(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 113746703 A
(43)申请公布日 2021.12.03

(21)申请号 202111033724.2

(22)申请日 2021.09.03

(71)申请人 上海众源网络有限公司
地址 200030 上海市长宁区临虹路365号9座501室

(72)发明人 景小琳 艾国信

(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 项京 孟维娜

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 12/24(2006.01)

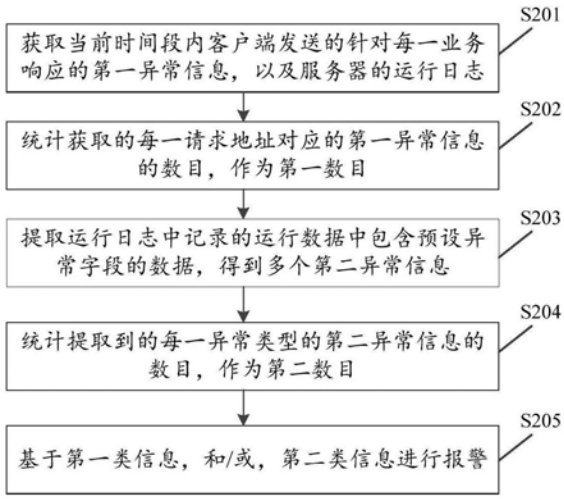
权利要求书4页 说明书15页 附图8页

(54)发明名称

一种异常链路监控方法、系统和装置

(57)摘要

本发明实施例提供了一种异常链路监控方法、系统和装置，该方法包括：获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志；统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：服务器响应客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警。本发明实施例提供的方法，能够对服务器异常自动监控，并进行报警，以及时的发现异常，提高服务器的维护的效率。



CN 113746703 A

1.一种异常链路监控方法,其特征在于,应用于服务器,所述方法包括:

获取当前时间段内客户端发送的针对每一业务响应的第一异常信息,以及所述服务器的运行日志;其中,每一第一异常信息包含:该业务响应对应的业务请求的请求地址,以及第一响应信息;所述第一响应信息为:所述客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下,提取到的该业务响应中携带的业务层的响应信息;所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常;

统计获取的每一请求地址对应的第一异常信息的数目,作为第一数目;

提取所述运行日志中记录的运行数据中包含预设异常字段的数据,得到多个第二异常信息;每一第二异常信息表示:所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常;

统计提取到的每一异常类型的第二异常信息的数目,作为第二数目;

基于第一类信息,和/或,第二类信息进行报警;其中,所述第一类信息包括:当前时间段内的所述第一数目、以及各第一异常信息;所述第二类信息包括:当前时间段内的所述第二数目、以及各第二异常信息。

2.根据权利要求1所述的方法,其特征在于,在所述基于第一类信息,和/或,第二类信息进行报警之前,所述方法还包括:

针对每一请求地址,获取前一时间段内所述客户端发送的该请求地址对应的第一异常信息的数目,作为第三数目;

所述基于第一类信息,和/或,第二类信息进行报警,包括:

若所述第三数目大于第一阈值,则以当前时间段内该请求地址对应的第一数目为报警信息进行报警;

若所述第三数目不大于所述第一阈值,则以当前时间段内该请求地址对应的第一异常信息为报警信息进行报警。

3.根据权利要求1所述的方法,其特征在于,在所述基于第一类信息,和/或,第二类信息进行报警之前,所述方法还包括:

针对每一异常类型,获取前一时间段内统计的该异常类型的第二异常信息的数目,作为第四数目;

所述基于第一类信息,和/或,第二类信息进行报警,包括:

若所述第四数目大于第二阈值,则以当前时间段内该异常类型对应的第二数目为报警信息进行报警;

若所述第四数目不大于所述第二阈值,则以当前时间段内该异常类型的第二异常信息为报警信息进行报警。

4.根据权利要求1所述的方法,其特征在于,每一第一异常信息还包括:所述客户端生成的该业务请求所属的业务链路的链路标识、所述客户端发送该业务请求时显示的页面的页面地址,以及当前登录所述客户端的用户的用户标识;

每一第二异常信息包括以下至少一项:异常类型的类型标识、异常堆栈信息、所述运行日志所属的项目的标识,以及用于运行该第二异常信息对应的服务的容器的标识。

5.根据权利要求1所述的方法,其特征在于,所述获取当前时间段内客户端发送的针对每一业务响应的第一异常信息,包括:

从第一消息队列中，获取所述客户端预先添加的针对当前时间段内每一业务响应的第一异常信息。

6.根据权利要求1所述的方法，其特征在于，所述提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息，包括：

通过预设日志处理工具，提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到所述服务器运行异常的异常信息，作为第二异常信息，并添加至第二消息队列中；

在所述统计提取到的每一异常类型的第二异常信息的数目，作为第二数目之前，所述方法还包括：

通过预设数据流处理工具，从所述第二消息队列中依次获取各第二异常信息；

所述统计提取到的每一异常类型的第二异常信息的数目，作为第二数目，包括：

通过所述预设数据流处理工具，统计每一异常类型的第二异常信息的数目，作为第二数目。

7.一种异常链路监控方法，其特征在于，应用于客户端，所述方法包括：

当接收到服务器发送的针对每一业务请求的业务响应时，提取所述业务响应中业务层的状态码，作为第一状态码；

若所述第一状态码为预设的异常状态码，则提取所述业务响应中业务层的响应信息，作为第一响应信息；其中，所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

向所述服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；以使所述服务器统计当前时间段内每一请求地址对应的第一异常信息的数目，作为第一数目，以及提取当前时间段内所述服务器的运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括：当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

8.根据权利要求7所述的方法，其特征在于，在向所述服务器发送当前时间段内每一业务响应的第一异常信息之前，所述方法还包括：

生成该业务请求所属的业务链路的标识，作为链路标识；

获取发送该业务请求时显示的页面的页面地址，以及当前登录所述客户端的用户的用户标识；

每一第一异常信息还包括：对应的链路标识、页面地址和用户标识。

9.根据权利要求7所述的方法，其特征在于，所述向所述服务器发送当前时间段内每一业务响应的第一异常信息，包括：

将当前时间段内每一业务响应的第一异常信息依次添加至第一消息队列，以使所述服务器从所述第一消息队列获取针对当前时间段内每一业务响应的各第一异常信息。

10.一种异常链路监控系统，其特征在于，所述异常链路监控系统包括客户端和服务

器，其中：

所述客户端，用于当接收到所述服务器发送的针对每一业务请求的业务响应时，提取所述业务响应中业务层的状态码，作为第一状态码；若所述第一状态码为预设的异常状态码，则提取所述业务响应中业务层的响应信息，作为第一响应信息；其中，所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；向所述服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；

所述服务器，用于获取当前时间段内客户端发送的针对各业务响应的各第一异常信息，以及所述服务器的运行日志；统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

11.一种异常链路监控装置，其特征在于，应用于服务器，所述装置包括：

获取模块，用于获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及所述服务器的运行日志；其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；所述第一响应信息为：所述客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下，提取到的该业务响应中携带的业务层的响应信息；所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

第一统计模块，用于统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；

第二异常信息提取模块，用于提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；

第二统计模块，用于统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；

报警模块，用于基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括：当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

12.一种异常链路监控装置，其特征在于，应用于客户端，所述装置包括：

状态码提取模块，用于当接收到服务器发送的针对每一业务请求的业务响应时，提取所述业务响应中业务层的状态码，作为第一状态码；

第一响应信息提取模块，用于若所述第一状态码为预设的异常状态码，则提取所述业务响应中业务层的响应信息，作为第一响应信息；其中，所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

发送模块，用于向所述服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；以使

所述服务器统计当前时间段内每一请求地址对应的第一异常信息的数目，作为第一数目，以及提取当前时间段内所述服务器的运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括：当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

13.一种电子设备，其特征在于，包括处理器、通信接口、存储器和通信总线，其中，处理器，通信接口，存储器通过通信总线完成相互间的通信；

存储器，用于存放计算机程序；

处理器，用于执行存储器上所存放的程序时，实现权利要求1-6，或7-9任一所述的方法步骤。

14.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质内存储有计算机程序，所述计算机程序被处理器执行时实现权利要求1-6，或7-9任一所述的方法步骤。

一种异常链路监控方法、系统和装置

技术领域

[0001] 本发明涉及网络应用技术领域，特别是涉及一种异常链路监控方法、系统和装置。

背景技术

[0002] 随着网络技术的发展，网络服务的提供商可以为用户提供不同的网络服务。用户可以通过客户端向提供商的服务器发送业务请求，服务器则可以基于该业务请求向客户端发送对应的业务响应。

[0003] 为了保证业务的正常进行，需要监控服务器是否异常，以及时对服务器进行维护。

发明内容

[0004] 本发明实施例的目的在于提供一种异常链路监控方法、系统和装置，以实现对服务器异常的自动监控，并进行报警，以及时的发现异常，提高服务器的维护的效率。具体技术方案如下：

[0005] 在本发明实施的第一方面，首先提供了一种异常链路监控方法，应用于服务器，所述方法包括：

[0006] 获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及所述服务器的运行日志；其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；所述第一响应信息为：所述客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下，提取到的该业务响应中携带的业务层的响应信息；所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

[0007] 统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；

[0008] 提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；

[0009] 统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；

[0010] 基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括：当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

[0011] 可选的，在所述基于第一类信息，和/或，第二类信息进行报警之前，所述方法还包括：

[0012] 针对每一请求地址，获取前一时间段内所述客户端发送的该请求地址对应的第一异常信息的数目，作为第三数目；

[0013] 所述基于第一类信息，和/或，第二类信息进行报警，包括：

[0014] 若所述第三数目大于第一阈值，则以当前时间段内该请求地址对应的第一数目为报警信息进行报警；

[0015] 若所述第三数目不大于所述第一阈值，则以当前时间段内该请求地址对应的第一

异常信息为报警信息进行报警。

[0016] 可选的，在所述基于第一类信息，和/或，第二类信息进行报警之前，所述方法还包括：

[0017] 针对每一异常类型，获取前一时间段内统计的该异常类型的第二异常信息的数目，作为第四数目；

[0018] 所述基于第一类信息，和/或，第二类信息进行报警，包括：

[0019] 若所述第四数目大于第二阈值，则以当前时间段内该异常类型对应的第二数目为报警信息进行报警；

[0020] 若所述第四数目不大于所述第二阈值，则以当前时间段内该异常类型的第二异常信息为报警信息进行报警。

[0021] 可选的，每一第一异常信息还包括：所述客户端生成的该业务请求所属的业务链路的链路标识、所述客户端发送该业务请求时显示的页面的页面地址，以及当前登录所述客户端的用户的用户标识；

[0022] 每一第二异常信息包括以下至少一项：异常类型的类型标识、异常堆栈信息、所述运行日志所属的项目的标识，以及用于运行该第二异常信息对应的服务的容器的标识。

[0023] 可选的，所述获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，包括：

[0024] 从第一消息队列中，获取所述客户端预先添加的针对当前时间段内每一业务响应的第一异常信息。

[0025] 可选的，所述提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息，包括：

[0026] 通过预设日志处理工具，提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到所述服务器运行异常的异常信息，作为第二异常信息，并添加至第二消息队列中；

[0027] 在所述统计提取到的每一异常类型的第二异常信息的数目，作为第二数目之前，所述方法还包括：

[0028] 通过预设数据流处理工具，从所述第二消息队列中依次获取各第二异常信息；

[0029] 所述统计提取到的每一异常类型的第二异常信息的数目，作为第二数目，包括：

[0030] 通过所述预设数据流处理工具，统计每一异常类型的第二异常信息的数目，作为第二数目。

[0031] 在本发明实施的第二方面，提供了一种异常链路监控方法，应用于客户端，所述方法包括：

[0032] 当接收到服务器发送的针对每一业务请求的业务响应时，提取所述业务响应中业务层的状态码，作为第一状态码；

[0033] 若所述第一状态码为预设的异常状态码，则提取所述业务响应中业务层的响应信息，作为第一响应信息；其中，所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

[0034] 向所述服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；以使所述服务

器统计当前时间段内每一请求地址对应的第一异常信息的数目，作为第一数目，以及提取当前时间段内所述服务器的运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括：当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

[0035] 可选的，在向所述服务器发送当前时间段内每一业务响应的第一异常信息之前，所述方法还包括：

[0036] 生成该业务请求所属的业务链路的标识，作为链路标识；

[0037] 获取发送该业务请求时显示的页面的页面地址，以及当前登录所述客户端的用户的用户标识；

[0038] 每一第一异常信息还包括：对应的链路标识、页面地址和用户标识。

[0039] 可选的，所述向所述服务器发送当前时间段内每一业务响应的第一异常信息，包括：

[0040] 将当前时间段内每一业务响应的第一异常信息依次添加至第一消息队列，以使所述服务器从所述第一消息队列获取针对当前时间段内每一业务响应的各第一异常信息。

[0041] 在本发明实施的第三方面，提供了一种异常链路监控系统，所述异常链路监控系统包括客户端和服务器，其中：

[0042] 所述客户端，用于当接收到所述服务器发送的针对每一业务请求的业务响应时，提取所述业务响应中业务层的状态码，作为第一状态码；若所述第一状态码为预设的异常状态码，则提取所述业务响应中业务层的响应信息，作为第一响应信息；其中，所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常；向所述服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；

[0043] 所述服务器，用于获取当前时间段内客户端发送的针对各业务响应的各第一异常信息，以及所述服务器的运行日志；统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；提取所述运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，所述第一类信息包括当前时间段内的所述第一数目、以及各第一异常信息；所述第二类信息包括：当前时间段内的所述第二数目、以及各第二异常信息。

[0044] 在本发明实施的第四方面，提供了一种异常链路监控装置，应用于服务器，所述装置包括：

[0045] 获取模块，用于获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及所述服务器的运行日志；其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；所述第一响应信息为：所述客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下，提取到的该业务响应中携带的业务层

的响应信息;所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常;

[0046] 第一统计模块,用于统计获取的每一请求地址对应的第一异常信息的数目,作为第一数目;

[0047] 第二异常信息提取模块,用于提取所述运行日志中记录的运行数据中包含预设异常字段的数据,得到多个第二异常信息;每一第二异常信息表示:所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常;

[0048] 第二统计模块,用于统计提取到的每一异常类型的第二异常信息的数目,作为第二数目;

[0049] 报警模块,用于基于第一类信息,和/或,第二类信息进行报警;其中,所述第一类信息包括:当前时间段内的所述第一数目、以及各第一异常信息;所述第二类信息包括:当前时间段内的所述第二数目、以及各第二异常信息。

[0050] 在本发明实施的第五方面,提供了一种异常链路监控装置,应用于客户端,所述装置包括:

[0051] 状态码提取模块,用于当接收到服务器发送的针对每一业务请求的业务响应时,提取所述业务响应中业务层的状态码,作为第一状态码;

[0052] 第一响应信息提取模块,用于若所述第一状态码为预设的异常状态码,则提取所述业务响应中业务层的响应信息,作为第一响应信息;其中,所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常;

[0053] 发送模块,用于向所述服务器发送当前时间段内每一业务响应的第一异常信息,其中,每一第一异常信息包含:该业务响应对应的业务请求的请求地址,以及第一响应信息;以使所述服务器统计当前时间段内每一请求地址对应的第一异常信息的数目,作为第一数目,以及提取当前时间段内所述服务器的运行日志中记录的运行数据中包含预设异常字段的数据,得到多个第二异常信息;每一第二异常信息表示:所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常;统计提取到的每一异常类型的第二异常信息的数目,作为第二数目;基于第一类信息,和/或,第二类信息进行报警;其中,所述第一类信息包括:当前时间段内的所述第一数目、以及各第一异常信息;所述第二类信息包括:当前时间段内的所述第二数目、以及各第二异常信息。

[0054] 在本发明实施的又一方面,还提供了一种电子设备,包括处理器、通信接口、存储器和通信总线,其中,处理器,通信接口,存储器通过通信总线完成相互间的通信;

[0055] 存储器,用于存放计算机程序;

[0056] 处理器,用于执行存储器上所存放的程序时,实现上述任一所述的异常链路监控方法。

[0057] 在本发明实施的又一方面,还提供了一种计算机可读存储介质,所述计算机可读存储介质内存储有计算机程序,所述计算机程序被处理器执行时实现上述任一所述的异常链路监控方法。

[0058] 在本发明实施的又一方面,还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述任一所述的异常链路监控方法。

[0059] 采用本发明实施例提供的异常链路监控方法,获取当前时间段内客户端发送的针对每一业务响应的第一异常信息,以及所述服务器的运行日志;其中,每一第一异常信息包

含:该业务响应对应的业务请求的请求地址,以及第一响应信息;所述第一响应信息为:所述客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下,提取到的该业务响应中携带的业务层的响应信息;所述第一响应信息用于表示该业务请求所属的业务链路所发生的异常;统计获取的每一请求地址对应的第一异常信息的数目,作为第一数目;提取所述运行日志中记录的运行数据中包含预设异常字段的数据,得到多个第二异常信息;每一第二异常信息表示:所述服务器响应所述客户端的每一业务请求的业务链路所发生的异常;统计提取到的每一异常类型的第二异常信息的数目,作为第二数目;基于第一类信息,和/或,第二类信息进行报警;其中,所述第一类信息包括:当前时间段内的所述第一数目、以及各第一异常信息;所述第二类信息包括:当前时间段内的所述第二数目、以及各第二异常信息。

[0060] 本发明实施例提供的方法,能够实现对服务器异常的自动监控,并进行报警,以及时的发现异常,提高服务器的维护的效率。

附图说明

[0061] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

[0062] 图1为本发明实施例中提供的一种异常链路监控系统的结构图;

[0063] 图2为本发明实施例中提供的一种异常链路监控方法的流程图;

[0064] 图3为本发明实施例中提供的一种运行日志的示例图;

[0065] 图4为本发明实施例中提供的一种第一异常信息的示意图;

[0066] 图5为本发明实施例中提供的一种第二异常信息的示意图;

[0067] 图6为本发明实施例中提供的另一种异常链路监控方法的流程图;

[0068] 图7为本发明实施例中提供的另一种异常链路监控方法的流程图;

[0069] 图8为本发明实施例中提供的一种异常链路监控方法的流程图;

[0070] 图9为本发明实施例中提供的另一种异常链路监控方法的流程图;

[0071] 图10为本发明实施例中提供的另一种异常链路监控方法的流程图;

[0072] 图11为本发明实施例中提供的一种异常链路监控方法的原理示意图;

[0073] 图12为本发明实施例中提供的另一种异常链路监控方法的原理示意图;

[0074] 图13为本发明实施例中提供的一种异常链路监控系统的整体架构框图;

[0075] 图14为本发明实施例中提供的一种异常链路监控装置的结构图;

[0076] 图15为本发明实施例中提供的一种异常链路监控装置的结构图;

[0077] 图16为本发明实施例提供的一种电子设备的结构示意图。

具体实施方式

[0078] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行描述。

[0079] 为了保证网络服务的业务正常进行,需要监控服务器是否异常,以及时对服务器进行维护。本发明实施例提供了一种异常链路监控系统。参见图1,图1为本发明实施例提供的一种异常链路监控系统的结构图,该系统包括:

[0080] 客户端101,用于当接收到服务器102发送的针对每一业务请求的业务响应时,提

取业务响应中业务层的状态码，作为第一状态码；若第一状态码为预设的异常状态码，则提取业务响应中业务层的响应信息，作为第一响应信息；其中，第一响应信息用于表示该业务请求所属的业务链路所发生的异常；向服务器102发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息。

[0081] 服务器102，用于获取当前时间段内客户端101发送的针对各业务响应的各第一异常信息，以及服务器102的运行日志；统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目；提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：服务器102响应客户端101的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，第一类信息包括当前时间段内的第一数目、以及各第一异常信息；第二类信息包括：当前时间段内的第二数目、以及各第二异常信息。

[0082] 本发明实施例的系统，可以实现对服务器异常的自动监控，并进行报警，以及时的发现异常，提高服务器的维护的效率。针对上述系统中的客户端101与服务器102的其他实施例，可以参见下文中关于客户端和服务器方法实施例的具体介绍。

[0083] 本发明实施例提供了一种异常链路监控方法，该方法可以应用于服务器，该服务器可以为上述系统中的服务器102。参见图2，图2为本发明实施例提供了一种异常链路监控方法的流程图，该方法可以包括以下步骤：

[0084] S201：获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志。

[0085] 其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；第一响应信息为：客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下，提取到的该业务响应中携带的业务层的响应信息；第一响应信息用于表示该业务请求所属的业务链路所发生的异常。

[0086] S202：统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目。

[0087] S203：提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息。

[0088] 每一第二异常信息表示：服务器响应客户端的每一业务请求的业务链路所发生的异常。

[0089] S204：统计提取到的每一异常类型的第二异常信息的数目，作为第二数目。

[0090] S205：基于第一类信息，和/或，第二类信息进行报警。

[0091] 其中，第一类信息包括：当前时间段内的第一数目、以及各第一异常信息；第二类信息包括：当前时间段内的第二数目、以及各第二异常信息。

[0092] 本发明实施例的方法，可以实现对服务器异常自动监控，并进行报警，以及时的发现异常，提高服务器的维护的效率。

[0093] 在步骤S201中，在本发明实施例中，一个时间段的时长可以由技术人员根据业务需求进行设置，例如，一个时间段的时长可以为5分钟，或者，也可以为10分钟，但并不限于此。

[0094] 一种实现方式中，业务请求可以为XML HTTP Request(Extensible Markup Language Hypertext Transfer Protocol Request，可扩展标记语言超文本传输协议请求)，则业务响应可以为XML HTTP Request对应的响应，该响应可以包括协议层和业务层。

[0095] 业务层的状态码(可以称为业务层状态码)可以表示该业务请求在业务层面是否异常。

[0096] 在一种实施方式中，可以采用重写XMLHTTPRequest方式，使得客户端在接收到响应后，能够提取到业务层状态码。

[0097] 示例性地，在接收到响应后，客户端可以提取业务层状态码，若业务层状态码为预设的业务请求异常码，表明业务请求所属的业务链路出现异常情况。

[0098] 预设的异常状态码为技术人员根据需求设置的表示业务层异常的类型，技术人员根据需求设置多个预设的异常状态码。例如，可以分别用不同的数值表示业务逻辑判断条件错误、调用栈时序错误、交数据时网络中断，以及系统错误，但并不限于此。第一状态码为任一预设的异常状态码，则表明业务请求在业务层面发生了与该预设的异常状态码对应的异常。

[0099] 业务请求的请求地址表示客户端请求的服务的地址(例如，可以为提供该服务的业务服务器的地址)。基于请求地址，能够确定到异常的业务服务器。

[0100] 在步骤S202中，一种实现方式中，可以基于flink框架，确定每一时间段内每一请求地址对应的第一异常信息的数目。flink框架可以包括KeyBy(基于键的分组)函数、时间窗口函数和aggregate(聚合)函数。flink框架可以基于KeyBy函数基于请求地址对第一异常信息进行分组，得到的每一组中的第一异常信息包含的请求地址相同。另外，还可以基于时间窗口函数对分组后的第一异常信息进行划分，进而，可以基于aggregate函数进行统计，得到每一时间段内每一请求地址对应的第一异常信息的数目。

[0101] 在步骤S203中，一种实现方式中，服务器可以通过正则表达式解析运行日志中记录的运行数据，从运行数据中查找到服务器运行异常的异常信息。

[0102] 例如，正则表达式可以为“[\W\.]+Exception.*”，通过该正则表达式解析运行数据，可以查找到包含Exception的字段，作为ExceptionName(异常名称)。正则表达式还可以为“[\W\.]+Exception.*?Thread.java”，通过该正则表达式解析运行数据，可以查找到包含Exception的字段到包含Thread.Java字段之间的所有字段，作为ExceptionDetail(异常详情)。服务器运行异常的异常信息可以包括ExceptionName和ExceptionDetail。

[0103] 例如，参见图3，图3为本发明实施例提供的一种运行日志的示例图。

[0104] 图3中，基于第一个正则表达式“[\W\.]+Exception.*”，可以解析得到“java.lang.RuntimeException:正在处理，请稍后重试!”，可以作为ExceptionName。

[0105] 基于第二个正则表达式“[\W\.]+Exception.*?Thread.java”，可以解析得到从“java.lang.RuntimeException:正在处理，请稍后重试!”到“at java.lang.Thread.run(Thread.java:748)”之间的所有字段，作为ExceptionDetail。

[0106] 异常堆栈记录了从请求开始到异常发生，服务器内部的调用过程。获取异常堆栈信息，可以获取业务请求的报错行，即上述ExceptionName，然后，获取异常原因链，即上述“java.lang.RuntimeException:正在处理，请稍后重试!”到“at java.lang.Thread.run(Thread.java:748)”之间的所有字段行。通过获取异常堆栈信息可以清楚的显示业务请求

时,服务器内部的调用过程,可以快速定位异常问题。

[0107] 在步骤S204中,一种实现方式中,可以基于flink框架,确定每一时间段内每一ExceptionName对应的第二异常信息的数目。flink框架可以包括KeyBy(基于键的分组)函数、时间窗口函数和aggregate(聚合)函数。flink框架可以基于KeyBy函数基于ExceptionName对第二异常信息进行分组,得到的每一组中的第二异常信息包含的ExceptionName相同。另外,还可以基于时间窗口函数对分组后的第二异常信息进行划分,进而,可以基于aggregate函数进行统计,得到每一时间段内每一ExceptionName对应的第二异常信息的数目。

[0108] 在步骤S205中,一种实现方式中,服务器可以只根据第一类信息进行报警,也可以只根据第二类信息进行报警,还可以结合第一类信息和第二类信息进行报警。

[0109] 例如,当只根据第一类信息进行报警时,服务器可以显示第一类信息中的第一数目,或者,可以显示第一类信息中的各第一异常信息,或者,可以显示第一类信息中的第一数目和各第一异常信息。

[0110] 例如,参见图4,图4为本发明实施例提供的一种第一异常信息的示意图,该第一异常信息可以包括:

[0111] ErrorType(错误类型)、Uid(用户id)、Eventid(事件id)、Url(业务请求地址)、Response(响应信息)、Link(页面地址)。

[0112] ErrorType对应于上述异常状态码表示的异常类型,Uid对应于上述用户的用户标识,Eventid表示每个报警信息的标识,Url对应于上述业务请求地址,Response对应于上述业务层的响应信息,Link对应于上述发送业务请求时显示的页面的页面地址。

[0113] 例如,当只根据第二类信息进行报警时,服务器可以显示第二类信息中的第二数目,或者,可以显示第二类信息中的各第二异常信息,或者,可以显示第二类信息中的第二数目和各第二异常信息。

[0114] 例如,参见图5,图5为本发明实施例提供的一种第二异常信息的示意图,该第二异常信息可以包括:

[0115] ID(事件ID)、Project(项目标识)、QaeApp(容器标识)、Traceid(第一标识)、ExceptionName(异常类别)。

[0116] ID对应于上述Eventid,Project表示第二异常信息对应服务所在项目的标识,QaeApp对应于上述服务器中运行第二异常信息对应的服务的容器的标识。

[0117] 例如,当结合第一类信息和第二类信息进行报警时,服务器可以显示第一类信息中的第一数目和第二类信息中的第二数目,或者,可以显示第一类信息中的各第一异常信息和第二类信息中的各第二异常信息,或者,可以显示第一类信息中的第一数目和第二类信息中的各第二异常信息,或者,可以显示第二类信息中的第二数目和第一类信息中的各第一异常信息,或者,可以显示第一类信息中的第一数目、各第一异常信息、第二类信息中的第二数目以及各第二异常信息。

[0118] 在一个实施例中,参见图6,在图2的基础上,步骤S205之前,该方法还可以包括:

[0119] S206:针对每一请求地址,获取前一时间段内客户端发送的该请求地址对应的第一异常信息的数目,作为第三数目。

[0120] 步骤S205,包括:

[0121] S2051:若第三数目大于第一阈值,则以当前时间段内该请求地址对应的第一数目为报警信息进行报警。

[0122] S2052:若第三数目不大于第一阈值,则以当前时间段内该请求地址对应的第一异常信息为报警信息进行报警。

[0123] 一种实施方式中,第一阈值可以根据业务需求进行设置,例如,第一阈值可以为50次,或者,也可以为100次,但并不限于此。

[0124] 若前一时间段内的第三数目大于第一阈值,表明该请求地址对应的服务频繁异常,即,该请求地址对应的服务可能存在故障,而若已显示了前一时间段内该请求地址对应的各个第一异常信息,相应的,技术人员也就能够基于显示的各个第一异常信息,确定具体的异常原因。因此,为了避免显示过多无用的报警信息,则可以显示当前时间段内该请求地址对应的第一数目,而不显示具体的报警信息。

[0125] 若前一时间段内该请求地址对应的第三数目不大于第一阈值,表明请求地址所请求的服务可能是正常,当前时间段内存在多个第一异常信息,则表明请求地址所请求的服务当前异常,则可以显示各个第一异常信息,以使得技术人员根据显示的各第一异常信息,确定具体的异常原因。

[0126] 在一个实施例中,参见图7,在图2的基础上,步骤S205之前,该方法还可以包括:

[0127] S207:针对每一异常类型,获取前一时间段内统计的该异常类型的第二异常信息的数目,作为第四数目。

[0128] 步骤S205,包括:

[0129] S2053:若第四数目大于第二阈值,则以当前时间段内该异常类型对应的第二数目为报警信息进行报警。

[0130] S2054:若第四数目不大于第二阈值,则以当前时间段内该异常类型的第二异常信息为报警信息进行报警。

[0131] 一种实现方式中,第二阈值可以根据业务需求进行设置,例如,第二阈值可以为50次,或者,也可以为100次,但并不限于此。

[0132] 若前一时间段内的第四数目大于第二阈值,表明该ExceptionName频繁异常,则表示故障类型相同,而若已显示了前一时间段内该ExceptionName对应的各个第二异常信息,相应的,技术人员也就能够基于显示的各个第二异常信息,确定具体的异常原因。因此,为了避免显示过多无用的报警信息,则可以显示当前时间段内该ExceptionName对应的第二数目,而不显示具体的报警信息。

[0133] 若前一时间段内该ExceptionName对应的第四数目不大于第二阈值,表明服务可能是正常,当前时间段内存在多个第二异常信息,则表明出现Exception Name异常,则可以显示各个第二异常信息,以使得技术人员根据显示的各第二异常信息,确定具体的异常原因。

[0134] 在一个实施例中,每一第一异常信息还包括:客户端生成的该业务请求所属的业务链路的链路标识、客户端发送该业务请求时显示的页面的页面地址,以及当前登录客户端的用户的用户标识。

[0135] 每一第二异常信息包括以下至少一项:异常类型的类型标识、异常堆栈信息、运行日志所属的项目的标识,以及用于运行该第二异常信息对应的服务的容器的标识。

[0136] 一种实现方式中，客户端在发送业务请求时，可以为该业务请求生成对应的Trace ID(链路ID)，用于唯一标识业务请求从发起到响应的完成过程。基于该Trace ID，可以对客户端发起业务请求到服务器响应业务请求的整个过程，以及整个过程中产生的关联的运行日志进行关联。

[0137] 客户端向服务器发送业务请求时，显示的页面的页面地址。基于该页面地址，能够确定客户端发送业务请求时显示的页面。

[0138] 当前登录客户端的用户的用户标识可以是用户的ID。基于该用户的ID，能够确定发生业务请求异常的用户。

[0139] 异常类别可以为上述ExceptionName，异常堆栈信息可以为上述Exception Detail。

[0140] 在一个实施例中，步骤S201包括：从第一消息队列中，获取客户端预先添加的针对当前时间段内每一业务响应的第一异常信息。

[0141] 一种实现方式中，客户端可以基于消息队列的方式，将第一异常信息发送至服务器。

[0142] 例如，客户端可以将第一异常信息添加到Rocket MQ(消息中间件)中，作为统一的数据源供后续存储和计算使用。同时，服务器从Rocket MQ获取第一异常信息。

[0143] Rocket MQ框架中包括消息生产者、MQ消息服务和消息消费者。消息生产者(对应于客户端)为负责生成数据的角色，消息生产者生成数据后，将数据添加至MQ消息服务(对应于上述Rocket MQ)。MQ消息服务为MQ消息服务器的统称，用于消息存储与消息转发。消息消费者(对应于服务器)为使用数据的角色，消息消费者从MQ消息服务器中获取数据。

[0144] Rocket MQ可以满足海量信息处理的需求，使用Rocket MQ可以避免业务高峰时期，大量上报的异常事件可能导致服务器瘫痪的情况。

[0145] 在一个实施例中，参见图8，在图2的基础上，步骤S203包括：

[0146] S2031：通过预设日志处理工具，提取运行日志中记录的运行数据中包含预设异常字段的数据，得到服务器运行异常的异常信息，作为第二异常信息，并添加至第二消息队列中。

[0147] 在步骤S204之前，方法还包括：

[0148] S208：通过预设数据流处理工具，从第二消息队列中依次获取各第二异常信息。

[0149] 步骤S204包括：

[0150] S2041：通过预设数据流处理工具，统计每一异常类型的第二异常信息的数目，作为第二数目。

[0151] 一种实现方式中，预设日志处理工具可以是Venus日志管理平台，Venus可以将运行日志中记录的运行数据以文件流的形式引流出来，并可以通过正则表达式对运行数据进行字段解析。

[0152] 一种实现方式中，预设数据流处理工具可以基于flink框实现。可以基于flink框架，确定每一时间段内每一ExceptionName对应的第二异常信息的数目。

[0153] 基于相同的发明构思，本发明实施例提供了一种异常链路监控方法，该方法可以应用于客户端，该客户端可以为上述系统中的客户端101。参见图9，图9为本发明实施例提供了一种异常链路监控方法的流程图，该方法可以包括以下步骤：

[0154] S901:当接收到服务器发送的针对每一业务请求的业务响应时,提取业务响应中业务层的状态码,作为第一状态码。

[0155] S902:若第一状态码为预设的异常状态码,则提取业务响应中业务层的响应信息,作为第一响应信息。

[0156] 其中,第一响应信息用于表示该业务请求所属的业务链路所发生的异常。

[0157] S903:向服务器发送当前时间段内每一业务响应的第一异常信息。

[0158] 其中,每一第一异常信息包含:该业务响应对应的业务请求的请求地址,以及第一响应信息;以使服务器统计当前时间段内每一请求地址对应的第一异常信息的数目,作为第一数目,以及提取当前时间段内服务器的运行日志中记录的运行数据中包含预设异常字段的数据,得到多个第二异常信息;每一第二异常信息表示:服务器响应客户端的每一业务请求的业务链路所发生的异常;统计提取到的每一异常类型的第二异常信息的数目,作为第二数目;基于第一类信息,和/或,第二类信息进行报警;其中,第一类信息包括:当前时间段内的第一数目、以及各第一异常信息;第二类信息包括:当前时间段内的第二数目、以及各第二异常信息。

[0159] 本发明实施例的方法,可以实现对服务器异常自动监控,并进行报警,以及时的发现异常,提高服务器的维护的效率。

[0160] 针对步骤S901-S903,客户端可以向服务器发送业务请求;服务器接收到该业务请求,可以向客户端返回该业务请求对应的业务响应;进而,客户端可以提取该业务响应中业务层的状态码,若该状态码为预设的异常状态码,则提取该业务响应中业务层的响应信息,并将该响应信息发送给服务器。服务器的处理方法,可以参考上述实施例中S201-S205的详细介绍。

[0161] 在一个实施例中,参见图10,在图9的基础上,步骤903之前,方法还可以包括:

[0162] S904:生成该业务请求所属的业务链路的标识,作为链路标识。

[0163] S905:获取发送该业务请求时显示的页面的页面地址,以及当前登录客户端的用户的用户标识。

[0164] 每一第一异常信息还包括:对应的链路标识、页面地址和用户标识。

[0165] 一种实现方式中,客户端在发送业务请求时,可以为该业务请求生成对应的Trace ID(链路ID),用于唯一标识业务请求从发起到响应的完成过程。基于该Trace ID,可以对客户端发起业务请求到服务器响应业务请求的整个过程,以及整个过程中产生的关联的运行日志进行关联。

[0166] 客户端向服务器发送业务请求时,显示的页面的页面地址。基于该页面地址,能够确定客户端发送业务请求时显示的页面。

[0167] 当前登录客户端的用户的用户标识可以是用户的ID。基于该用户的ID,能够确定发生业务请求异常的用户。

[0168] 在一个实施例中,步骤903包括:将当前时间段内每一业务响应的第一异常信息依次添加至第一消息队列,以使服务器从第一消息队列获取针对当前时间段内每一业务响应的各第一异常信息。

[0169] 客户端与服务器之间通过消息队列传输第一异常信息的方式,可以参考上述实施例中相关介绍。

[0170] 在一个实施例中,该方法还包括:

[0171] 将第一异常信息和第二异常信息包含的字段存储在第一数据库中,并将第一异常信息存储在第二数据库中,以及将第二异常信息存储在第三数据库中。

[0172] 第一数据库可以为ES(Elasticsearch,搜索服务器)数据库,第二数据库可以为MySQL(关系型数据库管理系统)数据库,第三数据库可以为Hbase(分布式存储系统)数据库。

[0173] 将第一异常信息和第二异常信息包含的字段存储在ES,ES可以提供快速便捷的大量数据搜索服务。技术人员可以通过存储在ES中的第一异常信息包含的字段,快速搜索到存储在第二数据库的对应的第一异常信息,通过存储在ES中的第二异常信息包含的字段,搜索到第三数据库中的对应的第二异常信息。

[0174] 第一异常信息数据量小,可以存储在MySQL数据库中,提高检索效率。第二异常信息中包含了ExceptionDetail,数据量较大,因此可以使用适合存储海量数据的Hbase数据库存储第二异常信息。

[0175] 参见图11,图11为本发明实施例提供的一种异常链路监控方法的原理示意图。

[0176] 业务名称表示业务请求的名称、业务代码表示业务请求的标识。

[0177] 客户端的发生异常事件对应于上述业务请求所属的业务链路发生异常。接口请求异常,即表示业务请求所属的业务链路异常。客户端,可以基于Ajax event handle(Ajax接口事件集)获取请求中携带的异常的业务层状态码(包括业务1错误码、业务2错误码和业务3错误码)。基于JS error handler and other error handler(JAVA脚本错误集和其他错误集)获取请求中业务层状态码。

[0178] 采集服务,具体用于采集包含上述状态码的异常信息,并发送给监控后台(对应于上述服务器)。

[0179] 针对业务1错误码、业务2错误码和业务3错误码,可以分别向技术人员发送对应的提醒消息。即对应图11中的报警话题1、报警话题2和报警话题3。

[0180] 监控后台可以基于页面URL匹配规则和接口URL匹配规则,对接口请求异常进行分组,确定每一地址对应的异常次数,得到每一地址对应的异常次数的统计图表。

[0181] 监控后台也可以在异常统计界面显示每一地址对应的异常次数的统计图表,即图11中的业务1问题管理、业务2问题管理和业务3问题管理。

[0182] 监控后台可以为每个提醒消息生成对应的报警话题ID(对应于上述Eventid)。

[0183] 参见图12,图12为本发明实施例提供的另一种异常链路监控方法的原理示意图。

[0184] Qae日志对应于上述第二异常信息对应的服务的容器的日志(即本发明实施例中的运行日志)。qiyihao-withdraw-api表示获取日志的接口,Venus可以通过qiyihao-withdraw-api将Qae日志中记录的运行数据以文件流的形式引流出来,并可以通过正则解析,对运行数据进行字段解析,解析出Exception-name对应于上述ExceptionName,解析出Exception-detail对应于上述ExceptionDetail。Venus实时队列对应于上述第二消息队列,qiyihao-withdraw-online-flink表示实时队列名称,Venus将第二异常信息添加至Venus实时队列。

[0185] Flink通过Venus SDK(Software Development Kit,软件开发工具包)消费监控数据:从Venus实时队列获取解析到的Exception-name、Exception-detail、SDK参数。SDK参数

包括:项目名(mp-iqiyihao)、实时队列名(qiyihao-withdraw-online-flink)、消费组(qiyihao-withdraw-dev-exception)。项目名表示运行日志所属的项目的名称,实时队列名表示第二异常信息所在的Venus实时队列,消费组表示Flink消费监控数据的线程。基于Exception-name进行分组,统计每一Exception-name对应的第二异常信息的数目。

[0186] Flink将数据存储到es:Flink将第二异常信息包含的字段存储到es,Index:backend-exception-detail表示生成exception-detail的储存索引。存储的数据包括:Id、ExceptionName、ExceptionDetail、ProjiectName、serviceName、createTimeStamp和Traceid。Id对应于上述事件ID,ProjiectName对应于上述项目标识,serviceName对应于上述QaeApp,createTimeStamp表示该第二异常信息生成的时间。最后用过Qixin报警平台进行警报。

[0187] 参见图13,图13为本发明实施例提供的一种异常链路监控系统的整体架构框图。

[0188] 包含三层:数据源层、引擎层和数据开发层。

[0189] 数据开发层包括:鹰眼监控平台、Grafana(图形)报表和报警平台。

[0190] 基于数据开发层,可以显示包含异常信息对应的可视化图表和报警信息的界面(异常显示界面)。具体的,通过鹰眼监控平台可以显示异常信息。Grafana报表用于生成异常信息对应的可视化图表,便于技术人员直观的查看异常信息。通过报警平台可以客户端发送报警信息。

[0191] 数据源层包括Rocket MQ,对应于上述第一消息队列,客户端将第一异常信息添加至Rocket MQ,作为统一的数据源供后续存储和计算使用。

[0192] 引擎层包括:Flink(流式计算引擎)、YARN(资源管理器)、HDFS(分布式文件系统)、ES、Redis(远程字典服务)、MySQL和Hbase。Flink在YARN(资源管理器)、HDFS(分布式文件系统)运行。

[0193] Flink(对应于上述Flink框架)可以对客户端上报的异常信息进行的计算和聚合,将同一类异常信息进行统计。YARN是一种通用资源管理系统,可以为数据开发层提供统一的资源管理和调度。HDFS是一种分布式文件系统,可以实现流式读取文件数据。Flink在YARN(资源管理器)、HDFS(分布式文件系统)运行。Redis可以用于存储上述异常显示界面中的显示项。MySQL可以用于存储上述第一异常信息。Hbase可以用于存储上述第二异常信息。ES可以用于存储异常信息中的部分字段,技术人员可以使用ES检索MySQL数据库和Hbase数据库中完整的异常信息。

[0194] 基于相同的发明构思,本发明实施例还提供了一种异常链路监控装置,应用于服务器,参见图14,图14为本发明实施例提供的一种异常链路监控装置的结构图,装置包括:

[0195] 获取模块1401,用于获取当前时间段内客户端发送的针对每一业务响应的第一异常信息,以及服务器的运行日志;其中,每一第一异常信息包含:该业务响应对应的业务请求的请求地址,以及第一响应信息;第一响应信息为:客户端在判定该业务响应中业务层的第一状态码为预设的异常状态码的情况下,提取到的该业务响应中携带的业务层的响应信息;第一响应信息用于表示该业务请求所属的业务链路所发生的异常;

[0196] 第一统计模块1402,用于统计获取的每一请求地址对应的第一异常信息的数目,作为第一数目;

[0197] 第二异常信息提取模块1403,用于提取运行日志中记录的运行数据中包含预设异

常字段的数据，得到多个第二异常信息；每一第二异常信息表示：服务器响应客户端的每一业务请求的业务链路所发生的异常；

[0198] 第二统计模块1404，用于统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；

[0199] 报警模块1405，用于基于第一类信息，和/或，第二类信息进行报警；其中，第一类信息包括：当前时间段内的第一数目、以及各第一异常信息；第二类信息包括：当前时间段内的第二数目、以及各第二异常信息。

[0200] 基于相同的发明构思，本发明实施例还提供了一种异常链路监控装置，应用于客户端，参见图15，图15为本发明实施例提供的一种异常链路监控装置的结构图，装置包括：

[0201] 状态码提取模块1501，用于当接收到服务器发送的针对每一业务请求的业务响应时，提取业务响应中业务层的状态码，作为第一状态码；

[0202] 第一响应信息提取模块1502，用于若第一状态码为预设的异常状态码，则提取业务响应中业务层的响应信息，作为第一响应信息；其中，第一响应信息用于表示该业务请求所属的业务链路所发生的异常；

[0203] 发送模块1503，用于向服务器发送当前时间段内每一业务响应的第一异常信息，其中，每一第一异常信息包含：该业务响应对应的业务请求的请求地址，以及第一响应信息；以使服务器统计当前时间段内每一请求地址对应的第一异常信息的数目，作为第一数目，以及提取当前时间段内服务器的运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息；每一第二异常信息表示：服务器响应客户端的每一业务请求的业务链路所发生的异常；统计提取到的每一异常类型的第二异常信息的数目，作为第二数目；基于第一类信息，和/或，第二类信息进行报警；其中，第一类信息包括：当前时间段内的第一数目、以及各第一异常信息；第二类信息包括：当前时间段内的第二数目、以及各第二异常信息。

[0204] 本发明实施例还提供了一种电子设备，如图16所示，包括处理器1601、通信接口1602、存储器1603和通信总线1604，其中，处理器1601，通信接口1602，存储器1603通过通信总线1604完成相互间的通信，

[0205] 存储器1603，用于存放计算机程序；

[0206] 处理器1601，用于执行存储器1603上所存放的程序时，实现上述实施例中任一所述的异常链路监控方法。

[0207] 上述电子设备提到的通信总线可以是外设部件互连标准(Peripheral Component Interconnect，简称PCI)总线或扩展工业标准结构(Extended Industry Standard Architecture，简称EISA)总线等。该通信总线可以分为地址总线、数据总线、控制总线等。为便于表示，图中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0208] 通信接口用于上述电子设备与其他设备之间的通信。

[0209] 存储器可以包括随机存取存储器(Random Access Memory，简称RAM)，也可以包括非易失性存储器(non-volatile memory)，例如至少一个磁盘存储器。可选的，存储器还可以是至少一个位于远离前述处理器的存储装置。

[0210] 上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，简称CPU)、网络处理器(Network Processor，简称NP)等；还可以是数字信号处理器

(Digital Signal Processor,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现场可编程门阵列(Field－Programmable Gate Array,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0211] 在本发明提供的又一实施例中,还提供了一种计算机可读存储介质,所述计算机可读存储介质内存储有计算机程序,所述计算机程序被处理器执行时实现上述实施例中任一所述的异常链路监控方法。

[0212] 在本发明提供的又一实施例中,还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述实施例中任一所述的异常链路监控方法。

[0213] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

[0214] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0215] 本说明书中的各个实施例均采用相关的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统、装置、电子设备、计算机可读存储介质以及计算机程序产品而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0216] 以上所述仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等,均包含在本发明的保护范围内。


101
客户端
102
服务器

图1

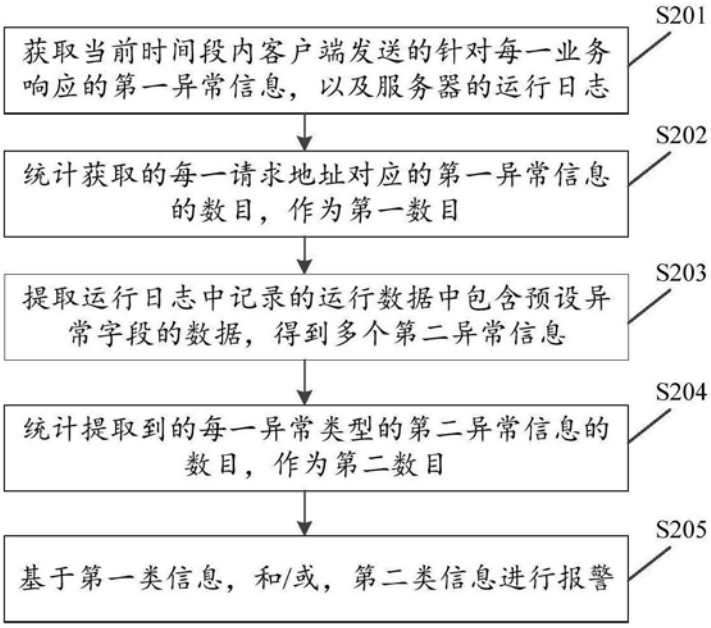

S201
获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志
S202
统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目
S203
提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息
S204
统计提取到的每一异常类型的第二异常信息的数目，作为第二数目
S205
基于第一类信息，和/或，第二类信息进行报警

图2


xxxxxxx…
java.lang.RuntimeException: 正在处理，请稍后重试！
at com.iqiyi.mbd.qiyihao.withdraw.utils.ForbidOvermuchReqUtil.checkReqPass(ForbidOvermuchReqUtil.java:30)
at com.iqiyi.mbd.qiyihao.withdraw.service.impl.BalanceCentreServiceImpl.saveBankInfo(BalanceCentreServiceImpl.java:281)
at com.iqiyi.mbd.qiyihao.withdraw.api.controller.BalanceCentreController.saveUserBankInfo(BalanceCentreController.java:118)
at sun.reflect.GeneratedMethodAccessor856.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
at org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:205)
at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:133)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)

图3


ErrorType:Service API Error
Uid:2002590244
EventId:6afd44fa76ac53e1ab1cdd3077bfda7e
Url:[-20006]{//mp-api.iqiyi.com/uv/api/2.0/rz/info/nickname_and_profile}
Response:{msg=系统错误}
Link:https://mp.iqiyi.com/u

图4

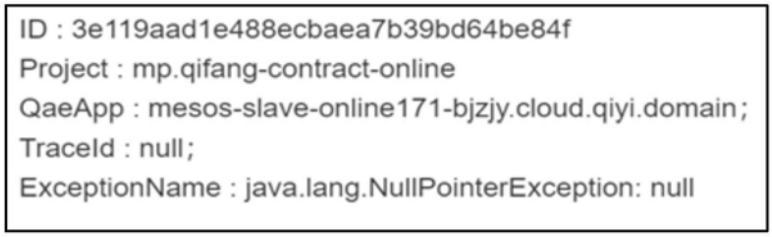

ID : 3e119aad1e488ecbaea7b39bd64be84f
Project : mp.qifang-contract-online
QaeApp : mesos-slave-online171-bjzjy.cloud.qiyi.domain;
TraceId : null;
ExceptionName : java.lang.NullPointerException: null

图5

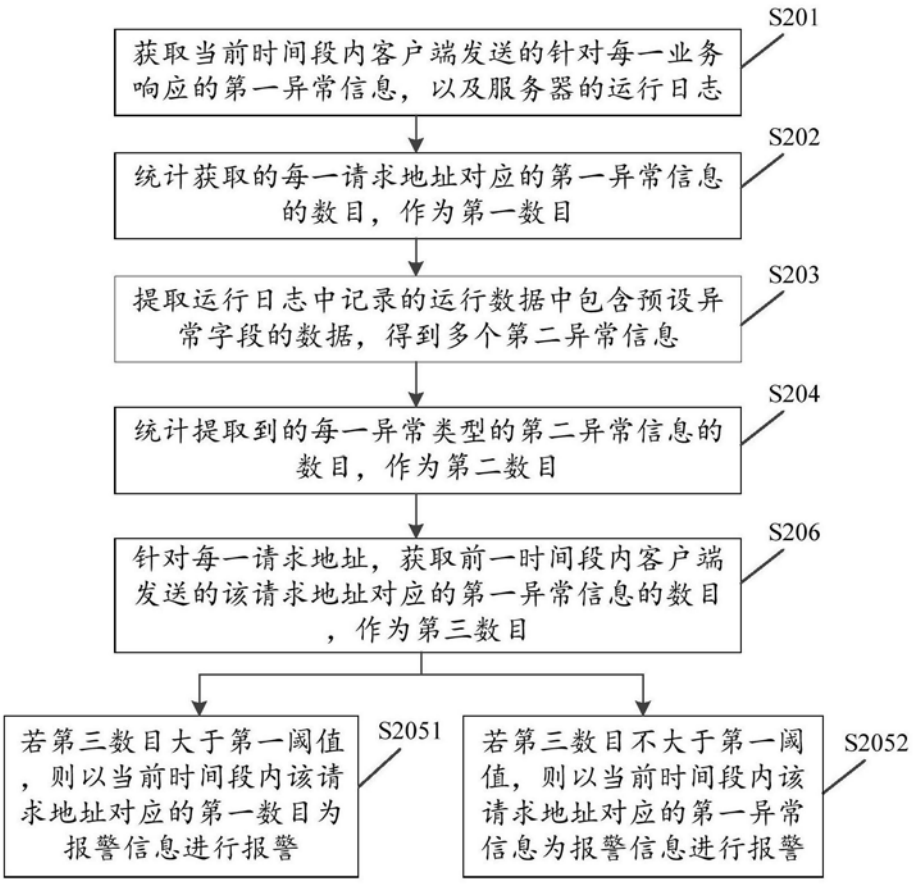

S201
获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志
S202
统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目
S203
提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息
S204
统计提取到的每一异常类型的第二异常信息的数目，作为第二数目
S206
针对每一请求地址，获取前一时间段内客户端发送的该请求地址对应的第一异常信息的数目，作为第三数目
S2051
若第三数目大于第一阈值，则以当前时间段内该请求地址对应的第一数目为报警信息进行报警
S2052
若第三数目不大于第一阈值，则以当前时间段内该请求地址对应的第一异常信息为报警信息进行报警

图6

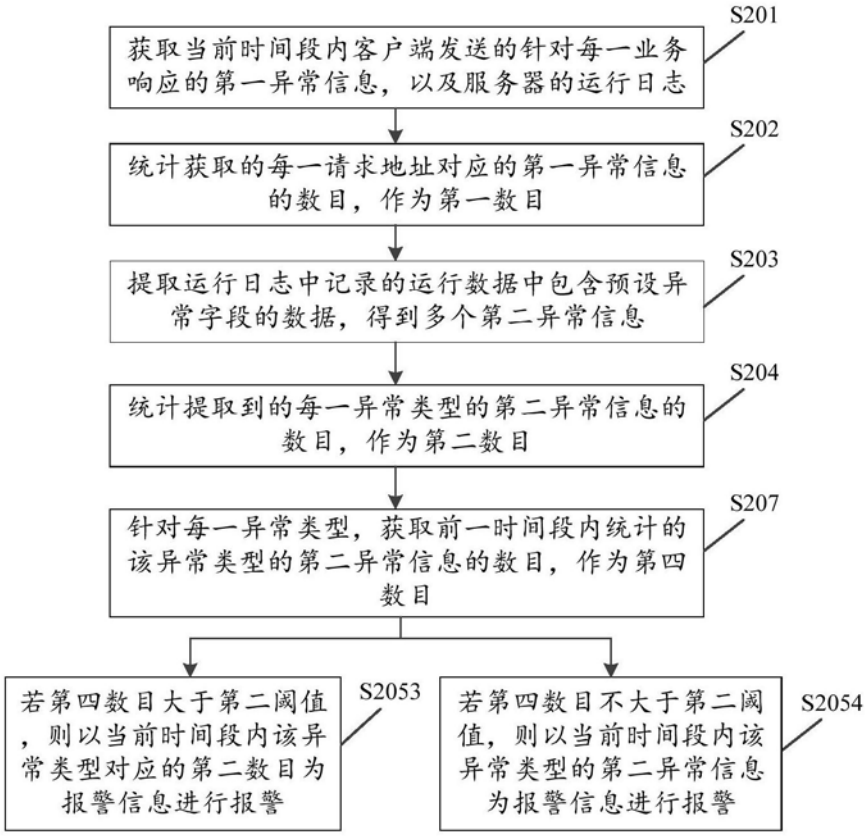

S201
获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志
S202
统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目
S203
提取运行日志中记录的运行数据中包含预设异常字段的数据，得到多个第二异常信息
S204
统计提取到的每一异常类型的第二异常信息的数目，作为第二数目
S207
针对每一异常类型，获取前一时间段内统计的该异常类型的第二异常信息的数目，作为第四数目
S2053
若第四数目大于第二阈值，则以当前时间段内该异常类型对应的第二数目为报警信息进行报警
S2054
若第四数目不大于第二阈值，则以当前时间段内该异常类型的第二异常信息为报警信息进行报警

图7

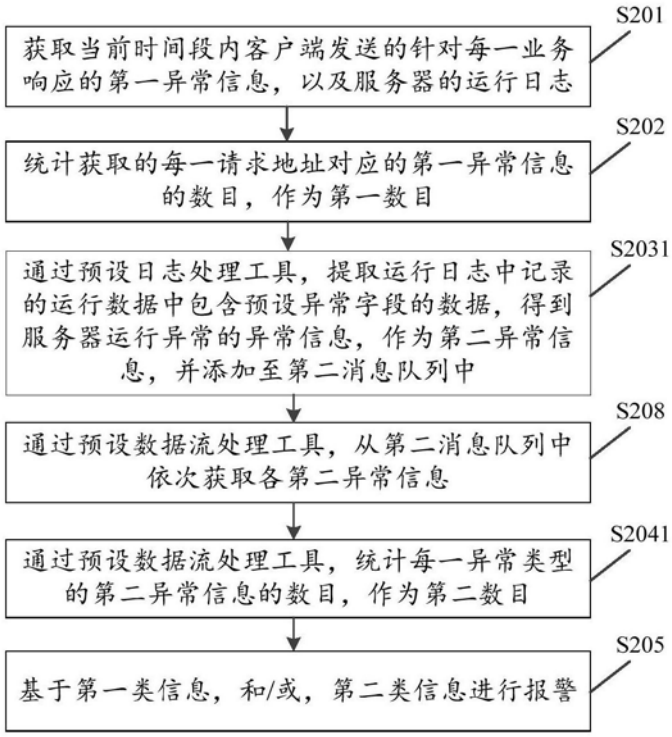

S201
获取当前时间段内客户端发送的针对每一业务响应的第一异常信息，以及服务器的运行日志
S202
统计获取的每一请求地址对应的第一异常信息的数目，作为第一数目
S2031
通过预设日志处理工具，提取运行日志中记录的运行数据中包含预设异常字段的数据，得到服务器运行异常的异常信息，作为第二异常信息，并添加至第二消息队列中
S208
通过预设数据流处理工具，从第二消息队列中依次获取各第二异常信息
S2041
通过预设数据流处理工具，统计每一异常类型的第二异常信息的数目，作为第二数目
S205
基于第一类信息，和/或，第二类信息进行报警

图8

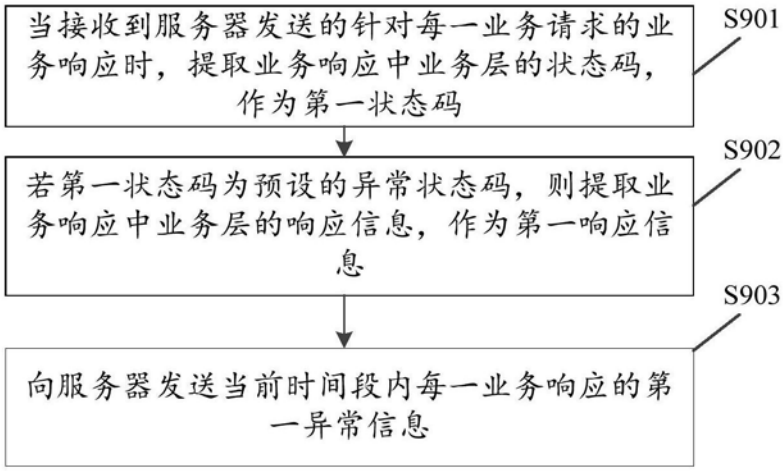

当接收到服务器发送的针对每一业务请求的业务响应时，提取业务响应中业务层的状态码，作为第一状态码
S901
若第一状态码为预设的异常状态码，则提取业务响应中业务层的响应信息，作为第一响应信息
S902
向服务器发送当前时间段内每一业务响应的第一异常信息
S903

图9

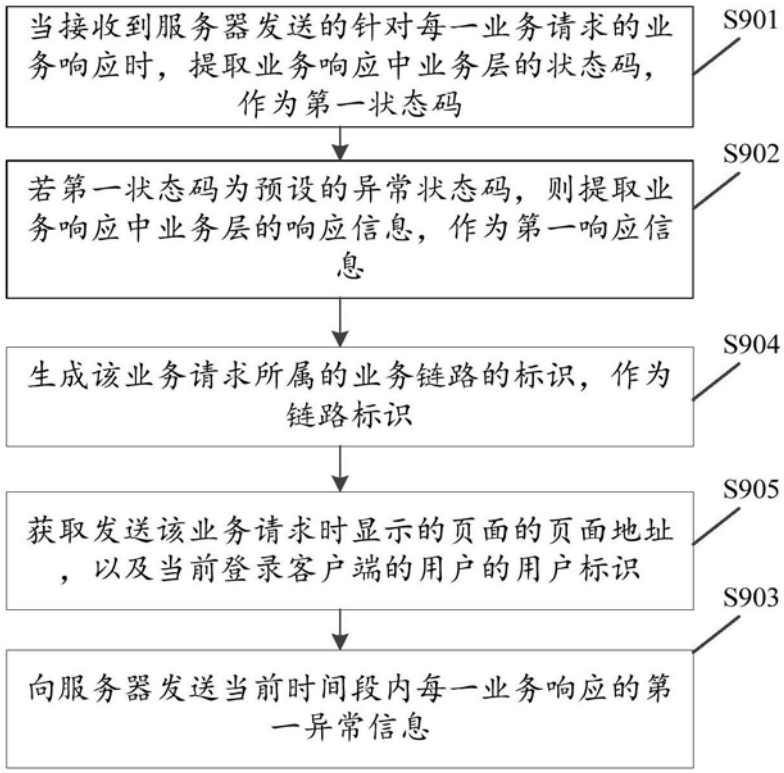

当接收到服务器发送的针对每一业务请求的业务响应时，提取业务响应中业务层的状态码，作为第一状态码
S901
若第一状态码为预设的异常状态码，则提取业务响应中业务层的响应信息，作为第一响应信息
S902
生成该业务请求所属的业务链路的标识，作为链路标识
S904
获取发送该业务请求时显示的页面的页面地址，以及当前登录客户端的用户的用户标识
S905
向服务器发送当前时间段内每一业务响应的第一异常信息
S903

图10

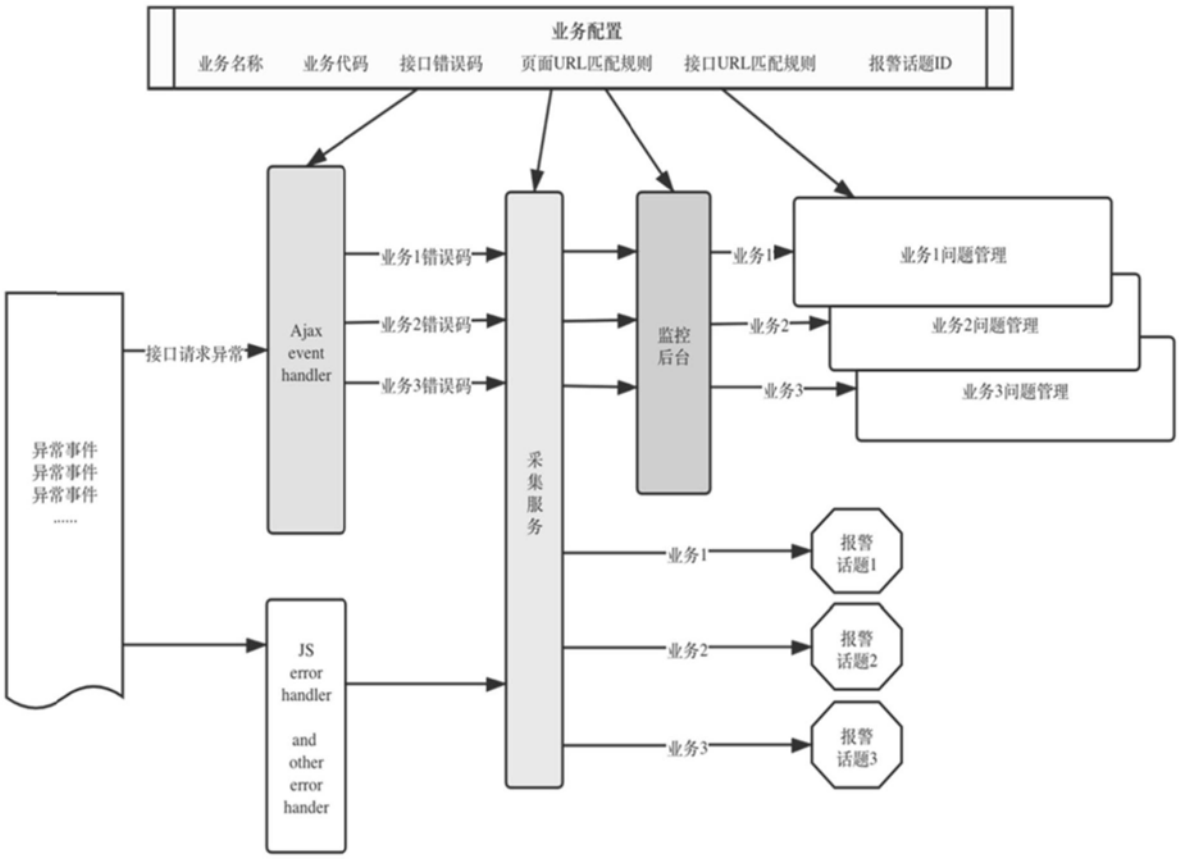

业务配置
业务名称
业务代码
接口错误码
页面URL匹配规则
接口URL匹配规则
报警话题ID
异常事件
异常事件
异常事件
.....
接口请求异常
Ajax
event
handler
业务1错误码
业务2错误码
业务3错误码
采集服务
监控后台
业务1
业务2
业务3
业务1问题管理
业务2问题管理
业务3问题管理
JS
error
handler
and
other
error
hander
报警话题1
报警话题2
报警话题3

图11

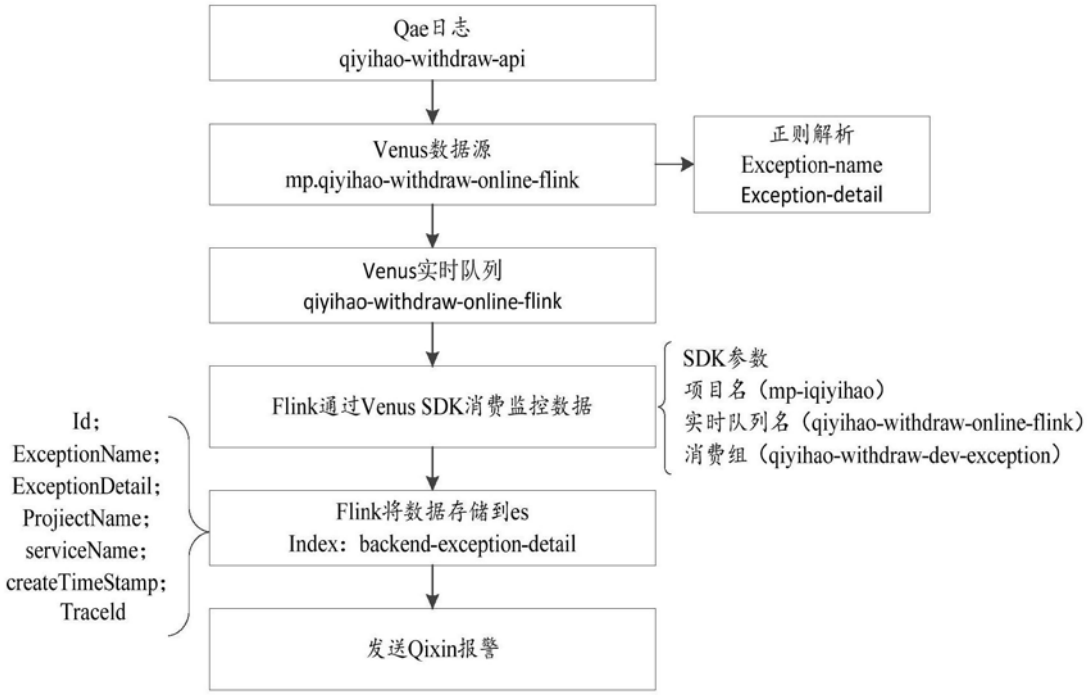

Qae日志
qiyihao-withdraw-api
Venus数据源
mp.qiyihao-withdraw-online-flink
正则解析
Exception-name
Exception-detail
Venus实时队列
qiyihao-withdraw-online-flink
Flink通过Venus SDK消费监控数据
SDK参数
项目名（mp-iqiyihao）
实时队列名（qiyihao-withdraw-online-flink）
消费组（qiyihao-withdraw-dev-exception）
Id;
ExceptionName;
ExceptionDetail;
ProjiectName;
serviceName;
createTimeStamp;
TraceId
Flink将数据存储到es
Index：backend-exception-detail
发送Qixin报警

图12

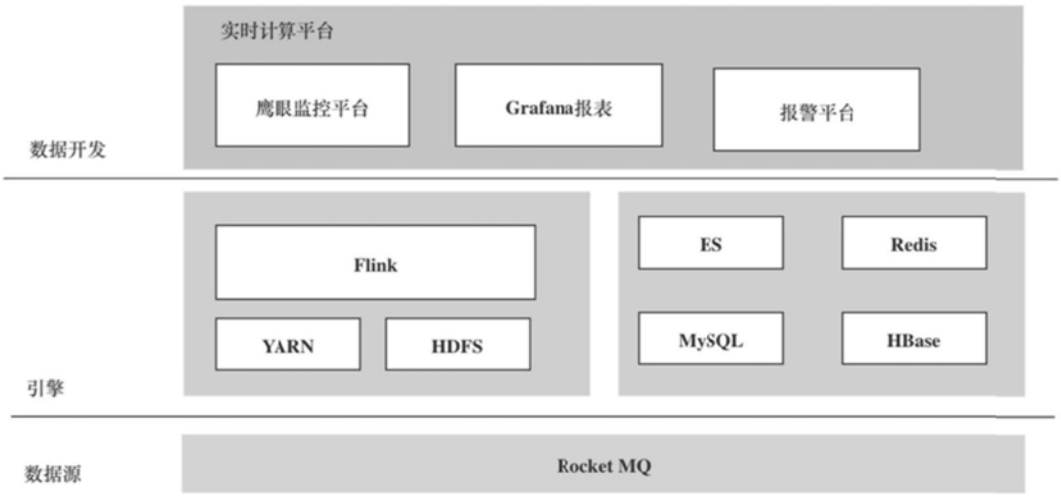

实时计算平台
鹰眼监控平台
Grafana报表
报警平台
数据开发
Flink
YARN
HDFS
ES
Redis
MySQL
HBase
引擎
数据源
Rocket MQ

图13


1401
获取模块
1402
第一统计模块
1403
第二异常信息提取模块
1404
第二统计模块
1405
报警模块

图14

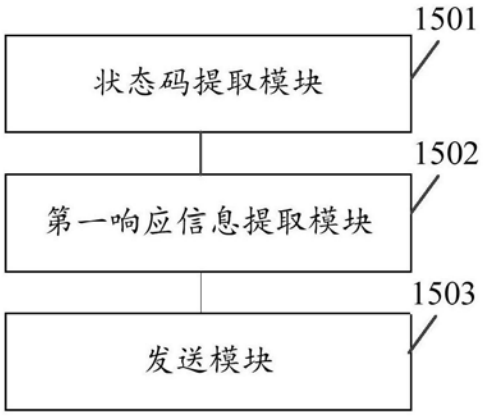

1501
状态码提取模块
1502
第一响应信息提取模块
1503
发送模块

图15

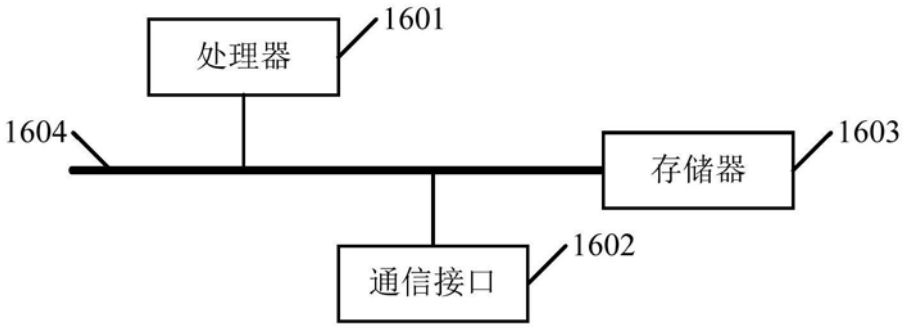

1601
处理器
1604
存储器
1603
通信接口
1602

图16