(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 110086682 A
(43)申请公布日 2019.08.02

(21)申请号 201910427429.1

(22)申请日 2019.05.22

(71)申请人 四川新网银行股份有限公司
地址 610094 四川省成都市成都高新区吉泰三路8号1栋1单元26楼1-8号

(72)发明人 杨阳 韩晨阳 余波

(74)专利代理机构 成都智言知识产权代理有限公司 51282
代理人 李龙

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

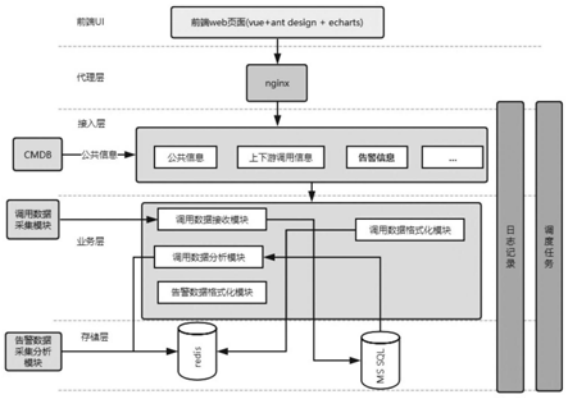
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于TCP的服务链路调用关系视图和故障根因定位方法

(57)摘要

本发明属于信息技术领域，提供了基于TCP的服务链路调用关系视图和故障根因定位方法，本发明的目的在于针对上述缺陷，提供提供一种能确定故障影响的范围的方法。其主要方案包括：对服务器所在主机进行netstat采集数据，得到服务器之间原始调用信息，并对原始数据进行数据清洗并存入数据库；分别从数据库读取IP调用关系信息和IP详细属性；根据IP调用关系信息，获得服务间调用关系和服务的详细属性存入redis；获取原始告警并进行分析，得到关联服务的告警数据并存入redis；从redis中获取步骤4存入的数据和告警数据，在可视化链路图中的链路中将对应告警服务标红并改变节点形状，然后在详情中展示告警信息。



CN 110086682 A

1.基于TCP的服务链路调用关系视图和故障根因定位方法,包括以下步骤:

步骤1:步骤1:对服务器所在主机进行netstat采集数据,得到服务器之间原始调用信息,并对原始数据进行数据清洗,调用数据存储接口将数据存入数据库;

步骤2:分别从数据库读取IP调用关系信息和IP详细属性;

步骤3:链路数据初步分析,根据IP调用关系信息,通过CMDB,获得服务间调用关系和服务的详细属性,得到服务信息,将服务信息数据存入redis;

步骤4:获取原始告警并进行分析,得到关联服务的告警数据并存入redis;

步骤5:从redis中获取步骤4存入的数据;

步骤6:从redis中获取告警数据,在可视化链路图中的链路中将对应告警服务标红并改变节点形状,然后在详情中展示告警信息。

2.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,步骤1包括以下步骤:

步骤1.1:纳入监控的所有主机分别获取与自己通信的IP和端口信息;

步骤1.2:对获取的IP端口信息进行初步分析,根据本地端口是否在本地监听的端口列表来判断上下游关系,得到包含其上下游调用关系的IP调用关系信息,然后调用数据存储接口将IP调用关系信息存入数据库。

3.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,步骤2包括以下步骤:

步骤2.1:从数据库获取IP调用关系信息;

步骤2.2:根据IP调用关系信息,通过配置管理数据库获取IP的详细属性,IP的详细属性包括所属服务、服务类型。

4.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,步骤3包括以下步骤:

步骤3.1:根据之前步骤获取到IP信息、IP调用关系、机房分布信息,资源使用情况信息;

步骤3.2:将包含服务之间的调用关系和服务的详细属性的服务信息,存入redis。

5.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,步骤4包括以下步骤:

步骤4.1:设置cron任务,每分钟采集一次告警数据;

步骤4.2:获取静态资源数据,将告警数据与服务的详细属性匹配;告警数据通过告警平台API采集,采集到的数据中会有IP信息,通过IP信息去CMDB中查询相关的应用、系统名称,构造{系统名:告警数据}的k-v结构;

步骤4.3:将匹配到的数据带上时间标志,push到redislist结构中,,保存最近30分钟数据,每次获取告警。

6.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,步骤5包括以下步骤:

步骤5.1:配置charts可视化库,获取后台数据;

步骤5.2:遍历节点数据,将对应的服务信息存放入服务列表,绘制出可视化链路图。

7.一种根据权利要求1所述的基于TCP的服务链路调用关系视图和故障根因定位方法,

步骤6包括以下步骤：

步骤6.1:后台通过redis,获取告警数据进行遍历；

步骤6.2:将告警数据与服务列表进行匹配,并将告警标志展示在时间选择框上；

步骤6.3:对于可视化链路图,将告警的节点重新绘制,颜色标红并且改变样式；

步骤6.4:在节点详情中展示告警信息。

基于TCP的服务链路调用关系视图和故障根因定位方法

技术领域

[0001] 本发明展示服务之间调用关系，属于信息技术、软件开发技术领域，适用于服务之间调用关系展示和故障根因分析。

背景技术

[0002] 目前已知的故障定位技术方案有：网络层面的数据包加以分析，获取故障节点地址，再进一步分析故障发生源头；通过跟踪应用之间的调用关系来进行监控。

[0003] 现有的与本提案相关的的技术方案是，【CN107294780A】基于网络监听的资源类互联网故障定位方法，采用网络监听技术捕获计算机所传输的数据帧并对其加以分析，获取故障IP，最后通过路由跟踪定位出互联网业务故障的源地址厂商。

[0004] 该技术方案和本提案的技术方案的不同在于，一是该技术方案只定位单节点故障，本提案除了定位单节点故障，还会通过链路调用链图分析出该故障节点可能影响的其他节点；二是该技术方案是通过网络监听技术获取数据包判断故障节点，本提案是通过监控服务端口和进程是否存活定位到故障节点，并展示到链路调用链图，如果发生服务故障，可以根据链路调用关系确定该故障影响的范围，并调用告警平台接口通知相关业务人员该故障可能带来的影响。

[0005] 该技术方案有以下缺点：一是不能确定故障影响的范围，没有链路调用展示图；二是监控手段单一，仅从网络层面做了故障分析。本提案有多种采集数据的手段，结合告警系统做了链路调用展示图，以及告警通知，可以直观的看到故障的影响范围。

发明内容

[0006] 本发明的目的在于针对上述缺陷，提供一种基于TCP的服务链路调用关系视图和故障根因定位方法。

[0007] 本发明为解决上述问题提供以下技术方案：

[0008] 基于TCP的服务链路调用关系视图和故障根因定位方法，包括以下步骤：

[0009] 步骤1：对服务器所在主机进行netstat采集数据，得到服务器之间原始调用信息，并对原始数据进行数据清洗，调用数据存储接口将数据存入数据库；

[0010] 步骤1包括以下步骤：

[0011] 步骤1.1：纳入监控的所有主机分别获取与自己通信的IP和端口信息；

[0012] 步骤1.2：对获取的IP端口信息进行初步分析，根据本地端口是否在本地监听的端口列表来判断上下游关系，得到包含其上下游调用关系的IP调用关系信息，然后调用数据存储接口将IP调用关系信息存入数据库；

[0013] 步骤2：分别从数据库读取IP调用关系信息和IP详细属性；

[0014] 步骤2包括以下步骤：

[0015] 步骤2.1：从数据库获取IP调用关系信息；

[0016] 步骤2.2：根据IP调用关系信息，通过配置管理数据库获取IP的详细属性，IP的详

细属性包括所属服务、服务类型。

[0017] 步骤3:链路数据初步分析,根据IP调用关系信息,通过CMDB(配置管理数据库),获得服务间调用关系和服务的详细属性(应用名,系统名,子系统名,机房分布信息,主机的资源使用情况包括cpu,内存),得到服务信息,将服务信息数据存入redis(key-value存储系统);

[0018] 步骤3包括以下步骤:

[0019] 步骤3.1:根据之前步骤获取到IP详细属性、IP调用关系信息、机房分布信息,资源使用情况信息;

[0020] 步骤3.2:将包含服务之间的调用关系和服务的详细属性的服务信息,存入redis;

[0021] 步骤4:获取原始告警并进行分析,得到关联服务的告警数据并存入redis;

[0022] 步骤4包括以下步骤:

[0023] 步骤4.1:设置cron任务,每分钟采集一次告警数据;

[0024] 步骤4.2:获取静态资源数据,将告警数据与服务的详细属性匹配;告警数据通过告警平台API采集,采集到的数据中会有IP信息,通过IP信息去CMDB中查询相关的应用、系统名称,构造{系统名:告警数据}的k-v结构;

[0025] 步骤4.3:将匹配到的数据带上时间标志,push到redislist结构中,结构类似于[{timestamp:xxxx,data:{}},{timestamp:xxx,data:{}}],保存最近30分钟数据,每次获取告警。

[0026] 步骤5:获取后台返回格式化数据(从redis中获取步骤四存入的数据),绘制链路图形;

[0027] 步骤5包括以下步骤:

[0028] 步骤5.1:配置charts可视化库,获取后台数据;

[0029] 步骤5.2:遍历节点数据(数据节点是子系统、系统和应用,子系统之间是调用关系,子系统与对应的系统、应用之间是所属关系。子系统与系统、应用对应关系从CMDB中获取),将对应的服务信息存放入服务列表(服务列表是echarts绘图需要的一个list。代码中的变量),绘制出可视化链路图;

[0030] 链路关系和redis中的告警信息是解耦的,对于一个链路关系图,加载到浏览器中基本的节点信息和关系信息就不会发生改变,而告警信息需要实时展示。告警数据获取是数据流,不是一次初始化加载的数据。为此本发明还提供了步骤6:从redis中获取告警数据,在可视化链路图中的链路中将对应告警服务标红并改变节点形状,然后在详情中展示告警信息。

[0031] 步骤6包括以下步骤:

[0032] 步骤6.1:后台通过redis,获取告警数据进行遍历;

[0033] 步骤6.2:将告警数据与服务列表进行匹配,并将告警标志展示在时间选择框上;步骤4.2是告警和IP匹配,但是对于一个链路图来说,一个链路图中的IP不一定会有告警的IP。这里主要是匹配链路图中服务的IP是否有告警,并展示出来。

[0034] 步骤6.3:对于可视化链路图,将告警的节点重新绘制,颜色标红并且改变样式;

[0035] 步骤6.4:在节点详情中展示告警信息。

[0036] 因为本发明采用以上技术方案,因此具备以下有益效果:

[0037] 一、针对现有技术方案不能确定故障影响范围，本提案通过TCP调用关系，能够绘制出服务的调用关系视图，可视化展示链路关系，由于存在服务直接的链路调用关系，当单个服务出现故障的时候，如果存在和其他服务直接的调用关系，那么该故障可能会影响存在调用关系的其他服务，可以在告警发生的时候能够确定告警影响范围。

[0038] 二、采用的技术手段：通过netstat和ss命令采集主机上TCP调用信息；然后过滤无用信息，关联对应的服务，初步分析存入redis中。

[0039] 三、丰富数据采集手段，与单一网络层面故障分析不同，本提案通过TCP采集数据进行服务调用关系梳理和展示，并通过接入告警信息进行红盘展示。能够确定服务上下游信息和数据大盘可视化。

[0040] 四、采用的技术手段：监控打点，前端echarts库进行可视化展示，使用UI库进行前端设计。

附图说明

[0041] 图1是本发明的平台基本架构图；

[0042] 图2是本发明的数据流向图；

[0043] 图3是本发明的效果展示图。

具体实施方式

[0044] 基于TCP的服务链路调用关系视图和故障根因定位方法，包括以下步骤：

[0045] 步骤1：对服务器所在主机进行netstat采集数据，得到服务器之间原始调用信息，如下表1所示，并对原始数据进行数据清洗，调用数据存储接口将数据存入数据库；

[0046]

表 1

协议	本地地址	外部地址	状态
TCP	192.168.0.179:3389	www133:55934	CLOSE_WAIT
TCP	192.168.0.179:3389	www133:55936	CLOSE_WAIT
TCP	192.168.0.179:3389	www133:55938	CLOSE_WAIT
TCP	192.168.0.179:50046	118.123.100.129:https	ESTABLISHED
TCP	192.168.0.179:50047	118.123.100.129:https	ESTABLISHED
TCP	192.168.0.179:50048	118.123.100.129:https	ESTABLISHED
TCP	192.168.0.179:50049	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50050	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50051	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50052	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50053	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50054	a23-51-210-157:http	ESTABLISHED
TCP	192.168.0.179:50763	123.151.72.17:http	ESTABLISHED
TCP	192.168.0.179:50945	101.227.139.187:8080	ESTABLISHED
TCP	192.168.0.179:51137	183.61.38.179:http	CLOSE_WAIT
TCP	192.168.0.179:51144	183.61.38.179:http	CLOSE_WAIT
TCP	192.168.0.179:51639	14.17.41.210:https	CLOSE_WAIT
TCP	192.168.0.179:51863	113.96.200.115:imaps	ESTABLISHED
TCP	192.168.0.179:52786	101.89.15.105:https	ESTABLISHED
TCP	192.168.0.179:53527	14.17.41.210:https	CLOSE_WAIT

[0047]

TCP	192.168.0.179:54749	14.17.41.210:https	CLOSE_WAIT
TCP	192.168.0.179:55591	182.140.177.147:https	CLOSE_WAIT
TCP	192.168.0.179:55592	182.140.177.147:https	CLOSE_WAIT
TCP	192.168.0.179:55768	59.37.116.35:https	CLOSE_WAIT
TCP	192.168.0.179:55769	59.37.116.35:https	CLOSE_WAIT

[0048] 步骤1包括以下步骤：

[0049] 步骤1.1：纳入监控的所有主机分别获取与自己通信的IP和端口信息；

[0050] 步骤1.2：对获取的IP端口信息进行初步分析，根据本地端口是否在本地监听的端口列表来判断上下游关系，得到其上下游调用关系，然后调用数据存储接口存入数据库；

[0051] 步骤2：分别从数据库读取IP调用关系信息和服务IP信息；

[0052] 步骤2包括以下步骤：

[0053] 步骤2.1：从数据库获取IP调用关系信息；

[0054] 步骤2.2：根据IP信息，通过配置管理数据库获取IP的详细属性，包括所属服务、服务类型。

[0055] 步骤3：链路数据初步分析，根据IP调用关系信息IP，通过CMDB(配置管理数据库)，获得服务间调用关系和服务的详细属性，完成数据格式化，将格式化后的数据存入redis(key-value存储系统)；

[0056] 步骤3包括以下步骤：

[0057] 步骤3.1:根据之前步骤获取到IP信息、tcp调用关系、告警信息、服务信息、机房分布信息,资源使用情况信息；

[0058] 步骤3.2:将服务之间的调用关系和服务的详细属性,存入redis；

[0059] 步骤4:获取原始告警并进行分析,得到关联服务的告警数据并存入redis；

[0060] 步骤4包括以下步骤：

[0061] 步骤4.1:设置cron任务,每分钟采集一次告警数据；

[0062] 步骤4.2:获取静态资源数据,将告警数据与服务信息匹配;告警数据通过告警平台API采集,采集到的数据中会有IP信息,通过IP信息去CMDB中查询相关的应用、系统名称,构造{系统名:告警数据}的k-v结构；

[0063] 步骤4.3:将匹配到的数据带上时间标志,push到redislist结构中,结构类似于[{timestamp:xxxx,data:{}},{timestamp:xxx,data:{}}],保存最近30分钟数据,每次获取告警。

[0064] 步骤5:获取后台返回格式化数据,绘制链路图形；

[0065] 步骤5包括以下步骤：

[0066] 步骤5.1:导入echarts可视化库,获取后台数据；

[0067] 步骤5.2:遍历节点数据,将对应的服务存放入服务列表,绘制出可视化链路图；

[0068] 步骤6:从redis中获取告警数据,在链路中将对应告警服务标红并改变节点形状,然后在详情中展示告警信息。

[0069] 步骤6包括以下步骤：

[0070] 步骤6.1:后台通过redis,获取告警数据进行遍历；

[0071] 步骤6.2:将告警数据与服务列表进行匹配,并将告警标志展示在时间选择框上；

[0072] 步骤6.3:对于可视化链路图,将告警的节点重新绘制,颜色标红并且改变样式。

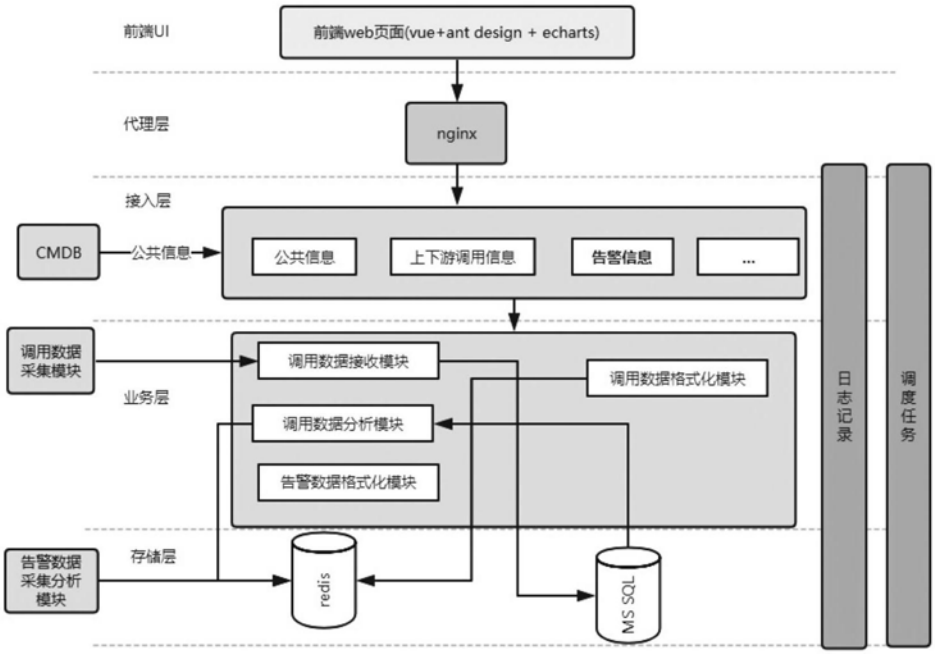

前端UI
前端web页面(vue+ant design + echarts)
代理层
nginx
接入层
CMDB
公共信息
公共信息
上下游调用信息
告警信息
...
调用数据采集模块
业务层
调用数据接收模块
调用数据格式化模块
调用数据分析模块
告警数据格式化模块
告警数据采集分析模块
存储层
redis
MS SQL
日志记录
调度任务

图1

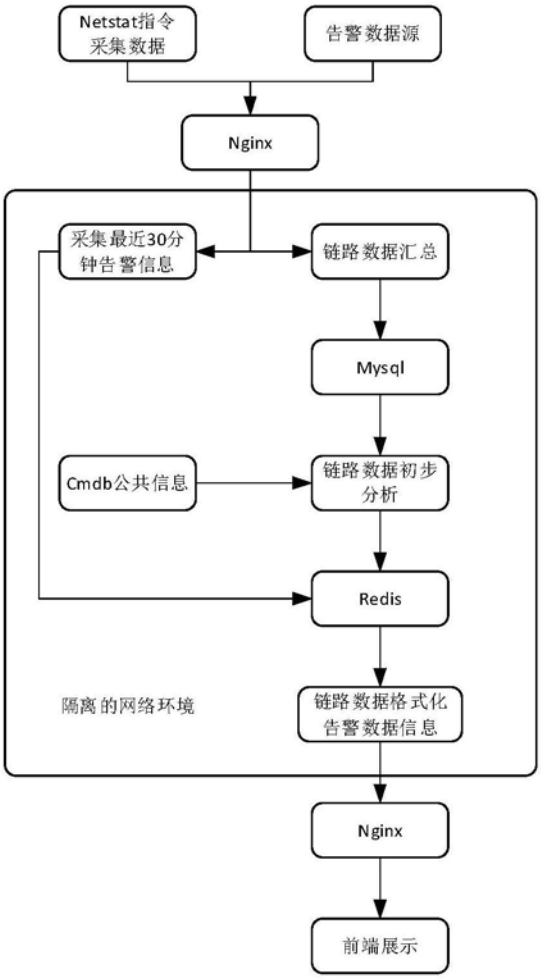

Netstat指令
采集数据
告警数据源
Nginx
采集最近30分
钟告警信息
链路数据汇总
Mysql
Cmdb公共信息
链路数据初步
分析
Redis
隔离的网络环境
链路数据格式化
告警数据信息
Nginx
前端展示

图2

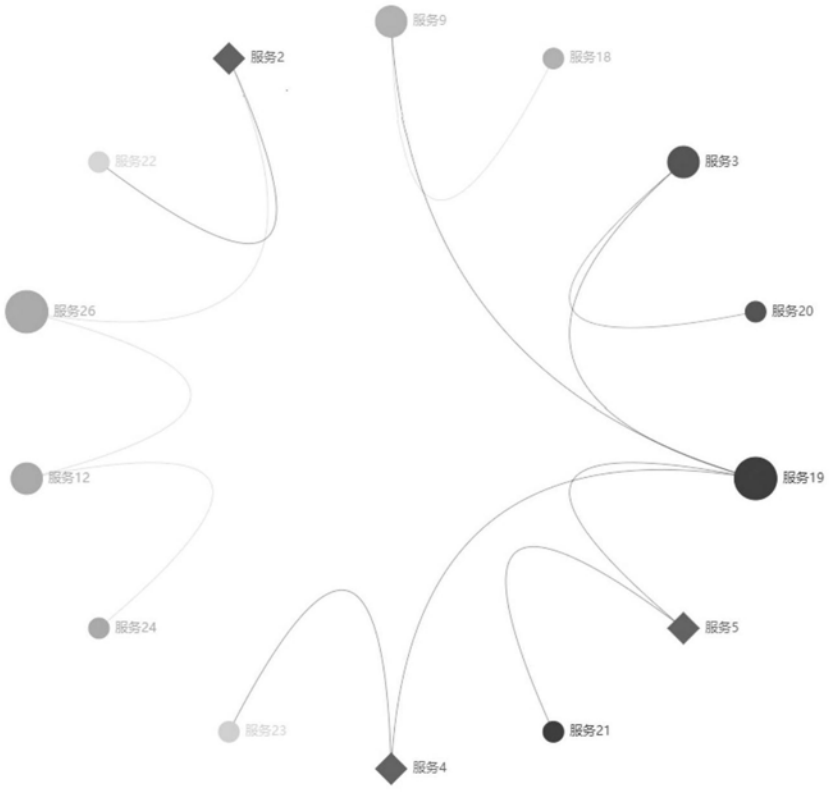

服务9
服务2
服务18
服务22
服务3
服务26
服务20
服务19
服务12
服务5
服务24
服务23
服务21
服务4

图3