(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102685180 B
(45)授权公告日 2015.07.08

(21)申请号 201110316666.4

(22)申请日 2011.10.18

(73)专利权人 国网电力科学研究院
地址 210003 江苏省南京市鼓楼区南瑞路 8 号

(72)发明人 邓松 林为民 张涛 余勇 车建华 王玉斐 黄秀丽 华晔

(74)专利代理机构 南京知识律师事务所 32207
代理人 汪旭东

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 12/24(2006.01)

(56)对比文件
CN 1349328 A,2002.05.15, 说明书第 4 页第 16 行至第 6 页最后一行,附图 1.
谢振国 . 网络安全预警系统的研究与实现 .《中国优秀硕士学位论文全文数据库 信息科技辑(月刊)》.2011,(第 10 期),I139-171,正文第 19 至 44 页 .

审查员 牛爽

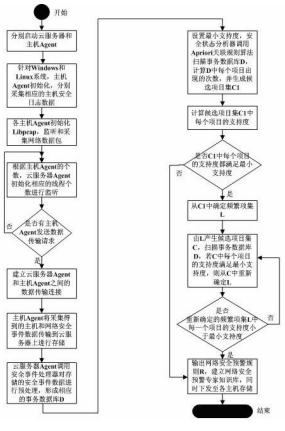
权利要求书1页 说明书5页 附图3页

(54)发明名称

一种面向云计算的网络安全预警方法

(57)摘要

一种面向云计算的网络安全预警方法是一种为了保证云计算环境下网络通信的安全可靠,动态实时地识别和监控云计算环境下各种攻击企图和行为,为面向云计算下各种网络攻击提供实时预警和安全防护的方法。它主要有安全事件采集器、安全事件处理器、安全状态分析器以及网络安全预警操作核心等部分组成。通过 Agent 技术和 Apriori 关联规则算法来更好地解决云计算环境下网络安全预警问题,既解决了云计算环境下各主机安全事件数据的分布式采集,又提高了云计算环境下的网络安全预警和防护能力。



CN 102685180 B

1.一种面向云计算的网络安全预警方法,其特征就在于,包括以下步骤:

步骤1:用户分别启动云服务器和主机Agent;

步骤2:针对Windows和Linux操作系统的主机安全数据,各主机Agent初始化,分别通过Win 32 EventLog API和SWATCH程序来获取相应的日志数据;

步骤3:针对网络安全数据的采集,各主机Agent初始化Libpcap,设置网卡为混杂模式,监听和采集网络数据包;

步骤4:云服务器Agent根据主机Agent的个数N,初始化N个线程分别监听来自各主机Agent的数据传输请求;

步骤5:若云服务器Agent监听到主机Agent有数据传输请求,则云服务器Agent给主机Agent返回一个确认信息,建立云服务器Agent与主机Agent之间的连接,并转至步骤6,否则转至步骤4;

步骤6:各主机Agent则将采集得到的主机和网络安全数据传输到云服务器中进行存储,并提交给安全事件处理器进行预处理,形成符合安全状态分析器所需的主机和网络安全事件事务数据库D;

步骤7:扫描事务数据库D,计算D中所包含的每个项目出现的次数,生成候选项目集C1;

步骤8:计算C1中每个项目的支持度,若大于等于最小支持度,则从C1中确定频繁项集L,否则转至步骤11;

步骤9:由频繁项集L产生候选项目集C,扫描事务数据库D,对候选项目集C中的项进行统计,若大于等于最小支持度,从C中重新确定频繁项集L;

步骤10:若重新确定的频繁项集L中每一个项目的支持度小于最小支持度,转至步骤11,否则转至步骤9;

步骤11:输出网络安全预警规则R,建立网络安全预警专家知识库,并将网络安全预警专家知识库中的网络安全预警规则R下发至各主机;

步骤12:过程结束。

一种面向云计算的网络安全预警方法

技术领域

[0001] 本发明是一种面向云计算环境构建网络安全预警的方法，主要用于云计算网络环境下各种安全威胁的动态监测预警问题，属于信息安全软件领域。

背景技术

[0002] 云计算是分布式计算、并行计算和网格计算发展的延伸，资源共享和按需服务是云计算的主要特征之一，各种业务应用系统能够根据实际需求从共享资源池中获取所需的计算、存储和软件资源。随着云计算的不断发展，各种云计算模式包括公有云、私有云、混合云等共存，各种云计算平台共同组成 Internet 中一个大的资源共享和处理平台，任何一个云计算平台无论受到来自内部或外部的网络攻击，都会给企业带来无法估量的损失。

[0003] 云计算在给人们带来便利的同时，由于其资源的绝对开放和共享也导致各种网络攻击日益频繁和严重。如何在开放、动态和多变的云计算网络环境下实现网络安全主动预警已成为基于云计算的业务应用面临的安全挑战之一。为了保证云计算环境下网络通信的安全可靠，传统的诸如防火墙、入侵检测系统等安全部件部署到网络中。但是，这些安全技术和措施只能事后分析处理和补救。应该需要应用安全预警技术来动态实时地识别和监控云计算环境下各种攻击企图和行为，在攻击发生时或发生前，预先采取相应的安全防护措施来阻止相应的攻击。因此，构建一种面向云计算的网络安全预警方法对于解决云计算环境下来自内部和外部的网络攻击的实时预警和保护，建立云计算环境下网络安全主动防御体系具有重要的意义，同时为云计算环境下各种业务系统的稳定运行提供安全支撑。

[0004] 网络安全预警主要从以下两个方面进行考虑：(1)针对云计算下各主机上所发生的安全事件数据，为了能够为及时预警和防范提供支撑，首先需要对这些安全事件数据进行采集；(2)针对云计算环境下各主机采集得到的安全事件数据经过预处理得到相应的事务数据库后，结合关联规则算法实现网络安全预警规则的挖掘，形成网络安全预警专家知识库，并下发至云计算网络环境下的各主机上，为云计算环境下各主机的安全预警和防护提供依据。

发明内容

[0005] 本发明的目的就是提供一种新的网络安全预警方法，来解决云计算网络环境下网络安全的预警问题，本机制是一种策略性方法，通过使用本方法可以使得在发生网络安全时最大限度地保护网络安全，从而保障整个网络中各种业务应用的安全。

[0006] 本发明的方法是一种策略性的方法，首先通过 Agent 采集部署在云计算环境下各种网络设备的安全事件，并进行相应的预处理，然后通过 Aprior 关联规则算法挖掘分析安全事件中蕴含的攻击模式，从而为网络安全预警提供依据。

[0007] 一、体系结构

[0008] 图 1 给出了一种面向云计算的网络安全预警的结构图，它主要包括四个部分：安全事件采集器、安全事件处理器、安全状态分析器及网络安全预警操作核心。图中的网络安

全预警操作核心包括了在网络中各种安全数据的采集和智能处理分析好的情况下，对各种安全威胁进行检测和预警的具体操作。本发明增加了其它三个部分保证安全威胁防护更加顺利有效地进行，最大限度地保证各种安全威胁事件的动态监测和预警。

[0009] 下面给出具体介绍：

[0010] 安全事件采集器：在进行网络威胁防护中，最基础的就是各种网络安全事件的采集，在本发明中采用 Agent 的方式对分布在网络中的各种网络安全数据进行分布式采集，利用各种 Agent 之间的分布式协作，实时采集网络和主机上的各种安全事件和数据，同时各个 Agent 对实时采集到的各种网络安全事件和数据进行相应的预处理。

[0011] 安全事件处理器：网络安全数据来源于交换机、路由器、防病毒软件以及各类网络管理软件，可能包含噪声数据、空缺数据和不一致数据，这对数据分析将会产生不良后果。在本发明中，分别通过数据清理、数据转换和数据归并三个步骤来保证采集得到的各种网络安全事件数据的完整性、冗余数据及其属性的去除和归一化，以便完成各种网络安全事件数据的形式和内容符合下面关联分析的要求。在本专利中对安全事件处理器的具体实现不做任何限制。

[0012] 安全状态分析器：通过安全事件采集器的网络安全数据经过安全事件处理器预处理后，首先将其分布式存储在云计算数据中心中，然后通过安全状态分析器对存储在云计算数据中心中的各种网络安全事件基于 Apriori 关联规则算法进行智能关联分析，得出各种网络安全事件之间的关联规则，同时将分析的结果返回给连接在云计算中的所有客户端，以便客户端及时对各种网络安全威胁进行及时预警。

[0013] 二、方法流程

[0014] 1、安全事件采集器

[0015] 数据源的选择是网络安全预警系统中最重要的部分。在系统运行过程中，无论是内部行为还是外部行为，都会在系统中留下痕迹，并且对于一个特定的事件，不同的网络安全数据之间存在着某种必然的联系。因此，为了确保更好地进行分析，系统必须做到多层次、多角度的数据采集。

[0016] 本发明专利中使用 Agent 技术实现云计算环境下多数据源的分布式采集，如图 2 所示。将数据采集 Agent 分布在云计算环境下的各种主机、服务器或其他网络节点上，根据事先制定的数据采集规则进行采集，同时将采集得到的各种网络安全数据通过安全信道传递到云服务器端进行综合分析。在本发明专利中，同时还提供数据采集 Agent 的配置功能，保证 Agent 的有用性，同时还实现云计算环境下的多数据协同关联分析。

[0017] 从图 2 中可以看出，本发明专利中所选取的数据源主要分为主机安全数据和网络安全数据两部分。本发明中主机安全数据主要针对 Windows 和 Linux 系统，其他操作系统不在考虑范围内，两种操作系统的主机安全数据都是基于日志采集得到，其中 Windows 操作系统的主机安全数据使用 Win 32 EventLog API 来获取，Linux 操作系统的主机安全数据通过使用 Todd Atkins 开发的 SWATCH 程序获取。本发明中网络安全数据主要基于开源的 Libpcap 包来采集得到。

[0018] 整个基于 Agent 的分布式安全事件采集的流程如下：

[0019] (1) 分别启动云服务器和主机 Agent；

[0020] (2) 待采集的主机和网络安全事件数据的属性、格式定义；

[0021] (3) 云服务器 Agent 与各主机 Agent 建立连接，云服务器 Agent 等待主机 Agent 发送采集的主机和网络日志数据；

[0022] (4) 针对 Windows 和 Linux 操作系统的主机安全数据，各主机 Agent 初始化，分别通过 Win 32 EventLog API 和 SWATCH 程序来获取相应的日志数据；

[0023] (5) 针对网络安全数据的采集，各主机 Agent 初始化 Libpcap，设置网卡为混杂模式，监听和采集网络数据包；

[0024] (6) 各主机 Agent 向云服务器 Agent 发送数据传输请求，云服务器 Agent 接收到该请求后返回给各主机 Agent 一个确认信息，各主机 Agent 则将采集得到的主机和网络安全数据传输到云服务器中进行分布式存储，并提交给安全事件处理器进行预处理，形成符合安全状态分析器所需的数据格式。

[0025] 2、安全状态分析器

[0026] 随着云计算环境的日益复杂化及网络数据的急剧膨胀，基于主机和网络等安全数据以惊人的速度增长，云计算环境下网络安全预警亟需从大量的安全数据中发现用户违规或可能发生的威胁行为。本专利使用 Apriori 关联规则算法进行各种用户或威胁行为之间的智能关联分析，挖掘出这些安全数据之间的关联规则，并将挖掘得到的各种关联规则存储在云服务器端的专家知识库中，同时将各种关联规则自动下发至各主机中存储，各主机依据此规则及时对各种网络安全威胁进行防护和预警。

[0027] 设当前由安全事件处理器得到的主机和网络安全事件数据库为事务数据库 D，最小支持度为 minSup。其中 D 中的每一个项目对应主机和网络安全数据中的属性，项目值对应属性值。

[0028] 主要工作流程如下：

[0029] (1) 扫描事务数据库 D，计算 D 中所包含的每个项目出现的次数，生成候选项目集 C1；

[0030] (2) 计算 C1 中每个项目的支持度，若大于等于 minSup，则从 C1 中确定频繁项集 L，否则转至第 (5) 步；

[0031] (3) 由频繁项集 L 产生候选项目集 C，扫描事务数据库 D，对候选项目集 C 中的项进行统计，若大于等于 minSup，从 C 中重新确定频繁项集 L；

[0032] (4) 若 L 中每一个项目的支持度小于 minSup，转至第 (5) 步，否则转至第 (3) 步；

[0033] (5) 过程结束，输出规则 R；

[0034] 通过 Apriori 关联规则算法从主机和网络安全事件数据中挖掘出相应的行为关联规则，为云计算环境下的网络安全预警提供支撑。

[0035] 本发明的一种面向云计算的网络安全预警方法的步骤为：

[0036] 步骤 1：用户分别启动云服务器和主机 Agent；

[0037] 步骤 2：针对 Windows 和 Linux 操作系统的主机安全数据，各主机 Agent 初始化，分别通过 Win 32 EventLog API 和 SWATCH 程序来获取相应的日志数据；

[0038] 步骤 3：针对网络安全数据的采集，各主机 Agent 初始化 Libpcap，设置网卡为混杂模式，监听和采集网络数据包；

[0039] 步骤 4：云服务器 Agent 根据主机 Agent 的个数 N，初始化 N 个线程分别监听来自各主机 Agent 的数据传输请求；

[0040] 步骤 5 :若云服务器 Agent 监听到主机 Agent 有数据传输请求,则云服务器 Agent 给主机 Agent 返回一个确认信息,建立云服务器 Agent 与主机 Agent 之间的连接,并转至步骤 6,否则转至步骤 4 ;

[0041] 步骤 6 :各主机 Agent 则将采集得到的主机和网络安全数据传输到云服务器中进行存储,并提交给安全事件处理器进行预处理,形成符合安全状态分析器所需的主机和网络安全事件事务数据库 D ;

[0042] 步骤 7 :扫描事务数据库 D,计算 D 中所包含的每个项目出现的次数,生成候选项目集 C1 ;

[0043] 步骤 8 :计算 C1 中每个项目的支持度,若大于等于最小支持度,则从 C1 中确定频繁项集 L,否则转至步骤 11 ;

[0044] 步骤 9 :由频繁项集 L 产生候选项目集 C,扫描事务数据库 D,对候选项目集 C 中的项进行统计,若大于等于最小支持度,从 C 中重新确定频繁项集 L ;

[0045] 步骤 10 :若重新确定的频繁项集 L 中每一个项目的支持度小于最小支持度,转至步骤 11,否则转至步骤 9 ;

[0046] 步骤 11 :输出网络安全预警规则 R,建立网络安全预警专家知识库,并将网络安全预警专家知识库中的网络安全预警规则 R 下发至各主机 ;

[0047] 步骤 12 :过程结束。

[0048] 本发明方法提出了一种面向云计算的网络安全预警方法,主要用于解决云计算环境下的网络安全预警问题,通过使用本发明中提出的方法既可以监控当前云计算环境下各主机和网络的安全状态,又可以提高云计算环境下的网络安全预警能力。

[0049] 安全事件采集器首先通过将 Agent 部署在云计算中的各个主机和云服务器上,然后建立主机 Agent 和云服务器 Agent 之间的网络连接,接着主机 Agent 通过 Win 32 EventLog API 和 SWATCH 程序采集 Windows 和 Linux 下的主机安全日志数据 ;通过调用 Libpcap 工具包采集网络安全数据。最后主机 Agent 向云服务器 Agent 发送一个数据传输请求,在云服务器 Agent 返回一个确认信息后,各主机 Agent 分布式并行把各自采集得到的主机和网络安全事件数据传送给云服务器进行存储。

[0050] 安全状态分析器通过使用 Apriori 关联规则算法来对各主机采集来的主机和网络安全事件数据所组成的事务数据库 D 进行规则挖掘,首先设置最小支持度 minSup,然后扫描事务数据库 D 中每个项目出现的次数,生成相应的候选项目集 C1,根据事先设置的最小支持度计算 C1 中的每一个项目的支持度,并确定频繁项集 L,直到频繁项集 L 中的每一个项目的支持度都满足最小支持度为止,同时输出相应的网络安全预警规则 R,并建立专家知识库下发至云计算网络中的各主机上,各主机根据专家知识库中的网络安全预警规则进行及时预警和防护。

附图说明

[0051] 图 1 是一种面向云计算的网络安全预警组成结构图。主要包括 :安全事件采集器、安全事件处理器、安全状态分析器以及网络安全预警操作核心 ;

[0052] 图 2 是云计算环境下多数据源的分布式采集示意图 ;

[0053] 图 3 是参考体系结构示意图。表示本发明方法包括的组件 ;

[0054] 图 4 是本发明方法的流程示意图。

具体实施方式

[0055] 为了方便描述，我们假设有如下应用实例：

[0056] 某企业基于 Internet 建立公有云计算平台，其中包含 N 个主机和由多台服务器组成的云服务器集群，同时分别在 N 个主机和云服务器上部署相应的 Agent 程序。为了构建面向该云计算的网络安全预警平台，需要 N 各主机各自采集相应的主机和网络安全事件数据传输到云服务器中进行存储、预处理和分析，并建立网络安全预警规则库，以便在发生网络安全事件时及时进行网络安全预警，从而为公司云计算平台提供及时的安全防护。

[0057] 其具体的实施方案为：

[0058] (1) 分别启动主机和云服务器 Agent，同时云服务器 Agent 处于网络监听状态，不断监听主机 Agent 是否有数据传输请求，若主机 Agent 有数据传输请求，则建立主机 Agent 和云服务器 Agent 的网络连接；

[0059] (2) 安全事件采集器针对 Windows 和 Linux 操作系统的主机安全数据，各主机 Agent 初始化，分别通过 Win 32 EventLog API 和 SWATCH 程序来获取相应的日志数据；针对网络安全数据的采集，各主机 Agent 初始化 Libpcap，设置网卡为混杂模式，监听和采集网络数据包；

[0060] (3) 各主机 Agent 将采集得到的主机和网络安全数据传输到云服务器中进行存储，并提交给安全事件处理器进行去噪、合并和归一化等预处理，形成符合安全状态分析器所需的主机和网络安全事件事务数据库 D；

[0061] (4) 安全状态分析器调用 Apriori 关联规则算法对各主机采集来的主机和网络安全事件数据所组成的事务数据库 D 进行关联规则挖掘；

[0062] (5) 将安全状态分析器得到的网络安全预警关联规则进行存储，形成网络安全预警专家知识库；

[0063] (6) 云服务器 Agent 将网络安全预警专家知识库下发至各主机中进行备份；

[0064] (7) 整个面向云计算的网络安全预警规则已经形成，同时在云计算网络中的各主机上进行了规则更新备份，便于为各主机在发生网络安全事件时提供及时预警和安全防护。整个面向云计算的网络安全预警过程结束。


网络安全预警
操作核心
安全状态分析器
安全事件处理器
安全事件采集器

图 1

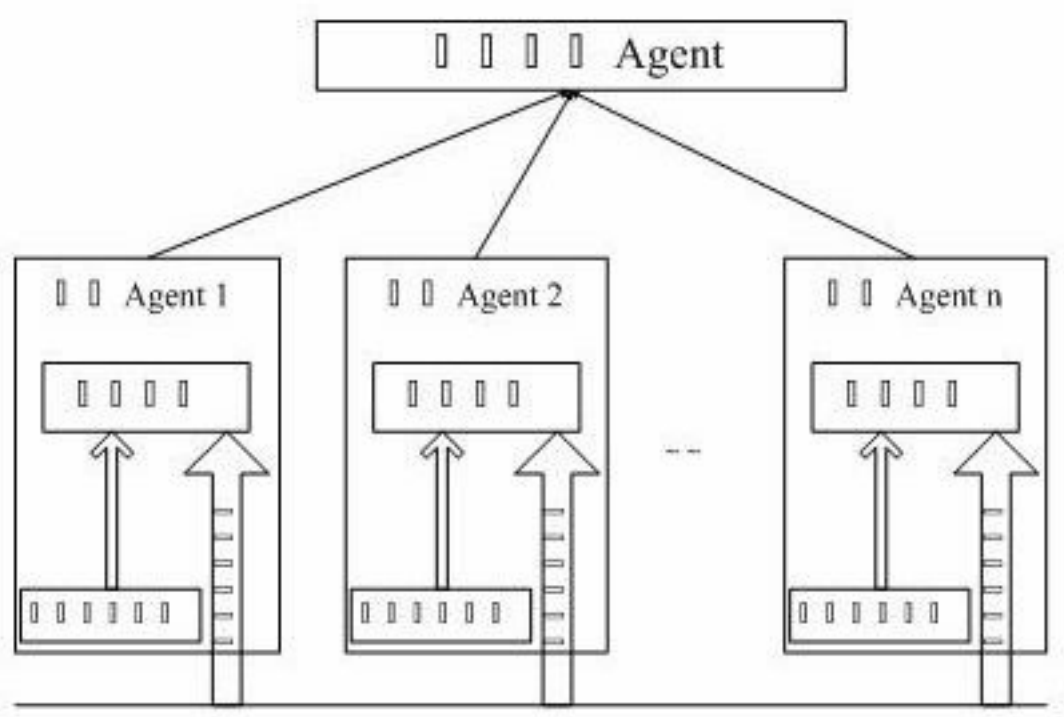

Agent
Agent 1
Agent 2
Agent n

图 2

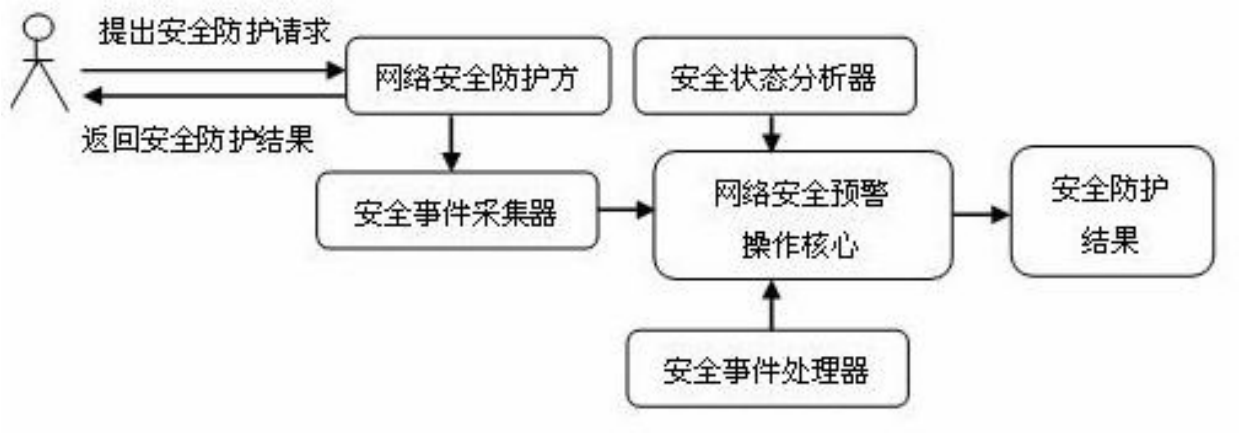

提出安全防护请求
返回安全防护结果
网络安全防护方
安全状态分析器
安全事件采集器
网络安全预警
操作核心
安全防护
结果
安全事件处理器

图 3

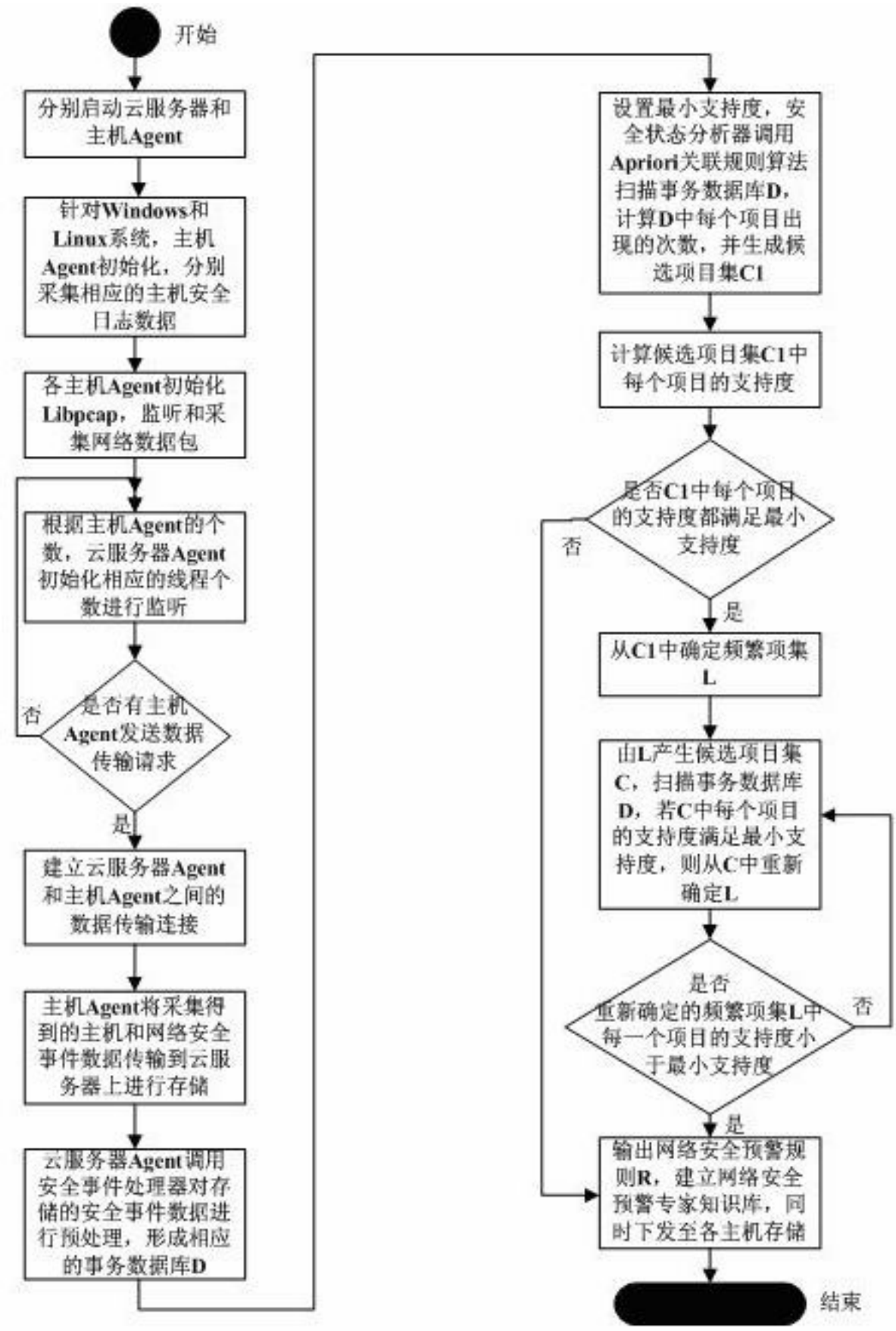

开始
分别启动云服务器和主机Agent
针对Windows和Linux系统，主机Agent初始化，分别采集相应的主机安全日志数据
各主机Agent初始化Libpcap，监听和采集网络数据包
根据主机Agent的个数，云服务器Agent初始化相应的线程个数进行监听
是否有主机Agent发送数据传输请求
否
是
建立云服务器Agent和主机Agent之间的数据传输连接
主机Agent将采集得到的主机和网络安全事件数据传输到云服务器上进行存储
云服务器Agent调用安全事件处理器对存储的安全事件数据进行预处理，形成相应的事务数据库D
设置最小支持度，安全状态分析器调用Apriori关联规则算法扫描事务数据库D，计算D中每个项目出现的次数，并生成候选项目集C1
计算候选项目集C1中每个项目的支持度
是否C1中每个项目的支持度都满足最小支持度
否
是
从C1中确定频繁项集L
由L产生候选项目集C，扫描事务数据库D，若C中每个项目的支持度满足最小支持度，则从C中重新确定L
是否重新确定的频繁项集L中每一个项目的支持度小于最小支持度
否
是
输出网络安全预警规则R，建立网络安全预警专家知识库，同时下发至各主机存储
结束

图 4