ELK 日志平台

1. 功能描述

什么使 ELK?

ELK 实际上是三个工具的集合，Elasticsearch + Logstash + Kibana，这三个工具组合形成了一套 实用、易用的监控架构，很多公司利用它来搭建可视化的海量日志分析平台。

a. ElasticSearch

ElasticSearch 是一个基于 Lucene 的搜索服务器。它提供了一个分布式多用户能力的全文搜索引 擎，基于 RESTful web 接口。Elasticsearch 是用 Java 开发的，并作为 Apache 许可条款下的开放源码 发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快 速，安装使用方便。

b. Logstash

Logstash 是一个用于管理日志和事件的工具，你可以用它去收集日志、转换日志、解析日志并将 他们作为数据提供给其它模块调用，例如搜索、存储等。

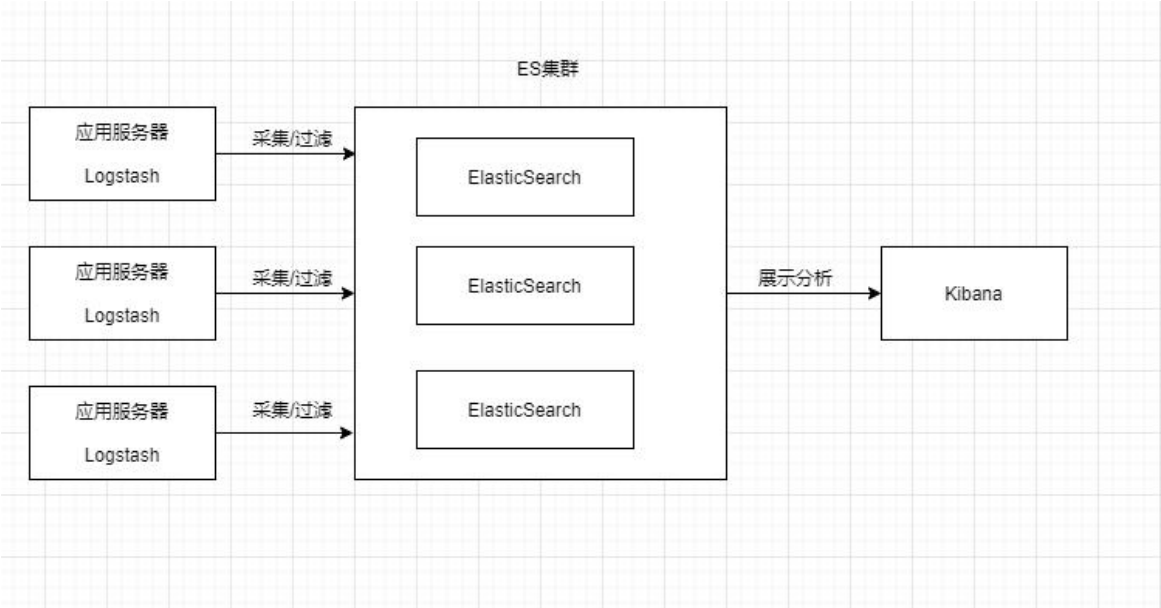
c. Kibana

Kibana 是一个优秀的前端日志展示框架，它可以非常详细的将日志转化为各种图表，为用户提供 强大的数据可视化支持。

为什么要使用 ELK?

目前系统大都采用分布式微服务架构，服务集群部署，这样就会产生很多日志文件，如果每次查问题都是登录到各个服务器看日志文件，是非常困难的。因此需要有统一收集日志的工具，来帮我们收集查看日志。ELK 可以让快速准确的定位问题。提高效率。

2. ELK 架构图



3. ES 安装

a.导入密钥

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

```
[root@teacher3 ~]# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
[root@teacher3 ~]#
```

b.创建 es 仓库

vim /etc/yum.repos.d/elasticsearch.repo

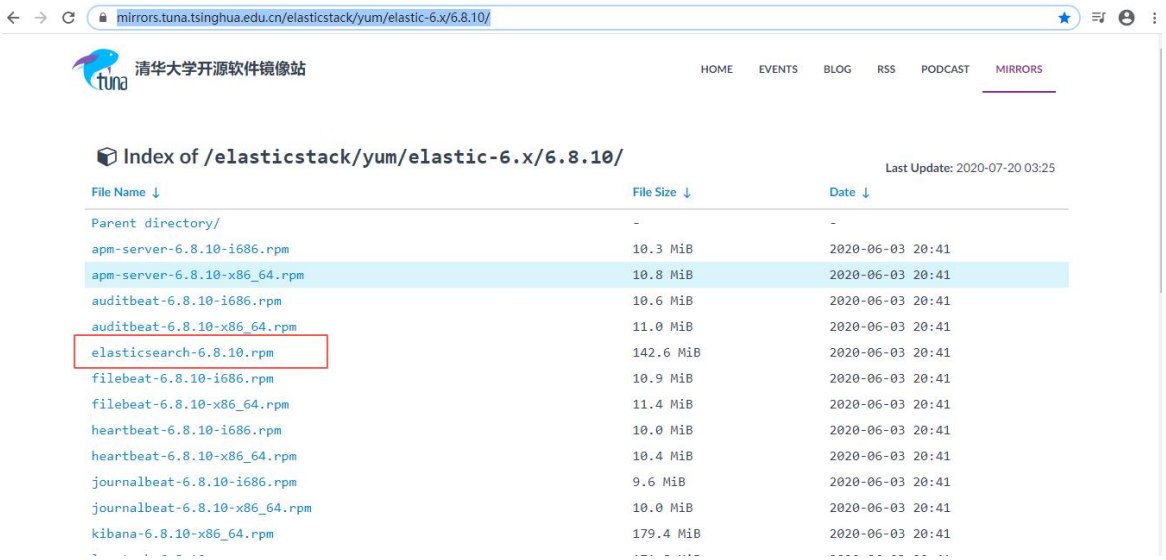
1. [elasticsearch-6.x]
2. name=Elasticsearch repository for 6.x packages
3. baseurl=https://artifacts.elastic.co/packages/6.x/yum
4. gpgcheck=1
5. gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
6. enabled=1
7. autorefresh=1
8. type=rpm-md

```
[root@teacher3 ~]# vim /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
~
~
~
~
~
~
~
```

c.下载 ES 安装包

1. 地址：https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/



1. wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/elasticsearch-6.8.10.rpm

```
[root@teacher3 elk]# wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/elasticsearch-6.8.10.rpm
--2020-07-20 14:28:00--  https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/elasticsearch-6.8.10.rpm
Resolving mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)... 101.6.8.193, 2402:f000:1:408:8100::1
Connecting to mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)|101.6.8.193|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 149520716 (143M) [application/x-redhat-package-manager]
Saving to: 'elasticsearch-6.8.10.rpm'

100%[===================================================================================================================================>] 149,520,716 4.51MB/s   in 29s

2020-07-20 14:28:31 (4.83 MB/s) - 'elasticsearch-6.8.10.rpm' saved [149520716/149520716]
```

```
[root@teacher3 elk]# wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/filebeat-6.8.10-x86_64.rpm
--2020-07-20 14:39:56--  https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/filebeat-6.8.10-x86_64.rpm
Resolving mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)... 101.6.8.193, 2402:f000:1:408:8100::1
Connecting to mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)|101.6.8.193|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11901537 (11M) [application/x-redhat-package-manager]
Saving to: ‘filebeat-6.8.10-x86_64.rpm’

100%[===================================================================================================================================>] 11,901,537  1.63MB/s   in 13s

2020-07-20 14:40:09 (917 KB/s) - ‘filebeat-6.8.10-x86_64.rpm’ saved [11901537/11901537]
```

d.安装 es

1. rpm -ivh elasticsearch-6.8.10.rpm

```
[root@teacher3 elk]# rpm -ivh elasticsearch-6.8.10.rpm
Preparing...                          ################################# [100%]
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Updating / installing...
   1:elasticsearch-0:6.8.10-1         ################################# [100%]
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch
```

e.修改 es 配置

1. vim /etc/elasticsearch/elasticsearch.yml

```
#
# ---------------------------------- Memory -----------------------------------
#
# Lock the memory on startup:
#
#bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ---------------------------------- Network -----------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: localhost
#
# Set a custom port for HTTP:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when new node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.zen.ping.unicast.hosts: ["host1", "host2"]
#
# Prevent the "split brain" by configuring the majority of nodes (total number of master-eligible nodes / 2 + 1):
#
-- INSERT --
```

注：打开 network.host 改为 localhost; 打开 http.port

f.启动 es

1. systemctl start elasticsearch

```
[root@teacher3 elk]# systemctl start elasticsearch
[root@teacher3 elk]#
```

1. systemctl status elasticsearch

查看 es 启动状态

```
[root@teacher3 elk]# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Mon 2020-07-20 14:57:49 CST; 13min ago
     Docs: http://www.elastic.co
  Process: 34872 ExecStart=/usr/share/elasticsearch/bin/elasticsearch -p ${PID_DIR}/elasticsearch.pid --quiet (code=exited, status=1/FAILURE)
 Main PID: 34872 (code=exited, status=1/FAILURE)

Jul 20 14:57:49 teacher3 systemd[1]: Started Elasticsearch.
Jul 20 14:57:49 teacher3 elasticsearch[34872]: which: no java in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin)
Jul 20 14:57:49 teacher3 elasticsearch[34872]: warning: Falling back to java on path. This behavior is deprecated. Specify JAVA_HOME
Jul 20 14:57:49 teacher3 elasticsearch[34872]: could not find java; set JAVA_HOME
Jul 20 14:57:49 teacher3 systemd[1]: elasticsearch.service: main process exited, code=exited, status=1/FAILURE
Jul 20 14:57:49 teacher3 systemd[1]: Unit elasticsearch.service entered failed state.
Jul 20 14:57:49 teacher3 systemd[1]: elasticsearch.service failed.
```

如果看到这些信息，证明启动失败

解决方案：

在/etc/sysconfig/elasticsearch 的这个文件里面设置 JAVA_HOME 环境变量：

```
################################
# Elasticsearch
################################

# Elasticsearch home directory
#ES_HOME=/usr/share/elasticsearch

# Elasticsearch Java path
JAVA_HOME=/opt/module/jdk1.8.0_231

# Elasticsearch configuration directory
ES_PATH_CONF=/etc/elasticsearch

# Elasticsearch PID directory
#PID_DIR=/var/run/elasticsearch

# Additional Java OPTS
#ES_JAVA_OPTS=

# Configure restart on package upgrade (true, every other setting will lead to not restarting)
#RESTART_ON_UPGRADE=true

################################
# Elasticsearch service
################################

# SysV init.d
#
# The number of seconds to wait before checking if Elasticsearch started successfully as a daemon process
ES_STARTUP_SLEEP_TIME=5
```

再次执行

1. systemctl start elasticsearch

再查看状态

1. systemctl status elasticsearch

```
[root@teacher3 elk]# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-07-20 15:11:04 CST; 2s ago
     Docs: http://www.elastic.co
 Main PID: 35762 (java)
   CGroup: /system.slice/elasticsearch.service
           ├─35762 /opt/module/jdk1.8.0_231/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Des.networkaddress.cach...
           └─35859 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jul 20 15:11:04 teacher3 systemd[1]: Started Elasticsearch.
```

提示这些信息 证明 es 服务启动成功。

g.验证 es 服务

1. curl -X GET "localhost:9200"

```
[root@teacher3 elk]# curl -X GET "localhost:9200"
{
  "name" : "v-UIfxi",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "M4nZs5u_TNGI4Z5PClsyLw",
  "version" : {
    "number" : "6.8.10",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "537cb22",
    "build_date" : "2020-05-28T14:47:19.882936Z",
    "build_snapshot" : false,
    "lucene_version" : "7.7.3",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
[root@teacher3 elk]#
```

看到这些信息 证明 es 服务可用。

4. Logstash 安装

a. 下载 Logstash 安装包

1. wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/logstash-6.8.10.rpm

```
[root@teacher3 elk]# wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/logstash-6.8.10.rpm
--2020-07-20 14:36:24--  https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/logstash-6.8.10.rpm
Resolving mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)... 101.6.8.193, 2402:f000:1:408:8100::1
Connecting to mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)|101.6.8.193|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 180162293 (172M) [application/x-redhat-package-manager]
Saving to: ‘logstash-6.8.10.rpm’

100%[===================================================================================================================================>] 180,162,293 5.37MB/s   in 53s

2020-07-20 14:37:17 (3.24 MB/s) - ‘logstash-6.8.10.rpm’ saved [180162293/180162293]
```

b.安装 logstash

1. rpm -ivh logstash-6.8.10.rpm

```
[root@teacher3 elk]# rpm -ivh logstash-6.8.10.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:logstash-1:6.8.10-1              ################################# [100%]
Using provided startup.options file: /etc/logstash/startup.options
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.30/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
```

c.添加 logstash 配置文件

1. vim /etc/logstash/conf.d/edu-front-boot.conf

```
1. input {
2.    # 从文件读取日志信息 输送到控制台
3.    file {
4.        path => "/data/logs/edu-front-boot/edu-front-boot.log.2020-07-20.0.log"
5.        codec => "json" ## 以 JSON 格式读取日志
6.        type => "edu-front-boot"
7.        start_position => "beginning"
8.    }
9. }
10.
```

```
# filter {
#
# }

output {
    # 标准输出
    # stdout {}
    # 输出进行格式化，采用 Ruby 库来解析日志
     stdout { codec => rubydebug }
    if [type] == "edu-front-boot"{
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "edu-front-boot-%{+YYYY.MM.dd}"
            }
     }
}
```

```
[root@teacher3 elk]# vim /etc/logstash/conf.d/edu-front-boot.conf

input {
    # 从文件读取日志信息 输送到控制台
    file {
        path => "/data/logs/edu-front-boot/edu-front-boot.log.2020-07-20.0.log"
        codec => "json" ## 以JSON格式读取日志
        type => "edu-front-boot"
        start_position => "beginning"
    }
}

# filter {
#
# }

output {
    # 标准输出
    # stdout {}
    # 输出进行格式化，采用Ruby库来解析日志
     stdout { codec => rubydebug }
    if [type] == "edu-front-boot"{
        elasticsearch {
                        hosts => ["localhost:9200"]
                        index => "edu-front-boot-%{+YYYY.MM.dd}"
        }
     }
}
~
```

d.启动 logstash 服务

首先进入/usr/share/logstash/bin

```
./logstash -f /etc/logstash/conf.d/
```

```
          "path" => "/data/logs/edu-front-boot/edu-front-boot.log.2020-07-20.0.log",
       "message" => "2020-07-20 15:43:22.213 [http-nio-8081-exec-4] INFO  com.lagou.edu.front.interceptor.GlobalInterceptor:31 - url:/user/getInfo, get userId:100030016, userName:15510792995
from header",
          "host" => "teacher3",
      "@version" => "1",
          "type" => "edu-front-boot",
    "@timestamp" => 2020-07-20T07:44:56.392Z
}
{
          "tags" => [
        [0] "_jsonparsefailure"
    ],
          "path" => "/data/logs/edu-front-boot/edu-front-boot.log.2020-07-20.0.log",
       "message" => "2020-07-20 15:43:22.648 [http-nio-8081-exec-5] INFO  com.lagou.edu.front.interceptor.GlobalInterceptor:31 - url:/user/refresh_token, get userId:100030016, userName:15510
92995 from header",
          "host" => "teacher3",
      "@version" => "1",
          "type" => "edu-front-boot",
    "@timestamp" => 2020-07-20T07:44:56.395Z
}
{
          "tags" => [
        [0] "_jsonparsefailure"
    ],
          "path" => "/data/logs/edu-front-boot/edu-front-boot.log.2020-07-20.0.log",
       "message" => "2020-07-20 15:43:22.654 [hystrix-edu-oauth-boot-10] ERROR c.l.e.f.u.service.impl.OAuthRemoteServiceFallback:19 - refreshToken[eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2
yX2lkIjoiMTAwMDMwMDE2IiwidXNlcl9uYWllIjoiMTU1MTA3OTI5OTUiLCJzY29wZSI6WyJyZWFkIl0sIm9yZ2FuaXphdGlvbiI6IjE1NTEwNzkyOTk1IiwiYXRpIjoiaiIwenJpUEwxYWNlQjc3MHk2dnZpZkdCZGZZIiwiZXhwIjoxNTk1MzM4ODM5L
JhdXRob3JpdGllcyI6WyJDT1VSU0VfTUFOQUdFUiIsIkFVVEhPUklUWV9NQU5BR0VSIiwiQUFNSU4iXSwianRpIjoiNl9RdXcydEFmelFFNlRNb3dLSXBhSWt5aji4IiwiY2xpZW50X2lkIjoidGVzdF9jbGllbnQifQ.hjWCNpmsh7tZxWEZOkPhYgxBc
GyYmcBqq4LpxDFIqA],刷新access_token发生异常",
          "host" => "teacher3",
      "@version" => "1",
          "type" => "edu-front-boot",
    "@timestamp" => 2020-07-20T07:44:56.396Z
}
```

查看启动服务

1. ps -ef | grep logstash

```
[root@teacher3 sysconfig]# ps -ef | grep logstash
root     38177 30316 75 15:44 pts/1    00:01:36 /opt/module/jdk1.8.0_231/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnl
y -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -Djruby.jit.threshold=0 -Djruby.regexp.interruptible=true -XX:+HeapDumpOnOutOfMemoryError -Djava.security.e
gd=file:/dev/urandom -cp /usr/share/logstash/logstash-core/lib/jars/animal-sniffer-annotations-1.14.jar:/usr/share/logstash/logstash-core/lib/jars/commons-codec-1.11.jar:/usr/share/logstash/l
ogstash-core/lib/jars/commons-compiler-3.0.8.jar:/usr/share/logstash/logstash-core/lib/jars/error_prone_annotations-2.0.18.jar:/usr/share/logstash/logstash-core/lib/jars/google-java-format-1.
1.jar:/usr/share/logstash/logstash-core/lib/jars/gradle-license-report-0.7.1.jar:/usr/share/logstash/logstash-core/lib/jars/guava-22.0.jar:/usr/share/logstash/logstash-core/lib/jars/j2objc-an
notations-1.1.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-annotations-2.9.10.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-core-2.9.10.jar:/usr/share/logstash/logstash-cor
e/lib/jars/jackson-databind-2.9.10.1.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-dataformat-cbor-2.9.10.jar:/usr/share/logstash/logstash-core/lib/jars/janino-3.0.8.jar:/usr/share/l
ogstash/logstash-core/lib/jars/javassist-3.22.0-GA.jar:/usr/share/logstash/logstash-core/lib/jars/jruby-complete-9.2.7.0.jar:/usr/share/logstash/logstash-core/lib/jars/jsr305-1.3.9.jar:/usr/s
hare/logstash/logstash-core/lib/jars/log4j-api-2.9.1.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-core-2.9.1.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-slf4j-impl-2.9.1.jar:
/usr/share/logstash/logstash-core/lib/jars/logstash-core.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.commands-3.6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.ecli
pse.core.contenttype-3.4.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.expressions-3.4.300.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.filesystem-1.3
.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.jobs-3.5.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.resources-3.7.100.jar:/usr/share/logstash/log
stash-core/lib/jars/org.eclipse.core.runtime-3.7.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.app-1.3.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.eq
uinox.common-3.6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.preferences-3.4.1.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.registry-3.5.101.jar
:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.jdt.core-3.10.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.osgi-3.7.1.jar:/usr/share/logstash/logstash-core/lib/jars/or
g.eclipse.text-3.5.101.jar:/usr/share/logstash/logstash-core/lib/jars/slf4j-api-1.7.25.jar org.logstash.Logstash -f /etc/logstash/conf.d/
root     38373 34309  0 15:46 pts/2    00:00:00 grep --color=auto logstash
```

看到这些信息 证明启动成功

5. Kibana 安装

a.下载 Kibana 安装包

1. wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/kibana-6.8.10-x86_64.rpm

```
[root@teacher3 elk]# wget https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/kibana-6.8.10-x86_64.rpm
--2020-07-20 14:37:39--  https://mirrors.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-6.x/6.8.10/kibana-6.8.10-x86_64.rpm
Resolving mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)... 101.6.8.193, 2402:f000:1:408:8100::1
Connecting to mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)|101.6.8.193|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 188138485 (179M) [application/x-redhat-package-manager]
Saving to: ‘kibana-6.8.10-x86_64.rpm’

100%[===================================================================================================================================>] 188,138,485 6.79MB/s   in 35s

2020-07-20 14:38:14 (5.15 MB/s) - ‘kibana-6.8.10-x86_64.rpm’ saved [188138485/188138485]
```

b.安装 Kibana

1. rpm -ivh kibana-6.8.10-x86_64.rpm

```
[root@teacher3 elk]# rpm -ivh kibana-6.8.10-x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:kibana-6.8.10-1                  ################################# [100%]
```

c.修改 Kibana 配置文件

1. vim /etc/kibana/kibana.yml

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
#elasticsearch.preserveHost: true
```

注：打开 server.port ；打开 server.host

d.启动 Kibana

1. systemctl start kibana

```
[root@teacher3 elk]# systemctl start kibana
```

查看启动状态

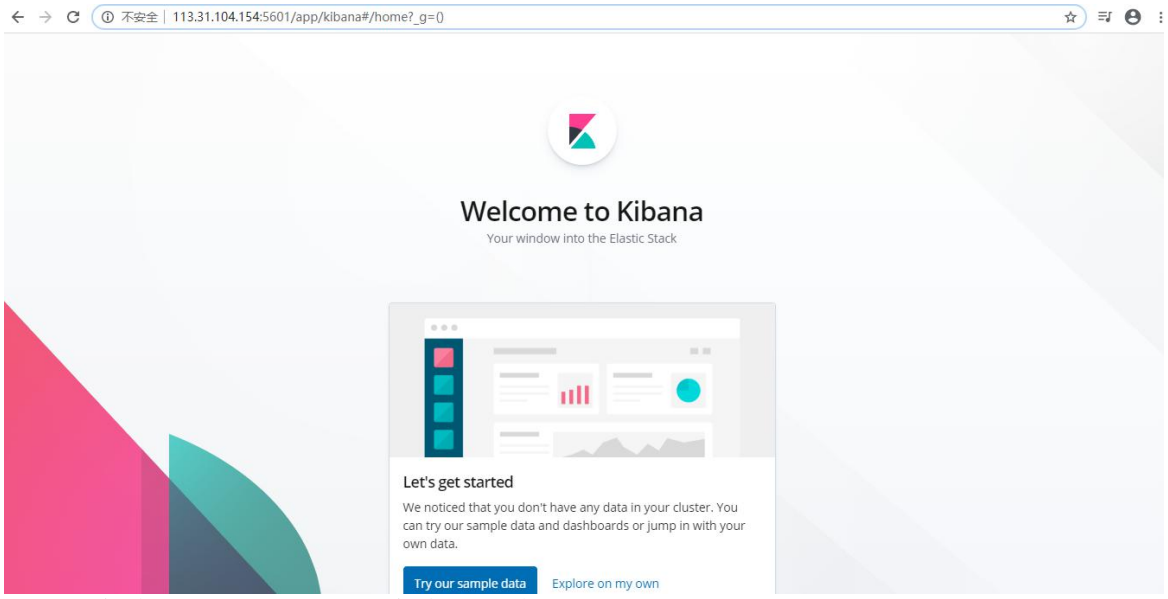
1. systemctl status kibana

```
[root@teacher3 elk]# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2020-07-20 15:27:37 CST; 15s ago
 Main PID: 36855 (node)
   CGroup: /system.slice/kibana.service
           └─36855 /usr/share/kibana/bin/../node/bin/node --no-warnings --max-http-header-size=65536 /usr/share/kibana/bin/../src/cli -c /etc/kibana/kibana.yml

Jul 20 15:27:37 teacher3 systemd[1]: Started Kibana.
```

看到这些信息 证明启动成功

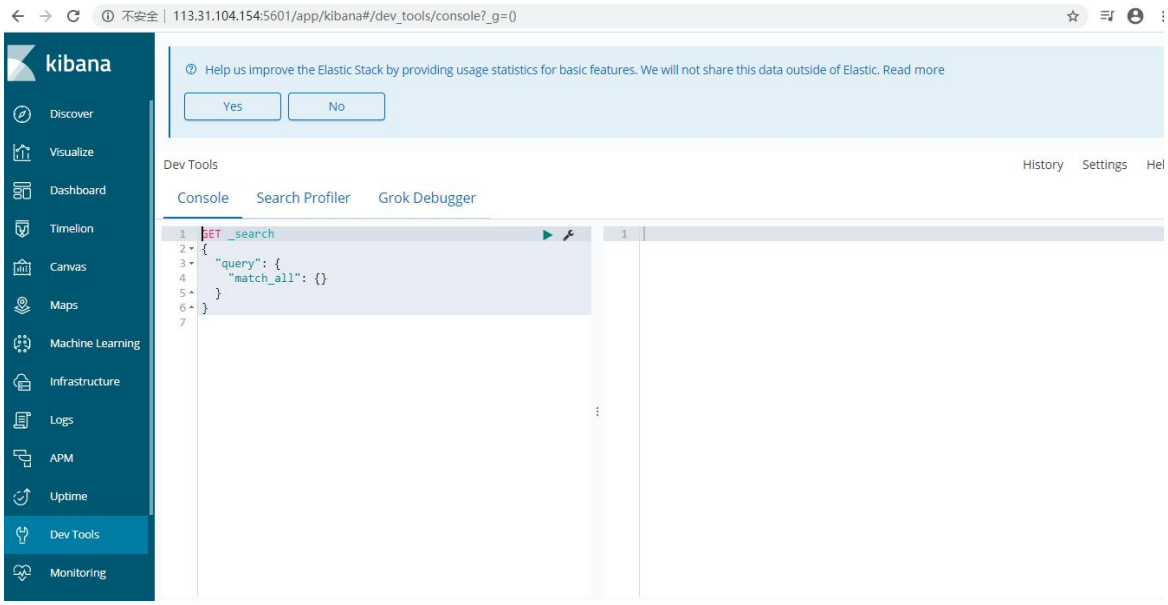
e.浏览器访问 http://113.31.104.154:5601/验证下服务



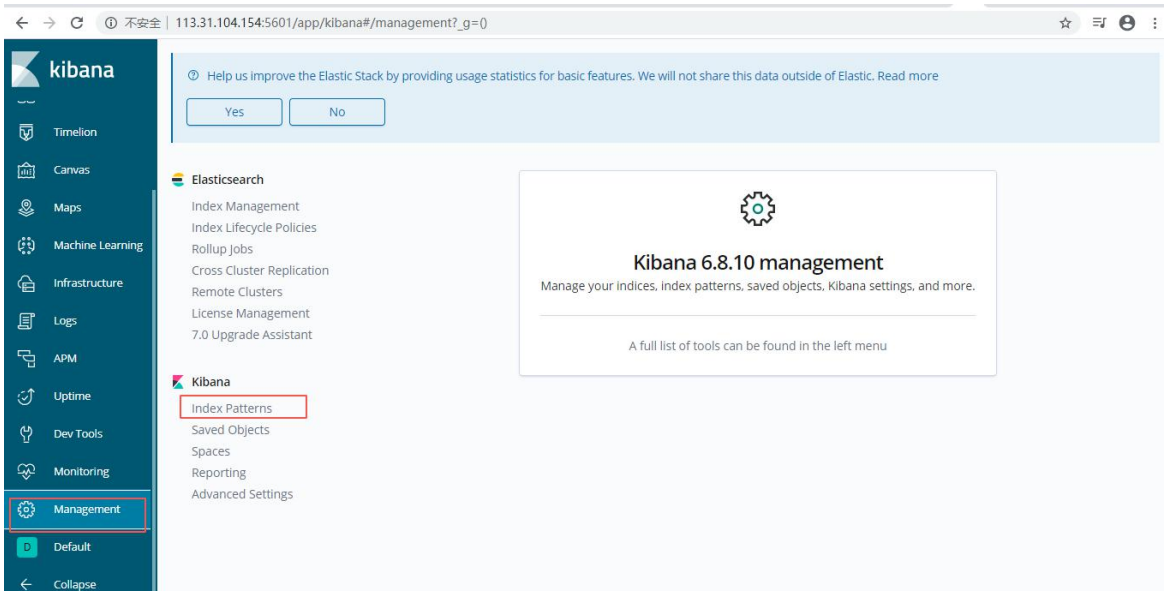
看到这个效果，证明 kibana 服务启动成功

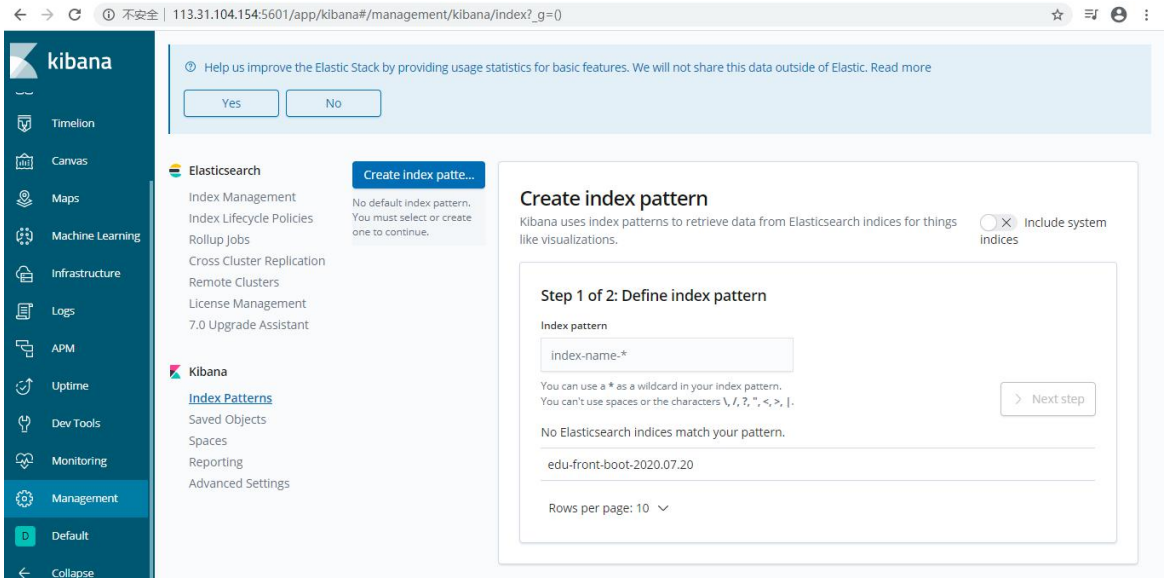
f.在 Kibana 中创建索引

点击 try our sample data 进入控制台

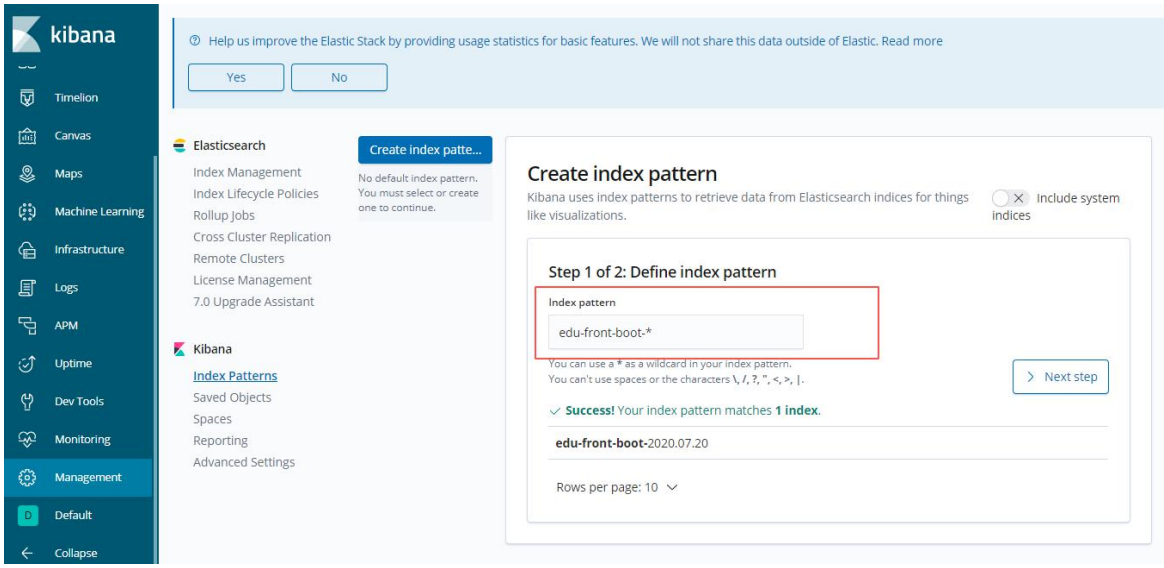


点击 Management -> index Patterns

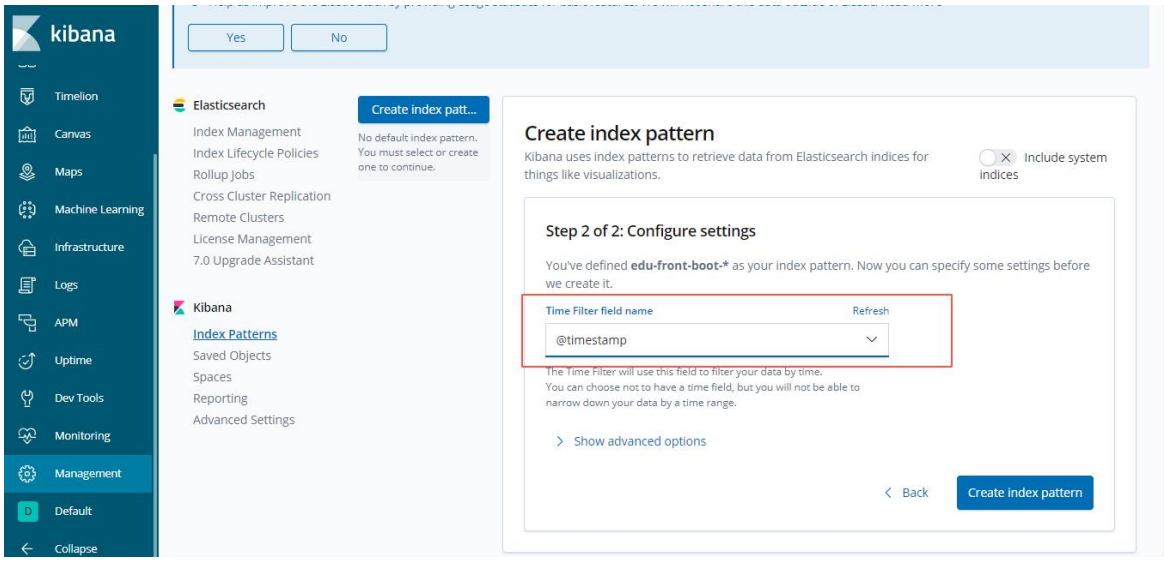




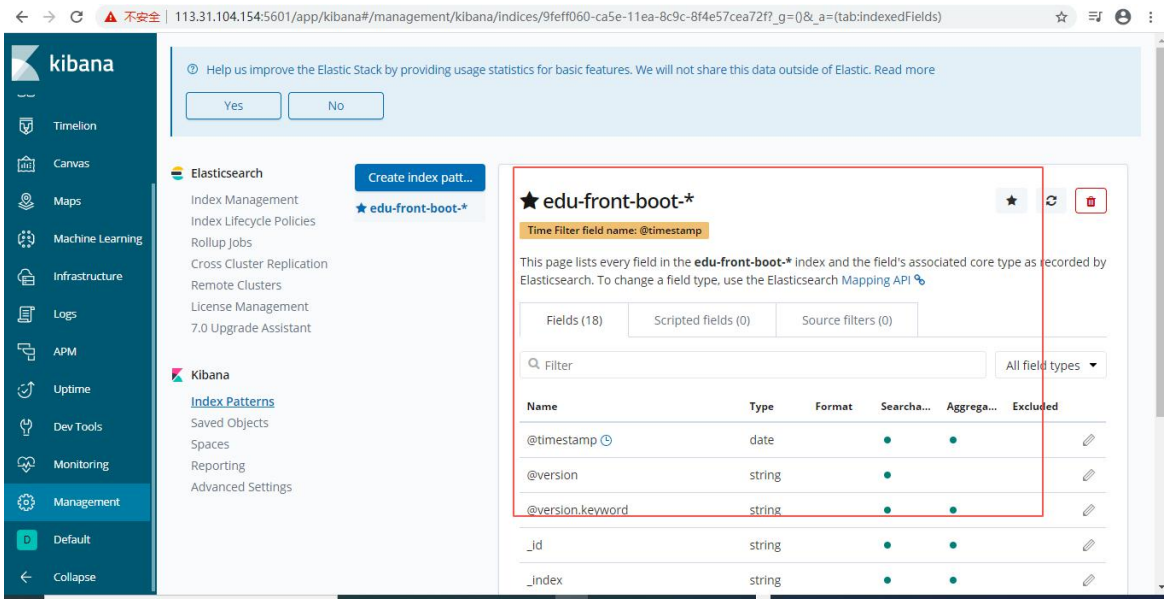
填写索引名称，点击 Next step



选择@timestamp,点击 Create index pattern



创建成功



点击 Discover 可以看到采集的日志信息