第 7 章　文件系统的安全

7.1　Windows 2000 的文件系统

Windows 2000 支持 NTFS、FAT16 和 FAT32 等多种文件系统格式。而只有使用 NTFS 文件系统格式，才能实现 Windows 2000 中的全部功能，其中包括一些特有的安全特性。但如果需要从其他操作系统（包含 MS-DOS）上访问这个磁盘的文件，则必须将该磁盘格式化为 FAT 文件系统（包括 FAT16 和 FAT32），不过这将缺乏安全性。

Windows 2000 包括 NTFS 文件系统的最新版本 NTFS v5，它具有以下这些重要的安全特性：

- 权限控制
- 加密
- 压缩
- 磁盘配额

1. 文件系统基础

表 7-1 说明了 Windows 文件系统的一些基础概念和术语：

表 7-1 文件系统的基础名词表

名词	说明
分区	是物理磁盘的一部分，其作用如同一个物理分隔单元。分区通常指主分区或扩展分区。用户可以创建一个分区用来储存信息（例如备份数据），或者和实现操作系统的双重启动。当用户在硬盘上创建分区时，磁盘被分割成一个或多个可用不同文件系统（例如 FAT 或 NTFS）格式化的区域。
主分区	是标记为由操作系统使用的一部分物理磁盘。一个磁盘最多可有 4 个主分区（如果有 1 个扩展分区，则最多有 3 个主分区）。只有主分区可标记为活动分区，即硬件寻找启动操作系统的启动文件的地方（只能有一个活动分区）。
扩展分区	是从硬盘的可用空间上创建的分区，而且可以将其再划分为逻辑驱动器。每个物理磁盘上的 4 个分区只允许使用其中之一作为扩展分区。创建扩展分区不需要有主分区。
逻辑驱动器	是从扩展分区中划分出来的段，每个段就是一个逻辑驱动器
卷	是格式化后由文件系统使用的分区或分区集合。可以为 Windows 2000 的卷指定驱动器名，并使用它来组织目录和文件。
卷集	是作为一个逻辑驱动器出现的分区组合。

2. FAT 文件系统

FAT 文件系统最初用于小型磁盘和简单文件结构的简单文件系统。FAT 文件系统得名于它的组织方法：放置在卷起始位置的文件分配表（File Allocation Table）。为了保护卷，FAT 文件分配表还有复本，确保即使损坏了一份也能正常工作。

因为需要与早期版本的 Windows 系统以及其他大多数的操作系统兼容，Windows 2000 中仍然支持 FAT16。对于 Windows 2000 和 Windows NT 系统而言，FAT16 卷所支持的最大空间为 4GB。而理论上来说，FAT32 可使卷最大达到 2TB。

FAT16 与 FAT32 之间最主要的区别就是逻辑分区大小的不同。FAT32 通过扩展单个逻辑驱动器容量达到至少 127GB，从而打破了 FAT16 的 2GB 逻辑驱动器的限制。

3. NTFS 文件系统

Windows 2000 中包含有 NTFS v5。该版本的 NTFS 提供了 FAT 中所没有的功能和性能。NTFS 是以卷为基础的，而卷建立在磁盘分区上。当以 NTFS 格式来格式化磁盘分区时就创建了 NTFS 卷。分区（partition）包括基本分区和扩展分区。扩展分区可以由逻辑分区组成。分区是磁盘的组成部分，是一个能够被格式化和单独使用的逻辑单元，在磁盘的自由空间上创建的。一个磁盘可以有多个卷，一个卷也可以由多个磁盘组成，如 RAID 磁盘阵列。

NTFS 具有分布式环境下文件服务器和高端个人计算机所需的安全性特点，且数据访问控制及用户权限对于数据的安全性非常重要。

- 多数据流：NTFS 支持多数据流，此处流的名称标识了文件中新的数据属性。句柄对每个数据流是公开的，因此数据流是惟一的文件属性集合。流除了一般性的使用权限之外，还具有独立的随机锁、文件锁以及文件大小属性。该特点可使用户将数据作为单个元素进行管理。
- 重析点：重析点是 NTFS v5 中的新型文件系统对象。它具有一个用户控制数据的可定义属性，且在输入输出子系统中用于扩展功能。
- 改动日志：NTFS 所使用的改动日志提供了对卷中文件所做改动的持续的记录。对每个卷，NTFS 使用改动日志以跟踪有关于添加、删除和改动文件的信息。改动日志比用于决定给定名字区的改变的时间戳或文件标志信息更有效。
- 加密：在 NTFS v5 中实现的文件与目录级的加密可增强 NTFS 卷中的安全性。Windows 2000 使用加密文件系统（Encrypting File System, EFS）将数据存储在加密表当中，它在访问存储介质时提供安全机制。
- 压缩：Windows 2000 支持对 NTFS 卷单个文件的压缩。被压缩在 NTFS 卷中的文件可被任意基于 Windows 的应用程序读写，而无须先用另一程序进行解压。解压操作会在读取文件的时候自动发生，而在文件被关闭或保存时，文件将再次被压缩。
- 磁盘配额：磁盘配额是 NTFS 中的新特性。
- 稀疏文件支持：稀疏文件允许程序创建更大的文件，但消耗了所必需的磁盘空间。

NTFS 系统也有如下一些缺陷。

- 用 NTFS 格式化的卷在 MS-DOS、Windows 95 及 Windows 98 系统中不可访问。Windows 2000 中实现的 NTFS 高级特性在 Windows NT 4.0 及以前版本中不可用。
- 当较小的卷中包含许多小文件时，与 FAT 相比较而言管理 NTFS 的开销可能导致性能的略微降低。

4. NTFS 文件属性

NTFS 将每个文件（或文件夹）作为文件属性的集合来看待。该集合的组成元素包括文件名，安全性信息及其数据等文件属性。每个属性名和属性类型编码定义为一个属性。

当文件属性可存于该文件的 MFT 文件记录中时，则称之为驻留属性。如文件名和时间戳等。当文件信息过大而不能存在其 MFT 文件记录中时，则是非驻留属性。非驻留属性定位于磁盘空间的一个或多个簇中，且作为卷中可变数据流来存储。NTFS 创建属性列表的属性以描述驻留与非驻留属性记录的位置。

表 7-1 列出了由 NTFS 文件系统格式所定义的文件属性。

表 7-1　NTFS 文件属性类型

属性类型	描述
标准信息	包括时间戳与链接数量的信息
属性列表	列出不适宜于 MFT 记录中的所有属性记录的位置
文件名	对长的或短的文件名均可重复使用。文件的长名称最多可达到 255 个统一编码的字符。文

	件的短名称是 MS-DOS 读取、8.3 结构、密集型名称。另外 POSIX 所需的名称和硬链接可作为附加文件名属性包括在内
安全性描述	文件所有者和访问文件用户的信息
数据	包含文件数据。NTFS 允许每个文件有多个数据属性
对象标识符	卷的惟一文件标识符
记录工具流	同数据流相似，但对记录工具流的操作像 NTFS 元数据的改动那样记录在了 NTFS 记录文件中。用于文件加密系统（EFS）

5. FAT 到 NTFS 的转换

FAT 卷在任何时候均可使用 Convert.exe 工具转换为 NTFS 卷。用户在执行转换之前没有必要备份原有的文件系统，因为使用 Convert 转换文件系统格式并不会给卷中原有的文件数据带来任何改变。但要注意的是：从 FAT 文件系统格式转换而来的卷性能没有初始就使用 NTFS 文件系统格式化的卷的性能好。此外，这个过程是不可逆向的，即无法从 NTFS 卷返回到 FAT 卷。

Convert 的命令语法为：

CONVERT volume /FS:NTFS [/V]

7.2 NTFS 的权限控制

NTFS 权限是与文件系统相关的访问控制规则，作用的对象是文件和文件夹，它用来指定哪些用户可以访问文件系统对象以及可以使用什么样的方式访问。

NTFS 权限只能使用在 NTFS 卷上，而不能使用在 FAT 或 FAT32 文件系统上。无论用户是通过计算机控制台还是网络来访问文件或文件夹，NTFS 的权限控制都有效。此外，Windows 2000 还支持共享的权限控制，该控制在功能上很相似，但只是通过网络来控制用户对共享的访问。

7.2.1 标准的 NTFS 权限

NTFS 文件系统对文件和目录的标准权限控制，由于和 Windows NT 系统中几乎完全一样，所以其原理和技术可参看第 2 章中相关描述。

拥有“完全控制”权限的 Administrators 组和用户以及文件和文件夹所有者可通过执行以下操作来给用户和组分配 NTFS 文件对象权限。

（1）在“Windows 资源管理器”中右击要为其分配权限的文件或文件夹。

（2）从弹出菜单项中选择“属性”命令。

（3）在“属性”对话框中切换到“安全”选项卡，如图 7-1 所示。

（4）在“权限”栏里根据需要配置权限。

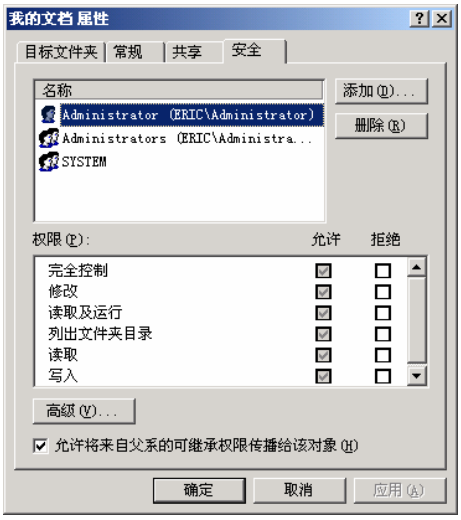

图 7-1 设置 NTFS 权限

7.2.2 NTFS 权限控制原则

1. 权限积累

用户对资源（对象）的有效权限是分配给单个用户账户以及用户所述的所有组的 NTFS 权限的总和。也就是说，如果一个用户同时属于两个组，那么他就有了这两个组所允许的所有权限。

举个例子，如果一个用户即是 A 组的成员，又是 B 组的成员。A 组拥有对某文件夹的“读取”权限，而 B 组拥有对该文件夹的“写入”权限，则该用户同时拥有对该文件夹的“读取”和“写入”权限。

2. 文件权限优先于文件夹权限

NTFS 文件权限优先于 NTFS 文件夹权限。也就是说如果一个用户拥有对一个文件的访问权限，即便他不拥有对该文件所在文件夹的访问权限，他仍然能够访问该文件。虽然由于用户不具有相应的文件夹权限，文件所在的文件夹将对他不可见，但通过使用完整的 UNC（Universal Naming Convention）路径或本地路径就可从相应的应用程序打开该文件，获得对他们拥有权限的文件的访问。换句话说，如果没有文件所在文件夹的访问权限，就必须知道该文件的完整路径。这是因为无法看到该文件夹，也不能浏览文件夹中需要访问的文件。

3. “拒绝”权限优先于其他权限

NTFS 的权限控制可以拒绝用户或组访问特定的文件或文件夹。“拒绝”权限要比其他所有权限的优先权要高。即使用户作为组成员可以访问文件或文件夹，但“拒绝”权限仍可以阻止该用户所拥有的其他权限。这是因为在访问控制列表中，有关“拒绝”的 ACE 放置在 ACL 的最前面，所以会优先匹配。

举个例子，如果一个用户即是 A 组的成员，又是 B 组的成员。A 组拥有对某文件夹的“写入”权限，而该文件夹中包含有 File 1 和 File 2 这两个文件；B 组则明确被拒绝了对 File 2 的“写入”权限。结果就是该用户能够写入 File 1，而不能写入 File 2。

7.2.3 NTFS 权限继承

默认情况下，分配给父文件夹的权限将可应用于该文件夹内的子文件夹和文件。当分配

NTFS 权限以允许用户或组访问文件夹时，也就为用户或组分配了相同的权限以访问该文件夹内的所有现有文件和子文件夹，以及在该文件夹内新建的所有文件和文件夹。

若要阻止子文件夹和文件继承文件夹的权限，需要设置相关选项来防止特定文件或文件夹继承分配给父文件夹的所有权限。如果阻止文件夹的权限继承，那么该文件夹则成为顶级父文件夹。分配给该文件夹的权限仍然会被其子文件夹和文件所继承。

在文件或文件夹的“属性”对话框的“安全”选项卡中，这种继承关系由“允许将来自父系的可继承权限传播给该对象”复选框内的复选标记来表示。如果该复选框选中，但颜色为灰色，那么说明该文件或文件夹已从文件夹继承权限。若要阻止子文件夹或文件从父文件夹继承权限，可将该复选框设置为不选中。这时候，系统会提示用户进行选择，如图 7-2 所示。

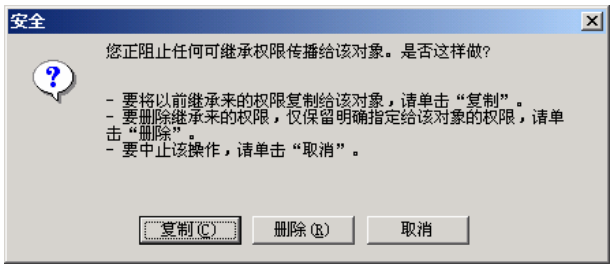

图 7-2 阻止权限继承的选项选择

其中，“复制”表示将权限从父文件夹复制到当前文件夹，然后拒绝从父文件夹继承随后分配的权限。而“删除”表示将删除从父文件分配过来的权限，只保留明确给文件或文件夹的权限。

7.2.4 特殊的 NTFS 权限

通常情况下，标准的 NTFS 权限就可以提供保护文件系统对象所需的所有访问控制。但是，标准的 NTFS 权限有时并不能够满足需要分配给用户和组特定级别访问权限的要求。若要创建特定级别的访问，可分配 NTFS 特殊权限。

通常用来控制文件系统资源访问的标准权限实际上是称为特殊权限的具体权限预先配置好的组合。特殊权限给管理员提供了额外的访问控制能力。可以给文件和文件夹分配多种类型的特殊权限，这其中比较重要的是“更改权限”和“更改所有者”这两个特殊权限。

1. 更改权限

通过向其他用户分配“更改权限”这个特殊权限，就可以让他们更改文件或文件夹的权限，而无需分配给他们文件或文件夹的“完全控制”权限。这样，该用户将不能删除或写入文件或文件夹，但却能够控制其他用户对该文件或文件夹的访问。

2. 更改所有者

使用“更改所有者”这个特殊权限可以让用户或组成为文件或文件夹所有者的能力。文件或文件夹的当前所有者或拥有“完全控制”权限的任何一位用户都可给其他用户或组授予“完全控制”标准权限或“更改所有者”特殊权限，将文件或文件夹的所有权转让给该用户或组成员。

无论分配了什么权限，管理员始终都能够取得任何一个文件或文件夹的所有权。如果一位管理员取得了某文件的所有权，那么 Administrators 组就成为了该文件的所有者，而且 Administrators 组的任何成员都可以更改该文件的权限，并可将“更改所有者”权限分配给其他用户或组。

若要更改文件或文件夹的所有权，可按照如下步骤操作：

（1）在“ Windows 资源管理器 ”中右击要为其分配权限的文件或文件夹。

（2）从弹出菜单项中选择“ 属性 ”命令。

（3）在“ 属性 ”对话框中切换到“ 安全 ”选项卡。

（4）单击“ 高级 ”按钮打开“ 访问控制设置 ”对话框。

（5）切换到“ 所有者 ”选项卡，如图 7-3 所示。

（6）在“ 将所有者更改为 ”栏中选中自己的用户名称。若还要接管所有子文件夹和对象所有权的话，就选中“ 替换子容器及对象的所有者 ”复选框。

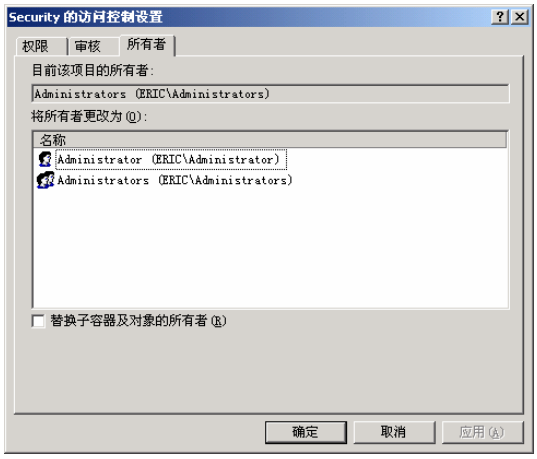

图 7-3　接管文件和文件夹的所有权

7.2.5　Cacls 命令行工具

用户可使用 Cacls 命令来显示和修改文件和目录的访问控制列表（ACL），该命令的语法为。

Cacls Filename [/T] [/E] [/C] [/G user:perm] [/R user [...]] [/P user:perm [...]] [/D user [...]]

表 7-2 描述了该命令的选项。

表 7-2　Cacls.exe 的选项

选项	描述
/ t	改变当前目录及所有子目录
/ e	编辑 ACL 而不替换
/ c	在出现拒绝访问错误时继续
/g user:perm	赋予指定用户的访问权限，此处 perm 可为：R（读取）；C（更改）；F（完全控制）
/r user	撤销指定用户的访问权限（必须与/e 一起使用）
/p user:perm	替换指定用户的访问权限，此处 perm 可为：N（无）；R（读取）；C（更改）；F（完全控制）
/d user	拒绝指定用户的访问

在 Cacls 命令中可使用通配符来指定多个文件。也可在命令中指定多个用户。

如果用户文件或目录上对多个用户已经有了访问权限的集合，而且在运行时不使用/e 选项，那么除了命令行中指定的用户与访问权限之外，其他所有用户的访问权限都将被删除。所以，如果需要针对某文件更改某用户的访问权限，而不改变其他用户在该文件上的访问权限，那么应该使用以下语法：

- Cacls Filename | Folder /e /r username
- Cacls Filename | Folder /e /g username : permission
- Cacls Filename | Folder /e /p username : permission

7.3 加密文件系统（EFS）

7.3.1 加密文件系统概述

重要数据通常是作为未保护的文件存在于计算机的磁盘之中。如果 Windows 2000 是惟一可以运行的操作系统并且硬盘不会被物理拆除的话，那么可以对存储在 NTFS 分区中的敏感信息进行访问的权限控制。但如果有人能够从物理上访问计算机或者磁盘驱动器的话，那么就可以轻而易举的获取这些敏感信息。

1. 数据的非授权访问

通常个人计算机系统是可以在使用硬盘引导之前从软盘引导，用户可以用它来修复磁盘损坏和修复损坏的引导分区，但这也增加了可以引导不同的操作系统的便利。这也就意味着能够以物理途径访问系统的人可以使用允许从 MS-DOS 和 UNIX 操作系统访问 NTFS 文件的工具（如 Ntfs4dos 等）来读取 Windows NTFS 的磁盘结构，来绕过 Windows 2000 系统文件访问控制的内置安全特性。虽然许多硬件配置提供了类似于引导密码的特性用来限制此类访问，但这种特性并没有广泛使用。在多用户共享一个工作站的特定环境中，它们就不能很好的发挥作用。甚至有可能的话，攻击者可以重新安装一套 Windows 2000 操作系统，这样就可以使用新的管理员账号完全访问磁盘上的数据。

未经授权的数据访问已成为一个严重问题，比较典型的有：

- 失窃的笔记本计算机
- 不受限制的访问

2. 传统的数据加密技术

数据加密是上述问题的惟一解决方案。市场上有很多产品使用由口令演变而来的密钥技术来提供应用程序级的文件加密。但这些加密方法大多具有一些比较严重的局限性。

- 手动加解密：对大多数产品而言，加密服务对用户不透明。每次使用前，用户须先手动将文件解密，文件完成后再重新加密。如果用户忘记了加密文件，那么该文件将不受到保护。因为每次使用必须指定要加密（和解密）文件，所以它可能会被忽略。
- 临时文件和分页文件的泄密：很多应用程序在用户编辑文档时创建临时文件（如 Microsoft Word）。这些临时文件存放在磁盘上未经加密，即使原始文档加过密也是如此，这样数据很容易被窃取。应用程序级加密运行在 Windows 用户模式下，这意味着用户的密钥可能存储在分页文件中。仅仅通过挖掘一个内存分页文件，就可以轻而易举地使用一个密钥来访问所有文档。
- 安全性差：密钥来自口令，如果使用很容易记忆但强度不大的口令，那么基于字典的攻击将可以轻易的破坏这种安全性。
- 缺乏数据恢复：大多数的产品不提供数据恢复的服务。而提供基于口令的数据恢复时，又产生了另一个访问的漏洞：要窃取数据的攻击只需获得此恢复机制的口令，就可以获得对加密文件的访问。

3. Windows 2000 的文件加密系统

Windows 2000 操作系统在设计的时候综合考虑了包括上述局限性在内的众多问题，它所包含的文件加密系统（EFS）提供了在磁盘上保存 NTFS 加密文件的核心技术。由于 Windows 2000 的文件加密系统所使用的加密技术是基于公私钥机制的，而且 EFS 作为综合

系统服务运行，这就使得它容易管理、很难被攻击并且对于用户是透明的。如果试图访问加密文件的用户拥有该文件的密钥的话，他就能够打开这个文件，并且像普通文档一样透明的使用它。而没有此文件密钥的用户就无法访问，即使是新安装系统的管理员也一样。

7.3.2 EFS 的结构

在 Windows 2000 操作系统中，加密文件系统（EFS）的结构如图 7-4 所示。

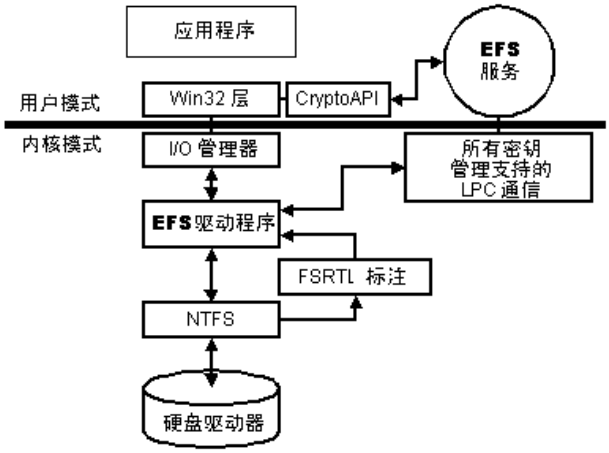

图 7-4 加密文件系统（EFS）的结构图

EFS 由以下组件组成。

- EFS 驱动程序。EFS 驱动程序在 NTFS 的上面一层。它与 EFS 服务通信，请求文件加密密钥、DDF、DRF 和其他密钥管理服务。它将信息送到 EFS 文件系统运行时库（FSRTL），以透明地执行各种文件系统操作（打开、读取、写入和附加）。
- EFS FSRTL。FSRTL 是 EFS 驱动程序中的一个模块，用于实现 NTFS 标注以处理各种文件系统操作，如对加密文件和目录的读取、写入和打开操作，以及文件数据写入磁盘或从磁盘中读取时对文件数据的加密、解密和恢复。即使 EFS 驱动程序和 FSRTL 都是以单个组件实现的，它们之间从不直接通信。它们使用 NTFS 文件控制标注机制相互传递消息。这保证了 NTFS 参与所有的文件操作。使用文件控制机制完成的操作包括，将 EFS 属性数据（DDF 和 DRF）作为文件属性写入，以及将 EFS 服务中计算的 FEK 传送到 FSRTL，使之可以在开放文件上下文中建立起来。此文件上下文又可用于磁盘文件读写操作的透明加密和解密。
- EFS 服务。EFS 服务是安全子系统的一部分。它使用本地安全授权（LSA）和内核模式安全参考监视器之间的现有 LPC 通信端口与 EFS 驱动程序进行通信。在用户模式下，它针对 CryptoAPI 提供文件加密密钥并生成 DDF 和 DRF。EFS 服务也支持 Win32 API 的加密、解密、恢复、导入和导出。
- Win32 API。它为加密明文文件、解密和恢复密文文件、导入和导出加密文件（没有先解密）提供了编程接口。Advapi32.dll（一个标准的系统 DLL）提供对这些 API 的支持。

7.3.3 EFS 的数据加解密过程

当一个用户使用 EFS 去加密文件时，必须已经存在一对公钥和私钥，如果用户暂时还没有的话，EFS 服务会自动为用户生成一对。所以对于一个初级用户来说，即使他完全不懂加密，也能加密文件。他可以对单个文件进行加密，也可以对一个文件夹进行加密，这样所有写入文件夹的文件将自动被加密。

在用户发布命令加密文件或试图添加一个文件到一个已加密的文件夹中，EFS 将执行以

下操作：

（1）文件被复制到临时文件。若复制过程中发生错误，则利用此文件进行恢复。

（2）文件被一个随机产生的 Key 加密，这个 Key 叫作文件加密密钥（FEK），FEK 的长度为 128 位（仅美国和加拿大），这个文件使用 DESX 加密算法进行加密。

（3）数据加密区域（DDF）产生，这个区域包含了使用 RSA 加密的 FEK 和用户的公钥。

（4）数据恢复区域（DRF）产生，这个区域的目的是为了在用户解密文件的中可能解密文件不可用（丢失 Key、离开公司等）。这些用户叫做恢复代理，恢复代理在加密数据恢复策略（EDRP）中定义，它是一个域的安全策略。如果一个域的 EDRP 没有设置，本地 EDRP 被使用。在任一种情况下，在一个加密发生时，EDRP 必须存在（因此至少有一个恢复代理被定义）。DRF 包含使用 RSA 加密的 FEK 和恢复代理的公钥。如果在 EDRP 列表中有多个恢复代理，FEK 必须用每个恢复代理的公钥进行加密，因此，必须为个恢复代理创建一个 DRF。

（5）包含加密数据、DDF 及所有 DRF 的加密文件被写入磁盘。

（6）在第（1）步中创建的临时文件被删除。

上述的整个数据加密过程如图 7-5 所示。

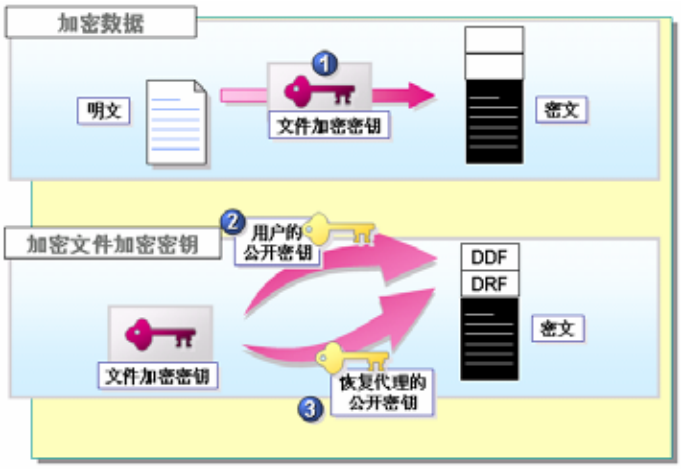

图 7-5　EFS 的数据加密过程

而下面的操作将在数据被解密时发生。

（1）使用 DDF 和用户的私钥解密 FEK（文件加密密钥）。

（2）使用 FEK 解密文件。

在恢复代理恢复文件的过程中，将产生同样的操作。只是在第（1）步中是 DRF 而不是 DDF。

图 7-6 说明了 EFS 的数据解密过程。

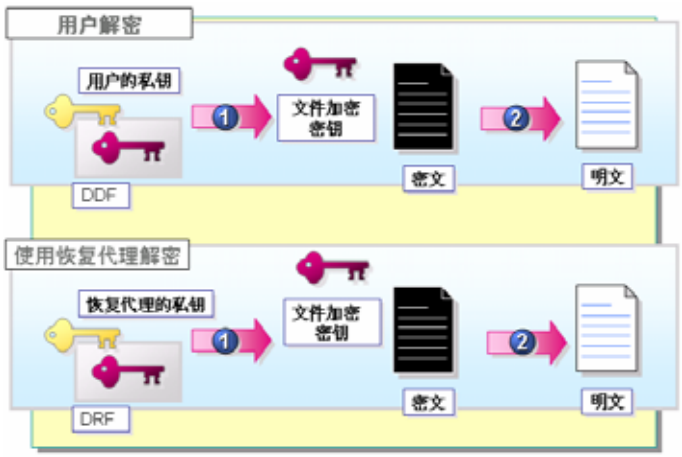

图 7-6　EFS 的数据解密过程

从上述的数据加解密过程中可以看出，EFS 结合了对称加密（DESX）和非对称加密（RSA）的优点，优于只对数据使用非对称加密（用这种方法仅 FEK 被加密），数据使用对称加密进行加密。此外，备份进程备份加密格式的文件，消除了备份操作需要访问数据的需要。

7.3.4　EFS 的故障恢复

使用文件加密系统带来的一个不便之处是 :如果一个用户采用加密方式存储了公司重要的资料后又离开了公司，那么将如何再读取这些资料；或者是由于不慎的操作，管理员把用户账号或是用户的安全密钥删除了；或者最常见的问题就是操作系统万一崩溃了，需要重新安装新的系统，这时候将无法再读取磁盘上的加密资料。

EFS 通过实施故障恢复策略要求来提供内置数据的故障恢复。为了能够恢复数据，EFS 在加密文件的时候生成了两份 FEK 的拷贝，并把它们都存储到本地机器的硬盘上，第一份采用用户提供的公钥加密，第二份采用恢复代理公钥加密，这些措施保证在必要时恢复代理可以访问 EFK 并对文件进行解密。

默认情况下，域的默认恢复项被存储在域的第一台域控制器上，域管理员是默认的恢复代理；本地系统的管理员是单机系统的恢复代理。此外还可以使用组策略来指定另外的恢复代理。管理员也可以导出用户的私有密钥证书，只需要把该用户的证书导入给新的用户，就可以提供新的 EFS 恢复代理。

1. 故障恢复策略

“故障恢复策略”是指计算机环境中的用户在恢复加密的数据时所遵从的策略。故障恢复策略是一种公钥策略类型。

安装 Windows 2000 Server 时，如果已设置第一个域控制器时，将自动对域执行故障恢复策略。域管理员被颁发自签名的证书，该证书将域管理员指派为故障恢复代理。

EFS 通过实施故障恢复策略要求来提供内置数据的故障恢复。要求故障恢复策略必须在用户可以加密文件之前就位。故障恢复策略提供指派为故障恢复代理的人员。当管理员第一次登录到系统时，故障恢复策略将自动就位，让管理员成为故障恢复代理。

2. 配置恢复策略

默认故障恢复策略是为单独的计算机在本地配置的。对于网络中的计算机，可以在域、组织单元或单独计算机级别上配置故障恢复策略，并在所定义的影响范围内将其应用到所有基于 Windows 2000 的计算机。故障恢复证书由证书颁发机构（CA）颁发，并用 Microsoft 管理控制台（MMC）中的证书来管理。

在网络上，故障恢复策略由域管理员或故障恢复代理设置，它控制策略影响范围内所有计算机的控制恢复项。

由于安全子系统处理故障恢复策略的实施、复制和缓存，因此用户可以在暂时脱机的系统上（如便携机）执行文件加密（此进程类似于使用缓存的凭据登录到域账户）。

3. 故障恢复策略的类型

管理员可以定义三种策略中的一种：非故障恢复策略、空故障恢复策略，或者带一个或多个故障恢复代理的故障恢复策略。

- 故障恢复代理策略。当管理员添加一个或多个故障恢复代理时，故障恢复代理策略生效。这些代理负责在其管理范围内恢复任何加密的数据。这是最常用的故障恢复策略类型。
- 空故障恢复策略。当管理员删除所有的故障恢复代理及其公钥证书时，空故障恢复策略生效。空故障恢复策略意味着没有故障恢复代理，而且用户无法在故障恢复策略影响范围内的计算机上加密数据。空故障恢复策略的结果是完全关闭 EFS。
- 非故障恢复策略。当管理员删除组故障恢复策略时，非故障恢复策略生效。由于没有组故障恢复策略，因此单个计算机上的默认本地策略被用于恢复数据。这意味着本地管理员控制其计算机上的数据恢复。

4. 更改故障恢复策略

要更改域的默认故障恢复策略，必须以管理员身份登录第一个域控制器。然后，必须通过“ Active Directory 用户和计算机 ”管理单元激活“ 组策略 ”，并选择“ 安全设置 ”、“ 公钥策略 ”和“ 加密数据的故障恢复代理 ”。

5. 故障恢复代理

故障恢复代理就是获得授权解密由其他用户加密的数据的管理员。例如，当雇员离开公司而其剩余数据需要解密时故障恢复代理非常有用。在添加域的故障恢复代理之前，必须确保每个故障恢复代理都已经颁发 X509 第三版的证书。

故障恢复代理拥有特殊证书和相关私钥，允许在故障恢复策略的影响范围内恢复数据。故障恢复代理有足够的理由需要在 Microsoft 管理控制台（MMC）的证书中使用“ 导出 ”命令，将故障恢复证书和相关私钥备份到安全位置。备份完成后，应该使用 MMC 中的证书删除故障恢复证书。然后，在需要为用户执行故障恢复操作时，应该首先从 MMC 的证书中使用“ 导入 ”命令还原故障恢复证书和相关私钥。恢复数据之后，应该再次删除故障恢复证书。不必重复导出过程。

要对域添加故障恢复代理，请将它们的证书添加到现有的故障恢复策略中。可以通过“ Active Directory 用户和计算机 ”管理单元激活“ 添加故障恢复代理 ”向导来完成。

7.3.5 加密文件系统的优势

Windows 2000 操作系统中的加密文件系统（EFS）具有如下一些优势。

- EFS 是基于公钥的加密技术，它使用了 Windows 的 CryptoAPI 结构。每个文件都是使用随机产生的密钥加密的，这种密钥独立于用户的公钥/私钥对，从而扼制了多种基于密码分析的攻击。文件加密可以使用任何对称加密算法。第一版的 EFS 将 DES 作为加密算法。而此后的发行版本则允许使用其他的加密算法。
- EFS 与 NTFS 文件系统紧密地集成在一起。因此一个恶意的用户不可能绕过文件系统而访问到硬盘。而且，所有运行在内核模式的 EFS 驱动程序不能由用户直接访

问。此外，当创建临时文件时，只要所有的文件在 NTFS 卷上，原始文件的属性就会被复制到临时文件中。如果加密了一个文件，EFS 也会将其临时文件进行加密。EFS 驻留在操作系统内核中，并且使用不分页的池存储文件加密密钥，保证了密钥不会出现在分页文件中。

- EFS 的默认配置允许用户无须进行管理上的设置即可开始对文件进行加密。EFS 会自动的为用户文件加密生成一个公钥对（如果以前还没有的话）。
- EFS 既支持对单个文件的加密和解密，也支持对完整目录的加密和解密。目录的加密是强制为透明的。在标为加密的目录中创建的所有文件（和子目录）将自动被加密。每个文件具有惟一的加密密钥，这样文件重命名很安全。如果将加密目录中的一个文件重命名到同一卷上的未加密目录上，该文件仍是加密的。加密和解密服务可从 Windows 资源浏览器中获得，此外对高级用户和恢复代理还提供了命令行工具和管理界面。
- 加密文件使用前不需要解密。当向磁盘存储和从磁盘读取字节时，加密和解密透明地完成。EFS 自动检测加密文件，并从系统密钥存储区定位用户密钥。
- EFS 还提供内置的数据恢复支持。只有当系统配置了一个或多个恢复密钥时，才可以使用文件加密。数据恢复是出于对大多数业务环境的考虑，例如员工离开公司后或加密密钥丢失时公司要恢复员工加密过的文件。恢复策略可以在 Windows 域的域控制器中定义，该域中的所有计算机都将被强制执行此策略。恢复策略处在域管理员控制之下，域管理员使用 Windows 活动目录服务的委派功能，可以将此策略委派给受托的数据安全管理员账户。这提供了更好、更灵活的方法控制被授权恢复加密数据者。通过允许多恢复密钥配置，EFS 还支持多恢复代理，为单位实现恢复过程提供了冗余和灵活性。 EFS 允许恢复代理配置用于启用文件恢复的公钥。但使用恢复密钥时，仅仅文件随机产生的密钥可用，用户的私钥不可用。这也就保证了其他私人信息不会无意中泄露给恢复代理。
- Windows 2000 的 CryptoAPI 体系允许用户在智能卡上存取他们的私钥，这比将加密钥匙放在硬盘或软盘上更为安全，这也使多个位置访问成为可能。
- EFS 也支持对存储在远程文件服务器上的文件进行加密和解密。但在这种情况下，EFS 只对磁盘上的数据加密，而不加密在网络上传输的数据（Windows 提供了诸如 SSL/PCT 的网络协议来对网络上的数据访问进行加密）。
- EFS 也可用于家庭环境。在没有 Windows 域的情况下，EFS 自动生成恢复密钥，并将其存为计算机密钥。通过使用管理员账户，家庭用户也可以使用命令行工具来恢复数据，减少了家庭用户的管理开销。

7.3.6 加密文件系统的局限性

加密文件系统的一般局限性体现在以下几点。

- 安全性的增加伴随着花费的增加，任何加密进程都将会增加处理量和降低某些方面的性能。
- 仅对存储在磁盘上的文件进行加密，而不包括网络传输上的加密。所以必须应用其他的加密技术手段，如 IPSec 协议，来进行安全的网络传输。
- 自动病毒监测程序，如 Norton Antivirus 不能扫描被加密过的文件（除非能访问到用户的私钥）。
- 如果一个文件或硬盘被偷，恶意的用户将有大量的时间，如果有能力破译加密数据的话，数据可能会被解密。

而 Windows 2000 的加密文件系统也有以下一些独有的局限性。

- EFS 仅工作在 NTFS 卷，目前 EFS 在 FAT 卷上不支持。
- EFS 目前使用 DESX 作为它的加密算法，有必要采取更强壮的加密算法。
- 如果系统文件被加密，系统将不可用，EFS 仅对数据文件加密。OS 操作需要引导的文件不能被加密，否则在开始的时候将不能访问。为保护这些，加密被限制在文件属性的设置上，然而，在 2000 年 7 月 25 日，SecuriTeam 报告了一个有关 EFS 的 DoS，如果批处理文件（没有系统属性）被加密后，系统将不能被引导。
- 定义太多的恢复代理将影响性能，对每一个恢复代理，FEK 发布被加密的同时，一个 DRF 被创建。这将引起两个问题：一是为存储多个 DRF 需要大量的磁盘空间；二是创建多个 DRF 将花费更多的时间和处理器资源。
- Windows 2000 中的加密文件系统不支持文件共享，仅仅创建 DDF 用户的钥匙能访问到文件。
- EFS 将增加系统管理员的管理，而且管理加密钥匙的区域是非常重要的。
- 在加密进程的第一步中创建的文本备份文件在进程中以未加密的格式存在，恶意用户可能在文件存在时访问到这个文件。

7.3.7 加密文件系统的使用

1. 文件和文件夹的加密

Windows 2000 操作系统的用户可以使用加密工具 cipher.exe 或是 Windows 2000 资源管理器来进行文件和文件夹的加密。作为一个拥有者，用户可以非常容易的加密自己的文件。如果加密文件夹的话，其他用户虽然可以看到文件名称，可是仍然不能打开文件。

需要注意的是，压缩文件和系统文件不能够采用 EFS 加密，这样会造成系统启动或是其他的问题。同样地，加密文件系统不能加密在根目录中的文件。

（1）在 Windows 2000 资源管理器中选择待设置加密属性的文件或文件夹。

（2）单击鼠标右键，选择“ 属性 ”命令，启动文件属性设置对话框，如图 7-7 所示。

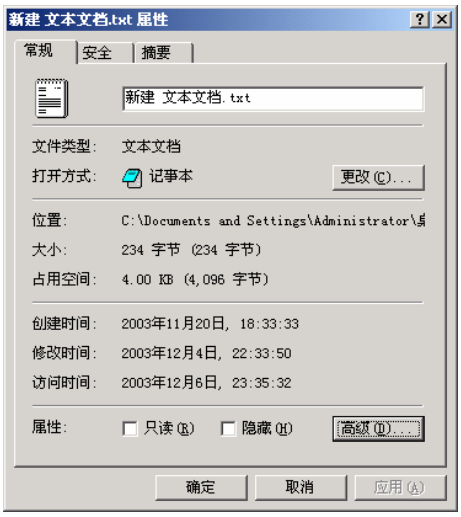

图 7-7 文件的属性及高级属性

（3）单击“ 常规 ”选项卡中的“ 高级 ”按钮，启动“ 高级属性 ”对话框，如图 7-8 所示。

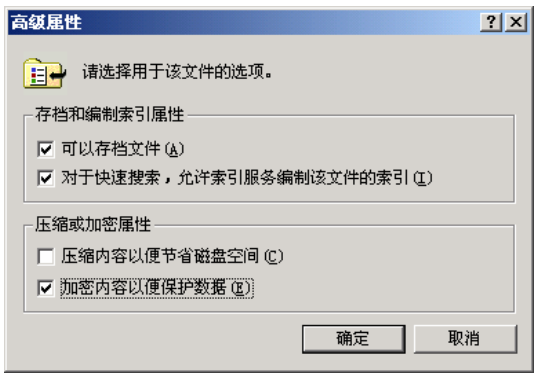

图 7-8 文件和文件夹的加密

（4）选择“压缩或加密属性”栏中的“加密内容以便保护数据”复选框，单击“确定”按钮，即可完成文件或文件夹的加密。

2. 访问加密文件

访问和打开加密文件对于用户来说是透明的，用户不需要使用其他的操作来打开加密文件，甚至不需要输入密码。此外，备份管理员也可以自由地备份所有的加密文件，同时保留加密文件的设置。即使备份管理员，同样也没有查看文件内容的权限。

3. 复制加密文件

加密文件与普通文件相同，也可以进行复制、移动以及重命名等操作，但是其操作方式可能会影响加密文件的加密状态。一般来说，复制文件的话，复制过去的文件属性将根据其目的文件夹的属性变化。

（1） 在 Windows 2000 资源管理器中选中待复制的加密文件。

（2） 用鼠标右击加密文件，选择“复制”命令。

（3） 切换到加密文件复制的目标位置，单击鼠标右键，选择“粘贴”命令，即可完成。

此外，复制命令也同时加上了不同的参数，包括：/E 和/I。如果不使用这两个参数，Windows 2000 将事先解密文件，然后复制解密后的文件到磁盘上。表 7-3 说明了复制之后的新文件在不同情况下的加密属性。

表 7-3 复制文件的加密属性

开始加密	复制到	新文件
目录和文件都加密	目录未加密	加密
目录和文件都加密	目录加密	加密
目录加密文件未加密	目录加密	加密
目录加密文件未加密	目录未加密	未加密
目录和文件都未加密	目录加密	加密
目录和文件都未加密	目录未加密	未加密

4. 移动和更名加密文件

如果更名加密文件，系统对文件内容没有做任何修改，只是修改了文件的文件名称，所以不会对加密的内容作出变化。

- 在同一磁盘里移动加密文件的话，只改变文件分配表，所以文件属性不变。
- 在不同磁盘间移动文件的话，其实是把旧文件删除，在另外的磁盘里复制新的文件，所以新的文件属性将根据其目的文件夹的属性变化。

相关的操作步骤如下：

（1）在 Windows 2000 资源管理器中选中待复制的加密文件。

（2）用鼠标右键单击加密文件，选择“ 剪切 ”命令。

（3）切换到加密文件待移动的目标位置，单击鼠标右键，选择“ 粘贴 ”命令，即可完成。

需要注意的是：对加密文件进行复制或移动时，加密文件有可能被解密。尤其要注意的是：加密文件复制或移动到 FAT 文件系统中时，文件自动解密，所以建议对加密文件进行复制或移动后应重新进行加密。

5. 文件解密

文件解密的操作步骤如下。

（1）利用 Windows 2000 资源管理器中选中待设置加密属性的文件或文件夹。

（2）单击鼠标右键，选择“ 属性 ”命令，启动文件/文件夹属性对话框。

（3）单击“ 常规 ”选项卡中的“ 高级 ”按钮，启动“ 高级属性 ”对话框。

（4）清除“ 高级属性 ”对话框中“ 压缩或加密属性 ”栏中的“ 加密内容以便保护数据 ”复选框。

6. 文件夹加密

Windows 2000 的 EFS 允许设置在文件夹和文件的级别，当一个文件夹被设置在加密的时候，所有添加到其中的文件和文件夹将自动的被设置为加密。所以用户最好为自己创建一个加密的文件夹，以便存储自己所有的重要文件。文件夹本身不能加密，被加密的只是其中的文件。

加密文件夹的时候，系统会提示你是否加密该文件夹中的子文件夹和文件，如图 7-9 所示。

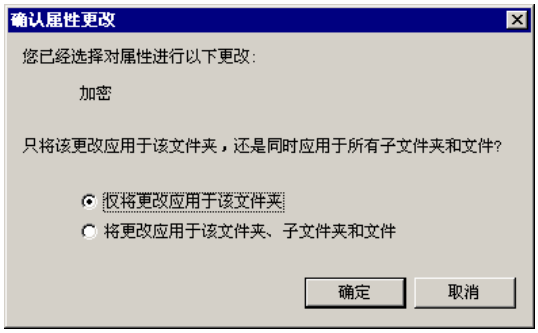

图 7-9　加密文件夹

如果选择第一项“ 仅将更改应用于该文件夹 ”的话，加密结果如表 7-4 所示。

表 7-4 选择“ 仅将更改应用于该文件夹 ”的加密结果

文件描述	加密状态
该文件夹或文件夹中的已有文件	不改变。不管它们原来状态如何，它们保留已加密或未加密状态
用户后来在文件夹中创建或拷贝入文件夹之中的文件	用用户的私有密钥加以保护
其他用户后来在文件夹中创建或拷贝入文件夹（共享文件夹）之中的文件	用其他用户的私有密钥加以保护
后来在子文件夹中创建或拷贝入子文件夹的文件	不改变
后来移动到文件夹或子文件夹的文件	不改变

而选择第二项“ 将更改应用于该文件夹、子文件夹和文件 ”的加密结果如表 7-5 所示。

表 7-5　选择“ 将更改应用于该文件夹、子文件夹和文件 ”的加密结果

文件描述	加密状态

文件夹和文件夹的子文件夹中的已有文件	如果用户有 Write Attributes 权限，用用户私有密钥保护，否则文件没有改变
用户后来在文件夹或子文件夹中创建或拷贝入文件夹或子文件夹的文件	用用户私有密钥保护
其他用户后来在文件夹或子文件夹中创建或拷贝入文件夹或子文件夹的文件	用其他用户的私有密钥保护
后来移入文件夹或子文件夹的文件	没有改变

无论选择哪一种，文件夹的文件列表仍然是明文，只要用户能访问文件夹，就能和平常一样列举文件。如果文件夹中的文件较多的话，那么加密这些文件可能需要较多的时间，如图 7-10 所示。

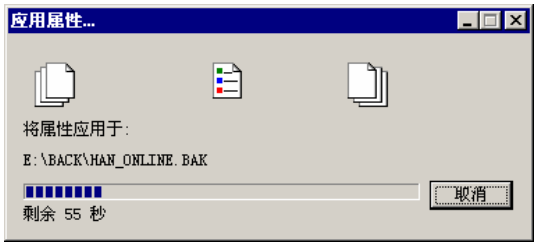

图 7-10　加密包含大量文件的文件夹

7. Cipher 工具

除了图形界面外还提供命令行工具 Cipher.exe 以丰富管理操作的功能。可以使用 Cipher.exe 来查看 EFS 的状态，也可以使用它来进行文件的加密和解密。

完整的 Cipher.exe 命令支持以下选项：

Cipher [/e | /d] [/s:dir] [/a] [/i] [/f] [/q] [/h] [/k] [pathname [...]]

用户可以使用 Cipher /?来查看详细的选项说明。常用的使用选项及其含义如表 7-6 所示：

选项	含义
/e	加密指定的目录。目录将被标记，所以之后加进目录中的文件将被加密
/d	解密指定的目录。目录将被标记，所以之后加进目录中的文件将不被加密
/s	在给定的目录和其所有子目录执行指定的操作
/i	即使发生错误仍然继续指定的操作。默认发生错误时 Cipher 停止
/f	强制对所有指定的对象加密，即使它们已经被加密。 默认为跳过已经加密的对象
/q	只报告最基本的信息
/k	为运行 Cipher 的用户创建新的文件密钥。如果选择了此选项，则忽略所有其他选项

表 7-6 Cipher 工具的常用选项说明

例如：

- 查看某个目录中文件的加密情况

C:\ >Cipher DirName

- 查看某个目录中某个文件的加密情况

C:\ >Cipher DirName\FileName

- 加密“ C:\Documents and Settings ”目录

C:\>Cipher /e "Documents and Settings"

- 加密所有带有“ info ”的文件

C:\ >Cipher /e /s *info*

8. 将默认的恢复代理备份到软盘

（1）单击“开始”→“运行”命令，输入 mmc /a，然后单击“确定”按钮。

（2）在“控制台”菜单上，选择“添加/删除管理单元”命令，然后在打开的对话框中单击“添加”按钮，打开“添加独立管理单元”对话框，如图 7-11 所示。

图 7-11 “证书”管理单元

（3）在“添加独立管理单元”对话框下，单击“证书”，然后单击“添加”按钮，打开“证书管理单元”对话框，如图 7-12 所示。

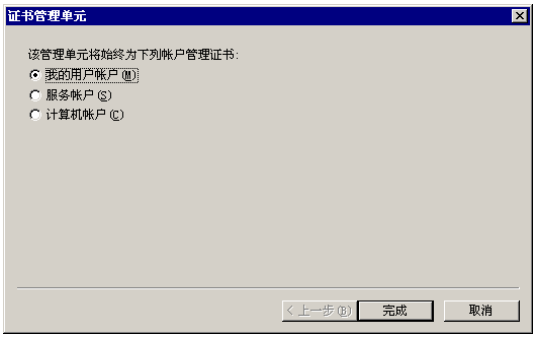

图 7-12 管理“我的用户账户”证书

（4）单击“我的用户账户”单选按钮，然后单击“完成”按钮。

（5）单击“关闭”按钮，然后单击“确定”按钮。

（6）双击“证书-当前用户”（管理员），双击“个人”，然后单击“证书”，如图 7-13 所示。

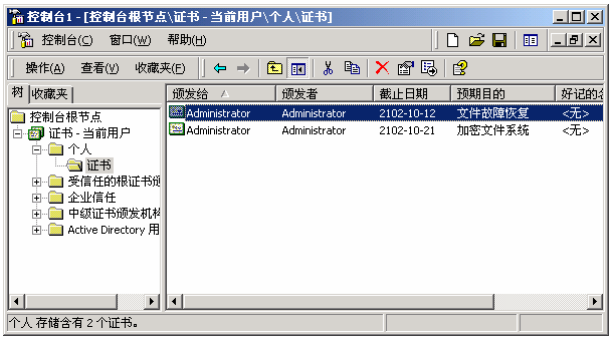

图 7-13 “文件故障恢复”证书

（7）单击在“预期目的”栏中显示“文件恢复”字样的证书。

（8）右键单击该证书，指向“所有任务”，然后选择“导出”命令。

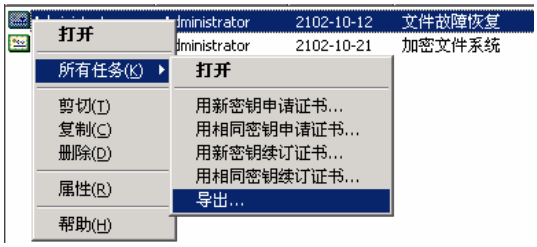

图 7-14　证书的导出

（9）按照“证书管理器导出”向导的指示导出证书，并将私钥与.pfx 文件格式相关联。当向导要求输入文件名时，单击“浏览”按钮，打开软盘上要保存该文件的文件夹。确保将软盘保存在安全的位置。

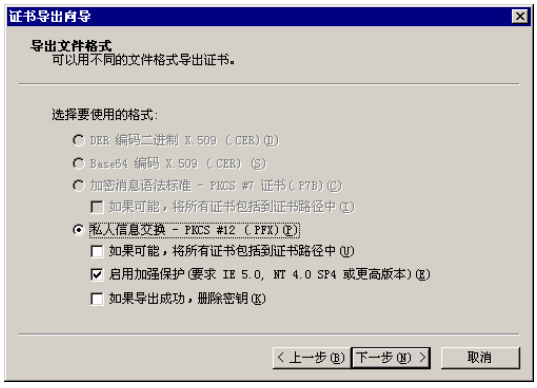

图 7-15　证书导出的格式

要完成该过程，必须登录为管理员或管理员组成员。如果计算机连接在网络上，则网络规则设置也可能会禁止完成该过程。

9. 恢复加密的文件或文件夹

如果文件加密证书丢失，正常的用户将无法访问加密文件。然而，恢复代理能够将该文件解密。

使用 Windows 2000 中的“备份”功能或任何为 Windows 2000 设计的备份程序制作加密文件或文件夹的备份版本。为 Windows 2000 设计的备份程序保留了所备份文件的加密。用户可以将加密文件或文件夹的备份版本作为电子邮件附件发送给恢复代理。恢复代理拥有为用户解密文件或文件夹的特殊证书。恢复代理将备份解密文件或文件夹，然后将备份版本返回给用户。

如果在软盘上以.pfx 文件格式保存了文件加密证书和私钥的备份副本，则可以自己恢复加密的文件或文件夹。使用 Micorosoft 管理控制台（MMC）中的“导入”命令将软盘中的.pfx 文件导入到“个人”存储区。

7.4　磁盘配额

7.4.1　磁盘配额基础

对于文件服务器和 Web 服务器来说，如果不设置磁盘资源消耗的界限，那么就为粗心或有企图的用户提供了攻击的方便之门，可能导致服务器无法为客户提供正常的服务。

在 Windows 2000 中的磁盘配额特性允许监视和限制磁盘空间的使用。磁盘配额是以每个用户每个卷为基础来进行跟踪的，用户只能对它们所拥有的文件进行配额管理。系统为不

同的卷独立地跟踪配额，即使这些卷是同一个物理驱动器上的不同的卷。但是，如果用户在相同卷上有些份额，那么指定给该卷的配额适用于所有这些份额，用户对两种份额的使用不能超过该卷上指定的配额。

系统管理员可以将 Windows 配置为：

- 当用户超过所指定的磁盘空间配额时，阻止进一步使用磁盘空间，并记录事件。
- 当用户超过指定的磁盘空间警告级别时，记录事件。

当启用磁盘配额时，可以设置两个值：磁盘配额限制和磁盘配额警告级别。

磁盘配额限制指定了允许一个用户所使用的磁盘空间量。磁盘配额警告级别指明了用户在什么时候临近了磁盘配额限制。例如，可以把用户的磁盘配额限度设为 50MB，并把磁盘配额警告级别设为 45MB。这种情况下，用户可在卷上存储不超过 50MB 的文件。如果用户在卷上存储的文件超过 45MB，则把磁盘配额系统记录为系统事件。可以指定用户能超过其配额限度。如果不想拒绝用户访问卷但想跟踪每个用户的磁盘空间使用情况，启用配额但不限制磁盘空间使用将非常有用。也可指定不管用户超过配额警告级别还是超过配额限度时是否要记录事件。

启用卷的磁盘配额时，系统从那个值起自动跟踪新用户卷使用。但是，磁盘配额不应用到现有的卷用户上。可以通过在“ 配额项目 ”对话框中添加新的配额项目将磁盘空间配额应用到现有的卷用户上。可以在本地卷和网络卷上启用配额，但是只能在从卷的根目录共享以及用 NTFS 文件系统格式化的卷上启用配额。

综上所述，我们可以看出磁盘配额提供了一种基于用户和分区的文件存储管理，使得管理员可以方便地利用这个工具合理地分配存储资源，避免由于磁盘空间使用的失控可能造成的系统崩溃，从而提高了系统的安全性。

7.4.2 深入了解磁盘配额

1. 磁盘配额和用户

由于磁盘配额监视单个用户的卷使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷上的其他用户的磁盘配额。例如，如果用户把 50MB 的文件保存到 F 卷上，则那个用户必须从该卷删除或移动一些过时文件，才能把其他数据写到这个卷上。但是，其他用户在那个卷上可继续存储直到 50 MB 空间的文件。

磁盘配额是以文件所有权为基础的，并且不受卷中用户文件的文件夹位置的限制。例如，如果用户把文件从一个文件夹移到相同卷上的其他文件夹，则卷空间用量不变。但是，如果用户将文件复制到相同卷上的不同文件夹中，则卷空间用量加倍。

2. 物理磁盘和目录对磁盘配额的影响

磁盘配额只适用于卷，且不受卷的文件夹结构及物理磁盘上的布局的限制。

如果卷有多个文件夹，则分配给该卷的配额将应用于所有文件夹。例如，如果 \\Production\QA 和\\Production\Public 是 F 卷上的共享文件夹，则用户对这两个文件夹的使用不能超过已指派的 F 卷配额。

如果单个物理磁盘包含多个卷，并把配额应用到每个卷，则每个卷配额只适于特定的卷。例如，如果用户共享两个不同的卷，分别是 F 卷和 G 卷，那么即使这两个卷在相同的物理磁盘上，也将分别对这两个卷的配额进行跟踪。

如果一个卷跨越多个物理磁盘，则整个跨区卷使用该卷的同一配额。例如，如果 F 卷有 50 MB 的配额限度，那么不管 F 卷是在物理磁盘上还是跨越三个磁盘，都不能把超过 50 MB 的文件保存到 F 卷。

3. 磁盘配额的状态

管理员可以打开配额执行，也可以关闭配额执行。总共有三种配额状态，如表 7-7 所示。

表 7-7 磁盘配额的状态

状态	描述
配额禁用	不对配额使用情况变化进行跟踪。但仍保留该配额限制。在这种状态下，磁盘配额不会影响性能。该状态为默认状态
配额跟踪	对配额使用情况变化进行跟踪。但不实施配额限制。在这种状态下，不会产生任何配额违规事件，而且由于磁盘配额违规，因此，任何文件操作都不会失败
配额执行	对配额使用情况变化进行跟踪，并且实施配额限制

4. 磁盘配额详细信息的更新

在 NTFS 文件系统中，卷使用信息按用户安全标识（SID）存储，而不是按用户账户名称存储。第一次打开“ 配额项目 ”窗口时，磁盘配额必须从网络域控制器或者本地用户管理器上获得用户账户名称，将这些用户账户名与当前卷用户的 SID 相匹配，并组装带有用户名的“ 名称 ”列上的项目。从域控制器或本地用户管理器中获得这些名称时，名称将显示在该区域中。第一次查看配额项目时，这个过程立即开始。

获得这些名称之后，名称将保存在卷上的文件中，以便下次打开“ 配额项目 ”窗口时可立即使用。但是，因为此文件可能持续几天使用而没有被 Windows 更新，所以“ 配额项目 ”窗口可能不反映查看配额项目后对域用户账户列表所做的更改。

5. 磁盘配额和转换的 NTFS 卷

因为磁盘配额都是以文件所有权为基础的，所以对影响文件所有权状态的卷所做的任何更改，包括文件系统转换，都可能影响该卷的磁盘配额。因此，在现有的卷从一个文件系统卷转换到另一文件系统之前，用户应该了解这种转换可能引起的所有权变化。

因为使用存储在 NTFS 文件系统字段的数据来识别文件所有者，所以磁盘配额可以在用于 Windows 2000 的 NTFS 版本和用于 Windows NT 4.0 及更早版本的 NTFS 中工作。但是，由于 FAT 和 FAT32 卷上的文件归该系统所有，因此从 FAT 或 FAT32 转换到 NTFS 的卷上的文件不是根据拥有文件的用户来计算的。在这种情况下，这些文件由管理员账户负责。因为管理员拥有无限的卷使用权限，因此这几乎不是问题。

6. 本地和远程实现

管理员可在本地计算机和远程计算机的卷上启用磁盘配额。在本地计算机上，可以使用配额限制登录本地计算机的不同用户可使用的卷空间容量。在远程计算机上，可以使用配额限制远程用户的卷使用情况。管理员可使用磁盘配额确保：

- 登录到相同计算机的多个用户不干涉其他用户的工作能力。
- 公用服务器上的磁盘空间不由一个或多个用户独占。
- 在个人计算机的共享文件夹中，用户不使用过多的磁盘空间。

要启用远程计算机卷上的配额，这些卷必须是通过在 Windows 2000 中使用的 NTFS 版本格式化的，并且是从卷的根目录共享的。同样，用户必须是远程计算机卷上的 Administrators 组的成员才能启用和管理。

由于系统文件都被包含在将 Windows 2000 安装到本地计算机上的用户的卷空间中。当在一个本地卷上执行磁盘限额时，一定要考虑这些文件所占用的磁盘空间。依据该卷上可用的空闲空间，管理员应该为安装该操作系统的用户设定一个高的限额界限或者不设定界限。

7.4.3 磁盘配额的管理

1. 启用磁盘配额

若要启用磁盘配额，可按照如下操作步骤进行：

（1）打开“ 我的电脑 ”。

（2）右击要启用磁盘配额的磁盘卷，然后单击“ 属性 ”按钮。

（3）在“ 属性 ”对话框中，打开“ 配额 ”选项卡。

（4）选中“ 启用配额管理 ”复选框。

（5）设置配额限制，然后单击“ 确定 ”按钮，如图 7-16 所示：

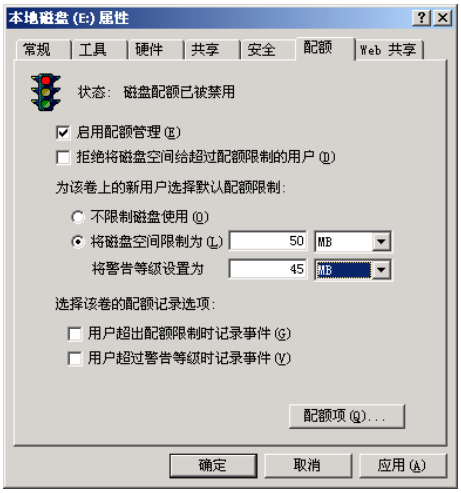

图 7-16 启用“ 磁盘配额 ”

通过该选项卡，管理员还可以执行以下任务：

- 禁用磁盘配额
- 拒绝超过限制的用户使用磁盘空间
- 指派默认配额值
- 查看磁盘配额设置

2. 添加新的配额项目

添加新的磁盘配额项目可按照如下操作步骤进行：

（1）打开“ 我的电脑 ”。

（2）右击要添加新磁盘配额项目的卷，然后单击“ 属性 ”按钮。

（3）在“ 属性 ”对话框中，打开“ 配额 ”选项卡。

（4）单击“ 配额项 ”按钮。

（5）在“ 配额项目 ”窗口中，选择“ 配额 ”菜单中的“ 新建配额项 ”命令，如图 7-16 所示。

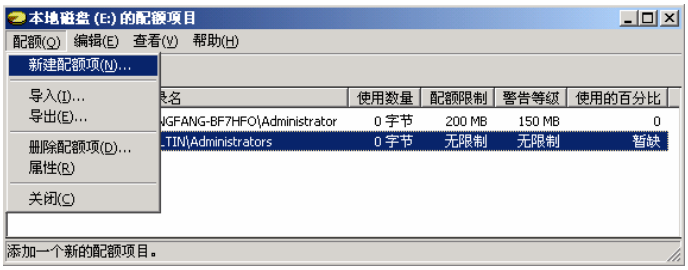

图 7-17　添加新的磁盘配额项目

（6）在“选择用户”对话框的“搜索范围”列表框中，选择要从中选择用户名的域或工作组的名称。单击“添加”按钮，然后单击“确定”按钮。

（7）在“添加新配额项”对话框（如图 7-18 所示）中，指定下列选项之一。

- 不限制磁盘的使用：不限制磁盘空间而跟踪磁盘空间的使用。
- 将磁盘空间限制为：设置激活限制磁盘空间以及设置警告级别的字段。输入的值不能超过卷的最大容量。

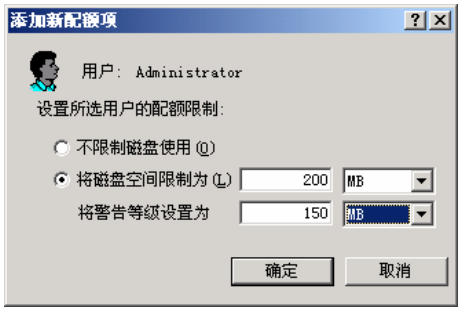

图 7-18　设置新的配额项目

（8）单击“确定”按钮。

在“配额项目”窗口中，管理员还可以实现以下任务：

- 查看卷用户的磁盘配额信息
- 删除配额项目
- 修改用户磁盘空间限制和警告级别
- 在“配额项目”窗口中查找配额项目
- 排序配额项目
- 更改“配额项目”窗口中的列顺序
- 创建配额报告
- 从其他卷导入配额设置
- 将配额设置导出到其他卷上

7.5　网络共享的安全

7.5.1　文件夹共享

Windows 2000 系统允许文件在网络中共享，即能够让网络中的其他主机访问到本机的文件。除了可以明确共享文件夹之外，Windows 2000 还创建默认共享，这些默认共享被称为管理共享（也称为特殊共享）。这些共享文件夹通常在共享名后加一个$来区别（如 C$、D$、ADMIN$等）。只有 Administrators 组的成员才能访问这些共享。下面是典型的管理共享列表。

- Drive$：Windows 2000 为系统上的每一个驱动器都创建了这个默认共享，如 C$、D$、E$等等。
- ADMIN$：在远程管理任务时使用，指向%SYSTEMROOT%文件夹。
- IPC$：系统使用它来共享命名管道。
- NETLOGON：该共享只能由 Windows 2000 服务器使用。它指向%SYSTEMROOT%\SYSVOL\SYSVOL\domain\SCRIPTS 文件夹。
- SYSVOL：该共享由 Windows 2000 域控制器用来在域控制器之间存储域公共文件

的副本，它指向%SYSTEMROOT%\SYSVOL\SYSVOL 文件夹。

虽然，文件夹共享提供了在一个网络上的所有用户之间共享某个特定文件（或多个文件）的好方法，但从安全性的角度来看，文件夹共享对安全性造成了新的威胁。一方面，如果配置不当，就可能会对系统文件造成威胁。另一方面，许多计算机管理员使用这些服务来使他们的文件系统具有可读性和可写性，以此来提高数据访问的便捷性。但是不用多久，其他人就会发现这些开放的文件共享，并窃取其中的文件。

1. 共享协议基础

SMB（Server Message Block）协议是 Windows 系统中用来进行文件共享的协议。在 Windows NT 系统中，SMB 运行于 NBT（NetBIOS over TCP/IP）上，使用 UDP 137、UDP139 和 TCP 139 端口。而在 Windows 2000 系统中，SMB 可以直接运行在 TCP/IP 上，而没有额外的 NBT 层，使用 TCP 445 端口。Windows 2000 的管理员可以在“网络连接/属性/TCPIP 协议/属性/高级/WINS”中设置“启用或者禁用 NBT”。

那么当 Windows 2000 使用网络共享的时候，那么是如何选择 139 还是 445 端口呢。下面的过程将确定会话所使用的端口：

（1）如果客户端启用了 NBT，那么连接的时候将同时访问 139 和 445 端口。如果从 445 端口得到回应，那么客户端将发送 RST 到 139 端口，终止这个端口的连接，接着就从 445 端口进行 SMB 的会话了；如果没有从 445 端口而是从 139 得到回应，那么就从 139 端口进行会话；如果没有得到任何回应，那么 SMB 会话失败。

（2）如果客户端禁用了 NBT，它就将只从 445 端口进行连接。当然，如果服务器（开共享端）没有 445 端口进行 SMB 会话的话，那么就会访问失败。所以禁用 445 端口后，对访问 NT 机器的共享会失败。

所以对于 Windows 2000 来说，文件的网络共享问题就不仅仅是 139 端口了，445 端口同样能够完成。

2. Windows 的“空会话”漏洞

所谓的空会话就是能够同服务器建立的无信任支持的会话。一般的一个会话会包含用户的认证信息，而空会话则没有用户的认证信息，也就好比是个匿名用户一样。没有认证就不可能为系统建立安全通道，而建立安全通道也是双重的：第一，就是建立身份标志，第二就是建立一个临时会话密匙，这样双方才能用这个会话进行加密数据交换（比如 RPC 和 COM 的认证等级是 PKT_PRIVACY）。不管是经过 NTLM 还是经过 Kerberos 认证的票据，终究是为会话创建一个包含用户信息的令牌。

根据 Windows 2000 系统的访问控制模型，对于空会话同样需要提供一个令牌。但是空会话由于是没有经过认证的会话，所以令牌中不包含用户信息，因此，建立会话双方没有密钥的交换，这也不能让系统间发送加密信息。这并不表示空会话的令牌中不包含 SID，对于一个空会话，LSA 提供的令牌的 SID 是 S-1-5-7，这就是空会话建立的 SID，用户名是 Anonymous Logon。这个用户名可以在用户列表中看到，但是不能在 SAM 数据库中找到，属于系统内置的账号。

能够以“空会话”连接一个系统，首先需要对方开放相应的服务，也就是需要打开 TCP 139 和 TCP 445 端口。其次，服务器还必须得打开 IPC$共享。这两项都是 Windows NT 和 2000 系统所默认的。如果没有 IPC 共享，即使共享一个文件，有权限为 Anonymous Logon，也不能建立会话，即使权限设置为完全控制，出现的连接错误依然是权限不够。这和其他账号是不一样的。如果要允许一个文件夹共享能够类似 IPC$（命名管道而非共享）而能够使用空会话，那么需要修改注册表键：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\中的 NullSessionShares 子键，添加新的共享名，这样才能建立一个共享的空会话。这时将不依赖 IPC$的存在了。

只要能够通过这个“ 空会话 ”连接成功，那么就能够通过这个系统的默认漏洞来列举对方系统的一些敏感系统信息，如用户和组信息（包括用户名、最后登录日期、密码策略、RAS 信息等）、系统信息和特定注册信息等。

3. 文件共享的安全

在准备将文件和文件夹在网络上共享的时候，必须考虑以下一些安全措施。

- 对加载的驱动器进行共享时，确保只共享了需要共享的目录。
- 为了增强安全系数，只允许指定的 IP 地址能够访问共享资源（一般不要支持域名访问功能，因为域名可能被伪造）。
- 确保所有的共享资源都有高强度的密码保护。
- 禁止通过“ 空会话 ”连接以匿名的方式列举用户、群组、系统配置和注册表键值。在网络层面上，可以在路由器上进行规则设置，屏蔽向路由器或主机上的 NetBIOS 会话服务端口）发出的越界连接请求。而在单机或无信任域的环境中对与 Internet 连接的主机执行限制匿名访问等。具体操作步骤是：在本地安全设置的本地安全策略中，选择“ 对匿名连接的额外限制 ”项，对其进行设置，将值设为“ 没有显式匿名权限就无法访问 ”项，如图 7-19 所示。

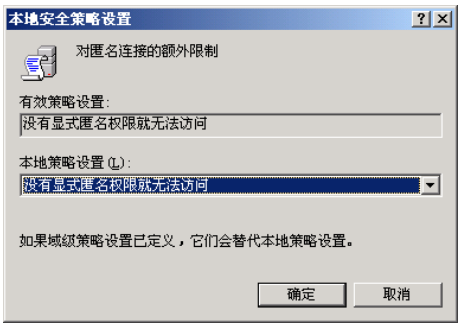

图 7-19　通过本地安全策略对匿名连接的额外限制进行设置

这也可以通过修改注册表来实现，方法是：打开注册表子键 HKLM\SYSTEM\CurrentControlSet\Control\Lsa，将名称为 RestrictAnonymous（类型为 REG_DWORD）的值设为 2，即对应“ 没有显式匿名权限就无法访问 ”，这样匿名用户将无法列举主机用户列表了。如图 7-20 所示。

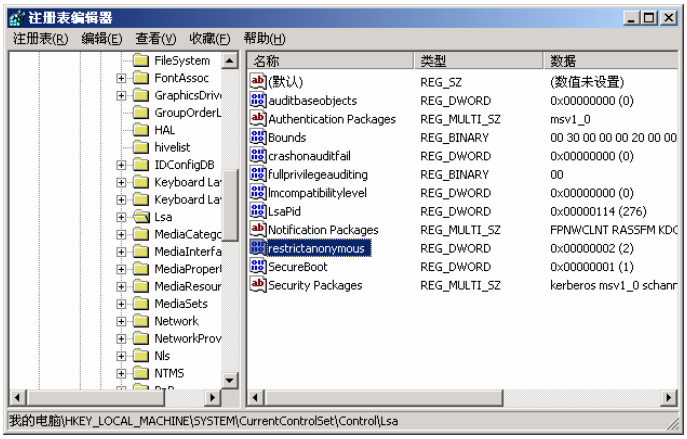

图 7-20 通过注册表对匿名连接的额外限制进行设置

此外，如果把该值设为 1 时，即对应在本地安全设置中将“ 对匿名链接的额外限制 ”设置为 “ 不允许枚举 SAM 账号和共享 ”。

7.5.2 分布式文件系统

系统管理员可以利用分布式文件系统（DFS），使用户访问和管理那些物理上跨网络分布的文件更加容易。通过 DFS，可以是分布在多个服务器上的文件在用户面前显示时，就如同位于网络上的同一个位置。用户在访问文件的时候不再需要知道和指定它们的实际物理位置。

1. 分布式文件系统特性

分布式文件系统（DFS）提供了以下几个重要特性。

（1）容易访问文件

分布式文件系统使得用户可以更容易的访问文件。即使文件可能在物理上跨越多个服务器，用户也只需要转到网络上的某个位置即可访问文件。而且当更改共享文件夹的物理位置时，不会影响用户访问文件夹。用户不再需要多个驱动器映射来访问文件。最后，计划文件服务器维护、软件升级和其他任务（一般需要服务器脱机）可以在不中断用户访问的情况下完成。通过选择 Web 站点的根目录作为 DFS 根目录，可以在分布式文件系统中移动资源，而不会断开任何 Web 访问链接。

（2）可用性

基于域的 DFS 以两种方法确保用户保持对文件的访问。

- Windows 2000 自动将 DFS 拓扑发布到活动目录。这确保 DFS 拓扑对域中所有服务器上的用户总是可见的。
- 作为管理员，用户可以复制 DFS 根目录和 DFS 共享文件夹。复制意味着可以在域中的多个服务器上复制 DFS 根目录和 DFS 共享文件夹，即使这些文件驻留的一个物理服务器不可用，用户将仍然可以访问文件。

（3）服务器负载平衡

DFS 根目录可以支持物理上通过网络分布的多个 DFS 共享文件夹，例如，当用户有一个知道用户将大量访问的文件时。并非所有的用户都在单个服务器上物理地访问此文件，这将会增加服务器的负担，DFS 确保访问文件的用户分布于多个服务器。然而，从用户的角度看来，文件驻留在网络上的相同位置。

2. 分布式文件系统拓扑

分布式文件系统拓扑由 DFS 根目录、一个或多个 DFS 链接、一个或多个 DFS 共享文件夹或每个 DFS 所指向的副本所组成。

DFS 根目录所驻留的域服务器被称为 “ 宿主服务器 ”。通过在域中的服务器上创建 “ 根目录共享 ”，就可以复制 DFS 根目录。这将确保在宿主服务器不可用时，文件仍可使用。

对于用户来说，DFS 拓扑对所需网络资源提供统一和透明的访问。对于系统管理员而言，DFS 拓扑是单个 DNS 名称空间：使用基于域的 DFS，将 DFS 根目录共享的 DNS 名称解析到 DFS 根目录的宿主服务器。

因为基于域的分布式文件系统的宿主服务器是域中的成员服务器，所以在默认情况下，会将 DFS 拓扑自动发布到活动目录中，从而提供了跨越主服务器的 DFS 拓扑同步。这反过来又对 DFS 根目录提供了容错性，并支持 DFS 共享文件夹的可选复制。

通过将 DFS 链接到 DFS 根目录，可以扩展 DFS 拓扑。对 DFS 拓扑中分层结构的层数的惟一限制是对任何文件路径最多使用 260 个字符。新 DFS 链接可以引用共享文件夹或子

文件夹，甚至整个 Windows 2000 卷。如果有足够的权限，则也可以访问任何本地子文件夹，该子文件夹存在于或被添加到 DFS 共享文件夹中。

3. 分布式文件系统的安全性

除了创建必要的管理员权限之外，分布式文件系统服务不实施任何超出 Windows 2000 系统所提供的其他安全措施。指派到 DFS 根目录或 DFS 链接的权限决定可以添加新 DFS 链接的用户。

共享文件的权限与 DFS 拓扑无关。例如，假定有一个名为 TeachingDocs 的 DFS 链接，并且有适当的权限可以访问 TeachingDocs 所指向的特殊 DFS 共享文件夹。在这种情况下，用户就可以访问该 DFS 文件夹组中所有其他 DFS 共享文件夹，而不管是否有访问其他共享文件夹的权限。然而，有权访问这些共享文件夹的权限决定用户是否访问文件夹中的任何信息。

总之，当用户尝试访问 DFS 共享文件夹及其内容时，NTFS 文件系统的卷提供了完整的 Windows 2000 安全性，而 FAT 文件系统仅提供了文件上的共享级安全。

7.6 备份工具

管理员对系统中的系统状态数据、文件及其他数据进行备份是建立安全可靠性配置的一个重要方面。如果不备份数据，则当问题出现时就不能恢复重要的信息或设置，会给系统带来严重的灾难。Windows 2000 系统提供了备份应用工具，可以确保系统数据的更新副本不断地重新存储。

7.6.1 数据备份

1. 备份类型

通常情况下对服务器和本地硬盘的备份可预防数据的丢失或损坏。这些数据的丢失或损坏可能是由磁盘驱动器故障、电力中断、病毒感染以及其他可能的计算机问题所引起的。基于细致规划和可靠设备的备份操作可以使得文件恢复更容易，使用的时间更少。

备份包括以下几种类型。

- 常规备份（normal backup）：这种备份方式将复制所有选定的文件，且将其标记为已备份状态。常规备份时，仅需要备份文件的最近一次副本用以恢复所有的文件。
- 增量备份（incremental backup）：这种备份方式只备份那些自从上一次常规或增量备份后创建的或改动的文件，且将其标记为已备份。如果用户将常规备份与增量备份结合起来使用，则需要最后一次常规备份集合和所有的增量备份集合以便于用来恢复数据。
- 差异备份（differential backup）：这种备份方式将复制那些自从上一次常规或增量备份后创建的或改动的文件，但不将文件标记为已备份。如果用户结合使用常规备份和差异备份，那么需要最后一次常规备份集合和最后一次差异备份集合以用于恢复数据。
- 拷贝备份（copy backup）：这种备份方式将复制所有选定的文件，但不将文件标记为已备份。复制对于常规备份和增量备份之间的文件备份而言十分有用，因为它不影响其他备份操作。
- 每日备份（daily backup）：这种备份方式则是复制在实施日常备份的当天被改动的特定文件，而不管文档属性的当前状态。备份文件不标记已备份状态。

2. 备份的存储介质

Windows 2000 可能将数据备份到不同的存储介质，包括磁带驱动器。数据可备份到逻辑驱动器、可移动磁盘、网络共享区等。如果没有独立的存储设备，则可以备份到另一个硬盘、软盘或移动硬盘上。

3. 备份策略

一个好的备份策略可以最大限度地预防数据丢失。下面是三种常见的备份方法，在不同的环境下根据特定的需要分别采取不同的策略。

- 备份网络还是仅备份服务
- 独立存储介质备份还是本地计算机备份
- 服务器备份还是计算机备份

表 7-8 分析了服务器备份和计算机备份的优缺点。

表 7-8 仅备份服务器与备份本地计算机的比较

备份类型	优点	缺点
只针对服务器	■ 只需很少的存储设备 ■ 由于共享介质存储多个备份，需管理的介质较少 ■ 如果每个服务器有多于一个的客户机，只备份服务器比备份单个计算机的费用低	■ 远程计算机的注册表和事件日志表不能备份 ■ 备份与恢复缓慢，与网络的吞吐量有关 ■ 备份与恢复需大规模的计划与准备。在网络通信量低或需尽可能快地备份关键数据时必须排序
本地计算机	■ 较少的网络资源用于冗余备份过程 ■ 文件恢复快捷	■ 使用的存储介质多、费用高

4. 备份的安全性考虑

可从以下几个方面来增强备份和恢复操作的安全性。

- 在建立备份计划时，应考虑保证存储设备与备份介质的安全。
- 注意备份与恢复权限的划分：备份与恢复的权限是相互独立的。但是一个用户可以同时拥有两种权限。用户必须有管理的权限才可以恢复系统，而用户只需要恢复的权限就可以恢复文件。所以管理员只能将备份与恢复的权限赋予对备份网络负责任的使用者。在低级安全性或中级安全性网络中，赋予一个使用者备份的权限而给另一个使用者恢复的权限。而在高级安全性网络当中，只有管理员自己才可以恢复文件。

如果在一个大型站点中，可参照如下方法来为备份和恢复分配权限。

- 建立名为备份操作员的本地组，只赋予其备份的权限，并给予其成员备份文件和目录的用户权限。然后，建立一个名为只备份的全局组，并将其添加到本地组当中。
- 建立名为恢复操作员的本地组，只赋予其恢复权限，并给予其成员恢复文件和目录的用户权限。接着建立一命名为只恢复的全局组，并将其添加到本地组当中。

7.6.2 Windows 2000 备份工具

Windows 2000 提供了多种创建和执行备份作业的方法。无论采用哪种方法，创建备份作业都包括下面几个基本步骤：

（1）选择要备份的驱动器、目录和文件。

（2）指定要作为备份目标的存储媒介。

（3）配置备份选项，例如备份类型、日志以及排除在外的文件。

在 Windows 2000 系统中，通过“开始”→“程序”→“附件”→“系统工具”→“备份”一系列操作就可以运行 Windows 200 的图形化（GUI）备份工具。这里既可以使用“备份向导”，也可以使用“备份”选项卡来进行备份操作，如图 7-21 所示。

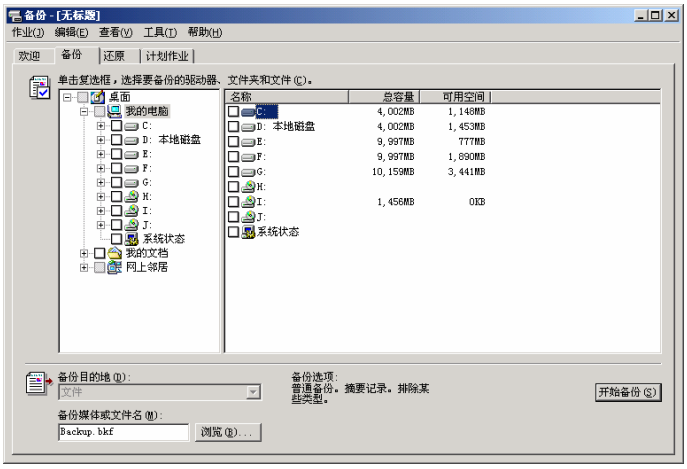

图 7-21 图形化“备份”工具