(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102970158 B
(45)授权公告日 2017.02.08

(21)申请号 201210437253.6

(22)申请日 2012.11.05

(65)同一申请的已公布的文献号
申请公布号 CN 102970158 A

(43)申请公布日 2013.03.13

(73)专利权人 广东睿江云计算股份有限公司
地址 528000 广东省佛山市禅城区岭南大道北121号二座705-708房

(72)发明人 何作祥 闵宇 史伟 麦剑

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 马晓亚

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 102622407 A,2012.08.01,
CN 102236581 A,2011.11.09,
CN 102622407 A,2012.08.01,
US 2002/0147736 A1,2002.10.10,

审查员 高悦

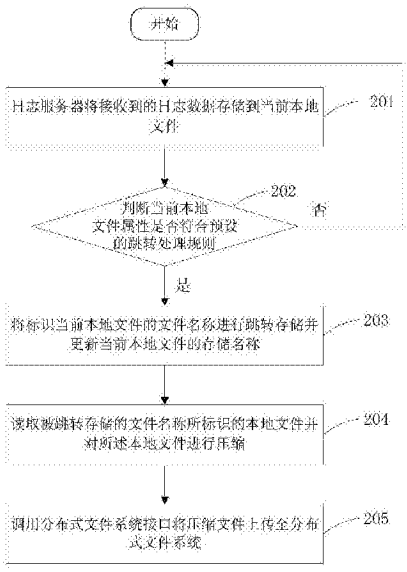
权利要求书2页 说明书5页 附图4页

(54)发明名称

日志存储与处理的方法及日志服务器

(57)摘要

本发明公开了一种日志存储与处理的方法及日志服务器，先将日志数据存储成文件，并对文件进行压缩后上传至分布式文件系统，该方法先压缩后存储，减少了存储空间的占用；分布式存储使得日志的存储容量可以动态扩展；副本备份上传，保证了数据能够安全存储；分布式处理数据时，能够对多个数据块进行同步处理，提高了大数据处理的能力，提高了系统性能。



CN 102970158 B

1.一种日志存储的方法，其特征在于，包括：

日志服务器将接收到的日志数据存储到当前本地文件；

判断所述当前本地文件的属性是否符合预设的跳转处理规则；

如否，继续向所述当前本地文件存储日志数据；如是，将标识当前本地文件的文件名称进行跳转存储并更新当前本地文件的存储名称；

读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

调用分布式文件系统接口将压缩文件上传至分布式文件系统；

其中，所述当前本地文件的属性包括文件大小和当前时间，预设的跳转处理规则包括：

判断当前本地文件大小是否超过预设的文件大小阈值或者判断当前时间与文件生成时间是否不属于同一个预设的存储时间周期。

2.根据权利要求1所述的日志存储方法，其特征在于，所述对所述本地文件进行压缩包括，采用Lempel-Ziv-Oberhumer算法将本地文件压缩成二进制文件。

3.根据权利要求1所述的日志存储方法，其特征在于，所述方法还包括定时执行步骤，所述定时执行步骤为在预定时间对前一个存储时间周期内的被跳转存储的文件名称所标识的本地文件进行上传情况检查，如有未上传的本地文件，进行本地文件压缩后补上传，并删除所述前一个存储时间周期之前的日志数据。

4.一种日志服务器，所述日志服务器包括日志存储模块和日志处理模块，其特征在于，所述日志存储模块包括创建单元、判断单元、跳转单元、更新单元、压缩单元和发送单元，所述日志处理模块包括分配单元、关键信息提取单元和关键信息统计合并单元，

所述创建单元，与判断单元连接，用于创建当前本地文件并存储接收到的日志数据；

所述判断单元，分别与创建单元和跳转单元连接，用于判断当前本地文件属性是否符合预设的跳转处理规则；

所述跳转单元，分别与判断单元、更新单元和压缩单元连接，用于在当前本地文件的属性符合预设的跳转处理规则时，将标识当前本地文件的文件名称进行跳转存储；

所述更新单元，分别与跳转单元和创建单元连接，用于更新当前本地文件的存储名称；

所述压缩单元，分别与跳转单元和发送单元连接，用于读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

所述发送单元，与压缩单元连接，用于调用分布式文件系统接口将压缩文件上传至分布式文件系统；

所述分配单元，与关键信息提取单元连接，用于主服务器将待处理的日志数据分块，分配给从服务器；

所述关键信息提取单元，分别与关键信息统计合并单元和分配单元连接，用于从服务器从日志数据中提取关键信息；

所述关键信息统计合并单元，与关键信息提取单元连接，用于主服务器根据所述关键信息对日志数据进行统计合并；

其中，所述当前本地文件的属性包括文件大小和当前时间，预设的跳转处理规则包括：

判断当前本地文件大小是否超过预设的文件大小阈值或者判断当前时间与文件生成时间是否不属于同一个预设的存储时间周期。

5.根据权利要求4所述的日志服务器，其特征在于，所述压缩单元采用Lempel-Ziv-

Oberhumer算法将本地文件压缩成二进制文件。

6.根据权利要求4所述的日志服务器，其特征在于，所述日志存储模块还包括定时执行单元，分别与跳转单元和压缩单元连接，用于在预定时间对前一个存储时间周期内的被跳转存储的文件名称所标识的本地文件进行上传情况检查，如有未上传的本地文件，进行本地文件压缩后补上传，并删除所述前一个存储时间周期之前的日志数据。

日志存储与处理的方法及日志服务器

技术领域

[0001] 本发明涉及日志管理技术领域，尤其涉及一种日志存储与处理的方法及日志服务器。

背景技术

[0002] 日志是网络设备、系统及服务程序等在运行时产生的一个叫log的事件记录；每一行日志都记载着日期、时间、使用者及动作等相关操作的描述信息。日志记录了系统的生命周期，通过查阅日志，可以了解到系统在某个时刻所处的状态；通过对日志的分析，收集有用的数据，可以得到用户的使用信息和访问统计，为服务系统的优化和网络安全问题预防等提供依据。

[0003] 日志的存储与处理分析，是一个成熟的服务系统必不可少的。图1为现有技术中日志存储和处理的过程流程图，包括：1)应用程序通过调用syslog()函数，产生日志数据，并发送到syslog服务程序；2)syslog服务程序将日志数据重定向到日志服务器(日志数据实质是通过udp报文的方式发送到日志服务器的53端口)；3)日志服务器的syslog-ng服务程序收到日志后，将日志存储到本地磁盘中；4)日志服务器上的日志处理程序，对保存在本地的日志数据进行处理，得到关键信息。

[0004] 云存储和大数据背景下，面对海量的存储数据，现有的日志存储和处理方法存在如下几方面不足：1)日志服务器的存储空间是有限的，使得日志存储的空间也是有限的；2)日志没有经过压缩处理，直接存储到磁盘，浪费很多存储空间；3)日志存储没有做备份处理，很容易做成日志的大量丢失；4)单台的服务器对日志进行处理，性能有限，处理时间长，无法很好的对大数据进行处理。

[0005] 针对以上问题，本方案提出了一种分布式日志存储与处理的方法。

发明内容

[0006] 本发明要解决的技术问题是提供一种日志存储与处理的方法及日志服务器，通过分布式文件系统存储日志数据，使得系统的存储空间可动态扩展，分布式文件系统通过文件备份，能够实现安全存储；同时，分布式处理很好的解决了大数据处理难的问题。

[0007] 为达到上述目的，本发明是通过以下技术方案来实现的：

[0008] 一种日志存储的方法，包括：

[0009] 日志服务器将接收到的日志数据存储到当前本地文件；

[0010] 判断所述当前本地文件的属性是否符合预设的跳转处理规则，

[0011] 如否，继续向所述当前本地文件存储日志数据；如是，将标识当前本地文件的文件名称进行跳转存储并更新当前本地文件的存储名称；

[0012] 读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

[0013] 调用分布式文件系统接口将压缩文件上传至分布式文件系统。

[0014] 一种日志处理的方法，基于分布式文件系统实现，包括步骤，

[0015] 主服务器将待处理的日志数据分块，分配给从服务器；

[0016] 从服务器从日志数据中提取关键信息；

[0017] 主服务器根据所述关键信息对日志数据进行统计合并。

[0018] 一种日志服务器，

[0019] 所述日志存储模块包括创建单元、判断单元、跳转单元、更新单元、压缩单元和发送单元，所述日志处理模块包括分配单元、关键信息提取单元和关键信息统计合并单元，

[0020] 所述创建单元，与判断单元连接，用于创建当前本地文件并存储接收到的日志数据；

[0021] 所述判断单元，分别与创建单元和跳转单元连接，用于判断当前本地文件属性是否符合预设的跳转处理规则；

[0022] 所述跳转单元，分别与判断单元、更新单元和压缩单元连接，用于在当前本地文件的属性符合预设的跳转处理规则时，将标识当前本地文件的文件名称进行跳转存储；

[0023] 所述更新单元，分别与跳转单元和创建单元连接，用于更新当前本地文件的存储名称；

[0024] 所述压缩单元，分别与跳转单元和发送单元连接，用于读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

[0025] 所述发送单元，与压缩单元连接，用于调用分布式文件系统接口将压缩文件上传至分布式文件系统；

[0026] 所述分配单元，与关键信息提取单元连接，用于主服务器将待处理的日志数据分块，分配给从服务器；

[0027] 所述关键信息提取单元，分别与关键信息统计合并单元和分配单元连接，用于从服务器从日志数据中提取关键信息；

[0028] 所述关键信息统计合并单元，与关键信息提取单元连接，用于主服务器根据所述关键信息对日志数据进行统计合并。

[0029] 本发明的技术方案，先将日志数据存储成文件，并对文件进行压缩后上传至分布式文件系统，该方法先压缩后存储，减少了存储空间的占用；分布式存储使得日志的存储容量可以动态扩展；副本备份上传，保证了数据能够安全存储；分布式处理数据时，能够对多个数据块进行同步处理，提高了大数据处理的能力，提高了系统性能。

附图说明

[0030] 图1为现有技术中日志存储和处理的过程流程图；

[0031] 图2为本发明实施例的日志存储的方法流程图；

[0032] 图3为本发明实施例一提供的日志存储的具体方法流程图；

[0033] 图4为本发明实施例的日志处理的方法流程图；

[0034] 图5为本发明实施例的日志服务器的结构示意图。

具体实施方式

[0035] 下面结合附图和实施例对本发明作进一步说明。

[0036] 图2为本发明实施例的日志存储的方法流程图。如图2所示，该方法包括，

[0037] 步骤201：日志服务器将接收到的日志数据存储到当前本地文件；

[0038] 日志存储程序接收日志数据，并分析日志数据来源的ip地址，把收到的日志数据保存到本地文件中，所述文件存储名称命名如下：{/opt/log/ip地址/日期/时间}。

[0039] 步骤202：判断所述当前本地文件的属性是否符合预设的跳转处理规则；

[0040] 所述当前本地文件的属性包括文件大小和当前时间，

[0041] 预设的跳转处理规则包括：

[0042] 判断当前本地文件大小是否超过预设的文件大小阈值或者判断当前时间与文件生成时间是否不属于同一个预设的存储时间周期。

[0043] 步骤203：如否，继续向所述当前本地文件存储日志数据；如是，将标识当前本地文件的文件名称进行跳转存储并更新当前本地文件的存储名称；

[0044] 所述跳转存储包括，将标识当前本地文件的文件名称压入到存储队列，所述存储队列为一系列地址连续的存储空间，可以按照先入先出的规则进行数据存储。

[0045] 步骤204：读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

[0046] 日志存储程序利用另一进程读取被跳转存储的文件名，即将存储队列中已存储的标识本地文件的文件名称进行出队，采用lzo算法将该文件名存储的本地文件压缩成二进制文件，所述本地文件以文本形式进行存储。

[0047] 步骤205：调用分布式文件系统接口将压缩文件上传至分布式文件系统。

[0048] 文件上传的目录名称与本地文件的名称结构相同。

[0049] 该方法还包括定时执行的步骤，所述定时执行步骤为在预定时间对前一个存储时间周期内的被跳转存储的文件名称所标识的本地文件进行上传情况检查，如有未上传的本地文件，进行本地文件压缩后补上传，并删除所述前一个存储时间周期之前的日志数据。

[0050] 分布式文件系统，将待存储数据分散存储在多台独立的设备上。开源项目hadoop提供了对分布式存储与分布式处理的基础接口。hadoop的hdfs提供分布式存储能力，hdfs是将一个大文件分成若干块，每块将有若干个副本，每个副本存储在不同的服务器上，这样便将一个大文件存储到多台服务器上，并实现了安全的文件备份(多个副本)。

[0051] 图3为本发明实施例一提供的日志存储的方法流程图。具体流程包括如下步骤：

[0052] 步骤301：应用程序通过调用syslog程序(syslog，一个linux服务器的日志处理程序)记录日志数据，服务器通过系统的syslog程序，将日志数据发往日志服务器，假定应用服务器的ip地址为192.168.1.100。

[0053] 步骤302：日志服务器中的日志存储程序接收日志数据，并分析日志数据来源的ip地址，假定为192.168.1.100，程序把收到的日志数据保存到创建的本地文件{/opt/log/ip地址/日期/时间}中，其中ip地址为192.168.1.100，时间则为文件首次写入时的时分秒值，例如

[0054] “/opt/log/192.168.1.100/2012-09-01/12-50-55”。

[0055] 所述日志数据以文本形式存储。

[0056] 步骤303：日志存储程序向当前本地文件写入日志数据后，预设文件大小的存储阈值(如50M、100M等)和存储时间周期(如一天、一周、一个月等)，判断当前本地文件的大小和当前时间，若当前本地文件大小超过预设的文件大小阀值或当前时间与文件生成的时间不

属于同一个预设的存储时间周期(如将存储时间周期设为一天,则当前时间与文件生成的时间不属于同一天),便把标识当前本地文件的文件名称压入存储队列并更新当前本地文件的保存名称,更新后的本地文件保存名称为{/opt/log/ip地址/当前时间},当下一个日志数据被写入时,会默认写入到更新后的本地文件中。

[0057] 步骤304:日志存储程序的另一个线程将步骤303中压入存储队列的标识旧的本地文件的文件名称出队,并通过lzo算法将文本文件压缩成二进制文件。

[0058] Lzo(Lempel-Ziv-Oberhumer)是致力于解压速度的一种数据压缩算法,能够实现最快的压缩/解压,在进行日志处理时,还支持直接以lzo的格式输入数据提取关键信息。

[0059] 步骤305:程序通过调用分布式文件系统接口,将压缩后的文件上传上分布式文件系统(Hadoop Distributed File System,hdfs),上传的文件目录名称为{/log/ip址/日期/时间},与本地文件的存储名称结构相同,如:

[0060] “/log/192.168.1.100/2012-09-01/12-50-55.lzo。”

[0061] 所述压缩文件上传分两步进行:先获取压缩文件的下一个块(默认块大小为64M),并向分布式文件系统的主服务器(master)申请一个块的空间,主服务器返回n(n为系统设定的副本数,默认为3)个从服务器(slave)的地址;程序将块的n个副本,分别保存到从服务器上。

[0062] 通过上述两个步骤循环执行,直到执行到压缩文件末尾的一个块。这样,压缩文件便成功保存到分布式的文件系统上了,而文件在分布式文件系统的目录保存在主服务器上。

[0063] 该方法还包括一个定时执行的步骤,所述定时执行的步骤包括,定时执行程序在预定时间(如凌晨3点)执行,对前一个存储时间周期内的被跳转存储的文件名称所标识的本地文件进行上传情况检查,如有未上传的本地文件,进行本地文件压缩后补上传,并删除所述前一个存储时间周期之前的日志数据。。

[0064] 分布式日志存储首先将日志存储成文件,再压缩成更小的文件,再将压缩后的文件存储到分布式文件系统,该方法减少了存储空间的占用,使得系统的存储空间可以动态扩展,同时文件的备份处理,实现了安全存储的目的。

[0065] 图4为本发明实施例的日志处理的方法流程图。如图4所示,该方法包括,

[0066] 步骤401:主服务器将待处理的日志数据分块,分配给从服务器;

[0067] 步骤402:从服务器从日志数据中提取关键信息;

[0068] 该步骤可以通过输入lzo格式的数据提取关键信息。

[0069] 步骤403:主服务器根据所述关键信息对日志数据进行统计合并。

[0070] 分布式处理是将数据处理任务分散到不同的设备上同时运行处理。基于hdfs的mapreduce程序(一种编程模型)提供了对大数据进行分布式处理的功能。

[0071] 分布式的日志处理程序首先由主服务器将要处理的数据分成若干份,并分派到若干个从服务器,MapReduce分布式处理的过程分两个阶段进行:map阶段从每行的日志记录中提取关键信息,并提交到执行reduce任务的机器;reduce阶段根据所述关键信息对数据进行统计合并,并把输出结果保存到分布式文件系统。

[0072] 分布式处理以分布式存储为基础,很好地解决了大数据难以处理的问题。先将数据分析的工作分成多个小的任务,分派给不同的从服务器完成,并把统计结果汇总到主服

务器，能够实现同步处理的效果。

[0073] 图5为本发明实施例的日志服务器的结构示意图。如图5所示，所述服务器包括日志存储模块50和日志处理模块51，所述日志存储模块50包括创建单元501、判断单元502、跳转单元503、更新单元504、压缩单元505和发送单元506，所述日志处理模块51包括分配单元511、关键信息提取单元512和关键信息统计合并单元513，

[0074] 所述创建单元501，与判断单元502连接，用于创建当前本地文件并存储接收到的日志数据；

[0075] 所述判断单元502，分别与创建单元501和跳转单元503连接，用于判断当前本地文件属性是否符合预设的跳转处理规则；

[0076] 所述跳转单元503，分别与判断单元502、更新单元504和压缩单元505连接，用于在当前本地文件的属性符合预设的跳转处理规则时，将标识当前本地文件的文件名称进行跳转存储；

[0077] 所述更新单元504，分别与跳转单元503和创建单元501连接，用于更新当前本地文件的存储名称；

[0078] 所述压缩单元505，分别与跳转单元503和发送单元506连接，用于读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩；

[0079] 所述发送单元506，与压缩单元505连接，用于调用分布式文件系统接口将压缩文件上传至分布式文件系统；

[0080] 所述分配单元511，与关键信息提取单元512连接，用于主服务器将待处理的日志数据分块，分配给从服务器；

[0081] 所述关键信息提取单元512，分别与关键信息统计合并单元513和分配单元511连接，用于从服务器从日志数据中提取关键信息；

[0082] 所述关键信息统计合并单元513，与关键信息提取单元512连接，用于主服务器根据所述关键信息对日志数据进行统计合并。

[0083] 此外，所述日志存储模块还包括定时执行单元507，分别与跳转单元503和压缩单元505连接，用于在预定时间对前一个存储时间周期内的被跳转存储的文件名称所标识的本地文件进行上传情况检查，如有未上传的本地文件，进行本地文件压缩后补上传，并删除所述前一个存储时间周期之前的日志数据。

[0084] 本发明的技术方案，先将日志数据存储成文件，并对文件进行压缩后上传至分布式文件系统，该方法减少了存储空间的占用；分布式文件系统使得日志的存储容量可以动态扩展；副本备份上传，保证了数据能够安全存储；分布式处理数据时，能够对多个数据块进行同步处理，提高了大数据处理的能力，提高了系统性能。

[0085] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，所述的存储介质，如：ROM/RAM、磁碟、光盘等。

[0086] 上述仅为本发明的较佳实施例及所运用技术原理，任何熟悉本技术领域的技术人员在本发明披露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围内。

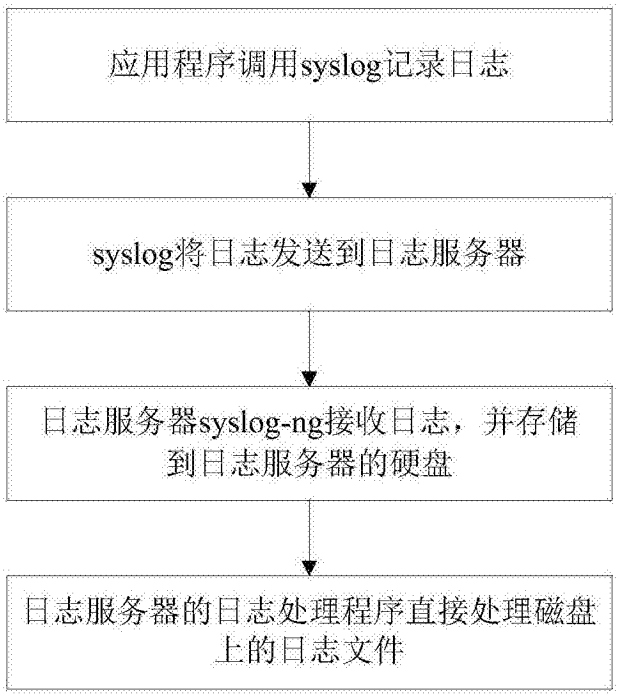

应用程序调用syslog记录日志
syslog将日志发送到日志服务器
日志服务器syslog-ng接收日志，并存储到日志服务器的硬盘
日志服务器的日志处理程序直接处理磁盘上的日志文件

图1

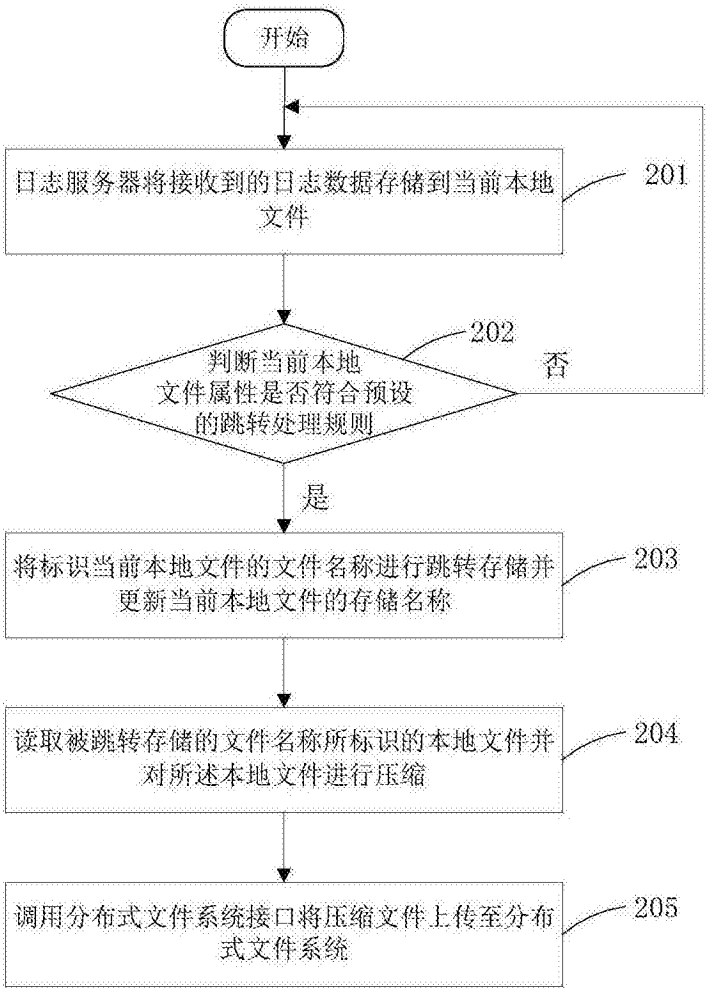

开始
日志服务器将接收到的日志数据存储到当前本地文件
201
判断当前本地文件属性是否符合预设的跳转处理规则
202
否
是
将标识当前本地文件的文件名称进行跳转存储并更新当前本地文件的存储名称
203
读取被跳转存储的文件名称所标识的本地文件并对所述本地文件进行压缩
204
调用分布式文件系统接口将压缩文件上传至分布式文件系统
205

图2

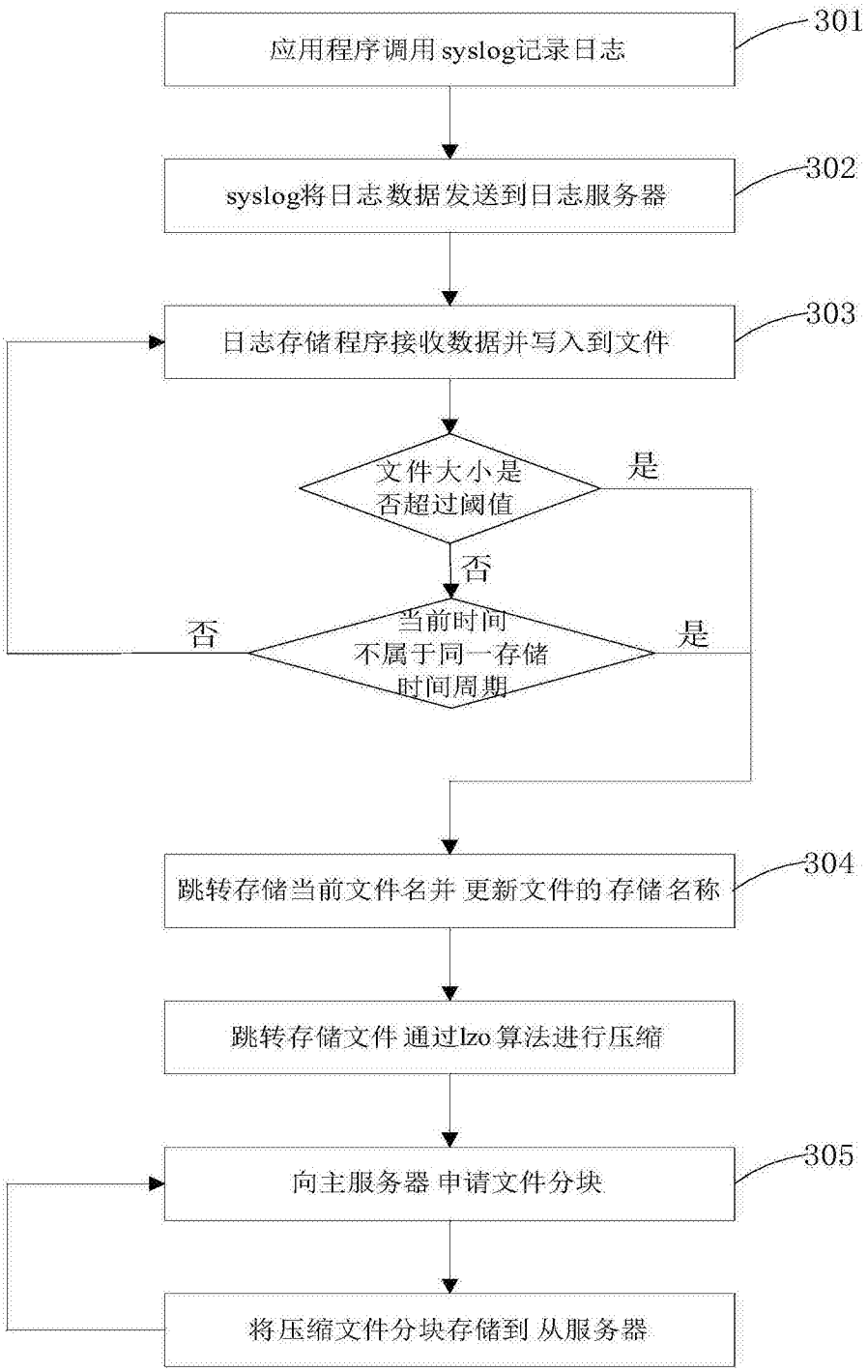

应用程序调用 syslog记录日志
301
syslog将日志数据发送到日志服务器
302
日志存储程序接收数据并写入到文件
303
文件大小是否超过阈值
是
否
当前时间不属于同一存储时间周期
否
是
跳转存储当前文件名并 更新文件的 存储 名称
304
跳转存储文件 通过lzo 算法进行压缩
向主服务器 申请文件分块
305
将压缩文件分块存储到 从服务器

图3

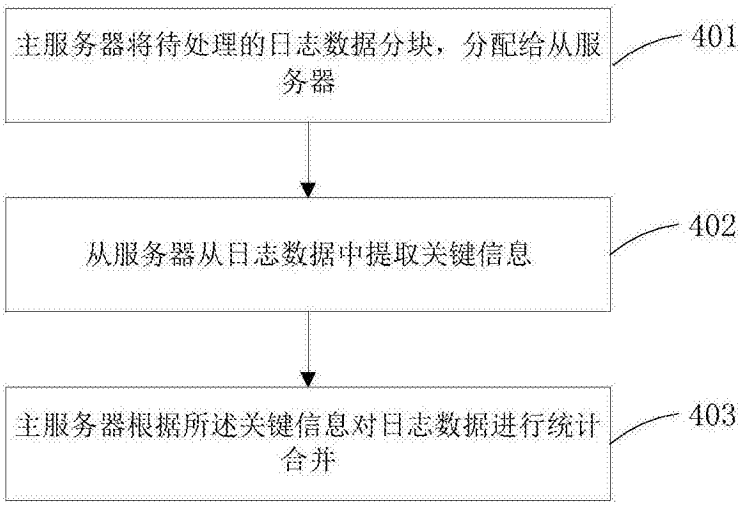

主服务器将待处理的日志数据分块，分配给从服务器
401
从服务器从日志数据中提取关键信息
402
主服务器根据所述关键信息对日志数据进行统计合并
403

图4

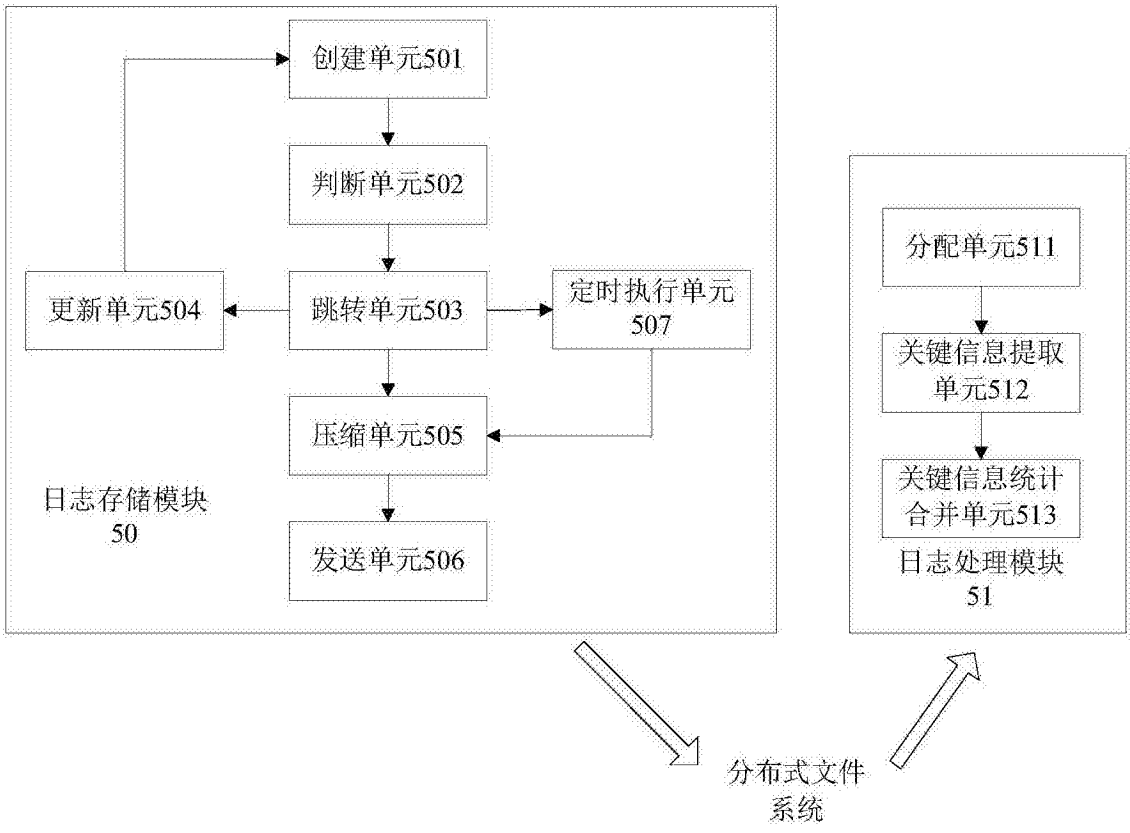

创建单元501
判断单元502
更新单元504
跳转单元503
定时执行单元507
压缩单元505
发送单元506
日志存储模块50
分配单元511
关键信息提取单元512
关键信息统计合并单元513
日志处理模块51
分布式文件系统

图5