## 概述

日志分析主要包括系统日志、应用程序日志和安全日志。系统运维和开发人员可以通过日志了解服务器软硬件信息、检查配置过程中的错误及错误发生的原因。经常分析日志可以了解服务器的负荷，性能安全性，从而及时采取措施纠正错误。通常，日志被分散的储存不同的设备上，依次登录每台机器查阅日志的传统方法很繁琐并且效率低下。所以将日志集中管理成为运维工作必不可少的手段。

开源实时日志分析框架ELK是当前最流行的日志管理架构之一，能够实现对日志集中管理，并提供全文检索功能，组件kibana提供丰富的展示方法。ELK能够起到实时系统监测、应用监测、网络监测、事件管理和发现bug等作用。

## 建设目的

为运维人员提供日志信息，实时了解操作系统、业务、数据库的运行情况。提高解决故障的效率，提升故障预警能力。

为开发人员排查故障提供日志查看和搜索功能。

## ELK简介

ELK是Elasticsearch、Logstash、Kibana的简称。

* Elasticsearch是实时全文搜索和分析引擎，提供搜集、分析、存储数据三大功能；是一套开放REST和[Java](http://lib.csdn.net/base/17) API等结构提供高效搜索功能，可扩展的分布式系统。它构建于Apache Lucene搜索引擎库之上。
* Logstash是一个用来搜集、分析、过滤日志的工具。它支持几乎任何类型的日志，包括系统日志、错误日志和自定义应用程序日志。它可以从许多来源接收日志，这些来源包括 syslog、消息传递（例如 RabbitMQ）和JMX，它能够以多种方式输出数据，包括电子邮件、websockets和Elasticsearch。
* Kibana是一个基于Web的图形界面，用于搜索、分析和可视化存储在 Elasticsearch指标中的日志数据。它利用Elasticsearch的REST接口来检索数据，不仅允许用户创建他们自己的数据的定制仪表板视图，还允许他们以特殊的方式查询和过滤数据。
* Beats：包括filebeat和packetbeat，用来取代logstash-forward的轻量级日志代理，相对于logstash占用系统资源少。

## 日志类型

1. MySQL日志：包括MySQL错误、慢查询、MySQL methods、读写、流量。
2. Redis日志：
3. Nginx日志：按照固定格式输出的日志。
4. Tomcat日志：按照固定格式输出的日志。
5. 系统日志messages：整体系统信息，系统层错误、告警、信息等。
6. 系统日志secure：验证和授权方面信息。

## 部署架构

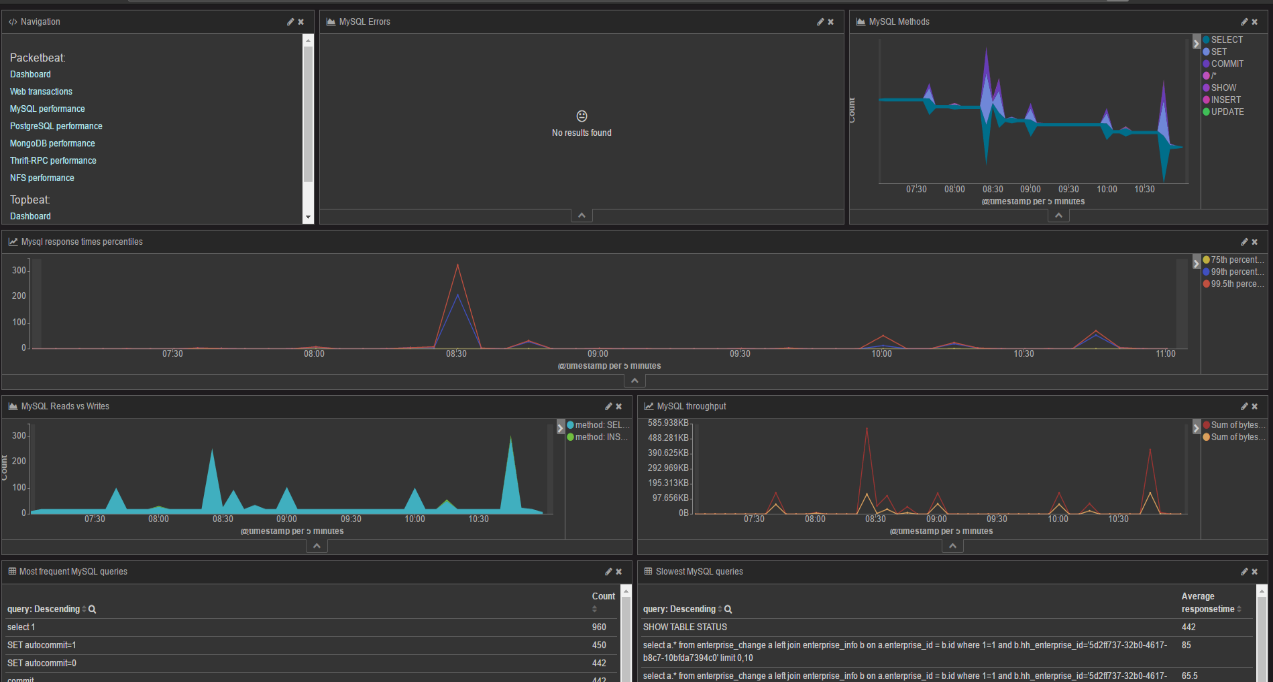
由于当前日志量不大，所以暂时没有使用redis或kafka等队列工具，也没有使用集群。后续可以根据实际负载情况加入缓存和集群。具体部署方案如下：

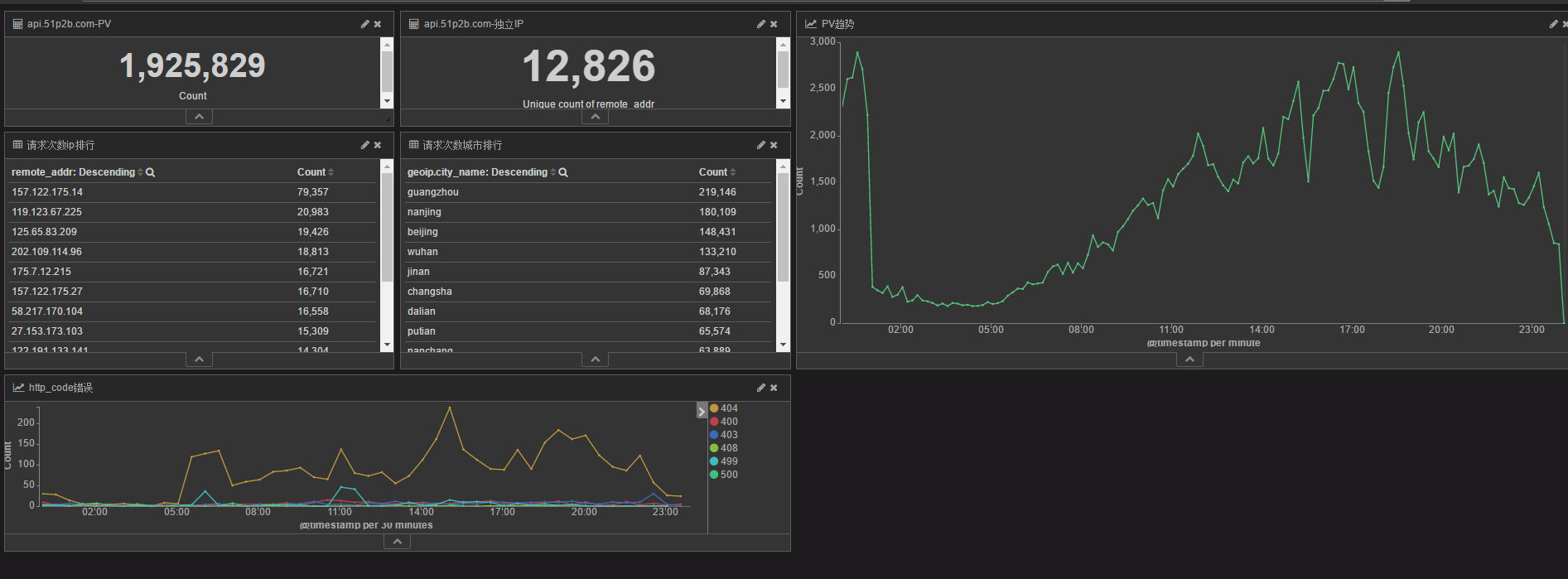
1. 使用filebeat收集所有服务器的/var/log/messages和/var/log/secure日志，并发送给logstash集中转发给elasticsearch。
2. 使用filebeat收集负载均衡访问和WEB服务器的Nginx日志和tomcat日志。并发送给logstash 匹配、解析后发送给elasticsearch。
3. 使用packetbeat收集数据库MySQL和redis日志，直接发送给elasticsearch。
4. 使用kibana做为日志展示与搜索的工具。

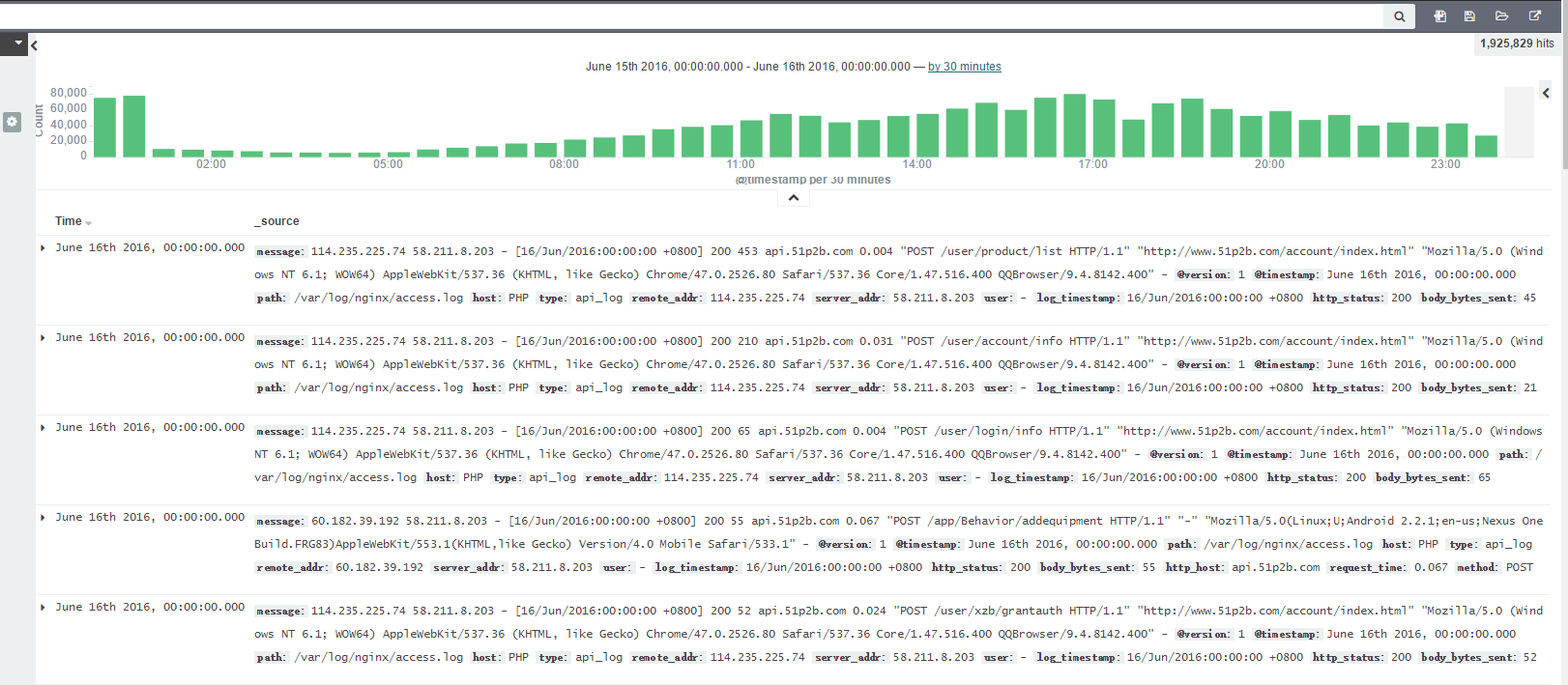
架构图：



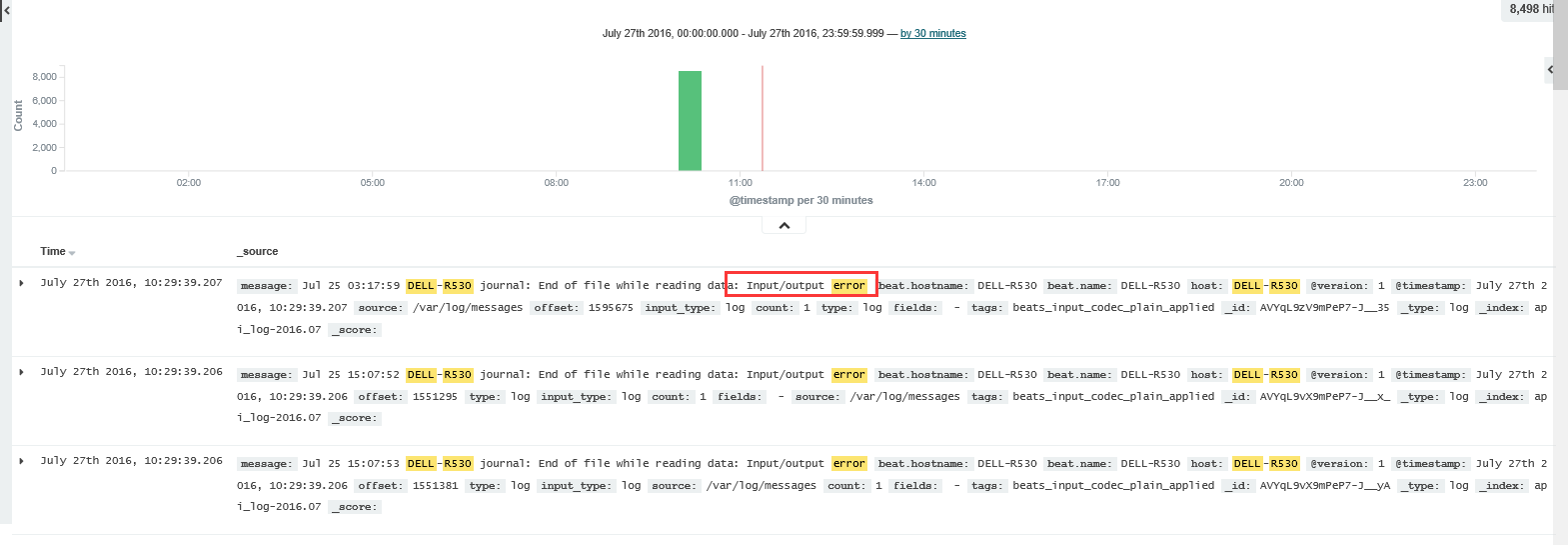
## 效果展示

MySQL日志仪表盘

Nginx日志仪表盘

Nginx日志

系统报错日志



## 部署文档

|  |  |  |  |
| --- | --- | --- | --- |
| IP | 域名 | 组件 | 日志文件 |
| 10.10.10.199 | old.71dai.com | filebeat | /usr/local/nginx/logs/access.log |
| 10.10.10.200 | Web03 | filebeat | /var/log/messages |
| 10.10.10.206 | qyd.test.71dai.com | filebeat | /usr/local/syqyd2\_809/log/catalina.out |
| 10.10.20.20 | mysql | packetbeat | 9032端口 日志 |
| 10.10.10.210 | kibana.test.com.cn | ELK | /var/log/message |

## 示例：

修改hosts文件，增加域名与IP的映射关系

10.10.10.201 kibana.test.com.cn

之后即可通过如下URL访问：

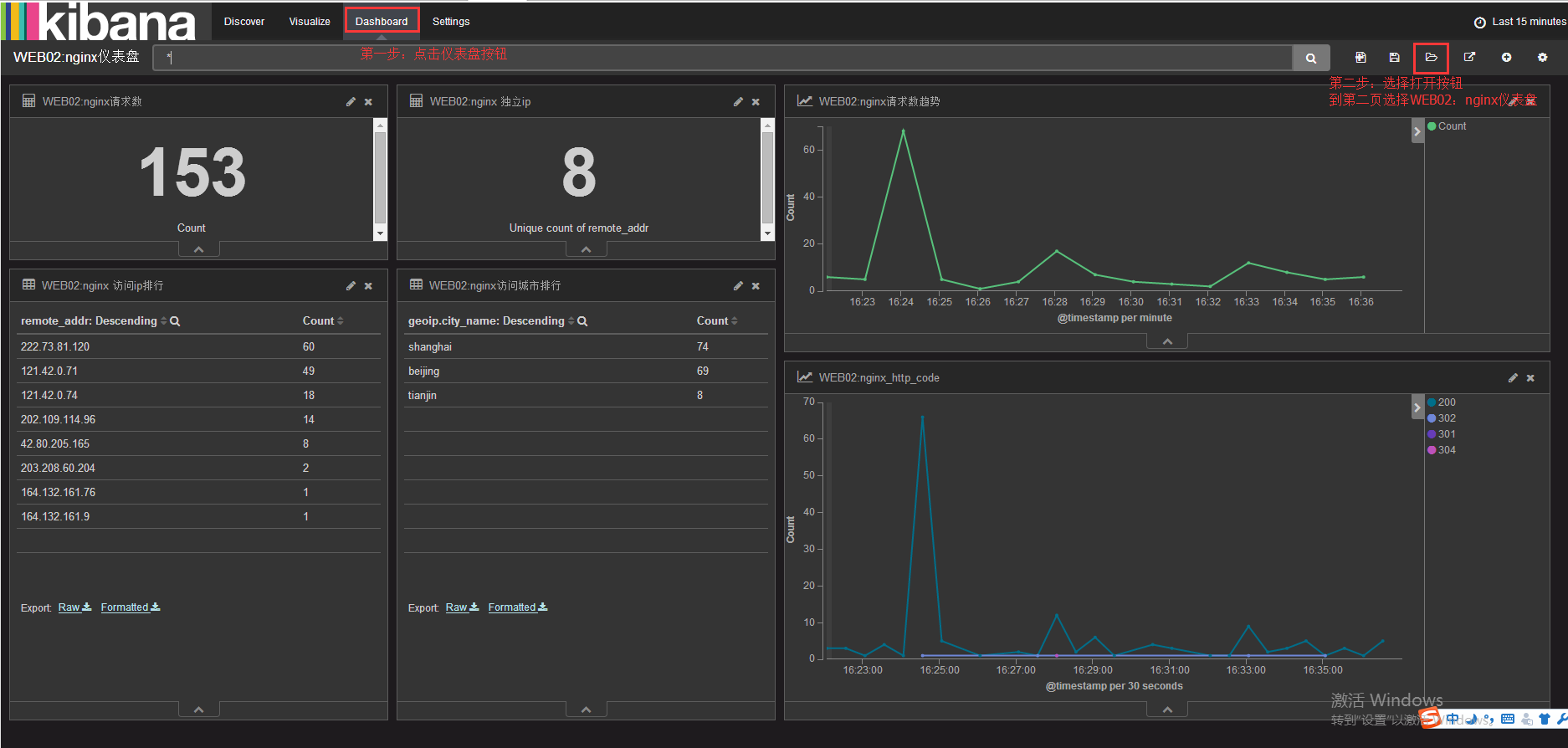
[http://kibana.test.com.cn](http://kibana.51p2b.com)

本例采集了不同服务器的nginx日志，tomcat日志，mysql日志，系统日志messages。当然EKL可以采集任何日志，只要想要的都可以通过ELK收集和展现。

### Nginx仪表盘

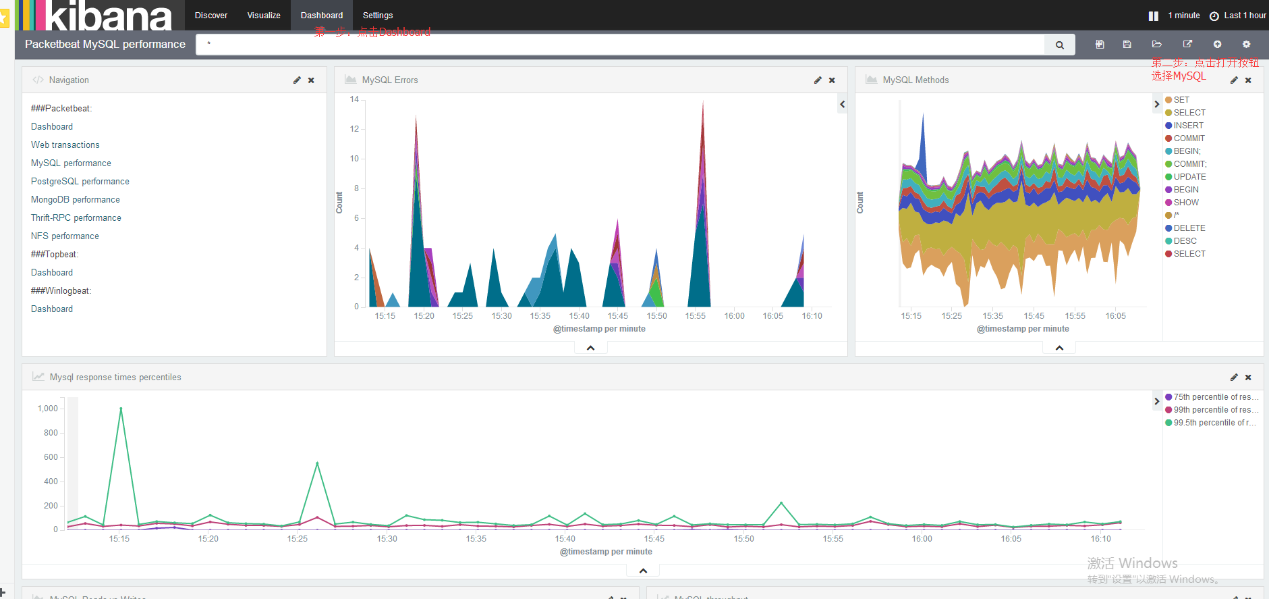
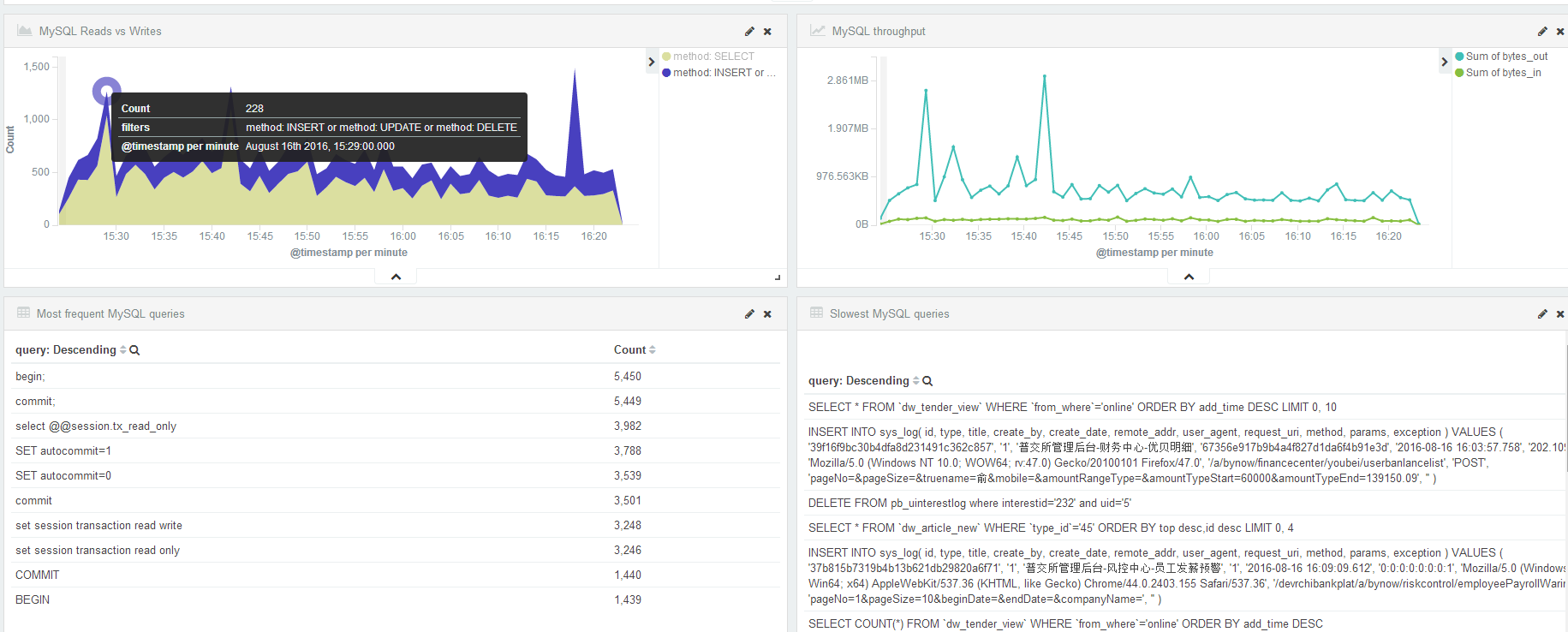
仪表盘如下截屏：点击仪表盘按钮”Dashboard”，点打开按钮，选择要打开的仪表盘名称。

可查看的信息包括：请求数、独立ip数、请求数趋势、独立ip排行、访问城市排行、http\_code趋势。



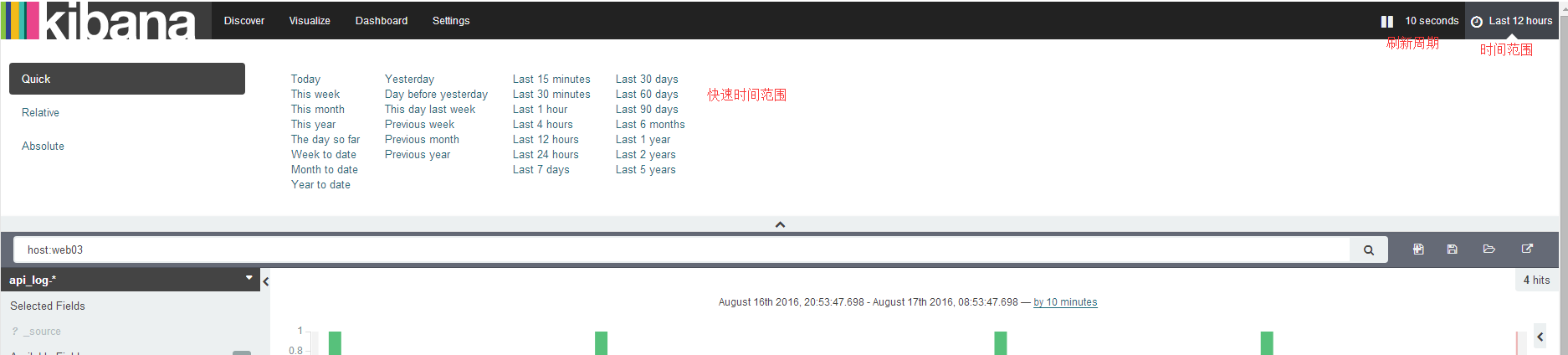
### MySQL仪表盘

可查看的信息包括：错误、方法、读写次数、出入流量、频繁的查询次数排行、慢查询。



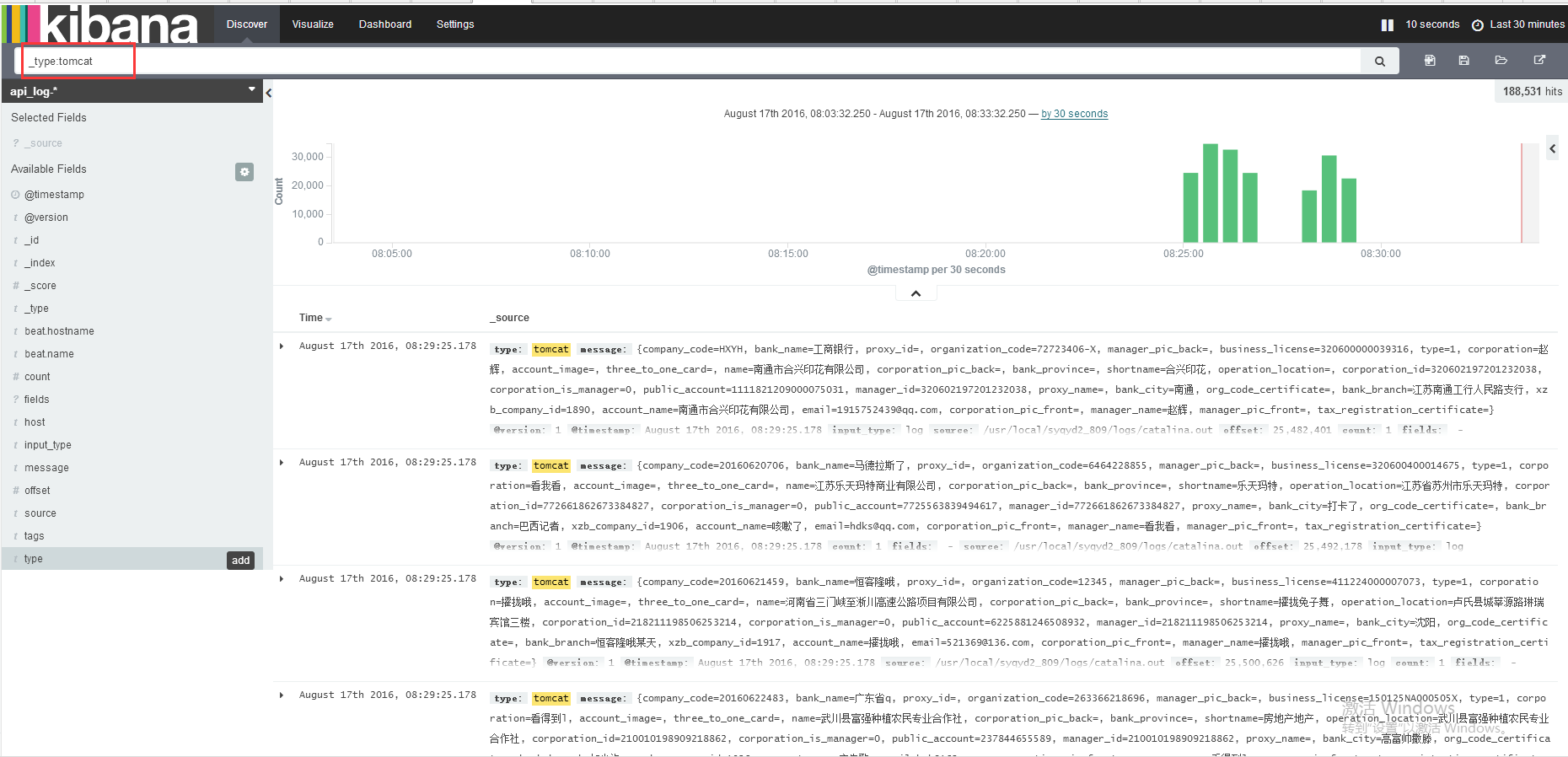
### Discover 实时查看搜索日志

首先在搜索日志界面的右上角可以选择要搜索的时间范围，也可以设置页面自动刷新时间。



**Tomcat日志：**

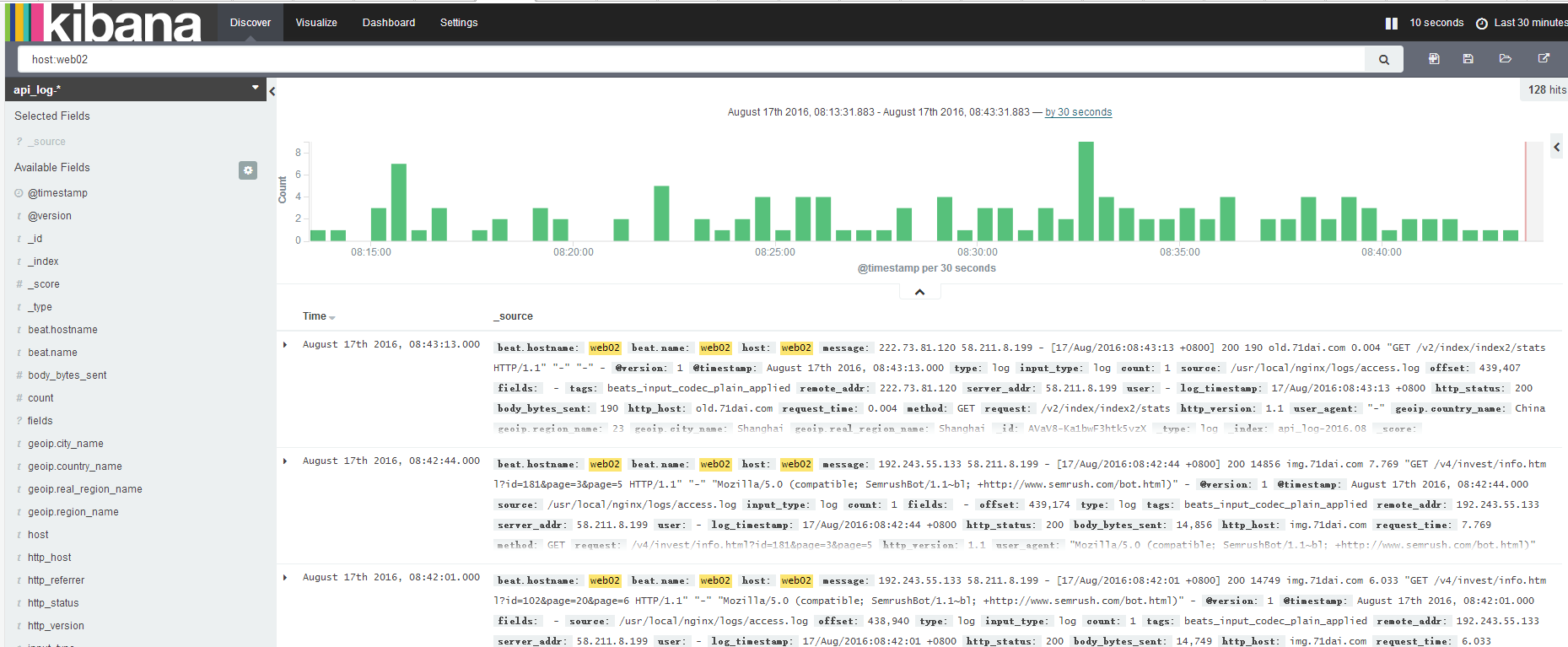
Tomcat日志采集了企易贷测试环境10.10.10.206 qyd.test.71dai.com的访问日志，在discover菜单可以实时查看和搜索。如在搜索栏输入：\_type:tomcat；或者输入beat.hostname:TEST-QYD



**Nginx日志**

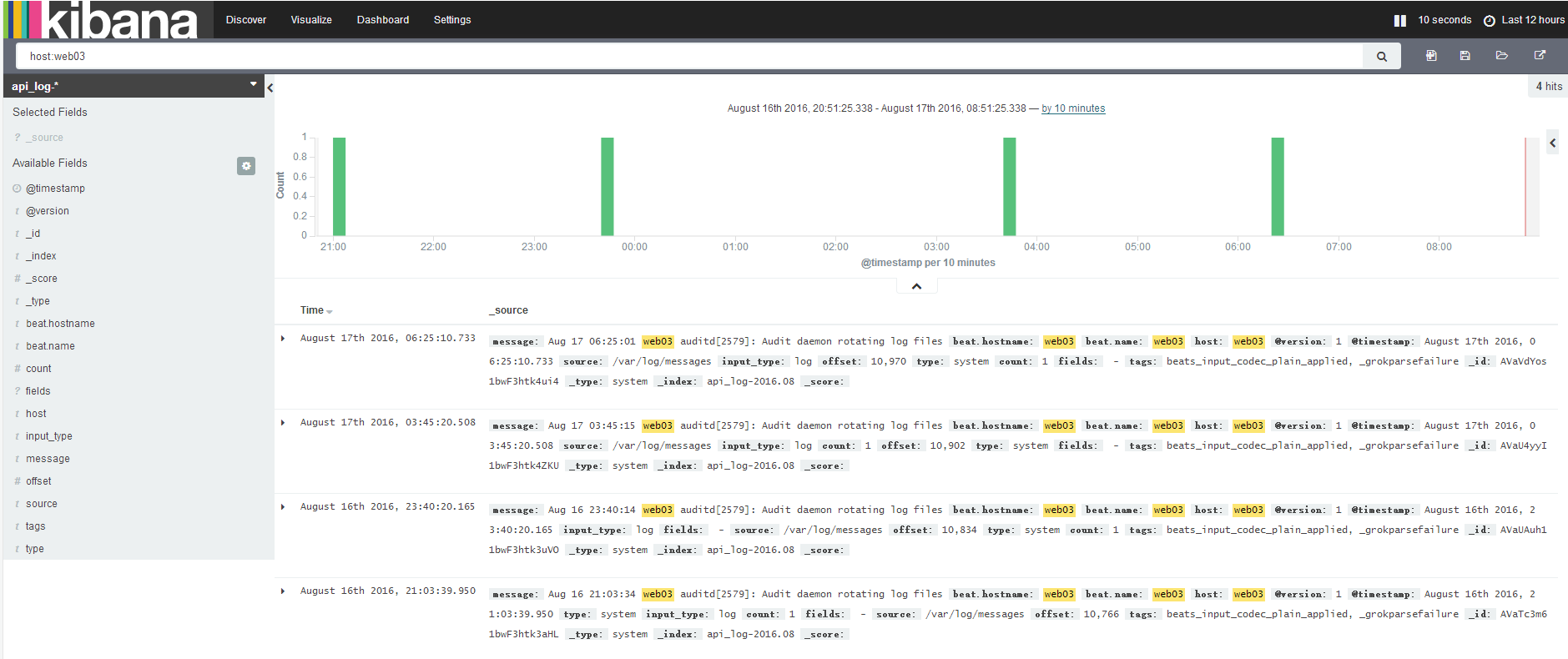
Nginx日志采集的是WEB02的nginx日志

在搜索栏输入：host:web02即可查看日志，也可以输入想要搜索的任何关键字。如搜某一特定ip地址的日志，或者某个城市访问的日志。



**系统messages日志**

本例采集了web03的/var/log/messages日志，可以输入host:web03显示web03的messages日志，



## 使用Shield实现权限控制

使用shield插件可以实现不同用户只允许访问特定日志。

\*注：测试环境没加权限控制。