某局点WX2560X 本地802.1X（EAP-GTC）+LDAP认证失败

802.1X 王子腾 2023-05-05 发表

组网及说明

WX2560X+WA6530，集中转发+二层注册，AC与LDAP服务器都旁挂核心交换机。

问题描述

手机端无线用户连接到WLAN网络，并使用对应用户名进行802.1X认证，阶段2认证选择GTC，认证失败。

过程分析

1、首先检查AC的配置。

```
#已配置PKI域，且证书已导入设备
pki domain eap-gtc
 public-key rsa general name eap-gtc
 undo crl check enable
pki import domain eap-gtc p12 local filename local.pfx
pki import domain eap-gtc pem ca filename server.cer
#已配置SSL服务器端策略且引用PKI域。
ssl server-policy ssl-eap
 pki-domain eap-gtc
#已指定认证方式为peap-gtc，且引用ssl服务器策略
eap-profile eap-ldap
 method peap-gtc
 ssl-server-policy ssl-eap
#802.1X已指定EAP认证
dot1x authentication-method eap
#已配置ISP域
domain eap-gtc
 authentication lan-access ldap-scheme 802.1x
 authorization lan-access none
 accounting lan-access none
#已配置LDAP方案，并指定LDAP认证服务器
ldap scheme 802.1x
 authentication-server 802.1x
#已配置LDAP服务器，IP和用户名密码都正确
ldap server 802.1x
 login-dn cn=administrator,cn=users,dc=itgfinacne,dc=com,dc=cn
 search-base-dn ou=itg 财务公司  ,dc=itgfinacne,dc=com,dc=cn
 ip 10.10.10.10
 login-password cipher $c$3$Ci9VdK/Xq3+Bll4EKskzBx3i7wtPfV5aUlLdkA==
#服务模板已应用802.1X认证
wlan service-template h3c
 ssid H3C
 vlan 100
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain eap-gtc
 dot1x eap-termination eap-profile eap-ldap
 dot1x eap-termination authentication-method pap
 service-template enable
#对应AP的Radio已绑定对应服务模板
wlan ap ap1 model WA6530
serial-id xxxxxxx
ap-model WA6530
  radio 1
   radio enable
   service-template h3c
  radio 2
   radio enable
   service-template h3c
  radio 3
   radio enable
   service-template h3c
  gigabitethernet 1
  smartrate-ethernet 1
```

2、检查AC与LDAP服务器连通性，也正常。

3、收集debugging dot1x all、debugging ldap all信息

PAM_LDAP:Processing LDAP authentication.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Processing LDAP request data.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:LDAP server is: 10.8.24.10.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Current bind state is 4.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Search user when authentication.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Username is wangshanshan.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP[Authen]:Search filter is (&(objectClass=person)(cn=wangshanshan)).

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP[Authen]:Search base DN is ou=itg财务公司,dc=itgfinacne,dc=com,dc=cn.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Response timeout timer successfully created.

*Apr 21 16:28:09:460 2023 ac LDAP/7/EVENT:

PAM_LDAP:Data of authentication request successfully sent.

*Apr 21 16:28:09:461 2023 ac LDAP/7/EVENT:

PAM_LDAP:Get result message errno = 32

*Apr 21 16:28:09:461 2023 ac LDAP/7/EVENT:

PAM_LDAP:User wangjingjing search done.

***Apr 21 16:28:09:461 2023 ac LDAP/7/ERROR:**

PAM_LDAP:Failed to search users.

***Apr 21 16:28:09:461 2023 ac LDAP/7/EVENT:**

PAM_LDAP:Processing LDAP authentication.

***Apr 21 16:28:09:462 2023 ac LDAP/7/EVENT:**

PAM_LDAP:Data of authentication reply successfully obtained, resultCode: 1.

%Apr 21 16:28:09:462 2023 ac DOT1X/5/DOT1X_WLAN_LOGIN_FAILURE: -Username=wangshanshan-UserMAC=7e2e-5d6e-ede3-BSSID=7c7a-3c28-acb0-SSID=CWGS-APName=ap13-RadioID=1-VLANID=126; A user failed 802.1X authentication.Reason:AAA processed authentication request and return 26.

AAA处理认证请求反馈的错误code26，一般为用户名或密码错误、认证类型错误、服务器上没有添加设备IP地址、服务模板下认证域配置错误。 /////这些已确认都无误

LDAP error提示查找用户失败，查看登录的administrator用户在user文件夹下，真正用户在ITG财务公司文件夹下，后排查发现绑定的administrator管理员没有查询ITG财务公司目录的权限，添加查询权限后可以认证成功。