Win7 搭建 ELKB 平台分析 nginx 日志

作者：Xtianduo4
原文链接：https://ld246.com/article/1539101820043
来源网站：链滴

前言

生产环境上应用在多台机器上分布式部署，分布式在提高性能的同时也带来了很多问题，其中一个问就是日志分散导致定位问题变得繁琐困难。尤其项目采用微服务架构、容器化部署时，这个问题变得加明显。今天小编以nginx日志为例，通过搭建ELKB平台，实现nginx日志归集，日志分析。

ELKB是什么

E:Elasticsearch 是一个基于Lucene的分布式搜索和分析引擎，具有高可伸缩、高可靠和易管理等特。支持对大容量的数据进行接近实时的存储、搜索和分析操作。

L:Logstash 是开源的服务器端数据处理管道，能够同时从多个来源采集数据，过滤转换数据，然后存到用户指定的位置。

K:Kibana是一个数据分析和可视化平台。一般与 Elasticsearch 配合使用，对其中数据进行搜索、分和图表方式展示;

B:Beats 集合了多种单一用途数据采集器，分别是：Filebeat（搜集日志文件）；Metricbeat（搜集标数据）；Packetbeat（搜集网络数据）；Winlogbeat（搜集 Windows 事件日志数据）；Auditbeat（搜集审计数据）；Heartbeat（搜集运行监控数据）。这些采集器安装后可用作轻量型代理，从成上千或成千上万台机器向 Logstash 或 Elasticsearch 发送数据。

未完待续