(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 103297441 A
(43)申请公布日 2013.09.11

(21)申请号 201310255700.0

(22)申请日 2013.06.25

(71)申请人 福建伊时代信息科技股份有限公司
地址 350015 福建省福州市马尾区江滨东大道 108 号福建留学人员创业园 B 区 4F

(72)发明人 许元进 黄永权 杨泉清

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 韩建伟 吴贵明

(51)Int.Cl.
H04L 29/06(2006.01)

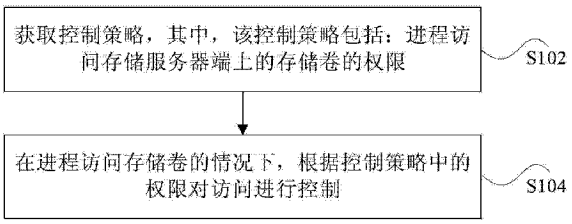
权利要求书2页 说明书7页 附图3页

(54)发明名称

访问控制方法和装置

(57)摘要

本申请公开了一种访问控制方法和装置，其中，该方法包括：获取控制策略，其中，该控制策略包括：进程访问存储服务器端上的存储卷的权限；在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制。通过本申请，解决了基于网络的存储系统没有访问控制机制的问题，提高了存储系统的安全性。



CN 103297441 A

1. 一种访问控制方法，其特征在于包括：

获取控制策略，其中，所述控制策略包括：进程访问存储服务器端上的存储卷的权限；

在所述进程访问所述存储卷的情况下，根据所述控制策略中的权限对所述访问进行控制。

2. 根据权利要求 1 所述的方法，其特征在于，根据所述控制策略中的权限对所述访问进行控制包括：

根据所述进程的信息从所述控制策略中查找所述进程对应的权限，其中，所述进程的信息包括以下至少之一：所述进程的进程名、所述进程的签名哈希值；

根据所述控制策略中的所述进程对应的权限对所述访问进行控制。

3. 根据权利要求 2 所述的方法，其特征在于，在根据所述进程的信息查找所述进程对应的权限之后，所述方法还包括：

在从所述控制策略中未查找到所述进程对应的权限的情况下，拒绝所述访问。

4. 根据权利要求 1 所述的方法，其特征在于，获取所述控制策略包括：

从所述服务器端获取所述控制策略，其中，所述服务器端提供用于管理所述控制策略的接口，所述管理包括以下至少之一：添加、修改、删除。

5. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

获取连接参数；

根据所述连接参数对所述映射进行管理，其中，所述管理包括以下至少之一：将所述存储卷挂载到本地以形成所述映射、移除所述映射、在连接所述存储卷失败的情况下重新挂载所述存储卷。

6. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述进程的子进程通过权限继承获得与所述进程访问所述存储卷相同的权限。

7. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述存储卷包括因特网小型计算机系统接口存储卷。

8. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述权限包括以下至少之一：所述进程是否被允许从所述存储卷读取数据、所述进程是否被允许向所述存储卷写入数据、所述进程是否被允许修改所述存储卷上的数据、所述进程是否被允许执行所述存储卷上的数据。

9. 一种访问控制装置，其特征在于包括：

第一获取模块，用于获取控制策略，其中，所述控制策略包括：进程访问存储服务器端上的存储卷的权限；

控制模块，用于在所述进程访问所述存储卷的情况下，根据所述控制策略中的权限对所述访问进行控制。

10. 根据权利要求 9 所述的装置，其特征在于，所述控制模块包括：

查找单元，用于根据所述进程的信息从所述控制策略中查找所述进程对应的权限，其中，所述进程的信息包括以下至少之一：所述进程的进程名、所述进程的签名哈希值；

控制单元，用于根据所述控制策略中的所述进程对应的权限对所述访问进行控制。

11. 根据权利要求 10 所述的装置，其特征在于，所述控制单元还用于在从所述控制策略中未查找到所述进程对应的权限的情况下，拒绝所述访问。

12. 根据权利要求 9 所述的装置，其特征在于，所述第一获取模块用于从所述服务器端获取所述控制策略，其中，所述服务器端提供用于管理所述控制策略的接口，所述管理包括以下至少之一：添加、修改、删除。

13. 根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

第二获取模块，用于获取连接参数；

管理模块，用于根据所述连接参数对所述映射进行管理，其中，所述管理包括以下至少之一：将所述存储卷挂载到本地以形成所述映射、移除所述映射、在连接所述存储卷失败的情况下重新挂载所述存储卷。

访问控制方法和装置

技术领域

[0001] 本申请涉及通信领域，具体而言，涉及访问控制方法和装置。

背景技术

[0002] 随着网络技术的发展，基于网络的存储系统得到了广泛的应用。例如，因特网小型计算机系统接口（Internet Small Computer System Interface，简称为 iSCSI）存储系统因其具有容量大、性能高、扩展性能好等优点，已经得到了广泛的应用。

[0003] iSCSI 技术是基于小型计算机系统接口（Small Computer Systems Interface，简称为 SCSI）技术发展起来的，该 SCSI 技术是被磁盘、磁带等设备广泛采用的存储标准。并且，iSCSI 沿用了传输控制协议 / 因特网协议（Transmission Control Protocol/Internet Protocol，简称为 TCP/IP），SCSI 和 TCP/IP 技术为 iSCSI 的扩展提供了技术基础。

[0004] iSCSI 协议定义了在 TCP/IP 网络发送、接收数据块（block）级的存储数据的规则和方法。发送端将 SCSI 命令和数据封装到 TCP/IP 包中通过网络转发，接收端收到该 TCP/IP 包之后，将其还原为 SCSI 命令和数据并执行，完成之后将返回的 SCSI 命令和数据再封装到 TCP/IP 包中再传送回发送端。整个过程在用户看来，使用远端的存储设备就象访问本地的 SCSI 设备一样。支持 iSCSI 技术的服务器和存储设备能够直接连接到现有的 IP 交换机和路由器上，因此 iSCSI 技术具有易于安装、成本低廉、不受地理限制、良好的互操作性等优势。

[0005] iSCSI 在实际应用中也存在着问题。由于 iSCSI 的设计标准是在不受信任的广域网环境中使用，iSCSI 技术的核心是在 TCP/IP 网络上传输 SCSI 协议，使得 SCSI 命令和数据可以在普通以太网络上进行传输，由 IP 网络负责其传输的可靠性。这就使得 iSCSI 也不得不面临 IP 网络中的安全性问题，例如身份伪装、伪造信息插入、数据删除 / 修改、窃听、数据分析等。在 iSCSI 存储系统中没有进行任何访问认证控制，无法保护 iSCSI 卷不被非法访问，容易造成数据泄密。对于其他网络存储系统，其也存在于 iSCSI 相似的问题。

[0006] 针对相关技术中基于网络的存储系统没有访问控制机制的问题，目前尚未提出有效的解决方案。

发明内容

[0007] 本申请提供了一种访问控制方法和装置，以至少解决基于网络的存储系统没有访问控制机制的问题。

[0008] 根据本申请的一个方面，提供了一种访问控制方法，包括：获取控制策略，其中，所述控制策略包括：进程访问存储服务器端上的存储卷的权限；在所述进程访问所述存储卷的情况下，根据所述控制策略中的权限对所述访问进行控制。

[0009] 优选地，根据所述控制策略中的权限对所述访问进行控制包括：根据所述进程的信息从所述控制策略中查找所述进程对应的权限，其中，所述进程的信息包括以下至少之一：所述进程的进程名、所述进程的签名哈希值；根据所述控制策略中的所述进程对应的

权限对所述访问进行控制。

[0010] 优选地，在根据所述进程的信息查找所述进程对应的权限之后，所述方法还包括：在从所述控制策略中未查找到所述进程对应的权限的情况下，拒绝所述访问。

[0011] 优选地，获取所述控制策略包括：从所述服务器端获取所述控制策略，其中，所述服务器端提供用于管理所述控制策略的接口，所述管理包括以下至少之一：添加、修改、删除。

[0012] 优选地，所述方法还包括：获取连接参数；根据所述连接参数对所述映射进行管理，其中，所述管理包括以下至少之一：将所述存储卷挂载到本地以形成所述映射、移除所述映射、在连接所述存储卷失败的情况下重新挂载所述存储卷。

[0013] 优选地，所述进程的子进程通过权限继承获得与所述进程访问所述存储卷相同的权限。

[0014] 优选地，所述存储卷包括因特网小型计算机系统接口存储卷。

[0015] 优选地，所述权限包括以下至少之一：所述进程是否被允许从所述存储卷读取数据、所述进程是否被允许向所述存储卷写入数据、所述进程是否被允许修改所述存储卷上的数据、所述进程是否被允许执行所述存储卷上的数据。

[0016] 根据本申请的另一个方面，还提供了一种访问控制装置，包括：第一获取模块，用于获取控制策略，其中，所述控制策略包括：进程访问存储服务器端上的存储卷的权限；控制模块，用于在所述进程访问所述存储卷的情况下，根据所述控制策略中的权限对所述访问进行控制。

[0017] 优选地，所述控制模块包括：查找单元，用于根据所述进程的信息从所述控制策略中查找所述进程对应的权限，其中，所述进程的信息包括以下至少之一：所述进程的进程名、所述进程的签名哈希值；控制单元，用于根据所述控制策略中的所述进程对应的权限对所述访问进行控制。

[0018] 优选地，所述控制单元还用于在从所述控制策略中未查找到所述进程对应的权限的情况下，拒绝所述访问。

[0019] 优选地，所述第一获取模块用于从所述服务器端获取所述控制策略，其中，所述服务器端提供用于管理所述控制策略的接口，所述管理包括以下至少之一：添加、修改、删除。

[0020] 优选地，所述装置还包括：第二获取模块，用于获取连接参数；管理模块，用于根据所述连接参数对所述映射进行管理，其中，所述管理包括以下至少之一：将所述存储卷挂载到本地以形成所述映射、移除所述映射、在连接所述存储卷失败的情况下重新挂载所述存储卷。

[0021] 通过本申请，采用获取控制策略，其中，该控制策略包括：进程访问存储服务器端上的存储卷的权限；在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制的方式，解决了基于网络的存储系统没有访问控制机制的问题，提高了网络存储系统的安全性。

附图说明

[0022] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0023] 图 1 是根据本申请实施例的访问控制方法的流程图；

[0024] 图 2 是根据本申请实施例的访问控制装置的结构框图；

[0025] 图 3 是根据本申请实施例的访问控制装置的优选结构框图一；

[0026] 图 4 是根据本申请实施例的访问控制装置的优选结构框图二；

[0027] 图 5 是根据本申请优选实施例的访问控制系统的结构框图；

[0028] 图 6 是根据本申请优选实施例的访问控制系统的工作流程图。

具体实施方式

[0029] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0030] 需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。以下实施例可以应用于因特网小型计算机系统接口系统中，其中的存储卷包括因特网小型计算机系统接口存储卷。但并不限于此，其他的基于网络的存储系统也可以应用以下实施例中的方案。

[0031] 以下实施例可以使用其它通用或专用计算或通信环境或配置来操作。适用于以下实施例的众所周知的计算系统、环境和配置的示例包括但不限于，个人计算机、服务器，多处理器系统、基于微处理的系统、小型机、大型计算机、智能设备、终端(包括移动终端)、以及包括任一上述系统或设备的分布式计算环境。

[0032] 本申请实施例提供了一种访问控制方法，图 1 是根据本申请实施例的访问控制方法的流程图，如图 1 所示，该方法包括如下的步骤：

[0033] 步骤 S102，获取控制策略，其中，该控制策略包括：进程访问存储服务器端上的存储卷的权限；

[0034] 步骤 S104，在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制。

[0035] 通过上述步骤，根据控制策略中进程访问存储服务器端上的存储卷的权限对进程的访问进行控制，从而提供了一种基于网络的访问控制方案，解决了基于网络的存储系统没有访问控制机制的问题，提高了存储系统的安全性。

[0036] 优选地，可以针对不同的进程分配不同的访问存储卷的权限，根据进程的信息查找该进程对应的权限，例如，可以在确定某个进程的访问存储服务器端的存储卷权限的情况下，根据该进程的进程名或者该进程的签名哈希值从控制策略中查找进程对应的权限的方式值。更优的，为了使进程的权限查找更加准确，可以根据进程名和进程的签名哈希值共同确定该进程所对应的权限。如果能够在控制策略中查找到相应的进程的信息，则根据该进程的信息对应的权限对该进程的访问进行控制。进程的信息与权限的对应方式可以有多种，例如，可以设置权限黑名单，该黑名单中对应的进程的权限被设置为拒绝访问该存储卷；也可以设置为权限白名单，该白名单中对应的进程被设置为相应的访问该存储卷的权限，即，在进行上述的查找后，若从控制策略中未查找到进程对应的权限的情况下，拒绝该进程对该存储卷的访问。

[0037] 为了对控制策略的统一管理，提高安全性能，可以将控制策略保存在服务器端上，在获取控制策略时，则可以从该服务器端获取控制策略。优选地，在服务器端上还可以提供

用于管理控制策略的接口，该接口可以对控制策略进行配置，例如对控制策略进行添加、修改或删除。例如，可以提供一个或几个 Web 页面，在该页面中可以对控制进行配置，这种实现方式可以使控制策略的配置更加灵活。

[0038] 在某些网络存储系统中，可以在进程访问存储服务器端上的存储卷时，先将存储卷映射到本地。在这种情况下访问存储卷时，可以像操作本地的磁盘一样进行操作。优选地，在本实施例中，还可以提供对映射的管理，例如，可以获取连接参数；然后根据该连接参数对映射进行管理，其中，管理包括以下至少之一：将存储卷挂载到本地以形成映射、移除映射、在连接存储卷失败的情况下重新挂载存储卷。

[0039] 通常情况下，在一个父进程运行时，可以还会运行多个子进程。如果父进程被认为是安全的，子进程一般情况下也被认为是安全的。因此，优选地，在对一个父进程设置了相应的权限后，其子进程也可能需要具有相应的权限，在这种情况下通过权限继承的方式，父进程的子进程可以获得与父进程访问存储卷相同的权限。当然，如果是处于安全的考虑，父进程的权限可以和子进程的权限不同，或者，父进程和子进程对于不同的存储卷，其权限是不相同的。

[0040] 优选地，上述权限包括以下至少之一：进程是否被允许从存储卷读取数据、进程是否被允许向存储卷写入数据、进程是否被允许修改存储卷上的数据、进程是否被允许执行存储卷上的数据。

[0041] 本实施例还可以提供一个用于执行上述实施例的计算机程序以及保存上述计算机程序的载体，即本申请上述实施例可以通过一个合适的计算体系结构来进行符合自然规律的运行过程。另外，尽管在上述上下文中描述本申请，但上述用于实现执行步骤的计算机程序并不意味着是限制性的，所描述的动作和操作的各方面也可用硬件来实现。

[0042] 本实施例还提供了一种访问控制装置，该装置用于实现上述访问控制方法。在该装置中涉及的对应功能也能结合上述方法所对应的描述进行结合描述和说明。

[0043] 图 2 是根据本申请实施例的访问控制装置的结构框图，如图 2 所示，该装置包括：第一获取模块 22 和控制模块 24，其中，第一获取模块 22，用于获取控制策略，其中，控制策略包括：进程访问存储服务器端上的存储卷的权限；控制模块 24 耦合至上述第一获取模块 22，，用于在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制。

[0044] 通过上述装置，采用了第一获取模块 22 获取控制策略，其中，控制策略包括：进程访问存储服务器端上的存储卷的权限；控制模块 24 在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制的方式。从而提供了一种基于网络的访问控制方案，解决了基于网络的存储系统没有访问控制机制的问题，提高了存储系统的安全性。

[0045] 本实施例中所涉及到的模块、单元可以通过软件的方式实现，也可以通过硬件的方式来实现。本实施例中所描述的模块、单元也可以设置在处理器中，例如，可以描述为：一种处理器包括第一获取模块 22 和控制模块 24。其中，这些模块的名称在某些情况下并不构成对该模块本身的限定，例如，第一获取模块 22 还可以描述为“用于获取控制策略的模块”。

[0046] 需要说明的是，上述的“第一获取模块 22”中的“第一”以及下文中可能出现的“第二获取模块”中的“第二”等类似命名方式仅用于对相应的模块进行标识，并不表示二者之间存在顺序方面的限定。

[0047] 图 3 是根据本申请实施例的访问控制装置的优选结构框图一，如图 3 所示，该控制模块 24 可以包括：查找单元 32 和控制单元 34，其中，查找单元 32，用于根据进程的信息从控制策略中查找进程对应的权限，其中，进程的信息包括以下至少之一：进程的进程名、进程的签名哈希值；控制单元 34 耦合至上述查找单元 32，用于根据控制策略中的进程对应的权限对访问进行控制。

[0048] 优选地，控制单元 34 还可以用于在从控制策略中未查找到进程对应的权限的情况下，拒绝访问。

[0049] 优选地，第一获取模块 22 用于从服务器端获取控制策略，其中，服务器端提供用于管理控制策略的接口，管理包括以下至少之一：添加、修改、删除。

[0050] 图 4 是根据本申请实施例的访问控制装置的优选结构框图二，如图 4 所示，优选地，在进程通过访问存储卷在本地的映射访问存储卷的情况下，该装置还包括：第二获取模块 42 和管理模块 44，其中，第二获取模块 42 耦合至管理模块 44，用于获取连接参数；管理模块 44 耦合至控制模块 24，用于根据连接参数对映射进行管理，其中，管理包括以下至少之一：将存储卷挂载到本地以形成映射、移除映射、在连接存储卷失败的情况下重新挂载存储卷。

[0051] 优选地，进程的子进程通过权限继承获得与进程访问存储卷相同的权限。

[0052] 优选地，上述存储卷包括因特网小型计算机系统接口存储卷。

[0053] 优选地，上述权限包括以下至少之一：进程是否被允许从存储卷读取数据、进程是否被允许向存储卷写入数据、进程是否被允许修改存储卷上的数据、进程是否被允许执行存储卷上的数据。

[0054] 下面的优选实施例是以 iSCSI 为例进行说明。

[0055] 针对相关技术中的 iSCSI 存储系统所存在的容易造成数据泄密的等不安全隐患，本优选实施例提供了一种安全快捷的用户访问 iSCSI 存储系统的方法，通过使用本优选实施例的客户端，用户在访问 iSCSI 存储系统时，能确保放置于 iSCSI 存储系统的数据安全、保障用户重要资料不遭恶意泄密和窃取。

[0056] 本优选实施例的安全访问方法采用应用系统内核进程访问控制的方式，系统由存储网关设备（也称为存储网关服务端）、应用访问控制服务构成，应用访问控制服务安装在需要进行存储控制的应用终端上，以根据存储网关服务端配置的安全控制策略对进行应用访问控制；存储网关服务端实现应用服务客户端逻辑卷的应用进程访问策略配置。

[0057] 图 5 是根据本申请优选实施例的访问控制系统的结构框图，如图 5 所示，该系统包括：应用终端和存储网关服务端。以下应用终端的功能可以通过该应用终端上运行的服务实现，可以以系统服务的形式存在。

[0058] 存储网关服务端主要实现对存储网关硬件设备模块的运行管理、维护、以及信息查看；其中，用户在存储网关服务端给应用终端配置 iSCSI 存储卷连接参数和每个卷的进程访问控制策略。存储网关服务端可以包括以下模块：

[0059] 1、参数设置模块，该模块用于完成应用终端存储卷参数设置配置；

[0060] 2、iSCSI 卷（即 iSCSI 存储卷）访问进程控制策略设置模块：该模块用于根据应用需求，添加、修改、删除不同应用终端侧（或称为存储终端）对其连接的 iSCSI 存储卷的访问或读写进程的控制策略。

[0061] 应用终端可以使向 iSCSI 存储设备提交存储数据的应用服务器或者用户终端，主要以系统服务的形式存在。应用终端上运行的服务可以包括以下模块：

[0062] 1、服务通讯模块，用于与存储网关服务端进行通讯，以自动获取 iSCSI 存储卷连接信息及进程访问控制策略；

[0063] 2、iSCSI 卷管理模块，可以根据获得的 iSCSI 存储卷连接参数实现对 iSCSI 存储卷的自动连接挂载和终止，以及实现多个 iSCSI 存储卷的管理和支持 iSCSI 存储卷连接中断的情况下，实现自动重新连接的功能；

[0064] 3、应用进程监控模块，对存储卷读写进程的访问控制，以保护连接的存储卷不被非法进程访问和操作。例如，根据存储网关下发的控制策略，实现系统应用进程(如 IIS、SQL SERVER、Oracle、Apache、Tomcat、Exchange、My SQL、FTP 等) 对 iSCSI 存储卷的访问控制。

[0065] 通过上述的应用终端可以实现安全访问 iSCSI 存储卷，保证了存储卷数据的安全性。

[0066] 图 6 是根据本申请优选实施例的访问控制系统的工作流程图，如图 6 所示，该流程包括如下步骤：

[0067] 步骤 S602，获取存储网关服务端下发的该应用终端连接 iSCSI 卷的连接参数和进程访问控制策略；

[0068] 步骤 S604，应用终端自动连接 iSCSI 存储卷，并解析下发的控制策略；

[0069] 步骤 S606，根据控制策略启动对 iSCSI 存储卷的读写访问进程控制；

[0070] 步骤 S608，判断读写访问进程是否是合法进程，在判断为是的情况下执行步骤 S610，否则执行步骤 S606；

[0071] 步骤 S610，允许进程对 iSCSI 存储卷进行数据读写等相关操作。

[0072] 在本优选实施例还提供了一个相对具体的操作流程，该流程中的步骤仅仅是一种较优的实现，该操作流程如下列步骤所示：

[0073] 步骤 S2：在需要操作的用户终端上安装应用终端的软件；

[0074] 步骤 S4：通过网页浏览器(例如其中安装的 WEB 插件)配置应用服务终端参数设置模块、和 iSCSI 卷访问进程控制策略设置模块；

[0075] 步骤 S6：获取存储网关服务端下发的该应用终端连接 iSCSI 卷的连接参数和进程控制策略；

[0076] 步骤 S8：连接挂载 iSCSI 存储盘(即 iSCSI 存储卷)，并对 iSCSI 存储盘启动执行内核进程应用控制；

[0077] 步骤 S10：根据存储网关服务端下发的该存储卷的控制策略内配置的进程名及对应的进程签名哈希值列表载入内核进程应用控制模块(即应用进程监控模块)，使存储网关服务端对该存储卷配置的所有进程成为可对该存储卷进行访问的可信进程；其中在可信进程中有个应用访问权限继承机制，即子应用进程将自动继承父应用进程的访问权限。

[0078] 步骤 S12：重复步骤 S4、S6 将存储网关服务端对该用户终端(即应用服务终端)配置所有 iSCSI 存储盘连接挂载，并进行内核进程应用控制；

[0079] 步骤 S14：当有进程访问存储盘时，内核进程应用控制模块根据进程名及对应的进程签名哈希值判断正要访问 iSCSI 存储盘的进程是否为可信进程，是否允许进程对存储卷进行数据读写等相关操作。

[0080] 在上述的优选实施例中，采用了验证和存取控制机制，确保只有授权的使用者和应用程序才可存取所存储的资料，用户可以根据自身需要的安全策略来进行调整，以支持各种进程访问控制。采用的 iSCSI 控制管理机制，实现了 iSCSI 存储卷在用户端或主机上的自动连接挂载和断开功能。

[0081] 通过上述方案的应用进程访问策略控制，解决了相关技术中的 iSCSI 存储系统中没有数据访问认证控制机制的问题，通过对前端实现应用访问权限的策略控制，实现了对 iSCSI 存储设备映射在用户相信终端主机上的逻辑卷进行监控、管理和访问控制，保证存储在逻辑卷上的数据是安全的；防范了非法进程的访问、窃取、分析数据的安全问题，有效保障了数据安全。

[0082] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0083] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

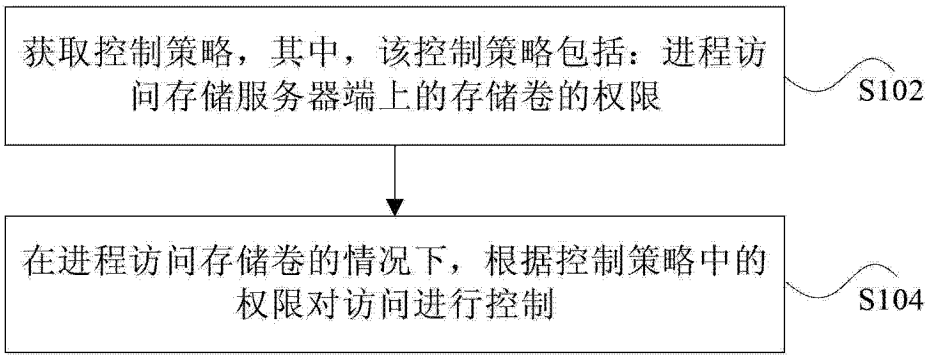

获取控制策略，其中，该控制策略包括：进程访问存储服务器端上的存储卷的权限
S102
在进程访问存储卷的情况下，根据控制策略中的权限对访问进行控制
S104

图 1

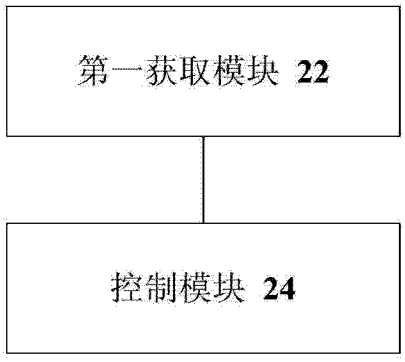

第一获取模块 22
控制模块 24

图 2

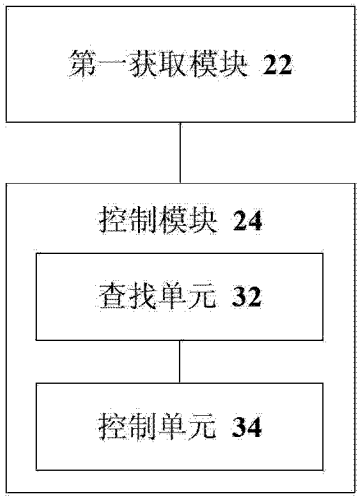

第一获取模块 22
控制模块 24
查找单元 32
控制单元 34

图 3

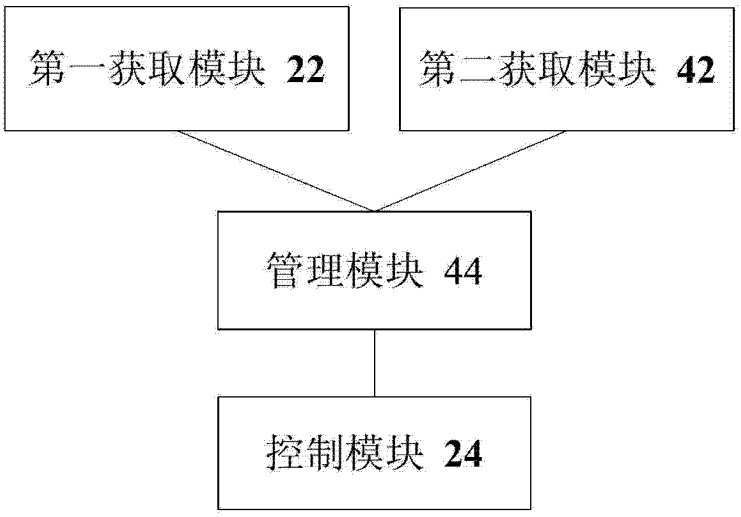

第一获取模块 22
第二获取模块 42
管理模块 44
控制模块 24

图 4

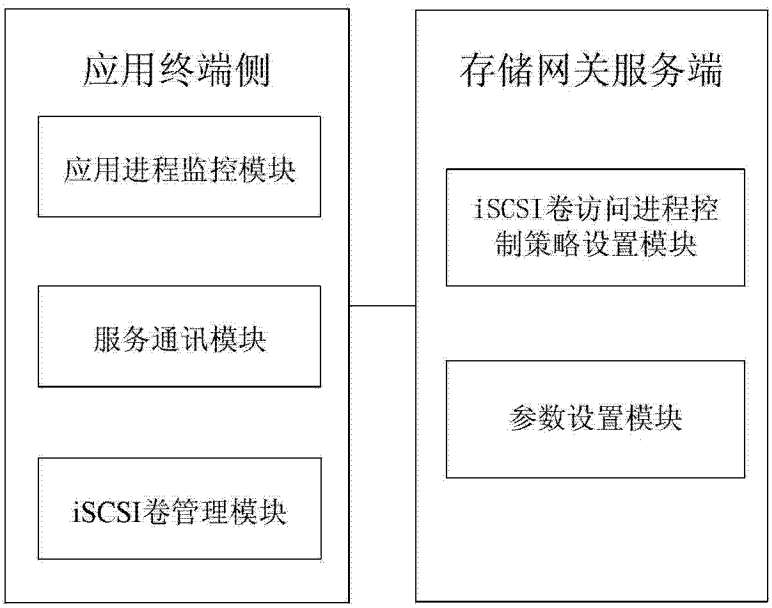

应用终端侧
应用进程监控模块
服务通讯模块
iSCSI卷管理模块
存储网关服务端
iSCSI卷访问进程控制策略设置模块
参数设置模块

图 5

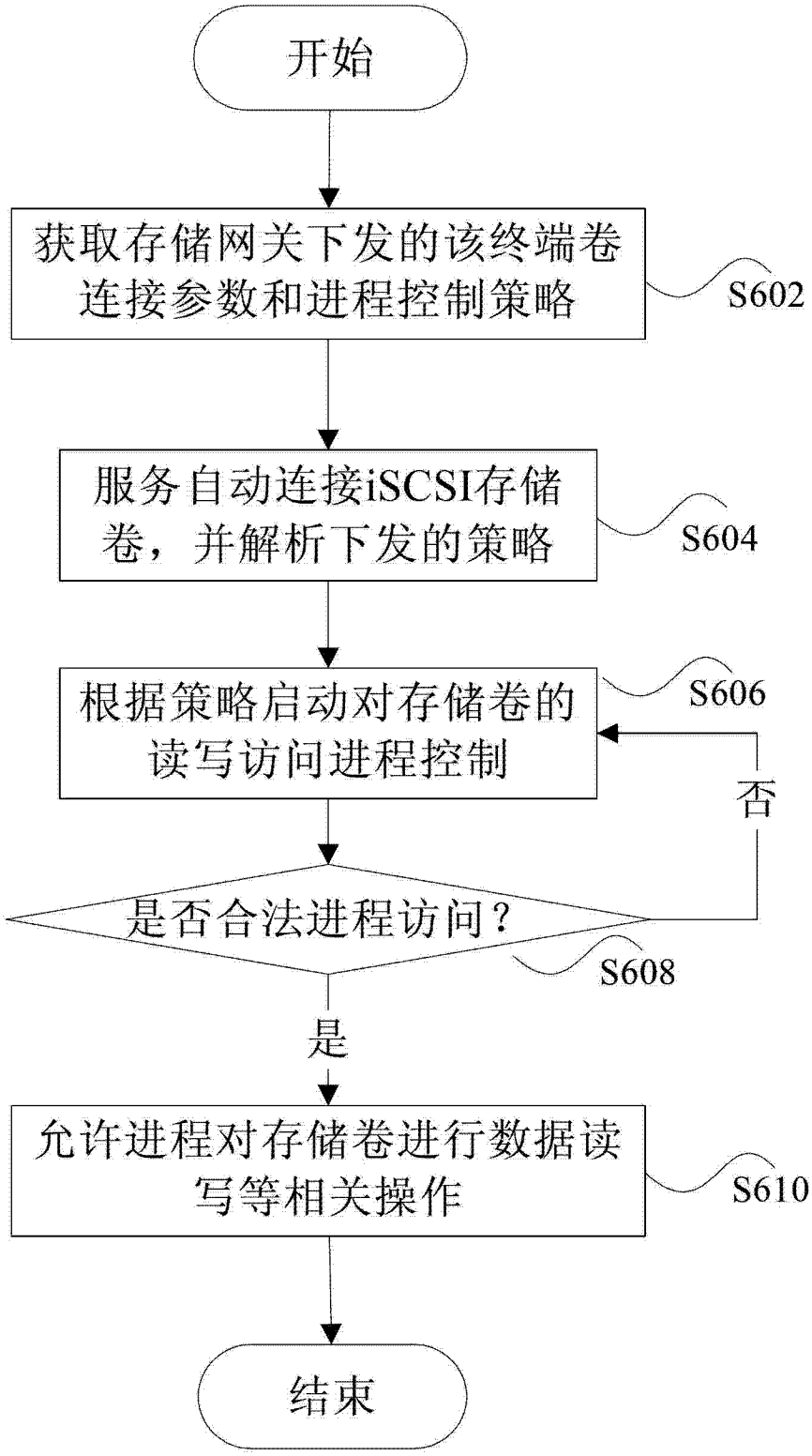

开始
获取存储网关下发的该终端卷连接参数和进程控制策略
S602
服务自动连接iSCSI存储卷，并解析下发的策略
S604
根据策略启动对存储卷的读写访问进程控制
S606
否
是否合法进程访问？
S608
是
允许进程对存储卷进行数据读写等相关操作
S610
结束

图 6