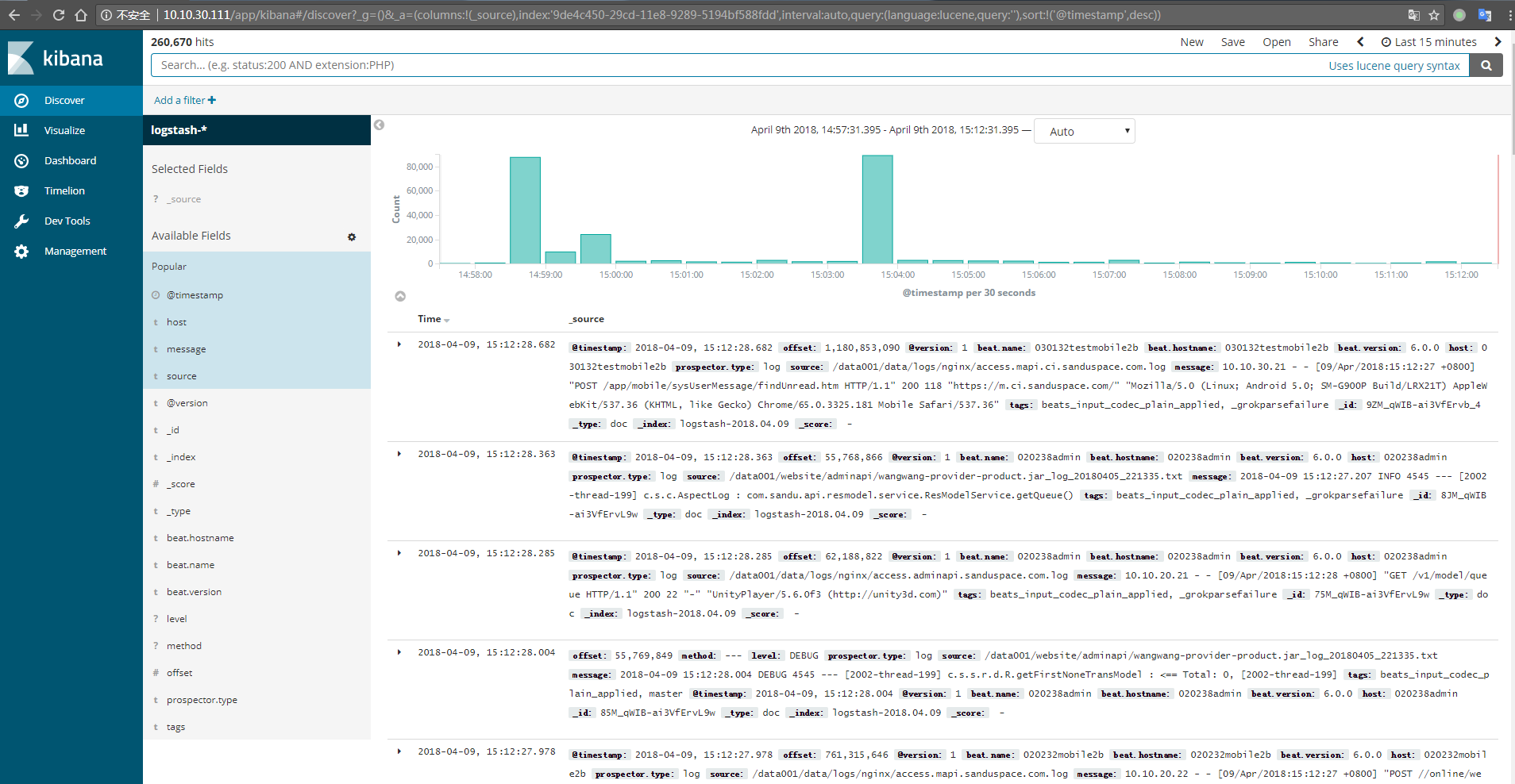
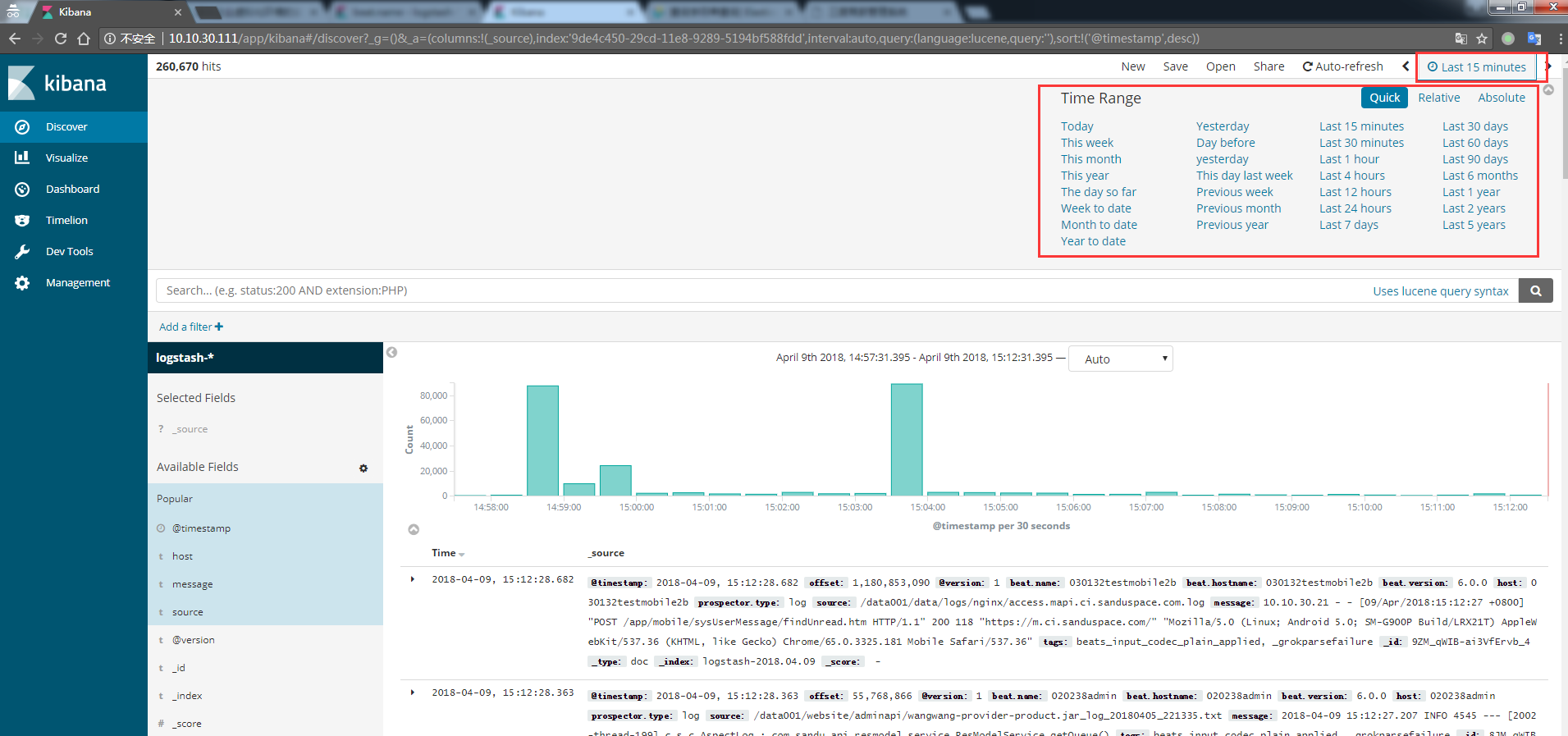
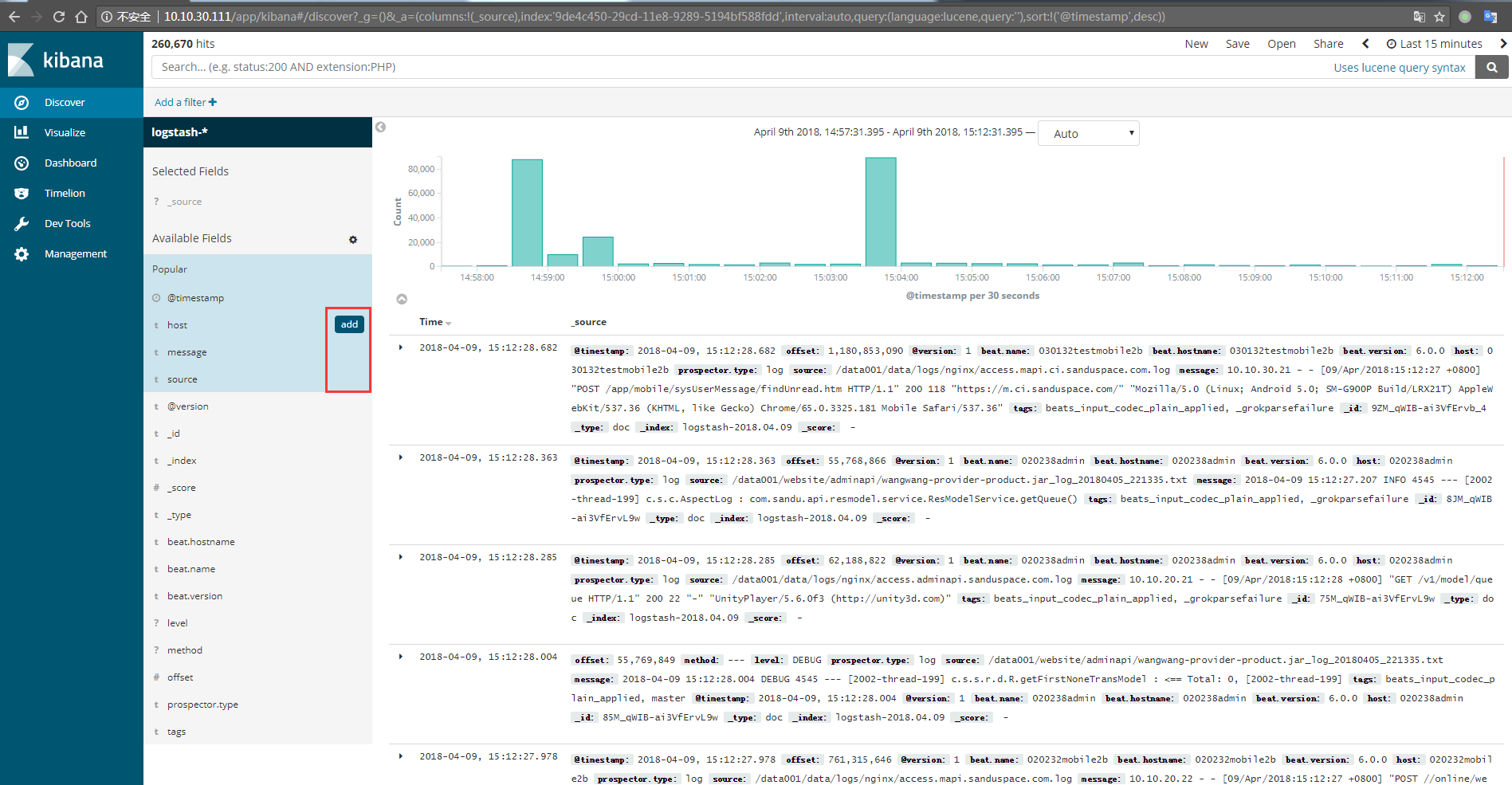
1、谷歌浏览器访问<http://10.10.30.111>，用户名：sanduspace密码：sanduelk 显示如下图表示正常访问



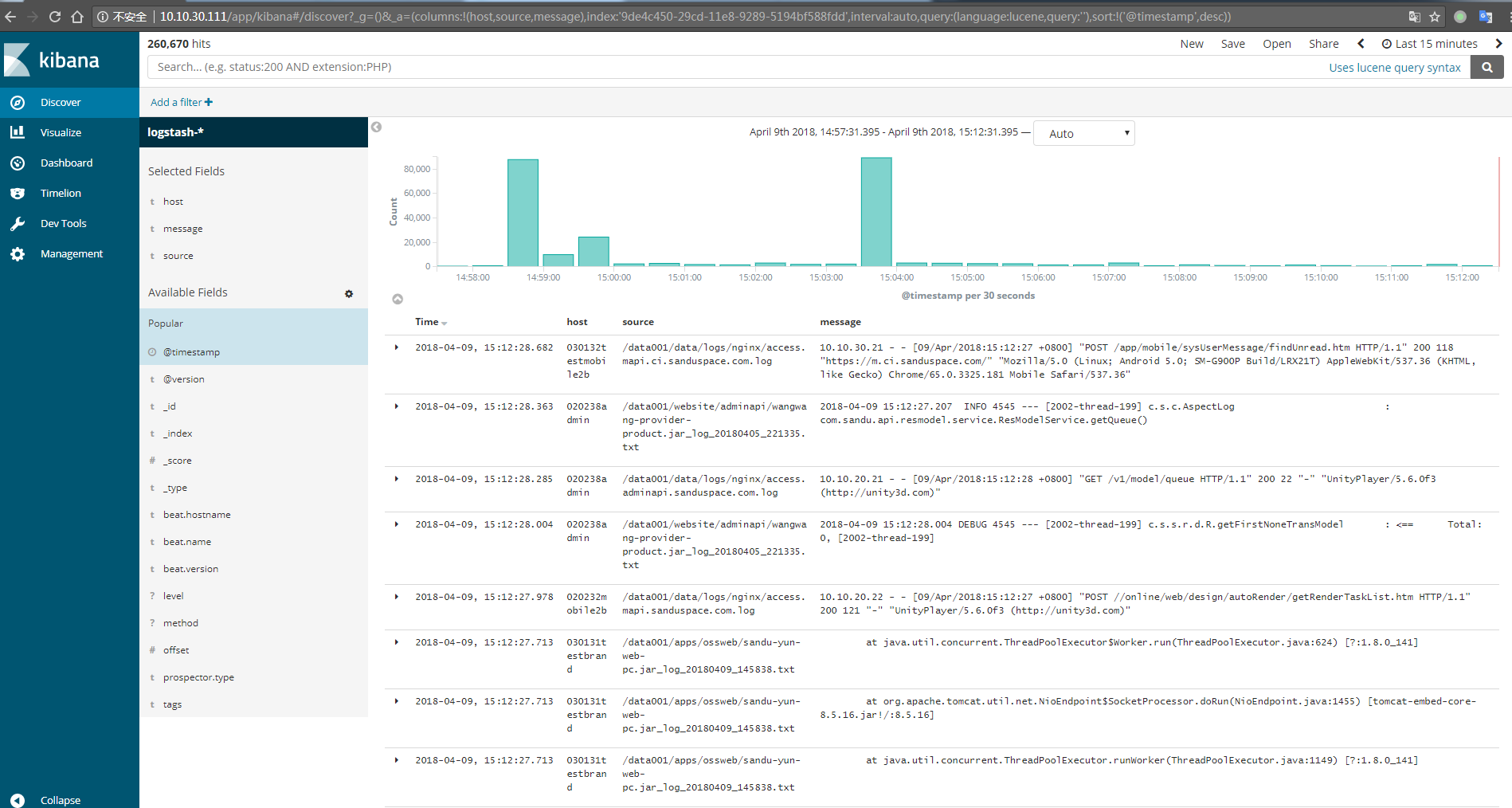
2、根据自己需求选择需要查询的日志时间段，默认为十五分钟之前



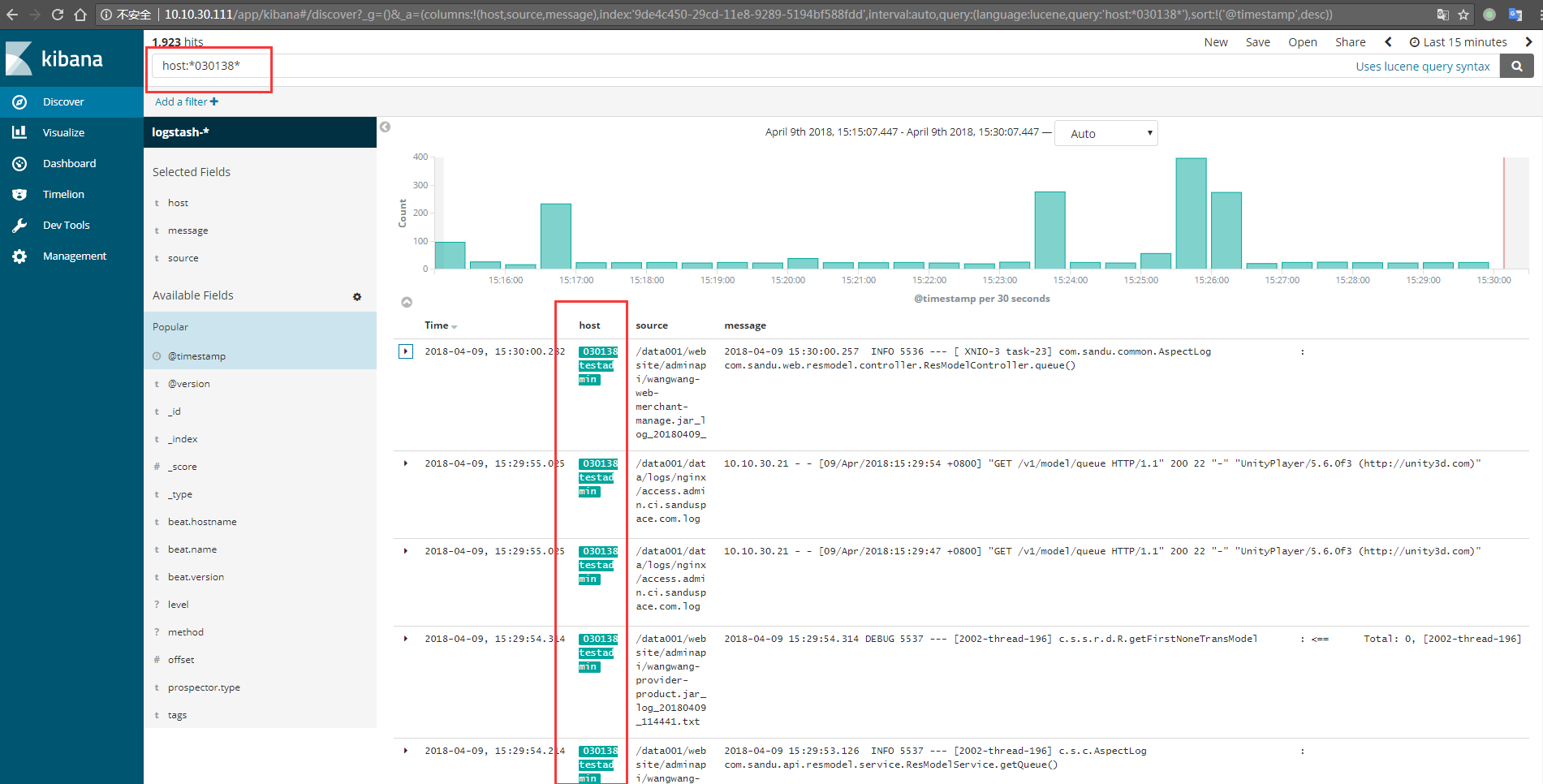
3、选择需要显示的字段，建议显示“host”“source”“message”字段，其中“host”字段表示主机名；“source”字段表示日志路径；“message”字段表示日志内容，其余字段可根据自己需求显示。如下图，点击add即可选择显示的字段。也可不选择字段



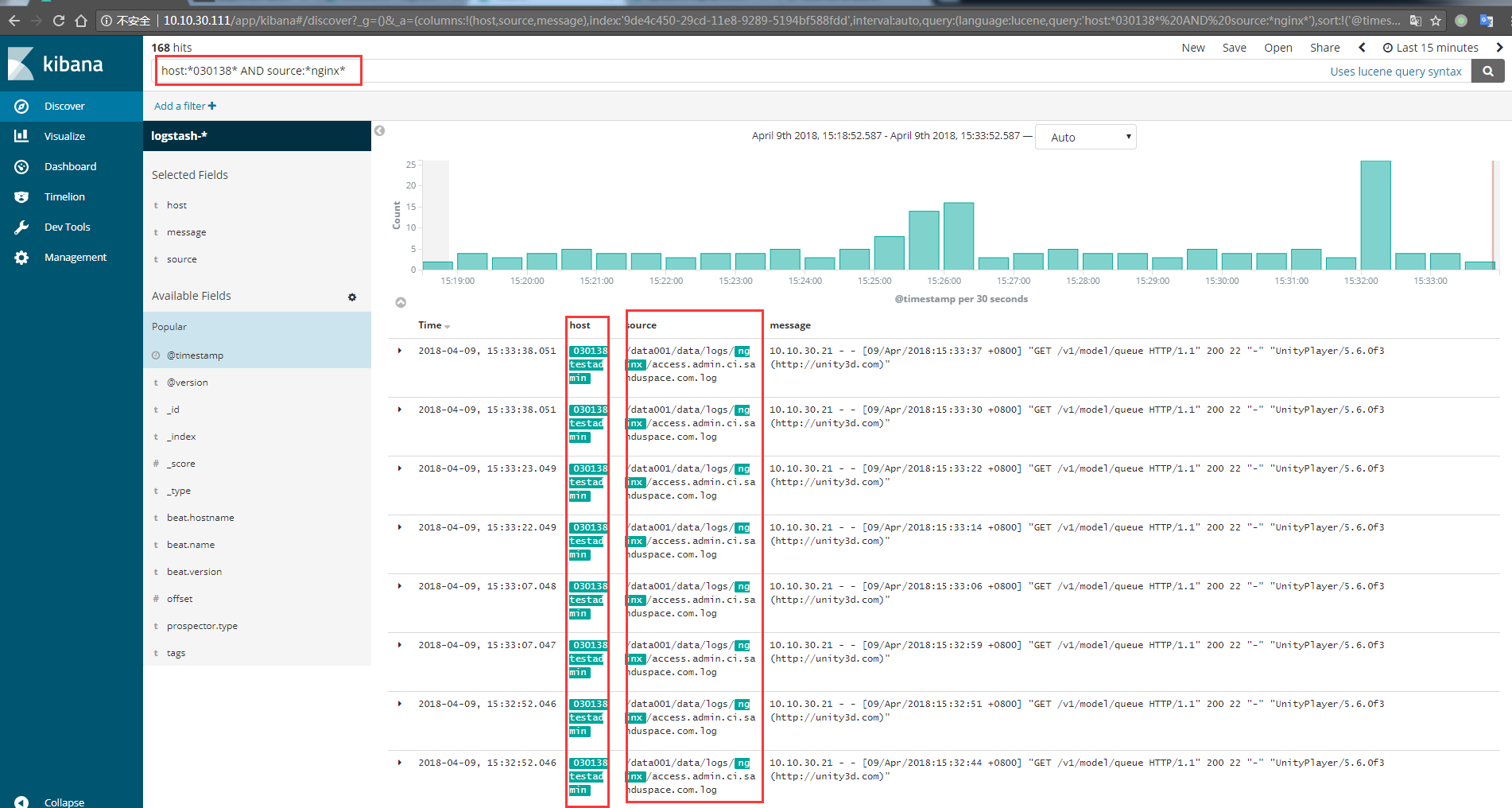
4、添加好显示的字段效果如下图



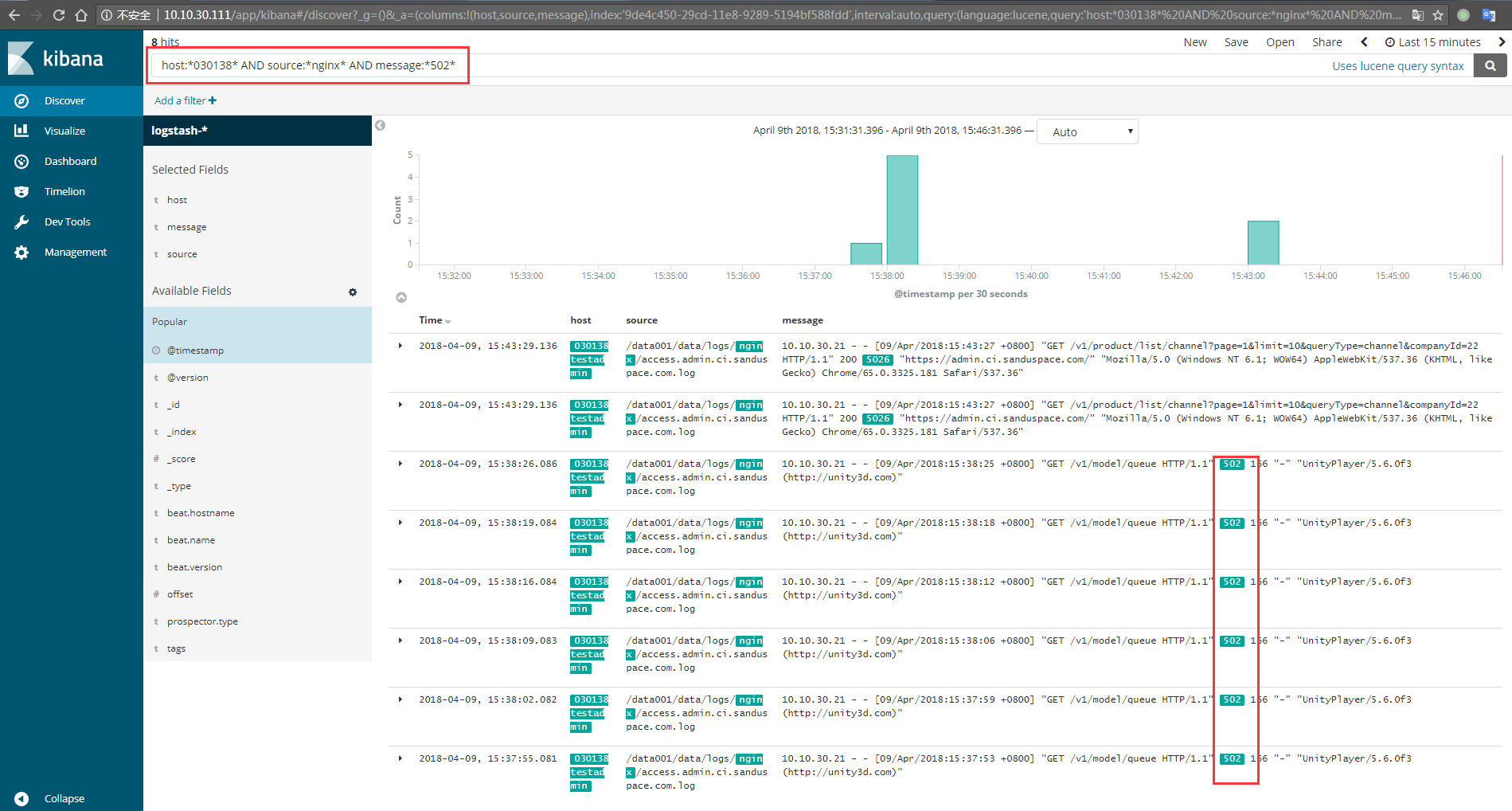
5、搜素日志，例如需要显示“集成商家后台”服务器所有日志，可在搜索栏输入“host:\*030138\*”，表示搜索最近十五分钟服务器主机名包含“030138”的主机，星号表示通配符，效果如下图



6、继续搜索日志，例如需要显示“集成商家后台”服务器Nginx日志，则在搜索栏输入“host:\*030138\* AND source:\*nginx\*”，这句话表示搜索最近十五分钟主机名包含030138和日志来源为nginx的日志



7、继续搜索日志，例如需要搜索“集成商家后台”服务器Nginx日志里面的某个字段，则在搜索栏输入“host:\*030138\* AND source:\*nginx\* AND message:\*502\*”，这句语句表示搜索最近十五分钟主机名包含030138和日志来源为nginx且日志内容包含502的日志，效果如下图



更多搜索语法请访问：[https://www.elastic.co/guide/en/elasticsearch/reference/6.0/query-dsl-query-string-query.html#query-string-syntax](https://www.elastic.co/guide/en/elasticsearch/reference/6.0/query-dsl-query-string-query.html" \l "query-string-syntax)

更多关于kibana使用教程请访问：

<https://www.elastic.co/guide/en/elasticsearch/reference/6.0/index.html>

搜索时可能用到的主机名称：

020231 正式brand

020232 正式mobile2b

020233 正式通用版

020234 正式公共服务

020235 正式fullsearch

020236 正式mobile2c

020237 正式housedraw

020238 正式商家后台

020239 正式微信小程序（暂不可用）

030131 集成brand

030132 集成mobile2b

030133 集成通用版

030134 集成公共服务

030135 集成fullsearch

030136 集成mobile2c

030137 集成housedraw

030138 集成商家后台

030139 集成微信小程序