(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 105074692 B
(45)授权公告日 2018.02.06

(21)申请号 201480017932.5

(22)申请日 2014.04.09

(65)同一申请的已公布的文献号
申请公布号 CN 105074692 A

(43)申请公布日 2015.11.18

(30)优先权数据
61/810,480 2013.04.10 US
61/899,468 2013.11.04 US

(85)PCT国际申请进入国家阶段日
2015.09.24

(86)PCT国际申请的申请数据
PCT/US2014/033540 2014.04.09

(87)PCT国际申请的公布数据
WO2014/169062 EN 2014.10.16

(73)专利权人 伊尔拉米公司
地址 美国加利福尼亚州

(72)发明人 P·J·柯纳 D·R·库克
J·G·范德利 M·K·格伦
M·格普塔 A·S·鲁宾
J·B·斯科特 S·常
A·B·斯托克尔

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华

(51)Int.Cl.
*G06F 17/00*(2006.01)

(56)对比文件
CN 102379139 A,2012.03.14,
CN 102204267 A,2011.09.28,
US 7813484 B2,2010.10.12,
US 2010064009 A1,2010.03.11,
US 2004039803 A1,2004.02.26,
US 7418490 B1,2008.08.26,
US 2008060080 A1,2008.03.06,
US 2004039789 A1,2004.02.26,
US 2012023546 A1,2012.01.26,
US 7747736 B2,2010.06.29,

审查员 王高云

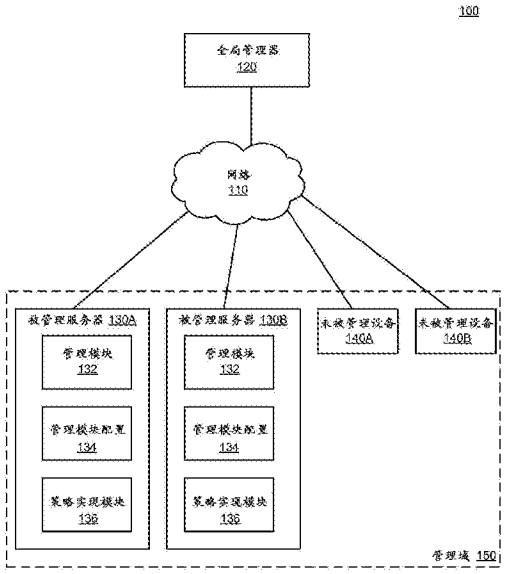
权利要求书3页 说明书22页 附图8页

(54)发明名称

使用基于逻辑多维标签的策略模型的分布式网络管理系统

(57)摘要

处理管理域内的特定被管理服务器的状态的变化。管理域包括多个被管理服务器，多个被管理服务器使用管理指令来配置管理模块，使得所配置的管理模块实现包括一个或多个规则的集合的管理域范围管理策略。修改特定被管理服务器的第一描述，以指示所述特定被管理服务器的改变的状态，从而指定特定被管理服务器的第二描述。将未修改的第一描述与第二描述相比较，从而指定描述变化。基于描述变化确定，做出关于是否更新先前向特定被管理服务器发送的管理指令的确定。




CN 105074692 B

1.一种处理多个被管理服务器中所包括的特定被管理服务器的状态的变化的方法，所述多个被管理服务器使用管理指令来配置管理模块，使得配置的所述管理模块实现一个或多个规则的集合，所述方法包括：

存储所述一个或多个规则的集合，每个规则指定规则功能、服务、描述哪些被管理服务器能够提供所述服务的提供者部分、以及描述哪些被管理服务器能够使用所述服务的使用者部分；

修改所述特定被管理服务器的第一描述以指示所述特定被管理服务器的改变的状态，从而指定所述特定被管理服务器的第二描述；

比较未修改的所述第一描述与所述第二描述，从而指定描述变化；

基于所述第二描述来确定所述规则的集合中的哪些规则指定可应用于所述特定被管理服务器的提供者部分或使用者部分，从而指定当前相关规则；

确定所述当前相关规则是否不同于先前相关规则，其中所述先前相关规则基于未修改的所述第一描述而被确定；以及

响应于确定所述当前相关规则不同于所述先前相关规则：

确定相对于所述先前相关规则应当被添加的规则；

基于所确定的规则来生成功能级指令；以及

向所述特定被管理服务器发送所述功能级指令以及用于添加所述功能级指令的指令。

2.根据权利要求1所述的方法，还包括：基于所述描述变化来确定是否更新先前向所述特定被管理服务器发送的管理指令，其中所述被管理服务器响应于确定更新所述特定被管理服务器的管理指令而确定所述当前相关规则是否不同于先前相关规则。

3.根据权利要求2所述的方法，还包括响应于确定更新所述特定被管理服务器的管理指令并且响应于确定所述当前相关规则不同于所述先前相关规则：

更新高速缓存的参与者集合以指示所述特定被管理服务器的改变的状态，从而指定更新的参与者集合；

确定哪些更新的参与者集合与所述特定被管理服务器相关，从而指定当前相关更新的参与者集合；

确定所述当前相关更新的参与者集合是否不同于先前向所述特定被管理服务器发送的参与者集合；以及

响应于确定所述当前相关更新的参与者集合不同于先前发送的所述参与者集合：

确定相对于先前发送的所述参与者集合应当被添加的更新的参与者集合；以及

向所述特定被管理服务器发送所述更新的参与者集合以及用于添加所述更新的参与者集合的指令。

4.根据权利要求3所述的方法，其中确定哪些更新的参与者集合与所述特定被管理服务器相关包括：分析所述当前相关规则的提供者部分和使用者部分，以确定特定参与者集合是否由所述当前相关规则的提供者部分和使用者部分中的任一个引用。

5.根据权利要求3所述的方法，其中所述更新的参与者集合包括参与者集合记录，每个参与者集合记录包括被管理服务器的唯一标识符、所述被管理服务器的操作系统的标识符以及所述被管理服务器的IP地址。

6.根据权利要求2所述的方法，其中确定是否更新先前向所述特定被管理服务器发送

的管理指令包括：

确定所述描述变化是否指示所述特定被管理服务器从在线转到离线；以及

响应于确定所述描述变化指示所述特定被管理服务器从在线转到离线，确定不更新所述特定被管理服务器的管理指令。

7.根据权利要求2所述的方法，其中确定是否更新先前向所述特定被管理服务器发送的管理指令包括：

确定所述描述变化是否指示所述特定被管理服务器从离线转到在线；以及

响应于确定所述描述变化指示所述特定被管理服务器从离线转到在线，确定更新所述特定被管理服务器的管理指令。

8.根据权利要求2所述的方法，其中确定是否更新先前向所述特定被管理服务器发送的管理指令包括：

确定所述描述变化是否包括标签集合变化或者配置的特性变化；以及

响应于确定所述描述变化包括标签集合变化或者配置的特性变化，确定更新所述特定被管理服务器的管理指令。

9.根据权利要求2所述的方法，其中确定是否更新先前向所述特定被管理服务器发送的管理指令包括：

确定所述描述变化是否包括网络曝光信息变化；以及

响应于确定所述描述变化包括网络曝光信息变化，确定更新所述特定被管理服务器的管理指令。

10.根据权利要求1所述的方法，其中所述描述变化包括离线/在线变化、标签集合变化、配置的特性变化或网络曝光信息变化。

11.根据权利要求1所述的方法，还包括在比较未修改的所述第一描述与所述第二描述之前：

基于所述第二描述来确定关于所述特定被管理服务器的附加信息；以及

修改所述第二描述以指示所述附加信息。

12.根据权利要求1所述的方法，其中所述功能级指令指定相同的规则功能作为所确定的规则、相同的服务部分作为所确定的规则、描述所述被管理服务器中能够提供所述服务的一个被管理服务器的提供者部分、描述所述被管理服务器中能够使用所述服务的一个被管理服务器的使用者部分，所述被管理服务器由所述功能级指令的所述提供者部分或所述功能级指令的所述使用者部分中的任一个指定。

13.一种用于处理管理域内的特定被管理服务器的状态的变化的装置，其中所述管理域包括多个被管理服务器，所述多个被管理服务器使用管理指令来配置管理模块，使得配置的所述管理模块实现包括一个或多个规则的集合的管理域范围管理策略，所述装置可执行用于执行权利要求1-12中任一项所述的方法。

14.一种用于处理多个被管理服务器中所包括的特定被管理服务器的状态的变化的系统，所述多个被管理服务器使用管理指令来配置管理模块，使得配置的所述管理模块实现一个或多个规则的集合，所述系统包括：

非瞬态计算机可读存储装置，以及

计算机处理器，所述计算机处理器用于执行以下步骤：

存储所述一个或多个规则的集合，每个规则指定规则功能、服务、描述哪些被管理服务器能够提供所述服务的提供者部分、以及描述哪些被管理服务器能够使用所述服务的使用者部分；

修改所述特定被管理服务器的第一描述以指示所述特定被管理服务器的改变的状态，从而指定所述特定被管理服务器的第二描述；

比较未修改的所述第一描述与所述第二描述，从而指定描述变化；

基于所述第二描述来确定所述规则的集合中的哪些规则指定可应用于所述特定被管理服务器的提供者部分或使用者部分，从而指定当前相关规则；

确定所述当前相关规则是否不同于先前相关规则，其中所述先前相关规则基于未修改的所述第一描述而被确定；以及

响应于确定所述当前相关规则不同于所述先前相关规则：

确定相对于所述先前相关规则应当被添加的规则；

基于所确定的规则来生成功能级指令；以及

向所述特定被管理服务器发送所述功能级指令以及用于添加所述功能级指令的指令。

# 使用基于逻辑多维标签的策略模型的分布式网络管理系统

## 技术领域

[0001] 本文所描述的主题总体上涉及管理管理域的(物理的或虚拟的)服务器的领域，并且更具体地涉及根据附着到基于逻辑多维标签的策略模型的管理域范围策略来管理服务器。

## 背景技术

[0002] 根据策略来管理管理域的(物理的或者虚拟的)服务器。例如，安全策略可以指定访问控制和/或安全连接，而资源使用策略可以指定管理域的计算资源(例如磁盘和外围设备)的使用。传统的策略涉及物理设备并且在低层构造(诸如因特网协议(IP)地址、IP地址范围、子网络和网络接口)方面被表达。这些低层构造使得很难以抽象和自然的方式来写入细粒度的策略。

## 发明内容

[0003] 通过用于处理管理域内的特定被管理服务器的状态的变化的方法、非瞬态计算机可读存储介质以及系统来解决以上以及其他问题。管理域包括多个被管理服务器，该多个被管理服务器使用管理指令配置管理模块，使得所配置的管理模块实现包括一个或多个规则的集合的管理域范围管理策略。该方法的实施例包括修改特定被管理服务器的第一描述，以指示所述特定被管理服务器的改变的状态，从而指定特定被管理服务器的第二描述。该方法还包括将未修改的第一描述与第二描述相比较，从而指定描述变化。该方法还包括基于描述变化来确定是否更新先前向特定被管理服务器发送的管理指令。该方法还包括响应于确定更新所述特定被管理服务器的管理指令：基于第二描述确定规则的集合中的哪些规则当前与特定被管理服务器相关，从而指定当前相关规则；确定当前相关规则是否不同于先前相关规则，其中先前相关规则基于未修改的第一描述而被确定；以及响应于确定当前相关规则与先前相关规则相同，不采取进一步的行动。

[0004] 介质的实施例存储可执行的计算机程序模块以执行步骤。这些步骤包括修改特定被管理服务器的第一描述，以指示所述特定被管理服务器的改变的状态，从而指定特定被管理服务器的第二描述。这些步骤还包括将未修改的第一描述与第二描述相比较，从而指定描述变化。这些步骤还包括基于描述变化来确定是否更新先前向特定被管理服务器发送的管理指令。这些步骤还包括响应于确定更新所述特定被管理服务器的管理指令：基于第二描述确定规则的集合中的哪些规则当前与特定被管理服务器相关，从而指定当前相关规则；确定当前相关规则是否不同于先前相关规则，其中先前相关规则基于未修改的第一描述而被确定；以及响应于确定当前相关规则与先前相关规则相同，不采取进一步的行动。

[0005] 系统的实施例包括非瞬态计算机可读存储介质，该非瞬态计算机可读存储介质存储可执行的计算机程序模块以执行步骤。这些步骤包括修改特定被管理服务器的第一描述，以指示所述特定被管理服务器的改变的状态，从而指定特定被管理服务器的第二描述。这些步骤还包括将未修改的第一描述与第二描述相比较，从而指定描述变化。这些步骤还

包括基于描述变化来确定是否更新先前向特定被管理服务器发送的管理指令。这些步骤还包括响应于确定更新所述特定被管理服务器的管理指令：基于第二描述确定规则的集合中的哪些规则当前与特定被管理服务器相关，从而指定当前相关规则；确定当前相关规则是否不同于先前相关规则，其中先前相关规则基于未修改的第一描述而被确定；以及响应于确定当前相关规则与先前相关规则相同，不采取进一步的行动。

## 附图说明

[0006] 图1是图示根据一个实施例的用于管理管理域的(物理的或虚拟的)服务器的环境的高层框图。

[0007] 图2是图示根据一个实施例的用于用作图1中图示的实体中的一个或多个实体的计算机的示例的高层框图。

[0008] 图3是图示根据一个实施例的全局管理器的详细视图的高层框图。

[0009] 图4是图示根据一个实施例的被管理服务器的策略实现模块的详细视图的高层框图。

[0010] 图5是图示根据一个实施例的生成针对特定被管理服务器的管理指令的方法的流程图。

[0011] 图6是图示根据一个实施例的生成用于被管理服务器的管理模块的配置的方法的流程图。

[0012] 图7是图示根据一个实施例的监视被管理服务器的本地状态并且向全局管理器发送本地状态信息的方法的流程图。

[0013] 图8是图示根据一个实施例的处理管理域的计算机网络架构的状态的变化的方法的流程图。

## 具体实施方式

[0014] 附图和以下描述仅通过说明的方式来描述某些实施例。本领域技术人员根据以下描述应当认识到，可以在不偏离本文中所描述的原理的情况下采用本文中说明的结构和方法的替选实施例。现在将参考若干实施例，这些实施例的示例在附图中被图示。应当注意，任何可用的类似的或者相似的参考标记可以在附图中被使用并且可以表示类似的或者相似的功能。

[0015] 图1是图示根据一个实施例的用于管理管理域150的(物理的或者虚拟的)服务器130的环境100的高层框图。管理域150可以对应于企业，诸如例如服务提供者、公司、大学或者政府机关。环境100可以由企业自身来维护，或者可以由帮助企业管理其服务器130的第三方(例如第二企业)来维护。如所示出的，环境100包括网络110、全局管理器120、多个被管理服务器130和多个未被管理设备140。多个被管理服务器130和多个未被管理设备140与管理域150相关联。例如，它们可以由企业或者代表企业的第三方(例如公共云服务提供者)来操作。虽然图1中所描绘的实施例中为了清楚仅示出了1个全局管理器120、2个被管理服务器130和2个未被管理设备140，但是其他实施例可以具有不同数目的全局管理器120、被管理服务器130和/或未被管理设备140。

[0016] 网络110表示全局管理器120、被管理服务器130和未被管理设备140之间的通信路

径。在一个实施例中，网络110使用标准通信技术和/或协议并且可以包括因特网。在另一个实施例中，网络110上的企业可以使用定制和/或专用数据通信技术。

[0017] 被管理服务器130是实现管理域范围管理策略330(图3中所示)的(物理的或者虚拟的)机器。在一个实施例中，服务器是根据操作系统水平的虚拟化的虚拟服务器(有时被称为容纳器、虚拟化引擎、虚拟专用服务器或者监禁)的用户空间实例，其是在其中操作系统的内核实现多个单独的用户空间实例而非仅一个实例的服务器虚拟化方法。如果被管理服务器130是物理的机器，则被管理服务器130是计算机或者计算机的集合。如果被管理服务器130是虚拟的机器，则被管理服务器130在计算机或者计算机的集合上执行。管理域范围管理策略330指定是否和/或如何允许与管理域150相关联的实体访问其他实体(或被其他实体访问)或者消耗(或提供)服务。例如，管理域范围管理策略330指定安全或资源使用。安全策略可以指定访问控制、安全连接、磁盘加密和/或可执行过程的控制，而资源使用策略可以指定管理域的计算资源(例如磁盘、外围设备和/或带宽)的使用。

[0018] 被管理服务器130包括管理模块132、管理模块配置134和策略实现模块136。管理模块132实现管理域范围管理策略330。例如，在安全的情况下，管理模块132可以是低层网络或者安全引擎，诸如操作系统层的防火墙、因特网协议安全(IPsec)引擎、或者网络流量过滤引擎(例如基于Windows过滤平台(WFP)开发平台)。在资源使用的情况下，管理模块132可以是磁盘使用引擎或者外围设备使用引擎。

[0019] 管理模块配置134影响管理模块132的操作。例如，在安全的情况下，管理模块配置134可以是由防火墙应用的访问控制规则、由IPsec引擎应用(例如在Linux操作系统中被实施为iptable实体和ipset实体)的安全连接策略、或者由过滤引擎应用的过滤规则。在资源使用的情况下，管理模块配置134可以是由磁盘使用引擎应用的磁盘使用策略或者由外围设备使用引擎应用的外围设备使用策略。

[0020] 策略实现模块136基于a)从全局管理器120接收的管理指令和b)被管理服务器130的状态，来生成管理模块配置134。管理指令至少部分地基于管理域范围管理策略330而被生成。由策略实现模块136生成的管理模块配置134实现该管理域范围管理策略330(在策略涉及被管理服务器130的程度上)。这个两步骤过程(生成管理指令和生成管理模块配置134)被称为“实例化”管理策略。策略实现模块136还监视被管理服务器130的本地状态并且向全局管理器120发送本地状态信息。

[0021] 在一个实施例中，策略实现模块136是更大的专有模块(未示出)的一部分。专有模块被加载到已经具有管理模块132和管理模块配置134的设备上，从而从未被管理设备140向被管理服务器130变换设备。下面参考图4、6和7进一步描述策略实现模块136。

[0022] 未被管理设备140是不包括策略实现模块136的计算机(或者计算机的集合)。未被管理设备140不实现管理域范围管理策略330。然而，被管理服务器130与未被管理设备140之间的交互可以受制于管理域范围管理策略330(如由被管理服务器130实现)。未被管理设备140的一个示例是由管理域150使用的网络电路。未被管理设备140的另一示例是由个人使用以向管理域150认证他自己的设备(例如笔记本或台式计算机、平板计算机、或者移动电话)。

[0023] 全局管理器120是生成用于被管理服务器130的管理指令并且向服务器发送所生成的管理指令的计算机(或者计算机的集合)。基于a)管理域的计算机网络架构的状态320

以及b)管理域范围管理策略330，来生成管理指令。管理域的计算机网络架构的状态320包括被管理服务器130的描述以及(可选地)包括未被管理设备140的描述。全局管理器120还处理从被管理服务器130接收的本地状态信息。

[0024] 管理域范围管理策略330基于不涉及使用低层构造(诸如IP地址、IP地址范围、子网络和网络接口)的被管理服务器130的逻辑管理模型。相反，逻辑管理模型基于它们的高层特性(本文中被称为“标签”)涉及被管理服务器130。标签是包括“维度”(高层特性)和“值”(该高层特性的值)的对。在该多维空间中构造的管理策略比根据基于单特性网络/IP地址的策略模型构造的管理策略更有表现力。具体地，使用“标签”的高层抽象来表达管理策略使得人们能够更好地理解、虚拟化和修改管理策略。

[0025] 逻辑管理模型(例如可用维度的数目和类型以及这些维度的可能的值)是可配置的。在一个实施例中，逻辑管理模型包括下面的维度和值，如表1所示：

[0026]

| **维度** | **含义 (M), 值 (V)** |
|---|---|
| 角色 | M: 管理域内的被管理服务器的角色。<br>V: web、API、数据库 |
| 环境 | M: 被管理服务器的生命周期阶段。<br>V: 生产、分段、开发 |
| 应用 | M: 被管理服务器所属的逻辑应用（被管理服务器的高层分组）。<br>V: 交易、人力资源 |
| 业务范围 | M: 被管理服务器所属的业务单元。<br>V: 营销、工程 |
| 位置 | M: 被管理服务器的位置。可以是物理的（例 |

[0027]

| | |
|---|---|
| | 如国家或地理区域）或逻辑的（例如网络）。物理位置对于表达地理合规要求特别有用。<br>V: 美国或者欧洲（物理的）、美国西部 1 或者美国东部 2（逻辑的） |

[0028] 表1-逻辑管理模型的示例

[0029] 逻辑管理模型使得能够通过指定描述组中的所有被管理服务器130的一个或多个标签(本文中被称为“标签集合”)来将多个被管理服务器130分组在一起。标签集合包括用于逻辑管理模型中的维度的0值或者1值。标签集合不需要包括用于逻辑管理模型中的所有维度的标签。通过该方式，逻辑管理模型实现管理域的被管理服务器130的分段和分离以及被管理服务器130的任意分组的创建。逻辑管理模型还允许单个被管理服务器130存在于多

个交叠的集合(即被管理服务器的多个交叠的组)中。逻辑管理模型没有将单个被管理服务器130限制为存在于嵌套的集合的层级中。

[0030] 例如,在安全的情况下,可以与访问控制策略一起使用分段以定义受制于特定策略的被管理服务器130的组。类似地,可以与安全连接策略一起使用分段以定义被管理服务器130的组以及应用于组内通信和组间通信的策略。因此,可以将被管理服务器130的(由第一标签集合来指定)第一组之间的通信限制为第一安全连接设置(例如不要求的安全连接),并且可以将被管理服务器的第一组与被管理服务器的(由第二标签集合来指定)第二组之间的通信限制为第二安全连接设置(例如,IPsec软件包安全载荷(ESP)/认证报头(AH)高级加密标准(AES)/安全散列算法2(SHA-2))。

[0031] 环境100中的每个被管理服务器130实现管理域范围管理策略330(在策略涉及被管理服务器130的程度上)。因此,遍及管理域150以分布式方式来应用管理域范围管理策略330,并且不存在瓶颈。另外,在逻辑层独立于管理域的物理网络拓扑结构和网络寻址方案来应用管理域范围管理策略330。

[0032] 下面参考图3、5和8来进一步描述全局管理器120、管理域的计算机网络架构的状态320以及管理域范围管理策略330。

[0033] 图2是图示根据一个实施例的用于用作图1中图示的实体中的一个或多个实体的计算机200的示例的高层框图。图示的是耦合到芯片集204的至少一个处理器202。芯片集204包括存储器控制器集线器220和输入/输出(I/O)控制器集线器222。存储器206和图形适配器212耦合到存储器控制器集线器220,并且显示设备218耦合到图形适配器212。存储设备208、键盘210、指向设备214和网络适配器216耦合到I/O控制器集线器222。计算机200的其他实施例具有不同的架构。例如,在一些实施例中,存储器206直接耦合到处理器202。

[0034] 存储设备208包括一个或多个非瞬态计算机可读存储介质,诸如硬盘驱动器、光盘只读存储器(CD-ROM)、DVD或者固态存储器设备。存储器206保持由处理器202使用的指令和数据。指向设备214结合键盘210用于向计算机系统200中输入数据。图形适配器212在显示设备218上显示图像和其他信息。在一些实施例中,显示设备218包括用于接收用户输入和选择的触摸屏能力。网络适配器216将计算机系统200耦合到网络110。计算机200的一些实施例与图2所示的部件相比具有不同的和/或其他的部件。例如,全局管理器120和/或被管理服务器130可以由多个刀片服务器形成并且缺少显示器设备、键盘和其他部件,而未被管理设备140可以是笔记本计算机或台式计算机、平板计算机或者移动电话。

[0035] 计算机200被适配为用于提供本文中所描述的功能的执行计算机程序模块。如本文中所使用的,术语“模块”是指用以提供指定的功能的计算机程序指令和/或其他逻辑。因此,可以用硬件、固件和/或软件来实现模块。在一个实施例中,由可执行计算机程序指令形成的程序模块被存储在存储设备208上,被加载到存储器206中,并且由处理器202来执行。

[0036] 图3是图示根据一个实施例的全局管理器120的详细视图的高层框图。全局管理器120包括储存库300和处理服务器310。储存库300是存储管理域的计算机网络架构的状态320和管理域范围管理策略330的计算机(或者计算机的集合)。在一个实施例中,储存库300包括响应于请求而向处理服务器310提供对管理域状态320和管理策略330的访问的服务器。

[0037] 管理域的计算机网络架构的状态320包括被管理服务器130的描述以及(可选地)

包括未被管理设备140的描述。被管理服务器130的描述包括例如唯一标识符(UID)、在线/离线指示符、一个或多个配置的特性(可选)、网络曝光信息、服务信息、以及描述被管理服务器130的一个或多个标签(标签集合)。

[0038] UID唯一地标识被管理服务器130。在线/离线指示符指示被管理服务器130在线还是离线。“配置的特性”存储与被管理服务器130相关联的值并且可以是任何类型的信息(例如,哪个操作系统运行在被管理服务器上的指示)。配置的特性结合规则的条件部分(下面描述)而被使用。

[0039] 网络曝光信息涉及被管理服务器的网络接口。在一个实施例中,网络曝光信息包括(对于每个被管理服务器的网络接口)网络接口附接至其的“双向可读网络”(BRN)的标识符以及用于在BRN内操作的零个或多个IP地址(及其子网络)。在另一实施例中,网络曝光信息包括路由信息和/或被管理服务器是否在网络地址转换器(NAT)之后(以及如果其在NAT之后,则NAT的类型是什么—1:1还是1:N)。BRN是组织内或者跨组织的子网络的集合,其中BRN内的任何节点可以与BRN中的其他节点建立通信。例如,BRN中的所有节点具有唯一的IP地址。换言之,BRN不包含任何NAT。网络曝光信息(例如网络接口的BRN标识符)可以结合规则的条件部分而被使用。

[0040] 服务信息包括例如过程信息和/或软件包(package)信息。过程信息包括例如被管理服务器130正在运行的进程的名称、这些进程正在倾听哪些网络端口和网络接口、哪些用户发起这些进程、这些进程的配置、以及这些过程的命令行启动参数(这些进程对应于提供服务或者使用服务的被管理服务器130)。软件包信息包括例如哪些软件包(可执行文件、库或者其他组件)被安装在被管理服务器130上、这些软件包的版本、这些软件包的配置、以及这些软件包的散列值。

[0041] 未被管理设备140的描述包括例如网络曝光信息(例如未被管理设备的IP地址以及未被管理设备连接到的BRN的标识符)。未被管理设备140是“未被管理设备组”(UDG)的一部分。UDG包括一个或多个未被管理设备140。例如,“总部UDG”可以包括主电路以及由管理域的总部来使用的备份电路,其中每个电路与IP地址相关联。UDG与唯一标识符(UID)相关联。管理域状态320中所存储的与UDG相关的信息包括UDG的UID以及UDG中与未被管理设备140相关的信息(例如它们的网络曝光信息)。

[0042] 可以以各种方式(诸如通过经由图形用户接口(GUI)或者应用编程接口(API)与全局管理器120交互)将被管理服务器130的描述和未被管理设备140的描述加载到管理域状态320中。还可以基于从被管理服务器接收的本地状态信息(下面描述)来将被管理服务器130的描述加载到管理域状态320中。

[0043] 具体地,关于被管理服务器的标签(以及在存在的情况下的配置的特性),可以以甚至更多的方式来执行针对维度的值的分配(或者重新分配)(或者配置的特性的值的设置)。例如,可以作为提供被管理服务器130的一部分使用部署和配置工具来执行分配/设置。可以使用任何这样的工具,包括现成的第三方工具(例如Puppet Labs的Puppet软件、Opscode的Chef软件、或者CFEngine AS的CFEngine软件)以及管理域150可以具有的定制工具。

[0044] 作为另一示例,可以由计算标签和/或配置的特性(“CC”)值的“标签/配置的特性引擎”来执行分配/设置。在一个实施例中,标签/CC引擎基于标签/CC分配规则来计算标签/

CC值。标签/CC分配规则是一种访问来自管理域状态320的数据并且分配标签或CC值(或者建议标签或CC值的分配)的功能。标签/CC分配规则可以预先设置或者用户可配置。例如,全局管理器120包括预定义的规则的集合,但是端用户可以基于用户自己的定制需求来修改和/或删除这些规则和添加新的规则。可以在初始化过程期间针对被管理服务器130评估标签/CC分配规则。然后可以针对任何维度/CC做出标签/CC值建议,并且端用户可以接受或者拒绝这些建议。例如,如果被管理服务器130正在执行Postgres数据库或者MySQL数据库,则建议的标签可以是<角色,数据库>。如果被管理服务器正在执行Linux操作系统,则用于操作系统CC的建议的值可以是"Linux"。

[0045] 在另一实施例中,标签/CC引擎基于聚类分析来计算标签/CC值。例如,标签/CC引擎利用连接的图形的附加启发的最小割和K－means算法的组合来自动标识高度连接的被管理服务器130的聚类。被管理服务器130的聚类可以对应于管理域150中的"应用"(参见表1)。端用户可以选择将用于应用维度(或者任何其他维度)的值整体地应用于那些被管理服务器130。

[0046] 管理域范围管理策略330包括一个或多个规则。广义上而言,"规则"指定服务的一个或多个提供者与该服务的一个或多个消费者之间的关系。

[0047] 规则功能—关系受制于"规则功能",其是规则的实际效果。例如,在安全的情况下,规则功能可以是访问控制、安全连接、磁盘加密或者可执行过程的控制。具有访问控制功能的规则指定消费者是否可以使用提供者的服务。在一个实施例中,访问控制功能使用纯"白名单"模型,这表示仅表达允许的关系,并且所有其他关系默认被阻止。具有安全连接功能的规则指定消费者可以通过哪些安全通道(例如使用点到点数据加密的加密网络会话)来使用提供者的服务。例如,具有安全连接功能的规则可以指定当提供者位于美国并且消费者位于欧洲时必须对提供者的服务的使用进行加密。具有磁盘加密功能的规则指定提供者是否必须将其数据存储在加密文件系统上。具有可执行过程控制功能的规则指定提供者是否必须执行在加密文件系统上。

[0048] 在资源使用的情况下,规则功能可以是磁盘使用或者外围设备使用。具有磁盘使用功能的规则指定消费者可以在提供者上存储的数据的量。注意,规则可以指定其他规则功能以及远超过访问控制、安全连接、磁盘加密、可执行过程的控制、磁盘使用以及外围设备使用。例如,规则功能可以指定要向网络通信应用哪些开放式系统互连(OSI)模型七层服务、针对安全分析采集的元数据的量、或者用于捕获完整的网络分组的触发器。管理策略模型支持可以被应用的任何数目的规则功能。

[0049] 规则功能可以与指定与规则的实际效果相关的细节的一个或多个设置(本文中被称为"功能简档")相关联。例如,与安全连接规则功能相关联的设置可以是用于加密网络通信的加密算法的列表。在一个实施例中,规则功能可以与多个功能简档相关联,并且功能简档包括优先级。该优先级由如下面描述的功能级指令生成模块360来使用。

[0050] 服务—通常,"服务"是使用特定网络协议执行在特定网络端口上的任意过程。管理策略330内的规则的服务由端口/协议对和(可选的)附加资格(诸如过程信息和/或软件包信息(以上在管理域状态320内关于被管理服务器130的描述所描述的))来指定。如果被管理服务器130具有多个网络接口,则可以在所有网络上或者仅在这些网络的子集上曝光服务。端用户指定在哪些网络上曝光服务。

[0051] 提供者/消费者—服务的一个或多个提供者以及服务的一个或多个消费者(即用户)是被管理服务器130和/或未被管理设备140。

[0052] 在一个实施例中，使用包括规则功能部分、服务部分、提供者部分、使用者部分和可选的规则条件部分的信息的集合来在管理域范围管理策略330内表示规则。规则功能部分描述规则的实际效果并且可以与一个或多个设置(功能简档)相关联。服务部分描述规则应用于的服务。如果服务部分指示“所有”，则规则应用于所有服务。

[0053] 由谁提供(PB)部分描述哪些被管理服务器130和/或未被管理设备140可以提供服务(即“提供者”是谁)。如果PB部分指示“任何人”，则任何人(例如任何被管理服务器130或者未被管理设备140)可以提供服务。如果PB部分指示“任何被管理服务器”，则任何被管理服务器130可以提供服务。(“任何被管理服务器”等同于指定包含通配符的标签集合，从而匹配所有的被管理服务器130。)由谁使用(UB)部分描述哪些被管理服务器130和/或未被管理设备140可以使用服务(即“消费者”是谁)。类似于PB部分，UB部分还可以指示“任何人”或者“任何被管理服务器”。

[0054] 在PB部分和UB部分内，使用标签集合(即描述被管理服务器的一个或多个标签)或者UID来指定被管理服务器130。使用标签集合指定被管理服务器130的能力起源于逻辑管理模型，其基于它们的维度和值(标签)来涉及被管理服务器。使用未被管理设备组(UDG)的UID来指定未被管理设备140。如果规则指定UDG，则规则包括与该组中的未被管理设备140相关的附加信息(例如，设备的网络曝光信息)。规则的PB部分和/或规则的UB部分可以包括多个项，包括标签集合(用于指定被管理服务器130)、被管理服务器UID和/或UDG UID。

[0055] 可选的规则条件部分指定规则是否应用于特定的被管理服务器130和/或被管理服务器的特定的网络接口。规则条件部分是包括一个或多个配置的特性(“CC”；管理域状态320中的被管理服务器的描述的一部分)和/或网络曝光信息(例如网络接口的BRN标识符；也是管理域状态320中的被管理服务器的描述的一部分)的布尔表达式。表达式的CC部分指定规则是否应用于特定的被管理服务器，而表达式的网络曝光信息部分指定规则是否应用于被管理服务器的特定的网络接口。如果表达式针对特定的被管理服务器的配置的特性(特定地，对于该被管理服务器的配置的特性的值)和特定的网络接口的信息评估为“真”，则规则应用于该被管理服务器和该被管理服务器的相关网络接口。如果表达式评估为“假”，则规则不应用于该被管理服务器和该被管理服务器的相关网络接口。例如，如果配置的特性存储哪个操作系统运行在被管理服务器上的指示，则包括该配置到特性的规则条件部分可以基于服务器的操作系统来控制规则是否应用于特定的被管理服务器。

[0056] 管理域范围管理策略330内的规则被组织成规则列表。特定地，管理策略330包括一个或多个规则列表，并且规则列表包括一个或多个规则以及(可选地)包括一个或多个范围。“范围”约束规则应用的情况(即应用于哪些被管理服务器130)。范围包括限制规则列表中的规则的应用的由谁提供(PB)部分和由谁使用(UB)部分。范围的PB部分限制规则的PB部分，并且范围的UB部分限制规则的UB部分。范围的PB和UB部分可以通过使用标签集合来指定被管理服务器130的组。如果标签集合不包含针对特定维度的标签，则不存在用于被管理服务器130的所得到的组的该维度的区域划分。如果规则列表不包括任何范围，则其规则被全局应用。

[0057] 不同的范围可以应用于单个规则列表。例如，端用户可以构建表达web服务等级如

何根据数据库等级来消耗服务、负载平衡等级如何根据web服务等级来消耗服务等的规则的集合。因此，如果端用户想要将该规则列表应用于其生产环境以及其分段环境，则他不需要拷贝或者复制规则列表。相反，他将多个范围应用于单个规则列表。范围抽象从可用性全貌(perspective)和计算全貌来做出规则列表缩放。

[0058] 既然已经描述了管理域范围管理策略330，给出一些示例对工作很有帮助。考虑来其中用户设备访问web服务器(第一等级)并且web服务器访问数据库服务器(第二等级)的具有两级应用的管理域150。在第一等级，用户设备是消费者，web设备是提供者。在第二等级，web服务器是消费者，数据库服务器是提供者。管理域150包括该应用的两个实例：一个在生产环境中、一个在分段环境中。

[0059] Web服务器和数据库服务器是被管理服务器130，并且其描述(例如标签集合)存在于管理域状态320中。例如，其标签集合为：生产中的web服务器：<角色，web>和<环境，生产>

[0060] 生产中的数据库服务器：<角色，数据库>和<环境，生产>

[0061] 分段中的web服务器：<角色，web>和<环境，分段>

[0062] 分段中的数据库服务器：<角色，数据库>和<环境，分段>

[0063] (应用维度、业务范围维度和位置维度与本示例不相关，因此省略了其标签。)

[0064] 现在考虑下面的管理域范围管理策略330，其是指定访问控制和安全连接的安全策略：

[0065] ●范围

[0066] ○<环境，产品>

[0067] ○<环境，分段>

[0068] ●规则

[0069] ○#1

[0070] ■功能：访问控制

[0071] ■服务：Apache

[0072] ■PB：<角色，web>

[0073] ■UB：任何人

[0074] ○#2

[0075] ■功能：访问控制

[0076] ■服务：PostgreSQL

[0077] ■PB：<角色，数据库>

[0078] ■UB：<角色，web>

[0079] 规则列表#2

[0080] ●范围：名称

[0081] ●规则

[0082] ○#1

[0083] ■功能：安全连接

[0084] ■服务：所有

[0085] ■PB：<角色，数据库>

[0086] ■UB：任何被管理服务器

[0087] 注意，以上规则为了清楚而将服务简称为“Apache”和“PostgreSQL”。请记住服务是一个过程并且由端口/协议对和(可选的)附加限制(诸如过程信息和/或软件包信息(以上关于管理域状态320内的被管理服务器130的描述所描述的))来指定。

[0088] 规则列表#1和#1允许任何设备(例如用户设备)连接到web服务器并且使用Apache服务。具体地，连接的许可由功能部分中的“访问控制”来指定。“任何设备”由UB部分中的“任何人”来指定。“web服务器”由PB部分中的“<角色，web>”(仅包括一个标签的标签集合)来指定。Apache服务由服务部分中的“Apache”来指定。

[0089] 规则列表#1和#2允许web服务器连接到数据库服务器上的PostgreSQL。具体地，连接的许可由功能部分中的“访问控制”来指定。“web服务器”由UB部分中的“<角色，web>”来指定。“PostgreSQL”由服务部分中的“PostgreSQL”来指定。“数据库服务器”由PB部分中的“<角色，数据库>”(仅包括一个标签的标签集合)来指定。

[0090] 规则列表#1还防止环境间连接。例如，如果web服务器和数据库服务器二者在相同的环境中(例如都在生产环境中或者都在分段环境中)，则允许web服务器连接到数据库服务器上的PostgreSQL。生产环境中的两个服务器由范围部分中的“<环境，生产>”(仅包括一个标签的标签集合)来指定，而分段环境中的两个服务器由范围部分中的“<环境，分段>”(仅包括一个标签的标签集合)来指定。因此，如果服务器在不同的环境中(例如如果web服务器在分段环境中，而数据库服务器在生产环境中)，则不允许web服务器连接到数据库服务器上的PostgreSQL。

[0091] 规则列表#2指出无论何时任何被管理服务器连接到数据库服务器，该连接必须通过加密通道来执行。具体地，“数据库服务器”由PB部分中的“<角色，数据库>”来指定。“加密通道”由功能部分中的“安全连接”来指定。“任何被管理服务器”由UB部分中的“任何被管理服务器”来指定。“无论何时”由服务部分中的“全部”来指定。

[0092] 撇开以上示例，考虑下面的两个被管理服务器130：服务器1是作为生产的一部分(是app1的一部分)并且被加利福尼亚的工程所拥有的web服务器。其应当被标记为：

[0093] <角色，web>

[0094] <环境，生产>

[0095] <应用，app1>

[0096] <LB，工程>

[0097] <位置，美国>

[0098] 服务器2是作为生产的一部分(也是app1的一部分)但是由德国的工程所拥有的数据库服务器。其应当被标记为：

[0099] <角色，数据库服务器>

[0100] <环境，生产>

[0101] <应用，app1>

[0102] <LB，工程>

[0103] <位置，欧洲>

[0104] 假定访问控制规则允许对作为app1的一部分的所有被管理服务器130的所有访问。该规则将允许服务器1和服务器2彼此通信并且将不允许作为app2的一部分的德国的被管理服务器130与服务器1或者服务器2通信。现在假定安全连接规则指定必须对欧洲和美

国之间的所有网络通信进行加密。规则功能独立地被应用。换言之，安全连接规则是独立于访问控制规则而被应用的单独的策略。因此，从服务器1到服务器2的网络流量将被允许(给定访问控制规则)并且被加密(给定安全连接规则)。

[0105] 返回图3，处理服务器310生成针对被管理服务器130的管理指令并且向服务器发送所生成的管理指令。处理服务器310还处理从被管理服务器130接收的本地状态信息。处理服务器130包括各种模块，诸如策略引擎模块340、相关规则模块350、功能级指令生成模块360、参与者列举模块370、相关参与者模块380和管理域状态更新模块385。在一个实施例中，处理服务器310包括与储存库300通信并且处理数据(例如通过执行策略引擎模块340、相关规则模块350、功能级指令生成模块360、参与者列举模块370、相关参与者模块380和管理域状态更新模块385)的计算机(或者计算机的集合)。

[0106] 相关规则模块350将管理域范围管理策略330和特定被管理服务器130的指示(例如该服务器的UID)作为输入，生成与该服务器相关的规则的集合，并且输出规则的集合。这是一个相关规则模块350通过其来检查管理策略330并且仅提取针对给定被管理服务器130的相关规则的过滤过程。相关规则模块350通过以下方式来执行过滤：迭代通过管理策略330中的所有规则列表、分析每个规则列表的范围以确定该范围是否适用于该被管理服务器130以及(如果这些范围适用于该被管理服务器130，则)分析每个规则列表中的规则以确定这些规则是否适用于该被管理服务器130。如果a)规则的PB部分和/或规则的UB部分指定被管理服务器并且b)规则的条件部分(如果存在)针对该被管理服务器(特别是针对该被管理服务器的配置的特性和网络曝光信息的值)评估为“真”，则规则适用于被管理服务器130。最终结果(本文中被称为“管理策略全貌”)是规则的两个集合的集合：其中该被管理服务器130提供服务的规则以及其中该被管理服务器130消耗服务的规则。

[0107] 功能级指令生成模块360将规则的集合(例如，由相关规则模块350生成的管理策略全貌)作为输入，生成功能级指令，并且输出功能级指令。稍后向被管理服务器130发送功能级指令作为管理指令的一部分。功能级指令类似于规则，因为每个都包括规则功能部分、服务部分、PB部分和UB部分。然而，规则可以在其PB部分和/或UB部分内包括多个项目(包括标签集合、被管理服务器UID和/或UDG UID)，而功能级指令在其PB部分中仅包括一个项目并且在其UB部分中仅包括一个项目。另外，规则可以在其PB部分和/或UB部分中指定被管理服务器(包括其多个网络接口)，而功能级指令在其PB部分和UB部分内仅包括一个网络接口。

[0108] 功能级指令生成模块360分析规则并且基于该规则生成一个或多个功能级指令。如果规则的PB部分包括多个项目，规则的UB部分包括多个项目，或者由(PB部分或者UB部分中的)规则涉及的被管理服务器具有多个网络接口，则功能级指令生成模块360生成多个功能级指令(例如用于PB项目、UB项目和特定网络接口的每个可能的组合的一个功能级指令)。

[0109] 考虑在其PB部分中包括两个项目(A和B)并且在其UB部分中包括两个项目(C和D)的规则。功能级指令生成模块360将生成具有以下PB和UB部分的4个功能级指令：1)PB＝A，UB＝C；2)PB＝A，UB＝D；3)PB＝B，UB＝C；4)PB＝B，UB＝D。现在考虑在其PB部分或者UB部分中覆盖被管理服务器(例如通过指定UID或者标签集合)并且该被管理服务器具有多个网络接口的规则。功能级指令生成模块360将生成多个功能级指令(例如针对被管理服务器的每

个网络接口的一个功能级指令)。

[0110] 功能级指令生成模块360分析规则、这些规则内的功能、以及由这些规则涉及的功能简档。如果规则列表包括多个范围,则功能级指令生成模块360以迭代方式将这些范围多次应用于规则列表(从而生成针对每个范围的功能级指令的完整集合)。回忆起,规则功能可以与多个功能简档相关联,并且功能简档可以包括优先级。功能级指令生成模块360基于各个功能简档的优先级来对规则排序,使得具有最高优先级的功能简档被使用。功能级指令生成模块360将排序后的规则转换成用于被管理服务器130的功能级指令以执行。考虑到与规则相关联的服务的网络曝光细节,功能级指令引用适当的被管理服务器130和/或未被管理设备140(例如在输入规则中被引用的被管理服务器130和/或未被管理设备140)。

[0111] 应当注意功能级指令生成模块360可以针对特定被管理服务器130生成被证明与该服务器不相关的功能级指令。例如,该被管理服务器被规则的由谁提供(PB)部分覆盖,因此功能级指令生成模块360生成对应的功能级指令。然而,规则还包括指定被管理服务器的本地状态的部分(例如,描述所提供的服务的服务部分)。由于全局管理器120不知道被管理服务器的本地状态(例如,被管理服务器是否实际上提供该服务),所以向被管理服务器发送所生成的功能级指令。如下面参考策略编译模块410所解释的,被管理服务器检查其本地状态(例如,其是否提供该服务)并且相应地处理功能级指令。

[0112] 参与者列举模块370将被管理服务器130的描述和未被管理设备组(UDG)的描述的集合(例如管理域的计算机网络架构320的状态)作为输入,生成服务器和UDG的那些描述的列举形式的表示(被称为"参与者集合"),并且输出参与者集合。例如,参与者列举模块370列举管理域状态320内的被管理服务器130和UDG以及可能的标签集合并且向每个分配唯一标识符(UID)。然后,可以结合规则和范围的UB部分和PB部分来使用这些参与者集合,其使用被管理服务器UID、UDG UID和/或标签集合来指定参与者。

[0113] 考虑包括N个维度$D_i$($i=1,\cdots\cdots,N$)的集合的逻辑管理模型并且每个维度$D_i$包括可能的值$V_j$($j=1,\cdots\cdots,M_i$)的集合$S_i$(其中通配符"*"是可能的值之一)。在一个实施例中,参与者列举模块370基于逻辑管理模型来列举可能的所有标签集合,其等于通过$S_1\times S_2\times\cdots\times S_N$给定的笛卡尔积。该集合的大小为$M_1\times M_2\times\cdots\times M_N$。列举过程将被管理服务器130的多维标签空间重叠(collapse)成简单的列举形式。

[0114] 在另一实施例中,参与者列举模块370基于管理域状态320(例如基于管理域150内的被管理服务器的描述)仅列举可能的那些标签集合。例如,考虑包括2个维度(X和Y)的逻辑管理模型并且每个维度包括3个可能的值(A、B和*)。具有标签集合"<X=A>,<Y=B>"的被管理服务器可以是4个可能的标签集合的成员:1)"<X=A>,<Y=B>",2)"<X=A>,<Y=*>",3)"<X=*>,<Y=B>",4)"<X=*>,<Y=*>"。应当注意被管理服务器的标签集合存在于2维空间(X和Y)中,而可能的标签集合2、3和4是被管理服务器的标签集合到子维度空间中的投影(标签集合2是1维空间(X),标签集合3是1维空间(Y),标签集合4是0维空间)。因此,参与者列举模块370列举那些4个可能的标签集合。具有标签集合"<X=A>,<Y=B>"的被管理服务器可以不是标签集合"<X=A>,<Y=A>"的成员,因此参与者列举模块370不列举该标签集合。

[0115] 参与者集合包括UID以及零个或更多个参与者集合记录。参与者集合记录包括UID(被管理服务器UID或者UDG UID)、参与者的操作系统的标识符、以及被给予特定BRN的参与

者(被管理服务器130或者未被管理设备140)的IP地址。例如,参与者集合可以包括其IP地址对应于由标签集合<角色,数据库>和<环境,生产>覆盖的所有被管理服务器130的参与者集合记录。作为另一示例,参与者集合可以包括其IP地址对应于总部UDG中的所有未被管理设备140的参与者集合记录。单个参与者(例如被管理服务器130或者未被管理设备140)可以出现在多个参与者集合中。

[0116] 参与者集合计算中的另一因素是具有多个网络接口的参与者以及包括网络拓扑结构(诸如网络地址转换(NAT))。因此,标签集合<角色,数据库>和<环境,生产>可以存在2个参与者集合:一个参与者集合具有那些被管理服务器130(即与第一BRN相关联)的面向因特网的IP地址,并且不同的参与者集合用于具有这些被管理服务器(即与第二BRN相关联)的面向专用的网络的IP地址的那些相同的被管理服务器。

[0117] 在一个实施例中,参与者列举模块370还可以基于管理域的状态320来更新参与者集合。例如,参与者列举模块370将参与者集合(由参与者列举模块先前输出的)以及(管理域状态320内的)被管理服务器的描述的变化作为输入,生成更新的参与者集合(其与已变化服务器描述相同),并且输出已更新参与者集合。参与者列举模块370根据被管理服务器的描述的变化类型以不同的方式来生成更新的参与者集合。

[0118] 离线/在线变化—如果描述变化指示服务器从在线转到离线,则参与者列举模块370通过从服务器是其成员的所有输入参与者集合中去除服务器的参与者集合记录来生成更新的参与者集合。如果描述变化指示服务器从离线转到在线,则参与者列举模块370通过向任何相关的输入参与者集合添加服务器的参与者集合记录来生成已更新参与者集合。(根据需要,参与者列举模块370创建新的参与者集合并且向该新的参与者集合添加服务器的参与者集合记录)。

[0119] 标签集合变化—如果描述变化指示服务器的标签集合改变,则参与者列举模块370与转到离线的第一服务器(具有旧的标签集合)和转到在线的第二服务器(具有新的标签集合)类似地处理该变化。

[0120] 网络曝光信息变化—如果描述变化指示服务器去除网络接口,则参与者列举模块370通过从服务器是其成员的所有输入参与者集合(与网络接口的BRN相关联)中去除服务器的参与者集合记录来生成更新的参与者集合。如果描述变化指示服务器添加网络接口,则参与者列举模块370通过向任何相关的输入参与者集合(与该网络接口的BRN相关联)添加服务器的参与者集合记录来生成已更新参与者集合。(根据需要,参与者列举模块370创建新的参与者集合(与该网络接口的BRN相关联)并且向该新的参与者集合添加服务器的参与者集合记录)。如果描述变化指示服务器改变网络接口的BRN,则参与者列举模块370与被去除的第一服务器(具有旧的标签集合)和被添加的第二服务器(具有新的标签集合)类似地处理该变化。如果描述变化指示服务器改变网络接口的IP地址(而非BRN),则参与者列举模块370通过修改服务器是其成员的所有输入参与者集合(与网络接口的BRN相关联)中的服务器的参与者集合记录来生成更新的参与者集合。

[0121] 相关参与者模块380将一个或多个参与者集合(例如管理域状态320内的列举形式的被管理服务器130和UDG)以及规则的集合(例如管理策略全貌)作为输入,确定哪些参与者集合与那些规则相关,并且仅输出这些参与者集合。这是一个相关参与者模块380通过其来检查参与者集合并且仅提取用于给定的规则集合的相关参与者集合的过滤过程。相关参

与者模块380通过以下方式来执行过滤：迭代通过所有输入的参与者集合、分析输入规则的PB部分和UB部分以确定特定的参与者集合是否由规则PB部分或UB部分中的任何部分引用。最终结果(本文中被称为“参与者全貌”)是参与者集合的集合。稍后向被管理服务器130发送参与者全貌作为管理指令的一部分。

[0122] 在一个实施例中，相关参与者模块380使用规则的输入集合来生成“参与者集合过滤器”。参与者集合过滤器从输入参与者集合中仅选择与输入规则相关的参与者集合。换言之，相关参与者模块380使用参与者集合过滤器来将输入参与者集合过滤成相关参与者集合。

[0123] 策略引擎模块340生成用于被管理服务器130的管理指令并且向服务器发送所生成的管理指令。策略引擎模块340基于a)管理域的计算机网络架构的状态320以及b)管理域范围管理策略330，来生成管理指令(包括相干规则模块350、功能级指令生成模块360、参与者列举模块370、和相关参与者模块380)。

[0124] 例如，策略引擎模块340执行相关规则模块350，以提供管理域范围管理策略330和特定被管理服务器130的UID作为输入。相关规则模块350输出与该服务器相关的规则的集合(“管理策略全貌”)。策略引擎模块340执行参与者列举模块370，以提供管理域状态320作为输入。参与者列举模块370输出管理域状态320内的被管理服务器130和未被管理设备组(UDG)的描述的列举形式的表示(“参与者集合”)。策略引擎模块340执行功能级指令生成模块360，以提供管理策略全貌(由相关规则模块350输出)作为输入。功能级指令生成模块360输出功能级指令。策略引擎模块340执行相关参与者模块380，以提供参与者集合(由列举模块370输出)以及管理策略全貌(由相关规则模块350输出)作为输入。相关参与者模块380仅输出与那些规则相关的那些参与者集合(“相关远方集合”)。策略引擎模块340向特定被管理服务器130发送功能级指令(由功能级指令生成模块360输出)以及相关参与者集合(由相关参与者模块380输出)。

[0125] 在一个实施例中，策略引擎模块340对以上过程期间生成的信息进行高速缓存。例如，策略引擎模块340对与特定被管理服务器130相关联的管理策略全貌、功能级指令、参与者集合过滤器和/或相关参与者集合进行高速缓存。作为另一示例，策略引擎模块340对参与者集合(其并不特定于特定被管理服务器130)进行高速缓存。

[0126] 由于管理域的参与者集合基于管理域状态320，所以管理域状态320的变化可以要求管理域的参与者集合的变化。类似地，由于被管理服务器的管理指令基于管理域状态320和管理域范围管理策略330，所以管理域状态320的变化和/或管理域范围管理策略330的变化可以要求被管理服务器的管理指令的变化。在一个实施例中，策略引擎模块340可以更新管理域的参与者集合和/或更新被管理服务器的管理指令并且然后向被管理服务器130分发这些变化(如果需要)。以上提及的高速缓存的信息帮助策略引擎模块340更高效地更新管理域的参与者集合和/或被管理服务器的管理指令并且分发变化。

[0127] 在一个实施例中，策略引擎模块340如下(基于管理域状态320的变化)更新管理域的参与者集合并且向被管理服务器130分发变化：策略引擎模块340执行参与者列举模块370，以提供高速缓存的参与者集合(由参与者列举模块先前输出)以及管理域状态320的改变部分(即改变的服务器描述)作为输入。参与者列举模块370输出更新的参与者集合。在一个实施例中，策略引擎模块340然后向管理域150内的所有被管理服务器130发送所有更新

的参与者集合。然而，因为并非所有被管理服务器被所有参与者集合的变化所影响，所以该实施例并不高效。

[0128] 在另一实施例中，仅向所选择的服务器发送所选择的参与者集合。例如，仅向特定被管理服务器发送以下参与者集合：a)先前向该服务器被发送并且b)已经改变。高速缓存的相关参与者集合指示先前向该服务器发送了哪些参与者集合(参见以上(a))。策略引擎模块340将高速缓存的参与者集合与更新的参与者集合相比较以确定哪些参与者集合已经变化(参见以上(b))。策略引擎模块340然后计算(a)和(b)的交集。向特定被管理服务器发送该交集中的参与者集合。在一个实施例中，对于甚至更高的效率，以“diff”格式来发送参与者集合。例如，diff格式指定参与者集合标识符、参与者标识符(例如被管理服务器UID或者UDG UID)、以及该参与者是否应当被添加、被去除或者被修改的指示。

[0129] 在又一实施例中，两个表格被维护并且用于提高效率。第一表格使得被管理服务器130与被管理服务器是其成员的参与者集合相关联。第二表格使得被管理服务器130与和该被管理服务器相关的参与者集合(例如由相关参与者模块380确定)相关联。在这些表格中，被管理服务器130例如由该被管理服务器的UID来表示，参与者集合例如由该参与者集合的UID来表示。策略引擎模块340使用管理域状态320的改变的部分(即改变的服务器描述)来确定哪个被管理服务器的描述变化。策略引擎模块340使用第一表格来确定该被管理服务器是哪个参与者集合的成员。这些参与者集合可以随着改变的服务器描述而变化。因此，策略引擎模块340使用第二表格来确定这些参与者集合与哪些被管理服务器相关。策略引擎模块340仅针对这些被管理服务器以上描述的交集计算。

[0130] 在一个实施例中，策略引擎模块340如下(基于管理域状态320的变化)更新被管理服务器的管理指令并且向被管理服务器发送更新的管理指令：策略引擎模块340执行相关规则模块350，以提供管理域范围管理策略330以及被管理服务器130的UID作为输入。相关规则模块350输出与该服务器相关的规则的集合(“管理策略全貌”)。策略引擎模块340将刚输出的管理策略全貌与高速缓存的管理策略全貌相比较以确定它们是否不同。如果刚输出的管理策略全貌与高速缓存的管理策略全貌相同，则策略引擎模块340不采取进一步的行动。在该情况下，先前生成的被管理服务器的管理指令(具体地是功能级指令和相关的参与者集合)与管理域状态320的变化一致并且不需要重新生成并且向被管理服务器重新发送。

[0131] 如果刚输出的管理策略全貌与高速缓存的管理策略全貌不同，则策略引擎模块340确定应当向高速缓存的全貌添加哪些规则以及应当从高速缓存的全貌去除哪些规则。策略引擎模块340执行功能级指令生成模块360，以提供要添加的规则和要去除的规则作为输入。功能级指令生成模块360输出要添加的功能级指令和要去除的功能级指令(与高速缓存的功能级指令相关，其先前向被管理服务器被发送)。策略引擎模块340指示被管理服务器适当地添加或者去除各种功能级指令。在一个实施例中，为了更高的效率，以“diff”格式来发送功能级指令。例如，diff格式指定功能级指令标识符以及是否应当向先前发送的功能级指令添加该功能级指令的指示或者从先前发送的功能级指令去除该功能级指令的指示。

[0132] 策略引擎模块340还执行参与者列举模块370，以提供高速缓存的参与者集合以及管理域状态320的改变的部分(即改变的服务器描述)作为输入。参与者列举模块370输出更新的参与者集合。策略引擎模块340执行相关参与者模块380，以提供更新的参与者集合以

及刚输出的管理策略全貌作为输入。相关参与者模块380仅输出与这些规则相关的这些更新的参与者集合(“更新的相关参与者集合”)。

[0133] 策略引擎模块340将更新的相关参与者集合与高速缓存的相关参与者集合相比较以确定它们是否不同。如果更新的相关参与者集合与高速缓存的相关参与者集合相同,则策略引擎模块340不向被管理服务器发送任何参与者集合。在这种情况下,先前生成的相关参与者集合与管理域状态320的变化一致并且不需要向被管理服务器重新发送。如果更新的相关参与者集合与高速缓存的相关参与者集合不同,则策略引擎模块340确定应当相对于高速缓存的相关参与者集合添加、去除或修改哪些参与者集合。策略引擎模块340指示被管理服务器适当地添加、去除或修改各个参与者集合。在一个实施例中,为了更高效,以“diff”格式来发送参与者集合。例如,diff格式指定参与者集合标识符以及是否应当相对于先前发送的参与者集合添加、去除或修改该参与者集合的指示。

[0134] 回想起策略引擎模块340可以(基于管理域范围管理策略330的变化)更新被管理服务器的管理指令并且向被管理服务器发送以更新管理指令。管理策略330的变化例如是规则或者规则集合的添加、去除或修改。在一个实施例中,管理策略330的变化通过经由GUI或者API与全局管理器120的交互来生成。在另一实施例中,管理策略330的变化通过全局管理器120内的自动过程(例如响应于由全局管理器检测到安全威胁)来生成。策略引擎模块340更新被管理服务器的管理指令并且以类似的方式向被管理服务器发送更新的管理指令,而不管是否存在管理策略330的变化或者管理域状态320的变化。然而,存在若干差异。

[0135] 在管理策略330变化的情况下,策略引擎模块340不必针对所有的被管理服务器130更新管理指令。相反,策略引擎模块340将先前的管理策略330与新的管理策略330相比较以确定应当相对于先前的管理策略330添加、去除或修改哪些规则。策略引擎模块340确定哪些被管理服务器130受到改变的规则的影响(例如哪些被管理服务器由a)规则的和/或范围的PB和/或UB部分以及b)规则的条件部分(如果存在)覆盖)。策略引擎模块340执行相关规则模块350,以提供改变的规则(而非整个新的管理策略330)以及被管理服务器130的UID(仅针对受到改变的规则的影响的那些服务器)作为输入。

[0136] 管理域状态更新(ADSU)模块385接收管理域状态320的变化并且处理那些变化。管理域状态320的变化例如是被管理服务器130的描述的添加、去除或修改(包括被管理服务器的标签集合或配置特性的修改)或者未被管理设备或未被管理设备组的描述的添加、去除或修改。在一个实施例中,管理域状态320的变化源自从特定被管理服务器130接收的本地状态信息。在另一实施例中,管理域状态320的变化通过经由GUI或者API与全局管理器120的交互来生成。在又一实施例中,管理域状态320的变化通过全局管理器120内的自动过程(例如响应于由全局管理器检测到安全威胁)来生成。

[0137] 例如,ADSU模块385接收与特定被管理服务器130相关的变化。ADSU模块385在管理域状态320中存储新的信息作为该特定被管理服务器130的描述的一部分。ADSU模块385然后(可选地)分析该被管理服务器的描述以确定与服务器相关的附加信息并且在描述中存储该信息。ADSU模块385然后基于被管理服务器的描述的变化来确定是否更新管理域的参与者集合和/或被管理服务器的管理指令。如果ADSU模块385确定更新管理域的参与者集合,则ADSU模块385指示策略引擎模块340更新管理域的参与者集合。在一个实施例中,ADSU模块385在指示策略引擎模块340更新管理域的参与者集合之前等待某个事件的发生。如果

ADSU模块385确定更新被管理服务器的管理指令，则ADSU模块385指示策略引擎模块340更新被管理服务器的管理指令。在一个实施例中，ADSU模块385在指示策略引擎模块340更新被管理服务器的管理指令之前等待某个事件的发生。上述事件可以例如是用户命令的接收或者指定的维护窗口的出现。

[0138] ADSU模块385是否确定更新管理域的参与者集合和/或被管理服务器的管理指令取决于被管理服务器的描述的变化的类型。在一个实施例中，ADSU模块385如表2所示做出该确定：

[0139]

| 变化的类型 | 是否更新 |
| --- | --- |
| 在线到离线 | 管理域的参与者集合：是<br>被管理服务器的管理指令：否 |

[0140]

| | |
| --- | --- |
| 离线到在线 | 管理域的参与者集合：是<br>被管理服务器的管理指令：是 |
| 标签列表 | 管理域的参与者集合：是<br>被管理服务器的管理指令：是 |
| 配置的特性 | 管理域的参与者集合：否<br>被管理服务器的管理指令：是 |
| 网络曝光信息 | 管理域的参与者集合：是<br>被管理服务器的管理指令：是（除非 IP 地址是唯一的变化） |
| 服务信息 | 管理域的参与者集合：否<br>被管理服务器的管理指令：是（仅在指定的情况下） |

[0141] 表2-是否基于服务器描述变化的类型来更新管理域的参与者集合和/或被管理服务器的管理指令

[0142] 在一个实施例中，ADSU模块385通过执行标签/配置的特性引擎并且提供服务器的描述作为输入来确定与服务器相关的附加信息。标签/CC引擎基于服务器的描述和标签/CC分配规则来计算针对服务器的标签/CC值。

[0143] 在另一实施例中，ADSU模块385确定服务器是否在网络地址转换器(NAT)的后面(并且如果其在NAT后面，则确定NAT是什么类型—1:1还是1:N)。例如，ADSU模块385通过将(a)根据全局管理器与服务器之间的TCP连接的服务器的IP地址与(b)根据从服务器接收的本地状态信息的服务器的IP地址相比较来确定全局管理器120与被管理服务器130之间是否存在NAT。如果(a)与(b)不同，则全局管理器120与被管理服务器130之间存在NAT。如果存

在NAT，则ADSU模块385通过执行数据中心检测来确定NAT的类型(1:1还是1:N)。例如，ADSU模块385通过数据中心的公共IP地址来标识服务器的数据中心。(替选地，被管理服务器通过查询在服务器外部但是在数据中心内部的信息来执行数据中心检测。服务器然后向全局管理器发送该信息作为本地状态的一部分。)配置信息指示哪些数据中心使用哪些类型的NAT。如果没有NAT信息与特定的数据中心相关联，则ADSU模块385假定NAT类型为1:N。

[0144] 图4是图示根据一个实施例的被管理服务器130的策略实现模块136的详细视图的高层框图。策略实现模块136包括本地状态储存库400、策略编译模块410和本地状态更新模块420。本地状态储存库400存储与被管理服务器130的本地状态相关的信息。在一个实施例中，本地状态储存库400存储关于被管理服务器的操作系统(OS)、网络曝光、和服务的信息。OS信息包括例如哪个OS正在运行的指示。以上关于管理域状态320内的被管理服务器130的描述已经描述了网络曝光信息和服务信息。

[0145] 策略编译模块410将输入管理指令以及被管理服务器130的状态作为输入并且生成管理模块配置134。例如，管理指令从全局管理器120被接收并且包括功能级指令(由功能级指令生成模块360生成)和相关参与者集合(由相关参与者模块380输出)。从本地状态储存库400检索被管理服务器130的状态。在一个实施例中，通过a)上电或转到在线的被管理服务器、b)接收功能级指令的被管理服务器、和/或c)改变的本地状态储存库400的内容，来触发策略编译模块410的执行。

[0146] 策略编译模块410将功能级指令和相关的参与者集合映射成管理模块配置134。例如，策略编译模块410将访问控制功能级指令(其包含端口和参与者集合引用)映射成Linux操作系统中的iptables条目和ipset条目或者Windows操作系统中的Windows过滤平台(WFP)规则。

[0147] 被管理服务器130处的管理策略的应用可以受到该服务器的本地状态的影响。在一个实施例中，策略编译模块410评估与所接收的功能级指令相关联的条件并且基于该评估的结果生成管理模块配置134。例如，策略编译模块410评估涉及被管理服务器的同级(即关系中的另一参与者)的操作系统的条件并且基于该评估的结果选择功能简档属性，其中所选择的功能简档属性在管理模块配置134中被表达。

[0148] 作为另一示例，回想起被管理服务器130可以接收被证明与该服务器无关的功能级指令。例如，规则包括指定被管理服务器的本地状态的一部分(例如描述所提供的服务的服务部分)。由于全局管理器120不知道被管理服务器的本地状态(例如被管理服务器是否实际上提供该服务)，因此向被管理服务器发送所生成的功能级指令。策略编译模块410检查被管理服务器的本地状态(例如确定被管理服务器是否提供该服务)。该确定相当于评估涉及被管理服务器的本地状态的条件。策略编译模块410相应地处理功能级指令。如果策略编译模块410确定条件评估为“真”(例如被管理服务器提供该服务)，则策略编译模块410将该功能级指令合并到管理模块配置134中。具体地，策略编译模块410仅在评估相关联的条件(其涉及该服务器的本地状态)之后将功能级指令合并到管理模块配置134中。如果条件的评估为假，则策略编译模块410不在管理模块配置134中表达功能级指令。特定条件(例如它们的属性和特定值)是可扩展的。在一个实施例中，条件与“服务”的定义相关并且包括过程信息和/或软件包信息(以上关于管理域状态320内的被管理服务器130的描述所描述的)。

[0149] 例如，考虑仅允许对端口80上的入站Apache服务的访问的功能级指令(即其中被管理服务器130是“提供者”或者端点)。被管理服务器130在管理模块配置134中表达该功能级指令以允许仅在评估相关联的条件之后的端口80上的访问，其涉及正在端口80上监听的应用(执行在该服务器上)实际上是否是Apache而非某个其他应用(欺骗或其他)。被管理服务器130仅在确定关联的条件评估为“真”之后在管理模块配置134中表达该功能级指令。如果关联的条件评估为“假”，则被管理服务器130不在管理模块配置134中表达该功能级指令。因此，阻止了网络流量。

[0150] 在一个实施例中，被管理服务器130监视其出站连接。被管理服务器130将出站网络通信与其内部过程表格相比较以确定该表格中的哪些过程建立这些出站连接。被管理服务器130可以强迫仅使得某些过程(给定要求的集合，以上所涉及的)建立出站连接的规则。

[0151] 在一个实施例(未示出)中，策略编译模块410位于全局管理器120处，而非被管理服务器130处。在该实施例中，全局管理器120不向被管理服务器130发送管理指令。相反，被管理服务器130向全局管理器120发送器本地状态。在策略编译模块410(在全局管理器120处)生成管理模块配置134之后，从全局管理器120向被管理服务器130发送管理模块配置134。

[0152] 本地状态更新(LSU)模块420监视被管理服务器130的本地状态并且向全局管理器120发送本地状态信息。在一个实施例中，LSU模块420确定被管理服务器130的初始本地状态，在本地状态储存库400中存储适当的本地状态信息，并且向全局管理器120发送该本地状态信息。LSU模块420通过检查服务器的操作系统(OS)和/或文件系统的各个部分来确定被管理服务器130的本地状态。例如，LSU模块420从OS的内核表格(连网信息)、OS的系统表格(软件包信息)、和文件系统(文件和散列值)获取服务信息。LSU模块420从OS的内核和/或OS级数据结构获得网络曝光信息。

[0153] 在LSU模块420向全局管理器120发送初始本地状态信息之后，LSU模块监视本地状态的变化。LSU模块通过例如轮询(例如周期性地执行检查)或者监听(例如订阅事件流)来监视变化。LSU模块420将最近获得的本地状态信息与本地状态储存库400中已经存储的信息相比较。如果信息匹配，则LSU模块420不采取进一步的行动(直到本地状态信息被再次获得)。如果它们不同，则LSU模块420在本地状态储存库400中存储最近获得的信息，执行策略编译模块410以重新生成管理模块配置134(并且相应地重新配置管理模块132)，并且向全局管理器120通知变化。在一个实施例中，LSU模块420以“diff”格式向全局管理器120发送本地状态信息的变化。例如，diff格式指定本地状态信息的类型(例如操作系统)以及用于该信息类型的新的值。在另一实施例中，LSU模块420向全局管理器120发送本地状态储存库400的整个内容。

[0154] 图5是图示根据一个实施例的生成用于特定被管理服务器130的管理指令的方法500的流程图。其他实施例可以按照不同的顺序来执行步骤并且可以包括不同的和/或另外的步骤。另外，可以由除了图1所示的实体之外的其他实体来执行这些步骤中的一些或全部步骤。在一个实施例中，方法500被执行多次(例如对于管理域150中的每个被管理服务器130执行一次)。

[0155] 当方法500开始时，管理域的计算机网络架构的状态320以及管理域范围管理策略330已经被存储在全局管理器120的储存库300中。在这点上，方法500开始。

[0156] 在步骤510，访问管理域状态320和管理域范围管理策略330。例如，策略引擎模块340向储存库300发送请求并且响应于此接收管理域状态320和管理域范围管理策略330。

[0157] 在步骤520，确定一个或多个相关规则。例如，策略引擎模块340执行相关规则模块350，以提供管理域范围管理策略330以及特定被管理服务器130的UID作为输入。相关规则模块350输出与该服务器相关的规则的集合(管理策略全貌)。

[0158] 在步骤530，列举参与者。例如，策略引擎模块340执行参与者列举模块370，以提供管理域状态320作为输入。参与者列举模块370生成管理域状态320内的被管理服务器130以及未被管理设备组(UDG)的列举形式的表示(参与者集合)。

[0159] 在步骤540，生成一个或多个功能级指令。例如，策略引擎模块340执行功能级指令生成模块360，以提供管理策略全貌(在步骤520被生成)作为输入。功能级指令生成模块360生成功能级指令。

[0160] 在步骤550，确定一个或多个相关参与者。例如，策略引擎模块340执行相关参与者模块380，以提供参与者集合(在步骤530被生成)以及管理策略全貌(在步骤520被生成)作为输入。相关参与者模块380仅输出与那些规则相关的那些参与者集合(相关参与者集合)。

[0161] 在步骤560，向特定被管理服务器130发送管理指令。例如，策略引擎模块340向特定被管理服务器130发送功能级指令(在步骤540被生成)以及相关参与者集合(在步骤550被生成)。

[0162] 注意，步骤520和540涉及生成用于特定被管理服务器130的管理策略全貌(以及所得到的功能级指令)，而步骤530和550涉及生成用于该被管理服务器的参与者全貌。管理策略全貌的生成和参与者全貌的生成最低限度地取决于彼此，因为步骤520生成由步骤550使用的规则的集合。即便如此，保持管理策略计算(即步骤520和540)与参与者集合计算(即步骤530和550)独立增强了策略引擎模块340的可扩展性。由于管理策略计算和参与者集合计算通常保持独立，所以可以并行地执行它们(例如甚至对于相同的被管理服务器130)。另外，也可以并行地执行用于不同被管理服务器130的全貌计算。另外，如果参与者变化，则仅需要重新计算参与者集合。(不需要重新计算功能级指令)。如果规则变化，则仅需要重新计算功能级指令和相关的参与者集合。(不需要重新列举参与者)。

[0163] 图6是图示根据一个实施例的生成用于被管理服务器130的管理模块132的配置134的方法600的流程图。其他实施例可以按照不同的顺序来执行步骤并且可以包括不同的和/或另外的步骤。另外，可以由除了图1所示的实体之外的其他实体来执行这些步骤中的一些或全部步骤。

[0164] 当方法600开始时，与被管理服务器130的本地状态相关的信息已经被存储在被管理服务器130中的策略实现模块136的本地状态储存库400中。在这点上，方法600开始。

[0165] 在步骤610，从全局管理器120接收管理指令。例如，策略编译模块410从全局管理器120接收功能级指令和相关的参与者集合。

[0166] 在步骤620，访问本地状态。例如，策略编译模块410访问与本地状态储存库400中所存储的被管理服务器130的本地状态相关的信息。

[0167] 在步骤630，生成管理模块配置134。例如，策略编译模块410将管理指令(在步骤610被接收)和本地状态(在步骤620被访问)作为输入，并且生成管理模块配置134。

[0168] 在步骤640，配置管理模块132。例如，策略编译模块410配置管理模块132以根据管

理模块配置134(在步骤630被生成的)进行操作。

[0169] 图7是图示根据一个实施例的监视被管理服务器130的本地状态并且向全局管理器120发送本地状态信息的方法700的流程图。其他实施例可以按照不同的顺序来执行步骤并且可以包括不同的和/或另外的步骤。另外,可以由除了图1所示的实体之外的其他实体来执行这些步骤中的一些或全部步骤。

[0170] 当方法700开始时,与被管理服务器130的本地状态相关的信息已经被存储在被管理服务器130的本地状态储存库400中。在这点上,方法700开始。

[0171] 在步骤710,确定与被管理服务器130的当前本地状态相关的信息。例如,LSU模块420通过检查服务器的操作系统(OS)和/或文件系统的各个部分来确定被管理服务器130的本地状态。

[0172] 在步骤720,执行与关于当前本地状态相关的信息是否不同于本地状态储存库400中存储的信息有关的确定。例如,LSU模块420执行该确定。如果信息没有不同,则方法继续进行到步骤730并且结束。如果信息不同,则方法继续进行到步骤740。

[0173] 在步骤740,将不同的信息存储在本地状态储存库400中。例如,LSU模块420执行该步骤。

[0174] 在步骤750,(由于本地状态储存库400的内容已经改变)重新生成管理模块配置134并且相应地重新配置管理模块132。例如,LSU模块420执行策略编译模块410,策略编译模块410重新生成管理模块配置134。

[0175] 在步骤760,向全局管理器120发送不同的信息。例如,LSU模块420执行该步骤。

[0176] 图8是图示根据一个实施例的处理管理域的计算机网络架构320的状态的变化的方法800的流程图。其他实施例可以按照不同的顺序来执行步骤并且可以包括不同的和/或另外的步骤。另外,可以由除了图1所示的实体之外的其他实体来执行这些步骤中的一些或全部步骤。

[0177] 在步骤810,接收与特定被管理服务器130相关的变化。例如,管理域状态更新(ADSU)模块385从被管理服务器130接收在线/离线指示符、操作系统指示符、网络曝光信息、和/或服务信息作为本地状态信息的一部分。

[0178] 在步骤820,存储所接收的信息。例如ADSU模块385在管理域状态320中(具体地,在与信息相关的被管理服务器130的描述中)存储所接收的在线/离线指示符、网络曝光信息、和/或服务信息。

[0179] 在步骤830,分析服务器描述以确定与服务器相关的附加信息。例如,ADSU模块385使用标签/配置的特性引擎来计算服务器的标签/CC和/或确定服务器是否在网络地址转换器(NAT)之后(并且如果其在NAT之后,则确定NAT的类型—1:1还是1:N)并且在服务器描述中存储该信息。步骤830是可选的。

[0180] 在步骤840,做出是否更新管理域的参与者集合的确定。例如,ADSU模块385基于被管理服务器的描述的变化来确定是否更新管理域的参与者集合。如果做出更新管理域的参与者集合的确定,则方法继续进行到步骤850。如果做出不更新管理域的参与者集合的确定,则方法继续进行到步骤860。

[0181] 在步骤850,更新管理域的参与者集合。例如,ADSU模块385指示策略引擎模块340更新管理域的参与者集合。在一个实施例(未示出)中,ADSU模块385在指示策略引擎模块

340更新管理域的参与者集合之前等待事件的发生。

[0182] 在步骤860，做出是否更新被管理服务器的管理指令的确定。例如，ADSU模块385基于被管理服务器的描述的变化来确定是否更新被管理服务器的管理指令。如果做出更新被管理服务器的管理指令的确定，则方法继续进行到步骤870。如果做出不更新被管理服务器的管理指令的确定，则方法继续进行到步骤880。

[0183] 在步骤870，更新被管理服务器的管理指令。例如，ADSU模块385指示策略引擎模块340更新被管理服务器的管理指令。在一个实施例(未示出)中，ADSU模块385在指示策略引擎模块340更新被管理服务器的管理指令之前等待事件的发生。

[0184] 在步骤880，方法结束。

[0185] 以上描述被包括以说明某些实施例的操作而非意在限制本发明的范围。本发明的范围仅受所附的权利要求的限制。根据以上讨论，相关领域技术人员将很清楚也被本发明的精神和范围包括的多个变型。

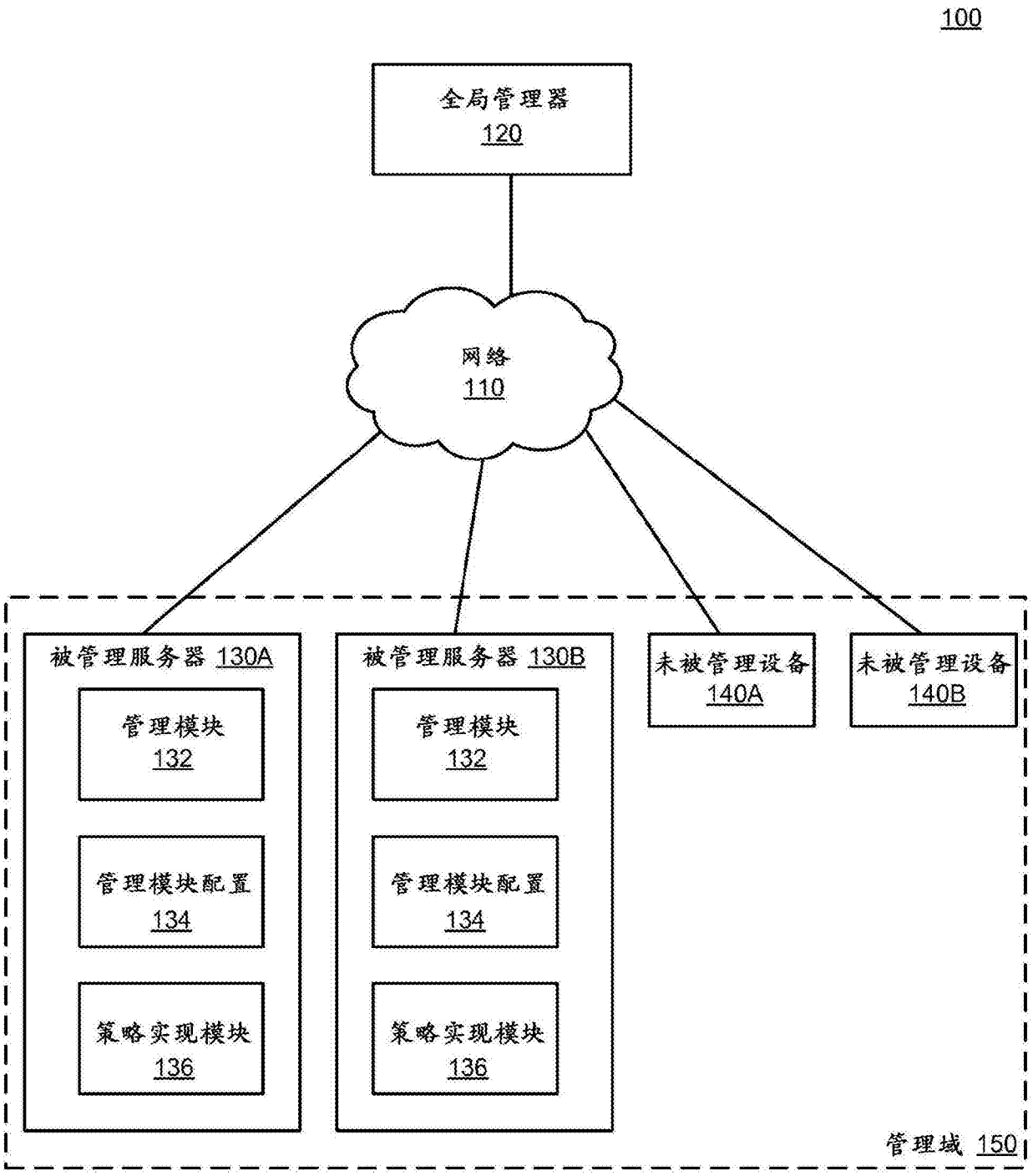

100
全局管理器
120
网络
110
被管理服务器 130A
管理模块
132
管理模块配置
134
策略实现模块
136
被管理服务器 130B
管理模块
132
管理模块配置
134
策略实现模块
136
未被管理设备
140A
未被管理设备
140B
管理域 150

图1

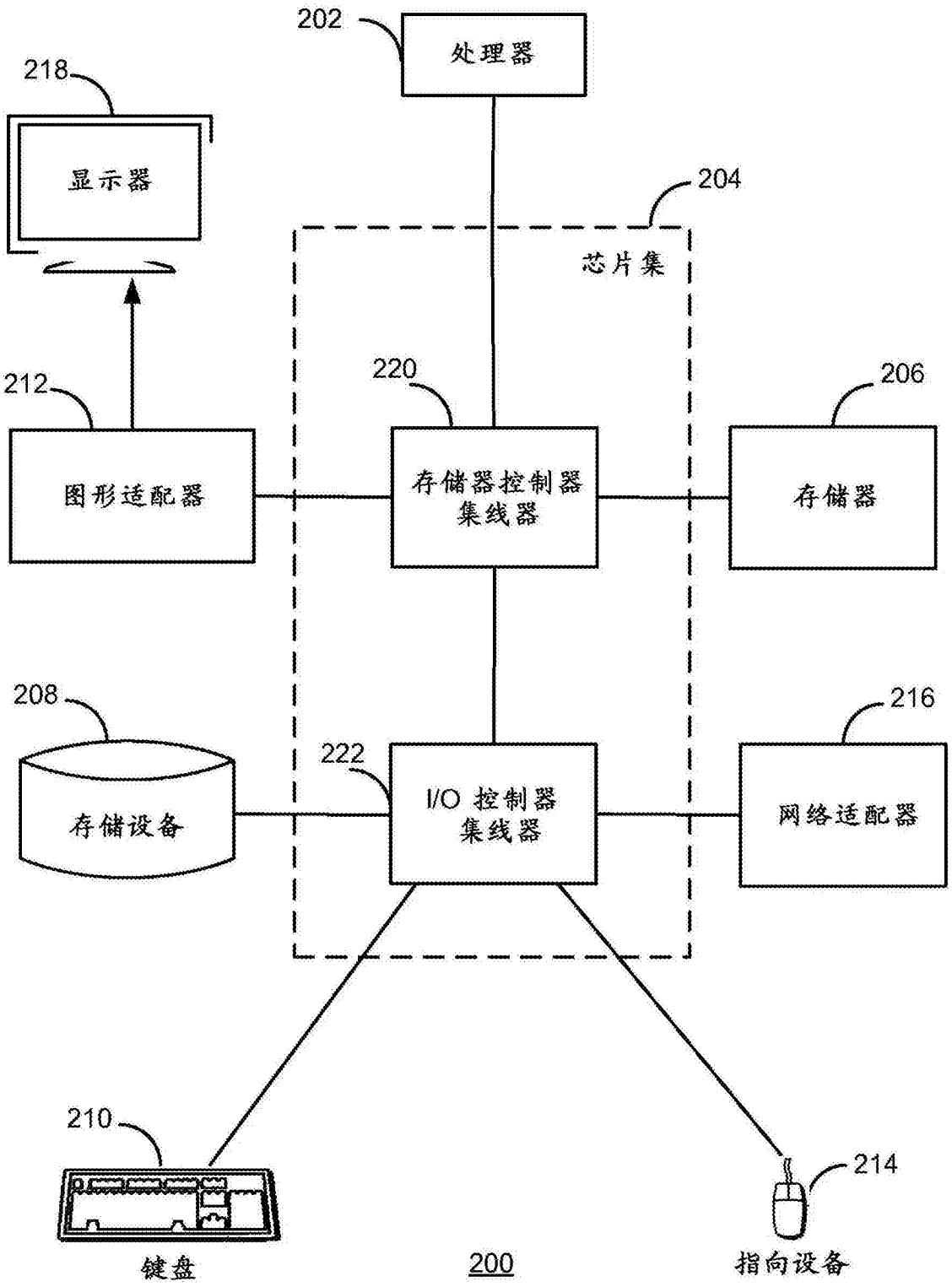

202
处理器
218
显示器
204
芯片集
212
220
206
图形适配器
存储器控制器
集线器
存储器
208
216
222
存储设备
I/O 控制器
集线器
网络适配器
210
214
键盘
200
指向设备

图2

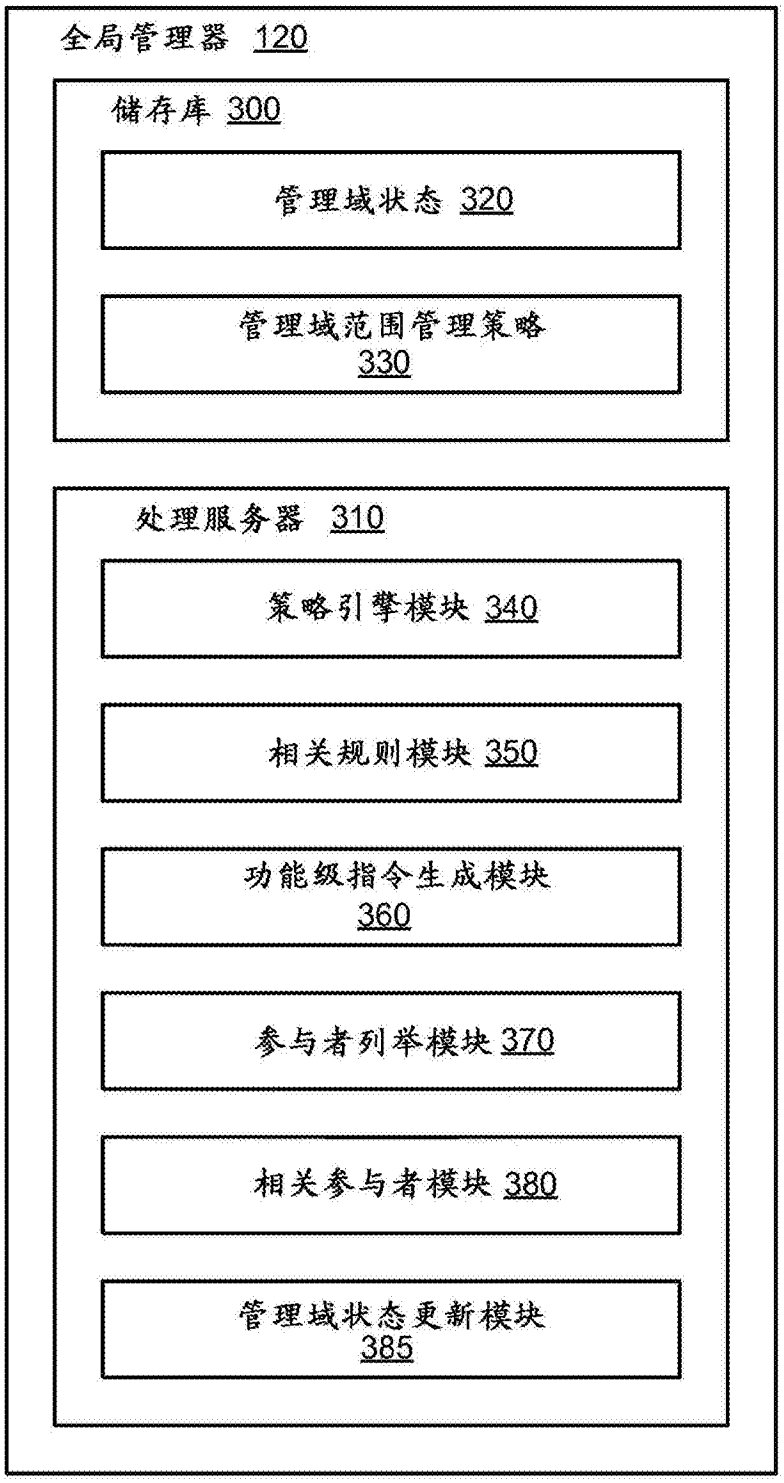

全局管理器 120
储存库 300
管理域状态 320
管理域范围管理策略 330
处理服务器 310
策略引擎模块 340
相关规则模块 350
功能级指令生成模块 360
参与者列举模块 370
相关参与者模块 380
管理域状态更新模块 385

图3

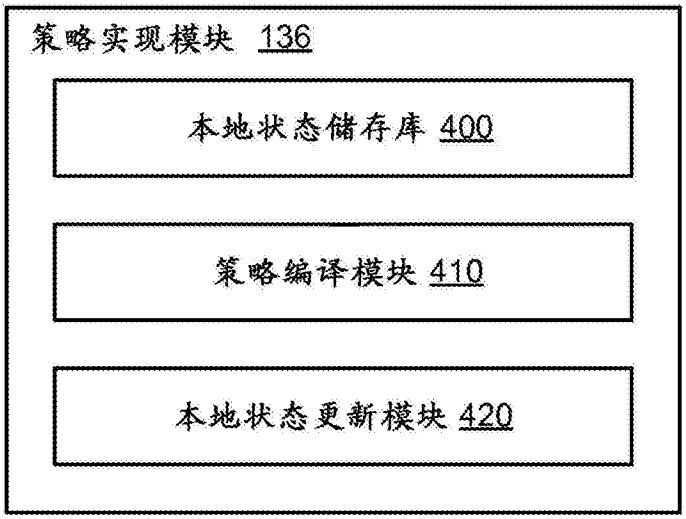



图4

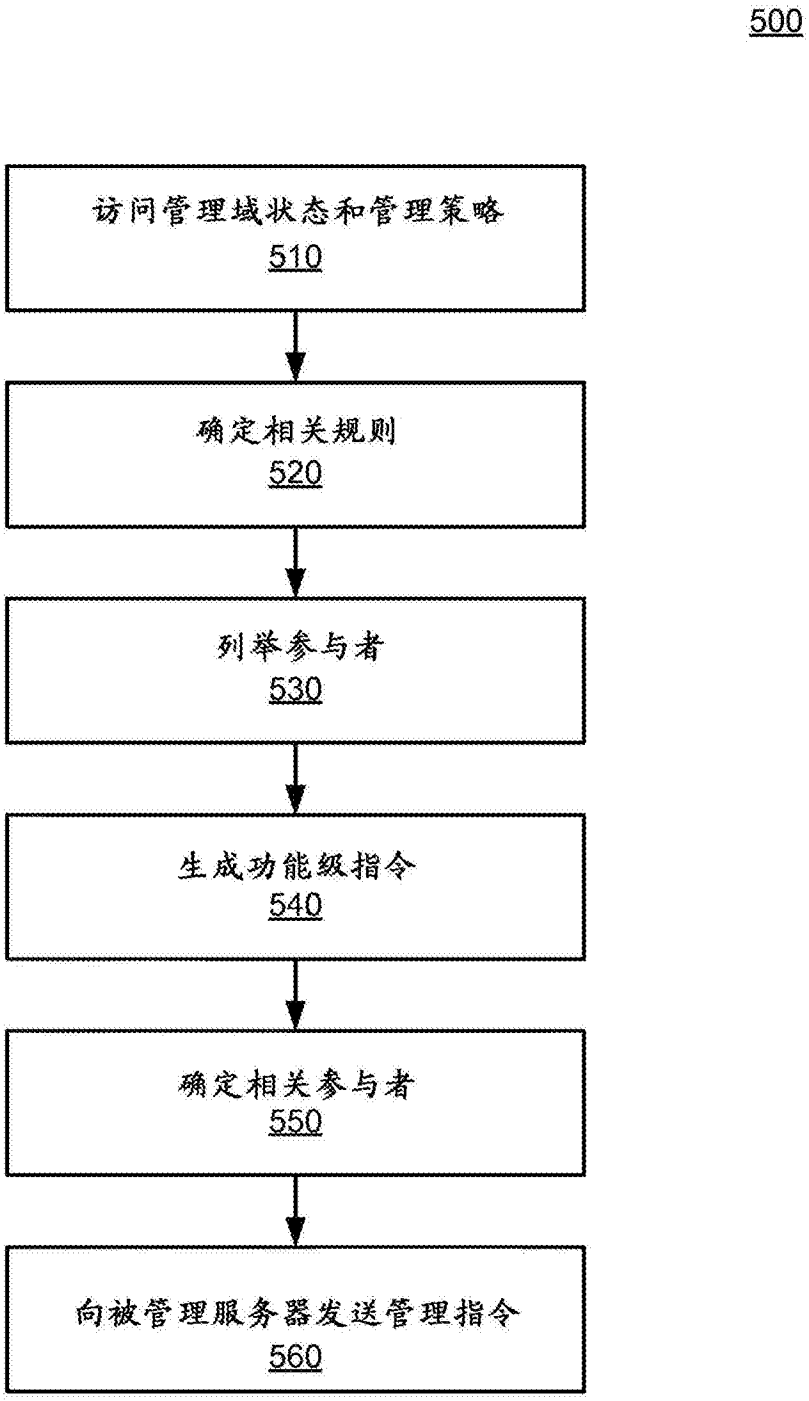

500
访问管理域状态和管理策略
510
确定相关规则
520
列举参与者
530
生成功能级指令
540
确定相关参与者
550
向被管理服务器发送管理指令
560

图5

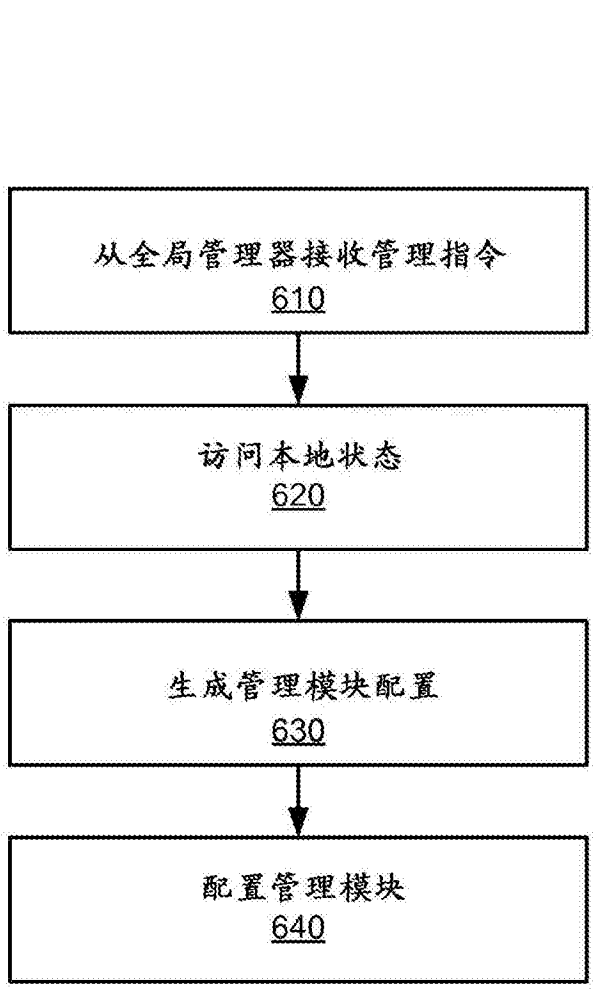



图6

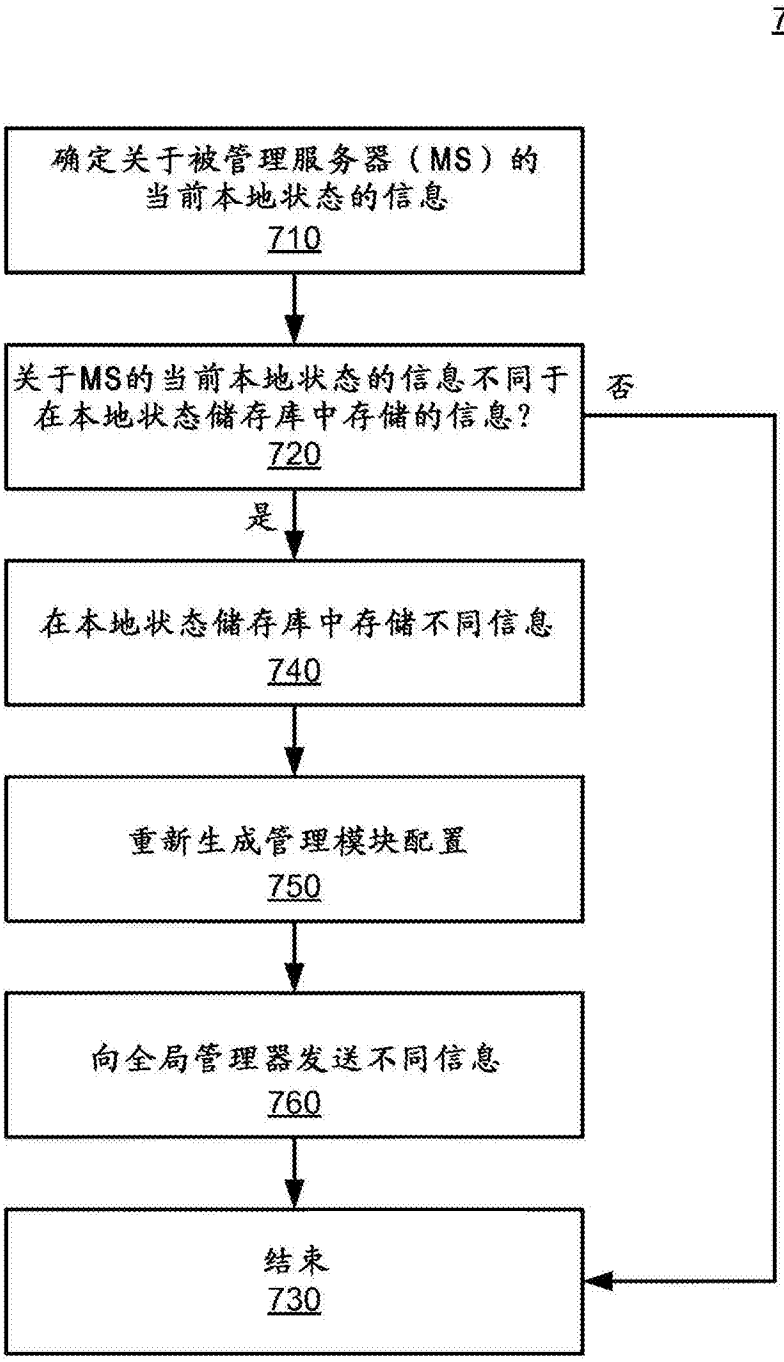

700
确定关于被管理服务器（MS）的当前本地状态的信息
710
关于MS的当前本地状态的信息不同于在本地状态储存库中存储的信息？
720
否
是
在本地状态储存库中存储不同信息
740
重新生成管理模块配置
750
向全局管理器发送不同信息
760
结束
730

图7

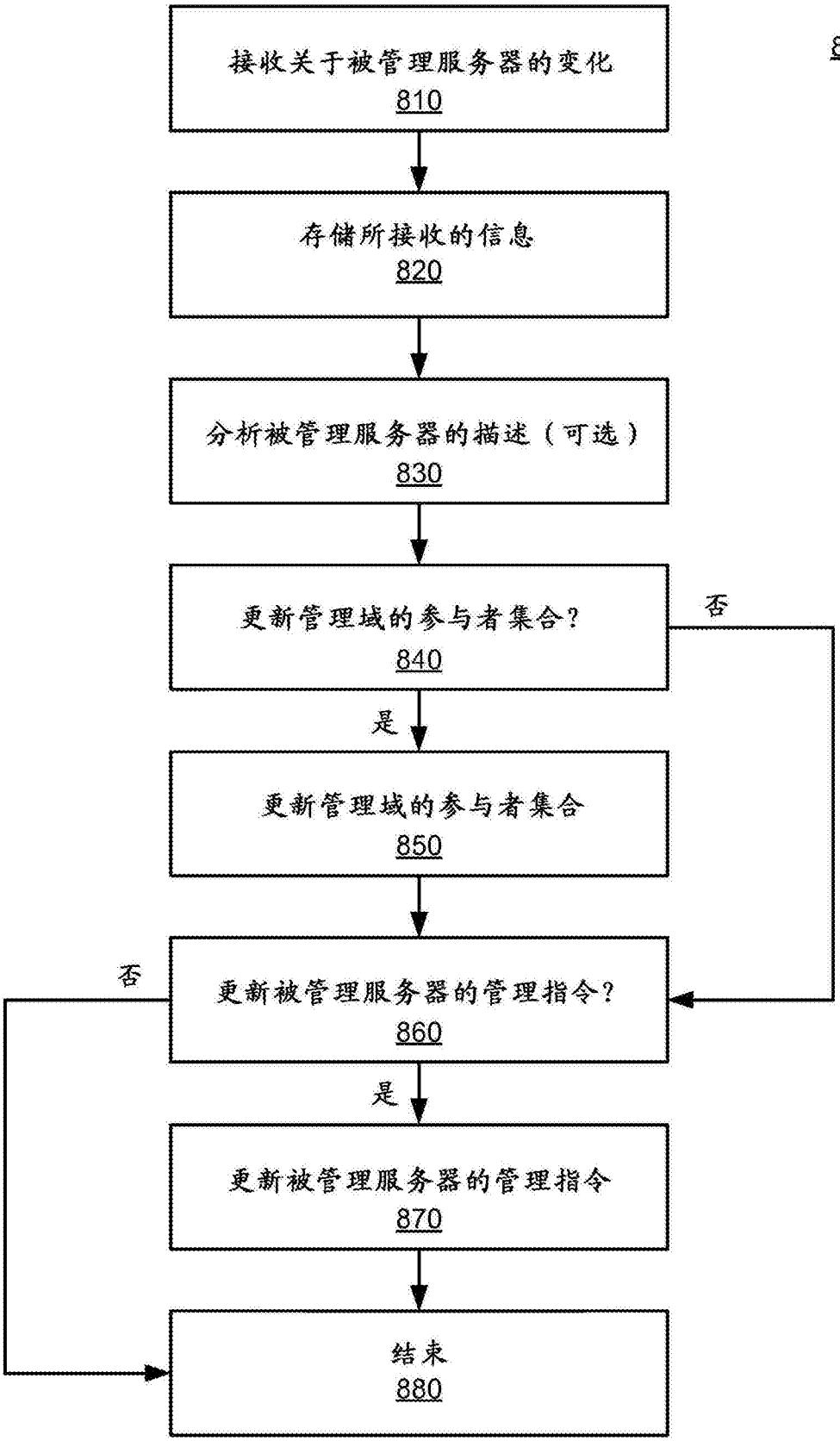

800
接收关于被管理服务器的变化
810
存储所接收的信息
820
分析被管理服务器的描述（可选）
830
更新管理域的参与者集合？
840
否
是
更新管理域的参与者集合
850
更新被管理服务器的管理指令？
860
否
是
更新被管理服务器的管理指令
870
结束
880

图8