某局点 SecPath F1000-AK135(V7) ssl vpn 结合ldap不成功

SSL VPN 王燕 2020-04-28 发表

组网及说明

不涉及

问题描述

ssl vpn 结合ldap认证不成功，查看debug 发现ldap 查询用户失败。

过程分析

1、检查设备相关配置，调用本地证书

```
pki domain sslvpn
 public-key rsa general name sslvpn
 undo crl check enable

 sslvpn gateway sslvpn_gateway
 ip address 221.5.10X.X
 service enable

 interface SSLVPN-AC1
 ip address 10.1.229.254 255.255.255.0

 sslvpn ip address-pool sslvpnpool 10.1.229.1 10.1.229.253

sslvpn context sslvpn_instance
 gateway sslvpn_gateway
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool sslvpnpool mask 255.255.255.0
 ip-route-list H3Colud_Desktop
  include 10.1.1.1 255.255.255.255
  include 10.1.200.1 255.255.255.255
  include 10.1.200.219 255.255.255.255
  include 10.1.219.0 255.255.255.0
  include 10.1.242.0 255.255.255.0
 policy-group resourcegrp
  filter ip-tunnel acl 3999
  ip-tunnel access-route ip-route-list H3Colud_Desktop
  ip-tunnel address-pool sslvpnpool mask 255.255.255.0
 default-policy-group resourcegrp
 aaa domain rdc
 service enable

 domain rdc
 authentication sslvpn ldap-scheme grgit.com
 authorization sslvpn ldap-scheme grgit.com
 accounting sslvpn none

 ldap scheme grgit.com
 authentication-server grgit.com
 authorization-server grgit.com
 attribute-map grgit.com


 ldap server grgit.com
 login-dn cn=h3cldap,cn=users,dc=grgit,dc=com
 search-base-dn dc=grgit,dc=com,cn=users
 ip 10.1.1.1
 login-password cipher $c$3$6zyzJh/1YDe9Y42IYNHPtHl73Ueps+22bSej

 ldap attribute-map grgit.com  //添加用户时设置的属性字段
 map ldap-attribute memberof prefix cn= delimiter , aaa-attribute user-group
```

2、

<H3C>debugging ldap all
<H3C>debugging sslvpn aaa
Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Processing LDAP authentication.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Data of authentication request successfully sent.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Processing AAA request data.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:LDAP server is: 10.1.1.1.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Current bind state is 4.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Search user when authentication.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Username is jiayu.
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(cn=jiayu)).
*Apr 3 18:11:51:843 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP[Authen]:Search base DN is dc=grgit,dc=com,cn=users.
*Apr 3 18:11:51:844 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Response timeout timer successfully created.
*Apr 3 18:11:51:844 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Get result message errno = 1
Apr 3 18:11:51:844 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:User jiayu search done.
*Apr 3 18:11:51:844 2020 H3C LDAP/7/ERROR: -COntext=1;
 PAM_LDAP:Failed to search users.
*Apr 3 18:11:51:844 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Processing LDAP authentication.
*Apr 3 18:11:51:844 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

解决方法

去掉cn=users后打debug出现了如下报错
*Apr 7 14:41:27:115 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP:User jiayu search done.
*Apr 7 14:41:27:115 2020 H3C LDAP/7/EVENT: -COntext=1;
 PAM_LDAP[State]:State switch from authentication searching to binding user.
*Apr 7 14:41:27:115 2020 H3C LDAP/7/ERROR: -COntext=1;
 PAM_LDAP:Failed to bind user jiayu for the result of searching DN is NULL.
用户名不对，增加 user-parameters user-name-attribute sAMAccountName解决。