[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 9/44 (2006.01)
G06F 9/46 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200480019392.0

[43] 公开日 2006 年 8 月 16 日

[11] 公开号 CN 1820249A

[22] 申请日 2004.7.9
[21] 申请号 200480019392.0
[30] 优先权
[32] 2003.7.17 [33] US [31] 10/621,935
[86] 国际申请 PCT/EP2004/051434 2004.7.9
[87] 国际公布 WO2005/015387 英 2005.2.17
[85] 进入国家阶段日期 2006.1.6
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 保罗·安东尼·阿什利
斯里德哈·马皮迪
马克·范登沃维尔

[74] 专利代理机构 北京市金杜律师事务所
代理人 酆 迅

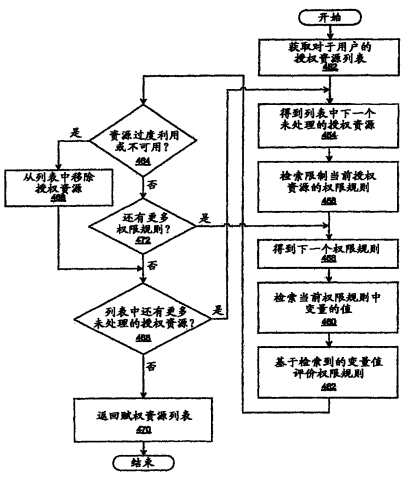
权利要求书 3 页 说明书 15 页 附图 7 页

[54] 发明名称

分布式数据处理环境中的权限自动调整的方法和系统

[57] 摘要

示出了用于在分布式数据处理系统中限制对资源集合的访问的方法、系统及计算机程序产品。服务器确定授权用户访问的授权资源集合；授权资源集合是在分布式数据处理系统中可操作的资源集合的子集。基于与授权资源集合有关的状况信息做出与授权资源集合的可用性有关的评价。然后生成对于用户的赋权资源集合的列表；赋权资源集合是授权资源集合的子集。可以将赋权资源集合的指示发送给用户，之后系统将响应用户访问赋权资源集合的请求。



1. 一种用于在分布式数据处理系统中限制对资源集合的访问的方法，该方法包括：确定授权用户访问的授权资源集合，其中该授权资源集合是该资源集合的子集；获得与该授权资源集合有关的状况信息；基于与该授权资源集合有关的该状况信息评价该授权资源集合的可用性；以及响应于该授权资源集合的可用性评价，生成对于该用户的赋权资源集合列表，其中该赋权资源集合是该授权资源集合的子集。

2. 如权利要求 1 所述的方法，进一步包括：向该用户发送该赋权资源集合的指示。

3. 如权利要求 1 或 2 所述的方法，进一步包括：响应该用户访问该赋权资源集合的请求。

4. 如权利要求 1、2 或 3 所述的方法，进一步包括：防止该用户访问在该授权资源集合中但是不在该赋权资源集合中的资源。

5. 如权利要求 1 至 4 中任一所述的方法，进一步包括：在评价该授权资源集合的可用性时考虑该用户的用户属性。

6. 如权利要求 1 至 5 中任一所述的方法，进一步包括：根据与该授权资源集合中一个或多个资源相关联的可配置规则执行该授权资源集合的可用性评价。

7. 如权利要求 1 至 6 中任一所述的方法，进一步包括：使用分布式监控应用收集对于该资源集合的状况信息。

8. 一种用于在分布式数据处理系统中限制对资源集合的访问的装置，该装置包括：用于确定授权用户访问的授权资源集合的装置，其中该授权资源集合是该资源集合的子集；用于获取与该授权资源集合有关的状况信息的装置；用于基于与该授权资源集合有关的该状况信息评价该授权资源集合的可用性的装置；以及用于响应于该授权资源集合的可用性评价生成对于该用户的赋权资源集合列表的装置，其中该赋权资源集合是该授权资源集合的子集。

9. 如权利要求 8 所述的装置，进一步包括：用于向该用户发送该

赋权资源集合的指示的装置。

10. 如权利要求 8 或 9 所述的装置，进一步包括：用于响应该用户访问该赋权资源集合的请求的装置。

11. 如权利要求 8、9 或 10 所述的装置，进一步包括：用于防止该用户访问在该授权资源集合中但是不在该赋权资源集合中的资源的装置。

12. 如权利要求 8、9 或 11 所述的装置，进一步包括：用于在评价该授权资源集合的可用性时考虑该用户的用户属性的装置。

13. 如权利要求 8 至 12 中任一所述的装置，进一步包括：用于根据与该授权资源集合中一个或多个资源相关联的可配置规则执行该授权资源集合的可用性评价的装置。

14. 如权利要求 8 至 13 中任一所述的装置，进一步包括：用于使用分布式监控应用收集对于该资源集合的状况信息的装置。

15. 一种在分布式数据处理系统中使用的、用于限制对资源集合的访问的计算机可读介质中的计算机程序产品，该计算机程序产品包括：用于确定授权用户访问的授权资源集合的装置，其中该授权资源集合是该资源集合的子集；用于获取与该授权资源集合有关的状况信息的装置；用于基于与该授权资源集合有关的该状况信息评价该授权资源集合的可用性的装置；以及用于响应于该授权资源集合的可用性评价生成对于该用户的赋权资源集合列表的装置，其中该赋权资源集合是该授权资源集合的子集。

16. 如权利要求 15 所述的计算机程序产品，进一步包括：用于向该用户发送该赋权资源集合的指示的装置。

17. 如权利要求 15 或 16 所述的计算机程序产品，进一步包括：用于响应该用户访问该赋权资源集合的请求的装置。

18. 如权利要求 15、16 或 17 所述的计算机程序产品，进一步包括：用于防止该用户访问在该授权资源集合中但是不在该赋权资源集合中的资源的装置。

19. 如权利要求 15 至 18 中任一所述的计算机程序产品，进一步包

括：用于在评价该授权资源集合的可用性时考虑该用户的用户属性的装置。

20. 如权利要求 15 至 19 中任一所述的计算机程序产品，进一步包括：用于根据与该授权资源集合中一个或多个资源相关联的可配置规则执行该授权资源集合的可用性评价的装置。

21. 如权利要求 15 至 20 中任一所述的计算机程序产品，进一步包括：用于使用分布式监控应用收集对于该资源集合的状况信息的装置。

分布式数据处理环境中的权限自动调整的方法和系统

技术领域

本发明涉及改进的数据处理系统，特别涉及用于多计算机数据传送的方法和装置。更特别地，本发明提供用于多计算机分布式资源管理的方法和装置。

背景技术

用户向机构进行注册，以便获取对由该机构提供的在线应用的访问，例如代表用户通过计算机网络执行事务处理的网络应用和电子商务网站。用户与权限集合相关联，这些权限是使得用户能够访问某些应用、账户、或其它受控的资源的属性。例如，用户可以被注册来使用在线经纪应用，并且此后，可以认为该用户具有该在线经纪应用的权限。该用户还可以具有与该在线经纪应用有关的其它权限，例如访问实时股票行情。

当用户试图访问机构的在线站点时，该用户需要完成验证操作。如果用户成功验证，则基于该用户的权限，向用户示出该用户可以访问的应用或其它受控的资源的列表。产生权限数据的权限引擎通常接收来自多个资源的输入数据，以便为用户创建权限列表，例如用户注册、机构的各种验证策略、及第三方源数据。

然而，当前的权限系统并不考虑与其操作的计算环境的实时状态有关的信息，这样会对这些系统的用户产生不一致的性能。例如，应用可能由于故障、由于维护、或由于已经到达容量限制而不可用。由于权限系统不知道应用的状态，所以该权限系统可以向用户显示出与访问这些应用或其它资源有关的信息，例如，网页中的超链接，即使这些资源可能是不可用的。如果用户接着试图访问已经被提供但是不可用或已经满

负荷的资源，则该用户可能经历可用性问题，这样给用户留下该机构的计算机系统（例如它的网站）不健壮的印象。

因此，具有一种能够自动地调整用户权限使得用户不经历性能问题和不一致结果的方法和系统将是有利的。

发明内容

示出了用于在分布式数据处理系统中限制对资源集合的访问的方法、系统及计算机程序产品。服务器确定授权用户访问的授权资源（authorized resource）集合；授权资源集合是在分布式数据处理系统中可操作的资源集合的子集。基于与授权资源集合有关的状况信息做出与授权资源集合的可用性有关的评价。然后生成对于用户的赋权资源（entitled resource）集合的列表；赋权资源集合是授权资源集合的子集。可以将赋权资源集合的指示发送给用户，之后系统将响应用户访问赋权资源集合的请求。

附图说明

认为本发明特有的新颖特征在所附权利要求书中进行了阐述。通过参考下面的详细说明并结合阅读附图，可以最好地理解本发明本身、进一步的目的和它的优点，其中：

图 1A 描述了数据处理系统的典型网络，其中每个数据处理系统都可以实现本发明；

图 1B 描述了本发明可以在其中实现的数据处理系统中可以使用的典型计算机体系结构；

图 1C 描述了数据流程图，该图说明当客户机试图访问在服务器中受保护的资源时可能被使用的典型的验证处理；

图 1D 描述了一个框图，该图示出了企业域的典型的分布式数据处理系统；

图 2 描述了一个框图，该图示出了具有权限服务器的分布式数据处理系统，根据本发明，该权限服务器已经被扩展为包括对在分布式数据

处理系统中已经收集的状态信息进行处理;

图 3 描述了一个流程图，该图示出用于创建控制权限服务器的权限规则集合的处理;

图 4A 描述了一个流程图，该图示出了确定将向用户示出的资源集合的处理，这些资源是明确授权给用户的以及这些资源是基于与服务器端环境有关的计算状态信息已经明确赋权给用户的;

图 4B 描述了一个流程图，该图示出根据本发明的实施例使用权限规则集合来为用户生成赋权资源集合的处理; 以及

图 5A-5C 描述了权限服务器使用与服务器端分布式数据处理系统的资源利用率有关的信息来调整被指示为用户可用的资源的一组示例。

具体实施方式

通常，可以包括或涉及本发明的设备包括多种多样的数据处理技术。因此，作为背景技术，在更详细地描述本发明之前，描述分布式数据处理系统中硬件和软件部件的典型组织。

现在参考附图，图 1A 描述了数据处理系统的典型网络，其每一个数据处理系统可以实现本发明的一部分。分布式数据处理系统 100 包含网络 101，可以作为用于提供在与分布式数据处理系统 100 中连接在一起的不同的设备和计算机之间的通信链路的介质。网络 101 可以包括诸如电线或光纤光缆的永久的连接，或者通过电话或无线通信构成的暂时连接。在描述的示例中，服务器 102 和服务器 103 与存储单元 104 一道连接至网络101。此外，客户机105-107也连接至网络101。客户机105-107和服务器 102-103 可以由多种计算设备代表，诸如大型机、个人计算机、个人数字助理（PDA）等。分布式数据处理系统 100 可以包括未示出的附加服务器、客户机、路由器、其它设备，以及对等体系结构。

在描述的示例中，分布式数据处理系统 100 可以包括具有网络 101 的因特网，网络 101 代表使用不同的协议相互通信的世界范围内的网络和网关的集合，这些集合诸如轻型目录访问协议（LDAP）、传输控制协议/网间协议（TCP/IP）、超文本传输协议（HTTP）、无线应用协议（WAP）

等。当然，分布式数据处理系统 100 还可以包括多个不同类型的网络，例如，内联网、局域网（LAN）、或广域网（WAN）。例如，服务器 102 直接支持客户机 109 和结合无线通信链路的网络 110。网络启动的电话 111 通过无线链路 112 连接至网络 110，PDA 113 通过无线链路 114 连接至网络 110。电话 111 和 PDA 113 也可以使用适当的技术，诸如蓝牙™无线技术，通过无线链路 115 在它们之间直接传送数据，以便创建所谓的个人局域网（PAN）或个人 ad-hoc 网。以类似的方式，PDA 113 可以通过无线通信链路 116 向 PDA 107 传送数据。

本发明可以在不同的硬件平台上实现；图 1A 意图作为不同种类的计算环境的示例，而不是作为对本发明体系结构的限制。

现在参考图 1B，该图描述了如图 1A 中所示的本发明可以在其中实现的数据处理系统的典型的计算机体系结构。数据处理系统 120 包含一个或多个连接至内部系统总线 123 的中央处理单元（CPU）122，总线 123 互连了随机访问存储器（RAM）124、只读存储器 126、及支持不同 I/O 设备的输入/输出适配器 128，该 I/O 设备诸如打印机 130、盘单元 132、或其它未示出的设备，诸如音频输出系统等。系统总线 123 还连接提供对通信链路 136 的访问的通信适配器 134。用户接口适配器 148 连接不同的用户设备，诸如键盘 140 和鼠标 142，或其它未示出的设备，诸如触摸屏、指示笔（stylus）、麦克风等。显示适配器 144 将系统总线 123 连接至显示设备 146。

本领域普通技术人员能够理解图 1B 中的硬件可以根据系统实现而变化。例如，系统可以具有一个或多个处理器，诸如基于 Intel®Pentium® 的处理器和数字信号处理器（DSP），及一个或多个类型的易失性和非易失性存储器。可以附加地使用或代替图 1B 中描述的硬件来使用其它外围设备。描述的示例并不意味着暗示关于本发明的体系结构的限制。

除了能够在多种的硬件平台上实现，本发明还可以在多种软件环境中实现。典型的操作系统可以用于在每个数据处理系统中控制程序执行。例如，一个设备可以运行 Unix®操作系统，而另一设备包含一简单 Java®运行时间环境。代表性的计算机平台可以包括浏览器，浏览器是用

于访问多种格式的超文本文档，诸如图形文件、字处理文件、扩展标记语言（XML）、超文本标记语言（HTML）、手持设备标记语言（HDML）、无线标记语言（WML），和各种其它格式和类型的文件的公知的软件应用。

本发明可以在如以上对于图 1A 和图 1B 中所描述的多种硬件和软件平台上实现。不过，更具体地说，本发明把注意力放在改进的数据处理环境上。在更详细地描述本发明之前，描述典型的分布式数据处理环境。

这里的图的描述涉及客户机设备或该客户机设备的用户的某些动作。本领域普通技术人员应该理解，到/来自客户机的响应和/或请求有时由用户发起而在其它时候由客户机通常代表客户机的用户自动地发起。由此，当在图中的描述中提及客户机或客户机的用户时，应该理解术语“客户机”和“用户”在不显著影响所描述的处理的意义的前提下，可以互换使用。

现在参考图 1C，数据流程图示出了当客户机试图访问在服务器中受保护的资源时，可以使用的典型的验证处理。如所示，位于客户机工作站 150 的用户，通过客户机工作站上执行的用户的网络浏览器，经由计算机网络上尝试访问服务器 151 上的受保护的资源。受保护或受控的资源是控制或限制对其进行访问的资源（应用、目标、文档、页面、文件、可执行代码、或其它计算资源、通信类型资源等）。受保护的资源由统一资源定位符（URL），或更一般地，统一资源标识符（URI）来标识，仅能够由经验证的授权用户访问。计算机网络可以为因特网、内联网、或其它网络，如图 1A 或图 1B 所示，并且服务器可以为网络应用服务器（WAS）、服务器应用、小服务程序（servlet）处理等。

当用户请求服务器端受保护的资源，诸如域“ibm.com”中的网页（步骤 152）时，发起该处理。术语“服务器端”和“客户机端”分别指在联网的环境中的服务器处或客户机处的动作或实体。网络浏览器（或相关的应用或小程序）生成被发送到托管域“ibm.com”的网络服务器的 HTTP 请求（步骤 153）。术语“请求”和“响应”应该被理解为

包括适合于传送与特定操作有关的信息的数据格式，这种信息例如消息、通信协议信息、或其它相关信息。

服务器确定其不具有对客户机的活动会话（步骤 154），因此服务器发起并完成服务器和客户机之间的 SSL（加密套接字协议层）会话的建立（步骤 155），其承担了服务器与客户机之间信息的多路传送。SSL 会话建立之后，随后在 SSL 会话中传送通信消息；由于在 SSL 会话中加密通信消息，任何保密的信息仍然是安全的。

然而，在允许用户访问受保护资源之前，服务器需要确定用户的身份，因此，服务器通过向客户机发送某种验证的质询（步骤 156）以要求用户执行验证处理。验证质询可以为各种格式，诸如 HTML 形式。然后用户提供被请求的或被要求的信息（步骤 157），诸如带有相关联的密码或其它形式的保密信息的用户名或其它类型的用户标识符。

验证响应信息被发送给服务器（步骤 158），此时，服务器通过例如检索先前提交的注册信息并将当前验证信息与用户的存储信息相匹配，来验证用户或客户机（步骤 159）。假设验证成功，建立对于经验证的用户或客户机的活动的会话。

然后，服务器检索原始请求的网页并发送 HTTP 响应消息给客户机（步骤 160），由此满足用户对受保护的信息的原始请求。那时，用户可以通过点击浏览器窗口中的超文本链接，请求“ibm.com”中的另一页面（步骤 161），并且浏览器向服务器发送另一 HTTP 请求消息（步骤 162）。那时，服务器识别出该用户具有活动会话（步骤 163），并且该服务器在另一个 HTTP 响应消息中将所请求的网页发送回给客户机（步骤 164）。

现在参考图 1D，框图描述企业域的典型的分布式数据处理系统。如在典型的公司计算环境或基于因特网的计算环境中，企业域 170 托管有受控资源，用户 171 可以例如通过使用客户机设备 173 上的浏览器应用 172 经由网络 174 访问该受控资源。应用服务器 175 通过基于 Web 的应用或其它类型的应用，包括遗留应用，来支持可访问的资源。验证服务器 176 支持不同的验证机制，诸如用户名/密码、X.509 证书、或安

全令牌。企业域 170 支持多服务器。代理服务器 177 为企业域 170 执行广泛范围的功能。可以通过配置文件和企业策略数据库 178 有管理地配置代理服务器 177 以控制代理服务器 177 的功能，例如，为了镜像来自于应用服务器的内容而高速缓存网页，或者通过输入数据流过滤器单元 179 和输出数据流过滤器单元 180 过滤传入和传出的数据流。输入数据流过滤器单元 179 可以在传入请求上执行多重检查，而输出数据流过滤器单元 180 可以在传出的响应上执行多重检查；每个检查可以根据各种企业策略中指定的目标和条件来执行。

企业域 170 包括权限服务器 181，其接受用户注册数据库 182、访问控制列表（ACL）数据库 183、来自其它域的第三方数据流 184 中的信息。权限服务器 181 通过针对用户对这些服务的请求检查策略和/或访问控制列表来确定是否授权了该用户访问由域 170 中的应用服务器 175 提供的某种服务。用户特定的权限集合由代理服务器 177、权限服务器 181，或代理服务器 177 和权限服务器 181 之间的组合的或协调的作用来使用，以响应于用户请求，确定或控制对应用服务器 175 和其它受控的资源的访问。

上述企业域 170 中的实体代表许多计算环境中典型的实体。如对于图 1C 所示，基于 Web 的应用可以利用各种手段来提示用户输入验证信息，通常如在 HTML 表单中的用户名/密码组合。在图 1D 中示出的示例中，可以要求在客户机 173 可以访问资源之前验证用户 171，之后，以类似于上面图 1C 中描述的方法为客户机 173 建立会话。在图 1D 中，接收到来自客户机 173 的传入请求后，输入数据流过滤器单元 179 可以确定客户机 173 是否已经建立了会话；如果没有，可以调用验证服务器 176 上的验证服务，以便验证用户 171。如果客户机 173 已经建立会话，则在准许对受控的资源访问之前可以在传入请求上执行附加的检查；该附加的检查可以在企业验证策略中指定。

现在来看本发明，如上所述，一些分布式数据处理系统在向这些分布式数据处理系统的用户提供一致的性能和结果上存在问题。本发明针对于一种改进的权限服务器，其功能被扩展为自动地调整它关于与该权

限服务器正工作于其中的分布式数据处理环境有关的状况信息或状态信息所进行的处理。下面参照余下的附图更详细地描述本发明。

现在参考图 2，框图描述了带有权限服务器的分布式数据处理系统，根据本发明，权限服务器已经被扩展为包括对在分布式数据处理系统中已经收集的状态信息进行的处理。图 2 中示出的实体区别于图 1D 中示出的实体，但是图 2 代表的分布式数据处理系统具有与图 1D 所示的类似功能；例如，图 2 示出了验证服务器，其也包含作为代理服务器的功能。可以在图 2 的分布式数据处理系统中包含其它实体，但是并未示出。

以类似于上面关于图 1D 中描述的方式，客户机 202 支持 web 浏览器应用或类似类型的用户应用，用于访问来自诸如电子商务服务器的不同应用的资源和服务。由诸如电子商务企业的机构运行的分布式数据处理系统，包括验证服务器 204 和一组用于响应客户机发起的资源请求的应用服务器。权限服务器 206 接受来自用户注册数据库 208、验证策略数据库 210、及来自其它域的第三方数据流 212 的信息。权限服务器 206 通过针对用户对这些服务的请求检查策略和/或访问控制列表来确定用户是否被授权访问由相关应用服务器提供的某种服务。由权限服务器 206 提供至验证服务器 204 的用户特定的权限集合由验证服务器 204 使用，以响应于用户请求，确定或控制对应用服务器和其它受控的资源的访问。

对照图 1D，图 2 描述了带有权限服务器的分布式数据处理系统，该权限服务器具有已经被扩展为包括对在分布式数据处理系统中已经收集的状态信息进行的处理。权限服务器 206 已经被扩展为包括状态处理单元 220，其从中央监控服务器 222 和其状态信息数据库 224 中获取与其计算环境有关的状况信息。权限服务器 206 负责确定哪个应用或其它资源被指示为从分布式数据处理系统到特定用户是可用的。权限服务器 206 的操作通过权限规则的使用来控制，该权限规则存储在权限规则数据库 226 中并且通过权限规则管理应用 228 进行管理。权限服务器 206 获取与那些资源有关的状态信息，并且解释它报告对特定用户可用的资源中的状态信息。

权限服务器 206 可以通过各种操作从中央监控服务器中获取信息：响应于发送给中央监控服务器的请求；由中央监控服务器发起的周期的或定期的信息传送；或者以一些其它的方式。在图 2 中示出的示例中，中央监控服务器被描述为独立的实体，但是在可选实施例中，与状态信息的中央数据存储器相关的功能可以合并至代理服务器、验证服务器、授权服务器、权限服务器、或与在给定时间点与用户特定权限集合的确定相关联的某些其它实体。

与服务器端数据处理系统状况有关的信息可以通过多种技术获得。如第一示例中，代理服务器可以 ping 应用服务器来确定应用服务器是否主动地并/或快速地响应 ping，如果不是，则该代理服务器可以标记该应用服务器为脱机，直到其响应来自代理服务器的某些形式的请求为止。在图 2 示出的示例中，应用服务器 231-234 中的每一个包括分布式监控代理，诸如分布式监控代理 235-238。分布式监控代理监控在它们各自的应用服务器上的计算资源和/或规格。多种通用的计算机资源都可以被监控，诸如 CPU 利用率或存储器负载，并且/或者多种特定应用资源可以被监控，诸如同时被服务的客户机请求的数量。被监控的资源可以主动地参与报告其状态，或者信息收集代理可以被动地检测资源的状态或状况。每个分布式监控代理向中央监测服务器 222 报告它的测量值，中央监控服务器 222 将收集到的值存储至状态信息数据库 224 中。数据采集工作可以以多种方式执行。例如，代理可以以如下方式发送所采集的数据：周期性地；根据可配置的调度；响应于来自中央监控服务器的轮询请求；或者以某些其它方式。

现在参考图 3，流程图描述了根据本发明的实施例的用于创建控制权限服务器的权限规则集合的处理。该处理开始于管理用户或某些其它类型的具有特定服务器端特权的用户操作如图 2 中所示的权限规则管理应用（步骤 302）。管理员通过管理应用选择要被限制的资源（步骤 304）。该资源可以从正如由管理应用显示给管理员的服务器端计算环境中的计算资源列表中进行选择。可通过管理应用来限制的计算资源列表也可以通过管理应用进行配置。然后管理员选择或输入将与所选资源相关联

的利用率或可用性的阈值（步骤306）。然后生成权限规则（步骤308），并且该新近生成的权限规则与所选资源的指示相关联地进行存储（步骤309），由此结束处理。

权限规则的格式可以根据本发明的不同实施例而变化。例如，权限规则可以是包含代表服务器端数据处理环境中的计算资源利用率的变量的规则表达式。变量的值由分布式监控系统或通过某些形式的状态信息获取处理来收集或累积。计算资源可以是硬件相关或软件相关的。可以被限制的特定资源可以根据计算环境的类型、可能对用户可用的应用、运行企业域的机构的各种商业目标、或其它考虑而改变。在最简单的情况下，单一利用率等级可以与资源相关；在更复杂的情况下，多重资源的利用率或可用性的值可以结合到单一权限规则中。此外，如下面更详细地描述，权限规则不限制为代表计算资源的变量，而是还可以包括涉及用户属性的变量。

现在参考图 4A，流程图描述了根据本发明实施例的、用于确定将向用户显示的资源集合的处理，这些资源是明确授权给用户的以及这些资源是基于与服务器端环境有关的计算状态信息已经明确赋权给用户的。处理开始于接收来自于由用户操作的客户机设备的请求（步骤402）。尽管确定赋权的资源的处理可以结合验证操作一起执行，但是可以假设用户已经被验证，所以客户机请求与关于活动用户会话的信息相关联（步骤404）。例如，在验证操作期间检索并高速缓存的验证策略可以基于与该用户相关联的会话标识符来进行检索。然后，根据用户的身份、适当的验证策略、或其它的考虑确定这个特定用户的授权资源的列表（步骤406）。

对照现有技术中将授权资源集合显示给用户作为用户可用的资源的系统，本发明缩小了可用资源的列表以根据计算环境状态信息确定赋权资源列表（步骤408）。然后，同赋权资源的指示一起生成对客户机的响应（步骤410）；换句话说，该响应仅包含那些考虑到用户验证策略是用户特定的、并且考虑到计算资源可用性是权限特定的资源。然后，向用户的客户机设备发送该响应（步骤412），并且处理结束。

现在参考图 4B，流程图表述了根据本发明的实施例使用权限规则集合来为用户生成赋权资源集合的处理。图 4B 提供了对图 4A 中步骤 406 和 408 的附加细节，用来确定作为特定用户授权资源子集的赋权资源的列表。

处理开始于获取对于正在试图访问资源的用户的授权资源列表（步骤 452）。如下更详细地描述，该处理在授权资源列表中循环，通过处理列表中每个条目以确定特定的条目是否应该留在赋权资源列表中。以这种方式处理授权资源列表，直到可认为剩余的授权资源列表是赋权资源列表。由此，处理得到授权资源列表中的下一个授权资源（步骤 454），例如，授权资源的标识符，此后被认为是当前的授权资源，即当前正在处理的授权资源。

然后从适当的数据存储器中检索限制或涉及当前授权资源的任何权限规则（步骤 456）。在下文中，处理在权限规则列表中循环，通过处理权限规则列表中的每个条目以确定特定权限规则是否导致特定授权资源或者授权资源集合对用户不可用。由此，处理得到权限规则列表中的下一个权限规则（步骤 458），此后被认为是当前的规则，即当前正在处理的权限规则。

检索当前权限规则中的变量的值（步骤 460），并且基于检索到的变量值评价权限规则（步骤 462）。该值可以从存储在用户注册表中的用户属性中、从服务器状态信息数据库中、或其它类型的数据存储器中进行检索。

然后关于权限规则是否评价为应该认为当前授权资源过度利用或不可用的断言做出确定（步骤 464）。如果是，则授权资源从授权资源列表中移除（步骤 466）；以这种方式，授权资源列表可能被逐条目减少。然后，关于授权资源列表中是否还有任何未处理的授权资源，作出确定（步骤 468）。如果没有，则处理过的零或更多剩余授权资源的列表代表返回给调用功能的零或更多赋权资源的列表（步骤 470），并且处理结束。

如果步骤 464 中当前权限规则没有评价为应该认为当前授权资源过度利用或不可用的断言，则在步骤 466 中当前授权资源不从授权资源列

表中移除。代替地，关于是否还有与当前授权资源相关联的更多权限规则，做出确定（步骤472）。如果有，则处理分支返回至步骤458来获取并评价另一权限规则。如果没有另外的权限规则来评价，则处理转移至步骤468来检查是否还有未处理的另外的授权资源。如果在步骤468中授权资源列表中存在有未处理的授权资源，则处理分支返回至步骤454，来获取并处理授权资源列表中的下一个授权资源。如上所述，在整个授权资源列表已经被处理后，剩余的授权资源列表也代表用户被赋权访问的资源列表。

鉴于上面提供的详细描述，本发明的优点应该是明显的。在现有技术中，权限引擎基于用户被授权访问的资源确定对于该用户的赋权资源的列表。相反，本发明提供了权限引擎，该权限引擎在确定应该向计算环境中的服务器的用户显示的可用资源列表时，考虑了其计算环境的状况。使用本发明，系统在资源已经超过阈值情况时，不将与这样的资源集合有关的信息显示给用户。这种情况可能需要考虑用户可能在这些情况下经历了不良的性能的事实。其它考虑可以包括基于用户属性保留那些资源的权限决定，正如在下面谈到的示例中详细描述的那样。

本发明的优点的一个方面是，本发明由于服务器端系统的状况提前主动地防止用户获取请求某个资源的能力，即使在不同的服务器端情况下用户可能被授权请求那些资源；用户的赋权资源总是用户通常的授权资源的子集，尽管该赋权资源集合可以等于或者和授权资源集合一样大。通过提前主动地防止用户将服务器端系统推向更过度利用的情况，本发明减少了某些试图调整服务器端处理以容忍过度利用的情况的服务器端解决方案的需要。

关于图5A-5C，一组示图描述权限服务器使用与服务器端分布式数据处理系统的资源利用率相关的信息，来调整被指示为对用户可用的资源的一组示例。图5A-5C代表通常的考虑或数据流而并不意在示出电子商务网站的操作中可能涉及的各种计算实体的细节。在这组示例中，在线的经纪服务为其所注册的客户操作网站。假设用户响应于用户访问该网站的请求成功地完成了验证质询，则权限服务器需要确定哪个服务应

该被指示为对该用户是可用的。

现在参考图 5A，权限服务器 500 接收应用的利用率等级的状态信息 502，在这个示例中该应用为生成实时股票和证券行情的数据流的应用。在这组示例中，系统管理员可以已经预先确定了当该应用的利用率上升到太高时，实时牌价流应用提供不良的响应时间或不一致的性能。为了防止过度利用的情况，系统管理员预先创建权限规则，只有当应用低于 70%利用率等级时，其才指示实时牌价流应用对用户可用。由于权限服务器对实时牌价流应用收到 40%的利用率值，所以权限服务器确定该实时牌价流应用应该指示为可用。权限服务器可以将授权资源的列表提供给动态地生成发送给客户机的网页 504 的另一服务器。客户机的 web 浏览器应用显示窗口 506，其示出了通过在线经纪网站对用户可用的赋权资源列表 510-513；赋权资源列表可以由超链接或某些其它类型的嵌入在网页中的用户可选择的控件来代表。在这个示例中，超链接 511 代表实时牌价流应用的可用性；用户可以选择超链接 511 来访问实时牌价流应用的功能。

现在参考图 5B，权限服务器 500 接收应用的利用率等级的状态信息 522，在这个示例中，该应用也是生成股票和证券行情的实时数据流的应用。同样，系统管理员之前已经创建了权限规则，只有当应用低于 70%的利用率等级时，其才指示实时牌价流应用对用户可用。由于权限服务器对实时牌价流应用收到 90%的利用率值，所以权限服务器确定该实时牌价流应用不应该被指示为可用。

在这个示例中，发送给客户机的网页 524 不包括赋权资源 526-529 列表中的实时牌价流应用的超链接。代替地，实时牌价流应用仅由具有不同字体属性的文本串 527 来代表，该字体属性指示该文本串 527 为纯文本而不代表超链接，由此指示用户该网页不包含对实时牌价流应用的用户可选择的控件；可以显示其它解释该实时牌价流应用为何不可用的信息。因此，不向用户显示实时牌价流应用为可用的指示，并且该用户不能发起访问实时牌价流应用的请求，即使用户被授权访问该实时牌价流应用。此外，在包含本发明的系统中，一般情况下可以防止用户访问

不在赋权资源列表中的任何资源。以此方式，权限服务器根据由系统管理员配置的权限规则，提前主动地减少授权用户对实时牌价流应用的进一步利用。

现在参考图 5C，权限服务器 500 接收用于股票和证券行情的实时数据流的利用率等级的状态信息 532。在图 5C 中表示的示例中，比图 5A 和 5B 的示例中使用的权限规则更复杂的权限规则是有效的。系统管理员预先创建权限规则，只有当应用低于 70%的利用率等级时，其才指示实时牌价流应用对标准用户可用；然而，如果该用户具有高级账户，在利用率值达到 95%之前该实时牌价应用都可用。

这样，权限服务器访问用户注册表 540 来获取存储在用户帐户 542 中的该用户的用户特定属性，并且权限服务器发现用户属性 544，其指示该用户已预先订购高级账户。因为权限服务器确定该用户具有高级账户，并且因为权限服务器接收到实时牌价流应用的 90%的利用率值，于是权限服务器确定该实时牌价流应用应该对该特殊用户指示为可用。权限服务器将赋权资源列表提供给动态生成发送给客户机的网页 554 的另一服务器。客户机的 web 浏览器应用显示窗口 506，其示出了通过在线经纪网站对高级用户可用的赋权资源 555-559 的列表；赋权资源列表可以由超链接或某些其它类型的嵌入在网页中的用户可选择的控件来代表。在这个示例中，超链接 559 代表对具有高级账户的用户可用的高级资源。更重要地，超链接 556 代表实时牌价流应用的可用性；用户可以选择超链接 556 来访问实时牌价流应用的功能。

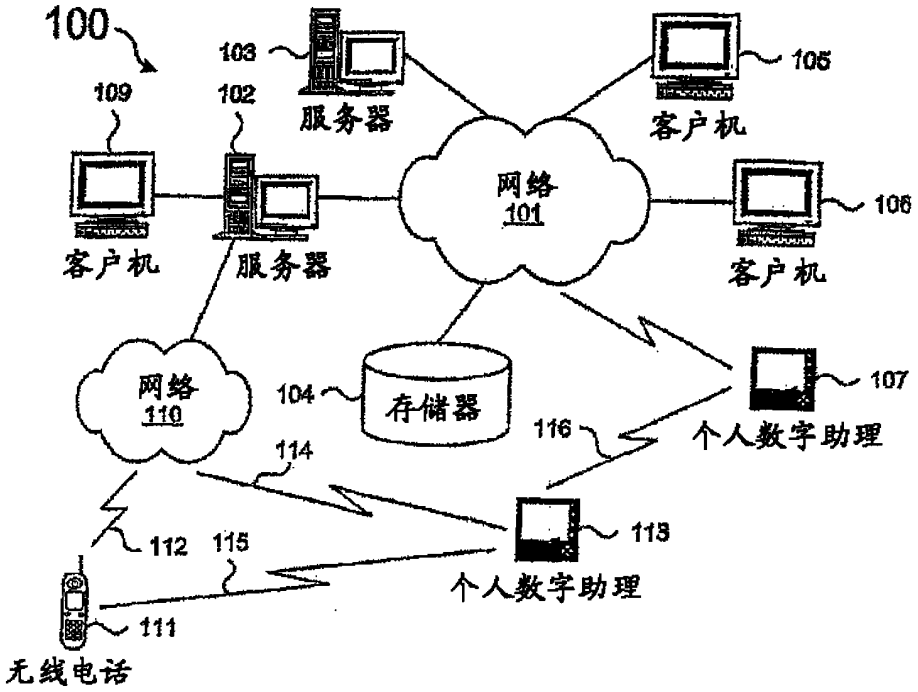
在图 5C 示出的示例中，服务器端系统已经确定该用户可以正常地被授权访问特殊的资源，例如，实时牌价流应用。在确定资源的利用率因子后，权限规则指示某些被授权访问资源的用户没有被赋权访问资源，而其它具有不同用户属性的用户被赋权访问该资源。向某些用户显示资源可用的指示而不向其它用户提供资源可用的指示；即使所有的用户都被授权访问该资源，某些用户可以发起另外的请求来访问该资源，而其它用户不能发起请求来访问该资源。同样，权限服务器已经提前主动地减少某些授权用户对实时牌价流应用的进一步利用而保留 5%利用

率的缓冲以保证具有高级账户的用户从该资源得到足够的服务等级。

重要的是要注意，尽管本发明在完整功能的数据处理系统的上下文中进行了描述，但是本领域技术人员能够理解，本发明的处理能够以计算机可读介质中的指令形式和多种其它形式散发，而不管实际用来执行该散发的信号承载介质的特定种类。计算机可读介质的示例包括诸如EPROM、ROM、磁带、纸件、软盘、硬盘驱动器、RAM 以及 CD-ROM 的介质以及诸如数字和模拟通信链路的传输类型介质。

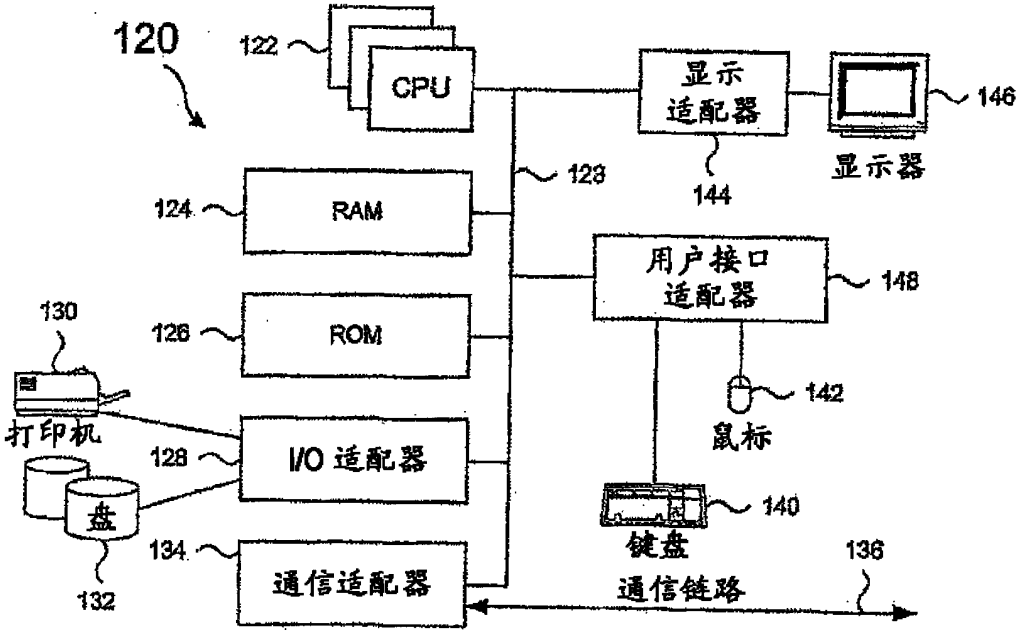
方法通常被构想为是产生期望的结果的自相一致的步骤序列。这些步骤要求物理量的物理操作。通常，尽管不是必需的，这些量采用能够被存储、传送、组合、比较和其它操作的电或者磁性形式。主要由于通常使用的原因，作为比特、值、参数、项目、要素、目标、符号、字符、术语、数目等引用这些信号有时是方便的。然而需要注意的是所有的这些术语和类似的术语需要与适当的物理量相结合并且它们仅是应用于这些量的方便标记。

已经以说明为目的给出了本发明的描述，但并不是意图穷举或限于所公开的实施例。多种修改和变形对于本领域普通的技术人员来说将是明显的。选择了实施例以解释本发明的原理和其实际应用并使本领域的普通技术人员理解本发明，以便实现具有可能适合于其它设想用途的各种改进的各种实施例。



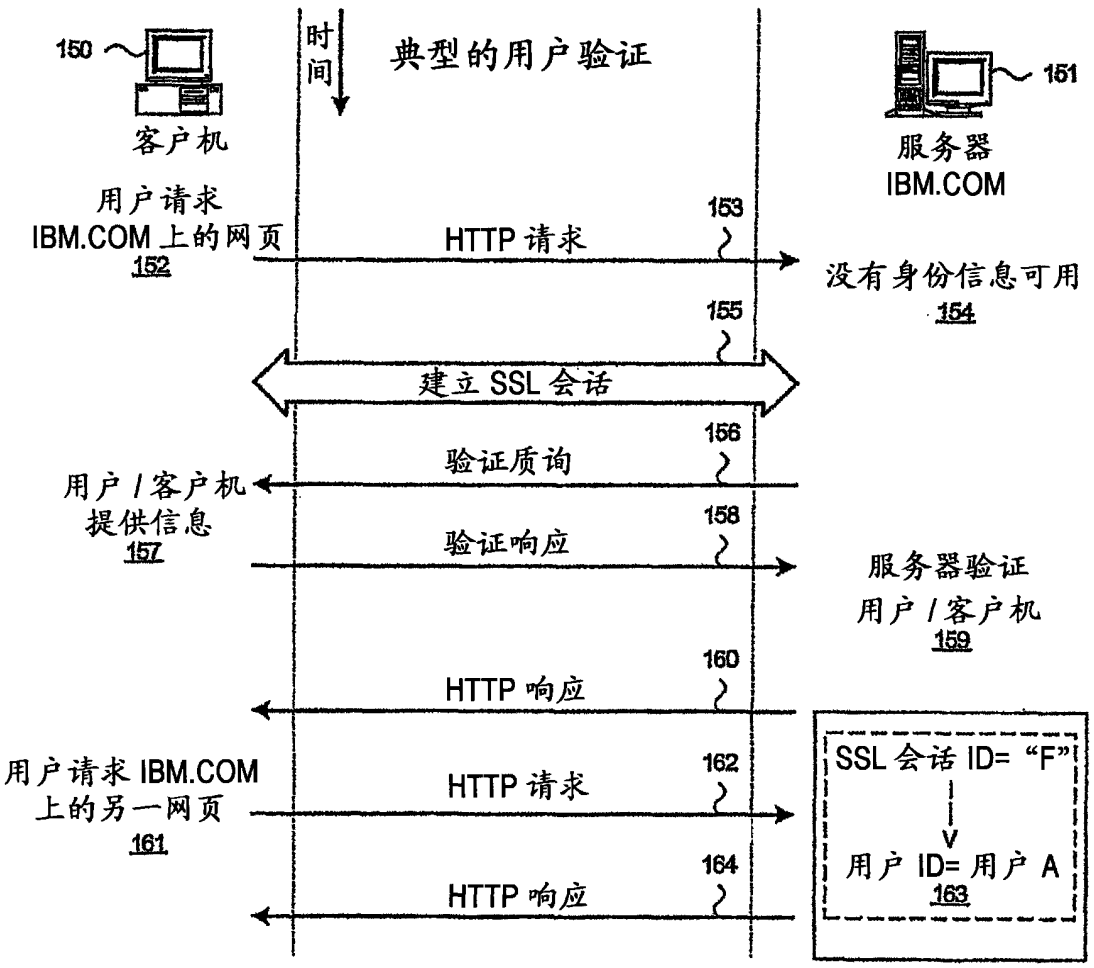
现有技术

图 1A



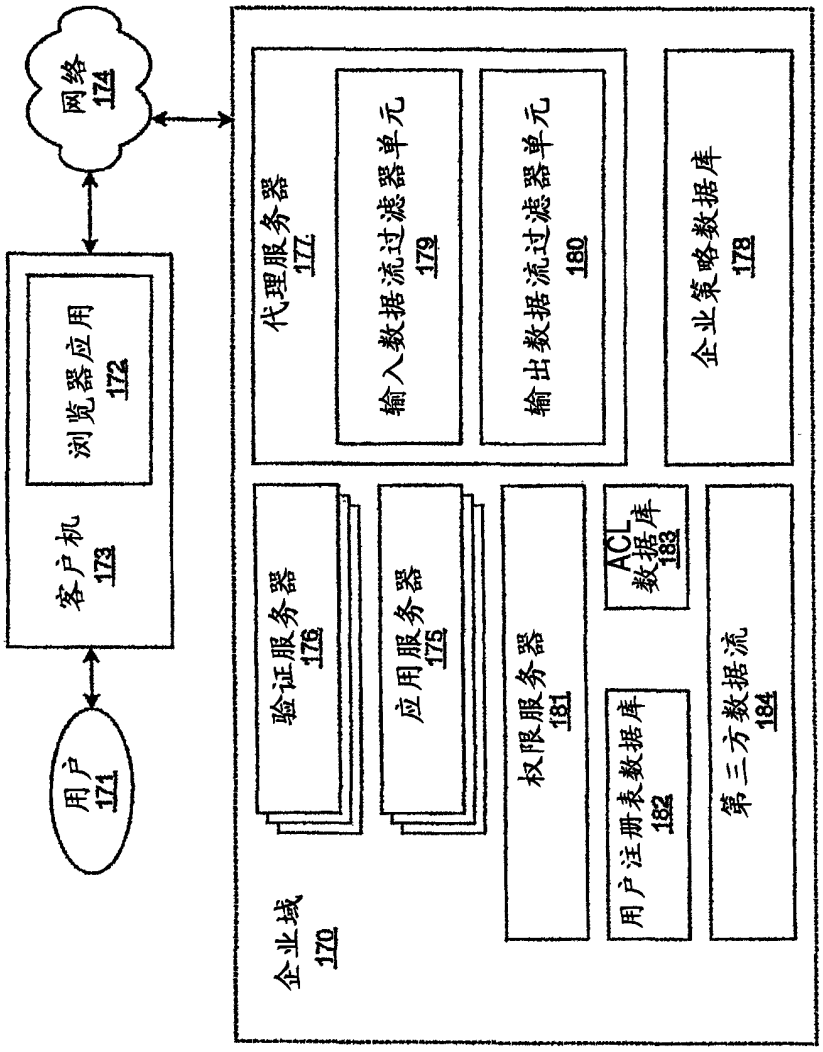
现有技术

图 1B


典型的用户验证
时间
150
客户机
151
服务器
IBM.COM
用户请求
IBM.COM 上的网页
152
153
HTTP 请求
没有身份信息可用
154
155
建立 SSL 会话
156
验证质询
用户 / 客户机
提供信息
157
158
验证响应
服务器验证
用户 / 客户机
159
160
HTTP 响应
SSL 会话 ID= "F"
V
用户 ID= 用户 A
163
用户请求 IBM.COM
上的另一网页
161
162
HTTP 请求
164
HTTP 响应

现有技术

图 1C


网络
174
浏览器应用
172
客户机
173
用户
171
企业域
170
验证服务器
176
应用服务器
175
权限服务器
181
用户注册表数据库
182
ACL
数据库
183
第三方数据流
184
代理服务器
177
输入数据流过滤器单元
179
输出数据流过滤器单元
180
企业策略数据库
178

现有技术
图 1D

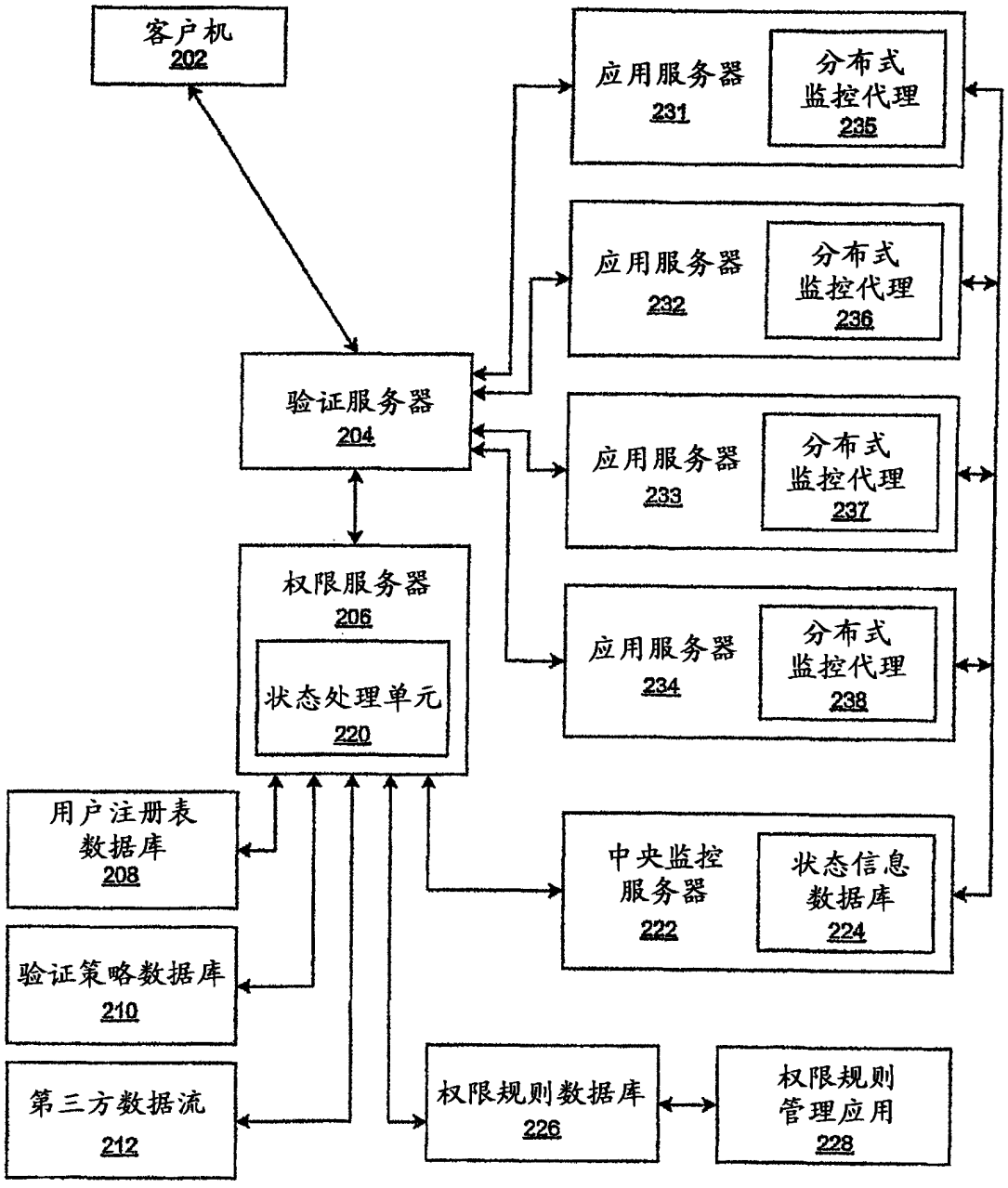

客户机
202
应用服务器
231
分布式
监控代理
235
应用服务器
232
分布式
监控代理
236
验证服务器
204
应用服务器
233
分布式
监控代理
237
权限服务器
206
状态处理单元
220
应用服务器
234
分布式
监控代理
238
用户注册表
数据库
208
中央监控
服务器
222
状态信息
数据库
224
验证策略数据库
210
第三方数据流
212
权限规则数据库
226
权限规则
管理应用
228

图 2

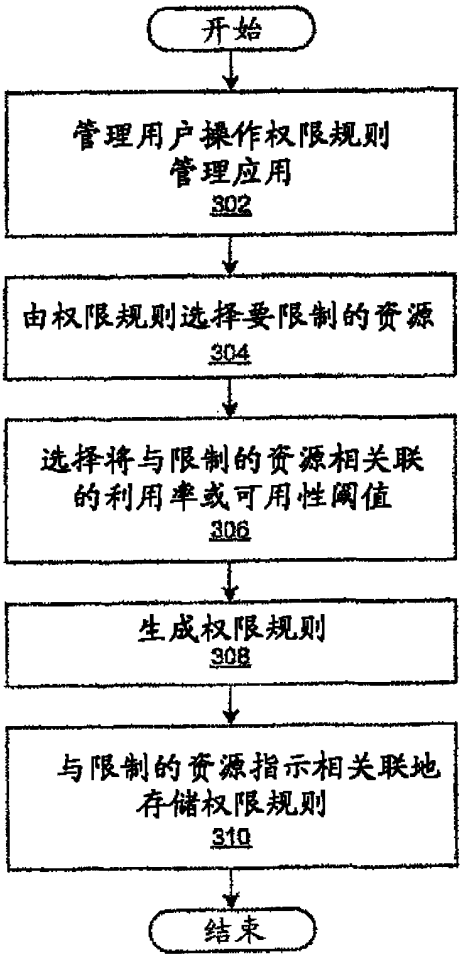

开始
管理用户操作权限规则管理应用
302
由权限规则选择要限制的资源
304
选择将与限制的资源相关联的利用率或可用性阈值
306
生成权限规则
308
与限制的资源指示相关联地存储权限规则
310
结束

图 3

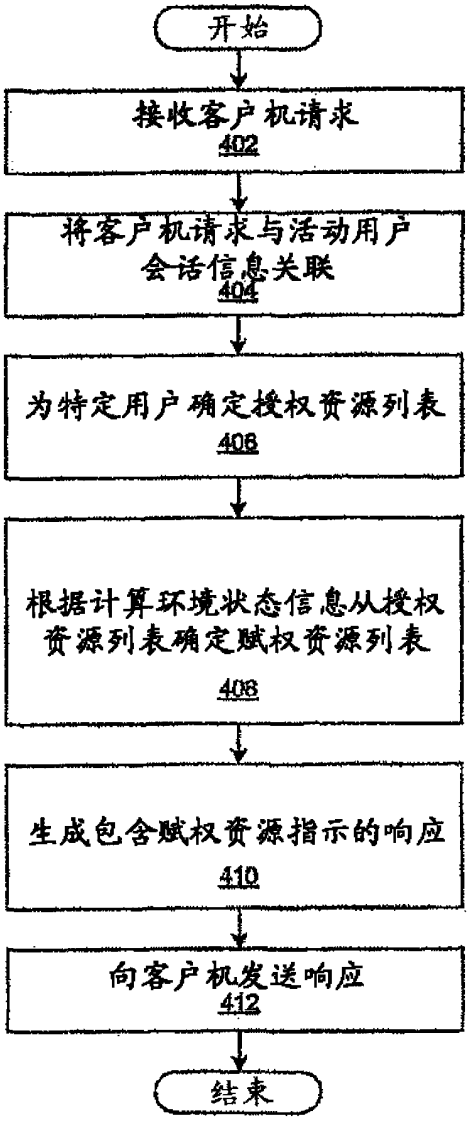

开始
接收客户机请求
402
将客户机请求与活动用户会话信息关联
404
为特定用户确定授权资源列表
406
根据计算环境状态信息从授权资源列表确定赋权资源列表
408
生成包含赋权资源指示的响应
410
向客户机发送响应
412
结束

图 4A

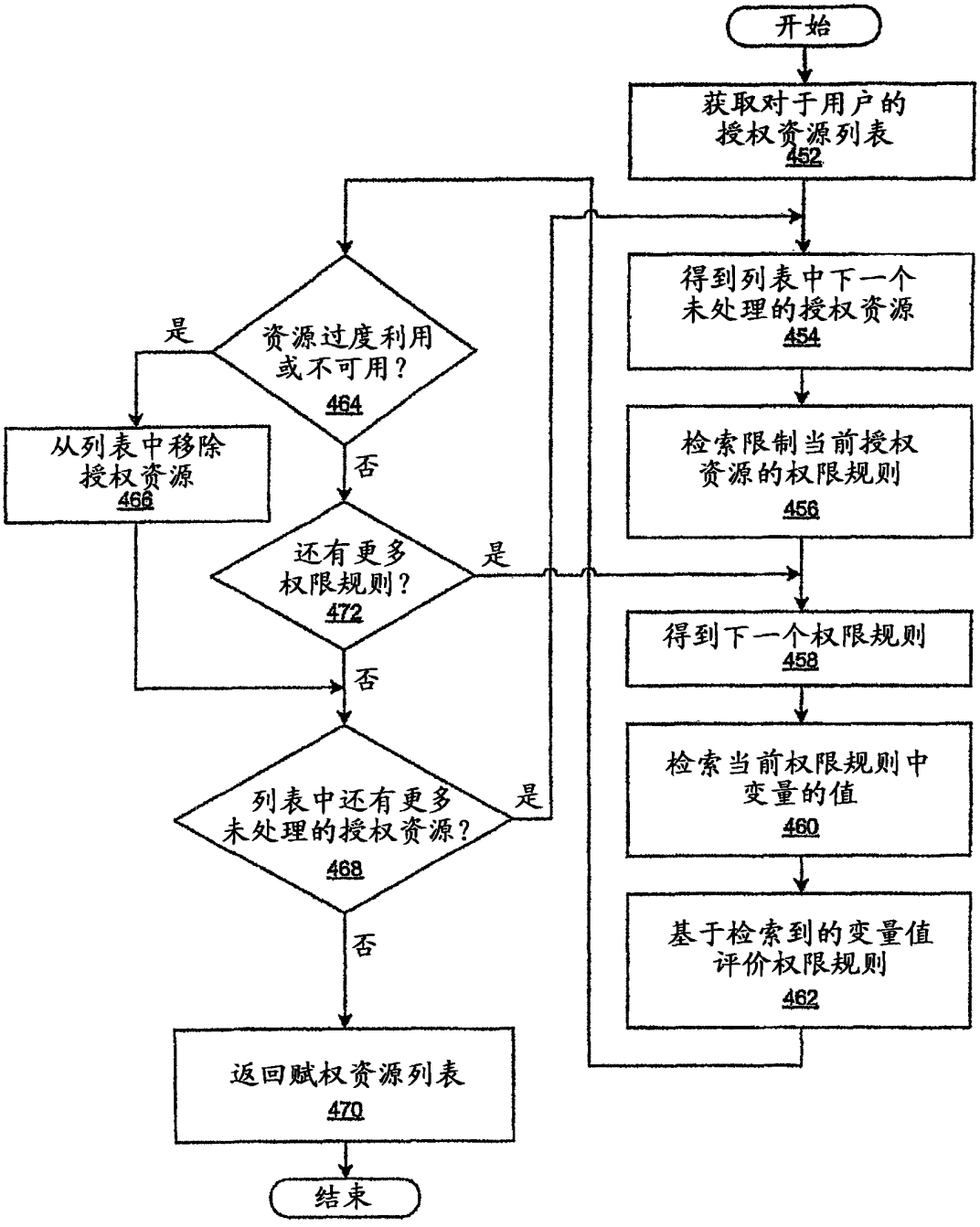

开始
获取对于用户的授权资源列表
452
得到列表中下一个未处理的授权资源
454
检索限制当前授权资源的权限规则
456
得到下一个权限规则
458
检索当前权限规则中变量的值
460
基于检索到的变量值评价权限规则
462
资源过度利用或不可用？
464
是
否
从列表中移除授权资源
466
还有更多权限规则？
472
是
否
列表中还有更多未处理的授权资源？
468
是
否
返回赋权资源列表
470
结束

图 4B

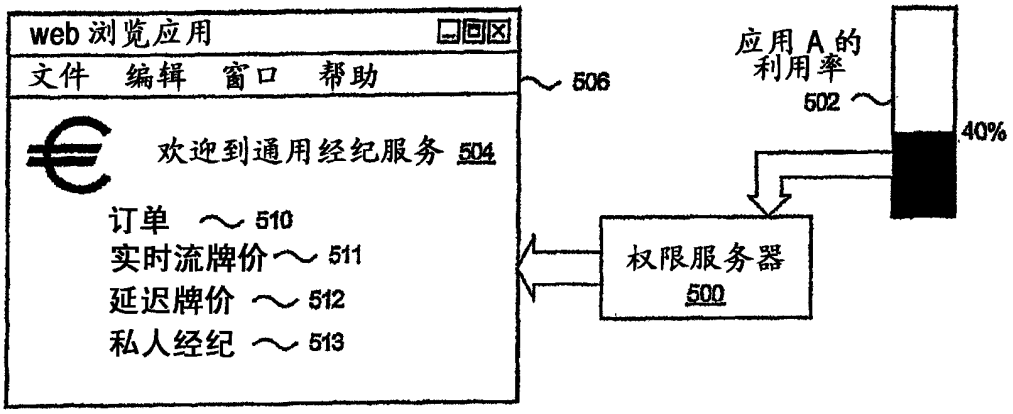

web 浏览应用
文件 编辑 窗口 帮助
506
欢迎到通用经纪服务 504
订单 510
实时流牌价 511
延迟牌价 512
私人经纪 513
应用 A 的
利用率
502
40%
权限服务器
500

图 5A

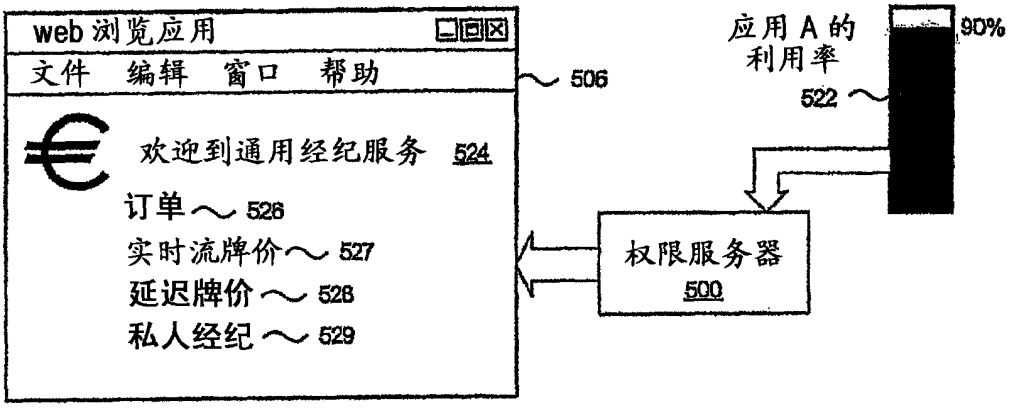

web 浏览应用
文件 编辑 窗口 帮助
506
欢迎到通用经纪服务 524
订单 526
实时流牌价 527
延迟牌价 528
私人经纪 529
应用 A 的
利用率
522
90%
权限服务器
500

图 5B

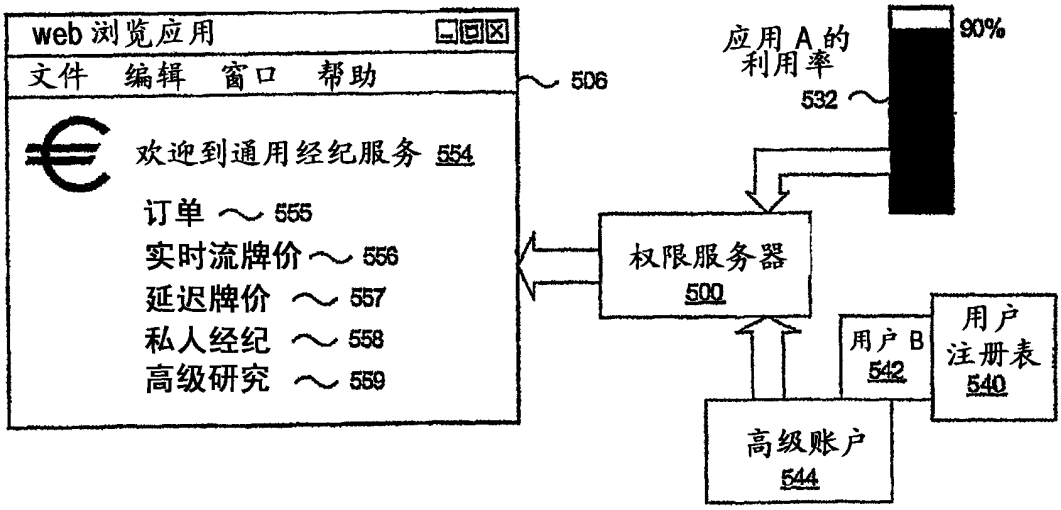

web 浏览应用
文件 编辑 窗口 帮助
506
欢迎到通用经纪服务 554
订单 555
实时流牌价 556
延迟牌价 557
私人经纪 558
高级研究 559
应用 A 的
利用率
532
90%
权限服务器
500
用户 B
542
用户
注册表
540
高级账户
544

图 5C