802.1X AAA **朱恺** 2017-09-21 发表

```
准备环境
1、centos 6.4 最小安装。
2、centos 已与外网调通,可以通过yum进行安装配置。
3、FAT AP或AC与centos三层网络可通。
操作步骤:
step1:
yum install freeradius
期间遇到Y/N选项一直选Y
yum install freeradius-utils
期间遇到Y/N选项一直选Y
step2:
执行radiusd -X
进入freeradius的调试模式。平时查看认证错误相关的日志也可以通过该模式进行log分析。
另开一个窗口或者另开一个ssh登录进程。执行
radtest steve test 127.0.0.1 0 testing123
                                (此步骤很重要)
此时正常情况会提示如下:
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=115, length=20 (该提示能证明r
adius服务已经开启)
step3:
centos 6.4环境下 安装完成之后的配置目录在 /etc/raddb/文件夹下
配置本地用户帐号:
vi /etc/raddb/users
               (编辑users文件,进入后按 i 进行编译)
在第一行输入test Cleartext-Password := "test" (添加帐号为test密码为test的用户,其他用户只需要
另起一行修改账户密码即可,修改完毕按esc键退出编译模式,输入:wq保存)
1 Cleartext-Password := "1"
2 Cleartext-Password := "2"
添加radius client信息:
vi /etc/raddb/clients.conf (编辑client.conf文件,进入后按 i 进行编译)
输入
client 172.20.50.253 {
 secret = h3cap
 shortname = Wireless-AP
}
client 172.20.94.241 {
 secret = h3cap
 shortname = Wireless-AP
}
client 172.20.94.180 {
 secret = h3cap
 shortname = Wireless-AP
}
其中client 172.20.50.253为AP的管理地址,可以写成网段模式代表该网段的AP,即172.20.50.0/24
其中secret = h3cap 代表ap当中与raidus server交互的密钥
其中shortname = Wireless-AP 代表作为配置的一个标记,仅用于方便记忆AP的作用,不起实际配置
作用。
(修改完毕按esc键退出编译模式, 输入: wq 保存)
step4:
关闭默认防火墙
```

关闭默认防火墙 /etc/init.d/iptables stop 开启radius 服务 service radiusd start 或者 radiusd -X 在启动服务中关闭防火墙&开启radius服务; chkconfig iptables off chkconfig radiusd on

step5: FAT AP或AC侧配置参考802.1X配合radius server典型配置

这样完成了简要的freeradius的1X认证基本配置,可以运行在虚拟机等轻量环境中,方便平时的测试或 者问题对比排查。

终端认证方式: 以上述步骤的认证方式为主; iPhone:在连入SSID时,输入帐号密码(服务器中配置的用户帐号和密码);完成之后点击信任证 书即可。 andriod:搜索到SSID,在连入SSID的时候输入账号密码,即可完成认证。 windows电脑: 以win7为例,其他系统大同小异;

每当需要连接不同的SSID名称时,都需要手动创建一个配置文件。 配置方法如下: 点击**安全类型**:选择WPA2-企业,加密类型选择AES

🚱 📶 手动连接到无线网络	ă.	
输入您要添加的表	6线网络的信息	
网络名(E):	EEI-TSG	
安全类型(S):	WPA2 - 企业	
加密类型(R):	AES 👻	
安全密钥(C):		嚴字符(H)
📄 自动启动此连接	(T)	
🔲 即使网络未进行	广播也连接(O)	
警告: 如果选择	比选项,则计算机的隐私信息可能存在风险。	
		下一步(N) 取消

点击下一步,如下图所示

~					
④! 手动道	④ ····································				
成功地》	泰加了 EEI-TSG				
•	更改连接设置(H) 可开连银屋栏以便更改设置。				
		关闭			

点击更改连接设置,如下图所示

选择网络身份验证方位为受保护的EAP(PEAP),点击安全标签:

连接 安全类型(B): WFA2 - 企业 加密类型(B): AES ▼ 边密类型(B): AES ▼ 选择网络身份验证方法(D): Microsoft: 受保护的 EAF (FEAF) ▼ 设置(S) 「加密支型のののののでのです。 ● ● 法择网络身份验证方法(D): ● ● Microsoft: 受保护的 EAF (FEAF) ▼ 设置(S) ● ● ●	EEI-TSG 无线网络属性	
安全类型 (2): WFA2 - 企业	连接安全	
安全类型(3): WFA2 - <u>企业</u> → 加密类型(3): AES → 选择网络身份验证方法(0): Microsoft: 受保护的 EAP (PEAP) → 设置(5) ☑ 每次登录时记住此连接的凭据(3) 高级设置(0)		
加密类型 00): AES	安全类型(E): ₩PA2 - 企业 ▼	
选择网络身份验证方法 (0): Microsoft: 受保护的 EAP (PEAP) ▼ 设置(S) ▼ 每次登录时记住此连接的凭据 (B) 高级设置(D)	加密类型 (M): AES 🗸	
选择网络身份验证方法 (0): Microsoft:受保护的 EAP (FEAP) → 设置 (3) ② 每次登录时记住此连接的凭据 (8) 高级设置 (0)		
Microsoft:受保护的 EAP (PEAP) ▼ 设置(S) ▼ 每次登录时记住此连接的凭据(B) 高级设置(D)	注极网络良心心证素注(n)。	
☑ 每次登录时记住此连接的凭据 (8) 高級设置 (0)	选择网络身份短趾方法 (U): Microsoft: 晉保拍的 KAP (PFAP) ▼	
高级设置 (0)	☑ 每次登录时记住此连接的凭据 (8)	
高级设置 @)		
高級设置 @)		
高级设置 (0)		
	高级设置 (0)	
	确定 取消	ן

去除勾选框"**每次登录时记住此链接的凭据**",因为客户有可能修改密码,如果修改密码修改后,这里还 是保存的以前的旧密码,这样连接无线网络就不能认证了。

EEI-TSG 无线网络属性	x
连接安全	
安全类型(Œ): ₩PA2 - 企业 ▼	
加密类型(M): AES	
选择网络身份验证方法 (1)	
Microsoft: 受保护的 EAP (PEAP) ▼ 设置(S)	
□ 每次登录时记住此连接的凭据 (8)	
高级设置 (0)	
确定	消

点击**高级设置**按钮,选择指定**身份验证模式**为:用户或计算机身份验证

高级设置	×
802.1	X 设置 802.11 设置
	】指定身份验证模式 (P):
	用户或计算机身份验证 ▼ 保存凭据(C)
	□删除所有用户的凭据(0)
	为此网络启用单一登录 (S)
	 ● 用户登录前立即执行 (2) ● 用户登录后立即执行 (7) 最大班沢(伊)(0)):
	☑ 允许单一登录期间显示其他对话框 (L)
	□该网络为计算机和用户身份验证使用单独的虚拟 LAR(V)
	<u> </u>

点击**设置**按钮,如下图所示



去除掉验证服务器证书,如下图所示

受保护的 EAP 属性
当连接时间
□ 连接到这些服务器 (0):
受信任的根证书颁发机构(B):
AddTrust External CA Root
🔲 Alibaba. com Corporation Root CA
ALIPAY_ROOT
Baltimore CyberTrust Root
China Trust Network
China Irust Network
□ 不提示用戶驗证新脈旁裔或受信任的址书授权机构 (P)。
安全密码 (EAP-MSCHAP v2) ▼ 配置 (C)
 ✓ 启用快速重新连接(F) □ 强制执行网络访问保护(M) □ 如果服务器未提供加密绑定的 TLV 则断开连接(D) □ 启用标识隐私(C)
TTm 3316

选择身份验证方法中的配置按钮,去除勾选框如下图所示:

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

点击确定返回, 创建完成。