(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 106664323 B
(45)授权公告日 2020.05.15

(21)申请号 201580047019.4

(22)申请日 2015.04.20

(65)同一申请的已公布的文献号
申请公布号 CN 106664323 A

(43)申请公布日 2017.05.10

(30)优先权数据
62/054,544 2014.09.24 US
14/690,062 2015.04.17 US

(85)PCT国际申请进入国家阶段日
2017.03.02

(86)PCT国际申请的申请数据
PCT/US2015/026596 2015.04.20

(87)PCT国际申请的公布数据
WO2016/048415 EN 2016.03.31

(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚

(72)发明人 H·玛赫什瓦里
M·R·G·莫哈麦德·阿布杜尔
(续)

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李晓芳

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04W 12/08*(2009.01)
*H04W 4/50*(2018.01)
*H04W 4/08*(2009.01)
*H04L 12/24*(2006.01)
*H04L 29/08*(2006.01)
*H04W 4/60*(2018.01)
*H04L 9/32*(2006.01)
*H04W 28/08*(2009.01)
*H04W 4/70*(2018.01)
*G06F 9/4401*(2018.01)
*G06F 9/445*(2018.01)
*G06F 21/45*(2013.01)
*G06F 21/31*(2013.01)
*G06F 8/60*(2018.01) (续)

(56)对比文件
US 2005125509 A1,2005.06.09,
US 2014259178 A1,2014.09.11,
US 2014032759 A1,2014.01.30,
WO 2014047168 A1,2014.03.27,
CN 102281286 A,2011.12.14,

审查员 马琼华

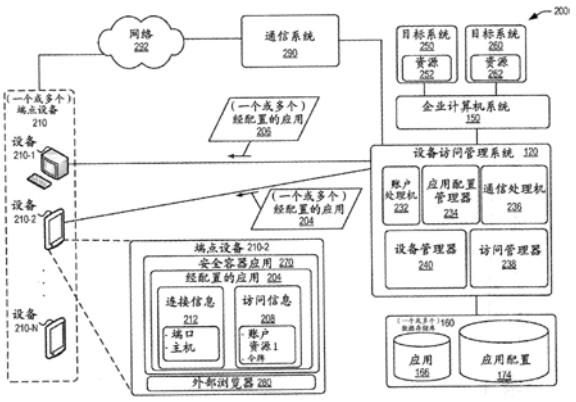
权利要求书3页 说明书39页 附图13页

(54)发明名称

企业系统中的设备上的应用的统一供应

(57)摘要

本公开一般涉及管理利用远程设备对企业系统的访问。公开了用于在远程设备上供应应用以访问企业系统中的资源的技术。具体而言,应用可以被自动配置为具有访问信息(例如,帐户信息)和连接信息,以利用远程设备访问企业系统中的资源。配置应用可以包括确定利用该应用访问资源的账户。如果尚未建立帐户,则可以供应帐户。在配置应用后,设备访问管理系统可以向为其配置应用的(一个或多个)远程设备提供经配置的应用。一旦接收到经配置的应用,该应用就可以被自动安装在远程设备上,之后该应用可以被执行以访问资源。




CN 106664323 B

[转续页]

[接上页]

(72)发明人 S·达斯 R·帕卡斯 S·卡蒂

(51)Int.Cl.

*G06F 8/71*(2018.01)

1.一种用于管理应用的供应的方法,所述方法包括:

为企业系统的用户识别与身份相关联的用户角色;

检索注册所述身份以访问所述企业系统的第一远程设备的设备信息;

基于所述用户角色,确定向所述身份提供对所述企业系统中可访问的第一资源的访问的账户 ,其中所述第一资源是利用所述用户角色可访问的多个应用中的第一应用从所述第一远程设备可访问的;

由计算机系统将所述第一应用配置为具有连接信息,所述连接信息使得所述第一应用能够连接到第一目标系统,以利用所述第一远程设备访问用于所述账户的所述第一资源,其中所述第一目标系统提供对所述第一资源的访问;

由所述计算机系统将所述第一应用配置为具有访问信息,所述访问信息使得所述第一应用能够基于由所述账户 向所述用户允许的访问来访问所述第一资源;以及

在将所述第一应用配置为具有所述连接信息和所述访问信息后,将所述第一应用发送到所述第一远程设备。

2.如权利要求1所述的方法,还包括:

检测注册所述身份以访问所述企业系统的多个远程设备中的第二远程设备;以及

在将所述第一应用配置为具有所述连接信息和所述访问信息后将所述第一应用发送到所述第二远程设备。

3.如权利要求1所述的方法,还包括:

检测所述用户角色从第一用户角色到第二用户角色的改变;

基于所述第二用户角色来确定所述身份对所述第一资源的访问的改变;以及

指示所述第一远程设备基于所述访问的改变来修改所述第一应用的配置。

4.如权利要求3所述的方法,还包括:

发现注册所述身份以访问所述企业系统的多个远程设备;

在配置所述第一应用后将所述第一应用发送到所述多个远程设备;以及

指示所述多个远程设备中的每一个基于所述访问的改变来修改所述第一应用的所述配置。

5.如权利要求3或4所述的方法,其中对所述第一资源的访问的改变包括撤销对所述第一资源的访问,并且其中修改所述第一应用的所述配置包括删除为所述第一应用配置的所述连接信息和所述访问信息。

6.如权利要求3或4所述的方法,其中对所述第一资源的访问的改变包括撤销对所述第一资源的访问,并且其中修改所述第一应用的所述配置包括从所述第一远程设备移除所述第一应用。

7.如权利要求3或4所述的方法,其中修改所述第一应用的所述配置包括调整为所述第一应用配置的所述访问信息。

8.如权利要求1至4中任一项所述的方法,还包括:

检测所述用户角色从第一用户角色到第二用户角色的改变;

基于所述第二用户角色,发现所述第二用户角色可访问的所述多个应用中的第二应用;

利用所述身份来配置所述第二应用,以用于从所述第一远程设备进行访问,其中所述

第二应用被配置为具有用于访问由第二目标系统提供的第二资源的信息;以及

将所述第二应用发送到所述第一远程设备。

9.如权利要求1至4中任一项所述的方法,其中所述设备信息指示所述第一远程设备的配置,所述配置指示所述第一远程设备上的操作系统配置和所述第一远程设备的硬件配置,并且其中所述第一应用是利用所述第一远程设备的所述配置来配置的。

10.如权利要求1至4中任一项所述的方法,其中所述连接信息包括所述第一目标系统的端口地址、所述第一目标系统的主机地址,以及所述第一目标系统的轻量级目录访问协议(LDAP)。

11.如权利要求1至4中任一项所述的方法,还包括:

基于所述用户角色,识别所述多个应用中的第二应用,所述第二应用使得所述用户能够执行所述用户角色;

供应所述第二应用,以访问所述企业系统中的第二资源;

配置所述第二应用,以从所述第一远程设备访问所述第二资源;以及

在配置所述第二应用后发送所述第二应用。

12.如权利要求1至4中任一项所述的方法,其中确定所述账户 包括:

确定是否为了访问所述第一目标系统的所述第一资源而供应所述账户 ;

在确定没有为了访问所述第一资源而供应所述账户 时,供应所述账户 ,以向所述身份提供对所述第一目标系统的所述第一资源的访问;以及

在确定为所述身份供应所述账户 后,检索关于所述账户 的账户 信息。

13.一种用于保护计算机免于包含恶意代码的电子通信的非暂态计算机可读介质,所述非暂态计算机可读介质包括存储在其上的指令,所述指令当在处理器上执行时,执行如权利要求1至12中任一项所述的步骤。

14.一种用于管理应用的供应的系统,所述系统包括:

一个或多个处理器;以及

存储指令的存储器,所述指令当由所述一个或多个处理器执行时,使得所述一个或多个处理器:

为企业系统的用户识别与身份相关联的用户角色;

检索注册所述身份以访问所述企业系统的多个远程设备的设备信息;

基于所述用户角色,确定向所述身份提供对所述企业系统中可访问的第一资源的访问的账户 ,其中所述第一资源是利用所述用户角色可访问的多个应用中的第一应用从所述多个远程设备可访问的;

由计算机系统将所述第一应用配置为具有连接信息,所述连接信息使得所述第一应用能够连接到第一目标系统,以利用所述多个远程设备来访问用于所述账户的所述第一资源,其中所述第一目标系统提供对所述第一资源的访问;

由所述计算机系统将所述第一应用配置为具有访问信息,所述访问信息使得所述第一应用能够基于由所述账户 向所述用户允许的访问来访问所述第一资源;以及

在将所述第一应用配置为具有所述连接信息和所述访问信息后,将所述第一应用发送到所述多个远程设备。

15.如权利要求14所述的系统,其中配置所述第一应用包括为所述多个远程设备中的

每个远程设备配置所述第一应用的实例，并且其中所述第一应用的实例是基于远程设备的配置来为所述远程设备配置的。

16.如权利要求15所述的系统，其中所述远程设备的配置包括所述远程设备的设备配置或操作系统配置中的一个或两者。

17.如权利要求15或16所述的系统，其中所述第一应用的实例针对所述多个远程设备中的第一远程设备和第二远程设备中的每一个被不同地配置，并且其中所述第一远程设备的配置不同于所述第二远程设备的配置。

18.一种用于管理应用的供应的方法，所述方法包括：

为企业系统的用户识别与身份相关联的用户角色；

检索注册所述身份以访问所述企业系统的第一远程设备的设备信息；

基于所述用户角色，为所述身份供应对多个应用的访问，其中所述多个应用中的每个应用被供应，以用于利用所述第一远程设备来访问所述企业系统中的不同资源；

由计算机系统将所述多个应用中的第一应用配置为具有第一连接信息和第一访问信息，以便从所述第一远程设备访问第一资源；

由所述计算机系统将所述多个应用中的第二应用配置为具有第二连接信息和第二访问信息，以便从所述第一远程设备访问第二资源；

在配置所述第一应用后将所述第一应用发送到所述第一远程设备；以及

在配置所述第二应用后将所述第二应用发送到所述第一远程设备。

19.如权利要求18所述的方法，还包括：

检测所述用户角色从第一用户角色到第二用户角色的改变；

基于所述用户角色的改变，确定由所述身份对所述第二资源的访问被撤销，并且由所述身份对第三资源的访问被允许，其中所述第一资源、所述第二资源和所述第三资源彼此不同；

基于确定对所述第二资源的访问被撤销，指示所述第一远程设备移除所述第二应用；

基于所述第二用户角色，为所述身份供应对第三应用的访问，所述第三应用提供从所述第一远程设备对所述企业系统中的第三资源的访问；

将所述多个应用中的第三应用配置为具有第三连接信息和第三访问信息，以从所述第一远程设备访问所述第三资源；以及

在配置所述第三应用后将所述第三应用发送到所述第一远程设备。

20.如权利要求18或19所述的方法，其中为所述身份供应对应用的访问包括为所述身份供应提供对由所述应用可访问的资源的访问的账户 。

21.一种非暂态计算机可读介质，所述非暂态计算机可读介质包括存储在其上的指令，所述指令当在处理器上执行时，执行如权利要求18至20中任一项所述的步骤。

22.一种用于管理应用的供应的系统，所述系统包括：

一个或多个处理器；以及

存储指令的存储器，所述指令当由所述一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要求18至20中任一项所述的步骤。

23.一种用于管理应用的供应的设备，所述设备包括用于执行如权利要求1至12或权利要求18至20中任一项所述的步骤的装置。

# 企业系统中的设备上的应用的统一供应

[0001] 对相关申请的交叉引用

[0002] 本申请要求于2015年4月17日提交的标题为“UNIFIED PROVISIONING OF APPLICATIONS ON DEVICES IN AN ENTERPRISE SYSTEM(企业系统中的设备上的应用的统一供应)”的美国非临时申请No.14/690,062的权益和优先权,该美国非临时申请要求于2014年9月24日提交的标题为“Mobile Security Manager(MSM)(移动安全管理器)”的美国临时申请No.62/054,544的权益和优先权。出于所有目的将上述专利申请的全部内容通过引用并入本文。

## 技术领域

[0003] 本公开一般涉及管理利用远程设备对企业系统的访问。更特别地,公开了用于为了实现对企业系统的访问而统一远程设备和用户身份的管理的技术。公开了用于管理远程设备上的应用的供应以访问企业系统中的资源的技术。

## 背景技术

[0004] 随着设备(包括移动设备)的激增,许多企业正在采用“带自己的设备”(BYOD)策略。BYOD使得用户能够带他们自己的设备以连接到企业的系统,以便访问由企业提供的资源(例如,应用或数据)。BYOD策略可以允许用户为了个人使用而继续使用他们自己的设备。管理企业系统中用户拥有的设备的不同使用(例如,个人使用和公司使用)成为企业的首要关注点。允许用户自己的设备访问企业系统可能带来新的安全风险。一旦用户拥有的设备获得对企业系统的访问,则企业系统可能会暴露于来自非合规设备和设备的非合规使用的安全风险。企业系统可能面临寻找在用户拥有的设备上将个人数据与企业数据分开的方式的挑战。用户拥有的设备可能包含个人信息并且具有特殊的隐私考虑。许多用户拥有的设备可能缺乏使得这些设备能够被集成到企业系统中的企业安全控制。当用户拥有的设备受到威胁(例如,被黑、被盗或丢失)时,安全性变得更加令人关注。出于安全和合规性的原因,企业正在寻找新的和改进的方式来将用户拥有的设备与企业身份治理(governance)和访问控制基础设施集成。

[0005] 为了便于对访问企业系统的用户拥有的设备和公司设备的管理,一些企业可以实现移动设备管理(MDM)系统和/或移动应用管理(MAM)系统。这样的系统可以便于对访问企业系统的管理和控制,以确保企业系统及其资源是受保护的。对企业系统的访问的管理和控制可以包括传送关于合规性和资源的信息以及为了维持对企业系统的访问而必须采取的动作。

[0006] 具有成千上万个用户(例如,雇员、承包商和客户)的企业可能面临管理访问企业的成千上万个设备的访问和合规性的任务。用户可以操作不同的设备并且可以具有用于访问企业系统的不同角色。许多用户可能负担为企业系统管理访问和合规性,这往往可能是复杂的。使事情进一步复杂化的是,用户可能注册了不同类型的设备,这些不同类型的设备中的一些设备可能需要针对应用而被不同地配置。例如,可以基于支持应用的平台(例如,

操作系统)和/或设备的类型来不同地配置应用。对于操作多个设备的用户,这些用户面临跟踪影响用于访问企业系统中的资源的应用的配置的不同因素的挑战。企业使得用户遵守它们的策略并且配置用于访问由这些企业提供的资源的应用可能有困难。使事情进一步复杂化的是,用户可以依照个人使用而不同地操作设备,以致于企业面临确保与用户相关联的每个设备能够访问由企业提供的资源的方式的挑战。

[0007] 由于管理访问企业系统的设备的复杂性,企业和访问由企业提供的资源的用户不能例行地管理应用的配置。为了确保对企业系统的访问不受威胁,当访问资源的应用的配置已经改变时,企业可以完全限制或禁止对企业系统的访问。这样的改变可以由用户角色的改变或用于访问企业的策略(例如,访问策略或合规性策略)的改变而引起。一些应用可能需要被手动配置以合规。因此,用户可能有必须单独地调整其设备中的每个设备上的其应用的配置的负担。企业正在寻找管理使得设备能够访问企业系统中的资源的应用的配置的方式。

## 发明内容

[0008] 本公开一般涉及管理利用远程设备对企业系统的访问。更特别地,公开了用于为了实现对企业系统的访问而统一远程设备和用户身份的管理的技术。公开了用于供应远程设备上的应用以访问企业系统中的资源的技术。具体而言,可以将应用自动配置为具有访问信息(例如,帐户信息)和连接信息,以利用远程设备访问企业系统中的资源。经配置的应用可以使得远程设备的用户能够访问资源,而不必为了访问资源而手动配置应用。

[0009] 在一些实施例中,设备访问管理系统可以被实现以配置应用,以便利用远程设备访问资源。可以出于任何数量的原因来自动配置应用,这些原因包括为用户注册远程设备、接收访问资源的请求、发现对新资源的访问已被准许或者发现新应用。配置应用可以包括确定用于利用该应用访问资源的账户。可以为与要为其配置应用的远程设备相关联的用户确定账户。如果尚未为资源供应帐户,则可以基于用户的角色供应帐户以访问该资源。在一些实施例中,对资源的访问可以基于用户的角色而不同。通过确定用户的帐户,在配置应用以访问资源之前,用户不会负担检索帐户信息或请求帐户的附加过程。

[0010] 设备访问管理系统可以自动配置应用,以减少或消除用户可能必须通过其来配置应用的过程。通常,远程设备的属性(例如,设备的类型和设备的平台)可以不同,以使得取决于设备的属性,配置应用可以涉及不同的过程。用户可能不熟悉用于配置应用的不同过程。对于具有若干远程设备的用户,用户可能有必须配置这些远程设备中的每个远程设备上的应用的负担。企业可能同样有必须提供用于确保可以在为用户注册的远程设备中的每个远程设备上正确配置应用的机制的负担。设备访问管理系统可以对于为用户注册的远程设备中的每个远程设备将应用自动配置为至少具有访问信息(例如,帐户信息)和连接信息(例如,端口地址、主机地址或数据访问协议)。在一些实施例中,可以配置与应用的特征相关的一个或多个设置。可以基于用户的角色或用户的偏好来配置(一个或多个)设置。一旦配置了应用,则可以执行该应用以访问资源。用户可能必须提供机密访问信息(例如,密码),以利用已经被配置的应用来访问资源。用户和企业都可以不必手动配置应用以访问资源。

[0011] 在配置应用后,设备访问管理系统可以将经配置的应用发送到为其配置该应用的

(一个或多个)远程设备。在一些实施例中,可以利用推送通知服务将经配置的应用发送到远程设备。一旦接收到经配置的应用,该应用就可以被自动安装在远程设备上,之后可以执行该应用以访问资源。在一些实施例中,经配置的应用可以被存储在数据存储库(data store)(例如,应用目录)中,在该数据存储库中远程设备可以访问和/或检索应用。远程设备可以接收数据存储库中的应用的可用性的通知。在一些实施例中,应用的配置而不是经配置的应用可以被发送到远程设备。远程设备可以基于接收到的配置来配置应用。

[0012] 应用可以被配置为用于多个远程设备,这些远程设备可以被注册到不同的用户。在可以针对为用户注册的多个远程设备类似地配置应用的情况下,设备访问管理系统可以将应用发送到这些远程设备中的每个远程设备。通过为用户配置应用,企业可以确保向远程设备提供了当前应用,而用户不必采取措施来识别和获得用于这些远程设备中的每个远程设备的应用。为多个设备配置应用可以通过减少对企业系统的应用的请求总数来提高应用分发的处理效率。

[0013] 在发现对企业系统中的资源的访问的改变时,设备访问管理系统可以自动地修改提供对该资源的访问的应用的配置。访问的改变可以由任何数量的改变事件引起,这些改变事件包括但不限于一个或多个用户的用户角色的改变、对应用的更新、与策略的合规性的改变以及远程设备的配置的改变。设备访问管理系统可以基于改变为受该改变影响的一个或多个远程设备修改应用的配置。例如,当对资源的访问被撤销时,可以修改应用的配置以删除配置。在一些实施例中,设备访问管理系统可以向受改变影响的远程设备发送指令。该指令在其被接收时可以使远程设备基于访问的改变来修改应用的配置。当撤销对资源的访问时,指令可以指示远程设备移除提供对该资源的访问的应用。在发现对新资源的访问被准许时,可以为被注册到被允许访问所发现的资源的用户的远程设备配置应用。新配置的应用可以被发送到被允许安装经配置的应用的那些远程设备。

[0014] 本发明的一些实施例可以由计算系统来实现。计算系统可以被实现为设备访问管理系统的一部分。计算系统可以实现方法和操作。在至少一个实施例中,计算系统可以包括一个或多个处理器和存储指令的存储器,当指令由该一个或多个处理器执行时,使得该一个或多个处理器实现操作。可以实现操作以执行方法。在一些实施例中,非暂态计算机可读介质可以包括指令,当该指令由一个或多个处理器执行时,使得操作被执行。在一些实施例中,非暂态计算机可读介质可以保护计算机免于包含恶意代码的电子通信。在一个示例中,当存储在计算机可读介质上的指令由一个或多个处理器执行时,可以使得下文描述的方法和操作被实现。还有其它实施例涉及采用或存储用于下文描述的方法和操作的指令的系统和机器可读有形存储介质。

[0015] 在至少一个实施例中,方法可以由计算机系统实现。该方法可以包括为企业系统的用户识别与身份相关联的用户角色。该方法可以包括检索注册身份以访问企业系统的第一远程设备的设备信息。该方法可以包括基于用户角色确定向身份提供对企业系统中可访问的第一资源的访问的帐户。可以利用用户角色可访问的多个应用中的第一应用从第一远程设备来访问第一资源。该方法可以包括配置第一应用,以利用第一远程设备访问用于账户的第一资源。可以利用连接信息来配置第一应用,以连接到提供第一资源的第一目标系统。第一应用可以被配置为具有访问信息,以访问用于帐户的第一资源。该方法可以包括在配置第一应用后将第一应用发送到第一远程设备。

[0016] 在一些实施例中，设备信息指示第一远程设备的配置，该配置指示第一远程设备上的操作系统配置和第一远程设备的硬件配置。可以利用第一远程设备的配置来配置第一应用。

[0017] 在一些实施例中，连接信息包括第一目标系统的端口地址、第一目标系统的主机地址以及第一目标系统的轻量级目录访问协议(LDAP)。

[0018] 在一些实施例中，该方法可以包括检测注册身份以访问企业系统的多个远程设备中的第二远程设备。该方法可以包括在配置第一应用后将第一应用发送到第二远程设备。

[0019] 在一些实施例中，该方法可以包括检测用户角色从第一用户角色到第二用户角色的改变。该方法可以包括基于第二用户角色来确定身份对第一资源的访问的改变。对第一资源的访问的改变可以包括撤销对第一资源的访问。修改第一应用包括删除为第一应用配置的连接信息和访问信息。修改第一应用可以包括从第一远程设备移除第一应用。修改第一应用可以包括调整为第一应用配置的访问信息。该方法可以包括指示第一远程设备基于访问的改变来修改第一应用的配置。在至少一个实施例中，该方法可以包括发现注册身份以访问企业系统的多个远程设备。该方法可以包括在配置第一应用后将第一应用发送到多个远程设备。该方法可以包括指示多个远程设备中的每个远程设备基于访问的改变来修改第一应用的配置。

[0020] 在一些实施例中，该方法可以包括检测用户角色从第一用户角色到第二用户角色的改变。该方法可以包括基于第二用户角色来发现第二用户角色可访问的多个应用中的第二应用。该方法可以包括配置第二应用，以用于利用身份从第一远程设备进行访问。第二应用可以被配置为具有用于访问由第二目标系统提供的第二资源的信息。该方法可以包括将第二应用发送到第一远程设备。

[0021] 在一些实施例中，该方法可以包括基于用户角色来识别多个应用中的第二应用，第二应用使得用户能够执行用户角色。该方法可以包括供应第二应用，以访问企业系统中的第二资源。该方法可以包括配置第二应用，以从第一远程设备访问第二资源。该方法可以包括在配置第二应用后发送第二应用。

[0022] 在一些实施例中，确定帐户包括：确定是否为访问第一目标系统的第一资源供应帐户；在确定没有为访问第一资源供应帐户时，供应该帐户，以向身份提供对第一目标系统的第一资源的访问；以及在确定为身份供应该帐户时，检索关于该帐户的帐户信息。

[0023] 在至少一个实施例中，另一种方法可以由计算机系统实现。该方法可以包括为企业系统的用户识别与身份相关联的用户角色。该方法可以包括检索注册身份以访问企业系统的多个远程设备的设备信息。该方法可以包括基于用户角色来确定向该身份提供对企业系统中可访问的第一资源的访问的帐户。可以利用用户角色可访问的多个应用中的第一应用从多个远程设备来访问第一资源。该方法可以包括配置第一应用，以利用多个远程设备访问用于账户的第一资源。第一应用可以被配置为具有连接信息，以连接到提供第一资源的第一目标系统。第一应用可以被配置为具有访问信息，以访问用于帐户的第一资源。该方法可以包括在配置第一应用后将第一应用发送到多个远程设备中的每个远程设备。在一些实施例中，配置第一应用可以包括为多个远程设备中的每个远程设备配置第一应用的实例。可以基于远程设备的配置来为远程设备配置第一应用的实例。远程设备的配置可以包括远程设备的设备配置或操作系统配置中的一个或两者。可以为多个远程设备中的第一远

程设备和第二远程设备中的每一个不同地配置第一应用的实例。第一远程设备的配置可以不同于第二远程设备的配置。

[0024] 在至少一个实施例中，另一种方法可以由计算机系统实现。该方法可以包括为企业系统的用户识别与身份相关联的用户角色。该方法可以包括检索注册身份以访问企业系统的第一远程设备的设备信息。该方法可以包括基于用户角色来为该身份供应对多个应用的访问。多个应用中的每个应用可以被供应，以用于利用第一远程设备访问企业系统中的不同资源。该方法可以包括将多个应用中的第一应用配置为具有第一连接信息和第一访问信息，以从第一远程设备访问第一资源。该方法可以包括将多个应用中的第二应用配置为具有第二连接信息和第二访问信息，以从第一远程设备访问第二资源。该方法可以包括在配置第一应用后将第一应用发送到第一远程设备。该方法可以包括在配置第二应用后将第二应用发送到第一远程设备。

[0025] 在一些实施例中，该方法还可以包括检测用户角色从第一用户角色到第二用户角色的改变。该方法可以包括基于用户角色的改变来确定由身份对第二资源的访问被撤销以及由身份对第三资源的访问被允许。第一资源、第二资源和第三资源可以彼此不同。该方法可以包括基于确定对第二资源的访问被撤销来指示第一远程设备移除第二应用。该方法可以包括基于第二用户角色为该身份供应对第三应用的访问，第三应用提供从第一远程设备对企业系统中的第三资源的访问。该方法可以包括将多个应用中的第三应用配置为具有第三连接信息和第三访问信息，以从第一远程设备访问第三资源。该方法可以包括在配置第三应用后将第三应用发送到第一远程设备。为身份供应对应用的访问可以包括为该身份供应提供对应用可访问的资源的访问的帐户。

[0026] 通过参考以下说明书、权利要求和附图，前述内容以及其它特征和实施例将变得更加明显。

## 附图说明

[0027] 下面参考附图详细描述本发明的说明性实施例：

[0028] 图1绘出了根据本发明的一些实施例的、包括用于管理利用远程设备对企业系统的访问的设备访问管理系统的计算系统的简化的高级示意图。

[0029] 图2示出了根据本发明的一些实施例的设备访问管理系统的更详细的高级示意图。

[0030] 图3示出了根据本发明的一些实施例的、用于向远程设备供应应用的操作序列。

[0031] 图4示出了根据本发明的一些实施例的、用于向远程设备供应应用的操作序列。

[0032] 图5绘出了根据本发明的一些实施例的数据结构的示例，该数据结构用于存储指示企业系统中的角色可访问的资源的信息。

[0033] 图6绘出了根据本发明的一些实施例的数据结构的示例，该数据结构用于存储识别用于访问企业系统中的不同资源的应用的配置的信息。

[0034] 图7绘出了根据本发明的一些实施例的数据结构的示例，该数据结构用于存储关于被注册以访问企业系统的远程设备的信息。

[0035] 图8绘出了根据本发明的一些实施例的数据结构的示例，该数据结构用于存储识别用于远程设备的应用配置的状况的信息。

[0036] 图9是示出根据本发明的一些实施例的、用于向远程设备供应应用的过程的流程图。

[0037] 图10是示出根据本发明的一些实施例的、用于向远程设备供应应用的过程的流程图。

[0038] 图11绘出了用于实现实施例的分布式系统的简化图。

[0039] 图12是根据本公开的实施例的、其中服务可以作为云服务被提供的系统环境的一个或多个组件的简化框图。

[0040] 图13示出了可以被用来实现本发明的实施例的示例性计算机系统。

## 具体实施方式

[0041] 在下面的描述中，为了解释的目的，阐述了具体细节，以便提供对本发明的实施例的透彻理解。然而，将明显的是，可以在没有这些具体细节的情况下实践各种实施例。例如，为了不以不必要的细节使实施例模糊，电路、系统、算法、结构、技术、网络、过程和其它组件可以被示为框图形式的组件。附图和描述不旨在是限制性的。

[0042] 而且，要指出的是，各个实施例可以被描述为被描绘为流程图、流图、数据流图、结构图或框图的过程。虽然流程图可以将操作描述为顺序过程，但是这些操作中的许多操作可以并行地或并发地执行。此外，操作的顺序可以被重新安排。过程在其操作完成时终止，但是可以具有未包括在附图中的附加步骤。过程可以对应于方法、函数、程序(procedure)、子例程、子程序等。当过程对应于函数时，其终止可以对应于函数返回到调用函数或主函数。

[0043] 本公开一般涉及管理利用远程设备对企业系统的访问。更特别地，公开了用于为了实现对企业系统的访问而统一远程设备和用户身份的管理的技术。公开了用于供应远程设备上的应用以访问企业系统中的资源的技术。具体而言，应用可以被自动配置为具有访问信息(例如，帐户信息)和连接信息，以利用远程设备访问企业系统中的资源。经配置的应用可以使得远程设备的用户能够访问资源，而不必为了访问资源而手动配置应用。

[0044] 在一些实施例中，设备访问管理系统可以被实现为配置应用以利用远程设备访问资源。可以出于任何数量的原因而自动配置应用，这些原因包括为用户注册远程设备、接收访问资源的请求、发现对新资源的访问已被准许或者发现新应用。配置应用可以包括确定用于利用该应用来访问资源的账户。可以为与要为其配置应用的远程设备相关联的用户确定账户。如果尚未为该资源供应帐户，则可以基于用户的角色供应帐户以访问资源。在一些实施例中，对资源的访问可以基于用户的角色而不同。通过确定用户的帐户，在配置应用以访问资源之前，用户不会有检索帐户信息或请求帐户的附加过程的负担。

[0045] 设备访问管理系统可以自动配置应用，以减少或消除用户可能必须通过其配置应用的过程。通常，远程设备的属性(例如，设备的类型和设备的平台)可以不同，以使得取决于设备的属性，配置应用可以涉及不同的过程。用户可能不熟悉用于配置应用的不同过程。对于具有若干远程设备的用户，用户可能有必须配置这些远程设备中的每个远程设备上的应用的负担。企业可能同样有必须提供用于确保可以在为用户注册的远程设备中的每个远程设备上正确配置应用的机制的负担。设备访问管理系统可以对于为用户注册的远程设备中的每个远程设备将应用自动配置为至少具有访问信息(例如，帐户信息)和连接信息(例

如，端口地址、主机地址或数据访问协议)。在一些实施例中，可以配置与应用的特征相关的一个或多个设置。可以基于用户的角色或用户的偏好来配置(一个或多个)设置。一旦配置了应用，则可以执行该应用以访问资源。用户可能必须提供机密访问信息(例如，密码)，以利用已经被配置的应用来访问资源。用户和企业都可以不必手动配置应用以访问资源。

[0046] 在配置应用后，设备访问管理系统可以将经配置的应用发送到为其配置该应用的(一个或多个)远程设备。在一些实施例中，可以利用推送通知服务将经配置的应用发送到远程设备。一旦接收到经配置的应用，则可以在远程设备上自动安装该应用，之后可以执行该应用以访问资源。在一些实施例中，经配置的应用可以被存储在数据存储库(例如，应用目录)中，在数据存储库中远程设备可以访问和/或检索应用。远程设备可以接收数据存储库中的应用的可用性的通知。在一些实施例中，应用的配置而不是经配置的应用可以被发送到远程设备。远程设备可以基于接收到的配置来配置应用。

[0047] 应用可以被配置为用于多个远程设备，这些远程设备可以被注册到不同的用户。在可以针对为用户注册的多个远程设备类似地配置应用的情况下，设备访问管理系统可以将应用发送到这些远程设备中的每个远程设备。通过为用户配置应用，企业可以确保向远程设备提供当前应用，而用户不必采取措施来识别和获得用于这些远程设备中的每个远程设备的应用。为多个设备配置应用可以通过减少对企业系统的应用的请求总数来提高应用分发的处理效率。

[0048] 在发现对企业系统中的资源的访问的改变时，设备访问管理系统可以自动地修改提供对该资源的访问的应用的配置。访问的改变可以由任何数量的改变事件引起，这些改变事件包括但不限于一个或多个用户的用户角色的改变、对应用的更新、与策略的合规性的改变以及远程设备的配置的改变。基于改变，设备访问管理系统可以为受该改变影响的一个或多个远程设备修改应用的配置。例如，当对资源的访问被撤销时，可以修改应用的配置以删除配置。在一些实施例中，设备访问管理系统可以向受改变影响的远程设备发送指令。该指令在其被接收时可以使远程设备基于访问的改变来修改应用的配置。当撤销对资源的访问时，指令可以指示远程设备移除提供对该资源的访问的应用。在发现对新资源的访问被准许时，可以为被注册到被允许访问所发现的资源的用户的远程设备配置应用。新配置的应用可以被发送到被允许安装经配置的应用的那些远程设备。

[0049] 图1绘出了根据本发明的一些实施例的、用于管理利用远程设备对企业系统的访问的计算系统100的简化的高级示意图。具体而言，计算系统100可以统一对远程设备和用户身份的管理，以用于实现对企业系统的访问。计算系统100可以便于应用向远程设备的供应，以访问企业系统中的资源。图1中绘出的实施例仅仅是示例并且不旨在不适当地限制本发明的所要求保护的实施例。本领域的普通技术人员将认识到许多变化、替代和修改。

[0050] 计算系统100可以是为企业实现的企业系统的一部分。计算系统100可以包括企业计算机系统150，企业计算机系统150提供对由企业系统提供的一个或多个资源的访问。资源的示例可以包括硬件资源、软件资源(例如，应用)、数据资源、服务资源、地点、对象等。资源可以由企业计算机系统150提供，或者可以由第三方提供商托管并由企业计算机系统150提供给远程设备。在一些实施例中，资源可以由一个或多个目标系统提供，该一个或多个目标系统可以由企业计算机系统150或第三方提供商实现。例如，电子邮件服务可以由电子邮件服务系统提供给远程设备的用户。可以利用被配置为与电子邮件服务系统通信的应用来

从远程设备访问电子邮件服务。电子邮件服务系统可以包括在企业计算机系统150中或从企业计算机系统150可访问。

[0051] 用户可以利用诸如远程设备108-1、108-2、...108-N(统称为远程设备108)之类的一个或多个远程设备来访问企业计算系统150。利用远程设备108对企业计算机系统150的访问可以由设备访问管理系统120控制和管理。远程设备108中的每个远程设备可以包括安全容器应用。安全容器应用可以提供用于与设备访问管理系统120通信以访问企业计算机系统150的安全执行环境。远程设备108可以与设备访问管理系统120通信,以获得对由企业计算机系统150提供的资源的访问。

[0052] 设备访问管理系统120可以管理远程设备108的认证和登记(enrollment),以用于访问企业计算机系统150。远程设备108可以登记被注册以访问企业计算机系统150的用户身份。就像用户身份被用来认证用户一样,可以用被用来认证远程设备的身份来注册远程设备。身份可以被供应给远程设备并且可以被用来认证来自该远程设备的所有进一步通信。数据存储库160中的用户信息数据存储库172可以包括关于被注册以访问企业计算机系统150的用户的信息。该信息可以包括关于用户的用户身份信息。参考图5描述用户信息的示例。

[0053] 被注册以访问企业计算机系统150的用户可以注册远程设备108中的一个或多个远程设备,以访问企业计算机系统150。设备访问管理系统120可以提供用于针对企业计算机系统150的身份来注册远程设备的接口。例如,设备访问管理系统120可以向远程设备的用户提供图形用户界面(GUI),该图形用户界面使得远程设备的用户能够注册关于远程设备的信息,以与被注册以访问企业计算机系统150的该用户的身份相关联。设备访问管理系统120可以向远程设备发出证书,以用于利用用户身份来登记该远程设备以用于访问企业计算机系统150。如果请求来自与远程设备的身份相关联的用户身份,则设备访问管理系统120可以允许远程设备访问企业计算机系统150。

[0054] 设备访问管理系统120可以在“设备记录”中存储关于远程设备的设备信息。设备记录可以与指示注册该远程设备的用户的身份的用户信息相关联地存储。用户信息可以被存储在用户信息数据存储库172中。在一些实施例中,远程设备可以被注册到多个身份,这些身份中的每个身份可以与单个用户或不同用户相关联。设备记录可以被存储在设备注册表162中。参考图7描述用户信息和设备记录的示例。

[0055] 通过与用于访问企业计算机系统150的用户信息(例如,身份)相关联地存储设备信息,可以以统一的方式管理远程设备108和身份。被用来访问企业计算机系统150的远程设备可以基于远程设备的设备记录与用户的身份之间的关联利用用户的身份来识别。如下文所描述的,远程设备108与一个或多个身份之间的关联可以改进对利用远程设备108对企业计算机系统150的访问的管理。

[0056] 在一些实施例中,一个或多个远程设备108可以利用被配置为访问资源的应用来访问由企业计算机系统150提供的资源。设备访问管理系统120可以为与用户的身份相关联的远程设备供应应用。如下文进一步描述的,设备访问管理系统120可以配置被供应的应用,以用于与企业计算机系统150通信,以访问资源或与提供该资源的目标系统直接通信。应用可以被配置为用于在被注册到用户的身份的远程设备上操作。例如,应用可以被配置为具有访问信息(例如,用户身份、访问令牌或其它凭证信息)和连接信息(例如,主机服务

器、端口地址、通信信息或其它协议)，以用于与计算系统(例如，目标系统的计算系统)连接以访问企业计算机系统中的资源。供应提供对资源的访问的应用可以包括为从远程设备访问资源的用户的身份确定帐户。如果还没有为用户的身份供应帐户，则企业计算机系统150可以供应帐户以访问资源。为用户的身份配置的应用可以被发送到对于该身份被注册的远程设备。与该身份相关联的用户可以操作所配置的应用，以访问用于所供应的账户的资源。

[0057] 计算系统100可以由多个区定义，每个区对应于不同的通信区。在一些实施例中，远程设备108可以位于外部通信区(“外部区”)102中。设备访问管理系统120和企业计算机系统150可以位于绿色通信区(“绿色区”)106中。绿色区106可以包括一个或多个安全网络(例如，公司网络)。绿色区106可以位于企业计算环境的防火墙内部。外部区102可以是外部网络(例如，因特网)的一部分，该外部网络可以是不安全的。例如，外部区102可以位于绿色区106的防火墙外部。

[0058] 在一些实施例中，远程设备108可以通过位于非军事区(DMZ)104中的安全访问系统110与绿色区106中的计算机系统通信。DMZ104的示例可以是公司DMZ。安全访问系统110可以便于远程设备108和设备访问管理系统120之间的安全通信。例如，安全访问系统110可以提供远程设备108中的任何远程设备上的安全容器应用和设备访问管理系统120之间的安全通信连接(例如，隧道)。

[0059] 安全访问系统110可以提供认证远程设备的用户的服务。安全访问系统110可以与用户访问管理系统130通信，以获得对远程设备的用户的授权。例如，安全访问系统110可以从用户访问管理系统130获得授权令牌，以便于对由企业计算机系统150提供的资源的单点登录(SSO)认证。在一个示例中，安全访问系统110可以被包括在Oracle Mobile Security Access Server(Oracle移动安全访问服务器)中，Oracle移动安全访问服务器是Oracle®公司提供的Oracle Mobile Security Suite(Oracle移动安全套件)的一部分。

[0060] 远程设备108可以具有各种不同的类型，这些不同的类型包括但不限于端点设备、可穿戴设备(例如，智能手表)、消费者设备(例如，电器)、个人计算机、台式机、物联网(IOT)设备、移动设备或手持设备(诸如膝上型计算机、移动电话、平板电脑、计算机终端等)、以及其它类型的设备。在一些实施例中，远程设备可以是在计算设备(例如，移动设备、IOT网关或IOT边缘设备)上托管的应用。在一些实施例中，远程设备可以是在另一设备上运行的端点，诸如工作空间。工作空间可以是受控环境，以提供对运行该工作空间的设备上的企业数据和应用的访问。例如，安全容器应用可以在远程设备108中的一个或多个远程设备上运行。远程设备的示例可以包括但不限于由与企业计算机系统150相关联的企业发布的设备(例如，公司设备)或者用来访问企业计算机系统150的用户的个人设备(“BYOD设备”)。

[0061] 远程设备可以存储关于其身份的信息，例如，MAC(介质访问控制)地址、唯一设备标识符(UDID)或其它设备标识符。远程设备可以存储关于远程设备的元数据属性，包括远程设备上的操作系统的类型、操作系统的版本、主机标识符(如果远程设备在另一设备上托管)、设备类型、IMEI(国际移动设备身份)号码、远程设备的型号、远程设备的服务提供商(例如，运营商)、设备名称、设备状态、合规性状况或关于远程设备的其它信息。

[0062] 在一些实施例中，远程设备可以被配置为确定关于远程设备的设备信息。设备信息可以包括远程设备的操作的状态。操作的状态可以指示以下各项中的任何项：应用何时被安装、执行和/或卸载；远程设备中的硬件和/或软件是否已被更改；关于应用的信息(例

如,用于应用的密码);与远程设备的使用相关的活动或不活动;或者与远程设备的执行或使用相关的其它信息。远程设备可以被配置为与设备访问管理系统120通信。例如,远程设备可以周期性地与设备访问管理系统120同步(“设备同步”),以向设备访问管理系统120提供关于远程设备的设备信息。在一些实施例中,设备访问管理系统120可以基于从远程设备接收到的或未接收到的信息来确定关于远程设备的信息。

[0063] 在某些实施例中,远程设备可以被配置为实现(例如,执行和操作)一个或多个应用。例如,远程设备108中的一个或多个远程设备可以执行被设计为保持“容器化的”应用(即,已经被安全地链接到其具体容器的应用)的安全容器应用。应用的示例可以包括但不限于计算机应用、客户端应用、专有客户端应用、工作空间、容器等。在一些实施例中,由远程设备实现的应用可以经由一个或多个网络来访问或操作。由企业计算机系统150配置并且从企业计算机系统150接收的用于访问资源的应用可以在安全容器应用中被安装和执行。安全容器应用可以被配置为基于从设备访问管理系统120接收的指令来修改应用的配置。

[0064] 远程设备可以包括可以利用硬件、固件、软件或其组合来实现的计算设备。远程设备可以包括存储器和一个或多个处理器。存储器可以被耦接到(一个或多个)处理器并且可以包括存储在其上的指令,当这些指令由(一个或多个)处理器执行时,使得(一个或多个)处理器实现本文公开的一个或多个操作、方法或过程。存储器可以利用诸如计算机可读存储介质之类的任何类型的持久存储设备来实现。

[0065] 在一些实施例中,远程设备108可以经由具有各种类型的一个或多个通信网络可通信地耦接到设备访问管理系统120和企业计算机系统150。通信网络的示例包括但不限于因特网、广域网(WAN)、局域网(LAN)、以太网、公共或专用网络、有线网络、无线网络等、及其组合。可以使用不同的通信协议以便于通信,这些不同的通信协议包括有线协议和无线协议,诸如IEEE 802.XX协议组、TCP/IP、IPX、SAN、AppleTalk、**Bluetooth®**和其它协议。

[0066] 设备访问管理系统120可以在计算机系统中实现,该计算机系统可以包括一个或多个计算机和/或服务器,该一个或多个计算机和/或服务器可以是通用计算机、专用服务器计算机(举例来说,包括PC服务器、UNIX服务器、中型服务器、大型计算机、机架安装式服务器等)、服务器场、服务器集群、分布式服务器或任何其它适当的布置和/或其组合。例如,设备访问管理系统120可以包括服务器。服务器中的全部或一些可以位于相同的地理位置或不同的地理位置。构成设备访问管理系统120的计算设备可以运行操作系统中的任何操作系统或各种附加的服务器应用和/或中间层应用,这些附加的服务器应用和/或中间层应用包括HTTP服务器、FTP服务器、CGI服务器、Java服务器、数据库服务器等。示例性数据库服务器包括但不限于来自Oracle、Microsoft等的商用数据库服务器。设备访问管理系统120可以利用硬件、固件、软件或其组合来实现。在一个示例中,设备访问管理系统120可以被包括在Oracle移动安全管理器中,Oracle移动安全管理器是由Oracle公司提供的Oracle移动安全套件的一部分。

[0067] 设备访问管理系统120可以包括至少一个存储器、一个或多个处理单元(或(一个或多个)处理器)和存储装置。(一个或多个)处理单元可以在硬件、计算机可执行指令、固件或其组合中适当地实现。(一个或多个)处理单元的计算机可执行指令或固件实现可以包括以任何合适的编程语言编写的计算机可执行指令或机器可执行指令,以执行本文描述的各

种操作、功能、方法和/或过程。设备访问管理系统120中的存储器可以存储可以在(一个或多个)处理单元上加载和执行的程序指令以及在这些程序的执行期间生成的数据。存储器可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存存储器等)。存储器可以利用诸如计算机可读存储介质之类的任何类型的持久存储设备来实现。在一些实施例中,计算机可读存储介质可以被配置为保护计算机免于包含恶意代码的电子通信。计算机可读存储介质可以包括存储在其上的指令,当这些指令在处理器上被执行时,执行本文描述的操作。

[0068] 设备访问管理系统120还可以包括附加的存储装置或被耦接到附加的存储装置,该附加存储装置可以利用任何类型的持久存储设备(诸如存储器存储设备或其它非暂态计算机可读存储介质)来实现。在一些实施例中,本地存储装置可以包括或实现一个或多个数据库(例如,文档数据库、关系数据库或其它类型的数据库)、一个或多个文件存储库、一个或多个文件系统或其组合。例如,设备访问管理系统120可以被耦接到一个或多个数据存储库或可以包括一个或多个数据存储库,例如数据存储库160。存储器和附加存储装置都是计算机可读存储介质的示例。例如,计算机可读存储介质可以包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据之类的信息的任何方法或技术实现的易失性或非易失性、可移动或不可移动介质。

[0069] 设备访问管理系统120可以可通信地耦接到身份管理系统140。身份管理系统140可以管理企业计算机系统150的用户的生命周期以及为从企业计算机系统150访问的资源供应的他们的相关联的帐户。身份管理系统140可以管理为访问企业计算机系统150而定义的角色(例如,用户组)。在一些实施例中,身份管理系统140可以实现用于为访问企业计算机系统150而定义的角色的管理策略。用户信息数据存储库172可以包括从身份管理系统140获得的关于用户的信息。该信息可以包括与用户的身份相关联的一个或多个用户角色。身份管理系统140可以管理为访问企业计算机系统150而定义的(一个或多个)角色。身份管理系统140的示例可以包括由Oracle®公司提供的Oracle Identity Manager(Oracle身份管理器)。

[0070] 用户访问管理系统130可以可通信地耦接到设备访问管理系统120。用户访问管理系统130可以处理范围管理、授权令牌的发布、刷新令牌的发布、以及访问令牌的发布。例如,用户访问管理系统130可以处理来自安全访问系统110的对由远程设备108进行访问的请求。在一些实施例中,用户访问管理系统130可以管理用于访问由企业计算机系统150提供的资源的访问策略。用户访问管理系统130的示例可以包括由Oracle®公司提供的Oracle Access Manager(Oracle访问管理器)。

[0071] 在一些实施例中,设备访问管理系统120可以管理被登记以访问企业计算机系统150的远程设备108的设置。设置的示例可以包括但不限于设备设置、安装设置、同步设置、通信设置、应用设置、或者与访问企业系统相关的其它设置。关于设置的信息可以被存储在数据存储库160中。一些设置可以对应于从远程设备108接收的信息。用于一些远程设备108的设置(例如,设备设置和安装设置)可以由登记的远程设备108为了登记来验证并且为了合规性来检查。在一些实施例中,设置(例如,同步设置)可以被传送到一些远程设备108,以使得远程设备108上的安全容器应用能够配置与设备访问管理系统120和企业计算机系统150的通信的同步。

[0072] 可以利用一个或多个策略来管理利用远程设备108对企业计算机系统150的访问。策略可以被存储在数据存储库160中的策略数据存储库164中并且可以从策略数据存储库164访问。策略的示例可以包括但不限于登记策略、合规性策略、工作空间策略和设备策略。在一些实施例中，可以从企业计算机系统150、身份管理系统140和/或用户访问管理系统130接收关于合规性策略的信息。一个或多个策略可以基于从设备访问管理系统120的操作者(例如，管理员)接收的输入来配置。设备访问管理系统120可以确定远程设备108是否与策略合规。策略可以定义利用远程设备对企业计算机系统150的访问。在一些实施例中，设备访问管理系统120可以基于策略来执行补救动作，以调整远程设备的访问。设备访问管理系统120可以向远程设备传送指令，以指示远程设备根据策略响应于合规性而采取补救动作。通知可以被发送到远程设备108，以向它们通知与策略的合规和/或不合规以及合规的时间段。

[0073] 设备访问管理系统120可以管理实现对企业计算机系统150中的一个或多个资源的访问的一个或多个应用。应用可以被存储在应用数据存储库166中。应用数据存储库166可以由在远程设备上执行的安全容器应用访问。应用可以提供对企业计算机系统150中的一个或多个资源的访问。例如，电子邮件应用可以提供对由企业计算机系统150提供的电子邮件服务的访问。在另一个示例中，人力资源(HR)应用可以提供对由企业计算机系统150管理的人力资源数据的访问。

[0074] 如下文进一步讨论的，应用可以被供应给注册到用户的远程设备108中的一个或多个远程设备。可以出于各种原因来供应应用。例如，可以出于任何数量的原因来供应应用，所述任何数量的原因包括为用户注册远程设备、接收访问资源的请求、发现已准许对新资源的访问或者发现新应用。供应应用可以包括自动配置应用，以利用该应用来访问资源。

[0075] 为了供应应用，对于为用户注册的远程设备108中的每个远程设备，设备访问管理系统120可以将应用自动配置为至少具有访问信息(例如，帐户信息)和连接信息(例如，端口地址、主机地址或数据访问协议)。访问信息可以在数据存储库160的访问信息数据存储库168中被管理。连接信息可以在数据存储库160的连接信息数据存储库170中被管理。在一些实施例中，与应用的特征相关的一个或多个设置可以被配置。可以基于用户的角色或用户的偏好来配置(一个或多个)设置。设备访问管理系统120可以将经配置的应用存储在应用数据存储库166中。在一些实施例中，应用的配置可以被存储在应用配置174中。

[0076] 在一些实施例中，供应应用可以包括确定用于利用该应用来访问资源的账户。可以为与要为其配置应用的远程设备相关联的用户确定账户。如果尚未为资源供应帐户，则设备访问管理系统120可以基于用户的角色来供应帐户以访问资源。

[0077] 设备访问管理系统120可以利用各种技术向为其配置该应用的(一个或多个)远程设备自动提供经配置的应用。在一些实施例中，设备访问管理系统120可以向(一个或多个)远程设备提供应用的配置而不是整个应用。在一些实施例中，设备访问管理系统120可以使用推送通知服务来将经配置的应用提供给(一个或多个)远程设备。应用可以根据提供给远程设备的配置应用或应用的配置而被自动安装在远程设备上。

[0078] 通过向远程设备的用户提供经配置的应用，用户可能没有必须管理各个应用以访问资源的负担。此外，当新的应用变得可用时，可以自动向用户提供应用。通过消除对应用的单独请求，可以减少企业系统上的处理负载。当用户注册有多个远程设备时，可以向远程

设备中的每个远程设备供应包括帐户信息的经配置的应用。通过向远程设备供应应用，企业可以确保访问企业系统的远程设备被配置为具有满足企业的访问策略的应用。当企业系统中的访问改变时，远程设备可以利用经修改的应用而被自动更新，而不必评估合规性并且确定对资源的访问。在具有成千上万个远程设备的企业系统中，被配置为用于在多个远程设备上使用的应用可以被配置一次，并且被高效地分发到这些远程设备。

[0079] 现在转向图2，示出了根据本发明的一些实施例的设备访问管理系统120的更详细的高级示意图。如图2中所示，设备访问管理系统120可以包括若干子系统和/或模块，这些子系统和/或模块包括账户处理机232、应用配置管理器234、通信处理机236、访问管理器238和设备管理器240。这些子系统和模块可以以软件(例如，程序代码、可由处理器执行的指令)、硬件或其组合来实现。在一些实施例中，软件可以被存储在存储器(例如，非暂态计算机可读介质)中、存储设备或某些其它物理存储器上，并且可以由一个或多个处理单元(例如，一个或多个处理器、一个或多个处理器核心、一个或多个GPU等)执行。

[0080] 随着采用BYOD以用于实现对企业系统(例如，企业计算机系统150)的访问，许多用户可以利用他们的远程设备来访问企业系统。诸如端点设备210-1、...210-N(统称为端点设备210)之类的一个或多个远程设备可以被操作以访问企业计算机系统150。虽然图2绘出了被用来访问企业计算机系统150的一些远程设备，但是企业计算机系统150可以由成千上万的用户利用成千上万的远程设备来访问。可以通过包括设备访问管理系统120的计算系统(例如，计算系统100)来控制对企业系统的访问。远程设备可以被用来访问企业计算机系统150中的一个或多个资源。

[0081] 在图2所示的示例中，企业计算机系统150可以包括一个或多个目标系统或可以可通信地耦接到一个或多个目标系统，例如，目标系统250和目标系统260。目标系统250、260中的每个目标系统可以提供企业计算机系统150中的资源。例如，目标系统250可以提供资源252，而目标系统260可以提供资源262。对资源252、262中的每个资源的访问可以由为访问这些资源中的每个资源而供应的帐户来控制。

[0082] 端点设备210中的每个端点设备可以包括被配置为与设备访问管理系统120通信的安全容器应用。安全容器应用270可以不同于在远程设备上执行的其它应用(例如，外部浏览器280)。例如，端点设备210-2可以包括在端点设备210-2上执行的安全容器应用270。安全容器应用270可以被配置为与设备访问管理系统120通信。在一些实施例中，安全容器应用270可以被配置为基于用于访问企业计算机系统150的一个或多个策略来管理对企业计算机系统150的访问。安全容器应用270可以被配置为执行由设备访问管理系统120配置的应用。

[0083] 端点设备210-2可以执行设备同步通信(“设备同步(device synchronization)”或“设备同步(device sync)”)，以将关于端点设备210-2的设备信息传送到设备访问管理系统120。端点设备210-2可以周期性地与设备访问管理系统120同步。在一些实施例中，设备访问管理系统120可以发起与一个或多个远程设备(例如，端点设备210)的设备同步。

[0084] 在一些实施例中，端点设备210中的每个端点设备可以访问存储在数据存储库160中的信息，以配置应用以便访问来自远程设备的资源。在一些实施例中，安全容器应用270可以被配置为基于来自设备访问管理系统120的指令来执行一个或多个操作(例如，配置应用以访问企业计算机系统150中的资源)。

[0085] 在成千上万个远程设备访问企业系统的情况下，为这些远程设备配置应用以访问企业系统中的资源可能难以管理。实现对资源的访问的应用可能需要被配置为遵守治理(govern)对企业计算机系统150中的这些资源的访问的一个或多个策略。可以基于一个或多个因素来不同地配置实现对资源的访问的应用，该一个或多个因素包括但不限于设备属性、连接属性、用户角色或正在访问的资源的类型。照此，可以针对为用户注册的多个远程设备中的一个或多个远程设备不同地配置应用。基于企业系统中发生的改变事件来调整用于访问资源的应用的配置甚至更困难。

[0086] 对资源的访问可以基于企业计算机系统150中的改变事件的发生而改变。改变事件可以对应于与访问企业系统的改变相关的事件。对资源(例如，资源252或资源262)的访问可以基于与改变事件对应的访问的改变而改变。改变事件的示例可以包括但不限于基于与策略不合规的对企业计算机系统150的访问的改变、远程设备上的改变(例如，远程设备上的硬件或软件的修改)、与远程设备相关联的用户角色的改变、对企业计算机系统150中的资源的被准许的访问的改变、以及影响对企业计算机系统150的访问的其它改变。为了克服配置用于成千上万个远程设备的应用的这些障碍和许多其它障碍，设备访问管理系统120可以自动配置应用，以使得远程设备能够访问企业计算机系统150中的资源。应用的配置可以基于影响利用该应用对资源的访问的改变事件来修改。

[0087] 设备管理器240可以管理远程设备(例如，端点设备210)对企业计算机系统150的访问。具体而言，设备管理器240可以基于一个或多个登记策略来管理远程设备对于访问企业计算机系统150的登记。设备管理器240可以处理与远程设备的通信。通信可以包括远程设备与设备访问管理系统120之间的同步(“设备同步”)。设备同步可以包括关于远程设备的设备信息从远程设备到设备访问管理系统120的传送。设备信息可以被存储在设备注册表162中的设备记录中。用于远程设备的设备信息可以被用来配置用于在该远程设备上执行的应用。设备管理器240可以发现被注册以访问企业计算机系统150的新的远程设备。

[0088] 设备管理器240可以检测何时设备信息指示与所注册的远程设备中的改变对应的改变事件。对远程设备的改变的示例可以包括但不限于调整远程设备上的硬件的配置或者在远程设备上安装应用或移除应用。设备管理器240可以确定远程设备是否与治理对企业计算机系统150的访问的一个或多个策略合规。

[0089] 访问管理器238可以实现或可以便于与身份管理系统(例如，身份管理系统140)和用户访问管理系统(例如，用户访问管理系统130)的通信。可以从身份管理系统140获得包括与用户身份相关联的(一个或多个)角色的用户信息。访问管理器238可以接收关于与访问企业计算机系统150的改变相关的改变事件的信息。例如，访问管理器238可以从身份管理系统140接收指示用户角色从一个用户角色到另一个用户角色的变化的信息。用户角色的改变可以对应于用户角色与用户的身份的关联或者用户角色与用户的身份的解除关联。

[0090] 访问管理器238可以从用户访问管理系统130接收指示对企业计算机系统150的访问的改变的信息。访问的改变可以对应于对资源的访问的改变已经被撤销或准许。对资源的访问可以基于策略的改变而改变。访问的改变可以对应于对于一个或多个角色的访问的改变。对资源的访问的改变可以影响被注册到其访问受该改变影响的用户的远程设备对资源的访问。在一些实施例中，关于对资源的访问的信息可以利用参考图5描述的技术来存储。这样的信息可以从用户访问管理系统130获得。该信息可以指示关于一个或多个用户角

色被允许或不被允许的资源。访问管理器238可以使用该信息来基于用户角色确定对资源的访问。

[0091] 通信处理机236可以管理设备访问管理系统120与远程设备(例如,端点设备210)之间的消息(例如,消息208)的传送。通信处理机236可以接收来自端点设备210的请求。请求可以包括对从目标系统访问资源的请求或者对用于从目标系统访问资源的应用的请求。通信处理机236可以从端点设备210接收为了设备同步而传送的信息。该信息可以包括设备信息。设备信息可以包括指示改变事件的信息,该改变事件诸如远程设备的操作或配置的改变或者合规性的改变。

[0092] 通过通信系统290可以便于端点设备210和设备访问管理系统120之间的消息(例如,请求)的传送。通信系统290可以提供发送、接收、存储和/或访问“消息”的服务,其中“消息”可以包括由发送者生成并且被指引到一个或多个接收者的任何电子讯息,诸如电子邮件消息、即时消息(例如,在利用各种“聊天”服务的用户之间发送的消息)、SMS/MMS消息(例如,符合由各种蜂窝网络和其它无线数据网络支持的短消息传送服务协议和/或多媒体消息传送服务协议的消息)、语音消息、照片/图像消息、社交网络消息,等等。消息传送服务的示例可以包括诸如Gmail™(Google公司的服务)和Yahoo®Mail(Yahoo!公司的服务)之类的电子邮件服务。其它示例可以包括即时消息传送或聊天服务,诸如Gmail的聊天特征或Facebook的聊天(Facebook公司的服务)、由蜂窝数据运营商提供的SMS/MMS服务、具有消息传送组件的社交网络服务(例如,由Facebook公司或LinkedIn公司提供的社交网络)。通信系统290可以提供用于便于设备访问管理系统120和端点设备210之间的通信的基于web的客户端接口、专用应用程序、应用程序接口(API)和/或其它工具。

[0093] 通信系统290可以经由具有各种类型的一个或多个通信网络(例如,网络292)与端点设备通信。通信网络的示例包括但不限于因特网、WAN、LAN、以太网网络、公共或专用网络、有线网络、无线网络等、及其组合。不同的通信协议可以被用来便于包括有线协议和无线协议(诸如IEEE 802.XX协议组、TCP/IP、IPX、SAN、AppleTalk、Bluetooth®和其它协议)的通信。

[0094] 为了配置应用,帐户处理机232可以处理确定是否已经向用户供应帐户以用于访问用于用户的身份的资源。帐户处理机232可以访问用户信息数据存储库172,以便为已经被准许访问资源的每个身份识别帐户(如果存在的话)。在确定尚未为用户供应帐户时,帐户处理机232可以与企业计算机系统150通信,以便为用户供应帐户。在一些实施例中,账户处理机232可以与目标系统直接通信,以供应账户。可以在应用中配置关于帐户的信息。

[0095] 应用配置管理器234可以确定是否配置用于访问资源(例如,资源262或资源252)的应用。在许多不同的情况下可以为远程设备配置应用,这些情况包括但不限于从远程设备接收访问利用应用可访问的资源的请求、新远程设备的注册以及对资源的访问的改变。例如,用户角色的改变可以使得用户能够访问一个或多个资源。在一些实例中,多个应用可以被定义为与角色相关联的组。可以为被指派了与该组相关联的角色的用户供应该多个应用。在一些实施例中,可以在检测到远程设备处的改变事件时为远程设备配置应用。改变事件可以对应于远程设备的不合规或者远程设备的操作或使用的改变(例如,调整远程设备的配置)。一旦被配置,则在确定利用应用对资源的访问的后续改变时可以修改该应用的配置。基于对资源的被允许的访问,可以为不同用户不同地配置提供对资源的访问的应用。

[0096] 应用配置管理器234可以访问应用数据存储库166，以检索要配置的应用，以提供对用于用户身份的资源的访问。应用可以被配置为提供对资源的访问或撤销对资源的访问。应用配置管理器234可以访问应用配置数据存储库174，以识别一个或多个应用的配置。可以针对不同的标准定义应用配置，这些标准包括但不限于设备属性、资源、用户角色、特征和设置。在一些实施例中，应用的配置可以基于上述一个或多个标准来预定义。例如，可以基于提供资源的计算系统来预定义用于应用的连接信息。

[0097] 应用配置管理器234可以基于对利用应用可访问的资源的被允许的访问来为被注册到用户的一个或多个远程设备配置该应用。可以利用各种技术来配置应用。应用的配置可以被部分地预定义。应用的配置可以被存储在应用配置数据存储库174中。应用配置管理器234可以利用参考图6描述的技术来存储应用配置。

[0098] 一种技术可以包括修改用于应用的代码(例如，执行代码)，以指示一个或多个连接属性，以用于建立到提供资源的计算系统(例如，目标系统)的连接。例如，用于应用的代码可以被配置为具有指示为了资源要访问的计算系统的统一资源定位符(URL)。URL可以指示可以被用来连接到计算系统的一个或多个连接属性。在一些实施例中，可以基于应用的经修改的代码来再生应用。连接属性的示例可以包括但不限于计算系统的端口地址、计算系统的主机地址、计算系统支持的一个或多个访问协议或者用于定义与计算系统的连接的其它属性。在一些实施例中，由应用访问的配置文件可以被配置为具有用于一个或多个连接属性的值。配置文件可以被存储在执行期间应用可访问的存储器中，或者可以被包括在用于应用的代码中。在一些实施例中，可以在为应用存储配置的应用配置数据存储库174中引用应用的配置。在一些实施例中，应用可以提供用于应用的动态配置的接口(例如，应用编程接口)。接口可以接受用于应用的配置的一个或多个属性。

[0099] 应用配置管理器234可以配置用于应用的一个或多个访问属性。访问属性可以被用来确定来自应用的对资源的访问。可以利用上文描述的配置技术中的一个或多个配置技术将应用配置为具有用于一个或多个访问属性的访问信息。访问属性的示例可以包括但不限于用来确定对资源的访问的帐户标识符、用户的访问令牌、凭证信息以及其它信息。访问管理器238可以获得用于由注册用户访问资源的访问信息。

[0100] 在一些实施例中，应用配置管理器234可以配置应用的一个或多个设置。应用的设置可以对应于应用的一个或多个特征。可以利用上文描述的配置技术中的一个或多个配置技术来配置设置。可以针对对于用户来说被允许的对资源的访问来配置设置。例如，一个或多个设置可以被配置为基于被允许的对资源的访问来启用或禁用应用中的特征。在另一个示例中，可以基于一个或多个设备属性为应用配置设置。在一些实施例中，可以基于设备属性(例如，远程设备的类型或远程设备上的平台)不同地配置应用中的设置。

[0101] 应用配置管理器234可以在确定已经发生改变事件(例如，应用对资源的访问已经改变)时修改应用的配置。在检测到与对资源的访问的改变相关的改变事件时，应用配置管理器234可以调整或撤销对资源的访问。可以基于访问的改变来配置一个或多个连接属性、一个或多个访问属性和/或一个或多个设置。可以利用上文描述的技术中的一个或多个技术来修改应用的配置。例如，当利用应用对资源的访问被撤销时，可以删除为该应用配置的一个或多个连接属性和/或一个或多个访问属性。在一些实施例中，当对资源的访问被撤销时，可以从远程设备完全移除应用。应用配置管理器234可以利用通信处理机236来向远程

设备传送指令，以请求远程设备移除应用。在其它示例中，当准许对资源的访问时，可以相应地配置应用以访问该资源。在一些实施例中，可以对于一个或多个设置修改应用的配置，以启用提供对附加资源的访问的特征。

[0102] 应用配置管理器234可以利用参考图8描述的技术来管理用于远程设备的经配置的应用的状况。应用的配置的状况可以被用来确定是否修改应用的配置。

[0103] 应用一旦被配置，就可以利用各种技术被提供给远程设备。在一些实施例中，经配置的整个应用可以被发送到对于用户被注册的一个或多个远程设备。通信处理机236可以将经配置的应用发送到一个或多个远程设备。例如，通信处理机236可以将一个或多个经配置的应用204发送到端点设备210-2，并且可以将一个或多个经配置的应用206发送到端点设备210-1。经配置的应用204和经配置的应用206中的每一个可以被供应，以用于访问相同的或不同的资源。

[0104] 在一些实施例中，通信处理机236可以经由通信系统290向远程设备提供经配置的应用。通信系统290可以实现推送通知服务(例如，由**Apple®**公司提供的Apple推送通知服务或者由**Google®**公司提供的Google通知服务)。推送通知服务可以便于通过网络292与远程设备(例如，端点设备210)的通信。推送通知服务可以将经配置的应用递送到端点设备。端点设备210可以被配置为针对推送通知来检查网络292并且拉取包括关于经配置的应用的通知的任何这样的通知。

[0105] 在一些实施例中，可以向端点设备210提供应用的配置而不是整个应用。通过利用上文描述的技术，通信处理机236可以发送配置，该配置可以通过发送指示应用的配置的通知或者指示可以在应用配置数据存储库174中访问配置的通知而被发送到端点设备。在端点设备上执行的安全容器应用可以使用或访问该配置并且可以基于该配置来配置应用。在一些实施例中，如果应用还没有被安装在端点设备上，安全容器应用可以首先检索应用，并且然后可以配置应用。在一些实施例中，可以利用指示经配置的应用位于数据存储库160中的信息来发送通知。例如，经配置的应用可以被存储在可以通过接口(例如，应用目录)来访问的应用数据存储库166中。通知可以被传送到端点设备，以通知端点设备在应用数据存储库166中一个或多个经配置的应用可用。端点设备上的安全容器应用可以访问应用数据存储库166，以检索经配置的应用。

[0106] 在图2所示的示例中，端点设备210-2可以接收经配置的应用204。安全容器应用270可以安装经配置的应用204，以用于在安全容器应用270中执行。经配置的应用204可以被配置为具有指示用于一个或多个连接属性(例如，目标系统的端口地址和目标系统的主机地址)的值的连接信息212。经配置的应用204可以被配置为具有用于一个或多个访问属性(例如，用于资源的帐户信息和访问令牌)的访问信息208。与端点设备210-2相关联的用户可以操作端点设备210-2，以使用经配置的应用204来访问由连接信息识别出的目标系统中的资源。在一些实施例中，可以请求用户提供凭证，以利用由访问信息208配置的帐户来访问资源。

[0107] 现在转向图3，示出了根据本发明的一些实施例的、用于向远程设备供应应用的操作序列300的示例。在这个示例中，多个远程设备(例如，端点设备302、304和306)可以登记以访问企业系统(例如，企业计算机系统150)。在图3所示的示例中，端点设备302、304、306中的每一个被描述为注册有用于企业系统的用户的身份。

[0108] 操作序列300可以由来自注册用户的身份以访问企业系统的远程设备(例如,端点设备302)的请求310发起。为了访问企业系统中的资源或应用,请求310可以被传送。

[0109] 设备访问管理系统120可以响应于请求310来执行操作312。设备访问管理系统120可以识别或者在请求310中指示或者提供对由请求310指示的一个或多个资源的访问的一个或多个应用。识别出的(一个或多个)应用可以被配置为利用与请求310相关联的远程设备来访问企业系统中的资源。应用可以被配置为具有使得账户能够访问企业系统中的资源的访问信息。应用可以被配置为具有使得执行应用的远程设备能够连接到提供对资源的访问的目标系统的连接信息。在一些实施例中,可以基于远程设备的配置(例如,远程设备的类型或远程设备的平台)来为远程设备配置应用。在一些实施例中,实现对资源的访问的应用可以具有不同的版本,每个版本对应于远程设备的不同配置。

[0110] 在图3所示的示例中,可以向注册了请求310的用户的身份的多个端点设备提供经配置的应用。请求(例如请求310)可以从注册用户的身份的一个远程设备接收,并且作为响应,经配置的应用可以被分发到注册该身份的远程设备。例如,由设备访问管理系统120响应于请求310而配置的应用可以分别被发送314、316到端点设备302和端点设备304中的每一个。可以向用户提供接收被配置用于用户注册的远程设备中的所有远程设备的应用的好处,而不必在该用户注册的每个远程设备上单独地请求和配置应用。可以基于注册的每个远程设备的配置来具体地配置应用。用户可以操作他注册的远程设备中的任何远程设备,以利用经配置的应用来访问资源。企业系统可以通过减少每个注册的设备对应用的单独请求的数量来提高其处理效率。相反,设备访问管理系统120可以配置一次应用并且将它分发到所有远程设备。

[0111] 在一些实施例中,设备访问管理系统120可以发现320已经向企业系统注册了用户的身份(例如,端点设备302、304注册的身份)的一个或多个远程设备(例如,远程设备306)。可以通过设备注册表162中设备信息(例如,设备记录)的添加来发现远程设备。设备信息可以与用户的身份相关联。在应用已经被配置并且被发送到注册了同一身份的其它远程设备之后,(一个或多个)远程设备可以被发现。例如,在经配置的应用被发送到被注册到身份的其它远程设备之后,可以发现新注册的远程设备注册了用户的该身份。

[0112] 在发现注册的远程设备时,先前为其它远程设备配置的应用可以被发送322到所发现的远程设备。在一些实施例中,设备访问管理系统120可以利用上文描述的技术为所发现的(一个或多个)远程设备配置应用。

[0113] 在一些实施例中,设备访问管理系统120可以检测330企业系统中的改变事件。改变事件可以是影响用户的身份对资源的访问的事件。例如,改变事件可以对应于用户角色从一个用户角色到另一个用户角色的改变。在另一个示例中,改变事件可以对应于用于用户角色的访问策略的改变。照此,对资源的访问可以基于改变事件而改变。对资源的访问的改变的示例可以包括但不限于撤销对资源的访问和准许对新资源的访问。基于由身份对资源的访问的改变,可以为注册该身份的远程设备修改332提供对资源的访问的应用的配置。例如,当撤销对资源的访问时,可以修改应用的配置以删除使得应用能够访问资源的连接信息。在一些实施例中,可以基于改变事件来修改先前被配置并且被发送到远程设备的应用的配置。在图3的示例中,可以基于访问的改变来修改之前由操作312配置的应用的配置。设备访问管理系统120可以分别向端点设备302、端点设备304和端点设备306中的每一个发

送334、336、338对应用的配置的修改。在一些实施例中，应用可以被重新配置，并且整个应用可以被发送到端点设备302、304、306。

[0114] 在一些实施例中，设备访问管理系统120可以发现340一个或多个应用以访问企业系统。例如，设备访问管理系统120可以发现可以提供对被指派给身份的一个或多个用户角色可访问的资源的访问的应用。在另一个示例中，设备访问管理系统120可以发现实现对新资源的访问的新应用。

[0115] 设备访问管理系统120可以执行操作342，以配置由设备访问管理系统120发现340的应用。在一些实施例中，如果应用实现对先前没有供应对其的访问的资源的访问，则设备访问管理系统120可以为与端点设备302、304、306相关联的身份供应帐户以访问该资源。可以基于与身份相关联的一个或多个用户角色来供应帐户。可以基于该一个或多个用户角色来确定对资源的访问。在一些实施例中，设备访问管理系统120可以识别提供对利用所发现的应用可访问的资源的访问的帐户。所发现的应用可以被配置为利用注册了该身份的(一个或多个)远程设备(例如，端点设备302、304、306)来访问资源。

[0116] 一旦所发现的应用被配置，则设备访问管理系统120可以发送该应用。经配置的应用可以被发送344、346、348到注册了用户的身份的端点设备302、端点设备304和端点设备306中的每一个。

[0117] 在一些实施例中，设备访问管理系统120可以基于企业系统中发生的不同类型的改变事件来修改应用的配置。从图3中的示例继续，图4示出了根据本发明的一些实施例的、其中设备访问管理系统120可以向远程设备供应应用的操作序列400的示例。具体而言，图4中的示例示出了设备访问管理120可以执行以基于改变事件来配置应用的操作，所述改变事件中的每个改变事件可以影响对企业系统的访问。可以从从被注册以访问企业系统的远程设备接收的信息检测改变事件。改变事件可以由设备访问管理系统120基于从企业系统或支持企业系统的一个或多个其它系统(例如，身份管理系统140和用户访问管理系统130)接收的信息来检测。在这个示例中，操作400可以在操作300在图4所示的示例中已经被执行之后发生。在一些实施例中，基于何时检测到改变事件，操作400中的全部或一些可以与操作300并发地发生。

[0118] 设备访问管理系统120可以接收来自一个或多个远程设备的指示改变事件(例如，合规性事件或设备事件)的信息。例如，设备访问管理系统120可以从端点设备304接收关于设备事件420的信息。信息420可以指示端点设备304处的改变，该改变可能影响对企业系统的访问。在一些实施例中，信息420可以包括可以被用来识别端点设备304中的改变的设备信息。例如，端点设备304中的改变可以对应于端点设备304的硬件的改变(例如，在端点设备304上执行的越狱(jail-breaking))、端点设备304的软件的改变(例如，被列入黑名单的应用的安装或升级到不支持的操作系统)或者端点设备304的操作和/或使用的其它改变。在另一个示例中，设备访问管理系统120可以从端点设备302接收关于合规性事件的信息422。信息422可以由在远程设备上执行的安全容器应用来确定。关于合规性事件的信息422可以包括可以被用来评估远程设备的合规性的设备同步信息。在一些实施例中，关于合规性事件的信息可以指示远程设备的合规或不合规。

[0119] 设备访问管理系统120可以执行操作430，以检测用于远程设备(例如，端点设备302、304、306)中的一个或多个远程设备的改变事件。可以基于从远程设备接收的信息(例

如，信息420或信息422)来检测改变事件。在一些实施例中，设备访问管理系统120可以基于从企业系统或者支持企业系统的一个或多个其它系统(例如，身份管理系统140和用户访问管理系统130)接收的信息来检测改变事件。该信息可以指示改变事件或者可以被用来检测改变事件。例如，该信息可以指示与注册了端点设备302、304、306的用户的身份相关联的用户角色的改变。在另一个示例中，该信息可以指示用于资源的访问策略的改变。改变事件可以引起对企业系统的访问的改变。访问的改变可以改变对从为用户注册的远程设备可访问的资源的访问。

[0120] 可以修改这些远程设备上的应用的配置，以调整对受检测到的改变事件影响的资源的访问。访问的改变可以包括准许或拒绝对资源或资源的一个或多个特征的访问。设备访问管理系统120可以执行操作432，以基于改变事件来确定是否需要修改端点设备302、304、306中的任何端点设备上的应用的配置以反映访问。在一些实施例中，可以在注册到用户的所有远程设备或一些远程设备上修改应用的配置。在一个示例中，当改变事件是与由合规性策略定义的不合规相关的合规性事件时，设备访问管理系统120可以基于合规性策略来确定对(一个或多个)资源的访问。

[0121] 基于可访问的资源，设备访问管理系统120可以确定如下应用：该应用可以被配置为访问与为端点设备302、304、306中的每个端点设备注册的身份相关联的(一个或多个)用户角色可访问的资源。一些远程设备可以不受改变事件的影响，因为这些远程设备不具有受改变影响的应用。对于安装在端点设备上的(一个或多个)应用，设备访问管理系统120可以根据对于(一个或多个)用户角色所允许的访问来自动修改该(一个或多个)应用的配置。可以修改应用的配置，以允许或拒绝对由应用访问的资源的访问。可以通过添加或删除与应用的设置的配置相关的访问信息、连接信息或其它信息来修改应用的配置。在一些实施例中，可以基于由于改变事件而被允许的访问来为资源配置新应用。修改应用的配置可以包括修改未安装在远程设备上的新应用的配置。可以通过包括访问信息和连接信息来修改新应用的配置。

[0122] 在修改应用的配置后，设备访问管理系统120可以将经修改的(一个或多个)应用或(一个或多个)应用的经修改的配置发送到受改变事件影响的远程设备。在一些实施例中，为用户注册的所有远程设备(例如，端点设备302、304、306)可以受改变事件的影响。例如，设备访问管理系统120可以分别向端点设备302、端点设备304和端点设备306中的每一个发送434、436、438应用的经修改的配置。

[0123] 通过基于改变事件来自动修改应用的配置并且使得利用经修改的配置来更新远程设备，用户可以没有必须基于改变事件来手动请求更新后的应用的负担。在一些实施例中，用户可能不知道改变事件，以使得当访问远程设备上的应用时，用户可能发现访问不被允许。通过自动提供经修改的配置，如果被允许，则用户可以通过利用被自动配置的应用来访问资源。因为用户可能已经注册了不同类型的远程设备，这些远程设备中的一些远程设备可以针对同一应用被不同地配置，所以用户可以没有必须获得并且单独地配置受改变事件影响的应用的每个实例的负担。

[0124] 图5绘出了根据本发明的一些实施例的数据结构510的示例，该数据结构510用于存储指示企业系统(例如，企业计算机系统150)中的角色可访问的资源的信息。数据结构510中的信息可以指示为了访问企业系统而被定义的一个或多个用户角色所允许和/或不

允许的一个或多个资源。数据结构510中的信息可以被用来确定提供对在数据结构510中识别出的资源的访问的应用的配置。

[0125] 数据结构510可以被实现为不同类型的数据结构中的一个类型的数据结构或不同类型的数据结构的组合，所述不同类型的数据结构包括但不限于数组、记录、关系数据库表、散列表、链表或其它类型的数据结构。为了说明的目的，数据结构510以具有特定数量的字段(例如，字段512和514)的布置示出；然而，数据结构510可以由与示出的不同的布置中的更多或更少的字段来定义。数据结构510的每个实例可以被存储在访问信息数据存储库168中。

[0126] 数据结构510中的字段512(“用户角色”)可以包括指示为了访问企业系统而被定义的一个或多个用户角色的信息。字段514(“允许的资源”)可以包括指示允许由在字段512中指示的用户角色访问的一个或多个资源的信息。在一些实施例中，数据结构510可以包括指示对于一个或多个用户角色来说被拒绝的一个或多个资源。在一些实施例中，可以基于用户角色来控制对由资源提供的特征的访问。数据结构510可以指示对于一个或多个用户角色来说被允许或被拒绝的(一个或多个)特征。在一些实施例中，可以基于一个或多个策略(例如，合规性策略)来确定数据结构510中的信息。在一些实施例中，可以访问策略以确定用户角色对一个或多个资源的被许可的访问。

[0127] 在图5所示的示例中，数据结构510中的条目520可以指示用于字段512的“管理员”角色并且可以指示包括“VPN服务”、“Outlook电子邮件服务”和“人力资源服务”的允许的资源514。数据结构510中的条目530可以指示用于字段512的“执行官(executive)”角色并且可以指示包括“Outlook电子邮件服务”和“人力资源服务”的允许的资源514。数据结构510中的条目540可以指示用于字段512的“雇员”角色并且可以指示包括“Outlook电子邮件服务”的允许的资源514。

[0128] 图6绘出了根据本发明的一些实施例的数据结构610的示例，该数据结构610用于存储识别用于访问企业系统(例如，企业计算机系统150)中的不同资源的应用的配置的信息。

[0129] 数据结构610可以被实现为不同类型的数据结构中的一种类型的数据结构或不同类型的数据结构的组合，所述不同类型的数据结构包括但不限于数组、记录、关系数据库表、散列表、链表或其它类型的数据结构。为了说明的目的，数据结构610以具有特定数量的字段(例如，字段612-616)的布置示出；然而，数据结构610可以由与示出的不同的布置中的更多或更少的字段来定义。数据结构610的每个实例可以被存储在应用配置数据存储库174中。设备访问管理系统120可以访问应用配置数据存储库174，以检索要被配置的应用的配置。

[0130] 数据结构610中的信息可以指示提供对企业系统中的资源的访问的一个或多个应用。数据结构610包括如下连接信息：该连接信息指示用于提供对资源的访问的应用的连接信息的配置。在一些实施例中，可以创建数据结构610的实例，以用于为企业系统中的身份存储应用的配置。

[0131] 虽然未被示出，但是数据结构610可以包括用于特定于一个或多个标准的应用的配置的连接信息，其中该一个或多个标准特定于远程设备。例如，用于应用的配置的连接信息可以基于远程设备的类型、远程设备上支持的平台、远程设备的硬件配置、远程设备的软

件配置或者与远程设备的操作和/或使用相关的信息来定义。

[0132] 在一些实施例中，数据结构610可以包括关于利用应用可访问的资源的该应用的一个或多个设置的配置。设置可以对应于提供对资源的访问的应用的特征。在一些实施例中，可以为将使用应用来访问资源的一个或多个用户角色配置设置。

[0133] 数据结构610中的字段612(“(一个或多个)应用”)可以包括指示为其在数据结构610中存储配置的应用的信息。字段614(“(一个或多个)资源”)可以包括指示利用由字段612指示的应用可访问的资源的信息。

[0134] 数据结构610中的字段616(“连接信息”)可以包括指示用于由字段612指示的应用的配置的一个或多个连接属性的信息。在一些实施例中，连接属性可以基于特定于设备的标准(诸如远程设备的设备类型或平台)来定义。在一些实施例中，用于不同应用的连接信息可以被存储在连接信息数据存储库170中。连接信息可以指示用于应用的配置的一个或多个连接属性的值。连接信息可以指示基于特定于设备的标准的用于连接属性的值。数据结构610的每个实例可以被存储在访问信息数据存储库168中。

[0135] 在图6所示的示例中，数据结构610中的条目620可以指示用于“Outlook电子邮件服务”(字段614)的“电子邮件应用”(字段612)的配置。字段616可以指示用于电子邮件应用的连接信息。字段616中的连接信息可以指示用于连接属性的值，该连接属性诸如提供电子邮件服务的电子邮件服务系统的端口地址、电子邮件服务系统的主机地址以及电子邮件服务系统的LDAP。

[0136] 数据结构610中的条目630可以指示用于“VPN服务”(字段614)的“VPN应用”(字段612)的配置。字段616可以指示用于VPN应用的连接信息。字段616中的连接信息可以指示用于连接属性的值，该连接属性诸如提供VPN服务的VPN服务系统的端口地址以及VPN服务系统的主机地址。

[0137] 数据结构610中的条目640可以指示用于“人力资源(HR)服务”(字段614)的“HR应用”(字段612)的配置。字段616可以指示用于HR应用的连接信息。字段616中的连接信息可以指示用于连接属性的值，该连接属性诸如提供HR服务的HR服务系统的端口地址以及HR服务系统的主机地址。

[0138] 现在转向图7，绘出了数据结构710的示例。根据本发明的一些实施例，数据结构710可以存储关于被注册以访问企业系统的远程设备的信息。可以创建类似数据结构710的一个或多个数据结构，以存储关于多个远程设备的信息。为了配置用于远程设备的应用，可以考虑存储在数据结构710中的用于远程设备的信息。数据结构710可以存储关于用于在数据结构710中识别出的每个远程设备的一个或多个应用的配置的信息。

[0139] 数据结构710可以被实现为不同类型的数据结构中的一种类型的数据结构或不同类型的数据结构的组合，该不同类型的数据结构包括但不限于数组、记录、关系数据库表、散列表、链表或其它类型的数据结构。为了说明的目的，数据结构710以具有特定数量的字段(例如，字段712-728)的布置示出；然而，数据结构710可以由与示出的不同的布置中的更多或更少的字段来定义。数据结构710的每个实例可以被存储在诸如设备注册表162之类的数据存储库中。

[0140] 数据结构710可以存储用于被注册以访问企业系统的每个远程设备的设备记录。每个条目(例如，条目730和条目740)可以是设备记录。

[0141] 字段712(“设备标识符”)可以指示远程设备的设备标识符。设备标识符的示例可以包括但不限于远程设备的硬件设备标识符、为了向企业系统注册远程设备而生成的令牌、UDID或者可以与远程设备相关联并且可以从注册的其它远程设备中唯一地识别远程设备的其它类型的标识符。条目730可以包括被注册以访问企业系统的第一远程设备的设备标识符(例如,“AX1759UGJKY”),而条目740可以包括被注册以访问企业系统的第二远程设备的设备标识符(例如,“AX1759UGJKK”)。

[0142] 字段714(“平台版本”)可以包括识别在远程设备上配置的平台的版本的信息。平台版本的示例包括但不限于安装在远程设备上的操作系统(OS)版本、安装在远程设备上的硬件平台或者安装在远程设备上的用于远程设备的操作的其它软件。条目730中的字段714可以指示远程设备上的OS版本(“iOS 7.0.1”),而条目740中的字段714可以指示另一个远程设备上的OS版本(“Android 5.0.1”)。

[0143] 字段716(“地理位置”)可以指示远程设备的地理位置。例如,条目730、740中的每个条目中的字段716可以包括指示与该条目对应的远程设备的最后已知的物理地理位置的坐标(例如,经度坐标和纬度坐标)的信息。地理位置可以由包括在远程设备中或可由远程设备访问的全球定位系统(GPS)来确定。

[0144] 字段718(“主机标识符”)可以指示主机系统的标识符。例如,当远程设备是在另一个设备(“主机设备”)上托管的端点时,主机标识符可以指示该主机设备的标识符。主机设备的设备标识符是主机标识符的一个示例。在一些实施例中,可以为远程设备注册主机设备,并且可以基于主机设备的合规性来评估远程设备的合规性。

[0145] 数据结构710的一个或多个字段可以包括描述远程设备的信息。例如,条目730中的字段720(“显示名称”)可以指示对应于条目730的远程设备的显示名称(例如,“User1_Device1”),而条目740中的字段720可以指示对应于条目740的远程设备的显示名称(例如,“User2_Device2”)。可以在远程设备的登记期间提供关于远程设备的描述性信息。该描述性信息可以被用来将为用户注册的一个远程设备与为该用户注册的其它远程设备区分开。字段722(“设备类型”)可以指示与设备记录对应的远程设备的类型。设备类型的示例可以包括移动电话、台式计算机、智能电话或可穿戴设备。

[0146] 在一些实施例中,设备记录可以与为了访问企业系统而建立的用户身份相关联。如上文所解释的,远程设备可以被注册,以供一个或多个用户身份使用以访问企业系统。用来注册远程设备的用户身份可以与用于该远程设备的设备记录相关联。例如,字段724可以包括指示与为了访问企业系统而建立的一个或多个用户身份的用户关联的信息。字段724可以包括指示存储装置中用户身份信息的位置。在图7所示的示例中,条目730、740中的每个条目中的字段724可以包括对存储器中存储数据结构760的位置的引用。数据结构760可以包括与如下用户身份对应的用户身份信息:该用户身份与由条目730、740中的每个条目识别出的远程设备相关联。

[0147] 用户身份可以由身份管理系统(例如,身份管理系统140)来建立。数据结构760可以由身份管理系统创建和管理。数据结构760可以被存储在设备访问管理系统120可访问的用户信息数据存储库172中。在一些实施例中,设备访问管理系统120可以与身份管理系统140通信,以获得与远程设备相关联的用户身份信息。图7中示出的是存储关于用户身份的数据的数据结构760的示例。数据结构760可以包括指示用户身份(例如,User_1)的字段762

(“用户身份”)。数据结构760还可以包括与用户身份的注册相关的数据。例如,数据结构760中的字段764可以指示与用户身份相关联的一个或多个角色。数据结构760可以包括指示用于访问一个或多个资源的一个或多个帐户的字段766。每个帐户可以被注册到用户身份。例如,帐户766可以指示提供对电子邮件服务的访问的帐户的用户身份(例如,User_ID)。

[0148] 基于由字段724指示的用户身份关联,可以从数据结构760为远程设备相关联的用户身份确定一个或多个角色。该(一个或多个)角色可以被用来确定远程设备的合规性。

[0149] 在一些实施例中,可以为远程设备将合规性信息存储在数据结构710中。合规性信息可以与访问企业系统的远程设备的合规性相关。数据结构710中的字段726可以包括合规性状况信息,该合规性状况信息指示由数据结构710识别出的远程设备的合规性状况。

[0150] 字段728可以包括关于由数据结构710中的记录识别出的远程设备上的应用的(一个或多个)配置的信息。例如,字段728可以指示远程设备上的应用的配置的状况。在另一个示例中,字段728可以包括指示远程设备上的每个应用的配置的信息。例如,条目730中的字段728可以指示关于由条目730识别出的远程设备上的电子邮件应用的配置,并且可以指示在该远程设备上没有配置VPN应用。条目740中的字段728可以指示由条目740识别出的远程设备上的电子邮件应用被移除,并且可以指示在该远程设备上没有配置VPN应用。在一些实施例中,字段728可以包括指示对包括远程设备上的一个或多个应用的配置的另一个数据结构(例如,下文描述的图8中的数据结构)的存储器中的位置的引用的信息。

[0151] 图8示出了根据本发明的一些实施例的数据结构810的示例,该数据结构810用于存储识别用于远程设备的应用配置的状况的信息。可以创建类似数据结构810的一个或多个数据结构来存储关于多个远程设备上的应用的配置的信息。数据结构810可以存储指示在针对用户的身份被注册的一个或多个远程设备上的一个或多个应用的配置和/或配置状况的信息。在一些实施例中,当用户被指派多个用户角色时,可以基于与用户相关联的不同用户角色来识别关于应用的配置的信息。

[0152] 数据结构810可以被实现为不同类型的数据结构中的一种类型的数据结构或不同类型的数据结构的组合,该不同类型的数据结构包括但不限于数组、记录、关系数据库表、散列表、链表或其它类型的数据结构。为了说明的目的,数据结构810以具有特定数量的字段(例如,字段8-12-818)的布置示出;然而,数据结构810可以由与示出的不同的布置中的更多或更少的字段来定义。数据结构810的每个实例可以被存储在诸如设备注册表162或应用配置数据存储库174之类的数据存储库中。

[0153] 字段812可以包括指示远程设备上的应用的配置的状况的信息。配置的状况可以指示应用是否被安装在远程设备上,并且如果应用被安装在远程设备上,则还指示应用是否被配置。

[0154] 字段814可以包括为由字段812识别出的应用配置的访问信息。访问信息的示例可以包括但不限于用于访问使用由字段812指示的应用可访问的资源的用户ID、访问令牌或其它信息。

[0155] 字段816可以指示基于其配置由字段812识别出的应用的一个或多个用户角色。在一些实施例中,当由字段816指示的(一个或多个)用户角色不被允许访问由应用提供的资源时,该应用可以不被配置或者可以被移除。

[0156] 字段818可以包括用于由字段818指示的应用的连接信息。连接信息可以指示用于

为由字段812识别出的应用配置的一个或多个连接属性中的每个连接属性的值。当应用没有在远程设备上被配置时，字段818可以不指示连接信息。

[0157] 图8示出了存储在数据结构810中的、用于注册了用户的身份的远程设备的信息的示例。在一个示例中，条目820的字段812指示远程设备上的电子邮件应用被配置。电子邮件应用为了执行官角色而被配置。电子邮件应用被配置为具有访问信息814(例如，电子邮件服务的user_ID)和连接信息818。用于条目820的连接信息818可以指示电子邮件服务系统的端口地址、电子邮件服务系统的主机地址以及电子邮件服务系统的LDAP。在另一个示例中，条目830的字段812指示已经为与针对远程设备而被注册的身份相关联的执行官角色从远程设备移除VPN应用。因为VPN已经被移除，所以访问信息814和连接信息818可以包括空值。

[0158] 图9是示出根据本发明的一些实施例的、用于向远程设备供应应用的过程的流程图900。在一些实施例中，可以利用本文描述的设备访问管理系统120来实现图9中绘出的过程。

[0159] 由流程图900绘出的过程可以在由一个或多个处理单元(例如，处理器核心)执行的软件(例如，代码、指令、程序)、硬件或其组合中实现。软件可以被存储在存储器中(例如，在存储器设备上、在非暂态计算机可读存储介质上)。流程图900的处理步骤的特定序列不旨在是限制性的。根据替代实施例还可以执行其它步骤序列。例如，本发明的替代实施例可以以不同的顺序执行上文概述的步骤。另外，图9中所示的各个步骤可以包括可以以对于各个步骤适当的各种序列来执行的多个子步骤。此外，取决于特定应用，可以添加或移除附加步骤。虽然图9中绘出的处理是关于访问企业系统中的资源的单个应用，但是处理可以对实现对资源的访问的任何数量的应用和从应用可访问的任何数量的资源执行。虽然图9中绘出的处理是关于与用户的身份相关联的单个角色，但是处理可以对与身份相关联的多个角色执行。本领域普通技术人员将认识到许多变化、修改和替代物。

[0160] 在步骤902处，通过为企业系统的用户识别与身份相关联的用户角色，发起流程图900中的处理。例如，设备访问管理系统120可以访问用户信息数据存储库172，以确定与用户的身份相关联的用户角色。用户信息数据存储库172中的用户信息可以指示被供应给用户以访问企业系统的一个或多个身份以及被指派给这些身份的一个或多个角色。一个或多个角色可以被指派给用户的身份。可以基于被指派给用户的角色来定义对企业系统的访问。用户可以是操作远程设备以访问企业系统的人。例如，用户可以操作远程设备，以请求访问企业系统中的资源。在另一个示例中，用户可以是已经登记了远程设备以访问企业系统的人。

[0161] 在步骤904处，可以为被注册以访问企业系统的一个或多个远程设备检索设备信息。远程设备可能已经注册了对于企业系统的用户被注册的身份(例如，与在步骤902处识别出的用户角色相关联的身份)。例如，设备访问管理系统120可以访问设备注册表162，以获得关于注册身份以访问企业系统的一个或多个远程设备的设备信息。设备信息可以指示注册用户的身份的远程设备的配置。配置可以指示远程设备上的操作系统配置和远程设备的硬件配置。远程设备的配置可以被用来配置应用以访问资源。

[0162] 在步骤906处，可以确定向身份提供对企业系统中可访问的资源的访问的帐户。可以基于与身份相关联的用户角色(例如，在步骤902处识别出的用户角色)来确定帐户。可以

为企业系统中可访问的一个或多个资源供应帐户。可以基于与身份相关联的(一个或多个)用户角色来确定对资源的访问。对于向身份提供对资源的访问的帐户,注册了该身份的一个或多个远程设备可以访问该资源。可以利用一个或多个应用来访问资源。基于用户角色可访问的资源,应用可以是用户角色可访问的。

[0163] 在一些实施例中,可以访问访问信息数据存储库(例如,访问信息数据存储库168),以确定是否向用户的身份供应了任何帐户以用于访问由目标系统提供的资源。如上文所解释的,企业系统中的资源可以由目标系统提供。在确定为用户的身份供应了帐户时,可以从访问信息数据存储库检索帐户信息,在访问信息数据存储库中帐户信息识别向用户的身份供应的帐户。在确定没有为用户的身份供应帐户时,可以供应帐户,以向该身份提供对由目标系统提供的资源的访问。

[0164] 在步骤908处,应用可以被配置为利用注册了用户的身份的一个或多个远程设备来访问用于账户的资源(例如,在步骤906处针对其供应了账户的资源)。可以从在步骤904处检索出的设备信息中识别(一个或多个)远程设备。应用可以使得用户能够从注册了用户的身份的远程设备访问资源。例如,消息传送应用可以被配置为利用远程设备来访问用于消息传送账户的消息传送服务,其中该远程设备被注册到与账户相关联的用户。应用可以被配置为具有连接信息,以连接到提供资源的目标系统。连接信息的示例包括目标系统的端口地址、目标系统的主机地址以及目标系统的LDAP。应用可以被配置为具有用于利用账户访问资源的访问信息。访问信息的示例包括识别访问相关的信息的用户身份、访问令牌或其它信息。

[0165] 在配置应用后,在步骤910处可以将应用发送到为其配置了该应用的远程设备。在一些实施例中,可以在请求访问应用或请求访问利用应用可访问的资源时,将该应用发送到远程设备。例如,可以在从识别远程设备可访问的一个或多个应用的应用目录中进行选择时,将应用发送到远程设备。应用可以由设备访问管理系统存储并且在请求时被发送。

[0166] 在步骤912处,检测用与身份相关联的户角色(例如,在步骤902处识别出的用户角色)的改变。该身份可以属于远程设备被注册到的用户。用户角色的改变可以对应于从一个用户角色到另一个用户角色的改变。例如,用户角色的改变可以对应于新用户角色向用户的身份的指派。用户角色的改变可以对应于移除被指派给用户的身份的用户角色。可以访问用户信息数据存储库172中的用户信息,以确定与用户相关联的用户角色。在一些实施例中,可以从身份管理系统140获得关于用户角色的改变的信息。

[0167] 在步骤914处,可以确定身份对资源的访问的改变。可以基于用户角色的改变来确定访问的改变。可以基于被允许访问资源的用户角色来供应对资源的访问。身份对资源的访问可以基于用户角色的改变而改变。例如,可以基于失去用户角色(例如,管理用户角色)的指派来撤销或限制对资源(例如,人力资源应用)的访问。在另一个示例中,可以基于允许访问资源的新用户角色(例如,管理用户角色)的指派来准许对资源(例如,人力资源应用)的访问。

[0168] 在步骤916处,可以指示一个或多个远程设备(例如,注册用户的身份的(一个或多个)远程设备)基于访问的改变(例如,在步骤914处确定的访问的改变)来修改应用的配置。对利用应用可访问的资源的访问可以基于与用户的身份相关联的用户角色的改变而改变。作为对资源的访问的改变的结果,可能必须修改提供对资源的访问的应用的配置。可以为

与受用户角色的改变影响的身份相关联的远程设备上的应用修改配置。配置可以被修改，以调整对资源的访问或阻止对资源的访问。

[0169] 可以以许多方式来修改应用的配置。应用的配置可以针对与使用应用以访问资源相关的它的访问信息、连接信息或其它配置进行修改。例如，修改可以包括删除应用中的连接信息，以阻止对资源的访问。指示远程设备修改应用的配置可以包括发送包括指示对配置的修改的指令的消息。该指令可以使得远程设备根据该指令来修改配置。在一些实施例中，指示远程设备修改应用的配置可以包括根据对应于访问的改变的修改来配置应用，并且将经配置的应用发送到远程设备，从而指示要利用经配置的应用来修改远程设备上的应用。

[0170] 流程图900中的处理可以在步骤918处结束。

[0171] 图10是示出根据本发明的一些实施例的、用于向远程设备供应应用的过程的流程图1000。在一些实施例中，图10中绘出的过程可以利用本文描述的设备访问管理系统120来实现。

[0172] 由流程图1000绘出的过程可以在由一个或多个处理单元(例如，处理器核心)执行的软件(例如，代码、指令、程序)、硬件或其组合中实现。软件可以被存储在存储器中(例如，在存储器设备上、在非暂态计算机可读存储介质上)。流程图1000的处理步骤的特定序列不旨在是限制性的。根据替代实施例还可以执行其它步骤序列。例如，本发明的替代实施例可以以不同的顺序执行上文概述的步骤。另外，图10中所示的各个步骤可以包括可以以对于各个步骤适当的各种序列来执行的多个子步骤。此外，取决于特定应用，可以添加或移除附加步骤。虽然图10中绘出的处理是关于访问企业系统中的资源的单个应用，但是处理可以对应用可访问的任何数量的资源执行。虽然图10中绘出的处理是关于与用户的身份相关联的单个角色，但是处理可以对与身份相关联的多个角色执行。本领域普通技术人员将认识到许多变化、修改和替代物。

[0173] 在步骤1002处，通过为企业系统的用户识别与身份相关联的用户角色，发起流程图1000中的处理。在步骤1004处，可以为被注册以访问企业系统的一个或多个远程设备检索设备信息。

[0174] 在步骤1006处，为身份供应对多个应用的访问，其中该多个应用中的每个应用为了利用被注册以访问企业系统的远程设备对企业系统中的不同资源的访问而被供应。不同的资源中的每个资源可以是该身份可访问的。不同的资源可以被识别为与该身份相关联的所识别出的用户角色可访问的那些资源。多个应用中的每个应用可以被识别为提供对不同资源中的一种资源的访问的应用。

[0175] 供应对应用的访问可以包括向身份供应提供对应用可访问的资源的访问的账户。可以请求企业系统供应对应用可访问的不同资源中的每种资源的访问。在一些实施例中，可以请求提供对资源的访问的目标系统来供应用于该身份的帐户。人力资源系统可以便于资源的供应。资源可以是为该身份识别出的(一个或多个)用户角色可访问的。

[0176] 在步骤1008处，供应访问的多个应用中的每个应用可以被配置为具有连接信息和访问信息，以利用远程设备从该应用访问资源。应用可以被配置为具有连接信息，以连接到提供资源的目标系统。应用可以被配置为具有访问信息，以利用为了访问资源而供应的帐户来访问资源。

[0177] 在步骤1010处，经配置的多个应用中的每个应用可以被发送到被注册以访问企业系统的远程设备。在一个示例中，经配置的应用可以被发送，以被存储在存储器(例如，与应用目录相关联的存储装置)中，其中该应用可以由远程设备检索。在另一个示例中，经配置的应用可以被发送到为其配置了该应用的远程设备。

[0178] 在步骤1012处，可以确定身份对一个或多个资源的访问的改变。可以基于用户角色的改变来确定访问的改变。可以基于被允许访问资源的用户角色来供应对资源的访问。身份对资源的访问可以基于与该身份相关联的用户角色的改变而改变。例如，对于被指派给用户的身份的用户角色，对资源的访问可以被撤销。在另一个示例中，可以为被指派给用户的身份的用户角色准许对新资源的访问。

[0179] 在步骤1014处，可以指示一个或多个远程设备(例如，注册了用户的身份的(一个或多个)远程设备)基于访问的改变(例如，在步骤1012处确定的访问的改变)来修改应用的配置。例如，可以指示远程设备修改应用的配置，以阻止对基于用户角色的改变已经被撤销的资源的访问。

[0180] 在一些实施例中，远程设备可以不具有提供对用户的身份被准许访问的新资源的访问的应用。在步骤1016处，可以基于用户角色的改变来供应身份对新应用的访问。如上文所解释的，资源可以是其用户角色已改变的身份可访问的。照此，可以识别使得用户的身份能够访问资源的新应用。向身份供应对新应用的访问包括供应为该身份提供对新应用的访问的帐户。在步骤1018处，新应用可以被配置为具有连接信息和访问信息，以利用被注册到该身份的远程设备从应用访问资源。在步骤1020处，经配置的新应用可以被发送到远程设备。

[0181] 流程图1000中的处理可以在步骤1022处结束。

[0182] 在图11所绘出的配置中，系统1100的软件组件1118、1120和1122被示为在服务器1112上实现。在其它实施例中，系统1100的组件中的一个或多个组件和/或由这些组件提供的服务也可以由客户端计算设备1102、1104、1106和/或1108中的一个或多个实现。然后，操作客户端计算设备的用户可以利用一个或多个客户端应用来使用由这些组件提供的服务。这些组件可以在硬件、固件、软件或其组合中实现。应当理解的是，可以不同于分布式系统1100的各种不同的系统配置是可能的。因此，图11中所示的实施例是用于实现实施例系统的分布式系统的一个示例，并且不旨在是限制性的。

[0183] 客户端计算设备1102、1104、1106和/或1108可以包括各种类型的计算系统。例如，客户端计算设备可以包括运行诸如Microsoft Windows**Mobile®**之类的软件，和/或诸如iOS、Windows Phone、Android、BlackBerry 10，Palm OS等之类的各种移动操作系统的便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如，Google**Glass®**头戴式显示器)。设备可以支持各种应用(诸如各种因特网相关的应用、电子邮件、短消息服务(SMS)应用)，并且可以使用各种其它通信协议。客户端计算设备还可以包括通用个人计算机，举例来说，包括运行各种版本的Microsoft **Windows®**、Apple**Macintosh®**和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行包括但不限于各种GNU/Linux操作系统(诸如像Google Chrome OS)的各种商用的**UNIX®**或类UNIX操作系统中的任何操作系统的工作站计算机。客户端计算设备还可以包括能够经(一个或多个)网络1110通信的电子设备，诸如瘦客

户端计算机、启用因特网的游戏系统(例如,具有或不具有Kinect®姿势输入设备的Microsoft Xbox游戏机)和/或个人消息传送设备。

[0184] 虽然图11中的分布式系统1100被示为具有四个客户端计算设备,但是任何数量的客户端计算设备可以被支持。诸如具有传感器的设备等之类的其它设备可以与服务器1112交互。

[0185] 分布式系统1100中的(一个或多个)网络1110可以是本领域技术人员熟悉的可以利用各种可用协议中的任何可用协议来支持数据通信的任何类型的网络,其中各种可用协议包括但不限于TCP/IP(传输控制协议/因特网协议)、SNA(系统网络架构)、IPX(因特网分组交换)、AppleTalk等。仅仅作为示例,(一个或多个)网络1110可以是局域网(LAN)、基于以太网的网络、令牌环、广域网、因特网、虚拟网络、虚拟专用网络(VPN)、内联网、外联网、公共交换电话网络(PSTN)、红外网络、无线网络(例如,在电气和电子协会(IEEE)802.11协议组中的任何协议、Bluetooth®、和/或任何其它无线协议下操作的网络)和/或这些网络和/或其它网络的任何组合。

[0186] 服务器1112可以包括一个或多个通用计算机、专用服务器计算机(举例来说,包括PC(个人计算机)服务器、UNIX®服务器、中型服务器、大型计算机、机架安装式服务器等)、服务器场、服务器集群或任何其它适当的布置和/或组合。服务器1112可以包括运行虚拟操作系统的一个或多个虚拟机或涉及虚拟化的其它计算架构。一个或多个灵活的逻辑存储设备池可以被虚拟化,以维护用于服务器的虚拟存储设备。虚拟网络可以由服务器1112利用软件定义网络来控制。在各种实施例中,服务器1112可以适于运行在前述公开内容中描述的一个或多个服务或软件应用。例如,服务器1112可以对应于用于根据本公开的实施例执行如上文描述的处理的服务器。

[0187] 服务器1112可以运行包括上文讨论的操作系统中的任何操作系统的操作系统以及任何商用的服务器操作系统。服务器1112还可以运行各种附加的服务器应用和/或中间层应用中的任何服务器应用和/或中间层应用,这些附加的服务器应用和/或中间层应用包括HTTP(超文本传输协议)服务器、FTP(文件传输协议)服务器、CGI(公共网关接口)服务器、JAVA®服务器、数据库服务器等。示例性数据库服务器包括但不限于来自Oracle、Microsoft、Sybase、IBM(国际商业机器)等的商用数据库服务器。

[0188] 在一些实施方式中,服务器1112可以包括一个或多个应用,以分析和整合从客户端计算设备1102、1104、1106和1108的用户接收到的数据馈送和/或事件更新。作为示例,数据馈送和/或事件更新可以包括但不限于从一个或多个第三方信息源和持续数据流接收到的Twitter®馈送、Facebook®更新或实时更新,该持续数据流可以包括与传感器数据应用、金融报价机、网络性能测量工具(例如,网络监视和业务管理应用)、点击流分析工具、汽车交通监视等相关的实时事件。服务器1112还可以包括经由客户端计算设备1102、1104、1106和1108的一个或多个显示设备显示数据馈送和/或实时事件的一个或多个应用。

[0189] 分布式系统1100还可以包括一个或多个数据库1114和1116。这些数据库可以提供用于存储诸如用户交互信息、使用模式信息、适配规则信息、以及由本发明的实施例使用的其它信息之类的信息的机制。数据库1114和1116可以驻留在各种位置中。作为示例,数据库1114和1116中的一个或多个可以驻留在服务器1112本地(和/或驻留在服务器1112中)的非暂态存储介质上。可替代地,数据库1114和1116可以远离服务器1112,并且经由基于网络的

或专用的连接与服务器1112通信。在一组实施例中，数据库1114和1116可以驻留在存储区域网络(SAN)中。类似地，用于执行属于服务器1112的功能的任何必要的文件可以适当地在服务器1112本地存储和/或远程存储。在一组实施例中，数据库1114和1116可以包括适于响应于SQL格式的命令来存储、更新和检索数据的关系数据库，诸如由Oracle提供的数据库。

[0190] 在一些实施例中，云环境可以提供用于管理利用远程设备对企业系统的访问的一个或多个服务。图12是根据本公开的实施例的其中服务可以作为云服务被提供的系统环境1200的一个或多个组件的简化框图。在图12所示的实施例中，系统环境1200包括一个或多个客户端计算设备1204、1206和1208，该一个或多个客户端计算设备可以被用户用来与提供云服务(包括用于管理利用远程设备对企业系统的访问的服务)的云基础设施系统1202交互。云基础设施系统1202可以包括一个或多个计算机和/或服务器，该一个或多个计算机和/或服务器可以包括上文针对服务器1112所描述的计算机和/或服务器。

[0191] 应当理解的是，图12中所绘出的云基础设施系统1202可以具有除了所绘出的组件之外的其它组件。另外，图12中所示的实施例仅仅是可以结合本发明的实施例的云基础设施系统的一个示例。在一些其它实施例中，云基础设施系统1202可以具有比图中示出的更多或更少的组件、可以组合两个或更多个组件或者可以具有不同的组件配置或布置。

[0192] 客户端计算设备1204、1206和1208可以是与上文针对客户端计算设备1102、1104、1106和1108描述的设备类似的设备。客户端计算设备1204、1206和1208可被配置为操作客户端应用(诸如web浏览器、专有客户端应用(例如，Oracle Forms)或某些其它应用)，该客户端应用可以被客户端计算设备的用户用来与云基础设施系统1202交互，以使用由云基础设施系统1202提供的服务。虽然示例性系统环境1200被示为具有三个客户端计算设备，但是可以支持任何数量的客户端计算设备。诸如具有传感器的设备等之类的其它设备可以与云基础设施系统1202交互。

[0193] (一个或多个)网络1210可以便于客户端计算设备1204、1206和1208与云基础设施系统1202之间的通信和数据交换。每个网络可以是本领域技术人员熟悉的可以支持利用各种商用协议(包括上文针对(一个或多个)网络1110所描述的协议)中的任何商用协议的数据通信的任何类型的网络。

[0194] 在某些实施例中，由云基础设施系统1202提供的服务可以包括按需对云基础设施系统的用户可用的许多服务。除了与管理利用远程设备对企业系统的访问相关的服务之外，还可以提供各种其它服务，这些服务包括但不限于在线数据存储和备份解决方案、基于Web的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管理的技术支持服务等。由云基础设施系统提供的服务可以动态缩放，以满足其用户的需求。

[0195] 在某些实施例中，由云基础设施系统1202提供的服务的具体实例化在本文中可以被称为“服务实例”。一般而言，经由通信网络(诸如因特网)从云服务提供商的系统对用户可用的任何服务被称为“云服务”。通常，在公共云环境中，构成云服务提供商的系统的服务器和系统不同于客户自己的本地服务器和系统。例如，云服务提供商的系统可以托管应用，并且用户可以经由诸如因特网之类的通信网络来按需订购和使用应用。

[0196] 在一些示例中，计算机网络云基础设施中的服务可以包括对由云供应商向用户提供或者如本领域已知的以其它方式提供的存储装置、托管的数据库、托管的web服务器、软件应用或者其它服务的受保护的计算机网络访问。例如，服务可以包括通过因特网对云上

的远程存储装置的受密码保护的访问。作为另一个示例，服务可以包括基于web服务的托管的关系数据库和脚本语言中间件引擎，以供联网的开发者私人使用。作为另一个示例，服务可以包括对在云供应商的网站上托管的电子邮件软件应用的访问。

[0197] 在某些实施例中，云基础设施系统1202可以包括以自助服务、基于订阅、弹性可扩展、可靠、高度可用和安全的方式交付给客户的一套应用、中间件和数据库服务提供物。这样的云基础设施系统的示例是由本受让人提供的Oracle公共云。

[0198] 云基础设施系统1202还可以提供与“大数据”相关的计算服务和分析服务。术语“大数据”一般用来指可以由分析员和研究者存储和操纵以可视化大量数据、检测趋势和/或以其它方式与数据交互的极大数据集。这种大数据和相关应用可以由基础设施系统在许多级别和不同规模上进行托管和/或操纵。并行链接的数十个、数百个或成千上万个处理器可以作用于这样的数据，以便呈现它或者模拟对数据或它代表的内容的外力。这些数据集可以涉及结构化数据(诸如在数据库中组织或以其它方式根据结构化模型组织的数据)，和/或非结构化数据(例如，电子邮件、图像、数据blob(二进制大对象)、网页、复杂事件处理)。通过利用实施例相对快速地将更多的(或更少的)计算资源集中在目标上的能力，云基础设施系统可以更好地可用于基于来自企业、政府机构、研究组织、私人个人、一群志同道合的个人或组织或其它实体的需求来对大数据集执行任务。

[0199] 在各种实施例中，云基础设施系统1202可以适于自动地供应、管理和跟踪对由云基础设施系统1202提供的服务的客户订阅。云基础设施系统1202可以经由不同的部署模型提供云服务。例如，服务可以在公共云模型下被提供，在该公共云模型中云基础设施系统1202由销售云服务的组织拥有(例如，由Oracle公司拥有)，并且服务对一般公众或不同的工业企业可用。作为另一个示例，服务可以在私有云模型下被提供，在该私有云模型中云基础设施系统1202仅针对单个组织操作，并且可以为该组织内的一个或多个实体提供服务。云服务还可以在社区云模型下被提供，在该社区云模型中云基础设施系统1202和由云基础设施系统1202提供的服务由相关社区中的若干组织共享。云服务还可以在作为两个或更多个不同模型的组合的混合云模型下被提供。

[0200] 在一些实施例中，由云基础设施系统1202提供的服务可以包括在软件即服务(SaaS)类别、平台即服务(PaaS)类别、基础设施即服务(IaaS)类别或包括混合服务的其它服务类别下提供的一个或多个服务。经由订阅订单，客户可以订购由云基础设施系统1202提供的一个或多个服务。然后云基础设施系统1202执行处理，以提供客户的订阅订单中的服务。

[0201] 在一些实施例中，由云基础设施系统1202提供的服务可以包括但不限于应用服务、平台服务和基础设施服务。在一些示例中，应用服务可以由云基础设施系统经由SaaS平台提供。SaaS平台可以被配置为提供落入SaaS类别下的云服务。例如，SaaS平台可以提供在集成的开发和部署平台上构建和交付按需应用套件的能力。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础设施。通过利用由SaaS平台提供的服务，客户可以利用在云基础设施系统上执行的应用。客户可以获取应用服务，而无需客户购买分开的许可和支持。可以提供各种不同的SaaS服务。示例包括但不限于为大型组织提供用于销售业绩管理、企业集成和业务灵活性的解决方案的服务。

[0202] 在一些实施例中，平台服务可以由云基础设施系统1202经由PaaS平台提供。PaaS

平台可以被配置为提供落入PaaS类别下的云服务。平台服务的示例可以包括但不限于使得组织(诸如Oracle)能够在共享的公共架构上整合现有应用的服务以及构建利用由平台提供的共享服务的新应用的能力。PaaS平台可以管理和控制用于提供PaaS服务的底层软件和基础设施。客户可以获取由云基础设施系统1202提供的PaaS服务,而无需客户购买分开的许可和支持。平台服务的示例包括但不限于Oracle Java云服务(JCS)、Oracle数据库云服务(DBCS)以及其它。

[0203] 通过利用由PaaS平台提供的服务,客户可以采用由云基础设施系统支持的编程语言和工具,并且还可以控制所部署的服务。在一些实施例中,由云基础设施系统提供的平台服务可以包括数据库云服务、中间件云服务(例如,Oracle Fusion Middleware服务)和Java云服务。在一个实施例中,数据库云服务可以支持共享服务部署模型,该共享服务部署模型使得组织能够汇集数据库资源并且以数据库云的形式向客户提供数据库即服务。在云基础设施系统中,中间件云服务可以为客户提供开发和部署各种业务应用的平台,而Java云服务可以为客户提供部署Java应用的平台。

[0204] 各种不同的基础设施服务可以由云基础设施系统中的IaaS平台提供。基础设施服务便于利用由SaaS平台和PaaS平台提供的服务的客户对底层计算资源(诸如存储装置、网络和其它基本计算资源)的管理和控制。

[0205] 在某些实施例中,云基础设施系统1202还可以包括基础设施资源1230,以用于提供用来向云基础设施系统的客户提供各种服务的资源。在一个实施例中,基础设施资源1230可以包括用于执行由PaaS平台和SaaS平台提供的服务的硬件(诸如服务器、存储装置和联网资源)的预先集成和优化的组合以及其它资源。

[0206] 在一些实施例中,云基础设施系统1202中的资源可以由多个用户共享并且根据需求被动态地重新分配。此外,资源可以分配给在不同时区中的用户。例如,云基础设施系统1202可以使得第一时区中的第一用户集合能够利用云基础设施系统的资源指定的小时数,然后实现将同一资源重新分配给位于不同时区中的另一用户集合,由此最大化资源的利用率。

[0207] 在某些实施例中,可以提供若干内部共享服务1232,内部共享服务1232由云基础设施系统1202的不同组件或模块共享,以使得云基础设施系统1202能够供应服务。这些内部共享服务可以包括但不限于安全和身份服务、集成服务、企业储存库服务、企业管理器服务、病毒扫描和白名单服务、高可用性、备份和恢复服务、用于实现云支持的服务、电子邮件服务、通知服务、文件传输服务等。

[0208] 在某些实施例中,云基础设施系统1202可以在云基础设施系统中提供云服务(例如,SaaS、PaaS和IaaS服务)的综合管理。在一个实施例中,云管理功能可以包括用于供应、管理和跟踪由云基础设施系统1202接收到的客户的订阅的能力等。

[0209] 在一个实施例中,如图12中所绘出的,云管理功能可以由诸如订单管理模块1220、订单编排模块1222、订单供应模块1224、订单管理和监视模块1226以及身份管理模块1228之类的一个或多个模块提供。这些模块可以包括一个或多个计算机和/或服务器或者可以利用一个或多个计算机和/或服务器来提供,该一个或多个计算机和/或服务器可以是通用计算机、专用服务器计算机、服务器场,服务器集群或任何其它适当的布置和/或组合。

[0210] 在示例性操作中,在步骤1234处,使用客户端设备(诸如客户端计算设备1204、

1206或1208)的客户可以通过请求由云基础设施系统1202提供的一个或多个服务并且对由云基础设施系统1202提供的一个或多个服务的订阅下订单来与云基础设施系统1202交互。在某些实施例中,客户可以访问云用户界面(UI)(诸如云UI 1212、云UI 1214和/或云UI 1216)并且经由这些UI下订阅订单。响应于客户下订单而由云基础设施系统1202接收到的订单信息可以包括识别客户和客户旨在订阅的由云基础设施系统1202提供的一个或多个服务的信息。

[0211] 在步骤1236处,从客户接收到的订单信息可以被存储在订单数据库1218中。如果这是新订单,则可以为该订单创建新记录。在一个实施例中,订单数据库1218可以是由云基础设施系统1202操作以及与其它系统元素结合操作的若干数据库中的一个数据库。

[0212] 在步骤1238处,订单信息可以被转发到订单管理模块1220,订单管理模块1220可以被配置为执行与订单相关的计费和记帐功能,诸如验证订单,并且在通过验证时,预订订单。

[0213] 在步骤1240处,关于订单的信息可以被传送到订单编排模块1222,订单编排模块1222被配置为编排用于客户下的订单的服务和资源的供应。在一些实例中,订单编排模块1222可以使用订单供应模块1224的服务以用于供应。在某些实施例中,订单编排模块1222实现对与每个订单相关联的业务过程的管理,并且应用业务逻辑来确定订单是否应当继续供应。

[0214] 如图12中绘出的实施例中所示,在步骤1242处,在接收到对新订阅的订单时,订单编排模块1222向订单供应模块1224发送分配资源和配置履行订购订单所需的资源的请求。订单供应模块1224实现用于由客户订购的服务的资源分配。订单供应模块1224提供由云基础设施系统1202提供的云服务和用来供应用于提供所请求的服务的资源的物理实现层之间的抽象级别。这使得订单编排模块1222能够与诸如服务和资源实际上被实时供应还是被预先供应并且仅在请求时才被分配/指派之类的实现细节隔离。

[0215] 在步骤1244处,一旦供应了服务和资源,就可以向订阅的客户发送指示所请求的服务现在准备好使用的通知。在一些实例中,可以向客户发送使得客户能够开始使用所请求的服务的信息(例如,链接)。

[0216] 在步骤1246处,客户的订阅订单可以由订单管理和监视模块1226管理和跟踪。在一些实例中,订单管理和监视模块1226可以被配置为收集关于所订阅的服务的客户使用的使用统计数据。例如,可以针对所使用的存储装置量、传送的数据量、用户的数量以及系统启动时间和系统停机时间的量等来收集统计数据。

[0217] 在某些实施例中,云基础设施系统1202可以包括身份管理模块1228,身份管理模块1228被配置为提供身份服务,诸如云基础设施系统1202中的访问管理和授权服务。在一些实施例中,身份管理模块1228可以控制关于希望利用由云基础设施系统1202提供的服务的客户的信息。这样的信息可以包括认证这些客户的身份的信息和描述这些客户被授权相对于各种系统资源(例如,文件、目录、应用、通信端口、存储器段等)执行的动作的信息。身份管理模块1228还可以包括对关于每个客户的描述性信息以及关于如何和由谁来访问和修改描述性信息的管理。

[0218] 图13示出了可以被用来实现本发明的实施例的示例性计算机系统1300。在一些实施例中,计算机系统1300可以被用来实现上文描述的各种服务器和计算机系统中的任何服

务器和计算机系统。如图13中所示，计算机系统1300包括各种子系统，这些子系统包括经由总线子系统1302与多个外围子系统通信的处理子系统1304。这些外围子系统可以包括处理加速单元1306、I/O子系统1308、存储子系统1318和通信子系统1324。存储子系统1318可以包括有形的计算机可读存储介质1322和系统存储器1310。

[0219] 总线子系统1302提供用于使计算机系统1300的各种组件和子系统按照预期彼此通信的机制。虽然总线子系统1302被示意性地示为单条总线，但是总线子系统的替代实施例可以利用多条总线。总线子系统1302可以是利用各种总线架构中的任何总线架构的若干类型的总线结构中的任何类型的总线结构，包括存储器总线或存储器控制器、外围总线和局部总线。例如，这样的架构可以包括工业标准架构(ISA)总线、微通道架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围组件互连(PCI)总线等，其中PCI总线可以被实现为根据IEEE P1386.1标准制造的夹层(Mezzanine)总线。

[0220] 处理子系统1304控制计算机系统1300的操作并且可以包括一个或多个处理单元1332、1334等。处理单元可以包括一个或多个处理器，该一个或多个处理器包括单核处理器或多核处理器、处理器的一个或多个核心、或其组合。在一些实施例中，处理子系统1304可以包括一个或多个专用协处理器，诸如图形处理器、数字信号处理器(DSP)等。在一些实施例中，处理子系统1304的处理单元中的一些或全部可以利用诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)之类的定制电路来实现。

[0221] 在一些实施例中，处理子系统1304中的处理单元可以执行存储在系统存储器1310中或计算机可读存储介质1322上的指令。在各种实施例中，处理单元可以执行各种程序或代码指令，并且可以维护多个并发执行的程序或进程。在任何给定时间，要执行的程序代码中的一些或全部可以驻留在系统存储器1310中和/或在计算机可读存储介质1322上(潜在地包括在一个或多个存储设备上)。通过合适的编程，处理子系统1304可以提供用于管理利用远程设备对企业系统的访问的上文描述的各种功能。

[0222] 在某些实施例中，可以提供处理加速单元1306，以用于执行定制的处理或用于卸载由处理子系统1304执行的处理中的一些处理，以便加速由计算机系统1300执行的整体处理。

[0223] I/O子系统1308可以包括用于向计算机系统1300输入信息和/或用于输出来自计算机系统1300的信息或经由计算机系统1300输出信息的设备和机制。一般而言，术语“输入设备”的使用旨在包括用于向计算机系统1300输入信息的所有可能类型的设备和机构。用户接口输入设备可以包括例如键盘、诸如鼠标或轨迹球之类的指示设备、结合到显示器中的触摸板或触摸屏、滚轮、点拨轮、拨盘、按钮、开关、键板、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备还可以包括诸如使得用户能够控制输入设备并与其交互的Microsoft**Kinect®**运动传感器之类的运动感测和/或姿势识别设备、Microsoft**Xbox®**360游戏控制器、提供用于接收利用姿势和口头命令的输入的接口的设备。用户接口输入设备还可以包括眼部姿势识别设备，诸如检测用户的眼睛活动(例如，当拍摄图片和/或进行菜单选择时的“眨眼”)并且将眼部姿势变换为到输入设备(例如，Google**Glass®**)中的输入的Google**Glass®**眨眼检测器。此外，用户接口输入设备可以包括使得用户能够通过语音命令与语音识别系统(例如，**Siri®**导航器)交互的语音识别感测设备。

[0224] 用户接口输入设备的其它示例包括但不限于三维(3D)鼠标、操纵杆或指示杆、游戏板和图形平板、以及音频/视觉设备，诸如扬声器、数码照相机、数字摄像机、便携式媒体播放器、网络摄像机、图像扫描仪、指纹扫描仪、条形码读取器3D扫描仪、3D打印机、激光测距仪、以及视线跟踪设备。此外，用户接口输入设备还可以包括例如医疗成像输入设备，诸如计算机断层扫描设备、磁共振成像设备、正电子发射断层扫描设备、医疗超声检查设备。用户接口输入设备还可以包括例如音频输入设备，诸如MIDI键盘、数字乐器等。

[0225] 用户接口输出设备可以包括显示子系统、指示器灯或诸如音频输出设备之类的非视觉显示器等。显示子系统可以是阴极射线管(CRT)、诸如利用液晶显示器(LCD)或等离子显示器的平板设备之类的平板设备、投影设备、触摸屏等。一般而言，术语“输出设备”的使用旨在包括用于向用户或其它计算机输出来自计算机系统1300的信息的所有可能类型的设备和机构。例如，用户接口输出设备可以包括但不限于可视地传达文本、图形和音频/视频信息的各种显示设备，诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备和调制解调器。

[0226] 存储子系统1318提供用于存储由计算机系统1300使用的信息的储存库(repository)或数据存储库。存储子系统1318提供有形的非暂态计算机可读存储介质，以用于存储提供一些实施例的功能的基本编程和数据构造。当由处理子系统1304执行时提供上文描述的功能的软件(程序、代码模块、指令)可以被存储在存储子系统1318中。软件可以由处理子系统1304的一个或多个处理单元执行。存储子系统1318还可以提供用于存储根据本发明使用的数据的储存库。

[0227] 存储子系统1318可以包括一个或多个非暂态存储器设备，该一个或多个非暂态存储器设备包括易失性存储器设备和非易失性存储器设备。如图13中所示，存储子系统1318包括系统存储器1310和计算机可读存储介质1322。系统存储器1310可以包括若干存储器，这些存储器包括用于在程序执行期间存储指令和数据的易失性主随机存取存储器(RAM)和其中存储固定指令的非易失性只读存储器(ROM)或闪存存储器。在一些实施方式中，包含帮助诸如在启动期间在计算机系统1300内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以被存储在ROM中。RAM通常包含当前正由处理子系统1304操作和执行的数据模块和/或程序模块。在一些实施方式中，系统存储器1310可以包括多个不同类型的存储器，诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。

[0228] 作为示例而非限制，如在图13中绘出的，系统存储器1310可以存储应用程序1312、程序数据1314和操作系统1316，应用程序1312可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等。作为示例，操作系统1316可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商用的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google **Chrome®** OS等)和/或诸如iOS、**Windows®** Phone、**Android®** OS、**BlackBerry®** 10OS和**Palm®** OS操作系统之类的移动操作系统。

[0229] 计算机可读存储介质1322可以存储提供一些实施例的功能的编程和数据构造。当由处理子系统1304执行时使得处理器提供上文描述的功能的软件(程序、代码模块、指令)可以被存储在存储子系统1318中。作为示例，计算机可读存储介质1322可以包括非易失性存储器，诸如硬盘驱动器、磁盘驱动器、诸如CD ROM、DVD、Blu-**Ray®**(蓝光)盘或其它光学

介质之类的光盘驱动器。计算机可读存储介质1322可以包括但不限于Zip®驱动器、闪存存储器卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质1322还可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态ROM等)、基于易失性存储器的SSD(诸如固态RAM、动态RAM、静态RAM、基于DRAM的SSD、磁阻RAM(MRAM)SSD)、以及使用基于DRAM的SSD和基于闪存存储器的SSD的组合的混合SSD。计算机可读介质1322可以为计算机系统1300提供计算机可读指令、数据结构、程序模块和其它数据的存储。

[0230] 在某些实施例中,存储子系统1318还可以包括计算机可读存储介质读取器1320,计算机可读存储介质读取器1320可以被进一步连接到计算机可读存储介质1322。与系统存储器1310一起并且可选地与系统存储器1310组合,计算机可读存储介质1322可以全面地表示远程存储设备、本地存储设备、固定存储设备和/或可移动存储设备加上用于存储计算机可读信息的存储介质。

[0231] 在某些实施例中,计算机系统1300可以提供对执行一个或多个虚拟机的支持。计算机系统1300可以执行诸如管理程序之类的程序,以便于虚拟机的配置和管理。每个虚拟机可以被分配存储器资源、计算资源(例如,处理器、核心)、I/O资源和联网资源。每个虚拟机通常运行可以与由计算机系统1300执行的其它虚拟机执行的操作系统相同或不同的其自己的操作系统。相应地,多个操作系统可以潜在地由计算机系统1300并发运行。每个虚拟机一般独立于其它虚拟机运行。

[0232] 通信子系统1324提供到其它计算机系统和网络的接口。通信子系统1324充当用于从来自计算机系统1300的其它系统接收数据和向来自计算机系统1300的其它系统发送数据的接口。例如,通信子系统1324可以使得计算机系统1300能够经由因特网建立到一个或多个客户端设备的通信信道,以用于从客户端设备接收信息和向客户端设备发送信息。

[0233] 通信子系统1324可以支持有线通信协议和/或无线通信协议两者。例如,在某些实施例中,通信子系统1324可以包括用于(例如,利用蜂窝电话技术、诸如3G、4G或EDGE(全球演进的增强数据速率)之类的高级数据网络技术、WiFi(IEEE 802.11族标准)、或其它移动通信技术、或其任何组合)访问无线语音网络和/或数据网络的射频(RF)收发器组件、全球定位系统(GPS)接收器组件和/或其它组件。在一些实施例中,除了无线接口之外或者作为无线接口的替代,通信子系统1324可以提供有线网络连接(例如,以太网)。

[0234] 通信子系统1324可以接收和发送以各种形式的数据。例如,在一些实施例中,通信子系统1324可以接收以结构化和/或非结构化的数据馈送1326、事件流1328、事件更新1330等的形式的输入通信。例如,通信子系统1324可以被配置为从社交媒体网络的用户和/或其它通信服务实时地接收(或发送)数据馈送1326(诸如Twitter®馈送、Facebook®更新、诸如丰富站点摘要(RSS)馈送之类的web馈送)和/或来自一个或多个第三方信息源的实时更新。

[0235] 在某些实施例中,通信子系统1324可以被配置为接收没有明确结束的本质上可以是连续的或无界的连续数据流形式的数据,其中连续数据流可以包括实时事件的事件流1328和/或事件更新1330。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如网络监视和业务管理应用)、点击流分析工具、汽车交通监视等。

[0236] 通信子系统1324还可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送1326、事件流1328、事件更新1330等，其中该一个或多个数据库可以与耦接到计算机系统1300的一个或多个流数据源计算机通信。

[0237] 计算机系统1300可以是各种类型中的一种类型，这些类型包括手持便携式设备(例如，iPhone®蜂窝电话、iPad®计算平板、PDA)、可穿戴设备(例如，GoogleGlass®头戴式显示器)、个人计算机、工作站、大型机、信息亭、服务器机架或任何其它数据处理系统。

[0238] 由于计算机和网络不断变化的本质，对图13中绘出的计算机系统1300的描述旨在仅仅作为具体示例。具有比图13中绘出的系统更多或更少的组件的许多其它配置是可能的。基于本文提供的公开内容和教导，本领域普通技术人员将理解实现各种实施例的其它方式和/或方法。

[0239] 根据本发明的实施例，提供了计算系统中的一种设备访问管理系统。该实施例的设备访问管理系统可以是前面的实施例中描述的设备访问管理系统120。此外，设备访问管理系统及其组件可以基于如前面的实施例中描述的本发明的原理来执行适当的操作中的任何操作。

[0240] 在该实施例的示例中，这样的设备访问管理系统可以包括帐户处理机、应用配置管理器、通信处理机、访问管理器和设备管理器。访问管理器可以为企业系统的用户识别与身份相关联的用户角色。设备管理器可以检索注册该身份以访问企业系统的第一远程设备的设备信息。帐户处理机可以基于用户角色来确定向身份提供对企业系统中可访问的第一资源的访问的帐户，其中第一资源是利用该用户角色可访问的多个应用中的第一应用从第一远程设备可访问的。应用配置管理器可以配置第一应用，以利用第一远程设备访问用于账户的第一资源，其中第一应用被配置为具有用于连接到提供第一资源的第一目标系统的连接信息，并且其中第一应用被配置为具有用于访问用于帐户的第一资源的访问信息。另外，通信处理机可以在配置第一应用后将第一应用发送到第一远程设备。

[0241] 在该实施例的示例中，设备管理器可以检测注册身份以访问企业系统的多个远程设备中的第二远程设备。在这个示例中，通信处理机还可以在配置第一应用后将第一应用发送到第二远程设备。

[0242] 在该实施例的示例中，访问管理器可以检测用户角色从第一用户角色到第二用户角色的改变，并且基于第二用户角色来确定身份对第一资源的访问的改变。应用配置管理器可以指示第一远程设备基于访问的改变来修改第一应用的配置。

[0243] 在该实施例的示例中，设备管理器可以发现注册身份以访问企业系统的多个远程设备。通信处理机可以在配置第一应用后将第一应用发送到多个远程设备。应用配置管理器可以指示多个远程设备中的每个远程设备基于访问的改变来修改第一应用的配置。

[0244] 在该实施例的示例中，对第一资源的访问的改变包括撤销对第一资源的访问，并且其中修改第一应用包括删除为第一应用配置的连接信息和访问信息。

[0245] 在该实施例的示例中，对第一资源的访问的改变包括撤销对第一资源的访问，并且其中修改第一应用包括从第一远程设备移除第一应用。

[0246] 在该实施例的示例中，修改第一应用包括调整为第一应用配置的访问信息。

[0247] 在该实施例的示例中，访问管理器可以检测用户角色从第一用户角色到第二用户

角色的改变。帐户处理机可以基于第二用户角色发现第二用户角色可访问的多个应用中的第二应用。应用配置管理器可以利用身份来配置用于从第一远程设备进行访问的第二应用，其中第二应用被配置为具有用于访问由第二目标系统提供的第二资源的信息。通信处理机可以将第二应用发送到第一远程设备。

[0248] 在该实施例的示例中，设备信息指示第一远程设备的配置，该配置指示第一远程设备上的操作系统配置和第一远程设备的硬件配置，并且其中第一应用是利用第一远程设备的配置来配置的。

[0249] 在该实施例的示例中，连接信息包括第一目标系统的端口地址、第一目标系统的主机地址以及第一目标系统的轻量级目录访问协议(LDAP)。

[0250] 在该实施例的示例中，帐户处理机可以基于用户角色来识别多个应用程序中的第二应用，第二应用使得用户能够执行用户角色。帐户处理机还可以供应第二应用，以访问企业系统中的第二资源。应用配置管理器可以配置第二应用，以从第一远程设备访问第二资源。通信处理机可以在配置第二应用后发送第二应用。

[0251] 在该实施例的示例中，帐户处理机确定帐户包括确定是否为访问第一目标系统的第一资源供应帐户；在确定没有为访问第一资源供应帐户时供应帐户，以向身份提供对第一目标系统的第一资源的访问；以及在确定为该身份供应了帐户时检索关于该帐户的帐户信息。

[0252] 根据本发明的另一个实施例，提供了计算系统中的另一种设备访问管理系统。该实施例的设备访问管理系统可以是上面的实施例中描述的设备访问管理系统120。此外，设备访问管理系统及其组件可以基于如前面的实施例中描述的本发明的原理来执行适当的操作中的任何操作。

[0253] 在该实施例的示例中，这样的设备访问管理系统可以包括若干子系统和/或模块，这些子系统和/或模块包括帐户处理机、应用配置管理器、通信处理机、访问管理器和设备管理器。访问管理器可以为企业系统的用户识别与身份相关联的用户角色。设备管理器可以检索注册该身份以访问企业系统的第一远程设备的设备信息。帐户处理机可以基于用户角色为身份供应对多个应用的访问，其中该多个应用中的每个应用被供应以用于利用第一远程设备访问企业系统中的不同资源。应用配置管理器可以将多个应用中的第一应用配置为具有第一连接信息和第一访问信息以从第一远程设备访问第一资源，并且将多个应用中的第二应用配置为具有第二连接信息和第二访问信息以从第一远程设备访问第二资源。另外，通信处理机可以在配置第一应用后将第一应用发送到第一远程设备以及在配置第二应用后将第二应用发送到第一远程设备。

[0254] 在该实施例的示例中，访问管理器可以检测用户角色从第一用户角色到第二用户角色的改变，并且基于用户角色的改变确定由身份对第二资源的访问被撤销以及由身份对第三资源的访问被允许，其中第一资源、第二资源和第三资源彼此不同。应用配置管理器可以基于确定对第二资源的访问被撤消而指示第一远程设备移除第二应用，并且将多个应用中的第三应用配置为具有第三连接信息和第三访问信息，以从第一远程设备访问第三资源。账户处理机可以基于第二用户角色来为身份供应对第三应用的访问，该第三应用提供从第一远程设备对企业系统中的第三资源的访问。在这个示例中，应用配置管理器还可以。通信处理机可以在配置第三应用后将第三应用发送到第一远程设备。

[0255] 在该实施例的示例中，为身份供应对应用的访问包括为该身份供应提供对该应用可访问的的资源的访问的帐户。

[0256] 虽然已经描述了本发明的具体实施例，但是各种修改、更改、替代构造和等价物也包含在本发明的范围之内。修改包括所公开的特征的任何相关的组合。本发明的实施例不限于某些具体数据处理环境内的操作，而是可以在多个数据处理环境内自由操作。此外，虽然已利用特定系列的事务和步骤描述了本发明的实施例，但是对本领域技术人员应当明显的是，本发明的范围不限于所描述的系列的事务和步骤。上文描述的实施例的各种特征和方面可以被单独使用或结合使用。

[0257] 另外，虽然已经利用硬件和软件的特定组合描述了本发明的实施例，但是应当认识到，硬件和软件的其它组合也在本发明的范围之内。本发明的实施例可以仅在硬件中、或仅在软件中、或利用其组合来实现。本文描述的各种过程可以在同一处理器上实现或者以任何组合在不同处理器上实现。相应地，在组件或模块被描述为被配置为执行某些操作的情况下，这样的配置可以例如通过设计电子电路以执行操作、通过对可编程电子电路(诸如微处理器)进行编程以执行操作、或其任何组合来实现。进程可以利用包括但不限于用于进程间通信的常规技术的各种技术来通信，并且不同的进程对可以使用不同的技术，或者同一对进程可以在不同时间使用不同的技术。

[0258] 相应地，应当在说明性的意义而不是限制性的意义上考虑说明书和附图。然而，将明显的是，在不背离比权利要求中阐述的更广泛精神和范围的情况下，可以对其进行添加、减少、删除以及其它修改和改变。因此，虽然已描述了具体的发明实施例，但是这些实施例不旨在是限制性的。各种修改和等价物在以下权利要求的范围之内。

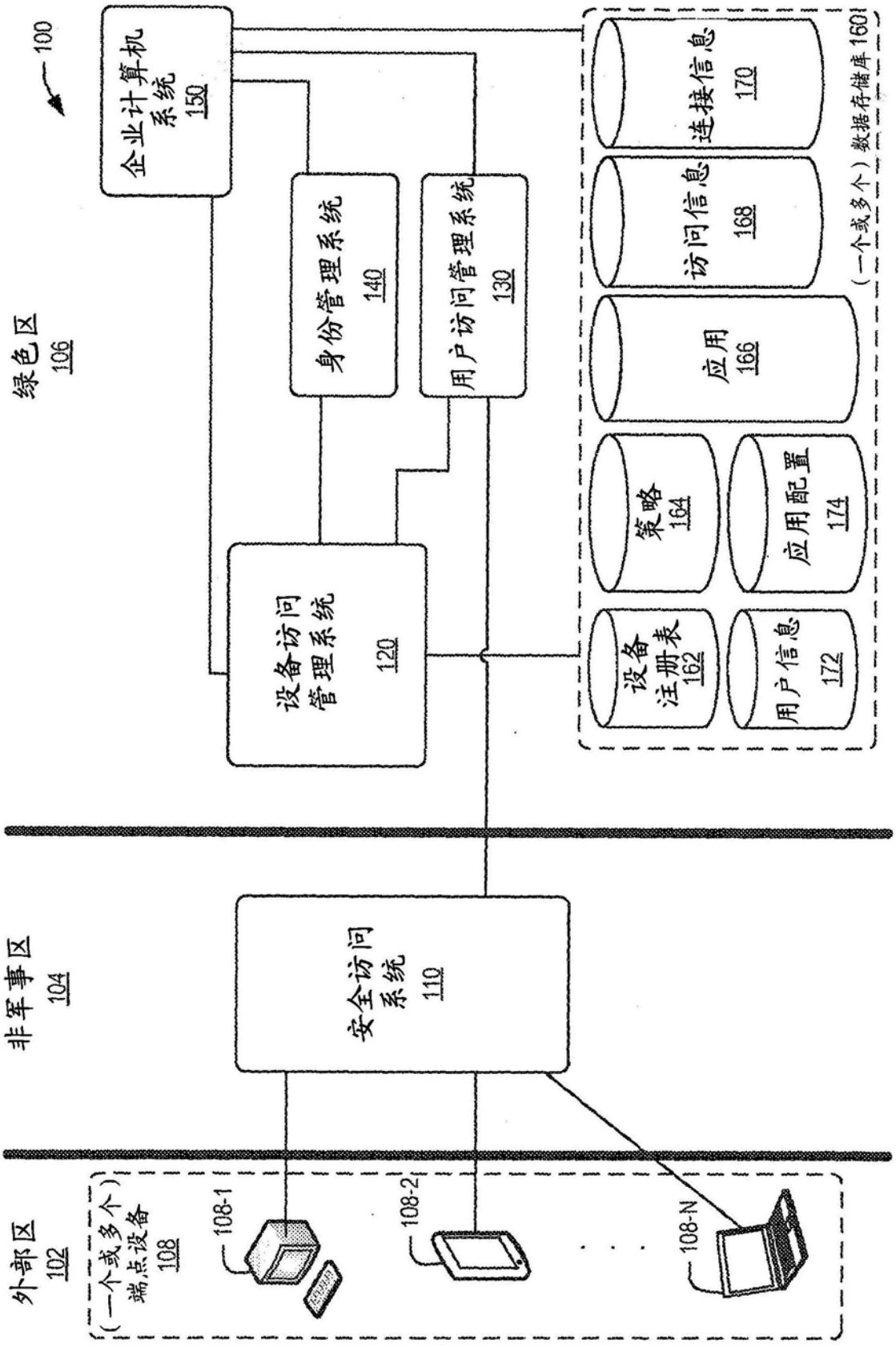

100
企业计算机系统 150
绿色区 106
身份管理系统 140
用户访问管理系统 130
设备访问管理系统 120
(一个或多个)数据存储库 160
连接信息 170
访问信息 168
应用 166
策略 164
应用配置 174
用户信息 172
设备注册表 162
非军事区 104
安全访问系统 110
外部区 102
(一个或多个)端点设备 108
108-1
108-2
108-N

图1

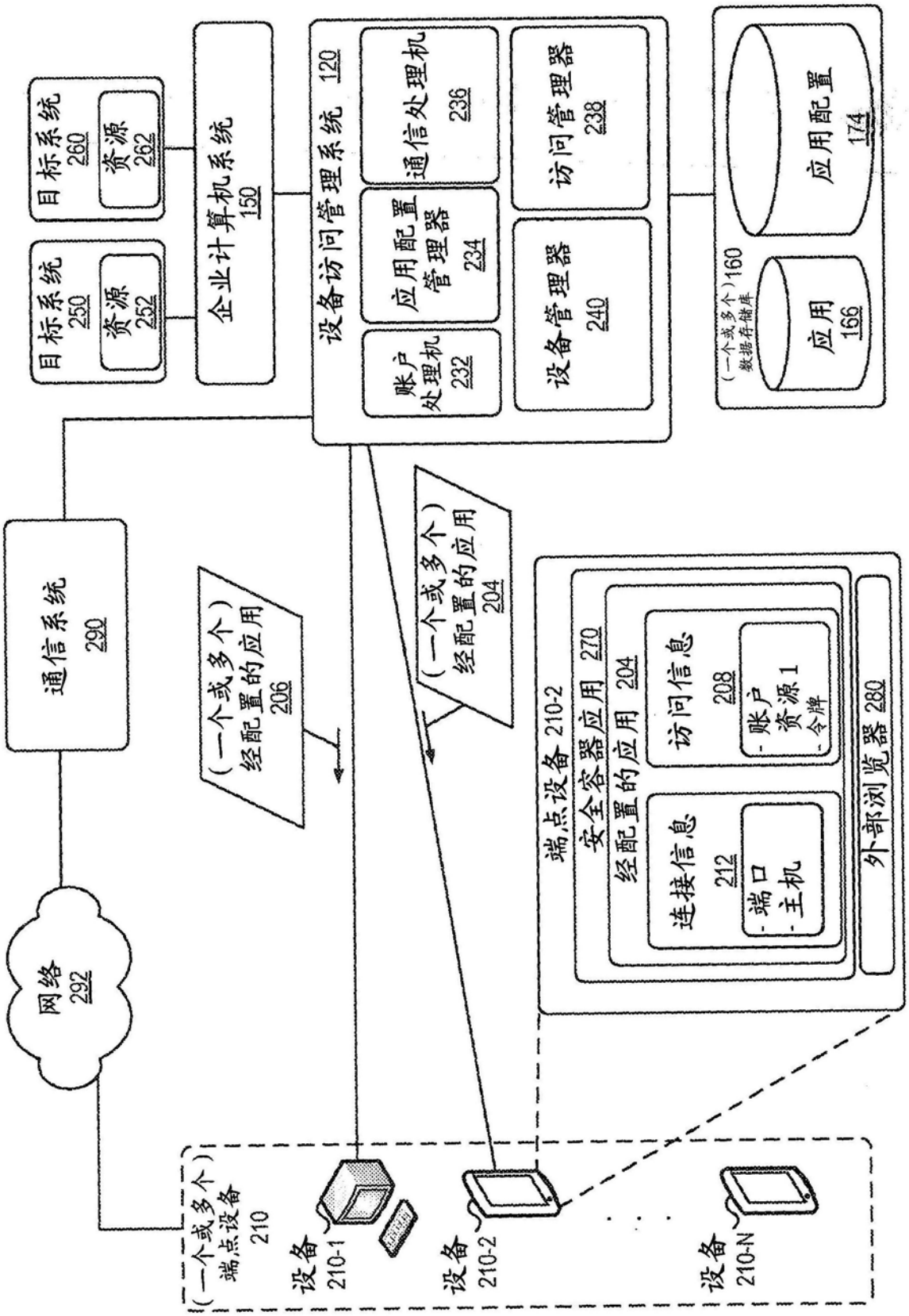

目标系统 260
资源 262
目标系统 250
资源 252
企业计算机系统 150
设备访问管理系统 120
通信处理机 236
应用配置管理器 234
访问管理器 238
账户处理机 232
设备管理器 240
(一个或多个)数据存储库 160
应用 166
应用配置 174
通信系统 290
(一个或多个)经配置的应用 206
(一个或多个)经配置的应用 204
网络 292
端点设备 210-2
安全容器应用 270
经配置的应用 204
访问信息 208
连接信息 212
- 端口
- 主机
- 账户
资源 1
- 令牌
外部浏览器 280
(一个或多个)端点设备 210
设备 210-1
设备 210-2
设备 210-N

图2

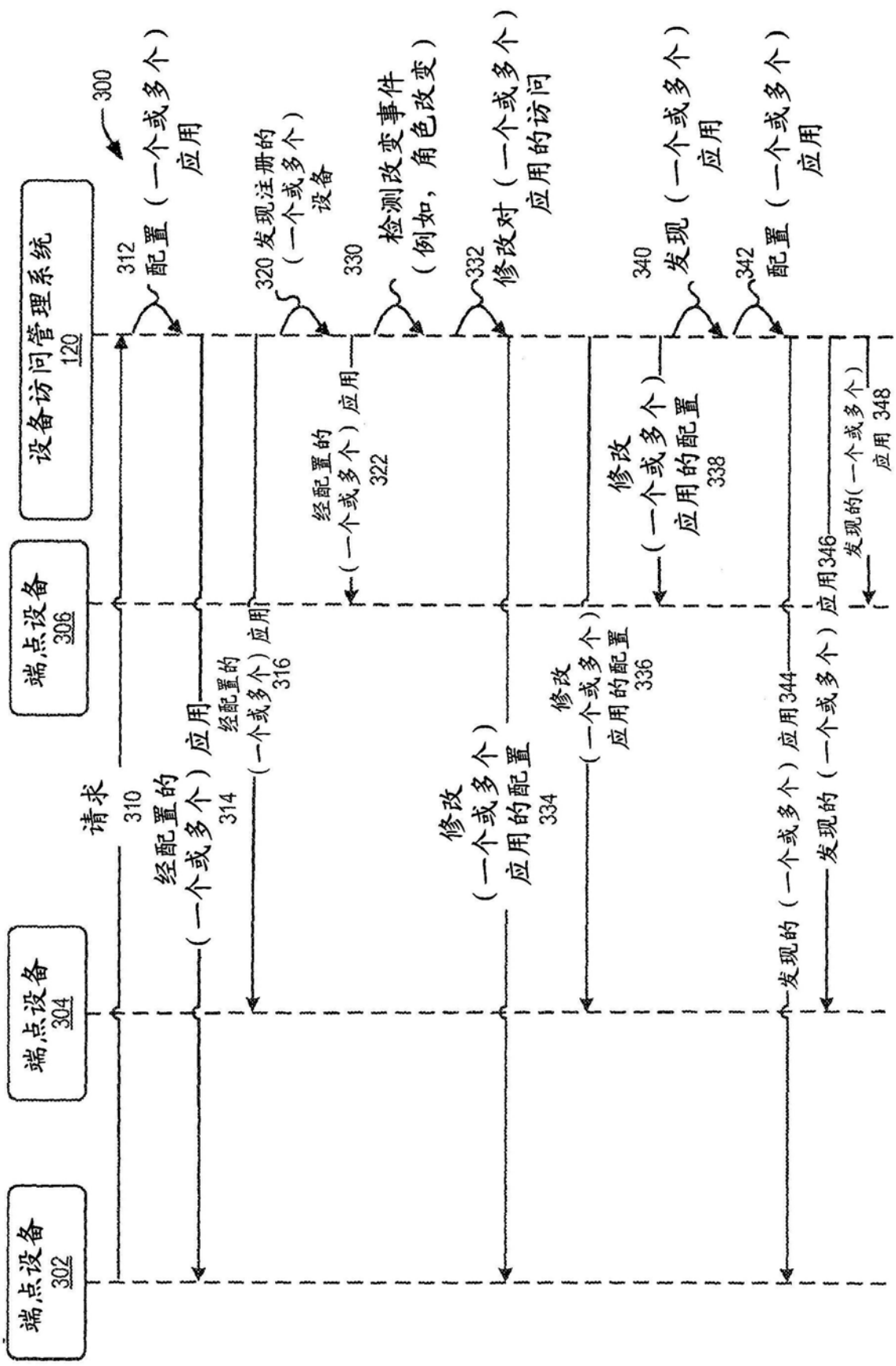

300
端点设备 302
端点设备 304
端点设备 306
设备访问管理系统 120
请求 310
312 配置（一个或多个）应用
经配置的（一个或多个）应用 314
经配置的（一个或多个）应用 316
320 发现注册的（一个或多个）设备
经配置的（一个或多个）应用 322
330 检测改变事件（例如，角色改变）
332 修改对（一个或多个）应用的访问
修改（一个或多个）应用的配置 334
修改（一个或多个）应用的配置 336
340 发现（一个或多个）应用
修改（一个或多个）应用的配置 338
342 配置（一个或多个）应用
发现的（一个或多个）应用 344
发现的（一个或多个）应用 346
发现的（一个或多个）应用 348

图3

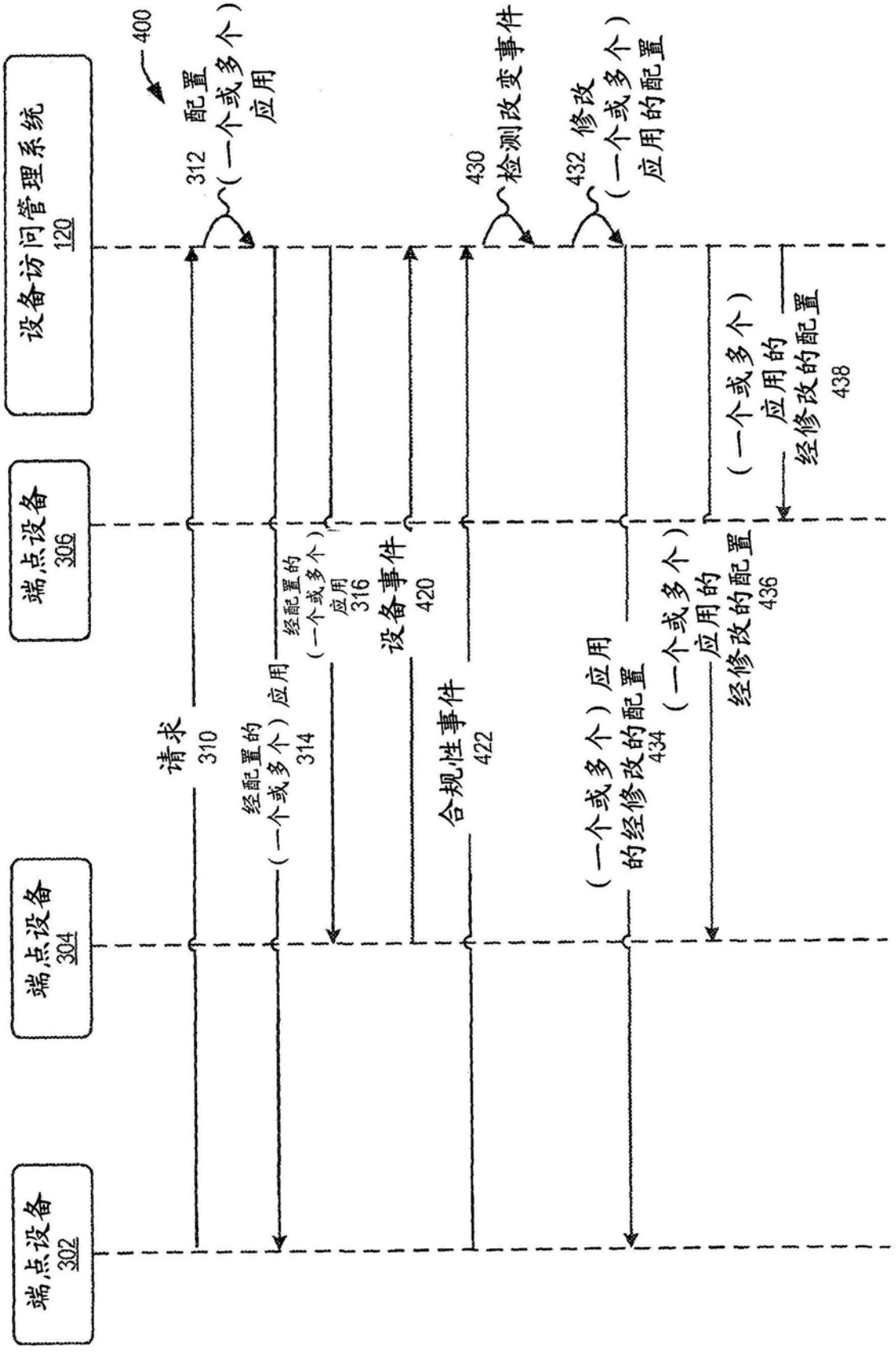

400
设备访问管理系统
120
端点设备
306
端点设备
304
端点设备
302
312 配置（一个或多个）应用
请求
310
经配置的（一个或多个）应用
314
经配置的（一个或多个）应用
316
设备事件
420
合规性事件
422
430 检测改变事件
432 修改（一个或多个）应用的配置
（一个或多个）应用的经修改的配置
434
（一个或多个）应用的经修改的配置
436
（一个或多个）应用的经修改的配置
438

图4

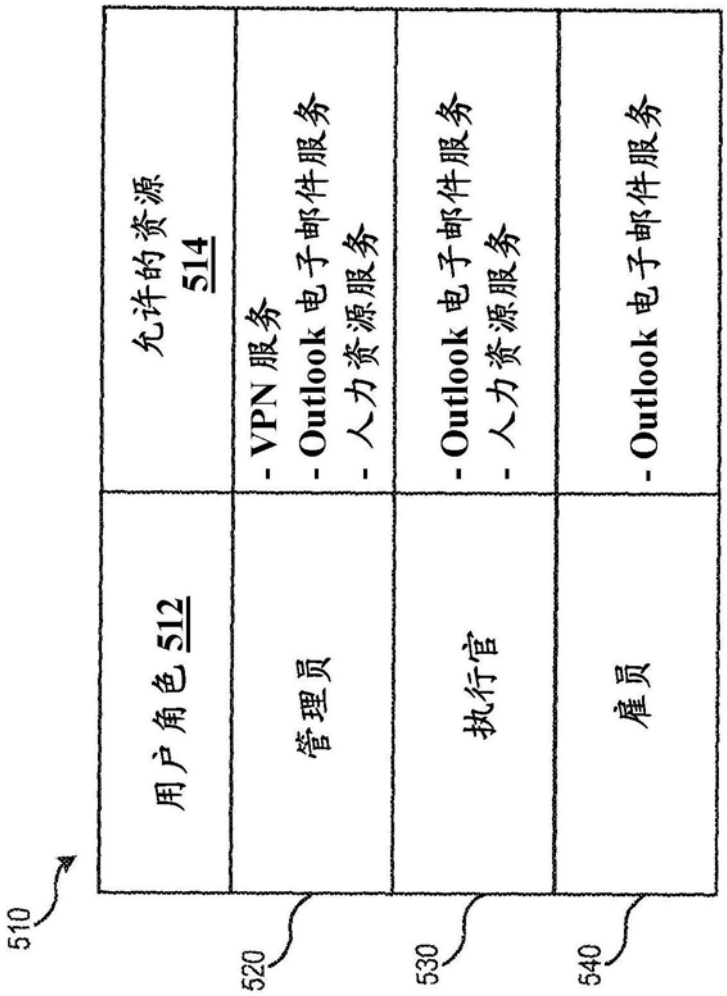

510
用户角色 512
允许的资源 514
管理员
- VPN 服务
- Outlook 电子邮件服务
- 人力资源服务
520
执行官
- Outlook 电子邮件服务
- 人力资源服务
530
雇员
- Outlook 电子邮件服务
540

图5

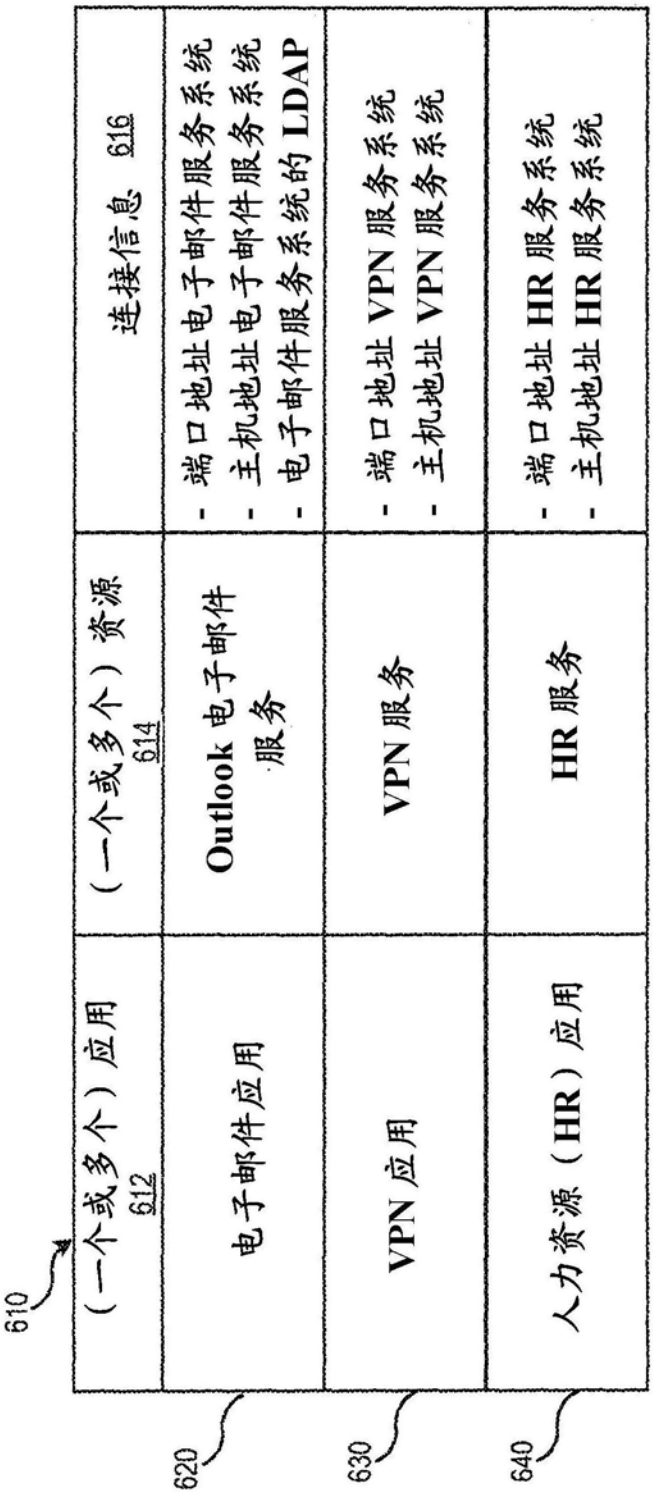

610
（一个或多个）应用 612
（一个或多个）资源 614
连接信息 616
620
电子邮件应用
Outlook 电子邮件服务
- 端口地址电子邮件服务系统
- 主机地址电子邮件服务系统
- 电子邮件服务系统的 LDAP
630
VPN 应用
VPN 服务
- 端口地址 VPN 服务系统
- 主机地址 VPN 服务系统
640
人力资源（HR）应用
HR 服务
- 端口地址 HR 服务系统
- 主机地址 HR 服务系统

图6

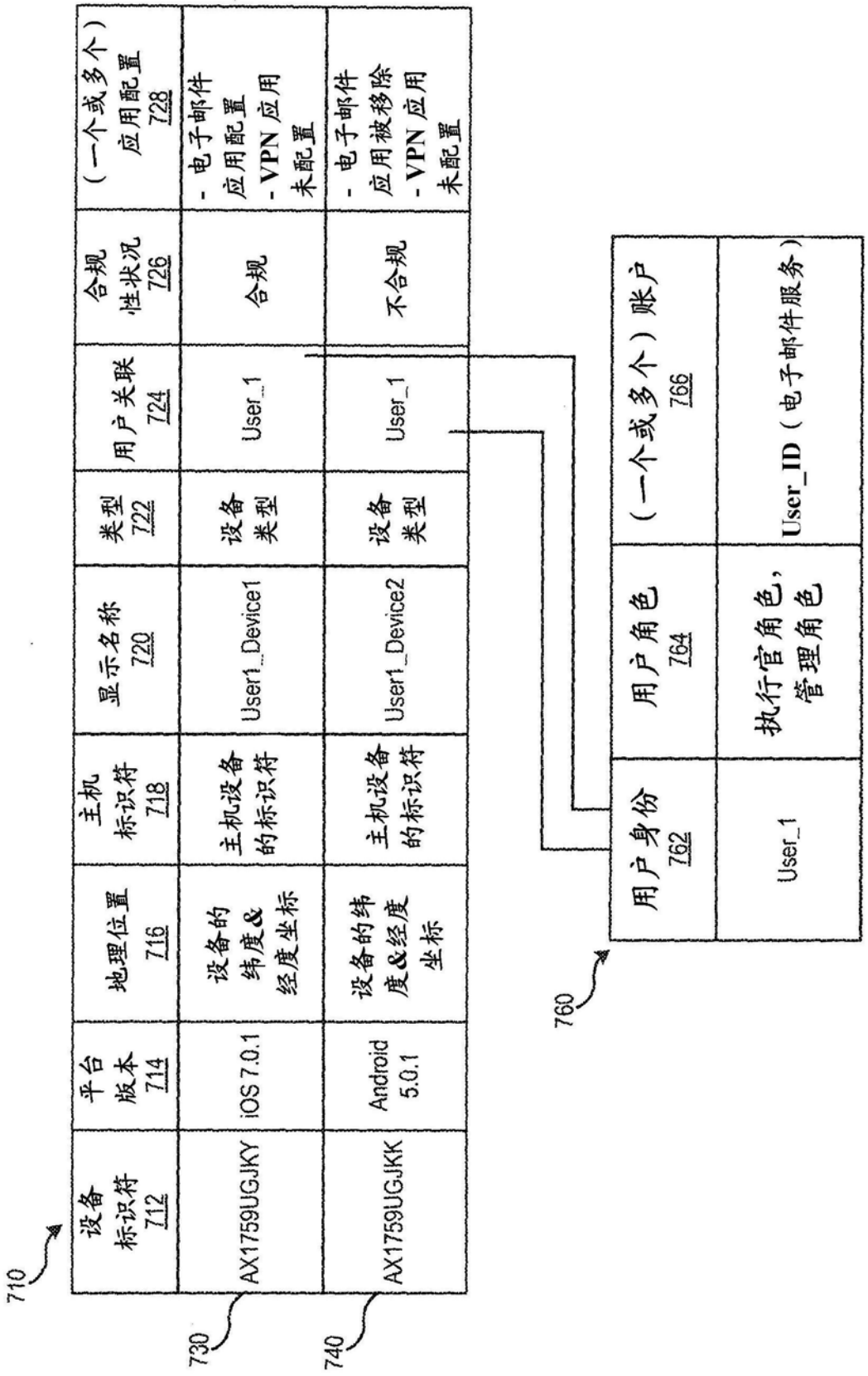

710
设备标识符 712
平台版本 714
地理位置 716
主机标识符 718
显示名称 720
类型 722
用户关联 724
合规性状况 726
（一个或多个）应用配置 728
730
AX1759UGJKY
iOS 7.0.1
设备的纬度&经度坐标
主机设备的标识符
User1_Device1
设备类型
User_1
合规
- 电子邮件应用配置
- VPN 应用未配置
740
AX1759UGJKK
Android 5.0.1
设备的纬度&经度坐标
主机设备的标识符
User1_Device2
设备类型
User_1
不合规
- 电子邮件应用被移除
- VPN 应用未配置
760
用户身份 762
用户角色 764
（一个或多个）账户 766
User_1
执行官角色，管理角色
User_ID（电子邮件服务）

图7

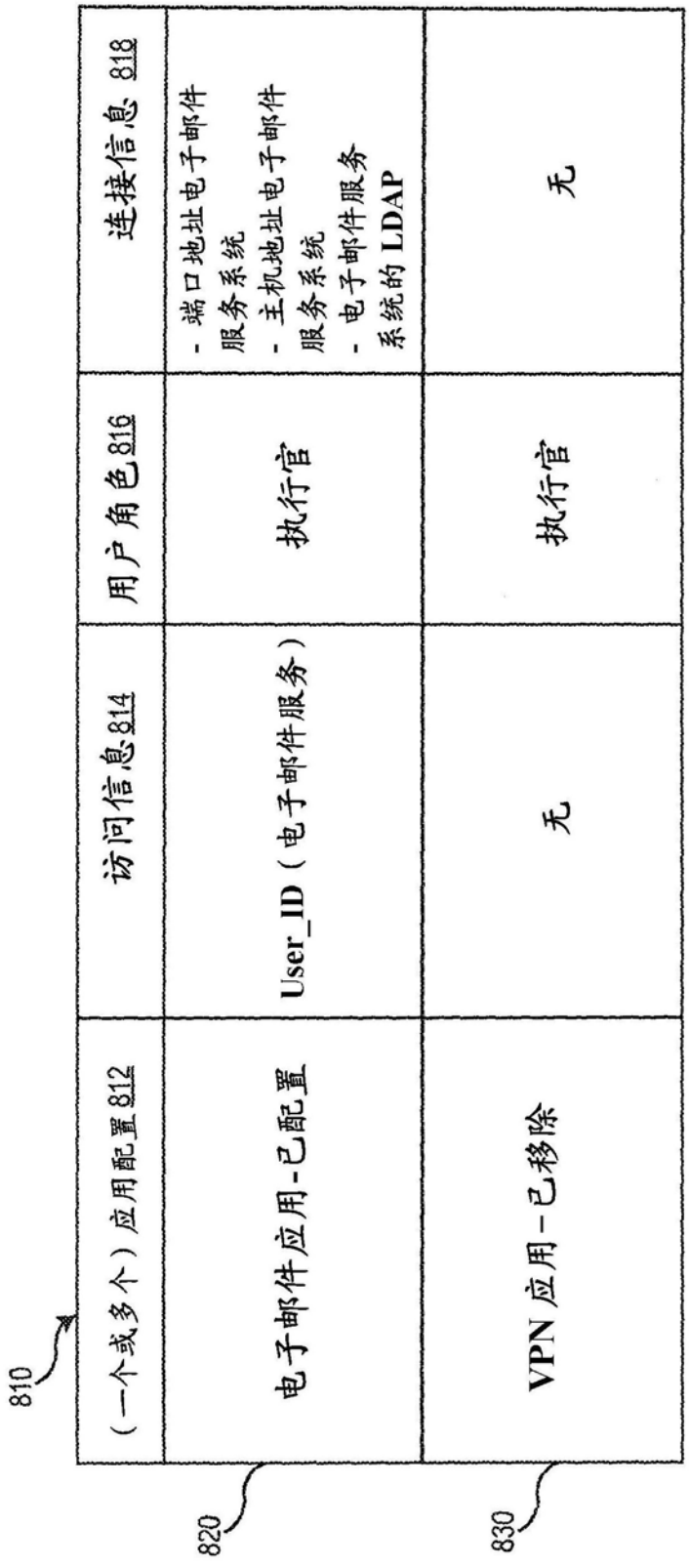

810
820
830
（一个或多个）应用配置812
访问信息814
用户角色816
连接信息 818
电子邮件应用-已配置
User_ID（电子邮件服务）
执行官
- 端口地址电子邮件服务系统
- 主机地址电子邮件服务系统
- 电子邮件服务系统的 LDAP
VPN 应用－已移除
无
执行官
无

图8

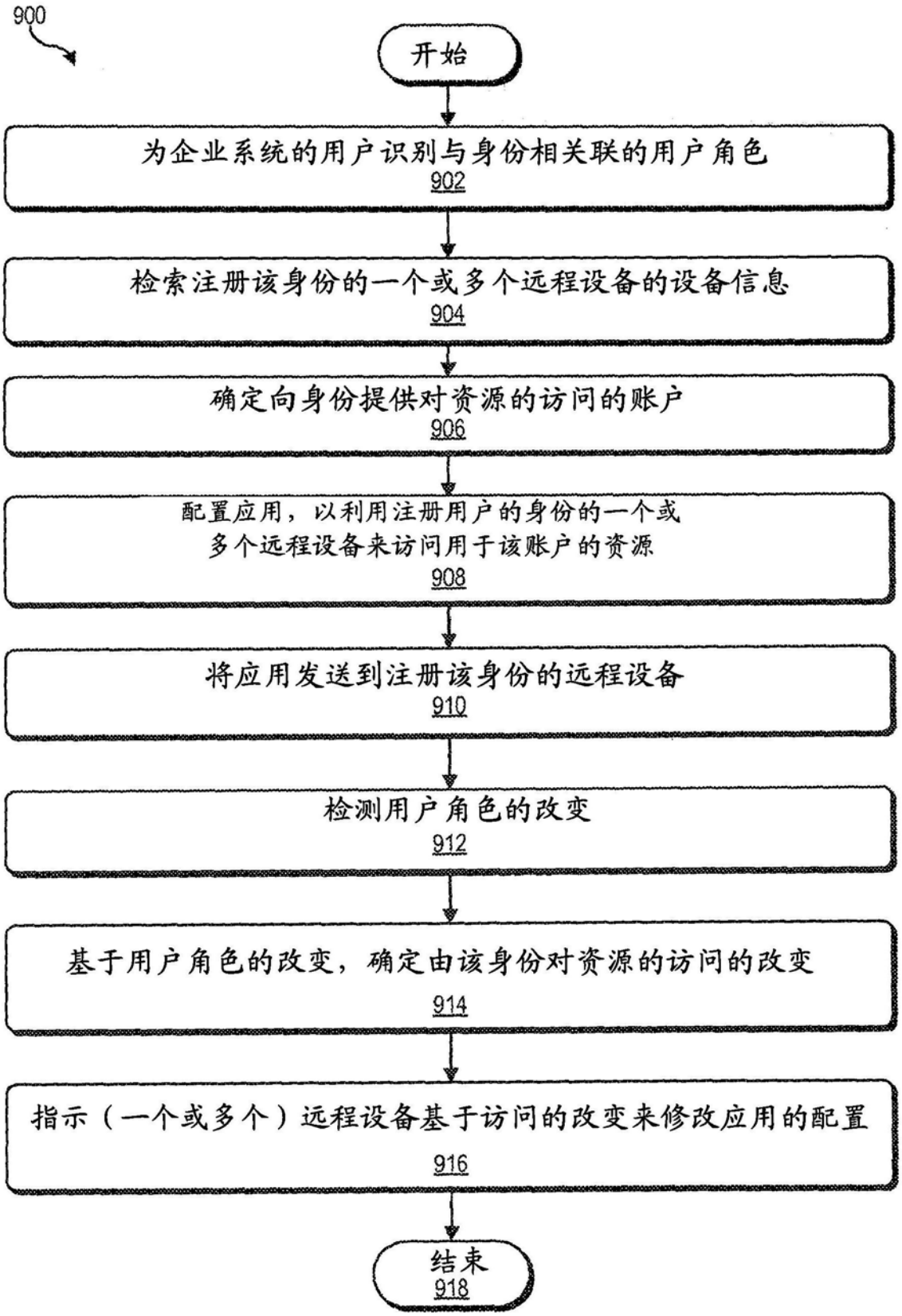

900
开始
为企业系统的用户识别与身份相关联的用户角色
902
检索注册该身份的一个或多个远程设备的设备信息
904
确定向身份提供对资源的访问的账户
906
配置应用，以利用注册用户的身份的一个或多个远程设备来访问用于该账户的资源
908
将应用发送到注册该身份的远程设备
910
检测用户角色的改变
912
基于用户角色的改变，确定由该身份对资源的访问的改变
914
指示（一个或多个）远程设备基于访问的改变来修改应用的配置
916
结束
918

图9

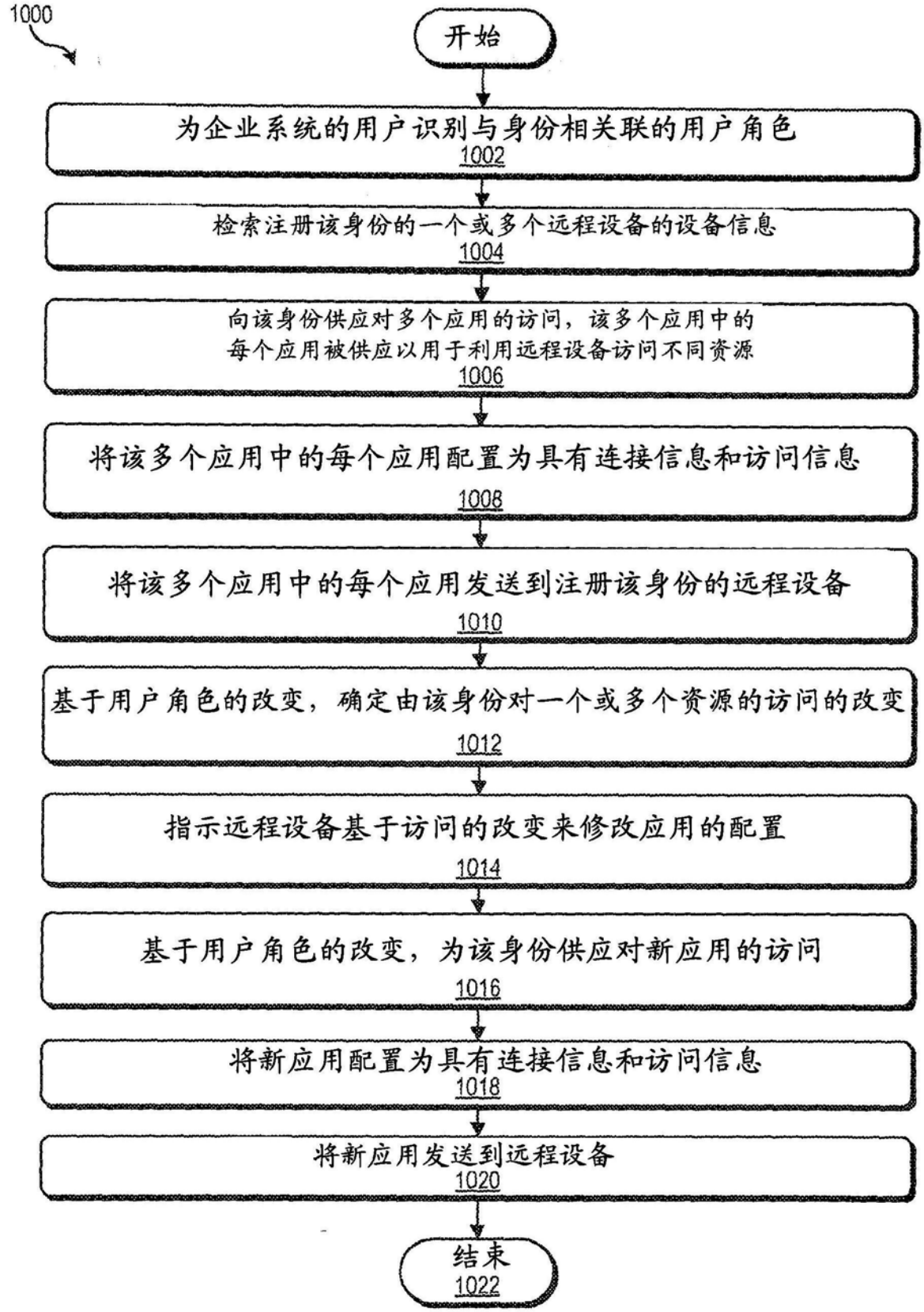

1000
开始
为企业系统的用户识别与身份相关联的用户角色
1002
检索注册该身份的一个或多个远程设备的设备信息
1004
向该身份供应对多个应用的访问，该多个应用中的每个应用被供应以用于利用远程设备访问不同资源
1006
将该多个应用中的每个应用配置为具有连接信息和访问信息
1008
将该多个应用中的每个应用发送到注册该身份的远程设备
1010
基于用户角色的改变，确定由该身份对一个或多个资源的访问的改变
1012
指示远程设备基于访问的改变来修改应用的配置
1014
基于用户角色的改变，为该身份供应对新应用的访问
1016
将新应用配置为具有连接信息和访问信息
1018
将新应用发送到远程设备
1020
结束
1022

图10

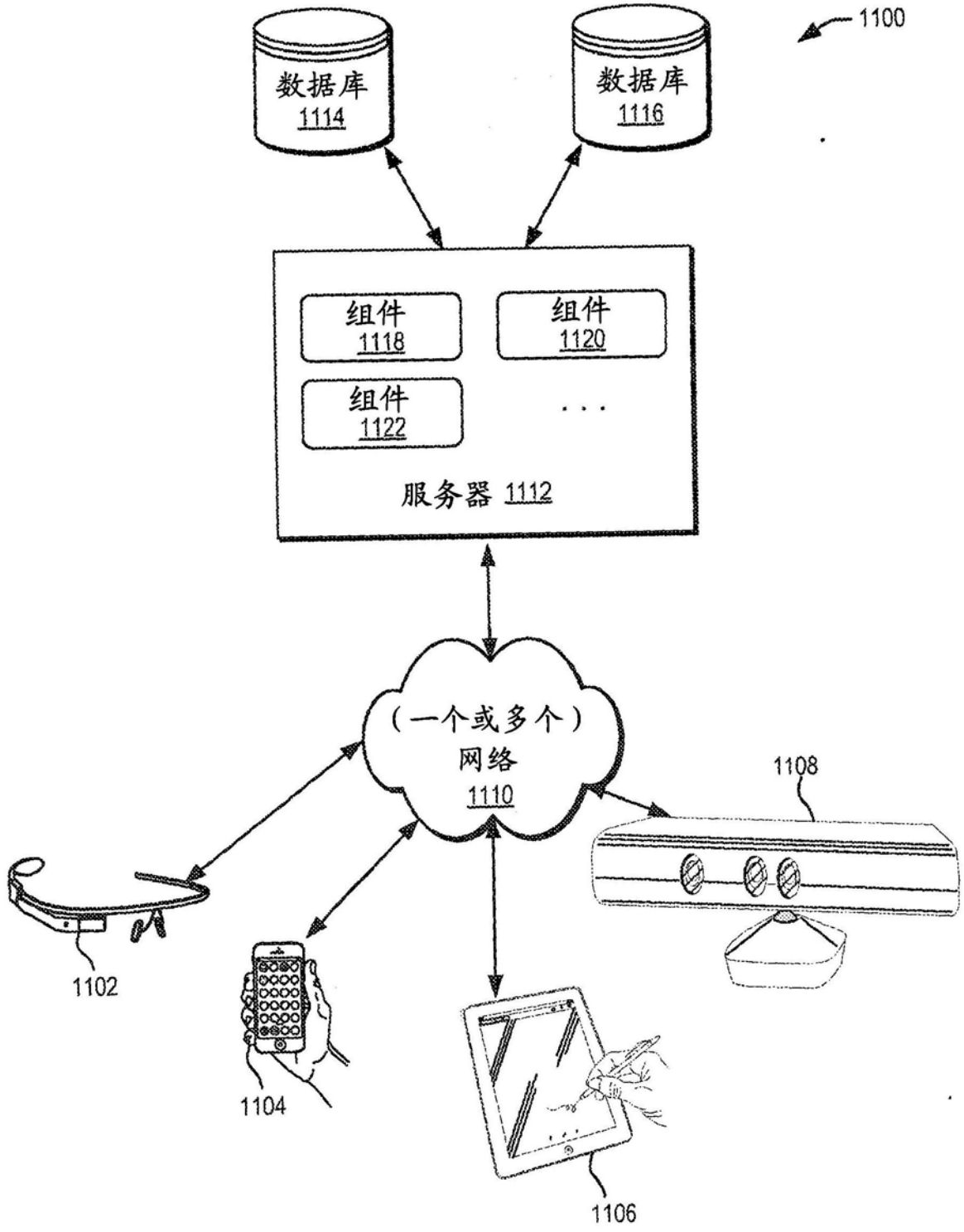

1100
数据库
1114
数据库
1116
组件
1118
组件
1120
组件
1122
. . .
服务器 1112
（一个或多个）
网络
1110
1108
1102
1104
1106

图11

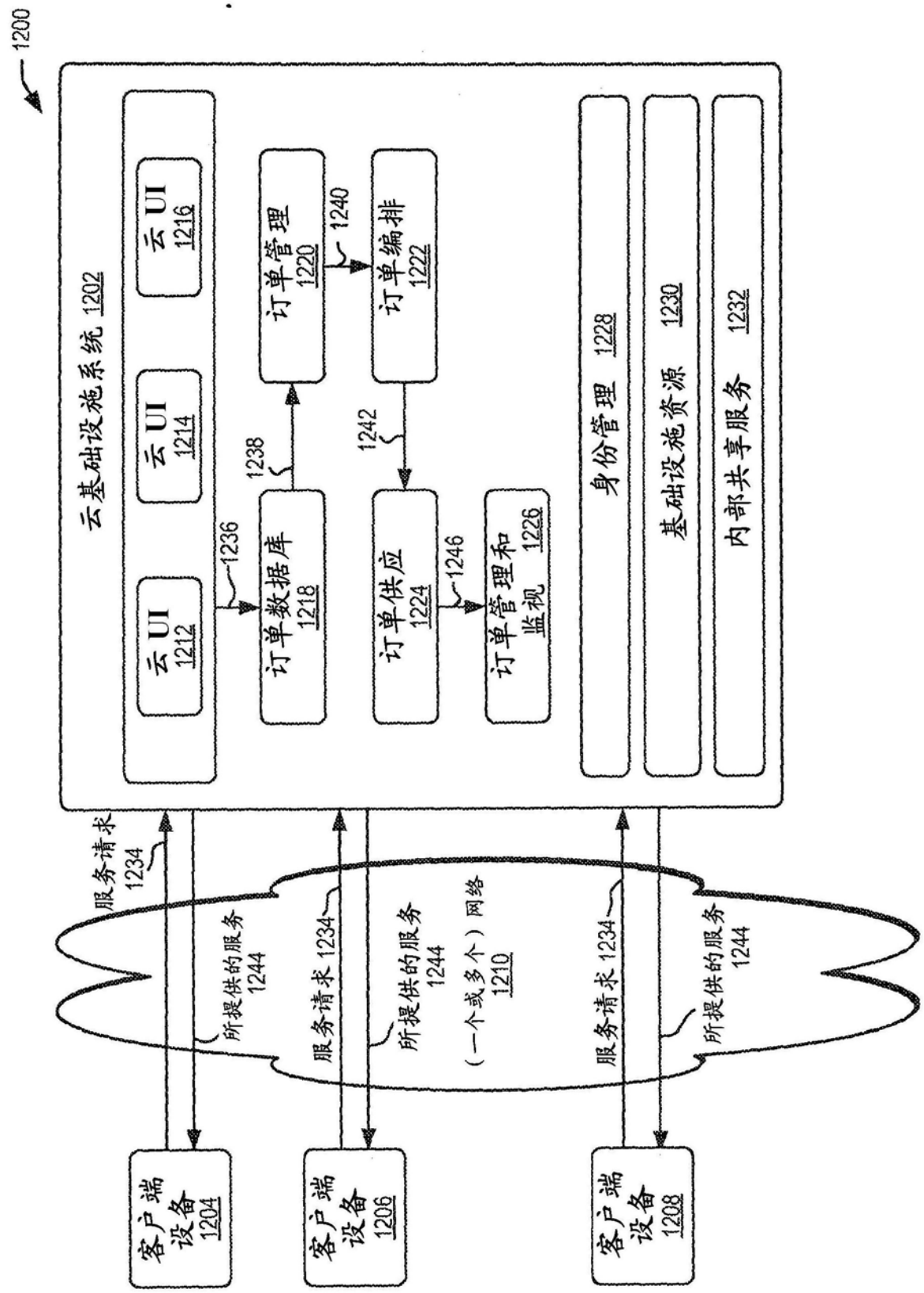

1200
云基础设施系统 1202
云 UI 1212
云 UI 1214
云 UI 1216
订单数据库 1218
订单管理 1220
订单编排 1222
订单供应 1224
订单管理和监视 1226
身份管理 1228
基础设施资源 1230
内部共享服务 1232
1236
1238
1240
1242
1246
服务请求 1234
所提供的服务 1244
（一个或多个）网络 1210
客户端设备 1204
客户端设备 1206
客户端设备 1208

图12

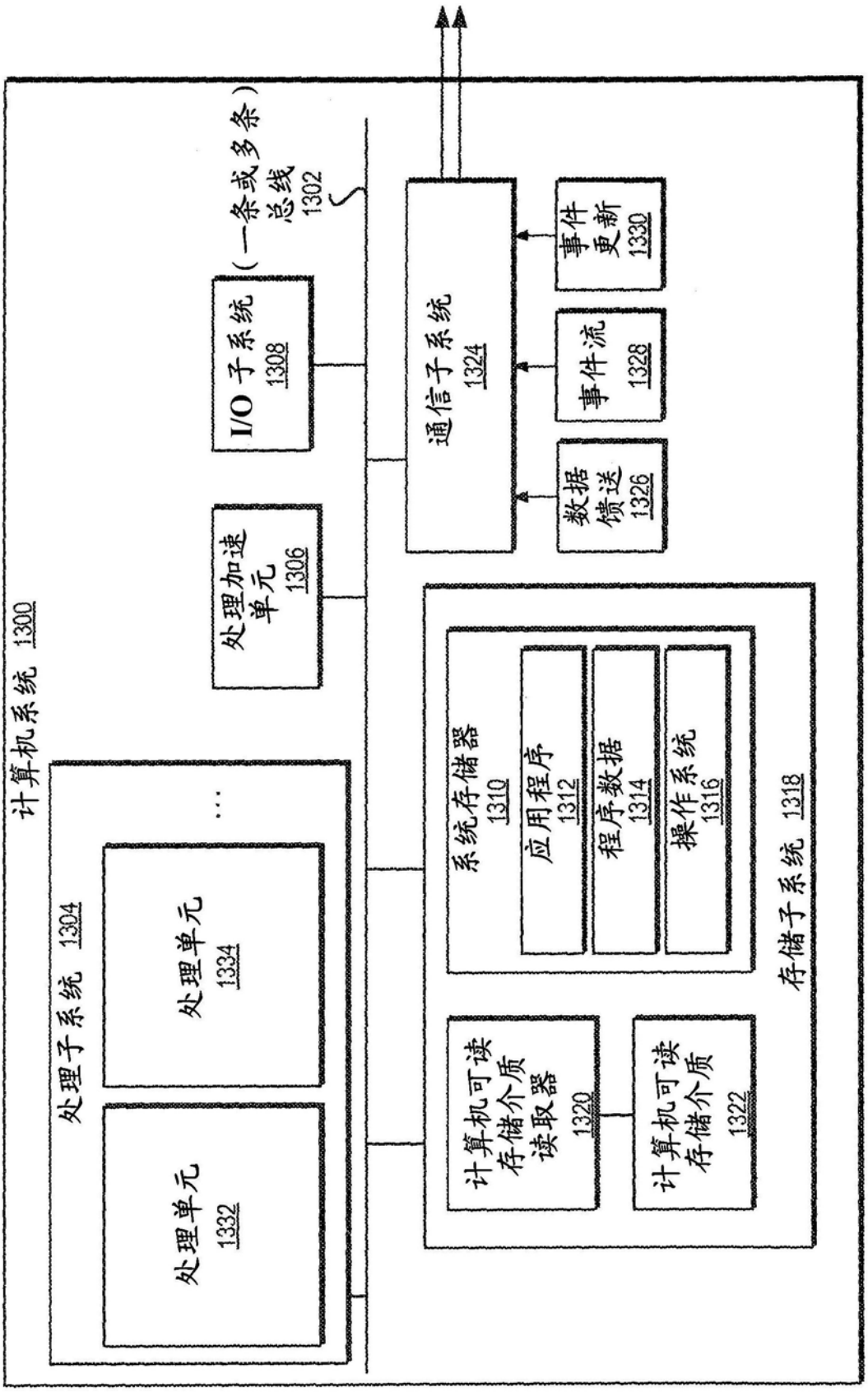

计算机系统 1300
处理子系统 1304
处理单元 1332
处理单元 1334
...
处理加速单元 1306
I/O 子系统 1308
(一条或多条)总线 1302
通信子系统 1324
事件更新 1330
事件流 1328
数据馈送 1326
存储子系统 1318
系统存储器 1310
应用程序 1312
程序数据 1314
操作系统 1316
计算机可读存储介质读取器 1320
计算机可读存储介质 1322

图13