(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109413080 B
(45)授权公告日 2021.05.25

(21)申请号 201811330911.5

(22)申请日 2018.11.09

(65)同一申请的已公布的文献号
申请公布号 CN 109413080 A

(43)申请公布日 2019.03.01

(73)专利权人 厦门市美亚柏科信息股份有限公司
地址 361000 福建省厦门市软件园二期观日路12号102-402单元

(72)发明人 郑政宇 周海涛 齐战胜

(74)专利代理机构 厦门市精诚新创知识产权代理有限公司 35218
代理人 何家富

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 106992988 A,2017.07.28
CN 101997876 A,2011.03.30
CN 102694867 A,2012.09.26
CN 101398771 A,2009.04.01
US 2012060207 A1,2012.03.08
冯黎晓.《云计算环境下基于属性的访问控制方法研究》.《中国优秀硕士学位论文全文数据库 信息科技辑》.2015,

审查员 翟美玲

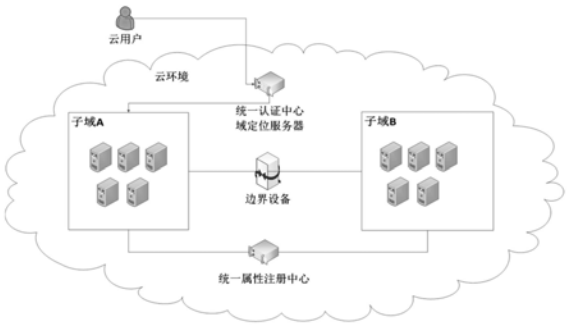
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种跨域动态权限控制方法及系统

(57)摘要

本发明涉及一种跨域动态权限控制方法及系统,在该方法中,包括:在云环境下注册多个子域,每两个子域之间均通过边界设备进行隔离,并且在云环境下部署统一认证中心、域定位服务器和统一属性注册中心,所述统一认证中心和域定位服务器分别用于对用户进行认证和鉴定用户具有权限的子域,用户通过统一认证中心登陆到云环境后,通过域定位服务器分配到所属的子域,所述统一属性注册中心用于对所有子域的属性进行注册和管理。本发明以属性访问控制模型为基础,来对各个子域的属性进行实时注册,实现更高扩展性和安全性的资源访问机制。



CN 109413080 B

1.一种跨域动态权限控制方法,其特征在于,包括:在云环境下注册多个子域,每两个子域之间均通过边界设备进行隔离,并且在云环境下部署统一认证中心、域定位服务器和统一属性注册中心,所述统一认证中心和域定位服务器分别用于对用户进行认证和鉴定用户具有权限的子域,用户通过统一认证中心登陆到云环境后,通过域定位服务器分配到所属的子域,所述统一属性注册中心用于对所有子域的属性进行注册和管理;

跨域的访问控制方法具体包括以下步骤:

S301:A域用户登陆云环境,通过该云环境对应的统一认证服务和域定位服务完成身份认证,并跳转到该用户所属的子域;

S302:发起跨域资源访问请求;

S303:A域的策略实施点拦截该跨域资源访问请求,根据属性访问控制模型对该跨域资源访问请求添加A域的属性后,将该跨域资源访问请求发往A域的策略决策点来判断该用户是否有权限访问B域资源;

S304:A域的策略决策点从A域的策略管理点调取策略规则集;

S305:A域的策略决策点从A域的策略信息点调取策略属性;

S306:A域的策略决策点综合策略规则集和策略属性,对A域的策略实施点的跨域资源访问请求进行鉴权,判断该用户是否有权限访问B域资源,并返回经过鉴权的请求响应至A域的策略实施点;

S307:A域的策略实施点根据请求响应判断该用户是否有权限访问B域资源,如果用户具有访问B域资源的权限,则调取统一属性中心存储的B域对应的属性,添加到跨域资源访问请求中;

S308:将新的跨域资源访问请求发送到B域的策略实施点;

S309:B域的策略实施点将该跨域资源访问请求拦截,并发往B域的策略决策点;

S310:B域的策略决策点从B域的策略管理点调取策略规则集;

S311:B域的策略决策点从B域的策略信息点调取策略属性;

S312:B域的策略决策点综合策略规则集和策略属性,对B域的策略实施点的跨域资源访问请求进行鉴权,判断该用户是否有权限访问B域资源,并返回经过鉴权的请求响应至B域的策略实施点;

S313:B域的策略实施点根据请求响应判断该用户是否有权限访问B域资源,如果用户具有访问B域资源的权限则能够获得资源,如果用户没有权限则返回提示信息。

2.根据权利要求1所述的跨域动态权限控制方法,其特征在于,所述在云环境下注册子域包括以下步骤:

S101:在云环境下创建子域;

S102:构建该子域下的资源管理系统;

S103:基于属性访问控制模型,设定该子域的策略管理点、策略决策点、策略信息点和策略实施点;

S104:设定该子域的属性和策略规则

S105:将该子域的属性和策略规则注册到统一属性注册中心;

S106:统一属性注册中心将该子域的属性和策略规则分发到所述云环境下的所有子域。

3.根据权利要求1所述的跨域动态权限控制方法,其特征在于:还包括域内的访问控制方法,具体包括以下步骤:

S201:A域用户登陆云环境,通过该云环境对应的统一认证服务和域定位服务完成身份认证,并跳转到该用户所属的子域;

S202:发起域内资源访问请求;

S203:A域的策略实施点拦截该请求,根据属性访问控制模型对该请求添加A域的属性后,将该请求发往A域的策略决策点;

S204:A域的策略决策点从A域的策略管理点调取策略规则集;

S205:A域的策略决策点从A域的策略信息点调取策略属性;

S206:A域的策略决策点综合策略规则集和策略属性,对A域的策略实施点的请求进行鉴权,判断该用户是否有权限访问A域资源,并返回经过鉴权的请求响应至A域的策略实施点;

S207:A域的策略实施点根据请求响应判断该用户是否有权限访问A域资源,如果用户具有访问A域资源的权限则能够获得资源,如果用户没有权限则返回提示信息。

4.一种跨域动态权限控制系统,其特征在于:包括位于同一云环境下的多个子域、统一认证中心、域定位服务器和统一属性注册中心,所述系统实现如权利要求1～3中任一所述方法的步骤。

一种跨域动态权限控制方法及系统

技术领域

[0001] 本发明涉及访问权限管理技术领域，尤其涉及一种跨域动态权限控制方法及系统。

背景技术

[0002] 云计算是当前信息技术领域的热点之一，是产业界、学术界、政府等各界均十分关注的焦点。其核心思想是将大量计算资源、存储资源与软件资源链接在一起，形成规模巨大的共享资源池，数据拥有者包括企业、个人或者组织等。云服务商为数据拥有者提供数据托管服务，同样也可为云用户提供各种类型的云资源/服务。传统架构模式下的物理安全边界域消失，而是以逻辑安全域的形式存在，云资源失去了物理边界域的安全控制，存在数据安全性与隐私性的隐患。

[0003] 目前，针对云环境下多安全域的访问控制没有统一的方法，一般上是采用不做控制、边界设备控制、切换子系统、单点登录等方法进行控制。

[0004] (1)、不做控制：同一云环境下采用云认证机制登陆，对认证成功后的用户，云内所有资源对其开放，实际上默认整体云环境为同一个安全域，是最粗犷的控制方法，用于安全要求不高，各个安全域之间差别不大的环境。

[0005] (2)、边界设备控制：在云中利用不同域之间的边界设备，通过预置静态的控制策略，对资源访问进行控制，由于控制策略固定，灵活度不高，可以作为基础的控制策略，主要缺点是细粒度不高，控制能力差，适合简单控制。

[0006] (3)、切换子系统：在不同域中部署不同的服务体系，采用独立的认证模式，云用户通过切换不同的子系统来达到访问不同安全域的资源的目的，但是各子系统相互之间没有联系，只能通过部分开放的接口进行数据层的调用，而且用户在几个系统之间相互切换，操作繁琐，容易失误。

[0007] (4)、单点登录：在不同域中部署不同的服务系统，各系统包含独立的认证模式，并部署单点登录服务，打通各个域的权限体系，即A域服务请求B域时会带有认证信息，表明请求是A域认证通过，并给予简单的用户信息使得B域为此用户鉴权并分配资源，构造单点登录服务实际上依然是两个相互独立的系统，两个系统之间需要用户表相同或相互对应，是基于用户身份的访问控制，灵活度和扩展性不高，相互之间缺乏策略决策等信息的交互。

发明内容

[0008] 针对上述问题，本发明旨在提供一种跨域动态权限控制方法及系统，以属性访问控制模型为基础，来对各个子域的属性进行实时注册，实现更高扩展性和安全性的资源访问机制。

[0009] 具体方案如下：

[0010] 一种跨域动态权限控制方法，包括：在云环境下注册多个子域，每两个子域之间均通过边界设备进行隔离，并且在云环境下部署统一认证中心、域定位服务器和统一属性注

册中心，所述统一认证中心和域定位服务器分别用于对用户进行认证和鉴定用户具有权限的子域，用户通过统一认证中心登陆到云环境后，通过域定位服务器分配到所属的子域，所述统一属性注册中心用于对所有子域的属性进行注册和管理。

[0011] 进一步的，所述在云环境下注册子域包括以下步骤：

[0012] S101：在云环境下创建子域；

[0013] S102：构建该子域下的资源管理系统；

[0014] S103：基于属性访问控制模型，设定该子域的策略管理点、策略决策点、策略信息点和策略实施点；

[0015] S104：设定该子域的属性和策略规则

[0016] S105：将该子域的属性和策略规则注册到统一属性注册中心；

[0017] S106：统一属性注册中心将该子域的属性和策略规则分发到所述云环境下的所有子域。

[0018] 进一步的，还包括域内的访问控制方法，具体包括以下步骤：

[0019] S201：A域用户登陆云环境，通过该云环境对应的统一认证服务和域定位服务完成身份认证，并跳转到该用户所属的子域；

[0020] S202：发起域内资源访问请求；

[0021] S203：A域的策略实施点拦截该请求，根据属性访问控制模型对该请求添加A域的属性后，将该请求发往A域的策略决策点；

[0022] S204：A域的策略决策点从A域的策略管理点调取策略规则集；

[0023] S205：A域的策略决策点从A域的策略信息点调取策略属性；

[0024] S206：A域的策略决策点综合策略规则集和策略属性，对A域的策略实施点的请求进行鉴权，判断该用户是否有权限访问A域资源，并返回经过鉴权的请求响应至A域的策略实施点；

[0025] S207：A域的策略实施点根据请求响应判断该用户是否有权限访问A域资源，如果用户具有访问A域资源的权限则能够获得资源，如果用户没有权限则返回提示信息。

[0026] 进一步的，还包括跨域的访问控制方法，具体包括以下步骤：

[0027] S301：A域用户登陆云环境，通过该云环境对应的统一认证服务和域定位服务完成身份认证，并跳转到该用户所属的子域；

[0028] S302：发起跨域资源访问请求；

[0029] S303：A域的策略实施点拦截该跨域资源访问请求，根据属性访问控制模型对该跨域资源访问请求添加A域的属性后，将该跨域资源访问请求发往A域的策略决策点来判断该用户是否有权限访问B域资源；

[0030] S304：A域的策略决策点从A域的策略管理点调取策略规则集；

[0031] S305：A域的策略决策点从A域的策略信息点调取策略属性；

[0032] S306：A域的策略决策点综合策略规则集和策略属性，对A域的策略实施点的跨域资源访问请求进行鉴权，判断该用户是否有权限访问B域资源，并返回经过鉴权的请求响应至A域的策略实施点；

[0033] S307：A域的策略实施点根据请求响应判断该用户是否有权限访问A域资源，如果用户具有访问B域资源的权限，则调取统一属性中心存储的B域对应的属性，添加到跨域资

源访问请求中；

[0034] S308:将新的跨域资源访问请求发送到B域的策略实施点；

[0035] S309:B域的策略实施点将该跨域资源访问请求拦截，并发往B域的策略决策点；

[0036] S310:B域的策略决策点从B域的策略管理点调取策略规则集；

[0037] S311:B域的策略决策点从B域的策略信息点调取策略属性；

[0038] S312:B域的策略决策点综合策略规则集和策略属性，对B域的策略实施点的跨域资源访问请求进行鉴权，判断该用户是否有权限访问B域资源，并返回经过鉴权的请求响应至B域的策略实施点；

[0039] S313:B域的策略实施点根据请求响应判断该用户是否有权限访问B域资源，如果用户具有访问B域资源的权限则能够获得资源，如果用户没有权限则返回提示信息。

[0040] 一种跨域动态权限控制系统，包括位于同一云环境下的多个子域、统一认证中心、域定位服务器和统一属性注册中心，所述系统实现本发明实施例所述方法的步骤。

[0041] 本发明采用如上技术方案，为云环境下的各子域构建基于属性的访问控制后，对应于各子域之间属性的不同而造成的跨域访问鉴权问题的情况，提出了一种基于属性的访问控制模型的跨域动态权限控制方法及系统，并具有有益效果：

[0042] (1)、建立了统一的属性注册中心，由该中心统一的管理和分发各个子域的属性；

[0043] (2)、以基于属性的访问控制为基础，将其引申到多子域的鉴权中，继承了其策略扩展性高，决策灵活的特点；

[0044] (3)、各子域从统一属性注册中心获取其他子域的属性，并添加到跨域请求中，方便其他子域的鉴权和管理；各个子域拥有自身的策略决策，且不会暴露各个子域自身的鉴权策略，安全性更强，更加可控；

[0045] (4)、属性访问控制的鉴权与登陆统一认证中心不相关，只保留统一认证中的登陆属性作为属性访问控制的外部属性，避免认证过程复杂造成用户体验不好。

附图说明

[0046] 图1所示为本发明实施例的结构示意图。

[0047] 图2所示为该实施例的跨域的访问控制过程的流程图。

[0048] 图3所示为该实施例的注册子域的流程图。

[0049] 图4所示为该实施例的域内的访问控制过程的流程图。

具体实施方式

[0050] 为进一步说明各实施例，本发明提供有附图。这些附图为本发明揭露内容的一部分，其主要用以说明实施例，并可配合说明书的相关描述来解释实施例的运作原理。配合参考这些内容，本领域普通技术人员应能理解其他可能的实施方式以及本发明的优点。

[0051] 以下首先对本发明的相关技术术语进行解释和说明：

[0052] 属性(Attribute，简称attr)：属性是人为定义的事物的特征点，一般包括外在属性、内在属性、行为属性等，例如资源所在服务器的系统环境、网络情况(外在属性)；登录人的认证信息、角色、性别(内在属性)；访问动作(行为属性)；在不同的情况下，这些属性是动态可变的。

[0053] 属性访问控制(Attribute Based Access Control,ABAC)即将访问控制中的主体、客体、权限三大实体用其属性进行统一描述,用实体属性之间的关系对安全需求进行形式化的建模,通过预先定义的属性访问策略实现对客体资源的有效访问。

[0054] 策略管理点(Policy administration point,PAP)策略及策略规则集存储仓库,策略编辑接口。

[0055] 策略决策点(Policy decision point,PDP)策略评估和授权决定组件。ABAC的核心组件。

[0056] 策略信息点(Policy information point,PIP)服务检索与主体,客体,环境相关的属性。

[0057] 策略实施点(Policy enforcement point,PEP)是接受策略管理的网络实体,负责执行由策略决策点分配的决策。

[0058] 现结合附图和具体实施方式对本发明进一步说明。

[0059] 参考图1所示,本发明实施例提供了一种基于属性访问控制模型的跨域动态权限控制方法,包括:在云环境下注册多个子域,每两个子域之间均通过边界设备进行隔离,并且在云环境下部署统一认证中心、域定位服务器和统一属性注册中心,所述统一认证中心和域定位服务器分别用于对用户进行认证和鉴定用户具有权限的子域,用户通过统一认证中心登陆到云环境后,通过域定位服务器分配到所属的子域,所述统一属性注册中心用于对所有子域的属性进行注册和管理。

[0060] 当需要在所述云环境下新建子域时,应由统一属性注册中心对该子域的属性进行注册,以便统一管理,参考图3所示,注册子域包括以下步骤:

[0061] S101:在云环境下创建子域。

[0062] 所述子域的创建方法与现有的常用方法相同。

[0063] S102:构建该子域下的资源管理系统。

[0064] S103:基于属性访问控制模型,设定该子域的策略管理点、策略决策点、策略信息点和实施点等策略相关机构。

[0065] S104:设定该子域的属性和策略规则。

[0066] S105:将该子域的属性和策略规则注册到统一属性注册中心。

[0067] 具体的,可以将属性和策略规则通过接口或者人工的方式注册到统一属性注册中心,由统一属性注册中心进行管理。

[0068] S106:统一属性注册中心将该子域的属性和策略规则分发到所述云环境下的所有子域。

[0069] 参考图4所示,所述云环境下域内的访问控制过程包括以下步骤:

[0070] S201:A域用户登陆云环境,通过该云环境对应的统一认证服务和域定位服务完成身份认证,并跳转到该用户所属的子域,该实施例中为A域。

[0071] S202:发起域内资源访问请求。

[0072] S203:A域的策略实施点(A.PEP)拦截该请求,根据属性访问控制模型对该请求添加A域的属性后,将该请求发往A域的策略决策点(A.PDP)。

[0073] S204:A域的策略决策点(A.PDP)从A域的策略管理点(A.PAP)调取策略规则集。

[0074] S205:A域的策略决策点(A.PDP)从A域的策略信息点(A.PIP)调取策略属性。

[0075] S206:A域的策略决策点(A.PDP)综合策略规则集和策略属性,对A域的策略实施点(A.PEP)的请求进行综合鉴权,判断该用户是否有权限访问A域资源,并返回经过鉴权的请求响应至A域的策略实施点(A.PEP)。

[0076] S207:A域的策略实施点(A.PEP)根据请求响应判断该用户是否有权限访问A域资源,如果用户具有访问A域资源的权限则能够获得资源,如果用户没有权限则返回提示信息。

[0077] 参考图2所示,在所述云环境下跨域的访问控制包括以下步骤:

[0078] S301:A域用户登陆云环境,通过该云环境对应的统一认证服务和域定位服务完成身份认证,并跳转到该用户所属的子域,该实施例中为A域。

[0079] S302:发起跨域资源访问请求。

[0080] S303:A域的策略实施点(A.PEP)拦截该跨域资源访问请求,根据属性访问控制模型对该跨域资源访问请求添加A域的属性后,将该跨域资源访问请求发往A域的策略决策点(A.PDP)来判断该用户是否有权限访问B域资源。

[0081] S304:A域的策略决策点(A.PDP)从A域的策略管理点(A.PAP)调取策略规则集。

[0082] S305:A域的策略决策点(A.PDP)从A域的策略信息点(A.PIP)调取策略属性。

[0083] S306:A域的策略决策点(A.PDP)综合策略规则集和策略属性,对A域的策略实施点(A.PEP)的跨域资源访问请求进行鉴权,判断该用户是否有权限访问B域资源,并返回经过鉴权的请求响应至A域的策略实施点(A.PEP)。

[0084] S307:A域的策略实施点(A.PEP)根据请求响应判断该用户是否有权限访问A域资源,如果用户具有访问B域资源的权限,则调取统一属性中心存储的B域对应的属性,添加到跨域资源访问请求中。

[0085] S308:将新的跨域资源访问请求发送到B域的策略实施点(B.PEP)。

[0086] S309:B域的策略实施点(B.PEP)将该跨域资源访问请求拦截,并发往B域的策略决策点(B.PDP)。

[0087] S310:B域的策略决策点(B.PDP)从B域的策略管理点(B.PAP)调取策略规则集。

[0088] S311:B域的策略决策点(B.PDP)从B域的策略信息点(B.PIP)调取策略属性。

[0089] S312:B域的策略决策点(B.PDP)综合策略规则集和策略属性,对B域的策略实施点(B.PEP)的跨域资源访问请求进行鉴权,判断该用户是否有权限访问B域资源,并返回经过鉴权的请求响应至B域的策略实施点(B.PEP)。

[0090] S313:B域的策略实施点(B.PEP)根据请求响应判断该用户是否有权限访问B域资源,如果用户具有访问B域资源的权限则能够获得资源,如果用户没有权限则返回提示信息。

[0091] 本发明采用如上技术方案,为云环境下的各子域构建基于属性的访问控制后,对应于各子域之间属性的不同而造成的跨域访问鉴权问题的情况,提出了一种基于属性的访问控制模型的跨域动态权限控制方法及系统,并具有有益效果:

[0092] (1)、建立了统一的属性注册中心,由该中心统一的管理和分发各个子域的属性;

[0093] (2)、以基于属性的访问控制为基础,将其引申到多子域的鉴权中,继承了其策略扩展性高,决策灵活的特点;

[0094] (3)、各子域从统一属性注册中心获取其他子域的属性,并添加到跨域请求中,方

便其他子域的鉴权和管理;各个子域拥有自身的策略决策,且不会暴露各个子域自身的鉴权策略,安全性更强,更加可控;

[0095] (4)、属性访问控制的鉴权与登陆统一认证中心不相关,只保留统一认证中的登陆属性作为属性访问控制的外部属性,避免认证过程复杂造成用户体验不好。

[0096] 实施例二

[0097] 参考图1所示,本发明实施例二提供了一种基于属性访问控制模型的跨域动态权限控制系统,该系统主要包括:位于同一云环境下的多个子域、统一认证中心、域定位服务器和统一属性注册中心,所述系统实现实施例一中所述方法的步骤。

[0098] 尽管结合优选实施方案具体展示和介绍了本发明,但所属领域的技术人员应该明白,在不脱离所附权利要求书所限定的本发明的精神和范围内,在形式上和细节上可以对本发明做出各种变化,均为本发明的保护范围。

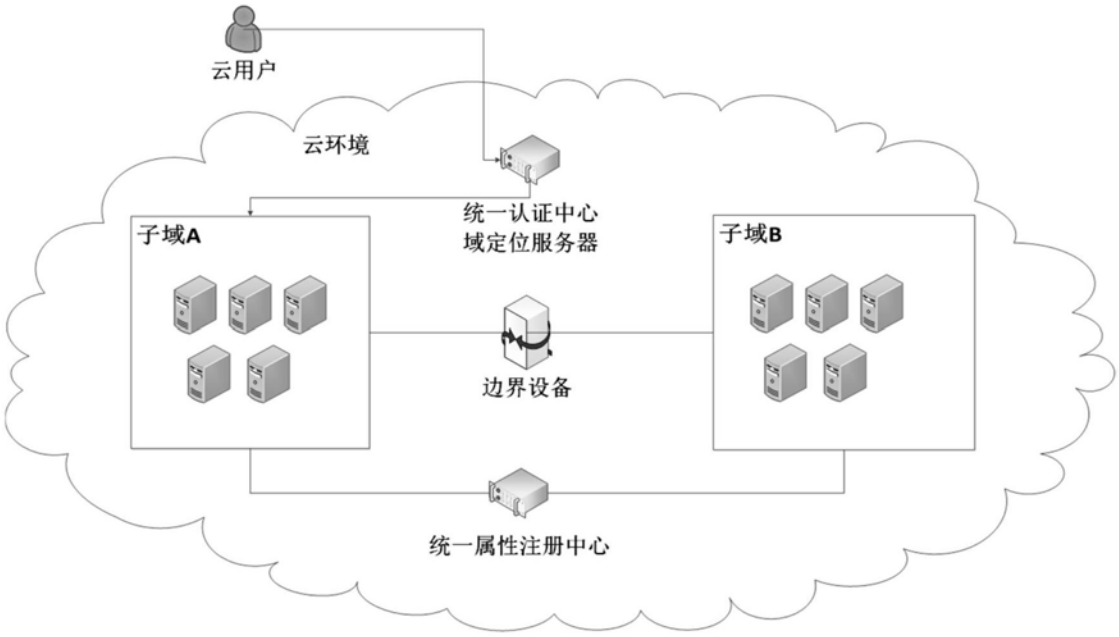

云用户
云环境
统一认证中心
域定位服务器
子域A
子域B
边界设备
统一属性注册中心

图1

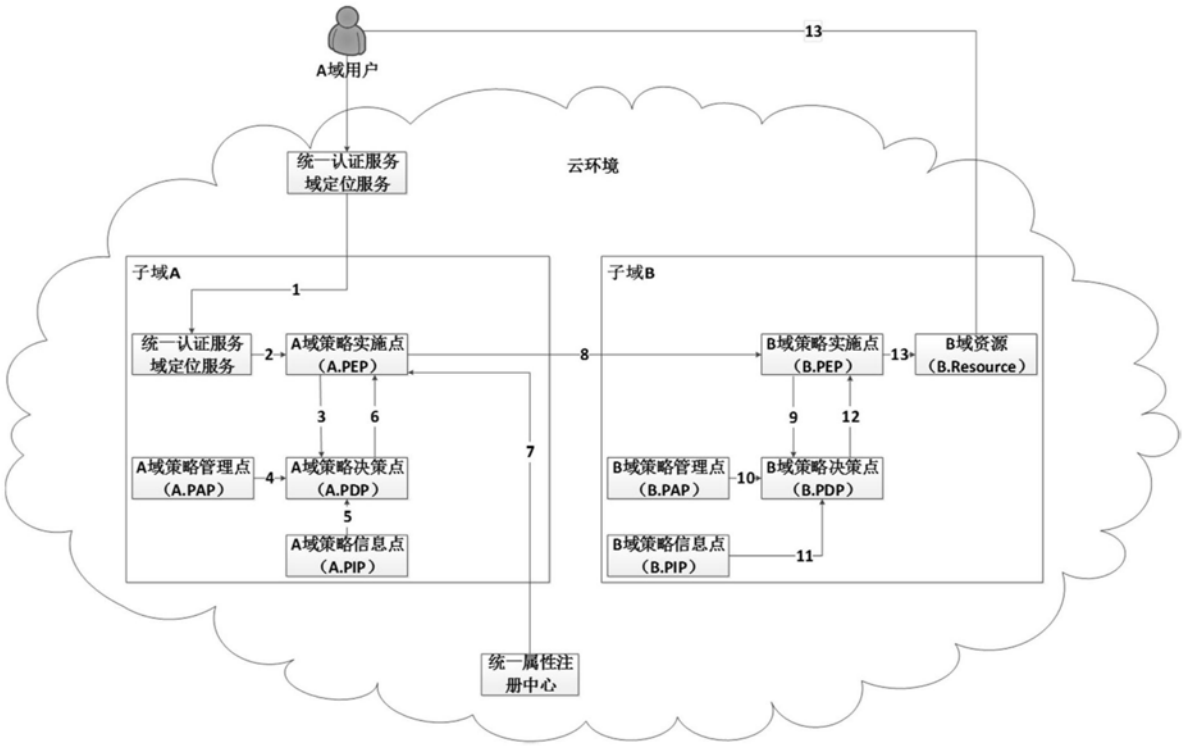

A域用户
13
统一认证服务
域定位服务
云环境
子域A
子域B
1
统一认证服务
域定位服务
2
A域策略实施点
（A.PEP）
8
B域策略实施点
（B.PEP）
13
B域资源
（B.Resource）
3
6
9
12
7
A域策略管理点
（A.PAP）
4
A域策略决策点
（A.PDP）
B域策略管理点
（B.PAP）
10
B域策略决策点
（B.PDP）
5
A域策略信息点
（A.PIP）
B域策略信息点
（B.PIP）
11
统一属性注
册中心

图2


开始
创建子域
构建资源管理系统
设定PEP、PAP、PIP、PDP等策略相关机构
设定该子域的属性和策略规则
注册到统一属性注册中心
分发到各个子域的PEP模块
结束

图3

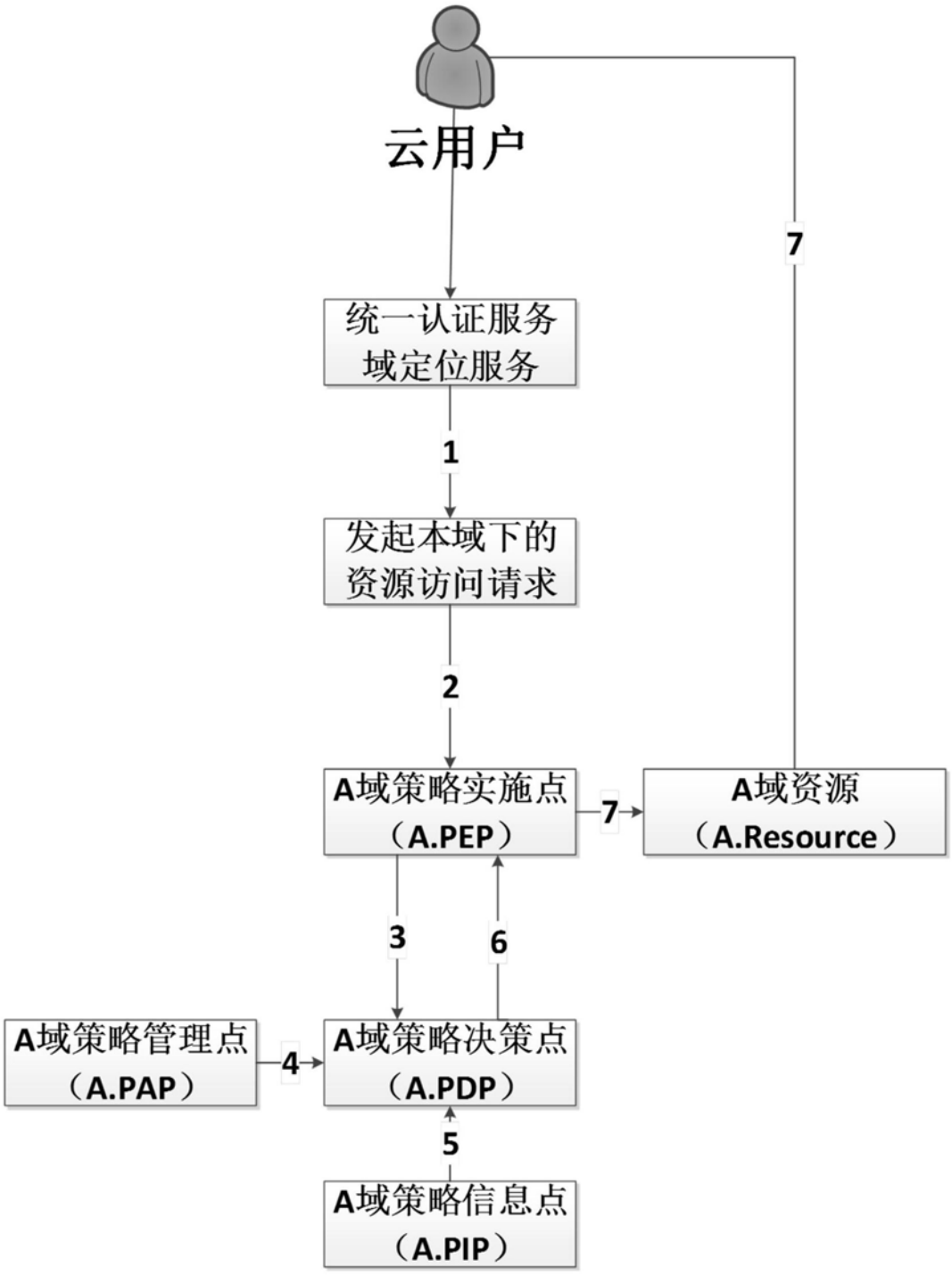

云用户
7
统一认证服务
域定位服务
1
发起本域下的
资源访问请求
2
A域策略实施点
（A.PEP）
7
A域资源
（A.Resource）
3
6
A域策略管理点
（A.PAP）
4
A域策略决策点
（A.PDP）
5
A域策略信息点
（A.PIP）

图4