**分布式ELK平台**

基础知识

ELK是什么？

sina、饿了么、携程、华为、美团、这些公司都在使用elk。ELK不是一个软件，而是一套解决方案，是三个软件产品的首字母缩写

Elasticsearch：负责日志检索和储存

logstash：负责日志的收集和分析、处理

kibana：负责日志的可视化

这三款软件都是开源软件，通常是配合使用，而且又先后归于Elastic.co公司名下，故被简称为ELK

ELK能做什么

ELK组件在海量日志之系统的运维中，课用于解决：

分布式日志数据集中式查询和管理

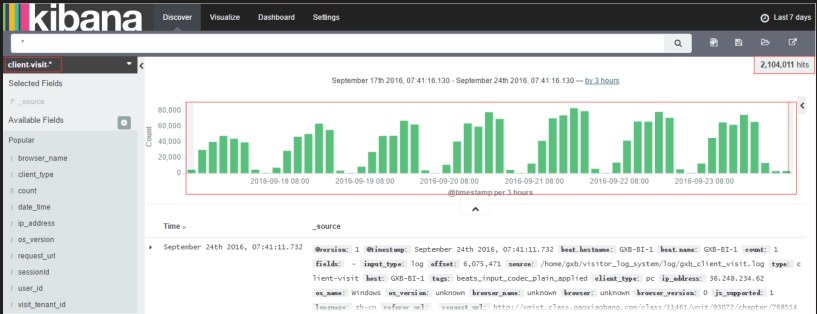
系统监控，包含系统硬件和应用各个组件的监控

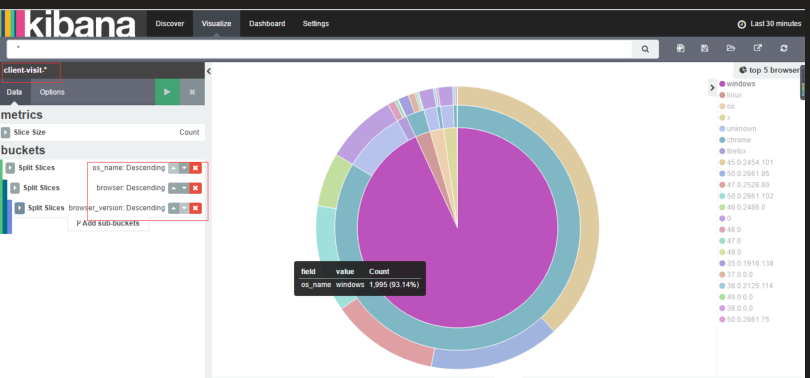
故障排查

安全信息喝事件管理

报表功能

ELK是什么样子的







elasticsearch

elasticsearch部分

elasticsearch是一个基于lucene的搜索服务器，它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful API的web接口

elasticsearch是用java开发的，并作为apache许可条件下的开放源码发布，是当前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索，稳定，可靠，快速，安装使用方便