**Elastic Stack**

英文地址：<https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html>

版本：6.2.2

一、安装

1、安装JDK8

<https://www.elastic.co/guide/en/elasticsearch/reference/6.2/setup.html>

2、安装es

<https://www.elastic.co/guide/en/elasticsearch/reference/6.2/install-elasticsearch.html>

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.2.tar.gz wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.2.tar.gz.sha512 sha512sum -c elasticsearch-6.2.2.tar.gz.sha512 tar -xzf elasticsearch-6.2.2.tar.gz cd elasticsearch-6.2.2/

./bin/elasticsearch

./bin/elasticsearch &    ## -d或&以后代的方式进行启动

org.elasticsearch.bootstrap.StartupException: java.lang.RuntimeException: can not run elasticsearch as root

不能用root 启动，换个用户doren，授权这个用户 es安装目录权限，重新启动

java.lang.UnsupportedOperationException: seccomp unavailable: CONFIG\_SECCOMP not compiled into kernel, CONFIG\_SECCOMP and CONFIG\_SECCOMP\_FILTER are needed

警告，关系不大

ERROR: [4] bootstrap checks failed

[1]: max file descriptors [4096] for elasticsearch process is too low, increase to at least [65536]

[2]: max number of threads [1024] for user [doren] is too low, increase to at least [4096]

[3]: max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least [262144]

[4]: system call filters failed to install; check the logs and fix your configuration or disable system call filters at your own risk

切换到root用户， (1) vi /etc/security/limits.conf 添加如下内容: \* soft nofile 65536 \* hard nofile 131072 \* soft nproc 2048 \* hard nproc 4096

(2) vi /etc/security/limits.d/90-nproc.conf 修改如下内容： \* soft nproc 1024 #修改为 \* soft nproc 4096

(3) vi /etc/sysctl.conf 添加下面配置： vm.max\_map\_count=655360 并执行命令： sysctl -p

(4)如果是 Centos6，在elasticsearch.yml中配置bootstrap.system\_call\_filter为false，注意要在Memory下面:

bootstrap.memory\_lock: false

bootstrap.system\_call\_filter: false

3、安装 kibana

<https://www.elastic.co/guide/en/kibana/6.2/targz.html>

修改配置 config目录

启动：nohup ./bin/kibana &

4、安装 logstash

<https://www.elastic.co/guide/en/logstash/6.2/index.html>

安装方式：解压

<https://www.elastic.co/guide/en/logstash/6.2/installing-logstash.html>

[目录结构：](https://www.elastic.co/guide/en/logstash/6.2/installing-logstash.html)<https://www.elastic.co/guide/en/logstash/6.2/dir-layout.html>

测试：<https://www.elastic.co/guide/en/logstash/6.2/first-event.html>

配置：<https://www.elastic.co/guide/en/logstash/6.2/config-setting-files.html>

两种配置文件；1、logstash 自身的配置文件 2、Pipeline 管道配置文件，也就是配置抓去数据的配置文件，只支持.conf 扩展名

5、Metricbeat

<https://www.elastic.co/guide/en/beats/metricbeat/6.2/index.html>

安装方式：

RPM包安装

<https://www.elastic.co/guide/en/beats/metricbeat/6.2/metricbeat-installation.html>

配置：

<https://www.elastic.co/guide/en/beats/metricbeat/6.2/metricbeat-configuration.html>

安装ES模版：

metricbeat setup

<https://www.elastic.co/guide/en/beats/metricbeat/6.2/metricbeat-template.html>

Metricbeat is a lightweight shipper for metrics.

## Getting Started

To get started with metricbeat, you need to set up Elasticsearch on your localhost first. After that, start metricbeat with:

./metricbeat -c metricbeat.yml -e

This will start the beat and send the data to your Elasticsearch instance. To load the dashboards for metricbeat into Kibana, run:

./metricbeat setup -e

For further steps visit the [Getting started](https://www.elastic.co/guide/en/beats/metricbeat/6.2/metricbeat-getting-started.html) guide.

## Documentation

Visit [Elastic.co Docs](https://www.elastic.co/guide/en/beats/metricbeat/6.2/index.html) for the full metricbeat documentation.

## Release notes

<https://www.elastic.co/guide/en/beats/libbeat/6.2/release-notes-6.2.2.html>

5、Filebeat

<https://www.elastic.co/guide/en/beats/filebeat/current/index.html>

安装方式：

RPM包安装 <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation.html>

[主配置文件配置](https://www.elastic.co/guide/en/beats/filebeat/current/configuration-filebeat-options.html" \l "config-json)：

[https://www.elastic.co/guide/en/beats/filebeat/current/configuration-filebeat-options.html#config-json](https://www.elastic.co/guide/en/beats/filebeat/current/configuration-filebeat-options.html" \l "config-json)

支持json格式日志配置：

json.keys\_under\_root: true

json.add\_error\_key: true

json.message\_key: log

安装ES模版：

filebeat setup

<https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-template.html>

Parse logs by using ingest node，ES格式化数据配置：

<https://www.elastic.co/guide/en/beats/filebeat/current/configuring-ingest-node.html>