# 第3章 域网络环境的构建与配置

相对于工作组环境的网络来说，域环境网络具有更高的安全性和可靠性，而且更利于网络资源的集中控制和账户的管理。Windows Server 2003 域网络基础结构的核心就是活动目录 AD(Active Directory)，本章主要介绍活动目录的安装、设置，以及如何在域网络环境下实现简单的用户及组策略的配置与管理等。

## 实训5　域网络环境的构建

### 【预备知识】

AD 指存储网络资源信息的目录，安装了活动目录的服务器称为 DC(Domain Controller)。构建域网络环境，网络中至少要有一台域控制器，当然，也可以存在多台 DC，域网络中的所有资源都可以在 DC 中进行控制，这些资源可以是硬件资源，如打印机、计算机等，也可以是软件资源或用户账户等。本节实训主要基于单域控制器实现域网络环境的搭建。

### 【实训目的】

(1) 掌握如何安装 AD。
(2) 掌握如何将客户机或服务器加入域。

### 【主要任务】

(1) 在 w2003-1 上安装 AD，并同时集成安装 DNS。
(2) 将服务器与客户机加入域。

### 【实训过程参考】

#### 1. 活动目录的安装

(1) 对于要安装活动目录的服务器来说，要满足一些条件，例如必须

是 NTFS 分区，有一组完整静态的 TCP/IP 参数等。由于这些环境在第 2 章搭建基本环境的时候已经完成，这里可以直接单击“开始”→“运行”，在弹出的对话框中输入“dcpromo”，然后单击“确定”按钮，开启活动目录安装向导，如图 3-1 所示。


图 3-1

（2）单击“下一步”按钮，进入如图 3-2 所示的对话框。

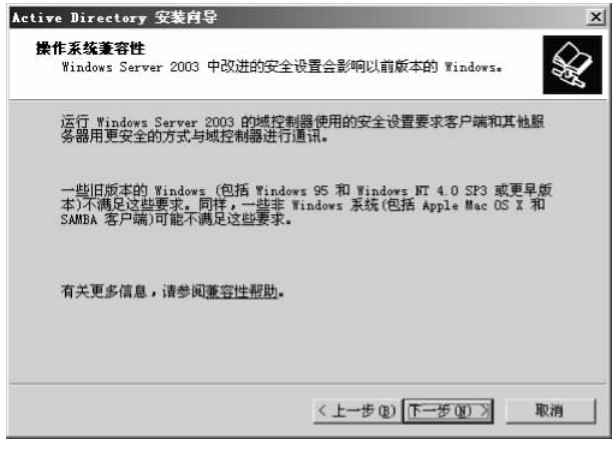


图 3-2

（3）单击“下一步”按钮，进入如图 3-3 所示的对话框。

（4）由于安装的是第一个 DC，所以这里保持默认设置，单击“下一步”按钮，进入如图 3-4 所示的对话框。

（5）当一个网络中有多个域时是可以构成域林的，由于本实训使用单域形式，所以这里保持默认设置，单击“下一步”按钮，进入如图 3-5 所示的对话框。

（6）参考第 1 章的任务要求，输入一个规划好的域名，然后单击“下一步”按钮，进入如图 3-6 所示的对话框。

（7）采用默认设置，单击“下一步”按钮，进入如图 3-7 所示的对话框。

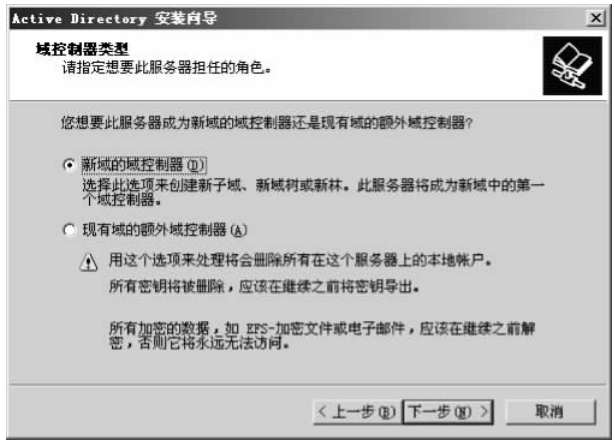
Active Directory 安装向导
域控制器类型
请指定想要此服务器担任的角色。
您想要此服务器成为新域的域控制器还是现有域的额外域控制器?
新域的域控制器(D)
选择此选项来创建新子域、新域树或新林。此服务器将成为新域中的第一个域控制器。
现有域的额外域控制器(A)
用这个选项来处理将合册除所有在这个服务器上的本地帐户。
所有密钥将被册除,应该在继续之前将密钥导出。
所有加密的数据,如 EFS-加密文件或电子邮件,应该在继续之前解密,否则它将永远无法访问。
< 上一步(B)
下一步(N) >
取消

图 3-3

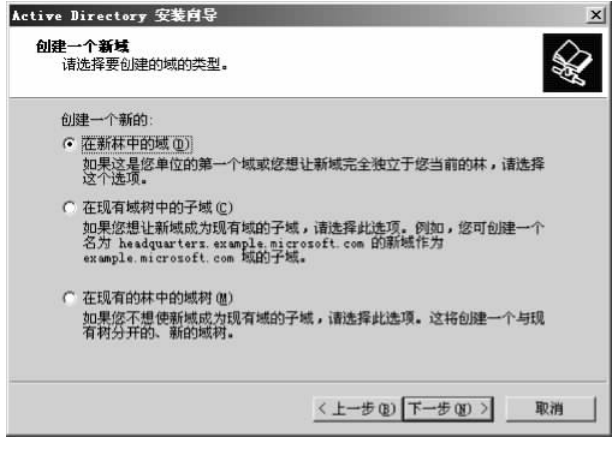
Active Directory 安装向导
创建一个新域
请选择要创建的域的类型。
创建一个新的:
在新林中的域(D)
如果这是您单位的第一个域或您想让新域完全独立于您当前的林,请选择这个选项。
在现有域树中的子域(C)
如果您想让新域成为现有域的子域,请选择此选项。例如,您可创建一个名为 headquarters.example.microsoft.com 的新域作为 example.microsoft.com 域的子域。
在现有的林中的域树(M)
如果您不想使新域成为现有域的子域,请选择此选项。这将创建一个与现有树分开的、新的域树。
< 上一步(B)
下一步(N) >
取消

图 3-4


Active Directory 安装向导
新的域名
请指定新域的名称。
为新域键入一个 DNS 全名(如:
headquarters.example.microsoft.com)。
新域的 DNS 全名(F):
network.com
< 上一步(B)
下一步(N) >
取消

图 3-5

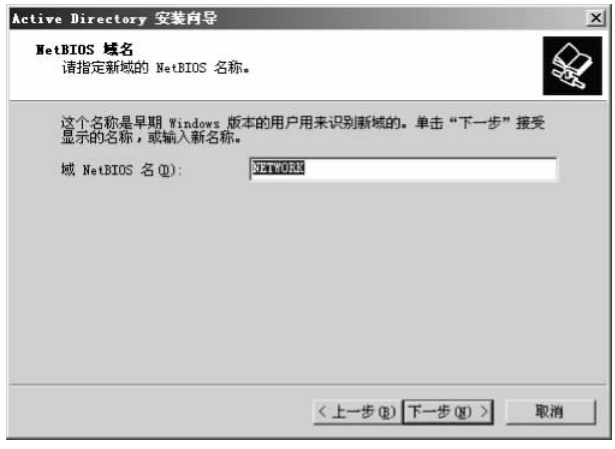


图 3-6


图 3-7

（8）如果是生产环境，不建议将数据库和日志文件放在 C 盘，由于虚拟系统时没有进行分区操作，所以这里采用默认设置，单击“下一步”按钮，进入如图 3-8 所示的对话框。

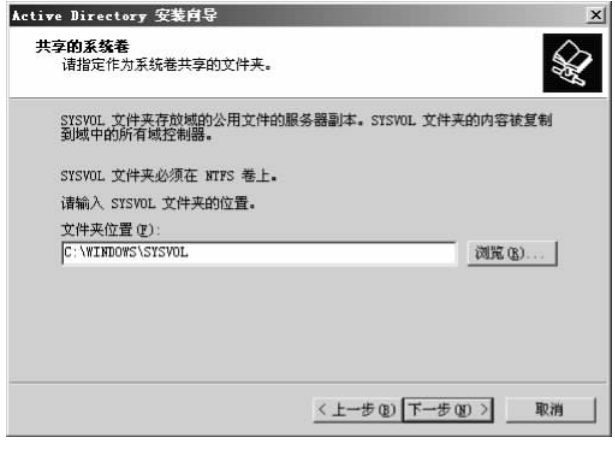


图 3-8

(9) 同样采用默认设置,单击“下一步”按钮,进入如图 3-9 所示的对话框。

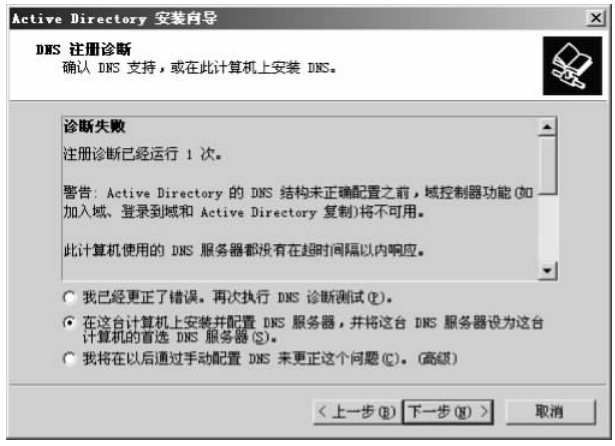


**图 3-9**

(10) 因为要在这台服务器上同时集成 DNS(参看综合拓扑结构图),所以这里选择第二个单选按钮,然后单击“下一步”按钮,进入如图 3-10 所示的对话框。

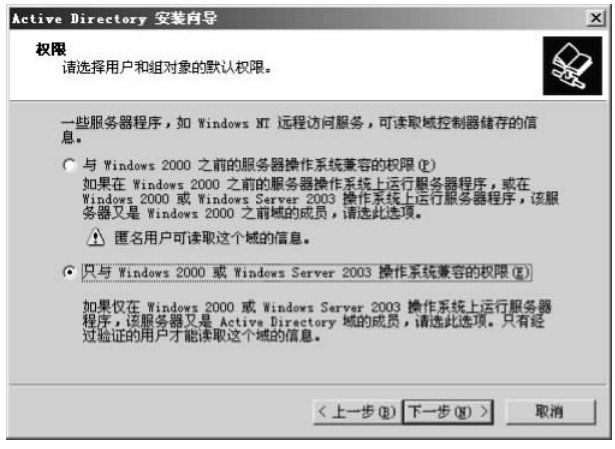


**图 3-10**

(11) 因为这里只有 Windows Server 2003 操作系统,所以采用默认设置,单击“下一步”按钮,进入如图 3-11 所示的对话框。

(12) 如果是生产环境,建议设置比较复杂的密码,这里不设置密码,单击“下一步”按钮,进入如图 3-12 所示的对话框。

(13) 仔细查看域信息,确认无误后单击“下一步”按钮,进入如图 3-13 所示的对话框。

(14) 活动目录开始安装,经过几分钟的等待,活动目录安装完成。重启服务器后,在如图 3-14 所示的登录界面上单击“选项”按钮。

此时用户会发现,这个装有活动目录的服务器会自动登录到 NETWORK 域,注意,此时 Administrator 账户已经是域用户账户了,也就是说,DC 的本地账户会自动变成域用户账户,因为我们一开始并没有给该账户设定密码,所以现在不需要密码就可以登录,单击“确

定”按钮就可以进入系统了。为了满足实训的需要，进入系统后最好创建一个名为“AD”的快照，以方便以后活动目录出问题的时候恢复，这其实是告诉大家每做一个实训最好生成一个状态快照，以备不时之需。

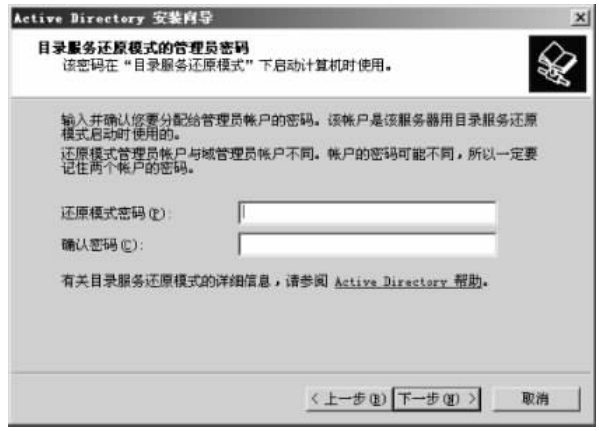


图 3-11

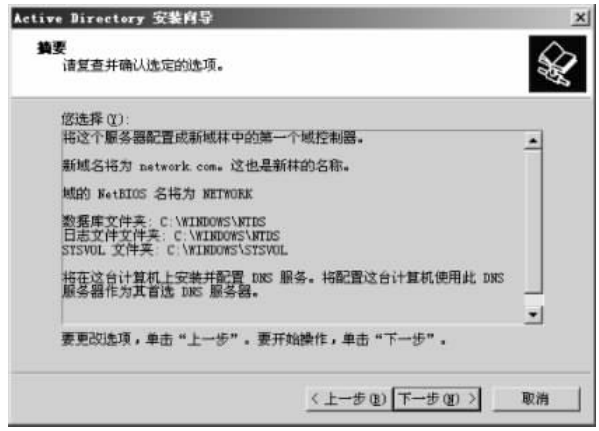


图 3-12


图 3-13


图 3-14

## 2. 将客户机加入域

(1) 如果要加入域并登录到域,必须有域用户账户,在域控制器(注意是 w2003-1 虚拟机)上依次单击“开始”→“管理工具”→“Active Directory 用户和计算机”,打开如图 3-15 所示的窗口。

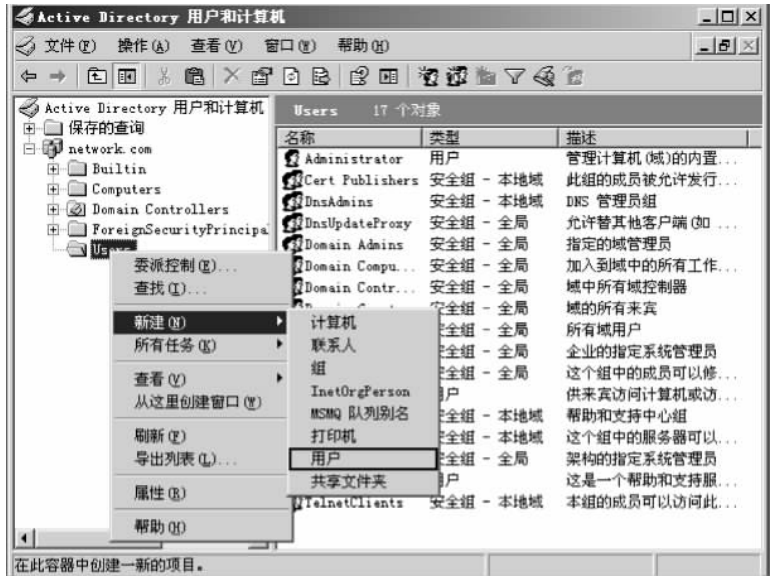


图 3-15

(2) 在图 3-15 中单击 Users,可以看到所有的域用户账户。这里右击 Users,在快捷菜单中选择“新建”→“用户”命令,弹出如图 3-16 所示的对话框。

(3) 这里重要的是用户登录名,它是用来登录域的账号,单击“下一步”按钮,进入如图 3-17 所示的对话框。

(4) 在设置密码时应注意复杂度(密码复杂度设定参看实训六)要求,这里设置的密码为“qaz123@%*”,单击“下一步”按钮,进入如图 3-18 所示的对话框。

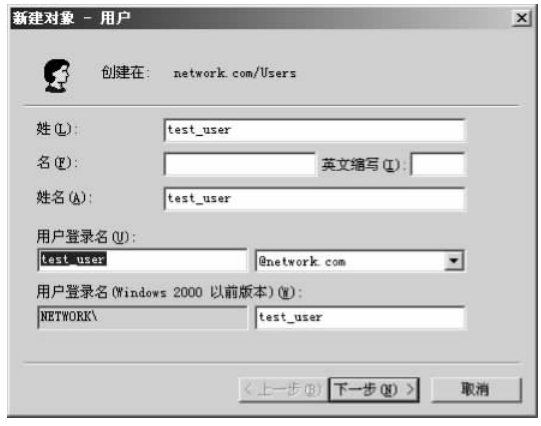


图 3-16


图 3-17


图 3-18

(5) 单击“完成”按钮,则新用户建立完成,如图 3-19 所示。


图 3-19

(6) 这时已经有了一个名为 test_user 的域用户账户,切换到内网测试机(任意一台计算机都可以,这里使用 w2003-8 虚拟机),必须要保证它能够和 w2003-1 连通,在此把这台计算机和 w2003-1 连接到交换机 VMnet1 上,并给这台计算机设置一组静态的 TCP/IP 参数,在 CMD 窗口中用 ipconfig/all 命令查看信息,如图 3-20 所示。

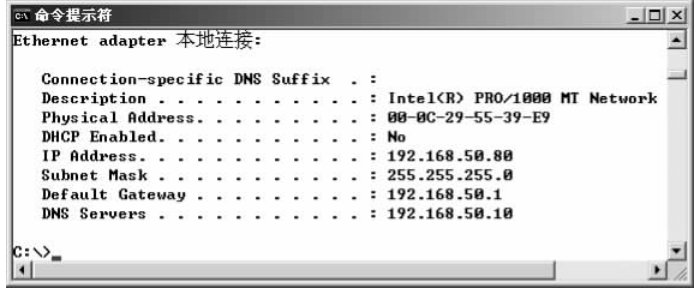


图 3-20

(7) 在 w2003-8 虚拟机上右击“我的电脑”,选择“属性”命令,弹出“系统属性”对话框,切换到“计算机名”选项卡,然后单击“修改”按钮,在弹出的“计算机名称更改”对话框中修改计算机名,如图 3-21 所示。


图 3-21

(8) 单击“确定”按钮,弹出“计算机名更改”对话框,如图 3-22 所示。


图 3-22

(9) 输入刚刚建立的用户名和密码,单击“确定”按钮,弹出如图 3-23 所示的对话框。


图 3-23

(10) 该对话框提示用户已经加入了 network.com 域,单击“确定”按钮后重启系统到登录界面,如图 3-24 所示。


图 3-24

(11) 填好用户名和密码后,一定要选择登录到域,然后单击“确定”按钮就完成了客户机加入域并登录域的过程,系统会为新登录的用户准备属于这个账户的桌面内容。

### 3. 将内网服务器加入域

在第 1 章的任务描述中,要求所有的内网服务器(包括 NAT_VPN 服务器)都要加入域(加入域的服务器称为域成员服务器),对于这些内网服务器来说,一定是先加入域后安装相应服务的,用户可以参照将客户机加入域的方法逐一将这些内网服务器加入到域中。需要

注意的是,因为这些服务器要在加入域后安装一些服务,所以这些服务器登录域的账户需要具有很高的权限,推荐使用 Administrator 账户登录域。Administrator 账户不是本地计算机账户,而是域账户。当然,用户也可以再建立其他具有管理员权限的账户去登录域(在生产环境中就是这么做的,这里只是实训练习),也就是说,在加入域的过程中弹出图 3-24 时应该用管理员账户登录域。因为将服务器加入域的过程与将普通客户机加入域的过程基本上是一样的,这里不再描述其详细步骤,请读者自行完成。

## 【测试验证】

(1) 在 DC 中使用"Active Directory 用户和计算机"窗口查看加入到域的计算机。
(2) 分别使用 Administrator 账户和普通账户登录域,并比较一下权限上有什么不同。

# 实训 6　用户及组策略配置与管理

## 【预备知识】

域环境对域中的对象(如用户)提供了很好的控制功能,再配合使用组策略,能够对这些对象在安全、权限等方面进行非常精细的设置,通过这些设置,不仅可以大大减轻网络管理员的负担,对于网络的安全性和可靠性而言,也非常具有意义。所谓组策略就是指一组标准的安全、控件、规则或选项,网络管理员把这些规则或选项设置在对象上,用于达到网络配置与管理的目的。组策略的功能十分强大,本节实训只是通过简单的设置让读者了解一下如何设置组策略,因为组策略的设置往往是根据网络功能需求进行的,都是为了实现安全或控制目的的一些设置。

## 【实训目的】

(1) 掌握域用户账户的常用配置。
(2) 掌握组策略的设置方法。

## 【主要任务】

通过用户设置和组策略设置实现网络在安全或控制方面的功能需求。

## 【实训过程参考】

### 1. 密码策略设置

(1) 在实训五中建立 user_test 账户的时候,为其设置的密码很复杂,这是因为要满足密码复杂性的要求。这个要求其实就是组策略中的密码策略,用户可以通过修改组策略设

置来修改该密码。首先打开“Active Directory 用户和计算机”窗口，然后右击域控制器，弹出一个快捷菜单，如图 3-25 所示。


图 3-25

(2) 选择“属性”命令，弹出相应的对话框，将其切换到“组策略”选项卡，如图 3-26 所示。


图 3-26

(3) 采用默认组策略，然后单击“编辑”按钮，打开组策略编辑器，如图 3-27 所示。

(4) 找到并单击“计算机配置”下的“密码策略”，用户可以在窗口右侧看到默认启用的密码策略选项，首先双击“密码长度最小值”选项打开其属性，这个属性的两个选项卡如图 3-28 所示。

(5) 用户可以修改这个最小长度值以方便实训，建议将其修改成 3 个字符(考虑到实训的时候较多人喜欢用密码 123)，然而仅仅修改这个长度值就想使用密码 123 是不行的，还

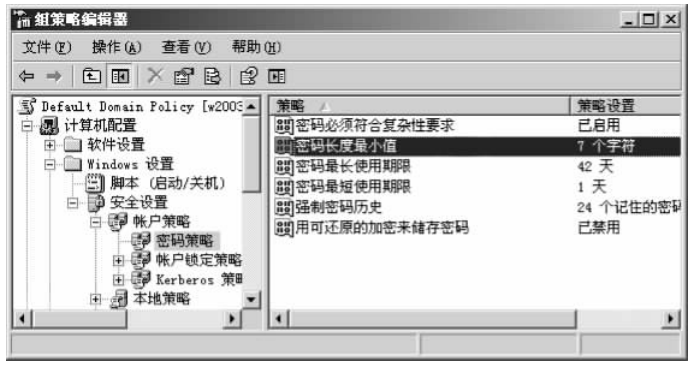


图 3-27

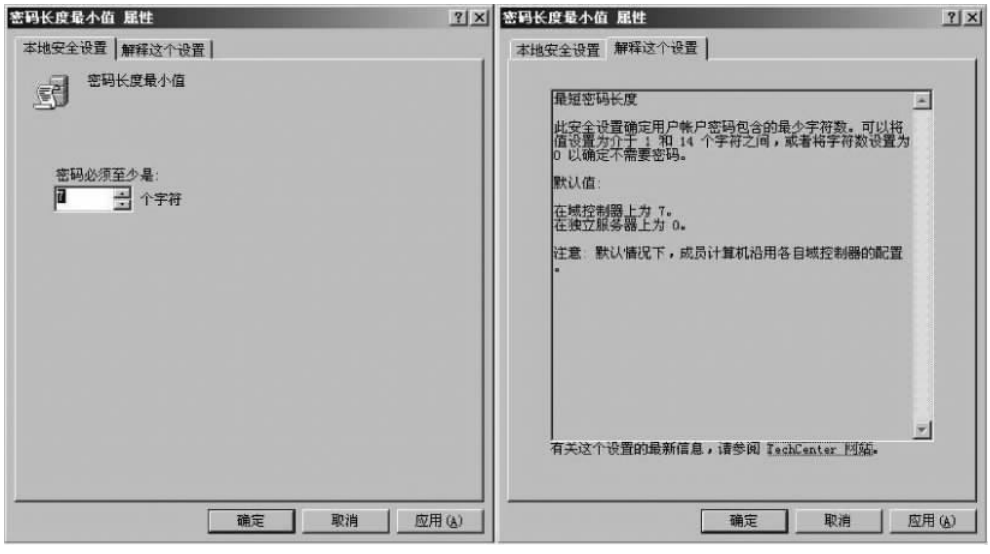


图 3-28

需要降低密码的复杂性,这就需要双击图 3-27 中的“密码必须符合复杂性要求”选项,该选项用来设置密码的复杂性,双击后会弹出如图 3-29 所示的对话框。

(6) 选择“已禁用”单选按钮,如果用户对这个属性不了解,可以在“解释这个设置”选项卡中查看该属性的具体细节。当然,用户也可以尝试设置其他的策略,在图 3-27 中单击左侧的“账户锁定策略”选项,在右侧窗口中会显示如图 3-30 所示的内容。

(7) 双击“账户锁定阈值”选项,弹出如图 3-31 所示的对话框。

(8) 将默认的 0 次无效登录改成 3 次,该账户锁定阈值主要出于对账户安全性的考虑,定义这个阈值后,如果 3 次输入密码不成功,用户账户就要被锁定,只有网络管理员通过对账户进行设置才能解锁。最后,单击“确定”按钮设置完毕,对于其他一些策略请读者自行设置。

**提示**:对于组策略的各种设置,在组策略编辑器中设置好后,一定要在图 3-26 所示的对话框中单击“确定”按钮,并且对组策略进行刷新操作,这样设置的策略才能生效。默认情

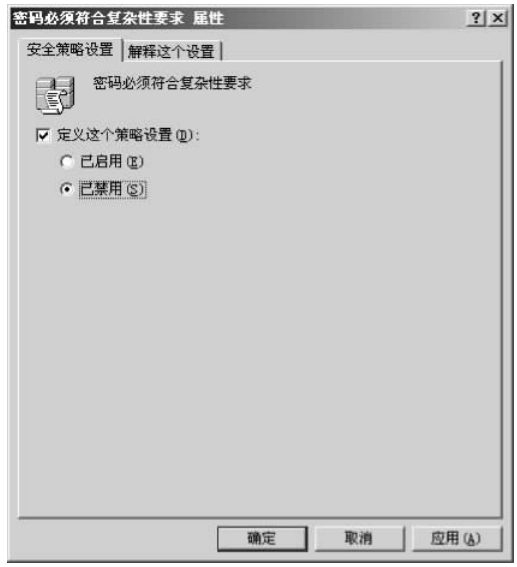


图 3-29

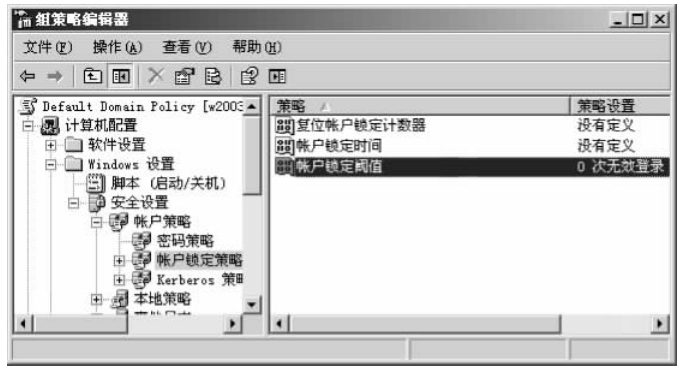


图 3-30

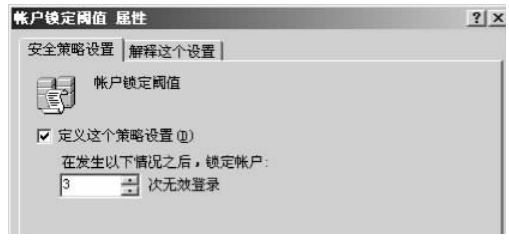


图 3-31

况下，组策略自动刷新的时间是 90 分钟，为了使这里设置的组策略立即生效，以测试和验证实训的结果，需要在 DC 的 CMD 窗口中使用命令 gpupdate/force 强制刷新组策略，有的时候需要强制刷新多次，还可能需要在验证客户机上使用这个命令强制刷新，这样才能保证域控制器、域客户机的组策略同步。

### 2. 域网络登录管理设置

假如公司规定销售部的员工张三只能在周一到周三的8:00到17:00登录公司网络,类似这样的功能实现必须依靠域环境对用户账户进行设置。

(1) 首先在域中新建一个组织单位xsb(销售部),然后右击network.com,在快捷菜单中选择“新建”→“组织单位”命令,如图3-32所示。


图 3-32

(2) 组织单位是域当中的一种容器,用来存放资源,本节实训用它来存放“张三”这个用户的账户,选择“组织单位”命令后,会弹出如图3-33所示的对话框。


图 3-33

(3) 输入组织单位名称,然后单击“确定”按钮,如图3-34所示。

(4) 现在已经建好了一个容器,右击这个容器,在快捷菜单中选择“新建”→“用户”命令,弹出如图3-35所示的对话框。


图 3-34


图 3-35

(5) 用户对这个图很熟悉,在此按照提示建立一个名为 zhangsan、密码为 123(已修改过密码策略)的普通用户,如图 3-36 所示。


图 3-36

(6) 双击这个用户,弹出其相应的属性对话框,切换到“账户”选项卡,如图 3-37 所示。

(7) 在该选项卡中可以设置很多内容,这里只设置账户的登录时间,对于其他内容,请读者根据需要自行设置。单击“登录时间”按钮,会弹出如图 3-38 所示的对话框。


图 3-37

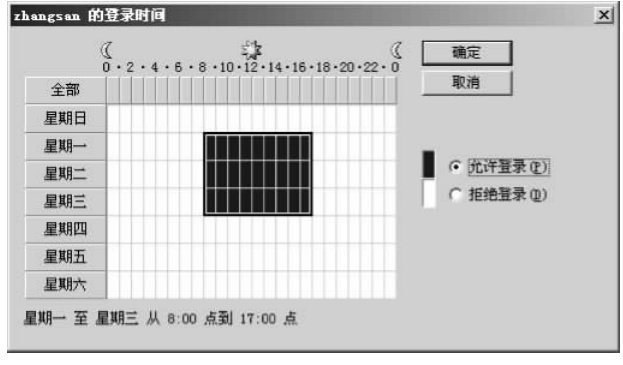


图 3-38

(8) 通过设置实现对 zhangsan 账户的登录时间的控制。当然,用户也可以单击图 3-37 中的“登录到”按钮,在弹出的对话框中设置该账户只能登录到网络中的哪台计算机,有兴趣的读者请自行尝试。

### 3. 用户漫游配置文件设定

为用户创建漫游配置文件,可以保证用户无论从哪台计算机登录到域都可以获取自己的私有文件。对于张三,首先要在服务器上为该用户建立一个用来存储私有文件的共享文件夹,并且只允许张三完全访问。

(1) 在 DC 的 C:\UsersFiles 目录中建立一个文件夹——zhangsan,并设置为共享,如图 3-39 所示。

(2) 单击“权限”按钮,在弹出的对话框中设置权限,如图 3-40 所示。

(3) 删除 Everyone 用户,然后单击“添加”按钮,弹出如图 3-41 所示的对话框。


图 3-39


图 3-40


图 3-41

(4) 单击“高级”按钮,然后单击“立即查找”按钮,对话框如图 3-42 所示。


**图 3-42**

(5) 找到 zhangsan 账户,单击“确定”按钮,关闭“选择用户、计算机或组”对话框,返回如图 3-43 所示的对话框。

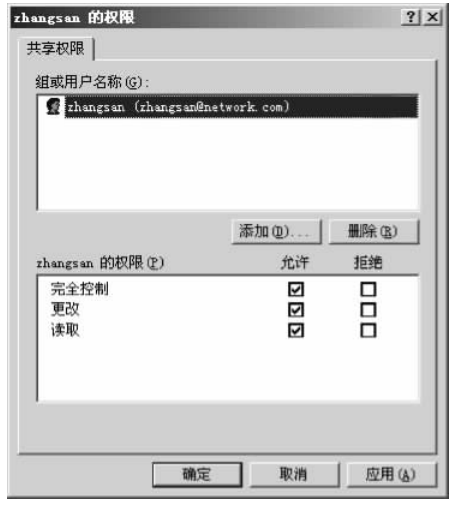


**图 3-43**

(6) 使 zhangsan 账户具有对所创建共享文件夹的完全控制权限,单击两次“确定”按钮后打开如图 3-44 所示的窗口。


图 3-44

(7) 这个共享文件夹用来存放 zhangsan 账户的私有文件,打开 zhangsan 账户的属性对话框,设置“配置文件”选项卡中的选项如图 3-45 所示。


图 3-45

**注意**:设置的配置文件路径的格式是“\\DC 主机名\共享文件夹名”,而且这里为 zhangsan 账户映射了一个虚拟的 Z 盘。

(8) 单击“确定”按钮,完成设置,这样在任意一台加入域的计算机上用 zhangsan 账户登录后,打开“我的电脑”,都会看到如图 3-46 所示的内容。


图 3-46

(9) 图 3-46 中出现了刚才映射的 Z 盘,而且明确地指出了它在 w2003-1 上,也就是服务器 DC 上。用户可以打开这个 Z 盘随意地进行操作,例如新建文件夹或文件等,然后注销这个账户,进入到 DC 的 zhangsan 目录下,会看到如图 3-47 所示的内容。


**图 3-47**

这些文件都是自动存储过来的,这些文件也是下次用户张三无论在哪台计算机上登录域时,将会呈现在 Z 盘的内容,读者可以换一台计算机进行登录、查看。

## 【测试验证】

本章的实训目的非常明确,测试验证也比较容易操作,例如对于实训的第一部分进行验证,只要在 DC 上新建一个用户,设置一个简单的密码,如果能通过就说明所设置的组策略生效了。当然,对于其他一些设置也可以采用相应的测试验证,这里不再赘述,请读者自行测试验证。