(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 113676356 A
(43)申请公布日 2021.11.19

(21)申请号 202110997537.X

(22)申请日 2021.08.27

(71)申请人 创新奇智(青岛)科技有限公司
地址 266200 山东省青岛市即墨市通济新经济区九江路17号A1-9

(72)发明人 王凯 马鑫意

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 唐正瑜

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

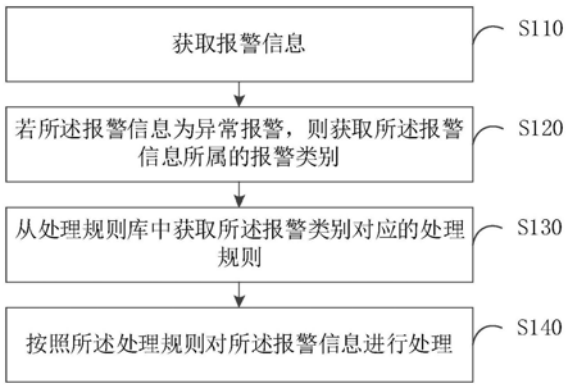
权利要求书2页 说明书10页 附图2页

(54)发明名称

报警信息处理方法、装置、电子设备及可读存储介质

(57)摘要

本申请提供一种报警信息处理方法、装置、电子设备及可读存储介质，涉及计算机技术领域。该方法通过在报警信息为异常报警时，获取报警信息所属的报警类别，然后从处理规则库中获取该报警类别对应的处理规则，并按照处理规则对报警信息进行处理，这样可以使得设备在出现异常报警时，可以优先按照规则实现自动处理，无需通知运维人员，能够及时对异常报警进行处理，节省了运维时间。



CN 113676356 A

1.一种报警信息处理方法,其特征在于,所述方法包括:

获取报警信息;

若所述报警信息为异常报警,则获取所述报警信息所属的报警类别;

从处理规则库中获取所述报警类别对应的处理规则;

按照所述处理规则对所述报警信息进行处理。

2.根据权利要求1所述的方法,其特征在于,通过以下方式判断所述报警信息是否为异常报警:

判断所述报警信息是否为异常报警信息中的一种;

若是,则确定所述报警信息为异常报警;或者

向设备使用人员输出所述报警信息;

若接收到所述设备使用人员针对所述报警信息的反馈信息为异常报警时,则确定所述报警信息为异常报警。

3.根据权利要求1所述的方法,其特征在于,所述按照所述处理规则对所述报警信息进行处理之后,还包括:

若按照所述处理规则对所述报警信息处理失败,则向设备使用人员输出包含有连接设备的websockt接口的提示信息,以提示所述设备使用人员通过所述websockt接口连接所述设备后对所述报警信息进行处理。

4.根据权利要求3所述的方法,其特征在于,所述向设备使用人员输出包含有连接设备的websockt接口的提示信息之后,还包括:

若确定所述设备使用人员对所述报警信息处理失败,则向运维人员输出对所述报警信息进行处理的提示信息。

5.根据权利要求3所述的方法,其特征在于,所述向设备使用人员输出包含有连接设备的websockt接口的提示信息之后,还包括:

在所述websockt接口断开之前,停止向所述设备使用人员输出处理其他报警信息的提示信息。

6.根据权利要求1所述的方法,其特征在于,所述获取报警信息,包括:

从配置管理数据库CMDB中获取报警信息。

7.根据权利要求1-6任一所述的方法,其特征在于,所述按照所述处理规则对所述报警信息进行处理之后,还包括:

若对所述报警信息处理成功,则将所述报警信息记录到日志中,所述日志中还包括历史的报警信息;

根据所述日志中的报警信息分析各种报警项的报警频率;

根据所述报警频率输出是否加增资源或调整报警阈值的提示信息。

8.一种报警信息处理装置,其特征在于,所述装置包括:

信息获取模块,用于获取报警信息;

类别获取模块,用于若所述报警信息为异常报警,则获取所述报警信息所属的报警类别;

规则获取模块,用于从处理规则库中获取所述报警类别对应的处理规则;

报警处理模块,用于按照所述处理规则对所述报警信息进行处理。

9.一种电子设备,其特征在于,包括处理器以及存储器,所述存储器存储有计算机可读取指令,当所述计算机可读取指令由所述处理器执行时,运行如权利要求1-7任一所述的方法。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时运行如权利要求1-7任一所述的方法。

报警信息处理方法、装置、电子设备及可读存储介质

技术领域

[0001] 本申请涉及计算机技术领域，具体而言，涉及一种报警信息处理方法、装置、电子设备及可读存储介质。

背景技术

[0002] 为了及时获知设备(如服务器、网络设备)的工作状态，一般可以对设备进行监控，当设备的工作状态出现异常时，发出报警信息。目前的做法是直接将报警信息通知网管人员，由网管人员来对报警信息进行处理。但是网管人员需要面对的设备数量通常较多，接收到的报警信息也可能是成百上千条，所以导致一些报警信息不能得到及时处理，设备可能会长时间处于异常状态而得不到处理。

发明内容

[0003] 本申请实施例的目的在于提供一种报警信息处理方法、装置、电子设备及可读存储介质，用以改善现有技术中报警信息较多而不能及时得到处理的问题。

[0004] 第一方面，本申请实施例提供了一种报警信息处理方法，所述方法包括：获取报警信息；若所述报警信息为异常报警，则获取所述报警信息所属的报警类别；从处理规则库中获取所述报警类别对应的处理规则；按照所述处理规则对所述报警信息进行处理。

[0005] 在上述实现过程中，该方法通过在报警信息为异常报警时，获取报警信息所属的报警类别，然后从处理规则库中获取该报警类别对应的处理规则，并按照处理规则对报警信息进行处理，这样可以使得设备在出现异常报警时，可以优先按照规则实现自动处理，无需通知运维人员，能够及时对异常报警进行处理，节省了运维时间。

[0006] 可选地，通过以下方式判断所述报警信息是否为异常报警：

[0007] 判断所述报警信息是否为异常报警信息中的一种；

[0008] 若是，则确定所述报警信息为异常报警；或者向设备使用人员输出所述报警信息；

[0009] 若接收到所述设备使用人员针对所述报警信息的反馈信息为异常报警时，则确定所述报警信息为异常报警。

[0010] 在上述实现过程中，通过设备使用人员来判断报警信息是否为异常报警，则可以通过人工对异常报警进行确认，更加准确。

[0011] 可选地，所述按照所述处理规则对所述报警信息进行处理之后，还包括：

[0012] 若按照所述处理规则对所述报警信息处理失败，则向设备使用人员输出包含有连接设备的websockt接口的提示信息，以提示所述设备使用人员通过所述websockt接口连接所述设备后对所述报警信息进行处理。

[0013] 在上述实现过程中，在自动对报警信息进行处理失败时，才通知设备使用人员进行处理，可以让设备使用人员对报警信息先进行处理，不需要通知运维人员，这样可以减少运维人员的运维压力。

[0014] 可选地，所述向设备使用人员输出包含有连接设备的websockt接口的提示信息之

后,还包括:

[0015] 若确定所述设备使用人员对所述报警信息处理失败,则向运维人员输出对所述报警信息进行处理的提示信息。这样在按照处理规则且设备使用人员对报警信息处理失败后,最后才让运维人员参与对报警信息的处理,而不是一开始就让运维人员进行处理,从而可以减少运维人员的运维压力。

[0016] 可选地,所述向设备使用人员输出包含有连接设备的websockt接口的提示信息之后,还包括:

[0017] 在所述websockt接口断开之前,停止向所述设备使用人员输出处理其他报警信息的提示信息。这样可以避免不停地向设备使用人员输出提示信息而造成设备使用人员负担较大的问题。

[0018] 可选地,所述获取报警信息,包括:

[0019] 从配置管理数据库CMDB中获取报警信息。通过CMDB的相关功能可以自动对报警信息进行归类,这样可以快速对海量的报警信息进行归类。

[0020] 可选地,所述按照所述处理规则对所述报警信息进行处理之后,还包括:

[0021] 若对所述报警信息处理成功,则将所述报警信息记录到日志中,所述日志中还包括历史的报警信息;

[0022] 根据所述日志中的报警信息分析各种报警项的报警频率;

[0023] 根据所述报警频率输出是否加增资源或调整报警阈值的提示信息。

[0024] 在上述实现过程中,通过对报警信息进行分析,可以统计各个报警项的报警频率,从而输出对应的提示信息,使得相关人员能够了解各个报警项的报警情况,进而为调整报警情况提供数据依据。

[0025] 第二方面,本申请实施例提供了一种报警信息处理装置,所述装置包括:

[0026] 信息获取模块,用于获取报警信息;

[0027] 类别获取模块,用于若所述报警信息为异常报警,则获取所述报警信息所属的报警类别;

[0028] 规则获取模块,用于从处理规则库中获取所述报警类别对应的处理规则;

[0029] 报警处理模块,用于按照所述处理规则对所述报警信息进行处理。

[0030] 可选地,通过以下方式判断所述报警信息是否为异常报警:

[0031] 判断所述报警信息是否为异常报警信息中的一种;

[0032] 若是,则确定所述报警信息为异常报警;或者向设备使用人员输出所述报警信息;

[0033] 若接收到所述设备使用人员针对所述报警信息的反馈信息为异常报警时,则确定所述报警信息为异常报警。

[0034] 可选地,所述报警处理模块,还用于若按照所述处理规则对所述报警信息处理失败,则向设备使用人员输出包含有连接设备的websockt接口的提示信息,以提示所述设备使用人员通过所述websockt接口连接所述设备后对所述报警信息进行处理。

[0035] 可选地,所述报警处理模块,还用于若确定所述设备使用人员对所述报警信息处理失败,则向运维人员输出对所述报警信息进行处理的提示信息。

[0036] 可选地,所述报警处理模块,还用于在所述websockt接口断开之前,停止向所述设备使用人员输出处理其他报警信息的提示信息。

[0037] 可选地，所述信息获取模块，用于从配置管理数据库CMDB中获取报警信息。

[0038] 可选地，所述报警处理模块，还用于若对所述报警信息处理成功，则将所述报警信息记录到日志中，所述日志中还包括历史的报警信息；根据所述日志中的报警信息分析各种报警项的报警频率；根据所述报警频率输出是否加增资源或调整报警阈值的提示信息。

[0039] 第三方面，本申请实施例提供一种电子设备，包括处理器以及存储器，所述存储器存储有计算机可读取指令，当所述计算机可读取指令由所述处理器执行时，运行如上述第一方面提供的所述方法中的步骤。

[0040] 第四方面，本申请实施例提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时运行如上述第一方面提供的所述方法中的步骤。

[0041] 本申请的其他特征和优点将在随后的说明书阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请实施例了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0042] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0043] 图1为本申请实施例提供的一种报警信息处理方法的流程图；

[0044] 图2为本申请实施例提供的一种报警信息处理方法的完整流程图；

[0045] 图3为本申请实施例提供的一种报警信息处理装置的结构框图；

[0046] 图4为本申请实施例提供的一种用于执行报警信息处理方法的电子设备的结构示意图。

具体实施方式

[0047] 下面将结合本申请实施例中附图，对本申请实施例中的技术方案进行清楚、完整地描述。

[0048] 需要说明的是，本发明实施例中的术语“系统”和“网络”可被互换使用。“多个”是指两个或两个以上，鉴于此，本发明实施例中也可以将“多个”理解为“至少两个”。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，字符“/”，如无特殊说明，一般表示前后关联对象是一种“或”的关系。

[0049] 本申请实施例提供一种报警信息处理方法，该方法通过在报警信息为异常报警时，获取报警信息所属的报警类别，然后从处理规则库中获取该报警类别对应的处理规则，并按照处理规则对报警信息进行处理，这样可以使得设备在出现报警时，可以先按照规则实现自动处理，无需通知运维人员，能够及时对异常报警进行处理，节省了运维时间。

[0050] 请参照图1，图1为本申请实施例提供的一种报警信息处理方法的流程图，该方法包括如下步骤：

[0051] 步骤S110：获取报警信息。

[0052] 其中,报警信息是设备在运行期间出现问题时所产生的,设备可以指服务器、网络设备、终端等设备。设备上可以部署有监控服务,监控服务可用于监控设备的运行状态,并在监测到设备出现异常时,产生报警信息,监控服务可以采用Prometheus监控器实现等。设备上还可以部署有报警服务,报警服务用于对报警信息进行相应处理,即报警服务可用于执行本申请的方法。

[0053] 在一些实施方式中,监控服务在获取到报警信息后,可将报警信息存储在配置管理数据库(Configuration Management Database,CMDB)中,报警服务在进行报警信息处理时,可以从CMDB中获取报警信息。CMDB可以存储并管理设备的各种配置信息,其与所有服务支持和服务交付流程都紧密相连,支持这些流程的运转、发挥配置信息的价值,同时依赖于相关流程保证数据的准确性。

[0054] CMDB包括几种关键的功能,如整合、调和、同步、映射和可视化等,整合是指能够充分利用来自其他数据源的信息,对CMDB中包含的记录源属性进行存取,将多个数据源合并至一个视图中,生成连同来自CMDB和其他数据源信息在内的报告;调和能力是指通过对来自每个数据源的匹配字段进行对比,保证CMDB中的记录在多个数据源中没有重复现象,维持CMDB中每个配置项目数据源的完整性,自动调整流程使得初始实施、数据库管理员的手动运作和现场维护支持工作降至最低;同步是指确保CMDB中的信息能够反映联合数据源的更新情况,在联合数据源更新频率的基础上确定CMDB更新日程,按照经过批准的变更来更新CMDB,找出未被批准的变更;应用映射与可视化是指举例说明应用间的关系并了解应用和其他组件之间的依存关系,了解变更造成的影响并帮助诊断问题。

[0055] 本申请中可以利用CMDB的相关功能,将报警信息进行整合,如将属于相同类别的报警信息进行整合,CMDB可以通过获得各个报警信息之间的关联来判断报警信息是否属于同一报警类别,以便能够在获取到新的报警信息后,快速将新的报警信息进行归类。

[0056] 需要说明的是,报警服务可以实时从CMDB中获取新存储的报警信息,也可以是间隔一定时间从CMDB中获取新存储的报警信息,此时获取的报警信息包括多条,报警服务获取到多条报警信息后,可针对每条报警信息按照本申请的方法进行处理。

[0057] 步骤S120:若所述报警信息为异常报警,则获取所述报警信息所属的报警类别。

[0058] 报警服务在获得报警信息后,可判断报警信息是否为异常报警,异常报警可以是指对设备的安全威胁造成较大影响的报警。例如,可提取报警信息中的关键字,与设备中存储的表征异常报警的异常关键字进行匹配,如果匹配上,则认为该报警信息是异常报警,如果匹配不上,则认为该报警信息是正常报警,正常报警可以是指对设备的安全威胁有较小影响的报警,对于正常报警,报警服务可不用对报警信息进行处理,可以将报警信息记录到日志即可,以便于后续对日志进行分析。或者,对于正常报警,若出现多次,报警服务可在达到设定次数后,确定该报警转为异常报警,则按照同样的方式对其进行处理。

[0059] 若报警信息为异常报警,则获取该报警信息所属的报警类别。具体地,异常报警可以如木马程序、内存溢出等,异常报警对应的报警类别可以如CPU报警、内存报警、存储报警、木马程序等类别,报警服务可以通过提取报警信息中的关键字来确定对应的报警类别,如报警信息为内存使用率不足而导致内存溢出,则可确定该报警信息的报警类别为内存溢出。其中,报警信息中的关键字还可以如产生报警信息的进程名称,还可以根据进程名称来确定报警类别,如该报警信息对应的进程名称是内存进程,则可确定该报警信息的报警类

别为内存报警。

[0060] 或者,CMDB在存储报警信息后,可自动将报警信息归类到对应的报警类别下,这样报警服务读取到报警信息后,可自动确定报警信息所属的报警类别。

[0061] 步骤S130:从处理规则库中获取所述报警类别对应的处理规则。

[0062] 设备中预先可存储有针对不同报警类别设置的处理规则,这些处理规则均存储在一个处理规则库中,换言之,处理规则库包括有各种报警类别对应的处理规则,这些处理规则可以是运维人员预先配置到处理规则库中的。例如,针对内存溢出的报警,其对应的处理规则可以是保存设备当前正在运行的信息后,对设备进行重启;又如,对木马程序的报警,其对应的处理规则可以是对木马程序进行追踪溯源,然后对其进行拦截。

[0063] 其中,这些处理规则可以是指一些运行脚本,运维人员可事先将这些运行脚本写入到处理规则库中,这些运行脚本可以是指修复脚本,这样出现异常报警时,可以自动运行对应的修复脚本对出现的问题进行修复。

[0064] 需要说明的是,若没有找到该报警信息对应的报警类别,则可向设备使用人员或运维人员输出提示信息,以提示设备使用人员或运维人员来判断该报警信息所属的报警类别,并提示设备使用人员或运维人员对该报警类别对应的处理规则进行配置。这样报警服务即可获得该报警类别对应的处理规则。

[0065] 步骤S140:按照所述处理规则对所述报警信息进行处理。

[0066] 所以,在上述步骤获取到报警类别对应的处理规则后,可按照处理规则对报警信息进行处理,如运行对应的修复脚本,以自动对报警信息进行处理,从而对出现的问题进行修复,确保设备的稳定运行。

[0067] 在上述实现过程中,通过在报警信息为异常报警时,获取报警信息所属的报警类别,然后从处理规则库中获取该报警类别对应的处理规则,并按照处理规则对报警信息进行处理,这样可以使得设备在出现异常报警时,可以优先按照规则实现自动处理,无需通知运维人员,能够及时对异常报警进行处理,节省了运维时间。

[0068] 在上述实施例的基础上,还可以通过以下方式判断报警信息是否为异常报警:判断报警信息是否为异常报警信息中的一种,若是,则确定报警信息为异常报警;或者,可以向设备使用人员输出报警信息,若接收到设备使用人员针对报警信息的反馈信息为异常报警时,则确定报警信息为异常报警。

[0069] 其中,判断报警信息是否为异常报警信息中的一种的方式可以如上述实施例所述,如通过将报警信息中的关键字与设备中存储的表征异常报警的异常关键字进行匹配,如果匹配上,则表示报警信息为异常报警信息中的一种,该报警信息为异常报警。

[0070] 或者,报警服务可以向设备使用人员(指使用该设备的人员)输出报警信息,如向设备使用人员发送邮件、短信或微信,具体内容包括详细的报警信息以及确认是否为异常报警的提示信息,这样设备使用人员可以通过邮件、短信或微信查看报警信息,并人工确认报警信息是否为异常报警,然后通过邮件、短信或微信反馈给报警服务,如设备使用人员在确认报警信息为异常报警后,可通过邮件、短信或微信发送包含是异常报警的反馈信息给报警服务,若设备使用人员在确认报警信息不是异常报警时,也可以通过邮件、短信或微信发送包含不是异常报警的反馈信息给报警服务,这样报警服务即可根据反馈信息确定报警信息是否为异常报警。这样通过设备使用人员来判断报警信息是否为异常报警,则可以对

报警信息进行更准确的判断，这样报警服务就可以更准确地对报警信息进行相应处理。

[0071] 其中，在设备使用人员确认该报警信息是正常报警时，则报警服务可以关闭对该报警信息的推送，即关闭向设备使用人员发送邮件、短信或微信以确认该报警信息是否为异常报警，也就是说，报警服务若在后续接收到相同的报警信息后，则不再向设备使用人员发送邮件、短信或微信进行通知。并且，报警服务还可以设置关闭的时长，如关闭一天或几个小时，在关闭时长过期之后，则报警服务接收到相同的报警信息后，还会继续向设备使用人员发送提示信息。在具体实现时，在关闭时，报警服务可记录该报警信息对应的进程名称、host信息、IP地址等信息，这样在后续接收到报警信息后，若报警信息的进程名称、host信息、IP地址信息等与记录的信息一致，则在关闭时长内不向设备使用人员输出对应的提示信息。

[0072] 在上述实现过程中，通过设备使用人员来判断报警信息是否为异常报警，则可以通过人工对异常报警进行确认，更加准确。

[0073] 在上述实施例的基础上，若报警服务按照处理规则对报警信息进行处理后，若成功处理，则可以将报警信息记录到日志，若是处理失败，则可以向设备使用人员输出包含有连接设备的websockt接口的提示信息，以提示设备使用人员通过websockt接口连接设备后对报警信息进行处理。

[0074] 例如，报警服务可以实时监控运行修复脚本后的处理结果，若运行修复脚本后，对应的问题并没有得到解决，则表示报警信息没有成功得到处理，即处理失败，此时可让设备使用人员参与处理。报警服务则可向设备使用人员发送邮件、短信或微信，其内容包括有连接设备的websockt接口，设备使用人员可以通过点击websockt接口，这样就可以使得设备使用人员可以在客户端与服务端建立连接，方便设备使用人员对报警信息进行处理。

[0075] 在上述实现过程中，在自动对报警信息进行处理失败时，才通知设备使用人员进行处理，可以让设备使用人员对报警信息先进行处理，不需要通知运维人员，这样可以减少运维人员的运维压力。

[0076] 在上述实施例的基础上，在设备使用人员对报警信息进行处理后，报警服务可以获取处理结果，若处理结果为处理失败时，则报警服务可进一步向运维人员输出对报警信息进行处理的提示信息，例如，通过邮件、短信或微信等方式向运维人员发送提示信息，以进一步通知运维人员参与对报警信息的处理。这样在按照处理规则且设备使用人员对报警信息处理失败后，最后才让运维人员参与对报警信息的处理，而不是一开始就让运维人员进行处理，从而可以减少运维人员的运维压力。

[0077] 其中，在设备使用人员对报警信息进行处理后，设备使用人员可以向报警服务反馈是否处理成功的反馈信息，这样报警服务即可快速确定报警信息是否成功处理；或者，在设备使用人员在对报警信息处理完成后，报警服务自动监控出现的问题是否被修复，若被修复(例如报警信息为某个进程高负载的报警信息，则在进行处理后，查看该进程的负载是否下降，若下降到设定阈值，则可认为该问题被修复)，则确定对报警信息的处理成功，若未被修复，则确定对报警信息的处理失败。此时报警服务可以自动触发向运维人员来发送提示信息，而不是由设备使用人员来向运维人员发送提示信息，可以减少设备使用人员的操作，从而自动通知运维人员进行处理。

[0078] 在上述实施例的基础上，在设备使用人员对报警信息进行处理的过程中，报警服

务可以停止向设备使用人员输出处理其他报警信息的提示信息，换言之，在websockt接口断开之前，报警服务停止向设备使用人员输出处理其他报警信息的提示信息。这样可以避免不停地向设备使用人员输出提示信息而造成设备使用人员负担较大的问题。

[0079] 例如，报警服务可实时对websockt接口的状态进行监控，若websockt接口处于连接状态，则确定设备使用人员目前还在对报警信息进行处理过程中，若websockt接口处于断开状态，则确定设备使用人员对报警信息处理完成，在websockt接口连接到断开这一过程中，表示设备使用人员通过websockt接口与设备建立连接，并对报警信息进行处理，在这过程中，报警服务若接收到其他报警信息需要设备使用人员进行处理，则停止向设备使用人员输出提示信息，而是可以等待websockt接口断开后才向设备使用人员发送对应的提示信息，这样可以避免设备使用人员同时接收到大量的提示信息而不好选择对哪个报警信息优先处理的问题，以及可能导致设备使用人员看到需要处理大量的报警信息而产生消极情绪的问题。

[0080] 在上述实施例的基础上，若有多个报警信息需要设备使用人员处理时，则报警服务可以对这多个报警信息的处理紧急程度进行排序后，按照处理紧急程度高低依次向设备使用人员发送提示信息。

[0081] 例如，报警服务接收到多个报警信息，然后针对这多个报警信息按照对应的处理规则进行处理，若处理规则均无法处理时，则需要向设备使用人员发送提示信息，此时若向设备使用人员同时发送多个提示信息，则可以使得设备使用人员不知道该先处理哪个报警信息，为了避免这个问题，报警服务可以先对多个报警信息按照处理紧急程度进行排序。如定义木马程序的报警信息的处理紧急程度最高，其次是CPU报警的报警信息，再是内存报警的报警信息，所以可以各个报警信息所属的报警类别来确定各个报警信息的处理紧急程度，然后优先向设备使用人员发送处理紧急程度最高的报警信息的提示信息，在设备使用人员处理完该报警信息后，再向设备使用人员发送处理紧急程度次之的报警信息的提示信息，这样可以使得设备使用人员能够优先处理紧急程度高的报警信息，从而能够及时确保设备的稳定运行，及时排除设备的安全威胁问题。

[0082] 在上述实施例的基础上，在对报警信息进行处理之后，若报警信息处理成功，则可以将报警信息记录到日志中，该日志中还可以包括历史的报警信息，然后可根据日志中的报警信息分析各种报警项的报警频率，并根据报警频率输出是否加增资源或调整报警阈值的提示信息。

[0083] 其中，报警项可以根据CPU、内存、存储等方面进行划分，即报警项可以是各个报警类别下更细化的报警问题，或者报警项也可以按照报警类别进行划分，这种情况下可获取各种报警类别的报警频率。

[0084] 报警频率可以以每周或每天来进行统计，如针对内存使用率在95％以上的报警项，可统计其在一个月或两个月内的报警次数，然后获得每周报警的报警频率，如每周平均报警5次，则报警频率为5。若该报警频率高于设定值，则可输出是否增加资源或调整报警阈值的提示信息。

[0085] 增加资源可以理解为是否对设备的硬件条件进行升级等，如加装内存条、内容扩容等，报警阈值是针对报警信息设定的，如若运维人员调整报警阈值后，后可以根据报警阈值来判断是否进行报警，如内存使用率对应的报警阈值为90％，则在内存使用率高于90％

时则进行报警，如产生报警信息。

[0086] 例如，若针对内存使用率的报警频率高，则表示大多时候内存使用率都比较高，所以可以提示设备使用人员提高报警阈值，并增加资源。

[0087] 另外，在一些实施方式中，报警服务还可以将各个报警项的报警情况绘制成图像输出给运维人员，如针对内存使用率，将每次的报警信息中的内存使用率的数值绘制成柱状图输出，这样运维人员可以更直观地看到各个报警项的报警情况。

[0088] 在上述实现过程中，通过对报警信息进行分析，可以统计各个报警项的报警频率，从而输出对应的提示信息，使得相关人员能够了解各个报警项的报警情况，进而为调整报警情况提供数据依据。

[0089] 下面结合图2对上述实施方式进行介绍，如图2示出了其中一种报警信息处理方法的完整流程图，包括如下步骤：

[0090] 步骤S210：监控服务将报警信息存入CMDB中；

[0091] 步骤S220：报警服务通知设备使用人员判断报警信息是否为异常报警；

[0092] 若设备使用人员确认报警信息为正常报警，则执行步骤S230：关闭对该报警信息的报警，并将报警信息记录到日志中；若设备使用人员确认报警信息为异常报警，则执行步骤S240：根据报警类别对应的处理规则对该报警信息进行处理；

[0093] 若报警信息处理成功，则执行步骤S250：关闭对该报警信息的报警，并将报警信息记录到日志中；若报警信息处理失败，则执行步骤S260：通过日志分析模块获取备选处理规则对报警信息进行处理(针对每种报警类别可设置有处理规则和备选处理规则，先按照处理规则进行处理，若处理失败再采用备选处理规则进行处理)；

[0094] 若采用备选处理规则对报警信息处理成功，则执行步骤S270：将报警信息记录到日志中；若采用备选处理规则对报警信息进行多次处理(如三次)均处理失败，则执行步骤S280：向设备使用人员发送携带有websockt接口的提示信息；

[0095] 若设备使用人员对报警信息处理成功，则执行步骤S290：关闭对该报警信息的报警，并将报警信息记录到日志中；若设备使用人员对报警信息处理失败，则执行步骤S291：向运维人员发送处理报警信息的提示信息；

[0096] 步骤S292：通过日志分析模块对报警信息进行分析，如获取各种报警项的报警频率，并根据报警项频率输出是否增加资源或调整报警阈值的提示信息。

[0097] 所以，本申请中，可通过报警服务自动对报警信息进行处理，实现问题处理流程化，提升了问题处理的及时性，省去了一些人力成本和运维成本。

[0098] 请参照图3，图3为本申请实施例提供的一种报警信息装置300的结构框图，该装置300可以是电子设备上的模块、程序段或代码。应理解，该装置300与上述图1方法实施例对应，能够执行图1方法实施例涉及的各个步骤，该装置300具体的功能可以参见上文中的描述，为避免重复，此处适当省略详细描述。

[0099] 可选地，所述装置300包括：

[0100] 信息获取模块310，用于获取报警信息；

[0101] 类别获取模块320，用于若所述报警信息为异常报警，则获取所述报警信息所属的报警类别；

[0102] 规则获取模块330，用于从处理规则库中获取所述报警类别对应的处理规则；

[0103] 报警处理模块340,用于按照所述处理规则对所述报警信息进行处理。

[0104] 可选地,通过以下方式判断所述报警信息是否为异常报警:

[0105] 判断所述报警信息是否为异常报警信息中的一种;

[0106] 若是,则确定所述报警信息为异常报警;或者向设备使用人员输出所述报警信息;

[0107] 若接收到所述设备使用人员针对所述报警信息的反馈信息为异常报警时,则确定所述报警信息为异常报警。

[0108] 可选地,所述报警处理模块340,还用于若按照所述处理规则对所述报警信息处理失败,则向设备使用人员输出包含有连接设备的websockt接口的提示信息,以提示所述设备使用人员通过所述websockt接口连接所述设备后对所述报警信息进行处理。

[0109] 可选地,所述报警处理模块340,还用于若确定所述设备使用人员对所述报警信息处理失败,则向运维人员输出对所述报警信息进行处理的提示信息。

[0110] 可选地,所述报警处理模块340,还用于在所述websockt接口断开之前,停止向所述设备使用人员输出处理其他报警信息的提示信息。

[0111] 可选地,所述信息获取模块310,用于从配置管理数据库CMDB中获取报警信息。

[0112] 可选地,所述报警处理模块340,还用于若对所述报警信息处理成功,则将所述报警信息记录到日志中,所述日志中还包括历史的报警信息;根据所述日志中的报警信息分析各种报警项的报警频率;根据所述报警频率输出是否加增资源或调整报警阈值的提示信息。

[0113] 需要说明的是,本领域技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的装置的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再重复描述。

[0114] 请参照图4,图4为本申请实施例提供的一种用于执行报警信息处理方法的电子设备的结构示意图,所述电子设备可以包括:至少一个处理器410,例如CPU,至少一个通信接口420,至少一个存储器430和至少一个通信总线440。其中,通信总线440用于实现这些组件直接的连接通信。其中,本申请实施例中设备的通信接口420用于与其他节点设备进行信令或数据的通信。存储器430可以是高速RAM存储器,也可以是非易失性的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器430可选的还可以是至少一个位于远离前述处理器的存储装置。存储器430中存储有计算机可读取指令,当所述计算机可读取指令由所述处理器410执行时,电子设备执行上述图1所示方法过程。

[0115] 可以理解,图4所示的结构仅为示意,所述电子设备还可包括比图4中所示更多或者更少的组件,或者具有与图4所示不同的配置。图4中所示的各组件可以采用硬件、软件或其组合实现。

[0116] 本申请实施例提供一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时,执行如图1所示方法实施例中电子设备所执行的方法过程。

[0117] 本实施例公开一种计算机程序产品,所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,所述计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的方法,例如,包括:获取报警信息;若所述报警信息为异常报警,则获取所述报警信息所属的报警类别;从处理规则库中获取所述报警类别对应的处理规则;按照所述处理规则对所述报警信息进行处理。

[0118] 综上所述,本申请实施例提供一种报警信息处理方法、装置、电子设备及可读存储

介质，通过在报警信息为异常报警时，获取报警信息所属的报警类别，然后从处理规则库中获取该报警类别对应的处理规则，并按照处理规则对报警信息进行处理，这样可以使得设备在出现异常报警时，可以优先按照规则实现自动处理，无需通知运维人员，能够及时对异常报警进行处理，节省了运维时间。

[0119] 在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0120] 另外，作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0121] 再者，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0122] 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。

[0123] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

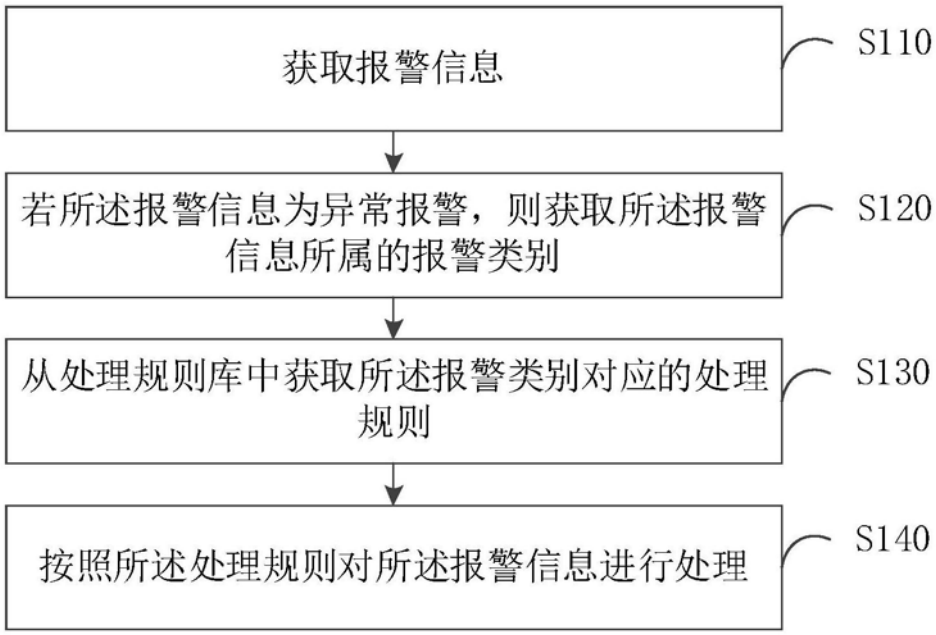

获取报警信息
S110
若所述报警信息为异常报警，则获取所述报警信息所属的报警类别
S120
从处理规则库中获取所述报警类别对应的处理规则
S130
按照所述处理规则对所述报警信息进行处理
S140

图1

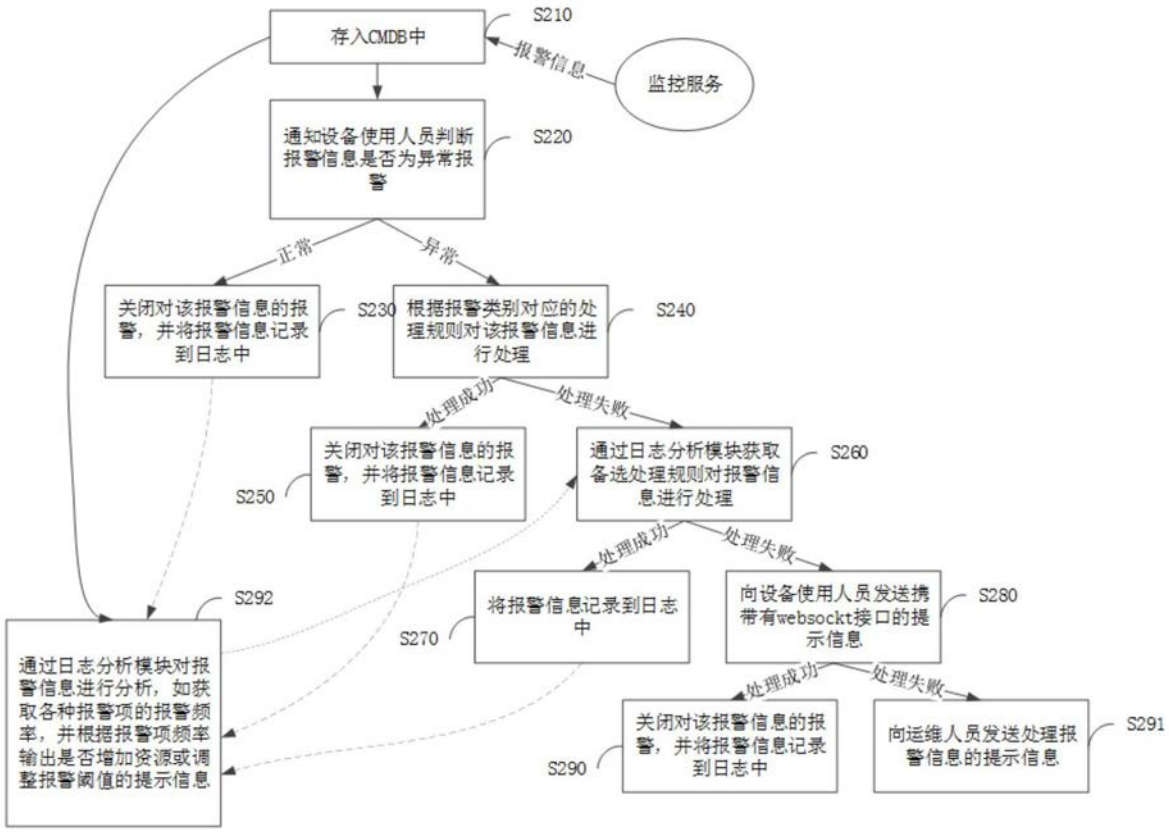

存入CMDB中
S210
报警信息
监控服务
通知设备使用人员判断报警信息是否为异常报警
S220
正常
异常
关闭对该报警信息的报警，并将报警信息记录到日志中
S230
根据报警类别对应的处理规则对该报警信息进行处理
S240
处理成功
处理失败
关闭对该报警信息的报警，并将报警信息记录到日志中
S250
通过日志分析模块获取备选处理规则对报警信息进行处理
S260
处理成功
处理失败
将报警信息记录到日志中
S270
向设备使用人员发送携带有websockt接口的提示信息
S280
处理成功
处理失败
关闭对该报警信息的报警，并将报警信息记录到日志中
S290
向运维人员发送处理报警信息的提示信息
S291
通过日志分析模块对报警信息进行分析，如获取各种报警项的报警频率，并根据报警项频率输出是否增加资源或调整报警阈值的提示信息
S292

图2

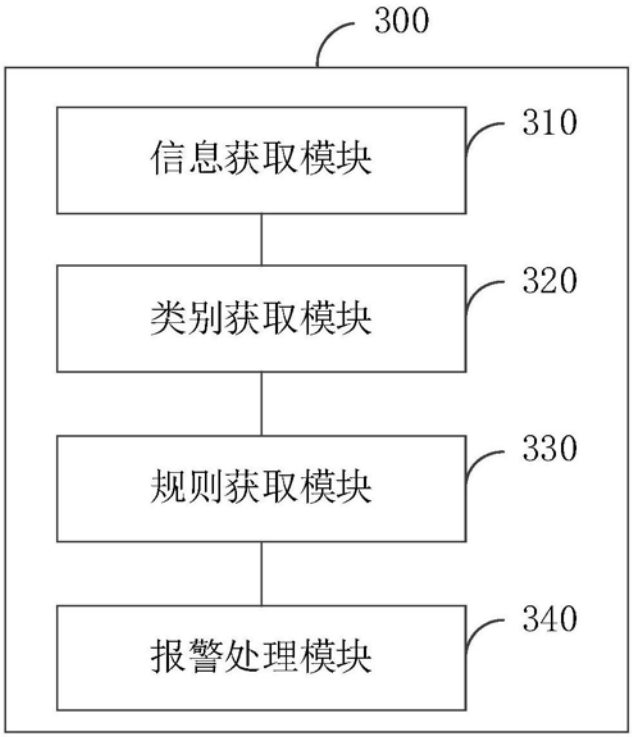

300
信息获取模块
310
类别获取模块
320
规则获取模块
330
报警处理模块
340

图3

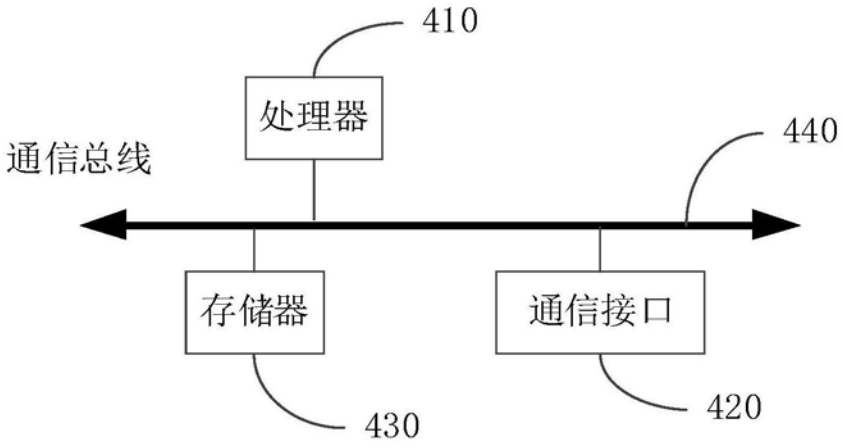

410
处理器
通信总线
440
存储器
通信接口
430
420

图4