第 3 章　文件系统管理

教学重点

- 文件系统管理基础；
- NTFS 文件系统主要管理。

在计算机系统中最为重要的资源就是数据资源，许多计算机操作系统都是通过特有的文件系统管理技术来为用户提供数据信息的，并且支持其自身独具特色的文件类型。Windows Server 2016 提供了不同于其他操作系统的 NTFS 文件系统管理类型，在文件系统管理、安全等方面提供了强大的功能，用户可以很方便地在计算机或者网络上使用、管理、共享和保护文件及文件资源。本章将介绍 Windows Server 2016 有关文件系统方面的内容，主要介绍文件系统的基本概念、NTFS 文件系统与 FAT 文件系统的区别、NTFS 文件系统在安全方面的特性、如何在 Windows Server 2016 内配置 NTFS 的权限，以及如何实现加密文件系统。

3.1　文件系统概述

所谓文件系统，是操作系统在存储设备上按照一定原则组织、管理数据所用的结构和机制。文件系统规定了计算机对文件和文件夹进行操作处理的各种标准和机制，用户对于所有的文件和文件夹的操作都是通过文件系统来完成的。

磁盘或分区和操作系统所包括的文件系统是不同的，在所有的计算机系统中，都存在一个相应的文件系统。FAT、FAT32 格式的文件系统是随着计算机各种软件、硬件的发展而成的文件系统，它们所能管理的文件的最大尺寸及磁盘空间总量都有一定的局限性。从 Windows NT 开始，采用了一种新的文件系统格式：NTFS 文件系统，它比 FAT、FAT32 功能更加强大，在文件大小、磁盘空间、安全可靠等方面都有了较大的进步。在日常工作中，我们常会听到这种说法，“我的硬盘是 FAT 格式的”“C 盘是 NTFS 格式的”，这是不恰当的，NTFS 或是 FAT 并不是格式，而是文件管理的系统类型。一般刚出厂的硬盘是没有任何类型文件系统的，在使用之前必须利用相应的磁盘分区工具对其进行分区，格式化后才会有一定类型的文件系统，才可正常操作使用。由此可见，无论硬盘有一个分区还是多个分区，文件系统都是对应分区的，而不是对应硬盘的。Windows Server 2016 的磁盘分区一般支持 3 种格式的文件系统：FAT、FAT32 和 NTFS。

在安装 Windows Server 2016 之前，应该先选择文件系统。Windows Server 2016 支持使用 NTFS 文件系统和文件分配表文件系统（FAT 或 FAT32）。下面将对这两类文件系统

进行简单介绍。

1. FAT/FAT32 文件系统

FAT（File Allocation Table）是“文件分配表”的意思，就是用来记录文件所在位置的表格。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式：放置在分区起始位置的文件分配表。为确保正确装卸启动系统所必需的文件，文件分配表和根目录必须存放在磁盘分区的固定位置。文件分配表对于硬盘的使用是非常重要的，假若丢失文件分配表，那么硬盘上的数据就会因为无法定位而不能使用了。

FAT 通常使用 16 位的空间来表示每个扇区（Sector）配置文件的情形，FAT 由于受到先天的限制，因此每超过一定容量的分区之后，它所使用的簇（Cluster）大小就必须扩增，以适应更大的磁盘空间。簇是磁盘空间的配置单位，就如图书馆内一格一格的书架一样。每个要保存的文件都必须配置足够数量的簇，才能存放到磁盘中。通过使用命令提示符“Format”，用户可以指定簇的大小。一个簇存放一个文件后，其剩余的空间不能再被其他文件利用。所以在使用磁盘时，无形中都会或多或少损失一些磁盘空间。

在运行 MS-DOS、OS/2、Windows 95/98 或 Windows 95 以前的版本操作系统的计算机时，FAT 文件系统格式是最佳的选择。需要注意的是，在不考虑簇大小的情况下，使用 FAT 文件系统的分区不能大于 2GB，因此 FAT 文件系统最好用在较小分区上。由于 FAT 额外开销的原因，在大于 512MB 的分区内不推荐使用 FAT 文件系统。

FAT32 使用 32 位空间来表示每个扇区（Sector）的配置文件。利用 FAT32 所能使用的单个分区，最大可达到 2TB（2048GB），而且各种大小的分区所能用到的簇的大小也恰如其分，这些优点使 FAT32 的系统在硬盘使用上有更高的效率。例如，两个分区容量都为 2GB，一个分区采用了 FAT 文件系统，另一个分区采用了 FAT32 文件系统。采用 FAT 分区的簇大小为 32KB，而采用 FAT32 分区的簇只有 4KB。那么 FAT32 就比 FAT 的存储效率要高很多，通常情况下可以提高 15%。

FAT32 文件系统可以重新定位根目录，同时 FAT32 分区的启动记录包含在一个含有关键数据的结构中，减少了计算机系统崩溃的可能性。

使用 FAT32 文件系统也有一定的限制，主要表现在以下几方面：

（1）与操作系统有限的兼容性。目前，支持 FAT32 格式的操作系统有 Windows 95、Windows 98、OS/2、Windows Me、Windows 2000、Windows XP、Windows Server 2003、Windows Server 2008 和 2012，一些 UNIX/Linux 版本也对 FAT32 提供有限支持。其他操作系统则不能读取 FAT32 的分区。例如，以 DOS 6.X 启动盘开机的话，硬盘中的 FAT32 分区就会凭空消失，完全看不到这个分区。

（2）虽然与 FAT 相比，FAT32 可以支持的磁盘容量达到 2TB（2048GB），但是 FAT32 不能支持小于 512MB 的分区。

（3）一些版本较旧的软件不能在 FAT32 的分区中执行，如 Office 95 等。

（4）不能在 FAT32 分区中做磁盘压缩，在 Windows 98 中进行磁盘压缩也是行不通的。

需要注意的是，这种分区格式还有明显的缺点，由于文件分配表的扩大，FAT32 格式运行速度比 FAT 格式慢。此外，FAT 和 FAT32 不能较好地集成，当分区变大时，文件分配表也随之变大，这就相应增加了系统重新启动的时间。因此，在 Windows Server

2008 中不支持用户使用格式化程序来创建超过 32GB 的 FAT32 分区。

2. NTFS 文件系统

NTFS（New Technology File System）是 Windows Server 2016 推荐使用的高性能文件系统，支持许多新的文件安全、存储和容错功能，而这些功能正是 FAT/FAT32 所缺少的，它支持文件系统大容量的存储媒体、长文件名。NTFS 文件系统的设计目标是在容量大的硬盘上能够快速执行，如读/写、搜索文件等标准操作。NTFS 还支持文件系统恢复高级操作。

NTFS 文件系统不仅支持企业环境中文件服务器和高端个人计算机所需的安全特性，还支持对于关键数据完整性十分重要的数据访问控制和私有权限。除了赋予 Windows Server 2016 计算机中的共享文件夹特定权限，NTFS 文件和文件夹无论共享与否都可以赋予权限。NTFS 是 Windows Server 2016 中唯一允许为单个文件指定权限的文件系统。

像 FAT 文件系统一样，NTFS 文件系统使用簇作为磁盘分配的基本单元。在 NTFS 文件系统中，默认的簇大小取决于卷的大小。在“磁盘管理器”窗口中，用户可以指定簇最大为 4KB。

NTFS 是以卷为基础的，卷建立在磁盘分区之上。分区是磁盘的基本组成部分，是一个能够被格式化和单独使用的逻辑单元。当以 NTFS 格式来格式化磁盘分区时，就创建了 NTFS 卷。一个磁盘可以有多个卷，一个卷也可以由多个磁盘组成。需要注意的是，当用户从 NTFS 卷移动或复制文件到 FAT 卷时，NTTS 文件系统权限和其他特有属性将会丢失。

NTFS 文件系统最为重要的是，它是一个基于安全性的文件管理系统，建立在保护文件和目录数据基础之上，同时兼顾节省存储资源、减少磁盘占用量，是一种先进的文件系统。早期的 Windows NT 4.0 采用的就是 NTFS 4.0 文件系统，它使系统的安全性得到了很大提高。Windows 2000/XP、Windows Server 2008 采用的是新版本的 NTFS 文件系统。NTFS 使用户不但可以像 Windows 9x 那样方便快捷地操作和管理计算机，而且可享受到 NTFS 所带来的系统安全性。NTFS 的特点主要体现在以下几方面：

（1）NTFS 是一个日志文件系统，这意味着除了向磁盘中写入信息，该文件系统还会为所发生的所有改变保留一份日志。这一功能让 NTFS 文件系统在发生错误时（如系统崩溃或电源供应中断）更容易恢复，也使系统更加强壮。在 NTFS 分区上用户很少需要运行磁盘修复程序，NTFS 通过使用标准的事务处理日志和恢复技术来保证分区的一致性。发生系统失败事件时，NTFS 使用日志文件和检查点信息自动恢复文件系统的一致性。

（2）良好的安全性是 NTFS 另一个引人注目的特点，这也是 NTFS 成为 Windows 网络中最常用的文件系统的主要的原因。NTFS 的安全系统非常强大，可以对文件系统中对象的访问权限（允许或禁止）做非常精确的设置。在 NTFS 卷上，可以为共享资源、文件夹及文件设置访问许可权限。许可权限的设置包括两方面的内容：一是允许哪些组或用户对文件夹、文件和共享资源进行访问；二是获得访问许可的组或用户可以进行什么级别的访问。访问许可权限的设置不但适用于本地计算机的用户，而且应用于通过网络的共享文件夹对文件进行访问的网络用户。与 FAT32 文件系统下对文件夹或文件进行的访问相比，安全性要高得多。另外，在采用 NTFS 格式的 Windows Server 2016 中，用审核策略可以对文件夹、文件及活动目录对象进行审核，审核结果记录在安全日志中。通过安全日志就可以查看组或用户对文件夹、文件或活动目录对象进行了什么级别的操

作，从而发现系统可能面临的非法访问，通过采取相应的措施，将这种安全隐患降到最低。这些在 FAT32 文件系统下，是不能实现的。

（3）NTFS 支持对卷、文件夹和文件的压缩。任何基于 Windows 的应用程序对 NTFS 卷上的压缩文件进行读/写时，不需要事先由其他程序进行解压缩，文件将自动进行解压缩，文件关闭或保存时会自动对文件进行压缩。

（4）在 Windows Server 2016 的 NTFS 文件系统中可以进行磁盘配额管理。磁盘配额是指管理员为用户所能使用的磁盘空间进行配额限制，每个用户只能使用最大配额范围内的磁盘空间。设置磁盘配额后，可以对每个用户的磁盘使用情况进行跟踪和控制，通过监测标识出超过配额报警阈值和配额限制的用户，从而采取相应的措施。磁盘配额管理功能使管理员方便合理地为用户分配存储资源，避免由于磁盘空间使用的失控造成的系统崩溃，提高了系统的安全性。

（5）对大容量的驱动器有良好的扩展性。在磁盘空间使用方面，NTFS 的效率非常高。NTFS 采用了更小的簇，可以更有效率地管理磁盘空间，相比之下，NTFS 比 FAT32 更有效地管理磁盘空间，最大限度地避免了磁盘空间的浪费。因此，NTFS 中最大驱动器的尺寸远远大于 FAT 格式，且 NTFS 的性能和存储效率并不像 FAT 那样随着驱动器尺寸的增大而降低。

Windows Server 2016 中提供的系统工具可以很轻松地把分区转化为新版本的 NTFS 文件系统，即使以前的分区使用的是 FAT 或 FAT32。在安装 Windows Server 2016 时，可以在安装向导的帮助下即可完成所有操作，安装程序会检测现有的文件系统格式，如果是 NTFS，则自动进行转换；如果是 FAT 或 FAT32，则会提示安装者是否转换为 NTFS。用户也可以在安装完毕，使用 Convert.exe 把 FAT 或 FAT32 的分区转化为 NTFS 分区。无论是在运行安装程序中还是在运行安装程序之后，这种转换都不会使用户的文件受到损害。

3.2 项目：NTFS 文件系统管理

3.2.1 任务 1：理解 NTFS 权限

Windows Server 2016 在 NTFS 类型卷上提供了 NTFS 权限，允许为每个用户或者组指定 NTFS 权限，以保护文件和文件夹资源的安全。通过允许、禁止或是限制访问某些文件和文件夹，NTFS 权限提供了对资源的保护。不论用户是访问本地计算机上的文件、文件夹资源，还是通过网络来访问，NTFS 权限都是有效的。

NTFS 权限可以实现高度的本地安全性，通过对用户赋予 NTFS 权限，可以有效地控制用户对文件和文件夹的访问。NTFS 卷上的每个文件和文件夹都有一个列表，称为访问控制列表（Access Control List，ACL），该列表记录了每个用户和组对该资源的访问权限。当用户要访问某一文件资源时，ACL 必须包含该用户账户或组的入口，只有入口允许的访问类型与请求的访问类型一致时，才允许用户访问该文件资源。如果在 ACL 中没有一个合适的入口，那么该用户就无法访问该文件资源。

Windows Server 2016 的 NTFS 许可权限包括了普通权限和特殊权限。

（1）NTFS 的普通权限有读取和写入、列出文件夹内容、读并且执行、修改、完全控制，以下将对它们分别进行说明。

- 读取：允许用户查看文件或文件夹；可以读取文件内容，但不能修改文件内容。
- 列出文件夹内容：仅文件夹有此权限，可查看文件夹下子文件和文件夹属性与权限，读取文件夹下子文件内容。
- 写入：允许授权用户可以对一个文件进行写操作。
- 读并且执行：用户可以运行可执行文件，包括脚本。
- 修改：用户可以查看并修改文件或者文件属性，包括在目录下增加或删除文件，以及修改文件属性。
- 完全控制：用户可以修改、增加、移动或删除文件，能够修改所有文件和文件夹的权限设置。

（2）NTFS 的特殊权限包括以下详细内容。

- 遍历文件夹/运行文件："遍历文件夹"允许或拒绝通过文件夹移动，以到达其他文件或文件夹，即使用户没有被禁止的文件夹的权限（仅适用于文件夹）。只有当"组策略"管理单元中没有授予组或用户"忽略通过检查"用户权限时，禁止文件夹才起作用（默认情况下，授予 Everyone 组"忽略通过检查"用户权限）。对于文件，"运行文件"允许或拒绝运行程序文件（仅适用于文件）。设置"遍历文件夹"权限不会自动设置该文件夹中所有文件的"运行文件"权限。
- 列出文件夹/读取数据：允许或拒绝用户查看文件夹内容列表或数据文件。
- 读取属性：允许或拒绝用户查看文件或文件夹的属性，如只读或者隐藏，属性由 NTFS 定义。
- 读取扩展属性：允许或拒绝用户查看文件或文件夹的扩展属性。扩展属性由程序定义，可能因程序而变化。
- 创建文件/写入数据："创建文件"权限允许或拒绝用户在文件夹内创建文件（仅适用于文件夹）；"写入数据"允许或拒绝用户修改文件，仅适用于文件。
- 创建文件夹/附加数据："创建文件夹"允许或拒绝用户在文件夹内创建文件夹（仅适用于文件夹）。"附加数据"允许或拒绝用户在文件的末尾进行修改，但是不允许用户修改、删除或者改写现有的内容（仅适用于文件）。
- 写入属性：允许或拒绝用户修改文件或者文件夹的属性，比如只读或者是隐藏，属性由 NTFS 定义。"写入属性"权限表示不可以创建或删除文件和文件夹，只能更改文件或文件夹的属性。要允许（或者拒绝）创建或删除操作，可参阅"创建文件/写入数据""创建文件夹/附加数据""删除子文件夹及文件""删除"中的说明。
- 写入扩展属性：允许或拒绝用户修改文件或文件夹的扩展属性。扩展属性由程序定义，可能因程序而变化。"写入扩展属性"权限表示不可以创建或删除文件和文件夹，只能更改文件或文件夹的属性。要允许（或者拒绝）创建或删除操作，可参阅"创建文件/写入数据""创建文件夹/附加数据""删除子文件夹及文件""删除"中的说明。
- 删除子文件夹及文件：允许或拒绝用户删除子文件夹和文件。
- 删除：允许或拒绝用户删除子文件夹和文件（如果用户对于某个文件或文件夹没有删除权限，但是拥有删除子文件夹和文件权限，仍然可以删除文件或文件夹）。

- 读取权限：允许或拒绝用户对文件或文件夹的读权限，如完全控制、读或写权限。
- 修改权限：允许或拒绝用户修改该文件或文件夹的权限分配，如完全控制、读或写权限。
- 获得所有权：允许或拒绝用户获得对该文件或文件夹的所有权。无论当前文件或文件夹的权限分配状况如何，文件或文件夹的拥有者总可改变他的权限。
- 同步：允许或拒绝不同的线程等待文件或文件夹的句柄，并与另一个向它发信号的线程同步。该权限只能用于多线程、多进程程序。

NTFS 的普通权限由更小的特殊权限元素组成。管理员可以根据需要，利用 NTFS 特殊权限，进一步控制用户对 NTFS 文件或文件夹的访问。

上述权限设置中比较重要的是修改权限和获得所有权，通常情况下，这两个特殊权限要慎重使用，一旦赋予了某个用户修改权限，便可以改变相应文件或者文件夹的权限设置。同样，一旦赋予了某个用户获得所有权权限，他就可以作为文件的所有者对其做出查阅并更改。

3.2.2 任务 2：设置 NTFS 权限

只有 Administrators 组内的成员、文件和文件夹的所有者、具备完全控制权限的用户，才有权更改这个文件或文件夹的 NTFS 权限。设置的方法为：打开“资源管理器”或“计算机”，在 NTFS 卷上指定要设置 NTFS 权限的文件夹或文件，单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在随后出现的“Test 属性”对话框中选择“安全”选项卡，如图 3-1 所示，然后进行 NTFS 权限设置。

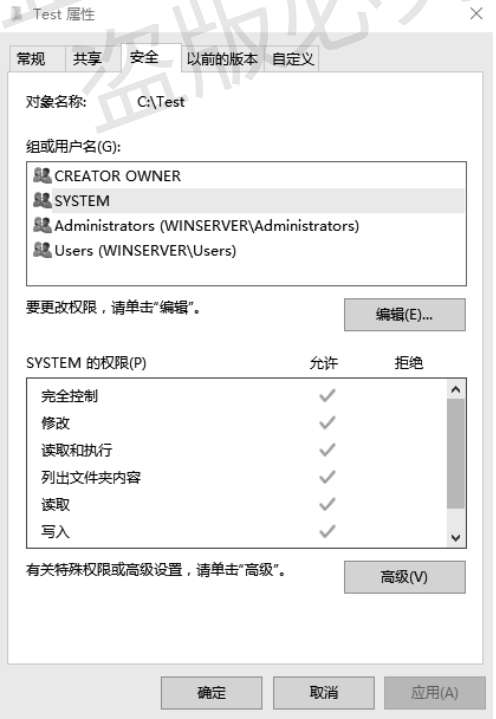

图 3-1 “Test 属性”对话框

进行 NTFS 权限设置实际上就是设置“谁”有“什么”权限，在图 3-1 所示的选项卡上端的窗口和按钮用于选取用户和组账户，解决“谁”的问题；下端的窗口和按钮则为已选中的用户或组设置相应的权限，解决“什么”的问题。

1. 添加/删除用户和组

若要添加权限用户，单击“编辑|添加”按钮，出现如图 3-2 所示的对话框，在这个对话框中可以直接在文本框中输入用户、账户名称。

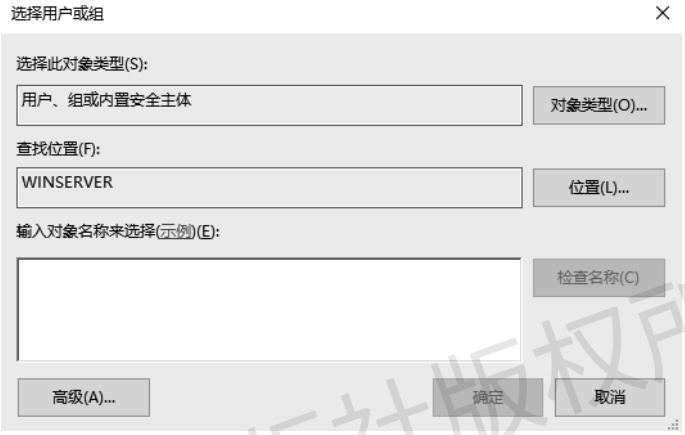

图 3-2　“选择用户或组”对话框添加用户或组

以选取的方式添加用户和组账户名称的方法是：单击“高级”按钮，在图 3-2 所示的对话框中单击“对象类型”按钮在打开的对话框中进行选择缩小搜索账户类型的范围（见图 3-3），再单击“位置”按钮搜索账户的位置，然后单击“立即查找”按钮。搜索完成后在“搜索结果”窗口中，用鼠标选取需要的账户，可以按住 Shift 键连续选取或者按住 Ctrl 键间隔选取多个账户，最后单击“确定”按钮返回，再次单击“确定”按钮完成账户的选取操作。此时，在“Test 属性”对话框的“安全”选项卡上端的窗口中已经可以看到新添加的用户和组，如图 3-4 所示。若要删除权限用户，在图 3-4 所示的“组或用户名”列表中选择这个用户，然后单击“删除”按钮即可。

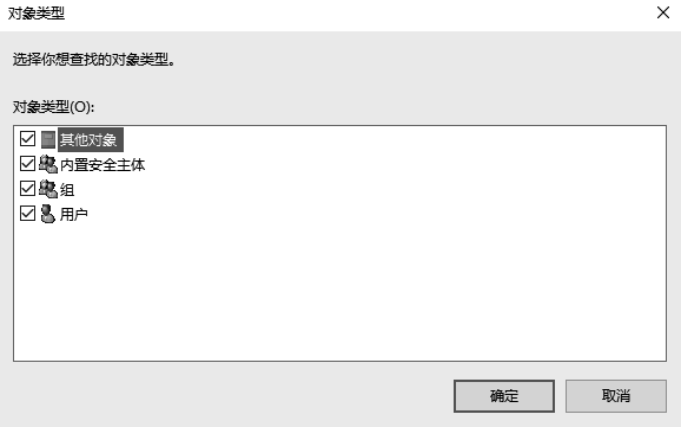

图 3-3　“对象类型”对话框以查找方式添加用户

图 3-4　添加用户账户后的属性对话框

2. 为用户和组设置权限

若要设置一个账户的 NTFS 权限，则在图 3-4 所示的对话框上端选取该账户，就可以在下端的窗口中对其设置相应的 NTFS 权限。在该对话框中显示的是 NTFS 标准权限，对于每一种标准权限，对钩表示“允许”，没有对钩表示“拒绝”，已经用灰色的对钩选中的权限表示这种默认的权限设置是从父对象继承的，选项继承了该用户（或组）对该文件或文件夹所在上一级文件夹的 NTFS 权限。

如果需要进一步设置 NTFS 权限，可以单击“高级”按钮，在如图 3-5 所示的对话框中进行设置。

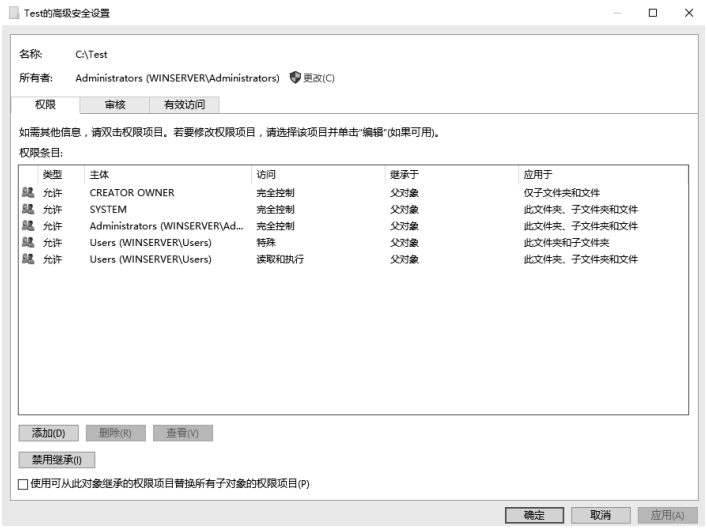

图 3-5　NTFS 权限的高级设置

3. NTFS 权限的应用规则

管理员可以根据需要赋予用户访问 NTFS 文件或文件夹的权限，同时管理员可以赋予用户所属组访问 NTFS 文件或文件夹的权限。用户访问 NTFS 文件或文件夹时，其有效权限必须通过相应的应用原则来确定。NTFS 权限应用遵循以下几个原则：

（1）NTFS 权限是累积的。用户对某个 NTFS 文件或文件夹的有效权限，是用户对该文件或文件夹的 NTFS 权限和用户所属组对该文件或文件夹的 NTFS 权限的组合。如果一个用户同时属于两个组或者多个组，而各组对同一个文件资源有不同的权限，这个用户会得到各组的累加权限。假设用户 Jack 属于 A 和 B 两个组，A 组对某文件有读取权限，B 组对此文件有写入权限，而 Jack 自己对此文件有修改权限，那么 Jack 对此文件的最终权限为“读取+写入+修改”。

（2）文件权限超越文件夹权限。当一个用户对某个文件及其父文件夹都拥有 NTFS 权限时，如果用户对父文件夹的权限小于文件的权限，那么该用户对该文件的有效权限是以文件权限为准的。例如，folder 文件夹包含 file 文件，用户 Jack 对 folder 文件夹有列出文件夹内容的权限，对 file 有写入的权限，那么 Jack 访问 file 时的有效权限则为写入权限。

（3）拒绝权限优先于其他权限。管理员可以根据需要拒绝指定用户访问指定文件或文件夹，当系统拒绝用户访问某文件或文件夹时，不管用户所属组对该文件或文件夹拥有什么权限，用户都无法访问文件。

假设用户 Jack 属于 A 组，管理员赋予 Jack 对某一文件拒绝写入的权限，赋予 A 组对该文件完全控制的权限，那么 Jack 访问该文件时，其有效权限则为读取权限。又如，Jack 属于 A 和 B 两个组，Jack 对某一文件有写入权限、A 组对此文件有读取权限，但是 B 组对此文件为拒绝读取权限，那么 Jack 对此文件只有写入权限。如果 Jack 对此文件只有写入权限，此时 Jack 写入权限有效吗？答案很明显，Jack 对此文件的写入权限无效，因为无法读取是不可能写入的。

（4）文件权限的继承。当用户对文件夹设置权限后，在该文件夹中创建的新文件和子文件夹将自动默认继承这些权限。从上一级继承下来的权限是不能直接修改的，只能在此基础上添加其他权限，也就是不能把权限上的钩去掉。灰色的框为继承的权限，是不能直接修改的，白色的框是可以添加的权限。

如果不希望子文件夹或文件继承父文件夹或文件的权限，可以在为父文件夹和文件设置权限时，设置为“不继承父文件夹”权限，这样子文件夹或文件的权限将改为用户直接设置的权限，从而避免了由于疏忽或者没有注意到而传播反应，导致后门大开，让一些人有机可乘。

（5）复制或移动文件或文件夹时权限的变化。文件和文件夹资源的移动、复制操作对权限继承是有些影响的，主要体现在以下几个方面：

- 在同一个卷内移动文件或文件夹时，此文件和文件夹会保留在原位置的 NTFS 权限；在不同的 NTFS 卷之间移动文件或文件夹时，文件或文件夹会继承目的卷中文件夹的权限。
- 当复制文件或文件夹时，不论是否复制到同一卷还是不同卷，都将继承目的卷中文件夹的权限。

- 从 NTFS 卷向 FAT 分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失。

在实际复制或移动文件或文件夹前，应该检查和确保移动、复制的所有权和权限。假如没有移动、复制文件夹的所有权或者权限，即使作为一名管理员也无法对该文件或文件夹操作。但是，如果先获得对文件夹或文件的所有权，再分配给自己必要的权限，就可以操作了。

4. NTFS 权限与共享权限的组合权限

NTFS 权限与共享权限都会影响用户获取网上资源的能力。共享权限只对共享文件夹的安全性做控制，即只控制来自网络的访问，但也适合 FAT 和 FAT32 文件系统。NTFS 权限则对所有文件和文件夹做安全控制（无论访问来自本地主机还是网络），但只适用于 NTFS 文件系统。当共享权限和 NTFS 权限冲突时，以两者中最严格的权限设定为准。需要强调的是，在 Windows XP、Windows Server 2008 及后续的 Windows 版本中，系统所默认的共享权限都是只读，这样通过网络访问 NTFS 卷所能获得的权限受到了限制。

共享权限有三种：读取、更改和完全控制。Windows Server 2016 默认的共享文件设置权限是 Everyone 用户只具有读取权限。而 Windows 2000 默认的共享文件设置权限是 Everyone 用户具有完全控制权限。下面解释三种权限。

（1）读取：读取权限是指派给 Everyone 组的默认权限，可实现以下操作：

- 查看文件名和子文件夹名。
- 查看文件中的数据。
- 运行程序文件。

（2）更改：更改权限不是任何组的默认权限。更改权限除允许所有的读取权限，还增加以下权限。

- 添加文件和子文件夹。
- 更改文件中的数据。
- 删除子文件夹和文件。

（3）完全控制：完全控制权限是指派给本机 Administrators 组的默认权限。完全控制权限除允许全部读取权限，还具有更改权限。

与 NTFS 权限一样，如果赋予某用户或者用户组拒绝的权限，则该用户或者该用户组的成员将不能执行被拒绝的操作。

当用户从本地计算机直接访问文件夹时，将不受共享权限的约束，只受 NTFS 权限的约束。当用户从网络访问一个存储在 NTFS 文件系统上的共享文件夹时，会受到 NTFS 权限与共享权限的约束，而有效权限是最严格的权限（也就是这两种权限的交集）。同样，这里也要考虑到两个权限的冲突问题。例如，共享权限为只读，NTFS 权限是写入，那么最终权限是完全拒绝，这是因为这两个权限的组合权限是两个权限的交集。

共享权限只对通过网络访问的用户有效，所以需要与 NTFS 权限配合（如果分区是 FAT/FAT32 文件系统，则不需要考虑）才能严格控制用户的访问。当一个共享文件夹设置了共享权限和 NTPS 权限后，就要受到两种权限的控制。如果希望用户完全控制共享

文件夹，首先要在共享权限中添加此用户（组），并设置完全控制的权限，然后在 NTFS 权限设置中添加此用户（组），并设置完全控制的权限，只有两个地方都设置了完全控制权限，才能最终拥有完全控制权限。

5. NTFS 所有权

在 Windows Server 2016 的 NTFS 卷上，每个文件和文件夹都有其“所有者”，我们称之为“NTFS 所有权”，系统默认创建文件或文件夹的用户是该文件或文件夹的所有者。NTFS 所有权即 NTFS 文件和文件夹所有权，当用户对某个文件或文件夹具有所有权时，就具备了更改该文件或文件夹权限设置的能力。

更改所有权的前提条件是用户必须具备“所有权”的权限，或者具备获得“取得所有权”的能力。Administrators 组的成员拥有“取得所有权”的权限，可以修改所有文件和文件夹的所有权设置。对于某个文件夹具备读取权限和更改权限的用户，就可以为自身添加“取得所有权”权限，也就是具备获得“取得所有权”的权限能力。获得或更改对象的所有权的步骤如下。

步骤 1：打开“资源管理器”或“计算机”，找到要修改 NTFS 权限的文件或文件夹（以“C:\Test\Mytest.txt”为例）。

步骤 2：在指定文件或文件夹上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，然后切换到“安全”选项卡。

步骤 3：单击“高级”按钮，然后在弹出的“MyTest 的高级安全设置”对话框中单击“更改”选项，如图 3-6 所示。

图 3-6 “更改”选项

步骤 4：在“将所有者更改为”列表框中，选择将获得所有权的用户或组的账户名称，如果要将所有权转移给其他用户或组，则依次单击“编辑|其他用户或组”按钮，选择输入指定的用户或组，最后单击“确定”按钮。

3.2.3 任务 3：NTFS 的压缩与加密属性

1. NTFS 文件系统的压缩属性

优化磁盘空间管理的一种方法是使用压缩技术，即压缩文件（或文件夹）减少其大小，同时减少它们在驱动器或可移动存储设备上所占用的空间。Windows Server 2016 的数据压缩功能是 NTFS 文件系统的内置功能，该功能可以对单个文件、整个目录或卷上的目录树进行压缩。NTFS 压缩只能在用户数据文件上执行，而不能在文件系统元数据上执行。NTFS 文件系统的压缩过程和解压缩过程对于用户而言是完全透明的（与第三方的压缩软件无关），用户只要将文件数据应用压缩功能即可。当用户或应用程序使用压缩的数据文件时，操作系统会自动在后台对数据文件进行解压缩，无须用户干预。这项功能可以节省一定的硬盘空间。

使用 Windows Server 2016 NTFS 压缩文件或文件夹的步骤如下。

步骤 1：打开“资源管理器”或“计算机”，找到要压缩的文件或文件夹。

步骤 2：在指定文件或文件夹上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，可以看到图 3-7 所示的“常规”选项卡。

图 3-7 文件属性的“常规”选项卡

步骤 3：在“常规”选项卡中，单击“高级”按钮。

步骤 4：在文件的“高级属性”对话框的“压缩或加密属性”下（如图 3-8 所示），选中“压缩内容以便节省磁盘空间”复选框，然后单击“确定”按钮。

图 3-8　选中“压缩内容以便节省磁盘空间”

步骤 5：如果是压缩指定的文件夹，那么在“高级属性”对话框中，单击“确定”按钮时，在弹出如图 3-9 所示的“确认属性更改”对话框中选择需要的选项。

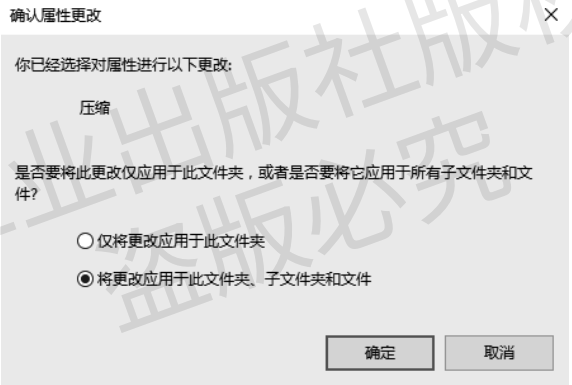

图 3-9　“确认属性更改”对话框

提示：可以使用 NTFS 压缩属性，压缩已格式化为 NTFS 卷上的文件和文件夹。如果没有出现“高级”按钮，则说明所选的文件或文件夹不在 NTFS 驱动器上。NTFS 的压缩和加密属性互斥，文件加密后就不能再压缩，压缩后就不能再加密。

在 Windows Server 2016 操作系统的 NTFS 卷内或卷间复制或移动 NTFS 文件或文件夹时，文件或文件夹的 NTFS 压缩属性会发生相应的变化。在 Windows Server 2016 操作系统中，不管是在 NTFS 卷内还是在卷间复制文件或文件夹，系统都将目标文件作为新文件对待，文件将继承目的地文件夹的压缩属性。

在 Windows Server 2016 操作系统的同一卷内移动文件或文件夹时，文件或文件夹不会发生任何变化，系统只更改卷中指向文件或文件夹头指针的位置，在 NTFS 卷间移动 NTFS 文件或文件夹时，系统将目标文件作为新文件对待。文件将继承目的地文件夹的压缩属性。另外，任何被压缩的 NTFS 文件移动或复制到 FAT/FAT32 分区时将自动解压，不再保留压缩属性。

2. NTFS 文件系统的加密属性

NTFS 文件系统的加密属性是通过加密文件系统（Encrypting File System，EFS）技术实现的，EFS 提供的是一种核心文件加密技术。EFS 仅能用于 NTFS 卷上的文件和文件夹加密。EFS 加密对用户是完全透明的，当用户访问加密文件时，系统自动解密文件，当用户保存加密文件时，系统会自动加密该文件，不需要用户任何手工交互动作。EFS 是 Windows 2000、Windows XP Professional（Windows XP Home 不支持 EFS）、Windows Server 2003/2008/2012/2016 NTFS 文件系统的一个组件。EFS 采用高级的标准加密算法实现透明的文件加密和解密，任何没有合适密钥的个人或者程序都不能读取加密数据。即便是物理上拥有驻留加密文件的计算机，加密文件仍然受到保护，甚至有权访问计算机及其文件系统的用户也无法读取这些数据。

（1）EFS 技术特性

EFS 加密技术作为集成的系统服务运行，具有管理容易、攻击困难、对文件所有者透明等特点。EFS 具有如下特性：

- 透明的加密过程，不要求用户（文件所有者）每次使用都进行加、解密。
- 强大的加密技术，基于公钥加密。
- 完整的数据恢复功能。
- 可保护临时文件和页面文件。

文件加密的密钥驻留在操作系统的内核中，并且保存在非分页内存中，这保证了密钥不会被复制到页面文件中，因而不会被非法访问。

EFS 具有类似于使用文件和文件夹上的权限。未经许可对加密文件、文件夹进行物理访问的入侵者将无法阅读其中的内容。入侵者如果试图打开或复制已加密文件或文件夹，则将收到拒绝访问消息。但文件和文件夹上的权限不能防止未授权的物理攻击。

EFS 将文件加密作为文件属性保存，通过修改文件属性对文件和文件夹进行加密和解密。正如设置其他属性（如只读、压缩或隐藏）一样，通过对文件夹和文件的加密属性，可以对文件夹或文件进行加密和解密。如果加密一个文件夹，则在加密文件夹中创建的所有文件和子文件夹都自动加密，推荐在文件夹级别上加密。Windows Server 2016 操作系统的 EFS 具有以下特征：

- 只能加密 NTFS 卷上的文件或文件夹。
- 不能加密压缩的文件或文件夹，如果用户加密某个压缩文件或文件夹，则该文件或文件夹会被解压。
- 如果将加密的文件复制或移动到非 NTFS 格式的分区上，则该文件会被解密。
- 如果将非加密文件移动到加密文件夹中，则这些文件将在新文件夹中自动加密。然而，反向操作则不能自动解密文件，文件必须明确解密。
- 无法加密标记为“系统”属性的文件，且位于“%systemroot%”目录结构中的文件也无法加密。
- 加密文件、文件夹不能防止删除或列出文件或目录。具有合适权限的人员可以删除或列出已加密文件或文件夹，因此建议应结合 NTFS 权限使用 EFS。
- 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，必须使用诸如SSL\TLS（安全套接字层/传输层安全性）或 Internet 协议安全性（IPSec）等协议通过有线加密数据。

（2）实现 EFS 属性的操作

用户可以使用 EFS 进行加密、解密、访问、复制文件或文件夹。下面就介绍如何实现文件的加密操作。

① 打开“资源管理器”或“计算机”，找到要加密的文件或文件夹。

② 在指定文件夹上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在弹出的“属性”对话框中单击“高级”按钮。

③ 弹出“高级属性”对话框，在“压缩或加密属性”区域中选择“加密内容以便保护数据”，如图 3-10 所示，然后单击“确定”按钮。

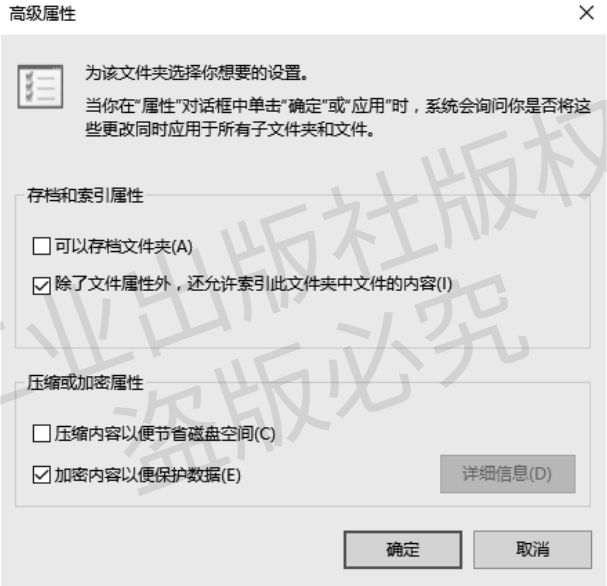

图 3-10　加密文件或文件夹

④ 如果是压缩指定的文件夹，在出现“确认属性更改”对话框时，选择“仅将更改应用于此文件夹”，系统将只对文件夹加密，里面原有内容并没经过加密，但是在其中创建的文件或文件夹将被加密。选择“将更改应用于此文件夹、子文件夹和文件”，则文件夹内部的所有内容都被加密。

⑤ 单击“确定”按钮，完成加密。

注意：在首次进行加密操作时，Windows Server 2016 操作系统提示操作者备份文件加密证书和密钥，如图 3-11 所示。创建备份文件可避免在丢失或损坏原始证书和密钥之后，无法再对加密文件的访问。加密操作者可根据不同选择进行备份。

文件的所有者也可以使用与加密相似的方法对文件夹进行解密，而且无须解密即可打开文件进行编辑（EFS 在所有者面前是透明的）。如果正式解密一个文件，将会使其他用户访问该文件。下面是解密文件或文件夹的具体步骤：

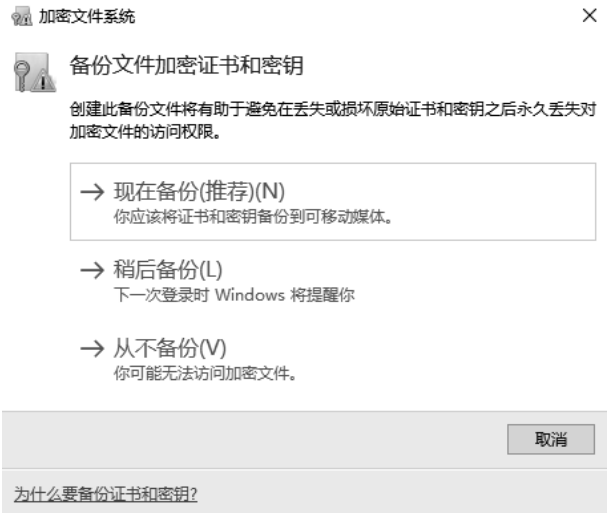

图 3-11　加密文件系统备份证书和密钥

① 打开“资源管理器”或“计算机”，找到要解密的文件或文件夹。

② 在指定文件或文件夹上，单击鼠标右键，在弹出的快捷菜单中选择“属性”命令。在弹出的“属性”对话框中单击“高级”按钮，打开“高级属性”对话框；在“压缩或加密属性”区域中取消选择“加密内容以便保护数据”，然后单击“确定”按钮。

③ 如果是文件夹操作，那么在弹出的“确认属性更改”对话框中选择是对文件夹及其所有内容进行解密，还是只解密文件夹本身，默认是对文件夹进行解密。最后单击“确定”按钮即可。

（3）使用加密文件或文件夹

作为当初加密一个文件的用户（即所有者），无须特定的解密操作就能使用它，EFS 会在后台透明地为用户执行解密任务。用户可正常地打开、编辑、复制和重命名。然而，如果用户不是加密文件的创建者或不具备一定的访问权限，则在试图访问文件时将会看到一条访问被拒绝的消息。

提示：如果一个文件夹的属性设置为“加密”，则指出文件夹中所有文件在创建时将进行加密；子文件夹在被创建时也将被标记为“加密”。

（4）复制或移动加密文件或文件夹

与文件的压缩属性相似，在 Windows Server 2016 操作系统的同一卷内移动文件或文件夹时，文件或文件夹的加密属性不会发生任何变化；在 NTFS 不同卷间移动 NTFS 文件或文件夹时，系统将目标文件作为新文件对待，文件将继承目的地文件夹的加密属性。另外，任何已经加密的 NTFS 文件移动或复制到 FAT/FAT32 分区时，文件将会丢失加密属性。最后，对用户在使用 EFS 加密文件（文件夹）时，应注意以下事项：

- 不要加密系统文件夹。
- 不要加密临时目录。
- 应该始终加密个人文件夹。
- 使用 EFS 后应尽量避免重新安装系统，重新安装前应先将文件解密。
- 加密文件系统不对传输过程加密。

实　训　3

1. 实训目的

熟练掌握 Windows Server 2016 NTFS 文件系统的管理。

2. 实训环境

正常的局域网络；安装 Windows Server 2016 操作系统的计算机。

3. 实训内容

（1）在 Windows Server 2016 系统中增加用户 userA 和 userB，并创建工作文件夹 A 和 B。

（2）设置权限，使用户 userB 在对文件夹 A 有完全控制权限的情况下，文件夹 A 中的文件却不能被 userB 读取。

（3）修改某个指定文件或文件夹的特殊权限。

（4）设置使一个文件或文件夹不能继承父文件夹的权限属性。

（5）实现对某个文件或文件夹的加密和解密。

（6）将压缩过的文件和加密过的文件移动到其他的 NTFS 分区，观察其压缩和加密属性的变化情况。

习　题　3

1. 填空题

（1）文件系统是操作系统在_____按照一定原则组织、管理数据所用的结构和机制。

（2）FAT 文件系统最初用于_____的简单文件系统。

（3）_____是 Windows Server 2016 推荐使用的高性能的文件系统，支持许多新的文件安全、存储和容错功能。

（4）NTFS 文件系统最为重要的就是，它是一个基于_____的文件管理系统，是建立在保护文件和目录数据基础上，同时兼顾节省存储资源、减少磁盘占用量的一种先进的文件系统。

（5）Windows Server 2016 的 NTFS 许可权限包括了_____和特殊权限。

（6）只有_____组内的成员、文件和文件夹的所有者、具备完全控制权限的用户，才有权更改这个文件或文件夹的 NTFS 权限。

（7）共享权限有三种：读取、更改和_____。

2. 简答题

（1）Windows Server 2016 NTFS 文件系统的主要特性有哪些？

（2）NTFS 权限的含义是什么？NTFS 权限的应用规则包括哪些？

（3）试述 NTFS 权限与共享权限对文件有何影响。

（4）Windows Server 2016 系统中，对已压缩或加密操作的文件，在同一分区或不同分区之间进行复制、移动操作时，会产生什么结果呢？