第3章 用户管理

3.1 导语：为什么要进行用户管理

在 Windows Server 2008 中，每个用户都必须要有一个帐户，以便利用这个帐户登录到某台计算机，返回访问该计算机的资源，或者利用这个帐户登录到域，然后访问网络上的资源。

Windows Server 2008 的用户管理有两种：本地用户帐户和域用户帐户。

本地用户帐户是创建在非域控制器的“本地安全帐户数据库”内，而不是域控制器的 Active Directory 数据库内。这些非域控制器包含 Windows Server 2008、Windows 2003、Windows 2000、Windows NT 独立服务器或成员服务器等计算机。本地用户帐户只存在于这台计算机内，它们既不会被复制到域控制器的活动目录，也不会被复制到其他计算机的“本地安全帐户数据库”内。当用户利用本地用户帐户登录时，由这台计算机利用其中的“本地安全帐户数据库”检查帐户名称与密码是否正确。

域用户帐户存储在域控制器的 Active Directory 数据库内。用户可以利用域用户帐户登录域，并利用它访问网络上的资源。当用户利用域用户帐户登录时，这个帐户数据会被送到域控制器，并由域控制器检查用户所输入的帐户名称与密码是否正确。在将用户帐户创建在某台域控制器后，这个帐户会被自动复制到同一个域内的其他所有域控制器内。因此，当用户登录时，该域内的所有域控制器都可以检查用户所输入的帐户名称与密码是否正确。

3.2 本地用户帐户

每台 Windows Server 2008 计算机都有一个本地安全帐户管理器(Security Account Manager，SAM)，用户在使用计算机前都必须登录该计算机，也就是要提供有效的用户名与密码。而这个帐户就是创建在本地安全帐户管理器内，这个帐户被称为本地用户帐户；同理，创建在本地安全帐户管理器内的组被称为本地组帐户。

3.2.1 内置本地用户帐户

Windows Server 2008 内置了两个用户帐户。

1. Administrator(系统管理员)

Administrator 拥有最高的权限，用户可以用它来管理计算机，例如创建、更改、删除用户与组帐户，设置安全原则、添加打印机、设置用户权限等。此帐户无法删除，不过为了更安全起见，建议将其改名。

2. Guest(来宾)

Guest 是提供给没有帐户的用户临时使用的,它只有有限的权限。可以更改其名称,但是无法将它删除。此帐户默认是禁用的。

3.2.2 内置本地组帐户

系统内置了许多本地组,这些组本身都已经被赋予一些权限,以便于它们具有管理本地计算机或访问本地资源的权限。只要将用户加入到这些本地组内,这些用户帐户也将具备该组所拥有的权限。

1. Administrators

此组内的用户具备系统管理员的权限,他们拥有对这台计算机最大的控制权,可以执行整台计算机的管理功能。内置的系统管理员帐户 Administrator 即属于此组,而且无法将它从此组内删除。

2. Backup Operators

此组内的用户可以通过 Windows Server Backup 工具来备份或还原计算机内的文件,不论它们是否有权限访问这些文件。

3. Guests

此组内的用户无法永久改变其桌面的工作环境,当用户登录时,系统会为其创建一个临时的用户配置文件,而注销时此配置文件就会被删除。此组默认成员为用户帐户 Guest。

4. Network Configuration Operators

此组内的用户可以执行一般的网络配置功能,例如更改 IP 地址;但是不可以安装、卸载驱动程序与服务,也不可以执行与网络服务器配置有关的功能。

5. Performance Monitor Users

这个组内的用户具备从本地和远程访问计算机的功能。

6. Power Users

为了简化组,这个在旧版 Windows 系统存在的组即将被淘汰。

7. Remote Desktop Users

此组内的用户可以从远程计算机使用终端服务登录。

8. Users

此组内的用户只拥有一些基本权限,但是他们不能将文件夹共享给网络上其他的用户、不能将计算机关闭等。添加的所有本地用户帐户都自动归属于此组。

3.2.3 特殊组帐户

Windows Server 2008 还有一些特殊组帐户,而且无法更改这些组的成员。

1. Everyone

任何一位用户都属于这个组。如果 Guest 帐户被启用,则给 Everyone 授予权限时需小心,因为如果一个在计算机没有帐户的用户,通过网络来登录该计算机时,他会被自动允许使用 Guest 帐户来连接。这样由于 Guest 属于 Everyone 组,他将会具有 Everyone 拥有的权限。

2. Authenticated Users

任何使用有效帐户登录计算机的用户。

3. Interactive

任何在被本地登录的用户。

4. Anonymous Logon

匿名登录。不属于 Everyone 组。

3.3 域用户帐户

3.3.1 域

域，是网络对象的逻辑组织单元。域既是 Windows Server 2008 网络操作系统环境下 Intranet 的逻辑组织单元，也是 Internet 的逻辑组织单元。这些对象如用户、组和计算机等。域中所有的对象都存储在 Active Directory 下。Active Directory 可以常驻在某个域中的一个或多个域控制器下。当一个域与其他域建立了信任关系后，两个域之间不但可以按需要相互进行管理，而且可以跨网分配文件和打印机等设备资源，使不同的域之间实现网络资源的共享与管理。

每个域都是一个安全界限，这意味着安全策略和设置（例如系统管理权利、安全策略和访问控制表）不能跨越不同的域。特定域的系统管理员有权设置仅属于该域的策略。每个域都是一个安全壁垒，因此不同的系统管理员可以在单位中创建和管理不同的域。

3.3.2 Active Directory 活动目录

Active Directory 即活动目录。Windows Server 2008 提供的目录服务，存储若干网络上的对象的信息，并使管理员和用户更方便地查找、使用这种信息。Active Directory 使用结构化的数据存储作为目录信息的逻辑化以及分层结构的基础。

通过登录验证及目录中对象的访问控制，将安全性集成到 Active Directory 中。通过一次登录，管理员可以管理整个网络中的目录数据和单位，并且获得授权的域用户可以访问网络上任何地方的资源。这样基于策略的管理减轻了复杂的管理带来的负担。

活动目录（Active Directory）主要提供以下功能：

（1）基础网络服务——包括 DNS、WINS、DHCP、证书服务等。

（2）服务器及客户端计算机管理——管理服务器及客户端计算机帐户，所有服务器及客户端计算机加入域管理并实施组策略。

（3）用户服务——管理用户域帐户、用户信息、企业通信录（与电子邮件系统集成）、用户组管理、用户身份认证、用户授权管理等，实施组管理策略。

（4）资源管理——管理打印机、文件共享服务等网络资源。

（5）桌面配置——系统管理员可以集中的配置各种桌面配置策略，如：用户使用域中资源权限限制、界面功能限制、应用程序执行特征限制、网络连接限制、安全配置限制等。

（6）应用系统支撑——支持财务、人事、电子邮件、企业信息门户、办公自动化、补丁管理、防病毒系统等各种应用系统。

3.3.3 域用户

域用户帐户是在整个域中的用户帐户，存储在域控制器中的活动目录里面。Windows Server 2008 通过 Active Directory 管理域用户帐户。

1. 域用户帐户类型

Windows Server 2008 系统安装并创建域是自动创建三个用户帐户：Administrator、Guest 和 HelpAssistant。

1) Administrator

Administrator 具有对域的完全控制权，可以在必要的时候为域用户指派用户权利和访问控制权限。该帐户只用于需要管理凭据的任务。该用户无法删除，但可以重命名或禁用该用户。

2) Guest

Guest 由域中没有实际帐户的人使用。帐户被禁用的用户也可以使用 Guest 帐户。默认时，该用户为禁用状态。

3) HelpAssistant

HelpAssistant 用于建立“远程协助”会话。

2. 计算机帐户

和用户帐户类似，计算机帐户提供了一种验证和审核计算机访问网络以及域资源的方法。每个计算机帐户必须是唯一的。

3. 域组

组可用于将用户帐户、计算机帐户和其他组帐户集中到可管理的单元中，使用组而不是单独的用户，可以大大简化网络的维护和管理。

Windows Server 2008 默认组位于 Builtin 容器和 Users 容器中。Builtin 容器包含用本地域作用域定义的组。Users 容器包含通过全局作用域定义的组合通过本地域作用域定义的组。这些组可以被移动到所在域中其他的组或组织单位中，但是不能移动到其他域。

在 Active Directory 中有两种类型的组：发布组和安全组。可以使用发布组创建电子邮件发布组列表，使用安全组给共享资源指派权限。

只有在电子邮件应用程序中，才能使用发布组将电子邮件发送给一组用户。发布组不启用安全，这意味着它们不能列在随机访问控制列表里。如果需要组来控制对共享资源的访问，则创建安全组。

4. 组作用域

组都有一个作用域，用来确定在域树或林中该组的应用范围。有 3 类不同的组作用域：通用、全局和本地域。

通用组的成员可包括域树或林中任何域中的其他组合帐户，而且可在该域树或林中的任何域中指派权限。

全局组的成员可包括在其中定义该组的其他组合帐户，而且可在林中的任何域中指派权限。

本地域组的成员可包括 Windows Server 2008、Windows Server 2003、Windows 2000 或 Windows NT 域中的其他组和其他帐户，而且只能在域内指派权限。

3.4 组 策 略

所谓组策略，就是基于组的策略。它以 Windows 中的一个 MMC 管理单元的形式存在，可以帮助系统管理员针对整个计算机或是特定用户来设置多种配置，包括桌面配置和安全配置。如，可以为特定用户或用户组定制可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个计算机范围内创建特殊的桌面配置。组策略是 Windows 中的一套系统更改和配置管理工具的集合。

组策略将系统重要的配置功能汇集成各种配置模块，供用户直接使用，达到方便管理计算机的目的。组策略设置就是在修改注册表中的配置。组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，比手工修改注册表方便、灵活，功能也更加强大。

组策略包含着计算机配置与用户配置两部分，其中计算机配置只对计算机环境有影响，而用户配置只对用户工作环境有影响。

可以通过以下两个途径来设置组策略：

1. 本地计算机策略

本地计算机策略可用来设置某一计算机的策略，这个策略内的计算机配置只会被应用到这台计算机，而用户配置会被应用到在此计算机登录的所有用户。

2. 域内的组策略

在域内可以针对站点、域或组织单元来设置组策略，其中的域组策略内的设置会被应用到域内的所有计算机与用户，而组织单元的组策略会被应用到该组织单位内的所有计算机用户。

对加入域的计算机来说，如果其本地计算机策略的设置与域或组织单元的组策略设置有冲突，则以域或组织单元组策略的设置优先，也就是此时本地计算机策略的设置无效。

3.5 应用案例 1：管理本地用户帐户

3.5.1 案例内容

DHY 是国内知名电子产品生产企业，公司主要生产移动存储、MP3、MP4、显卡、主板等电子产品。公司正处于快速成长期，在 2～3 年中，人员规模从原先仅 100 人的团队，迅速扩张为现在的 800 人规模。

在公司的数据中心，有多台 Windows 2008 Server 服务器，这些服务器要有专人来维护，作为数据中心的负责人，你应该做如下设置：

(1) 在所分配的 Windows 2008 Server 服务器上为不同的维护人员分别创建登录帐户；

(2) 每台 Windows 2008 Server 服务器需有多名人员进行维护，因此要有多个用户使用 1 台计算机；

(3) 为了便于管理员管理这些帐户，需要按照维护人员的责任管理这些新的登录帐户；

(4) 不同维护人员对计算机上的资源使用的权限不一样；

(5) 为了保证计算机安全，必须保证计算机登录帐户的密码安全；

(6) 维护结束后，禁用这些新建登录帐户。

3.5.2 案例分析

本案例中不允许维护人员访问公司域，只允许他们使用本地计算机，因此，这里要为这些维护人员创建本地用户帐户和组，并对这些本地用户帐户进行管理。

（1）为维护人员创建本地用户帐户；

（2）每台计算机供多个维护人员使用，根据案例要求，要创建与维护人员职责对应的本地组，并且将新建本地用户帐户按照员工其职责，移入相应的本地组；

（3）设置本地帐户锁定和密码策略；

（4）根据实际需要设置本地组和本地用户帐户的权限；

（5）禁用这些新建本地用户帐户。

3.5.3 案例实施过程

1. 创建本地用户帐户

本地帐户和组的管理工具位于“计算机管理”控制台中，具体操作是：单击“开始”|“管理工具”|“计算机管理”选项，展开目录树中的“本地用户和组”就可以进行帐户管理了。

操作：在目录树的“用户”上右击，选择“新用户”命令，如图 3-1 至图 3-4 所示。

图 3-1　本地用户和组

图 3-2　新建用户

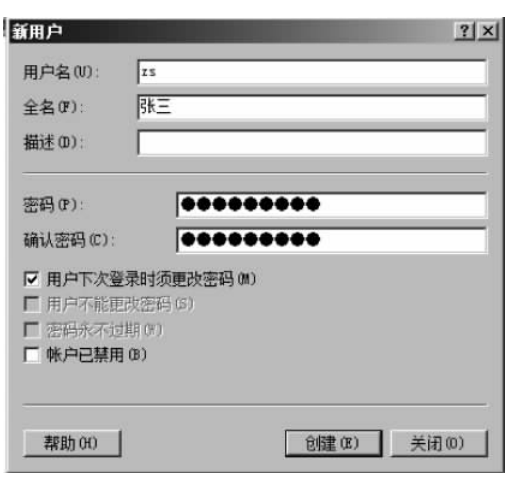

图 3-3　设置用户密码等属性

图 3-4　创建好用户

参数：

(1) 用户名：长度不能超过 20 个字符，同一台计算机中的帐户不能重名。

(2) 密码：长度不能超过 128 个字符。

(3) 密码选项。

说明：只有 Administrators 组和 Power Users 组的成员有权创建用户帐户。

2. 创建本地组

本地帐户和组的管理工具位于“计算机管理”控制台中：单击“开始”|“管理工具”|“计算机管理”选项。展开目录树中的“本地用户和组”就可以进行本地组管理。

操作：在目录树的“组”上右击，选择“新建组”命令，如图 3-5 所示。

3. 设置帐户所在的组

新建的帐户默认属于 Users 组。更改帐户所在的组主要有两种方法：

(1) 打开帐户的属性界面，在“隶属于”选项卡中设置该用户所在的组。

(2) 打开组的属性界面，在“成员”选项卡中设置该组的成员，如图 3-6 所示。

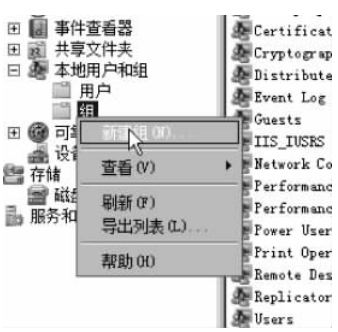

图 3-5　新建组

图 3-6　添加组成员

这里要注意，由于一个帐户可同时属于多个组，其权利是各组权利的叠加，所以如果想限定用户只属于某个组，应该把它从其余组中删除。

Administrators 组的成员有权将帐户加入任意组中，PowerUsers 组的成员只有权将帐户加入 Power Users 组、User 组和 Guest 组。

4. 更改帐户密码

方法一：用帐户本地登录计算机，按下 Ctrl＋Alt＋Del 组合键，选择“修改密码”功能。这种方法需要先输入正确的旧密码，再输入新密码。

方法二：用一个管理员帐户登录计算机，打开“计算机管理”控制台，在相应帐户上右击，选择“设置密码”命令，如图 3-7 所示。

图 3-7　更改密码

这种方法不需要输入旧密码，可直接输入新密码。

说明：方法二应该只用于忘记密码的情况，这时由管理员为你设置一个新密码。这种方法会导致该帐户的一些信息丢失，比如加密的信息会打不开等。

5. 禁用帐户

如果一个帐户暂不使用，可以禁用它，将来需要时再启用。

方法：用管理员身份登录计算机，打开“计算机管理”控制台，打开相应帐户的属性界面，选中“帐户已禁用”复选框，如图 3-8 所示。解除禁用时只需取消选中该复选框即可。

图 3-8　禁用帐户

6. 设置本地帐户锁定和密码策略

为了保护计算机的安全，可以通过设置一些安全策略强制使用者养成使用计算机的良好习惯。

打开“本地安全策略”控制台：单击“开始”|“管理工具”|“安全设置”选项。展开目录树中的“帐户策略”选项。设置某项策略时，只需双击该项策略就可以进行设置，如图 3-9、图 3-10 所示。

图 3-9　密码策略

图 3-10　帐户策略

主要设置项目有：

(1) 密码必须符合复杂性要求——默认为禁用。如果启用了，则用户在设置密码时必须使用复杂密码，即必须包含字母、数字和符号。

(2) 密码长度最小值——默认为 0，此时可以设置空密码。设置后就可以要求用户必须使用足够长的密码。

(3) 密码最长使用期限——默认为 42 天。当超过此期限时，用户在登录时会被要求更改密码。

说明：如果一个帐户的密码选项设置为“密码永不过期”，则该帐户的密码不受该期限限制。

(4) 密码最短使用期限——默认为 0，此时用户可随时更改密码。如果设置为 1 天，则用户更改密码后，必须在 1 天之后才能再次更改密码。

(5) 强制密码历史——默认为 0，此时用户设置的新密码可以和旧密码相同。假如设置为 3，则用户设置的新密码不能与最近 3 次用过的密码相同。

(6) 帐户锁定阈值——默认为 0，此时用户输入错误密码不会导致帐户锁定。假如设置为 5，则当一个用户登录时，如果输入了 5 次错误的密码，则该帐户将被自动锁定。

(7) 帐户锁定时间——假如该值设置为 10 分钟，则当一个帐户被锁定后，过 10 分钟就自动解除锁定。如果该值设置为 0，则该帐户不会自动解锁，只能由管理员手工解锁。

说明：设置锁定功能的目的是防止有人用猜测的方式破解密码。如果一个帐户被锁

定，则在解锁之前，该帐户不能登录计算机。

解除锁定的方法：可以耐心等待，直到系统自动解锁。也可以由管理员登录计算机，打开该帐户的属性界面，取消选中“帐户已锁定”复选框。

7. 本地用户权限分配

（1）权利设置在“本地安全设置”控制台中：单击“开始”|“管理工具”|“本地安全设置”选项。在目录树中选择“本地策略”→“用户权限分配”选项，如图 3-11 所示。

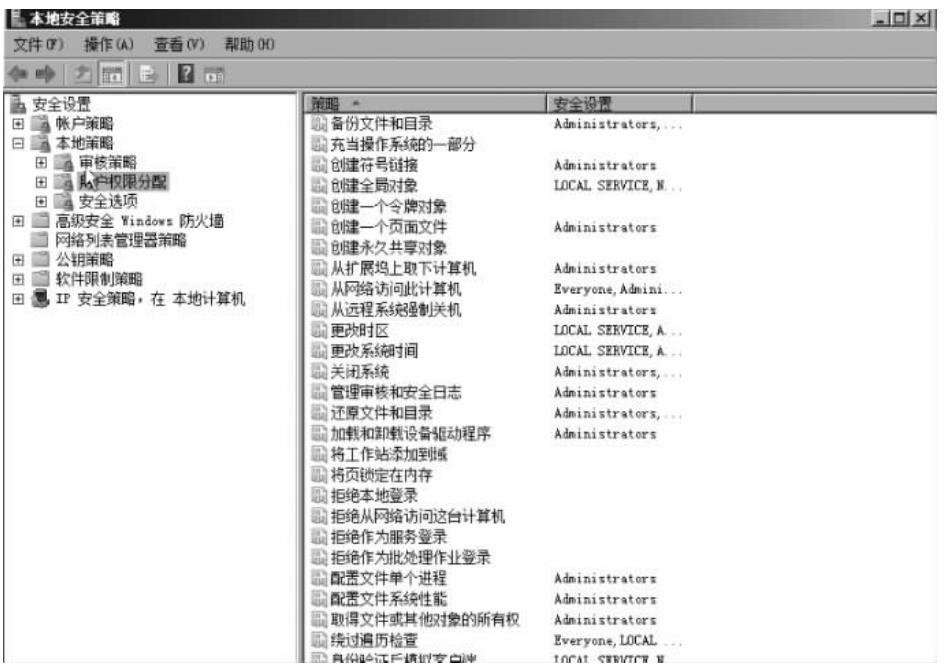

图 3-11　用户权限分配

（2）在右侧的窗口中列出的是各种权限，以及拥有权限的用户和组。设置时，只要双击权利名称，就可以修改拥有该权限的用户和组了，如图 3-12 所示。

图 3-12　添加用户权限

说明：有些权限同时具有“允许”和“拒绝”两种，如有“允许本地登录”权限，也有“拒绝本地登录”权限。如果一个用户或组同时设置了这两种权限，则“拒绝”权限优先。

3.6 应用案例 2：创建域并管理域用户

3.6.1 案例内容

DHY 是国内知名电子产品生产企业，公司主要生产移动存储、MP3、MP4、显卡、主板等电子产品。公司正处于快速成长期，在 2～3 年中，人员规模从原先仅 100 人的团队，迅速扩张为现在的 800 人规模。

随着公司规模的扩张，公司加快了信息化建设及管理的步伐，先后购置了 10 台服务器，其中网站服务器 1 台，邮件服务器 3 台，内部 OA 服务器 1 台，FTP 服务器 1 台。公司很多业务都是基于 B/S 系统的，相应的处理服务器有 4 台。同时为了公司对外交流的应用，公司申请了 dhynet.com 域名，为了更好地进行集中化的管理，公司决定采用基于 Windows 活动目录的管理方式。同时公司要求对员工使用公司域做到如下管理：

（1）为每个正式加入公司的新员工创建域用户帐户；

（2）根据员工所在部门，统一管理新员工；

（3）在培训结束前禁止这些用户帐户；

（4）在培训结束后启用这些用户帐户；

（5）正式工作时，禁止员工在工作时间外登录域。

3.6.2 案例分析

本案例中，作为管理员要为新员工创建域用户帐户，并进行管理。

（1）为公司创建域，创建网络当中的第一台域控制器；

（2）为新员工创建域用户帐户，因新建域用户很多，可以使用复制用户帐户功能；

（3）为部门创建域组，并将用户按其所在部门移入相应组；

（4）暂时禁用这些域用户帐户，在新员工培训结束后，启用这些域用户帐户；

（5）设置域用户登录时间。

3.6.3 案例实施过程

1. 创建域

（1）首先将计算机的 IP 地址设置为 10.0.0.1，并完成相应“子网掩码”及“首选 DNS 服务器”的设置，如图 3-13 所示。

（2）单击“开始”按钮，选择“管理工具”→“服务器管理器”命令，如图 3-14 所示。

（3）在“服务器管理器”对话框中，单击“角色”选项，如图 3-15 所示。

（4）在如图 3-15 所示的对话框中，在右侧的“角色摘要”处单击“添加角色”选项，在弹出的“添加角色向导”对话框中，选中“Active Directory 域服务”选项，然后单击“下一步”按钮，如图 3-16 所示。

（5）此时会出现“Active Directory 域服务安装向导”对话框，单击“下一步”按钮，如

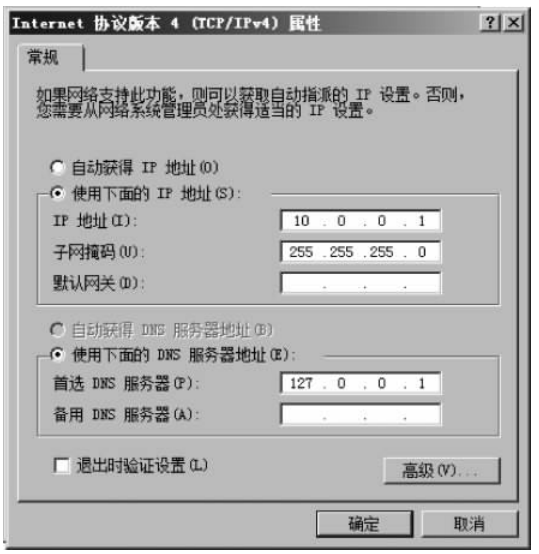

图 3-13　IP 地址的设置

图 3-14　安装 DNS 服务

图 3-17 所示。

（6）出现如图 3-18 所示对话框之后，选择“在新林中新建域”单选按钮，并且单击“下一步”按钮。

（7）之后，在出现的“命名林根域”窗格中输入域名 dhynet.com，并且单击“下一步”按钮，如图 3-19 所示。

图 3-15　服务器管理器

图 3-16　添加 Active Directory 域服务

图 3-17　Active Directory 域服务向导

图 3-18　在新林中新建域

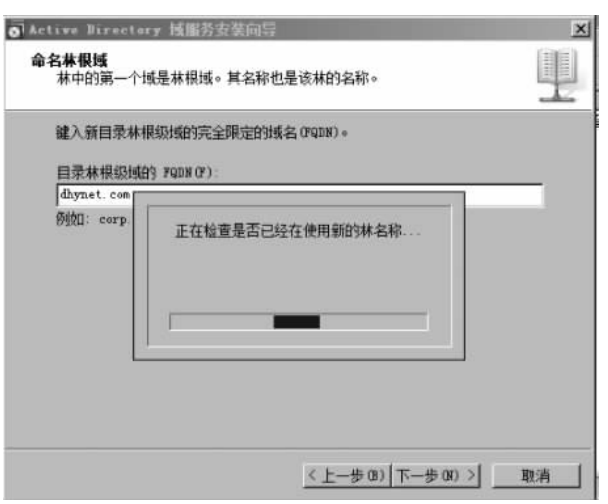

图 3-19　输入域名

（8）在“设置林功能级别”窗格中选择 Windows 2000 选项，并单击“下一步”按钮，如图 3-20 所示。

图 3-20　选择林功能级别

（9）在“设置域功能级别”窗格中选择“Windows 2000 纯模式”选项，并单击“下一步”按钮，如图 3-21 所示。

图 3-21　设置域功能级别

这里向导会在这台服务器上安装 DNS 服务器，同时第一台域控制器也必须是全局编录服务器的角色，第一台域控制器不可以是只读域控制器，如图 3-22 所示。

之后出现如图 3-23 所示界面，其中数据库文件夹：用来存储 Active Directory 数据库。

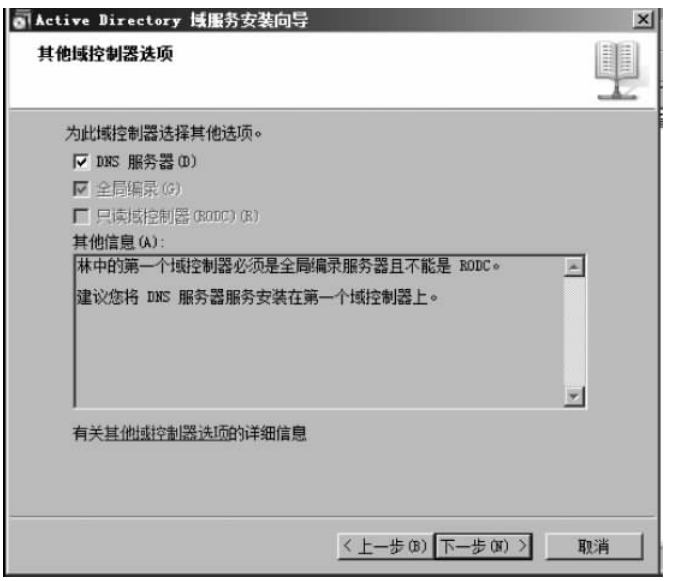

图 3-22　选择 DNS 服务器

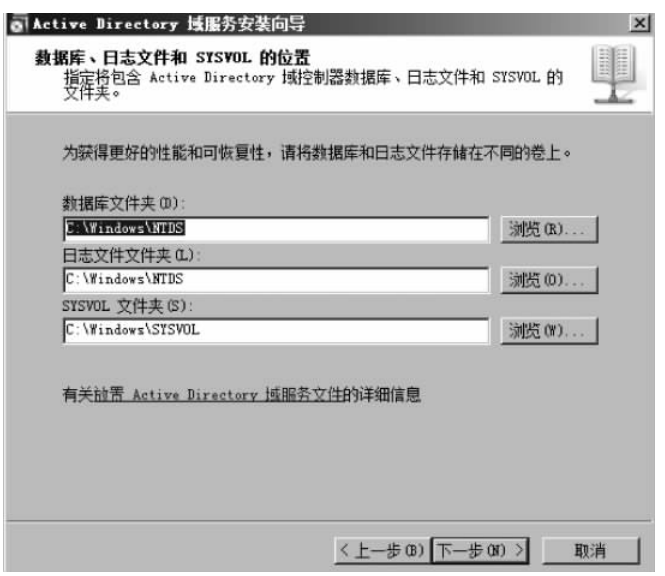

图 3-23　数据库、日志文件和 SYSVOL 文件夹位置

日志文件文件夹：用来存储 Active Directory 的变更日志，此日志文件可用来修复 Active Directory。

SYSVOL 文件夹：用来存储域共享文件。选择“下一步”按钮。出现如图 3-24 所示对话框，此时要求设置目录服务还原模式的管理员密码，设置完密码后，单击“下一步”按钮。

这里要求域用户的密码默认是必须至少 7 个字符，且不可包含用户帐户名称中超过两个以上的连续字符，还有至少要包含 A～Z、a～z、0～9、非字母数字这 4 组字符中的 3 组。

设置成功后，会出现如图 3-25 所示对话框。

图 3-24　设置密码

图 3-25　设置完成

完成后重启计算机，重新登录。

2. 创建域用户帐户

在服务器升级为域控制器后，原本位于本地安全数据库内的本地帐户，会被移动到 Active Directory 数据库内，而且被保存到 Users 容器中。

只有创建域中第一台域控制器时，该服务器原本的本地用户会被移动到 Active Directory 数据库，其他域控制器中原有的本地用户帐户并不会被移动到 Active Directory 数据库，而是被删除。

下面是在 Active Directory 中创建域用户帐户：

(1) 单击“开始”→“管理工具”→“Active Directory 用户和计算机”命令，在出现的窗口中右击域名：dhynet.com，选择“新建”→“用户”命令，如图 3-26 所示。

图 3-26　新建域用户

(2) 设置用户名等用户信息,如图 3-27 所示。

图 3-27　设置用户信息

(3) 单击“下一步”按钮,设置密码,如图 3-28 所示。

(4) 单击“下一步”按钮,设置用户属性,这里根据实际用户情况输入地址、电话等信息,如图 3-29 所示。

3. 创建域组

(1) 单击“开始”按钮,选择“管理工具”→“Active Directory 用户和计算机”选项,右击域名,选择“新建”→“组”命令,出现如图 3-30 所示对话框。

(2) 右击组帐户,选择“重命名”命令可以更改组名,选择“删除”命令可以将组删除,如图 3-31 所示。

图 3-28　密码设置

图 3-29　设置用户信息

图 3-30　新建组

图 3-31　对组进行操作

4. 添加组成员

右击刚刚新建的“生产部”组，选择“属性”，在弹出的属性对话框中选择“成员”选项卡，然后单击“添加”和“确定”按钮。

单击“添加”按钮，在弹出来的对话框中选择“高级”按钮，通过“立即查找”功能，可以选择想要添加的成员，如图 3-32 所示。

5. 禁用/启用域帐户

用域管理员身份登录计算机，打开“Active Directory 用户和计算机”控制台，选中相应帐户，右击选择“禁用帐户”命令即可，如图 3-33 所示。

图 3-32　添加组成员

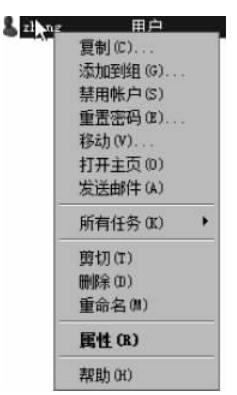

图 3-33　禁用帐户

6. 设定用户登录时间

用管理员身份登录计算机，打开“Active Directory 用户和计算机”控制台，打开相应帐户的属性界面，如图 3-34 所示，单击“登录时间”按钮，如图 3-35 所示。

图 3-34　设定登录时间

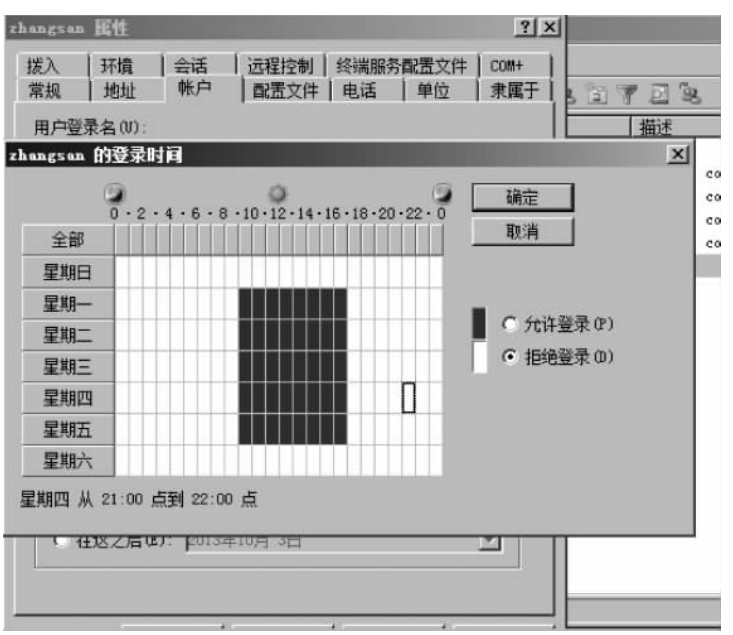

图 3-35　登录时间

3.7 应用案例3：设置组策略

3.7.1 案例内容

DHY公司已经实现了统一的域管理。域名为DHYnet.com，第一台域控制器由公司网络中心管理员专门管理。管理员在创建DHYnet.com域的开始，已经为各个部门统一建立了组织单位(OU)。

目前，DHY公司域已经运行了一段时间。公司网络中心为了方便管理，也为了减轻管理员日后维护域的工作，希望有方法能够统一地管理各个部门的计算机。要求如下：

(1) 设置统一的计算机工作环境，如统一桌面壁纸，实现DHY企业工作环境统一的形象；

(2) 确保用户在网络中任意节点登录，都可访问各自的数据，且确保不因为客户端故障导致“我的文档”“桌面”中文件丢失。

3.7.2 案例分析

根据案例要求，管理员可以通过设置Windows Server 2008中的组策略解决案例中的问题。

3.7.3 案例实施过程

由于会立即应用对GPO的更改，因此，在测试环境中全面测试GPO之前，请将GPO与其生产位置(站点、域或OU)取消链接。在开发GPO时，请将其与测试OU保持链接或取消链接。

1. 创建未链接的GPO

(1) 在GPMC控制台树中，在要创建新的未链接GPO的林和域中右击“组策略对象”选项，如图3-36所示。

图3-36 创建GPO

（2）单击“新建”命令，在“新建 GPO”对话框中，指定新 GPO 的名称，如“全域用户环境策略”，然后单击“确定”按钮，如图 3-37 所示。

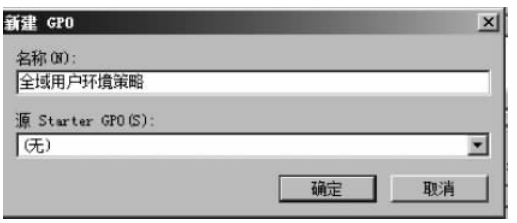

图 3-37　输入 GPO 名称

2. 链接 GPO

将 GPO 中的策略设置应用于用户和计算机的主要方法是：将 GPO 链接到 Active Directory 中的容器。GPO 可以链接到 Active Directory 中的三种类型的容器：站点、域和 OU。每个 GPO 可以链接到多个 Active Directory 容器。GPO 是针对各个域分别存储的。例如，如果将 GPO 链接到某个 OU，那么该 GPO 实际并未位于该 OU 中。GPO 是针对每个域的对象，可以将其链接到林中的任意位置。GPMC 中的 UI 可帮助指明链接和实际 GPO 之间的差异。

（1）右击某个站点、域或 OU 项目，然后单击“链接现有 GPO”命令，如图 3-38 所示。此步骤相当于在安装 GPMC 之前在“Active Directory 用户和计算机”管理单元中提供的“组策略”选项卡中选择“添加”选项。

图 3-38　链接 GPO

（2）除了上述方法还可以在“组策略对象”项目下面，将一个 GPO 拖到要将该 GPO 链接到的 OU 中。此拖放功能仅在相同的域中有效。

3. 统一桌面壁纸

（1）打开编辑“全域用户环境策略”选项，定位到“用户配置”选项，选择“管理模板”→在后侧选择“桌面”选项，如图 3-39 所示。

（2）设定统一的桌面墙纸文件，双击图 3-40 中右边的“桌面墙纸”选项，如图 3-41 所示进行配置。

图 3-39　选定"桌面"选项

图 3-40　设置"桌面墙纸"

图 3-41　启用"桌面墙纸"

(3) 设定用户不能自行修改桌面,双击"桌面墙纸"之上的"不允许更改"配置项进行启用配置,如图 3-42 所示。

4. 文件夹重定向

(1) 在域内文件服务器上新建一个共享文件夹,并赋予所有用户都有通过网络对此文件进行读写的权限。这里假定共享文件夹的访问路径为"\\Win-vmi86mg3i6q\文件夹重定向",如图 3-43 所示。

(2) 在"全域用户环境策略"选项下定位到"用户配置"→"文件夹重定向"→"文档"选项,在右键快捷菜单中选择"属性"命令,进行属性配置编辑,如图 3-44 所示。

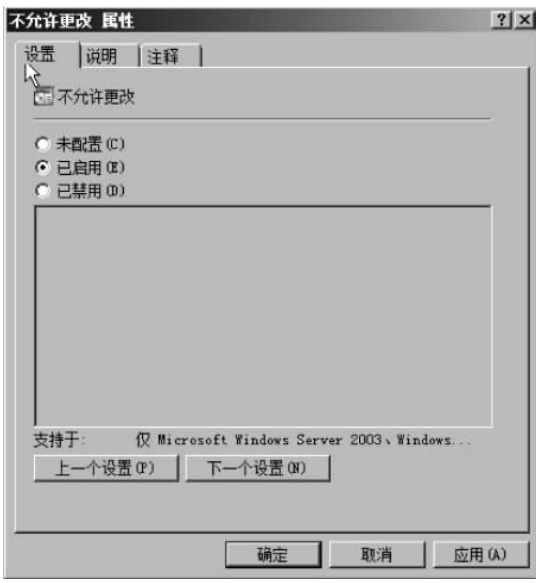

图 3-42　启用“不允许更改”

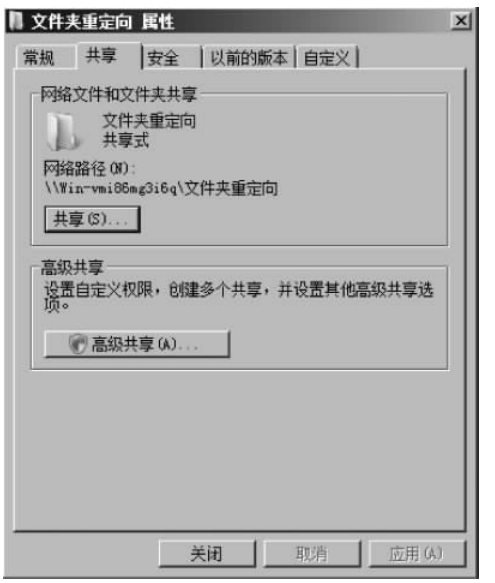

图 3-43　设置共享文件夹

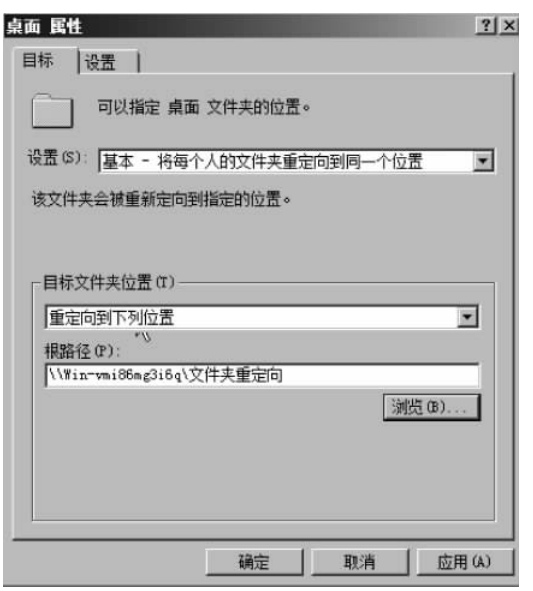

图 3-44　将桌面重定向

3.8　练 习 案 例

你是公司的网络管理员，公司名为 fabrikam。

你在数据中心有多台服务器，需要进行管理，并且有一台新的 Windows Server 2008 计算机需要安装活动目录并进行管理。你将该计算机命名为 server1，并配置成具有 IP 地址 10.10.30.1。

公司要求注重网络资源的安全性,要求严格管理公司网络资源。要求如下:

(1) 建立公司域,由专人管理;

(2) 严格限制公司员工使用公司域的权限;

(3) 为树立良好的企业形象,统一域内计算机的桌面壁纸;

(4) 域用户在域中任意计算机上登录时,“我的文档”中的文档不会丢失。

3.9 课 后 习 题

1. 什么时候使用本地帐户登录?

2. 什么时候使用域用户登录?

3. “文件夹重定向”可以将哪些文件夹重定向?