

(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 103365871 A

(43) 申请公布日 2013.10.23

(21) 申请号 201210088324.6

(22) 申请日 2012.03.29

(71) 申请人 北京恒安永通科技有限公司

地址 100061 北京市崇文区夕照寺中街 4 号
A 座 610 室

(72)发明人 包培文

(74) 专利代理机构 北京市盛峰律师事务所

11337

代理人 赵建刚

(51) Int. C1

G06E 17/30 (2006-01)

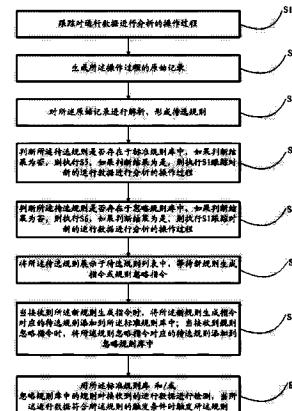
权利要求书1页 说明书4页 附图1页

(54) 发明名称

一种规则自动生成的方法

(57) 摘要

本发明提供了一种规则自动生成的方法，本发明通过跟踪用户对实际运行数据分析的操作过程自动构造规则，用户可根据分析结果决定是否添加新规则。本发明还能根据规则的应用情况提出新规则推荐和调整规则优先级，使用户可以在实际运行数据的基础上构建和维护规则，提高规则的实用性和准确性。应用本发明后，用户无需了解和学习与管理目标无关的编程、接口，就能轻易建立适合自己特定信息系统环境、持续适应系统各种变化的规则库。应用本发明后，使得建立规则更容易、效率更高。



1. 一种规则自动生成的方法,其特征在于包括以下步骤:

S1,跟踪对运行数据进行分析的操作过程;

S2,生成所述操作过程的原始记录;

S3,对所述原始记录进行解析,形成待选规则;

S4,判断所述待选规则是否存在与标准规则库中,如果判断结果为否,则执行 S5;如果判断结果为是,则执行 S1 跟踪对新的运行数据进行分析的操作过程;

S5,判断所述待选规则是否存在与忽略规则库中,如果判断结果为否,则执行 S6;如果判断结果为是,则执行 S1 跟踪对新的运行数据进行分析的操作过程;

S6,将所述待选规则展示于待选规则列表中,等待新规则生成指令或规则忽略指令;

S7,当接收到所述新规则生成指令时,将所述新规则生成指令对应的待选规则添加到所述标准规则库中;当接收到规则忽略指令时,将所述规则忽略指令对应的待选规则添加到忽略规则库中。

2. 根据权利要求 1 所述的规则自动生成的方法,其特征在于,S1 具体为,获取管理目标所对应的运行数据,将所述运行数据展示于运行数据列表中并等待分析触发,当所述运行数据列表中的运行数据被触发时,跟踪所述触发的操作过程。

3. 根据权利要求 2 所述的规则自动生成的方法,其特征在于,所述管理目标包括以下类型中的一种或几种:

文件、数据库、网页、流、数据包、数据流。

4. 根据权利要求 3 所述的规则自动生成的方法,其特征在于,一个以上所述管理目标组成管理目标集。

5. 根据权利要求 1 所述的规则自动生成的方法,其特征在于,S3 具体为,解析出所述原始记录中所包含的运行数据的逻辑关系和取值范围,生成待选规则。

6. 根据权利要求 1 所述的规则自动生成的方法,其特征在于,步骤 S7 后还包括步骤:

S8,用所述标准规则库和 / 或忽略规则库中的规则对接收到的运行数据进行检测,当所述运行数据符合所述规则的触发条件时触发所述规则。

7. 根据权利要求 6 所述的规则自动生成的方法,其特征在于,所述标准规则库中的规则按一定策略排序后对所述运行数据进行检测。

8. 根据权利要求 7 所述的规则自动生成的方法,其特征在于,所述策略为优先级策略,优先级高者排序在前。

9. 根据权利要求 8 所述的规则自动生成的方法,其特征在于,根据同一所述规则被触发的次数调整所述规则的优先级,被触发次数越多,优先级越高。

一种规则自动生成的方法

技术领域

[0001] 本发明涉及信息系统中规则的自动生成及维护领域,尤其涉及一种规则自动生成的方法。

背景技术

[0002] 目前大量信息系统的安全管理、监控管理等都需要设置各种规则来对检测到的实际运行情况进行报警或处理,它们一般采用以下方法的一种或几种。

[0003] 1. 规则库方法 :

[0004] 在产品中提供预先设定的规则库,由用户进行勾选使其生效或失效。规则库由产品提供者进行研发并提供。

[0005] 该技术一般由软件产品厂商在自己的研发中心使用并形成规则库,用户无法修改,只能选择。由于实际应用环境的复杂性和快速变化,这种方法已很难适用。

[0006] 2. 编程方法 :

[0007] 向用户提供编程接口或规则编程语言,由用户自己通过编程实现规则。

[0008] 该技术一般是构建一个规则引擎并提供一套编程方法,使用户能够自行编程来构造规则,由规则引擎进行解释并执行。该方法虽然提供了很高的灵活性和适应性,但用户需要为此学习一门独特的编程语言以及规则引擎的接口方法,对用户的要求极高,只能在少数具备条件的单位使用。

[0009] 3. 图形化选择 - 设置方法 :

[0010] 该技术提供规则引擎和规则设置的图形界面,供用户选择字段和条件表达式等来构造规则。这种方法避免了编程等方法的复杂性,同时又能提供一定程度的灵活性,但要求用户详细了解数据字段的含义,条件选择的含义以及相关的逻辑,因此用户使用时需要深度培训。另外,用户设置时选择哪些字段和条件缺乏依据,导致设置时的随意性和盲目性,实际使用效果有限。

发明内容

[0011] 为解决上述现有技术中存在的问题和缺点,本发明提供了一种规则自动生成的方法,本发明通过跟踪用户对实际运行数据分析的操作过程自动构造规则,用户可根据分析结果决定是否添加新规则。本发明还能根据规则的应用情况提出新规则推荐和调整规则优先级,使用户可以在实际运行数据的基础上构建和维护规则,提高规则的实用性和准确性。

[0012] 本发明提供的规则自动生成的方法包括以下步骤 :

[0013] S1, 跟踪对运行数据进行分析的操作过程 ;

[0014] S2, 生成所述操作过程的原始记录 ;

[0015] S3, 对所述原始记录进行解析,形成待选规则 ;

[0016] S4, 判断所述待选规则是否存在与标准规则库中,如果判断结果为否,则执行 S5 ;如果判断结果为是,则执行 S1 跟踪对新的运行数据进行分析的操作过程 ;

[0017] S5, 判断所述待选规则是否存在于忽略规则库中, 如果判断结果为否, 则执行 S6 ; 如果判断结果为是, 则执行 S1 跟踪对新的运行数据进行分析的操作过程 ;

[0018] S6, 将所述待选规则展示于待选规则列表中, 等待新规则生成指令或规则忽略指令 ;

[0019] S7, 当接收到所述新规则生成指令时, 将所述新规则生成指令对应的待选规则添加到所述标准规则库中 ; 当接收到规则忽略指令时, 将所述规则忽略指令对应的待选规则添加到忽略规则库中。

[0020] 优选的, S1 具体为, 获取管理目标所对应的运行数据, 将所述运行数据展示于运行数据列表中并等待分析触发, 当所述运行数据列表中的运行数据被触发时, 跟踪所述触发的操作过程。

[0021] 优选的, 所述管理目标包括以下类型中的一种或几种 :

[0022] 文件、数据库、网页、流、数据包、数据流。

[0023] 优选的, 一个以上所述管理目标组成管理目标集。

[0024] 优选的, S3 具体为, 解析出所述原始记录中所包含的运行数据的逻辑关系和取值范围, 生成待选规则。

[0025] 优选的, 步骤 S7 后还包括以下步骤 :

[0026] S8, 用所述标准规则库和 / 或忽略规则库中的规则对接收到的运行数据进行检测, 当所述运行数据符合所述规则的触发条件时触发所述规则。

[0027] 优选的, 所述标准规则库中的规则按一定策略排序后对所述运行数据进行检测。

[0028] 优选的, 所述策略为优先级策略, 优先级高者排序在前。

[0029] 优选的, 根据同一所述规则被触发的次数调整所述规则的优先级, 被触发次数越多, 优先级越高。

[0030] 本发明实现的有益效果是 :

[0031] 应用本发明后, 用户无需了解和学习与管理目标无关的编程、接口, 就能轻易建立适合自己特定信息系统环境、持续适应系统各种变化的规则库。

[0032] 本发明可广泛应用于信息系统的监控报警、安全管理、行为审计、合规管理等各个方面, 并具备以下好处 :

[0033] 1. 用户无需花费大量时间和精力学习一门新的编程语言或者数据接口、定义等。

[0034] 2. 用户分析问题的同时就完成了规则的构造, 使建立规则更容易、效率更高。

[0035] 3. 用户能够直观获得规则应用的效果, 更容易决定是否添加规则。

[0036] 4. 能迅速适应用户信息系统的各种变化, 包括管理目标的变化、运行环境的变化和数据来源的变化, 大大提高规则系统的实用性。

[0037] 5. 可以动态优化规则应用的优先级, 加快响应速度。

附图说明

[0038] 图 1 是本发明的规则自动生成的方法的步骤流程图。

具体实施方式

[0039] 实施本发明提供的规则自动生成的方法包括以下步骤 :

[0040] S1, 跟踪对运行数据进行分析的操作过程 ; 具体为, 获取管理目标所对应的运行数据, 将所述运行数据展示于运行数据列表中并等待分析触发, 当所述运行数据列表中的运行数据被触发时, 跟踪所述触发的操作过程 ; 所述管理目标包括文件、数据库、网页、流、数据包和数据流等各种形式的运行数据中的一种或几种 ; 将一个以上所述管理目标组成管理目标集 ;

[0041] S2, 生成所述操作过程的原始记录 ;

[0042] S3, 对所述原始记录进行解析, 形成待选规则 ; 具体为, 解析出所述原始记录中所包含的运行数据的逻辑关系和取值范围, 生成待选规则 ;

[0043] S4, 判断所述待选规则是否存在于标准规则库中, 如果判断结果为否, 则执行 S5 ; 如果判断结果为是, 则执行 S1 跟踪对新的运行数据进行分析的操作过程 ;

[0044] S5, 判断所述待选规则是否存在于忽略规则库中, 如果判断结果为否, 则执行 S6 ; 如果判断结果为是, 则执行 S1 跟踪对新的运行数据进行分析的操作过程 ;

[0045] S6, 将所述待选规则展示于待选规则列表中, 等待新规则生成指令或规则忽略指令 ;

[0046] S7, 当接收到所述新规则生成指令时, 将所述新规则生成指令对应的待选规则添加到所述标准规则库中 ; 当接收到规则忽略指令时, 将所述规则忽略指令对应的待选规则添加到忽略规则库中 ;

[0047] S8, 用所述标准规则库和 / 或忽略规则库中的规则对接收到的运行数据进行检测, 当所述运行数据符合所述规则的触发条件时触发所述规则。

[0048] 所述标准规则库中的规则按一定策略排序后对所述运行数据进行检测。所述策略为优先级策略, 优先级高者排序在前。根据同一所述规则被触发的次数调整所述规则的优先级, 被触发次数越多, 优先级越高。

[0049] 下面具体举例说明本发明的具体实施方式 :

[0050] 以防火墙工作状态监控系统为例, 目的是监控防火墙的 CPU 占用率, 当防火墙设备的 CPU 占用率异常后则报警。防火墙设备的 CPU 占用率即是管理目标, 该管理目标包含在防火墙管理目标集中 ; 防火墙设备上的 CPU 占用率通过 SNMP 接口实时将防火墙 CPU 占用率数据传输给数据源接口, 数据源接口接收到 CPU 占用率数据后实时将其展示在运行数据列表中。数据列表提供了 CPU 占用率按时间分布的数值列表和操作菜单, 包括“只看大于”、“只看小于”、“只看区间”、“只看等于”、“只看大于或等于”、“只看小于或等于”、“排除本数值”等。当某条数据所显示的 CPU 占用率达到 60% 时, 用户对此条数据进行选择“只看大于或等于”, 在结果集中触发并指令系统发出了报警信号, 此时分析跟踪引擎则对此分析操作、触发操作和指令操作进行记录, 生成了此操作过程的原始记录, 同时分析跟踪引擎对此原始记录进行解析, 解析出其中包含的逻辑关系和数值范围为防火墙 CPU 占用率大于或等于 60% 则报警, 随即生成了此条规则, 但此条规则尚未得到用户确认所以此条规则为待选规则 ; 将此待选规则与预设的标准规则库中的规则进行比较, 看此待选规则是否已存在于所述的标准规则库中, 如果此待选规则在所述标准规则库中不存在, 则判断所述待选规则是否存在预设的忽略规则库中, 如果此待选规则在所述标准规则库中存在则返回到对操作过程进行跟踪的步骤, 继续对分析操作过程进行跟踪, 同时由规则应用引擎应用此规则即报警 ; 当判断所述待选规则是否存在预设的忽略规则库中时, 如果此待选规则在所述

忽略规则库中不存在，则将所述待选规则展示于待选规则列表中，等待新规则生成指令或规则忽略指令；如果此待选规则在所述忽略规则库中存在，则返回到对操作过程进行跟踪的步骤，继续对分析操作过程进行跟踪；

[0051] 当所述待选规则列表中的选定待选规则接收到新规则生成指令时，则将所述新规则生成指令对应的待选规则添加到所述标准规则库中；当所述待选规则列表中的选定待选规则接收到规则忽略指令时，则将所述规则忽略指令对应的待选规则添加到忽略规则库中；本例中对“防火墙 CPU 占用率大于或等于 60% 则报警”这条规则发出了新规则生成指令，则将“防火墙 CPU 占用率大于或等于 60% 则报警”这条规则添加到了所述标准规则库中。

[0052] 那么至此标准规则库中就存在一条“防火墙 CPU 占用率大于或等于 60% 则报警”的规则了，此条规则的初始优先级为零；当所述数据源接口接收到新的防火墙 CPU 占用率数据时则由规则应用引擎将该条规则应用于所述数据源接口接收到的 CPU 占用率数据中，即用“防火墙 CPU 占用率大于或等于 60% 则报警”这条规则对所述 CPU 占用率数据进行检测，当所述 CPU 占用率数据中的 CPU 占用率值大于或等于 60% 时则触发报警，同时提高该规则的优先级。

[0053] 以上所述仅是本发明的优选实施方式，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，这些改进和润饰也应视本发明的保护范围。

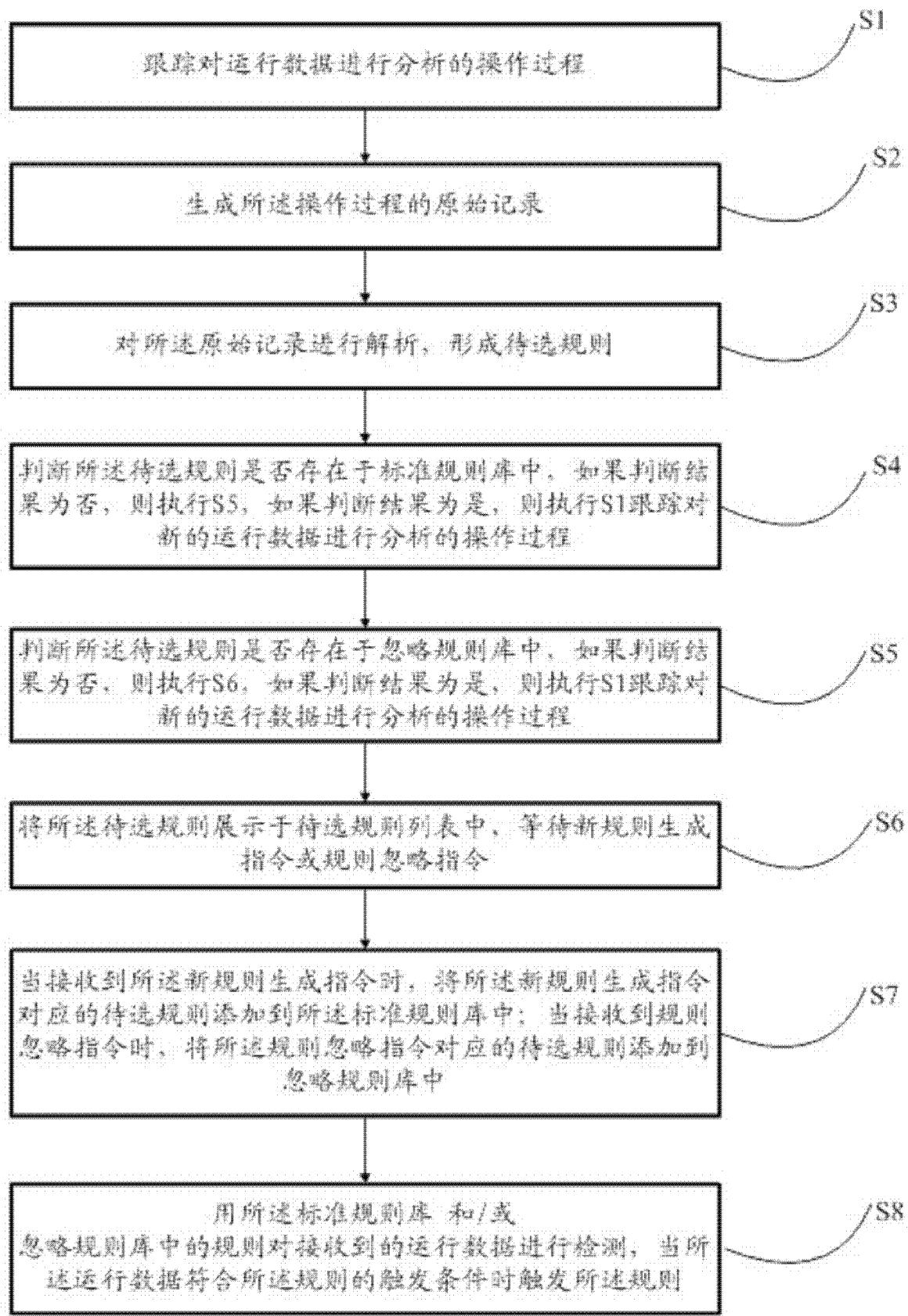


图 1