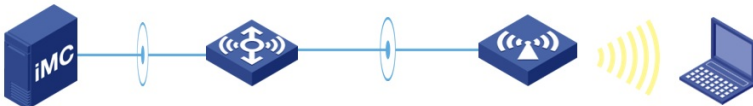


某局点使用Windows10自带客户端和iMC EIA组件做802.1x认证不成功的经验案例

802.1X iMC 李树兵 2018-09-13 发表

组网及说明

用户使用iMC EIA做无线802.1x认证，组网拓扑如下：



iMC EIA 7.3 E0501

问题描述

用户使用Windows10自带客户端 无法认证成功，提示报错为“无法连接此网络”，但是现场使用iNode客户端以及Windows 7自带客户端都是可以正常连接。



过程分析

通过日志发现UAM不识别TLS的版本

```
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.vrfyEapTls: The flags of received EAP-TLS message [0x0].
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.vrfyEapTls: non-fragment message (without TlsLen) received.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.procEapTls: begin - vrfyEapTls returned 11.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.extractRespPkt: received message - status:11, code:2, id:9, len1:46, type:25, len2:41.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.procEapTls: 0 bytes data already in stDirtyIn, received new 40 bytes data.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.plusRcord: adding 40 bytes to data.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.procEapTls: end with OK - Received tunneled data after successful handshake.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; PeapAuth.auth: procEapTls returned 11.
%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; EapTlsAuth.minusRcord: After getting 40, pRec stores 0 bytes data.
```

%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; tlsMsg: Other Record [ContentType:256, WriteFlag:0].

%% 2018-08-14 18:34:16.170 ; [LDBG] ; [21192] ; EAP ; tlsSessInfo: <<< Unknown TLS version [length 0005] ExInfo:ver-no:0x0 cntnt-type:[0]

windows10系统默认的TLS版本是1.2, 但是当前iMC EIA的版本不支持导致

解决方法

可以通过两种方法解决:

1. 修改Windows10客户端的注册表, 将TLS的版本改成1.1, 修改方法如下:

点击Win+R, 键入regedit, 然后回车, 找到并单击 (即选中) 以下注册表子项:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\PPP\EAP\13

在编辑菜单上 (即右侧空白处) 新建, 然后单击DWORD 值。DWORD值的名称, 键入TlsVersion, 然后按enter键。用鼠标右键单击TlsVersion, 然后单击修改。在数值数据框中, 针对不同的TLS版本键入以下值, 然后单击确定。将值改成0x300.

TLS 版本 双字节值

TLS 1.0 0xC0

TLS 1.1 0x300

TLS 1.2 0xC00

退出注册表编辑器, 然后重新启动计算机或重新启动 EapHost 服务。

2. 升级iMC EIA的版本到7.3 E0510H03版本, 并且使用非MD5作为签名摘要的证书 (比如iMC里面预置的证书)。不支持MD5作为签名摘要的证书是微软的限制, 对于TLS1.2版本是不支持MD5摘要的证书。