(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
2021 年 9 月 23 日 (23.09.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/184587 A1

(51) 国际专利分类号:
G06F 11/30 (2006.01) *G06F 16/27* (2019.01)
G06F 11/32 (2006.01)

(21) 国际申请号: PCT/CN2020/099190

(22) 国际申请日: 2020 年 6 月 30 日 (30.06.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010189434.6 2020年3月18日 (18.03.2020) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 梁桂明 (LIANG, Guiming); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市精英专利事务所 (SHENZHEN TALENT PATENT SERVICE); 中国广东省深圳市福田区深南中路6009号绿景广场B栋20层B, Guangdong 518000 (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,

WO 2021/184587 A1

(54) **Title:** PROMETHEUS-BASED PRIVATE CLOUD MONITORING METHOD AND APPARATUS, AND COMPUTER DEVICE AND STORAGE MEDIUM

(54) 发明名称: 基于Prometheus的私有云监控方法、装置、计算机设备及存储介质

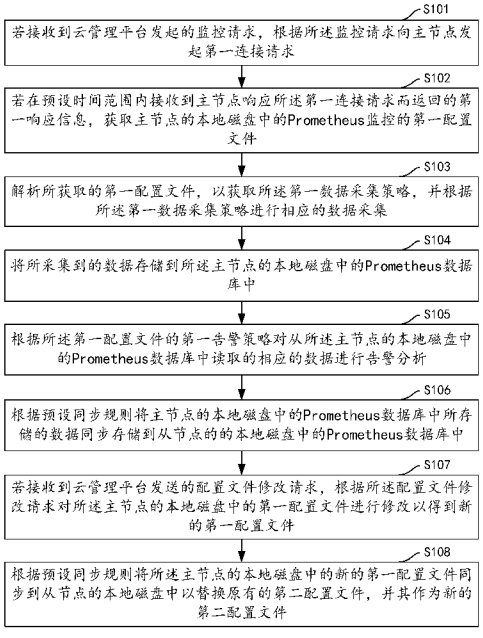

图 1

S101 If a monitoring request initiated by a cloud management platform is received, initiate a first connection request for a master node according to the monitoring request

S102 If first response information returned by the master node in response to the first connection request is received within a preset time range, acquire a first configuration file for Prometheus monitoring in a local disk of the master node

S103 Parse the acquired first configuration file to acquire a first data collection policy, and perform corresponding data collection according to the first data collection policy

S104 Store collected data in a Prometheus database in the local disk of the master node

S105 Perform, according to a first alarm policy of the first configuration file, alarm analysis on corresponding data read from the Prometheus database in the local disk of the master node

S106 According to a preset synchronization rule, synchronously store, in a Prometheus database in a local disk of a slave node, the data stored in the Prometheus database in the local disk of the master node

S107 If a configuration file modification request sent by the cloud management platform is received, modify the first configuration file in the local disk of the master node according to the configuration file modification request so as to obtain a new first configuration file

S108 Synchronize the new first configuration file in the local disk of the master node to the local disk of the slave node according to the preset synchronization rule so as to replace an original second configuration file, and take same as a new second configuration file

(57) **Abstract:** A Prometheus-based private cloud monitoring method and apparatus, and a computer device and a storage medium. The method is applied to the field of cloud monitoring and relates to big data technology. The method comprises: if a monitoring request initiated by a cloud management platform is received, initiating a first connection request for a master node according to the monitoring request (S101); if first response information returned by the master node in response to the first connection request is received within a preset time range, acquiring a first configuration file for Prometheus monitoring in a local disk of the master node (S102); parsing the

[见续页]

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, 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))。

acquired first configuration file, and performing corresponding data collection according to a first data collection policy (S103); storing collected data in a Prometheus database in the local disk of the master node (S104); and performing, according to a first alarm policy of the first configuration file, alarm analysis on corresponding data read from the Prometheus database in the local disk of the master node (S105). By means of the method, the high availability of private cloud monitoring can be improved and a prompt alarm can be generated, thereby facilitating the operation and maintenance thereof by a user.

(57) 摘要：一种基于Prometheus的私有云监控方法、装置、计算机设备及存储介质。该方法应用于云监控领域，涉及大数据技术，该方法包括若接收到云管理平台发起的监控请求，根据监控请求向主节点发起第一连接请求（S101）；若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的Prometheus监控的第一配置文件（S102）；解析所获取的第一配置文件，并根据第一数据采集策略进行相应的数据采集（S103）；将所采集到的数据存储到主节点的本地磁盘中的Prometheus数据库中（S104）；根据第一配置文件的第一告警策略对从主节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析（S105）。该方法能够提高私有云监控的高可用，并能及时产生告警，便于用户运维。

基于 Prometheus 的私有云监控方法、装置、计算机设备及存储介质

本申请要求于 2020 年 03 月 18 日提交中国专利局、申请号为 202010189434.6，发明名称为“基于 Prometheus 的私有云监控方法、装置、计算机设备及存储介质”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

本申请涉及云监控领域，尤其涉及一种基于 Prometheus 的私有云监控方法、装置、计算机设备及存储介质。

背景技术

云服务是基于互联网的相关服务的增加、使用和交互模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云服务可以将企业所需的软硬件、资料都放到网络上，在任何时间、地点，使用不同的 IT 设备互相连接，实现数据存取、运算等目的。当前，常见的云服务有公共云（Public Cloud）与私有云（Private Cloud）两种。其中的私有云(Private Clouds)是为一个客户单独使用而构建的，因而能够提供对数据、安全性和服务质量的最有效控制。

当前私有云方案是各个云厂商必争的兵家之地，而私有云中最为重要的是其设置的监控方案，监控的可用性决定了私有云方案交付的可靠性，以及私有云业务的可用性发生问题时，是否能及时产生告警。目前，私有云的监控方案大多数直接使用公有云的监控方案。同时公有云中采用的 Prometheus 的监控方案基本都是使用 Remote_read 和 Remote_write 的方式实现其高可用性。发明人意识到通常当私有云部署交付，而其又为很小的私有云产品方案时，通常并不提供远程读写的存储方案，只提供本地磁盘的存储方案时，私有云的远程读写方案就不可用，此时监控的高可用性将无法实现。

发明内容

本申请实施例提供一种基于 Prometheus 的私有云监控方法、装置、计算机设备及存储介质，能够提高私有云监控的高可用，并能及时产生告警，便于用户运维。

第一方面，本申请实施例提供了一种基于 Prometheus 的私有云监控方法，该方法包括：若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

第二方面，本申请实施例还提供了一种基于 Prometheus 的私有云监控装置，该装置包括：第一请求单元，用于若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；第一获取单元，用于若在预设时间范围内接收到主节点响应所述第一连接请

求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；第一处理单元，用于解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；第一存储单元，用于将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；第一分析单元，用于根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

第三方面，本申请实施例还提供了一种计算机设备，所述计算机设备包括存储器，以及与所述存储器相连的处理器；所述存储器用于存储计算机程序；所述处理器用于运行所述存储器中存储的计算机程序，以执行以下步骤:若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

第四方面，本申请实施例还提供了一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序当被处理器执行时使所述处理器执行以下操作:若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

本申请实施例提供了一种基于 Prometheus 的私有云监控方法、装置、计算机设备及存储介质。本申请实施例通过云管理平台的监控账号在监控服务系统的监控服务器的主从节点的本地磁盘上设置实现对应的私有云的 Prometheus 监控的配置文件，通过配置文件中所配置的告警策略实现对私有云的高可用的监控，可实现在私有云的相关数据发生异常问题时能及时产生告警，并确保在不增加成本的情况下提高私有云监控的高可用以及便于用户运维的效果。

附图说明

为了更清楚地说明本申请实施例技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例提供的一种基于 Prometheus 的私有云监控方法的流程示意图；

图 1a 是本申请实施例提供的一种基于 Prometheus 的私有云监控方法的应用场景示意图；

图 2 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控方法的流程示意图；

图 3 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控方法的流程示意图；

图 4 是本申请实施例提供的一种基于 Prometheus 的私有云监控装置的示意性框图；

图 5 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控装置的示意性框图；

图 6 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控装置的示意性框图

图 7 是本申请实施例提供的一种计算机设备结构组成示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

应当理解，当在本说明书和所附权利要求书中使用时，术语“包括”和 “包含”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

还应当理解，在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使
用的那样，除非上下文清楚地指明其它情况，否则单数形式的“一”、“一个”及“该”意在包括复数形式。

请参阅图 1 和图 1a，图 1 是本申请实施例提供的一种基于 Prometheus 的私有云监控方法的示意流程图，图 1a 是本申请实施例中基于 Prometheus 的私有云监控方法的场景示意图。该基于 Prometheus 的私有云监控方法应用于监控服务系统中的管理服务器 10 中。该管理服务器 10 根据基于 Prometheus 的私有云监控方法通过云管理平台 20 的监控账号在监控服务系统的监控服务器 10 的主从节点的本地磁盘上设置实现对应的私有云的 Prometheus 监控的配置文件，通过配置文件中所配置的告警策略实现对私有云的高可用的监控。该方法能够在保证 Prometheus 的监控服务不中断，且私有云的相关数据发生异常问题时可及时产生告警，以及确保监控成本不增加的情况下，提高私有云监控的高可用以及便于用户运维。以下将以管理服务器 10 的角度详细地介绍该基于 Prometheus 的私有云监控方法的各个步骤。

请参阅图 1，图 1 是本申请实施例提供的基于 Prometheus 的私有云监控方法的示意流程图。如图 1 所示，该基于 Prometheus 的私有云监控方法的步骤包括步骤 S101~S105。

步骤 S101，若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。在本实施例中，监控服务系统用于实现对云管理平台的相关数据信息的监控，当监控服务系统的监控服务器接收到用户云管理平台发起的监控请求,此时可以根据该监控请求向监控服务系统中的用于监控的主节点发起第一连接请求。通常，此处的云管理平台为用户的私有云的用于实现对其管理的平台，该平台可以包括提供私有云的相关服务器或者服务器群集等。而监控服务系统能够实现对私有云的相关数据信息的监控，为了实现对私有云的监控的高可用性，监控服务系统包括用于监控的主节点和用于备份该主节点中的相关信息的

从节点，其中的主节点为主要的监控节点，当主节点出现宕机或者连接不上的情况，此时则会启用从节点。

步骤 S102，若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略。在本实施例中，预设时间范围可以根据用户的需求进行相应的设定。主节点在接收到第一连接请求后，会相应地想监控服务器返回相应的第一响应信息。若在预设时间范围内，监控服务器能够接收到由主节点所返回的第一响应信息，则表明监控服务器与主节点之间能够建立完整的连接。监控服务器能够获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，以根据该第一配置文件来完成具体的监控。通常，第一配置文件是用于配置监控的相关信息，故其可以包括第一数据采集策略以及第一告警策略。同时，第一配置文件是需要预先在主节点的本地磁盘中根据用户需求进行设置的，不仅便于用户对该第一配置文件的增删改，将其变动同步更新到从节点中。

步骤 S103，解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。在本实施例中，监控服务器能够解析所获取的第一配置文件，从而获取到第一数据采集策略和第一告警策略。此处，获取第一数据采集策略之后，可以根据该第一数据采集策略来实现相应的数据的采集。例如，对于私有云而言，为对其性能及安全等进行实时监控，此时可以对于私有云中传输的数据流量信息、数据存储信息以及服务器的 CPU 占比等数据进行监控获取，并通过后续的对比分析来实现对私有云的性能的监控和告警等。作为可选的，该第一数据采集策略可以是每隔预设时间即对相关数据进行一次采集更新。

步骤 S104，将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。在本实施例中，当监控服务器采集到相应的数据后，为了便于对相关数据进行统计分析，可以将所采集到的数据都存储到主节点的本地磁盘中的 Prometheus 数据库中，当需要进行告警分析的时候，则从 Prometheus 数据库中进行数据调取，不仅方便数据的管理，还便于用户对数据的处理和分析。

步骤 S105，根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。在本实施例中，监控服务器能够根据所述第一配置文件中的第一告警策略，从主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据，并能够实现对所读取的相关数据进行告警分析处理。

在一实施例中，所述方法还可以包括以下步骤：步骤 S106，根据预设同步规则将所述主节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到从节点的本地磁盘中的 Prometheus 数据库中。在本实施例中，为了实现私有云监控的高可用性，通常会采用预设同步规则将所述主节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到从节点的本地磁盘中的 Prometheus 数据库中，从而实现主从节点的数据的同步更新，以便于在其中一个节点出现问题时，另一个节点能够实时顶替该节点的位置，从而不间断地实现对私有云的监控。作为可选的，该预设同步规则可以是 Rsync 工具，Rsync 工具是数据镜像备份工具，

能够实现本地不同路径下的文件的同步，即实现本地文件的同步的增删改等操作。

在进一步的实施例中，所述方法还可以包括以下步骤：步骤 S107，若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件。其中，监控服务器若收到到云管理平台发送的配置文件修改请求，则可以根据该配置文件修改请求来实现对所述主节点的本地磁盘中的第一配置文件的修改，修改后的第一配置文件即为新的第一配置文件。步骤 S108，根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并将其作为新的第二配置文件。其中，当主节点中的第一配置文件经过修改变为新的第一配置文件后，可以通过预设同步规则将其同步至从节点的本地磁盘中，并用于替换掉原有的第二配置文件，即将新的第一配置文件作为新的第二配置文件，由于从节点的本地磁盘中的内容相当于是对主节点的备份，故通常两者之间的第一配置文件和第二配置文件是相同的。

综上，本申请实施例通过云管理平台的监控账号在监控服务系统的监控服务器的主从节点的本地磁盘上设置实现对应的私有云的 Prometheus 监控的配置文件，通过配置文件中所配置的告警策略实现对私有云的高可用的监控，可实现在私有云的相关数据发生异常问题时能及时产生告警，并确保在不增加成本的情况下提高私有云监控的高可用以及便于用户运维的效果。

请参阅图 2，图 2 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控方法的示意流程图。如图 2 所示，该方法的步骤包括步骤 S201~S205′。其中步骤 S201~S205 与上述实施例中的步骤 S101~S105 的步骤的相关解释和详细说明在此不再赘述，下面详细说明的为本实施例中所增加的步骤。

步骤 S201，若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。步骤 S202，若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略。步骤 S203，解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。步骤 S204，将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。步骤 S205，根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

步骤 S202′，若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求。在本实施例中，若监控服务器止啊预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，则表明此时的主节点发生宕机或者不能够与云管理平台进行连接，此时需要根据监控请求，向从节点发起第二连接请求，以实现对云管理平台的持续监控。通常，可以通过 Keepalive 来实现主节点和从节点之间的切换，即能够快速的从主节点切换到从节点。

步骤 S202a′，若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二

响应信息，获取从节点的本地磁盘中的 Prometheus 监控的第二配置文件，所述第二配置文件包括第二数据采集策略以及第二告警策略。在本实施例中，当监控服务器进行主从切换之后，此时若在预设时间范围内，从节点接收第二连接请求并响应生成第二响应信息后，能够将第二响应信息返回给到监控服务器，此时监控服务器则能与从节点建立连接，进而可以从从节点的本地磁盘中获取到 Prometheus 监控的第二配置文件。由于从节点是相对于主节点的备份，故所述第二配置文件也与第一配置文件相同，即第二配置文件也包括第二数据采集策略以及第二告警策略。

步骤 S203′，解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集。在本实施例中，监控服务器能够解析所获取的第二配置文件，从而获取到第二数据采集策略和第二告警策略。此处，获取第二数据采集策略之后，可以根据该第二数据采集策略来实现相应的数据的采集。例如，对于私有云而言，为对其性能及安全等进行实时监控，此时可以对于私有云中传输的数据流量信息、数据存储信息以及服务器的 CPU 占比等数据进行监控获取，并通过后续的对比分析来实现对私有云的性能的监控和告警等。作为可选的，可以每隔预设时间即对相关数据进行一次采集更新。

步骤 S204′，将所采集到的数据存储到所述从节点的本地磁盘中的 Prometheus 数据库中。

在本实施例中，当监控服务器采集到相应的数据后，为了便于对相关数据进行统计分析，可以将所采集到的数据都存储到从节点的本地磁盘中的 Prometheus 数据库中，当需要进行告警分析的时候，则从 Prometheus 数据库中进行数据调取，不仅方便数据的管理，还便于用户对数据的处理和分析。

步骤 S205′，根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。在本实施例中，监控服务器能够根据所述第二配置文件中的第二告警策略，从主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据，并能够实现对所读取的相关数据进行告警分析处理。

在一实施例中，所述方法还可以包括以下步骤：步骤 S206′，根据预设同步规则将所述从节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到主节点的本地磁盘中的 Prometheus 数据库中。在本实施例中，为了实现私有云监控的高可用性，通常会采用预设同步规则将所述从节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到主节点的本地磁盘中的 Prometheus 数据库中，从而实现主从节点的数据的同步更新，以便于在其中一个节点出现问题时，另一个节点能够实时顶替该节点的位置，从而不间断地实现对私有云的监控。作为可选的，该预设同步规则可以是 Rsync 工具，Rsync 工具是数据镜像备份工具，能够实现本地不同路径下的文件的同步，即实现本地文件的同步的增删改等操作。作为可选的，监控服务器通过监控到主节点恢复正常后，还可以通过反向同步性能数据和监控配置信息数据再次使用主节点中的 Prometheus 监控，从而提供持续可用的主从模式的监控高可用方案。

在进一步的实施例中，所述方法还可以包括以下步骤：步骤 S207′，若接收到云管理平

台发送的配置文件修改请求，根据所述配置文件修改请求对所述从节点的本地磁盘中的配置文件进行修改以得到新的配置文件。在本实施例中，监控服务器若收到到云管理平台发送的配置文件修改请求，则可以根据该配置文件修改请求来实现对所述从节点的本地磁盘中的第二配置文件的修改，修改后的第二配置文件即为新的第二配置文件。

步骤 S208′，根据预设同步规则将所述从节点的本地磁盘中的新的配置文件同步到主节点的本地磁盘中以替换原有的配置文件。在本实施例中，当从节点中的第二配置文件经过修改变为新的第二配置文件后，可以通过预设同步规则将其同步至主节点的本地磁盘中，并用于替换掉原有的第一配置文件，即将新的第二配置文件作为新的第一配置文件，由于从节点的本地磁盘中的内容相当于是对主节点的备份，故通常两者之间的第一配置文件和第二配置文件是相同的。

请参阅图 3，图 3 是本申请另一实施例提供的一种基于 Prometheus 的私有云监控方法的示意流程图。如图 3 所示，该方法的步骤包括步骤 S301a~S305。其中与上述实施例中的步骤 S101-S105 类似的步骤的相关解释和详细说明在此不再赘述，下面详细说明的为本实施例中所增加的步骤。

步骤 S301a，若接收到云管理平台发送的用户监控登录请求，解析所述用户监控登录请求以获取相应的请求信息，所述请求信息包括用户账号和用户密码。步骤 S301b，若预设数据库中包括所述用户账号，判断所述用户账号所关联的预设密码是否与所述用户密码相匹配。步骤 S301c，若所述用户账号所关联的预设密码与所述用户密码相匹配，则用户监控登录成功。其中，用户可以根据自身需求在云管理平台注册监控管理账号，并能够阻止云管理平台进行登录，并向监控服务器发送用户监控登录请求，监控服务器能够解析该用户监控登录请求从而获取用户账号和用户密码，进而进行相应的匹配检测，若匹配通过，则用户监控登录成功，此时监控管理系统可以实现对私有云的云管理平台的全面可持续的高可用监控。步骤 S301，若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。步骤 S302，若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略。步骤 S303，解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。步骤 S304，将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。步骤 S305，根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

本领域普通技术员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）等。

请参阅图 4，对应上述一种基于 Prometheus 的私有云监控方法，本申请实施例还提出一种基于 Prometheus 的私有云监控装置，该装置 100 包括：第一请求单元 101、第一获取单元

102、第一处理单元 103、第一存储单元 104 以及第一分析单元 105。

所述第一请求单元 101，用于若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。

所述第一获取单元 102，用于若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略。

所述第一处理单元 103，用于解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。

所述第一存储单元 104，用于将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。

所述第一分析单元 105，用于根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

在一实施例中，所述装置 100 还可以包括以下单元：第一同步单元 106，用于根据预设同步规则将所述主节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到从节点的本地磁盘中的 Prometheus 数据库中。在进一步的实施例中，所述装置 100 还可以包括以下单元：第一修改单元 107，用于若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件。第一更新单元 108，用于根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并将其作为新的第二配置文件。

请参阅图 5，对应上述一种基于 Prometheus 的私有云监控方法，本申请另一实施例还提出一种基于 Prometheus 的私有云监控装置，该装置 200 包括：第一请求单元 201、第一获取单元 202、第一处理单元 203、第一存储单元 204、第一分析单元 205、第二请求单元 202′、第二获取单元 202a′、第二处理单元 203′、第二存储单元 204′以及第二分析单元 205′。其中与上述实施例中的第一请求单元 101、第一获取单元 102、第一处理单元 103、第一存储单元 104 以及第一分析单元 105 相同的单元的相关解释和详细说明在此不再赘述，下面详细说明的为本实施例中所增加的单元。

所述第一请求单元 201，用于若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。

所述第一获取单元 202，用于若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略。

所述第一处理单元 203，用于解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。

所述第一存储单元 204，用于将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。

所述第一分析单元 205，用于根据所述第一配置文件的第一告警策略对从所述主节点的

本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

所述第二请求单元 202′，用于若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求。

所述第二获取单元 202a′，用于若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二响应信息，获取从节点的本地磁盘中的 Prometheus 监控的第二配置文件，所述第二配置文件包括第二数据采集策略以及第二告警策略。

所述第二处理单元 203′，用于解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集。

所述第二存储单元 204′，用于将所采集到的数据存储到所述从节点的本地磁盘中的 Prometheus 数据库中。

所述第二分析单元 205′，用于根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

在一实施例中，所述装置 200 还可以包括以下单元：

第二同步单元 206′，用于根据预设同步规则将所述从节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到主节点的本地磁盘中的 Prometheus 数据库中。

在进一步的实施例中，所述装置 200 还可以包括以下单元：

第二修改单元 207′，用于若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述从节点的本地磁盘中的配置文件进行修改以得到新的配置文件。

第二更新单元 208′，用于根据预设同步规则将所述从节点的本地磁盘中的新的配置文件同步到主节点的本地磁盘中以替换原有的配置文件。

请参阅图 6，对应上述一种基于 Prometheus 的私有云监控方法，本申请另一实施例还提出一种基于 Prometheus 的私有云监控装置，该装置 300 包括：请求单元 301a、判断单元 301b、登录单元 301c、第一请求单元 301、第一获取单元 302、第一处理单元 303、第一存储单元 304 以及第一分析单元 305。其中与上述实施例中的第一请求单元 101、第一获取单元 102、第一处理单元 103、第一存储单元 104 以及第一分析单元 105 相同的单元的相关解释和详细说明在此不再赘述，下面详细说明的为本实施例中所增加的单元。

请求单元 301a，用于若接收到云管理平台发送的用户监控登录请求，解析所述用户监控登录请求以获取相应的请求信息，所述请求信息包括用户账号和用户密码。

判断单元 301b，用于若预设数据库中包括所述用户账号，判断所述用户账号所关联的预设密码是否与所述用户密码相匹配。

登录单元 301c，用于若所述用户账号所关联的预设密码与所述用户密码相匹配，则用户监控登录成功。

第一请求单元 301，用于若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求。

第一获取单元 302，用于若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一

配置文件包括第一数据采集策略以及第一告警策略。

第一处理单元 303，用于解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集。

第一存储单元 304，用于将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中。

第一分析单元 305，用于根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

需要说明的是，所属领域的技术人员可以清楚地了解到，上述基于 Prometheus 的私有云监控装置 100 和各单元的具体实现过程，可以参考前述方法实施例中的相应描述，为了描述的方便和简洁，在此不再赘述。

由以上可见，在硬件实现上，以上第一请求单元 101、第一获取单元 102、第一处理单元 103、第一存储单元 104 以及第一分析单元 105 等可以以硬件形式内嵌于或独立于基于 Prometheus 的私有云监控的装置中，也可以以软件形式存储于基于 Prometheus 的私有云监控装置的存储器中，以便处理器调用执行以上各个单元对应的操作。该处理器可以为中央处理单元（CPU)、微处理器、单片机等。

上述基于 Prometheus 的私有云监控装置可以实现为一种计算机程序的形式，计算机程序可以在如图 7 所示的计算机设备上运行。

图 7 为本申请一种计算机设备的结构组成示意图。该设备可以是服务器，其中，服务器可以是独立的服务器，也可以是多个服务器组成的服务器集群。

参照图 7，该计算机设备 400 包括通过系统总线 401 连接的处理器 402、存储器和网络接口 405，其中，存储器可以包括非易失性存储介质 403 和内存储器 404。

该非易失性存储介质 403 可存储操作系统 4031 和计算机程序 4032，该计算机程序 4032 被执行时，可使得处理器 402 执行一种基于 Prometheus 的私有云监控方法。该处理器 402 用于提供计算和控制能力，支撑整个计算机设备 400 的运行。该内存储器 404 为非易失性存储介质 403 中的计算机程序 4032 的运行提供环境，该计算机程序 4032 被处理器 402 执行时，可使得处理器 402 执行一种基于 Prometheus 的私有云监控方法。该网络接口 405 用于与其它设备进行网络通信。本领域技术人员可以理解，图 7 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备 400 的限定，具体的计算机设备 400 可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

其中，所述处理器 402 用于运行存储在存储器中的计算机程序 4032，以实现上述实施例中的基于 Prometheus 的私有云监控方法的步骤。

应当理解，在本申请实施例中，处理器 402 可以是中央处理单元 (Central Processing Unit，CPU)，该处理器 402 还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor，DSP)、专用集成电路 (Application Specific Integrated Circuit，ASIC)、现成可编程门阵列 (Field-Programmable Gate Array，FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、

分立硬件组件等。其中，通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

本领域普通技术人员可以理解的是实现上述实施例的方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成。该计算机程序可存储于一存储介质中，该存储介质为计算机可读存储介质。该计算机程序被该计算机系统中的至少一个处理器执行，以实现上述方法的实施例的流程步骤。

因此，本申请还提供一种存储介质。该计算机可读存储介质可以是非易失性，也可以是易失性。该存储介质存储有计算机程序，该计算机程序被处理器执行时使处理器执行上述实施例中的基于 Prometheus 的私有云监控方法的步骤。

所述存储介质为实体的、非瞬时性的存储介质，例如可以是 U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、磁碟或者光盘等各种可以存储程序代码的实体存储介质。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的。例如，各个单元的划分，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。例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。

本申请实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。本申请实施例装置中的单元可以根据实际需要进行合并、划分和删减。另外，在本申请各个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，也可以是两个或两个以上单元集成在一个单元中。

该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，终端，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1.一种基于 Prometheus 的私有云监控方法，其中，所述方法包括：

若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；

若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；

解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；

根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

2.如权利要求 1 所述的方法，其中，所述方法还包括：

根据预设同步规则将所述主节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到从节点的本地磁盘中的 Prometheus 数据库中。

3.如权利要求 1 所述的方法，其中，所述方法还包括：

若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件；

根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并将其作为新的第二配置文件。

4.如权利要求 1 所述的方法，其中，所述若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求的步骤之后，还包括：

若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求；

若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二响应信息，获取从节点的本地磁盘中的 Prometheus 监控的第二配置文件，所述第二配置文件包括第二数据采集策略以及第二告警策略；

解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述从节点的本地磁盘中的 Prometheus 数据库中；

根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

5.如权利要求 4 所述的方法，其中，所述方法还包括：

根据预设同步规则将所述从节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到主节点的本地磁盘中的 Prometheus 数据库中。

6.如权利要求 4 所述的方法，其中，所述方法还包括：

若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述从节

点的本地磁盘中的配置文件进行修改以得到新的配置文件；

根据预设同步规则将所述从节点的本地磁盘中的新的配置文件同步到主节点的本地磁盘中以替换原有的配置文件。

7.如权利要求 1 所述的方法，其中，所述若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求的步骤之前，还包括：

若接收到云管理平台发送的用户监控登录请求，解析所述用户监控登录请求以获取相应的请求信息，所述请求信息包括用户账号和用户密码；

若预设数据库中包括所述用户账号，判断所述用户账号所关联的预设密码是否与所述用户密码相匹配；

若所述用户账号所关联的预设密码与所述用户密码相匹配，则用户监控登录成功。

8.一种基于 Prometheus 的私有云监控装置，其中，所述装置包括：

第一请求单元，用于若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；

第一获取单元，用于若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；

第一处理单元，用于解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；

第一存储单元，用于将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；

第一分析单元，用于根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

9.一种计算机设备，包括存储器以及与所述存储器相连的处理器；其中，所述存储器用于存储计算机程序；所述处理器用于运行所述存储器中存储的计算机程序，以执行以下步骤：

若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；

若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；

解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；

根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

10.如权利要求 9 所述的计算机设备，其中，所述根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析之后，还包括：

根据预设同步规则将所述主节点的本地磁盘中的Prometheus数据库中所存储的数据同步存储到从节点的本地磁盘中的Prometheus数据库中。

11.如权利要求9所述的计算机设备，其中，所述根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析之后，还包括：

若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件；

根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并将其作为新的第二配置文件。

12.如权利要求9所述的计算机设备，其中，所述若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求之后，还包括：

若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求；

若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二响应信息，获取从节点的本地磁盘中的Prometheus监控的第二配置文件，所述第二配置文件包括第二数据采集策略以及第二告警策略；

解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述从节点的本地磁盘中的Prometheus数据库中；

根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析。

13.如权利要求12所述的计算机设备，其中，所述根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析之后，还包括：

根据预设同步规则将所述从节点的本地磁盘中的Prometheus数据库中所存储的数据同步存储到主节点的本地磁盘中的Prometheus数据库中。

14.如权利要求12所述的计算机设备，其中，所述根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析之后，还包括：

若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述从节点的本地磁盘中的配置文件进行修改以得到新的配置文件；

根据预设同步规则将所述从节点的本地磁盘中的新的配置文件同步到主节点的本地磁盘中以替换原有的配置文件。

15.如权利要求9所述的计算机设备，其中，所述若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求之前，还包括：

若接收到云管理平台发送的用户监控登录请求，解析所述用户监控登录请求以获取相应

的请求信息，所述请求信息包括用户账号和用户密码；

若预设数据库中包括所述用户账号，判断所述用户账号所关联的预设密码是否与所述用户密码相匹配；

若所述用户账号所关联的预设密码与所述用户密码相匹配，则用户监控登录成功。

16. 一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序当被处理器执行时使所述处理器执行以下操作：

若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求；

若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的 Prometheus 监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略；

解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述主节点的本地磁盘中的 Prometheus 数据库中；

根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

17.如权利要求 16 所述的计算机可读存储介质，其中，所述根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析之后，还包括：

根据预设同步规则将所述主节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到从节点的本地磁盘中的 Prometheus 数据库中。

18.如权利要求 16 所述的计算机可读存储介质，其中，所述根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析之后，还包括：

若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件；

根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并将其作为新的第二配置文件。

19.如权利要求 16 所述的计算机可读存储介质，其中，所述若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求之后，还包括：

若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求；

若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二响应信息，获取从节点的本地磁盘中的 Prometheus 监控的第二配置文件，所述第二配置文件包括第二数据采集策略以及第二告警策略；

解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集；

将所采集到的数据存储到所述从节点的本地磁盘中的 Prometheus 数据库中；

根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析。

20.如权利要求 19 所述的计算机可读存储介质，其中，所述根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的 Prometheus 数据库中读取的相应的数据进行告警分析之后，还包括：

根据预设同步规则将所述从节点的本地磁盘中的 Prometheus 数据库中所存储的数据同步存储到主节点的本地磁盘中的 Prometheus 数据库中。

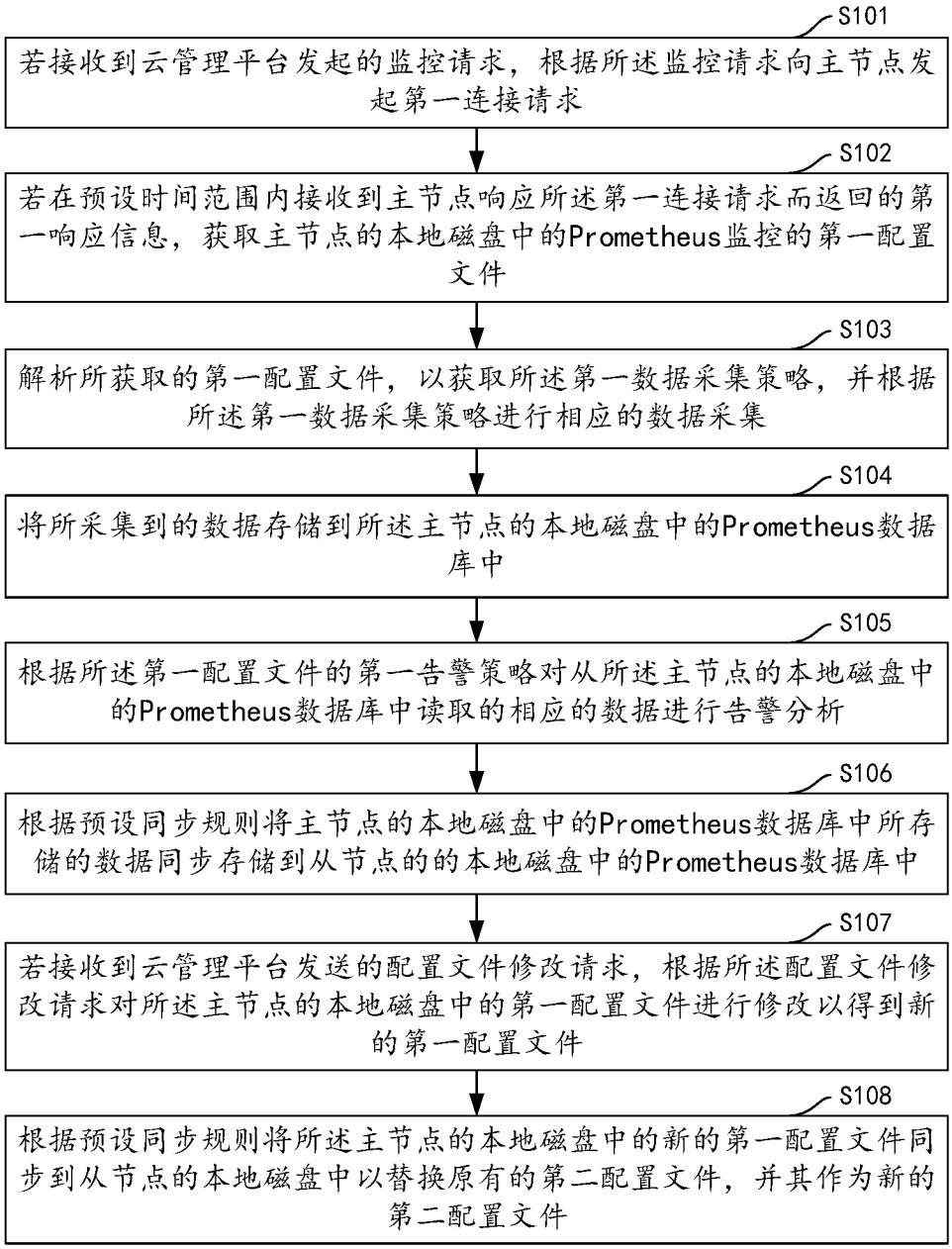
S101
若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求
S102
若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的Prometheus监控的第一配置文件
S103
解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集
S104
将所采集到的数据存储到所述主节点的本地磁盘中的Prometheus数据库中
S105
根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析
S106
根据预设同步规则将主节点的本地磁盘中的Prometheus数据库中所存储的数据同步存储到从节点的的本地磁盘中的Prometheus数据库中
S107
若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述主节点的本地磁盘中的第一配置文件进行修改以得到新的第一配置文件
S108
根据预设同步规则将所述主节点的本地磁盘中的新的第一配置文件同步到从节点的本地磁盘中以替换原有的第二配置文件，并其作为新的第二配置文件

图 1

图 1a

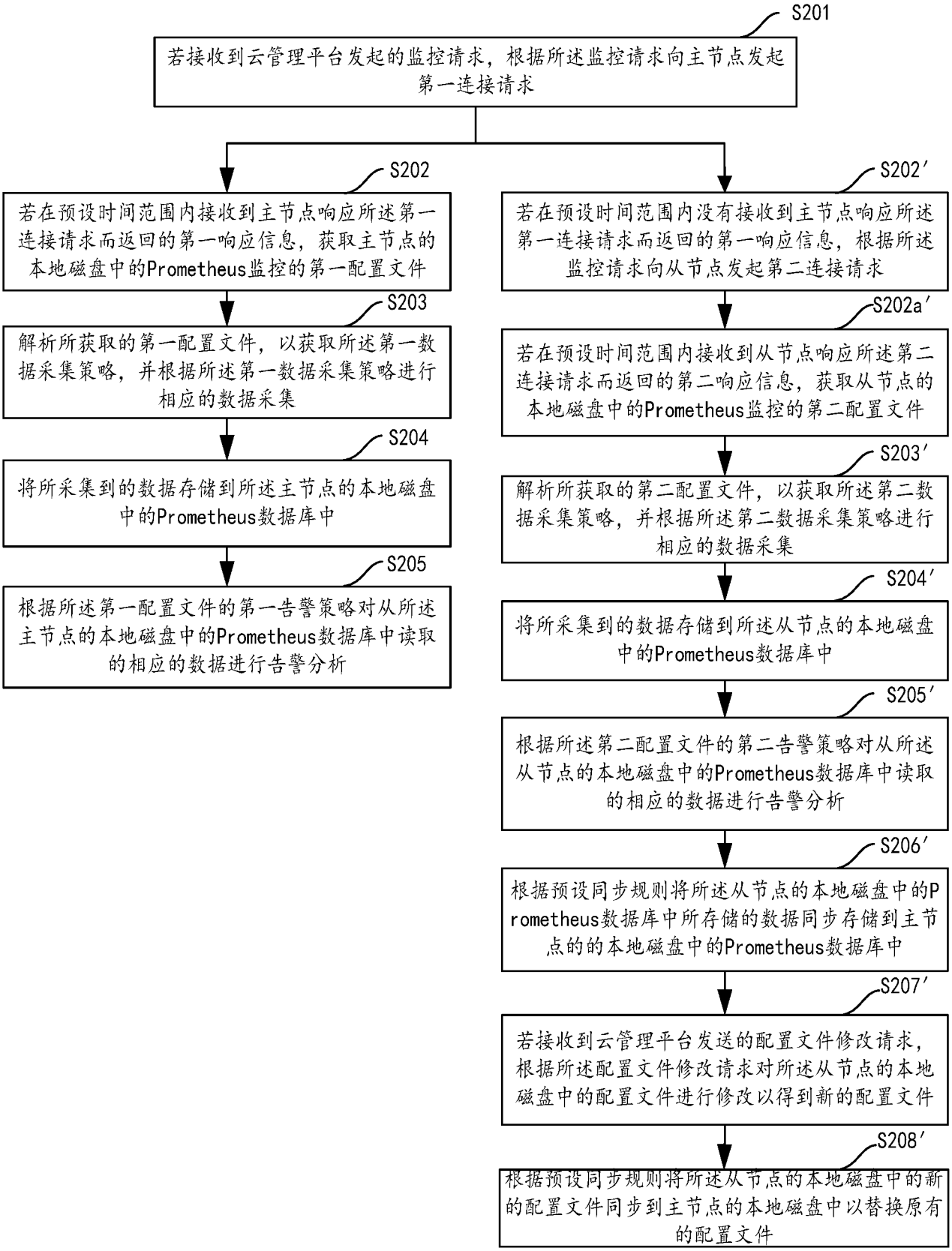
S201
若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求
S202
若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的Prometheus监控的第一配置文件
S203
解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集
S204
将所采集到的数据存储到所述主节点的本地磁盘中的Prometheus数据库中
S205
根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析
S202′
若在预设时间范围内没有接收到主节点响应所述第一连接请求而返回的第一响应信息，根据所述监控请求向从节点发起第二连接请求
S202a′
若在预设时间范围内接收到从节点响应所述第二连接请求而返回的第二响应信息，获取从节点的本地磁盘中的Prometheus监控的第二配置文件
S203′
解析所获取的第二配置文件，以获取所述第二数据采集策略，并根据所述第二数据采集策略进行相应的数据采集
S204′
将所采集到的数据存储到所述从节点的本地磁盘中的Prometheus数据库中
S205′
根据所述第二配置文件的第二告警策略对从所述从节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析
S206′
根据预设同步规则将所述从节点的本地磁盘中的Prometheus数据库中所存储的数据同步存储到主节点的的本地磁盘中的Prometheus数据库中
S207′
若接收到云管理平台发送的配置文件修改请求，根据所述配置文件修改请求对所述从节点的本地磁盘中的配置文件进行修改以得到新的配置文件
S208′
根据预设同步规则将所述从节点的本地磁盘中的新的配置文件同步到主节点的本地磁盘中以替换原有的配置文件

图 2

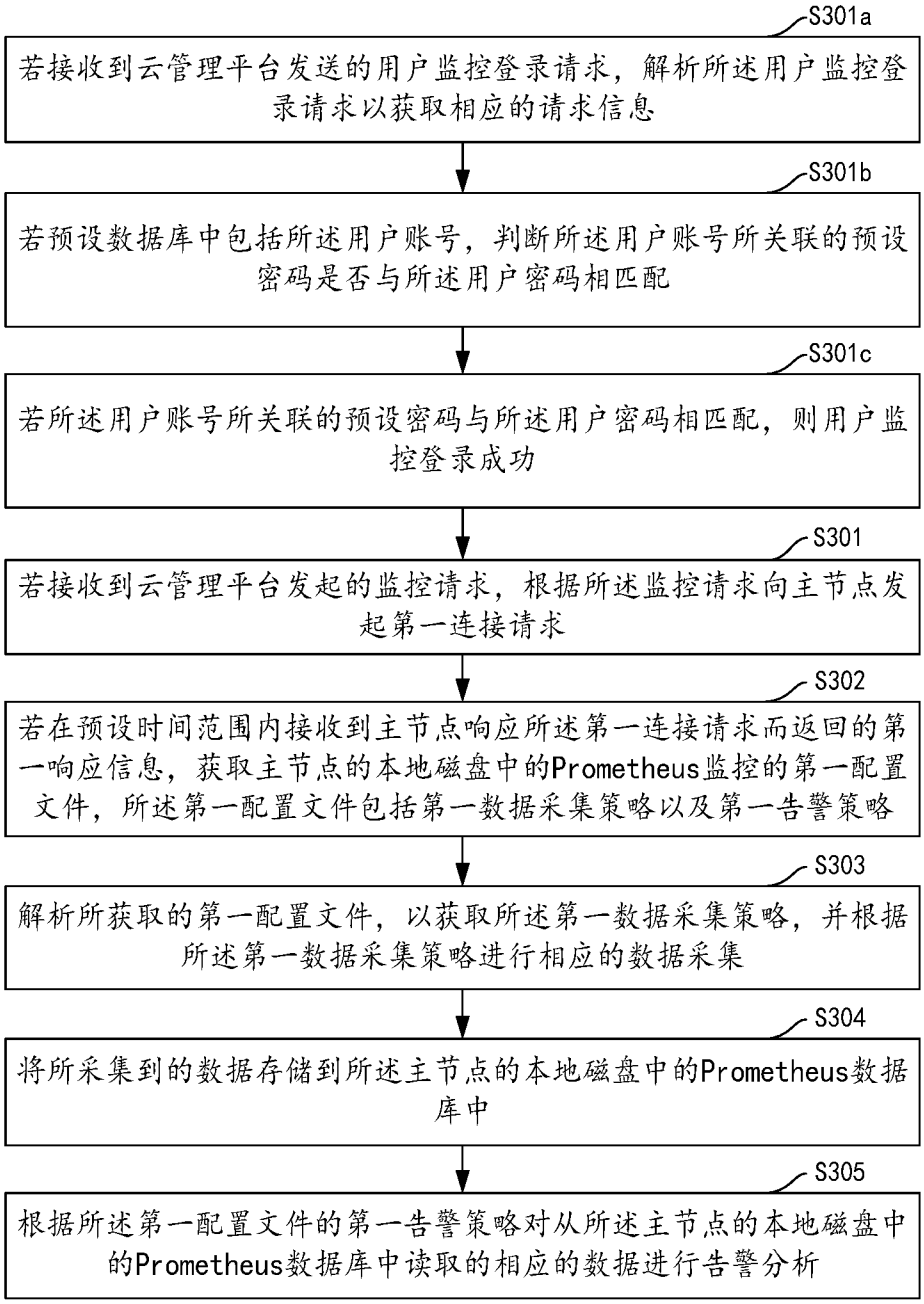
S301a
若接收到云管理平台发送的用户监控登录请求，解析所述用户监控登录请求以获取相应的请求信息
S301b
若预设数据库中包括所述用户账号，判断所述用户账号所关联的预设密码是否与所述用户密码相匹配
S301c
若所述用户账号所关联的预设密码与所述用户密码相匹配，则用户监控登录成功
S301
若接收到云管理平台发起的监控请求，根据所述监控请求向主节点发起第一连接请求
S302
若在预设时间范围内接收到主节点响应所述第一连接请求而返回的第一响应信息，获取主节点的本地磁盘中的Prometheus监控的第一配置文件，所述第一配置文件包括第一数据采集策略以及第一告警策略
S303
解析所获取的第一配置文件，以获取所述第一数据采集策略，并根据所述第一数据采集策略进行相应的数据采集
S304
将所采集到的数据存储到所述主节点的本地磁盘中的Prometheus数据库中
S305
根据所述第一配置文件的第一告警策略对从所述主节点的本地磁盘中的Prometheus数据库中读取的相应的数据进行告警分析

图 3

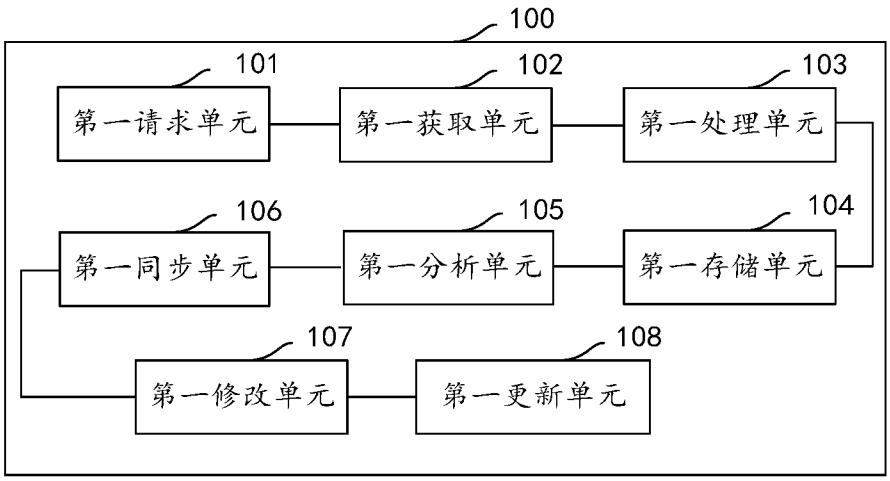
100
101
第一请求单元
102
第一获取单元
103
第一处理单元
106
第一同步单元
105
第一分析单元
104
第一存储单元
107
第一修改单元
108
第一更新单元

图 4

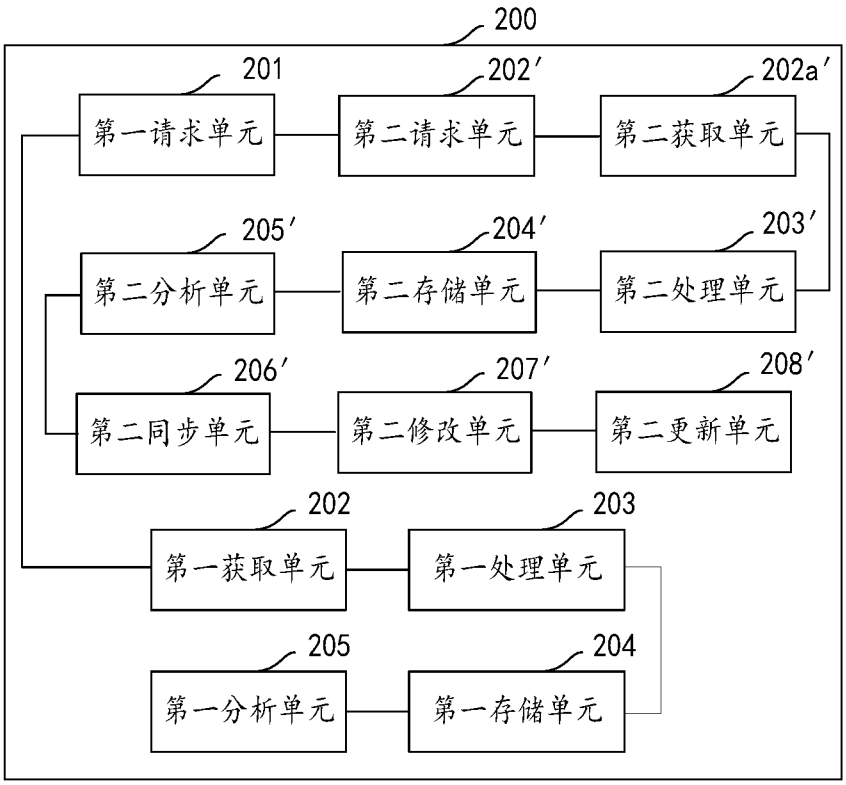
200
201
第一请求单元
202′
第二请求单元
202a′
第二获取单元
205′
第二分析单元
204′
第二存储单元
203′
第二处理单元
206′
第二同步单元
207′
第二修改单元
208′
第二更新单元
202
第一获取单元
203
第一处理单元
205
第一分析单元
204
第一存储单元

图 5

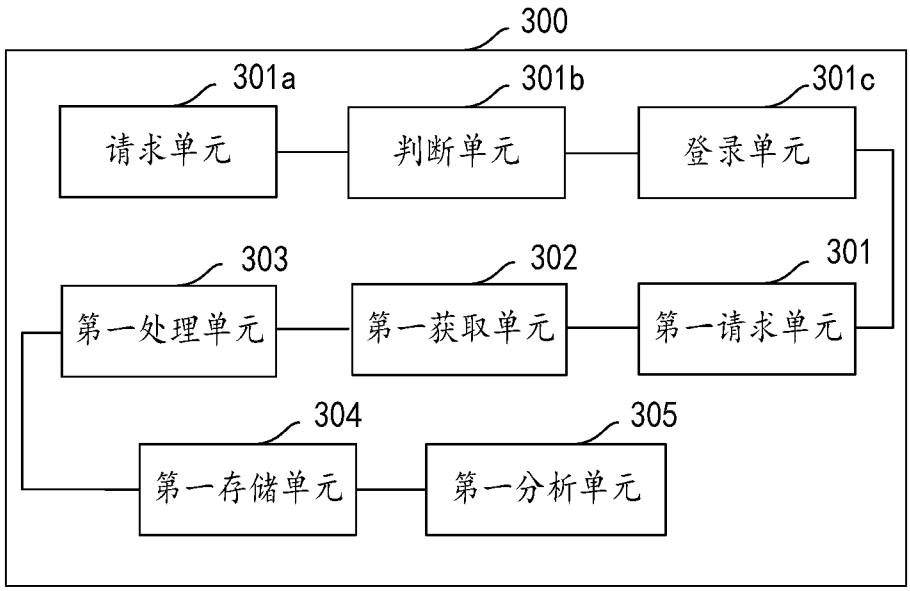
300
301a
请求单元
301b
判断单元
301c
登录单元
303
第一处理单元
302
第一获取单元
301
第一请求单元
304
第一存储单元
305
第一分析单元

图 6

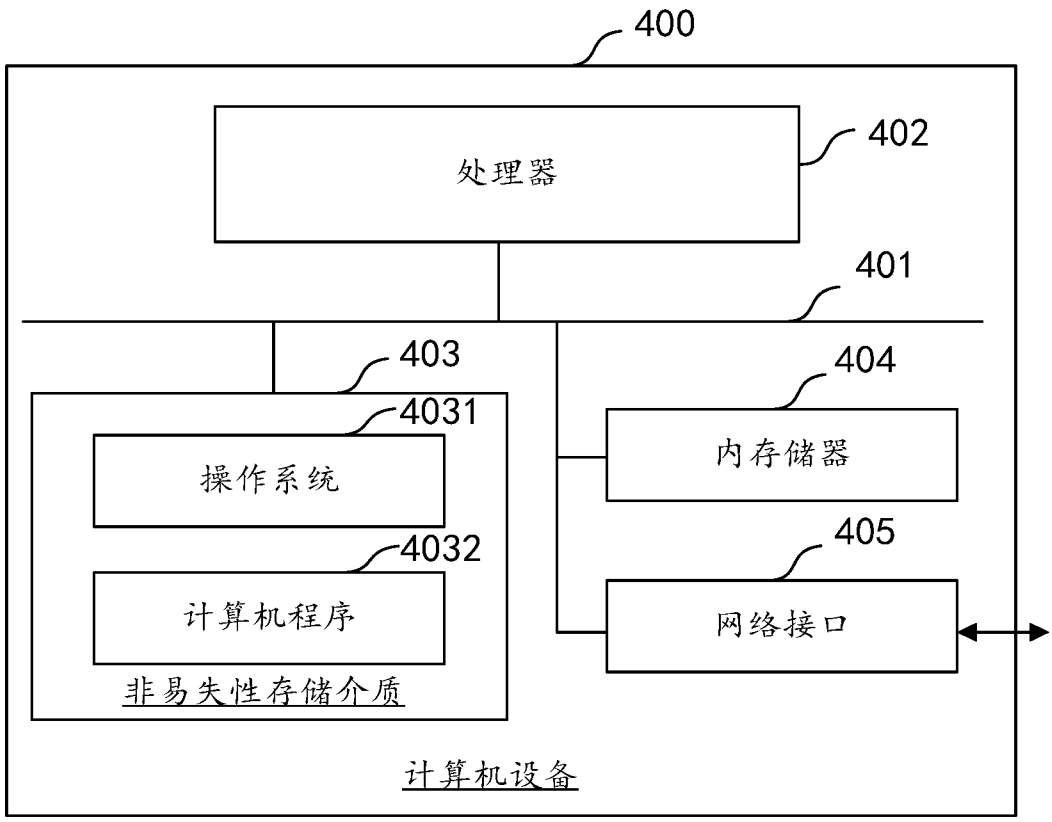
400
处理器
402
401
403
4031
操作系统
4032
计算机程序
非易失性存储介质
404
内存储器
405
网络接口
计算机设备

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/099190

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/30(2006.01)i; G06F 11/32(2006.01)n; G06F 16/27(2019.01)n

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)

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)

CNPAT, EPODOC, WPI, CNKI, ISI: 监控, 检测, 集群, 节点, 服务器, 云, 配置文件, 告警, 本地, 存储, 数据, 采集, prometheus, monitor, cluster, cloud, server, node, configuration, file, alert, store, data, collect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 110659109 A (SHANGHAI INESA (GROUP) R & D CENTER) 07 January 2020 (2020-01-07) description, paragraphs [0033]-[0053], figure 1	1-20
A	CN 110247810 A (LANGCHAO CLOUD INFORMATION TECHNOLOGY CO., LTD.) 17 September 2019 (2019-09-17) entire document	1-20
A	CN 104486445 A (BEIJING SKYCLOUD RONGCHUANG SOFTWARE TECHNOLOGY CO., LTD.) 01 April 2015 (2015-04-01) entire document	1-20
A	CN 109586999 A (SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY, CHINESE ACADEMY OF SCIENCES) 05 April 2019 (2019-04-05) entire document	1-20
A	CN 109245931 A (SICHUAN CHANGHONG ELECTRIC CO., LTD.) 18 January 2019 (2019-01-18) entire document	1-20

☑ 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
04 December 2020	**16 December 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/099190

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 102062576 B1 (FOUNDATION OF SOONGSIL UNIVERSITY-INDUSTRY COOPERATION) 06 January 2020 (2020-01-06) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/099190

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110659109 A	07 January 2020	None	
CN 110247810 A	17 September 2019	None	
CN 104486445 A	01 April 2015	CN 104486445 B	22 March 2017
CN 109586999 A	05 April 2019	None	
CN 109245931 A	18 January 2019	None	
KR 102062576 B1	06 January 2020	None	

国际检索报告

国际申请号
PCT/CN2020/099190

A. 主题的分类

G06F 11/30(2006.01)i; G06F 11/32(2006.01)n; G06F 16/27(2019.01)n

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)

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））

CNPAT, EPODOC, WPI, CNKI, ISI：监控，检测，集群，节点，服务器，云，配置文件，告警，本地，存储，数据，采集，prometheus，monitor，cluster，cloud，server，node，configuration，file，alert，store，data，collect

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 110659109 A (上海仪电集团有限公司中央研究院) 2020年 1月 7日 (2020-01-07) 说明书第[0033]-[0053]段，图1	1-20
A	CN 110247810 A (浪潮云信息技术有限公司) 2019年 9月 17日 (2019-09-17) 全文	1-20
A	CN 104486445 A (北京天云融创软件技术有限公司) 2015年 4月 1日 (2015-04-01) 全文	1-20
A	CN 109586999 A (深圳先进技术研究院) 2019年 4月 5日 (2019-04-05) 全文	1-20
A	CN 109245931 A (四川长虹电器股份有限公司) 2019年 1月 18日 (2019-01-18) 全文	1-20
A	KR 102062576 B1 (FOUNDATION OF SOONGSIL UNIVERSITY-INDUSTRY COOPERATION) 2020年 1月 6日 (2020-01-06) 全文	1-20

☐ 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
2020年 12月 4日	2020年 12月 16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 欧晓丹 电话号码 86-(10)-53961416

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/099190

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 110659109 A	2020年 1月 7日	无	
CN 110247810 A	2019年 9月 17日	无	
CN 104486445 A	2015年 4月 1日	CN 104486445 B	2017年 3月 22日
CN 109586999 A	2019年 4月 5日	无	
CN 109245931 A	2019年 1月 18日	无	
KR 102062576 B1	2020年 1月 6日	无	