(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113544644 B
(45)授权公告日 2025.06.03

(21)申请号 202080019507.5
(22)申请日 2020.03.02
(65)同一申请的已公布的文献号
申请公布号 CN 113544644 A
(43)申请公布日 2021.10.22
(30)优先权数据
16/296,306 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/EP2020/055469 2020.03.02
(87)PCT国际申请的公布数据
WO2020/182528 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 F·布萨巴 L·C·海勒 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 于静 刘薇

(51)Int.Cl.
G06F 9/455(2006.01)
G06F 21/78(2006.01)
(56)对比文件
CN 101520753 A,2009.09.02
CN 105431827 A,2016.03.23
审查员 刘栩宏

权利要求书3页 说明书23页 附图22页

(54)发明名称

跨多个安全域共享安全存储器

(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制处接收对存储器的安全页面的安全访问请求。安全接口控制可以检查与安全页面相关联的禁用虚拟地址比较状态。安全接口控制可以基于禁用虚拟地址比较状态被设置,禁用在访问安全页面时的虚拟地址检查,以支持从多个虚拟地址到至安全页面的相同绝对地址的映射,和/或支持使用绝对地址访问的、没有相关联的虚拟地址的安全页面。

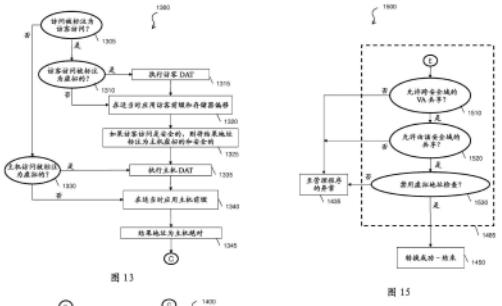

图13 图15

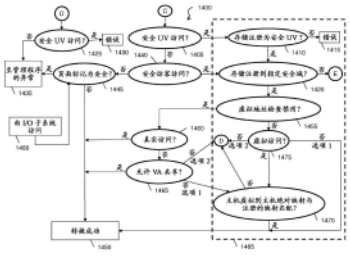

图14

CN 113544644 B

1.一种计算机实现的方法,包括:

在计算机系统的安全接口控制处接收对存储器的安全页面的安全访问请求;

由所述安全接口控制检查与所述安全页面相关联的禁用虚拟地址比较状态,其中,通过区安全表来存储和更新所述禁用虚拟地址比较状态,所述区安全表包括与所述安全页面相关联的安全域标识符、与所述安全页面相关联的虚拟地址映射数据以及所述禁用虚拟地址比较状态;

基于所述禁用虚拟地址比较状态被设置,由所述安全接口控制禁用在访问所述安全页面时的虚拟地址检查,以支持从多个虚拟地址到所述安全页面的相同绝对地址的映射;

由所述安全接口控制基于域标识符验证多个安全域中的安全域被授权访问共享页面;

确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,所述不安全主机被配置为针对能够访问所述安全页面的多个安全域中的任何安全域来管理所述多组动态地址转换表中的一组或多组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表;并且

基于检测到所述动态地址转换表的所述一组或多组中的变化来终止所述安全访问请求。

2.如权利要求1所述的方法,其中,将所述安全域的所述域标识符与被标识为允许共享的所述安全域的多个域标识符进行比较,以确认对访问所述共享页面的授权。

3.如权利要求1所述的方法,其中,所述安全接口控制包括固件、硬件、可信软件或固件、硬件和可信软件的组合,并且所述安全页面被分配给由管理程序或操作系统管理的安全虚拟机或安全容器。

4.一种计算机系统,包括:

存储器;

处理单元;以及

安全接口控制,所述安全接口控制被配置成用于执行多个操作,所述多个操作包括:

检查与来自在所述处理单元上执行的实体的对所述存储器的安全页面的安全访问请求相关联的禁用虚拟地址比较状态,其中,通过区安全表来存储和更新所述禁用虚拟地址比较状态,所述区安全表包括与所述安全页面相关联的安全域标识符、与所述安全页面相关联的虚拟地址映射数据以及所述禁用虚拟地址比较状态;

基于所述禁用虚拟地址比较状态被设置,禁用在访问所述安全页面时的虚拟地址检查,以支持从多个虚拟地址到所述安全页面的相同绝对地址的映射;

基于域标识符验证多个安全域中的安全域被授权访问共享页面;

确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,所述不安全主机被配置为针对能够访问所述安全页面的多个安全域中的任何安全域来管理所述多组动态地址转换表中的一组或多组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表;并且

基于检测到所述动态地址转换表的所述一组或多组中的变化来终止所述安全访问请求。

5.如权利要求4所述的系统,其中,将所述安全域的所述域标识符与被标识为允许共享的所述安全域的多个域标识符进行比较,以确认对访问所述共享页面的授权。

6.如权利要求4所述的系统,其中,所述安全接口控制包括固件、硬件、可信软件或固件、硬件和可信软件的组合,并且所述安全页面被分配给由管理程序或操作系统管理的安全虚拟机或安全容器。

7.一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制执行时使所述处理单元执行一种方法,所述方法包括:

检查与来自在所述处理单元上执行的实体的对存储器的安全页面的安全访问请求相关联的禁用虚拟地址比较状态,其中,通过区安全表来存储和更新所述禁用虚拟地址比较状态,所述区安全表包括与所述安全页面相关联的安全域标识符、与所述安全页面相关联的虚拟地址映射数据以及所述禁用虚拟地址比较状态;

基于所述禁用虚拟地址比较状态被设置,禁用在访问所述安全页面时的虚拟地址检查,以支持从多个虚拟地址到所述安全页面的相同绝对地址的映射;

基于域标识符验证多个安全域中的安全域被授权访问共享页面;

确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,所述不安全主机被配置为针对能够访问所述安全页面的多个安全域中的任何安全域来管理所述多组动态地址转换表中的一组或多组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表;并且

基于检测到所述动态地址转换表的所述一组或多组中的变化来终止所述安全访问请求。

8.如权利要求7所述的计算机程序产品,其中,将所述安全域的所述域标识符与被标识为允许共享的所述安全域的多个域标识符进行比较,以确认对访问所述共享页面的授权。

9.如权利要求7所述的计算机程序产品,其中,所述安全页面被分配给由管理程序或操作系统管理的安全虚拟机或安全容器。

10.一种计算机实现的方法,包括:

在计算机系统的安全接口控制处接收对存储器的安全页面的安全访问请求;

由所述安全接口控制检查与安全页面相关联的禁用虚拟地址比较状态,其中,通过区安全表来存储和更新所述禁用虚拟地址比较状态,所述区安全表包括与所述安全页面相关联的安全域标识符、与所述安全页面相关联的虚拟地址映射数据以及所述禁用虚拟地址比较状态;

基于作出所述安全访问请求的实体的授权状态以及所述禁用虚拟地址比较状态被设置,使能对没有指定虚拟地址的所述安全页面的绝对地址访问;

由所述安全接口控制基于域标识符验证多个安全域中的安全域被授权访问共享页面;

确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,所述不安全主机被配置为针对能够访问所述安全页面的多个安全域中的任何安全域来管理所述多组动态地址转换表中的一组或多组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表;并且

基于检测到所述动态地址转换表的所述一组或多组中的变化来终止所述安全访问请求。

11.如权利要求10所述的方法,其中,将所述安全域的所述域标识符与被标识为允许共

享的所述安全域的多个域标识符进行比较,以确认对访问所述共享页面的授权。

12.如权利要求10所述的方法,其中,所述安全接口控制包括固件、硬件或固件与硬件的组合,并且所述安全页面被分配给由管理程序或操作系统管理的安全容器或安全虚拟机。

13.一种计算机系统,包括:

存储器;

处理单元;以及

安全接口控制,所述安全接口控制被配置成用于执行多个操作,所述多个操作包括:

检查与来自在所述处理单元上执行的实体的对所述存储器的安全页面的安全访问请求相关联的禁用虚拟地址比较状态,其中,通过区安全表来存储和更新所述禁用虚拟地址比较状态,所述区安全表包括与所述安全页面相关联的安全域标识符、与所述安全页面相关联的虚拟地址映射数据以及所述禁用虚拟地址比较状态;

基于作出所述安全访问请求的实体的授权状态以及所述禁用虚拟地址比较状态被设置,使能对没有指定虚拟地址的所述安全页面的绝对地址访问;

控制基于域标识符验证多个安全域中的安全域被授权访问共享页面;

确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,所述不安全主机被配置为针对能够访问所述安全页面的多个安全域中的任何安全域来管理所述多组动态地址转换表中的一组或多组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表;并且

基于检测到所述动态地址转换表的所述一组或多组中的变化来终止所述安全访问请求。

14.如权利要求13所述的系统,其中,将所述安全域的所述域标识符与被标识为允许共享的所述安全域的多个域标识符进行比较,以确认对访问所述共享页面的授权。

跨多个安全域共享安全存储器

背景技术

[0001] 本发明总体上涉及计算机技术,并且更具体地涉及跨多个安全域共享安全存储器。

[0002] 云计算和云存储为用户提供在第三方数据中心中存储和处理他们的数据的能力。云计算促进快速且容易地向客户供应VM的能力,而不需要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变化的偏好或要求容易地扩展或收缩VM。通常,云计算提供商供应物理地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中的数据的安全性,特别是因为计算提供者通常在同一服务器上存储多于一个客户的数据。客户可能期望他们自己的代码/数据与云计算提供者的代码/数据之间的安全,以及他们自己的代码/数据与在提供者的站点处运行的其他VM的代码/数据之间的安全。此外,客户可能期望来自提供者的管理员的安全性以及防止来自机器上运行的其他代码的潜在安全漏洞。

[0003] 为了处理这样的敏感情况,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隔离。在实现云基础架构中虚拟化的广泛使用导致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(无论是其计算、存储或甚至联网硬件)之间的关系。这引入了虚拟化作为附加层,它本身必须被适当地配置、管理和安全。

[0004] 通常,在主机管理程序的控制下作为访客运行的VM依赖于该管理程序来透明地为该访客提供虚拟化服务。这些服务包括存储器管理、指令仿真和中断处理。

[0005] 在存储器管理的情况下,VM可以将其数据从盘移动(页面调入)以驻留在存储器中,并且VM还可以将其数据移回(页面调出)到盘。当页面驻留在存储器中时,VM(访客)使用动态地址转换(DAT)来将存储器中的页面从访客虚拟地址映射到访客绝对地址。此外,主机管理程序具有针对存储器中的访客页面的其自己的DAT映射(从主机虚拟地址到主机绝对地址),且其可独立地且对访客透明地将访客页面页面调入和调出存储器。通过主机DAT表,管理程序提供存储器隔离或在两个单独的访客VM之间共享访客存储器。主机还能够访问访客存储器,以在必要时代表访客模拟访客操作。

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制处接收对存储器的安全页面的安全访问请求。安全接口控制可以检查与安全页面相关联的禁用虚拟地址比较状态。基于禁用虚拟地址比较状态被设置,安全接口控制可在访问安全页面时禁用虚拟地址检查,以支持从多个虚拟地址到至安全页面的相同绝对地址的映射。优点可以包括跨多个安全域共享安全存储器。

[0007] 根据本发明的附加或替代实施例,安全接口控制可以基于域标识符来验证多个安全域中的安全域被授权访问共享页面。优点可以包括基于域标识符来约束共享。

[0008] 根据本发明的附加或替代实施例,可以将安全域的域标识符与被标识为允许共享的安全域的多个域标识符进行比较,以确认对访问共享页面的授权。优点可以包括限制对域标识符列表的成员的共享。

[0009] 根据本发明的附加或备选实施例,安全接口控制可以确认将虚拟地址映射到绝对地址的多组动态地址转换表未被不安全主机改变,该不安全主机被配置为针对能够访问安全页面的多个安全域中的任何安全域管理该多组动态地址转换表中的一个或多个组,其中,虚拟地址的每个表映射包括所述一组或多组动态地址转换表中的多个相关联的表。可以基于检测到一组或多组动态地址转换表中的变化来终止安全访问请求。优点可以包括确认不安全主机不修改用于访问安全页面的地址映射。

[0010] 根据本发明的附加或替代实施例,可以通过包括与安全页面相关联的安全域标识符、与安全页面相关联的虚拟地址映射数据以及禁用虚拟地址比较状态的区域安全表来存储和更新禁用虚拟地址比较状态。优点可以包括跟踪和配置每个安全域和/或存储器页面的选项。

[0011] 根据本发明的附加或替代实施例,安全接口控制可以是固件、硬件、可信软件或固件、硬件和可信软件的组合。安全页面可被分配给由管理程序或操作系统管理的安全虚拟机或安全容器。优点可以包括以对总体系统性能的低相关联的操作影响来实现安全接口控制。

[0012] 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制处接收对存储器的安全页面的安全访问请求。安全接口控制可以检查与安全页面相关联的禁用虚拟地址比较状态。安全接口控制可以基于做出安全访问请求的实体的授权状态和禁用虚拟地址比较状态被设置,使能对没有指定虚拟地址的安全页面的绝对地址访问。优点可包含支持用于共享安全页面的绝对地址存取。

[0013] 本发明的其他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。

[0014] 通过本公开的技术实现了附加特征和优点。本发明的其他实施例和方面在此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

[0015] 在说明书结论的权利要求书中特别指出并清楚地要求保护本文描述的独占权利的细节。从以下结合附图的详细描述中,本发明的实施例的前述和其他特征和优点是显而易见的,其中:

[0016] 图1描述了根据本发明的一个或多个实施例的区域安全表;

[0017] 图2描述了根据本发明的一个或多个实施例的用于执行DAT的虚拟和绝对地址空间;

[0018] 图3描绘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虚拟机(VM)的嵌套的多部分DAT;

[0019] 图4描绘了根据本发明的一个或多个实施例的安全访客存储的映射;

[0020] 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;

[0021] 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制存储器的系统示意图;

[0022] 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过程流程;

[0023] 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过程流程；

[0024] 图9描绘了根据本发明的一个或多个实施例的捐赠存储器操作的过程；

[0025] 图10描绘了根据本发明的一个或多个实施例的不安全管理程序页面到安全接口控制的安全页面的转换的过程流程；

[0026] 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制进行的安全存储访问的过程流程；

[0027] 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制和由硬件进行的访问标注的过程流程；

[0028] 图13描绘了根据本发明的一个或多个实施例的用于支持程序和安全接口控制的安全和不安全访问的转换的过程流程；

[0029] 图14描绘了根据本发明的一个或多个实施例的通过程序和通过安全接口控制进行安全存储保护的DAT的过程流程；

[0030] 图15描绘了根据本发明的一个或多个实施例的用于虚拟地址模式检查的过程流程；

[0031] 图16描绘了根据本发明一个或多个实施例的通过地址转换进行页面共享的框图；

[0032] 图17描绘了根据本发明一个或多个实施例的通过地址转换和页面复制进行页面共享的框图；

[0033] 图18描绘了根据本发明的一个或多个实施例的用于跨多个安全域共享安全存储器的过程流程；

[0034] 图19示出了根据本发明一个或多个实施例的云计算环境；

[0035] 图20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21描绘了根据本发明的一个或多个实施例的系统；并且

[0037] 图22描绘了根据本发明的一个或多个实施例的处理系统。

[0038] 本文所描绘的图是说明性的。在不背离本发明的精神的情况下，可以对本文所描述的图或操作进行许多变化。例如，这些动作可按不同次序执行，或动作可被添加、删除或修改。同样，术语“耦合”及其变体描述了在两个元件之间具有通信路径并且不暗示这些元件之间的在它们之间没有中间元件/连接的直接连接。所有这些变化被视为说明书的一部分。

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、轻量的安全接口控制以提供额外的安全性。

[0040] 在主机管理程序的控制下作为访客运行的虚拟机(VM)依赖于该管理程序来透明地为该访客提供虚拟化服务。这些服务可以应用于安全实体和另一不信任实体之间的传统上允许此其他实体访问安全资源的任何接口。如前所述，这些服务可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/或写入访客的前缀区域(低核)。如在此使用的术语“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(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。如本文中所使用的术语“管理程序”和“VM监测器(VMM)”是指管理并准许多个VM在同一主机上使用多个(并且有时是不同的)OS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(或开启)过程。在另一示例中,部署VM包括VM的激活(或开启)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访客,存在技术挑战,其中在管理程序和安全访客之间需要额外的安全性而不依赖于管理程序,使得管理程序不能访问来自VM的数据,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硬件机制以确保安全存储和不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。对于安全访客,在“不可信的”不安全管理程序与安全访客之间提供了额外的安全性。为了做到这一点,管理程序通常代表访客所做的许多功能需要被结合到机器中。在此描述了一种新的安全接口控制(在此也被称为“UV”),用于提供管理程序与安全访客之间的安全接口。术语安全接口控制和UV在本文中可互换使用。安全接口控制与硬件协作工作以提供该附加安全性。此外,较低层管理程序可以为该不可信管理程序提供虚拟化,并且如果在可信代码(例如,可信软件)中实现该较低层管理程序,则它也可以是安全接口控制的一部分。

[0043] 在一个示例中,安全接口控制在内部、安全和可信的硬件和/或固件中实现。该可信固件可以包括例如处理器毫代码(Millicode)或PR/SM逻辑分区代码。对于安全访客或实体,安全接口控制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。当安全访客积极地使用数据并且其驻留在主机存储中时,其在安全存储中保持“无危险(in the clear)”。安全访客存储可以由该单个安全访客访问——这由硬件严格地强制执行。即,该硬件防止任何不安全实体(包括管理程序或其他不安全访客)或不同的安全访客访问该数据。在该示例中,安全接口控制作为固件的最低级别的可信部分运行。最低级别或毫代码实际上是硬件的扩展,并且用于实现例如在来自IBM的zArchitecture®中定义的复杂指令和功能。毫代码能够访问存储的所有部分,其在安全执行的上下文中包括其自身的安全UV存储、不安全管理程序存储、安全访客存储和共享存储。这允许它提供安全访客或管理程序支持该访客所需的任何功能。安全接口控制还具有对硬件的直接访问,其允许硬件在由安全接口控制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,软件使用UV调用(UVC)指令来请求安全接口控制执行特定动作。例如,UVC指令可由管理程序使用以初始化安全接口控制、创建安全访客域(例如,安全访客配置)和在该安全配置内创建虚拟CPU。它也可以用于导入(解密并分配给安全访客域)和导出(加密并允许主机访问)安全访客页面,作为管理程序页面调入或页面调出操作的一部分。此外,安全访客具有定义与管理程序共享的存储、使得安全存储共享、以及使得共享存储安全的能力。

[0045] 类似于许多其他架构化指令,这些UVC命令可由机器固件执行。机器不进入安全接口控制模式,而是机器以其当前运行的模式执行安全接口控制功能。硬件维持固件和软件状态两者,因此没有上下文的切换以便处理这些操作。这种低开销允许软件、可信固件和硬件的不同层之间的紧密绑定协作,其方式为最小化和降低安全接口控制的复杂度,同时仍提供必要的安全级别。

[0046] 根据本发明的一个或多个实施例,在支持安全接口控制和硬件正确维护安全访客

和支持管理程序环境所需的控制块结构时,管理程序在初始化安全访客环境的同时向安全接口控制捐赠存储。因此,在准备1)初始化区域以运行安全访客)、2)创建安全访客域)和3)创建在每个域中运行的安全CPU时,管理程序发布查询UVC指令以确定捐赠所需的存储量等。一旦存储已经被捐赠,它就被标记为安全的并且被注册为属于安全接口控制;并且禁止任何不安全或安全访客实体的访问。保持这种情况,直到相关联的实体(例如,安全访客CPU、安全访客域或区域)被破坏为止。

[0047] 在一个示例中,用于支持区-专用UV控制块的UV存储的第一区段作为初始化UVC的一部分被捐献给安全接口控制,且驻留在本文中称为UV2存储的部分中。用于支持基础和可变安全-访客-配置控制块(对于每个安全访客域)的UV存储的第二和第三部分作为创建-安全-访客-配置UVC的一部分被捐献,并且分别驻留在UVS和UVV存储中。用于支持安全-CPU控制块的UV存储的第四和最后一段也驻留在UVS空间中,并且作为创建-安全-访客-CPU UVC的一部分被捐赠。当这些区域中的每一个被捐赠时,安全控制接口将它们标记为安全(以防止它们被任何不安全实体访问),并且还将它们在区安全表中注册为属于安全接口控制(以防止它们被任何安全访客实体访问)。为了在UV空间内提供进一步的隔离,UV2空间(其不与任何专用的安全访客域相关联)也用唯一的UV2安全域标注,而UVS和UVV空间两者都进一步用相关联的专用的安全访客域标注。在此示例中,UVV空间驻留在主机虚拟空间中,且因此可用主机虚拟到主机绝对映射来进一步识别。

[0048] 尽管安全接口控制能够访问所有存储(不安全存储、安全访客存储和UV存储),本发明的一个或多个实施例提供允许安全接口控制非常特定地访问UV存储的机制。使用在安全访客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。这保证了安全接口控制仅在预期和指定时访问UV存储;仅访问用于期望的指定的安全访客的安全访客存储;以及仅当指定时访问不安全存储器。即,安全接口控制可以非常明确地指定其意图访问的存储,使得硬件可以保证其确实访问该存储。此外,还可以指定其仅旨在访问与所指定的安全访客域相关联的UV存储。

[0049] 为了提供安全性,当管理程序透明地页面调入和调出安全访客数据时,与硬件一起工作的安全接口控制提供和保证数据的解密和加密。为了实现这一点,当页面调入和调出访客安全数据时,需要管理程序发布新的UVC。基于由安全接口控制在这些新UVC期间设置的控制,硬件将保证这些UVC确实由管理程序发布。

[0050] 在该新的安全环境中,每当管理程序页面调出安全页面时,需要从安全存储(导出)UVC发布新的转换。响应于此导出UVC,安全接口控制将1)指示页面被UV“锁定”,2)加密该页面,3)将页面设置为不安全,并且4)重置UV锁。一旦导出UVC完成,管理程序现在可以页面调出加密的访客页面。

[0051] 另外,每当管理程序正页面调入安全页面时,其必须发布到安全存储(导入)UVC的新转换。响应于此导入UVC,UV或安全接口控制将1)在硬件中将该页面标记为安全,2)指示该页面被UV“锁定”,3)解密该页面,4)设置对特定安全访客域的权限,以及5)重置UV锁。每当安全实体进行访问时,硬件在转换期间对该页面执行权限检查。这些检查包括:1)检查以验证该页面确实属于正尝试访问它的安全访客域;以及2)检查以确保当该页面已经驻留在访客存储器中时管理程序没有改变此页面的主机映射。一旦页面被标记为安全,硬件就防止管理程序或不安全访客VM访问任何安全页面。附加的转换步骤防止由另一安全VM访问并

且防止由管理程序重新映射。

[0052] 对于安全实体,诸如安全VM或容器,存储器的每个绝对页面通常被分配给一个安全VM(或容器)并且不允许被其他VM/容器或管理程序/OS访问或共享。在某些运行环境中,可以存在在不同安全VM/容器之间逻辑共享的公共安全存储器(例如,安全数据库或OS内核中的安全共享区域)。管理不同VM(或容器)的管理程序(或OS)可以为运行的VM(或容器)中的每一个分配不同的存储器地址空间,以实现所需的存储器隔离。每个运行VM(或容器)可以表现为具有其自己的地址空间,该地址空间对于任何其他运行VM(或容器)是唯一的。为了在这些VM之间共享公共存储,管理程序可以通过地址转换将来自不同运行VM的虚拟地址映射到相同的物理存储器中。对于安全VM/容器,管理程序/OS可能不是可信的,并且通常可以禁止将来自各种VM的不同虚拟地址映射到单个绝对地址。安全接口控制可以负责验证虚拟到物理地址的映射未被不安全管理程序/OS篡改。用于页面共享而没有重复映射的可能的变通方案可包括使用重复副本,一个副本被分配给每个运行的VM或容器。当共享公共安全数据库的复杂性被添加到管理副本镜像的复杂性时,该方法对于运行数千个VM或容器镜像的系统可能是不可行的。

[0053] 如上所述,安全接口控制尤其可以负责保证地址转换完整性。除了安全访客存储之外,可以存在从管理程序存储捐赠并且给予安全接口控制的存储器区域。这些区域仅可由安全接口控制访问。这些区域可以被维护和引用为绝对存储器,并且通常不经受动态地址转换。这些安全绝对页面可以不具有与其相关联的虚拟地址映射。本发明的实施例可以应用于运行安全容器或安全VM,并且允许在安全OS与安全容器之间或在管理程序与安全VM之间共享安全公共区域。如本文进一步描述的,还可在多个运行的安全容器/VM之间支持共享。

[0054] 现在转到图1,根据本发明的一个或多个实施例,总体上示出了用于区安全的表100。图1中所示的区安全表100由安全接口控制维护,并且由安全接口控制和硬件使用,来保证对由安全实体访问的任何页面的安全访问。区安全表100由主机绝对地址110索引。即,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。

[0055] 进一步地,如图1中所示,区安全表100包括安全域ID 120(标识与此页面相关联的安全域);UV位130(指示该页面被捐赠给安全接口控制并且由安全接口控制拥有);禁用地址比较(DA)位140(用于在某些情况下禁用主机地址对比较,诸如当定义为主机绝对的安全接口控制页面不具有相关联的主机虚拟地址时);共享(SH)位150(指示与不安全管理程序共享页面)和主机虚拟地址160(指示针对该主机绝对地址注册的主机虚拟地址,其被称为主机-地址对)。注意,主机-地址对指示主机绝对和相关联的、注册的主机虚拟地址。一旦由管理程序导入,主机-地址对表示该页面的映射,并且比较保证主机在访客使用该页面时不重新映射该页面。

[0056] 动态地址转换(DAT)用于将虚拟存储映射到真实存储。当访客VM在管理程序的控制下作为可分页面(pageable)访客运行时,访客使用DAT来管理驻留在其存储器中的页面。此外,当页面驻留在其存储器中时,主机独立地使用DAT来管理那些访客页面(连同其自己的页面)。管理程序使用DAT来提供不同VM之间的存储的隔离和/或共享以及防止对管理程序存储的访客访问。当访客以不安全模式运行时,管理程序能够访问所有访客的存储。

[0057] DAT使得能够将一个应用与另一应用隔离,同时仍允许它们共享公共资源。而且,它允许实现VM,这些VM可用于设计和测试OS的新版本以及应用程序的并发处理。虚拟地址标识在虚拟存储中的位置。地址空间是虚拟地址连同专用变换参数(包含DAT表)的连续序列,所述专用变换参数允许将每一虚拟地址转换成相关联的绝对地址,所述相关联的绝对地址以存储中的字节位置来标识所述地址。

[0058] DAT使用多表查找(例如,用于每个转换的一组DAT表)来将虚拟地址转换成相关联的绝对地址。该表结构通常由存储管理器定义和维护。此存储管理器例如通过页面调出一个页面以引入另一页面来在多个程序之间透明地共享绝对存储。当页面被页面调出时,存储管理器将例如在相关联的页面表中设置无效位。当程序尝试访问被页面调出的页面时,硬件将向存储管理器呈现通常被称为页面错误的程序中断。作为响应,存储管理器将页面调入所请求的页面并重置无效位。这都对程序透明地完成,并且允许存储管理器虚拟化存储并在各种不同用户之间共享存储。

[0059] 当虚拟地址被CPU用来访问主存储时,其首先通过DAT被转换成真实地址,然后通过前缀被转换成绝对地址。用于特定地址空间的最高层次表的指定(原点和长度)被称为地址-空间-控制元素(ASCE)并且定义相关联的地址空间。

[0060] 根据本发明的一个或多个实施例,图1的区安全表100中的DA位140可以与每个安全页面相关联,以禁用由安全接口控制为访问安全页面所进行的虚拟地址检查。DA位140可为在安全接口控制的控制下的字段。当安全页面被登记在区安全表中并被分配给安全域时,可适当地设置DA位140。当正在访问安全页面以确定是否允许访问时,DA位可用作由安全接口控制进行的安全检查的一部分。当DA位为零时,当正在对安全页面进行访问时由安全接口控制进行的安全检查的一部分将确保在没有安全接口控制的知识的情况下尚未修改用于安全页面的DAT转换表。一旦安全域被给予页面,就将该页面的主机虚拟地址160(与主机绝对地址组合以创建主机-地址对)连同相关联的安全域ID 120和与图1中所示的该安全页面相关联的其他属性一起注册在图1的区安全表100中。对于对该页面的每次访问,安全接口控制可以通过将访问虚拟/绝对主机地址对和访问安全域ID两者与先前注册的地址对和域ID进行比较来验证该访问。如果存在错误比较,则安全接口控制可以报告异常。由此,当DA=0时,仅一个主机虚拟地址可映射到任何给定主机绝对地址。

[0061] 如本发明的一个或多个实施例中所述,DA位标记在被设置时可允许许多主机虚拟地址到相同主机绝对地址的映射。DA位标记可在安全接口控制的控制下,并且可仅针对被授权与其他域共享页面的域和针对被标记为安全共用页面的主机虚拟页面来设置。因此,当DA=1时,可以存在跨不同安全域的唯一的或相同的一对一、虚拟至绝对地址映射,并且每个一对一映射可以由一个安全域拥有。还可以针对主机绝对页面设置DA位,所述主机绝对页面由管理程序捐赠给安全接口控制并且被定义为绝对地址(例如,其中未指定虚拟地址)。为了支持这两种使用,安全接口控制和/或其他系统组件可以忽略针对用DA=1标记的页面的虚拟地址检查。该标记可以与特定页面相关联并且不一定适用于整个安全域。另外,当该页面是安全页面时,该系统可验证仅经授权的容器/VM可访问该共享的安全页面。

[0062] 现在转到图2,根据本发明的一个或多个实施例,总体地示出了用于执行DAT的示例虚拟地址空间202和204以及绝对地址空间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)。虚拟页面A1.V 212a1、A2.V 212a2和A3.V 212a3在多表(段230和页面表232a、232b)查找中由存储管理器使用ASCE A 208映射到绝对页面A1.A 220a1、A2.A 220a2和A3.A 220a3。类似地,使用ASCE B 210在两表234和236查找中分别将虚拟页面B1.V 214b1和B2.V 214b2映射到绝对页面B1.A 222b1和B2.A 222b2。

[0063] 现在转到图3,根据本发明的一个或多个实施例,总体上示出了用于支持在管理程序下运行的VM的嵌套的多部分DAT转换的示例。在图3所示的示例中,访客A虚拟地址空间A 302(由访客ASCE(GASCE)A 304定义)和访客B虚拟地址空间B 306(由GASCEB 308定义)两者都驻留在共享主机(管理程序)虚拟地址空间325中。如图所示,属于访客A的虚拟页面A1.GV 310a1、A2.GV 310a2和A3.GV 310a3分别由访客A存储管理器使用GASCEA 304映射到访客绝对页面A1.HV 340a1、A2.HV 340a2和A3.HV 340a3;属于访客B的虚拟页面B1.GV 320b1和B2.GV 320b2分别由访客B存储管理器使用GASCEB 308独立地映射到访客绝对页面B1.HV 360b1和B2.HV 360b2。在此示例中,这些访客绝对页面直接映射到共享主机虚拟地址空间325中,且随后经历到主机绝对地址空间330的额外主机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。属于访客A的主机虚拟地址A2.HV 340a2和属于访客B的B2.HV 360b2两者都被映射到相同的主机绝对页面AB2.HA 380。这使得数据能够在这两个访客之间共享。在访客DAT转换期间,每个访客表地址被视为访客绝对地址,并且经历附加的嵌套主机DAT转换。

[0064] 本文所述的本发明的实施例提供安全访客和UV存储保护。禁止不安全访客和管理程序访问安全存储。管理程序规定对于给定的驻留安全访客页面,发生以下操作。相关联的主机绝对地址仅通过单个管理程序(主机)DAT映射是可访问的。即,存在映射到分配给安全访客的任何给定主机绝对地址的单个主机虚拟地址。与给定安全访客页面相关联的管理程序DAT映射(主机虚拟到主机绝对)在它被页面调入时不改变。针对单个安全访客映射与安全访客页面相关联的主机绝对页面。

[0065] 根据本发明的一个或多个实施例,安全访客之间的存储共享也被禁止。在安全访客的控制下,在单个安全访客与管理程序之间共享存储。UV存储是安全存储,并且可由安全接口控制而非访客/主机访问。存储由管理程序分配给安全接口控制。根据本发明的一个或多个实施例,硬件和安全接口控制禁止对这些规则的任何尝试违反。

[0066] 现在转到图4,根据本发明的一个或多个实施例总体上示出了安全访客存储的映射的示例。图4类似于图3,除了图4的示例不允许在安全访客A和安全访客B之间共享存储。在图3的不安全示例中,属于访客A的主机虚拟地址A2.HV 340a2和属于访客B的B2.HV 360b2两者被映射到相同的主机绝对页面AB2.HA 380。在图4的安全访客存储示例中,属于访客A的主机虚拟地址A2.HV 340a2映射到主机绝对地址A2.HA 490a,而属于访客B的B2.HV 360b2映射到其自己的B2.HA 490b。在这个示例中,在安全访客之间不存在共享。

[0067] 当安全访客页面驻留在盘上时,其被加密。当管理程序页面调入安全访客页面时,其发布UV调用(UVC),该UV调用使得安全接口控制将该页面标记为安全(除非共享)、解密该页面(除非共享)并且将该页面(在区安全表中)注册为属于适当的安全访客(例如,访客A)。此外,其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面(称为主机-地址对)。如果管理程序未能发布正确的UVC,则其在尝试访问安全访客页面时接收异常。当

管理程序页面调出访客页面时,发布类似的UVC,该UVC加密访客页面(除非共享)、将访客页面标记为不安全并且将其在区安全表中注册为不安全。

[0068] 在具有五个给定主机绝对页面K、P、L、M和N的示例中,主机绝对页面中的每一个在管理程序将它们页面调入时被安全接口控制标记为安全的。这防止不安全访客和管理程序访问它们。当被管理程序页面调入时,主机绝对页面K、P和M被注册为属于访客A;当被管理程序页面调入时,主机绝对页面L和N被注册为属于访客B。共享页面(在单个安全访客和管理程序之间共享的页面)在分页面期间不被加密或解密。它们在区安全表中未被标记为安全(允许由管理程序访问),而是以单个安全访客域注册。

[0069] 根据本发明的一个或多个实施例,当不安全访客或管理程序试图访问安全访客所拥有的页面时,管理程序接收安全存储访问(PIC3D)异常。不需要额外的转换步骤来确定这一点。

[0070] 根据一个或多个实施例,当安全实体尝试访问页面时,硬件执行验证存储确实属于该特定安全访客的附加转换检查。如果不是,则向管理程序呈现不安全访问(PIC3E)异常。此外,如果被转换的主机虚拟地址与来自区安全表中的注册的主机-地址对的主机虚拟地址不匹配,则识别安全存储违反('3F' x)异常。为了实现与管理程序的共享,只要转换检查允许访问,安全访客就可以访问未被标记为安全的存储。

[0071] 现在转向图5,根据本发明的一个或多个实施例,总体上示出DAT操作的系统示意图500。系统示意图500包括主机主要虚拟地址空间510和主机归属(home)虚拟地址空间520,页面从这里被转换(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对主机绝对存储的共享,并且还示出了不仅在两个访客之间而且另外与主机本身之间那些主机虚拟地址之一的共享。就这一点而言,主机主要虚拟地址空间510和主机归属虚拟地址空间520是两个主机虚拟地址空间的示例,这两个主机虚拟地址空间中的每一者分别由单独的ASCE、主机主要ASCE(HPASCE)591和主机归属ASCE(HHASCE)592来寻址。注意,所有安全接口控制存储(虚拟的和真实的)由管理程序捐赠并被标记为安全。一旦被捐赠,只要相关联的安全实体存在,安全接口控制存储就可仅由安全接口控制访问。

[0072] 如图所示,主机主要虚拟地址空间510包括访客A绝对页面A1.HV、访客A绝对页面A2.HV、访客B绝对页面B1.HV和主机虚拟页面H3.HV。主机归属虚拟地址空间520包括安全-接口-控制虚拟页面U1.HV、主机虚拟页面H1.HV和主机虚拟页面H2.HV。

[0073] 根据本发明的一个或多个实施例,在本文所描述的区安全表中,将所有安全访客(例如,安全访客A和安全访客B)存储注册为属于安全访客配置,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,在主机主要虚拟空间中映射所有安全访客存储。此外,所有安全接口控制存储也在区安全表中被注册为属于安全接口控制,并且可以基于相关联的安全访客域在区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真实存储不具有相关联的主机虚拟映射,并且区安全表中的DA位(其指示虚拟地址比较被禁用)被设置成指示这一点。主机存储被标记为不安全,并且还在区安全表中被注册为不安全。

[0074] 因此,在“访客绝对=主机虚拟”的情况下,管理程序(主机)主要DAT表(由HPASCE

591定义)如下转换主机主要虚拟地址空间510的页面:访客A绝对页面A1.HV被映射到属于安全访客A的主机绝对A1.HA;访客A绝对页面A2.HV被映射到属于安全访客A的主机绝对页面A2.HA;访客B绝对页面B1.HV被映射到属于安全访客B的主机绝对页面B1.HA;并且主机虚拟页面H3.HV被映射到主机绝对页面H3.HA不安全主机(并且不存在主机-地址对,因为它是不安全的)。进一步,(由HHASCE 592定义的)管理程序(主机)归属DAT表如下转换主机归属虚拟地址空间520的页面:安全接口控制虚拟页面U1.HV被映射到被定义为安全UV虚拟的主机绝对页面U1.HA;主机虚拟页面H1.HV被映射到被定义为不安全的主机绝对页面H1.HA;并且主机虚拟页面H2.HV被映射到被定义为不安全的主机绝对页面H2.HA。不存在与H1.HA或H2.HA相关联的主机-地址对,因为它们是不安全的。

[0075] 在操作中,如果安全访客尝试访问分配给安全接口控制的安全页面,则硬件将安全存储违反('3F'X)异常呈现给管理程序。如果不安全访客或管理程序尝试访问任何安全页面(包括分配给安全接口控制的那些页面),则硬件将安全存储访问('3D'X)异常呈现给管理程序。可替代地,可以为对安全接口控制空间做出的尝试访问呈现错误条件。如果硬件在安全接口控制访问上检测到安全分配中的失配(例如,存储在区安全表中被注册为属于安全访客而不是属于安全接口控制,或者在与所注册的对一起使用的主机-地址对中存在失配),则呈现检查。

[0076] 换言之,主机主要虚拟地址空间510包括主机虚拟页面A1.HV和A2.HV(属于安全访客A)以及B1.HV(属于安全访客B),它们分别映射到主机绝对A1.HA、A2.HA以及B1.HA。此外,主机主要虚拟地址空间510包括主机(管理程序)页面H3.HV,其映射到主机绝对H3.HA。主机归属虚拟空间520包括映射到主机绝对页面H1.HA和H2.HA的两个主机虚拟页面H1.HV和H2.HV。主机主要虚拟地址空间510和主机归属虚拟地址空间520两者映射到单个主机绝对530中。属于安全访客A和安全访客B的存储页面被标记为安全的,并且利用其安全域和相关联的主机虚拟地址注册在图1所示的区安全表100中。另一方面,主机存储被标记为不安全。当管理程序定义这些安全访客时,它必须将主机存储捐献给安全接口控制,以用于支持这些安全访客所需的安全控制块。该存储可以在主机绝对或主机虚拟空间中定义,并且在一个例子中,具体地,在主机归属虚拟空间中定义。返回到图5,主机绝对页面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-控制存储。因此,这些页面被标记为安全的,并且在图1所示的区安全表100中注册为属于安全接口控制并且具有相关联的安全域。因为页面被定义为主机绝对地址,所以不存在相关联的主机虚拟地址,所以在区安全表100中设置DA位。

[0077] 在转换之后,可在图6中找到管理程序(主机)绝对地址空间530的示例。图6是根据本发明的一个或多个实施例描绘关于安全接口控制存储的系统示意图600。系统示意图600示出管理程序(主机)绝对地址空间630,其包括主机绝对页面A2.HA安全访客A(用于A2.HV);主机绝对页面B1.HA安全访客B(用于B1.HV);主机绝对页面H1.HA不安全(主机);主机绝对页面H2.HA不安全(主机);主机绝对页面U3.HA安全UV真实(无HV映射);主机绝对页面U1.HA安全UV虚拟(用于U1.HV);以及主机绝对页面A1.HA安全访客A(用于A1.HV)。

[0078] 现在转到图7,根据本发明的一个或多个实施例总体上示出了用于导入操作的过程流程700。当安全访客访问由管理程序页面调出的页面时,发生诸如过程流程700中所示的事件序列,以便安全地将该页面带回。过程流程700在框705开始,其中安全访客访问访客

虚拟页面。因为该页面例如无效,所以硬件向管理程序呈现由程序中断代码11(PIC 11)指示的主机页面错误

[0079] (参见框715)。管理程序进而识别该访客页面的可用的、不安全主机绝对页面(参见框720),并将加密的访客页面页面调入到所识别的主机绝对页面(参见框725)。

[0080] 在框730处,然后将主机绝对页面映射到适当的(基于主机虚拟地址)主机DAT表中。在框735处,管理程序主机然后重新调度安全访客。在框740处,安全访客重新访问访客安全页面。页面错误不再存在,但是由于这是安全访客访问并且页面在图1的区安全表100中未被标记为安全,所以在框745处,硬件向管理程序呈现不安全存储异常(PIC3E)。此PIC3E防止访客对此安全页面的访问,直到已发布必要的导入为止。接下来,过程流程700前进至“A”,其连接至图8。

[0081] 现在转到图8,根据本发明的一个或多个实施例总体上示出了用于执行导入操作的过程流程800。响应于PIC3E,表现良好的管理程序(例如,以预期方式无错误地执行)将发布导入UVC(参见框805)。注意,此时,要导入的页面被标记为不安全,并且仅可由管理程序、其他不安全实体和安全接口控制来访问。它不能被安全访客访问。

[0082] 作为导入UVC的一部分,充当安全接口控制的可信固件进行检查以查看此页面是否已经由安全接口控制锁定(参见决策框810)。如果是,则过程流程800前进到框820。在框820处,“繁忙”返回代码被返回至管理程序,该管理程序将作为响应而延迟(参见框825)并且重新发布导入UVC(过程流程800返回至框805)。如果页面尚未被锁定,则过程流程800前进到决策框822。

[0083] 在决策框822处,安全接口控制进行检查以查看该页面是否是与不安全管理程序共享的页面。如果它被共享(过程流程800前进到决策框824),则安全接口控制将主机绝对地址与相关联的安全访客域、主机虚拟地址一起注册在区安全表中并作为共享。该页面保持标记为不安全。这完成了导入UVC,并且页面现在可用于由访客访问。处理继续进行,管理程序重新分派访客(框830)并且安全访客成功访问页面(框835)。

[0084] 如果要导入的主机虚拟页面不与管理程序共享(过程流程800前进到框840),则安全接口控制将把该页面标记为安全,使得管理程序不再能够访问该页面。在框845处,安全接口控制锁定所述页面,使得没有其他UVC可修改页面状态。一旦锁被设置(在框850),安全接口控制将验证访客页面的内容在其被加密时未改变。如果它们确实改变,则错误返回代码被返回到管理程序,否则,安全接口控制将解密安全页面。

[0085] 在框855处,安全接口控制解锁页面,允许由其他UVC访问,将页面在区安全表中注册为安全的,并与适当的访客域和主机虚拟地址相关联,以完成主机-地址HV->HA对。这允许访客访问并完成UVC。

[0086] 现在转到图9,根据本发明的一个或多个实施例,总体上示出了关于捐赠的存储器操作的过程流程900。过程流程900在框905处开始,其中管理程序向安全接口控制发布查询UVC。在框910处,安全接口控制返回数据(例如,查询UVC)。此数据可以包括所需的基础区-专用主机-绝对存储的量;所需的基础安全-访客-域-专用主机-绝对存储的量;每MB所需的可变安全-访客-域-专用主机-虚拟存储的量;和/或所需的基础安全-访客-CPU-专用主机-绝对存储的量。

[0087] 在框915处,管理程序保留基础主机-绝对区-专用存储(例如,基于由查询UVC返回

的大小)。在框920,管理程序向安全接口控制发布初始化。就这一点而言,管理程序可以发布初始化UVC,该初始化UVC为整个区的安全访客配置之间协调所需的UV控制块提供所捐赠的存储。初始化UVC指定基础区-专用存储来源。

[0088] 在框925处,安全接口控制通过将所捐赠的存储注册到UV并标记为安全来实施初始化(例如,初始化UVC)。对于初始化UVC,安全接口控制可以将捐赠的存储标记为安全;为区安全表分配该捐赠的存储中的一些;以及在区安全表中以唯一的安全域注册所捐赠的存储供UV使用,但是没有相关联的安全-访客-域,并且不具有相关联的主机-虚拟地址对。

[0089] 在框930,管理程序保留存储(例如,基础和可变安全-访客-域-专用存储)。例如,管理程序保留基础和可变(例如,基于安全-访客-域存储的大小)安全-访客-域-专用存储(例如,由查询UVC返回的大小)。在框935,管理程序向安全接口控制发布创建配置。就这一点而言,管理程序可以发布创建-安全-访客-配置UVC,其指定基础和可变安全-访客-域-专用存储来源。进一步,创建-安全-访客-配置UVC为支持该安全访客配置所需的UV控制块提供所捐赠的存储。

[0090] 在框940,安全接口控制实施创建配置(例如,创建-安全-访客-配置UVC)。对于创建-安全-访客-配置UVC,安全接口控制可以将捐赠的存储标记为安全;将该捐赠的存储注册在区安全表中供UV使用;并且将该捐赠的存储以相关联的安全-访客-域注册。捐赠的基础(主机-绝对)存储被注册为不具有相关联的主机-虚拟地址对。捐赠的可变(主机-虚拟)存储以相关联的主机-虚拟地址对被注册。

[0091] 在框945,管理程序保留基础安全-访客-CPU-专用存储(例如,由查询-UV返回的大小)。在框950,管理程序指定存储来源。例如,管理程序向UV发布指定基础安全-访客-CPU专用存储来源的创建-安全-访客-CPU。在框955,安全接口控制实施创建-CPU(例如,创建-安全-访客-CPU UVC)。对于创建-安全-访客-CPU UVC,安全接口控制可以将捐赠的存储标记为安全,并且在区安全表中注册捐赠的存储以供UV使用,但是不具有相关联的安全-访客-域并且不具有相关联的主机-虚拟地址对。

[0092] 现在转到图10,根据本发明的一个或多个实施例,总体示出关于不安全管理程序页面到安全接口控制的安全页面的转变的处理流程1000。在过程流程1000中,示出了三个管理程序页面(例如,不安全管理程序页面A、不安全管理程序页面B和不安全管理程序页面C)。

[0093] 管理程序(不安全)页面A、B和C可以由不安全实体(包括管理程序)访问。进一步,管理程序(不安全)页面A、B和C被标记为不安全(NS),连同在区安全表(例如,图1中所示的区安全表100)中被注册为不安全和非共享。在箭头1005处,发布初始化UVC,其将访客页面A转变到与整个区相关联的安全接口控制真实存储页面1010(UV2)。安全接口控制真实存储1010可以被标记为安全,连同在区安全表(例如,图1中所示的区安全表100)中注册为UV,没有安全访客域并且没有管理程序到主机绝对(HV->HA)映射。而是其以唯一UV2安全域注册,且将DA位设定为1。注意,安全接口控制真实存储1010可以由安全接口控制作为真实访问。

[0094] 在箭头1025处,从管理程序(不安全)页面B发布创建-SG-配置或创建-SG-CPU UVC,其将该页面过渡到与安全访客域相关联的安全接口控制真实存储1030(UVS)。安全接口控制真实存储1030可以被标记为安全,并且在区安全表(例如,图1中所示的区安全表100)中注册为具有相关联的安全访客域的UV,并且没有管理程序到主机绝对(HV->HA)映射

(即,DA位

[0095] =1)。注意,安全接口控制真实存储1010可以代表安全访客域由安全接口控制作为真实访问。

[0096] 在箭头1045处,从管理程序(不安全)页面C发布创建-SG-配置UVC,其将该页面转换到与安全访客域(UVV)相关联的安全接口控制虚拟存储1050。安全接口控制虚拟存储1050可以被标记为安全,并且在区安全表(例如,图1中所示的区安全表100)中注册为UV,具有安全访客域和管理程序到主机绝对(HV->HA)映射。注意,安全接口控制虚拟存储1050可以代表安全访客域作为UV虚拟被访问。

[0097] 现在转到图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制所进行的安全存储访问的过程流程1100。这表示安全接口控制将要访问访客存储或安全接口控制存储并且必须正确地标记该访问以便允许硬件验证该访问的安全性的情形。1100描述由安全接口控制标注的存储访问。过程流程1100在框1110开始,其中安全接口控制确定其是否正在访问安全接口控制存储。

[0098] 如果这不是对安全接口控制存储的访问,那么过程流程1100前进到决策框1112(如由“否”箭头所示)。在决策框1112处,安全接口控制确定其是否正在对安全访客存储进行访问。如果这不是对安全访客存储的访问,则过程流程1100前进至“B”(其连接至图12的过程流程1200),其将使用默认设置用于不安全访问。如果这是对安全访客存储的访问,那么过程流程1100前进到决策框1113,其中安全接口控制确定是否正在使用默认安全访客域。如果是,则过程流程1100继续前进至“B”(其连接至图12的过程流程1200),其将使用默认设置用于安全访客访问。如果否,则过程流程1100进行到框1114。在框1114处,将合适的安全访客域加载到SG-安全-域寄存器中(并且前进至“B”,其连接至图12的过程流程1200)。

[0099] 如果这是对安全接口控制存储的访问,那么过程流程1100进行到方框1120(如由“是”箭头所示)。在框1120处,将访问标注为安全UV(例如,使用UV-安全-域寄存器)。

[0100] 过程流程1100接着前进到决策框1130,其中安全接口控制确定这是否是对UVV空间(例如,SG-配置变量表)的访问。如果其是对UVV空间的访问,则过程流程1100进行到框1134(如由“是”箭头所示)。在框1134,将访问标注为虚拟的。在框1136处,将可应用的安全访客域加载到UV-安全-域寄存器中。在框1138,DAT转换和访问存储准备开始。返回到决策框1130,如果这不是对UVV空间的访问,那么过程流程1100前进到框1140(如由“否”箭头所示)。在框1140,将标注访问为真实的。

[0101] 在决策框1150处,安全接口控制确定这是否是对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,则过程流程1100前进到框1136(如由“是”箭头所示)。如果这不是对UVS空间的访问,那么过程流程1100前进到框1170(如由“否”箭头所示)。此访问随后将为对UV2空间(例如,区安全表)的访问。在框1170处,将唯一UV2安全域加载到UV-安全-域寄存器中。

[0102] 图12描绘了根据本发明的一个或多个实施例的过程流程1200。当一个访客被分派时,SIE进入固件可以向硬件指示一个访客正在运行(例如,访客模式活动)并且可以指示该访客是否是安全的。如果访客是安全的,相关联的安全访客域可以被加载到硬件中(例如,在SG安全域寄存器中)。当程序访问存储时,硬件可以基于程序在访问时的当前状态来标注访问。图12示出了过程流程1200中的这个过程的示例。在框1205处,硬件可以确定机器当前

是否以访客模式运行,并且如果不是,则可以在框1210处将访问标注为主机访问,并且在框1215处标注为不安全访问。如果在框1205机器以访客模式运行,则在框1220访问可被标注为访客访问,并且在框1225进一步确定当前访客是否是安全访客。如果访客不安全,则在框1215,访问可被标注为不安全。如果访客是安全的,硬件可在框1230处将访客标注为安全的,这可将安全访客与在分派安全访客时加载的SG-安全-域寄存器相关联。对于不安全和安全访客两者,可以在框1235检查DAT状态。如果DAT关闭,则在框1240,访问可被标注为真实的。如果DAT开启,则在框1245,访问可被标注为虚拟的。一旦访问在框1240被标注为真实而DAT关闭,或者在框1245被标注为虚拟而DAT开启,硬件就准备好在框1250开始转换和访问存储,如图13中进一步描述的。

[0103] 图13描绘了根据本发明的一个或多个实施例的由硬件完成以支持过程流程1300中的安全访问和不安全访问两者的转换的示例。在框1305处,硬件可以确定访问是否被标注为访客转换,并且如果是的话,并且在框1310处访问是虚拟的,则可以在框1315处执行访客DAT。在访客DAT转换期间,可以有用于访客DAT表的嵌套中间获取。如果原始转换被标注为安全,则表获取可被标注为访客真实的和安全的。表获取还可以跟随过程流程1300的转换过程。在对于在框1315被标注为访客虚拟的访问和对于在框1310被标注为访客真实的任何访问(虚拟=否)执行访客DAT之后,可以在框1320应用访客前缀和访客存储器偏移。在访客转换过程完成时,在框1325处,如果原始访客转换被标注为安全,则结果地址可被标注为主机虚拟的和安全的。对于被标注为主机虚拟的任何访问,过程1300可以继续。如果在框1305原始访问是主机访问,(访客=否)并且在框1330是虚拟的,则在框1335可以执行主机DAT。在框1335处,可将主机表获取标记为不安全。在框1335处执行主机DAT之后,或如果在框1330处将原始主机访问标注为真实(虚拟=否),则可在框1340处应用主机前缀。在框1345处,结果地址可为主机绝对地址。

[0104] 图14描述了根据本发明的一个或多个实施例的可以由硬件执行的过程流程1400中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处标识了安全UV访问,则硬件可以在框1410处验证存储是否被注册为安全UV存储,并且如果否,则在框1415处呈现错误。当访问UV存储时,安全接口控制可以进行安全UV访问。如果在框1410处存储被注册为安全UV存储,则除了UV-安全-域寄存器(在进行安全UV访问之前由安全接口控制设置)可以被用作框1420处的域检查的指定安全域(其中处理继续)之外,保护检查可以如针对任何安全访问所执行的那样继续。另外,在框1425处检测到的针对UV访问的任何违背(进入点D)可以在框1430处呈现为错误,而不是如在框1425处针对安全访客违背所做的那样在框1435处向管理程序呈现异常(安全-UV=否)。

[0105] 对于在框1405处未被标注为安全-UV访问的访问,硬件在框1440处确定该访问是否是安全访客访问,并且如果不是,并且如果在框1445处页面被标记为安全,则在框1435处可以向管理程序呈现异常。否则,如果在框1440处访问不是安全访客访问并且在框1445处页面未被标记为安全,则在框1450处转换成功。

[0106] 如果在框1440处访问是安全访客访问或者在框1410处安全UV访问是对注册为安全UV存储的存储,则在框1420处硬件可以检查以确保存储被注册到与访问相关联的安全实体。如果这是安全-UV访问,则可以从UV-安全-域寄存器(由安全接口控制基于正被访问的安全-UV存储加载)获得指定的安全域,并且对于安全-访客访问,从SG-安全-域寄存器(当

调度安全实体时加载)获得指定的安全域。如果在框1420正被访问的存储未被注册到指定的安全域,则如图15中关于区安全表接口1485所描绘的那样执行子过程1500。

[0107] 在子过程1500中,在框1510,执行检查以确定是否允许跨安全域共享虚拟地址。可以基于与区或分区相关联的寄存器值来执行检查。在框1520处,如果允许跨安全域共享并且允许由当前安全域共享,则可以在框1530处执行对虚拟地址检查是否被禁用的检查。对当前安全域是否允许共享的检查可以通过在区安全表中针对安全域的寄存器访问或表查找来执行,这可以特定于此主机绝对页面。对于虚拟地址检查是否被禁用的检查可以通过检查禁用虚拟地址比较状态(DA)来执行,其中,标记的页面(例如,DA=1)导致禁用虚拟地址检查。如果在框1510处不允许跨安全域的虚拟地址共享、在框1520处不允许由当前安全域共享、或者在框1530处不禁用虚拟地址检查(例如,DA=0),则可以在框1435处向管理程序呈现异常。或者,如果在框1520虚拟地址检查未被禁用(DA=0),则安全接口控制可检查用于此主机绝对页面和安全访客域的注册主机虚拟地址,以及,如果访问主机-地址对与注册的主机-地址对匹配,则在框1450转换将成功完成,并且如果对不匹配,则异常将被呈现给管理程序1435。否则,如果在框1530禁用虚拟地址检查,则子过程1500可以在框1450以成功的转换结束。

[0108] 返回至图14的过程1400,对于在框1420处注册到指定安全域的、在框1440和框1410处对存储的安全访问,如果虚拟地址检查被禁用,即,在框1455处DA位=1并且在框1460处访问是真实的,则在框1450完成转换。然而,如果在框1455处DA位=1但是在框1460处访问是虚拟的(真实=

[0109] 否),则如果在框1465处允许虚拟地址(VA)共享,则在框1450处转换也完成。然而,如果在框1455处DA位=1,在框1460处访问是虚拟的(真实=否)并且在框1465处不允许VA共享,则可发生两个选项之一。选项1继续在框1470处进行主机虚拟到主机绝对匹配。选项2是对于框1425处的安全-UV访问,在框1430处给出错误,并且对于框1425处的安全-访客访问(安全-UV=否),在框1435处向管理程序呈现异常。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匹配针对该主机绝对地址注册的映射。如果是,则在框1450转换成功完成。如果在框1470映射不匹配,则对于在框1425的安全-UV访问,在框1430给出错误,并且对于在框1425的安全-访客访问(安全-UV=

[0110] 否),在框1435向管理程序呈现异常。如果DA位=0并且在框1475处访问是真实访问(虚拟=否),则对于在框1425的安全-UV访问,在框1430给出错误,并且对于在框1425的安全-访客访问(安全-UV=否),在框1435向管理程序呈现异常(选项2);可替代地,转换可在框1450成功完成(选项1)。在框1480处由I/O子系统进行的任何访问可检查以查看在框1445处页面是否被标记为安全,并且如果页面是安全的,则在框1435处可向管理程序呈现异常;如果页面未被标记为安全,则在框1450处转换成功。

[0111] 可以通过区安全表接口1485来共同管理存储注册和映射的不同检查。例如,框1410、1420、1455、1470和1475可以与关联于相同区的区安全表对接以管理不同访问。类似地,图15的框1510、1520和1530可以与关联于相同区的区安全表对接以管理不同访问。

[0112] 作为进一步的示例,图16和17示出了映射过程选项。如前所述,来自安全域或安全接口控制的每个存储器访问可以用安全域、主机地址对和DA标记来标注。主机-地址对可以

包括虚拟地址和相关联的绝对地址。每个实体(例如,安全容器或VM)可以具有其自己的安全域ID。在以下示例中,定义了多个术语。V＝存储器访问的虚拟地址。A＝存储器访问的绝对地址。D＝安全域ID。DA＝禁用虚拟地址比较位。对于正常操作的安全域,所有存储器访问可以在页面调入时进行注册并且在访问时进行验证。作为示例,安全域X可以拥有存储器中的三个页面,具有以下注册的主机-地址对和相关信息,对于一个页面为(V1x,A1x),DA＝0(无共享),D＝X;对于另一页面为(V2x,A2x),DA＝0(无共享),D＝X;以及对于第三页面为(V3x,A3x),DA＝0(无共享),D＝X。除非例如通过图1的区安全表100在主机-地址对和安全访客域上发生匹配,否则不允许对这些页面的访问。另一个安全域Y也可以正在运行并且拥有存储器中的两个页面,这两个页面注册有两个主机地址对和相关信息,对于一个页面为(V1y,A1y),DA＝0(无共享),D＝Y;以及对于另一页面为(V2y,A2y),DA＝0(无共享),D＝Y。除非用于访问的主机-地址对和安全访客域匹配为该页面注册的那些访客-地址对和安全访客域,否则不允许对这些页面的访问。只要对应的绝对地址是唯一的,安全域X和Y都可以具有以相同虚拟地址值映射的页面。例如,由于对于所有这些页面DA＝0,所以V1x可以等于V2y,但是A1x必须不等于A2x、A3x、A1y或A2y中的任何一个。为了允许共享以虚拟地址注册的绝对页面或允许绝对(与虚拟相对)访问,设置图1的DA位140。

[0113] 以下示例展示了在两个安全域之间页面的共享。对于相同的两个安全域X和Y,可以共享A1x和A1y,使得A1x＝A1y＝A1。安全实体X和Y的注册的主机-地址-对和相关联的信息可以是(V1x,A1),DA＝1(共享页面),D＝X;(V2x,A2x),DA＝0(无共享),D＝X;(V3x,A3x),DA＝0(无共享),D＝X;(V1y,A1),DA＝1(共享页面),D＝Y;以及(V2y,A2y),DA＝0(无共享),D＝Y。可以仅允许域X和Y访问共享绝对页面A1,并且在一个示例中,因为DA＝1,所以跳过对虚拟地址的匹配检查。在另一种情况下,每个域X和Y可以为每个共享页面注册单独的(唯一的或匹配的)虚拟地址。安全域之间的页面请求的共享可以由一个或多个安全域开始并且由其余域验证。

[0114] 作为另一示例,如果页面以DA＝1注册,指示未进行虚拟地址检查,则安全接口控制可使用绝对地址来访问安全-UV页面。在这种情况下,该页面以主机-地址对(--,A1as)注册,其中主机虚拟地址无关紧要,DA＝1,并且D＝AS(指示它属于安全接口控制的辅助安全)。安全接口控制可以比较安全域以保证仅由安全接口控制允许对此页面的访问。因为DA＝1,所以不进行虚拟地址检查。

[0115] 图16描绘了在两个安全域之间共享页面的实现方式的示例,作为其中DA＝1(共享)的一个示例。在该示例中,从虚拟地址空间1602到绝对地址空间1604的主机-地址对是:(V1,A2),(V2,A1),(V3,A2),(V4,A3),(V5,A2)。绝对地址A2可以在三个不同的虚拟地址之间共享1606:来自相同安全访客域1608的V1和V5以及来自另一个安全域1610的V3。从虚拟地址空间1602到绝对地址空间1604的转换可以由非可信管理程序或OS拥有。这种共享在某些情况下可能是有益的;然而,如果域1608、1610两者都能够访问共享1606的相同的绝对地址A2,则在域1608、1610之间共享相同的绝对地址A2会引起安全问题。

[0116] 根据本发明的一个或多个实施例,图17示出了对图16的示例的修改,作为DA＝1(共享)的另一个示例,其中主机-地址对是:(V1,A2),

[0117] (V2,A1),(V4,A3),(V5,A2)。值得注意的是,地址转换对(V3,A2)在从虚拟地址空间1602到绝对地址空间1704的映射中不是直接可用的。安全容器/VM可能不允许页面的共

享。(V3,A2)被改变为(V3,A2’),这可以包括复制物理A2页面以便对于每个容器/VM具有一个唯一副本。由此,域1608、1610的访问均可查看A2的单独副本,但是改变A2的内容的任何尝试将对不同的绝对页面A2、A2’执行。图1的DA位140可以用于允许使用两个不同的虚拟地址(例如,域1608的V1和域1610的V3)在两个不同的安全域1608、1610之间共享一个绝对页面。

[0118] 现在转向图18,根据本发明的一个或多个实施例总体上示出了用于跨多个安全域共享安全存储器的处理流程1800。在框1805处,计算机系统的安全接口控制可接收对存储器的安全页面的安全访问请求。在框1810处,安全接口控制可以检查与安全页面相关联的禁用虚拟地址(例如,DA位140)比较状态。在框1815处,安全接口控制可基于禁用虚拟地址比较状态(例如,DA=1)被设置,在访问安全页面时禁用虚拟地址检查,以支持从多个虚拟地址到至安全页面的相同绝对地址的映射。可基于作出安全访问请求的实体的授权状态和禁用虚拟地址比较状态(例如,DA=1)被设置,来使能对没有指定虚拟地址的安全页面的绝对地址访问。该安全接口控制可以基于域标识符来验证多个安全域中的安全域被授权访问该共享页面。可以将安全域的域标识符与被标识为允许共享的安全域的多个域标识符进行比较以确认对访问共享页面的授权。

[0119] 安全接口控制可以检查安全页面相对于安全域的注册状态。安全接口控制可以基于确定安全页面未以安全域注册来确定安全域是否允许共享。可以基于确定安全域允许共享来检查禁用虚拟地址比较状态。安全接口控制可以确认允许跨多个安全域的虚拟地址共享。例如,安全接口控制可以确认将虚拟地址映射到绝对地址的多组DAT表未被不安全主机改变,该不安全主机被配置为针对能够访问安全页面的多个安全域中的任何安全域来管理多组DAT表中的一组或多组。虚拟地址的每一表映射可包含一组或多组DAT表中的多个相关联的表。可以基于检测到DAT表的一组或多组中的变化来终止安全访问请求。

[0120] 安全页面的虚拟-绝对地址对可以用安全域标识符例如注册在图1的区安全表100中。可以验证与该安全访问请求相关联的地址,并且可以响应于该安全访问请求来验证具有虚拟-绝对地址对和安全域标识符的访问安全域。可以通过区安全表100来存储和更新禁用虚拟地址比较状态,区安全表100包括与安全页面相关联的安全域标识符、与安全页面相关联的虚拟地址映射数据以及禁用虚拟地址比较状态。安全页面可被分配给由管理程序或操作系统管理的安全虚拟机或安全容器。

[0121] 应当理解,尽管本公开包括关于云计算的详细描述,但是本文所引用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他类型的计算环境来实现。

[0122] 云计算是一种服务交付模型,用于实现对可配置计算资源(例如,网络、网络带宽、服务器、处理、存储器、存储、应用、虚拟机和服务)的共享池的方便、按需的网络访问,所述可配置计算资源可以用最小的管理努力或与服务提供商的交互来快速配置和释放。该云模型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。

[0123] 特性如下:

[0124] 按需自助服务:云消费者可按需自动地单方面供应计算能力,诸如服务器时间和网络存储,而无需与服务提供商进行人工交互。

[0125] 广泛的网络接入:通过网络提供功能,并通过标准机制进行访问,所述标准机制促

进由异构的瘦客户端或厚客户端平台(例如,移动电话、膝上型计算机和PDA)的使用。

[0126] 资源池化:提供者的计算资源被汇集起来以使用多租户模型来服务于多个消费者,不同的物理和虚拟资源根据需要被动态分配和重新分配。存在位置独立性的意义,因为消费者通常对所提供资源的确切位置不具有控制权或知识,但可能能够指定更高抽象层级的位置(例如,国家、州或数据中心)。

[0127] 快速弹性:在某些情况下,可以快速且弹性地配置功能,以快速扩展缩小并迅速释放以快速收缩。对于消费者而言,可用于配置的功能通常似乎是无限的,可以在任何时间以任何数量购买。

[0128] 度量的服务:云系统通过利用与服务类型(例如,存储、处理、带宽和活动用户帐户)相适应的某种抽象层级的计量能力,自动控制和优化资源使用。可以监视、控制和报告资源使用情况,为所使用服务的提供者和使用者提供透明性。

[0129] 服务模型如下:

[0130] 软件即服务(SaaS):向消费者提供的能力是使用在云基础设施上运行的提供者的应用。这些应用可通过诸如web浏览器(例如,基于web的电子邮件)的瘦客户端接口从不同客户端设备访问。消费者不管理或控制包括网络、服务器、操作系统、存储或甚至个体应用功能的底层云基础结构,可能的例外是有限的用户特定的应用配置设置。

[0131] 平台即服务(PaaS):向消费者提供的能力是在云基础结构上部署消费者创建或获取的应用,所述应用是用提供者所支持的编程语言和工具创建的。消费者不管理或控制包括网络、服务器、操作系统或存储的底层云基础结构,但是具有对所部署的应用以及可能的应用托管环境配置的控制。

[0132] 基础设施即服务(IaaS):向消费者提供的能力是提供消费者能够部署和运行可包括操作系统和应用的任意软件的处理、存储、网络和其他基本计算资源。消费者不管理或控制底层云基础结构,而是具有对操作系统、存储、所部署的应用的控制,以及对所选联网组件(例如,主机防火墙)的可能有限的控制。

[0133] 部署模型如下:

[0134] 私有云:云基础结构仅为组织运营。它可以由组织或第三方管理,并且可存在于场所内或场所外。

[0135] 社区云:云基础结构由多个组织共享,并支持具有共同关注点(例如,任务、安全要求、策略和合规性考虑)的特定社区。它可以由组织或第三方管理,并且可存在于场所内或场所外。

[0136] 公共云:云基础结构可供公众或大型行业团体使用,并由销售云服务的组织拥有。

[0137] 混合云:云基础结构是由两个或更多个云(私有、社区或公共的)组成的,这些云仍然是唯一性实体,但通过标准化或专有技术来绑定在一起,这些技术实现数据和应用的可移植性(例如,用于云之间的负载平衡的云突发)。

[0138] 云计算环境是面向服务的,着重于无状态性、低耦合、模块化和语义互操作性。云计算的核心是包括互连节点网络的基础架构。

[0139] 现在参见图19,描绘说明性云计算环境50。如图所示,云计算环境50包括一个或多个云计算节点10,云消费者使用的本地计算设备(诸如个人数字助理(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)可与云计算节点10通信。节点

10可以彼此通信。它们可以在一个或多个网络中,诸如在上文所述的私有云、社区云、公共云或混合云或其组合中,被物理地或虚拟地分组(未示出)。这允许云计算环境50提供基础结构、平台和/或软件作为服务,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19中所示的计算设备54A-N的类型仅旨在是说明性的,并且计算节点10和云计算环境50可通过任何类型的网络和/或网络可寻址连接(例如,使用网络浏览器)与任何类型的计算机化设备进行通信。

[0140] 现在参见图20,示出了由云计算环境50(图19)提供的一组功能抽象层。应预先理解,图20中所示的部件、层和功能旨在仅是说明性的,并且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:

[0141] 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:主机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65;以及网络和联网组件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。

[0142] 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72;虚拟网络73,包括虚拟专用网络;虚拟应用和操作系统74;以及虚拟客户端75。

[0143] 在一个示例中,管理层80可提供下文所描述的功能。资源供应81提供用于执行云计算环境内的任务的计算资源和其他资源的动态获取。计量和定价82在云计算环境内利用资源时提供成本跟踪,并针对这些资源的消费进行计费或开票。在一个示例中,这些资源可以包括应用软件许可证。安全性为云消费者和任务提供身份验证,以及对数据和其他资源的保护。用户门户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84提供云计算资源分配和管理,使得满足所需的服务级别。服务水平协议(SLA)计划和履行85为根据SLA预期的云计算资源的未来要求提供云计算资源的预安排和采购。

[0144] 工作负载层90提供可以利用云计算环境的功能的示例。可以从该层提供的工作负荷和功能的示例包括:地图和导航91;软件开发和生命周期管理92;虚拟教室教育交付93;数据分析处理94;事务处理95;以及控制对与虚拟机相关联的安全存储的访问96。应当理解,这些仅仅是一些示例,并且在其他实施例中,层可以包括不同的服务。

[0145] 现在转到图21,描绘了根据本发明的一个或多个实施例的系统2100。系统2100包括例如经由网络165与一个或多个客户端设备20A-20E直接或间接通信的示例节点10(例如,托管节点)。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执行管理程序12,其促进部署一个或多个VM 15(15A-15N)。节点10还包括硬件/固件层13,其包括安全接口控制11。安全接口控制11包括促进管理程序12向虚拟机15提供一个或多个服务的一个或多个硬件模块和固件。在现有技术方案中,在管理程序12与安全接口控制11之间;安全接口控制11和一个或多个VM 15之间;管理程序12和一个或多个VM 15之间;以及管理程序12通过安全接口控制11到VM15存在通信。为了促进安全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VM15之间的任何直接通信。

[0146] 例如,托管节点10可促进客户端设备20A部署VM 15A-15N中的一个或多个。可响应于来自不同客户端设备20A-20E的相应请求部署VM 15A-15N。例如,VM 15A可以由客户端设备20A部署,VM 15B可以由客户端设备20B部署,并且VM 15C可以由客户端设备20C部署。节点10还可以促进客户端供应物理服务器(而不作为VM运行)。在此描述的示例将节点10中的

资源的供应具体化为VM的一部分,然而,所描述的技术方案还可以应用于将资源供应为物理服务器的一部分。

[0147] 在示例中,客户端设备20A-20E可以属于同一实体,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可以作为实体的私有云来操作。在这种情况下,节点10仅托管由属于实体的客户端设备20A-20E部署的VM 15A-15N。在另一示例中,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可以被操作为托管来自不同实体的VM的公共云。例如,VM 15A-15N可以以屏蔽方式部署,其中VM 15A不促进对VM 15B的访问。例如,节点10可使用IBM z Systems®处理器资源/系统管理器(PR/SM)逻辑分区(LPAR)特征来覆盖VM 15A-15N。这些特征(诸如PR/SM LPAR)提供分区之间的隔离,因此促进节点10在不同的逻辑分区中为同一物理节点10上的不同实体部署两个或更多个VM 15A-15N。PR/SM LPAR管理程序在具有特定硬件的可信的内部固件中实现以提供这种隔离。

[0148] 来自客户端设备20A-20e的客户端设备20A是通信设备,诸如计算机、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由节点10的管理程序12部署VM的任何其他通信设备。客户端设备20A可以经由网络165发送由管理程序接收的请求。来自VM 15A-15N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映像。管理程序12是VM监视器(VMM),其可以是创建和运行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。利用适当的特征和修改,管理程序12可以是IBMzSystems®、Oracle的VM Server、Citrix的XenServer、Vmware的ESX、Microsoft的Hyper-V管理程序或任何其他管理程序。管理程序12可以是直接在节点10上执行的本机管理程序,或者在另一管理程序上执行的托管管理程序。

[0149] 现在转到图22,根据本发明的一个或多个实施例示出了用于实现本文的教导的节点10。节点10可以是电子计算机框架,其包括和/或采用任意数量和组合的计算设备和利用不同通信技术的网络,如本文所述。节点10可以是容易地缩放的、可扩展的和模块化的,具有改变到不同服务或独立于其他而重新配置一些特征的能力。

[0150] 在本实施例中,节点10具有处理器2201,其可以包括一个或多个中央处理单元(CPU)2201a、2201b、2201c等。处理器2201(也被称为处理电路、微处理器、计算单元)经由系统总线2202耦合到系统存储器2203和不同其他组件。系统存储器2203包括只读存储器(ROM)2204和随机存取存储器(RAM)2205。ROM 2204耦合到系统总线2202,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是耦接到系统总线2202以供处理器2201使用的读写存储器。

[0151] 图22的节点10包括硬盘2207,其是可由处理器2201可执行地读取的有形存储介质的示例。硬盘2207存储软件2208和数据2209。软件2208被存储为由处理器2201在节点10上执行的指令(以便执行过程,如参见图1-21所描述的过程)。数据2209包括以不同数据结构组织以支持软件2208的操作和由软件2208的操作使用的定性或定量变量的一组值。

[0152] 图22的节点10包括互连和支持处理器2201、系统存储器2203、硬盘2207和节点10的其他组件(例如,外围设备和外部设备)之间的通信的一个或多个适配器(例如,硬盘控制器、网络适配器、图形适配器等)。在本发明的一个或多个实施例中,一个或多个适配器可以

连接到经由中间总线桥连接到系统总线2202的一个或多个I/O总线,并且一个或多个I/O总线可以利用公共协议,例如外围组件互连(PCI)。

[0153] 如图所示,节点10包括将键盘2221、鼠标2222、扬声器2223和麦克风2224互连到系统总线2202的接口适配器2220。节点10包括将系统总线2202互连到显示器2231的显示适配器2230。显示适配器2230(和/或处理器2201)可以包括图形控制器以提供图形性能,诸如GUI 2232的显示和管理。通信适配器2241将系统总线2202与网络2250互连,使得节点10能够与其他系统、设备、数据和软件(诸如服务器2251和数据库2252)通信。在本发明的一个或多个实施例中,软件2208和数据2209的操作可以由服务器2251和数据库2252在网络2250上实现。例如,网络2250、服务器2251、和数据库2252可以组合以提供软件2208和数据2209的内部迭代,作为平台即服务、软件即服务、和/或基础设施即服务(例如,作为分布式系统中的web应用)。

[0154] 本文描述的实施例必然以计算机技术为根源,并且具体地以托管VM的计算机服务器为根源。进一步,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(特别是托管VM的计算机服务器)的操作的改进,其中即使管理程序被禁止访问与安全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包括硬件、固件(例如,毫码)或其组合的安全接口控制(在此也被称为"UV"),向改进VM托管计算服务器提供重要步骤,促进安全VM和管理程序的分离并且因此维持由计算服务器托管的VM的安全性。安全接口控制提供轻量级中间操作以促进安全性,而不会向如本文所述的VM的初始化/退出期间的安全VM状态添加大量开销。

[0155] 在此公开的本发明的实施例可以包括控制对VM的安全存储的访问的系统、方法和/或计算机程序产品(在此为系统)。注意,对于每个解释,元件的标识符被重用于不同图的其他类似元件。

[0156] 在此参考相关附图描述本发明的不同实施例。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的元件之间阐述了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,并且本发明在这方面并非意图进行限制。因而,实体的耦合可以指直接或间接耦合,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工艺步骤可并入到具有本文未详细描述的附加步骤或功能的更全面的程序或工艺中。

[0157] 以下定义和缩写用于解释权利要求书和说明书。如在此使用的,术语"包含"、"包括"、"具有"或"含有"或其任何其他变体旨在覆盖非排他性的包含。例如,包含一系列元素的组合物、混合物、工艺、方法、制品或设备不一定仅限于那些元素,而是可包括未明确列出的或此类组合物、混合物、工艺、方法、制品或设备固有的其他元素。

[0158] 另外,术语"示例性"在此用于意指"充当示例、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他实施例或设计优选或有利。术语"至少一个"和"一个或多个"可以被理解为包括大于或等于一(即,一、二、三、四等)的任何整数。术语"多个"可以被理解为包括大于或等于两个(即,两个、三个、四个、五个等)的任何整数。术语"连接"可以包括间接"连接"和直接"连接"两者。"

[0159] 术语"约"、"基本上"、"大约"及其变体旨在包括与基于在提交本申请时可用的设备的特定量的测量相关联的误差程度。例如,"约"可以包括给定值的±8%或5%、或2%的

范围。

[0160] 本发明的各个方面可以是处于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。所述计算机程序产品可包含上面具有计算机可读程序指令的计算机可读存储介质(或媒体),所述计算机可读程序指令用于致使处理器执行本发明的方面。

[0161] 计算机可读存储介质可以是可以保留和存储指令以供指令执行设备使用的有形设备。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各项的任何合适的组合。计算机可读存储介质的更具体例子的非穷举列表包括以下:便携式计算机盘,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)、便携式致密盘只读存储器(CD-ROM),数字通用盘(DVD)、记忆棒、软盘、机械编码设备(诸如穿孔卡片)或具有记录在其上的指令的凹槽中的凸起结构),以及上述的任意合适的组合。如本文中所使用的计算机可读存储介质不应被解释为瞬态信号本身,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,通过光纤电缆的光脉冲)、或通过导线传输的电信号。

[0162] 本文所述的计算机可读程序指令可从计算机可读存储介质下载到相应的计算/处理设备,或经由网络(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器卡或网络接口从网络接收计算机可读程序指令并且转发这些计算机可读程序指令以便存储在对应的计算/处理设备内的计算机可读存储介质中。

[0163] 用于执行本技术方案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,或以一种或多种编程语言的任何组合编写的源代码或目标代码,包括面向对象的Smalltalk、C++等编程语言,以及过程式编程语言,例如“C”编程语言或类似的编程语言。计算机可读程序指令可完全在用户的计算机上执行、部分在用户的计算机上执行、作为独立软件包执行、部分在用户的计算机上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。在后一种情形中,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,通过使用互联网服务提供商的互联网)。在一些实施例中,电子电路(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))可以通过使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,以便执行本技术方案的各方面。

[0164] 在此参照根据技术方案的实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图来描述本技术方案的各方面。应当理解,流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合,都可以由计算机可读程序指令来实现。

[0165] 这些计算机可读程序指令可以被提供给通用计算机的处理器,专用计算机或其他可编程数据处理装置,以产生机器,其通过计算机或其他可编程数据处理装置的处理器执行,创建用于实现在流程图和/或方框图的一个或多个方框中指定的功能/动作的装置。这些计算机可读程序指令还可存储在可指导计算机的计算机可读存储介质中,可编程数据处理装置,和/或以特定方式起作用的其他设备,使得具有存储在其中的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/或框图中的一个或多个方框中规定的功能/动作的各方面的指令。

[0166] 计算机可读程序指令还可以加载到计算机、其他可编程数据处理装置上，或使得在计算机上执行一系列操作步骤的其他装置，其他可编程装置或其他设备，以产生计算机实现的过程，使得在计算机上执行的指令，其他可编程装置或其他设备实现流程图和/或框图中的一个或多个方框中指定的功能和动作。

[0167] 附图中的流程图和框图示出了根据本技术方案的不同实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。对此，流程图或框图中的每个方框可以代表模块、段或指令的一部分，其包括用于实现规定的逻辑功能的一个或多个可执行指令。在一些替代实施例中，框中所标注的功能可以不以图中所标注的次序发生。例如，取决于所涉及的功能，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。还将注意的是，框图和/或流程图中的每个框、以及框图和/或流程图中的框的组合可以由基于专用硬件的系统来实现，所述基于专用硬件的系统执行指定的功能或动作或执行专用硬件与计算机指令的组合。

[0168] 在此使用的术语仅用于描述具体实施例的目的并且不旨在是限制性的。如在此使用的，单数形式“一个”、“一种”和“该”旨在也包括复数形式，除非上下文另外清楚地指示。将进一步理解的是，当在本说明书中使用术语“包括”和/或“包含”时，其指定所陈述的特征、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他特征、整数、步骤、操作、元件组件和/或其组的存在或添加。

[0169] 出于说明的目的已经呈现了对在此的不同实施例的描述，但是并不旨在是穷尽性的或局限于所披露的实施例。在不背离所描述的实施例的范围和精神的情况下，许多修改和变化对本领域的普通技术人员而言将是显而易见的。选择在此使用的术语以最佳地解释实施例的原理、实际应用或在市场上找到的技术上的技术改进，或使得本领域普通技术人员能够理解在此披露的实施例。

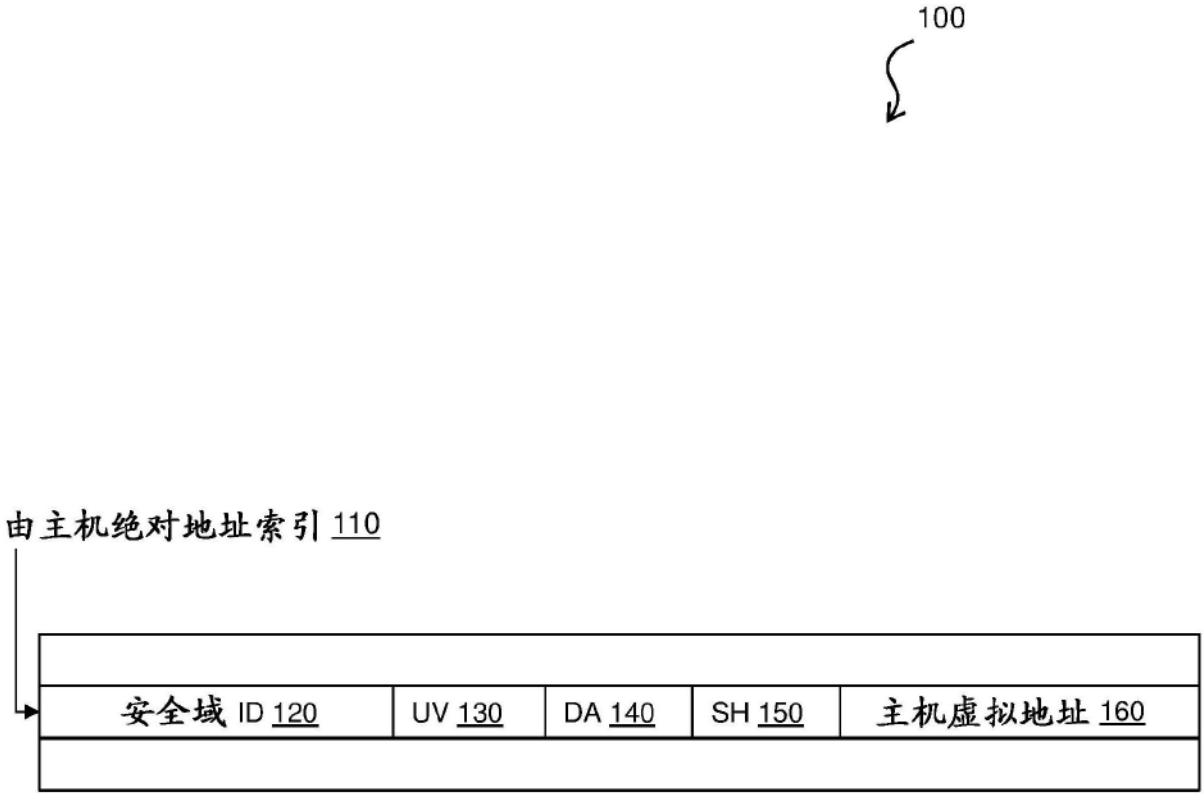

图1

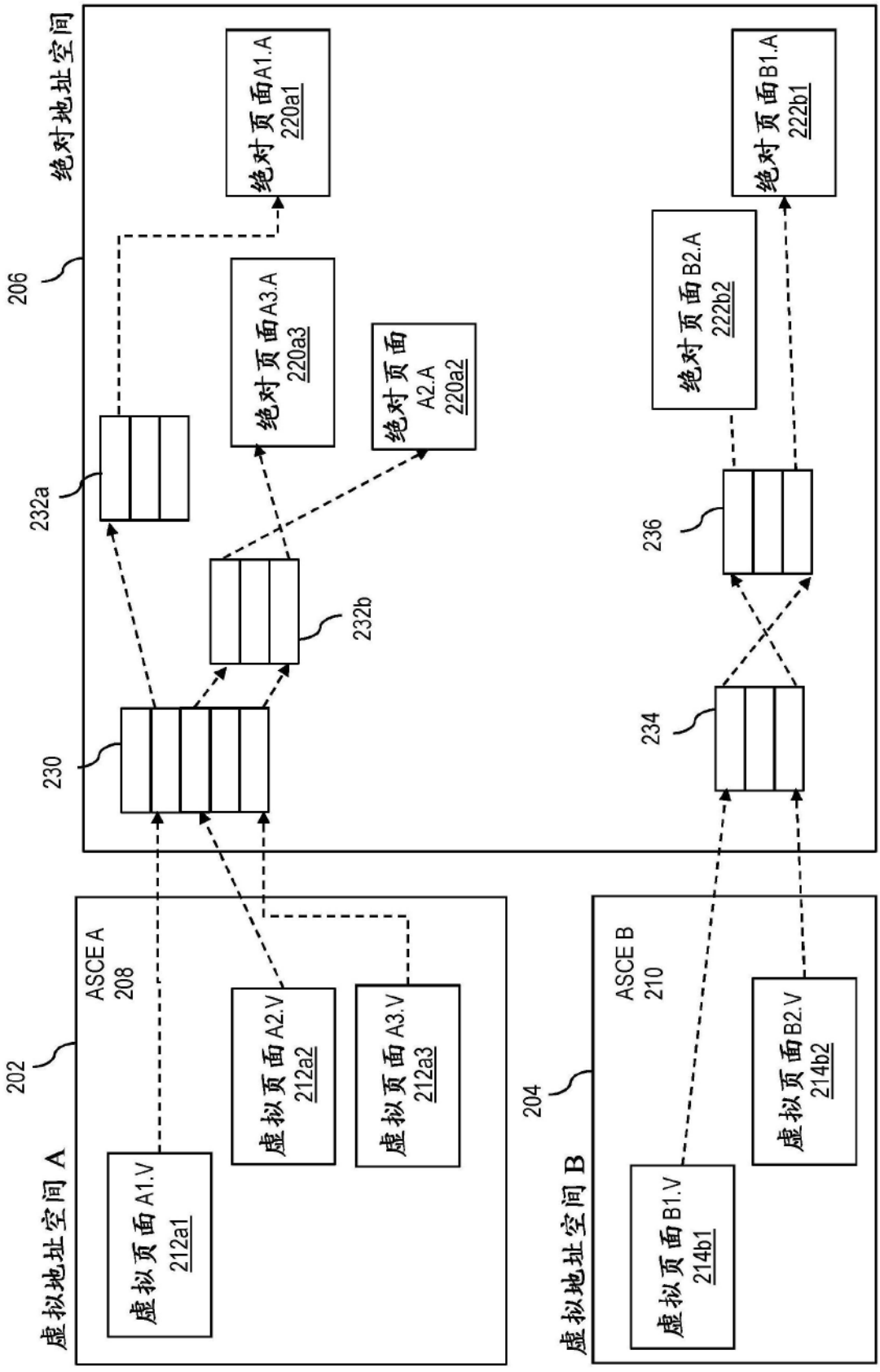
虚拟地址空间 A
202
ASCE A
208
虚拟页面 A1.V
212a1
虚拟页面 A2.V
212a2
虚拟页面 A3.V
212a3
虚拟地址空间 B
204
ASCE B
210
虚拟页面 B1.V
214b1
虚拟页面 B2.V
214b2
绝对地址空间
206
绝对页面 A1.A
220a1
绝对页面 A3.A
220a3
绝对页面 A2.A
220a2
绝对页面 B1.A
222b1
绝对页面 B2.A
222b2
230
232a
232b
234
236

图2

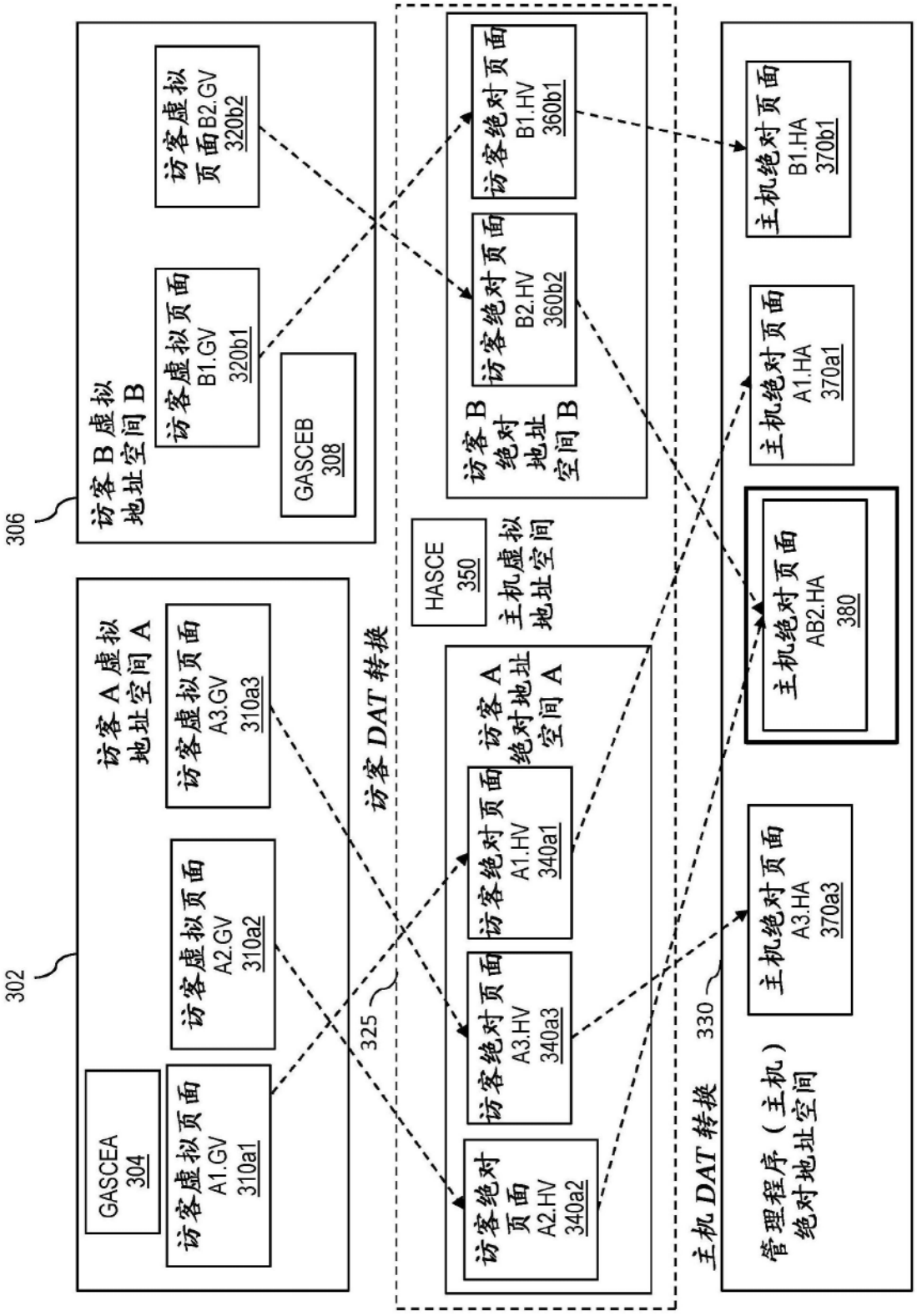
306
访客 B 虚拟地址空间 B
访客虚拟页面 B2.GV 320b2
访客虚拟页面 B1.GV 320b1
GASCEB 308
302
访客 A 虚拟地址空间 A
访客虚拟页面 A3.GV 310a3
访客虚拟页面 A2.GV 310a2
GASCEA 304
访客虚拟页面 A1.GV 310a1
325
访客 DAT 转换
HASCE 350
主机虚拟地址空间
访客 B 绝对地址空间 B
访客绝对页面 B1.HV 360b1
访客绝对页面 B2.HV 360b2
访客 A 绝对地址空间 A
访客绝对页面 A1.HV 340a1
访客绝对页面 A3.HV 340a3
访客绝对页面 A2.HV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

图3

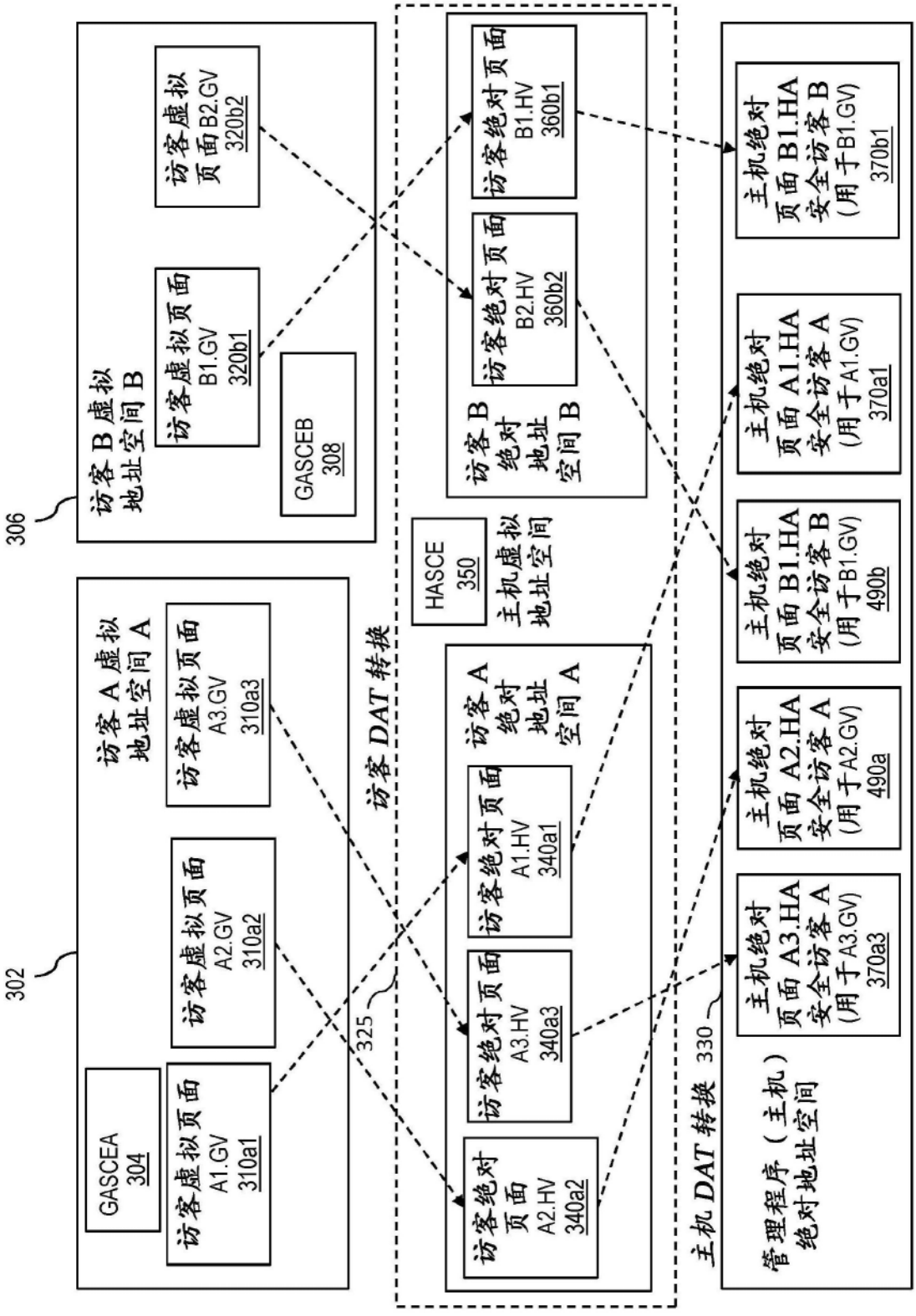
306
访客B虚拟地址空间B
访客虚拟页面B2.GV 320b2
访客虚拟页面B1.GV 320b1
GASCEB 308
302
访客A虚拟地址空间A
访客虚拟页面A3.GV 310a3
访客虚拟页面A2.GV 310a2
GASCEA 304
访客虚拟页面A1.GV 310a1
访客DAT转换
325
HASCE 350
主机虚拟地址空间
访客B绝对地址空间B
访客绝对页面B1.HV 360b1
访客绝对页面B2.HV 360b2
访客A绝对地址空间A
访客绝对页面A1.HV 340a1
访客绝对页面A3.HV 340a3
访客绝对页面A2.HV 340a2
主机DAT转换 330
管理程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

图4

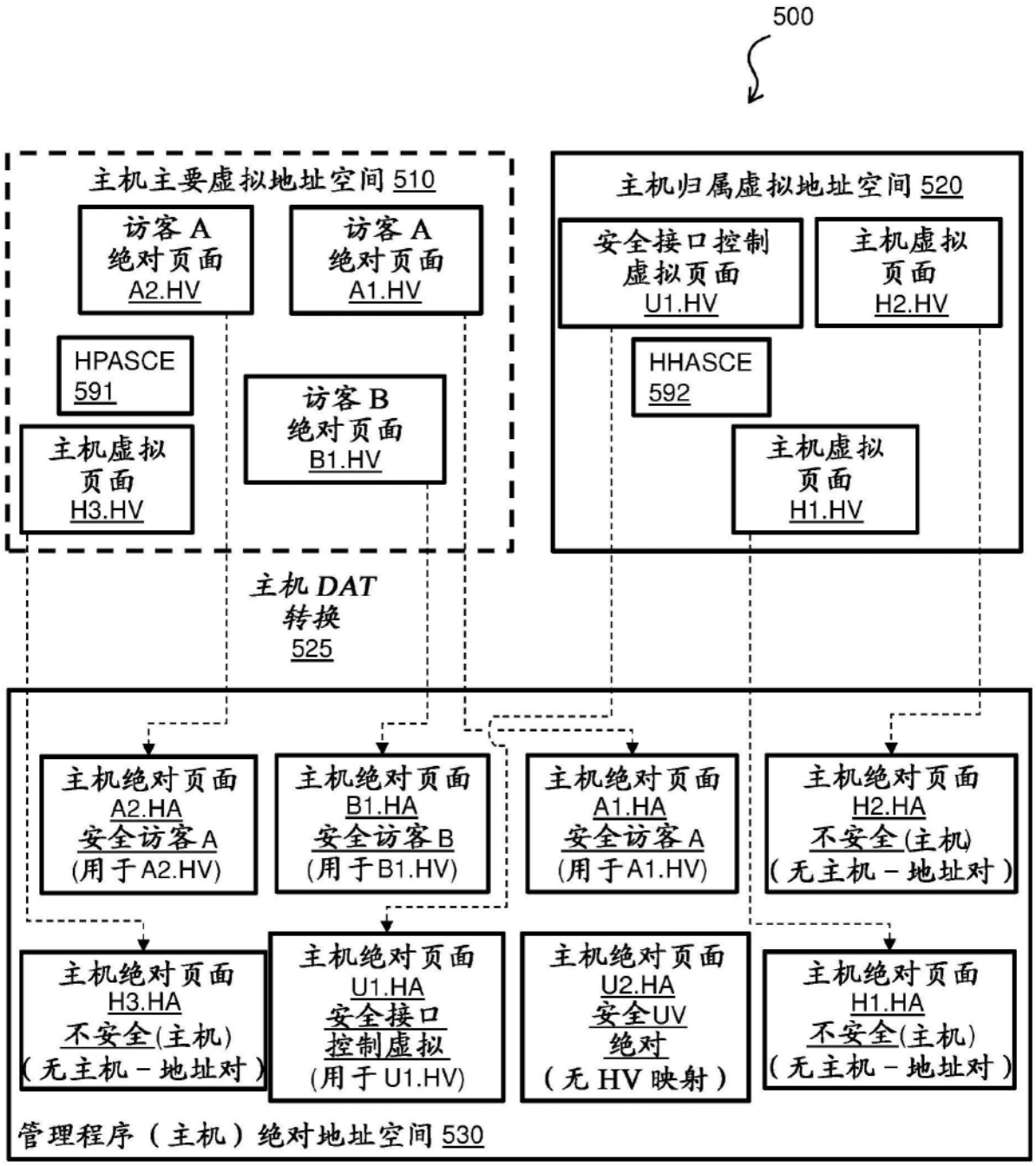
500
主机主要虚拟地址空间 510
访客 A
绝对页面
A2.HV
访客 A
绝对页面
A1.HV
HPASCE
591
访客 B
绝对页面
B1.HV
主机虚拟
页面
H3.HV
主机归属虚拟地址空间 520
安全接口控制
虚拟页面
U1.HV
主机虚拟
页面
H2.HV
HHASCE
592
主机虚拟
页面
H1.HV
主机 DAT
转换
525
主机绝对页面
A2.HA
安全访客 A
(用于 A2.HV)
主机绝对页面
B1.HA
安全访客 B
(用于 B1.HV)
主机绝对页面
A1.HA
安全访客 A
(用于 A1.HV)
主机绝对页面
H2.HA
不安全(主机)
(无主机 - 地址对)
主机绝对页面
H3.HA
不安全(主机)
(无主机 - 地址对)
主机绝对页面
U1.HA
安全接口
控制虚拟
(用于 U1.HV)
主机绝对页面
U2.HA
安全UV
绝对
(无 HV 映射)
主机绝对页面
H1.HA
不安全(主机)
(无主机 - 地址对)
管理程序 (主机) 绝对地址空间 530

图5

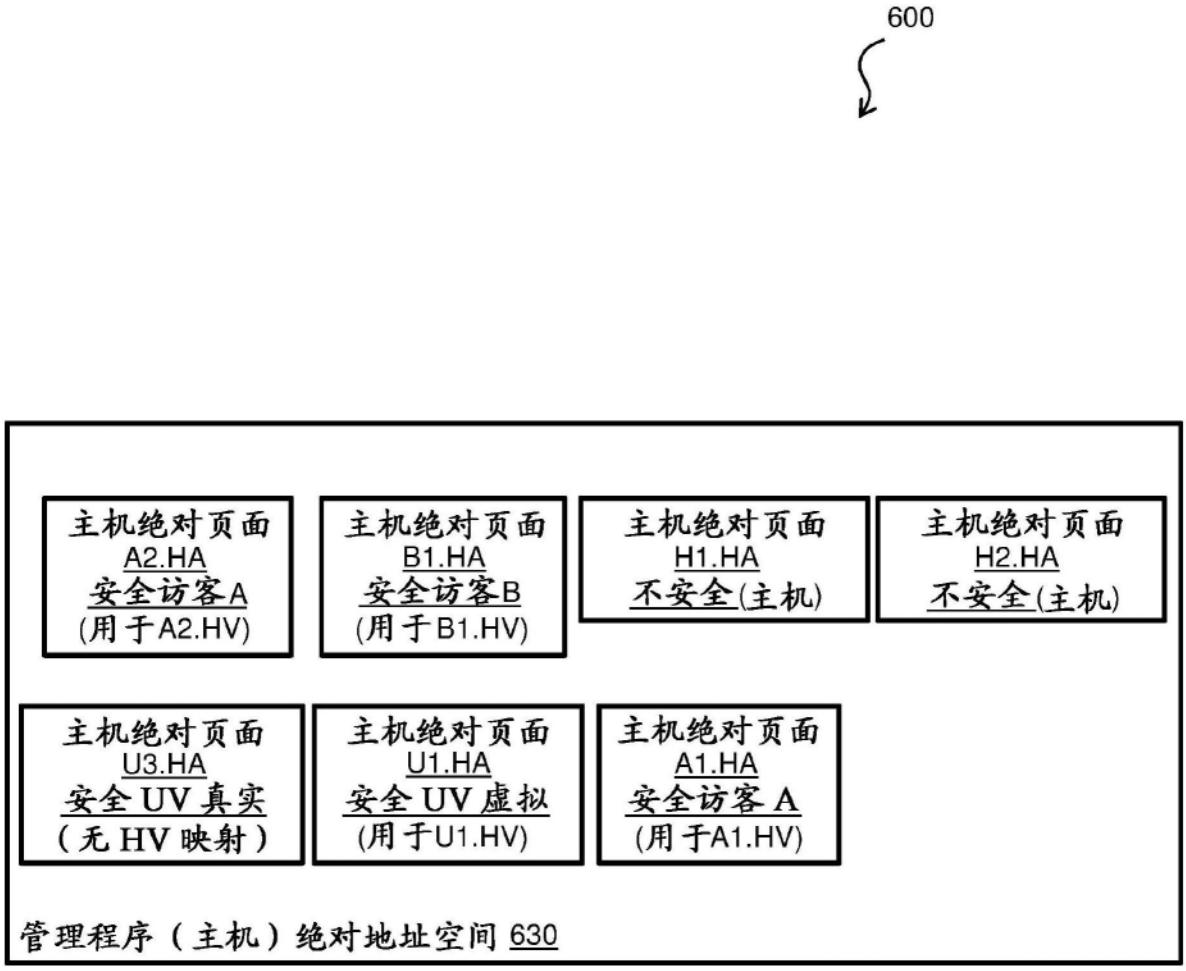
600
主机绝对页面
A2.HA
安全访客A
(用于A2.HV)
主机绝对页面
B1.HA
安全访客B
(用于B1.HV)
主机绝对页面
H1.HA
不安全(主机)
主机绝对页面
H2.HA
不安全(主机)
主机绝对页面
U3.HA
安全 UV 真实
(无 HV 映射)
主机绝对页面
U1.HA
安全 UV 虚拟
(用于U1.HV)
主机绝对页面
A1.HA
安全访客 A
(用于A1.HV)
管理程序(主机)绝对地址空间 630

图6

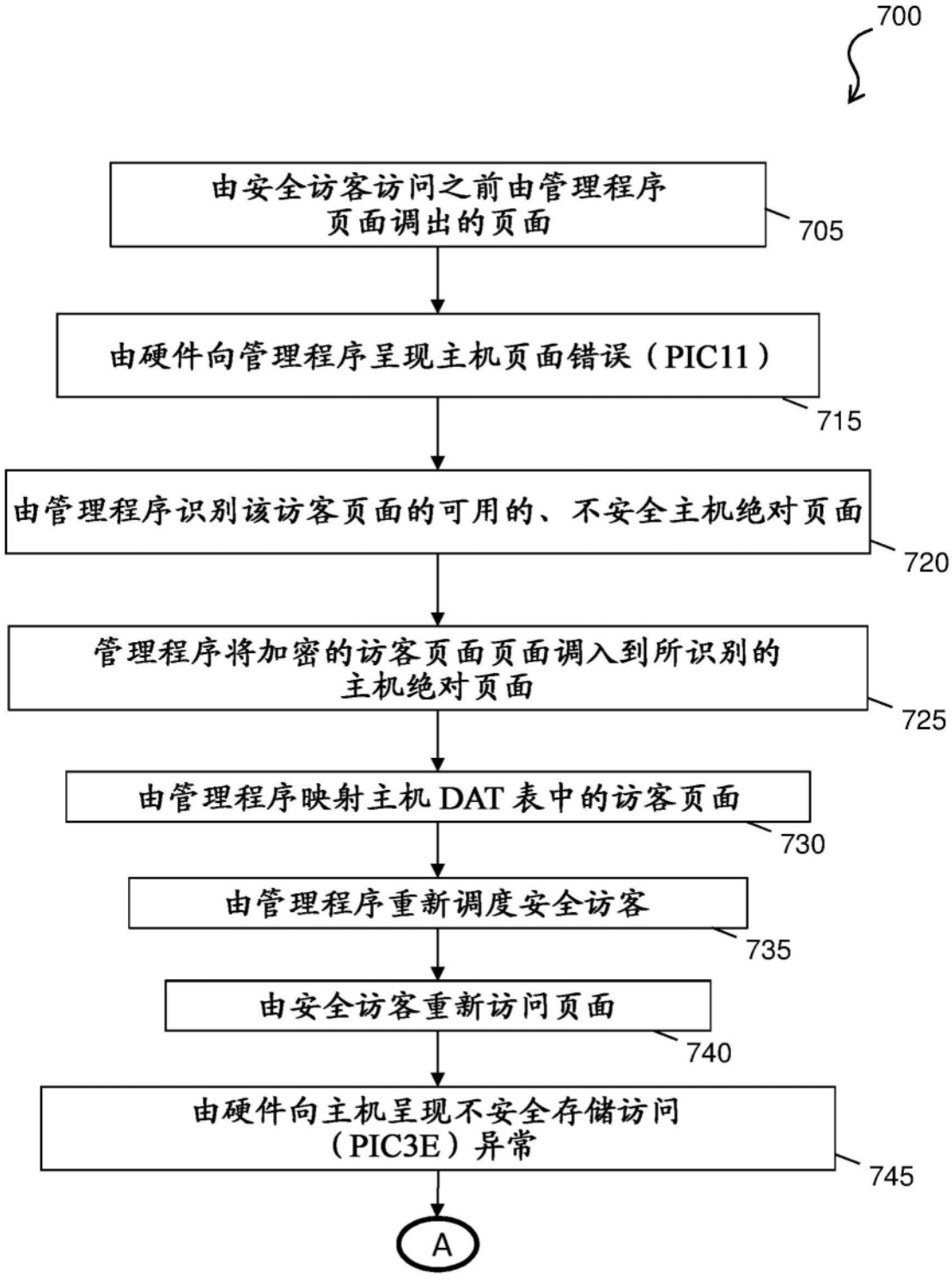
700
由安全访客访问之前由管理程序
页面调出的页面
705
由硬件向管理程序呈现主机页面错误（PIC11）
715
由管理程序识别该访客页面的可用的、不安全主机绝对页面
720
管理程序将加密的访客页面页面调入到所识别的
主机绝对页面
725
由管理程序映射主机 DAT 表中的访客页面
730
由管理程序重新调度安全访客
735
由安全访客重新访问页面
740
由硬件向主机呈现不安全存储访问
（PIC3E）异常
745
A

图7

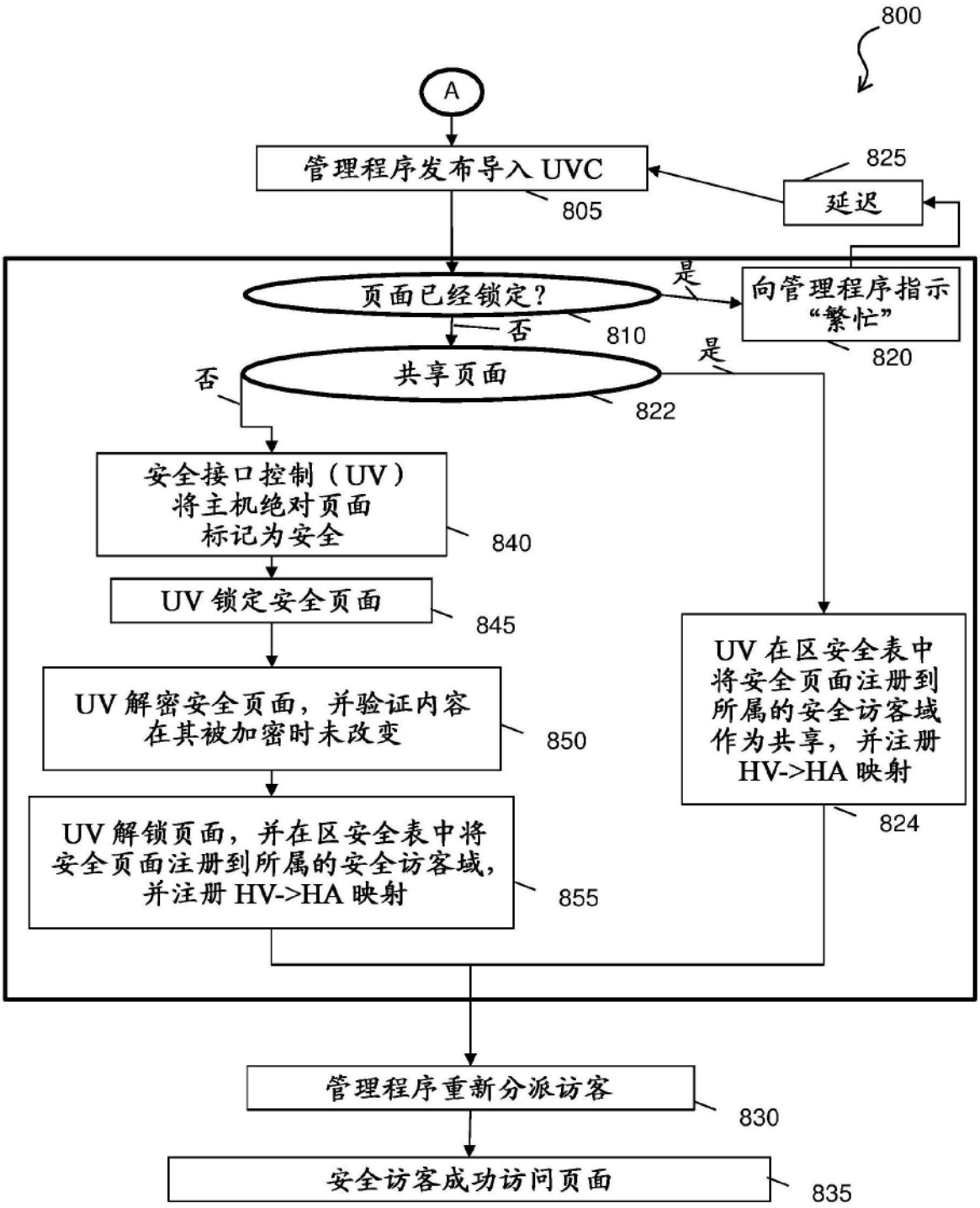
800
A
管理程序发布导入 UVC
805
825
延迟
页面已经锁定？
是
向管理程序指示“繁忙”
820
否
810
共享页面
是
否
822
安全接口控制（UV）将主机绝对页面标记为安全
840
UV 锁定安全页面
845
UV 解密安全页面，并验证内容在其被加密时未改变
850
UV 在区安全表中将安全页面注册到所属的安全访客域作为共享，并注册 HV->HA 映射
824
UV 解锁页面，并在区安全表中将安全页面注册到所属的安全访客域，并注册 HV->HA 映射
855
管理程序重新分派访客
830
安全访客成功访问页面
835

图8

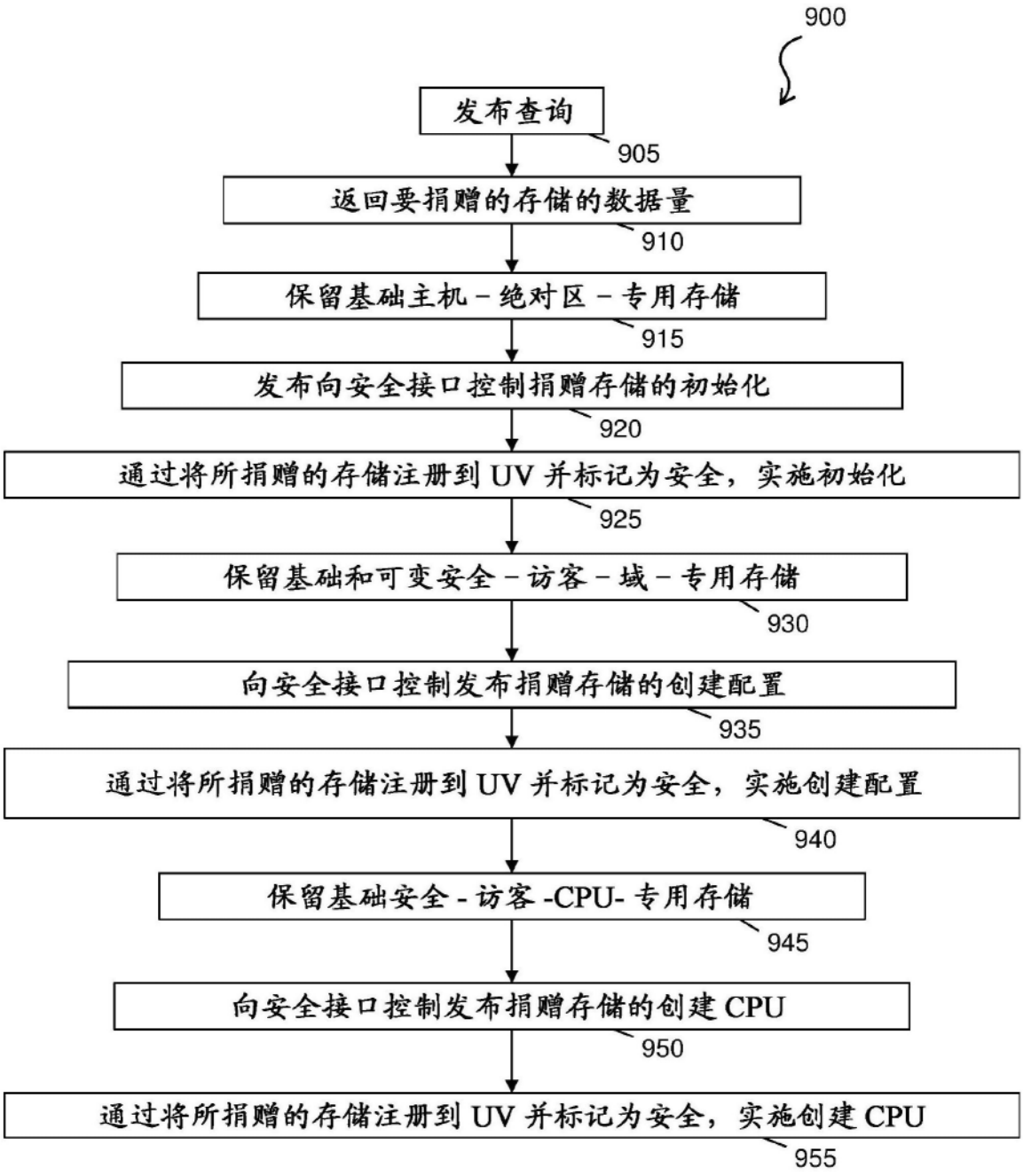
900
发布查询
905
返回要捐赠的存储的数据量
910
保留基础主机－绝对区－专用存储
915
发布向安全接口控制捐赠存储的初始化
920
通过将所捐赠的存储注册到 UV 并标记为安全，实施初始化
925
保留基础和可变安全－访客－域－专用存储
930
向安全接口控制发布捐赠存储的创建配置
935
通过将所捐赠的存储注册到 UV 并标记为安全，实施创建配置
940
保留基础安全 - 访客 -CPU- 专用存储
945
向安全接口控制发布捐赠存储的创建 CPU
950
通过将所捐赠的存储注册到 UV 并标记为安全，实施创建 CPU
955

图9

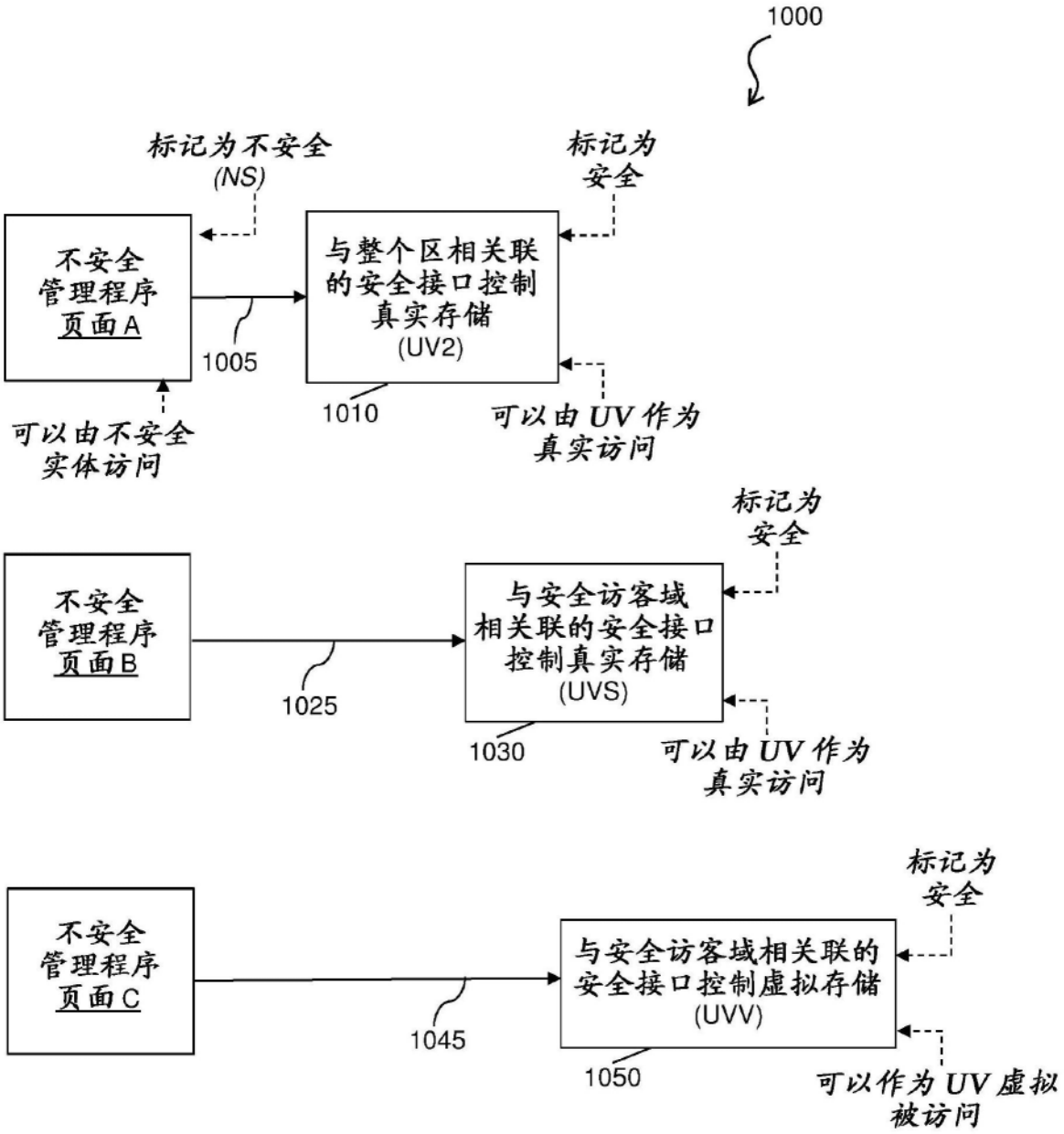
1000
标记为不安全
(NS)
标记为
安全
不安全
管理程序
页面A
与整个区相关联
的安全接口控制
真实存储
(UV2)
1005
1010
可以由不安全
实体访问
可以由UV作为
真实访问
标记为
安全
不安全
管理程序
页面B
与安全访客域
相关联的安全接口
控制真实存储
(UVS)
1025
1030
可以由UV作为
真实访问
标记为
安全
不安全
管理程序
页面C
与安全访客域相关联的
安全接口控制虚拟存储
(UVV)
1045
1050
可以作为UV虚拟
被访问

图10

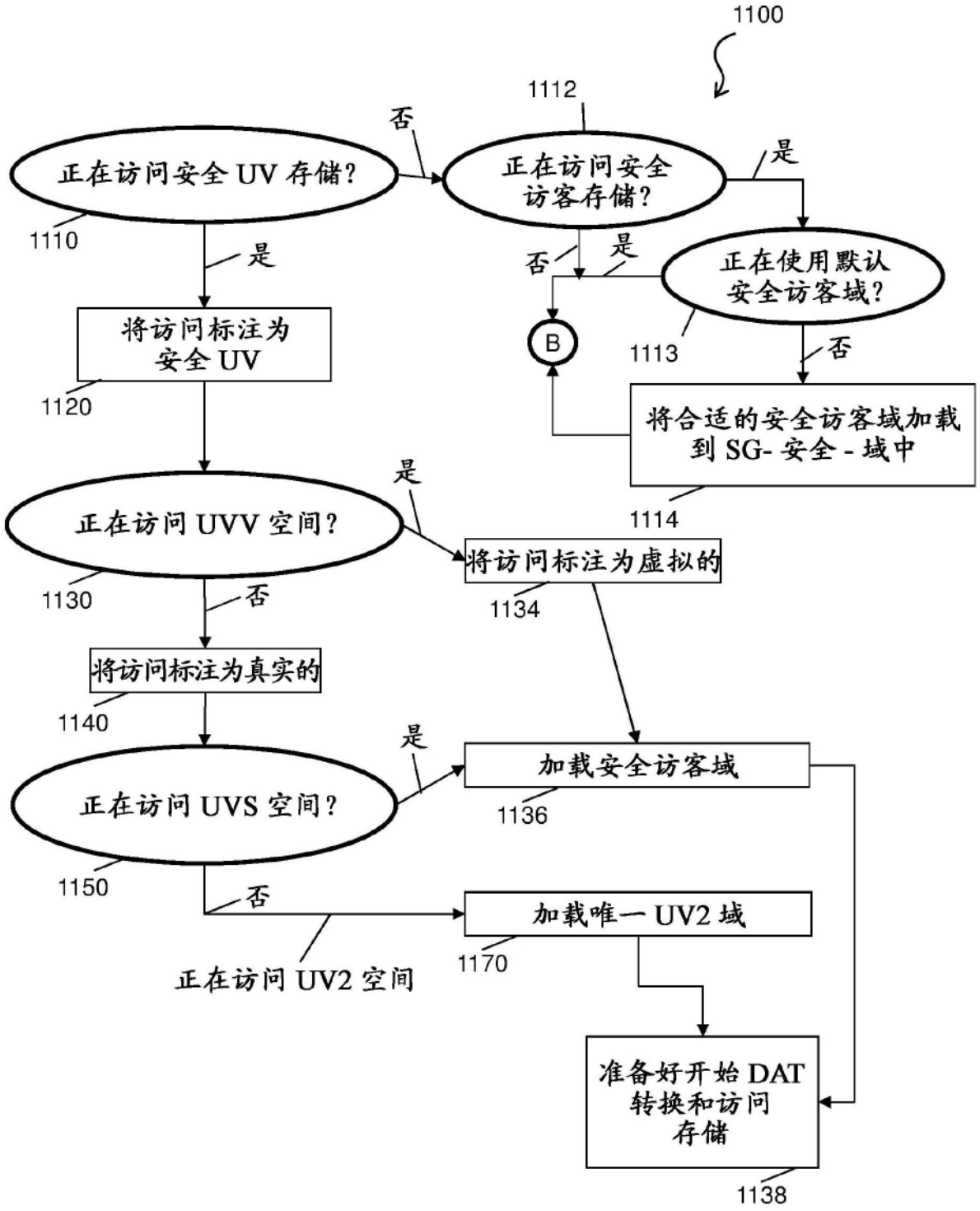
1100
1112
否
正在访问安全 UV 存储?
正在访问安全访客存储?
是
1110
是
否
是
正在使用默认安全访客域?
将访问标注为安全 UV
B
1113
否
1120
将合适的安全访客域加载到 SG- 安全 - 域中
1114
是
正在访问 UVV 空间?
将访问标注为虚拟的
1130
1134
否
将访问标注为真实的
1140
是
加载安全访客域
正在访问 UVS 空间?
1136
1150
否
加载唯一 UV2 域
1170
正在访问 UV2 空间
准备好开始 DAT 转换和访问存储
1138

图11

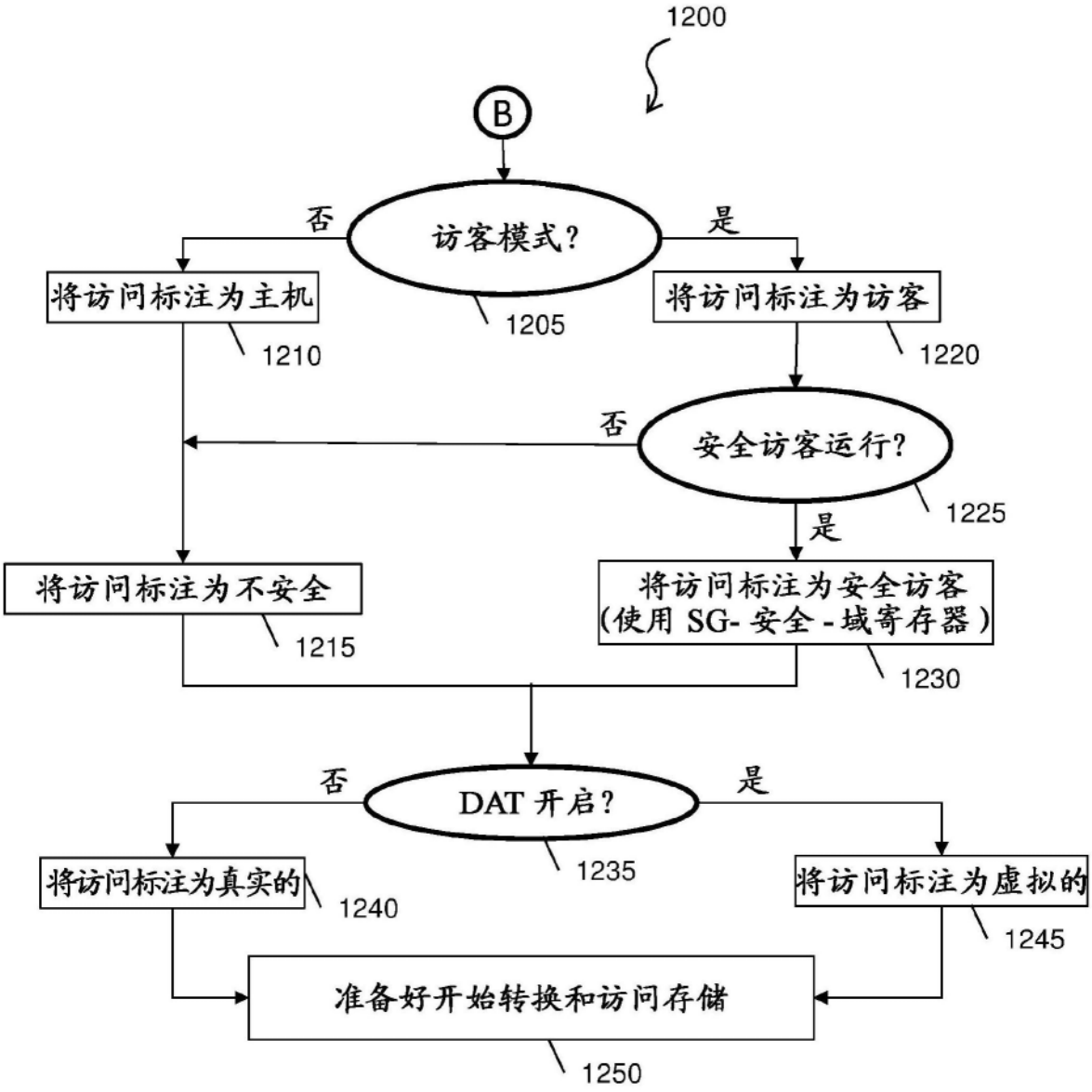
1200
B
访客模式?
否
是
1205
将访问标注为主机
1210
将访问标注为访客
1220
安全访客运行?
否
是
1225
将访问标注为不安全
1215
将访问标注为安全访客
(使用 SG- 安全 - 域寄存器)
1230
DAT 开启?
否
是
1235
将访问标注为真实的
1240
将访问标注为虚拟的
1245
准备好开始转换和访问存储
1250

图12

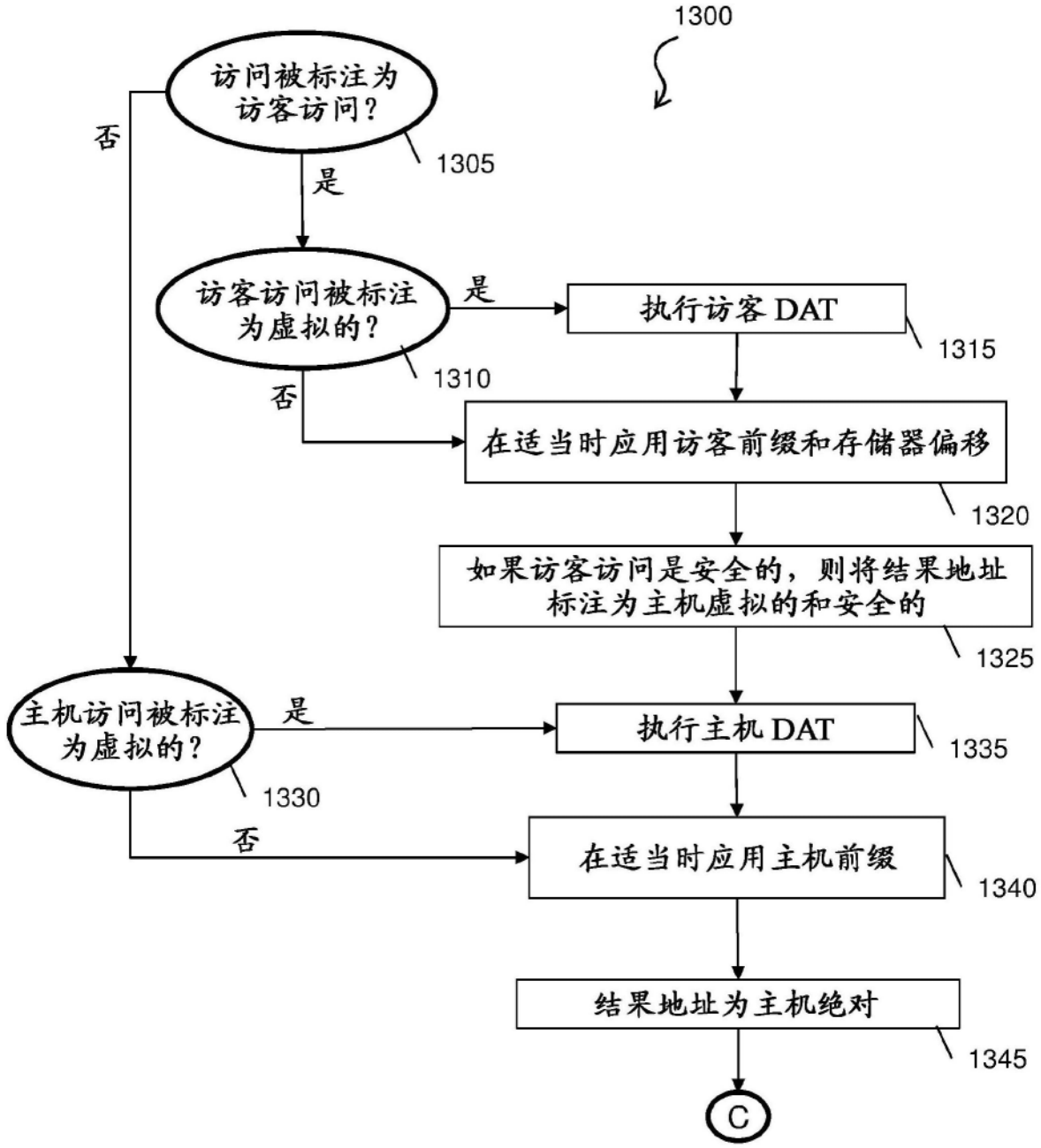
1300
访问被标注为访客访问？
1305
否
是
访客访问被标注为虚拟的？
1310
是
执行访客 DAT
1315
否
在适当时应用访客前缀和存储器偏移
1320
如果访客访问是安全的，则将结果地址标注为主机虚拟的和安全的
1325
主机访问被标注为虚拟的？
1330
是
执行主机 DAT
1335
否
在适当时应用主机前缀
1340
结果地址为主机绝对
1345
C

图13

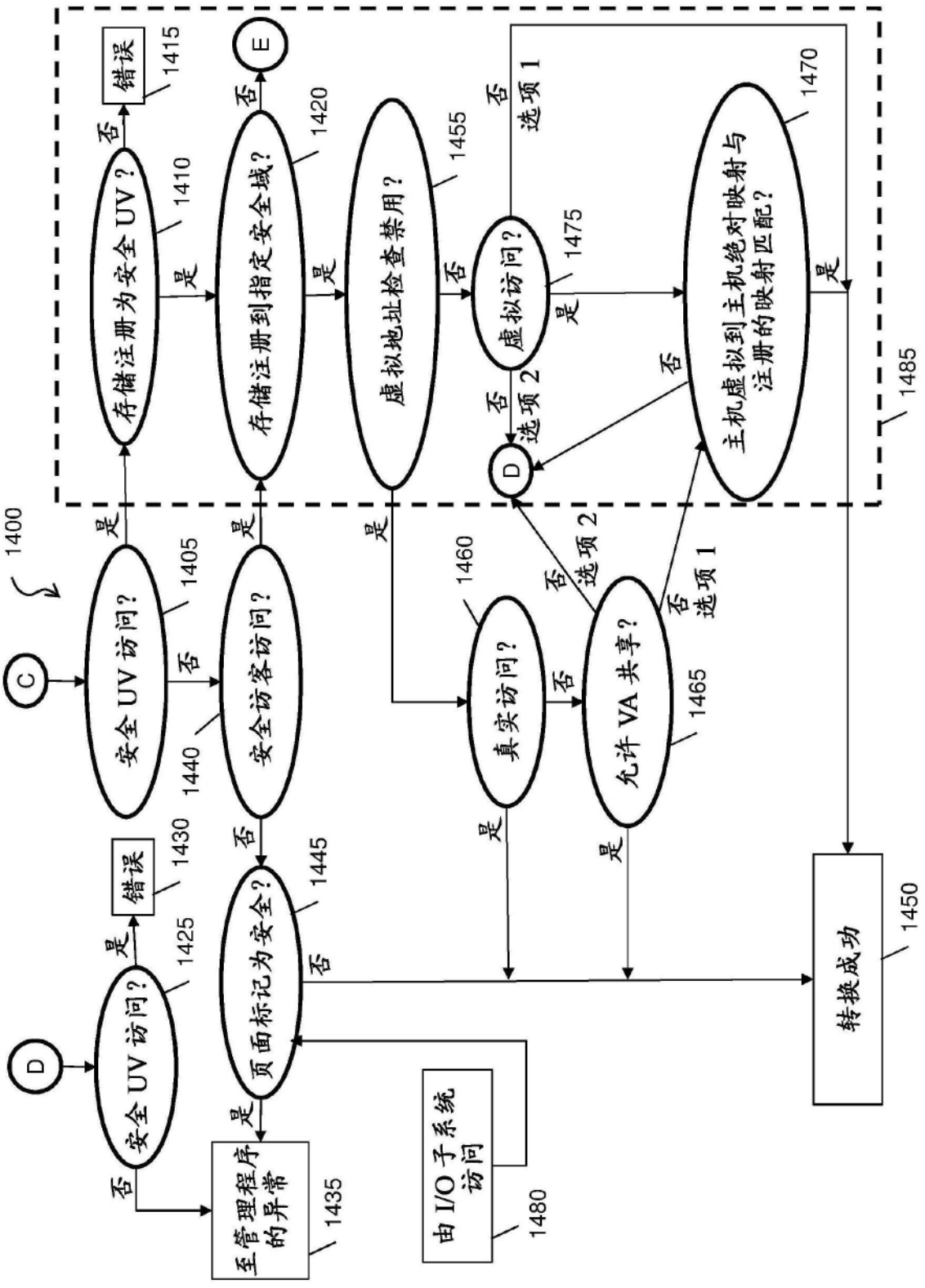
1400
C
安全 UV 访问？
1405
是
否
错误
1430
安全访客访问？
1440
是
否
D
安全 UV 访问？
1425
是
否
错误
1415
存储注册为安全 UV？
1410
是
否
存储注册到指定安全域？
1420
是
否
E
虚拟地址检查禁用？
1455
是
否
虚拟访问？
1475
是
否
选项 1
选项 2
D
主机虚拟到主机绝对映射与注册的映射匹配？
1470
是
否
1485
真实访问？
1460
是
否
允许 VA 共享？
1465
是
否
选项 2
选项 1
页面标记为安全？
1445
是
否
至管理程序的异常
1435
由 I/O 子系统访问
1480
转换成功
1450

图14

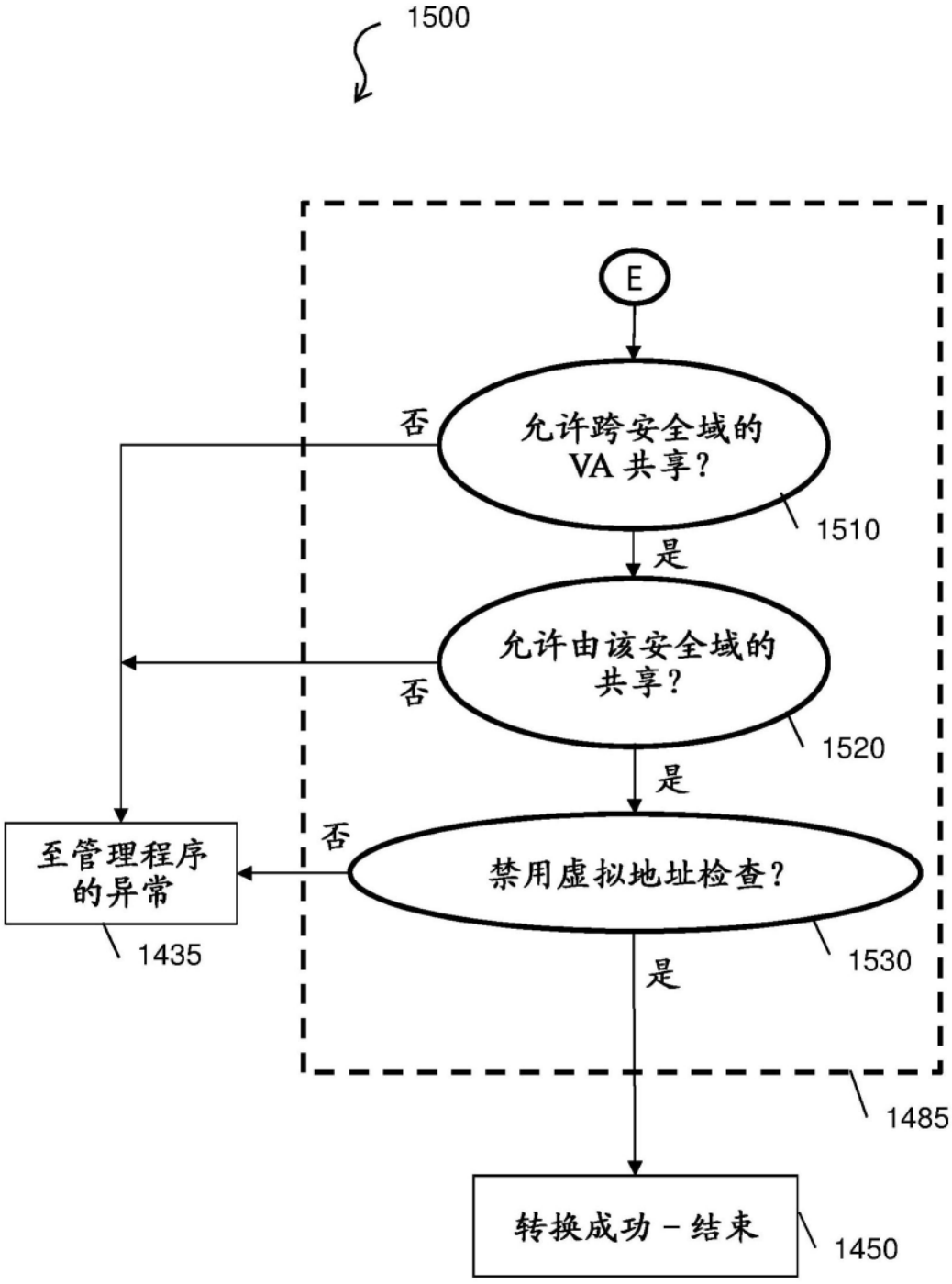
1500
E
允许跨安全域的VA共享?
否
是
1510
允许由该安全域的共享?
否
是
1520
禁用虚拟地址检查?
否
是
1530
至管理程序的异常
1435
1485
转换成功 - 结束
1450

图15

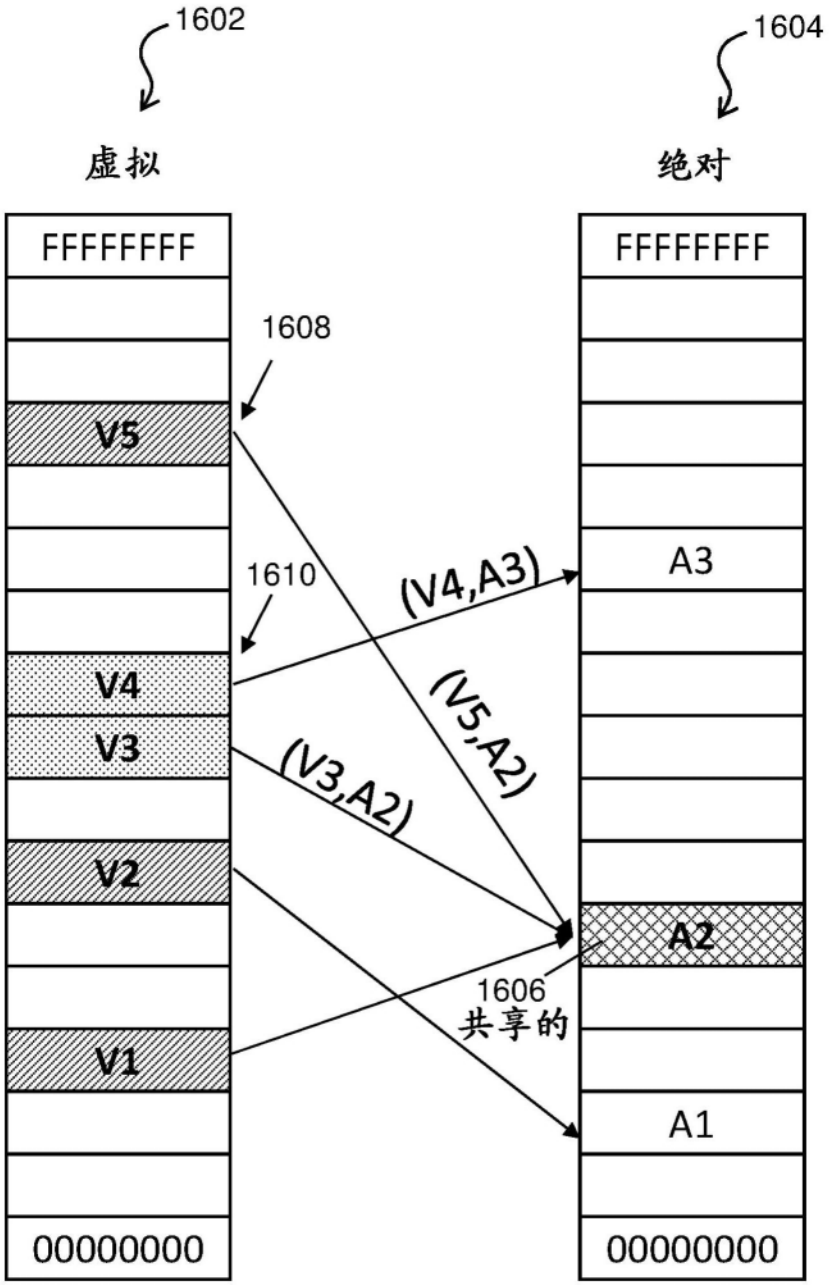
1602
1604
虚拟
绝对
FFFFFFFF
FFFFFFFF
1608
V5
1610
(V4,A3)
A3
V4
(V5,A2)
V3
(V3,A2)
V2
A2
1606
共享的
V1
A1
00000000
00000000

图16

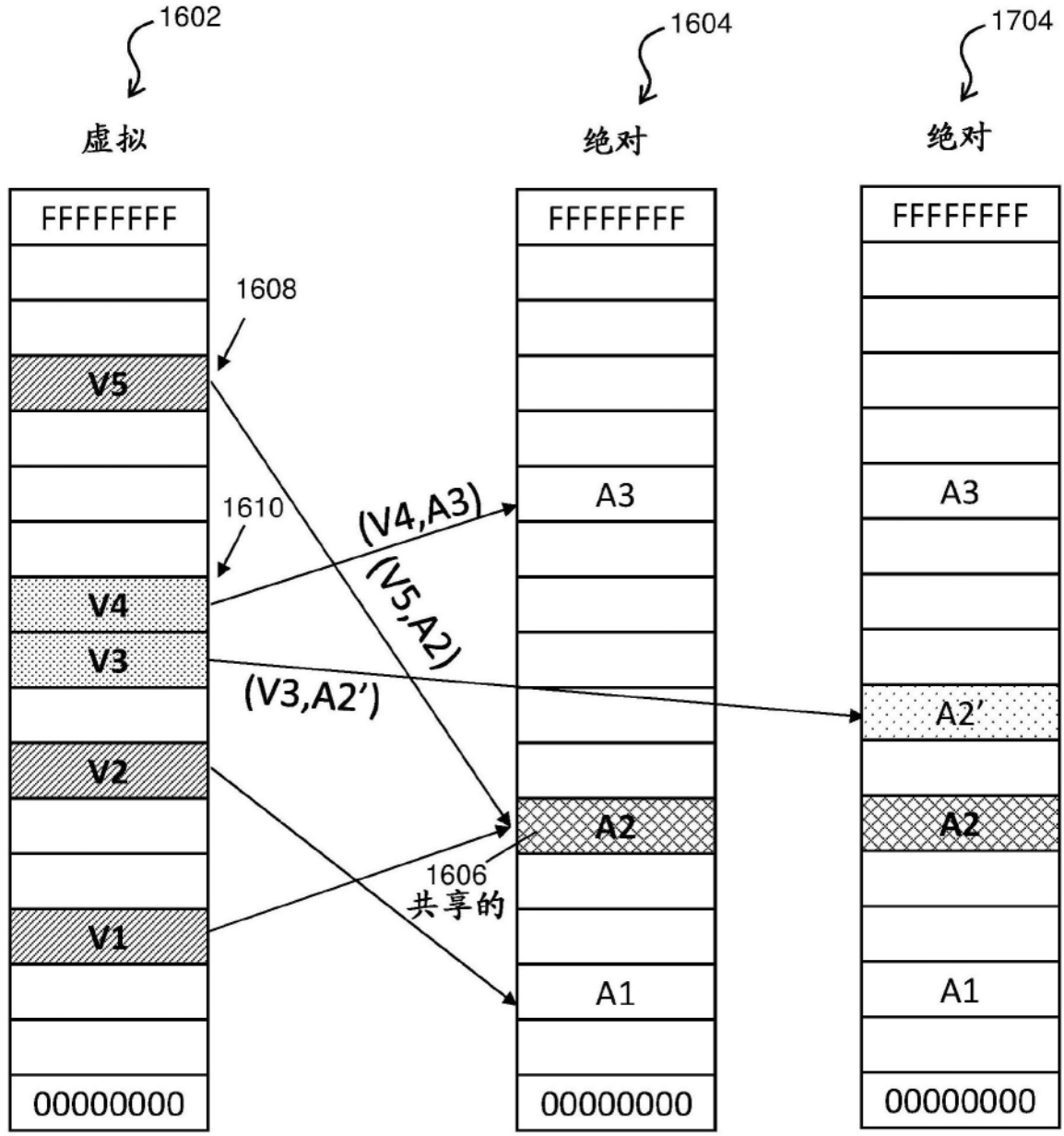
1602
虚拟
1604
绝对
1704
绝对
FFFFFFFF
00000000
V5
V4
V3
V2
V1
1608
1610
(V4,A3)
(V5,A2)
(V3,A2')
1606
共享的
A3
A2
A1
A3
A2'
A2
A1

图17

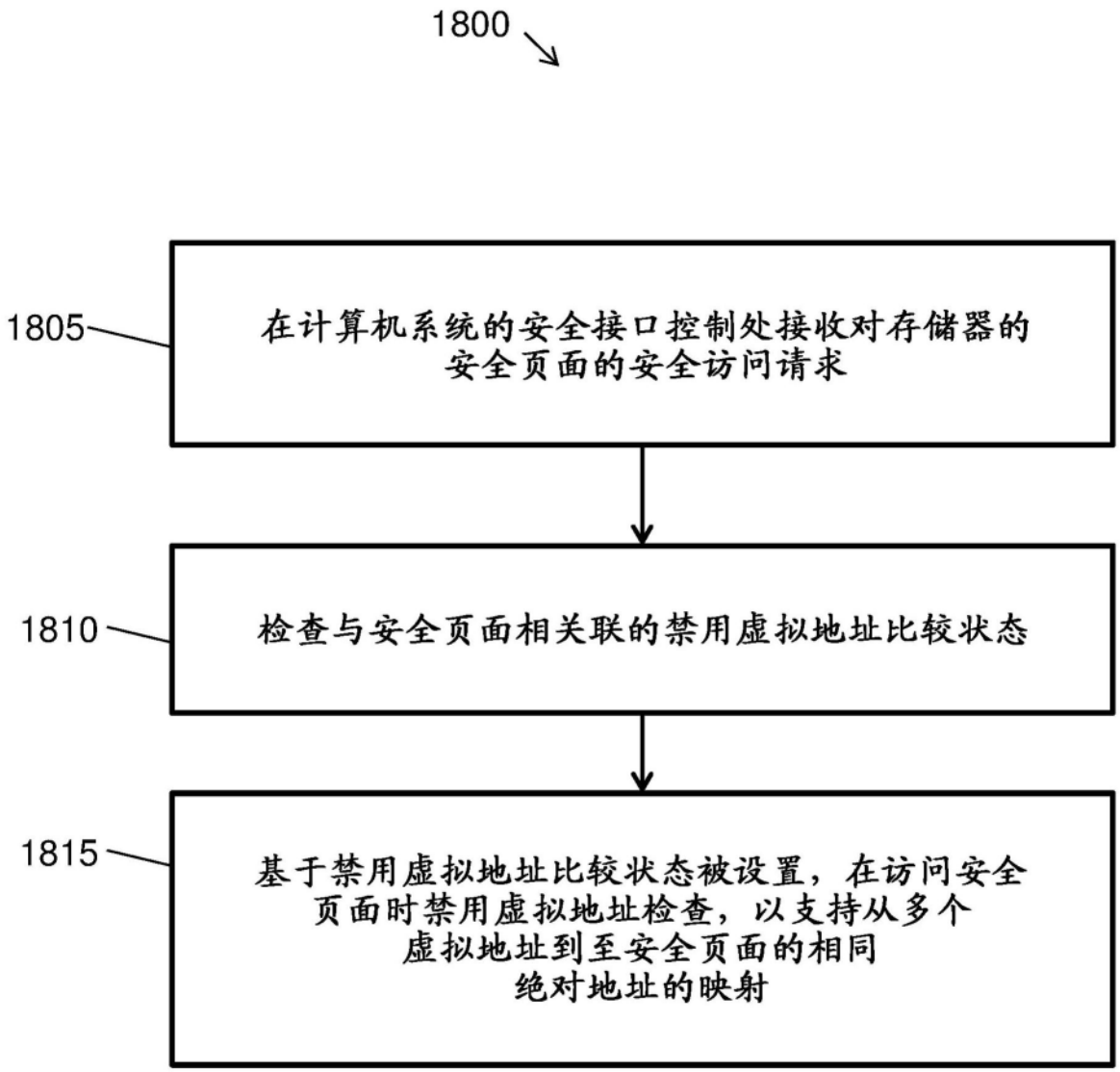
1800
1805
在计算机系统的安全接口控制处接收对存储器的安全页面的安全访问请求
1810
检查与安全页面相关联的禁用虚拟地址比较状态
1815
基于禁用虚拟地址比较状态被设置，在访问安全页面时禁用虚拟地址检查，以支持从多个虚拟地址到至安全页面的相同绝对地址的映射

图18

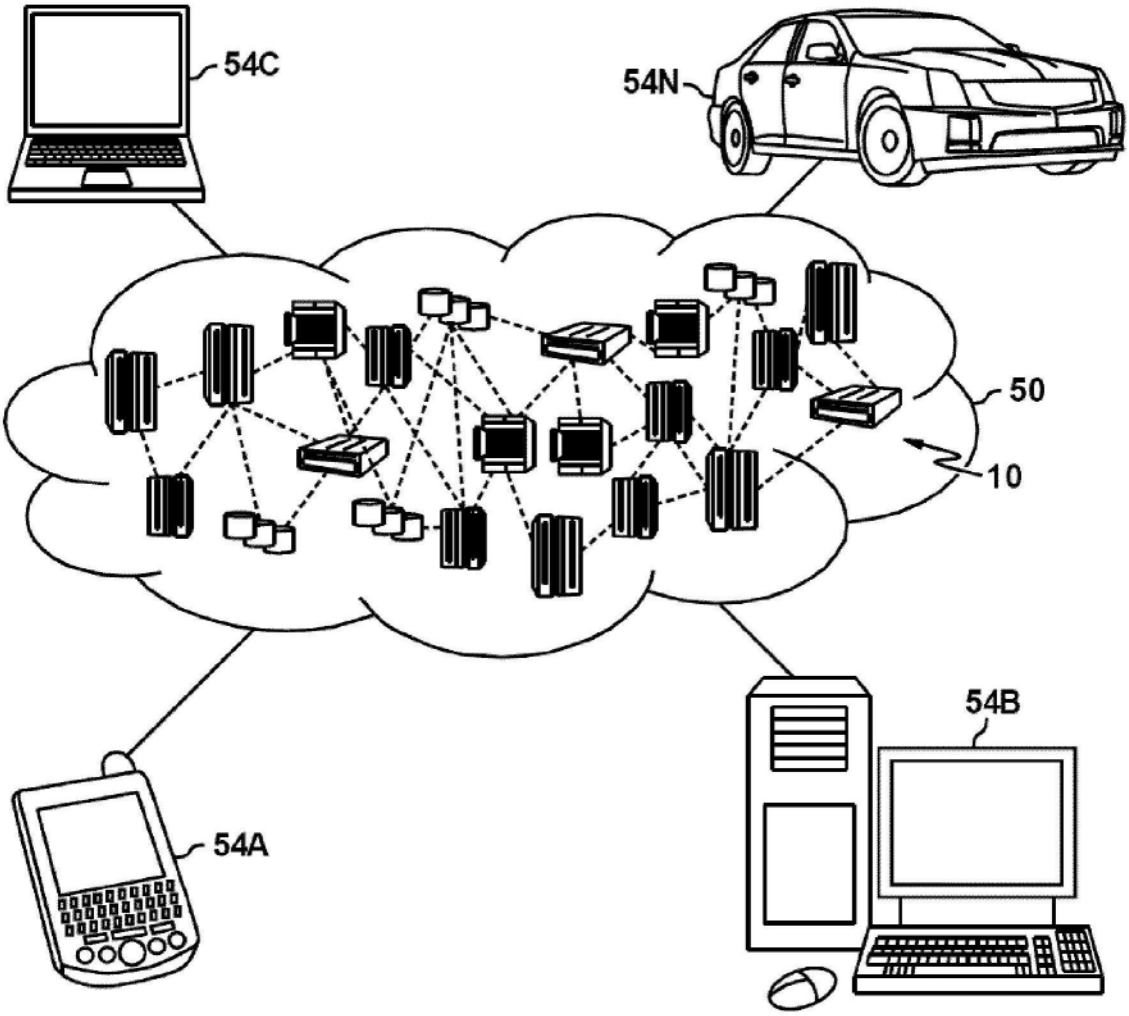

图19

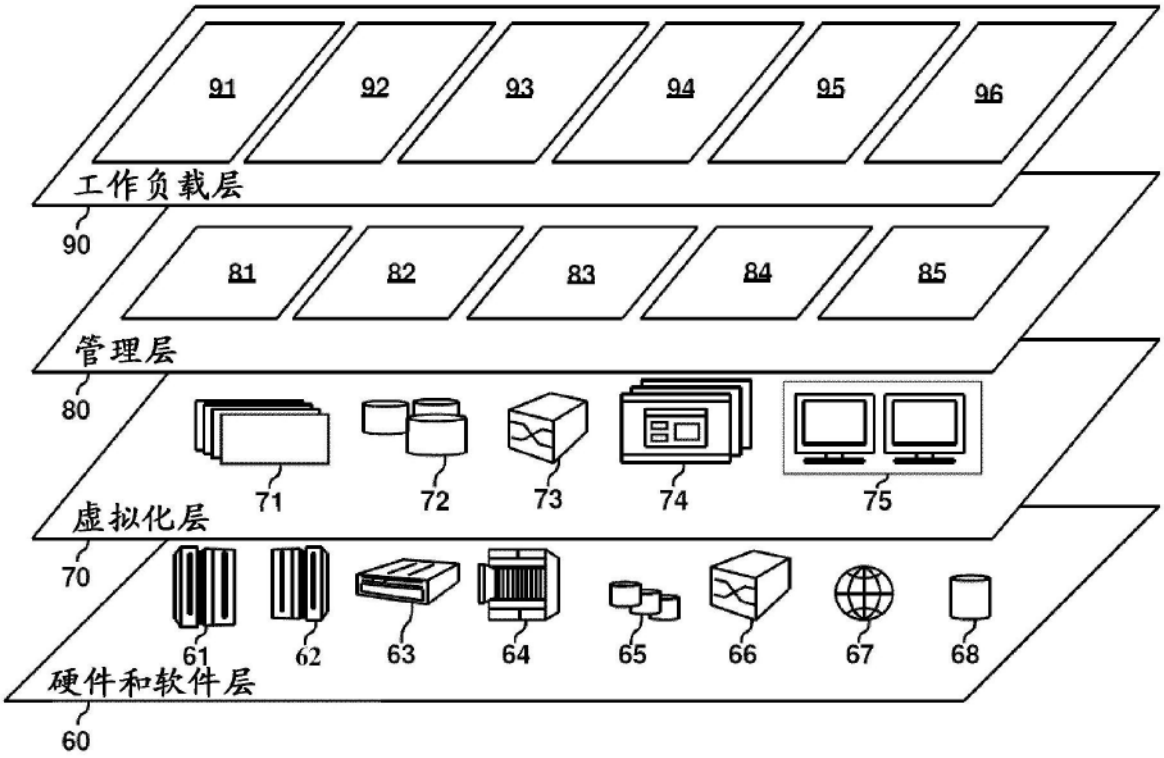
91
92
93
94
95
96
工作负载层
90
81
82
83
84
85
管理层
80
71
72
73
74
75
虚拟化层
70
61
62
63
64
65
66
67
68
硬件和软件层
60

图20

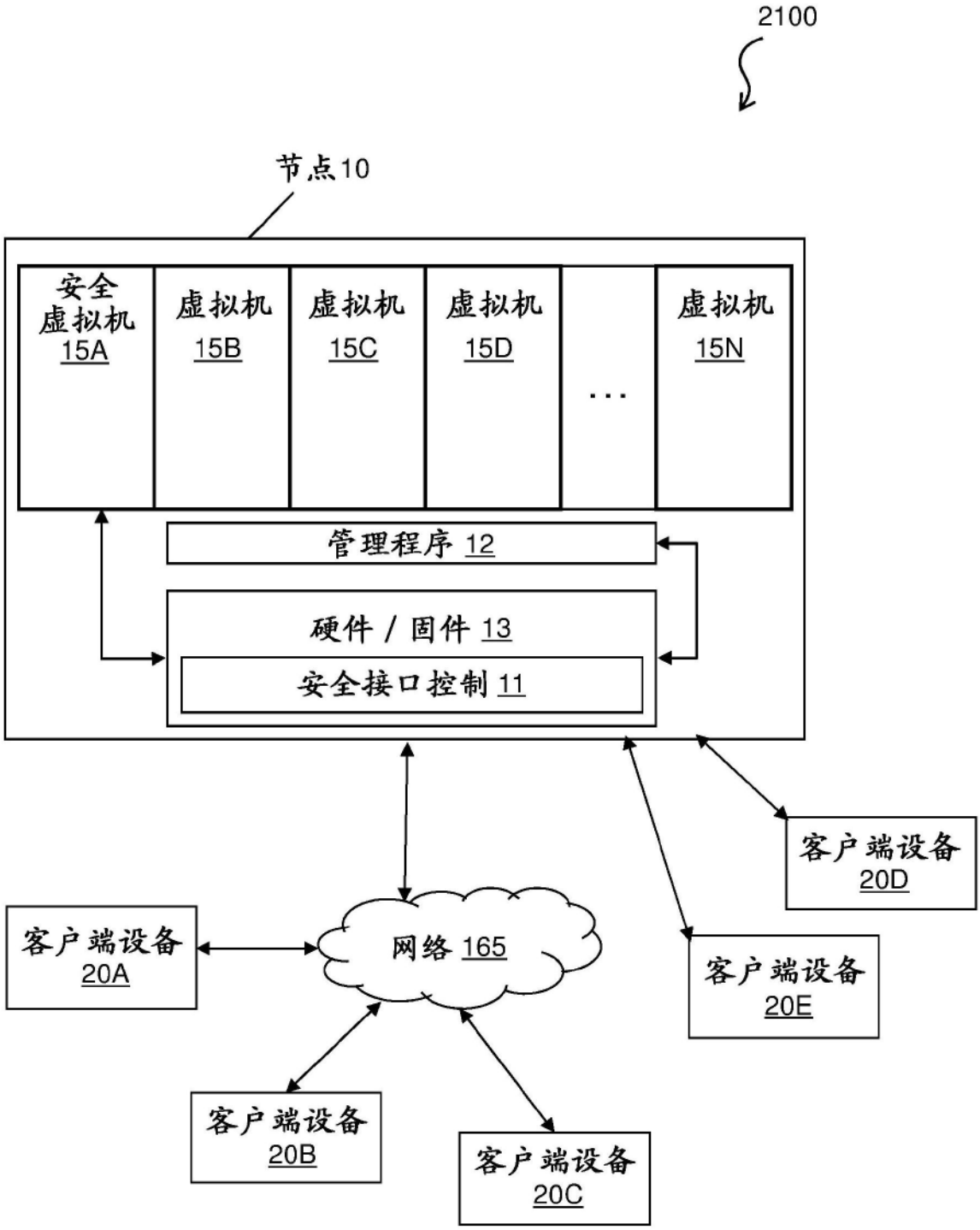
2100
节点10
安全虚拟机 15A
虚拟机 15B
虚拟机 15C
虚拟机 15D
...
虚拟机 15N
管理程序 12
硬件 / 固件 13
安全接口控制 11
客户端设备 20D
客户端设备 20A
网络 165
客户端设备 20E
客户端设备 20B
客户端设备 20C

图21

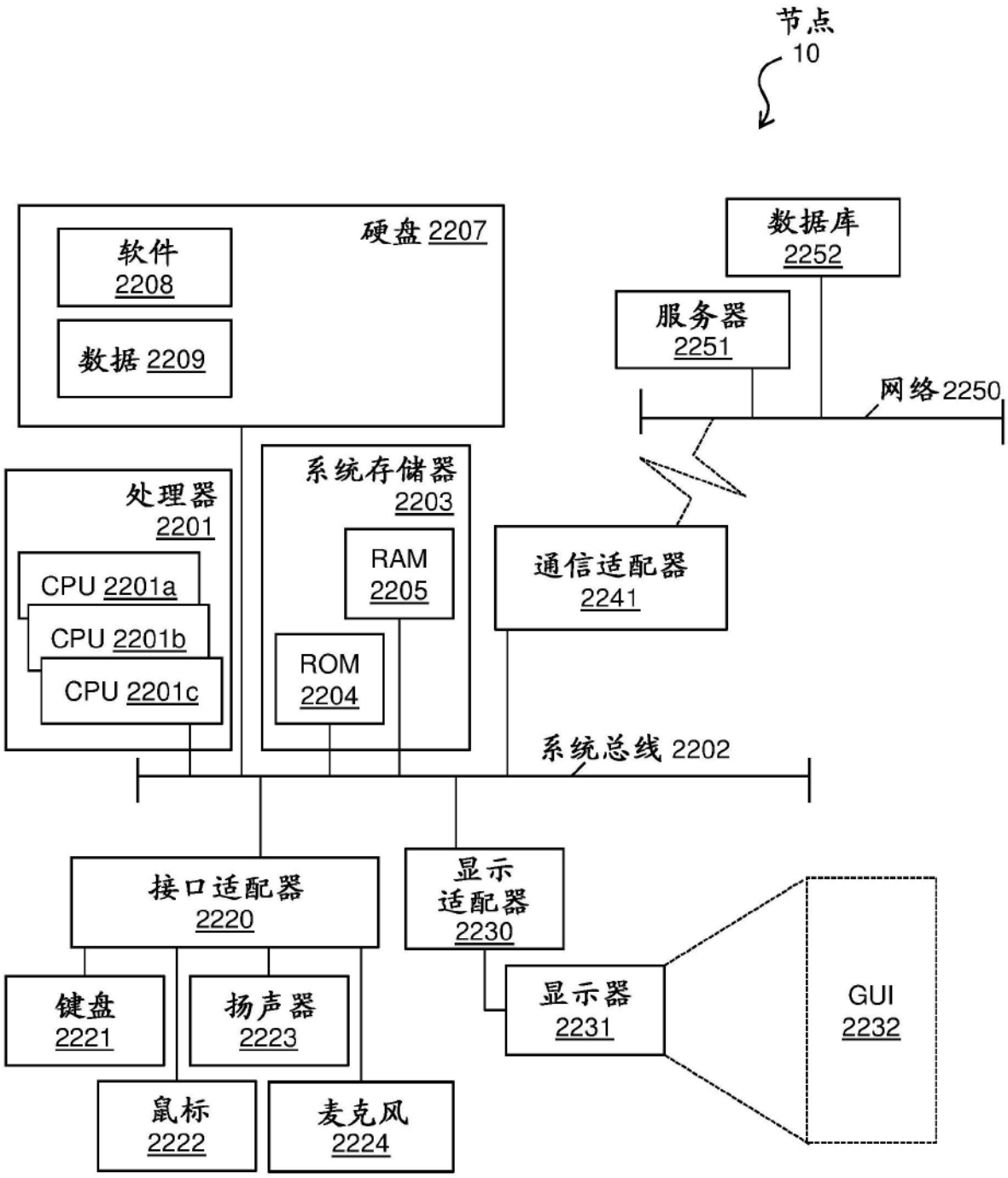
节点
10
硬盘 2207
软件
2208
数据 2209
数据库
2252
服务器
2251
网络 2250
处理器
2201
CPU 2201a
CPU 2201b
CPU 2201c
系统存储器
2203
RAM
2205
ROM
2204
通信适配器
2241
系统总线 2202
接口适配器
2220
显示
适配器
2230
键盘
2221
扬声器
2223
显示器
2231
GUI
2232
鼠标
2222
麦克风
2224

图22