



(12) 发明专利

(10) 授权公告号 CN 103297414 B

(45) 授权公告日 2016. 02. 10

(21) 申请号 201310057537. 7

审查员 杜晓萍

(22) 申请日 2013. 02. 22

(30) 优先权数据

13/402, 121 2012. 02. 22 US

(73) 专利权人 微软技术许可有限责任公司

地址 美国华盛顿州

(72) 发明人 薛纲 史秋芳

(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 29/06(2006. 01)

H04L 29/08(2006. 01)

(56) 对比文件

US 2012011244 A1, 2012. 01. 12, 全文.

CN 101911087 A, 2010. 12. 08, 全文.

US 2011016536 A1, 2011. 01. 20, 全文.

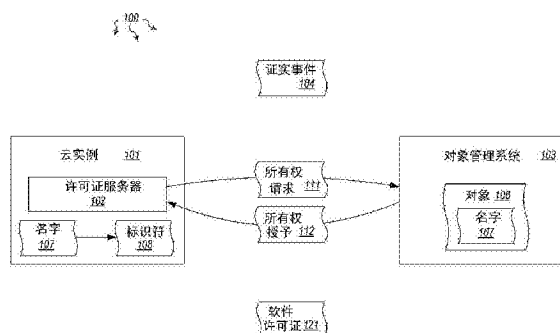
权利要求书2页 说明书5页 附图3页

(54) 发明名称

在虚拟化环境中证实许可证服务器

(57) 摘要

本发明提供用于在虚拟化环境中证实许可证服务器的方法、系统及计算机程序产品。本发明的实施例充分利用云计算环境中获得的或构建的一组特征, 以便于提供云中主持的许可证服务器的唯一性和不变性的基于软件的解决方案。避免底层硬件系统的特征导致更灵活和可靠的用于主持许可证服务器的平台。云存储服务的特征可被用于创建用于许可证服务器的唯一 ID。主持在公共云环境中的许可证服务器的安全性和可靠性也被提高。



1. 一种在云计算环境的云实例处的用于证实许可证服务器作为用于软件许可证的目标许可证服务器的方法,所述云实例运行在一底层计算机系统中,所述底层计算机系统包括一个或多个处理器以及系统存储器,所述云实例主持所述许可证服务器,所述方法包括:

对所述许可证服务器检测证实事件的动作,所述证实事件指示出所述许可证服务器要检查作为用于所述软件许可证的所述目标许可证服务器的状态,所述软件许可证可安装在具有唯一标识符的许可证服务器上,所述唯一标识符基于与所述云计算环境内基于云的对象相关联的唯一名字;

许可证服务器响应于所述证实事件请求承担对所述基于云的对象的所有权的动作,所述基于云的对象具有所有权的独占性,使得单个许可证服务器可在任何时刻拥有所述基于云的对象;

所述许可证服务器被授予对所述基于云的对象的所有权的动作;以及

所述许可证服务器使用所述唯一名字来建立所述唯一标识符作为用于所述许可证服务器的标识符的动作。

2. 如权利要求 1 所述的方法,其特征在于,检测证实事件的动作包括检测到所述软件许可证被存储在所述云计算环境内用于安装在具有所述唯一标识符的许可证服务器上的动作。

3. 如权利要求 1 所述的方法,其特征在于,检测证实事件的动作包括检测到自从所述许可证服务器的状态被上次检查以来已经经过了指定的时间段的动作。

4. 如权利要求 1 所述的方法,其特征在于,许可证服务器请求承担对所述基于云的对象的所有权的动作包括请求承担对与所述云计算环境中的存储位置相关联的所述基于云的对象的所有权的动作。

5. 如权利要求 1 所述的方法,其特征在于,所述唯一标识符是所述唯一名字,所述唯一名字是所述存储位置的名字。

6. 一种在云计算环境中的云实例处用于证实许可证服务器作为用于软件许可证的目标许可证服务器的系统,所述云实例运行在一底层计算机系统中,所述底层计算机系统包括一个或多个处理器以及系统存储器,所述云实例主持一许可证服务器,所述系统包括:

用于对所述许可证服务器检测证实事件的装置,所述证实事件指示出所述许可证服务器要检查作为用于所述软件许可证的所述目标许可证服务器的状态,所述软件许可证可安装在具有唯一标识符的许可证服务器上,所述唯一标识符基于与所述云计算环境内基于云的对象相关联的唯一名字;

用于响应于所述证实事件请求承担对所述基于云的对象的所有权的装置,所述基于云的对象具有所有权的独占性,使得单个许可证服务器可在任何时刻拥有所述基于云的对象;

用于授予所述许可证服务器对所述基于云的对象的所有权的装置;以及

用于使用所述唯一名字来建立所述唯一标识符作为用于所述许可证服务器的标识符的装置。

7. 如权利要求 6 所述的系统,其特征在于,所述用于检测证实事件的装置包括用于检测到所述软件许可证被存储在所述云计算环境内用于安装在具有所述唯一标识符的许可

证服务器上的装置。

8. 如权利要求 6 所述的系统, 其特征在于, 所述用于检测证实事件的装置包括用于检测到自从所述许可证服务器的状态被上次检查以来已经经过了指定的时间段的装置。

9. 如权利要求 6 所述的系统, 其特征在于, 所述用于请求承担对所述基于云的对象的所有权的装置包括用于请求承担对与所述云计算环境中的存储位置相关联的所述基于云的对象的所有权的装置。

10. 如权利要求 6 所述的系统, 其特征在于, 所述唯一标识符是所述唯一名字, 所述唯一名字是所述存储位置的名字。

在虚拟化环境中证实许可证服务器

技术领域

[0001] 本发明涉及在虚拟化环境中证实许可证服务器。

背景技术

[0002] 计算机系统及相关技术影响社会的许多方面。的确,计算机系统处理信息的能力已转变了人们生活和工作的方式。现在,计算机系统通常执行在计算机系统出现以前手动执行的许多任务(例如,文字处理、日程安排、会计等)。最近,计算机系统彼此耦合并耦合到其他电子设备以形成计算机系统及其他电子设备可在其上传输电子数据的有线和无线计算机网络。因此,许多计算任务的执行分布在多个不同的计算机系统和/或多个不同的计算环境中。

[0003] 在网络环境中,应用可在计算机系统之间移动。为制止盗版,许多应用依赖于浮动的软件许可证和许可证服务器。浮动的软件许可证可被部署在许可证服务器上以便防止被滥用。应用可被安装在任何计算机系统中。然而,除非有有效的许可证,否则应用将不会运行。为了确定应用是否可在计算机系统中运行,计算机系统查询许可证服务器来确定是否存在用于该应用的有效许可证。

[0004] 为了确保仅指定的目标许可证服务器被使用,需要通过唯一 ID(如指纹)来标识目标许可证服务器。在某些环境中,该唯一 ID 被制定为底层硬件系统的与众不同且不可变的特征,如网络接口卡(NIC)的媒介访问控制(MAC)地址。在其他实施例中,目标许可证服务器的硬件和软件特征的组合可被用于制定唯一 ID。该唯一 ID 被提供给应用实例,使得目标许可证服务器可被查询。

[0005] 不幸的是,虚拟系统不是固有地就具有可被用于生成唯一 ID 并从而制止盗版的特征。在虚拟系统中,诸如 BIOS GUID 和 MAC 地址等之类的硬件特征可被欺骗。被欺骗的硬件特征于是可被用于克隆许可证服务器。此外,当在云环境中操作时,云实例是不绑定于底层硬件的瞬态虚拟机。因此,在虚拟化系统中,硬件特征不能被可靠地用于制定唯一 ID。至少部分地由于这些困难,许多应用最终用户许可证协议(EULA)禁止在虚拟系统上执行。

发明内容

[0006] 本发明提供用于在虚拟化环境中证实许可证服务器的方法、系统及计算机程序产品。在某些实施例中,云实例在云计算环境中主持一许可证服务器。许可证服务器被证实为用于软件许可证的目标许可证服务器。

[0007] 对许可证服务器检测证实事件。证实事件指示出许可证服务器要检查作为用于软件许可证的目标许可证服务器的状态。软件许可证是可在具有唯一标识符的许可证服务器处安装的。该唯一标识符基于与云计算环境内基于云的对象相关联的唯一名字。

[0008] 该许可证服务器响应于该事件请求承担对该基于云的对象的所有权。该基于云的对象具有所有权的独占性,使得单个许可证服务器可在任何时刻拥有该基于云的对象。该许可证服务器被授予对该基于云的对象的所有权。该许可证服务器使用该唯一

名字来建立唯一标识符作为用于许可证服务器的标识符。

[0009] 提供本发明内容以便以简化的形式介绍将在以下的具体实施例中进一步描述的一些概念。本概述不旨在标识出所要求保护的主题的关键特征或必要特征,也不旨在用于帮助确定所要求保护的主题的范围。

[0010] 本发明的附加特征和优点将在以下描述中叙述,且其一部分根据本说明书将是显而易见的,或可通过对本发明的实践来获知。本发明的特征和优点可通过在所附权利要求书中特别指出的工具和组合来实现和获得。本发明的这些和其他特征将通过以下描述和所附权利要求书变得更加显而易见,或可通过对下文中所述的本发明的实践来领会。

附图说明

[0011] 为了描述可获得本发明的上述和其它优点和特征的方式,将通过引用附图中示出的本发明的具体实施例来呈现以上简要描述的本发明的更具体描述。可以理解,这些附图仅描述本发明的典型实施例,从而不被认为是对其范围的限制,本发明将通过使用附图用附加特征和细节来描述和说明,在附图中:

[0012] 图 1 示出便于在虚拟化环境中证实许可证服务器的示例计算机架构。

[0013] 图 2 示出用于在虚拟化环境中证实许可证服务器的示例方法的流程图。

[0014] 图 3 示出便于在虚拟化环境中证实许可证服务器的另一示例计算机架构。

具体实施方式

[0015] 本发明提供用于在虚拟化环境中证实许可证服务器的方法、系统及计算机程序产品。在某些实施例中,云实例在云计算环境中主持一许可证服务器。许可证服务器被证实为用于软件许可证的目标许可证服务器。

[0016] 对许可证服务器检测证实事件。证实事件指示出许可证服务器要检查作为用于软件许可证的目标许可证服务器的状态。软件许可证是可在具有唯一标识符的许可证服务器处安装的。该唯一标识符基于与云计算环境内基于云的对象相关联的唯一名字的。

[0017] 该许可证服务器响应于该事件请求承担对该基于云的对象的所有权。该基于云的对象具有所有权的独占性,使得单个许可证服务器可在任何时刻拥有该基于云的对象。该许可证服务器被授予对该基于云的对象的所有权。该许可证服务器使用该唯一名字来建立唯一标识符作为用于许可证服务器的标识符。

[0018] 本发明的各实施例可包括或利用专用或通用计算机,该专用或通用计算机包括诸如例如一个或多个处理器和系统存储器等计算机硬件,如下更详细讨论的。本发明范围内的各实施例还包括用于承载或存储计算机可执行指令和/或数据结构的物理和其他计算机可读介质。这样的计算机可读介质可以是可由通用或专用计算机系统访问的任何可用介质。存储计算机可执行指令的计算机可读介质是计算机存储介质(设备)。承载计算机可执行指令的计算机可读介质是传输介质。由此,作为示例而非限制,本发明的各实施例可包括至少两种显著不同的计算机可读介质:计算机存储介质(设备)和传输介质。

[0019] 计算机存储介质(设备)包括 RAM、ROM、EEPROM、CD-ROM、固态驱动器(SSD)(如基于 RAM)、闪存、相变存储器(PCM)、其它类型的存储器、其他光盘存储、磁盘存储或其他磁存储设备、或可用于存储计算机可执行指令或数据结构形式的所需程序代码装置且可由通用

或专用计算机访问的任何其他介质。

[0020] “网络”被定义为允许在计算机系统和 / 或模块和 / 或其他电子设备之间传输电子数据的一个或多个数据链路。当信息通过网络或另一个通信连接(硬连线、无线、或者硬连线或无线的组合)传输或提供给计算机时,该计算机将该连接适当地视为传输介质。传输介质可包括可用于携带计算机可执行指令或数据结构形式的所需程序代码装置并可由通用或专用计算机访问的网络和 / 或数据链路。上述的组合也应被包括在计算机可读介质的范围内。

[0021] 此外,在到达各种计算机系统组件之后,计算机可执行指令或数据结构形式的程序代码装置可从传输介质自动传输到计算机存储介质(设备)(或反之亦然)。例如,通过网络或数据链接接收到的计算机可执行指令或数据结构可被缓存在网络接口模块(例如,“NIC”)内的 RAM 中,然后最终被传输到计算机系统 RAM 和 / 或计算机系统处的较不易失性的计算机存储介质(设备)。因而,应当理解,计算机存储介质(设备)可被包括在还利用(甚至主要利用)传输介质的计算机系统组件中。

[0022] 计算机可执行指令例如包括,当在处理器处执行时使通用计算机、专用计算机、或专用处理设备执行某一功能或某组功能的指令和数据。计算机可执行指令可以是例如二进制代码、诸如汇编语言之类的中间格式指令、或甚至源代码。尽管用结构特征和 / 或方法动作专用的语言描述了本主题,但可以理解,所附权利要求书中定义的主题不必限于上述特征或动作。相反,上述特征和动作是作为实现权利要求的示例形式而公开的。

[0023] 本领域的技术人员将理解,本发明可以在具有许多类型的计算机系统配置的网络计算环境中实践,这些计算机系统配置包括个人计算机、台式计算机、膝上型计算机、消息处理器、手持式设备、多处理器系统、基于微处理器的或可编程消费电子设备、网络 PC、小型计算机、大型计算机、移动电话、PDA、平板、寻呼机、路由器、交换机等等。本发明也可在其中通过网络链接(或者通过硬连线数据链路、无线数据链路,或者通过硬连线和无线数据链路的组合)的本地和远程计算机系统两者都执行任务的分布式系统环境中实施。在分布式系统环境中,程序模块可位于本地和远程存储器存储设备中。

[0024] 在本说明书以及下面的权利要求中,“云计算”被定义为一种用于允许对可配置的计算资源(如网络、服务器、存储、应用、以及服务)的共享池进行无处不在的、方便的、按需的网络访问的模型,这些计算资源可用最小的管理努力或服务提供者交互来快速地被供应和发放。云模型可由各种特性(如按需自服务、广泛网络访问、资源池、快速灵活性、测定的服务等)、服务模型(如软件即服务(SaaS)、平台即服务(PaaS)、基础结构即服务(IaaS))以及部署模型(如私有云、社区云、公共云、混合云等)组成。

[0025] 图 1 示出便于在虚拟化环境中证实许可证服务器的示例计算机架构 100。参考图 1,计算机架构 100 包括云实例 101 和对象管理系统 103。云实例 101 可以是在云内操作的多种云实例之一。云实例 101 和对象管理系统 103 可通过诸如局域网(LAN)、广域网(WAN)和甚至因特网等之类的网络彼此连接(或作为网络的一部分)。因此,云实例 101 和对象管理系统 103 以及任何其他连接的计算机系统及其组件都可以创建消息相关数据并通过网络交换消息相关数据(例如,网际协议(IP)数据报和利用 IP 数据报的其他更高层协议,如传输控制协议(TCP)、超文本传输协议(HTTP)、简单邮件传输协议(SMTP)等)。

[0026] 如所描绘的,云实例 101 包括许可证服务器 102。许可证服务器 102 可以是响应于

许可证请求(如来自应用或其他软件模块)的服务器。对象管理系统 103 可管理诸如账户、文件、用户等之类的、可从云实例(或一般从云环境)访问的对象。对象管理系统 103 管理的对象可被给予唯一名字。对象管理系统 103 管理的对象还可被配置成供独占访问(即对象在任何时间可由单个云实例所拥有)。

[0027] 软件许可证 121 可被存储在计算机架构 100 内。

[0028] 图 2 示出用于在虚拟化环境中证实许可证服务器的示例方法 200 的流程图。方法 200 将参考计算机架构 100 的组件和数据来描述。

[0029] 方法 200 包括对许可证服务器检测证实事件的动作,证实事件指示出该许可证服务器要检查作为用于软件许可证的目标许可证服务器的状态,软件许可证是可在具有唯一标识符的许可证服务器上安装的,该唯一标识符基于与云计算环境内基于云的对象相关联的唯一名字(动作 201)。例如,证实事件 104 可被检测到。证实事件 104 可指示出许可证服务器 102 要检查作为用于软件许可证 121 的目标许可证服务器的状态。软件许可证 121 是可在具有基于名字 107 (对象 106 的名字)的唯一标识符的许可证服务器上安装的。对象 106 可以是具有独占访问权的对象。如此,对象 106 (以及对应的特性)可在任何时刻由单个许可证服务器所拥有。检测证实事件可包括检测软件许可证 121 被存储在云计算环境中。检测证实事件可包括检测指定的时间段已到期(如自从许可证服务器的状态上次被检查以来)。

[0030] 方法 200 包括许可证服务器响应于证实事件请求承担对该基于云的对象的所有权的动作,该基于云的对象具有所有权的所有权独占性,使得单个许可证服务器可在任何时刻拥有该基于云的对象(动作 202)。例如,许可证服务器 102 可响应于证实事件 104 将所有权请求 111 发送到对象管理系统 103。所有权请求 111 可以是承担对对象 106 (基于云的对象)的所有权的请求。

[0031] 方法 200 包括许可证服务器被授予对基于云的对象的所有权的动作(动作 203)。例如,对象管理系统 103 可向许可证服务器 102 授予对象 106 的所有权。对象管理系统 103 可形成指示出对象 106 的所有权的所有权授予 112。对象管理系统 103 可将所有权授予 112 发送给许可证服务器 102。

[0032] 接着,许可证服务器 102 可访问对象 106 以及相应的特性,包括名字 107。

[0033] 方法 200 包括许可证服务器使用该唯一名字来建立唯一标识符作为该许可证服务器的标识符的动作(动作 204)。例如,许可证服务器 102 可使用名字 107 来建立标识符 108 作为许可证服务器 102 的标识符。其他组件(如应用)于是可将对应于软件许可证 121 的许可证请求送往许可证服务器 102。在适当时,这些其他组件可验证许可证服务器 102 具有标识符 108 (且因此是用于软件许可证 121 的许可证服务器)。

[0034] 本发明的实施例包括使用支持由全局唯一账户名引用的存储账户的存储系统。存储系统可从在其中主持许可证服务器的云环境中被访问。在每个存储账户内,有一实体,该实体的访问权在任何时间可仅被云中的单个许可证服务器所拥有。通过将全局唯一存储账户名和对特定唯一实体的独占访问权相组合,可创建唯一 ID,在任何时间云中的单个实例可拥有该唯一 ID。

[0035] 从而,独立软件供应商(ISV)发出的软件许可证可使用唯一存储账户名来指定它可被安装在哪里。云中的许可证服务器周期性地检查对该存储账户中的该特定唯一实体的

访问权的所有权。检查所有权帮助确保许可证服务器是绑定到该相应唯一 ID 的仅有的许可证服务器。因此,许可证不能被重复地部署在多个许可证服务器实例上。

[0036] 对唯一 ID 的所有权可通过底层存储系统的安全机制来被确保。即,在没有对该账户内的特定唯一实体的访问权的情况下,许可证服务器不能采用唯一存储账户名作为其唯一 ID。从而,有可能充分利用用于主持许可证服务器的云环境的可靠性特征。例如,不同于基于硬件的 ID,基于存储账户的 ID 可被容易地从一个云实例转移到另一个。

[0037] 本发明的某些实施例是在 Windows Azure™平台中实现的。这些实施例利用全局独占 Azure 存储账户名,具有存储账户内的特定页团块(blob)的独占映射作为 Windows Azure XDrive。页团块(blob)是用于随机读写操作的页集合(如 512 字节)。xDrive 使得 Windows Azure™应用能够使用现有的应用程序接口(API)来访问持久驱动器。这允许 Windows Azure™应用将页团块(blob)装载为驱动器名(如“X:”)。该映射被用于创建一个 Azure 实例在任何时间能处理的 ID。

[0038] Azure 存储账户名可以是全局唯一的正式 DNS 名。Windows Azure XDrive 允许租用被格式化为单个新技术文件系统(NTFS)卷虚拟硬盘驱动器(VHD)的页团块(blob),用于装载要由单个 Azure 实例独占拥有的 XDrive。这使得 XDrive 有效地成为 Azure 实例的互斥体。软件许可证可因此使用 Azure 存储账户名来标识其安装位置。许可证服务器周期性地检查 XDrive 映射的有效性,以确保它拥有该 ID,且在它不再是所有者时终止其本身。

[0039] 图 3 示出便于在虚拟化环境中证实许可证服务器的另一示例计算机架构 300。如所描绘的,计算机架构 300 包括云环境 301 和存储系统 311。云环境 301 和存储系统 311 可通过网络连接而彼此连接。

[0040] 云环境 301 包括云许可证服务实例 302。云许可证服务实例 302 包括存储账户访问信息 303 以及许可证服务器 304,许可证服务器 304 还包括实施插件 306。存储系统 311 包括存储账户 312,存储账户 312 还包括唯一实体 313。

[0041] 如箭头 321 所指示的,云许可证服务实例 302 保持用于(存储账户云许可证服务实例 302 被绑定到的)存储账户 312 的存储账户访问信息 303。如箭头 322 所示,许可证服务器 304 通过许可证服务器 ID 实施插件 306 定位存储账户 312 中的唯一实体 313。许可证服务器 304 尝试承担对唯一实体 313 的独占访问权。如果尝试失败,云许可证服务实例 302 可将自己关闭。如箭头 323 所指示的,许可证服务器 304 周期性地检查对独占访问权的所有权。如果所有权曾经丢失,则云许可证服务实例 302 可尝试恢复它。如果尝试失败,云许可证服务实例 302 可将自己关闭。

[0042] 因此,本发明的实施例充分利用云计算环境中获得的或构建的一组特征,以便于提供云中主持的许可证服务器的唯一性和不变性的基于软件的解决方案。避免底层硬件系统的特征导致更灵活和可靠的用于主持许可证服务器的平台。云存储服务的特征可被用于创建用于许可证服务器的唯一 ID。主持在公共云环境中的许可证服务器的安全性和可靠性也被提高。

[0043] 本发明可具体化为其它具体形式而不背离其精神或本质特征。所描述的实施例在所有方面都应被认为仅是说明性而非限制性的。因此,本发明的范围由所附权利要求书而非前述描述指示。落入权利要求书的等效方案的含义和范围内的所有改变被权利要求书的范围所涵盖。

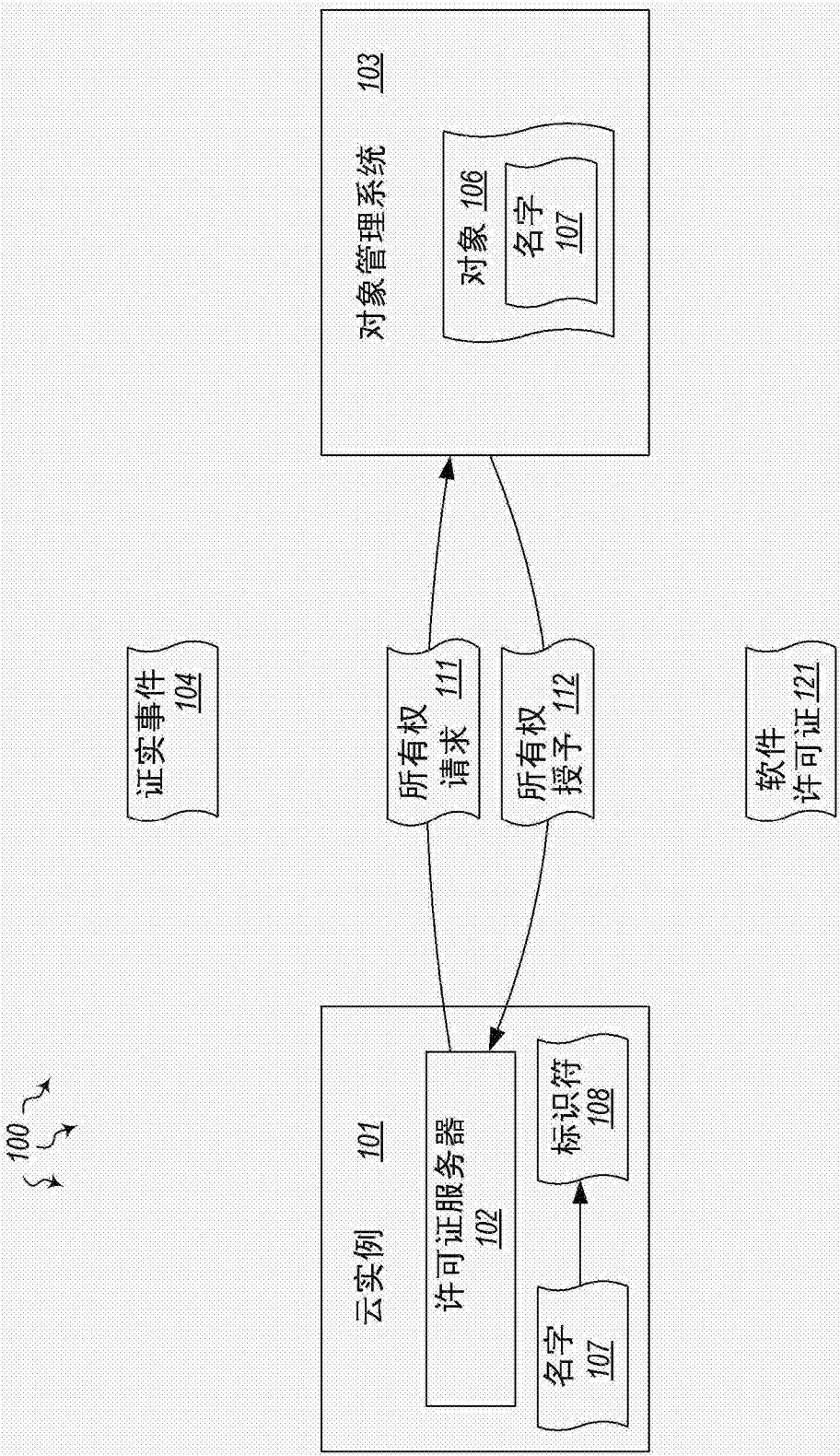


图 1

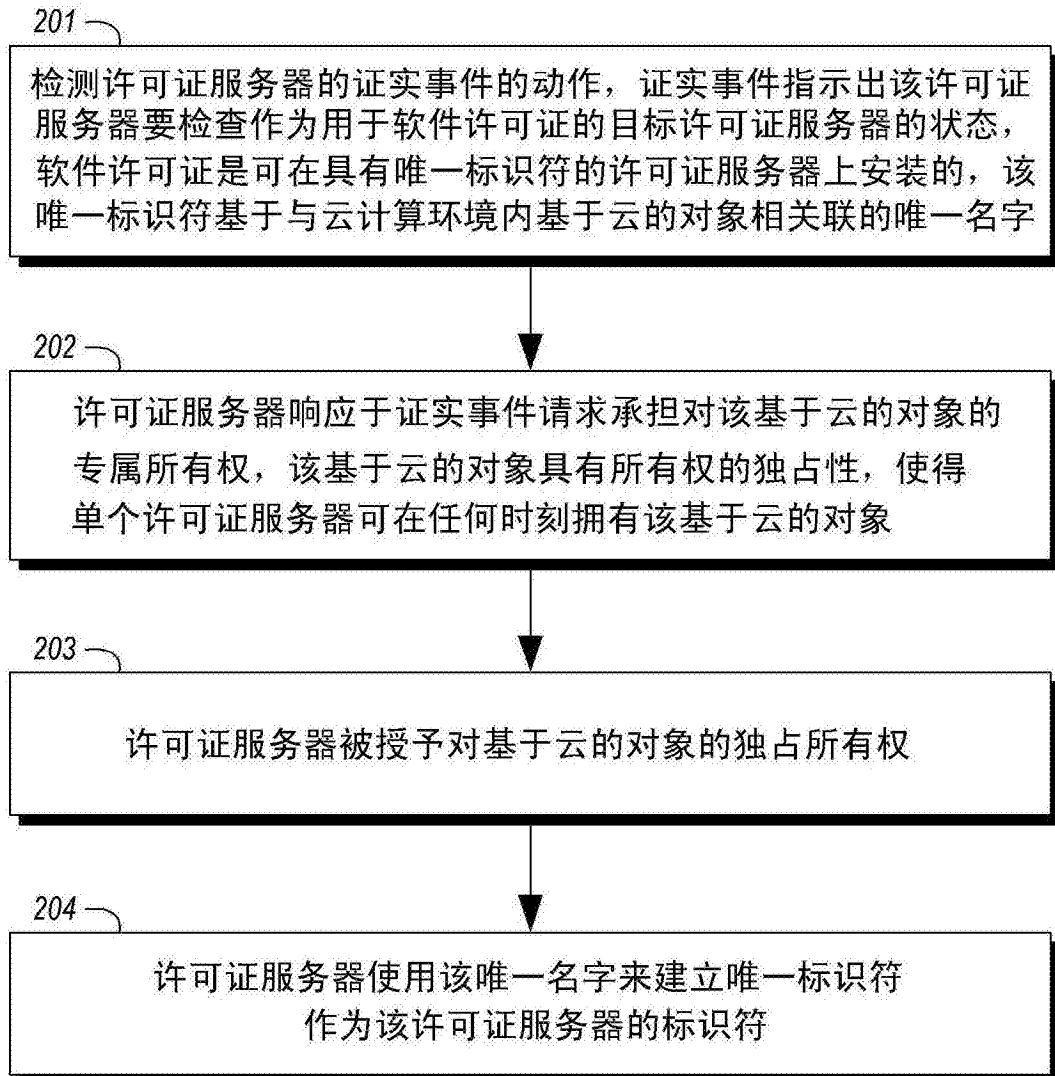
200

图 2

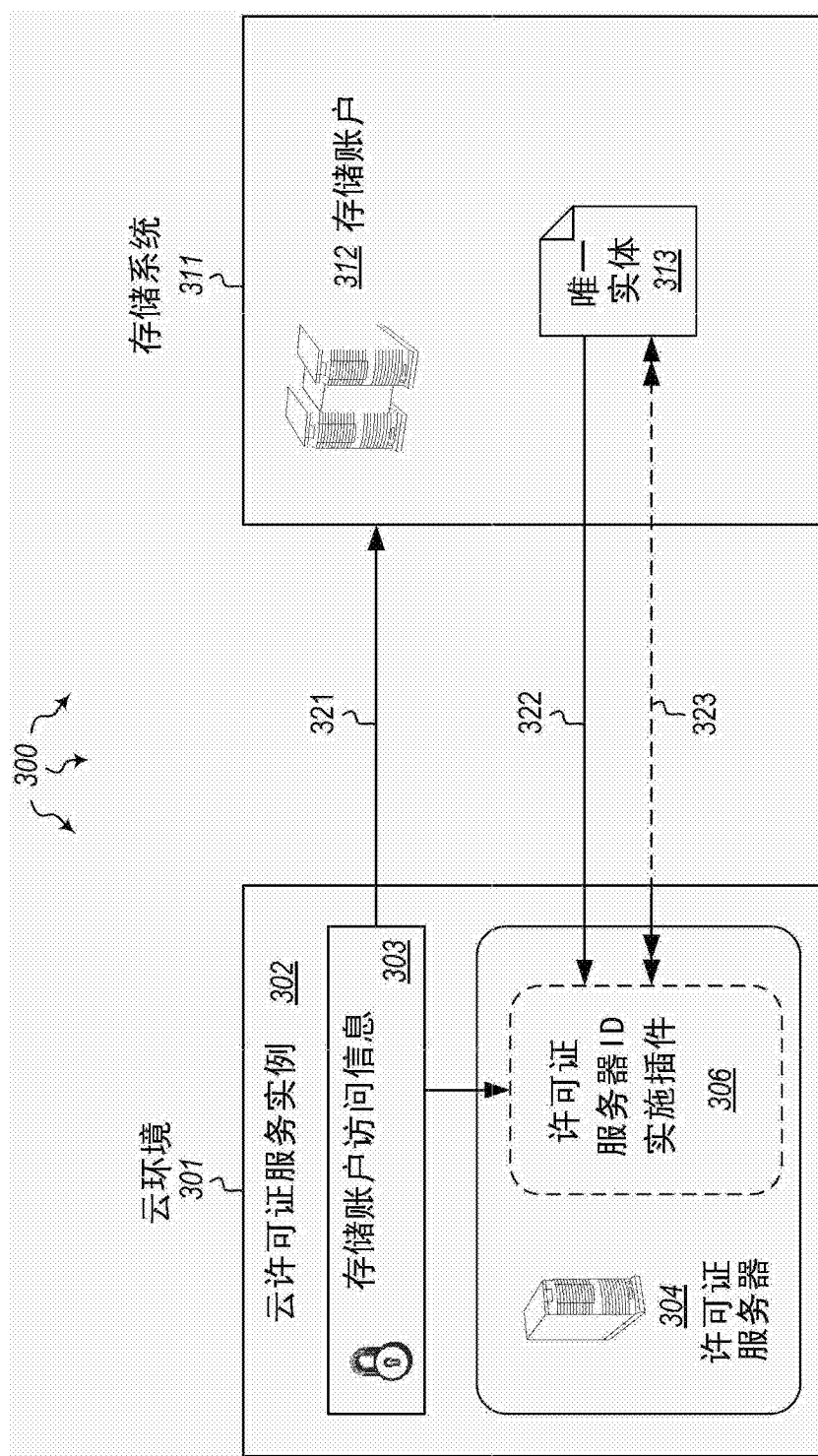


图 3