(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 113806173 A
(43)申请公布日 2021.12.17

(21)申请号 202111092078.7

(22)申请日 2021.09.17

(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 李耕寅 吴声 茅逸斐 常杰

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 张琛

(51)Int.Cl.
G06F 11/30(2006.01)

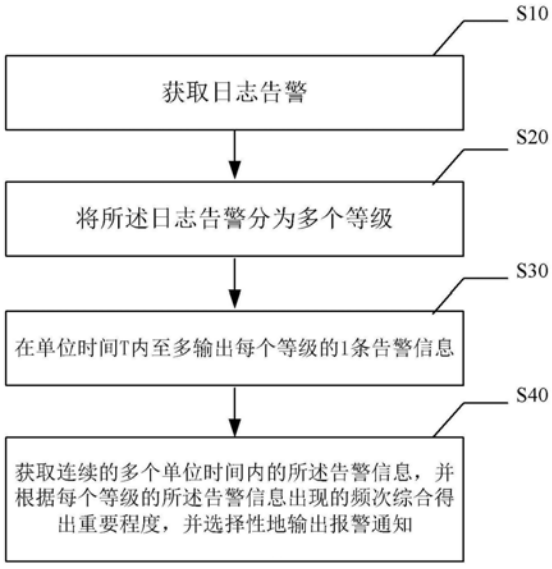
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种日志报警的归类方法、系统、电子设备

(57)摘要

本申请提供了一种日志报警的归类方法，可以用于金融领域或其他领域，该归类方法包括以下步骤：获取日志告警；将所述日志告警分为多个等级；在单位时间T内至多输出每个等级的1条告警信息；获取连续的多个单位时间内的所述告警信息，并根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。根据本申请的归类方法，对日志告警有较高的压缩比例，压缩后的日志告警能更有效地把系统内的问题第一时间暴露给一线运维人员，避免在报警风暴期间因告警过多，不能及时发现有用信息而导致系统瘫痪。本公开还提供了一种日志报警的归类系统、电子设备、存储介质和程序产品。



CN 113806173 A

1.一种日志报警的归类方法，其特征在于，基于日志告警的频度以及日志告警的对象，包括以下步骤：

获取日志告警；

将所述日志告警分为多个等级；

在单位时间T内至多输出每个等级的1条告警信息；

获取连续的多个单位时间内的所述告警信息，并根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。

2.根据权利要求1所述的归类方法，其特征在于，所述日志告警的所述等级包括：主要告警、次要告警和疑似告警。

3.根据权利要求2所述的归类方法，其特征在于，根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知，包括：

当主要告警的频次大于等于1时，重要程度为一级，输出报警通知；

当主要告警的频次为0且次要告警的频次大于等于1时，重要程度为一级或二级，输出报警通知；

当主要告警和次要告警的频次均为0且疑似告警的频次大于等于1时，重要程度为二级、三级或四级，选择地输出报警通知。

4.根据权利要求3所述的归类方法，其特征在于，当主要告警的频次为0且次要告警的频次大于等于1时，重要程度为一级或二级，输出报警通知，包括：

在连续的多个单位时间内，只在t-T内出现次要告警，其他时间内均未出现次要告警时，重要程度为二级，输出报警通知，其中，t为当前时刻；

在连续的多个单位时间内，在t-T内出现次要告警，且其他时间内也出现过次要告警时，重要程度为一级或二级，输出报警通知。

5.根据权利要求4所述的归类方法，其特征在于，在连续的多个单位时间内，在t-T内出现次要告警，且其他时间内也出现过次要告警时，重要程度为一级或二级，输出报警通知，包括：

当次要告警出现的频次小于第一预设值时，重要程度为二级，输出报警通知；

当次要告警出现的频次大于或等于第一预设值时，重要程度为一级，输出报警通知。

6.根据权利要求3所述的归类方法，其特征在于，当主要告警和次要告警的频次均为0且疑似告警的频次大于等于1时，重要程度为三级或四级，选择地输出报警通知，包括：

在连续的多个单位时间内，只在t-T内出现疑似告警，其他时间内均未出现疑似告警时，重要程度为三级或四级，选择性地输出报警通知；

在连续的多个单位时间内，在t-T内出现疑似告警时，且其他时间内也出现过疑似告警时，重要程度为二级或三级，输出报警通知。

7.根据权利要求6所述的归类方法，其特征在于，在连续的多个单位时间内，只在t-T内出现疑似告警，其他时间内均未出现次要告警时，重要程度为三级或四级，选择性地输出报警通知，包括：

当t-T内出现的疑似告警的频次小于第二预设值时，重要程度为四级，不报警；

当t-T内出现的疑似告警的频次大于或等于第二预设值时，重要程度为三级，输出报警通知。

8.根据权利要求6所述的归类方法，其特征在于，在连续的多个单位时间内，在t-T内出现疑似告警时，且其他时间内也出现过疑似告警时，重要程度为二级或三级，输出报警通知，包括：

当疑似告警出现的频次小于第三预设值时，重要程度为三级，输出报警通知；

当疑似告警出现的频次大于或等于第三预设值时，重要程度为二级，输出报警通知。

9.一种日志报警的归类系统，其特征在于，包括：

日志收集单元，所述日志收集单元用于获取日志告警；

日志风险确定单元，所述日志风险确定单元用于对所述日志告警分为多个等级；

日志输出单元，所述日志输出单元用于在单位时间内至多输出每个等级的1条告警信息；

日志报警单元，所述日志报警单元用于：根据时间段内每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。

10.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

其中，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行根据权利要求1-8中任一项所述的归类方法。

11.一种计算机可读存储介质，其特征在于，其上存储有可执行指令，该指令被处理器执行时使处理器执行根据权利要求1-8中任一项所述的归类方法。

12.一种计算机程序产品，包括计算机程序，其特征在于，所述计算机程序被处理器执行时实现根据权利要求1-8中任一项所述的归类方法。

一种日志报警的归类方法、系统、电子设备

技术领域

[0001] 本申请涉及运维技术领域，可用于金融领域或其他领域，具体地涉及一种日志报警的归类方法、系统、电子设备、可读存储介质和程序产品。

背景技术

[0002] 近几年来，数据中心信息系统监控逐步由传统监控向精细化转型，对日志的监控已然成为各大企业的重点关注方向。日志的智能监控往往基于日志模板的频度变化，但由于模板数量巨大，会产生大量的日志告警，运维人员无法及时获取日志告警中有用的信息，可能会造成巨大的经济损失。

发明内容

[0003] 本申请旨在至少解决现有技术中存在的技术问题之一。

[0004] 为此，本申请的第一个目的在于提出一种日志报警的归类方法，有效解决了在产生大量日志告警后，无法及时找到有用信息的问题；

[0005] 本申请的第二个目的在于提出一种日志报警的归类系统，可承载上述的归类方法；

[0006] 本申请的第三个目的在于提出一种电子设备，设备内包括上述的归类方法；

[0007] 本申请的第四个目的在于提出一种计算机可读存储介质，介质内存储有上述的归类方法；

[0008] 本申请的第五个目的在于提出一种计算机程序产品，可执行上述的归类方法。

[0009] 为了达到上述目的，本申请第一方面提供了一种日志报警的归类方法，基于日志告警的频度以及日志告警的对象，包括以下步骤：

[0010] 获取日志告警；

[0011] 将所述日志告警分为多个等级；

[0012] 在单位时间T内至多输出每个等级的1条告警信息；

[0013] 获取连续的多个单位时间内的所述告警信息，并根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。

[0014] 根据本申请的归类方法，对日志告警有较高的压缩比例，压缩后的日志告警能更有效地把系统内的问题第一时间暴露给一线运维人员，避免在报警风暴期间因告警过多，不能及时发现有用信息而导致系统瘫痪。

[0015] 进一步地，所述日志告警的所述等级包括：主要告警、次要告警和疑似告警。

[0016] 进一步地，根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知，包括：

[0017] 当主要告警的频次大于等于1时，重要程度为一级，输出报警通知；

[0018] 当主要告警的频次为0且次要告警的频次大于等于1时，重要程度为一级或二级，输出报警通知；

[0019] 当主要告警和次要告警的频次均为0且疑似告警的频次大于等于1时，重要程度为二级、三级或四级，选择地输出报警通知。

[0020] 进一步地，当主要告警的频次为0且次要告警的频次大于等于1时，重要程度为一级或二级，输出报警通知，包括：

[0021] 在连续的多个单位时间内，只在t-T内出现次要告警，其他时间内均未出现次要告警时，重要程度为二级，输出报警通知，其中，t为当前时刻；

[0022] 在连续的多个单位时间内，在t-T内出现次要告警，且其他时间内也出现过次要告警时，重要程度为一级或二级，输出报警通知。

[0023] 进一步地，在连续的多个单位时间内，在t-T内出现次要告警，且其他时间内也出现过次要告警时，重要程度为一级或二级，输出报警通知，包括：

[0024] 当次要告警出现的频次小于第一预设值时，重要程度为二级，输出报警通知；

[0025] 当次要告警出现的频次大于或等于第一预设值时，重要程度为一级，输出报警通知。

[0026] 进一步地，当主要告警和次要告警的频次均为0且疑似告警的频次大于等于1时，重要程度为三级或四级，选择地输出报警通知，包括：

[0027] 在连续的多个单位时间内，只在t-T内出现疑似告警，其他时间内均未出现疑似告警时，重要程度为三级或四级，选择性地输出报警通知；

[0028] 在连续的多个单位时间内，在t-T内出现疑似告警时，且其他时间内也出现过疑似告警时，重要程度为二级或三级，输出报警通知。

[0029] 进一步地，在连续的多个单位时间内，只在t-T内出现疑似告警，其他时间内均未出现次要告警时，重要程度为三级或四级，选择性地输出报警通知，包括：

[0030] 当t-T内出现的疑似告警的频次小于第二预设值时，重要程度为四级，不报警；

[0031] 当t-T内出现的疑似告警的频次大于或等于第二预设值时，重要程度为三级，输出报警通知。

[0032] 进一步地，在连续的多个单位时间内，在t-T内出现疑似告警时，且其他时间内也出现过疑似告警时，重要程度为二级或三级，输出报警通知，包括：

[0033] 当疑似告警出现的频次小于第三预设值时，重要程度为三级，输出报警通知；

[0034] 当疑似告警出现的频次大于或等于第三预设值时，重要程度为二级，输出报警通知。

[0035] 本申请第二方面提供了一种日志报警的归类系统，包括：日志收集单元，所述日志收集单元用于获取日志告警；日志风险确定单元，所述日志风险确定单元用于将所述日志告警分为多个等级；日志输出单元，所述日志输出单元用于在单位时间内至多输出每个等级的1条告警信息；日志报警单元，所述日志报警单元用于：根据时间段内每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。

[0036] 本申请第三方面提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，其中，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行根据所述的归类方法。

[0037] 本申请的第四方面还提供了一种计算机可读存储介质，其上存储有可执行指令，该指令被处理器执行时使处理器执行上述归类方法。

[0038] 本申请的第五方面还提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述归类方法。

[0039] 本申请的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

[0040] 通过以下参照附图对本申请实施例的描述，本申请的上述内容以及其他目的、特征和优点将更为清楚，在附图中：

[0041] 图1是根据本申请实施例中归类方法的流程图；

[0042] 图2是根据本申请实施例中归类系统的结构框图；

[0043] 图3是根据本申请实施例中适于实现归类方法的电子设备的方框图。

具体实施方式

[0044] 以下，将参照附图来描述本申请的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本申请的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本申请实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本申请的概念。

[0045] 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本申请。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

[0046] 在此使用的所有术语(包括技术和科学术语)具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

[0047] 在使用类似于“A、B和C等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释(例如，“具有A、B和C中至少一个的系统”应包括但不限于单独具有A、单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等)。

[0048] 近几年来，数据中心信息系统监控逐步由传统监控向精细化转型，对日志的监控已然成为各大企业的重点关注方向，网络系统中的各种网络设备、操作系统、安全设备等都会产生大量的日志数据，小则数十、多则上千，对运维人员而言，从海量日志中提取关键数据需要耗费大量时间，若没有及时修复，可能会造成巨大的经济损失。

[0049] 为了提高预警的功能，减少告警漏报、误报的情况，需要对原始日志告警进行归类，将繁杂的原始日志告警进行收敛，以达到清晰显示重要报警信息的目的，让运维人员更加高效地清楚并处理问题。

[0050] 本申请提供了一种日志报警的归类方法，有效解决了日志的智能监控报警，压缩比例较高，可以及时暴露出风险信息，以便运维人员可以更精准地做出判断并在第一时间采取措施。

[0051] 需要注意的是，本申请的归类方法是基于日志告警的频度以及日志告警的对象，

对其进行压缩归类,可用于金融领域,同时也可用于其他领域,本申请中以分部式存储Ceph的运维场景为其中一个具体实施例进行详细描述,但不能作为对本申请的具体限制。

[0052] 下面参照图1描述根据本申请实施例的日志报警的归类方法。

[0053] 根据本申请的一个实施例提供了一种日志报警的归类方法,该方法可以按照以下步骤或操作执行。

[0054] 在步骤S10,获取日志告警。

[0055] Ceph能够提供三种常见的存储需求:块存储、文件存储和对象存储,在这些存储的内部都有日志存储区,记录正在运行过程中的数据,将运行异常情况以日志告警的方式显示出来。

[0056] 首先将这些原始日志告警提取并收集,由于数量庞大,需要对其进行收敛,以便运维人员从中提取到关键性信息。

[0057] 在获取完日志告警之后,可以执行步骤S20。

[0058] 在步骤S20,将日志告警分为多个等级。

[0059] 通过对系统的损坏程度、或者根据运维人员的自身需求将日志告警分为多个等级,并在日志告警上进行标注。更具体地,可以通过拟定关键字的方式对日志告警进行筛选标注,自动匹配预设的知识库,并将匹配的结果反馈至告警事件中。例如:AIX的ERRPT代码,DB2的MESSAGE ID,存储的ERROR ID,HMC的SRC码等等。

[0060] 在一个具体实施例中,日志告警可以分为三个等级,包括:主要告警、次要告警和疑似告警。

[0061] 其中,主要告警对系统的影响较大,是重要关注的日志告警对象;次要告警对系统的影响居中,在一定范围内不会对系统产生较大的影响,只需要引起运维人员的注意即可;而疑似告警对系统的影响最小,可以是因常规事件更改而发出的告警,此部分在大多情况下可以忽略。

[0062] 当然,告警等级还可以分的更细,以区分日志告警的严重程度。

[0063] 在Ceph的场景中,可在severity字段中进行设计,将主要告警设为3,次要告警设为2,疑似告警设为1。

[0064] 在将日志告警分为多个等级后,可以执行步骤S30。

[0065] 在步骤S30,在单位时间T内至多输出每个等级的1条告警信息。

[0066] 也就是说,每个等级的告警信息在单位时间T内只能出现1条或者1条都不出现,以下为穷尽列举,是基于将等级分为主要告警、次要告警和疑似告警三种的形式列举。

[0067] 例如:在告警信息中,输出1条主要告警信息和1条次要告警信息和1条疑似告警信息,或者输出1条主要告警信息和1条次要告警信息,或者输出1条主要告警信息和1条疑似告警信息,或者输出1条次要告警信息和1条疑似告警信息,或者输出1条主要告警信息,或者输出1条次要告警信息,或者输出1条疑似告警信息。

[0068] 在步骤S30中,系统实现对原始日志告警集合压缩。具体是在单位时间T内,将所有相同等级的日志集合,并压缩在1条告警信息内。

[0069] 在一个实施例中,1条主要告警信息内包括有m个主要告警等级的日志告警,1条主要告警信息内包括有n个主要告警等级的日志告警,1条主要告警信息内包括有s个主要告警等级的日志告警,其中,m、n、s均为正整数,m、n、s的数值可相同,将将聚合后的alter_id

信息讯处在trace中，便于前端下钻，m、n、s的个数存入Event_Count字段。

[0070] 优选的，可以将单位时间T认为是1分钟，步骤S30在本实施例中可以理解为，将日志告警中同级别的事件按每分钟进行聚合，合并后每分钟最多报1条每个级别的告警信息。

[0071] 在得到单位时间T内的告警信息之后，可以执行步骤S40。

[0072] 在步骤S40，获取连续的多个单位时间内的告警信息，并根据每个等级的告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。

[0073] event_level根据当前告警信息发生的频次以及日志告警的等级将综合得出报送集中监控的报警通知。

[0074] 在聚合后，通过以下步骤对告警信息进行进一步地划分。在一些重要的告警信息出现时，需要输出报警通知，以在告警信息风暴中准确推送出危险性较高、对系统影响较大、需要运维人员及时处理的告警日志；同时，也会有一部分告警信息不足以令系统发出报警，这部分告警信息可以选择暂时忽略，运维人员只需要关注输出报警通知的重要信息即可，节省了运维人员的大量时间。

[0075] 获取连续的多个单位时间内的告警信息，连续的多个单位时间可以组成一个时间段，在本申请中，时间段即指多个单位时间的组合，时间段可是原始日志告警中的起始时间与结束时间，也可以是以某一刻为时间节点到另一刻时间节点的时间差。例如：时间段可以为从现在时刻到5分钟前的这段时间，单位时间为1分钟，也就是从现在时刻之前5分钟内，按每分钟对告警信息扫描聚合，将告警信息进行时间颗粒度的拆分。

[0076] 对步骤S40进一步地拆分，以先后顺序执行判断下列规则。

[0077] 根据每个等级的告警信息出现的频次综合得出重要程度，并选择性地输出报警通知，包括：

[0078] 当主要告警的频次大于等于1时，重要程度为一级，输出报警通知。

[0079] 在步骤S30之后，先判断时间段内是否出现主要告警，由于主要告警对系统的影响较大，只要在主要告警出现时，也就是频次大于等于1时，将重要程度判定为一级，并输出报警通知运维人员及时维护查看。

[0080] 当主要告警的频次为0且次要告警的频次大于等于1时，重要程度为一级或二级，输出报警通知。

[0081] 在时间段内没有出现主要告警，则在步骤S30后直接执行此规则。在时间段内若有次要告警出现时，重要程度可能为一级也可能为二级，具体重要程度由以下情况进行判断，然后输出报警通知。

[0082] 在连续的多个单位时间内，只在t-T内出现次要告警，其他时间内均未出现次要告警时，重要程度为二级，输出报警通知；

[0083] 在连续的多个单位时间内，在t-T内出现次要告警，且其他时间内也出现过次要告警时，重要程度为一级或二级，输出报警通知；

[0084] 当次要告警出现的频次小于第一预设值时，重要程度为二级，输出报警通知；

[0085] 当次要告警出现的频次大于或等于第一预设值时，重要程度为一级，输出报警通知；

[0086] 其中，t为当前时刻。

[0087] 在时间段内，若在此时刻起之前的一分钟内出现次要告警，而在一分钟前没有出

现过，重要等级为二级，输出告警通知；若在此时刻起之前的一分钟内出现次要告警，在时间段内的其他时间内也出现过次要告警，则需要根据时间段内次要告警出现的频次，进一步地判断重要程度的级别。在出现的频次较多时，说明需要维护的点问题较为严重，将重要程度设为一级，输出告警通知；在出现的频次较少时，对系统的影响不是很大，可以保持关注的态度，此时将重要程度设为二级，告警通知运维人员保持关注即可。

[0088] 在一个实施例中，将第一预设值设置为x条，当在时间段内次要告警一共出现的频次小于x条时，重要程度为二级，输出报警通知；当时间段内次要告警一共出现的频次大于或等于x条时，重要程度为一级，输出报警通知。

[0089] 需要注意的是，根据不同的重要等级，报警通知可以输出不同的文字内容提示运维人员，也可以仅显示重要程度等级以警示运维人员。

[0090] 当主要告警和次要告警的频次均为0且疑似告警的频次大于等于1时，重要程度为二级、三级或四级，选择地输出报警通知。

[0091] 在时间段内没有出现主要告警，也没有出现次要警告，则在步骤S30后直接执行此规则。在时间段内若有疑似告警出现时，重要程度可能为二级、也可能为三级、还可能为四级，具体重要程度由以下情况进行判断，是否需要输出报警通知，也要依据重要程度进行判断。

[0092] 在连续的多个单位时间内，只在t-T内出现疑似告警，其他时间内均未出现疑似告警时，重要程度为三级或四级，选择性地输出报警通知；

[0093] 当t-T内出现的疑似告警的频次小于第二预设值时，重要程度为四级，不报警；

[0094] 当t-T内出现的疑似告警的频次大于或等于第二预设值时，重要程度为三级，输出报警通知。

[0095] 在时间段内，若在此时刻起之前的一分钟内出现疑似告警，而在一分钟前没有出现过，重要等级为三级或四级，可能报警通知也可能不报警，具体根据一分钟内疑似告警总共出现的频次来判断。若在此时刻起之前的一分钟内出现疑似告警的次数小于第二预设值，也就是出现的频次较少时，由于疑似告警本身的等级就很低，属于不重要日志告警事件，综合频次和本身等级，重要程度很低，将重要程度设置为四级，可以不通知运维人员；若在此时刻起之前的一分钟内出现疑似告警的次数大于或等于第二预设值，由于疑似告警本身的等级就很低，属于不重要日志告警事件，但由于单位时间内出现频次较高，可将重要程度设为三级，重要程度较低，通知运维人员可选择性地关注、或者无需关注此告警信息。

[0096] 在一个实施例中，将第二预设值设置为y条，当单位时间内出现的疑似告警的频次小于y条时，重要程度为四级，不报警；当单位时间内出现的疑似告警的频次大于或等于y条时，重要程度为三级，输出报警通知。

[0097] 在连续的多个单位时间内，在t-T内出现疑似告警时，且其他时间内也出现过疑似告警时，重要程度为二级或三级，输出报警通知。

[0098] 当疑似告警出现的频次小于第三预设值时，重要程度为三级，输出报警通知；

[0099] 当疑似告警出现的频次大于或等于第三预设值时，重要程度为二级，输出报警通知。

[0100] 在时间段内，若在此时刻起之前的一分钟内出现疑似告警，在时间段内的其他时间内也出现过疑似告警，则需要根据时间段内次要告警出现的频次，进一步地判断重要程

度的级别。在时间段内出现的频次较多时，需要关注告警信息，将重要程度设为二级，输出告警通知；在时间段内出现的频次较少时，对系统的影响不是很大，此时将重要程度设为三级，告警通知运维人员可选择性地关注、或者无需关注此告警信息。

[0101] 在一个实施例中，将第三预设值设置为z条，当在时间段内疑似告警一共出现的频次小于z条时，重要程度为三级，输出报警通知；当疑似告警出现的频次大于或等于z条时，重要程度为二级，输出报警通知。

[0102] 需要注意的是，x、y和z为正整数。本申请中将重要程度分为一级、二级、三级、四级，其中，一级为最严重、对系统的破坏性最大，四级为最轻，可以选择不关注，当然，也可以设置更多级别，本申请只提供其中一个实施例，不能作为对本申请的具体限制。

[0103] 本申请中的归类系统，以从重原则为基准，显示最终报警结果，也就是说，当主要告警出现时，以主要告警的最终结果为报警通知结果，当无主要告警时，以次要告警的最终结果为报警通知结果，当无主要告警和次要告警时，以疑似告警的最终结果为报警通知结果，从对系统影响最大的到最小的进行逐级判断。

[0104] 本申请还具有逐级升级原则，在时间段内发生次要告警的频次小于第一预设值，此时的重要程度为二级，但在此时刻的下一个单位时间内，发生次要告警的频次大于等于第一预设值，此时的重要程度将由二级升级至一级，此规则同样适用于疑似告警。

[0105] 根据本申请的归类方法，对原始的日志告警有较高的压缩比例，压缩后的日志告警能更有效地把系统内的问题第一时间暴露给一线运维人员，避免在报警风暴期间因告警过多，不能及时发现有用信息而导致系统瘫痪。

[0106] 基于上述一种日志报警的归类方法，本申请还提供了一种日志报警的归类系统100，以下结合图2进行详细描述。

[0107] 根据本申请实施例中的归类系统100，包括：日志收集单元110、日志风险确定单元120、日志输出单元130和日志报警单元140。

[0108] 日志收集单元110用于获取日志告警。在一个实施例中，日志收集单元110可以用于执行前文描述的操作S10，获取日志告警，在此不再赘述。

[0109] 日志风险确定单元120用于将日志告警分为多个等级。在一个实施例中，日志风险确定单元120可以用于执行前文描述的操作S20，将日志告警分为多个等级，在此不再赘述。

[0110] 日志输出单元130用于在单位时间内至多输出每个等级的1条告警信息。在一个实施例中，日志输出单元130可以用于执行前文描述的操作S30，在单位时间内至多输出每个等级的1条告警信息，在此不再赘述。

[0111] 日志报警单元140用于：根据时间段内每个等级的告警信息出现的频次综合得出重要程度，并选择性地输出报警通知。在一个实施例中，日志报警单元140可以用于执行前文描述的操作S40，根据时间段内每个等级的告警信息出现的频次综合得出重要程度，并选择性地输出报警通知，在此不再赘述。

[0112] 本申请中日志报警的归类系统，可实现上述的日志报警的归类方法，由于对日志告警有较高的压缩比例，在日志告警被压缩后，能更有效地将系统内的问题第一时间暴露给一线运维人员，避免在报警风暴期间因告警过多，不能及时发现有用信息而导致系统瘫痪。

[0113] 根据本申请的实施例，日志收集单元110、日志风险确定单元120、日志输出单元

130和日志报警单元140中的任意多个模块可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本申请的实施例，日志收集单元110、日志风险确定单元120、日志输出单元130和日志报警单元140中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC)，或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，日志收集单元110、日志风险确定单元120、日志输出单元130和日志报警单元140中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

[0114] 根据本申请的归类系统，对原始的日志告警有较高的压缩比例，在Ceph场景中压缩比例高达10:1，压缩后的日志告警能更有效地把系统内的问题第一时间暴露给一线运维人员，避免在报警风暴期间因告警过多，不能及时发现有用信息而导致系统瘫痪。

[0115] 图3示意性示出了根据本申请实施例的适于实现归类方法的电子设备200的方框图。

[0116] 如图3所示，根据本申请实施例的电子设备200包括处理器201，其可以根据存储在只读存储器(ROM)202中的程序或者从存储部分208加载到随机访问存储器(RAM)203中的程序而执行各种适当的动作和处理。处理器201例如可以包括通用微处理器(例如CPU)、指令集处理器和/或相关芯片组和/或专用微处理器(例如，专用集成电路(ASIC))等等。处理器201还可以包括用于缓存用途的板载存储器。处理器201可以包括用于执行根据本申请实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

[0117] 在RAM 203中，存储有电子设备200操作所需的各种程序和数据。处理器201、ROM 202以及RAM 203通过总线204彼此相连。处理器201通过执行ROM 202和/或RAM 203中的程序来执行根据本申请实施例的方法流程的各种操作。需要注意，所述程序也可以存储在除ROM 202和RAM 203以外的一个或多个存储器中。处理器201也可以通过执行存储在所述一个或多个存储器中的程序来执行根据本申请实施例的方法流程的各种操作。

[0118] 根据本申请的实施例，电子设备200还可以包括输入/输出(I/O)接口205，输入/输出(I/O)接口205也连接至总线204。电子设备200还可以包括连接至I/O接口205的以下部件中的一项或多项：包括键盘、鼠标等的输入部分206；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分207；包括硬盘等的存储部分208；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分202。通信部分202经由诸如因特网的网络执行通信处理。驱动器210也根据需要连接至I/O接口205。可拆卸介质211，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器210上，以便于从其上读出的计算机程序根据需要被安装入存储部分208。

[0119] 本申请还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本申请实施例的方法。

[0120] 根据本申请的实施例，计算机可读存储介质可以是非易失性的计算机可读存储介

质，例如可以包括但不限于：便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。例如，根据本申请的实施例，计算机可读存储介质可以包括上文描述的ROM202和/或RAM 203和/或ROM 202和RAM 203以外的一个或多个存储器。

[0121] 本申请的实施例还包括一种计算机程序产品，其包括计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。当计算机程序产品在计算机系统中运行时，该程序代码用于使计算机系统实现本申请实施例所提供的物品推荐方法。

[0122] 在该计算机程序被处理器201执行时执行本申请实施例的系统/装置中限定的上述功能。根据本申请的实施例，上文描述的系统、装置、模块、单元等可以通过计算机程序模块来实现。

[0123] 在一种实施例中，该计算机程序可以依托于光存储器件、磁存储器件等有形存储介质。在另一种实施例中，该计算机程序也可以在网络介质上以信号的形式进行传输、分发，并通过通信部分202被下载和安装，和/或从可拆卸介质211被安装。该计算机程序包含的程序代码可以用任何适当的网络介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

[0124] 在这样的实施例中，该计算机程序可以通过通信部分202从网络上被下载和安装，和/或从可拆卸介质211被安装。在该计算机程序被处理器201执行时，执行本申请实施例的系统中限定的上述功能。根据本申请的实施例，上文描述的系统、设备、装置、模块、单元等可以通过计算机程序模块来实现。

[0125] 根据本申请的实施例，可以以一种或多种程序设计语言的任意组合来编写用于执行本申请实施例提供的计算机程序的程序代码，具体地，可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。程序设计语言包括但不限于诸如Java，C++，python，“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网(LAN)或广域网(WAN)，连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0126] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0127] 本领域技术人员可以理解，本申请的各个实施例和/或权利要求中记载的特征可

以进行多种组合或/或结合，即使这样的组合或结合没有明确记载于本申请中。特别地，在不脱离本申请精神和教导的情况下，本申请的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本申请的范围。

[0128] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“实例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0129] 以上对本申请的实施例进行了描述。但是，这些实施例仅仅是为了说明的目的，而并非为了限制本申请的范围。尽管在以上分别描述了各实施例，但是这并不意味着各个实施例中的措施不能有利地结合使用。本申请的范围由所附权利要求及其等同物限定。不脱离本申请的范围，本领域技术人员可以做出多种替代和修改，这些替代和修改都应落在本申请的范围之内。

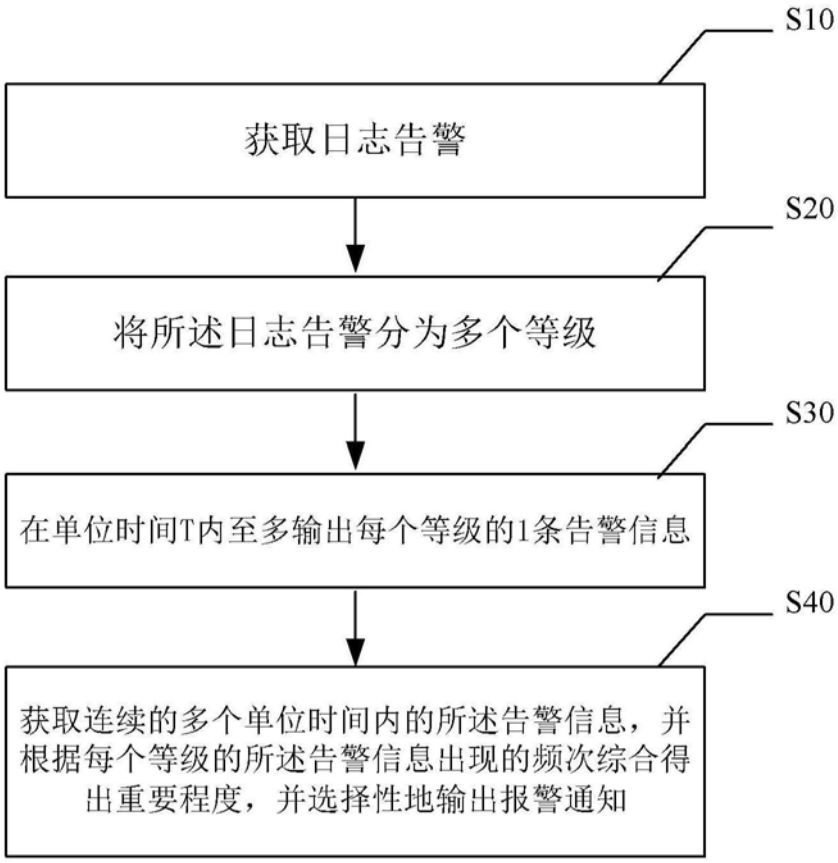

S10
获取日志告警
S20
将所述日志告警分为多个等级
S30
在单位时间T内至多输出每个等级的1条告警信息
S40
获取连续的多个单位时间内的所述告警信息，并根据每个等级的所述告警信息出现的频次综合得出重要程度，并选择性地输出报警通知

图1

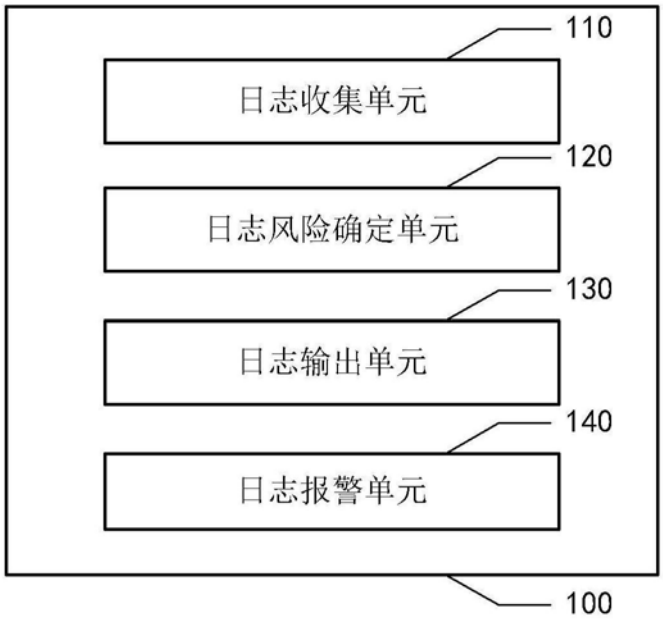

110
日志收集单元
120
日志风险确定单元
130
日志输出单元
140
日志报警单元
100

图2

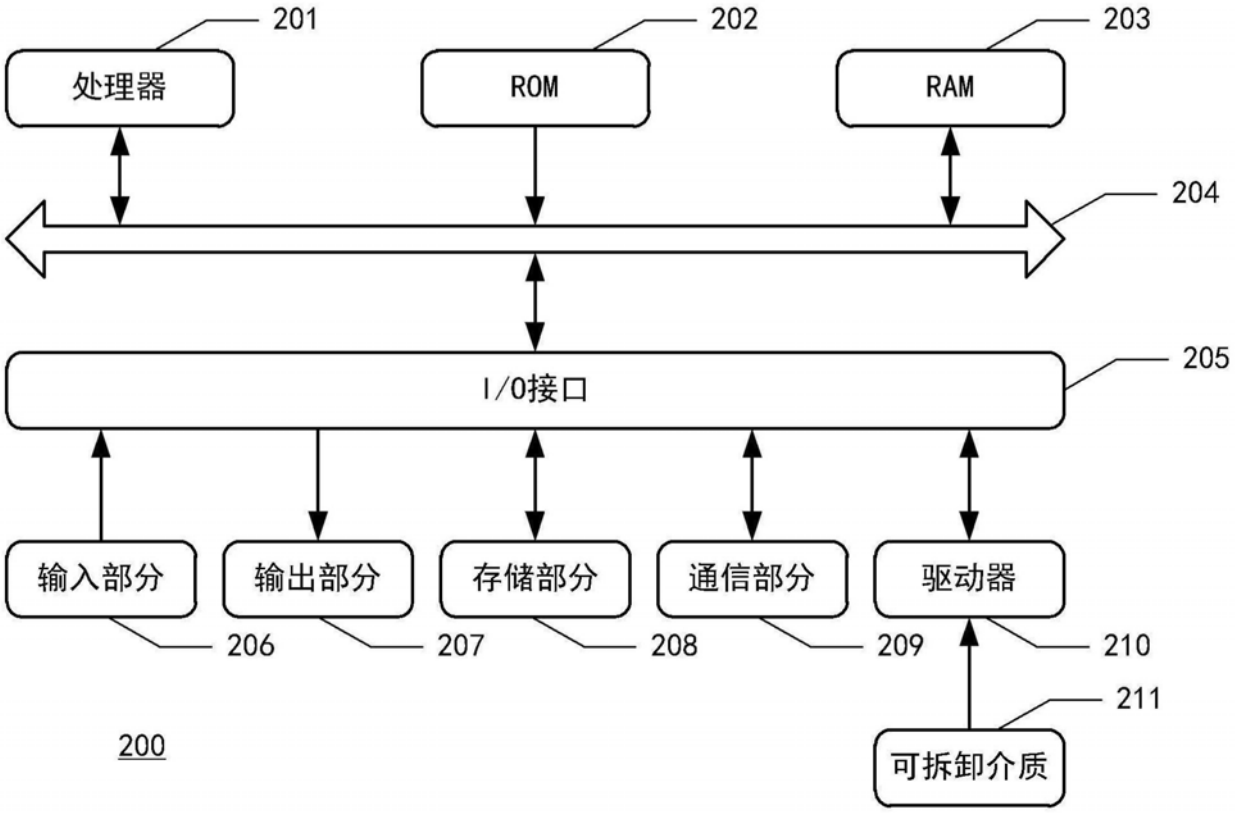

201
202
203
处理器
ROM
RAM
204
I/O接口
205
输入部分
输出部分
存储部分
通信部分
驱动器
206
207
208
209
210
211
200
可拆卸介质

图3