无线802.1x认证，AC采取eap方式，结合imc ldap用户认证时报用户密码错误

wlan接入 802.1X iMC EIA **刘建立** 2022-01-20 发表

组网及说明

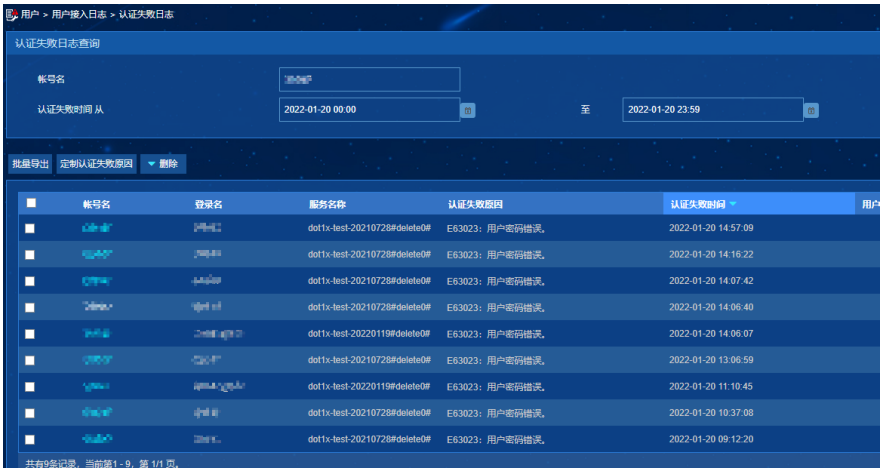
问题现象：imc中的本地用户认证成功，从ldap同步过来的用户报用户密码错误。两个用户接入服务一致。

基本配置如下：

1、iNode客户端，无线连接，PEAP自动类型；

2、无线AC采用dot1x认证，eap认证方式；

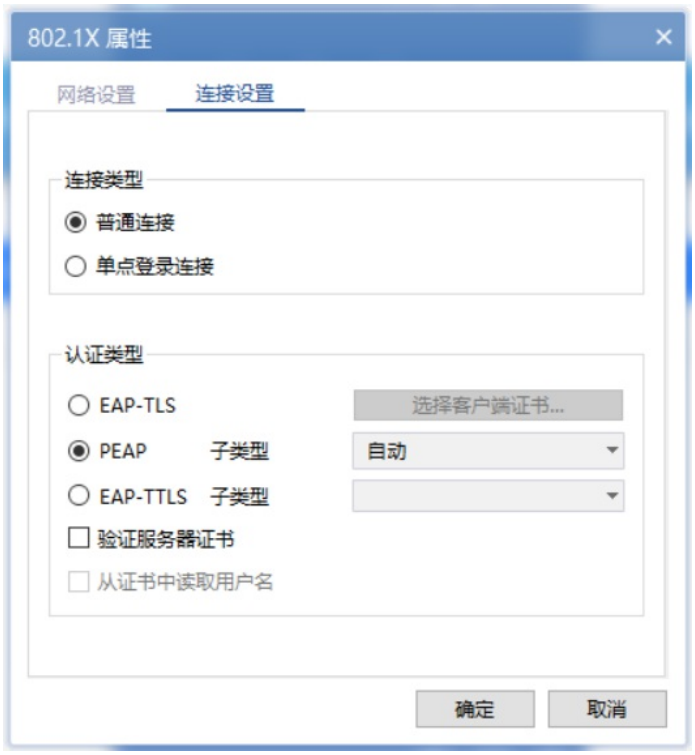
3、imc中自动同步ldap用户。



问题描述

基本配置如下：

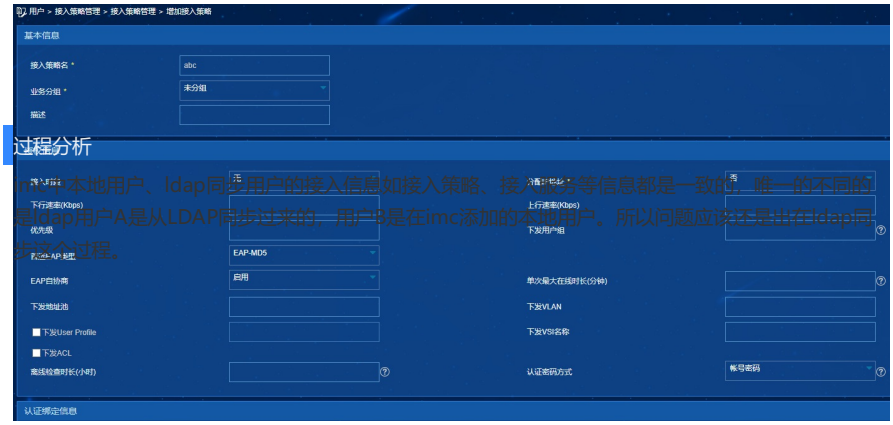
1、iNode客户端，无线连接，PEAP自动类型；



2、无线AC采用dot1x认证，eap认证方式；

```
 dot1x
 dot1x authentication-method eap
#
wlan service-template 1x-test
 description 1x-test
 ssid 1xtest client forwarding-location ap
 user-isolation enable
 client vlan-alloc static
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 security-ie wpa
 client-security authentication-mode dot1x
 dot1x domain 1xtest
 bss transition-management enable
 service-template enable
#
# domain 1xtest authentication lan-access radius-scheme admin
 authorization lan-access radius-scheme admin
 accounting lan-access radius-scheme admin
#
# radius scheme admin primary authentication 10.10.10.10
primary accounting 10.10.10.20
key authentication cipher $c$3$T0vH3oQSw4jrZ8TaA30h4pnbRrULahE5ShyCygo=
 key accounting cipher $c$3$2rY5jtbGDXCPjotZszdLJ0TWKF0GWDy9SeDqgHc=
 user-name-format keep-original
#
```

3、imc中自动同步ldap用户。



过程分析

imc中本地用户、ldap同步用户的接入信息如接入策略、接入时长等信息都是一致的，唯一的不同的是ldap用户A是从LDAP同步过来的，用户B是在imc添加的本地用户。所以问题应该主要出在在ldap同步这个过程。

解决方法

咨询imc研发，确认openldap不支持实时的peap-mschapv2，而在imc中配置接入策略时首选的 EAP类型中 EAP-PEAP 默认为 EAP-MSCHAPv2。导致从ldap同步过来的用户A认证失败。如下图修改类型之后，iNode接入成功：