(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110209518 A
(43)申请公布日 2019.09.06

(21)申请号 201910343502.7

(22)申请日 2019.04.26

(71)申请人 福州慧校通教育信息技术有限公司
地址 350000 福建省福州市闽侯县上街镇科技东路3号创新园一期6#楼3层

(72)发明人 王国美 林先榕

(74)专利代理机构 福州市鼓楼区京华专利事务所(普通合伙) 35212
代理人 林云娇

(51)Int.Cl.
G06F 11/07(2006.01)
G06F 16/18(2019.01)

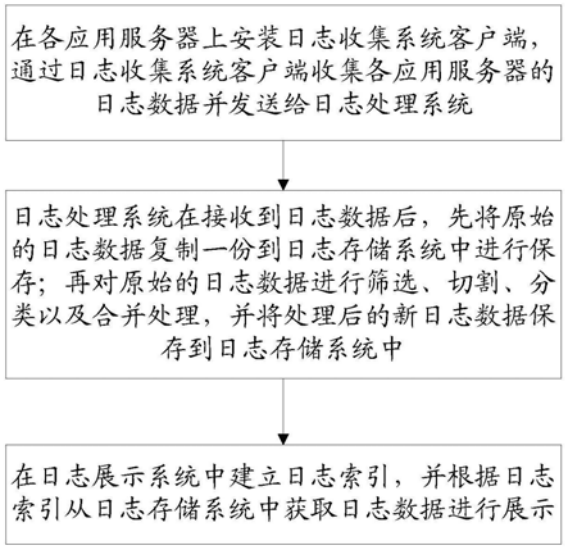
权利要求书3页 说明书8页 附图1页

(54)发明名称

一种多数据源日志数据集中收集存储方法及装置

(57)摘要

本发明提供一种多数据源日志数据集中收集存储方法,在各应用服务器上安装日志收集系统客户端,通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统;日志处理系统在接收到日志数据后,先将原始的日志数据复制一份到日志存储系统中进行保存;再对原始的日志数据进行筛选、切割、分类以及合并处理,并将处理后的新日志数据保存到日志存储系统中;在日志展示系统中建立日志索引,并根据日志索引从日志存储系统中获取日志数据进行展示。本发明还提供一种方法所对应的装置。通过本发明来实现多数据源日志的收集存储和检索,可提高故障处理效率,提升数据分析能力,并为后期的故障排查奠定良好的基础。



CN 110209518 A

1.一种多数据源日志数据集中收集存储方法,其特征在于:所述方法包括如下步骤:

步骤S1、在各应用服务器上安装日志收集系统客户端,通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统;

步骤S2、日志处理系统在接收到日志数据后,先将原始的日志数据复制一份到日志存储系统中进行保存;再对原始的日志数据进行筛选、切割、分类以及合并处理,并将处理后的新日志数据保存到日志存储系统中;

步骤S3、在日志展示系统中建立日志索引,并根据日志索引从日志存储系统中获取日志数据进行展示。

2.根据权利要求1所述的一种多数据源日志数据集中收集存储方法,其特征在于:所述步骤S2还包括:

在对原始的日志数据进行处理时,日志处理系统对新日志数据中的日志内容属性进行扫描,并自动匹配告警规则,且根据告警规则触发日志预警系统发送警报内容进行告警;所述警报内容包括应用服务器IP、日志别名、日志路径以及日志内容。

3.根据权利要求1所述的一种多数据源日志数据集中收集存储方法,其特征在于:所述步骤S1具体为:

在各应用服务器上安装日志收集系统客户端,并对日志收集系统的配置文件进行参数配置,配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志处理系统的地址以及日志间隔时间;

运行日志收集系统的应用程序,应用程序读取配置文件,并检查配置文件是否正确,如果否,则停止应用程序的运行,并发送提示消息给日志收集系统客户端;如果是,则按照配置文件中配置的收集规则扫描对应的日志文件,并将扫描到的日志数据实时发送给日志处理系统。

4.根据权利要求1所述的一种多数据源日志数据集中收集存储方法,其特征在于:所述日志存储系统上设置有一个本地服务器节点以及至少一个服务器从节点;

所述步骤S2具体包括:

步骤S21、日志处理系统在接收到日志数据后,将原始的日志数据复制一份给日志存储系统,日志存储系统将原始的日志数据保存至本地服务器节点上,同时将原始的日志数据同步给各服务器从节点;

步骤S22、日志处理系统对原始的日志数据进行属性提取,按照设定的属性合并规则来合并新日志数据,并根据设置的分类类型来对新日志数据进行分类;其中,提取的属性包括应用服务器IP、日志别名、日志路径、日志类型、服务器名称、日志内容、日志级别或者自定义属性;

步骤S23、将处理后的新日志数据发送给日志存储系统,日志存储系统将新日志数据保存至本地服务器节点上,同时将新日志数据同步给各服务器从节点。

5.根据权利要求1所述的一种多数据源日志数据集中收集存储方法,其特征在于:所述步骤S3具体为:

日志展示系统对存储在日志存储系统中的新日志数据进行扫描,并根据用户在日志展示系统的界面中设定的检索规则来建立日志索引,以从日志存储系统获取到对应的日志数据;

日志展示系统根据不同的属性来对获取的日志数据进行展示，或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示。

6.一种多数据源日志数据集中收集存储装置，其特征在于：所述装置包括日志收集模块、日志处理模块以及日志展示模块；

所述日志收集模块，用于在各应用服务器上安装日志收集系统客户端，通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统；

所述日志处理模块，用于日志处理系统在接收到日志数据后，先将原始的日志数据复制一份到日志存储系统中进行保存；再对原始的日志数据进行筛选、切割、分类以及合并处理，并将处理后的新日志数据保存到日志存储系统中；

所述日志展示模块，用于在日志展示系统中建立日志索引，并根据日志索引从日志存储系统中获取日志数据进行展示。

7.根据权利要求6所述的一种多数据源日志数据集中收集存储装置，其特征在于：所述日志处理模块，还用于在对原始的日志数据进行处理时，日志处理系统对新日志数据中的日志内容属性进行扫描，并自动匹配告警规则，且根据告警规则触发日志预警系统发送警报内容进行告警；所述警报内容包括应用服务器IP、日志别名、日志路径以及日志内容。

8.根据权利要求6所述的一种多数据源日志数据集中收集存储装置，其特征在于：所述日志收集模块具体为：

在各应用服务器上安装日志收集系统客户端，并对日志收集系统的配置文件进行参数配置，配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志处理系统的地址以及日志间隔时间；

运行日志收集系统的应用程序，应用程序读取配置文件，并检查配置文件是否正确，如果否，则停止应用程序的运行，并发送提示消息给日志收集系统客户端；如果是，则按照配置文件中配置的收集规则扫描对应的日志文件，并将扫描到的日志数据实时发送给日志处理系统。

9.根据权利要求6所述的一种多数据源日志数据集中收集存储装置，其特征在于：所述日志存储系统上设置有一个本地服务器节点以及至少一个服务器从节点；

所述日志处理模块具体包括日志备份单元、日志处理单元以及日志存储单元；

所述日志备份单元，用于日志处理系统在接收到日志数据后，将原始的日志数据复制一份给日志存储系统，日志存储系统将原始的日志数据保存至本地服务器节点上，同时将原始的日志数据同步给各服务器从节点；

所述日志处理单元，用于日志处理系统对原始的日志数据进行属性提取，按照设定的属性合并规则来合并新日志数据，并根据设置的分类类型来对新日志数据进行分类；其中，提取的属性包括应用服务器IP、日志别名、日志路径、日志类型、服务器名称、日志内容、日志级别或者自定义属性；

所述日志存储单元，用于将处理后的新日志数据发送给日志存储系统，日志存储系统将新日志数据保存至本地服务器节点上，同时将新日志数据同步给各服务器从节点。

10.根据权利要求6所述的一种多数据源日志数据集中收集存储装置，其特征在于：

所述日志展示模块具体为：

日志展示系统对存储在日志存储系统中的新日志数据进行扫描，并根据用户在日志展

示系统的界面中设定的检索规则来建立日志索引,以从日志存储系统获取到对应的日志数据;

日志展示系统根据不同的属性来对获取的日志数据进行展示,或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示。

一种多数据源日志数据集中收集存储方法及装置

技术领域

[0001] 本发明涉及日志处理领域，特别涉及一种多数据源日志数据集中收集存储方法及装置。

背景技术

[0002] 分布式应用是由不同的运行于分离的运行环境下的组件构成的应用程序，通常是在不同的平台上通过网络互联起来。典型的分布式应用有二端(Client/Server)，三端(client/middleware/server)和n端(client/multiple middleware/multiple server)。

[0003] 目前，分布式应用集群已得到了广泛的应用。在分布式应用集群出现异常或故障时，为了降低异常或故障所造成的影响，技术人员都需要第一时间去进行异常排查或故障定位。传统情况下都是通过人工依次登录成群服务器节点进行硬件资源检测、操作系统状态检查、应用日志分析等步骤。但是，由于服务器集群存在地域分散性、排查步骤繁多等因素，因此，在具体进行排查或定位时，通常都需要消耗大量的时间，根本无法实现第一时间修复故障，这也导致企业SLA指标下降，并严重影响了系统用户的体验，同时也造成了企业的经济损失。

发明内容

[0004] 本发明要解决的技术问题之一，在于提供一种多数据源日志数据集中收集存储方法，通过该方法来实现多数据源日志的收集存储和检索，可提高故障处理效率，提升数据分析能力，并为后期的故障排查奠定良好的基础。

[0005] 本发明是这样实现技术问题之一的：一种多数据源日志数据集中收集存储方法，所述方法包括如下步骤：

[0006] 步骤S1、在各应用服务器上安装日志收集系统客户端，通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统；

[0007] 步骤S2、日志处理系统在接收到日志数据后，先将原始的日志数据复制一份到日志存储系统中进行保存；再对原始的日志数据进行筛选、切割、分类以及合并处理，并将处理后的新日志数据保存到日志存储系统中；

[0008] 步骤S3、在日志展示系统中建立日志索引，并根据日志索引从日志存储系统中获取日志数据进行展示。

[0009] 进一步地，所述步骤S2还包括：

[0010] 在对原始的日志数据进行处理时，日志处理系统对新日志数据中的日志内容属性进行扫描，并自动匹配告警规则，且根据告警规则触发日志预警系统发送警报内容进行告警；所述警报内容包括应用服务器IP、日志别名、日志路径以及日志内容。

[0011] 进一步地，所述步骤S1具体为：

[0012] 在各应用服务器上安装日志收集系统客户端，并对日志收集系统的配置文件进行参数配置，配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志

处理系统的地址以及日志间隔时间；

[0013] 运行日志收集系统的应用程序，应用程序读取配置文件，并检查配置文件是否正确，如果否，则停止应用程序的运行，并发送提示消息给日志收集系统客户端；如果是，则按照配置文件中配置的收集规则扫描对应的日志文件，并将扫描到的日志数据实时发送给日志处理系统。

[0014] 进一步地，所述日志存储系统上设置有一个本地服务器节点以及至少一个服务器从节点；

[0015] 所述步骤S2具体包括：

[0016] 步骤S21、日志处理系统在接收到日志数据后，将原始的日志数据复制一份给日志存储系统，日志存储系统将原始的日志数据保存至本地服务器节点上，同时将原始的日志数据同步给各服务器从节点；

[0017] 步骤S22、日志处理系统对原始的日志数据进行属性提取，按照设定的属性合并规则来合并新日志数据，并根据设置的分类类型来对新日志数据进行分类；其中，提取的属性包括应用服务器IP、日志别名、日志路径、日志类型、服务器名称、日志内容、日志级别或者自定义属性；

[0018] 步骤S23、将处理后的新日志数据发送给日志存储系统，日志存储系统将新日志数据保存至本地服务器节点上，同时将新日志数据同步给各服务器从节点。

[0019] 进一步地，所述步骤S3具体为：

[0020] 日志展示系统对存储在日志存储系统中的新日志数据进行扫描，并根据用户在日志展示系统的界面中设定的检索规则来建立日志索引，以从日志存储系统获取到对应的日志数据；

[0021] 日志展示系统根据不同的属性来对获取的日志数据进行展示，或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示。

[0022] 本发明要解决的技术问题之二，在于提供一种多数据源日志数据集中收集存储装置，通过该装置来实现多数据源日志的收集存储和检索，可提高故障处理效率，提升数据分析能力，并为后期的故障排查奠定良好的基础。

[0023] 本发明是这样实现技术问题之二的：一种多数据源日志数据集中收集存储装置，所述装置包括日志收集模块、日志处理模块以及日志展示模块；

[0024] 所述日志收集模块，用于在各应用服务器上安装日志收集系统客户端，通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统；

[0025] 所述日志处理模块，用于日志处理系统在接收到日志数据后，先将原始的日志数据复制一份到日志存储系统中进行保存；再对原始的日志数据进行筛选、切割、分类以及合并处理，并将处理后的新日志数据保存到日志存储系统中；

[0026] 所述日志展示模块，用于在日志展示系统中建立日志索引，并根据日志索引从日志存储系统中获取日志数据进行展示。

[0027] 进一步地，所述日志处理模块，还用于在对原始的日志数据进行处理时，日志处理系统对新日志数据中的日志内容属性进行扫描，并自动匹配告警规则，且根据告警规则触发日志预警系统发送警报内容进行告警；所述警报内容包括应用服务器IP、日志别名、日志路径以及日志内容。

[0028] 进一步地，所述日志收集模块具体为：

[0029] 在各应用服务器上安装日志收集系统客户端，并对日志收集系统的配置文件进行参数配置，配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志处理系统的地址以及日志间隔时间；

[0030] 运行日志收集系统的应用程序，应用程序读取配置文件，并检查配置文件是否正确，如果否，则停止应用程序的运行，并发送提示消息给日志收集系统客户端；如果是，则按照配置文件中配置的收集规则扫描对应的日志文件，并将扫描到的日志数据实时发送给日志处理系统。

[0031] 进一步地，所述日志存储系统上设置有一个本地服务器节点以及至少一个服务器从节点；

[0032] 所述日志处理模块具体包括日志备份单元、日志处理单元以及日志存储单元；

[0033] 所述日志备份单元，用于日志处理系统在接收到日志数据后，将原始的日志数据复制一份给日志存储系统，日志存储系统将原始的日志数据保存至本地服务器节点上，同时将原始的日志数据同步给各服务器从节点；

[0034] 所述日志处理单元，用于日志处理系统对原始的日志数据进行属性提取，按照设定的属性合并规则来合并新日志数据，并根据设置的分类类型来对新日志数据进行分类；其中，提取的属性包括应用服务器IP、日志别名、日志路径、日志类型、服务器名称、日志内容、日志级别或者自定义属性；

[0035] 所述日志存储单元，用于将处理后的新日志数据发送给日志存储系统，日志存储系统将新日志数据保存至本地服务器节点上，同时将新日志数据同步给各服务器从节点。

[0036] 进一步地，所述日志展示模块具体为：

[0037] 日志展示系统对存储在日志存储系统中的新日志数据进行扫描，并根据用户在日志展示系统的界面中设定的检索规则来建立日志索引，以从日志存储系统获取到对应的日志数据；

[0038] 日志展示系统根据不同的属性来对获取的日志数据进行展示，或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示。

[0039] 本发明具有如下优点：通过预先在应用服务器集群上部署用于日志收集的客户端，以实时监测服务器上的各类资源；再通过配置客户端的收集规则来对感知到的异常数据进行收集上报，同时在服务端统一对异常数据进行过滤、分类、存储及预警，不仅可以很好的实现多数据源日志的收集存储和检索，提高故障处理效率，提升数据分析能力，而且可以很好的为后期的故障排查奠定良好的基础。

附图说明

[0040] 下面参照附图结合实施例对本发明作进一步的说明。

[0041] 图1为本发明涉及的系统架构图。

[0042] 图2为本发明一种多数据源日志数据集中收集存储方法的执行流程图。

具体实施方式

[0043] 请参阅图1和图2所示，本发明一种多数据源日志数据集中收集存储方法的较佳实

施例,所述方法包括如下步骤:

[0044] 步骤S1、在各应用服务器上安装日志收集系统客户端,通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统;

[0045] 步骤S2、日志处理系统在接收到日志数据后,先将原始的日志数据复制一份到日志存储系统中进行保存;再对原始的日志数据进行筛选、切割、分类以及合并处理,并将处理后的新日志数据保存到日志存储系统中;

[0046] 步骤S3、在日志展示系统中建立日志索引,并根据日志索引从日志存储系统中获取日志数据进行展示。

[0047] 在本发明中,所述步骤S2还包括:

[0048] 在对原始的日志数据进行处理时,日志处理系统对新日志数据中的日志内容属性进行扫描,并自动匹配告警规则,且根据告警规则触发日志预警系统发送警报内容进行告警,以通知对应的技术人员或者管理员及时对告警进行处理;在具体实施时,例如当匹配到达到对应的日志级别(如严重级别),就触发日志预警系统进行告警;又如,当匹配到连续多个日志级别均为ERROR时,就触发日志预警系统进行告警;当然,以上所举的例子仅是用于说明性用的,本发明不并仅限于此,在实际设置时,还可以根据实际需要来设置对应的告警规则。所述警报内容包括应用服务器IP(ip)、日志别名(index)、日志路径(source)以及日志内容(message)。在本发明中,日志预警系统可以支持以下三种模式来实现告警通知:

[0049] A:通过第三方邮箱来发送邮件进行报警;

[0050] B:调用微信接口以通过微信发送告警通知;

[0051] C:调用钉钉办公软件的接口进行告警通知。

[0052] 当然,本发明并不仅限于此,在具体实施时,还可以根据需要来增加其他的告警通知模式,例如还可以通过短信、QQ等来发送告警通知。

[0053] 所述步骤S1具体为:

[0054] 在各应用服务器上安装日志收集系统客户端,以用于收集日志数据,日志收集系统客户端的安装包是一个编译好的二进制文件,可直接在应用服务器上执行,且在安装包内可对配置文件进行参数配置;对日志收集系统的配置文件进行参数配置,配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志处理系统的地址以及日志间隔时间,当然,以上所列举的仅是一些较为常用的参数配置,在具体实施时,还可以根据实际需要来增加其他的参数配置;

[0055] 运行日志收集系统的应用程序,应用程序读取配置文件,并检查配置文件是否正确,如果否,则停止应用程序的运行,并发送提示消息给日志收集系统客户端;如果是,则按照配置文件中配置的收集规则扫描对应的日志文件,并将扫描到的日志数据实时发送给日志处理系统;其中,扫描的日志文件范围包括:应用日志、操作系统日志、以及硬件资源日志。

[0056] 所述日志存储系统上设置有一个本地服务器节点(Master)以及至少一个服务器从节点(slave);

[0057] 所述步骤S2具体包括:

[0058] 步骤S21、日志处理系统在接收到日志数据后,将原始的日志数据复制一份给日志存储系统,日志存储系统将原始的日志数据保存至本地服务器节点上,同时将原始的日志

数据同步给各服务器从节点；

[0059] 在本发明中，通过先在日志存储系统中保留一份最原始的日志数据，可使得后续可以方便进行日志溯源；且具体在进行原始日志数据的保存时，需要先在本地服务器节点建立一个init文件夹，并将原始的日志数据存放到init文件夹中，原始日志数据在init文件夹中保存的格式为：日志名称_服务器IP_时间戳.log，其中，时间戳可以精确到毫秒，例如：IQWebService_127.0.0.1_20190325161905.log。同时，本地服务器节点会自动检查当前在线的服务器从节点，并将原始的日志数据同步给各服务器从节点。

[0060] 步骤S22、日志处理系统对原始的日志数据进行属性提取，按照设定的属性合并规则来合并新日志数据，并根据设置的分类类型来对新日志数据进行分类；其中，提取的属性包括应用服务器IP(ip)、日志别名(index)、日志路径(source)、日志类型(type)、服务器名称(hostname)、日志内容(message)、日志级别(level)或者自定义属性；

[0061] 在具体实施时，自定义属性在日志处理系统中的优先级最高，日志处理系统是不会过滤掉自定义属性的；属性合并规则是可以根据实际使用需要来进行设定的，例如，设定属性合并规则为：日志别名+应用服务器IP+日志路径+日志内容+自定义属性，那么在具体实施时，就根据该属性合并规则进行合并成新日志数据；分类类型在默认情况下是以应用服务器IP来进行分类的，当然，本发明并不仅限于此，在具体实施时，还可以根据实际需要来设置其它的分类类型。

[0062] 步骤S23、将处理后的新日志数据发送给日志存储系统，日志存储系统将新日志数据保存至本地服务器节点上，同时将新日志数据同步给各服务器从节点。在具体实现时，需要先在本地服务器节点建立一个main文件夹，并将新日志数据存放到main文件夹中，新日志数据在main文件夹中保存的格式也为：日志名称_服务器IP_时间戳.log。

[0063] 所述步骤S3具体为：

[0064] 日志展示系统对存储在日志存储系统中的新日志数据进行扫描，并根据用户在日志展示系统的界面中设定的检索规则来建立日志索引，以从日志存储系统获取到对应的日志数据；在默认情况下，检索规则是以建立日志别名属性(index)的索引，并在日志展示系统的搜索框中可以对索引进行检索，并可支持正则表达式来进行检索；当然，在具体实施时，还可以根据实际需要来建立其它的检索规则。

[0065] 日志展示系统根据不同的属性来对获取的日志数据进行展示，例如，可以根据不同的属性来绘制条形图、圆饼图、折线图等，并展示给用户进行查看；

[0066] 或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示，比如针对web日志，可以统计全球用户访问的情况，页面请求的情况等等，并以条形图、圆饼图、折线图等进行展示。

[0067] 在具体实施时，日志展示系统还可以提供用户权限管理，具体是：通过userManager函数来对用户进行授权，系统默认在后台数据库表user中添加一条管理员记录；界面展示新建用户表单，提交后userManager函数会将表单写入后台数据库user表中，用户密码采用md5加密存储，每次登陆都会去数据库中匹配md5值和用户名。

[0068] 请参阅图1所示，本发明一种多数据源日志数据集中收集存储装置的较佳实施例，所述装置包括日志收集模块、日志处理模块以及日志展示模块；

[0069] 所述日志收集模块，用于在各应用服务器上安装日志收集系统客户端，通过日志

收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统；

[0070] 所述日志处理模块，用于日志处理系统在接收到日志数据后，先将原始的日志数据复制一份到日志存储系统中进行保存；再对原始的日志数据进行筛选、切割、分类以及合并处理，并将处理后的新日志数据保存到日志存储系统中；

[0071] 所述日志展示模块，用于在日志展示系统中建立日志索引，并根据日志索引从日志存储系统中获取日志数据进行展示。

[0072] 在本发明中，所述日志处理模块，还用于在对原始的日志数据进行处理时，日志处理系统对新日志数据中的日志内容属性进行扫描，并自动匹配告警规则，且根据告警规则触发日志预警系统发送警报内容进行告警，以通知对应的技术人员或者管理员及时对告警进行处理；在具体实施时，例如当匹配到达到对应的日志级别(如严重级别)，就触发日志预警系统进行告警；又如，当匹配到连续多个日志级别均为ERROR时，就触发日志预警系统进行告警；当然，以上所举的例子仅是用于说明性用的，本发明不并仅限于此，在实际设置时，还可以根据实际需要来设置对应的告警规则。所述警报内容包括应用服务器IP(ip)、日志别名(index)、日志路径(source)以及日志内容(message)。在本发明中，日志预警系统可以支持以下三种模式来实现告警通知：

[0073] A：通过第三方邮箱来发送邮件进行报警；

[0074] B：调用微信接口以通过微信发送告警通知；

[0075] C：调用钉钉办公软件的接口进行告警通知。

[0076] 当然，本发明并不仅限于此，在具体实施时，还可以根据需要来增加其他的告警通知模式，例如还可以通过短信、QQ等来发送告警通知。

[0077] 所述日志收集模块具体为：

[0078] 在各应用服务器上安装日志收集系统客户端，以用于收集日志数据，日志收集系统客户端的安装包是一个编译好的二进制文件，可直接在应用服务器上执行，且在安装包内可对配置文件进行参数配置；对日志收集系统的配置文件进行参数配置，配置的参数至少包括本机IP地址、日志文件路径、日志多行合并、收集规则、日志处理系统的地址以及日志间隔时间，当然，以上所列举的仅是一些较为常用的参数配置，在具体实施时，还可以根据实际需要来增加其他的参数配置；

[0079] 运行日志收集系统的应用程序，应用程序读取配置文件，并检查配置文件是否正确，如果否，则停止应用程序的运行，并发送提示消息给日志收集系统客户端；如果是，则按照配置文件中配置的收集规则扫描对应的日志文件，并将扫描到的日志数据实时发送给日志处理系统；其中，扫描的日志文件范围包括：应用日志、操作系统日志、以及硬件资源日志。

[0080] 所述日志存储系统上设置有一个本地服务器节点(Master)以及至少一个服务器从节点(slave)；

[0081] 所述日志处理模块具体包括日志备份单元、日志处理单元以及日志存储单元；

[0082] 所述日志备份单元，用于日志处理系统在接收到日志数据后，将原始的日志数据复制一份给日志存储系统，日志存储系统将原始的日志数据保存至本地服务器节点上，同时将原始的日志数据同步给各服务器从节点；

[0083] 在本发明中，通过先在日志存储系统中保留一份最原始的日志数据，可使得后续

可以方便进行日志溯源;且具体在进行原始日志数据的保存时,需要先在本地服务器节点建立一个init文件夹,并将原始的日志数据存放到init文件夹中,原始日志数据在init文件夹中保存的格式为:日志名称_服务器IP_时间戳.log,其中,时间戳可以精确到毫秒,例如:IQWebService_127.0.0.1_20190325161905.log。同时,本地服务器节点会自动检查当前在线的服务器从节点,并将原始的日志数据同步给各服务器从节点。

[0084] 所述日志处理单元,用于日志处理系统对原始的日志数据进行属性提取,按照设定的属性合并规则来合并新日志数据,并根据设置的分类类型来对新日志数据进行分类;其中,提取的属性包括应用服务器IP(ip)、日志别名(index)、日志路径(source)、日志类型(type)、服务器名称(hostname)、日志内容(message)、日志级别(level)或者自定义属性;

[0085] 在具体实施时,自定义属性在日志处理系统中的优先级最高,日志处理系统是不会过滤掉自定义属性的;属性合并规则是可以根据实际使用需要来进行设定的,例如,设定属性合并规则为:日志别名+应用服务器IP+日志路径+日志内容+自定义属性,那么在具体实施时,就根据该属性合并规则进行合并成新日志数据;分类类型在默认情况下是以应用服务器IP来进行分类的,当然,本发明并不仅限于此,在具体实施时,还可以根据实际需要来设置其它的分类类型。

[0086] 所述日志存储单元,用于将处理后的新日志数据发送给日志存储系统,日志存储系统将新日志数据保存至本地服务器节点上,同时将新日志数据同步给各服务器从节点。在具体实现时,需要先在本地服务器节点建立一个main文件夹,并将新日志数据存放到main文件夹中,新日志数据在main文件夹中保存的格式也为:日志名称_服务器IP_时间戳.log。

[0087] 所述日志展示模块具体为:

[0088] 日志展示系统对存储在日志存储系统中的新日志数据进行扫描,并根据用户在日志展示系统的界面中设定的检索规则来建立日志索引,以从日志存储系统获取到对应的日志数据;在默认情况下,检索规则是以建立日志别名属性(index)的索引,并在日志展示系统的搜索框中可以对索引进行检索,并可支持正则表达式来进行检索;当然,在具体实施时,还可以根据实际需要来建立其它的检索规则。

[0089] 日志展示系统根据不同的属性来对获取的日志数据进行展示,例如,可以根据不同的属性来绘制条形图、圆饼图、折线图等,并展示给用户进行查看;

[0090] 或者日志展示系统通过引入第三方的IP库来对日志的用户行为进行统计和展示,比如针对web日志,可以统计全球用户访问的情况,页面请求的情况等等,并以条形图、圆饼图、折线图等进行展示。

[0091] 在具体实施时,日志展示系统还可以提供用户权限管理,具体是:通过userManager函数来对用户进行授权,系统默认在后台数据库表user中添加一条管理员记录;界面展示新建用户表单,提交后userManager函数会将表单写入后台数据库user表中,用户密码采用md5加密存储,每次登陆都会去数据库中匹配md5值和用户名。

[0092] 综上所述,本发明具有如下优点:通过预先在应用服务器集群上部署用于日志收集的客户端,以实时监测服务器上的各类资源;再通过配置客户端的收集规则来对感知到的异常数据进行收集上报,同时在服务端统一对异常数据进行过滤、分类、存储及预警,不仅可以很好的实现多数据源日志的收集存储和检索,提高故障处理效率,提升数据分析能

力,而且可以很好的为后期的故障排查奠定良好的基础。

[0093] 虽然以上描述了本发明的具体实施方式,但是熟悉本技术领域的技术人员应当理解,我们所描述的具体的实施例只是说明性的,而不是用于对本发明的范围的限定,熟悉本领域的技术人员在依照本发明的精神所作的等效的修饰以及变化,都应当涵盖在本发明的权利要求所保护的范围内。

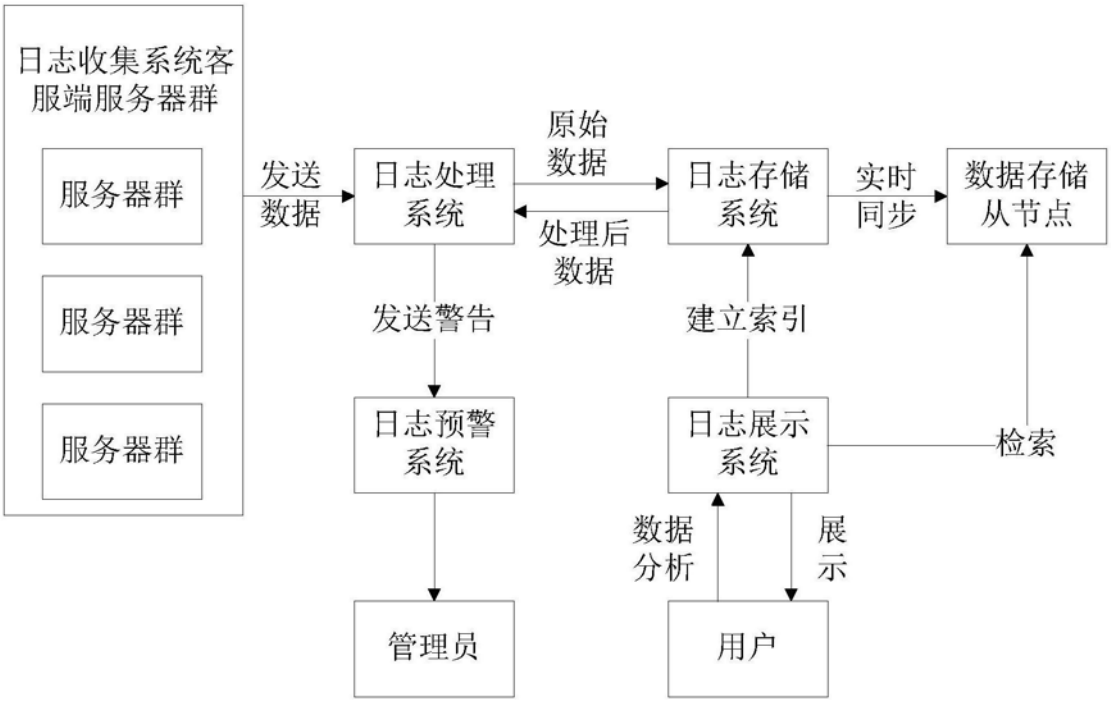

日志收集系统客服端服务器群
服务器群
服务器群
服务器群
发送数据
日志处理系统
原始数据
处理后数据
日志存储系统
实时同步
数据存储从节点
发送警告
建立索引
日志预警系统
日志展示系统
检索
数据分析
展示
管理员
用户

图1

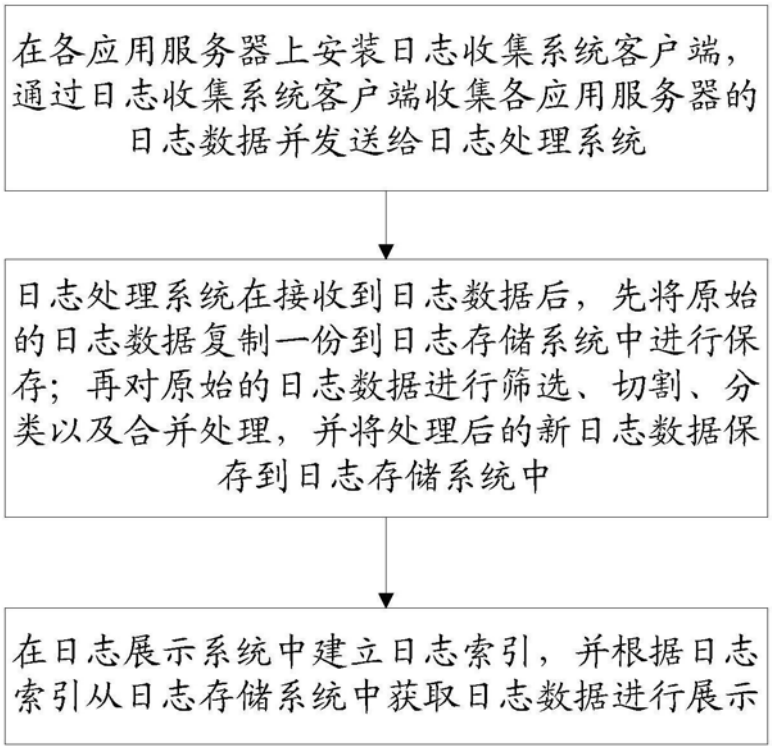

在各应用服务器上安装日志收集系统客户端，通过日志收集系统客户端收集各应用服务器的日志数据并发送给日志处理系统
日志处理系统在接收到日志数据后，先将原始的日志数据复制一份到日志存储系统中进行保存；再对原始的日志数据进行筛选、切割、分类以及合并处理，并将处理后的新日志数据保存到日志存储系统中
在日志展示系统中建立日志索引，并根据日志索引从日志存储系统中获取日志数据进行展示

图2