[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)
G06F 11/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510114302.2

[45] 授权公告日 2008 年 9 月 17 日

[11] 授权公告号 CN 100420202C

[22] 申请日 2005.10.20
[21] 申请号 200510114302.2
[73] 专利权人 联想(北京)有限公司
地址 100085 北京市海淀区上地信息产业基地创业路 6 号
[72] 发明人 李震海 柯 克
[74] 专利代理机构 北京银龙知识产权代理有限公司
代理人 郝庆芬

[56] 参考文献
CN 1648866A 2005.8.3
CN 1254478A 2000.5.24
CN 1506861A 2004.6.23
US 2004/0123288 A1 2004.6.24
一种虚拟化资源管理服务模型及其实现. 王敏，李静，范中磊，许鲁. 计算机学报，第 28 卷第 5 期. 2005

审查员 方 亮

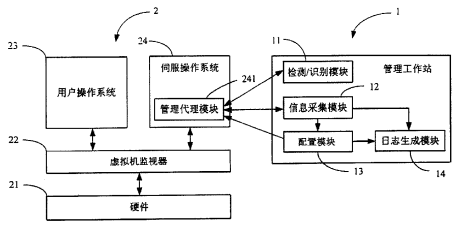
权利要求书 3 页 说明书 8 页 附图 4 页

[54] 发明名称

计算机管理系统以及计算机管理方法

[57] 摘要

本发明提供一种计算机管理系统以及计算机管理方法。 其中，该计算机管理系统包括一管理工作站以及至少一基于虚拟技术的计算机系统。 该计算机系统包括虚拟机监视器、伺服操作系统、管理代理模块以及至少一用户操作系统，该管理工作站包括检测/识别模块、信息采集模块以及配置模块。通过管理代理模块与管理工作站建立网络连接和通信，可以实现管理工作站对计算机系统的集中管理。



1. 一种计算机管理系统，包括一管理工作站以及至少一基于虚拟技术的计算机系统，其特征在于：

该计算机系统包括虚拟机监视器、伺服操作系统、管理代理模块以及至少一用户操作系统，其中，

该虚拟机监视器用于实时监控计算机设备或端口的访问控制状态，截取用户操作系统对计算机设备或端口的访问指令，并且，根据来自管理代理模块的、对用户操作系统访问计算机设备或者端口进行管理的管理控制信息，为用户操作系统分配计算机设备或端口；

该管理代理模块通过网络与管理工作站建立网络连接，并从虚拟机监视器读取的访问控制状态信息和/或访问指令，将上述访问控制状态信息和/或与访问指令相对应的授权访问请求发送给管理工作站，并将从管理工作站接收的管理控制信息发送给虚拟机监视器，

该管理工作站包括检测/识别模块、信息采集模块以及配置模块，其中，

检测/识别模块通过网络检测管理代理模块，建立与管理代理模块之间的网络连接；

信息采集模块采集来自管理代理模块的访问控制状态信息和/或授权访问请求，将其发送给配置模块；

配置模块根据访问控制状态信息或授权访问请求，产生相应的管理控制信息，并将其通过网络发送给管理代理模块。

2. 如权利要求 1 所述的计算机管理系统，其特征在于，管理代理模块将从虚拟机监视器读取的访问控制状态信息发送给管理工作站，信息采集模块采集该访问控制状态信息并发送给配置模块，配置模块对接收到的访问控制状态信息，根据策略、已存储的访问控制参数或者手工，设置相应的访问控制参数发送给管理代理模块，虚拟机监视器根据来自管理代理模块的访问控制参数，为用户操作系统分配计算机设备或端口。

3. 如权利要求 2 所述的计算机管理系统，其特征在于，该管理工作站进一步包括一日志生成模块，该信息采集模块进一步将采集到的访问控制状态

信息发送给日志生成模块，并且该配置模块将设置的访问控制参数发送给日志生成模块，由日志生成模块生成管理工作站的管理日志。

4. 如权利要求 1 至 3 任何一项所述的计算机管理系统，其特征在于，管理代理模块进一步产生系统日志。

5. 如权利要求 1 所述的计算机管理系统，其特征在于，管理代理模块将上述访问控制状态信息和与访问指令相对应的授权访问请求发送给管理工作站，信息采集模块采集该访问控制状态信息和授权访问请求，并将授权访问请求发送给配置模块，配置模块对接收到的授权访问请求，根据策略、已存储的访问控制参数，产生相应的回复发送给管理代理模块，虚拟机监视器根据来自管理代理模块的访问控制参数，为用户操作系统分配计算机设备或端口。

6. 如权利要求 5 所述的计算机管理系统，其特征在于，该管理工作站进一步包括一日志生成模块，该信息采集模块进一步将采集到的访问控制状态信息发送给日志生成模块，并且该配置模块将对授权访问请求的回复发送给日志生成模块，由日志生成模块生成管理工作站的管理日志。

7. 如权利要求 5 或者 6 任何一项所述的计算机管理系统，其特征在于，管理代理模块进一步产生系统日志。

8. 一种计算机管理方法，用于在如权利要求 1 所述的计算机管理系统中对计算机系统进行集中管理，该方法包括以下步骤：

步骤 1，通过检测/识别模块检测管理代理模块，建立计算机系统和管理工作站之间的网络连接；

步骤 2，通过虚拟机监视器实时监控计算机设备或端口的访问控制状态，截取用户操作系统对计算机设备或端口的访问指令；

步骤 3，通过管理代理模块读取上述访问控制状态信息和/或访问指令，并将访问控制状态信息和/或与访问指令对应的授权访问请求发送给管理工作站；

步骤 4，通过信息采集模块收集访问控制状态信息和/或授权访问请求，由配置模块根据来自信息采集模块的访问控制状态信息或授权访问请求产生管理控制信息，并发送给管理代理模块；

步骤 5，通过虚拟机监视器根据上述管理控制信息为用户操作系统分配计算机设备或端口。

9. 如权利要求 8 所述的计算机管理方法，其特征在于，进一步包括：

在步骤 4 和 5 之间或者在步骤 5 之后，根据访问控制状态信息和管理控制信息，由管理工作站生成管理工作站的管理日志。

10. 如权利要求 8 所述的计算机管理方法，其特征在于，进一步包括：

在步骤 5 之后，通过管理代理模块生成系统日志。

11. 如权利要求 8 至 10 任一项所述的计算机管理方法，其特征在于，当在步骤 3 中通过管理代理模块读取和发送的信息为访问控制状态信息时，该管理控制信息是由配置模块根据策略、已存储的访问控制参数或者手工所设置的访问控制参数。

12. 如权利要求 8 至 10 任一项所述的计算机管理方法，其特征在于，当在步骤 3 中通过管理代理模块读取和发送的信息为访问控制状态信息和授权访问请求时，该管理控制信息是由配置模块根据策略或已存储的访问控制参数所设置的与授权访问请求对应的回复。

计算机管理系统以及计算机管理方法

技术领域

本发明涉及一种计算机管理系统以及计算机管理方法，尤其是涉及一种基于虚拟技术的计算机管理系统以及计算机管理方法。

背景技术

随着计算机的普遍使用，对于计算机的管理也越来越成为一个重要的课题。加强计算机设备和端口的访问控制、对网络访问进行限制、授权刻盘、甚至是硬盘的授权拷贝、并对一定范围内的计算机进行集中管理，这是企业用户、教育用户以及高安全用户的需要。

现有对计算机设备和端口进行管理的方法主要通过改变硬件和增加管理软件来实现。其中，通过改变硬件对计算机设备和端口进行管理的方法有以下几种方式：

1. 物理方式，例如对 USB 接口、软驱贴封条；

2. 对 BIOS 进行重新设置；

3. 对 EFI 进行重新设置；

4. 通过主板管理控制器进行设置。

通过软件来管理计算机主要是在操作系统中加装管理软件，该管理软件用来对计算机硬件设备和端口进行访问控制，并可以根据需要实现其他的管理。

以上方式存在以下缺陷：

对于上述 1 中所述的物理方式，由于只能其单机操作、不能管理和监控，并且用户可以自行处理，例如撕毁封条，这样，使得端口访问控制无法方便的开关。

对于上述 2 中所述的 BIOS 设置，其只能单机操作、不可管理和监控，并且用户可以进入设置界面自行修改，对于端口访问的状态无法自动监控，只能人工检查。

对于上述 3 中所述的 EFI 设置，虽然其可以通过网络进行管理，但是不可监控，用户有可能进入管理界面自行设置。

对于上述 4 中所述的在主板上设置管理控制器，虽然可以实现网络管理但不是所有主板上都配有管理控制器。

以上四种方式都是硬件级的，可以实现对硬件设备和端口的控制，但无法实现其他管理。

对于在操作系统中加装管理软件的方法，虽然其可以远程管理，但用户可以自行操作操作系统，无法保证该管理软件不被破坏或失效。

同时，以后的计算机的发展将趋向于虚拟技术，该虚拟技术使得一台计算机可以同时支持多个操作系统。

因此，有必要提出一种基于虚拟技术的计算机管理系统和计算机管理方法，其可以通过网络对基于虚拟技术的计算机进行集中管理。

发明内容

本发明的目的在于，提供一种计算机管理系统。

本发明的另一目的在于，提供一种计算机管理方法。

一种计算机管理系统，包括一管理工作站以及至少一基于虚拟技术的计算机系统，其特征在于：

该计算机系统包括虚拟机监视器、伺服操作系统、管理代理模块以及至少一用户操作系统，其中，

该虚拟机监视器用于实时监控计算机设备或端口的访问控制状态，截取用户操作系统对计算机设备或端口的访问指令，并且，根据来自管理代理模块的、对用户操作系统访问计算机设备或者端口进行管理的管理控制信息，为用户操作系统分配计算机设备或端口；

该管理代理模块通过网络与管理工作站建立网络连接，并从虚拟机监视器读取的访问控制状态信息和/或访问指令，将上述访问控制状态信息和/或与访问指令相对应的授权访问请求发送给管理工作站，并将从管理工作站接收的管理控制信息发送给虚拟机监视器，

该管理工作站包括检测/识别模块、信息采集模块以及配置模块，其中，

检测/识别模块通过网络检测管理代理模块，建立与管理代理模块之间的

网络连接；

信息采集模块采集来自管理代理模块的访问控制状态信息和/或授权访问请求，将其发送给配置模块；

配置模块根据访问控制状态信息或授权访问请求，产生相应的管理控制信息，并将其通过网络发送给管理代理模块。

一种计算机管理方法，用于在上述计算机管理系统中对计算机系统进行集中管理，该方法包括以下步骤：

步骤 1，通过检测/识别模块检测管理代理模块，建立计算机系统和管理工作站之间的网络连接；

步骤 2，通过虚拟机监视器实时监控计算机设备或端口的访问控制状态，截取用户操作系统对计算机设备或端口的访问指令；

步骤 3，通过管理代理模块读取上述访问控制状态信息和/或访问指令，并将访问控制状态信息和/或与访问指令对应的授权访问请求发送给管理工作站；

步骤 4，通过信息采集模块收集访问控制状态信息和/或授权访问请求，由配置模块根据来自信息采集模块的访问控制状态信息或授权访问请求产生管理控制信息，并发送给管理代理模块；

步骤 5，通过虚拟机监视器根据上述管理控制信息为用户操作系统分配计算机设备或端口。

本发明的有益效果是：

1）对计算机设备或者端口的访问控制是通过虚拟机监视器进行参数设置实现的，非常方便管理；

2）虚拟机监视器一直运行在计算机系统的底层，可以对设备和端口的状态进行实时监控；

3）可以远程开关端口，可以采用网络集中管理的方式对端口访问进行监控；

4）除管理员，一般用户无法访问虚拟机监视器，也就无法逃避管理工作站对计算机系统的集中管理。

因此，本发明的计算机管理系统和管理方法可以很好地满足企业用户、

教育用户以及高安全用户对计算机进行集中管理的需要。

附图说明

图 1 为本发明对基于虚拟技术的计算机进行集中管理的计算机管理系统。

图 2 为计算机系统 2 的操作流程图。

图 3 为管理工作站 1 的操作流程图。

图 4 为本发明计算机管理系统的操作流程图。

具体实施方式

以下将结合附图说明本发明的计算机集中管理系统和计算机管理方法。

图 1 为本发明对基于虚拟技术的计算机进行集中管理的计算机管理系统，该计算机管理系统包括一个管理工作站 1 以及至少一基于虚拟技术的计算机系统 2。由于本发明中每个计算机系统 2 与管理工作站 1 的通信相同，因此，为了简化描述，图 1 中仅给出了一个计算机系统。

该管理工作站 1 包括检测/识别模块 11、信息采集模块 12 以及配置模块 13。另外，为了方便管理人员进行分析和管理，该管理工作站 1 可以进一步包括日志生成模块 14。该管理工作站 1 可以以主动管理和被动管理两种方式对计算机系统 2 进行集中管理。

该计算机系统 2 包括硬件 21、虚拟机监视器 22、至少一用户操作系统 23 以及伺服操作系统 24。其中，虚拟机监视器 22 安装在硬件之上，对硬件进行虚拟化，并且该虚拟机监视器 22 管理安装在其上的用户操作系统 23 对硬件 21 的访问和使用。

为了实现管理工作站 1 对计算机系统 2 中计算机设备和端口访问的管理，该伺服操作系统 24 中进一步设置了一个管理代理模块 241。该管理代理模块 241 可以通过网络与管理工作站 1 通信。通过管理代理模块 241 与管理工作站 1 的通信，可以实现管理工作站 1 对计算机系统 2 的集中管理。

图 2 为计算机系统 2 的操作流程图，具体步骤如下：

步骤 1，启动计算机系统 2；

步骤 2，启动伺服操作系统 24，载入虚拟机监视器 22，虚拟机监视器 22 虚拟计算机设备和端口；

步骤 3，启动管理代理模块 241，虚拟机监视器 22 根据管理代理模块 241 中的端口访问参数为用户操作系统 23 分配设备或者端口，该端口访问参数可以是为了用户操作系统能够访问操作所预先设定的参数，也可以是上次操作后所存储的端口访问参数；

步骤 4，启动用户操作系统 23，该用户操作系统 23 发出访问操作分配给它的设备和端口的指令；

步骤 5，虚拟机监视器 22 实时监控计算机设备或者端口的访问状态，并截取用户操作系统 23 对计算机设备或者端口的访问指令；

步骤 6，管理代理模块 241 定时从虚拟机监视器 22 读取计算机设备或者端口的访问控制状态，或者用户操作系统 23 对计算机设备或者端口的访问指令，然后，将访问控制状态和/或根据访问指令生成的授权访问请求通过网络发送给管理工作站 1，并从管理工作站 1 获得与访问控制状态对应的端口访问参数或者与授权访问请求对应的回复，并将其发送给虚拟机监视器 22；

步骤 7，虚拟机监视器 22 根据端口访问参数设置用户操作系统 23 可以访问的计算机设备或者端口，或者根据回复允许/屏蔽用户操作系统 23 访问的计算机设备或者端口。

为了便于本地对计算机系统 2 的管理，管理代理模块 241 将进一步生成系统日志。

图 3 为管理工作站的操作流程图，具体步骤如下：

步骤 a，启动管理工作站 1；

步骤 b，该检测/识别模块 11 通过网络发现管理代理模块 241，建立管理工作站 1 与被管理的计算机系统 2 的网络连接；

步骤 c，信息采集模块 12 可以通过网络采集从代理管理模块 241 发出的计算机设备或者端口的访问状态信息和/或者授权访问请求，然后将访问状态信息和/或者发送给配置模块 13；

步骤 d，配置模块 13 一方面可以根据访问状态信息，通过策略、已存储的访问控制参数或者手工设置等方式设置被管理设备的端口访问参数，并将设置的端口访问参数发送给管理代理模块 241，或者，另一方面可以根据访问状态信息和授权访问请求，通过策略或者已存储的访问控制参数对授权访

问请求作出回复（允许访问或者屏蔽），并将该回复发送给管理代理模块241；

步骤e，虚拟机监视器22根据从管理代理模块241接收的端口访问控制参数为用户操作系统23分配设备或者端口，或者根据从管理代理模块241接收的回复允许或者屏蔽用户操作系统23访问操作所分配的计算机设备或端口。借此，管理工作站1实现了对用户操作系统对设备或者端口的访问的控制。

进一步，该信息采集模块12可以将访问状态信息和/或者授权访问请求发送给日志生成模块14，同时，该配置模块13也可以将端口访问参数或者对授权访问请求的回复发送给日志生成模块14，日志生成模块14根据来自信息采集模块12的端口访问状态信息以及来自配置模块13的端口访问参数或者对授权访问请求的回复生成相应的日志。

为了更清楚地了解本发明，请参阅图4，为本发明计算机管理系统的操作流程图。

在管理工作站1启动后并且在计算机系统2启动用户操作系统23后，管理工作站1中的检测/识别模块11通过检测到管理代理模块241，建立与计算机系统2之间的网络连接。

在计算机系统2中，虚拟机监视器22实时监控计算机设备或者端口的访问状态，并截取用户操作系统23对计算机设备或者端口的访问指令。由于对于主动管理模式和被动管理模式，后续的操作流程将有所不同，因此以下将分别针对这两种管理模式对后续的操作流程进行说明。

i）在主动管理模式中，管理代理模块241定时从虚拟机监视器22读取计算机设备或者端口的访问控制状态信息，由管理工作站1的信息采集模块12通过网络采集这些访问控制状态信息，然后将这些访问控制状态信息发送给配置模块13。

配置模块13根据访问控制状态信息，通过策略、已存储的访问控制参数或者手工设置等方式设置被管理设备的端口访问参数，并将设置的端口访问参数发送给管理代理模块241。

虚拟机监视器22根据从管理代理模块241接收的端口访问控制参数为用户操作系统23分配计算机设备或者端口。这些计算机设备或者端口可以与启动用户操作系统23时相同，也可以不同。借此，管理工作站1实现了对用户

操作系统对设备或者端口的访问的控制。

进一步，该信息采集模块 12 可以将访问状态信息发送给日志生成模块 14，同时，该配置模块 13 也可以将端口访问参数发送给日志生成模块 14，日志生成模块 14 根据来自信息采集模块 12 的端口访问状态信息以及来自配置模块 13 的端口访问参数生成相应的日志。

ii）在被动管理模式中，管理代理模块 241 定时从虚拟机监视器 22 读取计算机设备或者端口的访问控制状态信息、以及用户操作系统 23 对计算机设备或者端口的访问指令，并根据用户操作系统 23 的访问指令产生相应的授权访问请求，然后通过网络将访问控制状态信息和授权访问请求发送给管理工作站 1，信息采集模块 12 采集这些访问控制状态信息和授权访问请求，然后将这些授权访问请求发送给配置模块 13。

配置模块 13 根据授权访问请求，通过策略或者已存储的访问控制参数判断是否允许用户操作系统 23 访问这些计算机设备或者端口（所有或者部分），并将相应的回复（访问权限）发送给管理代理模块 241。

虚拟机监视器 22 根据从管理代理模块 241 接收的回复为用户操作系统 23 分配设备或者端口。借此，管理工作站 1 实现了对用户操作系统对设备或者端口的访问的控制。

进一步，该信息采集模块 12 可以将访问状态信息发送给日志生成模块 14，同时，该配置模块 13 也可以将对授权访问请求的回复发送给日志生成模块 14，日志生成模块 14 根据来自信息采集模块 12 的端口访问状态信息以及来自配置模块 13 的对授权访问请求的回复生成相应的日志。

从上述描述可以看出，通过在计算机系统 2 中设置管理代理模块 241，网络中的管理工作站可以获得计算机系统 2 中计算机设备或者端口的访问控制状态，以及用户操作系统 23 对计算机设备或者端口的访问指令，进而可以策略的或者按照已存储的访问控制参数、或者对来自管理代理模块 241 的授权访问请求的回复来实现用户操作系统 23 对计算机设备或者端口的集中控制。

由此，本发明具有以下优点：

1）对计算机设备或者端口的访问控制是通过虚拟机监视器 22 进行参数设置实现的，非常方便管理；

2）虚拟机监视器 22 一直运行在计算机系统的底层，可以对设备和端口的状态进行实时监控；

3）可以远程开关端口，可以采用网络集中管理的方式对端口访问进行监控；

4）除管理员，一般用户无法访问虚拟机监视器 22，也就无法逃避管理工作站对计算机系统的集中管理。

因此，本发明的计算机管理系统和管理方法可以很好地满足企业用户、教育用户以及高安全用户对计算机进行集中管理的需要。

在以上的实施例中，管理代理模块 241 是设置在伺服操作系统 24 中，同样，其也可以设置在虚拟机监视器 22 中，或者作为单独的模块而独立于伺服操作系统和虚拟机监视器 22。

进一步，上述实施例中仅仅以用户操作系统 23 对计算机设备或者端口的访问为例说明本发明的计算机管理系统及其管理方法，可以理解的是，该计算机管理系统和管理方法同样可以应用到其他类似的对计算机系统进行集中管理的机制中。

因此，本发明并不局限于上述实施例，那些本领域普通技术人员通过阅读本申请后对本发明所做的简单的修饰、修改或者等同方案，都应该落在本发明的权利要求的系统和方法所要求保护的范围之内。

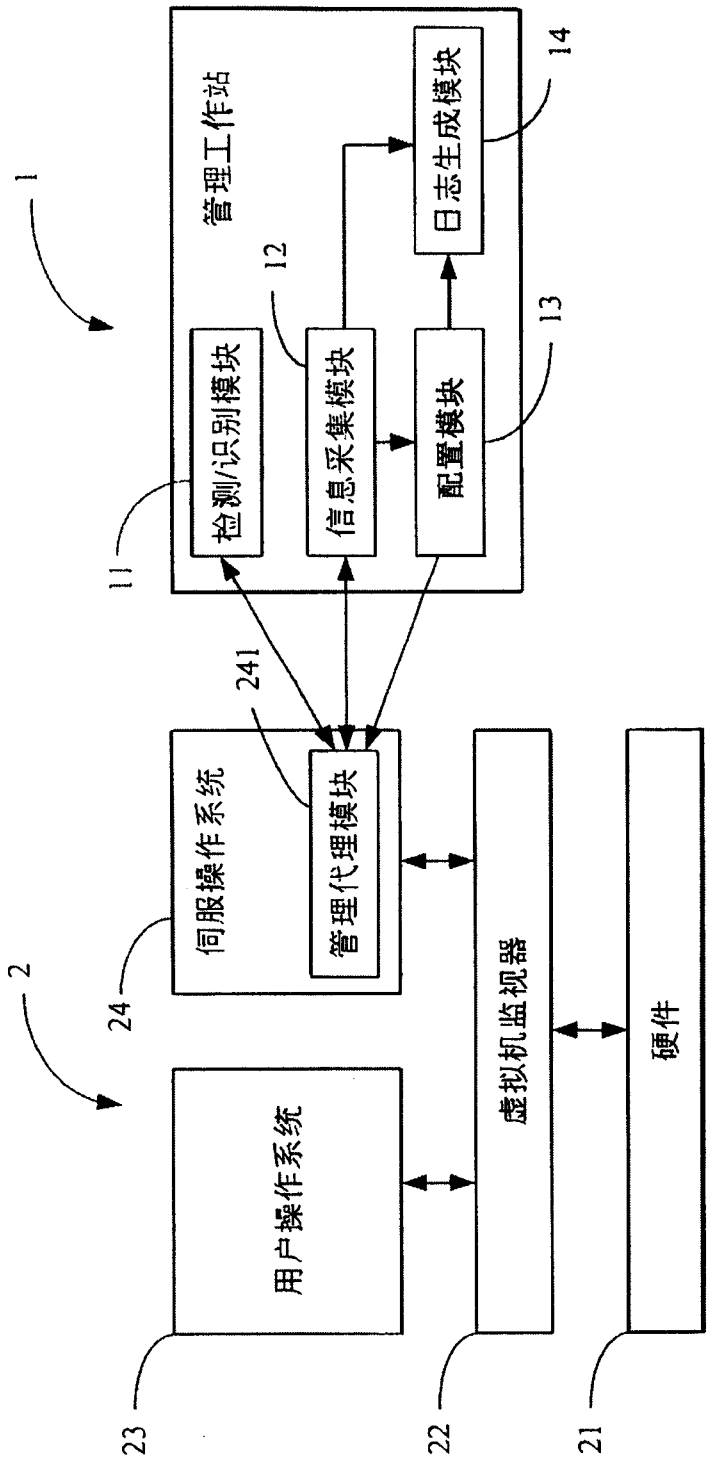

1
管理工作站
检测/识别模块
信息采集模块
配置模块
日志生成模块
11
12
13
14
241
2
伺服操作系统
管理代理模块
24
用户操作系统
虚拟机监视器
硬件
23
22
21

图 1

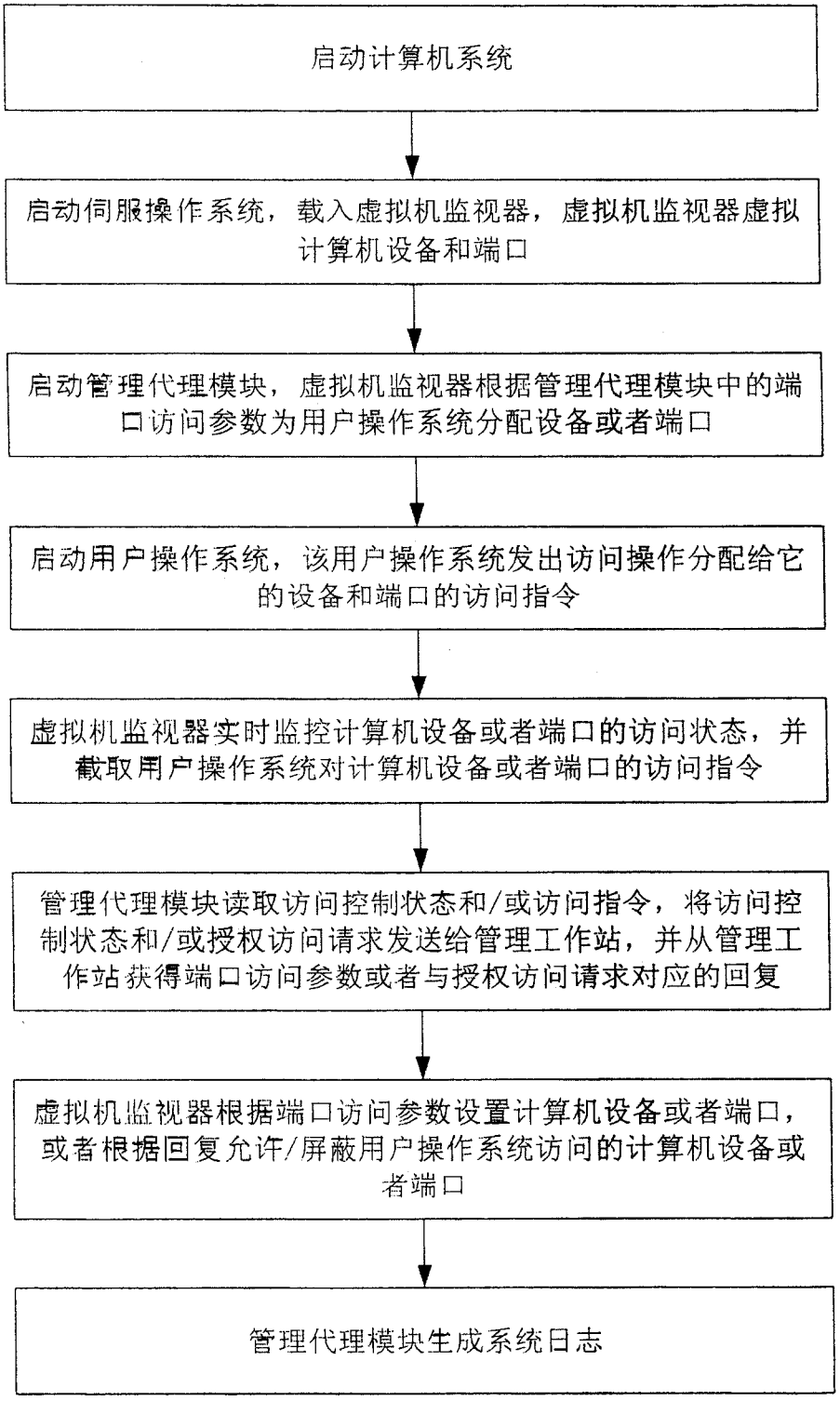

启动计算机系统
启动伺服操作系统，载入虚拟机监视器，虚拟机监视器虚拟计算机设备和端口
启动管理代理模块，虚拟机监视器根据管理代理模块中的端口访问参数为用户操作系统分配设备或者端口
启动用户操作系统，该用户操作系统发出访问操作分配给它的设备和端口的访问指令
虚拟机监视器实时监控计算机设备或者端口的访问状态，并截取用户操作系统对计算机设备或者端口的访问指令
管理代理模块读取访问控制状态和/或访问指令，将访问控制状态和/或授权访问请求发送给管理工作站，并从管理工作站获得端口访问参数或者与授权访问请求对应的回复
虚拟机监视器根据端口访问参数设置计算机设备或者端口，或者根据回复允许/屏蔽用户操作系统访问的计算机设备或者端口
管理代理模块生成系统日志

图 2

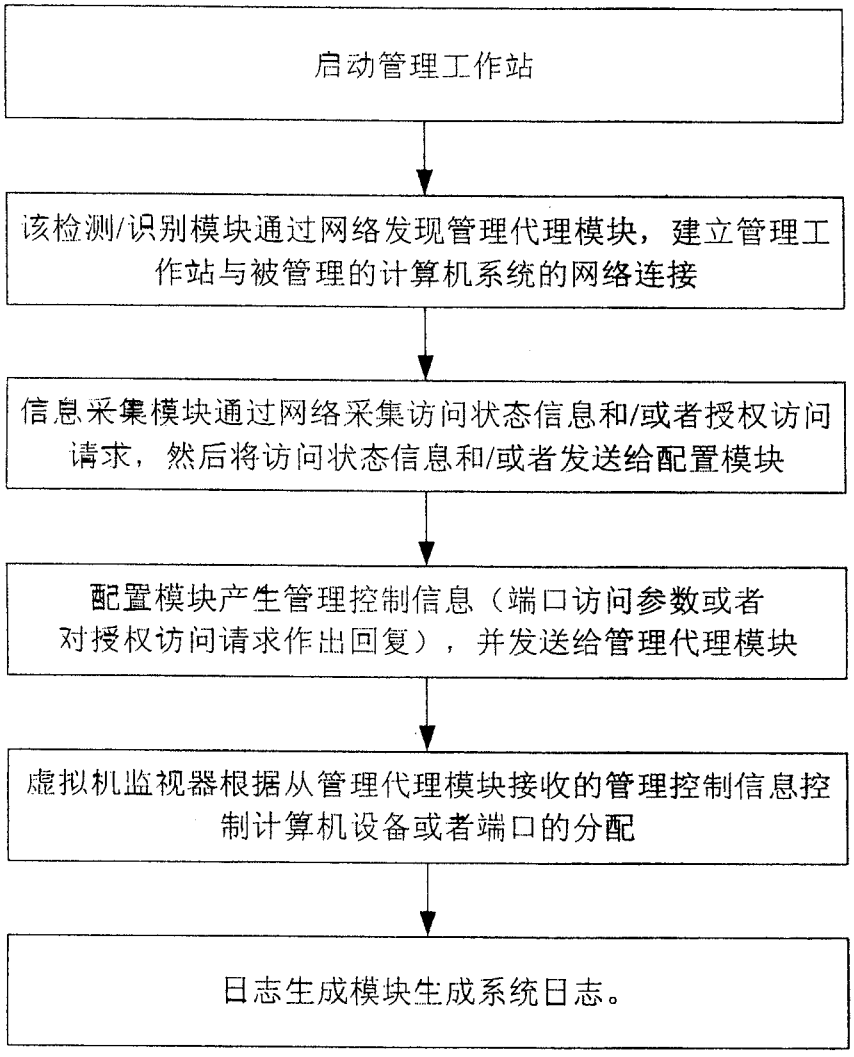

启动管理工作站
该检测/识别模块通过网络发现管理代理模块，建立管理工作站与被管理的计算机系统的网络连接
信息采集模块通过网络采集访问状态信息和/或者授权访问请求，然后将访问状态信息和/或者发送给配置模块
配置模块产生管理控制信息（端口访问参数或者对授权访问请求作出回复），并发送给管理代理模块
虚拟机监视器根据从管理代理模块接收的管理控制信息控制计算机设备或者端口的分配
日志生成模块生成系统日志。

图 3

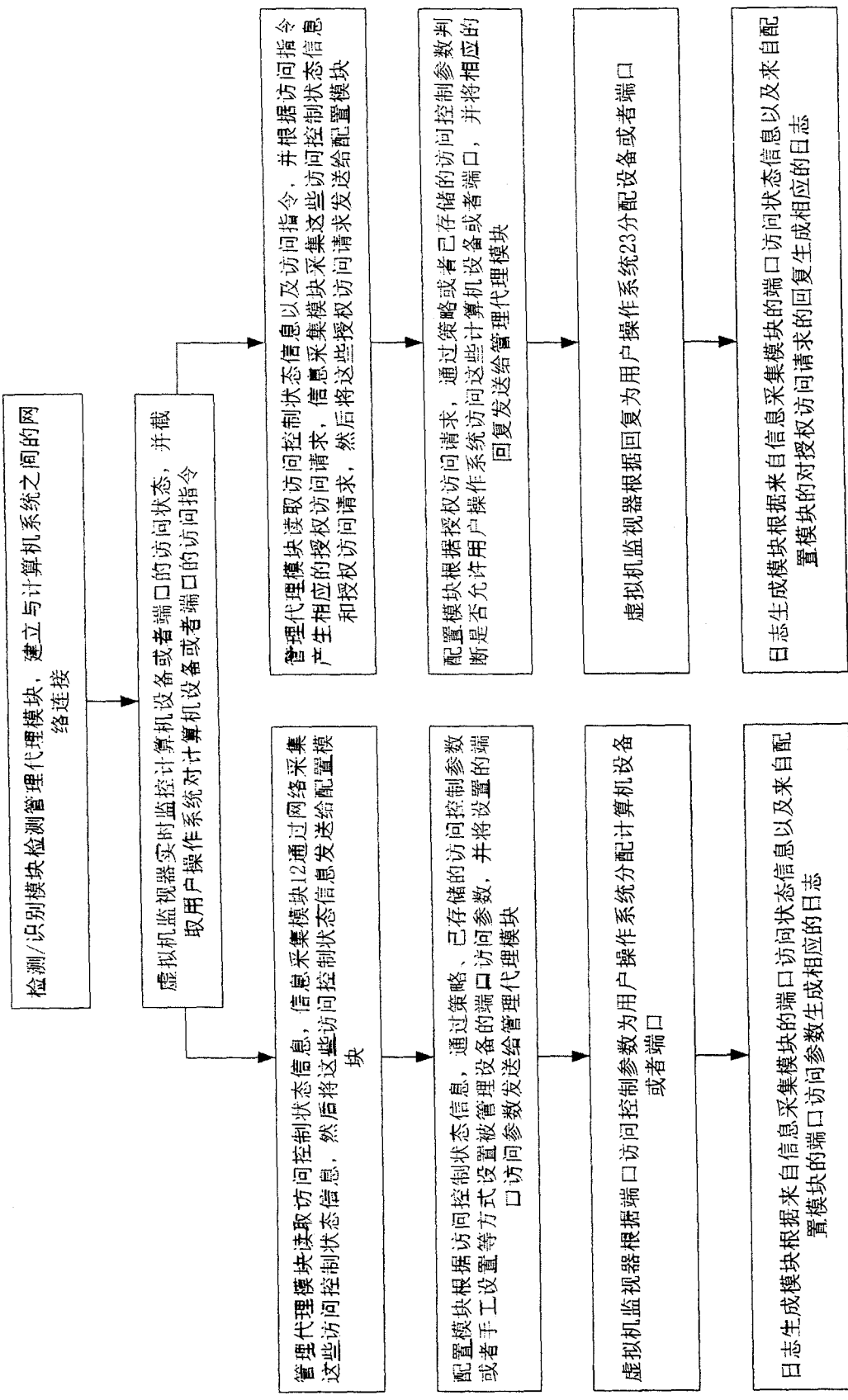

检测/识别模块检测管理代理模块，建立与计算机系统之间的网络连接
虚拟机监视器实时监控计算机设备或者端口的访问状态，并截取用户操作系统对计算机设备或者端口的访问指令
管理代理模块读取访问控制状态信息，信息采集模块12通过网络采集这些访问控制状态信息，然后将这些访问控制状态信息发送给配置模块
配置模块根据访问控制状态信息，通过策略、已存储的访问控制参数或者手工设置等方式设置被管理设备的端口访问参数，并将设置的端口访问参数发送给管理代理模块
虚拟机监视器根据端口访问控制参数为用户操作系统分配计算机设备或者端口
日志生成模块根据来自信息采集模块的端口访问状态信息以及来自配置模块的端口访问参数生成相应的日志
管理代理模块读取访问控制状态信息以及访问指令，并根据访问指令产生相应的授权访问请求，信息采集模块采集这些访问控制状态信息和授权访问请求，然后将这些授权访问请求发送给配置模块
配置模块根据授权访问请求，通过策略或者已存储的访问控制参数判断是否允许用户操作系统访问这些计算机设备或者端口，并将相应的回复发送给管理代理模块
虚拟机监视器根据回复为用户操作系统分配设备或者端口
日志生成模块根据来自信息采集模块的端口访问状态信息以及来自配置模块的对授权访问请求的回复生成相应的日志

图 4