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192.168.127.3 3。

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 I2-software model WA2620i-AGN serial-id 210235A1XXXXX000007 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。

户 > 接入策略管理 > 业务参数配置 > 证	书配置				Ċ
书文件校验 已导入证书校验 导入;	项置证书				
♥提示 同一种类型的服务器证书只能上传一个	0				
根证书配置 服务器证书配置					
导入EAP服务器证书 导入WAPI服务器	译证书				
領发者 \$	主题 ♦	类型 \$	有效起始时间 \$	有效终止时间 \$	动作
CN=GeoTrust SSL CA - G3,D=GeoTrust	CN=imc.h3c.com,0=Hangzhou H3C Technologies Co. Ltd	EAP服务器证书	2016-07-13	2019-07-14	0

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。

🗗 用户 > 接入策略管理 > 接	(用户> 接入嶺略管理> 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 *	zsf_pwd								
摘入位置分组	无	•							
辺々対象									
反面列权									
选择 手工增加	选择 手工增加 全部清除 <mark>请单击下方的"确定"按钮完编配置。</mark>								
设备名称	设备IP地址	设备型号	备注	删除					
WX3540H	192.168.127.33	H3C WX3540H		Ô					

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。

即用户>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	•	分配印地址 *	否	•
下行速室(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)		?

(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。

本信息					
服务名 *	1x		服务后缀	1х	
Ł务分组*	未分组	•	缺省接入策略*	1x	•
* 省安全策略	不使用	-	缺省内网外连策略*	不使用	-
电省私有属性下发策略 *	不使用	• ?			
管单帐号最大绑定终端数 *	0	?	缺省单帐号在线数量限制*	0	?
1日累计在线最长时间(分钟) *	0	?			
服务描述					
✔ 可申请 ⑦			✔ 无感知认证 ⑦		

(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。

服务器信息		
基本信息		
服务器名称 *	192.168.127.96	
服务器地址 *	192.168.127.96 🕐	
服务器类型	徽软活动目录	
管理员DN	cn=Administrator,cn=Users,dc=h3c,dc=com	0
管理员密码]
Base DN *	dc=h3c,dc=com	选择 ?
高級信息		

管理员DN为cn=Administrator,cn=Users,dc=h3c,dc=com,管理员密码为Administrator的密码,BaseDN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:

通过微软IAS/NPS中转认证					
域控服务器地址和LDAP服务 器地址一致			使用中的域控服务器	●主域控服务器 ● 备份域控服务器	
或控服务器地址 *	192.168.127.96	?	备份域控服务器地址		?
《控服务器全名 *	WIN-ITA0DLPP27Q.h3c.com	?	备份域控服务器全名		?
自动加入计算机域			虚拟计算机名称 *	hh	?
虚拟计算机密码 ★	h3c	?			
♀警告 如果LDAP服务器关联了按需同 当修改MS-CHAPv2参数时,服	步策略,则修改LDAP服务器的用户名 务器地址相同的LDAP服务器会同时更	或用户密码 新MS-CHAP、	属性后,需要在同步策略页面单 12参数。	击<按需同步生效>按钮进行生效。	

(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

	新建对象 - 计算机	x
文件(F) 操作(A) 查看(V) 帮助(H) ◆ → 2 〒 4 1 ※ □ 0 2 Active Directory 用户和计算机 (WIN-I ▷ □ 保存的音询	业 创建于: h3c.com/Computers	
⊿ ∰ h3c.com	计算机名(A): hh	
Computers ▷ 3 Domain Controllers ForeignSecurityPrincipals	计算机名(Windows 2000 以前版本)(P):	
Managed Service Accounts	HH 下列用户或组可以将此计算机加入到域。	
Users	用户或组(U):	
a 15	▲//// 兆日/主以 □把该计算机帐户分配为 Windows 2000 以前版本的计算机(S)	

(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:

● 用户 > 接入策略管理 > LDAP业务管理 > 参数配置	於 加入場	₹菴 ⑦帮助
LDAP功能参数		
基本参数		
LDAP按需认证模式	本地备份 🔻 ?	
LDAP服务器故障时逃生	禁用 ▼ ⑦	
LDAP主备机切换发送告警	禁止 • ⑦	
MSCHAPv2 Server日志级别	警告 ▼	
修改计算机密码脚本	http://192.168.127.96:8080/imc/peapPasswordScript?fileName=ModifyComputerAccountPass.vbs	

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:





(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 > L	DAP业务管理 > 同步策略配置 > 增加LDAP同步策略	
增加LDAP同步策略		
		1
同步策略名称*	RD人员	
服务器名称	192.168.127.96	
业务分组	未分组	
同步优先级 *	1	0
Base DN	dc=h3c,dc=com	
子BaseDN *	ou=RD,dc=h3c,dc=com	0
过滤条件 *	(&(objectclass=user)(sAMAccountName=*)(accountExpires>=n	
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。

无线SS	ID	不从LDAP	服务器同步 🔻			
设备序	列号	不从LDAP	服务器同步 🔻			
Windov	vs 域	不从LDAP	服务器同步 🔻			
接入周	服务					
	服务名		服务后缀	状态	缺省安全策略	分配IP地址
	zsf_por_se_gu			可申请	不使用	
	1х		1х	可申请	不使用	
_	第7 十					
系该	◎ 晉吉 - 鏡中存在同步策略后,请不要 - 情况,需要管理员手工修改LC	在"用户>用 IAP同步策略	i户附加信息"页面进行增加、册 ,重新设置同步附加信息,并	则除、修改用户附加信息的 将同步策略改为有效状态	的操作,否则将导致系统中已存在的同步锁 。接入设备绑定信息支持多值绑定,多值	'鹂变为无效状态。一旦发生 之间使用"I"分隔。
			Ŀ	一步 完成 取消		

(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。

AP同步策略查询										
同步策略名称			服务	器名称			•			
用户分组		ůŶ	前 同步的	的用户类型			•			
业务分组		•								间重
业务分组 常加 按票同步当 可步策略名称 ▲	<u>服</u> 券署名称	▼ 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	前里

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:

■月戸>し	DAP用户管理 > RD人员				⑦帮助
绑定用户	查询				
帐号名		用户分组		ů۵	
服务名		▼ 用户状态		•	查询 重置
批量绑	定 ▼批里解除 同步全部用户				
	帐号名 ≎	用户姓名 \$	用户分组 \$	同步策略名称 ≎	用户状态 \$
	liuming	liuming	未分组	RD人员	存在
	zhangyu	zhangyu	未分组	RD人员	存在
共有2	条记录,当前第1-2,第 1/1页。			« <	1 > » 50 v

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<u>liuming@1x</u>和密码,点击加入:

15:47 🕫	, 11 4 G 🗩
输入"1>	《"的密码
取消 输入	、密码 加入
用户名 liuming@1x	
密码 •••••	
模式	自动 >
话信任证书:	
15:47 🕫	. 11 4G 🔳
取消 证	书 信任
imc.h3c.com 签发者: GeoTrust	t SSL CA - G3
不可信	
过期日期 2019/7/14 07:59:	59
更多详细信息	>
接成功:	
15.18 4	
10-40 7	.111 46 🔳
く 设直 大线)	司戏网
7.1%/可线网	
✓ IX	■ ~ (]
选取网络	
ааа	₽ 중 (j
BYOD	₽ ? ()
cxc_portal	? ()
DIRECT-8A-HP Office.	Jet Pro 8720 🔒 훅 🪺
H3C	

在iMC服务器上可以查到到终端的在线信息:

💁 用户 > 在线用户									参 加入地	(權)
本地在线用户	漫游在线用户	设备在线用	<u>ج</u> ر							
本地在线用户查询									Ē	服查证
帐号名]	用户姓名					
用户IP地址 从					至					
用户分组				ů ⁹ 🗇					查询	重置
消息下发 强制	下线 清除在线	規信息 重认证	定制界	『面 批量导出						
● 帐号名 \$	登录名 \$	用户姓名 ≎	服务名	接入时间 ≎	接入时长 \$	设备IP地址 ≎	用户⊮地址 ≎	安全状态 🗘	客户端定制时间 \$	操作
liuming	liuming@1x	liuming	1x	2018-07-23 15:32:16	0秒	192,168,127,33	192.168.127.44	无需安全认证		

(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:

00-11.	控制面板 🕨 网络和 Internet 🕨	管理无线网络	
管理使用(Windows 将	🚱 📶 手动连接到无线网络		
添加 适配器属	输入您要添加的无线	网络的信息	
您可以查看、修改	网络名(E):	lx	支持项
	安全类型(S):	WPA2 - 企业	
, jn	加密类型(R):	AES 🔹	支持项
mayuan mayuan	安全密钥(C):	□	支持项
HUAWE	自动启动此连接(T)		支持项
iPhoneX	即使网络未进行广播 警告:如果选择此选	祂连接(O) 项,则计算机的隐私信息可能存在风险。	支持项
2			
iPhone6			支持项
I iPhone		下—步(N) 取消	5持顶

手动添加无线网络连接后,右键设置属性:

1x 无线网络属性		X
连接安全		
安全类型(8):	₩PA2 - 企业 👻	
加密类型(N):	AES 🔹	
	-14 /->	
选择网络身顶短距方	」法(U): 100 pup (npup)	
microsoft.安休护		
▶ 9八豆水町16日		
方の辺里の)	-	
高級役置の		
	确定即	消

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)":

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

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:

Windows 安全			X
网络身份验请输入用户凭损	证 g		
	zhangyu@1x		
		确定	取消

在iMC服务器上可以查看到终端的在线信息:

月户 > 在纸用户 ★加入收量 ⑦										
本地在线用户 漫游在线用户 设备在线用户										
我用户查询									á.	級查道
1					用户姓名					
地址 从					至					
组				ů ⁹ 🗇					查询	重贵
「发 强制」	下线 清除在約	能信息 重认证	定制界	『面 批量导出						
帐号名 ≎	登录名 ≎	用户姓名 ≎	服务名	接入时间 ≎	擴入时长 \$	设备IP地址 ≎	用户IP地址 ≎	安全状态 \$	客户端定制时间 \$	操作
zhangyu	zhangyu@1x	zhangyu	1x	2018-07-23 15:26:32	0秒	192,168,127,33	192.168.127.42	无需安全认证		
zhangyu	zhangyu@1x	zhangyu	1x	2018-07-23 15:05:41	12分钟0秒	192,168,127,33	192.168.127.44	无需安全认证		
	Etabler E我用户畫诲 地址从 组 来号名 ≎ zhangyu zhangyu	は SUDY (は低的ゲ (銘用户) 漫游在鉄用户 没当在线用 利用庁壹询 地址 从	(鉱用户	議員戶戶 選事在线用戶 设备在线用戶 須用戶壹询 建 通 建 第6年54 ◆ 登录名 ◆ 用戶姓名 ◇ 原分名 推出 zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x zhangyu@ 1x	議員戶 兼報在採用户 设备在採用户 採用戶畫海 第 第 # # #	議員内内 選書在採用户 设备在採用户 採用庁査询 第 ・	1 2	(諸田内) 満井在採用户 设备在採用户 (講用戸査询) (湯二女(田内)) (湯二女(田内)) (□	第本在线用户 漫畫在线用户 设量在线用户 3月戸雪山 第本在线用户 3月戸雪山 月戸雪山 3日 第月第年在线目 3日 第日月 3日 第日月 3日 第日月 3日 第日月 3日 第日月 3日 第日月 3日 第日 3日

(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:

	┣ᠠd En ♥ — ★ Node智能客户端
Ÿ≣ 1x	• C
用户名	
密码	
域	~
✓ 保存	評用户名 🔽 保存密码
	连接 ▼

点击连接旁边的下拉选项选择属性进行设置:

<mark>/</mark> 1x 属性	
连接 安全	
安全类型	WPA2
加密类型	AES 🗸
密钥索引	1 -
	🗌 自动连接
	📄 断线后自动重连
	自动重连次数 3 🔻
	802.1X 属性
	确定取消

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:

21 802.1X 属性	×
网络设置连接设置	
连接类型	
 普通连接 	
◎ 单点登录连接	
─认证类型	
C EAP-TLS	选择客户端证书
◎ PEAP 子类型	MS-CHAP-V2 -
◎ EAP-TTLS 子类型	
□ 验证服务器证书	
□ 从证书中读取用户名	
	确定 取消

输入用户名<u>liuming@1x</u>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:

<u>6</u>	用户;	在线用户									★ 加入收	₩ (? A		
[本地	在线用户	漫游在线用户	设备在线师	户									
	本地在线用户查询									高级重				
	帐号:	2					用户姓名							
	用户	⁰地址 从					至							
	用户分组				ů ¹ 🗇					查询	重置			
	消息	下发 强制	下线 清除在	线信息 重认计	E 定制	界面 批量导出								
		帐号名 ≎	登录名 ≎	用户姓名 \$	服务名	接入时间 ≎	接入时长 \$	设备IP地址 ≎	用户⊮地址 ≎	安全状态 \$	客户端定制时间 \$	操作		
		liuming	liuming@1x	liuming	1x	2018-07-23 15:03:05	0秒	192,168,127,33	192.168.127.42	无需安全认证	2018-07-23 10:12:21			
	共有	[1条记录,当	前第1-1,第	1/1页。						« <	1 > > 50	•		
配	雪关	键点												