**ELK日志用户行为分析操作手册**

常用操作总览

创建索引模式-->可视化-->仪表盘

1. 数据的导入与筛选、查看
2. 导入

数据已经通过logstash导入；

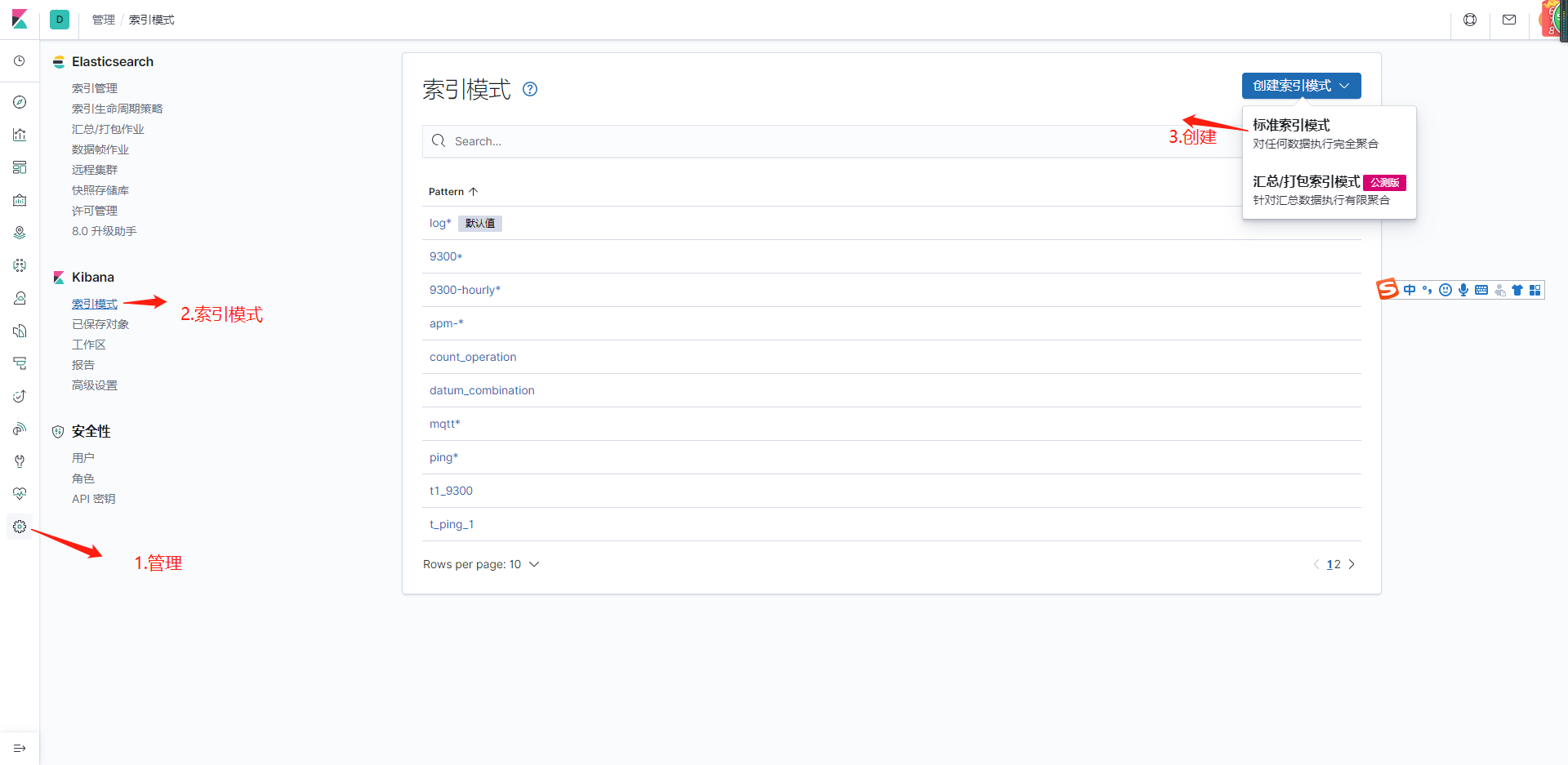
也可在kibana中手动导入进行探索，具体为：选择：机器学习-->数据可视化工具-->导入数据。支持分隔的文本文件，例如 CSV 和 TSV；换行符分隔的 JSON；具有时间戳通用格式的日志文件。



1. 创建索引模式

数据导入后需要创建索引模式方可查看。

选择：管理-->索引模式-->创建索引模式-->标准索引模式



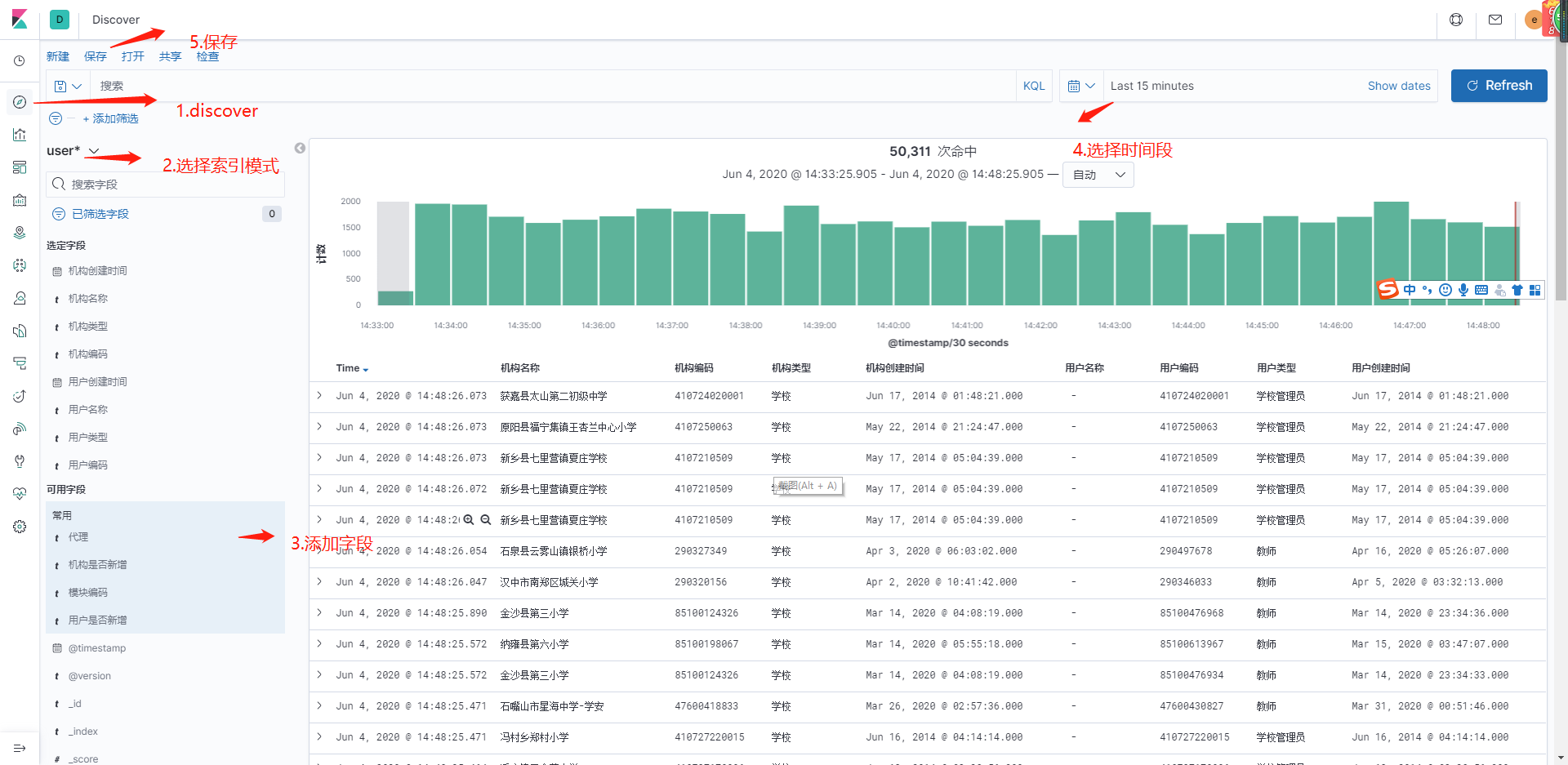
如每天的上传日志文件命名为user-2020.05.26，user-2020.05.27，user-2020.05.28...想要访问到这些日志，则索引模式可命名为user\*（其中\*是通配符，表示匹配以user开头的日志）。

下面案例以user\*索引模式为例。

1. 数据的查看与筛选

选择：discover-->索引模式名字-->添加字段-->选择时间段-->保存

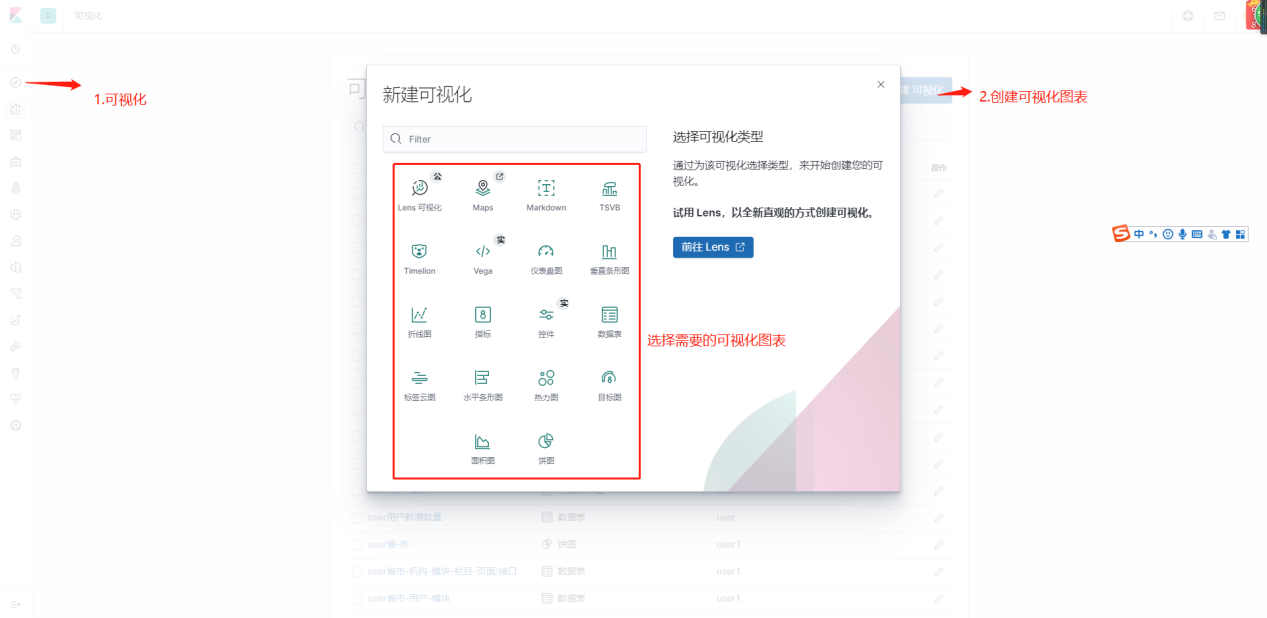
保存是可选项，如果保存，方便下次访问时，直接选择“打开”，不用再添加字段。



也可点击“+添加筛选”，根据需要对数据进行筛选。或者在搜索栏中对数据进行检索，可参考：<https://www.jianshu.com/p/83223427d089>

二、可视化操作

如图可根据需要创建需要的可视化图表，再选择图表的选择源-->user\*



常用的图表有

1. 仪表盘图

如想要可视化活跃用户的数量：在指标的聚合选项中选择需要的聚合方式，这里根据用户编码的唯一计数方式将日志中重复出现的用户只计一次；然后在存储桶中选择：聚合：词-->字段:用户类型-->排序依据：用户编码的唯一计数。表示按字段“用户类型”进行分类，每类的数量按用户编码唯一计数方式进行计数。

注意区分计数与唯一计数的区别：计数表示用户只要出现过一次就进行一次计数，唯一计数将相同用户只计数一次。

创建完成后，选择保存。



1. 垂直条形图

如想要查看不同用户主要访问了哪些模块，可创建垂直条形图。

选择：

Y轴 指标：计数

X轴 存储桶：聚合：词-->字段：用户编码-->指标：计数

拆分序列 子聚合：词-->字段：模块名字-->指标：计数

面板设置：在图表上显示值

保存名为“user用户-模块”



1. 折线图

方法同创建简单条形图相同，但是需要选择

指标和轴-->图表类型：折线图

1. 指标

指标与存储桶的选择依据与前面相同。

1. 数据表

如想要汇总机构在不同省市访问模块名字、栏目名字、页面/接口的次数，可通过选择：

指标 计数

存储桶 聚合：词-->字段：省

聚合：词-->字段：市

聚合：词-->字段：机构名称

聚合：词-->字段：模块名字

聚合：词-->字段：栏目名字

聚合：词-->字段：接口/页面

保存名为“user省市-机构-模块-栏目-页面/接口”

1. 标签云图

指标与存储桶的选择依据与前面相同。

1. 饼图

如果想要可视化不同省、市的占比，可通过饼图。

指标 切片大小：计数

存储桶 拆分切片：聚合：词-->字段：省-->指标：计数

拆分切片：聚合：词-->字段：市-->指标：计数

选项 标签设置：显示标签

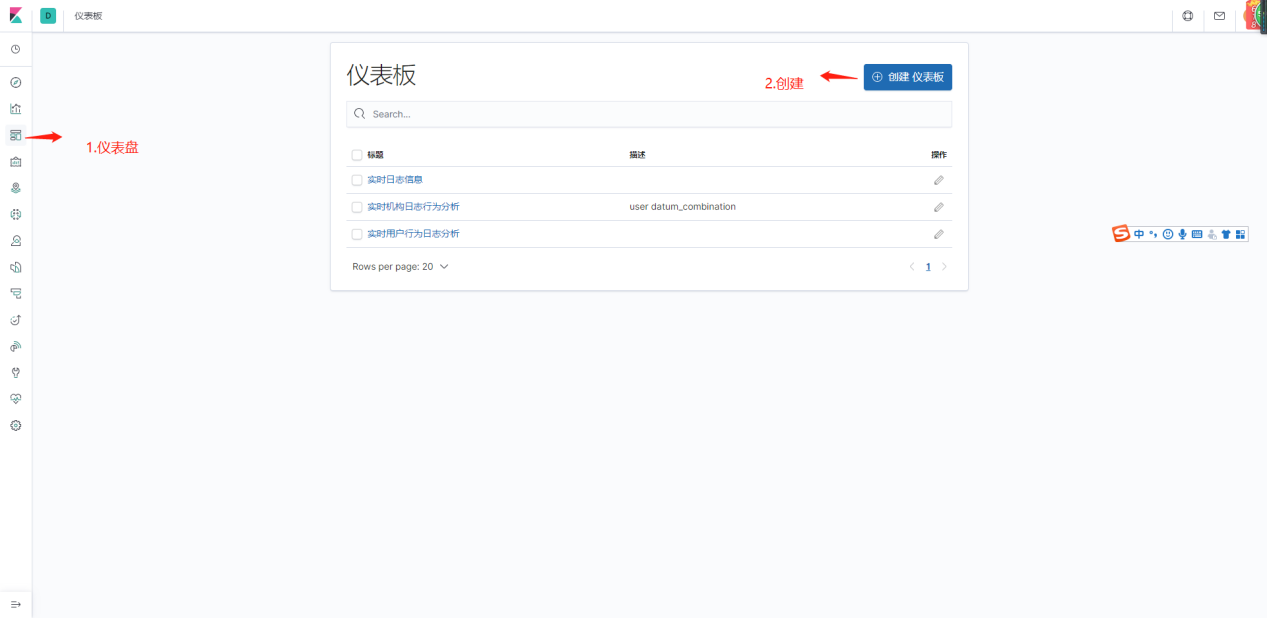
保存名为“user省-市”。

其他图标的创建方法类似，可自行探索。

三、仪表盘

创建仪表盘-->添加可视化图表-->保存

将可视化图表添加进来后，可以根据需要固定每个图表的时间范围。点击每个图表的右上角，选择定制时间范围。



1. 分析数据的导出
2. 分析数据

在创建的仪表盘中，可以通过添加筛选条件进一步分析数据。如在user\*索引模式中，想要具体研究河南省的用户行为。

点击左上角，添加筛选：

索引模式：user\*-->字段：省-->运算符：是-->值：河南省

可从饼图“user省-市”中看到河南省的用户中包括哪些市，从条形图“user省市-机构-模块-栏目-页面/接口”中可看到河南省中近段时间活跃的用户常访问的模块。也可在数据表中，按右上角：检查-->下载csv，将汇总的省-市-机构-模块-栏目-页面/接口的数据下载下来。同样的，其他的图表也可通过相同的方式下载。