(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110855493 B
(45)授权公告日 2022.08.09

(21)申请号 201911127908.8

(22)申请日 2019.11.18

(65)同一申请的已公布的文献号
申请公布号 CN 110855493 A

(43)申请公布日 2020.02.28

(73)专利权人 上海新炬网络信息技术股份有限公司
地址 201707 上海市青浦区外青松公路7548弄588号1幢1层R区113室

(72)发明人 程永新 郭伟 李宏旭

(74)专利代理机构 上海科律专利代理事务所(特殊普通合伙) 31290
专利代理师 袁亚军

(51)Int.Cl.
H04L 41/12(2022.01)

(56)对比文件
CN 103248512 A,2013.08.14
CN 108696450 A,2018.10.23
CN 105763357 A,2016.07.13
CN 107171879 A,2017.09.15

审查员 杨梅

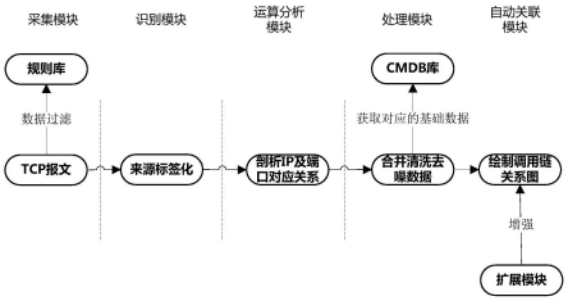
权利要求书2页 说明书5页 附图1页

(54)发明名称

用于混合环境的应用拓扑图绘制装置

(57)摘要

本发明公开了一种用于混合环境的应用拓扑图绘制装置,包括:采集模块,采集业务数据并生成TCP报文;识别模块,对采集模块传入的TCP报文进行来源和目的地识别,获取TCP报文对应的IP地址及端口信息;运算分析模块,根据TCP连接剖析IP地址及端口的对应关系;处理模块,根据IP地址及端口确认对应的应用进程,获取实际调用的应用模块名称,确认应用模块间的调用关系;自动关联模块,调用绘图功能绘制应用模块的调用链关系图。本发明增加规则库自动匹配,减少冗余数据传入;TCP报文自动识别,实现自动化分析过程;实现快速清洗数据及匹配CMDB库,生成调用链应用关系拓扑图。



CN 110855493 B

1.一种用于混合环境的应用拓扑图绘制装置,其特征在于,包括:

采集模块,采集业务数据并生成TCP报文;

识别模块,对采集模块传入的TCP报文进行来源和目的地识别,获取TCP报文对应的IP地址及端口信息;

运算分析模块,根据TCP连接剖析IP地址及端口的对应关系;

处理模块,根据IP地址及端口确认对应的应用进程,获取实际调用的应用模块名称,确认应用模块间的调用关系;

自动关联模块,调用绘图功能绘制应用模块的调用链关系图;

所述采集模块首先根据业务流量抓取cap数据包,然后通过分类识别器对cap数据包进行识别,保存识别出的TCP报文,并将非TCP报文丢弃,将识别出的TCP报文通过规则库中的业务规则进行数据过滤,最终按规则库的业务规则得到定制化的TCP报文;

所述识别模块识别采集模块传入的TCP报文,所述TCP报文封装在IP数据报中,所述识别模块解析封装TCP报文的IP数据报,获取TCP报文对应的IP数据报的源IP地址和目的IP地址;解析TCP报文的首部,获取TCP报文的源端口和目的端口;

所述源端口和源IP地址标识报文的返回地址,所述目的IP地址指明接收方计算机,所述目的端口指明接收方计算机上的应用程序接口;所述TCP报文的端口用来标识计算机不同的应用进程,TCP报文中的源端口和目的端口同IP数据报中的源IP地址与目的IP地址唯一确定一条TCP连接;

所述运算分析模块汇总识别模块分析TCP报文得到源IP地址、源端口、目的IP地址和目的端口,通过TCP连接建立源IP地址、源端口、目的IP地址和目的端口间的关联关系,筛选多段时间内多次进行相同的TCP连接的关联关系,归并具有相同的源IP地址、源端口、目的IP地址和目的端口的关联关系,生成一条调用关联关系,将无法合并的关联关系废弃,确认生成的调用关联关系的源IP地址、源端口、目的IP地址和目的端口;

所述处理模块查询配置管理数据库,将每条调用关联关系与配置管理数据库进行匹配,获取调用关联关系的源IP地址对应的计算机中源端口对应的应用进程及相关联的应用模块名称,获取调用关联关系的目的IP地址对应的计算机中目的端口对应的应用进程及相关联的应用模块名称,确认应用模块间的实际调用关系,将该调用关系存储在配置管理数据库;将在配置管理数据库中已存在的调用关系丢弃,完成去噪;将不存在调用关系的应用模块的名称推送至配置管理数据库管理页面提醒更新;在配置管理数据库数据更新后,将所有应用模块间的调用关系提交至自动关联模块。

2.如权利要求1所述的用于混合环境的应用拓扑图绘制装置,其特征在于,所述采集模块将捕获的不同网络传输协议下的网络数据帧格式存储下来,将每间隔一个时间周期获取的一个文件则定义为一个cap数据包;所述cap数据包是一种全十六进制的数据文件,通过解析cap数据包,得到的数据帧内容,所述数据帧内容包含有TCP报文、UDP和FTP各种网络协议的数据存储格式。

3.如权利要求1所述的用于混合环境的应用拓扑图绘制装置,其特征在于,所述自动关联模块通过应用模块间的调用关系,调用图形控件绘制应用模块间调用链关系图。

4.如权利要求1所述的用于混合环境的应用拓扑图绘制装置,其特征在于,所述自动关联模块设有扩展接口,所述扩展接口接入扩展模块,所述扩展模块包括日志预警模块和容

量监测模块;所述日志预警模块进行节点故障和预警的展示,所述日志预警模块将模块所在的应用日志的报错和错误分类实时推送至应用节点;所述容量监测模块进行节点容量的监测,所述容量监测模块将模块所在的应用主机及进程的性能指标和设置阈值实时推送至应用节点,并对增长趋势进行对比分析得到预测结果;所述自动关联模块通过日志预警模块和/或容量监测模块进行故障的定位及回溯。

用于混合环境的应用拓扑图绘制装置

技术领域

[0001] 本发明涉及一种应用拓扑图绘制装置，尤其涉及一种用于混合环境的应用拓扑图绘制装置。

背景技术

[0002] 由于虚拟化和容器化的普及，IT系统各种应用均迁移至虚拟化、容器化环境中，且各类业务系统不断更新迭代以及架构不断创新优化，使得系统模块调用链关系更加复杂，加之非常用链接识别难度加剧，导致模块相关的IT运维人员无法全面分析具体链路的应用异常，而自动应用拓扑的度量展示能力更显突出，更有利于识别系统故障的所在应用模块。

[0003] 目前现有的网络拓扑自动发现系统原理主要有3种方案：

[0004] 1、利用IP报文进行路由探测并分析结果绘制网络拓扑图。

[0005] 网络拓扑自动发现代理模块获取IP报文的网络类型直连网络，对IP报文的目的IP地址进行请求立即应答探测，得到第一探测结果；若IP报文的网络类型为路由网络，对IP报文的目的IP地址进行路由探测，以获取到本端和对端之间的路由器的IP地址；分别对路由器的IP地址、IP报文的目的IP地址进行请求立即应答探测，得到第二探测结果；向网络拓扑发现分析服务器上报第一探测结果或第二探测结果，以使网络拓扑发现分析服务器接收到第一探测结果或第二探测结果之后绘制网络拓扑图。基于集群化、容器化及多负载均衡的混合环境中，业务应用种类繁多无法区分，IP信息无需聚合应用为服务端，难以发现具体应用侧的相关性，只能展示网络侧理解，未能深入数据挖掘的二次开发。

[0006] 2、基于SNMP网络管理运行环境，采集数据节点信息进行拓扑发现及故障定位。

[0007] 在简单网络管理协议SNMP网络管理运行的环境中，目标网络的每个网络节点配置一个管理信息库MIB；通过应用层协议对每个管理信息库MIB进行访问，采集中间系统到中间系统IS-IS配置数据信息；根据采集到的IS-IS配置数据信息绘制目标网络的每个网络节点的IS-IS网络拓扑图。基于SNMP的IS-IS协议识别、拓扑发现、故障定位提供了实现方案，当集群化及容器化应用多IP信息未聚合应用服务端，导致网络拓扑图关联关系太多太乱，无法直观分析某个模块节点的应用异常。

[0008] 3、依据物理网络的逻辑拓扑结构，镜像流量从而进行网络链路的拓扑绘制。

[0009] 在网络流量镜像方法的获取中，需存储量巨大的服务侧，依据分析业务流向，侧重在分析流量，而未反映在应用侧的关联关系及拓扑数据聚合，以及部署应用探针，获取IP端口交互TCP报文，引起资源占用情况，该方案在数据过滤方面展现不足，存储机器及探针资源消耗较大，而绘制出的网络拓扑图未涉及应用侧调用关系，无法分析伸缩拓扑关系列表。

[0010] 基于小型机、集群化、容器化、跨区域、模块化及微服务的调用方式错综复杂，传统IT及新型IT应用大量融合及新业务不断扩展，并且分割模块化运维趋势越来越多，现有的方案难以掌控全面系统节点的应用调用链情况，造成遗漏的链接及临时增加链接无法实时识别，上述的3种方法主要存在以下缺点：

[0011] 方案1缺少自动化识别应用过程，无法实现业务故障节点定位，方案1主要依赖TCP

报文探测,能识别网络关系调用,也能绘制交换机及路由侧的网络关系,但当某应用模块通过负载均衡后端出现N台应用,此方案则无法自动化识别调用应用的服务方,更无从谈起应用故障的探测。

[0012] 方案2在混合环境中无法精简识别具体应用模块,方案2通过SNMP协议管理网络节点,依赖于网卡侧及固定端口监测并提供数据分析,如集群或容器中有多个不同应用部署,而是内部调用关系,该方案则在这种复杂的环境中难以识别是否同一个应用而分析出具体的拓扑关系;

[0013] 方案3实时报文信息过滤分析能力不足,无法满足繁多的应用业务系统,方案3是通过镜像流量,但拥有庞大流量分析,需提供更多机器资源进行存储,并且缺少丢弃冗余数据的过滤分析过程,无法快速精准在庞大业务群的服务侧识别关键调用链信息。

[0014] 现有的技术方案都存在各种的不足,无法满足庞大IT应用系统的应用分析需求,对业务生产故障无法全面掌控,缺乏直观应用故障异常点检测,以及不便于其他功能扩展及增强,因此本提案提出了适应于混合环境中,智能应用拓扑图绘制装置,通过TCP报文分析后,进行过滤聚合有用的信息,实现智能绘制应用拓扑图,同时引入日志分析结果集及容量管控等功能扩展,实现基于应用拓扑的功能增强,提升运维效率。

发明内容

[0015] 本发明要解决的技术问题是提供一种用于混合环境的应用拓扑图绘制装置,解决上述问题。

[0016] 本发明为解决上述技术问题而采用的技术方案是提供一种用于混合环境的应用拓扑图绘制装置,包括:采集模块,采集业务数据并生成TCP报文;识别模块,对采集模块传入的TCP报文进行来源和目的地识别,获取TCP报文对应的IP地址及端口信息;运算分析模块,根据TCP连接剖析IP地址及端口的对应关系;处理模块,根据IP地址及端口确认对应的应用进程,获取实际调用的应用模块名称,确认应用模块间的调用关系;自动关联模块,调用绘图功能绘制应用模块的调用链关系图。

[0017] 进一步的,所述采集模块首先根据业务流量抓取cap数据包,然后通过分类识别器对cap数据包进行识别,保存识别出的TCP报文,并将非TCP报文丢弃,将识别出的TCP报文通过规则库中的业务规则进行数据过滤,最终按规则库的业务规则得到定制化的TCP报文。

[0018] 进一步的,所述采集模块将捕获的不同网络传输协议下的网络数据帧格式存储下来,将每间隔一个时间周期获取的一个文件则定义为一个cap数据包;所述cap数据包是一种全十六进制的数据文件,通过解析cap数据包,得到的数据帧内容,所述数据帧内容包含有TCP报文、UDP和FTP各种网络协议的数据存储格式。

[0019] 进一步的,所述识别模块识别采集模块传入的TCP报文,所述TCP报文封装在IP数据报中,所述识别模块解析封装TCP报文的IP数据报,获取TCP报文对应的IP数据报的源IP地址和目的IP地址;解析TCP报文的首部,获取TCP报文的源端口和目的端口。

[0020] 进一步的,所述源端口和源IP地址标识报文的返回地址,所述目的IP地址指明接收方计算机,所述目的端口指明接收方计算机上的应用程序接口;所述TCP报文的端口用来标识计算机不同的应用进程,TCP报文中的源端口和目的端口同IP数据报中的源IP地址与目的IP地址唯一确定一条TCP连接。

[0021] 进一步的，所述运算分析模块汇总识别模块分析TCP报文得到源IP地址、源端口、目的IP地址和目的端口，通过TCP连接建立源IP地址、源端口、目的IP地址和目的端口间的关联关系，筛选多段时间内多次进行相同的TCP连接的关联关系，归并具有相同的源IP地址、源端口、目的IP地址和目的端口的关联关系，生成一条调用关联关系，将无法合并的关联关系废弃，确认生成的调用关联关系的源IP地址、源端口、目的IP地址和目的端口。

[0022] 进一步的，所述处理模块查询配置管理数据库，将每条调用关联关系与配置管理数据库进行匹配，获取调用关联关系的源IP地址对应的计算机中源端口对应的应用进程及相关联的应用模块名称，获取调用关联关系的目的IP地址对应的计算机中目的端口对应的应用进程及相关联的应用模块名称，确认应用模块间的实际调用关系，将该调用关系存储在配置管理数据库；将在配置管理数据库中已存在的调用关系丢弃，完成去噪；将不存在调用关系的应用模块的名称推送至配置管理数据库管理页面提醒更新；在配置管理数据库数据更新后，将所有应用模块间的调用关系提交至自动关联模块。

[0023] 进一步的，所述自动关联模块通过应用模块间的调用关系，调用图形控件绘制应用模块间调用链关系图。

[0024] 进一步的，所述自动关联模块设有扩展接口，所述扩展接口接入扩展模块，所述扩展模块包括日志预警模块和容量监测模块；所述日志预警模块进行节点故障和预警的展示，所述日志预警模块将模块所在的应用日志的报错和错误分类实时推送至应用节点；所述容量监测模块进行节点容量的监测，所述容量监测模块将模块所在的应用主机及进程的性能指标和设置阈值实时推送至应用节点，并对增长趋势进行对比分析得到预测结果；所述自动关联模块通过日志预警模块和/或容量监测模块进行故障的定位及回溯。

[0025] 本发明对比现有技术有如下的有益效果：本发明提供的用于混合环境的应用拓扑图绘制装置，具有以下优点：1、增加规则库自动匹配，无需分析所有的TCP报文，减少冗余数据传入；2、TCP报文自动识别，数据采集聚合后丢弃数据，实现自动化分析过程，无需增加大量存储；3、实现快速清洗数据及匹配CMDB库，完成基础数据比对及结果输出，生成调用链应用关系拓扑图；4、实现接口模块化接入，最终完成故障、容量的节点展示分析，提升自动化运维效率。

附图说明

[0026] 图1为本发明实施例中用于混合环境的应用拓扑图绘制装置结构示意图。

具体实施方式

[0027] 下面结合附图和实施例对本发明作进一步的描述。

[0028] 图1为本发明实施例中用于混合环境的应用拓扑图绘制装置结构示意图。

[0029] 请参见图1，本发明提供的用于混合环境的应用拓扑图绘制装置，包括：采集模块，采集业务数据并生成TCP报文；识别模块，对采集模块传入的TCP报文进行来源和目的地识别，获取TCP报文对应的IP地址及端口信息；运算分析模块，根据TCP连接剖析IP地址及端口的对应关系；处理模块，根据IP地址及端口确认对应的应用进程，获取实际调用的应用模块名称，确认应用模块间的调用关系；自动关联模块，调用绘图功能绘制应用模块的调用链关系图。

[0030] 具体的，本发明提供的用于混合环境的应用拓扑图绘制装置，采集模块首先根据业务流量抓取cap数据包，然后通过分类识别器对cap数据包进行识别，保存识别出的TCP报文，并将非TCP报文丢弃，将识别出的TCP报文通过规则库中的业务规则进行数据过滤，最终按规则库的业务规则得到定制化的TCP报文。采集模块将捕获的不同网络传输协议下的网络数据帧格式存储下来，将每间隔一个时间周期获取的一个文件则定义为一个cap数据包；所述cap数据包是一种全十六进制的数据文件，通过解析cap数据包，得到的数据帧内容，所述数据帧内容包含有TCP报文、UDP和FTP各种网络协议的数据存储格式。

[0031] 具体的，本发明提供的用于混合环境的应用拓扑图绘制装置，识别模块识别采集模块传入的TCP报文，所述TCP报文封装在IP数据报中，所述识别模块解析封装TCP报文的IP数据报，获取TCP报文对应的IP数据报的源IP地址和目的IP地址；解析TCP报文的首部，获取TCP报文的源端口和目的端口。源端口和源IP地址标识报文的返回地址，所述目的IP地址指明接收方计算机，所述目的端口指明接收方计算机上的应用程序接口；所述TCP报文的端口用来标识计算机不同的应用进程，TCP报文中的源端口和目的端口同IP数据报中的源IP地址与目的IP地址唯一确定一条TCP连接。

[0032] 具体的，本发明提供的用于混合环境的应用拓扑图绘制装置，运算分析模块汇总识别模块分析TCP报文得到源IP地址、源端口、目的IP地址和目的端口，通过TCP连接建立源IP地址、源端口、目的IP地址和目的端口间的关联关系，筛选多段时间内多次进行相同的TCP连接的关联关系，归并具有相同的源IP地址、源端口、目的IP地址和目的端口的关联关系，生成一条调用关联关系，将无法合并的关联关系废弃，确认生成的调用关联关系的源IP地址、源端口、目的IP地址和目的端口。

[0033] 处理模块查询配置管理数据库(CMDB)，将每条调用关联关系与配置管理数据库进行匹配，获取调用关联关系的源IP地址对应的计算机中源端口对应的应用进程及相关联的应用模块名称，获取调用关联关系的目的IP地址对应的计算机中目的端口对应的应用进程及相关联的应用模块名称，确认应用模块间的实际调用关系，将该调用关系存储在配置管理数据库；将在配置管理数据库中已存在的调用关系丢弃，完成去噪；将不存在调用关系的应用模块的名称推送至配置管理数据库管理页面提醒更新；在配置管理数据库数据更新后，将所有应用模块间的调用关系提交至自动关联模块。自动关联模块通过应用模块间的调用关系，调用图形控件绘制应用模块间调用链关系图。

[0034] 优选的，本发明提供的用于混合环境的应用拓扑图绘制装置，所述自动关联模块设有扩展接口，所述扩展接口接入扩展模块，所述扩展模块包括日志预警模块和容量监测模块；所述日志预警模块进行节点故障和预警的展示，所述日志预警模块将模块所在的应用日志的报错和错误分类实时推送至应用节点；所述容量监测模块进行节点容量的监测，所述容量监测模块将模块所在的应用主机及进程的性能指标和设置阈值实时推送至应用节点，并对增长趋势进行对比分析得到预测结果；所述自动关联模块通过日志预警模块和/或容量监测模块进行故障的定位及回溯。

[0035] 综上所述，本发明提供的用于混合环境的应用拓扑图绘制装置，增加规则库自动匹配，无需分析所有的TCP报文，减少冗余数据传入；TCP报文自动识别，数据采集聚合后丢弃数据，实现自动化分析过程，无需增加大量存储；实现快速清洗数据及匹配CMDB库，完成基础数据比对及结果输出，生成调用链应用关系拓扑图；实现接口模块化接入，最终完成故

障、容量的节点展示分析，提升自动化运维效率。

[0036] 虽然本发明已以较佳实施例揭示如上，然其并非用以限定本发明，任何本领域技术人员，在不脱离本发明的精神和范围内，当可作些许的修改和完善，因此本发明的保护范围当以权利要求书所界定的为准。

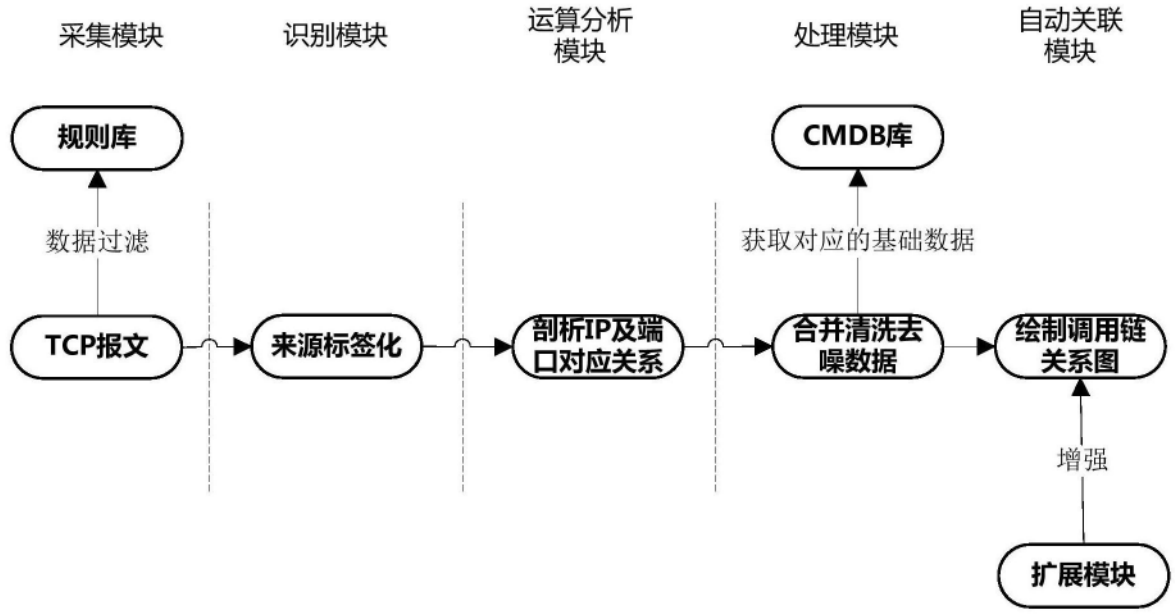

采集模块
识别模块
运算分析模块
处理模块
自动关联模块
规则库
CMDB库
数据过滤
获取对应的基础数据
TCP报文
来源标签化
剖析IP及端口对应关系
合并清洗去噪数据
绘制调用链关系图
增强
扩展模块

图1