iMC EIA无线802.1X MSCHAPv2 LDAP认证的典型配置案例

iMC 802.1X zhiliao_4Dtat 2018-08-25 发表

组网及说明

PEAP-MSCHAPv2认证类型是EAP证书认证的一种，当LDAP服务器使用Windows AD 时，LDAP用户支持EAP-PEAP-MSCHAPv2认证，本案例介绍iMC EIA无线802.1X MSCHAPv2 LDAP认证的配置方法。

本案例中iMC EIA服务器和Windows AD为同一台服务器，实际生产环境请分开部署。EIA、接入设备、Windows AD、iNode使用的版本分别如下：

iMC EIA版本为iMC EIA 7.3(E0511)

接入设备为H3C WX3540H Comware Software, Version 7.1.064, Release 5215P01

Windows AD为Windows Server 2012 AD

iNode版本为7.3(E0522)

配置前提说明：

接入设备支持802.1X协议，且与iMC EIA服务器路由可达。

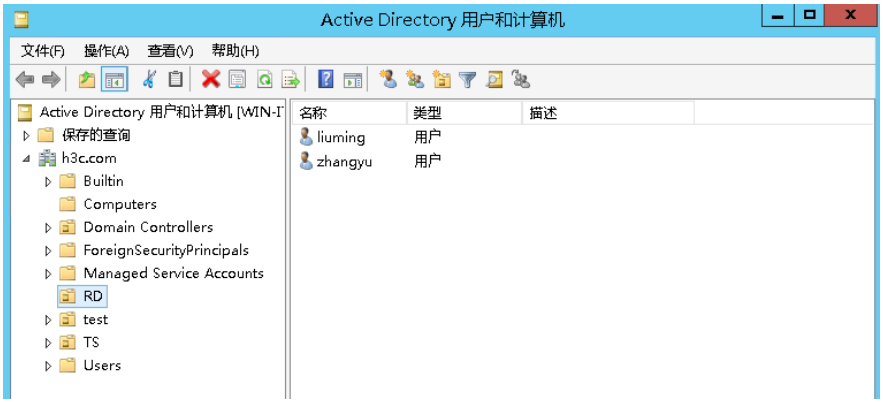
LDAP服务器为Windows AD，且与iMC EIA服务器路由可达。

相关根证书和服务器证书已申请完成。

配置步骤

1、Windows AD服务器相关配置

本案例中Windows AD命名林根域为h3c.com，在h3c.com下新建一个名为RD的组织单位，并在RD组织中新建两个用户liuming和zhangyu。



2、AC接入设备802.1X认证关键配置

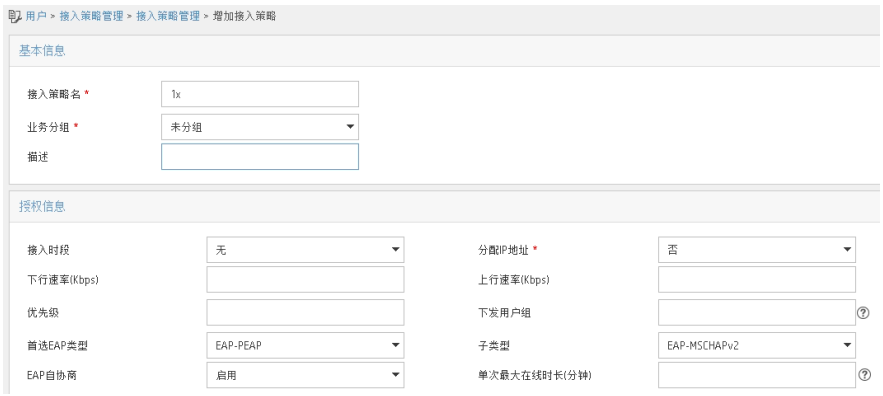
#创建认证方案1x，配置主认证/计费RADIUS服务器的IP地址为192.168.127.96，认证、计费RADIUS服务器的共享密钥为明文字符串zsf_pwd，配置设备发送RADIUS报文使用的源IP地址为192.168.127.33。

```
radius scheme 1x
 primary authentication 192.168.127.96
 primary accounting 192.168.127.96
 key authentication simple zsf_pwd
 key accounting simple zsf_pwd
 nas-ip 192.168.127.33
#创建认证域1x，配置802.1X用户使用RADIUS方案1x进行认证、授权、计费。
domain 1x
 authentication lan-access radius-scheme 1x
 authorization lan-access radius-scheme 1x
 accounting lan-access radius-scheme 1x
#配置802.1X的认证方式为EAP。
dot1x authentication-method eap
#使能radius session-control。
radius session-control enable
#创建并配置无线服务模板1x。
wlan service-template 1x
 ssid 1x
 vlan 10
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
```

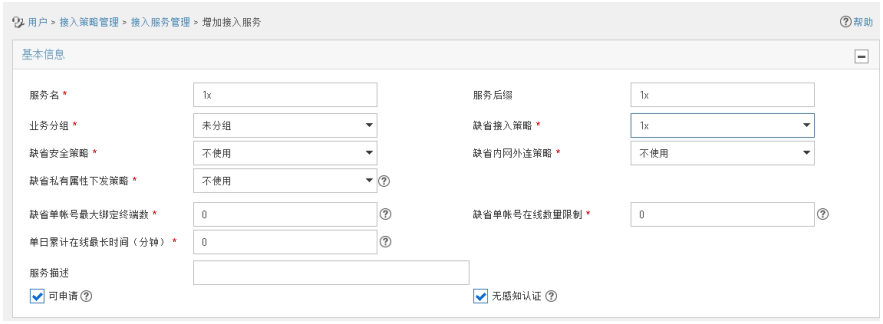
client-security authentication-mode dot1x
dot1x domain 1x
service-template enable
#将无线服务模板1x绑定到radio 1和radio 2，并开启射频。
wlan ap l2-software model WA2620i-AGN
serial-id 210235A1XXXXXX000007
radio 1
radio enable
service-template 1x
radio 2
radio enable
service-template 1x
3、iMC服务器的配置
（1）由于采用EAP-PEAP证书认证，所以iMC服务器侧需要配置根证书和服务器证书，如果客户端验证服务器的话，客户端需要安装根证书，否则客户端不需要安装任何证书。本案例客户端不验证服务器。
用户>接入策略管理>业务参数配置>证书配置，分别导入根证书和服务器证书。

注意：
EAP-PEAP认证之前请提前申请和下载证书，本案例不涉及介绍，如有问题可参考《iMC UAM证书使用指导》。
（2）用户>接入策略管理>接入设备管理>接入设备配置，增加接入设备192.168.127.33。

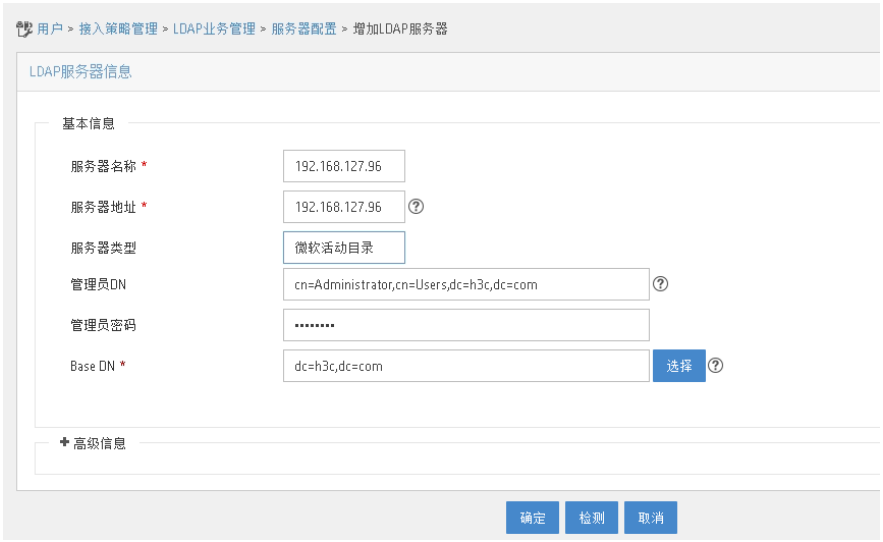
注意：
增加的接入设备IP需要和认证设备radius scheme下的nas-ip一致，共享密钥需要和radius scheme下的认证、计费radius服务器的密钥一致。
（3）用户>接入策略管理>接入策略管理，增加接入策略1x，首选EAP类型选择EAP-PEAP，子类型选择EAP-MSCHAPV2，其他参数保持缺省即可。



（4）用户>接入策略管理>接入服务管理，增加接入服务1x，服务后缀配置为认证设备上的domain域名1x，缺省接入策略选择1x。

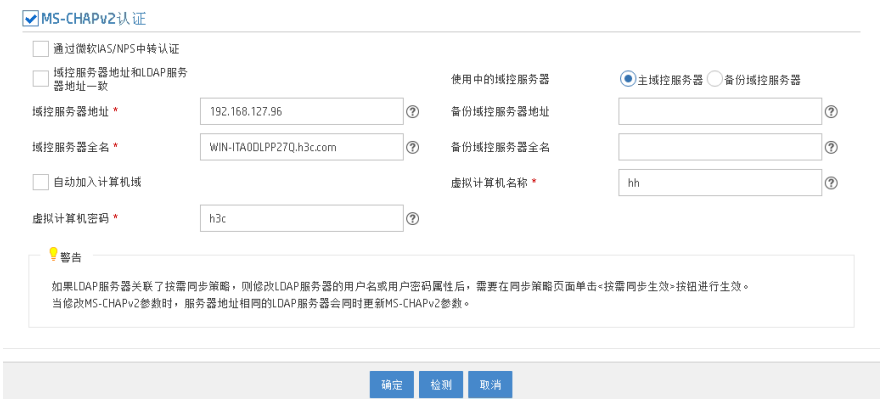


（5）用户>接入策略管理>LDAP业务管理>服务器配置，增加LDAP服务器。



管理员DN为cn=Administrator,cn=Users,dc=h3c,dc=com，管理员密码为Administrator的密码，Base DN为dc=h3c,dc=com，其他参数可根据实际需求配置。

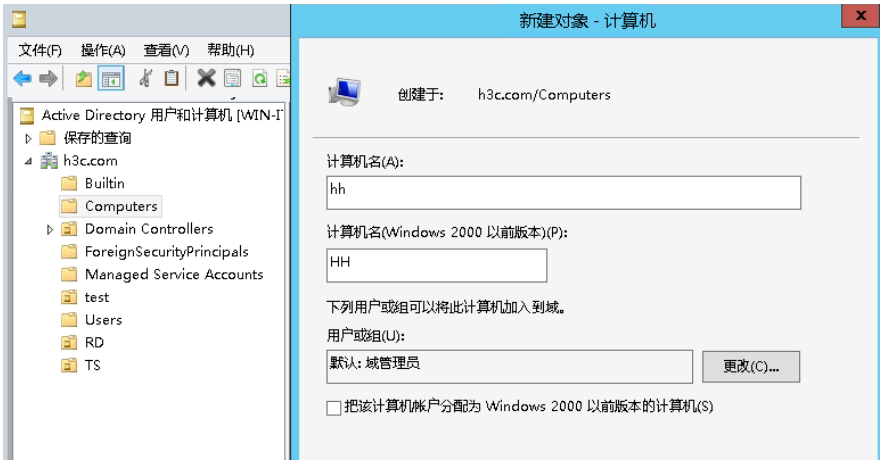
高级信息中启用MS-CHAPV2认证，虚拟计算机名称本案例命名为hh，虚拟机计算机密码为h3c：



（6）在Windows AD服务器上新建虚拟计算机。

在h3c.com下右键Computers选择新建计算机，其中计算机名和iMC服务器上的虚拟计算机名称保持一

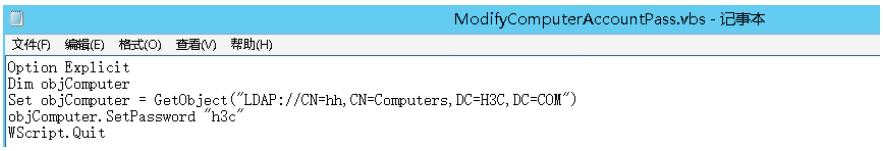
样为hh：



（7）给新建的虚拟计算机设置密码。

设置虚拟机计算机密码需要运行一个脚本程序ModiComputerAccoutPass.vbs，该脚本程序从用户>接入策略管理>LDAP业务管理>参数配置页面点击修改计算机密码脚本的下载链接获取：

下载计算机密码脚本程序到本地，使用文本编辑器打开该文件，将CN=testAccount,CN=Computers,DC=CONTOSO,DC=COM替换为虚拟计算机帐号DN，本例中DN为CN=hh,CN=Computers,DC=h3c,DC=com，将iMC123替换为虚拟计算机密码h3c：



将修改之后的计算机密码脚本程序拷贝到AD域控服务器，打开命令行窗口，cd进入脚本程序所在路径，执行cscript ModifyComputerAccountPass.vbs使重置后的虚拟计算机密码生效。

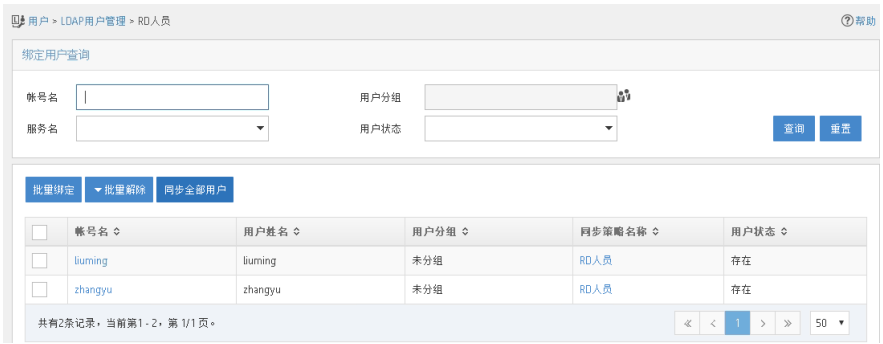
（8）用户>接入策略管理>LDAP业务管理>同步策略配置，增加LDAP同步策略。

同步Windows AD服务器h3c.com下组织RD的用户，所以子BaseDN为ou=RD,dc=h3c,dc=com，其他参数本案例保持为缺省选项。

在其他信息配置页面，在接入信息区域，输入密码h3c,当LDAP用户解除与LDAP服务器的绑定关系后作为iMC接入用户使用该密码可以通过认证。在接入服务区域分配接入服务1x。

（9）LDAP服务器同步策略配置完成后，在同步策略列表中，点击"同步"链接，手动同步LDAP用户。

同步成功之后，在同步策略列表中点击"LDAP用户"链接可以查看同步成功的LDAP用户信息：



4、客户端配置

（1）iOS客户端使用liuming@1x拨号认证测试

无线局域网中连接SSID信号1x，输入用户名liuming@1x和密码，点击加入：

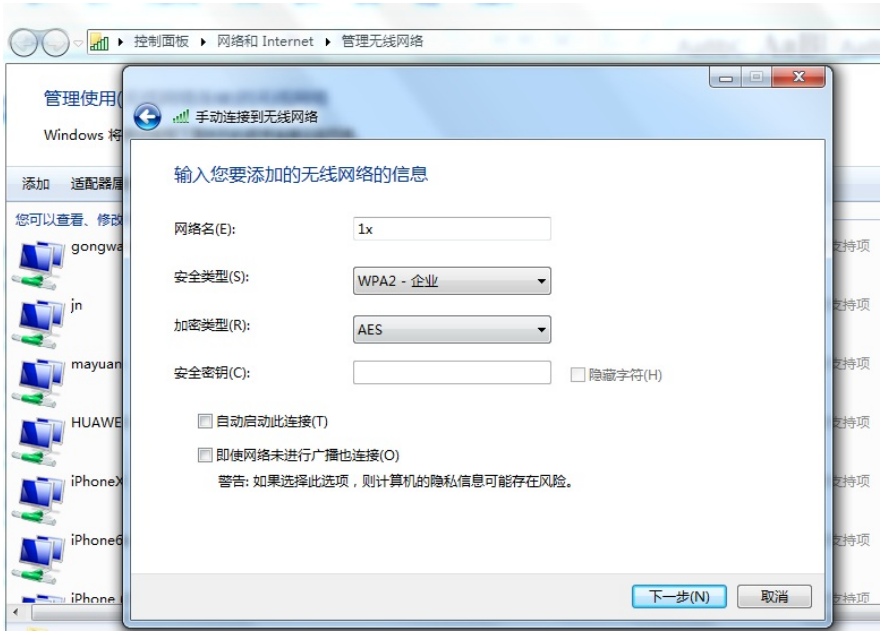
点击信任证书：

连接成功：

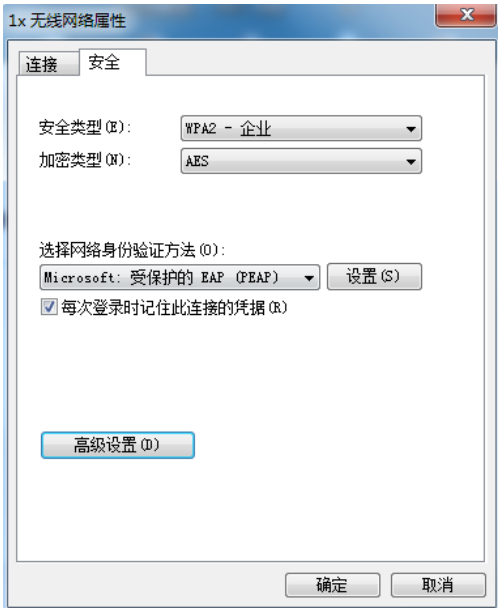
在iMC服务器上可以查到到终端的在线信息：

（2）Windows 7电脑终端使用zhangyu拨号认证测试

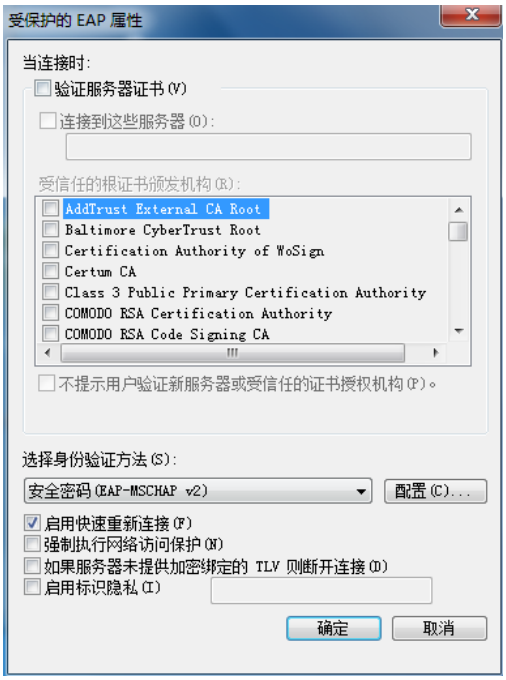
管理无线网络下手动添加SSID 1x的无线网络连接：



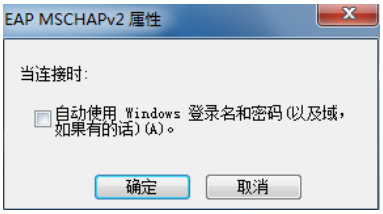
手动添加无线网络连接后，右键设置属性：



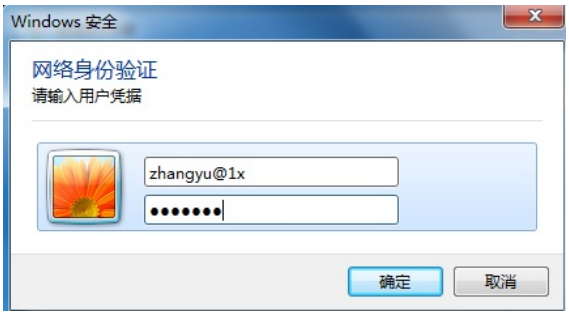
网络身份验证方法选择受保护的EAP（PEAP），点击设置，这里不验证服务器证书，所以去勾选“验证服务器证书”：



身份验证方式选择EAP-MSCHA V2，点击配置，属性去勾选“自动使用Windows登录名和密码（以及域，如果有的话）”：



设置无线网络连接属性后，连接信号1x，弹出的网络身份验证框中输入用户名zhangyu@1x和密码认证上线：

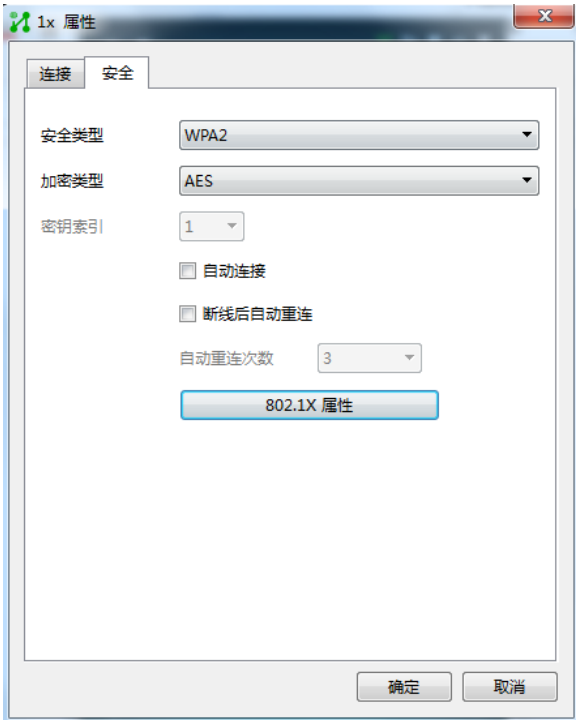


在iMC服务器上可以查看到终端的在线信息：

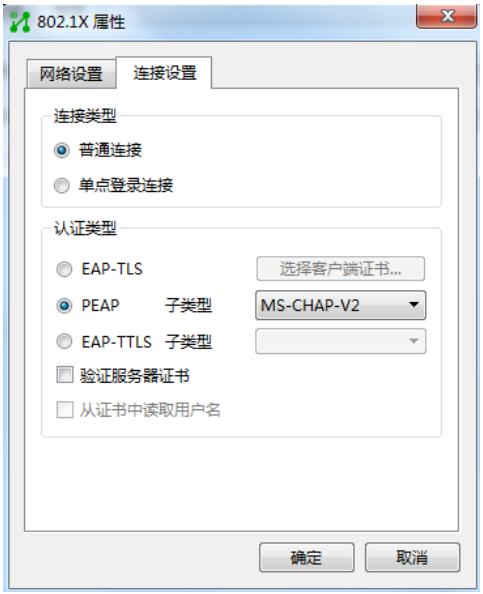
（3）iNode客户端

打开iNode客户端，右上角无线图标选择使用iNode管理无线，然后选择无线网络SSID信号1x：

点击连接旁边的下拉选项选择属性进行设置：



点击802.1X属性进行设置，认证类型选择PEAP，子类型选择MS-CHAP-V2，不勾选验证服务器证书：



输入用户名liuming@1x和密码，点击连接开始认证：

连接成功：

在iMC服务器上可以查看到终端的在线信息：

配置关键点