(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
2024 年 10 月 3 日 (03.10.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/198734 A1

(51) 国际专利分类号:
*H04L 41/50* (2022.01)

(21) 国际申请号: PCT/CN2024/075967

(22) 国际申请日: 2024 年 2 月 5 日 (05.02.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310339767.6 2023年3月31日 (31.03.2023) CN

(71) 申请人: 华为云计算技术有限公司 (**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。

(72) 发明人: 谢鹏 (**XIE, Peng**); 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (**LONGSUN LEAD IP LTD.**); 中国北京市海淀区北清路 81 号院二区 3 号楼 8 层 801-1 室, Beijing 100094 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚

(54) **Title:** METHOD AND SYSTEM FOR ACCESS MANAGEMENT

(54) 发明名称: 访问管理的方法和系统

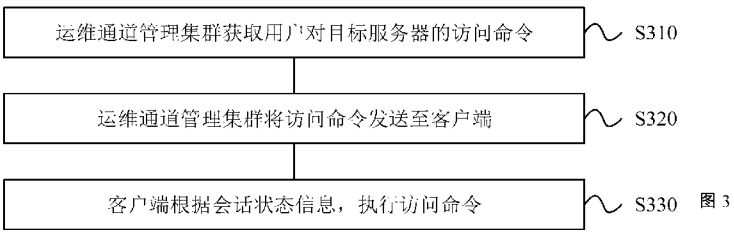


图 3

S310 An operation and maintenance channel management cluster acquires an access command of a user for a target server
S320 The operation and maintenance channel management cluster sends the access command to a client
S330 The client executes the access command according to session state information

(57) **Abstract:** The embodiments of the present application relate to the field of cloud computing. Provided are a method and system for access management. The system comprises an operation and maintenance channel management cluster and a client, wherein the client runs on a target server. The method comprises: an operation and maintenance channel management cluster acquiring an access command of a user for a target server; the operation and maintenance channel management cluster sending the access command to a client; and the client executing the access command according to session state information, wherein the session state information is access information of the user for the target server, which access information is recorded by the client. In the method, state information is recorded on a client located at a server, and an operation and maintenance channel instance allocates an access command to the client, such that the operation and maintenance channel instance is stateless, and thus the operation and maintenance channel instance can be switched without interrupting a service, thereby solving the problem of rapid capacity expansion and shrinkage of the operation and maintenance channel management cluster.

WO 2024/198734 A1

[见续页]

(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, ME, MK, MT, NL, NO, PL, PT, 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))。

**(57)** 摘要: 本申请实施例涉及云计算领域，提供了一种访问管理的方法和系统，该系统包括运维通道管理集群和客户端，客户端运行在目标服务器上，该方法包括：运维通道管理集群获取用户对目标服务器的访问命令；运维通道管理集群将访问命令发送至客户端；客户端根据会话状态信息，执行访问命令，会话状态信息是客户端记录的用户对目标服务器的访问信息。上述方法通过将状态信息记录在位于服务器的客户端上，运维通道实例将访问命令分发至客户端，使得运维通道实例是无状态的，从而能够在不中断服务的情况下切换运维通道实例，解决运维通道管理集群的快速扩缩容问题。

# 访问管理的方法和系统

本申请要求于 2023 年 3 月 31 日提交中国专利局、申请号为 202310339767.6、申请名称为“访问管理的方法和系统”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

本申请实施例涉及云计算领域，并且更为具体地，涉及一种访问管理的方法和系统。

## 背景技术

在云计算领域，云服务提供厂商需要管理的云服务资源越来越多，且云服务资源的访问安全也越来越重要。因此，很多云服务提供厂商选择部署堡垒机作为运维安全接入审计的系统，集中管理用户对服务器的访问请求。

但是，现有的堡垒机系统由于需要记录用户的登录状态以及用户与服务器建立的会话控制等状态信息，称之为有状态的服务。由于堡垒机节点都是有状态的，如果需要更换节点或增加新的节点，就需要重新配置堡垒机节点的状态，该过程需要一定时间，导致堡垒机系统无法快速容灾或扩容。因此，如何使运维通道管理集群能够不断开连接地快速更换节点成为亟需解决的技术问题。

## 发明内容

本申请实施例提供一种访问管理的方法和系统，可以将状态信息记录在位于服务器的客户端上，运维通道实例将访问命令分发至客户端，使得运维通道实例是无状态的，从而能够在不中断服务的情况下切换运维通道实例。

第一方面，提供一种访问管理的方法，该方法应用于访问管理的系统，该系统包括运维通道管理集群和客户端，客户端运行在目标服务器上，运维通道管理集群包括多个运维通道实例，每个运维通道实例用于与客户端进行信息交互，每个运维通道实例由至少一台计算实例组成，至少一台计算实例包括物理主机、虚拟机、容器中的至少一种，该方法包括：运维通道管理集群获取用户对目标服务器的访问命令；运维通道管理集群将访问命令发送至客户端；客户端根据会话状态信息，执行访问命令，会话状态信息是客户端记录的用户对目标服务器的访问信息。

根据本申请提供的技术方案，通过在服务器上设置客户端作为接入服务器的入口，运维通道管理集群直接与客户端通信，将访问命令分发至客户端，使得记录状态信息以及管理会话的任务由客户端完成，运维通道实例是无状态的，从而在通过运维通道管理集群隔离用户与服务器间直接交互，保证服务器访问安全性的前提下，能够在不中断服务的情况下切换运维通道实例，解决运维通道管理集群的快速扩缩容问题。

结合第一方面，在第一方面的某些实现方式中，运维通道管理集群还包括负载均衡组件，多个运维通道实例中包括第一运维通道实例和第二运维通道实例，将访问命令发送至客户端，包括：负载均衡组件将访问命令发送至第一运维通道实例；第一运维通道实例向客户端发送访问命令。

根据上述技术方案，通过在运维通道管理集群中设置多个节点，使得运维通道管理集群能够管理负责分发访问命令的节点，从而运维通道管理集群在需要时能够自主调控节点的工作情况。

结合第一方面，在第一方面的某些实现方式中，将访问命令发送至客户端，还包括：第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组件将访问命令发送至第二运维通道实例；第二运维通道实例向客户端发送访问命令。

根据上述技术方案，通过在当前负责转发访问命令的运维通道实例异常时，将转发任务重新分配给运维通道管理集群内的其他节点，实现不中断访问情况下的切换节点，从而提高运维通道管理集群的快速容灾或负载均衡的能力，提高运维通道管理集群服务的可用性。

结合第一方面，在第一方面的某些实现方式中，第一运维通道实例和第二运维通道实例部署在不同的区域。

根据上述技术方案，运维通道管理集群的节点能够跨区域（region）部署，使得切换前后负责转发的节点位于不同的物理地区，降低同时发生异常的可能性，从而实现异地容灾，进一步提高运维通道管理集群服务的可用性。

结合第一方面，在第一方面的某些实现方式中，将访问命令发送至客户端，还包括：第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组件建立第三运维通道实例；负载均衡组件将访问命令发送至第三运维通道实例；第三运维通道实例向客户端发送访问命令。

根据上述技术方案，通过在当前负责转发访问命令的运维通道实例异常时，部署新的运维通道实例，并将转发任务重新分配给该新的运维通道实例，实现不中断访问情况下的运维通道管理集群扩容，从而提高运维通道管理集群的快速扩容能力，提高运维通道管理集群服务的可用性。

结合第一方面，在第一方面的某些实现方式中，将访问命令发送至客户端，包括：运维通道管理集群根据传输控制协议向客户端发送访问命令。

根据上述技术方案，运维通道实例与客户端之间通过传输层的传输控制协议（transmission control protocol，TCP）直接通信，从而能够避免使用安全外壳协议（secure shell，SSH）作为远程连接工具，不需要服务器为SSH服务开启高风险的22端口，从而提高服务器的安全性。

结合第一方面，在第一方面的某些实现方式中，访问命令中包括会话标识，会话状态信息中包括会话标识与目标服务器的操作系统中的子进程的对应关系，根据会话状态信息，执行访问命令，包括：根据访问命令的会话标识和会话状态信息，确定与会话标识对应的子进程；调用子进程执行访问命令。

根据上述技术方案，通过客户端为每个用户的会话分配标识值，并基于用户指令中携带的标识值管理会话，调用服务器操作系统中相应的子进程执行命令，使得客户端能够将不同用户的会话分开管理，从而提高访问管理的效率。

结合第一方面，在第一方面的某些实现方式中，在获取用户对目标服务器的访问命令前，该方法还包括：运维通道管理集群获取用户的登录命令；运维通道管理集群向认证鉴权服务发送登录命令，认证鉴权服务用于认证用户的身份；运维通道管理集群接收来自认证鉴权服务的认证信息；运维通道管理集群根据认证信息，确定用户的登录状态。

根据本申请提供的技术方案，运维通道管理集群通过与外部服务交互为用户提供身份认证，使得用户的登录状态无需记录在运维通道管理集群的节点中，从而使用户登录后，提供服务的节点更换也无需用户重新登录，在保证用户访问安全性的基础上，提高用户的使用体验。

结合第一方面，在第一方面的某些实现方式中，在将访问命令发送至客户端前，该方法还包括：运维通道管理集群从外部存储服务获取访问权限；运维通道管理集群确定访问命令满足访问权限。

根据上述技术方案，运维通道管理集群通过从外部存储服务获取用户对服务器的访问权限，使得运维通道管理集群中的任意节点都能够在不预先配置的情况下对用户的访问权限进行管理，从而提高访问管理的安全性。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：客户端将访问命令的执行结果发送至运维通道管理集群；运维通道管理集群向用户发送执行结果。

根据上述技术方案，通过运维通道管理集群将访问结果展示给用户，从而使得运维通道管理集群能够监控用户访问服务器的全过程，便于对用户行为的监控和审计，提高访问管理的安全性。

第二方面，提供一种访问管理的系统，该系统包括运维通道管理集群和客户端，客户端运行在目标服务器上，运维通道管理集群包括多个运维通道实例，每个运维通道实例用于与客户端进行信息交互，每个运维通道实例由至少一台计算实例组成，至少一台计算实例包括物理主机、虚拟机、容器中的至少一种，运维通道管理集群包括：命令获取模块，用于获取用户对目标服务器的访问命令；命令分发模块，用于将访问命令发送至客户端；客户端用于：根据会话状态信息，执行访问命令，会话状态信息是客户端记录的用户对目标服务器的访问信息。

结合第二方面，在第二方面的某些实现方式中，运维通道管理集群还包括负载均衡组件，多个运维通道实例中包括第一运维通道实例和第二运维通道实例，命令分发模块，用于：负载均衡组件将访问命令发送至第一运维通道实例；第一运维通道实例向客户端发送访问命令。

结合第二方面，在第二方面的某些实现方式中，命令分发模块，还用于：第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组

件将访问命令发送至第二运维通道实例；第二运维通道实例向客户端发送访问命令。

结合第二方面，在第二方面的某些实现方式中，第一运维通道实例和第二运维通道实例部署在不同的区域。

结合第二方面，在第二方面的某些实现方式中，命令分发模块，还用于：第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组件建立第三运维通道实例；负载均衡组件将访问命令发送至第三运维通道实例；第三运维通道实例向客户端发送访问命令。

结合第二方面，在第二方面的某些实现方式中，命令分发模块，用于：根据传输控制协议向客户端发送访问命令。

结合第二方面，在第二方面的某些实现方式中，访问命令中包括会话标识，会话状态信息中包括会话标识与目标服务器的操作系统中的子进程的对应关系，客户端，用于：根据访问命令的会话标识和会话状态信息，确定与会话标识对应的子进程；调用子进程执行访问命令。

结合第二方面，在第二方面的某些实现方式中，运维通道管理集群还包括登录认证模块，在获取用户对目标服务器的访问命令前，用于：获取用户的登录命令；向认证鉴权服务发送登录命令，认证鉴权服务用于认证用户的身份；接收来自认证鉴权服务的认证信息；根据认证信息，确定用户的登录状态。

结合第二方面，在第二方面的某些实现方式中，运维通道管理集群还包括权限管理模块，在将访问命令发送至客户端前，用于：从外部存储服务获取访问权限；确定访问命令满足访问权限。

结合第二方面，在第二方面的某些实现方式中，客户端还用于：将访问命令的执行结果发送至运维通道管理集群；运维通道管理集群还包括结果展示模块，用于向用户发送执行结果。

第三方面，提供一种计算设备，包括处理器和存储器，其中，存储器用于存储指令，处理器用于从存储器中调用并运行该指令，使得该计算设备执行第一方面或第一方面任意一种可能的实现方式中的方法。

第四方面，提供一种计算设备集群，包括至少一个计算设备，每个计算设备包括处理器和存储器，其中，存储器用于存储指令，处理器用于从存储器中调用并运行该指令，使得该计算设备集群执行第一方面或第一方面任意一种可能的实现方式中的方法。

可选地，该处理器可以是通用处理器，可以通过硬件来实现也可以通过软件来实现。当通过硬件来实现时，该处理器可以是逻辑电路、集成电路等；当通过软件来实现时，该处理器可以是一个通用处理器，通过读取存储器中存储的软件代码来实现，该存储器可以集成在处理器中，可以位于该处理器之外独立存在。

第五方面，提供了一种芯片，该芯片获取指令并执行该指令来实现上述第一方面或第一方面任意一种可能的实现方式中的方法。

可选地，作为一种实现方式，该芯片包括处理器与数据接口，该处理器通过该数据接口读取存储器上存储的指令，执行上述第一方面或第一方面任意一种可能的实现方式中的方法。

可选地，作为一种实现方式，该芯片还可以包括存储器，该存储器中存储有指令，该处理器用于执行该存储器上存储的指令，当该指令被执行时，该处理器用于执行上述第一方面或第一方面任意一种可能的实现方式中的方法。

第六方面，提供了一种包含指令的计算机程序产品，当该指令被计算设备集群运行时，使得计算设备集群执行上述第一方面或第一方面任意一种可能的实现方式中的方法。

第七方面，提供了一种计算机可读存储介质，包括计算机程序指令，当该计算机指令由计算设备集群执行时，使得计算设备集群执行上述第一方面或第一方面任意一种可能的实现方式中的方法。

作为示例，这些计算机可读存储介质包括但不限于如下的一个或者多个：只读存储器（read-only memory，ROM）、可编程 ROM（programmable ROM，PROM）、可擦除的 PROM（erasable PROM，EPROM）、Flash 存储器、电 EPROM（electrically EPROM，EEPROM）以及硬盘驱动器（hard drive）。

可选地，作为一种实现方式，上述存储介质具体可以是非易失性存储介质。

**附图说明**

图 1 是一种堡垒机系统的示意图。

图 2 是本申请实施例提供的一种访问管理的系统架构示意图。

图 3 是本申请实施例提供的一种访问管理的方法的示意性流程框图。
图 4 是本申请实施例提供的一种调度运维通道实例的示意性流程框图。
图 5 是本申请实施例提供的另一访问管理的方法的示意性流程框图。
图 6 是本申请实施例提供的一种访问管理的系统的示意性结构框图。
图 7 是本申请实施例提供的一种访问管理的系统中运维通道管理集群的示意性流程框图。
图 8 是本申请实施例提供的一种计算设备的示意性结构框图。
图 9 是本申请实施例提供的一种计算设备集群的示意性结构框图。
图 10 是本申请实施例提供的另一计算设备集群的示意性结构框图。

**具体实施方式**

下面将结合附图，对本申请实施例中的技术方案进行描述。

本申请将围绕包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所有设备、组件、模块等。此外，还可以使用这些方案的组合。

另外，在本申请实施例中，“示例的”、“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用示例的一词旨在以具体方式呈现概念。

本申请实施例中，“相应的（corresponding，relevant）”和“对应的(corresponding)”有时可以混用，应当指出的是，在不强调其区别时，其所要表达的含义是一致的。

本申请实施例描述的网络架构以及业务场景是为了更加清楚地说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

在本说明书中描述的参考“一个实施例”或“一些实施例”等意味着在本申请的一个或多个实施例中包括结合该实施例描述的特定特征、结构或特点。由此，在本说明书中的不同之处出现的语句“在一个实施例中”、“在一些实施例中”、“在其他一些实施例中”、“在另外一些实施例中”等不是必然都参考相同的实施例，而是意味着“一个或多个但不是所有的实施例”，除非是以其他方式另外特别强调。术语“包括”、“包含”、“具有”及它们的变形都意味着“包括但不限于”，除非是以其他方式另外特别强调。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：包括单独存在 A，同时存在 A 和 B，以及单独存在 B 的情况，其中 A，B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a，b，或 c 中的至少一项（个），可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。

为了便于理解，下面先对本申请实施例可能涉及的相关术语和概念进行介绍。

1、运维通道管理集群：也叫做运维安全审计系统，负责对用户访问云服务资源进行集中管理的服务。运维通道管理集群负责接收用户输入的访问命令，并将访问命令分发至云服务资源所在的服务器，从而可以实时收集和监控网络环境中每个组成部分的系统状态、安全事件和网络活动，保障网络和数据不受来自外部或内部用户的入侵和破坏，便于集中报警、及时处理及审计定责。在其他实施方案中，运维通道管理集群也被叫做堡垒机或云堡垒机等。

2、会话控制：会话指的是一个终端用户与一个交互系统进行通信时建立的连接。会话控制（session）对象用于存储特定用户访问特定服务所需的属性及配置信息。这样，当用户在服务之间跳转时，存储在会话控制对象中的变量将不会丢失，而是在整个用户会话中一直存在下去。当用户请求访问特定服务时，如果该用户还没有会话，则服务器将自动创建一个会话控制对象。对于已经建立会话控制对象的会话，用户新发送的访问指令需要基于会话控制对象中存储的会话状态信息执行，会话状态信息是该用户对该服务器的访问信息。作为示例，会话状态信息可以包括用户身份、用户的首选项、用户对服务已执行的访问命令等。当会话过期或被放弃后，服务器将终止该会话。

在云计算领域，云服务提供厂商需要管理的云服务资源越来越多，同时伴随着访问云服务资源的用

户数量增加。如果由提供云服务资源的服务器直接管理用户的访问，会导致每个服务器都需要存储并处理大量的用户信息以及访问记录，不利于集中管理访问权限，造成大量运算资源浪费，访问效率低下。此外，云服务资源的重要程度也越来越高，因此访问安全也越来越重要。如果让用户能够直接访问服务器，会导致服务器地址暴露，存在安全隐患，且受到攻击时也不易排查与审计定责。

因此，很多云服务提供厂商选择在用户和服务器之间部署运维安全接入审计的系统，例如堡垒机，从而集中管理用户对服务器的访问请求。图 1 示出了一种现有的堡垒机系统。如图 1 所示，堡垒机系统包括多个堡垒机、用户界面（portal）和负载均衡（nginx）组件。堡垒机用于提供认证、授权、鉴权、命令审计、行为记录与回放等功能。用户界面用于提供用户登录堡垒机和访问云服务资源的前段操作界面，用户通过用户界面输入的访问命令通过负载均衡组件转发到某一个堡垒机上，该堡垒机通过安全外壳协议（secure shell，SSH）将访问命令发送至目标云服务资源所在的服务器。

但是，如图 1 所示的堡垒机系统中，由于堡垒机需要记录用户的登录状态以及用户与服务器建立的会话控制（session）等状态信息，称之为有状态的。由于堡垒机节点都是有状态的，如果需要更换节点或增加新的节点，就需要重新配置堡垒机节点的状态信息。作为示例，如果堡垒机集群有 N 个节点，当前单个堡垒机节点故障之后，用户正在进行中的会话可能会有 1/N 断开连接，运维人员需要重新认证建立新连接，整个过程至少需要几分钟才能恢复。堡垒机的有状态这一特点导致堡垒机系统无法快速容灾或扩容。因此，如何使运维通道管理集群能够不断开连接地快速更换节点成为亟需解决的技术问题。

鉴于此，本申请实施例提供一种访问管理的方法，该方法应用于访问管理的系统，该系统包括运维通道管理集群和运行在服务器上的客户端。通过将状态信息记录在位于服务器的客户端上，运维通道实例将访问命令分发至客户端，使得运维通道实例是无状态的，从而能够在不中断服务的情况下切换运维通道实例。

图 2 示出了本申请提供的访问管理的系统架构示意图。如图 2 所示，该系统包括运维通道管理集群 110 和运行在服务器 20 上的客户端 120。

客户端 120 用于建立并管理用户的会话控制对象。具体地，客户端 120 中存储有会话状态信息，当客户端 120 接收到访问命令时，根据会话控制对象中的会话状态信息与服务器 20 的操作系统（operating system，OS）进行命令交互，从而执行用户的访问命令，并将访问命令的执行结果返回给用户。

运维通道管理集群 110 用于对用户输入的访问命令进行分发，还可以将客户端 120 执行访问命令后返回的执行结果展示给客户。运维通道管理集群 110 由多个运维通道实例 111 组成，每个运维通道实例 111 可以由一台或多台计算实例组成，其中，计算实例可以包括物理主机（计算设备）、虚拟机、容器中的至少一种。可选地，不同运维通道实例 111 可以分布在不同的区域（region）中，也可以分布在相同的 region 中，也即每个 region 中可以包括多个运维通道实例，其中不同 region 对应不同的物理地区。可选地，运维通道管理集群 110 还可以包括负载均衡（nginx）组件 112，用于将用户运维接入运维通道管理集群的请求转发到一个具体的运维通道实例 111 上。

可选地，运维通道管理集群 110 可以与客户端 120 通过传输控制协议（transmission control protocol，TCP）进行命令传输。现有的堡垒机等运维通道管理集群实现方案中，运维通道管理集群通过安全外壳协议（secure shell，SSH）作为与服务器的远程连接工具。使用 SSH 服务需要开启服务器的 22 号端口，该端口存在较多漏洞，攻击者可以探测它以进行远程访问并发起安全攻击，从而造成服务器的安全隐患。系统内组件能够通过传输层的 TCP 协议直接通信，能够避免使用 SSH 服务，从而提高服务器的安全性。

可选地，该系统还可以包括前端组件用户界面 130。用户界面 130 提供访问接口（如界面或应用程序界面（application program interface，API）），用户可通过网页或应用程序等操作界面远程接入访问接口，在用户界面 130 注册云账号和密码，并登录运维通道管理集群 110。运维通道管理集群 110 对云账号和密码鉴权成功后，用户可进一步通过用户界面 30 向运维通道管理集群 110 发送访问命令，用户界面 130 还可以将运维通道管理集群 110 返回的执行结果通过操作界面展示给用户。

可选地，运维通道管理集群 110 可以与用户界面 130 通过网络套接字（WebSocket）协议进行通信。在 WebSocket 协议中，运维通道管理集群 110 与用户界面 130 只需要完成一次握手，两者之间就直接可以创建持久性的连接，并进行双向数据传输，使得运维通道管理集群 110 能够实时接收用户输入并返回执行结果。

可选地，运维通道管理集群 110 还可以与外部服务 30 进行信息交互，通过其它云服务为运维通道管理集群 110 提供额外功能。外部服务 30 可以包括但不限于认证鉴权服务、审计管理服务、存储服务等。

作为示例，认证鉴权服务可以是统一身份认证服务（identity and access management，IAM），为请求登录运维通道管理集群 110 的用户提供身份认证。又例如，审计管理服务可以是云审计服务（cloud trace service，CTS），为运维通道管理集群 110 记录其转发的访问命令以及执行结果，方便用户日后的查询、审计和回溯。再例如，存储服务可以是关系型数据库（relational database service，RDS），其中可以存储有用户对服务器或服务器中云服务的访问权限，从而使运维通道管理集群 110 能够获取该访问权限，从而对用户发送的访问命令进行权限管理。

下面结合图 3，详细描述本申请的访问管理的方法。

图 3 示出了本申请实施例提供的一种访问管理的方法的示意性流程图。可选地，图 3 的方法可以由访问管理的系统执行，例如上述图 2 中所示的系统。具体地，用于执行本申请实施例提供的访问管理的方法的系统包括运维通道管理集群和运行在服务器上的客户端。

如图 3 所示，该方法包括如下步骤。

S310：运维通道管理集群获取用户对目标服务器的访问命令。

例如，在步骤 S310 中，运维通道管理集群可以获取用户对目标服务器的访问命令。作为示例，用户可以在用户界面上选择要访问的云服务资源并输入具体的访问操作，根据该云服务资源所在的目标服务器，用户界面生成用户对目标服务器的访问命令，并将该访问命令发送至运维通道管理集群。可选地，运维通道管理集群可以通过 WebSocket 协议从用户界面获取访问命令。

S320：运维通道管理集群将访问命令发送至客户端。

例如，在步骤 S320 中，运维通道管理集群可以将用户对目标服务器的访问命令发送至客户端。作为示例，运维通道管理集群可以负责多个服务器的访问管理，每个服务器上都部署有客户端负责执行对应服务器的访问命令，访问命令指示了目标服务器，因此运维通道管理集群能够将该访问命令发送至目标服务器上的客户端。

可选地，运维通道管理集群可以根据 TCP 向目标服务器上的客户端发送访问命令。通过使运维通道管理集群与客户端之间通过传输层的 TCP 直接通信，能够避免使用 SSH 作为远程连接工具，从而不需要目标服务器为 SSH 服务开启高风险的 22 号端口，提高服务器的安全性。

S330：客户端根据会话状态信息，执行访问命令。

例如，在步骤 S330 中，目标服务器上的客户端可以执行访问命令。具体地，客户端能够为用户和目标服务器之间建立的会话创建 session 对象，session 对象中存储有客户端记录的会话状态信息，因此客户端能够根据会话状态信息执行该访问命令。

作为示例，用户在与服务器建立一次会话的时间内，用户可以发出了多个连续且相互关联的访问命令。例如，上述访问命令可以包括第一访问命令、第二访问命令和第三访问命令，其中，第一访问命令和第二访问命令先于第三访问命令发出并执行，第三访问命令需要基于第一访问命令和第二访问命令的内容和执行结果执行。当客户端收到第三访问命令时，客户端中存储的当前会话的会话状态信息中可以包括第一访问命令和第二访问命令的内容以及执行结果，因此客户端能够正确执行第三访问命令；如果上述会话状态信息丢失，则会导致第三访问命令无法正确执行。

可选地，客户端可以同时管理多个会话，客户端可以根据不同访问命令对应的不同会话调用不同的子进程执行。具体地，客户端可以根据不同用户对目标服务器上不同云服务的访问分别建立 session 对象，session 对象建立后会为每个 session 对象分配独有的会话标识，访问命令中可以包括会话标识，是的客户端可以根据访问命令中携带的会话标识确定该访问命令所对应的会话。进一步地，会话状态信息可以包括会话标识与目标服务器 OS 中的子进程的对应关系，其中不同的子进程可以用于对不同云服务执行访问操作，因此客户端在确定访问命令对应的会话后能够进一步确定用于执行该访问命令的子进程。通过上述方式，客户端能够根据访问命令中的会话标识以及会话状态信息，调用服务器 OS 中相应的子进程执行命令，使得客户端能够将不同用户的会话分开管理，从而提高访问管理的效率。

可选地，客户端在执行完成访问命令后，还可以通过运维通道管理集群将访问结果展示给用户。具体地，客户端可以将执行结果发送至运维通道管理集群，运维向用户发送执行结果。作为示例，运维通道管理集群可以将执行结果发送至用户界面，使用户界面生成用于向用户展示该执行结果的可视化界面。从而使得运维通道管理集群能够监控用户访问服务器的全过程，便于对用户行为的监控和审计，提高访问管理的安全性。

通过本申请实施例的技术方案，在服务器上设置客户端作为接入服务器的入口，运维通道管理集群

直接与客户端通信，将访问命令分发至客户端，使得会话状态信息能够被记录在客户端而不是运维通道管理集群上。因此运维通道管理集群中的节点是无状态的，切换节点时新的节点能够直接工作而无需配置会话状态信息，能够避免会话状态信息缺失导致已建立的会话中断，从而在不中断服务的情况下切换运维通道实例，解决运维通道管理集群的快速扩缩容问题。

对于上述步骤 S320，在一些可能的实施方式中，运维通道管理集群可以设置多个节点，使得运维通道管理集群能够管理负责分发访问命令的节点，由于运维通道管理集群中的节点是无状态的，从而运维通道管理集群在需要时能够自主调控节点的工作情况。具体地，运维通道管理集群中可以包括负载均衡组件和至少一个运维通道实例，负载均衡组件用于将获取到的访问命令转发至一个当前可工作的运维通道实例，该运维通道实例用于将向客户端发送该访问命令。

在该情况下，图 4 示出了本申请实施例提供的一种调度运维通道实例的示意性流程图。如图 4 所示，将用户和服务器间建立会话作为流程的开始，用户和服务期间建立的该会话断开作为结束。在该过程中，运维通道管理集群获取访问命令后，负载均衡组件将访问命令转发至当前可工作的运维通道实例，该运维通道实例向客户端发送该访问命令。

例如，运维通道管理集群可以包括第一运维通道实例，负载均衡组件可以将获取的第一访问命令转发至第一运维通道实例。第一运维通道实例向客户端发送第一访问命令，如果第一运维通道实例发送第一访问命令成功，则客户端能够接收第一访问命令并执行。可选地，客户端执行第一访问命令的具体过程可以包括是根据第一访问命令中携带的会话标识获取服务器 OS 中对应的子进程，调用该子进程执行第一访问命令并返回执行结果。第一访问命令执行结束后如果会话尚未结束，则运维通道管理集群能够继续获取访问命令并重复上述步骤。

如果运维通道实例向客户端发送访问命令失败，则运维通道实例能够向负载均衡组件上报异常，由负载均衡组件将访问命令转发至另一个当前可工作的运维通道实例。下面结合两个示例进行具体说明。

示例一，运维通道管理集群除第一运维通道实例外还可以包括第二运维通道实例。负载均衡组件将获取的第二访问命令转发至第一运维通道实例，但第一运维通道实例接收到第二访问命令后未能成功向客户端发送第二访问命令。例如，由于第一运维通道实例当前有大量其他会话的访问命令正在发送中，导致第一运维通道实例负载过高，第二访问命令等待超时；又例如，由于第一运维通道实例在接收到第二访问命令后出现了故障，导致第一运维通道实例失去了正常工作的能力。在上述情况下，第一运维通道实例能够向负载均衡组件上报异常信息，负载均衡组件收到第一运维通道实例的发送的异常信息后，负载均衡组件能够将第二访问命令转发至第二运维通道实例，由第二运维通道实例向客户端发送第二访问命令。第二运维通道实例成功向客户端发送第二访问命令后，客户端能够接收并执行第二访问命令。

通过本申请实施例的技术方案，在例如负载均衡或容灾等导致当前负责转发访问命令的运维通道实例异常的情况下，当前节点没有成功向客户端发送，将转发任务重新分配给运维通道管理集群内的其他节点，实现不中断访问情况下的切换节点，从而提高运维通道管理集群的快速容灾或负载均衡的能力，提高运维通道管理集群服务的可用性。

可选地，在上述示例中，第一运维通道实例和第二运维通道实例可以部署在不同的 region 中。由于切换节点不需要重新配置会话状态信息，因此运维通道实例节点间可以无需信息交互，不需要限制运维通道实例所在的物理地区，实现运维通道实例的跨 region 部署。使得切换前后负责转发的节点位于不同的物理地区，降低不同节点同时发生异常的可能性，从而实现异地容灾，进一步提高运维通道管理集群服务的可用性。

示例二，运维通道管理集群还可以部署新的运维通道实例。负载均衡组件将获取的第三访问命令转发至第一运维通道实例，第一运维通道实例未成功发送第三访问命令并上报异常后，例如运维通道管理集群负载已满或全部运维通道实例故障等导致第二运维通道实例也处于不可工作的状态时，负载均衡组件能够建立第三运维通道实例，并将将第三访问命令转发至第三运维通道实例，由第三运维通道实例向客户端发送第三访问命令。作为示例，负载均衡组件可以请求原本不包括在运维通道管理集群内一台或多台计算实例，将该一台或多台计算实例包括至运维通道管理集群范围内，从而用作第三运维通道实例。

应理解，上述示例二仅是以运维通道管理集群当前无可工作的运维通道实例的情况为例，说明运维通道管理集群具有扩展运维通道实例数量的能力，并不限定仅在该情况下才可以新增运维通道实例。例如，用户可以通过用户界面购买了更大规格的运维通道管理集群服务，此时用户界面也能够发出指令，指示运维通道管理集群建立新的运维通道实例。

通过本申请实施例的技术方案，运维通道管理集群能够部署新的运维通道实例，并将转发任务重新分配给该新的运维通道实例，实现不中断访问情况下的运维通道管理集群扩容，从而提高运维通道管理集群的快速扩容能力，提高运维通道管理集群服务的可用性。

可选地，与快速扩容能力相对的，运维通道管理集群还可以提供快速缩容的能力。作为示例，当运维通道管理集群需要删除第一运维通道实例时，第一运维通道实例能够将其当前尚未成功发送的访问命令上报负载均衡组件，由负载均衡组件将这些访问命令重新分配至其他运维通道实例，从而将第一运维通道实例从运维通道管理集群中删除。

由于本申请技术方案中运维通道实例是无状态的，负责转发访问命令的运维通道实例的切换不会影响记录在客户端中的会话状态信息。因此，上述全部示例中的运维通道实例的切换均不会导致用户与服务器已建立的会话断开，切换后的节点无需配置可直接使用，使得切换所需的时间可控且迅速，从而使上述切换过程都能够在用户无感知的情况下完成。

本申请实施例提供的访问管理的系统中，仅是将需要节点有状态的功能，例如会话控制，由运维通道管理集群转移至目标服务器上的客户端执行。可以在节点无状态下执行的功能，能够继续由运维通道管理集群执行，从而为用户提供操作审计、权限管理、等保合规等服务。通过运维通道管理集群转发用户对服务器的访问命令，能够隔离用户和服务器，从而确保服务器访问的安全性；此外，也能够对不同用户对不同服务器的访问实现集中管理，便于认证鉴权以及后续审计定责。

作为示例，运维通道管理集群能够为用户提供身份认证服务。在该情况下，图 5 示出了本申请实施例提供的一种访问管理的方法的示意性流程图。

如图 5 所示，该方法包括如下步骤。

S510：运维通道管理集群获取登录命令。

例如，在步骤 S510 中，运维通道管理集群能够在建立用户与目标服务器的会话前，先获取用户的登录命令。具体地，该登录命令用于确认当前请求登录以及后续发出访问命令的用户的身份。作为示例，用户可以通过在用户界面输入已注册的云账号和密码进行登录，用户界面能够根据用户的输入，生成登录命令并发送至运维通道管理集群。

S520：运维通道管理集群向认证鉴权服务发送登录命令。

例如，在步骤 S520 中，运维通道管理集群能够向认证鉴权服务发送该登录命令，从而由认证鉴权服务根据该登录命令认证用户的身份。可选地，认证鉴权服务包括但不限于 IAM 服务。

S530：运维通道管理集群接收来自认证鉴权服务的认证信息。

例如，在步骤 S530 中，认证鉴权服务能够根据运维通道管理集群发送的登录命令确认用户身份，从而生成认证信息并发送给运维通道管理集群，使得运维通道管理集群能够接收该认证信息。

S540：运维通道管理集群根据认证信息，确定用户的登录状态。

例如，在步骤 S540 中，运维通道管理集群能够根据认证信息确定用户的登录状态。作为示例，认证信息可以是认证成功信息，例如用户输入的云账号和密码是已注册且匹配的，且该云账户的用户有权限访问运维通道管理集群管理的至少部分云服务，则认证鉴权服务生成并发送认证成功信息，运维通道管理集群根据认证成功信息能够确定用户登录成功，能够继续执行后续访问步骤。认证信息也可以是认证失败信息，例如用户输入的云账号为注册，或云账号与密码不匹配，或该云账号无权限访问该运维通道管理集群管理的任何云服务等情况，则认证鉴权服务生成并发送认证失败信息，运维通道管理集群根据认证失败信息能够确定用户没有成功登录。可选地，认证失败时，运维通道管理集群能够通过用户界面告知用户登录失败并请求用户重新登录，如果用户未能重新正确登录，则无权进行后续访问。

应理解，上述方案中由于认证信息是由认证鉴权服务向运维通道管理集群发送的，运维通道管理集群内任意运维通道实例在需要时均能接收到来自认证鉴权服务的认证信息，因此用户的登录状态无需记录在运维通道管理集群的节点中，使得身份认证服务并不依赖于某一具体的运维通道实例。例如，在会话过程中切换负责转发访问命令的运维通道实例后，切换后的运维通道实例能够根据发送访问命令的用户再次向认证鉴权服务请求该用户的认证信息，从而确定该用户的登录状态，无需用户重新登陆。在保证用户访问安全性的基础上，提高用户的使用体验。

在认证用户登录成功的情况下，访问管理的系统能够继续对访问命令进行管理，具体包括如下步骤：

S550：运维通道管理集群获取访问命令。

S560：运维通道管理集群向客户端发送访问命令，或者说，客户端接收来自运维通道管理集群的访

问命令。

可选地，运维通道管理集群在向客户端发送访问命令前，还能够从外部存储服务获取该用户的访问权限，并根据访问命令是否满足访问权限，确定是否向客户端发送该访问命令。具体地，访问权限用于指示该用户能够访问的云服务以及具体能够执行的操作，如果运维通道管理集群确定访问命令满足访问权限，则运维通道管理集群能够执行步骤 S560 以及后续步骤；如果运维通道管理集群确定访问命令不满足访问权限，则运维通道管理集群不执行 S560，返回步骤 S550。可选地，外部存储服务包括但不限于数据库、云数据库、云存储服务等，本申请不做具体限定。作为示例，外部存储服务可以是认证鉴权服务，认证鉴权服务在存储已注册的用户身份的同时还可以存储用户身份对应的访问权限，从而在用户登录认证成功时将该用户的访问权限发送给运维通道管理集群；外部存储服务还可以是其他独立的存储服务，例如 RDS，用户的访问权限设置后运维通道管理集群能够将其上传至 RDS，从而使任意运维通道实例在需要时都能够从 RDS 请求该访问权限。

通过上述方案，运维通道管理集群能够从外部存储服务获取用户对服务器的访问权限，使得运维通道管理集群中的任意节点都能够在不预先配置的情况下对用户的访问权限进行管理，从而使运维通道管理集群能够提供权限管理服务，提高访问管理的安全性。

S570：客户端根据会话状态信息，执行访问命令。

可选地，该方法还可以包括：

S580：客户端向运维通道管理集群发送执行结果，或者说，运维通道管理集群接收来自客户端的执行结果。

可选地，上述步骤 S550 至 S580 的实现方式可以与前文所述访问管理的方法相同，具体实施方式可以参考前文中对图 3 和图 4 以及相应实施例的说明，这里不再赘述。

通过本申请实施例的技术方案，运维通道管理集群能够与外部的认证鉴权服务交互，从而加强用户身份认证管理。

应理解，图 5 所示方法仅是以认证鉴权服务为例，说明本申请实施例提供的运维通道管理集群能够提供无状态的功能，但并不仅限于提供身份认证或权限管理功能，运维通道管理集群还能提供例如等保合规、操作审计等其他无状态的功能。

作为示例，运维通道管理集群能够对用户的访问操作进行审计管理。具体地，在用户登录成功后，运维通道管理集群能够将会话期间每一次向客户端转发的访问命令同时发送至 CTS，同时将客户端反馈的对应的执行结果也发送至 CTS，从而由 CTS 监控并记录用户全程的行为。当 CTS 发现用户的访问行为存在安全风险时，运维通道管理集群能够接收来自 CTS 的预警信息，运维通道管理集群根据预警信息通过用户界面提示用户，必要时能够中止转发该用户的访问命令。当用户请求查看操作记录时，运维通道管理集群能够向 CTS 发出请求并接收来自 CTS 的操作记录，从而通过用户界面反馈给用户。

上文结合图 3 至图 5 说明了本申请提供的访问管理的方法实施例，下面结合图 6 至图 10，对本申请提供的访问管理的装置实施例进行说明。

图 6 示出了本申请实施例提供的一种访问管理的系统 600 的示意性结构图。如图 6 所示，系统 600 包括运维通道管理集群 610 和客户端 620，其中客户端 620 运行在目标服务器上。

图 7 示出了本申请实施例提供的一种访问管理的系统 600 中运维通道管理集群 610 示意性结构框图。

如图 7 所示，该运维通道管理集群 610 包括：命令获取模块 611，命令分发模块 612。

具体地，该命令获取模块 611 用于获取用户对目标服务器的访问命令。

具体地，该命令分发模块 612 用于将访问命令发送至客户端。

可选地，运维通道管理集群包括负载均衡组件，运维通道管理集群至少还包括第一运维通道实例和第二运维通道实例，命令分发模块 612 具体用于负载均衡组件将访问命令发送至第一运维通道实例；第一运维通道实例向客户端发送访问命令。

可选地，命令分发模块 612 具体还用于第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组件将访问命令发送至第二运维通道实例；第二运维通道实例向客户端发送访问命令。

可选地，第一运维通道实例和第二运维通道实例部署在不同的区域。

可选地，命令分发模块 612 具体还用于第一运维通道实例向负载均衡组件上报异常信息，异常信息用于指示第一运维通道实例向客户端发送访问命令失败；负载均衡组件建立第三运维通道实例；负载均

衡组件将访问命令发送至第三运维通道实例；第三运维通道实例向客户端发送访问命令。

可选地，命令分发模块 612 具体用于根据传输控制协议向客户端发送访问命令。

具体地，客户端 620 用于根据会话状态信息，执行访问命令，会话状态信息是客户端记录的用户对目标服务器的访问信息。

可选地，访问命令中包括会话标识，会话状态信息中包括会话标识与目标服务器的操作系统中的子进程的对应关系，客户端 620 具体用于根据访问命令的会话标识和会话状态信息，确定与会话标识对应的子进程；调用子进程执行访问命令。

可选地，运维通道管理集群 610 还可以包括登录认证模块 613，在获取用户对目标服务器的访问命令前，用于：获取用户的登录命令；向认证鉴权服务发送登录命令，认证鉴权服务用于认证用户的身份；接收来自认证鉴权服务的认证信息；根据认证信息，确定用户的登录状态。

可选地，运维通道管理集群 610 还可以包括权限管理模块 614，在将访问命令发送至客户端前，用于：从外部存储服务获取访问权限；确定访问命令满足访问权限。

可选地，客户端 620 还用于将访问命令的执行结果发送至运维通道管理集群；运维通道管理集群 610 还可以包括结果展示模块 615，用于向用户发送执行结果。

其中，上述模块均可以通过软件实现，或者可以通过硬件实现。示例性的，接下来以命令分发模块 612 为例，介绍命令分发模块 612 的实现方式。类似的，命令获取模块 611、登录认证模块 613、权限管理模块 614 和结果展示模块 615 的实现方式可以参考命令分发模块 612 的实现方式。

模块作为软件功能单元的一种举例，命令分发模块 612 可以包括运行在计算实例上的代码。其中，计算实例可以包括物理主机（计算设备）、虚拟机、容器中的至少一种。进一步地，上述计算实例可以是一台或者多台。例如，命令分发模块 612 可以包括运行在多个主机/虚拟机/容器上的代码。需要说明的是，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的区域（region）中，也可以分布在不同的 region 中。进一步地，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的可用区（availability zone，AZ）中，也可以分布在不同的 AZ 中，每个 AZ 包括一个数据中心或多个地理位置相近的数据中心。其中，通常一个 region 可以包括多个 AZ。

同样，用于运行该代码的多个主机/虚拟机/容器可以分布在同一个虚拟私有云（virtual private cloud，VPC）中，也可以分布在多个 VPC 中。其中，通常一个 VPC 设置在一个 region 内，同一 region 内两个 VPC 之间，以及不同 region 的 VPC 之间跨区通信需在每个 VPC 内设置通信网关，经通信网关实现 VPC 之间的互连。

模块作为硬件功能单元的一种举例，命令分发模块 612 可以包括至少一个计算设备，如服务器等。或者，命令分发模块 612 也可以是利用专用集成电路（application-specific integrated circuit，ASIC）实现、或可编程逻辑器件（programmable logic device，PLD）实现的设备等。其中，上述 PLD 可以是复杂程序逻辑器件（complex programmable logical device，CPLD）、现场可编程门阵列（field-programmable gate array，FPGA）、通用阵列逻辑（generic array logic，GAL）或其任意组合实现。

命令分发模块 612 包括的多个计算设备可以分布在相同的 region 中，也可以分布在不同的 region 中。命令分发模块 612 包括的多个计算设备可以分布在相同的 AZ 中，也可以分布在不同的 AZ 中。同样，命令分发模块 612 包括的多个计算设备可以分布在同一个 VPC 中，也可以分布在多个 VPC 中。其中，所述多个计算设备可以是服务器、ASIC、PLD、CPLD、FPGA 和 GAL 等计算设备的任意组合。

需要说明的是，在其他实施例中，命令获取模块 611、命令分发模块 612、登录认证模块 613、权限管理模块 614 和结果展示模块 615 可以分别用于执行上述访问管理的方法中的任意步骤，命令获取模块 611、命令分发模块 612、登录认证模块 613、权限管理模块 614 和结果展示模块 615 负责实现的步骤可根据需要指定，通过命令获取模块 611、命令分发模块 612、登录认证模块 613、权限管理模块 614 和结果展示模块 615 分别实现上述访问管理的方法中不同的步骤来实现运维通道管理集群的全部功能。

本申请还提供一种计算设备 100。如图 8 所示，计算设备 100 包括：总线 102、处理器 104、存储器 106 和通信接口 108。处理器 104、存储器 106 和通信接口 108 之间通过总线 102 通信。计算设备 100 可以是服务器或终端设备。应理解，本申请不限定计算设备 100 中的处理器、存储器的个数。

总线 102 可以是外设部件互连标准（peripheral component interconnect，PCI）总线或扩展工业标准结构（extended industry standard architecture，EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 中仅用一条线表示，但并不表示仅有一根总线或一种类型的总线。总线 102 可

包括在计算设备 100 各个部件（例如，存储器 106、处理器 104、通信接口 108）之间传送信息的通路。

处理器 104 可以包括中央处理器(central processing unit，CPU)、图形处理器（graphics processing unit，GPU）、微处理器（micro processor，MP）或者数字信号处理器（digital signal processor，DSP）等处理器中的任意一种或多种。

存储器 106 可以包括易失性存储器(volatile memory)，例如随机存取存储器(random access memory，RAM)。处理器 104 还可以包括非易失性存储器(non-volatile memory)，例如只读存储器(read-only memory，ROM)，快闪存储器，机械硬盘（hard disk drive，HDD）或固态硬盘（solid state drive，SSD）。

存储器 106 中存储有可执行的程序代码，处理器 104 执行该可执行的程序代码以分别实现前述命令获取模块、命令分发模块、登录认证模块、权限管理模块和结果展示模块的功能，从而实现上述访问管理的方法。也即，存储器 106 上存有用于执行上述访问管理的方法的指令。

通信接口 108 使用例如但不限于网络接口卡、收发器一类的命令分发模块，来实现计算设备 100 与其他设备或通信网络之间的通信。

本申请实施例还提供了一种计算设备集群。该计算设备集群包括至少一台计算设备。该计算设备可以是服务器，例如是中心服务器、边缘服务器，或者是本地数据中心中的本地服务器。在一些实施例中，计算设备也可以是台式机、笔记本电脑或者智能手机等终端设备。

如图 9 所示，所述计算设备集群包括至少一个计算设备 100。计算设备集群中的一个或多个计算设备 100 中的存储器 106 中可以存有相同的用于执行上述访问管理的方法的指令。

在一些可能的实现方式中，该计算设备集群中的一个或多个计算设备 100 的存储器 106 中也可以分别存有用于执行上述访问管理的方法的部分指令。换言之，一个或多个计算设备 100 的组合可以共同执行用于执行上述访问管理的方法的指令。

需要说明的是，计算设备集群中的不同的计算设备 100 中的存储器 106 可以存储不同的指令，分别用于执行上述运维通道管理集群的部分功能。也即，不同的计算设备 100 中的存储器 106 存储的指令可以实现命令获取模块、命令分发模块、登录认证模块、权限管理模块和结果展示模块中的一个或多个模块的功能。

在一些可能的实现方式中，计算设备集群中的一个或多个计算设备可以通过网络连接。其中，所述网络可以是广域网或局域网等等。图 10 示出了一种可能的实现方式。如图 10 所示，两个计算设备 100A 和 100B 之间通过网络进行连接。具体地，通过各个计算设备中的通信接口与所述网络进行连接。在这一类可能的实现方式中，计算设备 100A 中的存储器 106 中存有执行命令获取模块和命令分发模块的功能的指令。同时，计算设备 100B 中的存储器 106 中存有客户端的功能的指令。

应理解，图 10 中示出的计算设备 100A 的功能也可以由多个计算设备 100 完成。同样，计算设备 100B 的功能也可以由多个计算设备 100 完成。

本申请实施例还提供一种芯片，该芯片包括处理器与数据接口，该处理器通过该数据接口读取存储器上存储的指令，以执行上述访问管理的方法。

本申请实施例还提供了一种包含指令的计算机程序产品。所述计算机程序产品可以是包含指令的，能够运行在计算设备上或被储存在任何可用介质中的软件或程序产品。当所述计算机程序产品在至少一个计算设备上运行时，使得至少一个计算设备执行上述访问管理的方法。

本申请实施例还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可以是计算设备能够存储的任何可用介质或者是包含一个或多个可用介质的数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘）等。该计算机可读存储介质包括指令，所述指令指示计算设备执行上述管理的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的保护范围。

# 权利要求书

1. 一种访问管理的方法，其特征在于，所述方法应用于访问管理的系统，所述系统包括运维通道管理集群和客户端，所述客户端运行在目标服务器上，所述运维通道管理集群包括多个运维通道实例，每个运维通道实例用于与所述客户端进行信息交互，所述每个运维通道实例由至少一台计算实例组成，所述至少一台计算实例包括物理主机、虚拟机、容器中的至少一种，所述方法包括：

所述运维通道管理集群获取用户对所述目标服务器的访问命令；

所述运维通道管理集群将所述访问命令发送至所述客户端；

所述客户端根据会话状态信息，执行所述访问命令，所述会话状态信息是所述客户端记录的所述用户对所述目标服务器的访问信息。

2. 根据权利要求 1 所述的方法，其特征在于，所述运维通道管理集群还包括负载均衡组件，所述多个运维通道实例中包括第一运维通道实例和第二运维通道实例，所述将所述访问命令发送至所述客户端，包括：

所述负载均衡组件将所述访问命令发送至所述第一运维通道实例；

所述第一运维通道实例向所述客户端发送所述访问命令。

3. 根据权利要求 2 所述的方法，其特征在于，所述将所述访问命令发送至所述客户端，还包括：

所述第一运维通道实例向所述负载均衡组件上报异常信息，所述异常信息用于指示所述第一运维通道实例向所述客户端发送所述访问命令失败；

所述负载均衡组件将所述访问命令发送至所述第二运维通道实例；

所述第二运维通道实例向所述客户端发送所述访问命令。

4. 根据权利要求 3 所述的方法，其特征在于，所述第一运维通道实例和所述第二运维通道实例部署在不同的区域。

5. 根据权利要求 2 所述的方法，其特征在于，所述将所述访问命令发送至所述客户端，还包括：

所述第一运维通道实例向所述负载均衡组件上报异常信息，所述异常信息用于指示所述第一运维通道实例向所述客户端发送所述访问命令失败；

所述负载均衡组件建立第三运维通道实例；

所述负载均衡组件将所述访问命令发送至所述第三运维通道实例；

所述第三运维通道实例向所述客户端发送所述访问命令。

6. 根据权利要求 1 至 5 中任意一项所述的方法，其特征在于，所述将所述访问命令发送至所述客户端，包括：

所述运维通道管理集群根据传输控制协议向所述客户端发送所述访问命令。

7. 根据权利要求 1 至 6 中任意一项所述的方法，其特征在于，所述访问命令中包括会话标识，所述会话状态信息中包括会话标识与所述目标服务器的操作系统中的子进程的对应关系，所述根据会话状态信息，执行所述访问命令，包括：

根据所述访问命令的会话标识和所述会话状态信息，确定与所述会话标识对应的子进程；

调用所述子进程执行所述访问命令。

8. 根据权利要求 1 至 7 中任意一项所述的方法，其特征在于，在获取用户对所述目标服务器的访问命令前，所述方法还包括：

所述运维通道管理集群获取所述用户的登录命令；

所述运维通道管理集群向认证鉴权服务发送所述登录命令，所述认证鉴权服务用于认证所述用户的身份；

所述运维通道管理集群接收来自所述认证鉴权服务的认证信息；

所述运维通道管理集群根据所述认证信息，确定所述用户的登录状态。

9. 根据权利要求 1 至 8 中任意一项所述的方法，其特征在于，在将所述访问命令发送至所述客户端前，所述方法还包括：

所述运维通道管理集群从外部存储服务获取访问权限；

所述运维通道管理集群确定所述访问命令满足所述访问权限。

10. 根据权利要求 1 至 9 中任意一项所述的方法，其特征在于，所述方法还包括：

所述客户端将所述访问命令的执行结果发送至所述运维通道管理集群；

所述运维通道管理集群向所述用户发送所述执行结果。

11. 一种访问管理的系统，其特征在于，所述系统包括运维通道管理集群和客户端，所述客户端运行在目标服务器上，所述运维通道管理集群包括多个运维通道实例，每个运维通道实例用于与所述客户端进行信息交互，所述每个运维通道实例由至少一台计算实例组成，所述至少一台计算实例包括物理主机、虚拟机、容器中的至少一种，所述运维通道管理集群包括：

命令获取模块，用于获取用户对所述目标服务器的访问命令；

命令分发模块，用于将所述访问命令发送至所述客户端；

所述客户端用于：

根据会话状态信息，执行所述访问命令，所述会话状态信息是所述客户端记录的所述用户对所述目标服务器的访问信息。

12. 根据权利要求 11 所述的系统，其特征在于，所述运维通道管理集群还包括负载均衡组件，所述多个运维通道实例中包括第一运维通道实例和第二运维通道实例，所述命令分发模块，用于：

所述负载均衡组件将所述访问命令发送至所述第一运维通道实例；

所述第一运维通道实例向所述客户端发送所述访问命令。

13. 根据权利要求 12 所述的系统，其特征在于，所述命令分发模块，还用于：

所述第一运维通道实例向所述负载均衡组件上报异常信息，所述异常信息用于指示所述第一运维通道实例向所述客户端发送所述访问命令失败；

所述负载均衡组件将所述访问命令发送至所述第二运维通道实例；

所述第二运维通道实例向所述客户端发送所述访问命令。

14. 根据权利要求 13 所述的系统，其特征在于，所述第一运维通道实例和所述第二运维通道实例部署在不同的区域。

15. 根据权利要求 12 所述的系统，其特征在于，所述命令分发模块，还用于：

所述第一运维通道实例向所述负载均衡组件上报异常信息，所述异常信息用于指示所述第一运维通道实例向所述客户端发送所述访问命令失败；

所述负载均衡组件建立第三运维通道实例；

所述负载均衡组件将所述访问命令发送至所述第三运维通道实例；

所述第三运维通道实例向所述客户端发送所述访问命令。

16. 根据权利要求 11 至 15 中任意一项所述的系统，其特征在于，所述命令分发模块，用于：

根据传输控制协议向所述客户端发送所述访问命令。

17. 根据权利要求 11 至 16 中任意一项所述的系统，其特征在于，所述访问命令中包括会话标识，所述会话状态信息中包括会话标识与所述目标服务器的操作系统中的子进程的对应关系，所述客户端，用于：

根据所述访问命令的会话标识和所述会话状态信息，确定与所述会话标识对应的子进程；

调用所述子进程执行所述访问命令。

18. 根据权利要求 11 至 17 中任意一项所述的系统，其特征在于，所述运维通道管理集群还包括登录认证模块，在获取用户对所述目标服务器的访问命令前，用于：

获取所述用户的登录命令；

向认证鉴权服务发送所述登录命令，所述认证鉴权服务用于认证所述用户的身份；

接收来自所述认证鉴权服务的认证信息；

根据所述认证信息，确定所述用户的登录状态。

19. 根据权利要求 11 至 18 中任意一项所述的系统，其特征在于，所述运维通道管理集群还包括权限管理模块，在将所述访问命令发送至所述客户端前，用于：

从外部存储服务获取访问权限；

确定所述访问命令满足所述访问权限。

20. 根据权利要求 11 至 19 中任意一项所述的系统，其特征在于，所述客户端还用于：

所述客户端将所述访问命令的执行结果发送至所述运维通道管理集群；

所述运维通道管理集群还包括结果展示模块，用于向所述用户发送所述执行结果。

21．一种计算设备，其特征在于，包括处理器和存储器，所述处理器用于执行所述存储器中存储的指令，以使得所述计算设备执行如权利要求 1 至 10 中任一项所述的方法。

22．一种计算设备集群，其特征在于，包括至少一个计算设备，每个计算设备包括处理器和存储器；

所述至少一个计算设备的处理器用于执行所述至少一个计算设备的存储器中存储的指令，以使得所述计算设备集群执行如权利要求 1 至 10 中任一项所述的方法。

23．一种计算机可读存储介质，其特征在于，包括计算机程序指令，当所述计算机指令由计算设备集群执行时，使得所述计算设备集群执行如权利要求 1 至 10 中任一项所述的方法。

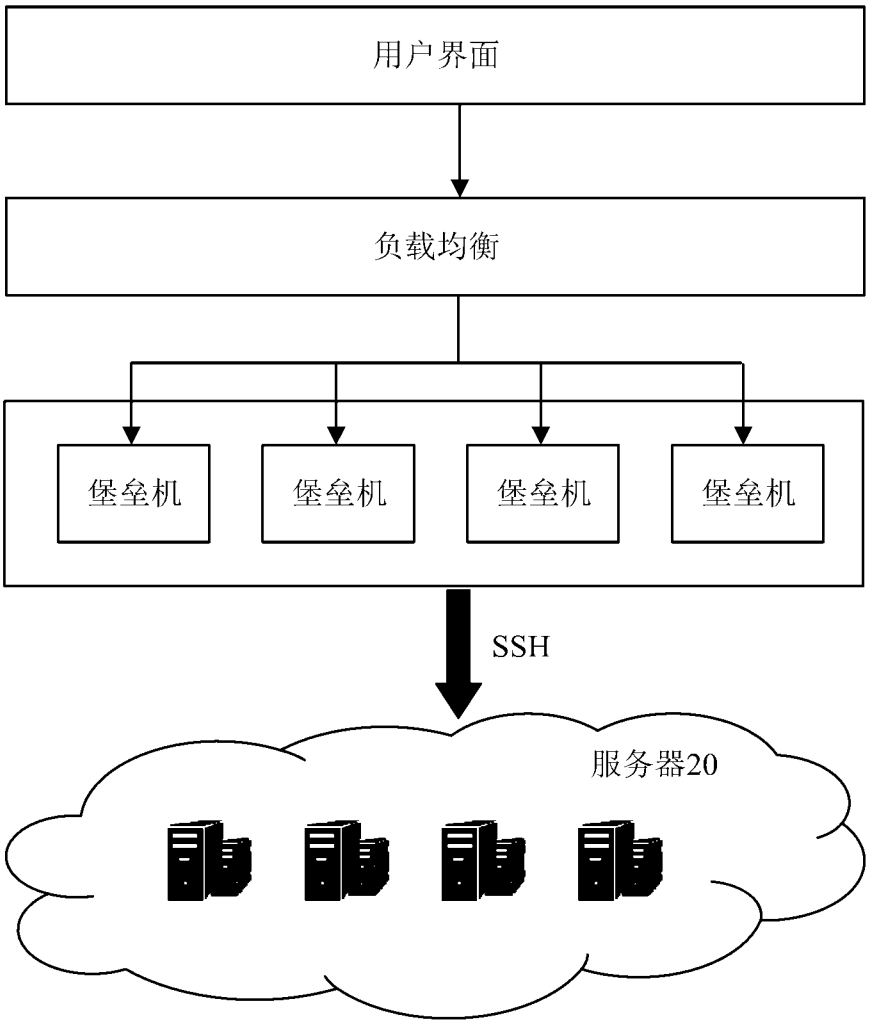


图 1

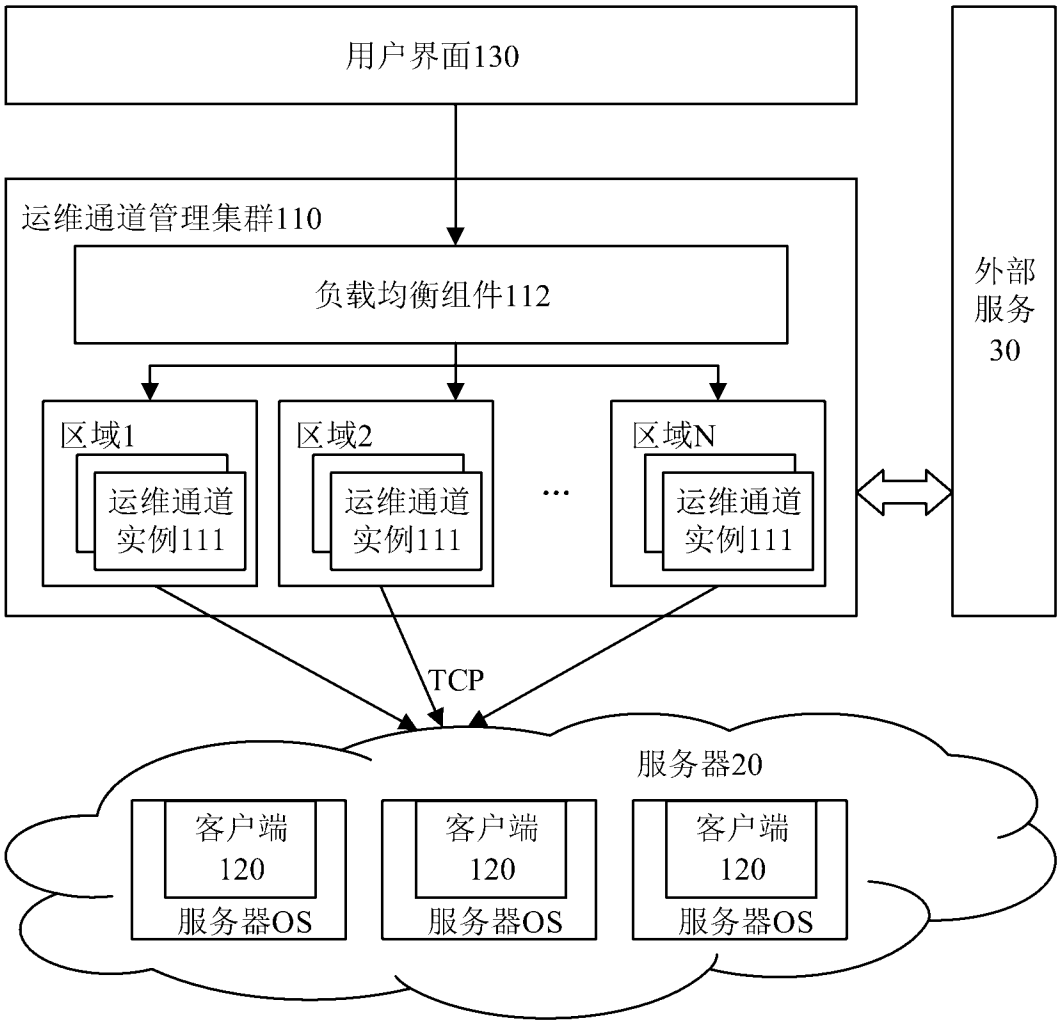
用户界面130
运维通道管理集群110
负载均衡组件112
区域1
运维通道实例111
区域2
运维通道实例111
...
区域N
运维通道实例111
外部服务30
TCP
服务器20
客户端120
服务器OS
客户端120
服务器OS
客户端120
服务器OS

图 2

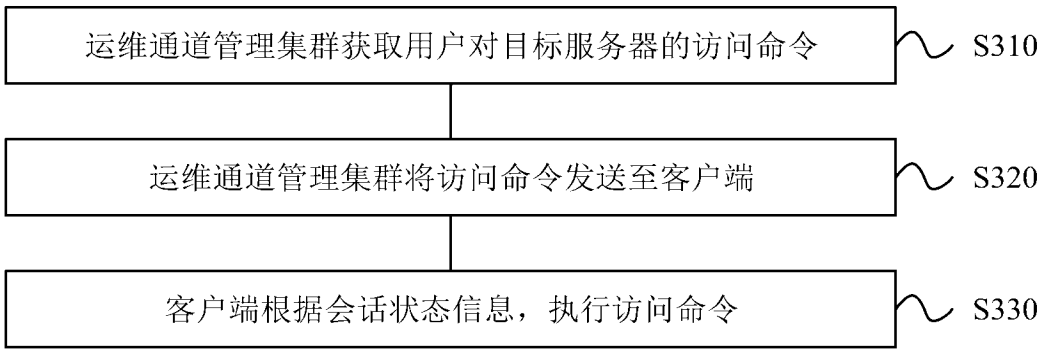
运维通道管理集群获取用户对目标服务器的访问命令
S310
运维通道管理集群将访问命令发送至客户端
S320
客户端根据会话状态信息，执行访问命令
S330

图 3

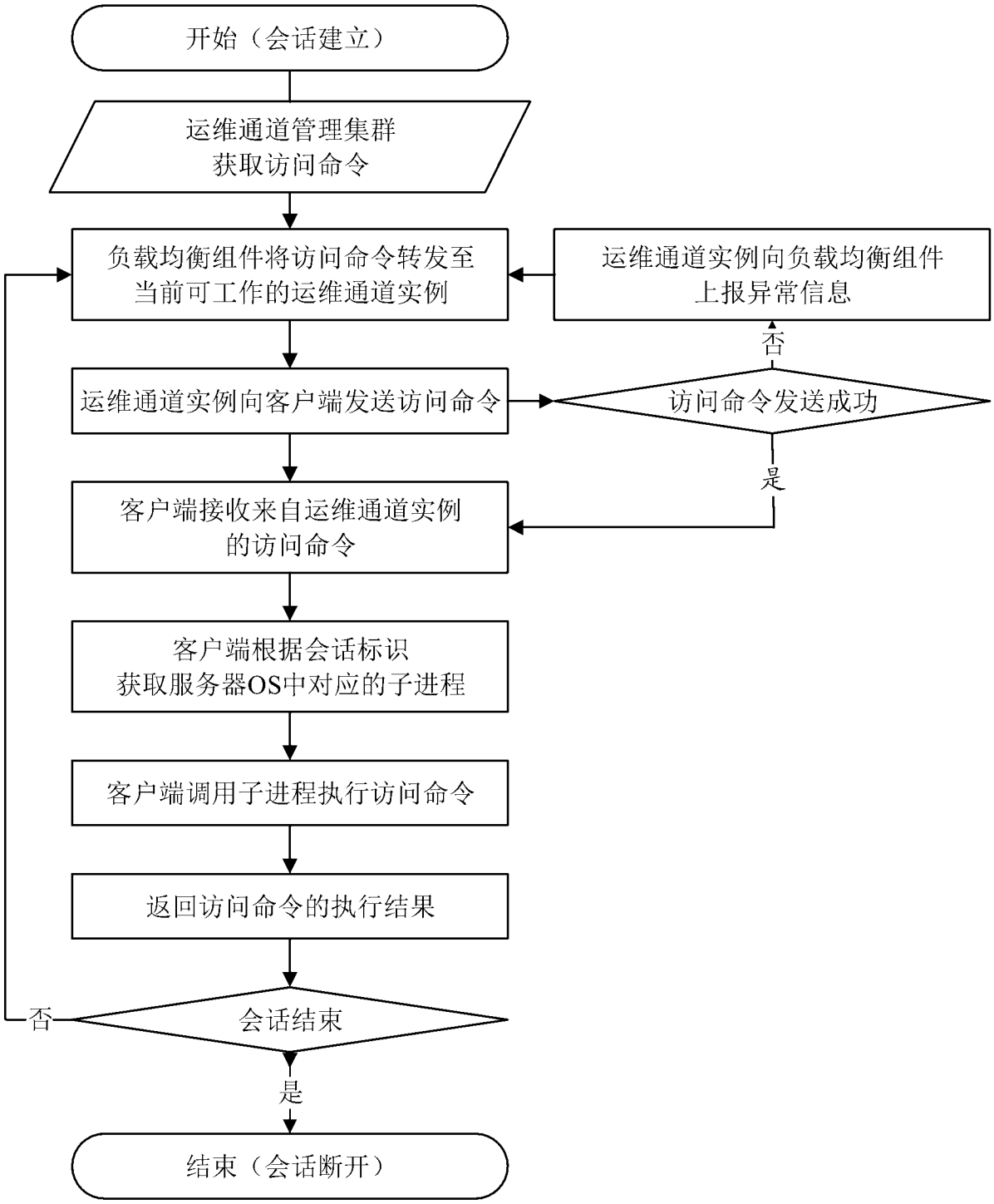
开始（会话建立）
运维通道管理集群
获取访问命令
负载均衡组件将访问命令转发至
当前可工作的运维通道实例
运维通道实例向负载均衡组件
上报异常信息
否
运维通道实例向客户端发送访问命令
访问命令发送成功
是
客户端接收来自运维通道实例
的访问命令
客户端根据会话标识
获取服务器OS中对应的子进程
客户端调用子进程执行访问命令
返回访问命令的执行结果
否
会话结束
是
结束（会话断开）

图 4

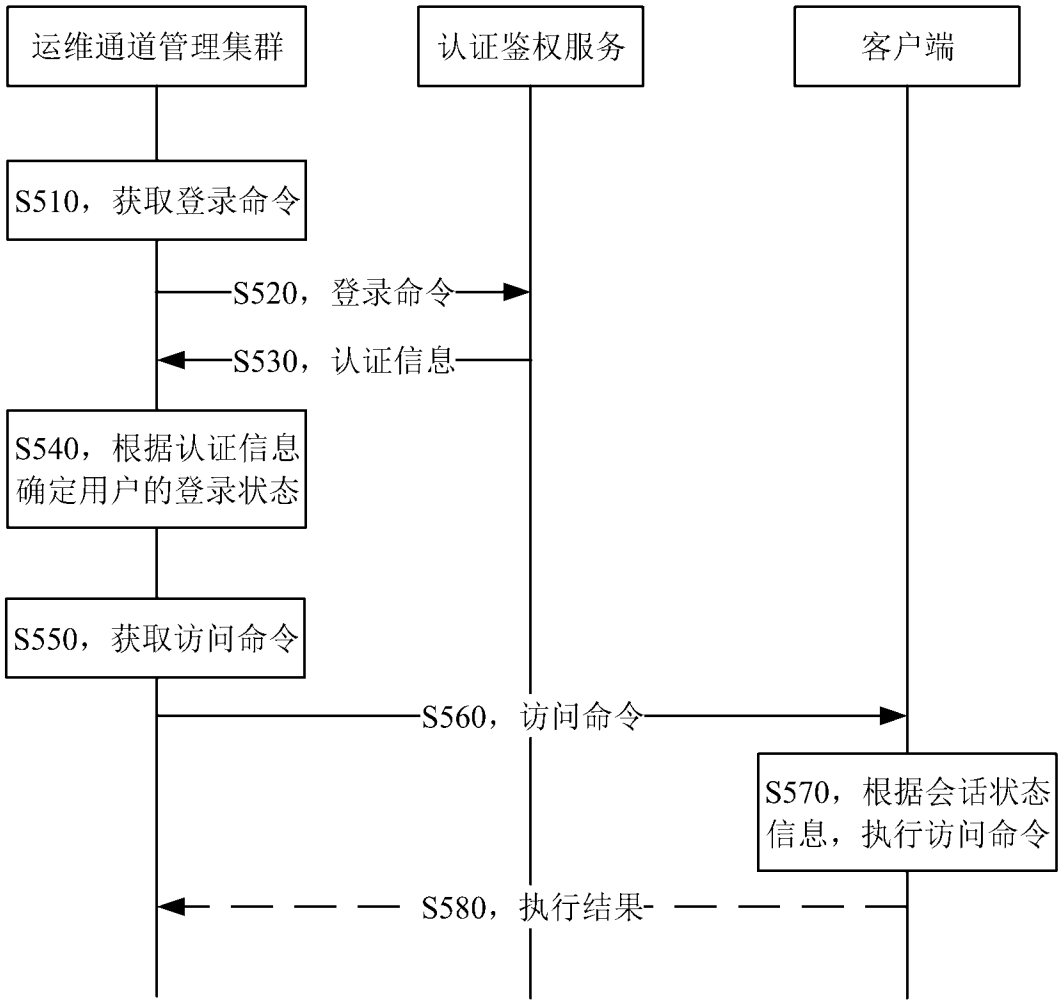
运维通道管理集群
认证鉴权服务
客户端
S510，获取登录命令
S520，登录命令
S530，认证信息
S540，根据认证信息确定用户的登录状态
S550，获取访问命令
S560，访问命令
S570，根据会话状态信息，执行访问命令
S580，执行结果

图 5

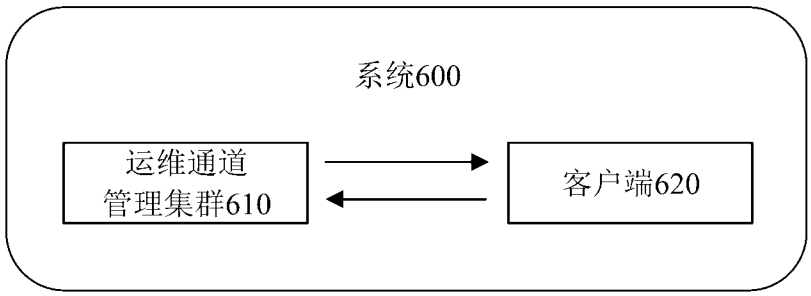
系统600
运维通道管理集群610
客户端620

图 6

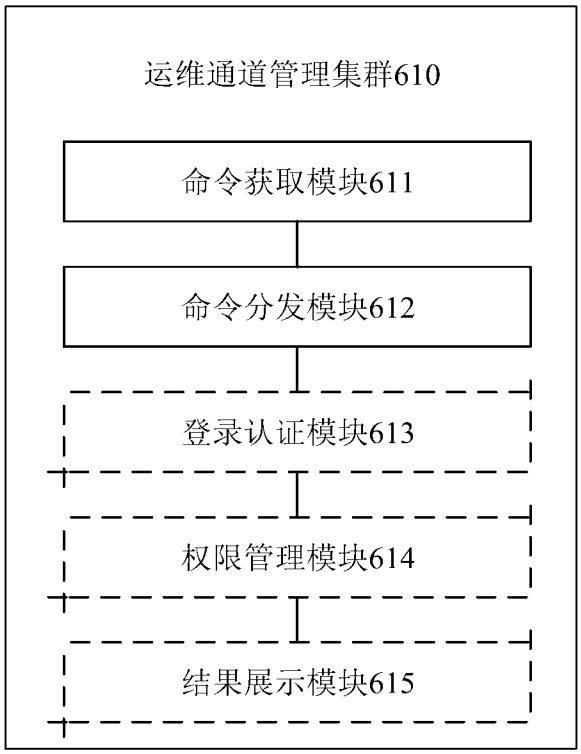
运维通道管理集群610
命令获取模块611
命令分发模块612
登录认证模块613
权限管理模块614
结果展示模块615

图 7

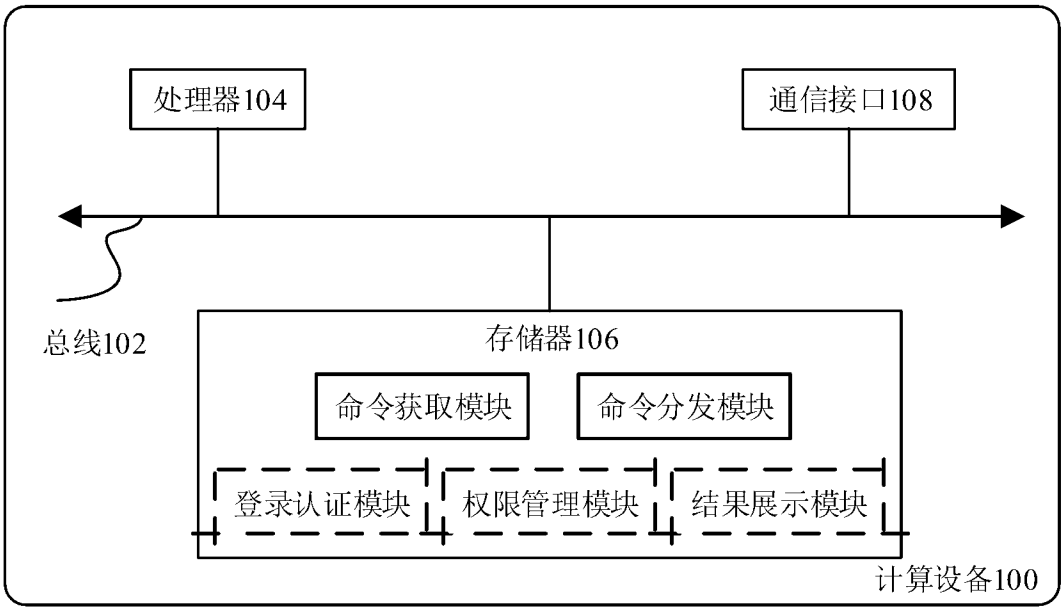
处理器104
通信接口108
总线102
存储器106
命令获取模块
命令分发模块
登录认证模块
权限管理模块
结果展示模块
计算设备100

图 8

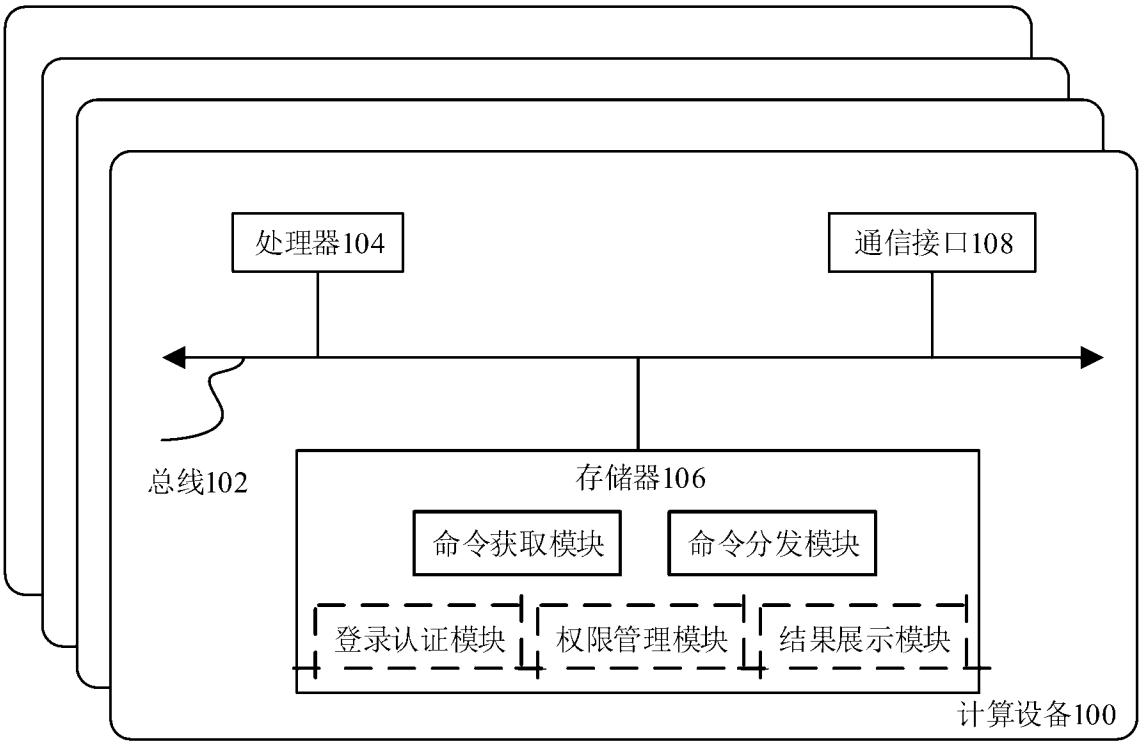
处理器104
通信接口108
总线102
存储器106
命令获取模块
命令分发模块
登录认证模块
权限管理模块
结果展示模块
计算设备100

图 9

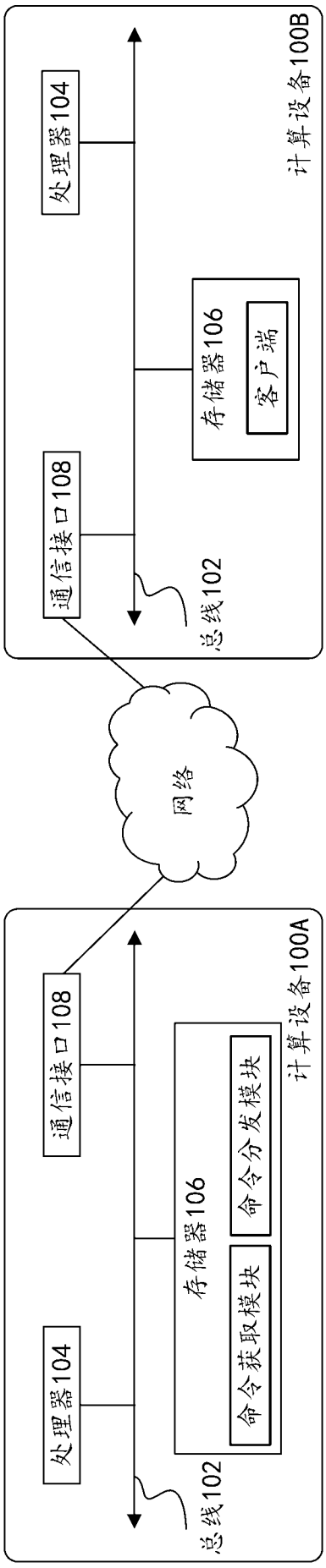
计算设备100A
处理器104
通信接口108
存储器106
命令获取模块
命令分发模块
总线102
网络
计算设备100B
处理器104
通信接口108
存储器106
客户端
总线102

图10

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2024/075967**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 41/50(2022.01)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)

IPC: H04L, G06F

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, VCN, ENTXT, DWPI, CNKI: 访问, 通道, 服务器, 客户端, 集群, 实例, 会话, 负载均衡, access, channel, server, client, cluster, instance, session, load balancing

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | CN 113114643 A (CHENGDU DBAPPSECURITY CO., LTD.) 13 July 2021 (2021-07-13)<br>description, paragraph [0028] | 1-23 |
| A | CN 111478937 A (NEW H3C INFORMATION SECURITY TECHNOLOGY CO., LTD.) 31 July 2020 (2020-07-31)<br>entire document | 1-23 |
| A | CN 115248922 A (HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.) 28 October 2022 (2022-10-28)<br>entire document | 1-23 |
| A | US 2021243250 A1 (NUTANIX, INC.) 05 August 2021 (2021-08-05)<br>entire document | 1-23 |

☐ 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
"D" document cited by the applicant in the international application
"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 |
|---|---|
| **06 May 2024** | **10 May 2024** |

| Name and mailing address of the ISA/CN | Authorized officer |
|---|---|
| **China National Intellectual Property Administration (ISA/CN)**<br>**China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** | Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2024/075967**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 113114643 A | 13 July 2021 | None | |
| CN 111478937 A | 31 July 2020 | None | |
| CN 115248922 A | 28 October 2022 | WO 2022227864 A1 | 03 November 2022 |
| US 2021243250 A1 | 05 August 2021 | None | |

# 国际检索报告

国际申请号
PCT/CN2024/075967

A. 主题的分类

H04L 41/50(2022.01)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)

IPC：H04L, G06F

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, VCN, ENTXT, DWPI, CNKI：访问，通道，服务器，客户端，集群，实例，会话，负载均衡，access, channel, server, client, cluster, instance, session, load balancing

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 113114643 A (成都安恒信息技术有限公司) 2021年7月13日 (2021 - 07 - 13)<br>说明书第[0028]段 | 1−23 |
| A | CN 111478937 A (新华三信息安全技术有限公司) 2020年7月31日 (2020 - 07 - 31)<br>全文 | 1−23 |
| A | CN 115248922 A (华为云计算技术有限公司) 2022年10月28日 (2022 - 10 - 28)<br>全文 | 1−23 |
| A | US 2021243250 A1 (NUTANIX, INC.) 2021年8月5日 (2021 - 08 - 05)<br>全文 | 1−23 |

☐ 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

“D” 申请人在国际申请中引证的文件

“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 |
|---|---|
| 2024年5月6日 | 2024年5月10日 |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局<br>中国北京市海淀区蓟门桥西土城路6号 100088 | 受权官员<br>吕淼<br>电话号码 (+86) 010−53961742 |

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/075967

| 检索报告引用的专利文件 | 公布日<br>(年/月/日) | 同族专利 | 公布日<br>(年/月/日) |
|---|---|---|---|
| CN 113114643 A | 2021年7月13日 | 无 | |
| CN 111478937 A | 2020年7月31日 | 无 | |
| CN 115248922 A | 2022年10月28日 | WO 2022227864 A1 | 2022年11月3日 |
| US 2021243250 A1 | 2021年8月5日 | 无 | |