LDAP iNode **寻尚岩** 2012-11-22 发表

iMC UAM MsChapV2 LDAP认证的典型配置

一、组网需求:

安装有iNode的客户端通过接入设备连接至iMC:

1. 接入设备将客户端发出的认证请求报文发往UAM,UAM根据用户帐号查得该用户需要进行 MsChapV2 LDAP认证;

2. UAM为该用户提交一个请求报文给mschapv2server.exe进程,后者再转交给域控服务器;

3. 域控服务器根据用户信息决定用户是否能认证通过,然后再将认证结果经由mschapv2server.exe进程返交给UAM;

4.UAM将认证结果通过接入设备返回给客户端。

说明: MsChapV2 LDAP认证方式是从iMC UAM 3.60-E6209才有的新特性。

二、组网图:

UAM MsChapV2 LDAP认证组网如图2-1所示



2.iMC侧配置:

(1):由于采用F 务器的话,需要	PEAP证书认证,所以服务器侧必 安装根证书,否则不需要安装任	%须安装根证书和服务器证书,客户端验证服 何证书。本案例客户端不验证服务器;
将从CA服务器中	中下载的根证书和服务器证书导入	、到iMC中(下载过程略):
业务-用户接入管	管理-业务参数配置-证书配置-动作	F, 如图3-1所示;
國 业务 >> 用户格入管理 >> 1	2为参数起置 >> 证书配置	
证书R2团列表 [19]110-2312	5.6	2440
EAPERAT	基于EAP推入方式的证书配置	0.00
WAPIER	基于WAPI接入方式的证书做置	
图3-1 点击浏览,找到林	艮证书文件,然后点击下一步, 如[图3-2所示;
	CRL教室 >> 1.服务器证书教室 >> 4.服务器证书机据密码 >> 6.证书教室给	2HE 0316
根证书配置		
模运书文件	C 3Users Administrator Downloads kertnew.cer	
	mbacabbie的。 やけら出生 name can. Autoute的。 やけら出生 name ca	· niest3niget118月、空体局性やysig n17。注意· NETILEFEndEr, N
不支持如何超过的私貌文件。	unneeden Sienen Sienen heude een een een seine Sienen on de re	A final at the state of the
	<u></u> ₹-\$	
图3-2		
保持默认值, 点:	击下一步, 如图3-3;	
读 证书配置 1. 供证书配置 >> 2	. CRL配置 ≫3.服务書证书配置 ≫4.服务書证书私辦密約 ≫5.证书	R.医鼠总网络
CRLRE		
 ・ 倉用CRL定时更新 ● 原始方式 		
更新闻期(1-30)		
更新时间(0-23)	et	
利接		
	上一步 测试的接 7	-# BA
图3-3 如图3-4所示 点击 务器证书和私钥径	示浏览,找到从IE里面导出的服务器 王同一文件,单击下一步;	¥证书(与根证书同一CA机构颁发),勾选服
● 毫特配置 1. 使更长配置 >> 2.	CIL报告 >> 3.服务書证书配置 >> 4.服务書证书私留書档 >> 5.证书配	549HS
の言葉を言語书 「「「「「「「「」」」、「」」、「」、「」、「」、「」、「」、「」、「」、「」、		
服务器证书文件	CitUsersiAdministrator/Desidoplserver-imc.pfx]
● ■C支持的服务营运书文件格式为 即C支持的服务营运书文件格式为	:pern/baseE4边编码,文件后提为pern或cer(),der(ded编码,文件后提为 d	er或.cer),pkcs12(pkcs12)编码,文件后因为pdig_p12)。注意:如果证书格式是pdMagg
	<u>L-9</u> T-9	EA.
图3-4		
输入之前创建的积	公钥密码;	
读书配置 1. 供证书配置 >> 2.	CPL程置 >> 3.服务器证书程置 >> 4.服务器证书权切密有 >> 5.证书程器	1.11 (A)
服务器和银密的		
服务器私销密码	•••	
	上一步	RA
图3-5		
占土协会 天山		
点击确定,至此引 所示;	双们任IMG侧守八了 依亚节和服务者	都正书,ⅢUC具有了证书从证的能门, 纵图3-0
建书配置 1.根证书配置 >>	2.CRL就置 >> 3.服务器证书配置 >> 4.服务器证书私钥密码 >> 5.	正书配置能意形态
证书配置信息任范		
根证书颁发者	CN=ca	
服务書证书主题 服务書证书有效起始时间	cnl=imc-server,C=CN 2012-10-24	
服务書証书有效终止时间	2013-10-24	
电19时时为表型数方式	 上一步	27A
图3-6		
200		

(2):新建服务chapv2ldap,后缀为之前新建的域dot1x,认证类型选择EAP-PEAP认证,点击确定,**如图3-7所示;**

基本信息					
• 服务名	chap/2idap		服务后端	dotte	
• 业务分组	未分组	-			
• 缺省安全策略	不使用安全策略		 缺省私有属性下发策略 	不使用	-
计直接暗	不计声	w			
服务描述					
🗵 司申请 🕄			III 智能终端快速认证 😯		
版权信息					
・ 進入時段	无	-	分配P地址	35	*
下行連军		Kbps	上行速率		Kbps
优先级			自用RSA认证		
证书认证	⑦ 不直用 ● EAP	E特认注 ◎ WAPIEFSUG	E		
认证证书类型	EAP-PEAPILIZ	-	认证证书子类型	MS-CHAPV21LE	
下发VLAN			下发User Profile		
THEOR		0			

(3):在LDAP服务器上(同iMC服务器)新建虚拟计算机,依次点击;



图3-8

输入新建计算机名称h3c,点击确定,如图3-9所示;

Active B	lirectory 田白和计算机 - 计算机	
	的建于: h3c. com/Computers	
计算机 [b3d]	<u>ま</u> 読い:	,
计算机: H3C	名(Windows 2000 以前版本)(P):	
下列用, 用户或: 默认:	戸頭組可以将此计算机加入到域。 組(U): Domain Admins 更改(C)	
匚 把诸	亥计算机帐户分配为 ₩indows 2000 以前版本的计算机(S)	
	确定 取消 帮助	

图3-9

为新建的虚拟计算机设置密码,需要运行一个脚本程序——ModiComputerAccoutPass.vbs,该脚本程序从PEAP认证域控配置界面下载获得,先下载到本地,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=h3c,CN=Computers,DC=h3c,DC=com,将iMC123替换为虚拟计算机密码"q1w2e3R4";

 · 通行服务器全名 	WIN-AUGGSOZWH9Z h3c com				
* 虚拟计算机名称	h3c	0	• 虚拟计算机密码	q1w2e3R4	0
 DNS服务器P 	10.2.0.2	0	• 城庄服务器中	10.2.0.2	
日志识别	调 成		* 本地服务器调口	9812	0
域控服务器操作系统版本	Windows 2008 成之后版本	•		_	
给改计算机密码相率	http://10.2.0.2.8080/mc/peapPass	wordScript?fileNam	e-ModifyComputerAccountPasa vba		
			宅 取消		

(4):在LDAP服务器中新建组织单元haha如图3-11依次点击;



(5): 在组织单元haha里面新建三个用户"x111"、"x112"、"x113",并为其设置LDAP密码,勾选密码永不过期(新建用户时会自动提示创建密码);



图3-13

(6): iMC中LDAP配置,业务-用户接入管理-LDAP业务管理-服务器配置,其中Base DN为获取用 户数据的范围;对于LDAP服务器来说,管理员DN确定为图3-14所示;其他选项意义分别为:

服务器类型:分为通用LDAP服务器和微软活动目录。前者表示所有符合LDAP标准的服务器,后者 专指Microsoft Windows活动目录;

服务同步方式:当"服务器类型"设置为通用LDAP服务器时,该参数只能设置为手工指定;当"服务器 类型"设置为微软活动目录时,该参数可以设置为手工指定或基于AD组;

手工指定:为LDAP服务器配置同步策略时,可以为绑定用户指定服务;

基于AD组:为LDAP服务器配置同步策略时,只能为LDAP组指定服务,根据绑定用户所属的LDAP 组自动为用户分配服务。

服务器名称	10.2.0.2	極旁器版本	3 •
服务器印地址	10.2.0.2	- 演口	389
服务器类型	微软活动程录 •	服务局步方式	手工编室 *
实时以证	······································	 這接種類的才长 	1944 -
11.000000000	50 B	· P15/88/14141	÷
业务分组	来分组 *	III 启用SSL连接	1 法通照务器
务器信息			
Base DN	ou=haha,dc=h3e,dc=com		
管理员DN	cn=administrator,cn=users,dc=h3c,dc=con		
管理员密码			
用戶名讓性名称	sAMAccountName		
用户密码属性名称			
3-14			
己置完后点击检测	则,看到如图3-15提示说	说明配置成功, 然后点击	确定;
□ 业务 >> 用户推入管理 >> LI	DAP业务管理 >> 服务器权置 >> 编改LDAP服务	3信息	
MPIE&英信印	2 11 11 11 11 11 11 11 11 11 11 11 11 11	戰豐正确,影够与LDAP服务器 = 102.02 连接成以	b•
本位息			
• 服务署名称	10.2.0.2	服务置版本	3 •
* 服务器中地址	10.2.0.2	* iiii	389
服务器会型	做炊活动回来 ·	服务同步方式	手工程定 -
※可以近 (1)10100101101	20	· 连接静默时长	1);) **
· 服白分组	ETHR	• PP20211月	v
 业务分组 	(于上18年 *)	一 会景S社 法接	▼ 法通知条件
3.5.7.8 後身器信息	(4-4)a	にご通知のない価格	10.1注意地方容
]3-15 DAP同步策略酉	2置;		
<mark>】</mark> 业务 >> 用户接入管理	>> LDAP业务管理 >> 同步策喻假置 >>	修改LDAP同步策略	
会改LDAP同步策略			
• 同步策略名称	chapv2idap		
服务署名称	10.2.0.2	*	
业务分组	未分组		
Base DN	oushaha dosh3c doscom		
Last Pit	ovenana,ucensc.ucecom		
+ →BaseON	ou=haha,dc=h3c,dc=com	P	
* 过滤条件	(&(objectclass=user)(sAMAccountNar	ne=*))	
• 状态	有效		
同志の用白米利	◎ 接入用户 ◎ 设备管理用户		
PS(PR)(7)/~94Cad			
同步访问广关金	📝 自动同步		
同步违项	自动同步		
M≥1310/-×∝ 同步选项	 自动同步 技業同步 		
四步追顶 同步追顶	 回 自动同步 技業同步 ✓ 新聞用户及其違入條号 		
Pipeling,2018	 ebildesity 技業同步 が増用户及其違入株号 が方口存在用户新聞違入株号		
四9年11月7日 9月 同步违项	 ☑ 自动同步 □ 技業同步 ☑ 新聞用户及其推入休号 ☑ 为已存在用户新聞推入休号 □ 内已存在用户新聞推入休号 □ 仅同步当解节点下的用户 		
Portuna - New Portuna	 elsippe 技業務長 状業務長 が着理ら及其推入休号 がご存在用户新建批入休号 のご得知当前市点下的用户 		A
P10-0-2007 P202	 ☑ 自动局参 技業局参 ☑ 新聞用の及其違入休号 ☑ 为己存在用户新聞推入休号 ☑ 仅同步当前书点下的用户 	18 (4–7	A
P#3307742 P#335 33-16 3果在LDAP配置 5用户和LDAP解	 ② 自动病歩 技業病歩 ③ 新電用户及其施入条号 ③ 为己存在用户结理施入条号 ② 内己存在用户结理施入条号 ① (内修当前节点下的用户 	下ー步 電 Imail, 则选择从LDAP- 将使用图3-17配置的密	导入,当从LDAP服务器同约 码"h3c"。
PB-B-00-742 PB-B-355 日3-16 の果在LDAP配置 5月一和LDAP能 B次LDAP的多策略	 ② 自动病参 技業病母> ③ 紙増用户及其施入条号 ③ 力已存在用户紙増換入条号 ② 内已存在用户紙増換入条号 ③ (内得些当前书点下的用户 	<mark>下─</mark> 步 和ail,则选择从LDAP 将使用图3-17配置的密	春 导入,当从LDAP服务器同约 码"h3c"。
PB-B-967 Page PB-365 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	 日均明歩	<u>下─</u> 步 和ail,则选择从LDAP- 将使用图3-17配置的密	春 导入,当从LDAP服务器同约 码"h3c"。
PB-B307 Maz PB-B355 PB-B355 日果在LDAP配置 5 5 5 日戸和LDAP節 5 3 3 3 4 5 5 1 6 5 1 6 5 5 5 5 5 5 5 5 5 5 5 5 5	 ② 自动病参 ● 技術内参 ● 技術内参 ② 新増用户及其違入条号 ② 为己存在用户新增推入条号 ● 仅两步当前节点下的用户 	<u>下−</u> ቃ № ロmail,则选择从LDAP- 将使用图3-17配置的密	▲ 导入,当从LDAP服务器同步 码"h3c"。
開歩送版 開歩送版 副3-16 の果在LDAP配置 均用户和LDAP 部 改LDAP 同少策略 基本信息 用户姓名 证件号码	 ② 自动病歩 ● 技業病サラ ○ 新着雨户及其違入条号 ② 为己存在用户结理推入条号 ○ (○用歩当前书点下的用户 	下─步 ■ 和 のmail,则选择从LDAP 将使用图3-17配置的密 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	● 导入,当从LDAP服务器同步 码"h3c"。
同步送项 引3-16 切果在LDAP配置 均用户和LDAP	 ② 自动病歩 技業病サラ ジ 結準用户及其違入係号 ジ カ己存在用戶新律権入係号 ① (内陽步当前市点下的用户 	下一步 1 和 Imail,则选择从LDAP 将使用图3-17配置的密	鲁入,当从LDAP服务器同约码"h3c"。
周3-16 四果在LDAP配置 5)用户和LDAP能 23 30 30 30 30 30 30 30 30 30 3	 ② 自动病歩 技業病サラジン(株式) ※ 紙増用户及其違入株号 ※ 約2存在用户紙増換入株号 ② 内已存在用户紙増換入株号 ② (内得当前市点下的用户) 	下-步 ■ 印mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ●	春 导入,当从LDAP服务器同约 码"h3c"。
用歩送项 開歩送项 開まる項 開た 和上DAP配置 の果在LDAP配置 の用户和LDAP節 認 な 協 の 用 や 和 し の 早 数 に の の 果 在 し の み や 部 で 置 の 、 の 和 に し の や 新 の 、 の 和 し の や 新 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の 、 の の 、 の の 、 の の の の の の の の の の の の の	図 自动病歩 技業病少 数者病户及其違入条号 ※ 新者病户及其違入条号 》 力启右五月中経環境入条号 ② 力启右五月中経環境入条号 ② 代荷歩当前书点下的用户	<u>下-</u> 步 № ロmail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ● ● ● ● ●	● 导入,当从LDAP服务器同步 码"h3c"。
同歩送版	図 自动病歩 技業病サラ 試業病サラ及其違入条号 ※ 新着市户及其違入条号 》力已存在用户結構進入条号 (内用少当前书点下的用户 2) 2) (日本)	下─步 ■ 和 口mail,则选择从LDAP- 将使用图3-17配置的密	鲁入,当从LDAP服务器同步 码"h3c"。
同歩33 同歩33 同歩33 可果在LDAP配置 5 5 5 日戸和LDAP館 2 なん 1 日戸姓名 近半号码 通讯地址 电話 电子部件 ・ 用户知 名 3 - 2 - - - - - - - - - - - - -	図 自动病参 技業病母少 ● 技業病母少 ● 秋電和户及其施入係号 ● クロタジョ第ち点下的用户 ● クロタジョ第ち点下的用户 ■ プtelephonenumber系 年外組	下-步 ■ □mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ●	春 导入,当从LDAP服务器同步 码"h3c"。
同歩送项 同歩送项 日3-16 の果在LDAP配置 の用户和LDAP能 認 本信息 用户姓名 证件号码 通讯地址 电话 电子部件 ・ 用户分组 参 入信息 体品 体品 体品 本 日 本 日 本 日 日 日 日 日 日 日 日 日 日 日 日 日	図 自动病歩 技業病サラ ● 技業病サラ ● 就着境中の及其違入係号 ● カロ存在用户紙準換入係号 ● (7月少当前市点下的用户	下-步 № 印mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	春 导入,当从LDAP服务器同约 码"h3c"。
PPからかで Mail PPからが PPからが PPからの PP PP PP PP PP PP PP PP PP P	 図 自动病歩 技業病サラ 試業病ウ及共振入株号 プロ市石用户結構換入株号 (○内歩当前市点下的用户 (○内歩当前市点下的用户 (○内歩当前市点下的用户 (○内歩当前市点下的用户 (○内歩当前市点下的用户 (○内歩当前市点下的用) (○内歩音) (○内赤音) (下-步 № □mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ●	导入,当从LDAP服务器同步 码"h3c"。
同歩送项	図 自动病歩 技業病サラ ※ 新着雨中及其違入条号 》为已存在用户结滞推入条号 》为已存在用户结滞推入条号 (何時步当前书点下的用户 2 2 7 7 7 6 (何時少当前书点下的用户 2 2 7 7 7 8 AMAccountNam 不从LDAP服务器 1 未分组 8 6 6 6 6 6 6 7 8 9	下─步 ■ 和 の mail,则选择从LDAP 将使用图3-17配置的密	鲁入,当从LDAP服务器同步 码"h3c"。
同歩送项 同歩送项 回果在LDAP配置 5月戸和LDAP館 総本価盤 用戸姓名 证件号码 通讯地址 电氏石 电子部件 ・用户分组 後入信息 株号名 株号名 株号名 株号名 株号名	 図 自动病歩 技業病外歩 技業病外歩 ※ 新着用户及其施入条号 》力已存在用户新律施入条号 ② 内已存在用户新律施入条号 ② (内除当前节点下的用户 	下─步 100 □mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	导入,当从LDAP服务器同步 码"h3c"。
PP-0-07-2022 PP-0-307	 図 自动病歩 技業病サラ 試着病中及其違入条号 シロ市在用中結環境入株号 シロ市在用中結環境入株号 (○同歩当前市点下的用户 	下ー步 1 和 ロmail, 则选择从LDAP- 将使用图3-17配置的密 e e ・ ・ ・ ・ ・ ・ ・ ・	导入,当从LDAP服务器同组码"h3c"。
PipeDinの Page Pipe	図 自時期歩 技業用歩 試業用・及其違入係号 グ 力に存在用・斥ば増払入係号 クロードは増払入休号 (内用歩当前市点下的用户	□mail,则选择从LDAP- 将使用图3-17配置的密 。	●入, 当从LDAP服务器同步 码"h3c"。
PloB 2007 Page PloB	図 自动病歩 技業病サラ ● 技業病サラ ● 新常市の及其施入休号 ● カロ市な用户科学施入休号 ● (内県少当前市点下的用户 日	下一步 和 口mail,则选择从LDAP- 将使用图3-17配置的密 ・ ・ ・ ・ ・ ・ ・ ・ ・	导入,当从LDAP服务器同约 码"h3c"。
PP>B>00 Pace PP>300	 図 自动明歩 技業明歩 ジ 新着用・P及拼違入係号 ジ カニ府在用・新環境入係号 マ 内歩当前市点下的用户 (の用歩当前市点下的用户 (の用歩当前市点下的用户 (の用歩当前市点下的用) (の用歩) (の用の一) (の用の一)	下-步 № 印mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ●	● 导入,当从LDAP服务器同步 码"h3c"。
PipeDinの Page PipeDinの Page PipeDinの Page PipeDinの Page PipeDinの Page PipeDinの Page PipeDinの PipeDin	図 自动病歩 技業病サラ ※ 新着雨中及井道入株号 》力已存五用户結準推入株号 ⑦ 内学当前书点下的用户 2 2 7 10 7 11 第 12 13 14 14 15 15 16 17 18 17 18 18 17 17 18 17 18 19 19 19 10 110 111 111 111 111 111 111 111 111 111 111 111 111 111 111 111 111 111 111 1111 <t< td=""><td>下一步 和 Qmail,则选择从LDAP- 将使用图3-17配置的密 。 。 。 。 。 。 。 。 、 元 同步 、</td><td>●</td></t<>	下一步 和 Qmail,则选择从LDAP- 将使用图3-17配置的密 。 。 。 。 。 。 。 。 、 元 同步 、	●
PipeDinの Page PipeDino Page PipeDino Page Pipe	図目的時時 技業時時 技業時時 新着雨户及井道入株号 カ2府在用户結準推入株号 (内時当前市点下的用户 2 2 7	下一步 和 口mail,则选择从LDAP- 将使用图3-17配置的密 。 。 。 。 。 。 。 。 。 。 。 。 。	●入, 当从LDAP服务器同步 码"h3c"。
Plot Plaz Plot Pla	図 自动病歩 技業商内歩 ● 技業商内歩 ● 秋海市内及井道入株号 ● カロ市在用户転借換入株号 ● (内内歩当前市点下的用户 ■ 「「日日の市のロロリン」 ■ 「「日日の市のロリン」 ■ 「「日日の市の日口リン」 ■ 「「日日の市の日口リン」 ■ 「日日の市の日口リン」 ■ 「日日の市の日」 ■ 「日の市の日」 ■ 「日の市の日」 ■ 「日の市の日」 ■ 「日の市の日」 ■ 「日の市の日」 ■ 「日の市の日」 ■ 「日の	下-步 ■ 口mail,则选择从LDAP- 将使用图3-17配置的密 ● ● ● ● ● ● ● ● ●	● 导入, 当从LDAP服务器同步 码"h3c"。
Pipe Bill の Page P	図 自時期歩 技業用サランス対象の ※ 新着用中及対象入条号 ※ 約点市在用中結環境入株号 ⑦ 力合在用中結環境入株号 ⑦ 内参当前书点下的用户 2 ⑦ Telephonenumber系 解除绑定关系后,认证时 ○	下ー步 1 和 口mail, 则选择从LDAP- 将使用图3-17配置的密 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	● 导入, 当从LDAP服务器同步 码"h3c"。
Pipe Diversion Pipe D	図 自动病歩 技業病サラ ※ 新着雨中及井道入株号 》力已存五用中結環境入株号 ⑦ 内学当前书点下的用户 2 7 7	下-步 和 口mail,则选择从LDAP- 将使用图3-17配置的密 ● ●	● →, 当从LDAP服务器同步 码"h3c"。
Pipe Bin0 Page Pipe Bin0 Page Pipe Bin0 Page Pipe Bin0 Page Pipe A Comparison Pipe A Comparison Pipe A Comparison Pipe A Comparison Comparison Pipe A Comparison Comparison Pipe A Comparison Compar	 ② 自动病歩 技業病サラ ジカロキロ用户経構施入株号 ウロキロ用户経構施入株号 (内用少当前书点下的用户 	下-步 和 口mail,则选择从LDAP. 将使用图3-17配置的密 ● ●	● 今 入, 当从LDAP服务器同步 码"h3c"。
Pipe Binの Peak Pipe Binの Peak Pipe Binの Peak Pipe Binの Peak Pipe Bin	図 自动病歩 技業病外歩 ● 技業病外歩 ● 対応市石用户科学権為入株号 ● クロタウム用から対象ない、水気の ● (内房少当前市点下的用户 ■ (内房少当前市点下的用户 ■ (内房少当前市点下的用户 ■ (内房少当前市点下的用户 ■ (内房少当前市点下的用户 ■ (内房少当前市点下的用户 ■ (内房少気大気后,)、认证日 ■ (内房少気大気后,)、い证日 ■ (内房大気,)、い证日 ■ (内方) ■ (内方) <t< td=""><td>下-歩 100 口mail,则选择从LDAP 将使用图3-17配置的密 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・</td><td>● 导入, 当从LDAP服务器同步 码"h3c"。</td></t<>	下-歩 100 口mail,则选择从LDAP 将使用图3-17配置的密 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	● 导入, 当从LDAP服务器同步 码"h3c"。
PipeDinの Page Pipe	 図 自時時歩 技業時歩 試業時から 対応中石用・料理推入株号 プロ中石用・料理推入株号 (7)時当前半点下的用户 (7)時当前半点下的用户 (7)時当前半点下的用户 (7)時当前半点下的用户 (7)時間 (7)時間	下ー步 1 和 口mail, 则选择从LDAP 将使用图3-17配置的密 。 。 。 。 。 、 、 、 、 、 、 、 、 、 、 、 、 、	●入, 当从LDAP服务器同步 码"h3c"。
Pipe Diversion Pipe	 図 自动病歩 技業病外歩 ジ 新着雨中及井道入条号 ジ カロ市石用中結構施入株号 (○ 内沙当前市点下的用户 (○ 内沙当前市点下的用户 (○ 内沙当前市点下的用户 (○ 内沙当前市点下的用户 (○ 内沙当前市点下的用) (○ 内) (○ 内	下-步 和 口mail,则选择从LDAP- 将使用图3-17配置的密 ●	● 一 ● 入, 当从LDAP服务器同步 码"h3c"。
Pipe Bill Product Pipe Bill Prod	図目的時時 技業時時 技業時時 第2時日月の及井道入係号 カ2日在日月の採港入係号 内2日本日月の採港入休号 (内時当前市点下的用户 2 2 (内時当前市点下的用户 2 (内時当前市点下的用户 2 (内時当前市点下的用户 2 (内市) (大) (日本) (日本) <t< td=""><td>下ーチ 1 口mail, 则选择从LDAP 将使用图3-17配置的密 ・ の の</td><td>●入, 当从LDAP服务器同步 码"h3c"。</td></t<>	下ーチ 1 口mail, 则选择从LDAP 将使用图3-17配置的密 ・ の の	●入, 当从LDAP服务器同步 码"h3c"。

```
勾选之前创建的服务,点击完成;
```

服务名	服务后提	状态	缺省安全等略	计表策略	分配印烛址
📋 melyong	h3c	司申请	不使用安全解释	不计费	ALL TO INTERACTOR
tomportal	h3c	司申请	不使用安全策略	不计费	
🛅 dottx	dottx	司申请	不使用安全解释	不计费	
mac mac		司申请	fp欣/\$3CDeamon	不计奏	
🛅 portal	h3c	司申请	不使用安全解释	不计费	
🖾 hah	h3c	司申请	不使用安全論唱	不计费	
802test	dottx	司申请	不使用安全解释	不计费	
🗇 tom tx	dot1x	司申请	不使用安全解暗	不计奏	
noneportal		司申请	不使用安全策略	不计费	
tomportai2		司申请	不使用安全解唱	不计费	
🛅 vpn	h3c	司申请	不使用安全解释	不计费	
📰 zhineng	h3c	司申请	不使用安全解職	不计奏	
Chapy2ldap	dottx	司申请	不使用安全策略	不计费	

(7): PEAP认证域控配置,业务-用户接入管理-业务参数配置;

2 业务 >> 用户接入管理 >> 业务参数配置 >> 1	系统政策	大加入附属
系统改置		
配置項名称	6 12	R2
系统参数数置	系统提供业务组织的常用参数信息	N
國服务营业的配置	羅暗線旁邊及安全管理相关的參數信息	N
IAM运行日志参数配置	配置系统运行环境相关参数	N
用户提示信息配置	藏示绘用,中的相关体理配置	N
在户端自动运行任务数置	配置有户端认证后自动运行相关程序的配置	×
1户尝码控制网络数置	戰鬥用户密码的控制解释	N
1962 <u>2</u>	没 靠业务的城等相关信息	N
冬号自动间,户配置	系统模仿各个参数的设置情况,为帐号进行自动纯户处理。	N
EAP认证规控配置	配置PEAP认证规控相关参数	× 1
用户自助Logo图片截置	配置用户自助装页的Logo信息	· ·
形成在位都對配置	配置无规定位的相关参数	N
用户上下线通知能到截置	用户上下线通知银兴的参数信息	N
1月18日秋闲秋西	配置客户间防被能功能依赖的字典文件	N
1286号器检测使数	iNode審戶讓检測主机是否自用代理服务器的參数	N
#举行编访问控制 成 置	算单同结论问题主制(SNAC)均能的提升提出	N
王信功能政置	使用短值功能所需要配置的音项基本管数	

图3-19

此处注意点较多:

1):域控服务器全名为安装域控服务器PC的全名,具体可通过单击我的电脑-右键-属性-查看;

2):虚拟计算机名称和之前新建的保持一致;

3):虚拟计算机密码为之前为虚拟计算机新建的密码。

◎ 业务 >> 用户推入管理 >> 业务参数配置 >> 系统配置 >> PEAP认证域数配置
PEAPLIEMIONT
・ 組成等格音会名 VMR-AUG6020HHZ Als com 0 ・ 虚似计算机定向 0 ・ 虚似计算机 Country 0
秘密を取り
全此,iMC侧的配置全部完成,接下来配置客户端。
3. iNode客户端配置:
1):新建802.1x连接(证书认证唯一支持);
新建连接向导
选择认证协议
iNode智能客户端为多种协议提供了统一的认证平台
 ● 802.1X协议(X) 802.1X是一种网络访问控制协议。
◎ Portal协议 (P) Portal是一种基于门户的宽带认证上网方式。 请选择认证使用的协议类型
 ● 使用IPv4协议认证(I) ● 使用IPv6协议认证(J)
◎ L2TP IPsec VPN 协议(V) 使用虚拟专用网(VPN),通过Internet连接到网络。

2):选择证书认证里面的PEAP认证,如图3-22所示,安全密码为LDAP里面创建用户时设置的密码,由于客户端不需要验证服务器,所以不选择验证服务器证书,当客户端安装有根证书时,可勾选此项。

My Node Crent COD Mirro CARD	• • •	Leopuspel) Albert Ann 👁 KH 💿 Hit 👔 🕅	۵	以证典型 〇 EAP-TLS(T) ● PEAP(A)	
Content sourcessing	~	A A A A	Idapchapv2 屋性	安全用户名(1):	x111@dot1x
		전 전 전 전	用户常规制它	教全法明(M):	
-	10025.***	我的VPN语 我的Portal语 我的802.1X Idapchapv2 接 接 连接	B0\$00-	□从证书读取用户#	1(G)
			(月7-41-00)	17.15.415	
			Date	4.57201857.00	
TO DEMAN	1000		46 00-	TAXABLE MIT IN	
				LACOSTACIO	<u></u>
AMAR		117mB	図 倉用高級认证 (t)		HE RA
		W248	© INCLUE OD	<u> </u>	
		2012-11-13 00:16:45 逐漸95% 2012-11-13 00:16:45 开始进行身份验证 [#1196+t1#] 2012-11-13 00:16:46 正在进行证书验证 2012-11-13 00:16:49 定的身份验证成功	 ○ 都広々以近の ● 在井以正の 	证书设置(3)]	
		Neas an		()) ()	
		上月11111 000:00:57		AB AB	

图3-22

配置完成后,发起连接,可以成功认证,如上图3-22所示。

4. 配置关键点:

1):该认证方式只能与802.1x配合,不支持Portal认证方式;

2):导入iMC的根证书和服务器证书为同一CA机构颁发;服务器证书需先安装 到IE里面,导出后 才能导入iMC中;

3): PEAP域控配置里面IP只能填写实际IP地址,不能填写127.0.0.1;

4): iNode客户端认证时,输入的密码为LDAP中为用户创建的密码,解除绑定关系后使用iMC中创 建的密码h3c;

5):客户端认证时尽量不要携带前缀;

6):有时PC认证不成功,在配置正确时,可以将域控服务器的类型选择为2003或以前,此时可以 解决问题。