# 🔎 某局点使用windows自带客户端进行有线802.1X认证失败案例

iMC 潘韬略 2020-03-13 发表

组网及说明
不涉及
问题描述
现场使用做有线802.1X认证,发现使用iNode客户端可以认证成功,但是使用windows自带客户端认证 失败。
过程分析
1、使用windows自带客户端进行认证时,查看iMC后台日志记录:[ERR];[6936];EAP;EapTIsAuth.reGenContxt:certificate file does not exist.

故怀疑现场没有配置证书。

2937 %% 2020-03-13 12:30:26.250 ; [LDBG] ; [6936] ; EAP 2938 %% 2020-03-13 12:30:26.250 ; [LDBG] ; [6936] ; EAP	, septismuth hit: mark. ; BapTisAuth.reGenContxt: current ssl index is 0 with tls=mode 0. : BanTisAuth.reGenContxt.centificate file tune is FRM
2005 WW 2020-03-13 12:30:26.265 [ERR] ; [6036] ; EAP ;	BapTisAuth.mcGenContwt: certificate file does not exist.
2941 WW 2020-03-13 12:30:26.265 ; [ERR] ; [6936] ; EAP ;	EapProc. typeSelect: can't load instance for type 25.
2942 WM 2020-03-13 12:30:26.265 ; [VAN] ; [6936] ; EAP ; 2943 WM 2020-03-13 12:30:26.265 ; [ERR] ; [6936] ; EAP ; 2944 WM 2020-03-13 12:30:26.265 ; [LDBC] : [6936] ; EAP	; captroc.auth: typeSelect returns 1 with ErrCode 0. capTsk.sv: calling auth failed, process request failed or request invalid, simply reject. :Bod@0214: 3 : 285746a607784dc76b58b5flba4fdd42 : capTsk.sv: Send packet to:192.168.0.3
2945 Code = 3 ID = 219 2946	
2947 W% 2020-03-13 12:30:26.265 ; [LDBC] ; [6936] ; EAP	; eapTsk.sv: Send packet to:192.168.0.3
2949 03 DB 00 2C B1 16 68 2C 78 86 E1 C5 D8 97 DC 5B	
2950 16 EE 75 3F 4F 06 04 02 00 04 50 12 6E 53 FA 4E 2951 DE 35 94 3D 0B C1 03 BE 07 D1 41 1D	

2、远程查看现场环境配置,发现接入策略中的首选EAP类型选择的是EAP-MD5,选择该认证类型时, iNode是可以支持的,但是windows自带客户端不支持该类型,只能使用PEAP或者TLS;故需要修 改iMC的接入策略首选EAP类型为EAP-PEAP,子类型为MSCHAPv2,并导入iMC预置证书后可以认 证成功。(注:此时设备上认证类型需要选为EAP)

### 解决方法

- 现场参考上述调整iMC配置即可。
- 1、修改iMC的接入策略首选EAP类型为EAP-PEAP, 子类型为MSCHAPv2;

HBC Intelligent Management Center		首页	92B	用户	445	69	报表	系统管理			۹ * 🖈		💧 Sbw 🗸
用户管理	6	1. 用户 > 接入策制	<b>信理 &gt; </b> 接入	黄疸管理 > 1	助接入策略								
· 接入用户管理 >		基本信息											
访客管理	н			_			-						
终端管理	L	接入策略名 *		有线80	2.1X								
用户接入日志	L	业务分组*	1	未分组									
接入策略管理 ~	L	描述		使用W	indows自带有	户端							
22 快速入门		1812/ILM											
9. 接入服务管理	1												
U. 接入策略管理		接入时段			无			•	分配IP地址	20		-	
<ul> <li>接入条件管理</li> </ul>		下行遗率(Kbps)	E.						上行速率(Kbps)				
<ul> <li>接入设备管理</li> </ul>	L	优先级							下发用户组			3	
▶ LDAP业务管理		首选EAP类型			EAP-PEA	,		-	子英型	EAP-MSCHAP	2	•	
<ul> <li>Portal服务管理</li> </ul>		EAP自协商			启用			•	单次最大在线时长(分钟)			1	
▼ 业务参数配置		下发地址地							下发VLAN				
15 系统範囲		下发User F	Profile						下发VSI名称				
<b>23</b> 证书配册		下发ACL											
1. 有些资料级 1. 有能终端有户端升级		高线检查时长(/)	NBJ)					1	认证密码方式	帐号密码	,	•	

## 2、导入iMC预置证书;

HBC Intelligent Management Center		前页	97 <b>2</b>	用户	468	48	18W	系统管理	(. saza	۹) ۲	★ в	🎒 Sbw 👻
用户管理	2	100 用户 > 接入策	略管理 > 业务	) < 聖法法令	Z-15 MR.SR							<b>⑦ 帮助</b>
接入用户管理	5		-		_							
访察管理	>	证书文件校验	已导入证书	始 早入	的资产书							
终端管理	>	♥提示			1							
用户接入日志	>	同一种类型	的服务器证书。	<b>R能上传一</b> 个								
接入策略管理	~	_										
12 快速入门	1	根证书配置	服务器证	BALER								
9. 接入服务管理	1	导入EAP根	证书 导入W	/API根征书	¥							
10. 接入策略管理	1											_
<ul> <li>接入条件管理</li> </ul>	1	創发者 ≎					±	題 0	奥型 ≎		动作	
AN 1 10 M 10 M	- 1	CN=VeriSi	gn Class 3 Pu	blic Primary	Certificatio	n Authority -	G5,O CI	N=Symantec Class 3 Secure Server CA - G4,OU=Symantec 1	rust EAP模记	E#6	D. 19. 1	9. E.
112人民國國法	1	CN=VeriSi	gn Class 3 Pu	blic Primary	Certificatio	n Authority -	G5,0 CI	N=VeriSign Class 3 Public Primary Certification Authority - 0	iS, EAP機管	[书	0.00	4 B.
◆ LDAP型务管理	- 1											
<ul> <li>Portal服务管理</li> </ul>												
▼ 业务参数配置												
き 系統配置												
18 证书和盟												
合: 客户纳升级												
2: 智能转换客户统升级												
· 单点登录配置									3	骸活 Windows		
&* 彩动和型型工士动											病"以識活 V	Vindows,

【附】

WIN7系统使用自带软件进行有线802.1X认证时的配置方法

### 前提条件

选择"开始 > 控制面板",依次单击"管理工具"和"服务",确认"Extensible Authentication Protocol"和"Wir

ed AutoConfig"两个服务的"启动类型"为"目动","状态"为"已启动"。

## 操作步骤

1、选择"开始 > 控制面板"。

2、在"控制面板"选择"网络和Internet > 网络和共享中心"(控制面板的"查看方式"选择"类别"时可显示" 网络和Internet")。

3、单击本地连接,选择"属性"。

4、在"身份验证"页签,选中"启用IEEE802.1X身份验证","选择网络身份验证方法"选择"PEAP"。单击" 设置"。

🔋 小网 雇性 📉 📉
网络 身份验证 共享
<ul> <li>选择此法项,以便为此以太网适配器提供已验证的网络 访问权限。</li> <li>☑ 启用 IEEE 802.1X 身份验证 (0)</li> <li>选择网络身份验证方法 (0):</li> <li>Microsoft: 受保护的 EAP (PEAP) →</li> <li>☑ 每次發录时记住此注接的賃据 (B)</li> </ul>
☑ 回滚到未经授权的网络访问 (7)
其他设置 0)
确定 取消

5、取消选中"验证服务器证书","选择身份验证方法"选择"安全密码 (EAP-MSCHAP v2)",并在右侧单击"配置"。

受保护的 EAP 属性
当连接时: □ 验证服务器证书 (V) □ 连接到这些服务器 (0):
受信任的根证书颁发机构 (B): Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert High Assurance EV Root CA Entrust. net Certification Authority (2048) Equifax Secure Certificate Authority GeoTrust Global CA GTE CyberTrust Global Root イ Ⅲ 不提示用户验证新服务器或受信任的证书授权机构 (P)。
法择身份验证方法(5): 安全密码(CAP-MSCHAP v2)    ■ 配置(C) ♥ 启用快速重新连接(P) □ 强制执行网络访问保护(0) □ 如果服务器未提供加密绑定的 TLV 则断开连接(0) ■ 启用标识隐私(1)

6、取消选中"自动使用 Windows 登录名和密码",单击"确定"。

EAP MSCHAPv2 属性
当连接时:
□ 自动使用 Windows 登录名和密码(以及域,
□ 如果有的话) (A)。
确定取消

说明:如果操作系统使用AD域帐号登录,并且用来进行802.1X认证的用户名和密码也是使用的登录操作系统的域帐号和密码,则勾选"自动使用Windows登录名和密码"。

7、等待Windows弹出认证框,即可输入用户名和密码进行认证。