(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 103875210 A
(43)申请公布日 2014.06.18

(21)申请号 201280050376.2
(22)申请日 2012.10.01
(30)优先权数据
13/273,415 2011.10.14 US
(85)PCT国际申请进入国家阶段日
2014.04.14
(86)PCT国际申请的申请数据
PCT/US2012/058225 2012.10.01
(87)PCT国际申请的公布数据
WO2013/055538 EN 2013.04.18
(71)申请人 阿尔卡特朗讯公司
地址 法国巴黎
(72)发明人 A·阿萨那 M·S·班诺威茨
U·钱德拉谢卡尔
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 宛丽宏 杨晓光
(51)Int.Cl.
H04L 12/24(2006.01)
G06F 9/50(2006.01)

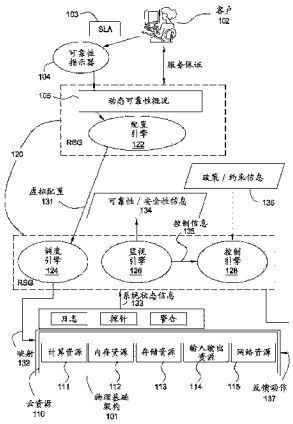
权利要求书2页 说明书21页 附图10页

(54)发明名称

在通信环境中提供动态可靠性和安全性

(57)摘要

提供了动态可靠性和安全性能力。动态可靠性和安全性能力。动态可靠性和安全性能力可以配置为支持动态可靠性概况(DRP)的使用,该DRP依据时间并依据客户的应用或服务的要求来指明客户的可靠性参数。可靠性参数可以指明客户的可靠性要求和/或目标,从而提供随时间而变化的要求/目标概况。动态可靠性和安全性能力可以配置为动态地配置云资源,以提供DRP所指明的要求的可靠性。RSG能力可配置为接着对行为进行监视和计量,以确保所指明的可靠性实际上得到递送,这包括使用自我治疗能力来提供服务保证。



CN 103875210 A

1. 一种装置，包括：

处理器和存储器，所述处理器配置为：

接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数；以及

基于所述客户的 DRP 确定用于所述客户的云资源的配置。

2. 如权利要求 1 所述的装置，其中所述处理器配置为通过以下方式基于客户的 DRP 确定用于所述客户的云资源的配置：

使用客户应用信息以及与云提供商的云系统相关联的云系统信息，确定用于所述客户的虚拟应用拓扑；

使用用于所述客户的所述虚拟应用拓扑以及与所述云系统相关联的云系统信息，确定可靠性绘图；以及

使用所述可靠性绘图和与所述云系统相关联的云系统信息，确定云资源的配置。

3. 如权利要求 1 所述的装置，其中所述处理器配置为，在多个时间段的每一个中确定用于所述客户的云资源的配置。

4. 如权利要求 1 所述的装置，其中所述处理器还配置为：

监视云资源的行为，用以确定所述 DRP 中指明的可靠性参数是否得到满足；

计量用以满足所述 DRP 中指明的可靠性参数的所述云资源的行为。

5. 如权利要求 1 所述的装置，其中所述处理器配置为提供配置引擎，该配置引擎配置为：

处理与所述客户相关联的 DRP，以产生虚拟配置；以及

将所述虚拟配置提供给调度引擎，该调度引擎配置为将所述虚拟配置映射到云资源。

6. 如权利要求 1 所述的装置，其中所述处理器配置为提供调度引擎，该调度引擎配置为：

接收虚拟配置，该虚拟配置满足与所述客户相关联的 DRP；以及

将该虚拟配置映射到云资源。

7. 如权利要求 1 所述的装置，其中所述处理器配置为提供监视引擎，该监视引擎配置为：

使用所述云系统的云提供商所指明的政策信息和约束信息中的至少一个和与云提供商的云系统相关联的系统状态信息，产生可靠性完整性计量和被配置用以在控制所述云系统的云资源时使用的控制信息中的至少一个。

8. 如权利要求 1 所述的装置，其中所述处理器配置为提供控制引擎，该控制引擎配置为：

接收控制信息，所述控制信息配置为用以在控制所述云资源时使用；以及

使用所述控制信息，产生至少一个反馈动作，该反馈动作配置为修改所述云资源的至少一部分。

9. 一种计算机可读存储介质，用于存储指令，所述指令当被计算机执行时，致使计算机执行一种方法，该方法包括：

接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数；以及

基于所述客户的 DRP 确定用于所述客户的云资源的配置。

10. 一种方法，包括 ：

使用处理器，用以 ：

接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数 ；以及

基于所述客户的 DRP 确定用于所述客户的云资源的配置。

在通信环境中提供动态可靠性和安全性

技术领域

[0001] 本发明总体上涉及通信环境，更具体但不排他地涉及在通信环境中提供可靠性和安全性。

背景技术

[0002] 云计算提供了使用快速、自服务的供应通过互联网向客户递送服务和资源的方式，同时将服务和资源的客户与底层基础架构的管理隔离开来。然而，尽管云计算有各种优势并且云计算的使用近来得到增长，但是，许多客户仍然在一些方面存有疑虑，例如云计算的可靠性和安全性，等等。

发明内容

[0003] 通过在云环境中提供可靠性和安全性的实施例解决了现有技术中的多项不足。

[0004] 在一个实施例中，一种装置包括处理器，该处理器配置为接收与云提供商的客户相关联的动态可靠性概况(profile)(DRP)，并基于所述客户的 DRP 确定用于该客户的云资源的配置，其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数。

[0005] 在一个实施例中，一种计算机可读存储介质存储有指令，所述指令当被计算机执行时，致使计算机执行这样一种方法，该方法包括，接收与云提供商的客户相关联的动态可靠性概况(DRP)，并基于所述客户的 DRP 确定用于该客户的云资源的配置，其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数。

[0006] 在一个实施例中，一种方法包括，接收与云提供商的客户相关联的动态可靠性概况(DRP)，并基于所述客户的 DRP 确定用于该客户的云资源的配置，其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数。

附图说明

[0007] 通过考虑接下来结合附图进行的详细描述，更易于理解本文的教导，在附图中：

[0008] 图 1 描绘了包括可靠性和安全性守卫(RSG)的云系统的一个实施例；

[0009] 图 2 描绘了用于图 1 的 RSG 的示例性动态可靠性概况(DRP)；

[0010] 图 3 描绘了用于图 1 的云系统的三个客户的随时间变化而变化的示例性应用组合；

[0011] 图 4 描述了用于将客户应用信息映射到图 1 的云系统的物理资源的过程的实施例；

[0012] 图 5 描绘了从应用拓扑到物理基础架构的示例性映射；

[0013] 图 6 描绘了图 1 的 RSG 的示例性使用，以执行事件关联并确定反应 / 预测控制信息；

[0014] 图 7 描绘了适用于执行图 1 的 RSG 的自可靠计算存储单元(CSU)的一个实施例；

[0015] 图 8 描绘了图 7 的多个 CSU 在客户域的示例性部署，以形成分布式自可靠云系统；

[0016] 图 9 描绘了在图 1 的云系统的一部分内部署的、适用于实现图 1 的 RSG 的系统控制单元（SCU）的一个实施例；

[0017] 图 10 描绘了用于为云系统的客户提供可靠性的方法的一个实施例；以及

[0018] 图 11 描绘了适用于执行本文所描述的功能的计算机的高层级框图。

[0019] 为了便于理解，在可能的情况下，使用相同的附图标记来指示图中共有的相同部件。

具体实施方式

[0020] 总体来说，本文描绘和描述了可靠性和安全性能力，不过也会提及各种其他能力。

[0021] 云计算提供了使用快速、自服务的供应通过互联网向客户递送服务和资源的方式，同时将服务和资源的客户与底层基础架构的管理隔离开来。在许多情况下，云提供商所提供的服务是效用计算，它典型地基于云系统的软件的抽象级别和云系统的资源的管理级别进行辨识。该图谱的一端例如是这样一种实施方式，其中抽象位于物理硬件层，客户可以控制整个软件栈，内核以上（尽管这使得难以提供故障转移能力）。该图谱的另一端例如是这样一种实施方式，它是利用无状态计算和有状态存储系统的、专用于 web 应用的应用域。应注意其他实施方式也可以落入该图谱的中间部分。

[0022] 云计算具有许多相关联的优势。总体来说，云计算使得能够实现高度的可扩展性、可配置性、资源可用性的动态弹性、易于返回，及类似优势。云计算为硬件供应提供众多能力，以创建这样一种表象，“无限”的计算资源基于需求而可用，足够快速地满足负载的浪潮，从而消除对提前供应的需要。在易于调整尺寸的前提下，云计算使得能够实现更廉价的故障转移方案，这是因为云服务的按需而定或现购现付的特点。在云计算中，客户根据需要短期地为计算资源的使用进行付费（例如，按小时计处理器，按天计存储量，等等），并可以根据需要对其进行请求和释放。云计算还考虑到了规模经济（例如，电力、净带宽、操作、软件和硬件等方面的改善因素），允许统计上的多重复用以增加资源利用率，并简化操作。还将意识到云计算的各种其他优势。

[0023] 然而，尽管云计算存在前述优势和增长，许多客户仍然为解决关于其可靠性和安全性的问题而挣扎。例如，物理资源的共享带来了安全性问题（例如，数据对于他人可见，在故障或退出之后留下数据印迹，等等）。此外，广泛采用云服务的障碍不能被忽略，例如，安全性 / 数据隐私和管辖权问题、服务级别协定（SLA）的可变性 / 初期、性能和访问控制 / 延迟、可靠性和卖主中立性、将云服务与商业应用相整合的能力、云服务模型的相对不成熟和持续的发展，等等。并且，注意到，部署有任务关键型应用的企业通常通过 SLA 寻求合理的系统响应率的保证，通过在多租户环境中的数据隔离寻求保护，寻求故障转移保护来最小化服务中断，寻求可预测的再装载率以及各种相关的服务和能力。而且，对于任务关键型应用的保证不是可以量化的，突出公共云（例如，提供便利）相对于私有云（例如，提供安全性和私密性的更好的控制和保证）的成本 / 收益的量度并不清楚。如此，云系统的软件的抽象级别和云系统的资源的管理级别具有成为云提供之间的关键区分的潜在可能。

[0024] 在一个实施例中，可以通过使用新系统体系架构、新设备 / 部件、新编程模型、新开发环境、和新测试方法中的一个或多个，来解决上述顾虑和 / 或需求的至少一部分，其中

这样的体系架构、设备 / 部件、模型、环境和 / 或方法可被配置为基于针对性能、可用性、安全性、弹性、使用计数等的对客户的 SLA 要求的更深理解，提供自可靠的系统。注意到，这将使得公共云计算和私有云计算都能够变得更加可靠和安全，因此，适合于任务关键型的使用。

[0025] 在一个实施例中，可以通过使用云系统中的可靠性和安全性守卫（RSG）能力来解决上述顾虑和 / 或需求的至少一部分。

[0026] RSG 能力可配置为支持动态可靠性概况（profile）（DRP）的使用，其中 DRP 可被包含为客户 SLA 的一部分，并依据时间，以及依据客户的应用或服务的要求这两者来指明客户的可靠性参数。可靠性参数可以指明客户的可靠性要求和 / 或目标，从而提供随时间变化的要求 / 目标概况。RSG 能力可配置为动态地配置云资源，以提供 DRP 所指明的所需的可靠性。RSG 能力可配置为，接下来对行为进行监视和计量，以保证所指明的可靠性事实上正被递送，这可包括使用自我治疗能力来提供服务保证。注意到，由于可靠性与可用性相关，动态可靠性概况在这里也可被称为动态可靠性 / 可用性概况。

[0027] RSG 能力可配置为执行或提供以下中的一个或多个：将递送到客户的服务的可靠性增加为不中断的体验；使得系统能够自动地重新均衡到功能可用性级别而没有用户可见的影响或手动干预；提供对性能、可靠性、可用性、安全性和弹性使用计数等等的服务级别协定（SLA）要求的动态保证，从而使得公共和 / 或私有云计算能够变得更加可靠、安全和弹性，因而适合于任务关键型使用；依据时间和应用或服务的要求这两者来描绘客户的可靠性要求 / 目标；提供自可靠的系统，其配置为动态地配置云资源，以提供所要求 / 所期望的可靠性；监视和计量该系统，以保证所要求 / 所期望的可靠性得到满足；通过安全收集和对可用的网络和服务数据的集中，跨整个方案接近实时地监视端对端服务的可用性；产生可靠性完整性计量，该计量从可用的网络和服务数据导出关键的端对端服务可用性的量度，并触发适当的恢复和控制动作；提供预防性的控制能力，该能力使得能够产生对紧迫问题和前摄的服务进行中测试的指示，以持续地检测并排除关键问题；等等。

[0028] RSG 能力可配置为提供各种其他相关联的功能。换而言之，就好像，客户可以呼叫一定可靠性，云系统做出反应来尝试递送该可靠性。

[0029] 在一个实施例中，RSG 能力部署在基础架构层之内。注意到，云计算的一个总体趋势是朝向与工业对齐的、动态的、自我学习的以及自我管理的方案。在一个实施例中，部署方案级别的能力，以能够构建有机的、自我意识以及自我治疗的网络，从而使得云提供商能够在客户需要的时候提供客户所需的保证。还注意到，这样的有机的、自我意识和自我治疗的网络可以支持各种客户应用，包括高价值的应用。在一个实施例中，为了支持这样的应用（包括高价值的应用），（1）在平台层之内将可靠性作为服务来提供（标注为 RaaS，可靠性作为服务），（2）在基础架构层之内提供被称为 RSG 能力的能力，其中 RSG 能力被配置为提供各种功能，诸如动态配置，用于高可用性的资源调度，完整性计量，服务进行中的鲁棒性测试，故障的预测和防止，网络事件的关联以识别并诊断故障边缘和安全条件边界，等等，以及以上功能的各种组合。以这样的方式，可以提供动态自可靠云系统。

[0030] 在一个实施例中，RSG 能力部署在客户网络之内。这克服了与现有云系统相关联的安全性障碍。也就是说，在现有云系统中，由于严格的安全性考虑，云服务提供商很少允许客户访问他们的内部管理系统或他们的性能和故障数据。例如，在极少数情况下，可以允许

客户“只读”访问报警和性能数据，用于离线分析的目的。相反，在支持 RaaS 的情况下，RSG 能力可以驻留在客户网络内，这样，RSG 能力和客户网络内的各种其他实体（例如，数据收集实体，管理实体，等等）之间的接口就可以被实现为信任接口。并不需要非军事化（DMZ）功能（例如，通过安全虚拟私有网络（VPN）路由的加密数据），因为所有数据都在客户域之内本地地访问和分析。并且，由于不涉及外部实体，有可能基于所监视的数据进行前摄性控制。因此，通过将 RSG 能力嵌入在客户网络之内而克服了现有的安全性障碍，这使得能够构建真正有机、自我意识以及自我治疗的网络。

[0031] 云系统可以经由一个或多个能力，诸如，经由这里描绘和描述的可靠性和安全性守卫（RSG），支持上述功能。参照图 1 描绘和描述一个示例性云系统中的示例性 RSG。

[0032] 图 1 描绘了包含可靠性和安全性守卫（RSG）的云系统的一个实施例。

[0033] 如图 1 所描绘，云系统 100 包括物理基础架构 101，它通过为客户 102 提供云服务的云提供商来管理。云系统 100 还包括可靠性 / 安全性守卫（RSG）120，配置为使得云提供商在使用物理基础架构 101 向客户 102 提供云服务的背景下，向客户 102 提供服务保证。

[0034] 物理基础架构 101 包括云资源 110，可选地还包括可以由云提供商部署来支持云服务的任何其他物理基础架构。

[0035] 客户 102 是可以访问和使用云资源 110 的任何适当类型的客户。例如，客户 102 可以是企业客户，家庭客户，等等。

[0036] 客户 102 能够提供可用于产生用于客户 102 的 SLA103 的信息。SLA 典型地是客户特定的，并定义客户的虚拟环境，客户典型地仅仅对相对于其虚拟环境所满足的 SLA 感兴趣，而对云系统的整个基础架构的整体不感兴趣。云提供商典型地支持多个客户（尽管，如以上所注意到的，这里出于清楚的目的仅仅描绘和描述了单个客户 120）。于是，云提供商典型地确保云系统的基础架构能够满足用于其所有客户的所有虚拟环境的 SLA。注意到，云系统 100 被配置为能够使得云提供商提供这样的能力。

[0037] 客户 102 能够提供可用于产生用于客户 102 的动态可靠性概况（DRP）105 的信息。用于客户 102 的 DRP105 可以由客户 102 直接指明，可以由客户 102 在 SLA103 之内指明，可以通过处理为 SLA103 而输入的信息，和 / 或处理 SLA103 自身（例如，通过可靠性指示器 104 和 / 或任何其他适当的系统或部件）而确定，等等，以及通过以上的各种组合来确定。DRP105 可以以任何适当的粒度提供（例如，用于具体的应用，用于一组应用，用于具体的服务，用于一组服务，用于一个或多个服务以及一个或多个应用，用于客户 102 整体，等等）。如图 1 所描绘，用于客户 102 的 DRP105 被提供给 RSG120。

[0038] 云资源 110 可以配置为由客户 102 使用。云资源 110 可包括计算资源 111，内存资源 112，存储资源 113，输入输出资源 114，以及网络资源 115。注意到，云资源 110 可以假定为虚拟无限的（也就是，有足够的云资源 110 来满足任何客户需求）。还注意到，云资源 110 可以是分布式的，并可以动态分组。本领域技术人员将可以理解将云资源 110 分配给客户 120 使用的典型方式。尽管对于特定类型的云资源 110 进行初步地描绘和描述，不过将可以理解，云资源 110 可以包含可配置为用于客户使用的任何其他类型的云资源。

[0039] RSG120 配置为提供使得云系统 100 可以操作为自可靠系统的各种功能。例如，RSG120 可以配置为接收客户 102 的 DRP105，动态配置云系统 100 的云资源 110，以提供 DRP105 所指明的要求的可靠性。RSG120 还配置为接着对行为进行监视和计量，以保证所指

明的可靠性实际上正得到递送。RSG120 还配置为提供各种其他相关联的功能。注意到，如图 1 所呈现的，RSG120 可以以集中的或分布式的方式实现。

[0040] RSG120 包括四个功能部件：配置引擎（CE）122，调度引擎（SE）124，监视引擎（ME）126，以及控制引擎（CE）128。注意到，这四个功能部件可以使用一个或多个物理设备来实现（例如，RSG120 的功能可以集中在单个系统中，跨一个或多个系统分布，等等）。相应地，RSG120 使用虚线框来表示，旨在示出四个功能部件可以在云系统 100 内执行的各种方式。

[0041] CE122 接收客户 102 定义的 DRP105（或者包含 DRP105 的 SLA103），使用 DRP105 来动态产生用于客户 102 的虚拟配置 131。虚拟配置 131 指明满足客户 102 的 DRP105（例如，满足 DRP105 的要求和 / 或目标）的用于客户 102 的虚拟配置。虚拟配置 131 可以依据时间而被指明。CE122 可以动态地产生满足 DRP105 的虚拟配置 131，同时负责云系统 100 的当前状态和 / 或云系统 100 所施加的政策 / 约束。CE122 将虚拟配置 131 提供给 SE124。CE122 可以提供本文所讨论的各种其他功能。

[0042] SE124 从 CE122 接收虚拟配置 131。SE124 在通过 DRP105 和云系统 100 的当前状态和 / 或云系统 100 施加的政策 / 约束管控的适当时间处，将虚拟配置 131 映射到物理基础架构 101（例如，映射到云资源 110）。由 SE124 确定的映射标注为映射 132。SE124 可以指明与 DRP105 的实现相关联的必要类型的冗余和 / 或恢复方案。注意到，如同 DRP105 可以以任何适当粒度指明一样，相关联的映射 132 可以以任何适当粒度来提供。SE124 配置为在物理基础架构 101 内执行映射 132（例如，经由物理基础架构 101 的配置使得客户 102 能够使用云资源 110），从而使得客户 102 于是可以利用云资源 110。SE124 可以提供本文所讨论的各种其他功能。

[0043] ME126 观测物理基础架构 101 的部件（例如，云资源 110 的计算资源 111，内存资源 112，存储资源 113，输入输出资源 114，网络资源 115，以及云资源 110 的任何其他相关联的物理部件或资源）的状态。ME126 通过接收和分析在 ME126 处从物理基础架构 101 接收的系统状态信息 133（例如，警报，探针，日志文件，等等，以及以上的各种组合），来观测物理基础架构 101 的部件的状态。ME126 将物理基础架构 101 的部件的所观测状态转译成客户 102 的虚拟环境的状态。ME126 可配置为将与可靠性和安全性相关的事件和状态捕获作为可靠性 / 安全性信息 134（在至少一些实施例中，该信息 134 可以表示为可靠性完整性计量（RIM））。ME126 可配置为确定用于 CE128 使用的控制信息（标注为控制信息 135）（例如，用于 CE128 在对云系统 100 中的事件或条件做出反应时使用的反应控制信息，用于 CE128 在防止云系统 100 中发生潜在事件或条件时使用的预先防止控制信息，等等，以及以上的各种组合）。ME126 可以提供本文所讨论的各种其他功能。

[0044] CE128 配置为从 ME126 接收控制信息 135，接收政策 / 约束信息 136（该信息例如可以被指明为 SLA103，DRP105 等等的一部分，以及以上的各种组合），并使用控制信息 135 和政策 / 约束信息 136 来确定适用于控制 / 配置云系统 100 的物理基础架构 101（例如，云资源 110）的反馈动作 137。CE128 将反馈动作 137 提供到物理基础架构 101，以控制 / 配置云系统 100 的物理基础架构 101。反馈动作 137 可以包括反应性反馈动作（例如，对识别的事件或条件作出反应）以及 / 或者预测性防止性反馈动作（例如，用于防止预测的事件或条件发生）。例如，CE128 可以当检测到故障时触发恢复动作，和 / 或启动防止性措施，以避免故障发生。CE128 可以提供本文所讨论的各种其他功能。

[0045] 如图 1 所描绘，RSG120 的部件可以以适当方式嵌入在云系统 100 中。例如，在一个实施例中，RSG120 的部件可以嵌入在云系统 100 的基础架构、平台和服务层中。将从图 1 和本文提供的其他描述中了解，云系统 100 的自可靠特性通过以下特征 / 益处中的一个或多个来表征 :(1) 向客户提供服务可用性，而不管硬件和 / 或软件故障或中断，(2) 保护服务、数据和基础架构免于攻击，确保个人数据的私密性，(3) 基于事件或政策实时提供灵活和动态的资源分配，也就是，可扩展性，(4) 可预测的性能，其横跨宽范围的工作负载需求并具有可接受的递送成本。通过图 1 和本文提供的其他描述将了解通过使用云系统 100 的实施例可以实现的各种其他特征 / 益处。

[0046] 如本文所描述的，DRP105 依据时间以及客户 102 的应用或服务的要求这两者指明客户 102 的可靠性参数 (例如，要求 / 目标)。应理解，并不是客户群组中的所有应用 / 服务都预期具有相同的可靠性需求，并且，应用 / 服务的可靠性需求可以随时间而改变。参照图 2 描绘和描述一个示例性 DRP105，它示出了其时间改变的特性。

[0047] 图 2 描绘了由图 1 的 RSG 使用的示例性动态可靠性概况 (DRP)。如图 2 所描绘，DRP105 表示客户的可靠性需求 (在 y 轴上示出) 随时间 (在 x 轴上示出) 的改变。如本文所描述，RSG120 配置为使用 DRP105 来动态配置云资源 110，以提供 DRP105 中指明的所要求的可靠性。注意到，在具有虚拟无限云资源的云系统中，这带来资源的更高利用率，节省成本，电源使用的高效，以及各种其他优势。

[0048] 如本文所描述的，云系统 100 可以支持多个客户 102，每个客户具有一个或多个相关联的 DRP105。于是，云系统 100 需要同时管理多个客户 102 的 DRP105，同时顾及到 DRP105 是随时间变化的概况这一事实。对于多个客户 102 的 DRP105 的随时间而改变的特性，这里考虑接下来的三种情况 (注意到，尽管也可以考虑各种其他情况):(1) 给定客户的应用组合的要求可能随时间变化，(2) 客户组的要求可能随时间变化，以及 (3) 给定应用的要求可能随时间变化。参照图 3 描绘和描述具有不同应用组合的三个客户 102 的例子。

[0049] 图 3 描绘了用于图 1 的云系统的三个客户的、依据时间的示例性应用组合。

[0050] 如图 3 所描绘，应用组合 300 示出标注为客户 A、B 和 C 的三个客户的应用的示例性组合。三个客户 A、B 和 C 的应用分别标注为 A_i、B_i 和 C_i。应用 A_i、B_i 和 C_i 的每个具有与其相关联的可靠性要求 (其中，出于清楚的目的，支持如下三个可能的可靠性要求 :高度 (HIGH)，、中度 (MED) 和低度 (LOW))。在这个例子中，高度的可靠性要求指示出，预期有完全的活动 / 活动冗余度，中度的可靠性要求指示出，预期活动 / 备用的冗余方案，而低度的可靠性要求指示出预期没有冗余度。

[0051] 应用组合 300 随时间而改变，描绘了四个示例性时间段 310_1-310_4 (总体上，时间段 310)，用于示出应用组合 300 随时间的改变。

[0052] 在时间段 310_1，客户 A 具有应用 A1 到 A5，其中应用 A1、，A3 和 A4 每个都具有高度的可靠性要求，应用 A2 具有中度的可靠性要求，而应用 A4 具有低度的可靠性要求。同样在时间段 310_1，客户 B 具有应用 B1 到 B4，其中应用 B1 和 B2 每个具有中度的可靠性要求，应用 B3 和 B4 每个具有高度的可靠性要求。同样在时间段 310_1，客户 C 具有应用 C1，它具有中度的可靠性要求。

[0053] 在时间段 310_2，客户 A、B 和 C 的应用的组合与时间段 310_1 的应用组合 300 相同 (也就是，没有改变)。

[0054] 在时间段 310_3，客户 A、B 和 C 的应用的组合发生了多种方式的改变(例如，之前的应用不再存在，仍然存在的之前应用的可靠性要求发生改变，引用新的应用，等等)。在时间段 310_3，客户 A 具有应用 A2、A4、A5、A6 (新的)和 A7 (新的)，其中应用 A2 和 A7 每个具有中度的可靠性要求，应用 A4 具有高度的可靠性要求，而应用 A5 和 A6 每个具有低度的可靠性要求。同样在时间段 310_3，客户 B 具有应用 B3、B5、B6 和 B7，其中应用 B3 和 B5 每个具有高度的可靠性要求，应用 B6 具有中度的可靠性要求，应用 B7 具有低度的可靠性要求。同样在时间段 310_3，客户 C 具有应用 C2 (新的)，它具有中度的可靠性要求。

[0055] 在时间段 310_4，客户 A、B 和 C 的应用的组合再次发生多种方式的改变(例如，之前的应用不再存在，仍然存在的之前应用的可靠性要求发生改变，引用新的应用，等等)。

[0056] 注意到，参照图 3 描绘和描述的可靠性要求仅仅是示例性的。实际中，粒度可以更加细致，应用的复杂性及其相关联的可靠性要求可以不同。例如，可以使用其他值表示示例性可靠性要求的一个或多个，可以以其他方式限定示例性可靠性要求的一个或多个，可以支持更少或更多的可靠性要求(包括不同的可靠性要求)，可以支持各种可靠性目标(例如，取代于以及 / 或者附加于上述可靠性要求)，等等，以及以上的各种组合。

[0057] 图 4 描绘了将客户应用信息映射到图 1 的云系统的物理资源的过程的一个实施例。

[0058] 总体来说，过程 400 执行一种受约束映射，该映射将客户 102 所需要的和 / 或所期望的映射到可在底层云基础架构中实现的(也就是，就好像，客户 102 可以呼叫一定可靠性，云系统 100 尝试递送它)。

[0059] 在一个实施例中，通过 RSG120 的 CE122 来执行方法 400。

[0060] 如图 4 所描绘，在方法 400 中的特定点处接收并使用输入信息。输入信息包括客户应用信息 401 和云系统信息 402。客户应用信息 401 包括客户 102 的客户应用拓扑信息(例如，可以从描述中具体地指明和 / 或提取)，客户 102 的客户 SLA 信息，客户 102 的 DRP105，等等。云系统信息 402 包括当前系统状态信息，政策 / 约束信息(例如，硬件和 / 或软件资源使用信息、客户概况信息、要求的性能信息、安全性约束、成本约束等信息中的一个或多个)，等等。

[0061] 在步骤 410，使用客户应用信息 401 的至少一部分和 / 或云系统信息 402 的至少一部分产生虚拟应用拓扑 415。例如，在一个实施例中，可以使用应用拓扑信息、当前系统状态信息和政策约束来产生虚拟应用拓扑 415。

[0062] 在步骤 420，使用云系统信息 402 的至少一部分和虚拟应用拓扑 415(可选地，还有客户应用信息 401 的至少一部分，尽管出于清楚的目的这被省略了)，产生可靠性绘图 425。可靠性绘图 425 标识出预期满足客户 102 的应用需求和 / 或目标的可靠性配置。在一个实施例中，可靠性绘图 425 可以表示为可靠性框图表(RBD)。注意到，有许多与可靠性绘图 425 的产生相关联的考虑。例如，冗余体系架构和故障转移方案受到处理器资源的位置的影响(例如，处理器资源是否位于同一多核芯片中，位于同一刀片上，跨多个刀片，跨底架，在 LAN 之内，跨 LAN，等等)。例如，还可以考虑内存和磁盘的分配。例如，还可以考虑磁盘分配，文件系统和数据库配置，本地还是远程。此外，可靠性绘图 425 的产生可以更加复杂，因为容错要求(例如，如 DRP105 所指明)可能仅仅是问题的一部分(例如，在确定最优配置时，连同 DRP105，性能、安全性、成本等等是需要考虑的其他要素)。

[0063] 在步骤 430，使用云系统信息 402 的至少一部分和可靠性绘图 425（可选地，还有客户应用信息 401 的至少一部分，尽管出于清楚的目的这被省略了），确定物理配置 435。例如，在一个实施例中，可以使用可靠性绘图 425、当前系统状态信息和政策 / 约束信息来确定物理配置 435。物理配置 435 指明从客户 102 的可靠性绘图 425 到云系统 100 的可用物理基础架构 101（例如，到云资源 110）的映射。例如，物理配置 435 指明从客户 102 的可靠性绘图 425 到处理器、内存单元、磁盘、文件、数据库、输入输出资源、网络资源等等中的一个或多个的映射。

[0064] 图 5 描绘了从应用拓扑到物理基础架构的示例性映射。

[0065] 图 5 的示例性映射 500 对应于参照图 4 的方法 400 描绘和描述的步骤。图 5 的示例性映射 500 示出了应用拓扑 510（例如，随时间提供应用可靠性说明）、可靠性绘图 520（例如，随时间提供 DRP 说明），以及物理配置 530（例如，随时间指明到物理部件的映射），这分别对应于图 4 的虚拟应用拓扑 415、可靠性绘图 425 和物理配置 435。

[0066] 如图 5 所描绘，示例性映射 500 用于其可靠性需求随时间而改变的应用。应用随时间而改变，示出了四个示例性时间段 501_1-501_4（总体上，时间段 501），用于示出应用随时间的改变。

[0067] 应用拓扑 510 示出应用中的应用部件 511 和应用部件 511 的相关联的可靠性要求（图示地，使用 H、M 和 L 来分别标注出高度、中度和低度可靠性要求）。在时间段 501_1，应用包括两个应用部件，包括具有高度可靠性要求的第一应用部件和具有低度可靠性要求的第二应用部件。在其他的时间段 501，应用拓扑 510 随着应用的改变而改变。

[0068] 可靠性绘图 520 表示为 RBD 的形式。在时间段 501_1，应用映射成两个部件 A 和 B，其中部件 A 是冗余对 A1 和 A2（由于其高度可靠性要求）。部件 B 与部件 A 级联，并且单工操作（由于其低度可靠性要求）。在其他时间段 501，表示为 RBD 的可靠性绘图 520 随着应用拓扑 510 的改变而改变。

[0069] 物理配置 530 指明从应用的可靠性绘图（图示地，应用的 RBD 的应用部件）到云系统的可用物理基础架构的映射。例如，物理配置 530 可以指明从可靠性绘图 520 到处理器、内存单元、磁盘、文件、数据库、输入输出资源、网络链路等等中的一个或多个的映射。在时间段 501_1，包括冗余对 A1 和 A2 的应用部件 A 映射到被配置为提供这样的冗余度的两个处理器资源，应用部件 B 映射到一个处理器资源。在其他时间段 501，物理配置 530 随着表示为 RBD 的可靠性绘图 520 的改变而改变。尽管主要参照映射到处理器资源进行描绘和描述，应注意，物理配置 530 可以指明从应用的可靠性绘图 520 到任何适当的资源的映射，例如，更详细地映射到处理器资源（例如，与安全性和用户概况说明相一致对文件、数据库、I/O 和通信端口具有适当特权、读 / 写 / 执行许可和访问权的处理器，等等），映射到其他类型的资源（例如，内存单元，磁盘，文件，数据库，输入输出资源，网络链路，等等），等其他，以及以上的各种组合。

[0070] 再次回到图 1，ME126 配置为执行对云系统 100 的监视和计量功能。ME126 可以与 RSG120 的其他部件协作，以使得自可靠能力能够在云系统 100 中得到支持。

[0071] ME126 可以配置为周期性地扫描云系统 100 中的计算资源，以识别出故障，识别出安全性攻击，测量应用的性能，等等，并进一步地汇报相关联的结果（例如，故障的识别，安全性攻击的识别，性能降级的检测，等等，以及以上的各种组合）。

[0072] ME126 可以配置为在检测到异常时产生警报，相关的警报被关联和分析，以确定影响网络状况的服务的存在(或不存在)。

[0073] ME126 可配置为收集警告(例如，从云系统 100 的一些或全部网络部件)，并基于时间和 / 或空间相关性，将收集的警告相对于警报条件进行关联。

[0074] ME126 可配置为聚集云系统 100 的网络拓扑信息，并将网络拓扑信息并入到用于执行这样的关联功能的一个或多个模型中。

[0075] ME126 可配置为确定独立网络事件的根本原因，并且可选地，还将检测的网络事件标记为中断相关的(影响服务的)和非中断相关的(不影响服务的)。

[0076] ME126 可配置为计算在特定时间段中用于特定聚合级别的服务可用性，这通过以下方式实现：分析独立根本原因事件的组，以确定落入所述特定时间段的组，组合相关联事件的持续时间，以计算所述特定时间段中的中断时间的总量，将所述事件与网络拓扑信息和受事件影响的服务类型相对比，以及，使用网络影响的范围和中断时间的百分比，确定所评估的服务的总服务可用性。注意到，服务可用性的确定可以依赖于所考虑的子网络，所使用的底层网络技术，网络拓扑 / 大小，等因素。

[0077] ME126 可配置为确定可靠性完整性计量，并确定用于 CE128 使用的控制信息。参照图 6 描绘和描述了示例性地使用 ME126 来执行这样的功能。

[0078] 图 6 描绘了示例性使用图 1 的 RSG 来执行事件关联 / 聚合并确定反应性 / 前摄性控制信息。

[0079] 如图 6 所描绘，ME126 配置为执行事件关联 / 聚合，并确定反应性 / 前摄性控制信息。

[0080] ME126 接收事件 602 和政策 / 约束信息 604。如图 6 所描绘，事件 602 可以直接从云系统 100 的物理基础架构 101 接收，和 / 或从代表云系统 100 的物理基础架构 101 的其他一个或多个监视和 / 或管理元件 / 系统接收(例如，一个或多个探针，一个或多个元件管理系统(EMS)，一个或多个网络管理系统(NMS)，等等)。事件 602 的监视可以由 ME126 执行，和 / 或跨云系统 100 的物理基础架构 101 执行(例如，用于报告给 ME126)。对其执行监视的事件 602 的类型可以包括，子系统产生的软件警报、在用于各种量度的测量计数器中出现的阈值穿越、应用故障(例如，总的和 / 或部分的)、导致服务受到影响的安全性攻击、硬件故障(例如，可恢复的或不可恢复的)、业务负载的变动、网络故障，等等。如图 4 所描绘，政策 / 约束信息 604 可以包括硬件和 / 或软件资源使用信息、客户概况信息、要求的性能信息、安全性约束、成本约束等等中的一个或多个，以及以上的各种组合。

[0081] ME126 包括聚合引擎 612、关联分析引擎 614 以及处理引擎 616。ME126 还包括历史数据库 619。

[0082] 聚合引擎 612 接收与物理基础架构 101 相关联的事件 602，并对事件 602 进行聚合。在执行用于特定时间段的处理时，聚合引擎 612 可以通过分析事件 602 以确定落入该特定时间段的组，以此来聚合事件 602。聚合引擎 612 可以将聚合的事件信息提供给关联分析引擎 614 和 / 或历史数据库 619。

[0083] 关联分析引擎 614 接收聚合的事件信息(例如，从聚合引擎 612 和 / 或从历史数据库 619)，并对聚合的事件执行关联。关联分析引擎 614 可以执行任何适当的关联功能。例如，相关的事件 602 可以被关联和分析，以确定存在(或不存在)影响网络状况的服务，事件

602 可以基于时间上和 / 或空间上的相关性相对于警报条件进行关联，等等，以及以上的各种组合。关联分析引擎 614 可以将关联的事件信息提供给处理引擎 616 和 / 或历史数据库 619。

[0084] 处理引擎 619 接收政策 / 约束信息 604 并接收关联的事件信息（例如，从关联分析引擎 614 和 / 或从历史数据库 619）。

[0085] 处理引擎 616 产生可靠性完整性计量（RIM）622，其可以包括对 ME126 所监视、聚合和关联的信息的总结。处理引擎 616 可以本地地存储 RIM622（例如，存储在历史 DB619），和 / 或将 RIM622 提供给适当的系统、设备、引擎和 / 或其他部件或元件。

[0086] 处理引擎 616 产生反应性 / 预测性控制信息 624。ME126 将该反应性 / 预测性控制信息 624 提供给 CE128，用于 CE128 在执行云系统 100 的物理基础架构 101 中的控制功能时使用。例如，ME126（1）将反应性控制信息提供给 CE128 用于 CE128 的一个或多个反应性控制引擎使用，以提供云系统 100 的物理基础架构 101 中的反应性控制功能，（2）将预测性防止控制信息提供给 CE128 用于 CE128 的一个或多个预测性防止控制引擎使用，以提供云系统 100 的物理基础架构 101 中的预测性防止控制功能。

[0087] 处理引擎 616 可配置为，从 ME126 所收集的原始数据计算各种类型的性能量度（例如，关键质量指标（KQI），关键性能指标（KPI），等等）。这些量度可以计算用于包含在 RIM622 中。例如，可用于可靠性计量的性能量度可以包括用于硬件和 / 或软件的故障频率（例如，在服务层级，部件层级，或任何其他适当层级），用于硬件和 / 或软件的停机时间（例如，在服务层级，部件层级，或任何其他适当层级），用于硬件和 / 或软件的可用性（例如，在服务层级，部件层级，或任何其他适当层级），数据不可用性（例如，由于故障、安全性攻击等等）等等中的一个或多个，以及以上的各种组合。注意到，量度可以在任何适当层级指明（例如，用于虚拟化的应用或部件，用于一组虚拟化的应用或部件，用于服务，用于一组服务，用于端对端的解决方案，用于数据中心，等等，以及以上的各种组合）。注意到，性能指标可以是与所考虑的客户 102 最为相关的指标。处理引擎 616 还可以配置为将性能指标与预期值相比较。

[0088] 如图 6 所进一步描绘的，CE128 配置为从 ME126 接收反应性 / 预测性控制信息 624，并使用该反应性 / 预测性控制信息 624 来执行云系统 100 的物理基础架构 101 中的反应性 / 预测性控制功能。CE128 可以通过将相关联的反馈动作（例如，参照图 1 描绘和描述的反馈动作 137）提供给物理基础架构 101，来提供反应性控制功能和预测性防止性控制功能。注意到，在 ME126 观察并测量云系统 100 的行为的同时，CE128 关闭环路以确保测量的行为与预期行为相匹配，进一步地，如果存在偏差，则启动适当的纠正动作。进一步注意到，ME126 执行功能，并产生最终驱动 CE128 所执行的控制动作的结果（例如，ME126 将关联分析引擎 614 的结果和政策 / 约束信息 604 组合，产生包含在 RIM622 中的量度，将结果和当前状态作为历史信息存储在历史数据库 619 中，并使用政策 / 约束信息 604 和历史信息来驱动 CE128 所执行的反应性和预测性防止性控制动作）。

[0089] CE128 包括反应性控制引擎 632 和预测性防止性控制引擎 634。

[0090] 反应性控制引擎 632 从 ME126 接收反应性控制信息，在物理基础架构 101 中执行反应性控制功能。反应性控制引擎 632 可配置为用动作进行响应，以从某种状况（例如，事件、故障，等等）中恢复。例如，恢复动作可以包括，执行进程的重新开始，执行处理器重引导

并在另一处理器上(例如,本地的或远程的)执行进程的重新开始,重新建立失效的网络连接,在存储单元上执行重新开始,执行与软故障有关的恢复动作(例如,数据的重新初始化,进程的重新存储或重置,等等),等等,以及以上的各种组合。反应性控制引擎 632 可以配置为运行诊断测试,以识别状况的来源或根本原因。

[0091] 预测性防止控制引擎 634 从 ME126 接收预测性防止性控制信息,并在物理基础架构 101 中执行预测性防止性控制功能。预测性防止控制引擎 634 可配置为执行预测性防止性措施,诸如,执行重组,执行再均衡动作,执行审计,执行预先测试,等等。

[0092] 例如,预测性防止控制引擎 634 可配置为对资源进行重组(例如,由于构成新服务或由于系统中出现的近期事件而进行的动态模型构建,改变现有复合服务的结构的再构成,等等)。

[0093] 例如,预测性防止控制引擎 634 可配置为执行碎片整理(例如,通过周期性对存储系统进行碎片整理来使得磁盘访问更加平滑更加有效,从而改善性能,节约磁盘寿命)。

[0094] 例如,预测性防止控制引擎 634 可配置为执行动态可靠性建模,其中动态可靠性计算是基于失效数据的递增更新。在一个实施例中,动态可靠性建模集中于从运行时数据收集到可靠性评估的整个过程,重点在于数据收集和动态建立概况,而不是仅使用历史数据。在一个实施例中,RIM622 可以动态更新,因为软件被重新构成以满足云系统 100 的变化的环境。

[0095] 例如,预测性防止控制引擎 634 可配置为执行再均衡操作(例如,通过对服从于政策 / 约束信息 604 的可用资源上的负载进行再均衡)。

[0096] 例如,预测性防止控制引擎 634 可配置为执行审计。在一个实施例中,执行周期性审计,以追踪物理和逻辑资源,维持数据完整性并确保安全性。在一个实施例中,可以对(1)资源库(例如,CPU,内存,I/O 以及网络资源)以及(2)基础架构的拓扑(例如,包括冗余配置的部件之间的连接性)执行审计。在一个实施例中,对用户数据库和文件执行审计,以确保数据完整性和揭露任何潜在问题。

[0097] 例如,预测性防止控制引擎 634 可配置为执行前摄性测试。在一个实施例中,前摄性测试可以包括,执行服务进行中的模拟攻击、故障边缘条件测试、以及与计划的维护动作(例如,拔下插头)有关的测试。在一个实施例中,这样的前摄性测试的至少一部分依赖于物理基础架构 101 中的虚拟无限资源的可用性。这种类型的测试可以帮助确保云系统 100 持续保持健壮。

[0098] 以这样的方式,RSG120 配置为使得云系统 100 能够作用为自可靠的系统。

[0099] 尽管参照 RSG120 的提供特定功能的特定部件(图示地,CE122,SE124,ME126 和 CE128)进行了初步描绘和描述,不过应注意,RSG120 的功能可以使用任何适当的一个或多个部件来提供。例如,描绘和描述为分别由图示的部件所执行的功能可以以不同方式跨所图示的部件分布。例如,可以使用一个或多个其他部件(例如,取代于和 / 或附加于图示的部件)来提供被描绘和描述为由图示的部件所执行的功能。

[0100] 尽管参照云系统 100 中的 RSG120 的特定部署(例如,使用特定的分布式体系)进行了初步描绘和描述,但可以了解,RSG120 可以使用任何其他适当的部署,包括集中地或分散地部署 RSG120 的各个功能,在云系统 100 中执行。

[0101] 因此,可以了解,RSG120 可以以任何适当的方式并入到云系统 100 中。

[0102] 在一个实施例中，RSG120 可以使用以下项目并入到云系统 100 中：(1) 虚拟层，由一个或多个计算存储单元(CSU)构成，其示例性实施例参照图 7 和 8 进行描绘和描述，(2)物理层，由一个或多个系统控制单元(SCU) 构成，其示例性实施例参照图 9 进行描绘和描述。

[0103] 图 7 描绘了适用于实现图 1 的 RSG 的自可靠的计算存储单元(CSU)的一个实施例。

[0104] CSU700 是云系统 100 的分布式版本的抽象基本构造框图。CSU700 可以由客户 102 指明，客户 102 期望 CSU700 是安全的以及可恢复的。CSU700 可以基于可以由客户 102 提供的各种参数(例如，SLA103，DRP105，QoS 参数，等等) 来控制。客户 102 还可以提供有关信息(例如，分布式云系统的拓扑，用于分布式云系统的管控政策规则，等等)。注意到，客户域可包括一个或多个 CSU。在客户域包括多个 CSU700 的情况下，多个 CSU700 可以彼此通信，以形成虚拟的分布式计算机器。在一个实施例中，RSG120 嵌入在每个 CSU700 中，以确保每个 CSU700 如所指示的那样自可靠。

[0105] CSU700 包括虚拟机(VM) 710，虚拟存储卷体(VSV) 720，虚拟子网接口(VSI) 730，虚拟探针(VP) 740，虚拟可靠性 / 安全性守卫(VRSG) 750，CSU 控制器(CC) 760，以及 CSU 说明(CS) 770。

[0106] VM710 包括配置为提供 CSU700 的各种功能的处理器和相关联的内存。它可以作为基本计算引擎使用，配置用于若干级别的性能和可靠性。

[0107] VSV720 为 CSU700 提供存储。VSV720 可以包括一个或多个数据库，一个或多个文件，一个或多个磁盘，一个或多个闪存部件，等等，以及以上的各种组合。

[0108] VSI730 提供到云系统 100 的其他 CSU700 的接口(例如，用于共享与 VM710 相关联的虚拟内存，用于共享 VSV 中的存储，等等)。VSI730 可以支持安全连接，以提供这样的共享能力。参照图 8 描绘和描述示例性分布式自可靠云系统，该云系统使用多个 CSU700，它们经由多个相关联的 VSI730 通信。

[0109] VP740 收集用于 CSU700 的使用率、可靠性、性能和安全性数据。

[0110] VRSG750 配置为，作为 CSU700 的 RSG120 操作，执行参照图 1-6 描绘和描述的分别由 CE122、SE124、ME126 和 CE128 执行的配置、调度、监视和控制功能。VRSG750 还可配置为监视和管理 CSU700 的部件(例如，用于监视和管理 CSU700 中的部件的恢复，包括执行恢复动作，该恢复动作用于从其中执行 VRSG750 的 CSU700 和 / 或具有其他 VRSG750 的 CSU700 内的故障中恢复)。

[0111] CC760 配置为管理 CSU400 的操作。CC760 可以与云提供商交互。CC760 还可以经由 VRSG750 监视虚拟基础架构的状态。CC760 配置为与 SCU 通信。

[0112] CS770 维持与 CSU700 相关联的属性(例如，CPU 要求，内存要求，用于 VSV720 的存储卷体附加，经由 VSI730 与其他 CSU700 的连接，可靠性等级，恢复方案，在诸如故障之类的状况时的行为，可扩展性政策属性，QoS 属性，安全性约束，性能约束，等等，以及以上的各种组合)。注意到，在 CSU700 内的元件之间可能存在安全性，类似地，在包含多个自可靠 CSU700 的分布式云系统的情况下，在自可靠 CSU700 之间也可能存在安全性。CS770 可以通过供应来支持属性的改变。

[0113] 如本文所述，客户域可以包括任何适当数目的 CSU700。在其中客户域包括多个 CSU700 的一个实施例中，多个 CSU700 可以彼此通信，以形成分布式自可靠云系统，该系统配置为操作为虚拟的分布式的计算机器。在一个这样的实施例中，多个 CSU700 的 VRSG750

可以经由多个 CSU700 的 VSI730 彼此通信，以形成分布式子可靠云系统。参照图 8 描绘和描述一个例子。

[0114] 图 8 示出图 7 的多个 CSU 在客户域的示例性部署，以形成分布式自可靠云系统。

[0115] 如图 8 所描绘，客户域 800 包括三个 $CSU700_1$-700_3，其中每个 CSU700 如参照图 7 的 CSU700 所描绘和描述的那样实现。

[0116] 三个 CSU700 配置为经由通信网络 810 彼此通信。更具体地，CSU700 的 VRSG750 配置为通过经由 CSU700 各自的 VSI 访问通信网络 810 来彼此通信。在一个实施例中，如果 CSU700 在物理服务器上巩固合并，于是相关联的对平台的网络化需求加强，那么可以将本地通信虚拟化（例如，取代于将 CSU700 之间的所有通信强制到平台的物理层），其中虚拟化可以以任何适当方式执行（例如，使用一个或多个虚拟交换机，其可以配置为像物理交换机一样运作，但是被虚拟化到平台，或者以其他适当方式运作）。

[0117] 三个 CSU700 可以配置为使用可靠适应性分布协议（RADP）彼此通信。RADP 使得三个 CSU700 能够交换各种类型的信息（例如，关于可靠性、安全性、性能、拓扑、事件数据等中的一个或多个的信息，以及以上的各种组合），从而使得三个 CSU700 能够协调动作。

[0118] 注意到，可以支持其他有关通信的能力。例如，在一个实施例中，缺省网络被局限为在同一子网上的 VM710 之间交换。例如，在一个实施例中，VSV720 仅对于同一 CSU700 内的连接和映像可见。例如，在一个实施例中，CSU700 之间对来自 VSV720 的信息的共享局限为通过安全路径传输。

[0119] 以这样的方式，云提供商可以使用通信网络 810 的延伸和标度，跨物理基础架构 101 有效地分布云服务。

[0120] 如以上注意到的，RSG120 除了使用由一个或多个 CSU700 构成的虚拟层，还可以使用由一个或多个 SCU 构成的物理层，由此并入到云系统 100 中。

[0121] 图 9 描绘了在图 1 的云系统的一部分中部署的、适用于在图 1 的 RSG 中执行的系统控制单元（SCU）的一个实施例。

[0122] 如图 9 所描绘，简化的物理基础架构 900 包括物理资源部分 910 和 SCU920。

[0123] 物理资源部分 910 包括物理基础架构 900 的物理资源 911（其可以是参照图 1 描绘和描述的物理基础架构 101 的一部分）和管理程序 919。

[0124] 物理资源 911 可以包括计算资源，内存资源，输入输出资源，存储资源，等等，以及以上的各种组合。

[0125] 管理程序 919 配置为提供物理资源 911 的管理功能。管理程序 919 配置为支持 CPU 虚拟化，从而使得 CPU 能够被多个操作系统所共享。管理程序 919 可以提供各种其他功能。

[0126] SCU920 配置为提供 CSU 管理功能，用于管理客户域的 CSU（例如，图 7 的 CSU700 中的一个或多个）。SCU920 配置为与客户域的 CSU700 的 CC760 通信。SCU920 配置为执行 CSU 管理功能，这可以包括诸如创建 / 管理 / 删除虚拟部件，管理针对 CSU 内和 CSU 间交互而限定的连接性政策等功能，以及以上的各种组合。

[0127] SCU920 包括主机管理器（HM）921，资源管理器（RM）922，存储管理器（SM）923，物理可靠性 / 安全性守卫（PRSG）924，以及物理探针（PP）925。

[0128] HM921 在特许的虚拟机中的物理主机上（例如，主机 OS）运行，管理和批准在物理主机上发生的动作。HM921 通过中转对物理主机的各种资源（例如，计算，存储，网络，等等）

的访问，迫使CSU700彼此隔离并与SCU920隔离。HM921将抽象虚拟模型转译成适合于物理主机的底层管理程序919的配置数据。HM921与SM923交互，以根据主机化的虚拟机的要求，创建和移除虚拟块设备。CSU700可以执行为单个共享物理网络上的虚拟覆盖网络，而不需要任何特殊硬件。网络层提供资源控制，以限制虚拟机带宽消耗并区分其优先次序。

[0129] SCU920和管理程序919可以协作，以执行从虚拟应用拓扑到云系统的物理基础架构的映射(例如，如参照图4和图5所描绘和描述的)。客户102指明对于虚拟机、虚拟存储块和虚拟网络的想要的拓扑，其中预期指明的拓扑满足一组定义的约束。上述约束包括，允许的通信样式、虚拟机托管约束、QoS约束等等，以及以上的各种组合。拓扑和约束描述可以响应于各种条件(例如，负载条件，故障条件，等等)而动态改变。客户域的CSU700于是可以自动地适应以满足改变的要求。注意到，在存储侧，存在可扩展的、持久的以及加密的存储，该存储即使是在负载条件下也允许服务维持数据吞吐量。

[0130] 参照图1-9描绘和描述的自可靠体系可以利用和/或提供各种其他能力和/或技术，其中的至少一部分对于自可靠体系内的服务可靠性具有支撑和关联。

[0131] 第一能力涉及自可靠体系背景下的故障模式和恢复。

[0132] 在许多情况下，自可靠系统与冗余度和容错有关。由于没有单一部件可以确保100%正常运行时间，所述体系允许个别部件出现故障而不影响整个系统的可用性。自可靠操作预期，分布式系统中的许多系统(如果不是全部的话)可以容忍它所依赖的其他系统的故障。

[0133] 在一个实施例中，RSG120在虚拟层级和在物理层级处负责检测、抑制各种类型的故障并从中恢复。在一个这样的实施例中，由于云系统100的物理基础架构的共享特性，错误抑制可以担当极高的重要性。

[0134] 在一个实施例中，可以支持以下的故障类型和相关联的恢复模式：(1)进程故障(例如，本地进程重置/重启；进程在另一CPU上重启；进程在另一托管的刀片、支架、容器和/或CPU上重启；进程在远程CPU上重启，以及其他)，(2)应用故障(例如，本地重启；另一CPU，刀片，支架，容器；遍布服务器的多个进程，远程的，其他的)，(3)处理器/CPU故障(例如，CPU，刀片，支架，容器，站点的故障；其他)，以及(4)网络故障(例如，链路、节点等的故障，网络路径的周期性审计，其他)。

[0135] 在一个实施例中，一旦检测到错误，立即“检疫隔离”物理单元。冻结安全性边界。该恢复可以由DRP105、与云系统100相关联的系统状态信息和/或与云系统100相关联的政策/约束信息来指导。恢复策略可以是预先建立的，或者可以由RSG120决定。在恢复策略由RSG120决定的一个实施例中，RSG120可以基于一个或多个因素(例如，可靠性等级，成本，性能，安全性考虑，等等)决定恢复策略。例如，在从进程故障恢复的情况下，RSG120可以决定在本地重启进程，在同一刀片上的另一处理器上重启进程，在同一机架中的不同刀片上重启进程，在另一支架中的刀片上重启进程，或者在远程支架中的刀片上重启进程。RSG120可以针对其他类型的故障条件和相关联的恢复模式做出其他决定。

[0136] 第二能力涉及在自可靠体系的背景下提供前摄性测试。

[0137] 在一个实施例中，前摄性测试的目的是周期性地执行服务进行中的弹性和鲁棒性测试，以确保系统的准备就绪能够实际上经受住故障。例如，前摄性测试可以包括，模拟各种条件来验证云系统100在所模拟的条件下继续运行的能力。例如，前摄性测试可以包括

模拟故障边缘条件，以验证云系统 100 在高压力条件期间继续运作的能力。

[0138] 在一个实施例中，RSG120 周期性执行这样的测试，该测试随机禁用产品实例，以确保云系统 100 可以经受住这样的常见类型的故障，而不影响客户。在一个实施例中，RSG120 执行前摄性诊断，以揭露无声故障（silent failure）。在一个实施例中，云系统 100 的“无限资源”的特点使得 RSG120 能够以更大的规模执行活动的、备用的恢复场景。在至少一些这样的实施例中，测试可以设计为覆盖任何适当的部件（例如，CPU，内存，存储器，I/O，网络，等等，以及以上的各种组合）。

[0139] 在一个实施例中，RSG120 可以支持适用于评估云系统 100 的可靠性和安全性的一个或多个服务进行中的测试。例如，RSG120 可配置为执行服务进行中的配置测试，诸如：（1）使用多个版本的网络驱动器，调节 OS 和驱动器等级网络设置，使内核获得热修复，并将其施用于服务中；（2）切换虚拟化提供商，改变 TCP/IP 主机模型，以及（3）在多个地理位置核查配置和运行时问题。例如，RSG120 可以配置为执行服务进行中的破坏和故障转移测试，诸如：（1）随机地启用、禁用、断连和重连处理器、内存、磁盘、网络端口等资源，以模拟故障和 / 或维护动作并触发恢复动作，（2）对处理器和数据库执行故障转移测试，确保跨 CSU700 存在数据的多份冗余拷贝，并核查 N+1 冗余度，以及（3）周期地或恒常地进行安全性攻击。例如，RSG120 可配置为执行服务进行中的负载和能力测试，诸如，验证云系统 100 应付由不常见的活动导致的大的负载尖峰的能力，以及，验证云系统 100 应付瞬时故障的连锁效应的能力。例如，RSG120 可配置为执行服务进行中的延迟和超时测试，诸如，（1）核查超时，设置侵略性的超时，核查低效运行，以及验证恢复时间，（2）在客户服务器通信层诱导人为延迟，以模拟服务降级并测量上游服务响应以及核查依赖性故障。例如，RSG120 可配置为执行服务进行中的审计和健康核查测试，诸如，（1）在每个实例上运行健康核查，监视健康的外部迹象（例如，CPU 负载）以检测不健康的实例，执行在线测试（例如，使用坏的输入，缺乏命令条目，以及类似条件）以揭露事务性故障，（2）执行测试以找出那些不遵从最佳实践的子系统实例，（3）搜索不使用的资源并确保它们被返回到可用资源池，以及（4）运行测试以找出安全性违反或弱点。

[0140] 第三能力涉及在自可靠体系的背景下，数据的完整性 / 安全性和数据的机密性。总体来说，客户 102 易于受到可靠性问题引起的数据丢失。在一个实施例中，使用 RSG120，每个 CSU700：（1）保护客户免于彼此的不法行为，（2）保护基础架构免于客户的不法行为，（3）保护客户免于提供商的不法行为。注意到，安全性故障可以因为以下原因中的一个或多个而产生：不是所有资源都得到虚拟化，虚拟化软件有程序缺陷，代码毁坏的情况，不正确的网络虚拟化（它允许客户访问云提供商基础架构的敏感部分或其他客户的资源）。

[0141] 第四能力涉及在自可靠体系的背景下数据的可用性 / 不可用性。

[0142] 在许多情况下，软件应用和数据对于商业相当重要，从而使得，在软件应用和 / 或数据不可用时（例如，由于中断的状况），商业被延缓或者甚至潜在地停滞，直到可用性得到恢复。在短期内，这样的中断状况导致数据丢失，员工和客户受挫，失去收益。长期地，这样的中断状况会在整个商业的生命期对该商业造成影响（并且，丢失记录、交易和 / 或会计文件甚至可能将商业置于违反法规的风险中）。可以了解，数据可能因为许多原因而变得不可用，这可以用状态图表来表示，该图表汇总从数据完全可访问的正常状态（标注为正常状态）到数据部分可用或不可用的异常状态的转变。例如，当系统由于安全性攻击而受到黑客

袭击时(标注为袭击状态),由于操作员失误或程序瑕疵而当机时(标注为当机/受损状态),由于丢失加密密钥而变得不可用时(标注为当机/受损状态),或者经历计划中的维护动作时(标注为维护状态),会出现上述异常状态。

[0143] 在一个实施例中,RSG120 配置为保卫客户数据以确保其可用性不会受损。RSG120 可以通过审计、服务进行中的测试、数据修复,等等,以及以上的各种组合,来保卫客户数据。注意到,数据备份和存储方案通常是灾难恢复计划的主要组成。在一个实施例中,客户数据可以根据需要容易地、自动地移动。在一个实施例中,可以通过在多个位置存储客户数据的多个拷贝,其中数据保持同步,以此恢复客户数据。在一个实施例中,可以针对特定类型的条件而指明数据恢复策略(例如,在文件或数据库或磁盘故障的情况下,可以使用以下数据恢复策略中的一个或多个:(1)冷备份方案,其中抓取文件快照,并存储和备份文件;(2)暖备份方案,其中为客户保留资源;(3)热备份方案,其中由远程站点处的同步化资源管理数据的复制(例如,在中断的情况下,作为副本的替代性的故障转移站点立即接管)。

[0144] 第五能力涉及自可靠体系背景下的错误和警告处理。

[0145] 在一个实施例中,RSG120 配置为执行主动监视,以在客户服务受到影响之前早期检测 CSU700 和 SCU920 上的异常行为。

[0146] 在一个实施例中,VRSG750 配置为分析问题,确定相关联的防止性控制动作。在一个这样的实施例中,VRSG750 配置为,响应于接收到 CSU700 的部件检测到异常事件并恢复时产生的警报,执行这样的功能。

[0147] 在一个实施例中,VRSG750 配置为处理各种类型的输入信息,以提供各种控制功能(例如,控制,过滤,错误分析,等等,以及以上的各种组合)。

[0148] VRSG750 可以处理关于每个 CSU700 的信息,以提供各种控制功能。云系统 100 配置为,在其操作期间,在任何或所有层级(例如,在物理 SCU 层级,虚拟 CSU 层级,网络层级,服务层级,等等中的一个或多个),产生异常事件(例如,警报,警告,等等)。云系统 100 还配置为,收集各种类型的性能数据。如果达到异常条件,被监视的事件变量的值会遭受到阈值。在至少一些情况下,应用过滤准则,记录满足准则的变量(例如,在日志文件中)。应理解,对于每个时间间隔,存在有限数目的事件变量被记录。事件变量捕获相关联的部件的行为,并提供附加的上下文用于事件处理。例如,事件变量可以包括,攀升的函数错误,恢复的陷入/异常,CPU 总使用率,内存总使用率,中断的事务,进程重启,发送的错误 TPDU,接收的错误 TPDU,发生传输超时,健全超时的数目,刀片重启,故障转移的数目,磁盘访问故障,文件访问故障,磁盘使用,以及关键警告的数目。如以上注意到的,VRSG750 配置为处理关于每个 CSU700 的这样的信息,以提供各种控制功能。

[0149] VRSG750 可以接收和处理来自若干源的信息(例如,来自 CSU750 的部件的自主故障报告,来自客户和对等 VRSG750 的问题报告,来自 VRSG750 的诊断/训练/审计的结果,(4)来自性能管理器的损伤指示,来自配置管理器的网络配置数据,等等,以及以上的各种组合)。VRSG750 配置为整合这样的信息,并提供诸如控制、过滤、错误分析之类的功能。作为 VRSG750 进行这样的处理的结果,可以识别故障的基础架构资源,辨识出错误的根本原因,安排和规划修复动作,并将故障的资源返回到服务。

[0150] VRSG750 和 PRSG924 可以配置为接收事件通知。警报和警告采集可以包括硬件和/或软件事件,其中的至少一些基于 CSU700 (用于 VRSG750) 和 SCU920 (用于 PRSG924) 所

指明的准则在本地主机中进行处理。在一个实施例中，即使状况得到解决，事件通知也被发送到PRSG750和VRSG924。以这样的方式，可以保持历史信息用于特征分析并确定可能的防止性动作。注意到，在软件错误的情况下，仅仅相对小数目的这样的错误会导致不可恢复的异常，因为大部分错误通常被异常处理器所解决。进一步注意到，至少一些动作由主机机器在本地执行，在这样的情况下，可以只是通知PRSG750和PRSG924已采取的动作。

[0151] 第六能力涉及自可靠体系架构背景下的可靠和可扩展存储。在许多情况下，为了满足规模和成本的目标，云系统用商品服务器、磁盘和网络的集群构建，它们分布在多个地理上分散的数据中心。注意到，在这样的环境中，可能有大数目的故障场景(例如，磁盘故障，网络中断，电力分布中断和灾难，等等)。于是，在一些情况中的底层存储系统的语义不明时，从存储故障进行恢复对于云应用的开发者来说非常困难。例如，导致数据不一致的故障状况包括部分写入、存储节点冲突、网络分区、在多个站点的多个读取者/写入者，等等。在一个实施例中，客户可以指明不同的编码，以实现不同的成本、能力和可靠性的平衡。例如，临时的、容易再创建的数据可以以最小冗余度进行存储，而耗成本的、档案性的数据可以广泛分散，以提高可靠性，存储可以提供最终一致的语义，等等。在一个实施例中，存储系统可以在不同操作条件下(例如，数据的复制，RAID，擦除编码，等等)提供不同类型的冗余度和一致性。

[0152] 第七能力涉及自可靠体系背景下的性能和超负荷。在许多情况下，对服务的需求随时间而变化，从而导致性能不可预测。应理解，为数据中心提供仅持续数据中心的操作时间中的很小百分比的峰值负载条件将导致数据中心资源的利用。于是，可以优选现购现付方案(例如，对计算资源按小时计费)。然而，现购现付方式也可能具有相关联的问题(例如，需求是预先未知的(例如，在开始是很大的尖峰，后面是稳定的业务量)，经由云所购买的小时可以随时间不均匀地变化，等等)。此外，许多服务还经历季节性或周期性的需求变化(例如，十二月中的电子商务，由于新事件导致的非预期的需求，等等)。并且，性能降级可能是由于故障、超负荷或设计(例如，由于计划中的受控的超负荷政策控制而导致的失去交易可用性，业务量超负荷，VM之间的I/O性能的变化，VM之间的I/O干扰，等等，以及以上的各种组合)。

[0153] 第八能力涉及自可靠体系背景下的电源管理和硬件寿命。在一些情况下，数据中心具有大数目的服务器上的大数目的用户(例如，支持几百万用户的几千个服务器)。在许多这样的情况下，电源和冷却是主要的问题和开销。在一个实施例中，通过使用软件栈、可扩展的存储、具有密集刀片的服务器块、具有基于闪存的非易失性存储器的分解的存储器刀片、跨层的电源管理等等，以及以上的各种组合，可以使得基础架构的各个部分更加高效。在一个实施例中，可以通过软件策略延长硬件寿命，所述软件策略例如是自动的磁盘碎片整理，其防止或延迟客户抱怨的最常见原因之一，等等。

[0154] 第九能力涉及自可靠体系背景下的系统可用性和商业连续性。注意到，连续性是另一个因素，因为单个公司进行的云计算服务的管理是单点故障(例如，甚至对不同位置的多个数据中心，它们具有共同的软件基础架构、账目、和其他共同的元件和能力)。在一个实施例中，支持商业连续性策略。在一个这样的实施例中，商业连续性策略可以不仅仅指明数据恢复，因为在多数情况下，数据仅仅是真正的商业连续性和灾难恢复计划的一个组成。

[0155] 尽管独立地对分开的能力进行了初步描述，但是注意到，可以一起使用这样的能

力的各种组合，以提供各种功能。

[0156] 图 10 描绘了用于为云系统的客户提供可靠性的方法的一个实施例。注意到，当结合本文描绘和描述的图 1 到图 9 的相关部分进行考虑时，可以更好地理解方法 1000 的各个步骤。

[0157] 在步骤 1010，方法 1000 开始。

[0158] 在步骤 1020，接收客户的 DRP。该客户可以是管理云系统的云提供商的客户。

[0159] 在步骤 1030，基于客户的 DRP，确定用于该客户的云资源的配置。

[0160] 在步骤 1040，使用确定的云资源的配置，为该客户配置云资源。

[0161] 在步骤 1050，监视云系统的状况和 / 或潜在状况。

[0162] 在步骤 1060，确定是否检测到一个或多个状况。如果没有检测到状况，那么方法 1000 返回步骤 1050（也就是，继续监视云系统的状况和 / 或潜在状况）。如果检测到状况，方法 1000 前进到步骤 1070。

[0163] 在步骤 1070，基于检测到的状况，启动一个或多个动作。从步骤 1070，方法 1000 返回到步骤 1050（也就是，继续监视云系统的状况和 / 或潜在状况）。

[0164] 注意到，在云系统中，可靠性仅仅是要考虑的一个组成（例如，要考虑的其他组成包括，性能，安全性，成本，等等）。因此，尽管本文参照云系统的可靠性和可用性方面的考虑进行了初步描绘和描述，但是应理解，参照改善云系统的可靠性和可用性方面所描绘和描述的各种原则、能力和功能可以扩展，以处理一个或多个这样的其他考虑（例如，性能，安全性，成本，等等）。

[0165] 尽管在云系统的背景下进行了初步描绘和描述，注意到，本文描绘和描述的各种能力和功能可以适用于其他环境。例如，本文在云系统的背景下描绘和描述的各种能力和功能可以适用于机器对机器的环境，智能计量环境，等等。

[0166] 图 11 描绘了适用于执行本文描述的功能的计算机的高层级框图。

[0167] 如图 11 所描绘，计算机 1100 包括处理器元件 1102（例如，中央处理单元（CPU）和 / 或其他适当的处理器）以及存储器 1104（例如，随机存取存储器（RAM），只读存储器（ROM），等等）。计算机 1100 还可以包括协作模块 / 过程 1105 和 / 或各种输入 / 输出设备 1106（例如，用户输入设备（诸如键盘，键板，鼠标，等等），用户输出设备（诸如显示器，扬声器，等等），输入端口，输出端口，接收器，发送器，和存储设备（例如，磁带驱动器，软盘驱动器，硬盘驱动器，光盘驱动器，等等））。

[0168] 可以了解，本文描绘和描述的功能可以用软件执行（例如，通过在一个或多个处理器上执行软件）和 / 或可以用硬件执行（例如，使用通用目的计算机，一个或多个应用专用集成电路（ASIC），和 / 或任何其他硬件等同物）。

[0169] 可以了解，本文描绘和描述的功能可以用软件执行（例如，在通用目的计算机上执行（例如，经由一个或多个处理器的执行），以执行特殊目的计算机）和 / 或可以用硬件执行（例如，使用一个或多个应用专用集成电路（ASIC），和 / 或任何其他硬件等同物）。

[0170] 在一个实施例中，协作过程 1105 可以被加载到存储器 1104 并由处理器 1102 执行，以执行本文讨论的功能。因此，协作过程 1105（包括相关联的数据结构）可以存储在计算机可读的存储介质上，例如，RAM 存储器，磁盘或光盘驱动器或软盘，等等。

[0171] 应理解，图 11 描绘的计算机 1100 提供适用于执行本文描述的功能元件和 / 或本

文描述的功能元件的部分的通用体系和功能性。例如，计算机 1100 提供适用于执行本文描述的各种物理资源、模块、单元、元件、部件等等中的一个或多个的通用体系和功能性。

[0172] 可以设想，本文描述的作为软件方法的一些步骤可以在硬件中执行，例如，作为与处理器协作来执行各种方法步骤的电路。本文所描述的功能 / 元件的部分可以执行为计算机程序产品，其中计算机指令当由计算机处理时可调配计算机的操作，使得本文描述的方法和 / 或技术得到调用或以其他方式提供。调用发明性方法的指令可以存储在固定的或可移除的介质中，经由广播或其他信号承载介质中的数据流传输，和 / 或存储在根据指令进行操作的计算设备中的存储器中。

[0173] 权利要求指明各个实施例的方面。下面编号的条款指明各个实施例的那些和其他方面 ：

[0174] 1. 一种装置，包括 ：

[0175] 处理器和存储器，所述处理器配置为 ：

[0176] 接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数 ；以及

[0177] 基于所述客户的 DRP 确定用于该客户的云资源的配置。

[0178] 2. 如条款 1 所述的装置，其中 DRP 配置为被指明为与客户相关联的服务级别协定（SLA）的一部分。

[0179] 3. 如条款 1 所述的装置，其中所述云资源包括计算资源、内存资源、输入输出资源、存储资源和网络资源中的至少一个。

[0180] 4. 如条款 1 所述的装置，其中所述处理器配置为通过以下方式基于客户的 DRP 确定用于客户的云资源的配置 ：

[0181] 使用客户应用信息以及与云提供商的云系统相关联的云系统信息，确定用于客户的虚拟应用拓扑 ；

[0182] 使用用于客户的所述虚拟应用拓扑以及与所述云系统相关联的云系统信息，确定可靠性绘图 ；以及

[0183] 使用所述可靠性绘图和与所述云系统相关联的云系统信息，确定云资源的配置。

[0184] 5. 如条款 4 所述的装置，其中所述云系统信息包括，政策信息和约束信息中的至少一个，以及与所述云系统相关联的当前系统状态信息。

[0185] 6. 如条款 4 所述的装置，其中所述可靠性绘图表示为可靠性框图表（RBD），其配置为就应用部件的各自可靠性需求以及应用部件之间的至少一个关系而言来表示应用的多个应用部件。

[0186] 7. 如条款 1 所述的装置，其中所述处理器配置为，在多个时间段的每一个中确定用于客户的云资源的配置。

[0187] 8. 如条款 1 所述的装置，其中所述处理器还配置为 ：

[0188] 监视云资源的行为，用以确定所述 DRP 中指明的可靠性参数是否得到满足。

[0189] 9. 如条款 1 所述的装置，其中所述处理器还配置为 ：

[0190] 计量用以满足所述 DRP 中指明的可靠性参数的所述云资源的行为。

[0191] 10. 如条款 1 所述的装置，其中所述处理器还配置为提供配置引擎，该配置引擎配置为 ：

[0192] 处理与所述客户相关联的 DRP，以产生虚拟配置；以及

[0193] 将所述虚拟配置提供给调度引擎，该调度引擎配置为将虚拟配置映射到云资源。

[0194] 11. 如条款 1 所述的装置，其中所述处理器配置为提供调度引擎，该调度引擎配置为：

[0195] 接收虚拟配置，该虚拟配置满足与客户相关联的 DRP；以及

[0196] 将该虚拟配置映射到云资源。

[0197] 12. 如条款 1 所述的装置，其中所述处理器配置为提供监视引擎，该监视引擎配置为：

[0198] 使用所述云系统的云提供商所指明的政策信息和约束信息中的至少一个和与云提供商的云系统相关联的系统状态信息，产生可靠性完整性计量和配置用以在控制云系统的云资源时使用的控制信息中的至少一个。

[0199] 13. 如条款 12 所述的装置，其中所述监视引擎包括：

[0200] 聚合引擎，配置为接收并聚合与所述云系统的物理基础架构相关联的事件；

[0201] 关联分析引擎，配置为对聚合的事件进行关联，以形成与所述云系统相关联的系统状态信息；以及

[0202] 处理引擎，配置为处理所述云系统的云提供商所指明的政策信息和约束信息中的至少一个和与所述云系统相关联的所述系统状态信息，以产生可靠性完整性计量和配置用以在控制云系统的云资源时使用的控制信息中的至少一个。

[0203] 14. 如条款 12 所述的装置，其中所述可靠性完整性计量包括，系统状态信息和从系统状态信息导出的量度中的至少一个。

[0204] 15. 如条款 12 所述的装置，其中配置用以在控制云系统的云资源时使用的所述控制信息包括以下中的至少一个：配置为对云系统中的至少一个状况进行反应的反应性控制信息，以及配置为防止至少一个状况在云系统中发生的预测性防止性控制信息。

[0205] 16. 如条款 1 所述的装置，其中所述处理器配置为提供控制引擎，该控制引擎配置为：

[0206] 接收控制信息，所述控制信息配置为用以在控制云资源时使用；以及

[0207] 使用所述控制信息，产生至少一个反馈动作，该反馈动作配置为修改所述云资源的至少一部分。

[0208] 17. 如条款 1 所述的装置，其中所述处理器配置为支持计算存储单元（CSU），其中所述 CSU 包括以下中的至少一个：

[0209] 虚拟机，包括虚拟处理器和内存资源；

[0210] 虚拟存储卷体，包括虚拟存储资源；

[0211] 虚拟子网络接口，配置为支持与至少一个其他 SCU 的至少一个安全连接；

[0212] 虚拟可靠性 / 安全性守卫（VRSG），配置为执行以下中的至少一个：

[0213] 管理 CSU 的元件的恢复；以及

[0214] 与至少一个其他 CSU 交换可靠性、安全性、性能、拓扑和事件数据中的至少一个；

[0215] 虚拟探针，配置为收集用于 CSU 的利用率、可靠性、性能和安全性数据中的至少一个；

[0216] 控制器，配置为管理所述 CSU；以及

[0217] CSU 说明，包括 CSU 的多个属性。

[0218] 18. 如条款 1 所述的装置，其中所述处理器布置在物理主机上，其中所述处理器配置为支持用于物理主机的系统控制单元（SCU），其中 SCU 包括以下中的至少一个 ：

[0219] 主机管理器（HM），配置为执行以下中的至少一个 ：管理所述物理主机上的动作，创建和删除用于所述物理主机上使用的计算存储单元（CSU），以及强制进行在所述物理主机和至少一个其他物理主机上的 CSU 之间的安全通信 ；

[0220] 资源管理器（RM），配置为管理所述物理主机上的资源 ；

[0221] 存储管理器（SM），配置为管理所述物理主机上的存储 ；

[0222] 物理可靠性 / 安全性守卫（PRSG），配置为监视和管理物理主机上的 CSU 的恢复 ；以及

[0223] 物理探针，配置为收集与所述物理主机相关联的利用率、可靠性、性能和安全性数据中的至少一个。

[0224] 19. 一种计算机可读存储介质，用于存储指令，所述指令当被计算机执行时，致使计算机执行一种方法，该方法包括 ：

[0225] 接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数 ；以及

[0226] 基于所述客户的 DRP 确定用于该客户的云资源的配置。

[0227] 20. 一种方法，包括 ：

[0228] 使用处理器，用以 ：

[0229] 接收与云提供商的客户相关联的动态可靠性概况（DRP），其中所述 DRP 指明依据时间和所述客户的应用或服务的要求两者的该客户的可靠性参数 ；以及

[0230] 基于所述客户的 DRP 确定用于该客户的云资源的配置。

[0231] 尽管本文详细示出和描述了并入有本发明的教导的各种实施例，本领域技术人员可以容易地设计出也并入有这些教导的许多其他变形的实施例。

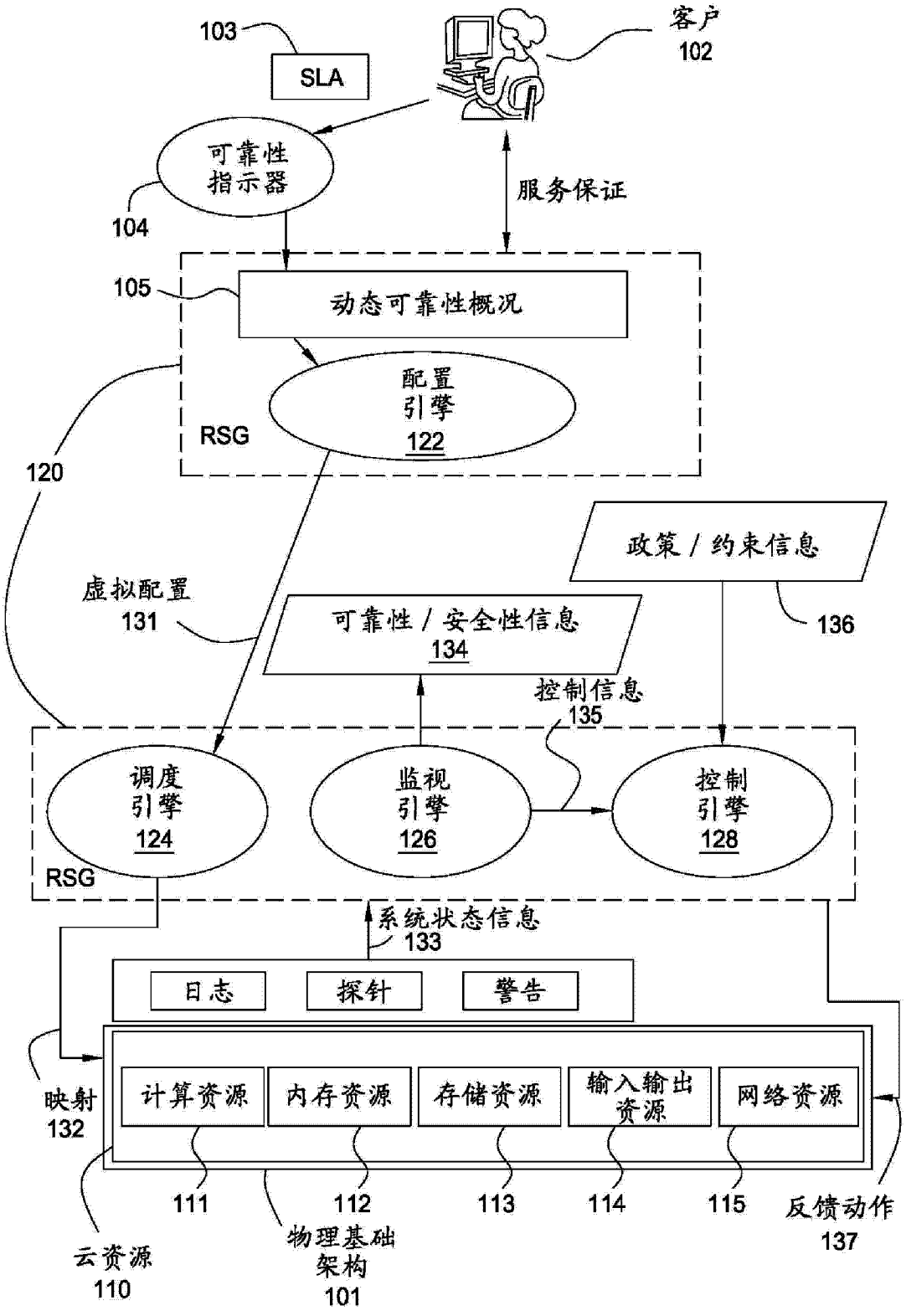

103
SLA
客户
102
可靠性
指示器
104
服务保证
105
动态可靠性概况
配置
引擎
122
RSG
120
政策 / 约束信息
虚拟配置
131
可靠性 / 安全性信息
134
136
控制信息
135
调度
引擎
124
监视
引擎
126
控制
引擎
128
RSG
系统状态信息
133
日志
探针
警告
映射
132
计算资源
内存资源
存储资源
输入输出
资源
网络资源
111
112
113
114
115
反馈动作
137
云资源
110
物理基础
架构
101

图 1

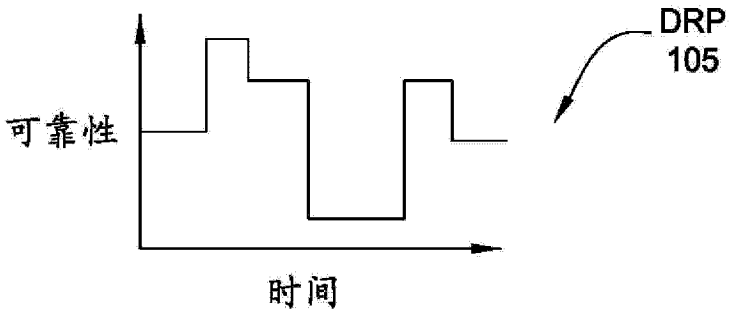

DRP
105
可靠性
时间

图 2

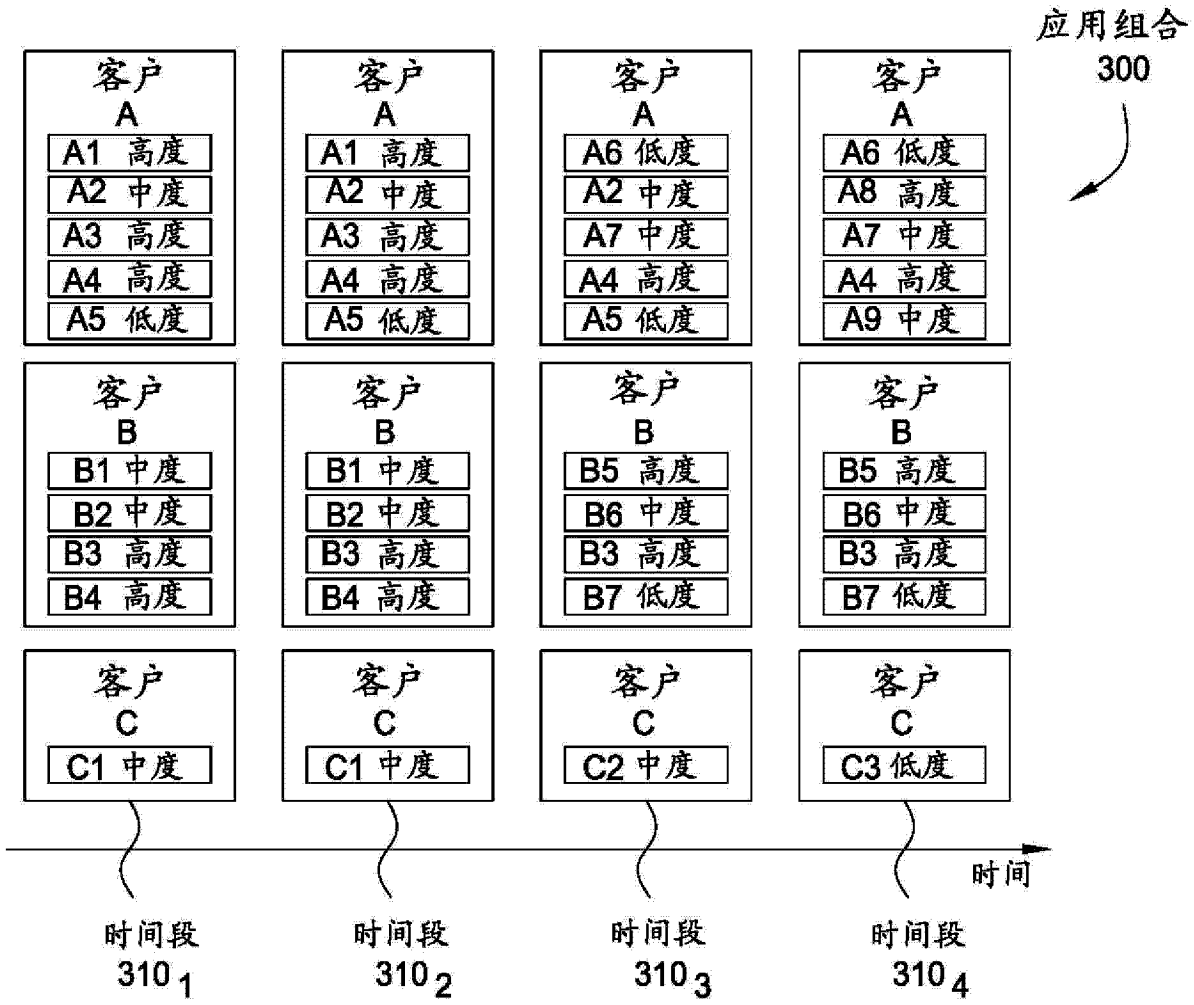

应用组合
300
客户 A
A1 高度
A2 中度
A3 高度
A4 高度
A5 低度
客户 A
A1 高度
A2 中度
A3 高度
A4 高度
A5 低度
客户 A
A6 低度
A2 中度
A7 中度
A4 高度
A5 低度
客户 A
A6 低度
A8 高度
A7 中度
A4 高度
A9 中度
客户 B
B1 中度
B2 中度
B3 高度
B4 高度
客户 B
B1 中度
B2 中度
B3 高度
B4 高度
客户 B
B5 高度
B6 中度
B3 高度
B7 低度
客户 B
B5 高度
B6 中度
B3 高度
B7 低度
客户 C
C1 中度
客户 C
C1 中度
客户 C
C2 中度
客户 C
C3 低度
时间
时间段 310 1
时间段 310 2
时间段 310 3
时间段 310 4

图 3

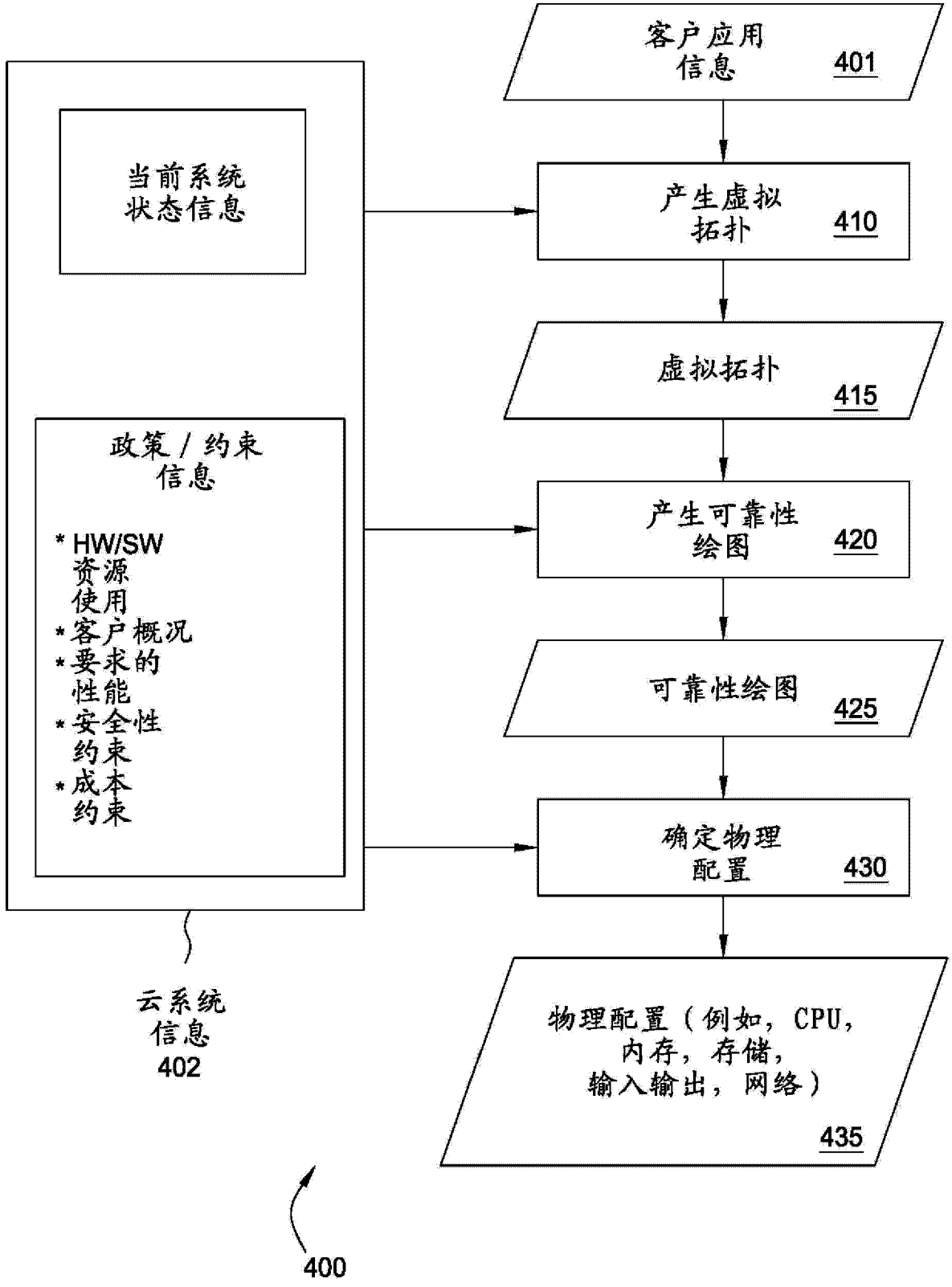

客户应用
信息
401
当前系统
状态信息
产生虚拟
拓扑
410
虚拟拓扑
415
政策 / 约束
信息
* HW/SW
资源
使用
*客户概况
*要求的
性能
*安全性
约束
*成本
约束
产生可靠性
绘图
420
可靠性绘图
425
确定物理
配置
430
物理配置（例如，CPU，
内存，存储，
输入输出，网络）
435
云系统
信息
402
400

图 4

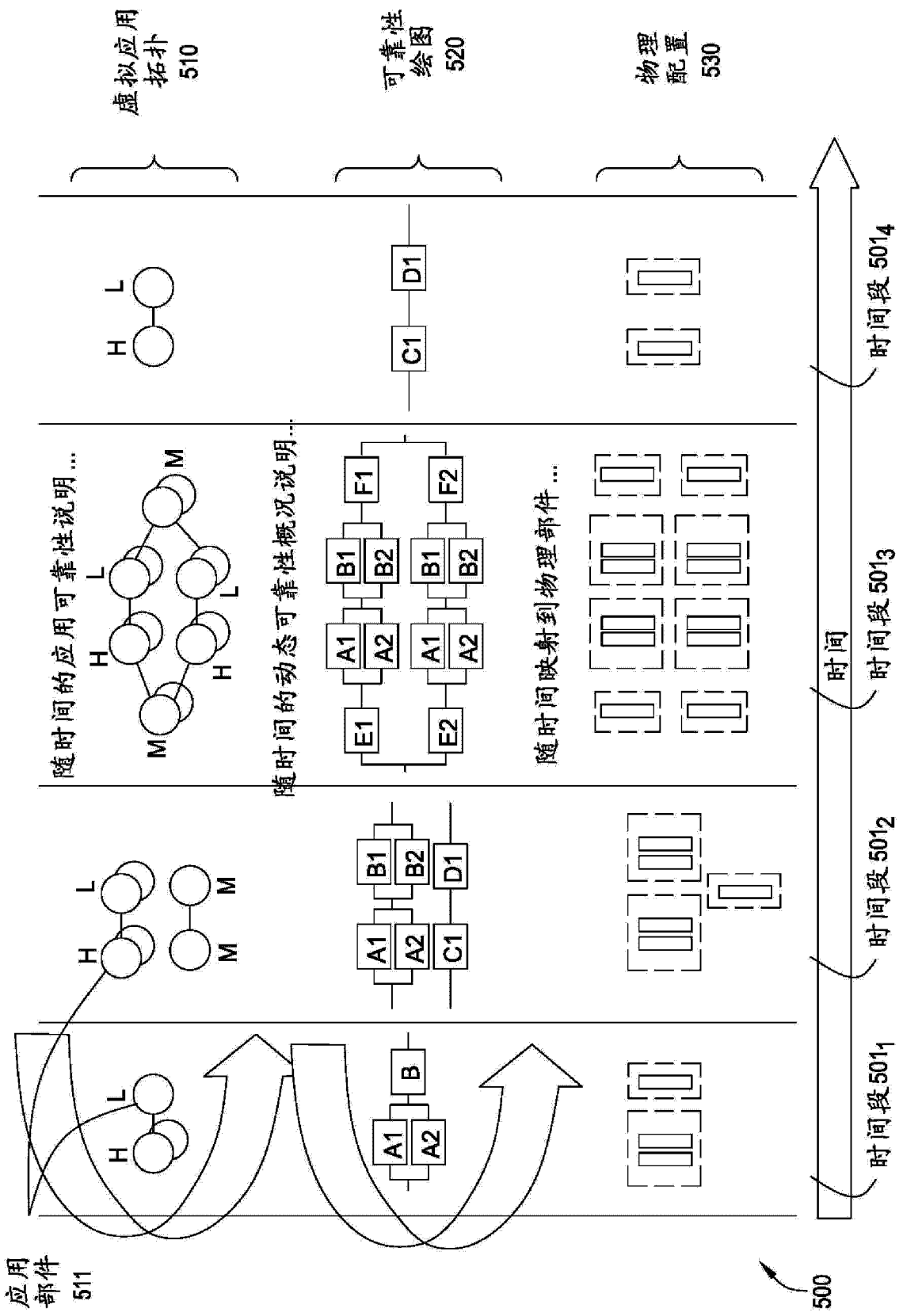

虚拟应用拓扑 510
可靠性绘图 520
物理配置 530
随时间的应用可靠性说明...
随时间的动态可靠性概况说明...
随时间映射到物理部件...
应用部件 511
时间
时间段 501₁
时间段 501₂
时间段 501₃
时间段 501₄
500
H
L
M
A1
A2
B
B1
B2
C1
D1
E1
E2
F1
F2

图 5

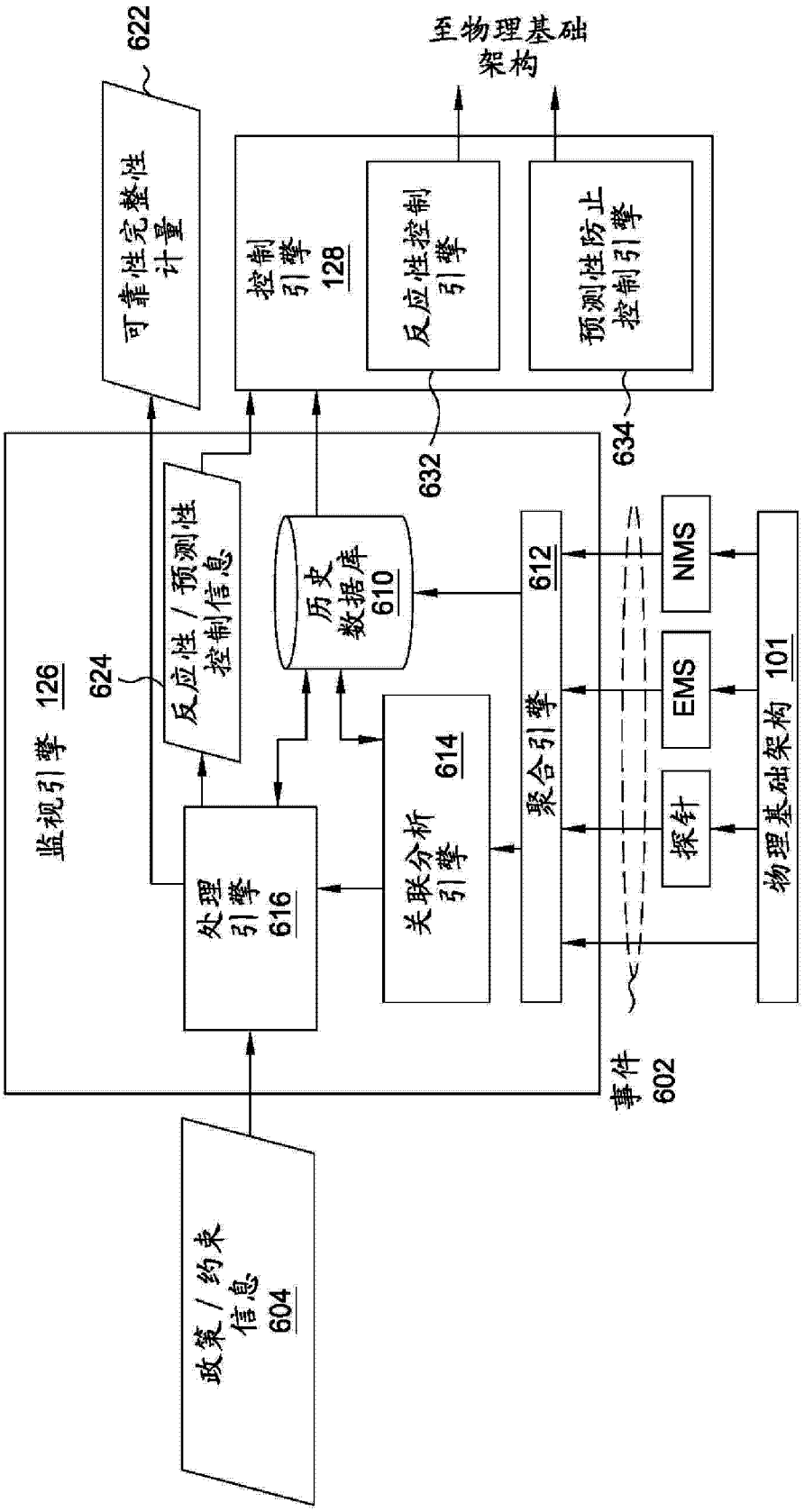

622
至物理基础架构
可靠性完整性计量
控制引擎 128
反应性控制引擎
预测性防止控制引擎
632
634
监视引擎 126
624
反应性 / 预测性控制信息
历史数据库 610
612
NMS
EMS
探针
物理基础架构 101
处理引擎 616
关联分析引擎 614
聚合引擎
事件 602
政策 / 约束信息 604

图 6

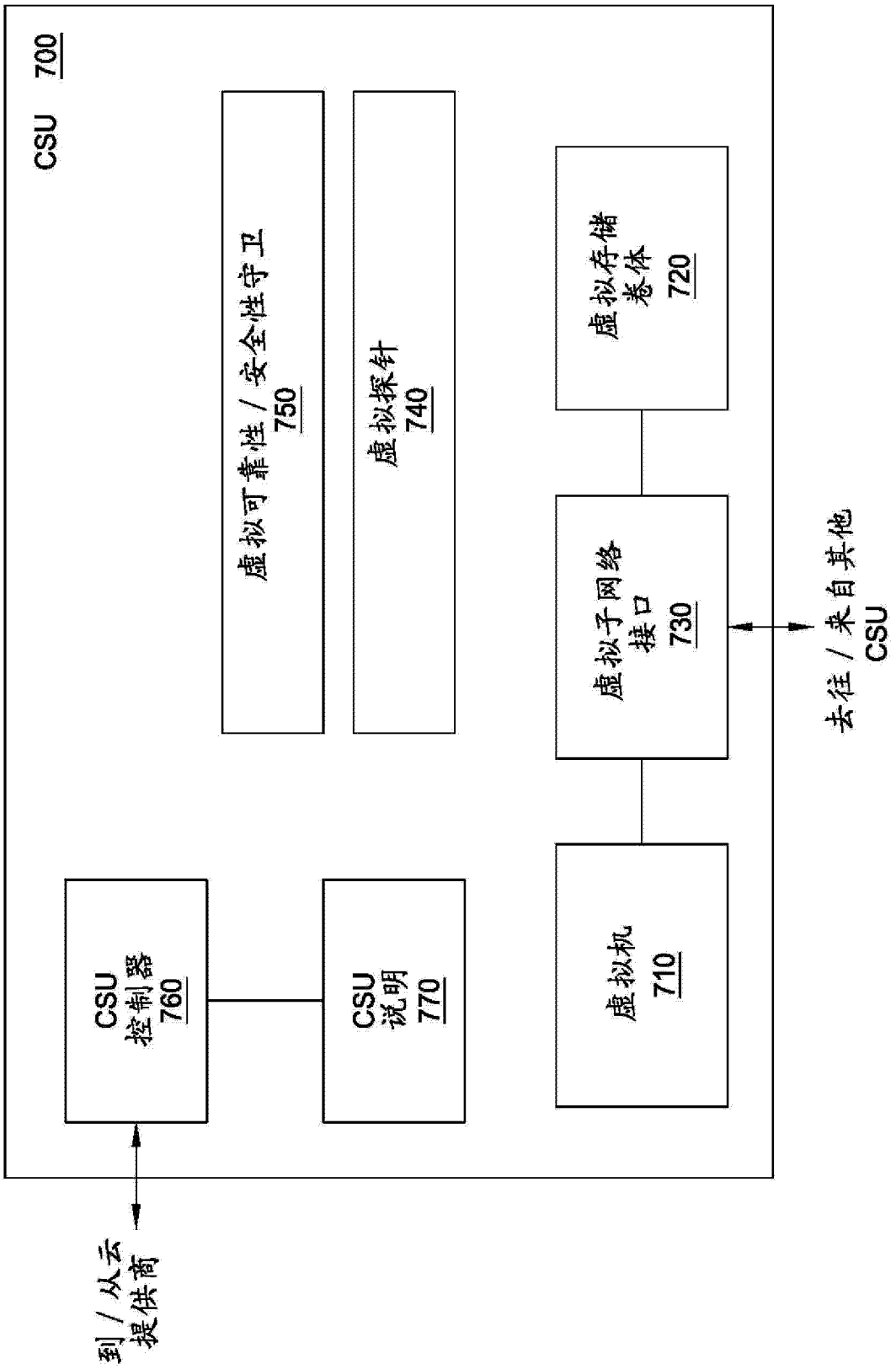

CSU 700
虚拟可靠性 / 安全性守卫 750
虚拟探针 740
虚拟存储卷体 720
虚拟子网络接口 730
虚拟机 710
CSU 控制器 760
CSU 说明 770
到 / 从云提供商
去往 / 来自其他 CSU

图 7

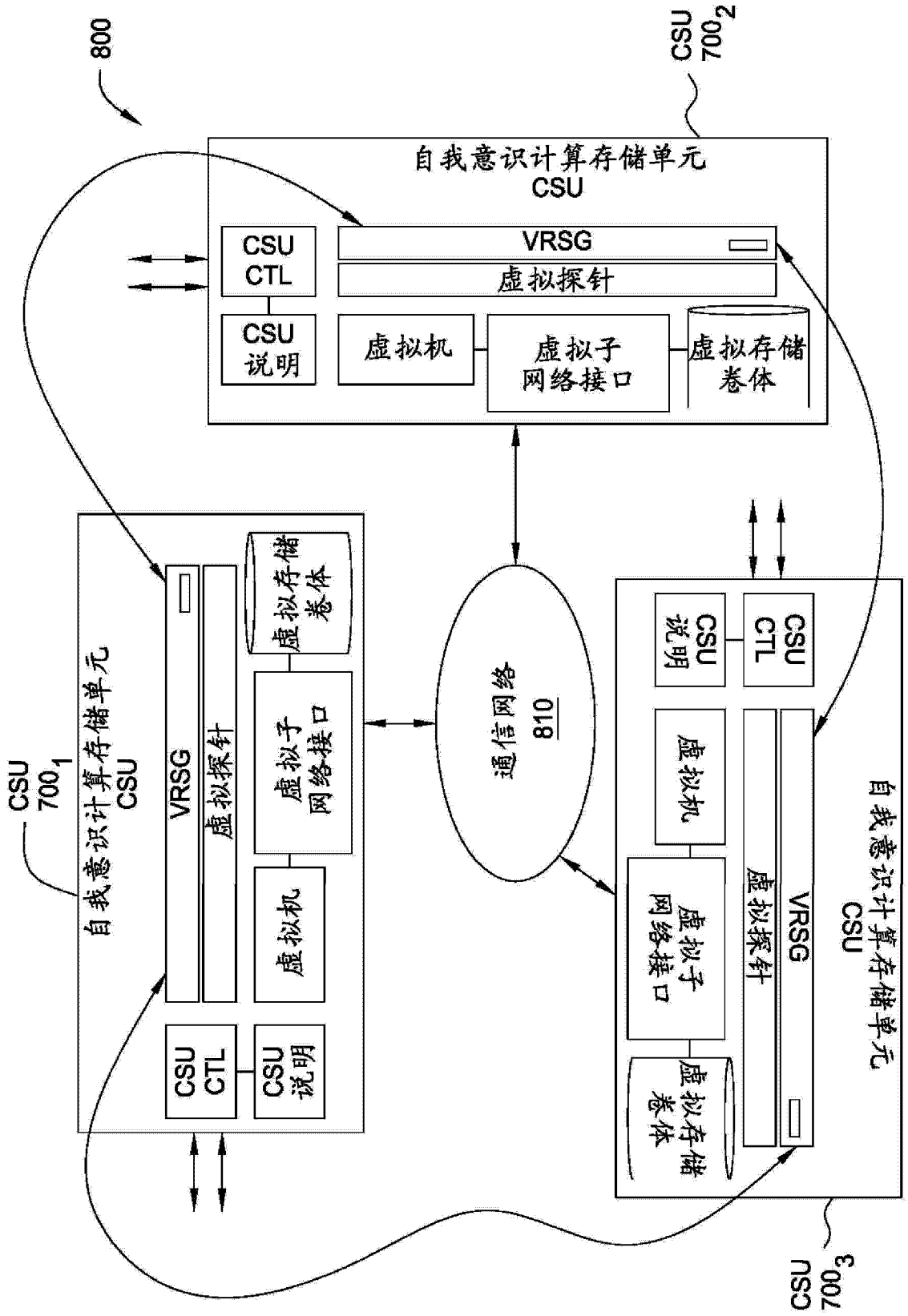

800
CSU 700 2
自我意识计算存储单元 CSU
CSU CTL
VRSG
虚拟探针
CSU 说明
虚拟机
虚拟子网络接口
虚拟存储卷体
通信网络 810
CSU 700 1
自我意识计算存储单元 CSU
VRSG
虚拟探针
虚拟存储卷体
虚拟子网络接口
虚拟机
CSU CTL
CSU 说明
CSU 700 3
自我意识计算存储单元 CSU
CSU 说明
CSU CTL
虚拟机
虚拟子网络接口
虚拟存储卷体
虚拟探针
VRSG

图 8

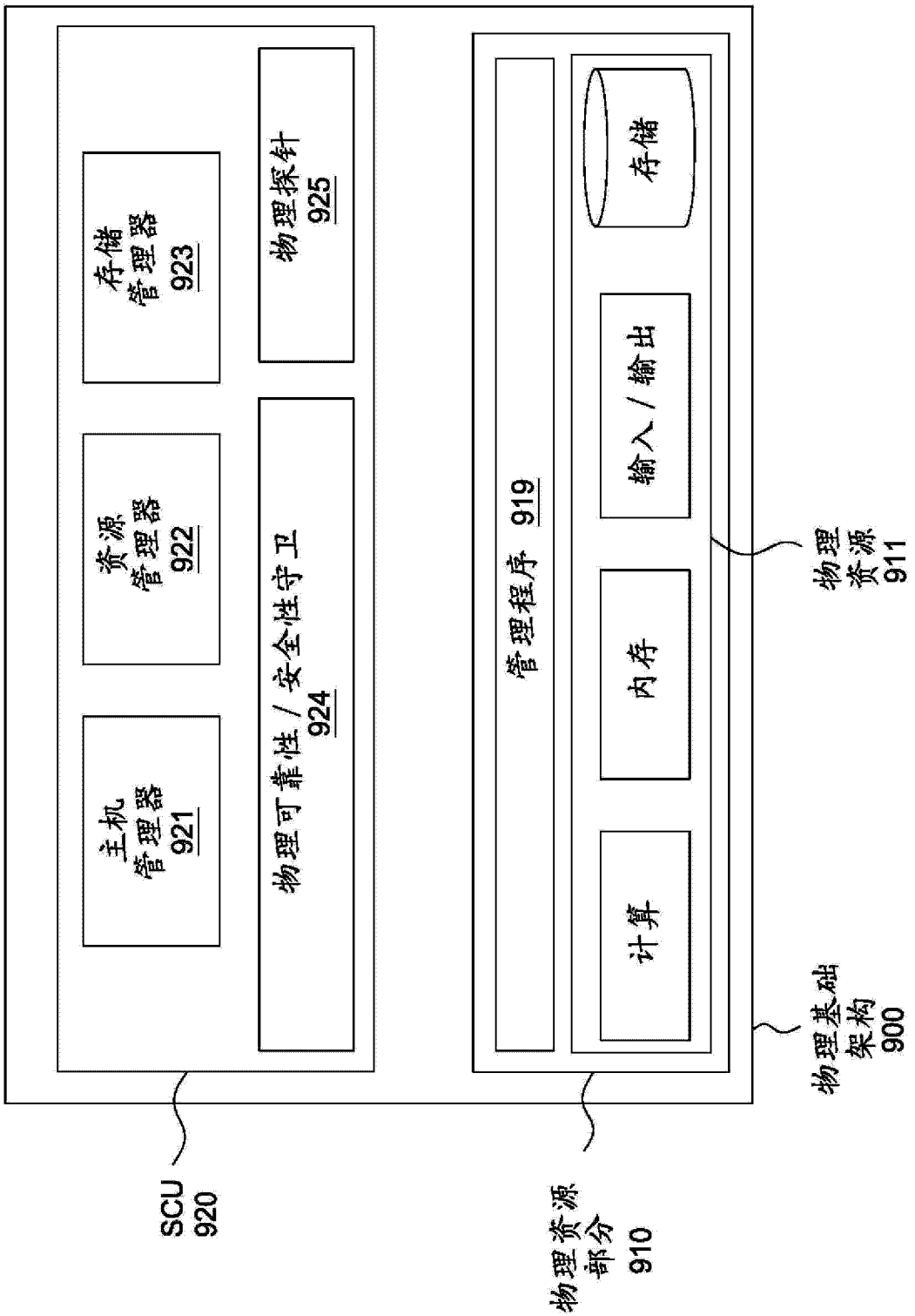

主机
管理器
921
资源
管理器
922
存储
管理器
923
物理可靠性 / 安全性守卫
924
物理探针
925
SCU
920
管理程序 919
计算
内存
输入 / 输出
存储
物理资源
911
物理基础
架构
900
物理资源
部分
910

图 9

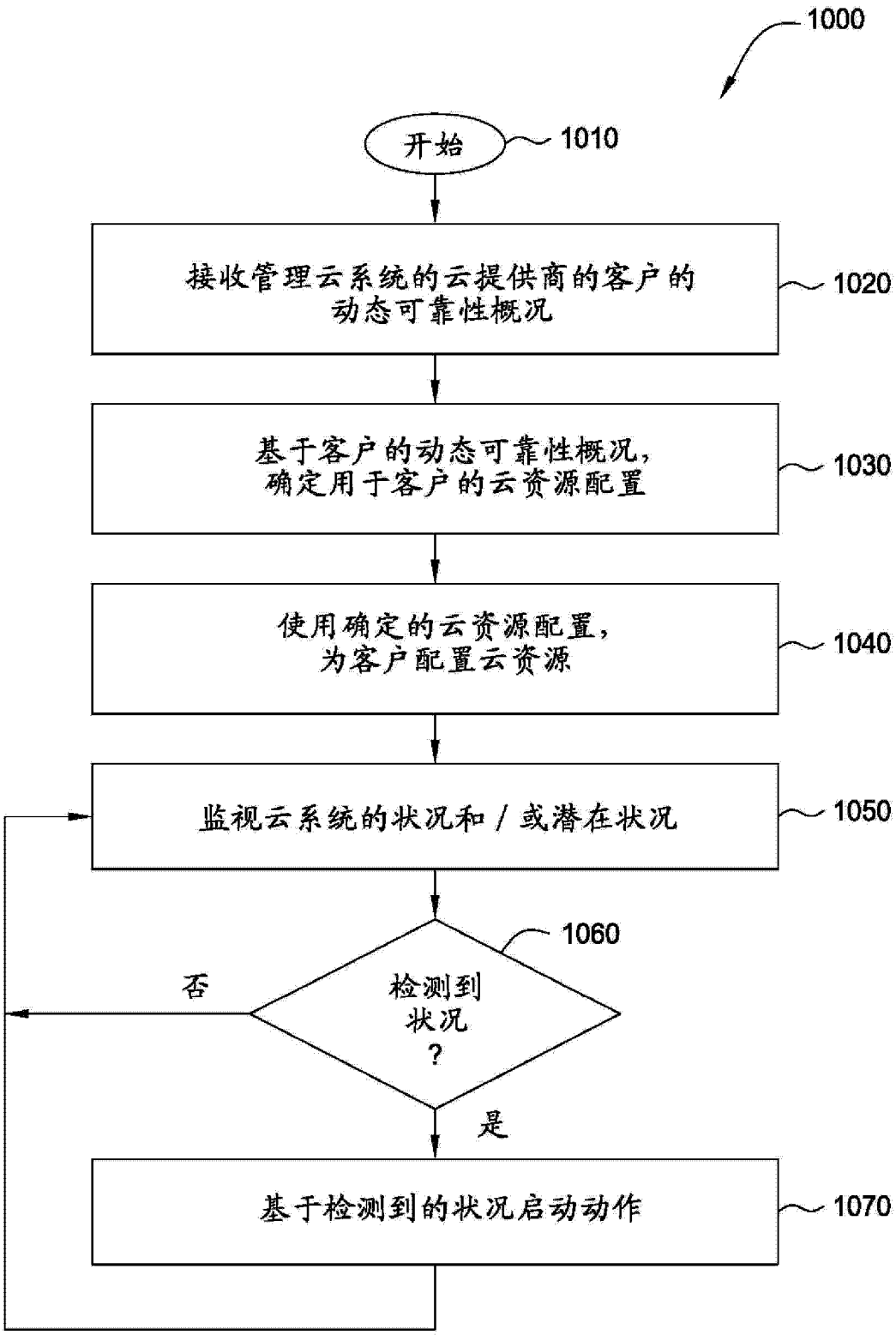

1000
开始
1010
接收管理云系统的云提供商的客户的动态可靠性概况
1020
基于客户的动态可靠性概况，确定用于客户的云资源配置
1030
使用确定的云资源配置，为客户配置云资源
1040
监视云系统的状况和 / 或潜在状况
1050
1060
检测到状况？
否
是
基于检测到的状况启动动作
1070

图 10

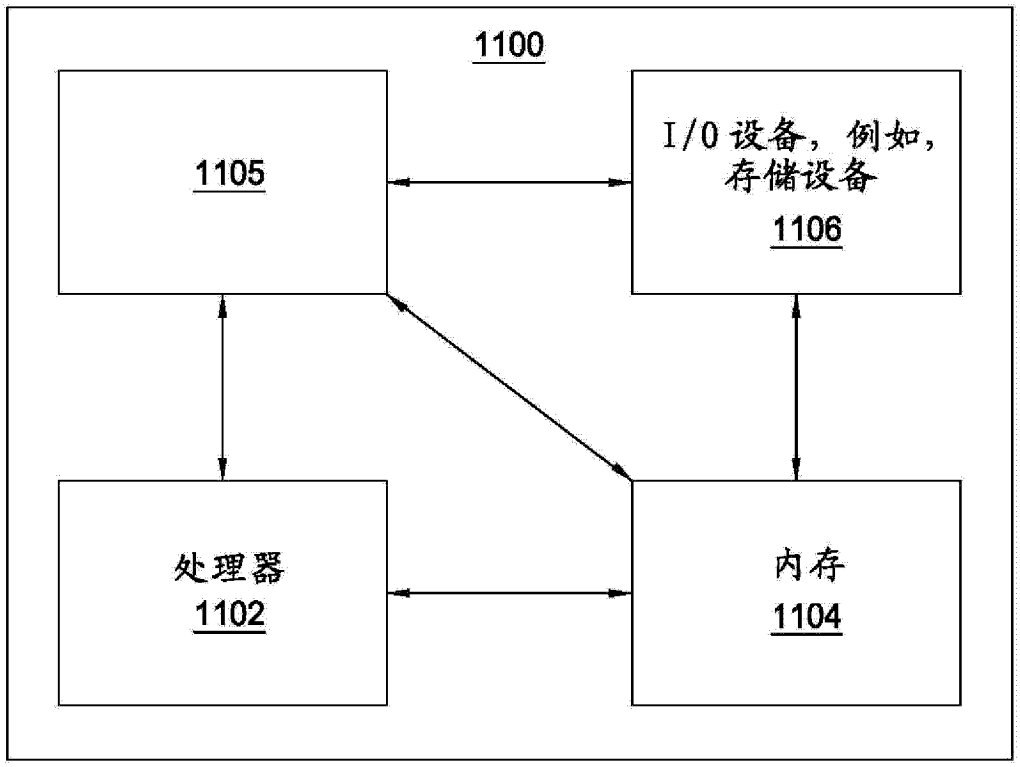


图 11