(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 105308614 B
(45)授权公告日 2022.04.26

(21)申请号 201480035065.8
(22)申请日 2014.06.19
(65)同一申请的已公布的文献号
申请公布号 CN 105308614 A
(43)申请公布日 2016.02.03
(30)优先权数据
13/923,004 2013.06.20 US
(85)PCT国际申请进入国家阶段日
2015.12.18
(86)PCT国际申请的申请数据
PCT/US2014/043246 2014.06.19
(87)PCT国际申请的公布数据
WO2014/205257 EN 2014.12.24

(73)专利权人 亚马逊技术股份有限公司
地址 美国内华达州
(72)发明人 G·B·罗斯
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 姬利永

(51)Int.Cl.
G06F 21/60(2013.01)
(56)对比文件
US 8171522 B2,2012.05.01
US 7478419 B2,2009.01.13
US 2006/0259901 A1,2006.11.16
审查员 李莎

权利要求书2页 说明书20页 附图11页

(54)发明名称

策略强制执行延迟

(57)摘要

策略被用来控制对资源的访问。至少在一些情况下,只有将更改策略集的请求提交成使得所述请求的更改将在与针对延迟的强制执行的要求相符的将来某一时刻变得有效,所述请求才可以是能够实现的。可将针对延迟的强制执行的所述要求编码到所述策略集中的策略中。

CN 105308614 B

1.一种用于管理策略的计算机实现的方法,其包括:

接收针对更改一个或多个策略集的请求;

至少部分地基于所述请求,确定所述请求的更改是否满足为策略更改变得有效而指定先决条件的现有策略的一个或多个要求,所述一个或多个要求中的至少一个是由所述请求所指示的有效时间符合所述现有策略的针对所述更改的延迟要求;以及

由于确定所述请求的更改满足所述一个或多个要求,根据所述要求使所述更改变得有效。

2.如权利要求1所述的计算机实现的方法,其还包括:

向指定为有权取消所述更改的身份传输通知。

3.如权利要求1所述的计算机实现的方法,其中:

所述请求是具有应用程序编程接口参数集的应用程序编程接口调用;以及

确定所述请求的更改是否满足一个或多个要求包括确定来自所述应用程序编程接口参数集的参数是否满足所述一个或多个要求。

4.如权利要求1所述的计算机实现的方法,其中:

所述一个或多个策略集应用于以计算资源服务提供商的客户的名义管理的计算资源集;以及

存储具有所述计算资源服务提供商的其他客户的一个或多个策略的其他集的所述一个或多个策略集。

5.如权利要求1所述的计算机实现的方法,其中所述更改是向所述一个或多个策略集添加策略。

6.如权利要求1所述的计算机实现的方法,其中所述要求是来自所述一个或多个策略集的结果。

7.如权利要求1所述的计算机实现的方法,其还包括致使传输所述请求的一个或多个通知。

8.如权利要求1所述的计算机实现的方法,其还包括:

在所述更改变得有效之前接收取消所述更改的请求;以及

由于接收取消所述更改的所述请求,禁止所述更改变得有效。

9.如权利要求1所述的计算机实现的方法,其中确定所述请求的更改是否满足所述一个或多个要求包括确定编码提议的策略是否包括指示与所述一个或多个请求一致的强制执行延迟的参数。

10.一种用于管理策略的系统,其包括:

一个或多个处理器;以及

存储指令的存储器,所述指令能由所述一个或多个处理器执行以引起所述系统:

至少部分地基于针对更改一个或多个策略集的请求,从另一系统接收信息;

至少部分地基于所述接收的信息,确定所述请求的更改是否与为策略更改变得有效而指定先决条件的现有策略的一个或多个延迟要求相符,所述请求的更改包括由所述信息指示的有效时间;

由于确定所述请求的更改与所述一个或多个要求相符,使所述请求的更改变得有效。

11.如权利要求10所述的系统,其中所述请求是网页服务请求。

12.如权利要求10所述的系统，其中所述信息是编码所提议的策略。

13.如权利要求10所述的系统，其中所述指令进一步能执行来引起所述系统：在接收到第二请求之后，

从策略集选择编码指示当前正在实行的有效时间的策略的子集；以及

至少部分地基于所述选择的策略集，提供确定是否实现所述第二请求。

14.如权利要求10所述的系统，其中所述要求是由所述系统强制执行的现有策略的结果。

15.如权利要求10所述的系统，其中所述指令进一步能执行来能够取消变得有效的所述请求的更改。

策略强制执行延迟

[0001] 相关申请的交叉引用

[0002] 本申请要求2013年6月20日提交的共同待决的美国专利申请号13/923,004的优先权,所述申请的全部内容特此以引用的方式并入本文。

[0003] 背景

[0004] 现代计算网络提供对广泛范围的计算资源诸如数据档案库、搜索引擎、数据处理、数据管理、通信、电子市场以及媒体和娱乐服务的访问。由于此类计算资源及其用户社区的数量和大小已经增长并且变得更加复杂,因而需要建立日益复杂的使用策略。例如,此类策略可包括着手解决安全性、私密性、访问、管理和成本考虑的策略。然而,策略强制执行的常规方法具有缺点。

[0005] 例如,策略强制执行的常规方法可以是特设的,受限于特定类型的计算资源和/或受限于策略控制的特定集。在甚至并入有适当数量的计算资源类型的异构计算环境中,特定方法可能产生显著的管理负担。此外,由于计算资源的数量增长过大,一些常规方法规模很差。较小的管理和/或低效的性能在较大规模下可能变得成问题。一些常规方法缺乏集中的策略管理服务,这可能妨碍在分布式计算环境中一致的策略管理。一些常规方法受限于集中的策略管理,所述集中的策略管理可响应于不断变化的要求而不够灵活。策略集的复杂性对策略强制执行的一些常规方法来说也可能成问题。

[0006] 附图简述

[0007] 将参照附图描述根据本公开的各种实施方案,在附图中:

[0008] 图1示出说明本公开的各个方面的图;

[0009] 图2示出可实现各种实施方案的环境的说明性实例;

[0010] 图3示出根据至少一个实施方案的服务和可包括所述服务的组件的说明性实例;

[0011] 图4示出根据至少一个实施方案的策略管理服务和可包括所述策略管理服务的组件的说明性实例;

[0012] 图5示出根据至少一个实施方案的策略文档的说明性实例;

[0013] 图6示出根据至少一个实施方案的策略文档的说明性实例;

[0014] 图7示出根据至少一个实施方案的策略文档的语句的说明性实例;

[0015] 图8示出根据至少一个实施方案的用于实现请求的过程的说明性实例;

[0016] 图9示出根据至少一个实施方案的用于实现更改策略的请求的过程的说明性实例;

[0017] 图10示出根据至少一个实施方案的用于管理策略的过程的说明性实例;并且

[0018] 图11示出可实现各种实施方案的环境。

[0019] 详述

[0020] 在以下描述中,将描述各种实施方案。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,没有具体细节的情况下也可以实行实施方案。此外,为了不使所描述的实施方案变得模糊,可能会省略或简化众所周知的特征。

[0021] 本文所描述和建议的技术涉及与计算资源有关的策略的有效管理。策略集可由计算机系统强制执行，以便控制对各种计算资源的访问。策略集可以是可配置的，这样使得用户可如所希望地向策略集进行添加和/或以其他方式更改策略集。在各种实施方案中，策略控制改变策略集的能力。例如，可制作策略来限制能够更改策略的那些人，限制做出怎样的更改以及以其他方式帮助确保策略更改对以其名义而强制执行策略的实体是有益的。

[0022] 在一些实施方案中，系统在对策略集做出的更改变得有效之前强制执行延迟。所述延迟通常可由系统强制执行，或可归因于需要所述延迟的策略而被强制执行。在一个实施方案中，当接收到添加策略的请求时，至少部分地基于根据所需延迟是否提交所述请求，所述请求可以被批准(例如，允许实现)或被拒绝。例如，请求待被添加的策略可包括指示策略应何时变得有效的信息，诸如将来某个时刻或限定延迟的持续时间。作为另一个实例，请求可以是具有参数的应用程序编程接口(API)调用的形式，所述参数指定指示策略应何时变得有效的信息。如果指示策略应何时变得有效的信息符合要求，那么就可实现添加策略的请求。换言之，至少部分地基于所请求的策略添加指示延迟大于或等于所要求的延迟，可以允许所述请求。当允许实现请求时，系统可根据指示策略应何时变得有效的信息来使对应的策略变得有效。如下文所述，在使策略在将来某一时刻变得有效之后，可在其生效之前取消所述策略。在取消策略之后，策略就可能变得禁用而不能生效。

[0023] 在各种实施方案中，当用户提交更改策略的请求(例如，向策略集添加策略)时，一个或多个通知就被触发。通知系统(例如，电子邮件系统或提供通知的其他系统)可被通知，并且其结果是，可向一个或多个指定方(例如一个或多个策略管理员、合规职员和/或其他人)发送通知。一方或多方可以在关于添加/更改策略的策略中或以另一种方式被指定，并且可以在关于添加/更改策略的策略中被指定为有权取消要求延迟其有效性的策略。通知还可包括用于取消策略更改的机制，诸如如果超链接被选定，那么就致使取消策略更改。以此方式，指定方可被提供机会来取消策略更改，否则所述策略更改在所需延迟之后允许变得有效。另外，用于取消尚未变得有效的策略更改(即，系统尚未强制执行的策略更改)的条件可能与用于取消已经变得有效的策略更改的条件相比较不严格。例如，用于取消尚未实行的策略的要求可能比用于取消已经实行的策略的要求更低(较不严格)。例如，用于已经实行的策略比用于尚未实行的策略存在更高的认证要求。另外，取消已经实行的策略可能需要策略指定的延迟，而取消尚未实行的策略可能不需要延迟或可能需要更短的延迟。众多的变化认为在本公开的范围内，其包括但不限于下文明确地论述的那些变化。

[0024] 图1是说明本公开的各个方面的图。如上文所述，根据本文所描述的各种实施方案操作的系统允许动态策略集的有效管理。在各种实施方案中，经授权的用户可更新用于各种计算资源的系统策略。例如，用户可利用向服务提供商的策略管理系统提交适当配置的应用程序编程接口(API)调用(诸如网页服务调用)的计算机系统。如图1所示，本公开的各个方面涉及在所请求的策略更改变得有效之前的延迟。在一些实施方案中，如图中沙漏所示，策略管理系统在策略变得有效之前强制执行延迟。此外，如图中警报铃所示，由于某些类型的更改策略集的请求，可实现各种警报。可以各种方式，诸如通过电子通知、增强的审计日志、实际警报，以及通常以向一个或多个感兴趣方提供关于所请求的策略更改的通知的任何方式实现警报。以此方式，感兴趣方诸如策略管理员在策略更改变得有效之前有机会将其取消。如下文更加详细地所述，在策略变得有效之前强制执行延迟允许对系统强制

执行哪个策略进行鲁棒的管理控制。

[0025] 图2示出可实践本公开的各种实施方案的环境200的说明性实例。在环境200中，计算资源服务提供商202可向客户204提供各种服务。客户204可以是可利用由计算资源服务提供商202提供的各种服务来保持信息并向其可位于各种地理位置中的雇员传递信息的组织。另外地，客户204可以是可利用各种服务来向位于远处的工作组传递内容的个体。如图2所示，客户204可通过一个或多个通信网络206(诸如互联网)与计算资源服务提供商202进行通信。从客户204到计算资源服务提供商202的一些通信可致使计算资源服务提供商202根据本文所描述的各种技术或其变型进行操作。

[0026] 如以上所指出，计算资源服务提供商202可向其客户提供各种计算资源服务。在这个实例中，由计算资源服务提供商提供的服务包括虚拟计算机系统服务208、块级数据存储服务210、加密服务212(也称为密钥管理服务)、按需数据存储服务214和一个或多个其他服务216，但是不是本公开的所有实施方案都将包括所有此类服务，并且除本文明确描述的服务之外或作为替代本文明确描述的服务，可提供另外的服务。每种服务可包括一个或多个网页服务接口，所述网页服务接口使客户204能够通过网页服务请求向各种服务提交适当配置的API呼叫。此外，每种服务可包括一个或多个服务接口，所述一个或多个服务接口使服务能够彼此相互访问(例如，使虚拟计算机系统服务208的虚拟计算机系统能够将数据存储在按需数据存储服务中或检索来自按需数据存储服务的数据，和/或访问由块级数据存储服务提供的块级数据存储装置)。

[0027] 虚拟计算机系统服务208可以是计算资源的集合，其被配置来以计算资源服务提供商202的客户204的名义将虚拟机实例实例化到虚拟计算资源上。计算资源服务提供商202的客户204可(经由适当配置并已认证的API调用)与虚拟计算机系统的服务交互，以便供应和操作在由计算资源服务提供商202托管并操作的物理计算装置上实例化的虚拟计算机系统。虚拟计算机系统可用于各种目的，诸如以便操作为支持网站的服务器，操作业务应用程序或通常用作用于客户的计算能力。用于虚拟计算机系统的其他应用程序可以用来支持数据库应用程序、电子商务应用程序、业务应用程序和/或其他应用程序。

[0028] 块级数据存储服务210可包括计算资源的集合，其共同地操作来使用块级存储装置(和/或其虚拟化)存储用于客户204的数据。例如，块级数据存储服务210的块级存储装置可以可操作地附接到由虚拟计算机系统服务208提供的虚拟计算机系统，以用作用于计算机系统的逻辑单元(例如，虚拟驱动器)。块级存储装置可能够永久性存储所使用的/由对应的虚拟计算机系统产生的数据，在所述对应的虚拟计算机系统中虚拟计算机系统服务208可仅提供临时的数据存储。

[0029] 如图2中所示，计算资源服务提供商202可操作加密服务，所述加密服务会结合图3在下文更加详细地进行描述。通常，加密服务可以是计算资源的集合，其共同地被配置来管理和使用用于计算资源服务提供商的客户的密钥。由加密服务212使用的密钥可具有相关联的标识符，当提交请求来执行加密操作(诸如加密、解密和消息签署)和/或其他操作(诸如密钥转动)时，所述相关联的标识符可供客户参考。加密服务可安全地维护密钥以避免未经授权方的访问。

[0030] 计算资源服务提供商202还可包括按需数据存储服务。按需数据存储服务214可以是计算资源的集合，其被配置来同步地处理请求以存储和/或访问数据。按需数据存储服务

214可使用能够使按需数据存储服务214快速地定位并检索数据的计算资源(例如,数据库)进行操作,以便允许响应于针对数据的请求而提供数据。例如,按需数据存储服务可保持所存储的数据,方式为使得当检索针对数据对象的请求时,可响应于所述请求而提供数据对象(或可启动数据对象的流式处理)。如上所述,可将存储在按需数据存储服务214中的数据组织到数据对象中。也许除了对大小进行某些限制之外,数据对象可具有任意大小。因此,按需数据存储服务214可存储具有大小不一的众多数据对象。按需数据存储服务214可操作为将数据对象与数据对象的标识符相关联的密钥值存储器,所述数据对象的标识符可由客户204使用,以检索或执行与由按需数据存储服务214存储的数据对象有关的其他操作。按需数据存储服务214也可访问加密服务212。例如,在一些实施方案中,加密服务使用按需数据存储服务来存储客户的呈加密形式的密钥,其中能够用来解密客户密钥的密钥仅可访问加密服务212的特定装置。可通过适当配置的API调用来由客户、另一个服务或其他实体访问数据存储服务。

[0031] 在图2示出的环境中,包括通知服务216。通知服务216可包括计算资源的集合,其共同地被配置来提供网页服务或其他接口、以及可用来创建客户想要通知给应用程序(或人)的主题的基于浏览器的管理控制台,使客户端预订这些主题,发布消息以及在客户端的选择的协议(即,HTTP、电子邮件、SMS等)上传递这些消息。通知服务可使用“推送”机制将通知提供给客户端,无需对新信息和更新定期地检查或“轮询”。通知服务可用于各种目的,诸如监控在虚拟计算机系统服务中执行的应用程序、工作流系统、时间敏感信息更新、移动应用程序以及许多其他。

[0032] 计算资源服务提供商202另外地可基于其客户204的需要来维护一个或多个其他服务218。例如,计算资源服务提供商202可维护用于其客户204的数据库服务。数据库服务可以是计算资源的集合,其共同地操作以运行用于一个或多个客户204的一个或多个数据库。计算资源服务提供商202的客户204可通过利用适当配置的API调用来操作和管理来自数据库服务的数据库。这进而可允许客户204维护并潜在地缩放数据库中的操作。其他服务包括但不限于对象级档案库数据存储服务、管理和/或监控其他服务的服务和/或其他服务。

[0033] 如图2中所示,在各种实施方案中,计算资源服务提供商202包括认证系统220和策略管理服务222。在一个实施方案中,认证系统是被配置来执行认证客户的用户所包括的操作的计算机系统(即,计算资源的集合)。例如,服务中的一个可向认证服务提供来自用户的信息,以接收指示用户请求是否可信的信息作为回报。确定用户请求是否可信可以任何合适的方式来执行,并且执行认证的方式在各种实施方案之间可能有所不同。例如,在一些实施方案中,用户以电子方式签署传输给服务的消息(即,由用户操作的计算机系统以电子方式签署消息)。电子签名可使用认证实体(例如,用户)和认证系统都可用的秘密信息(例如,与用户关联的密钥对的私人密钥)而生成。可向认证系统提供请求和针对请求的签名,认证系统可使用秘密信息计算用于与所接收签名进行比较的参考签名,以便确定请求是否可信。

[0034] 如果请求可信,那么认证服务可以向服务提供以下信息,服务可以使用所述信息来确定是否实现未决请求和/或执行其他动作,诸如向其他服务(诸如密码服务)证明请求是可信的,从而使得其他服务能够相应地操作。例如,认证服务系统可提供另一个服务可分

析以验证请求可信性的令牌。电子签名和/或令牌可具有以各种方式来限制的有效性。例如，电子签名和/或令牌可在一定时间量内是有效的。在一个实例中，电子签名和/或令牌至少部分地基于将时间戳看作输入的函数(例如，基于散列的消息认证码)生成，时间戳包括在用于验证的电子签名和/或令牌内。检验所提交电子签名/或令牌的实体可以检查所接收时间戳是足够当前的(例如，在从当前时间开始的预先确定的时间量内)并使用所接收时间戳生成参考签名/令牌。如果用于生成所提交电子签名/令牌的时间戳不是足够当前的和/或所提交签名/令牌和参考签名/令牌不匹配，那么认证可能失败。以此方式，如果电子签名泄露，它将仅在短时间内有效，从而限制由泄露造成的潜在危害。应注意，验证可信性的其他方式也被视为是在本公开的范围内。

[0035] 在一个实施方案中，策略管理服务222是被配置来以计算资源服务提供商的客户的名义管理策略的计算机系统。策略管理服务222可包括使客户能够提交与策略的管理有关的请求的接口。此类请求例如可以是添加、删除、更改或以其他方式修改用于客户或用于其他管理动作(诸如提供现有策略的库存清单)等的策略的请求。策略管理服务222也可与其他服务进行接口连接，以便使服务能够根据对应于针对其作出请求的客户的策略确定是否可允许实现未决请求。例如，当服务接收请求时，服务(如果服务在本地未高速缓存此类信息)可将关于请求(和/或请求本身)的信息传输给策略管理系统，所述策略管理系统可分析用于客户的策略来确定客户的现有策略是否允许实现所述请求并且根据所述确定将信息提供给服务。下文结合图4描述示例性策略管理系统。环境200中还可包括其他服务和/或组件。类似地，本公开的技术应用到其他环境。

[0036] 图3示出根据各种实施方案的服务300的说明性实例。服务300例如可以是上文结合图2描述的服务中的一个。例如，服务300可以是诸如上文所述的虚拟计算机系统服务208、块级数据存储服务210、加密服务212、按需数据存储服务214、通知服务216或一个或多个其他服务218。应注意，尽管图3示出服务300的各种组件，但是各种服务将根据各种不同实施方案而变化，并且可包括与本文所示出的那些组件不同的组件。如图3所示，服务300包括服务前端302。服务前端302可包括计算资源的集合，其共同地被配置来诸如通过应用程序编程接口(API)调用向服务前端302提供客户可通过其进行通信的接口。例如，服务前端302可包括一个或多个网页服务器、一个或多个负载均衡器、一个或多个应用服务器以及本文大体描述的其他计算资源。

[0037] 在一个实施方案中，服务前端302被配置来接收客户请求并且对那些客户请求作出响应。服务前端302还可包括能够接收和处理来自其他服务的请求的接口。为了处理所述请求，服务前端302可与服务300的各种其他组件交互。例如，如图3所示，服务300包括认证运行时间服务304。认证运行时间服务304(就像前端302处的服务)可以是服务300的子系统，其包括共同地被配置来作出关于认证的确定，以使服务前端302视情况拒绝或实现请求的计算资源的集合。在一个实施方案中，当服务前端302接收请求时，服务前端302与认证运行时间服务304进行通信来确定请求是否可信。例如，请求可包括使用客户与诸如上文结合图2所述的认证系统之间共享的秘密而生成的电子签名。认证运行时间服务304可经由认证系统接口306传输信息，认证系统接口306使认证运行时间服务304能够从诸如上文结合图2所述的认证系统获得请求是否可信的确定。在操作以确定请求是否可信中，认证运行时间服务304可高速缓存某些信息，以便使认证运行时间服务304能够作出关于认证的确定，而

无需通过认证系统接口306对认证系统进行认证。应注意，尽管图3示出特定的实施方案，但是服务300可以任意合适的方式并且不一定以示出的方式认证请求。

[0038] 如图3中所示，服务前端302也与策略强制执行服务308通信，以便确定是否实现某些请求。策略强制执行服务308可以是服务300的子系统，其包括共同地被配置来使服务前端302能够确定是否实现或拒绝请求的计算资源的集合。如同认证运行时间服务304一样，策略强制执行服务308可与策略管理系统(图中未示出)进行通信，以便达到确定请求的实现是否与策略相符的目的。例如，当服务前端302接收请求时，服务前端302可将所述请求或至少部分地基于所述请求的信息传输给策略强制执行服务308。策略强制执行服务308可经由策略管理系统接口310将信息传输给策略管理系统以便作出确定。如同认证运行时间服务304一样，策略强制执行服务308可高速缓存各种信息，以便能够确定在不与策略管理系统进行通信的情况下请求的实现是否与策略相符。

[0039] 在各种实施方案中，当所接收的请求在与策略相符的情况下确定为既可信又可实现时，服务前端302也与服务网络312进行通信。服务网络312可以是服务300的子系统，其包括被配置来操作支持提供服务的计算资源的集合。例如，在服务300是虚拟计算机系统服务的实施方案中，服务网络312可包括以服务300的客户的名义实现虚拟计算机系统的多个物理主机计算装置。通过服务前端302的请求可涉及使用服务网络312实现的虚拟计算机系统的操作。例如，可将请求提交给服务前端302，为了达到供应、解除供应、修改或以其他方式远程管理虚拟计算机系统的目的。在块级数据存储服务210的实例中，服务网络312可包括数据存储服务器与对应的数据存储装置的集合。服务前端302可与服务网络312交互以便达到各种目的，诸如将存储空间分配给客户、不将存储空间分配给客户、以及通常与由服务300提供的一个或多个虚拟块级数据存储装置的管理有关。在加密服务的实例中，服务网络312可包括能够安全管理密钥的各种硬件装置。例如，服务网络312可包括可以是安全地存储密钥材料的装置的多个安全模块(例如，硬件安全模块)。用于加密服务的服务网络还可包括用于以客户的名义存储密钥的数据存储装置和通常支持加密服务的操作的其他装置。在按需数据存储服务的实例中，服务网络312如同块级数据存储服务一样可包括数据存储服务器和对应的数据存储装置。服务网络还可包括一个或多个数据库，以便操作为密钥值存储器来启用数据在服务网络312内的位置。服务网络312还可包括其他装置(例如，服务器计算机系统)，诸如进行操作以持久地(即，冗余地)存储数据来执行无用单元收集过程的装置等。通常，服务网络312可包括可适用于所提供的服务的计算资源。同样，尽管未示出，但是服务网络312可包括适当的联网装置，诸如路由器、开关、负载均衡器和能够共同操作服务网络312中的装置的其他装置。当然，所包括的确切资源以及其集中式配置将根据各种服务和实现其共同配置的各种实施方案而变化。

[0040] 图4示出根据各种实施方案的策略管理服务400的说明性实例。如图4所示，策略管理服务400包括策略管理系统前端402。策略管理系统前端402可被配置成诸如上文结合图3所描述的服务前端302。具体地，策略管理系统前端402可被配置来接收客户的请求并且提供对那些请求作出的响应。策略管理系统前端402也可被配置来从其他服务接收请求，诸如用于确定根据策略是否实现请求。策略管理系统前端402的请求可以是与策略的管理或计算资源提供商的账户有关的各种请求。例如，策略管理系统前端的请求可以是适当配置的API调用，以添加策略、删除策略、更改策略以及通常执行与策略有关的各种动作(诸如提供

策略的库存清单)等。如同本文所描述的其他前端系统一样,策略管理系统前端402可包括执行不同操作的一个或多个网页服务器。例如,在一个实施方案中,策略管理系统前端402可包括在网络(诸如互联网)上提供用于管理策略的控制台接口的网页服务器。所述控制台接口可以是具有各种GUI控件的图形用户接口(GUI),所述各种GUI控件允许用户执行与策略的管理有关的各种动作。示例性动作包括定义策略和提交所定义的策略。例如,用户可使用用于定义策略的各种GUI控件(下拉菜单、复选框、文本输入框等),并且随后与GUI交互来使网页服务器提交所定义的策略。提交请求中所定义的策略(或通常提交经由GUI传输的任何请求)可致使请求从提供GUI的网页服务器传输到协调处理所述请求的另一个网页服务器,诸如下文所述。另一个网页服务器也可被客户访问,以用于直接提交请求而不通过提供GUI的网页服务器。其他变型也被视为是在本公开的范围内。

[0041] 如同上文结合图3所描述的服务300一样,策略管理服务400可包括认证运行时间服务404和认证系统接口406,以便使策略管理系统前端402能够视情况实现或拒绝请求。如同服务前端302一样,策略管理系统前端402可(例如,经由适当配置的通信信号)与各种组件交互,以便提供策略管理服务。例如,如图4所示,策略管理系统前端402可利用通知系统接口408来与诸如上文所述的通知系统进行通信。如下文更加详细地所述,可使用通知系统以便提醒与某些类型的活动的账户相关联的用户,所述某些类型的活动的账户与所述账户的策略有关。例如,如下文更加详细地所述,向用于账户的策略集的尝试添加可致使策略管理系统前端402使得通知系统提供一个或多个所尝试的策略添加的通知。以此方式,通知的接收能够采取适当的动作,诸如何时添加策略是不适当的。

[0042] 在一个实施方案中,策略管理系统前端402利用策略引擎410,策略引擎410可以是策略管理服务400的子系统,其包括共同地被配置来评估策略的计算资源的集合。策略引擎410可从策略管理系统前端402接收已经接收到的请求和/或至少部分地基于该请求的信息。策略引擎410可识别可适用于请求的任何策略,评估请求的实现是否与任何可适用的策略相符,以及向策略管理系统前端402提供请求的实现是否与现有的策略相符的通知。策略引擎410可根据各种实施方案以各种方式来操作。例如,如下文所述,可将策略编码到策略文档中,所述策略文档编码关于策略所应用到的主体、资源及其他项目的各种信息。策略引擎(或与策略引擎协同工作的另一个系统)可使用策略中的信息来确定策略集中的哪一个应用到特定请求。例如,如果由在请求中识别的特定实体提交请求,那么策略引擎就可选择可适用于该实体的策略。如果请求包括特定的资源,那么策略引擎就可选择可适用于特定资源的策略。此外,如下文更加详细地所述,策略文档可包括指示策略文档当前是否有效(即,编码到策略文档中的一个或多个策略当前是否被强制执行)的信息,诸如指示编码到策略文档中的一个或多个策略何时开始有效的时间的信息。识别可应用的策略文档可包括选择施行的策略文档并且忽视未施行的策略文档。

[0043] 策略引擎可依次地或以其他方式处理策略以确定所选择的策略中的每一个是否允许实现请求。策略引擎可向策略管理系统前端402(例如,以对请求评估由策略管理系统前端402提交的策略作出的响应的形式)传输指示对应于策略的用于账户的策略集是否允许或阻止实现该请求的通知。策略排除其他信息,诸如实现请求的一个或多个原因(例如,识别请求的实现将违背的一个或多个策略的信息,和/或至少部分地基于请求的实现将违背的策略的信息)。

[0044] 为了针对多个用户进行大规模管理，策略管理服务400可包括策略存储库412，其可包括存储策略文档的一个或多个数据存储装置，所述策略文档编码计算资源服务提供商的各个账户的策略。在一些实施方案中，策略存储库412存储用于多个实体(例如，计算资源服务提供商的客户)的策略，并且因此存储与策略对应的实体直接或间接关联的策略。

[0045] 如图4所示，在策略管理系统前端402接收到请求之后可利用认证运行时间服务404来确定请求是否可信。如果请求可信，那么策略管理系统前端402可向策略引擎410提交策略评估请求，以便确定请求是否与可应用的现有策略相符。如果策略引擎410并未高速缓存此类信息，则其可与策略存储库412交互以便获得可应用的策略。例如，策略引擎410可访问用于与来自策略存储库412的请求相关联的账户的所有策略，并且从所访问的策略中识别可适用于请求的任何策略。如上所述，策略引擎可高速缓存策略，以便避免与可在来自策略引擎410的网络上实现的存储库412进行通信。

[0046] 对于某些类型的请求来说，策略管理系统前端402可与策略存储库412交互。例如，如果现有策略允许此类动作，那么策略管理系统前端402就可向策略存储库412传输新的策略，可向策略存储库412传输命令，以便(例如，通过修改现有策略)删除一个或多个策略，和/或通常更改策略集或与请求相关联的账户。

[0047] 如以上所指出，可以策略文档的形式编码由计算资源服务提供商的客户利用的各种策略。在一个实施方案中，策略文档是操作为一个或多个语句的容件的文档，即，所组织的信息的集合。策略文档可以是JavaScript对象标记(JSON)、可扩展标记语言(XML)文档、使用结构化标记语言的另一种文档或组织信息的其他方法。应注意，策略文档可编码由对应的语句定义的一个或多个策略。应注意，策略可包括一个或多个子策略。换言之，策略可包括策略的集合。例如，计算资源服务提供商的账户可具有用于数据存储服务的策略(“数据存储服务策略”)，所述用于数据存储服务的策略包括多个单一策略，每个单一策略限定特定的许可。另外地，应注意，术语“策略”可在不同的上下文中具有不同的意义。作为举例，当术语“策略”用作不可数(质量)名词时，而非当用作可数(计数)名词时可具有不同的意义。例如，诸如“策略是否允许实现请求”的短语可解释为意指单一策略的集合是否允许实现请求。同样地，尽管策略文档用于说明的目的，但是也可以根据各种实施方案使用编码策略的其他方法(例如，通过使用关系数据库的关系表来存储将由策略文档编码的各种信息)。语句可包括可以是关于语句的任何限制或细节的条件。例如，所述条件可指定用于待实行策略的情况。

[0048] 在各种实施方案中，策略能够定义用于更改策略集的条件，诸如用于计算资源服务提供商的账户的策略集的条件。关于策略添加的策略(其可称为“策略添加策略”)可能要求，为了是能够实现的，向策略集添加所提议的策略的请求必须被配置成使得所提议的策略将不会变得有效(即，由强制执行该策略集的系统强制执行)，直到将来某一时刻，诸如从某个时间参考点测量的在将来的指定小时数。关于策略添加的策略可定义策略所应用到的主体集、策略所应用到的资源、必须实现的一个或多个其他条件、以及除如果条件不能实现那么就拒绝(或者，如果条件可以实现那么就允许)之外的一个或多个动作。例如，由策略定义的其他动作可包括导致通知添加策略的请求的一个或多个主体的一个或多个动作。例如，策略管理员可允许一个或多个其他人向策略集添加策略，但可配置关于策略添加的策略以使得策略管理员可以在无所需延迟的情况下添加策略，但是只有添加策略以致于策略

在与所需延迟相符的情况下变得有效，所允许的一个或多个其他人才能够成功地添加策略。

[0049] 图5示出根据一个实施方案的策略文档的说明性实例。在一个实施方案中，策略文档500编码与由策略文档编码的策略有关的各种信息。策略可以陈述性访问控制策略语言来编码，如可扩展访问控制标记语言(XACML)、企业隐私授权语言(EPAL)、亚马逊网络服务访问策略语言、Microsoft SecPol或编码执行密码操作必须满足的一个或多个条件的任何合适的方式。如图5所示，策略文档500包括名称502，名称502可包括用于策略文档500的字符串。例如，名称502可用来以使用人可读的术语提供便利标识符。作为举例，名称502可以是对我的数据存储服务策略起作用的字符串。同样如图5中所示，策略文档500可包括版本504。由于各种请求被接收和实现以更新策略，因而版本504可用来追踪策略文档500如何随时间而发生更改。对策略文档500的每次更新可致使版本504被更新成新值。策略文档500还可包括发行人506，发行人506可以是用于用户的标识符，该用户提交导致产生具有当前版本的策略文档500的请求。

[0050] 如图5中所示及如上所述，策略文档500可包括一个或多个语句508。可使用逻辑OR处理策略文档中的语句。如下文更加详细地所述，一个或多个语句508可编码指示由策略文档500编码的策略何时有效的将来时间的信息。例如，语句可编码用于将来某一时刻的时间戳，在该时间戳处由策略文档500编码的策略将是有效的。语句可编码指示在策略文档500有效之前所必须经过的时间量的持续时间，其中所述持续时间可以从某个时间点进行测量，所述某个时间点可以是全球时间(例如，Unix时间)，或所述某个时间点可以从特定事件(诸如提交添加策略的请求，所述添加策略的请求包含策略管理系统对策略的同意的语句)进行测量。通常，语句可编码立刻或最终呈现可确定的将来时刻的任何信息，在该可确定的将来时刻处，由策略文档500编码的策略变得有效。应注意，语句可包含图中并未示出的其他信息，诸如唯一识别(至少在策略文档内的)语句的语句标识符，和可被策略管理系统使用的其他信息。

[0051] 图6示出根据各种实施方案的策略文档600的说明性实例。策略文档600可被配置成与上文结合图5所述的策略文档500相似。例如，如图6所示，策略文档600可包括名称602、版本604、发行人606和一个或多个语句608，诸如上文所述。然而，代替决定由策略文档600编码的策略何时变得有效的语句608(或除其之外)，策略文档600可包括除语句608之外的其他信息，并且具体地说包括有效性定时信息610。换言之，可将有效定时信息编码到策略文档的语句的内侧和/或外侧。如以上所指出，有效性定时信息610可以是从其可确定将来某一时刻的任何信息，在该将来某一时刻处由策略文档600编码的策略变得有效。上文论述了示例性有效性定时信息，诸如指示由策略文档600编码的策略何时有效的持续时间或时间点的值。

[0052] 如以上所指出，语句可以是对许可的形式描述。因此，图7示出语句700的说明性实例，可将语句700编码到策略文档中，诸如上文所述。如图7所示，语句700可包括识别一个或多个主体702的信息。主体可以是语句700应用到的实体(例如，用户、计算机系统或可被授予许可访问系统的任何实体)。作为举例，计算资源服务提供商的客户可具有账户。账户可与多个子账户相关联，每个子账户对应于客户的用户。每个用户可具有可包含于语句中作为主体的对应的标识符。也可以其他方式识别主体。例如，主体集可由该集的标识符识别。

作为说明性实例，组织中的部门可具有对应的标识符。语句可通过在语句中列出所述部门的标识符而适用于与所述部门相关联的用户。例如，当主体集动态地改变时，诸如当雇员被组织和/或其中的部门解雇、和/或被其留下时，用于主体集的标识符可能是有用的。主体的标识符也可以是开放的。例如，可包括指示语句700可适用于任何人的信息，也就是说，可适用于能够以计算资源服务提供商或通常所有用户的账户的名义提交请求的所有用户。

[0053] 如图7所示，语句700还可识别一个或多个资源704。资源可以是如上文所述的计算资源。例如，资源可以是由计算资源服务提供商提供的服务的对象。作为举例，资源可以是虚拟计算机系统，可以是用来将数据对象关联在一起的逻辑型数据容件，可以是块级数据存储装置的卷标识符、数据库、存储于数据库中的项目、数据对象(例如，文件)和通常可以被提供为服务的任何类型的资源。如同主体一样，资源可使用资源集的标识符进行描述。例如，在一些实施方案中，虚拟计算机系统能够与生成标签的用户相关联，所述标签可描述由虚拟计算机系统实现的角色。作为举例，一组虚拟计算机系统可与标签“网页服务器”相关联。因此，资源可由此类标签标识。作为另一个实例，资源可对应于逻辑型数据容件，从而致使语句700可应用存储在逻辑型数据容件内(即，与逻辑型数据容件相关联)的任何数据对象。

[0054] 如图7所示，语句700还可包括一个或多个条件。在一个实施方案中，所述条件决定在特定的上下文中是否应用策略文档中的语句，即，在条件被提交的上下文中应用到所提交的请求。所述条件可利用布尔算子(等于、小于等)以允许评估在语句(主体、资源等)中的其他值和在认证上下文中的其他值下的条件，其在评估策略的请求中可以或可以不提供。条件值可包括日期、时间、请求者的互联网协议(IP)地址、请求资源的标识符、用户名称、用户标识符和/或请求者和/或其他值的用户代理。值对条件所应用于的服务也可以是唯一的。条件可以是逻辑连接的，以用于使用逻辑连接器(诸如AND和OR)进行评估。

[0055] 语句也可编码一个或多个动作708。所编码的动作可表示当实现和/或不实现条件706时发生的操作。示例性动作包括允许实现请求(例如，允许所请求的访问)或拒绝请求。其他动作包括根据编码到语句700中的信息传输通知，诸如向在语句700中指定的一个或多个电子邮件地址传输电子邮件消息，向通知服务的主题发布通知和/或其他动作。因此，所编码的动作708可包括足以执行该动作的信息。

[0056] 应注意，本公开的各种实施方案以说明性的方式论述由策略文档定义的策略(即，由策略文档定义的一个或多个策略集)在与要求相符的将来某一日期变得有效的要求。换言之，本文所论述的说明性的实例涉及策略文档在将来某一时刻变得有效的要求。与本文论述的所有实施方案一样，变型被认为是在本公开的范围内。例如，每个语句可包括有效性定时信息，所述有效性定时信息可用来确定语句生效的将来时刻。在替代的关于延迟有效性的策略文档级要求中或除其之外，各种实施方案包括关于在语句级上定义的策略的要求。确定语句是否生效可包括确定(针对要求延迟的)每个语句是否与针对延迟的要求相符。策略文档中的不同语句可具有不同的延迟，并且关于策略更改/添加的现有策略可具有针对不同语句的不同延迟要求。

[0057] 图8示出根据实施方案的处理请求的过程的说明性实例。过程800可由任何合适的系统或其组件，诸如上文结合图3描述的服务300和/或结合图4描述的策略管理服务400来执行。在一个实施方案中，过程800包括接收802请求。例如，请求可被接收为对前端系统诸

如上文所描述的服务前端302或策略管理系统前端402的适当配置的API调用。例如，API调用可以是配置有可适用于请求的各种参数的网页服务调用的形式。在接收到802请求之后，过程800可包括确定804请求是否可信。确定804请求是否可信可以任何合适的方式来执行。例如，在一些实施方案中，请求可签署有电子签名。确定804请求是否可信可包括验证电子签名。电子签名的验证可由任何合适的系统或其组件完成。例如，参考上文所述的实施方案，认证运行时间服务或认证系统可执行所述验证。应注意，验证可由其他实体执行。例如，在一些实施方案中，验证并不以分布式方式进行，但通过诸如上文所述的前端系统完成。通常，可使用可确定认证请求的任何方式。

[0058] 如果确定804请求不可信，那么可拒绝806请求。可以任何合适的方式执行拒绝请求，诸如利用仅通过不采取动作指示拒绝的信息来对请求作出响应，和/或提供指示请求被拒绝的一个或多个原因的信息和/或对于寻找拒绝的理由可能所必需的另外的信息。然而，如果确定804请求可信，那么过程800可包括访问808一个或多个可应用的策略。可由任何合适的系统或其组件执行访问808可应用的策略，诸如由上文所描述的策略管理服务。例如，可通过从诸如上文所述的策略存储库检索策略文档来访问可应用的策略。在一些实施方案中，指示策略何时变得有效的定时信息用来从可应用的策略集(例如，在不考虑定时信息的情况下，将应用到请求的策略集)中选择策略的子集。所选择的子集可包括具有指示当前正在实行子集中的策略的定时信息的那些策略。

[0059] 随后，可做出810可应用的策略是否允许实现请求的确定。策略是否允许实现请求的确定810可由任何合适的系统执行，诸如由上文结合图4所描述的策略引擎410。确定策略是否允许实现请求的策略引擎或其他系统可分析可应用的策略，以便确定策略是否允许实现请求。如上文所述，分析所采用的方式可根据各种实施方案而变化。例如，可依序分析可应用的策略，或通常潜在的可应用策略。如果请求的实现将违背处于策略序列中的策略，那么可做出策略不允许实现请求的确定，而(如果有的话)无需分析序列的其余部分。此外，确定810策略是否允许实现请求可包括至少部分地基于在策略文档中编码的信息来确定策略文档当前是否有效或策略文档的强制执行是否正在被延迟。例如，可在定时信息在执行一个或多个先前操作期间不用来排除策略的实施方案中执行确定策略文档当前是否有效。

[0060] 也可执行更加复杂的处理。例如，如果策略文档中的语句指示请求的实现将违背语句中编码的策略，那么可做出任何其他策略是否取代该策略并允许实现请求的确定。通常，可以任何合适的方式分析策略，并且所述方式可根据被配置的各种系统和如何编码策略而变化。如果确定810策略不允许执行请求，那么过程800可诸如上所述包括拒绝806请求。然而，如果确定810策略允许实现请求，那么可实现812请求。

[0061] 如上文所指出，根据各种实施方案的请求可发生很大变化。因此，请求的实现可相应地发生变化。通常，请求的实现可包括配置一个或多个计算资源，提供提供访问数据，以及通常根据请求执行一个或多个动作。如上文所指出，本公开的各种实施方案应用于请求以添加或以其他方式更改策略。因此，图9示出过程900的说明性实例，所述过程900可用来强制执行与更改现有策略有关的策略。如图9所示，过程900包括接收902添加策略的请求。添加策略的请求可以是适当配置的API调用的形式。应注意，尽管图9论述了添加策略的请求，但是过程900可适于其他类型的请求，诸如更改现有策略的请求。在一个实施方案中，在接收到902添加策略的请求之后，可做出904诸如上文所述的请求是否可信的确定。如果确

定904请求不可信，那么可拒绝906添加策略的请求。请求的拒绝可诸如上文所述来执行。然而，如果确定904请求可信，那么过程900可诸如上文所述包括访问908可应用的策略。

[0062] 如图9所示，过程900包括检测910时间延迟要求。检测910时间延迟要求可根据多个实施方案以各种方式来执行。例如，尽管为了简化的目的从图9中被省略，尽管在图中未示出，但是过程900可包括处理所访问的可应用的策略和确定任何可应用的策略是否将阻止实现添加策略的请求。在此类处理期间，可检测具有时间延迟要求的策略。应注意，时间延迟要求不一定在存储有其他策略的策略中进行编码，但是系统可进行编码或以其他方式被配置来强制执行延迟，无需将此类要求编码到策略文档中。在未将时间延迟要求编码到用于账户的策略集中的此类实施方案中，应注意，可在访问908可应用的策略之前执行检测时间延迟要求。通常，应注意，尽管这里的图示出了以特定顺序发生的各种操作，但是在许多实例中，操作的顺序可不同于示出的顺序。此外，可以并不遵循严格顺序的方式执行操作，但是例如，可以并行的方式或至少部分并行的方式执行操作。

[0063] 回到图9中示出的特定实施方案，在检测到910时间延迟要求之后，可做出912所请求的策略添加是否与时间延迟要求相符的确定。可以任何合适的方式做出确定912，并且做出确定912的方式可根据编码关于策略的信息的方式发生变化。例如，在能够从策略文档中的语句确定待被添加的所请求策略的有效性的将来时刻的实施方案中，可评估所述语句以确定其是否与时间延迟要求相符。作为说明性实例，时间延迟要求可以是，只有当策略的生效日期是在将来的48小时才可添加策略。可分析在语句中编码的信息，以便确定添加策略的请求是否与要求相符。类似地，在策略文档的语句外侧编码有效性时间和信息的实施方案中，可相应地分析有效性时间和信息。例如，在有效性时间和信息包括指示请求待被添加的策略变得有效的时间的时间戳的实施方案中，可检查时间戳来确定时间戳相对于某个时间参考点(诸如，当接收到添加策略的请求时的时间)是否多于在将来的48个小时。通常，所请求的策略与时间延迟要求相符的确定912可根据多个实施方案以各种方式来执行，并且本公开并不限于这里明确描述的实施方案。

[0064] 如果确定所请求的策略添加与时间延迟要求不符，那么过程900就可以包括拒绝添加策略的请求并且诸如上文所述可以包括拒绝906添加策略的请求。然而，如果确定912所请求的策略添加实际上与时间延迟要求相符，那么过程900可如上文所述包括实现914请求。在各种实施方案中，当请求对策略进行某些更改时，可传输一个或多个通知。例如，用于客户或计算资源提供商的策略管理员可以接收指示尝试更改策略的电子邮件或其他电子消息。因此，在实施方案中的过程900包括启动916通知过程。可以任何合适的方式执行通知过程的启动，诸如通过致使诸如上文所述的通知系统向一个或多个实体发起一个或多个通知。

[0065] 通知过程可包括执行被配置来引起执行各种警报/通知动作的工作流。警报/通知动作可包括例如：引起通知系统(如上文所述)向一个或多个个体或系统传输一个或多个消息。例如，与账户(其与策略集相关联)相关联的组织的合规职员或策略管理员。作为另一个实例，警报/通知动作可包括引起审计系统执行增强的审计，在增强的审计中，例如收集更多与对系统的各种访问有关的信息。在一些实施方案中，警报/通知动作还可包括发警报信号，其可包括警报的可听和/或可见指示。其他警报动作被视为是在本公开的范围内。通知还可包括传输包括超链接(或其他机制)的消息，当所述消息被选择时，致使请求取消待被

传输至能够取消请求的系统(例如,策略管理系统)。在不经消息的接收端认证的情况下,消息可允许取消。也可使用使得请求通过通知能够被取消的其他方法。

[0066] 如上文本公开的各种实施方案所指出,强制执行用于策略的有效性的延迟,以便提供机会来消除此类策略的影响。因此,图10示出过程1000的示例性实例,所述过程1000可用来提供机会来取消如果不被取消将以其他方式生效的策略。过程1000可由任何合适的系统,诸如包括图2中的各种服务的系统和/或上文结合图4描述的策略管理服务400来执行。在一个实施方案中,过程1000包括接收1002添加在将来某一时刻处有效的策略的请求。可以任何合适的方式(诸如适当配置的API调用)接收添加在将来某一时刻处有效的策略的请求。可将有效时间编码在请求可被添加或可以其他方式被编码的策略中。例如,在一些实施方案中包括诸如上文所述的将来时刻或通常有效性定时信息,作为API调用中而不是处于策略文档本身内的参数。如上文所述,可做出请求是否可信的确定1004,并且如果确定1004请求不可信,那么过程1000可包括拒绝1006添加策略的请求。

[0067] 然而,如果确定1004请求可信,那么过程1000可包括确认1008现有策略通常是否允许策略添加。确认1008是否允许策略添加可以任何合适的方式执行,诸如通过执行上文所述的过程800和过程900的可应用的操作。应注意,尽管在图10中未示出,但是过程1000可包括拒绝1006添加策略的请求。如果不确定允许策略添加,那么在确定1008允许策略添加之后,可向策略存储库添加1010策略,并且如果策略是可应用的,那么诸如上文所述可发起通知。

[0068] 在向策略存储库添加策略之后的某个时间点,可接收1012请求以便诸如上文所述(例如,经由通知),或以其他方式(诸如通过登录到管理控制台并且使用对应的GUI来提交请求)取消策略添加。在接收到1012取消策略添加的请求之后,过程1000可诸如上文所述包括确定1014所添加的策略是否有效。例如,可分析在策略文档的语句中或语句外侧编码的有效性定时信息,以便确定是否已经经过足够的时间来允许策略变得有效,所述策略文档编码被添加到策略存储库的策略。如果确定1014添加策略并不是有效的,那么过程1000可包括确定1016放宽的取消条件集是否允许取消。放宽的条件可以比用于取消已经实行的策略的条件较不严格。例如,在所请求的策略添加/更改的通知提供用于取消策略添加的机制(例如,超链接)的实施方案中,可取消策略添加,而无需可能被已经实行的策略所需的另外的认证。类似地,与能够取消实行的策略的主体集相比,可允许更大的主体集以便取消用于尚未实行的策略的策略添加。作为另一个实例,策略更改可能需要相对于同意取消策略更改的主体而强制执行法定规章。用于尚未实行的添加策略的法定规章可以比用于已经实行的策略的法定规章较不严格。其他实例也被视为是在本公开的范围内。

[0069] 如果确定1016放宽的取消条件不允许取消,那么过程1000可以包括拒绝取消的请求并且可以包括拒绝1018取消的请求,并且如果策略尚未有效,并且还未接收到另一个取消请求或允许策略继续有效,那么从而允许策略变得有效。然而,如果确定1016放宽的取消条件集允许取消,那么过程1000可包括实现1020取消的请求。实现1020取消的请求可以简单的方式执行,诸如通过删除或以其他方式将策略从策略存储库移除或(例如,通过更新用于策略的元数据)将策略电子地标记为未实行。

[0070] 如果确定1014所添加的策略有效,那么可诸如上文所述作出1022更加严格的取消条件集是否允许取消的确定。如果确定1022更加严格的取消条件不允许取消,那么过程

1000可诸如上所述包括拒绝1018取消的请求。然而，如果确定1022更加严格的取消条件允许取消，那么过程1000可包括实现1020取消策略添加的请求。

[0071] 可鉴于以下条款对本公开的各个实施方案进行描述：

[0072] 1.一种用于管理策略的计算机实现的方法，其包括：

[0073] 在被配置有可执行指令的一个或多个计算机系统的控制下，

[0074] 存储包括策略添加策略的一个或多个策略集，所述策略添加策略指定包括针对强制执行所提议策略的延迟的要求的一个或多个条件；

[0075] 接收添加所提议策略的请求，所述策略添加策略可适用于所述提议的策略；

[0076] 至少部分地基于所提供的与所述请求有关的信息，确定所述提议的策略是否与所述要求相符；

[0077] 其中，由于确定所述提议的策略与所述要求相符，所述提议的策略根据所述要求而变得有效；以及

[0078] 其中，由于确定所述提议的策略不与所述要求相符，就拒绝所述请求。

[0079] 2.如条款1所述的计算机实现的方法，其中致使所述策略变得有效包括致使传输所述添加所述提议的策略的请求的一个或多个通知。

[0080] 3.如条款1或2所述的计算机实现的方法，其中致使所述提议的策略变得有效包括提供防止所述提议的策略在一个或多个要求集下变得有效的能力，所述一个或多个要求集比用于将策略从所述一个或多个策略集移除的另一个一个或多个要求集较不严格。

[0081] 4.如前述条款中任一项所述的计算机实现的方法，其中提供有所述请求的所述信息包括编码限定所述提议的策略的策略文档，所述策略文档编码可决定与所述要求相符的值。

[0082] 5.如前述条款中任一项所述的计算机实现的方法，其中：

[0083] 所述请求是具有应用程序编程接口参数集的应用程序编程接口调用；

[0084] 提供有所述请求的所述信息是来自所述应用程序编程接口参数集的参数。

[0085] 6.如前述条款中任一项所述的计算机实现的方法，其中：

[0086] 所述一个或多个策略集应用于以计算资源服务提供商的客户的名义管理的计算资源集；以及

[0087] 存储所述一个或多个策略包括存储具有所述计算资源服务提供商的其他客户的一个或多个策略的其他集的所述一个或多个策略集。

[0088] 7.如前述条款中任一项所述的计算机实现的方法，其中：

[0089] 所述提议的策略包括指示所述提议的策略何时变得有效的时间的值；并且

[0090] 所述方法还包括：

[0091] 向所述一个或多个策略集添加所述提议的策略；

[0092] 接收所述提议的策略应用到的第二请求；

[0093] 至少部分地基于所述指示的时间，在确定是否实现所述请求时确定是否使用所述提议的策略；

[0094] 在与所述确定一致的情况下，评估是否实现所述第二请求。

[0095] 8.一种用于管理策略的计算机实现的方法，其包括：

[0096] 在被配置有可执行指令的一个或多个计算机系统的控制下，

[0097] 接收针对更改一个或多个策略集的请求；

[0098] 至少部分地基于所述请求，确定所述请求的更改是否满足用于在将来变得有效的一个或多个要求；以及

[0099] 由于确定所述请求的更改满足所述一个或多个要求，根据所述要求使所述更改变得有效。

[0100] 9.如条款8所述的计算机实现的方法，其中所述更改是向所述一个或多个策略集添加策略。

[0101] 10.如条款8或9所述的计算机实现的方法，其中所述要求是来自所述一个或多个策略集的结果。

[0102] 11.如条款8至10中任一项所述的计算机实现的方法，其还包括致使传输所述请求的一个或多个通知。

[0103] 12.如条款8至11中任一项所述的计算机实现的方法，其还包括：

[0104] 在所述更改变得有效之前接收取消所述更改的请求；以及

[0105] 由于接收取消所述更改的所述请求，禁止所述更改变得有效。

[0106] 13.如条款8至12中任一项所述的计算机实现的方法，其中确定所述请求的更改是否满足所述一个或多个要求包括确定编码提议的策略是否包括指示与所述一个或多个请求一致的强制执行延迟的参数。

[0107] 14.一种系统，其包括：

[0108] 前端子系统，其被配置来接收更改策略的请求；

[0109] 策略管理子系统，其被配置来在接收到针对通过前端子系统而更改策略的请求之后：

[0110] 至少部分地基于所述请求，从所述前端子系统接收信息；

[0111] 至少部分地基于所述接收的信息，确定所述请求的更改是否与针对所述更改的延迟有效性的一个或多个要求相符；

[0112] 由于确定所述请求的更改与所述一个或多个要求相符，使所述请求的更改变得有效。

[0113] 15.如条款14所述的系统，其中所述请求是网页服务请求。

[0114] 16.如条款14或15所述的系统，其中所述信息是编码所提议的策略。

[0115] 17.如条款14至16中任一项所述的系统，其还包括通知系统，所述通知系统由于接收到所述请求而被配置来传输一个或多个通知。

[0116] 18.如条款14至17中任一项所述的计算机实现的方法，其中所述策略管理子系统在接收到第二请求之后，还被配置来：

[0117] 从策略集选择编码指示当前正在实行的有效时间的策略的子集；以及

[0118] 至少部分地基于所述选择的策略集，提供确定是否实现所述第二请求。

[0119] 19.如条款14至18中任一项所述的系统，其中所述要求是由所述系统强制执行的现有策略的结果。

[0120] 20.如条款14至19中任一项所述的系统，其中所述策略管理子系统还被配置来能够取消变得有效的所述请求的更改。

[0121] 21.一种或多种计算机可读存储介质，其具有共同地存储在其上的指令，当由系统

的一个或多个处理器执行时，所述指令致使所述计算机系统：

[0122] 管理用于访问以实体的名义访问计算资源的策略集；

[0123] 接收针对更改所述策略集的请求；以及

[0124] 处理所述请求，这样使得根据针对用于策略更改的延迟有效性的一个或多个要求，在所述更改变得有效一定时间量之前是可取消的。

[0125] 22.如条款21所述的一种或多种计算机可读存储介质，其中所述指令进一步致使所述系统使得传输关于所述更改的一个或多个通知。

[0126] 23.如条款22所述的一种或多种计算机可读存储介质，其中传输所述一个或多个通知包括向指定为有权取消所述更改的实体传输通知。

[0127] 24.如条款21至23中任一项所述的一种或多种计算机可读存储介质，其中在所述更改变得有效之前，依据一个或多个要求取消所述更改，所述一个或多个要求比在所述更改变得有效之后有效的其他要求较不严格。

[0128] 25.如条款21至24中任一项所述的一种或多种计算机可读存储介质，其中针对所述更改的所述请求包括编码新策略，所述新策略包括指示用于待变得有效的所述新策略的所提议延迟的信息。

[0129] 26.如条款21至25中任一项所述的一种或多种计算机可读存储介质，其中处理所述请求包括根据针对用于策略更改的延迟有效性的所述一个或多个要求，由于所述请求缺乏指示延迟的信息而拒绝所述请求。

[0130] 与本文论述的所有过程一样，变型被认为是在本公开的范围内。例如，如图10所示，一旦确定策略与任何时间延迟要求相符，就可向策略存储库添加所述策略，甚至当所述策略尚未有效时也可添加。本公开的变型包括系统通过延迟向策略存储库添加策略直到所述强制执行的延迟已经发生来强制执行时间延迟要求的实施方案。以此方式，处理策略以确定是否实现各种请求可以进行执行，而无需确定可应用的策略是否已经变得有效。其他变型也被视为是在本公开的范围内。

[0131] 图11示出用于实现根据各个实施方案的各方面的示例性环境1100的各方面。如将了解，尽管出于解释目的使用基于网页的环境，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1102，电子客户端装置1102可包括可操作来在适当网络1104上发送和接收请求、消息或信息并且将信息传送回装置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、手持消息接发装置，笔记本计算机、平板计算机、机顶盒，个人数据助理、嵌入计算机系统、电子书阅读器等。网络可包括任何适当网络，包括内部网、互联网、蜂窝网、局域网或任何其他此类网络或上述网络的组合。此类系统所用的组件可以至少部分地取决于所选网络和/或环境的类型。用于通过此类网络通信的协议和组件是众所周知的，因而本文不再详细论述。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页服务器1106，然而对于其他网络来说，可使用服务类似目的的替代装置，如本领域技术人员所显而易见的。

[0132] 所示出的环境包括至少一个应用程序服务器1108和数据存储器1110。应当理解，可以存在可以链接起来或以其它方式来配置的若干应用程序服务器、层或其它元件、过程或组件，这些应用程序服务器、层或其它元件、过程或组件可交互来执行如从适合的数据存

储器获取数据的任务。如本文所使用的服务器可以各种方式实现，诸如硬件装置或虚拟计算机系统。在一些上下文中，服务器可以指代在计算机系统上执行的编程序模块。如本文所使用的，术语“数据存储器”指代能够存储、访问和检索数据的任何装置或装置组合，所述装置的装置组合可包括任何标准、分布式或集群式环境中的任何组合和任何数目的数据服务器、数据库、数据存储装置和数据存储介质。应用程序服务器可包括任何适当硬件和软件，所述硬件和软件视执行客户端装置的一个或多个应用程序的各方面的需要而与数据存储器集成、处置应用程序的一些(甚至大多数)数据访问和业务逻辑。应用程序服务器可提供与数据存储器协作的存取控制服务，并且能够生成将要传送到用户的内容、如文本、图片、音频和/或视频，在这个实例中，所述内容可以超文本标记语言(“HTML”)、可扩展标记语言(“XML”)或另一种适当结构化语言的形式由网页服务器向用户提供。所有请求和响应的处置以及客户端装置1102与应用程序服务器1108之间的内容递送可由网页服务器来处置。应当理解，网页服务器和应用程序服务器不是必要的，且仅仅是示例性组件，因为本文所论述的结构化代码可在如本文其他地方所论述的任何适当装置或主机上执行。此外，除非上下文中另外清楚地指出，否则本文描述为由单个装置执行的操作可以由可形成分布式系统的多个装置共同地地执行。

[0133] 数据存储器1110可包括若干单独的数据表、数据库或其他数据存储机构和介质，用来存储与本公开的特定方面相关的数据。例如，所示出的数据存储器可包括用于存储生成数据1112和用户信息1116的机构，生成数据1112和用户信息1116可用于提供用于生成端的内容。数据存储器还被示出为包括用于存储日志数据1114的机构，所述日志数据1114可用于报告、分析或其他此类目的。应当理解，可能存在可能需要存储在数据存储器中的许多其他方面，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所列机构中的任何机构中或存储在数据存储器1110中的另外机构中。数据存储器1110可通过与它关联的逻辑来操作，以便从应用程序服务器1108接收指令，并且响应于所述指令而获取、更新或以其他方式处理数据。在一个实例中，用户可以通过由用户操作的装置针对某种类型的项目提交搜索请求。在此状况下，数据存储器可能访问用户信息来验证用户的身份，并且可访问目录详细信息以获取有关所述类型的项目的信息。随后，可将信息诸如以网页上的结果列表的形式返回给用户，用户能够经由用户装置1102上的浏览器来查看所述网页。可在浏览器的专用页面或窗口中查看到感兴趣的特定项目的信息。然而，应该指出，本公开的实施方案不一定限于网页的上下文，但一般而言，可以是通常更适用于处理请求，其中所述请求不一定是针对内容的请求。

[0134] 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)，当由服务器的处理器执行时，所述指令允许服务器实行其期望的功能。操作系统的适合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，尤其是根据本文中的公开来实现。

[0135] 在一个实施方案中，环境是利用通过通信链路、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组件的分布式计算环境。然而，本领域普通技术人员应理解，这种系统可在具有比图11所示的组件更少或更多组件的系统中同样顺利地操作。因此，图11中的系统1100的描绘本质上应视为说明性的，并且不限制本公开的范围。

[0136] 各种实施方案可进一步在广泛范围的操作环境中实现，在一些情况下，所述环境可包括一个或多个用户计算机、计算装置或可用于操作多个应用程序中的任一个的处理装置。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、膝上计算机或平板计算机，以及运行移动软件并且能够支持多个网络连接协议和消息传递协议的蜂窝装置、无线装置和手持式装置。这种系统还可包括多个工作站，所述工作站运行各种可商购得的操作系统和用于诸如开发和数据库管理等目的的其他已知应用程序中的任一个。这些装置还可包括其他电子装置，如虚拟终端、薄型客户端、游戏系统和能够经由网络通信的其他装置。

[0137] 本公开的各种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各种各样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”)、在开放系统互连(“OSI”)模型的各个层级中操作的协议、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、外联网、公共交换电话网、红外网络、无线网络以及上述网络的任何组合。

[0138] 在利用网页服务器的实施方案中，网页服务器可以运行各种各样服务器或中间层应用程序中的任一种，包括超文本传输协议(“HTTP”)服务器、FTP服务器、公共网关接口(“CGI”)服务器、数据服务器、Java服务器和业务应用程序服务器。服务器还能够响应来自用户装置的请求而执行程序或脚本，诸如通过执行可以实施为以任何编程语言(诸如Java®、C、C#或C++)或任何脚本语言(诸如Perl、Python或TCL)以及其组合写成的一个或多个脚本或程序的一个或多个网页应用程序。所述服务器还可以包括数据库服务器，包括但不限于那些可商购的Oracle®、Microsoft®、Sybase®和IBM®。

[0139] 环境可包括如上文所论述的各种各样数据存储区以及其他存储器和存储介质。这些可驻留在各种各样位置，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或所有计算机。在实施方案的特定集中，信息可驻留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的文件可视情况本地或远程存储。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经由总线电耦合的硬件元件，所述元件包括例如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)和至少一个输出装置(例如，显示装置、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、光存储装置和如随机存取存储器(“RAM”)或只读存储器(“ROM”)的固态存储装置、以及可移动媒体装置、存储卡、闪存卡等。

[0140] 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、网卡(无线或有线)、红外线通信装置等)和工作存储器，如上文所论述。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被配置来接收计算机可读存储介质，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程序、模块、服务系统或其他元件，包括操作系统和应用程序，如客户端应用程序或网络浏览器。应当了解，替代实施方案可具有与上述实施方案不

同的众多变型。例如，也可使用定制硬件，和/或特定元件可以在硬件、软件(包括可移植软件，如小程序)或两者中实现。此外，可以采用与如网络输入/输出装置的其他计算装置的连接。

[0141] 用于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，诸如但不限于以用于存储和/或传输信息(如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术所实现的易失性和非易失性、可移动和不可移动的介质，包括RAM、ROM、电可擦可编程只读存储器(“EEPROM”)、闪存或其他存储器技术、只读光盘驱动器(“CD-ROM”)、数字通用光盘(DVD)或其他光学存储器、磁盒、磁带、磁盘存储装置或其他磁性存储装置，或可用于存储所需信息且可由系统装置访问的任何其他介质。基于本文所提供的公开内容和教导，本技术领域普通技术人员将了解实现各种实施方案的其他方式和/或方法。

[0142] 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。

[0143] 其他变型也在本公开的精神内。因此，尽管所公开的技术可容许各种修改和替代构造，但在附图中已示出并且在上文中详细描述所示的其特定实施方案。然而，应当了解，并不旨在将本发明限制于所公开的一种或多种具体形式，相反地，旨在涵盖落在如所附权利要求书限定的本发明的精神和范围内的所有修改、替代构造和等效物。

[0144] 在描述所公开实施方案的上下文中(尤其是在以下权利要求书的上下文中)，术语“一个(a，an)”和“所述”以及类似指称对象的使用应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。当术语“连接的”非经修改并且指代物理连接时，应解释为部分地或全部地纳入在以下解释内：附接至或结合在一起，即使存在介入物。除非本文另外指明，否则本文中值范围的列举仅仅意图用作个别地表示属于所述范围的各单独值的速记方法，并且犹如本文个别描述地那样将各单独值并入到本说明书中。除非本文另外指明或与上下文矛盾，否则术语“集”(例如，“项目集”)或“子集”解释为包括一个或多个成员的非空集合。此外，除非本文另外指明或与上下文矛盾，否则术语对应集的“子集”不一定指对应集的真子集，但可子集和对应集可以相等。

[0145] 连接性语言，诸如除非本文另外特别指明或明显地与上下文矛盾，否则如一般情况下使用的，“A、B和C中的至少一个”形式的或“A、B和C中的至少一个”的短语另外与上下文一起理解来表示一个物品、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，在具有上文连接性短语中所使用的三个成员的集合的说明性实例中，“A、B和C中的至少一个”和“A、B和C中的至少一个”指代以下集合中的任意一个：{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。

[0146] 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)可在配置有可执行指令的一个或多个计算机系统的控制下实行，并且可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程序)、由硬件或其组合来实施。代

码可以例如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存储在计算机可读储存介质上。计算机可读储存介质可以是非暂时性的。

[0147] 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。本说明书中的语言不应解释为将任何非要求的要素指示为实践本发明所必需。

[0148] 本文中描述了本公开的优选实施方案,包括发明人已知用于执行本发明的最佳模式。阅读上述说明后,那些优选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特别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。

[0149] 本文所引用的所有参考文献、包括出版物、专利申请和专利据此以引用方式并入,其程度等同于每个参考文献单独地且具体地被表示为以引用方式并入本文并且以其全文在本文得以陈述。

图1

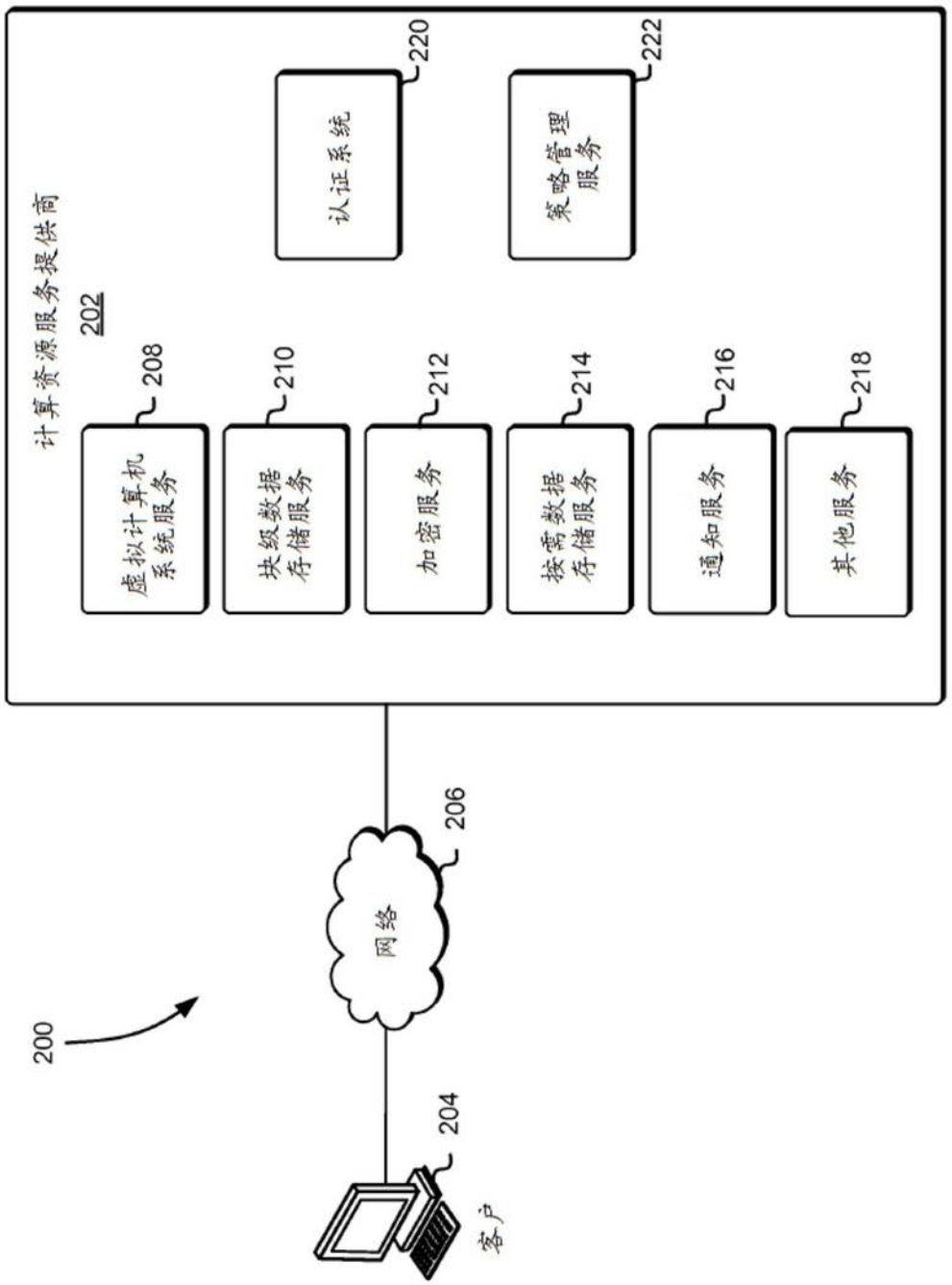
计算资源服务提供商
202
虚拟计算机系统服务
208
块级数据存储服务
210
加密服务
212
按需数据存储服务
214
通知服务
216
其他服务
218
认证系统
220
策略管理服务
222
网络
206
200
204
客户

图2

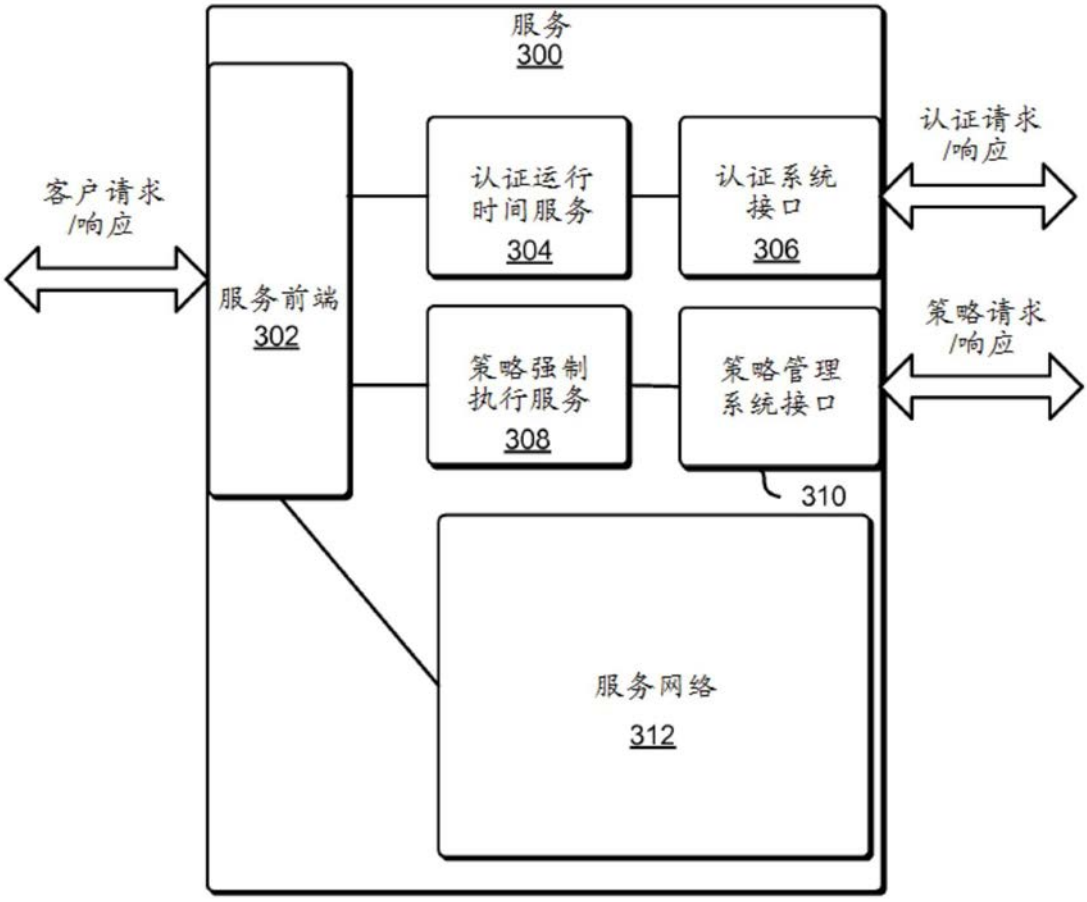
服务
300
客户请求
/响应
服务前端
302
认证运行
时间服务
304
认证系统
接口
306
认证请求
/响应
策略强制
执行服务
308
策略管理
系统接口
策略请求
/响应
310
服务网络
312

图3

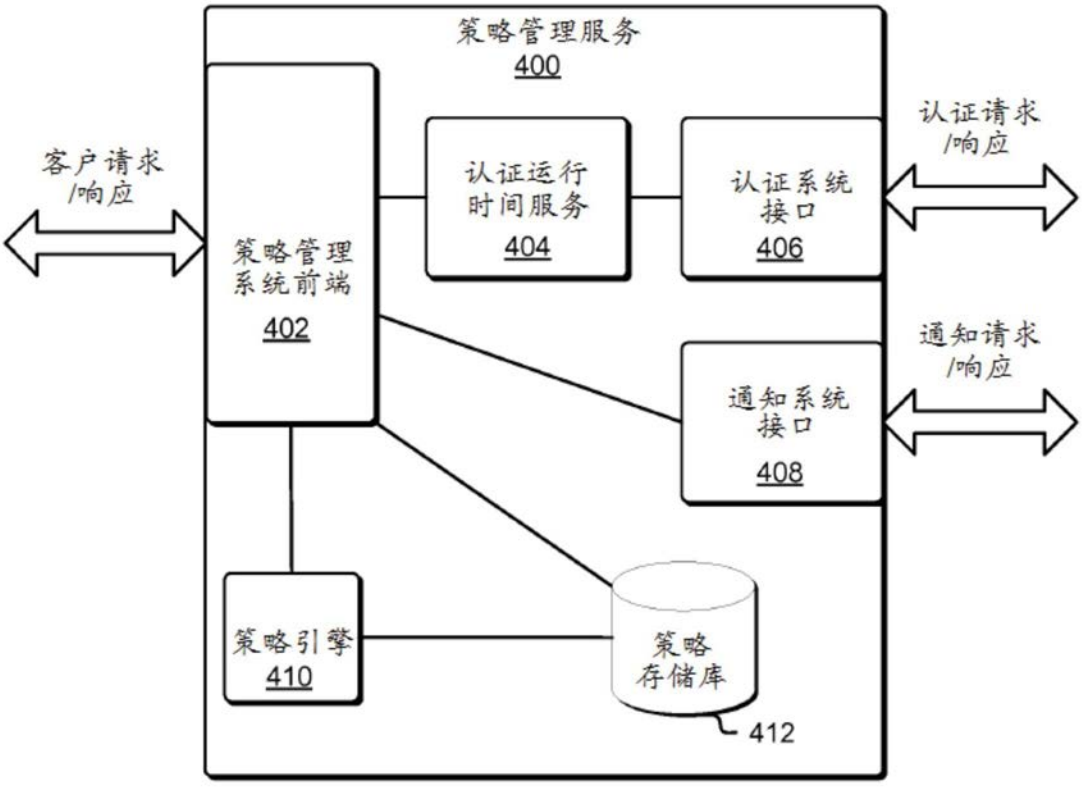
策略管理服务
400
客户请求
/响应
策略管理
系统前端
402
认证运行
时间服务
404
认证系统
接口
406
认证请求
/响应
通知系统
接口
408
通知请求
/响应
策略引擎
410
策略
存储库
412

图4

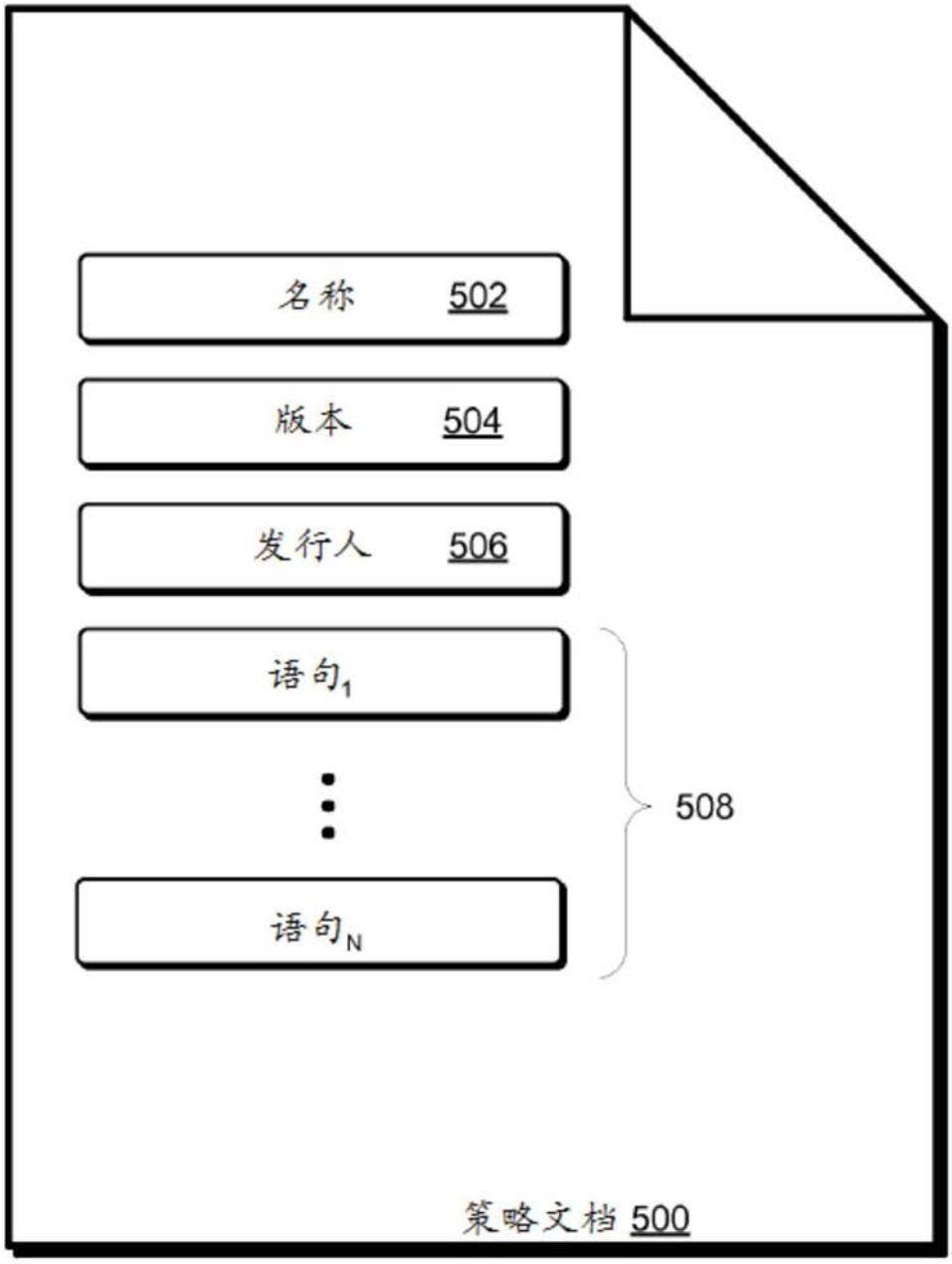

图5

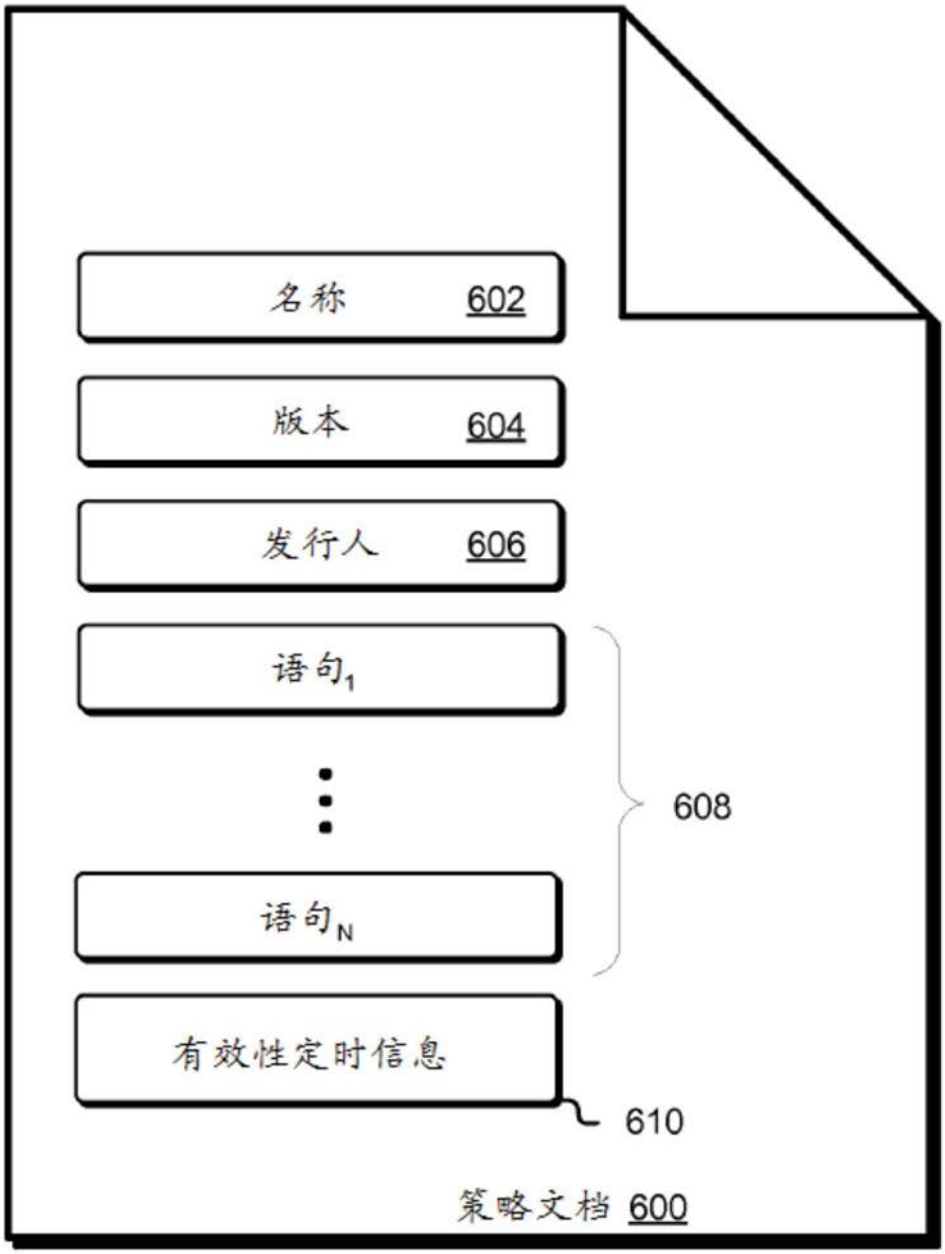

图6

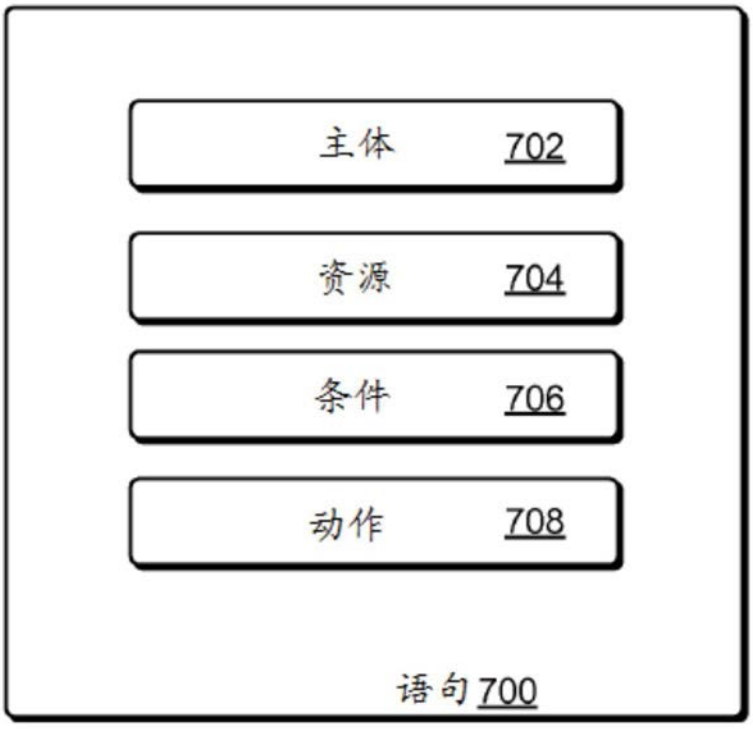

图7

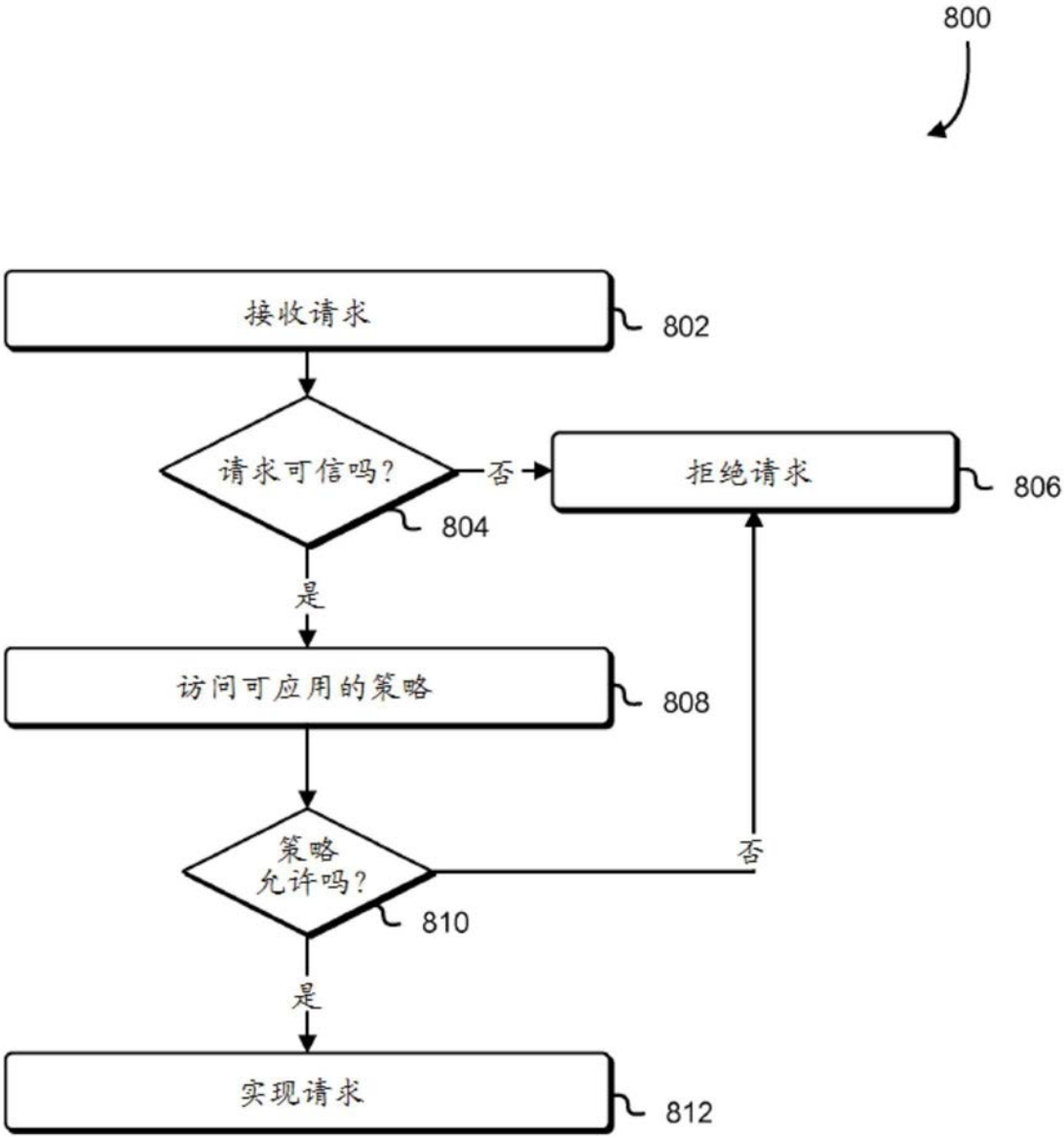
800
接收请求
802
请求可信吗?
804
否
拒绝请求
806
是
访问可应用的策略
808
策略
允许吗?
810
否
是
实现请求
812

图8

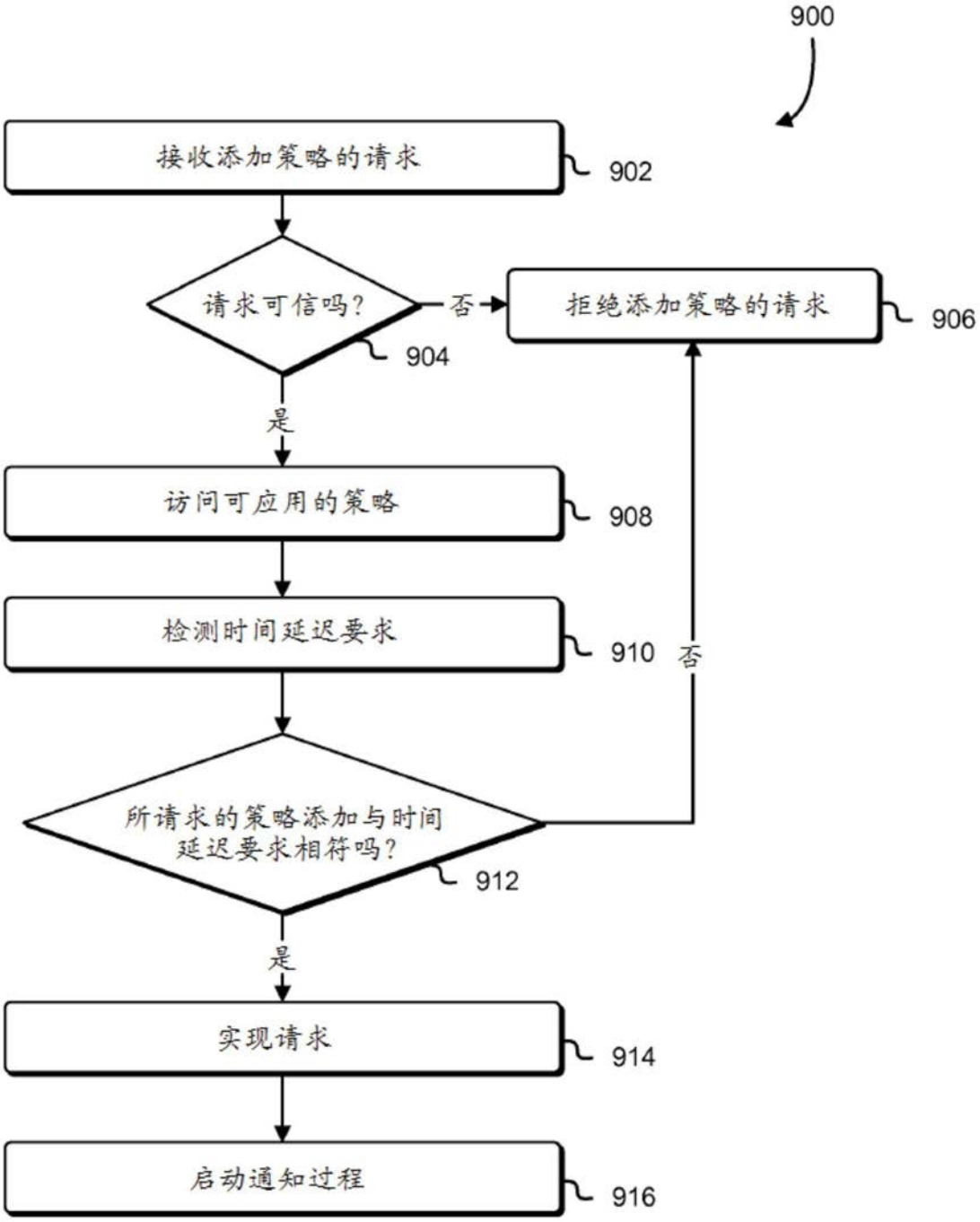
900
接收添加策略的请求
902
请求可信吗?
904
否
拒绝添加策略的请求
906
是
访问可应用的策略
908
检测时间延迟要求
910
否
所请求的策略添加与时间延迟要求相符吗?
912
是
实现请求
914
启动通知过程
916

图9

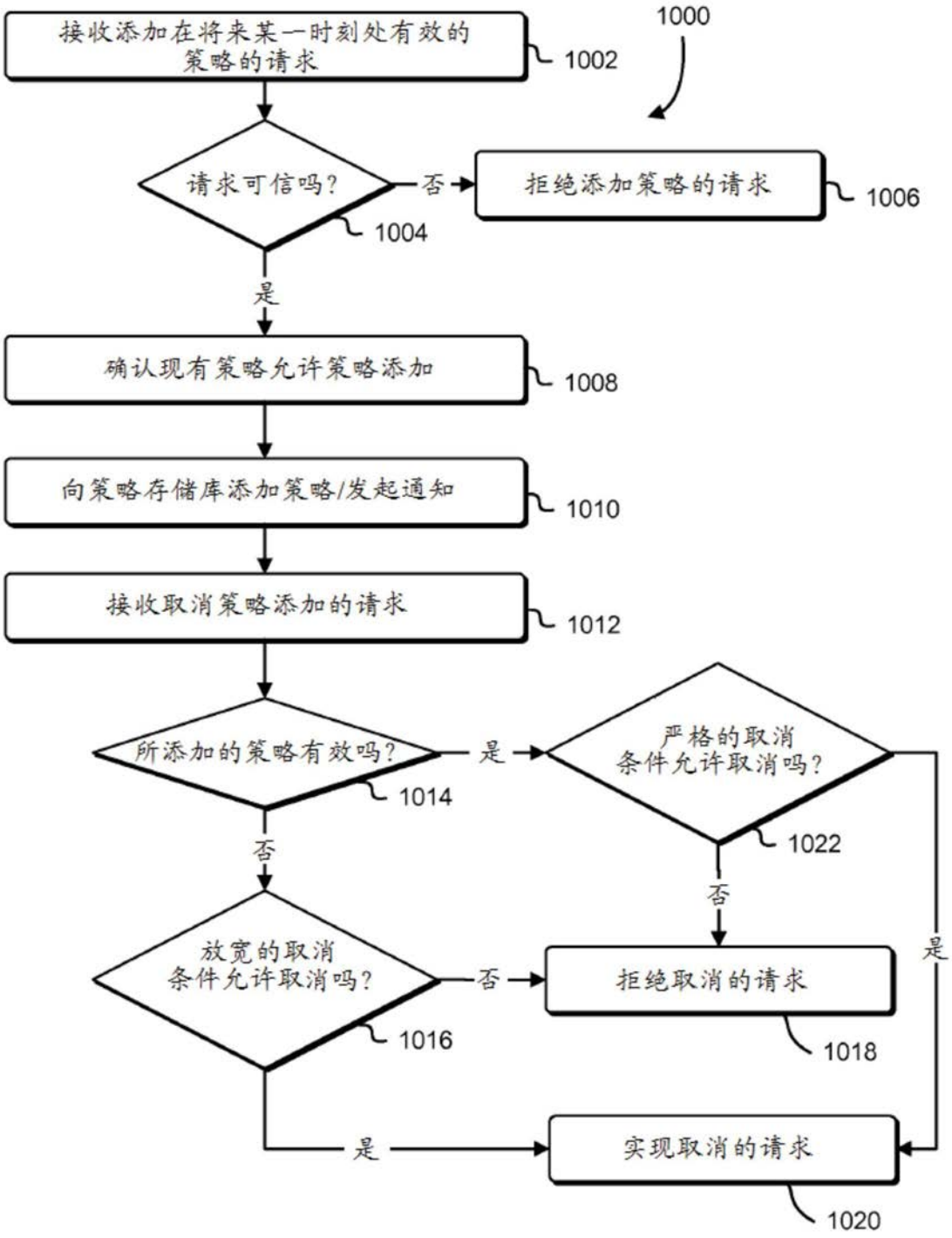
1000
接收添加在将来某一时刻处有效的策略的请求
1002
请求可信吗?
1004
否
拒绝添加策略的请求
1006
是
确认现有策略允许策略添加
1008
向策略存储库添加策略/发起通知
1010
接收取消策略添加的请求
1012
所添加的策略有效吗?
1014
是
严格的取消条件允许取消吗?
1022
否
放宽的取消条件允许取消吗?
1016
否
拒绝取消的请求
1018
是
是
实现取消的请求
1020

图10

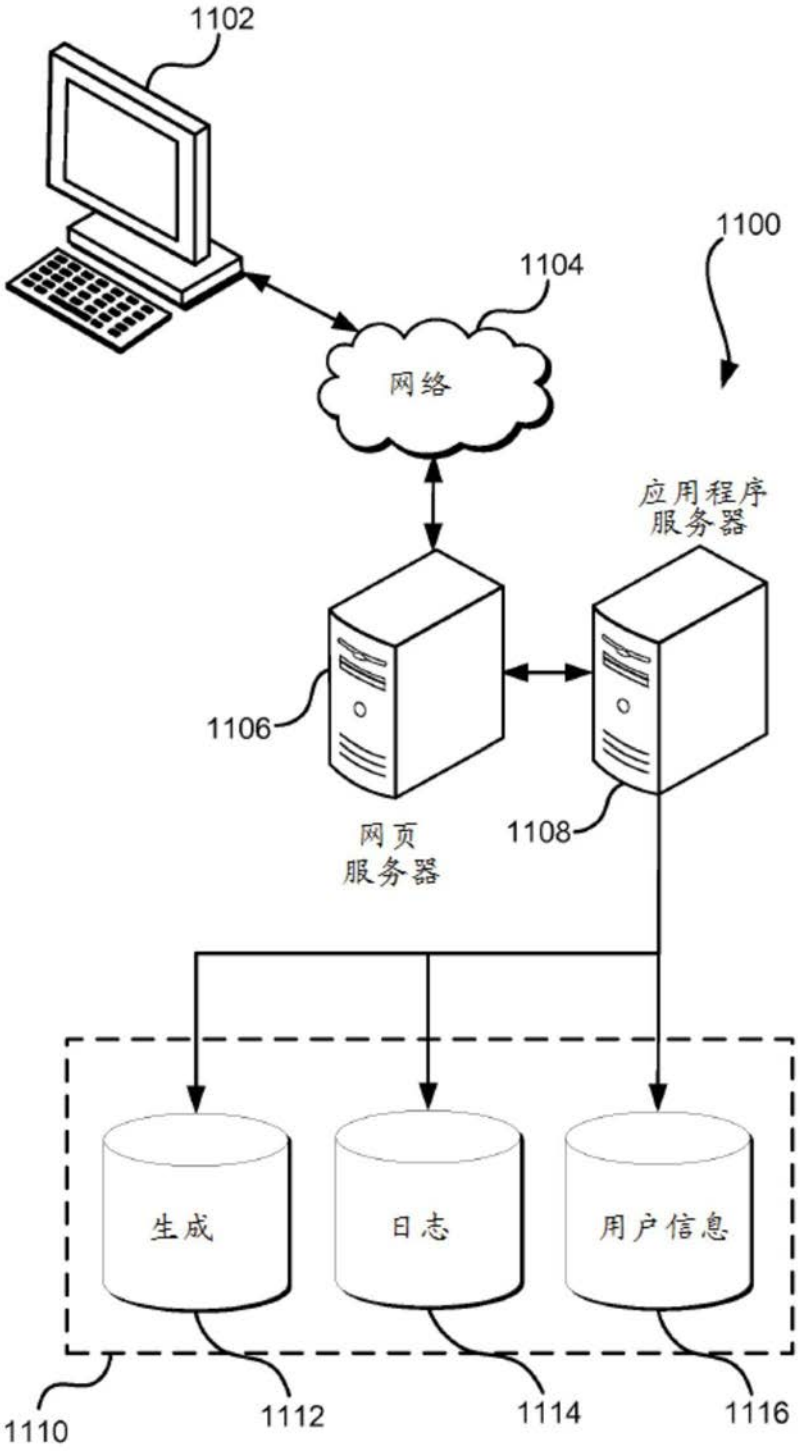
1102
1100
1104
网络
应用程序
服务器
1106
网页
服务器
1108
生成
日志
用户信息
1110
1112
1114
1116

图11