(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
2018 年 5 月 31 日 (31.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/095240 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/110785

(22) 国际申请日: 2017 年 11 月 14 日 (14.11.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611052641.7 2016年11月24日 (24.11.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 秦海博 (QIN, Haibo); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, 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,

WO 2018/095240 A1

(54) **Title:** METHOD AND DEVICE FOR ESTABLISHING SECURE CHANNEL IN CLUSTER

(54) 发明名称: 一种在集群中建立安全通道的方法和装置

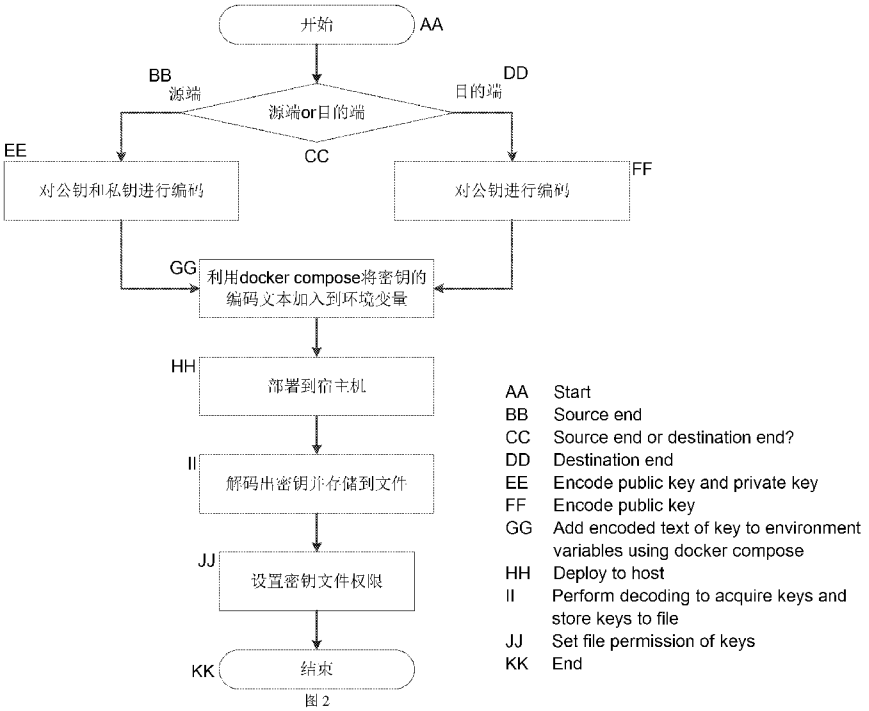


图 2

(57) **Abstract:** The application provides a method for establishing a secure channel in a cluster. The method is characterized by comprising steps of: acquiring a request for establishing a secure channel between specified user spaces in a specified cluster; generating a key pair of the secure channel corresponding to the request, wherein the key pair comprises a public key and a private key; transmitting, in corresponding manners corresponding to the user spaces, the keys needed by the specified user spaces to the specified user spaces; storing, in the specified user spaces, keys corresponding to the corresponding manners of the keys; and establishing, by means of the

[见续页]

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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))。

keys, a secure channel between the specified user spaces. The method provided by the application reduces the complexity for establishing a secure channel and improves the efficiency of establishing a secure channel. Further, in the application, keys are transmitted in forms corresponding to user spaces, thus reducing workload for establishing a secure channel in a cluster and further improving the efficiency of establishing a secure channel.

(57) 摘要：本申请提供一种在集群中建立安全通道的方法，特征在于，包括以下步骤：获取为指定集群内各指定的用户空间之间建立安全通道的请求；生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥；将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间；将所述密钥的相应形式所对应的密钥存储到所述各指定的用户空间；利用所述密钥在所述各个指定的用户空间之间建立安全通道。本申请提供的方法能够起到降低安全通道建立的复杂度，提高建立安全通道的效率的作用；以与用户空间相应的形式传送密钥，能够起到简化集群内建立安全通道的工作量作用，达到提高建立安全通道的效率的效果。

一种在集群中建立安全通道的方法和装置

本申请要求2016年11月24日递交的申请号为201611052641.7、发明名称为“一种在集群中建立安全通道的方法和装置”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

本申请涉及一种建立安全通道的方法，具体涉及一种在集群中建立安全通道的方法和装置，还涉及一种部署带有安全通道配置的docker容器的方法和装置，还涉及一种启动带有安全通道配置的docker容器的方法和装置。

背景技术

集群中通常会包含有不同的用户空间，包括容器（如docker容器），虚拟机和物理机，不同的用户空间之间或相同的用户空间之间需要通信交换信息，为了保证信息安全，需要在不同的用户空间之间或相同的用户空间之间建立安全通道进行信息交换，所述安全通道，通常采用非对称加密的方式来保证信息的安全性。

非对称加密的安全通道包含源端和目的端，源端是源端用户所处的用户空间，目的端为源端用户想要远程访问的用户空间。源端保存有公钥和私钥，目的端保存有公钥。

安全通道建立之后，源端用户可以以目的端用户的身份（权限由目的端的系统管理员来分配）来访问目的端，通道为单向，只能由源端访问目的端，反之则不成立。

现有的在集群内为不同的用户空间之间或相同的用户空间之间建立安全通道通常采用以下方式：

对于一条安全通道的源端和目的端，生成包含公钥和私钥的一对密钥对，通过现有的安全通道将所述密钥对存储到源端相应的文件中，通过现有的安全通道将公钥存储到目的端相应的文件中。这样集群中可能会存在多个密钥对分别对应不同的安全通道。特别地，对于用户空间为docker容器的用户空间，由于docker容器删除后，存储密钥的文件会被删除。重新部署同一个docker容器时还是需要通过安全通道登录到docker容器的宿主机重新传输存储相应的密钥。

可见现有在集群内建立安全通道的方式具有密钥管理和安全通道建立流程复杂，建立安全通道的工作量大，效率低下的问题。

发明内容

本申请提供一种在集群中建立安全通道的方法。本申请同时提供一种在集群中建立安全通道的装置；还提供一种部署带有安全通道配置需求的 docker 容器的方法，同时提供一种部署带有安全通道配置需求的 docker 容器的装置；还提供一种启动带有安全通道配置的 docker 容器的方法，同时提供一种启动带有安全通道配置的 docker 容器的装置。

本申请提供的一种在集群中建立安全通道的方法，包括以下步骤：

获取为指定集群内各指定的用户空间之间建立安全通道的请求；

生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥；

将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间；

将所述密钥的相应形式所对应的密钥存储到所述各指定的用户空间；

利用所述密钥在所述各个指定的用户空间之间建立安全通道。

可选地，所述用户空间包括 docker 容器；

相应地，所述将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间包括：

对各指定的 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

将所述与各个 docker 容器的安全通道的属性相对应的密钥的编码文本放入相应 docker 容器的环境变量中；

将所述带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机；

所述将所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间包括：

所述各指定的 docker 容器启动后，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥；

将所述解码得到的密钥存储到相应的指定的 docker 容器中。

可选地，所述安全通道的属性包括：安全通道的源端；

相应地，所述密钥的编码文本包括公钥的编码文本和私钥的编码文本。

可选地，所述安全通道的属性包括：安全通道的目的端；

相应地，所述密钥的编码文本包括公钥的编码文本。

可选地，所述用户空间包括虚拟机或物理机；

相应地，所述将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间包括：

将与各指定的虚拟机或物理机的安全通道的属性相对应的密钥传送到相应的虚拟机或物理机；

所述将所述所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间包括：

将与各指定的虚拟机或物理机的安全通道的属性相对应的密钥存储到相应的虚拟机或物理机。

可选地，所述安全通道包括 SSH 安全通道。

可选地，所述密钥对为一个密钥对。

本申请提供的一种部署带有安全通道配置需求的 docker 容器的方法，包括以下步骤：

获取部署带有安全通道配置需求的 docker 容器的请求；

对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放入该 docker 容器的环境变量中；

将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

可选地，所述 docker 容器的安全通道的属性包括安全通道的源端，

相应地，所述密钥的编码文本包括公钥的编码文本和私钥的编码文本。

可选地，所述 docker 容器的安全通道的属性包括安全通道的目的端，

相应地，所述密钥的编码文本包括公钥的编码文本。

可选地，所述安全通道包括 SSH 安全通道。

本申请提供的一种启动带有安全通道配置的 docker 容器的方法，包括以下步骤：

启动所述 docker 容器；

解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥；

将所述密钥存储到所述 docker 容器。

本申请提供的一种在集群中建立安全通道的装置，包括：

获取单元，用于获取在指定集群内各指定的用户空间之间建立安全通道的请求；

密钥生成单元，用于生成所述请求所对应的安全通道的密钥对，所述密钥对包括公

钥和私钥；

传送单元，用于将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间；

存储单元，用于将所述所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间；

建立单元，用于利用所述密钥在所述各个指定的用户空间之间建立安全通道。

可选地，所述用户空间包括 docker 容器，相应地，所述传送单元，包括：

编码子单元，用于对各指定的 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

放入子单元，用于将所述与各个 docker 容器的安全通道的属性相对应的密钥的编码文本放入相应 docker 容器的环境变量中；

部署子单元，用于将所述带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机；

所述存储单元包括：

解码子单元，用于所述各指定的 docker 容器启动后，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥；

存储子单元，用于将所述解码得到的密钥存储到相应的指定的 docker 容器中。

可选地，所述密钥生成单元，具体用于生成所述请求所对应的安全通道的一个密钥对，所述密钥对包括公钥和私钥。

本申请提供的一种部署带有安全通道配置需求的 docker 容器的装置，包括：

获取单元，用于获取部署带有安全通道配置需求的 docker 容器的请求；

编码单元，用于对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

配置单元，用于将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放入该 docker 容器的环境变量中；

部署单元，用于将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

本申请提供的一种启动带有安全通道配置的 docker 容器的装置，包括：

启动单元，用于启动所述 docker 容器；

解码单元，用于解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥；

存储单元，用于将所述密钥存储到所述 docker 容器。

与现有技术相比，本申请提供的一种在集群中建立安全通道的方法具有以下优点：

在集群中不同的用户空间之间和同样的用户空间之间建立使用密钥对的安全通道时，统一生生密钥对，能够起到降低安全通道建立的复杂度，提高建立安全通道的效率的作用；以与用户空间相应的形式传送密钥，能够起到简化集群内建立安全通道的工作量作用，达到提高建立安全通道的效率的效果。

与现有技术相比，本申请提供的一种部署带有安全通道配置需求的 docker 容器的方法具有以下优点：

部署 docker 容器时，利用环境变量传送安全通道的密钥，能够起到简化安全通道建立的流程的作用，达到提高建立安全通道的效率的效果。

与现有技术相比，本申请提供的一种启动带有安全通道配置的 docker 容器的方法具有以下优点：

启动后解码还原安全通道的密钥并存储，能够起到简化安全通道建立的流程的作用，达到提高建立安全通道的效率的效果。

附图说明

图 1 为本申请第一实施例一种在集群中建立安全通道的方法的流程示意图；

图 2 为本申请第一实施例一种在集群中建立安全通道的方法的为集群中 docker 容器建立安全通道的方法的示意图；

图 3 为本申请第二实施例一种部署带有安全通道配置需求的 docker 容器的方法的流程示意图；

图 4 为本申请第三实施例一种启动带有安全通道配置的 docker 容器的方法的流程示意图；

图 5 为本申请第四实施例在集群中建立安全通道的装置的结构框图；

图 6 为本申请第五实施例一种部署带有安全通道配置需求的 docker 容器的装置的结构框图；

图 7 为本申请第六实施例一种启动带有安全通道配置的 docker 容器的装置的结构框图。

具体实施方式

在下面的描述中阐述了很多具体细节以便于充分理解本申请。但是本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似推广，因此本申请不受下面公开的具体实施的限制。

本申请第一实施例提供一种在集群中建立安全通道的方法，其流程示意图如图 1 所示，该实施例包括以下步骤：

步骤 S101，获取为指定集群内各指定的用户空间建立安全通道的请求。

当需要在计算机集群内不同的用户空间之间建立安全的通信通道时，获取这一请求。所述用户空间既可以是物理计算机（简称物理机），也可以是虚拟计算机（简称虚拟机），还可以是容器，如 docker 容器（简称 docker）。

本实施例以在集群中建立 SSH 安全通道为例进行说明。SSH（Secure Shell）为建立在应用层和传输层基础上的安全协议，使用非对称的 RSA 加密算法来实现计算机之间的安全通信。一条 SSH 通道包含源端、目的端、源端用户、目的端用户四个要素，源端用户是建立通道的发起方，源端是源端用户所用的计算机，目的端为源端用户想要远程操控的目标设备，通道建立之后，源端用户可以目的端用户的身份（权限由目的端的系统管理员来分配）来操作目的端，通道为单向，只能由源端操作目的端，反之则不成立。

步骤 S102，生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥。

为了实现通信的安全性，通常需要采用不对称加密的技术对用于通信的通道进行加密，不对称加密需要一对由私有密钥（简称私钥）和公有密钥（简称公钥）组成的密钥对。本实施例中，以采用 RSA 算法的公钥和私钥为例进行相应的说明。

对于集群中多个用户空间之间建立安全通道的情况，除了每个通道采用不同的密钥对意外，还可以采用相同的密钥对，即仅采用一个密钥对，这样能够简化对安全通道的管理，方便部署，提高部署的效率，降低维护工作量。

当获取到建立安全通道的请求后，采用 RSA 算法，为所述待建立的安全通道生成一对密钥。所述密钥对包括一个公钥和一个私钥。

例如，对于 Unix 操作系统，可以利用以下命令生成长度为 1024 位的 RSA 算法私钥并将生成的私钥保存到“privatekeyfile”文件内：

openssl genrsa -3 -out privatekeyfile 1024

生成私钥后，可以根据所生成的私钥，利用以下命令生成对应的公钥,并将所生成的公钥保存到 publickeyfile 文件：

ssh-keygen -f privatekeyfile －y > publickeyfile

步骤 S103，将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间。

各个用户空间作为安全通道的属性不同，其所需要的密钥也不相同，作为安全通道的源端的用户空间，其所需要的密钥为完整的密钥对，即公钥和私钥都需要。作为安全通道的目的端的用户空间，仅需要密钥对中的公钥即可。

进将于安全通道的属性相关的密钥传送给相应的用户空间，能够确保网络的安全性。

对于用户空间为 docker 容器的情况，采用以下步骤将其所需要的密钥传送到各个指定的 docker 容器：

根据各个 docker 容器的安全通道的属性，利用文本编码工具，将与各个 docker 容器的安全通道的属性相对应的密钥进行编码，得到所述密钥的编码文本。

例如，对于操作系统为 Unix 的情况，可以采用下述命令对前面步骤中生成的 RSA 算法的私钥进行编码：

base64 -i pkeyfile

其中，pkeyfile 为保存有所述私钥的文件，上述命令的输出即为所述私钥的编码文本，例如对于 pkeyfile 的内容为“abcdefg”的情况，即私钥为“abcdefg”，执行上述命令可以得到所述私钥的编码文本“YWJjZGVmZw==”。

对公钥进行编码的方式与对私钥进行编码的方式类似，在此不做赘述。

对于作为 SSH 安全通道源端的 docker 容器，对所生成的公钥和私钥都进行文本编码，生成公钥的编码文本和私钥的编码文本；对于仅作为目的端的 docker 容器，可以仅对公钥进行文本编码生成公钥的编码文本。

对于所述各个用户空间公用一对密钥来建立安全通道的情况，仅需对密钥对的公钥或私钥进行一次编码，对于后续其他 docker 容器，只需要直接利用此前已经编码的密钥的编码文本即可。

将所述与各个 docker 容器的安全通道的属性相对应的密钥放入相应 docker 容器的环境变量中。即公钥的编码文本需要被放入到所有待部署的需要建立 SSH 安全通道的 docker 容器的环境变量中，私钥的编码文本仅需要放入到待部署的作为源端的 docker 容器的环境变量中。

对于在 Unix 操作系统上生成 docker 容器的情况，可以采用下述方式将生成的 RSA 算法的私钥的编码文本传给 docker 容器的环境变量 SSH_PRIVATE_KEY

利用 docker compose 工具，生成 docker 容器配置文件 docker-compose.yml 文件,在需

要建立 SSH 安全通道的 docker 容器所对应的环境变量 environment 中，将变量 SSH_PRIVATE_KEY 所对应的值设置为前述生成的 RSA 算法的私钥的编码文本：

environment:

SSH_PRIVATE_KEY: 'YWJjZGVmZw=='

此处仅给出了 docker 容器配置文件 docker-compose.yml 文件中与密钥相关的主要参数的设置情况，完整的 docker 容器配置文件 docker-compose.yml 文件请参考 docker compose 工具的相关文档进行确定。

将公钥的编码文本加入到 docker 容器的环境变量中的方式与将私钥的编码文本加入到 docker 容器的环境变量中类似，在此不做赘述。

将所述带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机。所述宿主机包括集群中需要部署 docker 容器的物理机甚至虚拟机，并且所述 docker 容器需要与其他用户空间建立安全通道。

对于 Unix 操作系统，宿主机上已经安装运行了 docker 容器的后台守护进程 docker deamon 的情况下，可以利用下述方式将配置了环境变量的 docker 容器部署到宿主机上：

export DOCKER_HOST=tcp://10.1.1.1:4243

docker-compose up -d

其中 expost 命令设置宿主机信息，“10.1.1.1”为宿主机的 IP 地址，“4243”为宿主机上 docker 容器守护进程 docker deamon 的端口 ，docker-compose 命令按照 docker-compose.yml 文件的描述远程部署 docker 容器。docker-compose.yml 包含有所述 docker 容器的黄静变量，所述环境变量中哦哦那个包含有密钥的编码文本。

此处仅给出部署 docker 容器主要的相关参数，完整的命令可以根据 docker 容器部署的实际情况和 docker 容器相关的说明文档确定。此外也可以采用其他方式部署 docker 容器。

对于用户空间为物理机或虚拟机的情况，可以直接将密钥存入文件中，再将内容为密钥的文件发送到相应的各个用户空间，即将内容为公钥的文件发送到所有需要建立 SSH 安全通道的指定的物理机和虚拟机，将内容为私钥的文件发送到所有需要建立 SSH 安全通道，并作为 SSH 安全通道的源端的指定的物理机和虚拟机。

步骤 S104，将所述密钥的相应形式所对应的密钥存储到所述各指定的用户空间。

用户空间不同相应的处理也不尽相同。

对于用户空间为 docker 容器的情况，各个宿主机上部署了所述 docker 容器后，启动

所述 docker 容器时，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥。

例如，对于部署在 Unix 操作系统上的的 docker 容器，可以采用下述方式得对前面步骤中生成的相应的环境变量进行解码：

首先利用下述命令将包含有密钥的编码文本的环境变量 SSH_PRIVATE_KEY 输出到文件 private_key_file：

SSH_PRIVATE_KEY > private_key_file

再利用下述命令对所述 private_key_file 所包含的私钥的编码文本进行解码：

base64 -D private_key_file

执行上述命令的输出即为私钥，如 private_key_file 文件的内容为“YWJjZGVmZw==”，执行上述命令即可解码得到私钥的值：“abcdefg”。

对公钥的编码文本进行解码得到公钥的方式与对私钥的编码文本进行解码得到私钥的方式类似，在此不做赘述。

将所述解码得到的密钥以适当的形式存储到相应的指定的 docker 容器中。如将解码得到的私钥存入作为源端的 docker 容器的用户目录下的.ssh\id_rsa 文件中，将解码得到的公钥存入作为源端的 docker 容器的用户目录下的.ssh\id_rsa.pub 文件中。对于作为目的端的 docker 容器，将解码得到的公钥存入作为目的端的 docker 容器的用户目录下的.ssh\id_rsa.pub 文件中

对于用户空间为物理机或虚拟机的情况，密钥文件被传送到指定的物理机或虚拟机后，将所述内容为相应密钥的文件保存到相应的位置。

例如对于作为 SSH 安全通道源端的物理机或虚拟机，将内容为公钥的文件保存为使用所述安全通道的用户的.ssh\id_rsa.pub 文件，将内容为私钥的文件保存为使用所述安全通道的用户的.ssh\id_rsa 文件。对于作为 SSH 安全通道目的端的物理机或虚拟机，将内容为公钥的文件保存为使用所述 SSH 安全通道的用户的.ssh\zuthorized_keys 文件。

将与用户空间的通道属性相对应的密钥保存到用户空间后，还可以对所保存的密钥进行权限管理，仅允许被授权的用户能够访问所述密钥，以加强安全性。

步骤 S105，利用所述密钥在所述各个指定的用户空间之间建立安全通道。

建立 SSH 安全通道所需的密钥被存储到相应的用户空间后，可以根据相应的安全协议，建立安全通道进行通信。

下面再以为集群中的某一 docker 容器建立 SSH 安全通道为例进行简要说明，如图 2

所示：

集群内需要建立的 SSH 安全通道所需的 RSA 密钥已经生成，当需要为集群中某一 docker 容器建立 SSH 安全通道时，首先根据该 docker 容器的 SSH 安全通道属性，对相应的密钥进行编码。如果该 docker 容器需要作为集群内 SSH 安全通道的源端，对公钥和私钥进行编码，得到公钥的编码文本和私钥的编码文本；如果该 docker 容器需要作为集群内 SSH 安全通道的目的端，对公钥进行编码，得到公钥的编码文本。

在利用 docker compose 工具将所得到的相应的密钥的编码文本加入到 docker 容器的环境变量中。

将带有上述环境变量的 docker 容器部署到集群内预先指定的宿主机。启动该 docker 容器后，对环境变量中的相应的密钥的编码文本进行解码得到相应的密钥。将相应的密钥存储到相应的 docker 容器的相应文件中。例如若所述 docker 容器为 SSH 安全通道的源端，则将公钥存储到该 docker 容器的相应用户的.ssh\id_rsa.pub 文件中，将私钥存储到该 docker 容器的相应用户的.ssh\id_rsa 文件；若所述 docker 容器为 SSH 安全通道的目的端，则将将公钥存储到该 docker 容器的相应用户的.ssh\id_rsa.pub 文件中。

将相应的密钥存储到该 docker 容器的相应文件后，可以对所述密钥文件设置相应的权限，使得仅获得授权的相应用户能够访问所述密钥文件，增加安全性。

至此成功将建立 SSH 安全通道所需的密钥部署到了该 docker 容器，可以和该 docker 容器建立相应的 SSH 安全通道进行通信。

以上为本申请的一种在集群中建立安全通道的方法的实施例，该方法在集群中各个用户空间之间建立安全通道时，统一生成密钥，能够起到降低安全通道建立的复杂度，提高建立安全通道的效率的作用；以与用户空间相应的形式传送密钥，能够起到简化集群内建立安全通道的工作量作用，达到提高建立安全通道的效率的效果。

本申请第二实施例提供一种部署带有安全通道配置需求的 docker 容器的方法，其流程示意图如图 3 所示，包括以下步骤：

步骤 S201，获取部署带有安全通道配置需求的 docker 容器的请求.

当需要在集群中为不同的用户空间之间建立安全通道时，所述用户空间包括 docker 容器，即 docker 容器可以作为安全通道的源端也可以作为目的端。

本步骤获取部署 docker 容器到集群内指定的宿主机的请求，所述 docker 容器需要与集群内其他用户空间建立安全通道。本实施例中以 SSH 安全通道为例进行说明。所述 SSH 安全通道所需的密钥为 RSA 密钥，已经生成。

步骤 S202，对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本。

本步骤中，对于作为 SSH 安全通道源端的 docker 容器，将公钥和私钥都进行编码得到公钥的编码文本和私钥的编码文本。对于作为 SSH 安全通道目的端的 docker 容器，将公钥进行编码得到公钥的编码文本。具体的操作可以参考本申请第一实施例中步骤 S103 中的描述，在此不做赘述。

步骤 S203，将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放入该 docker 容器的环境变量中。

本步骤的具体操作可以参考本申请第一实施例中步骤 S103 中的描述，在此不做赘述。

步骤 S204，将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

本步骤的具体操作可以参考本申请第一实施例中步骤 S103 中的描述，在此不做赘述。

本申请第三实施例提供一种启动带有安全通道配置的 docker 容器的方法，其流程示意图如图 4 所示，包括以下步骤：

步骤 S301，启动所述 docker 容器。

所述带有安全通道配置的 Docker 容器被部署到宿主机后，启动所述 docker 容器。所述安全通道配置包括所需的密钥，所述密钥以编码文本的形式存在于该 docker 容器的环境变量中。所述安全通道为 SSH 安全通道。所述密钥为 RSA 算法密钥。

步骤 S302，解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥。

启动所述带有安全通道配置的 docker 容器后，将所述 docker 容器的黄静变量中所携带的密钥的编码文本解码得到相应的密钥。

本步骤的具体操作可以参考本申请第一实施例步骤 S104 中相应的描述，在此不再赘述。

步骤 S303，将所述密钥存储到所述 docker 容器。

将解码得到的密钥存入 docker 容器的相应文件中。具体操作卡伊参考本申请第一实施例步骤 S104 中相关的描述，在此不再赘述。

本申请第四实施例提供一种在集群中建立安全通道的装置，其结构框图如图 5 所述，包括：获取单元 U401，密钥生成单元 U402，传送单元 U403，存储单元 U404 和建立单元 U405。

所述获取单元 U401，用于获取在指定集群内各指定的用户空间之间建立安全通道的请求。

所述用户空间包括 docker 容器。

所述密钥生成单元 U402，用于生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥。

所述密钥生成单元，可以具体用于生成所述请求所对应的安全通道的一个密钥对，所述密钥对包括公钥和私钥。

所述传送单元 U403，用于将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间。

对于所述用户空间为 docker 容器的情况，所述传送单元可以包括：编码子单元，放入子单元和部署子单元。

所述编码子单元，用于对各指定的 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

所述放入子单元，用于将所述与各个 docker 容器的安全通道的属性相对应的密钥的编码文本放入相应 docker 容器的环境变量中；

所述部署子单元，用于将所述带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机；

所述存储单元 U404，用于将所述所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间。

对于对于所述用户空间为 docker 容器的情况，所述存储单元可以包括：解码子单元和存储子单元。

所述解码子单元，用于所述各指定的 docker 容器启动后，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥；

所述存储子单元，用于将所述解码得到的密钥存储到相应的指定的 docker 容器中。

所述建立单元 U405，用于利用所述密钥在所述各个指定的用户空间之间建立安全通道。

本申请第五实施例提供一种部署带有安全通道配置需求的 docker 容器的装置，其结构框图如图 6 所述，包括：获取单元 U501，编码单元 U502，配置单元 U503 和部署单元 U504。

所述获取单元 U501，用于获取部署带有安全通道配置需求的 docker 容器的请求。

所述编码单元 U502，用于对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本。

所述配置单元 U503，用于将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放入该 docker 容器的环境变量中。

所述部署单元 U504，用于将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

本申请第六实施例提供一种启动带有安全通道配置的 docker 容器的装置，其结构框图如图 7 所述，包括：启动单元 U601，解码单元 U602 和存储单元 U603。

所述启动单元 U601，用于启动所述 docker 容器；

所述解码单元 U602，用于解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥；

所述存储单元 U603，用于将所述密钥存储到所述 docker 容器。

本申请虽然以较佳实施例公开如上，但其并不是用来限定本申请，任何本领域技术人员在不脱离本申请的精神和范围内，都可以做出可能的变动和修改，因此本申请的保护范围应当以本申请权利要求所界定的范围为准。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、 输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

1、计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、 程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、 其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

2、本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

权 利 要 求 书

1.一种在集群中建立安全通道的方法，特征在于，包括以下步骤：

获取为指定集群内各指定的用户空间之间建立安全通道的请求；

生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥；

将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间；

将所述密钥的相应形式所对应的密钥存储到所述各指定的用户空间；

利用所述密钥在所述各指定的用户空间之间建立安全通道。

2.根据权利要求 1 所述的在集群中建立安全通道的方法，其特征在于，所述用户空间包括 docker 容器；

相应地，所述将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间包括：

对各指定的 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

将所述与各个 docker 容器的安全通道的属性相对应的密钥的编码文本放入相应 docker 容器的环境变量中；

将带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机；

所述将所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间包括：

所述各指定的 docker 容器启动后，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥；

将所述解码得到的密钥存储到相应的指定的 docker 容器中。

3.根据权利要求 2 所述的在集群中建立安全通道的方法，其特征在于，所述安全通道的属性包括：安全通道的源端；

相应地，所述密钥的编码文本包括公钥的编码文本和私钥的编码文本。

4.根据权利要求 2 所述的在集群中建立安全通道的方法，其特征在于，所述安全通道的属性包括：安全通道的目的端；

相应地，所述密钥的编码文本包括公钥的编码文本。

5.根据权利要求 1 所述的在集群中建立安全通道的方法，其特征在于，所述用户空间包括虚拟机或物理机；

相应地，所述将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间包括：

将与各指定的虚拟机或物理机的安全通道的属性相对应的密钥传送到相应的虚拟机或物理机；

所述将所述所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间包括：

将与各指定的虚拟机或物理机的安全通道的属性相对应的密钥存储到相应的虚拟机或物理机。

6.根据权利要求 1 所述的在集群中建立安全通道的方法，其特征在于，所述安全通道包括 SSH 安全通道。

7.根据权利要求 1 所述的在集群中建立安全通道的方法，其特征在于，所述密钥对为一个密钥对。

8.一种部署带有安全通道配置需求的 docker 容器的方法，特征在于，包括以下步骤：

获取部署带有安全通道配置需求的 docker 容器的请求；

对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放入该 docker 容器的环境变量中；

将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

9.根据权利要求 8 所述的部署带有安全通道配置需求的 docker 容器的方法，其特征在于，所述 docker 容器的安全通道的属性包括安全通道的源端，

相应地，所述密钥的编码文本包括公钥的编码文本和私钥的编码文本。

10.根据权利要求 8 所述的部署带有安全通道配置需求的 docker 容器的方法，其特征在于，所述 docker 容器的安全通道的属性包括安全通道的目的端，

相应地，所述密钥的编码文本包括公钥的编码文本。

11.根据权利要求 8 所述的部署带有安全通道配置需求的 docker 容器的方法，其特征在于，所述安全通道包括 SSH 安全通道。

12.一种启动带有安全通道配置的 docker 容器的方法，特征在于，包括以下步骤：

启动所述 docker 容器；

解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥；

将所述密钥存储到所述 docker 容器。

13.一种在集群中建立安全通道的装置，特征在于，包括：

获取单元，用于获取在指定集群内各指定的用户空间之间建立安全通道的请求；

密钥生成单元，用于生成所述请求所对应的安全通道的密钥对，所述密钥对包括公钥和私钥；

传送单元，用于将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间；

存储单元，用于将所述所需的密钥的相应形式所对应的密钥存储到所述各指定的用户空间；

建立单元，用于利用所述密钥在所述各指定的用户空间之间建立安全通道。

14.根据权利要求 13 所述的在集群中建立安全通道的装置，其特征在于，所述用户空间包括 docker 容器，相应地，所述传送单元，包括：

编码子单元，用于对各指定的 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

放入子单元，用于将所述与各个 docker 容器的安全通道的属性相对应的密钥的编码文本放入相应 docker 容器的环境变量中；

部署子单元，用于将带有所述环境变量的各指定的 docker 容器部署到所述集群内预先指定的各宿主机；

所述存储单元包括：

解码子单元，用于所述各指定的 docker 容器启动后，对所述各指定的 docker 容器的环境变量中包含的密钥的编码文本进行解码得到密钥；

存储子单元，用于将所述解码得到的密钥存储到相应的指定的 docker 容器中。

15.根据权利要求 13 所述的在集群中建立安全通道的装置，其特征在于，所述密钥生成单元，具体用于生成所述请求所对应的安全通道的一个密钥对，所述密钥对包括公钥和私钥。

16.一种部署带有安全通道配置需求的 docker 容器的装置，特征在于，包括：

获取单元，用于获取部署带有安全通道配置需求的 docker 容器的请求；

编码单元，用于对所述 docker 容器的安全通道的属性相对应的密钥进行编码，得到与各个 docker 容器的安全通道的属性相对应的密钥的编码文本；

配置单元，用于将与所述 docker 容器的安全通道的属性相对应的密钥的编码文本放

入该 docker 容器的环境变量中；

部署单元，用于将带有所述环境变量的 docker 容器部署到预先指定的宿主机。

17.一种启动带有安全通道配置的 docker 容器的装置，特征在于，包括：

启动单元，用于启动所述 docker 容器；

解码单元，用于解码所述 docker 容器的环境变量中所包含的密钥的编码文本，得到密钥；

存储单元，用于将所述密钥存储到所述 docker 容器。

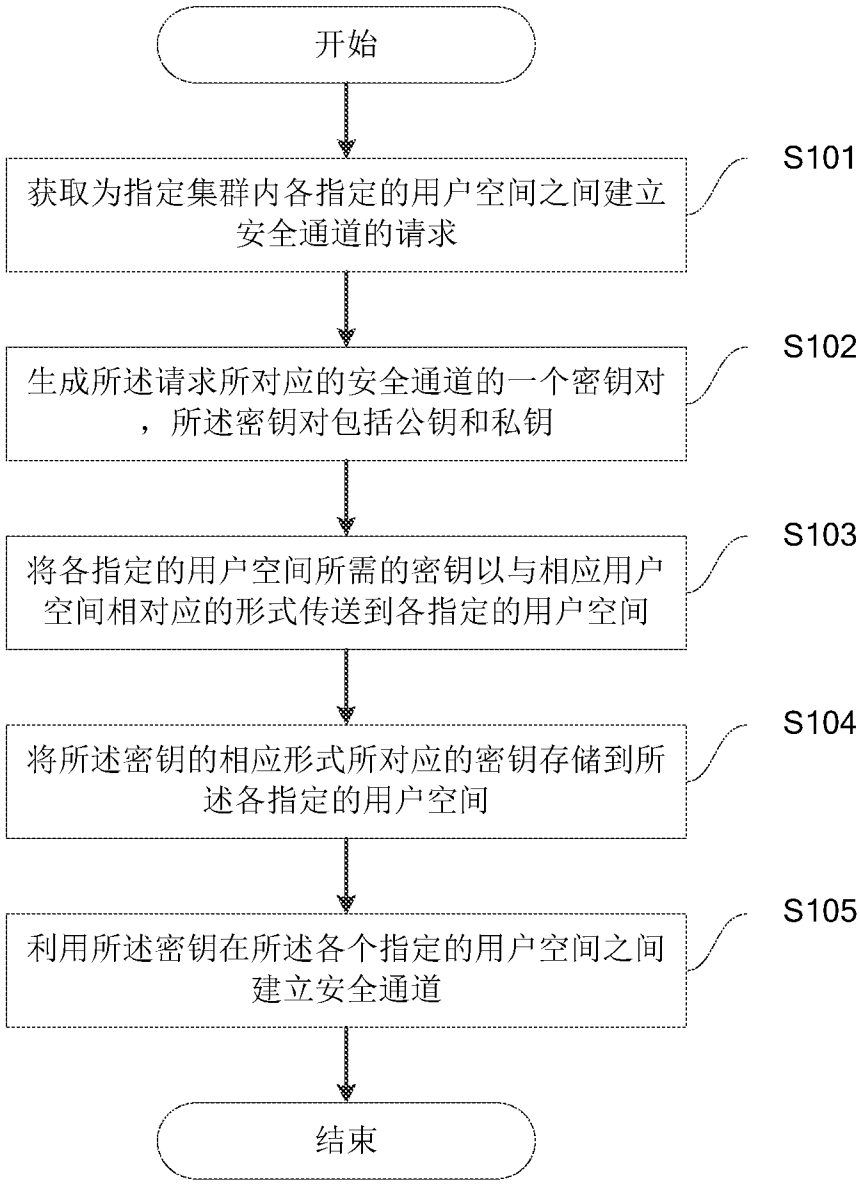

开始
获取为指定集群内各指定的用户空间之间建立安全通道的请求
S101
生成所述请求所对应的安全通道的一个密钥对，所述密钥对包括公钥和私钥
S102
将各指定的用户空间所需的密钥以与相应用户空间相对应的形式传送到各指定的用户空间
S103
将所述密钥的相应形式所对应的密钥存储到所述各指定的用户空间
S104
利用所述密钥在所述各个指定的用户空间之间建立安全通道
S105
结束

图 1

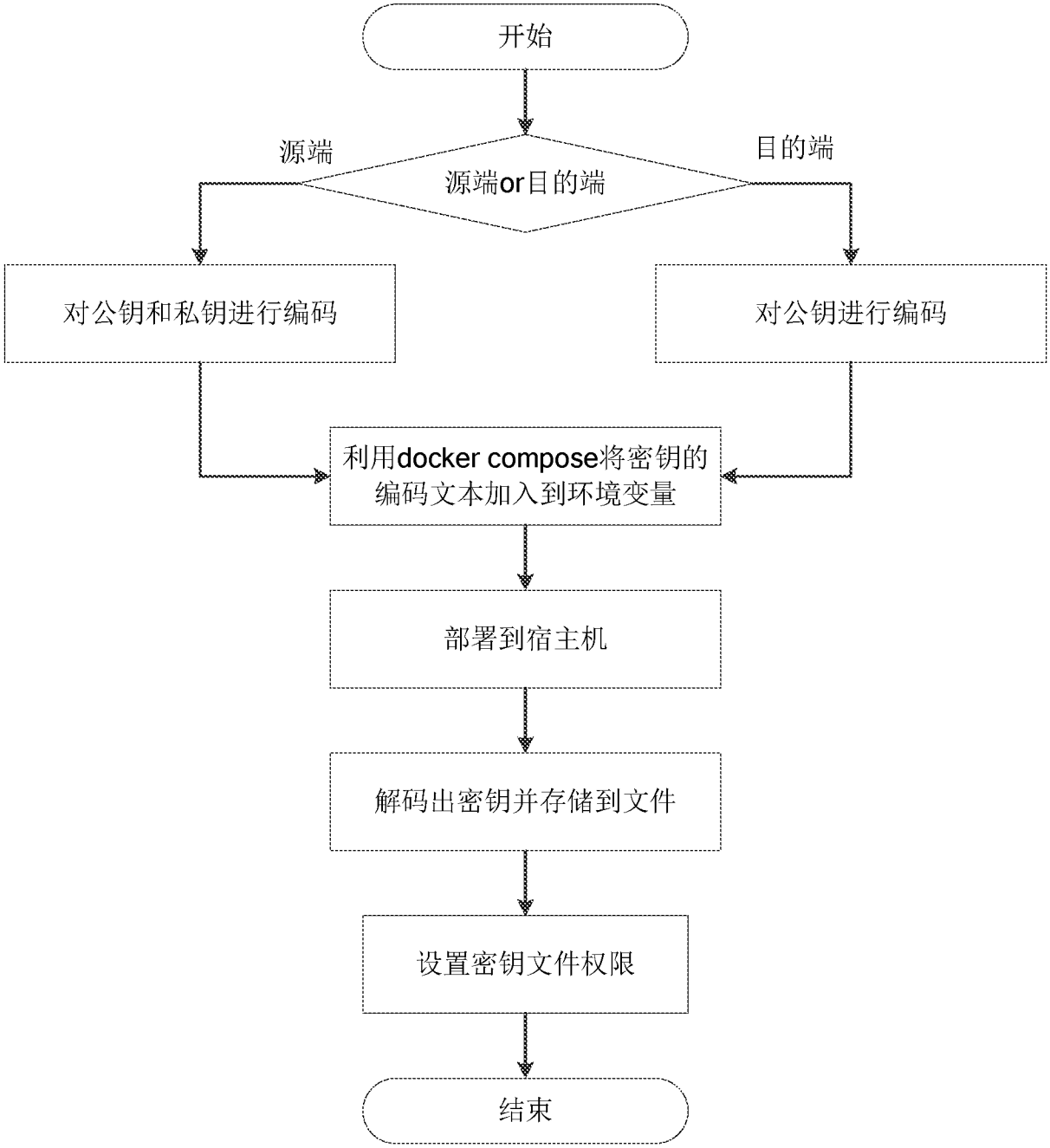

开始
源端
源端or目的端
目的端
对公钥和私钥进行编码
对公钥进行编码
利用docker compose将密钥的编码文本加入到环境变量
部署到宿主机
解码出密钥并存储到文件
设置密钥文件权限
结束

图 2

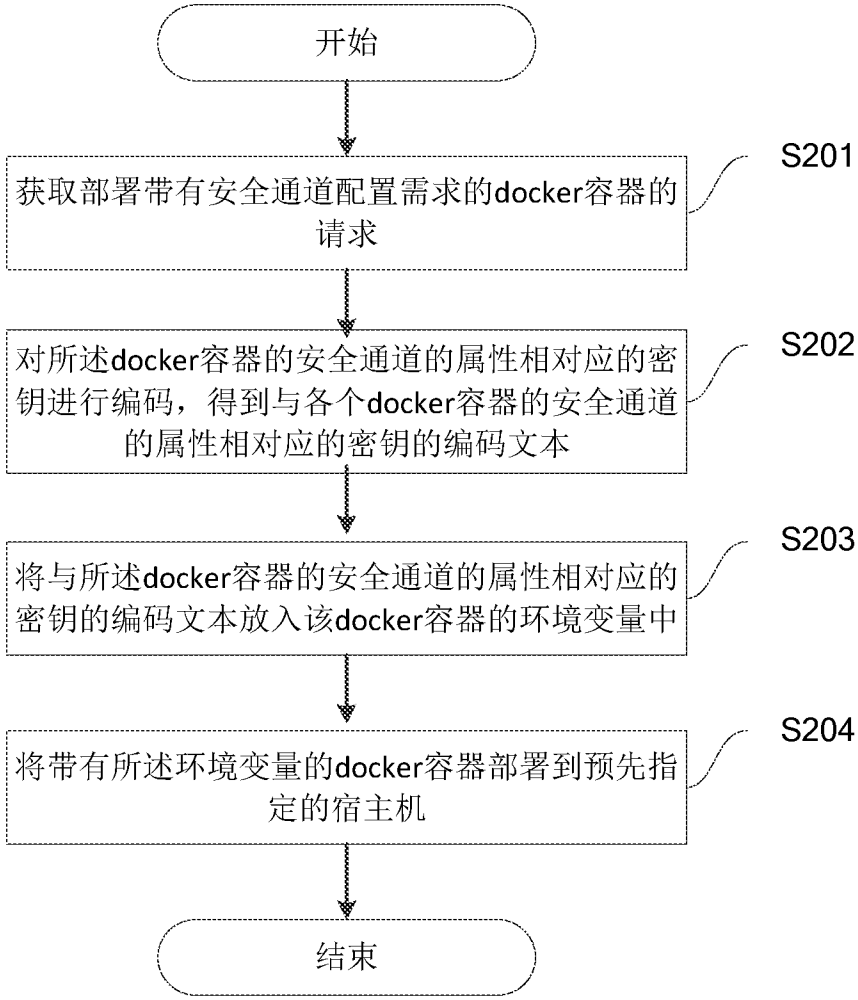

开始
获取部署带有安全通道配置需求的docker容器的请求
S201
对所述docker容器的安全通道的属性相对应的密钥进行编码，得到与各个docker容器的安全通道的属性相对应的密钥的编码文本
S202
将与所述docker容器的安全通道的属性相对应的密钥的编码文本放入该docker容器的环境变量中
S203
将带有所述环境变量的docker容器部署到预先指定的宿主机
S204
结束

图 3

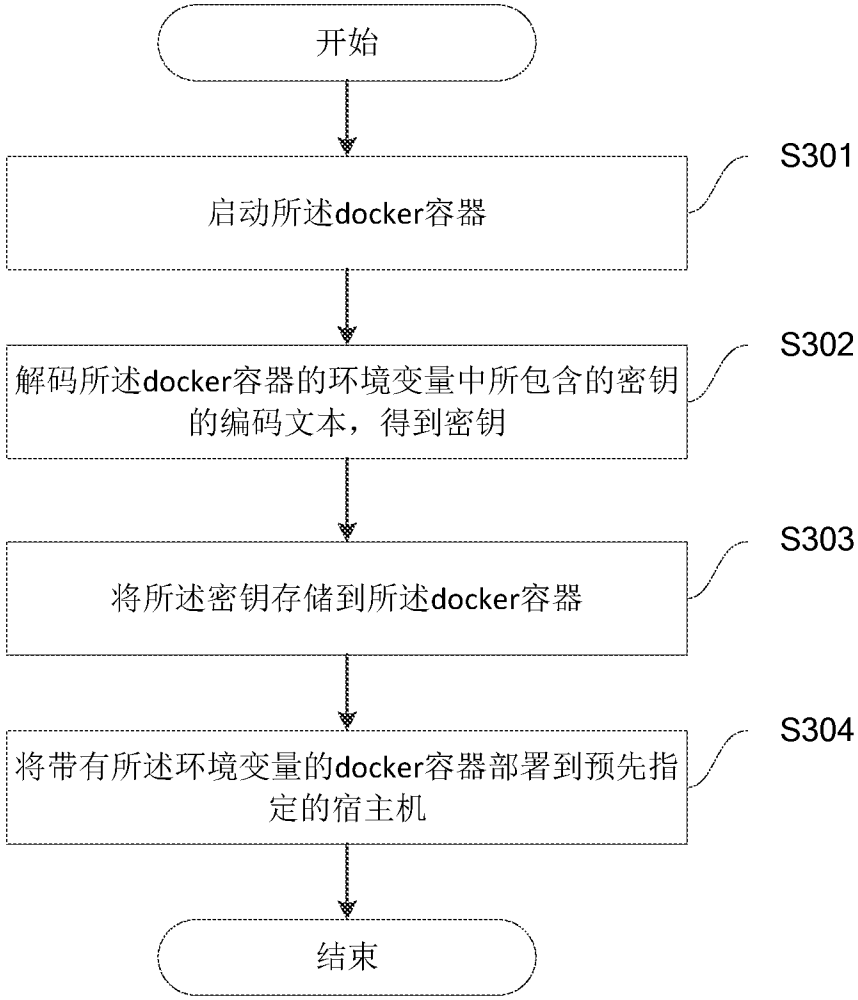

开始
S301
启动所述docker容器
S302
解码所述docker容器的环境变量中所包含的密钥的编码文本，得到密钥
S303
将所述密钥存储到所述docker容器
S304
将带有所述环境变量的docker容器部署到预先指定的宿主机
结束

图 4

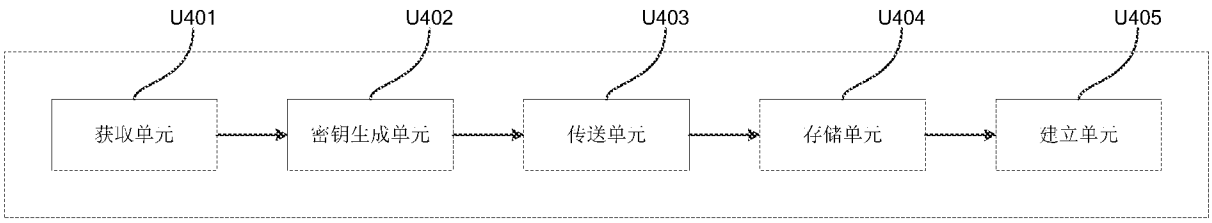

U401
U402
U403
U404
U405
获取单元
密钥生成单元
传送单元
存储单元
建立单元

图 5

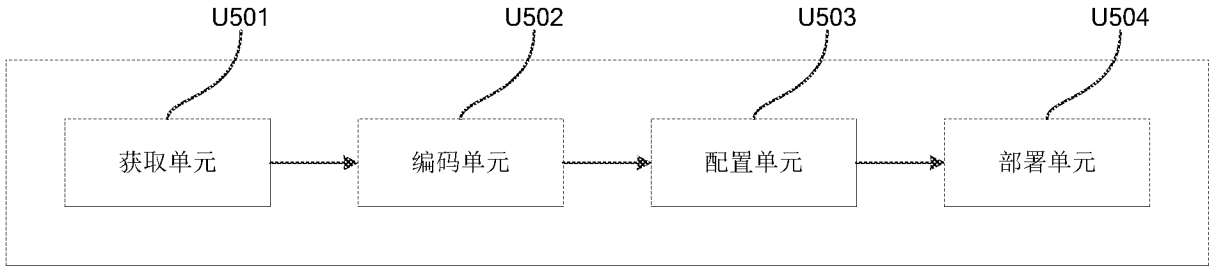

U501
U502
U503
U504
获取单元
编码单元
配置单元
部署单元

图 6

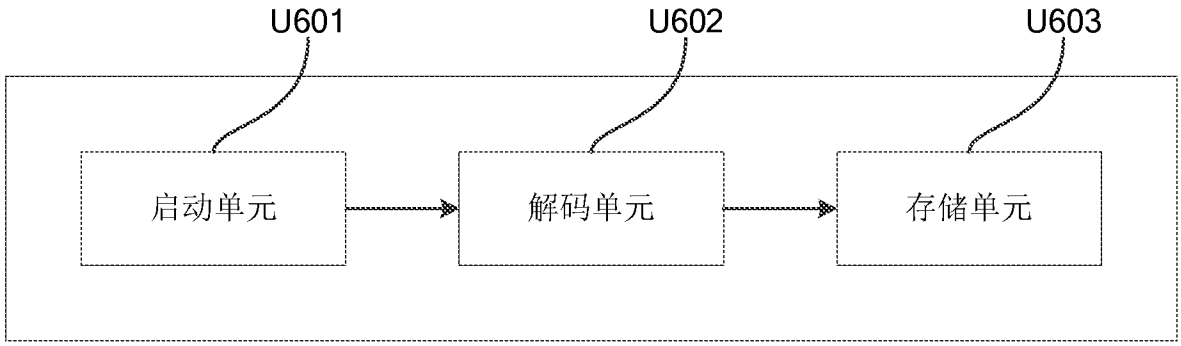

U601
U602
U603
启动单元
解码单元
存储单元

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/110785

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L

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)

CNKI, CNPAT, WPI, EPODOC: 集群, 容器, 用户空间, 密钥, 安全通道, 源端, 主机, 目的端, 编码, 公钥, 私钥, 环境变量, 解码, 属性, 对应, 非对称加密, docker, SSH, key, safety, container, private, cluster, content, server, user, encrypt, information, public, secure, shell

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 201663659 U (BEIJING NOVEL-SUPERTV DIGITAL TV TECHNOLOGY CO., LTD.) 01 December 2010 (01.12.2010), description, paragraphs [0020]-[0076]	1-17
A	CN 102333068 A (BEIJING DIGITAL CHINA SI-TECH INFORMATION TECHNOLOGY CO., LTD.) 25 January 2012 (25.01.2012), entire document	1-17
A	CN 104506483 A (ZTE CORPORATION) 08 April 2015 (08.04.2015), entire document	1-17
A	US 2016150053 A1 (AUTHO, INC.) 26 May 2016 (26.05.2016), entire document	1-17
A	US 2016328006 A1 (VMWARE, INC.) 10 November 2016 (10.11.2016), entire document	1-17
A	WO 2016054272 A1 (NICIRA, INC.) 07 April 2016 (07.04.2016), entire document	1-17

☒ 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
18 January 2018	25 January 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer NIU, Xiaojia Telephone No. (86-10) 53961761

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/110785

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	刘熙等. 基于 Docker 容器的 Web 集群设计与实现. 电子设计工程. 30 April 2016 (30.04.2016), 24(8), entire document. (LIU, Xi et al. Design and Implementation of Web Cluster Based on Docker Container. Electronic Design Engineering.)	1-17

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/110785

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 201663659 U	01 December 2010	None	
CN 102333068 A	25 January 2012	CN 102333068 B	02 April 2014
CN 104506483 A	08 April 2015	WO 2016062157 A1	28 April 2016
		EP 3197123 A4	27 September 2017
		JP 2017531967 A	26 October 2017
		US 2017338950 A1	23 November 2017
		EP 3197123 A1	26 July 2017
US 2016150053 A1	26 May 2016	AR 102797 A1	22 March 2017
		KR 20170107431 A	25 September 2017
		CA 2968858 A1	02 June 2016
		EP 3210150 A1	30 August 2017
		WO 2016086111 A1	02 June 2016
		AU 2015353500 A1	08 June 2017
US 2016328006 A1	10 November 2016	US 9665163 B2	30 May 2017
WO 2016054272 A1	07 April 2016	US 2016094457 A1	31 March 2016
		US 2016094661 A1	31 March 2016
		US 2016094384 A1	31 March 2016
		EP 3202109 A1	09 August 2017
		US 2016094632 A1	31 March 2016
		CN 107005584 A	01 August 2017
		US 2016094633 A1	31 March 2016

国际检索报告

国际申请号
PCT/CN2017/110785

A. 主题的分类

H04L 29/06(2006.01)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)

H04L

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）)

CNKI,CNPAT,WPI,EPODOC：集群，容器，用户空间，密钥，安全通道，源端，主机，目的端，编码，公钥，私钥，环境变量，解码，属性，对应，非对称加密，docker, SSH, key, safety, container, private, cluster, content, server, user, encrypt, information, public, secure, shell

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 201663659 U (北京视博数字电视科技有限公司) 2010年 12月 1日 (2010-12-01) 说明书第[0020]-[0076]段	1-17
A	CN 102333068 A (北京神州数码思特奇信息技术股份有限公司) 2012年 1月 25日 (2012-01-25) 全文	1-17
A	CN 104506483 A (中兴通讯股份有限公司) 2015年 4月 8日 (2015-04-08) 全文	1-17
A	US 2016150053 A1 (AUTHO, INC.) 2016年 5月 26日 (2016-05-26) 全文	1-17
A	US 2016328006 A1 (VMWARE, INC.) 2016年 11月 10日 (2016-11-10) 全文	1-17
A	WO 2016054272 A1 (NICIRA, INC.) 2016年 4月 7日 (2016-04-07) 全文	1-17
A	刘熙 等. "基于Docker容器的Web集群设计与实现" 电子设计工程, 第24卷, 第8期, 2016年 4月 30日 (2016-04-30), 全文	1-17

☐ 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
2018年 1月 18日	2018年 1月 25日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 牛晓佳 电话号码 (86-10)53961761

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/110785

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	201663659	U	2010年 12月 1日	无			
CN	102333068	A	2012年 1月 25日	CN	102333068	B	2014年 4月 2日
CN	104506483	A	2015年 4月 8日	WO	2016062157	A1	2016年 4月 28日
				EP	3197123	A4	2017年 9月 27日
				JP	2017531967	A	2017年 10月 26日
				US	2017338950	A1	2017年 11月 23日
				EP	3197123	A1	2017年 7月 26日
US	2016150053	A1	2016年 5月 26日	AR	102797	A1	2017年 3月 22日
				KR	20170107431	A	2017年 9月 25日
				CA	2968858	A1	2016年 6月 2日
				EP	3210150	A1	2017年 8月 30日
				WO	2016086111	A1	2016年 6月 2日
				AU	2015353500	A1	2017年 6月 8日
US	2016328006	A1	2016年 11月 10日	US	9665163	B2	2017年 5月 30日
WO	2016054272	A1	2016年 4月 7日	US	2016094457	A1	2016年 3月 31日
				US	2016094661	A1	2016年 3月 31日
				US	2016094384	A1	2016年 3月 31日
				EP	3202109	A1	2017年 8月 9日
				US	2016094632	A1	2016年 3月 31日
				CN	107005584	A	2017年 8月 1日
				US	2016094633	A1	2016年 3月 31日