

知 iMC EIA无线802.1X MSCHAPv2 LDAP认证双机备份的典型配置案例

802.1X LDAP 802.1X zhiliao_AgjTC 2018-12-28 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。当主域控服务器无法正常工作时（例如：主域控服务器重启或断网等连通性错误），iMC会自动切换到备份域控服务器进行认证，整个切换过程约1分钟，在此期间用户无法通过认证。直到备份域控服务器无法正常工作时，iMC才会自动切换到主域控服务器进行认证。支持通过手工修改“使用中的域控服务器”参数以切换主备域控服务器的工作状态。

本案例介绍iMC EIA无线802.1X MSCHAPv2 LDAP认证双机备份的配置方法。

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(E0505)

接入设备为H3C WX3010H-X Comware Software, Version 7.1.064, Release 5208p03

Windows AD为Windows Server 2008 R2 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。

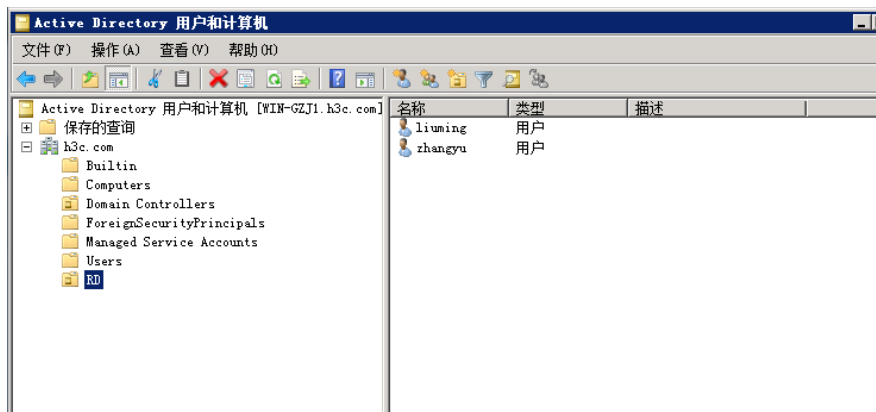
LDAP服务器为Windows AD，且与iMC EIA服务器路由可达。

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zhang。



同时在备用域控服务器中的h3c.com下新建一个同样的名为RD的组织单位，并在RD组织中创建相同的两个用户liuming和zhangyu（两个账户的密码也与主域控服务器中设置的相同）。

2、AC接入设备802.1X认证关键配置

1、#创建认证方案1x，配置主认证/计费RADIUS服务器的IP地址为192.168.113.126，认证、计费RADIUS服务器的共享密钥为明文字符串admin，配置设备发送RADIUS报文使用的源IP地址为192.168.205.1。

radius scheme 1x

primary authentication 192.168.113.126

primary accounting 192.168.113.126

key authentication simple admin

key accounting simple admin

nas-ip 192.168.205.1

#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gzj。

wlan service-template gzj

```
ssid 1x
vlan 500
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gzj绑定到radio 1和radio 2，并开启射频。
wlan ap lh-test model WA4320-CAN-SI
serial-id 219801A0T78166E00247

radio 1
radio enable
service-template gzj vlan 500

radio 2
radio enable
service-template gzj vlan 500
```

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。若无特殊安全需求或在测试环境使用，可以直接在页面点击“导入预置证书”按钮，导入iMC EIA内置的证书文件。

用户 > 接入策略管理 > 业务参数配置 > 证书配置

证书文件校验 已导入证书校验 导入预置证书

提示
同一种类型的服务器证书只能上传一个。

根证书配置 服务器证书配置

导入EAP根证书 导入WAPI根证书

颁发者	主题	类型	动作
CN=GeoTrust Global CA,O=GeoTrust Inc.,C=US	CN=GeoTrust SSL CA - G3,O=GeoTrust Inc.,C=US	EAP根证书	  

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192.168.205.1。

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

接入配置

认证端口 *	1812	计费端口 *	1813
业务类型	不限	强制下线方式	断开用户连接
接入设备类型	H3C (General)	业务分组	未分组
共享密钥 *	*****	确认共享密钥 *	*****
接入位置分组	无		

设备列表

选择 手工增加 全部清除

设备名称	设备IP地址	设备型号	备注	删除
WX3010H-X	192.168.205.1	H3C WX3010H-X		

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。

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 *

1x

业务分组 *

未分组

描述

授权信息

接入时段

无

分配IP地址 *

否

下行速率(Kbps)

上行速率(Kbps)

优先级

下发用户组

首选EAP类型

EAP-PEAP

子类型

EAP-MSCHAPV2

EAP自协商

启用

单次最大在线时长(分钟)

下发地址池

下发VLAN

☐ 下发User Profile

下发VSI名称

☐ 下发ACL

(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。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 *

1x

服务后缀

1x

业务分组 *

未分组

缺省接入策略 *

1x

缺省安全策略 *

不使用

缺省内网外连策略 *

不使用

缺省私有属性下发策略 *

不使用

缺省单帐号在线数量限制 *

0

缺省单帐号最大绑定终端数 *

0

单日累计在线最长时间(分钟) *

0

服务描述

☒ 可申请

☒ 无感知认证

接入场景列表

(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。

用户 > 接入策略管理 > LDAP业务管理 > 服务器配置 > 增加LDAP服务器

LDAP服务器信息

基本信息

服务器名称 *

192.168.113.132

服务器地址 *

192.168.113.132

服务器类型

微软活动目录

管理员DN

cn=Administrator,cn=Users,dc=h3c,dc=com

管理员密码

Base DN *

dc=h3c,dc=com

选择

高级信息

确定

检测

取消

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 其他参数根据需求配置。

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。因为本案例中同时配置了主域控服务器以及备份域控服务器，因此主备域控服务器的地址和全名均需要填写：

☒ MS-CHAPv2认证

☐ 域控服务器地址和LDAP服务器地址一致

域控服务器地址 *

192.168.113.132

备份域控服务器地址

192.168.113.136

域控服务器全名 *

WIN-GZJ1.h3c.com

备份域控服务器全名

WIN-GZJ2.h3c.com

虚拟计算机密码 *

...

确认虚拟计算机密码 *

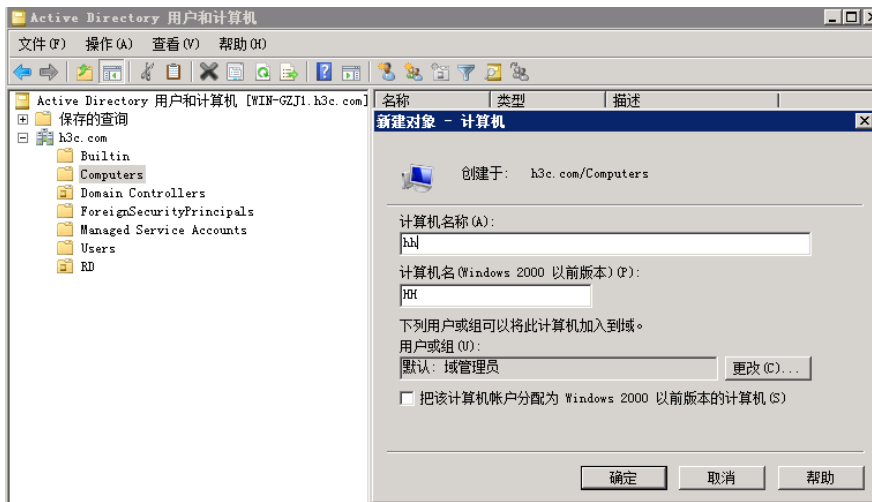
...

虚拟计算机名称 *

hh

(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致为hh，备机也在相同的路径下创建名称密码一致的虚拟计算机：



(7) 给新建的虚拟计算机设置密码。

设置虚拟计算机密码需要运行一个脚本程序ModiComputerAccountPass.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：

```
Option Explicit
Dim objComputer
Set objComputer = GetObject("LDAP://CN=hh,CN=Computers,DC=h3c,DC=com")
objComputer.SetPassword "h3c"
WScript.Quit
```

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。

```
C:\Users\Administrator\Desktop>cscript ModifyComputerAccountPass.vbs
Microsoft (R) Windows Script Host Version 5.8
版权所有 (C) Microsoft Corporation 1996-2001。保留所有权利。
```

(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。

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

增加LDAP同步策略

同步策略名称 *	RD人员
服务器名称	192.168.113.132
业务分组	未分组
同步优先级 *	1
Base DN	dc=h3c,dc=com
子BaseDN *	ou=RD,dc=h3c,dc=com
过滤条件 *	(&(objectclass=user)(sAMAccountName=*)(accountExi
状态 *	有效
同步的用户类型	☒ 接入用户 ☐ 设备管理用户
同步选项	☒ 自动同步 ☐ 按需同步 ☒ 新增用户及其接入帐号 ☒ 为已存在用户新增接入帐号 ☐ 仅同步当前节点下的用户 ☒ 过滤计算机帐号

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。

帐号名 *	sAMAccountName	
失效时间	不从LDAP服务器同步	信息
密码	不从LDAP服务器同步	...
最大闲置时长(分钟)	不从LDAP服务器同步	
在线数量限制	不从LDAP服务器同步	1
登录提示信息	不从LDAP服务器同步	

(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。

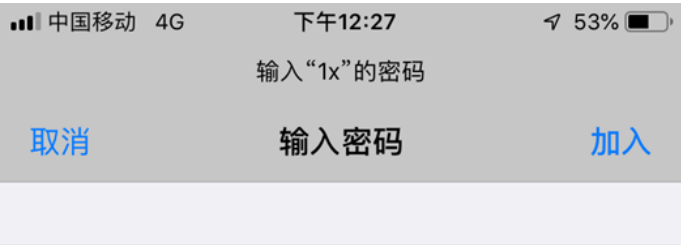
同步策略名称	服务器名称	同步的用户类型	业务分组	状态	同步优先级	按需同步	LDAP用户	同步	修改	删除
RD人员	192.168.113.132	接入用户	未分组	有效	1	否	liuming	同步	修改	删除

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：

liuming	liuming	未分组	RD人员	存在
zhangyu	zhangyu	未分组	RD人员	存在

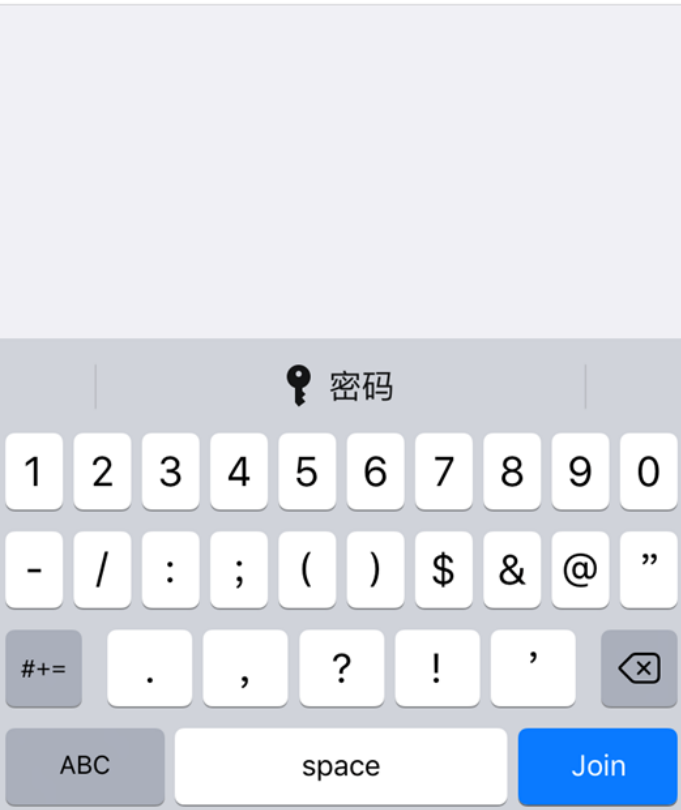
4、客户端配置

(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：



用户名 [liuming@1x](#)

密码 ●●●●●●●●●●



点击信任证书：

取消

证书

信任



imc.h3c.com

签发者: GeoTrust SSL CA - G3

不可信

过期日期 2019/7/14 上午7:59:59

更多详细信息

>

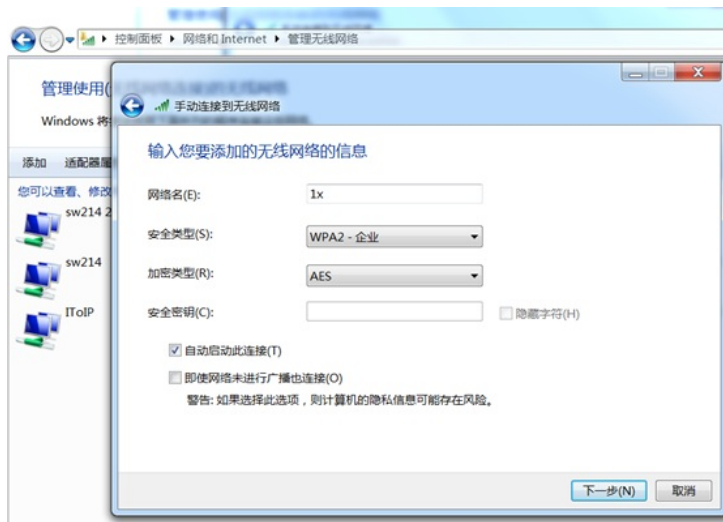
连接成功:



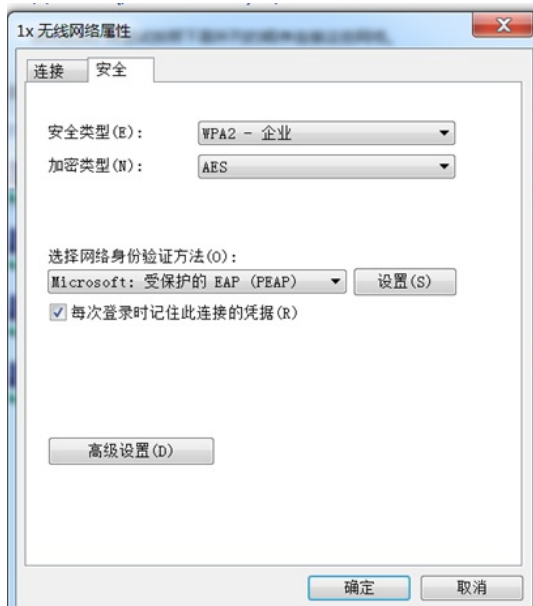
在iMC服务器上可以查看到终端的在线信息：



(2) Windows7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：



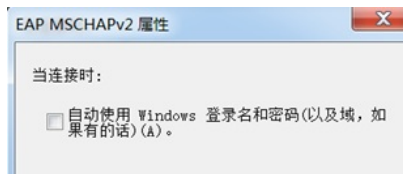
手动添加无线网络后，右键设置属性：



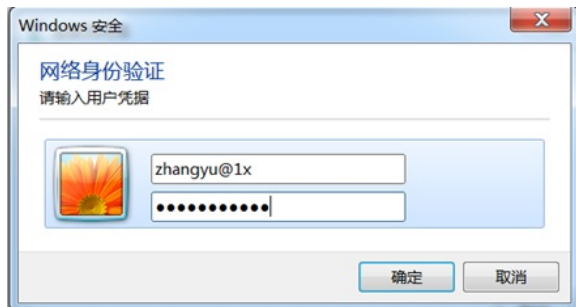
网络身份验证方法选择受保护的EAP（PEAP），点击设置，这里不验证服务器证书，所以去勾选“验证服务器证书”：



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：



上线成功后，可以在iMC服务器上查看到终端的在线信息：

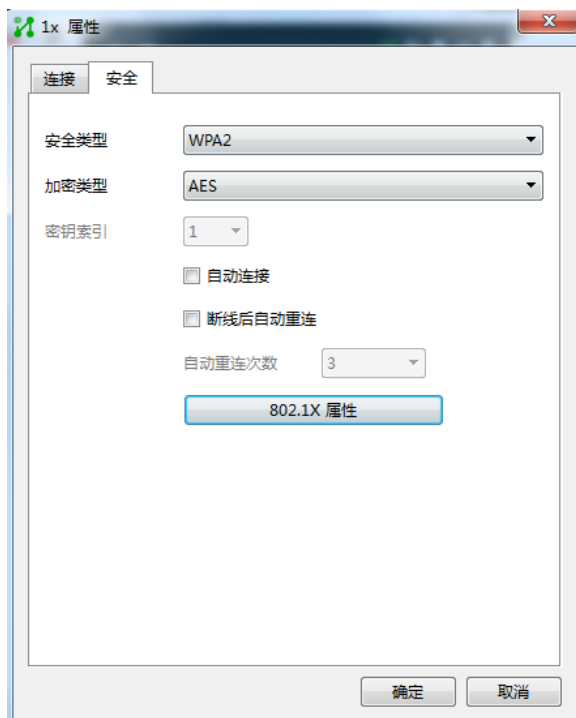


(3) iNode客户端

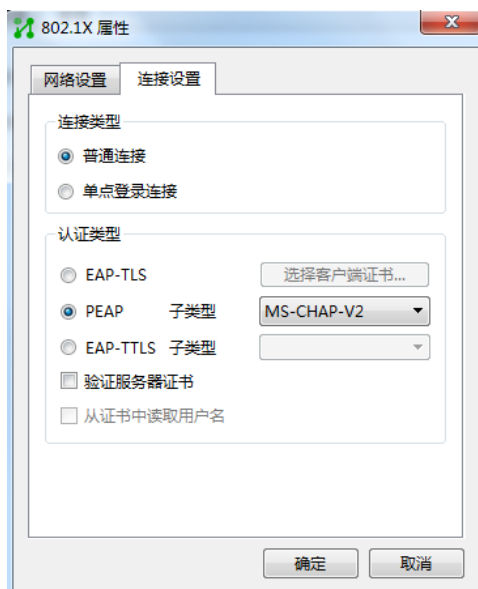
打开iNode客户端，右上角无线图标选择使用iNode管理无线，然后选择无线网络SSID信号1x：



点击连接旁边的下拉选项选择属性进行设置：



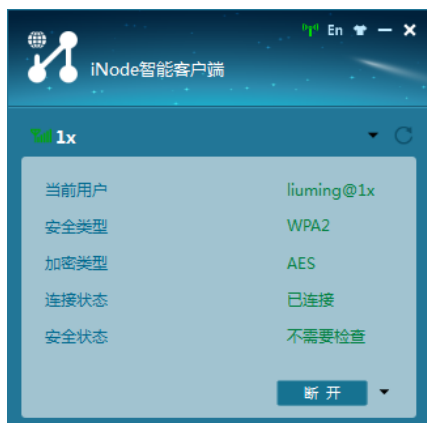
点击802.1x属性进行设置，认证类型选择PEAP，子类型选择MS-CHAP-V2，不勾选验证服务器证书：



输入用户名liuming@1x和密码，点击连接开始认证：



连接成功：



配置关键点