(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 110113360 B
(45)授权公告日 2022.03.08

(21)申请号 201910454769.3

(22)申请日 2014.11.11

(65)同一申请的已公布的文献号
申请公布号 CN 110113360 A

(43)申请公布日 2019.08.09

(30)优先权数据
61/902,790 2013.11.11 US
14/098,341 2013.12.05 US

(62)分案原申请数据
201480068869.8 2014.11.11

(73)专利权人 亚马逊技术有限公司
地址 美国华盛顿

(72)发明人 托马斯·克里斯托弗·里索
孙·基兰·沙阿
高朗·潘卡吉·梅赫塔
委那塔·N·S·S·哈沙·孔那帕拉如
古鲁普拉卡斯·班加罗尔·饶

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 冯薇

(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/41(2013.01)
G06F 21/62(2013.01)
H04L 67/02(2022.01)
H04L 67/10(2022.01)
H04L 67/306(2022.01)
G06F 9/455(2006.01)

(56)对比文件
FR 2964813 A1,2012.03.16
CN 101076033 B,2011.11.09
CN 101076033 A,2007.11.21
US 2005204143 A1,2005.09.15
CN 101060407 A,2007.10.24
CN 101379794 A,2009.03.04
CN 101321063 A,2008.12.10
US 2009112875 A1,2009.04.30
Amazon.AWS Identity and Access Management Using IAM.《AWS Identity and Access Management Using IAM》.2010,22-25,46,113,120.

审查员 杨金雪

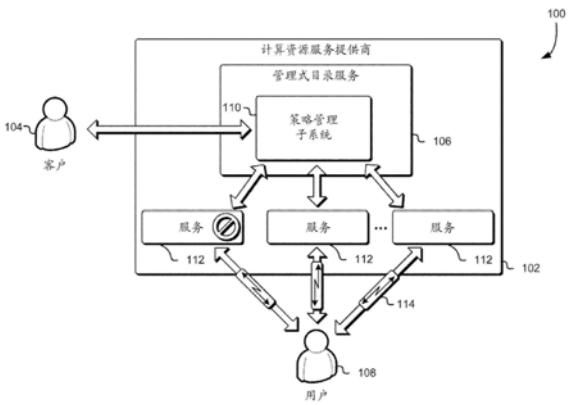
权利要求书2页 说明书20页 附图10页

(54)发明名称

用于访问多个计算资源服务的单组证书

(57)摘要

用户可利用一组证书来通过管理式目录服务访问由计算资源服务提供商提供的一个或多个服务。所述管理式目录服务可被配置来识别可应用于所述用户的一个或多个策略。这些策略可限定对由所述计算资源服务提供商提供的所述一个或多个服务的访问级别。至少部分地基于这些策略,所述管理式目录服务可向身份管理系统传输获得一组临时证书的请求,所述一组临时证书可用于使所述用户能够访问所述一个或多个服务。因此,所述管理式目录服务可被配置来至少部分地基于所述策略以及所述一组临时证书使所述用户能够访问可用于访问所述一个或多个服务的接口。



CN 110113360 B

1.一种计算机系统,包括:

一个或多个处理器;和

存储器,具有共同存储在其中的指令,如果所述指令由计算机系统执行,则使计算机系统:

在目录服务处获得来自请求者的请求,所述请求要求在由目录服务管理的目录内生成用户简档,以使用户能够访问所述目录;

作为认证所述请求者的结果,在所述目录内生成用户简档;

在所述目录服务处生成用户能够用于访问所述目录服务和目录的证书集合;

从所述请求者获得针对用户的访问控制策略集合,以使用户能够根据所述访问控制策略集合访问计算资源服务集合;以及

将所述访问控制策略集合并入所述用户简档,以使用户能够通过所述目录服务、根据所述访问控制策略集合并通过使用所述证书集合来访问所述计算资源服务集合。

2.根据权利要求1所述的计算机系统,其中所述指令使所述计算机系统:

获得所述访问控制策略还使所述计算机系统通过接口提供策略生成器,以使所述请求者能够生成所述访问控制策略集合。

3.根据权利要求1或2所述的计算机系统,其中认证所述请求者的指令包括执行以下操作的指令:

将所述请求发送给所述目录的管理用户,以确定所述请求者是否被授权访问所述目录;

获得来自所述管理用户的响应;以及

基于所述响应确定是否认证所述请求者。

4.根据权利要求1或2所述的计算机系统,其中所述指令还使所述计算机系统能够使所述请求者从所述目录服务对接口进行访问,以至少部分地完成生成所述用户简档的请求,所述接口至少部分地基于对所述请求者的认证才能访问。

5.根据权利要求1或2所述的计算机系统,其中所述指令还使所述计算机系统提供能被所述用户用于根据所述访问控制策略集合来访问所述计算资源服务集合的网络地址的表示。

6.根据权利要求1或2所述的计算机系统,其中使计算机系统获得所述访问控制策略集合的指令还使计算机系统:

识别由所述请求者实现的对应于所述目录的用户简档的策略;

通过接口向所述请求者呈现所述策略;

通过所述接口检测从通过接口呈现的策略中选择的所述访问控制策略集合。

7.根据权利要求1或2所述的计算机系统,其中所述证书集合被配置为由于所述请求者终止用户对所述计算资源服务集合的访问而变得不能被所述请求者使用。

8.一种计算机可读存储介质,其上共同存储有可执行指令,如果所述指令由计算机系统的一个或多个处理器执行,则使所述计算机系统至少:

在目录服务处从请求者获得在所述目录服务管理的目录内生成用户简档的请求;

作为所述请求有效的结果,生成所述用户简档;

生成与所述用户简档关联的用户能够用于访问所述目录的证书集合;

从所述请求者获得适用于用户确定对服务集合的访问级别的策略集合;以及

向所述用户提供所述证书集合,以使用户能够根据所述策略集合通过所述目录来访问所述服务集合。

9.根据权利要求8所述的计算机可读存储介质,其中所述可执行指令还使所述计算机系统:

将所述请求发送给所述目录的管理用户以验证所述请求;

获得来自所述管理用户的响应,所述响应指示所述请求者的请求有效;以及

生成所述用户简档。

10.根据权利要求8或9所述的计算机可读存储介质,其中所述可执行指令还使所述计算机系统能够使所述请求者从所述目录服务对接口进行访问,以至少部分地完成生成所述用户简档的请求,所述接口至少部分地基于对所述请求者的验证才能访问。

11.根据权利要求8或9所述的计算机可读存储介质,其中所述指令还使所述计算机系统向所述用户提供用户可用于提交访问所述服务集合的请求的接口的网络地址的表示。

12. 根据权利要求8或9所述的计算机可读存储介质,其中所述指令还使所述计算机系统:

获得废除所述证书集合的第二请求;以及

作为废除了所述证书集合的结果,终止用户通过目录访问所述服务集合。

13.根据权利要求8或9所述的计算机可读存储介质,其中使所述计算机系统获得所述策略集合的指令还使所述计算机系统通过接口向所述请求者提供策略生成器,以使所述请求者能够通过所述策略生成器生成所述策略集合。

14. 根据权利要求8或9所述的计算机可读存储介质,其中使所述计算机系统获得所述策略集合的指令还使所述计算机系统:

通过接口向所述请求者提供适用于所述目录的用户简档的访问控制策略集合;以及

通过所述接口检测从通过接口呈现的访问控制策略集合中选择的所述策略集合。

15.一种计算机实现的方法,包括:

在目录服务处从请求者获得在所述目录服务管理的目录中生成用户的用户简档的请求,所述用户简档能用于使用户能够通过所述目录访问服务集合;

响应于所述请求,在所述目录中生成所述用户简档;

获得所述用户的证书集合,所述证书集合能被用户用于访问所述目录;

识别所述用户的策略集合以确定对服务集合的访问级别;以及

将所述策略集合应用于所述用户简档,以使所述用户能够根据所述策略集合、利用所述证书集合并通过所述目录来访问所述服务集合。

用于访问多个计算资源服务的单组证书

[0001] 本申请是2006年6月16日(申请日:2004年11月11日)向中国专利局递交并进入中国国家阶段的题为“用于访问多个计算资源服务的单组证书”的发明专利申请No.201480068869.8(PCT国际申请No.PCT/US2014/065081)的分案申请。

[0002] 相关申请的交叉引用

[0003] 本申请出于所有目的以引用的方式并入以下专利申请的完整公开内容:2013年11月11日提交的标题为“MANAGED DIRECTORY SERVICE”的美国专利临时申请号61/902,790,以及2013年12月5日提交的标题为“SINGLE SET OF CREDENTIALS FOR ACCESSING MULTIPLE COMPUTING RESOURCE SERVICES”的美国专利申请号14/098,341。

背景技术

[0004] 客户利用目录服务创建并维持用于数据管理并且通常用于访问多种资源的目录(例如,文件系统、文件、用户、安全策略、网络资源、应用、系统存储等)。目录服务可被配置来取决于客户的业务需求在由客户操作的数据中心中(例如,本地)或在远程网络中(例如,外地)创建目录。然而,期望维持本地和外地目录的客户可能遇到众多困难。例如,利用本地目录的客户可能需要创建单独的外地目录并且在两个目录之间创建同步数据以便维持相同数据集。这可需要客户针对目录的每名用户维持多个账户。此外,多个目录的维护可能增加客户的管理负担,因为多个目录的维护和安全可能需要执行另外的资源。用户可能必须执行一组复杂的操作来获得用于访问目录以及由计算资源服务提供商提供的一个或多个其他服务的一组或多组另外的证书,这样使得问题更为严重。

附图说明

[0005] 将参考附图描述根据本公开的各个实施方案,在附图中:

[0006] 图1示出可实现各个实施方案的环境的说明性实例;

[0007] 图2示出根据至少一个实施方案的用于访问分布式计算机系统环境上的目录对象以及在其上运行的相关联代码的环境的说明性实例;

[0008] 图3示出根据至少一个实施方案的用于服务用户请求认证、授权以及访问分布式计算机系统环境上的远程目录对象的环境的说明性实例;

[0009] 图4示出可实现各个实施方案的环境的说明性实例;

[0010] 图5示出根据至少一个实施方案的应用到用户的一组策略的说明性实例;

[0011] 图6示出根据至少一个实施方案的用于建立可应用于管理式目录服务的用户的策略的策略生成器的说明性实例;

[0012] 图7示出根据至少一个实施方案的由策略生成器产生的应用到管理式目录服务的用户的一组策略的说明性实例;

[0013] 图8示出根据至少一个实施方案的用于限定用户访问一个或多个计算资源服务的过程的说明性实例;

[0014] 图9示出根据至少一个实施方案的用于使用户能够访问一个或多个计算资源服务

的过程的说明性实例;并且

[0015] 图10图示可实现各个实施方案的环境。

具体实施方式

[0016] 在以下描述中,将描述各个实施方案。出于解释的目的,将阐述具体的配置和细节,以便提供实施方案的透彻理解。然而,对本领域的技术人员将是显而易见的是,在没有具体细节的情况下也可实践实施方案。此外,为了不使所描述的实施方案晦涩,可能会省略或简化众所周知的特征。

[0017] 本文描述和建议的技术涉及一个或多个用户的集中策略管理,使得一组证书可用于访问目录以及由计算资源服务提供商提供的一个或多个服务。在一个实施方案中,负责管理可通过管理式目录服务可用的目录的实体(例如,组织)为利用目录的一个用户或多个用户指定一个或多个策略。实体可以是操作各种服务的计算资源服务提供商的客户,所述服务诸如虚拟计算机系统服务、基于对象的数据存储服务、数据库服务、上述管理式目录服务以及多个其他服务。

[0018] 在一些实施方案中,客户与管理式目录服务内的策略管理子系统通信,以便限定影响用户访问由目录管理的应用和资源和/或影响用户访问由计算资源服务提供商提供的一个或多个其他服务的一个或多个策略。例如,客户可创建防止用户或用户群执行目录内的特定应用(例如,文字处理应用、照片编辑应用等)的策略。在另一个实例中,客户可创建防止用户或用户群防问由计算资源服务提供商提供的虚拟计算机系统服务或者在由计算资源服务提供商提供的数据库服务内执行写入动作的策略。

[0019] 在一个实施方案中,一旦用户策略已经生成,用户就可利用统一资源标识符(URI),用户或用户群可使用所述URI来访问计算资源服务提供商接口。此计算资源服务提供商接口可被配置来使用户或用户群能够访问由计算资源服务提供商提供的一个或多个服务。例如,用户可使用计算资源服务提供商接口来访问虚拟计算机系统服务并且请求提供虚拟机实例。另外,可根据所限定可应用用户策略定制计算资源服务提供商接口。例如,如果所限定用户策略指定不准许用户访问基于对象的数据存储服务,那么计算资源服务提供商接口可被配置来不包括与这类服务相关的任何授权。

[0020] 在一个实施方案中,当用户利用URI来访问计算资源服务提供商接口时,管理式目录服务内的策略管理子系统获得所限定用户策略来确定访问由计算资源服务提供商提供的各种服务的参数。一旦已获得用户策略,策略管理子系统就可与身份管理服务通信,诸如通过一个或多个适当配置的应用编程接口(API)调用服务,以便请求与已经同意用户访问的服务相关的临时证书。因此,可将这些临时证书传输到策略管理子系统以便使用户能够访问准许的服务和操作。另外,策略管理子系统还可与身份管理服务通信来提供有待实施的用户专用策略。一旦策略管理子系统已经接收一组临时证书并且已经将有待实施的策略传输到身份管理服务,策略管理子系统就可使用户能够访问定制的计算资源服务提供商接口。

[0021] 以此方式,目录的用户或用户群可使用用于访问目录的一组单个证书以便访问由计算资源服务提供商提供的一个或多个其他服务,而无需管理用于这些一个或多个其他服务的另外组的证书。另外,本文描述和建议的技术促进另外的技术优点。例如,因为客户可

利用管理式目录服务内的策略管理子系统来为由计算资源服务提供商提供的任何服务指定用户策略，客户可能不需要访问任何其他服务或接口来指定服务专用的用户策略。这进而可减小客户的潜在管理负担。

[0022] 图1示出可实践各个实施方案的环境100的说明性实例。在环境100中，计算资源服务提供商102向计算资源服务提供商的一个或多个客户提供各种计算资源服务。计算资源服务提供商102可以是代表一个或多个客户托管各种计算资源的组织。例如，计算资源服务提供商可操作用于托管各种计算硬件资源的一个或多个设施(诸如硬件服务器、数据存储装置、网络装置)以及其他设备(诸如服务器机架、联网电缆等等)。计算资源服务提供商可利用其计算硬件资源来操作一个或多个服务。此类服务可包括使计算资源服务提供商的客户能够远程管理计算资源来支持客户的操作，同时减少或甚至消除客户投资物理设备的需求的服务。示例性服务包括但不限于：各种数据存储服务(基于对象的存储服务、档案数据存储服务、数据库服务等等)、程序执行服务以及其他服务。服务可由客户使用来支持广泛多种活动，诸如运营网站、操作支持组织的企业系统、分布式计算和/或其他活动。

[0023] 因此，如图1所示，环境100包括客户104。客户104可以是可利用由计算资源服务提供商102提供的一个或多个服务来操作并管理一个或多个目录(例如，文件系统、文件、用户、安全策略、网络资源、应用、系统存储等)以支持他或她的操作的组织。客户104可通过客户计算机系统装置向由计算资源服务提供商102提供的管理式目录服务106提交对可用于促进在一个或多个用户108之间的数据共享和/或可用性的目录进行配置的一个或多个请求。因此，管理式目录服务106可另外包括策略管理子系统110，所述策略管理子系统110可被配置来允许客户104生成并修改一个或多个用户配置文件，以便限定远程访问目录内可用的一个或多个应用和资源和/或由计算资源服务提供商102提供的一个或多个其他服务112。例如，客户104可访问策略管理子系统110以允许用户108访问目录内的文字处理应用以及由计算资源服务提供商102提供的虚拟计算机系统服务，同时禁止访问其他应用和服务。

[0024] 如下将更详细描述的，客户104可与用户配置文件接口交互以访问策略生成器并因此访问策略管理子系统110。在一个实施方案中，客户104可通过管理式目录服务106内的每个用户配置文件中可用的策略生成器按钮访问策略管理子系统110。策略生成器可使客户104能够为特定用户108指定可用于限定对各种应用和/或服务的访问级别的一个或多个策略。因此，当客户104限定有待通过策略生成器应用到特定用户108的可应用策略时，策略生成器可将一个或多个可执行指令传输到策略管理子系统110以便并入并实施所指定策略。另外，在一个实施方案中，当客户104指定使用户108能够访问由计算资源服务提供商112提供的一个或多个服务102的一个或多个策略时，策略管理子系统110将URI114传输给用户108，所述用户108可使用所述URI 114来访问计算机资源服务提供商接口以便根据所实现策略访问并利用可应用服务112。可替代地，一旦一个或多个策略已被限定用于用户108，客户104就可将URI 114诸如通过电子邮件或其他递送系统传输给用户108。

[0025] 当用户108访问目录并且使用URI 114来访问计算资源服务提供商接口时，策略管理子系统110可访问用户的目录配置文件来识别由客户104指定的有待实施的策略。至少部分地基于这些策略，策略管理子系统可被配置来将一个或多个可执行指令传输到身份管理系统(未示出)，以便获得用于访问由计算资源服务提供商102提供的一个或多个服务112的

临时证书，和/或限定用户108可在这些服务内采取的一个或多个动作。一旦策略管理子系统110已经获得这些证书，策略管理子系统110就可生成用户专用计算资源服务提供商接口，并且使用户108能够根据由客户104限定并且可应用于用户108的策略访问由计算资源服务提供商102提供的一个或多个服务112。

[0026] 图2图示根据至少一个实施方案的用于访问分布式和/或虚拟计算机系统环境上的计算机系统目录资源以及在其上运行的相关联代码的环境200，所述资源包括但不限于计算机系统服务，诸如目录服务和资源(诸如与目录服务相关联的用户资源、策略资源、网络资源和/或存储资源)。计算机系统实体、用户或过程202可通过计算机系统客户端装置204连接到计算机系统，并且可请求通过连接206访问一个或多个服务226。请求访问服务的一条或多条命令可起源于外部计算机系统和/或服务器，或者可起源于远程网络位置上的实体、用户或过程，或者可起源于计算机系统，或者可起源于计算机系统客户端装置的用户，或者可起源于这些和/或其他此类对象的组合。在一些实施方案中，请求访问服务的一条或多条命令可由以下各项发布：特权用户、或非特权用户、或自主过程、或警报或状态，或者这些和/或其他方法的组合。

[0027] 计算机系统客户端装置可请求通过一个或多个网络216和/或与其相关联的实体访问服务，所述实体诸如直接或间接连接到网络的其他服务器。计算机系统客户端装置可包括能够通过网络与计算机系统连接的任何装置，所述装置至少包括以下各项：服务器、膝上型计算机、移动装置(诸如智能手机或平板计算机)、其他智能装置(诸如智能手表、智能电视、机顶盒、视频游戏控制台以及其他此类网络启用的智能装置)、分布式计算系统及其部件、抽象部件(诸如客户计算机系统或虚拟机)，和/或其他类型的计算装置和/或部件。网络可包括例如，本地网络、内部网络、公共网络(诸如互联网)、广域网、无线网、移动网络、卫星网络，具有多个网络节点的分布式计算系统和/或类似物。网络还可根据各种协议操作，诸如以下列举的协议：蓝牙、WiFi、蜂窝网络协议、卫星网络协议和/或其他协议。

[0028] 在一些实施方案中，计算机系统可包括一个或多个本地计算机系统资源208，所述本地计算机系统资源208可至少部分地位于客户驻地上并且可在其上存储文件和/或其他计算机系统资源，所述其他计算机系统资源包括但不限于，目录、应用、数据、数据库、到其他计算机系统资源的链路、系统驱动器、计算机操作系统、虚拟机和/或其他此类资源。在一些实施方案中，本地计算机系统资源可以是本地文件系统资源并且可被存储在多种存储装置上，诸如系统随机存取存储器(RAM)、磁盘驱动器、固态驱动器、可移动驱动器或者这些和/或其他此类存储装置的组合。在一些实施方案中，本地计算机系统资源可至少部分地位于数据中心(可并置的多个计算机系统资源、服务和/或存储装置)，所述数据中心可由计算机系统客户端装置通过一个或多个连接(例如像本文描述的网络连接)访问。计算机系统资源和/或数据中心可本地或者本地和远程的组合定位。例如，在一些实施方案中，文件系统和/或目录可位于定位在本地数据中心中的磁盘上，并且文件系统和/或目录的内容还可被复制到位于远程数据中心中的磁盘。在一些其他实施方案中，文件系统和/或目录可使其内容的至少一部分位于可以是本地的一个数据中心中，并且使其内容的其他部分位于可以是本地或远程的一个或多个其他数据中心中。存储装置可包括物理装置(诸如本文描述的那些)和/或此类物理装置的虚拟表示。例如，文件系统和/或目录存储装置可包括一定数目的物理存储器，所述物理存储器的部分致力于作为虚拟磁盘驱动器存储，其中文件系统在虚

拟磁盘驱动器上创建。其他此类本地存储装置可被认为是在本公开的范围内。

[0029] 在一些实施方案中，服务226可需要访问一个或多个计算机系统目录资源，诸如本文描述的那些。在一些实施方案中，服务226可包括多种其他计算机系统实体，包括但不限于用户、其他计算机系统、过程和/或自动化过程和/或其他此类计算机系统实体。在一些实施方案中，对系统目录资源的访问214可由诸如管理式目录服务218的服务提供，所述服务可提供对一个或多个系统资源的访问。管理式目录服务可提供多种服务来使计算机系统和/或计算机系统客户端装置能够访问系统资源，包括但不限于220认证、222授权以及224目录服务。

[0030] 例如，管理式目录服务可提供220认证服务，所述认证服务可认证用户、计算机系统、过程、自动化过程或其他此类实体的证书以便至少确定实体是否被授权访问管理式目录服务和/或与管理式目录服务相关联的系统资源。在一些实施方案中，证书可由管理式目录服务本身认证，或者它们可由在管理式目录服务的控制下的过程、程序或服务认证，或者它们可由管理式目录服务可与其通信的过程、程序或服务认证，或者它们可由这些和/或其他此类服务或实体认证。

[0031] 管理式目录服务还可提供222授权服务，所述授权服务可授权用户、计算机系统、过程、自动化过程或其他此类实体来至少确定实体可执行一个或多个可能动作中的哪些动作。例如，就计算机系统资源，诸如文件系统资源而言，实体可被或可不被授权链路执行的动作包括但不限于：在文件系统资源上创建文件系统；销毁文件系统资源上的文件系统；附接到文件系统资源上的文件系统；从文件系统资源上的文件系统分离；提供到文件系统资源上的文件系统的访问；改造到文件系统资源上的文件系统的访问链路；允许从文件系统资源上的文件系统读取；允许写入文件系统资源上的文件系统和/或其他此类文件资源动作。

[0032] 对系统资源的动作可包括但不限于：对目录、文件、应用、数据、数据库、到其他资源的链路、系统驱动器、操作系统、虚拟机和/或其上的其他此类系统资源对象的动作，并且可包括如本文提及的动作的此类动作。开始、停止、改造、销毁和/或以其他方式管理系统资源的动作以及其他此类动作也可被包括在可用动作中。执行动作的授权可由实体管理，诸如证书授予或策略系统，诸如一个系统，所述系统例如维持与某一实体相关的一组证书和/或策略，并且可至少部分地基于所述一组证书和/或策略确定实体被授权执行哪些动作。实体可被授权执行的动作可以是静态的或者可根据许多因素改变，所述因素包括但不限于：时刻，证书类型，系统策略，正被访问对象的本质、类型或位置，或者这些和/或其他此类授权因素的组合。例如，计算机系统实体可仅被授权读取文件系统上的某些文件、读取和写入文件系统上的某些其他文件，并且添加和删除文件系统上的某些其他文件。不同计算机系统实体可被授权对文件系统执行任何动作，但是只有当这些动作从某一位置并且在某一时刻开始时才执行。一个或多个过程可仅被授权向文件系统上的文件写入例如像系统日志，而其他过程可仅被授权从文件读取。如可设想的，这些是说明性实例。其他类型的操作可由管理式目录服务授权系统授权，并且此类其他类型的操作还可被认为是在本公开的范围内。

[0033] 管理式目录服务还可提供224目录服务，所述目录服务可根据授权证书和/或策略提供所认证实体对计算机系统资源的访问214。例如，在计算机系统实体可被授权读取和写

入存储在计算机系统资源(诸如文件系统资源)上的某些数据的实施方案中,读取和写入的能力可由目录服务提供。目录服务可通过提供到文件系统资源位置的链路(诸如通过URI对象或一些其他此类链路)来提供对文件系统资源的访问。URI可由以下各项提供:计算机系统客户端装置、或在数据中心处运行的过程、或在连接到数据中心的计算机系统上运行的过程、或管理式目录服务,或者这些和/或其他此类计算机系统实体的组合。

[0034] 在一些实施方案中,对计算机系统资源的访问可以请求实体不可见所述访问的形式提供。例如,访问214可被提供给请求实体作为URI或到本地文件系统208上的位置210的其他此类链路。计算机系统资源上的位置可由在计算机系统上运行的一个或多个过程翻译212成URI。请求访问计算机系统资源的服务或实体226可使用228所接收URI来访问计算机系统资源,而无需依赖于计算机系统资源的位置的配置,并且在一些实施方案中,可使用URI来链接到计算机系统资源,以便犹如服务或实体226被直接连接到计算机系统资源一样工作。例如,似乎向文件(所述文件对于服务或实体来说可能似乎是有待位于服务或实体本地的位置)写入一组数据的操作可实际上将数据打包成网络数据包,并随后可通过网络216通过访问链路214传送所述包,以实际写入位于本地文件系统208上的文件。如可设想的,这些是说明性实例,并且可由管理式目录服务执行的其他类型的操作还可被认为是在本公开的范围内。

[0035] 图3示出如本文所述至少结合图2并且根据至少一个实施方案的环境300,所述环境300用于服务用户请求本地和/或远程服务认证、授权并访问分布式和/或虚拟计算机系统环境上的本地和/或远程计算机系统资源。计算机系统实体、用户或过程302可通过计算机系统客户端装置304连接到计算机系统,并且可306请求认证证书以便促进计算机系统实体、用户或过程访问一个或多个本地和/或远程服务。请求认证证书的一条或多条命令可起源于外部计算机系统和/或服务器,或者可起源于远程网络位置上的实体、用户或过程,或者可起源于计算机系统,或者可起源于计算机系统客户端装置的用户,或者可起源于这些和/或其他此类对象的组合。在一些实施方案中,请求认证证书的一条或多条命令可由以下各项发布:特权用户、或非特权用户、或自主过程、或警报或状态,或者这些和/或其他方法的组合。

[0036] 计算机系统客户端装置304可通过使用一个或多个网络308和/或与其相关联的实体连接到计算机系统,所述实体诸如直接或间接连接到网络的其他服务器。计算机系统客户端装置可包括能够通过网络与计算机系统连接的任何装置,所述装置至少包括以下各项:服务器、膝上型计算机、移动装置(诸如智能手机或平板计算机)、其他智能装置(诸如智能手表、智能电视、机顶盒、视频游戏控制台以及其他此类网络启用的智能装置)、分布式计算系统及其部件、抽象部件(诸如客户计算机系统或虚拟机),和/或其他类型的计算装置和/或部件。网络可包括例如,本地网络、内部网络、公共网络(诸如互联网)、广域网、无线网、移动网络、卫星网络,具有多个网络节点的分布式计算系统和/或类似物。网络还可根据各种协议操作,诸如以下列举的协议:蓝牙、WiFi、蜂窝网络协议、卫星网络协议和/或其他协议。

[0037] 在一些实施方案中,计算机系统客户端装置304可访问在管理式目录服务310上运行和/或在其控制下的一个或多个认证过程312,其中所述认证过程可被配置来至少响应于来自外部过程的请求并且认证请求计算机系统实体、用户或过程的证书。例如,认证过程可

验证314是否允许正请求的计算机系统实体、用户或过程访问管理式目录服务。认证过程可通过以下方式验证访问管理式目录服务:核实用户名和密码组合;或者核实存储在硬件、软件、固件或其他此类装置上的密码密钥;或者核实计算机系统客户端装置是否被授权请求访问;或者核实网络是否被授权请求访问;或者这些和/或其他此类核实方法的组合。认证过程可执行其他此类认证任务,并且在一些实施方案中可结合在计算机系统上和/或在其他计算机系统上运行的其他过程和/或结合存储在所述计算机系统和/或其他计算机系统上的数据执行认证任务。

[0038] 在一些实施方案中,如本文所述的计算机系统实体、用户或过程302可使用如本文所述的一个或多个网络308和/或与其相关联的实体通过如本文所述的计算机系统客户端装置304连接到计算机系统,并且可316请求授权在一个或多个计算机系统资源332上执行一个或多个操作和/或过程,所述一个或多个计算机系统资源332可例如至少部分地位于数据中心中,诸如本文至少部分结合图2并且根据至少一个实施方案所述的数据中心。在一些实施方案中,所请求的操作授权可以是直接执行一个或多个计算机系统资源操作的请求授权。在一些实施方案中,所请求的操作授权可以是间接执行一个或多个计算机系统资源操作的请求操作。例如,所请求的操作授权可以是授权在计算机系统实体、用户或过程302控制下的远程计算机系统服务、过程或实体的请求以用于授权执行一个或多个计算机系统资源操作。授权可从在管理式目录服务310上运行和/或在其控制下的一个或多个授权过程318请求,其中所述授权过程可被配置来至少响应于来自外部过程的请求并且授权计算机系统实体、用户或过程在一个或多个计算机系统资源332上执行一个或多个操作和/或过程。计算机系统资源可位于本地(诸如位于客户驻地上的数据中心)、或者可位于外地、或者可位于多个远程位置(诸如分布式和/或虚拟计算机系统),或者可位于本地和/或远程位置的组合。例如,文件系统可位于定位在本地数据中心中的本地磁盘上,并且文件系统的内容还可被复制到位于一个或多个远程数据中心中的一个或多个远程磁盘。在一些实施方案中,文件系统可使其内容的至少一部分位于可以是本地或远程的一个数据中心中,并且使其内容的其他部分位于一个或多个其他数据中心中。

[0039] 可授权的操作和/或过程的实例包括但不限于:320创建和/或销毁资源对象;322读取和/或写入资源对象和/或其他此类系统资源操作。授权可根据以下各项变化:实体、用户或过程;时刻;实体类别;用户类别;过程类别;一个或多个系统策略;请求实质;或者这些和/或其他此类考虑的组合。例如,计算机系统实体可被授权创建文件和/或目录但不能被授权删除所述文件和/或目录,或者过程可仅被授权删除由所述过程创建的文件和/或目录,并且其他人或实体不能被授权读取某些目录中的文件,而其他人则能够读取。如可设想的,这些是说明性实例。其他类型的操作可由管理式目录服务授权系统授权,并且此类其他类型的操作还可被认为是在本公开的范围内。

[0040] 在一些实施方案中,如本文所述的计算机系统实体、用户或过程302可使用如本文所述的一个或多个网络308和/或与其相关联的实体通过如本文所述的计算机系统客户端装置304连接到计算机系统,并且可324创建和/或例示可请求访问一个或多个文件系统332的一个或多个本地和/或远程服务328。在一些实施方案中,计算机服务、过程或实体328可访问在管理式目录服务310上运行和/或在其控制下的一个或多个目录服务过程326,其中所述目录服务过程可被配置来至少响应于来自外部过程的请求并且提供对一个或多个文

件系统的访问。访问一个或多个文件系统可包括访问操作，诸如文件和/或其他文件系统对象(诸如目录、应用、数据、数据库、到其他文件系统的链路、系统驱动器、计算机操作系统、虚拟机和/或其他此类文件系统对象)上的操作，诸如读取、写入、执行、删除、创建、例示和/或其他此类操作。在一些实施方案中，访问操作可通过与如本文所述的一个或多个授权过程318的通信330促进，从而根据包含在其中的资源授权策略提供授权。

[0041] 图4示出根据至少一个实施方案的包括由计算资源服务提供商402提供的管理式目录服务404的各个部件的环境400的说明性实例。管理式目录服务404可向客户和委托管理用户(例如，由客户识别的具有执行通常允许客户进行的一个或多个动作的管理权限的用户)提供可使客户或委托管理用户能够访问管理式目录服务404的接口406。客户或委托管理用户可通过诸如互联网的一个或多个通信网络利用接口406。接口406可包括某些安全保障来确保客户或委托管理用户具有访问管理式目录服务404的授权。例如，为了访问管理式目录服务404，客户在使用接口406时可能需要提供用户名和对应密码或加密密钥。另外，提交给接口406的请求(例如，API调用)可需要使用密码密钥生成的电子签名，使得电子签名可由管理式目录服务404核实，诸如通过授权系统(未示出)。

[0042] 通过接口406，客户或委托管理用户可以能够查看目录结构，包括目录内所有可用计算机以及被授权访问目录的用户的列表。因此，客户或委托管理用户可使用接口406来访问一个或多个用户配置文件408以便查看用户属性(例如，姓氏和名字、位置、手机号等)，并且限定可用于确定对由计算资源服务提供商402提供的一个或多个服务414的访问级别、以及对一个或多个应用412和/或由目录管理的其他资源的访问级别的一个或多个策略。如以下将结合图5-7更详细描述的，每个用户配置文件408可包括策略生成器按钮，所述策略生成器按钮在被选择时使客户或委托管理用户能够访问策略生成器来限定这些一个或多个策略。例如，通过策略生成器，客户或委托管理用户可指定用户可访问的服务414以及用户可在这些服务414内采取的动作。因此，一旦客户或委托管理用户已通过策略生成器限定可应用用户策略，客户或委托管理用户就可以能够查看用户配置文件408内所应用的策略。另外，策略生成器可将一个或多个可执行指令传输到策略管理子系统410，所述一个或多个可执行指令可致使策略管理子系统410使用户能够利用URI来访问计算资源服务提供商接口。此计算资源服务提供商接口可使用户能够访问由来自目录内的计算资源服务提供商402提供的一个或多个服务414。

[0043] 在一个实施方案中，当用户利用来自目录内的URI访问计算资源服务提供商接口时，管理式目录服务404内的策略管理子系统410将访问用户配置文件408来获得可应用于用户的一组策略。如上所指出的，策略可包括由计算资源服务提供商402提供的可由用户访问的一个或多个服务414。因此，策略管理子系统410可将一个或多个可执行指令传输到身份管理服务以便获得可用于访问一个或多个服务414的临时证书。策略管理子系统410可被配置来生成包括已经同意用户访问的一个或多个服务414的定制计算资源服务提供商接口。由于策略管理子系统管理访问一个或多个服务414所必需的临时证书，用户可利用此定制接口来访问一个或多个服务414而无需另外的证书。

[0044] 除了可被建立来控制用户访问由计算资源服务提供商402提供的一个或多个服务414的策略之外，客户或委托管理用户可利用接口406来访问策略管理子系统410以便限定可影响用户访问目录内的一个或多个应用412的一个或多个策略。例如，客户或委托管理用

户可通过接口406与策略管理子系统410交互以便创建策略，所述策略在被实施时禁止用户或用户群访问目录内的文字处理应用。因而，当用户试图利用文字处理应用时，用户可接收通知用户他/她并不能访问应用的错误消息。

[0045] 如上所指出的，客户或委托管理用户可利用管理式目录服务接口来访问一个或多个用户配置文件以便指定一组策略，所述一组策略在被实施时可禁止或使用户能够访问由计算资源服务提供商提供的一个或多个服务。因此，图5是根据至少一个实施方案的用于生成一个或多个策略的用户配置文件接口502的说明性实例。用户配置文件接口502可包括策略显示器504，所述策略显示器504被配置来提供关于当前应用到用户配置文件的策略的说明性信息。例如，如图5所示，提供在策略显示器504上的策略可允许用户(在这种情况下为Joe B)访问基于对象的数据存储服务以便生成和/或访问一个或多个数据对象。因而，当用户利用URI访问计算资源服务提供商接口时，上述策略管理子系统可获得此策略并且将一个或多个可执行指令传输到由计算资源服务提供商提供的身份管理系统，以便获得用于访问基于对象的数据存储服务的临时证书。另外，策略管理子系统可使用所获得的这个策略来根据/遵守策略定制计算资源服务提供商接口。

[0046] 用户配置文件接口502可包括策略生成器按钮506，，所述策略生成器按钮506在由客户或委托管理用户选择时可将一个或多个可执行指令传输到网络浏览应用，所述一个或多个可执行指令可致使应用访问策略生成器。策略生成器可包括可用于针对指定用户创建一个或多个策略的接口。应注意，只有客户或委托管理用户可利用策略生成器按钮506来使用策略发生器创建或修改特定用户策略。例如，如果并未被识别为委托管理用户的用户试图使用策略生成器按钮506，那么错误消息可被传输到用户接口，所述用户接口可被配置来通知用户还未同意他/她访问策略生成器。可替代地，如果用户并不能访问策略生成器，那么可隐藏或禁用策略生成器按钮506。

[0047] 图6是根据至少一个实施方案的用于创建和/或修改与由计算资源服务提供商提供的一个或多个服务相关的一个或多个策略的策略生成器602的说明性实例。如上结合图5所指出的，客户或委托管理用户可选择用户配置文件接口内的策略生成器按钮来访问策略生成器602。因此，一旦策略生成，使用策略生成器602限定的任何策略就可直接应用到相应用户配置文件。

[0048] 策略生成器602可包括可用于限定不同策略参数的多个部件。例如，策略生成器602可包括策略类型选择菜单604，所述策略类型选择菜单604用于选择客户或委托管理用户可选择来创建和实现的策略类型。因此，策略类型选择菜单604可包括可被选择的一个或多个不同策略类别。在此说明性实例中，策略类型选择菜单604已经被设定成计算资源服务提供商策略，所述计算资源服务提供商策略可用于指定用户是否能够访问由计算资源服务提供商提供的一个或多个服务。虽然出于说明的目的，计算资源服务提供商策略的用途贯穿本公开使用，但是策略类型选择菜单604可包括通知服务策略、排队服务策略、逻辑数据容器策略以及其他策略。

[0049] 至少部分地基于使用策略类型选择菜单604指定的策略类型，策略生成器602可生成不同输入选项以用于限定所选择特定类型的策略的参数或语句。例如，如图6所示，如果客户或委托管理用户从策略类型选择菜单604选择计算资源服务提供商策略，那么策略生成器602可呈现用于生成可应用于由计算资源服务提供商提供的一个或多个服务的策略语

句的多种选项。

[0050] 策略生成器602可允许客户或委托管理用户确定策略语句的效应。例如，策略生成器602可包括“允许”单选按钮606以及“拒绝”单选按钮608，所述按钮可使客户能够选择策略语句对用户在服务内权限的效应。例如，如果客户或委托管理用户选择“允许”单选按钮606，那么所生成的策略将使用户能够访问所指定的服务并且在服务内执行一个或多个动作。可替代地，如果客户或委托管理用户选择“拒绝”单选按钮608，那么所生成的策略可拒绝用户访问由计算资源服务提供商提供的一个或多个服务和/或拒绝在服务内执行一个或多个动作的用户权限。

[0051] 策略生成器602可另外包括服务选择菜单610，所述服务选择菜单610可使客户或委托管理用户能够指定哪个服务是策略语句的目标。例如，如图6所示，客户已经从服务选择菜单610选择数据库服务。虽然出于说明的目的，数据库服务的用途贯穿本公开使用，但是服务选择菜单610可包括多种其他服务，诸如基于对象的数据存储服务、虚拟计算机系统服务及其他服务。因此，策略生成器602可被配置来提供与所选择服务相关联的可用动作的列表，以便于客户或委托管理用户指定哪一个或多个动作有待被包括在策略语句中。此可用动作的列表可被编译成动作选择菜单612。

[0052] 因而，策略生成器602可包括动作选择菜单612，所述动作选择菜单612可使客户或委托管理用户能够指定特定用户或用户群可在所选择服务内采取或不采取(取决于选择“允许”单选按钮606或“拒绝”单选按钮608)的一个或多个动作。包括在动作选择菜单612内的动作列表可包括与所选择服务相关的多个API调用或命令，所述多个API调用或命令在传输到服务时可致使服务执行这些动作。动作选择菜单612中列举的每个动作可包括选择框，客户或委托管理用户可使用所述选择框来选择有待是策略语句的部分的一个或多个动作。可替代地，客户或委托管理用户可选择“所有动作”以便涵盖所有动作，而无需选择动作选择菜单612内的所有选择框。

[0053] 客户或委托管理用户可维持由计算资源服务提供商提供的每个服务内可经受不同访问和安全级别的一个或多个资源。因此，策略生成器602可包括资源名字字段614，客户或委托管理用户可使用所述资源名字字段614来选择所选择服务内的将经受策略语句的资源。例如，如图6所示，客户或委托管理用户已经选择数据库服务内的用户专用的资源，“JoeB-数据库”。因此，使用上述动作选择菜单612选择的任何动作将只应用到所选择服务内的这个资源。然而，如果客户或委托管理用户期望将所选择动作应用到服务内的多个资源，那么客户或委托管理用户可以能够使用多种通配符字符串来识别多个资源。例如，如果客户或委托管理用户选择将此策略语句应用到所选择服务内所有可用资源，那么客户或委托管理用户可使用资源名字字段614内的“*”指定所有资源。

[0054] 一旦客户或委托管理用户已经为相关策略语句指定所有参数(服务、动作以及资源)，那么客户或委托管理用户可选择添加可应用于其他服务或资源的另外策略语句。因而，策略生成器602可包括添加语句按钮616，所述添加语句按钮616可用于并入当前策略语句并且允许客户或委托管理用户生成另外策略语句。因而，针对此另外策略语句，客户或委托管理用户可再次选择“允许”单选按钮606或“拒绝”单选按钮608来限定新语句的效应；使用服务选择菜单610来选择策略语句的目标服务；使用动作选择菜单612来识别特定用户准许或拒绝的一个或多个动作，并且使用资源名字字段614来识别目标服务内将会是另外策

略语句的主题的目标资源。客户或委托管理用户可使用添加语句按钮616来进行添加，因为许多策略语句对限定特定用户策略来说是必要的。

[0055] 如果客户或委托管理用户已经完成生成限定特定用户策略的必要策略语句，那么客户或委托管理用户可选择生成策略按钮618。当客户或委托管理用户选择生成策略按钮618时，策略生成器602可继续根据由客户或委托管理用户提供的指定策略语句生成用户策略。随后，策略生成器602可将一个或多个可执行指令传输到管理式目录服务，所述一个或多个可执行指令当在由管理式目录服务执行时可致使所生成策略应用到特定用户配置文件并且还显示用户配置文件接口内的策略，如下将说明的。另外，策略生成器602可将一个或多个可执行指令传输到管理式目录服务内的策略管理子系统，所述一个或多个可执行指令在由策略管理子系统执行时可致使策略管理子系统使用户能够利用URI访问计算资源服务提供商接口。此接口可被配置来使用户能够仅利用由计算资源服务提供商提供的、用户已经在策略语句内识别为可准许使用的那些服务。可替代地，如果客户或委托管理用户并不期望生成用户策略，那么客户或委托管理用户相反可选择取消按钮620并且退出策略生成器602。

[0056] 如上所指出的，通过利用策略生成器生成新用户策略可致使新策略显示在用户配置文件接口中。因此，图7是根据至少一个实施方案的具有一个或多个新引入的用户策略的用户配置文件接口702的说明性实例。如上所指出的，用户策略接口702可包括多个部件，即，策略显示器704和策略生成器按钮706。策略显示器704可被配置来显示可应用于用户配置文件正被复审的特定用户的一个或多个策略。因此，一旦客户或委托管理用户已经利用策略生成器来创建并实现一个或多个新策略语句，这些新策略语句就可出现在策略显示器704上。

[0057] 例如，如果利用图6所示的输入创建策略，那么策略显示器内的新策略语句可包括这些输入。例如，如图7所示，新策略语句可包括由计算资源服务提供商提供的受影响服务(例如，数据库服务)、服务内的可应用资源(例如，JoeB-数据库)、策略效应(例如，允许)以及用户可在服务中所引用的资源内采取的动作(例如，“*”或所有动作)。

[0058] 除了这些策略语句之外，策略显示器704可显示受影响用户的服务标识值。此标识值可以是用户的临时标识名，所述临时标识名可用于访问在策略显示器704中显示的一个或多个服务。例如，在这个此说明性实例中，用户可分配有用于访问数据库服务的临时标识名。因而，当用户使用URI访问由计算资源服务提供商提供的一个或多个服务时，管理式目录服务通过策略管理子系统可访问此用户配置文件来获得用户的临时标识名。随后，策略管理子系统可将此信息传输给身份管理服务以便获得临时用户证书。因此，当用户通过由管理式目录服务提供的接口提交访问由计算资源服务提供商提供的一个或多个服务的请求时，管理式目录服务可使用这些临时证书来获得用户对这些服务的访问。

[0059] 如果客户或委托管理用户期望生成新策略语句或者对当前实现的策略做出改变，那么客户或委托管理用户可再次利用策略生成器按钮706来访问策略生成器并且做出期望改变。对用户策略做出的改变可因此根据需要出现在策略显示器704中。应注意，在图7的说明性实例中，策略显示器704包括使用策略生成器生成的新策略语句以及图5引入的策略语句。虽然出于说明的目的，通过使用策略生成器添加策略语句贯穿本公开使用，但是应注意，策略生成器还可用于重写或擦除可应用于用户的任何现有策略。

[0060] 如上所指出的，客户可将一个或多个请求提交给管理式目录服务以便对可用于促进在一个或多个用户之间的数据共享和/或可用性的目录进行配置。这可包括建立可被委托访问目录以及由计算资源服务提供商的一个或多个其他服务的一个或多个用户的一个或多个请求。因此，图8是根据至少一个实施方案的用于限定用户访问一个或多个计算资源服务的过程800的说明性实例。过程800可由客户或具有通过策略管理子系统管理所述管理式目录服务中的目录的授权的其他委托管理用户执行。

[0061] 如上所指出的，客户可以是可使用目录支持其业务需求的组织。因此，客户可要求一个或多个其他用户访问目录以便访问支持业务任务所必需的信息。因而，客户或其他委托管理用户可接收802在管理式目录服务内创建新用户配置文件使得用户可访问目录的请求。请求可起源于客户组织的期望获得对目录的访问以便执行一个或多个任务的一个或多个雇员。请求还可起源于客户组织外部的可以是客户组织的客户的实体。

[0062] 由于所接收请求可起源于无数的源，客户或委托管理用户可能需要确定804所接收请求是否有效。例如，客户或委托管理用户可评估确定请求是否起源于组织内的雇员账户以及是否应同意所述雇员访问目录的请求。或者，如果请求起源于外部实体，那么客户或委托管理用户可评估是否应准许实体访问目录或者实体是否不必具有必要的授权。因此，如果创建新用户的请求无效，那么客户或委托管理用户可拒绝806请求。

[0063] 如果在管理式目录服务内创建新用户账户的请求有效，那么客户或委托管理用户可在服务内生成808新用户账户。例如，客户或委托管理用户可为新用户创建新用户配置文件，并且将任何用户细节并入到配置文件中以便提高用户对服务的访问。另外，客户或委托管理用户可利用管理式目录服务来为用户生成一组证书，用户可使用所述一组证书访问管理式目录服务。如下将更详细描述的，用户可使用此组证书来另外访问由计算资源服务提供商提供的一个或多个服务，从而排除对另外组的证书的需求。

[0064] 一旦管理式目录服务内的用户账户已经创建，客户或委托管理用户就可访问用户配置文件来限定810用于访问由计算资源服务提供商提供的一个或多个服务的一个或多个策略。如上结合图5和图7指出的，用户配置文件接口可包括当前实现的所有策略的列表以及可用于访问策略生成器的策略生成器按钮。通过使用策略生成器，客户或委托管理用户可限定一个或多个策略语句。每个策略语句可被配置来限定用户是否能够访问由计算资源服务提供商提供的一个或多个服务，以及用户可在这些服务内利用的动作和资源。可替代地，客户或委托管理用户可利用策略生成器来限定对用户访问这些一个或多个服务的某些限制。一旦客户或委托管理用户已经限定有待实施的策略，策略就可出现在用户配置文件接口内并且可基于客户的要求在任何时候进行修改。

[0065] 如上所指出的，在客户或委托管理用户已经完成在策略生成器内生成一个或多个策略语句之后，策略生成器可将一个或多个可执行指令传输到策略管理子系统，所述一个或多个可执行指令在由策略管理子系统执行时致使策略管理子系统并入新生成的用户策略。除了并入这些策略之外，策略管理子系统可另外使用户能够利用URI访问计算资源服务提供商接口以便访问由计算资源服务提供商提供的一个或多个服务。因此，客户或委托管理用户可将URI递送给用户以便于用户访问由计算资源服务提供商提供的服务。

[0066] 一旦用户已经从客户或委托管理用户接收URI，用户就可现在开始提交访问由计算资源服务提供商提供的一个或多个服务的一个或多个请求。因此，图9是根据至少一个实

施方案的用于使用户能够访问一个或多个计算资源服务的过程900的说明性实例。过程900可由管理式目录服务的策略管理子系统执行。策略管理子系统可被配置来访问管理式目录服务的一个或多个其他部件，即，提交一个或多个请求的用户的用户配置文件，并且另外与计算资源服务提供商通信以便建立用户对一个或多个服务的访问。

[0067] 当用户使用URI访问计算资源服务提供商接口以便进一步访问由计算资源服务提供商提供的一个或多个服务时，策略管理子系统可检测到用户已经利用URI并且可开始核实用户请求以便确保已经同意用户访问这些服务。因此，策略管理子系统可从用户接收902访问由计算资源服务提供商提供的一个或多个服务的请求。如上所指出的，URI可用于访问接口。由于通过URI访问接口可被提供给多种客户和/或委托管理用户，许多用户可能够访问URI。例如，如果URI被提供给特定用户但是用户将URI提供给没有访问这些服务的授权的其他实体，那么这些其他实体可试图访问这些服务而不管他们的授权级别。

[0068] 因此，策略管理子系统可被配置来确定904提交通过利用URI访问接口来访问一个或多个服务的请求的用户的身份。例如，为了利用URI，每个用户可能需要提供一组证书来访问管理式目录服务，并且从服务内利用URI来访问接口。因此，策略管理子系统可以能够通过此组证书识别提交请求的用户。

[0069] 一旦策略管理子系统已经确定提交请求的用户的身份，策略管理子系统就可确定906这名特定用户是否是有效用户并且因此是否已经被同意访问所请求的一个或多个服务。如上所指出的，如果用户将URI提供给一个或多个其他用户，那么这些其他用户可使用URI来试图访问这些服务。然而，由于管理式目录服务的每个用户需要提供一组证书来访问管理式目录服务并且利用URI，策略管理子系统可以能够确定904利用URI的用户的身份。如果用户并未被同意访问由计算资源服务提供商提供的任何服务，那么未授权用户可能不是有效用户，并且策略管理子系统可拒绝908访问这些一个或多个服务。另外，如果用户已经具有在使用户能够利用URI访问计算资源服务提供商之后取消的他/她对这些一个或多个服务的访问，那么策略管理子系统可评估用户配置文件并因此拒绝908访问这些服务。

[0070] 如果策略管理子系统评估用户的一组证书并且确定用户并不能够适当访问由计算资源服务提供商提供的一个或多个服务，那么策略管理子系统可访问用户配置文件以便识别910可应用于用户的一个或多个策略。如上所指出的，客户或委托管理用户可通过用户配置文件访问策略生成器以便通过用户的配置文件限定应用到用户的一个或多个策略语句。这些策略语句可用于限定用户对由计算资源服务提供商提供的一个或多个服务的访问的参数。在策略语句已经生成之后，策略可出现在用户配置文件内。因而，策略管理子系统可访问用户配置文件并且提取用户已经请求访问的一个或多个服务的可应用策略。

[0071] 一旦策略管理子系统已经从用户配置文件获得可应用策略，策略管理子系统就可将这些策略传输912到由计算资源服务提供商提供和管理的身份管理服务以便处理。身份管理服务可被配置来应用包括在用户配置文件内的策略，使得当用户访问这些一个或多个服务时，用户可根据由客户或委托管理用户建立的策略仅在服务内执行动作。另外，策略管理子系统可将一个或多个请求传输到身份管理服务以便获得914一组或多组临时证书，所述一组或多组临时证书可用于访问由计算资源服务提供商提供的一个或多个服务。因而，当用户利用接口访问一个或多个服务时，策略管理子系统可访问这些组的临时证书并且将它们传输到由计算资源服务提供商提供的适当服务以便建立用户对服务的访问。应注意，

这些组的临时证书在一组证书在特定事件发生之后不可由用户访问的意义上可以是临时的。例如，当用户终止与由计算资源服务提供商提供的服务的会话(例如，通过关闭浏览器应用)时，证书可因此变得不可由用户访问，尽管证书尚未到期。在此类实例中，为了开始新的会话，管理式目录服务可能需要获得新组的临时证书来使用户能够访问服务。

[0072] 一旦策略管理子系统已经获得访问由计算资源服务提供商提供的一个或多个服务所必要的一组临时证书，策略管理子系统就可利用可应用于用户的策略来根据可应用的用户策略生成916一个或多个重定向URI以便访问这些服务。一个或多个重定向URI可由用户使用来访问根据用户配置文件中提供的策略已经同意用户防问的一个或多个服务的接口以及用户可用的任何资源和动作。

[0073] 用户可针对每个服务使用重定向URI来执行可准许在针对一个或多个服务内的用户限定的策略下进行的一个或多个动作。因此，策略管理子系统可被配置来将用户请求连同所述一组临时证书传输到计算资源服务提供商管理子系统以便根据针对用户提出的策略使918用户能够访问一个或多个服务。因而，用户现在可访问一个或多个服务并且执行与客户或委托管理用户要求一致的各种任务。

[0074] 图10示出根据各个实施方案的用于实现方面的示例性环境1000的方面。如将理解的，尽管出于解释的目的使用基于网络的环境，但是可视情况使用不同环境来实现各个实施方案。环境包括电子客户端装置1002，所述电子客户端装置1002可包括可操作来通过适当网络1004发送和/或接收请求、消息或信息并且在一些实施方案中将信息传送回装置的用户的任何适当装置。此类客户端装置的实例包括：个人计算机、手机、手持通信装置、膝上型计算机、平板计算机、机顶盒、个人数据助理、嵌入式计算机系统、电子书阅读器等。网络可包括任何适当网络，所述适当网络包括内部网络、互联网、蜂窝网、局域网、卫星网络，或任何其他此类网络或上述网络的组合。此类系统所用的部件可至少部分地取决于所选网络和/或环境的类型。用于通过这样的网络通信的协议和部件是众所周知的并且本文将不再详细论述。网络上的通信可通过有线或无线连接及其组合来实现。在这个实例中，网络包括互联网，因为环境包括用于接收请求并且响应于所述请求而提供内容的网络服务器1006，然而对于其他网络来说，可使用服务类似目的的替代装置，如本领域普通技术人员所显而易见的。

[0075] 说明性环境包括至少一个应用服务器1008和数据存储库1010。应理解，可存在可链接起来或以其他方式来配置的若干应用服务器、层或其他元件、过程或部件，这些应用服务器、层或其他元件、过程或部件可交互来执行诸如从适当数据存储库获得数据的任务。本文所使用的服务器可以各种方式来实现，诸如硬件装置或虚拟计算机系统。在一些上下文中，服务器可指代在计算机系统上执行的程序设计模块。如本文所使用的，除非从上下文另外声明或清楚，术语“数据存储库”指代能够存储、防问和检索数据的任何装置或装置组合，所述装置可包括在任何标准、分布、虚拟或集群环境中的数据服务器、数据库、数据存储装置和数据存储介质的任何组合和任何数目。应用服务器可包括任何适当硬件、软件和固件，所述硬件、软件和固件视执行客户端装置的一个或多个应用的方面的需要与数据存储库集成且处置应用的一些或全部数据访问和业务逻辑。应用服务器可提供与数据存储库协作的访问控制服务，并且能够生成可被使用来提供给用户的内容，诸如但不限于文本、图片、音频、视频和/或其他文本，所述内容可以超文本标记语言(“HTML”)、可扩展标记语言

(“XML”)、JavaScript、层叠样式表(“CSS”)或另一种适当客户端结构化语言的形式由网络服务器向用户提供。传送到客户端装置的内容可由客户端装置处理以便提供以下一个或多个形式的内容,包括但不限于:用户可听、可视和/或通过其他感官(包括触觉、味觉和/或嗅觉)的形式。所有请求和响应的处置以及客户端装置1002与应用服务器1008之间的内容递送可由网络服务器使用以下PHP来处置:在这个实例中为超文本预处理器(“PHP”)、Python、Ruby、Perl、Java、HTML、XML或另一种适当服务器端结构化语言。应理解,网络服务器和应用服务器不是必要的,且仅仅是示例性部件,因为本文所论述的结构化代码可在如本文其他地方所讨论的任何适当装置或主机上执行。此外,本文描述为由单个装置执行的操作可以(除非上下文另有规定)由可形成分布式和/或虚拟系统的多个装置共同执行。

[0076] 数据存储库1010可包括若干单独数据表、数据库、数据文件、动态数据存储方案和/或其他数据存储机构和介质以用于存储与本公开的特定方面相关的数据。例如,所示数据存储库可包括用于存储生成数据1012和用户信息1016的机构,所述生成数据和用户信息可用于提供用于生成端的内容。数据存储库还被示出为包括用于存储日志数据1014的机构,所述机构可用于报告、分析或其他此类目的。应理解,可能存在可需要被存储在数据存储库中的许多其他方面,诸如页面图像信息和访问权信息,所述方面可视情况存储在上文列出的机构中的任何机构中或存储在数据存储库1010中的另外机构中。数据存储库1010可通过与其相关联的逻辑来操作,以便从应用服务器1008接收指令,并且响应于所述指令获得数据、更新数据或以其他方式处理数据。应用服务器1008可响应于所接收指令提供静态、动态数据或静态和动态数据的组合。诸如网页日志(博客)、购物应用、新闻服务以及其他此类应用中使用的数据的动态数据可由如本文所描述的服务器端结构化语言生成或者可由在应用服务器上操作或在其控制下的内容管理系统(“CMS”)提供。在一个实例中,用户通过由用户操作的装置可提交针对某种类型的项目的搜索请求。在这种情况下,数据存储库可能访问用户信息以便核实用户的身份,并且可访问目录详细信息以便获得有关所述类型的项目的信息。接着可将信息如以网页上的结果列表的形式返回给用户,用户能够通过用户装置1002上的浏览器来查看所述网页。可在专用浏览器页面或窗口中查看感兴趣的特定项目的信息。然而,应注意,本公开的实施方案未必局限于网页的上下文,而可更一般地应用于处理一般请求,其中请求未必是上下文的请求。

[0077] 每个服务器通常将包括提供用于所述服务器的一般管理和操作的可执行程序指令的操作系统,并且通常将包括存储指令的计算机可读存储介质(例如,硬盘、随机存取存储器、只读存储器等),所述指令在由服务器的处理器执行时允许所述服务器执行其预期的功能。操作系统的合适的实现方式和服务器的一般功能是众所周知的或可商购的,并且易于由本领域普通技术人员实现,尤其是鉴于本文中的公开来实现。

[0078] 在一个实施方案中,环境是分布式和/或虚拟计算环境,所述环境利用通过通信链路、使用一个或多个计算机网络或直接连接来互连的若干计算机系统和部件。然而,本领域普通技术人员应理解,这种系统可在具有比图10所示的部件更少或更多个部件的系统中同样顺利地操作。因而,图10中的系统1000的描绘本质上应视为说明性的,并且不限制本公开的范围。

[0079] 可在广泛多种操作环境中进一步实现各个实施方案,所述操作环境在一些情况下可包括一个或多个用户计算机、计算装置或者可用于操作多个应用中的任何一个的处理装

置。用户或客户端装置可包括多个通用个人计算机中的任何一个，诸如运行标准操作系统的台式计算机、膝上型计算机或平板计算机，以及运行移动软件并且能够支持许多网络连接协议和消息传递协议的蜂窝装置、无线装置和手持装置。这种系统还可包括许多工作站，所述工作站运行多种可商购得的操作系统和用于诸如开发和数据库管理目的的其他已知应用中的任一个。这些装置还可包括其他电子装置，诸如虚拟终端、薄型客户端、游戏系统以及能够通过网络通信的其他装置。这些装置还可包括虚拟装置，诸如虚拟机、管理程序以及能够通过网络通信的其他虚拟装置。

[0080] 本公开的各个实施方案利用本领域技术人员可能熟悉的至少一种网络来使用多种可商购得的协议中的任一种支持通信，所述协议诸如传输控制协议/互联网协议(“TCP/IP”)、用户数据报协议(“UDP”)、在开放系统互连(“OSI”)模型的各个层中操作的协议、文件传送协议(“FTP”)、通用即插即用(“UpnP”)、网络文件系统(“NFS”)、公共互联网文件系统(“CIFS”)以及AppleTalk。网络例如可以是局域网、广域网、虚拟专用网、互联网、内部网、外部网、公共交换电话网、红外网、无线网、卫星网络以及上述网络的任何组合。

[0081] 在利用网络服务器的实施方案中，网络服务器可运行多种服务器或中间层级应用中的任何一个，所述服务器包括超文本传送协议(“HTTP”)服务器、FTP服务器、通用网关接口(“CGI”)服务器、数据服务器、Java服务器、Apache服务器以及业务应用服务器。所述服务器还可以能够响应于来自用户装置的请求而执行程序或脚本，诸如通过执行一个或多个可实现为一个或多个以任何编程语言(诸如Java®、C、C#或C++)或任何脚本语言(诸如Ruby、PHP、Perl、Python或TCL)及其组合撰写的脚本或程序的网络应用程序。所述服务器还可包括数据库服务器，包括但不限于可从Oracle®、Microsoft®、Sybase®和IBM®商购得的服务器以及开源服务器(诸如MySQL、Postgres、SQLite、MongoDB)，以及能够存储、检索和访问结构化或非结构化数据的任何其他服务器。数据库服务器可包括基于表格的服务器、基于文档的服务器、非结构化服务器、关系型服务器、非关系型服务器，或者这些和/或其他数据库服务器的组合。

[0082] 环境可包括如上文所论述的多种数据存储库以及其他存储器和存储介质。这些可驻留在多种位置，诸如在一个或多个计算机本地(和/或驻留在一个或多个计算机中)的存储介质上，或远离网络上的计算机中的任何一个或所有计算机。在特定组的实施方案中，信息可驻留于在本领域技术人员熟悉的存储区域网(“SAN”)中。类似地，用于执行属于计算机、服务器或其他网络装置的功能的任何必要文件可视情况本地和/或远程存储。在系统包括计算机化装置的情况下，每个这种装置可包括可通过总线电耦合的硬件元件，所述元件例如包括至少一个中央处理单元(“CPU”或“处理器”)、至少一个输入装置(例如，鼠标、键盘、控制器、触摸屏或小键盘)以及至少一个输出装置(例如，显示设备、打印机或扬声器)。这种系统还可包括一个或多个存储装置，诸如硬盘驱动器、光存储装置以及固态存储装置(诸如随机存取存储装置器(“RAM”)或只读存储器(“ROM”))，以及可移动媒体装置、存储器卡、闪存卡等。

[0083] 此类装置还可包括计算机可读存储介质读取器、通信装置(例如调制解调器、网络卡(无线或有线)、红外线通信装置等)以及工作存储器，如上文所描述的。计算机可读存储介质读取器可与计算机可读存储介质连接或者被配置来接收计算机可读存储介质，所述计算机可读存储介质表示远程、本地、固定和/或可移动存储装置以及用于暂时和/或更永久

地含有、存储、传输和检索计算机可读信息的存储介质。系统和各种装置通常还将包括位于至少一个工作存储器装置内的多个软件应用、模块、服务或其他元件，包括操作系统和应用程序，诸如客户端应用或网络浏览器。应当了解，替代实施方案可具有与上述实施方案不同的众多变形。例如，还可使用定制硬件，和/或特定元件可以在硬件、软件(包括可移植软件，诸如小程序)或两者中实现。此外，可采用与诸如网络输入/输出装置的其他计算装置的连接。

[0084] 含有代码或部分代码的存储介质和计算机可读介质可包括本领域已知或已使用的任何适当介质，包括存储介质和通信介质，诸如但不限于用于存储和/或传输信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中所实现的易失性和非易失性、可移动和不可移动介质，包括RAM、ROM、电可擦除可编程只读存储器(“EEPROM”)、快闪存储器或其他存储器技术、紧密光盘只读存储器(“CD-ROM”)、数字通用光盘(DVD)或其他光学存储器、磁盒、磁带、磁盘存储器或其他磁性存储装置，或可用于存储所要信息且可供系统装置访问的任何其他介质。基于本文所提供的公开和教义，本技术领域普通技术人员将理解实现各个实施方案的其他方式和/或方法。

[0085] 本公开的实施方案可鉴于以下条款来描述：

[0086] 1.一种用于使能够访问由计算资源服务提供商提供的一个或多个计算系统服务的计算机实现的方法，其包括：

[0087] 在配置有可执行指令的一个或多个计算机系统的控制下，

[0088] 使用户能够利用一组证书访问管理式目录服务内的目录中的资源；

[0089] 在所述管理式目录服务处从所述用户接收访问由所述计算资源服务提供商提供的所述一个或多个计算系统服务的不同于所述管理式目录服务的子集的第一请求，所述第一请求包括至少部分地基于所述一组证书的信息；

[0090] 在所述管理式目录服务处至少部分地基于所述一组证书认证所述用户；

[0091] 在已经认证所述用户的第一条件下，在所述管理式目录服务处识别可应用于所述用户的一个或多个策略，所述一个或多个策略至少部分地基于所述第一请求至少限定对所述一个或多个服务的访问级别；

[0092] 在所识别的一个或多个策略允许访问的第二条件下，向身份管理服务传输一组一个或多个临时证书的第二请求，其中所述临时证书使所述用户能够访问所述一个或多个服务的子集；

[0093] 从所述身份管理服务接收所述一组一个或多个临时证书；以及

[0094] 利用所接收的一组一个或多个临时证书来至少部分地实现来自所述用户的访问所述一个或多个服务的所述第一请求。

[0095] 2.如条款1所述的计算机实现的方法，其中所述一个或多个策略由所述管理式目录服务内的所述目录的管理用户使用策略生成器接口限定，所述策略生成器接口使所述管理用户能够至少部分地基于所述一个或多个服务限定所述一个或多个策略。

[0096] 3.如条款1至2所述的计算机实现的方法，其还包括使所述用户能够从所述管理式目录服务访问可用于访问所述一个或多个服务的接口，以便至少部分地实现来自所述用户的访问所述一个或多个服务的所述第一请求。

[0097] 4.如条款3所述的计算机实现的方法，其中使所述用户能够访问所述接口包括向

所述用户提供用于访问所述接口的网络位置的参考,所述参考在限定至少限定对所述一个或多个服务的访问级别的所述一个或多个策略时可用。

[0098] 5.如条款3至4所述的计算机实现的方法,其中所述接口进一步被配置来使能够将来自所述用户的访问所述一个或多个服务的请求传输到所述身份管理服务。

[0099] 6.如条款1至5所述的计算机实现的方法,其中可应用于所述用户的所述一个或多个策略被限定在所述管理式目录服务处的配置文件中,所述配置文件特定于所述用户。

[0100] 7.一种计算机系统,其包括:

[0101] 一个或多个处理器;以及

[0102] 存储器,其具有共同存储在其中的指令,所述指令在由所述计算机系统执行时致使所述计算机系统来:

[0103] 在目录服务处认证利用证书信息访问所述目录服务内的目录的请求者;

[0104] 从所述请求者接收访问由计算资源服务提供商提供的一个或多个服务的子集的请求,对所述一个或多个服务的所述子集的访问由所述目录服务内的所述目录管理;

[0105] 由于认证所述请求者,从不同于所述目录服务的第二服务获得临时证书信息以访问所述一个或多个服务的所述子集;并且

[0106] 利用从所述第二服务获得的所述临时证书信息来至少部分地实现访问所述一个或多个服务的所述子集的所述请求。

[0107] 8.如条款7所述的计算机系统,其中所述请求包括至少部分地基于所述证书信息的信息。

[0108] 9.如条款7至8所述的计算机系统,其中用于认证所述请求者的所述指令包括用于识别可应用于所述请求者的一个或多个策略的指令,所述一个或多个策略至少限定对所述一个或多个资源的所述子集的访问级别。

[0109] 10.如条款7至9所述的计算机系统,其中所述指令进一步致使所述计算机系统使所述请求者能够从所述目录服务访问可至少部分地基于对所述请求者的所述认证访问的接口,以便至少部分地实现访问所述一个或多个服务的所述子集的所述请求。

[0110] 11.如条款10所述的计算机系统,其中所述指令进一步致使所述计算机系统提供所述接口的网络地址的表示,所述接口可由所述请求者用来提交访问所述一个或多个服务的所述子集的所述请求。

[0111] 12.如条款7至11所述的计算机系统,其中致使所述计算机系统获得所述临时证书信息的所述指令进一步致使所述计算机系统与所述第二服务通信,以便请求所述临时证书信息并且从所述第二服务接收所述临时证书信息。

[0112] 13.如条款7至12所述的计算机系统,其中所述临时证书信息被配置成由于所述请求者终止其对所述一个或多个服务的所述子集的访问而变得不可由所述请求者使用。

[0113] 14.一种非暂态计算机可读存储介质,其具有共同存储在其上的可执行指令,所述指令在由计算机系统的一个或多个处理器执行时致使所述计算机系统至少:

[0114] 在目录服务处核实利用证书信息访问所述目录服务内的目录的请求者被授权访问所述目录;

[0115] 从所述请求者接收访问由计算资源服务提供商提供的一个或多个服务的子集的请求;

[0116] 由于在所述目录服务处核实所述请求者被授权访问所述目录，识别可应用于所述请求者的一个或多个策略，所述一个或多个策略由所述目录服务内的所述目录管理并且可用于限定对所述一个或多个服务的所述子集的访问级别；

[0117] 在所识别的一个或多个策略允许访问的条件下，从不同于所述目录服务的第二服务获得临时证书信息以访问所述一个或多个服务的所述子集；并且

[0118] 利用从所述第二服务获得的所述临时证书信息来至少部分地实现访问所述一个或多个服务的所述子集的所述请求。

[0119] 15.如条款14所述的非暂态计算机可读存储介质，其中所述请求包括至少部分地基于所述证书信息的信息。

[0120] 16.如条款14至15所述的非暂态计算机可读存储介质，其中所述可执行指令进一步致使所述计算机系统使所述请求者能够从所述目录服务访问可至少部分地基于对所述请求者的所述核实访问的接口，以便至少部分地实现访问所述一个或多个服务的所述子集的所述请求。

[0121] 17.如条款16所述的非暂态计算机可读存储介质，其中所述指令进一步致使所述计算机系统提供所述接口的网络地址的表示，所述接口可由所述请求者用来提交访问所述一个或多个服务的所述子集的所述请求。

[0122] 18.如条款14至17所述的非暂态计算机可读存储介质，其中可应用于所述请求者的所述一个或多个策略被限定在存储于所述目录内的配置文件中，所述配置文件特定于所述请求者。

[0123] 19.如条款14至18所述的非暂态计算机可读存储介质，其中所述临时证书信息被配置成由于所述请求者终止其对所述一个或多个服务的所述子集的访问而变得对所述请求者不可用。

[0124] 20.如条款14至19所述的非暂态计算机可读存储介质，其中致使所述计算机系统获得所述临时证书信息的所述指令进一步致使所述计算机系统与所述第二服务通信，以便请求所述临时证书信息并且从所述第二服务接收所述临时证书信息。

[0125] 因此，应在说明性意义而不是限制性意义上理解本说明书和附图。然而，将显而易见的是：在不脱离如在权利要求书中阐述的本发明的更宽广精神和范围的情况下，可以对其做出各种修改和改变。

[0126] 其他变型也在本公开的精神内。因此，虽然所公开的技术易受各种修改和替代构造的影响，但在附图中示出且在上文详细描述其特定说明的实施方案。然而，应理解，并不意图将本发明限于具体形式或所公开的形式，但相反，意图涵盖属于本发明的精神和范围内的所有修改、替代构造和等效物，如随附权利要求书中所限定。

[0127] 在描述所公开实施方案的上下文中(尤其是在随附权利要求的上下文中)，术语“一个(a，an)”和“所述(the)”以及类似的提及的使用意图解释为涵盖单数和复数两者，除非在本文另外地指示或明显地与上下文矛盾。术语“包含”、“具有”、“包括”和“含有”应解释为开放式术语(即，意味着“包括但不限于”)，除非另外地注解。当未修改并且指代物理连接时，术语“连接的”应解释为部分地或全部地纳入在以下解释内：附接至或连接在一起，即使存在介入物。除非在此另有说明，否则本文各值的范围的叙述仅意欲用作单独指代属于该范围内的各独立值的速记方法，并且各独立值如同其在本文单独叙述一般结合到本说明书

中。除非以其他方式指出或与上下文矛盾，术语“集”或“子集”的使用(例如，“项目集”)应解释为包括一个或多个构件的非空集合。此外，除非以其他方式指出或与上下文矛盾，术语相应集的“子集”未必表示相应集的真子集，但子集和相应集可以相等。

[0128] 除非以其他方式确切地陈述或以其他方式与上下文明显地矛盾，连接语言如“A、B、和C中的至少一个”或“A、B和C中的至少一个”形式的短语以如通常使用的上下文来另外理解，以呈现项目、术语等可以是A或B或C，或A和B和C的集合的任何非空子集。例如，在具有三个成员的集的说明性实例中，连接短语“A、B和C中的至少一个”和“A、B和C中的至少一个”指代以下集中的任一集：{A}、{B}、{C}、{A、B}、{A、C}、{B、C}、{A、B、C}。因此，此类连接性语言一般并非意在暗示某些实施方案需要对于各自来说存在A中的至少一个、B中的至少一个以及C中的至少一个。

[0129] 可按任何合适的顺序来执行本文所述的过程的操作，除非本文另外指明或另外明显地与上下文矛盾。本文描述的过程(或变型和/或其组合)可以在配置有可执行指令的一个或多个计算机系统的控制下执行，并且可以作为共同地在一个或多个处理器上执行的代码(例如，可执行指令、一个或多个计算机程序或一个或多个应用)、由硬件或其组合来实现。所述代码可例如以包括可由一个或多个处理器执行的多个指令的计算机程序的形式而存储在计算机可读存储介质上。计算机可读存储介质可以是非暂态的。

[0130] 本文所提供的任何以及所有实例或示例性语言(例如，“诸如”)的使用仅意图更好地说明本发明的实施方案，并且除非另外要求，否则不会对本发明的范围施加限制。说明书中的语言不应解释为表明任何未要求保护的要素对实施本发明必不可少。

[0131] 本文中描述了本发明的优选实施方案，其包括为发明者所知用来执行本发明的最佳模式。阅读上述说明后那些优选的实施方案的变型对于本领域的普通技术人员可以变得显而易见。发明人希望技术人员视情况采用此类变型，并且发明人意图以不同于如本文所具体描述的方式来实践本公开的实施方案。因此，经适用的法律许可，本公开的范围包括在此附加的权利要求中叙述的主题的所有改良形式和等价物。此外，除非本文另外指示或另外明显地与上下文矛盾，否则本公开的范围涵盖其所有可能变型中的上述元素的任何组合。

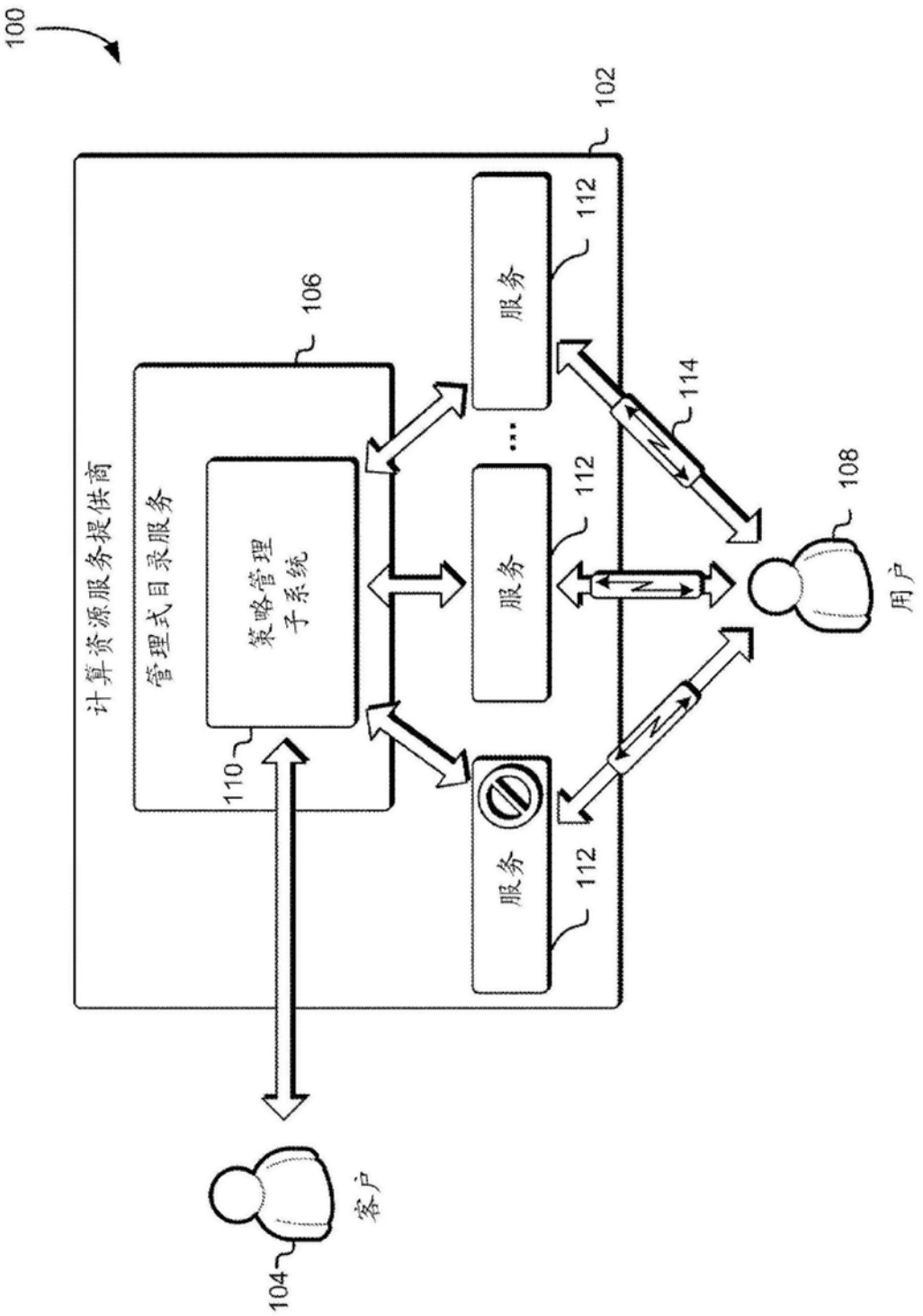

100
102
计算资源服务提供商
管理式目录服务
106
策略管理
子系统
110
服务
112
服务
112
服务
112
114
108
用户
客户
104

图1

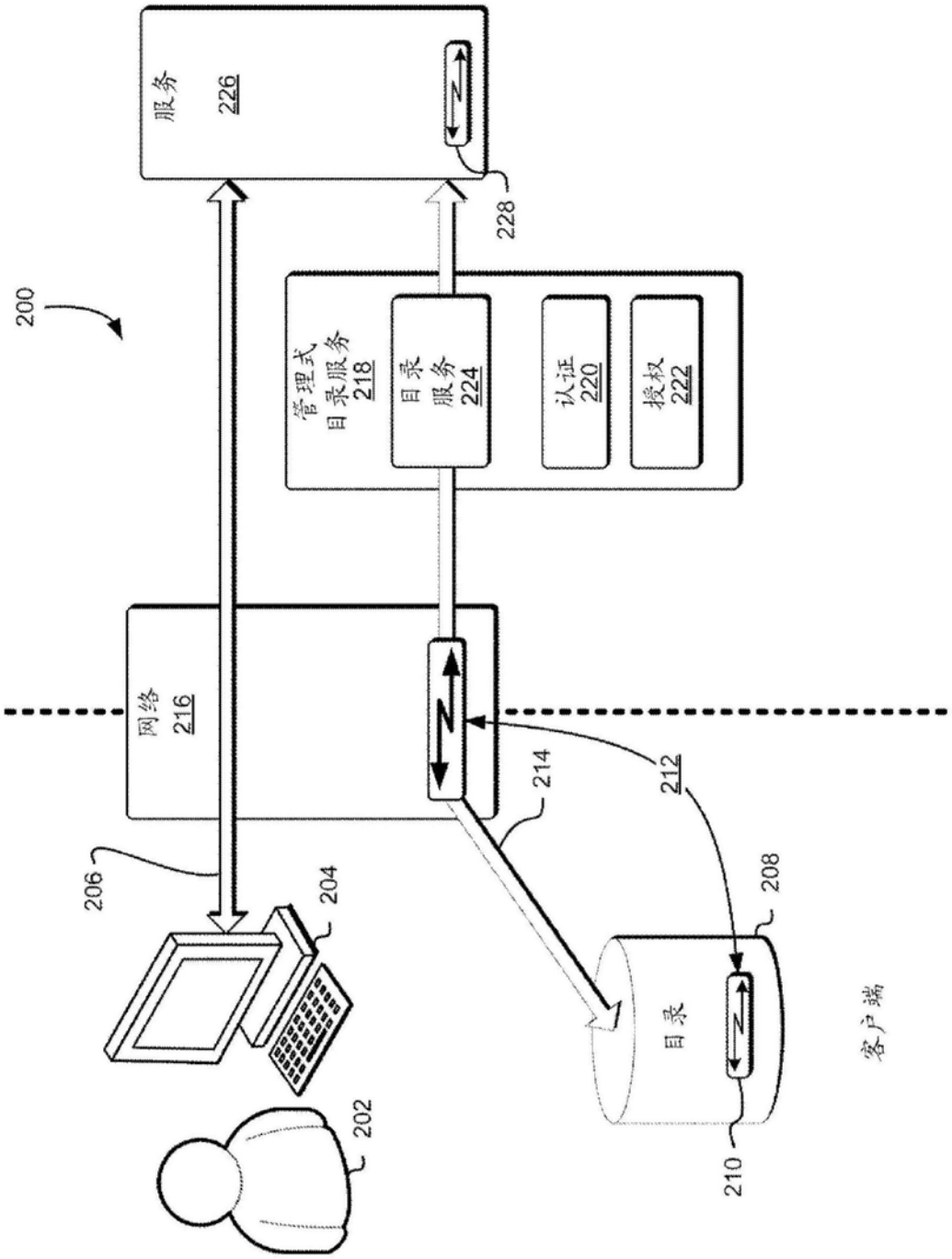

服务
226
228
200
管理式
目录服务
218
目录
服务
224
认证
220
授权
222
网络
216
214
212
206
204
208
目录
客户端
202
210

图2

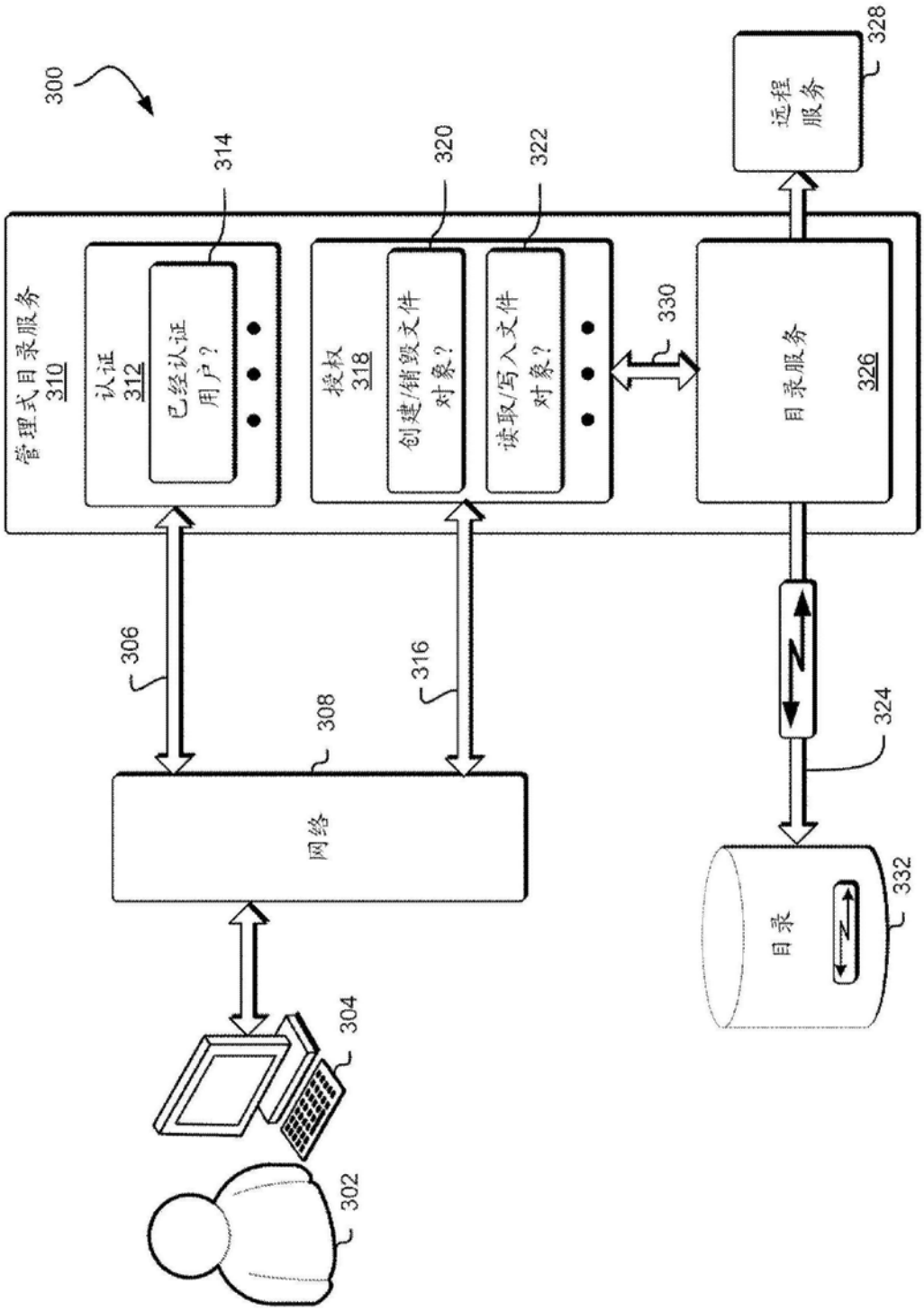

300
远程服务
328
314
320
322
管理式目录服务
310
认证
312
已经认证用户?
授权
318
创建/销毁文件对象?
读取/写入文件对象?
330
目录服务
326
306
316
308
324
网络
目录
332
304
302

图3

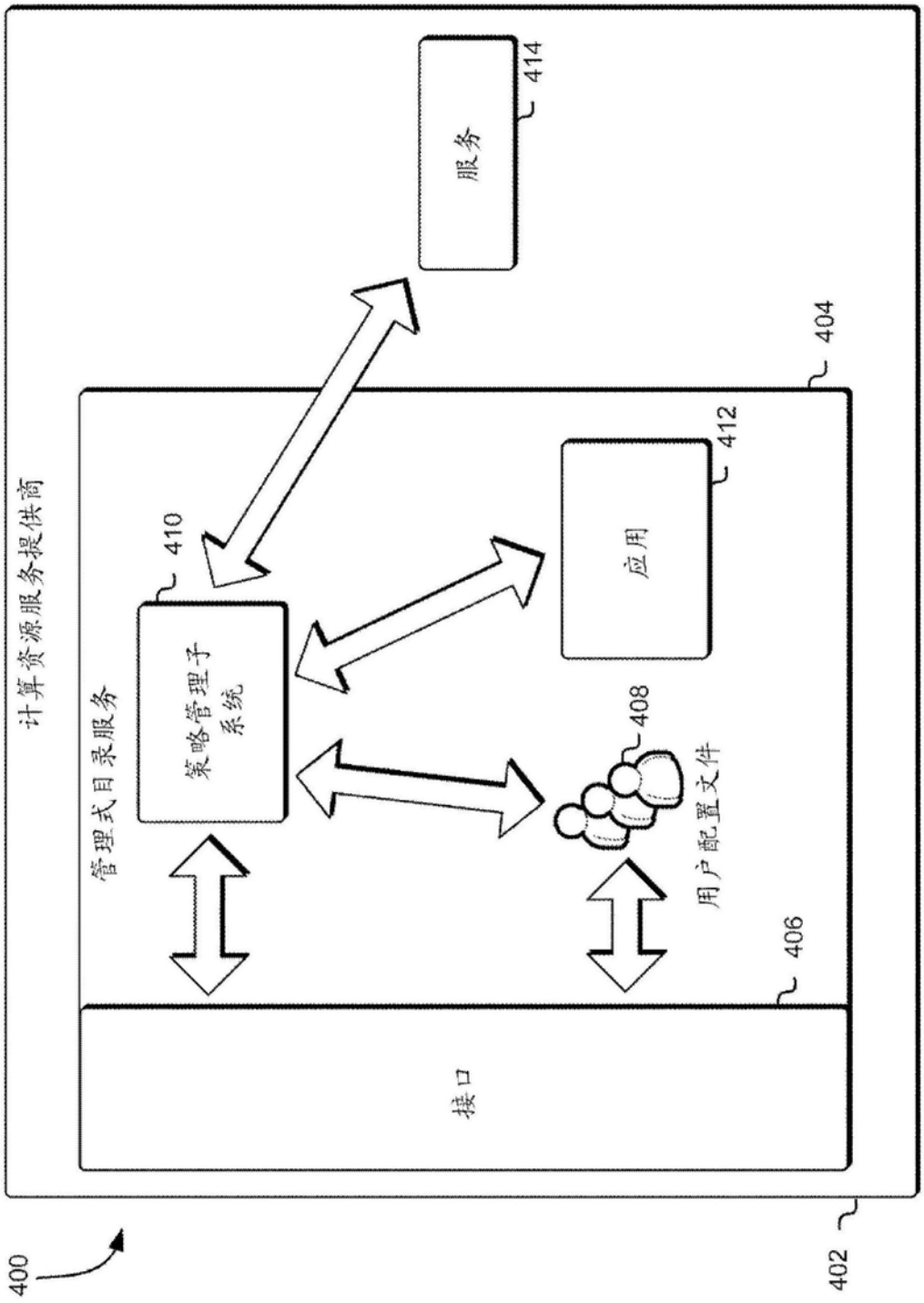

400
计算资源服务提供商
402
管理式目录服务
404
接口
406
策略管理子系统
410
用户配置文件
408
应用
412
服务
414

图4

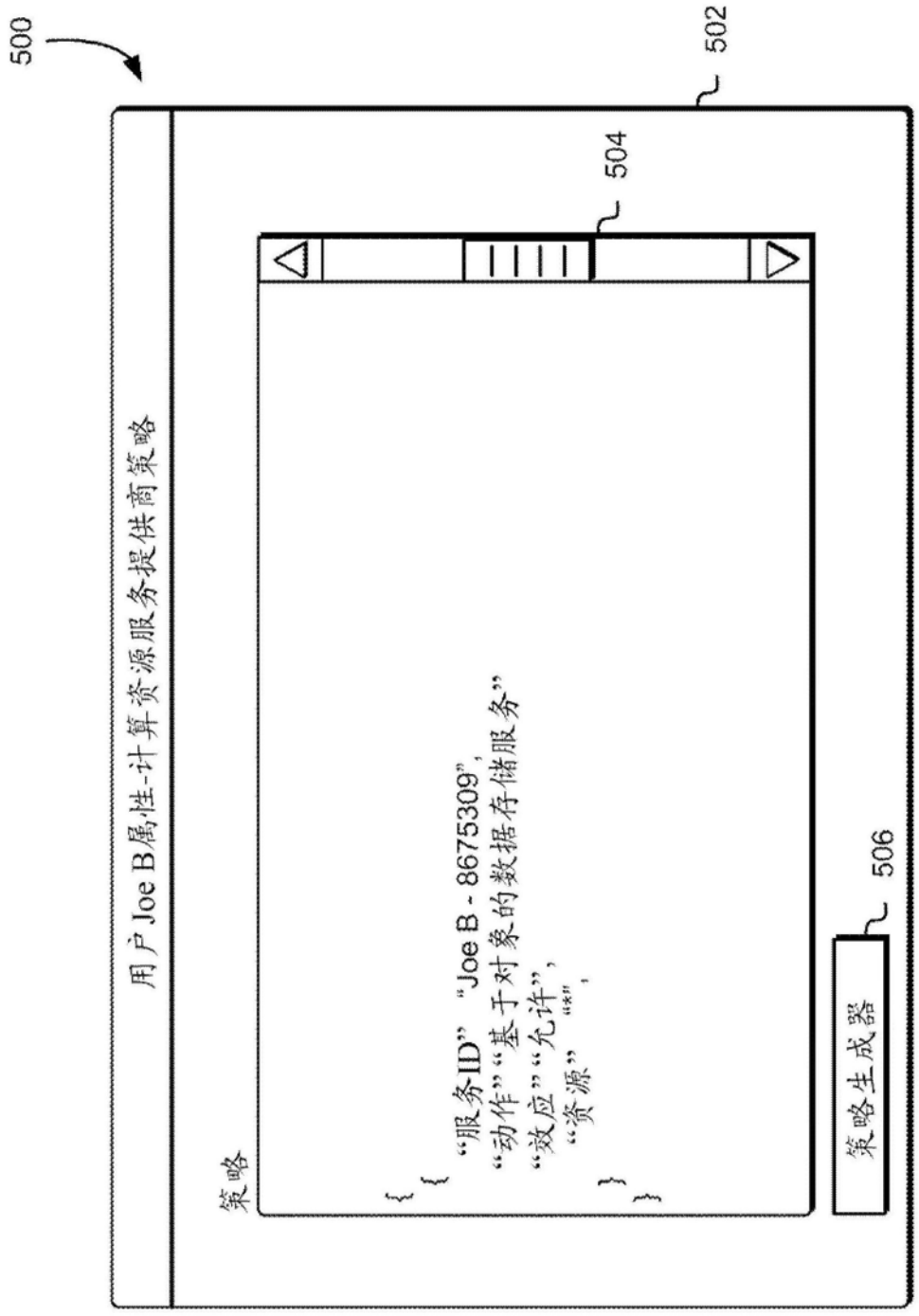

500
502
504
506
用户Joe B属性-计算资源服务提供商策略
策略
{
{
"服务ID" "Joe B - 8675309",
"动作" "基于对象的数据存储服务"
"效应" "允许",
"资源" "*"
}
}
策略生成器

图5

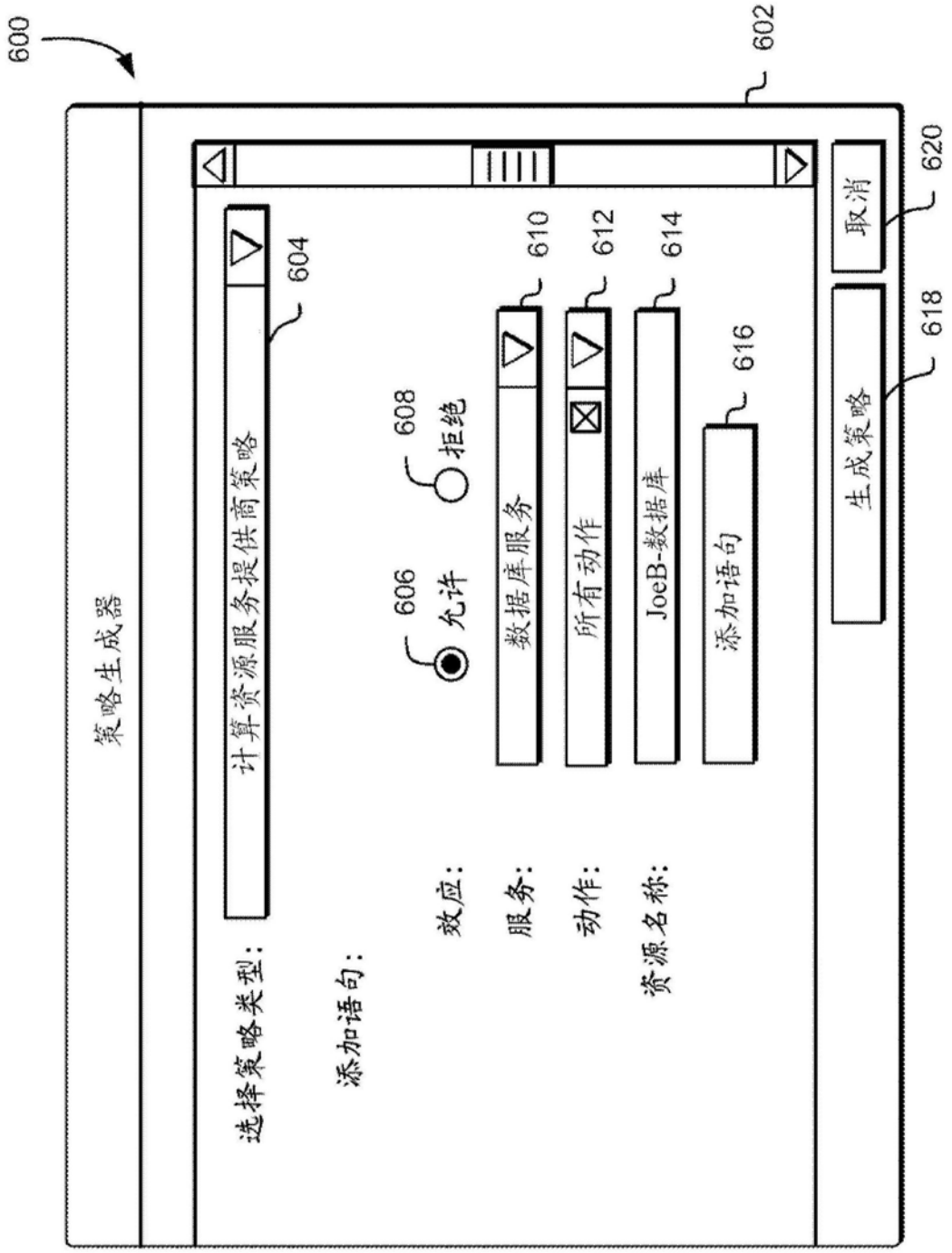

600
602
策略生成器
选择策略类型:
计算资源服务提供商策略
604
添加语句:
效应:
606
允许
608
拒绝
服务:
数据库服务
610
动作:
所有动作
612
资源名称:
JoeB-数据库
614
添加语句
616
取消
620
生成策略
618

图6

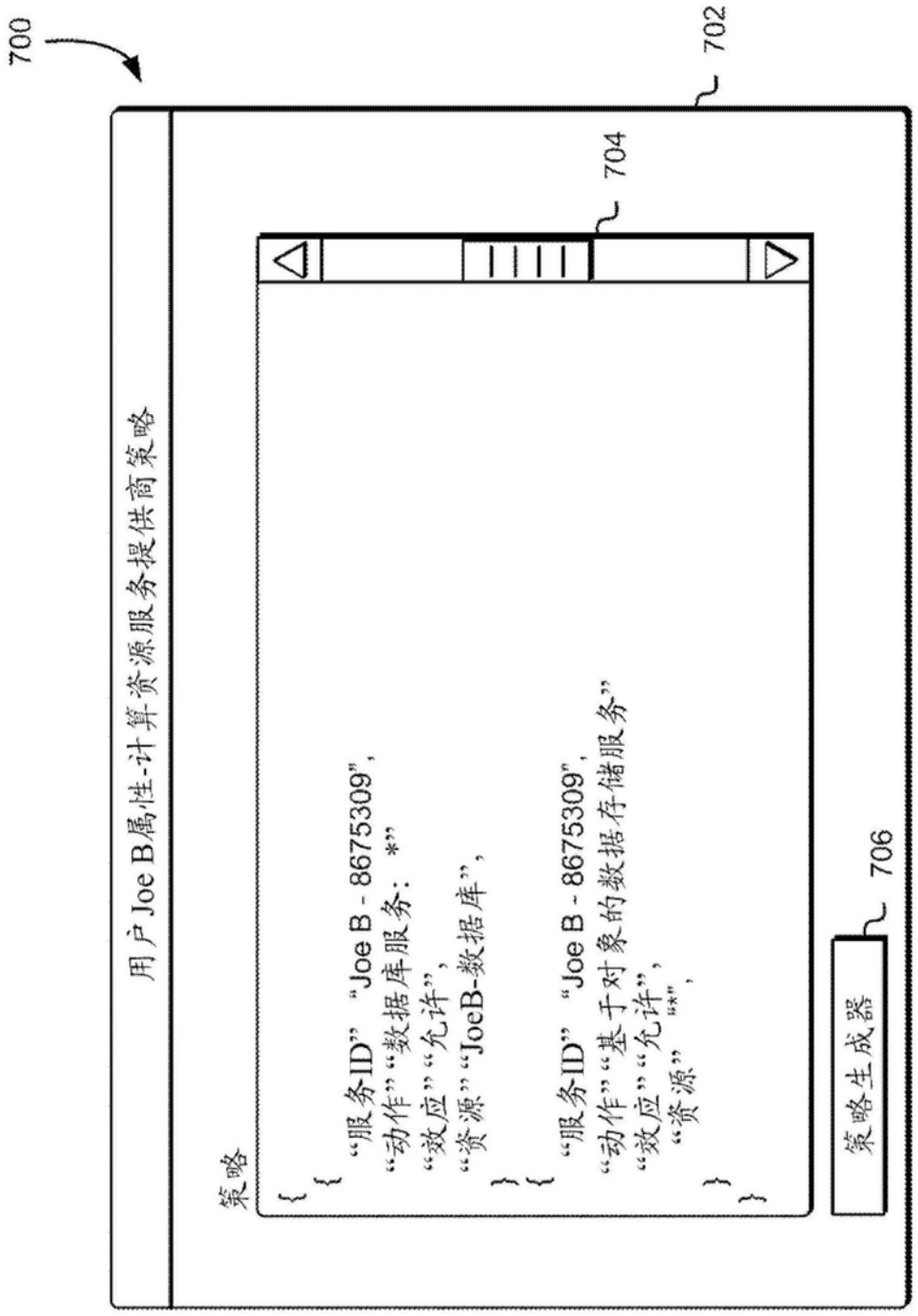

700
702
704
706
用户Joe B属性-计算资源服务提供商策略
策略
{
{
"服务ID" "Joe B - 8675309",
"动作""数据库服务: *"
"效应""允许",
"资源""JoeB-数据库",
}
{
"服务ID" "Joe B - 8675309",
"动作""基于对象的数据存储服务"
"效应""允许",
"资源" "*",
}
}
策略生成器

图7

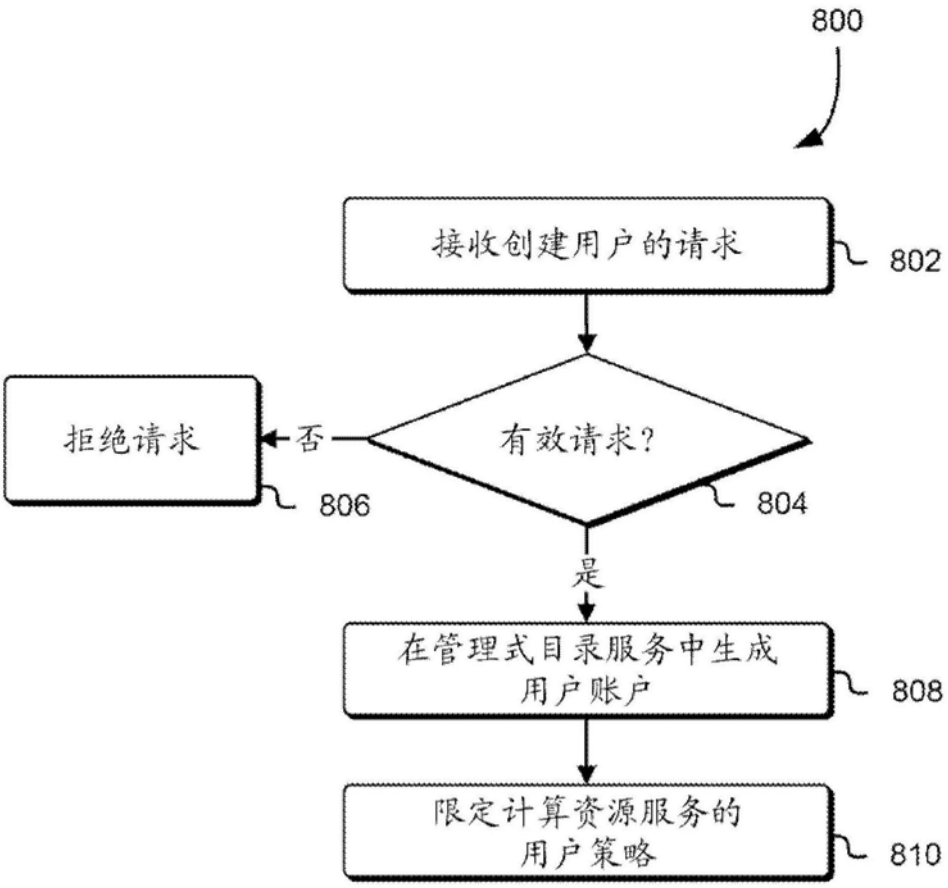

800
接收创建用户的请求
802
有效请求?
804
否
拒绝请求
806
是
在管理式目录服务中生成
用户账户
808
限定计算资源服务的
用户策略
810

图8

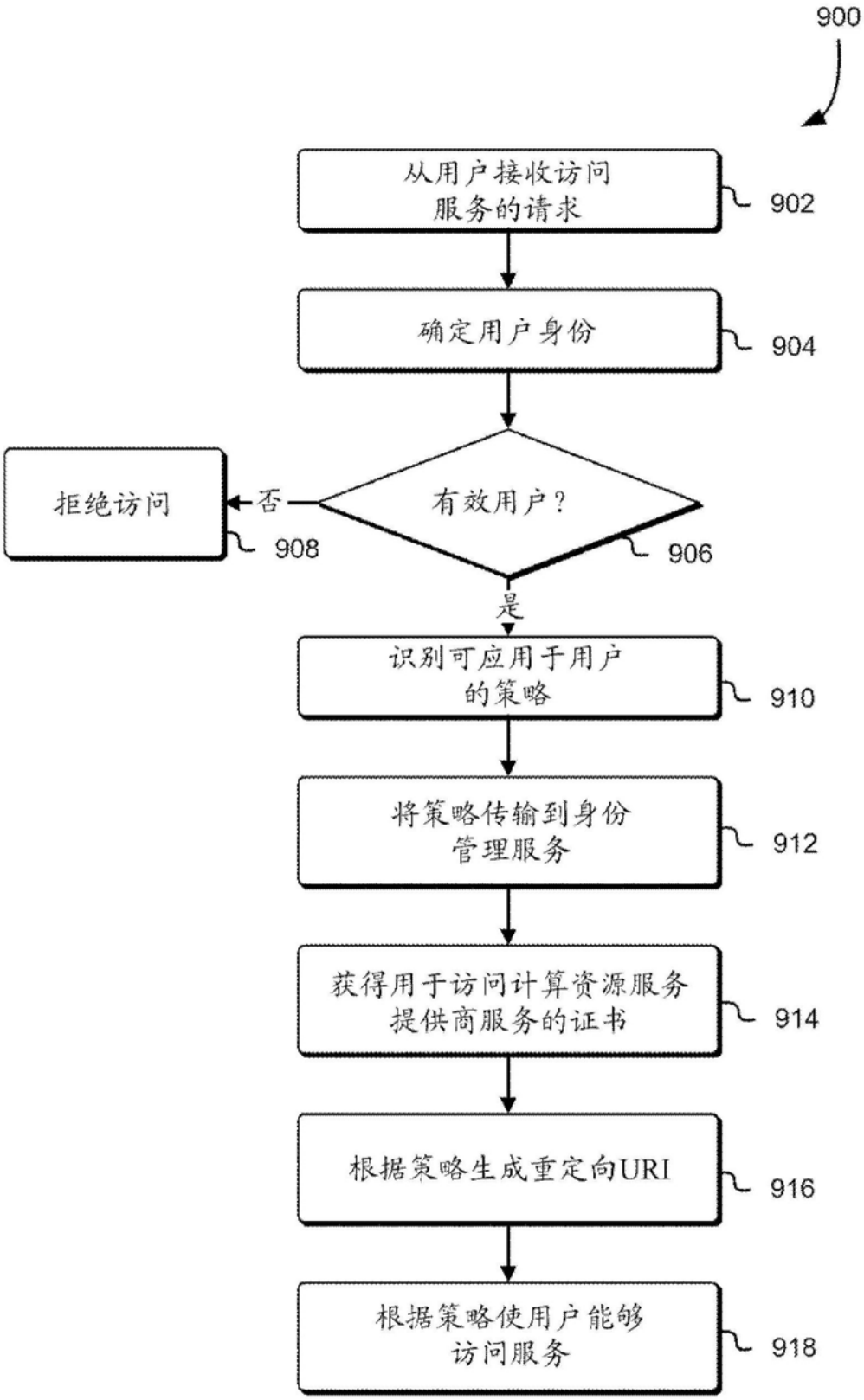

900
从用户接收访问服务的请求
902
确定用户身份
904
有效用户？
906
否
拒绝访问
908
是
识别可应用于用户的策略
910
将策略传输到身份管理服务
912
获得用于访问计算资源服务提供商服务的证书
914
根据策略生成重定向URI
916
根据策略使用户能够访问服务
918

图9

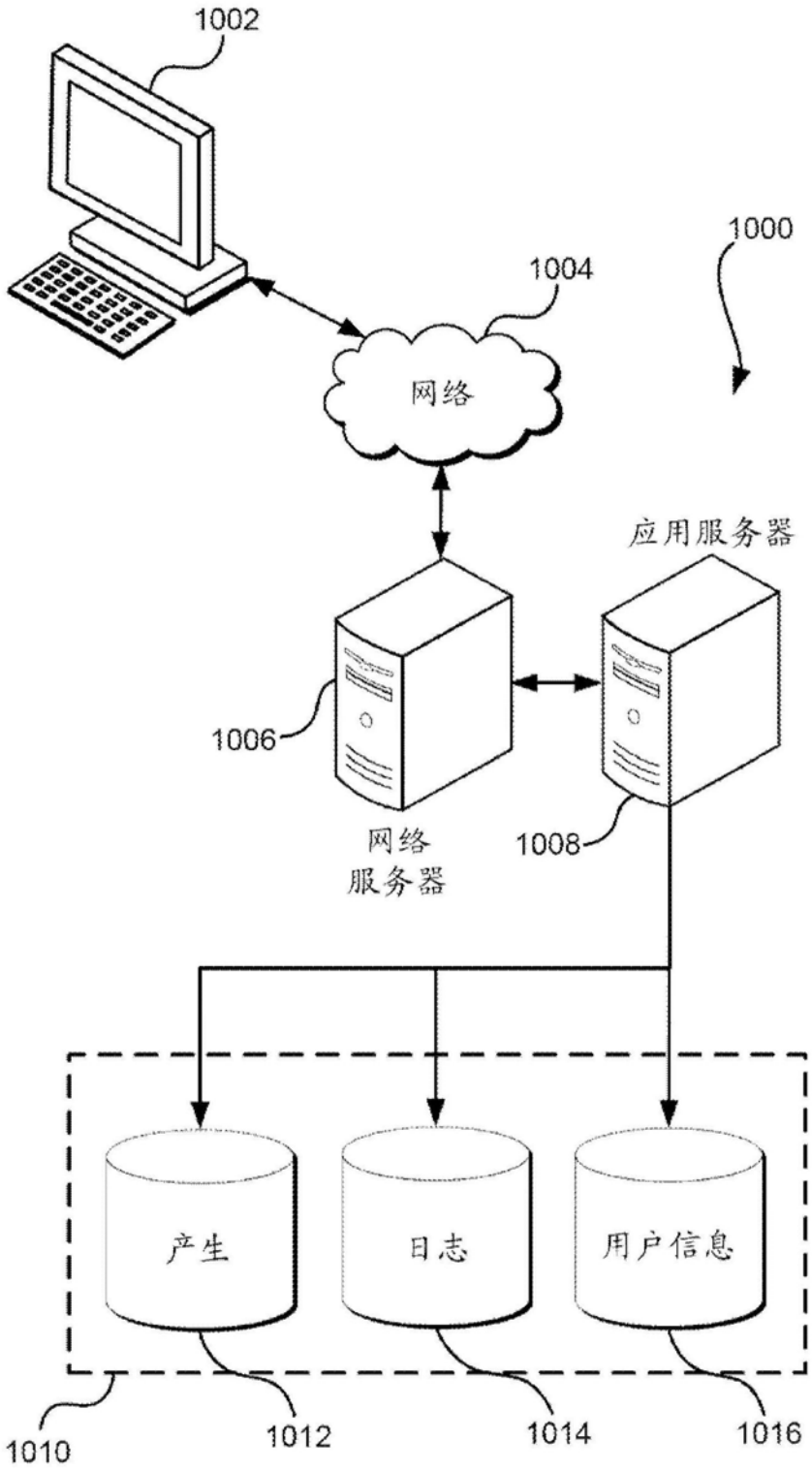

1002
1000
1004
网络
应用服务器
1006
网络
服务器
1008
产生
日志
用户信息
1010
1012
1014
1016

图10