QQ截图20151201103408.png

**ELK日志服务器普通用户使用手册**

信息技术中心

2016年11月13日

[1. 前言 4](#_Toc467595562)

[2． 登录使用ELK日志服务器 5](#_Toc467595563)

[2.1 ELK web 登录 5](#_Toc467595564)

[2.1 选择应用日志 5](#_Toc467595565)

[2.2 搜索查看应用日志 6](#_Toc467595566)

**文档修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 版本 | 描述信息 | 作者 |
| 2016-11-13 | 1.0 | 新建 | 陈俊彦 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 前言

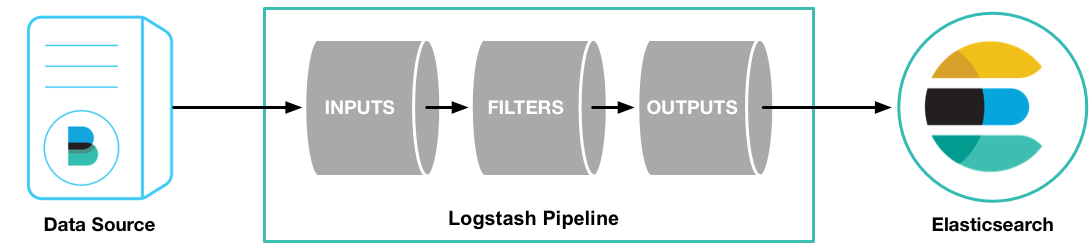
ELK 由 ElasticSearch 、 Logstash 和 Kiabana 三个开源工具组成。官方网站：https://www.elastic.co

其中的3个软件是：

Elasticsearch 是个开源分布式搜索引擎，它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制， restful 风格接口，多数据源，自动搜索负载等。

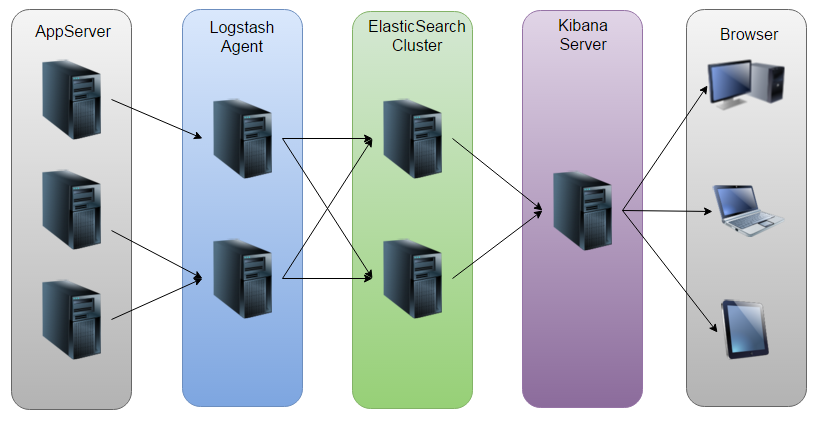
Logstash 是一个完全开源的工具，他可以对你的日志进行收集、分析，并将其存储供以后使用（如，搜索）。

A Logstash pipeline has two required elements, input and output, and one optional element,filter. The input plugins consume data from a source, the filter plugins modify the data as you specify, and the output plugins write the data to a destination.



kibana 也是一个开源和免费的工具，他 Kibana 可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助您汇总、分析和搜索重要数据日志

ELK工作的原理图：



如图：Logstash收集AppServer产生的Log，并存放到ElasticSearch集群中，而Kibana则从ES集群中查询数据生成图表，再返回给Browser。

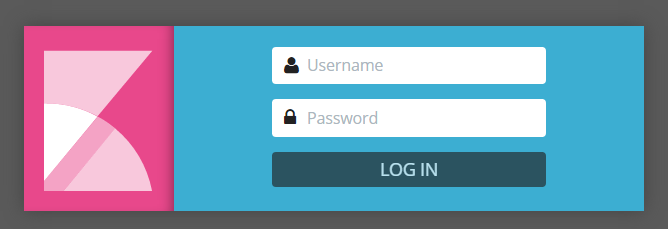
# 2． 登录使用ELK日志服务器

## 2.1 ELK web 登录

ELK website如下

<http://10.163.36.21:5601/>

在弹出的对话框输入相应用户名和密码



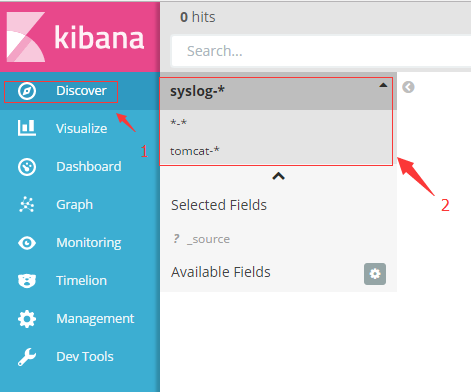
## 2.1 选择应用日志

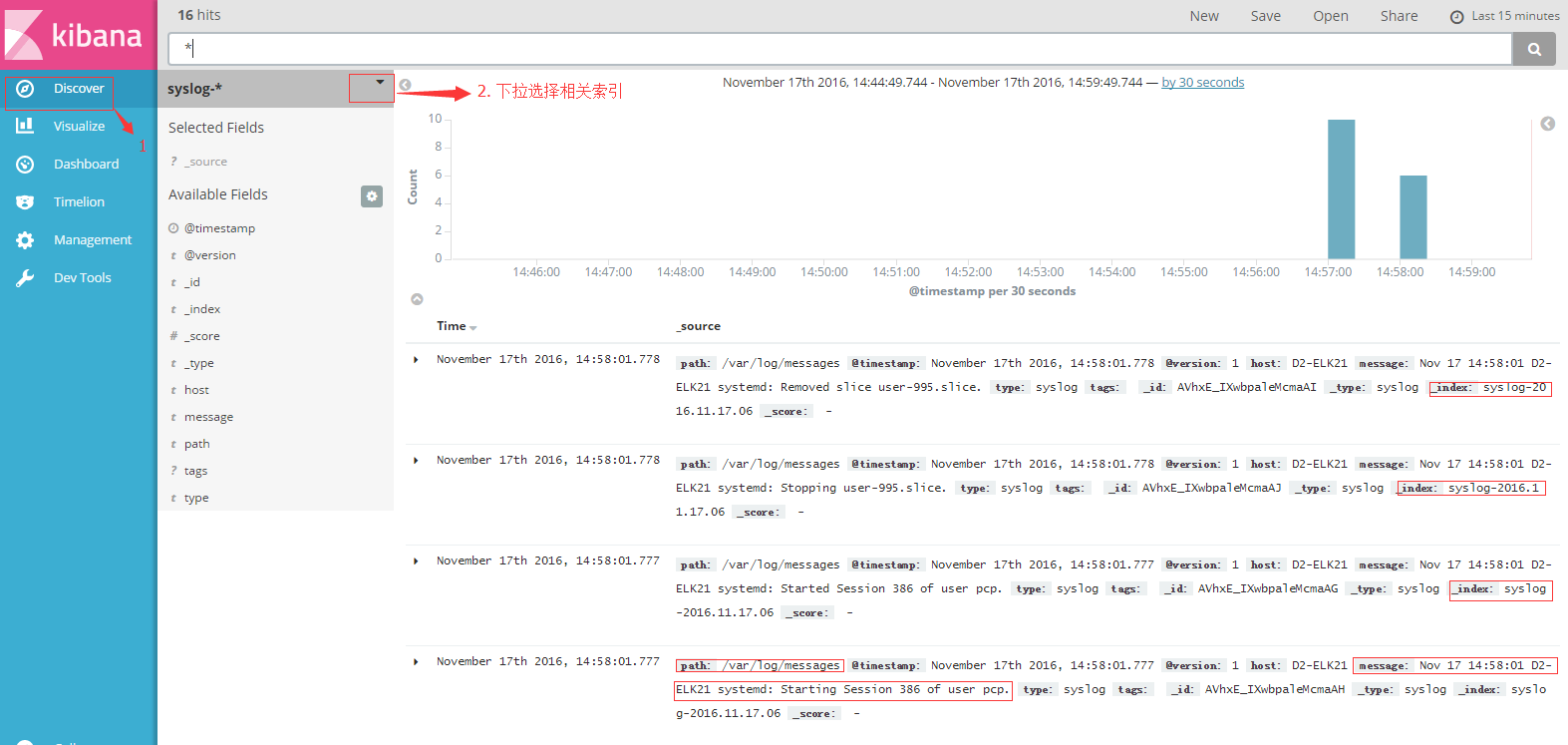
登录主界面后

在”Discovery” 下拉选择syslog-\* ，查看相关系统日志

在”Discovery” 下拉选择tomcat-\* ，查看相关Tomcat应用日志

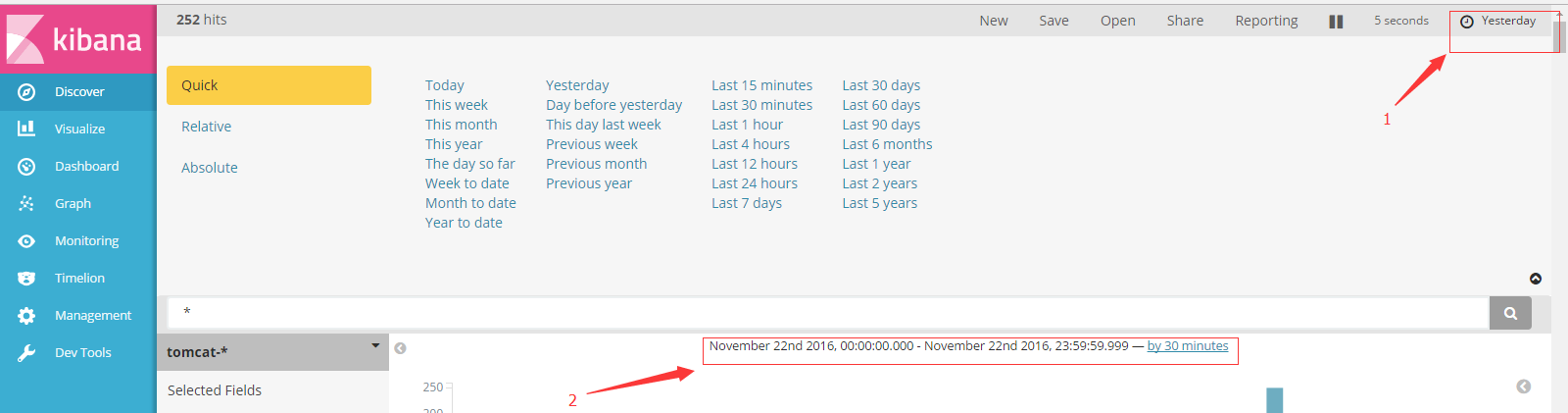
如有其他日志没有显示，请联系运维人员给予配置



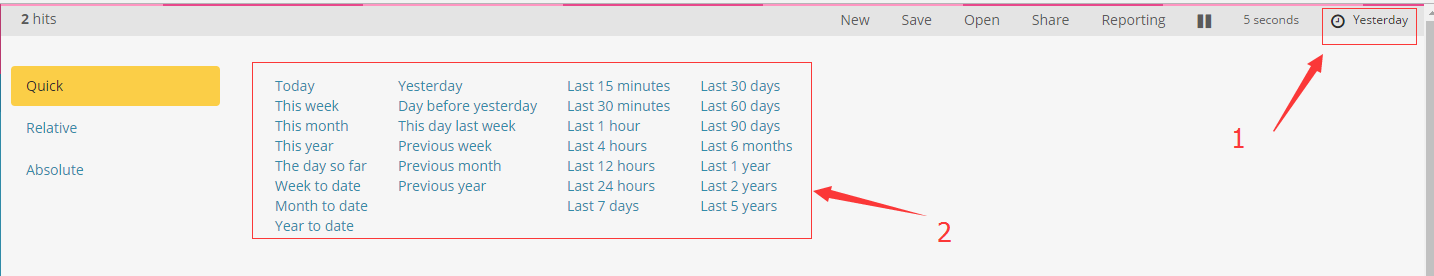


## 2.2 查看不同时间点的应用日志

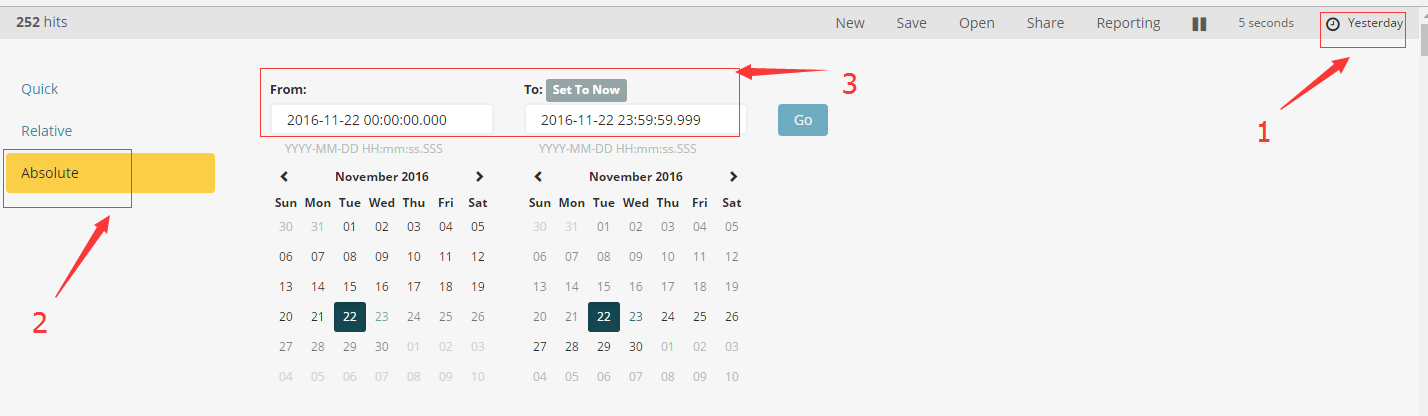
点击界面右上角的时间段，选择合适的时间查看应用日志



选择快速定义的时间段

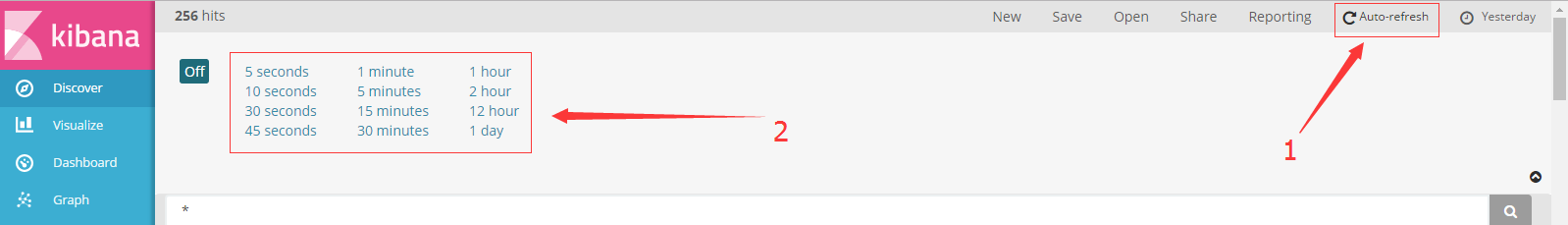


选择自定义的时间段



## 2.3 自动更新界面获取最新应用日志

点击界面右上角的时间段，选择Auto-refresh



选择界面自动刷新的频率

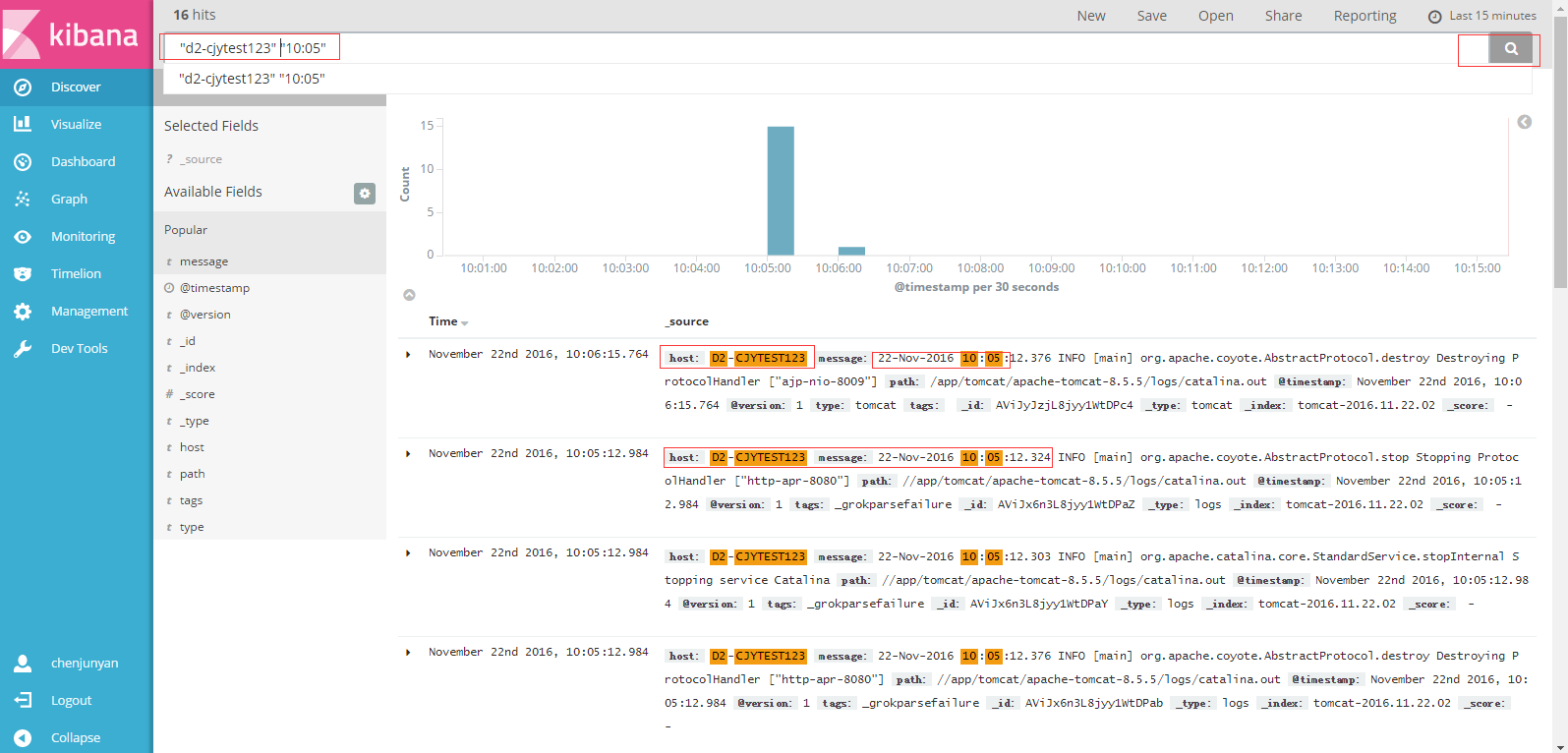


## 2.4 搜索查看应用日志

在搜索框，输入相关内容，类如主机名或者日志时间（需要双引号定义范围）

"d2-cjytest123" "10:05"

点击搜索后，相关内容就会如下图显示



在想要看的日志，点击展示三角符号，查看详细信息

