

知 关于EIA产品使用windows 11操作系统自带客户端进行802.1x证书认证失败问题的技术公告

802.1X 李大维 2021-11-19 发表

问题描述

【产品型号】

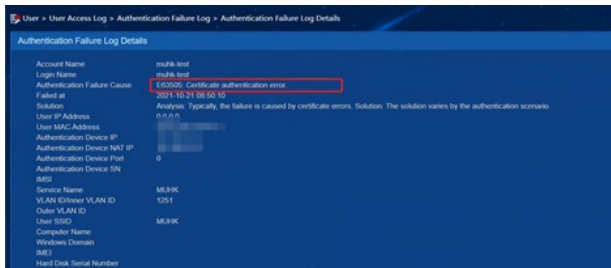
H3C_EIA_V7、H3C_EIA_V9

【涉及版本】

H3C_EIA_V7、H3C_EIA_V9所有发布的版本

【问题描述】

若使用Windows 11操作系统自带客户端结合EIA服务器进行802.1x证书认证（包括TLS和PEAP-MSChapv2），会发生认证失败，报错“E63505证书认证错误”，报错示例如下：



原因分析

【原因分析】

经微软定位问题发生在Windows 11操作系统进行EAP认证校验阶段，当EIA服务器向Windows 11终端发送标准的Server Hello交换秘钥报文后，该终端返回了拒绝，在EIA服务器网卡抓包信息如下：

No.	Time	Source	Destination	Protocol	Length	Info
13	2021-11-16 20:47:04.871267	Hangzhou_da:68:c:e	WShare_Rb:28:36	EAP	64	Request, Protected EAP (EAP-PEAP)
14	2021-11-16 20:47:05.069999	WShare_Rb:28:36	Nearest non-1998-br:	TLSv1	132	Client Hello
15	2021-11-16 20:47:05.268000	WShare_Rb:28:36	Nearest non-1998-br:	EAP	132	Response, Protected EAP (EAP-PEAP)
16	2021-11-16 20:47:05.084592	Hangzhou_da:68:c:e	WShare_Rb:28:36	EAP	1056	Request, Protected EAP (EAP-PEAP)
17	2021-11-16 20:47:05.899844	WShare_Rb:28:36	Nearest non-1998-br:	EAP	24	Response, Protected EAP (EAP-PEAP)
18	2021-11-16 20:47:05.909998	WShare_Rb:28:36	Nearest non-1998-br:	EAP	24	Response, Protected EAP (EAP-PEAP)
19	2021-11-16 20:47:05.109383	Hangzhou_da:68:c:e	WShare_Rb:28:36	EAP	1052	Request, Protected EAP (EAP-PEAP)
20	2021-11-16 20:47:05.117408	WShare_Rb:28:36	Nearest non-1998-br:	EAP	24	Response, Protected EAP (EAP-PEAP)
21	2021-11-16 20:47:05.117479	WShare_Rb:28:36	Nearest non-1998-br:	EAP	24	Response, Protected EAP (EAP-PEAP)
22	2021-11-16 20:47:05.126123	Hangzhou_da:68:c:e	WShare_Rb:28:36	TLSv1	140	Server Hello, Certificate, Server Key Exchange, Server Hello Done
23	2021-11-16 20:47:05.166922	WShare_Rb:28:36	Nearest non-1998-br:	TLSv1	41	Alert (Level: Fatal, Description: Access Denied)

其他版本的Windows操作系统没有该问题。

规避措施/解决方案

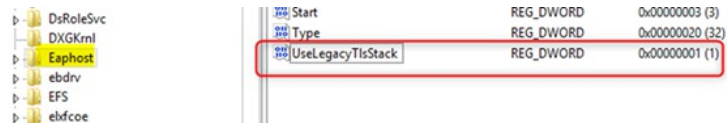
【规避措施 / 解决方案】

规避措施：

方案一：根据微软建议,通过修改Windows 11操作系统注册表进行规避,方法如下:

- 1、在无法认证的Windows 11终端上以管理员身份执行脚本regEAP.bat,
- 2、重启Windows 11操作系统生效,
- 3、若Windows 11操作系统终端注册表

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EapHost\ 下UseLegacyTlsStack的
DWORD键值为1时,说明注册表修改成功。



方案二：安装iNode E0558版本客户端进行证书认证。

