(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113597609 B
(45)授权公告日 2025.04.04

(21)申请号 202080019505.6
(22)申请日 2020.03.06
(65)同一申请的已公布的文献号
申请公布号 CN 113597609 A
(43)申请公布日 2021.11.02
(30)优先权数据
16/296,301 2019.03.08 US
(85)PCT国际申请进入国家阶段日
2021.09.06
(86)PCT国际申请的申请数据
PCT/EP2020/056033 2020.03.06
(87)PCT国际申请的公布数据
WO2020/182664 EN 2020.09.17
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 C·英布伦达 C·博恩特雷格
L·海勒 F·布萨巴
J·布拉德伯里
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 刘薇 于静
(51)Int.Cl.
G06F 21/62(2013.01)
G06F 12/10(2016.01)
G06F 9/455(2006.01)
(56)对比文件
US 2009222816 A1,2009.09.03
审查员 汤婧

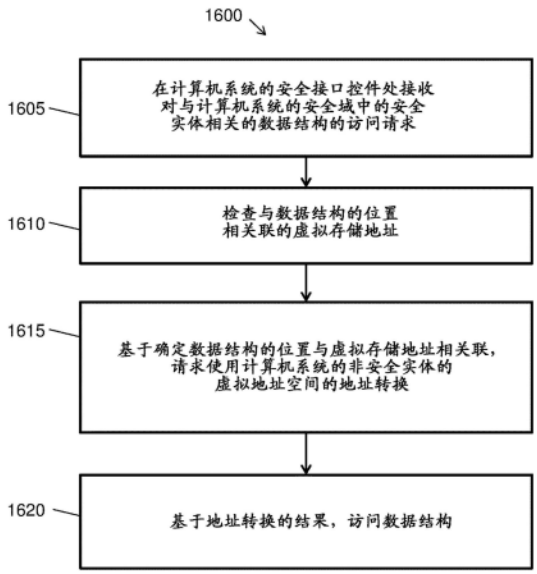
权利要求书2页 说明书21页 附图20页

(54)发明名称

用于安全接口控件存储的主机虚拟地址空间

(57)摘要

根据本发明的一个或多个实施例,一种计算机实现的方法包括:在计算机系统的安全接口控件处接收对与计算机系统的安全域中的安全实体相关的数据结构的访问请求。安全接口控件可检查与数据结构的位置相关联的虚拟存储地址。安全接口控件可基于确定数据结构的位置与虚拟存储地址相关联,请求使用计算机系统的非安全实体的虚拟地址空间的地址转换。安全接口控件可基于地址转换的结果来访问数据结构。



CN 113597609 B

1.一种用于安全接口控件存储的方法,包括:

在计算机系统的安全接口控件处接收对与所述计算机系统的安全域中的安全实体相关的数据结构的访问请求,其中,所述安全接口控件包括固件、硬件、可信软件或者固件、硬件和可信软件的组合;

由所述安全接口控件检查与所述数据结构的位置相关联的虚拟存储地址,其中检查所述虚拟存储地址还包括:检查区域安全表以确定与主机虚拟地址相关联的虚拟地址比较被启用还是被禁用,其中区域安全表包括用于主机绝对存储的每个页面的一个条目,每个条目由主机绝对地址索引,并且每个条目包括用于验证该条目属于安全实体的信息;

由安全接口控件基于确定虚拟地址比较指示被启用来验证由非安全实体提供的所述虚拟存储地址的映射;

由所述安全接口控件基于确定所述数据结构的所述位置与所述虚拟存储地址相关联,请求使用所述计算机系统的所述非安全实体的虚拟地址空间的地址转换;以及

由所述安全接口控件基于所述地址转换的结果来访问所述数据结构。

2.根据权利要求1所述的方法,还包括:

由所述安全接口控件基于确定所述数据结构的所述位置不与所述虚拟存储地址相关联,使用绝对地址来访问所述数据结构。

3.根据权利要求1所述的方法,其中,验证所述虚拟存储地址的所述映射包括:检查所述映射相较于先前映射的改变。

4.根据权利要求1-3中任一项所述的方法,其中,与所述安全域中的所述安全实体相关的所述数据结构被分布在多个存储器页面之间。

5.根据权利要求4所述的方法,其中,由所述非安全实体捐献的所述存储器页面驻留在连续的虚拟地址范围。

6.根据权利要求1-3中任一项所述的方法,其中,所述非安全实体包括被配置为将一个或多个安全客户机作为所述安全实体托管的管理程序。

7.一种计算机系统,包括:

存储器;

处理单元;以及

安全接口控件,被配置为执行多个操作,所述多个操作包括:

接收对与安全域中的安全实体相关的数据结构的访问请求,其中,所述安全接口控件包括固件、硬件、可信软件或者固件、硬件和可信软件的组合;

检查与所述数据结构在所述存储器中的位置相关联的虚拟存储地址,其中检查所述虚拟存储地址还包括:检查区域安全表以确定与主机虚拟地址相关联的虚拟地址比较被启用还是被禁用,其中区域安全表包括用于主机绝对存储的每个页面的一个条目,每个条目由主机绝对地址索引,并且每个条目包括用于验证该条目属于安全实体的信息;

基于确定虚拟地址比较指示被启用来验证由非安全实体提供的所述虚拟存储地址的映射;

基于确定所述数据结构的所述位置与所述虚拟存储地址相关联,请求使用所述处理单元的所述非安全实体的虚拟地址空间的地址转换;以及

基于所述地址转换的结果来访问所述数据结构。

8.根据权利要求7所述的计算机系统,其中,所述安全接口控件被配置为执行包括以下各项的操作:

基于确定所述数据结构的所述位置不与所述虚拟存储地址相关联,使用绝对地址来访问所述数据结构。

9.根据权利要求7所述的系统,其中,验证所述虚拟存储地址的映射包括:检查所述映射相较于先前映射的改变。

10.根据权利要求7至9中任一项所述的系统,其中,与所述安全域中的所述安全实体相关的所述数据结构被分布在所述存储器的多个页面之间。

11.根据权利要求10所述的系统,其中,由所述非安全实体捐献的所述存储器的所述页面驻留在连续的虚拟地址范围。

12.根据权利要求7至9中任一项所述的系统,其中,所述非安全实体包括被配置为将一个或多个安全客户机作为所述安全实体托管的管理程序。

13.一种包括计算机可读存储介质的计算机程序产品,所述计算机可读存储介质包括计算机可执行指令,所述计算机可执行指令在由处理单元的安全接口控件执行时使所述处理单元执行一种方法,所述方法包括:

在所述安全接口控件处接收对与安全域中的安全实体相关的数据结构的访问请求,其中,所述安全接口控件包括固件、硬件、可信软件或者固件、硬件和可信软件的组合;

由所述安全接口控件检查与所述数据结构的位置相关联的虚拟存储地址,其中检查所述虚拟存储地址还包括:检查区域安全表以确定与主机虚拟地址相关联的虚拟地址比较被启用还是被禁用,其中区域安全表包括用于主机绝对存储的每个页面的一个条目,每个条目由主机绝对地址索引,并且每个条目包括用于验证该条目属于安全实体的信息;

由所述安全接口控件基于确定虚拟地址比较指示被启用来验证由非安全实体提供的所述虚拟存储地址的映射;

由所述安全接口控件基于确定所述数据结构的所述位置与所述虚拟存储地址相关联,请求使用所述非安全实体的虚拟地址空间的地址转换;以及

由所述安全接口控件基于所述地址转换的结果来访问所述数据结构。

14.根据权利要求13所述的计算机程序产品,其中,所述可执行指令进一步使所述处理单元执行:

由所述安全接口控件基于确定所述数据结构的所述位置不与所述虚拟存储地址相关联,使用绝对地址来访问所述数据结构。

15.根据权利要求13所述的计算机程序产品,其中,验证所述虚拟地址的所述映射包括:检查所述映射相较于先前映射的改变。

16.根据权利要求13至15中任一项所述的计算机程序产品,其中,与所述安全域中的所述安全实体相关的所述数据结构被分布在多个存储器页面之间。

17.根据权利要求16所述的计算机程序产品,其中,由所述非安全实体捐献的所述存储器页面驻留在连续的虚拟地址范围。

用于安全接口控件存储的主机虚拟地址空间

背景技术

[0001] 本发明一般涉及计算机技术,更具体地,涉及使用主机虚拟地址空间来用于安全接口控件存储。

[0002] 云计算和云存储向用户提供了在第三方数据中心存储和处理他们的数据的能力。云计算促进了快速且容易地向客户提供VM的能力,无需客户购买硬件或为物理服务器提供地面空间。客户可以根据客户的偏好或要求的变化来容易地扩展或收缩VM。通常,云计算提供商提供物理上驻留在提供商的数据中心处的服务器上的VM。客户通常关心VM中数据的安全性,特别是因为计算提供商通常在同一服务器上存储不止一个客户的数据。客户可能期望他们自己的代码/数据与云计算提供商的代码/数据之间的安全性,以及他们自己的代码/数据与在提供商的站点运行的其他VM的代码/数据之间的安全性。此外,客户可能期望来自提供商的管理者的安全性以及防止来自在机器上运行的其它代码的潜在安全性破坏。

[0003] 为了处理这种敏感情形,云服务提供商可以实现安全控制以确保适当的数据隔离和逻辑存储分离。在实现云基础设施中广泛使用虚拟化导致了针对云服务的客户的独特安全问题,因为虚拟化改变了操作系统(OS)与底层硬件(无论是计算、存储还是甚至联网硬件)之间的关系。这引入了虚拟化作为附加层,其本身必须被正确地配置、管理和保护。

[0004] 通常,在主机管理程序的控制下作为客户机运行的VM依赖于该管理程序对该客户机透明地提供虚拟化服务。这些服务包括存储器管理、指令仿真以及中断处理。

[0005] 在存储器管理的情况下,VM可以将它的数据从盘中移动(页入)以驻留在存储器中,并且VM还可以将它的数据移回(页出)到盘中。当页面驻留在存储器中时,VM(客户机)使用动态地址转换(DAT)来将存储器中的页面从客户机虚拟地址映射到客户机绝对地址。此外,主机管理程序具有它自己的用于存储器中的客户机页的DAT映射(从主机虚拟地址到主机绝对地址),并且它可以独立地且对客户机透明地将客户机页页入和页出存储器。通过主机DAT表,管理程序提供两个分离的客户机VM之间的存储器隔离或客户机存储器的共享。主机还能够访问客户机存储器以在必要时代表客户机模拟客户机操作。

发明内容

[0006] 根据本发明的一个或多个实施例,一种计算机实现的方法包括在计算机系统的安全接口控件处接收对与计算机系统的安全域中的安全实体相关的数据结构的访问请求。安全接口控件可检查与数据结构的位置相关联的虚拟存储地址。安全接口控件可基于确定数据结构的位置与虚拟存储地址相关联,请求使用计算机系统的非安全实体的虚拟地址空间的地址转换。安全接口控件可基于地址转换的结果来访问数据结构。优点可以包括对安全接口控件存储提供主机虚拟地址空间。

[0007] 根据本发明的附加或替代实施例,安全接口控件可以基于确定数据结构的位置不与虚拟存储地址相关联,使用绝对地址来访问数据结构。优点可以包括针对绝对寻址的寻址灵活性。

[0008] 根据本发明的附加或替代实施例,可以验证由非安全实体提供的虚拟存储地址的

映射。优点可以包括检查由非安全实体管理的用于安全实体的数据的完整性。

[0009] 根据本发明的附加或替代实施例,验证虚拟存储地址的映射可以包括检查映射相较于先前映射的改变。优点可以包括确认非安全实体没有修改用于安全实体的地址映射。

[0010] 根据本发明的附加或替代实施例,与安全域中的安全实体相关的数据结构可以被分布在多个存储器页之间。优点可以包括支持数据结构分段。

[0011] 根据本发明的额外或替代实施例,由非安全实体捐献的存储器页可驻留在连续的虚拟地址范围。优点可以包括使被分段的绝对地址看起来连续。

[0012] 根据本发明的附加或替代实施例,检查虚拟存储地址还可以包括检查区域安全表以确定与主机虚拟地址相关联的虚拟地址比较被启用还是被禁用。优点可包括按域或页管理寻址模式选项。

[0013] 根据本发明的附加或替代实施例,安全接口控件可以是固件、硬件、可信软件、或者固件、硬件和可信软件的组合。优点可以包括实现对于整个系统性能的相关操作影响低的安全接口控件。

[0014] 根据本发明的附加或替换实施例,非安全实体可以是被配置为将一个或多个安全客户机作为安全实体来托管的管理程序。优点可以包括由非安全管理程序来托管安全客户机。

[0015] 本发明的其它实施例在计算机系统和计算机程序产品中实现上述方法的特征。

[0016] 附加特征及优点通过本公开的技术来实现。本发明的其它实施例和方面在此被详细描述,并且被认为是本发明的一部分。为了更好地理解本发明的优点和特征,参考说明书和附图。

附图说明

[0017] 在说明书的结尾处的权利要求中特别指出并清楚地要求了本文描述的专有权的细节。从下面结合附图的详细描述中,本发明的实施例的前述和其它特征和优点将变得显而易见,其中:

[0018] 图1描绘了根据本发明的一个或多个实施例的用于区域安全的表;

[0019] 图2描绘了根据本发明的一个或多个实施例的用于执行DAT的虚拟地址空间和绝对地址空间;

[0020] 图3描绘了根据本发明的一个或多个实施例的支持在管理程序下运行的虚拟机(VM)的嵌套多部分DAT;

[0021] 图4描绘了根据本发明的一个或多个实施例的安全客户机存储的映射;

[0022] 图5描绘了根据本发明的一个或多个实施例的动态地址转换(DAT)操作的系统示意图;

[0023] 图6描绘了根据本发明的一个或多个实施例的安全接口控件存储器的系统示意图;

[0024] 图7描绘了根据本发明的一个或多个实施例的导入操作的处理流程;

[0025] 图8描绘了根据本发明的一个或多个实施例的导入操作的处理流程;

[0026] 图9描绘了根据本发明的一个或多个实施例的所捐献存储器操作的过程;

[0027] 图10描绘了根据本发明的一个或多个实施例的将非安全管理程序页转变成安全

接口控件的安全页的处理流程；

[0028] 图11描绘了根据本发明的一个或多个实施例的由安全接口控件进行的安全存储访问的处理流程；

[0029] 图12描绘了根据本发明的一个或多个实施例的由安全接口控件和硬件进行的访问标记的处理流程；

[0030] 图13描绘了根据本发明的一个或多个实施例的由程序和安全接口控件进行的转换以支持安全和非安全访问的处理流程；

[0031] 图14描绘了根据本发明的一个或多个实施例的由程序和安全接口控件进行的具有安全存储保护的DAT的处理流程；

[0032] 图15描绘了根据本发明的一个或多个实施例的用于寻址模式确定的处理流程；

[0033] 图16描绘了根据本发明的一个或多个实施例的使用主机虚拟地址空间来用于安全接口控件存储的处理流程；

[0034] 图17示出了根据本发明的一个或多个实施例的云计算环境；

[0035] 图18描绘了根据本发明的一个或多个实施例的抽象模型层；

[0036] 图19描绘了根据本发明的一个或多个实施例的系统；以及

[0037] 图20描绘了根据本发明的一个或多个实施例的处理系统。

[0038] 在此描绘的图是说明性的。在不脱离本发明的精神的情况下，可以对其中所描述的图或操作进行许多变化。例如，可以以不同的顺序执行动作，或者可以添加、删除或修改动作。此外，术语“耦合”及其变型描述了在两个元件之间具有通信路径，并且并不暗示元件之间的直接连接而在它们之间没有中间元件/连接。所有这些变化都被认为是说明书的一部分。

具体实施方式

[0039] 本发明的一个或多个实施例利用软件与机器之间的高效、轻量的安全接口控件来提供附加的安全性。

[0040] 在主机管理程序的控制下作为客户机运行的虚拟机(VM)依赖于该管理程序对该客户机透明地提供虚拟化服务。这些服务可以应用于安全实体与另一个非受信实体之间的任何接口，该接口传统上允许该另一个实体访问安全资源。如前所述，这些服务可以包括但不限于存储器管理、指令仿真、和中断处理。例如，对于中断和异常注入，管理程序通常读取和/或写入客户机的前缀区域(低核)。如本文所使用的术语“虚拟机”或“VM”是指物理机器(计算设备、处理器等)及其处理环境(操作系统(OS)、软件资源等)的逻辑表示。VM被维护为在底层主机机器(物理处理器或处理器组)上执行的软件。从用户或软件资源的角度来看，VM看起来是它自己的独立物理机器。如本文所使用的术语“管理程序”和“VM监控器(VMM)”是指管理和允许多个VM使用在同一主机上的多个(有时是不同的)OS来执行的处理环境或平台服务。应当理解，部署VM包括VM的安装过程和VM的激活(或启动)过程。在另一个示例中，部署VM包括VM的激活(或启动)过程(例如，在VM先前被安装或已经存在的情况下)。

[0041] 为了促进和支持安全客户机，存在如下的技术挑战：在管理程序与安全客户机之间需要附加的安全性而不依赖管理程序，以使得管理程序不能从VM访问数据，并且因此不能以上述方式提供服务。

[0042] 本文描述的安全执行提供了一种硬件机制,以保证安全存储与非安全存储之间以及属于不同安全用户的安全存储之间的隔离。对于安全客户机,在“非受信”非安全管理程序与安全客户机之间提供附加的安全性。为了这样做,管理程序通常代表客户机所做的许多功能需要被结合到机器中。本文描述了一种新的安全接口控件(本文也被称为“UV”)以在管理程序与安全客户机之间提供安全接口。术语“安全接口控件”和“UV”在本文可互换使用。安全接口控件与硬件合作工作以提供该附加的安全性。另外,低级管理程序可以为该非受信管理程序提供虚拟化,并且如果低级管理程序以可信代码/软件实现,则它还可以是安全接口控件的一部分。

[0043] 在一个示例中,安全接口控件以内部安全且可信的硬件和/或固件实现。该可信固件可包括例如处理器毫代码或PR/SM逻辑分区代码。对于安全客户机或实体,安全接口控件提供安全环境的初始化和维护以及这些安全实体在硬件上的分派的协调。当安全客户机在主动使用数据并且它驻留在主机存储中时,它在安全存储中被保持为“没有危险”。安全客户机存储可被该单个安全客户机访问,这由硬件严格地执行。也就是说,硬件防止任何非安全实体(包括管理程序或其它非安全客户机)或不同的安全客户机访问该数据。在该示例中,安全接口控件作为最低级别的固件的可信部分运行。最低级别或毫代码实际上是硬件的扩展,并被用于实现例如在IBM的**zArchitecture®**中定义的复杂指令和功能。毫代码可以访问所有的存储部分,在安全执行的上下文中,存储包括它自己的安全UV存储、非安全管理程序存储、安全客户机存储和共享存储。这允许它提供安全客户机或支持该客户机的管理程序所需的任何功能。安全接口控件还具有对硬件的直接访问,这允许硬件在由安全接口控件建立的条件的控制下有效地提供安全检查。

[0044] 根据本发明的一个或多个实施例,在硬件中提供安全存储位以标记安全页。当该位被设置时,硬件防止任何非安全客户机或管理程序访问该页面。此外,每个安全页或共享页被注册在区域安全表中,并用安全客户机域标识(ID)来标记。当页面是非安全时,它在区域安全表中被如此标记。该区域安全表由每分区或区域的安全接口控件来维护。每个主机绝对页有一个条目,该条目由硬件用在由安全实体进行的任何DAT转换中以验证页面仅由拥有它的安全客户机或实体访问。

[0045] 根据本发明的一个或多个实施例,安全接口控件有它自己的安全UV存储,该安全UV存储仅可由安全接口控件自身访问。该存储由安全接口控件和硬件使用以对安全客户机提供所需的安全性。安全接口控件使用该安全存储来存储关于它自己、被启用以运行安全客户机的区域、安全客户机、和安全虚拟CPU的信息。与安全客户机存储类似,安全接口控件存储也被标记为安全页,以防止任何非安全实体的访问。此外,安全接口控件存储有它自己的安全域ID,该安全域ID用于防止任何其他安全实体访问安全接口控件存储。

[0046] 本发明的一个或多个实施例使用主机虚拟地址空间以用于安全接口控件存储。用于存储关于安全接口控件、客户机和虚拟CPU的信息的存储器区域通常位于绝对存储器中,这意味着安全接口控件可直接访问存储器区域而无需地址转换。为了允许安全交换,可以在从主机捐献给安全接口控件的存储器区域中创建、维护和使用诸如完整性表的数据结构。完整性表可以保存当页面被换出到磁盘时每个页面的内容和相关信息的校验和,因此,一旦页面被换回,则可检查页面的内容。完整性表的大小可以取决于安全客户机的存储的大小,并且可以跨越大的存储器区域。安全接口控件的完整性表和其它数据结构可在运行

时被分配,并且可能需要表现为每数据结构的连续存储器。一旦系统已经运行了一段时间,则由于存储器分段,找到大的连续存储区域可变得具有挑战性。本发明的一个或多个实施例通过甚至在系统已经运行了一段时间时也允许对安全接口控件分配大的连续存储区域,提供了针对存储器分段问题的变通方法。并非仅将安全接口控件限制为作为绝对地址的地址存储器,安全接口控件可以使用非受信管理程序的地址空间中的虚拟存储来存储一个或多个数据结构,诸如完整性表。这可以使得安全接口控件能够使用动态地址转换(DAT)来访问主机虚拟地址空间中用于安全接口控件存储的结构。

[0047] 根据本发明的一个或多个实施例,软件使用UV调用(UVC)指令来请求安全接口控件执行特定动作。例如,UVC指令可以由管理程序使用以初始化安全接口控件、创建安全客户机域(例如,安全客户机配置)、以及在该安全配置内创建虚拟CPU。它也可以用于导入(解密和分配给安全客户机域)和导出(加密和允许主机访问)安全客户机页,作为管理程序页入或页出操作的一部分。此外,安全客户机具有定义与管理程序共享的存储、使安全存储被共享、以及使共享存储安全的能力。

[0048] 这些UVC命令可以与许多其它架构指令类似地由机器固件执行。机器不进入安全接口控件模式,而是机器在它当前正在其中运行的模式中执行安全接口控件功能。硬件维持固件状态和软件状态两者,因此,不存在上下文切换以便处理这些操作。该低开销以如下方式允许在软件、可信固件和硬件的不同层之间的紧密联系的协作:最小化并降低安全接口控件的复杂性,同时仍然提供必要的安全级别。

[0049] 根据本发明的一个或多个实施例,为了支持安全接口控件和硬件所需的控制块结构以正确地维护安全客户机和支持管理程序环境,管理程序在初始化安全客户机环境时向安全接口控件捐献存储。结果,为了准备1)初始化区域以运行安全客户机,2)创建安全客户机域,以及3)创建在每个域中运行的安全CPU,管理程序发出查询UVC指令以确定其中捐献所需的存储量。一旦存储已被捐献,则它被标记为安全,并被注册为属于安全接口控件;并且禁止任何非安全或安全客户机实体的访问。这保持该情况,直到相关联的实体(例如,安全客户机CPU、安全客户机域或区域)被破坏的时候为止。

[0050] 在一个示例中,用于支持区域特定的UV控制块的UV存储的第一区段被捐献给安全接口控件,作为初始化UVC的一部分,并驻留在本文中被称为UV2存储的地方。用于支持基本和可变安全客户机配置控制块(针对每个安全客户机域)的UV存储的第二区段和第三区段被捐献作为创建安全客户机配置UVC的一部分,并分别驻留在UVS存储和UVV存储中。用于支持安全CPU控制块的UV存储的第四部分和最后部分也驻留在UVS空间中,并被捐献作为创建安全客户CPU UVC的一部分。当这些区域中的每一个被捐献时,安全控制接口将它们标记为安全(以防止它们被任何非安全实体访问),并且还在区域安全表中将它们注册为属于安全接口控件(以防止它们被任何安全客户机实体访问)。为了在UV空间内提供进一步的隔离,UV2空间(其不与任何特定安全客户机域相关联)也用唯一的UV2安全域来标记,同时UVS和UVV空间都进一步用相关联的特定安全客户机域来标记。在该示例中,UVV空间驻留在主机虚拟空间中,并且因此可以进一步用主机虚拟到主机绝对映射来识别。

[0051] 尽管安全接口控件可以访问所有的存储(非安全存储、安全客户机存储和UV存储),但是,本发明的一个或多个实施例非常具体地提供了允许安全接口控件访问UV存储的机制。使用在安全客户机域之间提供隔离的相同硬件机制,本发明的实施例可以在UV存储

内提供类似的隔离。这保证安全接口控件仅在被预期和指定时访问UV存储;仅访问用于所指定的期望的安全客户机的安全客户机存储;以及仅在被指定时访问非安全存储。也就是说,安全接口控件可以非常明确地指定它意图访问的存储,以使得硬件可以保证它确实访问该存储。此外,它还可以指定它仅意图访问与所指定的安全客户机域相关联的UV存储。

[0052] 为了提供安全性,当管理程序透明地将安全客户机数据页入和页出时,与硬件一起工作的安全接口控件提供并保证数据的解密和加密。为了实现这一点,需要管理程序在页入和页出客户机安全数据时发出新的UVC。基于由安全接口控件在这些新UVC期间建立的控制,硬件将保证这些UVC确实由管理程序发出。

[0053] 在这个新的安全环境中,每当管理程序页出安全页时,需要发出从安全存储(导出)UVC的新转换。响应于该导出UVC,安全接口控件将:1)指示页面被UV“锁定”,2)加密页面,3)将页面设置为非安全,以及4)重置UV锁定。一旦完成了导出UVC,管理程序就可以立刻将被加密的客户机页面页出。

[0054] 此外,每当管理程序在页入安全页时,它必须发出到安全存储(导入)UVC的新转换。响应于该导入UVC,UV或安全接口控件将:1)在硬件中将页面标记为安全,2)指示页面被UV“锁定”,3)解密页面,4)将权限设置成特定的安全客户机域,以及5)重置UV锁定。每当由安全实体进行访问时,硬件在转换期间对该页面执行授权检查。这些检查包括:1)验证页面确实属于正试图访问它的安全客户机域的检查,以及2)确保管理程序在该页面已经驻留在客户机存储器中时还没有改变该页面的主机映射的检查。一旦页面被标记为安全,则硬件防止管理程序或非安全客户机VM访问任何安全页。附加的转换步骤防止另一个安全VM的访问,并且防止管理程序的重新映射。

[0055] 现在转向图1,一般性地示出了根据本发明的一个或多个实施例的用于区域安全的表100。图1所示的区域安全表100由安全接口控件维护,并由安全接口控件和硬件使用以保证对由安全实体访问的任何页面的安全访问。区域安全表100通过主机绝对地址110来索引。也就是说,对于主机绝对存储的每个页面存在一个条目。每个条目包括用于验证该条目属于进行访问的安全实体的信息。

[0056] 进一步地,如图1所示,区域安全表100包括安全域ID 120(其标识与该页面相关联的安全域);UV位130(其指示该页面被捐献给安全接口控件并由安全接口控件拥有);禁用地址比较(DA)位140(用于在诸如当被定义为主机绝对的安全接口控件页不具有相关联的主机虚拟地址时的情况下禁用主机地址对比较);共享(SH)位150(其指示与非安全管理程序共享该页面)和主机虚拟地址160(其指示被注册用于该主机绝对地址的主机虚拟地址,其被称为主机地址对)。注意,主机地址对指示主机绝对地址和相关联的已注册主机虚拟地址。主机地址对表示该页的映射,一旦由管理程序导入,并且该比较保证主机在该页面正由客户机使用时没有重新映射该页。

[0057] 动态地址转换(DAT)用于将虚拟存储映射到实际存储。当客户机VM在管理程序的控制下作为可分页客户机运行时,客户机使用DAT来管理驻留在它的存储器中的页面。另外,主机在页面驻留在它的存储器中时独立地使用DAT来管理那些客户机页(连同它自己的页面)。管理程序使用DAT来提供不同VM之间的存储隔离和/或共享,以及防止客户机访问管理程序存储。当客户机在非安全模式下运行时,管理程序可以访问所有的客户机的存储。

[0058] DAT使一个应用能够与另一个应用隔离,同时仍然允许它们共享公共资源。而且,

它允许实现VM可用于OS的新版本以及应用程序的并发处理的设计和测试的VM。虚拟地址标识虚拟存储中的位置。地址空间是连续的虚拟地址序列连同特定变换参数(包括DAT表),这些特定变换参数允许每个虚拟地址被转换成相关联的绝对地址,该绝对地址用存储中的字节位置来标识该地址。

[0059] DAT使用多表查找来将虚拟地址转换成关联的绝对地址。该表结构通常由存储管理器定义和维护。该存储管理器通过页出一个页面以例如带来另一页,在多个程序之间透明地共享绝对存储。例如,当页面被页出时,存储管理器将在相关联的页表中设置无效位。当程序试图访问已被页出的页面时,硬件将向存储管理器提交程序中断,通常被称为页错误。作为响应,存储管理器将页入所请求的页,并重置无效位。这都是对程序透明地完成的,并且允许存储管理器对存储虚拟化并在各种不同用户之间共享它。

[0060] 当CPU使用虚拟地址来访问主存储时,首先通过DAT将虚拟地址转换成实际地址,然后通过加前缀来转换成绝对地址。用于特定地址空间的最高级别表的名称(来源和长度)被称为地址空间控制元素(ASCE),并定义相关联的地址空间。

[0061] 现在转向图2,一般性地示出了根据本发明的一个或多个实施例的用于执行DAT的示例性虚拟地址空间202、204和绝对地址空间206。在图2所示的示例中,存在两个虚拟地址空间:虚拟地址空间202(由地址空间控制元素(ASCE)A 208定义)和虚拟地址空间204(由ASCE B 210定义)。虚拟页A1.V 212a1、A2.V 212a2和A3.V 212a3由存储管理器在多表(分段230和页表232a、232b)查找中使用ASCE A 208映射到绝对页A1.A 220a1、A2.A 220a2和A3.A 220a3。类似地,虚拟页B1.V 214b1和B2.V 214b2使用ASCE B 210在双表234和236查找中被分别映射到绝对页B1.A 222b1和B2.A 222b2。

[0062] 现在转向图3,一般性地示出了根据本发明的一个或多个实施例的用于支持在管理程序下运行的VM的嵌套多部分DAT转换的示例。在图3所示的例子中,客户机A虚拟地址空间A 302(由客户机ASCE(GASCE)A 304定义)和客户机B虚拟地址空间B 306(由GASCEB 308定义)都驻留在共享主机(管理程序)虚拟地址空间325中。如图所示,属于客户机A的虚拟页A1.GV 310a1、A2.GV 310a2和A3.GV 310a3由客户机A存储管理器使用GASCEA 304分别映射到客户机绝对页A1.HV 340a1、A2.HV 340a2和A3.HV 340a3;属于客户机B的虚拟页B1.GV 320b1和B2.GV 320b2由客户机B存储管理器使用GASCEB 308独立地分别映射到客户机绝对页B1.HV 360b1和B2.HV 360b2。在该示例中,这些客户机绝对页直接映射到共享主机虚拟地址空间325中,随后经历到主机绝对地址空间330的附加的主机DAT转换。如图所示,主机虚拟地址A1.HV 340a1、A3.HV 340a3和B1.HV 360b1由主机存储管理器使用主机ASCE(HASCE)350映射到A1.HA 370a1、A3.HA 370a3和B1.HA 370b1。属于客户机A的主机虚拟地址A2.HV 340a2和属于客户机B的B2.HV 360b2都被映射到同一主机绝对页AB2.HA 380。这使得数据能够在这两个客户机之间共享。在客户机DAT转换期间,每个客户机表地址被当作客户机绝对,并经历附加的嵌套主机DAT转换。

[0063] 这里描述的本发明的实施例提供了安全的客户机和UV存储保护。禁止非安全客户机和管理程序对安全存储的访问。管理程序规定,对于给定的驻留安全客户机页,以下情况发生。相关联的主机绝对地址仅可通过单个管理程序(主机)DAT映射来访问。也就是说,存在映射到被分配给安全客户机的任何给定主机绝对地址的单个主机虚拟地址。与给定安全客户机页相关联的管理程序DAT映射(主机虚拟到主机绝对)在它被页入时不改变。针对单

个安全客户机,映射与安全客户机页相关联的主机绝对页。

[0064] 根据本发明的一个或多个实施例,还禁止安全客户机之间的存储共享。在单个安全客户机与在该安全客户机控制下的管理程序之间共享存储。UV存储是安全存储,并可由安全接口控件而不是客户机/主机访问。存储由管理程序分配给安全接口控件。根据本发明的一个或多个实施例,硬件和安全接口控件禁止对这些规则的任何尝试违反。

[0065] 现在转向图4,一般性地示出了根据本发明的一个或多个实施例的安全客户机存储的映射的示例。图4类似于图3,除了图4的示例不允许在安全客户机A与安全客户机B之间共享存储之外。在图3的非安全示例中,属于客户机A的主机虚拟地址A2.HV 340a2和属于客户机B的主机虚拟地址B2.HV 360b2两者被映射到同一主机绝对页AB2.HA 380。在图4的安全客户机存储示例中,属于客户机A的主机虚拟地址A2.HV 340a2映射到主机绝对地址A2.HA 490a,而属于客户机B的B2.HV 360b2映射到它自己的B2.HA 490b。在该示例中,在安全客户机之间不存在共享。

[0066] 当安全客户机页驻留在盘上时,它被加密。当管理程序页入安全客户机页时,它发出UV调用(UVC),该UVC使得安全接口控件将页面标记为安全(除非共享),对页面解密(除非共享),并将页面(在区域安全表中)注册为属于适当的安全客户机(例如客户机A)。此外,它将相关联的主机虚拟地址(例如,A3.HV 340a3)注册到该主机绝对页(被称为主机地址对)。如果管理程序未发出正确的UVC,则它在试图访问安全客户机页时接收到异常。当管理程序页出客户机页时,发出类似的UVC,该UVC在将客户机页标记为非安全并将其在区域安全表中注册为非安全之前加密客户机页(除非共享)。

[0067] 在具有五个给定主机绝对页K、P、L、M和N的示例中,当管理程序将它们页入时,每个主机绝对页被安全接口控件标记为安全。这防止非安全客户机和管理程序访问它们。主机绝对页K、P和M在管理程序将它们页入时被注册为属于客户机A;主机绝对页L和N在被管理程序页入时被注册到客户机B。共享页面,即在单个安全客户机与管理程序之间共享的页面,在分页期间不被加密或解密。它们没有被标记为安全(允许管理程序访问),而是在区域安全表中被注册到单个安全客户机域。

[0068] 根据本发明的一个或多个实施例,当非安全客户机或管理程序试图访问由安全客户机拥有的页面时,管理程序接收到安全存储访问(PIC3D)异常。不需要附加的转换步骤来确定这一点。

[0069] 根据一个或多个实施例,当安全实体试图访问页面时,硬件执行验证存储确实属于该特定安全客户机的附加转换检查。如果不是,则向管理程序提交非安全访问(PIC3E)异常。另外,如果正被转换的主机虚拟地址与来自区域安全表中的注册主机地址对的主机虚拟地址不匹配,则识别出安全存储违反('3F' x)异常。为了能够与管理程序共享,只要转换检查允许访问,则安全客户机可以访问未被标记为安全的存储。

[0070] 现在转到图5,一般性地示出了根据本发明的一个或多个实施例的DAT操作的系统示意图500。系统示意图500包括主机主虚拟地址空间510和主机归属虚拟地址空间520,页面从这些空间被转换(例如,参见主机DAT转换525;注意,虚线表示通过DAT转换525的映射)到管理程序(主机)绝对地址空间530。例如,图5示出了由两个不同的主机虚拟地址空间共享主机绝对存储以及不仅在两个客户之间而且还与主机本身共享那些主机虚拟地址之一。在这一点,主机主虚拟地址空间510和主机归属虚拟地址空间520是两种主机虚拟地址空间

的示例,每个主机虚拟地址空间分别由单独的ASCE(主机主ASCE(HPASCE)591)和主机归属ASCE(HHASCE)592寻址。注意,所有安全接口控件存储(虚拟和实际两者)都由管理程序捐献并被标记为安全。一旦被捐献,安全接口控件存储仅可由安全接口控件访问,只要存在相关联的安全实体。

[0071] 如图所示,主机主虚拟地址空间510包括客户机A绝对页A1.HV、客户机A绝对页A2.HV、客户机B绝对页B1.HV\以及主机虚拟页H3.HV。主机归属虚拟地址空间520包括安全接口控件虚拟页U1.HV、主机虚拟页H1.HV、以及主机虚拟页H2.HV。

[0072] 根据本发明的一个或多个实施例,所有安全客户机(例如,安全客户机A和安全客户机B)存储在本文所描述的区域安全表中被注册为属于安全客户机配置,并且相关联的主机虚拟地址(例如,A1.HV、A2.HV、B1.HV)也被注册为主机地址对的一部分。在一个或多个实施例中,所有安全客户机存储被映射在主机主虚拟空间中。此外,所有安全接口控件存储也在区域安全表中被注册为属于安全接口控件,并且可以基于相关联的安全客户机域而在区域安全表中被进一步区分。根据本发明的一个或多个实施例,UV虚拟存储被映射在主机归属虚拟空间中,并且相关联的主机虚拟地址被注册为主机地址对的一部分。根据一个或多个实施例,UV实际存储不具有相关联的主机虚拟映射,并且区域安全表中的DA位(其指示虚拟地址比较被禁用)被设置成指示这一点。主机存储被标记为非安全,并且还在区域安全表中被注册为非安全。

[0073] 因此,在“客户绝对=主机虚拟”的情况下,管理程序(主机)主DAT表(由HPASCE 591定义)如下地转换主机主虚拟地址空间510的页面:客户机A绝对页A1.HV被映射到属于安全客户机A的主机绝对A1.HA;客户机A绝对页A2.HV被映射到属于安全客户机A的主机绝对A2.HA;客户机B绝对页B1.HV被映射到属于安全客户机B的主机绝对B1.HA;以及主机虚拟页H3.HV被映射到主机绝对页H3.HA非安全主机(并且由于它是不安全的,因此,没有主机地址对)。进一步地,管理程序(主机)归属DAT表(由HHASCE 592定义)如下地转换主机归属虚拟地址空间520的页面:安全接口控件虚拟页U1.HV被映射到被定义为安全UV虚拟的主机绝对页U1.HA;主机虚拟页H1.HV被映射到被定义为非安全的主机绝对页H1.HA;以及主机虚拟页H2.HV被映射到被定义为非安全的主机绝对页H2.HA。由于H1.HA或H2.HA是不安全的,因此,不存在与H1.HA或H2.HA相关联的主机-地址对。

[0074] 在操作时,如果安全客户机试图访问被分配给安全接口控件的安全页,则由硬件向管理程序提交安全存储违反('3F'X)异常。如果非安全客户机或管理程序试图访问任何安全页面(包括被分配给安全接口控件的那些页面),则由硬件向管理程序提交安全存储访问('3D'X)异常。可替代地,可以针对对安全接口控件空间进行的尝试访问,提交错误条件。如果硬件检测到安全分配中关于安全接口控件访问的不匹配(例如,存储在区域安全表中被注册为属于安全客户机而不是属于安全接口控件,或者在所使用的主机地址对中存在与注册对的不匹配),则提交检查。

[0075] 换句话说,主机主虚拟地址空间510包括主机虚拟页A1.HV、A2.HV(属于安全客户机A)和B1.HV(属于安全客户机B),其分别映射到主机绝对A1.HA、A2.HA和B1.HA。另外,主机主虚拟地址空间510包括主机(管理程序)页H3.HV,其映射到主机绝对H3.HA。主机归属虚拟空间520包括两个主机虚拟页H1.HV和H2.HV,其映射到主机绝对页H1.HA和H2.HA中。主机主虚拟地址空间510和主机归属虚拟地址空间520两者都映射到单个主机绝对530中。属于安

全客户机A和安全客户机B的存储页被标记为安全,并在图1所示的区域安全表100中被注册到它们的安全域和相关联的主机虚拟地址。另一方面,主机存储被标记为非安全。当管理程序在定义安全客户机时,它必须将主机存储捐献给安全接口控件以用于支持这些安全客户机所需的安全控制块。该存储可以在主机绝对空间或主机虚拟空间中(在一个示例中,具体地,在主机归属虚拟空间中)被定义。返回到图5,主机绝对页U1.HA和U2.HA安全UV绝对是被定义为主机绝对存储的安全接口控件存储。结果,这些页面被标记为安全,并在图1所示的区域安全表100中被注册为属于安全接口控件并被注册到相关联的安全域。由于页面被定义为主机绝对地址,因此,不存在相关联的主机虚拟地址,因此,DA位被设置在区域安全表100中。

[0076] 在转换之后,可以在图6中找到管理程序(主机)绝对地址空间530的示例。图6描绘了根据本发明的一个或多个实施例的关于安全接口控件存储器的系统示意图600。系统示意图600示出了管理程序(主机)绝对地址空间630包括主机绝对页A2.HA安全客户机A(针对A2.HV);主机绝对页B1.HA安全客户机B(针对B1.HV);主机绝对页H1.HA非安全(主机);主机绝对页H2.HA非安全(主机);主机绝对页U3.HA安全UV实际(无HV映射);主机绝对页U1.HA安全UV虚拟(针对U1.HV);以及主机绝对页A1.HA安全客户机A(针对A1.HV)。

[0077] 现在转向图7,一般性地示出了根据本发明的一个或多个实施例的用于导入操作的处理流程700。当安全客户机访问已由管理程序页出的页面时,出现诸如在处理流程700中所示的事件序列,以便安全地将该页面带回。处理流程700在框705处,其中安全客户机访问客户机虚拟页。由于该页面例如是无效的,因此,硬件向管理程序提交由程序中断代码11(PIC11)指示的主机页错误(参见框715)。管理程序进而针对该客户机页标识可用的非安全主机绝对页(参见框720),并将加密的客户机页页入到所标识的主机绝对页(参见框725)。

[0078] 然后在框730处,主机绝对页被映射到适当的(基于主机虚拟地址的)主机DAT表中。然后,在框735处,管理程序主机重新分派安全客户机。在框740处,安全客户机重新访问客户机安全页。页错误不再存在,但由于这是安全客户机访问,并且页面在图100的区域安全表100中未被标记为安全,因此,在框745处,硬件向管理程序提交非安全存储异常(PIC3E)。该PIC3E防止客户机访问该安全页,直到必要的导入已被发出。接下来,处理流程700进行到“A”,其被连接到图8。

[0079] 现在转向图8,一般性地示出根据本发明的一个或多个实施例的用于执行导入操作的处理流程800。响应于PIC3E,行为良好的管理程序(例如,以预期的方式无错误地执行)将发出导入UVC(参见框805)。注意,此时,要被导入的页面被标记为非安全,并且只能由管理程序、其它非安全实体、和安全接口控件访问。它不能被安全客户机访问。

[0080] 作为导入UVC的一部分,充当安全接口控件的可信固件检查以查看页面是否已被安全接口控件锁定(参见判决框810)。如果是,则处理流程800进行到框820。在框820处,“忙碌”返回代码被返回到管理程序,作为响应,管理程序将延迟(参见框825)并重新发出导入UVC(处理流程800返回到框805)。如果页面尚未被锁定,则处理流程800进行到判决框822。

[0081] 在判决框822处,安全接口控件检查以查看页面是否是与非安全管理程序共享的页面。如果它是共享的(处理流程800进行到判决框824),则安全接口控件将主机绝对地址在区域安全表中注册到相关联的安全客户机域、主机虚拟地址并注册为共享。该页面保持被标记为非安全。这完成了导入UVC,并且页面现在可用于被客户机访问。处理继续,管理程

序重新分派客户机(框830),并且安全客户机成功访问页面(框835)。

[0082] 如果要被导入的主机虚拟页不与管理程序共享(处理流程800进行到框840),则安全接口控件将页面标记为安全,以使得管理程序不再能访问该页面。在框845处,安全接口控件锁定该页面,以使得没有其它UVC可以修改页面状态。一旦锁定被设置(在框850处),则安全接口控件将验证客户机页的内容在被加密时没有改变。如果它们确实改变了,则错误返回代码被返回给管理程序,否则,安全接口控件将解密该安全页面。

[0083] 在框855处,安全接口控件解锁该页面,允许其它UVC访问,并将页面在区域安全表中注册为安全并与适当的客户机域和主机虚拟地址相关联,以完成主机地址HV→HA对。这允许客户机的访问并完成UVC。

[0084] 现在转向图9,一般性地示出了根据本发明的一个或多个实施例的关于所捐献存储器操作的处理流程900。处理流程900在框905处开始,其中管理程序向安全接口控件发出查询UVC。在框910处,安全接口控件返回数据(例如,查询UVC)。该数据可以包括:所需的基本区域特定主机绝对存储量;所需的基本安全客户机域特定主机绝对存储量;每MB所需的可变安全客户机域特定主机虚拟存储量;和/或所需的基本安全客户机CPU特定主机绝对存储量。

[0085] 在框915处,管理程序保留基本主机绝对区域特定存储(例如,基于由查询UVC返回的大小)。在框920处,管理程序向安全接口控件发出初始化。在这一点,管理程序可发出初始化UVC,其为在针对整个区域的安全客户机配置之间进行协调所需的UV控制块提供所捐献的存储。该初始化UVC指定基本区域特定存储原点。

[0086] 在框925处,安全接口控件通过将所捐献的存储注册到UV并标记为安全来实现初始化(例如,初始化UVC)。对于初始化UVC,安全接口控件可将所捐献的存储标记为安全;向区域安全表分配该所捐献的存储中的一些;以及将所捐献的存储在区域安全表中注册到唯一的安全域以用于UV使用,但是没有注册到相关联的安全客户机域,并注册为没有相关联的主机虚拟地址对。

[0087] 在框930处,管理程序保留存储(例如,基本和可变安全客户机域特定存储)。例如,管理程序保留基本和可变(例如,基于安全客户机域存储的大小)安全客户机域特定存储(例如,由查询UVC返回的大小)。在框935处,管理程序向安全接口控件发出创建配置。在这一点,管理程序可以发出指定基本和可变安全客户机域特定存储原点的创建安全客户机配置UVC。进一步地,创建安全客户机配置UVC提供用于支持该安全客户机配置所需的UV控制块的所捐献的存储。

[0088] 在框940处,安全接口控件实现创建配置(例如,创建安全客户机配置UVC)。对于创建安全客户机配置UVC,安全接口控件可将所捐献的存储标记为安全;将所捐献的存储注册在区域安全表中以用于UV使用;以及将所捐献的存储注册到相关联的安全客户机域。所捐献的基本(主机绝对)存储被注册为没有相关联的主机虚拟地址对。所捐献的可变(主机虚拟)存储被注册到相关联的主机虚拟地址对。

[0089] 在框945处,管理程序保留基本安全客户机CPU特定存储(例如,由查询UV返回的大小)。在框950处,管理程序指定存储原点。例如,管理程序向UV发出指定基本安全客户机CPU特定存储原点的创建安全客户机CPU。在框955处,安全接口控件实现创建CPU(例如,创建安全客户机CPU UVC)。对于创建安全客户机CPU UVC,安全接口控件可以将所捐献的存储标记

为安全,并将所捐献的存储注册在区域安全表中以用于UV使用,但是没有注册到相关联的安全客户机域,并且注册为不具有相关联的主机虚拟地址对。

[0090] 现在转到图10,一般性地示出了根据本发明的一个或多个实施例的关于将非安全管理程序页转变到安全接口控件的安全页的处理流程1000。在处理流程1000中,示出了三个管理程序页(例如,非安全管理程序页A、非安全管理程序页B和、非安全管理程序页C)。

[0091] 管理程序(非安全)页A、B和C可由非安全实体(包括管理程序)访问。进一步地,管理程序(非安全)页A、B和C被标记为非安全(NS),并且在区域安全表(例如,图1所示的区域安全表100)中被注册为非安全和非共享。在箭头1005处,发出初始化UVC,其将客户机页A转变成与整个区域(UV2)相关联的安全接口控件实际存储页1010。安全接口控件实际存储1010可被标记为安全,并且在区域安全表(例如,图1所示的区域安全表100)中被注册为不具有安全客户机域和管理程序到主机绝对(HV→HA)映射的UV。相反,它被注册到唯一的UV2安全域,并且DA位被设置为1。注意,安全接口控件实际存储1010可以由安全接口控件作为实际来访问。

[0092] 在箭头1025处,从管理程序(非安全)页B发出创建SG配置或创建SG CPU UVC,其将该页面转移到与安全客户机域(UVS)相关联的安全接口控件实际存储1030。安全接口控件实际存储1030可被标记为安全的,并且在区域安全表(例如,图1所示的区域安全表100)中被注册为具有相关联的安全客户机域且没有管理程序到主机绝对(HV→HA)映射(即,DA位=1)的UV。注意,安全接口控件实际存储1010可作为代表安全客户机域的实际而被安全接口控件访问。

[0093] 在箭头1045处,从管理程序(非安全)页C发出创建SG配置UVC,其将该页面转移到与安全客户机域(UVV)相关联的安全接口控件虚拟存储1050。安全接口控件虚拟存储1050可被标记为安全,并且在区域安全表(例如,图1所示的区域安全表100)中被注册为具有安全客户机域和管理程序到主机绝对(HV→HA)映射的UV。注意,安全接口控件虚拟存储1050可作为代表安全客户机域的UV虚拟来被访问。

[0094] 现在转向图11,描绘了根据一个或多个实施例的关于由程序或安全接口控件进行的安全存储访问的处理流程1100。这表示安全接口控件将要访问客户机存储或安全接口控件存储并且必须正确对该访问进行标记以便允许硬件验证该访问的安全性的情况。1100描述了由安全接口控件对存储访问的这种标记。处理流程1100在框1110处开始,其中安全接口控件确定它是否正在进行对安全接口控件存储的访问。

[0095] 如果这不是对安全接口控件存储的访问,则处理流程1100进行到判决框1112(如由“否”箭头所示)。在判决框1112,安全接口控件确定它是否正在进行对安全客户机存储的访问。如果这不是对安全客户机存储的访问,则处理流程1100进行到“B”(其被连接到图12的处理流程1200),其将使用用于非安全访问的默认设置。如果这是对安全客户机存储的访问,则处理流程1100进行到判决框1113,其中安全接口控件确定是否正在使用默认安全客户机域。如果是,则处理流程1100进行到“B”(其被连接到图12的处理流程1200),其将使用用于安全客户机访问的默认设置。如果否,则处理流程1100进行到框1114。在框1114,适当的安全客户机域被加载到SG安全域寄存器中(并进行到“B”,其被连接到图12的处理流程1200)。

[0096] 如果这是对安全接口控件存储的访问,则处理流程1100进行到框1120(如由“是”

箭头所示)。在框1120处,访问被标记为安全UV(例如,使用UV安全域寄存器)。

[0097] 然后,处理流程1100进行到判决框1130,其中安全接口控件确定这是否是对UVV空间(例如SG-config变量表格)的访问。如果是对UVV空间的访问,则处理流程1100进行到框1134(如由“是”箭头所示)。在框1134处,访问被标记为虚拟。在框1136处,适用的安全客户机域被加载到UV安全域寄存器中。在框1138处,准备好开始DAT转换和访问存储。返回到判决框1130,如果这不是对UVV空间的访问,则处理流程1100进行到框1140(如由“否”箭头所示)。在框1140处,访问被标记为实际。

[0098] 在判决框1150,安全接口控件确定这是否是对UVS空间(例如SG配置或CPU表)的访问。如果这是对UVS空间的访问,则处理流程1100进行到框1136(如由“是”箭头所示)。如果这不是对UVS空间的访问,则处理流程1100进行到框1170(如由“否”箭头所示)。然后,该访问会是对UV2空间(例如,区域安全表)的访问。在框1170处,唯一的UV2安全域被加载到UV安全域寄存器中。

[0099] 图12描绘了根据本发明的一个或多个实施例的处理流程1200。当客户机被分派时,SIE条目(SIE Entry)固件可以向硬件指示客户机正在运行(例如,客户机模式活动),并且可以指示客户机是否是安全的。如果客户机是安全的,则相关联的安全客户机域可以被加载到硬件中(例如,在SG安全域寄存器中)。当程序正在访问存储时,硬件可以基于程序在访问时的当前状态来对该访问进行标记。图12示出了处理流程1200中的该过程的示例。在框1205处,硬件可以确定机器当前是否正在客户机模式下运行,如果不是,则硬件可在框1210处将该访问标记为主机访问,并在框1215处将该访问标记为非安全访问。如果在框1205处机器正在客户机模式下运行,则在框1220处该访问可被标记为客户机访问,并在框1225处进一步确定当前客户机是否是安全客户机。如果客户机是不安全的,则在框1215处,该访问被标记为非安全。如果客户机是安全的,则在框1230处,硬件可以将客户机标记为安全,这可以将安全客户机与在安全客户机被分派时被加载的SG安全域寄存器相关联。对于非安全客户机和安全客户机两者,可在框1235处检查DAT状态。如果DAT关闭,则在框1240出,访问被标记为实际。如果DAT开启,则在框1245处,访问可被标记为虚拟。一旦在框1240处访问随着DAT关闭被标记为实际,或者在框1245处访问随着DAT开启被标记为虚拟,则在框1250处,硬件准备好开始转换和访问存储,如在图13中进一步描述的。

[0100] 图13描绘了根据本发明的一个或多个实施例的处理流程1300中的由硬件进行的转换以支持安全访问和非安全访问两者的示例。在框1305,硬件可以确定访问是否被标记为客户机转换,如果是并且在框1310处访问是虚拟的,则在框1315处可执行客户机DAT。在客户机DAT转换期间,可以存在对客户机DAT表的嵌套中间获取。如果原始转换被标记为安全的,则表获取可以被标记为客户机实际且安全。表获取也可遵循处理流程1300的转换过程。在框1315处针对被标记为客户机虚拟的访问以及在框1310处针对被标记为客户机实际(虚拟=否)的任何访问执行了客户机DAT之后,在框1320处可应用客户机加前缀和客户机存储器偏移。在完成客户机转换过程时,在框1325处,如果原始客户机转换被标记为安全,则所得到的地址可被标记为主机虚拟且安全。过程1300可以针对被标记为主机虚拟的任何访问而继续。如果原始访问在框1305处是主机访问(客户机=否)并且在框1330处是虚拟的,则在框1335处可以执行主机DAT。在框1335处,主机表获取可被标记为非安全。在框1335处执行了主机DAT之后,或者如果在框1330处原始主机访问被标记为实际(虚拟=否),则在

框1340可应用主机加前缀。在框1345处,所得到的地址可以是主机绝对地址。

[0101] 图14描绘了根据本发明的一个或多个实施例的处理流程1400中的可由硬件执行的具有安全存储保护的DAT转换的示例。从图13的框1345继续,如果在框1405处识别安全UV访问,则在框1410处,硬件可以验证存储是否被注册为安全UV存储,如果否,则在框1415处提交错误。当访问UV存储时,安全UV访问可由安全接口控件进行。如果在框1410处存储被注册为安全UV存储,则保护检查可以继续,如可针对任何安全访问执行,除了UV安全域寄存器(由安全接口控件在进行安全UV访问之前设置)在框1420处可被用作用于域检查的指定安全域,在框1420处,处理继续。另外,在框1425处针对UV访问而被检测到的任何违反(入口点D)可在框1430处作为错误被提交,而不是在框1435处作为异常向管理程序提交,如在框1425处针对安全客户机违反(安全UV=否)所做的。

[0102] 对于在框1405处未被标记为安全UV访问的访问,在框1440处,硬件确定访问是否是安全客户机访问,如果不是并且如果在框1445处页面被标记为安全,则在框1435处,可向管理程序提交异常。否则,如果在框1440处访问不是安全客户机访问并且在框1445处页面未被标记为安全,则在框1450处,转换成功。

[0103] 如果在框1440处访问是安全客户机访问或者在框1410处访问是对被注册为安全UV存储的存储的安全UV访问,则在框1420处,硬件可以进行检查以确保存储被注册到与访问相关联的安全实体。如果是安全UV访问,则可以从(由安全接口控件基于正被访问的安全UV存储而加载的)UV安全域寄存器获得指定安全域,并且对于安全客户机访问,从(在分派安全实体时被加载的)SG安全域寄存器获得指定安全域。如果在框1420处,正被访问的存储未被注册到指定安全域,则对于在框1425处的安全UV访问,在框1430处出现错误,并且对于在框1425处的安全客户机访问(安全UV=否),在框1435处,向管理程序提交异常。

[0104] 对于在框1440和框1410处对存储(其在框1420处被注册到指定安全域)的安全访问,如果在框1455处禁用虚拟地址检查(即DA位=1)并且在框1460处访问是实际的,则在框1450处,完成转换。然而,如果在框1455处DA位=1但在框1460处访问是虚拟的(实际=否),则对于在框1425处的安全UV访问,在框1430处出现错误,并且对于在框1425处的安全客户机访问(安全UV=否),在框1435处向管理程序提交异常。如果在框1455处DA位=0并且在框1475处访问是虚拟访问,则在框1470处,硬件可以确定访问的主机虚拟到主机绝对映射是否与针对该主机绝对地址所注册的映射相匹配。如果是,则在框1450处,转换成功完成。如果在框1470处映射不匹配,则对于在框1425处的安全UV访问,在框1430处出现错误,并且对于在框1425处的安全客户机访问(安全UV=否),在框1435处,向管理程序提交异常。如果DA位=0并且在框1475处访问是实际访问(虚拟=否),则对于在框1425处的安全UV访问,在框1430处出现错误,并且对于在框1425处的安全客户机访问(安全UV=否),在框1435处,向管理程序提交异常;或者,在框1450处,转换可成功完成。可以检查在框1480处的I/O子系统的任何访问以查看在框1445处页面是否被标记为安全,如果页面是安全的,则在框1435处,可以向管理程序提交异常;如果页面未被标记为安全,则在框1450处,转换成功。

[0105] 可以通过区域安全表接口1485来集中管理存储注册和映射的各种检查。例如,框1410、1420、1455、1470和1475可以与关联于同一区域的区域安全表进行接口,以管理各种访问。

[0106] 现在转到图15,一般性地示出了根据本发明的一个或多个实施例的用于寻址模式

确定的处理流程1500。如先前关于图10所描述的,安全接口控件可访问页面,例如UVS中的页面B,该页面已被建立为可通过安全接口控件实际存储1030访问的实际/绝对存储。进一步地,安全接口控件可以访问页面,诸如UVV中的页面C,该页面在图10的处理流程1000中已被建立为安全接口控件虚拟存储1050。图11的处理流程1100可以在框1130处确定是否应当执行对UVV空间的访问(诸如为了完整性表),或者在框1150处确定是否应当执行对UVS空间的访问。处理流程1500进一步示出了可以支持图11的处理流程1100的地址转换处理。在图15的框1505,当安全接口控件需要访问与安全客户机相关的一个或多个数据结构(诸如图1的完整性表或区域安全表100)时,处理流程1500进行到框1510。在框1510处,安全接口控件可确定访问是否与虚拟存储地址相关联。在框1515处,如果访问与虚拟存储地址相关联,则安全接口控件可以使用管理程序的虚拟地址空间来转换虚拟存储地址,诸如通过DAT表。在框1520处,安全接口控件和/或支持硬件/固件可执行一个或多个检查,以确保虚拟存储地址的预期映射(例如,先前针对该绝对页所注册的映射)通过管理程序DAT从访问返回。作为一个示例,安全接口控件可确认管理程序没有改变如先前所配置的数据结构的关联主机映射。在框1525处,一旦绝对地址已经通过管理程序的DAT表来确定,或者如果访问已经与绝对地址相关联(例如,框1510=否),则安全接口控件可以访问在绝对地址处的数据结构。

[0107] 现在转向图16,一般性地示出了根据本发明的一个或多个实施例的用于使用主机虚拟地址空间来进行安全接口控件存储的处理流程1600。处理流程1600是图15的处理流程1500的变体。在框1605处,计算机系统的安全接口控件可以接收对与计算机系统的安全域中的安全实体相关的数据结构的访问请求。访问请求可以是通过安全接口控件来管理安全性的内部序列的一部分。安全实体可以是一个或多个安全客户机,诸如VM或安全容器。在框1610处,安全接口控件可检查与数据结构的位置相关联的虚拟存储地址。与安全域中的安全实体相关的数据结构可被分布在多个存储器页之间。存储器页可以由非安全实体在多个固定位置处捐献,以供安全接口控件的安全使用。由非安全实体捐献的存储器页可驻留在连续的虚拟地址范围处。非安全实体可以是被配置为将一个或多个安全客户机或容器作为安全实体托管的管理程序或操作系统。检查虚拟存储地址映射可以包括检查图1的区域安全表100以确定与主机虚拟地址相关联的虚拟地址比较被启用还是被禁用(例如,DA位140状态)。

[0108] 在框1615处,安全接口控件可基于确定数据结构的位置与虚拟存储地址相关联,使用计算机系统的非安全实体的虚拟地址空间来执行地址转换。可以使用先前所描述的任何过程和元件来执行地址转换。由非安全实体提供的虚拟存储地址的映射可由安全接口控件来验证。对虚拟存储地址的映射的验证可以包括检查映射相较于先前注册的映射的变化。通过地址转换表的映射可被配置为将被分布在非连续绝对位置的存储器页呈现为连续的虚拟地址。因此,不能适合连续的绝对存储器块的数据结构可在主机的虚拟地址空间中表现为连续。

[0109] 在框1620处,安全接口控件可基于从地址转换得到的绝对地址来访问数据结构。可替代地,安全接口控件可基于确定数据结构的位置不与虚拟存储地址相关联,使用绝对地址来直接访问数据结构。

[0110] 应当理解,尽管本公开包括关于云计算的详细描述,但是本文所记载的教导的实现不限于云计算环境。相反,本发明的实施例能够结合现在已知或以后开发的任何其它类

型的计算环境来实现。

[0111] 云计算是一种服务交付模式,用于实现对共享的可配置计算资源(例如,网络、网络带宽、服务器、处理、存储器、存储、应用、VM和服务)池池的方便、按需的网络访问,可配置计算资源可以以最小的管理成本或与服务提供商进行最少的交互来快速供应和释放。这种云模式可以包括至少五个特性、至少三个服务模型和至少四个部署模型。

[0112] 特征如下:

[0113] 按需自助式服务:云的消费者可以单方面自动地按需提供计算能力(诸如服务器时间和网络存储),而无需与服务提供者进行人工交互。

[0114] 广泛的网络接入:能力在网络上可用并通过促进异构的瘦或厚客户端平台(例如,移动电话、膝上型计算机和PDA)的使用的标准机制来接入。

[0115] 资源池:提供商的计算资源被归入资源池以使用多租户模型来服务多个消费者,其中不同的物理和虚拟资源根据需求被动态地分配和再分配。一般情况下,消费者不能控制或不知道所提供的资源的确切位置,但是可以在较高抽象程度上指定位置(例如国家、州或数据中心),因此具有位置无关性。

[0116] 迅速弹性:可以迅速且有弹性地(在一些情况下自动地)提供能力以快速向外扩展并被迅速释放以快速缩小。对于消费者,可用于提供的能力通常看起来是无限的,并可以在任何时间以任何数量购买。

[0117] 可测量的服务:云系统通过利用在适于服务类型(例如,存储、处理、带宽和活动用户账户)的某一抽象程度的计量能力,自动地控制和优化资源使用。可以监视、控制和报告资源使用情况,为所利用的服务的提供者和消费者双方提供透明度。

[0118] 服务模型如下:

[0119] 软件即服务(SaaS):向消费者提供的能力是使用提供者在云基础架构上运行的应用。可通过诸如网络浏览器的瘦客户机接口(例如,基于网络的电子邮件)来从各种客户机设备访问应用。除了有限的特定于用户的应用配置设置以外,消费者既不管理也不控制包括网络、服务器、操作系统、存储、或甚至单个应用能力等的底层云基础架构。

[0120] 平台即服务(PaaS):向消费者提供的能力是在云基础架构上部署消费者创建或获得的应用,这些应用是使用由提供商支持的编程语言和工具创建的。消费者既不管理也不控制包括网络、服务器、操作系统或存储的底层云基础架构,但对其部署的应用具有控制权,对应用托管环境配置可能也具有控制权。

[0121] 基础架构即服务(IaaS):向消费者提供的能力是提供消费者能够在其中部署并运行包括操作系统和应用的任意软件的处理、存储、网络和其它基础计算资源。消费者既不管理也不控制底层云基础架构,但对操作系统、存储、所部署的应用具有控制权,对所选择的网络组件(例如,主机防火墙)可能具有有限的控制权。

[0122] 部署模型如下:

[0123] 私有云:云基础架构单独为某个组织运行。它可以由该组织或第三方管理,并且可以存在于该组织内部或外部。

[0124] 共同体云:云基础架构被若干组织共享,并支持具有共同利害关系(例如,任务、安全要求、政策和合规考虑)的特定共同体。它可以由该组织或第三方管理,并且可以存在于该组织内部或外部。

[0125] 公共云:云基础架构可用于一般公众或大型产业群,并由销售云服务的组织拥有。

[0126] 混合云:云基础架构由两个或更多云(私有云、共同体云或公共云)组成,这些云依然是独特实体,但是通过使数据和应用能够移植的标准化技术或私有技术(例如,用于云之间的负载平衡的云突发)绑定在一起。

[0127] 云计算环境是面向服务的,特点集中在无状态性、低耦合性、模块性和语义的互操作性。计算的核心是包括互连节点网络的基础架构。

[0128] 现在参考图17,描述了说明性的云计算环境50。如图所示,云计算环境50包括云消费者使用的本地计算设备可以与其通信的一个或多个云计算节点10,本地计算设备例如是个人数字助理(PDA)或蜂窝电话54A、台式计算机54B、膝上型计算机54C和/或汽车计算机系统54N。节点10可以彼此通信。它们可以被物理地或虚拟地分组(未示出)在一个或多个网络(诸如如上文所描述的私有云、共同体云、公共云或混合云或其组合)中。这允许云计算环境50提供基础架构即服务、平台即服务和/或软件即服务,而云消费者不需要为其在本地计算设备上维护资源。应当理解,图17中所示的各类计算设备54A-N仅仅是示意性的,计算节点10和云计算环境50可以在任何类型的网络和/或网络可寻址连接上(例如,使用网络浏览器)与任何类型的计算设备通信。

[0129] 现在参考图18,示出了由云计算环境50(图17)提供的一组功能抽象层。首先应当理解,图18所示的组件、层和功能仅仅是示意性的,本发明的实施例不限于此。如图所示,提供了以下层和相应的功能:

[0130] 硬件和软件层60包括硬件和软件组件。硬件组件的示例包括:大型机61;基于RISC(精简指令集计算机)架构的服务器62;服务器63;刀片服务器64;存储设备65;以及网络和网络组件66。在一些实施例中,软件组件包括网络应用服务器软件67和数据库软件68。

[0131] 虚拟化层70提供抽象层,从该抽象层可以提供虚拟实体的以下示例:虚拟服务器71;虚拟存储器72;虚拟网络73,包括虚拟专用网络;虚拟应用程序和操作系统74;以及虚拟客户端75。

[0132] 在一个示例中,管理层80可以提供以下描述的功能。资源供应功能81提供用于在云计算环境中执行任务的计算资源和其它资源的动态获取。计量和定价功能82提供对在云计算环境内使用资源的成本跟踪,并为这些资源的消耗提供账单或发票。在一个示例中,这些资源可以包括应用软件许可。安全功能为云消费者和任务提供身份认证,并为数据和其他资源提供保护。用户门户功能83为消费者和系统管理员提供对云计算环境的访问。服务水平管理功能84提供云计算资源的分配和管理,以满足所需的服务水平。服务水平协议(SLA)计划和履行功能85提供对根据SLA针对其预测未来需求的云计算资源的预安排和采购。

[0133] 工作负载层90提供可以利用云计算环境的功能的示例。在该层中,可提供的工作负载和功能的示例包括:地图绘制与导航91;软件开发及生命周期管理92;虚拟教室的教学提供93;数据分析处理94;交易处理95;以及控制对与虚拟机相关联的安全存储的访问96。可以理解,这些仅是一些示例,在其他实施例中,这些层可包括不同的服务。

[0134] 现在转向图19,描绘了根据本发明的一个或多个实施例的系统1900。系统1900包括示例节点10(例如,托管节点),其例如经由网络165与一个或多个客户端设备20A-20E直接或间接地进行通信。节点10可以是云计算提供商的数据中心或主机服务器。节点10执行

便于部署一个或多个VM 15(15A-15N)的管理程序12。节点10还包括硬件/固件层13,其包括安全接口控件11。安全接口控件11包括一个或多个硬件模块和固件,其便于管理程序12向虚拟机15提供一个或多个服务。可以在以下之间存在通信:管理程序12与安全接口控件11;安全接口控件11与一个或多个VM 15;管理程序12与一个或多个VM 15;以及通过安全接口控件11从管理程序12到VM 15。为了促进安全的VM环境,根据本发明的一个或多个实施例的托管节点10不包括管理程序12与一个或多个VM 15之间的任何直接通信。

[0135] 例如,节点10可以促进客户端设备20A部署VM 15A-15N中的一个或多个。可以响应于来自不同客户端设备20A-20E的相应请求来部署VM 15A-15N。例如,VM 15A可由客户端设备20A部署,VM 15B可由客户端设备20B部署,VM 15C可由客户端设备20C部署。节点10还可以促进客户端提供物理服务器(而不是作为VM运行)。这里描述的示例将在节点10中提供资源体现为VM的一部分,然而,所描述的技术方案也可以被应用于作为物理服务器的一部分来提供资源。

[0136] 在一个示例中,客户端设备20A-20E可以属于相同的实体,诸如个人、企业、政府机构、公司内的部门、或任何其他实体,并且节点10可以作为该实体的私有云来操作。在这种情况下,节点10单独托管由属于该实体的客户端设备20A-20E部署的VM 15A-15N。在另一个示例中,客户端设备20A-20E可以属于不同的实体。例如,第一实体可以拥有客户端设备20A,而第二实体可以拥有客户端设备20B。在这种情况下,节点10可以作为托管来自不同实体的VM的公共云来操作。例如,VM 15A-15N可以以其中VM 15A不便于访问VM 15B的遮蔽方式来部署。例如,节点10可以使用**IBM z Systems®**处理器资源/系统管理器(PR/SM)逻辑分区(LPAR)特征来遮蔽VM 15A-15N。因此,这些特征(例如PR/SM LPAR提供分区之间的隔离)便于节点10在不同的逻辑分区中针对在同一物理节点10上的不同实体部署两个或更多个VM 15A-15N。PR/SM LPAR管理程序被实现在具有特定硬件以提供这种隔离的可信内部固件中。

[0137] 客户端设备20A-20E中的客户端设备20A是通信装置,例如计算机、智能电话、平板计算机、台式计算机、膝上型计算机、服务器计算机、或请求节点10的管理程序12部署VM的任何其它通信装置。客户端设备20A可经由网络165发送由节点10的管理程序12接收的请求。VM 15A-15N中的VM 15A是管理程序12响应于来自客户端设备20A-20E中的客户端设备20A的请求而部署的VM镜像。管理程序12是VM监视器(VMM),其可以是创建并运行VM的软件、固件或硬件。管理程序12促进VM 15A使用节点10的硬件组件来执行程序和/或存储数据。采用适当的特征和修改,管理程序12可以是**IBM z Systems®**、Oracle的VM服务器、Citrix的XenServer、Vmware的ESX、Microsoft Hyper-V管理程序或任何其它管理程序。管理程序12可以是直接在节点10上执行的本机管理程序,或者是在另一个管理程序上执行的托管管理程序。

[0138] 现在转到图20,示出了根据本发明的一个或多个实施例的用于实现本文的教导的节点10。节点10可以是电子计算机架构,其包括和/或采用任何数量的计算设备和计算设备的组合以及利用各种通信技术的网络,如本文所述。节点10可以容易地可伸缩、可扩展和模块化,能够改变成不同的服务或独立地重新配置一些特征。

[0139] 在该实施例中,节点10具有处理器2001,其可以包括一个或多个中央处理单元

(CPU)2001a、2001b、2001c等。处理器2001(也称为处理电路、微处理器、计算单元)经由系统总线2002耦合到系统存储器2003和各种其它组件。系统存储器2003包括只读存储器(ROM)2004和随机存取存储器(RAM)2005。ROM 2004被耦合到系统总线2002,并且可以包括基本输入/输出系统(BIOS),其控制节点10的某些基本功能,RAM是被耦合到系统总线2002以由处理器2001使用的读写存储器。

[0140] 图20的节点10包括硬盘2007,其是可由处理器2001读取执行的有形存储介质的示例。硬盘2007存储软件2008和数据2009。软件2008被存储为由处理器2001在节点10上执行的指令以执行过程,例如参考图1-19描述的过程。数据2009包括以各种数据结构组织的定性或定量变量的值集合,以支持软件2008的操作并由其使用。

[0141] 图20的节点10包括一个或多个适配器(例如,硬盘控制器、网络适配器、图形适配器等),其相互连接并支持处理器2001、系统存储器2003、硬盘2007、和节点10的其他组件(例如,外围设备和外部设备)之间的通信。在本发明的一个或多个实施例中,一个或多个适配器可以被连接到一个或多个I/O总线,该一个或多个I/O总线经由中间总线桥被连接到系统总线2002,并且该一个或多个I/O总线可以利用公共协议,例如外围部件互连(PCI)协议。

[0142] 如图所示,节点10包括将键盘2021、鼠标2022、扬声器2023和麦克风2024互连到系统总线2002的接口适配器2020。节点10包括将系统总线2002与显示器2031互连的显示适配器2030。显示适配器2030(和/或处理器2001)可以包括图形控制器以提供图形性能,例如GUI 2032的显示和管理。通信适配器2041将系统总线2002与网络2050互连,使得节点10能够与诸如服务器2051和数据库2052的其它系统、设备、数据和软件通信。在本发明的一个或多个实施例中,软件2008和数据2009的操作可由服务器2051和数据库2052在网络2050上实现。例如,网络2050、服务器2051和数据库2052可组合以提供软件2008和数据2009的内部迭代作为平台即服务、软件即服务和/或基础架构即服务(例如,作为分布式系统中的网络应用)。

[0143] 本文描述的实施例必然根植于计算机技术,尤其是托管VM的计算机服务器。进一步地,本发明的一个或多个实施例通过促进托管VM的计算机服务器托管安全VM来促进对计算技术本身的操作的改进,特别是托管VM的计算机服务器,在安全VM中,甚至管理程序也被禁止访问与安全VM相关联的存储器、寄存器和其他这样的数据。此外,本发明的一个或多个实施例通过使用安全接口控件(这里也被称为“UV”)来提供对VM托管计算服务器的改进的重要步骤,其中安全接口控件包括硬件、固件(例如,毫代码)或其组合,以便于安全VM和管理程序的分离,并因此保持由计算服务器托管的VM的安全性。安全接口控件提供轻量级的中间操作以促进安全性,而在如本文所述的VM的初始化/退出期间不增加保护VM状态的实质开销。

[0144] 本文所公开的本发明的实施例可包括控制对VM的安全存储的访问的系统、方法和/或计算机程序产品(在本文中是系统)。注意,对于每个说明,元件的标识符被重复用于不同附图的其他类似元件。

[0145] 在此参考相关附图描述了本发明的各种实施例。在不脱离本发明的范围的情况下,可以设计本发明的替代实施例。在以下描述和附图中,阐述了元件之间的各种连接和位置关系(例如,上方、下方、相邻等)。除非另有说明,这些连接和/或位置关系可以是直接的或间接的,并且本发明并不旨在在这方面进行限制。因此,实体的耦合可以是指直接耦合或

间接耦合,并且实体之间的位置关系可以是直接或间接位置关系。此外,本文所述的各种任务和过程步骤可被并入具有本文未详细描述的附加步骤或功能的更综合的程序或过程中。

[0146] 以下定义和缩写用于权利要求和说明书的解释。如本文所使用的,术语“包含”、“包括”、“具有”、“含有”或其任何其它变型旨在涵盖非排他性的包括。例如,包括一系列要素的组合物、混合物、过程、方法、制品、或装置并不一定仅限于那些要素,而是可以包括未明确列出的或对于此类组合物、混合物、过程、方法、制品、或装置固有的其他要素。

[0147] 另外,术语“示例性”在本文中用于表示“用作示例、实例或说明”。在此描述为“示例性”的任何实施例或设计不一定被解释为比其它实施例或设计更优选或有利。术语“至少一个”和“一个或多个”可被理解为包括大于或等于一的任何整数,即,一、二、三、四等。术语“多个”可以被理解为包括大于或等于二的任何整数,即二、三、四、五等。术语“连接”可以包括间接“连接”和直接“连接”两者。

[0148] 术语“大约”、“基本上”、“近似”及其变型旨在包括与基于提交本申请时可用的设备的特定量的测量相关联的误差度。例如,“大约”可以包括给定值的±8%或±5%或±2%的范围。

[0149] 本发明可以是任何可能的技术细节集成水平的系统、方法和/或计算机程序产品。计算机程序产品可以包括在其上具有计算机可读程序指令的(一个或多个)计算机可读存储介质,计算机可读程序指令用于使处理器执行本发明的各方面。

[0150] 计算机可读存储介质可以是可保持并存储由指令执行设备使用的指令的有形设备。计算机可读存储介质可以是例如但不限于电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备、或前述存储设备的任何合适的组合。计算机可读存储介质的更具体示例的非穷举列表包括以下:便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式光盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、诸如在上面记录有指令的打孔卡或凹槽中的凸起结构的机械编码设备、以及上述设备的任何适当的组合。如本文所使用的计算机可读存储介质不应被解释为是暂时性信号本身,诸如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如,通过光纤线缆的光脉冲)、或通过导线传输的电信号。

[0151] 本文描述的计算机可读程序指令可以从计算机可读存储介质下载到相应的计算/处理设备,或者经由网络(例如互联网、局域网、广域网和/或无线网络)下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输光纤、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或网络接口从网络接收计算机可读程序指令,并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0152] 用于执行本发明的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据、或者以一种或多种编程语言(包括面向对象的编程语言,例如Smalltalk、C++等)和过程编程语言(例如“C”编程语言或类似的编程语言)的任意组合编写的源代码或目标代码。计算机可读程序指令可以完全在用户的计算机上执行、部分在用户的计算机上执行、作为独立的软件包执行、部分在用户的计算机上并且部分在远程计算机上执行、或者完全在远程

计算机或服务器上执行。在后一种场景下,远程计算机可以通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接到用户的计算机,或者可以连接到外部计算机(例如,使用互联网服务提供商通过互联网)。在一些实施例中,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来执行计算机可读程序指令以使电子电路个性化,以便执行本发明的各方面。

[0153] 在此参考根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明的各方面。将理解,流程图和/或框图的每个框以及流程图和/或框图中的框的组合可以由计算机可读程序指令来实现。

[0154] 这些计算机可读程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器,以使得经由计算机或其他可编程数据处理装置的处理器而执行的指令创建用于实现流程图和/或框图的一个或多个框中指定的功能/动作的装置。这些计算机可读程序指令还可以存储在计算机可读存储介质中,其可以引导计算机、可编程数据处理装置和/或其他设备以特定方式工作,已使得在其中存储有指令的计算机可读存储介质包括制品,该制品包括实现流程图和/或框图的一个或多个框中指定的功能/动作的各方面的指令。

[0155] 计算机可读程序指令还可以被加载到计算机、其他可编程数据处理装置或其他设备上,以使一系列操作步骤将在计算机、其他可编程装置或其他设备上执行,以产生计算机实现的过程,以使得在计算机、其他可编程装置或其他设备上执行的指令实现流程图和/或框图的一个或多个框中指定的功能/动作。

[0156] 附图中的流程图和框图示出了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实现的架构、功能和操作。在这点上,流程图或框图中的每个框可以表示指令的模块、段或部分,其包括用于实现指定的逻辑功能的一个或多个可执行指令。在一些替代实施方案中,框中所注明的功能可不按图中所注明的次序发生。例如,连续示出的两个框实际上可以基本上同时执行,或者这些框有时可以以相反的顺序执行,这取决于所涉及的功能。还将注意,框图和/或流程图图示的每个框以及框图和/或流程图图示中的框的组合可以由执行指定功能或动作或执行专用硬件和计算机指令的组合的专用的基于硬件的系统来实现。

[0157] 本文所用的术语仅是为了描述特定实施例的目的,而不是旨在进行限制。如本文所使用的,单数形式“一”、“一个”和“该”旨在也包括复数形式,除非上下文另有明确指示。还将理解,术语“包括”和/或“包含”在本说明书中使用时指定所陈述的特征、整数、步骤、操作、元件和/或组件的存在,但不排除一个或多个其它特征、整数、步骤、操作、元件组件和/或其群组的存在或添加。

[0158] 本文已经出于说明的目的呈现了对各种实施例的描述,但其并非旨在是穷尽性的或限于所公开的实施例。在不背离所描述的实施例的范围和精神的情况下,许多修改和变化对于本领域的普通技术人员将是显而易见的。选择本文所使用的术语以最好地解释实施例的原理、实际应用或对市场上存在的技术改进,或使本领域的其他普通技术人员能够理解本文所公开的实施例。

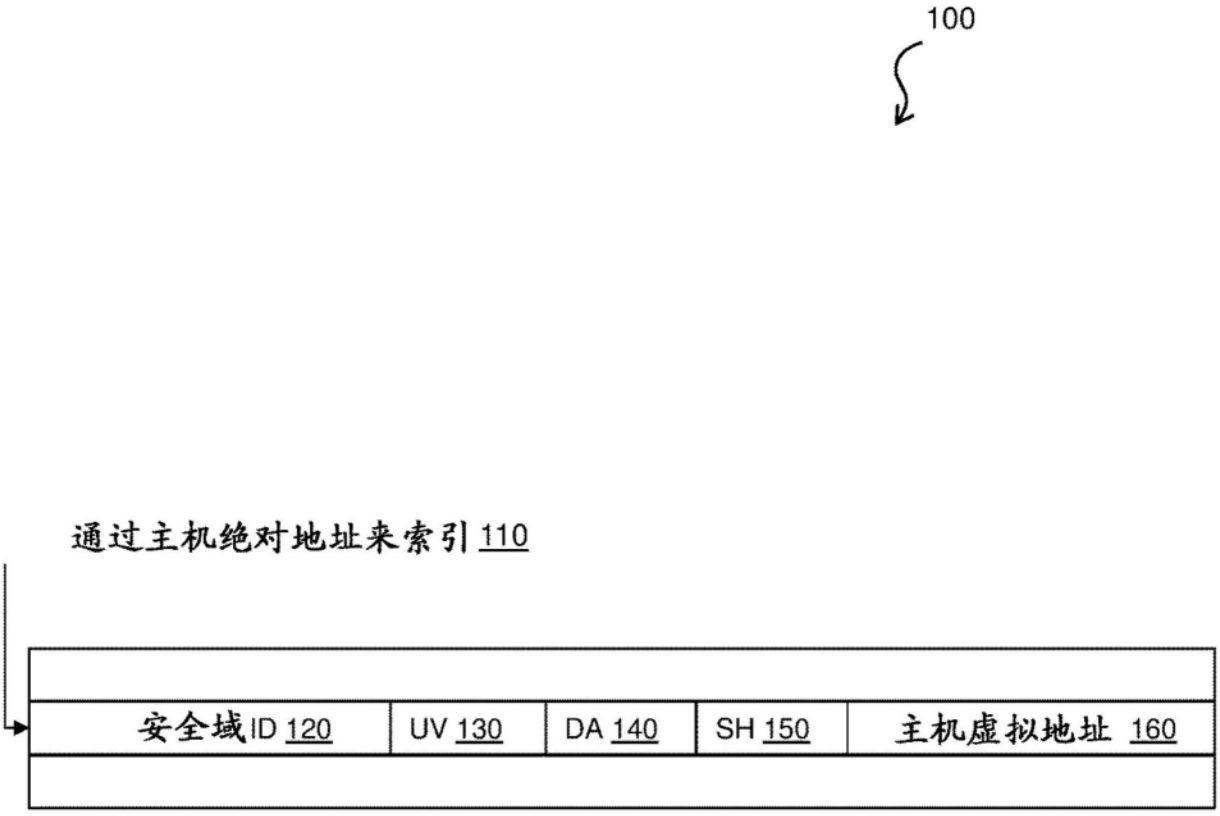


图1

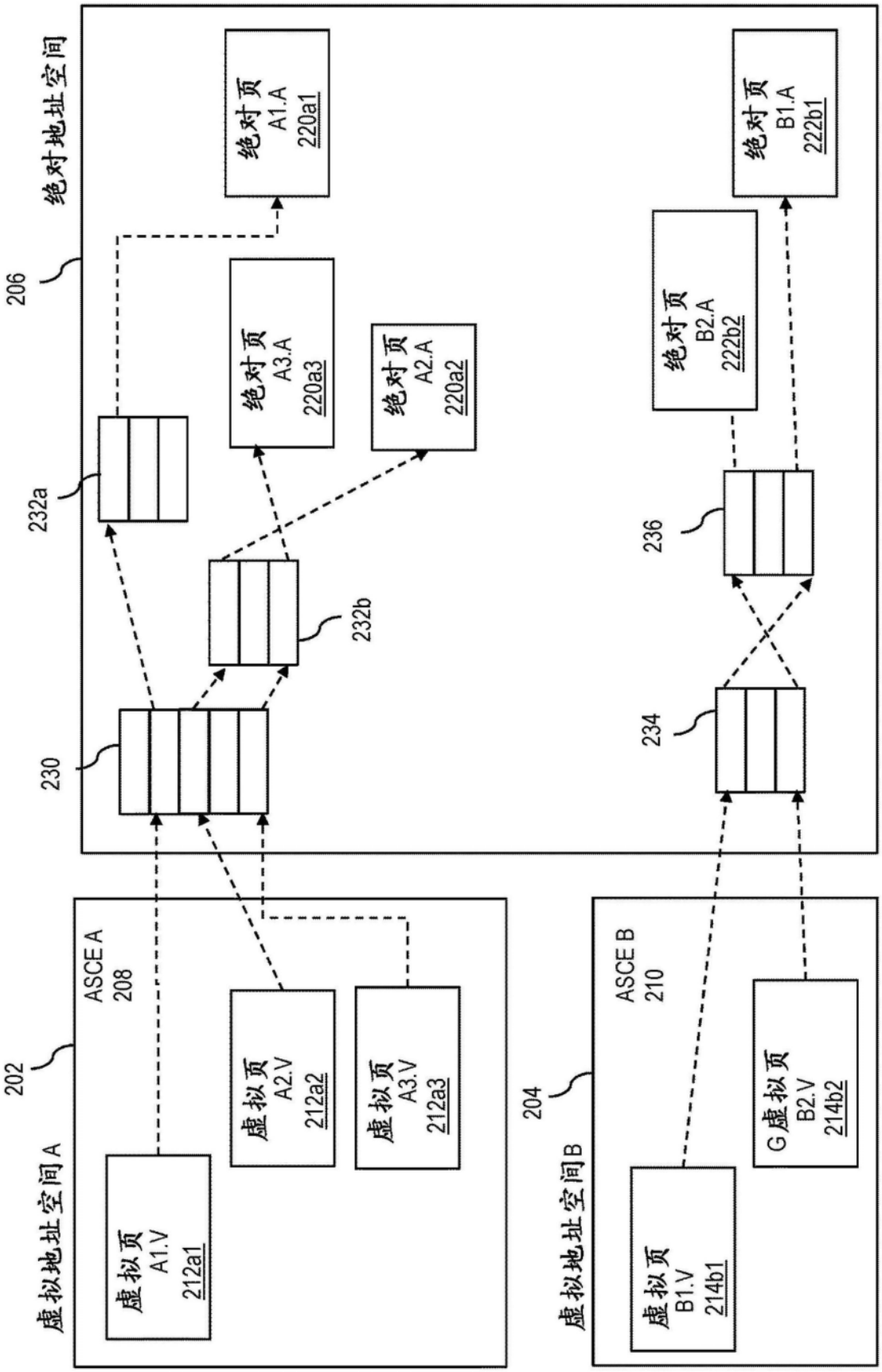

虚拟地址空间A
202
ASCE A
208
虚拟页
A1.V
212a1
虚拟页
A2.V
212a2
虚拟页
A3.V
212a3
虚拟地址空间B
204
ASCE B
210
虚拟页
B1.V
214b1
G虚拟页
B2.V
214b2
绝对地址空间
206
230
232a
232b
234
236
绝对页
A1.A
220a1
绝对页
A3.A
220a3
绝对页
A2.A
220a2
绝对页
B2.A
222b2
绝对页
B1.A
222b1

图2

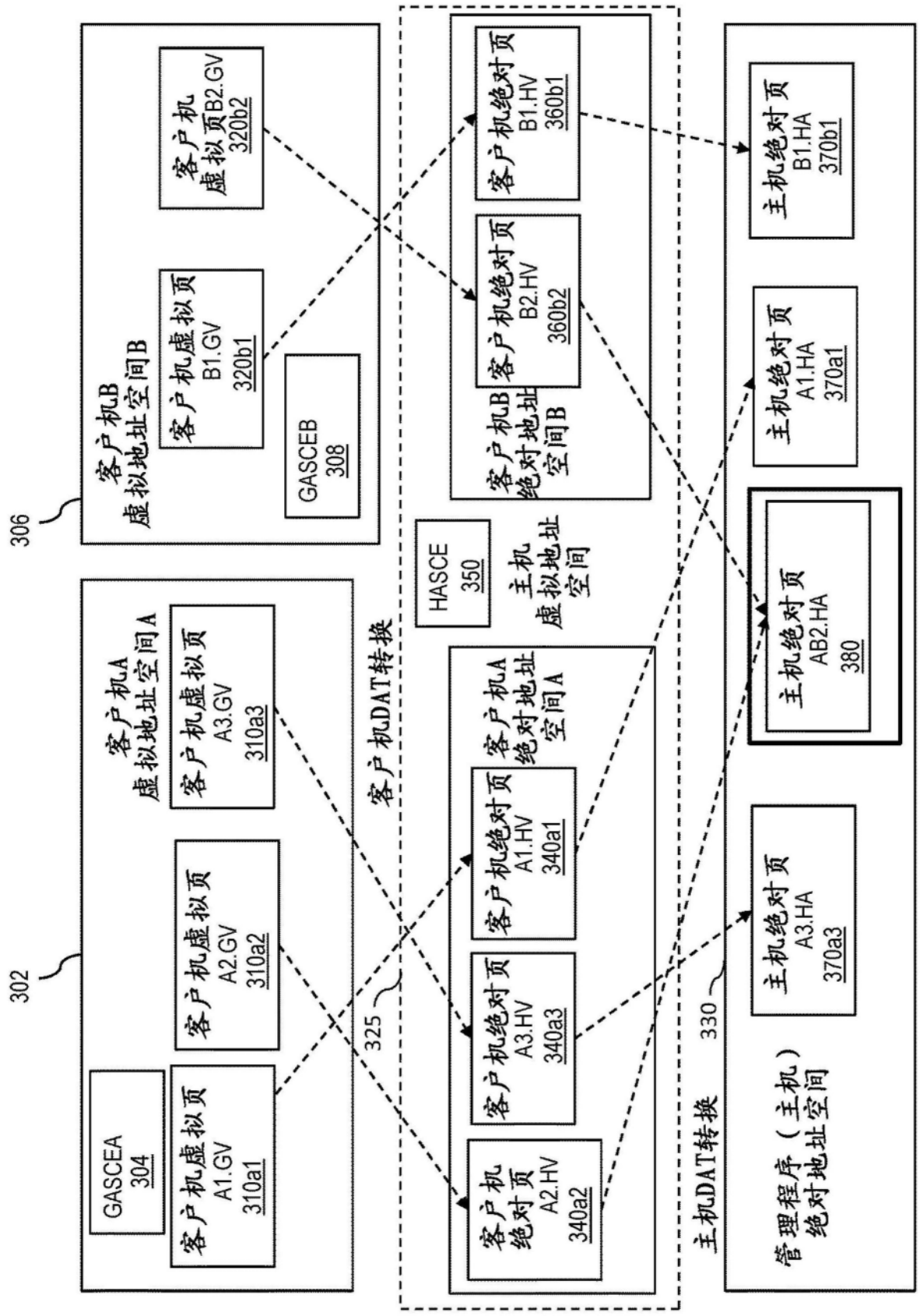

302
306
325
330
客户机A
虚拟地址空间A
客户机虚拟页
A1.GV
310a1
客户机虚拟页
A2.GV
310a2
客户机虚拟页
A3.GV
310a3
GASCEA
304
客户机B
虚拟地址空间B
客户机虚拟页
B1.GV
320b1
客户机虚拟页B2.GV
320b2
GASCEB
308
客户机DAT转换
HASCE
350
主机
虚拟地址
空间
客户机A
绝对地址
空间A
客户机绝对页
A2.HV
340a2
客户机绝对页
A3.HV
340a3
客户机绝对页
A1.HV
340a1
客户机B
绝对地址
空间B
客户机绝对页
B2.HV
360b2
客户机绝对页
B1.HV
360b1
主机DAT转换
管理程序（主机）
绝对地址空间
主机绝对页
A3.HA
370a3
主机绝对页
A1.HA
370a1
主机绝对页
B1.HA
370b1
主机绝对页
AB2.HA
380

图3

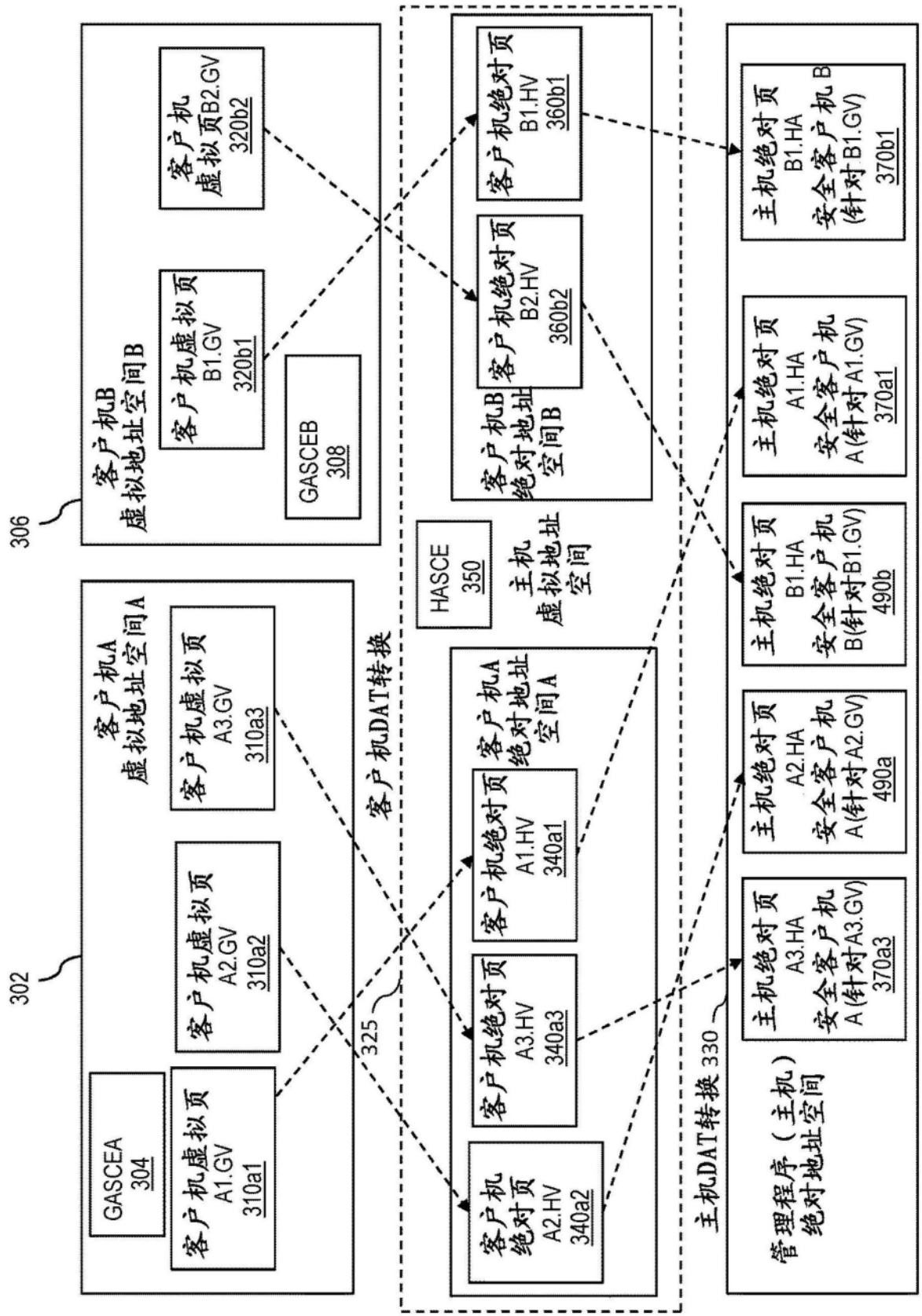

306
客户机B
虚拟地址空间B
客户机虚拟页
B2.GV
320b2
客户机虚拟页
B1.GV
320b1
GASCEB
308
302
客户机A
虚拟地址空间A
客户机虚拟页
A3.GV
310a3
客户机虚拟页
A2.GV
310a2
GASCEA
304
客户机虚拟页
A1.GV
310a1
325
客户机DAT转换
HASCE
350
主机
虚拟地址
空间
客户机绝对页
B1.HV
360b1
客户机绝对页
B2.HV
360b2
客户机B
绝对地址
空间B
客户机绝对页
A1.HV
340a1
客户机绝对页
A3.HV
340a3
客户机A
绝对地址
空间A
客户机
绝对页
A2.HV
340a2
主机绝对页
B1.HA
安全客户机B
(针对B1.GV)
370b1
主机绝对页
A1.HA
安全客户机
A(针对A1.GV)
370a1
主机绝对页
B1.HA
安全客户机
B(针对B1.GV)
490b
主机绝对页
A2.HA
安全客户机
A(针对A2.GV)
490a
主机绝对页
A3.HA
安全客户机
A(针对A3.GV)
370a3
主机DAT转换 330
管理程序（主机）
绝对地址空间

图4

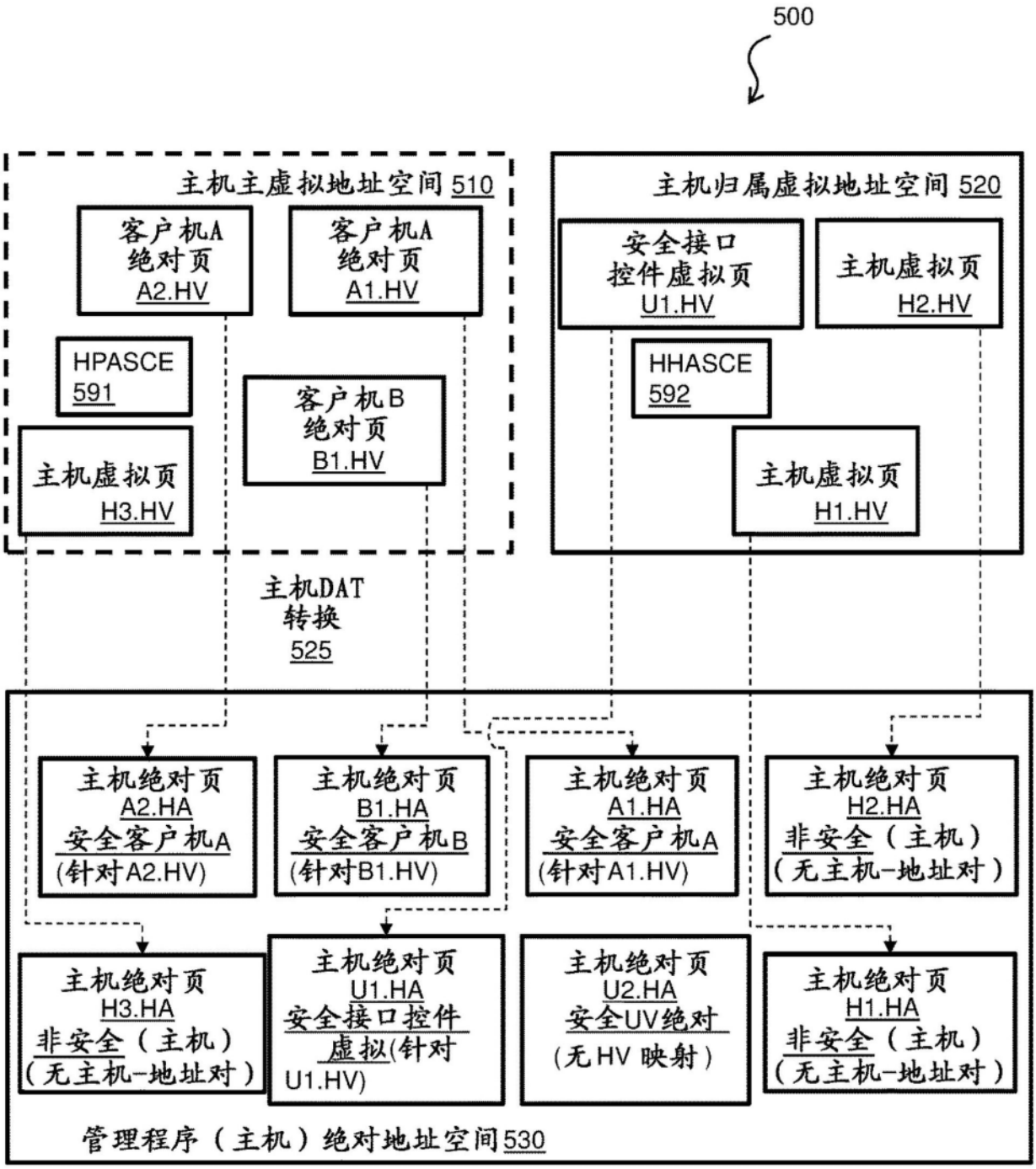

500
主机主虚拟地址空间 510
客户机A 绝对页 A2.HV
客户机A 绝对页 A1.HV
HPASCE 591
客户机B 绝对页 B1.HV
主机虚拟页 H3.HV
主机归属虚拟地址空间 520
安全接口控件虚拟页 U1.HV
主机虚拟页 H2.HV
HHASCE 592
主机虚拟页 H1.HV
主机DAT 转换 525
主机绝对页 A2.HA 安全客户机A (针对A2.HV)
主机绝对页 B1.HA 安全客户机B (针对B1.HV)
主机绝对页 A1.HA 安全客户机A (针对A1.HV)
主机绝对页 H2.HA 非安全（主机）（无主机-地址对）
主机绝对页 H3.HA 非安全（主机）（无主机-地址对）
主机绝对页 U1.HA 安全接口控件虚拟(针对U1.HV)
主机绝对页 U2.HA 安全UV绝对 (无HV 映射)
主机绝对页 H1.HA 非安全（主机）（无主机-地址对）
管理程序（主机）绝对地址空间530

图5

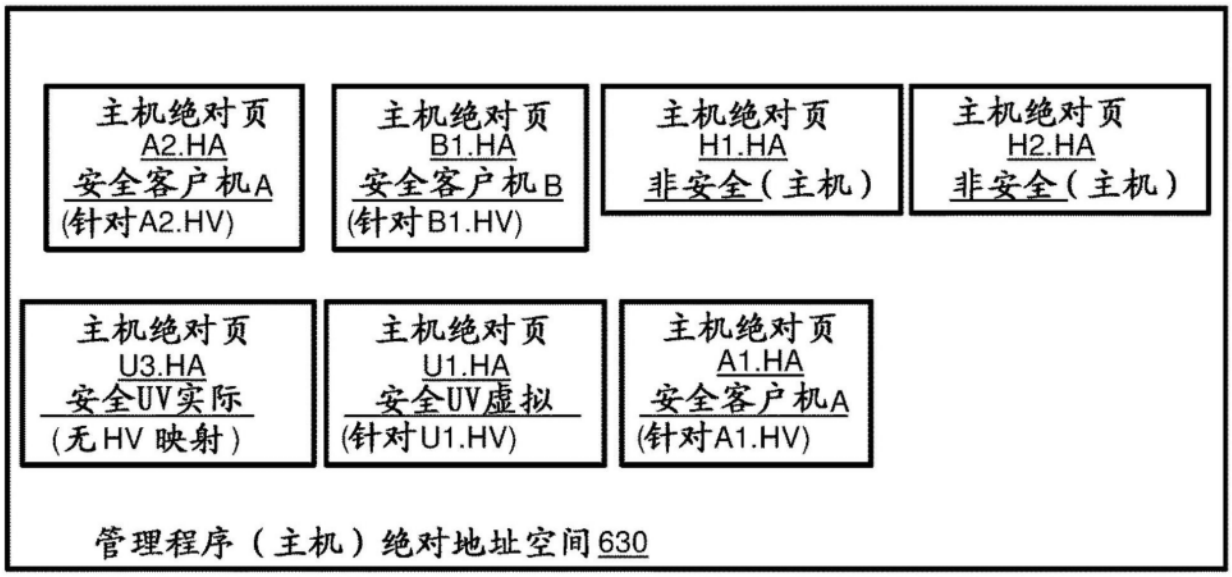

主机绝对页
A2.HA
安全客户机A
(针对A2.HV)
主机绝对页
B1.HA
安全客户机B
(针对B1.HV)
主机绝对页
H1.HA
非安全(主机)
主机绝对页
H2.HA
非安全(主机)
主机绝对页
U3.HA
安全UV实际
(无HV 映射)
主机绝对页
U1.HA
安全UV虚拟
(针对U1.HV)
主机绝对页
A1.HA
安全客户机A
(针对A1.HV)
管理程序(主机)绝对地址空间630

图6

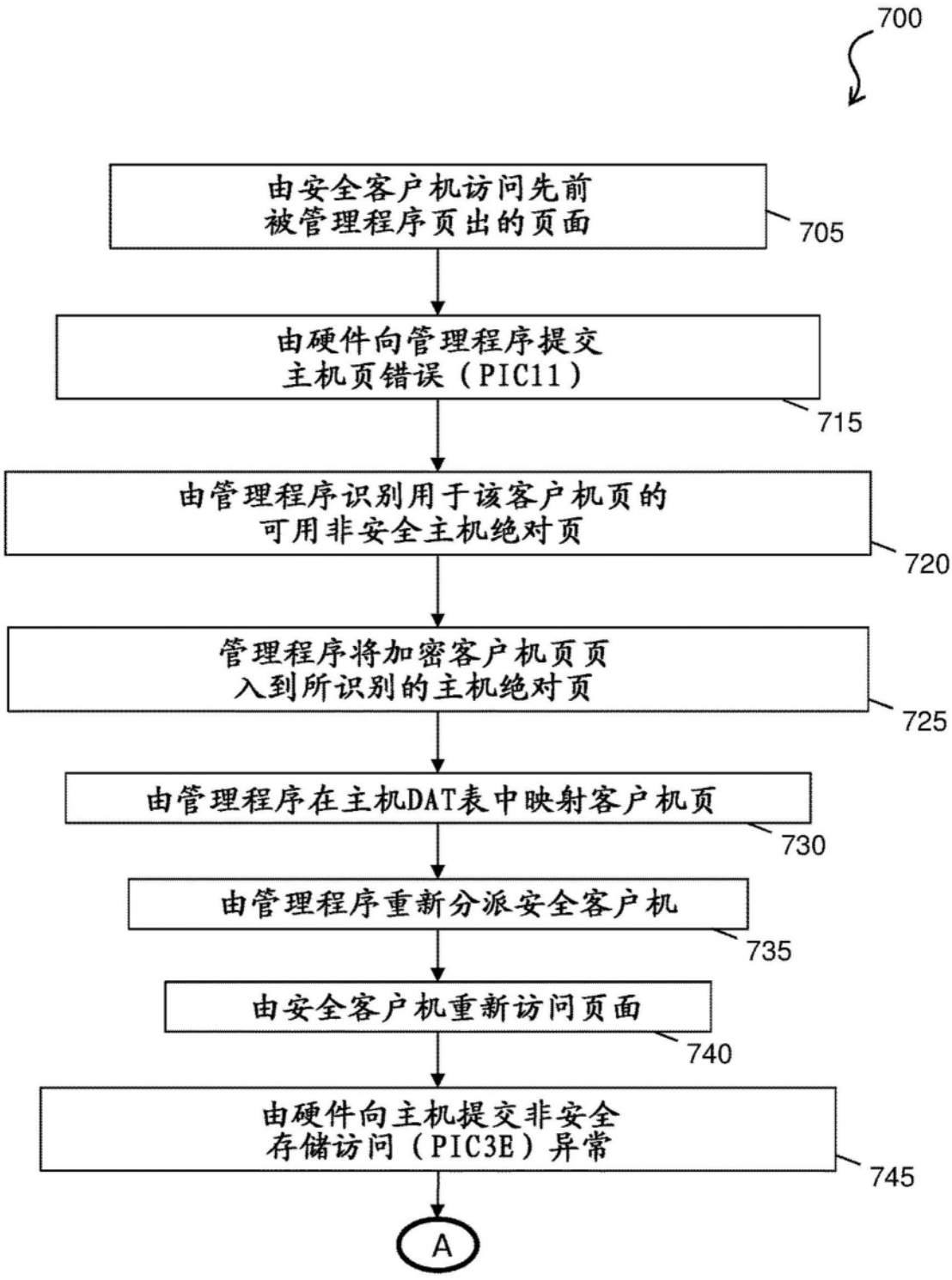

700
由安全客户机访问先前
被管理程序页出的页面
705
由硬件向管理程序提交
主机页错误（PIC11）
715
由管理程序识别用于该客户机页的
可用非安全主机绝对页
720
管理程序将加密客户机页页
入到所识别的主机绝对页
725
由管理程序在主机DAT表中映射客户机页
730
由管理程序重新分派安全客户机
735
由安全客户机重新访问页面
740
由硬件向主机提交非安全
存储访问（PIC3E）异常
745
A

图7

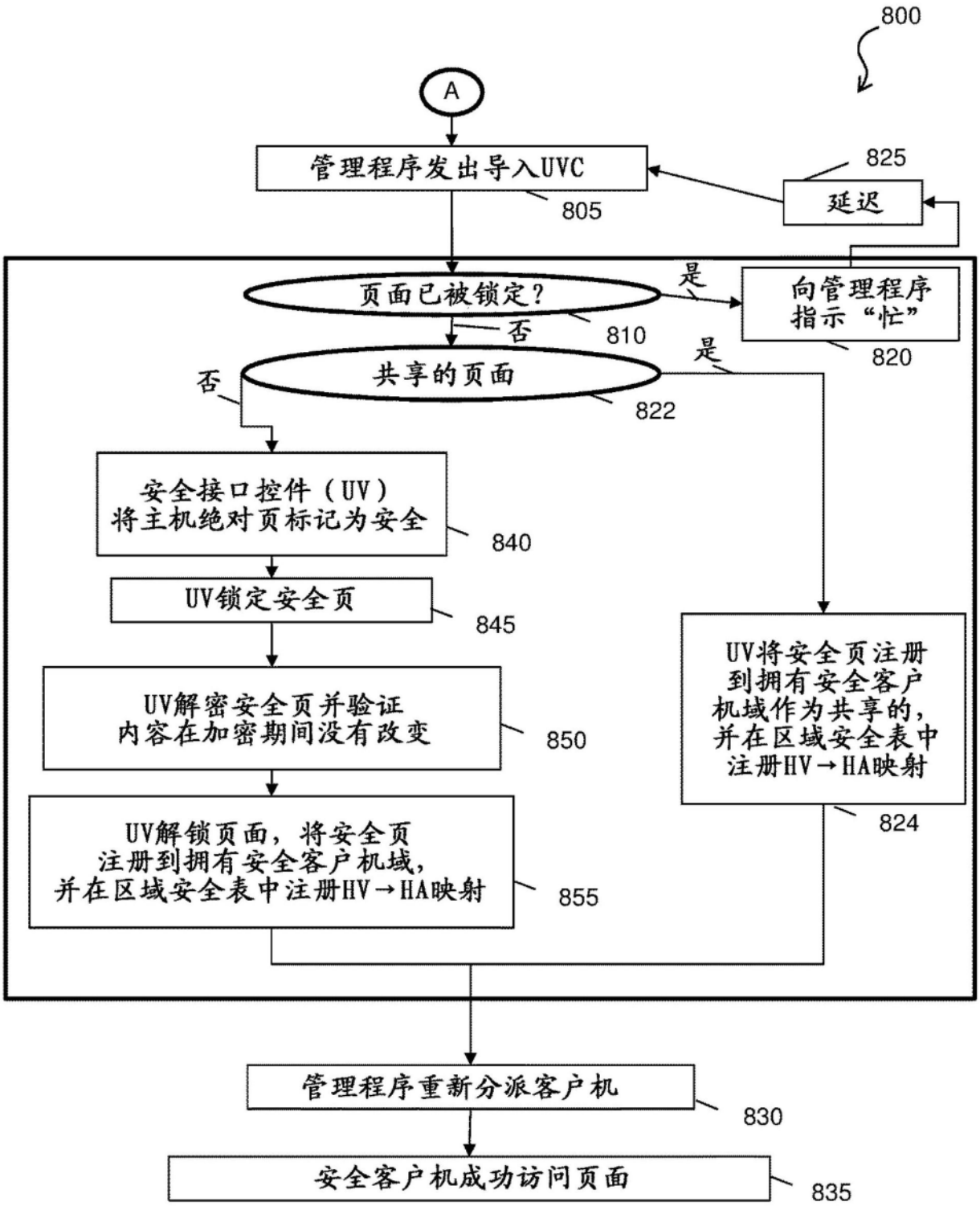

800
A
管理程序发出导入UVC
805
825
延迟
页面已被锁定？
是
向管理程序
指示“忙”
820
否
810
共享的页面
是
否
822
安全接口控件（UV）
将主机绝对页标记为安全
840
UV锁定安全页
845
UV解密安全页并验证
内容在加密期间没有改变
850
UV将安全页注册
到拥有安全客户
机域作为共享的，
并在区域安全表中
注册HV→HA映射
824
UV解锁页面，将安全页
注册到拥有安全客户机域，
并在区域安全表中注册HV→HA映射
855
管理程序重新分派客户机
830
安全客户机成功访问页面
835

图8

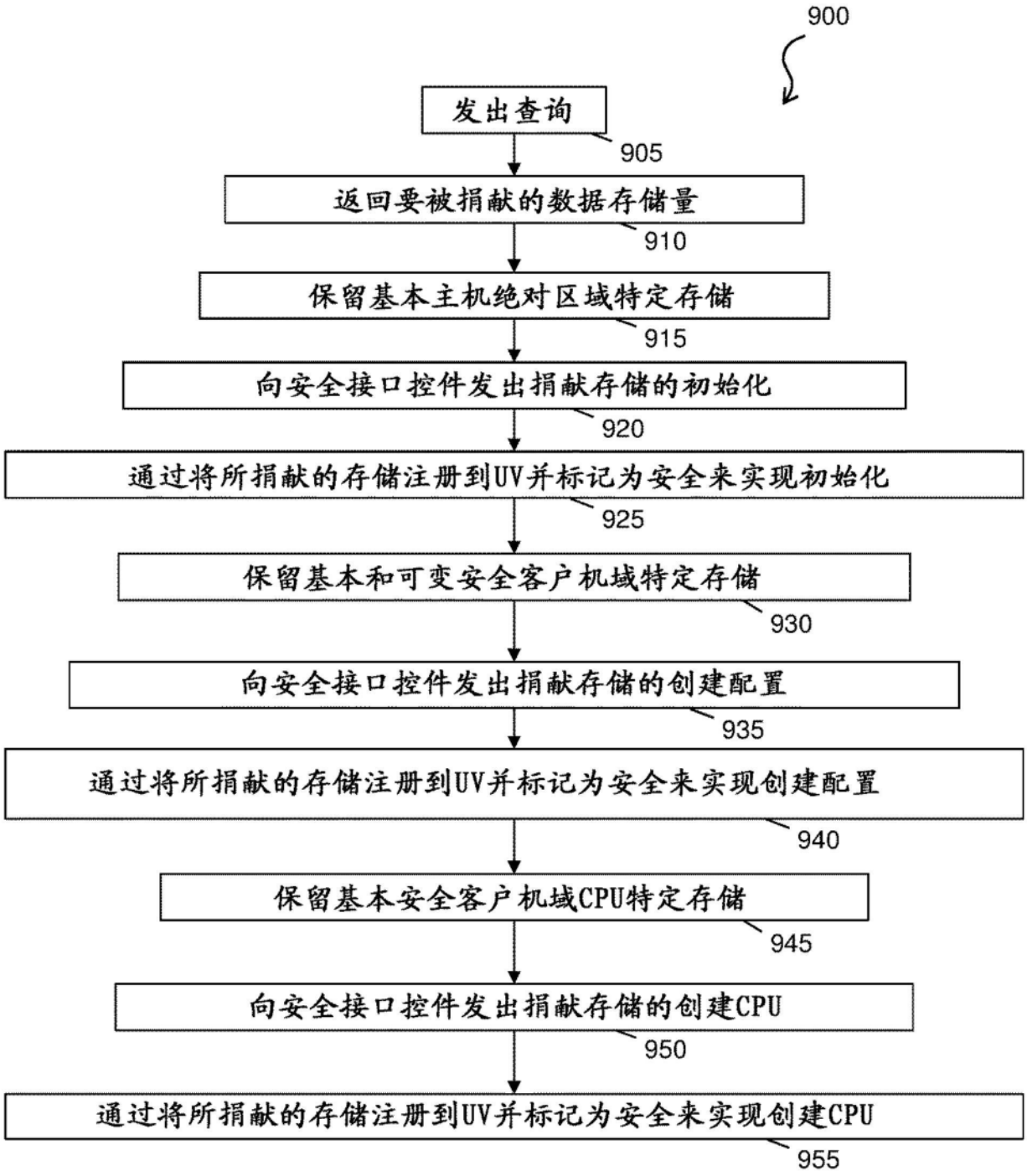

900
发出查询
905
返回要被捐献的数据存储量
910
保留基本主机绝对区域特定存储
915
向安全接口控件发出捐献存储的初始化
920
通过将所捐献的存储注册到UV并标记为安全来实现初始化
925
保留基本和可变安全客户机域特定存储
930
向安全接口控件发出捐献存储的创建配置
935
通过将所捐献的存储注册到UV并标记为安全来实现创建配置
940
保留基本安全客户机域CPU特定存储
945
向安全接口控件发出捐献存储的创建CPU
950
通过将所捐献的存储注册到UV并标记为安全来实现创建CPU
955

图9

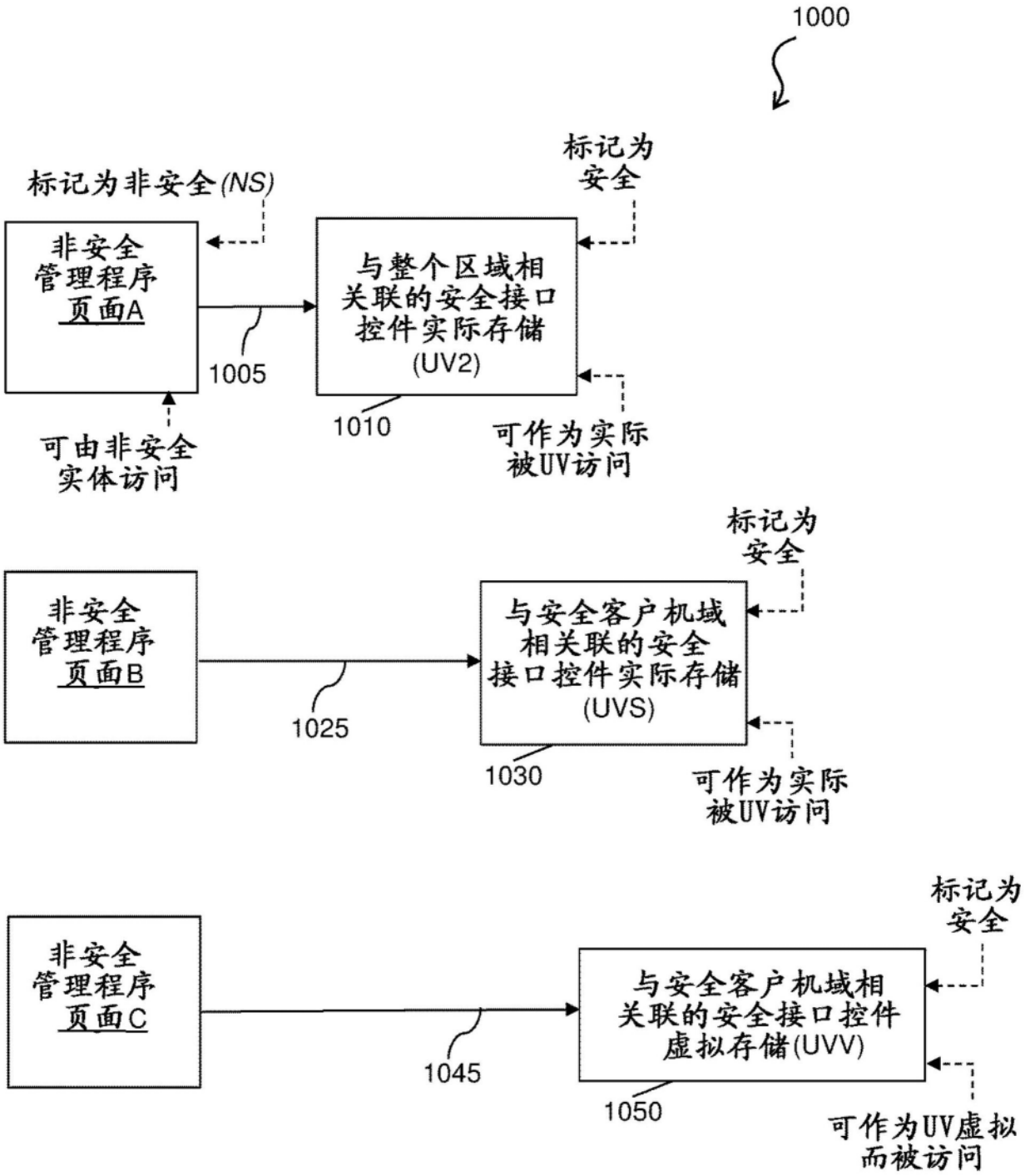

1000
标记为非安全(NS)
标记为安全
非安全管理程序页面A
与整个区域相关联的安全接口控件实际存储(UV2)
1005
1010
可由非安全实体访问
可作为实际被UV访问
标记为安全
非安全管理程序页面B
与安全客户机域相关联的安全接口控件实际存储(UVS)
1025
1030
可作为实际被UV访问
标记为安全
非安全管理程序页面C
与安全客户机域相关联的安全接口控件虚拟存储(UVV)
1045
1050
可作为UV虚拟而被访问

图10

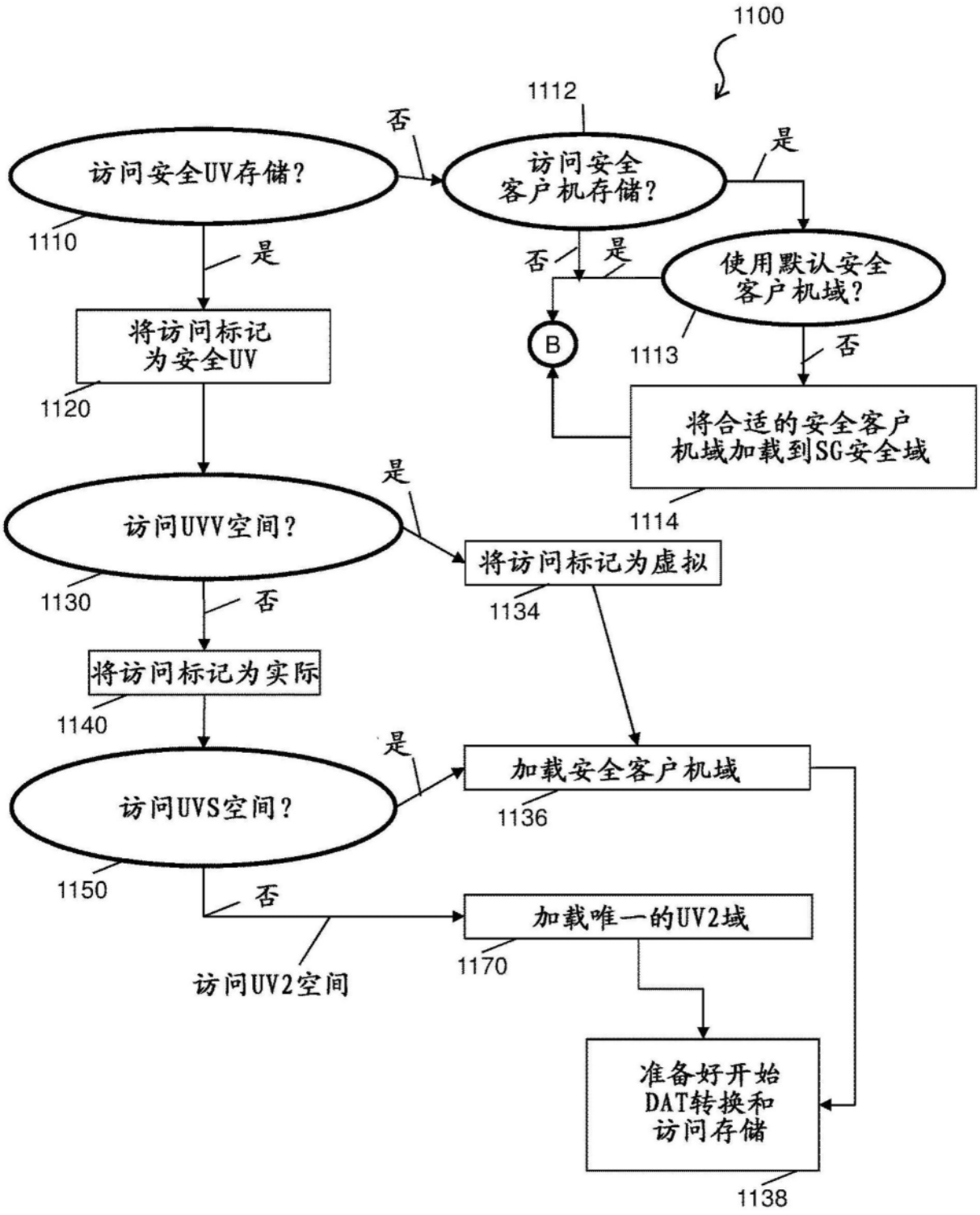

1100
1112
访问安全UV存储?
否
访问安全
客户机存储?
是
1110
是
否
是
使用默认安全
客户机域?
将访问标记
为安全UV
B
1113
否
1120
将合适的安全客户
机域加载到SG安全域
1114
是
访问UVV空间?
将访问标记为虚拟
1130
1134
否
将访问标记为实际
1140
是
加载安全客户机域
访问UVS空间?
1136
1150
否
加载唯一的UV2域
1170
访问UV2空间
准备好开始
DAT转换和
访问存储
1138

图11

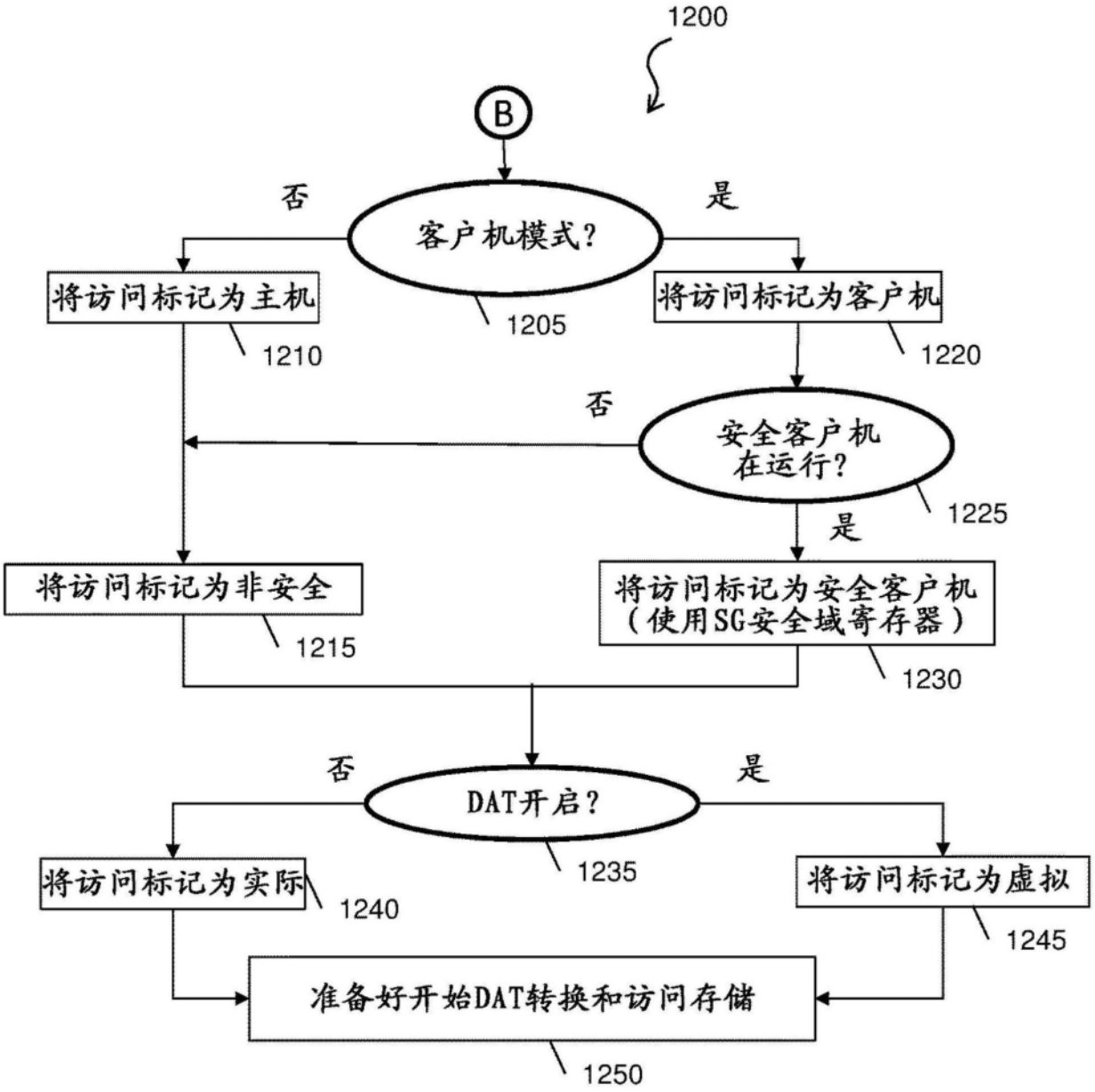

1200
B
否
客户机模式?
是
1205
将访问标记为主机
1210
将访问标记为客户机
1220
否
安全客户机
在运行?
1225
是
将访问标记为非安全
1215
将访问标记为安全客户机
(使用SG安全域寄存器)
1230
否
DAT开启?
是
1235
将访问标记为实际
1240
将访问标记为虚拟
1245
准备好开始DAT转换和访问存储
1250

图12

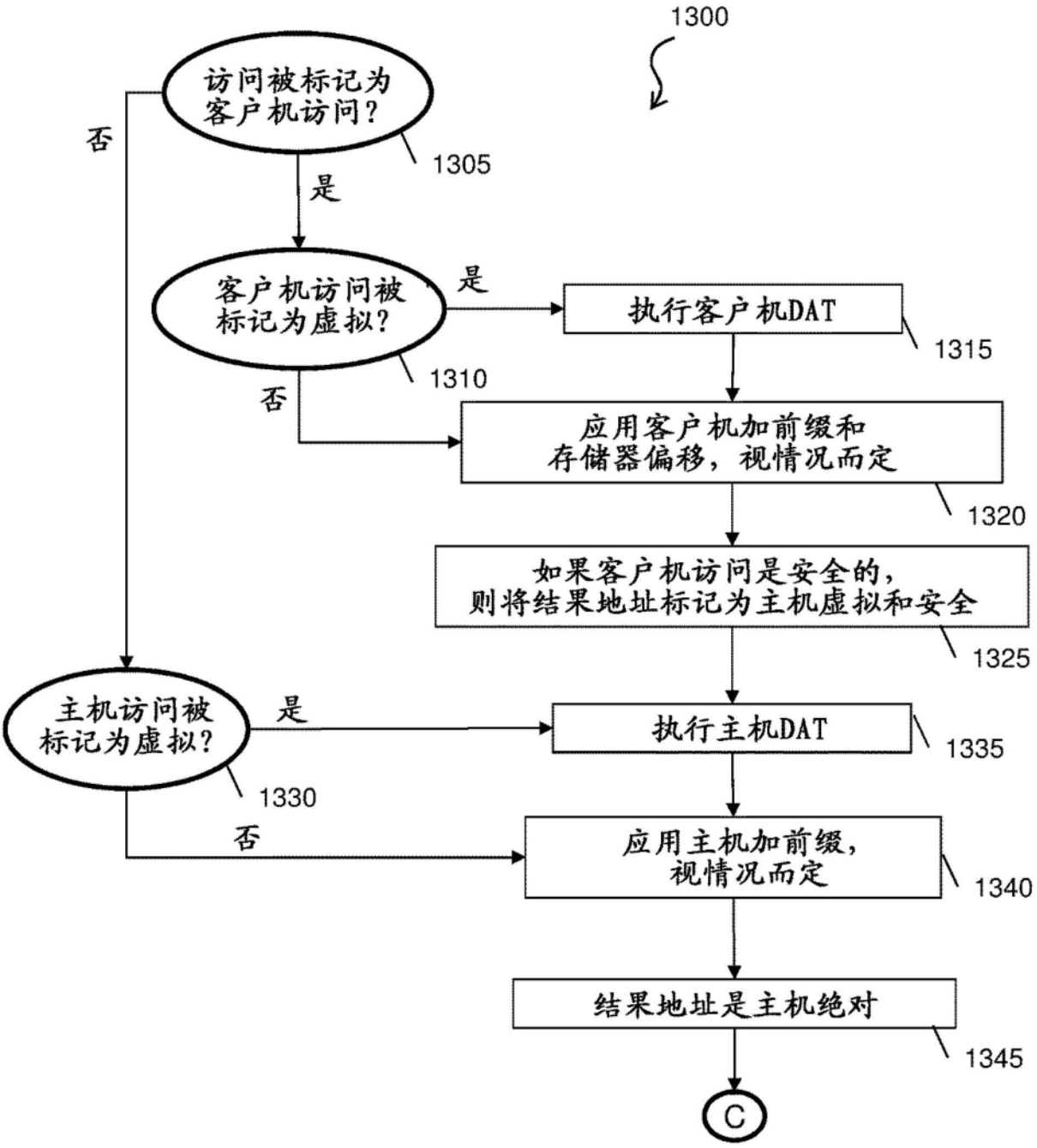

1300
访问被标记为客户机访问？
1305
否
是
客户机访问被标记为虚拟？
1310
是
执行客户机DAT
1315
否
应用客户机加前缀和存储器偏移，视情况而定
1320
如果客户机访问是安全的，则将结果地址标记为主机虚拟和安全
1325
主机访问被标记为虚拟？
1330
是
执行主机DAT
1335
否
应用主机加前缀，视情况而定
1340
结果地址是主机绝对
1345
C

图13

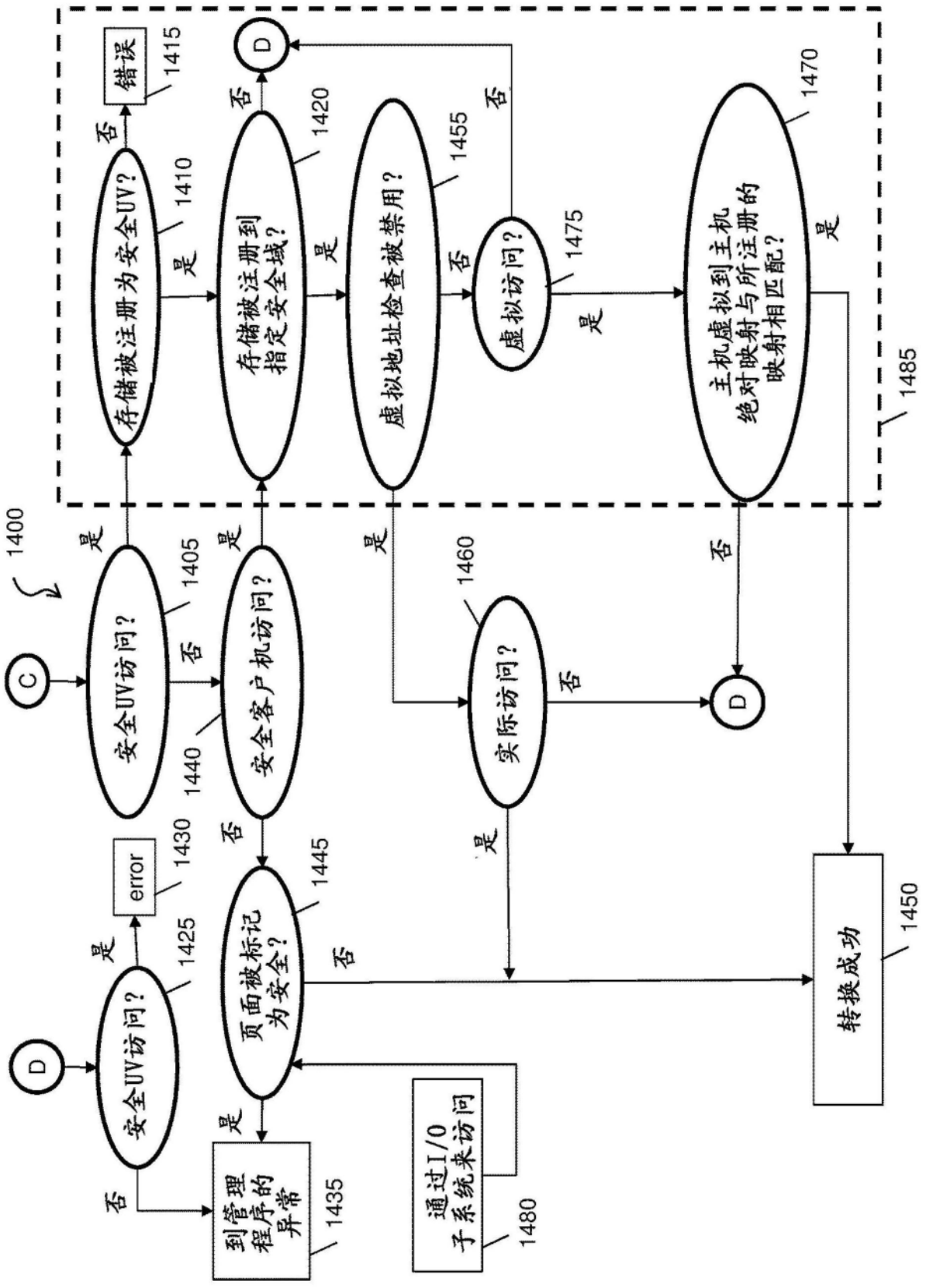

1400
C
安全UV访问？
1405
是
否
存储被注册为安全UV？
1410
是
否
错误
1415
存储被注册到指定安全域？
1420
是
否
虚拟地址检查被禁用？
1455
是
否
虚拟访问？
1475
是
否
主机虚拟到主机绝对映射与所注册的映射相匹配？
1470
是
否
1485
安全客户机访问？
1440
是
否
实际访问？
1460
是
否
D
error
1430
安全UV访问？
1425
是
否
D
页面被标记为安全？
1445
是
否
转换成功
1450
到管理程序的异常
1435
是
通过I/O子系统来访问
1480

图14

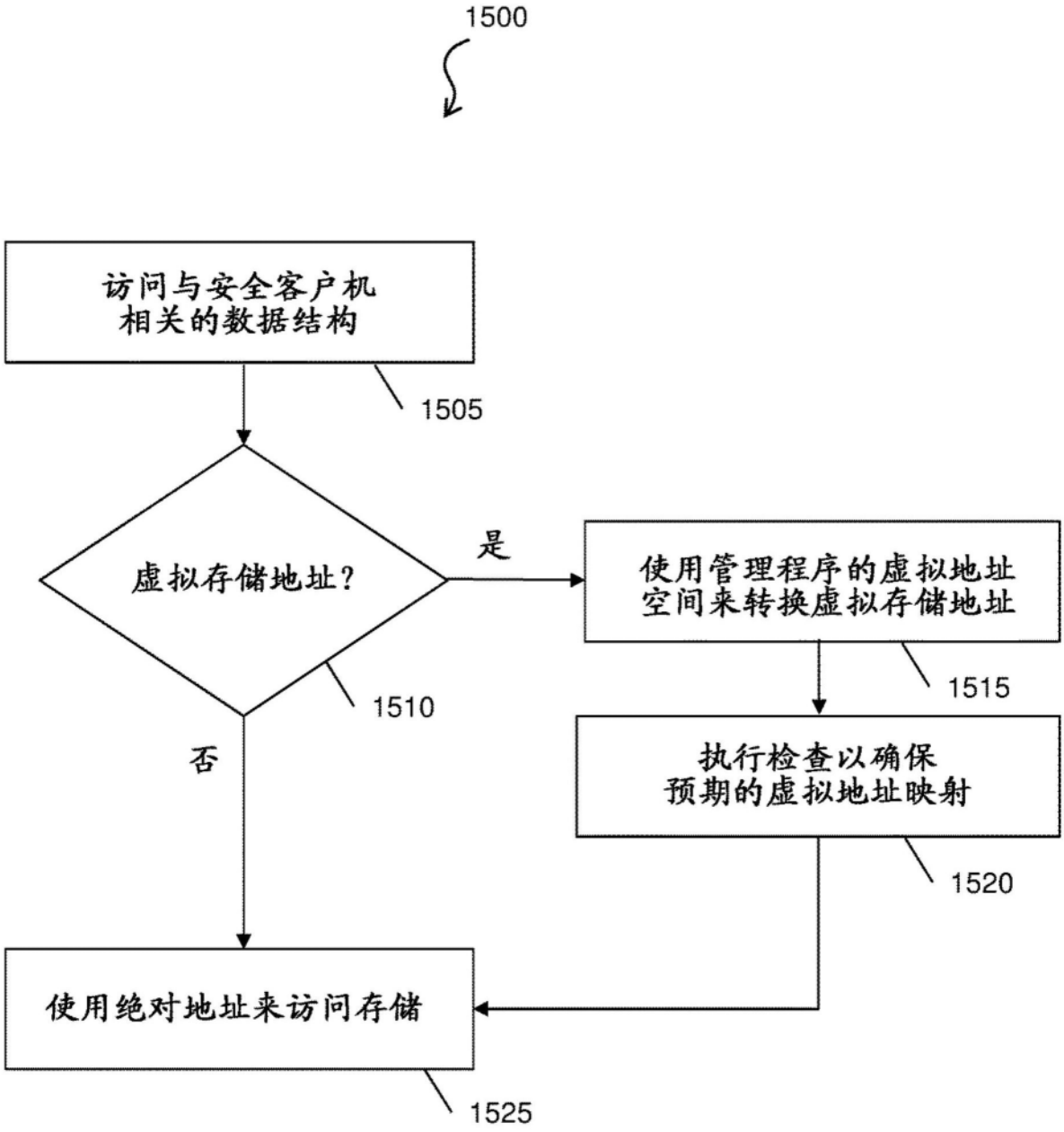

1500
访问与安全客户机
相关的数据结构
1505
虚拟存储地址?
是
1510
使用管理程序的虚拟地址
空间来转换虚拟存储地址
1515
执行检查以确保
预期的虚拟地址映射
1520
否
使用绝对地址来访问存储
1525

图15

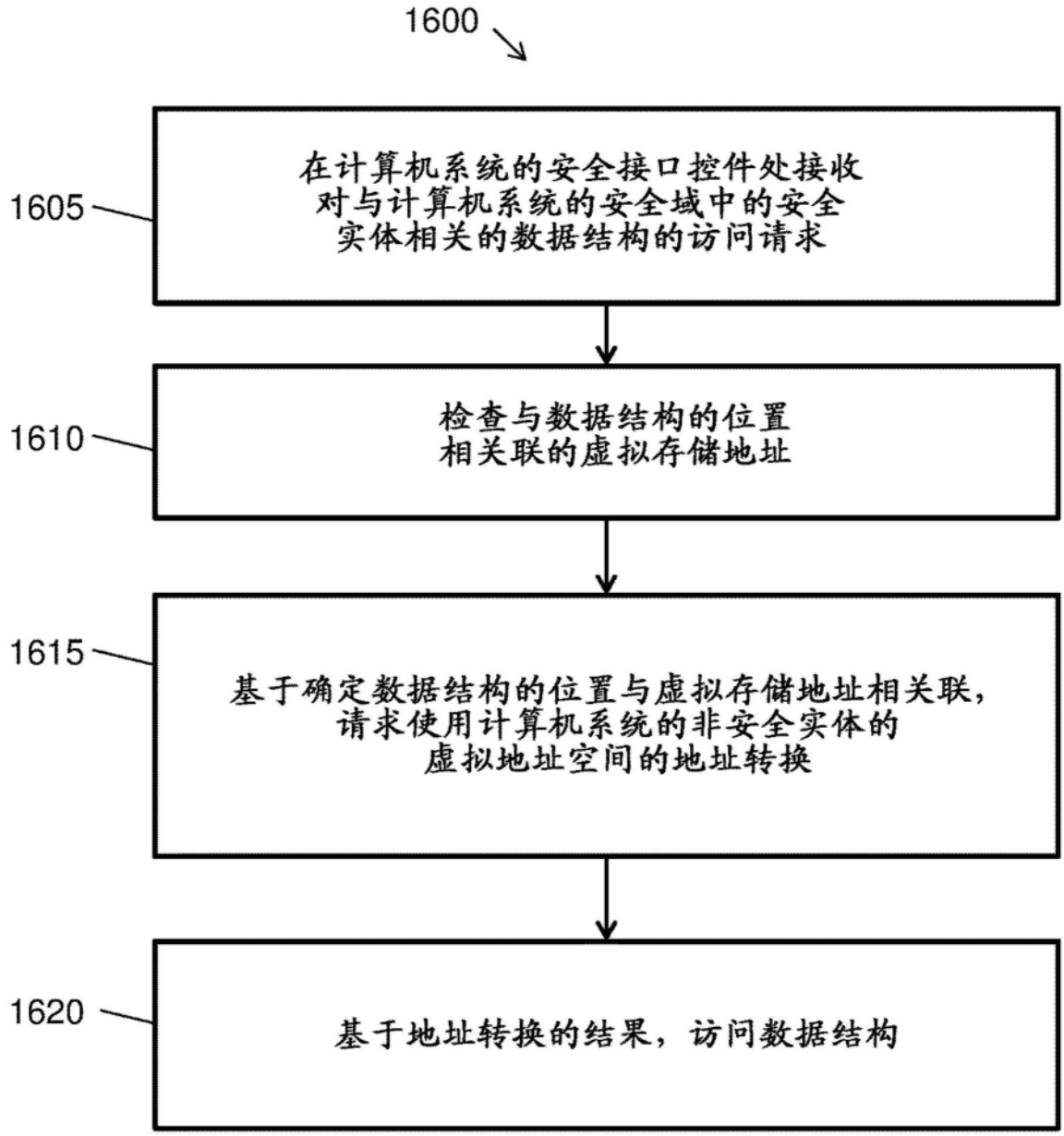

1600
1605
在计算机系统的安全接口控件处接收
对与计算机系统的安全域中的安全
实体相关的数据结构的访问请求
1610
检查与数据结构的位置
相关联的虚拟存储地址
1615
基于确定数据结构的位置与虚拟存储地址相关联，
请求使用计算机系统的非安全实体的
虚拟地址空间的地址转换
1620
基于地址转换的结果，访问数据结构

图16

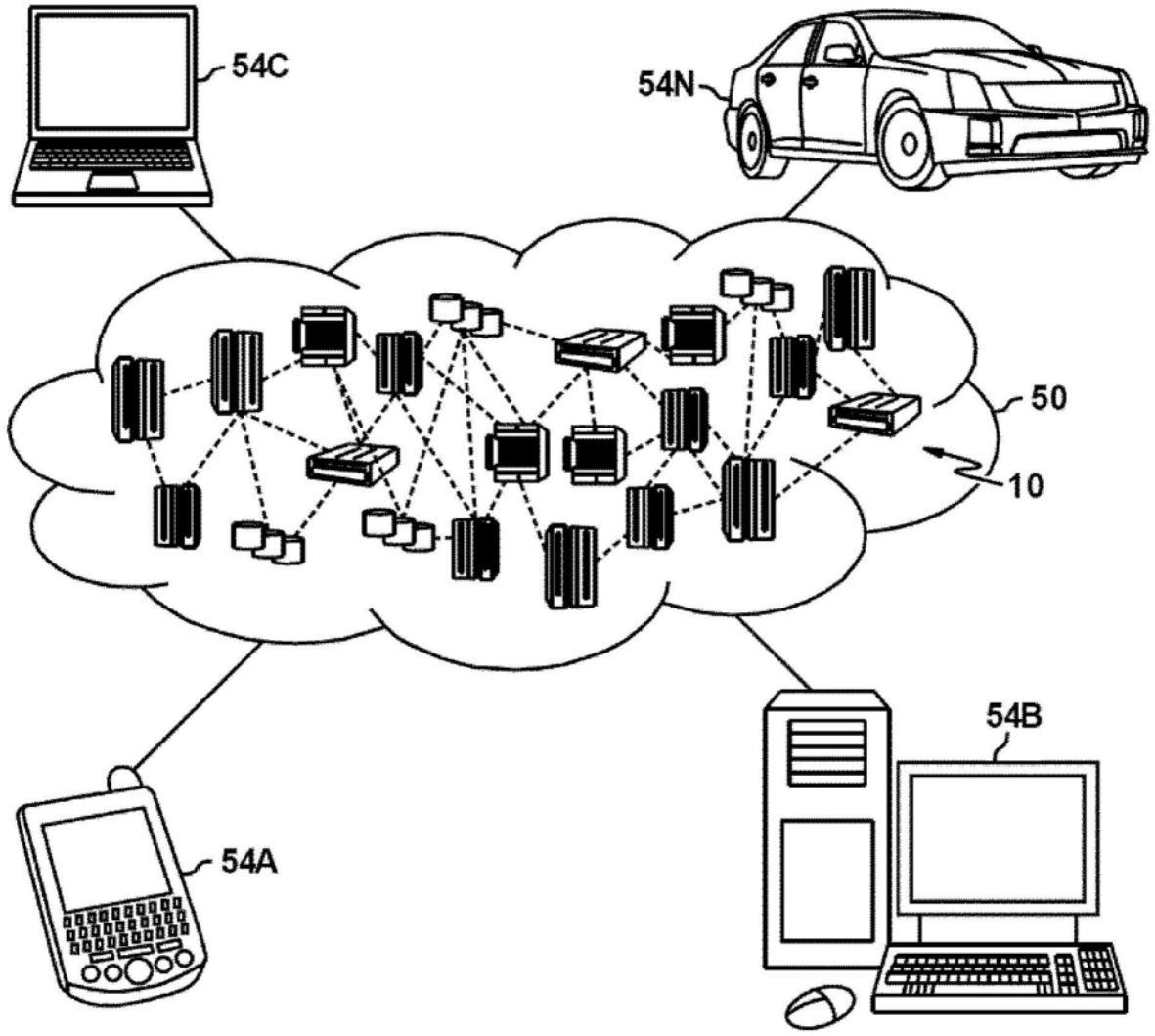


图17

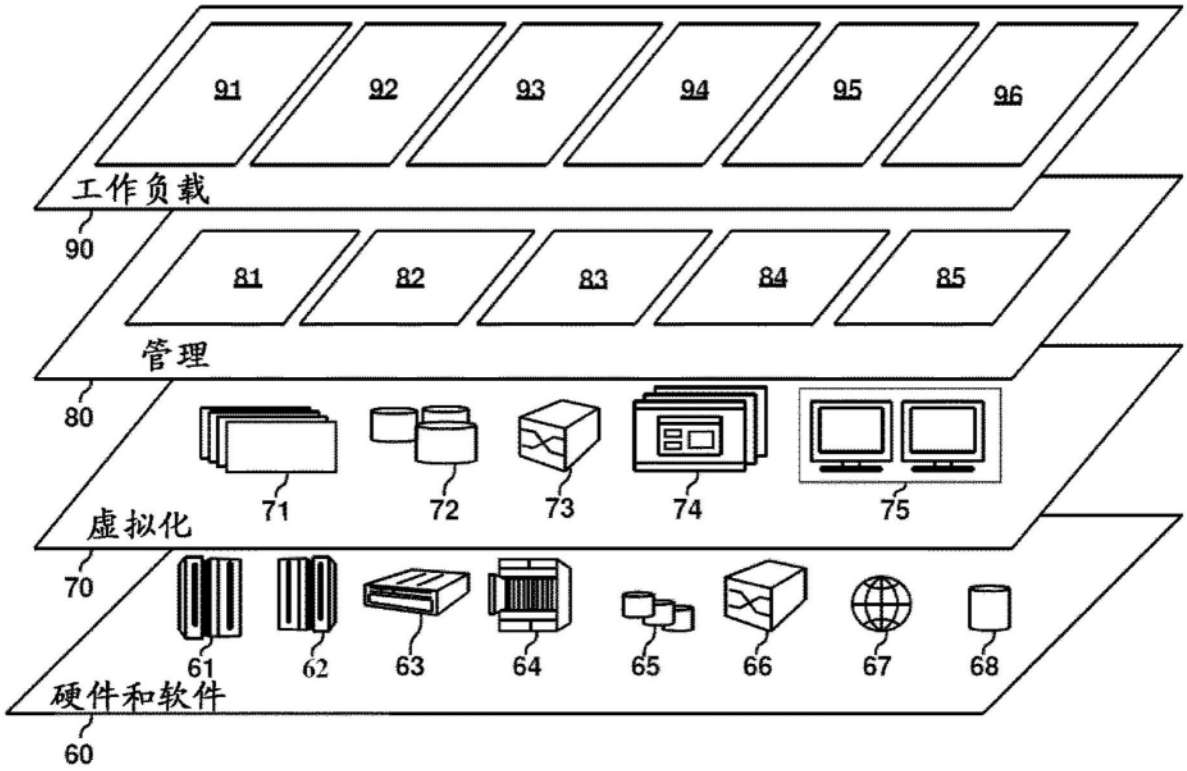

91
92
93
94
95
96
工作负载
90
81
82
83
84
85
管理
80
71
72
73
74
75
虚拟化
70
61
62
63
64
65
66
67
68
硬件和软件
60

图18

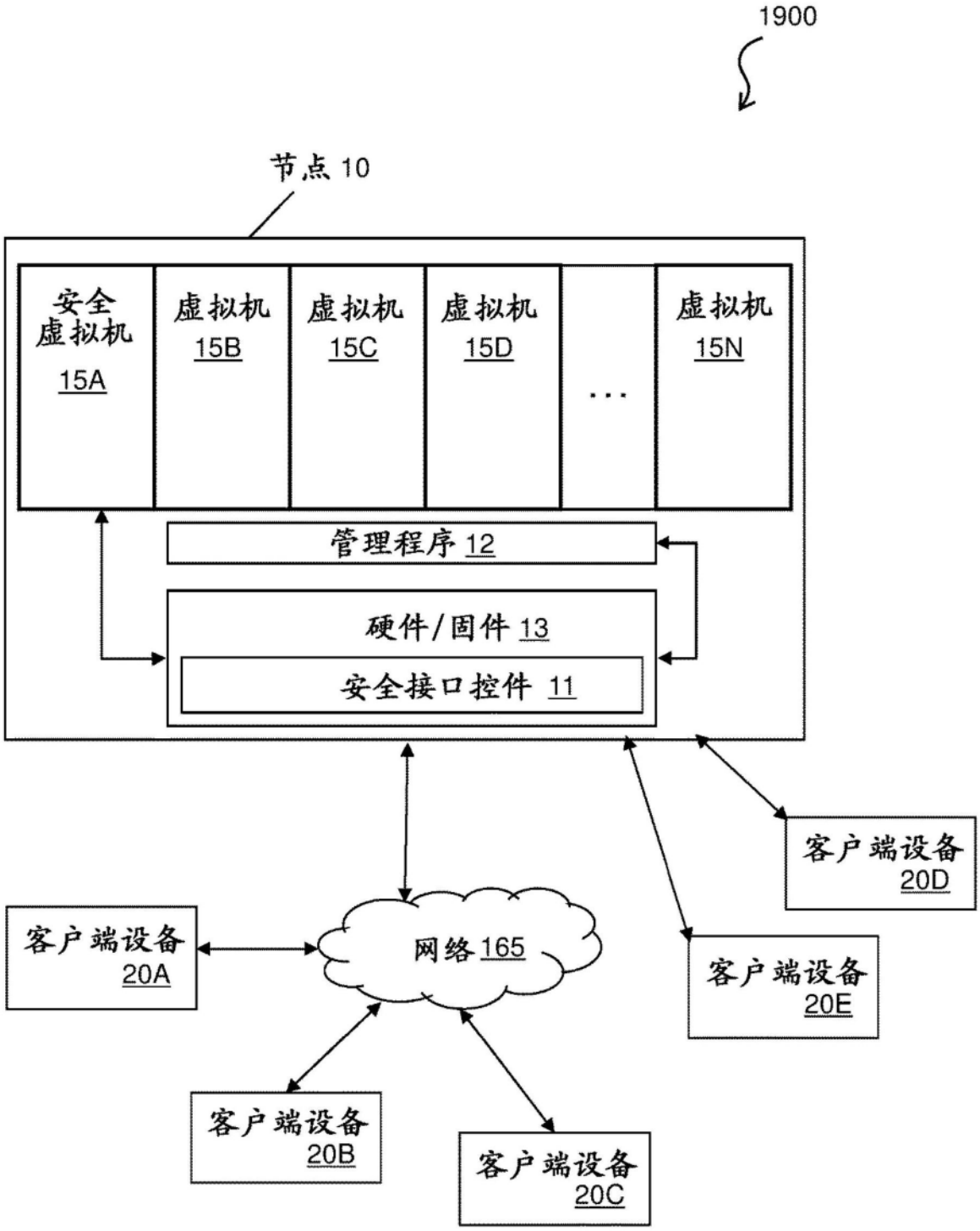

1900
节点 10
安全虚拟机 15A
虚拟机 15B
虚拟机 15C
虚拟机 15D
...
虚拟机 15N
管理程序 12
硬件/固件 13
安全接口控件 11
客户端设备 20D
客户端设备 20A
网络 165
客户端设备 20E
客户端设备 20B
客户端设备 20C

图19

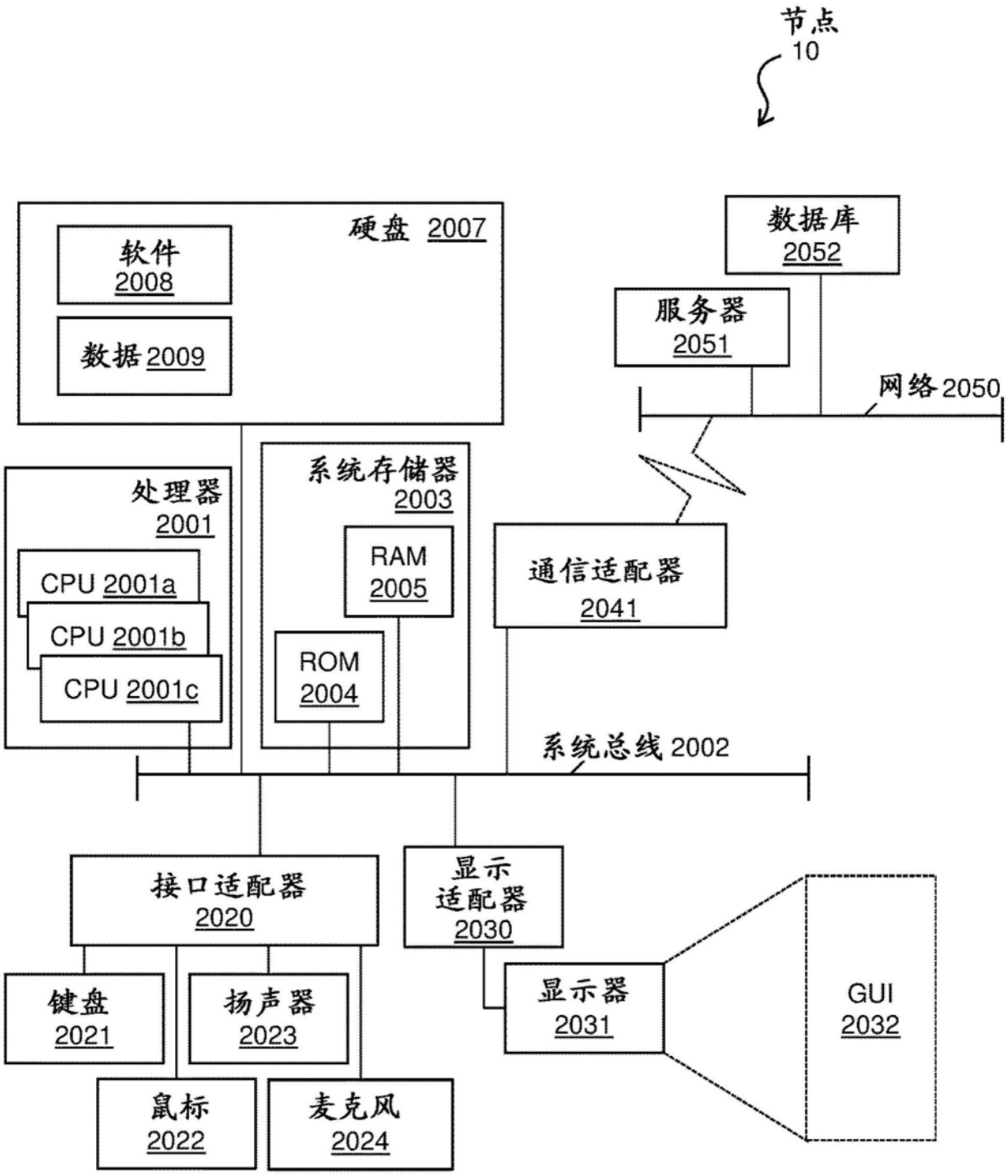

节点
10
硬盘 2007
软件
2008
数据 2009
数据库
2052
服务器
2051
网络 2050
处理器
2001
CPU 2001a
CPU 2001b
CPU 2001c
系统存储器
2003
RAM
2005
ROM
2004
通信适配器
2041
系统总线 2002
接口适配器
2020
显示
适配器
2030
键盘
2021
扬声器
2023
鼠标
2022
麦克风
2024
显示器
2031
GUI
2032

图20