

第三章 Windows 2000 Server 的文件管理

内容摘要

Windows 2000 文件系统支持 FAT16、FAT32 和 NTFS 等。由于 Windows 2000 Server 中的 NTFS 引入了许多新特性，故本章将详细介绍 NTFS，并针对 Windows 2000 中的高级文件系统——分布式文件系统进行具体阐述。学完本章，您将掌握以下内容：

- NTFS 权限
- 共享文件夹权限
- 加密文件系统
- 磁盘配额
- 分布式文件系统

考点提示

- 利用 NTFS 和共享文件夹权限管理资源
- NTFS 分区上的文件压缩和磁盘配额
- 分布式文件系统

3.1 FAT 文件系统概述

FAT 文件系统中，文件分配表复制为两份存在磁盘分区上，其中一份损坏后，可以接着使用另外一份。Windows 2000 支持 FAT 文件系统的两个版本：FAT16 和 FAT32。

用 FAT16 格式化的分区分成 512 字节的扇区，文件按簇写在磁盘上，也称为分配单元。默认的簇尺寸由分区容量决定，可小至 4KB，即 8 扇区，也可大至 64KB，即 128 扇区。FAT32 的主要优点是，它支持的分区比 FAT16 所能处理的分区更大，FAT16 支持最大为 4GB 的分区容量，而 FAT32 能够控制最大为 2047GB 的容量。注意 Windows 2000 用 FAT32 格式化分区最大只到 32GB 的容量，但能够装入 2047GB 的 FAT32 分区。实现 FAT32 时，只对现有 FAT16 的体系结构、内部数据结构、API 和盘上格式做了尽可能小的改变。关于 FAT 文件的详细特点及与操作系统的关系，请参阅 70-210 课程。

3.2 NTFS 文件系统

3.2.1 NTFS 简介

Windows 2000 带有 NTFS 的新版本——NTFS 5.0，这个最新版本提供了 FAT 中没有的性能——可靠性和兼容性，并内置了各种最新的功能和安全特性，可帮助用户更好地管理域和用户账号。另外，它还提供了文件服务器安全特征、数据访问控制以及对于数据完整性很重要的所有者特权等功能。

3.2.2 NTFS 权限

NTFS 权限是一组标准权限，允许或拒绝用户、组对资源的访问。

Windows 2000 提供了下列 NTFS 权限：

- NTFS 文件夹权限 包括“完全控制 (Full Control)”、“修改 (Modify)”、“读取及运行 (Read & Execute)”、“列出文件夹目录 (List Folder Content)”、“读取 (Read)”、“写入 (Write)”六个标准权限。
- NTFS 文件权限 包括“完全控制 (Full Control)”、“修改 (Modify)”、“读取及运行 (Read & Execute)”、“读取 (Read)”、“写入 (Write)”五个标准权限。。

使用 NTFS 权限时，应注意以下重要问题：

1. NTFS Full Control 权限

Full Control 权限授予访问资源的所有权限，其默认的指定情况如下：

- 用户创建文件或文件夹时，会成为 Creator Owner，并获得 Full Control 权限。
- 用 NTFS 格式化卷时，Full Control 权限指定给驱动器根区的 Everyone 组。
- 在 FAT16 或 FAT32 分区转换成 NTFS 时，Full Control 权限指定给该卷所有资源的 Everyone 组。

2. 多重 NTFS 权限

文件或文件夹权限可以指定给用户或组，用户有可能获得指定给他的多重权限，因此用户的有效权限是指定给单个用户的 NTFS 权限和指定给用户所属的所有组的权限的结合。例如，用户有对一个文件夹有 Write 权限，同时用户也是对同一个文件夹有 Read 权限的组的成员之一，则用户对该文件夹有 Read 和 Write 两种权限。

3. NTFS 文件权限优先于 NTFS 文件夹权限

例如，用户得到对文件夹的 Write 权限和对该文件夹中文件的 Modify 权限，则用户既可写文件也可修改文件，即使用户没有权力访问文件夹也一样。通过使用完全的 UNC（通用命名规则名称，格式为 \\servername\sharename），或是从应用程序中打开文件的路径，用户总是能够访问他拥有权限的文件。例如，用户对一个文件夹没有权限，但该文件夹包括一个用户有 Change 权限的文件，那么，用户可以键入完全的 UNC 或指向文件的路径，从该文件的适当的应用程序中打开它。

4. 拒绝用户或组的权限会阻碍来自用户的权限，即使该权限已授予用户所属的组

例如，Everyone 组获得了一个文件的 Full Control 权限，而用户已被拒绝了对该文件的 Delete 权限，则用户能够读和修改文件，但不能删除它。

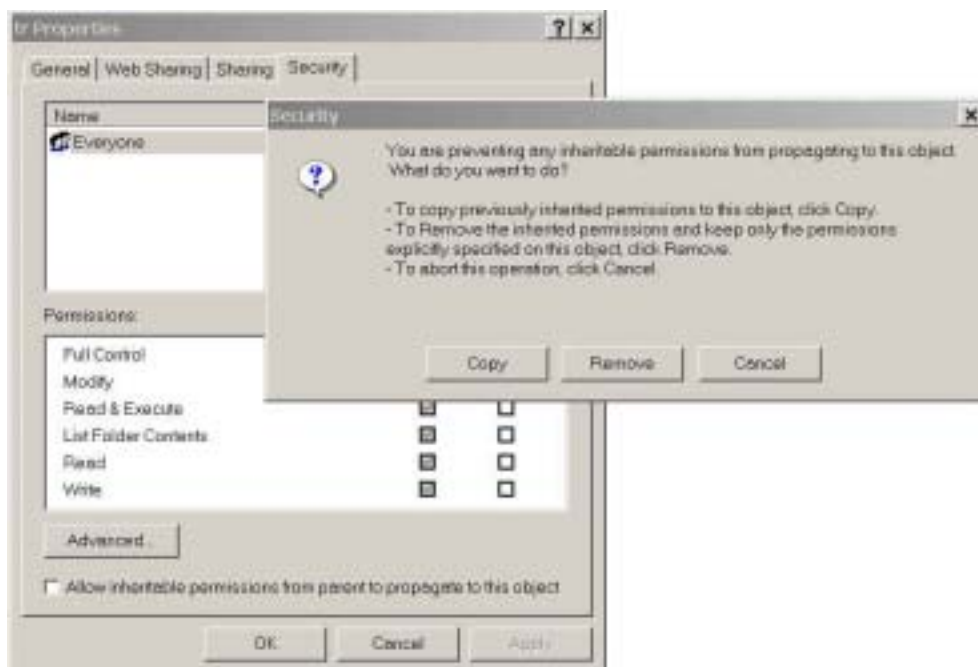


图 3.1

5. 权限继承

默认情况下，父文件夹的权限可被其中的子文件夹和文件继承。但是，这种继承是可

以阻止的。去掉“允许将来自父系的可继承权限传播给该对象”可选框，会出现一个询问对现有权限进行处理的对话框（如上图 3.1 所示）。此时，您可以进行权限的复制与删除工作。

6．对文件进行复制移动操作时，NTFS 权限的变化如下表所示：

	复制	移动
在同一 NTFS 分区内	继承目标文件夹的权限	保留原有权限
在不同 NTFS 分区内	继承目标文件夹权限	
从 NTFS 分区到 FAT 分区	丢失 NTFS 权限	
从 FAT 分区到 NTFS 分区	继承目标文件夹权限	

7．NTFS 特殊访问权限

单击文件或文件夹属性中“安全”选项卡上的“高级”，出现 NTFS 的高级权限，如图 3.2 所示：（这里只针对文件夹进行说明）

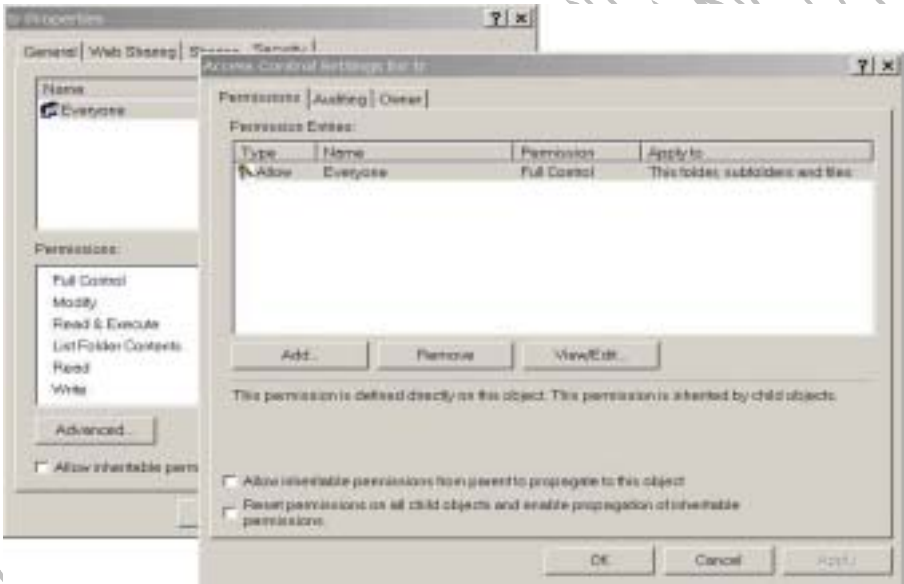


图 3.2

给文件夹和文件指定特殊访问权限需要三个步骤：

- 配置更多的权限。

通常，标准 NTFS 权限提供了所有必需的权限来保护数据。但是，在某些情况下，标准权限也不提供可能需要的特殊访问。可以使用 NTFS 权限创建特殊访问。

特殊访问权限为指定访问资源提供了更好的控制，有 13 种特殊访问权限，它们之间的组合就构成了标准 NTFS 权限，如 Read & Execute、Modify、Full Control。例如，标准 NTFS Read 权限包括 Read Data、Read Attributes 及 Read extended attributes 权限（如图 3.3 所示）。

值得注意的是“Take Ownership”权限，拥有该权限，则用户将可以获得该文件或文件夹的所有权。



图 3.3

- 转移所有权。

除了更改权限外，所有权也可以转移，有几种方法可转移所有权：

当前拥有者可以给其他用户授予 Full Control 标准权限，或 Take Ownership 特殊访问权限，允许这些用户获取所有权。

管理员可以获取在他管理控制下的任何文件夹或文件的所有权。例如，如果雇员离开公司，管理员可以获取该雇员的文件的所有权，并更改权限，让其他人能够访问这些文件或文件夹。改变所有权的界面如下图 3.4 所示：

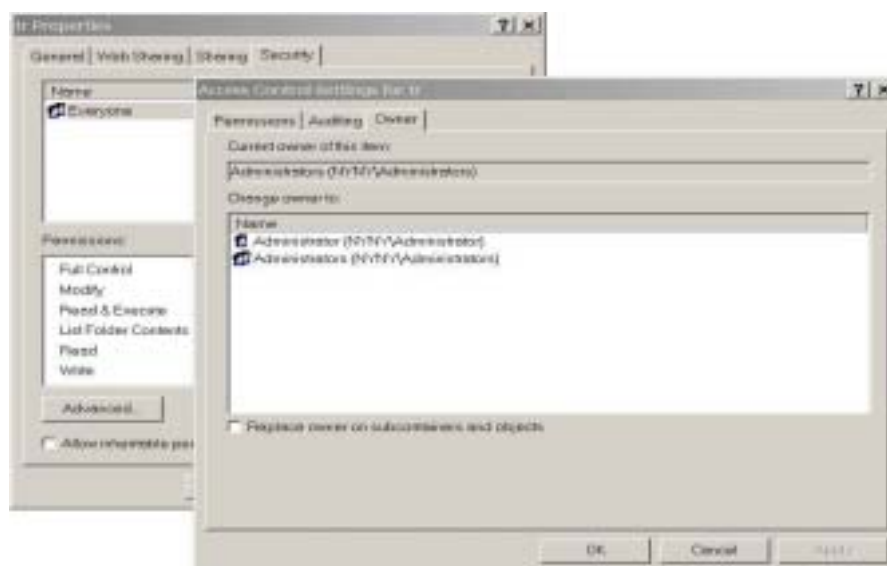


图 3.4

- 审核访问。审核涉及到 Windows 2000 的安全问题，本书将在第五章——Windows 2000 的安全管理中详细介绍。

3.2.3 磁盘压缩

NTFS 文件压缩是文件系统的一个功能。用户可以压缩整个硬盘分区上的数据，也可以对 NTFS 分区上的文件和文件夹进行压缩。

- 对于某个磁盘分区，选择其“属性”中的“常规”选项卡，选定“压缩驱动器以节约磁盘空间”选项即可进行压缩。

- 对于一个文件或文件夹进行压缩，首先打开其“属性”对话框，在“常规”选项卡上单击“高级”按钮。在“高级属性”对话框中，选定“压缩内容以便节省磁盘空间”复选框，如图 3.5 所示。

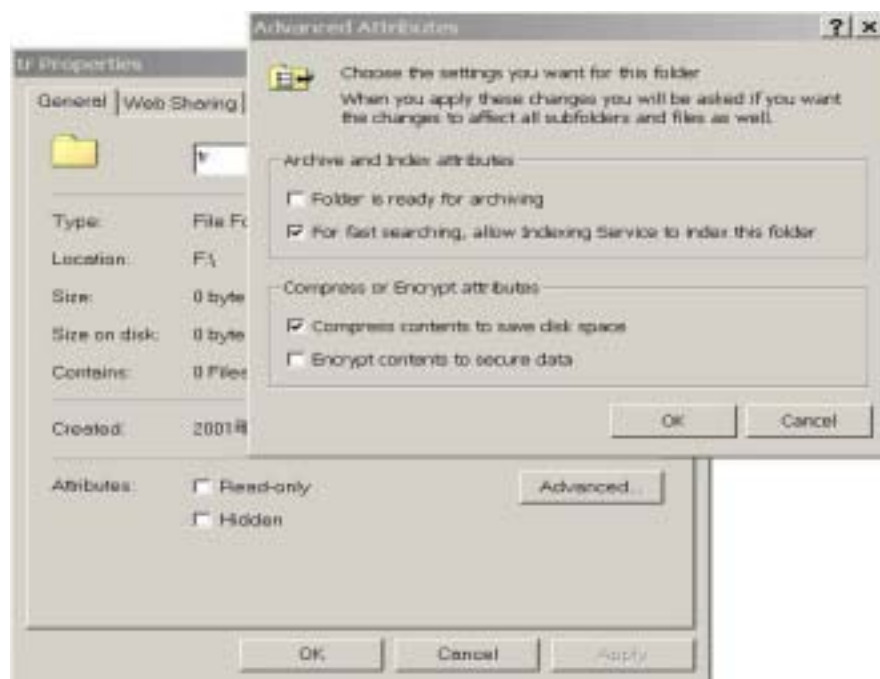


图 3.5

关于文件和文件夹在移动和复制过程中，压缩状态的改变问题请参阅 70-210 课程。

3.2.4 加密文件系统（EFS）

“加密文件系统”（EFS）提供一种核心文件加密技术，该技术用于在 NTFS 文件系统上存储已加密的文件。最重要的是，使用 EFS 可以防止非授权用户访问物理存储上的敏感数据，从而确保了文档的安全。

文件或文件夹被加密之后，用户可以象使用其它文件和文件夹一样使用它们而不必在使用之前解密已加密的文件。因为对加密该文件的用户而言，加密文件是透明的。但是，非授权用户对这些加密文件或文件夹的访问将被拒绝。

加密文件的设置方法同其它属性（如压缩）一样，具体步骤不再详述，可参考本系列教材 70-210。

值得注意的是，在使用加密文件和文件夹时，要记住：

- 只有 NTFS 卷上的文件和文件夹才能被加密。
- 不能加密压缩的文件或文件夹。首先必须对文件和文件夹解压缩，然后才能加密。
- 只有对文件实施加密的用户才能打开它。
- 不能共享加密文件。EFS 不能用于发布私人数据。
- 如果将加密的文件复制或移动到非 NTFS 格式的卷上，该文件将会被解密。

- 使用剪切和粘贴将文件移动到已加密的文件夹。如果使用拖放式操作来移动文件，则不会将它们在新文件夹中自动加密。
- 无法加密系统文件。
- 加密的文件夹或文件不能防止被删除。任何拥有删除权限的人均可以删除加密的文件夹或文件。
- 在允许进行远程加密的远程计算机上可以加密或解密文件及文件夹。然而，如果通过网络打开已加密文件，通过此过程在网络上传输的数据并未加密。
- 恢复策略是当对第一个文件或文件夹进行加密时自动执行的，以便如果丢失了文件加密证书和相关的私钥，恢复代理可以解密文件。

实验 3.1：设置 NTFS 文件和文件夹的属性

1. 打开资源管理器，在 NTFS 分区的硬盘中选择一个文件夹，单击鼠标右键，在快捷菜单中选择“属性”项；
2. 在“属性”对话框的“常规”General 选项卡中，点击“高级”按钮，在高级属性对话框中，选择是否压缩或加密文件；
3. 在“属性”对话框的“共享”Share 选项卡中，选择是否将该文件夹共享并输入共享名；点击“权限”按钮，设置共享文件夹的属性；
4. 如果系统中已安装 IIS 服务，则在“属性”对话框的“Web 共享”选项卡中选择共享，可以将该文件夹设置为一个 Web 站点的虚拟目录；
5. 在“属性”对话框的“安全”选项卡中，添加成员组，设置访问权限；点击“高级”按钮，在“访问控制设置”对话框中，设置其特殊权限，更改其所有者并添加审核项；
6. 在该文件夹选择一个文件，单击鼠标右键，在快捷菜单中选择“属性”项；
7. 文件的“常规”及“安全”选项卡中的设置与文件夹相同，注意两者的权限种类有所不同；
8. 注意文件的“属性”对话框中没有“共享”这一项，在“摘要”和“自定义”选项卡中，可以输入与文件相关的摘要信息。

3.3 共享权限与 NTFS 权限

共享文件夹（shared folder）用来向网络用户提供对文件资源的访问。当一个文件夹被共享的时候，用户可通过网络连接到该文件夹并访问其中包含的文件。要获得对文件的访问，用户必须拥有访问共享文件夹的合适权限。

注意共享文件夹的权限仅针对通过网络访问的用户，当用户在共享文件夹所在的计算机上时访问文件时，共享文件夹的权限不起任何作用。

在 NTFS 分区上提供资源访问的一种策略是首先设置默认共享文件夹的权限，然后通过分配 NTFS 权限来进行访问控制。有关共享文件夹及其权限已在本教材 70-210 中详细介绍，下面只介绍共享文件夹权限与 NTFS 权限的关系。注意这种关系仅针对用户通过网络访问 NTFS 分区的资源而言：

- 拒绝权限覆盖其它权限。对于某一用户或组，不管是 NTFS 权限被设置为拒绝访问，还是共享权限被设置为拒绝访问，只要有一个存在，那么该用户或组对该资源的访问权限为拒绝。
- 如果共享权限对文件夹进行配置，NTFS 权限对此文件夹或文件夹中的文件进行配置，那么，最严格的权限将成为用户访问资源的有效权限。

例如，某个用户对一个文件夹的共享权限为“Change”，但所拥有的 NTFS 权限为

“ Read ”, 取两者权限相对较严格的, 则此用户对这个文件夹的权限为 “ Read ”。

实验 3.2 : NTFS 权限与共享权限的组合

1. 在本地机器上新建一个文件夹, 如: E:\Doc;
2. 在 E:\Doc 的文件夹下新建一个文件 SubDoc, 所有属性按默认设置;
3. 切换到此文件夹的安全选项卡, 去掉 Allow inheritable permissions from parent to this object 选项, 在弹出的对话框中选择 copy;
4. 在文件夹的安全选项卡中, 为 Everyone 仅设置 read 权限 (去掉其它复选框);
5. 单击 Apply 应用按钮;
6. 切换到 E:\Doc 文件夹属性的 Share 选项卡中, 选中 Share this folder, 其它则按默认设置, 单击 OK;
7. 通过网上邻居访问此 Doc 共享文件夹, 试着删除 SubDoc, 看有何结果以验证权限的设置。

注意: 上述实验中, 虽然文件夹的共享权限为 Full Control, 但由于文件的 NTFS 权限为 Read, 故用户没有权限删除此文件。

3.4 磁盘配额

3.4.1 磁盘配额概述

磁盘配额提供了一种管理用户可以占用的磁盘空间数量的方法。利用磁盘配额, 可以根据用户所拥有的文件和文件夹来分配磁盘使用空间; 也可以设置磁盘配额、配额上限, 以及对所有用户或者单个用户的配额限制; 还可以监视用户已经占用的磁盘空间和他们的配额剩余量。

值得注意的是, 在应用磁盘配额之前应该考虑:

- 磁盘卷必须用 Windows 2000 中的 NTFS 版本格式化磁盘卷;
- 必须是 Administrators 组的成员才能管理磁盘分区上的配额;
- 文件压缩不影响配额统计。例如, 如果用户 A 限制使用 3MB 的磁盘空间, 那么只能存储 3MB 的文件, 即使文件是压缩的。

3.4.2 磁盘配额 (Disk Quota) 的启用与应用

一、启用磁盘配额

要启用磁盘配额, 首先打开这个磁盘分区的 Properties 对话框, 单击 Quota (配额) 选项卡, 选中 Enable Quota Management (启用磁盘管理) 的复选框即可对磁盘配额选项进行配置 (如图 3.6 所示)。



图 3.6

二、设置默认的磁盘配额

可以为配额设置两个值，即磁盘配额限制和磁盘配额警告级别。前者指允许一个用户使用的磁盘空间数量；后者设置的值表明了用户已经使用的磁盘空间已接近了磁盘限额的上限。

三、判断磁盘配额的状态

在 Properties 对话框中，通过检查交通信号灯图标并读取图标右边的状态信息，可以对配额的状态进行判断（如上图 3.6 所示）。交通信号灯的颜色和对应的状态如下：

- 红色的交通信号灯表示磁盘配额没有启用。
- 黄色的交通信号灯表示 Windows 2000 正在重建磁盘配额的信息。
- 绿灯表明磁盘配额系统已经激活。

四、设置用户配额项

可能有一些用户，它们的配额应当比你规定的默认限制大一些或少一些；还有一些用户不应加以任何限制。如果要为用户定制配额项，单击“配额项”，打开“配额项目对话框”，如下图 3.7 所示：

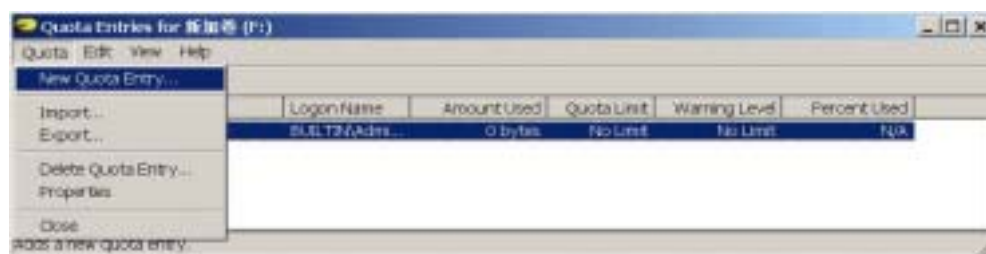


图 3.7

在默认情况下，对话框列出 administrator 组，且对其没有任何限制。如果要规定一个配额项，选择如上图所示的“新建配额项”，然后从选择用户对话框中选定用户，再单击“确定”。你可以选定多个用户，只要你想对这些用户指定同样的配额限制。选定后，单击“确

定”，就可以对用户应用相应的配额了（如图 3.8 所示）。



图 3.8

3.4.3 使用磁盘配额应注意的原则

下面列出的是使用磁盘配额的一些原则：

- 默认情况下，管理员不受磁盘配额的限制；
- 清除 Deny Disk Space To Users Exceeding Quota Limit 复选框，用户在超过限额后仍能继续存储数据，但系统可以通过监视硬盘的使用情况，作出相应的决策。
- 通常，需要在共享的磁盘卷上设置磁盘配额，以限制用户存储数据使用的空间。
- 在删除用户的磁盘配额项之前，这个用户具有所有权的全部文件都必须被删除，或者将所有权移交给其他用户。

实验 3.3：使用磁盘配额

1. 选择一个 NTFS 分区的磁盘，打开“属性”对话框，选择“配额”选项卡；
2. 根据上文的论述，配置磁盘配额。

3.5 分布式文件系统（Dfs）

3.5.1 Dfs 概述

分布式文件系统(distributed file system, DFS)是一个 Windows2000 服务。该服务帮助网络管理员在分布式企业网络中管理文件资源。分布式文件系统(distributed file system, DFS)将分布在多个域和多个计算机上面的共享数据组织成一个统一结构的树状视图和命名体系，便于用户在网络中查找和定位要访问的文件资源。

Dfs 共享使用包含根和 Dfs 链接的一个树状结构。要建立 Dfs 共享，必须首先建立 Dfs 根 Root。在 Dfs 根下，可以有多个 Dfs 链接，每一个链接都指向网络中的一个共享文件夹。Dfs 根下的 Dfs 链接表示可以在不同文件服务器上进行物理定位的共享文件夹（<computer_name>\share_name>）。

3.5.2 Dfs 的优点

同普通的共享文件夹相比，Dfs 有以下优点：

- 简化了网络管理。如果一个服务器失效，可以将 Dfs 链接从一个服务器移动到另一个，而用户并不知道这种更改。
- 使客户访问资源变得简单。客户通过使用一个简单的名称空间（Dfs 根）来访问文件资源，而不需要在整个共享资源中变换路径查找。
- 使文件服务器的更换变得容易。管理员只需要简单地更新 Dfs 管理单元中的新服务器的

路径,就可以替换文件服务器,而不影响网络客户使用的名称空间。

- 提供了负载平衡与容错。由于 Dfs 客户随机地从 Dfs 服务器返回的备用列表选择一个物理服务器来连接,则 Dfs 提供了一级负荷平衡和容错功能。

3.5.3 Dfs 根的类型

有两种类型的 Dfs 根可以在 Windows 2000 Server 上进行配置:独立 Dfs 根和域 Dfs 根(有时称做容错 Dfs 根)。

1. 独立 Dfs 根

下面是独立 Dfs 根的一般特征:

- 独立 Dfs 的信息存储在本地注册表中。
- 一个独立 Dfs 根只允许一级 Dfs 链接。
- 当使用 Distributed File System 管理单元去连接现有的独立 Dfs 根时,浏览列表知道的所有服务器都被检索,这是因为启用 Dfs 的服务器没有注册唯一的 NetBIOS 名称。
- 虽然我们推荐将资源放在 NTFS 的格式化分区,但独立 Dfs 的根可以位于所有支持的文件系统中。
- 独立 Dfs 根不提供复制或备份;相应地,该 Dfs 根代表了一个单独的故障点。可以在独立 Dfs 根下创建一个副本,但是,文件复制服务是不可行的。

2. 域 Dfs 根

下面是域 Dfs 根(也称为 Dfs 容错根)的一般特征:

- 在一个域 Dfs 根下,多个服务器为 Dfs 名称空间分发备用对象。容错 Dfs 根使用 Active Directory 服务来存储 Dfs 树的拓扑结构,并将这个根作为一个单独的故障点删去。
- 一个容错 Dfs 根存放在 Active Directory 服务中,并在每一个参与的服务器中复制。Dfs 树的更改自动与 Active Directory 服务同步。这样,不论 Dfs 根因为何种原因离线,都可以确保您总可以恢复 Dfs 树的拓扑结构。还可以通过为 Dfs 指定后备资源来在文件和内容级别上执行容错功能。在 Dfs 树中,任一分支节点都可以由一组复制的资源来提供服务。如果一个客户对一个后备资源的连接不管出于何种原因失败,Dfs 的客户将会尝试连接另一个。Dfs 客户循环搜索后备资源,直至发现可用的资源。
- 容错根必须位于 NTFS 5.0 版的硬盘分区中。
- 域和服务列表可以通过查询所有容错 Dfs 根的全局编录来获得(ObjectClass=ftDfs)。
- Dfs 副本拓扑结构使用现有的 Active Directory 副本拓扑。

3.5.4 Dfs 服务的安装与配置

一、Dfs 的安装

Dfs 服务是随着 Windows 2000 Server 的安装而自动安装的。这个服务可以被暂停、终止和启动,但不能从操作系统中将删去。

二、Dfs 的创建与配置

• 独立 Dfs 根的创建

独立的 Dfs 在一台单独的计算机上存放 Dfs 拓扑结构。如果存放 Dfs 拓扑结构的计算机或是 Dfs 使用的共享文件夹失效时,这种类型的 Dfs 不提供容错功能。

要创建独立 Dfs 根,应使用 Distributed File System 管理单元来启动 New Dfs Root 向导。下图 3.9 给出了选择“Create A Stand-Alone Dfs Root”单选按钮后的“Select The Dfs Root Type”屏幕。

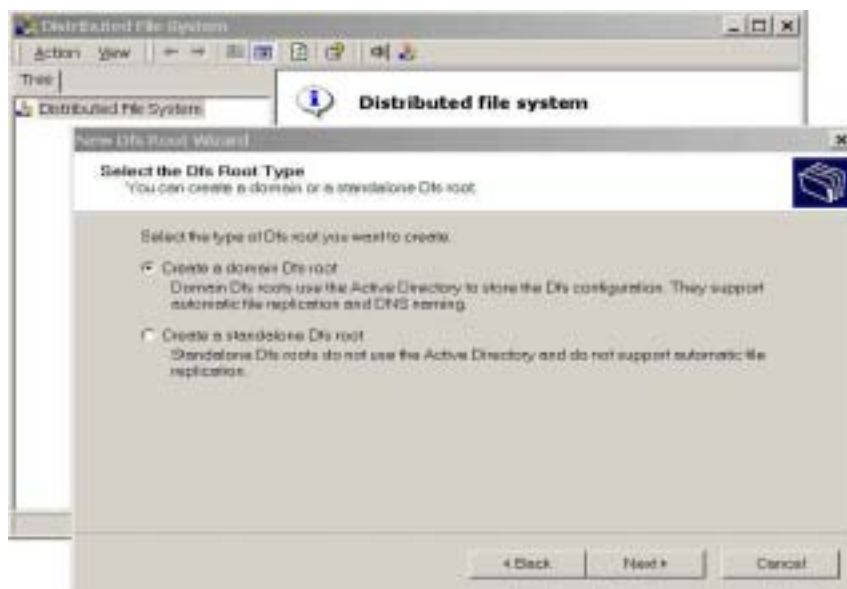


图 3.9

- 域 Dfs 根的创建

域 Dfs 将 Dfs 拓扑结构写在 Active Directory 存储器中。这种类型的 Dfs 允许 Dfs 链接为了容错而指向多个同一共享文件夹(也称为副本)。此外,它还支持 DNS、多级子卷和文件复制。

要创建容错 Dfs 根,使用 Distributed File System 工具来启动 New Dfs Root 向导。

3.5.5 配置新的 Dfs 链接

用户可以在不知道所引用资源的物理位置的情况下浏览 Dfs 根下的文件夹。在创建 Dfs 根后,就可以创建 Dfs 链接(也称做子节点)。

要创建 Dfs 链接,打开 Distributed File System 管理单元,单击需要连接 Dfs 链接的 Dfs 根。在 Action 菜单中,单击 New Dfs Link。此时出现 Create A New Dfs Link 对话框,如图 3.10 所示:

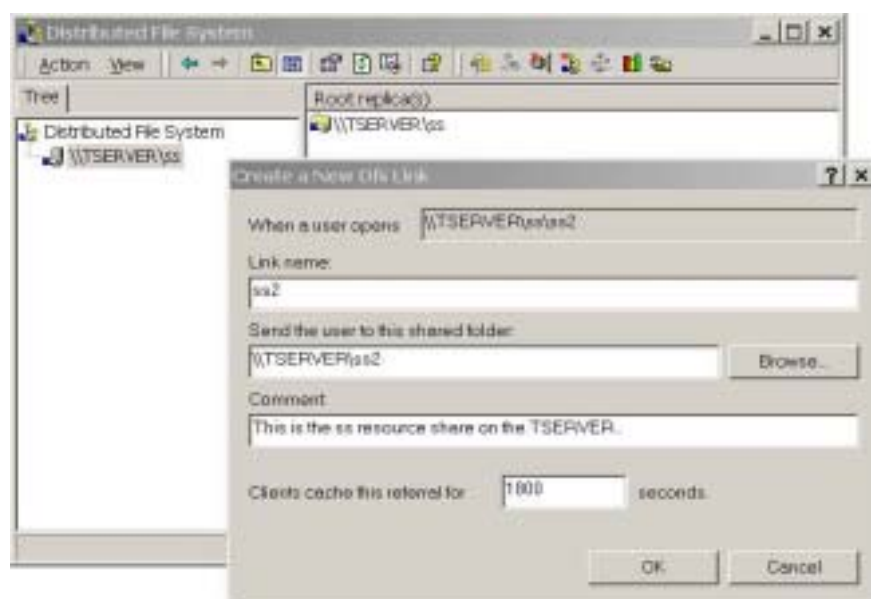


图 3.10

在创建一个新的 Dfs 链接的对话框中，“Link name”表示在连接到 Dfs 后，用户即可在 Dfs 根下看见的名称。“Send the users to this shared folder”表示了 Dfs 链接指向的共享文件夹的实际位置的 UNC 名。

创建完后，Dfs 链接将出现在 Distributed File System 工具中的 Dfs 根卷下，并在 Dfs 根下，作为启用 Dfs 客户的文件夹出现。下图 3.11 表示了名为 \\TIANR\\humanGX 的 Dfs 根的外观，以及另一个服务器上的 Dfs 链接。

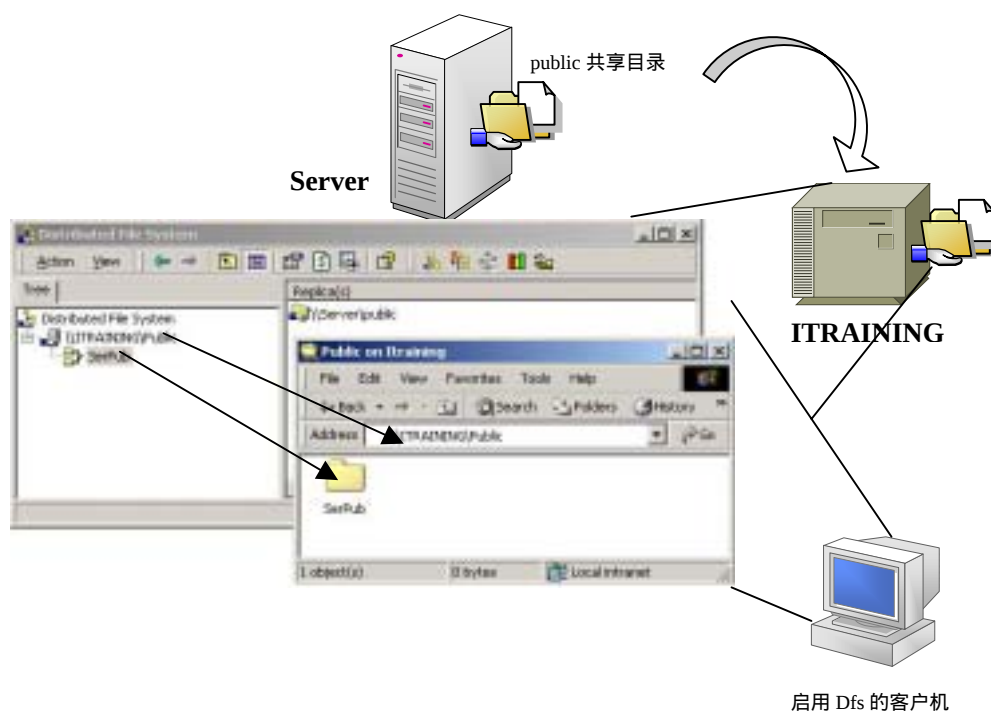


图 3.11

注意 Windows2000、Windows NT 4.0 和 Windows 98 系统中已包括 Dfs 客户端软件，可

以直接访问 Dfs 资源，而 Windows 95 系统则必须另外安装客户端软件。

实验 3.3：在 Server01 上创建独立 DFS 根

1. 在本地计算机上创建一个文件夹，如 E:\Public，共享该文件夹；
2. 打开 DFS 管理单元，在 Action 菜单中单击 New Dfs Root；
3. 在出现的 DFS 向导中单击 Next，在 Select The Dfs Root Type 界面上，选择 Create A Stand-Alone Dfs 选项，单击 Next；
4. 在 Specify The Host Server For The Dfs Root 界面上，确认服务器的存在并输入服务器名，如 Server01，或者浏览选择，单击 Next；
5. 选择 Use An Existing Share 单选按钮，再从下拉菜单中选择第一步已建好的共享目录 Public，单击 Next；
6. 填入相应的 Comment 注释信息，单击 Next；
7. 单击 Finish 完成独立 DFS 根的创建；

实验 3.4：在上一个实验的基础上创建 DFS 链接

1. 在 Dfs 管理单元中选择\\Server01\Public
2. 单击 Action 菜单，单击 New Dfs Link；
3. 在出现的 Create A New Dfs Link 中的 Link Name 文本框中键入链接名，如 intranet；
4. 单击 Browse，选择要链接的对象，如 Server02\internal；
5. 在 Comment 文本框中键入相应的 Comment，单击 OK 完成 DFS 链接的创建；

创建完 DFS 根和 DFS 链接之后，可以通过网络访问该分布式共享资源，观察 DFS 分布式文件系统的特点。