D2020-G审计不到数据库语句

数据库审计 张志潮 2020-07-27 发表

组网及说明

交换机将流量镜像到D2020-G进行事件审计

问题描述

按照官网事件审计配置指导部署完后审计不到数据库查询语句

过程分析

1、检查监控系统状态是否正常

使用系统管理员登录设备web管理界面，在“运行状态”中查看监听服务是否正常运行。

如果显示异常，请点击监听服务的“配置”并重启服务。

2、检查监听网卡是否开启

•旁路镜像检测需要确保业务口是否勾选监听网卡并处于开启状态。

•流量探针检测需要确保业务口是否配置IP地址和静态路由并处于开启状态，同时确保数据库服务器到业务口可达。

3、镜像模式下，交换机是否镜像的双向流量。抓包能否看到报文

数据库审计系统Web界面只能抓取3s的报文不足以用以定位问题，一般需要把交换机的镜像口直接连接至电脑使用Wireshark抓包，也可以通过设备后台进行抓包，如图所示观察监听端口是否有正常的业务报文且报文中是否携带SQL语句信息

4、数据是否携带VLAN TAG

携带VLAN TAG需要勾选支持vlan数据。 是否指定了源IP审计

登录url后面加/API，密码tcpdump。在进入的页面上勾选支持vlan数据

解决方法

按上述步骤排查发现镜像的报文中携带了vlan tag，在相应页面中勾选支持vlan数据后解决