

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 9 月 14 日 (14.09.2017)



(10) 国际公布号
WO 2017/152763 A1

- (51) 国际专利分类号:
G06F 11/07 (2006.01)
- (21) 国际申请号: PCT/CN2017/074618
- (22) 国际申请日: 2017 年 2 月 23 日 (23.02.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610136817.0 2016 年 3 月 10 日 (10.03.2016) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 张文 (ZHANG, Wen) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (CN)。

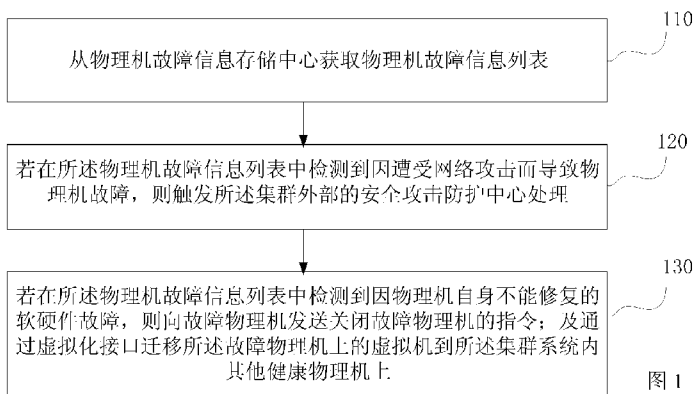
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: PHYSICAL MACHINE FAILURE CLASSIFICATION HANDLING METHOD AND DEVICE, AND VIRTUAL MACHINE RECOVERY METHOD AND SYSTEM

(54) 发明名称: 物理机故障分类处理方法、装置和虚拟机恢复方法、系统



- 110 OBTAIN A PHYSICAL MACHINE FAILURE INFORMATION LIST FROM A PHYSICAL MACHINE FAILURE INFORMATION STORAGE CENTER
- 120 IF A PHYSICAL MACHINE FAILURE CAUSED BY A NETWORK ATTACK IS DETECTED IN THE PHYSICAL MACHINE FAILURE INFORMATION LIST, TRIGGER AN ATTACK PREVENTION AND PROTECTION SECURITY CENTER OUTSIDE A CLUSTER FOR HANDLING
- 130 IF A SOFTWARE/HARDWARE FAILURE THAT CANNOT BE FIXED BY A PHYSICAL MACHINE IS DETECTED IN THE PHYSICAL MACHINE FAILURE INFORMATION LIST, SEND A FAILED PHYSICAL MACHINE TURN-OFF INSTRUCTION TO THE FAILED PHYSICAL MACHINE; AND MIGRATE THE VIRTUAL MACHINE ON THE FAILED PHYSICAL MACHINE TO ANOTHER HEALTHY PHYSICAL MACHINE IN THE CLUSTERED SYSTEM BY MEANS OF A VIRTUALIZED INTERFACE

图 1

(57) Abstract: A clustered physical machine failure classification handling method and device, and virtual machine recovery method and system. The physical machine failure classification handling method comprises: obtaining a physical machine failure information list from a physical machine failure information storage center (110); if a physical machine failure caused by a network attack is detected in the physical machine failure information list, triggering an attack prevention and protection security center outside a cluster for handling (120); if a software/hardware failure that cannot be fixed by a physical machine is detected in the physical machine failure information list, sending a failed physical machine turn-off instruction to the failed physical machine; and migrating the virtual machine on the failed physical machine to another healthy physical machine in the clustered system by means of a virtualized interface (130). By refined, quick and accurate recognition of failures in multiple physical machine failure scenes and targeted classification handling, the method implements quick and highly-reliable physical machine failure recovery, thereby ensuring quick recovery of virtual machine services on the physical machines.

(57) 摘要:

[见续页]



一种集群物理机故障分类处理方法、装置及虚拟机恢复方法、系统。所述物理机故障分类处理方法包括：从物理机故障信息存储中心获取物理机故障信息列表（110）；若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理（120）；若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上（130）。该方法通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

物理机故障分类处理方法、装置和虚拟机恢复方法、系统

技术领域

本申请涉及通信技术领域，特别是涉及一种应用于虚拟化集群系统的物理机故障分类处理方法、装置及虚拟机恢复方法、系统。

5 背景技术

随着计算机技术的迅猛发展，人们开始越来越多的关注如何降低能耗和提高资源利用率，云计算模式应运而生。云计算将所有的计算机抽象成特定的计算资源，然后将这些计算资源提供给用户，而不是像传统那样直接提供一台或多台计算机。云计算模式最大的好处就是用户可以根据自己的需要来申请资源，避免不必要的资源浪费，提高资源利用率。

在云计算环境中，虚拟化集群技术是关键技术之一。虚拟化集群将多台虚拟化服务器组成为一个有机的整体，从而获得很高的计算速度，提升虚拟化系统整体的计算能力。虚拟化集群对多台服务器进行统一管理，通过虚拟化技术将物理资源抽象为存储、计算、网络等各种资源组成大的资源池，通过按需申请资源的方式提供虚拟机给用户。

随着虚拟化集群规模的逐渐扩大，由于集群内物理机软硬件问题导致物理机故障的概率也逐渐增大。物理机故障会直接影响其上所运行的虚拟机服务。为了保证虚拟机业务的正常运行，需要及时发现其所在的物理机故障并迅速处理以恢复虚拟机业务；否则，虚拟机用户会受到物理机故障的影响，无法保证业务的连续性。现有技术可以定时监控物理机状态，当发生物理机故障时，则会对其上的虚拟机进行关机，然后再开机操作；或者是关闭故障物理机，将其上的虚拟机迁移到集群内其他物理机上。

然而，物理机故障通常是由不同的原因而导致的，且物理机故障的现象也会有很多种，而现有技术并未对物理机故障进行精细划分，并未针对性的进行分类处理，因此在实际商业化用途中会存在较多的误判和漏判的情况，从而实现物理机故障后其上的虚拟机高可用（High Availability, HA）。

因此,如何更准确、高效、有针对性地进行物理机故障分类修复处理,成为亟需本领域技术人员解决的技术问题。

发明内容

5 鉴于上述问题,提出了本申请实施例以便提供一种克服上述问题或者至少部分地解决上述问题的一种应用于虚拟化集群系统的物理机故障分类处理方法、装置及虚拟机恢复方法、系统。

本申请公开一种集群物理机故障分类处理方法,包括:

从物理机故障信息存储中心获取物理机故障信息列表;

10 若在上述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障,则触发所述集群外部的安全攻击防护中心处理;

若在上述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障,则向故障物理机发送关闭故障物理机的指令;及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

本申请还公开了一种集群物理机故障分类处理装置,包括:

15 获取模块,用于从物理机故障信息存储中心获取物理机故障信息列表;

第一处理模块,用于若在上述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障,则触发所述集群外部的安全攻击防护中心处理;

第二处理模块,进一步包括:

20 关闭处理单元,用于若在上述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障,则向故障物理机发送关闭故障物理机的指令;

迁移处理单元,用于通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

本申请还公开了一种虚拟机恢复方法,应用于虚拟化集群系统,所述方法包括:

虚拟化集群系统内的物理机自主检测自身的故障动态;

若自主检测到物理机自身能容错修复的软硬件故障, 通过容错方式修复;

5 若自主检测到物理机自身能重启修复的软硬件故障, 通过重启物理机方式修复;

从物理机故障信息存储中心获取物理机故障信息列表;

若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障, 则触发所述集群外部的安全攻击防护中心处理;

10 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令; 及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

相应的, 本申请公开了一种虚拟机恢复系统, 包括:

15 物理机故障修复装置, 应用于虚拟化集群系统内的物理机上自主检测物理机自身的故障动态, 若自主检测到物理机自身能容错修复的软硬件故障, 通过容错方式修复; 若自主检测到物理机自身能重启修复的软硬件故障, 通过重启物理机方式修复;

物理机故障信息存储中心, 用于将所有上报的物理故障信息汇集成物理机故障信息列表;

20 物理机故障分类处理装置, 用于从所述物理机故障信息存储中心获取物理机故障信息列表, 若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障, 则触发所述集群外部的安全攻击防护中心处理; 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令, 及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

25 根据本申请提供的具体实施例, 本申请公开了以下技术效果:

本申请实施例可以在大规模的云计算集群中, 通过对多种物理机故障

场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并有针对性的采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机的频繁迁移而影响系统性能情况的发生。

当然，实施本申请的任一产品并不一定需要同时达到以上所述的所有优点。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，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的附图。

图1是本申请的一种集群物理机故障分类处理方法实施例的步骤流程图；

图 2 是本申请的另一种集群物理机故障分类处理方法实施例的步骤流程图；

图 3 是本申请的一种虚拟机恢复方法实施例的步骤流程图；

图 4 是本申请的另一种虚拟机恢复方法实施例的步骤流程图；

5 图 5 是本申请的一种物理机故障修复装置实施例的结构框图；

图 6 是本申请的一种集群物理机故障分类处理装置实施例的结构框图；

图 7 是本申请的一种虚拟机恢复系统实施例的结构框图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，
10 而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

15 为了方便理解本发明实施例，首先在此介绍本发明实施例描述中会涉及的几个要素：

A、云计算

云计算是一种基于互联网技术的相关服务的增加、使用和交付模式，是在所有使用的服务器上实践分布式计算的服务器集群。也就是说，云计算
20 算提供了一个虚拟化的按需动态供应硬件、软件和数据集的弹性资源平台。

B、虚拟集群

在云计算平台上进行集群管理就构成了虚拟集群。所谓的虚拟集群就是通过采用虚拟化技术来虚拟出多台计算节点，从而构建出与物理集群相似而且规模巨大的一个集群系统。也就是说，虚拟集群就是将那些协同完
25 成特定任务的多台同构或异构的计算机连接起来的系统。

C、物理机

虚拟集群系统内协同完成特定任务的多台计算机即为集群物理计算机，简称集群物理机。其中，一台物理机上可以模拟出一台或者多台虚拟的计算机。

D、虚拟机

通过虚拟机软件可以在一台物理机上模拟出一台或者多台虚拟的计算机，而这些虚拟机就像真正的计算机那样进行工作，虚拟机上可以安装操作系统和应用程序，虚拟机还可访问网络资源。对于在虚拟机中运行的应用程序而言，虚拟机就像是在真正的计算机中进行工作。

本申请实施例可以应用在大规模的云计算虚拟化集群系统中，可以通过集群系统内的物理机自主检测自身的故障动态，进而对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；而对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

影响虚拟机运行和管理的物理机故障现象可以归纳如下几种：

1、物理机网络不通

其原因主要包括：物理机宕机、网卡异常、上联交换机故障、硬件异常、内核模块异常、物理机重启、网络分布式拒绝服务攻击（Distributed Denial of Service, DDoS）等。

2、物理机丢包

其原因主要包括：物理机负载高、上联网络设备切换、网络 DdoS 攻击等。

3、物理机硬件系统故障

例如，物理机磁盘、内存、中央处理器（Central Processing Unit, CPU）故障等。

4、物理机软件异常

例如，物理机的文件系统、虚拟化相关模块、操作系统内核模块等操作系统层面的软件异常等。

5、物理机远程访问通道不通

5 其原因主要包括：网络丢包、系统服务异常、文件系统异常等。

6、物理机性能异常

例如，可能表现为物理机输入输出（Input/Output，I/O）卡顿、负载高等。其原因主要包括：物理机硬件故障、物理机内核模块异常、物理机用户态进程异常等。

10 可以看出，以上物理机故障的现象并不是一成不变的，而是在一定时间内可以相互转化的，甚至是相关关联、相互交织的。并且，相同的物理机现象其背后的原因可能不一样，因此故障物理机的修复处理方式需要具体区分，例如，对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的，如果在物理机正
15 遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机，会产生骨牌效应，导致扩大故障风险，即其他物理机陆续被攻击而不可用，最终可能造成全集群网络设备的泛洪（flooding），导致全集群物理机故障风险。

基于上述物理机故障现象和异常的深层原因分析，本发明实施例中，可以将物理机故障归纳为如下几类：

20 A、物理机自身能容错修复的软硬件故障类型

例如，存储数据的磁盘故障、虚拟化相关内核模块异常、存储数据的文件系统异常等。

B、物理机自身能重启修复的软硬件故障类型

例如，根文件系统只读等异常、网卡驱动重启可修复的异常、操作系
25 统内核模块异常等。

C、物理机自身不能修复的软硬件故障类型

例如，物理机宕机、物理机 CPU 异常、物理机内存异常、物理机电源模块等各类硬件问题异常。

另外，还包括未知原因的故障类型，例如，系统负载类、系统网络类、
5 硬件故障类等。这类故障虽然本质的原因比较难查，但是这类故障的现象却很明确，主要是：物理机网络丢包、物理机管理通道访问异常、物理机性能使用异常。

D、物理机遭受网络攻击而导致物理机故障类型

例如，网络 DDoS 类型安全攻击，从而造成网络大量丢包甚至网络不
10 通。这类故障的现象主要包括：物理机网络不通、网络丢包、管理通道不通等。

因此，本申请实施例通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。例如，本申
15 请实施例可以在十几分钟内处理完成故障物理机上的虚拟机恢复且该虚拟机的功能具备超过 99.95% 的商用可用性标准。

实施例一

参照图 1，示出了本申请的一种集群物理机故障分类处理方法实施例
20 的步骤流程图，所述物理机故障分类处理方法可以应用于虚拟化集群系统，具体可以包括如下步骤：

步骤 210，从物理机故障信息存储中心获取物理机故障信息列表；

需要说明的是，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息
25 存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故

障信息。

步骤 220, 若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障, 则触发所述集群外部的安全攻击防护中心处理;

可以理解的是, 在实际应用中, 所述集群外部的安全攻击防护中心被
5 触发后, 会启动安全清洗程序, 例如进行流量清洗等, 从而使得故障物理机恢复健康。需要说明的是, 对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的, 如果在物理机正遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机, 会产生骨牌效应, 导致扩大故障风险, 即其他物理机陆续被攻击而不可用,
10 最终可能造成全集群网络设备的泛洪 (flooding), 导致全集群物理机故障风险。

步骤 230, 若在所述物理机故障信息列表中检测到因物理机自身不能
修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令; 及通过
15 虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上;

优选的, 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块。

需要说明的是, 所述的物理机自身不能修复的软硬件故障类型可以包
20 括: 物理机宕机、物理机 CPU 异常、物理机内存异常、物理机电源模块等各类硬件问题异常。这类故障会直接导致物理机不可用, 且需要更换硬件模块方可修复, 因此, 本申请实施例通过从集群中将故障物理机隔离后再对故障物理机进行硬件更换或者维护。

此外, 针对物理机自身不能修复的软硬件故障的情况下, 传统物理机
25 上的带外管控系统由于硬件故障率和成本问题, 通常可用性在 90% 左右甚至更低, 在云计算服务本身至少 99.95% 的商用可用性要求下, 全年的不可用性时长共计 262.8 分钟, 如果一台故障物理机无法得到及时修复, 则由于一台物理机故障就会直接导致几十分钟的人工处理时耗, 因此, 现有技

术中的带外管控系统的可用性指标无法匹配商用云计算服务的故障恢复服务等级协议(Service-Level Agreement, SLA)。而本申请实施例提供的技术方案,对传统的带外管控系统进行改进,在带外管理模块可用性达不到商用标准时,可以通过所述集群外部的物理机故障分类处理模块的指令指示故障物理机自主关闭,再由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上;从而大量缩短故障物理机的修复时间,进而提高系统的商用可用性。

本申请实施例可以在大规模的云计算集群中,通过对多种物理机故障场景,进行精细化故障快速、准确的识别,并有针对性的进行分类处理,从而实现快速、高可靠的物理机故障修复处理,以保证其上的虚拟机服务的快速恢复。

另外,本申请实施例针对物理机自身不能修复的物理机故障情况,除了可以通过故障物理机上的带外管理模块关闭故障物理机之外,还可以通过集群外部的物理机故障分类处理模块,指示故障物理机自主关机,从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题,同时也确保自动化物理机隔离的有效性。

实施例二

参照图 2,示出了本申请的另一种集群物理机故障分类处理方法实施例的步骤流程图,具体可以包括如下步骤:

步骤 210,从物理机故障信息存储中心获取物理机故障信息列表;

需要说明的是,所述物理机故障信息列表包括:由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息,及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

步骤 220, 若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障, 则触发所述集群外部的安全攻击防护中心处理;

可以理解的是, 在实际应用中, 所述集群外部的安全攻击防护中心被触发后, 会启动安全清洗程序, 例如进行流量清洗等, 从而使得故障物理机恢复健康。需要说明的是, 对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的, 如果在物理机正遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机, 会产生骨牌效应, 导致扩大故障风险, 即其他物理机陆续被攻击而不可用, 最终可能造成全集群网络设备的泛洪 (flooding), 导致全集群物理机故障风险。

步骤 230, 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令; 及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上;

优选的, 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块。

需要说明的是, 所述的物理机自身不能修复的软硬件故障类型可以包括: 物理机宕机、物理机 CPU 异常、物理机内存异常、物理机电源模块等各类硬件问题异常。这类故障会直接导致物理机不可用, 且需要更换硬件模块方可修复, 因此, 本申请实施例通过从集群中将故障物理机隔离后再对故障物理机进行硬件更换或者维护。

此外, 针对物理机自身不能修复的软硬件故障的情况下, 传统物理机上的带外管控系统由于硬件故障率和成本问题, 通常可用性在 90% 左右甚至更低, 在云计算服务本身至少 99.95% 的商用可用性要求下, 全年的不可用性时长共计 262.8 分钟, 如果一台故障物理机无法得到及时修复, 则由于一台物理机故障就会直接导致几十分钟的人工处理时耗, 因此, 现有技术中的带外管控系统的可用性指标无法匹配商用云计算服务的故障恢复

服务等级协议(Service-Level Agreement, SLA)。而本申请实施例提供的技术方案,对传统的带外管控系统进行改进,在带外管理模块可用性达不到商用标准时,可以通过所述集群外部的物理机故障分类处理模块的指令指示故障物理机自主关闭,再由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上;从而大量缩短故障物理机的修复时间,进而提高系统的商用可用性。

步骤 240,若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间;判断网络不通的物理机数量是否超过预设数量,如果是则通知运营维修人员人工修复;否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上;

其中,所述预设时间可以依据实际情况设定为 3 分钟、5 分钟等适合的时间段。

需要说明的是,在检测到物理机网络完全不通且网络不通持续时间达到预设时间的情况下,本申请实施例需要进一步检查网络不通的故障物理机的数量是否超过一个机柜的物理机数量或者一个交换机下联物理机数量,如果超过,则认为是集群规模性网络故障,则需要采取电话报警通知运营维修人员人工修复,而不再自动处理。这是由于对于大规模物理机故障,在进行隔离物理机迁移虚拟机时,会导致大量物理机被关闭,当机房设备(网络设备或者电力设备等)恢复后,还需要再次重启物理机,然后恢复虚拟机,这一系列的操作将直接导致人工处理时间加倍甚至更多,从而大大加大虚拟机的不可用时长。因此,本申请实施例提供的方法,对此种物理机故障类型加以区分处理,可以大量缩短故障物理机的修复时间,从而大大缩短其上的虚拟机不可用的时长,进而提高系统的商用可用性。

优选的,本申请实施例所述方法还可以进一步包括:

步骤 250,若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常,且确定物理机网络不通是物理机重启所导致的,则判断当前的物理机是否健康,如果健康则

通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上；

步骤 260，若在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上；

需要说明的是，所述物理机网络不稳定且网络不稳定持续时间达到预设时间的情况主要是一些未知原因造成物理机故障，例如，系统负载类、系统网络类、硬件故障类等。这类故障虽然本质原因比较难查，但是这类故障的现象却很明确，主要是：物理机网络丢包、物理机管理通道访问异常、物理机性能使用异常。对于这类物理机故障，可以采用相同的处理方式，即向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，在本申请的一个实施例中，通过以下方式确定所述健康物理机：

在所述物理机故障信息列表中匹配所述集群内的所有物理机；

将没有匹配成功的物理机确定为健康物理机。

本申请实施例可以在大规模的云计算集群中，通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和

漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而
5 弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并
10 有针对性的采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机的频繁迁移而影响系统性能情况的发生。

实施例三

参照图 3，示出了本申请的一种虚拟机恢复方法的实施例示意图，具体
15 可以包括如下步骤：

步骤 310，虚拟化集群系统内的物理机自主检测自身的故障动态；

优选的，每台物理机可以以固定的时间间隔定期自主检测自身的故障动态，例如每隔 30 秒自主检测一次。

步骤 320，若自主检测到物理机自身能容错修复的软硬件故障，通过
20 容错方式修复；

可以理解的是，本申请实施例所述的物理机自身能容错修复的软硬件故障，可以包括：存储数据的磁盘故障、虚拟化相关内核模块异常、存储数据的文件系统异常等。例如，针对存储数据的磁盘故障，容错修复方式
25 具体是，首先隔离磁盘，然后利用集群分布式存储多份数据的机制，实现该磁盘上数据自动复制至其他健康磁盘上，这样可以有效保证该故障磁盘隔离后不会影响系统稳定运行。同样，针对存储数据的文件系统损坏，也

可以通过隔离该文件系统挂载的磁盘达到容错修复的目的。

步骤 330, 若自主检测到物理机自身能重启修复的软硬件故障, 通过重启物理机方式修复;

可以理解的是, 本申请实施例所述的物理机自身能修复的软硬件故障, 可以包括: 根文件系统只读等异常、网卡驱动重启可修复的异常、操作系统内核模块异常等。这类软硬件故障都可以通过重启物理机的方式予以修复。

步骤 340, 从物理机故障信息存储中心获取物理机故障信息列表;

需要说明的是, 由物理机故障分类处理模块从物理机故障信息存储中心获取物理机故障信息列表。所述物理机故障信息列表包括: 由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息, 及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

步骤 350, 若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障, 则触发所述集群外部的安全攻击防护中心处理;

可以理解的是, 在实际应用中, 所述集群外部的安全攻击防护中心被触发后, 会启动安全清洗程序, 例如进行流量清洗等, 从而使得故障物理机恢复健康。需要说明的是, 对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的, 如果在物理机正遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机, 会产生骨牌效应, 导致扩大故障风险, 即其他物理机陆续被攻击而不可用, 最终可能造成全集群网络设备的泛洪 (flooding), 导致全集群物理机故障风险。

步骤 360, 若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机; 及

通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

需要说明的是，所述的物理机自身不能修复的软硬件故障类型可以包括：物理机宕机、物理机 CPU 异常、物理机内存异常、物理机电源模块等
5 各类硬件问题异常。这类故障会直接导致物理机不可用，且需要更换硬件模块方可修复，因此，本申请实施例通过从集群中将故障物理机隔离后再对故障物理机进行硬件更换或者维护。

此外，针对物理机自身不能修复的软硬件故障的情况下，传统物理机上的带外管控系统由于硬件故障率和成本问题，通常可用性在 90%左右甚至更低，在云计算服务本身至少 99.95%的商用可用性要求下，全年的不可
10 可用性时长共计 262.8 分钟，如果一台故障物理机无法得到及时修复，则由于一台物理机故障就会直接导致几十分钟的人工处理时耗，因此，现有技术中的带外管控系统的可用性指标无法匹配商用云计算服务的故障恢复服务等级协议(Service-Level Agreement, SLA)。而本申请实施例提供的技术
15 方案，对传统的带外管控系统进行改进，在带外管理模块可用性达不到商用标准时，可以通过所述集群外部的物理机故障分类处理模块的指令指示故障物理机自主关闭，再由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上；从而大量缩短故障物理机的修复时间，进而提高系统的商用
20 可用性。

优选的，本申请实施例所述方法还可以进一步包括：

步骤 370，若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间；判断网络不通的物理机数量是否超过预设数量，如果是则通知运营维修人员人工修复；否则通过虚拟化接口
25 迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

其中，所述预设时间可以依据实际情况设定为 3 分钟、5 分钟等适合的时间段。

需要说明的是，在检测到物理机网络完全不通且网络不通持续时间达

到预设时间的情况下，本申请实施例需要进一步检查网络不通的故障物理机的数量是否超过一个机柜的物理机数量或者一个交换机下联物理机数量，如果超过，则认为是集群规模性网络故障，则需要采取电话报警通运营维修人员人工修复，而不再自动处理。这是由于对于大规模物理机故障，

5 在进行隔离物理机迁移虚拟机时，会导致大量物理机被关闭，当机房设备（网络设备或者电力设备等）恢复后，还需要再次重启物理机，然后恢复虚拟机，这一系列的操作将直接导致人工处理时间加倍甚至更多，从而大大加大虚拟机的不可用时长。因此，本申请实施例提供的方法，对此种物理机故障类型加以区分处理，可以大量缩短故障物理机的修复时间，从而

10 大大缩短其上的虚拟机不可用的时长，进而提高系统的商用可用性。

优选的，本申请实施例所述方法还可以进一步包括：

步骤 380，若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则

15 通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

优选的，本申请实施例所述方法还可以进一步包括：

步骤 390，若在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

20

需要说明的是，所述物理机网络不稳定且网络不稳定持续时间达到预设时间的情况主要是一些未知原因造成物理机故障，例如，系统负载类、系统网络类、硬件故障类等。这类故障虽然本质原因比较难查，但是这类故障的现象却很明确，主要是：物理机网络丢包、物理机管理通道访问异常、物理机性能使用异常。对于这类物理机故障，可以采用相同的处理方式，即向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机

25

或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，在本申请的一个实施例中，通过以下方式确定所述健康物理机：

5 在所述物理机故障信息列表中匹配所述集群内的所有物理机；

将没有匹配成功的物理机确定为健康物理机。

本申请实施例可以在大规模的云计算集群中，通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并有针对性的采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机的频繁迁移而影响系统性能情况的发生。

实施例四

参照图 4，示出了本申请的另一种虚拟机恢复方法的实施例示意图，具体可以包括如下步骤：

物理机故障探测模块每隔 30 秒检查集群内每台物理机的网络情况，并更新至物理机故障信息存储中心；集群系统内的每台物理机自主检测自身的故障情况，并通过物理机故障收集模块更新至物理机故障信息存储中心。

对于物理机自身能容错修复的软硬件故障的场景，则由物理机自身通过容错方式修复处理；对于物理机自身能重启修复的软硬件故障，则由物理机自身通过重启物理机方式修复处理；如果是物理机自身不能修复的软硬件故障，则进行关机处理。

物理机故障分类处理模块每隔 1 分钟从物理机故障信息存储中心获取物理机故障信息列表；判断该物理机故障信息列表是否为空，如果是则返回循环；否则继续判断所述物理机故障信息列表中是否有因遭受网络攻击而导致物理机故障的情况，如果有，则触发所述集群外部的安全攻击防护中心处理；否则继续判断在所述物理机故障信息列表中是否有因物理机自身不能修复的软硬件故障的情况，如果有，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；再通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

如果确定所述物理机故障信息列表中没有因遭受网络攻击而导致物理机故障的情况，则继续判断在所述物理机故障信息列表中是否有物理机网络完全不通且网络不通持续时间达到预设时间，例如 3 分钟；如果有则再判断网络不通的物理机数量是否超过预设数量，例如，故障物理机的数量是否超过一个机柜的物理机数量或者一个交换机下联物理机数量，如果超过，则认为是集群规模性网络故障，则需要采取电话报警通运营维修人员人工修复，而不再自动处理。否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

判断在所述物理机故障信息列表中是否有检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

如果在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

需要说明的是，所述物理机网络不稳定且网络不稳定持续时间达到预设时间的情况主要是一些未知原因造成物理机故障，例如，系统负载类、系统网络类、硬件故障类等。这类故障虽然本质原因比较难查，但是这类故障的现象却很明确，主要是：物理机网络丢包、物理机管理通道访问异常、物理机性能使用异常。对于这类物理机故障，可以采用相同的处理方式。

优选的，在本申请的一个实施例中，通过以下方式确定所述健康物理机：

在所述物理机故障信息列表中匹配所述集群内的所有物理机；

将没有匹配成功的物理机确定为健康物理机。

本申请实施例可以在大规模的云计算集群中，通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处

理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并有针对性地采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机的频繁迁移而影响系统性能情况的发生。

需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请实施例所必须的。

实施例五

参照图 5，示出了本申请的一种物理机故障修复装置实施例的结构框图，所述物理机故障修复装置 500 应用于虚拟化集群系统内的物理机上，具体可以包括：自主检测模块(selfChecker)510、自主处理模块(selfHandler)520；其中：

自主检测模块 510 具体包括：检测单元 511，用于自主检测物理机自身的故障动态；优选的，检测单元 511 可以以固定的时间间隔定期自主检测物理机自身的故障动态，例如每隔 30 秒自主检测一次。

自主处理模块 520，具体包括：

容错单元 521，用于若所述检测单元 511 检测到物理机自身能容错修复的软硬件故障，则通过容错方式修复；

可以理解的是，本申请实施例所述的物理机自身能容错修复的软硬件故障，可以包括：存储数据的磁盘故障、虚拟化相关内核模块异常、存储数据的文件系统异常等。例如，针对存储数据的磁盘故障，容错修复方式具体是，首先隔离磁盘，然后利用集群分布式存储多份数据的机制，实现该磁盘上数据自动复制至其他健康磁盘上，这样可以有效保证该故障磁盘隔离后不会影响系统稳定运行。同样，针对存储数据的文件系统损坏，也可以通过隔离该文件系统挂载的磁盘达到容错修复的目的。

重启单元 522，用于若所述检测单元 511 检测到物理机自身能重启修复的软硬件故障，则通过重启物理机方式修复。

可以理解的是，本申请实施例所述的物理机自身能重启修复的软硬件故障，可以包括：根文件系统只读等异常、网卡驱动重启可修复的异常、操作系统内核模块异常等。这类软硬件故障都可以通过重启物理机的方式予以修复。

优选的，所述自主处理模块 520 还可以进一步包括：

关机单元 523，用于若所述检测单元 511 检测到物理机自身不能修复的软硬件故障，则根据所述集群外部的物理机故障分类处理模块的指令或通过所述物理机上的带外管理模块 530 关闭故障物理机，由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

需要说明的是，针对物理机自身不能修复的软硬件故障的情况下，传统物理机上的带外管控系统由于硬件故障率和成本问题，通常可用性在 90% 左右甚至更低，在云计算服务本身至少 99.95% 的商用可用性要求下，全年的不可用性时长共计 262.8 分钟，如果一台故障物理机无法得到及时修复，则由于一台物理机故障就会直接导致几十分钟的人工处理时耗，因此，现

有技术中的带外管控系统的可用性指标无法匹配商用云计算服务的故障恢复服务等级协议(Service-Level Agreement, SLA)。而本申请实施例提供的技术方案,对传统的带外管控系统进行改进,在带外管理模块 530 可用性达不到商用标准时,可以通过所述集群外部的物理机故障分类处理模块的指令指示故障物理机自主关闭,再由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上;从而大量缩短故障物理机的修复时间,进而提高系统的商用可用性。

优选的,所述自主检测模块 510 还可以进一步包括:

- 10 上报单元 512,用于当检测单元 511 自主检测到因遭受网络攻击而导致物理机故障时,通过物理机故障收集模块上报物理机故障信息到物理机故障信息存储中心,由所述集群外部的物理机故障分类处理模块触发所述集群外部的安全攻击防护中心处理。

- 15 其中,所述集群外部的安全攻击防护中心被触发后,会启动安全清洗程序,例如进行流量清洗等,从而使得故障物理机恢复健康。需要说明的是,对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的,如果在物理机正遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机,会产生骨牌效应,导致扩大故障风险,即其他物理机陆续被攻击而不可用,最终可能造成全集群网络设备的泛洪(flooding),导致全集群物理机故障风险。
- 20

本申请实施例可以在大规模的云计算集群中,通过对多种物理机故障场景,进行精细化故障快速、准确的识别,并有针对性的进行分类处理,从而实现快速、高可靠的物理机故障修复处理,以保证其上的虚拟机服务的快速恢复。

- 25 进一步的,本申请实施例通过物理机自主检测自身的故障动态,并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理;对物理机自身不能修复的物理机故障情况,通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理,从而有效降低物理机故障的误判和

漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而
5 弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

实施例六

参照图 6，示出了本申请的一种集群物理机故障分类处理装置实施例
10 的结构框图，所述物理机故障分类处理装置 600 具体可以包括如下模块：

获取模块 610，用于从物理机故障信息存储中心获取物理机故障信息列表；需要说明的是，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块
15 从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

第一处理模块 620，用于若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理；

20 可以理解的是，在实际应用中，所述集群外部的安全攻击防护中心被触发后，会启动安全清洗程序，例如进行流量清洗等，从而使得故障物理机恢复健康。需要说明的是，对于因网络 DDoS 攻击而导致的某台物理机网络不通与因物理机宕机而导致的物理机网络不通是需要区别对待的，如果在物理机正遭受网络 DDoS 攻击时将其上的虚拟机迁移至其他物理机，
25 会产生骨牌效应，导致扩大故障风险，即其他物理机陆续被攻击而不可用，最终可能造成全集群网络设备的泛洪（flooding），导致全集群物理机故障风险。

第二处理模块 630, 进一步包括:

关闭处理单元, 用于若在上述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障, 则向故障物理机发送关闭故障物理机的指令; 优选的, 所述指令可以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机;

迁移处理单元, 用于通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

需要说明的是, 所述的物理机自身不能修复的软硬件故障类型可以包括: 物理机宕机、物理机 CPU 异常、物理机内存异常、物理机电源模块等各类硬件问题异常。这类故障会直接导致物理机不可用, 且需要更换硬件模块方可修复, 因此, 本申请实施例通过从集群中将故障物理机隔离后再对故障物理机进行硬件更换或者维护。

优选的, 所述物理机故障分类处理装置 600 还可以进一步包括第三处理模块 640, 该第三处理模块 640 具体包括:

通知处理单元, 用于若在上述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间, 并且网络不通的物理机数量超过一台, 则通知运营维修人员人工修复;

迁移处理单元, 用于若在上述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间, 并且网络不通的物理机数量未超过预设数量, 则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

其中, 所述预设时间可以依据实际情况设定为 3 分钟、5 分钟等适合的时间段。

需要说明的是, 在检测到物理机网络完全不通且网络不通持续时间达到预设时间的情况下, 本申请实施例需要进一步检查网络不通的故障物理机的数量是否超过一个机柜的物理机数量或者一个交换机下联物理机数量, 如果超过, 则认为是集群规模性网络故障, 则需要采取电话报警通运

营维修人员人工修复,而不再自动处理。这是由于对于大规模物理机故障,在进行隔离物理机迁移虚拟机时,会导致大量物理机被关闭,当机房设备(网络设备或者电力设备等)恢复后,还需要再次重启物理机,然后恢复虚拟机,这一系列的操作将直接导致人工处理时间加倍甚至更多,从而大大加大虚拟机的不可用时长。因此,本申请实施例提供的方法,对此种物理机故障类型加以区分处理,可以大量缩短故障物理机的修复时间,从而大大缩短其上的虚拟机不可用的时长,进而提高系统的商用可用性。

优选的,所述物理机故障分类处理装置 600 还可以进一步包括第四处理模块 650,所述第四处理模块 650 具体包括:

10 重启处理单元,用于若在上述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常,且确定物理机网络不通是物理机重启所导致的,则在确定当前的物理机是健康的情况下,通过虚拟化接口重启所述物理机上的虚拟机;

15 迁移处理单元,用于若在上述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常,且确定物理机网络不通是物理机重启所导致的,则在确定当前的物理机是不健康的情况下,通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

20 优选的,所述物理机故障分类处理装置 600 还可以进一步包括第五处理模块 660,所述第五处理模块 660 具体包括:

关机处理单元,用于若在上述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间,则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机;

25 迁移处理单元,用于通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

需要说明的是,所述物理机网络不稳定且网络不稳定持续时间达到预

设时间的情况主要是一些未知原因造成物理机故障，例如，系统负载类、系统网络类、硬件故障类等。这类故障虽然本质原因比较难查，但是这类故障的现象却很明确，主要是：物理机网络丢包、物理机管理通道访问异常、物理机性能使用异常。对于这类物理机故障，可以采用相同的处理方式，即向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，所述物理机故障分类处理装置 600 还可以进一步包括：

确定模块 670，用于在所述物理机故障信息列表中匹配所述集群内的所有物理机，将没有匹配成功的物理机确定为健康物理机。

本申请实施例可以在大规模的云计算集群中，通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并有针对性的采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机

的频繁迁移而影响系统性能情况的发生。

实施例七

参照图 7，示出了本申请的一种虚拟机恢复系统实施例的架构图，该虚拟机恢复系统包括：物理机故障修复装置 710，其应用于虚拟化集群系统 700 内的每台物理机上；物理机故障分类处理装置 720 及物理机故障信息存储中心 730；其中：

所述物理机故障修复装置 710 具体可以包括：自主检测模块 711、自主处理模块 712；其中：自主检测模块 711 用于自主检测物理机自身的故障动态；自主处理模块 712 用于若所述自主检测模块 711 检测到物理机自身能容错修复的软硬件故障，则通过容错方式修复；还用于若自主检测模块 711 检测到物理机自身能重启修复的软硬件故障，通过重启物理机方式修复。

优选的，所述自主处理模块 712 还可以用于若所述自主检测模块 711 检测到物理机自身不能修复的软硬件故障，则根据所述集群外部的物理机故障分类处理模块 720 的指令或通过所述物理机上的带外管理模块 713 关闭故障物理机，由所述集群外部的物理机故障分类处理模块 720 通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，所述自主检测模块 712 还可以用于当自主检测模块 711 自主检测到因遭受网络攻击而导致物理机故障时，通过物理机故障收集模块 760 上报物理机故障信息到物理机故障信息存储中心 730，由所述集群外部的物理机故障分类处理模块 720 触发所述集群外部的安全攻击防护中心 740 处理。

需要说明的是，在本申请另一实施例中，该自主检测模块 711 和自主处理模块 712 可以是部署在集群每台物理机上的软件模块，在物理机开机时自动启动，该自主检测模块 711 和自主处理模块 712 的运行不依赖文件

系统，仅仅依赖 CPU、内存。

所述物理机故障信息存储中心 730，用于将所有上报的物理故障信息汇集成物理机故障信息列表；其中，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块 750 从故障物理机处探测到并上报给所述物理机故障信息存储中心 730 的物理机故障信息，及由所述集群外部的物理机故障收集模块 760 从故障物理机处收集到并上报给所述物理机故障信息存储中心 730 的物理机故障信息。

所述物理机故障分类处理装置 720，用于通过获取模块 721 从所述物理机故障信息存储中心 730 获取物理机故障信息列表，若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则通过第一处理模块 722 触发所述集群外部的安全攻击防护中心 740 处理；若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则通过第二处理模块 723 向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块 713 关闭故障物理机，及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，所述物理机故障分类处理装置 720 还可以进一步包括第三处理模块 724，用于若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间；判断网络不通的物理机数量是否超过预设数量，如果是则通知运营维修人员人工修复；否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

优选的，所述物理机故障分类处理装置 720 还可以进一步包括第四处理模块 725，用于若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

优选的，所述物理机故障分类处理装置 720 还可以进一步包括第五处理模块 726，用于若在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

优选的，所述物理机故障分类处理装置 720 还可以进一步包括确定模块 727，用于在所述物理机故障信息列表中匹配所述集群内的所有物理机，将没有匹配成功的物理机确定为健康物理机。

需要说明的是，所述物理机故障修复装置 710 以及物理机故障分类处理装置 720 的具体结构请参见前述实施例的详细说明，此处不再赘述。

需要说明的是，在本申请另一个实施例中，虚拟机恢复系统中的物理机故障分类处理装置 720、物理机故障探测模块 750、物理机故障收集模块 760 均为部署在虚拟化集群系统 700 以外的物理机上的软件模块，其可以各自独立部署在不同的物理机上，也可以合并部署在同一台物理机上。此外，物理机故障信息存储中心 730 是部署在虚拟化集群系统 700 以外的一套数据库系统。安全攻击防护中心 740 可以直接采用现有的安全攻击防护系统。本申请实施例对此不做限制。

本申请实施例，具备以下优点：

本申请实施例可以在大规模的云计算集群中，通过对多种物理机故障场景，进行精细化故障快速、准确的识别，并有针对性的进行分类处理，从而实现快速、高可靠的物理机故障修复处理，以保证其上的虚拟机服务的快速恢复。

进一步的，本申请实施例通过物理机自主检测自身的故障动态，并对物理机自身能修复的物理机故障情况有针对性的进行分类修复处理；对物理机自身不能修复的物理机故障情况，通过集群外部的物理机故障分类处理模块有针对性的进行分类修复处理，从而有效降低物理机故障的误判和漏判情况的发生，更安全、稳定、快速的进行虚拟机自动恢复。

另外，本申请实施例针对物理机自身不能修复的物理机故障情况，除了可以通过故障物理机上的带外管理模块关闭故障物理机之外，还可以通过集群外部的物理机故障分类处理模块，指示故障物理机自主关机，从而弥补带外管理模块调用关机操作的可用性无法达到商用标准的问题，同时也确保自动化物理机隔离的有效性。

此外，本申请实施例也同时考虑到大规模云计算集群内发生物理机规模故障情况的可能性，通过判断故障物理机的数量是否构成机房级别，并有针对性采取不同的修复处理方式。尤其是针对大规模物理机故障的情况，采用人工处理的方式修复，从而有效避免由于故障物理机上的虚拟机的频繁迁移而影响系统性能情况的发生。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

在一个典型的配置中，所述计算机设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、

数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD@ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非持续性的电脑可读媒体 (transitory media)，如调制的数据信号和载波。

本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所

以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

最后，还需要说明的是，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。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

以上对本申请所提供的一种应用于虚拟化集群系统的物理机故障修复方法、装置和集群物理机故障分类处理方法、装置及虚拟机恢复方法、系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均可有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种集群物理机故障分类处理方法，其特征在于，包括：

从物理机故障信息存储中心获取物理机故障信息列表；

- 5 若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理；

若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

- 10 2、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间；

判断网络不通的物理机数量是否超过预设数量，如果是则通知运营维修人员人工修复；

- 15 否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

3、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

- 若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。
- 20

4、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

- 若在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物
- 25

理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

5 5、如权利要求 1 所述的方法，其特征在于，所述若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令的步骤包括：

向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机。

10 6、如权利要求 1 所述的方法，其特征在于，通过以下方式确定所述健康物理机：

在所述物理机故障信息列表中匹配所述集群内的所有物理机；

将没有匹配成功的物理机确定为健康物理机。

15 7、如权利要求 1 所述的方法，其特征在于，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

8、一种集群物理机故障分类处理装置，其特征在于，包括：

获取模块，用于从物理机故障信息存储中心获取物理机故障信息列表；

20 第一处理模块，用于若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理；

第二处理模块，进一步包括：

关闭处理单元，用于若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令；

25 迁移处理单元，用于通过虚拟化接口迁移所述故障物理机上的虚拟机

到所述集群系统内其他健康物理机上。

9、如权利要求 8 所述的装置，其特征在于，所述装置还包括第三处理模块，所述第三处理模块包括：

5 通知处理单元，用于若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间，并且网络不通的物理机数量超过一台，则通知运营维修人员人工修复；

10 迁移处理单元，用于若在所述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间，并且网络不通的物理机数量未超过预设数量，则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

10、如权利要求 8 所述的装置，其特征在于，所述装置还包括第四处理模块，所述第四处理模块包括：

15 重启处理单元，用于若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则在确定当前的物理机是健康的情况下，通过虚拟化接口重启所述物理机上的虚拟机；

20 迁移处理单元，用于若在所述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则在确定当前的物理机是不健康的情况下，通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

11、如权利要求 8 所述的装置，其特征在于，所述装置还包括第五处理模块，所述第五处理模块包括：

25 关机处理单元，用于若在所述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；

迁移处理单元，用于通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

12、如权利要求 8-11 任一项所述的装置，其特征在于，所述关闭处理单元，用于若在上述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机。

13、如权利要求 8-11 任一项所述的装置，其特征在于，所述装置还包括：

10 确定模块，用于在上述物理机故障信息列表中匹配所述集群内的所有物理机，将没有匹配成功的物理机确定为健康物理机。

14、如权利要求 8 所述的装置，其特征在于，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

15、一种虚拟机恢复方法，其特征在于，应用于虚拟化集群系统，所述方法包括：

虚拟化集群系统内的物理机自主检测自身的故障动态；

20 若自主检测到物理机自身能容错修复的软硬件故障，通过容错方式修复；

若自主检测到物理机自身能重启修复的软硬件故障，通过重启物理机方式修复；

从物理机故障信息存储中心获取物理机故障信息列表；

25 若在上述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理；

若在上述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

16、如权利要求 15 所述的方法，其特征在于，所述方法还包括：

5 若在上述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间；判断网络不通的物理机数量是否超过预设数量，如果是则通知运营维修人员人工修复；否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

17、如权利要求 15 所述的方法，其特征在于，所述方法还包括：

10 若在上述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

15 18、如权利要求 15 所述的方法，其特征在于，所述方法还包括：

若在上述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

19、如权利要求 15 所述的方法，其特征在于，通过以下方式确定所述健康物理机：

在上述物理机故障信息列表中匹配所述集群内的所有物理机；

将没有匹配成功的物理机确定为健康物理机。

25 20、如权利要求 15 所述的方法，其特征在于，所述从物理机故障信息存储中心获取物理机故障信息列表的步骤包括：

物理机故障分类处理模块从物理机故障信息存储中心获取物理机故障信息列表。

21、如权利要求 15 所述的方法，其特征在于，所述若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令的步骤包括：

向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机。

22、如权利要求 15 所述的方法，其特征在于，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

23、一种虚拟机恢复系统，其特征在于，所述系统包括：

物理机故障修复装置，应用于虚拟化集群系统内的物理机上自主检测物理机自身的故障动态，若自主检测到物理机自身能容错修复的软硬件故障，通过容错方式修复；若自主检测到物理机自身能重启修复的软硬件故障，通过重启物理机方式修复；

物理机故障信息存储中心，用于将所有上报的物理故障信息汇集成物理机故障信息列表；

物理机故障分类处理装置，用于从所述物理机故障信息存储中心获取物理机故障信息列表，若在所述物理机故障信息列表中检测到因遭受网络攻击而导致物理机故障，则触发所述集群外部的安全攻击防护中心处理；若在所述物理机故障信息列表中检测到因物理机自身不能修复的软硬件故障，则向故障物理机发送关闭故障物理机的指令，及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

24、如权利要求 23 所述的系统，其特征在于，所述物理机故障分类处理装置还用于：

若在上述物理机故障信息列表中检测到物理机网络完全不通且网络不通持续时间达到预设时间；判断网络不通的物理机数量是否超过预设数量，如果是则通知运营维修人员人工修复；否则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内到其他健康物理机上。

5 25、如权利要求 23 所述的系统，其特征在于，所述物理机故障分类处理装置还用于：

若在上述物理机故障信息列表中检测到物理机网络不通但网络不通持续时间未达到预设时间后网络又恢复正常，且确定物理机网络不通是物理机重启所导致的，则判断当前的物理机是否健康，如果健康则通过虚拟化接口重启所述物理机上的虚拟机，如果不健康则通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群内其他健康物理机上。

10

26、如权利要求 23 所述的系统，其特征在于，所述物理机故障分类处理装置还用于：

若在上述物理机故障信息列表中检测到物理机网络不稳定且网络不稳定持续时间达到预设时间，则向故障物理机发送指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机；及通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

15

27、如权利要求 23 所述的系统，其特征在于，所述物理机故障分类处理装置还用于：

20

在上述物理机故障信息列表中匹配所述集群内的所有物理机，将没有匹配成功的物理机确定为健康物理机。

28、如权利要求 23 所述的系统，其特征在于，所述物理机故障分类处理装置还用于：

25 向故障物理机发送关闭故障物理机的指令以指示所述故障物理机自主关闭故障物理机或通过所述物理机上的带外管理模块关闭故障物理机。

29、如权利要求 23 所述的系统，其特征在于，所述物理机故障信息列表包括：由所述集群外部的物理机故障探测模块从故障物理机处探测到并上报给所述物理机故障信息存储中心的物理机故障信息，及由所述集群外部的物理机故障收集模块从故障物理机处收集到并上报给所述物理机故障信息存储中心的物理机故障信息。

30、如权利要求 23 所述的系统，其特征在于，所述物理机故障修复装置包括：

自主检测模块，包括：

检测单元，用于自主检测物理机自身的故障动态；

自主处理模块，包括：

容错单元，用于若所述检测单元检测到物理机自身能容错修复的软硬件故障，则通过容错方式修复；

重启单元，用于若所述检测单元检测到物理机自身能重启修复的软硬件故障，则通过重启物理机方式修复。

31、如权利要求 30 所述的系统，其特征在于，所述自主处理模块还包括：

关机单元，用于若所述检测单元检测到物理机自身不能修复的软硬件故障，则根据所述集群外部的物理机故障分类处理模块的指令或通过所述物理机上的带外管理模块关闭故障物理机，由所述集群外部的物理机故障分类处理模块通过虚拟化接口迁移所述故障物理机上的虚拟机到所述集群系统内其他健康物理机上。

32、如权利要求 30 所述的系统，其特征在于，所述自主检测模块还包括：

上报单元，用于当自主检测模块自主检测到因遭受网络攻击而导致物理机故障时，通过物理机故障收集模块上报物理机故障信息到物理机故障信息存储中心，由所述集群外部的物理机故障分类处理模块触发所述集群外部的安全攻击防护中心处理。

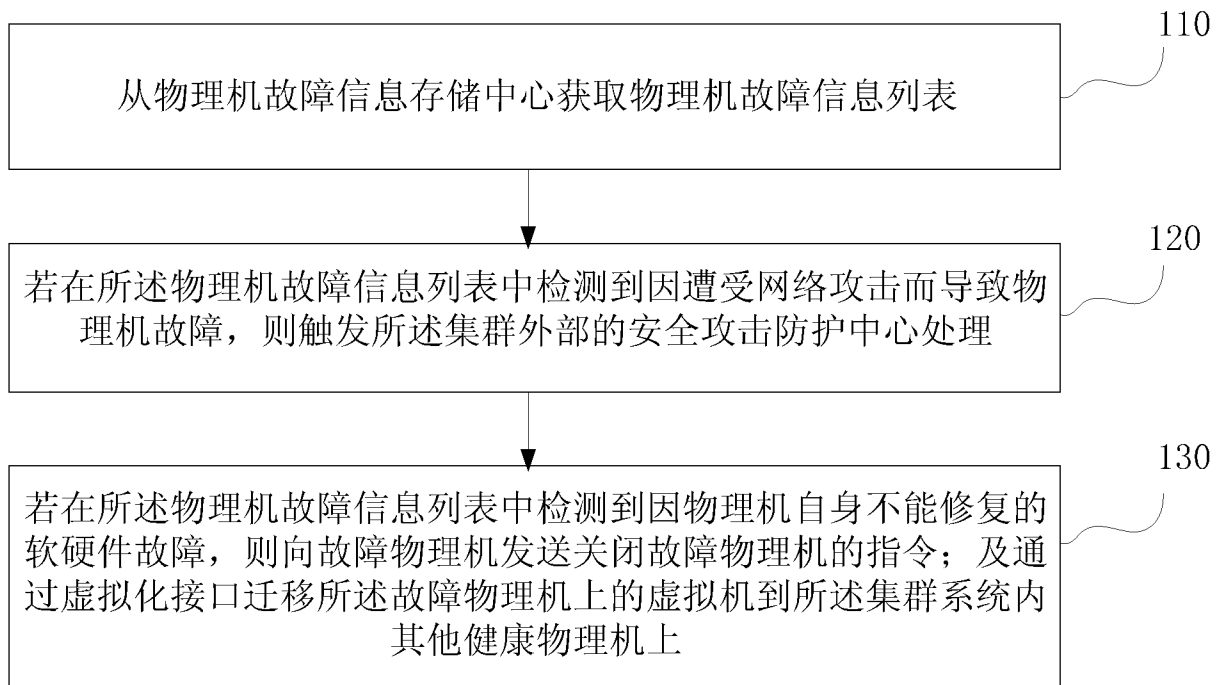


图 1

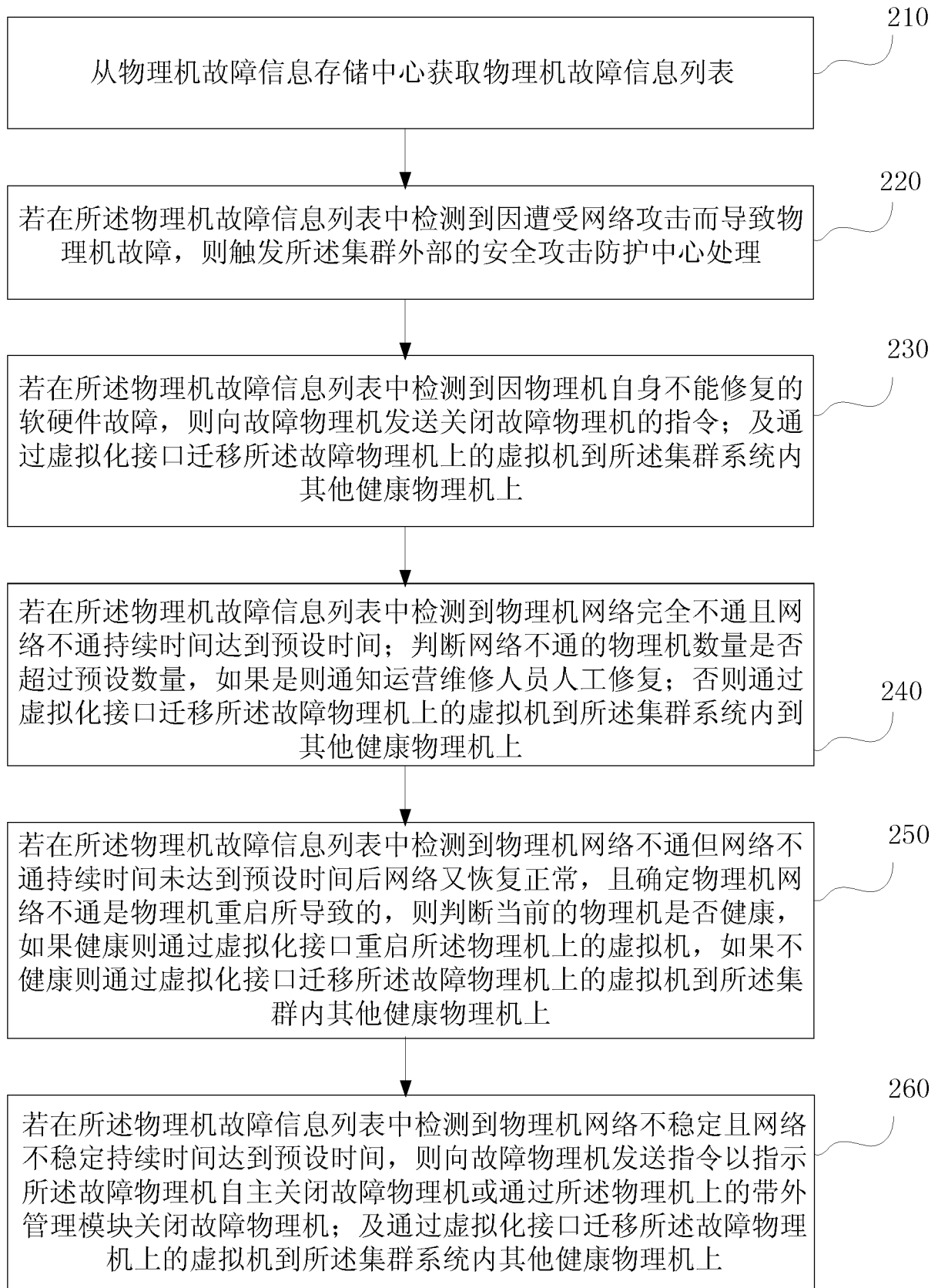


图 2

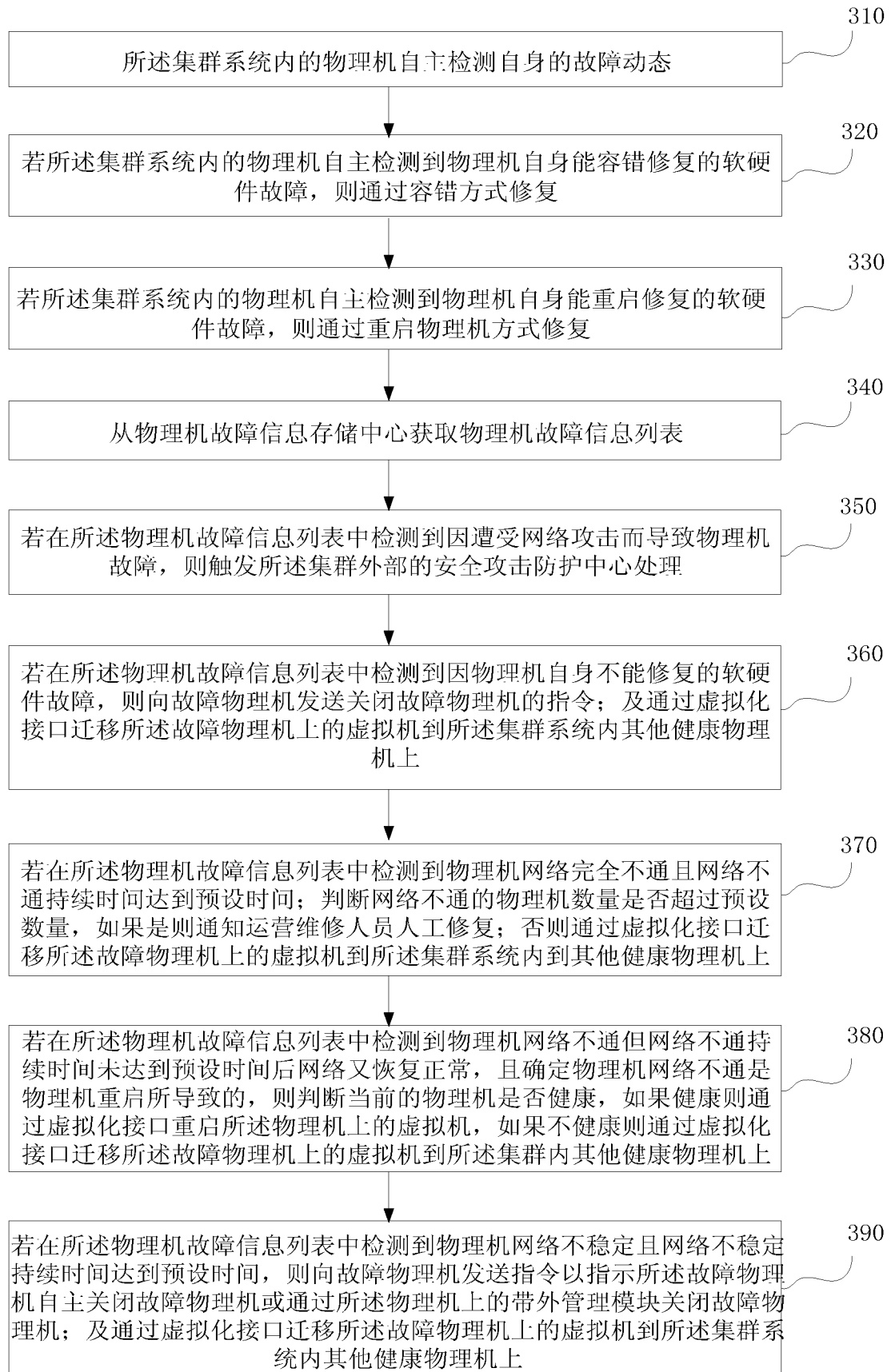


图 3

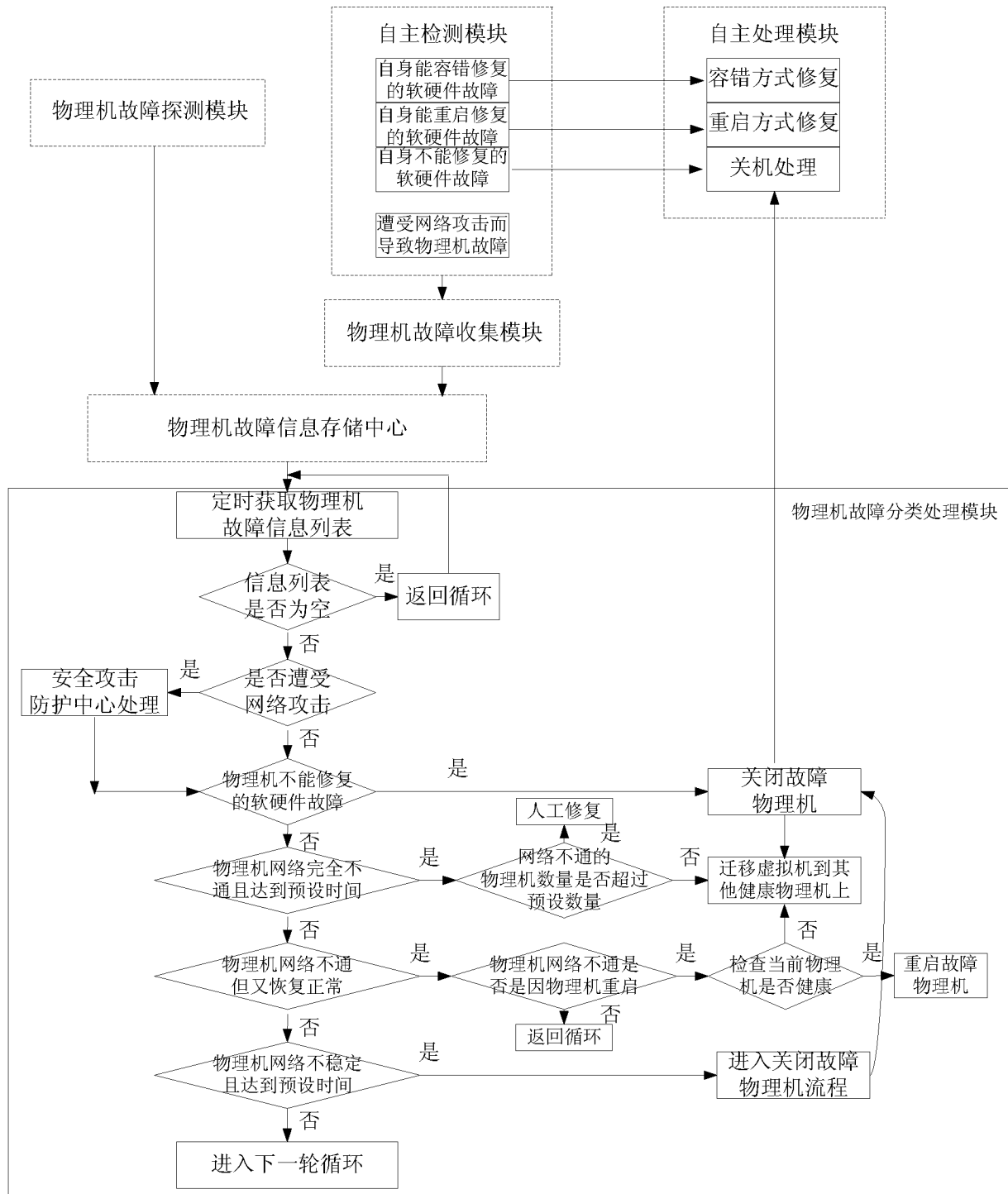


图 4

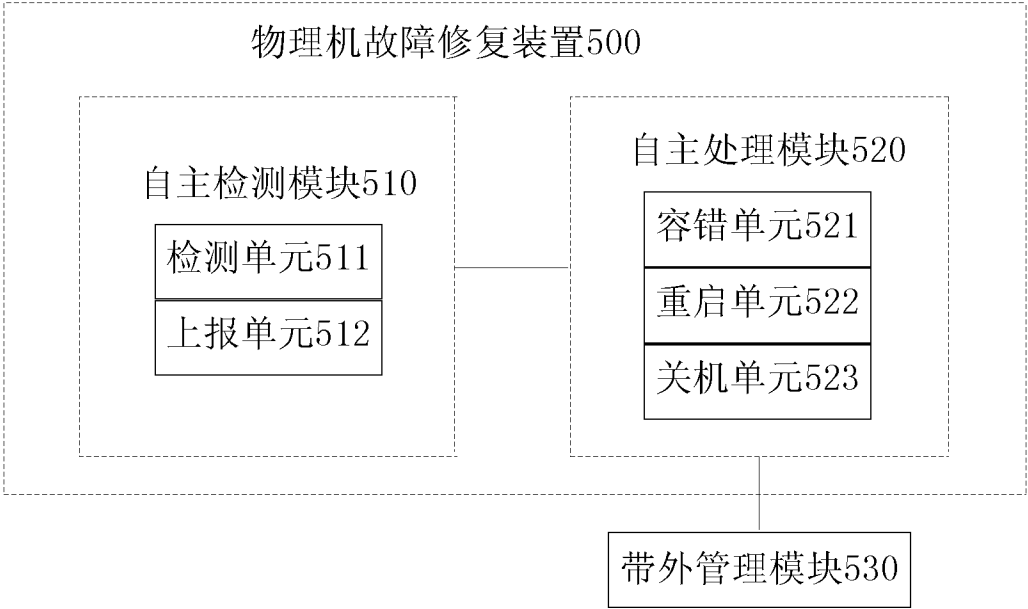


图 5

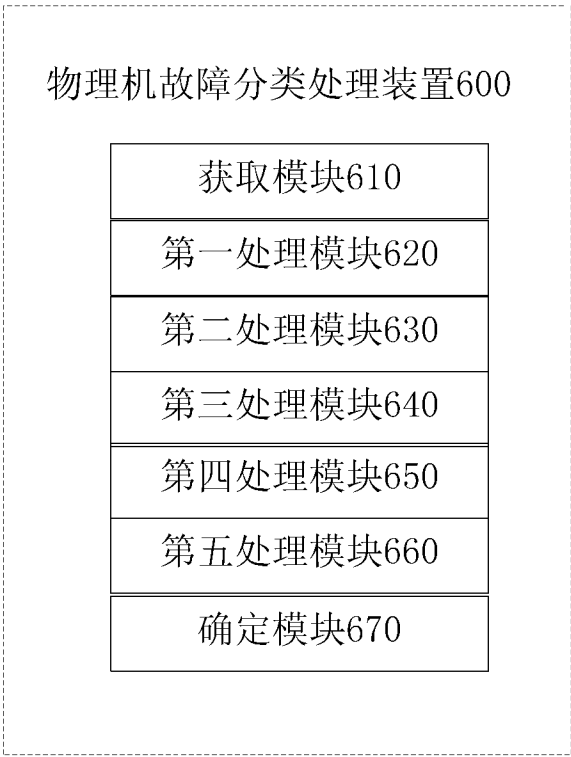


图 6

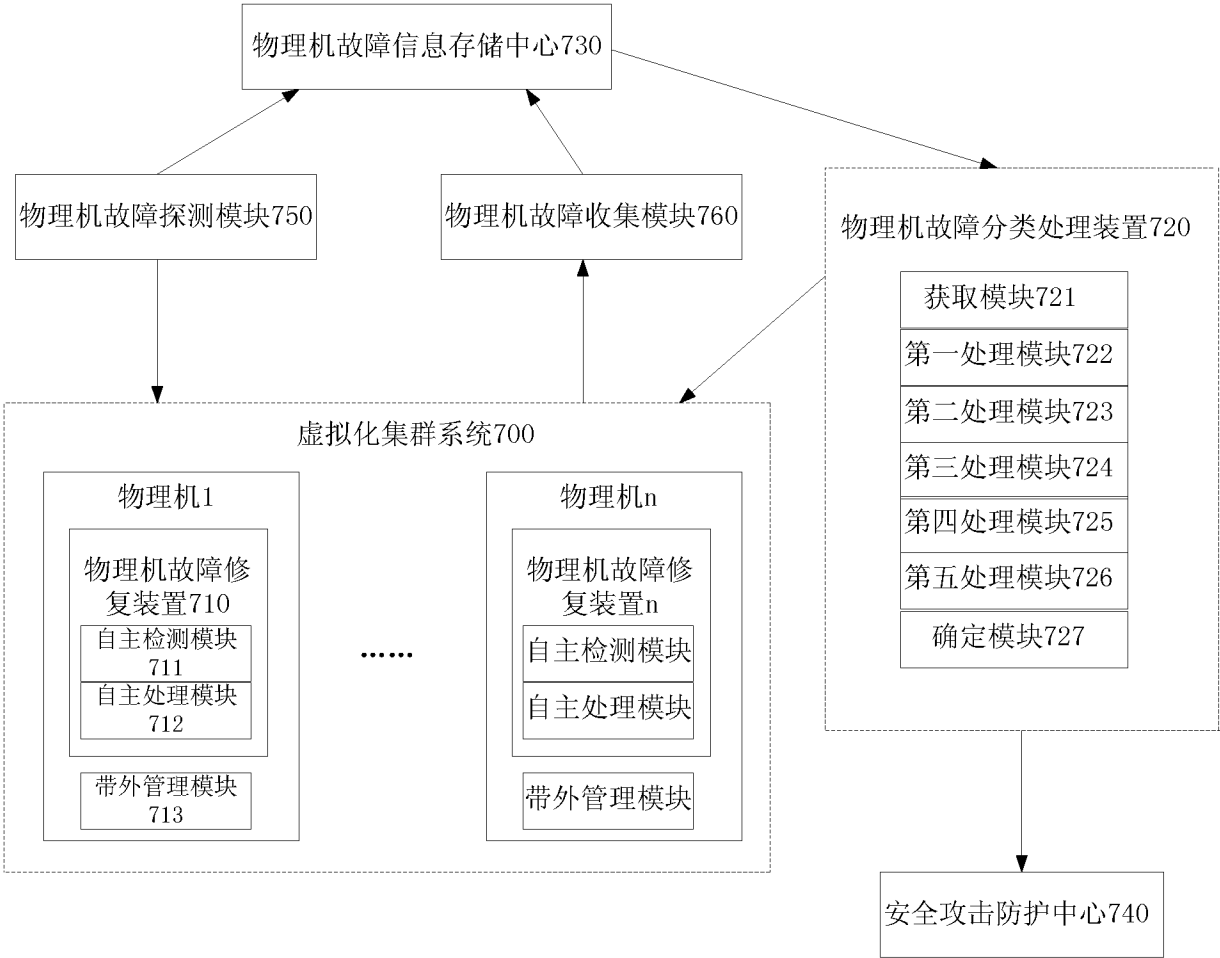


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/074618

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/07 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI, CNPAT, CNKI, IEEE, GOOGLE: physical machine, fault, classify, machine, computer, network, attack, hardware, software, close, health, instruction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102984739 A (ZTE CORP.), 20 March 2013 (20.03.2013), description, paragraphs [0005]-[0013]	1-32
Y	CN 102629224 A (GUANGDONG ELECTRONICS INDUSTRY INSTITUTE LTD.), 08 August 2012 (08.08.2012), description, paragraphs [0019] and [0024]	1-32
A	CN 103095506 A (INSPUR ELECTRONIC INFORMATION INDUSTRY CO., LTD.), 08 May 2013 (08.05.2013), the whole document	1-32
A	CN 102394774 A (GUANGDONG ELECTRONICS INDUSTRY INSTITUTE LTD.), 28 March 2012 (28.03.2012), the whole document	1-32
A	US 2011060722 A1 (ICON BUSINESS SYSTEMS LIMITED), 10 March 2011 (10.03.2011), the whole document	1-32

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 03 May 2017 (03.05.2017)	Date of mailing of the international search report 24 May 2017 (24.05.2017)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer GAO, Minfang Telephone No.: (86-10) 010-82246811

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/074618

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102984739 A	20 March 2013	None	
CN 102629224 A	08 August 2012	None	
CN 103095506 A	08 May 2013	None	
CN 102394774 A	28 March 2012	None	
US 2011060722 A1	10 March 2011	GB 0922212 D0	03 February 2010
		GB 2473303 A	09 March 2011
		CN 102012789 A	13 April 2011
		HK 1151599 A1	29 August 2014
		HK 1155245 A0	11 May 2012

国际检索报告

国际申请号

PCT/CN2017/074618

A. 主题的分类

G06F 11/07 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

EPDOC, WPI, CNPAT, CNKI, IEEE, GOOGLE: 物理机, 故障, 分类, 网络, 攻击, 硬件, 软件, 关闭, 指令, 健康, machine, computer, network, attack, hardware, software, close, health, instruction

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 102984739 A (中兴通讯股份有限公司) 2013年 3月 20日 (2013 - 03 - 20) 说明书第[0005]-[0013]段	1-32
Y	CN 102629224 A (广东电子工业研究院有限公司) 2012年 8月 8日 (2012 - 08 - 08) 说明书第[0019], [0024]段	1-32
A	CN 103095506 A (浪潮电子信息产业股份有限公司) 2013年 5月 8日 (2013 - 05 - 08) 全文	1-32
A	CN 102394774 A (广东电子工业研究院有限公司) 2012年 3月 28日 (2012 - 03 - 28) 全文	1-32
A	US 2011060722 A1 (ICON BUSINESS SYSTEMS LIMITED) 2011年 3月 10日 (2011 - 03 - 10) 全文	1-32

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 5月 3日

国际检索报告邮寄日期

2017年 5月 24日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

高民芳

传真号 (86-10) 62019451

电话号码 (86-10) 010-82246811

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/074618

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102984739	A	2013年 3月 20日	无			
CN	102629224	A	2012年 8月 8日	无			
CN	103095506	A	2013年 5月 8日	无			
CN	102394774	A	2012年 3月 28日	无			
US	2011060722	A1	2011年 3月 10日	GB	0922212	D0	2010年 2月 3日
				GB	2473303	A	2011年 3月 9日
				CN	102012789	A	2011年 4月 13日
				HK	1151599	A1	2014年 8月 29日
				HK	1155245	A0	2012年 5月 11日

表 PCT/ISA/210 (同族专利附件) (2009年7月)