

基于并行计算的海量日志分析系统实现

白超¹, 杨静², 吴建国¹

(1. 安徽大学, 安徽 合肥 230000;

2. 解放军电子工程学院 计算机系, 安徽 合肥 230027)

摘要:通过深入研究日志的类型和特点,设计并实现了一套基于并行计算的海量日志文件分析系统。该系统采用集群方式并行地收集日志文件,采用分布式文件系统存储,最终利用并行计算对日志进行分析处理。该系统实现了日志采集、分析的完全自动化处理,在系统部署之后能够有效地进行系统安全的维护、系统性能的优化、系统故障的排查。该系统结合云计算提高了日志分析的效率,解决了海量日志处理过程中存在的问题,为海量日志分析提供了一个完整有效的解决方案。

关键词:分布式计算;分布式文件系统;云计算;日志处理

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2013)07-0080-04

doi:10.3969/j.issn.1673-629X.2013.07.020

Implementing of Massive Log Analysis System Based on Parallel Computing

BAI Chao¹, YANG Jing², WU Jian-guo¹

(1. Anhui University, Hefei 230000, China;

2. Department of Computer, College of Electronic Engineering of PLA, Hefei 230027, China)

Abstract:On the basis of analyzing log type and features deeply, design and implement a massive log processing system based on parallel computing. It adopts the method of cluster to collect log in parallel way, store in the distributed file system, and analyze log by parallel computing. The system achieves log collection and analysis through automated processing, can effectively carry on security maintenance, system performance optimization, system failure check after the system deployment. The system combines distributed and cloud computing solutions to improve efficiency of log processing, solves the major problems of massive logs processing effectively, provides a complete and effective solutions for massive logs processing.

Key words:distributed computing; distributed file system; cloud computing; log processing

0 引言

日志^[1]是一个完整系统里面重要的功能组成部分,其利用特定的形式准确并且规范地表达出系统产生的所有行为。依据对日志的分析不仅可以对系统自身的性能进行有效的优化,而且当系统发生故障时,能够准确、及时地定位错误,方便加以修正。在当代信息爆炸的形式之下,一个企业级的公司服务器系统每天产生海量的日志数据,而且会随着时间不断增长。因此必须借助工具才能够分析复杂、庞大的日志。海量日志分析处理系统应运而生。针对信息爆炸的时代,

传统的工具在技术方面存在诸多缺陷,无法满足日益增长的爆炸式数据。海量日志分析系统提供了成熟的分布式处理解决方案,利用分布式计算很好地解决了这一难题,已经成为行业的趋势。

1 系统概述

1.1 系统简介

日志分析处理的现状:

①当数据规模较小,直接采用Linux等工具进行人工的查看,此种方法效率低下。

收稿日期:2012-10-18

修回日期:2013-01-22

网络出版时间:2013-04-08

基金项目:安徽省科技攻关项目(07010200057)

作者简介:白超(1988-),男(回族),安徽六安人,硕士研究生,研究方向为云计算;吴建国,博士,教授,博士生导师,研究方向为智能EDA、中文信息处理、嵌入式系统。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130408.1559.018.html>

②当数据规模变大,引入数据库,由于数据量不断变大,单机处理能力无法满足海量日志数据的处理。

③海量日志分析系统:使用分布式文件系统存储海量日志文件信息,利用分布式计算对日志信息进行处理。

系统以云计算作为基础^[2],构建分布式集群结构,基于成熟的 Hadoop 分布式计算框架,对海量日志文件进行收集和处理。建立了一个分布式存储(HDFS),并行计算(MapReduce),实时搜索(Elastic Search)为一体的海量日志处理平台。系统前端采用 Java Web 技术,向用户提供简洁的界面,方便使用,便于理解,减少发生错误的几率,具有丰富的优点:

- ①跨平台性,可以在任何的平台下移植和使用;
- ②采用成熟的框架,提供安全稳定的服务。

系统服务器端采用分布式计算框架,以并行计算为基础能够快速地对日志进行分析,具有很强的市场应用价值。

1.2 功能需求

系统功能大致分为四个主要部分:日志收集,信息存储,并行计算,信息检索。

1.2.1 日志收集

系统提供四种收集日志的解决方案:

- ①使用 Flume 集群收集日志;
- ②使用 Linux 服务器搭建 syslog 服务收集日志;
- ③通过 log4j. Appender 发送日志文件;
- ④搭建 Restful 服务器集群,客户端调用 Restful

API 接口发送日志文件。

具体设计如图 1 所示:

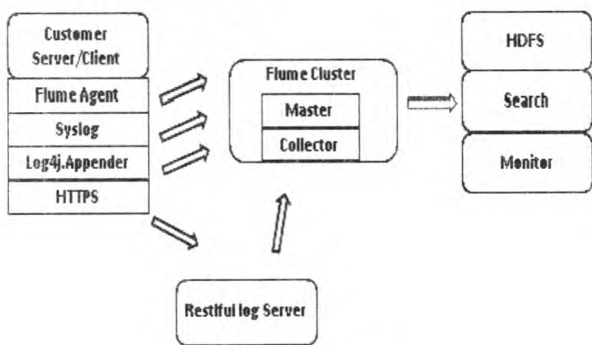


图 1 日志收集示意图

1.2.2 信息存储

日志收集组件将所有收集的日志文件存储到日志存储服务器上,日志存储服务器采用分布式文件系统(HDFS)根据不同的日志类型进行分类存储。用户可以定制日志的回滚方式,例如每天回滚一次,同时日志以固定大小为单位方便用户查看。除此之外系统还支持网络方式进行文件操作,用户可以方便地通过网络浏览器进行上传、下载、新建目录、查看信息等功能。

1.2.3 并行计算

系统通过 MapReduce 和 Hive 操作实现对日志文件进行并行计算处理。MapReduce 是一种编程模型,能够对大规模的数据进行并行的运算和处理。Hive 是一个基于 Hadoop 的数据仓库工具,其构建在分布式,按列存储的数据仓库上,负责管理 HDFS 中存储的数据,并提供完整的 sql 查询功能。Hive 在执行时由引擎翻译成 MapReduce 任务进行运行。系统通过实现 MapReduce 操作,从而对大规模的日志文件进行并行处理。

由于日志文件已经存储在系统的分布式文件系统中,因此系统能够充分地利用 MapReduce 和 Hive 的优势,对日志文件敏感的信息进行非实时的分析和处理。

1.2.4 信息检索

系统采用 Elastic Search 技术^[3]来实现对日志文件进行实时检索功能,提供分布式搜索引擎服务,保持稳定的服务,同时支持多类型的租户,高扩展性,多种持久化策略等诸多功能。用户可以根据自身的需求保存日志信息检索的历史事务。历史事务利用动态图标形式向用户友好地展示每天日志的具体量化信息。同时用户还可以保存检索的结果,保存结果信息涵盖丰富的日志信息,如日志检索范围、敏感信息状态的波动趋势、信息的统计结果等等。

1.3 安全需求

日志信息包括一个系统运行状态下的诸多敏感信息,例如用户的信息、操作的信息、数据库的设计^[3]等很多有用的信息,因此保障系统的安全性显得尤为重要。本系统采取众多安全保证措施,其中包括防止非法用户登录,防止用户恶意操作,SQL 注入攻击,数据文件的存储隔离,用户的权限控制管理等等。

2 系统设计

2.1 系统结构设计

系统深入考虑高扩展性,模块之间的独立性,低耦合度等基本原则^[4]。系统将前台框架设计为表现层,业务层以及持久层的三层体系结构。具体系统结构设计如图 2 所示:

2.2 系统流程设计

系统的核心目标是针对不同类型的日志信息进行分类的分析和处理,在这一过程中贯穿着各种模块和组件之间的协调工作^[5],用户的隶属组问题和权限控制,安全认证问题。

通过梳理系统的业务流程,准确把握系统的整体框架,针对系统的框架进行有效准确的设计。系统参照成熟收集日志的策略方针,并加以改进,结合自身的特殊处理要求,通过对日志类型的分析,对系统流程进

行统筹设计。海量日志分析系统的总体流程设计如图 3 所示。

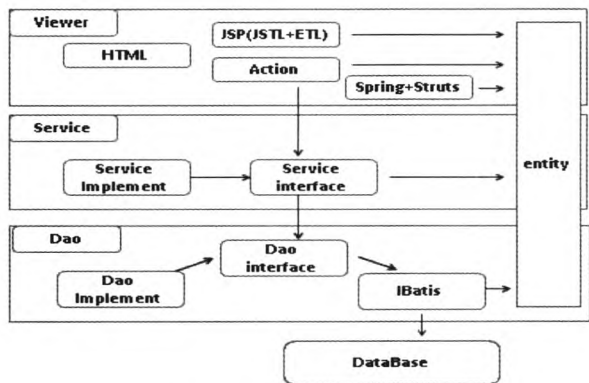


图 2 系统结构设计示意图

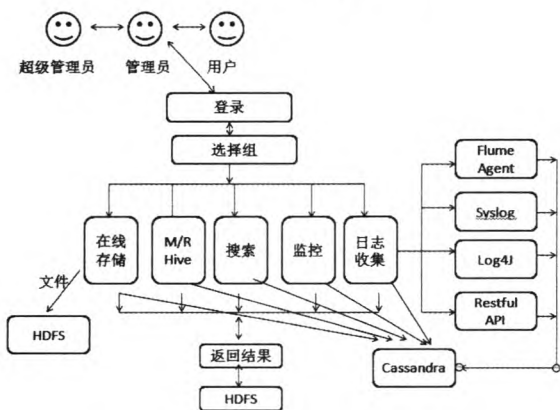


图 3 系统整体流程设计示意图

2.3 系统数据流分析

通过对系统的流程进行分析设计后,针对日志处理系统的数据流进行分析和整理。系统数据流分析结果如图 4 所示。

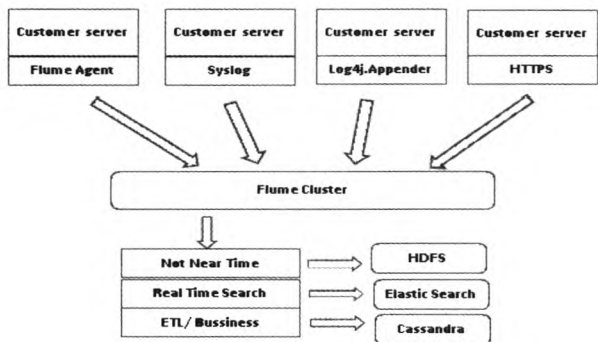


图 4 系统数据流分析

3 系统实现

3.1 系统功能实现

海量日志分析系统以云计算为基础,利用分布式存储,并行计算,结合实时搜索技术^[6],向用户提供了一个方便、快捷的日志分析处理系统。针对不同类型的日志种类,提取特征,同时支持结构化,半结构化,以及用户自定义的日志类型,适用范围广泛。

系统的功能由日志收集、分布式文件系统存储、并行计算 (MapReduce/Hive)、实时搜索、实时监控、用户管理等 6 个子系统构成。

3.2 核心功能实现

3.2.1 系统前台框架实现

系统在提供前台 Web 服务时,采用目前企业成熟的开源框架 SSI (Struts2+Spring+IBatis)^[7],帮助开发人员降低代码的耦合度,搭建一个结构清晰、高维护性的应用程序。同时增强代码健壮性和可重用性,可以明显提高开发的速度。

①利用 Struts2 框架搭建 MVC (Model+View+Control)^[8] 框架模式,清晰地区分控制,事务逻辑和外观。它将业务逻辑和页面代码分离开;简化了开发应用程序的过程。

②在系统的业务逻辑层,引入 Spring 框架,利用 Spring 框架的依赖注入原则从而实现系统中对业务逻辑类和数据库访问类的实例托管,从而减少系统组件之间的耦合度。

③由于系统是针对海量数据文件进行分析处理,因此对 SQL 语句的执行效率要求很高,因此引入半自动化框架 IBatis^[9]。利用 IBatis 提供的半自动化对象关系映射,自己编写定制的 SQL 语句,对 SQL 的语句进行了细粒度的优化和控制,同时具有可维护性强、执行效率高的特点。

3.2.2 日志收集的服务器集群实现

针对海量日志的收集,如果使用单一的服务器进行收集处理,显然会产生系统性能的瓶颈问题,同时也无法实现实时搜索的功能。海量日志分析系统利用 Flume 这一分布式、可靠、同时具有高可用性特征的海量日志聚合的工具,实现以集群的方式收集,汇总不同来源的海量日志信息,并直接存储到海量日志分析系统的分布式文件系统中。

3.2.3 MapReduce/Hive 实现

①MapReduce 作业流:系统向用户提供大量的 MapReduce 脚本对用户的日志文件进行处理,同时系统还支持用户自定义脚本文件。用户自定义创建新的作业流,并通过 Web 服务器进行上传的脚本文件。系统执行用户上传到的脚本文件,脚本正确执行完成后,用户可以查询作业执行的结果并保存。如果脚本执行发生错误,则作业流执行失败,产生执行错误的信息,方便用户排查。

②Hive:用户进入 Hive 命令行界面输入 Hive 执行语句,系统将 Hive 语句转换成 MapReduce 任务,交付后台服务器进行计算。

优点方便直观,用户可以直接在 Hive 命令行界面查看执行结果,并保存结果。

3.2.4 组件通信和调用方式实现

由于海量日志分析系统的组件众多,而组件之间存在着大量的数据交换,并且数据交换的次数连续,频繁。为了保证系统组件之间通信的流畅和稳定,系统采用 Thrift 提供一种跨语言的过程调用方式,具有很强的扩展性。通过在系统内定义统一的数据类型和服务接口,系统组件之间可以进行无缝的数据流动,RPC 的协议层和传输层可以跨语言实现,需要和某种动态的系统绑定,因此避免了动态类型的检查和转换。因此系统内部组件的通信和调用具有很高的效率,保证了日志分析处理的实时性。

3.3 系统运行部署

通过文章上述的分析,系统功能丰富,并且组件较多,必须充分考虑到系统的性能和稳定性的需求。

①集群策略:系统的各个组件都部署在不同的服务器集群上,实现了系统组件之间的独立性和可插拔性。即使系统的一个功能组件服务器发生崩溃或产生错误,也不会影响到其他组件服务的正常运行。系统组件内部的自身设计都是以集群方式进行管理和配置,因此集群中某台服务器发生崩溃或产生错误,也不会影响到系统组件内部其他服务器,该组件仍可提供稳定的服务。

②采用多重数据库管理模式:利用 Cassandra 非关系型数据库,对文件的元信息进行存储;利用 Oracle 关系型数据库集中对用户的权限进行控制,管理配置用户的隶属组。

4 结束语

系统以云计算为基础,建立在大规模分布式计算上,针对海量的日志进行处理分析。

文中对系统的功能进行了详细的阐述,详细说明了系统前端以及后台服务器集群采用的技术框架,分

析了系统内部的数据流程。系统从近几年国内外的的发展趋势出发,结合目前提出的云计算框架,从解决当前日志方面处理效率和瓶颈问题出发,在对云计算进行充分的研究和分析之后,对目前分布式计算体系的组织结构,功能需求进行优化和修改,结合数据库,服务器集群部署进行了完整的设计,对系统予以实现,为海量日志文件信息处理提供了一个完整有效的解决方案。

参考文献:

- [1] Dean J, Ghemawat S. MapReduce: Simplified Data Processing on Large Clusters[J]. Communications of ACM, 2005, 51(1): 107-113.
- [2] Leverich J, Kozyrakis C. On the energy efficiency of Hadoop cluster[J]. ACM SIGOPS Operating Systems Review, 2010, 44(1): 61-65.
- [3] Sarma J S, Zheng Shao, Chakka P, et al. Hive - a petabyte scale data warehouse using Hadoop[C]//Proc. of 2010 IEEE 26th International Conference on Data Engineering. [s. l.]: [s. n.], 2010.
- [4] 李扬, 王景中, 杨义先. 综合安全管理平台中日志格式化系统的设计与实现[J]. 计算机应用, 2010, 30(6): 1708-1710.
- [5] 黄海隆, 陈赛博. 计算机日志分析与管理方法的研究[J]. 大众科技, 2006(7): 67-68.
- [6] 王伟, 彭勤科. 主机日志分析及其在入侵检测中的应用[J]. 计算机工程与应用, 2002, 38(13): 35-37.
- [7] 郭岩, 白硕, 杨志峰, 等. 网络日志规模分析和用户兴趣挖掘[J]. 计算机学报, 2005, 28(9): 1483-1496.
- [8] 张健沛, 刘建东, 杨静. 基于 Web 的日志挖掘数据预处理方法的研究[J]. 计算机工程与应用, 2003, 39(10): 191-193.
- [9] 张建成, 宋丽华. 云计算方案分析研究[J]. 计算机技术与发展, 2012, 22(1): 165-167.

(上接第 79 页)

[s. n.], 2007: 675-680.

- [4] 梁吉业, 高嘉伟, 常瑜. 半监督学习研究进展[J]. 山西大学学报(自然科学版), 2009, 32(4): 528-534.
- [5] 徐庆伶. 基于半监督学习的遥感图像分类研究[D]. 西安: 陕西师范大学, 2010.
- [6] Seeger M. Learning with labeled and unlabeled data[R]. Edinburgh: University of Edinburgh, 2002.
- [7] Blum A, Mitchell T. Combining labeled and unlabeled data with co-training[C]//Proceedings of the 11th Annual Conference on Computational Learning Theory. Madison, WI: [s. n.], 1998: 92-100.
- [8] Zhou Zhihua, Li M. Tri-Training: exploiting unlabeled data using three classifiers[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(11): 1529-1541.
- [9] 李昆仑, 张伟, 代运娜. 基于 Tri-Training 的半监督 SVM[J]. 计算机工程与应用, 2009, 45(22): 103-106.
- [10] 徐庆伶, 汪西莉. 一种基于支持向量机的半监督分类方法[J]. 计算机技术与发展, 2010, 20(10): 115-117.
- [11] 邓超, 郭茂祖. 基于 Tri-Training 和数据剪辑的半监督聚类算法[J]. 软件学报, 2008, 19(3): 663-673.
- [12] Blake C, Keogh E, Merz C J. UCI repository of machine learning databases[D]. Irvine: University of California, 1998.
- [13] Li Ming, Zhou Zhihua. SETRED: Self-training with editing[C]//Proc of the Advances in Knowledge Discovery and Data Mining (PAKDD 2005). Heidelberg: Springer-Verlag, 2005: 611-621.

基于并行计算的海量日志分析系统实现

作者:

[白超](#), [杨静](#), [吴建国](#), [BAI Chao](#), [YANG Jing](#), [WU Jian-guo](#)

作者单位:

[白超, 吴建国, BAI Chao, WU Jian-guo \(安徽大学, 安徽合肥, 230000\)](#), [杨静, YANG Jing \(解放军电子工程学院计算机系, 安徽合肥, 230027\)](#)

刊名:

[计算机技术与发展](#) 

英文刊名:

[Computer Technology and Development](#)

年, 卷(期):

2013, 23 (7)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201307020.aspx