(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108292234 A
(43)申请公布日 2018.07.17

(21)申请号 201680068162.6

(22)申请日 2016.11.22

(30)优先权数据
14/979,134 2015.12.22 US

(85)PCT国际申请进入国家阶段日
2018.05.22

(86)PCT国际申请的申请数据
PCT/US2016/063334 2016.11.22

(87)PCT国际申请的公布数据
WO2017/112256 EN 2017.06.29

(71)申请人 英特尔公司
地址 美国加利福尼亚

(72)发明人 S·T·巴勒莫 H·K·塔德帕利
R·N·帕特尔 A·J·赫德里奇
E·韦尔普兰科

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 9/455(2006.01)

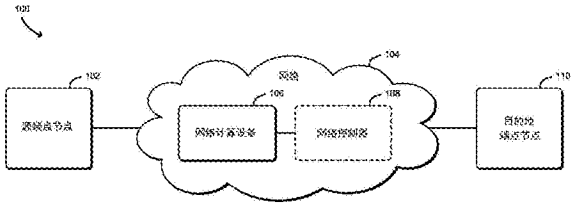
权利要求书3页 说明书12页 附图5页

(54)发明名称

用于实施对虚拟机的网络访问控制的技术

(57)摘要

用于实施虚拟机网络访问控制的技术包括网络计算设备，该网络计算设备包括多个虚拟机。网络计算设备被配置为从分配给网络计算设备的请求虚拟机的虚拟功能接收访问请求。网络计算设备另外被配置为确定分配给请求机器的第一特权级别和分配给目的地虚拟机的第二特权级别，并且基于对第一特权级别与第二特权级别的比较来确定请求虚拟机是否被授权访问目的地虚拟机。在确定请求虚拟机被授权访问目的地虚拟机后，网络计算设备另外被配置为允许请求虚拟机访问目的地虚拟机。本文描述了其他实施例。



CN 108292234 A

1.一种用于实施虚拟机网络访问控制的网络计算设备,所述网络计算设备包括:

一个或多个处理器;以及

一个或多个数据存储设备,其中存储有多个指令,所述多个指令当由所述一个或多个处理器执行时使所述网络计算设备用于:

从分配给请求虚拟机的虚拟功能接收访问请求,其中,所述请求虚拟机是在所述网络计算设备上初始化的多个虚拟机中的一个,其中,所述访问请求包括对目的地虚拟机的至少一部分进行访问的请求,其中,所述目的地虚拟机是在所述网络计算设备上初始化的所述多个虚拟机中的一个;

确定分配给所述请求机器的第一特权级别和分配给所述目的地虚拟机的第二特权级别;

基于对所述第一特权级别与所述第二特权级别的比较来确定所述请求虚拟机是否被授权对所述目的地虚拟机进行访问;以及

响应于确定所述请求虚拟机被授权对所述目的地虚拟机进行访问,允许所述请求虚拟机对所述目的地虚拟机进行访问。

2.根据权利要求1所述的网络计算设备,其中,所述多个指令还使所述网络计算设备用于:

对所述多个虚拟机中的每个虚拟机进行初始化;以及

向所述多个虚拟机中的每个虚拟机分配特权级别,其中,所述特权级别包括特许级别或非特许级别中的一个。

3.根据权利要求2所述的网络计算设备,其中,所述多个指令还使所述网络计算设备用于:

针对所述多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化;以及

向所述多个虚拟机中的对应的一个虚拟机分配所述一个或多个虚拟功能中的每个虚拟功能。

4.根据权利要求2所述的网络计算设备,其中,向所述多个虚拟机中的每个虚拟机分配所述特权级别包括:向所述请求虚拟机分配所述第一特权级别,并且向所述目的地虚拟机分配所述第二特权级别。

5.根据权利要求4所述的网络计算设备,其中,允许所述请求虚拟机对所述目的地虚拟机进行访问包括:在确定所述第一特权级别对应于所述特许级别并且所述第二特权级别对应于所述特许级别之后,允许进行访问。

6.根据权利要求4所述的网络计算设备,其中,允许所述请求虚拟机对所述目的地虚拟机进行访问包括:在确定所述第一特权级别对应于所述特许级别并且所述第二特权级别对应于所述非特许级别之后,允许进行访问。

7.根据权利要求2所述的网络计算设备,其中,所述多个指令还使所述网络计算设备用于:响应于确定所述请求虚拟机未被授权对所述目的地虚拟机进行访问,拒绝所述请求虚拟机对所述目的地虚拟机进行访问。

8.根据权利要求7所述的网络计算设备,其中,向所述多个虚拟机中的每个虚拟机分配所述特权级别包括:向所述请求虚拟机分配所述第一特权级别,并且向所述目的地虚拟机分配所述第二特权级别,并且其中,拒绝所述请求虚拟机对所述目的地虚拟机进行访问包

括:在确定所述第一特权级别对应于所述非特许级别并且所述第二特权级别对应于所述特许级别之后,拒绝进行访问。

9.根据权利要求1所述的网络计算设备,其中,允许所述请求虚拟机对所述目的地虚拟机进行访问包括:允许访问限于所述目的地虚拟机的与所述访问请求相对应的所述至少一部分。

10.根据权利要求1所述的网络计算设备,其中,所述第一虚拟机和所述目的地虚拟机是相同的虚拟机。

11.根据权利要求1所述的网络计算设备,其中,所述第一虚拟机和所述目的地虚拟机是不同的虚拟机。

12.根据权利要求1所述的网络计算设备,其中,所述访问请求包括VM到VM访问请求或VM到网络访问请求中的一个。

13.一种用于实施虚拟机网络访问控制的方法,所述方法包括:

由网络计算设备从分配给请求虚拟机的虚拟功能接收访问请求,其中,所述请求虚拟机是在所述网络计算设备上初始化的多个虚拟机中的一个,其中,所述访问请求包括对目的地虚拟机的至少一部分进行访问的请求,其中,所述目的地虚拟机是在所述网络计算设备上初始化的所述多个虚拟机中的一个;

由所述网络计算设备确定分配给所述请求机器的第一特权级别和分配给所述目的地虚拟机的第二特权级别;

由所述网络计算设备基于对所述第一特权级别与所述第二特权级别的比较来确定所述请求虚拟机是否被授权对所述目的地虚拟机进行访问;以及

由所述网络计算设备并且响应于确定所述请求虚拟机被授权对所述目的地虚拟机进行访问,允许所述请求虚拟机对所述目的地虚拟机进行访问。

14.根据权利要求13所述的方法,还包括:

由所述网络计算设备对所述多个虚拟机中的每个虚拟机进行初始化;以及

由所述网络计算设备向所述多个虚拟机中的每个虚拟机分配特权级别,其中,所述特权级别包括特许级别或非特许级别中的一个。

15.根据权利要求14所述的方法,还包括:

由所述网络计算设备针对所述多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化;以及

由所述网络计算设备向所述多个虚拟机中的对应的一个虚拟机分配所述一个或多个虚拟功能中的每个虚拟功能。

16.根据权利要求14所述的方法,其中,向所述多个虚拟机中的每个虚拟机分配所述特权级别包括:向所述请求虚拟机分配所述第一特权级别,并且向所述目的地虚拟机分配所述第二特权级别。

17.根据权利要求16所述的方法,其中,允许所述请求虚拟机对所述目的地虚拟机进行访问包括:在确定所述第一特权级别对应于所述特许级别并且所述第二特权级别对应于所述特许级别,或者确定所述第一特权级别对应于所述特许级别并且所述第二特权级别对应于所述非特许级别之后,允许进行访问。

18.根据权利要求14所述的方法,还包括:由所述网络计算设备并且响应于确定所述请

求虚拟机未被授权对所述目的地虚拟机进行访问，拒绝所述请求虚拟机对所述目的地虚拟机进行访问。

19.根据权利要求18所述的方法，其中，向所述多个虚拟机中的每个虚拟机分配所述特权级别包括：向所述请求虚拟机分配所述第一特权级别，并且向所述目的地虚拟机分配所述第二特权级别，并且其中，拒绝所述请求虚拟机对所述目的地虚拟机进行访问包括：在确定所述第一特权级别对应于所述非特许级别并且所述第二特权级别对应于所述特许级别之后，拒绝进行访问。

20.根据权利要求13所述的方法，其中，允许所述请求虚拟机对所述目的地虚拟机进行访问包括：允许访问限于所述目的地虚拟机的与所述访问请求相对应的所述至少一部分。

21.根据权利要求13所述的方法，其中，所述第一虚拟机和所述目的地虚拟机是相同的虚拟机。

22.根据权利要求13所述的方法，其中，所述第一虚拟机和所述目的地虚拟机是不同的虚拟机。

23.根据权利要求13所述的方法，其中，接收所述访问请求包括接收VM到VM访问请求或VM到网络访问请求中的一个。

24.一种网络计算设备，包括：

处理器；以及

存储器，其中存储有多个指令，所述多个指令当由所述处理器执行时使所述网络计算设备执行根据权利要求13-23中的任一项所述的方法。

25.一种或多种机器可读存储介质，包括存储在其上的多个指令，所述多个指令响应于被执行而使得网络计算设备执行根据权利要求13-23中的任一项所述的方法。

用于实施对虚拟机的网络访问控制的技术

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年12月22日提交的题为“TECHNOLOGIES FOR ENFORCING NETWORK ACCESS CONTROL OF VIRTUAL MACHINES”的美国实用专利申请第14/979,134号的优先权。

背景技术

[0003] 网络运营商和通信服务提供商典型地依赖由大量网络计算设备(例如,服务器、交换机、路由器等)组成的复杂的大规模数据中心来处理通过数据中心的网络业务。为了提供可扩展性以满足网络业务处理需求并降低运营成本,特定的数据中心操作典型地在网络计算设备的虚拟化环境中的容器或虚拟机(VM)内运行。为了协调支持VM在其上运行的网络计算设备的物理硬件与VM的虚拟环境的功能,VM典型地要求公开虚拟功能的虚拟化实例。例如,诸如快速PCI(PCIe)虚拟功能之类的虚拟功能可以提供用于在VM与网络计算设备的网络接口控制器(NIC)之间直接传输数据的机制。为此,网络计算设备通常依赖虚拟功能驱动器来管理虚拟功能(例如,读取/写入虚拟功能的配置空间)。

附图说明

[0004] 本文描述的概念在附图中通过示例的方式而非通过限制的方式示出。为了说明的简单和清楚起见,图中所示的元件不一定按比例绘制。在认为合适的地方,附图标记在图中重复以指示对应或类似的元件。

[0005] 图1是用于由网络计算设备实施对虚拟机的网络访问控制的系统的至少一个实施例的简化框图;

[0006] 图2是图1的系统中的网络计算设备的至少一个实施例的简化框图;

[0007] 图3是可以由图2的网络计算设备建立的环境的至少一个实施例的简化框图;

[0008] 图4是可以由图2的网络计算设备建立的环境的另一实施例的简化框图;

[0009] 图5是可以由图2的网络计算设备执行的用于向初始化的虚拟机分配特权级别的方法的至少一个实施例的简化流程图;以及

[0010] 图6是可以由图2的网络计算设备执行的用于实施对初始化的虚拟机的网络访问控制的方法的至少一个实施例的简化流程图。

具体实施方式

[0011] 虽然本公开的概念易受各种修改和替代形式影响,但是其具体实施例已经在附图中通过示例的方式示出,并且将在本文中详细描述。然而,应理解,不旨在将本公开的概念限制于所公开的特定形式,而是相反,意图是覆盖与本公开和所附权利要求一致的所有修改、等同方案和替代方案。

[0012] 说明书中对“一个实施例”、“实施例”、“说明性实施例”等的引用指示所描述的实施例可以包括特定的特征、结构或特性,但是每个实施例可以一定或可以不一定包括该特

定的特征、结构或特性。此外，这样的短语不一定指代相同的实施例。此外，当结合实施例描述特定的特征、结构或特性时，认为结合其他实施例来实现这样的特征、结构或特性在本领域技术人员的知识内，而无论是否明确描述。另外，应理解，以“A、B和C中的至少一个”的形式在列表中包括的项目可以表示(A)；(B)；(C)；(A和B)；(A和C)；(B和C)；或(A、B和C)。类似地，以“A、B或C中的至少一个”的形式列出的项目可以表示(A)；(B)；(C)；(A和B)；(A和C)；(B和C)；或(A、B和C)。

[0013] 在一些情况下，所公开的实施例可以以硬件、固件、软件或其任何组合来实现。所公开的实施例还可以被实现为由一种或多种暂时性或非暂时性机器可读(例如，计算机可读)存储介质(例如，存储器、数据存储装置等)承载或存储在其上的指令，该指令可以由一个或多个处理器读取和执行。机器可读存储介质可以体现为用于以机器可读的形式存储或传输信息的任何存储设备、机构或其他物理结构(例如，易失性或非易失性存储器、介质盘或其他介质设备)。

[0014] 在附图中，可以以特定的布置和/或排序示出一些结构或方法特征。然而，应理解，可能不要求这种具体的布置和/或排序。相反，在一些实施例中，这些特征可以以与说明性图中所示的不同的方式和/或次序来布置。另外，在特定图中包括结构或方法特征并不意味着暗指在所有实施例中都要求这样的特征，并且在一些实施例中可以不包括这些特征或者可以将这些特征与其他特征组合。

[0015] 现在参考图1，在说明性实施例中，用于实施对虚拟机的网络访问控制的系统100包括源端点节点102，其经由网络104的网络计算设备106通信地耦合到目的地端点节点110。虽然在说明性系统100的网络104中仅示出了单个网络计算设备106，但应理解，网络104可以包括以各种架构配置的多个网络计算设备106。

[0016] 在使用中，网络计算设备106对在网络计算设备106处接收到的网络业务(即，网络分组、消息等)执行各种操作(例如，服务)。应理解，接收到的网络业务可以被丢弃或转发，例如，转发到通信地耦合到网络计算设备106的附加的其他网络计算设备或目的地端点节点110。为了处理网络业务，网络计算设备106被配置为在网络计算设备106处加速多个虚拟机(VM)。因此，网络计算设备106被配置为将网络计算设备106的物理组件的虚拟表示映射到各种VM的虚拟化组件。

[0017] 例如，虚拟网络接口控制器(NIC)可以由网络计算设备106初始化以促进物理NIC(参见例如图2的NIC 212)与虚拟NIC之间的通信。在这样的实施例中，可以实现虚拟机监视器(VMM)(参见例如图4的VMM 418)以向实例化的VM中的每个公开虚拟NIC，使得所有的VM到VM通信都经过单个逻辑实体(即，VMM)。类似地，VMM可以被配置为创建虚拟功能和虚拟功能驱动器以用于分配给VM，以管理物理NIC与虚拟NIC之间的通信。应理解，在一些实施例中，VM中的一个或多个可以在通信地耦合到网络计算设备106的一个或多个其他网络计算设备上产生。

[0018] NIC 212的流引导器能力被配置为将网络业务引导至VM的恰当的虚拟功能(例如，使用由VMM建立的访问控制列表(ACL))；然而，在处理网络业务期间，虚拟功能驱动器易受破坏性网络分组(例如，来自畸形网络分组、无效存储器访问请求、受限存储器区域访问请求、受限硬件访问请求等)进行的操纵的影响，这典型地导致在检测到破坏性网络分组时重置虚拟设备以将虚拟设备的状态清零。

[0019] 因此，为了抢先确定网络业务是否是允许的(例如，在网络计算设备106的另一VM内，通过另一VM到网络计算设备106外部的主机等)，网络计算设备106(即，NIC 212)被配置为实现基于硬件的VM特权级别。为此，如下面进一步详细描述的，在VM初始化时，VMM确定VM是特许的还是非特许的，并且将特权级别(即，特许级别或非特许级别)存储在安全位置，例如，存储在NIC的安全存储器(例如，参见图2的NIC 212的安全存储器214)处的VM网络特权级别表内。换言之，网络计算设备106被配置为控制网络特权而不是VM的执行特权。

[0020] 源端点节点102和/或目的地端点节点110可以体现为能够执行本文描述的功能的任何类型的计算设备或计算机设备，包括但不限于：包括移动硬件(例如，处理器、存储器、存储装置、无线通信电路等)和软件(例如，操作系统)以支持移动架构和便携性的便携式计算设备(例如，智能电话、平板电脑、膝上型计算机、笔记本、可穿戴设备等)、计算机、服务器(例如，独立式、机架安装式、刀片式等)、网络装置(例如，物理或虚拟的)、web装置、分布式计算系统、基于处理器的系统和/或多处理器系统。

[0021] 网络104可以体现为任何类型的有线或无线通信网络，包括无线局域网(WLAN)、无线个域网(WPAN)、蜂窝网络(例如，全球移动通信系统(GSM)、长期演进(LTE)等)、电话网络、数字订户线(DSL)网络、有线网、局域网(LAN)、广域网(WAN)、全球网络(例如，互联网)或其任何组合。应理解，在这样的实施例中，网络104可以用作集中式网络，并且在一些实施例中，网络104可以通信地耦合到另一网络(例如，互联网)。因此，根据需要，网络104可以包括各种其他网络计算设备(例如，虚拟和物理的路由器、交换机、网络集线器、服务器、存储设备、计算设备等)，以促进源端点节点102与目的地端点节点110之间的通信，这些设备未示出以便保持描述的清楚。

[0022] 网络计算设备106可以体现为能够执行本文描述的功能的任何类型的网络业务处理设备，例如但不限于服务器(例如，独立式、机架安装式、刀片式等)、网络装置(例如，物理或虚拟的)、交换机(例如，机架安装式、独立式、完全管理的、部分管理的、全双工和/或半双工通信模式使能的等)、路由器、web装置、分布式计算系统、基于处理器的系统和/或多处理器系统。

[0023] 如图2所示，说明性网络计算设备106包括处理器202、输入/输出(I/O)子系统204、存储器206、数据存储设备208和通信电路210。当然，在其他实施例中，网络计算设备106可以包括其他或者附加的组件，例如，在计算设备中常见地发现的组件。另外，在一些实施例中，说明性组件中的一个或多个可以并入另一组件或以其他方式形成另一组件的一部分。例如，在一些实施例中，存储器206或其部分可以并入处理器202。此外，在一些实施例中，可以从网络计算设备106中省略说明性组件中的一个或多个。

[0024] 处理器202可以体现为能够执行本文描述的功能的任何类型的处理器。例如，处理器202可以体现为单核或多核处理器、数字信号处理器、微控制器或者其他处理器或处理/控制电路。类似地，存储器206可以体现为能够执行本文描述的功能的任何类型的易失性或非易失性存储器或数据存储装置。在操作中，存储器206可以存储在网络计算设备106的操作期间使用的各种数据和软件，例如，操作系统、应用、程序、库和驱动程序。

[0025] 存储器206经由I/O子系统204通信地耦合到处理器202，该I/O子系统204可以体现为促进与处理器202、存储器206以及网络计算设备106的其他组件的输入/输出操作的电路和/或组件。例如，I/O子系统204可以体现为或以其他方式包括存储器控制器中心、输入/输

出控制中心、固件设备、通信链路(即,点对点链路、总线链路、电线、电缆、光导、印刷电路板迹线等)和/或促进输入/输出操作的其他组件和子系统。在一些实施例中,I/O子系统204可以形成片上系统(SoC)的一部分并且与处理器202、存储器206以及网络计算设备106的其他组件一起并入单个集成电路芯片。

[0026] 数据存储设备208可以体现为被配置用于短期或长期存储数据的任何类型的设备或多个设备,例如,存储器设备和电路、存储器卡、硬盘驱动器、固态驱动器或其他数据存储设备。应理解,数据存储设备208和/或存储器206(例如,计算机可读存储介质)可以存储如本文描述的各种数据,包括操作系统、应用、程序、库、驱动程序、指令等,其能够由网络计算设备106的处理器(例如,处理器202)执行。

[0027] 通信电路210可以体现为能够实现通过网络(例如,网络104)在网络计算设备106与其他计算设备(例如,源端点节点102、目的地端点节点110、另一网络计算设备等)之间进行通信的任何通信电路、设备或其集合。通信电路210可以被配置为使用任何一种或多种通信技术(例如,无线或有线通信技术)和相关联的协议(例如,以太网、Bluethooth®、Wi-Fi®、WiMAX、LTE、5G等)来实现这种通信。

[0028] 说明性通信电路210包括NIC 212。NIC 212可以体现为可以由网络计算设备106使用的一个或多个插件、子卡、网络接口卡、控制器芯片、芯片组或其他设备。例如,在一些实施例中,NIC 212可以与处理器202集成,体现为通过扩展总线(例如,快速PCI)耦合到I/O子系统204的扩展卡,作为包括一个或多个处理器的SoC的一部分,或包括在也包含一个或多个处理器的多芯片封装上。另外或替代地,在一些实施例中,NIC 212的功能可以以板级别、插口级别、芯片级别和/或其他级别集成到网络计算设备106的一个或多个组件中。

[0029] 说明性NIC 212包括安全存储器214。NIC 212的安全存储器214可以体现为被配置为安全地存储位于NIC 212本地的数据的任何类型的存储器。应理解,在一些实施例中,NIC 212还可以包括位于NIC 212本地的本地处理器(未示出)。在这样的实施例中,NIC 212的本地处理器能够执行可以被卸载到NIC 212的功能(例如,复制、网络分组处理等)。

[0030] 再次参考图1,说明性网络104可以附加地包括通信地耦合到网络计算设备106的网络控制器108。网络控制器108可以体现为能够引导网络分组流并管理网络计算设备106的策略并且执行本文描述的功能的任何类型的设备、硬件、软件和/或固件,例如但不限于服务器(例如,独立式、机架安装式、刀片式等)、网络装置(例如,物理或虚拟的)、交换机(例如,机架安装式、独立式、完全管理的、部分管理的、全双工和/或半双工通信模式使能的等)、路由器、web装置、分布式计算系统、基于处理器的系统和/或多处理器系统。

[0031] 网络控制器108可以被配置为向网络计算设备106提供一个或多个策略(例如,网络策略)或指令。应理解,在一些实施例中,网络控制器108可以被配置为在软件定义的联网(SDN)环境中操作(即,SDN控制器)和/或在网络功能虚拟化(NFV)环境中操作(即,NFV管理器和网络编排器(MANO))。因此,网络控制器108可以包括在网络控制设备或类似的计算设备中常见地发现的设备和组件(例如,处理器、存储器、通信电路和数据存储设备,类似于针对图2的网络计算设备106描述的那些),这些设备和组件为了描述的清楚而未在图1中示出。

[0032] 现在参考图3,在说明性实施例中,网络计算设备106在操作期间建立环境300。说明性环境300包括网络通信模块310、虚拟机管理模块320、数据流管理模块330和虚拟网络

策略实施模块340。环境300的模块、逻辑和其他组件中的每个可以体现为硬件、软件、固件或其组合。例如，环境300的模块、逻辑和其他组件中的每个可以形成处理器202、通信电路210(例如，NIC 212)和/或网络计算设备106的其他硬件组件的一部分或以其他方式由其建立。因此，在一些实施例中，环境300的模块中的一个或多个可以体现为电路或电子设备的集合(例如，网络通信电路310、虚拟机管理电路320、数据流管理电路330、虚拟网络策略实施电路340等)。

[0033] 网络计算设备106的说明性环境300附加地包括网络策略数据302、访问控制数据304和特权级别数据306，其中的每个都可以由网络计算设备106的各种模块和/或子模块访问。应理解，网络计算设备106可以包括在计算设备中常见地发现的其他组件、子组件、子模块、子模块和/或设备，其为了描述的清楚而未在图3中示出。

[0034] 网络通信模块310被配置为促进去往和来自网络计算设备106的、入站和出站网络通信(例如，网络业务、网络分组、网络流等)。为此，网络通信模块310被配置为接收和处理来自其他计算设备(例如，源端点节点102、目的地端点节点110、经由网络104通信地耦合到网络计算设备106的另一网络计算设备等)的网络分组。另外，网络通信模块310被配置为准备网络分组并且将网络分组发送到另一计算设备(例如，源端点节点102、目的地端点节点110、经由网络104通信地耦合到网络计算设备106的另一网络计算设备等)。因此，在一些实施例中，网络通信模块310的功能中的至少一部分功能可以由通信电路210执行，并且更具体地由NIC 212执行。

[0035] 虚拟机管理模块320被配置为管理网络计算设备106的VM以及与其相关联的虚拟功能中的每个(例如，参见图4的VM 400和虚拟功能410)。为此，虚拟机管理模块320被配置为基于待对网络业务执行的各种服务功能(例如，基于与网络分组流相对应的服务功能链的服务功能)来部署(即，加快、执行实例化等)和关闭(即，减慢、从网络移除等)VM。因此，虚拟机管理模块320被配置为管理与相应VM相关联的虚拟功能驱动器中的每个。

[0036] 数据流管理模块330被配置为将传入的网络业务的流引导至适当的虚拟功能。换言之，数据流管理模块330被配置为确定传入的网络业务要被引导用于(即，基于访问请求)的预期目的地(例如，VM)，并将传入的网络业务引导至预期目的地的接口(即，VM的虚拟功能)。然而，在将网络业务引导至预期目的地之前，针对虚拟网络策略来检查访问请求(例如，可以由虚拟网络策略实施模块340执行)。在一些实施例中，虚拟网络策略可以存储在网络策略数据302中。应理解，访问请求可以是VM到VM访问请求、VM到网络访问请求(即，目标为进入或离开另一VM的外部网络业务)等。还应理解，可以由数据流管理模块330执行上面描述的NIC 212的流引导器能力的至少一部分。

[0037] 虚拟网络策略实施模块340被配置为实施网络计算设备106的虚拟网络策略(例如，VM到VM业务策略、外部业务策略等)。因此，虚拟网络策略实施模块340被配置为基于策略信息(例如，与请求起源VM和/或请求目的地VM相关联的特权级别)来做出分组处理决定(例如，是否允许访问请求)。为此，说明性虚拟网络策略实施模块340包括策略表访问模块342、特权级别确定模块344和授权访问确定模块346。

[0038] 策略表访问模块342被配置为访问由VMM建立的访问控制列表(ACL)，其控制VM之间允许何种网络业务。例如，在VM的初始化时，VMM确定该VM是特许的还是非特许的，并将这些信息存储在ACL中。在一些实施例中，这样的信息可以存储在访问控制数据304中。虚拟网

络策略信息可以基于可以包含于网络分组的报头中的、网络分组的标识符，例如，进行网络访问控制请求的VM的介质访问控制(MAC)地址、目标VM的MAC地址。应理解，可以从网络控制器或编排器(例如，网络控制器108)接收虚拟网络策略。

[0039] 特权级别确定模块344被配置为确定访问请求VM的特权级别和目的地VM的特权级别。应理解，请求VM和目的地VM可以是相同的VM或不同的VM，这取决于请求的类型。为了确定特权级别，特权级别确定模块344被配置为访问VM网络特权级别表，该VM网络特权级别表包括VM中的每个VM的特权级别以及VM中的每个VM的对应标识符(例如，域标识符)。在一些实施例中，VM网络特权级别表(即，特权级别和对应的标识符)可以存储在特权等级数据306中。应理解，在一些实施例中，特权级别数据306可以存储在例如可以使用信任平台模块技术来保护的NIC212的安全部分(例如，安全存储器214)中。

[0040] 授权访问确定模块346被配置为确定是否允许访问请求被发送到目的地VM，例如，可以由数据流管理模块330来执行。为此，授权访问确定模块346被配置为将访问请求VM的特权级别与目的地VM的特权级别进行比较，例如，可以由特权级别确定模块344来确定。

[0041] 现在参考图4，在另一说明性实施例中，网络计算设备106在操作期间建立环境400。说明性环境400包括在网络计算设备106上执行的多个VM402，其中的每个VM通信地耦合到NIC 212的多个虚拟功能410中的一个。说明性VM 402包括被指定为VM(1)404的第一VM，被指定为VM(2)406的第二VM，以及被指定为VM(N)408的第三VM(即，VM 402的“第N个”计算节点，其中“N”是正整数，并且指定一个或多个附加的VM 402)。说明性虚拟功能410包括被指定为VF(1)412的第一虚拟功能，被指定为VF(2)414的第二虚拟功能，以及被指定为VF(N)416的第三虚拟功能(即，虚拟功能410的“第N个”计算节点，其中“N”是正整数，并且指定一个或多个附加的虚拟功能410)。虚拟功能408中的每个由NIC 212管理，并且其之间的业务由图3的数据流管理模块330管理，如上面详细描述的。数据流管理模块330还耦合到图3的虚拟网络策略实施模块340，这也在上面详细描述。如所示出的，说明性实施例400的NIC 212包括图3的特权级别数据306。

[0042] 同样如先前描述的，特权级别数据306的内容(即，特权级别和对应的VM标识符)由通信地耦合到NIC 212的VMM 418管理。VMM 418负责控制和处理特许的指令执行。与被配置为防止应用运行或访问平台共享资源的传统技术不同，如先前描述地，网络计算设备106被配置为在不期望的网络业务经由其对应的虚拟功能被引导向特定VM之前阻止不期望的网络业务。因此，网络计算设备106被配置为控制网络特权而不是VM执行特权。为此，网络计算设备106被配置为在部署VM托管网络相关的服务期间例如从网络控制器108接收网络特权级别信息。在网络控制器108已经选择了合适的节点时，网络控制器108指示VMM 418应用所要求的特权级别，例如，该特权级别可以存储在先前描述的VM网络特权级别表中。

[0043] 现在参考图5，在使用中，网络计算设备106可以执行用于向初始化的VM分配特权级别的方法500。应理解，可以针对初始或未注册的访问请求来执行方法500。方法500开始于框502，其中网络计算设备106确定是否网络计算设备106请求VM(例如，图4的VM 402中的一个)进行初始化(即，已经实例化)。如果是，则方法500前进到框504，其中网络计算设备106确定要被初始化的VM的特权级别(例如，特许级别或非特许级别)。如先前描述的，特权级别可以由网络控制器108确定并且与接收到针对VM的初始化的请求一起或者在接收到针对VM的初始化的请求之后接收。

[0044] 在框506中，网络计算设备106利用待初始化的VM的标识符来存储待初始化的VM的特权级别。在一些实施例中，在框508中，网络计算设备106将特权级别存储在VM网络特权级别表的条目中。另外或可替代地，在一些实施例中，在框510中，网络计算设备106将VM的特权级别和标识符存储在NIC的安全存储器(例如，图2的NIC 212的安全存储器214)中。在框512中，网络计算设备106对VM进行初始化。在框514中，网络计算设备106对用于在框512中初始化的VM的虚拟功能和虚拟功能驱动器进行初始化。在框516中，网络计算设备106将初始化的虚拟功能分配给在框512中初始化的VM。

[0045] 现在参考图6，在使用中，网络计算设备106可以执行用于实施对初始化的虚拟机的网络访问控制的方法600。应理解，方法600可以在已经建立初始或未注册的访问请求之后执行，如在图5的方法500中所描述的。方法600开始于框602，其中网络计算设备106确定是否从VM接收到访问请求(例如，通过图3和图4的数据流管理模块330)。如先前描述的，访问请求可以是VM到VM访问请求、VM到网络访问请求(即，目标为进入或离开另一VM的外部网络业务)等。如果网络计算设备106确定从VM接收到访问请求时，网络计算设备106确定从其接收访问请求的请求VM的特权级别。为此，在一些实施例中，在框606中，网络计算设备106基于VM网络特权级别表中的与请求VM相对应的条目来确定请求VM的特权级别。

[0046] 在框608中，网络计算设备106确定已经针对其请求访问的目的地VM的特权级别。为此，在一些实施例中，在框610中，网络计算设备106基于VM网络特权级别表中的与目的地VM相对应的条目来确定目的地VM的特权级别。在框612中，网络计算设备106确定请求网络访问的VM(即，请求VM)是否被授权访问目的地VM。为此，在框614中，网络计算设备106将在框604中确定的请求VM的特权级别与在框608中确定的目的地VM的特权级别进行比较。

[0047] 在框616中，网络计算设备106基于网络策略来确定从请求VM到目的地VM的网络访问是否被授权。如果否，则方法600分支到框618，其中访问请求被拒绝；否则，如果所请求的访问被授权，则方法600相反分支到框620，其中允许访问请求。例如，如果网络计算设备106确定分配给请求VM的特权级别为特许级别并且分配给目的地VM的特权级别为特许级别，则网络计算设备106可以允许访问请求经由对应的虚拟功能被引导至目的地VM。

[0048] 在另一示例中，如果网络计算设备106确定分配给请求VM的特权级别为特许级别并且分配给目的地VM的特权级别为非特许级别，则网络计算设备106可以允许访问请求经由对应的虚拟功能被引导至目的地VM。在又一示例中，如果网络计算设备106确定分配给请求VM的特权级别是非特许级别并且分配给目的地VM的特权级别是特许级别，则网络计算设备106可以拒绝访问请求经由对应的虚拟功能被引导至目的地VM。

[0049] 应理解，方法500和600中的一个或两者的至少一部分可以由网络计算设备106的NIC 212执行。还应理解，在一些实施例中，方法500和600中的一个或两者可以体现为存储在计算机可读介质上的各种指令，其可以由处理器202、NIC 212和/或网络计算设备106的其他组件执行，以使网络计算设备106执行方法500和600。计算机可读介质可以体现为能够被网络计算设备106读取的任何类型的介质，包括但不限于存储器206、数据存储设备208、NIC 212的安全存储器214、网络计算设备106的其他存储器或数据存储设备、可由网络计算设备106的外围设备读取的便携式介质和/或其他介质。

[0050] 示例

[0051] 下面提供了本文公开的技术的说明性示例。这些技术的实施例可以包括下面描述

的示例中的任何一个或多个以及其任何组合。

[0052] 示例1包括一种用于实施虚拟机网络访问控制的网络计算设备，该网络计算设备包括：一个或多个处理器；以及一个或多个数据存储设备，其中存储有多个指令，该指令当由一个或多个处理器执行时使网络计算设备用于：从分配给请求虚拟机的虚拟功能接收访问请求，其中，请求虚拟机是在网络计算设备上初始化的多个虚拟机中的一个，其中，访问请求包括对目的地虚拟机的至少一部分进行访问的请求，其中，目的地虚拟机是在网络计算设备上初始化的多个虚拟机中的一个；确定分配给请求机器的第一特权级别和分配给目的地虚拟机的第二特权级别；基于对第一特权级别与第二特权级别的比较来确定请求虚拟机是否被授权对目的地虚拟机进行访问；以及响应于确定请求虚拟机被授权对目的地虚拟机进行访问，允许请求虚拟机对目的地虚拟机进行访问。

[0053] 示例2包括示例1的主题，并且其中，该多个指令还使网络计算设备用于：对多个虚拟机中的每个虚拟机进行初始化；以及向多个虚拟机中的每个虚拟机分配特权级别，其中，特权级别包括特许级别或非特许级别中的一个。

[0054] 示例3包括示例1和2中任一项的主题，并且其中，该多个指令还使网络计算设备用于：针对多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化；以及向多个虚拟机中的对应的一个虚拟机分配一个或多个虚拟功能中的每个虚拟功能。

[0055] 示例4包括示例1-3中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别。

[0056] 示例5包括示例1-4中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于特许级别之后，允许进行访问。

[0057] 示例6包括示例1-5中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于非特许级别之后，允许进行访问。

[0058] 示例7包括示例1-6中任一项的主题，并且其中，该多个指令还使得网络计算设备用于：响应于确定请求虚拟机未被授权对目的地虚拟机进行访问，拒绝请求虚拟机对目的地虚拟机进行访问。

[0059] 示例8包括示例1-7中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别，并且其中，拒绝请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于非特许级别并且第二特权级别对应于特许级别之后，拒绝进行访问。

[0060] 示例9包括示例1-8中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：允许访问限于目的地虚拟机的与访问请求相对应的至少一部分。

[0061] 示例10包括示例1-9中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是相同的虚拟机。

[0062] 示例11包括示例1-10中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是不同的虚拟机。

[0063] 示例12包括示例1-11中任一项的主题，并且其中，访问请求包括VM到VM访问请求

或VM到网络访问请求中的一个。

[0064] 示例13包括一种用于实施虚拟机网络访问控制的方法，该方法包括：由网络计算设备从分配给请求虚拟机的虚拟功能接收访问请求，其中，请求虚拟机是在网络计算设备上初始化的多个虚拟机中的一个，其中，访问请求包括对目的地虚拟机的至少一部分进行访问的请求，其中，目的地虚拟机是在网络计算设备上初始化的多个虚拟机中的一个；由网络计算设备确定分配给请求机器的第一特权级别和分配给目的地虚拟机的第二特权级别；由网络计算设备基于对第一特权级别与第二特权级别的比较来确定请求虚拟机是否被授权对目的地虚拟机进行访问；以及由网络计算设备并且响应于确定请求虚拟机被授权对目的地虚拟机进行访问，允许请求虚拟机对目的地虚拟机进行访问。

[0065] 示例14包括示例13的主题，还包括：由网络计算设备对多个虚拟机中的每个虚拟机进行初始化；以及由网络计算设备向多个虚拟机中的每个虚拟机分配特权级别，其中，特权级别包括特许级别或非特许级别中的一个。

[0066] 示例15包括示例13和14中任一项的主题，并且还包括：由网络计算设备针对多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化；以及由网络计算设备向多个虚拟机中的对应的一个虚拟机分配一个或多个虚拟功能中的每个虚拟功能。

[0067] 示例16包括示例13-15中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别。

[0068] 示例17包括示例13-16中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于特许级别之后，允许进行访问。

[0069] 示例18包括示例13-17中任一项的主题，并且其中，由网络计算设备允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于非特许级别之后，允许进行访问。

[0070] 示例19包括示例13-18中任一项的主题，并且还包括：由网络计算设备并且响应于确定请求虚拟机未被授权对目的地虚拟机进行访问，拒绝请求虚拟机对目的地虚拟机进行访问。

[0071] 示例20包括示例13-19中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别，并且其中，拒绝请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于非特许级别并且第二特权级别对应于特许级别之后，拒绝进行访问。

[0072] 示例21包括示例13-20中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：允许访问限于目的地虚拟机的与访问请求相对应的至少一部分。

[0073] 示例22包括示例13-21中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是相同的虚拟机。

[0074] 示例23包括示例13-22中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是不同的虚拟机。

[0075] 示例24包括示例13-23中任一项的主题，并且其中，接收访问请求包括接收VM到VM访问请求或VM到网络访问请求中的一个。

[0076] 示例25包括一种网络计算设备，其包括：处理器；以及其中存储有多个指令的存储器，该多个指令当由处理器执行时使网络计算设备执行根据示例13-24中任一项的方法。

[0077] 示例26包括一种或多种机器可读存储介质，包括存储在其上的多个指令，该多个指令响应于被执行而使得网络计算设备执行根据示例13-24中任一项的方法。

[0078] 示例27包括一种用于实施虚拟机网络访问控制的网络计算设备，该网络计算设备包括：网络通信电路，其用于从分配给请求虚拟机的虚拟功能接收访问请求，其中，请求虚拟机是在网络计算设备上初始化的多个虚拟机中的一个，其中，访问请求包括对目的地虚拟机的至少一部分进行访问的请求，其中，目的地虚拟机是在网络计算设备上初始化的多个虚拟机中的一个；虚拟机网络策略实施电路，其用于(i)确定分配给请求机器的第一特权级别和分配给目的地虚拟机的第二特权级别，并且(ii)基于对第一特权级别与第二特权级别的比较来确定请求虚拟机是否被授权对目的地虚拟机进行访问；数据流管理电路，其用于响应于确定请求虚拟机被授权对目的地虚拟机进行访问而允许请求虚拟机对目的地虚拟机进行访问。

[0079] 示例28包括示例27的主题，并且还包括用于对多个虚拟机中的每个虚拟机进行初始化的虚拟机管理电路，其中，虚拟机网络策略实施电路还用于向多个虚拟机中的每个虚拟机分配特权级别，其中，特权级别包括特许级别或非特许级别中的一个。

[0080] 示例29包括示例27和28中任一项的主题，并且其中，虚拟机管理电路还用于：(i)针对多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化，以及(ii)向多个虚拟机中的对应的一个虚拟机分配一个或多个虚拟功能中的每个虚拟功能。

[0081] 示例30包括示例27-29中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别。

[0082] 示例31包括示例27-30中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于特许级别之后，允许进行访问。

[0083] 示例32包括示例27-31中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于非特许级别之后，允许进行访问。

[0084] 示例33包括示例27-32中任一项的主题，并且其中，数据流管理电路还用于：响应于确定请求虚拟机未被授权对目的地虚拟机进行访问，拒绝请求虚拟机对目的地虚拟机进行访问。

[0085] 示例34包括示例27-33中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别，并且其中，拒绝请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于非特许级别并且第二特权级别对应于特许级别之后，拒绝进行访问。

[0086] 示例35包括示例27-34中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：允许访问限于目的地虚拟机的与访问请求相对应的至少一部分。

[0087] 示例36包括示例27-35中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是相同的虚拟机。

[0088] 示例37包括示例27-36中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是不同的虚拟机。

[0089] 示例38包括示例27-37中任一项的主题，并且其中，访问请求包括VM到VM访问请求或VM到网络访问请求中的一个。

[0090] 示例39包括一种用于实施虚拟机网络访问控制的网络计算设备，该网络计算设备包括：网络通信电路，其用于从分配给请求虚拟机的虚拟功能接收访问请求，其中，请求虚拟机是在网络计算设备上初始化的多个虚拟机中的一个，其中，访问请求包括对目的地虚拟机的至少一部分进行访问的请求，其中，目的地虚拟机是在网络计算设备上初始化的多个虚拟机中的一个；用于确定分配给请求机器的第一特权级别和分配给目的地虚拟机的第二特权级别的单元；用于基于对第一特权级别与第二特权级别的比较来确定请求虚拟机是否被授权对目的地虚拟机进行访问的单元；数据流管理电路，其用于响应于确定请求虚拟机被授权对目的地虚拟机进行访问而允许请求虚拟机对目的地虚拟机进行访问。

[0091] 示例40包括示例39的主题，并且还包括用于对多个虚拟机中的每个虚拟机进行初始化的虚拟机管理电路，其中，虚拟机网络策略实施电路还用于向多个虚拟机中的每个虚拟机分配特权级别，其中，特权级别包括特许级别或非特许级别中的一个。

[0092] 示例41包括示例39和40中任一项的主题，并且其中，虚拟机管理电路还用于(i)针对多个虚拟机中的每个虚拟机对一个或多个虚拟功能进行初始化，以及(ii)向多个虚拟机中的对应的一个虚拟机分配一个或多个虚拟功能中的每个虚拟功能。

[0093] 示例42包括示例39-41中任一项的主题，并且其中，向多个虚拟机中的每个虚拟机分配特权级别包括：向请求虚拟机分配第一特权级别，并且向目的地虚拟机分配第二特权级别。

[0094] 示例43包括示例39-42中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于特许级别之后，允许进行访问。

[0095] 示例44包括示例39-43中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于特许级别并且第二特权级别对应于非特许级别之后，允许进行访问。

[0096] 示例45包括示例39-44中任一项的主题，并且其中，数据流管理电路还用于：响应于确定请求虚拟机未被授权对目的地虚拟机进行访问，拒绝请求虚拟机对目的地虚拟机进行访问。

[0097] 示例46包括示例39-45中任一项的主题，并且其中，用于向多个虚拟机中的每个虚拟机分配特权级别的单元包括：用于向请求虚拟机分配第一特权级别并且向目的地虚拟机分配第二特权级别的单元，并且其中，拒绝请求虚拟机对目的地虚拟机进行访问包括：在确定第一特权级别对应于非特许级别并且第二特权级别对应于特许级别之后，拒绝进行访问。

[0098] 示例47包括示例39-46中任一项的主题，并且其中，允许请求虚拟机对目的地虚拟机进行访问包括：允许访问限于目的地虚拟机的与访问请求相对应的至少一部分。

[0099] 示例48包括示例39-47中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是相同的虚拟机。

[0100] 示例49包括示例39-48中任一项的主题，并且其中，第一虚拟机和目的地虚拟机是不同的虚拟机。

[0101] 示例50包括示例39-49中任一项的主题，并且其中，访问请求包括VM到VM访问请求或VM到网络访问请求中的一个。

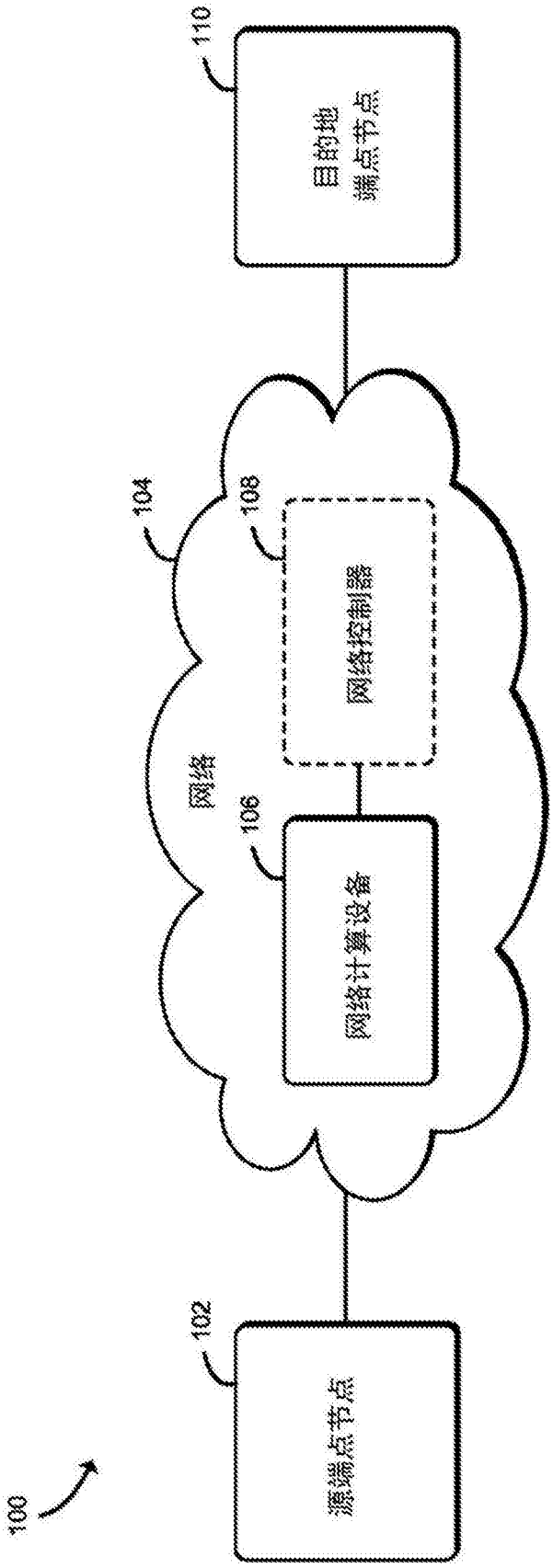


图1

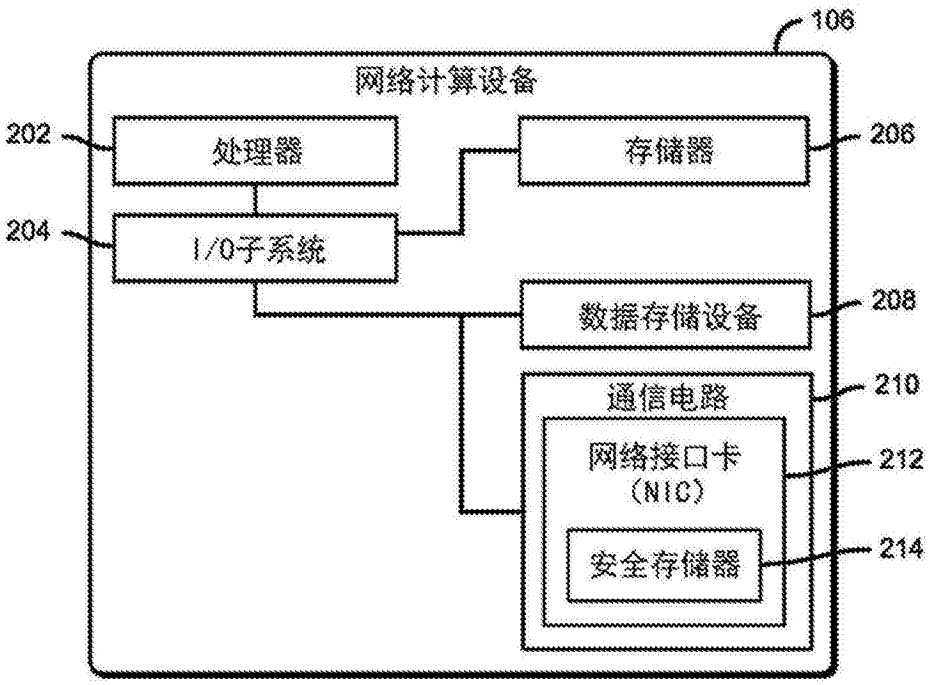

106
网络计算设备
202
处理器
存储器
206
204
I/O子系统
数据存储设备
208
通信电路
210
网络接口卡
(NIC)
212
安全存储器
214

图2

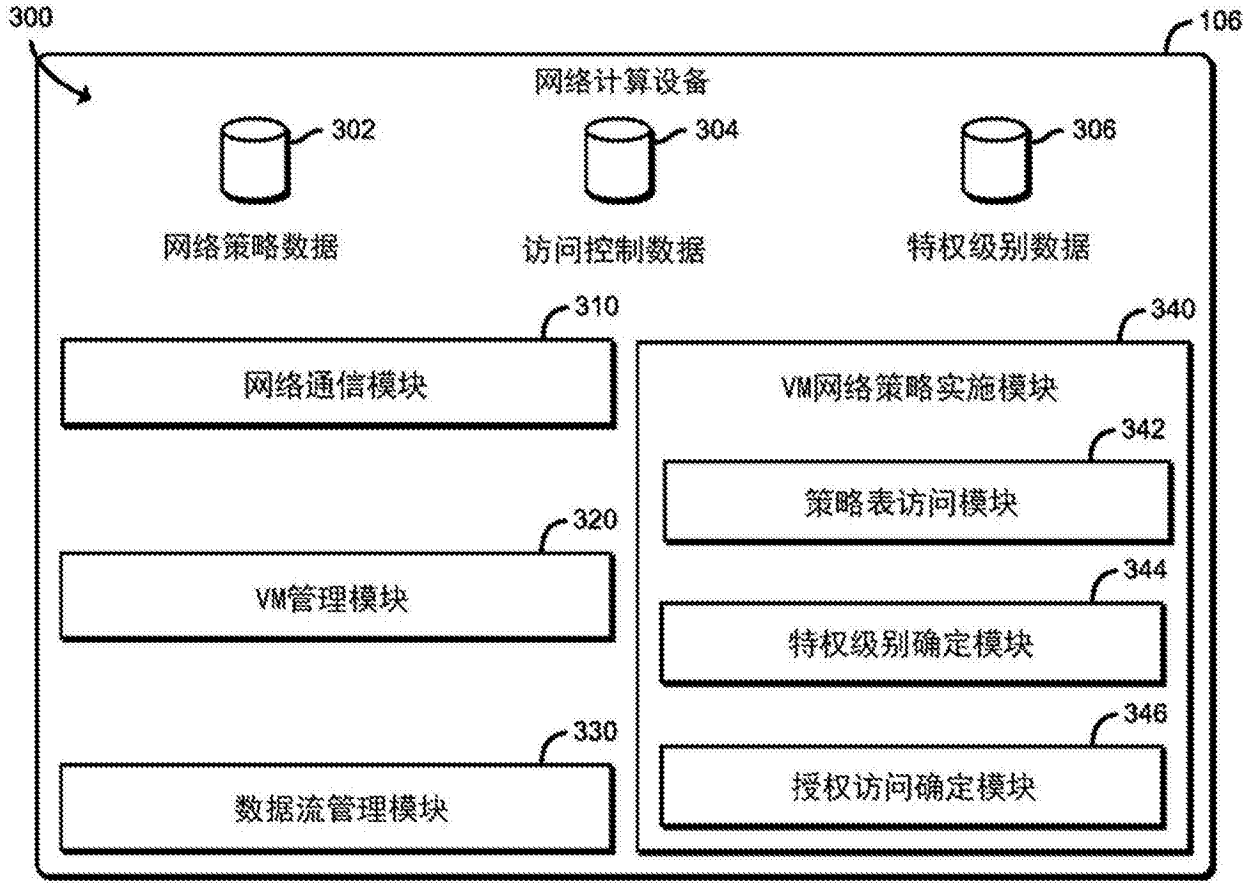

300
106
网络计算设备
302
304
306
网络策略数据
访问控制数据
特权级别数据
310
340
网络通信模块
VM网络策略实施模块
342
策略表访问模块
320
VM管理模块
344
特权级别确定模块
330
346
数据流管理模块
授权访问确定模块

图3

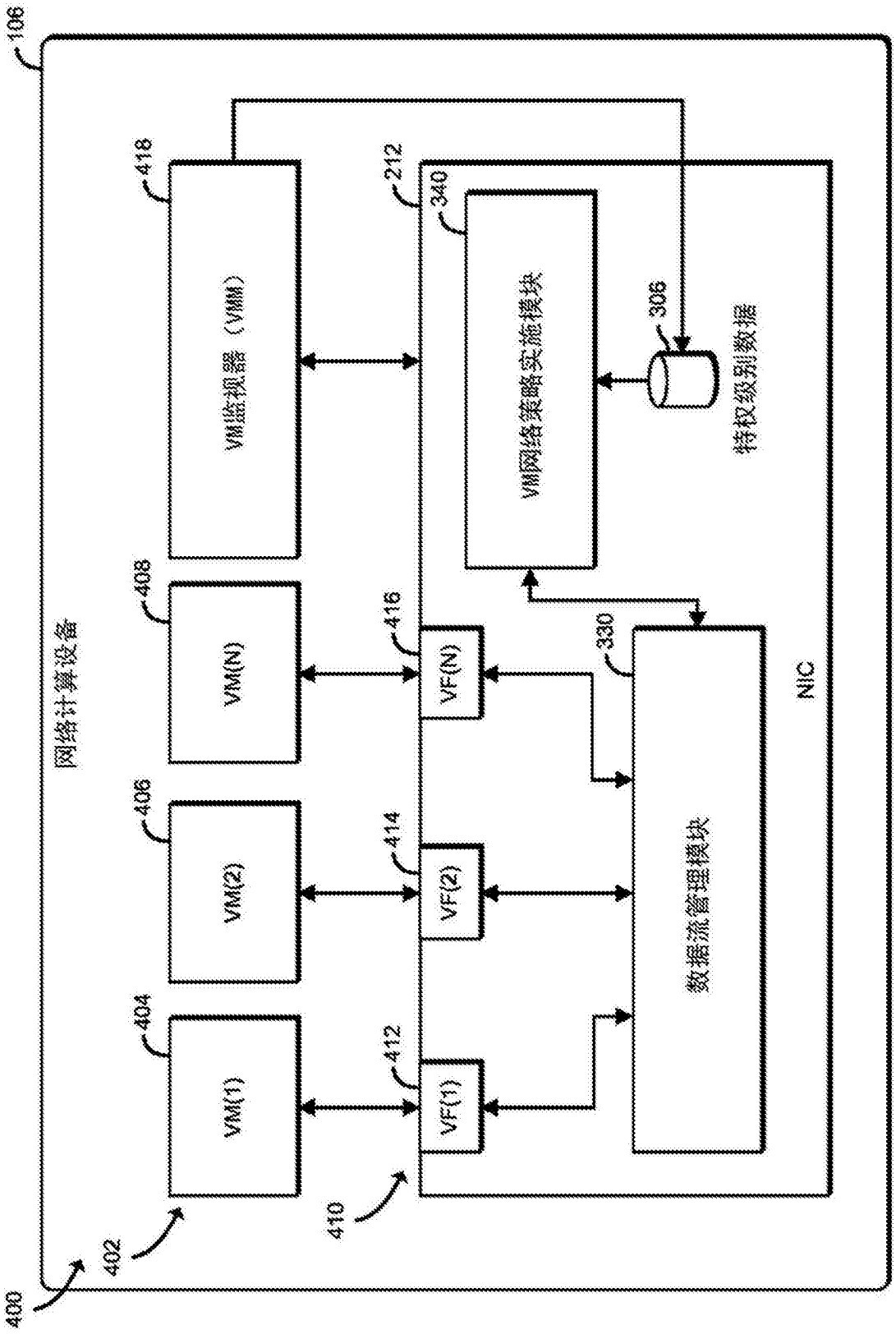

106
网络计算设备
418
VM监视器（VMM）
212
340
VM网络策略实施模块
306
特权级别数据
408
VM(N)
416
VF(N)
330
NIC
406
VM(2)
414
VF(2)
数据流管理模块
404
VM(1)
412
VF(1)
410
402
400

图4

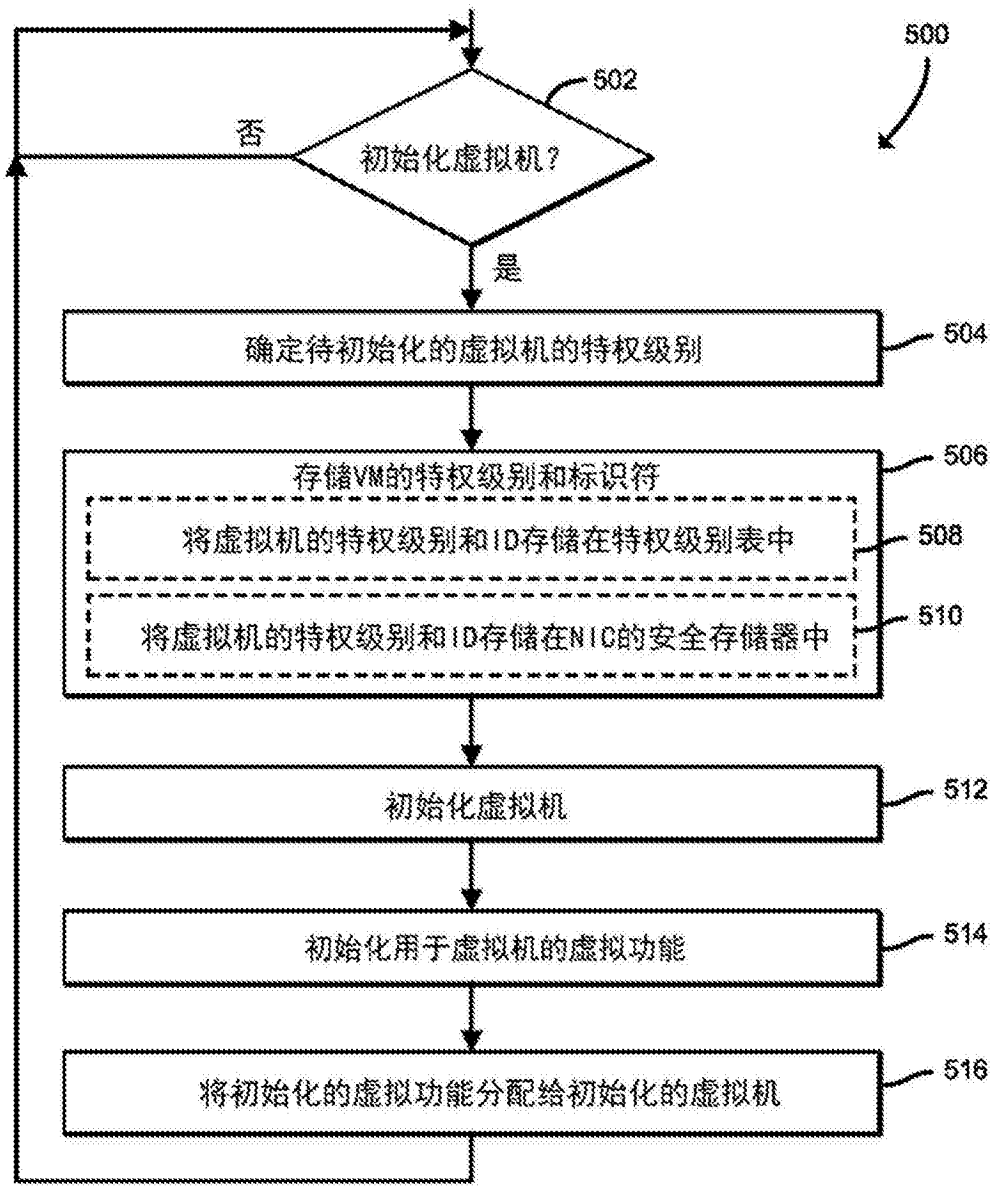

500
502
初始化虚拟机?
否
是
确定待初始化的虚拟机的特权级别
504
存储VM的特权级别和标识符
506
将虚拟机的特权级别和ID存储在特权级别表中
508
将虚拟机的特权级别和ID存储在NIC的安全存储器中
510
初始化虚拟机
512
初始化用于虚拟机的虚拟功能
514
将初始化的虚拟功能分配给初始化的虚拟机
516

图5

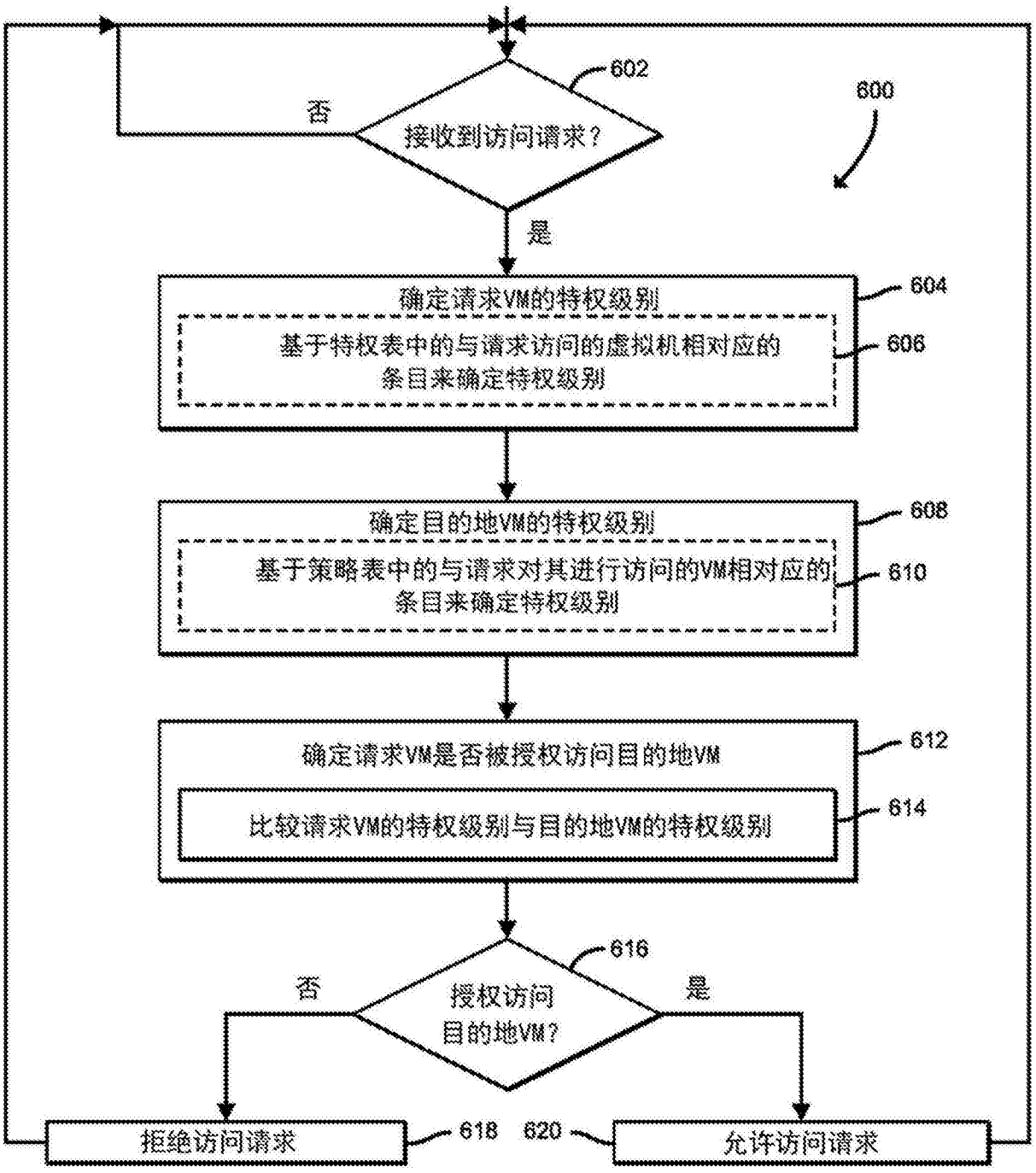

600
602
接收到访问请求？
否
是
604
确定请求VM的特权级别
606
基于特权表中的与请求访问的虚拟机相对应的条目来确定特权级别
608
确定目的地VM的特权级别
610
基于策略表中的与请求对其进行访问的VM相对应的条目来确定特权级别
612
确定请求VM是否被授权访问目的地VM
614
比较请求VM的特权级别与目的地VM的特权级别
616
授权访问目的地VM？
否
是
618
拒绝访问请求
620
允许访问请求

图6