

知 误配指定源IP审计导致SecPath D2020-G无法对Oracle数据库进行审计问题

数据库审计

王英凯 2019-11-09 发表

组网及说明

无

问题描述

SecPath D2020-G旁路部署在核心交换机上，并且交换机已经将访问数据库的流量镜像至D2020-G的业务接口，现场完成部署后在实时查询中并没有找到访问Oracle数据库的记录。

过程分析

1、检查D2020-G配置

1) D2020-G通过万兆板卡1/0与1/1接口与交换机互联，其中交换机侧两个接口做聚合并设置了最大选中端口数为1，正常使用过程中只有1/1接口负责接收镜像数据，同时勾选监听网卡。



网卡名	设备	接口类型	IP地址	子网掩码	默认网关	接收流量	连接状态	监听网卡?	开关网卡
网卡14	GE0/13	光口				0.00 KIB	断开	☐	☒
网卡15	GE0/14	光口				0.00 KIB	断开	☐	☒
网卡16	GE0/15	光口				0.00 KIB	断开	☐	☒
网卡17	XGE1/0	光口				1.57 GIB	连接	☒	☒
网卡18	XGE1/1	光口				24.53 GIB	连接	☒	☒
网卡19	XGE1/2	光口				0.00 KIB	断开	☐	☒
网卡20	XGE1/3	光口				0.00 KIB	断开	☐	☒

2) 监听配置

分别将需要监听的服务器地址加入业务系统，在返回值配置中可以填写访问数据库的账号密码，并且在返回值检测中数据库审计与各数据库连接正常。



3、通过上一步排查将问题逐渐锁定在设备侧，于是继续排查设备配置。发现客户配置了指定源IP审计，将指定源IP审计中IP地址删除后数据审计正常。

解决方法

将指定源IP审计中IP地址删除后数据审计正常

业务系统配置

中间件服务器配置

应用审计配置

指定源IP审计

流量探针

☐ 支持Vlan数据 ?

局域网

包含IP

IP类型：

单个IP

IP地址：172.20.20.46

删除

添加

不包含IP

IP类型：

单个IP

IP地址：

删除

添加

Vxlan云环境

包含IP

IP类型：

单个IP

IP地址：

删除

添加

不包含IP

IP类型：

单个IP

IP地址：

删除

添加

问题处理总结：

对于实时语句中查看不到数据此类问题，简单可以按照下面方法排查：（其中1、2、4、5为必查项）

- 1、监听配置没有配置，填写监听配置；
- 2、检测是否勾选了网卡监听、监听服务是否正常使用。
- 3、系统时间与审计系统时间不一样，建议校正一下审计系统的时间。
- 4、确认交换机的镜像端口是否正常。
- 5、检测是否配置指定源IP审计和指定源IP不审计。