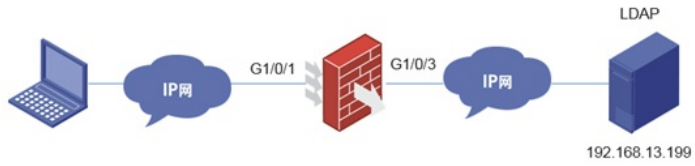
SSLVPN结合ldap用户账号认证不成功经验案例

SSL VPN 孙兆强 2019-11-21 发表

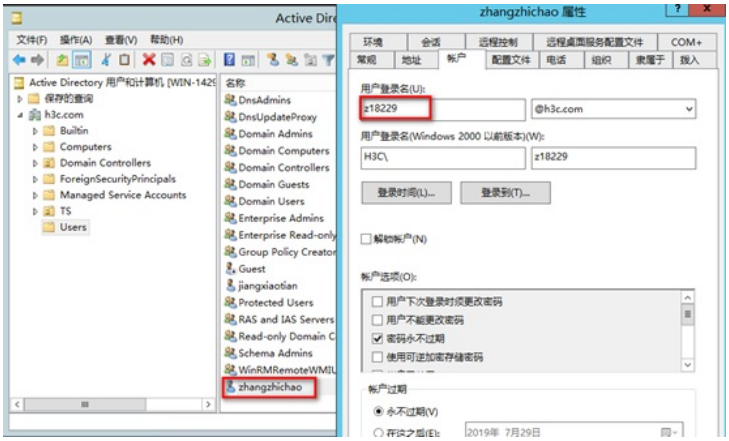
组网及说明



FW结合ldap服务器做sslvpn认证

问题描述

使用用户的用户名” zhangzhichao”可以登陆,使用用户的账号”z18229”ldap无法认证通过



过程分析

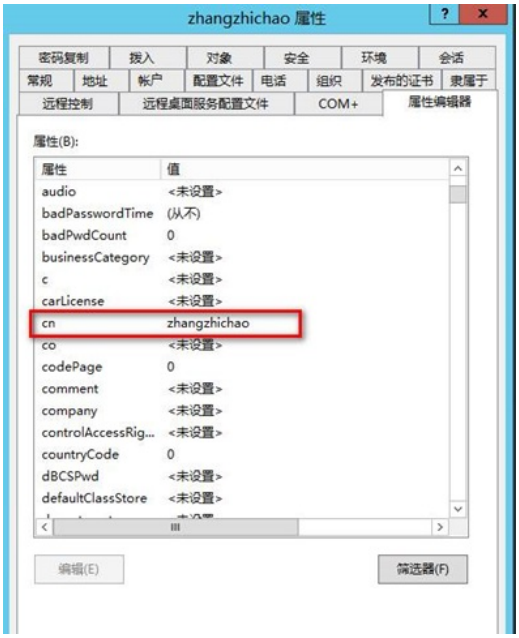
在设备上debug

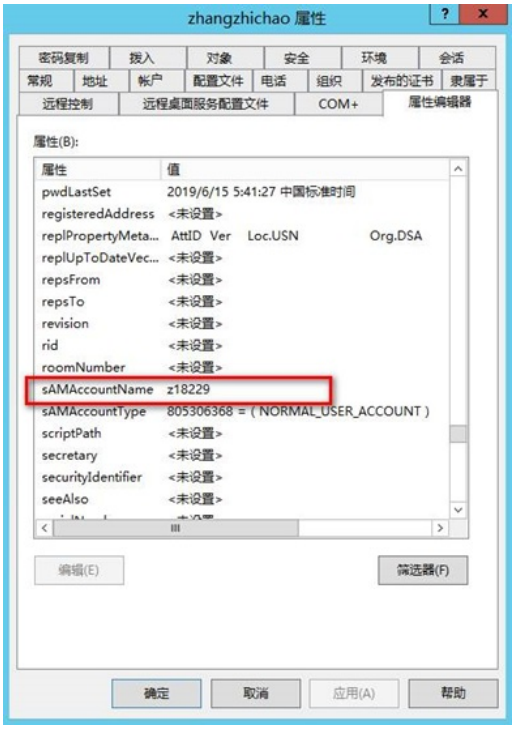
*Nov 12 13:52:53:196 2019 F1030-old LDAP/7/EVENT: -COntext=1;
PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(cn=z18229)).
*Nov 12 13:52:53:196 2019 F1030-old LDAP/7/EVENT: -COntext=1;
PAM_LDAP[Authen]:Search base DN is dc=h3c,dc=com.

*Nov 10 11:05:16:429 2019 F1030-old LDAP/7/ERROR: -COntext=1;
PAM_LDAP:Failed to bind user z18229 for the result of searching DN is NULL.
从上面debug看用账号查询无法查出用户

“zhangzhichao”可以叫做“用户” 属性为CN
我们设备默认查询用户名属性CN，也就是以“用户”去查询，如果要以“账号”去查询需要修改FW配置。
user-name-attribute { name-attribute | cn | uid }：表示用户名的属性类型。其中，name-attribute表示属性类型值，为1～64个字符的字符串，不区分大小写；cn表示用户登录帐号的属性为cn（Common Name）；uid表示用户登录帐号的属性为uid（User ID）。
设备配置修改如下
ldap server ldapserver
login-dn cn=administrator,cn=users,dc=h3c,dc=com
search-base-dn dc=h3c,dc=com
ip 192.168.13.199
login-password cipher c3$qqlHtd4Wz+iB0puZbbAHEUocFNwODy3oFWc=
user-parameters user-name-attribute samaccountname

用用户属性 sAMAccountName 去查询即可。





解决方法

增加命令

user-parameters user-name-attribute samaccountname

再次收集debug设备查询的过滤条件已改变,属性由CN变为samaccountname

*Nov 10 12:25:40:448 2019 F1030-old LDAP/7/EVENT: -COntext=1;

PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(samaccountname=z18229)).