通过 iMC NTA/UBA 服务器统计和分析网络流量时，流量分析任务或用户审计结果中没有数据的排查方法

NTA UBA paner 2018-09-30 发表

组网及说明

不涉及

问题描述

用户通过 iMC NTA/UBA 服务器统计和分析网络流量，流量分析任务或用户审计结果中没有数据

过程分析

一、不使用采集器的场景

在使用设备发送的流日志信息进行网络流量分析的场景中，问题的原因可能有以下几种：

1. iMC NTA/UBA 服务器配置中，监听端口与设备配置不一致。
2. 防火墙隔离了 iMC NTA/UBA 服务器端口。
3. 数据库磁盘使用率超过阈值。
4. 在 iMC NTA/UBA 服务器中检查$IMC_INSTALL/data/recieverData 和 $IMC_INSTALL/data/processorData/data 目录，发现有数据积压。
5. NTA 报表没有数据，原因可能是 NTA 设备接口索引错误。
6. UBA 审计报表没有数据，原因可能是服务器配置中内网监控信息配置错误。

二、使用采集器的场景

在使用采集器获取数据信息进行网络流量分析的场景中，问题的原因除了 iMC NTA/UBA 服务器 端的故障外还可能有以下几种：

1. 采集器没有正常启动。
2. 采集器版本错误。
3. 采集器网卡没有启动。
4. 设备镜像端口配置错误。
5. 采集器服务器数据积压。
6. 采集器时间与 iMC NTA/UBA 服务器时间不一致。
7. FTP 服务器配置问题

解决方法

一、不使用采集器的场景，即在使用设备发送的流日志信息进行网络流量分析的场景中，解决办法如下：

1. iMC NTA/UBA 服务器监听端口配置与设备配置保持一致，默认端口号为 9020、 9021、 6343。
2. 检查设备与 iMC NTA/UBA 服务器之间的网络是否联通，是否存在放火墙，如果有防火墙请 开启 iMC NTA/UBA 服务器进程使用的 18801、 18802、 18803 三个 UDP 端口以及监听数据 使用的 9020、9021、 6343 等 UDP 端口。检查 iMC NTA/UBA 所在 Windows 服务器是否开 启了防火墙，如果开启防火墙请关闭或者开启上述端口。
3. 通过“业务 > 流量分析与审计 > 数据库空间使用”查看当前数据库磁盘使用情况。在 iMC NTA/UBA 服务器中查看$IMC_INSTALL/unba/conf/目录下的 pcsGeneralCammand.xml 和 rcvGeneralCammand.xml 文件，确认是否是因为磁盘满导致没有数据， command 为 1 表示 当前进程已经停止处理数据。
4. 通过监控代理停掉 receiver.exe 和 processor.exe 两个进程，手工删除 $IMC_INSTALL/data/recieverData 和$IMC_INSTALL/data/processorData/data 这两个目录 下文件。然后清空 iMC NTA/UBA 服务器数据库中的表 unba_slave.tbl_storing_task，再启动 receiver.exe 和 processor.exe 两个进程。
5. 手动增加 NTA 设备时，输入正确的接口索引，接口索引应该与设备发送的流统计报文中的接 口索引一致。建议从平台添加设备。 6. 通过“业务 > 流量分析与审计 > 配置管理 > 服务器管理 > 服务器配置”配置正确的内网监控 网段，被监控网络地址必须在该监控网段内，否则统计流量会被过滤掉。

二、使用采集器的场景 ，即在使用采集器获取数据信息进行网络流量分析的场景中，解决办法如下：

1. 在采集器服务器上执行 ps aux|grep probe 检查采集器进程是否启动。
2. iMC NTA 5.1 (E0201) 之前版本，如果安装在 Red Hat Enterprise Linux Server 5 系统下，操 作系统开启了 PAE 特性，采集器能够安装成功并且可以运行，但是无法生成数据。
3. 在采集器服务器上执行 ifconfig 查看网卡的状态，执行 tcpdump –i eth0 查看网卡上的数据。 eth0 为监听网卡名。
4. 如果监听网卡上没有数据，请检查设备的镜像端口配置是否正确。
5. 检查采集器服务器/data 目录下是否有数据积压。数据积压解决办法： a) 通过监控代理停止 processor 进程； b) 在采集器上执行/usr/local/unba/bin/monitor stop 停止采集器； c) 执行 rm -rf /opt/unba_data 删除 unba_data 目录及文件； d) 执行 mkdir /opt/unba_data 创建 unba_data 目录； e) 执行 rm -rf /usr/local/unba/conf/readysendfilelist.txt 删除 readysendfilelist.txt 文件； f) 执行/usr/local/unba/bin/monitor，重新启动 processor 进程。
6. 修改采集器时间与 iMC NTA/UBA 服务器时间一致。
7. FTP 服务器中配置的用户名、密码及文件目录必须和 iMC NTA/UBA 服务器配置中的 FTP 参 数配置

相同。