(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 108599977 A
(43)申请公布日 2018.09.28

(21)申请号 201810150782.5

(22)申请日 2018.02.13

(71)申请人 南京途牛科技有限公司
地址 210000 江苏省南京市玄武区玄武大道699-32号途牛大厦

(72)发明人 梅存兵

(74)专利代理机构 南京众联专利代理有限公司 32206
代理人 叶涓涓

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

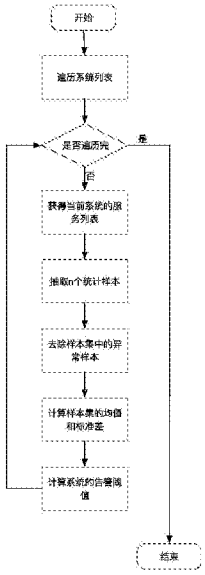
权利要求书3页 说明书7页 附图4页

(54)发明名称

基于统计方法监控系统可用性的系统及方法

(57)摘要

本发明提出了基于统计方法监控系统可用性的系统及方法，系统包括：系统间服务调用日志模块、报警阈值分析模块、告警分析模块、监控告警展示模块；通过采集系统间的调用日志，定期对历史数据进行分析学习，取得每个系统的一般表现；对最近一个单位时间t内的数据进行分析，辨别每个系统当前的错误数是否反常、系统间调用的错误率是否异常、系统各服务各实例的可用性是否异常；并在系统拓扑图上以告警形式标记出异常的系统、异常的系统间调用关系。在展示告警信息时，本发明在系统拓扑图上显示了系统状态、系统间调用的状态、系统服务和实例的状态，以便在大面积系统出现问题时快速定位出问题系统。



CN 108599977 A

1.基于统计方法监控系统可用性的系统，其特征在于，包括：系统间服务调用日志模块、报警阈值分析模块、告警分析模块、监控告警展示模块；

系统间服务调用日志模块用于采集记录系统间所有调用的日志信息，调用时间、调用方IP和端口号、被调用方IP和端口号、调用的服务标识、成功与否；

报警阈值分析模块用于定期对历史数据进行学习，找出每一个系统一般情境下的表现，获得了当前系统的n份样本，每一个样本描述了单位时间t内错误数，并去除样本集中的异常点，去除异常点的过程包括：

i.计算当前样本集的均值$u=\sum_{i=1}^{n}xi$和标准差$std=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi-u)^2}$；

ii.找到样本集中所有大于u+3*std的样本点、计算其个数n1，并将这些数据从样本集中去除，计算取出上述样本点后的新样本集的个数n2；

iii.如果满足条件，则完成异常点的去除，继续执行以下步骤；否则，执行步骤i；

计算该系统的错误数告警线alertNum＝u+std*3；

告警分析模块用于定时采集最近一个t时间段内的日志，逐次分析每个系统的错误数是否异常、每个系统的每个服务错误率是否异常、实例错误率是否异常、任意两个系统间的错误数情况，并遍历系统列表后具体进行如下判断：

a)如果该系统的累计错误数大于该系统的告警阈值，则标记该系统异常；

b)遍历该系统的每一个服务，应用异常判断方法，判定其错误率是否异常；

c)遍历该系统的每一个实例，应用异常判断方法，以判定其错误率是否异常；

所述异常判断方法包括：

a)将正确的次数记为tNum，错误的次数记为fNum，总调用次数num＝tNum+fNum；

b)如果fNum<第一阈值，返回正常；否则下一步；

c)如果num>＝第二阈值则下一步，否则当fNum＝第一阈值时返回正常，否则返回异常；

d)如果fNum/num<第三阈值，返回正常；否则下一步；

e)当fNum<tNum时，k＝fNum+第四阈值，否则k＝fNum-第五阈值；

f)计算$z=\frac{(k-num*0.5)}{\sqrt{num*0.5*0.5}}$

如果z>第六阈值则返回异常，否则返回正常；

判断完成后整理数据，计算每一组clientInstance调用serverInstance的错误数；

从系统拓扑图上反查clientInstance和serverInstance对应的系统client和server，统计每一组client系统调用server系统的累计错误数；

告警展示模块用于基于系统拓扑图，在告警数据分析完成后将其展示在系统拓扑图上。

2.根据权利要求1所述的基于统计方法监控系统可用性的系统，其特征在于：报警阈值分析模块还用于设置告警阈值，在计算该系统的错误数告警线之后，如果alertNum<告警阈值则alertNum设置为告警阈值。

3.根据权利要求1所述的基于统计方法监控系统可用性的系统，其特征在于：所述去除异常点过程中条件如下：

n1＝0或者(n-n2)>30或者(n-n2)>n/3。

4.根据权利要求1所述的基于统计方法监控系统可用性的系统，其特征在于：告警展示模块还用于：

1、当系统异常时，在系统图标上添加警告的标志：

2、当系统的服务、实例异常时，点击系统图标，弹层显示错误信息；

3、当系统间调用错误数不为0时，绘制连线和指向性箭头。

5.根据权利要求4所述的基于统计方法监控系统可用性的系统，其特征在于：所述连线的宽度与错误数相关。

6.基于统计方法监控系统可用性的方法，其特征在于，包括如下步骤：

步骤一，采集记录系统间所有调用的日志信息，调用时间、调用方IP和端口号、被调用方IP和端口号、调用的服务标识、成功与否；

步骤二，定期对历史数据进行学习，找出每一个系统一般情境下的表现，获得了当前系统的n份样本，每一个样本描述了单位时间t内错误数，并去除样本集中的异常点，去除异常点的过程包括：

i.计算当前样本集的均值$u=\sum_{i=1}^{n} xi$和标准差$std=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi-u)^2}$；

ii.找到样本集中所有大于u+3*std的样本点、计算其个数n1，并将这些数据从样本集中去除，计算取出上述样本点后的新样本集的个数n2；

iii.如果满足条件，则完成异常点的去除，继续执行以下步骤；否则，执行步骤i；

计算该系统的错误数告警线alertNum＝u+std*3；

步骤三，定时采集最近一个t时间段内的日志，逐次分析每个系统的错误数是否异常、每个系统的每个服务错误率是否异常、实例错误率是否异常、任意两个系统间的错误数情况，并遍历系统列表后具体进行如下判断：

a)如果该系统的累计错误数大于该系统的告警阈值，则标记该系统异常；

b)遍历该系统的每一个服务，应用异常判断方法，判定其错误率是否异常；

c)遍历该系统的每一个实例，应用异常判断方法，以判定其错误率是否异常；

所述异常判断方法包括：

a)将正确的次数记为tNum，错误的次数记为fNum，总调用次数num＝tNum+fNum；

b)如果fNum<第一阈值，返回正常；否则下一步；

c)如果num>＝第二阈值则下一步，否则当fNum＝第一阈值时返回正常，否则返回异常；

d)如果fNum/num<第三阈值，返回正常；否则下一步；

e)当fNum<tNum时，k＝fNum+第四阈值，否则k＝fNum-第五阈值；

f)计算$z=\frac{(\delta-num*0.01)}{\sqrt{num*0.01*0.99}}$

如果z>第六阈值则返回异常，否则返回正常；

判断完成后整理数据，计算每一组clientInstance调用serverInstance的错误数；

从系统拓扑图上反查clientInstance和serverInstance对应的系统client和server，统计每一组client系统调用server系统的累计错误数；

步骤四，基于系统拓扑图，在告警数据分析完成后将其展示在系统拓扑图上。

7.根据权利要求6所述的基于统计方法监控系统可用性的方法，其特征在于，步骤一还包括：

设置告警阈值，在计算该系统的错误数告警线之后，如果alertNum<告警阈值则alertNum设置为告警阈值。

8.根据权利要求6所述的基于统计方法监控系统可用性的方法，其特征在于，步骤二去除异常点过程中条件如下：

n1＝0或者(n-n2)>30或者(n-n2)>n/3。

9.根据权利要求6所述的基于统计方法监控系统可用性的方法，其特征在于，步骤四还包括如下步骤：

1、当系统异常时，在系统图标上添加警告的标志；

2、当系统的服务、实例异常时，点击系统图标，弹层显示错误信息；

3、当系统间调用错误数不为0时，绘制连线和指向性箭头。

10.根据权利要求9所述的基于统计方法监控系统可用性的方法，其特征在于：所述连线的宽度与错误数相关。

基于统计方法监控系统可用性的系统及方法

技术领域

[0001] 本发明属于软件系统监控技术领域，涉及一种基于统计方法监控系统可用性的系统及方法。

背景技术

[0002] 互联网企业一般包含了大量的应用系统，除了对外开放的网站、APP等，内部也会有很多应用系统支撑企业的运营、管理。内部的应用系统间一般存在较复杂的调用关系，一个系统提供给另一个系统调用的功能称之为服务。应用系统的可用性监控业界一般采取以下手段：

[0003] 方法一：使用zabbix等工具，监控系统服务器的某一些指标，如：Web系统进程数/线程数、CPU负载、可用内存、http异常状态码数量、请求响应时间等。当指标超过设定阈值时进行报警。

[0004] 方法二：模拟客户端进行周期性调用，检测服务端系统响应的内容、速度等指标是否符合设定阈值。当指标超过设定阈值时进行报警。

[0005] 但现有的监控方式存在多种缺陷：

[0006] 1.方法一及方法二中的阈值都需要人工设定，不同系统的阈值千差万别、同一系统不同时期阈值也截然不同，阈值的设定与维护都有很大的工作量。实际操作中，一般采用试错法，即误报后放宽阈值、漏报后收紧阈值，这样误报率、漏报率都很高。

[0007] 2.方法一的监控只能部分反应可用性，而不能作为实际的可用性指标，检测出来的异常不代表系统可用性降低、系统不可用时也不都反应在这些监控指标上。

[0008] 3.方法二的监控直接反应了可用性，但其作为抽检手段样本数量较少、覆盖面较窄，仅能监测读操作而较少用于写操作。

[0009] 4.当系统较多、较复杂时，上述两种监控方法的指标过多、告警数量多、告警噪音大，会影响问题的判断及定位。

[0010] 5.在新系统上线、新的服务上线、系统及服务部署发生变更时，上述两种监控方法都需要人工维护监控项，不适用于具有故障自动切换、动态扩充服务能力的系统。

[0011] 6.在进行错误率监测告警时，阈值法常常造成误报，例如当错误率要求不超过1%时，如果只发生了一次操作并且失败了(错误率100%)就会告警，但多数情况下无需告警。

[0012] 7.复杂系统集群多个系统同时出现故障时，难以快速定位出真正出现故障的系统，只能胡子眉毛一把抓，浪费了宝贵的时间。

发明内容

[0013] 为解决上述问题，本发明提出了基于统计方法监控系统可用性的系统及方法，通过采集系统间的调用日志，定期对历史数据进行分析学习，取得每个系统的一般表现；对最近一个单位时间t内的数据进行分析，辨别每个系统当前的错误数是否反常、系统间调用的错误率是否异常、系统各服务各实例的可用性是否异常；并在系统拓扑图上以告警形式标

记出异常的系统、异常的系统间调用关系。

[0014] 为了达到上述目的，本发明提供如下技术方案：

[0015] 基于统计方法监控系统可用性的系统，包括：系统间服务调用日志模块、报警阈值分析模块、告警分析模块、监控告警展示模块；

[0016] 系统间服务调用日志模块用于采集记录系统间所有调用的日志信息，调用时间、调用方 IP和端口号、被调用方IP和端口号、调用的服务标识、成功与否；

[0017] 报警阈值分析模块用于定期对历史数据进行学习，找出每一个系统一般情境下的表现，获得了当前系统的n份样本，每一个样本描述了单位时间t内错误数，并去除样本集中的异常点，去除异常点的过程包括：

[0018] i.计算当前样本集的均值$u=\sum_{i=1}^{n}xi$和标准差$std=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi-u)^2}$；

[0019] ii.找到样本集中所有大于u+3*std的样本点、计算其个数n1，并将这些数据从样本集中去除，计算取出上述样本点后的新样本集的个数n2；

[0020] iii.如果满足条件，则完成异常点的去除，继续执行以下步骤；否则，执行步骤 i；

[0021] 计算该系统的错误数告警线alertNum＝u+std*3；

[0022] 告警分析模块用于定时采集最近一个t时间段内的日志，逐次分析每个系统的错误数是否异常、每个系统的每个服务错误率是否异常、实例错误率是否异常、任意两个系统间的错误数情况，并遍历系统列表后具体进行如下判断：

[0023] a)如果该系统的累计错误数大于该系统的告警阈值，则标记该系统异常；

[0024] b)遍历该系统的每一个服务，应用异常判断方法，判定其错误率是否异常；

[0025] c)遍历该系统的每一个实例，应用异常判断方法，以判定其错误率是否异常；

[0026] 所述异常判断方法包括：

[0027] a)将正确的次数记为tNum，错误的次数记为fNum，总调用次数num＝tNum+fNum；

[0028] b)如果fNum<第一阈值，返回正常；否则下一步；

[0029] c)如果num>＝第二阈值则下一步，否则当fNum＝第一阈值时返回正常，否则返回异常；

[0030] d)如果fNum/num<第三阈值，返回正常；否则下一步；

[0031] e)当fNum<tNum时，k＝fNum+第四阈值，否则k＝fNum-第五阈值；

[0032] f)计算$z=\frac{(k-num*0.01)}{\sqrt{num*0.01*0.99}}$

[0033] 如果z>第六阈值则返回异常，否则返回正常；

[0034] 判断完成后整理数据，计算每一组clientInstance调用serverInstance的错误数；

[0035] 从系统拓扑图上反查clientInstance和serverInstance对应的系统client和server，统计每一组client系统调用server系统的累计错误数；

[0036] 告警展示模块用于基于系统拓扑图，在告警数据分析完成后将其展示在系统拓扑图上。

[0037] 进一步的，报警阈值分析模块还用于设置告警阈值，在计算该系统的错误数告警线之后，如果alertNum<告警阈值则alertNum设置为告警阈值。

[0038] 进一步的，所述去除异常点过程中条件如下：

[0039] n1＝0或者(n-n2)>30或者(n-n2)>n/3。

[0040] 进一步的，告警展示模块还用于：

[0041] 1、当系统异常时，在系统图标上添加警告的标志：

[0042] 2、当系统的服务、实例异常时，点击系统图标，弹层显示错误信息；

[0043] 3、当系统间调用错误数不为0时，绘制连线和指向性箭头。

[0044] 进一步的，所述连线的宽度与错误数相关。

[0045] 基于统计方法监控系统可用性的方法，包括如下步骤：

[0046] 步骤一，采集记录系统间所有调用的日志信息，调用时间、调用方IP和端口号、被调用方IP和端口号、调用的服务标识、成功与否；

[0047] 步骤二，定期对历史数据进行学习，找出每一个系统一般情境下的表现，获得了当前系统的n份样本，每一个样本描述了单位时间t内错误数，并去除样本集中的异常点，去除异常点的过程包括：

[0048] i.计算当前样本集的均值$u=\sum_{i=1}^{n}xi$和标准差$std=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi-u)^2}$；

[0049] ii.找到样本集中所有大于u+3*std的样本点、计算其个数n1，并将这些数据从样本集中去除，计算取出上述样本点后的新样本集的个数n2；

[0050] iii.如果满足条件，则完成异常点的去除，继续执行以下步骤；否则，执行步骤 i；

[0051] 计算该系统的错误数告警线alertNum＝u+std*3；

[0052] 步骤三，定时采集最近一个t时间段内的日志，逐次分析每个系统的错误数是否异常、每个系统的每个服务错误率是否异常、实例错误率是否异常、任意两个系统间的错误数情况，并遍历系统列表后具体进行如下判断：

[0053] a)如果该系统的累计错误数大于该系统的告警阈值，则标记该系统异常；

[0054] b)遍历该系统的每一个服务，应用异常判断方法，判定其错误率是否异常；

[0055] c)遍历该系统的每一个实例，应用异常判断方法，以判定其错误率是否异常；

[0056] 所述异常判断方法包括：

[0057] a)将正确的次数记为tNum，错误的次数记为fNum，总调用次数num＝tNum+fNum；

[0058] b)如果fNum<第一阈值，返回正常；否则下一步；

[0059] c)如果num>＝第二阈值则下一步，否则当fNum＝第一阈值时返回正常，否则返回异常；

[0060] d)如果fNum/num<第三阈值，返回正常；否则下一步；

[0061] e)当fNum<tNum时，k＝fNum+第四阈值，否则k＝fNum-第五阈值；

[0062] f)计算$z=\frac{(k-num*0.01)}{\sqrt{num*0.01*0.99}}$

[0063] 如果z>第六阈值则返回异常，否则返回正常；

[0064] 判断完成后整理数据，计算每一组clientInstance调用serverInstance的错误数；

[0065] 从系统拓扑图上反查clientInstance和serverInstance对应的系统client和server，统计每一组client系统调用server系统的累计错误数；

[0066] 步骤四，基于系统拓扑图，在告警数据分析完成后将其展示在系统拓扑图上。

[0067] 进一步的，步骤一还包括：

[0068] 设置告警阈值，在计算该系统的错误数告警线之后，如果alertNum<告警阈值则alertNum 设置为告警阈值。

[0069] 进一步的，步骤二去除异常点过程中条件如下：

[0070] n1＝0或者(n-n2)>30或者(n-n2)>n/3。

[0071] 进一步的，步骤四还包括如下步骤：

[0072] 1、当系统异常时，在系统图标上添加警告的标志：

[0073] 2、当系统的服务、实例异常时，点击系统图标，弹层显示错误信息；

[0074] 3、当系统间调用错误数不为0时，绘制连线和指向性箭头。

[0075] 进一步的，所述连线的宽度与错误数相关。

[0076] 与现有技术相比，本发明具有如下优点和有益效果：

[0077] 1.本发明能够通过分析实例间服务调用日志来监控系统、系统的服务、系统的实例是否异常，并结合系统拓扑图展示告警信息；在展示告警信息时，本发明在系统拓扑图上显示了系统状态、系统间调用的状态、系统服务和实例的状态，以便在大面积系统出现问题时快速定位出问题系统。

[0078] 2.本发明通过分析过去一段时间系统的正常表现，获得了告警阈值；在告警分析时，错误数超过该阈值就告警；对于数量型告警，提供了告警阈值的自动设置方法，减少了人工，提高了告警的准确率，大大降低了误报和漏报这两种情况。新系统上线运行一段时间后，本发明可以自动为其设置告警阈值。

[0079] 3.能够检验分析系统的服务、实例是否异常，对于比例型告警，提高了告警的准确率，减少了误报和漏报。

[0080] 4.监控方法取样的是实际数据，比定期采样覆盖更全面。

附图说明

[0081] 图1为正态分布示意图。

[0082] 图2为日志格式示例图。

[0083] 图3为报警阈值分析流程图。

[0084] 图4为调用Logstash接口得到的系统内样本错误数示意图。

[0085] 图5为实例间调用数据图。

[0086] 图6为添加警告标志的系统拓扑图。

[0087] 图7为弹层显示错误信息的系统拓扑图。

具体实施方式

[0088] 以下将结合具体实施例对本发明提供的技术方案进行详细说明，应理解下述具体实施方式仅用于说明本发明而不用于限制本发明的范围。另外，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0089] 我们认为，一个系统单位时间t内的错误数受到许多独立随机因素的因素的影响，一般情况下每个因素的影响都很小，故我们可以将其作为一个服从正态分布的随机变量来研究。正态分布的密度函数为：

[0090] $f(x)=\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$。

[0091] 通过采集该系统过去一段时间一般情况下的表现数据，我们可以计算出单位时间t内错误数的平均值u和标准差std。将最近一个单位时间t内的错误数记为failNum，如图1所示，我们很容易可以计算出概率P(failNum>=u+3*std)远小于0.01，即其是一个极端的小概率事件。所以我们去观测该系统最近一个单位时间t内出现的错误数，其值超出均值加上三个标准差的情况一定是极端情况，需要人工关注，应当发出告警信息。

[0092] 我们在通过观察系统的错误数研究系统和服务的错误率时，很容易就发现：即便错误率 p0最高可接受的值为0.01，实际观察100次调用时，超过1次调用失败也不能说明系统有问题，因为这是发生概率较大的事件。

[0093] 当调用次数比较少时(这里我们取少于40次)，我们来计算当系统本质上的错误率p不高于p0，但n次调用中观察到的错误数failNum大于failLevel的条件概率p1：

[0094]

$$p1=P(failNum>failLevel\mid p\le p0)=\sum_{k=failLevel+1}^{n}C_n^k p^k(1-p)^{n-k}\le\sum_{k=failLevel+1}^{n}C_n^k p0^k(1-p0)^{n-k}$$

[0095] 我们将发生概率低于0.05的事件称作小概率事件。在少量的有限次试验中，小概率事件不应该发生，即当小概率事件发生时，我们不能认为p不高于p0，而应当认为p高于p0，此时系统错误率过高、应当发出告警。通过数值运算，我们找到了所有使得p<0.05的failLevel 的临界点：当n<=5时，failLvel的临界点是0，当5<n<=35时，failLevel的临界点是1，当35<n<40时，failLevel的临界点是2。即：观察n次调用，如果错误数高于对应的failLevel，就认为发生了一个小概率事件，需要关注；如果不高于则认为系统正常。为便于处理，我们将n<40时的failLevel统一设定为1，实践中其误差在可接受范围内。

[0096] 当调用次数比较多时(这里我们认为不少于40次)，我们观察到的错误率为p1，系统本质上的错误率为p，正常情况下不高于p0。根据中心极限定理，我们知道p1近似服从均值为p、方差为p(1-p)/n的正态分布，亦即统计量$\frac{p1-p}{\sqrt{p(1-p)/n}}$服从标准正态分布。当p<=p0时，$\frac{p1-p0}{\sqrt{p0(1-p0)/n}}$近似服从标准正态分布；由标准正态分布分位数表可知，当$\frac{p1-p0}{\sqrt{p0(1-p0)/n}}>1.645$时，其概率低于0.05，是小概率事件，应当关注、发出告警。为方便应用，我们将$\frac{p1-p0}{\sqrt{p0(1-p0)/n}}$变形为：$\frac{n*p1-n*p0}{\sqrt{np0(1-p0)}}$，其中n*p1就是实际观察到的错误数。

[0097] 相应的异常判断方法包括如下步骤：

[0098] a)将正确的次数记为tNum，错误的次数记为fNum，总调用次数num=tNum+fNum；

[0099] b)如果fNum<1，返回正常；否则下一步；

[0100] c)如果num>=40则下一步，否则当fNum=1时返回正常，否则返回异常；

[0101] d)如果fNum/num<0.01，返回正常；否则下一步；

[0102] e)当fNum<tNum时，k=fNum+0.5，否则k=fNum-0.5(因为是近似正态分布，通过修正可以使统计量更加逼近正态分布)；

[0103] f)计算$z=\frac{(x-mean(x))}{\sqrt{mean(x)\cdot(1-mean(x))}}$

[0104] 如果z>1.645则返回异常，否则返回正常。

[0105] 异常判断方法中的各数据均可以根据需要调整。

[0106] 本发明提供的基于统计方法监控系统可用性的系统，包括：系统间服务调用日志模块、报警阈值分析模块、告警分析模块、监控告警展示模块。从系统拓扑图中可以直接获取各个系统的服务列表和实例列表。本司提交的申请号为2017109039551，名称为系统部署与依赖关系自动绘制系统及方法的发明专利中较为详细地阐述了服务列表、实例列表及有关服务和实例的日志。

[0107] 系统间服务调用日志模块采集和记录了系统间所有调用的日志信息。具体来说：我们将系统(Application)在服务器上的一个具体部署称之为实例(Instance)，实例由所在服务器的 IP和实例占用的端口号唯一标识。一个实例调用另一个实例的某一服务后，调用方会记录下调用日志(如图所示)，日志中包含：调用时间(startTime)、调用方IP(consumerIp)和端口号(consumerPort)、被调用方IP(serviceIp)和端口号(servicePort)、调用的服务标识(serviceName)、成功与否(success)。系统间服务调用日志模块使用Logstash这一开源工具存储了这些日志，在调用行为结束后2秒内就能将数据保存下来。存储日志如图2所示。

[0108] 报警阈值分析模块定期对历史数据进行学习，找出每一个系统一般情境下的表现，具体实现过程如图3所示，包括以下步骤：

[0109] 1、遍历系统列表：

[0110] a)取得当前系统的所有服务列表；

[0111] b)调用Logstash接口，取最近n*t的时间范围内的该系统所有服务的累计错误数，并以t为单位分为n份，即我们获得了当前系统的n份样本，每一个样本都描述了单位时间t内错误数，如图4所示；

[0112] c)去除样本集中的异常点：

[0113] i.计算当前样本集的均值$u=\sum_{i=1}^{n}xi$和标准差$std=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi-u)^2}$；

[0114] ii.找到样本集中所有大于u+3*std的样本点、计算其个数n1，并将这些数据从样本集中去除，计算取出上述样本点后的新样本集的个数n2，本步骤是将历史上的异常情况找出并剔除，避免其影响到对系统一般表现的评估；

[0115] iii.如果n1＝0或者(n-n2)>30或者(n-n2)>n/3，则完成异常点的去除，继续执行步骤d)；否则，执行步骤i；

[0116] d)计算新样本集的均值u和标准差std；

[0117] 计算该系统的错误数告警线alertNum＝u+std*3；如果alertNum<100则alertNum设置为 100。

[0118] 告警分析模块定时采集(例如每分钟采集一次，采集间隔可根据需要调整)最近一个t时间段内的日志，逐次分析每个系统的错误数是否异常、每个系统的每个服务错误率是否异常、实例错误率是否异常、任意两个系统间的错误数情况，具体方法如下：

[0119] 1、从Logstash中抽取最近t时间的日志，即穷举出所有存在的a实例调用b实例c服务成功数、失败数这样的关系，如图5所示，将其记作data：

[0120] 2、整理data，将字段consumerIp和字段consumerPort合并成字段clientInstance,将字段 serviceIp和字段servicePort合并成字段serverInstance；

[0121] 3、整理数据，计算每一个serverInstance和每一个serviceName的累计正确数、累计错误数；

[0122] 4、遍历系统列表：

[0123] a)统计每一个系统的累计错误数，即该系统下所有服务的错误数之和；

[0124] b)如果该系统的累计错误数大于该系统的告警阈值alertNum，则标记该系统异常；

[0125] c)遍历该系统的每一个服务(serviceName)，应用前述异常判断方法，代入serviceName的累计正确数、累计错误数，以判定其是否异常；

[0126] d)遍历该系统的每一个实例(serverInstance)，应用前述异常判断方法，代入serverInstance的累计正确数、累计错误数，以判定其是否异常；

[0127] 5、整理数据，计算每一组clientInstance调用serverInstance的错误数；

[0128] 从系统拓扑图上反查clientInstance和serverInstance对应的系统client和server，统计每一组client系统调用server系统的累计错误数。

[0129] 告警展示模块基于系统拓扑图，在告警数据分析完成后将其展示在系统拓扑图上。

[0130] 1、当系统异常时，在系统图标上添加警告的标志，如图6所示；

[0131] 2、当系统的服务、实例异常时，点击系统图标，弹层显示错误信息，如图7所示；

[0132] 3、当系统间调用错误数不为0时，绘制连线和指向性箭头，线的宽度为错误数的对数。也可采用其他代入错误数的常规公式来计算线的宽度，只要令线的宽度或者颜色与错误数相关即可满足本发明要求。

[0133] 当系统出现故障时，我们可以很容易的从图上看出：哪些系统出现了问题、影响到了哪些系统、系统的哪些实例和服务出现了问题。

[0134] 本发明还提供了基于统计方法监控系统可用性的方法，包括系统间服务调用日志步骤；报警阈值分析步骤；告警分析步骤；监控告警展示步骤；系统间服务调用日志步骤执行系统间服务调用日志模块实现的内容，报警阈值分析步骤执行报警阈值分析模块实现的内容，告警分析步骤执行告警分析模块实现的内容，监控告警展示步骤执行监控告警展示模块实现的内容。

[0135] 本发明方案所公开的技术手段不仅限于上述实施方式所公开的技术手段，还包括由以上技术特征任意组合所组成的技术方案。应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明的保护范围。

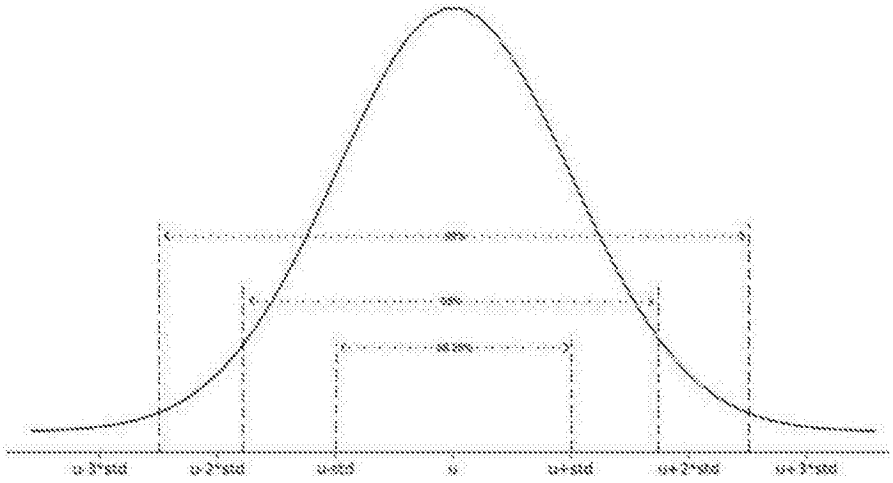


图1

serviceName: ZRB.ProductDatePrice.ProductDatePriceController.update srcServiceName: PRD.NM.ProductHotelController.refreshProductDatePrice msgType: 2 serviceMap: /zrb-web/productdateprice/update startTime: February 12th 2018, 18:16:06.000 success: true timeTaken: 7 agent: PRD.NM serviceIp: 10.40.50.18 servicePort: 12,901 consumerIp: 10.40.50.53 consumerPort: 11,401 statusCode: 0 callTimes: 0

图2

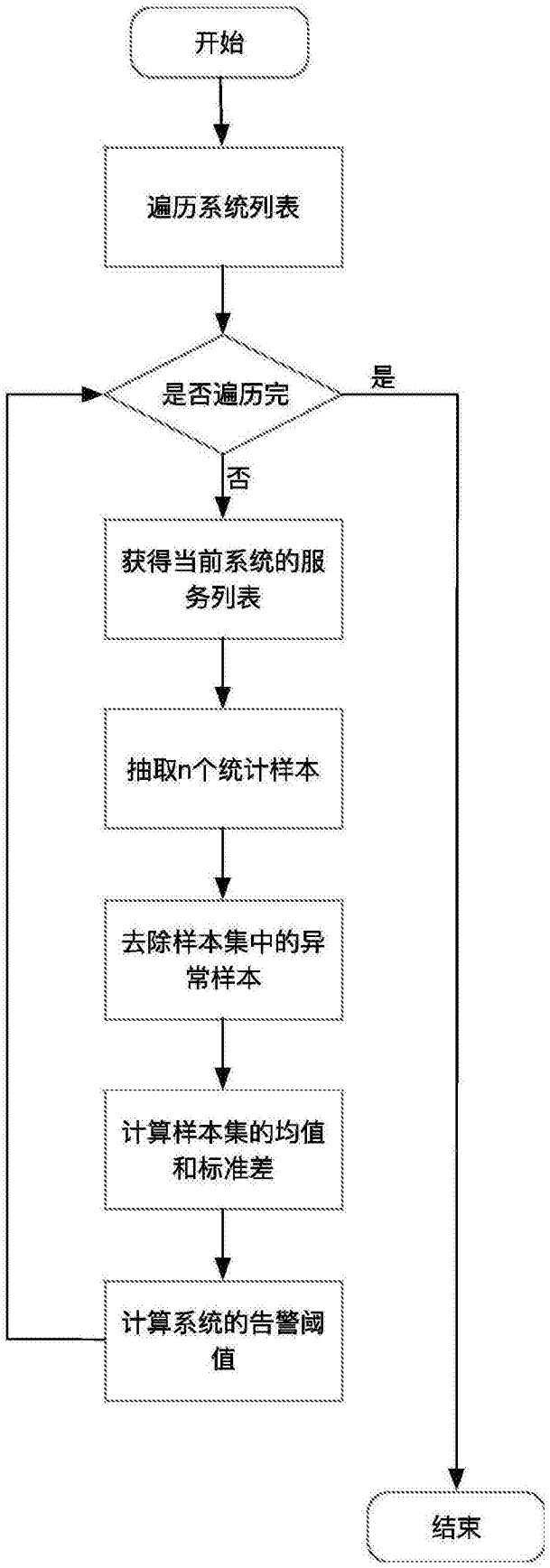

开始
遍历系统列表
是否遍历完
是
否
获得当前系统的服务列表
抽取n个统计样本
去除样本集中的异常样本
计算样本集的均值和标准差
计算系统的告警阈值
结束

图3

startTime per 15 minutes	Count
September 6th 2017, 23:45:00.000	2
September 7th 2017, 00:00:00.000	237
September 7th 2017, 00:15:00.000	203
September 7th 2017, 00:30:00.000	155
September 7th 2017, 00:45:00.000	168
September 7th 2017, 01:00:00.000	75
September 7th 2017, 01:15:00.000	91
September 7th 2017, 01:30:00.000	68
September 7th 2017, 01:45:00.000	45
September 7th 2017, 02:00:00.000	41

图4

Top 5 consumerIp	Top 5 consumerPort	Top 5 serviceIp	Top 5 servicePort	Top 5 serviceName	Top 5 success	Count
10.40.190.205	11,400	10.40.50.17	12,001	[illegible]	T	15,445
10.40.190.205	11,400	10.40.50.17	12,001	[illegible]	T	15,277
10.40.190.205	11,400	10.40.50.17	12,001	[illegible]	T	112
10.40.190.205	11,400	10.40.50.17	12,001	[illegible]	T	30
10.40.190.205	11,400	10.40.50.17	12,001	[illegible]	T	27
10.40.190.205	11,400	10.40.50.17	12,004	[illegible]	T	15,485
10.40.190.205	11,400	10.40.50.17	12,004	[illegible]	T	15,232
10.40.190.205	11,400	10.40.50.17	12,004	[illegible]	T	111
10.40.190.205	11,400	10.40.50.17	12,004	[illegible]	T	36
10.40.190.205	11,400	10.40.50.17	12,004	[illegible]	T	31

图5

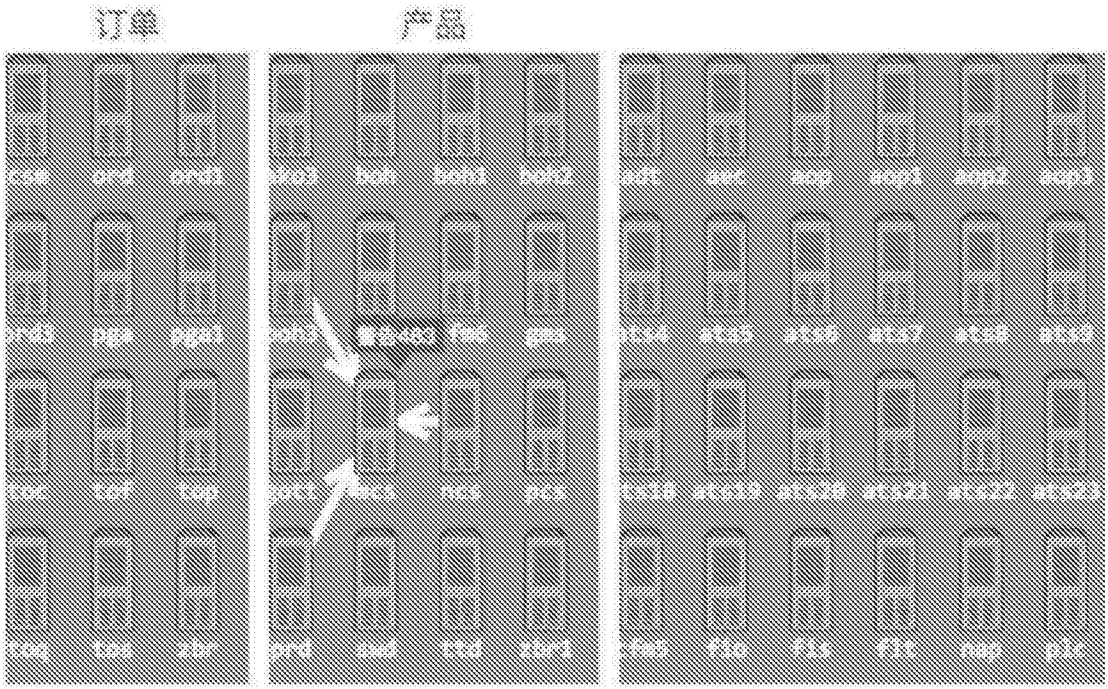


图6

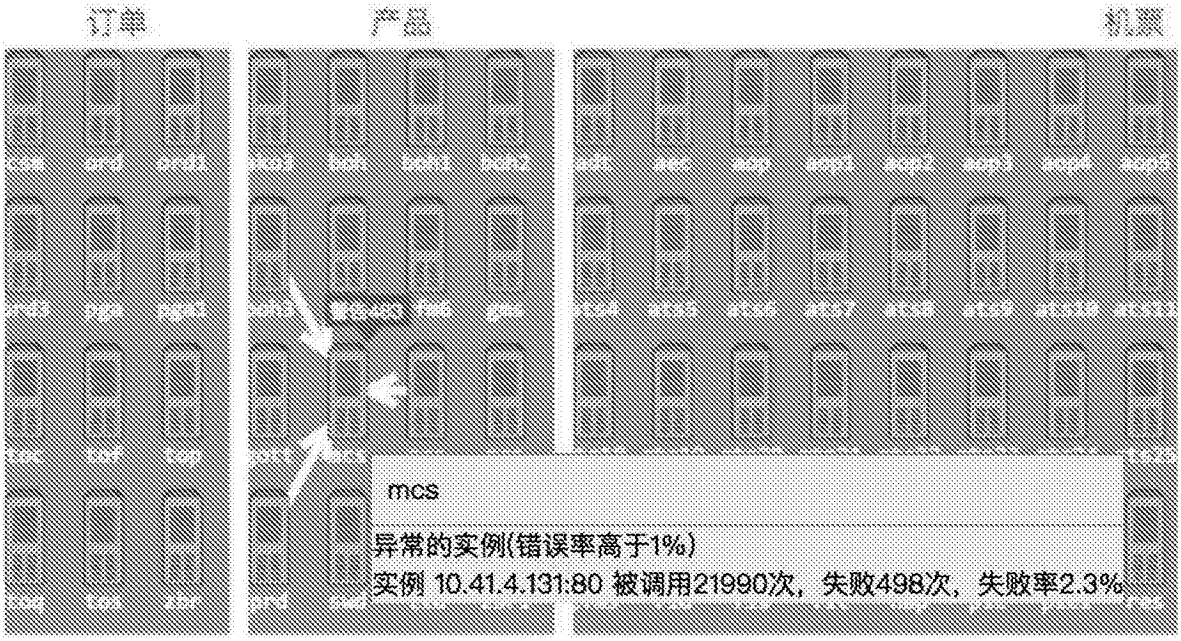

订单
产品
机票
mcs
异常的实例(错误率高于1%)
实例 10.41.4.131:80 被调用21990次，失败498次，失败率2.3%

图7