# CPPM 对接 AD, 无法使用 AD 账号实现 1X 认证

#### By CCE

## 现象描述:

CPPM v6.11.1, 采用加入 AD 域的方式来实现终端的 802.1x 认证(采用 EAP-PEAP 认证方法),无论是加域的终端还是非加域终端,在用户认证阶段失败。

在 Access Tracker 的 Alerts 选项卡中提示

MSCHAP:AD status:The user account is restricted so that it cannot be used to log on from the source workstation.(0xc0000070)

#### 错误信息截图如下:

Summary         Input         Output         Alerts           Error Code:         216           Error Category:         Authentication failure           Error Message:         User authentication failed           Alerts for this Request         RADIUS           MSCHAP:         AD status: The user account is restricted so that it cannot be used to log on from the source workstation. (0xc000070)           MSCHAP:         Authentication failed           EAP-MSCHAPv2:         User authentication or password change failed	lequest Deta	ils
Error Code: 216 Error Category: Authentication failure Error Message: User authentication failed Alerts for this Request RADIUS MSCHAP: AD status:The user account is restricted so that it cannot be used to log on from the source workstation. (0xc0000070) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication or password change failed	Summary	Input Output Alerts
Error Category: Authentication failure Error Message: User authentication failed Alerts for this Request RADIUS MSCHAP: AD status: The user account is restricted so that it cannot be used to log on from the source workstation. (0xc0000070) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication or password change failed	Error Code:	216
Error Message: User authentication failed Alerts for this Request RADIUS MSCHAP: AD status: The user account is restricted so that it cannot be used to log on from the source workstation. (0xc0000070) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication or password change failed	Error Categ	ory: Authentication failure
Alerts for this Request RADIUS MSCHAP: AD status: The user account is restricted so that it cannot be used to log on from the source workstation. (0xc0000070) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication or password change failed	Error Mess	age: User authentication failed
RADIUS MSCHAP: AD status:The user account is restricted so that it cannot be used to log on from the source workstation. (0xc0000070) MSCHAP: Authentication failed EAP-MSCHAPv2: User authentication or password change failed	Alerts fo	this Request
	RADIUS	ASCHAP: AD status: Ine doe does and a status of a stat
	12111 Harris	
	Poplar	
	1 section of	
	I A Sh	wing 4 of 1-75 records >>

### 问题原因:

这里报错的根本原因是 AD 上针对该账号开启了登录到功能,要求该账号只能在指 定的计算机名称主机上实现管理员登陆,如果该账号在其他的主机上登陆(该主机的 Hostname 不包含在登录到的 计算机名称列表中),那么 AD 是阻止其登陆权限的。

那我们用的加域终端本身就是该账号的登录到的指定计算机名称,为什么也是无法 登录呢?

原因就是在基于 AD 认证源的场景中, CPPM 采用 Join Domain 方式结合本地的 Samba 服务, 能够基于域控制器来认证 AD 域的用户.CPPM 在这个过程中会使用自己的 主机名向域控制器发送 user name, Challenge 和 response, 如果认证成功, AD 会返回 NT Key 给到 CPPM。

此时 AD 会认为该账号正登录到 CPPM 的主机名上,而 AD 中的该账号 的登录到中的计算机名称中没有 CPPM 的 Hostname。

Ad 的账号有个 登录到 属性, 一旦开启, 设置为该用户可以登录到指定的计算机 名称的主机上, 不在该列表中的其他主机上是不能使用该账号登录的。



	カク	自注时并例 0款归归显…
5	rin10 属性	? ×
51	拔入 环境	会话 远程控制
t.	远程桌面服务配置文件	│ 个人虚拟机 / COM+ /
	常规 地址 帐户	副置文件 电话 组织 隶属于
	用户登录名(V): win10	@arubal.local
8	用户登录名 (Windows 2000	以前版本)(11):
63	ARUBA1 \	win10
a:	, 登录时间 (L.) 登录	到(T)
1	□ 1 登录工作站	? ×
	<ul> <li>株产 在"计算机"名称中 名称。</li> <li>此用户可以登录到:</li> <li>C 所有计算机(C)</li> <li>「 下列计算机(T)</li> <li>计算机名称(D):</li> </ul>	a, 建入计算机的 NetBIOS 或域名系统(DMS)
	G	添加(4)
24	C windows-10	(编辑 Œ)
a		mig e co l
		UTUP IT CEL
		确定 取消
	- <u>m</u>	

## 解决办法:

- 在 AD 的每个账号的登录到的计算机名称中,增加 CPPM 的 Hostname。因为如果客 户使用该功能,那必然会针对每个账号所允许登录到的计算机名称是经常维护和变更 的。
  - i. 该方法不需要额外地在 AD 上开启 NPS 服务,降低操作的复杂性。
  - ii. 此时还是 CPPM+AD 认证源的方式,终端的信任 EAP 证书仍然是 CPPM
     RADIUS/EAP 服务器证书(强烈建议使用本地的 Onboard root ca 来签发一张
     私签的 RADIUS/EAP 服务器证书并导入到 CPPM 中)。
- iii. 终端的用户认证和机器认证需要提前在 Trusted Root Certification Authorities-受信任的根证书颁发机构中导入 CPPM Onboard root ca。 以下是 AD 账号的登录到的配置步骤截图:
- 在 AD 中找到指定的登录账号,然后鼠标双击下该账号,进入到账号属性界面,点击 账户选项卡,点击 登录到 按钮

vin10 属性 ? >
拨入         环境         会话         远程控制           远程桌面服务配置文件         个人虚拟机         COM+           常规         地址         帐户         配置文件         电话         组织         隶属于
用户登录名(0): win10
登录时间(L) 登录到(T)
■ 解锁账户(X) 帐户选项(0): □ 用户下次登录时须更改密码
<ul> <li>□ 用户不能更改密码</li> <li>□ 密码永不过期</li> <li>□ 使用可逆加密存储密码</li> </ul>
● 林戸过期 ● 永不过期(V) ● 在这之后(E): 2023年12月16日

2) 在登录到界面,在计算机名称中输入 CPPM Hostname, 点击添加按钮, 最后点击确

定按钮



2. 如果客户的终端数量多,且不想在每个终端的登录到的计算机名称中变更,那我们可以在 AD 上启用 NPS 服务并配置 ADCS.利用 AD 的 NPS 服务来实现 1X 认证,从而绕过了 登录到的指定计算机名称的限制,NPS RADIUS 需要 EAP 证书,同时开启用户认证组和机器认证组.实现的拓扑就是 无线接入-→CPPM-→ NPS(AD),认证源要变成 RADIUS Server 指向 NPS, CPPM 作为 RADIUS Proxy。

以下是 AD 上如何启用 NPS 服务的配置步骤截图:

🧇 🔿 🔲 🖬 🖬		
● MPS (本地)	WPS (本地)	
□ ■ NADIUS 香户端和服务器	λΠ	
<ul> <li>iii 远程 RADIUS 服务器组</li> <li>iiii 策略</li> <li>iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii</li></ul>	使用网络前尾属务器 (bts),可以总键和强制实施用于整个组织范围内的客户编建重、连接请求身份验证和连接请求授权的网络访问前局。	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	标准配置	
<ul> <li>● ● 阿強访问保护</li> <li>● ● 長板管理</li> </ul>	从列表中选择一种配置方案。然后单击下面的链接打开方案向导。	
	用于 802.1X 无线或有线连接的 RADIUS 服务器	
	PP留かり回接PORF/ 田上に居立、VPR は実体的 RADTIE 服装英 田土 RO2 17 手術の電話の第時の RADTIE 服装英	
		1798818L*1942×12×+
	■ 配置 802.1X	<ul> <li>了解详细信息</li> </ul>
	高級配置	
	<i>模板</i> 配置	



对于 NPS 来说, RADIUS Client 是 CPPM, 所以要添加 CPPM 信息。

<b>配置 802.1X</b>		×
	指定 802.1X 交换机 清指定 802.1X 交换机或无线访问点(BADIUS 客户编)	
RADIUS 客户的 端计算机。 若要指定 RAI	端都是网络访问服务器,如身份验证交换机和无线访问点。RADIUS DIUS 客户端,请单击"添加"。	客户端不是客户
RADIUS 客户 Aruba-7005 CPPM111	端 (C) :	<b>添加 (4)</b> /编辑 (2) 時時:(8)
	<b>上一步 10</b> 「下一步 00」 完成 (2)	

新建 RADIUS 客户端 🛛 🗙	配置 802.1Ⅰ ×
<b>设置</b> □ 选择现有模板(①):	<b>配置身份验证方法</b>
	法择此策略的 EAF 类型 ★毋 (基于访问方法和网络配置)(T): Dicrosoft: 受保护的 EAF (PEAF)
○ 手动(U)       ○ 生成(G)         共享机密(G):       ●●●●●●●●●●         确认共享机密(Q):       ●●●●●●●●●●         通定       取消	_ <b>上一步の」 下一步の </b> 完成の <b>取消</b>

这里调用的证书就是 EAP 证书,也叫做 RADIUS/EAP 服务器证书。

实际上是 ADCS 签发给 NPS 的服务器证书。

由 NPS 在 MMC 的机器账号的个人证书中创建 CSR, 然后由 ADCS 签发一张 RADIUS/EAP 服务器证书, 然后在 NPS 上下载并安装该服务器证书(实际就是导入该证书, 存储的位置 在 Local Machine 的 Personal 中)。

详细的配置步骤参考:https://arubase.club/archives/6422

E书颁发给 (I):	adi. arubai. local
支好名称: 顽发者:	arubal-ADI-CA
截止日期:	2024/2/21 21:31:25
。 启用快速重新 断开客户端而	连接 (7) 不加密绑定 (C)

配置 802.1X		×
	指定用户组 根据网络策略"访问权限"的设置。将允许或提她属于一个或多个选定组成员问。	的用户进行访
若要选择用户	组,请单击"添加"W。如果没有选择任何组,则此策略将应用于所有F	月户。
组		添加 @)
		071975 ( <u>A</u> )
		The Sale
	「ニータビ」「トータビ」「元成ビ」」	积消

选择组	? ×
选择此对象类型(S):	
组	对象类型(0)
查找位置 (F):	
arubai.local	位置 (L)
输入要选择的对象名称(例如) 图):	
domain users	检查名称(C)
「古伊山」	720
	明定 现洞 ///

选择组	? ×
选择此对象类型(S):	
组	对象类型(0)
查找位置 (F):	
arubal.local	位置 (1.)
输入要选择的对象名称(例如)(图):	
domain computers	检查名称(C)
高级(A)	确定 取消

在 NPS 上同时开启用户认证的用户组和机器认证的用户组

<b>配置 802.1X</b>					×
	指定用户组				
	根据网络策略"访问权限	"的设置,将允许	<b>午或拒绝属于一个</b>	或多个选定组成	员的用户进行访
	IC] •				
若要选择用户	组,请单击"添加"创。	如果没有选择的	任何组,则此策略	略将应用于所有	ī用户。
组 ARI/BA1\Dome	in liears				添加(0)
ARUBA1 \Doma	in Computers				刪除 (B)
1					
		上一步创	下一步创	完成 (E)	取消
配置 802.1X					×
	配置流量控制				
	使用虚拟 LAN (VLAN)和说	f间控制列表(AC	1) 控制网络流量。		
如果您的 RADI 则可以在此配法	CUS 客户端(身份验证交换 置这些属性。如果配置这些	机或无线访问点 些属性,则 NPS	5)支持使用 RAD 会指示 RADIUS	IUS 隧道属性分 客户端对已经	行配流里控制, 过身份验证和授
权的连接请求[	应用这些设置。 * 网络刺动 * 词* 后面和		" <b>下</b> 止"		
如果您不使用。	<sup>术</sup> 里投制以希望相后冉酉(1	至七川, 请早击	- h-\$~ •		
* 白小小山市13					
若要配置流量	ュ 型控制属性,请单击"配置	" °			
					配罟(C)
		上一步创	下一步回	完成创	取消



最后就是调整你创建好的网络策略的匹配顺序。

阿络策略服务器				
文件(F) 操作(A) 查看(V) 素	采動 00			
(= =) 2 📅 🛛 🖬				
🚯 NPS (本地)	品体 完成			
🖃 🚞 RADIUS 客户湍和服务器	Patron			
■ RADIUS 客户端 当 法程 RADIUS 服务契約	· 使用网络阑尾,可以指定已被使权注册到中国的用户,以及他们可以或无法连接到中国的环境。			
连接请求策略				
	TestTaschine"auth ビ目目 1 夜役切回 Unspecified あ subscholl Unspecified			
🗉 🌄 网络访问保护	资Connections to Microsoft Routing and Remote Access server 已自用 1000000 拒绝访问 Unspecified			
1 记帐	Connections to other access servers 已自用 1000001 拒绝访问 Unspecified			
🗉 🛫 锅饭酱理				
	7 test-machine-auth			
	条件 值 NSS 端门外刊 Nicolang = Okker OB Nicolang = TEPE 902 11			
	windows # AURAL Vionain Users OR AURAL Vionain Computers			
	设置 - 则应用下列设置:			
	设置值			
	身份验证方法 EAP OR MIS-CHAP v1 OR MIS-CHAP v1 (用户可以在密码过期之后更改密码) OR MIS-CHAP v2 OR MIS-CHAP v2 (用户可以在密码过期之后更改密码)			
	- 辺内形成 授取 2010 - 2000 - 2010			
	NAP 编制 / 代表全网络访问			
	France-Protocol PPP			
	ServiceType Franed weight True			
	可扩展的身份验证协议方法 Microsoft: 受保护的 EAP (PEAP)			
	可扩展的身份验证协议概要 已歐重			

在 CPPM 上创建认证源, 类型是 RADIUS 的, 指向 NPS, 然后在你需要的认证 service 中 调用该认证源.

Dashboard     O     Configuration » Authentication » Sources » Add - NPS       Monitoring     Authentication Sources - NPS       Configuration     Summary       General     Primary       Attributes       Services     Name:	
Monitoring     Authentication Sources - NPS	
Configuration     O       → © Service Templates & Wizards     - ○ Services         Name:     NPS	
—     Q Services Wizards     _     Q Services     Name:     NPS	
Authentication       Description:         Methods       Sources         Sources       Type:         RADIUS/RadSec Server       Use for Authorization:         Local Users       Use for Authorization:         Cal Users       Authorization Sources:         Static Host Lists       Remove View Det Compared         Cal Roles       Select	so fetch role e
Berger Discher Breiter Discher Discher Discher Breiter Discher Breiter	
□ · · · · · · · · · · · · · · · · · · ·	↑ /n↓ ₽

# Authentication Sources - NPS

Summary	General	Primary	Attributes		
Server Name:		10.254.5.	10.254.5.23		
Protocol:		RADIUS	RADIUS 🗸		
Port:		1812	1812 (Default is 1812)		
Secret:		••••••	••••••		