SecCenter CSAP-SA 态势感知综合日志审计平台无法显示日志

日志采集器 李熙 2021-01-31 发表

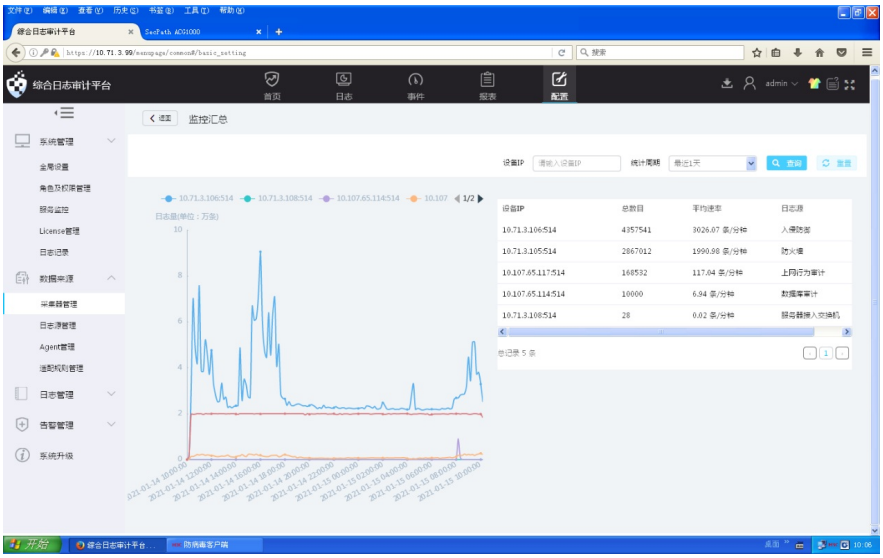
组网及说明

不涉及

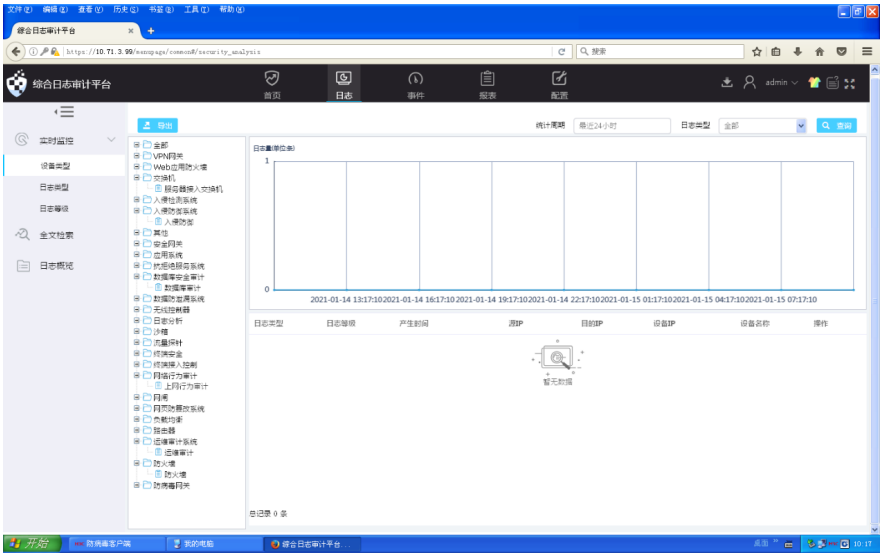
问题描述

对ACG等设备进行审计，完成日志源端syslog配置；在CSAP-SA综合日志审计平台配置好日志源，日志采集器处于在线状态；综合日志审计平台到日志源可以互通，采集器上也有看到日志上来，但日志页上没有显示；产品版本是E1707P04。

采集器信息：采集器监控汇总显示设备上报日志的统计信息

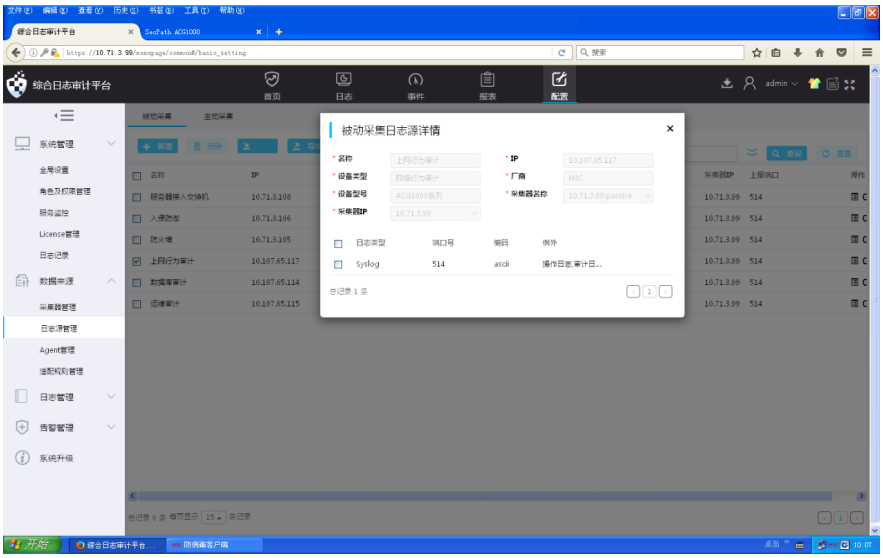


日志审计-日志详情页：无日志显示



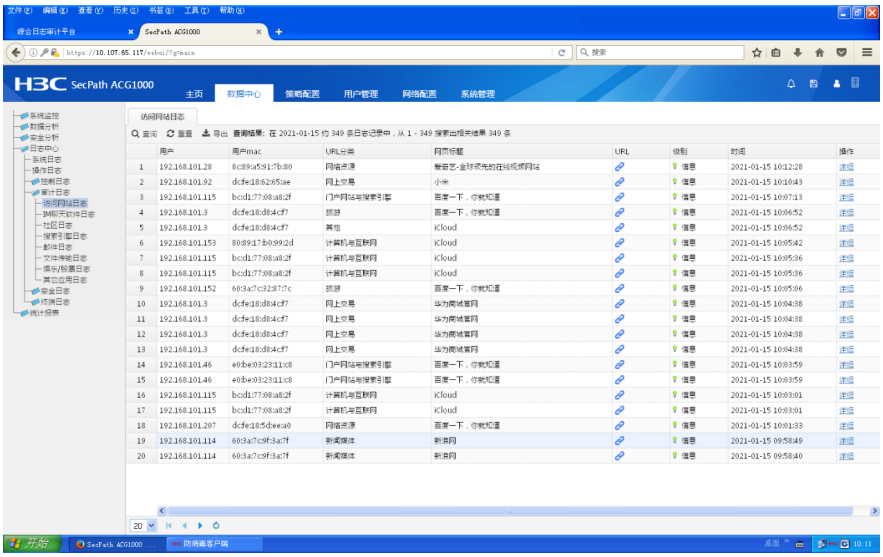
过程分析

综合日志审计平台上，查看对日志源的配置：

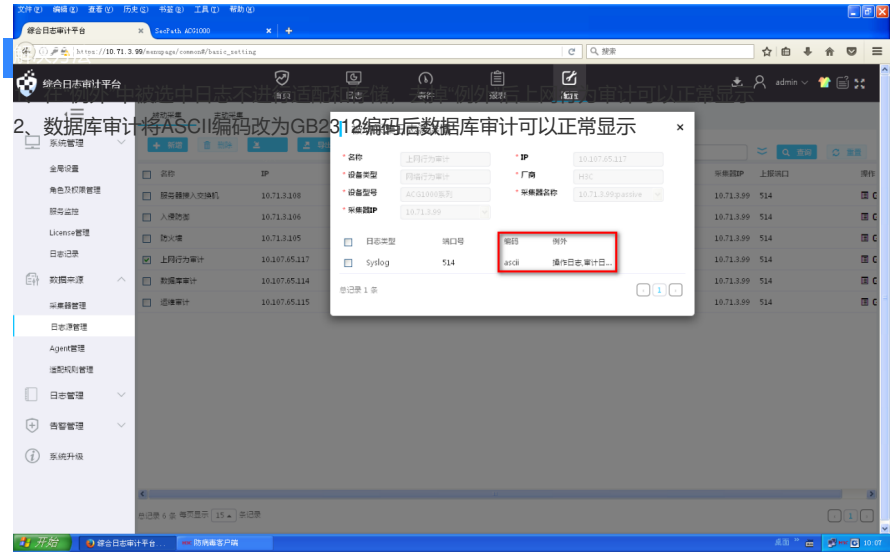


ACG端的上网行为管理-loghost配置，主机端口号与综合日志审计平台配置端口信息时所配置的端口号一致

ACG数据中心的日志详情，有上网行为流量产生：



综合审计平台上日志源配置：添加了“例外”的配置，在“例外”中添加了操作日志、审计日志等内容，导致审计平台能收到日志，但不会显示；且编码采用的是 ASCII 编码，导致数据库审计内容无法显示。



2、数据库审计将ASCII编码改为GB2312编码后数据库审计可以正常显示