



某局点SSLVPN结合LDAP登录失败

SSL VPN

AAA

赛祖尧

2021-12-07 发表

组网及说明

不涉及

问题描述

现场配置SSLVPN结合LDAP进行登录，经过现场配置测试发现，使用WEB页面输入用户名密码可以成功登陆，但是使用iNode无法拨号，有如下报错



过程分析

1、确认下login-dn 这个LDAP的超管的账户的路径对不对

ldap server svpn_ldap

login-dn it-ldap //该账号需要具有超级管理员权限，需要修改此项配置

search-base-dn ou=XXX,dc=gz-hanhua,dc=com

ip XXXXX

login-password cipher \$c\$3\$OGGAptiB4rB269rBrIodpxQw0OBKO6INk8VId0U=

user-parameters user-name-attribute samaccountname

2、之前说的增加映射表配置，并且在ldap scheme里面调用，具体配置参考这个案例核对下

<https://zhiliao.h3c.com/Theme/details/165528>

如果测试不通过需要收集一份最新的配置信息和最新的下列debug

debugging sslvpn error

debugging sslvpn event

debugging sslvpn aaa

debugging ldap all

经过查看debug后发现

*Dec 1 18:10:11:244 2021 SecPath F1000-AK1160 SSLVPNK/7/SSLVPN_ERROR: IPAC: Failed to allocate IP address. COntextID=0x1, OnlineID=0x30

有如上报错，并且查看iNode的日志发现，也有类似的报错信息

[2021-12-01 18:40:33] [Warn] [47a8] CSslClient::conn2Remote failed to build the SSL VPN network.

解决方法

后续修改SSLVPN地址池相关配置后解决

