(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 12 月 1 日 (01.12.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/247359 A1

(51) 国际专利分类号:
G06F 21/44 (2013.01)

(21) 国际申请号: PCT/CN2022/076922

(22) 国际申请日: 2022 年 2 月 18 日 (18.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110606924.6 2021年5月27日 (27.05.2021) CN

(71) 申请人: 北京百度网讯科技有限公司 (**BEIJING BAIDU NETCOM SCIENCE TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市海淀区上地十街 10 号百度大厦 2 层, Beijing 100085 (CN)。

(72) 发明人: **林战波 (LIN, Zhanbo)**; 中国北京市海淀区上地十街 10 号百度大厦 2 层, Beijing 100085 (CN)。

(74) 代理人: 北京品源专利代理有限公司 (**BEYOND ATTORNEYS AT LAW**); 中国北京市海淀区莲花池东路39号西金大厦6层, Beijing 100036 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) **Title:** CLUSTER ACCESS METHOD AND APPARATUS, ELECTRONIC DEVICE, AND MEDIUM

(54) **发明名称**: 集群访问方法、装置、电子设备和介质

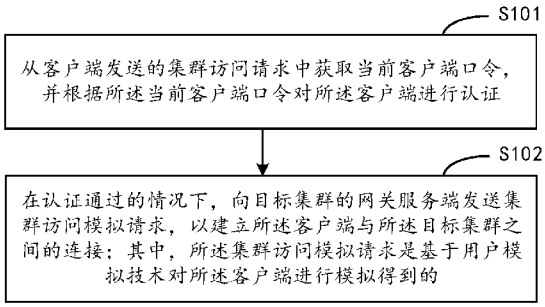


图 1

S101 Obtain a current client password from a cluster access request sent by a client, and authenticate the client according to the current client password

S102 When the authentication is successful, send a cluster access simulation request to a gateway server of a target cluster so as to establish a connection between the client and the target cluster, wherein the cluster access simulation request is obtained by simulating the client on the basis of a user simulation technology

(57) **Abstract:** Disclosed are a cluster access method and apparatus, an electronic device, and a medium. The cluster access method comprises: obtaining a current client password from a cluster access request sent by a client, and authenticating the client according to the current client password; and when the authentication is successful, sending a cluster access simulation request to a gateway server of a target cluster so as to establish a connection between the client and the target cluster, wherein the cluster access simulation request is obtained by simulating the client on the basis of a user simulation technology.

(57) **摘要**: 本文公开一种集群访问方法、装置、电子设备和介质。集群访问方法包括：从客户端发送的集群访问请求中获取当前客户端口令，并根据当前客户端口令对客户端进行认证；在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立客户端与目标集群之间的连接；其中，集群访问模拟请求是基于用户模拟技术对客户端进行模拟得到的。

WO 2022/247359 A1

[见续页]

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

集群访问方法、装置、电子设备和介质

本申请要求在2021年05月27日提交中国专利局、申请号为202110606924.6的中国专利申请的优先权，该申请的全部内容通过引用结合在本申请中。

技术领域

本公开涉及计算机技术领域，涉及容器技术、云计算及云服务技术领域，例如涉及一种集群访问方法、装置、电子设备和介质。

背景技术

随着 Kubernetes 技术的发展，实现了公共云和私有云内不同的基础设施之间可以无障碍地沟通。主流的沟通方法是通过云服务商将不同地区的 Kubernetes 集群统一纳管。

在一个客户端想要访问 Kubernetes 集群之前，通常需要通过集群的网关服务端对该客户端进行认证。

发明内容

本公开提供了一种用于客户端与集群之间建立连接的方法、装置、电子设备和介质。

根据本公开的一方面，提供了一种集群访问方法，包括：

从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证；

在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

根据本公开的另一方面，提供了一种集群访问装置，包括：

认证模块，设置为从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证；

通信连接模块，设置为在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

根据本公开的另一方面，提供了一种电子设备，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行上述的集群访问方法。

根据本公开的另一方面，提供了一种存储有计算机指令的非瞬时计算机可读存储介质，其中，所述计算机指令用于使所述计算机执行上述的集群访问方法。

根据本公开的另一方面，提供了一种计算机程序产品，包括计算机程序，所述计算机程序在被处理器执行时实现上述的集群访问方法。

附图说明

图 1 是根据本公开实施例公开的一种集群访问方法的流程图；

图 2 是根据本公开实施例公开的另一种集群访问方法的流程图；

图 3 是根据本公开实施例公开的一种集群访问装置的结构示意图；

图 4 是用来实现本公开实施例公开的集群访问方法的电子设备的框图。

具体实施方式

以下结合附图对本公开的示范性实施例做出说明，其中包括本公开实施例的多种细节以助于理解，应当将它们认为仅仅是示范性的。为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

集群访问过程中，客户端直接向目标集群的网关服务端发送集群访问请求，网关服务端通过 OpenID Connect 方案来对客户端进行认证。但是默认情况下网关服务端并未开启对于 OpenID Connect 方案的支持，因此需要首先在网关服务端配置 OpenID Connect 方案参数才能够开启。

然而由于需要在网关服务端进行参数配置，这就造成了对网关服务端的侵入，改变了网关服务端的运行环境，而网关服务端又是构建外界与集群之间连接的桥梁，因此这无疑加大了集群的安全风险，降低了集群的安全性。

图 1 是根据本公开实施例公开的一种集群访问方法的流程图，本实施例可以适用于客户端与集群之间建立连接的情况。本实施例方法可以由本公开实施例公开的集群访问装置来执行，所述装置可采用软件和/或硬件实现，并可集成在任意的具有计算能力的电子设备上。

如图 1 所示，本实施例公开的集群访问方法可以包括：

S101、从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证。

客户端表示想要访问目标集群的用户所使用的用户端设备，其可以是智能设备中安装的软件，也可以是网页浏览器，本实施例并不对客户端的形式进行限定。集群表示实现相同业务功能的设备的集合，例如本实施例中的集群可选的包括 Kubernetes 集群，即一组运行容器化应用程序的节点计算机。

在一种实施方式中，客户端通过代理服务端预先暴露的地址信息，例如统一资源定位器（Uniform Resource Locator，URL）地址，向代理服务端发送针对目标集群的集群访问请求。代理服务端获取到集群访问请求后对集群访问请求进行解析，确定集群访问请求中是否包含有当前客户端口令。若集群访问请求中没有包含当前客户端口令，则代理服务端立即拒绝客户端对于目标集群的访问；若集群访问请求中包含当前客户端口令，则代理服务端确定当前客户端口令的有效期，进而确定当前客户端口令是否过期。若当前客户端口令过期，则代理服务端拒绝客户端对于目标集群的访问；若当前客户端口令未过期，则代理服务端根据当前客户端口令对客户端进行认证，认证的方式包括但不限于如下的至少一种实现方式：

1）客户端将当前客户端口令通过私钥进行加密，并根据加密后的当前客户端口令生成集群访问请求并发送给代理服务端，代理服务端采用公钥对加密后的当前客户端口令进行解密，若解密得到的当前客户端口令与预先向客户端颁发的标准客户端口令相同，则对客户端的认证通过。

2)客户端将自身的标准客户端标识作为干扰码对当前客户端口令进行加密，并根据加密后的当前客户端口令生成集群访问请求并发送给代理服务端，代理服务端通过客户端的当前客户端标识对加密后的当前客户端口令进行解密，若可以解密成功，则对客户端的认证通过。

3）客户端授权代理服务端获取客户端的标准客户端信息，代理服务端根据标准客户端信息生成标准客户端口令并返回给客户端。客户端将携带有当前客户端口令的集群访问请求发送给代理服务端，代理服务端解析当前客户端口令得到当前客户端信息，并基于当前客户端信息与标准客户端信息进行比对，若比对成功则对客户端认证通过。

本实施例并不对根据当前客户端口令对客户端进行认证的实现方式进行限定，凡是基于客户端口令的身份认证方式均处于本实施例的保护范围内。

通过从客户端发送的集群访问请求中获取当前客户端口令，并根据当前客户端口令对客户端进行认证，实现了基于代理服务端对客户端的认证，保

证了客户端访问集群的安全性。

S102、在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

在一种实施方式中，当代理服务端对客户端认证通过后，采用用户模拟技术对客户端进行模拟，生成客户端对于目标集群的集群访问模拟请求，其中，用户模拟技术即 User Impersonation 技术，是一个用户模拟另一个用户进行相关操作的技术，在本实施例中即代理服务端模拟客户端向目标集群的网关服务端发送集群访问请求。代理服务端将生成的集群访问模拟请求发送给目标集群的网关服务端，由于集群访问模拟请求是基于用户模拟技术对客户端进行模拟得到的，所以从网关服务端一侧来看，等效于真实的客户端向网关服务端发送集群访问请求，从而网关服务端响应于集群访问模拟请求，向客户端暴露一个外部可访问的指定端口，以使得客户端基于该指定端口访问目标集群。

通过在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立客户端与目标集群之间的连接，实现了模拟客户端向网关服务端发送集群访问请求的效果,使得在代理服务端对客户端认证通过的情况下，能够建立客户端与目标集群之间的连接。

本公开通过从客户端发送的集群访问请求中获取当前客户端口令，并根据当前客户端口令对客户端进行认证，从而将客户端认证过程依托于代理服务端执行，而无需在网关服务端执行，避免了相关技术中由网关服务端进行客户端认证，存在侵入网关服务端，导致集群存在安全风险的问题，提高了集群的安全性；通过代理服务端基于用户模拟技术模拟客户端向网关服务端发送集群访问请求，保证了即使是由代理服务端本身发送的集群访问模拟请求，同样可以实现建立客户端与集群之间连接的效果，使得客户端对于目标集群的访问能够顺利进行。

在上述实施例的基础上，还包括：

根据用户对目标集群的权限配置操作，确定所述目标集群的待更新权限信息；根据所述待更新权限信息控制所述目标集群进行权限信息的更新。

权限信息表示集群权限的相关属性信息，其包括但不限于权限规则以及被授权人信息，权限规则即定义了集群中权限的内容，例如“访问 A 命名空间”权限或“修改 A 命名空间”权限等等，而被授权人信息表示任一权限规则适用的对象，例如将权限规则 A 赋予给用户 A，那么用户 A 就是权限规则 A

的被授权人。

在一种实施方式中，代理服务端与多个纳管集群之间通信连接，用户在代理服务端对应前端中对目标集群的权限信息进行配置，代理服务端则响应于用户在前端的权限配置操作，确定目标集群的待更新权限信息，并控制纳管的目标集群将当前权限信息更新为待更新权限信息。

示例性的，以集群为 Kubernetes 集群为例对上述实施方式进行解释说明。

用户在代理服务端对应的前端对目标 Kubernetes 集群进行权限信息配置，包括但不限于“Role”配置、“ClusterRole”配置、“Rolebinding”配置和“Cluster Rolebinding”配置等，其中，“Role”表示任一 Kubernetes 集群中针对一命名空间的权限规则，“ClusterRole”表示任一 Kubernetes 集群本身的权限规则，“Rolebinding”表示任一 Kubernetes 集群中任一“Role”对应的被授权人信息，“Cluster Rolebinding”表示任一 Kubernetes 集群中任一“ClusterRole”的被授权人信息。代理服务端根据用户的权限配置操作，确定更新后的“Role”、“ClusterRole”、“Rolebinding”和“Cluster Rolebinding”中的至少一种权限信息，并相应的控制目标 Kubernetes 集群进行权限信息的更新。例如若用户在前端对目标 Kubernetes 集群的“Role”进行了配置，则代理服务端相应的将配置后的“Role”同步更新到目标 Kubernetes 集群中。

通过根据用户对目标集群的权限配置操作，确定目标集群的待更新权限信息，根据待更新权限信息控制目标集群进行权限信息的更新，实现了基于代理服务端对集群权限信息的统一管理，提高了集群权限信息管理的效率。

图 2 是根据本公开实施例公开的另一种集群访问方法的流程图，基于上述技术方案进行扩展，并可以与上述可选实施方式进行结合。

如图 2 所示，本实施例公开的集群访问方法可以包括：

S201、根据客户端发送的访问配置文件获取请求，获取客户端的标准客户端信息。

访问配置文件是客户端访问集群所需的一种证书，每个客户端访问集群都需要基于访问配置文件来实现。访问配置文件需要客户端向权威方申请才能得到。标准客户端信息即客户端的一些私有信息，例如客户端名称和客户端状态等。

在一种实施方式中，客户端根据代理服务端暴露的地址信息向代理服务端发送访问配置文件获取请求。代理服务端根据访问配置文件获取请求，向客户端申请获取标准客户端信息，在客户端授权的情况下，获取客户端的标

准客户端信息。

示例性的，本实施例提供了一种真实场景中 S201 的实现方式。

用户登录浏览器，并在浏览器中输入代理服务端的地址信息以向代理服务端发送访问配置文件获取请求。代理服务端将访问配置文件获取请求转发给身份服务组件，身份服务组件根据预设的授权协议，例如开放授权 2.0（Open Authorization 2.0，OAuth2.0）协议等，控制浏览器跳转显示个人信息授权界面。用户在浏览器的个人信息授权界面中执行个人信息授权操作，包括但不限于根据账号密码授权、根据二维码授权或者根据验证码授权等等。当用户对个人信息授权后，身份服务组件从浏览器关联的第三方服务端中获取用户个人信息。

S202、根据标准客户端信息生成标准客户端口令，并根据标准客户端口令生成标准访问配置文件。

在一种实施方式中，采用预设编码技术，例如 Base64 编码等，对标准客户端信息进行编码，生成荷载信息；同样采用编码技术对标准客户端口令类型信息以及签名算法信息进行编码，生成头部信息；采用签名算法对荷载信息和头部信息进行加密，生成签名信息；最终根据头部信息、荷载信息和签名信息生成标准客户端口令。根据标准客户端口令生成包含该标准客户端口令的标准访问配置文件。

S203、将标准访问配置文件发送给客户端。

在一种实施方式中，代理服务端将生成的标准访问配置文件反馈给客户端，以使得客户端后续通过包含有标准访问配置文件的集群访问请求，进行集群访问。

S204、从客户端发送的集群访问请求中获取客户端的当前访问配置文件，并对当前访问配置文件进行解析确定当前客户端口令。

在一种实施方式中，客户端向代理服务端发送包含当前客户端口令的当前访问配置文件，代理服务端对当前访问配置文件进行解析，从预设字段区域间中提取出当前客户端口令。

在客户端通过集群访问请求进行集群访问时，该集群访问请求中的当前访问配置文件不一定是客户端在 S203 中获得的标准访问配置文件，因此，代理服务端需要对集群访问请求中的当前访问配置文件进行解析以及验证，确保客户端是在通过包含有标准访问配置文件的集群访问请求进行集群访问。

S205、根据当前客户端口令确定客户端的当前客户端信息，并根据当前客户端信息对客户端进行认证。

在一种实施方式中，代理服务端获取当前客户端口令后，首先对当前客户端口令的荷载信息部分进行解码得到口令过期时间，并基于当前时间和口令过期时间确定当前客户端口令是否过期，若当前客户端口令未过期，则取出当前客户端口令中的荷载信息和头部信息，再计算一次签名信息，并将计算出的签名信息与当前客户端口令中的签名信息比较，若计算出的签名信息与当前客户端口令中的签名信息一致，则对荷载信息进行解码得到当前客户端信息。进而根据当前客户端信息对客户端进行认证，认证的方式包括但不限于：1）将当前客户端信息与标准客户端信息进行比对，若当前客户端信息与标准客户端信息一致则确定客户端合法，即对客户端的认证通过。2）通过数据接口从第三方服务端获取当前客户端信息对应的客户端状态，并根据客户端状态对客户端进行认证，例如若确定客户端状态为异常状态，则对客户端的认证不通过。

S206、在认证通过的情况下，根据集群访问请求，确定目标集群。

在一种实施方式中，代理服务端根据集群访问请求中包含的目标集群标识，确定目标集群。在本实施例中，多个客户端都将各自的集群访问请求发送至代理服务端中，因此每个客户端在集群访问请求中添加目标集群标识，以使得代理服务端根据目标集群标识确定每个集群访问请求对应的目标集群。

S207、确定目标集群是否处于异常状态；其中，异常状态包括失联异常状态和健康值异常状态中的至少一种，并在目标集群未处于异常状态的情况下，向目标集群的网关服务端发送集群访问模拟请求。

失联异常状态表示集群断开了与网关服务端之间的连接，健康值异常状态表示集群的一些指标数据异常，例如中央处理单元（Central Processing Unit，CPU）占用率过高或者可用内存剩余过小等等。

在一种实施方式中，代理服务器通过 List-watch 的方式定时检查每个集群的连接状态和健康值，若确定目标集群处于异常状态时，则停止向目标集群的网关服务端发送集群访问模拟请求。若目标集群未处于异常状态，则向目标集群的网关服务端发送集群访问模拟请求。网关服务端根据接收到的集群访问模拟请求，建立与客户端之间的连接。

本公开通过根据客户端发送的访问配置文件获取请求，获取客户端的标准客户端信息，根据标准客户端信息生成标准客户端口令，并根据标准客户端口令生成标准访问配置文件，将标准访问配置文件发送给客户端，为后续客户端根据标准访问配置文件对目标集群进行访问奠定了基础，保证集群访问的顺利进行；通过从集群访问请求中获取客户端的当前访问配置文件，并对当前访问配置文件进行解析确定当前客户端口令，为后续根据当前客户端

口令对客户端进行认证奠定了基础；通过根据当前客户端口令确定客户端的当前客户端信息，并根据当前客户端信息对客户端进行认证，实现了对客户端进行认证的效果，提高了集群访问的安全性；通过根据集群访问请求，确定目标集群，实现了确定每个客户端想要访问的目标集群的效果，为后续向目标集群发送集群访问模拟请求奠定了基础；通过确定目标集群是否处于异常状态；其中，异常状态包括失联异常状态和健康值异常状态中的至少一种，并在目标集群未处于异常状态的情况下，向目标集群的网关服务端发送集群访问模拟请求，保证了目标集群能够正常访问，避免了客户端无法访问目标集群的问题。

本公开的技术方案中，所涉及的用户个人信息的获取，存储和应用等，均符合相关法律法规的规定，且不违背公序良俗。

图 3 是根据本公开实施例公开的一种集群访问装置的结构示意图，可以适用于客户端与集群之间建立连接的情况。本实施例装置可采用软件和/或硬件实现，并可集成在任意的具有计算能力的电子设备上。

如图 3 所示，本实施例公开的集群访问装置 30 可以包括认证模块 31 和通信连接模块 32，其中：

认证模块 31，设置为从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证；通信连接模块 32，设置为在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

可选的，所述装置还包括目标集群确定模块，设置为：

根据所述集群访问请求，确定所述目标集群。

可选的，所述认证模块 31 设置为通过如下方式从客户端发送的集群访问请求中获取当前客户端口令：

从所述集群访问请求中获取所述客户端的当前访问配置文件，并对所述当前访问配置文件进行解析确定所述当前客户端口令。

可选的，所述装置还包括访问配置文件发送模块，设置为：

根据所述客户端发送的访问配置文件获取请求，获取所述客户端的标准客户端信息；根据所述标准客户端信息生成标准客户端口令，并根据所述标准客户端口令生成标准访问配置文件；将所述标准访问配置文件发送给所述

客户端。

可选的,所述认证模块31设置为通过如下方式根据所述客户端口令对所述客户端进行认证:

根据所述当前客户端口令确定所述客户端的当前客户端信息，并根据所述当前客户端信息对所述客户端进行认证。

可选的，所述装置还包括异常状态判断模块，设置为:

确定所述目标集群是否处于异常状态；其中，所述异常状态包括失联异常状态和健康值异常状态中的至少一种;所述通信连接模块32设置为通过如下方式向目标集群的网关服务端发送集群访问模拟请求：在所述目标集群未处于异常状态的情况下，向所述目标集群的所述网关服务端发送所述集群访问模拟请求。

可选的，所述装置还包括权限信息更新模块，设置为:

根据用户对目标集群的权限配置操作，确定所述目标集群的待更新权限信息；根据所述待更新权限信息控制所述目标集群进行权限信息的更新。

本公开实施例所公开的集群访问装置 30 可执行本公开实施例所公开的集群访问方法，具备执行方法相应的功能模块和效果。本实施例中未详尽描述的内容可以参考本公开任意方法实施例中的描述。

根据本公开的实施例，本公开还提供了一种电子设备、一种可读存储介质和一种计算机程序产品。

图4示出了可以用来实施本公开的实施例的示例电子设备400的示意性框图。电子设备400旨在表示多种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备400还可以表示多种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或者要求的本公开的实现。

如图4所示，设备400包括计算单元401，其可以根据存储在只读存储器（Read-Only Memory，ROM）402中的计算机程序或者从存储单元408加载到随机访问存储器（Random Access Memory，RAM）403中的计算机程序，来执行多种适当的动作和处理。在RAM 403中，还可存储设备400操作所需的多种程序和数据。计算单元401、ROM 402以及RAM 403通过总线404

彼此相连。输入/输出（Input/Output，I/O）接口 405 也连接至总线 404。

设备 400 中的多个部件连接至 I/O 接口 405，包括：输入单元 406，例如键盘、鼠标等；输出单元 407，例如多种类型的显示器、扬声器等；存储单元 408，例如磁盘、光盘等；以及通信单元 409，例如网卡、调制解调器、无线通信收发机等。通信单元 409 允许设备 400 通过诸如因特网的计算机网络和/或多种电信网络与其他设备交换信息/数据。

计算单元 401 可以是多种具有处理和计算能力的通用和/或专用处理组件。计算单元 401 的一些示例包括但不限于 CPU、图形处理单元（Graphics Processing Unit，GPU）、多种专用的人工智能（Artificial Intelligence，AI）计算芯片、多种运行机器学习模型算法的计算单元、数字信号处理器（Digital Signal Processing，DSP）、以及任何适当的处理器、控制器、微控制器等。计算单元 401 执行上文所描述的方法和处理，例如集群访问方法。例如，在一些实施例中，集群访问方法可被实现为计算机软件程序，其被有形地包含于机器可读介质，例如存储单元 408。在一些实施例中，计算机程序的部分或者全部可以经由 ROM 402 和/或通信单元 409 而被载入和/或安装到设备 400 上。当计算机程序加载到 RAM 403 并由计算单元 401 执行时，可以执行上文描述的集群访问方法的一个或多个步骤。备选地，在其他实施例中，计算单元 401 可以通过其他任何适当的方式（例如，借助于固件）而被配置为执行集群访问方法。

本文中以上描述的系统和技术的多种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列（Field Programmable Gate Array，FPGA）、专用集成电路（Application Specific Integrated Circuit，ASIC）、专用标准产品（Application Specific Standard Parts，ASSP）、芯片上的系统（System on Chip，SoC）、复杂可编程逻辑设备（Complex Programmable Logic Device，CPLD）、计算机硬件、固件、软件、和/或它们的组合中实现。多种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

用于实施本公开的方法的程序代码可以采用一个或多个编程语言的任何组合来编写。这些程序代码可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器或控制器，使得程序代码当由处理器或控制器执行时使流程图和/或框图中所规定的功能/操作被实施。程序代码可以完全在机

器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

在本公开的上下文中，机器可读介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。机器可读存储介质的示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、RAM、ROM、可擦除可编程只读存储器（Erasable Programmable Read-Only Memory，EPROM 或快闪存储器）、光纤、便捷式紧凑盘只读存储器（Compact Disc Read-Only Memory，CD-ROM）、光学储存设备、磁储存设备、或上述内容的任何合适组合。

为了提供与用户的交互，可以在计算机上实施此处描述的系统和技术，该计算机具有：设置为向用户显示信息的显示装置（例如，阴极射线管（Cathode Ray Tube，CRT）或者液晶显示器（Liquid Crystal Display，LCD）监视器）；以及键盘和指向装置（例如，鼠标或者轨迹球），用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以设置为提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈（例如，视觉反馈、听觉反馈、或者触觉反馈）；并且可以用任何形式（包括声输入、语音输入或者、触觉输入）来接收来自用户的输入。

可以将此处描述的系统和技术实施在包括后台部件的计算系统（例如，作为数据服务器）、或者包括中间件部件的计算系统（例如，应用服务器）、或者包括前端部件的计算系统（例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互）、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信（例如，通信网络）来将系统的部件相互连接。通信网络的示例包括：局域网（Local Area Network，LAN）、广域网（Wide Area Network，WAN）、区块链网络和互联网。

计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，又称为云计算服务器或云主机，是云计算服务体系中的一项主机产品，以解决了传统物理主机与虚拟专用服务器（Virtual Private Server，VPS）

服务中，存在的管理难度大，业务扩展性弱的缺陷。服务器也可以为分布式系统的服务器，或者是结合了区块链的服务器。

可以使用上面所示的多种形式的流程，重新排序、增加或删除步骤。例如，本公开中记载的多个步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本公开公开的技术方案所期望的结果，本文在此不进行限制。

权 利 要 求 书

1. 一种集群访问方法，包括：

从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证；

在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

2. 根据权利要求 1 所述的方法，在所述向目标集群的网关服务端发送集群访问模拟请求之前，还包括：

根据所述集群访问请求，确定所述目标集群。

3. 根据权利要求 1 所述的方法，其中，所述从客户端发送的集群访问请求中获取当前客户端口令，包括：

从所述集群访问请求中获取所述客户端的当前访问配置文件，并对所述当前访问配置文件进行解析确定所述当前客户端口令。

4. 根据权利要求 1 所述的方法，在所述从客户端发送的集群访问请求中获取当前客户端口令之前，还包括：

根据所述客户端发送的访问配置文件获取请求，获取所述客户端的标准客户端信息；

根据所述标准客户端信息生成标准客户端口令，并根据所述标准客户端口令生成标准访问配置文件；

将所述标准访问配置文件发送给所述客户端，以使所述客户端通过包含所述标准访问配置文件的集群访问请求进行集群访问。

5. 根据权利要求 1 所述的方法，其中，所述根据所述当前客户端口令对所述客户端进行认证，包括：

根据所述当前客户端口令确定所述客户端的当前客户端信息，并根据所述当前客户端信息对所述客户端进行认证。

6. 根据权利要求 1 所述的方法，在所述认证通过之后，所述向目标集群的网关服务端发送集群访问模拟请求之前，还包括：

确定所述目标集群是否处于异常状态；其中，所述异常状态包括失联异常状态和健康值异常状态中的至少一种；

所述向目标集群的网关服务端发送集群访问模拟请求，包括：

在所述目标集群未处于异常状态的情况下，向所述目标集群的所述网关服务端发送所述集群访问模拟请求。

7. 根据权利要求 1 所述的方法，还包括：

根据用户对所述目标集群的权限配置操作，确定所述目标集群的待更新权限信息；

根据所述待更新权限信息控制所述目标集群进行权限信息的更新。

8. 一种集群访问装置，包括：

认证模块，设置为从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证；

通信连接模块，设置为在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的。

9. 根据权利要求 8 所述的装置，还包括目标集群确定模块，设置为：

根据所述集群访问请求，确定所述目标集群。

10. 根据权利要求 8 所述的装置，其中，所述认证模块设置为通过如下方式从客户端发送的集群访问请求中获取当前客户端口令：

从所述集群访问请求中获取所述客户端的当前访问配置文件，并对所述当前访问配置文件进行解析确定所述当前客户端口令。

11. 根据权利要求 8 所述的装置，还包括访问配置文件发送模块，设置为：

根据所述客户端发送的访问配置文件获取请求，获取所述客户端的标准客户端信息；

根据所述标准客户端信息生成标准客户端口令，并根据所述标准客户端口令生成标准访问配置文件；

将所述标准访问配置文件发送给所述客户端，以使所述客户端通过包含所述标准访问配置文件的集群访问请求进行集群访问。

12. 根据权利要求 8 所述的装置，其中，所述认证模块设置为通过如下方式根据所述客户端口令对所述客户端进行认证：

根据所述当前客户端口令确定所述客户端的当前客户端信息，并根据所述当前客户端信息对所述客户端进行认证。

13. 根据权利要求 8 所述的装置，还包括异常状态判断模块，设置为：

确定所述目标集群是否处于异常状态；其中，所述异常状态包括失联异常状态和健康值异常状态中的至少一种；

所述通信连接模块设置为通过如下方式向目标集群的网关服务端发送集群访问模拟请求：

在所述目标集群未处于异常状态的情况下，向所述目标集群的所述网关服务端发送所述集群访问模拟请求。

14. 根据权利要求 8 所述的装置，其中，所述装置还包括权限信息更新模块，设置为：

根据用户对所述目标集群的权限配置操作，确定所述目标集群的待更新权限信息；

根据所述待更新权限信息控制所述目标集群进行权限信息的更新。

15. 一种电子设备，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1-7 中任一项所述的集群访问方法。

16. 一种存储有计算机指令的非瞬时计算机可读存储介质，其中，所述计算机指令用于使所述计算机执行根据权利要求 1-7 中任一项所述的集群访问方法。

17. 一种计算机程序产品，包括计算机程序，所述计算机程序在被处理器执行时实现根据权利要求 1-7 中任一项所述的集群访问方法。

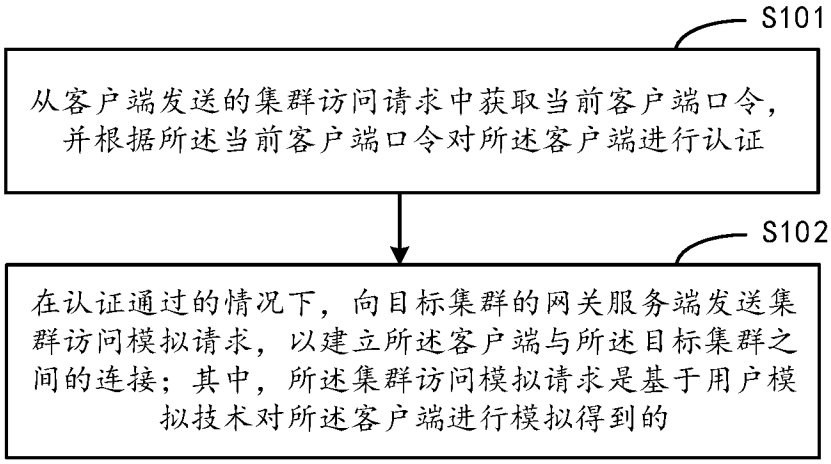

S101
从客户端发送的集群访问请求中获取当前客户端口令，并根据所述当前客户端口令对所述客户端进行认证
S102
在认证通过的情况下，向目标集群的网关服务端发送集群访问模拟请求，以建立所述客户端与所述目标集群之间的连接；其中，所述集群访问模拟请求是基于用户模拟技术对所述客户端进行模拟得到的

图 1

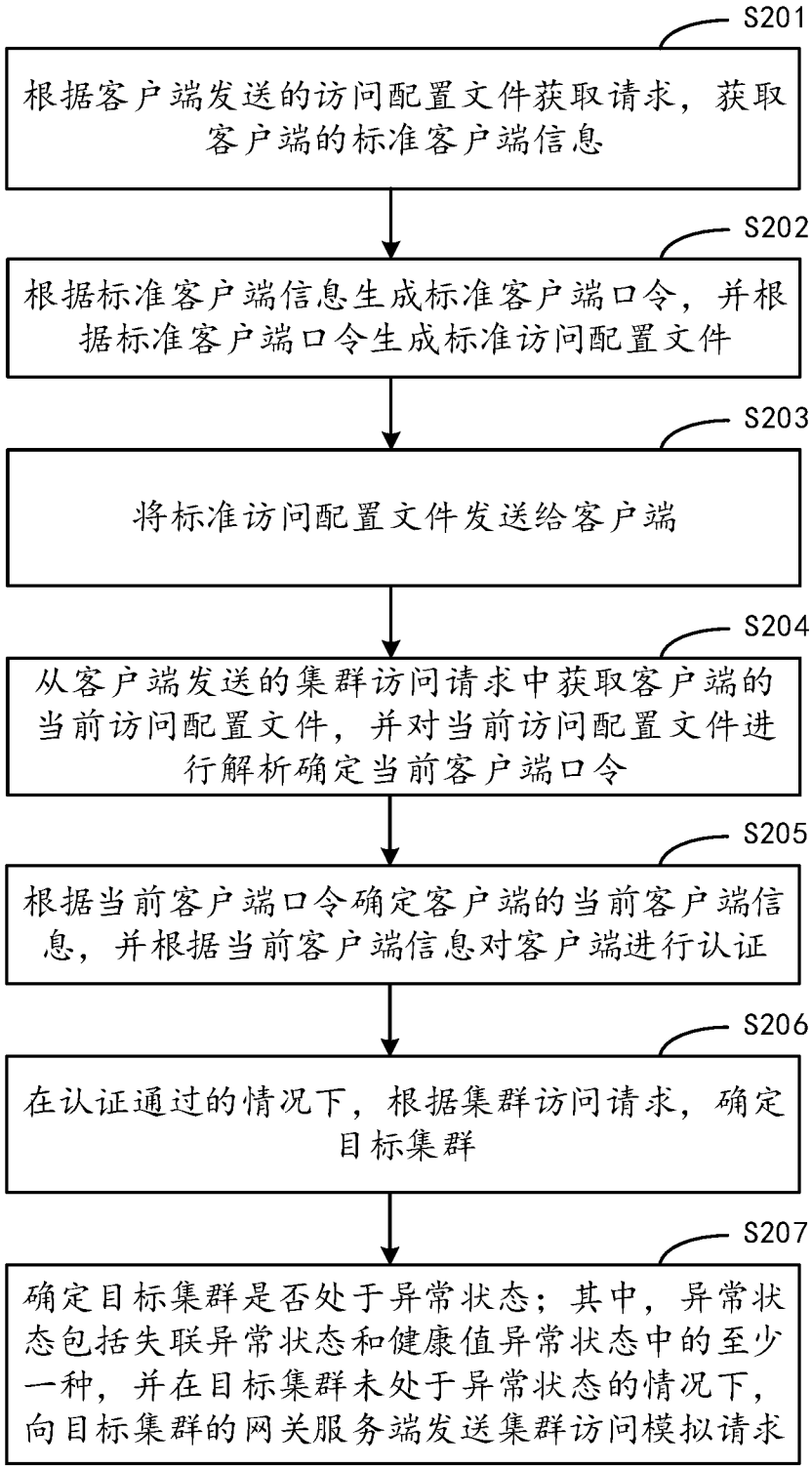

S201
根据客户端发送的访问配置文件获取请求，获取客户端的标准客户端信息
S202
根据标准客户端信息生成标准客户端口令，并根据标准客户端口令生成标准访问配置文件
S203
将标准访问配置文件发送给客户端
S204
从客户端发送的集群访问请求中获取客户端的当前访问配置文件，并对当前访问配置文件进行解析确定当前客户端口令
S205
根据当前客户端口令确定客户端的当前客户端信息，并根据当前客户端信息对客户端进行认证
S206
在认证通过的情况下，根据集群访问请求，确定目标集群
S207
确定目标集群是否处于异常状态；其中，异常状态包括失联异常状态和健康值异常状态中的至少一种，并在目标集群未处于异常状态的情况下，向目标集群的网关服务端发送集群访问模拟请求

图 2

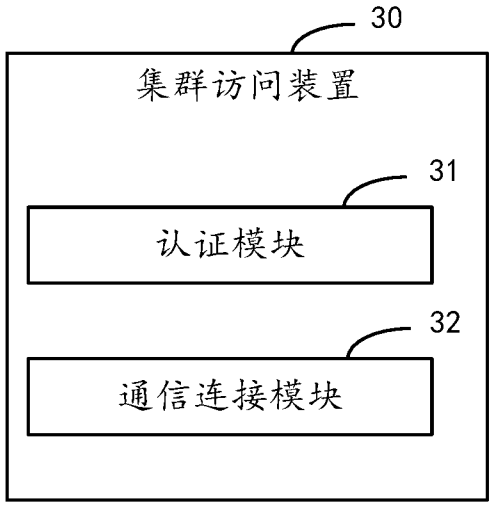

30
集群访问装置
31
认证模块
32
通信连接模块

图 3

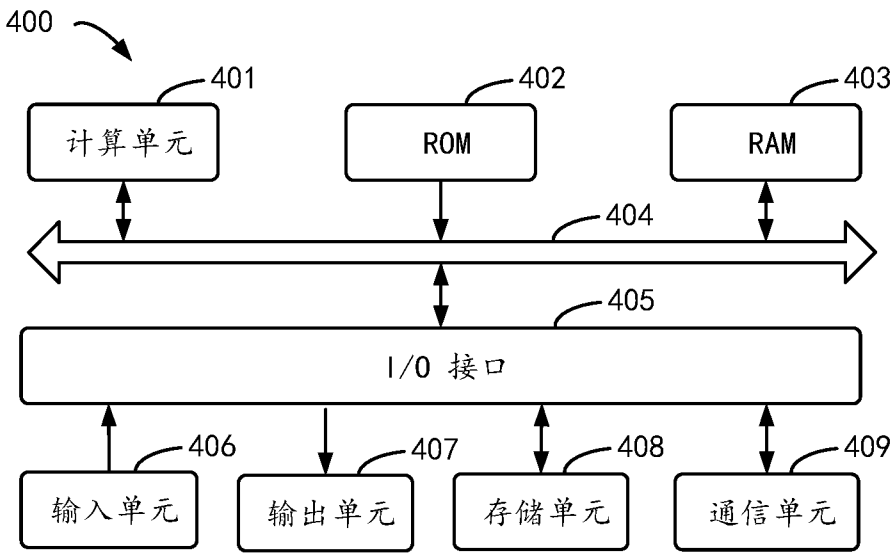

400
401
计算单元
402
ROM
403
RAM
404
405
I/O 接口
406
输入单元
407
输出单元
408
存储单元
409
通信单元

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/076922

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; CNABS; USTXT; WOTXT; EPTXT; VEN; DWPI; CNKI: kubernete集群, 访问, 服务, 请求, 客户端, 用户, 口令, 认证, 验证, 配置, 模拟, 健康, 异常, 状态, kubernete-cluster, access, service, request, client, user, password, authentication, verification, configuration , simulation, health, abnormal, state

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113360882 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 07 September 2021 (2021-09-07) claims 1-17, and description, paragraphs 28-96	1-17
Y	CN 111796858 A (KINGDEE SOFTWARE (CHINA) CO., LTD.) 20 October 2020 (2020-10-20) description, paragraphs 44-120	1-17
Y	CN 111212077 A (CHINA CONSTRUCTION BANK CORP. et al.) 29 May 2020 (2020-05-29) description, paragraphs 43-44	1-17
Y	CN 111510444 A (SHANGHAI YUNLI TECHNOLOGY CO., LTD.) 07 August 2020 (2020-08-07) description, paragraphs 59-75	1-17
Y	CN 112468442 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 09 March 2021 (2021-03-09) description, paragraphs 51-85	3-5, 10-12

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 April 2022	**28 April 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2020351332 A1 (KONG INC.) 05 November 2020 (2020-11-05) description, paragraphs 46-90	6, 7, 13, 14
Y	CN 110971646 A (ZHEJIANG UNIVERSITY) 07 April 2020 (2020-04-07) claims 1-16	6, 7, 13, 14
A	CN 111935110 A (BEIJING KINGSOFT CLOUD NETWORK TECHNOLOGY CO., LTD.) 13 November 2020 (2020-11-13) entire document	1-17
A	CN 110175077 A (LANGCHAO CLOUD INFORMATION TECHNOLOGY CO., LTD.) 27 August 2019 (2019-08-27) entire document	1-17

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/076922

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	113360882	A	07 September 2021	None	
CN	111796858	A	20 October 2020	None	
CN	111212077	A	29 May 2020	None	
CN	111510444	A	07 August 2020	None	
CN	112468442	A	09 March 2021	None	
US	2020351332	A1	05 November 2020	None	
CN	110971646	A	07 April 2020	None	
CN	111935110	A	13 November 2020	None	
CN	110175077	A	27 August 2019	None	

国际检索报告

国际申请号
PCT/CN2022/076922

A. 主题的分类

G06F 21/44(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F21

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNTXT;CNABS;USTXT;WOTXT;EPTXT;VEN;DWPI;CNKI; kubernete集群，访问，服务，请求，客户端，用户，口令，认证，验证，配置，模拟，健康，异常，状态，kubernete-cluster，access，service，request，client、user，password，authentication，verification，configuration ，simulation，health，abnormal，state

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 113360882 A (北京百度网讯科技有限公司) 2021年9月7日 (2021-09-07) 权利要求1-17，说明书第28-96段	1-17
Y	CN 111796858 A (金蝶软件中国有限公司) 2020年10月20日 (2020-10-20) 说明书第44-120段	1-17
Y	CN 111212077 A (中国建设银行股份有限公司 等) 2020年5月29日 (2020-05-29) 说明书第43-44段	1-17
Y	CN 111510444 A (上海云励科技有限公司) 2020年8月7日 (2020-08-07) 说明书第59-75段	1-17
Y	CN 112468442 A (苏州浪潮智能科技有限公司) 2021年3月9日 (2021-03-09) 说明书第51-85段	3-5、10-12
Y	US 2020351332 A1 (KONG INC) 2020年11月5日 (2020-11-05) 说明书第46-90段	6-7、13-14
Y	CN 110971646 A (浙江大学) 2020年4月7日 (2020-04-07) 权利要求1-16	6-7、13-14

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2022年4月15日	2022年4月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王慧敏 电话号码 86-(20)-28958356

国际检索报告

国际申请号
PCT/CN2022/076922

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 111935110 A（北京金山云网络技术有限公司）2020年11月13日（2020-11-13） 全文	1-17
A	CN 110175077 A（浪潮云信息技术有限公司）2019年8月27日（2019-08-27） 全文	1-17

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/076922

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	113360882	A	2021年9月7日	无	
CN	111796858	A	2020年10月20日	无	
CN	111212077	A	2020年5月29日	无	
CN	111510444	A	2020年8月7日	无	
CN	112468442	A	2021年3月9日	无	
US	2020351332	A1	2020年11月5日	无	
CN	110971646	A	2020年4月7日	无	
CN	111935110	A	2020年11月13日	无	
CN	110175077	A	2019年8月27日	无	