何颖 2008-09-05 发表

iMC与AD配合做域统一认证的典型配置 一、组网需求: 支持802.1x特性的交换机; iMC服务器; Microsoft Active Directory; iNode客户端。 二、组网图: WAN 192.168.1.99/24 LAN . 192.168.0.1/24 192.168.1.12 192.168.1.11 192.168.0.X/24 USER/iNode iMC AD 设备说明: NAS: S3652 iMC: V3.2 E0401P05或更高版本。其IP地址为192.168.1.12 Microsoft Active Directory 5.2: 其IP地址为192.168.1.11 iNode: V2.4-F0335或更新版本。 三、配置步骤: 前提条件是iMC、AD、NAS、User均路由可达。 NAS可以采用802.1X认证或者Portal认证,这里以 802.1X认证方式为例。 配置域统一认证的步骤只是在做身份认证的基础上多了关于LDAP的相关配置。所以关 于身份认证 (如802.1x或Portal) 的配置也可参考其他案例,本案例中的配置只是基本 配置。 1. 配置NAS #配置Radius服务器 [H3C]radius scheme test [H3C -radius-h3c]server-type extended [H3C -radius-h3c]primary authentication 192.168.1.12 1812 [H3C -radius-h3c]primary accounting 192.168.1.12 1813 [H3C -radius-h3c]key authentication h3c [H3C -radius-h3c]key accounting h3c [H3C -radius-h3c]user-name-format without-domain # 配置认证域 [H3C]domain h3c //此处域名必须与AD中的域名一致。 [H3C -domain-h3c]radius-scheme test [H3C]domain default enable test 对于若是使用ComwareV5平台的设备做NAS设备,其domain部分的配置有些区别, 需加上AAA认证中的authorization。802.1x的对应的类型是lan-access。 # domain h3c authentication lan-access radius-scheme test authorization lan-access radius-scheme test accounting lan-access radius-scheme test # 配置VLAN [H3C]Vlan 2 [H3C-vlan2]Port interface GigabitEthernet1/1/1 to GigabitEthernet1/1/4 [H3C]Interface vlan 2 //管理Vlan [H3C -Interface-vlan-2]ip add 192.168.1.99 255.255.255.0

[H3C]Interface vlan 1 //用户Vlan
[H3C -Interface-vlan-1]ip add 192.168.0.1 255.255.255.0
启动802.1X认证
[H3C] dot1x //全局启动802.1x
[H3C] dot1x authentication-method pap (或eap) //域统一认证时必须启用PAP或EA P认证
[H3C]interface Ethernet 1/0/1 //准备对接口启
用802.1x
[H3C-Ethernet1/0/1]dot1x //表示对下行口Ethernet 1/0/1 接口启动802.1x认证,当然 如果配置[H3C] dot1x interface Ethernet 1/0/1 to Ethernet 1/0/48则表示Ethernet 1/0/1
到 Ethernet 1/0/48所有下行口都启用dot1x认证。但不能对连接认证服务器的上行口启 动dot1x。
注: 这里只是列出了802.1X的所有必须的配置,还有一些高级选项可以自行配置,如

version check、accounting on等。

2. 安装AD

Windows 2000 server和windows server 2003都带有Active Directory, 这里已window s server 2003为例说明AD的安装过程。

1). 首先为服务器配置正确的IP地址并连接网络。

2). 选择"开始->所有程序->管理工具->配置您的服务器向导"



3). 在欢迎界面点击"下一步"



4). 直接点击"下一步"



HOS 名 运行非 Windows 2000, Windows XP 利 NetBIOS 域名。	D Windows Server 2003 家族的客户端将使用
铁认 NetBIOS 名称由 DNS 域名派生。	
0MS 域名:	
h3c.com	
要更改默认 NetBIOS 名称,请在下面	的框中键入新的名称。
нас	
	〈上一步(12) 下一步(12) 〉 取消 帮助
	; "下 一步 ":
эт <u>н</u> , тто <u>с</u> то,	
的服务器向导	
E转发 DNS 查询 设计为转发器的 DNS 服务器解析此	服务器不能解析的 DNS 查询。
此服务器可能会接收到它不能解析6 设置此服务器将这些查询转发到另-	的 DNS 查询(将 IP 地址转换为计算机名称的请求)。您可以 一个 DNS 服务器,成为转发器。
如果您的 Internet 连接是由 Inte 器的正确地址。如果您没有使用 IS	ernet 服务提供商 (ISP)提供的,请与 ISP 联系,以获得转; SP,请与您的网络管理员联系以获得地址。
	na na mangang ng mangang ng n
您想让此服务器转发未解析的 DMS	查询吗?
C 是,将查询转发到 IP 地址如下	的 DNS 服务器 (1):
● 否,不转发查询 @)	
○ 否,不转发查询(0)	
○ 否,不转发查询 @)	
○ 古,不特发查询 ②	
○ 否,不转发查询 @)]	
○ 活,不转发查询 (0)	< 上一步 (2) 下一步 (2) > 取消 希
○ 否,不特发查询 ②	< 上一步 (b) 下一步 (b) > 取消 希
● 香,不转发查询 ◎〕 角认选项正确后点击"下一步	< 上一步 (2) 下一步 (2) > 取消 再
○ 活,不转发查询 @〕 角认选项正确后点击"下一步 约累务署内导	<u>〈上→步@)下→步@)〉 取消 ₹</u> 長"
○ 香,不转发查询 @〕 角认选项正确后点击"下一步的服务器件导	<u>〈上一步@)〉 取消 </u> 步"
○ 否,不转发查询 ①] 角认选项正确后点击"下一步 的服务器件导 18结 查者并确认您选择的选项。	<u>〈上一步④】下一步④)〉 取消 </u> ¹ ¹
○ 否,不转发查询 (0) 角认选项正确后点击"下一步 約累务器向导 結結 查看并确认您选择的选项。 总结 (5):	<u>〈上一步④】下一步④)</u> 取消 構 ¹
(• 否,不转发查询 @) 角认选项正确后点击"下一步的服务器内导 6.54 查看并确认您选择的选项。 总结 (2): 安整 DICP 服务器 (DU果需要)	<上一步 (2) 下一步 (2) 〉 取消 ▲
● 香,不转发查询 @〕 ● 商, 不转发查询 @〕 ● 商, 法选项正确后点击"下一步 ● 的复数器内导 ● 自身 ● 查看并确认您选择的选项。 ● 总结 (S): ● 安整 Active Directory 和 DBS # ● 2010年 服务器 (如果需要) ● 安整 Active Directory 和 DBS # ● 2010年 服务器 (如果需要) ● 2010年 服务 服务 [100年 服务 [100年 [1005 [10	《上一步 (2) 下一步 (2) 》 取消 再
○ 活,不转发查询 (0)] 第 人 选项正确后点击"下一步 第 局认选项正确后点击"下一步 第 局 新 确认您选择的选项。 第 局 任 服务器 (00果需要) 安装 Active Directory 和 DNS 量 创建下列完整城名: h3c. com	(人上一步(2))下一步(2)) 取消 系 し、 取消 系 (特比服务器设置力域控制器)
○ 活,不转发查询 (0) 角认选项正确后点击"下一会 的服务器育导 移着 查看并确认您选择的选项。 总结 (2): 安裝 DACF 服务器 (30果需要) 安裝 DACF 服务器 (30果需要) 安裝 DACF 服务器 (30果需要) 台述下列完整城名: h3c. com	(上一步(2))下一步(2)) 取消 承
○ 活,不转发查询 (0)] 角认选项正确后点击"下一步 的服务器件导 指数结 查着并确认您选择的选项。 总结 (2): 安裝 Active Directory 和 DBS 計 创建下列元整城名: h3c. com	<u>〈上一步(B)</u> 下一步(B) 〉 取消 希 步" 男务器(将此服务器设置力域控制器)
 (*) 活,不转发查询(0)] (*) 活,不转发查询(0)] (*) 市场后点击"下一步 (*) 市场后点击 (*) 市场后点击<td><u>〈上→步(b) 下一步(b) 〕 取消 看</u> 步" 服务器 (将此服务器设置为域控制器)</td>	<u>〈上→步(b) 下一步(b) 〕 取消 看</u> 步" 服务器 (将此服务器设置为域控制器)
 () 否,不转发查询(0)] () 否,不转发查询(0)] () 角认选项正确后点击"下一步 () 原务器(6) () 原务器(6) () 原务器(0) () 原务器(0) () 原务器(0) () 原务器(0) () 原务器(0) () 原务器(0) () 原务器(2) () 原务器(2)	く上一步(2) 下一步(2) 取消 単 下一步(2) 次 1 (前 (前) (前) () () () () () () () (
 () 否,不转发查询(0) () 否,不转发查询(0) () 角认选项正确后点击"下一步 () 原务器向导 () 是结 () 定 報 DICF 服务器(00果需要) () 安裝 Active Directory 和 DIS 晶 () 建下列完整域名: h3c. com 	く上一步(2) 下一步(2) 取消 単
 () 否,不转发查询(0)] () 否,不转发查询(0)] () 命认选项正确后点击"下一步 () 意告(5): () 受装 Active Directory 和 DIS 計 () 建下列完整域名: h3c. com 	<u>く上一步(2)</u> 下一步(2) 取消 再 上" 日本ののでは、「「一歩(2)」、「下一歩(2)」、「取消 「 日本ののでは、「「一歩(2)」、「下一歩(2)」、「取消 「 日本ののでは、「「「一歩(2)」、「下一歩(2)」、「 日本ののでは、「「「一歩(2)」、「下一歩(2)」、「 日本ののでは、「「「一歩(2)」、「下一歩(2)」、「 日本ののでは、 日本のので
○ 活,不转发查询 (0) 角认选项正确后点击"下一步 約基务器育导 参告 查看并确认您选择的选项。 急结 (5): 安裝 Active Directory 和DIS 量 创建下列完整城名: h3c. com	<u>〈上一步 @)下一步 @)〉 取消 予</u>
(活,不转发查询 (0)] 角认选项正确后点击"下一步 的服务器件导 移给 查看并确认您选择的选项。 总结 (2): 安莱 Active Directory 和 DNS 册 创建下列完整城名: h3c. cos 要更政您的选择,单击"上一步"。	《上→步 (b) 下一步 (b) 》 取消 有 5" 次多器(将此服务器设置为域控制器) 系务器(将此服务器设置为域控制器)
○ 活,不转发查询 (0) 角认选项正确后点击"下一步 的服务器育导 移结 查看并确认您选择的选项。 总结 (2): 安裝 DACF 服务器 (DQ果需要) 安裝 DACF 服务器 (DQ果需要) 会结 (2): 安裝 DACF 服务器 (DQ果需要) 会话 (2): 安装 DACF 服务器 (DQ果需要) 会话 (2): 安装 DACF 服务器 (DQ果需要) 会话 (2): 安装 DACF 服务器 (DQ果需要) 会话 (2): 会话 (2): 安装 DACF 服务器 (DQ果需要) 会话 (2): 会话	〈上一步 @) 下一步 @) 〉 取消 系



音怒的。	医务器向导		
服务器		- 48. /-	V
止	住执行恣选挥的如何	操作。	E
-	指派静态 IP 地址		
~	安装 DHCP 服务器		
~	安装 Active Dire	ctory	
~	安装 DNS 服务器		
~	DNS 查询将不会被	转发。	
~	配置并激活 DHCP	作用域: 192.168.2.10 到 192.168.2.254	
~	在 Active Direct	ory 中对 DHCP 服务器进行身份验证	
~	在此域控制器上的	Active Directory 中设置一个应用程序命名上下文,供 TAPI	
	-B7 4002703273 0C		
80.4	* 9983981+++9.		
7025	5-88月6月721年。		
REP A	大學家已是一十		
周快当	今初间1月7日以4		
		<上一步(B) 下一步(D) 取消	帮助
占言	も"完成" 至此	试控制哭弃装完比	
• A.L			
您的	服务器向导		
		此服务器现在已配置好	
_		您已成功配置此服务器来担任作为第一台服务器的典型角色。	
-		本王山会会で石竹に雨	
	10	並有此用巴下面的步骤	
	125		

azirea Zorea Korna		
	Annu Strenge RIKS1216 Annu Strenge RIKS1216 Annu Strenge KARBE Annu Strenge KARBE Data See	
Administrator	6.84 0.84 1.97 2.97 2.84 2.84 2.84 2.84 2.84 3.84	
1 TERNES For Finders Updets 日日 Office 文化 Contractor 安都 町 料理 Office 文化	्री समय कार) दी नियद स्वयादन दी यह	
	© ntransizan Ganza Di teransizan W nansekata Di nansekata Di teransizante	
Bartonness DBb Dateret Eglerer Bureacht For Biscreeft Ford Storout Store		

要查看您的更改的记录,请参阅<u>"配置您的服务器向导"日志</u>。 要关闭此向导,请单击"完成"。

<上一步(B) 完成 取消 帮助

2). 右键菜单服务器图标"h3c.com",选择"新建->组织单位":

3. 配置AD

▲Active Directory 用户和计算机 ス TOP(2) 場合(2) 表表 20 第日(2) 影響(2)	× II.
	o 7 & c
Active Directory 用户和計算机 + 保存的查询 反称	个対象 四利 福休
□ [] [] [] [] [] [] [] [] [] [] [] [] []	builtinDomain more free free free free free free free f
	· 缅甸 Default container fo
F F 连接到城控制器 (C) sers	· 4989 Default container fo
操作主机 创	
新建(3) 计算机	
西看(V) , 超	
从这里创建窗口(E) InetOrgP MSNQ 队列	erson 1别名
制新(2) 组织单位 与出利用(1) 打印(1)	
展性 (8) 用户	-
帮助业	*
创建一个新对象	
3). 填写组织单位名称, 中英文皆	行:
新建对象 - 组织单位	×
()	
名称 (A)	
实验室	
	确定取消
0	
4). 右键菜单刚才新建的组织单位	
4). 右键菜单刚才新建的组织单位	Z,选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	Z,选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 ④ ttive Directory 用户和计算机 ◇ 文件② 操作④ 查看② 曾曰① 標時回 ◆ → ① 回 ※ 圖 × 曾 ② 国 ② 	Z,选择"新建->用户" ニロメ 2 遊 歯 マ ≪ ま
 4). 右键菜单刚才新建的组织单位 ▲ Active Birectory 用P和计算机 ◇ 文件 ② 操作 ③ 查看 ② 留中 ⑨ 標時 ⑨ ◇ 文件 ② 激 圖 ※ 앱 ② 国 ② ◇ Settive Birectory 用P和计算机 ◇ Settive Birectory 用P和计算机 	Z,选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 ▲ ctive Birectory 用户和计算机 ◇ x th v bit (a) 查看 v 留中 v 帮助 w ◇ x th v bit (a) 查看 v 留中 v 帮助 w ◇ x th v birectory 用户和计算机 ◇ x th v birectory 用户和计算机 ○ x th v birectory 用户和计和 th v birectory 用户和计算机 ○ x th v birectory 用户和 th birectory hot v birectory	Z,选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 ★ Active Birectory 用户和计算机 ◆ 文件 ② 操作 ③ 查看 ② 留中 ⑨ 带助 ⑨ ◆ → ○ 圖 法 圖 × 留 ② 目 ② ● ○ Ref的違词 ● ○ Regulars 	Z,选择"新建->用户" 2 辺 図 マ Q 2
 4). 右键菜单刚才新建的组织单位 ★ Ctive Birectory 用户和计算机 ◆ 文件 ② 掛你 ③ 查看 ② 留中 ⑨ 帮助 ⑨ ◆ → こ 回 法 圖 × 歐 ② 目 ③ 第 ◆ ● ○ Birectory 用户和计算机 ● ○ Birectory 用户和 ● ○ Birectory 用	Z,选择"新建->用户" 2 辺 図 マ Q 2 対象 此規图中没有可显示的项目・
4). 右键菜单刚才新建的组织单位 ▲ ctive Birectory 用户和计算机 ◆ 文件 ② 操作 ④ 查看 ⑨ 窗中 ⑨ 帮助 ⑨ ◆ → 亡 回 法 電 × 留 ② 喝 ⑨ ● Kive Birectory 用户和计算机 ● Constant ● Constant ● Duiltin ● Duiltin ● Constant ● Duiltin ● Constant ● Duiltin	Z,选择"新建->用户" 2 辺 図 マ Q 2 対象 此規图中没有可显示的项目・
4). 右键菜单刚才新建的组织单位	27,选择"新建->用户" 27 27 20 20 20 20 20 20 20 20 20 20 20 20 20
4). 右键菜单刚才新建的组织单位 《Active Directory 用户和计算机 《文件 0 操作 4 查看 0 留中 0 帮助 0 中 1 日 3 電 2 留 2 日 2 《 Active Directory 用户和计算机 ● C 保存的意调 ● Duiltin ● C Cogneters ● C Cogneters ● C Cogneters ● C Cogneters ● C Cogneters ● C C C Cogneters ● C C C Cogneters ● C C C Cogneters ● C C C C C C C C C C C C C C C C C C C	Z,选择"新建->用户" 2 辺 図 マ Q で 対象
 4). 右键菜单刚才新建的组织单位 	27,选择"新建->用户" 27 20 20 20 20 20 20 20 20 20 20 20 20 20
 4). 右键菜单刚才新建的组织单位 	Z,选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	ブンス ブンス ブンス 「東型」 東型」 此規图中设有可显示的项目・
 4). 右键菜单刚才新建的组织单位 《 trive birectory 用户和计算机 《 文件 ② 操作 ④ 查看 ⑨ 窗中 ⑨ 帮助 ⑨ ※ 计 ③ 通 毫 ⑨ 窗中 ⑨ 帮助 ⑨ ※ ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	ブン ジン
 4). 右键菜单刚才新建的组织单位 《 tive birectory 用户和计算机 《 文件 ② 操作 ④ 查看 ⑨ 曾中 ⑨ 帮助 ⑨ ② 中 亡 回 よ 電 ♪ 留 ② 思 ② ③ Kive birectory 用户和计算机 ● ○ (保存的意識 ● ○ balain ● ○ Cognetars ● ○ Paria (Sective) (Principal ● ○ (Breath Cattrollers) ● ○ (Breath Cattrollers) <li< td=""><td>ブ、选择"新建->用户" 「二〇× 「二〇× <!--</td--></td></li<>	ブ、选择"新建->用户" 「二〇× 「二〇× </td
 4). 右键菜单刚才新建的组织单位 《 ctive birectory 用户和计算机 《 文件 C 操作 (4) 查看 (2) 宫中 (2) 帮助 (3) (2) 中 (2) 同 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	ブ、选择"新建->用户" 「二〇メ」 「二〇メ」<
 4). 右键菜单刚才新建的组织单位 《 ctive Directory 用户和计算机 《 文件 C 操作 () 查看 O 留中 O 帮助 O) ※ 文件 C 操作 () 查看 O 留中 O 帮助 O) ※ 中 C 图 & 图 C 图 C 图 C 图 C 图 C 图 C 图 C 图 C 图	ブ、洗择"新建->用户" 「二〇× 「二〇× </td
 右键菜单刚才新建的组织单位 右键菜单刚才新建的组织单位 女件② 操作(4) 查看② 留口③ 帮助(5) 女件② 操作(4) 查看② 留口④ 帮助(5) 女件③ 操作的查询 人口、操作的查询 (4) 和目前前 (5) 和目前前 (5) 和目前前 (5) 和目前前 (7) 和目前 (7) 和目前<td>Z, 选择"新建->用户"</td>	Z, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户" 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
 4). 右键菜单刚才新建的组织单位 	次 法择"新建->用户" 「二〇× 」」 20 回 マ @ 回 」」 20 回 0 @ 0 @ 0 @ 回 」」 20 回 0 @ 0 @ 0 @ 0 @ 回 」」 20 回 0 @ 0 @ 0 @ 0 @ 0 @ 0 @ 0 @ 0 @ 0 @
 4). 右键菜单刚才新建的组织单位 	次 法择"新建->用户" 1 1 2 2 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 2 3 2 3 3
 4). 右键菜单刚才新建的组织单位 	次 法择"新建->用户" 1 1 2 2 2 1 2 1 2 1 2 1 2 1 2 1 1 1 2 1 1 1
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 《 Live Directory 用户和计算机 ② 文件② 操作 ④ 查卷 ⑨ 智中 ⑨ 帮助 ⑨ ● ● ○ ③ J ④ ② P ⑨ 可 ⑨ 帮助 ⑨ ● ● ○ ③ J ◎ ● ○ ③ ○ ◎ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	2, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户"
 4). 右键菜单刚才新建的组织单位 	27、选择"新建->用户" ▲□× <tr< td=""></tr<>
 4). 右键菜单刚才新建的组织单位 	2, 选择"新建->用户" 20 回 文 《 2 32 回 文 《 2 38 25 回 文 《 2 38 此規图中设有可显示的项目。 500 50
4). 右键菜单刚才新建的组织单位 《 本は い ひ ひ の の の の の の の の の の の の の の の の の	2, 选择"新建->用户" 20 回 文 《 2 30 □ 文 ⑦ ① ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦
4). 右键菜单刚才新建的组织单位	2, 选择"新建->用户" ***********************************
4). 右键菜单刚才新建的组织单位 《 Live birectory 用户都计算机 《 文件 ② 操作 ④ 查看 ③ 窗口 ④ 得助 ④ 》 本 1 *** Birectory 用户都计算机 》 文件 ③ 操作 ④ 查看 ④ 窗口 ④ 得助 ④ 》 ***********************************	2, 选择"新建->用户" 20 回 文 《 2 32 回 文 《 2 38 此規图中級有可显示的項目。 500 500 此規图中級有可显示的項目。 500 500 500 正述 「一文 2 「一文 3 「一文 3 「
4). 右键菜单刚才新建的组织单位 《 Live birectory 用户都计算机 《 文件 ② 操作 ④ 查看 ③ 窗口 ④ 得助 ④ 》 + five birectory 用户都计算机 》 文件 ③ 操作 ④ 查看 ④ 窗口 ④ 得助 ④ 》 + five birectory 用户和计算机 》 * five birectory 用户 》 * five birectory 用户和计算机 》 * five birectory 用户 》 * five birectory 用户和计算机 》 * five birectory 用户和计算机 》 * five birectory 用户和计算机 》 * five birectory 用户 》 * five birectory 用户 》 * five birectory 用户 》 * five birectory 用户 》 * five birectory 用户 * * * * * * * * * * * * * * * * * * *	2, 选择"新建->用户"
4). 右键菜单刚才新建的组织单位 《 Live birectory 用户都计算机 《 文件 ② 操作 ④ 查卷 ③ 窗口 ④ 得助 ④ 》 + C 窗 上 ▲ ③ × G ② G ③ ③ ④ ● Live birectory 用户和计算机 ● C 窗口 ▲ ③ × G ② G ④ ④ ④ ● Live birectory 用户和计算机 ● C apaters ● Divinio ● Divinio ● C apaters ● Divinio ● Divinio <td>2, 选择"新建->用户"</td>	2, 选择"新建->用户"
4). 右键菜单刚才新建的组织单位 《 Live birectory 用户都计算机 《 文件 ② 操作 ④ 查卷 ③ 窗口 ④ 得助 ④ 》 + ① 窗 法 @ 文 ② ③ ⑤ ③ ④ ④ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	2, 选择"新建->用户"
4). 右键菜单刚才新建的组织单位 《 Live birectory 用户都计算机 《 文件 ② 操作 ④ 查卷 ③ 窗口 ④ 得助 ④ 》 + [1] [2] [2] [2] [3] [3] [3] [3] [3] [3] [3] [3] [3] [3	2, 选择"新建->用户" ***********************************
 4). 右键菜单刚才新建的组织单位 《 tive birectory 用户都计算机 《 文件 ② 操作 ④ 產 ③ 留 ④ 《 物 ⑨ 》 + () 》 * () 》 * () ③ 《 ·) ③ 》 * () ③ * () ④ * () ● * (2, 选择"新建->用户"

	b3a com/实验室	
密码(E):	****	
确认密码(C):	жжжжж	
一 用户下次登录时须	〔更改密码(22)	
▶ 用户不能更改密码	B(S)	
☞ 密码永不过期 (@)		
□ 帐户已禁用 (@)		
□ 帐户已禁用 (0)		

7). 单击"完成",用户创建完毕。这样显示名为"业务软件"的用户就创建好了。重复如 上步骤,在"实验室"这个组织中创建多个用户。

新建对象	用户					×	
S	创建在: h30	2. com/实验	室				
您单击	"完成"后,下列	」对象将被	创建:				
全称:)	业务软件				<u>A</u>	1	
用户登	录名: ywrj@h3c.	com					
用户不(密码永	抱更改密码。 不过期。				<u>•</u>		
		<	上一步 [完成	取消		
Active Dir ② 文件 ② 書	ectoxy 用户和计算机 執作(a) 查看(y) 包	【 [口 ① 報助	00	7.0-			×
⇐ ⇒ E E Active Dire	etory 用户和计算机	字验室	1 个对象	8 C			
(KRADSM (KRADSM	cu		<u>茶整</u> 用户	憲述			5
. 配置iN). 配置排 这里必须将 共享密销	IC 主入设备参数: 等NAS的上行: 月和端口必须-	业务>> 端口(錆 与设备的	>接入业务>> 彭近iMC的端I]配置一致。	接入设备 コ)地址	昏配置 添加到起始	地址和结束	动地址之间
3 业务 >> 报	入业务 >> 接入设备	置				*	12人收藏 @相目
我人夜音重词 设备IP地址	ж Г		刺				
设备名称		_	接入设备类型	所有		查询	重查
接入设备列表							
增加		修改	LOANES	刷新			
共有1条记录,当	前第1-1,第 1/1页。	. 12	20.0.00	1.	1 1 10 Ar 10 M	每页显示:8	15] 50 100 200
L 048-8	а — — — — — — — — — — — — — — — — — — —	ME.	00015 Hummel 4020 11		2人或音乐社	BANE I	n AS

接入配置 (= 共享密钥		
= 共享密钥		
C	h3c	
= 认证端口	1812	 计费端口 1813
* 业务类型	LAN接入业务	(报入设备类型) H3C 💌
备列表		
选择 于. 者们在讨事。	LPW/JU I I TRANSPA	
各名称	设备印地址	
手工增加接	入设备 - ∎icrosoft]	Internet Explorer
手工増加接入	设备	1
. ±====================================	line and	
* NOYULLIQUE	192.168.1.99	
结束IP地址		
	确定	取消
a production of the		
完毕		Natural 🖉
里接λ认证	设备为iMC网管中已	3. 有的被管理设备 在增加接λ设备时可选择上述
的【远律】	0	
业务 >> 接入的	(务 >> 接入设备配置 >> 增加	u接入设备
後入配置		
* 共享密钥	h3c	
* 认证端口	1812	* 计费端口 1813
* 业务类型	LAN接入业务	• 接入设备类型 H3C 🖌
		n Miria da Ch
设备列表		
选择	工増加全部清除	
有0条记录。		
设备名称	设备P地	8址 많答캪号 📕
改完成后请	一定记得手工生效。	
a land and the second second		
赛入业务	*	
赛入业务 約 服务配置管	▲ "理	
姜入业务 □ 服务配置管 ☑ 接入区域制	★ 理 該管理	
後入业务 □ 服务配置管 □ 接入区域第 □ 按)时段	▲ 理 略管理 ※新常理	
後入业务 ● 服务配置管 ● 接入区域第 ● 接入区域第	▲ 理 略管理 略管理	
 後入业务 1) 服务配置管 2) 接入区域第 3) 接入时段第 2) 接入计段第 2) 接入设备 	▲ 理 略管理 踏管理 置	
 金入业务 服务配置管 接入区域第 接入时段第 接入计会都 接入设备都 接入业务招 	★ 理 略管理 略管理 置 指、 別	
 长入业务 服务配置管 接入区域第 通 接入区域第 通 接入时段第 1 接入设备 1 接入业务招 由 接入业务招 由 Porta服务 	★ 理 略管理 路管理 置 計視图 う理	
 ★入业务 ① 服务配置管 浸 接入区域第 ① 接入时段第 ⑦ 接入设备看 ● 接入业务邦 ● Porta服务 □ 业务参数 	★ 理理 略管理 置 指視图 許現 置	
 ★入业务 ① 服务配置信 ※ 接入区域第 ① 接入时段第 ◎ 接入设备看 ● 接入业务邦 ● Portal服务 ○ 业务参数面 ● ※ 系北 	★ 理理 略管理 路管理 置 計 視图 う理 置 置 ま の の の の の 管理 の の の の の の で の の の で の の の の で の	
 ★入业务 服务配置信 接入区域第 接入比段第 接入比条群 サ接入业务邦 中orta服务 业务参数面 ● 公系約 ○ (()) 	★ 理理 略管理 器管理 置 計 初图 許理 置 置 手 業数配置 高で置 ので置 のでする のでする のでする のでする のでする のでする のでする のでする	
 ★入业务 服务配置信 接入区域第 接入比段第 接入设备 接入业务邦 中orta服务 业务参数面 业务参数面 二、系統 二、系統 二、高、正 一、高、正 一、高、二 	★ 理理 部管理 器管理 器 置 外 视图 参理 置 置 素型 置 電子 電子 電子 電子 電子 電子 電子 電子 電子 電子 電子 書 書 書 書	
 入业务 服务配置信 接入区域第 接入比合額 接入比合額 接入业务非 中ortal服务 小务参数面 小务参数面 小家 系約 ○ 本3 	 ★ * 理 * 部管理 * 部管理 * 習 習 者 * 習 者 * 理 * 理 * 型 * = * 2 * = *	
会社劣 1 服务配置信 1 接入区域第 1 接入时段第 1 接入时段第 1 接入计路 1 接入公本第 1 日本公本委委員 1 日本公委委員	 ★ * 理 * 部管理 * 部管理 2置 計 视图 * 算 * 算 * 数配置 範二级配置 • 孤置手工生效 	
 入业务 服务配置信 接入区域第 接入比谷箱 接入北冬邦 中orta服务 小务参数配 小务参数配 小家参数配 小家 系約 二、小家 名 	 ★ * 理 * 略管理 * 習行理 * 認行理 * 部行或配置 * 部行或配置 * 部行重手工生效 	
 ★入业务 服务配置信 接入区域第 接入比易群 接入北易群 接入北易邦 中のれ服务 中のれ服务 小务参数配 小务参数配 小学系教 ○ 本 ○ 本 	★ *理 **********************************	
 ★入业务 服务配置信 接入区域第 強入时段第 接入以る額 接入北条邦 中 Porta服务 中 公系約 ○ 本条数範疇 ○ 本条数範疇 ○ 本条数範疇 ○ 本条数範疇 	★ *理 **********************************	家務委員会工業対応功。
会入业务 1 服务配置管 1 振入区域策 1 接入口段策 1 接入口段策 1 接入口级策 1 接入口级策 1 接入口级策 1 接入公会報 1 サンペ条 1 日本会参数範疇 1 日本会参数電 1 日本会参数電 1 日本会参数電 1 日本会参数電 1 日本会参数 1 日本会 会 1	★ *理 **********************************	癸 系线配置手工生效成功。
 会入业务 金 服务配置信 接入区域第 通 接入以合用 金 接入业务年 由 接入业务年 中 Portal服务 ○ 小务参数面 ○ 小会 小会 ○ 小会 小会 小会 ○ 小会 小会 小会 ○ 小会 小会 小会 ○ 小会 小会 ○ 小会 小会 小会 ○ 小会 小会 小会 小会 小会 ○ 小会 小会 小会 小会 小会 ○ 小会 小会	★ <	ジ ≭城電量手工生效成功. 业务>>服务配置管理>>增加服务配置
	★ <	✔★★##董手工生效成为. 化学为>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC
会入业务 ● 服务配置信 ● 接入区域第 ● 接入设备箱 ● 接入业务邦 ● 中のれる服务 ● 中のれる服务 ● 日本务参数範疇 ● 小公务参数範疇 ● 小公务参数範疇 ● ● ●	★ <	✔★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★
会入业务 1 服务配置管 1 振入区域策 1 振入口段策 1 接入口段策 1 接入计时段策 1 接入计时段策 1 接入计时段策 1 接入计数器 1 サンド教参数範疇 1 日本参参数範疇 1 日本参参数部 1 日本参参数部 1 日本参参数部 1 日本参参数部 1 日本参参 1	★ *理 **********************************	➢ 系統置手工生效成功. 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1x认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。
会入业务 1 服务配置管 1 振入区域策 1 振入可税策 1 接入可税策 1 接入可税策 1 接入公本第 1 接入公本第 1 サンス多参数範 1 日本多参数範 1 日本多参数範 1 日本多参数範 1 日本多参数範 1 日本多参数範 1 日本の参数数範 1 日本の参参数範 1 日本の参参数範 1 日本の参参数範 1 日本の参参数範 1 日本の参参数範 1 日本の参参数 1 日本の参参数 1 日本の参参数 1 日本の参参数 1 日本の参参数 1 日本の参参数 1 日本の参参 1 日本の参考 1 日本の参考 1 日本の参考 1 日本の参表 1 日本の参表 1 日本の参表 1	★ **********************************	永成電手工生效成功。 北京電手工生效成功。 北京電管理>>增加服务配置 充一认证时,若802.1x认证方式设置为eap,则iMC 北原务后缀"要和AD中域的NetBIOS名称一致。 张家正取客 >> 增加系列在 医名意取名 >> 增加系列在 北京
★人业务 1 服务配置信 1 振入区域策 1 接入口段策 1 接入口段策 1 接入计算机 日 按入计算机 日 按入业务邦 日 中方は服务 日 小学参数範疇 日 ● 小学参数範疇 ● 小学参数範疇 ● ③ 客方 ● ③ 客方 ● ③ 客方 ● ② 系参 ● ○ 名参 ● 配置 ● ○ 名参 ● 配置 ● ○ 名参 ● 配置 ● ○ 名参 ● ● ● ○ ○ 名参 ● ○ 名参	★ **********************************	★#####I1#效成功. 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1x认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 ##################################
★人业务 服务配置信 接入区域策 通接入时段前 通接入时段前 通接入时段前 通接入时段前 通接入时段前 通接入时段前 通接入回線第 ● Porta服务 ● Porta服务 ● Outa服务 ● OutaR	 ★ **理 ************************************	✔★##董業工生效成功. ¥务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 ¥##董券経選
	 ★ **理 ************************************	★K#型筆工生效成功。 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 K#ALTO? >> ₩ALESAEZ #SEE
・ 服务配置信 ・ 服务配置信 ・ 振入区域策 ・ 振入にしば ・ ホーム・	 ★ **理 **部管理 **部管理 **部等型 *** *** *** ** **<	★5年豊手工生効成功。 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 84年間第二次 84年間第二次 第2編 第2編 第2編 第2編
会入业务 服务配置管 接入区域第 接入日時第 接入日時第 接入日時第 日本分支参数配 日本分支参数 日本分支参数 日本分支支 日本分支	 ★ **理 ************************************	★5年豊手工生効成功。 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 比例子后缀"要和AD中域的NetBIOS名称一致。 比例子后缀"要和AD中域的NetBIOS名称一致。 比例子后缀"要和AD中域的NetBIOS名称一致。
	★ 評理 評書管理 評書管理 習者 許視图 等理 置 許知图 管理 書 第二日	 ※ 系統監筆工生效成功。 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 器系品質 >> 制施服务后缀
	★ *理 *理 **********************************	 ※ 私始電事工生效成功。 比务>>服务配置管理>>增加服务配置 充一认证时,若802.1×认证方式设置为eap,则iMC 1"服务后缀"要和AD中域的NetBIOS名称一致。 2842002 >> 制造量多起度
会入业务 副 服务配置信 通 接入区域第 通 接入口時段 通 接入口場第 一 接入业务邦 日 按入业务邦数配 日 少务参数配 - 业务参数配 - 小务参数配 - 小会参数配 - 一 公务参数配 - 公会工会 - 公会工会 - 公会工会 - 公会工会 - 公会工会 - 二 二 公会工会 - 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	★ **********************************	X场配置手工生效成功. VS>>服务配置管理>>增加服务配置 在一认证时,若802.1×认证方式设置为eap,则iMC "服务后缀"要和IAD中域的NetBIOS名称一致。 "你們受上類。 "不何度我AGM " "可申請 ● " 董 " "可申請 ● " 董 " " " " "

	1	*					
1 服务配置管理							
🧣 接入区域策略管	管理						
	管理						
📆 接入设备配置							
一 由 接入业务拓扑初	NB						
ー 中 Portal賜冬管理	i						
	1.						
	2 記書						
	略配置						
🔤 🌆 用户导出	Ш						
业务参数配置							
择"增加":							
业务 >> 接入业务 >>	LDAP业务管理	2 >> 服务器配置				χ ατημ.λ.	48 111 0 1
AP服务器列表							
增加 刷新							
有3条记录。 《男女命	医体测的水	肥水明的植材	新华建学 和	副公司安全的	46.70		127 A-24
ŝtAD	3	172.16.100.50	微软活动目录	手工指定	2	×	检测
) tsc节点	3	172.16.100.50	微软活动目录	手工指定	2	×	检测
软AD财务部门节点	3	172.16.100.50	微软活动目录	THE ALL ALL AND A		-	10/01
				于工报定	2	*	10.010
				于工指定	2		12.01
业务 >> 接入业务	>> LDAP业务	管理 >> 服务器	配置 >> 増加LDA	÷⊥指定 P 服务器			12.00
业务 >> 接入业务 DAP服务器信息	>> LDAP业务	管理 >> 服务器	配置 >> 増加LDA	÷⊥18∞ ₽服务器		^	U.CON
业务 >> 接入业务 DAP 服务器信息 基本信息	>> LDAP业务	管理 >> 服务器	配置 >> 地加加LDA	÷⊥18∞ P 服务器	2		
<u>业务 >> 接入业务</u> DAP 服务器信息 基本信息 * 服务器名称	>> LDAP业务 192.16	管理 >> 服务器 38.1.11	配致 >> 地加LDA ====================================	于上指定 P服务器 服务器版本	3	*	
业务 >> 按入业务 : DAP服务器信息 基本信息 : 服务器名称 : 服务器名称	>> LDAP业务 192.16 192.18	管理 ≫ 服务器 38.1.11 38.1.11	記號 >> 地加LDA : :	于上指定 ₽數多器 股务器版本 300	3389		×
<u>业务</u> >> 接入业务 : <u>加AP服务器信息</u> 董本信息 服务器名称 服务器PI地址 服务器PI地址 服务器IP地址 研究317 (国会社)	>> LDAP业务 192.16 192.16 微软法	管理 ≫ 服务器 38.1.11 38.1.11 38.1.11	<u>記録</u> >> 物加LDA = -	于上指定 P服务器 服务器版本 協口 服务同步策略 万年和月常報告報告報	3 389 手工指2 10000	ž	
<u>业务</u> >>	>> LDAP业务 192.16 192.16 微软法 是	管理 >> 服务器 38.1.11 38.1.11 动目录 ✓	nting >> Høbulda = = =	₽上指定 PLM元 服务器版本 端口 服务同步策略 连接服务器静默时长	 3 389 手工指: 1分钟 	ž	
业务 按入业务 DAP服务器信息 基本信息 車服务器名称 服务器内地址 車服务器共型 实时认证 服务器信息 * Base PN	>> LDAP业务 192.16 例软活 是	管理 ≫ 服务器 38.1.11 38.1.11 減目录 ▼ ▼	1232 >> 增加LDA 	₹上指定 P緊勞器 服务器版本 端口 服务同步策略 连接服务器静默时长	■ 3 389 手工指2 1分钟	ž	
<u>业务 >> 投入业务</u> <u>数本信息</u> 重 <u>本信息</u> 服务器名称 服务器件地址 服务器件地址 取务器类型 实时认证 <u>累务器信息</u> ・ Base DN * 管理BDN	>> LDAP业名 192.16 例软语 是 0u=实3 0u=实3	管理 >> 服务器 38.1.11 38.1.11 (动目录) ▼ (○) 絵室,dc=h3c;dc=c 条数件 ou=完全容	記録 >> 増加LDA ・ ・ ・ ・ ・	于上指定 P緊务器 服务器版本 端口 服务同步策略 连接服务器静默时长	3 389 手工指: 1分钟	ž	
<u>业务 >> 投入业务</u> 基本信息 - 服务器名称 ・服务器の地址 ・服务器共型 京时以证 <u>緊合器信息</u> · Base DN · 管理员のN · 管理员を码	>>> LDAP业务 192.16 前致活 点 0u=架3 0u=架3	管理 ≫ 服务器 38.1.11 39.1	negy >> H\$fullDA = = = om (dc=h3c;dc=com	于上指定 P緊告器 服务器版本 端口 服务同步策略 连接服务器静默时长	3 389 手工指7 1分钟	ž	
<u>业务 >> 投入业务</u> 基本信息 - 服务器名称 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务部のの ・服务部の ・取号の ・ 日本会の ・ ・	>>> LDAP业务 192.16 192.18 微软法 点 0u=采引 cn=业5 5AMAc	管理 ≫ 服务器 38.1.11 39.1	negy >> HybulDA = = = om (dc=h3c;dc=com	于上报定 P緊告器 服务器版本 端口 服务同步策略 连接服务器静默时长	3 389 手工指: 1分钟	Ē	
<u>业务 >> 投入业务</u> <u>基本信息</u> - 服务器名称 ・服务器の地址 ・服务器の地址 ・服务器構造 ・思参器信息 ・日本6日 N ・首理员のN ・首理员のN ・首理员のN ・目からのN ・目からのN ・首理員会称 用户名属性名称 用の密码属性名称	>>> LDAP业务	管理 ≫ 重务器 38.1.11 39.1	negy >> HybulDA = = = om (dc=h3c;dc=com	于上报定 P緊告器 服务器版本 端口 服务同步策略 连接服务器静默时长	3 389 手工指: 1分钟	Ē	
<u>业务 >> 投入业务</u> : <u>基本信息</u> - 服务器名称 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器の地址 ・服务器のの ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务器の ・服务部の ・服务部の ・服务部の ・服务部の ・ ・	>>> LDAP业务 1921년 御秋湖 元 0山=梁 6(四=梁 5AMAc	管理 ≫ 重务器 38.1.11 39.1	R2致 >> 増加LDA 。 。 。 。 の M (dc=h3c;dc=com	于上指定 P緊告器 服务器版本 端口 服务同步策略 连接服务器静默时长	3 389 手工指2 1分钟	Ē	
	>>> LDAP业务 1921년 潮秋活 是 0山=梁 6AMAc	管理 ≫ 重务器 38.1.11 39.1 39.2 39.1 39	NEW >> 培知LDA = = = om (dc=h3c;dc=com	于上指定 P緊答器 服务器版本 端口 服务同步策略 连接服务器静默时长 但用中的服务器	3 389 手工指2 1分钟	تو تو	

这里的Base DN就是指所要同步AD中目录的范围,即IMC只同步该Base DN路径下(包含所有子目录)的所有用户。若Base DN设置为根域h3c.com则会同步该AD中的所有用户。

管理员DN指具有查询权限的AD中的用户,可以与Base DN不在同一目录。

管理员DN和BaseDN的命名规则为:从左到右,依次从最小子目录到根目录,中间用 逗号隔开。根目录前缀为dc=,原始目录(如users)和用户名(如"业务软件")前缀 为cn=,新建的目录前缀为ou=,用户名前缀。

对于AD服务器,用户名属性建议修改为saMAccountName

4). 配置测试:在LDAP服务器管理中选择建立的LADP服务器,点击行末的<检测>, 若设置正确,会出现检测成功的提示。

LDAP服务器列表							
均加 易	N#F						
共有4条记录。							
服务器名称	服务器板本	服务器印地址	服务器类型	服务同步策略	修改		配置检测
微軟AD	3	172.16.100.50	徽软活动目录	手工指定	2	×	检测
AD tsc节点	3	172.16.100.50	微软活动目录	手工指定	Z	×	检测
微软AD财务部门节点	3	172.16.100.50	微软活动目录	手工指定	12	×	检测
192.168.1.11	3	192.168.1.11	微软活动目录	手工指定	1	×	检测

5). 配置LDAP同步策略配置: 业务>>接入业务>>LDAP业务管理>>同步策略配置 >> 增加

接入业务 🔿	● 业务 >> 推入业务 >>	>LDAP业务管理>>	同步策略配置						北北人	-
② 服务配置管理	LDAP同步策略列表									
22 接入区域策略管理	HØ 20 AGEE									
一般入时段策略管理	共有3条记录,当前第1-3	5第1/1页。						每页显	示:[[15]	50 100 2
包 接入设备配置	NSTRAK	14888	服务同步发电	用户分组	配置状态	0- M FI	LDAP/0/P	10.00	112	115
● 接入业务拓扑视图 ◎ Portai服体管理	問念AD附备每门下用户	微软AD财务部门节 点	手工指定	未分组	有效	A	Æ	M	×	105
⊖ LDAP\F委管理	同意能設ADtscOUT用P	AD toc To.d.	手工指定	未分组	有效	4	15	1	×	105
臣 服务制配置 日本 用き 無味を改 国、用户写出	局多做就ADusers节点下 用户	数\$PLAD	手工指定	未分组	有效	A	£	1	×	周步

出现如下的配置选项,选择LDAP服务器,配置过滤条件。

* 同步策略名称	121lab	
服务器名称	192.168.1.11	~
* 过滤条件	(&(objectclass=*)(sAMAcco	untName=*))
配置状态	有效	~
同步选项	✓ 自动同步	
	☑ 新增用户及其接入帐号	1.
	✓ 为已存在用户新增接入	桃号

点击下一步选择个列的属性,建议如下图配置,再选择相关的服务。由于AD中的用户密码加密不可逆,不能同步到iMC中,用户每次都会到AD中认证,所以这里的iMC本地密码可以任意设置。

基本信息				
* 用户姓名	cn	~		
* 证件号码	sAMAccountNam	~		
通讯地址	不从LDAP服务器制	~		
电话	不从LDAP服务器	~		
电子邮件	不从LDAP服务器制	~		
* 用户分组	未分组	~		
接入信息				
* 帐号名	eAMAccountivarrie			
失效日期	不从LDAP服务器	~		
* 密码	sAMAccountType	~		
最大闲置时长	不从LDAP服务器	~	分钟	
在线数量限制	不从LDAP服务器	×		
登录提示信息	不从LDAP服务器	~		
接入服务				
服务名		服务后级	安全策略	用户PP地址
✓ 用服部门认证服务			不使用安全策略	
TIN TEADER		hea	不使用完全策略	

6). 同步用户:在LDAP同步配置中选择同步配置,点击行尾的<同步>,则iMC系统会自动同步AD中的所有Base DN中的用户到iMC中。若同步成功会会出现"同步LADP服务器用户成功"的提示。

同步成功后会在LDAP用户管理里中发现 LDAP用户。

-						
绑定用 F	白查询					
帐号名			用户分组	~		
服务名	5	*	用户状态	~		
					查询	重置
脚定用 F	户列表					
增加 解除 同步全部用户		2				
共有2条	记录,当前第1-	2,第1/1页。			每页显示:	8 [15] 50 100 20
	板号名	用	户姓名	用户分组	同步策略名称	用户状态
	luser01	fus	er01	未分组	同步AD财务部门下用户	存在
-						

🖧 增加用户	接入用户信息					
所有用户	投入信息					
多用户附加值息	帐号名	fuser01 🕵LD	AP購定用户			
同用 戶批量操作	失效日期	失效日期				
10 导入用户	最大闲置时长		在线数量限制	在线数量限制		
接入用户视图 🔺	登录提示信息 接入服务					
由.所有接入用户	服务名	服务后缀	安全策略	用户PP地址		
由 所有在线用户	用服飾门认证服务					
	接入设备绑定信息					
17 接入设备列表	设备IP地址		端口号			
· 日志管理	VLAN ID:内层VLAN ID		外层VLANID			
C MATERO	无线用户SSID					
	终端绑定信息					
	计算机名称					
 □ LDAP用户管理 ● 同步微软ADusers ● 一 ● 同步微软ADtscOU 下- ● 同步AD射务部门下 用户 	已绑定的IPMAC					
121lb			近回			

至此, iMC与AD同步完成, 用户可以采用同步过来的用户进行LDAP认证。若需要进行域统一认证, 还需配置域统一认证客户端。请参考下面的配置。



3) 然后会在iNode中发现新的域统一认证连接,再在操作>>配置客户端运行方式中选择"启动域统一认证"。



6. 配置用户电脑

1) 设置PC的网络连接,配置正确的DNS服务器。本例中DNS服务器和AD在同一台服务器上。

果网络文持此功能,则可以; 需要从网络系统管理员处获;	获取自动指视的 IP 设置。否则, 得适当的 IP 设置。
〕自动获得 IP 地址 @)	
●使用下面的 IP 地址(፩):	
IP 地址(L):	192 .168 . 0 . 23
子网掩码(U):	255 . 255 . 255 . 0
默认网关 @):	192 .168 . 0 . 1
)自动获得 DMS 服务器地均	, E@)
◉使用下面的 DNS 服务器버	处址 (2):
首选 DNS 服务器(P):	192 . 168 . 1 . 11
备用 DNS 服务器(A):	

2) 将PC加入域:在我的电脑>>属性>>计算机名>>更改 中输入域名,再输入域管理员的用户名和密码,用户就可以加入到域中了。

统居住	2	×
常規 计算机名	硬件 高级 系统还原 自动更新 远程	
Windows 1	使用以下信息在网络中标识这台计算机。	
计算机描述 @):	ChenBin	
	举例: "Kitchen Computer" 或"Mary's Computer"。	计算机名称更改
完整的计算机名称:	c05672.	可以更改这会计算机的名称和成员身份。更改可能会影响
工作组:	WORKGROUP	x3 hdr4 74 fatH3 f0 hd •
要使用网络标识虑		计算机名 (C):
户,诸单击"网络	ID".	e05672
要重新命名此计算机	机或加入城,兼击"更改"。 (第37 (2))	完整的计算机名称:
	Ex.()	d05672.
		其它 (1)
		意識子
		b3c. con
		〇丁作組(約)
		WORKGEOGP
	職定 取消 应用 (4)	确定 取消

重起PC,至此域统一认证配置完毕。

7. 预期效果:

在PC登陆系统时,使用之前创建的域用户并选择登陆到域

登录到 Windo	ws Windows Server 2003 Standard Edition
Copyright © 1985-:	2003 Microsoft Corporation
用户名(11):	ywrj
密码(P):	****
登录到(L):	CLIENT (此计算机) CLIENT (此计算机) HSC
CH	· · · · · · · · · · · · · · · · · · ·

点击确定后,会在登陆窗口的右侧出现"正在进行域统一认证,请等待"的提示,之后 成功登陆。若在iMC中配置了EAD检查,则登陆到系统后,iNode还会对系统进行安全 检查,并采取相关策略。

四、配置关键点:

- 1、LDAP绑定认证与域统一认证的概念:
- 1) 域统一认证是指登录Windows域时, iNode将用户输入的域帐号和密码先拿来做身份认证, 再放开让windows去做域认证。
- 2) LDAP认证是指iMC/CAMS在收到NAS设备的认证请求后,将用户名和密码送给LD AP服务器(可能是AD)去认证。和Windows域就无关了。
- 2、NAS上802.1x的认证模式必须为pap或eap。

3、iMC的服务和NAS中配置的默认域都必须采用AD中域的NetBIOS名称,默认情况 下是域的第一部分。例如在AD上是h3c.com,则在iMC的服务配置和NAS中的domain 两处都应设置为h3c。

4、管理员DN配置时cn是填写显示名,而非登录名。例如,本案例中显示名为"业务软件",但登录名是"ywrj",此时,管理员DN设置是"业务软件"。

5、对于Base DN的配置,上文中已说明:"就是指所要同步AD中目录的范围,即IMC 只同步该Base DN路径下(包含所有子目录)的所有用户"。现举例说明。例如,用户 的AD设置如图所示,为更让大家理解Base DN,此AD上的域名设置为aaa.net.cn。

E 🙆 COffice 📃	Vsers 15	个对象		
CommonScenarios	名称	英型	描述	
Computers	1 CD19810005	用户	ITS	
(F) (20 Bark	1 CD19840003	用户	ITS	
(a) (a) Beasin Controllars	1 CD19840004	用户	ITS	
E CON	CD19850002	用户	ITS	
H 20 EDBoard	CD19880003	用户	ITS	
E 3 EDOffice	CD19940008	用户	ITS	
TEAT	CD19950003	甩户	ITS	
E CO FIN	CD19980005	用户	ITS	
+ - ForeignSecurityPrinci	CD19990012	用户	ITS	
🙂 😡 X02D	CD19990013	用户	ITS	
🕀 🧭 XB	CI20000009	用户	ITS	
🖲 😡 INSP	CD20020005	用户	ITS	
THI 🙆 🏵	C C120020005	用户	ITS	
🖻 🛃 ITS	C CD20040015	用户	ITS	
Computers	C 1111	田戸	ITS	
🐼 Users		141	110	
🗉 🥝 ISI				
🕀 🎯 XC				
🗈 🥝 OLY 🛁				
10 😡 🕫				
+ D Photo				
E Z PR				
E S PTCOM				

在此图中,用户新建的用户组是"ITS",并在ITS组中又建了两个小分组:Computer和 Users。在Users组里有一个用户名为"IMC"的用户。该用户为管理员。在此例中:

Base dn应该为 ou=users,ou=its,dc=aaa,dc=net,dc=cn

表示需要同步users这个分组中的所有用户。

如果是ou=its,dc=aaa,dc=net,dc=cn,则表示同步its中的所有分组的所有用户。当然就包括同步Users和Computers这两个分组了。

管理员DN 应该为cn=imc,ou=users,ou=its,dc=aaa,dc=net,dc=cn