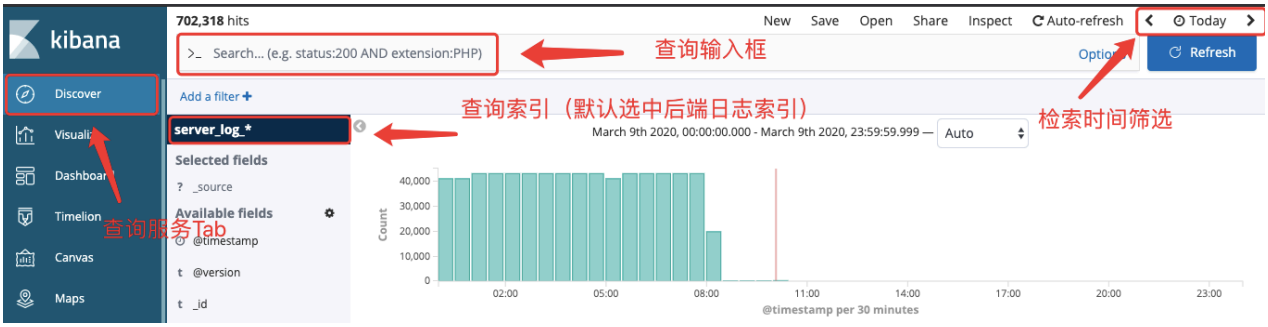
背景

后端提供众媒整体服务，每天产生大量服务日志，希望数据平台能提供一个索引和检索的服务。数据平台承接此需求，将后端产生的日志（除埋点上报日志外）通过Filebeat做搜集，实时传给LogStash写入到Elasticsearch中，通过Kibana提供日志的检索查询，后续部分主要介绍如何使用Kibana查询用法。

Kibana查询用法

1、选择要查询的索引和检索日志时间段



2、在查询输入框中发起检索查询

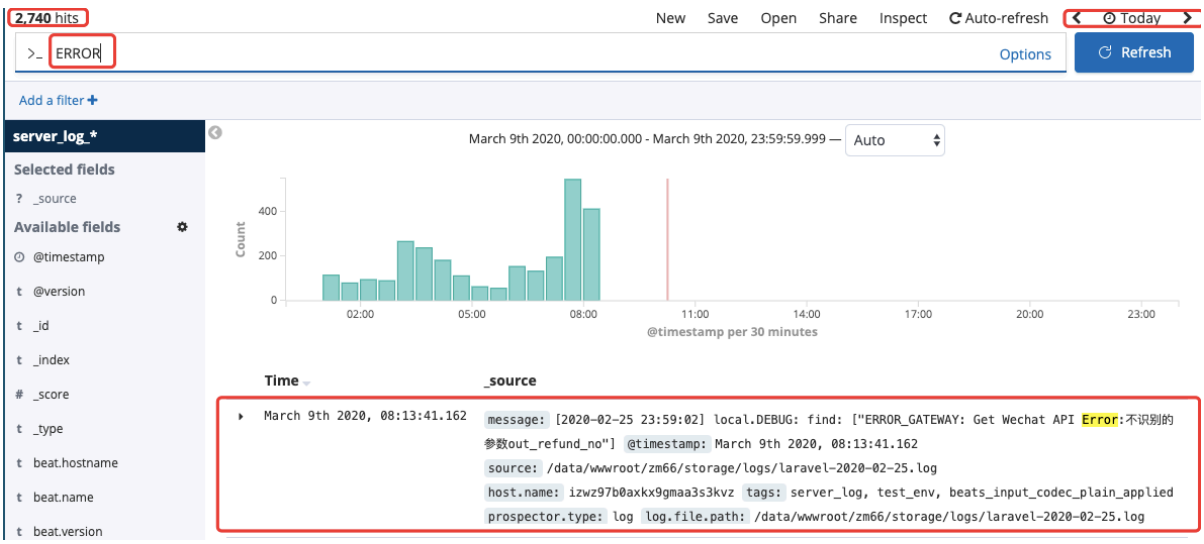
> Kibana支持的查询语法有两种：
>
> 基于Lucene查询语法的标准查询语句 和 基于json格式的ES查询DSL语句
>
> 本文档只介绍前者，Kibana的标准查询语句的语法

- 文本检索

  输入关键词，会查询文档所有字段的内容，匹配到的都会检索出来

  e.g. `ERROR`

  检索结果如下：

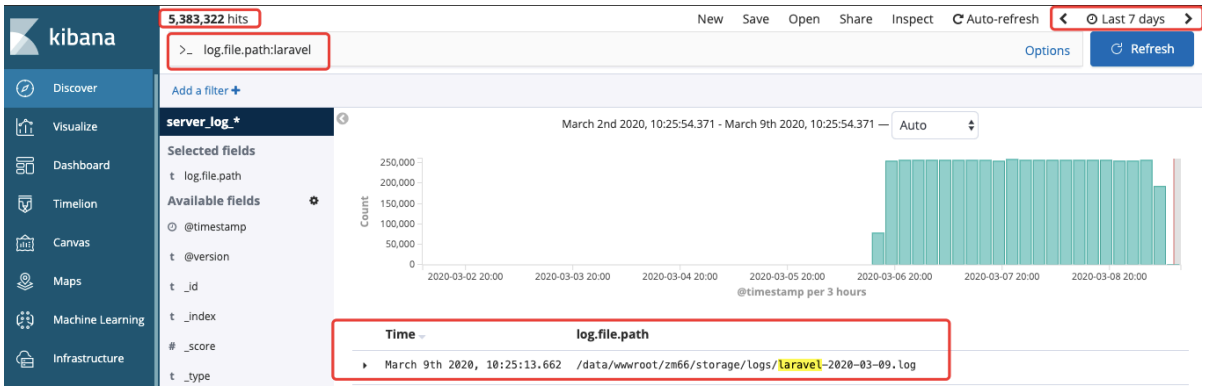


- 指定字段的文本检索

  日志的每一条记录都有固定的字段，可以在查询页左侧列表`Available fields`查看，指定字段和检索内容，将只在指定字段内检索内容匹配的记录。

  e.g. `log.file.path:laravel`

  检索结果如下:

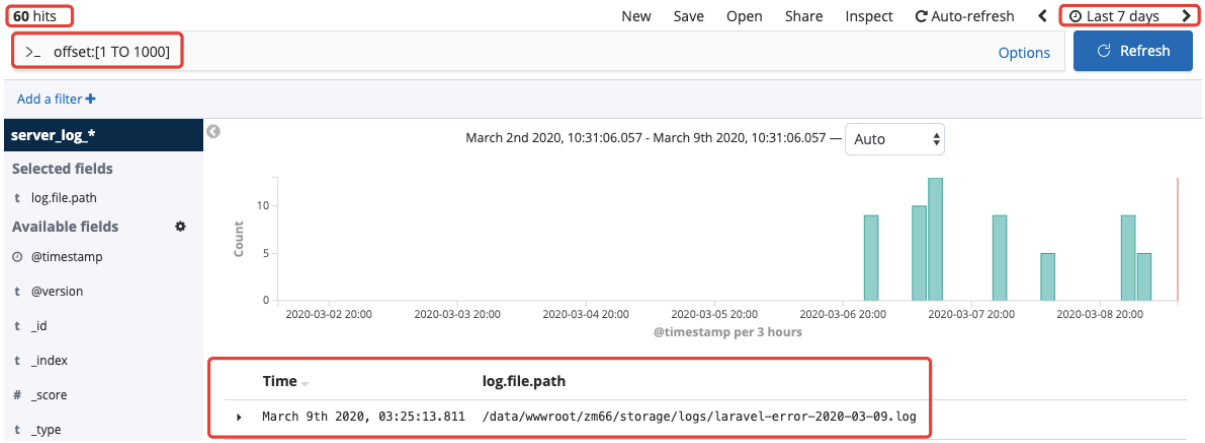


- 范围值检索

  有时要查询的不是固定的文本，而是一个范围的值，可以使用如下的范围查询语法:

  `[START_VALUE TO END_VALUE]`

  e.g. `offset:[1 TO 1000]`



- 查询条件组合

  要做更复杂的查询，可以使用布尔操作符组合查询条件

  支持的布尔操作符: `AND` `OR` `NOT`

  e.g. `log.file.path:(alipay OR wechat) AND message:yansongda.pay.DEBUG`

- 模糊查询

  可以使用通配符做模糊查询（通配符不能放在查询的第一个字符）

e.g. `message:yansongda.pay.*`

参考

Apache Lucene - Query Parser Syntax