(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 112882920 B
(45)授权公告日 2021.06.29

(21)申请号 202110470624.X

(22)申请日 2021.04.29

(65)同一申请的已公布的文献号
申请公布号 CN 112882920 A

(43)申请公布日 2021.06.01

(73)专利权人 云账户技术(天津)有限公司
地址 300384 天津市滨海新区滨海高新区华苑产业园区工华道2号天百中心1号楼6层、21至22层

(72)发明人 马瑞宽 杨宜 邹永强 杨晖

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静 胡影

(51)Int.Cl.
G06F 11/34(2006.01)
G06F 11/32(2006.01)
G06F 11/30(2006.01)
G06F 9/54(2006.01)

(56)对比文件
CN 112055336 A,2020.12.08
CN 103513983 A,2014.01.15
CN 104866410 A,2015.08.26
CN 108833383 A,2018.11.16
US 2019205191 A1,2019.07.04
CN 105183625 A,2015.12.23
CN 109542737 A,2019.03.29
CN 106649123 A,2017.05.10
洪权 等."湖南电网云上综合智能告警功能实现与分析".《湖南电力》.2021,第41卷(第1期),全文.
Wei Han 等."Research on Alert Strategy of Unmanned surface Vessel Based on Typical Missions".《2019 3rd International Symposium on Autonomous Systems》.2019,全文.

审查员 彭巧君

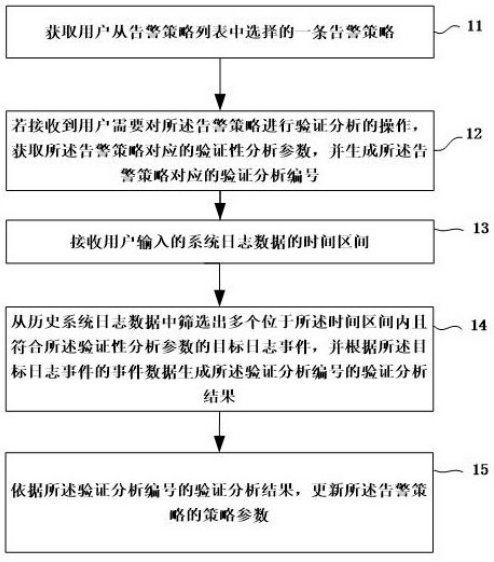
权利要求书2页 说明书9页 附图4页

(54)发明名称

告警策略验证方法、装置、电子设备和可读存储介质

(57)摘要

本发明提供一种告警策略验证方法、装置、电子设备和可读存储介质，涉及计算机技术领域。该方法包括：获取一条告警策略；若接收到用户需要对告警策略进行验证分析的操作，获取告警策略对应的验证性分析参数，并生成告警策略对应的验证分析编号；接收用户输入的系统日志数据的时间区间；从历史系统日志数据中筛选出多个位于时间区间内且符合验证性分析参数的目标日志事件，并根据目标日志事件的事件数据生成验证分析编号的验证分析结果；依据验证分析编号的验证分析结果，更新告警策略的策略参数。利用历史系统日志数据对告警策略的配置参数进行前置性验证分析，取得了在告警策略启用之前完成对策略的合理化配置和优化的技术效果。



CN 112882920 B

1.一种告警策略验证方法,其特征在于,包括:

获取用户从告警策略列表中选择的一条告警策略;

若接收到用户需要对所述告警策略进行验证分析的操作,获取所述告警策略对应的验证性分析参数,并生成所述告警策略对应的验证分析编号;

接收用户输入的系统日志数据的时间区间;

从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件,并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果;

依据所述验证分析编号的验证分析结果,更新所述告警策略的策略参数。

2.根据权利要求1所述的告警策略验证方法,其特征在于,所述告警策略每进行一次验证分析对应一个验证分析编号;所述方法还包括:

当一个告警策略对应多个验证分析编号时,接收用户输入的第一操作,基于所述第一操作显示所述多个验证分析编号对应的验证分析结果的比对界面,以反映所述告警策略的策略参数修改前后所述告警策略的优化情况。

3.根据权利要求1所述的告警策略验证方法,其特征在于,所述从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件,包括:

将历史系统日志数据中的位于所述时间区间内且符合所述验证性分析参数的第一条目标日志事件写入至图形数据列表中;

遍历所述历史系统日志数据,持续向所述图形数据列表中写入位于所述时间区间内且符合所述验证性分析参数的目标日志事件,直至所述图形数据列表中最后一个目标日志事件的写入时间大于所述时间区间的终止时间;

显示所述图形数据列表。

4.根据权利要求1所述的告警策略验证方法,其特征在于,所述目标日志事件的事件数据至少包括所述目标日志事件发生时间和所述目标日志事件数量的键值对。

5.根据权利要求1所述的告警策略验证方法,其特征在于,若更新所述告警策略的策略参数之前,所述告警策略被删除,所述方法还包括:

依据当前的验证分析编号的验证分析结果新增一条告警策略。

6.根据权利要求1所述的告警策略验证方法,其特征在于,所述验证性分析参数包括所述告警策略的策略参数时,若所述告警策略的策略参数有修改,所述获取所述告警策略对应的验证性分析参数包括:

将更新后的所述策略参数更新至所述验证性分析参数中。

7.根据权利要求4所述的告警策略验证方法,其特征在于,所述目标日志事件的事件数据还包括所述目标日志事件的事件类型时,所述验证分析编号的验证分析结果包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表和按不同次数的历史事件统计的操作频次列表中的至少之一。

8.一种告警策略验证装置,其特征在于,包括:

获取模块,用于获取用户从告警策略列表中选择的一条告警策略;

所述获取模块还用于若接收到用户需要对所述告警策略进行验证分析的操作,获取所述告警策略对应的验证性分析参数,并生成所述告警策略对应的验证分析编号;

接收模块，用于接收用户输入的系统日志数据的时间区间；

执行模块，用于从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果；

更新模块，用于依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数。

9.一种电子设备，其特征在于，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求1至7中任一项所述的告警策略验证方法的步骤。

10.一种可读存储介质，其特征在于，所述可读存储介质上存储有程序，所述程序被处理器执行时实现如权利要求1至7中任一项所述的告警策略验证方法的步骤。

告警策略验证方法、装置、电子设备和可读存储介质

技术领域

[0001] 本发明实施例涉及计算机技术领域，尤其涉及一种告警策略验证方法、装置、电子设备和可读存储介质。

背景技术

[0002] 告警事件管理是日志审计系统中的一个重要模块，可以实现基于系统日志数据对敏感事件进行告警以便及时处理告警事件和规避更大的风险。在告警事件管理中，告警策略配置是一个前提，告警策略配置的是否合适，直接影响到后续告警事件的健康度。

[0003] 现有技术中，通常是用户通过自己对业务的了解进行告警策略的参数配置，参数配置的合理性往往强依赖于配置人员的业务熟悉程度和配置的经验值，配置经验要求高，系统使用的局限性大；不合理的配置容易造成无效的告警事件，从而带来了较高的人工判读成本；不合理的配置容易造成告警事件的遗漏或者冗余，从而无法高效的达成告警提示的目标；现有技术提供的根据具体告警事件反向调整告警策略的方案，在实际应用中的时效性较差。

发明内容

[0004] 本发明实施例提供一种告警策略验证方法、装置、电子设备和可读存储介质，以解决现有技术中告警策略强依赖于配置经验且人工判读成本高、告警提示效率低且策略调优时效性差的问题。

[0005] 为了解决上述技术问题，本发明是这样实现的：

[0006] 第一方面，本发明实施例提供了一种告警策略验证方法，包括：

[0007] 获取用户从告警策略列表中选择的一条告警策略；

[0008] 若接收到用户需要对所述告警策略进行验证分析的操作，获取所述告警策略对应的验证性分析参数，并生成所述告警策略对应的验证分析编号；

[0009] 接收用户输入的系统日志数据的时间区间；

[0010] 从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果；

[0011] 依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数。

[0012] 可选的，所述告警策略每进行一次验证分析对应一个验证分析编号；所述方法还包括：

[0013] 当一个告警策略对应多个验证分析编号时，接收用户输入的第一操作，基于所述第一操作显示所述多个验证分析编号对应的验证分析结果的比对界面，以反映所述告警策略的策略参数修改前后所述告警策略的优化情况。

[0014] 可选的，所述从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，包括：

[0015] 将历史系统日志数据中的位于所述时间区间内且符合所述验证性分析参数的第一条目标日志事件写入至图形数据列表中；

[0016] 遍历所述历史系统日志数据，持续向所述图形数据列表中写入位于所述时间区间内且符合所述验证性分析参数的目标日志事件，直至所述图形数据列表中最后一个目标日志事件的写入时间大于所述时间区间的终止时间；

[0017] 显示所述图形数据列表。

[0018] 可选的，所述目标日志事件的事件数据至少包括所述目标日志事件发生时间和所述目标日志事件数量的键值对。

[0019] 可选的，若更新所述告警策略的策略参数之前，所述告警策略被删除，所述方法还包括：

[0020] 依据当前的验证分析编号的验证分析结果新增一条告警策略。

[0021] 可选的，所述验证性分析参数包括所述告警策略的策略参数时，若所述告警策略的策略参数有修改，所述获取所述告警策略对应的验证性分析参数包括：

[0022] 将更新后的所述策略参数更新至所述验证性分析参数中。

[0023] 可选的，所述目标日志事件的事件数据还包括所述目标日志事件的事件类型时，所述验证分析编号的验证分析结果包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表和按不同次数的历史事件统计的操作频次列表中的至少之一。

[0024] 第二方面，本发明实施例还提供了一种告警策略验证装置，包括：

[0025] 获取模块，用于获取用户从告警策略列表中选择的一条告警策略；

[0026] 所述获取模块还用于若接收到用户需要对所述告警策略进行验证分析的操作，获取所述告警策略对应的验证性分析参数，并生成所述告警策略对应的验证分析编号；

[0027] 接收模块，用于接收用户输入的系统日志数据的时间区间；

[0028] 执行模块，用于从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果；

[0029] 更新模块，用于依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数。

[0030] 第三方面，本发明实施例还提供了一种电子设备，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如第一方面任一项所述的告警策略验证方法的步骤。

[0031] 第四方面，本发明实施例还提供了一种可读存储介质，所述可读存储介质上存储有程序，所述程序被处理器执行时实现如第一方面任一项所述的告警策略验证方法的步骤。

[0032] 本发明中，利用历史系统日志数据对日志告警策略的配置参数进行前置性验证分析的技术手段，使得在告警策略启用之前就完成对策略的合理化配置和优化，大大节省了人力成本，同时规避了因配置不合理造成的告警事件遗漏和冗余风险，提高了日志审计系统中告警事件管理的易用性、时效性和实用性。本发明的告警策略验证方法适用于一般业务人员，通用性强；基于历史样本数据验证当前告警策略配置参数的合理性和针对性，最终一键化更新最合理的配置参数，从而保证了基于该告警策略触发的告警事件的健康度和实

用性的最大化。

附图说明

[0033] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0034] 图1为本发明实施例提供的告警策略验证方法的流程示意图之一；

[0035] 图2为本发明实施例提供的告警策略验证方法的流程示意图之二；

[0036] 图3为本发明实施例提供的告警策略验证装置的结构示意图之一；

[0037] 图4为本发明实施例提供的电子设备的结构示意图之一。

具体实施方式

[0038] 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清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0039] 请参考图1，图1为本发明实施例提供的告警策略验证方法的流程示意图之一；该告警策略验证方法包括：

[0040] 步骤11：获取用户从告警策略列表中选择的一条告警策略；

[0041] 步骤12：若接收到用户需要对所述告警策略进行验证分析的操作，获取所述告警策略对应的验证性分析参数，并生成所述告警策略对应的验证分析编号；

[0042] 步骤13：接收用户输入的系统日志数据的时间区间；

[0043] 步骤14：从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果；

[0044] 步骤15：依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数。

[0045] 本发明中，利用历史系统日志数据对日志告警策略的配置参数进行前置性验证分析的技术手段，使得在告警策略启用之前就完成对策略的合理化配置和优化，大大节省了人力成本，同时规避了因配置不合理造成的告警事件遗漏和冗余风险，提高了日志审计系统中告警事件管理的易用性、时效性和实用性。本发明的告警策略验证方法适用于一般业务人员，通用性强；基于历史样本数据验证当前告警策略配置参数的合理性和针对性，最终一键化更新最合理的配置参数，从而保证了基于该告警策略触发的告警事件的健康度和实用性的最大化。

[0046] 本发明的一些实施例中，可选的，所述本次验证分析编号的分析结果采用图表形式显示。

[0047] 本发明的一些实施例中，可选的，所述告警策略每进行一次验证分析时对应一个验证分析编号；所述方法还包括：

[0048] 当一个告警策略对应多个验证分析编号时，接收用户输入的第一操作，基于所述第一操作显示所述多个验证分析编号对应的验证分析结果的比对界面，以反映所述告警策

略的策略参数修改前后所述告警策略的优化情况。

[0049] 本发明的一些实施例中，可选的，用户通过比对界面综合对比分析各验证分析编号对应的验证分析结果，获取符合预设收敛效果的验证分析编号。

[0050] 本发明实施例中，告警策略验证方法基于历史样本数据验证当前告警策略配置参数的合理性和针对性，一个告警策略可对应多个验证分析编号，每一次验证分析实现对告警策略参数的调整，用户可通过操作多个验证分析编号对应的验证分析结果的比对界面，支持对各类配置参数进行调整和对比分析，查看告警策略的策略参数修改前后所述告警策略的优化情况，逐步调整目标策略参数实现告警策略效果的最终优化。

[0051] 在本发明的一些实施例中，可选的，当一个告警策略对应多个验证分析编号时，通过异步启动多个验证性分析任务同时进行验证分析。

[0052] 本发明的一些实施例中，可选的，所述从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，包括：

[0053] 将历史系统日志数据中的位于所述时间区间内且符合所述验证性分析参数的第一条目标日志事件写入至图形数据列表中；

[0054] 遍历所述历史系统日志数据，持续向所述图形数据列表中写入位于所述时间区间内且符合所述验证性分析参数的目标日志事件，直至所述图形数据列表中最后一个目标日志事件的写入时间大于所述时间区间的终止时间；

[0055] 显示所述图形数据列表。

[0056] 本发明实施例中，目标日志事件通过历史系统日志数据、验证性分析参数和时间区间进行筛选，得到目标日志事件的图形数据列表，直观展示了告警策略验证分析过程和验证分析结果，方便用户依据验证分析结果进行告警策略的参数修改，减少了对操作人员经验的依赖问题；基于历史目标日志事件进行验证减少了无效告警事件的数量，同时解决了对无效告警进行大量人工判读的问题；依据历史数据预先验证并调整策略参数也解决了必须通过告警事件反向调整告警策略造成的时效性问题。

[0057] 具体地，请参见图2，图2为本发明实施例提供的告警策略验证方法的流程示意图之二，根据验证分析编号，启动验证性分析任务，生成目标日志事件包括：

[0058] 步骤21：声明图形数据列表list变量；

[0059] 步骤22：声明整型变量i；

[0060] 步骤23：判断当前时间对应的数据量，如果是1，代表是首次写入数据，则转入步骤241；否则转入步骤251；

[0061] 步骤241：将i赋值为0，转入步骤242；

[0062] 步骤242：向list中写入样本区间内的第一条{key:value}数据；转入步骤26；

[0063] 步骤251：当前时间对应的数据量进行自增操作，转入步骤252；

[0064] 步骤252：判断list内最后一个数据的时间与样本终止时间是否不同，是则转入步骤2531；否则转入步骤2532；

[0065] 步骤2531：向list中写入样本区间内的{key:value}数据，变量i进行自增；转入步骤26；

[0066] 步骤2532：向list内最后一个元素的value列表添加数据，写入样本区间内的{key:value}数据，变量i进行自增；转入步骤26；

[0067] 步骤26:循环遍历符合验证分析参数的历史事件数据,并转入步骤23;否则退出遍历,返回以图形化方式展示的list数据。

[0068] 本发明的一些实施例中,可选的,所述目标日志事件的事件数据至少包括所述目标日志事件发生时间和所述目标日志事件数量的键值对。

[0069] 本发明实施例中,目标日志事件的事件数据为键值对,键值对的组成依据验证性分析参数名称、历史时间属性、用户数量等相关,可依据用户实际需求进行键值对的调整。

[0070] 在本发明的一些实施例中,可选的,所述验证性分析参数包括告警名称、告警类型、查询时间区间、触发条件、触发阈值、告警白名单中的至少之一。

[0071] 在本发明的一些实施例中,可选的,所述验证分析编号的分析结果包括:历史事件总数、关联用户数量和事件触发概率中的至少之一。

[0072] 在本发明的一些实施例中,可选的,所述图形数据列表包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表或按不同次数的历史事件统计的操作频次列表中的至少之一。

[0073] 本发明的一些实施例中,可选的,若更新所述告警策略的策略参数之前,所述告警策略被删除,所述方法还包括:

[0074] 依据当前的验证分析编号的验证分析结果新增一条告警策略。

[0075] 本发明实施例中,告警策略被删除时,用户可通过依据当前的验证分析编号对应的验证性分析参数和验证分析结果新增策略数据实现告警策略的生成,灵活地保证了告警策略参数的安全性。

[0076] 在本发明的一些实施例中,可选的,所述依据所述验证分析编号的验证分析结果,更新所述告警策略的策略参数,包括:

[0077] 依据所述验证分析编号获取所述告警策略编号;

[0078] 依据所述验证分析编号获取所述验证性分析参数,依据所述告警策略编号获取所述告警策略的详细信息;

[0079] 依据所述验证性分析参数和所述告警策略的详细信息更新所述告警策略。

[0080] 具体地,验证性分析任务结束后,如果用户确认该参数配置结果,可以对该告警策略进行更新,步骤如下:首先系统获取该任务的验证性分析编号和对应的验证性分析参数;根据验证性分析编号获取对应的告警策略编号,从而获取该告警策略详情;判断当前告警策略的状态,如果该告警策略为正常状态,则对原告警策略进行更新;如果该告警策略已经被删除,则根据验证性分析结果新增一条新的告警策略。

[0081] 本发明的一些实施例中,可选的,所述验证性分析参数包括所述告警策略的策略参数时,若所述告警策略的策略参数有修改,所述获取所述告警策略对应的验证性分析参数包括:

[0082] 将更新后的所述策略参数更新至所述验证性分析参数中。

[0083] 本发明实施例中,验证性分析参数包括告警策略的策略参数时,若用户修改了策略参数,当前的验证性分析参数包括最新的策略参数,保证了当前验证分析的时效性。

[0084] 具体地,根据告警策略编号和当前的验证性分析参数,查询当前的验证分析列表中是否已存在该目标任务;

[0085] 如果存在该目标任务,则进一步判断该任务的记录状态值,即是否已经完成了验

证分析；

[0086] 如果完成了验证分析，则返回该任务的验证性分析编号和状态值，否则仅返回状态值，该输出结果对接生成验证分析结果；

[0087] 如果不存在该目标任务，则生成该任务的验证性分析编号，并插入1条验证性分析数据，对接生成验证分析结果，异步开启验证性分析任务。

[0088] 本发明的一些实施例中，可选的，所述目标日志事件的事件数据还包括所述目标日志事件的事件类型时，所述验证分析编号的验证分析结果包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表和按不同次数的历史事件统计的操作频次列表中的至少之一。

[0089] 本发明实施例中，目标日志事件的事件数据包括：目标日志事件的事件类型、目标日志事件发生时间和所述目标日志事件数量时，验证分析结果的维度可涉及按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表或按不同次数的历史事件统计的操作频次列表，用户通过上述列表直观的获取不同维度的历史事件的告警可能性进行告警策略的参数调整，减少了对操作人员经验的依赖问题，使得一般业务人员可以通过多维度的图像验证分析结果确定合理的配置参数；基于历史目标事件的筛选也减少了无效告警事件的数量，解决了对无效告警需要进行大量人工判读的问题；统计多种目标事件的事件类型解决了必须通过具体告警事件反向调整告警策略造成的时效性问题。

[0090] 本发明的一些实施例中，可选的，所述告警策略的策略参数保存在策略表中，依据每一告警策略的策略编号查询得到。

[0091] 请参考图3，图3为本发明实施例提供的告警策略验证装置的结构示意图之一；本发明实施例还提供了一种告警策略验证装置30，包括：

[0092] 获取模块31，用于获取用户从告警策略列表中选择的一条告警策略；

[0093] 所述获取模块31还用于若接收到用户需要对所述告警策略进行验证分析的操作，获取所述告警策略对应的验证性分析参数，并生成所述告警策略对应的验证分析编号；

[0094] 接收模块32，用于接收用户输入的系统日志数据的时间区间；

[0095] 执行模块33，用于从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果；

[0096] 更新模块34，用于依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数。

[0097] 本发明实施例中，告警策略验证装置利用历史系统日志数据对日志告警策略的配置参数进行前置性验证分析的技术手段，使得在告警策略启用之前就完成对策略的合理化配置和优化，大大节省了人力成本，同时规避了因配置不合理造成的告警事件遗漏和冗余风险，提高了日志审计系统中告警事件管理的易用性、时效性和实用性。本告警策略验证装置适用于一般业务人员，通用性强；基于历史样本数据验证当前告警策略配置参数的合理性和针对性，最终一键化更新最合理的配置参数，从而保证了基于该告警策略触发的告警事件的健康度和实用性的最大化。

[0098] 本发明的一些实施例中，可选的，所述本次验证分析编号的分析结果采用图表形式显示。

[0099] 本发明的一些实施例中，可选的，所述告警策略每进行一次验证分析时对应一个验证分析编号；

[0100] 当一个告警策略对应多个验证分析编号时，所述执行模块33还用于接收用户输入的第一操作，基于所述第一操作显示所述多个验证分析编号对应的验证分析结果的比对界面，以反映所述告警策略的策略参数修改前后所述告警策略的优化情况。

[0101] 本发明的一些实施例中，可选的，用户通过比对界面综合对比分析各验证分析编号对应的验证分析结果，获取满足预设收敛效果的验证分析编号。

[0102] 本发明实施例中，告警策略验证装置基于历史样本数据验证当前告警策略配置参数的合理性和针对性，一个告警策略可对应多个验证分析编号，每一次验证分析实现对告警策略参数的调整，用户可通过操作多个验证分析编号对应的验证分析结果的比对界面，支持对各类配置参数进行调整和对比分析，查看告警策略的策略参数修改前后所述告警策略的优化情况，逐步调整目标策略参数实现告警策略效果的最终优化。

[0103] 在本发明的一些实施例中，可选的，当一个告警策略对应多个验证分析编号时，通过异步启动多个验证性分析任务同时进行验证分析。

[0104] 本发明的一些实施例中，可选的，所述执行模块33还用于将历史系统日志数据中的位于所述时间区间内且符合所述验证性分析参数的第一条目标日志事件写入至图形数据列表中；遍历所述历史系统日志数据，持续向所述图形数据列表中写入位于所述时间区间内且符合所述验证性分析参数的目标日志事件，直至所述图形数据列表中最后一个目标日志事件的写入时间大于所述时间区间的终止时间；显示所述图形数据列表。

[0105] 本发明实施例中，目标日志事件通过历史系统日志数据、验证性分析参数和时间区间进行筛选，得到目标日志事件的图形数据列表，直观展示了告警策略验证分析过程和验证分析结果，方便用户依据验证分析结果进行告警策略的参数修改，减少了对操作人员经验的依赖问题；基于历史目标日志事件进行验证减少了无效告警事件的数量，同时解决了对无效告警进行大量人工判读的问题；依据历史数据预先验证并调整策略参数也解决了必须通过告警事件反向调整告警策略造成的时效性问题。

[0106] 本发明的一些实施例中，可选的，所述目标日志事件的事件数据至少包括所述目标日志事件发生时间和所述目标日志事件数量的键值对。

[0107] 本发明实施例中，目标日志事件的事件数据为键值对，键值对的组成依据验证性分析参数名称、历史时间属性、用户数量等相关，可依据用户实际需求进行键值对的调整。

[0108] 在本发明的一些实施例中，可选的，所述验证性分析参数包括告警名称、告警类型、查询时间区间、触发条件、触发阈值、告警白名单中的至少之一。

[0109] 在本发明的一些实施例中，可选的，所述验证分析编号的分析结果包括：历史事件总数、关联用户数量和事件触发概率中的至少之一。

[0110] 在本发明的一些实施例中，可选的，所述图形数据列表包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表或按不同次数的历史事件统计的操作频次列表中的至少之一。

[0111] 本发明的一些实施例中，可选的，若所述更新策略参数至所述告警策略之前，所述告警策略被删除，所述执行模块33还用于依据当前的验证分析编号的验证分析结果新增一条告警策略。

[0112] 本发明实施例中，告警策略被删除时，用户可通过依据当前的验证分析编号对应的验证性分析参数和验证分析结果新增策略数据实现告警策略的生成，灵活地保证了告警策略参数的安全性。

[0113] 在本发明的一些实施例中，可选的，所述更新模块34还用于依据所述验证分析编号获取所述告警策略编号；依据所述验证分析编号获取所述验证性分析参数，依据所述告警策略编号获取所述告警策略的详细信息；依据所述验证性分析参数和所述告警策略的详细信息更新所述告警策略。

[0114] 具体地，验证性分析任务结束后，如果用户确认该参数配置结果，可以对该告警策略进行更新，步骤如下：首先系统获取该任务的验证性分析编号和对应的验证性分析参数；根据验证性分析编号获取对应的告警策略编号，从而获取该告警策略详情；判断当前告警策略的状态，如果该告警策略为正常状态，则对原告警策略进行更新；如果该告警策略已经被删除，则根据验证性分析结果新增一条新的告警策略。

[0115] 本发明的一些实施例中，可选的，所述验证性分析参数包括所述告警策略的策略参数时，若所述告警策略的策略参数有修改，所述获取模块31还用于将更新后的所述策略参数更新至所述验证性分析参数中。本发明实施例中，验证性分析参数包括告警策略的策略参数时，若用户修改了策略参数，当前的验证性分析参数包括最新的策略参数，保证了当前验证分析的时效性。

[0116] 具体地，根据告警策略编号和当前的验证性分析参数，查询当前的验证分析列表中是否已存在该目标任务；

[0117] 如果存在该目标任务，则进一步判断该任务的记录状态值，即是否已经完成了验证分析；

[0118] 如果完成了验证分析，则返回该任务的验证性分析编号和状态值，否则仅返回状态值，该输出结果对接生成分析结果；

[0119] 如果不存在该目标任务，则生成该任务的验证性分析编号，并插入1条验证性分析数据，对接生成分析结果，异步开启验证性分析任务。

[0120] 本发明的一些实施例中，可选的，所述目标日志事件的事件数据还包括所述目标日志事件的事件类型时，所述验证分析编号的验证分析结果包括按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表和按不同次数的历史事件统计的操作频次列表中的至少之一。

[0121] 本发明实施例中，目标日志事件的事件数据包括：目标日志事件的事件类型、目标日志事件发生时间和所述目标日志事件数量时，验证分析结果的维度可涉及按时间统计的历史事件数量列表、按事件类型统计的历史事件数量列表或按不同次数的历史事件统计的操作频次列表，用户通过上述列表直观的获取不同维度的历史事件的告警可能性进行告警策略的参数调整，减少了对操作人员经验的依赖问题，使得一般业务人员可以通过多维度的图像验证分析结果确定合理的配置参数；基于历史目标事件的筛选也减少了无效告警事件的数量，解决了对无效告警需要进行大量人工判读的问题；统计多种目标事件的事件类型解决了必须通过具体告警事件反向调整告警策略造成的时效性问题。

[0122] 本发明的一些实施例中，可选的，所述告警策略的策略参数保存在策略表中，依据每一告警策略的策略编号查询得到。

[0123] 本发明还提供一种电子设备，请参见图4，图4为本发明实施例提供的电子设备的结构示意图之一；

[0124] 该电子设备40包括：处理器41、存储器42及存储在所述存储器42上并可在所述处理器41上运行的程序，所述程序被所述处理器41执行时实现如实现上述任一所述的告警策略验证方法的实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

[0125] 本发明实施例还提供一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一所述的告警策略验证方法的实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

[0126] 其中，所述的计算机可读存储介质，如只读存储器(Read-Only Memory，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0127] 上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本发明的保护之内。

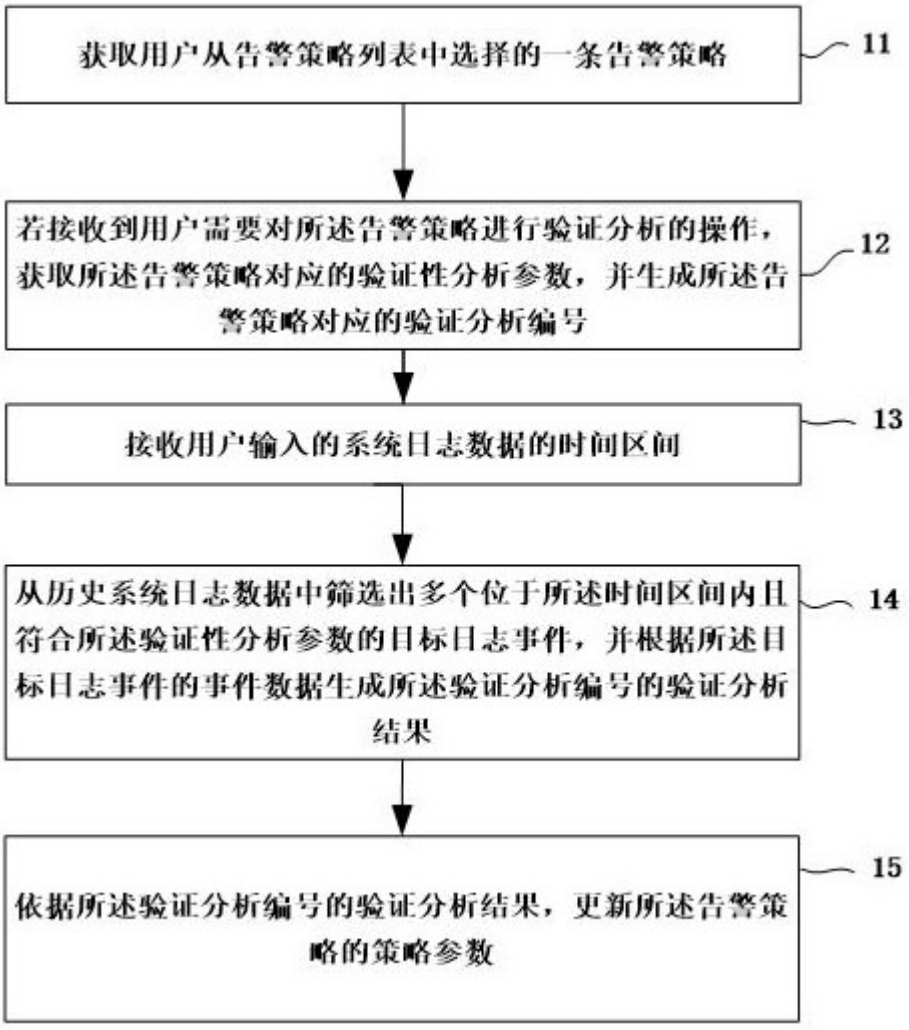

获取用户从告警策略列表中选择的一条告警策略
11
若接收到用户需要对所述告警策略进行验证分析的操作，获取所述告警策略对应的验证性分析参数，并生成所述告警策略对应的验证分析编号
12
接收用户输入的系统日志数据的时间区间
13
从历史系统日志数据中筛选出多个位于所述时间区间内且符合所述验证性分析参数的目标日志事件，并根据所述目标日志事件的事件数据生成所述验证分析编号的验证分析结果
14
依据所述验证分析编号的验证分析结果，更新所述告警策略的策略参数
15

图1

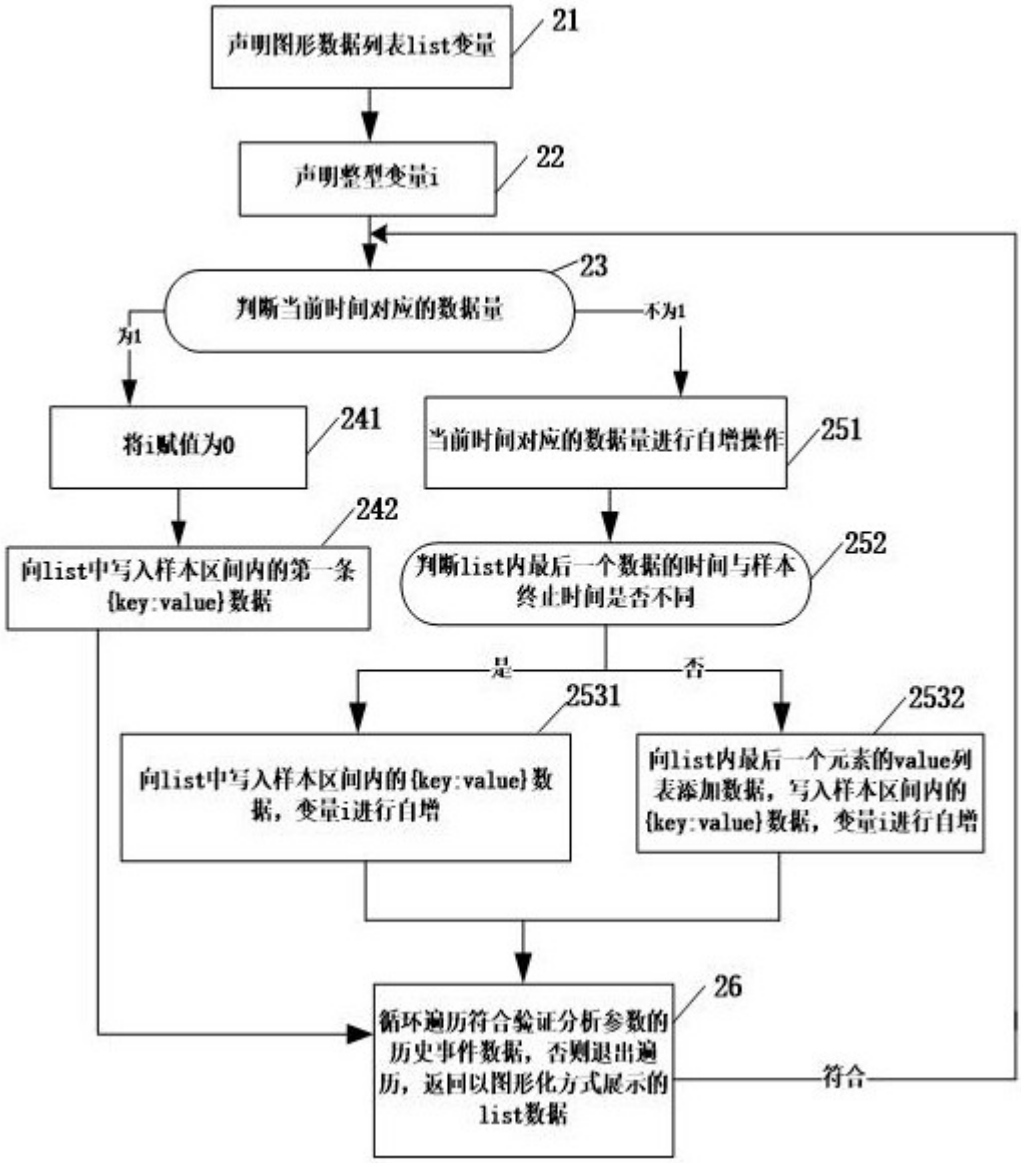

声明图形数据列表list变量
21
声明整型变量i
22
判断当前时间对应的数据量
23
为1
不为1
将i赋值为0
241
当前时间对应的数据量进行自增操作
251
向list中写入样本区间内的第一条{key:value}数据
242
判断list内最后一个数据的时间与样本终止时间是否不同
252
是
否
向list中写入样本区间内的{key:value}数据，变量i进行自增
2531
向list内最后一个元素的value列表添加数据，写入样本区间内的{key:value}数据，变量i进行自增
2532
循环遍历符合验证分析参数的历史事件数据，否则退出遍历，返回以图形化方式展示的list数据
26
符合

图2

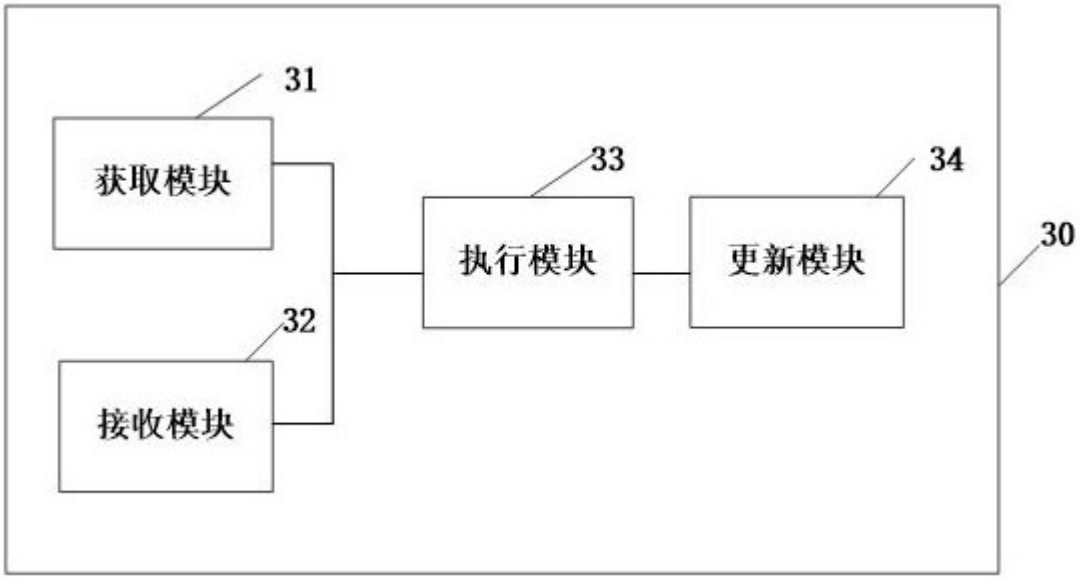


图3

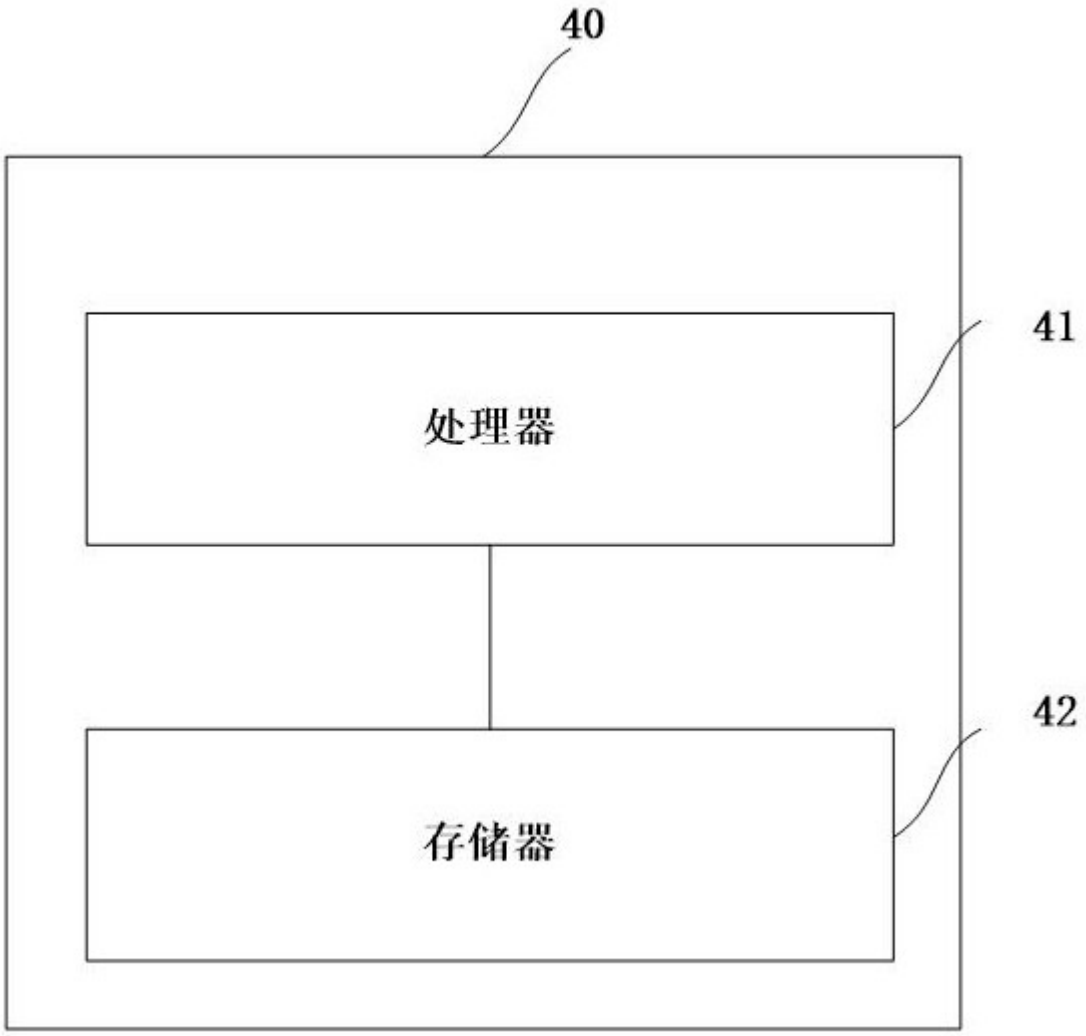


图4