地震科学进展
PROGRESS IN EARTHQUAKE SCIENCES
ISSN 2096-7780 CN 10-1665/P

基于ELK组件的日志系统在地震行业中的应用

边鹏飞，郝　丽

Application of ELK component-based log system in the seismic industry

Bian Pengfei and Hao Li

在线阅读 View online: https://doi.org/10.19987/j.dzkxjz.2023-121

边鹏飞, 郝丽. 基于 ELK 组件的日志系统在地震行业中的应用 [J]. 地震科学进展, 2023, 53(12): 576-580. doi:10.19987/j.dzkxjz.2023-121
Bian P F, Hao L. Application of ELK component-based log system in the seismic industry[J]. Progress in Earthquake Sciences, 2023, 53(12): 576-580. doi:10.19987/j.dzkxjz.2023-121

基于 ELK 组件的日志系统在地震行业中的应用*

边鹏飞※ 郝 丽

（河北省地震局，河北石家庄 050021）

摘要 网络设备、网络安全设备以及业务应用系统的日志在网络运维中是排除设备系统故障的一个重要数据资源。然而大量日志数据分散存储在不同的设备中，不便于查看和使用，难以满足网络运维中快速发现问题、定位问题和解决问题的要求。因此，为了提高业务人员的网络运维能力，建设一个统一的日志收集、存储、处理系统很有必要。本文介绍了一套以 ELK 开源组件搭建的日志系统，并在地震行业网中进行了实际应用，实现了地震行业网内业务系统、安全设备、网络设备等日志的实时收集、存储、处理和展示功能。对实现细节进行了详细阐述，为该架构的推广应用提供了典型示范。

关键词 网络运维；ELK；日志系统；地震

中图分类号： P315 **文献标识码：** A **文章编号：** 2096-7780(2023)12-0576-05

doi： 10.19987/j.dzkxjz.2023-121

Application of ELK component-based log system in the seismic industry

Bian Pengfei, Hao Li

(Hebei Earthquake Agency, Hebei Shijiazhuang 050021, China)

Abstract The logs of network devices, network security devices, and business application systems are an important data resource for troubleshooting equipment and system failures in network operations and maintenance. However, a large amount of log data is stored in different devices in a decentralized manner, which makes it difficult to view and use, and it is difficult to meet the requirements of quickly identifying, locating, and solving problems in network operation and maintenance. Therefore, in order to improve the network operation and maintenance capabilities of business personnel, it is necessary to build a unified log collection, storage, and processing system. This article introduces a log system built with ELK open source components, which has been applied in the earthquake industry network to achieve real-time collection, storage, processing, and display of logs from business systems, security devices, and network devices in the seismological industry network. The implementation details are elaborated in detail, providing a typical demonstration for the promotion and application of this architecture.

Keywords network operation and maintenance; ELK; log system; earthquake

0 引言

河北省地震行业网络系统在“十五”时期进行了大规模扩建，成为了地震行业重要的数据传输、共享和发布的基础平台。但随着网络规模的不断扩大，网络安全问题日益突出[1]。及时查看设备、系统及业

* 收稿日期：2023-09-05；采用日期：2023-11-02。
※ 通信作者：边鹏飞（1981-），男，高级工程师，主要从事地震应急信息、灾害评估及信息化等研究。E-mail：bianpf@hbdzj.gov.cn。

务应用日志，快速地发现问题和定位故障，是保障网络及业务系统安全正常运行的重要手段之一。然而大量日志信息分散存储在各种设备中，并且需要以人工命令查看，效率低，难以满足快速发现和定位故障的要求。ELK 日志系统是一种重要的解决方案，它通过集中收集、存储和分析大规模的日志数据，帮助运维人员更好地利用这些数据。本文将详细介绍 ELK 日志系统的组成部分及其功能，并重点探讨其在地震行业网中的应用。

1　相关研究

前人对 ELK 技术栈的研究主要集中在架构、原理和技术细节等方面，也有一些研究关注 ELK 日志系统在不同领域的应用。例如，Ngo 等[2]对环境数据收集、存储和分析进行了研究。龚锦红等[3]探讨了 ELK 在高校校园网的应用。李书达等[4]研究了 ELK 在企业运维中的应用。珠海华润银行日志管理与分析平台课题组等[5]探讨了 ELK 在金融系统的应用。谢磊等[6]探讨了 ELK 日志系统在电网系统的应用。然而，目前关于 ELK 日志系统在地震行业网中的应用研究还相对较少。因此，本文旨在通过实验设计和真实数据集的测试，对 ELK 日志系统在地震行业网中的应用进行全面的评估和分析。

2　系统架构设计

2.1　需求分析

结合河北省地震行业网实际环境，日志系统应具有以下功能：

（1）能够实时收集行业网中网络设备、安全设备、业务系统等产生的各种日志数据；

（2）能够将收集到的大量数据进行存储；

（3）能够对收集的日志数据进行统计分析及可视化展示。

2.2　日志系统架构

图 1 展示了 ELK 日志系统的基本架构，各组成部分详解如下。

2.2.1　日志采集

日志的集中存储和分析展示首先要解决日志收集问题，大量的网络设备、安全设备以及应用系统的日志都分布在不同的设备上，需要通过 Filebeat 和 Logstash 搭建日志的收集模块。

Filebeat 是一个使用 GO 语言开发的文件型日志采集器。在启动时，其 prospector 组件会监控指定的日志文件路径或某个特定文件。每个日志文件都会

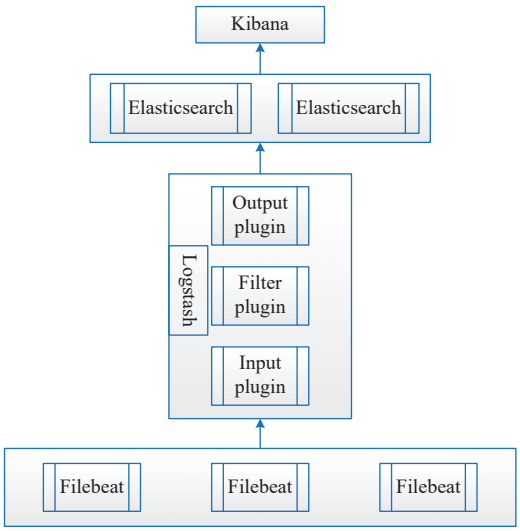

图 1　系统架构图

Fig. 1　System architecture diagram

启动一个 harvester，harvester 会根据文件的最后读取位置的偏移量来判断是否有新的日志内容。如果有新内容，它会将该内容发送至后台的 libbeat 程序。

在日志采集中，Logstash 起到管道和桥梁的作用，由 3 个主要部分组成：输入（Input）、过滤（Filter）和输出（Output）。Input 负责指定日志数据的采集源，Logstash 支持多种数据格式，包括 File、Syslog、Redis、Beats 等。Filter 是核心组件，负责对日志进行清洗和解析。Output 用于指定数据的输出目的地，通常选择的是 Elasticsearch。

2.2.2　日志存储

日志存储后还需要具有可扩展性才能够满足不断增长的需求，并且能够实现快速检索大量的日志数据。因此需要利用 Elasticsearch 搭建日志系统的存储和搜索分析模块。

Elasticsearch 是一个基于 Lucene 的搜索引擎，具有分布式、可扩展、高可靠性和 RESTful API 等特点。在 Elasticsearch 中，数据以索引的形式存储，每个索引包含类型和文档。索引、类型和文档的概念与关系型数据库中的数据库、表和记录类似。

2.2.3　日志可视化

为了便于运维人员使用，日志系统还需具备友好的日志分析及展示界面。需要通过 Kibana 将 Elasticsearch 中的数据以图表、表格等形式展示出来。

Kibana 是一款图形展示软件，它提供了发现功能，允许用户使用 Lucene 语句或 Query DSL 语句来检索 Elasticsearch 中的数据。此外，Kibana 还内置了多种类型的图表，包括柱状图、饼图、条形图和热力地图等。这些图表可以通过可视化方式创建，然后创

建仪表盘，由用户自定义加载和显示哪些图表。

3 系统实现及应用

本节将详细介绍我们将如何使用 ELK 系统来处理地震行业网的日志数据。由于利用 Logstash 作为日志收集器这种架构资源占用要比 Filebeat 的整体资源占用高很多[7]。因此，我们利用 Filebeat 作为日志收集器。

3.1 基础环境搭建

本次日志系统的搭建采用一台安装了 CentOS7 操作系统的虚拟机作为基础平台。由于 Elasticsearch、Logstash 各组件需要依赖 JAVA 环境运行，因此在开始安装 ELK 之前，需要安装 JDK，并配置环境变量。建议选择安装比较稳定的版本，本次实施我们采用的是 JDK8 版本。

3.2 系统安装配置

（1）首先，使用 yum 方式安装 Elasticsearch，默认安装到/usr/share/elasticsearch 目录下。配置文件默认在/etc/elasticsearch/目录下。安装完成后，修改配置文件 elasticsearch.yml 中主机地址为服务器 IP 地址。Elasticsearch 默认的 http 端口为 9200，配置完成后可以通过使用 http://IP:9200/进行验证 Elasticsearch 服务是否正常，如果服务无法访问，需注意防火墙配置。

（2）使用 yum 方式安装 Kibana，默认安装在/opt/kibana 目录下，配置文件路径为/opt/kibana/config/kibana.yml。Kibana 默认端口为 5601。安装完成后修改配置文件中主机地址和 Elasticsearch 服务地址，由于本次采用同一台服务器，修改为同一个 IP 地址即可。如果使用多台服务器或集群时需根据实际情况修改配置文件中 IP 地址。

（3）使用 yum 方式安装 Logstash，默认安装在/opt/logstash 目录下，所有的配置均在/etc/logstash/conf.d 目录下。Input、Filter、Output 组件均在该目录下创建并配置。配置 Input 需要指定从哪里接收数据；Filter 可根据需求配置合适的参数对不必要的字段进行过滤；Output 需要指定 Logstash 将数据发送到何处，我们一般需配置输出到 Elasticsearch。需要注意的是，Logstash 配置文件使用 YAML 格式编写，需要遵循 YAML 语法规范，以避免配置错误或无法正常启动 Logstash。建议通过命令 service logstash configtest 运行检验配置文件正确性，如果显示 Configuration OK 则表示没有任何语法错误。

（4）在需采集日志的服务器上下载并安装合适的版本（例如 Windows、Linux 等），并进行相应的配置和优化。Linux 系统 Filebeat 默认安装后其配置文件为/etc/filebeat/filebeat.yml；Windows 系统默认安装在 C:\Program Files\Filebeat 目录下，修改配置文件将 Filebeat 收集的日志输出到 Logstash。同时还需要在 filebeat.yml 配置文件中设置连接 Elasticsearch 和 Kibana 的详细信息。

（5）配置示例：以下配置是通过 Filebeat 监控指定路径下的日志文件，并将数据发送到 Logstash 的监听端口。Logstash 接收到数据后，会进一步处理和过滤日志数据，并将其发送到 Elasticsearch 进行存储和搜索。

在 filebeat.yml 中添加以下配置，表示 filebeat 收集/var/log/目录下所有以.log 结尾的日志文件，输出到 logstash：

```
filebeat:
  prospectors:
    -
      paths:
        - "/var/log/*.log"
      document_type: syslog
output:
  logstash:
    bulk_max_size: 1024
    hosts:
      - " localhost:5044"
    tls:
      certificate_authorities:
        - /etc/pki/tls/certs/logstash-forwarder.crt
```

在 logstash.yml 中添加以下配置，表示接收 5044 端口数据，并通过过滤器对日志进行解析处理，输出到 Elasticsearch：

```
input {
  beats {
    port => 5044
  }
}
```

这里使用 beats input，监听在 5044 端口上。

```
# 添加其他过滤器插件来解析和处理日志数据
filter {
  #为 syslog 创建一个 filter
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}%{SYSLOGHOST:syslog_hostname}%{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
```

```
            add_field => ["received_at", "%{@timestamp}"]
            add_field => [ "received_from", "%{host}" ]
        }
        syslog_pri { }
        date {
            match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]
        }
    }
}
output {
    elasticsearch {
        hosts => ["localhost:9200"] # Elasticsearch 服务的地址
        index => "myindex" # 数据推送的索引名称
    }
}
```

4　实际使用效果

在地震行业网生产环境中部署了测试的日志系统，该系统成功实现了对各类操作系统、交换机、防火墙、服务器软硬件等多种日志数据的集中采集。同时还实现了日志数据过滤和日志数据分析展示功能。如图 2 所示，系统可通过事件判断对日志进行分类，并创建唯一索引以方便搜索。根据工作需求，系统过滤并展示日志信息。如图 3 所示，用户还可以在 Kibana 中创建数据统计分析图表和定制仪表板，

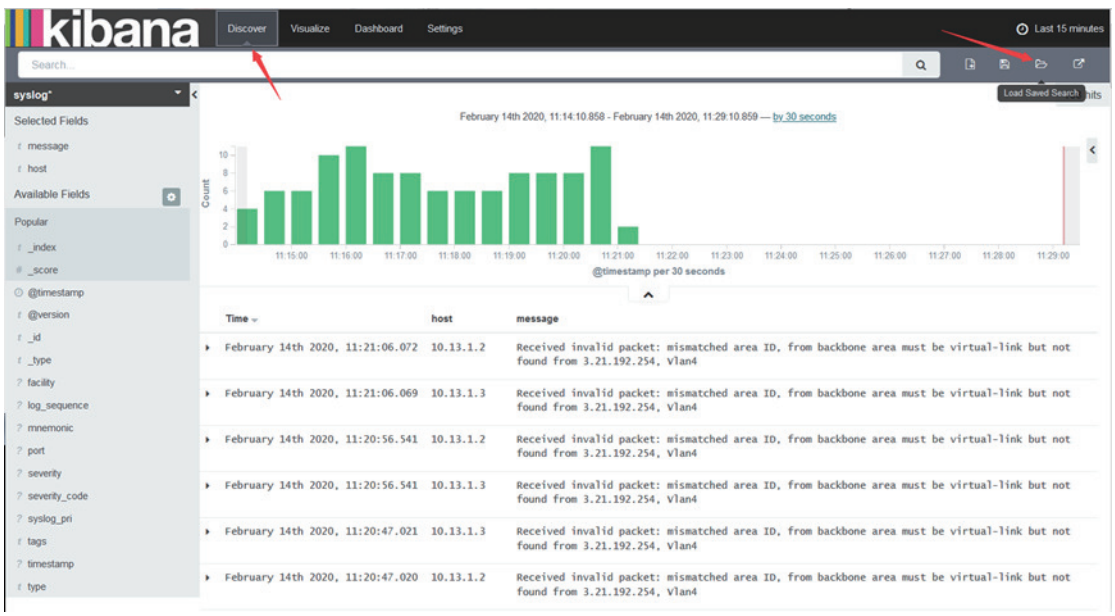

图 2　Kibana 搜索过滤日志信息界面截图

Fig. 2　Screenshot of Kibana search filter log information interface

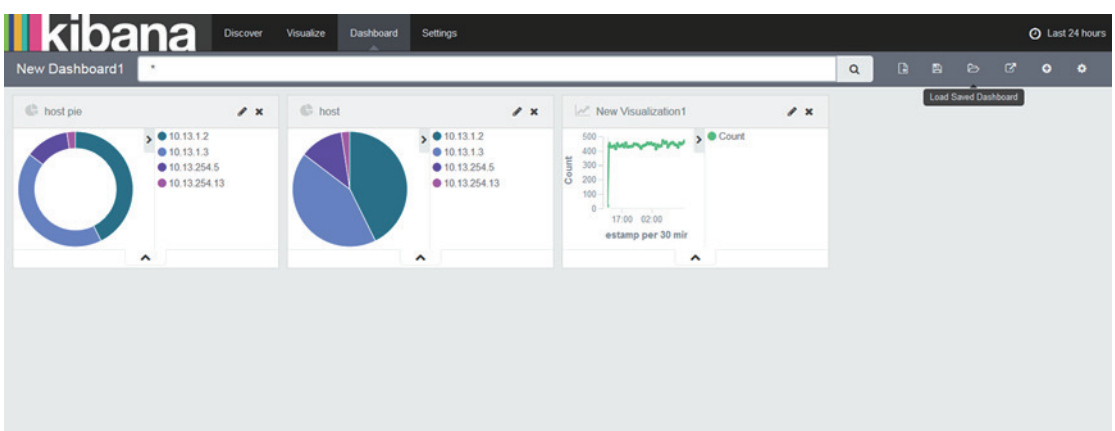

图 3　Kibana 创建统计图界面截图

Fig. 3　Screenshot of Kibana creating a statistical chart interface

以便于运维人员分析和查看。

5 结语

笔者介绍了利用 ELK 开源组件搭建的一套日志系统，并在河北地震行业网中进行了应用。通过实验验证了 ELK 日志系统的日志收集、处理以及展示功能。为地震行业网运维提供了一种实时监控和分析日志数据的解决方案，具有一定的推广应用价值。

参考文献

[1] 李刚，陈述新，赵洪壮，等. 地震行业网络安全全流量监控系统建设与应用 [J]. 地震工程学报，2018，40(增刊 1)：205-213
Li G，Chen S X，Zhao H Z，et al. Construction and application of a full-flow monitoring system for seismic network safety[J]. China Earthquake Engineering Journal，2018，40(S1)：205-213

[2] Ngo T T T，Sarramia D，Kang M A，et al. A new approach based on elk stack for the analysis and visualisation of geo-referenced sensor data[J]. SN Computer Science，2023，4(3)：241

[3] 龚锦红，凌仕勇. 基于 ELK 的高校 Web 日志安全分析 [J]. 计算机时代，2022(11)：38-42
Gong J H，Ling S Y. Security analysis of university Web log based on ELK[J]. Computer Era，2022(11)：38-42

[4] 李书达，刘遵仁，朱琦. 基于 ELK 的运维辅助系统的设计与实现 [J]. 青岛大学学报 (工程技术版)，2022，37(1)：18-23
Li S D，Liu Z R，Zhu Q. Design and realization of operation and maintenance auxiliary system based on ELK[J]. Journal of Qingdao University (Engineering & Technology Edition)，2022，37(1)：18-23

[5] 珠海华润银行日志管理与分析平台课题组，杨京健. 基于 ELK 的日志管理与分析平台实践 [J]. 金融科技时代，2022，30(1)：59-62
Research Group of Log Management and Analysis Platform of Zhuhai China Resources Bank, Yang J J. Practice of log management and analysis platform based on ELK[J]. Financial Technology Time，2022，30(1)：59-62

[6] 谢磊，张冰，杨猛. 基于 ELK 的日志分析系统研究与实践 [J]. 科技经济市场，2020(10)：17-18
Xie L，Zhang B，Yang M. Research and practice of log analysis system based on ELK[J]. Science & Technology Econony Market，2020(10)：17-18

[7] 李钦，杨程. 基于 ELK 的日志分析平台搭建与优化 [J]. 现代信息科技，2019，3(15)：193-194
Li Q，Yang C. Construction and optimization of log analysis platform based on ELK[J]. Modern Information Technology，2019，3(15)：193-194