针对飞地实例的云服务访问权限设置方法和云管理平台

相关申请的交叉引用

本申请要求在2022年02月25日提交中华人民共和国知识产权局、申请号为202210176632.8、申请名称为“基于云技术的服务提供方法和云管理平台”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；本申请要求在2022年05月30日提交中华人民共和国知识产权局、申请号为202210605661.1、申请名称为“针对飞地实例的云服务访问权限设置方法和云管理平台”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

本申请涉及云技术领域，特别涉及一种针对飞地实例的云服务访问权限设置方法和云管理平台。

背景技术

云技术（cloud technology）是指在广域网或局域网内将硬件、软件、网络等系列资源统一起来，实现数据的计算、储存、处理和共享的一种托管技术。随着云计算的发展，越来越多的租户将业务迁移到云上，由此也对云资源提出了更高的访问要求和安全要求。

其中，基于属性的访问控制（attribute based access control，ABAC）模型是业内常用的一种基于策略的访问控制方式，通过使用将属性组合在一起的策略，将访问权限授予用户，来实施较为精确的访问控制决策。

然而，该 ABAC 模型依赖于属性信息的收集、传递和使用，而如何安全有效地收集、传递和使用各类属性信息，仍为亟需解决的重要问题。

发明内容

本申请实施例提供一种针对飞地实例的云服务访问权限设置方法和云管理平台，有助于安全有效地收集、传递和使用各类属性信息，以保障不同类型的租户实现对云资源的集中、安全的访问管理。

第一方面，本申请实施例提供了一种针对飞地 enclave 实例的云服务访问权限设置方法，该方法可由云服务系统执行，该云服务系统可以包括云管理平台、目标云服务和 enclave 实例中的应用程序，其中，该云管理平台可以为云端服务器，enclave 实例中的应用程序可以部署在用户设备上。

该方法可以包括：云管理平台提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性；所述云管理平台提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌

获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

通过上述方法，云管理平台支持第一租户自定义安全管理服务配置信息，该安全管理服务配置信息包括第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，用于描述第一租户对自身订购的至少一个云服务的安全管理需求，以便 STS 根据接收到的令牌获取请求，向 enclave 实例中的应用程序发放关联于第一租户的安全管理需求的令牌，从而保障不同类型的租户实现对云资源的集中、安全的访问管理。

结合第一方面，在一种可能的实现方式中，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。可选地，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

通过上述方法，IAM 服务和 STS 可以根据证明文档，在满足授权策略的情况下，集中地向 enclave 实例中的应用程序发放访问目标云服务的个性化令牌，从而实现对不同类型的租户的云资源的集中、安全的访问管理。应理解的是，本申请实施例中，第一租户和第二租户是对用于实现不同管理功能的租户角色的划分，并不限定该租户为不同用户，在实际应用中，第一租户和第二租户可以为同一租户的不同角色，也可以为不同租户的不同角色，在此不再赘述。

结合第一方面，在一种可能的实现方式中，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

结合第一方面，在一种可能的实现方式中，所述方法还可以包括：所述 enclave 实例中的应用程序在发送所述令牌获取请求之前，从可信计算基 TCB 获取所述 enclave 实例的证明文档。

结合第一方面，在一种可能的实现方式中，所述方法还可以包括：所述 enclave 实例中的应用程序向所述目标云服务发送服务调用请求，所述服务调用请求携带有所述令牌；所述目标云服务接收所述服务调用请求，并向所述 STS 确认所述令牌的合法性，在所述 STS 确认所述令牌合法的前提下，所述目标云服务允许所述应用程序访问所述目标云服务。

结合第一方面，在一种可能的实现方式中，所述证明文档包括至少一个平台配置寄存器 PCR 度量值。

第二方面，本申请实施例提供了一种云服务系统，包括云管理平台和目标云服务，其中，所述云管理平台提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性；所述云管理平台提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问所述目标云服务的权限。

结合第二方面，在一种可能的实现方式中，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。

结合第二方面，在一种可能的实现方式中，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

结合第二方面，在一种可能的实现方式中，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

结合第二方面，在一种可能的实现方式中，所述 enclave 实例中的应用程序在发送所述令牌获取请求之前，从可信计算基 TCB 获取所述 enclave 实例的证明文档。

结合第二方面，在一种可能的实现方式中，所述 enclave 实例中的应用程序向所述目标云服务发送服务调用请求，所述服务调用请求携带有所述令牌；所述目标云服务接收所述服务调用请求，并向所述 STS 确认所述令牌的合法性，在所述 STS 确认所述令牌合法的前提下，所述目标云服务允许所述应用程序访问所述目标云服务。

结合第二方面，在一种可能的实现方式中，所述证明文档包括至少一个平台配置寄存器 PCR 度量值。

第三方面，本申请实施例提供了一种云管理平台，包括：第一服务提供模块，用于提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性；第二服务提供模块，用于提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

结合第三方面，在一种可能的实现方式中，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。

结合第三方面，在一种可能的实现方式中，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

结合第三方面，在一种可能的实现方式中，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

第四方面，本申请实施例提供了一种云管理平台，包括处理器和存储器，所述存储器存储有程序指令，所述处理器执行所述程序指令以执行上述第一方面中云管理平台执行的任一项方法。

第五方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质用于存储计算机程序，当所述计算机程序在计算装置上运行时，使得所述计算装置执行如上述第一方面以及第一方面任一可能实现方式所述的方法。

本申请实施例在上述各方面提供的实现的基础上，还可以进行进一步组合以提供更多

实现。

上述第二方面至第五方面中任一方面中的任一可能实现方式可以达到的技术效果，可以相应参照上述第一方面中任一方面中的任一可能实现方式可以达到的技术效果描述，重复之处不予论述。

附图说明

图 1 示出了本申请实施例适用的云服务系统架构示意图；

图 2 示出了一些基于云技术的服务提供方案的示意图；

图 3 示出了本申请实施例的云服务系统架构的示意图；

图 4 示出了本申请实施例的云服务访问权限设置方法的流程示意图；

图 5 示出了本申请实施例的云服务访问权限设置方法的流程示意图；

图 6 示出了本申请实施例的云管理平台的结构示意图；

图 7 示出了本申请实施例的通信装置的结构示意图。

具体实施方式

以下，对本申请实施例中的部分用语进行解释说明，以便于本领域技术人员理解。

1、云服务:

基于因特网（Internet）、以表现层状态转移应用程序接口（representational state transfer application programming interface，REST API）形式提供的、满足企业互联网技术（internet technology，IT）所需的弹性计算、虚拟网络、数据存储、数据库等服务。

本申请实施例中，可以将云服务的提供商简称为云厂商。

2、云资源:

云管理平台为租户提供的云计算资源的简称，是指云计算相关的资源的整合，包括云服务和云实例。

云服务例如可以包括但不限于私有网络（virtual private cloud，VPC）提供服务、网关提供服务、防火墙服务、NAT 服务、云盘、弹性公网 IP（elastic IP address，EIP）、云监控服务以及其他各种云厂商提供的云服务。云实例例如可以包括但不先于虚拟机、容器或裸金属服务器等，其中，虚拟机、容器或裸金属服务器均为云厂商在云厂商的数据中心提供给租户使用的虚拟实例。示例地，云实例可以包括飞地 enclave 实例。

3、租户:

云资源的属主，是对云资源拥有管理权限的主体。

其中，租户可以按照业务需求，通过付费方式，向云厂商订购或租用云资源。租户对购买的云资源的管理权限可以包括但不限于安全管理权限、访问控制权限等。其中，可以按照租户所实现的不同管理功能，将租户按角色划分为第一租户和第二租户，该第一租户例如可以用于实现对购买的云资源的安全管理权限，该第二租户可以用于实现对购买的资源的访问控制权限。

本申请实施例中，租户对云资源的管理权限可以通过租户的电子设备（包括实体设备和/或虚拟装置）实现。在一些实施例中，租户的电子设备可以称为租户节点。第一租户和

第二租户可以为同一租户的不同角色，也可以为不同租户的部分角色，本申请实施例对此不作限定。

4、用户：

云资源的操作人员，被云资源属主授权后才能操作云资源。

本申请实施例中，用户对云资源的操作可以通过用户的电子设备（包括实体设备和/或虚拟装置）实现。在一些实施例中，用户的电子设备可以称为用户节点。

本申请实施例中，用户可以包括 enclave 实例中的应用程序。

5、身份管理与访问控制（identity and access management，IAM）服务：

一种 Web 服务，可以帮助租户安全地控制对资源的访问，控制用户（例如 enclave 实例中的应用程序）进行身份验证（登录）和授权（具有权限）以使用资源，具有单点登录、强大的认证管理、基于策略的集中式授权和审计、动态授权、企业可管理性等功能。

在本申请实施例的云服务场景中，租户可以通过 IAM 服务来对用户实施访问控制管理，针对不同云资源向不同用户授予不同权限。

6、安全令牌服务（security token service，STS）：

一种临时访问权限管理服务，用于获取可以自定义时效和访问权限的临时访问凭证，即安全令牌（STS Token）。

在本申请实施例的云服务场景中，租户在向云厂商购买云资源时，可以在云厂商进行注册，获得租户的实体身份标识（tenant identity）以及访问凭证（例如包括身份密钥、登录密码等）。租户可以给用户创建对应的身份（user identity）及凭证（例如身份密钥等），并对用户授权；用户在获得凭证及授权后，可以基于用户的访问凭证从 STS 获取 STS Token，从而使用 STS Token 访问租户购买的云资源，例如目标云服务。

7、基于属性的访问控制（attribute based access control，ABAC）：

一种访问控制方法，根据主体的指派属性、客体的指派属性、环境条件和与这些属性和条件相关的一组策略，允许或拒绝主体对客体所请求的操作。

其中，属性是主体、客体或环境条件的特征。属性信息可以以“名称-值”对的形式定义。

主体是人或非执行实体（Non-Practicing Entities，NPE）（如对客体发起访问请求的设备）。主体可以被指派一个或多个属性。

由 ABAC 模型管理其访问机制的系统资源，例如包含或接收信息的设备、文件、记录、表、进程、程序、网络或域。它可以是资源或被请求访问的实体，也可以是任何可被主体操作的对象，包括数据、应用程序、服务、设备和网络等。

操作是应主体对客体的请求而需要被执行的功能，可以包括但不限于读、写、编辑、删除、复制、执行和修改等。

策略是规则或关系的表达，该策略使云管理平台能够根据给定的主体、客体和可能的环境条件的属性值来确定是否允许主体所请求的访问。

环境条件：访问请求所处的环境/态势上下文。环境条件是可检测的环境特征，独立于主体或客体，可以包括当前时间、星期几、用户位置或当前威胁级别、安全级别等。

需要说明的是，本申请实施例中，ABAC 是一种逻辑访问控制方法，该逻辑访问控制的目的是保护客体（无论是数据、服务、应用程序、网络设备或是其他类型的 IT 资源）不受未授权操作的影响，这些操作可能包括发现、读取、创建、编辑、删除和执行客体。受保护客体归个人或组织（例如本申请实施例的租户）所有，并具有某种内在价值，激励这

些所有者保护它们。作为客体的所有者，租户有责任建立一个策略，来描述可以对客体执行哪些操作、由谁执行，以及主体在什么上下文中可以执行这些操作。如果主体满足客体属主所建立的访问控制策略，则该主体被授权可以对客体执行所需的操作，即该主体被授予对该客体的访问权限。如果主体不满足策略，则拒绝对该客体的访问。

8、可信运行环境（trusted execution environment，TEE）:

一种基于硬件增强的运行环境隔离机制（例如 ARM Trust Zone），与片上系统（System-on-a-chip）的其他模块隔离并能够执行可信应用程序（trusted application，TA）的安全区域，能够确保敏感数据在隔离、可信环境中存储、处理和保护，通过提供隔离的、安全执行的授权软件，实现端到端安全。

其中，TEE 可以通过对硬件、固件、系统软件和应用程序等的度量来定义运行环境的特征，并可以提供运行环境特征的证明文档。

9、可信计算基（trusted computing base，TCB）:

指为实现计算机系统安全保护的所有安全保护机制的集合，各机制可以以硬件、固件和软件的形式出现。一旦可信计算基的某个构件出现程序错误或者安全隐患，就会对整个系统的安全造成危害。与之相反，如果除可信计算基之外的系统的其他部分出现问题，也只是泄漏了系统安全策略赋予它们的相关权限而已，这些权限一般都是比较低的，对系统的安全造成危害较小。

本申请实施例中，TCB 可以包括安全模块和公钥基础设施（public key infrastructure，PKI），其中，安全模块可以为用户节点提供业务安全相关的信息，例如可信硬件信息、可信软件信息、可信固件信息等；安全模块还提供对用户节点运行环境的启动度量，并提供对运行环境的证明文档。PKI 是安全模块的基础设施，它可为安全模块颁发数字证书，PKI 提供信任根证书。STS 会使用 PKI 的根证书来验证安全模块所提供的证明文档的合法性。

10、飞地 enclave:

在硬件安全扩展中，英特尔 SGX 提供的称为 enclave 的硬件安全的受信任执行环境。飞地可以为用户程序提供机密性和完整性的有力保证，以对云厂商的最小信任来保护用户外包数据的安全性。

11、服务提供模块:

云管理平台的用于实现管理服务的功能模块，以便帮助租户安全地控制用户对云资源的访问控制管理。该管理服务可以包括但不限于上述 IAM 服务、STS 等。其中，一些服务可以配合使用，例如 IAM 服务提供对用户的长期权限配置（不带有效期限的授权），而 STS 可以按用户的单次业务会话（session）来颁发一个较短有效期、按需进行权限收缩的安全访问令牌，以提供更为精细的访问控制管理。

本申请实施例中，该管理服务还可以包括安全管理服务，该安全管理服务可由云管理平台的安全管理服务提供模块提供，支持租户节点根据自身的应用场景需求、业务需求等，向云管理平台提供租户自定义的安全管理服务配置信息（包括租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则），以便云管理平台集中、安全地对租户购买的云服务实施访问控制管理。

其中，在具体应用中，一个可能的实现方式是，该安全管理服务提供模块可以为云管理平台的独立服务提供模块，该安全管理服务提供模块可以与云管理平台的其它服务提供模块（例如 IAM 服务提供模块和/或 STS 提供模块）具有信任关系，使得其它服务提供模

块能够结合租户自定义的安全管理服务配置信息，对云资源实施集中、安全的访问控制管理。另一种可能的实现方式是，该安全管理服务提供模块可以为云管理平台的某个服务提供模块（例如 IAM 服务提供模块或 STS 提供模块）的子模块，使得该服务提供模块能够结合租户自定义的安全管理服务配置信息，对云资源实施集中、安全的访问控制管理。本申请实施例对该安全管理服务提供模块的部署方式或者产品形态不做限定。

12、请求参数（request params）:

租户或者应用程序向云管理平台或云服务模块（用于向租户或应用程序提供至少一种云服务）发送的一系列参数，用于请求对租户节点购买的云资源进行管理配置或者实施访问操作。

本申请实施例中，租户或者应用程序可以通过调用云管理平台或云服务模块提供的应用程序接口（application program interface， API），分别向云管理平台或云服务模块传入相应的请求参数。该请求参数可以按照云管理平台或云服务模块支持的通信协议规定的格式进行组织或构建。例如，该请求参数可以承载在 API 请求报文中，该 API 请求报文可以包括 API 请求头（request header）和 API 请求体（request body）。该 API 请求头可以用于承载用于指示通信协议、请求方法（例如 SET 方法、GET 方法或 DELETE 方法等）、对 API 请求体的签名等的参数，该 API 请求体中用于承载 API 请求者的身份标识、用户节点的属性文档等参数。本申请实施例对该请求参数的具体内容以及组织方式不做限定。

本申请实施例涉及的至少一个，包括一个或者多个；其中，多个是指大于或者等于两个。另外，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述对象的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

下面结合附图及实施例详细介绍本申请。

图 1 示出了本申请实施例适用的云服务系统的架构示意图。

如图 1 所示，该云服务系统 100 可以包括云厂商提供的云管理平台 110、以及云服务模块 120。

云管理平台 110 对外可通过互联网与租户（例如权限管理员）操作的电子设备、或者用户（例如运维人员、应用程序等）操作的电子设备连接。云管理平台 110 在系统 100 内可通过内部网络与云服务模块 120 连接。租户可以在云管理平台 110 注册账号，该账号具有购买（包括订购或租用等不同付费形式）云资源的资格。在购买云资源成功后，云管理平台 110 可以通知云服务模块 120 创建云资源，并向租户以及租户授权的用户(例如其他租户)提供合适的访问方式，以便租户远程管理云资源，以及控制用户远程访问或使用云资源，来为租户和用户提供至少一种云服务，表示为云服务 1、云服务 2、……、云服务 n，n 为大于等于 1 的整数。

举例而言，云资源例如为一个虚拟机，租户可以在云管理平台选择虚拟机的规格（例如内存、处理器和磁盘等），云管理平台 110 在租户付费成功后，通知云服务模块 120 创建具有该规格的虚拟机。租户可以配置用户对该虚拟机的访问权限（如登录到虚拟机，对虚拟机的停机操作、删除操作等），配置成功后，该用户就可以对该虚拟机执行相应的授权操作。租户也可以将购买或创建虚拟机权限授予给用户。应理解，本申请实施例中，云资源也可以例如为容器、裸金属服务器、弹性公网 IP（Elastic IP Address，EIP）等各种云服务，本申请实施例对云服务类型不作限定。

云管理平台 110 可以包括至少一个服务提供模块，该至少一个服务提供模块可用于为租户和用户提供相应的服务，以便帮助租户安全地实现对购买的云资源的访问控制管理，针对不同云资源向不同用户授予不同的访问权限，以及控制用户进行身份验证和授权等，以便用户安全地访问或使用云资源。

示例地，该至少一个服务提供模块可以包括 IAM 服务提供模块 111 和 STS 提供模块 112。该 IAM 服务提供模块 111 为租户和用户提供前文述及的 IAM 服务，该 STS 提供模块 112 为租户和用户提供前文述及的 STS 服务。

目前，在一些基于云技术的服务提供方案中，租户会使用前文述及的 IAM 服务、STS 服务，来配置应用程序的访问控制策略，以及实施用户对云资源的访问控制管理。该方案可以包括如图 2 所示的方法步骤:

S21: 租户通过云管理平台 110 侧的 IAM 服务提供模块 111 提供的 IAM 服务，为用户设置（set）授权策略（authorization policy），也即访问控制策略。

S22: 设置完成后，IAM 服务提供模块 111 会向租户反馈授权应答结果。

如果设置成功，则被授权的用户可以使用相应的权限，可以对租户购买的云资源进行访问操作。如果设置失败，则用户未获得授权，该用户将无法对租户购买的云资源进行访问操作。

S23: 用户在获得授权后，可以获得正确的访问凭证（例如访问密钥（Access Keys））。该情形下，用户可以基于所获得的访问凭证，向云管理平台 110 侧的 STS 提供模块 112 发送请求参数，该请求参数中可以包含用户的访问凭证，该请求参数用于请求获取 STS 令牌，该 STS 令牌用于用户对租户购买的云资源进行访问操作。

S24: STS 提供模块 112 接收到来自应用程序的请求参数后，通过与 IAM 服务提供模块 111 之间的信任关系，在基于来自用户的访问凭证验证身份以及权限成功后，向用户发放目标 STS 令牌。

S25: 用户基于从 STS 提供模块 112 获得的目标 STS 令牌，向云服务模块 120 发起访问请求，以请求访问目标云服务，例如云服务 1。

S26: 云服务模块 120 侧的目标云服务通过与 STS 提供模块 112 之间的信任关系，在基于来自应用程序的目标 STS 令牌验证用户身份以及权限成功后，执行相应的访问处理操作，并向应用程序反馈访问应答。

其中，为了更精细地控制应用程序对云资源的安全访问，在一些设计中，云管理平台 110 还会在 IAM 服务提供模块 111 启用前文述及的 ABAC 模型，来为用户配置授权策略。

在这些设计中，在上述图 2 所示的 S21，租户可以适配于 ABAC 模型的使用要求，根据用户属性、资源属性、请求参数属性等来设置授权策略。在上述图 2 所示的 S25，当用户发起针对云资源的访问请求时，云服务模块 120 侧的目标云服务会根据来自用户的访问请求中携带的请求参数，来实施基于属性的访问控制检查，并在检查通过后，为用户提供目标云服务。

示例地，在启用 ABAC 模型时，云管理平台 110 可以提供 API，使得租户可以通过云管理平台 110 提供的 API，配置 ABAC 模型所需的相关属性信息，用于实现该配置的授权文档的格式例如如下所示:

{

"Effect" : //涉及的权限结果属性，例如：授权"Allow"，或者拒绝“Deny”，

"Principal" : //涉及的主体标识，例如：用户名"alice"，

"Action": [//对指定资源涉及的至少一个操作的操作标识，例如：对密钥管理服务（key mangement severce，KMS）资源的解密（Decrypt）、生成数据密钥（GenerateDataKey）等]，

"Resource": //涉及的资源标识，用于指定具体资源，可输入至少一个资源名称或资源标识等，

"Condition": { //涉及的访问控制条件属性，可通过字符串（String）的方式输入且可以用于访问条件控制，包括但不限于：主体标识涉及的相关属性，例如岗位、职称、资格、业务标签、状态等；资源属性，例如：资源标签、资源存放的地域等；用户请求相关属性，例如源 IP 地址（Source IP）、源 VPC 地址、通信协议（例如 https、http 等）；用户节点的运行环境相关属性，例如硬件标识、固件及软件的可信度量值（例如平台配置寄存器（platform configuration register，PCR），固件或软件的数字签名证书摘要值等，

}

}

其中，以授权语义为：“允许用户“张三”必须通过指定的信任级为 2 级的安全运行环境发起请求才可以执行指定的 KMS 操作；其中信任级为 2 级的安全运行环境被定义为预先知晓的一个可信赖的软件度量值 PCR0，以及预先知晓的一个可信赖的数字签名证书摘要值 PCR8”为例，该授权文档可以如下所示：

```
{
    "Effect" : "Allow",
    "Principal" : "张三",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
    ],
    "Resource": "* ",
    "Condition": {
        "StringEquals": {
            "g:Attestation:PCR0":
"0xaef0def2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcde
f5abcdef4abcdef3abcdef2abcdef1abcdef0a1ef2",
            "g:Attestation:PCR8":
"0x1af2def2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcde
f5abcdef4abcdef3abcdef2abcdef1abcdef0abcde"
        }
    }
```

在上述启用 IAM 服务、STS 服务以及 ABAC 模型的服务提供方案中，授权策略支持的控制维度属性越多，访问控制的安全强度就会越高，虽然可以在一定程度上更精细地帮

助实现对租户购买的云资源的安全访问控制，但该方案设计对租户授权管理的专业水平要求较高，例如它要求授权管理人员能理解每个访问控制属性的精确语义及其正确的取值，这个在实践中非常困难，一般的授权管理人员并不理解用户的可信度量方法及可信度量值的测定，在授权策略中存储度量值是非常容易导致出错而且难以发现错误，这个会导致极大的管理成本。随之而来的新的设计挑战是，每个云服务如何安全有效地收集和传递各类属性，以保障不同类型的租户实现对云资源的集中、安全的访问管理，这个也导致每个云服务极大的技术设计和改造实施成本。

针对上述问题，本申请实施例提供了一种针对飞地 enclave 实例的云服务访问权限设置方法和云管理平台，有助于安全有效地收集、传递和使用各类属性信息，以保障不同类型的租户节点实现对云资源的集中、安全的访问管理，满足不同类型的租户对云资源的管理诉求、以及不同用户对云资源的使用诉求。

为了便于理解，下面在图 1 所示的系统架构的基础上，介绍本申请实施例的云服务系统、云管理平台、以及针对飞地 enclave 实例的云服务访问权限设置方法的实现原理。

如图 3 所示，本申请实施例适用的云服务系统 300 可以包括云管理平台 310 和云服务模块 320。

与图 1 相似地，云管理平台 310 对外可通过互联网与租户或者用户的电子设备连接。云管理平台 310 在系统 300 内可通过内部网络与云服务模块 320 连接。租户可以在云管理平台 310 注册账号以购买（包括订购或租用等不同付费形式）云资源。在购买资源成功后，云管理平台 310 可以通知云服务模块 320 创建云资源，并向租户以及租户节点授权的用户提供合适的访问方式，以便租户远程管理云资源，以及控制用户远程访问或使用云资源，来为用户提供基于该云资源对应的云服务，例如，可以表示为云服务 1、云服务 2、……、云服务 n，n 为大于等于 1 的整数。该云资源可以为容器、裸金属服务器、弹性公网 IP（Elastic IP Address，EIP）等各种云服务，本申请实施例对云服务类型不作限定。

其中，云管理平台 310 可以包括至少一个服务提供模块，例如包括但不限于安全管理服务提供模块 311、IAM 服务提供模块 312 以及 STS 提供模块 313 等。可选地，该至少一个服务提供模块中的任一服务提供模块还可以包括子功能单元，例如，安全管理服务提供模块 311 可以包括对象管理单元，STS 提供模块 313 包括验证单元、属性转换单元和生成单元。该云管理平台 310 的至少一个服务提供模块及其子功能单元，可以帮助收集和传递各类属性信息，以保障不同类型的租户实现对其购买的云资源的集中、安全的访问管理，满足不同类型租户对云资源的管理诉求、以及不同用户对云资源的使用诉求，实现本申请实施例的方法。

可以理解的是，图 3 中仅示例性地表示该系统 300 可以包括的功能模块，并不限定各功能模块的数量以及功能，例如，该系统 300 中可以包括多种类型的云服务模块，任一云服务模块也可以包括各自的云服务子模块，来为不同类型租户提供不同类型的云服务，本申请实施例的云管理平台 310 的服务提供模块不限于图 3 所示的服务提供模块，对服务提供模块的子功能单元也不做限定，在此不再赘述。

下面以云实例为飞地 enclave 实例为例，结合附图及实施例，对图 3 所示的系统 300 以及该系统 300 所包含的功能模块及其子功能单元的功能进行介绍。

1、安全管理服务提供模块 311:

该安全管理服务提供模块 311 用于对租户、用户以及租户购买的云资源提供安全管理服务，包括但不限于基于安全管理服务配置信息实现对安全管理服务的生成（create）、描述（describe）、升级（update）或者删除（delete）等功能，以使得该安全管理服务提供模块 311 可以支持租户自定义属性，帮助安全有效地收集、传递以及使用租户自定义的用于实现安全管理服务的相关属性。

如图 3 所示，该安全管理服务提供模块 311 可以包括对象管理单元，该对象管理单元可以接收第一租户（例如安全管理员）输入或选择的安全管理服务配置信息，该安全管理服务配置信息例如可以包括用于描述属性对象的元数据以及转换规则，对象管理单元可以根据该安全管理服务配置信息创建至少一个属性对象，每个属性对象可以包括至少一个属性的元数据（metadata）和转换规则（rule），该元数据用于描述所述至少一个属性的类型和操作方法，该转换规则为所述至少一个属性的转换规则。IAM 服务提供模块 312 和 STS 提供模块 313 基于与该安全管理服务提供模块 311 之间的信任关系，可以利用该安全管理服务提供模块 311 的至少一个属性对象的元数据和转换规则，来集中、安全地实现对租户购买的云资源的访问控制管理。

具体而言，在具体配置时，在一个示例中，云管理平台 310 可以向第一租户提供安全管理服务配置 API，该安全管理服务配置 API 用于指示表示所述安全管理服务配置信息的不同属性对象的多个字段。第一租户可以在其电子设备上对每个字段输入相应的参数。云管理平台 310 可以接收第一租户的电子设备发送的安全管理服务配置信息，该安全管理服务配置信息可以包括该多个字段和所述租户节点针对每个字段输入的参数。在另一个示例中，云管理平台 310 可以向第一租户的电子设备提供控制台界面，该控制台界面可以提供多个属性配置项。第一租户可以在控制台界面的多个属性配置项输入或选择相应的参数。云管理平台 310 可以确定所述第一租户在所述控制台界面输入或选择的所述安全管理服务配置信息，该安全管理服务配置信息包括控制台界面提供的多个属性配置项及所述第一租户针对每个属性配置项输入或选择的参数。本申请实施例对此配置过程的具体实现方式不做限定。

第一租户在云管理平台 310 对安全管理服务提供模块 311 的功能配置完成后，安全管理服务提供模块 311 可以保存获取到的安全管理服务配置信息。该对象管理单元可以根据保存的安全管理服务配置信息中的属性对象描述信息创建至少一个属性对象，以便对购买的云资源实施访问控制管理。

其中，以云管理平台 310 提供 API 的方式来对安全管理服务提供模块 311 的功能配置为例，用于实现该安全管理服务配置的文档格式中可以包括元数据字段以及转换规则字段，例如如下所示:

{

Metadata: //描述属性对象涉及的属性的元数据，可以是以键值对形式输入或选择的，包括但不限于时间戳（timestamp）、摘要（digest）、硬件 ID、固件与软件的安全版本号、固件与软件代码的度量值（PCRs）、代码签名证书（Certificate，简写为 cert）以及其它与用户业务相关的应用数据（user data）等;

Rules: //属性对象涉及的转换规则，可以包括一条或多条转换规则；属性转换功能会将一组满足条件的输入属性集，根据相应的属性转换规则转换成一组输出属性集。

}

具体地，云管理平台 310 可以在互联网提供的网页上显示以上文档格式，并注明相应字段的用法，例如上述//后面的相关提示。租户在看到上述文档格式之后，根据上述文档格式填入相应的参数，例如在 "Metadata":后面填入以下信息（这里仅提供一个举例）:

```
{
    security_version_number: uint   .size 8        ; 运行环境的安全版本号
    timestamp: uint   .size 8,                     ; 证明文档的创建时间
    digest:  text,                                  ; 启动运行环境时计算 PCR 度量值的哈希算法
    pcrs:  [*  text]                                ; PCR 度量值列表，可以支持多个 PCR 值
    certificate: text,                             ; 证明文档的签名证书
    cabundle: [* text],                            ; 证明文档的签名证书的 CA 证书链
    public_key: text,                              ; 用户公钥数据
    user_data: text,                               ; 用户业务数据
    nonce: text,                                   ; 一次性随机数 nonce
}
```

表示某个属性对象的元数据格式，它可以包含多个不同的属性名称与属性值，并指明了属性值的取值类型。其中，“uint   .size 8”表示类型为无符号整数，共 8 个字节。“text”表示文本类型。[* text]表示列表，其中包含一个或多个 text 值。";" 表示对指定类型的语义解释。

进一步，第一租户可以在" Rules ":后面填入一条或多条转换规则。一条转换规则的一种描述方法是:（输入属性集需满足的条件表达式）=> （输出属性集）。一个 Rules 的实施举例如下所示:

```
“Rules”: {
    ([key==“security_version_number”,  value  >=  10])  =>  ([key=“DeviceUpdated”, value=“OK”]);
    ([key==“pcrs[0]”, value==“0xaef0def2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef0a1ef2”] &&
    [key==“pcrs[8]”, value==“0x1af2def2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef0abcde”])
    => ([key=“DeviceTrustLevel”, value=“2”])
}
```

其中，转换规则可以以键值对的形式存在并采用机器语言描述。以分号“; ”隔开不同的转换规则，每条属性转换规则中，“=>”表示输出，“=>”之前的键值对表示转换规则指定的输入属性集以及取值所需满足的条件，“=>”之后的键值对表示转换规则指定的输出属性集以及取值，符号“&&” 表示“并且”，或者称为“和”、“以及”等逻辑运算符，仅当输入的属性集及其取值满足指定条件时，才会输出指定的输出属性集。

例如，“[key==“security_version_number”, value >= 10]”中，key==“security_version_number”表示输入属性的键为 security_version_number，value >= 10 表示输入属性键 security_version_number 的取值条件为大于或等于 10。若待验证的相关属性信息满足 key==“security_version_number”以及 value >= 10，则满足相应的转换规则指定的条件，经过属性转换，能够得到输出属性集：[key=“DeviceUpdated”, value=“OK”]。

相似地，在 [key==“pcrs[0]”, value==“0xaef…a1ef2”] && [key==“pcrs[8]”, value==“0x1af2…abcde”] 中，key==“pcrs[0]”以及 key==“pcrs[8]”表示输入属性的键，value==“0xaef…a1ef2”以及 value==“0x1af2…abcde”分别表示输入属性的相应取值条件。若待验证的相关属性信息既满足 key==“pcrs[0]”, value==“0xaef…a1ef2” 又满足 key==“pcrs[8]”, value==“0x1af2…abcde”，则满足相应的转换规则指定的条件，经过属性转换能够得到输出属性集：[key=“DeviceTrustLevel”, value=“2”]，这个输出属性集中只有一个输出属性键 DeviceTrustLevel，该属性键的取值为 2。

应理解的是，上述的转换规则的描述语法只是一个举例，我们并不限制其它实施例也必须采用这种规则描述方法。在其它实施例中，可以采用完全不同的语法或符号语言来描述这些转换规则，在此不再赘述。

第一租户可以将上述输入了参数的多个字段以及相应的输入参数，以模板方式，通过互联网发送至云管理平台 310，云管理平台 310 检测该配置文档中不同字段对应的参数，从而获取第一租户针对不同字段对应的要求。因此，在本申请实施例中，安全管理服务配置信息可以包括安全管理服务配置字段和第一租户输入的参数。进一步，云管理平台 310 可以将来自第一租户的安全管理服务配置信息存储至安全管理服务提供模块 311 关联的存储器。安全管理服务提供模块 311 中的对象管理单元可以利用保存的安全管理服务配置信息来对属性对象实施管理，例如创建属性对象、提供基于属性对象的安全管理服务等。

本申请实施例中，待创建的属性对象可以与属性对象实例类型一一对应，属性对象实例类型可由云厂商和云管理平台 310 提供。根据云管理平台 310 支持的属性对象实例类型，第一租户在云管理平台 310 输入或选择的安全管理服务配置信息可以指示至少一个属性对象，对象管理单元可以根据该安全管理服务配置信息中的属性对象描述信息来创建至少一个属性对象，每个属性对象可以包括用于描述该属性对象的至少一个属性的元数据以及属性转换规则。

其中，每个属性对象涉及的元数据可以详细定义第一租户自定义的用于实施安全管理的实例类型以及取值范围，每个属性对象涉及的转换规则可以用于指定属性转换的计算规则，以便通过计算或逻辑判断，将实例类型对应的实例的指派属性、云资源的指派属性、环境条件和与这些属性和条件相关的一组策略（例如授权策略），判定允许或拒绝用户对云资源所请求的操作。云管理平台 310 的除安全管理服务提供模块 311 以外的其它服务提供模块可以基于与该安全管理服务提供模块 311 之间的信任关系，利用所述至少一个属性对象的元数据和属性转换规则，来实现相应的服务，从而提升安全性。例如，IAM 服务提供模块 312 可以利用至少一个属性对象的元数据和转换规则（包含有效的输出属性集），使用其输出属性集中的属性来帮助第二租户更有效地实施对云资源的访问控制管理。STS 提供模块 313 可以利用至少一个属性对象的元数据和属性转换规则（包含有效的输出属性集），使用其输出属性集中的属性来帮助第二租户实施对云资源的令牌管理服务。

需要说明的是，本申请实施例中，第一租户在属性对象描述信息中提供的元数据可以

是在属性对象实例提供商提供的元数据中选择的，也可以是第一租户自定义输入的。第一租户在属性对象描述信息中提供的转换规则可以是在属性对象实例提供商提供的属性转换规则中选择的，也可以是第一租户自定义输入的。属性对象描述信息中的元数据可以用于验证来自用户的相关信息的合法性，例如是否有配置信息指定的子属性、是否是配置信息指定的类型、是否符合配置信息指定的相关条件等。属性对象描述信息中的转换规则可以用于描述指定的输入属性集、指定该输入属性集转换为相应的输出属性集应满足的条件、以及相应的输出属性集。在来自用户的相关信息合法的情况下，属性对象描述信息中的转换规则，可以将来自用户的相关属性作为转换规则的输入属性集，在这些属性满足转换规则指定的条件的情况下，该输入属性集根据相应的转换规则可以得到相应的输出属性集。本申请实施例对配置信息的格式以及内容不做限定。IAM 服务提供模块 312 和 STS 提供模块 313 可以利用该输出属性集实施相应的服务。本申请实施例对该输出属性集的格式以及内容等也不做限定。

需要说明的，本申请实施例中，一种可能的实现方式是，该安全管理服务提供模块 311 可以为云管理平台 310 的独立服务提供模块，该安全管理服务提供模块 311 可以与云管理平台 310 的其它服务提供模块（例如 IAM 服务提供模块 312 和/或 STS 提供模块 313）具有信任关系，使得其它服务提供模块能够结合租户自定义的安全管理服务配置信息，对云资源实施集中、安全的访问控制管理。另一种可能的实现方式是，该安全管理服务提供模块 311 可以为云管理平台 310 的某个服务提供模块（例如 IAM 服务提供模块 312）的子模块，使得该服务提供模块能够结合租户自定义的安全管理服务配置信息，对云资源实施集中、安全的访问控制管理。本申请实施例对该安全管理服务提供模块 311 的部署方式或者产品形态不做限定。

2、IAM 服务提供模块 312:

该 IAM 服务提供模块 312 可以帮助租户安全地控制对云资源的访问，控制用户进行身份验证（登录）和授权（具有权限）以使用云资源，具有单点登录、强大的认证管理、基于策略的集中式授权和审计、动态授权、企业可管理性等功能。

其中，租户对云管理平台 310 的不同服务提供模块的配置可以是互通的。相似地，云管理平台 310 可以向第一租户或者第二租户（例如权限管理员）提供 IAM 服务配置 API 或者控制台界面，第一租户或者第二租户可以通过云管理平台 310 提供的 API 或者控制台界面，向 IAM 服务提供模块 312 提供 IAM 服务配置信息，例如授权策略。IAM 服务提供模块 312 可以保存来自第一租户或者第二租户的授权策略。进一步，IAM 服务提供模块 312 可以利用至少一个属性对象的元数据和属性转换规则（包含有效的输出属性集）、以及授权策略，来对用户实施访问控制管理。

以第一租户或者第二租户通过 API 在云管理平台 310 输入或选择授权策略为例，该授权策略可以通过采用如下格式的授权文档实现配置:

{

"Effect" : //涉及的权限结果属性，例如：授权"Allow"，或者拒绝“Deny”，

"Principal" : //涉及的主体标识，例如：用户名"alice"，

"Action": [//对指定资源涉及的至少一个操作的操作标识，例如：对密钥管理服务（key mangement severce，KMS）资源的解密（Decrypt）、生成数据密钥（GenerateDataKey）等]，

"Resource": //涉及的资源标识，用于指定具体资源，可输入至少一个资源名称或资源标识等，

"Condition": { //涉及的访问控制条件属性，可通过字符串（String）的方式输入且可以用于访问条件控制，包括但不限于：主体标识涉及的相关属性，例如岗位、职称、资格、业务标签、状态等；资源属性，例如：资源标签、资源存放的地域等；用户请求相关属性，例如源 IP 地址（Source IP）、源 VPC 地址、通信协议（例如 https、http 等）；用户节点的运行环境相关属性，例如硬件标识、固件及软件的可信度量值（例如 PCR 值），固件或软件的数字签名证书摘要值等，

}

}

其中，以授权语义为："允许用户"张三"必须通过指定的信任级为 2 级的安全运行环境发起请求才可以执行指定的 KMS 操作"为例，该授权文档可以如下所示（该授权文档使用了 DeviceTrustLevel 属性键，这一属性键是来自前文的转换规则举例中的一个输出属性集）：

```
{
    "Effect" : "Allow",
    "Principal" : "张三",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
    ],
    "Resource": "* ",
    "Condition": {
        "StringEquals": {
            "DeviceTrustLevel=2"
        }
    }
```

第一租户或者第二租户可以将上述输入了参数的多个字段以及相应的输入参数，以模板方式，通过互联网发送至云管理平台 310，云管理平台 310 检测该授权文档中不同字段对应的参数，从而获取第一租户或者第二租户针对不同字段对应的要求。因此，在本申请实施例中，IAM 服务配置信息可以包括 IAM 服务配置字段、第一租户或者第二租户输入的参数。进一步，云管理平台 310 可以将来自第一租户或者第二租户的 IAM 服务配置信息存储至 IAM 服务提供模块 312 关联的存储器。IAM 服务提供模块 312 可以利用保存的 IAM 服务配置信息，来帮助第一租户或第二租户集中、安全地对云资源实施访问控制管理。

需要说明的是，在实际应用中，若安全管理服务提供模块 311 为云管理平台 310 的某个服务提供模块（例如 IAM 服务提供模块 312）的子模块，相应地，可以通过对 IAM 服务提供模块 312 进行功能扩展或扩展功能组件，使得功能扩展后的该 IAM 服务提供模块 312 可以实现安全管理服务提供模块 311 所实现的功能，详细可参见上述结合安全管理服务提供模块 311 的相关描述，在此不再赘述。

3、STS 提供模块 313：

该 STS 提供模块 313 用于为用户提供自定义时效和访问权限的临时访问凭证，即安全令牌（STS Token）。

本申请实施例中，云管理平台 310 可以对 STS 提供模块 313 进行功能扩展，例如扩展 STS 令牌发放功能 API，使得 STS 提供模块 313 可以根据令牌发放功能 API 指定的输入属性，以及第一租户自定义的转换规则，向用户（例如 enclave 实例中的应用程序）返回带有租户自定义属性的令牌，该令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

其中，用户可以通过任意方式获取第一租户赋予用户的访问凭证。该用户可以从可信计算基 TCB 获取 enclave 实例的证明文档，并利用该访问凭证以及该证明文档请求调用云管理平台 310 提供的 API，以向云管理平台 310 的 STS 提供模块 313 发送令牌获取请求，该令牌获取请求中携带有请求参数，该请求参数用于请求获取对目标云服务的 API 的访问令牌。

该请求参数中除了包含用于发放 STS 令牌所需的基本信息（例如资格证书、数字签名等）以外，还可以包含第一租户在安全管理服务配置时自定义的输入属性所要求的待验证的属性信息，例如第一租户输入或选择的飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档。STS 提供模块 313 的验证单元可以基于 STS 提供模块 313 与安全管理服务提供模块 311、IAM 服务提供模块 312 之间的信任关系，先对请求参数进行合法性验证，包括但不限于验证用户的身份或权限、验证该请求参数中是否包含指定的输入属性、验证输入属性的合法性（包括对输入属性的数字签名及过期时间等的验证）。如果验证失败，云管理平台 310 向用户节点返回错误提醒。如果验证成功则验证通过。

在合法性验证通过后，STS 提供模块 313 的属性转换单元可以根据至少一个属性对象中的转换规则对请求参数中的输入属性集进行条件判断，输入属性集满足转换规则所指定的条件后进行属性转换，确定相应的输出属性集，即租户自定义属性。STS 提供模块 313 的生成单元可以根据该输出属性集生成目标访问令牌，即携带有租户自定义属性的令牌。云管理平台 310 可以向 enclave 实例中的应用程序发送该令牌。

enclave 实例中的应用程序可以利用所获得的目标访问令牌，向云服务模块 320 提供的目标云服务发送服务调用请求。云服务模块 320 中的目标云服务接收该服务调用请求后，向 STS 确认该令牌的合法性，在 STS 确认该令牌合法的前提下，目标云服务可以运行应用程序访问目标云服务。

其中，一个可选的实施方式中，目标云服务可以将来自应用程序的目标访问令牌，通过内部网络发送给云管理平台 310。云管理平台 310 的 STS 提供模块 313 可以对该目标访问令牌进行合法性验证，例如确定该目标访问令牌是否为 STS 提供模块 313 发放的、该目标访问令牌关联的属性集是否为安全管理服务提供模块 311 的转换规则转换得到的输出属性集。IAM 服务提供模块 312 可以对该目标访问令牌进行访问控制检查，例如该目标访问令牌关联的属性集是否满足授权策略授予应用程序的权限。另一个可选的实施方式中，目标云服务可以基于与云管理平台 310 的各个服务提供模块之间的信任关系，从相关的服务提供模块获取用于进行合法性验证以及访问控制检查等所需的信息（包括但不限于 STS 提供模块 313 所生成的 STS 令牌的验证密钥或证书），并利用所获得的信息，在云服务模块 320 本地对来自应用程序的目标访问令牌进行合法性验证以及访问控制检查，本申请实施例对此实现方式不做限定。

需要说明的是，在实际应用中，若安全管理服务提供模块 311 为云管理平台 310 的某个服务提供模块（例如 STS 提供模块 313）的子模块，相应地，可以通过对 STS 提供模块 313 进行功能扩展或扩展功能组件，使得功能扩展后的该 STS 提供模块 313 可以实现安全管理服务提供模块 311 所实现的功能，详细可参见上述结合安全管理服务提供模块 311 的相关描述，在此不再赘述。

至此，已经结合附图及实施例介绍了本申请实施例的云服务系统 300 及其功能模块。其中，云管理平台 310 可以提供租户期望的安全管理服务信息的自定义通道，以供租户自定义配置安全管理服务信息。对于通过 API 设置安全管理服务信息的租户，该云管理平台 310 会按照租户自定义的安全管理服务配置信息对关联的其它服务，例如 IAM 服务、STS 服务等进行功能扩展，使得该云管理平台 310 可以根据租户自定义的安全管理服务配置信息，集中、安全地实现对租户购买的云资源的访问控制管理。该方案能够将对云管理平台 310 的功能的升级改造与云服务模块解耦，使得无需对云服务模块进行改造，以较低的改造成本即可支持本申请实施例的服务提供方案。对于租户（例如安全管理员或权限管理员）而言，无需感知 enclave 实例中的应用程序的硬件或软件运行环境的底层特征语义以及不同应用程序对应的硬件特性的差异，编写授权策略更加简单易实现，极大地降低策略的编写和管理成本。同时，该方案使得应用程序在 STS 令牌的有效期内可以直接使用该 STS 令牌，能够极大地降低应用程序所在设备的性能开销。

需要说明的是，本申请上述实施例中，仅以云管理平台提供的 IAM 服务以及 STS 服务为例，对基于租户自定义配置的安全管理服务实现的权限管理功能的示例说明而非任何限定。在其它实施例中，云管理平台还可以向租户和用户提供其它服务，该其它服务也可以结合租户自定义配置的安全管理服务实现，以集中、安全地实施对租户购买的云资源的权限管理，相似实现可参见上文结合安全管理服务提供模块 311 的相关介绍，在此不再赘述。

需要说明的是，本申请实施例中，应用程序向云管理平台传入的请求参数中携带属性信息，仅是本申请实施例的服务提供方法的实现方式的示例说明而非限定。在另一个示例中，请求参数中可以不包含租户在安全管理服务配置时自定义的输入属性所要求的待验证的属性信息。例如，根据应用场景或业务需求，云管理平台可以在自身关联的（或者能够访问的）存储器中存储租户在安全管理服务配置时自定义的输入属性所要求的待验证的属性信息，来自用户的请求参数可以包含用户的身份信息以及发放 STS 令牌所需的基本信息（例如资格证书、数字签名等）。云管理平台的 STS 提供模块可以对用户的身份和权限的验证通过后，利用本地存储的（或者能够获得的）、与用户关联的属性信息，作为请求参数关联的输入属性集进行条件判断，输入属性集满足属性转换规则所指定的条件后进行属性转换，确定相应的输出属性集，以便 STS 提供模块的生成单元可以根据该输出属性集生成目标访问令牌。示例地，与用户关联的属性信息，例如可以包括但不限于基于用户的身份标识、网络 IP 等获得的属性信息，本申请对此不做限定。

下面结合附图及实施例介绍本申请实施例的针对飞地 enclave 实例的云服务访问权限设置方法。

图 4 示出了本申请实施例的针对飞地 enclave 实例的云服务访问权限设置方法的流程示意图。其中，该方法可由第一租户、第二租户、enclave 实例中的应用程序以及图 3 所示

的云管理平台及其功能模块实现。如图 4 所示，该方法可以包括以下步骤：

S410：云管理平台的 IAM 服务确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则。

本申请实施例中，飞地 enclave 实例类型以及转换规则可以是由第一租户自定义配置得到的，转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性，以帮助云管理平台实施对第一租户购买的云资源的集中、安全的访问控制管理。

一种可选的实现方式中，该飞地 enclave 实例类型以及转换规则可以是租户预先自定义配置，并持久化地存储在云管理平台的安全管理服务提供模块关联的存储器中的。实施 S410 时，云管理平台的 IAM 服务提供模块可以在该存储器确认飞地 enclave 实例类型以及转换规则。例如，IAM 服务可以根据第一租户的唯一标识，在该存储器中获取租户的安全管理服务配置信息。

另一种可选的实现方式中，该飞地 enclave 实例类型以及转换规则可以是第一租户实时配置的。实施 S410 时，云管理平台的 IAM 服务提供模块可以实时地接收第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，本申请实施例对该实例类型以及转换规则的确认方式不做限定。详细配置细节可参见上文中结合图 3 介绍的 API 和控制台界面的相关描述，在此不再赘述。

S420：云管理平台的 STS 接收 enclave 实例中的应用程序发送的令牌获取请求，根据转换规则将令牌获取请求中携带的所述 enclave 实例的证明文档转换为租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

本申请实施例中，云管理平台的 STS 提供模块可以向 enclave 实例中的应用程序提供 API。应用程序获得正确的访问凭证（例如访问密钥等）后，可以基于云管理平台提供的安全管理服务以及 STS 提供模块提供的 API，向 STS 提供模块发送令牌获取请求，以向 STS 传入请求参数，该请求参数用于请求获取租户节点订购的目标云服务的 API 的访问令牌。

示例地，该请求参数可以包括但不限于 enclave 实例的证明文档、API 请求者身份标识、API 请求体的数字签名等输入参数。

发放访问令牌的功能可由 STS 提供模块来提供，该 STS 提供模块经过功能扩展后，可以包括验证单元、属性转换单元和生成单元。实施 S420 时，该验证单元可以先根据至少一个属性对象中的元数据对请求参数进行合法性验证，例如验证请求者身份、请求体的数字签名、安全属性证明文档的合法性（例如是否包含指定的属性、属性证明文档的数字签名是否合法、过期时间是否合法）等。如果验证未通过即验证失败，则向用应用程序返回错误提醒。如果验证通过即验证成功，则该请求参数中携带的证明文档的相关属性信息可以作为属性转换单元的输入属性集，该属性转换单元可以利用至少一个属性对象中的转换规则，将该证明文档转换成租户自定义属性，即输出属性集。如果转换失败则向应用程序返回错误提醒。如果转换成功，生成单元可以根据该输出属性集以及预设的算法生成目标访问令牌，该目标访问令牌为携带有租户自定义属性的令牌。进一步，STS 提供模块可以向应用程序发送该目标访问令牌。

一种可选的实现方式中，云管理平台还可以提供 IAM 服务，云管理平台还可以获取第

一租户或者第二租户在云管理平台输入或选择的授权策略，该授权策略用于指示所述第一租户或者第二租户授权所述应用程序访问目标云服务应满足的访问控制条件，在上述实施S420的过程中，云管理平台的STS提供模块可以根据所述授权策略，对所述请求参数进行合法性验证以及访问控制检查。如果合法性验证失败或访问控制检查失败，则STS提供模块可以向应用程序返回错误提醒，并拒绝应用程序的令牌获取请求。详细实施细节可参见上文中结合图3的相关介绍，在此不再赘述。

在S420之后，一个可选的步骤包括：应用程序可以根据从云管理平台获得的目标访问令牌向云服务模块发起服务调用请求，该服务调用请求可以用于请求访问云服务模块的目标云服务。目标云服务可以在本地或者利用与STS提供模块、IAM服务提供模块等之间的信任关系，对该目标访问令牌进行合法性验证以及访问控制检查通过后，云服务模块向应用程序提供目标云服务。详细实施细节可参见上文中结合图3的相关介绍，在此不再赘述。

下面基于图3所示的系统架构，结合图5所示的方法，对图4示出的各个方法步骤进行详细介绍。

如图5所示，第一租户或者第二租户可以实现为与云管理平台的服务提供模块对应的管理模块，例如，安全管理模块和访问控制权限管理模块。

该安全管理模块可以根据云管理平台提供的API向云管理平台的安全管理服务提供模块发送安全管理服务配置信息，该安全管理服务配置信息可以被安全管理服务提供模块接收和保存，用于验证来自APP的请求参数的合法性，以及实施对租户购买的云资源的安全访问控制管理。

该访问控制权限管理模块可以根据云管理平台提供的API向云管理平台的IAM服务提供模块发送授权策略，该授权策略可以被IAM服务提供模块接收和保存，用于验证APP对租户所购买的云服务的操作权限，以及确定APP的访问控制策略。

其中，以租户自定义配置的至少一个属性对象包括安全证明对象为例，该安全证明对象的至少一个属性包括安全属性，该安全属性可以用于云管理平台对来自APP的证明文档（attestation document）进行验证，以便根据APP的可信计算环境或机密计算环境（比如Enclave）来实施更精确的访问控制决策，集中、安全地实现对云资源的管理。

示例地，该安全属性可以包括以下至少一项：硬件标识属性、安全固件版本属性、创建时间属性、程序度量相关属性、数字签名证书相关属性、或者租户自定义的业务安全属性。各个安全属性用于验证来自APP的证明文档的合法性（或称为有效性、可信性等）。其中，硬件标识属性用于指示硬件标识，表示来自用户节点的证明文档需要包括硬件标识属性才有可能是有效的，反之则合法性验证不通过。安全固件版本属性用于指示安全固件版本，表示来自APP的证明文档需要包括安全固件版本才有可能是有效的，反之则合法性验证不通过。创建时间属性用于指示创建时间，表示来自APP的证明文档需要包括创建时间才有可能是有效的，反之则合法性验证不通过。程序度量相关属性用于指示可执行程序的度量相关的属性、例如可信度量算法、可信度量值等，表示来自用户节点的证明文档需要包括可信度量相关信息才有可能是有效的，反之则合法性验证不通过。数字签名证书相关属性表示安全属性证明文档的数字签名证书、证书链等属性，表示来自APP的证明文档需要包括数字签名证书、证书链等信息才有可能是有效的，反之合法性验证不通过。租户

自定义的业务安全属性包括租户自定义的任意业务安全属性，在此不再赘述。

安全管理服务提供模块可以根据来自安全管理模块的安全管理服务配置信息中属性对象描述信息创建相应的属性对象，该属性对象可以包括至少一个属性的元数据和属性转换规则。

IAM 服务提供模块可以根据来自访问控制权限管理模块的授权策略，以及利用 IAM 服务提供模块与安全管理服务提供模块之间的信任关系，确定租户授予不同用户的针对不同云资源的不同访问权限。

用户侧的飞地 enclave APP（运行在机密计算环境中的客户应用程序）作为发起方，可以通过 TEE 操作系统（operating system，OS）接口，调用 TCB 的安全模块，以获取 enclave 机密计算环境的安全属性的证明文档。请求成功后，安全模块会向 Enclave APP 返回有效的证明文档。enclave APP 可以基于该证明文档，调用 STS Get Token API，向云管理平台的 STS 提供模块发送令牌获取请求，以向 STS 提供模块传入请求参数，该请求参数包括 enclave 实例的证明文档、请求者身份标识信息、请求体的数字签名信息等信息，该请求参数用于请求获取 STS 令牌。

云管理平台的 STS 提供模块的验证单元可以根据 IAM 服务提供模块侧配置的授权策略、安全管理服务提供模块侧配置的元数据，对令牌获取请求中携带的请求参数进行合法性验证和权限验证等。在该请求参数的合法性验证以及权限验证通过后，STS 提供模块的属性转换单元可以根据在安全管理服务提供模块的 Enclave 属性相关的转换规则，将证明文档中的相关属性作为输入属性集转换为租户自定义属性，即输出属性集，生成单元可以利用该输出属性集生成有效的目标访问令牌，即携带有租户自定义属性的令牌。之后，STS 提供模块可以向 APP 返回有效的目标访问令牌。

进一步，APP 可以利用从云管理平台获得的目标访问令牌，向云服务模块的目标云服务发送服务调用请求，以请求访问目标云服务。该目标云服务可以利用云管理平台提供的相关服务，对来自 APP 的目标访问令牌进行合法性验证和访问控制检查通过后，允许 APP 访问目标云服务，并向 APP 返回对目标云服务的访问结果。

由此，通过图 5 所示的方法，在对云管理平台的至少一个服务提供模块进行功能扩展后，云服务模块的至少一个云服务无需做任何改造升级（包括 API 改造或 SDK 改造），即可使得云管理平台能够支持基于 APP 的设备运行环境属性的访问控制策略，对云服务 API 没有侵入性，对应用程序生态以及开发者生态均友好。对租户而言，租户编写授权策略更加简单，而无需感知 APP 所在设备运行环境属性的底层语义特征，可以支持不同类型的用户设备特性，可以屏蔽不同类型用户设备的底层语义特征，以极小的设计和实施成本扩大应用场景。

需要说明的是，图 5 中仅是以 enclave 实例和 enclave 实例的证明文档为例，对本申请实施例的云服务访问权限设置方法进行解释说明，并不限定该方法所面向的属性对象为 enclave 实例，该 enclave 实例可以替换为其它类型实例，与 enclave 实例相关的服务配置信息或请求参数可以替换为其它属性，在此不再赘述。

结合上述方法实施例，本申请实施例还提供了一种云管理平台，该云管理平台具体结构可以参照上述图 3 所示，可用于执行上述方法实施例中云管理平台及其各个服务提供模块所执行的方法。

如图 6 所示，该云管理平台 600 可以包括：第一服务提供模块 610，用于提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性；第二服务提供模块 620，用于提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。详细实现细节可参见上述方法实施例的相关介绍，在此不再赘述。

需要说明的是，本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。在本申请的实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

在一个简单的实施例中，本领域的技术人员可以想到上述实施例中的云管理平台或电子端设备均可采用图 7 所示的形式。如图 7 所示的通信装置 700，包括至少一个处理器 710、存储器 720，可选的，还可以包括通信接口 730。

存储器 720 可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）、或者存储器 720 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 720 可以是上述存储器的组合。

本申请实施例中不限定上述处理器 710 以及存储器 720 之间的具体连接介质。

在如图 7 的装置中，还包括通信接口 730，处理器 710 在与其他设备进行通信时，可以通过通信接口 730 进行数据传输。

当云管理平台采用图 7 所示的形式时，图 7 中的处理器 710 可以通过调用存储器 720 中存储的计算机执行指令，使得装置 700 可以执行上述任一方法实施例中云管理平台所执行的方法。

当租户或用户侧电子设备采用图 7 所示的形式时，图 7 中的处理器 710 可以通过调用存储器 720 中存储的计算机执行指令，使得装置 700 可以执行上述任一方法实施例中租户或用户所执行的方法。

本申请实施例还涉及一种芯片系统，该芯片系统包括处理器，用于调用存储器中存储

的计算机程序或计算机指令，以使得该处理器执行上述方法实施例。

在一种可能的实现方式中，该处理器通过接口与存储器耦合。

在一种可能的实现方式中，该芯片系统还包括存储器，该存储器中存储有计算机程序或计算机指令。

本申请实施例还涉及一种处理器，该处理器用于调用存储器中存储的计算机程序或计算机指令，以使得该处理器执行上述方法实施例。

其中，上述任一处提到的处理器，可以是一个通用中央处理器，微处理器，特定应用集成电路（application-specific integrated circuit，ASIC），或一个或多个用于控制上述图 7 所示的实施例中的方法的程序执行的集成电路。上述任一处提到的存储器可以为只读存储器（read-only memory，ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM）等。

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。

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。

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。

显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请实施例范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1.一种针对飞地 enclave 实例的云服务访问权限设置方法，其特征在于，包括:

云管理平台提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性;

所述云管理平台提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

2.根据权利要求 1 所述的方法，其特征在于，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。

3.根据权利要求 2 所述的方法，其特征在于，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

4.根据权利要求 2 或 3 所述的方法，其特征在于，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

5.根据权利要求 1 至 4 任一项所述的方法，其特征在于，所述方法还包括:

所述 enclave 实例中的应用程序在发送所述令牌获取请求之前，从可信计算基 TCB 获取所述 enclave 实例的证明文档。

6.根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述方法还包括:

所述 enclave 实例中的应用程序向所述目标云服务发送服务调用请求，所述服务调用请求携带有所述令牌;

所述目标云服务接收所述服务调用请求，并向所述 STS 确认所述令牌的合法性，在所述 STS 确认所述令牌合法的前提下，所述目标云服务允许所述应用程序访问所述目标云服务。

7.根据权利要求 1 至 6 任一项所述的方法，其特征在于，所述证明文档包括至少一个平台配置寄存器 PCR 度量值。

8.一种云服务系统，其特征在于，包括云管理平台和目标云服务，其中，

所述云管理平台提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性;

所述云管理平台提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向

所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问所述目标云服务的权限。

9.根据权利要求 8 所述的系统，其特征在于，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。

10.根据权利要求 9 所述的系统，其特征在于，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

11.根据权利要求 8 或 9 所述的系统，其特征在于，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

12.根据权利要求 8 至 11 任一项所述的系统，其特征在于，所述 enclave 实例中的应用程序在发送所述令牌获取请求之前，从可信计算基 TCB 获取所述 enclave 实例的证明文档。

13.根据权利要求 8 至 12 任一项所述的系统，其特征在于，所述 enclave 实例中的应用程序向所述目标云服务发送服务调用请求，所述服务调用请求携带有所述令牌；所述目标云服务接收所述服务调用请求，并向所述 STS 确认所述令牌的合法性，在所述 STS 确认所述令牌合法的前提下，所述目标云服务允许所述应用程序访问所述目标云服务。

14.根据权利要求 8 至 13 任一项所述的系统，其特征在于，所述证明文档包括至少一个平台配置寄存器 PCR 度量值。

15.一种云管理平台，其特征在于，包括：

第一服务提供模块，用于提供身份管理与访问控制 IAM 服务，所述 IAM 服务用于确认第一租户输入或选择的飞地 enclave 实例类型以及所述第一租户输入或选择的转换规则，其中，所述转换规则用于将所述飞地 enclave 实例类型对应的 enclave 实例提供的 enclave 实例的证明文档转换成租户自定义属性；

第二服务提供模块，用于提供安全令牌服务 STS，所述 STS 用于接收所述 enclave 实例中的应用程序发送的令牌获取请求，其中，所述令牌获取请求携带有所述 enclave 实例的证明文档，所述 STS 还用于根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌，所述令牌用于指示 enclave 实例中的应用程序具有访问目标云服务的权限。

16.根据权利要求 15 所述的云管理平台，其特征在于，所述 IAM 服务还用于确认所述第一租户或者第二租户输入或选择的授权策略，所述 STS 在满足所述授权策略的条件下根据所述转换规则将所述证明文档转换为所述租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌。

17.根据权利要求 16 所述的云管理平台，其特征在于，所述第一租户的角色为安全管理员，所述第二租户的角色为权限管理员。

18.根据权利要求 16 或 17 所述的云管理平台，其特征在于，所述授权策略包括允许所述应用程序在所述飞地 enclave 实例类型对应的 enclave 实例中访问所述目标云服务。

19.一种云管理平台，其特征在于，包括处理器和存储器，所述存储器存储有程序指令，所述处理器执行所述程序指令以执行权利要求 1 至 7 任一项所述的方法。

20.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质用于存储计算机程序，当所述计算机程序在计算装置上运行时，使得所述计算装置执行如权利要求 1-7 中任一所述的方法。