iMC与AD配合做域统一认证的典型配置

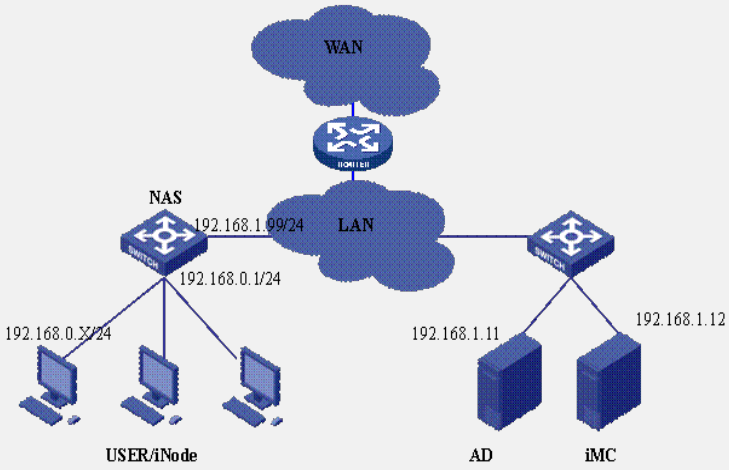
何颖　2008-09-05 发表

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：



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

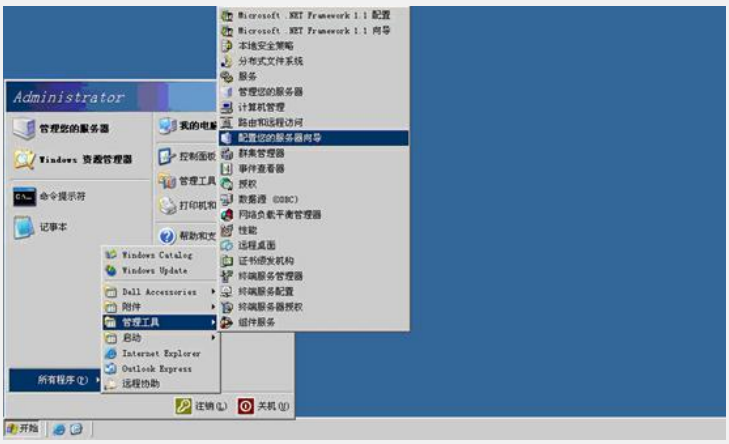
[H3C]Vlan 2

[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EAP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windows 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”

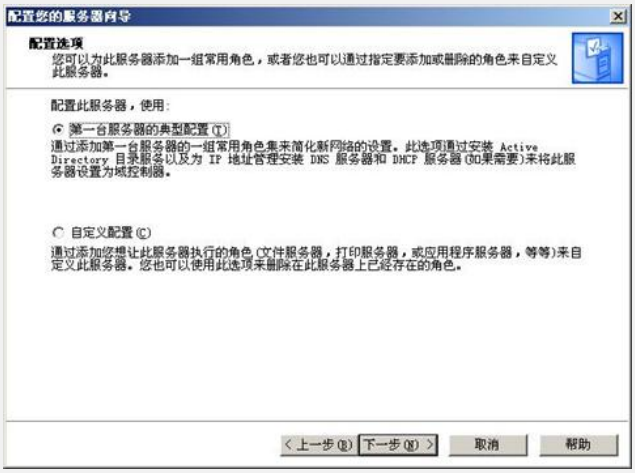


3）．在欢迎界面点击“下一步”

4）．直接点击“下一步”

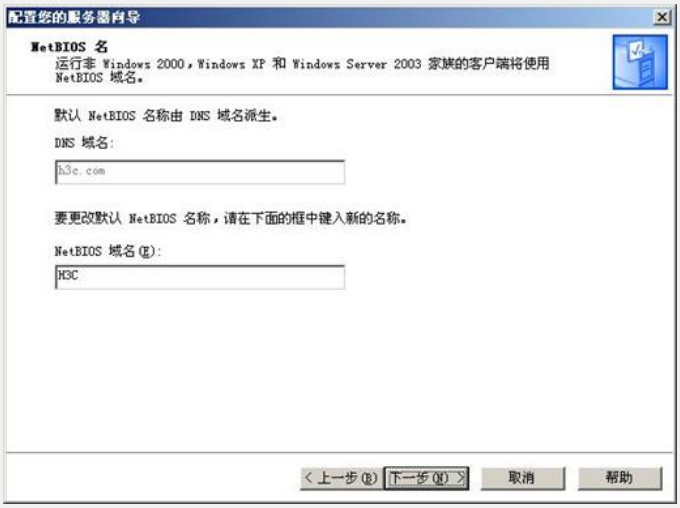
5)．会出现如下进度框

6)．选中“第一台服务器的典型配置”，点击下一步

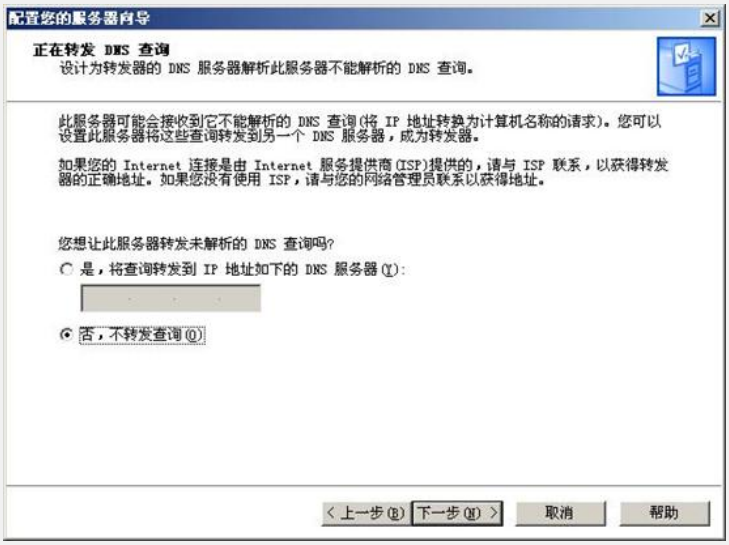


7)．在Active Directory域名一栏输入AD的域名，例如：“h3c.com”，然后点击“下一步”：

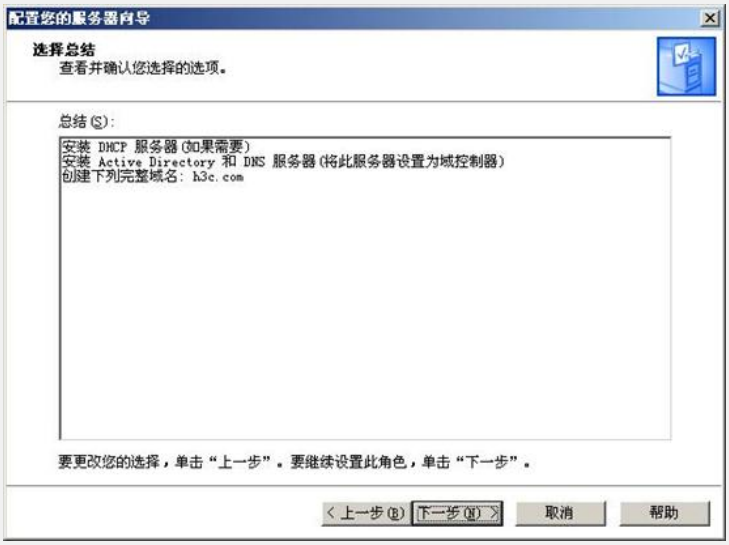
8)．输入NetBIOS域名（推荐采用默认值），然后点击“下一步”：



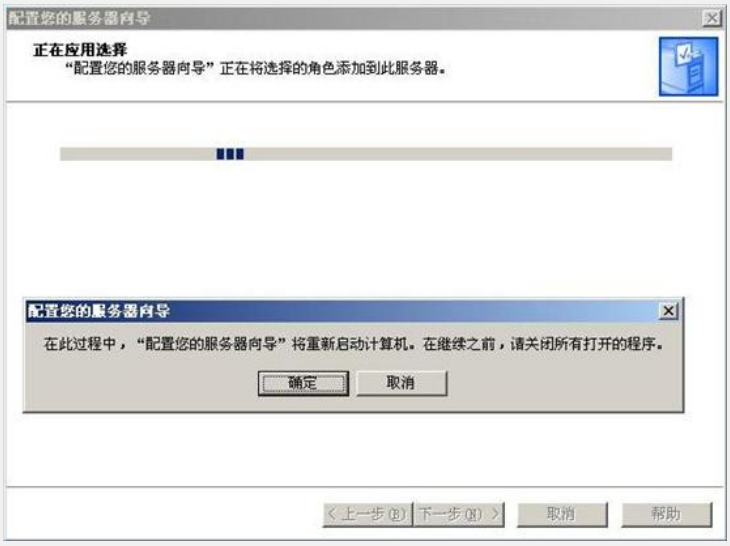
9)．选择“否，不转发查询”，点击“下一步”：



10)．确认选项正确后点击“下一步”

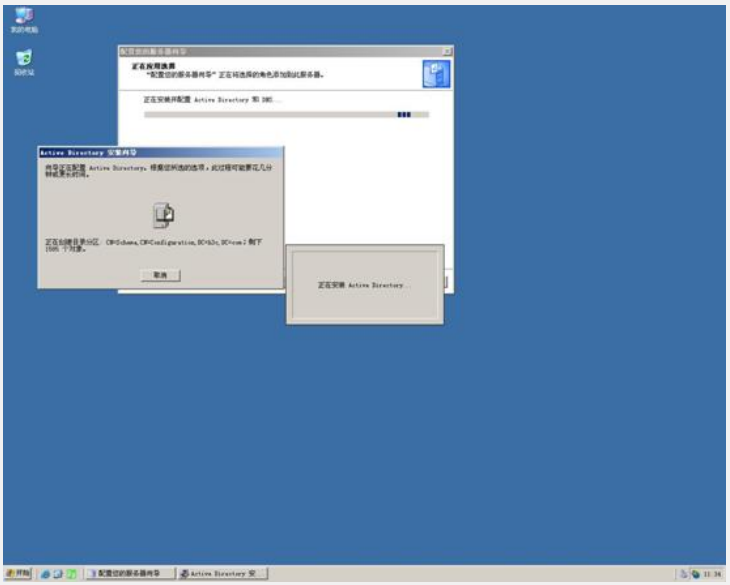


11)．点击“确定”，开始服务器配置



12)．放入操作系统光盘后，点击“确定”：

13)．配置过程当中会重新启动操作系统，无需人工干预，当下一次登陆系统后会继续完成域控制器的配置

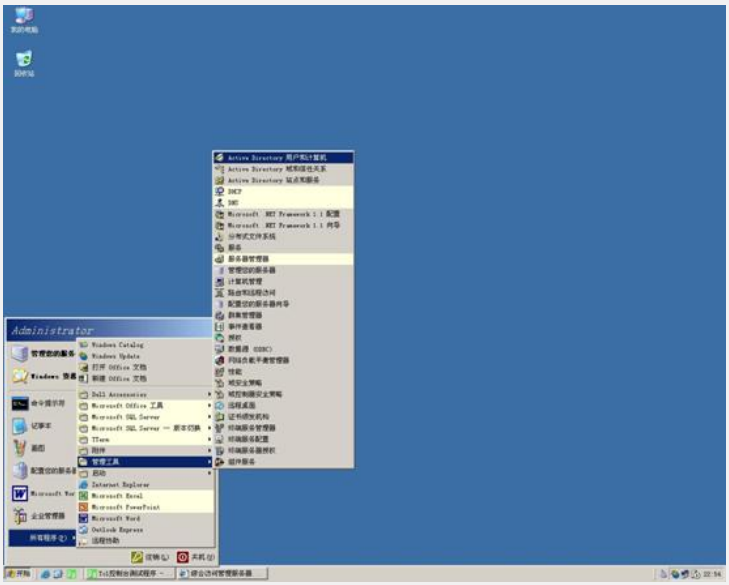


14)．点击“下一步”：

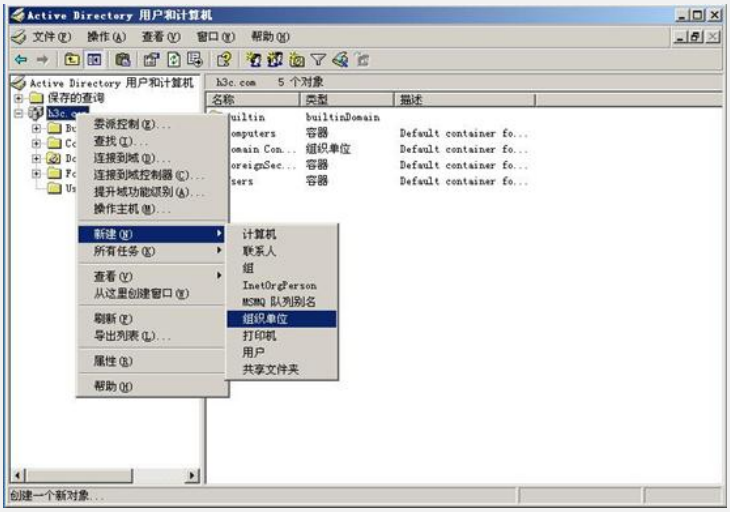
15)．点击“完成”，至此域控制器安装完毕

3．配置AD

1)．配置域用户，选择“开始->所有程序->管理工具->Active Directory用户和计算机”

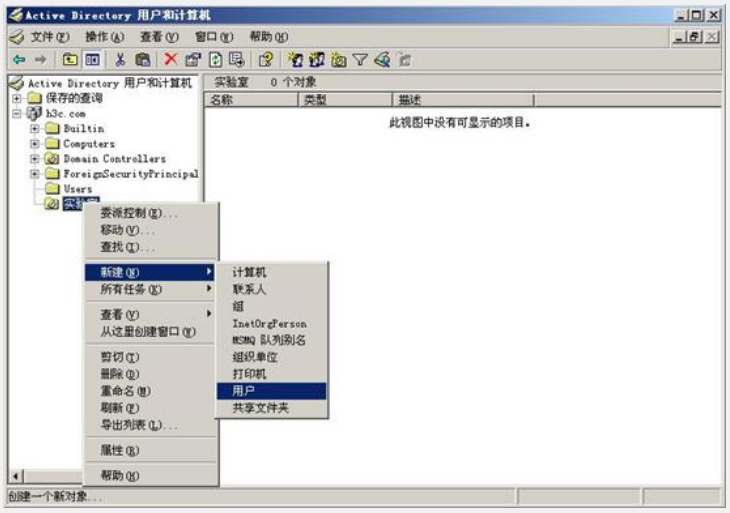


2)．右键菜单服务器图标“h3c.com”，选择“新建->组织单位”：



3)．填写组织单位名称，中英文皆可：

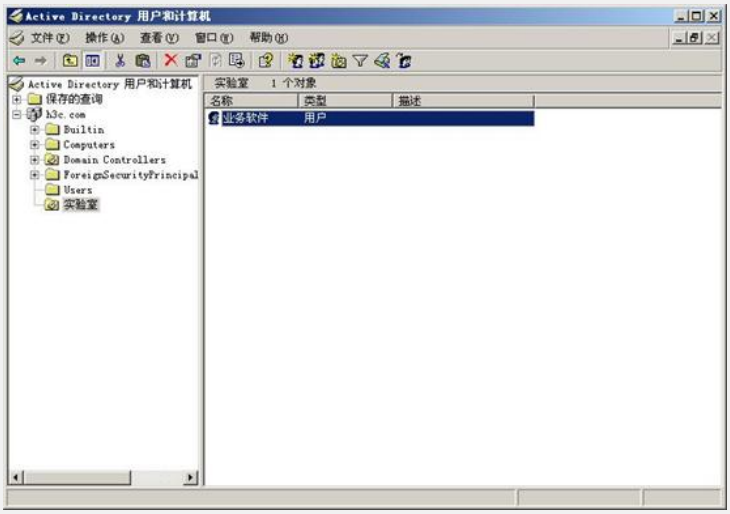
4)．右键菜单刚才新建的组织单位，选择“新建->用户”



5)．填写用户相关信息，用户姓名中英文皆可，登陆名务必填写英文

6）．创建密码，由于Windows 2003的域用户缺省密码策略，创建密码时需保证一定的复杂性。例子中创建为“h3c.com”，同时选中“用户不能更改密码”和“密码永不过期”：

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。



4．配置iMC

1）．配置接入设备参数：业务>>接入业务>>接入设备配置

这里必须将NAS的上行端口（靠近iMC的端口）地址添加到起始地址和结束地址之间。共享密钥和端口必须与设备的配置一致。

如果接入认证设备为iMC网管中已有的被管理设备，在增加接入设备时可选择上述图中的【选择】。

修改完成后请一定记得手工生效。

2）. 配置iMC服务：业务>>接入业务>>服务配置管理>>增加服务配置

服务名可根据需求取名。在做域统一认证时，若802.1x认证方式设置为eap，则iMC服务配置时必须配置“服务后缀”，且“服务后缀”要和AD中域的NetBIOS名称一致。

3）. 配置LDAP服务器：业务>>接入业务>>LDAP业务管理>>服务器配置

选择“增加”:

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。

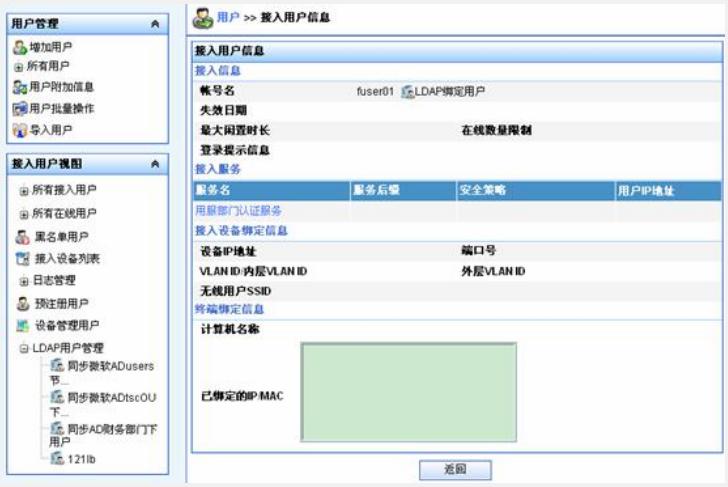
5）. 配置LDAP同步策略配置：业务>>接入业务>>LDAP业务管理>>同步策略配置 >>增加

出现如下的配置选项，选择LDAP服务器，配置过滤条件。

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。

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。

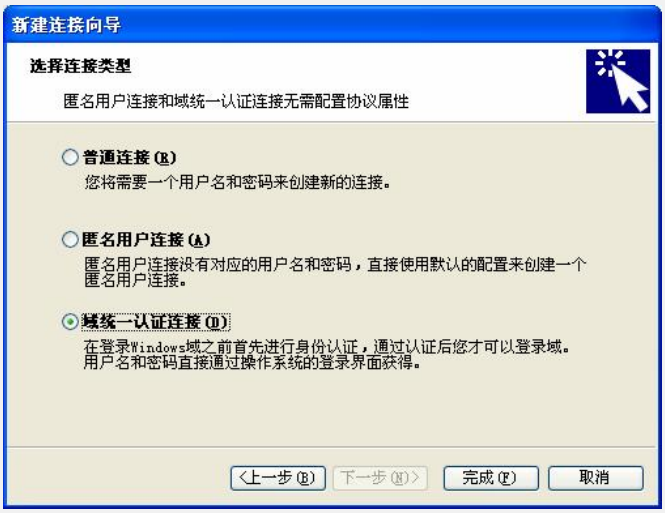


至此，iMC与AD同步完成，用户可以采用同步过来的用户进行LDAP认证。若需要进行域统一认证，还需配置域统一认证客户端。请参考下面的配置。

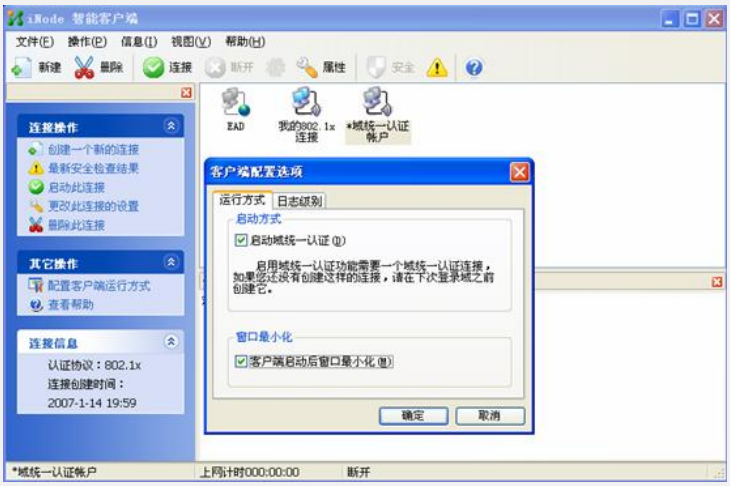
5．配置客户端

1). 在iNode客户端中点击<新建>创建域统一认证了连接

2) 选择基本的认证方式，本例中为802.1X认证，再选择<域统一认证连接>

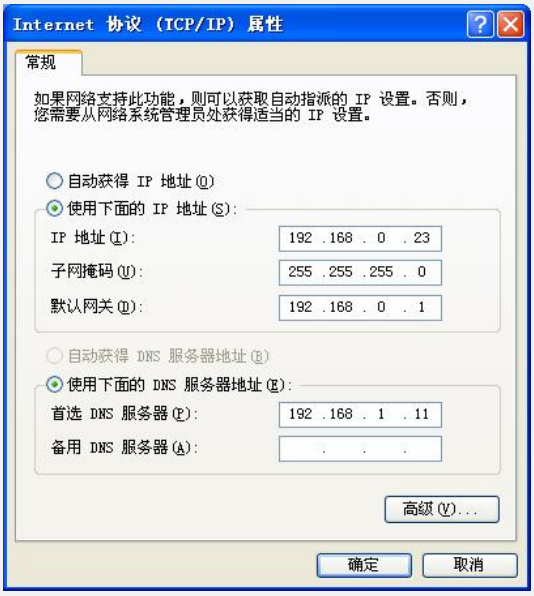


3) 然后会在iNode中发现新的域统一认证连接，再在操作>>配置客户端运行方式 中选择“启动域统一认证”。



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。



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。

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

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。

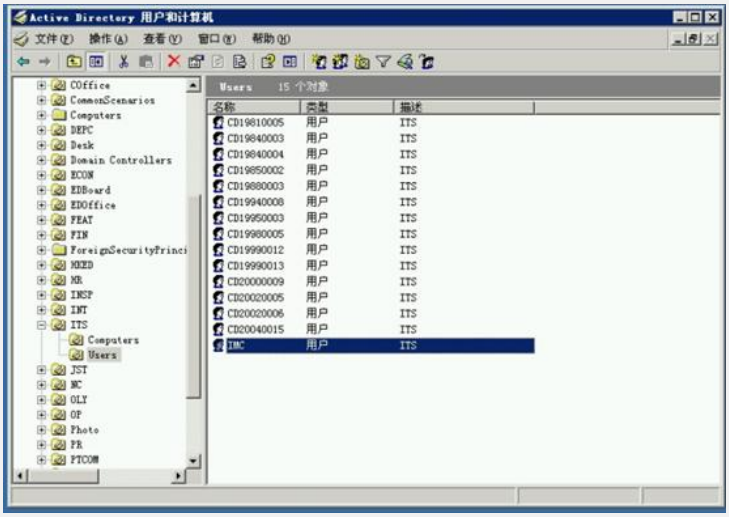
2）LDAP认证是指iMC/CAMS在收到NAS设备的认证请求后，将用户名和密码送给LDAP服务器（可能是AD）去认证。和Windows域就无关了。

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。



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