应用 Hadoop 提升数据库审计系统检索性能的研究①

方建生 [1], 王福民 [2]

[1](广东电信 大数据运营中心, 广州 510080)
[2](广州速方软件有限公司, 广州 510660)

摘　要: 鉴于单节点数据库审计系统检索性能低下的现状, 探讨应用 Hadoop 伪分布模式和 HBase 列存储模型重构数据库审计系统的检索存储体系, 重点研究 HDFS 存储机制、MapReduce 运算框架和 HBase 数据模型三者的集成, 以提升数据库审计系统实时检索和综合分析的性能. 重构方案有效提升了检索性能, 但鉴于数据的高可靠性和大体积, 提出结合生产现状应用 Hadoop 和 HBase 分布式集群的展望.

关键词: 数据库审计系统; Hadoop; HBase; RDMS

Study on Applying Hadoop to Enhance the Retrieval Performance of Database Audit Systems

FANG Jian-Sheng[1], WANG Fu-Min[2]

[1](Operation Center of Big Data, Guangdong Telecom, Guangzhou 510080, China)
[2](Guangzhou Soofound Software Co. Ltd., Guangzhou 510660, China)

Abstract: Based on the present situation of lower retrieval performance of the single node database audit system, this paper carries out research of application of the Hadoop pseudo distribution model and the HBase column storage model to reconstruct the database audit system of the single node deployment for enhancing the retrieval performance. This paper focuses on the study of integrating HDFS storage mechanism, MapReduce computing framework and HBase data model to improve the performance of real-time retrieval and comprehensive analysis of database audit system. Reconstruction scheme can effectively improve the retrieval performance, but in view of the high reliability and large volume of the data, the application of Hadoop and HBase distributed cluster is proposed in combination with the production status.

Key words: DB audit system; Hadoop; HBase; RDMS

1　数据库审计系统现状

数据和数据库的安全, 是计算机运维的一个重大课题, 催生数据库安全技术的研究[1], 集中在外部数据库入侵检测[2,3]和内部数据库操作审计两个方面.

数据库审计系统(Database Audit System, 下称: DBAS)主要是通过旁路监听的方式采集访问目标数据库的镜像数据流, 实时监控并记录以审计, 及时发现违规操作和异常行为[4-6], DBAS 的系统部署结构如图 1 所示.

DBAS 在定位异常数据操作行为上, 弥补了数据库自身日志的不足, 已广泛应用在银行、医院、电信等行业[7], 其核心模块是:

1) 集引擎模块, 主要从链路层采集网卡数据包, 提取数据库会话协议的内容入库, 涵盖 DQL、DDL、DML、DCL 操作记录, 支持各类数据库协议的解析, 包括 Oracle 的 TNS 协议、Sybase 和 SQLServer 的 TDS 协议、DB2 的 DRDA 协议等.

采集引擎的关键技术是及时捕获网卡接收的数据包, 较为常见的是应用 pcap 库和 dpdk 库. Intel 开发的网络数据包处理转发套件[8,9](DPDK, Data Plane Development Kit), 利用 Linux 的 CPU affinity 和大内存页机制提高处理效率, 并提供 UIO 机制支撑网卡硬件驱动在用户态下运行, 具有更强的性能.

2) Web 审计应用, 主要是对采集入库的 SQL 语句

① 收稿时间:2016-03-30;收到修改稿时间:2016-06-06　[doi:10.15888/j.cnki.csa.005562]

进行语义分析, 重组网络会话, 开展 4W 审计, 支持多关键字搜索和多维度统计分析.

Web 审计应用的核心是检索功能, 支持在月表亿级数据量中综合查询、分析. DBAS 由于其功能和生产特性, 多以单机集成部署采集引擎和 Web 审计应用, 受制于关系型数据库系统(Relational Database Management System, 下称 RDMS)的存储检索体系以及单机硬件资源不足的约束, 尤其是磁盘寻址和传输的 IO 性能, DBAS 检索效能低下.

针对该问题, DBAS 查询优化方案集中在 Web 应用体系和关系型数据库上, 如应用 Hibernate 架构和 Web 前端缓存技术[10]、应用数据库索引和分表技术[11], 本文则试图从 DBAS 存储检索体系上研究解决方案.

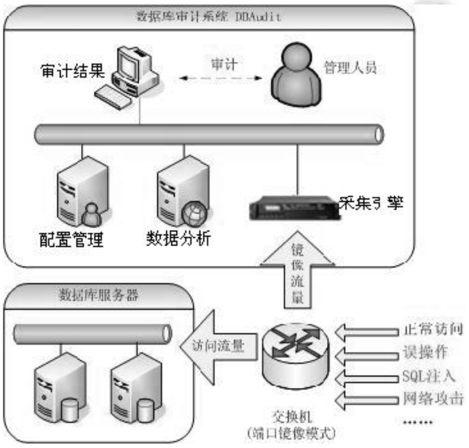

图 1 数据库审计系统部署

2 HBase数据模型的特性

Hadoop 是一套可靠的高性能的共享存储和分析系统[12], 可靠是首要, 高性能在于克服单机作业磁盘 IO 和并行作业网络带宽的两大瓶颈, 核心是负责存储的 HDFS[13](Hadoop Distributed File System, 下称: HDFS)分布式文件系统和负责并行分析的 MapReduce 计算框架[14].

HBase 具有分布式、面向列的存储模型特性, 存储的数据介于映射(key/value)和关系型数据之间[15]. 通过 Hadoop 生态系统圈, 可以看出 HBase 位于结构化存储层, 底层依赖 HDFS 提供的高可靠存储支持, 上层分析则借重 MapReduce 的高性能计算能力[16].

HBase 数据模型如表 1, 其列存储特性与倒排索引[17]原理一致, 又植根于 Hadoop 生态圈, 适合应用于全文检索, 主要组成说明如下:

1) Row Key: Table 主键、行键, Table 中记录按照 Row Key 排序;

2) Timestamp: 每次对数据操作对应的时间戳, 可视为数据的 version number;

3) Column Family: 列簇, 一个 table 在水平方向有一个或者多个列簇, 列簇可由任意多个 Column 组成, 列簇支持动态扩展, 无须预定义数量及类型, 二进制存储, 用户需自行进行类型转换.

表 1 HBase 数据模型

Table				
Row Key	Timestamp	Column Family		
		Field1	Field2	…
r1	t1			
	t2			
	…			
r2				
…				

得益于 Hadoop 生态圈和 HBase 的列存储数据模型特性, 使 HBase 适合于廉价 PC Server 上实现实时查询和综合分析并易于扩展成分布式集群生产.

3 重构DBAS存储检索体系

传统上, DBAS 存储检索体系应用 RDMS 支撑采集引擎模块的数据写入和 Web 审计应用模块的数据读取. 通过剖析 DBAS 现状和理解 HBase 存储模型特性, 结合 DBAS 数据具有列存储的基因特征, 显见基于 Hadoop 平台应用 HBase 可提升 DBAS 的检索性能[18,19].

本文研究应用 Hadoop 平台的高性能海量数据处理能力[20]和 HBase 数据库的列存储模型重构 DBAS 存储检索体系, 高效及时挖掘数据库操作的违规和异常行为. 重构核心是基于 DBAS 单机生产的特点部署 Hadoop 伪分布式模式, 并用 HBase 替换 RDMS.

3.1 DBAS 存储检索需求分析

DBAS 数据存储检索具有单机大数据量存储和高并发操作、数据持续写入和读取操作的特点. DBAS 数据存储检索的基本信息如表 2 所示, 主要是数据库操作信息的 4W 记录, 溯源什么时间什么人在哪里做了什么.

采集引擎模块解析网卡数据包中访问数据库操作的信息入库, 同时 Web 审计应用模块频繁、大量地读取数据支撑前台手工综合查询和后台自动综合统计,

单机性能和RDMS显然无法满足大数据的高并发读写. 为保证审计信息及时入库, 资源上侧重采集引擎模块的数据处理, 从而严重影响Web审计应用模块的使用.

DBAS 的查询和分析, 主要集中在 SQL 语句语义分析的全文关键词搜索和多关键字联合查询, 较为常用场景是: 操作类型、操作时间和 SQL 语句的综合查询.

表 2　RDMS 表信息

RDMS 存储列	示例值
操作时间	2015/8/16 16:16:16
数据库名	MYSQL-222
数据库类型	DB_MYSQL
数据库 IP	192.168.1.222
数据库 port	3306
操作来源 IP	192.168.1.99
操作来源 Port	3043
操作来源 MAC	00-23-24-00-2B-82
数据库实例名	mydb
数据库用户名	pas DbName
操作类型	select
操作对象	\`pas\`.\`mail\`
执行结果	成功
操作耗时(sec)	0.00
影响行数	0(update 有值)
SQL 语句	SELECT \`mail_id\`, \`from_emp_id\`, \`subject\`, LEFT(\`content\`, 256), \`send_time\` FROM \`pas\`.\`mail\` LIMIT 0, 1000

3.2 DBAS 存储检索体系重构方案

综合 DBAS 的数据特征和存储检索需求, DBAS 存储检索体系重构方案以 Hadoop 核心模块 HDFS 和 MapReduce 及其 HBase 整套体系来替换 DBAS 传统上单一 RDMS 的存储检索体系. 重构方案以具有列存储特性的 HBase 作为 DBAS 采集引擎模块写入和 Web 审计应用模块读取的数据库, 集成伪分布的 HDFS 存储和 MapReduce 运算框架, 支持 DBAS 单机大数据量的高速并发读写, 提升 RDMS 的读写性能.

重构方案重点研究 HBase 表结构设计、HBase 集成 HDFS 和 MapReduce、以及 DBAS 实时检索的实现.

1) HBase 表结构设计

针对表2信息, 综合DBAS检索的常用场景, 重构方案中将按照 4W 审计需求来定义 HBase 的列存储表结构, 如表 3 所示.

在 RDMS 中, 一般建立操作类型和时间作为索引满足常用查询, 重构方案中的 HBase 存储结构便以操作类型作为 Row 行键.

表 3　HBase 表结构

<table>
<tr><td colspan="6">DB Audit Table</td></tr>
<tr><td rowspan="2">Row Key</td><td rowspan="2">Timestamp</td><td colspan="4">Column Family</td></tr>
<tr><td>Field1</td><td>Field2</td><td>Field3</td><td>…</td></tr>
<tr><td rowspan="3">操作类型</td><td>操作时间 1</td><td>SQL 语句</td><td>数据库用户名</td><td>操作对象</td><td>…</td></tr>
<tr><td>操作时间 2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td></tr>
</table>

2) HBase 集成 HDFS 和 MapReduce

Web 审计应用模块提出的检索业务逻辑, 通过 HBase 提交到 MapReduce 作业, 而 MapReduce 基于 HDFS 上存储的 HBase 表运算并输出 HBase 表, 提供给 Web 审计应用统计分析结果, 三者集成的具体数据流如图 2 所示.

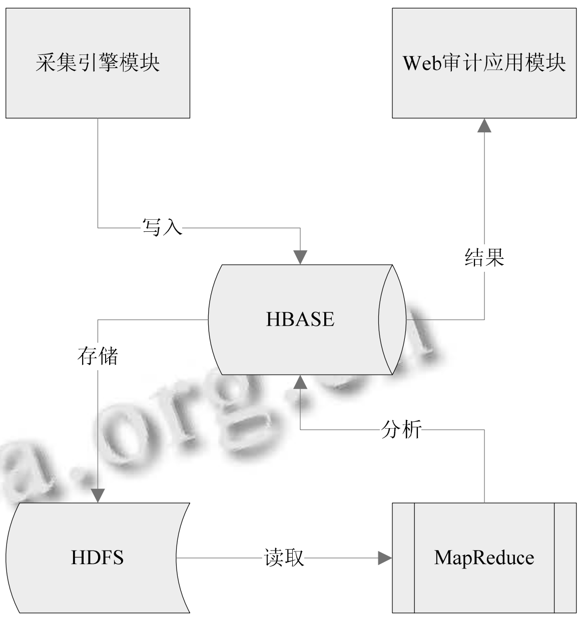

图 2　DBAS 数据流图

HBase 按行键分成<key,value>对存储在 HDFS, key 值对应行健, value 值为该行所包含的数据, 定义 MapReduce 的 Mapper 类和 Reducer 类支持 Web 审计应用模块提出的检索业务需求.

3) DBAS 实时检索的实现

不同于RDMS满足规范性数据持续性写入的存储和分析需求, Hadoop 适合应用于一次写入、多次读取的数据操作场景. 针对 DBAS 持续性写入 HBase 的需求, 重点研究数据实时存储到 HDFS 的实现.

HBase 底层的存储是采用 key/value 的文件结构, 写操作有三个步骤: 1)写入 HLog, 防止宕机丢失数据; 2)按 row 有序写入对应的 memstore 内存; 3)当 memstore 写满时, 数据被 flush 到 HDFS, 持久化到新的 storefile 数据文件. 基于 HBase 的存储机制, 应结合实际生产情况来设置 memstore 被 flush 时的阈值, 同时采集引擎模块建立多级缓存.

4 实验案例

DBAS 部署在 X86 结构的单服务器上, 操作系统为 centos, 采用 RAID1 镜像结构, 整体资源优先满足网卡采集的 IP 包持续性写入, 再而尽快响应大数据量读取的检索. 实验以某三甲医院 DBAS 为案例, 存储记录月表 8000 万条左右、存储空间 50G 左右.

在软硬环境一致、读写数据量和频度一致的情况下, 部署两套独立的 DBAS 及其存储检索数据库, A 方案采用 Mysql, B 方案基于 Hadoop 平台的 HBase. 实验中, 在正常生产情况下和资源优先保障磁盘写入下, 分别对两套独立的 DBAS 执行三类常见的检索场景, 观察磁盘 IO 和 CPU/内存利用率, 比较两个方案三类场景的执行响应时间.

场景一: 统计 delete 操作的次数, delete 的数据库操作记录比较少, 是审计中的敏感点, 经常被检索; 场景二: 统计 select 操作的次数, select 记录最多, 经常用于统计各类审计事件; 场景三: 查询两类处方药联合出现的记录, 是医院防统方的主要审计点. 三类场景执行的响应速度如图 3 执行时间, 并观察执行区间的资源利用率.

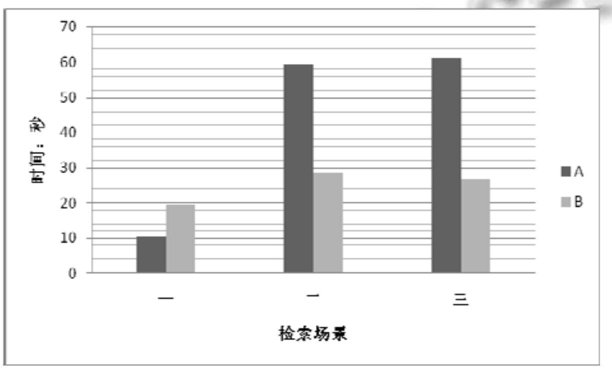

图 3 执行时间

首先, A 方案中, 磁盘 IO 保持在较高水平, 接近 30M/S 的满负荷状态, 而 B 方案基本在 10M/S 左右, 在同样数据量写入情况下, A 方案 Mysql 在读取 IO 请求上占用过高资源; 其次, A 方案的 CPU 和内存占用 80%以上, 而 B 方案基本维持在 50%左右. A 方案的资源利用率达到临界, 一旦出现突发数据请求, 则会出现系统各类响应延迟, 写入溢出; 而 B 方案还有很多资源空间来满足生产.

最后, 分析两个方案三个场景的执行时间: 1)场景一上 A 方案响应快, 主要在于 delete 记录少且 Mysql 针对操作类型建立索引; 2)场景二随着查询数据量的体积倍增, B 方案优势明显, 且实验中 A 方案仅做单表统计, 如果涉及跨月联表查询, A 方案性能更低; 3)场景三两个方案的执行速度和场景二一样, 对 A 方案来说, 处方药联合出现的查询事前无法建立索引和存储块, 全表检索耗时巨大.

在实验案例中, 更多的同类场景执行, 发现 B 方案的响应时间基本稳定在 20 秒上下, 而 A 方案检索大数据量的情况就要到 60 秒以上, 可见 HBase 列存储模型、HDFS 流式数据读取模式、MapReduce 批处理方式在大数据检索方面的优势.

5 展望

本文基于 DBAS 存储检索的现状, 应用 Hadoop 平台及其生态圈数据库 HBase 重构 DBAS 存储检索体系, 从 DBAS 的检索需求和数据特点出发, 研究 HDFS 及 MapReduce 机制和 HBase 的集成, 使三者有效发挥以提高 DBAS 单节点检索性能.

在实际产品运行中, 重构方案明显提升了 DBAS 检索性能, 但数据体积的不断膨胀和高可靠性要求, 面对审计产品行业应用的个性化要求, 展望未来, 综合权衡 DBAS 的生产现状和成本下, 研究 Hadoop 和 HBase 分布式[21,22]来支持 DBAS 存储检索是一个方向.

参考文献

1 吴溥峰,张玉清.数据库安全综述.计算机工程,2006, 32(12):85–88.

2 叶碧野.计算机数据库入侵检测技术探析.电脑知识与技术, 2012,8(2X):1012–1014.

3 肖大薇.计算机数据库入侵检测技术分析研究.信息系统工程,2012,(4):54–55.

4 晏明春,李酒.一种新型在线数据库审计系统.计算机工程与设计,2007,28(5):1012–1015.

5 杨磊.数据库安全审计检测系统的设计与实现[硕士学位论文].北京:北京交通大学,2014.

6 安鹏.基于云架构的统一审计平台设计与实现[硕士学位论文].长春:吉林大学,2015.

7 聂元铭,吴晓明.基于数据库安全审计的研究.信息网络安全,2009,(6):4–6.

8 Cerrato I, Annarumma M, Risso F. Supporting fine-grained network functions through intel DPDK. 2014 Third European Workshop on Software Defined Networks (EWSDN). IEEE Computer Society. 2014. 1–6.

9 Pongracz G, Molnar L, Kis ZL. Removing roadblocks from SDN: OpenFlow software switch performance on intel DPDK. 2013 Second European Workshop on Software Defined Networks. IEEE Computer Society. 2013. 62–67.

10 刘晨莹.数据库审计系统中数据快速查询与智能分析设计与实现[硕士学位论文].保定:华北电力大学,2015.

11 李凯,杨永清,范渊.一种在大数据量存储中快速检索的方法:CN, 2012. CN 102184222 B.

12 White T. Hadoop: The definitive guide. O'reilly Media IncGravenstein Highway North, 2010, 215(11): 1–4.

13 Kaushik RT, Bhandarkar M, Nahrstedt K. Evaluation and analysis of GreenHDFS: A self-adaptive, energy-conserving variant of the Hadoop distributed file system. IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010. IEEE. 2010. 274–287.

14 Wang L, Tao J, Ranjan R, et al. G-Hadoop: MapReduce across distributed data centers for data-intensive computing . Future Generation Computer Systems, 2013, 29(3): 739–750.

15 George L. HBase: The definitive guide. Andre, 2011, 12(1): 1–4.

16 Taylor RC. An overview of the Hadoop/MapReduce/HBase framework and its current applications in bioinformatics. Bmc Bioinformatics, 2010, 11(6): 3395–3407.

17 邓攀,刘功申.一种高效的倒排索引存储结构.计算机工程与应用,2008,44(31):149–152.

18 王欢,许暖,沈波.基于大数据的智能审计平台研究.电信工程技术与标准化,2014,(12):19–22.

19 张萌.基于 hadoop 的网络安全日志审计系统关键技术研究[硕士学位论文].哈尔滨:哈尔滨工程大学,2013.

20 翟岩龙,罗壮,杨凯,等.基于 Hadoop 的高性能海量数据处理平台研究.计算机科学,2013,40(3):100–103.

21 施磊磊,施化吉,束长波,等.基于 Hadoop 和 HBase 的分布式索引模型的研究.信息技术,2015,(6):109–111.

22 万轶,向广利.基于hadoop和hbase的分布式索引集群研究.信息技术与信息化,2015,(1):102–103.