(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 107004095 A
(43)申请公布日 2017.08.01

(21)申请号 201580063913.0

(22)申请日 2015.11.05

(30)优先权数据
14/555,739 2014.11.28 US
14/555,741 2014.11.28 US
14/555,745 2014.11.28 US
14/555,748 2014.11.28 US

(85)PCT国际申请进入国家阶段日
2017.05.24

(86)PCT国际申请的申请数据
PCT/IB2015/058543 2015.11.05

(87)PCT国际申请的公布数据
WO2016/083925 EN 2016.06.02

(71)申请人 国际商业机器公司
地址 美国纽约阿芒克

(72)发明人 J·R·霍伊 N·纳加拉纳姆 S·穆皮迪 S·R·伊耶

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 酆迅

(51)Int.Cl.
G06F 21/62(2006.01)

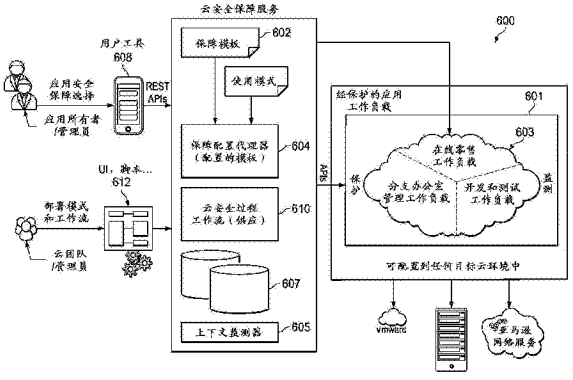
权利要求书2页 说明书20页 附图7页

(54)发明名称

基于上下文的云安全保障系统

(57)摘要

云基础架构被增强以提供基于上下文的安全保障服务从而使能安全的应用部署。服务检查网络和云拓扑以标识潜在的安全能力和需求。优选地,这些选项随后以表示安全保障级别的易于理解、预先配置的模板向用户进行显现。当模板(例如,表示预先配置的保障级别)被用户所选择时,系统随后应用具体能力和控制以将用户所选择的一般规范(例如,"高安全")转换为针对安全资源的具体集合的粒度要求。优选地,这些安全资源的标识基于系统配置、管理以及与预先配置的模板相关联的信息。



CN 107004095 A

1.一种用于云应用环境中的基于上下文的安全保障的方法,包括:

接收关于所述云应用环境中的可用的安全能力集合的信息以定义安全上下文;

接收对安全保障级别的选择,其中所述安全保障级别以不暴露实施所述安全保障级别所必需的至少一些具体安全资源要求的方式被指定;以及

响应于所述选择的接收,并且至少部分基于所述安全上下文,在所述云应用环境中配置安全资源集合;

其中所述接收和配置步骤在硬件元件中执行的软件中被执行。

2.根据权利要求1所述的方法,进一步包括提供模板集合,每个模板具有与之相关联的所述安全保障级别中的一个安全保障级别,并且其中对所述安全保障级别的所述选择对应于对模板的选择。

3.根据权利要求2所述的方法,其中所述模板集合经由与所述云应用环境相关联的用户界面工具作业而被提供给终端用户,其中所述选择的接收对应于由所述终端用户经由所述用户界面工具作业的选择。

4.根据权利要求2所述的方法,其中所述模板经由管理界面被提供给安全管理员。

5.根据权利要求4所述的方法,进一步包括经由所述管理界面调整与模板相关联的所述安全要求集合。

6.根据权利要求1所述的方法,其中所述方法进一步包括调整所配置的所述安全资源集合。

7.根据权利要求6所述的方法,其中所述调整在以下之一时出现:应用被取消部署时安全环境应用的解配置,第二应用被部署时针对第一应用的安全环境的修改,以及比所述第一应用具有更高安全级别的第二应用被解配置时针对第一应用的安全环境的修改。

8.一种用于云应用环境中的基于上下文的安全保障的方法,包括:

查询所述云应用环境,并且作为响应,接收关于所述云应用环境中的可用的安全能力的集合的信息,至少部分基于所述接收的信息在编辑器中呈现模板集合,其中模板具有与之相关联的安全保障级别,所述安全保障级别以不暴露实施所述安全保障级别所必需的至少一些具体安全资源要求的方式被指定,并且其中模板还呈现与已经被标识的至少一种安全能力相关联的成本信息,以及响应于对一个或多个模板的选择的接收而在所述云应用环境中配置安全资源集合,其中所述查询、呈现和配置步骤在硬件元件中执行的软件中被执行。

9.一种用于云应用环境中的基于上下文的安全保障的方法,包括:

提供安全保障服务,第一用户通过所述安全保障服务与关联于所述云应用环境的云管理平台交互,所述安全保障服务为所述第一用户提供模板集合,其中模板具有与之相关联的安全保障级别,所述安全保障级别以不向第一用户暴露实施所述安全保障级别所必需的至少一些具体安全资源要求的方式被指定,为不同于所述第一用户的至少一个第二用户提供与由所述第一用户的模板选择相关联的安全配置更改的安全管理视图,以及响应于经由所述安全管理视图的输入的接收而实施关于在所述云应用环境中一个或多个安全能力的配置的安全管理动作,其中所述提供和实施步骤在硬件元件中执行的软件中被执行。

10.一种用于云应用环境中的基于上下文的安全保障的方法,包括:

关联于在所述云应用环境中应用的部署而在编辑器中呈现模板集合,其中模板具有与

之相关联的安全保障级别，所述安全保障级别以不暴露实施所述安全保障级别所必需的至少一些具体安全资源要求的方式被指定，响应于对模板的选择的接收并且至少部分基于安全上下文，在所述云应用环境中配置安全资源集合以创建云应用区域，以及将所述应用部署到所述云应用区域中，其中所述呈现、配置和部署步骤在硬件元件中执行的软件中被执行。

11.一种用于在云应用环境中提供基于上下文的安全保障的装置，包括：

处理器；

保持计算机程序指令的计算机存储器，所述计算机程序指令在被所述处理器执行时使得所述装置：

接收关于所述云应用环境中可用的安全能力集合的信息以定义安全上下文；

接收对安全保障级别的选择，其中所述安全保障级别以不暴露实施所述安全保障级别所必需的至少一些具体安全资源要求的方式被指定；以及

响应于所述选择的接收并且至少部分基于所述安全上下文，在所述云应用环境中配置安全资源集合。

12.根据权利要求11所述的装置，其中所述计算机程序指令执行以定义模板集合，每个模板具有与之相关联的所述安全保障级别中的一个安全保障级别，并且其中对所述安全保障级别的所述选择对应于对模板的选择。

13.根据权利要求12所述的装置，其中所述模板集合经由与所述云应用环境相关联的用户界面工具作业而被提供给终端用户，其中所述选择的接收对应于由所述终端用户经由所述用户界面工具作业的选择。

14.根据权利要求12所述的装置，进一步包括管理界面，并且其中所述模板经由所述管理界面被提供给安全管理员。

15.根据权利要求14所述的装置，进一步包括所述计算机程序指令，所述计算机程序指令进一步包括程序代码以经由所述管理界面调整与模板相关联的所述安全要求集合。

16.根据权利要求11所述的装置，进一步包括计算机程序指令，所述计算机程序指令执行以调整所配置的所述安全资源集合。

17.根据权利要求16所述的装置，其中所述调整在以下之一时出现：应用被取消部署时安全环境应用的解配置，第二应用被部署时针对第一应用的安全环境的修改，以及比所述第一应用具有更高安全级别的第二应用被解配置时针对第一应用的安全环境的修改。

18.一种用于数据处理系统中的非瞬态计算机可读介质中的计算机程序产品，所述计算机程序产品保持计算机程序指令，所述计算机程序指令由所述数据处理系统执行以在云应用环境中提供基于上下文的安全保障，所述计算机程序指令被所述数据处理系统执行时执行权利要求1至10中任一项所述的方法。

基于上下文的云安全保障系统

技术领域

[0001] 本发明一般涉及在“云”计算环境中部署应用。

背景技术

[0002] 一种新兴的信息技术(IT)递送模型是云计算,共享资源、软件和信息通过云计算经互联网按需要被提供至计算机和其他设备。云计算能够明显降低IT成本和复杂度,同时改善工作负载优化和服务递送。利用该方法,应用实例能够被托管并且使得其从基于互联网的资源可用,该资源可经HTTP通过常规网页浏览器进行访问。示例应用可能是能够提供一般消息功能集合的应用,诸如电子邮件、日历、联系人管理和即时通讯。用户随后将通过互联网直接访问服务。使用该服务,企业将会将其电子邮件、日历和/或合作基础架构置入云中,并且终端用户将使用适当客户端来访问他的/她的电子邮件,或者执行日历操作。

[0003] 云计算资源通常被容纳在运行一个或多个网络应用的大型服务器场中,其通常使用虚拟化架构,其中应用在被映射到数据中心设施中的物理服务器上的虚拟服务器或所谓的“虚拟机”(VM)中运行。虚拟机通常在超监督者(hypervisor)顶端运行,超监督者是向虚拟机分配物理资源的控制程序。

[0004] 提供基于装置或基于平台的解决方案以促进基于云的提供的快速采用和部署是本领域已知的。通常,基于云的提供被部署为云应用包。一种可以被用于该目的的这样的装置是IBM® Workload Deployer(工作负载部署器),其基于IBM DataPower®7199/9005产品族。通常,该装置直接位于许多组织使用的业务工作负载和底层云基础架构以及平台组件之间。备选地,云应用包可以使用平台即服务(PAS)基础架构(诸如IBM® SmartCloud® Orchestrator开放式云管理平台)而被部署。这种类型的管理平台通常包括若干层(包括用于提供、配置和管理存储、计算和网络资源的基础架构服务层、平台服务层以及用以提供业务过程管理的编制服务层)。平台服务层包括虚拟机镜像生命周期管理能力以及模式服务,其中“模式”为业务服务提供部署和管理指令。模式优选地是供应和管理针对具体应用(或应用类型)工作负载的各种资源(例如,计算、网络、存储、操作系统、中间件等)所需的基础架构配置的基于可扩展标示语言(XML)的定义。

[0005] 随着安全软件的部署变得越来越复杂,应用开发方被进一步从安全环境的内部工作中移除。因此,安全操作经常被留给安全专家。然而,迁移至虚拟化和私有云授予了应用开发方越来越多的操作能力。应用开发方然后发现他们自身处于困难的位置。特别地,当将应用投入生产时,开发方可能并没有必要的背景和上下文来适当地评估他的/她的应用的安全影响和需求。如今,应用开发方经常与安全专家一起工作以设计用于安全应用部署的策略。然而,安全专家可能遇到来自其他方向的相同问题。由于应用和中间件变得越来越复杂和虚拟化,安全专家可能无法完全理解应用以适当评估其安全影响和要求。

[0006] 因此,需要弥合应用开发方和安全专家之间的这个知识差距,并且促进新的基于云的应用的无缝且可靠的部署。

发明内容

[0007] 根据本公开，云基础架构被增强以提供“基于上下文的安全保障”服务从而使得例如能够由应用开发方进行安全应用部署，而并不需要这样的个体拥有深入的安全技能或者对他们的应用可以在其上执行的底层安全机制的详细理解。通常，保障服务关联于包括应用部署机制的云应用平台操作。服务检查网络和云拓扑以标识潜在的安全能力和需求(例如，虚拟化虚拟周边网络(DMZ)、入侵防止系统(IPS)、资源隔离等)。优选地，这些选项随后以表示安全保障级别的易于理解、预先配置的模板向用户显现。当模板(例如，表示预先配置的保障级别)被用户所选择时，系统随后应用具体能力和控制以将用户所选择的一般规定(例如，“高安全”)转换为针对安全资源的具体集合的粒度要求。优选地，这些安全资源的标识基于系统配置、管理以及与预先配置的模板相关联的信息。通常，(关于由用户所选择的特定解决方案)所实施的安全资源按照保障级别而增加。

[0008] 因此，基于所选择的(多个)模板，并且优选地在应用部署期间，安全配置变化集合被应用于现有的应用执行环境以生成“基于上下文的”安全云应用“区域”。一旦云应用区域被定义，应用部署完成，并且该区域为应用提供主动保护。应用区域主动保护是如以上所提到的特定于安全上下文的，但是该方法不要求部署应用的个体详细了解底层安全基础架构。

[0009] 以上已经对本公开主题的一些更为相关的特征进行了概述。这些特征应当被理解为仅是说明性的。能够通过以不同方式对所公开的主题加以应用或者通过对将要描述的发明进行修改而获得许多其它的有益结果。

附图说明

[0010] 现在将参考附图仅以示例的方式对本发明的(多个)实施例进行描述，其中：

[0011] 图1描绘了可以在其中实施说明性实施例的示例性方面的分布式数据处理环境的示例性框图；

[0012] 图2是可以在其中实施说明性实施例的示例性方面的数据处理系统的示例性框图；

[0013] 图3图示了可以在其中实施所公开主题的示例性云计算架构；

[0014] 图4图示了基于网络的装置可以在其中被用来促进一个或多个基于云的提供的部署的示例性操作环境；

[0015] 图5图示了基于网络的装置的代表性功能组件；

[0016] 图6图示了本公开的安全保障服务的基础操作组件的框图；

[0017] 图7图示了安全保障服务的安全管理界面组件的代表性显示页面；

[0018] 图8图示了根据本公开安全保障服务可以如何关联于云应用平台被使用以促进基于上下文的安全云应用区域的创建。

具体实施方式

[0019] 现在参考附图特别是图1-2，其提供了可以在其中实施本公开的说明性实施例的数据处理环境的示例性示图。应当理解，图1-2仅是示例性的而并非旨在明示或暗示关于可

以在其中实施所公开主题的方面或实施例的任何限制。可以对所描绘的实施例进行许多修改而并不超出本发明的精神和范围。

[0020] 客户端-服务器技术

[0021] 现在参考附图，图1描绘了可以在其中实施说明性实施例的(多个)方面的示例性分布式数据处理系统的图形表示。分布式数据处理系统100可以包括可以在其中实施说明性实施例的(多个)方面的计算机网络。分布式数据处理系统100包含至少一个网络102，其是用以在分布式数据处理系统100内被连接在一起的各种设备和计算机之间提供通信链接的介质。网络102可以包括连接，诸如有线、无线通信链接或者光纤线缆。

[0022] 在所描绘的示例中，服务器104和服务器106连同存储单元108被连接至网络102。此外，客户端110、112和114也被连接至网络102。例如，这些客户端110、112和114可以是个人计算机、网络计算机等。在所描绘的示例中，服务器104向客户端110、112和114提供诸如引导文件、操作系统镜像和应用的数据。在所描绘的示例中客户端110、112和114是服务器104的客户端。分布式数据处理系统100可以包括未示出的附加服务器、客户端和其它设备。

[0023] 在所描绘的示例中，分布式数据处理系统100是互联网，其以网络102表示使用传输控制协议/互联网协议(TCP/IP)协议套件互相通信的全世界网络和网关集合。互联网的核心是主要节点或主机计算机之间的高速数据通信线路的主干网，其由数千个路由数据和消息的商业、政府、教育和其它计算机系统所构成。当然，分布式数据处理系统100也可以被实施以包括多种不同类型的网络，作为示例诸如企业内部网、局域网(LAN)、广域网(WAN)等。如上所述，图1旨在作为示例而并非针对所公开主题的不同实施例的架构性限制，因此图1中所示出的特定元素不应当被理解为是关于可以在其中实施本发明的说明性实施例的环境的限制。

[0024] 现在参考图2，其示出了可以在其中实施说明性实施例的(多个)方面的示例性数据处理系统的框图。数据处理系统200是计算机(诸如图1中的客户端110)的示例，实施本公开的说明性实施例的过程的计算机可用代码或指令可以位于数据处理系统200中。

[0025] 现在参考图2，示出了可以在其中实施说明性实施例的数据处理系统的框图。数据处理系统200是计算机(诸如图1中的服务器104或客户端110)的示例，实施说明性实施例的过程的计算机可用程序代码或指令可以位于数据处理系统200中。在该说明性示例中，数据处理系统20包括通信构架202，其提供处理器单元204、存储器206、持久性存储208、通信单元210、输入/输出(I/O)单元212和显示器214之间的通信。

[0026] 处理器单元204用来执行可以被加载到存储器206中的软件的指令。根据特定实施方式，处理器单元204可以是一个或多个处理器的集合或者可以是多个处理器核心。此外，处理器单元204可以使用一个或多个异构处理器系统来实施，其中主处理器和辅处理器一起出现在单个芯片上。作为另一个说明性示例，处理器单元204可以是包含多个相同类型的处理器的对称多处理器(SMP)系统。

[0027] 存储器206和持久性存储208是存储设备的示例。存储设备是能够以临时的基础和/或持久的基础来存储信息的任何硬件。在这些示例中，存储器206例如可以是随机存取存储器或者任何其它适当的易失性或非易失性存储设备。持久性存储208可以根据特定实施方式而采用各种形式。例如，持久性存储208可以包含一个或多个组件或设备。例如，持久性存储208可以是硬盘驱动器、闪速存储器、可重写光盘、可重写磁带或者以上的一些组合。

持久性存储208所使用的介质还可以是可移动的。例如，可移动硬盘驱动器可以用于持久性存储208。

[0028] 在这些示例中，通信单元210提供与其它数据处理系统或设备的通信。在这些示例中，通信单元210是网络接口卡。通信单元210可以通过使用物理和无线通信链接之一或二者来提供通信。

[0029] 输入/输出单元212允许利用可以被连接至数据处理系统200的其它设备来输入和输出数据。例如，输入/输出单元212可以提供用于通过键盘和鼠标的用户输入的连接。此外，输入/输出单元212可以向打印机发送输出。显示器214提供向用户显示信息的机制。

[0030] 用于操作系统以及应用或程序的指令位于持久性存储208上。这些指令可以被加载到存储器206中以由处理器单元204执行。不同实施例的过程可以由处理器单元204使用计算机实施的指令来执行，指令可以位于诸如存储器206的存储器中。这些指令被称作可以由处理器单元204中的处理器读取并执行的程序代码、计算机可用程序代码或计算机可读程序代码。不同实施例中的程序代码可以在诸如存储器206或持久性存储208的不同物理或有形计算机可读介质上被具化。

[0031] 程序代码216以功能形式位于计算机可读介质218上，其选择性地是可移动的并且可以被加载或传输到数据处理系统200以由处理器单元204执行。程序代码216和计算机可读介质218在这些示例中形成计算机程序产品220。在一个示例中，计算机可读介质218可以为有形形式，作为示例诸如被插入或置入到作为持久性存储208的部分的驱动器或其它设备之中以便传输到存储设备(诸如作为持久性存储208的部分的硬盘驱动器)的光盘或磁盘。以有形形式，计算机可读介质218也可以采用持久性存储的形式(诸如被连接至数据处理系统200的硬盘驱动器、拇指驱动器或闪速存储器)。有形形式的计算机可读介质218也被称作计算机可记录存储介质。在一些实例中，计算机可读介质218可以不是可移动的。

[0032] 备选地，程序代码216可以通过到通信单元210的通信链接和/或通过到输入/输出单元212的连接从计算机可读介质218被传输至数据处理系统200。在说明性示例中通信链接和/或连接可以是物理或无线的。计算机可读介质还可以采用非有形介质的形式，诸如包含程序代码的通信链接或无线传输。针对数据处理系统200所图示的不同组件并非旨在对可以实施不同实施例的方式提供架构性限制。不同说明性实施例可以在包括针对数据处理系统200所图示的那些附加的或者作为其替代的组件的数据处理系统中实施。图2所示的其它组件可以不同于所示出的说明性示例。作为一个示例，数据处理系统200中的存储设备是可以存储数据的任何硬件装置。存储器206、持久性存储208和计算机可读介质218是有形形式的存储设备的示例。

[0033] 在另一个示例中，可以使用总线系统来实施通信构架202，总线系统可以由一个或多个总线(诸如系统总线或输入/输出总线)组成。当然，总线系统可以使用提供在附接至总线系统的不同组件或设备之间的数据传输的任何适当类型的架构而被实施。此外，通信单元可以包括一个或多个用来传送和接收数据的设备，诸如调制解调器或网络适配器。而且，存储器例如可以是存储器206或者诸如在接口中发现的高速缓存以及可以出现在通信构架202中的存储控制器集线器。

[0034] 用于执行本发明的操作的计算机程序代码可以以一种或多种编程语言(包括诸如Java™、Smalltalk、C++、C#、Objective-C等的面向对象编程语言以及传统的过程编程语言)

的任何组合来编写。程序代码可以作为独立软件包整体在用户计算机上执行、部分在用户计算机上执行、部分在用户计算机上部分在远程计算机上执行或者整体在远程计算机或服务器上执行。在后者的场景中，远程计算机可以通过任何类型的网络(包括局域网(LAN)或广域网(WAN)，或者可以被形成的到外部计算机的连接(例如，使用互联网服务提供方以通过互联网))被连接至用户计算机。

[0035] 本领域技术人员将会意识到，图1-2中的硬件可以根据实施方式而更改。其它内部硬件或外部设备(诸如闪存、等同的非易失性存储器或光盘驱动器等)可以被用作为图1-2中所描绘的硬件的附加或替代。而且，说明性实施例的过程可以被应用于不同于之前所提到的SMP系统的多处理器数据处理系统，而并不超出所公开主题的精神和范围。

[0036] 如将会看到的，本文所描述的技术可以结合诸如图1所示的标准客户端-服务器范例进行操作，在该范例中客户端与在一个或多个机器集合上执行的互联网可访问的基于网络的门户通信。终端用户操作能够访问门户并与之交互的互联网可连接设备(例如，台式计算机、笔记本计算机、支持互联网的移动设备等)。通常，每个客户端或服务器机器是诸如图2所示的包括硬件和软件的数据处理系统，并且这些实体通过诸如互联网、企业内部网、外部网、私有网络或者任何其它通信介质或链接的网络相互通信。数据处理系统通常包括一个或多个处理器、操作系统、一个或多个应用以及一个或多个实用程序。数据处理系统上的应用为网络服务提供本地支持，其包括但不限于对超文本传输协议(HTTP)、文件传输协议(FTP)、简单邮件传输协议(SMTP)、简单对象访问协议(SOAP)、可扩展标记语言(XML)、网络服务描述语言(WSDL)、统一描述、发现和集成(UDDI)以及网络服务流程语言(WSFL)等的支持。关于SOAP、WSDL、UDDI和WSFL的信息可从万维网联盟(W3C)获取，其负责开发和维护这些标准；关于HTTP和XML的另外信息可从互联网工程任务组(IETF)所获取。假定对这些标准是熟悉的。

[0037] 云计算模型

[0038] 云计算是一种服务交付模式，用于对共享的可配置计算资源池进行方便、按需的网络访问。可配置计算资源是能够以最小的管理成本或与服务提供者进行最少的交互就能快速部署和释放的资源，例如可以是网络、网络带宽、服务器、处理、内存、存储、应用、虚拟机和服务。这种云模式可以包括至少五个特征、至少三个服务模型和至少四个部署模型，所有这些都在Peter Mell和Tim Grance在2009年10月7日所著的“Draft NIST Working Definition of Cloud Computing”中具有更为特别的描述和定义。

[0039] 特别的，以下典型特征包括：

[0040] 按需自助式服务：云的消费者在无需与服务提供者进行人为交互的情况下能够单方面自动地按需部署诸如服务器时间和网络存储等的计算能力。

[0041] 广泛的网络接入：计算能力可以通过标准机制在网络上获取，这种标准机制促进了通过不同种类的瘦客户机平台或厚客户机平台(例如移动电话、膝上型电脑、个人数字助理PDA)对云的使用。

[0042] 资源池：提供者的计算资源被归入资源池并通过多租户(multi-tenant)模式服务于多重消费者，其中按需将不同的实体资源和虚拟资源动态地分配和再分配。一般情况下，消费者不能控制或甚至并不知晓所提供的资源的确切位置，但可以在较高抽象程度上指定位置(例如国家、州或数据中心)，因此具有位置无关性。迅速弹性：能够迅速、有弹性地(有

时是自动地)部署计算能力,以实现快速扩展,并且能迅速释放来快速缩小。在消费者看来,用于部署的可用计算能力往往显得是无限的,并能在任意时候都能获取任意数量的计算能力。

[0043] 可测量的服务:云系统通过利用适于服务类型(例如存储、处理、带宽和活跃用户帐号)的某种抽象程度的计量能力,自动地控制和优化资源效用。可以监测、控制和报告资源使用情况,为服务提供者和消费者双方提供透明度。

[0044] 典型的,服务模型如下:

[0045] 软件即服务(SaaS):向消费者提供的能力是使用提供者在云基础架构上运行的应用。可以通过诸如网络浏览器的瘦客户机接口(例如基于网络的电子邮件)从各种客户机设备访问应用。除了有限的特定于用户的应用配置设置外,消费者既不管理也不控制包括网络、服务器、操作系统、存储、乃至单个应用能力等的底层云基础架构。平台即服务(PaaS):向消费者提供的能力是在云基础架构上部署消费者创建或获得的应用,这些应用利用提供者支持的程序设计语言和工具创建。消费者既不管理也不控制包括网络、服务器、操作系统或存储的底层云基础架构,但对其部署的应用具有控制权,对应用托管环境配置可能也具有控制权。

[0046] 基础架构即服务(IaaS):向消费者提供的能力是消费者能够在其中部署并运行包括操作系统和应用的任意软件的处理、存储、网络和其他基础计算资源。消费者既不管理也不控制底层的云基础架构,但是对操作系统、存储和其部署的应用具有控制权,对选择的网络组件(例如主机防火墙)可能具有有限的控制权。

[0047] 典型的,部署模型如下:

[0048] 私有云:云基础架构单独为某个组织运行。云基础架构可以由该组织或第三方管理并且可以存在于该组织内部或外部。

[0049] 共同体云:云基础架构被若干组织共享并支持有共同利害关系(例如任务使命、安全要求、政策和合规考虑)的特定共同体。共同体云可以由共同体内的多个组织或第三方管理并且可以存在于该共同体内部或外部。

[0050] 混合云:云基础架构由两个或更多部署模型的云(私有云、共同体云或公共云)组成,这些云依然是独特的实体,但是通过使数据和应用能够移植的标准化技术或私有技术(例如用于云之间的负载平衡的云突发流量分担技术)绑定在一起。

[0051] 云计算环境是面向服务的,特点集中在无状态性、低耦合性、模块性和语意的互操作性。云计算的核心是包含互连节点网络的基础架构。代表性的云计算节点如以上图2中所示。特别地,在云计算节点中具有计算机系统/服务器,其可与众多其它通用或专用计算系统环境或配置一起操作。众所周知,适于与计算机系统/服务器一起操作的计算系统、环境和/或配置的例子包括但不限于:个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任意系统的分布式云计算技术环境,等等。计算机系统/服务器可以在由计算机系统执行的计算机系统可执行指令(诸如程序模块)的一般语境下描述。通常,程序模块可以包括执行特定的任务或者实现特定的抽象数据类型的例程、程序、目标程序、组件、逻辑、数据结构等。计算机系统/服务器可以在通过通信网络链接的远程处理设备执行任务的分布式云计算环境中实施。在分布式云计算环境中,程序模

块可以位于包括存储设备的本地或远程计算系统存储介质上。

[0052] 现在参考图3，利用附加背景示出了云计算环境所提供的功能抽象层集合。首先应当理解，图3所示的组件、层以及功能都仅仅是示意性的，本发明的实施例不限于此。如图3所示，提供下列层和对应功能：

[0053] 硬件和软件层300包括硬件和软件组件。硬件组件的例子包括：主机，例如IBM® zSeries®系统；基于RISC(精简指令集计算机)体系结构的服务器，例如IBM pSeries®系统；IBM xSeries®系统；IBM BladeCenter®系统；存储设备；网络和网络组件。软件组件的例子包括：网络应用服务器软件，例如IBM WebSphere®应用服务器软件；数据库软件，例如IBM DB2®数据库软件。(IBM，zSeries，pSeries，xSeries，BladeCenter，WebSphere以及DB2是国际商业机器公司在全世界各地的注册商标)。

[0054] 虚拟层302提供一个抽象层，该层可以提供下列虚拟实体的例子：虚拟服务器、虚拟存储、虚拟网络(包括虚拟私有网络)、虚拟应用和操作系统，以及虚拟客户端。

[0055] 在一个示例中，管理层304可以提供下述功能：资源供应功能：提供用于在云计算环境中执行任务的计算资源和其它资源的动态获取；计量和定价功能：在云计算环境内对资源的使用进行成本跟踪，并为此提供帐单和发票。在一个例子中，该资源可以包括应用软件许可。安全功能：为云的消费者和任务提供身份认证，为数据和其它资源提供保护。用户门户功能：为消费者和系统管理员提供对云计算环境的访问。服务水平管理功能：提供云计算资源的分配和管理，以满足必需的服务水平。服务水平协议(SLA)计划和履行功能：为根据SLA预测的对云计算资源未来要求提供预先安排和供应。

[0056] 工作负载层306提供云计算环境可能实现的功能的示例。在该层中，可提供的工作负载或功能的示例包括：地图绘制与导航；软件开发及生命周期管理；虚拟教室的教学提供；数据分析处理；交易处理；以及其它(例如私有云中的企业特定功能)。

[0057] 首先应当理解，尽管本公开包括了对于云计算的详细描述，但是本文所叙述的教导的实施方式并不局限于云计算环境。相反，本发明的实施例能够结合现在已知或后续开发的任何其它类型的计算环境来实施。

[0058] 因此，代表性的云计算环境具有高级别功能组件集合，其包括前端身份管理器、业务支持服务(BSS)功能组件、操作支持服务(OSS)功能组件和计算云组件。身份管理器负责与进行请求的客户端接合以提供身份管理，并且该组件可以利用一个或多个已知系统(诸如可从纽约Armonk的IBM公司获取的Tivoli Federated Identity Manager(TFIM))来实施。在适当环境中，TFIM可以被用来向其它云组件提供联合单点登陆(F-SSO)。业务支持服务组件提供某些管理功能，诸如账单支持。操作支持服务组件被用来提供诸如虚拟机(VM)实例的其它云组件的供应和管理。云组件表示主要计算资源，其通常为用于执行对于经由云的访问可用的目标应用的虚拟机实例。一个或多个数据库被用于存储目录、日志和其它工作数据。所有这些组件(包括前端身份管理器)位于云“内”，但是这并非要求。在备选实施例中，身份管理器可在云外部被操作。服务提供方也可以在云外部被操作。

[0059] 一些云基于非传统IP网络。因此，例如云可以基于两层的基于CLOS的网络，其具有使用MAC地址的散列值的特殊单层IP路由。本文所描述的技术可以用于这样的非传统云。

[0060] 在非限制性实施方式中，代表性的平台技术是但不限于具有VMware vSphere 4.1

更新1和5.0的IBM的System x®服务器。

[0061] 代表性的云应用包括IBM的Sametime® Meetings、IBM的SmartCloud for Social Business等。

[0062] 云部署技术

[0063] 提供基于装置的解决方案以促进基础架构即服务和平台即服务供应的快速采用和部署是已知的。如上所述，一种这样的装置是IBM Workload Deployer(IWD)，并且该装置也被用来管理共享多租户环境，在共享多租户环境中隔离和安全极其重要。该物理装置(有时在本文被称作盒子)的安全性质通常由自行无效的开关所提供，其在装置盖子被移除的情况下被触发。这种物理安全使得装置能够充当证书的安全库，其能够贯穿其整个生命周期而被捆绑到虚拟镜像(在存储中、被分配、在云中运行或者从云中被移除)。IBM Workload Deployer还包含存储驱动器，其使得镜像定制的存储流线化。它还充当用于预先加载的和经定制的中间件虚拟镜像和模式的专用存储。装置还包括先进的压缩和存储技术，其使得大量这些虚拟镜像(每一个虚拟镜像的大小可设定)能够被存储。

[0064] 在操作中，装置能够供应标准的且定制的中间件虚拟镜像和模式，其能够在私有的或预置的云计算环境内被安全部署和管理。这些虚拟镜像能够帮助组织轻易且快速地开发、测试和部署业务应用，从而终止了经常与创建这些复杂环境相关联的人工、重复且易于出错的过程。在完成时，资源被自动返回至共享资源池以供未来使用，并且出于内部背后计费的目的而被进行记录。装置还管理个体用户和群组对资源的访问，这为IT管理员提供了以精细粒度级别优化效率所需的控制。

[0065] 通常，装置包括硬件和固件加密支持以对硬盘驱动器上的所有数据进行加密。该数据包括但不限于事件日志数据。包括管理用户在内的用户都无法访问物理盘上的任何数据。特别地，操作系统(例如，Linux)锁闭根帐户且不提供命令窗口，并且用户不具有文件系统访问。在管理员执行装置备份时，备份镜像被加密以保护数据的机密性。因此在恢复经加密的镜像时，需要解密密钥以对备份镜像进行解密以使得数据能够被恢复至装置。

[0066] 参考图4，代表性的操作系统包括物理装置400，其与云402接合。装置可以使用诸如以上关于图2所描述的数据处理系统来实施。优选地，装置400包括基于Web 2.0的用户界面(UI)、命令行界面(CLI)和基于REST的应用编程接口(API)。装置提供管理功能，其使能基于云的解决方案的快速部署。为此，装置提供了用于以下的存储：(i)用于管理用户和群组对资源的访问的数据404，(ii)预先加载和/或可定制的中间件虚拟镜像406，以及(iii)可配置模式和脚本包408。模式是包括特定解决方案的物理和虚拟资产的逻辑描述形式。如以下将更详细描述的，模式优选地根据云应用程序的拓扑结构和业务流程规范(TOSCA)规范进行构造。管理功能和接口提供了基于模板构建的方法，其允许快速创建和修改原本复杂的硬件和软件组件集合。特别地，模式的使用允许组织一次性地构建个体元素或集成解决方案，并且随后按需分配最终产品。通常，存在两种类型的模式：虚拟系统模式提供了这两种类型的最大灵活性和定制选项。其由操作系统以及潜在地附加的软件解决方案(诸如WebSphere®应用服务器)所构成。虚拟应用模式被优化并且通常出于支持单个工作负载的目的而被构建。

[0067] 还如图4中所看到的，中间件应用在其上运行的预置或私有云环境402通常构成被分配给该装置的超监督者、网络基础架构和存储设备。代表性的环境可以按照以上关于图3

所描述的方式来实施。

[0068] 图5图示了装置能够如何被用来构建定制私有云。在步骤1，标识用于云的硬件、超监督者和网络。在步骤2，用户选择并定制虚拟镜像。在步骤3，用户按照需要添加一个或多个脚本包以定制所部署的中间件环境。在步骤4，预先安装或定制的模式被用来描述所要部署的中间件拓扑。模式例如能够使用拖放接口而从虚拟镜像被构建。在步骤5，虚拟系统被部署至云。

[0069] 本文对IBM Workload Deployer的引用是示例性的，并不应当被理解为对所公开的技术进行限制，上述技术可以在具有一般特性以及已经描述的操作功能的任何装置(或者更一般地，机器)上实施。针对IWD的具体应用应当被理解为包括以上所标识的产品，以及实施以上所提到的功能的其它技术。

[0070] 作为附加的背景，云应用程序的拓扑结构和业务流程规范(TOSCA)是为了增强云应用和服务的便携性所设计的规范。其使能独立于创建服务的供应方以及任何特定的云提供方或托管技术而对应用和基础架构云服务、服务各部分之间的关系以及这些服务的操作行为(例如，部署、修补、关闭)的可协作的描述。除其它益处之外，TOSCA使能便携部署到任何兼容的云，并且促进现有应用到云的平滑迁移。使用TOSCA，云应用能够在来自多个供应商的产品和云平台间无缝地建模、分享、部署和管理。

[0071] TOSCA文档是描述要被部署至云的应用组件以及它们的相互关系的描述符。在描述符中，每个应用组件通常由标识符唯一标识，标识符由组件的名称、版本、架构以及供应商所组成。标识符被用作关于信息数据库的搜索关键词；如以下将会描述的，一种这样的数据库是针对该具体应用组件的已知缺陷和/或漏洞的数据库。

[0072] 提供实施兼容TOSCA的解决方案的云管理平台是已知的。作为一个示例，云管理平台是IBM® SmartCloud® Orchestrator开放云管理平台，其对诸如OpenStack和OSLC(生命周期协作的开放服务)的附加标准技术进行了权衡。这种类型的管理平台通常包括三个主要功能层：基础架构服务层，其优选地基于OpenStack，用于供应、配置和管理存储、计算和网络资源；平台服务层，其包括虚拟机镜像生命周期管理能力和模式服务；以及编制服务层。如上所述，“模式”为业务服务提供部署和管理指令。模式优选地是供应和管理具体应用(或应用类型)工作负载的各种资源(例如，计算、网络、存储、OS、中间件等)所需的基础架构配置的基于XML的定义。编制服务层提供了业务过程管理的解决方案。

[0073] 当然，以上所描述的云管理环境并非旨在作为限制，因为本文的技术可以在其它(开放、封闭或混合)环境中实施，和/或使用其它部署技术(无论是开放或专有的还是混合的)来实施。

[0074] 基于上下文的云安全保障服务

[0075] 利用以上内容作为背景技术，现在对本公开的主题进行描述。主题有时在本文被称作“基于上下文的云安全保障服务”或“安全保障服务或系统”，或者作为简写仅“服务”或“系统”。并非作为限制，主题可以在如已经描述的云部署平台系统或装置(图4)内实施或者与之相关联地实施，或者使用任何其它类型的部署系统、产品、设备、程序或过程来实施。可以被利用来实施安全保障服务的代表性的云能用平台包括但不限于IBM® SmartCloud Orchestrator，其如以上所提到的是为了运行应用而专门设计并调谐的平台系统，并且支持模式的使用以快速部署到其云环境之中。对该商业系统的引用并非旨在作为限制，因为

本公开的安全保障服务可以与任何云基础架构进行协作。

[0076] 本文的技术可以被实施为管理解决方案、服务、产品、装置、设备、过程、程序、执行线程等。通常，该技术在软件中被实施为关联于在一个或多个数据源(诸如问题数据库)中所存储的数据而在硬件处理元件中执行的一个或多个计算机程序。所描述的处理步骤的一些或全部可以是自动的并且关联于其它系统而自主操作。自动化可以是完全或部分的，并且操作(整体或部分)可以是同步或异步的、基于需求的或者为其它方式。

[0077] 以下是云安全保障服务的高级别描述。通常，服务一般操作以收集(或者以其它方式从其它数据源获取)有关可用云平台、拓扑和能力的信息。服务还标识可设置的安全能力。这些安全能力包括但不限于虚拟周边网络(DMZ)、网络分隔、存储隔离、入侵防止系统(IPS)部署、安全信息和事件管理(SIEM)部署、反向代理、防火墙、加密套接字协议层(SSL)通信、现有SIEM的配置、多因数认证、基于风险的认证等。优选地，服务将可用能力简化(或抽象)为针对环境的现有拓扑的易于理解的安全保障类别。

[0078] 保障服务(在应用部署期间)将多个类别作为“模板”展现给用户。优选地，服务被部署有默认模板集合。优选地，模板定义了特定安全保障级别的要求，例如，“中度安全”模板可能包括以下经指定的要求：“SSL、SIEM、IPS、磁盘加密、多因素认证、无资源分隔和隔离”。(服务的)安全管理员后来可能改变默认模板集合(通过添加不同模板)，或者可能更改现有模板的配置以添加或移除要求。然而，优选地，安全保障服务不需要解释模板的具体要求；相反，如以下将更为详细描述的，安全保障服务对特定部署形式的“上下文”进行解释以作出关于哪些安全资源(和/或它们的特定设置)满足模板的要求的确定。在该方法中，模板(例如，由安全专家)被加载到保障服务，并且旨在对于系统是高度指导性的。在使用中，模板优选地以诸如“高安全”、“中安全”或“低安全”的简化名称(或标识符、描述符等)被展现给终端用户。优选地，这些术语被(差不多逐字地)呈现给终端用户。并不要求终端用户理解作为该模板所表示的安全保障级别底层的资源(或者它们的操作特性)。然而，系统理解这些细节并且操作以应用具体能力和控制而将用户所选择的规范(例如，“高安全”)转换为粒度要求。该有意简单的终端用户术语可能以按钮或其它控件的形式被展现给终端用户，并且如所提到的，呈现给终端用户的术语形式并非旨在描述预期提供安全保障级别的特定底层要求或资源。相反，终端用户仅需要了解他或她想要为部署的应用实施什么总体保障级别。

[0079] 基于所指定的要求，模板具有与之相关联的一个或多个安全配置更改的给定集合。如将要描述的，终端用户(通常是应用开发方)选择他或她想要服务配置/供应应用所依照的这样的安全模板中的一个或多个。服务可以在该方面向用户提供推荐。基于用户选择，服务随后解释所请求的一个或多个安全保障模板，并且作为响应，服务生成一个或多个安全配置更改(通常是对现有安全基础架构的安全设置的更改/更新)的具体列表。可选地，服务还向(多个)安全管理员生成具有被用于应用的能力的注释。在应用部署期间，服务优选地使用基于REST的(或等同形式)接口对现有(经配置的)安全产品应用安全更改；并且除此之外，如为了满足(多个)模板所规定的安全保障级别所必要的，服务还可以部署新的安全软件实例(作为可适用的并且如果许可可用)。此外，同样如为了满足所选择的安全保障级别所必要的，服务还可以根据应用需要优选地使用现有的云设施来供应硬件和网络环境。以这种方式，安全保障服务针对被部署的应用创建特定于上下文的安全云应用区域。优选

地，应用部署平台在安全配置更新完成时被收回；平台随后完成部署。新部署的且安全的应用随后被激活(可能由服务直接激活)。

[0080] 如所描述的，本文所描述的保障服务优选地以基于上下文的方式进行操作，其将要在其中部署应用的“上下文”纳入考虑之中。代表性的“上下文”信息包括但不限于目标平台的性质、工作负载预期在其中被执行的环境的性质、针对工作负载的任何兼容或其它管理要求的性质、任何公司安全要求(由管理员所配置)、将要或可能影响安全资源如何与应用交互的所部署应用(软件、配置、拓扑等)的上下文等。因此，例如，如果工作负载被部署在Amazon®云(其是公共的)上，则服务可能考虑公共云的要求(诸如针对所有流量的SSL通信)，即使这样的要求在私有云中并不必须被实施。作为另一个示例，如果工作负载在测试或开发环境中运行，则服务可以仅供应围绕数据的最小控制，因为(该上下文中的)应用将不会处理真实(实况)的消费者数据。作为又另一个示例，如果工作负载需要兼容外部控制器接口(PCI)，则服务可以供应仅处于某些网络上而并不允许(或以其它方式阻止)工作负载移动至非安全的网络或虚拟局域网(VLAN)的工作负载。显然，以上仅是代表性示例。优选地，安全上下文信息被安全保障服务直接收集，或者使这样的信息对于来自具有该信息(或访问那样的信息)的其它经连接的数据源的安全保障服务是可用的。

[0081] 图6图示了根据一个实施例的本公开的云安全云保障服务600的基础组件。附图标记601图示了云平台以及在云平台上运行的系统(即，消费者工作负载)。云平台及其相关联的消费者工作负载被保障服务所保护，保障服务提供管理被(多个)应用部署到该平台所影响的所有(或者所定义的一些)安全资源的集中的或联合的服务。这些资源可以非常多变，并且除其它之外包括反向代理、HTTP服务器、授权更新、新标识添加、VPN供应、与SIEM解决方案的日志整合、DMZ、针对开放端口的防火墙配置等等。如将要描述的，优选地，服务调用远程接口(例如，基于REST的接口)以更新针对安全资源的配置。哪些安全资源被更新以及如何更新的确定取决于如所描述的基于模板的方法。在云平台上执行的各种工作负载603通常由(多个)云平台消费者提前建立。云平台由诸如IBM Pure™、Amazon®网络服务、VMWare®的图标所表示，它们仅是代表性的。

[0082] 云安全保障服务600包括上下文监测器组件(或“上下文监测器”)605，其操作以向云平台查询可用的能力，并且在保障服务数据库607中将它们编入目录。在操作中，上下文监测器605使用云提供的应用编程接口(API)查询云平台601以确定可用的资源，因为云平台通常以这种方式展现该信息。上下文监测器随后将可用软件映射至安全能力。产品至能力的映射可以由云平台直接提供，或者该知识可以被嵌入到保障服务数据库607中。因此，例如，云平台可以包括供IBM QRadar，其提供了SIEM能力。保障服务包括配置信息，其指定了哪些安全保障级别要求哪些特定能力。因此，例如，“高”或“中”的保障级别可以要求SIEM解决方案，而“低”级别则并不要求。如以上所提到的，针对特定安全保障级别的(多个)要求优选地(由安全专家)提前被链接至预定义模板。如所描述的以及在该特定示例场景中，当终端用户挑选特定的安全解决方案(例如，“高”)时，安全保障级别对云平台进行权衡以安装产品(或者在已经安装的情况下调整其安全设置)以满足该安全级别的SIEM要求。

[0083] 为此，服务600提供了安全保障模板602。如上所述，优选地，模板602的默认集合由服务所提供，并且每个模板定义特定安全保障级别的要求。通常，模板将具有不同类型或类别。如所解释的，模板(对于系统)是高度指导性的，其中其包括安全保障级别的经定义的要

求集合。因此，“中度”安全级别可以在定义了诸如“SSL、SIEM、IPS、磁盘加密”等的要求的模板中被指定。优选地以及如以上所描述的，服务并不需要解释这些要求；相反，服务解释特定部署形式的“上下文”(如上下文监测器组件所指定或确认的)以作出有关哪些安全资源(或者它们的设置)满足这些要求的确定。优选地，(多个)模板被预先配置。模板602的集合可以被增加以附加模板，或者特定模板的要求可以按照需要被调整。

[0084] 优选地，并如本文所使用的，安全保障模板602是提供易于理解的安全类别或简档以及它们的相关联安全级别(诸如“高/中/低内部网络安全”以及“高/度/低内部防火墙安全”等)的服务内的模块。服务600还包括保障配置代理器604，其标识经选择的模板的安全目标，并且操作以优选地基于系统配置和可用资源的上下文而将对模板的选择转换为详细配置步骤。转换操作在下文被更详细地描述。此外，服务优选地包括(或者具有与之相关联)安全管理接口608(例如，云工具作业UI，诸如IBM SmartCloud Orchestrator)，其是被用来添加或移除安全模板、提供被管理的安全资源的人工配置、和/或(在允许的情况下)覆盖终端用户所选择的安全模板的配置点。安全保障服务还包括云安全过程工作流程610，其是调用适当(例如，基于REST)接口以按照配置代理器604的指示应用改变到底层安全基础架构(安全资源)的模块。提供管理接口的保障模式模块612是特定于云的服务，其协调应用部署和供应安全保障服务600。通常，保障模式模块612包括云应用平台的管理接口组件，虽然并非要求如此。保障模式模块612基于被部署的应用而向保障服务查询可用保障模板602。

[0085] 在图6中，位于左上方的应用所有者/管理员表示(多个)应用部署方；这些是仅需要使用易于理解的安全保障级别模板(按照类别/安全级别)的个体。位于左下方的云团队或其它管理员则表示创建模板或者被提供以添加新的模板和/或修改预先配置的模板中的特定要求的能力的个体。云团队或其它管理员通过管理接口与系统或服务交互。每个以上所描述的组件通常被实施为软件，即被实施为在一个或多个硬件处理器中执行的计算机程序指令的集合。组件被示为是不同的，但是并非要求如此，因为组件也可以整体或部分地相互集成。组件的一个或多个可以在专用位置执行，或者远离彼此执行。组件的一个或多个可以具有共同执行以提供功能的(多个)子组件。并不要求安全保障服务的特定功能由如以上所提到的特定组件执行，因为本文的功能(或者其任何方面)可以在其它系统中实施。

[0086] 安全保障服务可以由云服务提供方所实施，其操作用于私有云、公共云或混合云的基础架构。安全保障系统部署并管理安全基础架构。优选地，并如以上所描述的，保障系统通过管理接口与云的安全管理员(等)交互，并且通过云工具作业UI与应用所有者交互。优选地，应用所有者主要与云工具作业UI(参见图7，其仅是代表性的)交互以定义高级别安全要求并且部署应用。图7代表编辑器，其是基于网络的，但是编辑器(或者促进模板以所描述方式呈现和管理的等同应用)的特定实施方式可以是任何类型。

[0087] 使用云工具作业UI(或者其等同)，用户还可以查询云应用环境(例如，请求有关被部署的应用的细节)，并且作为响应接收有关在云应用环境中可用的一个或多个可用安全能力(例如，适用于被部署的应用的特定安全资源)的信息。这些能力例如可以包括可用硬件、可用软件、现有许可和可用许可。

[0088] 因此，如已经描述的，不同类型的用户可以以不同方式与服务交互。在一个实施例中，第一类型的用户(例如，应用所有者)通过查看模板以及与之交互而利用服务工作，而第二类型的用户(例如，安全管理员)则通过查看一个或多个安全管理视图(例如具有与第一

类型的用户的模板选择相关联的安全更改)和与之交互而利用服务工作。安全管理视图使得系统能够接收来自安全管理员的输入,其可以触发有关云应用环境中的一个或多个安全能力的配置的一个或多个安全管理动作的实施。这样的输入例如可以包括批准未决的安全配置更改的输入、覆盖第一用户对模板的选择的输入、或者覆盖与模板相关联的安全能力的选择的输入、或者当具有与其相关联的最低安全保障级别的模板尚未被第一用户选择时禁止将应用部署到云应用环境之中的输入等。安全管理视图还可以提供一个或多个附加管理功能,例如:配置新模板或修改现有模板、使用安全分析来基于企业安全政策管理应用程序部署、定义针对云应用环境的安全要求、审计在云应用环境中可用安全能力等。在一个实施例中,在安全管理视图中所接收的输入启动云应用环境的安全扫描,然后可以向管理员呈现安全扫描的结果(例如,任何安全能力差距分析)。作为另一种使用情形,还可以使用输入将经升级的模板追溯地应用于已经在云应用环境中被部署的现有应用。

[0089] 在一个特定(但非限制性的)实施场景中,企业具有由云应用平台管理的相关联的私有云(在云服务内实施)。平台随后可以被增加以与本公开的安全保障服务协同操作(或实际包括安全保障服务)。

[0090] 更一般地,安全保障服务可以由企业以独立方式来实施。其可以作为云服务或其它服务提供方所提供的经管理的服务而获得。

[0091] 如所描述的,服务优选地通过使终端用户提供安全级别的一般规范(例如,“高网络安全”)来操作,服务然后(在解释应用要求和可用资源之后)使用该一般规范以为应用生成安全优化部署。通常,如上所述,应用被部署到现有环境中,并且安全保障服务操作以定义和/或裁剪(应用将被部署的)现有环境所需的安全配置更改。应用的安全优化部署有时在本文被称为基于安全上下文的“云应用区域”。

[0092] 如所描述的,如本文所使用的“安全级别”有时被称为“安全保障级别”。如上所述,与安全专家可能已知或可用的更精细粒度的具体说明相比,这些级别被展现为易于理解或“粗糙”粒度的描述符(“高”或“低”)。术语“粗糙”或“精细”是相对的短语,但是安全保障级别的“粗糙”指定的概念是仅提供可能不知道或不能够弄清(或关心)特定“粗糙”安全保障级别的底层明确安全要求的用户所能够获得的基础信息的级别。在这种情况下,用户(应用所有者)只要知道他或她(针对特定分类)所期望的安全级别是“高”或“低”或一些其他这样的分类(不管如何描述)就足够了。因此,术语“高”(关于特定的粗糙安全保障级别)可以备选地由数值、一些其它标识符或名称进行指定。然而,如所解释的,这些术语旨在被差不多逐字地呈现给终端用户。系统随后应用具体的能力和控制以将用户所选择的安全解决方案转换为底层安全资源的粒度要求。指定解决方案的优选方式是通过按钮或其它一般的显示制品。

[0093] 在代表性的实施例中,服务展现、提供安全模板集合或者与其交互操作,安全模板可以根据类型进行分类。这些模板由图6所示的保障模板模块所提供。因此,例如,服务可以展现具有以下类别的安全模板:“内部网络安全”、“应用安全”、“数据安全”和“入侵者保护”。这些仅仅是代表性的。随后可以根据定义的安全级别(例如“低”或“高”)来标识特定模板类别。服务可以仅提供“低”或“高”模板,或者可以提供另外的级别(例如,低、中和高,或者另外更为具体的级别等)。因此,被部署的特定企业应用可以具有与其相关联的一个或多个这样的安全模板,每个模板定义一个类别以及所指定的安全级别。因此,例如,所部署的

特定应用可以具有以下规范:内部网络安全(低)、应用安全(高)、数据安全(高)和入侵者保护(高)。可以使用基于网络或其他配置接口来指定与被部署的特定应用相关联的一个或多个安全模板。该接口可以与诸如IBM®工作负载部署器虚拟应用生成器(Workload Deployer Virtual Application Builder)的常规工作负载部署工具相关联。图7图示了用于此目的的代表性用户界面,其可以包括安全管理界面的部分(参见图6)。如上所述,该界面提供了添加或移除安全模板、提供被管理的安全资源的手动配置、或者(如果已配置)覆盖由终端用户选择的安全模板的配置点。在备选实施例中,类别和安全级别被自动地或以编程方式定义,或者这样的信息可以从另一个来源所公布的这种数据的库集获得。

[0094] 如已经描述的,模板定义了提供具体"安全保障"级别的要求集合,随后保障级别关于一个或多个安全资源被实现或实施。安全资源可以是安全基础架构内的系统、设备、装置、程序、过程或者其它计算实体。优选地,安全保障服务解释部署的上下文以作出有关需要什么安全资源(以及其中的什么设置)来满足特定模板的要求的确定。因此以及至少部分地基于特定部署上下文,安全模板具有与之相关联的针对上下文实施该类别(以及处于所指定的级别)的一个或多个安全配置(安全资源设置)。优选地,如上所述,这些安全配置由安全保障配置代理器组件(参见图6)所标识,其采用所选择模板的总体安全目标(作为输入),并且基于系统配置和可用安全资源的上下文(如上下文监测器所提供)将该选择转换成详细的配置步骤(或更改)。

[0095] 因此,例如,如果应用类别是"内部网络安全"并且安全级别为比如说"低",则代理器确定实施该模板所必需的详细安全步骤可能包括:(i)基于应用端点在前端代理服务器和后端Web应用服务器之间创建"连结",(ii)对该连结使用基础认证,并且在应用服务器中针对单次签入登录(SSO)配置信任关联拦截器(TAI),(iii)启用限制性防火墙并且打开到应用端点的端口。作为另一个示例,如果应用类别是"应用程序安全"而安全级别为比如说"高",则实施该模板所必需的详细安全步骤可能包括:(i)针对端点运行安全分析工具(例如AppScan),并且在标识出任何危险缺陷的情况下中止部署,(ii)指示云应用平台供应VPN以在云中托管应用程序,(iii)为应用所定义的经授权的角色配置访问管理器政策,以及(iv)在专用于应用的云中创建附加的基于软件的DMZ。作为又另一个示例,如果应用程序类别是"数据安全"并且安全级别为比如说"低",则实施该模板所必需的详细安全步骤可能包括(i)更新应用服务器以使用到数据库等的SSL连接。作为又另一个示例,如果应用类别是"入侵者保护",并且安全级别为"高",则实施该模板所必需的详细的安全步骤可能包括:(i)配置安全智能平台(例如,IBM® QRadar)日志源,(ii)更新用于应用的SIEM过滤器,以及(iii)更新用于应用的IPS规则。当然,这些只是安全配置更改的代表性(非限制性)示例。安全保障服务所实施的特定更改将取决于实施方式和可用资源(产品、系统、配置等)。

[0096] 因此,根据本公开,当云提供方部署应用(或启动部署)时,其向安全保障服务通知一个或多个经选择的(或以其它方式所定义或规定的)安全模板。优选地,云提供方还发送应用的保障服务细节。安全保障服务将被选择的模板作为指导,并且代理器组件随后对现有环境所需的详细安全配置更改进行裁剪以在已被指定的经选择的安全约束以及可用资源(由上下文监测器所确定的)的上下文内支持该应用。如果需要,这些安全配置更改可以在实施之前被呈现给安全管理员以验证。在验证时(如果该可选操作被实施),安全保障服务优选地调用远程接口进行软件配置。此外,如果有必要,服务与云提供方通信以获取关于

在部署应用时可能需要解决的(云提供方的)任何先决条件的信息。这些先决条件例如可以包括创建VPN或者提供方所特有的其它安全要求。

[0097] 模板还可以包括其它信息,诸如与特定安全能力相关联的成本信息。模板中的成本信息可以被导出为与云应用环境中的一个或多个安全配置更改的集合相关联的一个或多个成本的估计。成本信息也可以例如基于云应用环境中的安全能力的更改成本或者作为其它所变化条件的结果而不时地进行调整。当系统展现这样的成本信息时,优选地,由(例如,由一个或多个用户)对模板的选择所产生的成本信息可以被收集并且在编辑器(或一些其它应用)中的适当显示视图中被呈现给经允许的个体。

[0098] 系统(例如,UI编辑器)还可以提供接收设置一个或多个安全更改的安全成本的信息的能力。基于该信息,可以对展现给用户的模板集合进行调整。

[0099] 以下仅用于说明目的而提供对代表性使用情形的描述。该示例场景的细节并非旨在是限制性的,并且所有产品和服务都仅用于讨论的目的。如图8所示,企业(Acme银行)具有在私有云环境中实施的生产区800。该私有云可以经由位于一对防火墙804和806之间的DMZ 802而从互联网进行访问。根据本公开,安全区808托管安全保障服务810。如所示出的,假设该企业还具有已经部署的安全软件综合套件。例如,该套件包括用于访问管理的IBM安全问管理器(ISAM)812、用于身份管理的IBM安全身份管理器(ISIM)814、IBM安全网络网关设备(用于安全代理的DMZ)816、用于用户存储的IBM DB2数据库818、IBM PureApplication上托管的IBM QRadar SIEM 820、标准化云应用平台822、IBM Security AppScan 824以及DMZ 802中的网络IPS 826。Jane 828是Acme的应用开发方/管理员,其职责在于部署PocketBookTM应用830。为此,Jane使用云应用平台工具构建了包含适当企业节点(例如,用于各种组件或应用实例的Red Hat企业节点(RHEL)(诸如(在该示例情形中)用于WebSphere应用服务器(WAS)实例的节点832,用于IBM HTTP服务器(IHS)实例的节点834、以及用于IBM DB2实例的节点836等))的虚拟系统。虚拟系统优选地涵盖了针对Acme私有云中的应用功能和可扩展性(针对新应用)的碎片需求。然而,在该示例场景中,假设Jane创建的云模式并未覆盖或以其它方式表明保护是面向外部的网络应用所需要的安全碎片。因此,将需要本公开的安全保障服务。

[0100] 如同样在图8中所能够看到的,John 838是Acme的安全架构师,其职责在于公司生产系统的安全。为了协助系统范围的配置,John部署了本公开的安全保障服务810(例如参见图6),并且特别地,他配置管理云中的所有基于软件的安全相关资源的服务,以及与现有部署((在该示例场景中)诸如ISAM、ISIM、Web安全网关、QRadar、AppScan和IPS)的集成。当Jane 828使用云模式编辑器(由PureApplication系统822所提供)以准备用于部署的PocketBook应用830时,假设她不熟悉安全部署的内部工作从而无法对那些安全拼图的碎片进行正确配置。然而,Jane知晓(或要求)应用针对与互联网的任何通信需要是高度安全的,但是关于来自内部网络的请求方面则可能不那么安全。使用本公开的技术,Jane选择为该新部署的应用创建安全云应用区域所需(或所期望)的一个或多个安全模板。如上所述,安全保障服务可能与其它云部署工具作业进行整合,而使得在部署期间,Jane能够从其它部署模块旁边的一个或多个易于理解的安全保障模板中进行选择(例如参见图7)。在该示例中,假设Jane已经选择了图7所示已经上文所描述的四个模板。如以上所解释的,安全保障服务在定制现有环境(图8)所需的详细安全配置更改时采用所选择的模板作为指导。随

后利用其基于上下文的安全保障将应用部署在所配置的云应用区域之内。

[0101] 图8图示了详细的操作步骤。在步骤(1)Jane使用应用服务器接口创建用于部署PocketBook应用830的模式。在步骤(2)，云应用平台向安全保障服务810查询可用保障模板的列表。该查询包括有关经部署的应用的信息(例如，“具有单一上下文根的J2EE应用程序，构建于WebSphere应用服务器(WAS)上并使用DB2”)。给定该规范，安全保障服务810在步骤(3)继续提供“内部网络安全”、“应用安全”、“数据安全”和“入侵者保护”以及针对其中每一个的“高”或“低”的安全级别选项(参见图7)。安全保障服务所返回的(多个)类型(及其级别)可能会根据所指定的应用、可用资源等而变化。在步骤(4)，云应用平台在配置器(例如，IBM Workload Deployer模式构建器)中显示简单的安全模板以用于简单的用户选择。在步骤(5)，Jane选择四个模板，这例如基于她的以下一般感觉：内部网络是安全的，而频繁的攻击和高级持续威胁(APT)可能来自外部网络。在步骤(6)，优选地在应用部署时，云应用平台将经选择的安全模板优选地与被部署的应用的细节一起传送到云服务。在步骤(7)，安全保障服务生成配置步骤的列表，并将该列表呈现给John以进行确认。向John(与Jane相对的，或者其他人)呈现该列表并不是一项要求，但是其可能是典型使用情形。在步骤(8)，安全保障服务远程地应用配置更改以为所要部署的应用创建特定于上下文的安全云应用区域。在步骤(9)，当区域创建完成时，安全保障服务通知云应用平台(例如，通过回呼)配置设置完成，并且云应用平台可以继续部署过程。部署由云应用平台以通常方式完成。

[0102] 并非旨在作为限制，在该特定示例情形(涉及PocketBook应用)中，安全保障服务应用了多种配置更改，并且这些在上文被详细描述。因此，例如，在子步骤(8.1)，服务在Web安全网关816中为新的应用端点创建WebSEAL连结。在子步骤(8.2)，服务配置该连结和WAS实例832以使用针对内部通信的基础认证。在子步骤(8.3)，服务在新部署的RHEL实例上启用防火墙，这仅打开所需的端点端口。在子步骤(8.4)中，服务针对新部署的应用运行AppScan824(如果需要在沙箱中)，并且报告回用户或安全管理员。在子步骤(8.5)，服务为新部署供应VPN，例如通过PureApplication系统822。在子步骤(8.6)，服务为经授权的用户更新访问管理器812以使用新应用。在子步骤(8.7)，服务更新DB2 818和836以使用来自WAS的SSL连接。在子步骤(8.8)中，服务配置来自DB2、RHEL实例、WebSEAL和WAS的QRadar 820日志源。在步骤(8.9)，服务针对新应用更新QRadar规则。在步骤(8.10)，系统针对新应用更新IPS 826规则以完成特定于上下文的云应用安全区域的配置。

[0103] 如图8所示的特定配置形式以及配置更改和步骤的顺序仅是示例性的。如本领域技术人员将会意识到的，如果选择了不同的安全模板，和/或如果有不同资源可用，则各种配置更改的性质和序列当然将会相应地变化。

[0104] 下文对本公开的安全保障服务的代表性的或另外的能力进行描述。可以按照期望而提供这些附加能力中的一个或多个。

[0105] 云安全保障服务可以分析现有的安全环境以标识用于经定制的配置步骤的交互，例如，服务可以确定虚拟专用网(VPN)在特定配置中可能并不是必需的，因为该网络已被一些其它设备、网络或机制所隔离。

[0106] 安全保障服务可以操作以基于其它部署来更新配置。因此，例如，如果网络安全网关被部署并已经针对其它应用使用了证书，则安全保障服务可以识别该情况并且仅对新部署的应用进行升级以同样使用证书。

[0107] 优选地，系统中(例如，在模式编辑器中)可用的安全模板可以包括连线和交互逻辑。在终端用户的所见即所得类型的编辑器的上下文中，连线是指连接两个要素(例如，通过在它们之间绘制一条线)，并且是终端用户在他或她的应用上添加安全功能的方式。如图7中所看到的，PocketBook应用连线到数据库。优选地，在编辑器中显示的安全框具有一些相关联的元数据(可能是隐藏的)，其可以被用于确定多个框如何交互。作为一个简单示例，如果已经选择了高级别的“入侵者保护”模板，则元数据可以禁止这种类型的较低级别的模板被应用。作为另一个更为复杂的示例，安全管理员可能已经设置了网络必须至少与其所托管的应用一样安全的政策；那么，如果用户选择了高级别的数据安全，则可以将内部网络安全自动升级(例如，在模式编辑器中)为高级别。或者，在后一种情况下，系统可以禁止用户尝试将“高应用安全”框与“低应用安全”框连线在一起。概言之，根据元数据，可以允许或不允许用户对元件进行连线的尝试。

[0108] 因此在编辑器的典型使用情形中，第一模板已经被选择。响应于用户选择第二模板以及将第二模板连线至第一模板的指令，关于一个或两个模板可应用的安全限制然后被被实施。

[0109] 优选地，安全管理员直接与安全保障服务交互以向现有的部署应用模板，例如，以针对可能经被攻击的应用升级安全设置。

[0110] 优选地，服务使安全管理员能够覆盖特定分类。作为非限制性示例，即使是关于原本“低级别”的安全类别，高安全的银行网络也可以需要更高级别的控制。

[0111] 优选地，安全保障服务记录配置设置，并且可以在从系统移除应用时移除安全配置步骤。这种安全“移除”功能优选地还与其它系统交互，例如，如果其它应用的安全已经仅针对经移除的应用进行了升级，则可选地对它们的安全级别进行降级。

[0112] 优选地，安全管理员被提供更改服务中可用的安全模板的能力，以及更改在某种环境中哪些模板必须被使用的规则的能力。

[0113] 优选地，安全保障服务与一个或多个云平台交互以管理虚拟化的资源。因此，例如，安全保障服务可以查询企业中的现有软件目录以确定所安装的安全软件以及它们的位置和可用资源。服务还可以尝试在网络中自动发现软件，或者可以查询具体的安全解决方案(诸如日志管理器)以发现系统中所安装的其它软件。

[0114] 优选地，如果所关心的是来自高级别安全选项的资源消耗，则安全保障服务可以估计所选择的(多个)安全模板的总体成本并且将该信息呈现给应用部署方以供批准。或者，安全专家可以选择性地配置特定类型的应用所允许和要求的“最大”和“最小”总体安全级别。

[0115] 优选地，安全管理员能够使用安全保障服务以防止应用在最小安全级别尚未被选择的情况下被部署。

[0116] 优选地，安全保障服务能够挖掘应用部署和通常选择的安全级别之间的模式以为被部署的新应用自动建议安全级别。

[0117] 优选地，安全保障服务能够在应用部署期间与安全分析系统或服务(例如，Rational AppScan)交互或协同操作以测定被部署的应用的整体安全级别并且确定其在企业安全政策内是否适合。

[0118] 服务优选地还人工或自动地(例如，通过自动更新工具)提供安全保障模板的“补

丁”以基于经选择模板改善安全推荐，并且向现有应用追溯地应用新的安全配置。

[0119] 优选地，服务能够接收描述常见易损性或攻击模式文件(流入，APT模式)的报告或其它输出，并且确定这样的攻击是否利用现有安全配置而被防止。在可能暴露于攻击的情况下，服务随后生成并可选地应用配置更改以保护该环境。

[0120] 如上文所提到的，优选地，安全保障服务结合或关联于现有的云应用平台基础架构进行操作，云应用平台基础架构包括但并不限于具有工作负载部署功能的云应用平台。以这种方式，安全保障服务跨云基础架构补充或工作以促进基于安全上下文的应用部署。

[0121] 在图8的示例场景中，安全模板及其相关联的安全配置更改在应用部署过程期间被实施。在该示例中，应用部署被启动，随后安全配置更改被执行，此后预期进行该应用部署过程的其余部分。虽然这是一种典型的操作场景，但是安全配置更改可以与实际部署自身正交地实施。因此，例如，安全配置更改可以在启动实际应用部署之前的离线处理中被实施。在备选中，应用部署可以被启动并完成，并且随后是安全保障服务的单独执行线程。因此，可以在实际应用部署之前、期间或之后来创建给定的基于上下文的云应用安全区域。

[0122] 针对(如特定安全模板所标识的)一个或多个安全资源实施安全配置更改所需的工具作业可以由模板直接或间接地指定或控制。

[0123] 如上所述，经允许的管理员可以具有直接更新模板的能力。更常见的，可能期望定义与模板分离的安全政策。例如，“低”数据安全模板可能只需要SSL，但是管理员可能已经将保障服务(作为政策)配置为无论所选择模板如何针对所有部署都要求比如说磁盘加密。功能上，这相当于如所描述的管理员更新模板。因此，在备选实施例中，这样的管理员更改被存储为与模板分离的政策。随后，为了确定如何创建安全区域，系统检查可用软件和模板要求的引用以及管理员设置。这样的政策可以是系统范围的，或者它们被限定到某些领域，例如在某个云上运行的所有工作负载、或者建立在某些软件上的所有工作负载等。

[0124] 上述主题提供许多优点。特别地，本公开的以上描述和所说明的技术提供了一种跨系统的、基于模板的方法以使用应用的分类和部署技术来安全地将应用供应到环境中，利用该应用和部署拓扑所必需和/或合适的安全设置更新所有或相关的安全基础架构(例如，防火墙、事件记录器、目录、反向代理等)。这种基于模板的方法优选地依赖于抽象的或“广义的”类别，服务以“遮盖之下”的必要配置更改的形式自动提供高级配置。

[0125] 本文的方法提供集中的或联合的安全保障服务，其管理并供应应用安全所需的硬件、软件、网络和云资源。所描述的技术利用抽象的保障安全模板来增强应用开发。模板优选地是基于上下文的，其源于有关可用资源和所期望安全目标的信息。可以基于环境中的安全软件的可用性和/或与应用和中间件的属性相结合而容易地定制安全模板的列表。服务还对抽象的经合并的模板进行解释以生成具体的配置步骤。服务分析现有的安全和云环境以标识针对所定制的配置步骤的交互。服务为新部署的应用生成端到端的软件定义的安全环境。如果服务被新应用的安全要求所影响，则升级其它应用的安全。服务使得能够自动创建应用安全要求所需的安全解决方案，诸如创建VPN或DMZ，或者增加防火墙。所描述的方法使得能够对安全专家将理解的未决安全配置更改的列表进行精选，并且还提供对这样的更改的可选的确认和批准。模板方法还易于与诸如应用模式工具的其它云部署工具进行集成。

[0126] 保障服务可以利用所要部署的应用的细节进行查询，从而确定适用于应用的可用

安全措施。保障服务优选地被集中管理以提供更高或更低级别的安全保障。方法使得安全环境可以在应用取消部署时被解配置。当更高安全级别的应用被解配置时，服务还可以允许降低针对受影响应用的安全级别。服务还支持相关保障模板的实时交互管理以提供用户界面(UI)能力，诸如连线的或互斥的模板(例如，添加SSL可能会影响用于不同保障级别的密钥长度)。服务提供自动发现或者与软件库集成以标识可用的安全软件和经许可的资源以选择可用的保障模板。优选地，服务提供管理能力以基于逐个应用来覆盖经应用的安全模板。方法使得能够估计安全配置更改的系统范围内的成本，以及以易于理解的格式向用户呈现这些成本。服务还使得模板能够围绕安全设置的成本被设置，例如，将最大级别设置为安全环境成本，在这种情况下，最终用户只能选择安全保障能力的子集。方法使得用户能够建立集中式安全策略从而防止尚未选择最低安全级别的安全模板时的应用部署。

[0127] 服务提供能够被用来建议安全模板的分析，例如基于过往所使用的模板。在应用部署期间使用安全分析提供了确定应用安全部署是否符合企业的安全政策的有用方式。

[0128] 服务还提供经升级的安全模板到现有应用的追溯适用。服务还使得能够与执行安全扫描或输出安全智能报告的系统进行集成，从而促进对系统保护差距的标识，并且建议以及可选地自动应用缺失的配置或产品。

[0129] 如所描述的，本文的方法可以被人工实施，或者整体或部分地以自动方式来实施。

[0130] 虽然已经描述了优选的操作环境和使用情形(云部署装置或平台)，但是本文的技术可以在其中期望部署应用或其它服务同时实施给定安全上下文的任何其它操作环境中使用。

[0131] 如已经描述的，以上所描述的功能可以被实施为单独的方法，例如由一个或多个硬件处理器执行的一个或多个基于软件的功能，或者其可被用作经管理的服务(包括如经由SOAP/XML接口的网络服务)。本文所描述的特定硬件和软件实施方式的细节仅是出于说明的目的而并非旨在限制所描述主题的范围。

[0132] 更一般地，所公开主题的上下文中的计算设备均为包括硬件和软件的数据处理系统(诸如图2中所示)，并且这些实体通过网络(诸如互联网、企业内部网、外部网、私有网络，或者任何其它通信介质或链接)互相通信。数据处理系统上的应用提供对网络和其它已知服务和协议的本地支持，其包括但不限于对超文本传输协议(HTTP)、文件传输协议(FTP)、简单邮件传输协议(SMTP)、简单对象访问协议(SOAP)、可扩展标记语言(XML)、网络服务描述语言(WSDL)、统一描述、发现和集成(UDDI)以及网络服务流程语言(WSFL)等的支持。关于SOAP、WSDL、UDDI和WSFL的信息可从万维网联盟(W3C)获取，其负责开发和维护这些标准；关于HTTP和XML的另外信息可从互联网工程任务组(IETF)获取。假定对这些标准是熟悉的。

[0133] 除了基于云的环境之外，本文所描述的方案可以在各种服务器侧的架构(包括简单的n层架构、网络门户、联合系统等)中或者与之相结合进行实施。

[0134] 更一般地，本文所描述的主题可以采用完全硬件实施例、完全软件实施例或者包含硬件和软件元件的实施例的形式。在优选实施例中，安全保障服务(或者其任意组件)在软件中实施，软件包括但并限于固件、驻留软件、微代码等。此外，下载和删除接口和功能能够采取可从计算机可用或计算机可读介质访问的计算机程序产品的形式，该计算机可用或计算机可读介质提供程序代码以由计算机或任何指令执行系统使用或者结合其使用。出于该描述的目的，计算机可用或计算机可读介质可以为能够包含或存储程序以由指令执行系

统、装置或设备使用或者结合其使用的任何装置。介质可以为电子、磁、光、电磁、红外或半导体系统(或者装置或设备)。计算机可读介质的示例包括半导体或固态存储器、磁带、可移动计算机软盘、随机存取存储器(RAM)、只读存储器(ROM)、硬磁盘和光盘。光盘的当前示例包括紧致盘-只读存储器(CD-ROM)、紧致盘-读/写(CD-R/W)和数字化视频光盘(DVD)。计算机可读介质是有形的非瞬时介质。

[0135] 计算机程序产品可以是具有程序指令(或程序代码)以实施所描述的功能中的一个或多个的产品。那些指令或代码可以在通过网络从远程数据处理系统被下载之后被存储在数据处理系统的计算机可读存储介质中。或者,那些指令或代码可以被存储在服务器数据处理系统的计算机可读存储介质中并且适于通过网络被下载到远程数据处理系统中以在远程系统内的计算机可读存储介质中使用。

[0136] 在代表性实施例中,技术在专用计算平台中被实施,优选地在由一个或多个处理器执行的软件中实施。软件被保持在与一个或多个处理器相关联的一个或多个数据存储或存储器中,并且软件可以被实施为一个或多个计算机程序。共同地,专用硬件和软件包括以上所描述的功能。

[0137] 在如上所述的优选实施例中,本文所提供的功能被实施为对现有云计算部署管理解决方案的附属或扩展。

[0138] 虽然以上描述了由本发明的某些实施例所执行的特定顺序的操作,但是应当理解,这样的顺序是示例性的,比如备选实施例可以以不同顺序来执行操作、组合某些操作、重复某些操作等。说明书中对给定实施例的引用表示所描述的实施例可以包括特定特征、结构或特性,但是每个实施例都可以并非必需包括特定特征、结构或特性。

[0139] 最后,虽然已经单独地对系统的给定组件进行了描述,但是本领域技术人员将会意识到,一些功能可以在给定指令、程序序列、代码部分等中组合或共享。

[0140] 本文的技术提供了对技术或技术领域(即管理云部署的计算实体)的改进,以及对应用部署机制自身的功能的改进(即基于具有用于安全配置工具作业更改的相关联指令的易于理解的模板而通过将其常规功能扩展为安全上下文感知的)。

[0141] 如本文所使用的特定术语“模板”并不应当被认为局限于任何特定的格式或结构,因为该概念旨在指代包括所标识的信息类型(与特定安全保障级别相关联的预先配置的安全要求)的任何构建(无论结构或形式),其优选地利用易于理解的引用(例如,“高安全”)所指定,并且其适于由服务/系统(通常连同系统配置等)转换为实施所指定的安全级别所必需的粒度要求。根据实施方式,“模板”可以包括具有这些属性和特性的配置数据集合。

[0142] 已经描述了我们的发明,我们所请求保护的内容如下。

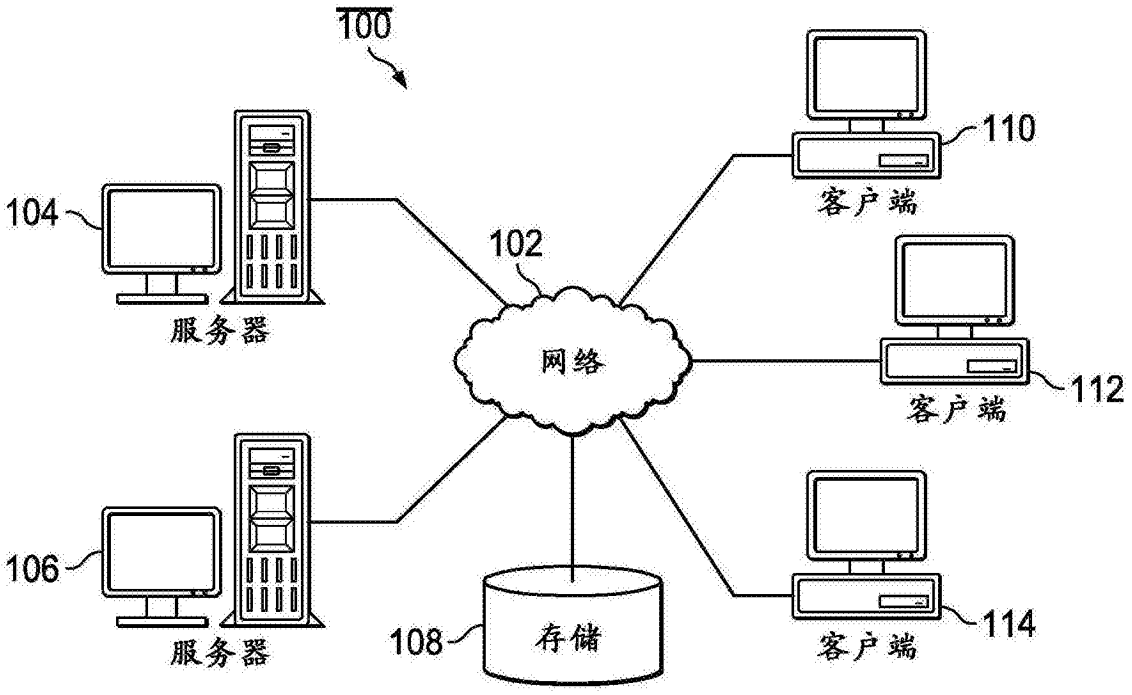

100
104
服务器
102
网络
110
客户端
112
客户端
106
服务器
108
存储
114
客户端

图1

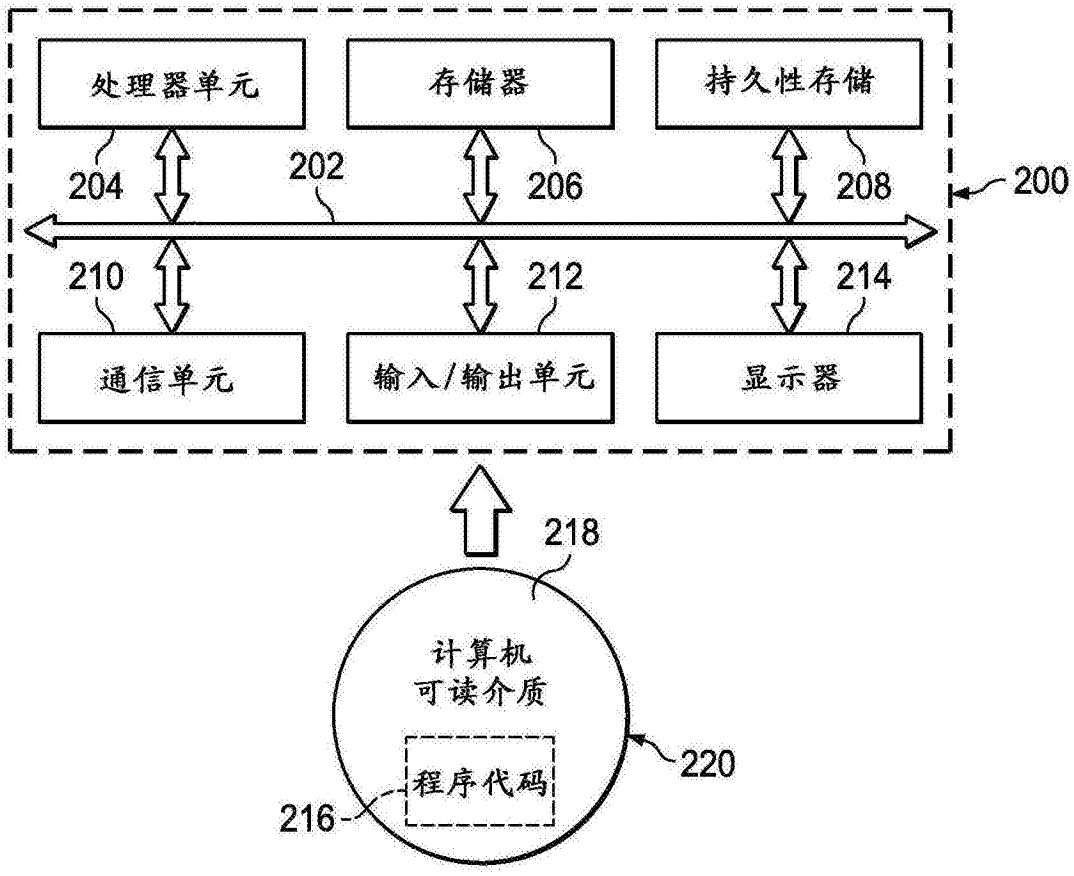

处理器单元
存储器
持久性存储
204
202
206
208
200
210
212
214
通信单元
输入/输出单元
显示器
218
计算机
可读介质
程序代码
216
220

图2

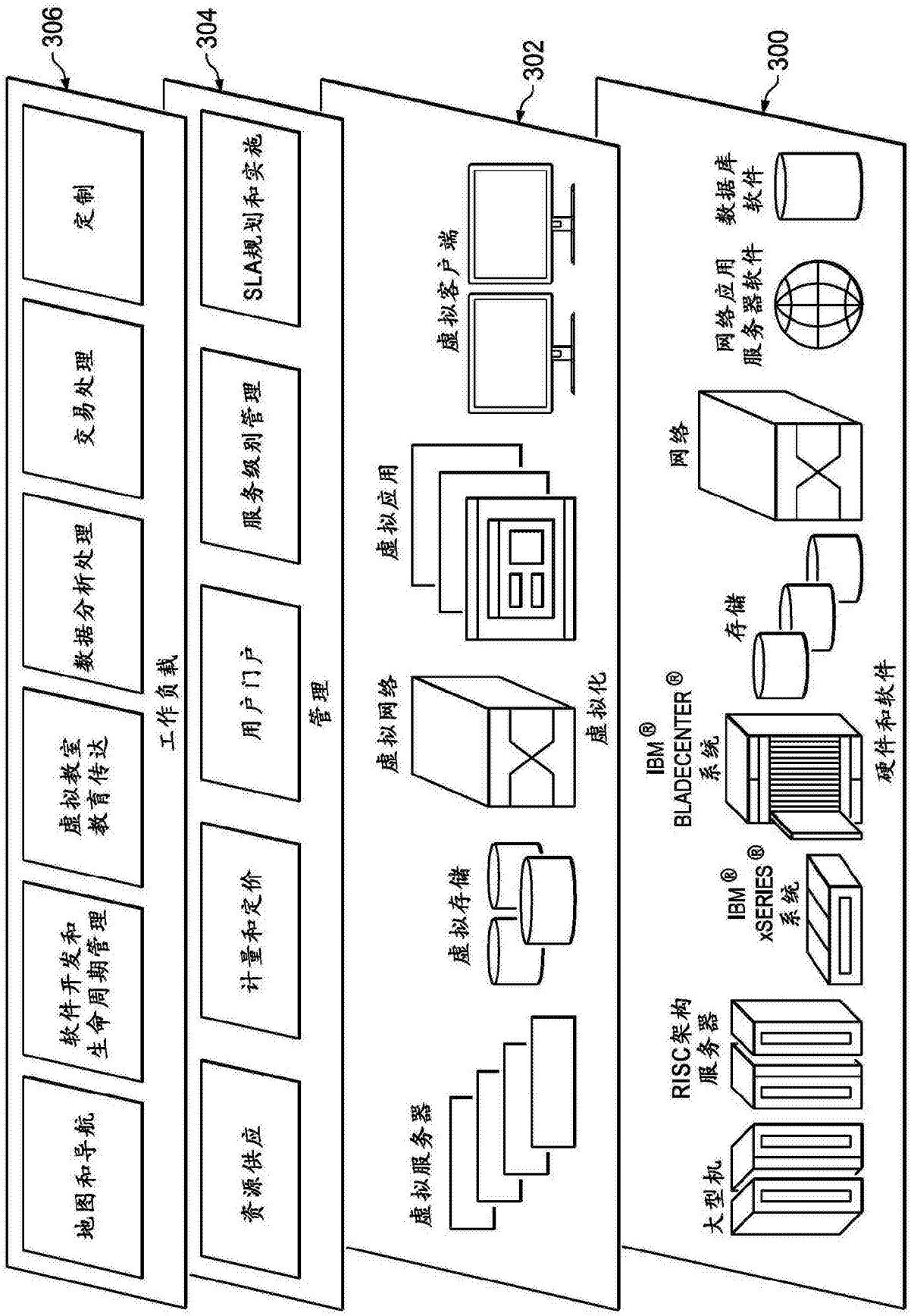

306
304
302
300
地图和导航
软件开发和生命周期管理
虚拟教室教育传达
数据分析处理
交易处理
定制
工作负载
资源供应
计量和定价
用户门户
服务级别管理
SLA规划和实施
管理
虚拟服务器
虚拟存储
虚拟网络
虚拟应用
虚拟客户端
虚拟化
大型机
RISC架构服务器
IBM® xSERIES® 系统
IBM® BLADECENTER® 系统
存储
网络
网络应用服务器软件
数据库软件
硬件和软件

图3

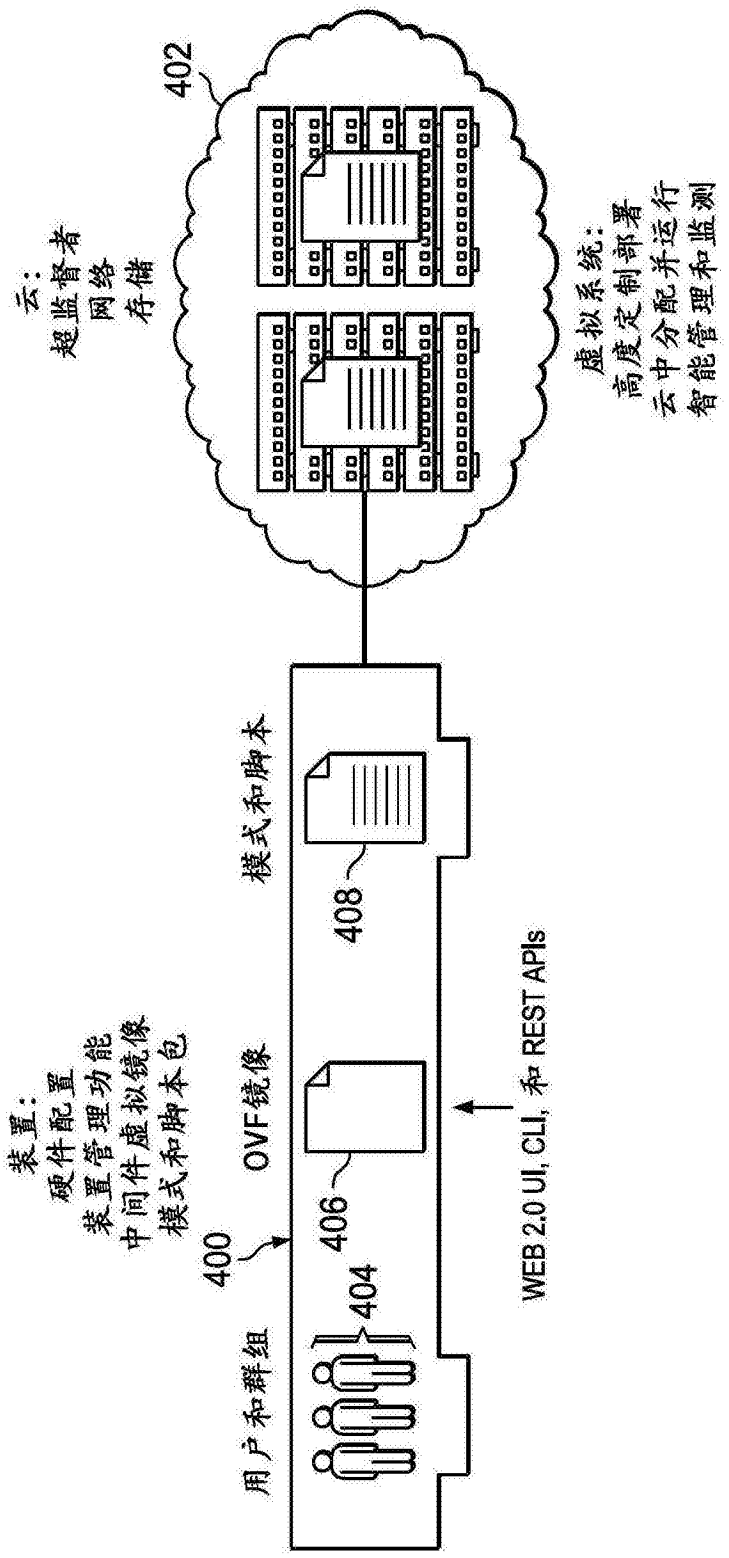

402
云：
超监督者
网络
存储
虚拟系统：
高度定制部署
云中分配并运行
智能管理和监测
装置：
硬件配置
装置管理功能
中间件虚拟镜像
模式和脚本包
400
OVF镜像
406
模式和脚本
408
404
用户和群组
WEB 2.0 UI, CLI, 和 REST APIs

图4

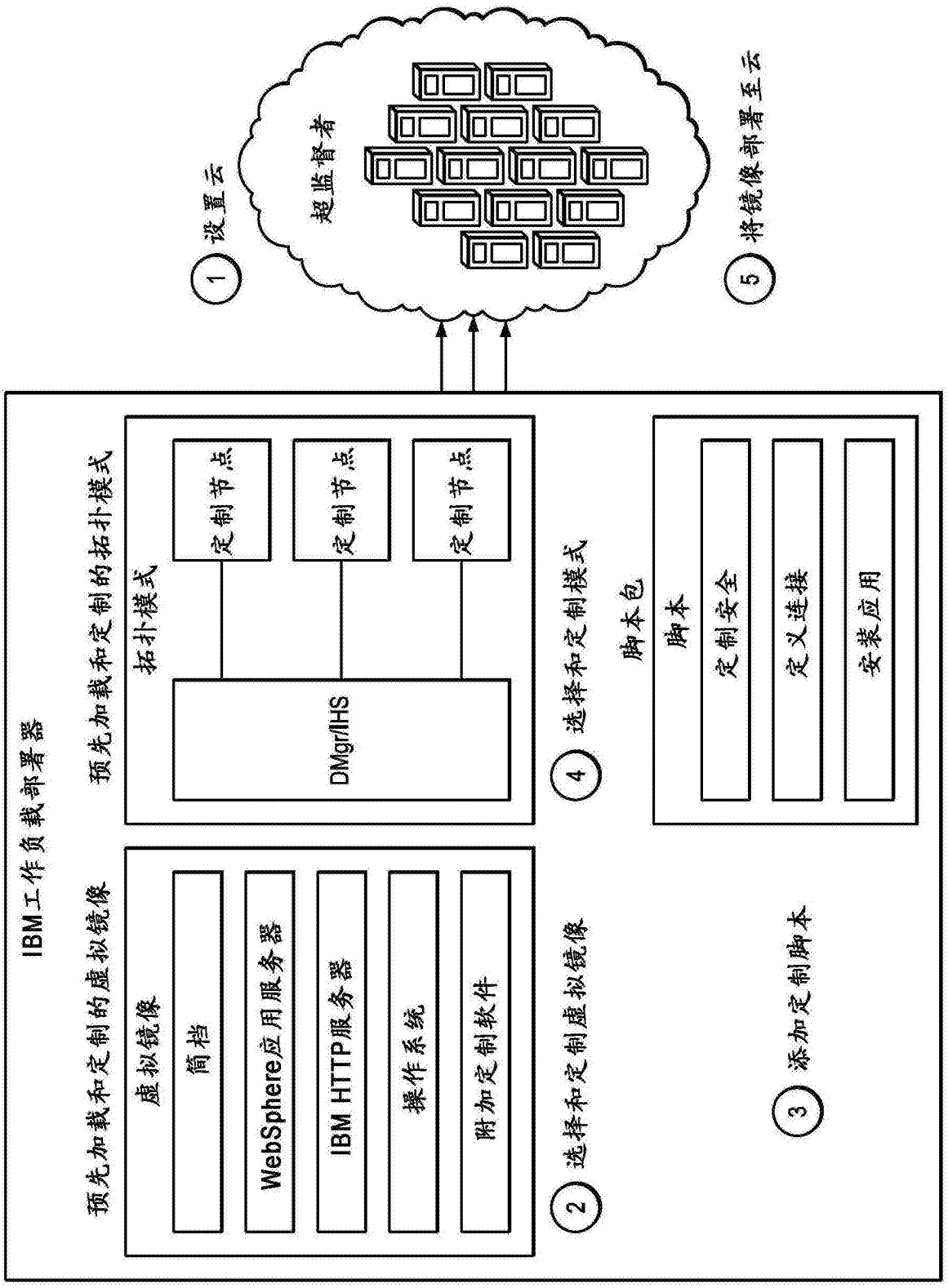

IBM工作负载部署器
预先加载和定制的虚拟镜像
虚拟镜像
简档
WebSphere应用服务器
IBM HTTP服务器
操作系统
附加定制软件
预先加载和定制的拓扑模式
拓扑模式
定制节点
定制节点
定制节点
DMgr/IHS
脚本包
脚本
定制安全
定义连接
安装应用
① 设置云
超监督者
② 选择和定制虚拟镜像
③ 添加定制脚本
④ 选择和定制模式
⑤ 将镜像部署至云

图5

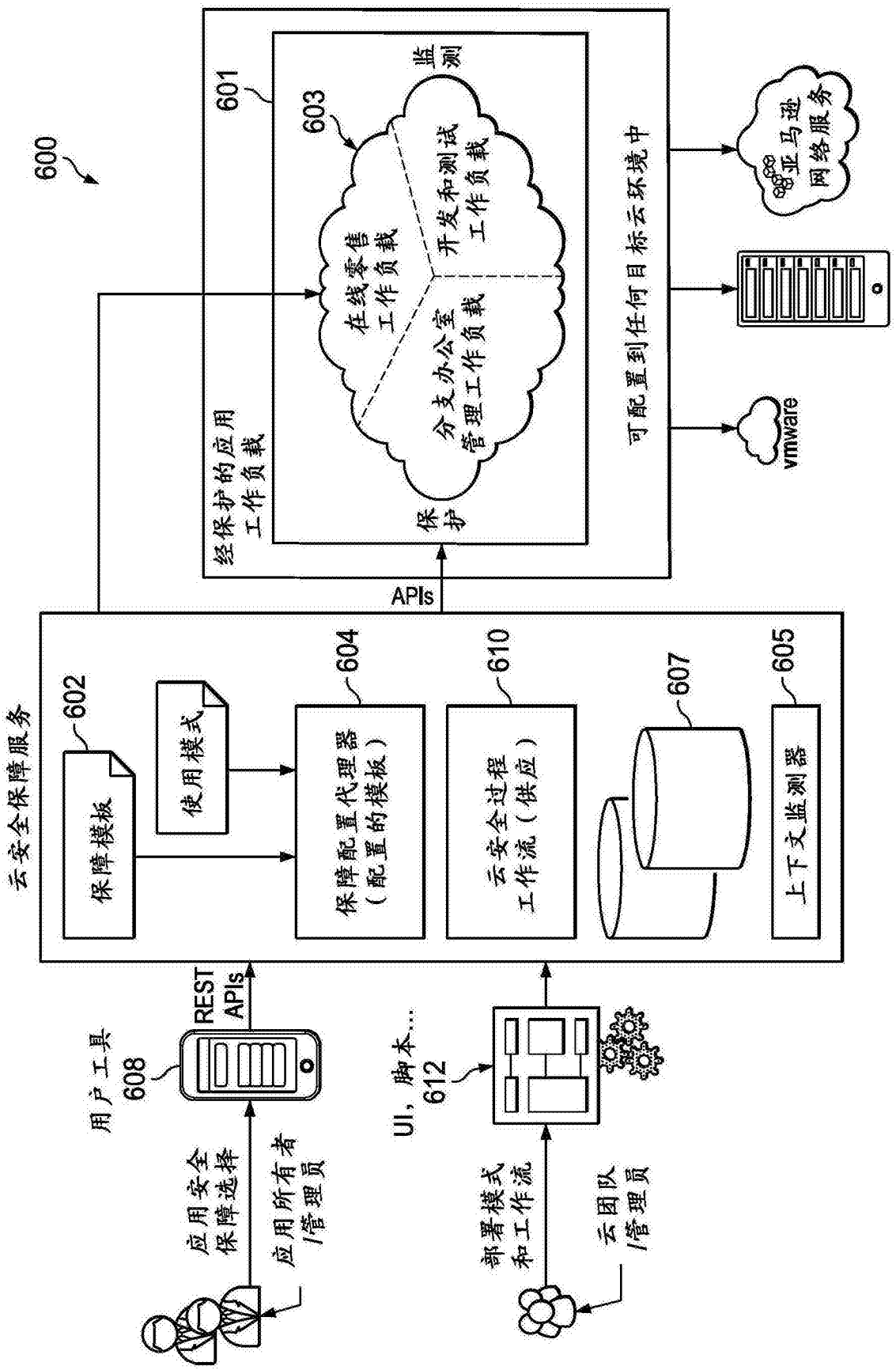

600
601
603
监测
在线零售工作负载
开发和测试工作负载
分支办公室管理工作负载
保护
经保护的应用工作负载
APIs
可配置到任何目标云环境中
亚马逊网络服务
vmware
云安全保障服务
602
保障模板
使用模式
604
保障配置代理器（配置的模板）
610
云安全过程工作流（供应）
607
605
上下文监测器
REST APIs
用户工具
608
应用安全保障选择
应用所有者/管理员
UI，脚本...
612
部署模式和工作流
云团队/管理员

图6

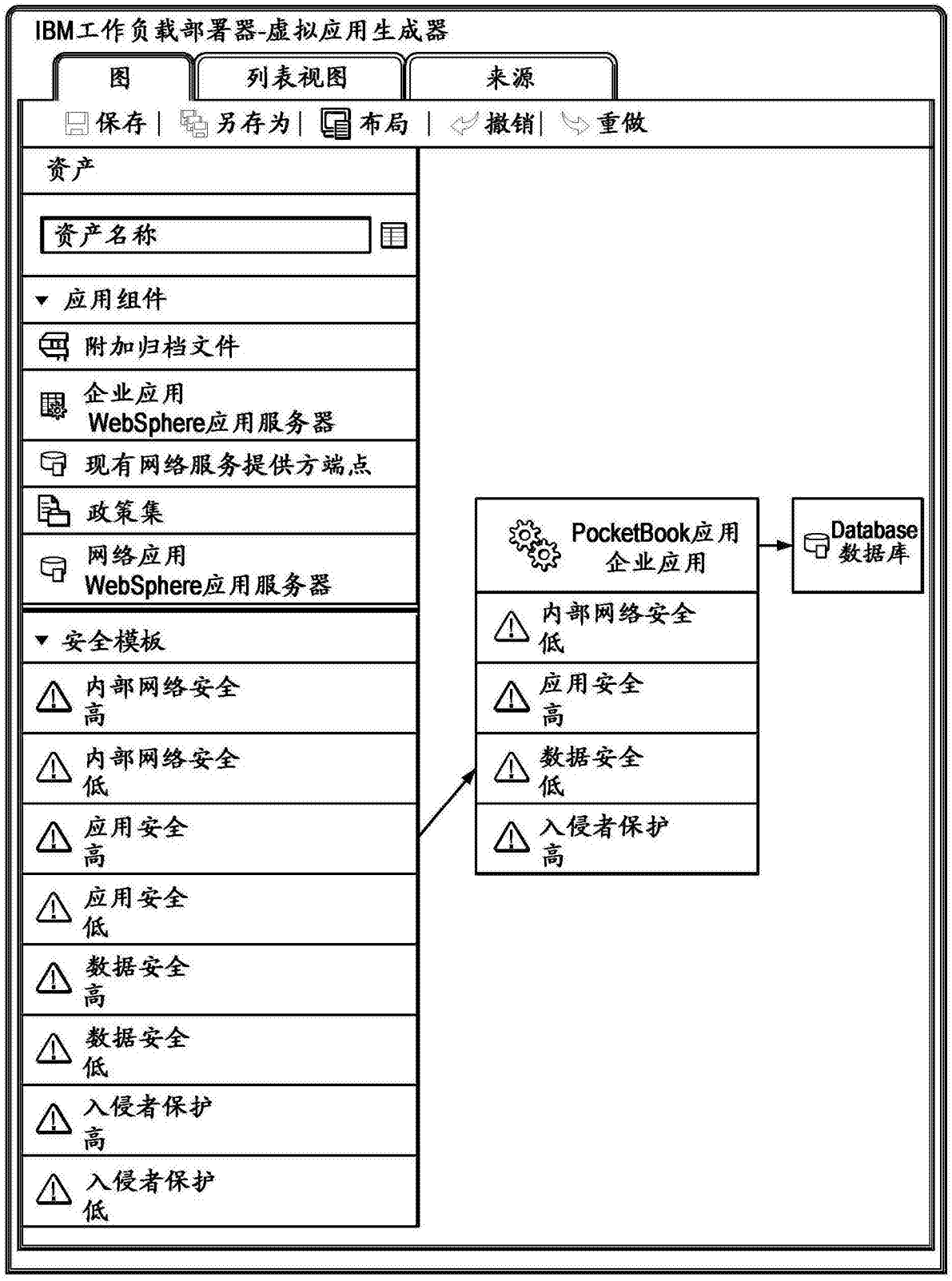

IBM工作负载部署器-虚拟应用生成器
图
列表视图
来源
保存
另存为
布局
撤销
重做
资产
资产名称
应用组件
附加归档文件
企业应用
WebSphere应用服务器
现有网络服务提供方端点
政策集
网络应用
WebSphere应用服务器
安全模板
内部网络安全
高
内部网络安全
低
应用安全
高
应用安全
低
数据安全
高
数据安全
低
入侵者保护
高
入侵者保护
低
PocketBook应用
企业应用
内部网络安全
低
应用安全
高
数据安全
低
入侵者保护
高
Database
数据库

图7

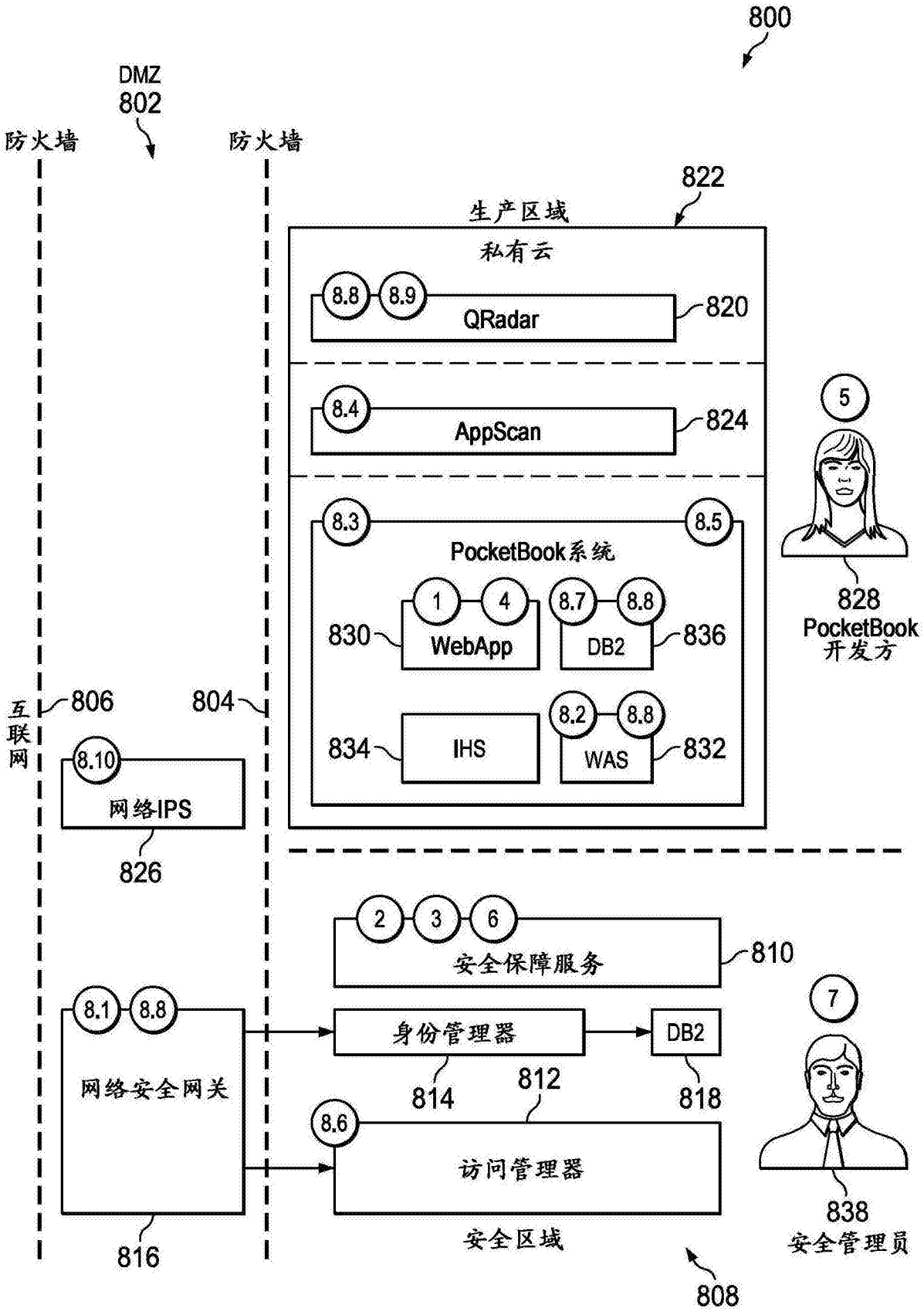

800
DMZ
802
防火墙
防火墙
822
生产区域
私有云
8.8
8.9
QRadar
820
8.4
AppScan
824
5
8.3
8.5
PocketBook系统
1
4
8.7
8.8
830
WebApp
DB2
836
828
PocketBook
开发方
互联网
806
804
8.2
8.8
834
IHS
WAS
832
8.10
网络IPS
826
2
3
6
安全保障服务
810
7
8.1
8.8
身份管理器
DB2
网络安全网关
814
812
818
8.6
访问管理器
838
安全管理员
816
安全区域
808

图8