(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102420846 B
(45)授权公告日 2014.07.23

(21)申请号 201110329037.5
(22)申请日 2011.10.14
(30)优先权数据
12/905,889 2010.10.15 US
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 A·拉玛拉铁纳姆 S·帕萨沙拉西 M·迈克尔
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌
(51)Int.Cl.
H04L 29/08(2006.01)
G06F 9/455(2006.01)

(56)对比文件
US 7243369 B2,2007.07.10,
CN 101212374 A,2008.07.02,
US 2007/0107048 A1,2007.05.10,

审查员 高冰

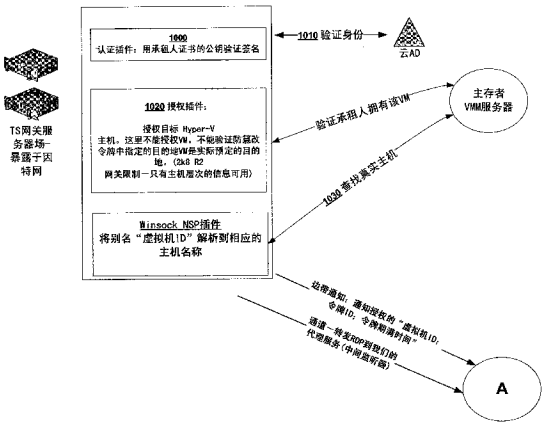
权利要求书2页 说明书20页 附图13页

(54)发明名称

企业用户对主存的虚拟机的远程访问

(57)摘要

本发明涉及企业用户对主存的虚拟机的远程访问。使企业的最终用户能够通过云提供者的虚拟化主机和远程呈现网关接收对公共云中的虚拟机的安全远程呈现访问。企业管理员可从云提供者购买计算容量并将该计算容量在企业最终用户间细分。云提供者不需要为每个最终用户创建影子账户。云提供者AD和企业AD不需要彼此信任。云提供者也不需要将主机信息暴露给承租人。使用终端服务网关处的定制授权插件和虚拟化主机处的间接监听器组件的组合,可提供授权。当客户端连接于远程呈现网关时主机细节可以被抽象,以保护结构免受攻击并使承租人虚拟机能够跨云提供者的虚拟化主机自由移动。



CN 102420846 B

1. 一种用于允许第一域中主存的虚拟机和第二域中的客户端计算机（20）之间的远程呈现会话的方法，所述方法包括：

在所述第二域中的服务器处建立（1202）与所述客户端计算机的通信会话；

由所述服务器接收（1204）指示所述第一域中主存的所述虚拟机的虚拟机标识符；

从所述第二域中的虚拟化管理器接收（1206）包括签署的令牌和公钥的 cookie；

使用所述公钥认证（1208）所述令牌并验证所述令牌映射到所述第一域中的用户账户；

向所述第一域中的虚拟化系统发送（1210）所述虚拟机标识符；

从所述第一域中的所述虚拟化系统接收（1212）所标识的虚拟机是有效的的确认和与所标识的虚拟机相关联的目标资源的身份；

向所述虚拟化系统中的中间监听服务发送（1214）所述虚拟机标识符和所接收的令牌，所述中间监听服务被配置成用作为边带通知而接收的授权的虚拟机标识符来交叉检查所述虚拟机标识符；以及

将远程呈现会话数据转发（1216）到所述中间监听器服务。

2. 如权利要求 1 所述的方法，其特征在于，所述建立还包括通过 HTTPS 隧道建立与所述客户端计算机的连接，其中所述 HTTPS 隧道指定目的地虚拟化服务器和所述中间监听服务的目的地端口。

3. 如权利要求 1 所述的方法，其特征在于，还包括执行主机层次的授权。

4. 如权利要求 1 所述的方法，其特征在于，还包括通过在所述服务器上执行的授权插件查询所述虚拟化服务器，以基于所述令牌确定所述客户端计算机是否被授权访问所述虚拟机。

5. 如权利要求 1 所述的方法，其特征在于，所述签署的令牌包括承租人 ID、令牌 ID、令牌期满时间以及授权的目标虚拟机 ID。

6. 一种用于向第二域中的客户端计算机允许对第一域中主存的虚拟机的访问的系统（1300），包括：

用于接收（1322）第一虚拟机标识符、用公钥签署的令牌、以及对与所述第一虚拟机标识符相关联的虚拟机主机的请求的装置；

用于实例化（1324）与所述客户端计算机的远程呈现会话的装置；

用于经由所述远程呈现会话接收（1326）目标虚拟机标识符并用所述第一虚拟机标识符相关和授权所述目标虚拟机标识符的装置；以及

用于确定（1328）所述目标和第一虚拟机标识符匹配并将经由所述远程呈现会话接收的数据转发到所述目标虚拟机的装置，其中所述第一虚拟机标识符和所述签署的令牌被发送到中间监听服务，所述中间监听服务被配置成用作为边带通知而接收的授权的虚拟机标识符来交叉检查所述第一虚拟机标识符。

7. 如权利要求 6 所述的系统，其特征在于，所述用于转发的装置包括用于在所述第一域中的单端口监听器处经由所述远程呈现会话转发所述数据的装置。

8. 如权利要求 6 所述的系统，其特征在于，所述用于相关和授权的装置还包括用于基于授权存储 XML 中的用户角色策略确定所述第一虚拟机是否具有对所述目标虚拟机的访问权的装置。

9. 如权利要求 8 所述的系统，其特征在于，所述确定是使用 CredSSP 执行的。

10. 一种用于由第二域中的客户端计算机访问第一域中主存的虚拟机的方法，所述方法包括：

与所述第一域中的虚拟化主机建立通信会话；

向所述第一域中的虚拟化主机发送虚拟机标识符和请求对所标识的虚拟机的访问的授权的声明；

从所述第二域中的虚拟化管理器接收签署的令牌；

通过所述第一域中的所述虚拟化主机建立远程呈现会话并发送基于 cookie 的授权将被执行的指示；

向所述第一域中的所述虚拟化主机发送包括签署的令牌和公钥的 cookie，其中虚拟机标识符和所述签署的令牌被发送到中间监听服务，所述中间监听服务被配置成用作为边带通知而接收的授权的虚拟机标识符来交叉检查所述虚拟机标识符；以及

建立与所请求的虚拟机的远程呈现会话。

企业用户对主存的虚拟机的远程访问

技术领域

[0001] 本发明涉及远程呈现系统，尤其涉及企业用户对主存的虚拟机的远程访问。

背景技术

[0002] 联网的一种日益流行的形式一般被称为远程呈现系统，其能使用诸如远程桌面协议（远程呈现）以及独立计算架构（ICA）等协议来与远程客户端共享桌面和在服务器上执行的其他应用。这样的计算系统通常将来自客户端的键盘按压和鼠标点击或选择传送到服务器，通过网络连接在另一方向将屏幕更新转播回去。由此，当实际上仅仅向客户端设备发送如在服务器侧上显现的桌面或应用的屏幕截图时，用户具有好像他的或她的机器正在完全地本地操作的体验。

[0003] 许多向其用户提供虚拟机的企业正在从公共云提供者购买计算容量。云提供者（也被称为公共主存者（public hoster））出售虚拟机形式的计算容量，最终用户在“即用即付（pay as you go）”的基础上为计算容量付费。类似地，企业也能够从这些云提供者购买计算容量以扩展其计算容量。云提供者可使用虚拟化主机来部署虚拟机并向企业承租人出售虚拟机。云提供者的数据中心中的虚拟化主机可被联结到云提供者的域，而承租人（云服务的计算容量的购买者）拥有实际的虚拟机。

[0004] 企业承租人通常有许多用户。承租人可进一步将计算容量细分并将从云租赁的个体虚拟机分配给来自他的企业的个体用户。这些用户需要以类似于他们访问他们的本地计算机的方式访问那些虚拟机。例如，远程桌面协议可被用来访问虚拟机。在服务提供者处，该基础结构可以以对虚拟机的所有远程桌面访问是通过主计算机完成的方式来被设置。

[0005] 通过云提供者提供远程服务可提供一些好处，诸如：

[0006] 1. 即使承租人虚拟机不具有联网设置也可提供访问。

[0007] 2. 可为诸如 Windows、Linux 等多操作系统（OS）虚拟机工作负荷提供访问。

[0008] 3. 在虚拟机上执行人工 / 网络操作系统安装的能力。

[0009] 4. 云提供者的网关和客虚拟机之间的网络连通性是不需要的，从而使得云提供者的网络和承租人的网络能够隔离（客虚拟机可进一步驻留于它们自己的隔离网络中）。

发明内容

[0010] 上述情形的一个问题是，通过云提供者的虚拟化主机对云中的虚拟机的远程呈现访问必须对承租人的企业的最终用户是安全的。

[0011] 在各实施例中，公开了用于使得企业的最终用户能够通过云提供者的虚拟化主机和远程呈现网关接收对主存（hosted）的公共云中的分配的虚拟机的安全远程呈现访问的方法和系统。因此企业管理员可从云提供者购买计算容量并进一步将购买的计算容量在企业最终用户间细分。云提供者不需要为作为计算容量的消费者的企业的每个最终用户创建影子账户。云提供者也不需要将主机信息暴露给承租人。云提供者也不需要将主机信息暴露给互联网。在一实施例中，用 X.509 证书签署的定制令牌可被用来保护远程呈现访问。在

其它实施例中，可使用具有用于身份联盟的安全令牌服务 (STS) 的 SAML 令牌。

[0012] 在一个实施例中，通过使用终端服务网关处的定制授权插件和虚拟化主机处的间接监听器组件的组合，可提供授权。因此企业管理员可以能够进一步细分购买的公共云容量并将承租人虚拟机在最终用户间分配，而不需要公共云提供者（被称为“主存者”）为每个企业最终用户创建影子账户。当客户端连接于远程呈现网关时主机细节还可以被抽象，以保护结构 (fabric) 免受攻击并使承租人虚拟机能够跨云提供者的虚拟化主机自由移动而不影响远程呈现访问。

[0013] 除了上述方面，构成本公开的一部分的权利要求、附图、以及文本还描述了其他方面。本领域技术人员之一可理解，本公开的一个或更多个方面可包括但不限于用于实现本公开的本文所提及的电路和 / 或编程 ；该电路和 / 或编程实质上可以是配置成实现本文所提及的方面的硬件、软件和 / 或固件的任何组合，这取决于系统设计者的设计选择。

[0014] 以上是概述，并且因此必然包含细节的简化、一般化及省略。本领域技术人员将明白，本概述只是说明性的并且决不旨在是限制性的。

附图说明

[0015] 参考附图来进一步描述根据本说明书的用于图形数据传输到远程计算设备的系统、方法和计算机可读介质，在附图中 ：

[0016] 图 1 和 2 描绘了其中可实现本公开的各方面的示例计算机系统。

[0017] 图 3 描绘了用于实施本公开的各方面的虚拟化操作环境。

[0018] 图 4 描绘了用于实施本公开的各方面的虚拟化操作环境。

[0019] 图 5 示出了包括用于实现远程桌面服务的电路的计算机系统。

[0020] 图 6 描绘了用于实施本公开的各方面的操作环境。

[0021] 图 7 描绘了用于实施本公开的各方面的操作环境。

[0022] 图 8 描绘了用于实施本公开的各方面的操作环境。

[0023] 图 9-11 描绘了用于实施本公开的各方面的示例性操作过程。

[0024] 图 12 描绘了用于实施本公开的各方面的示例性操作过程。

[0025] 图 13 描绘了用于实施本公开的各方面的示例性系统和操作过程。

具体实施方式

[0026] 概括的计算环境

[0027] 在以下描述和附图中阐明了某些具体细节，以提供对本公开的各个实施例的全面理解。通常与计算和软件技术相关联的某些公知细节不在以下公开中描述，以避免不必要地使本公开的各实施例晦涩难懂。此外，相关领域的普通技术人员会理解，他们可以无需以下描述的细节中的一个或多个而实现本公开的其它实施例。最后，尽管在以下公开中参考了步骤和序列来描述各个方法，但是如此的描述是为了提供本公开的实施例的清楚实现，且步骤以及步骤序列不应被认为是实现本公开所必需的。

[0028] 应该理解，此处描述的各种技术可以结合硬件或软件，或在适当时结合两者的组合来实现。因此，本公开的方法和装置或其某些方面或部分，可以采用包含在诸如软盘、CD-ROM、硬盘驱动器或任何其它机器可读存储介质等有形介质中的程序代码（即，指令）的

形式，其中，当程序代码被加载至诸如计算机等机器并由其执行时，该机器成为用于实践本公开的装置。在程序代码在可编程计算机上执行的情况下，计算设备通常包括处理器、该处理器可读的存储介质（包括易失性和非易失性存储器和／或存储元件）、至少一个输入设备、以及至少一个输出设备。一个或多个程序可以例如通过使用应用编程接口 (API)、可重用控件等来实现或利用结合本公开描述的过程。这样的程序优选地用高级过程语言或面向对象的编程语言来实现，以与计算机系统通信。然而，如果需要，程序可以用汇编语言或机器语言来实现。在任何情形中，语言可以是编译的语言或解释的语言，且与硬件实现相结合。

[0029] 远程桌面系统是维护可由客户端计算机系统远程地执行的应用和操作系统的计算机系统。输入是在客户端计算机系统处被输入的，并通过网络（例如，使用基于国际电信联盟 (ITU)T.120 系列协议等协议，如远程桌面协议（远程呈现））传送到终端服务器上的应用。该应用如同该输入是在终端服务器处被输入那样来处理该输入。该应用响应于所接收到的输入来生成输出，并且通过网络将该输出传送到客户端。

[0030] 各实施例可在一个或多个计算机上执行。图 1 和 2 以及下面的讨论旨在提供其中可实现本公开的合适的计算环境的简要概括描述。本领域的技术人员可以理解，计算机系统 200、300 可具有参照图 1 和 2 的计算机 100 描述的组件中的一部分或全部。

[0031] 贯穿本公开使用的术语电路可包括诸如硬件中断控制器、硬盘驱动器、网络适配器、图形处理器、基于硬件的视频／音频编解码器等硬件组件，以及用于操作这些硬件的固件／软件。术语电路还可包括被配置成通过固件或通过开关集来以特定方式执行功能的微处理器，或一个或多个逻辑处理器，例如，多核通用处理单元的一个或多个核。此示例中的逻辑处理器可以通过从存储器，例如，RAM、ROM、固件和／或虚拟存储器中加载的体现可操作以执行功能的逻辑的软件指令来配置。在其中电路包括硬件和软件的组合的示例实施例中，实现者可以编写具体化逻辑的源代码，该源代码随后被编译成可由逻辑处理器执行的机器可读代码。因为本领域技术人员可以明白现有技术已经进化到硬件、软件或硬件／软件的组合之间几乎没有差别的地步，因而选择硬件还是软件来实现功能只是一个设计选择。因此，由于本领域的技术人员可以理解软件进程可被变换成等效的硬件结构，且硬件结构本身可被变换成等效的软件进程，因此选择硬件实现或是软件实现是无足轻重的且留给了实现者。

[0032] 图 1 描绘了以本公开的各方面来配置的计算系统的示例。计算系统可包括计算机 20 等等，其中包括处理单元 21、系统存储器 22，以及将包括系统存储器在内的各种系统组件耦合到处理单元 21 的系统总线 23。系统总线 23 可以是若干类型的总线结构中的任一种，包括使用各种总线体系结构中的任一种的存储器总线或存储器控制器、外围总线、以及局部总线。系统存储器包括只读存储器 (ROM)24 和随机存取存储器 (RAM)25。基本输入／输出系统 26(BIOS) 被存储在 ROM 24 中，该基本输入／输出系统 26 包含了诸如在启动期间帮助在计算机 20 内的元件之间传输信息的基本例程。计算机 20 还可以包括用于读写硬盘（未示出）的硬盘驱动器 27、用于读写可移动磁盘 29 的磁盘驱动器 28，以及用于读写诸如 CD ROM 或其他光学介质之类的可移动光盘 31 的光盘驱动器 30。在一些示例实施例中，实施本公开的各方面的计算机可执行指令可存储在 ROM 24、硬盘（未示出）、RAM 25、可移动磁盘 29、光盘 31 和／或处理单元 21 的高速缓存中。硬盘驱动器 27、磁盘驱动器 28，以及光

盘驱动器 30 分别通过硬盘驱动器接口 32、磁盘驱动器接口 33，以及光盘驱动器接口 34 连接到系统总线 23。驱动器以及它们相关联的计算机可读介质为计算机 20 提供了对计算机可读指令、数据结构、程序模块，及其他数据的非易失性存储。虽然此处所描述的环境使用了硬盘、可移动磁盘 29、以及可移动光盘 31，但是，那些本领域普通技术人员应该理解，在操作环境中也可以使用诸如盒式磁带、闪存卡、数字视频盘、伯努利磁带盒、随机存取存储器 (RAM)、只读存储器 (ROM) 等等之类的可以存储可由计算机进行访问的数据的其他类型的计算机可读介质。

[0033] 可以有若干个程序模块存储在硬盘、磁盘 29、光盘 31、ROM 24 或 RAM 25 上，包括操作系统 35、一个或多个应用程序 36、其他程序模块 37、以及程序数据 38。用户可以通过诸如键盘 40 和定点设备 42 之类的输入设备向计算机 20 中输入命令和信息。其他输入设备（未示出）可包括话筒、游戏杆、游戏手柄、圆盘式卫星天线、扫描仪等等。这些及其他输入设备常常通过耦合到系统总线的串行端口接口 46 连接到处理单元 21，但是，也可以通过诸如并行端口、游戏端口、通用串行总线 (USB) 端口之类的其他接口来连接。显示器 47 或其他类型的显示设备也可以通过诸如视频适配器 48 之类的接口连接到系统总线 23。除了显示器 47 之外，计算机通常还包括其他外围输出设备（未示出），如扬声器和打印机。图 1 的系统也包括主机适配器 55、小型计算机系统接口 (SCSI) 总线 56，以及连接到 SCSI 总线 56 的外部存储设备 62。

[0034] 计算机 20 可以使用到一个或多个远程计算机（如远程计算机 49）的逻辑连接，以在联网环境中操作。远程计算机 49 可以是另一计算机、服务器、路由器、网络 PC、对等设备或其他常见的网络节点、虚拟机，并通常包括上文相对于计算机 20 所描述的许多或全部元件，但是在图 1 中只示出了存储器存储设备 50。图 1 中所描绘的逻辑连接可包括局域网 (LAN)51 和广域网 (WAN)52。这样的联网环境在办公室、企业范围的计算机网络、内联网和因特网中是普遍的。

[0035] 当用于 LAN 网络环境中时，计算机 20 可通过网络接口或适配器 53 连接到 LAN 51。当用于 WAN 网络环境中时，计算机 20 通常包括调制解调器 54，或用于通过诸如因特网之类的广域网 52 建立通信的其他手段。可以是内置的或外置的调制解调器 54 可通过串行端口接口 46 连接到系统总线 23。在联网环境中，相对于计算机 20 所描述的程序模块或其部分可被存储在远程存储器存储设备中。可以理解，所示出的网络连接只是示例，也可以使用用于在计算机之间建立通信链路的其他手段。此外，虽然可构想本发明的许多实施例尤其适用于计算机系统，然而在本文中不意味着将本公开限于这些实施例。

[0036] 现在参考图 2，描绘了示例性计算系统 100 的另一实施例。计算机系统 100 可包括逻辑处理器 102，如执行核。尽管示出了一个逻辑处理器 102，但在其他实施例中，计算机系统 100 可具有多个逻辑处理器，例如每一处理器基板有多个执行核，和 / 或各自可具有多个执行核的多个处理器基板。如图所示，各种计算机可读存储介质 110 可由一个或多个系统总线互联，系统总线将各种系统组件耦合到逻辑处理器 102。系统总线可以是几种类型的总线结构中的任何一种，包括存储器总线或存储器控制器、外围总线、以及使用各种总线体系结构中的任一种的局部总线。在示例实施例中，计算机可读存储介质 110 可以包括例如随机存取存储器 (RAM)104、存储设备 106（例如电机硬盘驱动器、固态硬盘驱动器等）、固件 108（例如闪速 RAM 或 ROM）、以及可移动存储设备 118（例如 CD-ROM、软盘、DVD、闪速驱动

器、外部存储设备等）。本领域的技术人员应当理解，可使用其他类型的计算机可读存储介质，如磁带盒、闪存卡、数字视频盘、柏努利盒式磁带。

[0037] 计算机可读存储介质为计算机 100 提供了对处理器可执行指令 122、数据结构、程序模块和其他数据的非易失性存储。基本输入 / 输出系统 (BIOS)120 可被存储在固件 108 中，它包含帮助在诸如启动期间在计算机系统 100 内的各元件之间传递信息的基本例程。若干个程序可被存储在固件 108、存储设备 106、RAM 104 和 / 或可移动存储设备 118 上，并且可由逻辑处理器 102 来执行，包括操作系统和 / 或应用程序。

[0038] 命令和信息可由计算机 100 通过输入设备 116 来接收，输入设备可包括但不限于键盘和定点设备。其他输入设备可以包括话筒、操纵杆、游戏手柄、扫描仪等等。这些和其他输入设备常通过耦合到系统总线的串行端口接口连接到逻辑处理器 102，但也可通过其他接口连接，如并行端口、游戏端口或通用串行总线 (USB)。显示器或其他类型的显示设备也可经由诸如视频适配器等可以是图形处理器 112 的一部分或可连接到图形处理器 112 的接口来连接到系统总线。除了显示器之外，计算机通常包括其他外围输出设备（未示出），如扬声器和打印机。图 1 的示例性系统还可包括主适配器、小型计算机系统接口 (SCSI) 总线和连接到 SCSI 总线的外部存储设备。

[0039] 计算机系统 100 可使用至一个或多个远程计算机，如远程计算机，的逻辑连接在网络化环境中操作。远程计算机可以是另一计算机、服务器、路由器、网络 PC、对等设备或其他常见的网络节点，并且通常包括上面关于计算机系统 100 所述的许多或全部元件。

[0040] 当在 LAN 或 WAN 联网环境中使用时，计算机系统 100 可通过网络接口卡 114 连接至 LAN 或 WAN。NIC 114（可以是内部或外部的）可以连接到系统总线。在联网环境中，相对于计算机系统 100 所描述的程序模块或其部分可被储存在远程存储器存储设备中。可以理解，所描述的网络连接是示例性的，且可以使用在计算机之间建立通信链路的其他手段。此外，虽然可构想本公开的许多实施例尤其适用于计算机化的系统，然而在本文中没有任何表述旨在将本公开限于那些实施例。

[0041] 远程桌面系统是维护可由客户端计算机系统远程地执行的应用的计算机系统。输入是在客户端计算机系统处被输入的，并通过网络（例如，使用基于国际电信联盟 (ITU) T.120 系列协议等协议，如远程桌面协议（远程呈现））传送到终端服务器上的应用。该应用如同该输入是在终端服务器处输入的那样来处理该输入。该应用响应于所接收到的输入生成输出，并且该输出通过网络传送到客户端计算机系统。客户端计算机系统呈现输出数据。由此，在客户端计算机系统处接收输入并呈现输出，而处理实际上是在终端服务器处发生的。会话可包括命令行界面 (shell) 和诸如桌面之类的用户界面、跟踪该桌面内的鼠标移动的子系统、将图标上的鼠标点击转换成实现程序实例的命令的子系统等等。在另一示例实施例中，会话可包括应用。在该示例中，当呈现应用时，桌面环境仍可被生成并对用户隐藏。应当理解，前述讨论是示例性的，且当前公开的主题可以在各种客户端 / 服务器环境中实现且不限于特定终端服务产品。

[0042] 即使不是全部也是在大多数远程桌面环境中，输入数据（在客户端计算机系统处输入）通常包括表示对应用的命令的鼠标和键盘数据，且输出数据（由终端服务器处的应用生成）通常包括用于在视频输出设备上显示的视频数据。许多远程桌面环境也包括扩展到传输其他类型的数据的功能。

[0043] 通过允许插件经由远程呈现连接传输数据，可使用通信信道来来扩展远程呈现协议。存在许多这样的扩展。诸如打印机重定向、剪贴板重定向、端口重定向等特征使用通信信道技术。由此，除了输入和输出数据之外，可以有许多需要传输数据的通信信道。因此，可能有传输输出数据的偶然请求和传输其他数据的一个或多个信道请求争用可用的网络带宽。

[0044] 转向图 3，示出了可被用来生成虚拟机的示例性虚拟机服务器。在该实施例中，系统管理程序 (hypervisor) 微内核 302 可被配置成控制并仲裁对计算机系统 300 的硬件的访问。系统管理程序微内核 302 可以隔离一个分区中的进程，使其不能访问另一分区的资源。例如，系统管理程序微内核 302 可以生成称为分区的执行环境，如子分区 1 到子分区 N（其中 N 是大于 1 的整数）。在该实施例中，子分区是系统管理程序微内核 302 支持的基本隔离单元。每一子分区可被映射到在系统管理程序微内核 302 控制之下的一组硬件资源，例如，存储器、设备、逻辑处理器周期等。在各实施例中，系统管理程序微内核 302 可以是独立的软件产品、操作系统的一部分、嵌入在主板的固件中、专用集成电路、或其组合。

[0045] 系统管理程序微内核 302 可以通过限制客操作系统对物理计算机系统中的存储器的视图来实施分区划分。当系统管理程序微内核 302 实例化一虚拟机时，它可以将系统物理存储器 (SPM) 的页（例如，具有开始和结束地址的固定长度存储器块）分配给虚拟机作为客物理存储器 (GPM)。在该实施例中，客机对系统存储器的受限视图受系统管理程序微内核 302 控制。术语“客物理存储器”是从虚拟机的观点描述存储器页的简写方式，且术语“系统物理存储器”是从物理系统的观点描述存储器页的简写方式。因此，被分配给虚拟机的存储器页会有客物理地址（虚拟机所使用的地址）和系统物理地址（页的实际地址）。

[0046] 客操作系统可以虚拟化客物理存储器。虚拟存储器是一种管理技术，其允许操作系统过度提交存储器，并且给予应用对连续工作存储器的唯一访问。在虚拟化环境中，客操作系统可以使用一个或多个页表来将被称为虚拟客地址的虚拟地址转换成客物理地址。在该示例中，存储器地址可以具有客虚拟地址、客物理地址以及系统物理地址。

[0047] 在所描绘的示例中，父分区组件（也可被认为是类似于 Xen 的开源系统管理程序的域 0）可以包括主机 304。主机 304 可以是操作系统（或一组配置实用程序），并且主机 304 可以被配置成通过使用虚拟化服务提供者 328(VSP) 向在子分区 1-N 中执行的客操作系统提供资源。VSP 328（一般在开源社区中被称为后端驱动程序）可用来通过虚拟化服务客户端 (VSC)（在开源社区或类虚拟化设备中一般称为前端驱动程序）对到硬件资源的接口进行多路复用。如图所示，虚拟化服务客户端可以在客操作系统的上下文中执行。然而，这些驱动程序不同于客机中的其余驱动程序，因为向它们提供了系统管理程序而非客机。在一示例性实施例中，虚拟化服务提供者 328 与虚拟化服务客户端 316 和 318 通信所使用的路径可以被认为是虚拟化路径。

[0048] 如图所示，仿真器 334（例如虚拟化 IDE 设备、虚拟化视频适配器、虚拟化 NIC 等）可被配置成在主机 304 中运行并被附连到对客操作系统 330 和 322 可用的资源。例如，当客操作系统接触被映射到设备的寄存器的所处位置的存储器位置或接触被映射到设备的存储器时，微内核系统管理程序 302 可截取该请求并将客机试图写入的值传递给相关联的仿真器。在该示例中，资源可被认为是虚拟设备所处的位置。仿真器的以这种方式的使用可以被认为是仿真路径。仿真路径与虚拟化路径相比是低效的，因为与在 VSP 和 VSC 之间

传递消息相比，它需要更多的CPU资源来仿真设备。例如，可以将经由仿真路径把值写入盘所需的、被映射至寄存器的存储器上的几百个动作减少为在虚拟化路径中从VSC被传递至VSP的单个消息。

[0049] 每一子分区可包括一个或多个虚拟处理器(320和322)，客操作系统(320和322)可管理并调度线程以在这些虚拟处理器上执行。一般而言，虚拟处理器是提供具有特定架构的物理处理器的表示的可执行指令以及相关联的状态信息。例如，一个虚拟机可具有带有英特尔x86处理器特性的虚拟处理器，而另一虚拟处理器可具有PowerPC处理器的特性。本示例中的虚拟处理器可被映射到计算机系统的逻辑处理器，使得实现虚拟处理器的指令将受到逻辑处理器的支持。由此，在包括多个逻辑处理器的实施例中，各虚拟处理器可以由各逻辑处理器同时执行，同时例如其他逻辑处理器执行系统管理程序指令。分区中虚拟处理器和存储器的组合可被认为是虚拟机。

[0050] 客操作系统(320和322)可以是任何操作系统，如来自微软®、苹果®、开源社区等的操作系统。客操作系统可包括用户/内核操作模式，并且可具有能包括调度器、存储器管理器等的内核。一般而言，内核模式可包括逻辑处理器中的执行模式，该执行模式授予对至少特权处理器指令的访问权。每一客操作系统可具有相关联的文件系统，该文件系统上存储有诸如终端服务器、电子商务服务器、电子邮件服务器等应用以及客操作系统本身。客操作系统可调度线程来在虚拟处理器上执行，并且可实现此类应用的实例。

[0051] 现在参考图4，示出的是基于一种替代架构的虚拟机服务器。图4描绘了与图3的组件相类似的组件；然而，在本示例实施方式中，系统管理程序402可包括微内核组件以及和图3的主机304中的组件(如虚拟化服务提供者328和设备驱动程序324)相类似的组件，而管理操作系统404可包含例如用于配置系统管理程序402的配置实用程序。在本架构中，系统管理程序402可以执行与图3的系统管理程序微内核302相同或相似的功能；然而，在本架构中，系统管理程序404可被配置成向在子分区中执行的客操作系统提供资源。图4的系统管理程序402可以是独立的软件产品、操作系统的一部分、嵌入在主板的固件内，或者系统管理程序402的一部分可以由专用集成电路来实现。

[0052] 现在参考图5，示出的是虚拟桌面服务器500的高层次框图。在一实施例中，虚拟桌面服务器500可以被配置成将虚拟桌面会话(VDS)部署到客户端，例如，诸如智能电话等移动设备、具有和图1所示组件相似的组件的计算机系统等等。简言之，虚拟桌面技术使用户能与虚拟机中运行的客操作系统远程地交互。不同于远程桌面会话，在虚拟桌面会话中，只有一个用户登录到客操作系统中并且对其具有总控制，例如，用户可以作为管理员运行并且在该客机上具有完全权限。在所示示例中，虚拟桌面服务器500可以具有与图3或图4的计算机系统300或400类似的组件。在所示示例中，虚拟化平台502是如上在图3和图4中所述的虚拟化基础结构组件的逻辑抽象。在以下章节中被描述为在虚拟化平台502“以内”的功能可以在图3或图4中描绘的一个或多个元件中实现。例如，虚拟桌面管理器530可以在图3的主机304中实现。更具体而言，虚拟桌面管理器530可以在虚拟化环境的父分区中运行的主操作系统中实现。

[0053] 启动虚拟桌面会话要求在虚拟机内对客操作系统进行实例化。在一示例性实施例中，虚拟桌面管理器530(例如，处理器可执行指令的模块)可以响应于请求而启动虚拟机514(连同客操作系统528)。虚拟桌面管理器530可以在逻辑处理器上执行，并且可以指示

虚拟化平台 502(例如微内核系统管理程序 202)为分区分配存储器。虚拟化平台 502 可以在虚拟机 514 内执行并设置虚拟设备,并且将引导加载程序加载到虚拟机存储器中。引导加载程序可以在虚拟处理器上执行并且加载客操作系统 528。例如,可以加载会话管理器 508,会话管理器 508 可以实例化诸如运行时子系统 526 等环境子系统,运行时子系统 526 可以包括诸如操作系统核 510 等内核模式部分。例如,在一实施例中,环境子系统可以被配置成将服务的子集暴露给应用程序并提供到内核 520 的接入点。当加载客操作系统 528 时,引导加载程序可以退出,并将对虚拟机的控制转交给客操作系统 528。客操作系统 528 可以执行图 5 所示的各个模块,并且将其自身配置为主存虚拟桌面会话。例如,客操作系统 528 可以包括使远程呈现引擎 506 和 / 或配置服务 534 在引导时启动的注册表值。

[0054] 虚拟桌面会话可以在客操作系统 528 通过网络从客户端接收到连接请求时启动。连接请求首先可由远程呈现引擎 506 处理。远程呈现引擎 506 可以被配置成监听连接消息并将它们转发至会话管理器 508。如图 3 所示,当会话被生成时,远程呈现引擎 506 可以运行该会话的协议栈实例。一般而言,协议栈实例可被配置成将用户界面输出路由到相关联的客户端、以及将从相关联的客户端接收到的用户输入路由到操作系统核 510。简言之,操作系统核 510 可以被配置成管理屏幕输出 ;收集来自键盘、鼠标和其它设备的输入。

[0055] 用户凭证(如用户名 / 密码组合)可由远程呈现引擎 506 接收并被传递至会话管理器 508。会话管理器 508 可以将凭证传递至登录过程,登录过程可以将凭证路由至认证引擎 524 以进行验证。认证引擎 524 可以生成系统令牌,系统令牌可以在每当用户尝试执行一进程时使用以确定用户是否具有运行该进程或线程的安全凭证。例如,当进程或线程尝试获得访问时(例如,打开、关闭、删除和 / 或修改例如文件、设置或应用等对象),线程或进程可由安全子系统 522 来认证。安全子系统 522 可以对照与对象相关联的访问控制列表来检查系统令牌,并且基于系统令牌中的信息与访问控制列表的比较来确定线程是否具有许可。如果安全子系统 522 确定线程被授权,则允许该线程访问对象。

[0056] 继续对图 5 的描述,在一实施例中,操作系统核 510 可以包括图形显示接口 516(GDI) 和输入子系统 512。在一示例实施例中,输入子系统 512 可以被配置成经由虚拟桌面会话的协议栈实例从客户端接收用户输入,并将该输入发送至操作系统核 510。在一些实施例中,用户输入可包括指示绝对和 / 或相对鼠标移动命令、鼠标坐标、鼠标点击、键盘信号、操纵杆移动信号等的信号。例如在图标上的鼠标双击等用户输入可被操作系统核 510 接收,并且输入子系统 512 可被配置成确定图标位于与该双击相关联的坐标处。输入子系统 512 随后可被配置成向可执行与该图标相关联的应用的进程的运行时子系统 526 发送通知。

[0057] 绘制命令可从应用和 / 或桌面被接收,并由 GDI 516 处理。GDI 516 一般可包括能生成图形对象绘制命令的进程。在本示例实施例中,GDI 516 可以被配置成将命令传递给远程显示子系统 518,该远程显示子系统 518 可为该会话实例化显示驱动程序。在一示例实施例中,远程显示子系统 518 可被配置成包括虚拟显示驱动程序,该虚拟显示驱动程序可被配置成接收绘制命令并将它们发送至客户端。

[0058] 图 5 中还示出配置服务 534。在一示例性实施例中,配置服务 534 可被用来设置客操作系统 528 以便在客户端连接前实施虚拟桌面会话。例如,配置服务 534 可以在客操作系统 528 内运行,并且在客操作系统 528 引导时执行。由于特定的配置设置需要管理特权,

因此可以将配置服务 534 配置成作为具有系统范围特权的进程来运行。配置服务 534 可采取的一些示例性动作包括但不限于以下动作 :将用户的帐户标识符添加至客操作系统 528 的管理用户列表,将帐户标识符添加至授权的虚拟桌面用户列表,设置注册表值,开启客操作系统防火墙,以及将远程呈现引擎 506 监听连接的端口打开。在以下段落中更详细地描述了配置服务 534。

[0059] 在一示例性实施例中,可以在虚拟化平台 502 和客操作系统 528 之间建立通信信道以便配置和控制客操作系统 528。由于远程用户可以对虚拟机 514 具有完全控制,因此需要有安全性,以确保用于配置和控制客操作系统 528 的任何信道不能也用来攻击虚拟化平台 502 或连接到内部网络的其它计算机系统。传统上,使用联网的通信信道来设置和控制客操作系统 528。然而,当客操作系统 528 不与虚拟化平台 502 处于同一网络域中时,网络信道难以部署,且虚拟化平台 502 被配置成拒绝来自该域外的传入的连接请求。

[0060] 在一示例性实施例中,可以使用分区间通信信道 504 来与配置服务器 534 通信,以便配置和 / 或管理虚拟桌面会话。分区间通信信道 504 可以被配置成由虚拟机 514 隐式地信任,而不被虚拟化平台 502 所信任。在本示例中,可以将例如数据和 / 或命令等信息容易地路由至客操作系统 528,而无需验证该信息。另一方面,可以在虚拟化平台 502 采取动作之前,验证和认证从虚拟机 514 接收到的数据。而且,由于分区间通信信道 504 不使用联网,所以客操作系统 528 可以被排除在内部网络以外。

[0061] 分区间通信信道 504 可以被虚拟机 514 隐式地信任 (即,经由该信道接收到的信息是固有地已认证 / 确认的),因为只有虚拟化平台 502 可以创建分区间通信信道 504。例如,在一实施例中,可以将分区间通信信道 504 至少部分地实现为在虚拟机 514 和虚拟化平台 502 之间共享的存储器区域。虚拟化平台 502 可使指示环形缓冲区等等的数据结构在可被用作虚拟化平台 502 和虚拟机 514 之间的全双工通信信道的共享的存储器区域中被创建。在一示例性实施例中,分区间通信信道可以包括在题为“Partition Bus(分区总线)”、专利号为 7,689,800 的美国专利中描述的特征,该专利的内容通过引用被完全结合于此。

[0062] 虚拟化平台 502 可以将信息写至可由虚拟机 514 读取的分区间通信信道 504。在一示例性实施例中,分区间通信信道 504 可以是基于消息的。也就是说,虚拟化平台 502 和虚拟机 514 可以被配置成将数据分组写至分区间通信信道 504。在同一个或另一个示例性实施例中,分区间通信信道 504 可以是事件驱动的。在此配置中,当信息被写入该信道时,可以指示接收者通过例如图 3 的系统管理程序 302 来从分区间通信信道 504 读取信息。

[0063] 现在参见图 6,示出的是数据中心的高层次框图,数据中心包括 :虚拟桌面服务器 500、虚拟桌面服务器 602、许可服务器 604、代理服务器 608、网关 612 和客户端 614。数据中心可被配置成向客户端部署虚拟桌面会话。在所示例子中,虚拟化平台 502、虚拟桌面服务器 602、许可服务器 604、代理服务器 608 和网关 612 可以是内联网的一部分,用于登录到这些计算机中的用户凭证可以是同一域 (即基础结构域 520) 的成员。基础结构域 520 以虚线示出,将虚拟桌面服务器 500 切成两半,以说明在一示例性实施例中,虚拟机 514 可以是一个不同的域的一部分,或者不是任何域的部分。而且,虚拟机 514 可以是不同的网络的一部分或者完全不是网络的一部分。

[0064] 数据中心可以包括内部网络,该内部网络将多个虚拟桌面服务器 (602 和 500) 耦合到代理服务器 608 和许可服务器 604,其中虚拟桌面服务器可包括类似于图 3 或 4 所示

组件的组件。如本领域的技术人员可理解的，尽管示出了两个虚拟桌面服务器，但数据中心可具有更多个虚拟桌面服务器。而且，尽管虚拟桌面服务器 500 被示出为运行一个虚拟机(514)，但是每个虚拟桌面服务器可以同时主存许多虚拟机。或者换句话说，数据中心可以有 M 个虚拟桌面服务器（其中 M 是大于 1 的整数），该 M 个虚拟化主机的每一个可以主存 N 个虚拟机（其中 N 也是大于 1 的整数）。

[0065] 代理服务器 608 可以充当客户端 614 到内联网的接口。简言之，代理服务器 608 可以包括与针对图 2 所述的组件相似的组件。代理服务器 608 可以具有将其接口到诸如因特网等公共网络的网络适配器，以及将其接口到内部网络（即，内联网）的另一网络适配器。在本示例中，代理服务器 608 可以充当内部网络的网关，从而允许虚拟桌面服务器和许可服务器 604 保持在公共网络之外。

[0066] 当客户端 614 的用户想要虚拟桌面会话时，他或她可以点击图标，而客户端 614 可以将一个或多个信息分组发送至代理服务器 608。代理服务器 608 可以包括软件指令模块，软件指令在执行时使逻辑处理器选择适当的虚拟化主机来实例化一虚拟机以主存虚拟桌面会话。可以收集用户凭证（例如用户名和密码组合），而代理服务器 608 可以检查会话数据库 610 以确定数据中心是否包括与诸如用户名 / 密码组合这样的用户凭证相关联的任何断开的虚拟桌面会话。如果会话数据库 610 包括与用户凭证相关联的断开的虚拟桌面会话，则代理服务器 608 可以向具有该断开的会话的虚拟化主机发送信号并指示它执行该虚拟机。如果会话数据库 610 不具有指示关于用户的断开的会话的信息，则代理服务器 608 可以选择适当的虚拟桌面服务器，例如，一个具有可用来实例化虚拟机以主存虚拟桌面会话的资源的服务器。

[0067] 虚拟化平台 502 可以实例化虚拟机 514，并且在虚拟处理器上执行客操作系统 528。回过头参考图 5，客操作系统 528 可以运行远程呈现引擎 506 ；将虚拟 NIC 616 的网际协议 (IP) 地址返回至代理服务器 608 ；并且等待来自客户端 614 的连接。代理服务器 608 可以在信息分组中将虚拟 NIC 616 的 IP 地址返回至客户端 614，该信息分组使客户端 614 的逻辑处理器将客户端重定向至 IP 地址虚拟机 514。网关 612 可以接收该连接请求并将它转发至虚拟 NIC 616。

[0068] 在至少一个示例性实施例中，会话管理器 508 可以被配置成检查客户端 614 在启动虚拟桌面会话之前是否与有效的许可证相关联。远程呈现引擎 506 可以从客户端 614 接收许可证（或与许可证相关联的信息），并将该信息发送至虚拟化平台 502，虚拟化平台 502 可以将许可证（或与许可证相关联的信息）发送至许可服务器 604。许可服务器 604 可以包括许可证确认引擎 606，许可证确认引擎 606 可以被配置成确定与客户端 614 相关联的许可证是否有效。如果许可证是有效的，许可证确认引擎 606 可以将信号发回虚拟桌面服务器 500，而虚拟桌面会话可被启动。在这一点上，远程呈现引擎 506 可以将指示客操作系统 528 的图形用户界面的一个或多个信息分组流式传送到客户端 614，并且从客户端 614 接收指示用户输入的一个或多个信息分组。

[0069] 在一示例性实施例中，当虚拟化平台 502 从代理服务器 608 接收请求以实例化虚拟机时，虚拟桌面管理器 530 可以执行命令和 / 或信息，并且经由分区间通信信道 504 将命令和 / 或信息发送至虚拟机 514 以使客操作系统 528 被配置成进行虚拟桌面会话。配置服务 534 可以接收该命令和 / 或信息，并且相应地配置客操作系统 528。例如，虚拟桌面管理

器 530 可以发送 :尝试连接的用户的身份、保护客操作系统 528 的防火墙的所需设置、注册表值、允许用户操作的应用的列表、用来启用虚拟桌面会话并且用来将用户的身份添加至授权的虚拟桌面用户列表的命令等等。配置服务 534 可以在虚拟处理器上执行并且改变适当的设置。

[0070] 一旦虚拟桌面会话在运行时,虚拟桌面管理器 530 就可以经由分区间通信信道 504 来管理运行的虚拟桌面会话。例如,虚拟桌面管理器 530 可以向虚拟机 514 发布命令,诸如使客操作系统 528 关闭、断开用户、重置客操作系统 528 等的命令。在同一个或另一个实施例中,虚拟桌面管理器 530 可以管理虚拟桌面会话,接收虚拟机 514 的状态信息、来自远程呈现引擎 506 的状况信息,并且 / 或者将控制虚拟桌面会话的命令发送至配置服务 534。例如,虚拟桌面管理器 530 可以接收虚拟机 514 的指示虚拟机 514 是否在运行、暂停、就绪、引导的状态信息,以及可被发送至客户端的 IP 地址列表。此外,虚拟桌面管理器 530 可以接收客操作系统 528 的状况信息,诸如登录到虚拟桌面会话的用户的身份,并且可以将该信息的一些或全部传送至代理服务器 608。

[0071] 图 7 描绘了其中客户端具有包括与多个服务器的远程会话的工作空间的示例系统。

[0072] 图 7 中所描绘的计算机可与图 1 中所描绘的计算机类似。在图 7 中,客户端 702 与部署 700 通信,部署 700 包括认证服务器 704、连接代理 706、网关 708、远程应用服务器场 714(远程应用服务器场进一步包括两个同样配置的服务器 :远程应用服务器 716a-b)、以及 VM 服务器场 710(VM 服务器场进一步包括两个同样配置的 VM :VM 712a-b)。

[0073] 客户端 702 具有包括由远程应用服务器 716 和 VM 712 中的一个或多个供应的多个远程资源的工作空间。客户端 702 可通过认证服务器 704 登入其工作空间。一旦被认证,客户端的连接至其工作空间的请求被从认证服务器 704 发送至连接代理 706。连接代理 706 被配置成代理客户端 702 与应用服务器 716 和 VM 712 之间的将向客户端 702 供应远程资源的连接,并且为此,连接代理 706 被配置成与应用服务器 716 和 VM 712 通信以确定它们当前正供应什么资源 (包括客户端 702 的用户的断开的远程资源)。

[0074] 客户端 702 可具有包括多个远程资源——包括来自远程应用服务器 716a 的远程应用的远程资源以及包括来自 VM 712a 的 VM 的远程资源——的工作空间。如所描绘的,客户端 702 不具有关于远程应用服务器 716b 或 VM 712b 的远程资源。这些远程资源可各自服务于不同应用或桌面、各版本的应用、或其它置换。例如,远程应用服务器 716a 可向客户端 702 供应远程文字处理应用,而 VM 712 可向客户端 702 供应远程桌面。

[0075] 通过这一说明可知,当用户想要重新连接回他或她的工作空间时,他可能想要通过一条命令重新连接至远程应用服务器 716a 和 VM 712a 两者的远程资源,而不是通过执行三次的一条命令。用户可从客户端 702 或从另一客户端计算机执行这一重新连接操作 (诸如当客户端 702 是用户在工作场所的计算机,而用户想要在周末时从家中的计算机重新连接)。

[0076] 图 8 描绘了用于客户端重新连接至工作空间的远程资源的示例通信流。

[0077] 图 8 描绘了一系统中的示例通信流,其中客户端重新连接包括与多个服务器的远程会话的工作空间。这一通信流可实现在诸如图 7 中所描绘的计算机系统之类的系统中。即,图 8 的远程部署 800、客户端 802、认证服务器 804、连接代理 806、网关 808、VM 场 810

和 VM 812a 可分别与图 7 的远程部署 200、客户端 202、认证服务器 204、连接代理 206、网关 208、VM 场 210 和 VM 212a 类似。

[0078] 客户端 802 的用户之前已具有到远程服务器场 800 的工作空间，该工作空间涉及访问来自 VM 812a 的远程资源，并且该工作空间现在被断开。在客户端 802 尝试重新连接至部署 800 之前，认证服务器 804（经由通信 (1)）向客户端 802 发布文档，该文档标识客户端 802 可用来访问部署 800 的远程资源的、关于部署 800 的信息。客户端 802 稍后通过将通信 (2) 发送给认证服务器 804 来重新连接。认证服务器 804 验证用户和 / 或客户端的凭证（诸如账户和密码）。若凭证被验证，认证服务器 804 与连接代理 806 通信以确定当重新连接到客户端 802 的工作空间时客户端 802 将要重新连接到哪些远程资源（此处为 VM812a）。认证服务器 804 通过向连接代理 806 发送通信 (3) 并作为响应在通信 (4) 中接收回客户端 802 要重新连接到的服务器场（此处为 VM 场 810）的列表来做出这一确定。在通信 (4) 中指示的这一信息由认证服务器 804 在通信 (5) 中传递给客户端 802。

[0079] 当客户端 802 从认证服务器 804 得到了要重新连接到的服务器的列表时，客户端 802 与那些服务器场中的每一个重新建立通信。如图 8 中所描绘的，该服务器场是 VM 场 810。客户端 802 没有直接接触连接代理 806 或 VM 场 810 的能力。因此网关 808 被用在联网环境的边缘以协助该请求并越过网络边界。客户端 802 与网关 808 通信 (6) 以访问这些服务器场的远程资源。网关 808 处理通信 (6)，并进而与通信代理 806 通信 (7) 以传递类似的信息。连接代理 806 从通信 (7) 获取服务器场的标识，并从该标识来标识具有该断开的远程资源的场 810 内的机器 (VM 812a)。连接代理 806 发送通信 (8) 至 VM 812a，指示 VM 812a 将该远程资源重新连接至客户端 802。通过发送指示同一内容的通信 (9) 至网关 808，VM 812a 与客户端 802 重新连接，而网关 808 又进而发送指示同一内容的通信 (10) 至客户端 802。

[0080] 可以理解，这是用于突出本发明的简化图示，并且可存在和 / 或连接至更多或更少的服务器场，并且可更多涉及所传递的通信（例如，示出的是通信 (9) 和 (10) 建立 VM 812a 和客户端 802 之间的重新连接，而这也可涉及从客户端 802 经网关 808 发送给 VM 812a 的通信）。

[0081] 用于实现上面提到的虚拟机的所有这些变型只是示例性实现，且本文没有任何表述应被解释为将本公开限制于任何特定的虚拟化方面。

[0082] 企业用户对主存虚拟机的远程访问

[0083] 许多向其用户提供虚拟机的企业正在从公共云提供者购买计算容量。云提供者（也被称为公共主存者 (public hoster)）出售虚拟机形式的计算容量，终端用户在“即用即付 (pay as you go)”的基础上为计算容量付费。类似地，企业也能够从这些云提供者购买计算容量以扩展其计算容量。云提供者可使用虚拟化主机来部署虚拟机并向企业承租人出售虚拟机。云提供者的数据中心中的虚拟化主机可被联结到云提供者的域，而承租人（云服务的计算容量的购买者）拥有实际的虚拟机。

[0084] 企业承租人通常有许多用户。承租人可进一步将计算容量细分并将从云租赁的个体虚拟机分配给来自他的企业的个体用户。这些用户需要以类似于他们访问他们的本地计算机的方式访问那些虚拟机。例如，远程桌面协议可被用来访问虚拟机。在服务提供者处，该基础结构可以以对虚拟机的所有远程桌面访问都是通过主计算机来完成的方式被设置。

[0085] 如上所述，域可以是共享中央目录数据库的计算机的逻辑分组。这个中央目录（例如，活动目录 (Active Directory)）含有用户账户和用于那个域中的资源的安全信息。域内的每个用户可接收唯一账户或用户名。然后可向这个账户分配对该域内的资源的访问。根据位置、组织结构或其它因素，可将域内的计算机分配为组织单位。计算机可使用 VPN 连接经由 LAN 或经由 WAN 连接到域。该域可为认证机构提供支持以确认身份。

[0086] 通过云提供者提供远程服务可提供一些好处，诸如：

[0087] 1. 即使承租人虚拟机不具有联网设置也可提供访问。

[0088] 2. 可为诸如 Window、Linux 等多操作系统 (OS) 虚拟机工作负荷提供访问。

[0089] 3. 在虚拟机上执行人工 / 网络操作系统安装的能力。

[0090] 4. 云提供者的网关和客虚拟机之间的网络连通性是不需要的，从而使得云提供者的网络和承租人的网络能够隔离（客虚拟机可在它们自己的隔离网络中）。

[0091] 上述情形的一个问题是，通过云提供者的虚拟化主机对云中的虚拟机的远程呈现访问必须对承租人企业的最终用户是安全的。通常使用来自主存者的域的凭证来保护这些虚拟机。然而，虚拟机的实际消费者（例如，客户端）没有对那些凭证的访问权，因为对此虚拟机的访问权是被分委托 (sub-delegate) 给它们的。

[0092] 在各实施例中，公开了用于使得企业的终端用户能够通过云提供者的虚拟化主机和远程呈现网关接收对主存 (hosted) 的公共云中的分配的虚拟机的安全远程呈现访问的方法和系统。因此企业管理员可从云提供者购买计算容量并进一步将购买的计算容量在企业最终用户间细分。云提供者不需要为企业的每个最终用户创建影子账户。云提供者也不需要将主机信息暴露给承租人。在一实施例中，可使用用 X.509 证书签署的定制令牌。在其它实施例中，可使用具有用于身份联盟的 STS 的 SAML 令牌。

[0093] 在一个实施例中，通过使用终端服务网关处的定制授权插件和虚拟化主机处的间接监听器组件的组合，可提供授权。因此企业管理员可以能够进一步细分购买的公共云容量并将承租人虚拟机在最终用户间分配，而不为每个最终用户创建影子账户。当客户端连接于远程呈现网关时主机细节还可以被抽象，以保护主存者的结构免受攻击并使承租人虚拟机能够跨云提供者的虚拟化主机自由移动。

[0094] 在各实施例中，可并入下述特征。

[0095] 1. 可使用 SAML 令牌 /STS 或定制令牌 /X.509 证书。安全断言标记语言 (SAML) 是一种用于在安全域之间交换认证和授权数据的基于 XML 的标准。安全域通常是身份提供者和服务提供者。X.509 是一种用于单点登录 (single sign-on(SSO)) 和特权管理基础结构 (PMI) 的公钥基础结构的 ITU-T 标准。

[0096] 2. 云提供者不需要为企业的每个最终用户在云提供者的活动目录中创建影子账户。

[0097] 3. 从云提供者购买容量的企业管理员可进一步将云资源在企业的最终用户间细分。每个最终用户应当只能访问由企业管理员分配给该用户的虚拟机。云提供者将虚拟机分配给企业管理员而企业管理员进而又将虚拟机在该企业的最终用户间细分。最终用户不能直接访问虚拟机。

[0098] 4. 云提供者不需要暴露主机信息。承租人虚拟机可在云提供者的虚拟化主机内自由迁移。

[0099] 5. 云提供者的主机不直接暴露于互联网，而且将通过远程呈现网关被掩蔽。

[0100] 6. 企业的最终用户客户端不使用代理通过企业服务器，但与云提供者的远程呈现网关直接通信。

[0101] 7. 承租人虚拟机可以在它们自己的隔离网络中，或者可以是任何其它的网络配置，包括完全没有网络连接。

[0102] 8. 远程桌面通信数据可以是 SSL/TLS 加密的。

[0103] 9. 应当支持多承租人情形。远程呈现网关应当在不同承租人间共享。许多企业可从服务提供者购买容量并充当承租人。而且，这些企业可以在它们各自的最终用户间细分该容量。

[0104] 10. 该方案应当是可缩放的。

[0105] 自服务门户可以是将虚拟机的管理扩展到最终用户的 web 组件。自服务门户可以是在虚拟化系统之上构建的可扩展组件。自服务门户可被用来统筹 (pool)、分配和管理资源以提供基础结构作为服务并供应用于企业内的私有云平台的基础。自服务门户将对虚拟机的分配扩展到最终用户。自服务门户可包括基于 web 的用户接口，该用户接口包括用于数据中心管理员和商业单元 IT 消费者的部分。自服务门户可包括动态供应引擎 (dynamic provisioning engine)，并可通过为参与的 (on-boarding) 商业单元和基础结构提供请求和变化管理来减少供应基础结构及其组件所需的时间。

[0106] 在一实施例中，终端服务网关可具有定制认证和授权插件。当客户端请求远程桌面时，客户端可发送具有他们的凭证的 cookie。该插件可认证该 cookie 并授权该调用者。可在虚拟化主机处需要附加的授权以授权对特定虚拟机的访问。在一个实施例中，这可以用主机上的中间监听服务实现。所有上面这些都是安全连接所需的。

[0107] 在一实施例中，企业最终用户可使用认证机制来登入企业的自服务门户。例如，企业用户可使用 Kerberos 认证来登入该自服务门户。

[0108] 更一般而言，当企业从云提供者购买容量时，云提供者具有其自己的域和活动目录。企业具有其自己的域和活动目录。相应地，企业和云提供者不需要他们之间的信任。因此，企业中的用户期望连接到云提供者处的、用户拥有的虚拟机。

[0109] 在一实施例中，进一步期望利用现有企业组件和能力，诸如终端服务网关和诸如 RDP 等现有远程呈现协议。

[0110] 在一实施例中，创建 cookie，该 cookie 包括定制授权插件所需的声明 (claim)。

[0111] 一个问题在于 ：一些系统可能是为直接对客 OS 的远程呈现访问而设计的，而不是为对主机的远程呈现访问而设计的。

[0112] 另一个问题在于如何实现通过非信任域对虚拟机的远程控制台连接。

[0113] 在一个实施例中，终端服务网关可提供可插拔式认证和授权模块以支持认证机制。客户端可通过 cookie 发送随意字节阵列到终端服务网关。在允许连接之前，终端服务网关可将目标资源的名称通知定制资源授权插件 (可插拔式认证和授权模块的一部分)。尽管这在到目标机器的远程会话的情况下可以工作，然而当被用于通过虚拟化主机的单端口监听器服务对客虚拟机的控制台访问时，指定的目标资源是该虚拟化主机。然而，真正的目标是在该虚拟化主机上运行的虚拟机。

[0114] 最终用户能够以至少两种方式连接到他的虚拟机 ：(a) 通过使用到虚拟机中的远

程桌面直接连接，或 (b) 通过利用单端口监听器 (SPL)。如果最终用户正在使用单端口监听器，则该用户连接到主计算机端口。该主机使用 CredSSP 认证并确认此用户能够访问他们想要连接到的虚拟机。然后该主机通过该主机上的私有接口将该远程桌面会话重定向到该虚拟机。执行这些功能的组件被称为单端口监听器。单端口监听器允许 VMM 通过主机连接来连接到任何虚拟机而不对虚拟机施加任何联网要求。单端口监听器还可允许最终用户使用诸如 Internet Explorer 等浏览器从客户端计算机连接到门户。然后最终用户可选择连接到虚拟机并查看控制台会话。

[0115] 虚拟机 ID 可作为远程呈现协议的一部分被传递（例如，在预连接团块 (pre-connection blob) 中）到目的地处的虚拟化主机的单端口监听器。因为预连接团块在定制资源授权插件处可不被暴露，所以使用作为 cookie 发送到终端服务网关的 SAML 令牌或定制证书令牌的完全的虚拟机水平的粒度的授权可能不是可能的。定制资源授权插件需要能够访问该连接的预连接团块以确认它是该连接的资源授权的一部分。授权插件需要用被访问的实际的目标资源来确认 cookie 中出现的信息。目标虚拟机 ID 可通过 cookie 被取回，但是关于来自网关的目标连接实际上是那个虚拟机的授权仍然被需要。

[0116] RD 网关处的定制资源授权模块仅意识到要访问的目标虚拟化主机和端口。然而，“真正的目标”是在该虚拟化主机上运行的客虚拟机。例如，恶意用户可向终端服务网关的授权插件提交签署的声明，请求访问在该主机中运行的虚拟机。该用户能够指定预连接团块指向同一主机中运行的另一虚拟机。网关的授权插件不能用在同一主机中运行的实际的目标虚拟机来“交叉检查”该声明。

[0117] 参考图 9 到 11，提供下面的示意性示例以描绘本公开的一个实施例。我们假定云域的虚拟机 VM1 和 VM2 被云提供者（“云 (Cloud)”）分配给企业（“企业 (Enterprise)”）。企业管理员将 VM1 分配给企业 \ 用户 1 并将 VM2 分配给企业 \ 用户 2。

[0118] 在本示例中，客户端指的是企业远程呈现客户端。企业远程呈现客户端可以是管理员控制台。在一实施例中，该控制台可以是一进程或加载到自服务门户的页面的 Active-X 控件。

[0119] 云提供者 (CloudProvider) 在其活动目录中为从它购买容量的每个企业创建两个用户账户。作为示例描绘，令“云 \ 企业”是在云域中为企业的管理员创建的用户账户。“云 \ 企业”不被企业管理员共享到企业的所有最终用户。令“云 \ 企业 T”是为该企业所拥有的所有虚拟机的控制台访问的唯一目的而在云域中创建的另一用户账户“云 \ 企业 T”对云提供者的域中的这一特定企业所拥有的所有虚拟机只具有“控制台访问 (consoleaccess)”特权（由虚拟化主机（例如使用 Azman 的 Hyper-V) 实施）。

[0120] 虚拟化主机的虚拟机管理系统（单端口监听器）使用 CredSSP 协议来托管认证进入的连接。企业最终用户的客户端需要使用用户账户“云 \ 企业 T”来使用 CredSSP 协议在云提供者的虚拟化主机处认证。这个凭证和签署的令牌一起被企业虚拟机管理系统转交给客户端。凭证 SSP 是提供单点登录 (SSO) 的安全支持提供者。重要的是 :注意，最终用户不显式地输入这一凭证，而是由客户端在与企业虚拟机管理系统通信之后自动处理。更重要的是，在我们的例子中，由单端口监听器施加的这一认证机制是无用的，因为我们不想要企业的用户获得对属于甚至同一企业的另一用户的 VM 的访问权。我们主要的认证和授权机制是使用签署的令牌。尽管如此，这的确充当了对其它不同企业保护一个企业承租人的额

外的防御层。

[0121] 1. 参考图 9，在操作 900 中，企业 \ 用户 1 使用应用编程接口 (API) 来与企业虚拟化管理器服务器通话以标识它自己为企业 \ 用户 1 并出示请求访问 VM1 的授权的声明。客户端和企业虚拟化管理器服务器之间的通信是受保护信道。在一实施例中，API 可以是 Windows 通信基础 (WCF)，WCF 是 .NET 框架中用于构建连接的、面向服务的应用的 API。

[0122] 2. 在操作 910 中，企业虚拟化管理器服务器通过验证企业 \ 用户 1 的身份来执行认证。

[0123] 3. 在操作 920 中，企业虚拟化管理器服务器通过验证企业 \ 用户 1 具有对 VM1 的访问权来执行授权。

[0124] 4. 在操作 930 中，一旦经认证和授权，企业虚拟化管理器服务器使用云服务提供者信任的证书（使用私钥签署）来签署该声明。该证书的私钥不被企业管理员共享给该企业的所有用户，且仅为该虚拟化管理器服务器所知。签署的令牌被返回到客户端。

[0125] a. 企业客户端还从企业虚拟化管理器服务器检索用于服务提供者的终端服务网关服务器。

[0126] b. 企业客户端使用虚拟机 ID 作为主机别名。企业客户端不知道真正的主机名称 /IP 地址。企业客户端将此别名作为主机名称转发给终端服务网关。

[0127] c. 在一个实施例中，该令牌含有数据块、签名块、以及仅带有公钥的承租人证书。该令牌的数据块含有承租人 ID、令牌 ID、令牌期满时间、以及授权的目标虚拟机 ID。提供期满时间和其它对策以避免被称为重放攻击的对服务提供者网络的常见攻击。签名块含有用承租人证书的私钥签署的数据块的散列 (hash)。承租人证书也被包括在内，但是仅含有公钥。

[0128] d. 企业客户端将令牌编码。企业客户端设置远程呈现连接的参数，向网关指示它想要使用基于 cookie 的授权。在一实施例中，预连接团块含有串“<Token ID>;<virtual machine ID>(< 令牌 ID>;< 虚拟机 ID>)”。远程呈现客户端被设定为用“云 / 企业 T”的凭证使用 CredSSP。

[0129] Cookie 大体而言是包括文本的数据并由用户的 web 浏览器存储或在存储器中存储。Cookie 能被用来认证、存储站点偏好、购物车内容、基于服务器的会话的标识符或可通过存储文本数据实现的其它任何东西。

[0130] 5. 在操作 940 中，企业客户端通过 HTTPS 隧道连接到终端服务网关，该 HTTPS 隧道指定目的地虚拟化服务器和中间监听器的目的地端口（例如 8114）。企业客户端还向网关发送签署的令牌作为 cookie。

[0131] a. 当使用 STS 服务器方案时，企业客户端向网关发送 SAML 令牌。企业客户端在企业和云提供者的 STS 服务器之间的认证之后获得 SAML 令牌。这需要在企业和云活动目录环境之间设置粒度化的信任水平。

[0132] 6. 参考图 10，在操作 1000 中，终端服务网关的定制认证插件接收签署的令牌并验证令牌未被篡改。认证插件使用证书的公钥。

[0133] a. 当使用 STS 服务器方案时，STS 服务器用云 ADFS 服务器验证签署的 SAML 令牌。ADFS 是提供 web 单点登录 (SSO) 技术以在单个在线会话的寿命期间向多个 web 应用认证用户的组件。

[0134] 7. 在操作 1010 中，终端服务网关的定制认证插件验证承租人证书映射到云提供者的域中的用户账户。

[0135] 8. 在操作 1020 中，终端服务网关的定制资源授权插件接收签署的令牌。

[0136] a. 在一个实施例中，执行主机层次的授权。

[0137] b. 在另一实施例中，授权插件查询云提供者虚拟化管理器服务器，以基于令牌中的声明来检查承租人是否对该虚拟机有访问权。

[0138] 9. 终端服务网关的定制资源授权插件将不能够执行完全的虚拟机层次的授权，因为远程呈现协议的预连接团块不被终端服务网关暴露，因为它不能够用实际的目的地来交叉检查签署的令牌中的签署的声明。

[0139] 10. 终端服务网关调用插件来解析别名化的主机名称，因为该别名不能被本地 windows DNS 提供者解析。在操作 1310 中，联系云提供者的虚拟化管理器服务器以找到在此时间点此虚拟机所驻留的真正的主机。

[0140] 11. 一旦主机被确定之后，定制授权插件可向目标虚拟化主机中的中间监听服务通知有关要被授权的目标虚拟机 ID 和令牌 ID。Windows 管理工具 (WMI) 提供者可被写入该主机中。WMI 提供者将控制授权和通信。

[0141] a. 一旦终端服务网关执行认证和授权之后，网关现在变成客户端连接和虚拟化主机处的目的地中间监听器之间的盲通道 (blind pass through)。

[0142] 12. 参考图 11，在操作 1100 中，虚拟化主机中的中间监听器从终端服务网关的定制授权插件接收“边带信息 (side band information)”。

[0143] 13. 在操作 1110 中，虚拟化主机中的中间监听器从终端服务网关接收远程呈现连接。中间监听器打开预连接团块（该连接的第一组字节）并用从终端服务网关的定制资源授权插件作为边带通知而接收的授权的虚拟机 ID 来交叉检查该团块中指定的目标虚拟机 ID。网关发送的授权的虚拟机 ID 和实际的目标虚拟机 ID 的相关是使用两者中出现的令牌 ID 来执行的。与典型虚拟桌面会话不同，最终用户没有为该会话而发送到该虚拟机的凭证。相应地，令牌被用来确认通过中间服务的访问。

[0144] a. 如果虚拟机 ID 不匹配，则该连接被舍弃。

[0145] b. 如果虚拟机 ID 相匹配，则该连接的剩余部分被盲目地转发到同一主机中的虚拟化主机的单端口监听器（例如，端口 2179）。

[0146] c. 每个令牌含有期满时间（例如，以秒计）。中间监听服务还通过精减旧的通知来管理边带通知。

[0147] 14. 然后虚拟化主机的单端口监听器基于授权存储 xml 中的用户角色策略来检查云 \ 企业 T（使用 CredSSP 确定）是否具有对那个虚拟机的访问权。

[0148] 15. 如果成功，则企业用户具有对那个虚拟机的控制台访问权。

[0149] 授权可在终端服务网关处或在目的地主机或两者处执行。然而，终端服务网关处的完全授权通常是不可能的。终端服务网关的定制资源授权插件需要对用于那个连接的预连接团块有访问权，且因此终端服务网关的定制资源授权插件不适于通过虚拟化主机的单端口监听器对客虚拟机的控制台访问。

[0150] 相应地，在一实施例中，授权是在虚拟化主机处执行的。因为不能在云提供者的活动目录中为企业的每个用户创建影子账户，所以一个选项是在本地主机中为每个虚拟机创

建本地账户。该本地账户会与企业最终用户共享，且会只被授权为访问虚拟机的控制台会话。替代地，如果不期望管理多个本地用户账户（这需要在主存者和企业虚拟机管理系统之间在带外 (out of band) 管理），这会是云提供者的一个关注，那么可使用中间监听器方案。

[0151] 虚拟化系统主机中的中间监听器服务可以是独立的服务（网络服务）或者是现有主机代理（本地系统账户）的一部分。为了保护从终端服务网关到该主机中的中间服务的边带通知，中间监听器可使用 WMI 提供者。

[0152] 如果恶意用户改变了令牌 ID，则该令牌上的签名可被无效。签署的令牌和预连接团块中的令牌 ID 必须相关。

[0153] 恶意用户情形 1 ：

[0154] a. 企业 \ 用户 1 被授权对虚拟机 VM1 的访问。用户的令牌 ID 是 t1。

[0155] b. 企业中的恶意用户不具有对那个虚拟机的访问权。恶意用户获得用于某个其它虚拟机的令牌，但是随后将预连接团块改变为指向虚拟机 VM1 并将预连接团块和 cookie 两者中的令牌 ID 修改为 t1 并尝试承载 (piggy back) 在应早已由网关为企业 \ 用户 1 发送到虚拟化主机的边带授权通知上。

[0156] c. 缓和 ：网关的认证插件检测到 cookie 中的签名是无效的并舍弃该连接。

[0157] 恶意用户情形 2 ：

[0158] a. 企业 \ 用户 1 被授权对虚拟机 VM1 的访问且该用户的令牌 ID 是 t1。

[0159] b. 企业中的恶意用户不具有对那个虚拟机的访问权。恶意用户获得用于某个其它虚拟机（比如说，具有令牌 ID t2 的虚拟机 VM2) 的令牌。恶意用户将 PCB 改变为指向令牌 ID 为 t1 的虚拟机 VM1，但是将 cookie 中的令牌 ID 保持为 t2。因为恶意用户没有改变 cookie 中的令牌，所以签名仍然有效。网关向包含的主机发送令牌 ID t2 作为授权的令牌 ID。如果同一主机含有 ID 为虚拟机 VM1 的虚拟机，且如果企业的另一用户被授权给虚拟机 VM1，那么该恶意用户能承载在应早已由网关为企业 \ 用户 1 发送到虚拟化主机的的边带授权通知上。

[0160] c. 缓和 ：

[0161] i. 从远程呈现客户端到承租人虚拟化管理器服务器的信道被加密，所以该用户没有办法获得为企业 \ 用户 1 授予的令牌 ID t1。

[0162] ii. 预连接团块也可被承租人的私钥签署，从而云提供者可以用承租人的公钥确认该签名。

[0163] 图 12 描绘了允许第一域中主存的虚拟机和第二域中的客户端计算机之间的远程呈现会话的示例性操作过程，包括操作 1200、1202、1204 和 1206。参考图 12，操作 1200 开始该操作过程，而操作 1202 示出在第二域的服务器处建立与该客户端计算机的通信会话。在一个实施例中，第一域可以是云提供者或主存者，而第二域可以是企业。操作 1204 示出由该服务器接收指示该第一域中主存的虚拟机的虚拟机标识符。操作 1206 示出从客户端计算机接收包括签署的令牌和公钥的 cookie。在一实施例中，cookie 由该客户端基于它从企业虚拟机管理系统接收的签署的令牌来构造。操作 1208 示出使用公钥认证该令牌并验证该令牌映射到第一域中的用户账户。操作 1210 示出向第一域中的虚拟化系统发送该虚拟机标识符。操作 1212 示出从第一域中的该虚拟化系统接收标识的虚拟机是有效的的确

认和与标识的虚拟机相关联的目标资源的身份。操作 1214 示出向该虚拟化系统中的中间监听服务发送该虚拟机标识符和接收的令牌。操作 1216 示出将远程呈现会话数据转发到中间监听器服务。

[0164] 图 13 描绘了用于向如上所述的第二域中的客户端计算机允许对第一域中主存的虚拟机的访问的示例性系统。参考图 13，系统 1300 包括处理器 1310 和存储器 1320。存储器 1320 进一步包括被配置成向第二域中的客户端计算机允许对第一域中主存的虚拟机的访问的计算机指令。框 1322 示出接收第一虚拟机标识符、用公钥签署的令牌、以及对与虚拟机标识符相关联的虚拟机主机的请求。框 1324 示出实例化与客户端计算机的远程呈现会话。框 1326 示出经由远程呈现会话接收目标虚拟机标识符并用第一虚拟机标识符相关和授权目标虚拟机标识符。框 1328 示出确定目标和第一虚拟机标识符匹配并将经由远程呈现会话接收的数据转发到目标虚拟机。

[0165] 上文所提及的方面中的任何一个方面都可以以方法、系统、计算机可读介质或任何类型的产品来实现。例如，计算机可读介质上可存储用于通过第二域中的客户端计算机访问第一域中主存的虚拟机的计算机可执行指令。这种介质可包括用于与第一域中的虚拟化主机建立通信会话的第一指令子集；用于向第一域中的虚拟化主机发送虚拟机标识符和请求对标识的虚拟机的访问的授权的声明的第二指令子集；用于从第二域中的虚拟化管理器接收签署的令牌的第三指令子集；用于通过第一域中的虚拟化主机建立远程呈现会话以及发送基于 cookie 的授权将被执行的指示的第四指令子集；用于向第一域中的虚拟化主机发送包括签署的令牌和公钥的 cookie 的第五指令子集；以及用于与请求的虚拟机建立远程呈现会话的第六指令子集。本领域技术人员可以理解，可以使用附加指令集来捕捉此处所公开的各其他方面，并且根据本发明，两个目前所公开的指令子集可以在细节方面不同。

[0166] 上述详细描述通过示例和 / 或操作图阐明了系统和 / 或过程的各种实施例。就这些框图和 / 或示例包含一个或多个功能和 / 或操作而言，本领域技术人员将理解，这些框图或示例中的每一功能和 / 或操作都可由各种各样的硬件、软件、固件、或实际上其任意组合来单独地和 / 或共同地实现。

[0167] 应该理解，此处描述的各种技术可以结合硬件或软件，或在适当时结合两者的组合来实现。因此，本公开的方法和装置或其某些方面或部分，可以采用包含在诸如软盘、CD-ROM、硬盘驱动器或任何其它机器可读存储介质等有形介质中的程序代码（即，指令）的形式，其中，当程序代码被加载至诸如计算机等机器并由其运行时，该机器成为用于实现本公开的装置。在程序代码在可编程计算机上执行的情况下，计算设备通常包括处理器、该处理器可读的存储介质（包括易失性和非易失性存储器和 / 或存储元件）、至少一个输入设备、以及至少一个输出设备。一个或多个程序可以例如，通过使用 API、可重用控件等来实现或利用结合本发明描述的过程。这样的程序优选地用高级过程语言或面向对象编程语言来实现，以与计算机系统通信。然而，如果需要，该程序可以用汇编语言或机器语言来实现。在任何情形中，语言可以是编译语言或解释语言，且与硬件实现相结合。

[0168] 尽管具体地参考其优选实施例来示出并描述了本发明，但本领域的技术人员可以理解，可以作出形式和细节上的各种改变而不脱离所附权利要求书中所述的本发明的范围。此外，尽管本发明的各元素可以用单数来描述或要求保护，但构想了复数，除非明确地

规定了限于单数。

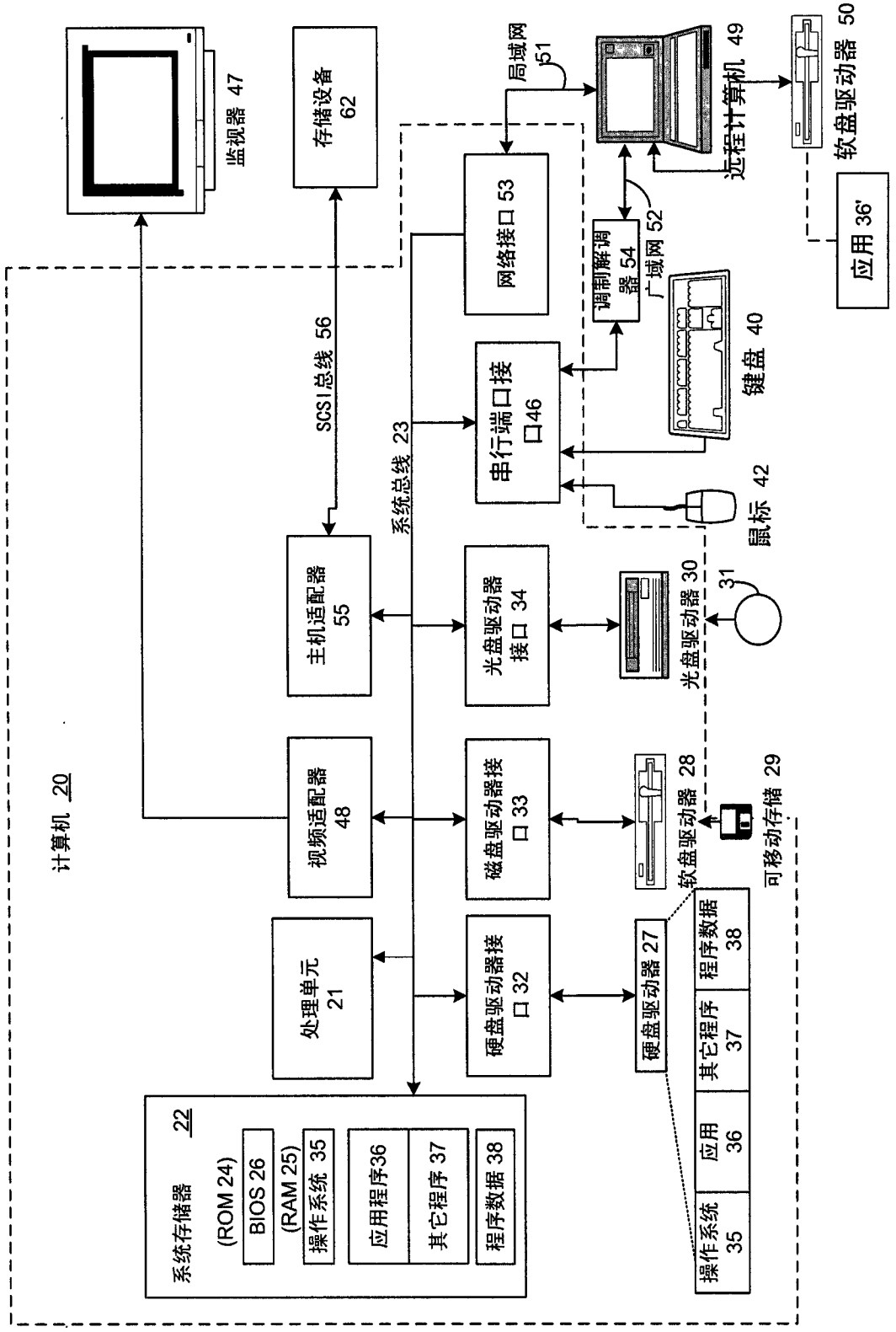

计算机 20
监视器 47
存储设备 62
局域网 51
远程计算机 49
软盘驱动器 50
应用 36'
网络接口 53
调制解调器 54
广域网 52
SCSI总线 56
系统总线 23
串行端口接口46
键盘 40
鼠标 42
主机适配器 55
光盘驱动器接口 34
光盘驱动器 30
31
视频适配器 48
磁盘驱动器接口 33
软盘驱动器 28
可移动存储 29
处理单元 21
硬盘驱动器接口 32
硬盘驱动器 27
操作系统 35
应用 36
其它程序 37
程序数据 38
系统存储器 22
(ROM 24)
BIOS 26
(RAM 25)
操作系统 35
应用程序36
其它程序 37
程序数据 38

图 1

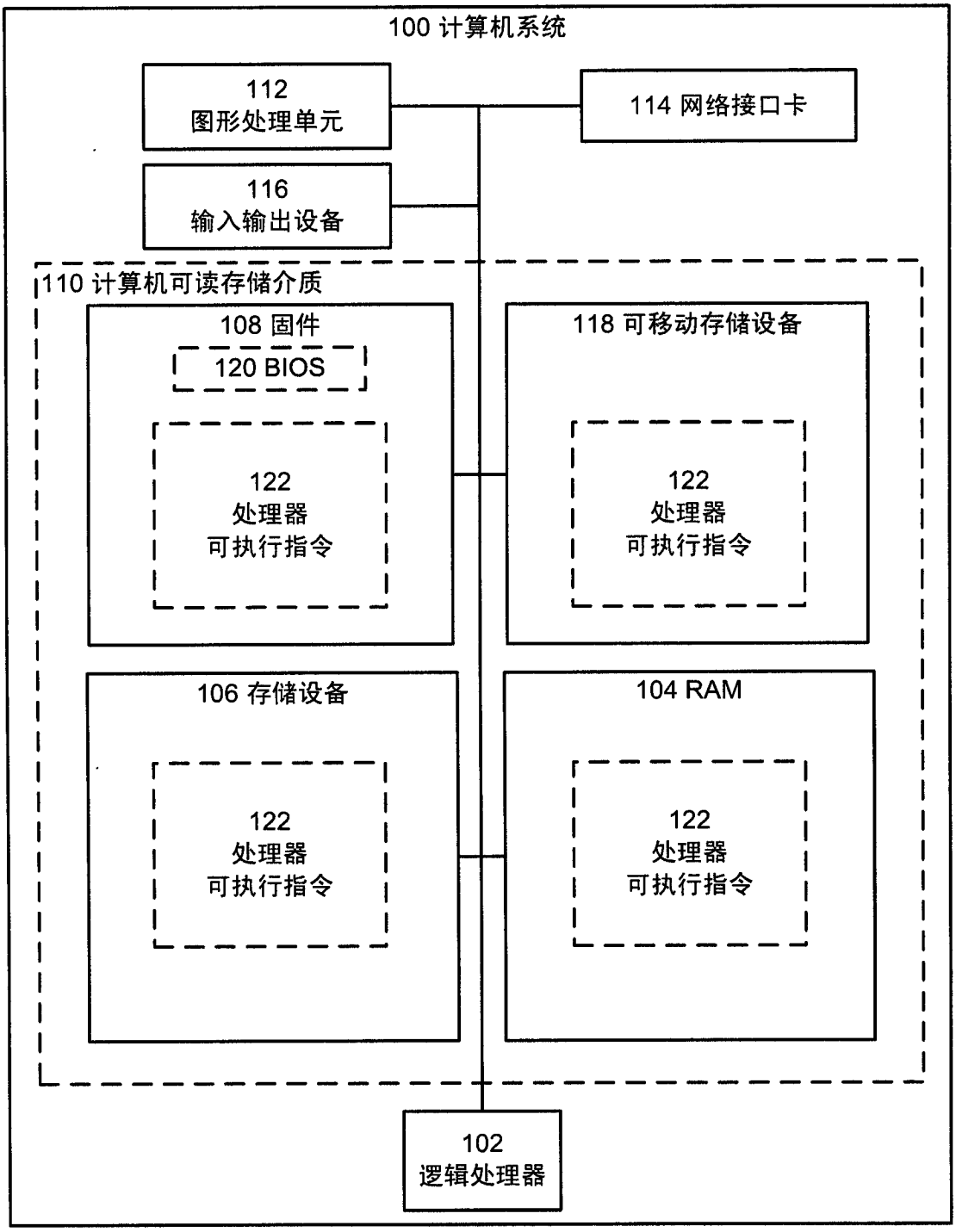

100 计算机系统
112
图形处理单元
114 网络接口卡
116
输入输出设备
110 计算机可读存储介质
108 固件
120 BIOS
122
处理器
可执行指令
118 可移动存储设备
122
处理器
可执行指令
106 存储设备
122
处理器
可执行指令
104 RAM
122
处理器
可执行指令
102
逻辑处理器

图 2

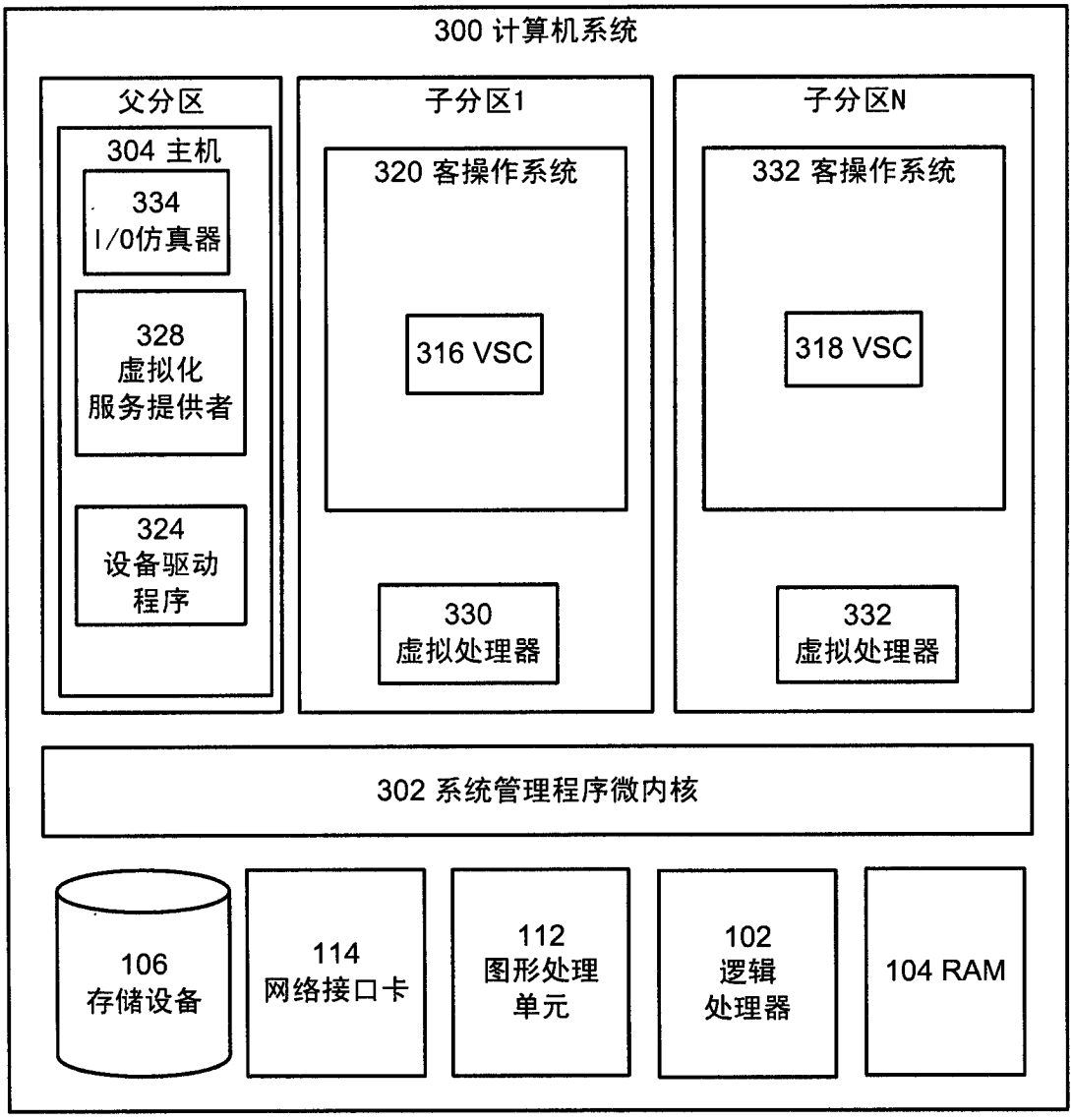

300 计算机系统
父分区
304 主机
334
I/O仿真器
328
虚拟化
服务提供者
324
设备驱动
程序
子分区1
320 客操作系统
316 VSC
330
虚拟处理器
子分区N
332 客操作系统
318 VSC
332
虚拟处理器
302 系统管理程序微内核
106
存储设备
114
网络接口卡
112
图形处理
单元
102
逻辑
处理器
104 RAM

图 3

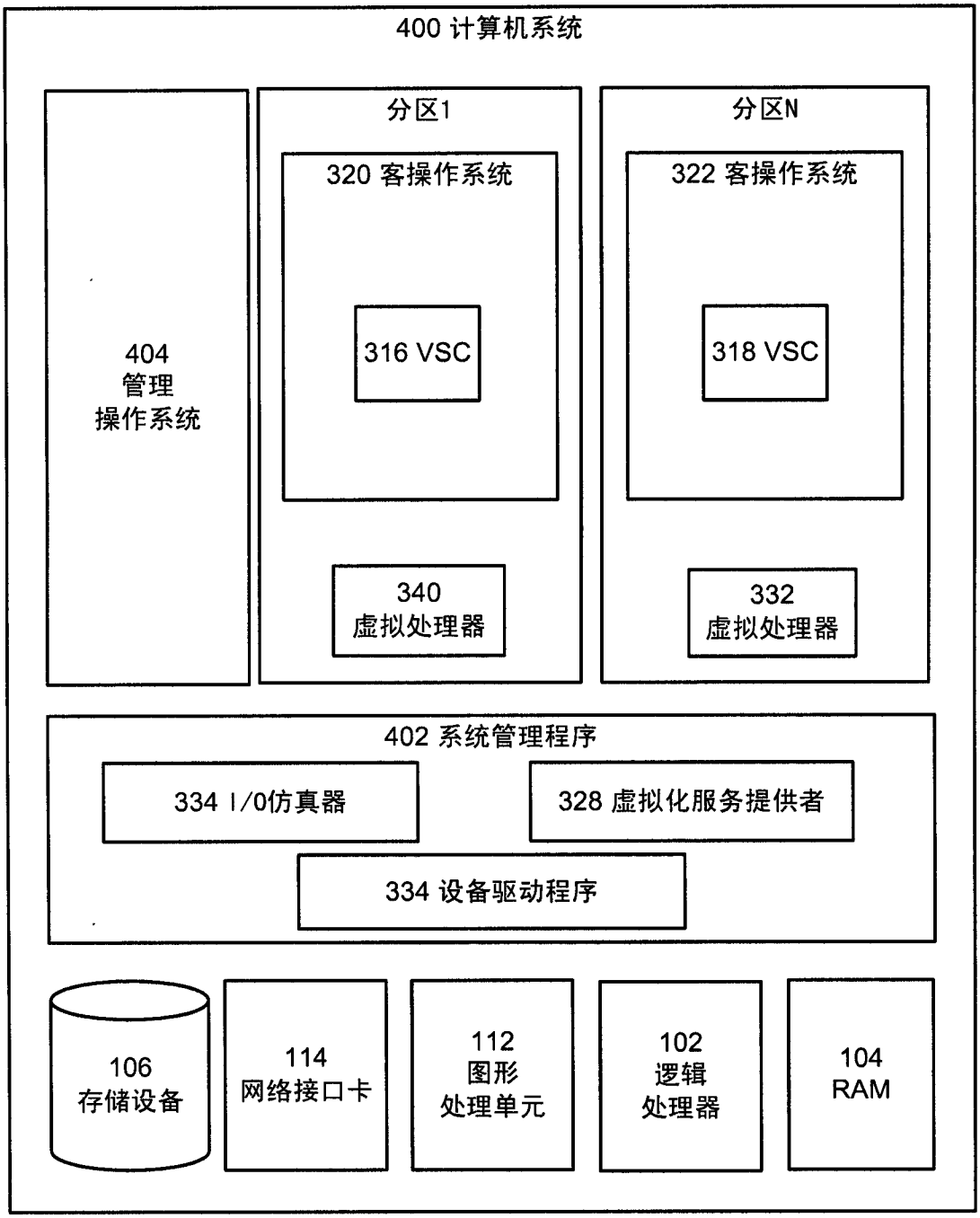

400 计算机系统
404
管理
操作系统
分区1
320 客操作系统
316 VSC
340
虚拟处理器
分区N
322 客操作系统
318 VSC
332
虚拟处理器
402 系统管理程序
334 I/O仿真器
328 虚拟化服务提供者
334 设备驱动程序
106
存储设备
114
网络接口卡
112
图形
处理单元
102
逻辑
处理器
104
RAM

图 4

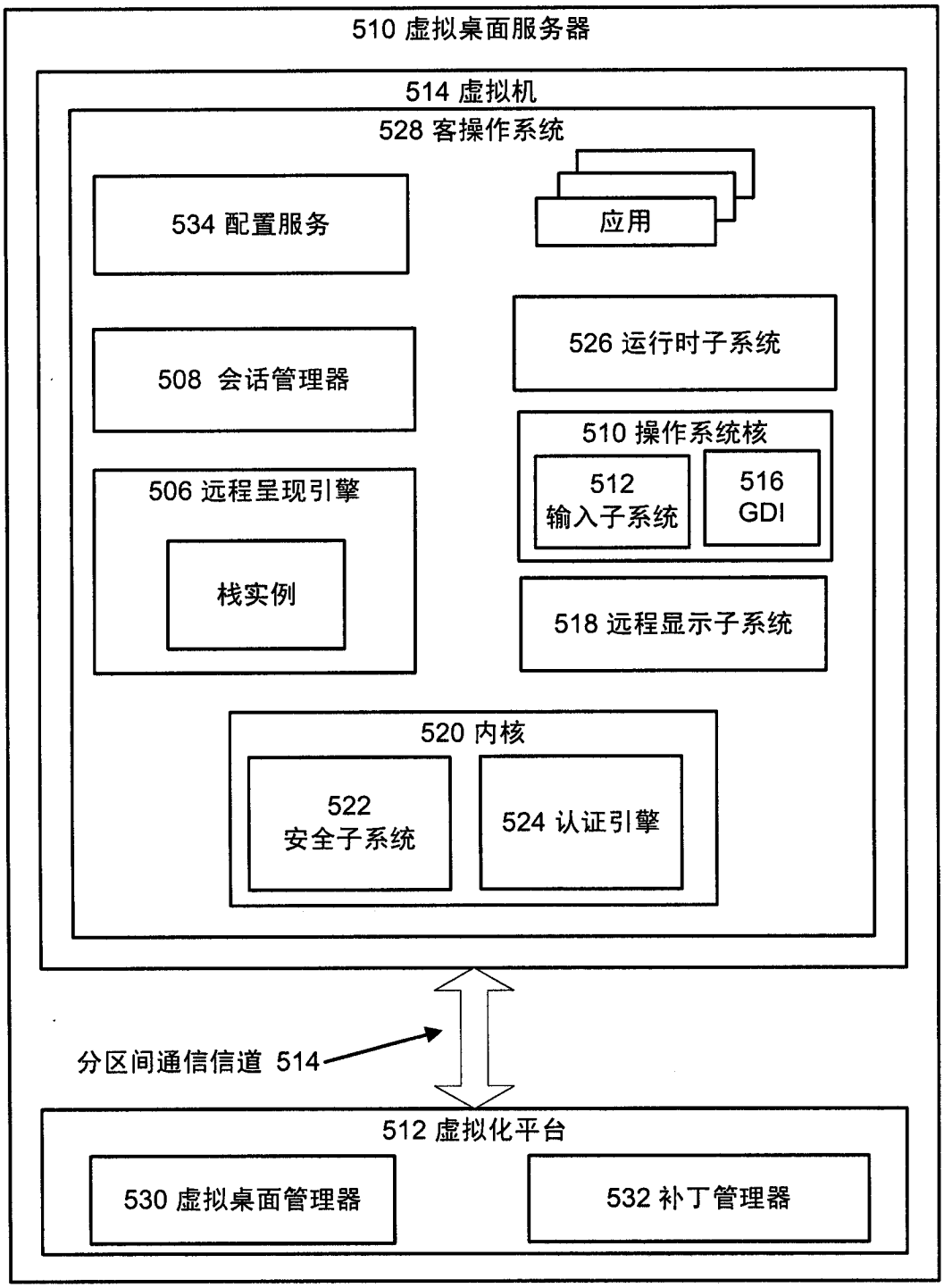

510 虚拟桌面服务器
514 虚拟机
528 客操作系统
534 配置服务
应用
526 运行时子系统
508 会话管理器
510 操作系统核
512
输入子系统
516
GDI
506 远程呈现引擎
栈实例
518 远程显示子系统
520 内核
522
安全子系统
524 认证引擎
分区间通信信道 514
512 虚拟化平台
530 虚拟桌面管理器
532 补丁管理器

图 5

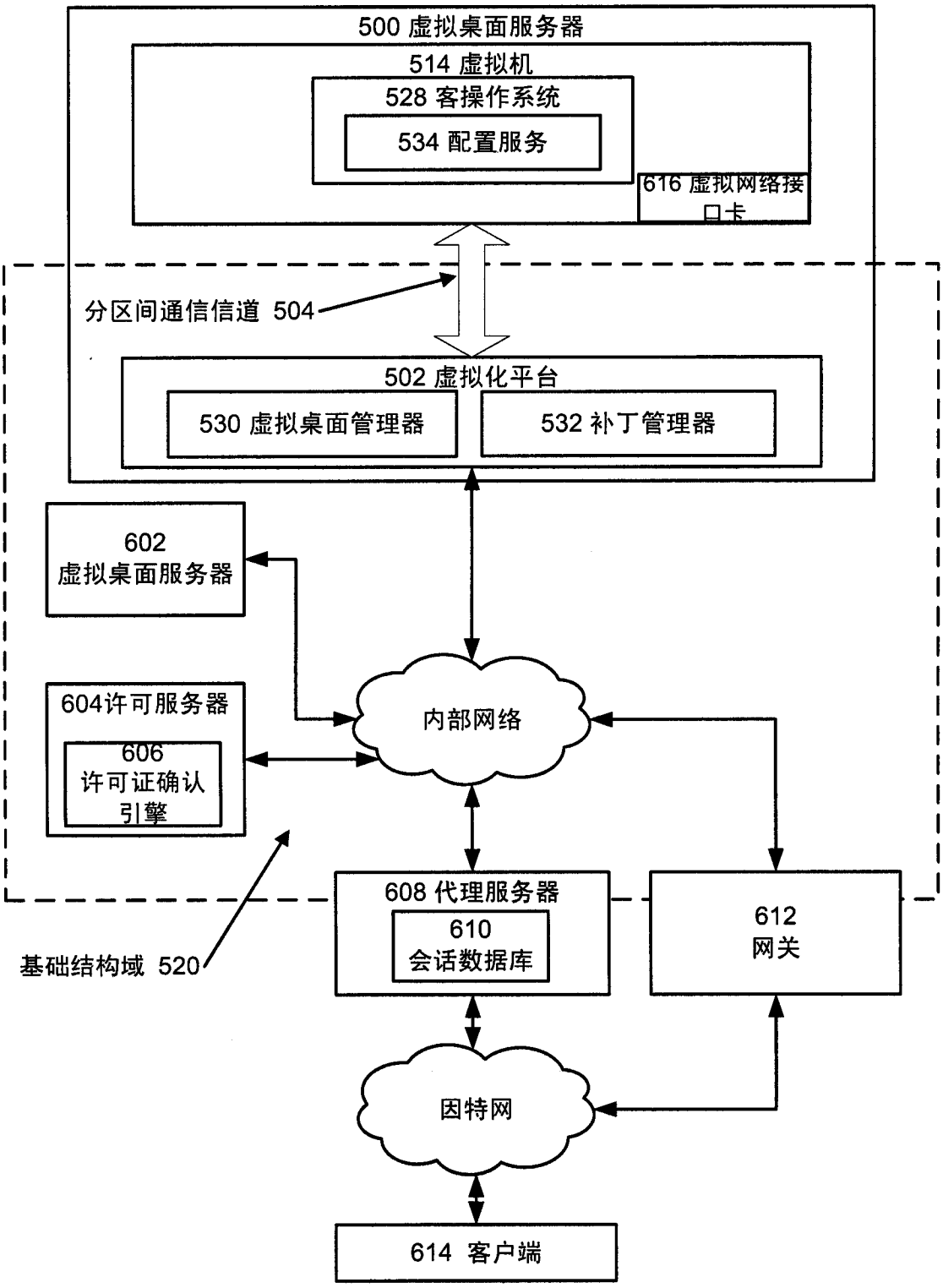

500 虚拟桌面服务器
514 虚拟机
528 客操作系统
534 配置服务
616 虚拟网络接口卡
分区间通信信道 504
502 虚拟化平台
530 虚拟桌面管理器
532 补丁管理器
602
虚拟桌面服务器
604许可服务器
606
许可证确认引擎
内部网络
608 代理服务器
610
会话数据库
612
网关
基础结构域 520
因特网
614 客户端

图 6

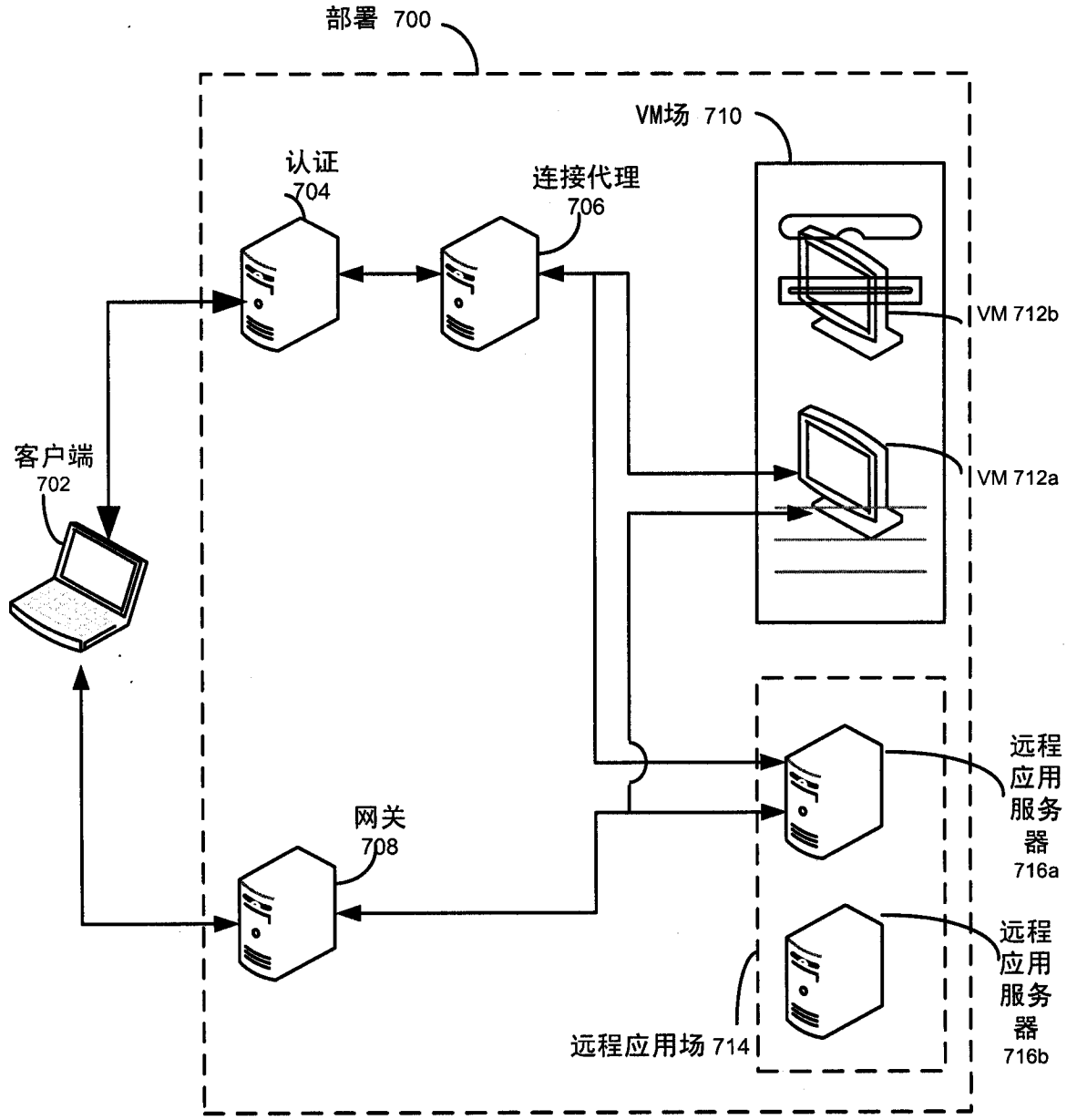

部署 700
VM场 710
认证
704
连接代理
706
VM 712b
VM 712a
客户端
702
网关
708
远程
应用
服务
器
716a
远程
应用
服务
器
716b
远程应用场 714

图 7

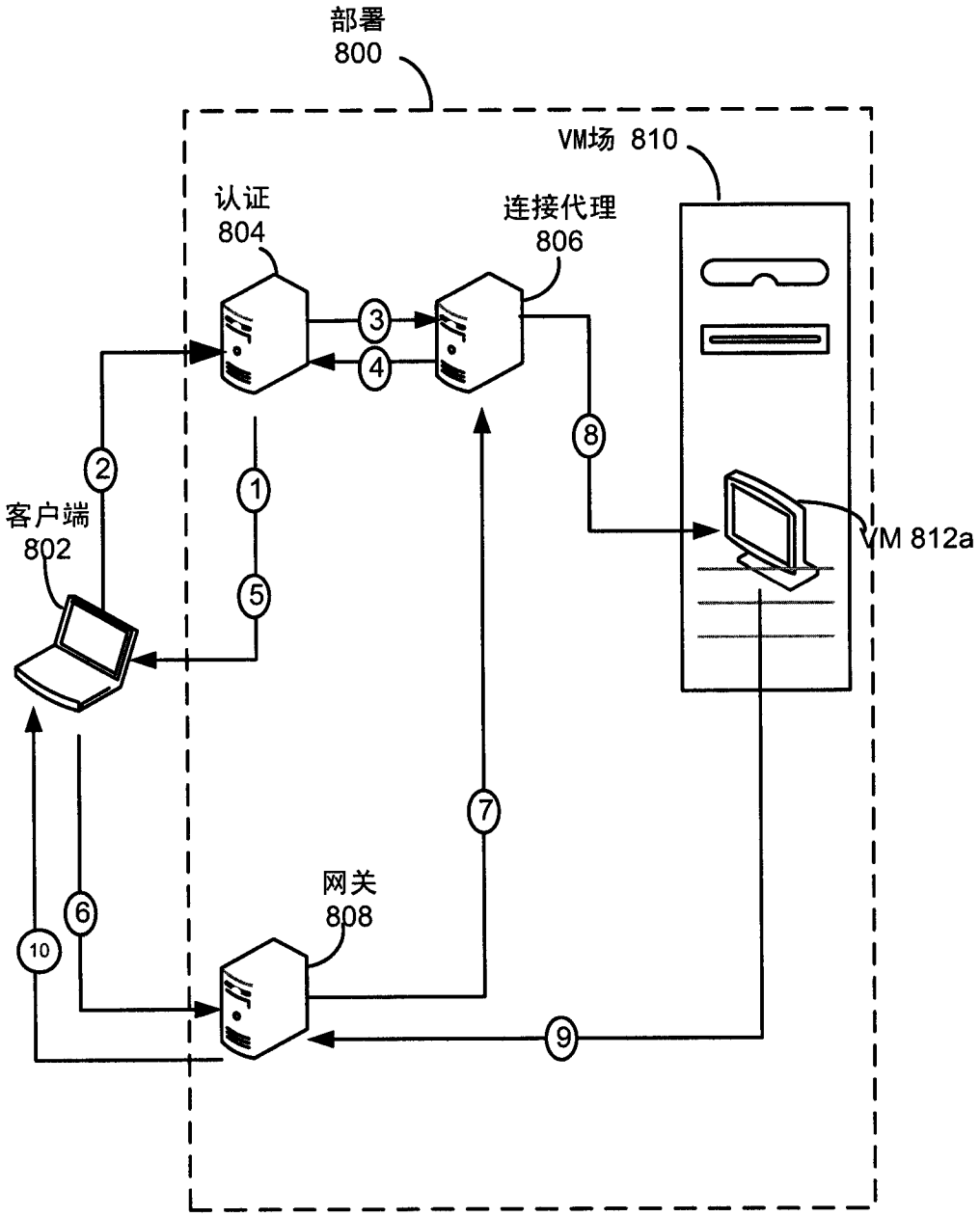

部署
800
VM场 810
认证
804
连接代理
806
客户端
802
网关
808
VM 812a
1
2
3
4
5
6
7
8
9
10

图 8

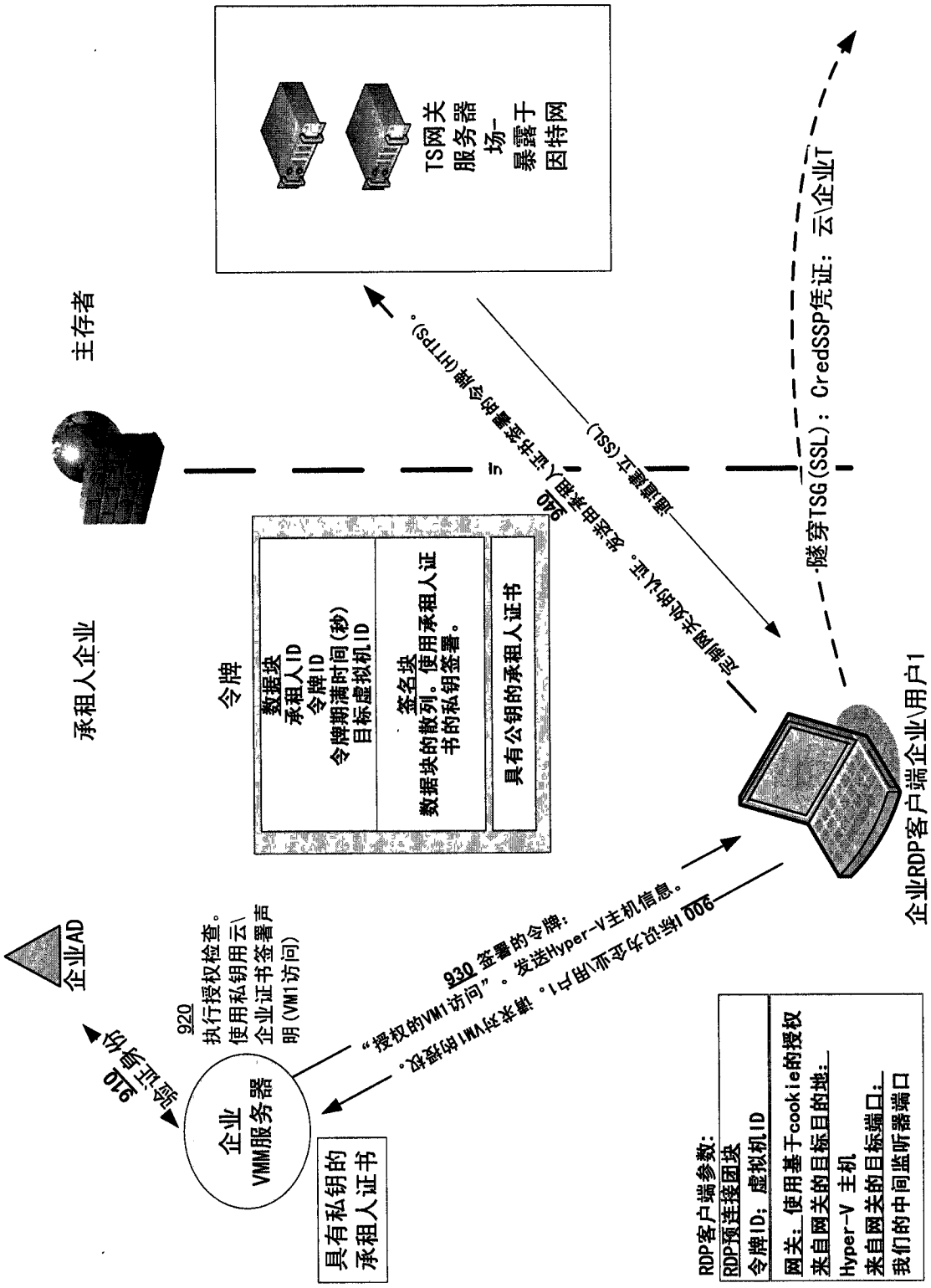

TS网关服务器场-暴露于因特网
主存者
承租人企业
令牌
数据块
承租人ID
令牌ID
令牌期满时间(秒)
目标虚拟机ID
签名块
数据块的散列。使用承租人证书的私钥签署。
具有公钥的承租人证书
940 发送带有承租人证书的令牌(HTTPS)。
隧道建立(SSL)
隧穿TSG(SSL)：CredSSP凭证：云\企业IT
完成网关处的执行证。
企业RDP客户端企业\用户1
910 验证身份
企业AD
920 执行授权检查。使用私钥用云\企业证书签署声明(VM1访问)
企业VMM服务器
具有私钥的承租人证书
930 签署的令牌："授权的VM1访问"。发送Hyper-V主机信息。
900 接受身份。请求对VM1的授权。
RDP客户端参数：
RDP预连接团块
令牌ID；虚拟机ID
网关：使用基于cookie的授权
来自网关的目标目的地：
Hyper-V 主机
来自网关的目标端口：
我们的中间监听器端口

图 9

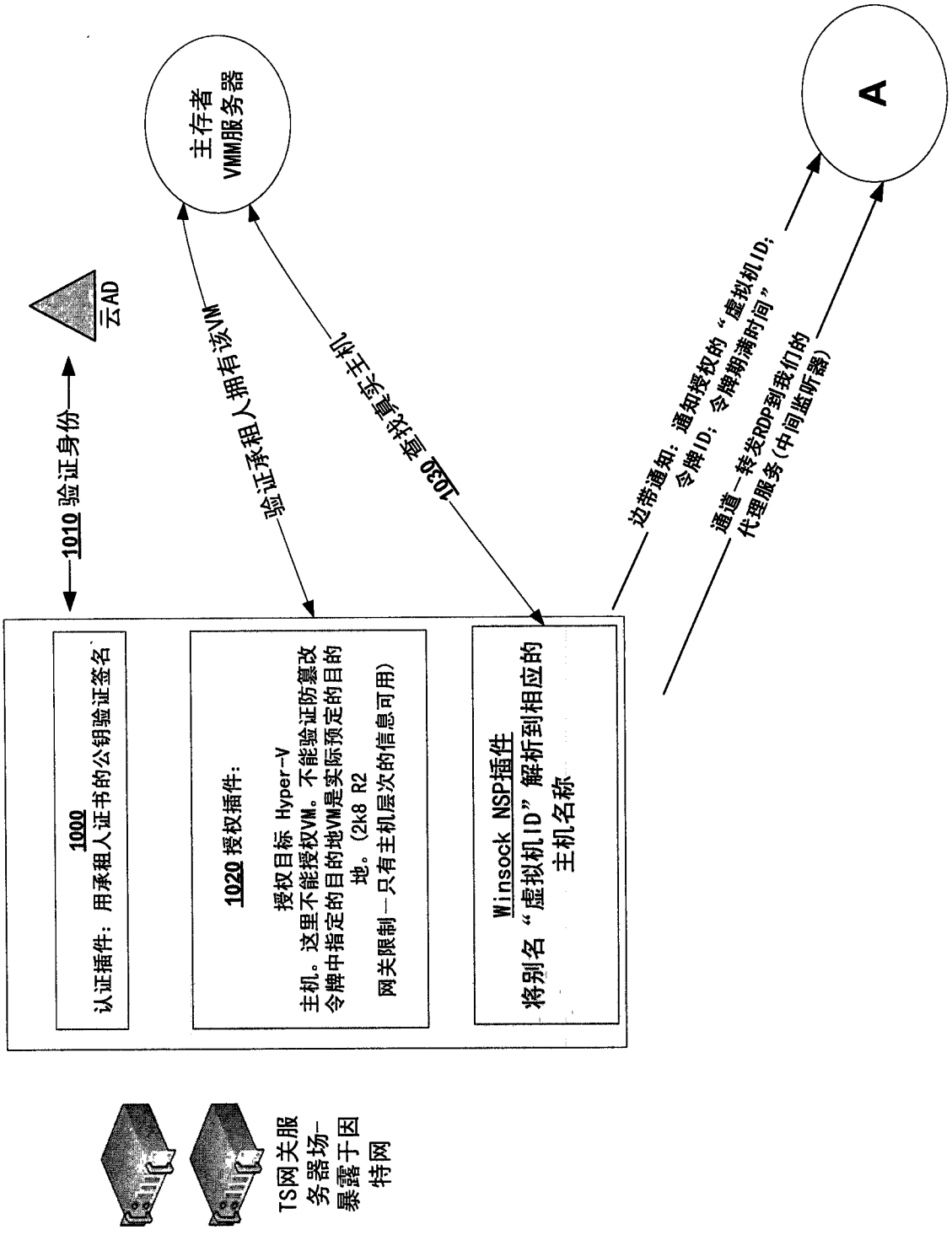

主存者
VMM服务器
A
云AD
1010 验证身份
验证承租人拥有该VM
1030 查找宿主主机
边带通知：通知授权的“虚拟机ID；
令牌ID：令牌期满时间”
通道—转发RDP到我们的
代理服务（中间监听器）
1000
认证插件：用承租人证书的公钥验证签名
1020 授权插件：
授权目标 Hyper-V
主机。这里不能授权VM。不能验证防篡改
令牌中指定的目的地VM是实际预定的目的
地。（2k8 R2
网关限制—只有主机层次的信息可用）
Winsock NSP插件
将别名“虚拟机ID”解析到相应的
主机名称
TS网关服
务器场—
暴露于因
特网

图 10

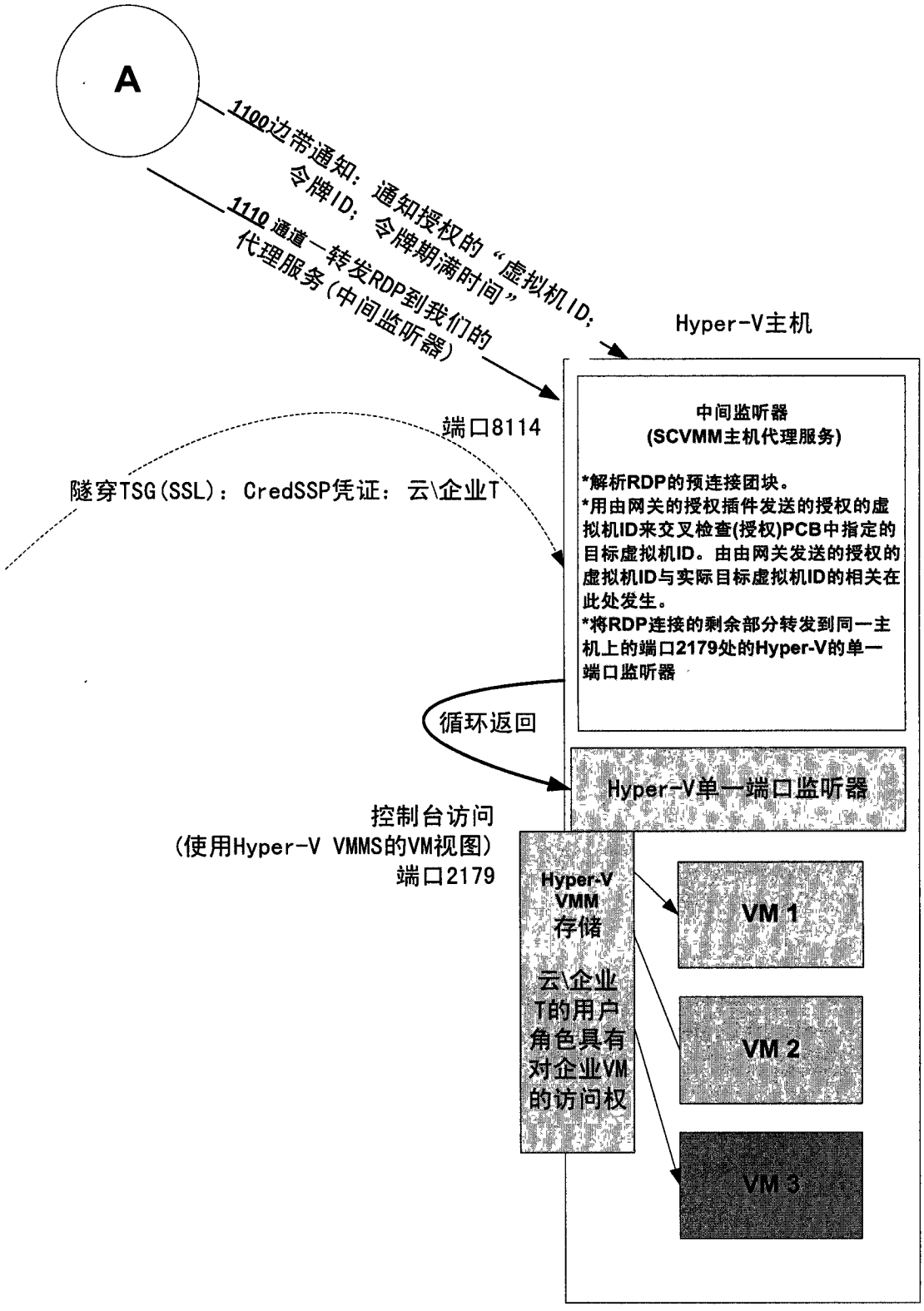

A
1100边带通知：通知授权的“虚拟机ID:
令牌ID：令牌期满时间”
1110 通道—转发RDP到我们的
代理服务(中间监听器)
Hyper-V主机
端口8114
隧穿TSG(SSL)：CredSSP凭证：云\企业T
中间监听器
(SCVMM主机代理服务)
*解析RDP的预连接团块。
*用由网关的授权插件发送的授权的虚拟机ID来交叉检查(授权)PCB中指定的目标虚拟机ID。由由网关发送的授权的虚拟机ID与实际目标虚拟机ID的相关在此处发生。
*将RDP连接的剩余部分转发到同一主机上的端口2179处的Hyper-V的单一端口监听器
循环返回
Hyper-V单一端口监听器
控制台访问
(使用Hyper-V VMMS的VM视图)
端口2179
Hyper-V VMM 存储
云\企业T的用户角色具有对企业VM的访问权
VM 1
VM 2
VM 3

图 11

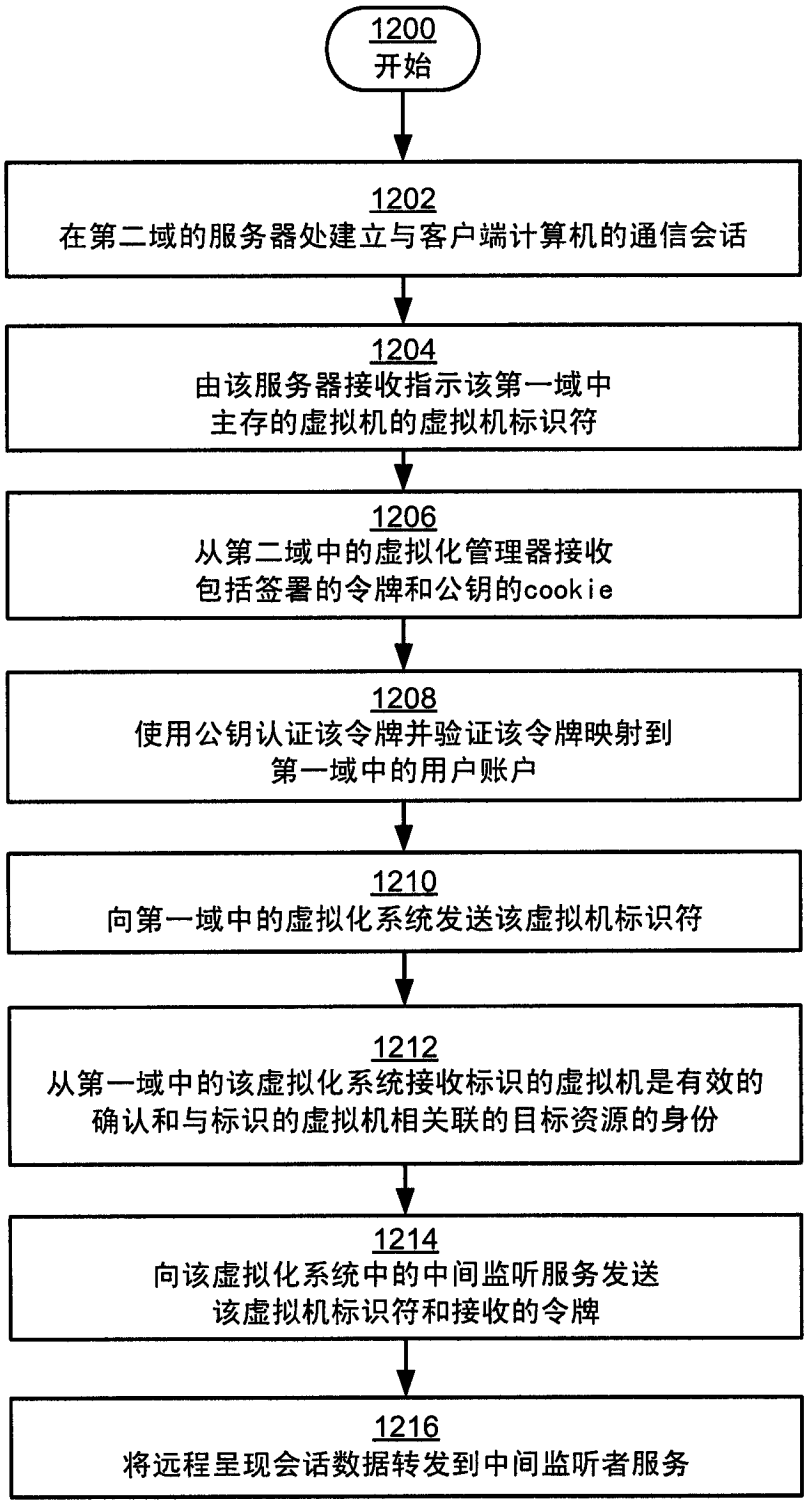

1200
开始
1202
在第二域的服务器处建立与客户端计算机的通信会话
1204
由该服务器接收指示该第一域中
主存的虚拟机的虚拟机标识符
1206
从第二域中的虚拟化管理器接收
包括签署的令牌和公钥的cookie
1208
使用公钥认证该令牌并验证该令牌映射到
第一域中的用户账户
1210
向第一域中的虚拟化系统发送该虚拟机标识符
1212
从第一域中的该虚拟化系统接收标识的虚拟机是有效的
确认和与标识的虚拟机相关联的目标资源的身份
1214
向该虚拟化系统中的中间监听服务发送
该虚拟机标识符和接收的令牌
1216
将远程呈现会话数据转发到中间监听者服务

图 12

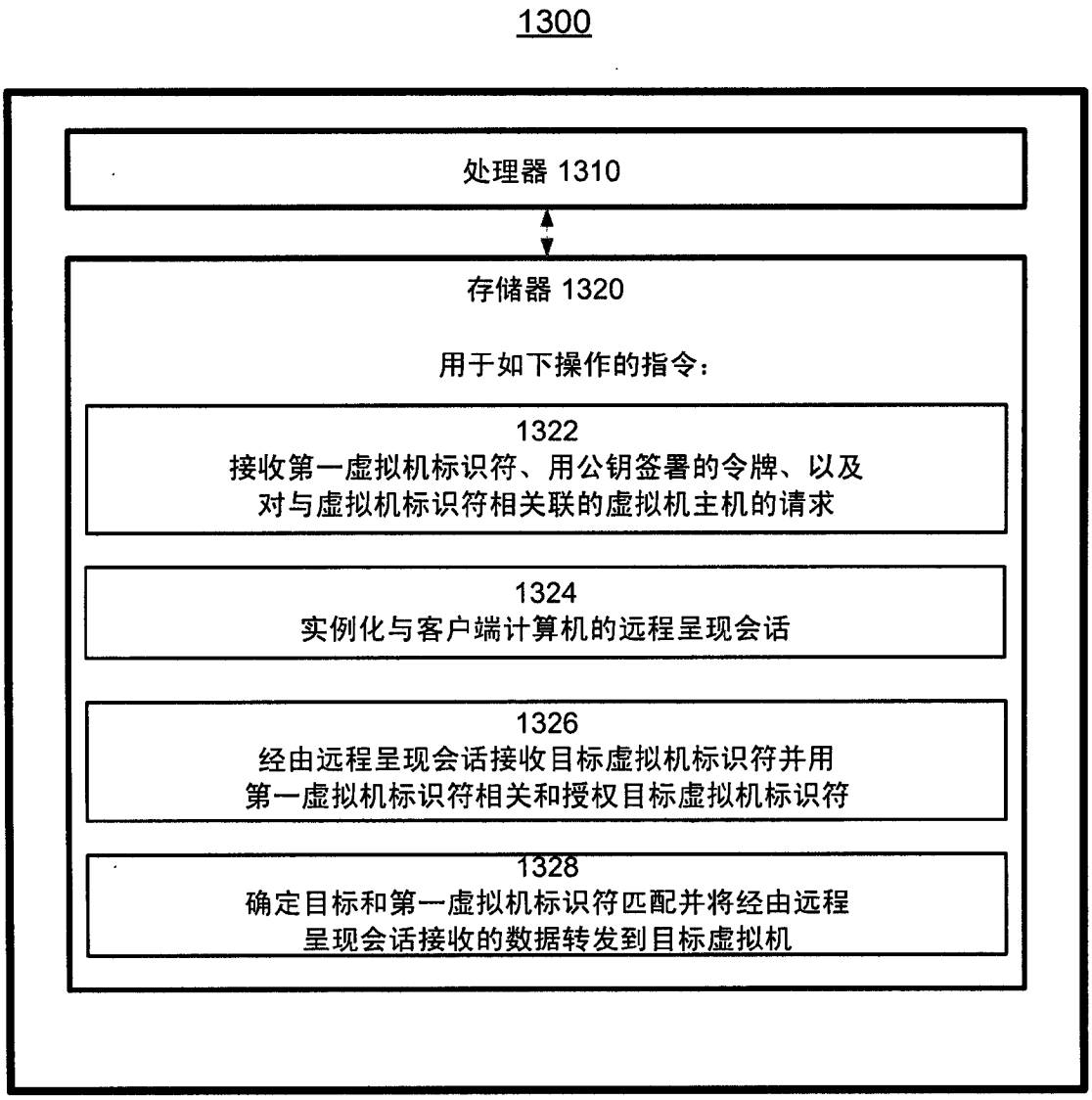

1300
处理器 1310
存储器 1320
用于如下操作的指令：
1322
接收第一虚拟机标识符、用公钥签署的令牌、以及对与虚拟机标识符相关联的虚拟机主机的请求
1324
实例化与客户端计算机的远程呈现会话
1326
经由远程呈现会话接收目标虚拟机标识符并用第一虚拟机标识符相关和授权目标虚拟机标识符
1328
确定目标和第一虚拟机标识符匹配并将经由远程呈现会话接收的数据转发到目标虚拟机

图 13