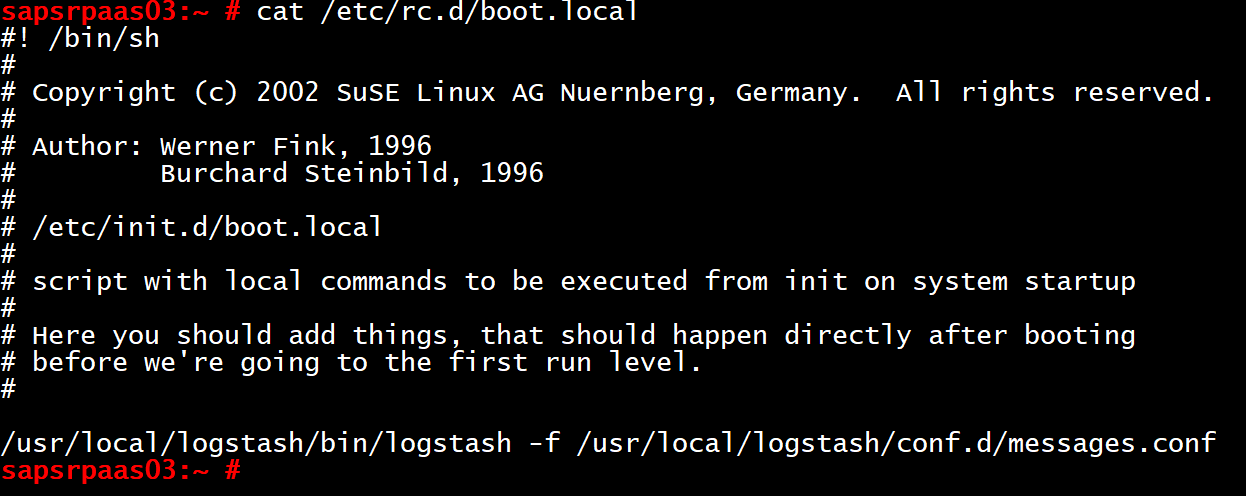




### 3.3.4添加开机自启动服务





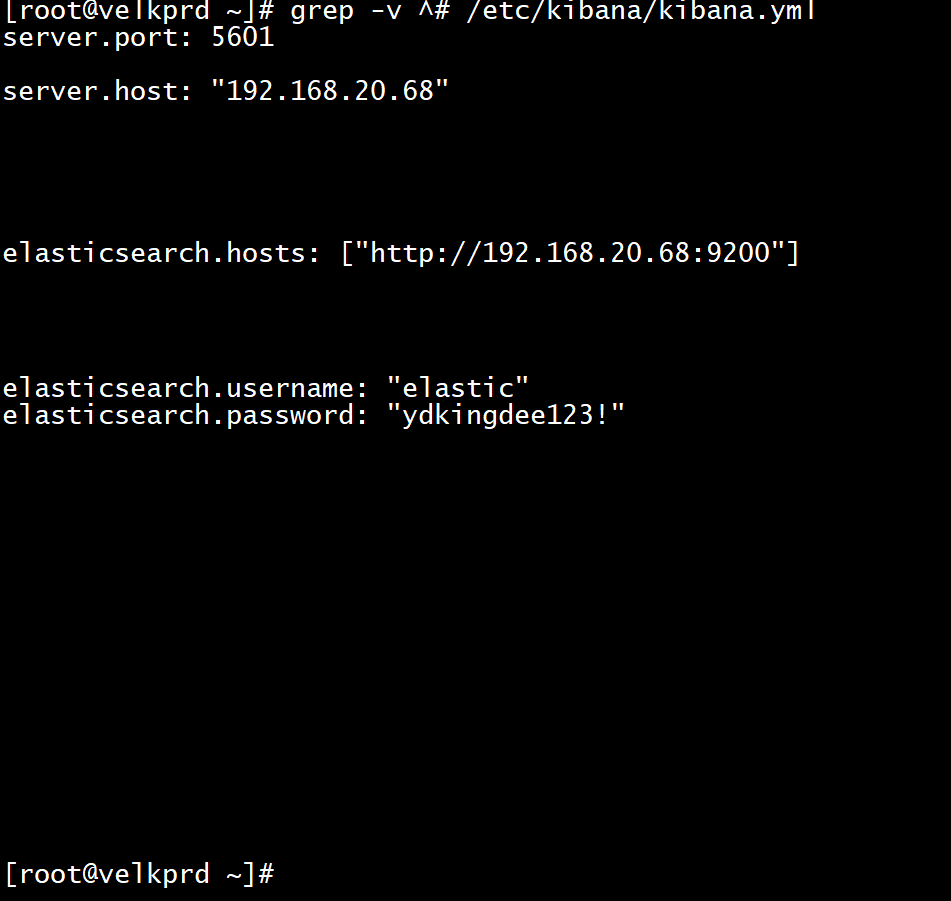


## 3.4安装配置kibana服务

### 3.4.1安装kibana包



### 3.4.2配置kibana.yml文件



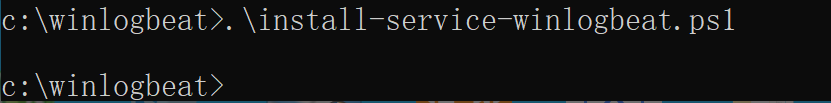
### 3.4.3添加开机自启动kibana服务



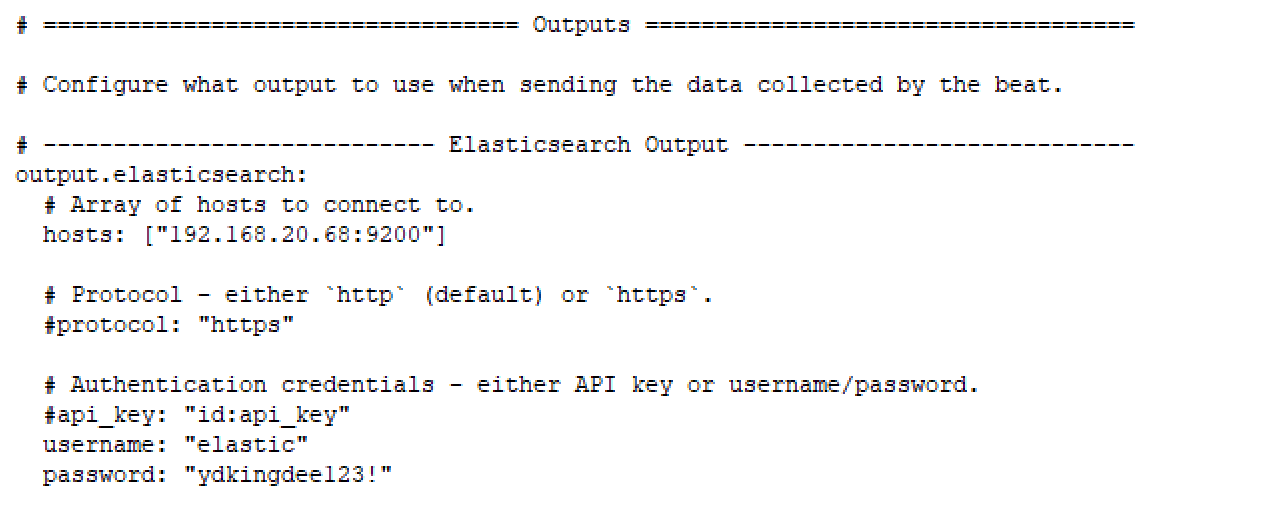
## 3.5安装配置winlogbeat服务

### 3.5.1安装winlogbeat

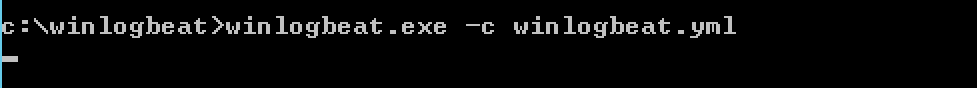
cmd进入解压缩软件目录，执行下面语句安装winlogbeat,安装后服务自动设置为开机启动



### 3.5.2配置winlogbeat.yml,设置主机地址和账户密码

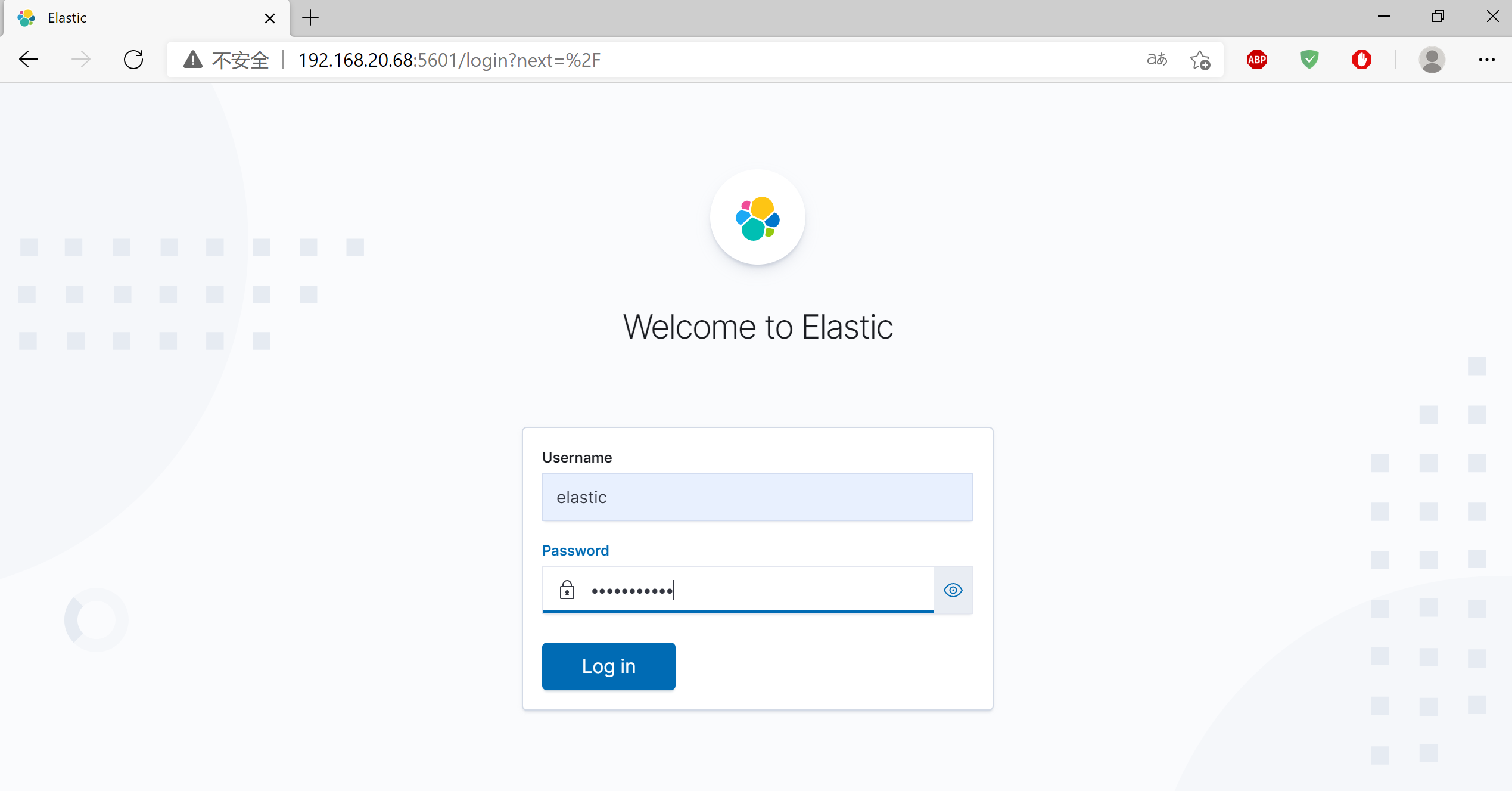


### 3.5.3启动winlogbeat服务

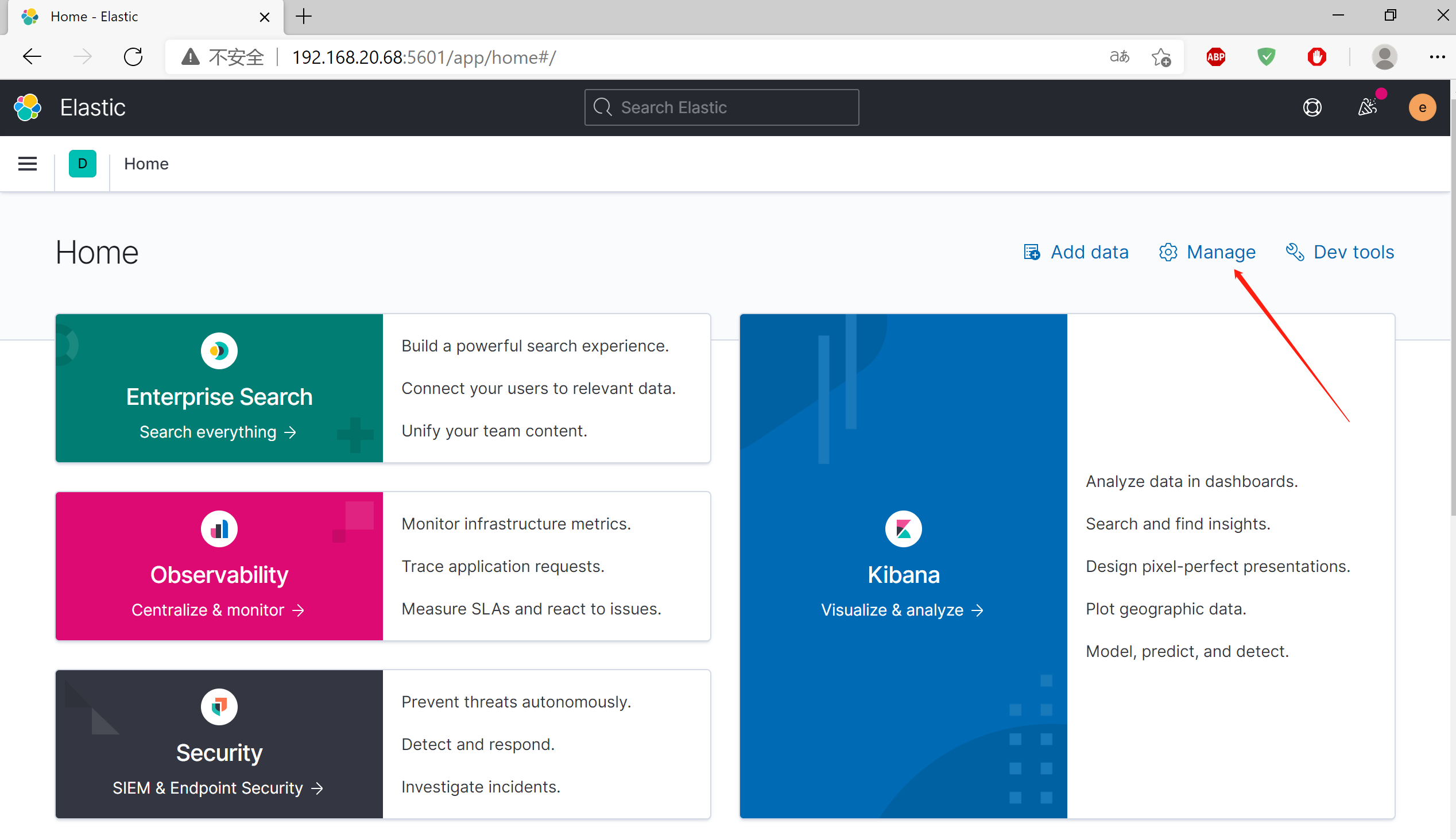


## 3.6监控权限配置设置

### 3.6.1登录kibana

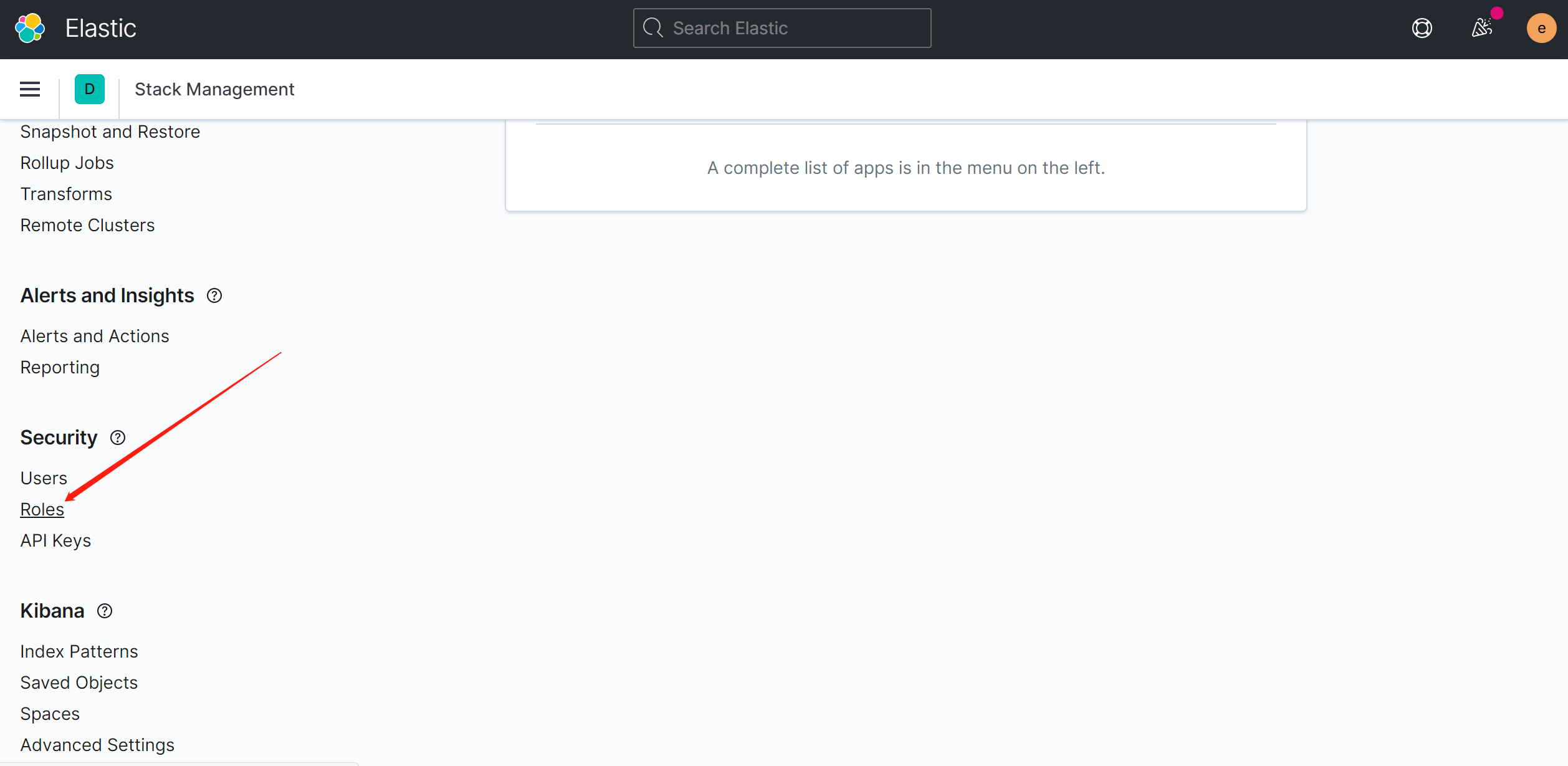


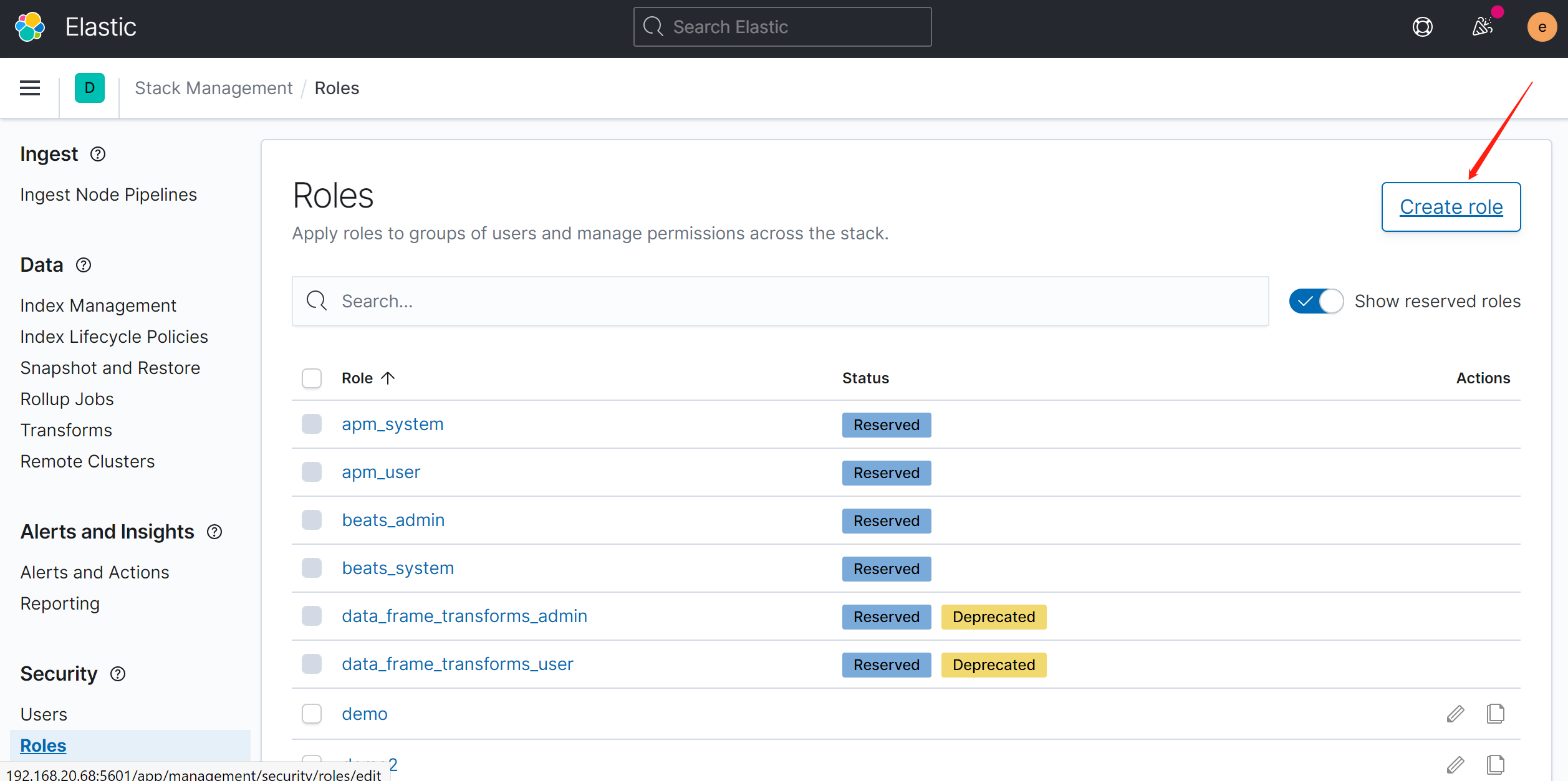
### 3.6.2选择manage



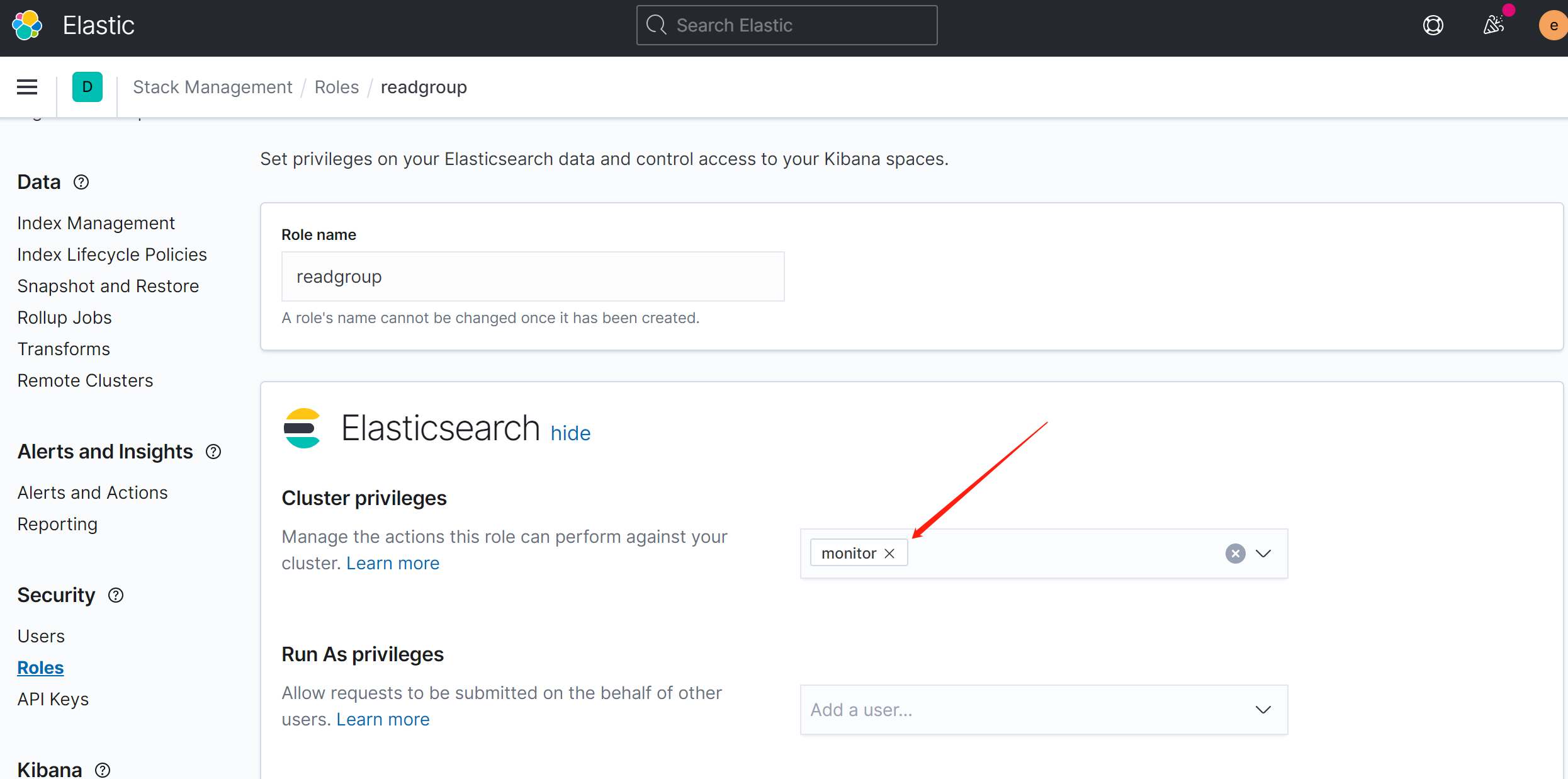
### 3.6.3选择创建用户或者角色

1）创建角色

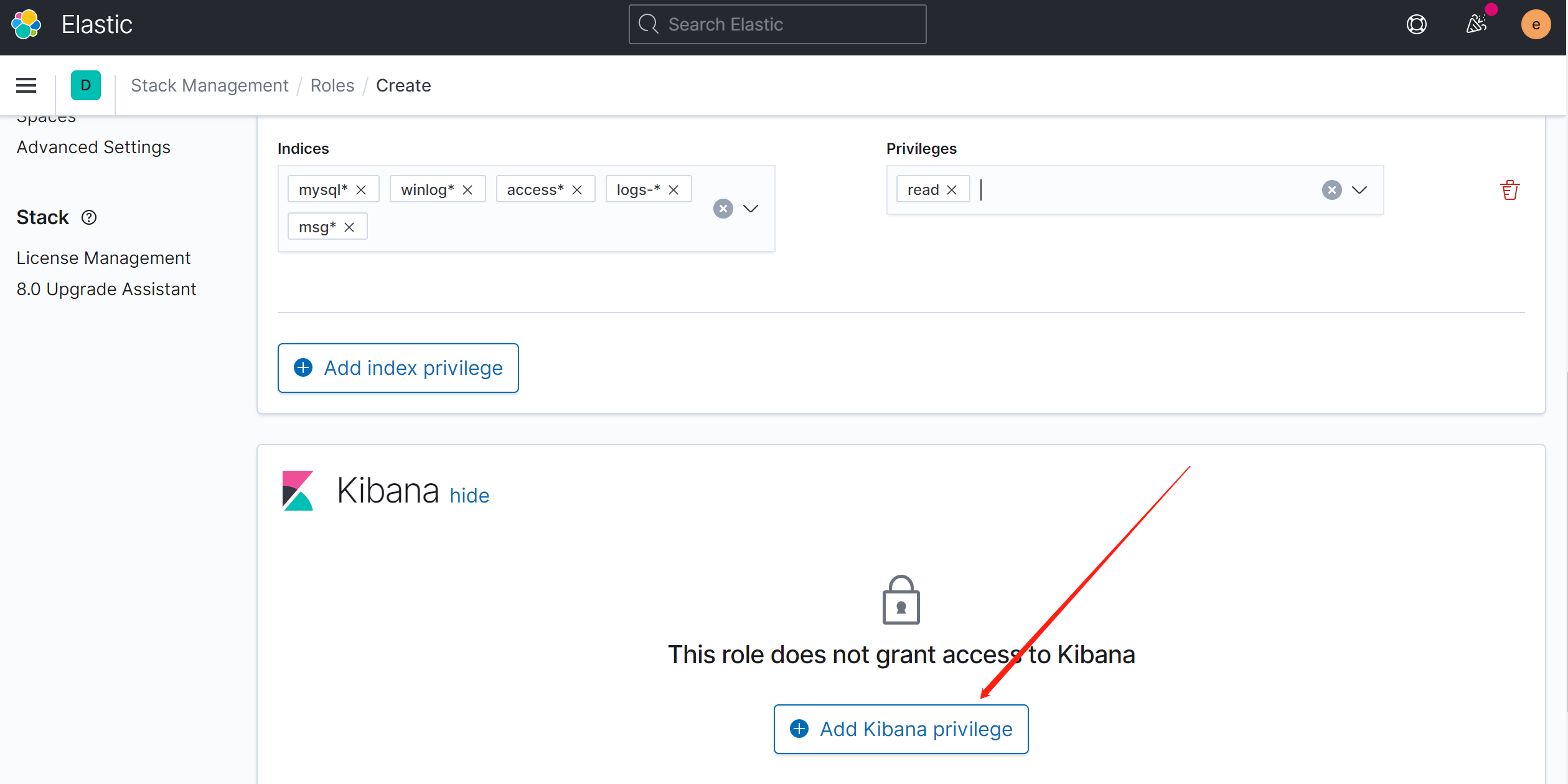




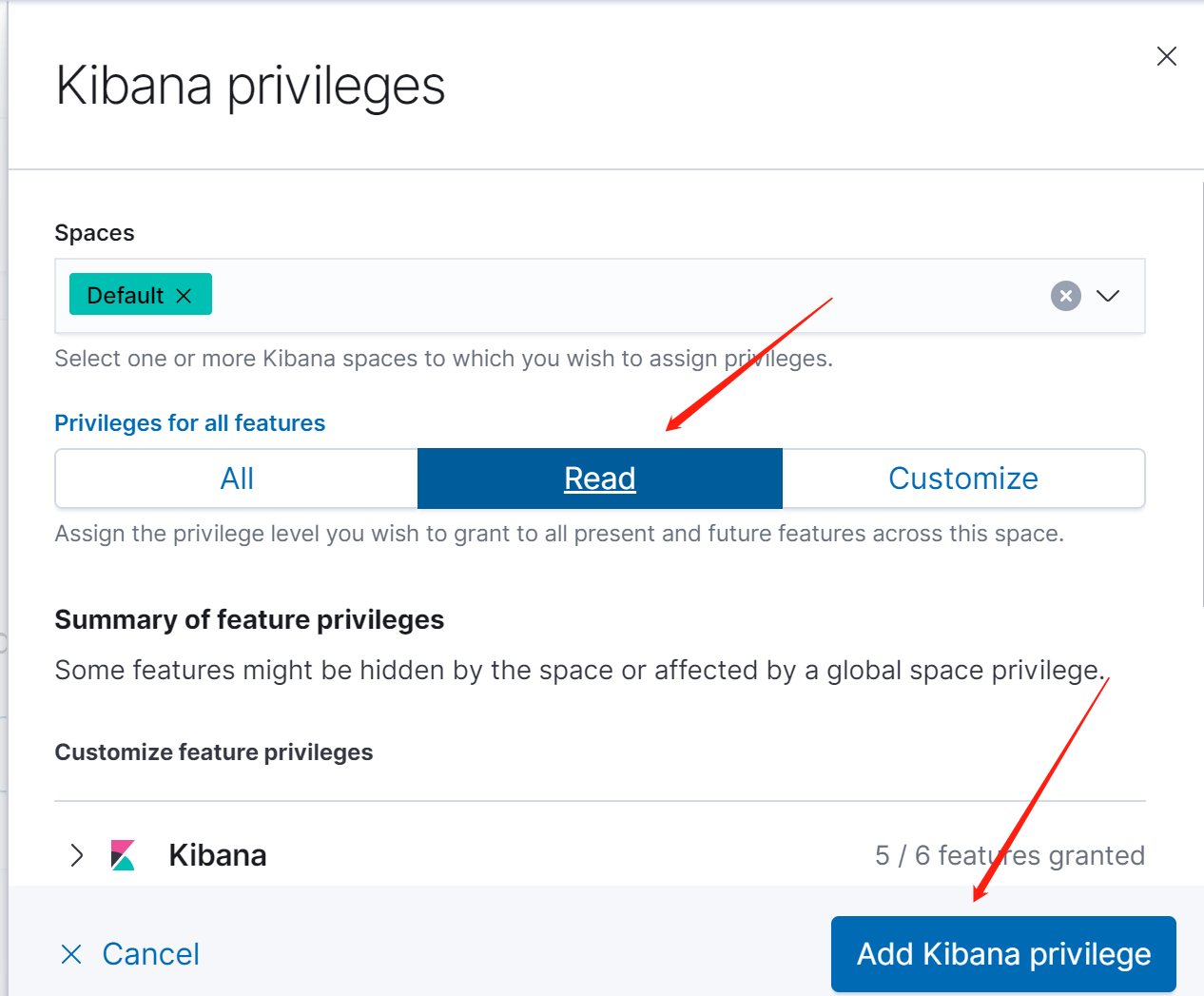
2）填写角色信息

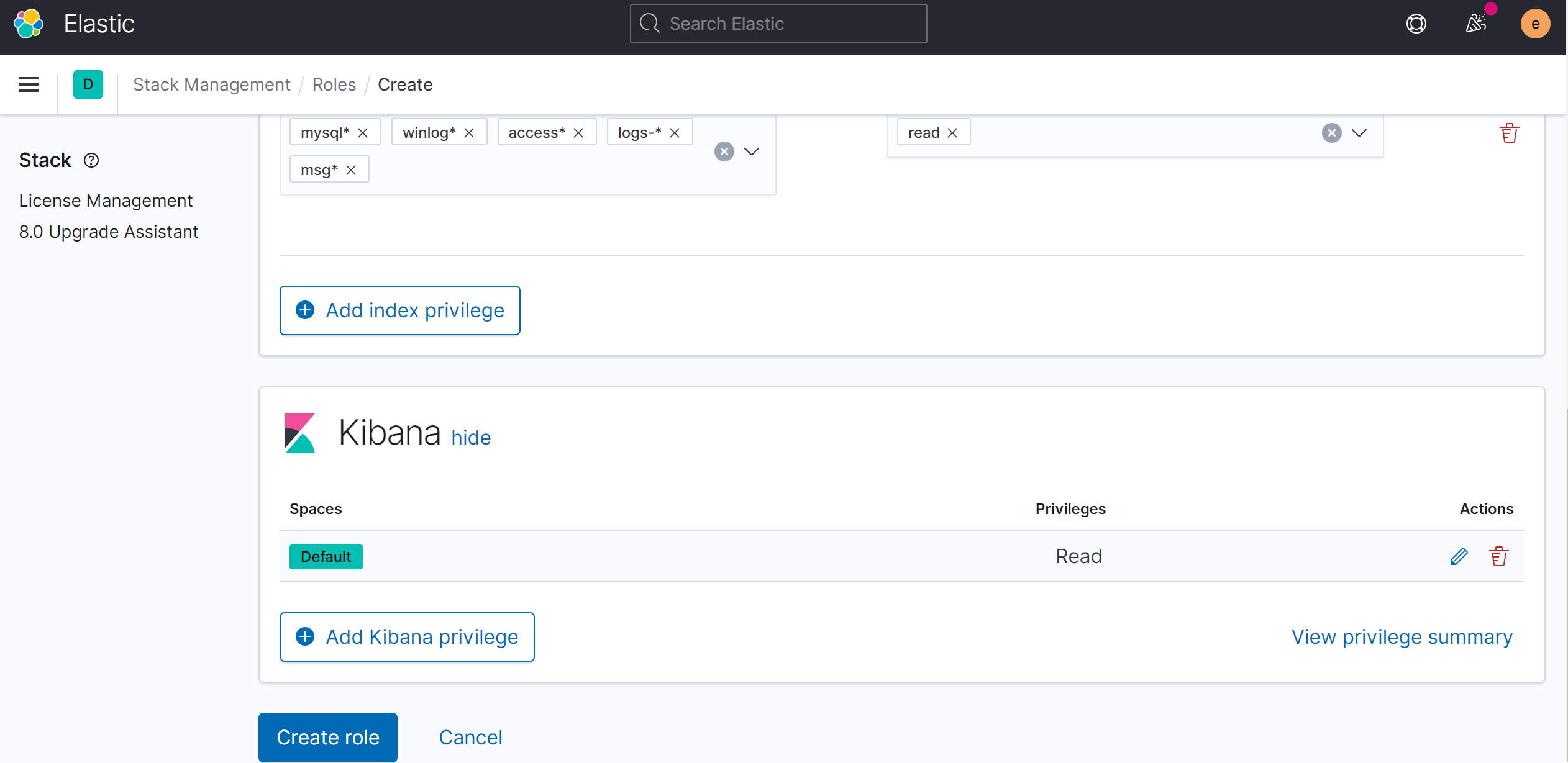


3）这里选择只读权限

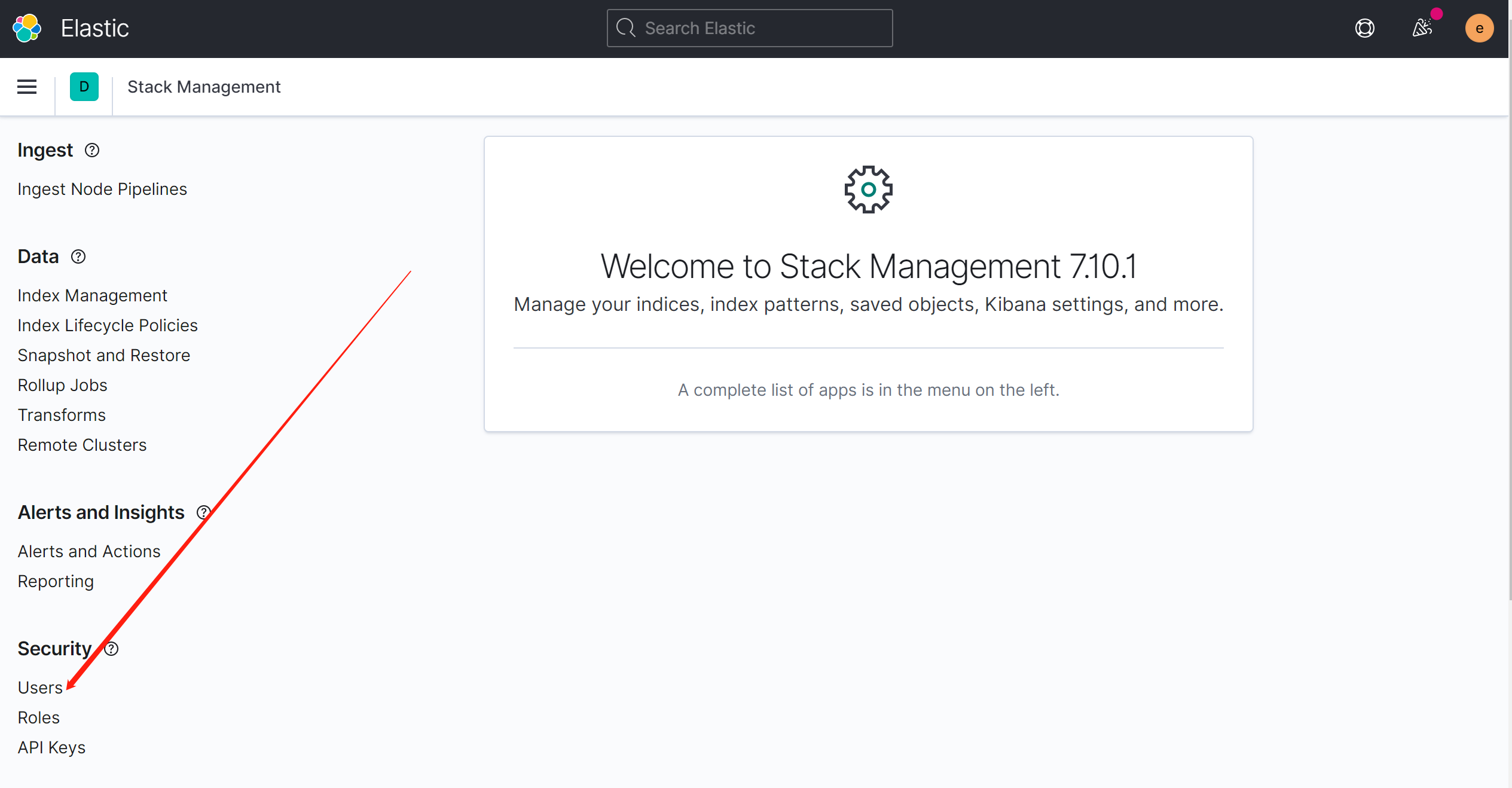


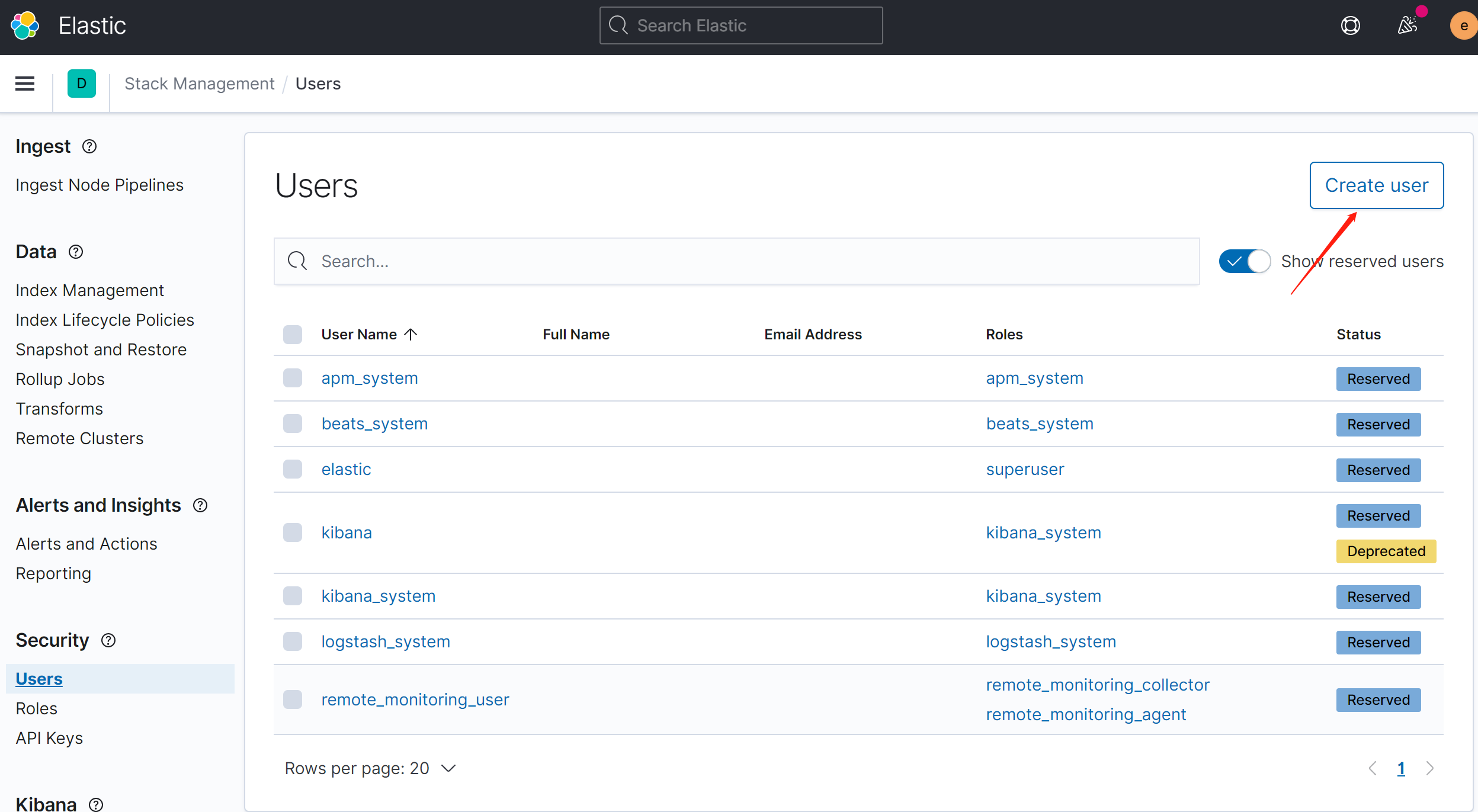
4）设置kibana权限





### 3.6.4创建只读用户





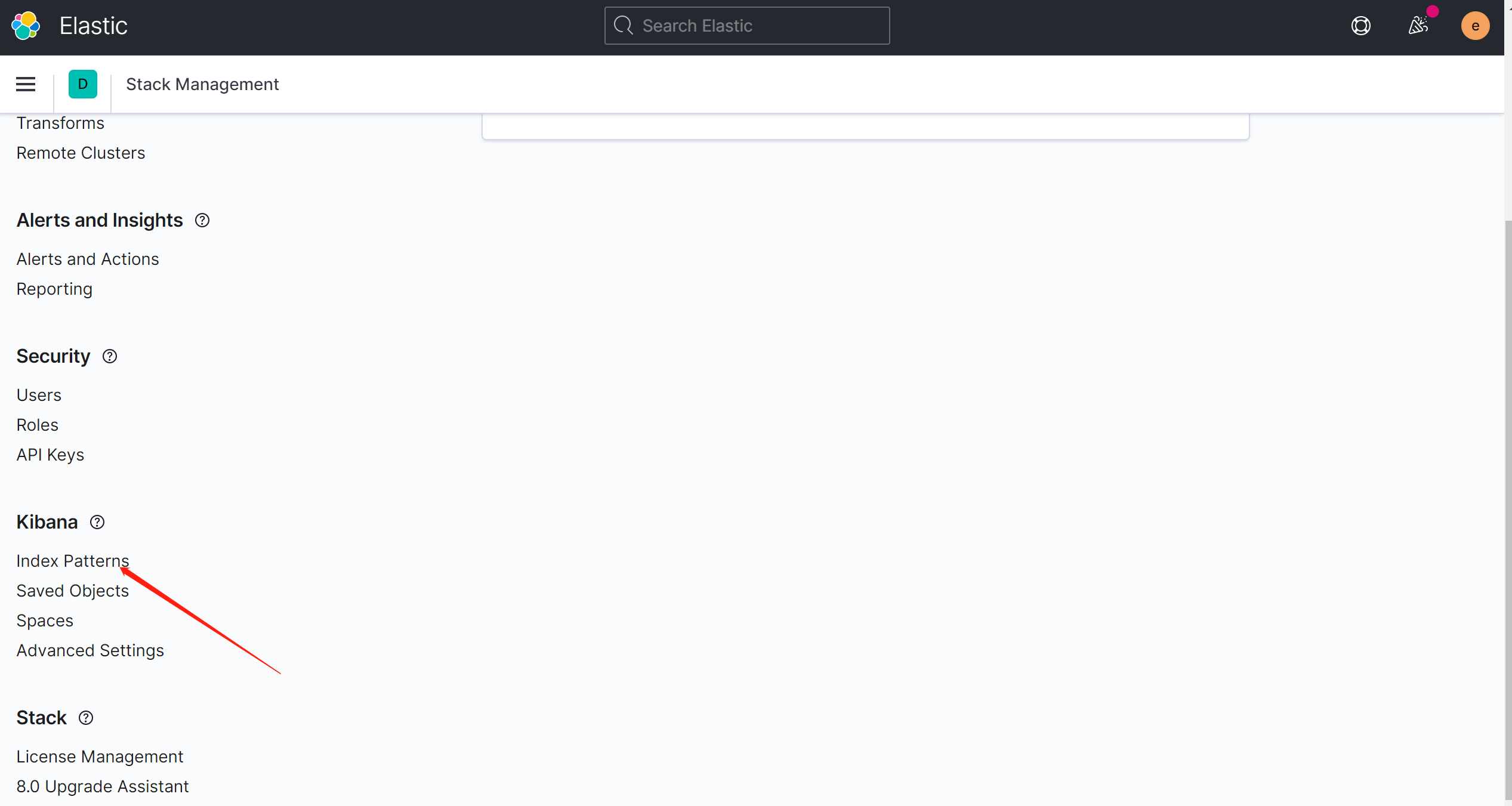
### 3.6.5填写用户信息角色



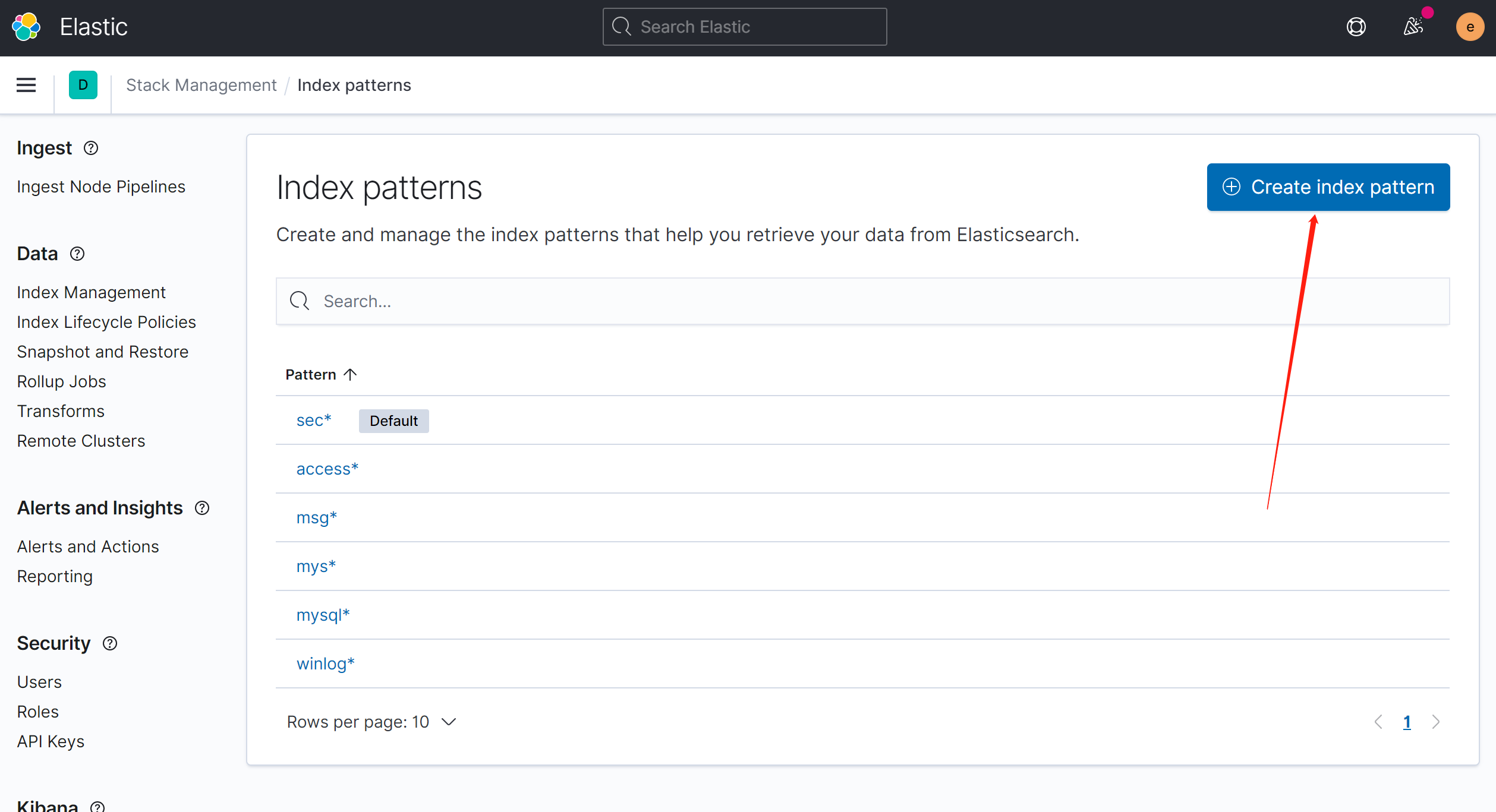


## 3.7创建索引信息

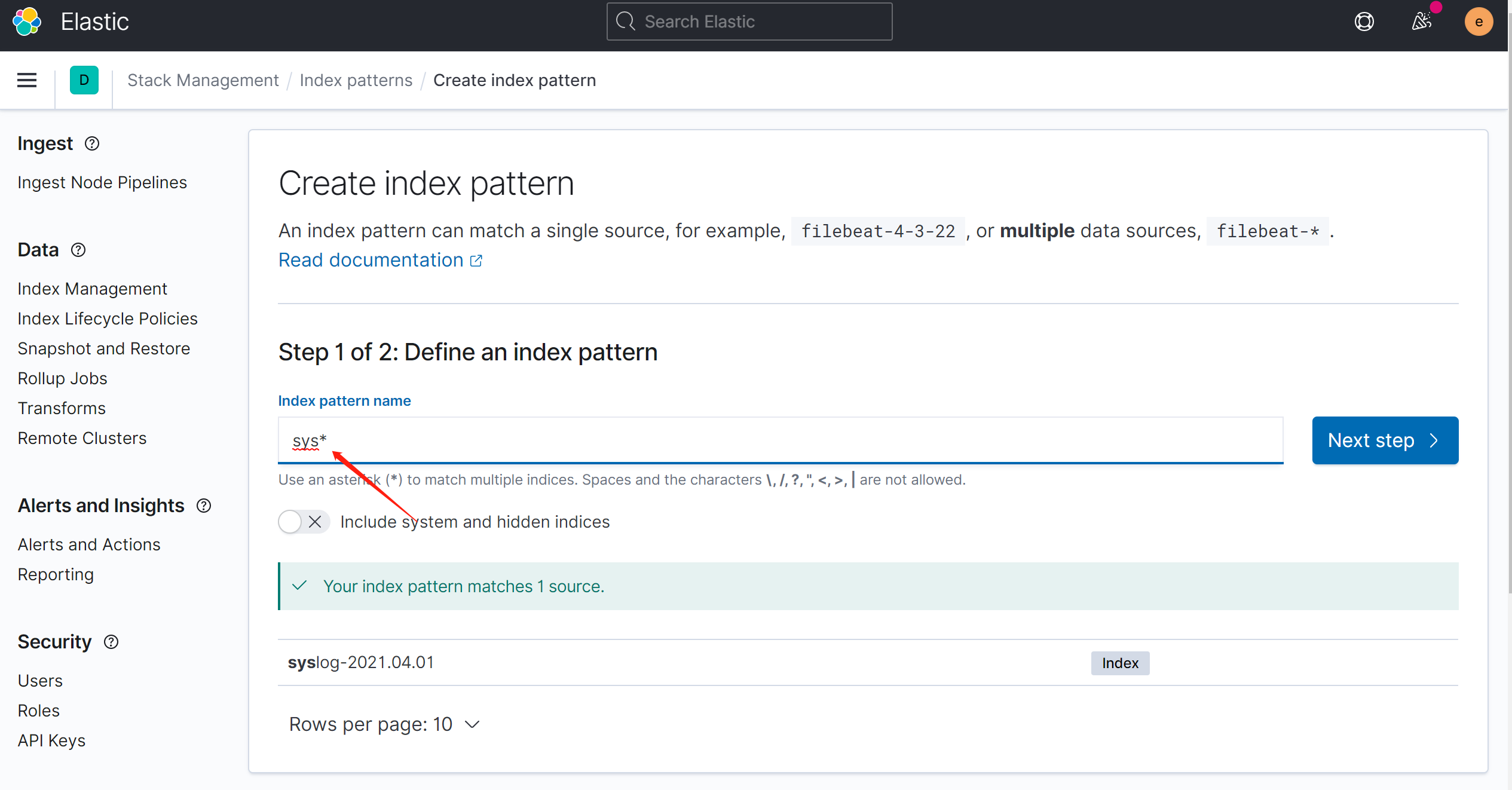
### 3.7.1选择kibana下面的index patterns

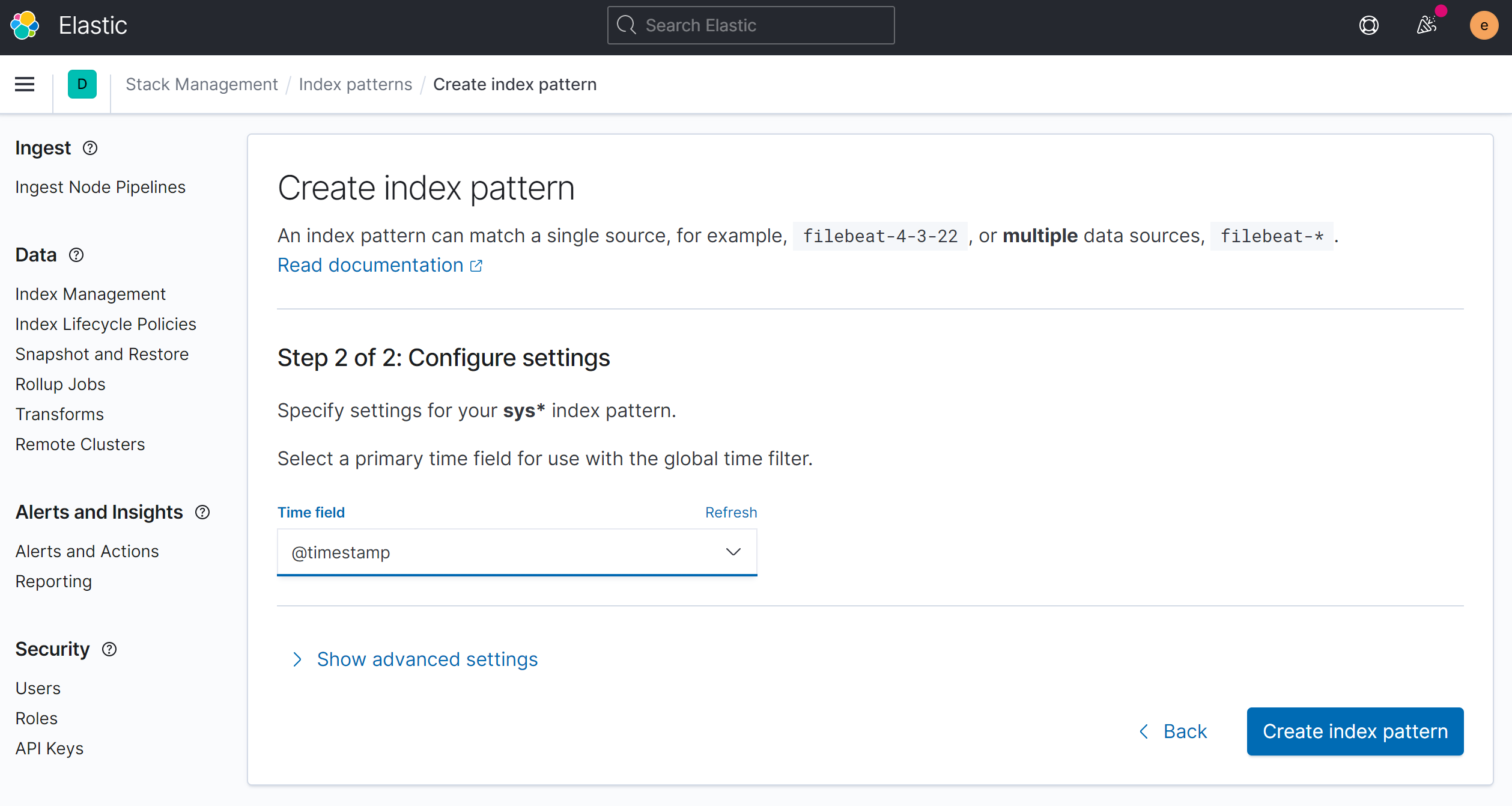


### 3.7.2创建index pattern



### 3.7.3添加index pattern name



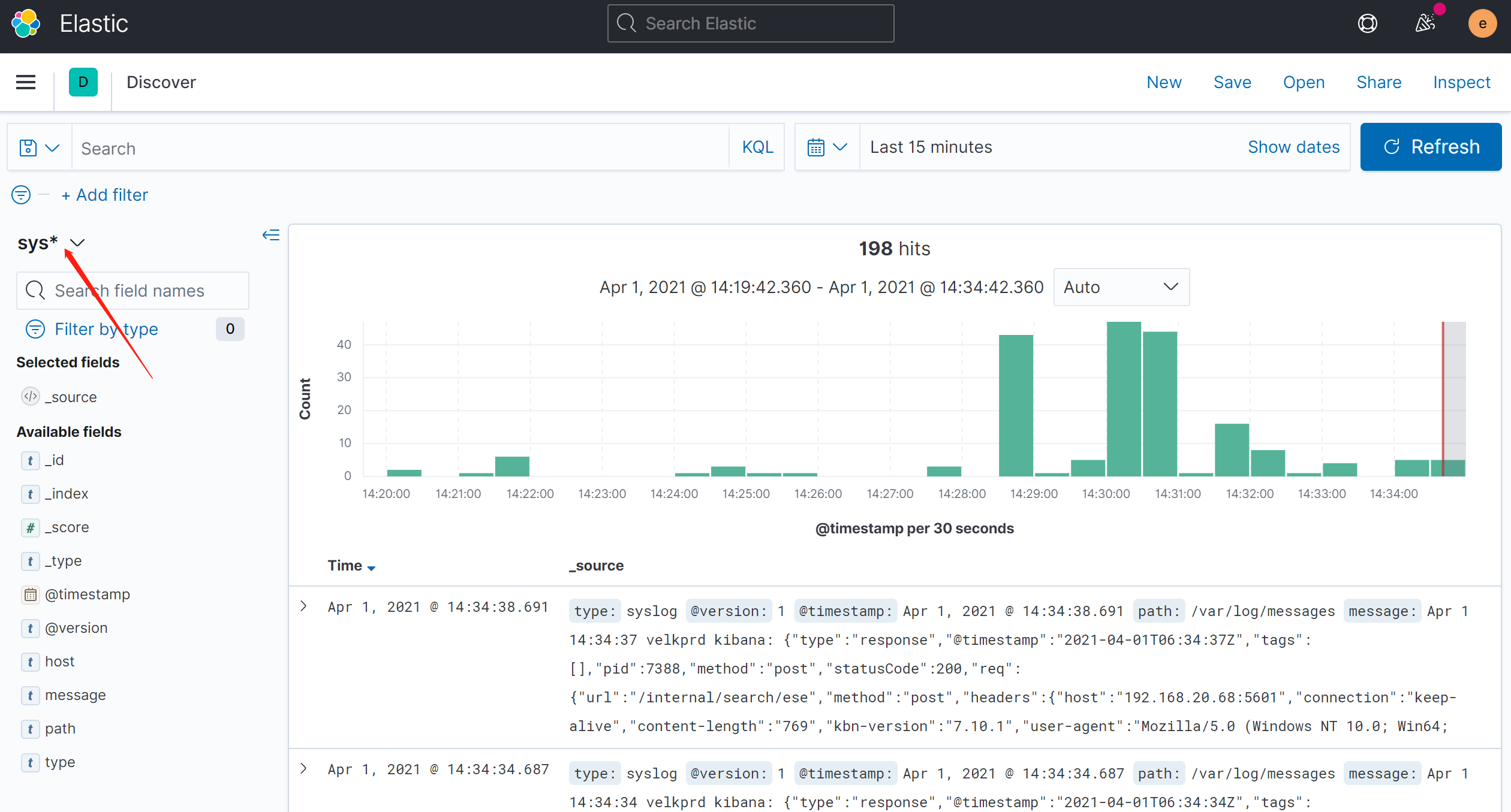


### 3.7.4查看日志





### 3.7.5选择查看日志类型



### 3.7.6定期删除索引

