

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

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。

帐号名	登录名	服务名称	认证失败原因	认证失败时间
test1	test1	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 14:57:09
test2	test2	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 14:16:22
test3	test3	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 14:07:42
test4	test4	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 14:06:40
test5	test5	dot1x-test-20220119#delete0#	E63023: 用户密码错误.	2022-01-20 14:06:07
test6	test6	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 13:06:59
test7	test7	dot1x-test-20220119#delete0#	E63023: 用户密码错误.	2022-01-20 11:10:45
test8	test8	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 10:37:08
test9	test9	dot1x-test-20210728#delete0#	E63023: 用户密码错误.	2022-01-20 09:12:20

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。

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 *

业务分组 *

描述

接收信息

接入时延

分配IP地址

过程分析

认证策略

前缀EAP类型

EAP认证策略

下发地址池

下发User Profile

下发ACL

鉴权检查时长(小时)

下发用户名

最少最大时长(分钟)

下发VLAN

下发VPI名称

认证密码方式

认证绑定策略

imc中本地用户、ldap同步用户的接入信息如接入策略、接入服务等信息都是一致的，唯一的不同的是用户A是从LDAP同步过来的，用户B是在imc添加的本地用户，所以问题应该还是出在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：

基本信息			
接入策略名 *	abc		
业务分组 *	未分组		
描述			
授权信息			
接入时段	无	分配IP地址 *	否
下行速率(Kbps)		上行速率(Kbps)	
优先级		下发用户组	?
首选EAP类型	EAP-PEAP	子策略	EAP-MSCHAPV2
EAP回退策略	启用	单次最大在线时长(分钟)	?
下发地址池		下发VLAN	
■ 下发User Profile		下发VSI名称	
■ 下发ACL		认证服务器	
策略生效时长(小时)		认证服务器方式	帐号密码



