某局点ACG1000看不到所有审计日志

应用审计　关萌　2020-10-30 发表

组网及说明

用户使用我司ACG1000-ak230做为流量审计设备，通过二层透明模式部署在网络出口。

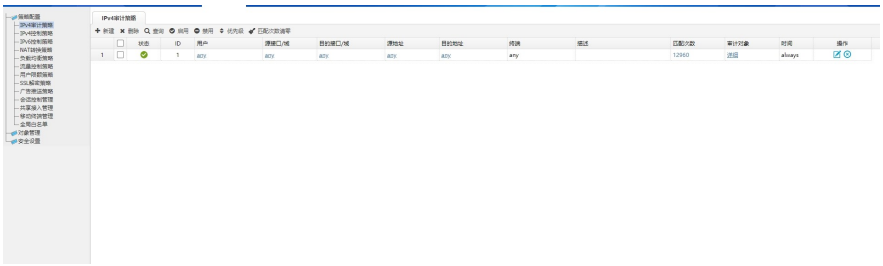
问题描述

设备上线之前对设备进行了版本升级，升级到了官网的最新版本R6611系列版本。设备上线后，发现无法看到审计日志，在审计日志子项中每个分类都没有任何日志。截图如下

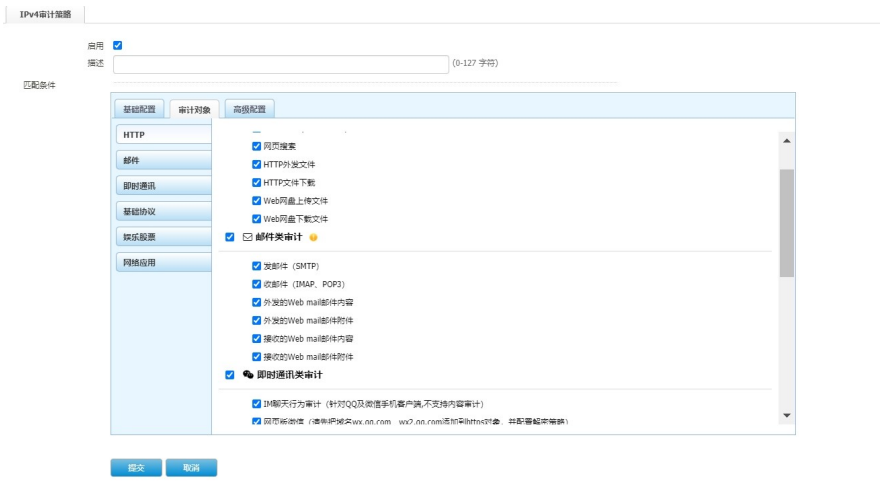
每一项都没有日志，这里不一一列举。

过程分析

对于没有日志的问题，首先检查配置，通过配置检查，发现用户棟了审计所有，看匹配次数也有匹配，从匹配上看也没有问题。多次查看策略匹配次数，匹配次数也有正常增长



检查审计对象的详细信息，怀疑没有审计相应对象，可以看到，用户配置的也是审计所有，也不存在异常配置。



查看设备硬盘状态，也都正常。

解决方法

经过进一步确认，设备在升级到6611版本后，数据库发生变化，需要重置数据库，于是通过如下命令重置后解决。

命令如下：

H3C> enable

H3C# recover database
H3C# reboot