

说明书

发明名称：一种公共云的扩展方法、设备、系统及存储介质

[0001] 本申请要求于2022年04月15日提交中国专利局、申请号为202210396407.5、申请名称为“一种公共云的扩展方法、设备、系统及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及云技术领域，尤其涉及一种公共云的扩展方法、设备、系统及存储介质。

背景技术

[0003] 公共云，是指把公共云提供方提供的基础设施作为一种服务，通过互联网对外提供。在这种服务模型中，用户不用自己构建数据中心，而是可通过租用的方式来使用服务器、存储和网络等基础设施。公共云服务通过提供虚拟环境(例如虚拟机)实现，公共云的核心属性是多用户共享云基础设施且用户之间隔离。

[0004] 目前，随着公共云的需求越来越多，公共云提供方需要以公共云为中心逐步拓展分布式云的边界。而在拓展边界的过程中，如何保证公共云的安全性成为亟待解决的问题。

[0005] 发明内容

[0006] 本申请的多个方面提供一种公共云的扩展方法、设备、系统及存储介质，用以解决公共云的扩展过程中可能出现的安全性问题。

[0007] 本申请实施例提供一种公共云的扩展方法，为公共云创建扩展可用区，所述扩展可用区铺设于用户机房中，所述公共云上配置有安全网关，所述方法适用于所述安全网关，包括：

[0008] 接收所述扩展可用区中的物理设备发起的认证请求，所述认证请求中包含所述物理设备的身份信息；

[0009] 在所述物理设备的身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；

[0010] 基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。

- [0011] 本申请实施例还提供一种公共云的扩展方法，为公共云创建扩展可用区，所述扩展可用区铺设于用户机房中，所述公共云上配置有安全网关，所述方法适用于所述扩展可用区中的物理设备，包括：
- [0012] 基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；
- [0013] 在身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；
- [0014] 基于所述网关代理程序，将所述物理设备中发起的针对所述公共云的流量引流至所述安全隧道，以通过所述安全隧道将所述扩展可用区纳管至所述公共云中。
- [0015] 本申请实施例还提供一种网关设备，部署于公共云中，所述公共云创建有扩展可用区，所述扩展可用区铺设于用户机房中，所述网关设备包括存储器、处理器和通信组件；
- [0016] 所述存储器用于存储一条或多条计算机指令；
- [0017] 所述处理器与所述存储器和所述通信组件耦合，用于执行所述一条或多条计算机指令，以用于：
- [0018] 通过所述通信组件接收所述扩展可用区中的物理设备发起的认证请求，所述认证请求中包含所述物理设备的身份信息；
- [0019] 在所述物理设备的身份信息认证成功的情况下，建立所述网关设备与所述物理设备之间的安全隧道；
- [0020] 基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。
- [0021] 本申请实施例还提供一种物理设备，公共云创建有扩展可用区，所述扩展可用区铺设于用户机房中，所述物理设备位于所述扩展可用区中，所述物理设备包括存储器、处理器和通信组件；
- [0022] 所述存储器用于存储一条或多条用于网关代理的计算机指令；
- [0023] 所述处理器与所述存储器和所述通信组件耦合，用于执行所述一条或多条计算机指令，以用于：

- [0024] 基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；
- [0025] 在身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；
- [0026] 基于所述网关代理程序，将所述物理设备中发起的针对所述公共云的流量引流至所述安全隧道，以通过所述安全隧道将所述扩展可用区纳管至所述公共云中。
- [0027] 本申请实施例还提供一种公共云的扩展系统，包含安全网关和为所述公有云创建的扩展可用区，所述安全网关部署于公共云中，所述扩展可用区铺设于用户机房中；
- [0028] 所述扩展可用区中的物理设备，用于基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；
- [0029] 所述安全网关用于接收所述认证请求；在所述物理设备的身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。
- [0030] 本申请实施例还提供一种存储计算机指令的计算机可读存储介质，当所述计算机指令被一个或多个处理器执行时，致使所述一个或多个处理器执行前述的公共云的扩展方法。
- [0031] 在本申请实施例中，为公共云创建扩展可用区，扩展可用区部署在用户机房中，这样，公共云的硬件设施以软硬一体化方式部署到用户机房，可满足用户的数据安全、数据本地处理、低延时等需求；而通过将扩展可用区纳管至公共云上，使得用户在本地即可拥有与公共云一致的使用体验，且扩展了公共云的边界；将扩展可用区作为不受信环境，通过部署在公共云中的安全网关对扩展可用区中的物理设备进行身份认证，建立起扩展可用区中物理设备与安全网关之间的安全隧道，基于安全网关对扩展可用区与公共云之间的进出流量进行严格校验，从而可保证公共云扩展过程中的安全性。

附图说明

- [0032] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：
- [0033] 图1为本申请一示例性实施例提供的一种公共云的扩展方法的逻辑示意图；
- [0034] 图2为本申请一示例性实施例提供的一种公共云的扩展方法的逻辑示意图；
- [0035] 图3为本申请一示例性实施例提供的一种示例性的握手方案的逻辑示意图；
- [0036] 图4为本申请一示例性实施例提供的一种公共云扩展方案的逻辑示意图；
- [0037] 图5为本申请一示例性实施例提供的一种双向透明方案的逻辑示意图；
- [0038] 图6为本申请一示例性实施例提供的另一种公共云的扩展方法的流程示意图；
- [0039] 图7为本申请另一示例性实施例提供的一种网关设备的结构示意图；
- [0040] 图8为本申请又一示例性实施例提供的一种物理设备的结构示意图；
- [0041] 图9为本申请又一示例性实施例提供的一种公共云的扩展系统的结构示意图。

具体实施方式

- [0042] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。
- [0043] 目前，对公共云的扩展需求越来越多，本申请的一些实施例中提出：为公共云创建扩展可用区，扩展可用区部署在用户机房中，这样，公共云的硬件设施以软硬一体化方式部署到用户机房，可满足用户的数据安全、数据本地处理、低延时等需求；而通过将扩展可用区纳管至公共云上，使得用户在本地产即可拥有与公共云一致的使用体验，且扩展了公共云的边界；将扩展可用区作为不受信环境，通过部署在公共云中的安全网关对扩展可用区中的物理设备进行身份认证，建立起扩展可用区中物理设备与安全网关之间的安全隧道，基于安全网关对扩展可用区与公共云之间的进出流量进行严格校验，从而可保证公共云扩展过程中的安全性。
- [0044] 以下结合附图，详细说明本申请各实施例提供的技术方案。

- [0045] 图1为本申请一示例性实施例提供的一种公共云的扩展方法的逻辑示意图，图2为本申请一示例性实施例提供的一种公共云的扩展方法的逻辑示意图。参考图1和2，本实施例中，可为公共云创建扩展可用区，扩展可用区与公共云中的传统可用区的创建方式相同，在此不做赘述，扩展可用区与传统可用区的差别在于，扩展可用区部署于用户机房中，而传统可用区通常部署在公共云提供方自己的机房中。
- [0046] 以下先对本实施例中涉及到的技术概念进行简要解释。
- [0047] 公共云，是指把公共云提供方提供的基础设施作为一种服务通过互联网对外提供。在这种服务模型中，用户不用自己构建一个数据中心，而是通过租用的方式来使用服务器、存储和网络等基础设施，公共云通过提供虚拟环境(例如虚拟机)实现，公共云的核心数据时多用户共享云基础设施且用户之间隔离。
- [0048] 可用区，是同一区域region内，电力和网络互相隔离的物理区域。一个可用区不受其它可用区故障的影响。一个区域内不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低延迟的网络连接。前述的传统可用区和扩展可用区均具备此处提及的可用区通用属性。
- [0049] 虚拟私有网络(Virtual Private Cloud, VPC)：VPC设置于公共云中，VPC是公共云服务的用户在云上数据中心的局域网。具体而言，VPC隔离了虚拟网络，每个VPC都有一个独立的隧道号，一个隧道号对应着一个虚拟化网络。一个VPC内的虚拟机之间的报文对应有相同的隧道标识，然后送到物理网络上进行传输。不同VPC内的虚拟机因为所在的隧道标识不同，本身处于两个不同的路由平面，所以不同VPC内的虚拟机无法进行通信，天然地实现了逻辑隔离。创建VPC需要指定区域region，在一个region内可部署多个可用区，VPC内的资源可以分布在不同的可用区中，本实施例中，扩展可用区可作为用户VPC中的其中一个可用区，VPC内的资源可以部署在扩展可用区中。
- [0050] 值得说明的是，本实施例中可为公共云创建多个扩展可用区，多个扩展可用区可分布在多个用户机房中。对于单个用户来说，分布在其机房中的扩展可用区可以是一个或多个。实际应用中，分布在其起机房中的扩展可用区可由该用户专用，以保证用户数据的安全，而且，正如前文提及的，可将用户机房中的扩

展可用区作为该用户在公共云上申请的VPC中的一个可用区。当然，本实施例对此不作现在，在其它需求下，扩展可用区也可不专属于某一个用户。

[0051] 为了便于描述，后文中将从单个扩展可用区的角度来说明公共云的安全扩展方案，但应当理解的是，其它扩展可用区可采用相同的方案来保证公共云的安全扩展。

[0052] 另外，本实施例中，公共云可将扩展可用区作为一种全托管、可部署的产品来进行管理，例如，可通过一组机柜来承载扩展可用区中的物理设备，这些物理设备可包括用于提供计算、存储、网络等服务的基础设备，用户机房只需要提供适合扩展可用区安装的机房环境即可。本实施例中，可采用集群等方式来组织扩展可用区中的物理设备，例如，可将扩展可用区中提供计算服务的物理设备组织为计算集群，将提供存储服务的物理设备组织为存储集群等，本实施例对扩展可用区中物理设备的组织形式、结构等均不作限定。这对用户来说，只需采用按需租用的方式即可在本地机房中铺设扩展可用区，而无需自己花费重金购买相关物理设备。而对于公共云来说，则可减少公共云机房的成本且可通过扩展可用区更加灵活地适配用户的地区region需求。

[0053] 但是，由于扩展可用区位于用户机房内，对于公共云来说，扩展可用区存在被用户篡改、破解、攻击等风险，而扩展可用区可能被作为对公共云进行恶意攻击的跳板。因此，本实施例在上述公共云扩展架构的基础上，提出了安全防护机制，来实现对公共云管控的保护，防止来自用户机房的恶意攻击。

[0054] 参考图1和2，本实施例可在公共云中部署安全网关，对于安全网关来说，本实施例提供的公共云的扩展方法，可包括：

[0055] 步骤100、接收扩展可用区中的物理设备发起的认证请求，认证请求中包含物理设备的身份信息；

[0056] 步骤101、在物理设备的身份信息认证成功的情况下，建立安全网关与物理设备之间的安全隧道；

[0057] 步骤102、基于安全隧道，将扩展可用区纳管至公共云中。

[0058] 值得说明的是，本实施例中，单个扩展可用区中可包含多台物理设备，为便于描述，本实施例中将从单台物理设备的角度来进行安全防护机制的说明，应当

理解的是，本实施例提供的安全防护机制可应用至扩展可用区中的其它物理设备。

- [0059] 本实施例中，在公共云上，可为不同的用户机房部署专属的安全网关，用户机房专属的安全网关可部署在与用户机房相同的地区region中，例如，当用户机房位于北京，该用户机房专属的安全网关也可部署在杭州。实际应用中，公共云提供方可通过VPC的方式来为安全防护机制划分地区，公共云提供方可在所需的地区中为安全防护工作创建VPC，这样，同地区的不同用户机房各自所专属的安全网关可分布在同一VPC中，而不同地区的用户机房所专属的安全网关将分布在不同的VPC中。例如，公共云提供方可在北京部署一VPC，该VPC中可分布有多个安全网关，单个安全网关可用于纳管位于北京的某个用户机房。又例如，某个用户位于北京的机房对应的安全网关将分布在公共云提供方在北京部署的VPC中，而该用户在上海的机房对应的安全网关则将分布在公共云提供方在上海部署的VPC中。这可有效提高安全网关的响应效率。另外，在公共云上，可为同一用户机房分配至少两个专属的安全网关，以保证用户机房拥有备用的安全网关来应对可能发生的安全网关故障。
- [0060] 本实施例中，安全网关可以是为了扩展安全性而在公共云上额外部署的边界网关，以在传统可用区接入方案的基础上增加安全防护机制，传统可用区位于公共云提供方自己的机房中，因此公共云默认传统可用区可受信的，而不需要对传统可用区应用本实施例的安全防护机制，应当理解的是，公共云为传统可用区的接入而部署的路由器、交换机等网络设备同样适用于扩展可用区，本实施例中，在这些已有网络设备的基础上还增设了安全网关。例如，用户机房可通过物理专线接入公共云的交换机设备中，以建立用户机房与公共云之间的物理连接通道。
- [0061] 本实施例中，可在扩展可用区中的物理设备上安装网关代理程序，以使物理设备能够按照图2中的相关逻辑来配合安全网关实现安全防护机制。本实施例中，可在扩展可用区的生产阶段，将网关代理程序集成到物理设备的内存操作系统RAMOS中，RAMOS是可用于安装操作系统的系统，通过将网关代理程序集成在RAMOS中，可保证网关代理设备可在物理设备进行装机之前即启动，从而保证

装机过程能够位于安全防护范围内，避免装机过程中发生对物理设备的操作系统的篡改等风险问题。在装机过程中，网关代理程序将被安装到物理设备的操作系统中，这样，在物理设备的运行阶段，网关代理程序可随物理设备的操作系统启动运行，并在物理设备所提供服务的运行期间与公用云上的安全网关配合来实施安全防护机制。本实施例中，可基于网关代理设备将安全防护机制部署至扩展可用区建设的每个阶段，使安全防护流程和部署运维流程保持一致，从而从根源处消除扩展可用区可能带来的安全隐患。

[0062] 参考图2，在步骤100中，物理设备可向安全网关发起认证请求，认证请求可包含物理设备的身份信息。其中，身份信息中可包括但不限于产品序列号SN、信道地址OoB MAC、IP地址、证书请求CSR以及根据时间戳对已有身份信息进行哈希计算而生成的身份验证码等。安全网关可基于物理设备的身份信息，对物理设备进行身份认证，本实施例对身份认证的方式不做限定，物理设备的身份信息符合预置的身份认证要求即可。后续实施例中将提供示例性的身份认证方案。

[0063] 本实施例中，将公共云作为受信环境，而将位于用户机房内的扩展可用区作为非受信环境，在受信环境和非受信环境之间部署安全网关，实现非受信环境和受信环境之间的安全互访。也即是，本实施例中，将扩展可用区作为非受信环境，而公共云对从扩展可用区中的一起网络访问的实体和请求均不信任，从非受信环境到公共云的所有网络访问均需要进行认证，对公共云的数据进行严格校验。

[0064] 在步骤101中，若物理设备的身份信息认证成功，则可建立安全网关与物理设备之间的安全隧道。可选地，这里的安全隧道可采用VPN隧道。VPN隧道两端的通信方需要遵循VPN协议进行流量交互，VPN隧道中的流量传输都是加密的，因此，建立起VPN隧道后，可保证数据在该隧道中传输过程的安全性。

[0065] 在步骤102中，可基于安全隧道，将扩展可用区纳管至公共云中。这里，纳管的含义是将安全隧道作为管控链路，公共云可远程管控位于用户机房内的扩展可用区，以保证扩展可用区位于公共云的安全保护范围内。

- [0066] 据此，本实施例中，可为公共云创建扩展可用区，扩展可用区部署在用户机房中，这样，公共云的硬件设施以软硬一体化方式部署到用户机房，可满足用户的数据安全、数据本地处理、低延时等需求；而通过将扩展可用区纳管至公共云上，使得用户在本地即可拥有与公共云一致的使用体验，且扩展了公共云的边界；将扩展可用区作为不受信环境，通过部署在公共云中的安全网关对扩展可用区中的物理设备进行身份认证，建立起扩展可用区中物理设备与安全网关之间的安全隧道，基于安全网关对扩展可用区与公共云之间的进出流量进行严格校验，从而可保证公共云扩展过程中的安全性。
- [0067] 在上述或下述实施例中，安全网关可采用多种实现方式对物理设备进行身份认证。
- [0068] 在一种可选的实现方式中，安全网关可响应于物理设备发起的认证请求，与物理设备进行握手，若在握手过程中确定物理设备为预先注册在公共云中的设备，则确定物理设备的身份信息认证成功，并建立安全网关与物理设备之间的安全隧道。其中，在该实现方式中，可为公共云维护一CMDB数据库，该数据库中可记录隶属于公共云的所有设备的信息，包含在该数据库中的设备即为预先注册在公共云中的设备，该数据库可由公共云提供方来维护，由公共云提供方来认定所有隶属于公共云的设备。这样，在用户机房中铺设扩展可用区后，可将扩展可用区中的物理设备注册至公共云中，也即是添加到该数据库中。另外，该数据库中记录的设备的设备信息可包括但不限于产品序列号SN、产品内存、厂商等信息，以描述设备各方面的属性。
- [0069] 为了更加客观地对物理设备进行身份认证，图3为本申请一示例性实施例提供的一种示例性的握手方案的逻辑示意图。参考图3，一种示例性的握手方案可以是：
- [0070] 根据物理设备的身份信息中包含的已有身份参数，计算身份验证码；
- [0071] 若计算得到的身份验证码与物理设备的身份信息中携带的身份验证码一致，则检测物理设备是否为预先注册在公共云中的设备；
- [0072] 若是，则向物理设备提供身份证书；
- [0073] 接收物理设备基于身份证书发起的安全隧道连接请求；

- [0074] 在物理设备的身份证书验证成功的情况下，建立安全网关与物理设备之间的安全隧道。
- [0075] 其中，正如前文提及的，物理设备发出的认证请求中包含的身份信息中携带有身份验证码，安全网关可采用与物理设备同样的计算方式，来为物理设备计算身份验证码，安全网关可将自身计算出的身份验证码与认证请求中携带的身份验证码进行比对，如果一致，则可确定认证请求确实是物理设备自身发出的，且并未被篡改，这样，可通过物理设备的SN、OOBMAC等信息以及身份验证码来双重验证物理设备的合法性。在确定物理设备具备合法性的基础上，可进一步检测物理设备是否为预先注册在公共云中的设备，参考图3，安全网关可基于物理设备的SN等信息来查询公共云的CMDB数据库，如果在该数据库中查询到物理设备，则可确定物理设备为预先注册在公共云中的设备。
- [0076] 本实施例中，可提供面向安全网关和扩展可用区中的物理设备的证书服务，安全网关可在确定物理设备为预先注册在公共云中的设备后，向证书服务申请属于物理设备的身份证书，并返回给物理设备。物理设备在收到身份证书后，可基于身份证书向安全网关发起安全隧道连接请求，安全网关可对物理设备的身份证书进行验证，确定安全隧道连接请求确系物理设备自身发起的，从而可建立起安全网关与物理设备之间的安全隧道，至此完成握手过程。其中，双方之间的安全隧道的建立过程可基于相互传输层(mTLS)加密技术。
- [0077] 图4为本申请一示例性实施例提供的一种公共云扩展方案的逻辑示意图。在图4中，示出了安全网关的一种示例性结构。
- [0078] 参考图4，在逻辑上，安全网关可包含控制面、数据面和安全防护部分。其中，控制面可用于向数据面下发配置指令、采集数据面的日志、心跳信息等。数据面则用于承担数据传输层面的工作，例如，转发、对流量报文进行加解密等工作。安全防护部分则用于提供安全网关的四层/七层防护能力，安全防护部分可采用网站应用级入侵防御WAF技术。基于安全防护部分，本实施例中的安全网关可具备：
- [0079] 1) 四层防护能力：

- [0080] 提供TCP/UDP两种协议的源目的端口、源目的IP的四层ACL防护能力；源目的应用分组的四层ACL防护能力；
- [0081] 提供针对地址组或者应用分组(及时更新分组IP)的四层ACL防护能力；
- [0082] 记录访问请求日志及阻断日志记录；
- [0083] 2)七层防护能力：
- [0084] 支持http和https的基础Web防护，包括对SQL注入、XSS跨站、WebShell上传、命令注入等攻击的防护能力；
- [0085] 支持http和https的自定义防护规则配置，包括针对URL、Query Arg、User-Agent等字段的自定义ACL规则。
- [0086] 可选地，本实施例中，从宏观的角度来看，可将公共云上所有安全网关的控制面进行中心化，也即是，所有的安全网关可共用一控制面，而将安全网关的数据面按照地区进行分布式部署。当然，这仅是示例性的，本实施例并不限于此。
- [0087] 图4中，还示出了物理设备上安装的网关代理程序的一种示例性逻辑结构。参考图4，物理设备上的网关代理程序在逻辑上可包含控制面代理程序和数据面代理程序，基于控制面代理程序，可控制物理设备执行采集自身的身份信息、向安全网关的控制面发送认证请求等操作，数据面代理程序则可控制物理设备执行向安全网关的控制面发起对公共云的访问流量、将访问流量引流至安全隧道、对访问流量进行加密封装等操作。
- [0088] 基于安全网关和物理设备上的网关代理程序的上述示例性结构，参考图3，一种示例性的握手方案可具体为：
- [0089] 1、物理设备的网关代理程序启动后，网关代理程序中的控制面代理程序(后续称为AuthAgent)可采集物理设备的SN、OOB mac地址、IP地址信息等，生成证书请求CSR，根据本地时间戳及Hash算法生成TOTP验证码作为物理设备的身份验证码。通过HTTPS的方式将这些信息携带在认证请求中，发送给安全网关的控制面。
- [0090] 2、安全网关的控制面可核验认证请求中的TOTP验证码，在核验通过的情况下，可使用SN等信息查询公共云的CMDB数据库中的设备信息，如果确定物理

设备为预先注册在CMDB中的设备，则可向证书服务发起针对物理设备的签发证书请求CSR，并将签发后的身份证书返回给物理设备的网关代理程序中的AuthAgent。

- [0091] 3、AuthAgent在收到身份证书后，可将身份证书配置给物理设备中网关代理程序中的数据面代理程序(后续称为ClientAgent)，并启动ClientAgent；ClientAgent可向安全网关的数据面发起安全隧道连接请求，以进行mTLS协商，并与安全网关的数据面交换身份证书；双方可进行身份证书的互验，其中，双方各自拥有从证书服务中获得的对方的根证书，因此具备证书互验的依据；在双方证书互验成功的情况下，双方可成功建立起安全隧道。
- [0092] 当然，上述的握手方案进行示例性的，本实施例并不限于此。
- [0093] 在完成握手过程后，扩展可用区中的物理设备与其在公共云上专属的安全网关之间建立起了安全隧道，双方的交互流量均将被引流至该安全隧道中，从而可通过公共云上的安全网关对所有的输入流量进行严格认证，保证输入流量的可信性。
- [0094] 另外，安全网关中还可预置扩展可用区中物理设备对应的访问控制规则，该访问控制规则中包含允许物理设备访问的公共云上的服务端的白名单，这里的服务端可以是公共云上的服务、设备或集群等各种层面的可访问对象，服务端可包括但不限于装机服务端、DNS服务端、云产品管控端或应用程序代理端等。其中，装机服务端可提供装机服务，扩展可用区中的物理设备可通过访问装机服务端来拉取装机所需的数据。DNS服务端可提供DNS服务，扩展可用区中的物理设备在发生域名解析需求时，可访问DNS服务端来使用DNS服务。云产品管控端，用于提供云产品管控服务，扩展可用区中的物理设备可向云产品管控端发起控制指令，以实现公共云上部分服务的管控，从这里可以清楚的感知到，扩展可用区中的物理设备是具有对公共云上部分服务的管控权限的，一旦扩展可用区失守，将对公共云造成巨大的安全漏洞，这也正是本实施例提出对扩展可用区应用安全防护机制的初衷。应用程序代理端，可用于提供应用程序安装服务，扩展可用区中的物理设备可从应用程序代理端中拉取数据以在物理设备

中安装相关应用程序。应当理解的是，这里提供的公共云上的服务端进行示例性的几种，本实施例中并不限于此。

- [0095] 基于此，安全网关可基于安全网关中存储的访问控制规则，对物理设备针对公共云发起的流量进行访问控制。实际应用中，安全网关可默认拒绝所有来自非受信环境(扩展可用区)的输入流量，并按需更新访问控制规则中的白名单，这样，一方面通过扩展可用区中物理设备上安装的网关代理程序将物理设备向公共云发起的流量引流至安全隧道；另一方面，通过在安全网关中预置访问控制规则，可保证来自扩展可用区的输入流量中只有符合访问控制规则的输入流量才会被放通。本实施例中，安全网关对扩展可用区最小化暴露公共云中云产品管控服务端这种涉及到管控平面的接口，从而尽可能降低这类结构收到外部攻击的可能性。
- [0096] 在上述或下述实施例中，安全网关可借助路由发布、路由拦截等机制，来实现对扩展可用区和对公共云的双向透明。
- [0097] 图5为本申请一示例性实施例提供的一种双向透明方案的逻辑示意图。参考图5，安全网关可获取物理设备发布的路由信息；将物理设备发布的路由信息公告至公共云上的服务端；将服务端发布的路由信息公告至物理设备；其中，物理设备和服务端发布的路由信息示意的传输路径均途经安全网关。
- [0098] 参考图5，其中示出了从扩展可用区中的物理设备中的应用程序app向公共云上的服务端发送的输入流量的路径(图中两条虚线路径中位于上方的路径)和从公共云的服务端返回物理设备中应用程序app的输出流量的路径(图中两条虚线路径中位于下方的路径)。基于此，扩展可用区中的物理设备可往安全网关发布用户机房的地址路由，安全网关学习后可通过专线发布给公共云上的云产品管控、DNS等服务端。相应地，公共云上的服务端可通过安全网关将服务端的路由信息发布至扩展可用区中的物理设备(具体可至物理设备中的app)。基于此，物理设备可按所需的服务端的地址向公共云发起输入流量，物理设备中的网关代理程序可通过Tproxy代理(通过IPtables拦截/转发等方式)来将输入流量引流至安全隧道，并在扩展可用区中的路由等网络设备的支持下可按照服务端发布的路由信息，使输入流量的传输路径途径安全网关，这样安全网关可按前文中提

及的访问控制规则来对输入流量进行访问控制，以保证输入流量的可信性。同样，公共云向扩展可用区中的物理设备返回的输出流量，也会被引流至安全隧道，并通过安全网关进行加密、封装等处理后，到达物理设备，这保证了输出流量的安全性。整个过程中，无论是物理设备还是服务端，均对安全网关无感知，安全网关对扩展可用区和对公共云是双向透明的。

[0099] 据此，本实施例中，安全网关对扩展可用区和对公共云双向透明，可实现扩展可用区的零成本接入，无需进行地址规划和网络变更，扩展可用区可无缝接入公共云。来自扩展可用区的输入流量，都将经过安全网关的认证、授权、加密，从而确保访问链路的安全性和完整性。

[0100] 图6为本申请一示例性实施例提供的另一种公共云的扩展方法的流程示意图。图6中所示的公共云的扩展方法可适用于扩展可用区中的物理设备。参考图6，该方法可包括：

[0101] 步骤600、基于物理设备中装配的网关代理程序，向公共云上配置的安全网关发起认证请求，认证请求中包含物理设备的身份信息；

[0102] 步骤601、在身份信息认证成功的情况下，建立安全网关与物理设备之间的安全隧道；

[0103] 步骤602、基于网关代理程序，将物理设备中发起的针对公共云的流量引流至安全隧道，以通过安全隧道将扩展可用区纳管至公共云中。

[0104] 在一可选实施例中，网关代理程序集成在物理设备的内存操作系统RAMOS中，该方法，还包括：

[0105] 在物理设备进行装机之前，启动网关代理程序；

[0106] 在建立安全网关与物理设备之间的安全隧道之后，通过安全隧道向公共云中的装机服务端发起装机请求，以从装机服务端中获取装机数据。

[0107] 在前述从安全网关侧描述的公共云的扩展方案相关的实施例中，也涉及到了物理设备侧的技术逻辑，为了节省篇幅，关于物理设备侧在公共云扩展方案中涉及到的技术细节可参考前述实施例中的相关描述，在此不再重复赘述，但这不应造成对本申请保护范围的损失。

- [0108] 需要说明的是，在上述实施例及附图中的描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的序号如101、102等，仅仅是用于区分开各个不同的操作，序号本身不代表任何的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。
- [0109] 图7为本申请另一示例性实施例提供的一种网关设备的结构示意图。如图7所示，该网关设备，部署于公共云中，公共云创建有扩展可用区，扩展可用区铺设于用户机房中，该网关设备包括存储器70、处理器71和通信组件72；
- [0110] 存储器70用于存储一条或多条计算机指令；
- [0111] 处理器71与存储器70和通信组件72耦合，用于执行一条或多条计算机指令，以用于：
- [0112] 通过通信组件72接收扩展可用区中的物理设备发起的认证请求，认证请求中包含物理设备的身份信息；
- [0113] 在物理设备的身份信息认证成功的情况下，建立安全网关与物理设备之间的安全隧道；
- [0114] 基于安全隧道，将扩展可用区纳管至公共云中。
- [0115] 在一可选实施例中，处理器72在物理设备的身份信息认证成功的情况下，建立安全网关与物理设备之间的安全隧道的过程中，可用于：
- [0116] 响应于认证请求，与物理设备进行握手；
- [0117] 若在握手过程中确定物理设备为预先注册在公共云中的设备，则建立安全网关与物理设备之间的安全隧道。
- [0118] 在一可选实施例中，处理器72在握手过程中，可用于：
- [0119] 根据物理设备的身份信息中包含的身份参数，计算身份验证码；
- [0120] 若计算得到的身份验证码与物理设备的身份信息中携带的身份验证码一致，则检测物理设备是否为预先注册在公共云中的设备；
- [0121] 若是，则向物理设备提供身份证书；
- [0122] 接收物理设备基于身份证书发起的安全隧道连接请求；

- [0123] 在物理设备的身份证书验证成功的情况下，建立安全网关与物理设备之间的安全隧道。
- [0124] 在一可选实施例中，身份信息中包括产品序列号SN、信道地址OoB MAC、IP地址、证书请求CSR和根据时间戳对身份信息中的已有身份参数进行哈希计算而生成的身份验证码中的一种或多种。
- [0125] 在一可选实施例中，处理器72在将扩展可用区纳管至公共云中，之后还可用于：
- [0126] 基于安全网关中存储的访问控制规则，对物理设备针对公共云发起的流量进行访问控制；
- [0127] 访问控制规则中包含允许物理设备访问的公共云上的服务端的白名单。
- [0128] 在一可选实施例中，处理器72还可用于：
- [0129] 获取物理设备发布的路由信息；
- [0130] 将物理设备发布的路由信息公告至公共云上的服务端；
- [0131] 将服务端发布的路由信息公告至物理设备；
- [0132] 其中，物理设备和服务端发布的路由信息示意的传输路径均途经安全网关。
- [0133] 在一可选实施例中，服务端包括装机服务端、DNS服务端、云产品管控端和应用程序代理端中的一种或多种。
- [0134] 进一步，如图7所示，该通信设备还包括：电源组件73等其它组件。图7中仅示意性给出部分组件，并不意味着网关设备只包括图7所示组件。
- [0135] 值得说明的是，上述关于网关设备各实施例中的技术细节，可参考前述的方法实施例中关于安全网关的相关描述，为节省篇幅，在此不再赘述，但这不应造成本申请保护范围的损失。
- [0136] 图8为本申请又一示例性实施例提供的一种物理设备的结构示意图。参考图8，公共云创建有扩展可用区，扩展可用区铺设于用户机房中，该物理设备位于扩展可用区中，物理设备可包括存储器80、处理器81和通信组件82；
- [0137] 存储器80用于存储一条或多条用于网关代理的计算机指令；
- [0138] 处理器81与存储器80和通信组件82耦合，用于执行一条或多条计算机指令，以用于：

- [0139] 基于物理设备中装配的网关代理程序，向公共云上配置的安全网关发起认证请求，认证请求中包含物理设备的身份信息；
- [0140] 在身份信息认证成功的情况下，建立安全网关与物理设备之间的安全隧道；
- [0141] 基于网关代理程序，将物理设备中发起的针对公共云的流量引流至安全隧道，以通过安全隧道将扩展可用区纳管至公共云中。
- [0142] 在一可选实施例中，网关代理程序集成在物理设备的内存操作系统RAMOS中，处理器72还可用于：
- [0143] 在物理设备进行装机之前，启动网关代理程序；
- [0144] 在建立安全网关与物理设备之间的安全隧道之后，通过安全隧道向公共云中的装机服务端发起装机请求，以从装机服务端中获取装机数据。
- [0145] 进一步，如图8所示，该通信设备还包括：电源组件83等其它组件。图8中仅示意性给出部分组件，并不意味着物理设备只包括图8所示组件。
- [0146] 值得说明的是，上述关于物理设备各实施例中的技术细节，可参考前述的方法实施例中关于物理设备的相关描述，为节省篇幅，在此不再赘述，但这不应造成本申请保护范围的损失。
- [0147] 相应地，本申请实施例还提供一种存储有计算机程序的计算机可读存储介质，计算机程序被执行时能够实现上述方法实施例中可由网关设备或物理设备执行的各步骤。
- [0148] 上述图5中的存储器，用于存储计算机程序，并可被配置为存储其它各种数据以支持在计算平台上的操作。这些数据的示例包括用于在计算平台上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器 (SRAM)，电可擦除可编程只读存储器 (EEPROM)，可擦除可编程只读存储器 (EPROM)，可编程只读存储器 (PROM)，只读存储器 (ROM)，磁存储器，快闪存储器，磁盘或光盘。
- [0149] 上述图5中的通信组件，被配置为便于通信组件所在设备和其他设备之间有线或无线方式的通信。通信组件所在设备可以接入基于通信标准的无线网络，如WiFi，2G、3G、4G/LTE、5G等移动通信网络，或它们的组合。在一个示例性实

施例中，通信组件经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件还包括近场通信(NFC)模块，以促进短程通信。例如，在NFC模块可基于射频识别(RFID)技术，红外数据协会(IrDA)技术，超宽带(UWB)技术，蓝牙(BT)技术和其他技术来实现。

- [0150] 上述图5中的电源组件，为电源组件所在设备的各种组件提供电力。电源组件可以包括电源管理系统，一个或多个电源，及其他与为电源组件所在设备生成、管理和分配电力相关联的组件。
- [0151] 图9为本申请又一示例性实施例提供的一种公共云的扩展系统的结构示意图。参考图9，该系统可包括安全网关90和为公有云创建的扩展可用区91，安全网关90部署于公共云中，扩展可用区91铺设于用户机房中；
- [0152] 扩展可用区91中的物理设备92，用于基于物理设备92中装配的网关代理程序，向公共云上配置的安全网关90发起认证请求，认证请求中包含物理设备92的身份信息；
- [0153] 安全网关90用于接收认证请求；在物理设备92的身份信息认证成功的情况下，建立安全网关90与物理设备92之间的安全隧道；基于安全隧道，将扩展可用区91纳管至公共云中。
- [0154] 在一可选实施例中，扩展可用区91中的物理设备92，还可用于：
- [0155] 在身份信息认证成功的情况下，建立安全网关90与物理设备92之间的安全隧道；
- [0156] 基于网关代理程序，将物理设备92中发起的针对公共云的流量引流至安全隧道，以通过安全隧道将扩展可用区91纳管至公共云中。
- [0157] 在一可选实施例中，网关代理程序集成在物理设备92的内存操作系统RAMOS中，物理设备92还可用于：
- [0158] 在物理设备92进行装机之前，启动网关代理程序；
- [0159] 在建立安全网关90与物理设备92之间的安全隧道之后，通过安全隧道向公共云中的装机服务端发起装机请求，以从装机服务端中获取装机数据。
- [0160] 在一可选实施例中，安全网关90在物理设备92的身份信息认证成功的情况下，建立安全网关90与物理设备92之间的安全隧道的过程中，可用于：

- [0161] 响应于认证请求，与物理设备92进行握手；
- [0162] 若在握手过程中确定物理设备92为预先注册在公共云中的设备，则建立安全网关90与物理设备92之间的安全隧道。
- [0163] 在一可选实施例中，安全网关90在握手过程中，可用于：
- [0164] 根据物理设备92的身份信息中包含的身份参数，计算身份验证码；
- [0165] 若计算得到的身份验证码与物理设备92的身份信息中携带的身份验证码一致，则检测物理设备92是否为预先注册在公共云中的设备；
- [0166] 若是，则向物理设备92提供身份证书；
- [0167] 接收物理设备92基于身份证书发起的安全隧道连接请求；
- [0168] 在物理设备92的身份证书验证成功的情况下，建立安全网关90与物理设备92之间的安全隧道。
- [0169] 在一可选实施例中，身份信息中包括产品序列号SN、信道地址OOB MAC、IP地址、证书请求CSR和根据时间戳对身份信息中的已有身份参数进行哈希计算而生成的身份验证码中的一种或多种。
- [0170] 在一可选实施例中，安全网关90在将扩展可用区91纳管至公共云中，之后还可用于：
- [0171] 基于安全网关90中存储的访问控制规则，对物理设备92针对公共云发起的流量进行访问控制；
- [0172] 访问控制规则中包含允许物理设备92访问的公共云上的服务端的白名单。
- [0173] 在一可选实施例中，安全网关90还可用于：
- [0174] 获取物理设备92发布的路由信息；
- [0175] 将物理设备92发布的路由信息公告至公共云上的服务端；
- [0176] 将服务端发布的路由信息公告至物理设备92；
- [0177] 其中，物理设备92和服务端发布的路由信息示意的传输路径均途经安全网关90。
- [0178] 在一可选实施例中，服务端包括装机服务端、DNS服务端、云产品管控端和应用程序代理端中的一种或多种。

- [0179] 值得说明的是，上述关于公共云的扩展系统各实施例中的技术细节，可参考前述的方法实施例中关于物理设备和安全网关的相关描述，为节省篇幅，在此不再赘述，但这不应造成本申请保护范围的损失。
- [0180] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。
- [0181] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。
- [0182] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。
- [0183] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。
- [0184] 在一个典型的配置中，通信设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。
- [0185] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

- [0186] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带式磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被通信设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。
- [0187] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。
- [0188] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

- [权利要求 1] 一种公共云的扩展方法，为公共云创建扩展可用区，所述扩展可用区铺设于用户机房中，所述公共云上配置有安全网关，所述方法适用于所述安全网关，包括：
- 接收所述扩展可用区中的物理设备发起的认证请求，所述认证请求中包含所述物理设备的身份信息；
- 在所述物理设备的身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；
- 基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。
- [权利要求 2] 根据权利要求1所述的方法，所述在所述物理设备的身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道，包括：
- 响应于所述认证请求，与所述物理设备进行握手；
- 若在握手过程中确定所述物理设备为预先注册在所述公共云中的设备，则建立所述安全网关与所述物理设备之间的安全隧道。
- [权利要求 3] 根据权利要求2所述的方法，所述握手过程包括：
- 根据所述物理设备的身份信息中包含的身份参数，计算身份验证码；
- 若计算得到的身份验证码与所述物理设备的身份信息中携带的身份验证码一致，则检测所述物理设备是否为预先注册在所述公共云中的设备；
- 若是，则向所述物理设备提供身份证书；
- 接收所述物理设备基于所述身份证书发起的安全隧道连接请求；
- 在所述物理设备的身份证书验证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道。
- [权利要求 4] 根据权利要求1所述的方法，所述身份信息中包括产品序列号SN、信道地址OOB MAC、IP地址、证书请求CSR和根据时间戳对身份信息

中的已有身份参数进行哈希计算而生成的身份验证码中的一种或多种。

[权利要求 5] 根据权利要求1所述的方法，在将所述扩展可用区纳管至所述公共云中，之后还包括：

基于所述安全网关中存储的访问控制规则，对所述物理设备针对所述公共云发起的流量进行访问控制；

所述访问控制规则中包含允许所述物理设备访问的公共云上的服务端的白名单。

[权利要求 6] 根据权利要求1所述的方法，还包括：

获取所述物理设备发布的路由信息；

将所述物理设备发布的路由信息公告至所述公共云上的服务端；

将所述服务端发布的路由信息公告至所述物理设备；

其中，所述物理设备和所述服务端发布的路由信息示意的传输路径均途经所述安全网关。

[权利要求 7] 根据权利要求6所述的方法，所述服务端包括装机服务端、DNS服务端、云产品管控端和应用程序代理端中的一种或多种。

[权利要求 8] 一种公共云的扩展方法，为公共云创建扩展可用区，所述扩展可用区铺设于用户机房中，所述公共云上配置有安全网关，所述方法适用于所述扩展可用区中的物理设备，包括：

基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；

在身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；

基于所述网关代理程序，将所述物理设备中发起的针对所述公共云的流量引流至所述安全隧道，以通过所述安全隧道将所述扩展可用区纳管至所述公共云中。

- [权利要求 9] 根据权利要求8所述的方法，所述网关代理程序集成在所述物理设备的内存操作系统RAMOS中，所述方法，还包括：
在所述物理设备进行装机之前，启动所述网关代理程序；
在建立所述安全网关与所述物理设备之间的安全隧道之后，通过所述安全隧道向所述公共云中的装机服务端发起装机请求，以从所述装机服务端中获取装机数据。
- [权利要求 10] 一种网关设备，部署于公共云中，所述公共云创建有扩展可用区，所述扩展可用区铺设于用户机房中，所述网关设备包括存储器、处理器和通信组件；
所述存储器用于存储一条或多条计算机指令；
所述处理器与所述存储器和所述通信组件耦合，用于执行所述一条或多条计算机指令，以用于：
通过所述通信组件接收所述扩展可用区中的物理设备发起的认证请求，所述认证请求中包含所述物理设备的身份信息；
在所述物理设备的身份信息认证成功的情况下，建立所述网关设备与所述物理设备之间的安全隧道；
基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。
- [权利要求 11] 一种物理设备，公共云创建有扩展可用区，所述扩展可用区铺设于用户机房中，所述物理设备位于所述扩展可用区中，所述物理设备包括存储器、处理器和通信组件；
所述存储器用于存储一条或多条用于网关代理的计算机指令；
所述处理器与所述存储器和所述通信组件耦合，用于执行所述一条或多条计算机指令，以用于：
基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；
在身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；

基于所述网关代理程序，将所述物理设备中发起的针对所述公共云的流量引流至所述安全隧道，以通过所述安全隧道将所述扩展可用区纳管至所述公共云中。

[权利要求 12] 一种公共云的扩展系统，包含安全网关和为公有云创建的扩展可用区，所述安全网关部署于公共云中，所述扩展可用区铺设于用户机房中；

所述扩展可用区中的物理设备，用于基于所述物理设备中装配的网关代理程序，向所述公共云上配置的安全网关发起认证请求，所述认证请求中包含所述物理设备的身份信息；

所述安全网关用于接收所述认证请求；在所述物理设备的身份信息认证成功的情况下，建立所述安全网关与所述物理设备之间的安全隧道；基于所述安全隧道，将所述扩展可用区纳管至所述公共云中。

[权利要求 13] 一种存储计算机指令的计算机可读存储介质，当所述计算机指令被一个或多个处理器执行时，致使所述一个或多个处理器执行权利要求1-9任一项所述的公共云的扩展方法。