某局点防火墙F1000系列防火墙SSL VPN结合LDAP认证失败

SSL VPN 方志伟 2020-03-17 发表

组网及说明

防火墙——核心——LDAP服务器

问题描述

现场账户结合ldap认证失败，创建本地用户认证正常

故把问题排查方向锁定为ldap配置及ldap服务器上的相关配置

过程分析

ldap相关配置

#

ldap server ldap1

login-dn cn=xxx,cn=xxx,dc=xxx,dc=xxx //管理员账号的路径

search-base-dn dc=xxx,dc=xxx //该搜索路径只要包含用户所在目录即可

ip x.x.x.x

login-password cipher xxxxxxx

相关配置未见明显异常

debug ldap 报错信息如下

*Mar 17 11:40:12:711 xxxx FW LDAP/7/EVENT: -COntext=1;

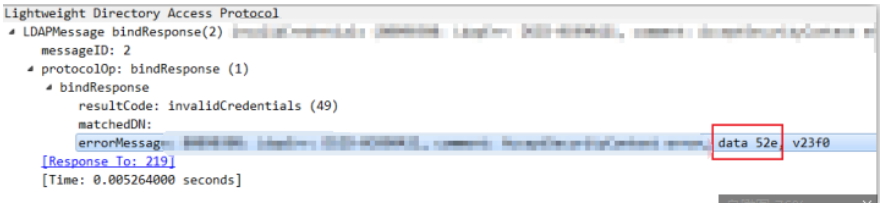
PAM_LDAP:Get result message errno = 49

*Mar 17 11:40:12:711 xxxx FW LDAP/7/ERROR: -COntext=1;

PAM_LDAP:Failed to perform binding operation as administrator.

抓取与ldap服务器交互的包

报错信息如下图所示（参考案例：https://zhiliao.h3c.com/Theme/details/30706）



debug报错（没有权限或者密码配置错误）及抓包结合来看指向了管理员账户密码配置错误

此时可以让用户使用提供给代理商的管理员账户及密码登陆ldap服务器来进行测试

解决方法

客户在登陆ldap服务器的过程中，发现管理员账户密码错误，后续修改管理员密码，sslvpn用户可正常登陆。

用户侧一般有众多密码，难免会记忆错误；此时需要坚信设备的debug信息及抓包信息，寻找到合适的方法让用户能够配合测试