CSAP-SA综合日志审计平台由于FTP服务器账号权限问题导致启用日志备份失败

Syslog日志 其他 **断桥残雪** 2021-04-16 发表

组网及说明

无

问题描述

CSAP-SA综合日志审计平台需要进行日志备份，但是启用时报错“FTP连接失败！请确认FTP连接正常后，再启用备份。”

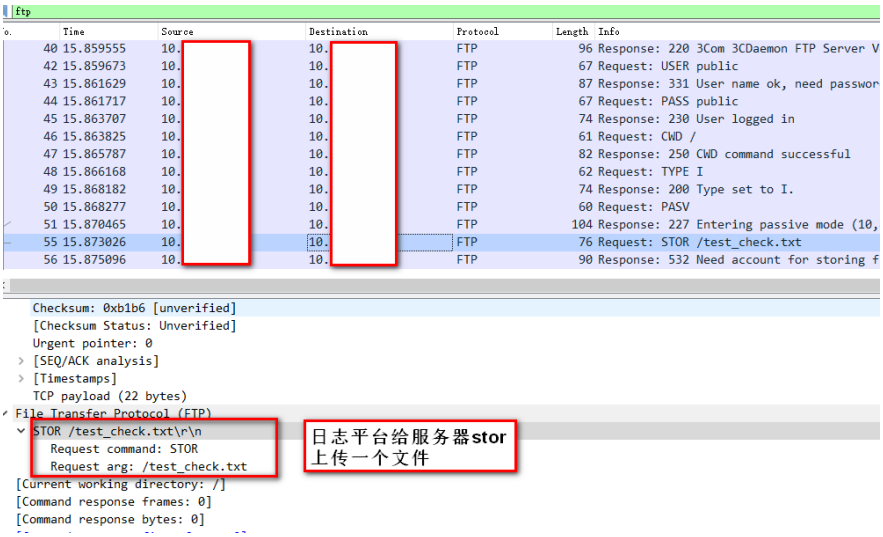
过程分析

1、根据报错信息怀疑FTP连接异常，因为本身CSAP-SA综合日志审计平台也可以其直接FTP登录测试，SSH登录到后台使用相同账号测试FTP连接正常，如下

```
[root@cyber ~]#
[root@cyber ~]#
[root@cyber ~]# ftp 10.
Connected to 10.
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.:root): public
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
```

2、FTP连接测试正常，但是web页面报错连接失败，于是本地模拟环境测试，客户故障现象并不存在，于是在故障时抓包（可以在日志平台或者FTP服务器侧进行tcpdump抓包）看启用时连接过程有何异常

[root@cyber ~]# tcpdump -i eth0 host 10.x.x.x -w ftp.pacp，抓包内容如下



前面交互账号名密码都successful log in成功，最后是SA日志平台向FTP服务器上传一个文件（文件名为test_check.txt）有提示失败，该操作是为了检测该账号对于FTP服务器是否有正常的写权限（正常日志备份是要对FTP服务器进行写入的），所以建议客户侧排查对应账号或者服务器是否有限制了对服务器的写入

解决方法

排查FTP服务器侧，放通写入权限