# ELK介绍

## 官网地址

<https://www.elastic.co/cn/elastic-stack>

## 为什么需要收集日志

在项目开发和测试过程中，日志是定位问题的重要依据

通过日志级别进行分级管理，debug,info,warn,error等

日志格式化，通过格式化提高日志可读性，常用日志格式：时间，日志级别，类与方法，线程名，日志内容

## 什么是ELK

ELK是指Elasticsearch、Logstash、Kibana，加上Beats也称为ELK Stack。

能够安全可靠的获取任务来源、任何格式的数据，然后实时的对数据进行搜索、分析和可视化

Elasticsearch：是一个分布式搜索和分析引擎，存储数据索引、并提供搜索和分析

Kibana：基于可视化界面访问ES数据索引，分析数据及数据可视化

Beats：从数据源中获取数据并存储到ES，也可以上传到Logstash，经过Logstash格式式化再存储到ES，我们日志收集主要是采集日志文件，所以Beats选用FileBeat

Logstash：负责收集数据，处理数据，上传数据（支持codec）

Input=>decode=>filter=>encode=>output

## ELK日志系统图示

Filebeat

Filebeat

Filebeat

Logstash

ES集群

Kibana

从服务器上收集日志数据

收集filebeat的数据过滤格式化上传到ES

数据索引存储提供搜索分析

基于可视化访问ES数据、分析

## 使用版本

Elasticsearch、Logstash、Kibana、Filebeat使用版本要统一

本文档中使用的是7.8.1

# ElasticSearch安装配置

## 安装

下载：<https://www.elastic.co/cn/downloads/elasticsearch>

下载对应平台的安装包，解压安装即可

## 配置

配置文件目录：elasticsearch-7.8.1\config\

配置说明：

elasticsearch.yml



jvm.options：可以配置jvm启动参数

log4j2.properties：

默认不用任何修改，即可在本地启动

## 启动

启动脚本目录：elasticsearch-7.8.1\bin

注意：在linux下不要用root账号下启动ES

# Filebeat安装配置

## 安装

下载：<https://www.elastic.co/cn/downloads/beats/filebeat>

下载对应平台的安装包，解压安装即可

## 配置

配置文件：filebeat-7.8.1\ filebeat.yml

配置文件说明：

<https://www.elastic.co/guide/en/beats/filebeat/7.8/configuration-filebeat-options.html>

可以配置日志文件位置、字段、多行日志处理等

本文档案例配置inputs/outputs：

# ========= Filebeat inputs =============

**filebeat.inputs**:

**- type**: log

**enabled**: **true**

**paths**:

- /var/log/\*.log

#- c:\programdata\elasticsearch\logs\\*

**- D**:\home\data\logs\nerp\nerp-ext\\*.log

**fields**:

#自定义字段

**beat\_type**: test\_logstash

# 多行日志，示例：2020-08-07 17:24:35.623 ERROR .......

**multiline.pattern**: '^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-9]{2}.[0-9]{3}'

**multiline.negate**: **true**

**multiline.match**: after

# ======== Outputs =================

# ----- Logstash Output -------------

**output.logstash**:

# The Logstash hosts

**hosts**: ["localhost:5044"]

## 启动

./filebeat –e

可以使用 –c 指定filebeat.yml文件：./filebeat –e –c filebeat-xxx.yml

# Logstash安装配置

## 安装

下载：<https://www.elastic.co/cn/downloads/logstash>

下载对应平台的安装包，解压安装即可

## 配置

### 官方文档

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

### 配置文件结构说明

配置文件结构：

配置文件结构：

# 日志导入

input {

}

# 日志筛选匹配处理

filter {

}

# 日志匹配输出

output {

}

配置文件的框架共分为三个模块,input,output,filter，每个模块里面存在不同的插件

常用插件：

一：输入插件（input）

输入插件主要是接受日志信息，有filebeat，kafka，file等

二：过滤器插件（Filter）

grok: 正则捕获是logstash最核心的功能，它的作用是将输入的字符串解析成需要的数据格式。

logstash 提供了一些默认的正则表达式，也可以自己定义正则表达式。

正则测试地址：<http://grokdebug.herokuapp.com/>

date: 插件可以用来转换你的日志记录中的时间字符串，变成 LogStash::Timestamp 对象，然后转存到 @timestamp 字段里

mutate: 插件是 Logstash 另一个重要插件，它提供了丰富的基础类型数据处理能力

包括类型转换，字符串处理和字段处理等

三：输出插件（output）

输出插件会将解析后的日志输出到什么地方，这时候就需要定义一些配置来定义输出条件

如：elasticsearch，redis，mysql等。

四：控制台输入输出，可用于测试

input {stdin{}}

output {stdout{ codec => rubydebug }}

### 配置示例

Logstash配置示例：



被处理的日志文件格式样版：



## 启动

-f 指定logstash的配置文件

./logstash-7.8.1/bin/logstash.bat -f logstash-sample.conf

# Kibana安装配置

## 安装

下载：<https://www.elastic.co/cn/downloads/kibana>

下载对应平台的安装包，解压安装即可

## 配置

配置文件：kibana-7.8.1-windows-x86\_64\config\ kibana.yml

主要配置：

server.port: 5601

elasticsearch.hosts: ["http://localhost:9200"]

i18n.locale: "zh-CN"

## 启动

./ kibana-7.8.1-windows-x86\_64/bin/ kibana

## 使用kibana

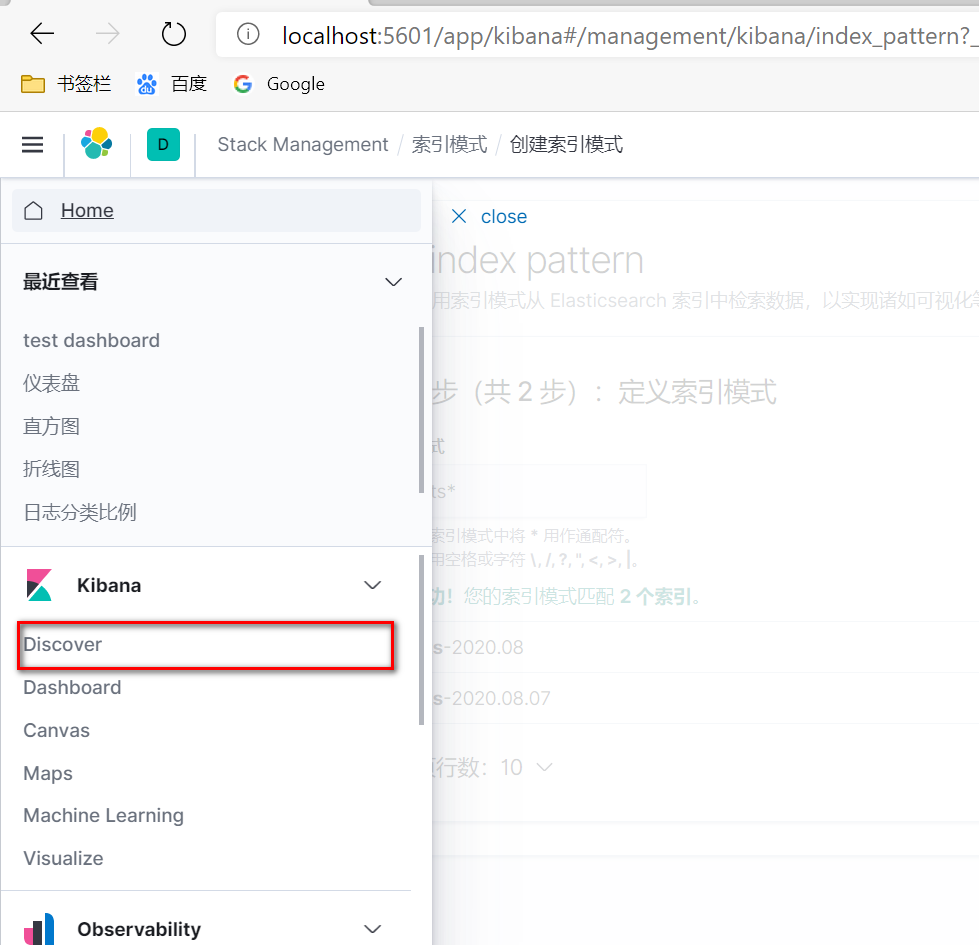
### 官方使用文档

<https://www.elastic.co/guide/cn/kibana/current/getting-started.html>

以下的使用示例，也是参考官方文档

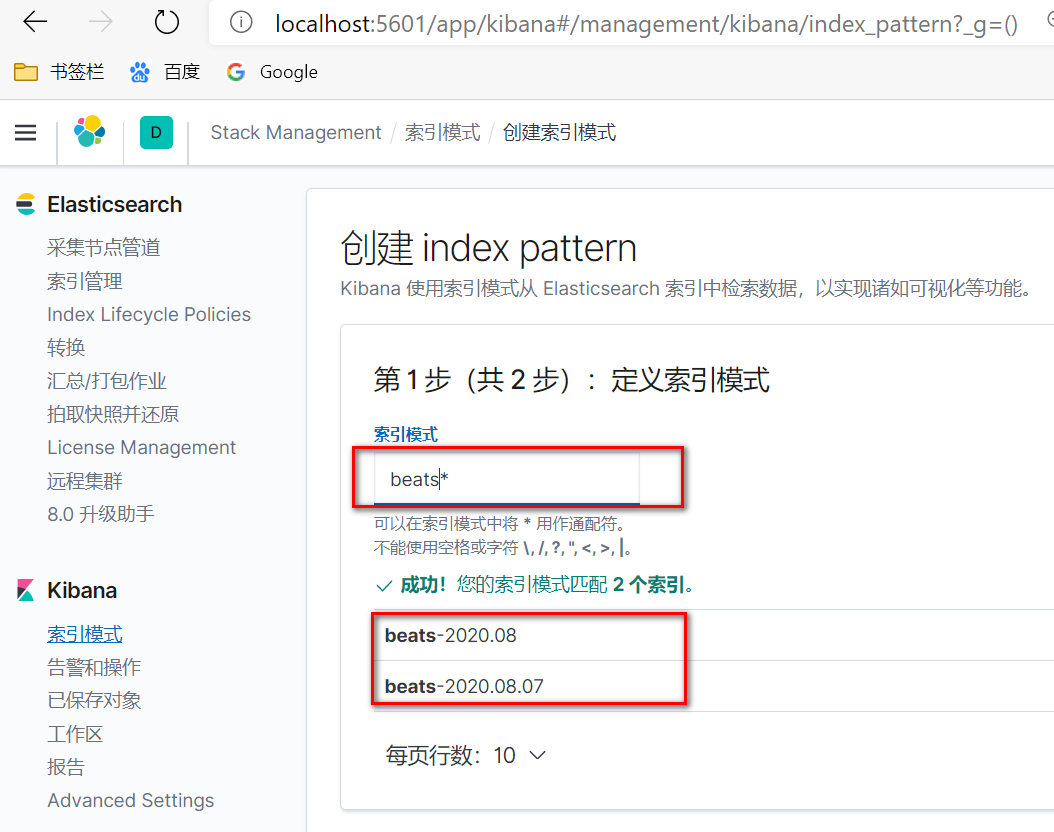
### 探索你的数据

1）：单击侧面导航中的 **Discover** 进入 Kibana 的数据探索功能



2）：创建索引模式

输入指定索引，可以指定通配符的



接着下一步



再次回到**Discover** 菜单

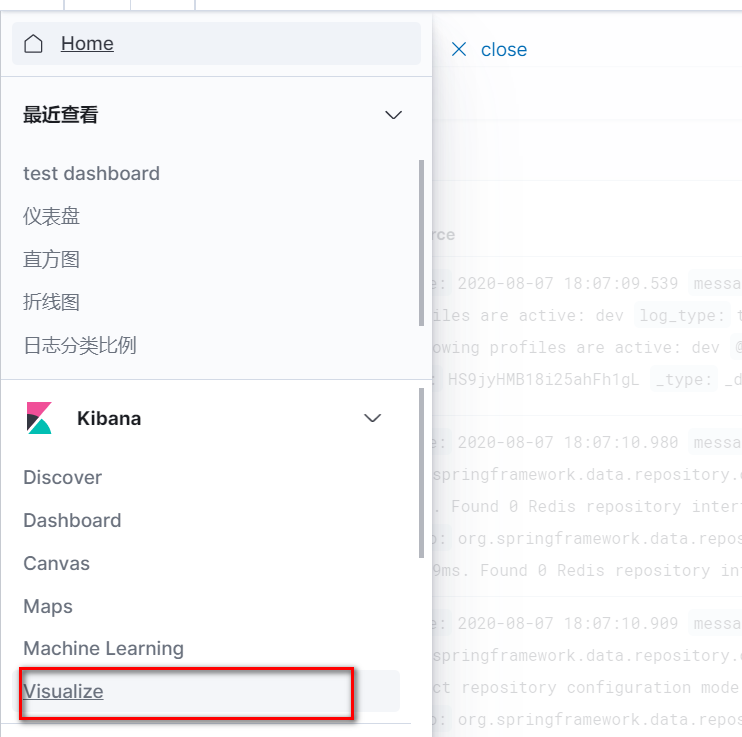


如上图，可以搜索我们的文档了，在可用字段可添加需要显示的字段

### 可视化数据

创建可视化

单击侧面导航中的 **visualize**进入 可视化功能

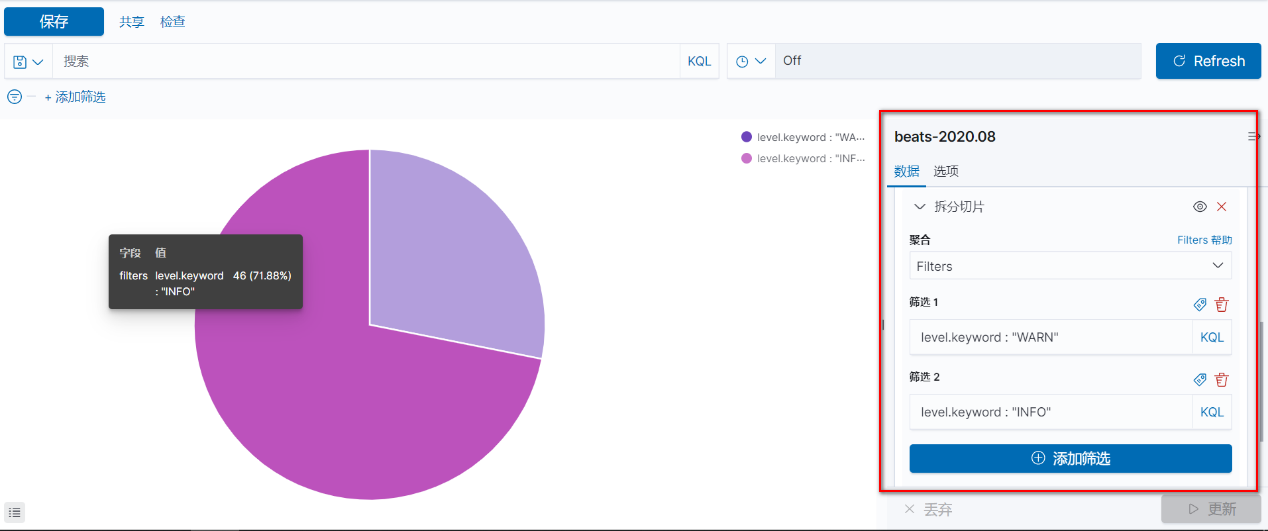


选择一个图表



您可以为已保存的搜索建立可视化效果，或者输入新的搜索条件。使用后者时，首先需要选择一个索引模式来指定搜索哪些索引

设置图表中的数据并保存：



### 使用仪表板汇总数据

仪表板可用于集中管理和分享可视化控件集合。构建一个仪表板用以包含您在本教程中已保存的可视化控件，方法如下：

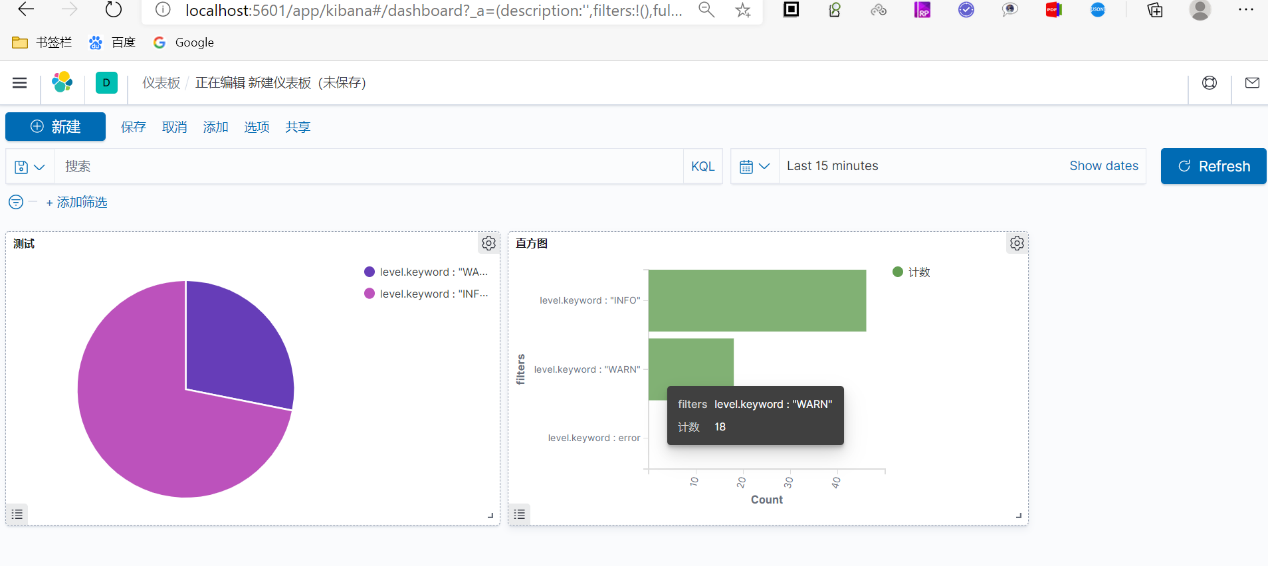
在侧边导航栏点击 Dashboard 。

点击 Add 显示已保存的可视化控件列表。

单击 Markdown Example 、 Pie Example 、 Bar Example 和 Map Example ，然后通过点击列表底部向上的小箭头关闭可视化控件列表。

将鼠标悬停在一个可视化控件上可以显示允许您编辑、移动、删除和调整它的控制器。

您的样本仪表板最终看起来应该大概像这样



### Dev tools

在侧边导航栏点击 Dev Tools

可以进行 ES API测试，Logstash Grok测试

