(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 105684391 B
(45)授权公告日 2019.06.07

(21)申请号 201480060313.4

(22)申请日 2014.10.30

(65)同一申请的已公布的文献号
申请公布号 CN 105684391 A

(43)申请公布日 2016.06.15

(30)优先权数据
61/899,468 2013.11.04 US
62/066,835 2014.10.21 US

(85)PCT国际申请进入国家阶段日
2016.05.03

(86)PCT国际申请的申请数据
PCT/US2014/063239 2014.10.30

(87)PCT国际申请的公布数据
WO2015/066369 EN 2015.05.07

(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 M·K·格伦 M·格普塔 R·N·纳卡希玛 T·V·弗格塞

(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.
H04L 29/06(2006.01)

(56)对比文件
US 2004199792 A1,2004.10.07,
US 2010058340 A1,2010.03.04,
US 2011209195 A1,2011.08.25,
US 2012155290 A1,2012.06.21,

审查员 石璐

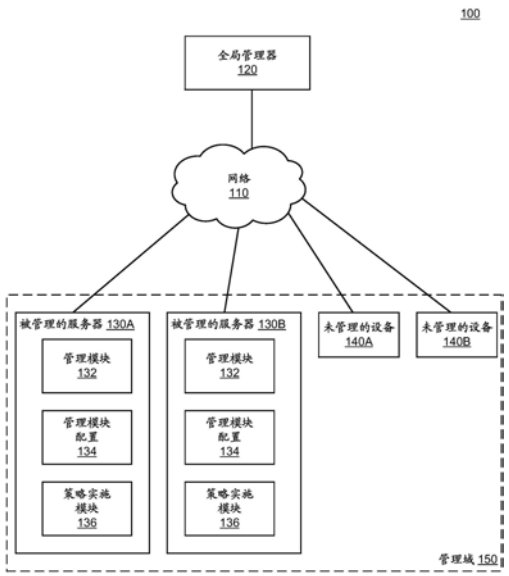
权利要求书5页 说明书32页 附图11页

(54)发明名称

基于标签的访问控制规则的自动生成

(57)摘要

确定一种授权管理域内的多个被管理的服务器之间的通信的访问控制规则。获得描述多个被管理的服务器之间的过往通信的通信信息。通过基于所获得的通信信息对多个被管理的服务器进行分组，来标识来自多个被管理的服务器的被管理的服务器的子集。分组级标签集被确定为与被管理的服务器的子集相关联。针对被管理的服务器的子集中的被管理的服务器确定角色标签。被管理的服务器与一个角色标签相关联。基于分组级标签集和角色标签，生成授权被管理的服务器的子集中的第一被管理的服务器与第二被管理的服务器之间的通信的访问控制规则。访问控制规则被存储为管理域范围管理策略的一部分。



CN 105684391 B

1.一种用于确定授权管理域内的多个被管理的服务器之间的通信的访问控制规则的方法,所述方法包括:

获得描述所述多个被管理的服务器之间的过往通信的通信信息;

通过基于获得的所述通信信息对所述多个被管理的服务器进行分组,来标识包含来自所述多个被管理的服务器中的被管理的服务器的子集的服务器组;

向所述组中的被管理的服务器的所述子集分配分组级标签集,所述分组级标签集包含描述所述组中的所述服务器的一个或多个分组标签;

向所述组内的单个被管理的服务器分配角色标签,其中与被管理的服务器相关联的角色标签基于关于所述被管理的服务器的信息而被确定;

基于所述通信信息、所述分组级标签集和所述角色标签,生成授权所述多个被管理的服务器之间的通信的访问控制规则;以及

将所述访问控制规则存储为管理域范围管理策略的一部分。

2.根据权利要求1所述的方法,

其中获得所述通信信息包括:标识由第一被管理的服务器提供并且由第二被管理的服务器使用的服务,以及

其中生成所述访问控制规则包括:生成指定所述服务的访问控制规则,所述访问控制规则包括指定所述第一被管理的服务器的进行提供部分和指定所述第二被管理的服务器的进行使用部分。

3.根据权利要求1所述的方法,其中所述生成包括:

标识第一被管理的服务器与第三被管理的服务器之间的过往未授权的通信,所述管理域范围管理策略缺乏描述所述未授权的通信的访问控制规则;

基于描述所述未授权的通信的信息、与所述第一被管理的服务器相关联的一个或多个标签和与所述第三被管理的服务器相关联的一个或多个标签,确定所述未授权的通信应当可允许;以及

生成授权先前未授权的通信的访问控制规则。

4.根据权利要求1所述的方法,其中所述生成包括:

标识与第一被管理的服务器类似的第三被管理的服务器,所述第一被管理的服务器和第三被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联;

标识与第二被管理的服务器类似的第四被管理的服务器,所述第二被管理的服务器和第四被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联;以及

生成授权所述第三被管理的服务器与所述第四被管理的服务器之间的通信的访问控制规则。

5.根据权利要求1所述的方法,其中所述生成包括:

标识与第一被管理的服务器类似的第三被管理的服务器,所述第一被管理的服务器和第三被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联;

标识与第二被管理的服务器类似的第四被管理的服务器,所述第二被管理的服务器和第四被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联;以及

将访问控制规则扩大以授权所述第三被管理的服务器与所述第四被管理的服务器之间的通信。

6.根据权利要求1所述的方法，其中所述生成包括：

生成授权第一被管理的服务器与所述管理域外部的设备之间的通信的访问控制规则；

标识与所述第一被管理的服务器类似的第三被管理的服务器，所述第一被管理的服务器和第三被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联；以及

生成授权所述第三被管理的服务器与所述管理域外部的所述设备之间的通信的新的访问控制规则。

7.根据权利要求1所述的方法，其中所述生成包括：

生成授权第一被管理的服务器与所述管理域外部的设备之间的通信的第二访问控制规则；

标识与所述第一被管理的服务器类似的第三被管理的服务器，所述第一被管理的服务器和第三被管理的服务器与匹配的角色标签和匹配的分组级标签集相关联；以及

将所述第二访问控制规则扩大以授权所述第三被管理的服务器与所述管理域外部的所述设备之间的通信。

8.根据权利要求1所述的方法，其中获得的所述通信信息描述所述多个被管理的服务器之间先前传送的数据的特性，并且其中标识被管理的服务器的所述子集包括：

通过基于所述多个被管理的服务器之间先前传送的数据的所述特性对所述多个被管理的服务器进行分组，来标识来自所述多个被管理的服务器的被管理的服务器的所述子集。

9.根据权利要求1所述的方法，其中获得的所述通信信息描述由被管理的服务器的所述子集执行的过程，并且其中分配所述角色标签包括：

基于由被管理的服务器执行的一个或多个过程，确定针对所述被管理的服务器的角色标签。

10.根据权利要求1所述的方法，其中获得的所述通信信息描述被管理的服务器的所述子集的硬件资源，并且其中分配所述角色标签包括：

基于被管理的服务器的硬件资源，确定针对所述被管理的服务器的角色标签。

11.根据权利要求1所述的方法，还包括：

请求管理员验证分配的所述分组级标签集和分配的所述角色标签中的至少一个；以及

响应于来自所述管理员的校正，修改所述分组级标签集和所述角色标签中的至少一个。

12.根据权利要求1所述的方法，还包括：

通过基于获得的所述通信信息对所述多个被管理的服务器进行分组，来标识多个服务器组。

13.一种处理来自实现一个或多个访问控制规则的被管理的服务器的警报的方法，所述方法包括：

获得来自第一被管理的服务器的警报，所述第一被管理的服务器被配置为响应于与第二被管理的服务器的过往通信并且响应于所述第一被管理的服务器确定所述一个或多个访问控制规则没有授权所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信而生成所述警报；

获得包括描述所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往

通信的通信信息的上下文信息；

基于所述通信信息，将所述过往通信分类为合法的或者恶意的；

响应于将所述过往通信分类为合法的，生成授权所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信的访问控制规则；以及

将所述访问控制规则存储为管理域范围管理策略的一部分。

14.根据权利要求13所述的方法，还包括指示所述第一被管理的服务器响应于所述第一被管理的服务器确定所述一个或多个访问控制规则没有授权所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信而终止所述过往通信。

15.根据权利要求13所述的方法，还包括指示所述第一被管理的服务器响应于将所述过往通信分类为恶意的而停止与所述第二被管理的服务器的所有通信。

16.根据权利要求13所述的方法，还包括指示所述第一被管理的服务器许可所述过往通信。

17.根据权利要求13所述的方法，

其中获得所述上下文信息包括：响应于由所述第二被管理的服务器发起的过往通信，确定生成警报的被管理的服务器的数目，并且

其中将所述过往通信分类包括：响应于被管理的服务器的所述数目超过被管理的服务器的阈值数目，将所述过往通信分类为恶意的。

18.根据权利要求13所述的方法，

其中获得所述上下文信息包括：标识所述第二被管理的服务器已经请求连接到的所述第一被管理的服务器的一个或多个端口，所述第一被管理的服务器缺乏监听标识的所述端口的任何过程，并且

其中将所述过往通信分类包括：响应于标识的所述端口的数目超过端口的阈值数目，将所述过往通信分类为恶意的。

19.根据权利要求13所述的方法，

其中获得所述上下文信息包括：在从所述第一被管理的服务器获得的所述警报之前，标识由所述第二被管理的服务器生成的一个或多个警报，标识的所述一个或多个警报响应于所述第二被管理的服务器与至少一个附加的被管理的服务器之间的过往通信而被生成，并且

其中将所述过往通信分类包括：基于由所述第二被管理的服务器生成的所述一个或多个警报，将所述过往通信分类为恶意的。

20.根据权利要求13所述的方法，其中生成所述访问控制规则包括：

请求管理员批准所述访问控制规则。

21.一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机程序模块，所述计算机程序模块由一个或多个处理器可执行以执行用于确定授权管理域内的多个被管理的服务器之间的通信的访问控制规则的步骤，所述步骤包括：

获得描述所述多个被管理的服务器之间的过往通信的通信信息；

通过基于获得的所述通信信息对所述多个被管理的服务器进行分组，来标识包含来自所述多个被管理的服务器中的被管理的服务器的子集的服务器组；

向所述组中的被管理的服务器的所述子集分配分组级标签集，所述分组级标签集包含

描述所述组中的所述服务器的一个或多个分组标签；

向所述组内的单个被管理的服务器分配角色标签，其中与被管理的服务器相关联的角色标签基于关于所述被管理的服务器的信息而被确定；

基于所述通信信息、所述分组级标签集和所述角色标签，生成授权所述多个被管理的服务器之间的通信的访问控制规则；以及

将所述访问控制规则存储为管理域范围管理策略的一部分。

22.一种用于处理来自实现一个或多个访问控制规则的被管理的服务器的警报的系统，所述系统包括：

一个或多个处理器；以及

非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机程序模块，所述计算机程序模块由一个或多个处理器可执行以执行步骤，所述步骤包括；

获得来自第一被管理的服务器的警报，所述第一被管理的服务器被配置为响应于与第二被管理的服务器的过往通信并且响应于所述第一被管理的服务器确定所述一个或多个访问控制规则没有授权所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信而生成所述警报；

获得包括描述所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信的通信信息的上下文信息；

基于所述通信信息，将所述过往通信分类为合法的或者恶意的；

响应于将所述过往通信分类为合法的，生成授权所述第一被管理的服务器与所述第二被管理的服务器之间的所述过往通信的访问控制规则；以及

将所述访问控制规则存储为管理域范围管理策略的一部分。

23.根据权利要求1所述的方法，其中标识服务器组还包括：

构建具有表示所述多个被管理的服务器中的被管理的服务器的节点和所述节点之间的边缘的图形，所述边缘表示所述被管理的服务器之间的通信；

将所述图形划分成子图形，所述子图形中的一个子图形对应于标识的所述服务器组。

24.根据权利要求1所述的方法，其中向所述组中的被管理的服务器的所述子集分配分组级标签集包括：

向所述服务器组中的被管理的服务器分配具有多个维度的分组级标签集，所述多个维度包括描述所述被管理的服务器所属的逻辑应用的应用维度；

将条件启发性应用于所述被管理的服务器以确定针对所述应用维度的值；

其中所述分组级标签集响应于针对所述应用维度的确定的所述值而被分配到所述组中的被管理的服务器的所述子集。

25.根据权利要求1所述的方法，其中向所述单个被管理的服务器分配角色标签包括：

基于所述被管理的服务器的硬件资源，向所述被管理的服务器分配所述角色标签。

26.根据权利要求1所述的方法，其中生成访问控制规则包括：

在所述通信信息中标识具有第一分组级标签和角色标签对的第一被管理的服务器和具有第二分组级标签和角色标签对的第二被管理的服务器之间的通信；

生成许可所述第一被管理的服务器与所述第二被管理的服务器之间的通信的访问控制规则；

标识所述多个被管理的服务器中具有第一标签对的其它被管理的服务器和所述多个被管理的服务器中具有第二标签对的其它被管理的服务器;以及

生成许可在具有所述第一标签对的所标识的其它被管理的服务器与具有所述第二标签对的所标识的其它被管理的服务器之间的通信的访问控制规则。

基于标签的访问控制规则的自动生成

技术领域

[0001] 本文所描述的主题内容总体上涉及管理管理域的服务器(物理或者虚拟)的领域，并且特别地涉及根据与基于逻辑多维标签的策略模型相符的管理域范围策略来管理服务器。

背景技术

[0002] 根据策略管理管理域的服务器(物理或者虚拟)。例如，安全策略可以指定访问控制和/或安全连通，而资源使用策略可以指定对监管预的计算资源(例如，磁盘和/或外设)的使用。常规策略引用物理设备并且在低级构造(比如网际协议(IP)地址、IP地址范围、子网和网络接口)方面被表达。这些低级构造使得难以用抽象和自然方式编写细粒度策略。

发明内容

[0003] 通过用于确定授权管理域内的多个被管理的服务器之间的通信的访问控制规则的方法、非暂态计算机可读存储介质和系统来解决以上和其他问题。该方法的实施例包括获得描述多个被管理的服务器之间的过往通信的通信信息。该方法还包括通过基于所获得的通信信息对多个被管理的服务器进行分组，来标识来自多个被管理的服务器的被管理的服务器的子集。该方法还包括确定与被管理的服务器的子集相关联的分组级标签集。该方法还包括确定用于被管理的服务器的子集中的被管理的服务器的角色标签，被管理的服务器与一个角色标签相关联。该方法还包括基于分组级标签集和角色标签，生成授权被管理的服务器的子集的第一被管理的服务器与第二被管理的服务器之间的通信的访问控制规则。该方法还包括存储访问控制规则作为管理域范围管理策略的一部分。

[0004] 介质的实施例存储由一个或多个处理器可执行以执行步骤的计算机程序模块。步骤包括获得描述多个被管理的服务器之间的过往通信的通信信息。步骤还包括通过基于所获得的通信信息对多个被管理的服务器进行分组，来标识来自多个被管理的服务器的被管理的服务器的子集。步骤还包括确定与被管理的服务器的子集相关联的分组级标签集。步骤还包括确定用于被管理的服务器的子集中的被管理的服务器的角色标签，被管理的服务器与一个角色标签相关联。步骤还包括基于分组级标签集和角色标签，生成授权被管理的服务器的子集的第一被管理的服务器与第二被管理的服务器之间的通信的访问控制规则。步骤还包括存储访问控制规则作为管理域范围管理策略的一部分。

[0005] 系统的实施例包括一个或多个处理器和存储由一个或多个处理器可执行以执行步骤的计算机程序模块的非暂态计算机可读存储介质。步骤包括获得描述多个被管理的服务器之间的过往通信的通信信息。步骤还包括通过基于所获得的通信信息对多个被管理的服务器进行分组，来标识来自多个被管理的服务器的被管理的服务器的子集。步骤还包括确定与被管理的服务器的子集相关联的分组级标签集。步骤还包括确定用于被管理的服务器的子集中的被管理的服务器的角色标签，被管理的服务器与一个角色标签相关联。步骤还包括基于分组级标签集和角色标签，生成授权被管理的服务器的子集的第一被管理的服

务器与第二被管理的服务器之间的通信的访问控制规则。步骤还包括存储访问控制规则作为管理域范围管理策略的一部分。

[0006] 通过用于处理来自实现一个或多个访问控制规则的被管理的服务器的警报的方法、非暂态计算机可读存储介质和系统来解决以上和其他问题。该方法的实施例包括获得来自第一被管理的服务器的警报，所述第一被管理的服务器被配置为响应于与第二被管理的服务器的过往通信并且响应于第一被管理的服务器确定一个或多个访问控制规则没有授权第一被管理的服务器与第二被管理的服务器之间的过往通信而生成警报。该方法还包括获得上下文信息，上下文信息包括描述第一被管理的服务器与第二被管理的服务器之间的过往通信的通信信息。该方法还包括基于通信信息，将过往通信分类为合法或者恶意的。方法还包括响应于将过往通信分类为合法的，生成授权第一被管理的服务器与第二被管理的服务器之间的过往通信的访问控制规则。该方法还包括存储访问控制规则作为管理域范围管理策略的一部分。

[0007] 介质的实施例存储由一个或多个处理器可执行以执行步骤的计算机程序模块。步骤包括获得来自第一被管理的服务器的警报，所述第一被管理的服务器被配置为响应于与第二被管理的服务器的过往通信并且响应于第一被管理的服务器确定一个或多个访问控制规没有未授权第一被管理的服务器与第二被管理的服务器之间的过往通信而生成警报。步骤还包括获得包括上下文信息，上下文信息描述第一被管理的服务器与第二被管理的服务器之间的过往通信的通信信息。步骤还包括基于通信信息，将过往通信分类为合法或者恶意的。步骤还包括响应于将过往通信分类为合法的，生成授权第一被管理的服务器与第二被管理的服务器之间的过往通信的访问控制规则。步骤还包括存储访问控制规则作为管理域范围管理策略的一部分。

[0008] 系统的实施例包括一个或多个处理器和存储由一个或多个处理器可执行以执行步骤的计算机程序模块的非暂态计算机可读存储介质。步骤包括获得来自第一被管理的服务器的警报，所述第一被管理的服务器被配置为响应于与第二被管理的服务器的过往通信并且响应于第一被管理的服务器确定一个或多个访问控制规则没有授权第一被管理的服务器与第二被管理的服务器之间的过往通信而生成警报。步骤还包括获得上下文信息，上下文信息包括描述第一被管理的服务器与第二被管理的服务器之间的过往通信的通信信息。步骤还包括基于通信信息，将过往通信分类为合法或者恶意的。步骤还包括响应于将过往通信分类为合法的，生成授权第一被管理的服务器与第二被管理的服务器之间的过往通信的访问控制规则。步骤还包括存储访问控制规则作为管理域范围管理策略的一部分。

附图说明

[0009] 图1是图示了根据一个实施例的用于管理管理域的服务器(物理或者虚拟)的环境的高级框图。

[0010] 图2是图示了根据一个实施例的用于用作图1中所图示的实体中的一个或者多个实体的计算机的示例的高级框图。

[0011] 图3是图示了根据一个实施例的全局管理器的具体视图的高级框图。

[0012] 图4是图示了根据一个实施例的被管理的服务器的策略实施模块的具体视图的高级框图。

[0013] 图5是图示了根据一个实施例的生成用于特定被管理的服务器的管理指令的方法的流程图。

[0014] 图6是图示了根据一个实施例的生成用于被管理的服务器的管理模块的配置的方法的流程图。

[0015] 图7是图示了根据一个实施例的监视被管理的服务器的逻辑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。

[0016] 图8是图示了根据一个实施例的处理对管理域的计算机网络基础结构的状态的改变的方法的流程图。

[0017] 图9是根据一个实施例的图示全局管理器的访问控制规则创建模块的详细视图的高级框图。

[0018] 图10是根据一个实施例的图示生成授权多个被管理的服务器之间的通信的访问控制规则的方法的流程图。

[0019] 图11是根据一个实施例的图示处理来自实现一个或多个访问控制规则的被管理的服务器的警报的方法的流程图。

具体实施方式

[0020] 附图和以下描述仅通过例示描述某些实施例。本领域技术人员将从以下描述容易地认识到可以运用这里例示的结构和方法的备选实施例而未脱离这里描述的原理。现在将参照若干实施例，在附图中图示了这些实施例的示例。注意，只要可实践，相似或者相同标号就可以在附图中被使用并且可以指示相似或者相同功能。

[0021] 图1是图示了根据一个实施例的用于管理管理域150的服务器(物理或者虚拟)130的环境100的高级框图。管理域150可以对应于企业，如例如服务提供者、公司、大学或者政府机关。环境100可以由企业本身或者由帮助企业管理它的服务器130的第三方(例如，第二企业)维护。如图所示，环境100包括网络110、全局管理器120、多个被管理的服务器130和多个未管理的设备140。多个被管理的服务器130和多个未管理的设备140与管理域150关联。例如，它们由企业或者由第三方(例如，公共云服务提供者)代表企业操作。尽管为了清楚而在图1中描绘的实施例中示出了一个全局管理器120、两个被管理的服务器130和两个未管理的设备140，但是其它实施例可以具有不同数目的全局管理器120、被管理的服务器130和/或未管理的设备140。

[0022] 网络110代表在全局管理器120、被管理的服务器130和未管理的设备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。在另一实施例中，网络110上的实体可以使用定制和/或专用数据通信技术。

[0023] 被管理的服务器130是实施管理域范围管理策略330(图3中所示)的机器(物理或者虚拟)。在一个实施例中，服务器是根据操作系统级虚拟化的虚拟服务器(有时被称为容器、虚拟化引擎、虚拟专有服务器或者jail)的用户空间实例，该操作系统级虚拟化是服务器虚拟化方法，其中操作系统的内核启用多个隔离的用户空间实例而不是仅一个实例。如果被管理的服务器130是物理机器，则被管理的服务器130是计算机或者计算机集合。如果被管理的服务器130是虚拟机，则被管理的服务器130在计算机或者计算机集合上执行。管理域范围管理策略330指定与管理域150关联的实体是否和/或如何被允许访问其它实体

(或者由其它实体访问)或者以别的方式消费(或者提供)服务。例如,管理域范围管理策略330指定安全或者资源使用。安全策略可以指定访问控制、安全连通、磁盘加密和/或对可执行过程的控制,而资源使用策略可以指定对管理域的计算资源(例如,磁盘、外设和/或带宽)的使用。

[0024] 被管理的服务器130包括管理模块132、管理模块配置134和策略实施模块136。管理模块132实施管理域范围管理策略330。例如,在安全的情况下,管理模块132可以是低级网络或者安全引擎,比如操作系统级防火墙、网际协议安全(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设使用引擎。

[0025] 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引擎应用的安全连通策略(例如,在Linux操作系统中体现为iptables条目和ipset条目)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设使用引擎应用的外设使用策略。

[0026] 策略实施模块136基于a)从全局管理器120接收的管理指令和b)被管理的服务器130的状态来生成管理模块配置134。管理指令部分地基于管理域范围管理策略330被生成。由策略实施模块136生成的管理模块配置134实施该管理域范围管理策略330(在策略涉及被管理的服务器130的程度上)。这一两步骤过程(生成管理指令和生成管理模块配置134)被称为对管理策略“实例化”。策略实施模块136也监视被管理的服务器130的本地状态并且向全局管理器120发送本地状态信息。

[0027] 在一个实施例中,策略实施模块136是更大专有模块(未示出)的部分。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(或虚拟设备)上,由此将设备(或虚拟设备)从未管理的设备140变换成被管理的服务器130。以下参照图4、图6和图7进一步描述策略实施模块136。

[0028] 未管理的设备140是不包括策略实施模块136的计算机(或者计算机集合)。未管理的设备140不实施管理域范围管理策略330。然而,在被管理的服务器130与未管理的设备140之间的交互可能受制于管理域范围管理策略330(如由被管理的服务器130实施的)。未管理的设备140的一个示例是由管理域150使用的网络电路。未管理的设备140的另一示例是由人用来向管理域150认证其自身的设备(例如,笔记本或者台式计算机、平板计算机或者移动电话)。

[0029] 全局管理器120是生成用于被管理的服务器130的管理指令并且向服务器发送生成的管理指令的计算机或者(或者计算机集合)。管理指令基于a)管理域的计算机网络基础结构320的状态和b)管理域范围管理策略330被生成。管理域的计算机网络基础结构320的状态包括对被管理的服务器130的描述和(可选地)对未管理的设备140的描述。全局管理器120也处理从被管理的服务器130接收的本地状态信息。

[0030] 管理域范围管理策略330基于逻辑管理模型,该逻辑管理模型可以基于被管理的服务器130的高级特性(这里被称为“标签”)来引用被管理的服务器。标签是包括“维度”(高级特性)和“值”(该高级特性的值)的对。在这一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昂贵。具体而言,使用对“标签”的更高级抽

象化来表达管理策略使人们能够更好地理解、可视化和修改管理策略。

[0031] 逻辑管理模型(例如,可用维度的数目和类型以及那些维度的可能的值)可配置。在一个实施例中,逻辑管理模型包括如表1中所示的以下维度和值:

[0032]

维度	含义(M)、值(V)
作用	M: 在管理域内的被管理的服务器的作用。 V: web、API、数据库

[0033]

环境	M: 被管理的服务器的生命周期阶段。 V: 生产、转运(staging)、开发
应用	M: 被管理的服务器属于的逻辑应用(对被管理的服务器的更高级分组)。 V: 贸易、人力资源
业务范围	M: 被管理的服务器属于的业务单位。 V: 营销、工程
位置	M:被管理的服务器的位置。可以是物理(例如,国家或者地区)或者逻辑(例如,网络)。物理对于表达地理顺应要求特别地有用。 V: US 或者 EU(物理)、us-west-1 或者 us-east-2(逻辑)

[0034] 表1-逻辑管理模型的示例

[0035] 逻辑管理模型使多个被管理的服务器130能够通过指定一个或者多个标签(这里称为"标签集合")而被分组在一起,该一个或者多个标签描述该组中的所有被管理的服务器130。标签集合包括用于逻辑管理模型中的维度的零个值或者一个值。标签集合无需包括用于逻辑管理模型中的所有维度的标签。以这一方式,逻辑管理模型实现对管理域的被管理的服务器130的分割和分离以及对被管理的服务器130的任意分组的创建。逻辑管理模型也允许单个被管理的服务器130存在于多个重叠集合(即,被管理的服务器的多个重叠组)中。逻辑管理模型未将单个被管理的服务器130限制于存在于嵌套集合的分级中。

[0036] 例如,在安全的情况下,分割可以与访问控制策略一起用来定义受制于特定策略的多组被管理的服务器130。相似地,分割可以与安全连通策略一起用来限定多组被管理的服务器130以及适用于组内通信和组间通信的策略。因此,在第一组被管理的服务器130(由第一标签集合指定)之中的通信可以受限于第一安全连接设置(例如,无需安全连接),并且在第一组被管理的服务器与第二组被管理的服务器(由第二标签集合指定)之间的通信可以受限于第二安全连接设置(例如,IPsec封装安全净荷(ESP)/认证报头(AH)高级加密标准(AES)/安全哈希算法-2(SHA-2))。

[0037] 在环境100中的每个被管理的服务器130实施管理域范围管理策略330(在策略涉及被管理的服务器130的程度上)。作为结果,管理域范围管理策略330以分布式方式贯穿管理域150被应用,并且没有扼流点。也在逻辑级、与管理域的物理网络拓扑和网络寻址方案

独立地应用管理域范围管理策略330。

[0038] 以下参照图3、图5和图8-11进一步描述全局管理器120、管理域的计算机网络基础结构320的状态和管理域范围管理策略330。

[0039] 图2是图示了根据一个实施例的用于用作图1中所图示的实体中的一个或者多个实体的计算机200的示例的高级框图。图示了耦合到芯片集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、指点设备214和网络适配器216耦合到I/O控制器集线器222。计算机200的其它实施例具有不同架构。例如，存储器206在一些实施例中直接地耦合到处理器202。

[0040] 存储设备208包括一个或者多个非瞬态计算机可读存储介质，比如硬驱动、紧致盘只读存储器(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。指点设备214与键盘210组合用来向计算机系统200中输入数据。图形适配器212在显示设备218上显示图像和其它信息。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的一些实施例具有与图2中所示部件不同的部件和/或除了图2中所示部件之外的部件。例如，全局管理器120和/或被管理的服务器130可以由多个刀片服务器形成并且没有显示设备、键盘和其它部件，而未管理的设备140可以是笔记本或者台式计算机、平板计算机或者移动电话。

[0041] 计算机200适于执行用于提供这里描述的功能的计算机程序模块。如这里所用，术语“模块”是指用来提供指定的功能的计算机程序指令和/或其它逻辑。因此，可以在硬件、固件和/或软件中实施模块。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、加载到存储器206中并且由处理器202执行。

[0042] 全局管理器

[0043] 图3是图示了根据一个实施例的全局管理器120的具体视图的高级框图。全局管理器120包括贮存库300和处理服务器310。贮存库300是存储管理域的计算机网络基础结构320的状态和管理域范围管理策略330的计算机(或者计算机集合)。在一个实施例中，贮存库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。

[0044] 管理域状态

[0045] 管理域的计算机网络基础结构320的状态包括对被管理的服务器130的描述和(可选地)对未管理的设备140的描述。对被管理的服务器130的描述例如包括唯一标识符(UID)、在线/离线指示符、一个或者多个配置的特性(可选)、网络暴露信息、服务信息和描述被管理的服务器130的一个或者多个标签(标签集合)。

[0046] UID唯一地标识被管理的服务器130。在线/离线指示符指示被管理的服务器130是在线还是离线。“配置的特性”存储与被管理的服务器130关联的值并且可以是任何类型的信息(例如，对哪个操作系统在被管理的服务器上运行的指示)。配置的特性与规则的条件部分(以下描述)结合被使用。

[0047] 网络暴露信息涉及被管理的服务器的网络接口。在一个实施例中，网络暴露信息对于被管理的服务器的网络接口中的每个网络接口包括网络接口附着到的“双向可达网络(BRN)”的标识符和用于在BRN内操作的零个或者更多个IP地址(及其子网)。BRN是在组织内

或者跨组织的子网集合，在BRN内的任何节点可以在这些子网中与BRN中的任何其它节点建立通信。例如，BRN中的所有节点具有唯一IP地址。换而言之，BRN节点不包含任何NAT。网络暴露信息(例如，网络接口的BRN标识符)可以与规则的条件部分结合被使用。

[0048] 在另一实施例中，网络暴露信息包括路由信息和被管理的服务器是否在网络地址翻译器(NAT)后面(以及如果它在NAT后面，则什么类型的NAT——1:1或者1:N)。全局管理器120可以确定被管理的服务器130是否在网络地址翻译器(NAT)后面(以及如果它在NAT后面，则什么类型的NAT——1:1或者1:N)。例如，全局管理器120通过比较(a)服务器的根据在全局管理器与服务器之间的TCP连接的IP地址和(b)服务器的根据从服务器接收的本地状态信息的IP地址来确定NAT是否存在于全局管理器120与被管理的服务器130之间。如果(a)和(b)不同，则NAT存在于全局管理器120与被管理的服务器130之间。如果NAT确实存在，则全局管理器120通过执行数据中心检测来确定NAT的类型(1:1或者1:N)。例如，全局管理器120用服务器的数据中心的公用IP地址来标识该数据中心。(备选地，被管理的服务器通过查询在服务器外部、但是在数据中心内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部分。)配置信息指示哪些类型的NAT由哪些数据中心使用。如果没有NAT信息与特定数据中心关联，则全局管理器120假设NAT类型是1:N。

[0049] 服务信息例如包括过程信息和/或封装信息。过程信息例如包括被管理的服务器130运行的过程的名称、那些过程在哪些网络端口和网络接口上监听、哪些用户发起那些过程、那些过程的配置、那些过程的命令行起动变元和那些过程的依赖性(例如，那些过程链接到的共享对象)。(那些过程对应于提供服务或者使用服务的被管理的服务器130。)封装信息例如包括哪些封装(可执行文件、库或者其它部件)被安装在被管理的服务器130上、那些封装的版本、那些封装的配置和那些封装的哈希值。

[0050] 对未管理的设备140的描述例如包括网络暴露信息(例如，未管理的设备140的IP地址和未管理的设备140连接到的BRN的标识符)。未管理的设备140是“未管理的设备组(UDG)”的部分。UDG包括一个或者多个未管理的设备140。例如，“总部UDG”可以包括由管理域的总部使用的主要电路和备用电路，其中每个电路与IP地址关联。UDG与唯一标识符(UID)关联。在管理域状态320中存储的关于UDG的信息包括UDG的UID和关于UDG中的未管理的设备140的信息(例如，它们的网络暴露信息)。

[0051] 对被管理的服务器130和未管理的设备140的描述可以按照各种方式被加载到管理域状态320中，比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。对被管理的服务器130的描述也可以基于从被管理的服务器接收的本地状态信息而被加载到管理域状态320中(以下描述)。

[0052] 具体地关于被管理的服务器的标签(以及配置的特性，如果有的话)，可以按照甚至更多方式执行对用于维度的值的指派(或者重新指派)(或者对配置的特性的值的设置)。例如，可以作为调配被管理的服务器130的部分、使用部署和配置工具来执行指派/设置。可以使用任何这样的工具，包括现货第三方工具(例如，Puppet Labs的Puppet软件、Opscode的Chef软件或者CFEngine AS的CFEngine软件)和管理域150可能具有的定制工具。

[0053] 作为另一示例，指派/设置可以由计算标签和/或配置的特性(“CC”)值的“标签/配置的特性引擎”(未示出)执行。在一个实施例中，标签/CC引擎基于标签/CC指派规则来计算标签/CC值。标签/CC指派规则是访问来自管理域状态320的数据并且指派(或者建议指派)

标签或者CC值的函数。标签/CC指派规则可以被预设或者可由用户配置。例如，全局管理器120包括预定义规则的集合，但是最终用户可以基于用户自己的定制要求来修改和/或删除那些规则并且添加新规则。可以在初始化过程期间为被管理的服务器130评估标签/CC指派规则。然后可以对于任何维度/CC做出标签/CC值建议，并且最终用户可以接受或者拒绝那些建议。例如，如果被管理的服务器130执行Postgres数据库或者MySQL数据库，则建议的标签可以是<作用，数据库>。如果被管理的服务器执行Linux操作系统，则用于操作系统CC的建议的值可以是“Linux”。

[0054] 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引擎使用连通图的最小切割和K均值算法与附加启发法的组合以自动地标识高连通的被管理的服务器130的聚类。被管理的服务器130的聚类可以对应于管理域150中的“应用”(见表1)。最终用户可以选择将用于应用维度(或者任何其它维度)的值全体地应用于那些被管理的服务器130。

[0055] 管理域范围管理策略

[0056] 管理域范围管理策略330包括一个或者多个规则。广而言之，“规则”指定在服务的一个或者多个提供者与该服务的一个或者多个消费者之间的关系。

[0057] 规则函数——关系受制于“规则函数”，这是规则的实践效果。例如，在安全的情况下，规则函数可以是访问控制、安全连通、盘加密或者对可执行过程的控制。具有访问控制函数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，访问控制函数使用纯粹“白名单”模型，这意味着仅可允许关系被表达，并且所有其它关系默认被阻止。具有安全连通函数的规则指定消费者可以在什么安全信道(例如，使用点到点数据加密的加密网络会话)之上使用提供者的服务。例如，具有安全连通函数的规则可以指定在提供者位于美国(US)而消费者位于欧洲(EU)时必须加密对提供者的服务的使用。具有磁盘加密函数的规则指定提供者是否必须在加密文件系统上存储它的数据。具有可执行过程控制函数的规则指定过程是否被允许执行。

[0058] 在资源使用的情况下，规则函数可以是磁盘使用或者外设使用。具有磁盘使用函数的规则指定消费者可以在提供者上存储的数据量。注意，规则可以指定其它规则函数以及超出仅访问控制、安全连通、磁盘加密、对可执行过程的控制、磁盘使用和外设使用。例如，规则函数可以指定哪些开放系统互连(OSI)模型第7层服务应用于网络流量、为安全分析而收集的元数据量或者用于捕获完整网络分组的触发。管理策略模型支持可以被应用的任何数目的规则函数。

[0059] 规则函数可以与一个或者多个设置(这里被称为“函数简档”)关联，该一个或者多个设置指定关于规则的实践效果的细节。例如，与安全连通规则函数关联的设置可以是用来加密网络流量的密码算法的列表。在一个实施例中，规则函数与多个函数简档关联，并且函数简档包括优先级。这一优先级如以下描述的那样由函数级指令生成模块360使用。

[0060] 服务——一般而言，“服务”是使用具体网络协议在具体网络端口上执行的任意过程。在管理策略330内的规则的服务由端口/协议对和(可选的)附加资格(比如(以上关于在管理域状态320内的对被管理的服务器130的描述而描述的)过程信息和/或封装信息)指定。如果被管理的服务器130具有多个网络接口，则可以在所有网络上或者仅在那些网络的子集上暴露服务。最终用户指定服务在哪些网络上被暴露。注意，取决于规则函数，服务可

以不使用任何网络资源。例如，用于可执行过程-控制规则函数的服务并不使用网络协议在网络端口上执行。

[0061] 提供者/消费者——服务的一个或者多个提供者和服务的一个或者多个消费者(即，用户)是被管理的服务器130和/或未管理的设备140。

[0062] 在一个实施例中，在管理域范围管理策略330内使用包括规则函数部分、服务部分、进行提供部分、进行使用部分和可选规则条件部分的信息集合来表示规则。规则函数部分描述规则的实践效果并且可以与一个或者多个设置(函数简档)关联。服务部分描述规则适用于的服务。如果服务部分指示“全部”，则规则适用于所有服务。

[0063] 进行提供(PB)部分描述哪些被管理的服务器130和/或未管理的设备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，任何被管理的服务器130或者未管理的设备140)可以提供服务。如果PB部分指示“任何被管理的服务器”，则任何被管理的服务器130可以提供服务。(“任何被管理的服务”等效于指定包含通配符的标签集合，由此匹配所有被管理的服务器130。)进行使用(UB)部分描述哪些被管理的服务器130和/或未管理的设备140可以使用服务(即，“消费者”是谁)。与PB部分相似，UB部分也可以指示“任何人”或者“任何被管理的服务器”。

[0064] 在PB部分和UB部分内，被管理的服务器130通过使用标签集合(即，描述被管理的服务器的一个或者多个标签)或者UID被指定。用于使用标签集合来指定被管理的服务器130的能力源于逻辑管理模型，该逻辑关联模型基于被管理的服务器的维度和值(标签)来引用被管理的服务器。未管理的设备140通过使用未管理的设备组(UDG)的UID被指定。如果规则指定UDG，则规则包括关于该组中的未管理的设备140的附加信息(例如，设备的网络暴露信息)。规则的PB部分和/或规则的UB部分可以包括多个项目，这些项目包括标签集合(用于指定被管理的服务器130)、被管理的服务器UID和/或UDG UID。

[0065] 可选的规则条件部分指定规则是否适用于特定被管理的服务器130和/或该被管理的服务器的特定网络接口。规则条件部分是包括一个或者多个配置的特性(“CC”；在管理域状态320中的对被管理的服务器的描述的部分)和/或网络暴露信息(例如，网络接口的BRN标识符；也是在管理域状态320中的对被管理的服务器的描述的部分)的布尔表达式。表达式的CC部分指定规则是否适用于特定被管理的服务器，而表达式的网络暴露信息部分指定规则是否适用于该被管理的服务器的特定网络接口。如果表达式对于特定被管理的服务器的配置的特性(具体地，对于被管理的服务器的配置的特性的值)和特定网络接口的信息评估为“真”，则规则适用于该被管理的服务器和该被管理的服务器的相关网络接口。如果表达式评估为“假”，则规则不适用于该被管理的服务器和该被管理的服务器的相关网络接口。例如，如果配置的特性存储对哪个操作系统在被管理的服务器上运行的指示，则包括配置的特性的规则条件部分可以基于特定被管理的服务器的操作系统来控制规则是否适用于该服务器。

[0066] 在管理域范围管理策略330内的规则被组织成规则列表。具体而言，管理策略330包括一个或者多个规则列表，并且规则列表包括一个或者多个规则和(可选的)一个或者多个范围。“范围”约束规则在何处被应用(即，应用于哪些被管理的服务器130)。范围包括限制对规则列表中的规则的应用的进行提供(PB)部分和进行使用(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

标签集合来指定一组被管理的服务器130。如果标签集合不包含用于具体维度的标签，则没有该维度的用于所得该组被管理的服务器130的范围设定。如果规则列表不包括任何范围，则全局地应用它的规则。

[0067] 不同范围可以应用于单个规则列表。例如，最终用户可以构建规则集合，这些规则表达web服务层(具有<作用，Web>标签的被管理的服务器130)如何消费来自数据库层(具有<作用，数据库>标签的被管理的服务器)的服务，负荷平衡层如何消费来自web服务层的服务，等等。然后，如果最终用户想要将这一规则列表应用于他的生产环境(具有<环境，生产>标签的被管理的服务器130)和他的转运环境(具有<环境，转运>标签的被管理的服务器)，则他无需复制或者重复规则列表。取而代之，他将多个范围应用于单个规则列表(第一范围和第二范围，在第一范围中，PB部分和UB部分包括<环境，生产>标签，在第二范围中，PB部分和UB部分包括<环境，转运>标签)。范围抽象化从可用性透视和计算透视二者使规则列表伸缩。

[0068] 现在，已经描述了管理域范围管理策略330，完成几个示例是有帮助的。考虑具有两层应用的管理域150，其中用户设备访问web服务器(第一层)，并且web服务器访问数据库服务器(第二层)。在第一层中，用户设备是消费者，并且web服务器是提供者。在第二层中，web服务器是消费者，并且数据库服务器是提供者。管理域150包括这一应用的两个实例：一个在生产环境中并且一个在转运环境中。

[0069] web服务器和数据库服务器是被管理的服务器130，并且它们的描述(例如，标签集合)在管理域状态320中存在。例如，它们的标签集合是：

[0070] 在生产中的web服务器：<作用，Web>和<环境，生产>

[0071] 在生产中的数据库服务器：<作用，数据库>和<环境，生产>

[0072] 在转运中的web服务器：<作用，Web>和<环境，转运>

[0073] 在转运中的的数据库服务器：<作用，数据库>和<环境，转运>

[0074] (应用维度、业务范围维度和位置维度与这一示例无关，因此省略它们的标签。)

[0075] 现在，考虑以下管理域范围管理策略330，该管理域范围管理策略330是指定访问控制和安全连通的安全策略：

[0076] 规则列表#1

[0077] • 范围

[0078] ○<环境，生产>

[0079] ○<环境，转运>

[0080] • 规则

[0081] ○#1

[0082] ■函数：访问控制

[0083] ■服务：Apache

[0084] ■PB：<作用，Web>

[0085] ■UB：任何人

[0086] ○#2

[0087] ■函数：访问控制

[0088] ■服务：PostgreSQL

[0089] ■PB:<作用,数据库>

[0090] ■UB:<作用,Web>

[0091] 规则列表#2

[0092] • 范围:无

[0093] • 规则:

[0094] ○#1

[0095] ■函数:安全连通

[0096] ■服务:全部

[0097] ■PB:<作用,数据库>

[0098] ■UB:任何被管理的服务器

[0099] 注意,以上规则为了清楚而将服务简称为“Apache”和“PostgreSQL”。记住,服务是过程并且由端口/协议对和(可选的)附加资格(比如(以上关于在管理域状态320内的对被管理的服务器130的描述而描述的)过程信息和/或封装信息)指定。

[0100] 规则列表#1/规则#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。具体而言,对连接的允许由函数部分中的“访问控制”指定。“任何设备”由UB部分中的“任何人”指定。“web服务器”由PB部分中的“<作用,Web>”(仅包括一个标签的标签集合)指定。Apache服务由服务部分中的“Apache”指定。

[0101] 规则列表#1/规则#2允许web服务器连接到数据库服务器上的PostgreSQL。具体而言,对连接的允许由函数部分中的“访问控制”指定。“web服务器”由UB部分中的“<作用,Web>”指定。“PostgreSQL”由服务部分中的“PostgreSQL”指定。“数据库服务器”由PB部分中的“<作用,数据库>”(仅包括一个标签的标签集合)指定。

[0102] 规则列表#1也防止环境间连接。例如,如果web服务器和数据库服务器二者在相同环境中(例如,二者在生产环境中或者二者在转运环境中)则允许web服务器连接到数据库服务器上的PostgreSQL。两个服务器在生产环境中由范围部分中的“<环境,生产>”(仅包括一个标签的标签集合)指定,而两个服务器在转运环境中由范围部分中的“<环境,转运>”(仅包括一个标签的标签集合)指定。(由于在这一示例中的范围在PB部分与UB部分之间不区分,所以每个范围的标签集合应用于PB部分和UB部分二者。)作为结果,如果服务器在不同环境中(例如,如果web服务器在转运环境中并且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。

[0103] 规则列表#2规定无论何时任何被管理的服务器连接到数据库服务器,必需通过加密的信道执行该连接。具体而言,“数据库服务器”由PB部分中的“<作用,数据库>”指定。“加密的信道”由函数部分中的“安全连通”指定。“任何被管理的服务器”由UB部分中的“任何被管理的服务器”指定。“无论何时”由服务部分中的“全部”指定。

[0104] 结束以上示例,考虑以下两个被管理的服务器130:服务器1是web服务器,该web服务器是生产的部分、app1的部分并且由在加利福尼亚的工程拥有。它将被标注为:

[0105] <作用,Web>

[0106] <环境,生产>

[0107] <应用,app1>

[0108] <LB,工程>

[0109] 〈位置,US〉

[0110] 服务器2是数据库服务器,该数据库服务器是生产的部分、也是app1的部分,并且也由工程拥有、但是在德国。它将被标注我:

[0111] 〈作用,数据库服务器〉

[0112] 〈环境,生产〉

[0113] 〈应用,app1〉

[0114] 〈LB,工程〉

[0115] 〈位置,EU〉

[0116] 假设访问控制规则允许对作为app1的部分的所有被管理的服务器130的访问。这一规则将允许服务器1和服务器2相互通信并且而将不允许作为app2的部分的在德国的被管理的服务器130与服务器1或者服务器2通信。现在假设安全连通规则指定必须加密在EU与US之间的所有网络流量。独立地应用规则函数。换而言之,安全连通规则是与访问控制规则独立应用的分离的策略。作为结果,从服务器1到服务器2的网络流量将被允许(假定访问控制规则)和加密(假定安全连通规则)。

[0117] 访问控制规则

[0118] 回到图3,管理域范围管理策略330包括以下在标题为“访问控制规则”的一节中描述访问控制规则的集合335。

[0119] 处理服务器

[0120] 处理服务器310生成用于被管理的服务器130的管理指令并且向服务器发送生成的管理指令。处理服务器310也处理从被管理的服务器130接收的本地状态信息。处理服务器310包括各种模型,比如策略引擎模块340、相关规则模块350、函数级指令生成模块360、动作者枚举模块370、相关动作者模块380、管理域状态更新模块385和访问控制规则创建模块390。在一个实施例中,处理服务器310包括与贮存库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、函数级指令生成模块360、动作者枚举模块370、相关动作者模块380、管理域状态更新模块385和访问控制规则创建模块390)的计算机(或者计算机集合)。

[0121] 相关规则模块350取得管理域范围管理策略330和对特定被管理的服务器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集合并且输出规则集合。这是相关规则模块350用来检查管理策略330并且仅提取用于给定的被管理的服务器130的相关规则的过滤过程。相关规则模块350通过迭代遍历管理策略330中的所有规则列表、分析每个规则列表的范围以确定范围是否适用于这一被管理的服务器130并且(如果范围确实适用于这一被管理的服务器130则)分析每个规则列表的规则以确定那些规则是否适用于这一被管理的服务器130来执行过滤。如果a)规则的PB部分和/或规则的UB部分指定被管理的服务器130和b)规则的条件部分(如果存在)对于该被管理的服务器(具体地,对于该被管理的服务器的配置的特性和网络暴露信息的值)评估为“真”,则规则适用于被管理的服务器。最后结果(这里被称为“管理策略透视”)是两个规则集合的汇集:其中这一被管理的服务器130提供服务的规则和其中这一被管理的服务器130消耗服务的规则。

[0122] 函数级指令生成模块360取得规则集合(例如,由相关规则模块350生成的管理策略透视)作为输入、生成函数级指令并且输出函数级指令。函数级指令然后被发送到被管理

的服务器130作为管理指令的部分。函数级指令与规则相似在于每个函数级指令包括规则函数部分、服务部分、PB部分和UB部分。然而，尽管规则可以在它的PB部分和/或UB部分内包括多个项目(包括标签集合、被管理的服务器UID和/或UDG UID)，但是函数级指令在它的PB部分内仅包括一个项目并且在它的UB部分内仅包括一个项目。同时，尽管规则可以在它的PB部分和/或UB部分内指定被管理的服务器(包括它的多个网络接口)，但是函数级指令在它的PB部分和UB部分内仅包括一个网络接口。

[0123] 函数级指令生成模块360分析规则并且基于该规则生成一个或者多个函数级指令。如果规则的PB部分包括多个项目，则规则的UB部分包括多个项目，或者由规则(在PB部分或者UB部分中)引用的被管理的服务器具有多个网络接口，则函数级指令生成模块360生成多个函数级指令(例如，每个函数级指令用于PB项目、UB项目和特定网络接口的一个可能组合)。

[0124] 考虑如下规则，该规则在它的PB部分内包括两个项目(A和B)并且在它的UB部分内包括两个项目(C和D)。函数级指令生成模块360将利用以下PB和UB部分生成四个函数级指令：1)PB＝A、UB＝C；2)PB＝A、UB＝D；3)PB＝B、UB＝C；4)PB＝B、UB＝D。现在考虑如下规则，该规则在它的PB部分或者UB部分中覆盖被管理的服务器(例如，通过指定UID或者标签集合)，并且该被管理的服务器具有多个网络接口。函数级指令生成模块360将生成多个函数级指令(例如，每个函数级指令用于被管理的服务器的一个网络接口)。

[0125] 函数级指令生成模块360分析规则、在那些规则内的函数和由那些规则引用的函数简档。如果规则列表包括多个范围，则函数级指令生成模块360将那些范围多次迭代地应用于规则列表(由此为每个范围生成函数级指令的完整集合)。回顾规则函数可以与多个函数简档关联，并且函数简档可以包括优先级。函数级指令生成模块360基于各种函数简档的优先级对规则进行排序，从而使得使用具有最高优先级的函数简档。函数级指令生成模块360将排序的规则翻译成供被管理的服务器130执行的函数级指令。函数级指令引用适当被管理的服务器130和/或未管理的设备140(例如，在输入的规则中引用的被管理的服务器130和/或未管理的设备140)，从而考虑与规则关联的服务的网络暴露细节。

[0126] 注意，函数级指令生成模块360可以生成供特定被管理的服务器130表现为对于该服务器而言无关的函数级指令。例如，该被管理的服务器由规则的进行提供(PB)部分覆盖，因此函数级指令生成模块360生成对应的函数级指令。然而，规则也包括指定被管理的服务器的本地状态的部分(例如，描述提供的服务的服务部分)。由于全局管理器120不知道被管理的服务器的本地状态(例如，被管理的服务器是否实际地提供该服务)，所以生成的函数级指令被发送到被管理的服务器。被管理的服务器如以下参照策略编译模块410而说明的那样检查它的本地状态(例如，它是否提供该服务)并且相应地处理函数级指令。

[0127] 动作者枚举模块370取得对被管理的服务器130和未管理的设备组(UDG)的描述的汇集(例如，管理域的计算机网络基础结构320的状态)作为输入、以枚举形式生成对服务器和UDG的那些描述的表示(被称为“动作者集合”)并且输出动作者集合。例如，动作者枚举模块370在管理域状态320和可能标签集合内枚举被管理的服务器130和UDG，并且指派每个唯一标识符。这些动作者集合然后可以与规则和范围的UB部分和PB部分结合被使用，这些UB部分和PB部分使用被管理的服务器UID、UDG UID和/或标签集合来指定动作者。

[0128] 考虑如下逻辑管理模型，该逻辑管理模型包括N个维度D_i(i＝1，…，N)的集合，并

且每个维度D_i包括可能值V_j(j＝1,…,M_i)的集合S_i(其中通配符“*”是可能值之一)。在一个实施例中,动作者枚举模块370枚举基于逻辑管理模型而可能的所有标签集合,这些标签集合等于由$S_1\times S_2\times\cdots\times S_N$给定的笛卡尔乘积。这一集合的大小是$M_1\times M_2\times\cdots\times M_N$。枚举过程将被管理的服务器130的多维标签空间折叠成简单枚举形式。

[0129] 在另一实施例中,动作者枚举模块370仅枚举基于管理域状态320(例如,基于对在管理域150内的被管理的服务器的描述)而可能的那些标签集合。例如,考虑如下逻辑管理模型,该逻辑管理模型包括2个维度(X和Y),并且每个维度包括3个可能值(A、B和*)。具有标签集合“<X＝A>,<Y＝B>”的被管理的服务器可以是4个可能标签集合的成员:1)“<X＝A>,<Y＝B>”、2)“<X＝A>,<Y＝*>”、3)“<X＝*>,<Y＝B>”和4)“<X＝*>,<Y＝*>”。注意,被管理的服务器的标签集合存在于2维空间(X和Y)中,而可能标签集合2、3和4是被管理的服务器的标签集合向子维空间中的投影(标签集合2是1维空间(X),标签集合3是1维空间(Y),并且标签集合4是0维空间)。因此,动作者枚举模块370枚举那些4个可能标签集合。具有标签集合“<X＝A>,<Y＝B>”的被管理的服务器不能是标签集合“<X＝A>,<Y＝A>”的成员,因此动作者枚举模块370未枚举该标签集合。

[0130] 在又一实施例中,动作者枚举模块370仅枚举在管理域范围管理策略330中(例如,在规则和范围的UB部分和PB部分中)使用的那些标签集合。

[0131] 动作者集合包括UID和零个或者更多个动作者集合记录。动作者集合记录在给定具体BRN时包括UID(被管理的服务器UID或者UDG UID)、动作者的操作系统的标识符和动作者(被管理的服务器130或者未管理的设备140)的IP地址。例如,动作者集合可以包括如下动作者集合记录,这些动作者集合记录的IP地址对应于由标签集合<作用,数据库>和<环境,生产>覆盖的所有被管理的服务器130。作为另一示例,动作者集合可以包括如下动作者集合记录,这些动作者集合记录的IP地址对应于总部UDG中的所有未管理的设备140。单个动作者(例如,被管理的服务器130或者未管理的设备140)可以在多个动作者集合中出现。

[0132] 动作者集合计算中的另一因素是具有多个网络接口的动作者加上包括网络拓扑(比如网络地址翻译(NAT))。因此,可以有用于标签集合<作用,数据库>和<环境,生产>的两个动作者集合:一个动作者集合具有那些被管理的服务器130的面向因特网的IP地址(即,与第一BRN关联),并且用于那些相同被管理的服务器的不同动作者集合具有那些被管理的服务器的面向私有网络的IP地址(即,与第二BRN关联)。

[0133] 在一个实施例中,动作者枚举模块370也可以基于对管理域状态320的改变来更新动作者集合。例如,动作者枚举模块370取得动作者集合(由动作者枚举模块先前输入)和对被管理的服务器的描述(在管理域状态320内)的改变作为输入、生成(与改变的服务器描述一致的)更新的动作者集合并且输出更新的动作者集合。动作者枚举模块370依赖于对被管理的服务器的描述的改变类型以不同方式生成更新的动作者集合。

[0134] 离线/在线改变——如果描述改变指示服务器从在线变成离线,则动作者枚举模块370通过从服务器是其成员的所有输入的动作者集合去除服务器的动作者集合记录来生成更新的动作者集合。如果描述改变指示服务器从离线变成在线,则动作者枚举模块370通过向任何相关的输入的动作者集合添加服务器的动作者集合来生成更新的动作者集合。(如果必需,则动作者枚举模块370创建新动作者集合,并且向该新动作者集合添加服务器的动作者集合记录。)

[0135] 标签集合改变——如果描述改变指示服务器的标签集合被改变，则动作者枚举模块370将这视为如第一服务器(具有旧标签集合)变成离线而第二服务器(具有新标签集合)变成在线。

[0136] 网络暴露信息改变——如果描述改变指示服务器去除网络接口，则动作者枚举模块370通过从服务器是其成员的所有输入的动作者集合(与网络接口的BRN关联)去除服务器的动作者集合记录来生成更新的动作者集合。如果描述改变指示服务器添加网络接口，则动作者枚举模块370通过向任何相关的输入的动作者集合(与该网络接口的BRN关联)添加服务器的动作者集合记录来生成更新的动作者集合。(如果必需，则动作者枚举模块370创建新动作者集合(与该网络接口的BRN关联)，并且向该新动作者集合添加服务器的动作者集合记录。)如果描述改变指示服务器改变网络接口的BRN，则动作者枚举模块370将这视为如去除第一网络接口(具有旧BRN)并且添加第二网络接口(具有新BRN)。如果描述改变指示服务器改变网络接口的IP地址(但是未改变BRN)，则动作者枚举模块370通过在服务器是其成员的所有输入的动作者集合(与该网络接口的BRN关联)中修改服务器的动作者集合记录来生成更新的动作者集合。

[0137] 相关动作者模块380取得一个或者多个动作者集合(例如，以枚举形式在管理域状态320中的被管理的服务器130和UDG)和规则集合(例如，管理策略透视)作为输入、确定哪些动作者集合与那些规则相关并且仅输出那些动作者集合。这是相关动作者模块380用来检查动作者集合并且仅提取用于给定的规则集合的相关动作者集合的过滤过程。相关动作者模块380通过迭代遍历所有输入的动作者集合、分析输入的规则的PB部分和UB部分以确定特定动作者集合是否被规则的PB部分或者UB部分中的任何部分引用来执行过滤。最终结果(这里被称为“动作者透视”)是动作者集合的汇集。动作者透视以后被发送到被管理的服务器130作为管理指令的部分。

[0138] 在一个实施例中，相关动作者模块380使用输入的规则集合以生成“动作者集合过滤器”。动作者集合过滤器从输入的动作者集合仅选择与输入的规则相关的动作者集合。换而言之，相关动作者模块380使用动作者集合过滤器以将输入的动作者集合过滤成相关动作者集合。

[0139] 策略引擎模块340生成用于被管理的服务器130的管理指令并且向服务器发送生成的管理指令。策略引擎模块340基于a)管理域的计算机网络基础结构320和b)管理域范围管理策略330来生成管理指令(使用相关规则模块350、函数级指令生成模块360、动作者枚举模块370和相关动作者模块380)。

[0140] 例如，策略引擎模块340执行相关规则模块350，从而提供管理域范围管理策略330和特定被管理的服务器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集合(“管理策略透视”)。策略引擎模块340执行动作者枚举模块370，从而提供管理域状态320作为输入。动作者枚举模块370以枚举形式输出在管理域状态320内对被管理的服务器130和未管理的设备组(UDG)的描述的表示(“动作者集合”)。策略引擎模块340执行函数级指令生成模块360，从而提供管理策略透视(由相关规则模块350输出)作为输入。函数级指令生成模块360输出函数级指令。策略引擎模块340执行相关动作者模块380，从而提供动作者集合(由枚举模块370输出)和管理策略透视(由相关规则模块350输出)作为输入。相关动作者模块380仅输出与那些规则相关的动作者集合(“相关动作者集合”)。策略引擎模块340

向特定被管理的服务器130发送函数级指令(由函数级指令生成模块360输出)和相关动作者集合(由相关动作者模块380输出)。

[0141] 在一个实施例中,策略引擎模块340高速缓存在以上过程期间生成的信息。例如,策略引擎模块340与特定被管理的服务器130关联地高速缓存管理策略透视、函数级指令、动作者集合过滤器和/或相关动作者集合。作为另一示例,策略引擎模块340高速缓存管理域的动作者集合(不是特定被管理的服务器130特有的)。

[0142] 由于管理域的动作者集合基于管理域状态320,所以对管理域状态320的改变无需对管理域的动作者集合的改变。相似地,由于被管理的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,所以对管理域状态320的改变和/或对管理域范围管理策略330的改变可能需要对被管理的服务器的管理指令的改变。在一个实施例中,策略引擎模块340可以更新管理域的动作者集合和/或更新被管理的服务器的管理指令,并且然后向被管理的服务器130分发这些改变(如果必需)。以上提到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动作者集合和/或被管理的服务器的管理指令以及分发改变。

[0143] 在一个实施例中,策略引擎模块340更新管理域的动作者集合(基于对管理域状态320的改变)并且如下向被管理的服务器130分发改变:策略引擎模块340执行动作者枚举模块370,从而提供高速缓存的动作者集合(由动作者枚举模块先前输出)和管理域状态320的改变的部分(例如,改变的服务器描述)作为输入。动作者枚举模块370输出更新的动作者集合。在一个实施例中,策略引擎模块340然后向在管理域150内的所有被管理的服务器130发送所有更新的动作者集合。然而,该实施例效率低,因为并非所有被管理的服务器受对所有动作者集合的改变所影响。

[0144] 在另一实施例中,仅选择的动作者集合被发送到选择的服务器。例如,向特定被管理的服务器仅发送a)向该服务器先前发送的和b)已经改变的那些动作者集合。高速缓存的相关动作者集合指示向该服务器先前发送了哪些动作者集合(见以上(a))。策略引擎模块340比较高速缓存的动作者集合与更新的动作者集合以确定哪些动作者集合已经改变(见以上(b))。策略引擎模块340然后计算(a)和(b)的交集。在该交集中的动作者集合被发送到特定被管理的服务器。在一个实施例中,为了甚至更大效率,在描述在高速缓存的动作者集合与更新的动作者集合之间的差异的“diff”格式中发送动作者集合。例如,diff格式指定动作者集合标识符、动作者标识符(例如,被管理的服务器UID或者UDG UID)和对该动作者是否应当被添加到动作者集合、从动作者集合被去除或者在动作者集合内被修改的指示。

[0145] 在又一实施例中,维护和使用两个表以提高效率。第一个表将被管理的服务器130与该被管理的服务器是其成员的动作者集合关联。第二个表将被管理的服务器130和与该被管理的服务器相关(例如,如由相关动作者模块380确定)的动作者集合关联。在这些表中,被管理的服务器130例如由该被管理的服务器的UID代表,并且动作者集合例如由该动作者集合的UID代表。策略引擎模块340使用管理域状态320的改变的部分(例如,改变的服务器描述)以确定哪些被管理的服务器的描述改变。策略引擎模块340使用第一个表以确定该被管理的服务器是哪些动作者集合的成员。那些动作者集合可能由于改变的服务器描述而改变。因此,策略引擎模块340使用第二个表以确定那些策略引擎模块340与哪些被管理的服务器相关。策略引擎模块340仅为那些被管理的服务器执行以上描述的计算交集计算。

[0146] 在一个实施例中,策略引擎模块340更新被管理的服务器的管理指令(基于对管理

域状态320的改变)并且如下向被管理的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,从而提供管理域范围管理策略330和被管理的服务器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集合(“管理策略透视”)。策略引擎模块340比较刚刚输出的管理策略透视与高速缓存的管理策略透视以确定它们是否不同。如果刚刚输出的管理策略透视和高速缓存的管理策略透视相同,则策略引擎模块340不采取进一步动作。在这一情形中,先前生成的被管理的服务器的管理指令(具体为函数级指令和相关动作者集合)与对管理域状态320的改变一致,并且无需被重新生成和重新发送到被管理的服务器。

[0147] 如果刚刚输出的管理策略透视和高速缓存的管理策略透视不同,则策略引擎模块340确定哪些规则应当被添加到高速缓存的透视以及哪些规则应当从高速缓存的透视被去除。策略引擎模块340执行函数级指令生成模块360,从而提供待添加的规则和待去除的规则作为输入。函数级指令生成模块360输出待添加的函数级指令和待去除的函数级指令(相对于向被管理的服务器先前发送的高速缓存的函数级指令)。策略引擎模块340在适当时指令被管理的服务器添加或者去除各种函数级指令。在一个实施例中,为了更大效率,以描述在高速缓存的函数级指令与更新的函数级指令之间的差异的“diff”格式发送函数级指令。例如,diff格式指定函数级指令标识符和对该函数级指令是否应当被添加到先前发送的函数级指令或者从先前发送的函数级指令被去除的指示。

[0148] 策略引擎模块340也执行动作者枚举模块370,从而提供高速缓存的动作者集合和管理域状态320的改变的部分(例如改变的服务器描述)作为输入。动作者枚举模块370输出更新的动作者集合。策略引擎模块340执行相关动作者模块380,从而提供更新的动作者集合和刚刚输出的管理策略透视作为输入。相关动作者模块380仅输出与那些规则相关的那些更新的动作者集合(“更新的相关动作者集合”)。

[0149] 策略引擎模块340比较更新的相关动作者集合与高速缓存的相关动作者集合以确定它们是否不同。如果更新的相关动作者集合和高速缓存的相关动作者集合相同,则策略引擎模块340不向被管理的服务器发送动作者集合。在这一情形中,先前生成的相关动作者集合与对管理域状态320的改变一致,并且无需被重新发送到被管理的服务器。如果更新的相关动作者集合和高速缓存的相关动作者集合不同,则策略引擎模块340确定哪些动作者集合相对于高速缓存的相关动作者集合而应当被添加、去除或者修改。策略引擎模块340在适当时指令被管理的服务器添加、去除或者修改各种动作者集合。在一个实施例中,为了更大效率,以描述在高速缓存的相关动作者集合与更新的相关动作者集合之间的差异的“diff”格式发送动作者集合。例如,diff格式指定动作者集合标识符和对该动作者集合是否应当被添加到先前发送的动作者集合、从先前发送的动作者集合被去除或者相对于先前发送的动作者集合被修改。

[0150] 回顾策略引擎模块340可以更新被管理的服务器的管理指令(基于对管理域范围管理策略330的改变)并且向被管理的服务器发送更新的管理指令。对管理策略330的改变例如是添加、去除或者修改规则或者规则集合。在一个实施例中,通过经由GUI或者API与全局管理器120交互来生成对管理策略330的改变。在另一实施例中,对管理策略330的改变由在全局管理器120内的自动化的过程生成(例如,响应于由全局管理器检测的安全威胁)。策略引擎模块340以相似方式更新被管理的服务器的管理指令并且向被管理的服务器发送更

新的管理指令而无论是否有对管理策略330的改变或者对管理域状态320的改变。然而，存在少许不同。

[0151] 在对管理策略330的改变的情况下，策略引擎模块340未必更新用于所有被管理的服务器130的管理指令。取而代之，策略引擎模块340比较先前管理策略330与新管理策略330以确定哪些规则相对于先前管理策略330应当被添加、去除或者修改。策略引擎模块340确定哪些被管理的服务器130受改变的规则影响(例如，哪些被管理的服务器被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(如果有)覆盖)。策略引擎模块340执行相关规则模块350，从而提供改变的规则(而不是整个新管理策略330)和被管理的服务器130的UID(仅对于受改变的规则影响的那些服务器)作为输入。

[0152] 管理域状态更新(ADSU)模块385接收对管理域状态320的改变并且处理那些改变。对管理域状态320的改变例如是添加、去除或者修改对被管理的服务器130的描述(包括修改被管理的服务器的标签集合或者配置的特性)或者对未管理的设备或者未管理的设备组的描述。在一个实施例中，对管理域状态320的改变在从特定被管理的服务器130接收的本地状态信息中始发。在另一实施例中，通过经由GUI或者APPI与全局管理器120交互来生成对管理域状态320的改变。在又一实施例中，对管理域状态320的改变由在全局管理器120内的自动化的过程生成(例如，响应于由全局管理器检测到安全威胁)。

[0153] 例如ADSU模块385接收关于特定未管理的设备140的改变。ADSU模块385在管理域状态320中存储新信息(例如，作为特定被管理的设备是其成员的未管理的设备组的部分)。ADSU模块385然后基于未管理的设备组改变来更新管理域的动作者集合。具体而言，ADSU模块385指令策略引擎模块340更新管理域的动作者集合。在一个实施例中，ADSU模块385在指令策略引擎模块340更新管理域的动作者集合之前等待事件出现。这一事件可以例如是接收用户命令或者出现指定的维护窗口。

[0154] 作为另一示例，ADSU模块385接收关于特定被管理的服务器130的改变。ADSU模块385在管理域状态320中存储新信息作为对该特定被管理的服务器130的描述的部分。ADSU模块385然后(可选地)分析该被管理的服务器的描述以确定关于该服务器的附加信息并且在描述中存储该信息。ADSU模块385然后基于对被管理的服务器的描述的改变来确定是否更新管理域的动作者集合和/或被管理的服务器的管理指令。如果ADSU模块385确定更新管理域的动作者集合，则ADSU模块385指令策略引擎模块340更新管理域的动作者集合。在一个实施例中，ADSU模块385在指令策略引擎模块340更新管理域的动作者集合之前等待事件出现。如果ADSU模块385确定更新被管理的服务器的管理指令，则ADSU模块385指令策略引擎模块340更新被管理的服务器的管理指令。在一个实施例中，ADSU模块385在指令策略引擎模块340更新被管理的服务器的管理指令之前等待事件出现。前述事件可以例如是接收用户命令或者出现指定的维护窗口。

[0155] ADSU模块385是否确定更新管理域的动作者集合和/或被管理的服务器的管理指令依赖于对被管理的服务器的描述的改变类型。在一个实施例中，ADSU模块385如表2中所示做出这一确定。

[0156]

改变类型	是否更新
在线到离线	管理域的动作者集合：是 被管理的服务器的管理指令：否
离线到在线	管理域的动作者集合：是 被管理的服务器的管理指令：是
标签集合	管理域的动作者集合：是 被管理的服务器的管理指令：是
配置的特性	管理域的动作者集合：是 被管理的服务器的管理指令：是
网络暴露信息	管理域的动作者集合：是 被管理的服务器的管理指令：是 （除非IP地址是仅有的改变）
服务信息	管理域的动作者集合：否 被管理的服务器的管理指令：是 （仅在指定的情形中）

[0157] 表2-是否基于服务器描述改变类型更新管理域的动作者集合和/或被管理的服务器的管理指令

[0158] 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关于服务器的附加信息。标签/CC引擎基于服务器的描述和标签/CC指派规则来计算用于服务器的标签/CC值。在另一实施例中，ADSU模块385确定服务器是否在网络地址翻译器(NAT)后面(以及如果它在NAT后面，则什么类型的NAT——1:1或者1:N)。

[0159] 以下在标题为“访问控制规则”的一节中描述访问控制规则创建模块390。

[0160] 策略实施模块

[0161] 图4是图示了根据一个实施例的被管理的服务器130的策略实施模块136的具体视图的高级框图。策略实施模块136包括本地状态贮存库400、策略编译模块410、本地状态更新模块420和警报生成模块430。本地状态贮存库400存储关于被管理的服务器130的本地状态的信息。在一个实施例中，本地状态贮存库400存储关于被管理的服务器的操作系统(OS)、网络暴露和服务的信息。OS信息例如包括对哪个OS正在运行的指示。以上关于在管理域状态320内的对被管理的服务器130的描述来描述网络暴露信息和服务信息。

[0162] 策略编译模块410取得管理指令和被管理的服务器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被接收并且包括函数级指令(由函数级指令生成模块360生成)和相关动作者集合(由相关动作者模块380输出)。从本地状态贮存库400接收被管理的服务器130的状态。在一个实施例中，对策略编译模块410的执行被以下触发：由a)被管理的服务器上电或者上线、b)被管理的服务器接收管理指令和/或c)本地状态贮存库400的内容改变。

[0163] 策略编译模块410将函数级指令和相关动作者集合映射到管理模块配置134中。例如，策略编译模块410将访问控制函数级指令(包含端口和动作者集合引用)映射到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)规则中。

[0164] 管理策略在被管理的服务器130处的应用可以受该服务器的本地状态影响。在一个实施例中，策略编译模块410评估与接收的函数级指令关联的条件，并且基于该评估的结果来生成管理模块配置134。例如，策略编译模块410评估对被管理的服务器的对等服务器(即，在关系中的另一动作者)的操作系统进行引用的条件，并且基于该评估的结果来选择函数简档属性，其中在管理模块配置134中表达选择的函数简档属性。

[0165] 作为另一示例，回顾被管理的服务器130可以接收表现为对于该服务器而言无关的函数级指令。例如，规则包括如下部分：该部分指定被管理的服务器的本地状态(例如，描述提供的服务的服务部分)。由于全局管理器120不知道被管理的服务器的本地状态(例如，被管理的服务器是否实际地提供该服务)，所以生成的函数级指令被发送到被管理的服务器。策略编译模块410检查被管理的服务器的本地状态(例如，确定被管理的服务器是否提供该服务)。这一确定相当于评估对被管理的服务器的本地状态进行引用的条件。策略编译模块410相应地处理函数级指令。如果策略编译模块410确定条件评估为“真”(例如，被管理的服务器提供该服务)，则策略编译模块410将该函数级指令并入到管理模块配置134中。具体而言，策略编译模块410仅在评估关联条件(涉及该服务器的本地状态)之后将函数级指令并入到管理模块配置134中。如果对条件的评估为假，则策略编译模块410在管理模块配置134中不表达函数级指令。具体条件(例如，它们的性质和特定值)可扩展。在一个实施例中，条件与对“服务”的定义有关并且包括过程信息和/或封装信息(以上关于在管理域状态320内的对被管理的服务器130的描述而被描述)。

[0166] 例如，考虑仅允许访问在端口80上入站的Apache服务的函数级指令(即，其中被管理的服务器130是“提供者”或者端点)。被管理的服务器130在管理模块配置134中表达这一函数级指令以仅在评估关联条件之后允许在端口80上的访问，该条件涉及在端口80上监听的应用(在该服务器上执行)是否实际地是Apache而不是某个其它应用(反常或者以别的方式)。被管理的服务器130仅在确定关联条件评估为“真”之后在管理模块配置134中表达这一函数级指令。如果关联条件评估为“假”，则被管理的服务器130在管理模块配置134中不表达这一函数级指令。作为结果，网络流量被阻止。

[0167] 在一个实施例中，被管理的服务器130监视它的出站连接。被管理的服务器130比较出站网络流量与它的内部过程表以确定该表中的哪些过程建立那些出站连接。被管理的服务器130可以强制实行仅允许某些过程(给定以上被称为“过程信息”的要求集合)建立出站连接的规则。

[0168] 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处而不是被管理的服务器130处。在该实施例中，全局管理器120不向被管理的服务器130发送管理指令。取而代之，被管理的服务器130向全局管理器120发送它的本地状态。在策略编译模块410生成管理模块配置134(在全局管理器120处)之后，从全局管理器120向被管理的服务器130发送管理模块配置134。

[0169] 本地状态更新(LSU)模块420监视被管理的服务器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确定被管理的服务器130的初始本地状态、在本地状态贮存库400中存储适当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/或文件系统的各种部分来确定被管理的服务器130的本地状态。例如，LSU模块420从OS的内核表(联网信息)、OS的系统表(封装信息)和文件系统(文件和哈希值)获得服务信息。LSU模块420从OS的内核和/或OS级数据结构获得网络暴露信息。

[0170] 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模块监视对本地状态的改变。LSU模块例如通过轮询(例如，周期地执行检查)或者监听(例如，预订事件流)来监视改变。LSU模块420比较新近地获得的本地状态信息与在本地状态贮存库400中已经存储的信息。如果信息匹配，则LSU模块420不采取进一步动作(直至再次获得本地状态信息)。如果它们不同，则LSU模块420在本地状态贮存库400中存储新近地获得的信息、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通知改变。在一个实施例中，LSU模块420以描述在本地状态贮存库400中先前存储(和因此向全局管理器120先前发送)的本地状态信息与新近地获得的本地状态信息之间的差异的“diff”格式向全局管理器120发送对本地状态信息的改变。例如，diff格式指定本地状态信息类型(例如，操作系统)和用于该信息类型的新值。在另一实施例中，LSU模块420向全局管理器120发送本地状态贮存库400的全部内容。

[0171] 以下在标题为“访问控制规则”的一节中描述警报生成模块430。

[0172] 生成管理指令

[0173] 图5是图示了根据一个实施例的生成用于特定被管理的服务器130的管理指令的方法500的流程图。其它实施例可以按照不同顺序执行步骤并且可以包括不同和/或附加步骤。此外，步骤中的一些或者所有步骤可以由除了图1中所示实体之外的实体执行。在一个实施例中，多次执行方法500(例如，对于在管理域150中的每个被管理的服务器130一次)。

[0174] 在方法500开始时，管理域的计算机网络基础结构320的状态和管理域范围管理策略330已经被存储在全局管理器120的贮存库300中。这时，方法500开始。

[0175] 在步骤510中，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向贮存库300发送请求并且作为响应而接收管理域状态320和管理域范围管理策略330。

[0176] 在步骤520中，确定一个或者多个相关规则。例如，策略引擎模块340执行相关规则模块350，从而提供管理域范围管理策略330和特定被管理的服务器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集合(管理策略透视)。

[0177] 在步骤530中，枚举动作者。例如，策略引擎模块340执行动作者枚举模块370，从而提供管理域状态320作为输入。动作者枚举模块370以枚举格式(动作者集合)在管理域状态320内生成对被管理的服务器130和未管理的设备组(UDG)的表示。

[0178] 在步骤540中，生成一个或者多个函数级指令。例如，策略引擎模块340执行函数级指令生成模块360，从而提供管理策略透视(在步骤520中生成)作为输入。函数级指令生成模块360生成函数级指令。

[0179] 在步骤550中，确定一个或者多个相关动作者。例如，策略引擎模块340执行相关动作者模块380，从而提供动作者集合(在步骤530中生成)和管理策略透视(在步骤520中生

成)作为输入。相关动作者模块380仅输出与那些规则相关的动作者集合(相关动作者集合)。

[0180] 在步骤560中,向特定被管理的服务器130发送管理指令。例如,策略引擎模块340向特定被管理的服务器130发送函数级指令(在步骤540中生成)和相关动作者集合(在步骤550中生成)。

[0181] 注意,步骤520和540涉及生成用于特定被管理的服务器130的管理策略透视(和所得函数级指令),而步骤530和550涉及生成用于该被管理的服务器的动作者透视。对管理策略透视的生成和对动作者透视的生成最少地相互依赖,因为步骤520生成由步骤550使用的规则集合。即使这样,保持管理策略计算(即,步骤520和540)和动作者集合计算(即,步骤530和550)分离增强策略引擎模块340的可伸缩性。由于保持管理策略计算和动作者集合计算最多地分离,所以可以并行执行它们(例如,即使对于相同被管理的服务器130)。此外,也可以并行执行用于不同被管理的服务器130的透视计算。同时,如果动作者改变,则仅需重新计算动作者集合。(无需重新计算函数级指令。)如果规则改变,则仅需重新计算函数级指令和相关动作者集合。(无需重新枚举动作者。)

[0182] 配置管理模块

[0183] 图6是图示了根据一个实施例的生成用于被管理的服务器130的管理模块132的配置134的方法600的流程图。其它实施例可以按照不同顺序执行步骤并且可以包括不同和/或附加步骤。此外,步骤中的一些或者所有步骤可以由除了图1中所示实体之外的实体执行。

[0184] 在方法600开始时,关于被管理的服务器130的本地状态的信息已经被存储在被管理的服务器130中的策略实施模块136的本地状态贮存库400中。这时,方法600开始。

[0185] 在步骤610中,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接收函数级指令和相关动作者集合。

[0186] 在步骤620中,访问本地状态。例如,策略编译模块410访问在本地状态贮存库400中存储的关于被管理的服务器130的本地状态的信息。

[0187] 在步骤630中,生成管理模块配置134。例如,策略编译模块410取得管理指令(在步骤610中接收)和本地状态(在步骤620中访问)作为输入,并且生成管理模块配置134。

[0188] 在步骤640中,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中生成)操作。

[0189] 监视被管理的服务器

[0190] 图7是图示了根据一个实施例的监视被管理的服务器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。其它实施例可以按照不同顺序执行步骤并且可以包括不同和/或附加步骤。此外,步骤中的一些或者所有步骤可以由除了图1中所示实体之外的实体执行。

[0191] 在方法700开始时,关于被管理的服务器130的本地状态的信息已经被存储在被管理的服务器130的本地状态贮存库400中。这时,方法700开始。

[0192] 在步骤710中,确定关于被管理的服务器130的当前本地状态的信息。例如,LSU模块420通过检查服务器的操作系统(OS)和/或文件系统的各种部分来确定被管理的服务器130的本地状态。

[0193] 在步骤720中，关于当前本地状态的信息是否与在本地状态贮存库400中存储的信息不同执行确定。例如，LSU模块420执行这一确定。如果信息并非不同，则该方法前进到步骤730并且结束。如果信息确实不同，则该方法前进到步骤740。

[0194] 在步骤740中，在本地状态贮存库400中存储不同信息。例如，LSU模块420执行这一步骤。

[0195] 在步骤750中，重新生成管理模块配置134(因为本地状态贮存库400的内容已经改变)，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，该策略编译模块410重新生成管理模块配置134。

[0196] 在步骤760中，向全局管理器120发送不同的信息。例如，LSU模块420执行这一步骤。

[0197] 更新管理域状态

[0198] 图8是图示了根据一个实施例的处理对管理域的计算机网络基础结构320的状态的改变的方法800的流程图。其它实施例可以按照不同顺序执行步骤并且可以包括不同和/或附加步骤。此外，步骤中的一些或者所有步骤可以由除了图1中所示实体之外的实体执行。

[0199] 在步骤810中，接收关于特定被管理的服务器130的改变。例如，管理域状态更新(ADSU)模块385从被管理的服务器130接收在线/离线指示符、操作系统指示符、网络暴露信息和/或服务信息作为本地状态信息的部分。

[0200] 在步骤820中，存储接收的信息。例如，ADSU模块385在管理域状态320中(具体地，在对信息与之有关的被管理的服务器130的描述中)存储接收的在线/离线指示符、网络暴露信息和/或服务信息。

[0201] 在步骤830中，分析服务描述以确定关于服务器的附加信息。例如，ADSU模块385使用标签/配置的特性引擎以计算用于服务器的标签/CC值和/或确定服务器是否在网络地址翻译器(NAT)后面(以及如果它在NAT后面，则什么类型的NAT——1:1或者1:N)，并且在服务器描述中存储该信息。步骤830是可选的。

[0202] 在步骤840中，关于是否更新管理域的动作者集合做出确定。例如，ADSU模块385基于对被管理的服务器的描述的改变来确定是否更新管理域的动作者集合。如果做出更新管理域的动作者集合的确定，则该方法前进到步骤850。如果做出不更新管理域的动作者集合的确定，则该方法前进到步骤860。

[0203] 在步骤850中，更新管理域的动作者集合。例如，ADSU模块385指令策略引擎模块340更新管理域的动作者集合并且相应地通知受影响的被管理的服务器130。在一个实施例(未示出)中，ADSU模块385在指令策略引擎模块340更新管理域的动作者集合之前等待事件出现。

[0204] 在步骤860中，关于是否更新被管理的服务器的管理指令做出确定。例如，ADSU模块385基于对被管理的服务器的描述的改变来确定是否更新被管理的服务器的管理指令。如果做出更新被管理的服务器的管理指令的确定，则该方法前进到步骤870。如果做出不更新被管理的服务器的管理指令的确定，则该方法前进到步骤880。

[0205] 在步骤870中，更新被管理的服务器的管理指令。例如，ADSU模块385指令策略引擎模块340更新被管理的服务器的管理指令。在一个实施例(未示出)中，ADSU模块385在指令

策略引擎模块340更新被管理的服务器的管理指令之前等待事件出现。

[0206] 在步骤880中，该方法结束。

[0207] 访问控制规则

[0208] 回忆全局管理器120的管理域范围管理策略330包括访问控制规则的集合335。访问控制规则的集合335包括一个或多个访问控制规则，其是关于访问控制规则功能的规则。宽广地，访问控制规则授权第一被管理的服务器130与第二被管理的服务器130或者与未管理设备140或者与管理域150外部的设备之间的通信。在一个实施例中，访问控制规则指定消费者是否可以使用提供者的服务。这样的访问控制规则指定进行提供(PB)部分、进行使用(UB)部分和服务。在一个实施例中，访问控制规则使用在纯“白名单”模型中，其中仅当访问控制规则的集合335包括具有匹配的PB、UB和服务部分的访问控制规则，消费者才可以访问对提供者的服务。

[0209] 访问控制规则可以通过使用通配符代替一个或多个部分仅部分地指定PB、UB和服务部分。例如，如果访问控制规则具有指定通配符的UB部分，那么任何被管理的服务器130、未管理设备140或者管理域150外部的其他设备可以访问服务。PB和UB部分可以指定一个或多个特定动作者(例如，使用被管理的服务器UID或者UDG UID)、一个或多个标签集或者其组合。示例访问控制规则具有指示特定被管理的服务器130的PB部分和指示标签集<角色，数据库服务器>和<环境，生产>的UB部分。示例访问控制规则允许具有“数据库服务器”角色并且属于“生产”环境的被管理的服务器130访问特定被管理的服务器130处的服务。

[0210] 回忆被管理的服务器130的策略实施模块136包括警报生成模块430。警报生成模块430监视被管理的服务器130与其他动作者(被管理的服务器130、未管理设备140或者管理域150外部的设备)之间的通信，以用于符合包含在管理模块配置134中的访问控制规则。警报生成模块430响应于检测到不符合访问控制规则的通信(被称为“未授权的通信”)而生成警报，并且将警报发送给全局管理器120，其中，警报是由访问控制规则创建模块390(特别地，通过警报处理模块950)来处理。未授权的通信包括用于使用由被管理的服务器130所提供的服务的消费者的尝试以及用于使用由另一动作者所提供的服务的被管理的服务器130的尝试。例如，将网络流量发送给与服务相关联的一部分或者从与服务相关联的端口接收网络流量的尝试可以是未授权的通信。在访问控制规则用作可允许活动的白名单的实施例中，管理模块132允许匹配访问控制规则的所尝试的通信并且拒绝不匹配访问控制规则的所尝试的通信。

[0211] 当管理模块132拒绝或者阻止向被管理的服务器130的通信或来自被管理的服务器130的通信时，警报生成模块430生成警报。警报描述与通信相对应的服务、服务的提供者和服务的消费者。警报可以包含关于服务的相关服务信息以及关于提供者和消费者的网络暴露信息。警报可以包含描述通信的特性的通信信息。通信信息可以包括所尝试的通信的定时、持续时间、频率、协议类型、数据大小(例如，总大小、分组大小)或者数据速率。例如，通信信息在访问服务的单个尝试与访问服务的重复尝试之间进行区分。通信信息还可以描述诸如源地址、目的地地址和路径信息的通信的路由信息(例如，负载均衡器和路由未授权的通信的NAT设备)。

[0212] 访问控制规则创建模块

[0213] 回忆全局管理器120的处理服务器310包括访问控制规则创建模块390。图9是根据

一个实施例的图示全局管理器120的访问控制规则(ACR)创建模块390的详细视图的高级框图。ACR创建模块390包括上下文信息采集模块910、被管理的服务器分组模块920、标签引擎930、流处理模块940、警报处理模块950和访问控制规则(ACR)创建接口960。

[0214] 上下文信息采集模块910获得描述管理域150中的动作者(被管理的服务器130或者未管理设备140)并且描述由管理域150中的动作者所发送或者所接收的通信的上下文信息。上下文信息包括被管理的服务器信息、未管理设备信息、外部设备信息、通信信息和管理域信息。

[0215] 被管理的服务器信息描述被管理的服务器130的特性。被管理的服务器信息包括诸如过程信息和封装信息的服务信息,如上文关于管理域状态320所描述的。被管理的服务器信息可以描述标识符(例如,UID、因特网协议(IP)地址、媒体访问控制(MAC)地址、主机名称)、硬件资源(例如,处理器类型、处理器吞吐量、处理器负载、总存储器、可用存储器、网络接口设备、存储设备类型)或者被管理的服务器类型(例如,物理设备、云提供式虚拟设备、虚拟机、Linux容器)。被管理的服务器信息可以描述软件资源,诸如操作系统和由过程信息和封装信息所描述的其他软件。

[0216] 虚拟化或者基于云的被管理的服务器130还与环境信息相关联,其描述被管理的服务器130的提供者(例如,专有数据中心、第三方私有数据中心、云提供者)以及与提供者通信的通信协议(例如,封装信息、网络地址、网络地址转换)。关于被管理的服务器130的被管理的服务器信息被存储在被管理的服务器的本地状态贮存库400中并且发送给全局管理器120以用于由上下文信息采集模块910处理。为了从虚拟化或者基于云的被管理的服务器130取回被管理的服务器信息,上下文信息采集模块910可以查询云服务提供者或者提供虚拟服务器的软件,以发送被管理的服务器信息或者其他上下文信息。

[0217] 未管理设备信息描述诸如网络暴露信息的未管理设备140的特性,如上文关于管理域状态320所描述的。未管理设备信息可以包括标识符(例如,UDG UID、IP地址、MAC地址、设备名称)、硬件资源、软件资源或者未管理设备140的网络连接性(例如,可用端口、端口与服务之间的映射)。被管理的服务器130可以采集关于未管理设备140的未管理设备信息,所述未管理设备140与被管理的服务器130通信并且将未管理设备信息发送给全局管理器120,以用于由上下文信息采集模块910处理。备选地或者附加地,全局管理器120查询管理域150中的未管理设备140以采集未管理设备信息。由于未管理设备140不包括报告未管理设备的局部状态的策略实施模块136,因而未管理设备信息可以是不完整的或者比被管理的服务器信息更不详细。

[0218] 外部设备信息描述与被管理的服务器130通信的管理域150外部的设备的特性。外部设备信息可以包括标识符(例如,IP地址、统一资源定位符(URL)、其他网络地址)、硬件资源、软件资源或者外部设备的网络连接性。被管理的服务器130可以采集外部设备信息并且将信息发送给全局管理器120,以用于由上下文信息采集模块910处理,但是许多外部设备信息对于被管理的服务器130可以不是可见的。另外,外部设备信息描述外部设备的声誉信息,其指示外部设备的可信度。在一个实施例中,上下文信息采集模块910获得匹配外部设备的标识符的声誉信息。使用声誉信息,上下文信息采集模块910将外部设备分类为安全、恶意或者中性的。声誉信息可以是二进制指示符(例如,外部设备的标识符是否在黑名单上)或者得分(例如,与标识符相关联的危险的相对评估)。

[0219] 上文关于警报生成模块430描述通信信息。被管理的服务器130将通信信息发送给全局管理器120，其描述由被管理的服务器130所发送或者所接收的通信。在一个实施例中，被管理的服务器130独立于评价通信是授权还是未授权的，而发送关于通信的通信信息。当上下文信息采集模块910接收描述相同通信的复制通信信息，上下文信息采集模块910可以合并或者去复制通信信息。例如，上下文信息采集模块910删除从两个被管理的服务器130(一个提供服务并且一个消费服务)所接收的通信信息。

[0220] 上下文信息采集模块910基于从被管理的服务器130所接收的上下文信息，来生成管理域信息。管理域信息聚集关于管理域150或者关于管理域150中的动作者的子集的上下文信息。管理域中的动作者的子集可以是由标签集所描述的被管理的服务器130。在一个实施例中，管理域信息描述具有至少一个共同特性的通信。共同特性可以是特定端口、过程、协议或者动作者(例如，被管理的服务器130、未管理设备140、外部设备)。例如，上下文信息采集模块910生成指示具有与特定服务相关联的损坏的二进制的被管理的服务器130的数目的管理域信息。作为另一示例，上下文信息采集模块910生成指示由特定动作者所扫描的被管理的服务器130的数目的管理域信息。“扫描”是指将请求(例如，探头)发送给被管理的服务器130并且使用被管理的服务器的响应(或者缺少其)获得或者自动确定被管理的服务器130的配置和在被管理的服务器130上执行的过程。

[0221] 在一个实施例中，上下文信息采集模块910生成指示管理域150内的异常活动的管理域信息。上下文信息采集模块910标识与特定动作者相关联的上下文信息、一组被管理的服务器130(例如，通过共同标签集表征)、共同服务或者某个其他特点。上下文信息采集模块910使用数量概括上下文信息(例如，通信量、损坏文件的数目)并且将数量与阈值数量相比较。阈值数量可以基于预配置设置或者可以基于针对数量的先前历史标准而动态地确定。例如，阈值数量是针对数量的每周移动平均值以上的两个标准偏差。响应于与阈值数量相比较，上下文信息采集模块910确定概括的上下文信息是否是异常的。例如，上下文信息采集模块910确定被管理的服务器130将试图在被管理的服务器130已经访问的这样的端口的数目超过阈值数目的情况下，访问与任何服务不相关联的异常数目的端口。

[0222] 被管理的服务器分组模块920获得描述管理域150中的动作者之间的通信的通信信息。基于通信信息，被管理的服务器分组模块920将被管理的服务器130分组为应用组。应用组是被管理的服务器130的集合，其与组外部的动作者的通信容量相比较具有组内的显著通信容量。在一个实施例中，被管理的服务器分组模块920构建图形，其中，节点表示管理域150的被管理的服务器130，并且其中边缘表示被管理的服务器130之间的通信。边缘具有指示节点之间的通信的存在/缺少的二进制值或者具有量化通信容量的非二进制值(例如，频率、数据大小、持续时间)。例如，将两个节点连接的边缘的值是与两个节点相对应的被管理的服务器130之间交换的数据的每天的量。图形可以是受忽视通信的方向的边缘未取向的，或者图形可以是受根据通信的方向的定向边缘取向的。例如，指向远离节点的定向边缘指示对应的被管理的服务器130是服务的消费者，并且指向节点的定向边缘指示被管理的服务器130是服务的提供者。被管理的服务器分组模块920将图形划分成各自与应用组相对应的子图形。例如，被管理的服务器分组模块920应用深度优先搜索、k-means聚类或者最小切割算法对图形进行分区。换句话说，被管理的服务器分组模块920基于通过上下文信息采集模块910所聚集的通信信息，将被管理的服务器130分组为应用组。

[0223] 标签引擎930获得被管理的服务器信息，并且至少部分基于被管理的服务器信息，确定用于被管理的服务器130的标签。标签引擎930与标签/CC引擎类似，但是不确定所配置的特性。在一个实施例中，标签引擎930确定与应用组中的被管理的服务器130相关联的分组级标签集(即，一个或多个分组级标签)。在一个实施例中，分组级标签集包括具有与被管理的服务器130的环境、应用和位置相对应的维度的标签。还关于表1和管理域范围管理策略330描述了标签。

[0224] 标签引擎930可以基于与被管理的服务器130相关联的网络地址(例如，IP地址和/或URL)的位置，来确定被管理的服务器的位置维度的值。标签引擎930可以基于使用上下文信息(和/或从上下文信息所导出的信息)的条件启发性，来确定被管理的服务器的标签的值。可以由管理员创建或者可以预配置条件启发性。例如，条件启发性指定如果被管理的服务器130由特定云服务提供者提供或者定位在特定数据中心中，那么标签引擎930确定针对被管理的服务器的环境维度的特定值。作为另一示例，条件启发性指定如果被管理的服务器130包含特定文件或者过程(或者特定文件或者过程的集合)，那么标签引擎930确定针对被管理的服务器的应用维度的特定值。标签引擎930可以请求管理员指示分组级标签集或者验证自动生成的分组级标签集。标签引擎930响应于管理员的指示或者校正而修改分组级标签集。

[0225] 除适于应用组的分组级标签集外，标签引擎930确定针对应用组内的单个被管理的服务器130的角色标签(即，具有角色维度的标签)。在一个实施例中，标签引擎930基于硬件资源、服务信息或者其他被管理的服务器信息，确定用于被管理的服务器130的角色标签。例如，标签引擎930确定如果总可用存储器超过阈值，则被管理的服务器130是数据库。作为另一示例，标签引擎930基于网络接口的数目，确定被管理的服务器130是负载均衡器。在一个实施例中，标签引擎930从被管理的服务器信息获得关于在被管理的服务器130上执行的过程的信息，并且基于过程确定角色维度的值。表3图示了过程与角色维度值之间的示例映射。

[0226]

过程	角色维度值
Postgres	数据库
Oracle	数据库
SQLServer	数据库
Apache	HTTP服务器
NGINX	HTTP服务器
HAProxy	负载均衡器

[0227] 表3-过程与角色维度值之间的映射

[0228] 流处理模块940获得管理域150中的动作者之间的通信信息并且生成与通信信息相对应的访问控制规则。在一个实施例中，流处理模块940标识没有由访问控制规则授权的通信并且生成授权通信的访问控制规则。为了生成访问控制规则，流处理模块940标识生成通信的服务、服务的提供者和服务的消费者。流处理模块940利用指示所标识的服务的服务部分、指示所标识的提供者的PB部分和指示所标识的消费者的UB部分，来生成访问控制规则。在一个实施例中，流处理模块940假定不存在管理域150中的异常或者恶意通信，并且因

此，生成授权存在于管理域150中的任何通信的访问控制规则。

[0229] 在一个实施例中，流处理模块940基于分组级标签集和被管理的服务器130的角色标签，生成访问控制规则。流处理模块940确定目标访问控制规则。例如，目标访问控制规则由管理员通过GUI指定(例如，通过指示与被管理的服务器分组模块920所生成的图形相对应的所显示的图形的特定边缘)。所生成的访问控制规则指定服务、第一被管理的服务器130作为服务的提供者和第二被管理的服务器130作为服务的消费者。流处理模块940标识由标签引擎930所生成的第一被管理的服务器和第二被管理的服务器130的角色标签和分组级标签集。然后，流处理模块940使用(与所显示的图形的特定边缘相对应的)所指定的服务来生成应用到被管理的服务器130的其他消费者-提供者对的附加访问控制规则。作为服务的提供者的所标识的被管理的服务器130具有与第一被管理的服务器130匹配的分组级标签集和角色标签。作为服务的消费者的所标识的被管理的服务器130具有与第二被管理的服务器130匹配的的分组级标签集和角色标签。备选地或者附加地，为了生成涵盖被管理的服务器130的所标识的消费者-提供者对的附加访问控制规则，流处理模块940将目标访问控制规则扩大为包括被管理的服务器130的所标识的消费者-提供者对。例如，经扩大的访问控制规则的PB部分和UB部分是根据包括角色标签和分组级标签集的标签集而不是根据特定被管理的服务器130的标识符来指定的。

[0230] 在一个实施例中，流处理模块940生成控制第一被管理的服务器130与另一动作者(例如，非被管理的服务器140、管理域外面的外部设备)之间的通信的访问控制规则。流处理模块940标识指定服务、第一被管理的服务器130和另一动作者的现有访问控制规则。流处理模块940标识与第一被管理的服务器130具有类似标签(包括角色标签和分组级标签集)的第二被管理的服务器130。第一被管理的服务器和第二被管理的服务器130二者是要么所指定的服务的消费者要么所指定的服务的提供者。流处理模块940生成授权第二被管理的服务器130与另一动作者之间的服务相关的通信的另一访问控制规则。备选地或者附加地，为了生成附加访问控制规则，流处理模块940通过根据第一被管理的服务器的标签集(包括角色标签和分组级标签集)，而不是根据第一被管理的服务器130的标识符来指定访问控制规则的PB部分或者UB部分，从而来扩大现有访问控制规则。

[0231] 在一个实施例中，流处理模块940生成用于修改管理域150内的被管理的服务器130的服务器状态的规则。服务器状态确定管理模块132实现访问控制规则到什么程度。在实施状态中，管理模块132阻止或者终止根据访问控制规则是未授权的通信。例如，在纯白名单策略中，管理模块132阻止或者终止不匹配至少一个访问控制规则的通信。服务器状态还包括建立状态和测试状态，其中，即使通信未由访问控制规则授权，管理模块132也许可通信。为了发起建造状态或者测试状态，流处理模块940利用指定通配符的PB、UB和服务部分生成无限制的访问控制规则。换句话说，无限制的访问控制规则授权所有通信，这是因为不存在对各种服务或者动作者的访问控制规则的适用性的限制。为了从建立状态或者测试状态转变到实施状态，流处理模块940移除无限制的访问控制规则。

[0232] 警报处理模块950获得来自被管理的服务器130的警报、处理警报，并且(如果适当的话)基于所获得的警报，生成访问控制规则。在一个实施例中，当被管理的服务器130处于实施状态或者测试状态时，警报处理模块950获得来自被管理的服务器130的警报。当被管理的服务器130处于建立状态时，警报处理模块950指示被管理的服务器130不响应于检测

到未由访问控制规则授权的通信而生成警报。当被管理的服务器130处于测试状态时，即使管理模块132不将实施访问控制规则以阻止未授权流量，警报生成模块430也生成指示未授权流量的警报。

[0233] 在响应于警报而生成访问控制规则之前，警报处理模块950对使用与警报相关的所获得的上下文信息触发警报的通信进行分类。上下文信息包括描述通信的通信信息、关于发送或者接收通信的任何被管理的服务器130的被管理的服务器信息或者管理域信息。如果响应于与外部设备的通信而生成警报，则上下文信息包括外部设备信息。如果响应于与未管理设备140的通信而生成警报，则上下文信息包括未管理设备信息。警报处理模块950基于所获得的上下文信息，将触发警报的通信分类为合法或者恶意的。例如，如果外部设备信息指示外部设备是恶意的，那么通信被分类为恶意的。

[0234] 在一个实施例中，如果管理域信息指示发起通信的动作者与异常活动相关联，则警报处理模块950将通信分类为恶意的。上下文信息采集模块910可以生成概括与共同特性(诸如共同动作者、过程、端口或者协议)相关联的警报的数目的管理域信息。如果与共同特点相关联的警报的数目超过阈值数目，那么上下文信息采集模块910将通信分类为恶意的。例如，如果响应于由被管理的服务器130所发起的流量所生成的警报的数目超过阈值数目，那么由被管理的服务器130所发起的通信被分类为恶意的。

[0235] 警报处理模块950可以确定所获得的管理域信息指示渐进感染的存在。在渐进感染中，恶意软件随时间跨越管理域150散布。如果管理域信息指示来自第一被管理的服务器130的警报的数目超过阈值并且如果与第一被管理的服务器130通信的第二被管理的服务器130开始生成警报，那么警报处理模块950确定警报与渐进感染相关联。因此，警报处理模块950将触发警报的通信分类为恶意的。

[0236] 备选地或者附加地，为了根据上下文信息对警报进行分类，警报处理模块950响应于接收到警报而通知管理员。通知管理员可以包括报告与触发警报的通信有关的上下文信息。警报处理模块950可以从管理员接收分类，其指示对应的通信是否是合法或者恶意的。

[0237] 警报处理模块950处理根据对应的通信的分类的警报。如果对应的通信被分类为恶意的，则警报处理模块950不生成授权对应的通信的访问控制规则。在一些实施例中，警报处理模块950指示被管理的服务器130停止与发起触发警报的通信的发起动作者通信。换句话说，隔离发起动作者。警报处理模块950响应于将对应的通信分类为恶意的，通知管理员关于警报。备选地或者附加地，警报处理模块950不管警报的分类，通知管理员关于警报。如果对应的通信被分类为合法的，那么警报处理模块950可以指示流处理模块940生成授权通信的访问控制规则。在一些实施例中，警报处理模块950在将访问控制规则添加到访问控制规则的集合335之前，可以从管理员请求针对访问控制规则的批准。

[0238] 访问控制规则(ACR)创建接口960向管理员提供用于回顾上下文信息的接口、应用组、分配给被管理的服务器130的标签集(例如，包括角色标签和/或分组级标签集)和访问控制规则。ACR创建接口960可以从管理员接收被管理的服务器130的所校正的应用组。作为响应，被管理的服务器分组模块920更新被管理的服务器的应用组以匹配经校正的应用组。此外，标签引擎930更新被管理的服务器130的分组级标签集以匹配新选择的应用组的分组级标签集。ACR创建接口960可以接收用于被管理的服务器130的经校正的标签集，并且标签引擎930根据校正来更新被管理的服务器的标签集。响应于管理员修改应用的分组级标签

集，标签引擎930修改应用组中的其他被管理的服务器130的分组级标签集以匹配经校正的分组级标签集。

[0239] ACR创建接口960可以从管理员接收目标访问控制规则(例如，通过指示所显示的图形的特定边缘的管理员)。例如，管理员的目标访问控制规则指示服务、服务的提供者和服务的消费者。流处理模块940根据管理员的指示来生成访问控制规则，并且可能基于服务和提供者和消费者的标签集而生成附加访问控制规则(或者扩大所生成的访问控制规则)。

[0240] ACR创建接口960可以关于由警报处理模块950所获得的警报通知管理员。ACR创建接口960可以接收触发警报的通信的分类，并且流处理模块940可以根据分类生成访问控制规则。在一个实施例中，ACR创建接口960向管理员呈现由流处理模块940自动生成的访问控制规则。ACR创建接口960可以接收对自动生成的访问控制规则的管理员的批准、修改或者拒绝。流处理模块940响应于接收到来自管理员的同意或者修改，将(可能地经修改的)自动生成的访问控制规则添加到访问控制规则的集合335。

[0241] 生成访问控制规则

[0242] 图10是根据一个实施例的图示生成授权多个被管理的服务器130之间的通信的访问控制规则的方法1000的流程图。其他实施例可以以不同的顺序执行步骤并且可以包括不同和/或附加的步骤。另外，可以通过除图1中所示的那些的实体执行步骤中的一些或者全部步骤。

[0243] 在步骤1010中，获得描述多个被管理的服务器130之间的过往通信的通信信息。例如，通信信息描述在每对被管理的服务器130之间传送的日数据量的通信信息。通过例如上下文信息采集模块910执行步骤1010。

[0244] 在步骤1020中，通过基于所获得的通信信息对多个被管理的服务器130进行分组，来从多个被管理的服务器130标识被管理的服务器130的子集。例如，通过向具有表示被管理的服务器130的节点和具有反映被管理的服务器130对之间传送的日数据量的值的边缘的图形应用k-means聚类算法确定子集。通过例如被管理的服务器分组模块920执行步骤1020。

[0245] 在步骤1030中，分组级标签集被确定为与被管理的服务器130的子集相关联。例如，标签集包括应用标签(例如，<应用，人力资源>)、位置标签(例如，<位置，北美>)和环境标签(例如，<环境，生产>)。通过例如标签引擎930执行步骤1030。

[0246] 在步骤1040中，针对被管理的服务器的子集中的被管理的服务器130确定角色标签。被管理的服务器130与一个角色标签相关联。例如，基于在相应的被管理的服务器130上执行的过程，第一被管理的服务器130与具有“数据库”值的角色标签相关联，并且第二被管理的服务器130与具有“网络服务器”值的角色标签相关联。通过例如标签引擎930执行步骤1040。

[0247] 在步骤1050中，基于分组级标签集和角色标签，生成授权被管理的服务器130的子集的第一被管理的服务器130与第二被管理的服务器130之间的通信的访问控制规则。第二服务器130可以是被管理的服务器130的子集的一部分或者被管理的服务器130的另一子集的一部分。例如，访问控制规则的PB部分指示第一被管理的服务器130是“sshd”(ssh守护进程)服务的提供者，并且访问控制规则的UB部分指示第二被管理的服务器130是“sshd”服务的消费者。通过例如流处理模块940执行步骤1050。

[0248] 在步骤1060中，访问控制规则被存储为访问控制规则的集合335的一部分。通过例如流处理模块940执行步骤1060。

[0249] 在步骤1070中，方法结束。然后，策略引擎模块340处理管理域范围管理策略330的改变。处理导致将访问控制规则转译为用于实现访问控制规则的一个或多个相关被管理的服务器130的功能级指令并且将功能级指令发送给相关被管理的服务器130。

[0250] 备选地或者附加地，为了生成访问控制规则，本文所描述的方法可以被用于利用不同的规则函数创建其他规则的创建作为管理域范围管理策略330的一部分。一些规则指定服务的提供者和服务的消费者二者。一个这样的示例规则具有指定待与用于服务的通信一起使用的协议、加密或者信道的安全连接性功能。对于这些规则而言，全局管理器120获得目标规则并且标识描述提供者的标签集(例如，包括角色标签和/或分组级标签)和描述消费者的标签集。全局管理器120然后生成附加规则(或者扩大现有规则)，其适用于具有相应的标签集对的提供者-消费者对，其匹配一对所标识的标签集。附加(或者扩大的)规则适用于相同服务并且具有与目标规则相同的函数简档(例如，加密协议、通信协议类型)。

[0251] 一些规则指定仅服务的提供者或者服务的消费者。指定消费者或者提供者之一的示例规则可以具有调节存储数据加密、磁盘使用、外围使用或者处理器使用的规则函数。对于这些规则而言，全局管理器120获得目标规则并且标识与提供者或者消费者相对应的标签集。对于指定提供者的规则而言，全局管理器120生成附加规则(或者扩大现有规则)，其适用于具有匹配所标识的标签集的标签集的服务的提供者。对于指定消费者的规则而言，全局管理器120生成附加规则(或者扩大现有规则)，其适用于具有匹配所标识的标签集的标签集的服务的消费者。附加(或者扩大的)规则适用于相同服务并且具有与目标规则相同的函数简档(例如，加密协议、资源使用限制)。

[0252] 不管由被管理的服务器130所提供或者所消费的服务如何，一些规则影响被管理的服务器130。示例规则调节哪些过程可以执行在被管理的服务器130上、通用磁盘加密设置或者何时获得用于安全性分析的网络分组。全局管理器120获得目标规则，标识来自目标规则的标签集并且生成(或者扩大)适用于具有匹配所标识的标签集的标签集的附加被管理的服务器130的规则。附加(或者扩大的)规则具有与目标规则相同的函数简档。除所生成的规则不指定服务之外，该过程与之前所描述的过程类似。

[0253] 在一些实施例中，流处理模块940基于与被用于其他规则(例如，访问控制规则)不同的标签的种类，生成规则。这样的规则影响由被管理的服务器130进行提供或者进行使用的服务并且可以基于用于被管理的服务器的一个或多个备选或者附加标签而被生成。标签引擎930可以确定适用于被管理的服务器130的过程的多个过程特定角色标签。在一个实施例中，流处理模块940基于用于服务的提供者或者消费者的备选角色标签来生成规则。备选角色标签是与由被管理的服务器130用于提供或者消费由规则所指定的服务的一个或多个过程相关联的过程特定角色标签。

[0254] 处理来自被管理的服务器的警报

[0255] 图11是根据一个实施例的图示处理来自实现一个或多个访问控制规则的被管理的服务器130的警报的方法1100的流程图。其他实施例可以以不同的顺序执行步骤并且可以包括不同和/或附加的步骤。另外，可以通过除图1中所示的那些的实体执行步骤中的一些或者全部步骤。

[0256] 在步骤1110中，从第一被管理的服务器130获得警报，所述第一被管理的服务器130被配置为响应于与第二被管理的服务器130通信而生成警报。响应于第一被管理的服务器130确定由第一被管理的服务器所实现的一个或多个访问控制规则没有授权第一被管理的服务器130与第二被管理的服务器130之间的通信，生成警报。

[0257] 在步骤1120中，获得与第一被管理的服务器130、第二被管理的服务器130和警报中的至少一个有关的上下文信息。例如，上下文信息是指示在第二被管理的服务器130处、第一被管理的服务器130已经请求连接到的端口的数目的管理域信息，其中，第二被管理的服务器130不具有监听端口的任何过程。作为另一示例，上下文信息是指示第一被管理的服务器130与第二被管理的服务器130之间的通信的频率的通信信息。

[0258] 在步骤130中，与警报相对应的通信被分类为合法或者恶意的。例如，响应于管理域信息中所标识的端口的数目超过端口的阈值数目，通信被分类为恶意的。作为另一示例，响应于通信的频率没有超过与服务相关联的通信的期望频率的阈值差，通信被分类为合法的。

[0259] 在步骤1140中，做出通信是否被分类为合法的确定。如果通信是合法的，则方法1100转到步骤1150。如果通信不是合法的，则方法1100转到步骤1170。

[0260] 在步骤1150中，生成访问控制规则，其许可第一被管理的服务器130与第二被管理的服务器130之间的通信。

[0261] 在步骤1160中，访问控制规则被存储为访问控制规则的集合335的一部分。

[0262] 在步骤1170中，向管理员通知关于警报。向管理员通知关于警报可以包括：如果通信被分类为合法的，则请求管理员批准用于授权与警报相对应的通信所生成的访问控制规则。通知管理员还可以包括：如果通信被分类为恶意的，则促进管理员隔离第一被管理的服务器130或者第二被管理的服务器130。

[0263] 在步骤1180中，方法结束。稍后，策略引擎模块340处理管理域范围管理策略330的改变。处理导致将访问控制规则转换为用于实现访问控制规则的一个或多个相关被管理的服务器130的功能级指令，并且导致将功能级指令发送给相关被管理的服务器130。

[0264] 上文描述被包括为图示某些实施例的操作并且不旨在限制本发明的范围。本发明的范围将仅由所附权利要求限制。根据上文讨论，还将由本发明的精神和范围包含的许多变型对于相关领域的技术人员将是显而易见的。

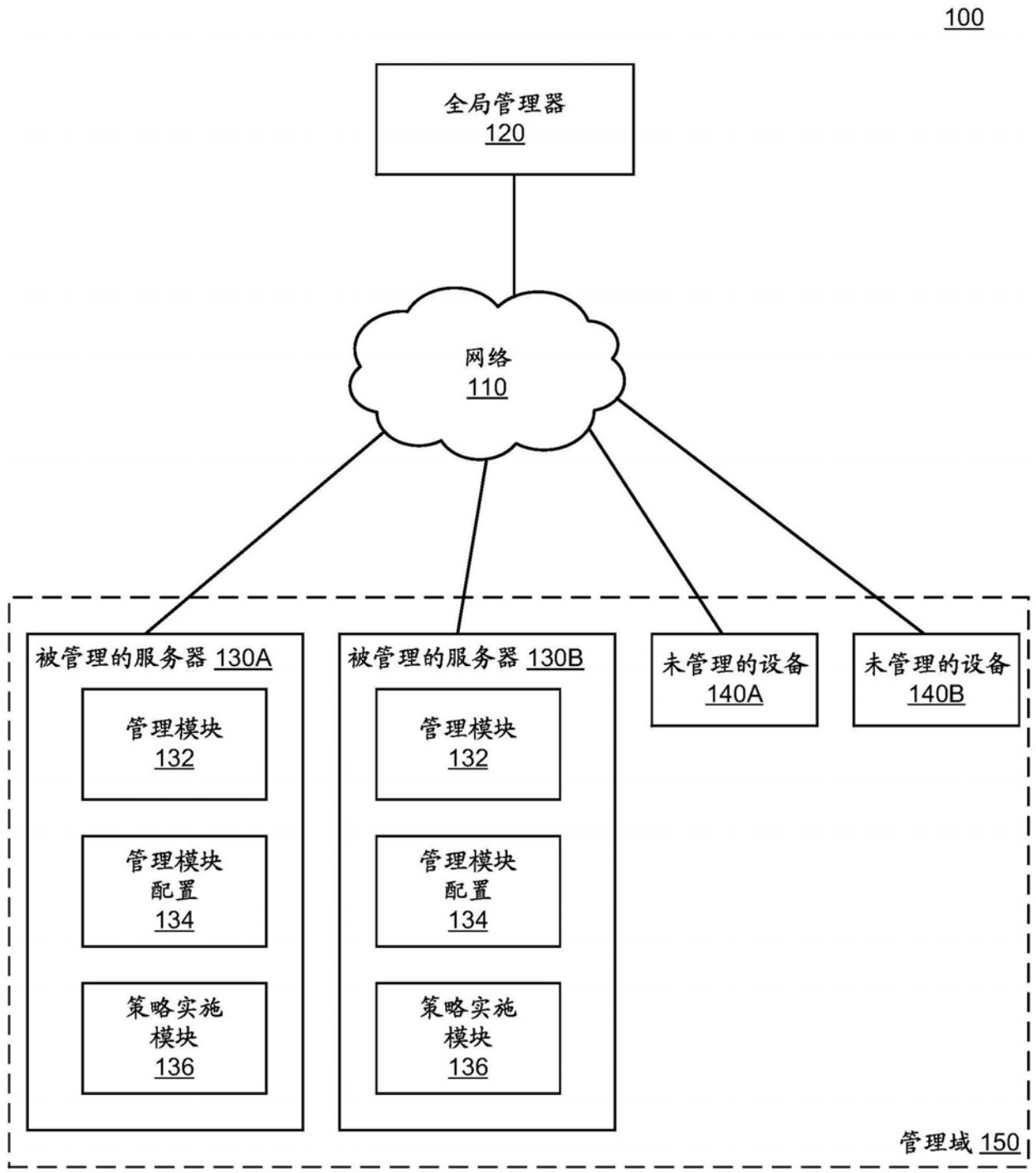

100
全局管理器
120
网络
110
被管理的服务器 130A
管理模块
132
管理模块
配置
134
策略实施
模块
136
被管理的服务器 130B
管理模块
132
管理模块
配置
134
策略实施
模块
136
未管理的设备
140A
未管理的设备
140B
管理域 150

图1

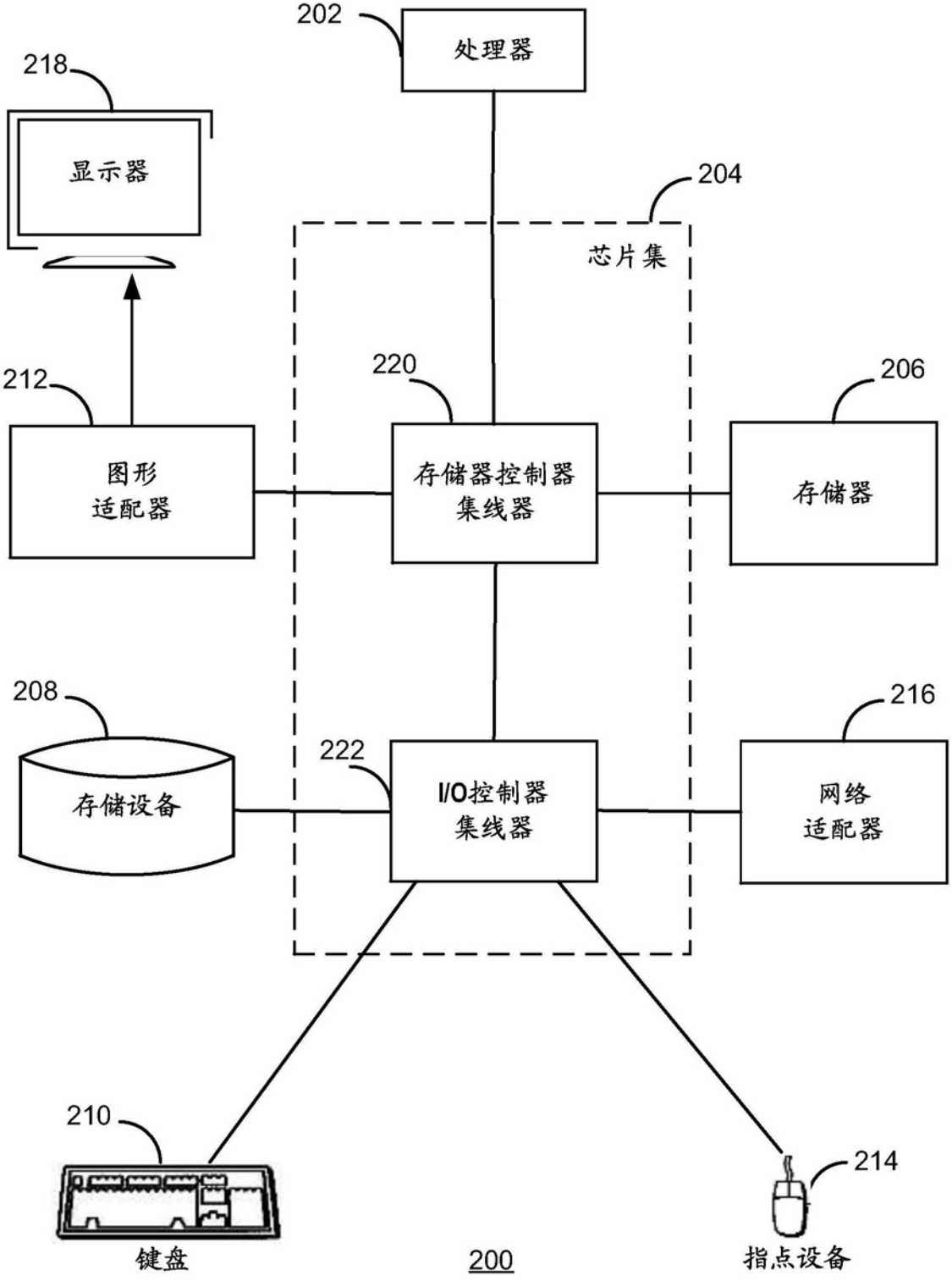

202
处理器
218
显示器
204
芯片集
212
220
206
图形
适配器
存储器控制器
集线器
存储器
208
216
222
存储设备
I/O控制器
集线器
网络
适配器
210
214
键盘
200
指点设备

图2


全局管理器 120
贮存库 300
管理域状态 320
管理域范围管理策略 330
访问控制规则的集合 335
处理服务器 310
策略引擎模块 340
相关规则模块 350
函数级指令生成模块 360
动作者枚举模块 370
相关动作者模块 380
管理域状态更新模块 385
访问控制规则创建模块 390

图3

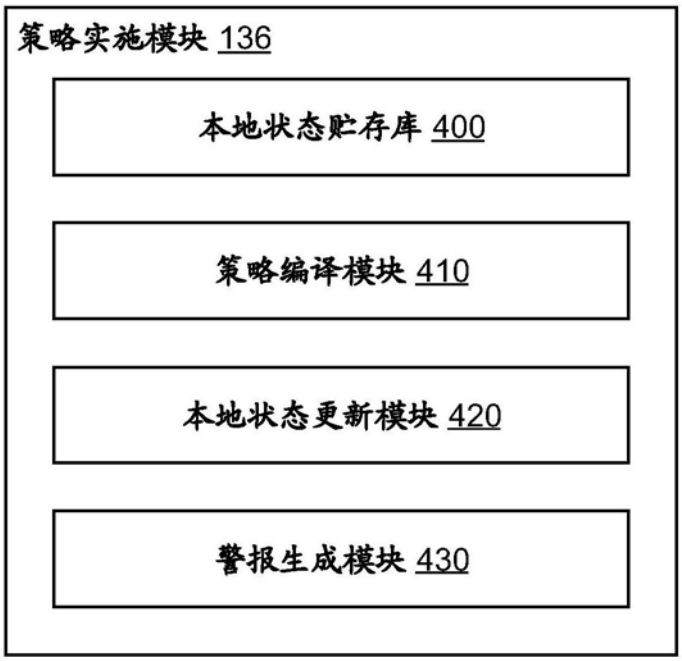


图4

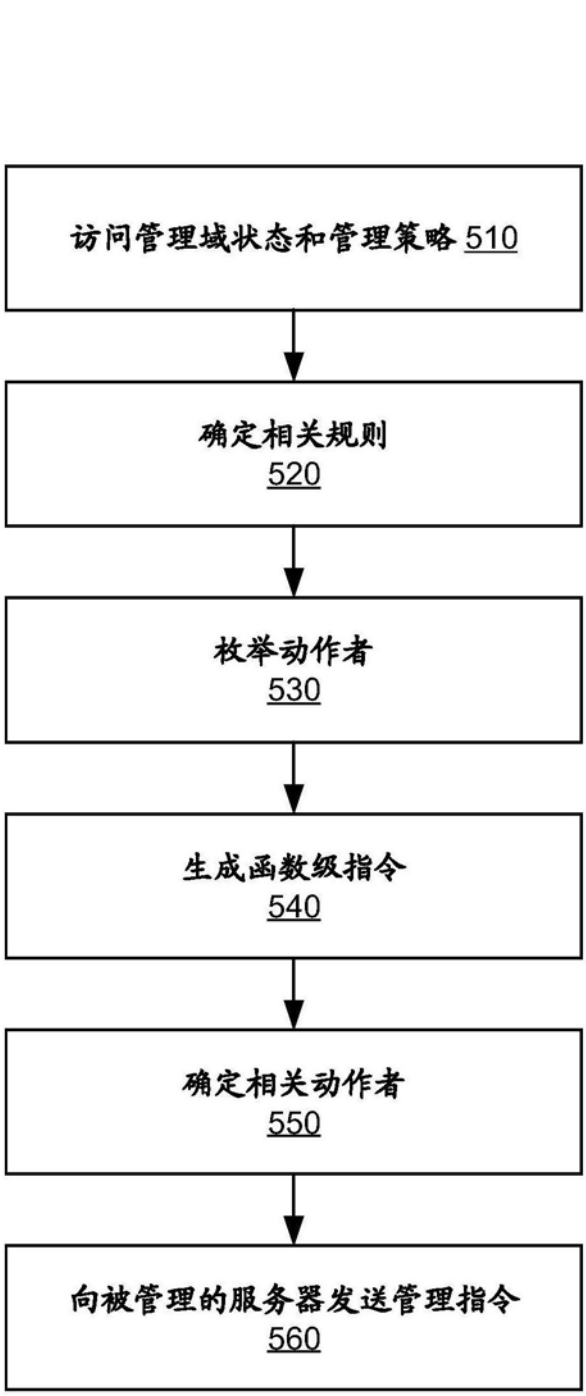

500
访问管理域状态和管理策略 510
确定相关规则
520
枚举动作者
530
生成函数级指令
540
确定相关动作者
550
向被管理的服务器发送管理指令
560

图5

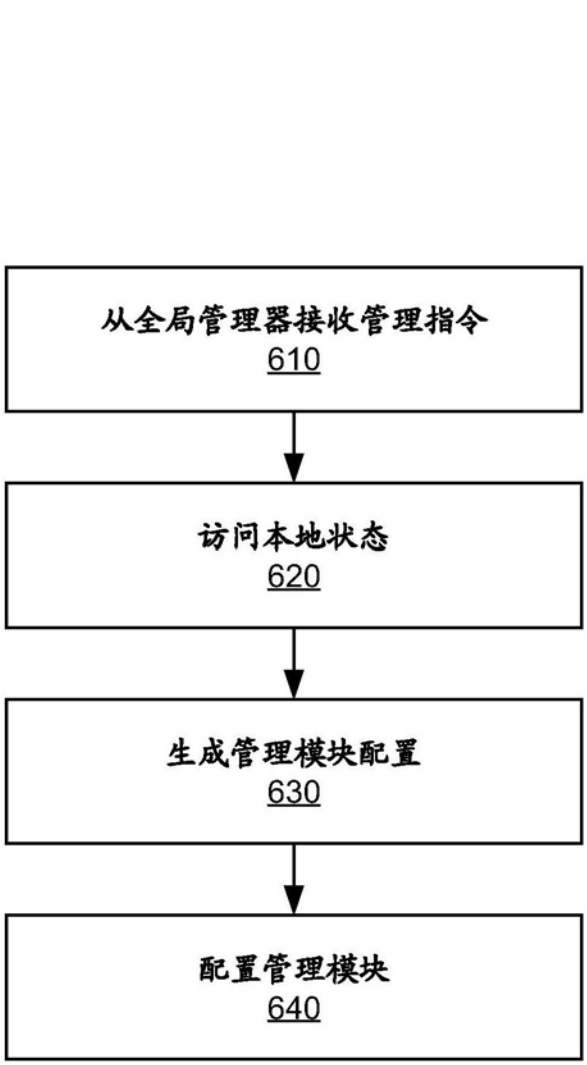


图6

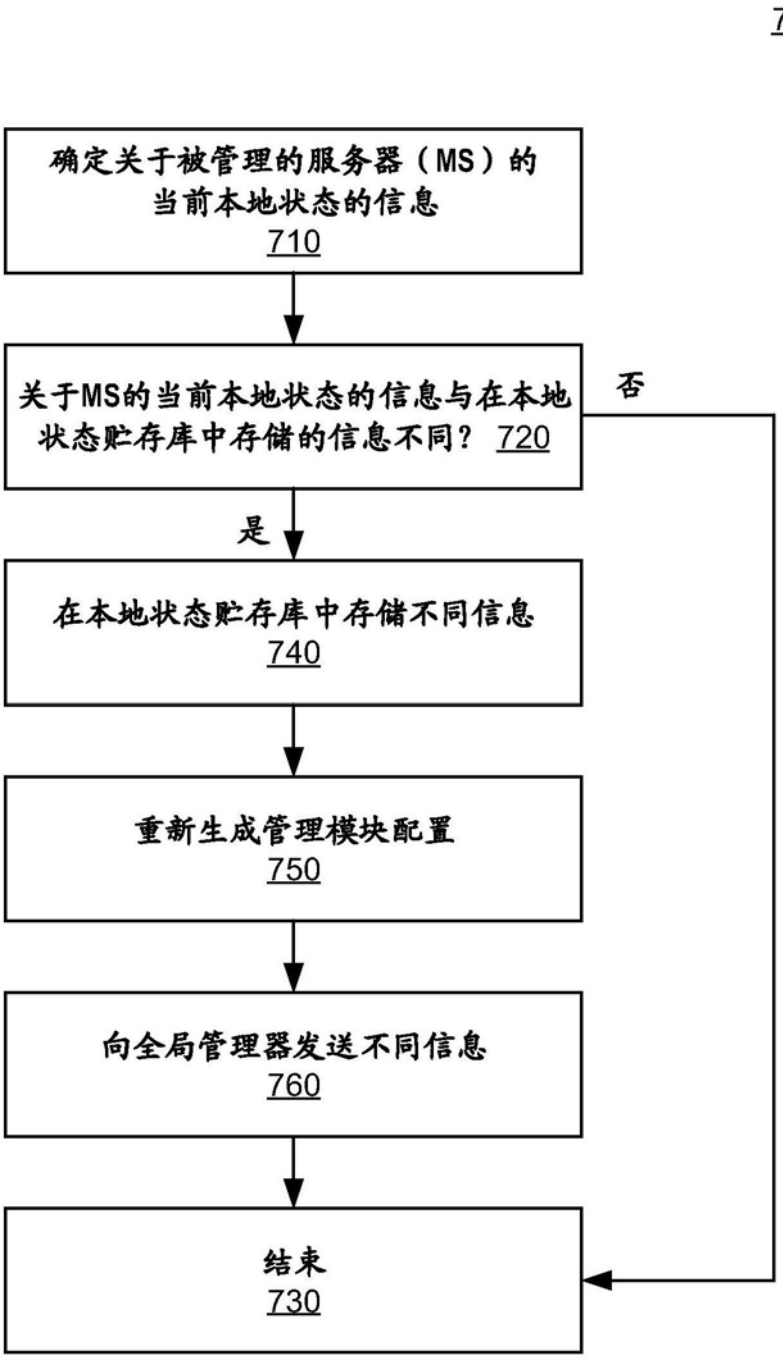

700
确定关于被管理的服务器（MS）的当前本地状态的信息
710
关于MS的当前本地状态的信息与在本地状态贮存库中存储的信息不同？ 720
否
是
在本地状态贮存库中存储不同信息
740
重新生成管理模块配置
750
向全局管理器发送不同信息
760
结束
730

图7

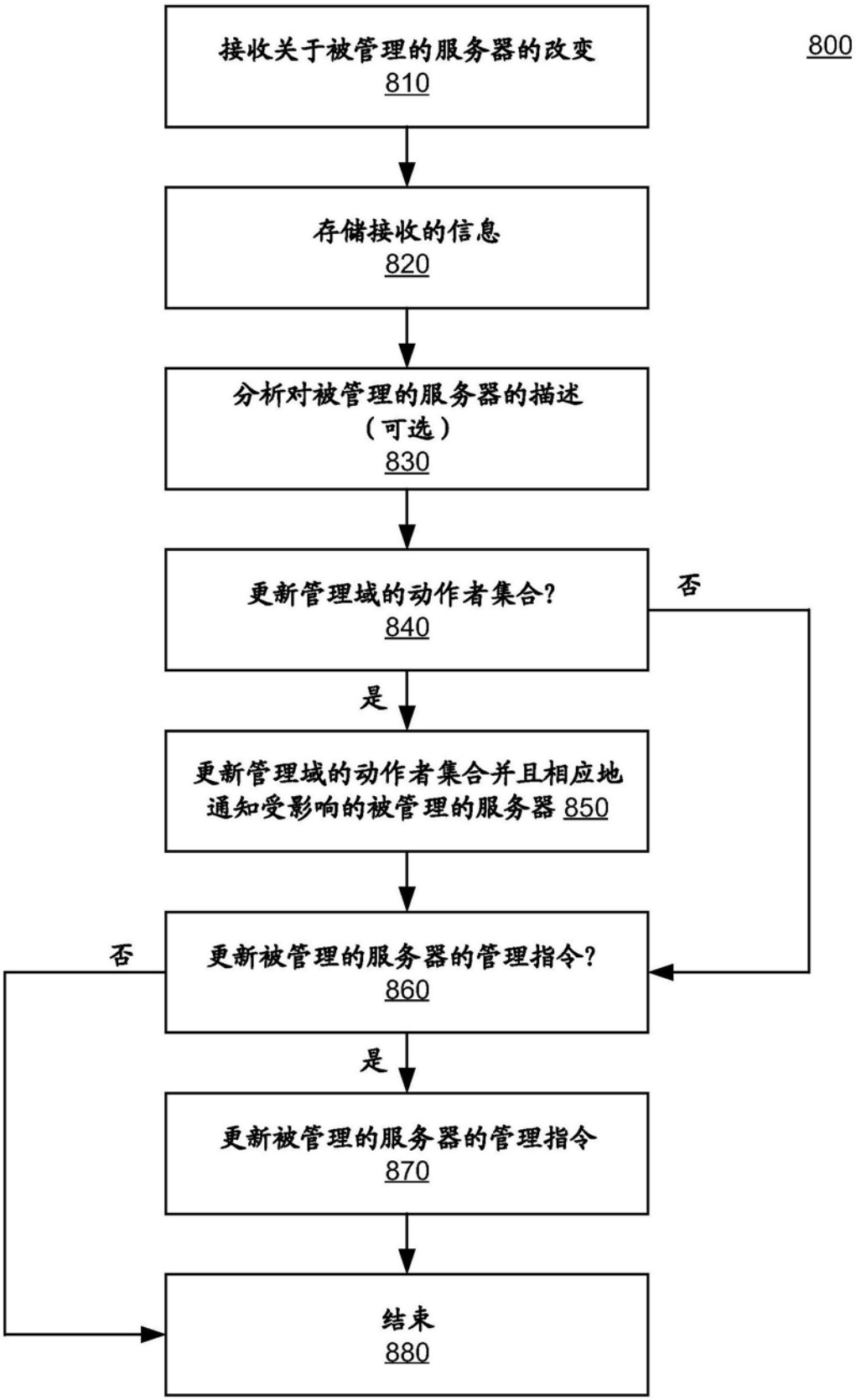

800
接收关于被管理的服务器的改变
810
存储接收的信息
820
分析对被管理的服务器的描述
（可选）
830
更新管理域的动作者集合?
840
否
是
更新管理域的动作者集合并且相应地
通知受影响的被管理的服务器 850
否
更新被管理的服务器的管理指令?
860
是
更新被管理的服务器的管理指令
870
结束
880

图8


访问控制规则创建模块 390
上下文信息采集模块 910
被管理的服务器分组模块 920
标签引擎 930
流处理模块 940
警报处理模块 950
访问控制规则创建接口 960

图9

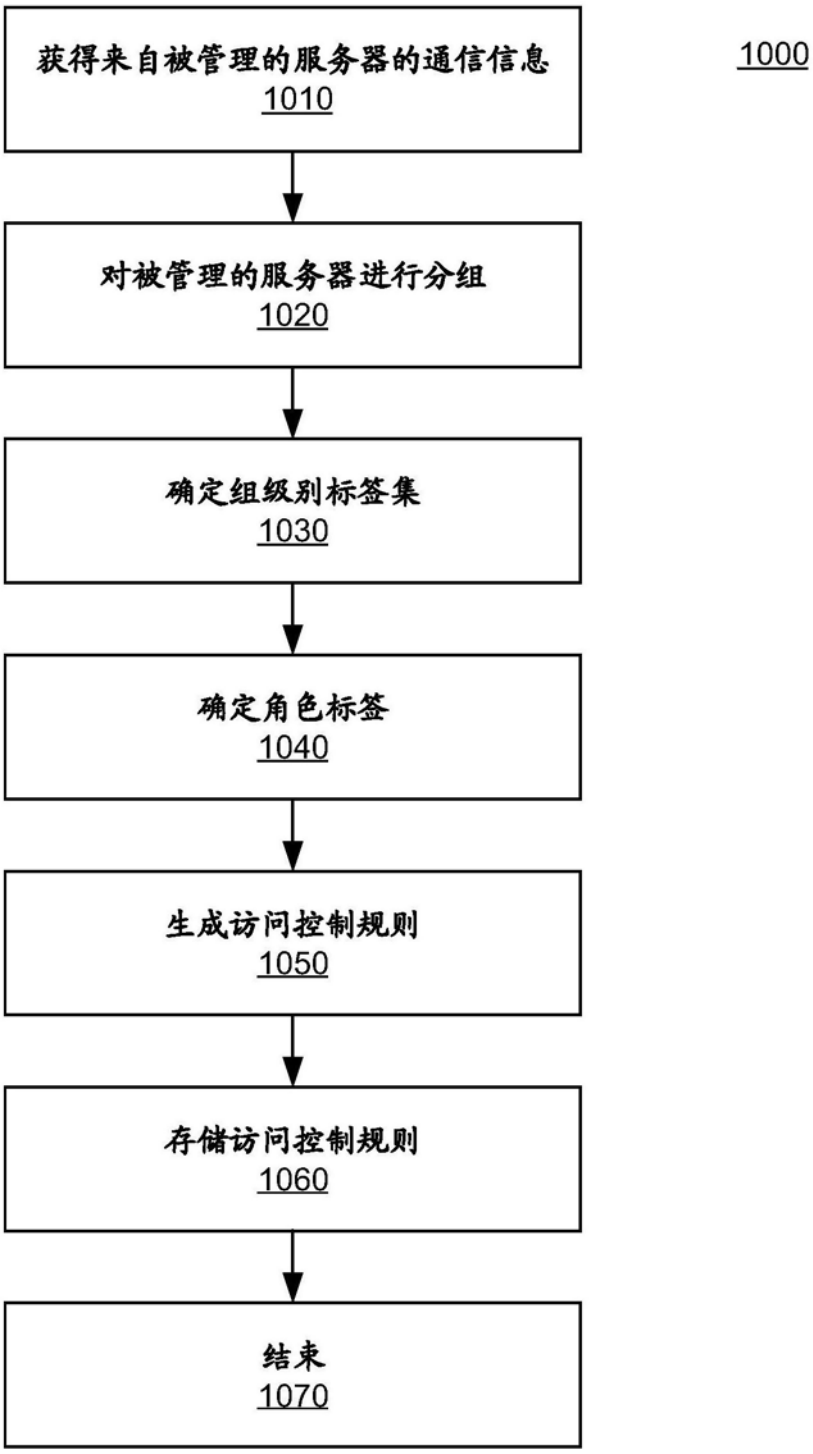

获得来自被管理的服务器的通信信息
1010
1000
对被管理的服务器进行分组
1020
确定组级别标签集
1030
确定角色标签
1040
生成访问控制规则
1050
存储访问控制规则
1060
结束
1070

图10

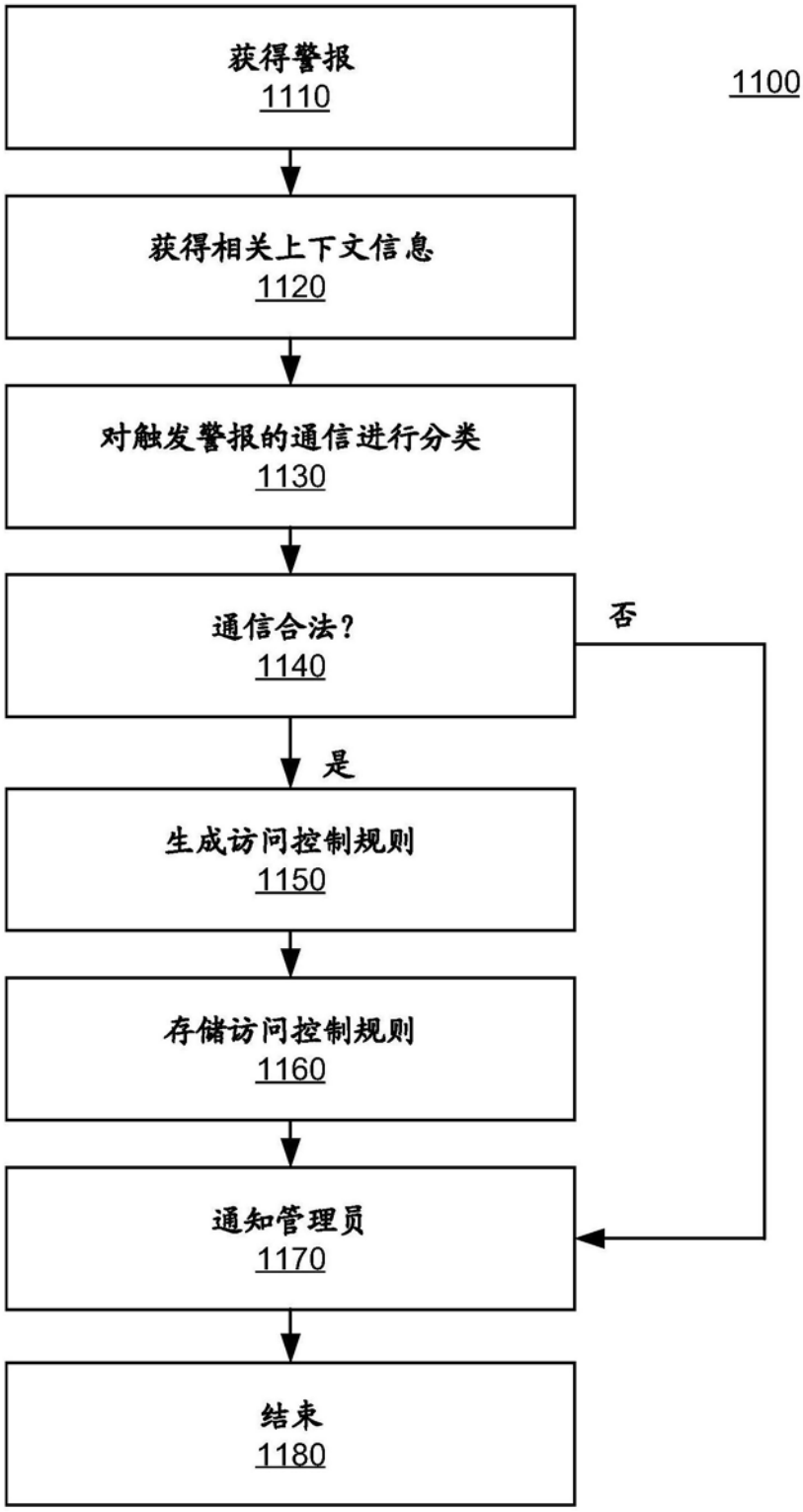

获得警报
1110
1100
获得相关上下文信息
1120
对触发警报的通信进行分类
1130
通信合法?
1140
否
是
生成访问控制规则
1150
存储访问控制规则
1160
通知管理员
1170
结束
1180

图11