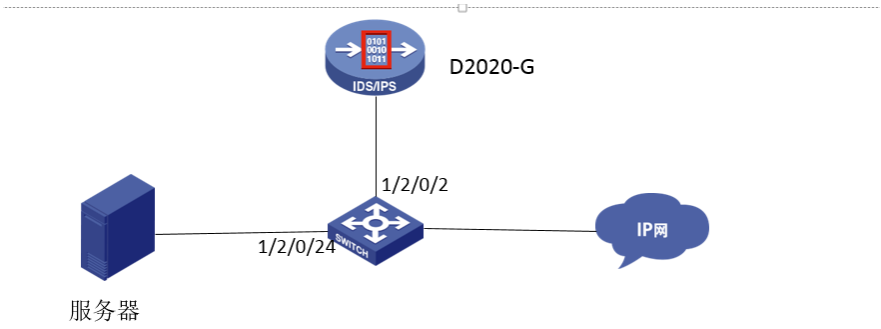
某局点D2020-G无法审计到数据库数据问题处理经验案例

数据库审计 刘文峰 2019-11-30 发表

组网及说明

见下图：



问题描述

某局点采用我司D2020-G旁路部署在核心交换机上，通过镜像服务器的数据到数据库审计系统上，实现审计功能，但是在部署完成之后，发现在D2020-G 上无法升级到数据，在D2020-G上抓包查看，发现已有数据镜像上来。

过程分析

在D2020-G 上抓包查看已能看到数据上来，说明镜像做的没有问题，查看D2020-G上的配置，也并无发现异常，具体参考下面配置截图：

1.审计设备的网卡配置

	网卡名	设备	接口类型	IP地址	子网掩码/前缀长度	默认网关	接收总量	连接状态	监听网卡?	开关网卡
1	网卡1	GE0/0	电口	IPV4：192.168.10.10 IPV6：2004::24	IPV4：255.255.255.252 IPV6：64	IPV4：192.168.10.9	23.28 MiB	连接		
2	网卡2	GE0/1	电口	IPV4：1.0.0.1	IPV4：255.255.0.0		0.00 KiB	断开		
3	网卡3	GE0/2	电口				818.17 MiB	连接		
4	网卡4	GE0/3	电口				0.00 KiB	断开		

2.监听配置

1	启用	SQLServer	SQLServer	自动识别	73 101 102 134 201 202 233 85	1433 1433 1433 1433 1433 1433 1433 1433		2019-10-17 13:28:51
2	启用	MySQL	MySQL	自动识别	73 101 102 134 201 202 233 85	3306 3306 3306 3306 3306 3306 3306 3306		2019-10-17 13:28:39

解决方法

进一步跟客户确认组网和镜像配置，发现镜像源接口是连接服务器的1/2/0/24口，并且服务器的网关在核心交换机上，所以交换机上镜像上来的数据是带着vlan标签，所以需要在D2020-G上勾选支持vlan数据，最终问题解决，能正常审计到数据。

```
interface GigabitEthernet1/2/0/22
 port link-mode bridge
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/2/0/23
 port link-mode bridge
 port access vlan 2
 packet-filter 3000 inbound
 packet-filter 3000 outbound
#
interface GigabitEthernet1/2/0/24
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 packet-filter 3000 inbound
 packet-filter 3000 outbound
 mirroring-group 1 mirroring-port both
#
```


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？
虚域网
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：
183.1.10.52
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