

组网及说明

不涉及

问题描述

某局点用EIA做传统的mac认证，EIA上没有加mac，但是AC上认证是通过的，EIA上在线用户列表没看到这个mac，mac地址是60ab-67ef-5ac9。

过程分析

Mac认证的逻辑相对简单，终端接入网络后自动发起用户认证请求，设备收到用户的认证请求后向AA发起认证请求。EIA根据设备发送的信息接收处理响应。本案例主要介绍EIA侧的故障问题排查。需要收集信息如下：

- 1、收集uam 调试级别的日志信息
 - 2、收集服务器侧的抓包信息（非必须）
 - 3、设备侧debug radius信息
- 设备侧初步排查，该用户在设备侧在线

MAC address	User name	AP name	R IP address	VLAN
00be-3bc1-		AP-11	3 10.181.	10
1c48-ceae-	id20	AP-14	3 10.188.	40
2479-f31a-	en	AP04	2 10.181.	10
287f-cf89-		AP-04	1 10.181.	10
28ff-3c11-		10F-AP03	3 10.187.	20
30d9-d9bd-	6e4	AP-11	1 10.188.	40
3cf5-919a-		10F-AP03	3 10.186.	30
48fd-a310-	an	AP-21	3 10.181.	10
48fd-a3f2-		10F-AP05	3 10.187.	10
60ab-67ef-5ac9	60ab67ef5ac9	AP-11	1 10.188.	40
bcd/-1f96-	136caaxx	AP-14	3 10.181.	10
70d9-23dc-	04	AP-21	3 10.181.	10
7836-cc7d-		10F-AP03	3 10.187.	20
7c03-5ef2-	ang02	AP-13	1 10.181.	10
8ec7-c47f-	77	AP01	3 10.188.	40

1、查看iMC侧UAM日志

EIA有正常接收该MAC地址的接入认证请求

```

%% 2020-10-14 16:54:16.295 ; [LDBG] ; [22236] ; LAN ; 60ab67ef5ac9:mac ; 1 ; 1876acd9de7d496e576705ca7c68355 ; ; Received message from 10.255.6.2:
Code = 1 ID = 34.
User-Name (1) = 60ab67ef5ac9:mac
Password(2) =
Service-Type(6) = 10.
Framed-Protocol(7) = 1.
NAS-Identifiers(3) =
NAS-Port(5) = 1677256.
NAS-Port-Type(6) = 13.
NAS-Port-Id(8) = 0100000000000040
Calling-Station-Id(31) = 60-AB-67-FF-5A-C9
Called-Station-Id(30) = 94-29-2F-E1-E7-10
hw_mac_status_timestamp(59) = 160260326
Acct-Session-Id(44) = 0000004202010141647160000017708100576
HW_NEW_USER_ATTRIBUTE_NAME(133) =
Framed-IP-Address(8) = 10029385.
hw_IP_Host_Addr(60) = 10.188.4.33 60rab67ef:5ac9
H3C_DHCP_Option53(208) = 0103060f1a1c33a3b2b
NAS-IP-Address(4) =
hw_Product_ID(255)

```

接收该用户的认证请求后

```

%% 2020-10-14 16:54:16.295 ; [WARN] ; [6840] ; LAN ; o.getUserInfo: user 60ab67ef5ac9 does not exist.
%% 2020-10-14 16:54:16.295 ; [LDBG] ; [6840] ; LAN ; o.getUserInfo: no user found for 60ab67ef5ac9:mac; go ldap sync-on-need.
%% 2020-10-14 16:54:16.295 ; [LDBG] ; [6840] ; LAN ; lanAuth.getUserInfo: ldap sync-on-need auth user 60ab67ef5ac9:mac.
%% 2020-10-14 16:54:16.295 ; [LDBG] ; [6840] ; ldap ; simpleldapAuthProc: begin.
%% 2020-10-14 16:54:16.295 ; [LDBG] ; [6840] ; ldapUserMgr ; realtimeGetPooler: begin to connect ldap Server(version 3).
%% 2020-10-14 16:54:16.301 ; [LDBG] ; [6840] ; ldapUserMgr ; realtimeGetPooler: to call realtime-sync with filter (&AMAccountName=60ab67ef5ac9).
%% 2020-10-14 16:54:16.301 ; [ERR] ; [6840] ; ldap ; searchldaptr: End to get attr.
%% 2020-10-14 16:54:16.301 ; [ERR] ; [6840] ; ldap ; ldapUserRealtimeSync: fail to call searchldaptr.
%% 2020-10-14 16:54:16.301 ; [LDBG] ; [6840] ; ldapUserMgr ; realtimeGetPooler: realtime-sync returned 63036 for svrid 2.
%% 2020-10-14 16:54:16.301 ; [LDBG] ; [6840] ; UserMgr ; realtimeGetPooler: no such a user in ldap server.
%% 2020-10-14 16:54:16.301 ; [WARN] ; [6840] ; UserMgr ; simpleldapAuth: fail to call realtimeGetPooler with err no 63036.
%% 2020-10-14 16:54:16.301 ; [ERR] ; [6840] ; ldap ; simpleldapAuthProc: Calling simpleldapAuthm failed. Error message: 63036: The user does not exist on the LDAP server..
%% 2020-10-14 16:54:16.301 ; [ERR] ; [6840] ; LAN ; lanAuth.getUserInfo: calling ldapAuthProc failed with error: 63036: The user does not exist on the LDAP server.

```

由于EIA侧不存在该用户，返回E63036的错误信息。

```

%% 2020-10-14 16:54:16.303 ; [LDBG] ; [6840] ; LAN ; Begin replyPrivateAttr, auth_step is 2, AttrPolicyId is -1, DeviceTypeid is 1100
%% 2020-10-14 16:54:16.303 ; [LDBG] ; [6840] ; LAN ; 60ab67ef5ac9:mac ; 0 ; ; Send message attribute list:
Code = 2 ID = 34:

```

但是日志中可以看到EIA回应了code = 2，认证成功，且本地未创建在线表等信息。

接下来需要分析EIA未按照正常方式回应的原因。

2、检查EIA侧配置

通常EIA检测不到用户的在线信息后，会回应code =3，用户认证失败。

在认证失败的情况下仍然回应认证成功，有以下2种情况：

1) 开启了用户仿真功能

用户认证仿真模式：启用该参数后，即使用户认证失败也返回认证成功，用户可以接入网络，但不会创建在线用户，用户下线后也不会生成接入明细。如果安装了CAMs计费管理组件，则不显示该参数。

在用户>接入策略管理>业务参数配置 > 系统配置 > 系统参数配置中，可以选择是否启用该功能。

2) 开启了UAM的逃生模式

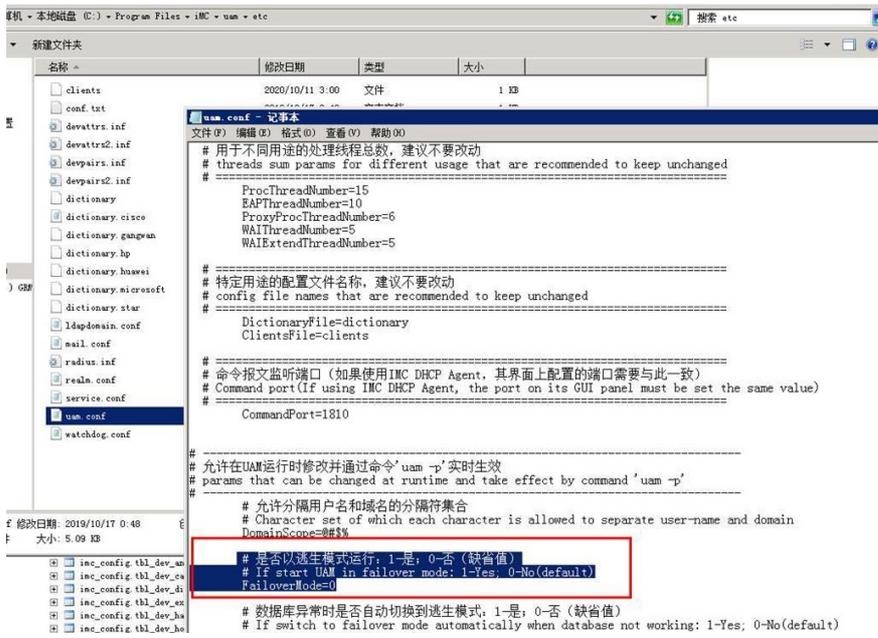
iMC安装目录下iMC/uam/etc下，uam.conf文件中，如下字段用于控制是否以逃生模式运行

```

# 是否以逃生模式运行: 1-是; 0-否 (缺省值)
# If start UAM in failover mode: 1-Yes; 0-No(default)

```

FailoverMode=0



解决方法

经现场确认, 系接入策略的系统参数中开启了用户认证仿真功能导致。

该参数默认关闭, 开启后即使用户认证失败也返回认证成功, 用户可以接入网络, 但不会创建在线用户, 用户下线后也不会生成接入明细。

仅在特定用户仿真的场景下开启, 现场关闭该功能后认证校验功能恢复正常。