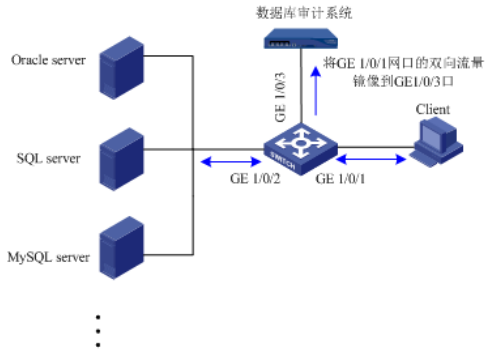
D2000-AK650 HIS数据库审计不到部分终端操作信息

数据库审计 郭尧 2020-04-28 发表

组网及说明

模拟组网如下：



问题描述

数据库审计系统，历史查询语句，有部分终端的访问动作无法审计到，部分终端能够正常审计到

过程分析

分析过程：

1. 查看监听配置，配置了相应IP
2. 检查设备业务系统配置数量只有一个未超标
3. 监听服务也已经开启，且处于正常状态
4. 设备业务口勾选监听网卡
5. 检查设备已经配置指定源IP审计

以上配置均没发现错误内容，在交换机设备上针对审计不到的终端做流镜像抓包，对抓取到的报文进行分析，追踪报文TCP流详细内容如下：

```
.....r....,....g.............pA....
.........Lj.............r.....................ORA-01403: ..............
....^si.........f....
.....................................3select count ( *) from INP_TA_NOW where SBRLSH =:1
.....................................`.....................T.......
134..............|d..Q.$.";.....zxw...
...Q.....................................COUNT(*)...................xx...
..............."..........................r.....................................qX..............
.....................t....,....g.............rX....
.........Lj.............t.....................ORA-01403: ..............
....^ui.........f....
.....................................3select count ( *) from INP_TA_NOW where SBRLSH =:1
.....................................`.....................T.......
435..............|d..Q.$.";.....zxw...
...Q.....................................COUNT(*)...................xx...
..............."..........................r.....................................sX..............
.....................v....,....g.............tX....
.........Lj.............v.....................ORA-01403: ..............
....^wi.........f....
.....................................3select count ( *) from INP_TA_NOW where SBRLSH =:1
.....................................`.....................T.......
```

抓包的报文里，也有终端的操作语句select，正常情况下有增、删、改、查等操作语句数据库审计都能够正常审计到终端的访问记录

在数据库审计设备上进行抓包，也能够抓到镜像到设备的访问报文，但数据库审计不到

后续对比审计不到的报文和能够正常审计到的报文，发现审计不到的报文在交换机上做端口镜像时携带了标签上到数据库审计设备，导致这部分报文无法正常审计到

解决方法

在监听配置，指定源IP审计配置时，勾选上支持vlan数据审计，能够正常审计到对应终端的访问信息，如下：

注意事项：

- 审计设备上使用的指定ip和指定非ip审计，基于性能考虑，默认指定源ip审计不支持带vlan的数据，面对存在vlan数据的镜像流，如果启用该模块的功能，审计设备会产生以下几种情况，如下；
- 当指定审计某ip时，所有vlan数据均不会被审计到；
- 当指定不审计某ip时，所有vlan数据均会被审计到；
- 当同时启用指定审计某ip和指定不审计某ip时，vlan数据优先被排除掉（vlan数据均不会被审计到），再根据条件进行过滤；
- 建议：用户现场的镜像数据请不要使用vlan方式，如果无法调整镜像，请避免使用指定ip审计；