# 一、时间过滤器

## 1、快速设置过滤器-Quick

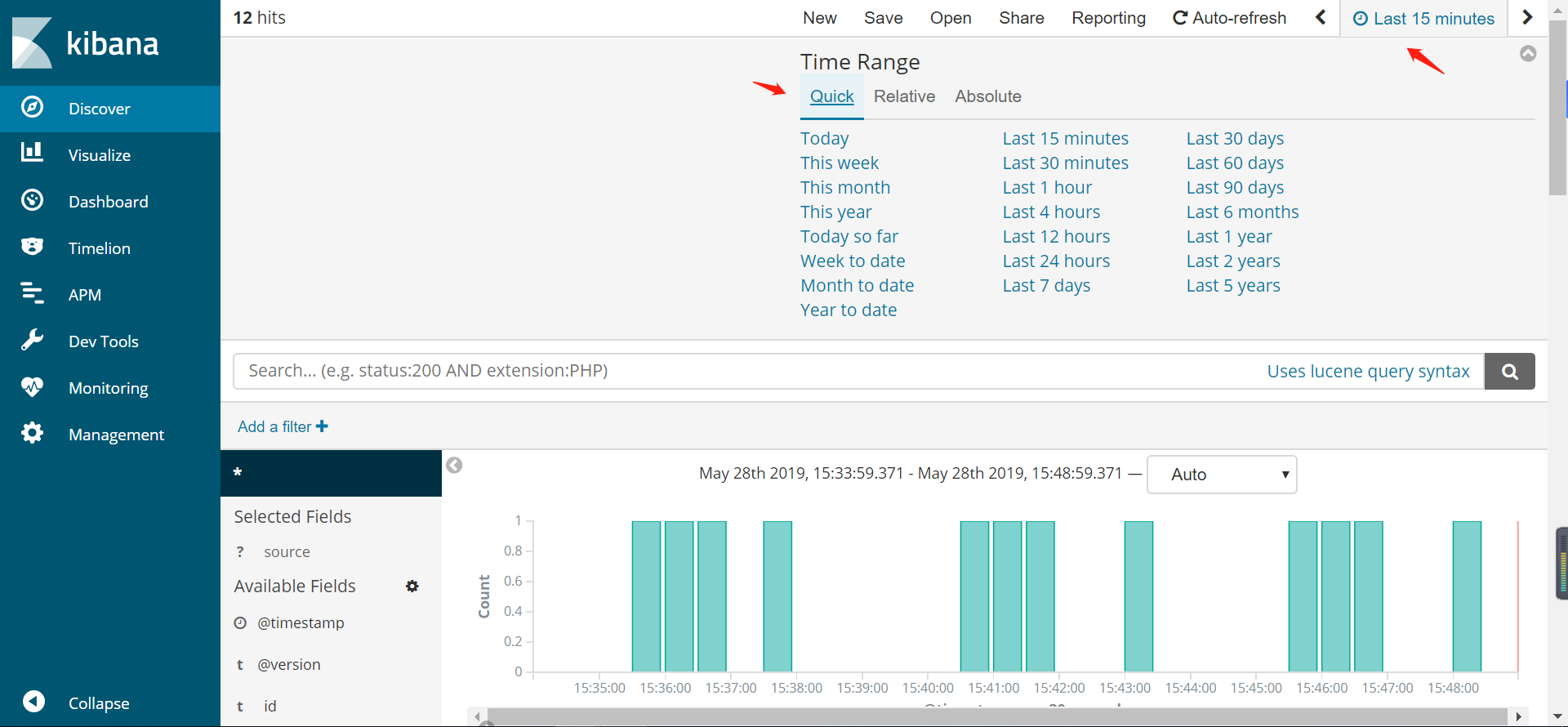


图 1 快速设置过滤器

如图1，从这里可以选今天昨天，和最近15min等，按需求显示日志

## 2、相对时间过滤器-Relative

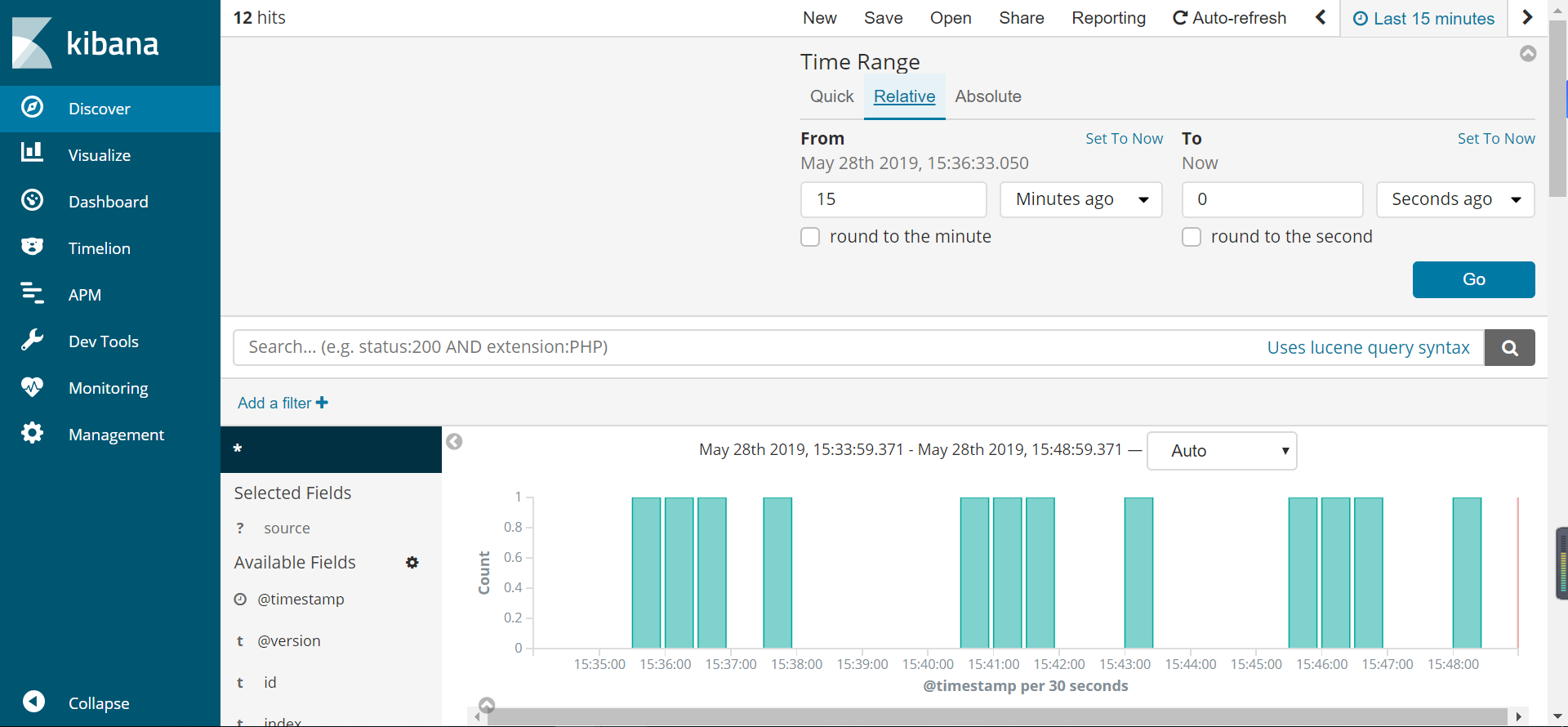


图 2 相对时间过滤器

如图2，从这里可以自定义几小时以前或者几周以前数据，按需求显示日志

## 3、绝对时间过滤器-Absolute

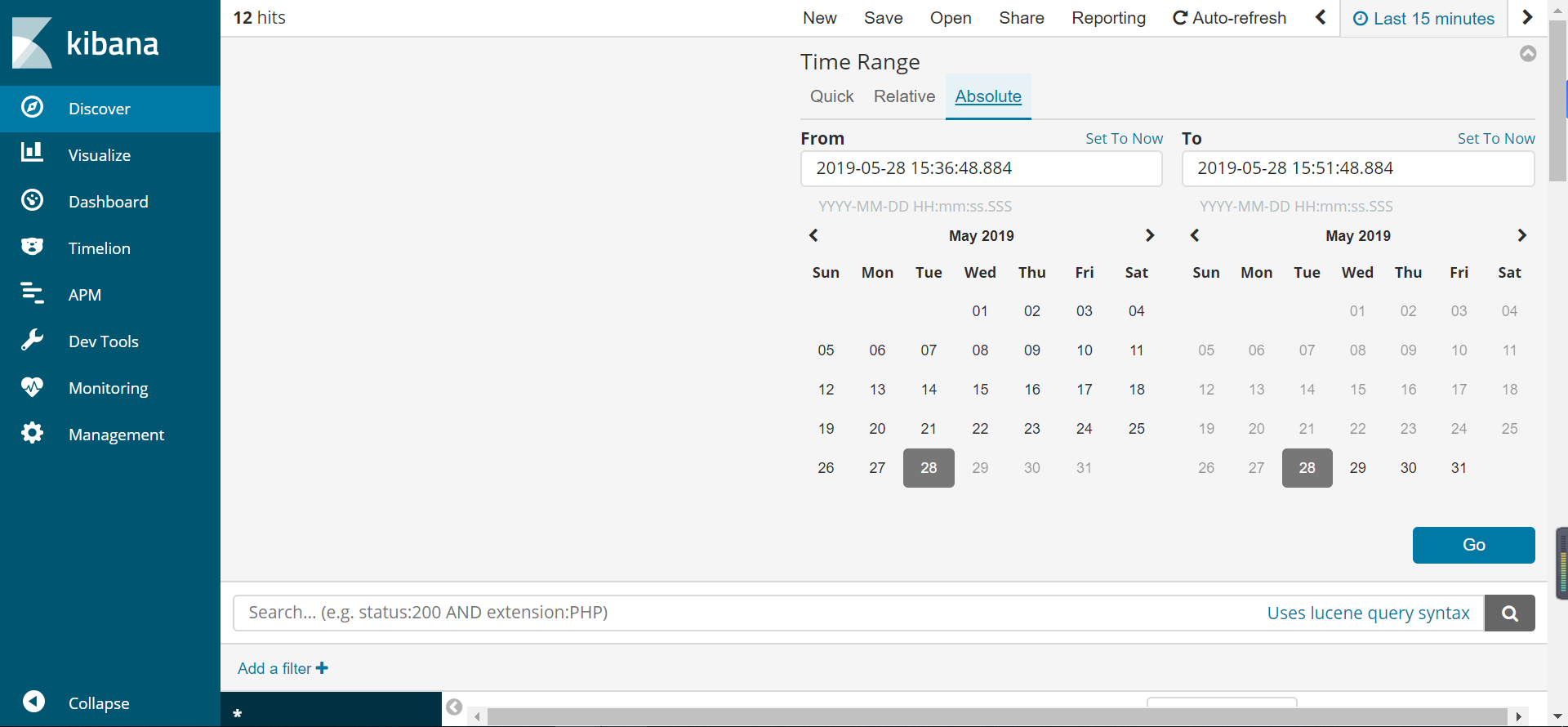


图 3 绝对时间过滤器

如图3，这里是一个绝对的时间，直接选就好了。

## 4、柱状图时间过滤器

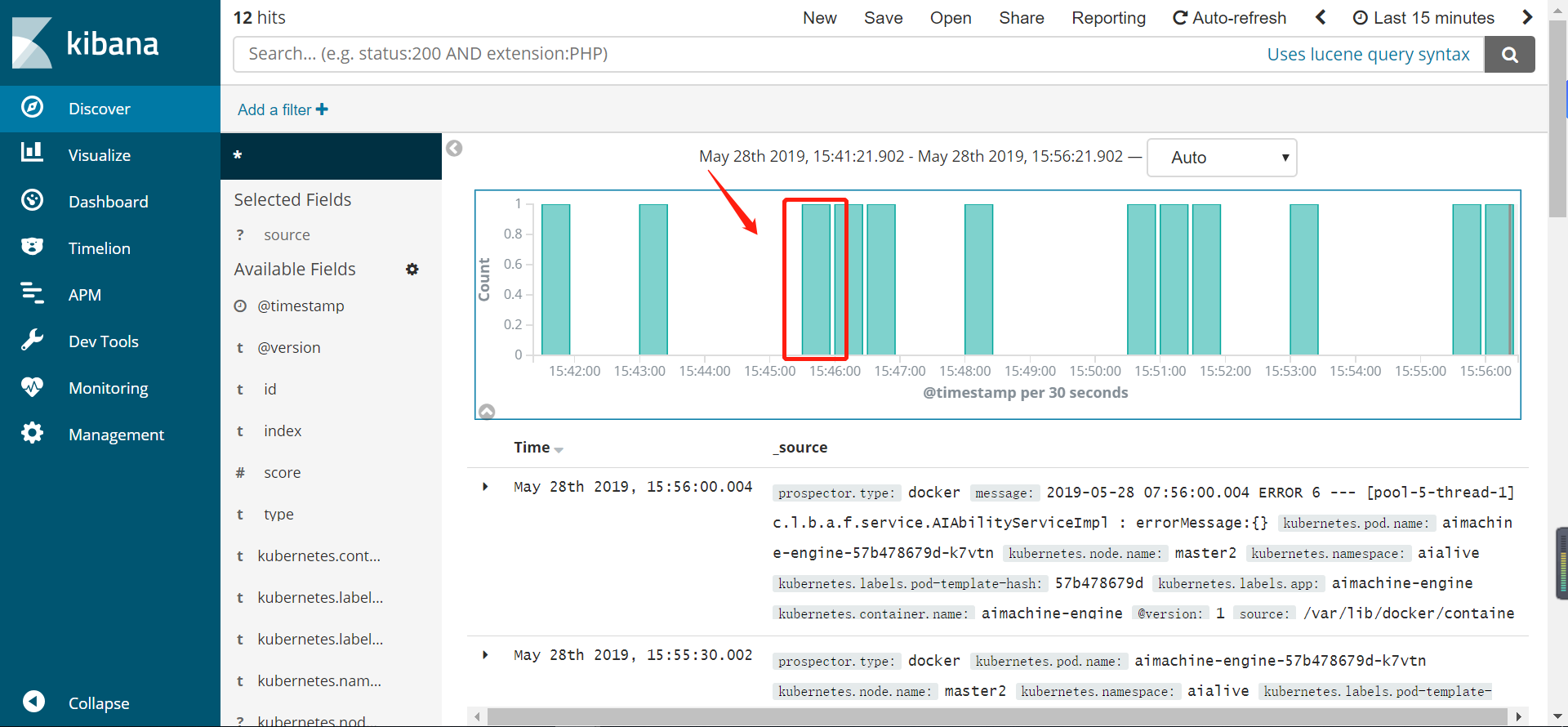


图 4 绝对时间过滤器

如图4，直接点击柱状图即可查看明细

# 二、搜索数据

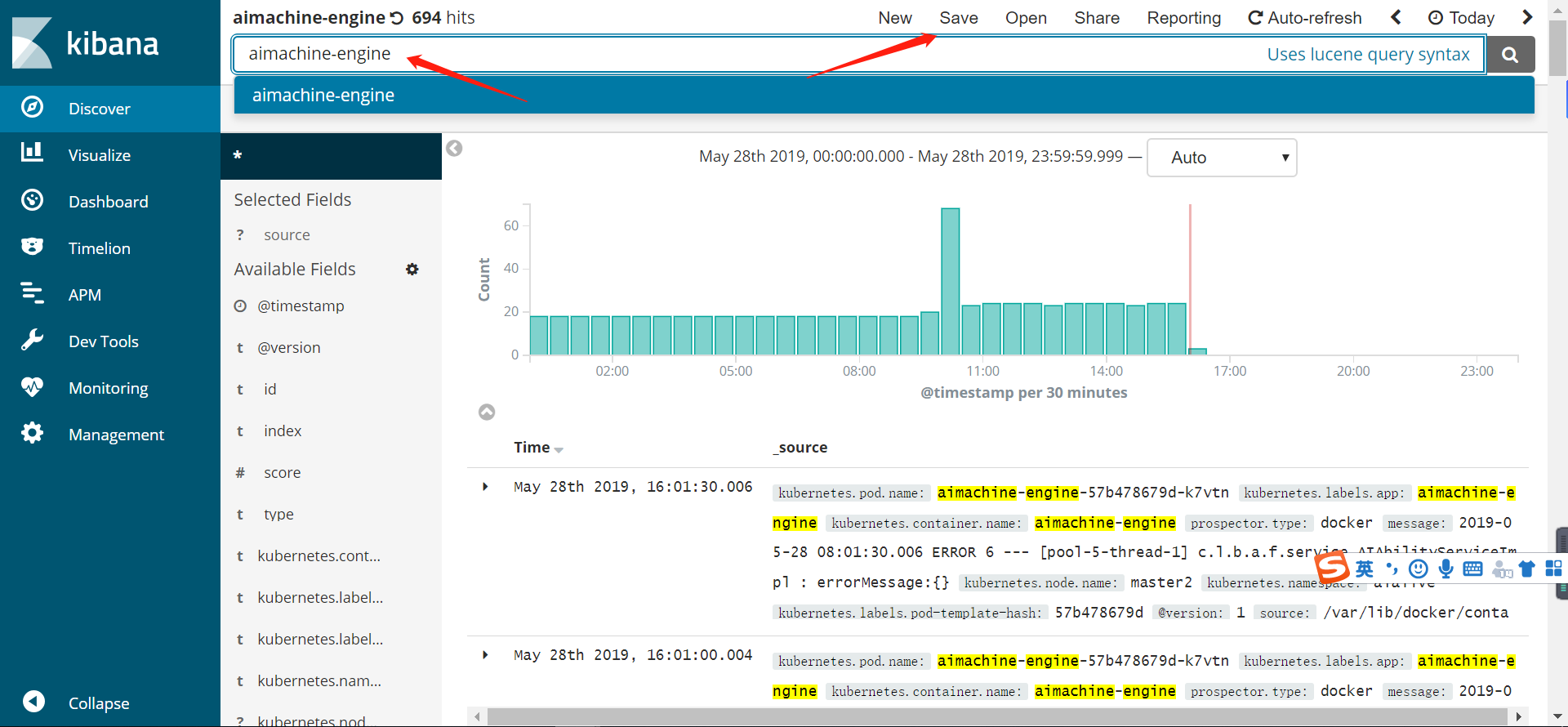


图 5 模糊搜索

如图5，比如想查询aimachine-service这个项目日志，直接在搜索框搜索，搜索完成后也可以点击箭头处的保存，保存这个搜索，如图6

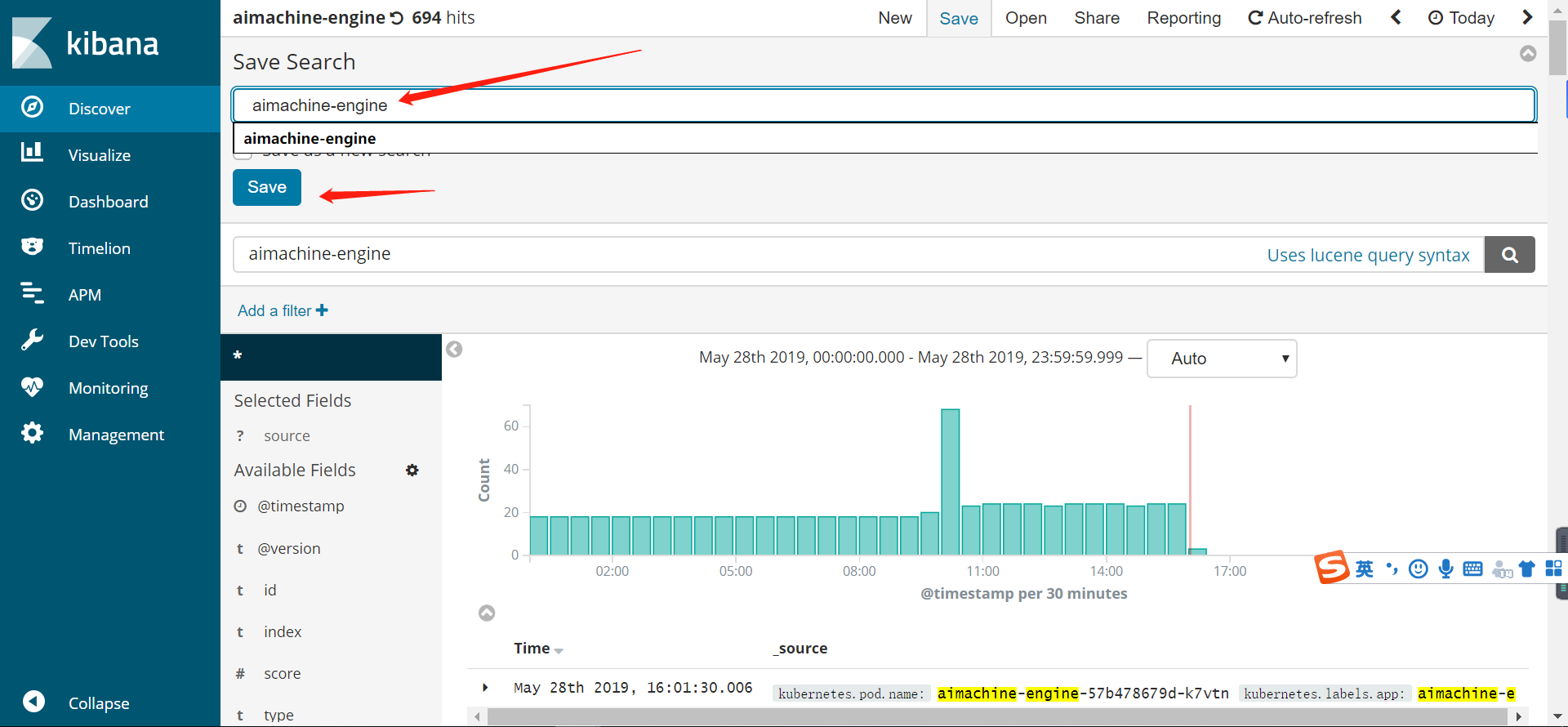


图 6 保存搜索

保存成功后我们可以在如图7所示中查看

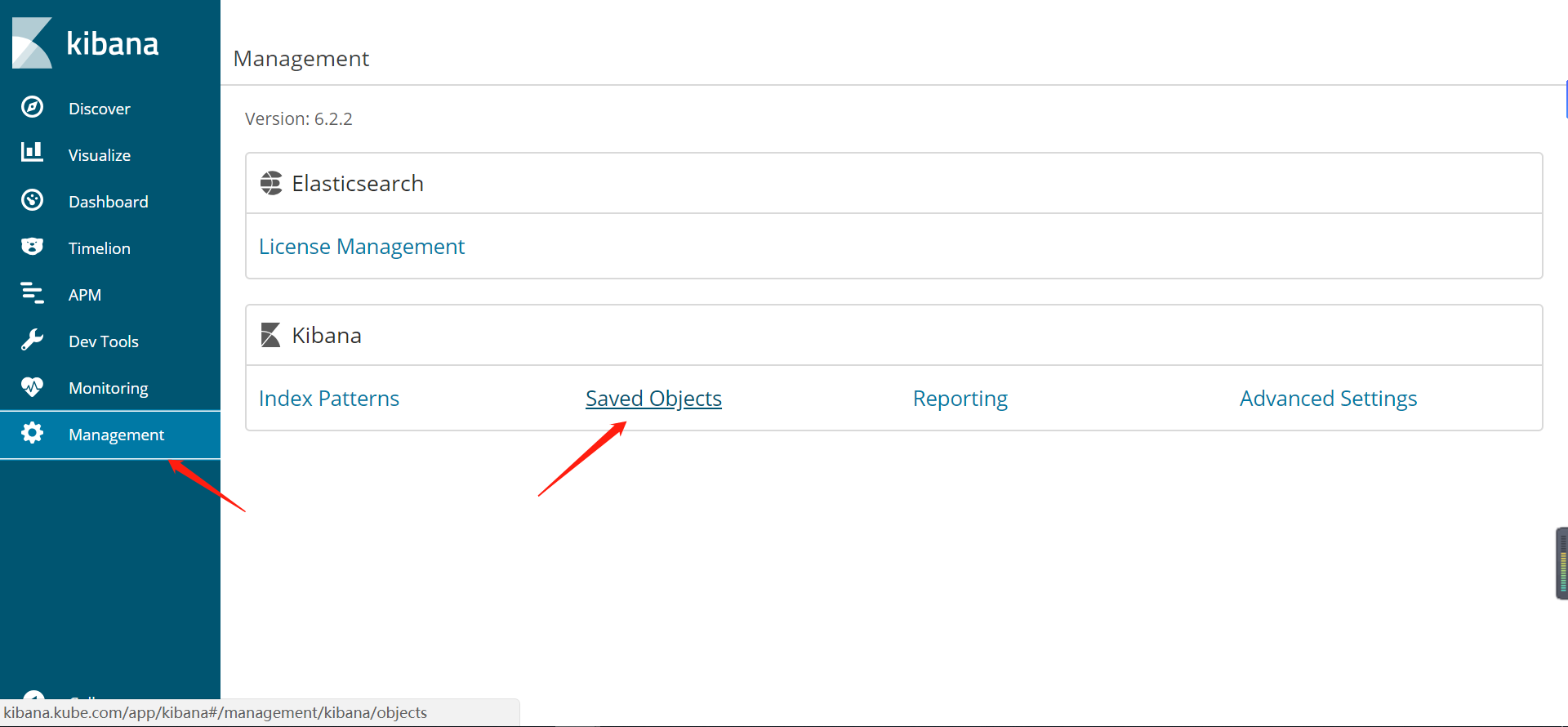


图 7 查看搜索

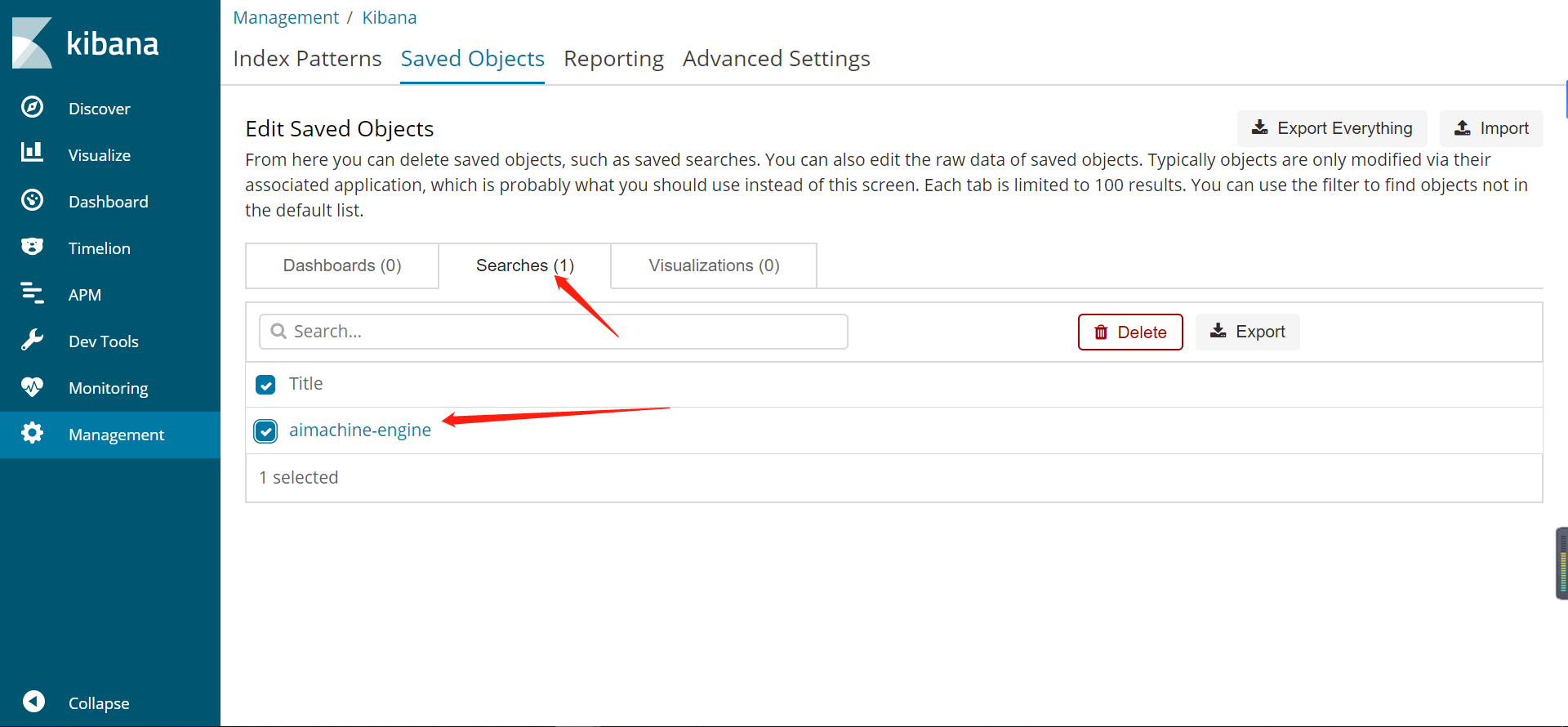


图 8 查看搜索

在图7位置打开已存搜索，在图8位置这里可以导出，也可以点击进去看es查询语法，点击进去如图9所示

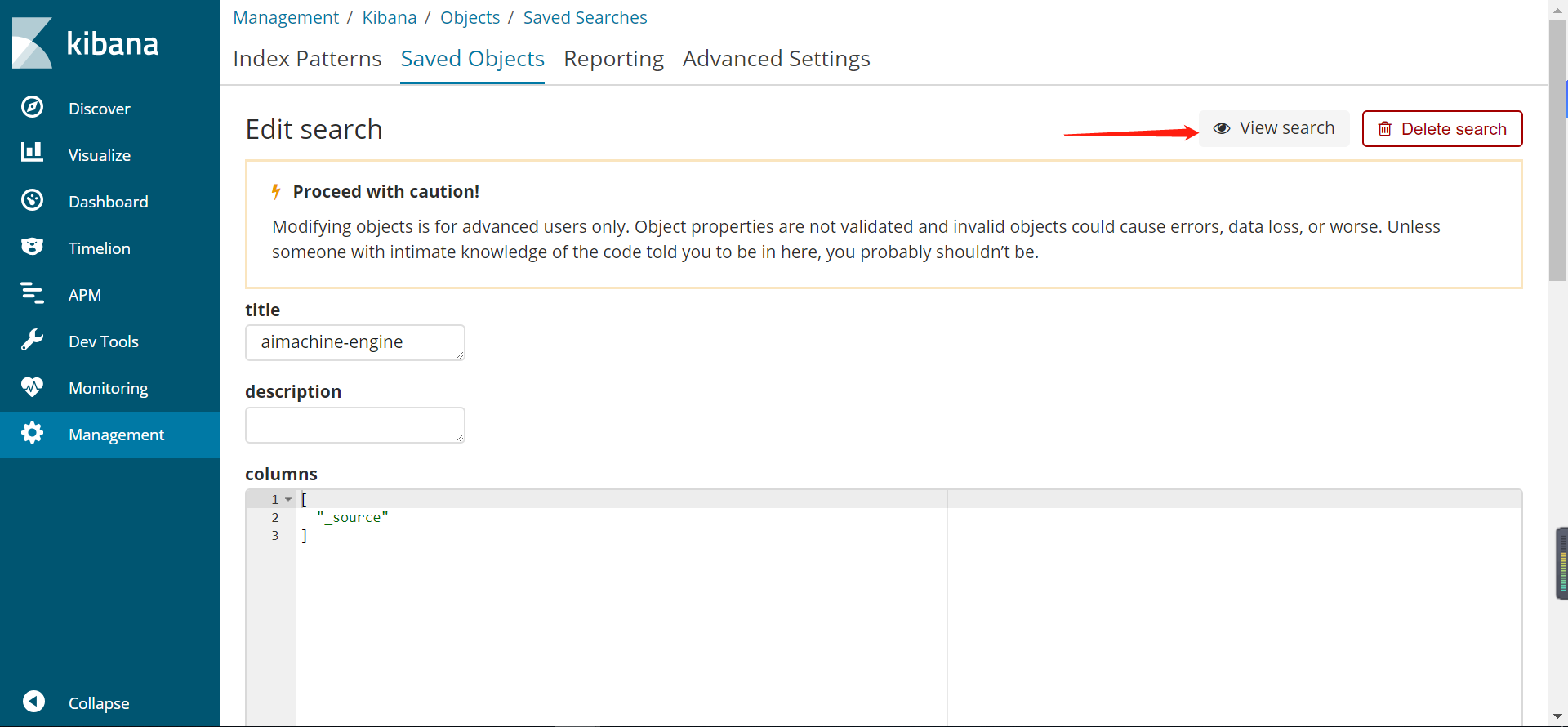


图 9查看保存

如图9所示，点击view\_search即可查询到这个保存的日志

搜索为模糊查询搜索，需要精确的查询需要使用kabina语法，见下文

# 三、按字段过滤搜索

在Discover页面鼠标悬浮，出现add字段，添加kubernetes.container.name 和message 这两个字段，当然，也可以按照需求添加其他，add字段前如图10，add字段后如图11

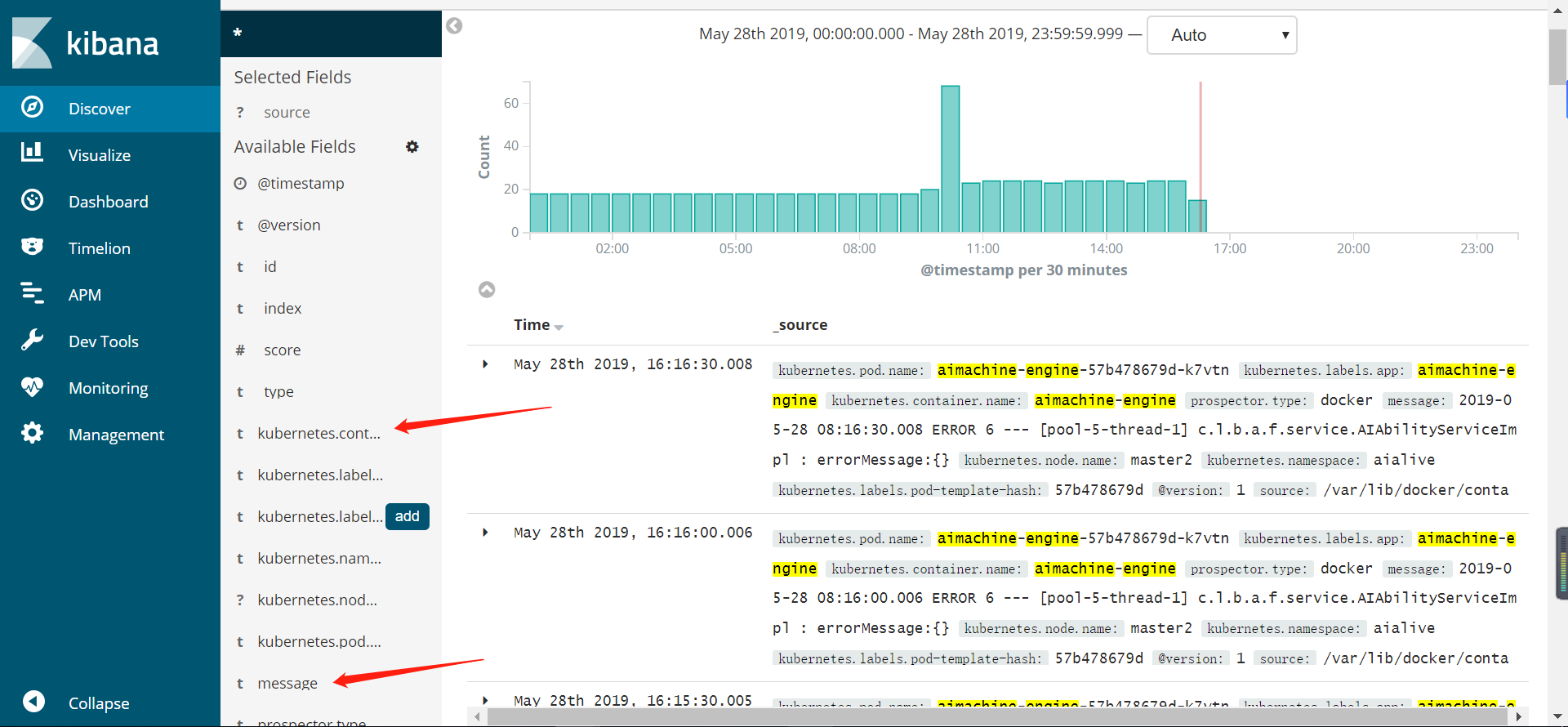


图 10 add字段前

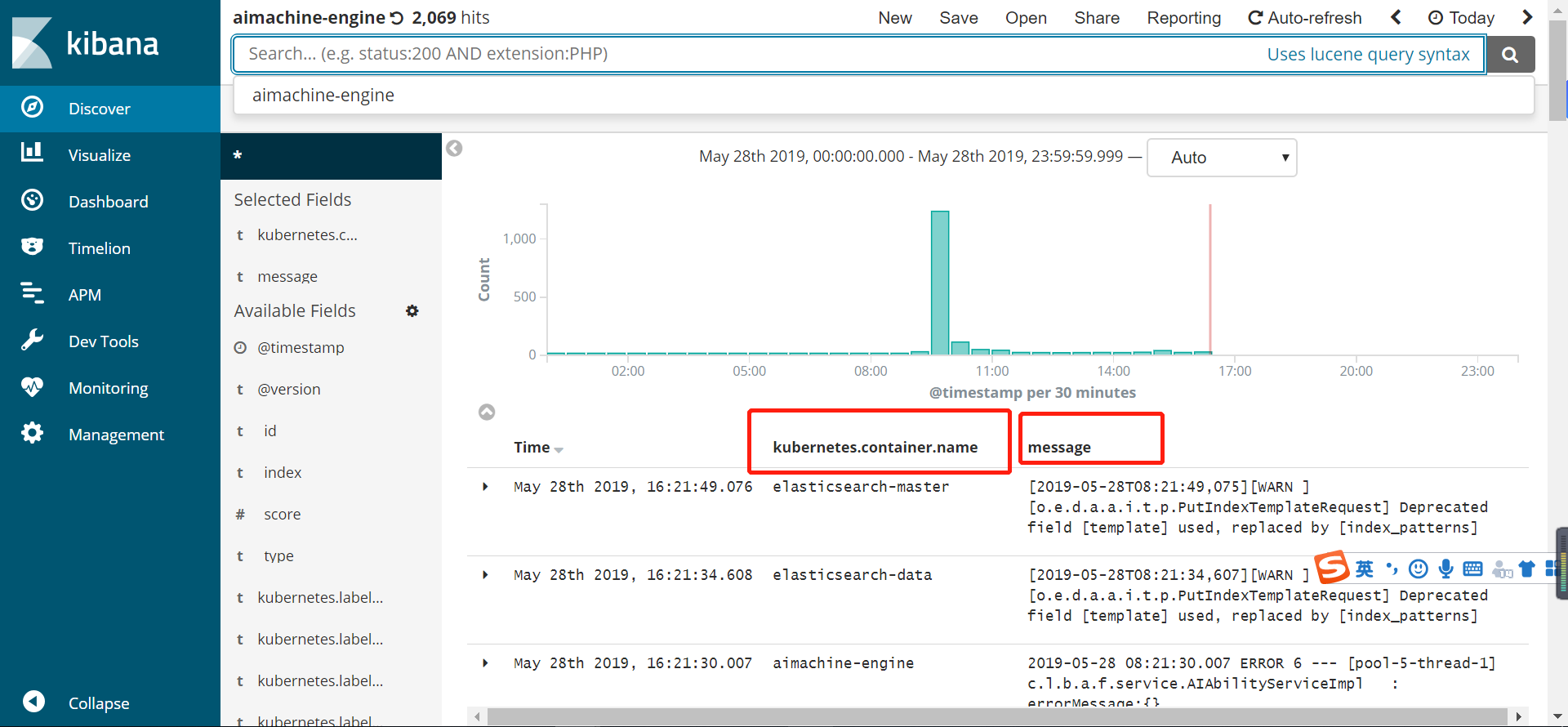


图 11 add字段后

这时候可以在搜索框输入kubernetes.container.name:"aimachine-engine"精确查询该项目日志，如图12所示，这里"aimachine-engine"一定要加上双引号，加上双引号才是精确查询，否则为模糊查询

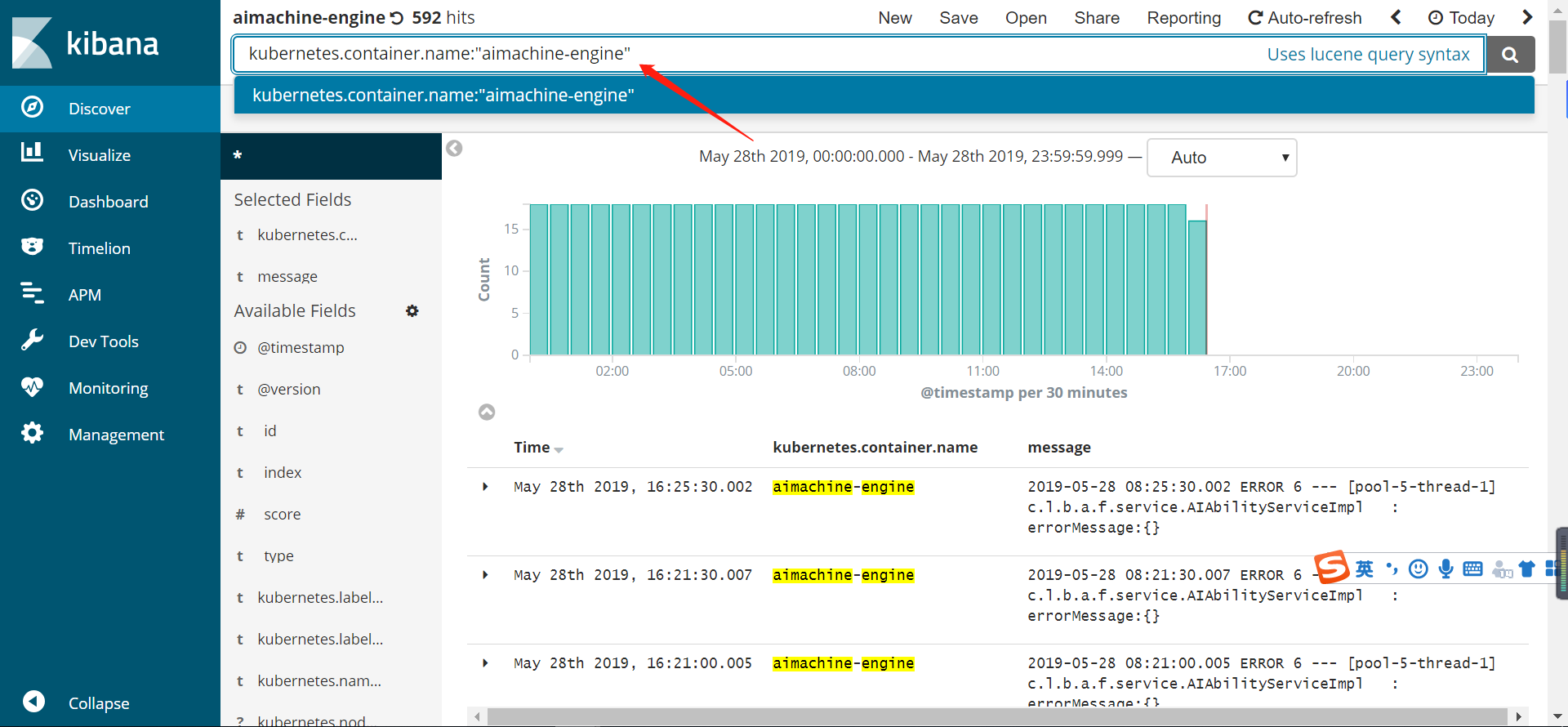


图 12 add字段后

各位同事可根据自己的项目查询实时日志，只收集ERROR和WARING的日志级别。