ELK-Stack在业务监控系统中的应用

龚 萍

（中国移动(深圳)有限公司，广东 深圳 518048）

[摘 要] 随着企业信息化程度的不断提高以及大规模集群的部署应用，日常运维工作面临着越来越严峻的考验，借助自动化运维手段提高系统运维效率成为一种趋势。以日志数据为突破口，借助ELK-Stack开源软件，构建日志分析管理平台，并与现有监控运维类平台进行融合，能快速增强系统运维分析能力，有效提高日常运维效率。

[关键词] ELK；日志分析；自动化运维；监控

中图分类号：TP277 文献标识码：A 文章编号：1008 - 6609 (2017) 10 - 0065 - 03

DOI:10.15966/j.cnki.dnydx.2017.10.019

1 引言

随着云计算和大数据技术的不断发展，IT系统架构和技术框架的变革，驱动着系统运维从传统的IT运维管理开始向IT运维分析转变，从运维人员手工操作向自动化运维服务转变。在日常运维工作中，操作系统、应用服务和业务逻辑等主要维护对象，每天都在不停地产生日志数据，这些数据包含了系统可用性信息、效能信息、安全信息、异常信息、错误信息等系统信息，在信息价值、获取成本上具有特有的优势。因此，日志数据的分析挖掘将成为IT运维分析的首要突破口。

过去，日志数据基本都存在于单机磁盘上，通过运维工程师登陆对应服务器，手工输入命令进行临时的、事后的分析和审计。在大数据的时代，海量日志分布在各个不同的地方，传统的日志处理方案显得非常笨拙和低效，对日志进行统一管理和分析成为亟待解决的问题。ELK技术栈的出现，实现了海量日志的统一管理和高效的挖掘分析，有效地发挥了系统日志在故障告警、问题定位、性能优化等实际运维中的作用，极大地提高了IT系统的运维效率。

2 ELK-Stack简介

ELK是一整套解决方案，是三个软件产品的首字母缩写：Elasticsearch，Logstash和Kibana。这三款软件都是开源软件，通常配合使用，而且又先后归于Elastic.co公司名下，故被简称为ELK技术栈。

Elasticsearch是一个建立在全文搜索引擎Apache Lucene基础上的实时的分布式搜索和分析引擎，使用Java语言编写。它可以用于全文搜索，结构化搜索以及实时分析，具备以下特点：支持分布式实时文件存储，并将每一个字段都编入索引；文档导向，所有的对象全部是文档；高可用性，易扩展，支持集群、分片和复制；接口友好，支持JSON。

Logstash是一个具有实时渠道能力的数据收集引擎，使用JRuby语言编写。Logstash几乎可以访问任何数据，它的四大组件（Shipper、Broker&indexer、Search&Storage和Web Interface）可以和多种外部应用结合，同时支持弹性扩展。

Kibana基于Apache开源协议，使用JavaScript语言编写。它为Elasticsearch提供分析和可视化的Web平台，可以在Elasticsearch的索引中查找、交互数据，并生成各种维度的表图。

图1展示了ELK-Stack中Logstash，Elasticsearch和Kibana三款软件的组织方式及协同工作的原理。

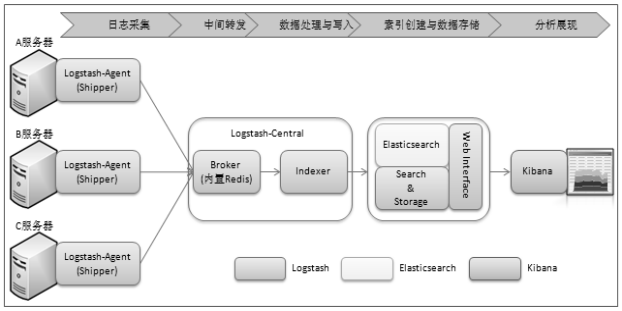

图1 ELK-Stack体系架构图

ELK技术栈在日志管理与分析方面具备以下优点：

(1) 处理方式灵活：Elasticsearch是实时全文索引，不需要像storm那样预先编程才能使用；

作者简介：龚萍(1989-)，女，湖北仙桃人，本科，研究方向为业务监控、自动化运维。

(2) 配置简易上手：Elasticsearch 全部采用 JSON 接口，Logstash 是 Ruby DSL 设计，都是目前业界最通用的配置语法设计；

(3) 检索性能高效：虽然每次查询都是实时计算，但是优秀的设计和实现基本可以达到百亿级数据查询的秒级响应；

(4) 集群线性扩展：不管是 Elasticsearch 集群还是 Logstash 集群都是可以线性扩展的；

(5) 前端操作炫丽：Kibana 界面上，只需要点击鼠标，就可以完成搜索、聚合功能，生成炫丽的仪表板。

3 ELK-Stack 应用实践

本次应用中，尝试将 ELK 技术栈融入某业务监控系统，通过在该系统中部署日志管理分析模块，实现日志统一管理与分析展现，达到提升运维自动化程度，从而提高运维效率的目标。

3.1 系统框架

为保证日志分析服务的可扩展性，采取搭建独立的 ELK 日志分析模块，然后以与原业务监控系统的能力贯通的方式构建整体应用框架。系统整体框架如图 2 所示。

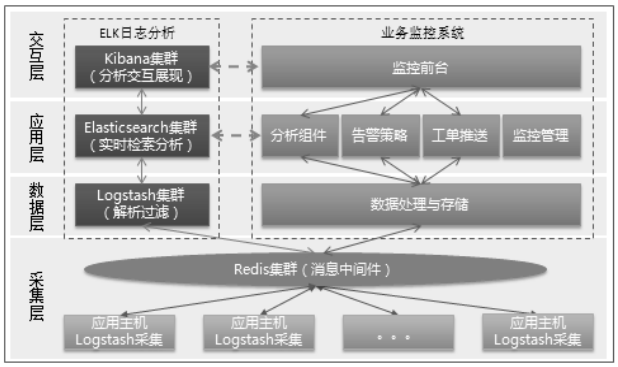

图 2 ELK 日志分析模块与业务监控系统融合架构图

这个架构中，首先在业务监控系统监控的各个监控对象（应用主机）上分别部署独立的 Logstash-Agent 进行原始日志采集，所有采集到的日志集成到 Redis 集群中，利用消息队列机制降低数据丢失的隐患；随后 Logstash 的 Indexer 组件将负责从 Redis 中取出日志数据，进行日志解析转换等数据预处理工作，并将经过预处理的数据输入 Elasticsearch 集群进行进一步的处理与存储；最终 Kibana 负责完成面向用户的日志数据统计、分析与展现。

在整个系统中，ELK 日志分析模块与业务监控系统各有一套独立的“数据采集-数据处理-数据分析-数据展现”机制，互不影响。ELK 日志分析模块只需根据监控需要，将日志处理后生成的相关数据或分析结果传送给业务监控系统，借助系统原有的监控告警及运维工单流转功能，即可发挥日志分析在日常监控运维中的作用。同时，ELK 日志分析模块的独立性保障了往后其它应用系统日志的快速接入。

3.2 环境部署

按照官方网站的安装指南完成 ELK 基础环境搭建，本文不赘述具体安装过程，只对安装完成后的重要配置进行说明。

(1) 配置日志生成样式

以采集 nginx 日志为例，在配置文件 nignx.conf 中指定日志输出格式及日志存放路径：

```
http {
log_format json '{"@timestamp":"$time_iso8601",'
        '"@version":"1",'
        '"client":"$remote_addr",'
        '"url":"$uri",'
        '"status":"$status",'
        '"domain":"$host",'
        '"host":"$server_addr",'
        '"size":$body_bytes_sent,'
        '"responsetime":$request_time,'
        '"referer": "$http_referer",'
        '"ua": "$http_user_agent"}';
}
server{
access_log /var/log/nginx/access_json.log json;
}
```

(2) 配置 Logstash 采集日志数据写入 Redis

创建 Logstash 配置文件，指定日志采集路径与输出路径：

```
input{
    file{
    path => "/var/log/nginx/access_json.log"
    codec => "json"
    }
}
output{
    redis{
    data_type => "list"
    key => "nginx-access-log"
    host => "192.168.1.21"
    port => "6379"
    db => "2"
    }
```

```
}
```

(3) 配置Logstash读取Redis中的日志数据写入Elasticsearch

配置输入指向Redis和输出指向Elasticsearch：

```
input{
    redis{
    data_type => "list"
    key => "nginx-access-log"
    host => "192.168.1.21"
    port => "6379"
    db => "2"
    }
}
output{
    elasticsearch{
    hosts => "192.168.1.20"
    protocol => "http"
    index => "logstash-nginx-redis-messages-%{+YYYY.MM.dd}"
    }
}
```

(4) 配置Elasticserach

只需要在Elasticsearch配置文件elasticsearch.yml中进行相关路径和端口设置：

```
cluster.name: elkcluster
node.name: elk-node1
path.data: /data/es-data
path.logs: /var/log/elasticsearch/
network.host: 0.0.0.0
http.port: 9200
```

(5) 配置Kibana

只需要在Kibana配置文件kibana.yml中配置Elasticsearch路径：

```
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.url: "http://192.168.1.20:9200"
kibana.index: ".kibana"
```

(6) 访问Kibana

所有安装和配置完成后，在浏览器中输入http://192.168.1.20:5601即可看到最终的Kibana界面，如图3所示。

3.3 应用效果

在本次应用中，ELK日志分析模块主要为原业务监控系统提供日志集中管理和日志分析两大功能。

图3 ELK日志分析统计示意图

在日志管理方面，不仅将以往分散在各台主机的日志进行了集中管理，而且简化了日志查询的方式，大幅调高了日志查询的效率：引入ELK之前，人工查看单台应用主机日志平均耗时5分钟；引入ELK之后，所有应用主机日志均可在界面上集中查询，平均耗时1s，且不受应用主机数量和日志数量的限制。

在日志分析方面，ELK的分析挖掘能力，对监控过程中的异常告警和故障诊断起到了极大的辅助作用：通过从日志中挖掘出被监控系统的各项指标，及时反映系统的健康状态和性能瓶颈，改变了原先需要编写复杂脚本才能部署监控的方式，不仅效率更高，同时对系统正常的业务运行没有任何影响；通过对多种日志的快速检索、关联分析和直观展现，有效地帮助运维人员提高了定位故障原因的速度和难度。

4 结语

大数据时代，服务器规模的不断扩大和分布式应用的快速普及，使得系统运行监控和日常维护变得尤为重要，而日志的管理和利用是其中一个不可忽视的部分。本文通过介绍ELK日志分析模块在业务监控系统中的部署方式和应用情况，体现了ELK技术栈在实现自动化运维分析服务、增强系统监控运维能力、提升日常运维效率方面的突出作用，也为以ELK技术栈为代表的自动化运维工具在IT系统运维工作中的快速引入和广泛使用提供了参考。

参考文献：

[1] 饶琛琳. ELK Stack权威指南[M]. 北京：机械工业出版社，2015.

[2] 魏山林. 基于ELK的日志分析系统[J]. 电脑知识与技术，2017(2)：69-70.

[3] 龙炜. 自动化运维工具在企业信息管理系统中的应用[J]. 微型机与应用，2017，36(5)：102-104.

（下转第77页）

供了可实施途径，强调课堂教学设计过程中，以学生为主体，注重学生能力培养，真正做到了“因材施教”，把OBE 的教育模式应用于计算机网络安全风险评估课程中，真正让学生参与课堂，实现学生的自主学习，更有利于实现应用型高校人才培养与企业需求的无缝对接，提高了人才培养质量。

参考文献：

[1] 邱剑锋，朱二周，周勇，等. OBE 教育模式下的操作系统课程教学改革[J]. 计算机教育，2015(6)：28-32.

[2] 顾佩华，胡文龙，林鹏，等. 基于“学习产出”(OBE)的工程教育模式——汕头大学的实践与探索[J]. 高等工程教育研究，2014(6)：27-37.

[3] OWASP. Category：OWASP Top 10 2013 Project[EB/OL]. 2015-08-30. https://www. owasp. org/index. php/Top_10_2013- Table_of_Contents.

[4] 唐屹，周权. Web 安全实验课程的教学探讨[J]. 计算机教育，2014(11)：87-90.

[5] 张博，南淑萍. 基于主动式学习的信息安全专业工程实践课程改革研究[J]. 新余学院学报，2015，20(4)：136-13.

Research on Teaching Innovation of *Computer Network Security Risk Assessment* Based on OBE

Lin Yuxiang　Liu Yan

（Nanyang Institute of Technology, Nanyang 473004, Henan）

【Abstract】 *Computer Network Security Risk Assessment* is a theoretical and practical course. This paper introduces the concept of OBE education in this course, uses the learning outcomes as the guidance, optimizes the teaching content, explores the teaching methods, emphasizes the experimental teaching and sets up diversified assessment methods. The reform and innovation of the course can improve the teaching effect and the quality of talent cultivation.

【Keywords】 OBE; risk assessment; teaching method

（上接第67页）

Application of ELK-Stack in Business Monitoring System

Gong Ping

(China Mobile (Shenzhen) Co., Ltd., Shenzhen 518048, Guangdong)

【Abstract】 With the continuous improvement of enterprise informatization and the deployment of large-scale clusters, daily operation and maintenance work is facing more and more severe test. Therefore, it has become a trend to improve the system operation efficiency by means of automated operation and maintenance. This paper builds the log analysis and management platform based on ELK-Stack, which integrates with the existing monitoring and operation platform. It can enhance the system operation and analysis ability, and improve the efficiency of daily operation

【Keywords】 ELK; log analysis; automated operation and maintenance; monitoring