(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109495331 A
(43)申请公布日 2019.03.19

(21)申请号 201710811225.9

(22)申请日 2017.09.11

(71)申请人 大唐移动通信设备有限公司
地址 100083 北京市海淀区学院路29号

(72)发明人 杨云杰 崔银晓

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王莹 李官

(51)Int.Cl.
H04L 12/26(2006.01)
H04L 12/24(2006.01)

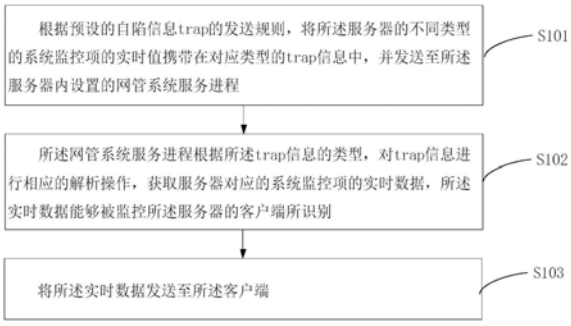
权利要求书2页 说明书6页 附图3页

(54)发明名称

网管系统的系统监控方法及装置

(57)摘要

本发明实施例提供了一种网管系统的系统监控方法及装置，该方法中，服务器将当前的系统监控项的是实时值携带在trap消息中发送给服务器内设置的网管系统服务进程，由该进程根据不同的系统监控项的类型进行适应的trap解析，再将解析后的数据发送至客户端，以使客户端能够及时获取服务器当前被监控项目的状态。从而改变了现有技术中系统监控功能原有的流程，在“推”模式下，借助数据流的流转，实现了查询模式向上报模式的转变，重新设计了系统监控功能的架构实现，使得原有的紧耦合的系统监控流程演变成现有的松散耦合架构，降低了系统监控功能对底层查询状态的接口依赖性，避免底层接口存在问题导致整个系统监控模块功能异常的情况的发生。



CN 109495331 A

1.一种网管系统的系统监控方法,应用于网管系统服务器端,其特征在于,包括:

根据预设的自陷信息trap的发送规则,将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中,并发送至所述服务器内设置的网管系统服务进程;

所述网管系统服务进程根据所述trap信息的类型,对trap信息进行相应的解析操作,获取服务器对应的系统监控项的实时数据,所述实时数据能够被监控所述服务器的客户端所识别;

将所述实时数据发送至所述客户端。

2.根据权利要求1所述的方法,其特征在于,所述预设的自陷信息trap的发送规则为:定时循环发送trap信息。

3.根据权利要求1所述的方法,其特征在于,所述将所述服务器对应的系统监控项的实时值携带在trap信息中,并发送至所述服务器内设置的网管系统服务进程的步骤之前,所述方法还包括:

所述网管系统服务进程在预设的trap信息发送开关开启时,向所述服务器发送trap信息发送请求,所述trap信息发送请求用于指示服务器开始向网管系统服务进程发送trap信息。

4.根据权利要求1所述的方法,其特征在于,所述网管系统服务进程根据所述系统监控项的类型,对trap信息进行相应的解析操作的步骤,包括:

所述网管系统服务进程根据所述系统监控项的不同类型,调用不同的解析处理器,利用各解析处理器将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构。

5.一种网管系统的系统监控装置,应用于网管系统服务器端,其特征在于,包括:

trap信息发送单元,用于根据预设的自陷信息trap的发送规则,将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中,并发送至所述服务器内设置的网管系统服务进程;

解析单元,用于根据所述trap信息的类型,对trap信息进行相应的解析操作,获取服务器对应的系统监控项的实时数据,所述实时数据能够被监控所述服务器的客户端所识别;

通信单元,用于将所述实时数据发送至所述客户端。

6.根据权利要求5所述的装置,其特征在于,所述预设的自陷信息trap的发送规则为:定时循环发送trap信息。

7.根据权利要求5所述的装置,其特征在于,所述装置还包括:

设置在网管系统服务进程内的开关单元,用于在预设的trap信息发送开关开启时,向所述服务器发送trap信息发送请求,所述trap信息发送请求用于指示服务器开始向网管系统服务进程发送trap信息。

8.根据权利要求5所述的装置,其特征在于,所述解析单元,进一步用于:

所述网管系统服务进程根据所述系统监控项的不同类型,调用不同的解析处理器,利用各解析处理器将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构。

9.一种网管系统服务器,包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1-4任一所述方

法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1-4任一所述方法的步骤。

网管系统的系统监控方法及装置

技术领域

[0001] 本发明实施例涉及通信技术领域，具体涉及一种网管系统的系统监控方法及装置。

背景技术

[0002] 在网管系统中，一般都包含系统监控模块，负责监控服务器的内存，磁盘空间，CPU利用率等服务器状态。现有的系统监控实现流程如图1所述。OMT(Operation Maintenance Terminal，操作维护终端)也即客户端启动后，首先进行系统监控模块的初始化设置，例如监控周期，监控粒度和监控数据项的设置。紧接着调用服务器(OMC，Operation Maintenance Center，操作维护中心)的状态监控并接收服务器返回的状态数据，最后在界面渲染数据展示结果。在调用过程中判断监控次数是否达到设定要求，如未达到，则循环。

[0003] 然而，在实现发明创造的过程中，发明人发现，在传统的系统监控模块的实现中，一般都是使用轮询jdk提供的关于主机状态查询的相关接口获取主机状态的实时数据进而监控主机的状态。传统的实现方法从客户端的角度来讲是“拉”模式的实现，也即客户端主动从服务器拉取服务器的状态数据。采用这样的方式使得系统监控功能依赖底层查询状态的接口，如果底层接口存在问题，则会导致整个系统监控模块功能异常，也即传统方法导致了底层实现细节和上层接口的紧耦合。

发明内容

[0004] 本发明实施例的目的在于提供一种用于网管系统的系统监控方法及装置。

[0005] 第一方面，本发明实施例提供了一种网管系统的系统监控方法，包括：

[0006] 根据预设的自陷信息trap的发送规则，将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中，并发送至所述服务器内设置的网管系统服务进程；

[0007] 所述网管系统服务进程根据所述trap信息的类型，对trap信息进行相应的解析操作，获取服务器对应的系统监控项的实时数据，所述实时数据能够被监控所述服务器的客户端所识别；

[0008] 将所述实时数据发送至所述客户端。

[0009] 可选地，所述预设的自陷信息trap的发送规则为：定时循环发送trap信息。

[0010] 可选地，所述将所述服务器对应的系统监控项的实时值携带在trap信息中，并发送至所述服务器内设置的网管系统服务进程的步骤之前，所述方法还包括：

[0011] 所述网管系统服务进程在预设的trap信息发送开关开启时，向所述服务器发送trap信息发送请求，所述trap信息发送请求用于指示服务器开始向网管系统服务进程发送trap信息。

[0012] 可选地，所述网管系统服务进程根据所述系统监控项的类型，对trap信息进行相应的解析操作的步骤，包括：

[0013] 所述网管系统服务进程根据所述系统监控项的不同类型，调用不同的解析处理

器，利用各解析处理器将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构。

[0014] 第二方面，本发明实施例提供了一种网管系统的系统监控装置，包括：

[0015] trap信息发送单元，用于根据预设的自陷信息trap的发送规则，将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中，并发送至所述服务器内设置的网管系统服务进程；

[0016] 解析单元，用于根据所述trap信息的类型，对trap信息进行相应的解析操作，获取服务器对应的系统监控项的实时数据，所述实时数据能够被监控所述服务器的客户端所识别；

[0017] 通信单元，用于将所述实时数据发送至所述客户端。

[0018] 可选地，所述预设的自陷信息trap的发送规则为：定时循环发送trap信息。

[0019] 可选地，所述装置还包括：

[0020] 设置在网管系统服务进程内的开关单元，用于在预设的trap信息发送开关开启时，向所述服务器发送trap信息发送请求，所述trap信息发送请求用于指示服务器开始向网管系统服务进程发送trap信息。

[0021] 可选地，所述解析单元，进一步用于：

[0022] 所述网管系统服务进程根据所述系统监控项的不同类型，调用不同的解析处理器，利用各解析处理器将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构。

[0023] 第三方面，本发明的又一实施例提供了一种网管系统服务器，包括存储器、处理器以及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如第一方面所述方法的步骤。

[0024] 第四方面，本发明的又一实施例提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现如第一方面所述方法的步骤。

[0025] 本发明实施例提供了一种网管系统的系统监控方法及装置，该方法中，服务器将当前的系统监控项的是实时值携带在trap消息中发送给服务器内设置的网管系统服务进程，由该进程根据不同的系统监控项的类型进行适应的trap解析，再将解析后的数据发送至客户端，以使客户端能够及时获取服务器当前被监控项目的状态。从而改变了现有技术中系统监控功能原有的流程，在“推”模式下，借助数据流的流转，实现了查询模式向上报模式的转变，重新设计了系统监控功能的架构实现，使得原有的紧耦合的系统监控流程演变成现有的松散耦合架构，降低了系统监控功能对底层查询状态的接口依赖性，避免底层接口存在问题导致整个系统监控模块功能异常的情况的发生。

附图说明

[0026] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0027] 图1是现有技术中网管系统交互示意图；

[0028] 图2是本发明实施例提供的一种网管系统的系统监控方法流程图；

[0029] 图3是本发明实施例提供的一种网管系统的系统监控方法完整流程图；

[0030] 图4是本发明提供的一种网管系统的系统监控装置实施例结构示意图；

[0031] 图5是本发明提供的一种网管系统服务器设备实施例结构框图。

具体实施方式

[0032] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0033] 第一方面，本发明实施例提供了一种网管系统的系统监控方法，如图2所示，包括：

[0034] S101、根据预设的自陷信息trap的发送规则，将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中，并发送至所述服务器内设置的网管系统服务进程；

[0035] S102、所述网管系统服务进程根据所述trap信息的类型，对trap信息进行相应的解析操作，获取服务器对应的系统监控项的实时数据，所述实时数据能够被监控所述服务器的客户端所识别；

[0036] S103、将所述实时数据发送至所述客户端。

[0037] 本发明实施例提供了一种网管系统的系统监控方法，该方法中，服务器将当前的系统监控项的是实时值携带在trap消息中发送给服务器内设置的网管系统服务进程，由该进程根据不同的系统监控项的类型进行适应的trap解析，再将解析后的数据发送至客户端，以使客户端能够及时获取服务器当前被监控项目的状态。从而改变了现有技术中系统监控功能原有的流程，在“推”模式下，借助数据流的流转，实现了查询模式向上报模式的转变，重新设计了系统监控功能的架构实现，使得原有的紧耦合的系统监控流程演变成现有的松散耦合架构，降低了系统监控功能对底层查询状态的接口依赖性，避免底层接口存在问题导致整个系统监控模块功能异常的情况的发生。

[0038] 其中，这里的网管监控系统为网络管理监控系统。该系统较为通用的协议为SNMP协议(Simple Network Management Protocol，简单网络管理协议)，该协议由一组网络管理的标准组成，包含一个应用层协议(application layer protocol)、数据库模型(database schema)和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。本发明实施例提供的方法正是基于SNMP协议而实现的。

[0039] 这里的预设的自陷信息trap的发送规则具体可以为定时循环发送。

[0040] 此外，这里的服务器对应的系统监控项具体可以是指服务器的内存、服务器的磁盘空间或服务器的CPU利用率等等参数。这里的系统监控项可以根据实际情况来设置，若需要定期监控服务器的内存，则可以定时循环地将服务器当前的内存的实际值携带在trap消息中，以供网管系统服务进程解析并获得客户端能够识别的当前的服务器的内存实际值。

[0041] 为便于理解，下面结合附图对本发明实施例提供的方法进行系统详细的说明。

[0042] 图3示出了本发明实施例提供的方法的流程示意图。为了便于说明其中的交互过程，在图3中将服务器(也即图3中的OMC服务器)中内置的网管系统服务进程(也即图3中的

OMC服务进程)与服务器分离开来进行说明。

[0043] 本发明实施例提供的方法为了避免对网管监控系统的重复开发,因此采用的是网管监控系统已提供的监控主机和自身服务状态的各种接口。具体来说采用的是前文中所述的SNMP协议及该协议支持的基本的通用接口。不难理解的是,为了能够使得网管监控系统的各个设备能够基于该协议进行交互,首先需要对服务器端进行SNMP协议的配置。具体的配置过程如下:

[0044] 在被监控的主机也即OMC服务器需要安装实现SNMP协议的软件,例如net-snmp,用以发送trap消息。本发明实施例中以net-snmp为例,具体发送trap的过程如下:

[0045] 1、在被监控主机上配置snmpd.conf文件(可能目录为/etc/snmp,/usr/local/share/snmp/),添加内容为:

[0046] trap2sink 127.0.0.1:162

[0047] 其中,trap2sink为配置命令;127.0.0.1表示管理端IP也即服务器的IP;冒号后面的162,表示网管系统服务进程接收trap数据的端口号,对于SNMP协议来说,SNMP是基于UDP协议的,固定使用的端口号为161和162,在这里不再对其进行赘述。服务器正是通过162端口向网管系统服务进程发送trap消息。

[0048] 在snmpd.conf文件添加了这一行之后,即表示服务器会主动把事件通过162端口发送给IP同样为127.0.0.1的网管系统服务进程。

[0049] 2、编写脚本,以使服务器能够定时循环发送trap信息,其中trap信息中携带监控项的实时值。

[0050] 例如:snmptrap-v 2c-c public主机IP地址"".1.3.6.1.2.1.25.2.3,

[0051] 其中,-v表示SNMP协议版本,-c为Community Name,也就是访问密码;主机即为服务器;.1.3.6.1.2.1.25.2.3是OID(Object Identifier,对象标识符),也可以是trap结点的名称,可以代表不同类型的trap。指定OID的trap消息只能携带指定类型的系统监控项实时值,例如,携带了服务器内存大小实时值的trap信息,或携带了服务器CPU利用率实时值的trap信息,从而便于后期根据不同的trap消息中的类型进行不同的解析操作。

[0052] 其中,.1.3.6.1.2.1.25.2.3是自定义mib文件中的主机内存trap结点。在本发明实施例中,由于对不同系统监控项的类别进行区分处理,因此需要为每一个系统监控项在自定义mib中编写notification数据结构。自定义mib文件的编写在此不展开。

[0053] 在经过上述步骤配置好了服务器之后,也可以对网管系统服务进程进行配置。可以在网管系统服务进程中配置能够触发服务器定时循环发送trap信息的trap信息发送开关。当该开关被配置为开启状态,则此时如图3所示,网管系统服务进程可以向服务器发送trap信息发送请求。服务器在接收到该请求之后就开始定时循环发送trap信息。而此时网管系统服务进程时刻监听162端口,并接收trap信息。

[0054] 在网管系统服务进程成功接收了trap信息之后,即可以开始根据trap信息的OID所对应的类型不同调用预设的用于处理不同系统监控项的处理器。在各个处理中,将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构,这样的数据结构是可以被客户端所识别的。

[0055] 最后利用jms把对应的Javabean数据发送到客户端也即图3中的OMT端。OMT端在接收了对应数据后,可以进行界面的渲染,将OMT订阅的OMC服务器发布的系统监控数据的jms

消息实时推送显示在界面上，以供工作人员通过显示界面获知OMC服务器的实时系统监控数据。

[0056] 第二方面，本发明实施例提供了一种网管系统的系统监控装置，应用于网管系统服务器端，如图4所示，包括：

[0057] trap信息发送单元201，用于根据预设的自陷信息trap的发送规则，将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中，并发送至所述服务器内设置的网管系统服务进程；

[0058] 解析单元202，用于根据所述trap信息的类型，对trap信息进行相应的解析操作，获取服务器对应的系统监控项的实时数据，所述实时数据能够被监控所述服务器的客户端所识别；

[0059] 通信单元203，用于将所述实时数据发送至所述客户端。

[0060] 可选地，所述预设的自陷信息trap的发送规则为：定时循环发送trap信息。

[0061] 可选地，所述装置还包括：

[0062] 设置在网管系统服务进程内的开关单元，用于在预设的trap信息发送开关开启时，向所述服务器发送trap信息发送请求，所述trap信息发送请求用于指示服务器开始向网管系统服务进程发送trap信息。

[0063] 可选地，所述解析单元202，进一步用于：

[0064] 所述网管系统服务进程根据所述系统监控项的不同类型，调用不同的解析处理器，利用各解析处理器将trap信息中的服务器对应的系统监控项的实时值转换为Java识别的Javabean数据结构。

[0065] 由于本实施例所介绍的网管系统的系统监控装置为可以执行本发明实施例中的网管系统的系统监控方法的装置，故而基于本发明实施例中所介绍的网管系统的系统监控的方法，本领域所属技术人员能够了解本实施例的网管系统的系统监控装置的具体实施方式以及其各种变化形式，所以在此对于该网管系统的系统监控装置如何实现本发明实施例中的网管系统的系统监控方法不再详细介绍。只要本领域所属技术人员实施本发明实施例中网管系统的系统监控方法所采用的装置，都属于本申请所欲保护的范围。

[0066] 图5示出本发明实施例提供的网管系统服务器设备的结构框图。

[0067] 参照图5，该网管系统服务器，包括：处理器(processor)301、存储器(memory)302、总线303以及总线接口304；

[0068] 其中，所述处理器301以及存储器302通过所述总线303完成相互间的通信，总线接口304用于与外界设备进行信息交互；

[0069] 所述处理器301用于调用所述存储器302中的程序指令，以执行上述各方法实施例所提供的方法。

[0070] 本发明实施例还公开一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机能够执行上述各方法实施例所提供的方法。

[0071] 本发明实施例还提供一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令使所述计算机执行上述各方法实施例所提供的方法。

[0072] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0073] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0074] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0075] 此外，本领域的技术人员能够理解，尽管在此的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0076] 本发明的某些部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的网关、代理服务器、系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0077] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

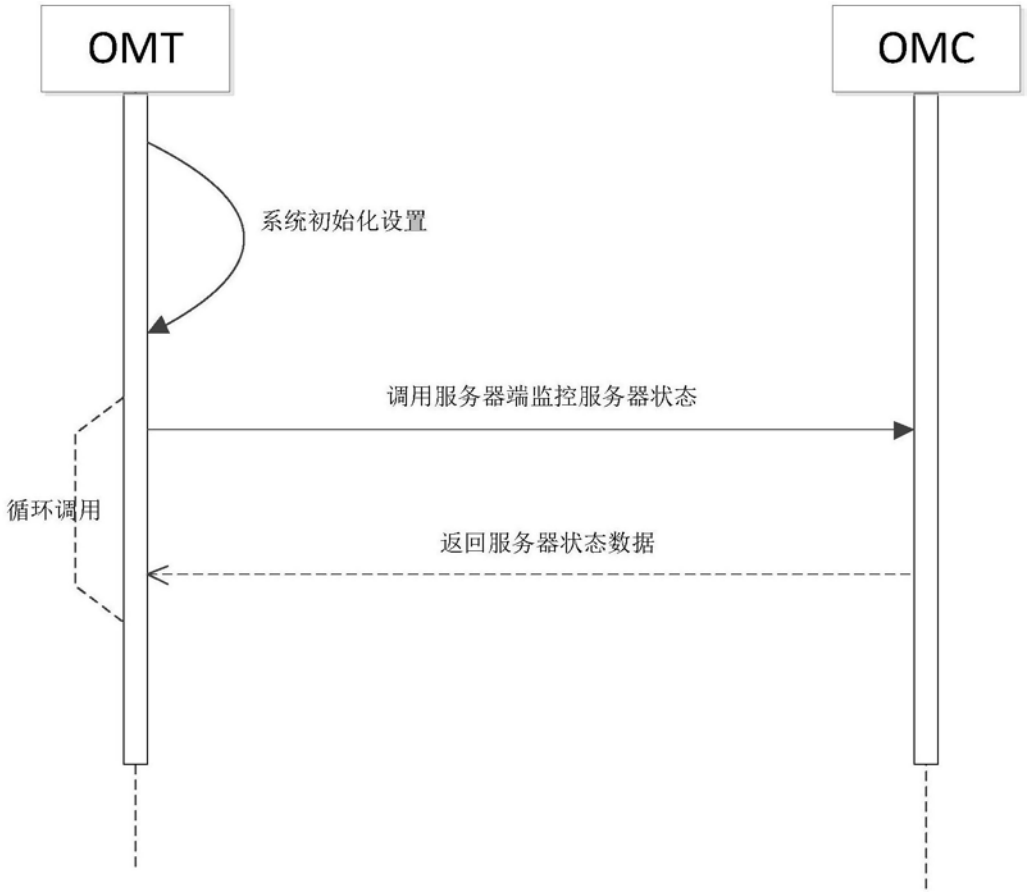

OMT
OMC
系统初始化设置
调用服务器端监控服务器状态
循环调用
返回服务器状态数据

图1

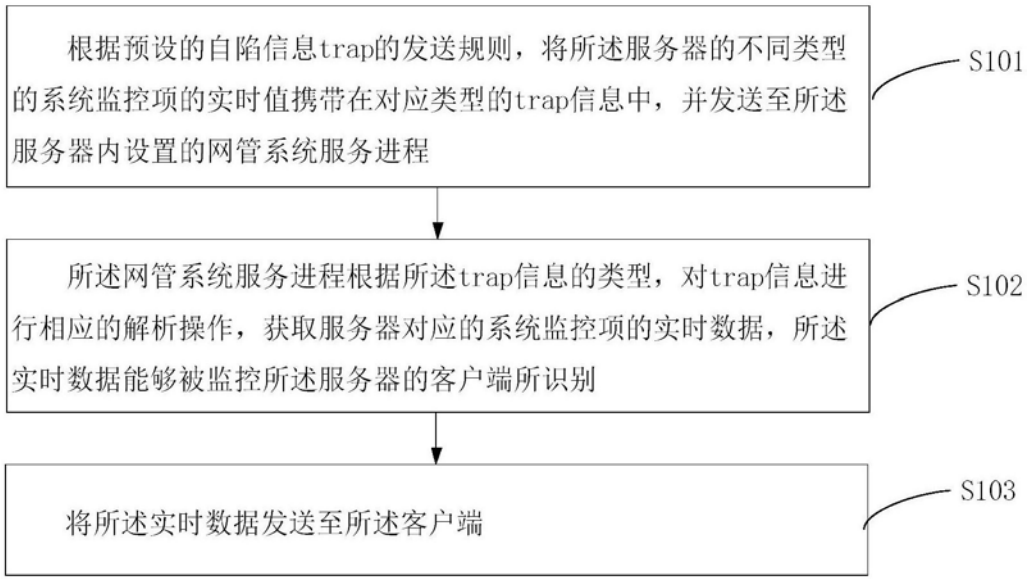

根据预设的自陷信息trap的发送规则，将所述服务器的不同类型的系统监控项的实时值携带在对应类型的trap信息中，并发送至所述服务器内设置的网管系统服务进程
S101
所述网管系统服务进程根据所述trap信息的类型，对trap信息进行相应的解析操作，获取服务器对应的系统监控项的实时数据，所述实时数据能够被监控所述服务器的客户端所识别
S102
将所述实时数据发送至所述客户端
S103

图2

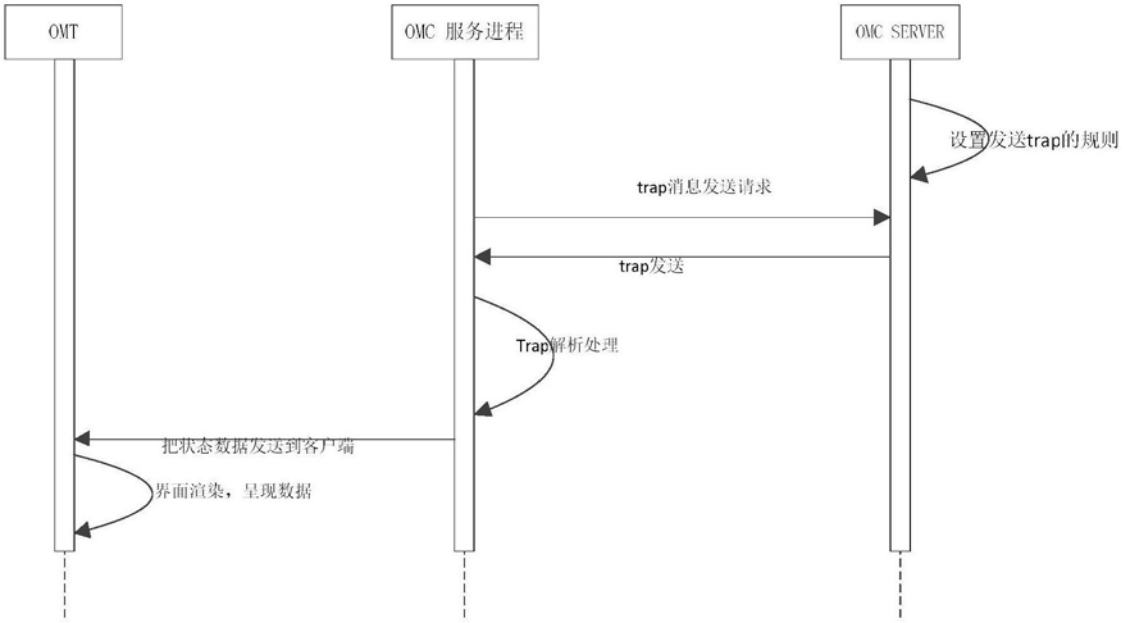

OMT
OMC 服务进程
OMC SERVER
设置发送trap的规则
trap消息发送请求
trap发送
Trap解析处理
把状态数据发送到客户端
界面渲染，呈现数据

图3

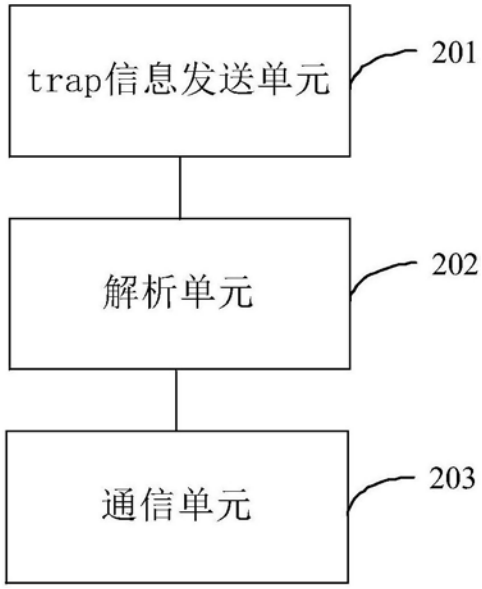

trap信息发送单元
201
解析单元
202
通信单元
203

图4

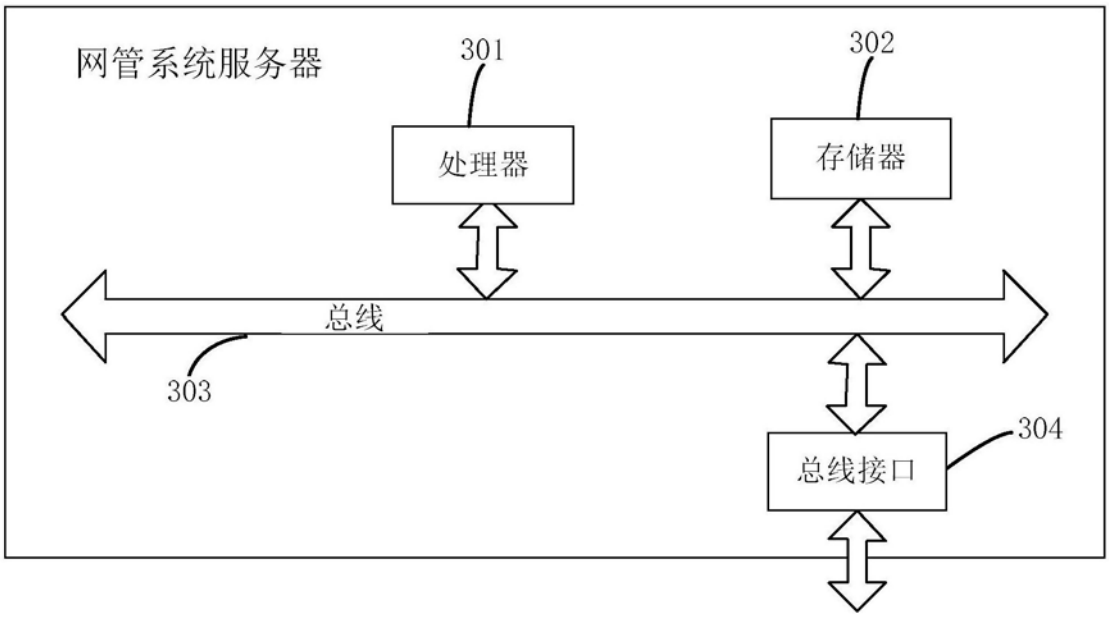


图5