A2000-G运维审计设备定期备份审计数据和审计数据本地离线查看

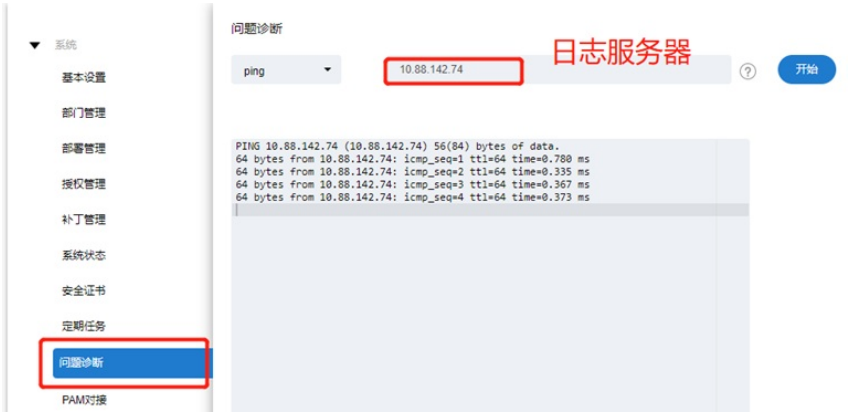
运维审计 zhiliao_k6c56S 2024-07-01 发表

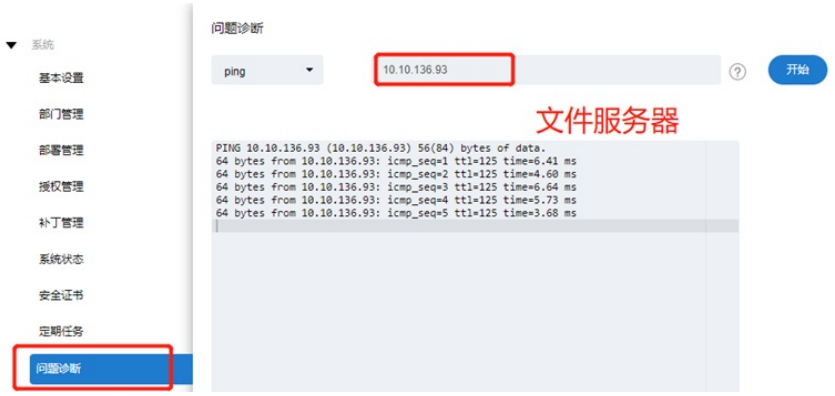
组网及说明

因为运维审计设备配置了磁盘空间利用率达到80%就定期清理,造成之前的审计信息丢失.那么可以在运维审计设备上配置告警日志外发到日志服务器,以及审计数据定期备份.

配置步骤

1、 确保运维审计平台和日志服务器能够正常互通，确保运维审计平台和文件服务器正常互通





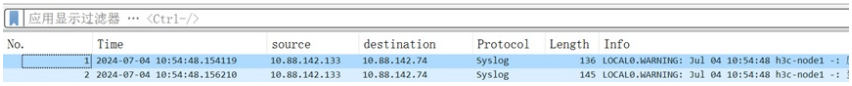
2、 配置告警信息外发到日志服务器，在配置日志服务器的时候默认情况日志是使用UDP的514端口进行外发，如果日志服务器那边使用的是非514端口，在配置的时候直接在IP地址后面：端口号，例如1.1.1.1:2000

3、 配置审计数据备份，找到相关的审计数据备份配置，将其启用起来，选择对应的文件服务器，然后配置文件服务器。

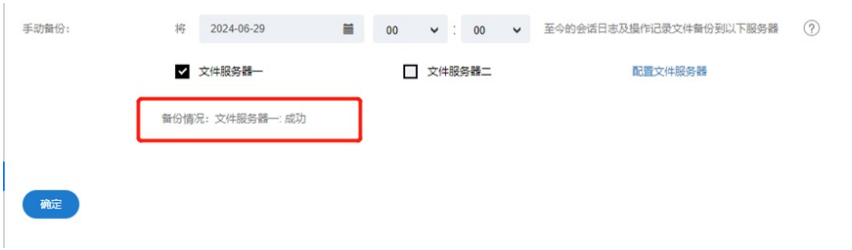
文件目录地方配置需要注意：文件存放目录，要求必须使用Unix格式的目录风格。支持通配符，例如Linux的家目录可以配置为/home/%username (%username表示用户名)。该项必填。建议采用绝对路径，例如/a/b/c。如果采用相对的是相对路径，例如a/b/c，对于Linux服务器会将/作为起点，对于Windows服务器会将FTP/SFTP的根目录作为起点。

4、 查看日志是否正常外发、审计数据是否备份正常。

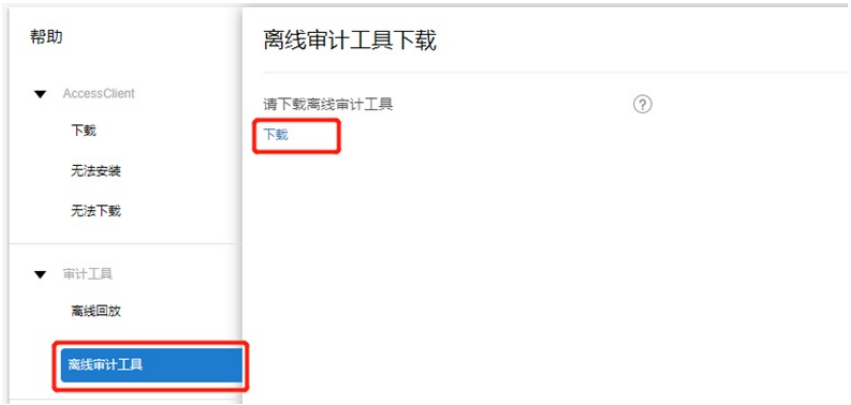
日志通过抓包测试

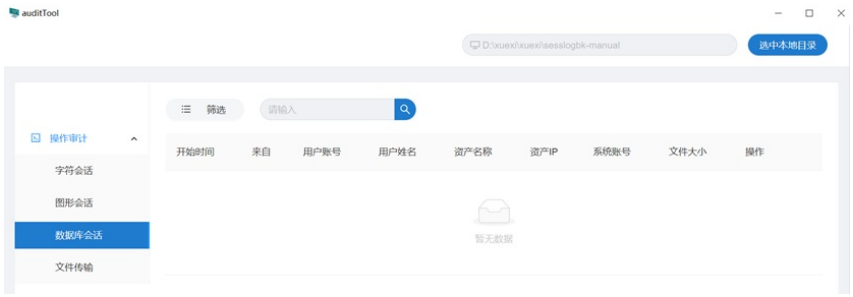


审计数据备份通过手动进行测试

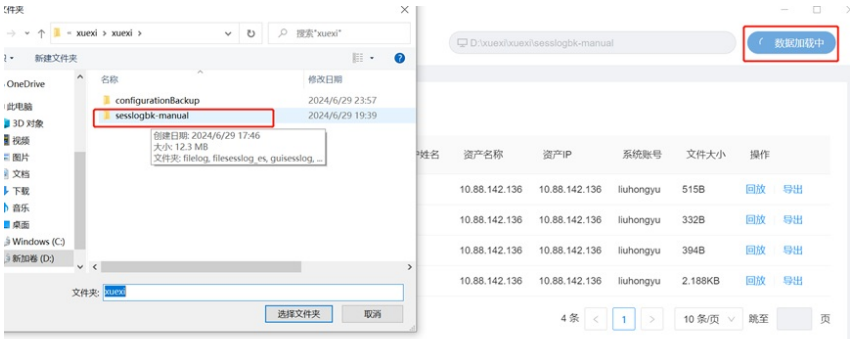


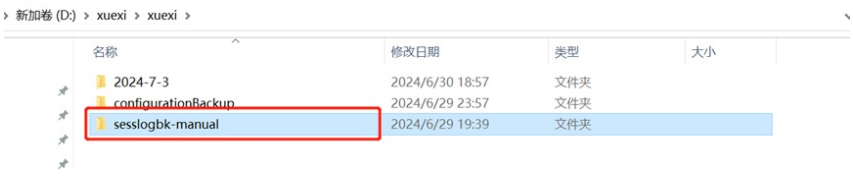
5、 审计数据备份如何离线查看，可以将运维审计设备升级到6614P02版本，在帮助à审计工具à离线审计工具。下载auditTool工具，安装后可以离线审计字符会话、数据库会话、图形会话、文件传输。





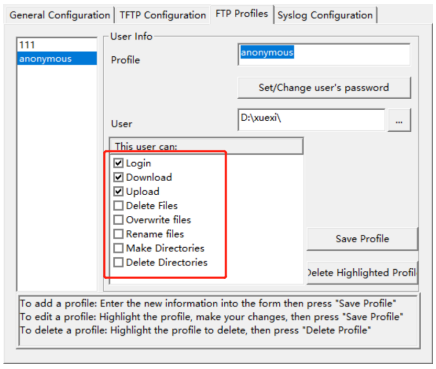
选择本地目录

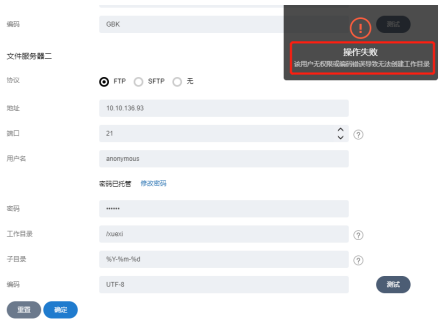




配置关键点

本案例是使用windows电脑安装3cd软件充当相关的ftp服务器,在配置3cd的时候FTP的用户权限时建议全部勾选，否则运维审计会报错权限不足.





附件下载：运维审计设备.docx