(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
2016 年 7 月 7 日 (07.07.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/106661 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2014/095847

(22) 国际申请日: 2014 年 12 月 31 日 (31.12.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **冯锐 (FENG, Rui)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, 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, KN, KP, KR, 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))。

WO 2016/106661 A1

(54) **Title**: ACCESS CONTROL METHOD FOR STORAGE DEVICE, STORAGE DEVICE, AND CONTROL SYSTEM

(54) **发明名称** : 一种存储装置的访问控制方法、存储装置以及控制系统

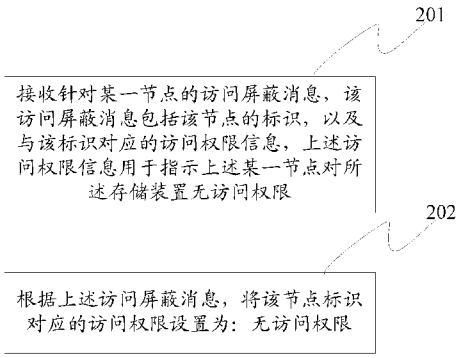

图 2 / FIG. 2

201 Receive an access mask message with respect to a certain node, where the access mask message comprises an identifier of the node and access permission information corresponding to the identifier, the access permission information is used for indicating that the certain node has no access permission with respect to the storage device

202 Configure, on the basis of the access mask message, an access permission corresponding to the identifier of the node as: no access permission.

(57) **Abstract**: Method and system for controlling access to storage device. The method comprises: the storage device receives an access mask message with respect to the node, where the access mask message comprises an identifier of the node and access permission information corresponding to the identifier, and the access permission information is used for indicating that the node has no access permission with respect to the storage device; the storage device configures, on the basis of the access mask message, the access permission corresponding to the identifier of the node as: no access permission; the storage device transmits a firewall policy modification notification to the storage device, where the firewall policy modification notification is used for instructing the node to modify a firewall policy of a firewall corresponding to the node, thus masking I/O access requests transmitted by the node to the storage device. Employment of the method allows effective implementation of control of access to the storage device.

(57) **摘要**: 一种对存储装置访问的控制方法以及系统，其中，该方法包括：所述存储装置接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；所述存储装置根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为：无访问权限；所述存储装置向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的 IO 访问请求。采用上述方法，能够有效地实现对存储装置的访问进行控制。

一种存储装置的访问控制方法、存储装置以及控制系统

技术领域

本发明涉及存储技术领域，更具体地，涉及一种存储装置的访问控制方法、存储装置以及控制系统。

背景技术

集群（Cluster）是一组相互独立的、通过高速网络互连的计算机。集群中的每一个计算机被称为一个节点（Node）。在集群中会存在一个管理节点，它是通过管理员指定或者系统配置设定，该管理节点的一项重要功能是检测集群中节点是否发生故障，并通知发生故障的节点从集群中退出。

在集群中的节点对存储装置进行访问的应用场景下，一旦某一节点发生故障，就需要通知该故障节点从集群中退出，以避免故障节点和其他无故障节点同时对存储资源进行读写访问时，所可能出现的数据不一致的问题。

在解决故障节点对存储装置的访问控制问题时，现有技术采用的是Fencing(隔离)技术，其中，包括三类解决方式: Persistent Reservation Fencing（持久保留隔离，以下简称PRF）技术，Fiber Channel Fencing（光纤信道隔离，以下简称FCF）技术，以及Power Fencing（电源隔离，以下简称PF）技术。其中，采用PRF技术，需要存储设备支持SCSI-3 Persistent Reservation（持久保留）功能，其中SCSI指的是小型计算机系统接口，其全称是Small Computer System Interface。采用FCF技术，通过控制光纤交换机，禁用故障节点所连接的光纤通道端口，切断存储资源到故障节点的光纤链路，从而达到禁止故障节点访问存储装置的目的。采用PF技术，通过控制故障节点的供电模块，直接切断故障节点的电源，从而就避免故障节点对存储装置的访问。

上述现有技术中，并非所有的存储设备都支持SCSI-3 Persistent

Reservation 功能，故采用 PRF 技术，就具有一定的局限性；而采用 FCF 技术或者 PF 技术，则可能存在安全性问题。

发明内容

鉴于此，本发明实施例提供了一种存储装置的访问控制方法、存储装置以及控制系统，能够有效地实现对故障节点访问存储装置进行控制。

第一方面，提供了一种存储装置的访问控制方法，应用于集群中节点对存储装置的访问过程，该方法包括：所述存储装置接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；所述存储装置根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为：无访问权限；所述存储装置向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的 IO 访问请求。

结合第一方面，在第一种可能的实现方式中，在所述存储装置根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为无访问权限之后，该方法包括：所述存储装置接收所述节点发送的 IO 访问请求，所述 IO 访问请求包括所述节点的标识；所述存储装置根据所述访问控制列表以及所述 IO 访问请求，确定所述节点的标识对应的访问权限为无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作。

结合第一方面的第一种可能的实现方式，在第二种可能的实现方式中，在所述存储装置向所述节点发送异常指示消息之后，该方法还包括：所述存储装置接收管理节点发送的访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限，所述访问屏蔽消息

是在所述节点向所述管理节点发送加入集群的请求，确定所述节点为恢复节点之后，由所述管理节点向所述存储装置发送的；所述存储装置根据所述访问屏蔽解除消息，在所述访问控制列表中，将所述节点标识对应的访问权限设置为：有访问权限。

结合第一方面的第二种可能的实现方式，在第三种可能的实现方式中，在所述根据所述访问屏蔽解除消息，在所述访问控制列表中，对所述节点标识对应的访问权限设置为有访问权限之后，所述方法还包括：所述存储装置向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，允许所述节点向所述存储装置发送的IO访问请求。

结合第一方面或者第一方面的第一至第三种可能的实现方式，在第四种可能的实现方式中，在所述接收针对所述节点的访问屏蔽消息之前，所述方法还包括：预先设置所述存储装置的访问控制列表，所述访问控制列表包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限；以及预先设置所述节点对应防火墙的防火墙策略，所述防火墙策略用于指示所述节点对应的防火墙，允许所述节点向所述存储装置发送的IO访问请求。

第二方面，提供了一种存储装置，该存储装置包括：

处理器，存储器，通信接口和总线，其中，所述处理器、所述存储器和所述通信接口通过所述总线通信；

所述通信接口用于与集群中的管理节点以及节点通信；

所述存储器用于存放程序；

当所述存储装置运行时，所述处理器用于执行所述存储器存储的所述程序，以执行上述第一方面的各种实现方式之一所述的方法。

第三方面，提供了一种具有访问控制功能的存储装置，该存储装置应用于集群中节点对所述存储装置的访问过程中，该存储装置包括：接收单元，用于接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；设置单元，用于根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为：无访问权限；发送单元，用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的IO访问请求。

结合第三方面，在第一种可能的实现方式中，所述接收单元，还用于接收所述节点发送的IO访问请求，所述IO访问请求包括所述节点的标识；所述发送单元，还用于根据所述访问控制列表以及所述IO访问请求，确定所述节点的标识对应的访问权限为无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作。

结合第三方面的第一种可能的实现方式，在第二种可能的实现方式中，所述接收单元，还用于接收管理节点发送的访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限，所述访问屏蔽消息是在所述节点向所述管理节点发送加入集群的请求，确定所述节点为恢复节点之后，由所述管理节点向所述存储装置发送的；所述设置单元，还用于根据所述访问屏蔽解除消息，在所述访问控制列表中，将所述节点标识对应的访问权限设置为：有访问权限。

结合第三方面的第二种可能的实现方式，在第三种可能的实现方式中，所述发送单元，还用于向所述节点的防火墙发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点的防火墙，允许所述节点向所述存储装置发送的IO访问请求。

结合第三方面或者第三方面的第一至第三种可能的实现方式，在第四种可能的实现方式中，所述设置单元，还用于预先设置所述存储装置的访问控制列表，所述访问控制列表包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限；以及预先设置所述节点防火墙的防火墙策略，所述防火墙策略用于指示所述节点的防火墙，允许所述节点向所述存储装置发送的 IO 访问请求。

第四方面，提供了一种实现存储装置访问的控制系统，该系统包括：集群以及存储装置，所述集群包括至少一个节点，所述至少一个节点中的某一个节点能够对所述存储装置进行访问，所述存储装置，用于接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；用于根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为无访问权限；以及用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的 IO 访问请求；所述节点，用于根据所述修改防火墙策略的通知，修改对应防火墙的防火墙策略。

结合第四方面，在第一种可能的实现方式中，所述存储装置，还用于接收所述节点发送的 IO 访问请求，所述 IO 访问请求包括所述节点的标识，根据所述访问控制列表以及所述 IO 访问请求，确定所述节点的标识对应的访问权限为无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作；所述节点，还用于根据所述异常指示消息，执行所述节点重启操作。

结合第四方面的第一种可能的实现方式，在第二种可能的实现方式中，所述集群中还包含管理节点，所述管理节点，用于接收所述节点发送的加入

集群的请求，确定所述节点为恢复节点之后，向所述存储盘发送访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限；所述存储装置，还用于接收管理节点发送的访问屏蔽解除消息，并根据所述访问屏蔽解除消息，在所述访问控制列表中，将所述节点标识对应的访问权限设置为有访问权限。

结合第四方面的第二种可能的实现方式，在第三种可能的实现方式中，所述存储装置，还用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，允许所述节点向所述存储装置发送的 IO 访问请求；所述节点，还用于根据所述修改防火墙策略的通知，修改对应防火墙的防火墙策略。

结合第四方面或者第四方面的第一至第三种可能的实现方式，在第四种可能的实现方式中，所述存储装置，还用于预先设置所述访问控制列表，所述访问控制列表包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限；以及 所述节点，还用于预先设置所述节点对应防火墙的防火墙策略，所述防火墙策略用于指示所述节点对应的防火墙，允许所述节点向所述存储装置发送的IO访问请求。

基于上述实现方案，本发明实施例通过存储装置接收针对某一节点的访问屏蔽消息，从而改变该节点访问存储装置的访问权限，并通过发送修改防火墙策略的通知给该节点，促使该节点修改对应防火墙的防火墙策略，从而有效地屏蔽了该节点对存储装置的IO访问请求。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中

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发明的一些实施例，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 是本发明实施例的集群和存储装置所构成的访问系统架构示意图。

图 2 是本发明的对存储装置的访问进行控制的方法实施例一的示意图。

图 3 是本发明的对存储装置的访问进行控制的方法实施例二的示意图。

图 4 是本发明的对存储装置的访问进行控制的方法实施例三的示意图。

图 5 是本发明的对存储装置的访问进行控制的方法实施例四的示意图。

图 6 是本发明实现的存储装置实施例一的示意性框图。

图 7 是本发明实现的存储装置实施例二的示意性框图。

图 8 是本发明实现存储装置访问的控制系统实施例的示意性框图。

具体实施方式

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的一部分实施例，而不是全部实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都应属于本发明保护的范围。

一般的，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、组件、数据结构、以及其他类型的结构。此外，本领域的技术人员可以明白，各实施例可以用其他计算机系统配置来实施，包括手持式设备、多处理器系统、基于微处理器或可编程消费电子产品、小型计算机、大型计算机以及类似计算设备。各实施例还能在任务由通过通信网络连接的远程处理设备来执行的分布式计算环境中实现。在分布式计算环境中，程序模块可位于本地和远程存储器存储设备中。

各实施例可被实现为计算机实现的过程、计算系统、或者诸如计算机程序产品或计算机系统执行示例过程的指令的计算机程序的计算机存储介质。

例如：计算机可读存储介质可经由易失性计算机存储器、非易失性存储器、硬盘驱动器、闪存驱动器、软盘或紧致盘和类似介质中的一个或多个来实现。

贯穿本说明书，术语“集群（Cluster）”是一组相互独立的、通过高速网络互联的计算机，它们构成了一个组，并以单一系统的模式加以管理。集群中的每台计算机被称为一个“节点”。

贯穿本说明书，术语“节点（Node）”一般指在联网环境中执行一个或多个软件程序的计算设备，然而，在具体应用中，“节点”还可以被实现为被视作网络中的服务器的一个或多个计算设备上执行的虚拟节点（软件程序）。节点指的是物理机或者安装在物理机上的虚拟机。

贯穿本说明书，术语“存储装置（Storage Device）”一般指用于储存信息的设备，通常是采用将信息数字化后再以利用电、磁或光学等方式存储在存储介质中。

贯穿本说明书，术语“防火墙（Firewall）”一般指的是一项协助确保信息安全的设备，会依照特定的规则，允许或是限制传输的数据通过。在具体实现中，防火墙可能是一台专属的硬件或是架设在一般硬件上的一套软件。

贯穿本说明书，术语“IO 访问请求”一般指的是存储设备所接收到的对该存储设备上所存储的数据进行读、或者写的请求。其中，对于 IO 读请求，一般包含需要读取的存储设备的地址信息；对于 IO 写请求，除包含需要写入的存储设备的地址信息，还包含需要写入的数据。

本发明实施例的系统架构

在介绍本发明的实施例之前，先整体介绍一下由集群和存储装置所构成的访问系统架构示意图，如图 1 所示。该系统包括：

集群 100，由 N 个节点组成（$N \geq 1$，且 N 为整数），每一个节点可以部署在物理节点（如：服务器）上，也可以部署在虚拟节点（如：虚拟机）上，负责接收应用或者客户端发送的数据访问请求，并将该数据访问请求转换成

对存储装置的IO访问请求。在集群100中所包含的N个节点中，会存在一个管理节点（以节点2作为管理节点为例），该管理节点通过管理员或者其他系统从节点中选择并加以配置。该管理节点负责检测出集群中其他节点的故障，并通知发生故障的节点从集群中退出。

存储装置资源池200，有M（M≥1，且M为整数）个存储装置构成，每个存储装置可以理解为包含了存储管理软件和存储介质的存储设备。存储装置资源池200中的M个存储装置的连接方式是多种多样的，图1所示的M个存储装置是环型结构的连接方式（这里仅作为示意），实际应用中，还可以有星型结构、总线结构、分布式结构、树型结构、网状结构、蜂窝状结构等，对此，本发明的实施例不加以赘述。

集群100中的节点和存储装置资源池200中的存储装置，可直接相连或者通过网络方式（图1未示）相连。由于上述这些连接方式属于本领域的公知常识，对此，本发明的实施例不加以赘述。

本发明的实施例

图2示出了对存储装置的访问进行控制的方法实施例一，该方法实施例包括:

201、接收针对某一节点的访问屏蔽消息，该访问屏蔽消息包括该节点的标识，以及与该标识对应的访问权限信息，上述访问权限信息用于指示上述某一节点对所述存储装置无访问权限。

其中，该方法流程可由存储装置来执行。当某一节点存在故障时，或者管理员打算对某一节点进行控制时，会由集群中的管理节点或者管理节点指定的某一节点向存储装置发送访问屏蔽消息。在具体实现中，节点的标识可以为节点的IP地址，或者节点在集群中的编号，对此，本发明的实施例不加以限制。

202、根据上述访问屏蔽消息，将该节点标识对应的访问权限设置为:

无访问权限。

在具体实现过程中，通过访问屏蔽消息中的节点的标识，可以在预设的访问控制列表（ACL，Access Control List）中查找该节点的标识对应的访问权限，将该访问权限修改为“拒绝访问”；也可以在存储盘上单独记录该节点标识对应的访问权限为：无访问权限。可以理解，上述预设的访问控制列表可以存储在存储装置上，也可以存储在其他的设备中，对此，本发明的所有实施例均不加以限定。对于本领域技术人员可以理解，访问控制列表 ACL 仅是一种实现方式，在实际应用中，还可以包含其他的实现方式，对此，本发明的实施例均不加以限制。

本实施例中，通过存储装置接收针对某一节点访问屏蔽消息，能够使得存储装置根据该屏蔽消息，对该节点访问权限进行控制，这样就屏蔽了该节点存在故障时，对该存储装置的发出的 IO 访问请求。

可以理解，上述的实施例是以集群中的某一节点存在故障时，对存储装置的访问进行控制，本实施例也可以应用在其他的应用场景，譬如：根据其他业务需求，欲设置某一节点对该存储装置的访问权限。

图 3 示出了对存储装置的访问进行控制的方法实施例二，应用于集群的节点对存储装置的访问过程中，参看图 3，该方法实施例包括：

301、存储装置接收针对某一节点的访问屏蔽消息，该访问屏蔽消息包括该节点的标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储装置无访问权限。

在具体实现中，该节点的标识可以为节点的 IP 地址，或者节点在集群中的编号。

302、存储装置根据上述访问屏蔽消息，将上述节点标识对应的访问权限设置为：无访问权限。

在具体的实现中，可以预先设置访问控制列表，该访问控制列表可以预

先存储在存储装置或者其他的网络设备中。当访问控制列表存储在存储装置上时，存储装置接收到上述访问屏蔽消息之后，直接在自身存储的访问控制列表中，对该节点标识对应的访问权限进行设置；当访问控制列表预先存储在其他的网络设备中，当存储装置接收到上述访问屏蔽消息之后，向存储该访问控制列表的其他网络设备发送修改该节点标识对应的访问权限的请求，由该网络设备进行访问权限的修改。另外一种实现方式是，并不预先设置访问控制列表，当存储装置接收到上述访问屏蔽消息后，将该节点标识对应的访问权限设置为：无访问权限。对此，实现过程中采用什么方式，本发明的所有实施例均不加以限制。

对该节点标识对应的访问权限进行设置，具体包括：将该节点标识对应的访问权限设置为“该节点对存储装置设置为无访问权限”。

303、存储装置向该节点发送修改防火墙策略的通知，上述修改防火墙策略的通知用于指示该节点修改该节点对应防火墙的防火墙策略，屏蔽该节点向存储装置发送的IO访问请求。

具体实现过程中，防火墙的实现方式是多种多样的，可以是网络层防火墙、或者应用层防火墙，以及其他类型的防火墙。在具体实现过程中，节点对应的防火墙可以是安装在节点上的防火墙软件，或者单独设置一个服务器，用来安装防火墙。修改防火墙策略的通知，用于指示该节点修改该节点对应防火墙的防火墙策略，修改防火墙策略的通知通过存储装置和节点之间的可靠信道进行传输。上述可靠信道的建立，可采用SSH（Secure SHell，安全外壳）协议来实现，利用SSH协议实现可靠信道属于现有技术，对此，不再进行赘述。

上述实施例中，通过存储装置接收针对某一节点访问屏蔽消息，能够使得存储装置根据该屏蔽消息，对该节点访问权限进行控制，在设置访问权限的同时，通过修改防火墙策略的通知，更新了该节点对应防火墙的防火墙策略，这样当该节点存在故障时，就有效地屏蔽了该节点向该存储装置的发出

的 IO 访问请求。

进一步的，在上述实施例二的基础上，还可包含如下的实现步骤：

在所述存储装置根据上述访问屏蔽消息，将所述节点标识对应的访问权限设置为无访问权限之后，所述方法还包括：

302'、存储装置接收上述节点发送的 IO 访问请求，上述 IO 访问请求包括上述节点的标识，上述存储装置根据所述节点标识对应的访问权限，确定发送所述 IO 访问请求的所述节点无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作。

在具体实现的过程中，上述的步骤 302'在步骤 302 之后执行，可以和步骤 303 并行执行，或者在步骤 303 之后且在节点根据上述修改防火墙策略的通知，完成对节点对应防火墙的防火墙策略的修改之前执行。对此，本发明的实施例并不限定上述步骤的执行顺序。

进一步的，在步骤 302'之后，该实施例还包含如下步骤：

302''、该节点接收到上述异常指示消息之后，执行重启操作。

其中，具体的，该节点执行操作，具体可通过如下两个步骤实现：

（1）存储装置向该节点发送异常指示消息，该异常指示消息用于指示该节点执行重启操作；

（2）该节点根据上述异常指示消息执行节点重启操作。

需要说明的是，节点的重启分为不同的模式：节点的整个系统的重启，主要针对该节点存在硬件或者操作系统的故障；节点的某一应用软件的重启，针对该节点的该应用软件存在故障。在具体实现过程中，可以根据实际场景，选择对应的重启模式。

进一步的，在步骤 303 之后，该实施例还包含如下的实现步骤：

304、该节点根据上述修改防火墙策略的通知，修改该节点对应防火墙的防火墙策略。

在具体实现中，该节点根据上述修改防火墙策略的通知，修改对应防火墙的防火墙策略。修改防火墙策略的方式和过程为本领域的公知常识，在此，不再赘述。

进一步，可选的，在步骤 302''该节点执行重启过程之后，该方法实施例还包括:

305、该节点向管理节点发送重新加入集群的请求，当管理节点确定该节点为重启节点之后，由管理节点向存储装置发送访问屏蔽解除消息。

在具体实现中，由于管理节点预先存有集群中的所有节点的信息（包含节点的标识），当该节点向管理节点发送重新加入集群的请求时，根据该节点的标识就确定该节点之前已经加入集群，现在重新发送加入集群的请求，则确定该节点为恢复节点，则由该管理节点向存储装置发送访问屏蔽解除消息。

节点加入集群的处理过程，属于本领域的现有技术，对此，本发明的所有实施例均不加以限定。

306、上述存储装置接收上述管理节点发送的访问屏蔽解除消息，该访问屏蔽解除消息包括: 该节点标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储装置有访问权限。

需要说明的是，上述访问屏蔽消息是由管理节点在接收到该节点的加入集群的请求，并确定该节点为恢复节点之后，由上述管理节点向该存储装置发送的。

307、存储装置根据上述访问屏蔽解除消息，将该节点标识对应的访问权限设置为: 有访问权限。

进一步，可选的，在根据访问屏蔽解除消息，存储装置将该节点标识对应的访问权限设置为有访问权限之后，上述方法实施例还包括:

308、存储装置向该节点发送修改防火墙策略的通知，上述修改防火墙策略的通知用于指示该节点修改该节点对应防火墙的防火墙策略，允许该节

点向存储装置发送的IO访问请求。

309、该节点根据上述修改防火墙策略的通知，修改该节点对应防火墙的防火墙策略。

进一步的，在步骤301中接收针对该节点的访问屏蔽消息之前，该方法还包括如下的步骤：

300、预先设置该节点对应防火墙的防火墙策略，上述防火墙策略用于允许该节点向存储装置发送的IO访问请求通过该防火墙。

进一步的，当采用访问控制列表ACL实现节点对存储盘的访问权限进行控制时，该方法实施例还包括如下的步骤：

300'、预先设置存储装置的访问控制列表，该访问控制列表包括：该节点的标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储装置具有访问权限。

通过上述的实现方式，使得存储装置能够根据访问控制列表实现对节点访问权限的记录，并根据访问权限向节点对应防火墙发送访问屏蔽/访问屏蔽解除消息，能够有效地实现对节点的IO访问请求进行控制的目的。

针对上述的实施例，本发明实施例还提供了两种具体的实现方式，分别介绍如下：

图4示出了对故障节点进行访问控制的方法实施例三，参看图4，在图4中，包含三个实体，分别是：管理节点、普通节点A以及存储装置A。其中，

管理节点：即对应本发明实施例的系统架构中所提及的集群中的管理节点。

普通节点A：即集群中除管理节点之外的任意一个节点，该普通节点A能够访问存储装置A。

存储装置A：即普通节点A所能够访问的一个存储装置或者所能够访问

的众多存储装置中的任意一个。

需要说明的是，对于基于存储装置的节点访问系统，存在两种应用模式，即：Share Everything（共享所有）以及 Share Nothing（无共享）。在 Share Everything 应用模式下，集群中的每一个节点都能够访问存储装置资源池中的任意一个存储装置；在 Share Nothing 应用模式下，集群中的每一个节点能够访问存储装置资源池中的部分存储装置。

该方法实施例包含如下过程：

步骤 0、系统初始化配置。

具体包含两类配置，其一，是对集群中各个节点的配置；其二，是对存储资源池中各个存储装置的配置。

针对集群中各个节点的配置有两种配置方式：

（1）将集群中的管理节点以及普通节点采用统一的配置方式：即对于集群中的每个节点，其上面均保存有针对集群中的各个节点所能够访问的存储装置的描述信息。

（2）对集群中的管理节点和普通节点采用不同的配置方式：即对于管理节点，其内部存储有针对每个节点能够访问的存储装置的描述信息；对于普通节点，其内部仅存储有针对本节点能够访问的存储装置的描述信息。

具体实现中，该描述信息包括：节点标识以及该节点所能够访问的存储装置标识的对应关系。如下作为举例，该集群包含五个节点，分别为：管理节点以及四个普通节点。针对该集群中的五个节点的配置信息如表一所示：

节点	节点所能够访问的存储装置
管理节点	存储装置 A、存储装置 B、存储装置 D
普通节点 A	存储装置 A、存储装置 C
普通节点 B	存储装置 B、存储装置 D
普通节点 C	存储装置 A、存储装置 D

普通节点 D	存储装置 B、存储装置 C

表一

针对各个存储装置的配置，具体包括：生成该存储装置的访问控制列表 ACL（Access Control List），该 ACL 包括：（1）能够访问该存储装置的节点的标识（具体实现中，节点的标识可以为该节点的 IP 地址，或者该节点在集群中的编号等）；（2）能够访问该存储装置的节点的访问权限（初始化配置该访问权限为：允许访问）。具体实现中，根据表一，以存储装置 A 为例，该存储装置的初始配置信息可通过表二所示：

节点标识	访问权限
管理节点标识	允许访问
普通节点 A 标识	允许访问
普通节点 C 标识	允许访问

表二

步骤 1、管理节点根据心跳或租约信息，检测出普通节点 A 为故障节点，记录该节点的标识。

具体实现中，由于种种原因，会导致普通节点 A 发生故障，节点的故障包含如下几种类型：物理节点的故障，节点的网络故障（如，网卡发生故障），或者节点的某一应用或者某一进程存在故障。管理节点在检测节点故障时包括两种方式：

（1）基于租约（Lease）的节点故障检测方法

在该方法中，集群中的每一个节点会定期向租约管理器（Lease Manager）申请租约；租约管理器为每个节点都维护一个有关该节点所持有租约的记录，其中记录该节点何时获取了该租约。每当租约管理器接收到来自各节点

的租约请求时，就更新该记录，以反映该节点获取租约的最新信息。如果租约管理器在指定的周期（租约期，Lease Duration）内都没有收到某个节点的续租请求，则会主动探测该节点的状态（例如：通过 Ping 方式来检测该节点是否发生故障或者该节点的网络连接状态是否发生故障），如果连续数次都探测不到该节点的状态（比如：对于 Ping 数据包，无响应），则认为该节点已经出现故障，并将该节点发生故障的通知发送给管理节点。

（2）基于心跳（Heartbeat）的节点故障检测方法

在该方法中，系统会按照某种拓扑结构在各个节点中构成一个心跳环（Heartbeat Ring），通过这个心跳环，会在各个节点之间发送心跳信息（发送心跳信息的周期通常都比租约期要短很多），当这些节点的心跳信息汇集到一起时，通常会在集群的管理节点上进行汇总，识别出是否丢失了来自某个节点的心跳信息。为了避免误判，通常会重复几次检测，如果有连续数次都没有收到来自某个节点的心跳信息，则判定该节点可能故障（此时也可以主动进行探测，进一步确认该节点是否故障）。

通过上述的节点故障检测方法，集群中的管理节点检测出普通节点 A 故障节点，则会记录该节点的标识。

这里，节点的标识可以有多种实现方式，如：该节点的 IP 地址（如：10.11.201.12），或该节点在集群中的唯一标识（如：编号 0010）或其他的实现方式，对此，本发明的实施例不加以赘述。

本步骤中，是针对发生故障的节点，记录该节点的标识，这是存在故障节点情况下的，对存储装置的访问控制的过程；对于本领域技术人员，可以理解，还可以有其他的应用场景，譬如：访问安全应用场景下，管理员控制部分节点对存储装置的访问，也可以采用本实施例的实现过程。对此，本实施例不加以限定。

步骤 2、管理节点向普通节点 A 能够访问的存储装置 A 下发访问控制消息，该消息中携带普通节点 A 的标识，以及对其访问权限的修改信息。

具体的，基于系统的初始化配置信息，管理节点上存储有集群中的每个节点所能够访问的存储装置的描述信息，管理节点可以根据该描述信息向发生故障的普通节点 A 能够访问的存储装置 A 下发访问控制消息，该消息携带有普通节点 A 的标识。作为举例，访问控制消息的格式可以表示如表三所示：

节点标识	访问权限修改信息
普通节点 A 的标识	允许访问—>拒绝访问

表三

步骤 3、存储装置 A 接收访问控制消息，并根据该访问控制消息更新自身的 ACL，将消息中携带的普通节点 A 的标识对应的访问权限设置为拒绝访问。

具体的，根据步骤 0 中的系统配置过程，存储装置 A 的配置信息参看表二，在接收到上述访问控制消息之后，将普通节点 A 标识对应的访问权限设置为拒绝访问，设置后的存储装置 A 的访问控制列表为：

节点标识	访问权限
管理节点标识	允许访问
普通节点 A 标识	拒绝访问
普通节点 C 标识	允许访问

表四

步骤 4、普通节点 A 产生针对存储装置 A 的 IO 请求，并将该 IO 请求下发给存储装置 A。

具体实现过程中，虽然普通节点 A 发生了故障，但是可能该节点并未识别自身出现发生故障（如该节点和管理节点的网络存在故障），该节点的应

用或者某一进程还会向它能够访问的存储装置 A 发送 IO 请求。上述的 IO 请求，包括对存储装置 A 中所存储的数据进行读或者写的请求。

步骤 5、存储装置 A 根据访问控制列表，判断普通节点 A 对应的访问权限是拒绝访问时，丢弃普通节点 A 所发送的 IO 请求。

具体的，参看表四的访问控制列表，存储装置 A 从中确定针对普通节点 A 对应的 IO 请求拒绝访问时，丢弃普通节点 A 的某一应用或者某一进程发送的 IO 请求。

需要说明的是，在具体实现过程中，访问控制列表可以存储在该存储装置 A 中，也可以存储在第三方设备中，对此，本发明的所有实施例均不加以限制。

步骤 6、存储装置 A 向普通节点 A 返回异常响应 E_OVERDUE。

具体的，存储装置 A 在丢弃普通节点 A 发送的 IO 请求之后，向普通节点 A 中发出该 IO 请求的某一应用或者某一进程返回异常响应代码 E_OVERDUE（错误码）。可以理解，E_OVERDUE 用于表示一种错误识别码，在具体实现中，还可能采用其他的错误码形式，对此，本实施例不加以限定。

步骤 7、普通节点 A 接收到存储装置 A 返回的异常响应 E_OVERDUE 后，则重新启动本节点。

具体的，普通节点 A 接收到异常响应 E_OVERDUE 后，就确定自身存在故障，则会重启本节点。对于节点的重启，包括两种实现方式：当普通节点 A 的硬件或者操作系统发生故障时，普通节点 A 会重启该节点的操作系统，即整个节点均会发生重启；当普通节点 A 的某一应用程序或者进程发生故障时，普通节点 A 会重启该节点的相应的应用程序或者相应的进程。

步骤 8、普通节点 A 向管理节点发送集群加入请求。

具体的，在节点发生重启之后，普通节点 A 向管理节点发送集群加入请求，该集群加入请求属于本领域的公知常识，对此，本实施例不再赘述。

步骤 9、管理节点接收到该集群加入请求后，确定普通节点 A 为故障恢复节点。

具体的，管理节点接收到普通节点 A 的集群加入请求之后，从中提取出普通节点 A 的标识，将该标识和步骤 1 记录的发生故障的节点标识对比，发现普通节点 A 的标识之前记录为发生故障，现在该节点发出集群加入请求，确定普通节点 A 为故障恢复节点。

步骤 10、管理节点向存储装置 A 下发访问屏蔽解除消息，该消息中携带普通节点 A 的标识，以及对其访问权限的修改信息。

具体的，相对应与表三中的访问控制消息，上述的访问解除消息可以采用如下的格式:

节点标识	访问权限修改信息
10.11.201.12	拒绝访问—>允许访问

步骤 11、存储装置 A 根据访问屏蔽解除消息，更新自身存储的访问控制列表 ACL，将消息中携带的普通节点 A 的标识所对应的访问权限设置为允许访问。

具体的，相对应于步骤 3 中的存储装置 A 配置信息，通过访问屏蔽解除消息，更新后的访问控制列表如表五所示:

节点标识	访问权限
管理节点标识	允许访问
普通节点 A 标识	允许访问
普通节点 C 标识	允许访问

表五

步骤 12、在完成对普通节点 A 的访问权限的设置之后，存储装置 A 向

管理节点发送访问控制解除完成消息。

步骤 13、管理节点接收到存储装置 A 发送的访问控制解除完成消息之后，向普通节点 A 返回加入集群成功响应信息。

通过上述的实现过程，存储装置通过维护能够访问该存储装置的节点的访问控制列表，能够实现对存储装置访问的控制，整个控制过程简单易行，效率较高。

上述步骤 1-2、8-10 以及 12-13 均为管理节点执行，可以理解，在具体实现的过程中，还可以由管理节点指定其他具备控制权限的节点来实现，对此，本发明的实施例不加以限定。

图 5 示出了对故障节点进行访问控制的方法实施例四，参看图 5，图 5 和图 4 所包含的实体相同，在此，不再赘述。

该方法实施例包含如下的过程:

步骤 0、系统初始化配置。

在具体实现的过程中，该实施例中除包含方法实施例三中的步骤 0 对集群中各个节点的配置以及对存储装置的配置之外，还需要对管理节点以及普通节点 A 对应防火墙的防火墙策略进行配置，即将防火墙策略预先设置为允许对所有的存储装置发送请求。此外，预先建立起普通节点 A 和存储装置 A 的可靠信道，用来传送防火墙策略的修改的通知。上述可靠信道可以有两种实现方式:

（1）采用通用的，经过加密且通过密钥进行认证的信道，如: SSH(Secure Shell，安全外壳协议)。

（2）采用专用的端口来建立专用信道，如: VPN(Virtual Private Network，虚拟专用网络)。

步骤 1-3、和方法实施例三中步骤 1-3 的实现方式类似，对此，本实施例不再赘述。

步骤 4、存储装置 A 通知普通节点 A 修改对应防火墙的防火墙策略，该防火墙策略为拒绝普通节点 A 再将 IO 请求发送给存储装置 A。

具体实现中，存储装置 A 通过系统初始化配置过程中建立的可靠信道，将修改防火墙策略的通知发送给普通节点 A。

步骤 5、普通节点 A 接收到存储装置 A 发送的修改防火墙策略的通知后，根据该通知修改对应防火墙的防火墙策略，并重新启动本节点。

具体的，普通节点 A 重新启动本节点的过程包括（图未示）：在普通节点 A 接收到存储装置 A 发送的修改防火墙策略的通知之后，存储装置 A 向普通节点 A 发送异常指示消息，该异常指示消息用于指示该节点执行重启过程；该节点根据所述异常指示消息执行节点重启过程。

步骤 6-9、和方法实施例三中步骤 8-11 的实现方式类似，对此，本实施例不再赘述。

步骤 10、存储装置 A 向普通节点 A 发送修改防火墙策略的通知，该通知用于指示普通节点 A 修改自身对应防火墙的防火墙策略，允许普通节点 A 向存储装置 A 发送 IO 请求。

步骤 11、普通节点 A 修改对应防火墙的防火墙策略，即允许该节点向存储装置 A 发送 IO 访问请求。

对于本领域技术人员来说，修改本地的防火墙策略的过程是本领域的公知常识，在此，本发明的实施例不再赘述。

步骤 12、普通节点 A 向存储装置 A 发送防火墙策略修改完成通知消息，该通知消息用于通知存储装置 A 该节点对应的防火墙策略修改完成。

步骤 13、存储装置 A 向管理节点发送访问控制解除完成消息，用来通知管理节点针对普通节点 A 的访问控制已经解除。

步骤 14、管理节点向普通节点 A 发送加入集群成功的响应。

可以理解，在具体实现过程中，本实施例中的步骤 11 可以放在步骤 14 之后执行。

通过上述的实现方式，使得存储装置能够根据访问控制列表实现对节点访问权限的记录，并根据访问权限向节点对应的防火墙发送访问屏蔽/访问屏蔽解除消息，能够有效地实现对节点的 IO 访问请求进行控制的目的。

图 6 为本发明实施例的存储装置的结构示意图。如图 6 所示，该控制器至少包括：处理器 610、存储器 620、通信接口 630 和总线 640。其中，所述处理器 610、所述存储器 620 和所述通信接口 630 通过所述总线 640 通信。

所述存储器 620 用于存放程序。具体的，程序中可以包括程序代码，所述程序代码包括计算机执行指令。所述存储器 620 可以为高速 RAM 存储器，也可以为非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。

所述处理器 610 用于执行所述存储器 620 存储的执行指令，可能为单核或多核中央处理单元（Central Processing Unit，CPU），或者为特定集成电路（Application Specific Integrated Circuit，ASIC），或者为被配置成实施本发明实施例的一个或多个集成电路。

所述通信接口 630 用于与控制点交换机通信。

当控制器运行时，处理器 610 运行程序，以执行上述四个方法实施例中任一方法实施例的方法。

参看图 7，本发明实施例还提供一种具有访问控制功能的存储装置 700，该存储装置 700 应用于集群中节点对所述存储装置的访问过程中，该存储装置 700 包括：

接收单元 710，用于接收针对节点的访问屏蔽消息，该访问屏蔽消息包括节点的标识，以及与节点的标识对应的访问权限信息，访问权限信息用于指示节点对存储装置无访问权限；

设置单元 720，用于根据访问屏蔽消息，将节点的标识对应的访问权限设置为：无访问权限；

发送单元 730，用于向节点发送修改防火墙策略的通知，该修改防火墙策略的通知用于指示节点修改该节点对应防火墙的防火墙策略，屏蔽该节点向存储装置发送的 IO 访问请求。

进一步的，在该存储装置 700 中：

接收单元 710，还用于接收节点发送的 IO 访问请求，上述 IO 访问请求包括节点的标识；

发送单元 730，还用于根据节点的标识对应的访问权限，确定发送 IO 访问请求的节点为无访问权限时，向节点发送异常指示消息，异常指示消息用于指示节点执行重启操作。

进一步的，在该存储装置 700 中：

接收单元 710，还用于接收管理节点发送的访问屏蔽解除消息，访问屏蔽解除消息包括：节点的标识，以及与节点标识对应的访问权限信息，访问权限信息用于指示节点对存储装置具有访问权限，访问屏蔽消息是在节点向管理节点发送加入集群的请求，确定节点为恢复节点之后，由管理节点发送的；

设置单元 720，还用于根据访问屏蔽解除消息，将节点标识对应的访问权限设置为：有访问权限。

进一步的，在该存储装置 700 中：

发送单元 730，还用于向节点发送修改防火墙策略的通知，该修改防火墙策略的通知用于指示节点修改对应防火墙的防火墙策略，允许节点向存储装置发送的 IO 访问请求。

进一步的，在该存储装置 700 中包括：

设置单元 720，还用于预先设置节点对应防火墙的防火墙策略，该防火墙策略用于指示节点对应防火墙，允许节点向存储装置发送的 IO 访问请求。

参看图 8，本发明实施例还提供一种实现存储装置访问的控制系统 800，

该系统实施例包括:

集群 810 以及存储装置 820，所述集群 810 包括至少一个节点，其中，该至少一个节点包含节点 811，上述节点 811 能够实现对上述存储装置 820 进行访问，其中:

上述存储装置 820，用于接收针对该节点 811 的访问屏蔽消息，上述屏蔽消息包括该节点 811 的标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点 811 对上述存储装置 820 无访问权限；用于根据上述访问屏蔽消息，将该节点标识对应的访问权限设置为无访问权限；以及用于向该节点 811 发送修改防火墙策略的通知，上述修改防火墙策略的通知用于指示上述节点 811 修改该节点 811 对应防火墙 813 的防火墙策略，屏蔽该节点 811 向上述存储装置 820 发送的 IO 访问请求。

上述节点的防火墙 813，用于根据修改防火墙策略的通知，修改自身的防火墙策略。

进一步的，对于上述控制系统 800，所述存储装置 820，还用于接收所述节点 811 发送的 IO 访问请求，所述 IO 访问请求包括节点的标识，根据节点的标识对应的访问权限，确定发送 IO 访问请求的节点 811 无访问权限时，向节点 811 发送异常指示消息，异常指示消息用于指示节点 811 执行重启操作;

节点 811，还用于根据异常指示消息，执行重启操作。

进一步的，对于上述控制系统 800，集群中还包含管理节点 812，

管理节点 812，用于接收节点 811 发送的加入集群的请求，确定节点 811 为恢复节点之后，向存储装置 820 发送访问屏蔽解除消息，上述访问屏蔽解除消息包括：节点的标识，以及与节点的标识对应的访问权限信息，上述访问权限信息用于指示节点 811 对存储装置 820 具有访问权限;

存储装置 820，还用于接收管理节点 812 发送的访问屏蔽解除消息，并根据访问屏蔽解除消息，将上述节点的标识对应的访问权限设置为有访问权

限。

进一步的，对于上述控制系统 800，

存储装置 820，还用于向节点 811 发送修改防火墙策略的通知，该修改防火墙策略的通知用于指示节点 811 对应防火墙 813 修改防火墙策略，允许节点 811 向存储装置 820 发送的 IO 访问请求；

节点 811，还用于根据上述修改防火墙策略的通知，修改对应防火墙 813 的防火墙策略。

进一步的，对于上述控制系统 800，

存储装置 820，还用于预先设置节点 811 对应防火墙 813 的防火墙策略，上述防火墙策略用于指示节点 811 对应的防火墙 813，允许节点 811 向存储装置 820 发送的 IO 访问请求。

应理解，本发明中的具体的例子只是为了帮助本领域技术人员更好地理解本发明实施例，而非限制本发明实施例的范围。

还应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

还应理解，在本发明实施例中，术语“和/或”仅仅是一种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，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超

出本发明的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的装置和单元的具体工作过程，以及方法的具体流程，可以参考前述系统实施例中的相应描述，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，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，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。另外，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接口、装置或单元的间接耦合或通信连接，也可以是电的，机械的或其它的形式连接。

所述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发明实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，

Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

权利要求

1、一种存储装置的访问控制方法，其特征在于，应用于集群中节点对所述存储装置的访问过程中，所述方法包括:

所述存储装置接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限;

所述存储装置根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为：无访问权限;

所述存储装置向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的IO访问请求。

2、根据权利要求1所述的方法，其特征在于，在所述存储装置根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为无访问权限之后，所述方法还包括:

所述存储装置接收所述节点发送的IO访问请求，所述IO访问请求包括所述节点的标识;

所述存储装置根据所述节点标识对应的访问权限，确定发送所述IO访问请求的所述节点无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作。

3、根据权利要求2所述的方法，其特征在于，在所述存储装置向所述节点发送异常指示消息之后，所述方法还包括:

所述存储装置接收管理节点发送的访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限，所述访问

屏蔽消息是在所述节点向所述管理节点发送加入集群的请求，所述管理节点确定所述节点为恢复节点后，由所述管理节点向所述存储装置发送的；

所述存储装置根据所述访问屏蔽解除消息，将所述节点标识对应的访问权限设置为：有访问权限。

4、根据权利要求 3 所述的方法，其特征在于，在所述存储装置根据所述访问屏蔽解除消息，将所述节点标识对应的访问权限设置为有访问权限之后，所述方法还包括：

所述存储装置向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，允许所述节点向所述存储装置发送的 IO 访问请求。

5、根据权利要求 1-4 任一所述的方法，其特征在于，在所述存储装置接收针对所述节点的访问屏蔽消息之前，所述方法还包括：

预先设置所述节点对应防火墙的防火墙策略，所述防火墙策略用于指示所述节点对应的防火墙，允许所述节点向所述存储装置发送的 IO 访问请求。

6、一种存储装置，其特征在于，所述存储装置包括：

处理器，存储器，通信接口和总线，其中，所述处理器、所述存储器和所述通信接口通过所述总线通信；

所述通信接口用于与集群中管理节点以及节点通信；

所述存储器用于存放程序；

当所述存储装置运行时，所述处理器用于执行所述存储器存储的所述程序，以执行所述权利要求 1-5 任一所述的方法。

7、一种具有访问控制功能的存储装置，其特征在于，该存储装置应用于集群中节点对所述存储装置的访问过程中，所述存储装置包括：

接收单元，用于接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；

设置单元，用于根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为：无访问权限；

发送单元，用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的IO访问请求。

8、根据权利要求7所述的存储装置，其特征在于，

所述接收单元，还用于接收所述节点发送的IO访问请求，所述IO访问请求包括所述节点的标识；

所述发送单元，还用于根据所述节点标识对应的访问权限，确定发送所述IO访问请求的所述节点为无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作。

9、根据权利要求8所述的存储装置，其特征在于，

所述接收单元，还用于接收管理节点发送的访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限，所述访问屏蔽消息是在所述节点向所述管理节点发送加入集群的请求，确定所述节点为恢复节点之后，由所述管理节点向所述存储装置发送的；

所述设置单元，还用于根据所述访问屏蔽解除消息，将所述节点标识对应的访问权限设置为：有访问权限。

10、根据权利要求9所述的存储装置，其特征在于，

所述发送单元，还用于向所述节点发送修改防火墙策略的通知，所述修

改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，允许所述节点向所述存储装置发送的IO访问请求。

11、根据权利要求7-10任一所述的存储装置，其特征在于，

所述设置单元，还用于预先设置所述节点对应防火墙的防火墙策略，所述防火墙策略用于指示所述节点对应的防火墙，允许所述节点向所述存储装置发送的IO访问请求。

12、一种实现存储装置访问的控制系统，其特征在于，所述系统包括：集群以及存储装置，所述集群包括至少一个节点，所述至少一个节点中的某一个节点能够对所述存储装置进行访问，

所述存储装置，用于接收针对所述节点的访问屏蔽消息，所述访问屏蔽消息包括所述节点的标识，以及与所述标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置无访问权限；用于根据所述访问屏蔽消息，将所述节点标识对应的访问权限设置为无访问权限；以及用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，屏蔽所述节点向所述存储装置发送的IO访问请求；

所述节点，用于根据所述修改防火墙策略的通知，修改对应防火墙的防火墙策略。

13、根据权利要求12所述的控制系统，其特征在于，

所述存储装置，还用于接收所述节点发送的IO访问请求，所述IO访问请求包括所述节点的标识，根据所述节点标识对应的访问权限，确定发送所述IO访问请求的所述节点无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作；

所述节点，还用于根据所述异常指示消息，执行所述节点重启操作。

14、根据权利要求 13 所述的控制系统，其特征在于，所述集群中还包含管理节点，

所述管理节点，用于接收所述节点发送的加入集群的请求，确定所述节点为恢复节点之后，向所述存储盘发送访问屏蔽解除消息，所述访问屏蔽解除消息包括：所述节点标识，以及与所述节点标识对应的访问权限信息，所述访问权限信息用于指示所述节点对所述存储装置具有访问权限；

所述存储装置，还用于接收所述管理节点发送的访问屏蔽解除消息，并根据所述访问屏蔽解除消息，将所述节点标识对应的访问权限设置为有访问权限。

15、根据权利要求 14 所述的控制系统，其特征在于，

所述存储装置，还用于向所述节点发送修改防火墙策略的通知，所述修改防火墙策略的通知用于指示所述节点修改所述节点对应防火墙的防火墙策略，允许所述节点向所述存储装置发送的 IO 访问请求；

所述节点，还用于根据所述修改防火墙策略的通知，修改对应防火墙的防火墙策略。

16、根据权利要求 12-15 任一所述的控制系统，其特征在于，

所述存储装置，还用于预先设置所述节点对应防火墙的防火墙策略，所述防火墙策略用于指示所述节点对应的防火墙，允许所述节点向所述存储装置发送的 IO 访问请求。

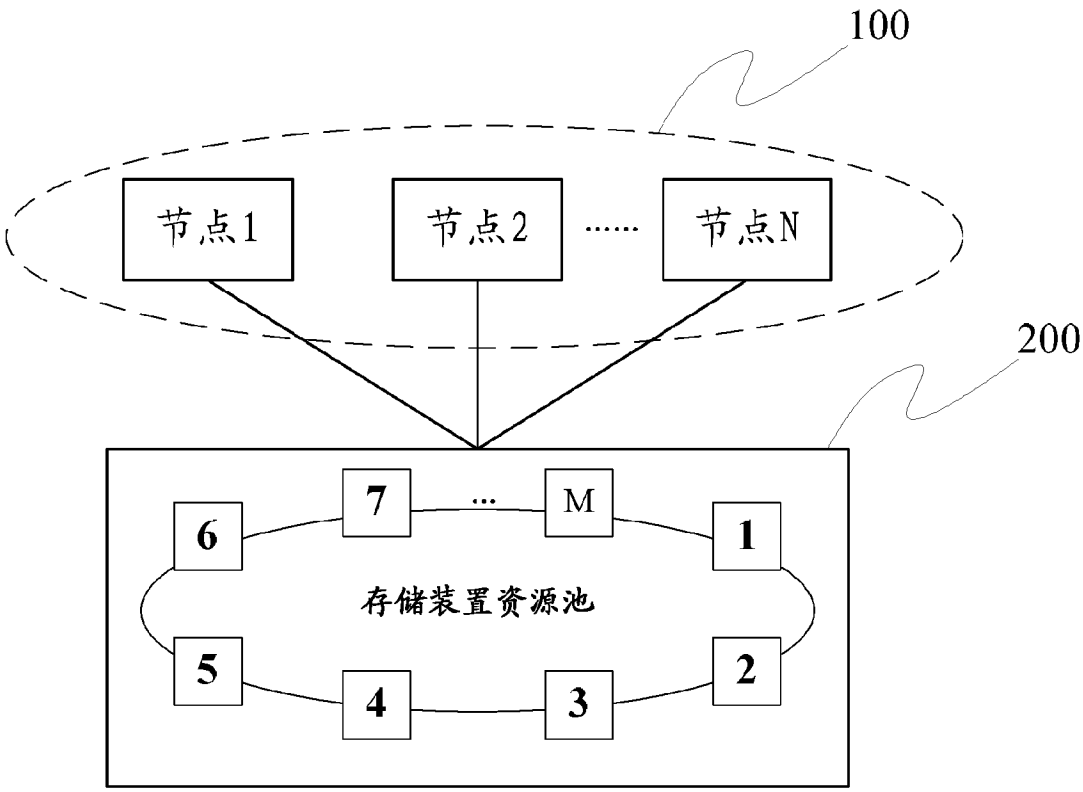

图1

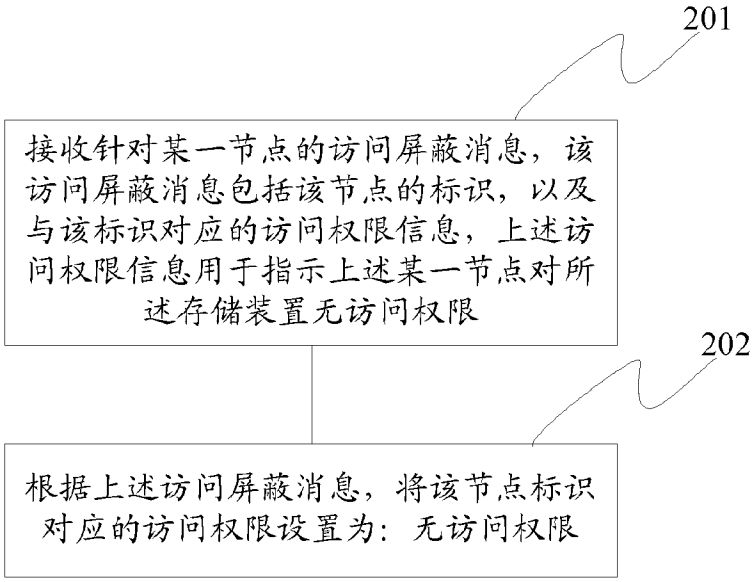
201
接收针对某一节点的访问屏蔽消息，该访问屏蔽消息包括该节点的标识，以及与该标识对应的访问权限信息，上述访问权限信息用于指示上述某一节点对所述存储装置无访问权限
202
根据上述访问屏蔽消息，将该节点标识对应的访问权限设置为：无访问权限

图2

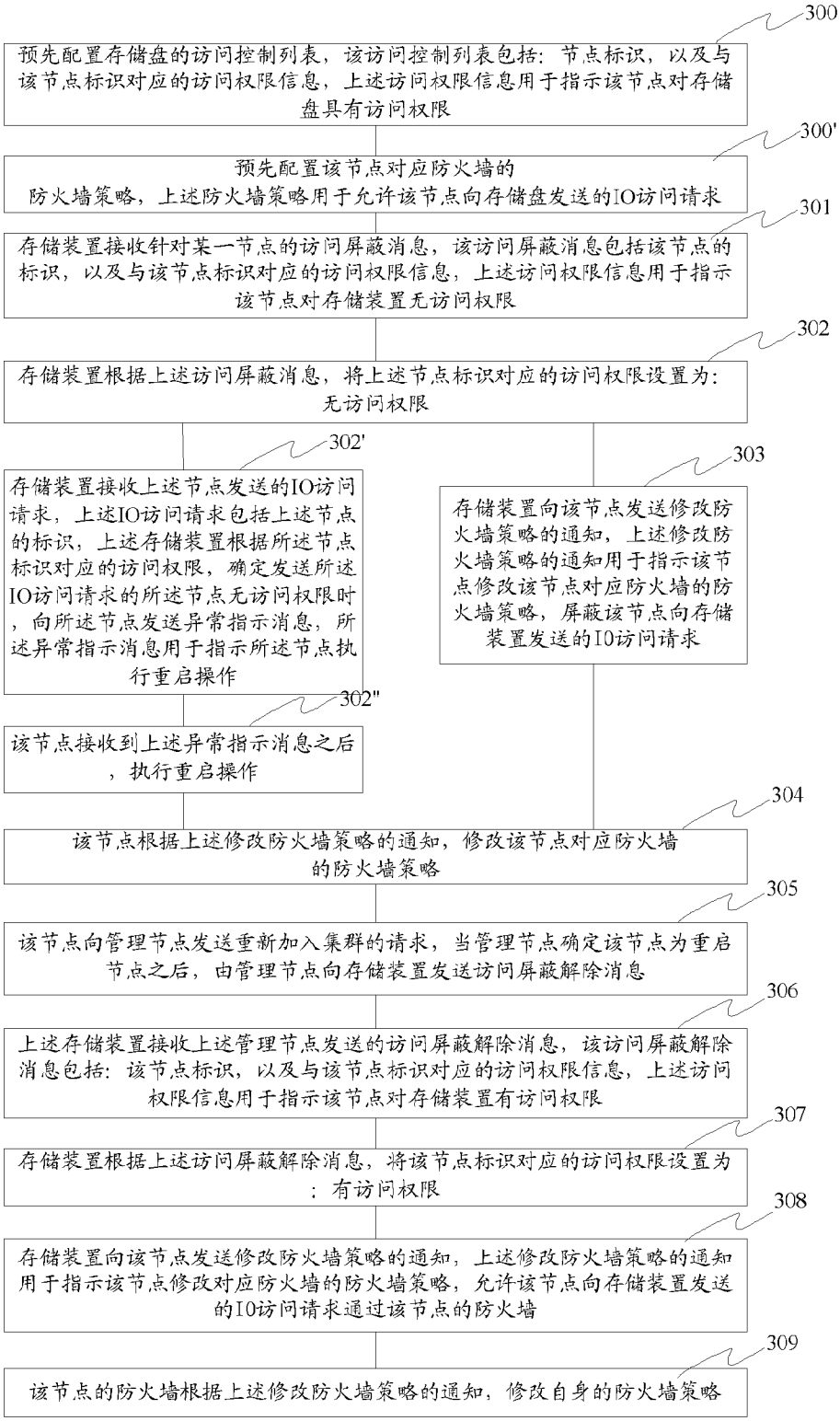
300
预先配置存储盘的访问控制列表，该访问控制列表包括：节点标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储盘具有访问权限
300'
预先配置该节点对应防火墙的防火墙策略，上述防火墙策略用于允许该节点向存储盘发送的IO访问请求
301
存储装置接收针对某一节点的访问屏蔽消息，该访问屏蔽消息包括该节点的标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储装置无访问权限
302
存储装置根据上述访问屏蔽消息，将上述节点标识对应的访问权限设置为：无访问权限
302'
存储装置接收上述节点发送的IO访问请求，上述IO访问请求包括上述节点的标识，上述存储装置根据所述节点标识对应的访问权限，确定发送所述IO访问请求的所述节点无访问权限时，向所述节点发送异常指示消息，所述异常指示消息用于指示所述节点执行重启操作
303
存储装置向该节点发送修改防火墙策略的通知，上述修改防火墙策略的通知用于指示该节点修改该节点对应防火墙的防火墙策略，屏蔽该节点向存储装置发送的IO访问请求
302"
该节点接收到上述异常指示消息之后，执行重启操作
304
该节点根据上述修改防火墙策略的通知，修改该节点对应防火墙的防火墙策略
305
该节点向管理节点发送重新加入集群的请求，当管理节点确定该节点为重启节点之后，由管理节点向存储装置发送访问屏蔽解除消息
306
上述存储装置接收上述管理节点发送的访问屏蔽解除消息，该访问屏蔽解除消息包括：该节点标识，以及与该节点标识对应的访问权限信息，上述访问权限信息用于指示该节点对存储装置有访问权限
307
存储装置根据上述访问屏蔽解除消息，将该节点标识对应的访问权限设置为：有访问权限
308
存储装置向该节点发送修改防火墙策略的通知，上述修改防火墙策略的通知用于指示该节点修改对应防火墙的防火墙策略，允许该节点向存储装置发送的IO访问请求通过该节点的防火墙
309
该节点的防火墙根据上述修改防火墙策略的通知，修改自身的防火墙策略

图 3

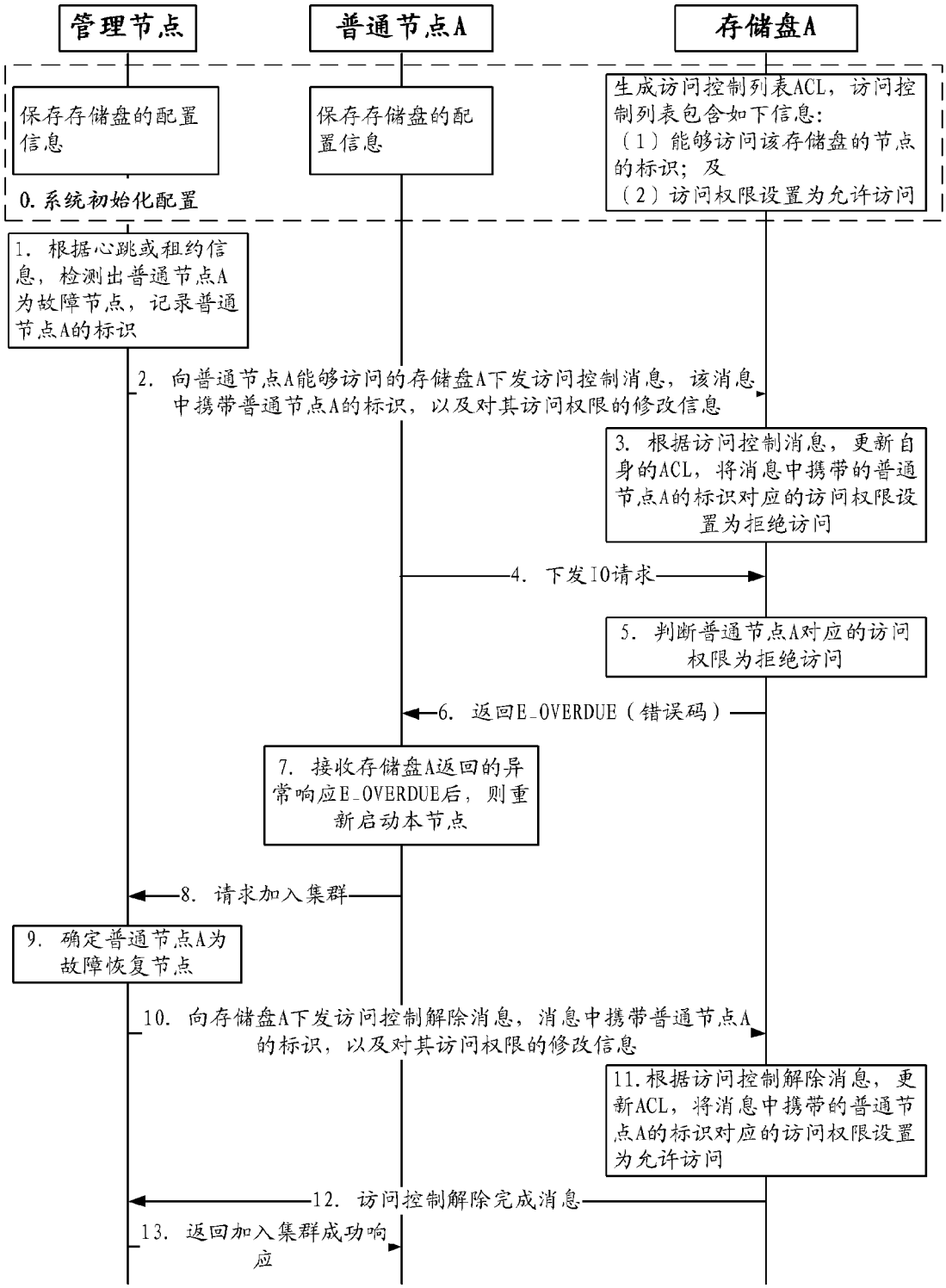
管理节点
普通节点A
存储盘A
保存存储盘的配置信息
保存存储盘的配置信息
生成访问控制列表ACL，访问控制列表包含如下信息：
（1）能够访问该存储盘的节点的标识；及
（2）访问权限设置为允许访问
0. 系统初始化配置
1. 根据心跳或租约信息，检测出普通节点A为故障节点，记录普通节点A的标识
2. 向普通节点A能够访问的存储盘A下发访问控制消息，该消息中携带普通节点A的标识，以及对其访问权限的修改信息
3. 根据访问控制消息，更新自身的ACL，将消息中携带的普通节点A的标识对应的访问权限设置为拒绝访问
4. 下发IO请求
5. 判断普通节点A对应的访问权限为拒绝访问
6. 返回E_OVERDUE（错误码）
7. 接收存储盘A返回的异常响应E_OVERDUE后，则重新启动本节点
8. 请求加入集群
9. 确定普通节点A为故障恢复节点
10. 向存储盘A下发访问控制解除消息，消息中携带普通节点A的标识，以及对其访问权限的修改信息
11. 根据访问控制解除消息，更新ACL，将消息中携带的普通节点A的标识对应的访问权限设置为允许访问
12. 访问控制解除完成消息
13. 返回加入集群成功响应

图4

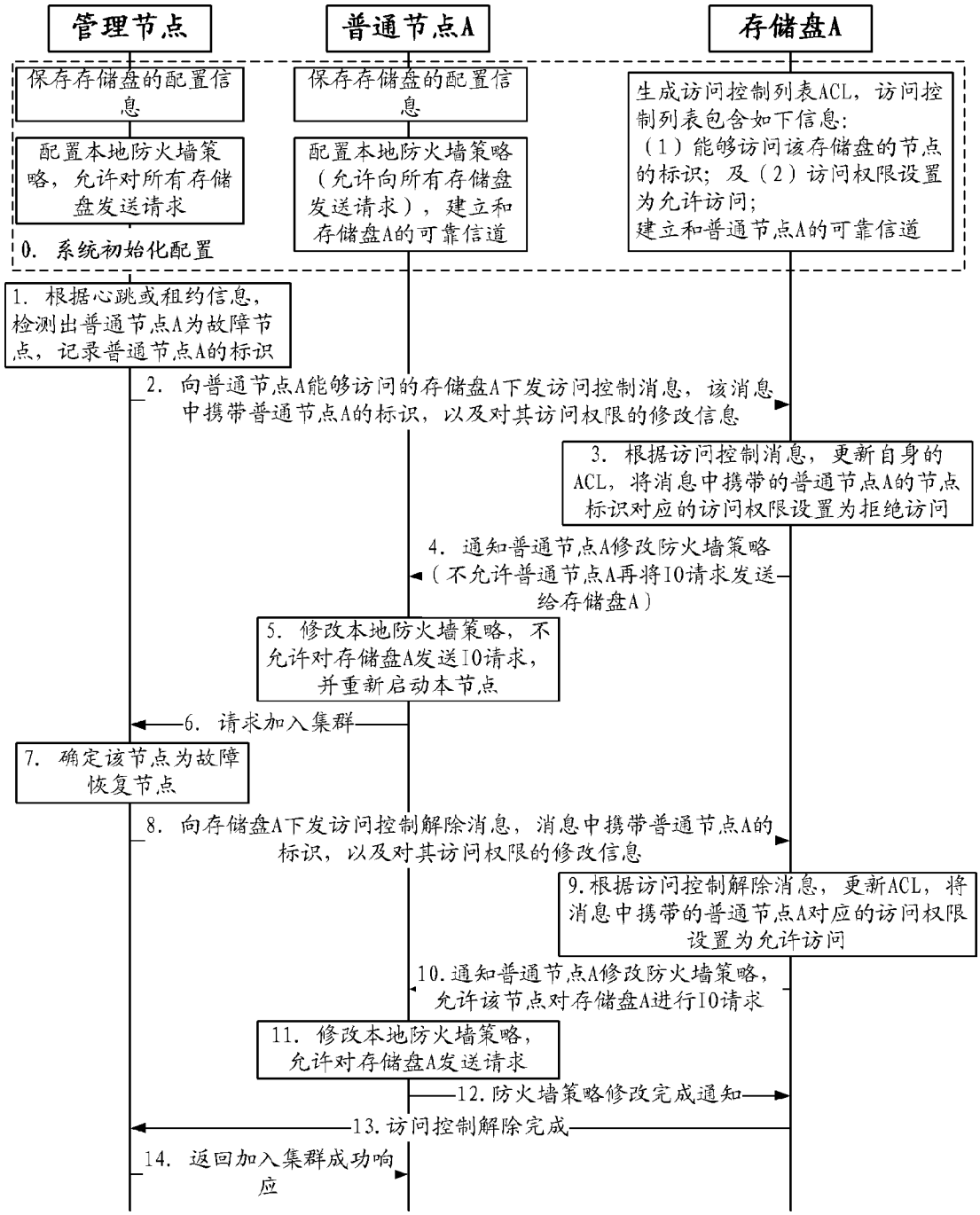
管理节点
普通节点A
存储盘A
保存存储盘的配置信息
保存存储盘的配置信息
生成访问控制列表ACL，访问控制列表包含如下信息：
（1）能够访问该存储盘的节点的标识；及（2）访问权限设置为允许访问；
建立和普通节点A的可靠信道
配置本地防火墙策略，允许对所有存储盘发送请求
配置本地防火墙策略（允许向所有存储盘发送请求），建立和存储盘A的可靠信道
0. 系统初始化配置
1. 根据心跳或租约信息，检测出普通节点A为故障节点，记录普通节点A的标识
2. 向普通节点A能够访问的存储盘A下发访问控制消息，该消息中携带普通节点A的标识，以及对其访问权限的修改信息
3. 根据访问控制消息，更新自身的ACL，将消息中携带的普通节点A的节点标识对应的访问权限设置为拒绝访问
4. 通知普通节点A修改防火墙策略（不允许普通节点A再将IO请求发送给存储盘A）
5. 修改本地防火墙策略，不允许对存储盘A发送IO请求，并重新启动本节点
6. 请求加入集群
7. 确定该节点为故障恢复节点
8. 向存储盘A下发访问控制解除消息，消息中携带普通节点A的标识，以及对其访问权限的修改信息
9. 根据访问控制解除消息，更新ACL，将消息中携带的普通节点A对应的访问权限设置为允许访问
10. 通知普通节点A修改防火墙策略，允许该节点对存储盘A进行IO请求
11. 修改本地防火墙策略，允许对存储盘A发送请求
12. 防火墙策略修改完成通知
13. 访问控制解除完成
14. 返回加入集群成功响应

图5

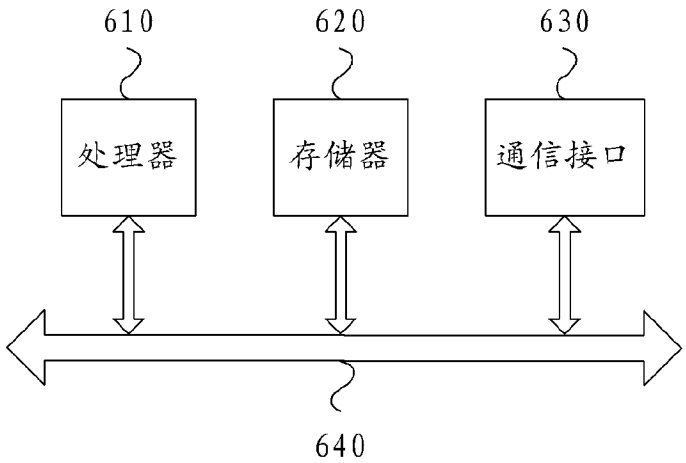

图6

700

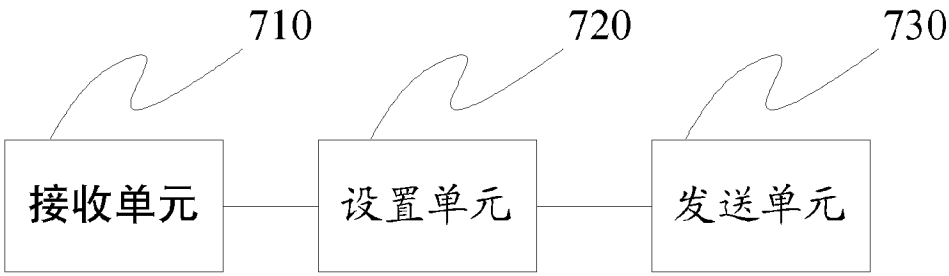

图7

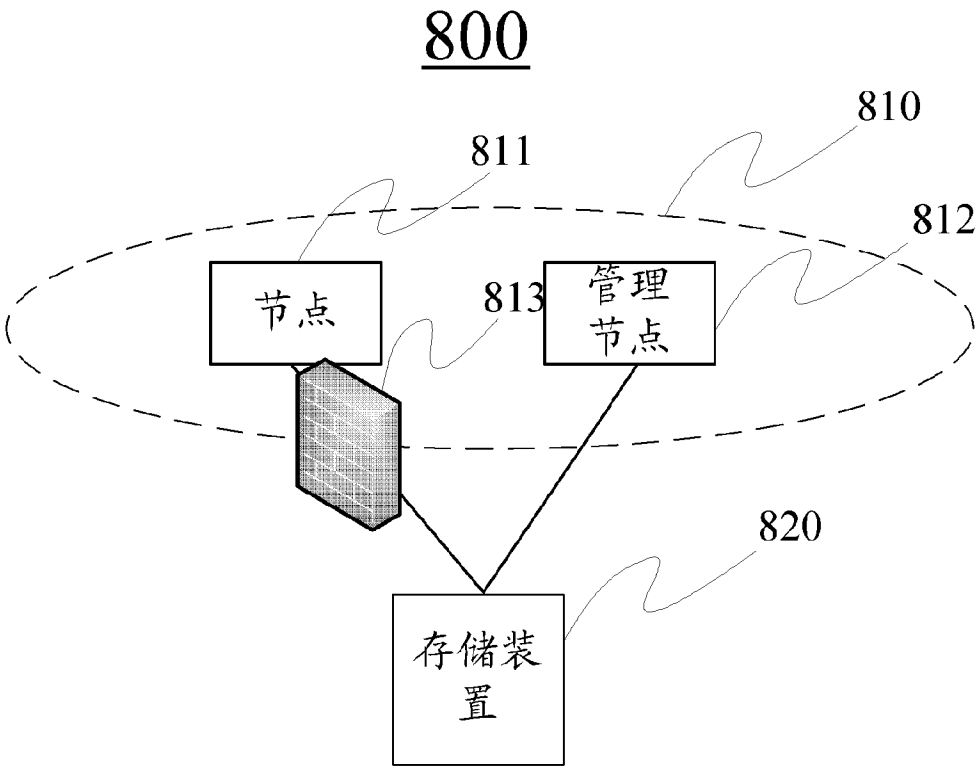

图8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/095847

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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)

H04L

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)

CNABS, EPODOC, WPI, CNKI, IEEE: isolation, shield, access, permission, storage, fencing, node, cluster, input, output, IO, I/O, firewall

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008209136 A1 (QI, Yanling et al.), 28 August 2008 (28.08.2008), description, paragraphs [0005]-[0017]	1-16
A	US 7631066 B1 (SYMANTEC OPERATING CORPORATION), 08 December 2009 (08.12.2009), the whole document	1-16
A	US 7590737 B1 (SYMANTEC OPERATING CORPORATION), 15 September 2009 (15.09.2009), the whole document	1-16
A	CN 103458036 A (H3C TECHNOLOGIES CO., LIMITED), 18 December 2013 (18.12.2013), the whole document	1-16
A	CN 1866966 A (HANGZHOU HUAWEI 3COM TECHNOLOGY CO., LTD.), 22 November 2006 (22.11.2006), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 September 2015 (09.09.2015)	**25 September 2015 (25.09.2015)**
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 **KANG, Kai** Telephone No.: (86-10) **62414043**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/095847

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2008209136 A1	28 August 2008	None	
US 7631066 B1	08 December 2009	None	
US 7590737 B1	15 September 2009	US 8370494 B1	05 February 2013
CN 103458036 A	18 December 2013	None	
CN 1866966 A	22 November 2006	CN 100563255 C	25 November 2009

国际检索报告

国际申请号
PCT/CN2014/095847

A. 主题的分类

H04L 29/06(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)

H04L

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）)

CNABS, EPODOC, WPI, CNKI, IEEE:存储，节点，集群，隔离，屏蔽，访问，权限，storage, fencing, node, cluster, input, output, IO, I/O, firewall

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
A	US 2008209136 A1 (QI, YANLING 等) 2008年 8月 28日 (2008-08-28) 说明书第[0005]-[0017]段	1-16
A	US 7631066 B1 (SYMANTEC OPERATING CORPORATION) 2009年 12月 8日 (2009-12-08) 全文	1-16
A	US 7590737 B1 (SYMANTEC OPERATING CORPORATION) 2009年 9月 15日 (2009-09-15) 全文	1-16
A	CN 103458036 A (杭州华三通信技术有限公司) 2013年 12月 18日 (2013-12-18) 全文	1-16
A	CN 1866966 A (杭州华为三康技术有限公司) 2006年 11月 22日 (2006-11-22) 全文	1-16

☐ 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	国际检索报告邮寄日期
2015年 9月 9日	2015年 9月 25日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	康凯
传真号 (86-10)62019451	电话号码 (86-10)62414043

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/095847

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）
US 2008209136 A1	2008年 8月 28日	无	
US 7631066 B1	2009年 12月 8日	无	
US 7590737 B1	2009年 9月 15日	US 8370494 B1	2013年 2月 5日
CN 103458036 A	2013年 12月 18日	无	
CN 1866966 A	2006年 11月 22日	CN 100563255 C	2009年 11月 25日

表 PCT/ISA/210（同族专利附件）（2009年7月）