Windows NT 和 UNIX 的集成

Windows NT and UNIX Integration

Gene Henriksen 著

石祥生 翟 炯 石秋云 译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

内容提要

本书详细而全面地介绍了在异种网络中两种不同的操作系统 Windows NT 和 UNIX 的集成。全书共分六部分十四章，还有两个附录。作者根据亲身工作实践和充实的知识，论述了在同一网络中集成这两个操作系统所涉及的关键性问题。在简要地介绍了 Windows NT 和 UNIX 的主要功能、特性、用途的基础上，深入浅出地论述了在 NT 和 UNIX 中的 TCP/IP、文件共享、打印共享、应用程序集成，以及集成这两种操作系统所必须的工具和实用程序等；并为集成这两个操作系统提供了权威性的指导。

本书对于系统工程师、系统体系设计者、网络管理员、系统管理员等是一本不可多得的理想读物。

原 书 名：Windows NT and UNIX Integration

书　　名：**Windows NT 和 UNIX 的集成**

著　　者：Gene Henriksen

译　　者：石祥生　翟　炯　石秋云

责任编辑：陆伯雄

印 刷 者：北京市天竺颖华印刷厂

出版发行：电子工业出版社出版、发行　URL：http://www.phei.com.cn

北京市海淀区万寿路 173 信箱　邮编　100036　发行部电话 68214070

经　　销：各地新华书店经销

开　　本：787×1092 1/16　印张：15.75　字数：360 千字

版　　次：1999 年 1 月第 1 版　1999 年 1 月第 1 次印刷

定　　价：26.00 元

印　　数：6000 册

书　　号：ISBN 7-5053-4948-1/TP·2429

著作权合同登记号　图字：01-98-1568

凡购买电子工业出版社的图书，如有缺页、倒页、脱页者，本社发行部负责调换

第一部分　Windows NT 和 UNIX 的基础

第 1 章　Windows NT 简介

- **Windows NT 的用户管理**　学习如何建立和控制用户帐号，如何限制登录时间和工作站，如何创建用户概况文件和策略。
- **在域中使用组**　学习如何在域中使用组去减轻管理任务，如何区别本地组和全局组，如何将资源许可权赋予组，了解许可权是如何起作用的。
- **域和委托**　学习如何建立域和利用服务器管理程序(Server Manager)去管理域中的 NT 计算机，了解域之间的委托关系是如何扩充域资源访问权范围的。
- **服务**　了解如何启动和监测 NT 服务，学习如何使用 AT 命令和如何去监测任务和系统性能。
- **盘驱动器**　学习在 NT 中可以使用的两种文件系统，如何用一个文件系统跨多个盘，如何建立 RAID1 和 RAID 5 进行崩溃恢复。
- **引导和关机**　探索在 RISC 或 Intel 中引导时所需的文件，构建当镜像根驱动器出现故障时进行恢复所用的应急软盘，了解如何合适地为 NT 关机。

Windows NT 操作系统综述

初看起来，Windows NT 似乎是一个很容易管理的操作系统，它有一个界面，看起来很像 Windows 95(NT 4.0 版)或 Windows 3.x (NT 3.51 版或更早的版本)。千万不要将这种图形界面的相似性错误地看成管理的简单性，隐藏在该界面下面的是一个很复杂的世界，虽然其中有很多可以用该图形界面进行配置，但仍然需要命令行和称为“注册表(Registry)”的数据库。

最初的 NT 操作系统本质上是一个单用户和多任务的系统，Citrix 开发了一个用于瘦客户(thin clients)的多用户版本，瘦客户是指无盘 PC 机，甚至是指基于 286 的老式 PC 机，它们可以在本地显示数据，而计算任务则在服务器中完成。广泛的多用户要求迫使 Microsoft 公司去取得 Citrix 技术的许可权，在名为“终端服务器(Terminal Server)”的产品中提供多用户功能，终端服务器推出时可用于 4.0 版，而且将成为 5.0 版的一部分。终端服务器为瘦客户提供了在 NT 服务器上运行程序的能力，因而允许 NT 具有真正的多用户功能。

管理 NT 的基本方法是使用 Administrative Tools(管理工具)，从 Start 菜单很容易到达 Administrative Tools，如图 1.1 所示。

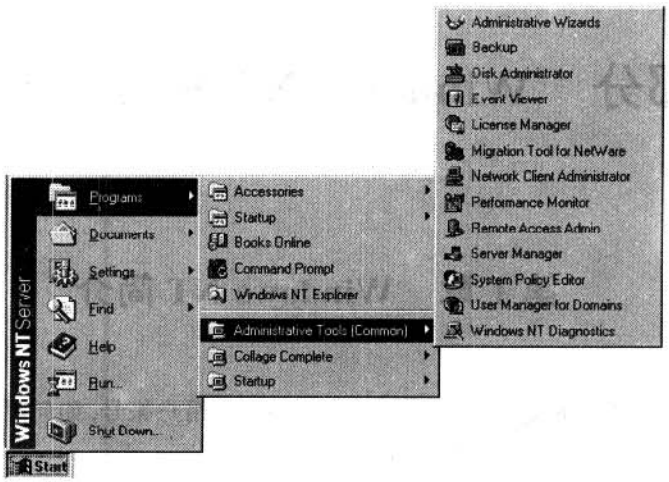

图 1.1　NT 4.0 版中到达 Administrative Tools 的路径

只要有可能，就可将 NT 的各个实用程序看作是 UNIX 中的相应部分，从而可帮助 UNIX 的管理员找到这两种操作系统之间的相似之处。

UNIX 的根帐号在 NT 中有一个相应的部分，称为管理员帐号(Administrator account)，它与根帐号一样，是一种全能的注册。

在 NT 中，共享一个帐号数据库的所有计算机的组合称为一个域(domain)。从字面的含义来看，NT 的域与域名系统(domain Name System——DNS)中的域是同一组的计算机。NT 的域有点类似于网络信息服务(Network Information Services——NIS)，它们都用一台主计算机去容纳帐户数据库，而且都可以将该数据库复制到其他计算机中。

NT Server 可以安装为域控制器或成员服务器。一个成员服务器(member server)，例如 NT Workstation，可以是一个域的一部分，但是在域控制中并不起作用。成员服务器一般可分成两种：文件和打印服务器及应用程序服务器。应用程序服务器可控制数据库应用程序，如 Microsoft SQL Server。

NT 利用组这一概念来管理大量的用户及这些用户的权限，它将用户分成组，并将资源访问权赋予各个组。有两种组类型，即本地组和全局组。各种权限可以赋予不同的用户，Microsoft 建议不要将权限赋予用户，而倾向于将权限赋予组，以简化管理任务。

在 DOS 和早期的 Windows NT 操作系统中，大部分的配置工作都是由 .ini 文件控制的，这些文件都是初始化文件，在某些方面类似于 .profile 或 .login 文件，系统和大多数应用程序都具有 .ini 文件。对于 NT 而言，Microsoft 构建了一个注册表(Registry)数据库，该数据库中的一部分包括了在引导时确定的、有关可用的硬件及调整和管理参数等的信息，这些参数是通过图形管理工具设定的。

某些可能需要调整的设定值只能通过注册表数据库获取，在编辑该数据库时，没有联机帮助会对非法的值提出警告。注册表帮助文件只能从 Resource Kit 中使用。

警告：在编辑注册表数据库之前通常有一个警告，编辑注册表数据库可能导致成为一个不能引导的系统，而且 Microsoft 不能保证可以挽救该系统。

通过点对点协议(PPP)的远程访问是NT的一个标准部分。利用Microsoft的远程访问服务(Remote Access Service——RAS),就可以配置高安全性所需的回拨,可以利用多链接将多根电话线组合到作为单个链接的服务器,并实现点对点隧道协议(PPTP)。利用PPTP就可以通过Internet提供一个虚拟专用网络(VPN)。

Microsoft已开发了一个网络操作系统,它所包括的内容比文件和打印服务还要多得多,在该操作系统中新增添的内容正在定期地推出。

Windows NT的用户管理

Windows NT的用户管理是通过NT Server中的User Manager for Domains以及NT Workstation和成员服务器中的User Manager完成的。User Manager for Domains可以更新域数据库的内容,而且只能在主域控制器(PDC)和备用域控制器(BDC)中使用,而User Manager却只能更新供成员服务器和NT工作站使用的本地数据库。

帐号数据库既包括用户帐号,又包括计算机帐号,作为该域成员的所有NT计算机都必须具有一个计算机帐号,这对于PDC、BDC、成员服务器和工作站等都是适用的。注册信息和安全信息的集合称为"安全帐号管理程序"(Security Accounts Manager——SAM),SAM数据库放在域控制器,而不是放在本地服务器中。但并不是用作域控制器的每一台计算机都有一个本地的SAM数据库。

主域控制器(PDC)的作用是维护SAM的主拷贝,并定期地将该SAM复制到各个备用域控制器(BDC),无论是PDC和BDC,都可以使用户注册生效。

User Manager for Domains位于Start按钮的Administrative Tools (Common)子菜单中(如图1.1所示)。

所有的用户帐号都显示在图1.2所示的窗口中,即使该域包含20,000个帐号也是如此。要想定位一个帐号,可使用在Username列表右边的滚动条。

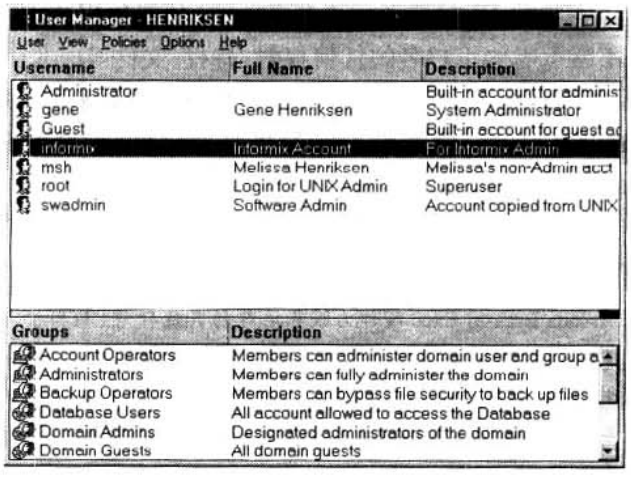

图1.2 User Manager for Domains主窗口

管理员帐号是在安装时创建的，该帐号不能删除，但出于安全目的可以更名。它相当于UNIX 的根(root)帐号。

在安装时创建的缺省用户帐号中有一个是 Guest，该帐号用于没有域帐号的用户或也许是另一域的成员的用户的连接。Guest 帐号的细节可以通过双点按它的名字获取，所显示的信息示于图 1.3 中。

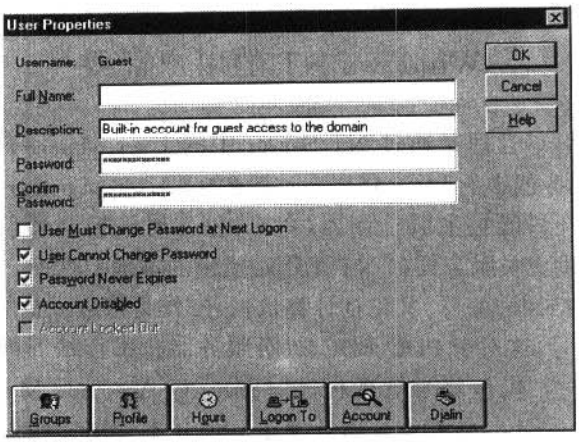

图 1.3　User Manager for domains 的用户属性(User Properties)对话框

请注意 User Manager 的功能，管理员可以修改用户名、全名、说明、帐号的口令等。

■ 用户属性

创建一个用户帐号时，就将一个安全标识符(Security Identifier——SID)赋予该帐号，SID 并不是用户名，是安全性的一个关键组成部分。与 UNIX 的 UID 相比，SID 是一个长的数字，Microsoft 并没有为生成 SID 提供任何公式。如果删除一个用户帐号，其 SID 就退役，如果重新建立该用户帐号，就赋予一个新的 SID，其新的用户名与老的用户名之间没有任何关系，而且并不继承老的用户名的任何权限、特权、文件等。

管理员可以要求用户在下一次登录时改变口令，这一选项对于初始创建帐号或重新设定已忘记的口令是很有用的。管理员可以禁止改变口令，并设置 Password Never Expires (口令永不过时)选项。他还可从屏幕上禁止一个帐号。

最后一个选项是 Account Locked Out(帐号封锁)，这并不是一个管理员功能，而是注册失败时被安全系统使用的一种功能。

提示：当你安装 Arcada Backup Exec 和作为服务运行的其他软件(相当于 UNIX 的守护神进程)时，必须为注册使用的软件提供一个帐号名。千万不要使用管理员(Administrator)帐号，使用 Administrator 的帐号时，该服务将正常工作到其口令修改为 Administrator 为止，在下一次系统引导时，这一服务将无法注册。正确的方法是创建一个新的用户和提供一个特别难以破解的口令，将其帐号设置为 Password Never Expires

在该屏幕的底边有一行其他的功能按钮，利用它们就可访问各种用户控制：Groups、Profile、Hours、Logon To、Account、Dialin 等。有关组的讨论将放在本章后面的“在域中使用

组"这一节中进行。

■ 利用帐号概况文件控制用户

帐号概况文件(account profiles)用来设置使用帐号的各种标准。概况文件(profile)是强制性的,可以防止修改帐号设定值;它可以为管理员提供对用户某种程度的控制,从而简化管理工作;还可使用户更有效和防止出现死机。

对于被临时求助使用的帐号,利用一个强制性的概况文件就可以防止用户修改网络连接和屏幕颜色、避免运行非授权的程序、防止使用改变环境的其他修改。由于不会产生永久性的修改,因而用户们将总是具有相同的配置。

Windows NT 和 Windows 95 使用不同的概况文件方法,概况文件必须在使用它的操作系统中创建。较早的操作系统(如 Windows 3.1 或 Windows for workgroups)并不支持概况文件,而是必须使用登录脚本。登录脚本也可用于 Windows 95 和 NT 用户。

图 1.4 说明了如何对远程服务器上的 Z 驱动器设置主目录。主目录可以在本地机器中,也可在一个网络共享的机器中,它的作用与 UNIX 中主目录的作用是不同的。NT 的主目录是用于 File Open 对话框和 Save As 对话框、以及设有定义工作目录的应用程序等的缺省位置。

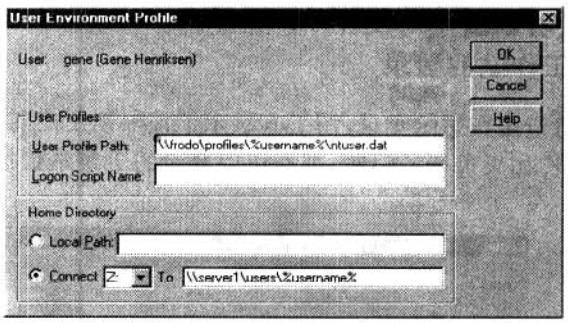

图 1.4 User Environment Profile(用户环境概况文件)对话框

在 UNIX 中,主目录用来存储开机文件。.profile 和 .login 的对应部分就是用户概况文件和登录脚本。

提示:在提供主目录路径时,一种较方便的方法是为使用该主目录的用户命名主目录,在定义路径名时,利用%USERNAME%去表示当前用户。在 UNIX 中的等价部分是 LOGNAME 环境变量。

■ 登录时间限制

可以限制个别用户的登录时间。在图 1.5 中,用户的登录时间限定为上午 7 点到下午 6 点,这样设定以后,就可防止用户在不允许的时间内向计算机登录。利用这种限制,就可使得用户在备份期间处于脱机状态,作为一种安全防范措施,这种限定可使用户在非授权时间内与系统脱开。

如果用户试图在不允许登录的时间内进行登录,就会接收到一条消息:

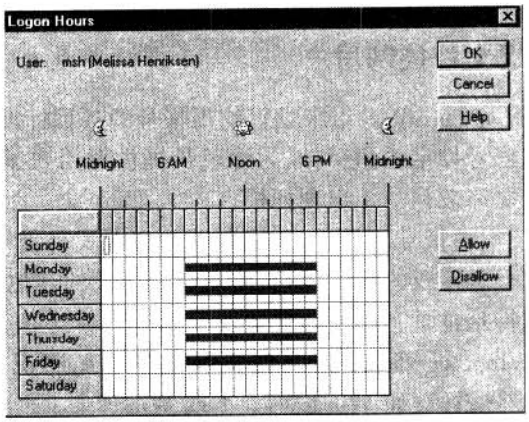

图 1.5　限制登录时间

Your account has time restrictions that prevent you from logging on at this time. Please try again later.

该限定适用于来自该域内任何计算机的注册企图。如果注册时间已过，已经注册的用户将会接收到一条消息，该消息的内容是如果试图连接一个网络资源，该资源是不可使用的。

■ 限制对特定工作站的登录

可以限制用户对特定工作站的登录，图 1.6 展示了该限制用户的过程。缺省时，用户可以对所有的工作站登录，如果进行了限制，那么可以登录的工作站数量最多为 8 个。

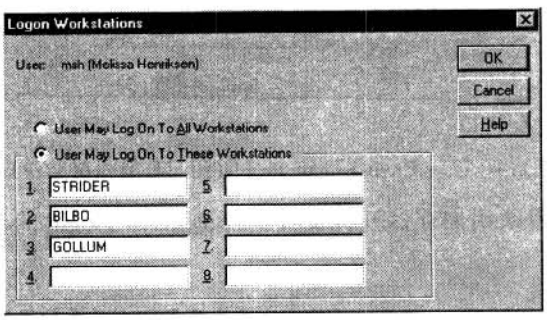

图 1.6　用户可以向所有工作站登录，或者只能向列出的工作站登录

■ 帐号信息

帐号信息(Account Information)选项允许管理员为一个帐号选择一个过期时间，其缺省值是 Never (永不)。对于已经租借了一段特定时间后的用户帐号，如果其租借期已满，就可将它置成过期帐号，如图 1.7 所示。利用这一选项，管理员就不必记住去作废该帐号或者在用户租借日期到达时修改其口令。

该屏幕中的第二个选项允许创造一个全局(Global)或本地(Local)帐号，其缺省值是全

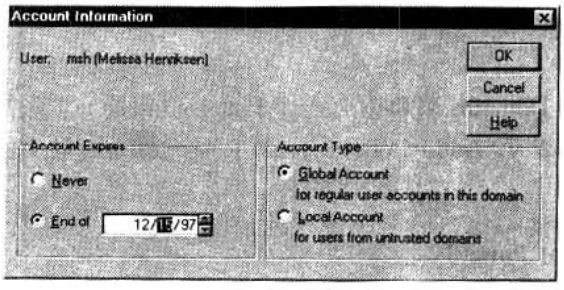

图 1.7 Account Information 对话框

局帐号。Microsoft 对本地帐号特性的解释是：为那些需要访问特定服务器，可是又不是该服务器所在域的成员的用户创建一个本地帐号。

提示：在安装软件时，可能要求你为该软件本身建立一个帐号，例如，Informix NewEra 需要一个本地帐号，如果为 Informix 建立一个正常的全局帐号，那么当你试图使用该软件时，就会收到一条"unknown user"(不知名用户)的出错消息

■ 拨入许可权

将拨入许可权赋予用户就允许该用户通过远程访问服务(RAS)去访问其域，这也称为"拨入"(Dialin)。

提示：如果该计算机是一个域控制器，那么设置该选项时的设定值适用于全域范围；如果该计算机是一台安装为成员服务器或 NT 工作站的 NT 服务器，其设定值就适用于该本地计算机。

Call Back(回拨)选项主要用于记帐(见图 1.8)，其缺省值是 No Call Back。当将该选项选择为 Set by Caller 时，服务器就提示一个电话号码，断开其电话线，并拨入该用户。使用 Call Back 就由服务器支付记帐的费用，而不是拨入者。

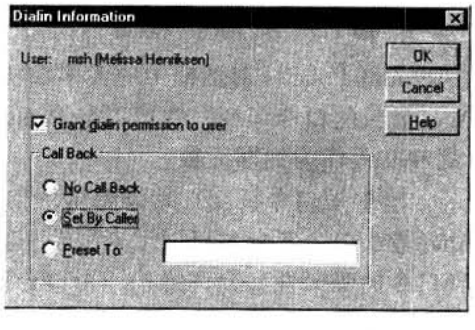

图 1.8 一个用户的拨入许可权

选择 Preset To(预置到)选项就可确定回拨号码，如果该远程用户总是在同一个地点，这是一个很好的安全性特点，但对移动的用户却不一定适用。这一特点还限制使用多链路功能，因为系统只能拨一个号码，而多链路要求拨多个号码。但是有一种特殊情况，即如果

其链路是一条使用一个电话号码的双通道 ISDN 线路，则不属此例。

■ 策略

User Manager for Domains 菜单中有一个 Policies（策略）选项，它包括 4 个选项：Account Policy、User Rights Policy、Audit Policy、Trust Relationships，其中的第 4 个选项将与前 3 个选项分开讨论。

帐号策略（Account Policy）

帐号策略是全域适用的，当某些个人的帐号策略与域帐号策略有矛盾时，管理员可以利用帐户设定值去覆盖个人的帐户策略。图 1.9 说明了 Account Policies 对话框。

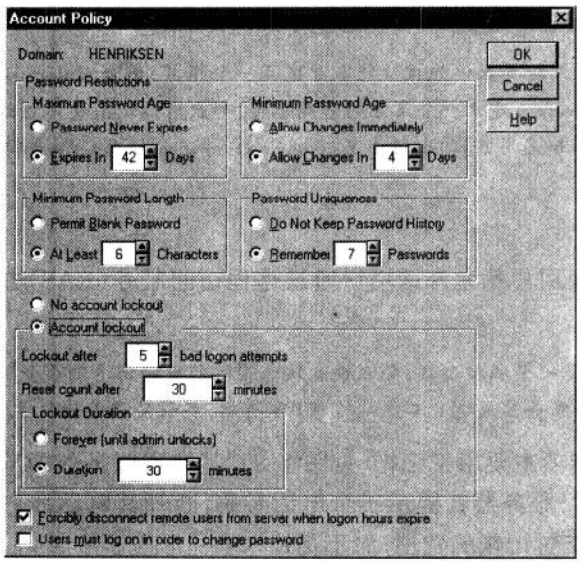

图 1.9　帐号策略设定值

UNIX 的管理员应该对 Account Policies 对话框中的大多数功能非常熟悉，它们包括：

- Maximum Password Age（最长的口令年令），它可以是 Password Never Expries（口令永不过期），也可以将 1 到 999 天作为到期天数。
- Minimum Password Length（最短口令长度），其范围可从空口令到 14 个字符长。
- Minimum Password Age（最小口令年令），可以用来限制用户修改口令的频度。
- Password Uniqueness（口令的唯一性），允许维护一个口令历史记录，在该历史记录中的口令不能重复，最多的历史记录是 24 个口令。

在一个设定次数的注册企图失败后，就会自动封锁该帐号，在封锁之前的最多失败次数为 999 次，既然是这样，选用 No Account Lockout（没有帐号封锁）选项可能更好一些。在失败发生以后，经过一段固定的时间后，这一数值就会恢复。这一段时间可以从 1 到 99,999 分钟，约为 69.5 天。

一旦一个帐号被封锁，该封锁状态可以保持为 Forever（永久），或直到管理员解锁该帐

号为止(请记住图 1.2 中 Account 主对话框中的 Account Locked Out 框)。该锁可以设置成经过一段设定的时间后,自动清除,这一段时间最长为 99,999 分钟。

在 Account Policy 对话框底部是一个不应该忽视的选项,如果将帐号设置成限制其登录时间(见图 1.5),那么在登录周期没有结束时,系统不会强行断开它们。复选"Forcibly Disconnect Remote Users from Server When Logon Hours Expire"选项就可断开其共享资源,受到影响的用户将会收到一个通知,说明登录时间已过,请注销。

用户权限策略

NT 采用一个简单的过程将权限赋予用户或组,请从 User Manager 窗口中选择 Policies, User Rights。就像前面讨论的帐户策略一样,用户权限策略(User Rights Policy)适用于全域,但并不适用于在选择该选项时加亮的特定帐号。

在该过程中并不是选择一个组或一个用户,然后赋予一组权限,而是采用别的方法。先选择一个权限,然后增加或删除用户和组。目前,除了通过实用程序查看与用户和组相关的权限外,还没有一种简易的方法可以将它们列出来。

提示:某些 UNIX 系统可以提供类似的功能。SCO 版本的 UNIX 允许将特权和授权赋予单独的用户,但不能赋予组;Solaris 则不能提供相应的工具。

图 1.10 展示了 User Rights Policy 对话框。

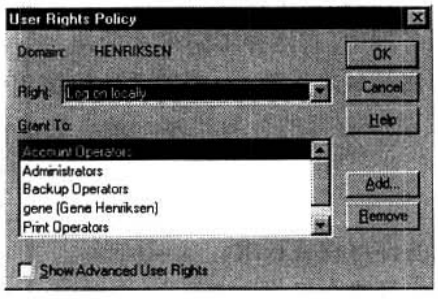

图 1.10 User Rights Policy 对话框

图 1.11 说明了如何将特定的权限赋予组。当单点按一个用户或组的名字去选择它们时,Add 按钮就被激活,点按 Add 按钮就可增加该权限。另一种方法是双点按其名字就可增加该权限。缺省时,只显示组,要想显示用户,可点按 Show Users 按钮。

请注意,其缺省值是将一种权限增加到组,而不是用户,这样做的目的是可以减轻管理工作量。

审计策略

在 Options 组中的最后一个选项是 Audit(审计),可以在七个方面对审计进行配置。审计一般用来满足安全性要求,而且类似于 UNIX 的审计。Windows NT 可以达到 C2 级安全标准。

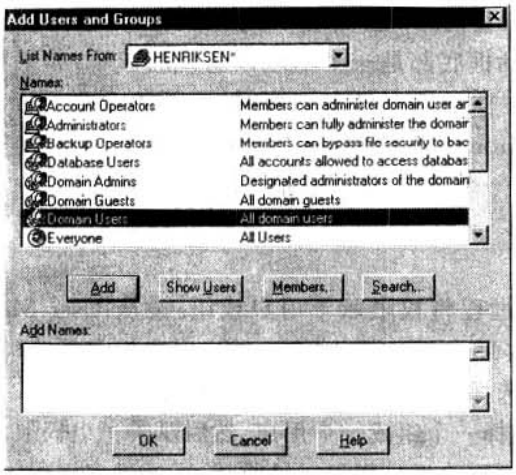

图 1.11　将一种权限赋予一个组

在域中使用组

在 Windows NT 中，使用组来减轻赋予许可权的管理工作量。有两种类型的组，即本地组和全局组。在域控制器和服务器中，有两种不同形式的组，域控制器既可以具有本地组，也可以具有全局组。其本地组属该域本地的，一个域本地组可用于该域的任何地方。在成员服务器中的本地组是用作成员服务器的计算机本地的。在成员服务器中不能建立全局组。

本地组具有下列特点：

· 为用户提供对各种资源的许可权或权限。
· 包括来自任何域的用户帐号或全局组。
· 不包括其他的本地组。
· 具有在本地域中赋予的许可权和权限。
· 可以在域控制器中将该域任何地方的资源赋予它。
· 在 NT 工作站或成员服务器中只能将本地机器的资源赋予它。

另一方面，全局组具有如下特点：

· 在工作站或成员服务器中不能建立全局组。
· 只能包括来自本地域的用户。
· 不能包含本地组或全局组。
· 不能分配本地资源。
· 必须在其帐号所在的域控制器中建立全局组。
· 可用来将用户分成组。
· 可以分配给本地组。

将一个资源的许可权或权限赋予一个用户的步骤如下：

1. 将帐号包含到全局组中。
2. 将全局组包含到本地组中。
3. 将资源的许可权或权限赋予本地组。

提示：不应该将一个资源的许可权赋予全局组。

Microsoft 提供了一些现成的组，可以满足大多数的一般要求，应尽可能地使用这些现成的组，以避免出现太多的组。太多的组所引起的问题与不能用一个组来管理大量的实体是相同的。

组(Groups)显示在 User Manager 窗口的底部，在 User Manager 屏的底部列出了不同的组(请参考本章前面的图 1.2)。在组的列表中，请观察本地组和全局组之间的差别。缺省的全局组将 Domain 作为其名字的第一部分，这是在创建新的全局组时应该遵循的一个标准。

全局组的图标有一个小球，显示在两个头的左边，而本地组的图标则在该球的位置上有一台计算机。

■ 建立组

在设计用户管理的各种要求时，请努力使用现成的组。要想建立一个全局组，可从 User Manager for Domains 中选择 User、New Global Group，在一个成员服务器中，该选项呈现灰色。图 1.12 说明了如何建立一个全局组，要想把一个成员增加到该组中，可在选项卡为 Not Members 的右边栏中点按其用户名，选择该用户后，其名字就从 Not Member 栏中消失，而显示在 Member 栏中。

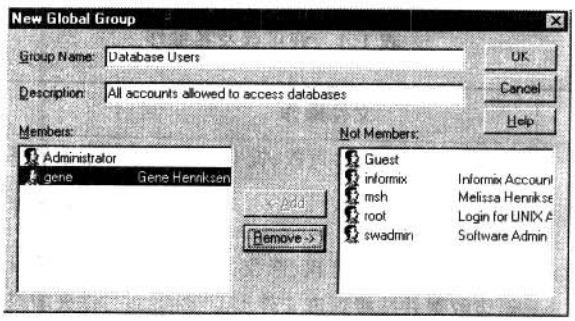

图 1.12　建立一个新的全局组

要想允许特定的用户访问一个 NT 服务器中的数据，可执行下列步骤：

1. 建立一个全局组(如 Domain Database User)。
2. 将用户帐号增加到该全局组中。
3. 建立一个名为 Database User 的本地组(对该域或服务器是本地的)。
4. 将该全局组分配给该本地组。
5. 将该数据库文件夹和文件的特权赋予该本地组。

■ 赋予许可权

运行 Windows NT 时，在计算机中可使用两个文件系统。从 DOS 的初期开始，就一直在使用文件分配表(FAT)文件系统，许可权不能赋予文件或文件夹，在控制台上注册的任何人可以“拥有”FAT 文件系统中的全部文件。对一台 NT 计算机具有访问权的任何人可以用 DOS 引导盘重新引导，如果该计算机使用 FAT 文件系统，那么他就“拥有”该计算机中的全部文件。FAT 文件系统的唯一安全性措施就是通过网络上各个 FAT 共享部分的许可权。

另一个文件系统是 NT 文件系统(NTFS)，它支持许可权的赋予。如果计算机是用 DOS 盘引导的，那么 NTFS 是不可读的。NT 文件系统的开销比 FAT 文件系统大，但是它比较容易从崩溃中恢复。对于不要求安全性的小分区(少于 400 MB)，可使用 FAT 文件系统，而对于安全性很重要的大分区则应使用 NTFS。

对于 NTFS 共享资源，可以赋予本地许可权和共享许可权。对于共享的 NTFS 资源，通过进一步的限制共享许可权和本地许可权就可确定访问权。

故障查找技巧：将一个卷格式化为 NTFS 时，就批准了 Everyone 组(在网络上的每个人)对该卷具有 Full Control(全部控制)许可权，这可能是一个主要的安全问题，在该卷内创建的各个文件和文件夹都继承其缺省许可权。为了解决这一问题，可删除 Everyone 组的各种许可权，然后将 Full Control 许可权赋予 Admins 组，然后再根据需要赋予其他许可权。

此处所说的许可权不同于通常的 UNIX 许可权 rwxrwxrwx，后者只允许单个拥有者、单个组、注册的任何人。当用户试图访问一个文件时，其操作将受到赋予他的许可权的控制，表 1.1 列出了各种许可权和可以对文件或文件夹执行的相应操作。

表 1.1　许可权及其操作

许可权	文件操作	文件夹操作
Read (R)	显示数据、文件、许可权、拥有者。	显示名字、属性、许可权、拥有者。
Delete (D)	删除文件。	删除文件夹。
Write (W)	显示拥有者和许可权、修改文件属性、创建数据并挂接到该文件上。	显示拥有者和许可权、将文件和文件夹增添到该文件夹中、修改属性。
Execute (X)	显示属性、拥有者、许可权，如果该文件是可执行的就运行该文件。	显示属性、拥有者、许可权，利用该文件夹修改其他文件夹。
Change Permissions (P)	修改一个文件的许可权。	修改文件夹的许可权。
Take Owaership (O)	取得该文件的拥有权。	取得该文件夹的拥有权。

此外，各种许可权可组合成为标准许可权，在上面的表中没有列出标准许可权，不过标准许可权是由上面列出的一个或多个许可权组成的。表 1.2 中列出 3 各种标准许可权。

表 1.2　标准许可权

许可权	文件操作	文件夹操作	文件夹中的文件
Full	全部许可权	全部许可权	全部许可权
No Access	无许可权	无许可权	无许可权
List	不能选择	RX	不能指定
Read	RX	RX	RX
Add	不能选择	WX	不能指定
Add & Read	不能选择	RWX	RX
Change	RWXD	RWXD	RWXD

要将许可权赋予一个 NTFS 资源，可以点按该资源，并选择 Properties、Security、Permissions。图 1.13 说明了如何修改对一个文件具有访问权的组的许可权，请注意，可用的许可权显示在 Type of Access 下拉列表中。

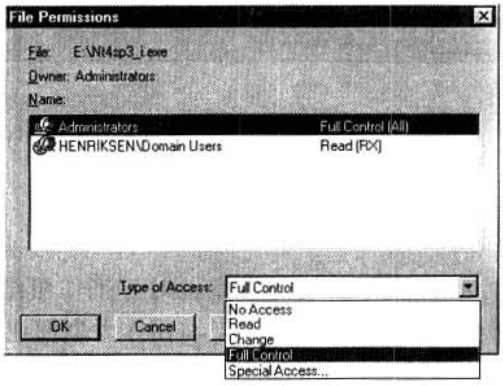

图 1.13　在文件 NT4sp3_i.exe 中修改 Everyone 组的许可权

要想为对一个资源没有许可权的组增加许可权，可点按 Add 按钮，这时就显示 Add Users and Groups 对话框，点按要增加的用户或组，然后点按 Add 按钮，并从 Type of Access 下拉列表中选择许可权。Add User and Groups 对话框(参见图 1.11)可用于多种目的。

■ 许可权的工作原理

当用户在 NT 域中登录时，就会生成一个令牌，该令牌由该用户的权限和特权组成。在该域中的每个资源或对象都有一个访问控制表(Access Control List－ACL)，它包含着获取该资源访问权的要求。该令牌与该用户生成的每个进程相关联，当一个用户进程请求访问一个资源时，就将其令牌与 ACL 比较，如果通过了检查，就可批准访问。

如果一个用户属于特别指定对一个资源没有访问权的任何组，那么无论其他的成员关系和访问权是什么，都拒绝该用户的访问。拒绝访问的优先权高于访问权。

故障查找技巧：Bob 属于 Domain Users、Programmers 和 Testers 等全局组，作为 Programers 组的成员，他对文件夹 C:\Program_Notes 具有全部(Full)控制权，但 Testers 组对 C:\program_Notes 文件夹没有访问权，因此，就拒绝 Bob 的访问。Bob 就打电话给管理员，要求退出 Testers 组，因为他已不再在该部门工作，管理员就将 Bob 从 Testers 组中删除。当 Bob 再次试图访问该资源时却得到同样的结果，问题在哪里？Bob 需要注销，然后再登录，以取得一个新的令牌，在该令牌中就不再包括 Testers 组。

图 1.14 说明如何修改一个帐号的组成员关系。要将一个用户增加到一个组中，可点按 Not Member of 栏中的组名，然后点按 Add 按钮。要删除一个组，可点按 Member of 栏中的组名，然后点按 Remove 按钮。

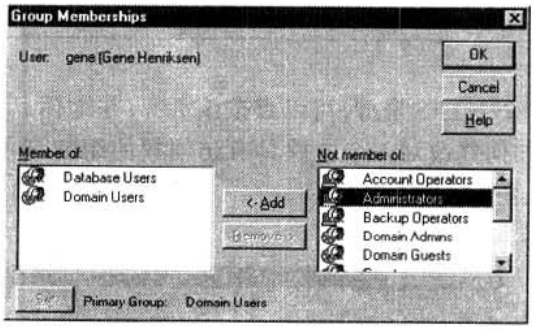

图 1.14　修改一个用户的组成员关系

创建 NT 域和委托

在 Windows NT 之前，Microsoft 的联网模型由对等工作组组成，就像在 Windows for Workgroups 中所实现的那样。由于 Windows NT 将用作大型商业网络方案中的服务器，因此 Microsoft 创建了一个集中管理和控制的客户/服务器网络模型。

Microsoft 的目标是创建一个网络操作系统，在该系统之中，用户具有访问所有授权资源的单个登录和口令。为了满足客户/服务器模型网络的要求，Microsoft 创建了 NT 域。

将安全帐号管理程序(SAM)复制到备份域控制器(BDC)中就可允许用户登录，并被主域控制器(PDC)或任何备份域控制器(BDC)验证，这种验证已被用于 Microsoft 的 BackOffice 应用程序系列中，包括 SQL Server、Exchange Server、SNA Server、Systems Management Server。

在小型网络环境(用户数小于 2,000)中，无需 BDC，一个 PDC 就可处理登录验证，然而，将没有 PDC 的备份，而且 PDC 出现故障时就使得用户无法向该域登录，因而建议至少使用一个 BDC 作为备份。在一个非常小的环境中，PDC 可能也是唯一的应用程序服务器，在这种情况下，如果 PDC 不工作，那么应用程序也就不能运行。只有 NT 服务器可以用作域控制器，NT 工作站就不能用作域控制器。在安装时就应决定是否将一台服务器用作域

控制器，如果不重新安装就不能指定域控制器。

SAM 必须作为一个整体放在每一个域控制器中，并驻留在该域控制器的内存中，因此，域控制器必须具有足够的内存空间去支持这一负载。在域控制器中，内存是最重要的资源。

为了计算 SAM 所需的空间量，可估算每个用户帐号为 1K，每个 Windows NT 计算机帐号为 0.5K。Microsoft 建议的 SAM 数据库最大空间为 40MB，这就将域限制为约 25000 个用户帐号(25MB)和 25000 个计算机帐号(12.5MB)。请记住，Windows 95 计算机在域中不需要具有计算机帐号。域控制器的内存总容量约为 SAM 容量的三倍，因此最大为 40 MB 的 SAM 就需要 120 MB 的 RAM。

■ 域的建立

当开始创建域的过程时，安装的第一台 Windows NT 计算机必须是主域控制器(PDC)，安装时，必须询问用户该计算机是否是主域控制器(PDC)、备份域控制器(BDC)或成员服务器。如果该计算机是一台 BDC，那么在安装时就必须能与 PDC 通信。不能离开了网络、不与 PDC 通信就去安装一台 BDC，然后再加入到域中。

一旦作为一台 PDC 或 BDC 进行安装，该计算机要想成为成员服务器就必须重新安装。同样，不经过重新安装，一个成员服务器就不能提升为 BDC 或 PDC。在大型网络中，不应将域控制器配置成去处理应用程序负载，域的开销已足以成为域控制器的沉重负担。

■ 服务器管理程序(Server Manager)

在域中操作 NT 计算机的主要工具是 Server Manager (服务器管理程序)，它位于 Administrative Tools (common)菜单选项内。图 1.15 说明了 Server Manager。

Server Manager 列出了已成为该域成员的所有计算机。

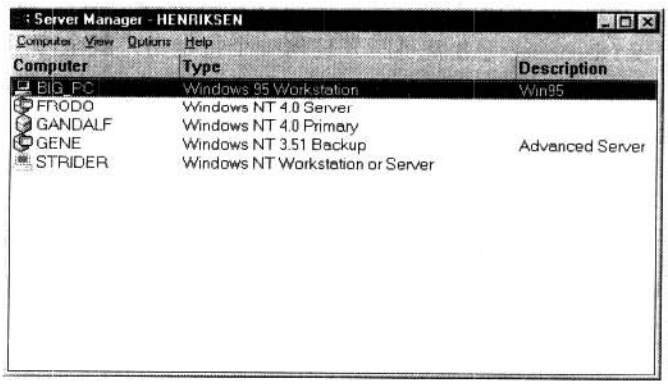

图 1.15　Server Manager 的主屏

提示：计算机名的前面有一个图标，请注意有三种图标。域控制器 GANDALF 的图标是一个不带计算机监视器或显示器的小方框，备份域控制器 GENE 的图标是在前面有一个小显示屏的小方框，服务器的图标与备份域控制器的图标相同。此处的工作站只有一个，是一台 Windows 95 计算机，它的图标是一台桌上计算机。当前不运行的计算机的图标是灰色的，发灰的符号是一