项目 3　文件系统管理

项目描述：某公司创建了自己的文件服务器，内有公司最新的设备资料、考勤状况、行政文件和各部门资料等。在使用过程中发现有以下需求：管理员需对所有文件夹拥有完全控制权；普通员工对共享文件夹只拥有读取权限；每位员工只对自己的文件夹拥有完全控制权，且不能读取其他员工的文件夹；每位员工所能使用的磁盘空间有一定的限制；每位员工希望能保存尽量多的数据。

项目目标：为了有效地在 Windows 2019 中进行文件系统管理，必须掌握 NTFS 的概念和应用。利用 NTFS 权限，管理员对使用共享数据的用户进行控制访问。利用文件夹的压缩功能，有效扩大磁盘的使用空间。利用加密文件系统加密文件数据，增强文件数据的安全性。

任务 1　安全权限管理

任务描述：在网络中会有很多资源，例如操作系统、文件、目录和打印机等各种网络共享资源以及其他资源对象。在 Windows Server 2019 操作系统中，管理员可以灵活地控制特定的用户、组使用特定的资源，这样才能避免非授权的访问，并提供一个安全的网络环境。

任务目标：通过学习，读者应掌握资源对象访问控制的基本概念，以及文件和目录等资源对象的访问控制的操作技能。

3.1.1　Windows Server 2019 文件系统简介

文件系统是操作系统在硬盘上命名、存储和组织文件的方法，是在硬盘上存储信息的格式，在所有的计算机系统中都存在一个相应的文件系统，它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。用户对所有的文件和文件夹的操作都是通过文件系统来完成的。

Windows Server 2019 操作系统支持 FAT、FAT32、NTFS、ReFS、exFAT 等文件系统。FAT 和 FAT32 文件系统提供了与其他系统的兼容性，使 Windows Server 2019 的计算机可安装多个操作系统，支持多引导功能；NTFS 文件系统是微软公司基于 Windows NT 内核操作系统特有的文件系统格式，它提供了多种特有的功能；ReFS 是为了保持较高的稳定性，可以自动验证数据是否损坏，并尽力恢复数据；exFAT 适用于闪存的文件系统，为了解决 FAT32 等不支持 4GB 及其更大的文件而推出；CDFS 是适用于光盘存储的文件系统。

1. FAT 文件系统

FAT(file allocation table,文件分配表)也称 FAT16,用于跟踪硬盘上每个文件的数据库,而 FAT 表存储关于簇的信息,这样以后就可以检索文件了。FAT 文件系统可以在所有版本 Windows、MS-DOS 或 OS/2 等众多操作系统上被正确识别。

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。为了保护卷,使用了两份备份。另外,为确保正确装卸启动系统所必需的文件,文件分配表和根文件必须存放在固定的位置。

采用 FAT 文件系统格式化的卷以簇的形式进行分配,支持最大簇数为 65536。默认的簇大小由卷的大小决定。对于 511MB 的卷,其簇大小为 8KB。由于额外开销的原因,在大于 511MB 的卷中不推荐使用 FAT 文件系统。

2. FAT32 文件系统

FAT32(增强的文件分配表)文件系统提供了比 FAT 文件系统更为先进的文件管理特性,通过使用更小的簇来更有效率地使用磁盘空间,可以在大到 2TB 的驱动器上使用。

FAT32 是在大型磁盘驱动器(超过 512MB)上存储文件的极有效的系统,如果用户的驱动器使用了这种格式,则会在驱动器上创建多至几百兆的额外硬盘空间,从而更有效地存储数据。此外,可使程序运行加快,而使用的计算机系统资源却更少。

FAT 和 FAT32 可以与 Windows Server 2019 之外的其他操作系统兼容。如果设置了双重启动配置,很有可能需要 FAT 或 FAT32 文件系统。如果用户正在对 Windows Server 2019 和另外一个操作系统进行双重启动配置,请选择一个适用于后者的文件系统。选择的标准如下。

(1) 如果安装分区小于 2GB,或者如果希望双重启动配置 Windows Server 2019 和 Windows 98 等较早版本,将安装分区格式化为 FAT。

(2) 在大于或等于 2GB 的分区上使用 FAT32 文件系统。在 Windows Server 2019 安装程序中选择使用 FAT 格式化,且分区大于 2GB,安装程序将自动按 FAT32 格式化。

(3) 对于大于 32GB 的分区,建议使用 NTFS 而不用 FAT32 文件系统。

3. NTFS 文件系统

NTFS(new technology file system,新技术文件系统)是 Windows NT 操作环境和 Windows NT 高级服务器网络操作系统环境的文件系统,只有运行基于 NT 内核的操作系统才可以存取 NTFS 卷中的文件。NTFS 文件系统提供了 FAT 和 FAT32 文件系统所没有的、全面的性能,可靠性和兼容性,支持文件和文件夹级的访问控制(权限),可限制用户对文件或文件夹的访问,审计文件的安全;支持文件压缩和文件加密功能,可节省磁盘空间和保护数据安全;支持磁盘配额功能。

NTFS 文件系统的设计目标就是用来在很大的硬盘上能够很快地执行诸如读、写和搜索这样的标准文件操作,甚至包括像文件系统恢复这样的高级操作。

NTFS 文件系统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。除了可以赋予 Windows Server 2019 计算机中的共享文件夹特定权限外，NTFS 文件和文件夹无论共享与否都可以赋予权限。NTFS 是允许为单个文件指定权限。

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。

Windows Server 2019 包括一个新版本的 NTFS，具有以下的功能和优点。

(1) 更好的伸缩性使扩展为大驱动器成为可能：NTFS 中最大驱动器的尺寸远远大于 FAT，而且 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。

(2) 活动目录：使网络管理者和网络用户可以方便灵活地查看和控制网络资源。域控制器和活动目录需要使用 NTFS。

(3) 压缩功能：包括压缩或解压缩驱动器、文件或者特定文件的功能。

(4) 文件加密：能够大幅提高信息的安全性。

(5) 文件级权限：可以对单个文件而不仅对文件夹设置权限。

(6) 远程存储：通过使可移动媒体(如磁带)更易访问，从而扩展了磁盘空间。

(7) 稀疏文件：稀疏文件是一些大型文件，应用程序以一种仅需有限磁盘空间的方式创建了这些文件。也就是说，NTFS 只为文件的写入部分分配磁盘空间。

(8) 磁盘配额：管理者可以管理和控制每个用户所能使用的最大磁盘空间。

(9) 磁盘活动的恢复日志：它将帮助用户在电源失效或其他系统故障时快速恢复信息。

(10) 重析点：是新型文件系统对象。重析点具有一个用户控制数据的可定义属性，且在输入输出(I/O)子系统中用于扩展功能。

(11) 改动日志：NTFS 使用改动日志以跟踪有关添加、删除和改动文件的信息。

(12) 分布式链接跟踪：Windows Server 2019 提供了分布式链接跟踪服务技术，这使客户应用程序可以跟踪在局部域内被移动或在一个域中移动的链接源。

4. ReFS 文件系统

ReFS 文件系统是微软公司的最新文件系统，可最大程度提升数据可用性、跨各种工作负载高效扩展到大数据集，并通过损坏复原提供数据完整性。ReFS 引入了复原功能，可以准确地检测到损坏并且还能够在保持联机状态的同时修复这些损坏，从而有助于增加数据的完整性和可用性。

(1) 完整性流。ReFS 将校验和用于元数据和文件数据(可选)，这使 ReFS 能够可靠地检测到损坏。

(2) 存储空间集成。在与镜像或奇偶校验空间配合使用时，ReFS 可使用存储空间提供的备用数据副本自动修复检测到的损坏。修复过程将本地化到损坏区域且联机执行，并且不会出现卷停机时间。

(3) 挽救数据。如果某个卷损坏并且损坏数据的备用副本不存在，则 ReFS 将从命名空间中删除损坏的数据。ReFS 在处理大多数不可更正的损坏时，可将卷保持在联机状态，但在极少数情况下将卷保持在脱机状态。

(4) 主动纠错。除了在读取和写入前对数据进行验证之外，ReFS 还引入了称为“清理

器”的数据完整性扫描仪。此清理器会定期扫描卷，从而识别潜在损坏，然后主动触发损坏数据的修复。

除了提供复原能力改进外，ReFS 还针对性能极其敏感和虚拟化的工作负载引入新功能。实时层优化、块克隆和稀疏 VDL 都是不断发展的 ReFS 功能，它们专为支持各种动态工作负载而设计。

- 镜像加速奇偶校验：镜像加速奇偶校验为数据提供高性能和容量高效的存储。
- 加快 VM 操作：ReFS 引入了为改善虚拟化工作负载的性能而专门设计了块克隆和稀疏 VDL 功能。块克隆可加快复制操作的速度，并且能够实现快速、低影响的 VM 检查点合并操作。稀疏 VDL 允许 ReFS 文件快速清零，从而将创建固定 VHD 所需的时间从几十分钟减少到仅仅几秒钟。
- 可变簇大小：ReFS 支持 4KB 和 64KB 的簇大小，4KB 是针对大多数部署的簇大小，64KB 簇适合于大型的、顺序输入/输出的工作负载。ReFS 不再支持 NTFS 的命名流、对象 ID、短名称、压缩、EFS、用户数据事务、稀疏、硬链接、扩展属性和配额等功能。目前，ReFS 不能用于启动分区，也不支持可移动存储。

5. exFAT 文件系统

exFAT(extended file allocation table，扩展文件分配表)是 Windows Embeded 5.0 以上引入的一种适合于闪存的文件系统，为了解决 FAT32 等不支持 4GB 及其更大的文件而推出。对于闪存，NTFS 文件系统不适合使用，exFAT 更为适用。对于磁盘则不太适用。

6. 将 FAT32 转换为 NTFS 文件系统

与早期的某些 Windows 版本中使用的 FAT 文件系统相比，NTFS 文件系统为硬盘和分区或卷上的数据提供的性能更好、安全性更高。如果有分区使用早期的 FAT16 或 FAT32 文件系统，则可以使用 convert 命令将其转换为 NTFS。转换为 NTFS 不会影响分区上的数据。具体步骤如下。

步骤 1：关闭要转换的分区或逻辑驱动器上所有正在运行的程序。

步骤 2：在 Windows 运行文本框中输入 cmd 命令，单击“确定”按钮。

步骤 3：在命令提示符窗口中，输入 convert *volume* /FS:ntfs，然后按 Enter 键。

步骤 4：输入要转换的卷的名称，然后按 Enter 键。

注意：将分区转换为 NTFS 后，无法再将其转换回来。如果要在该分区上重新使用 FAT 文件系统，则需要重新格式化该分区，这样会删除其上的所有数据。

3.1.2　文件权限

权限是指与计算机上或网络上的对象(如文件和文件夹)关联的规则。权限确定是否可以访问某个对象以及可以对它执行哪些操作。例如，用户可能有访问网络上共享文件夹中文档的权限，但是只能读取该文档而不能对其进行更改。系统管理员可以为个用户和组分配权限。

在 Windows Server 2019 中，文件权限只能适用于 NTFS、ReFS 磁盘分区，不能用于由

FAT 或者 FAT32 文件系统格式化的磁盘分区。

对于 NTFS、ReFS 磁盘分区上的每一个文件和文件夹，存储一个远程访问控制列表（ACL）。ACL 中包含那些被授权访问该文件或者文件夹的所有用户的帐户、组和计算机，还包含被授予的访问类型。针对相应的用户帐户、组或者该用户所属的计算机，ACL 中必须包含一个对应的元素，这样的元素叫作访问控制元素（ACE）。为了让用户能够访问文件或者文件夹，访问控制元素必须具有用户所请求的访问类型。如果 ACL 中没有相应的 ACE 存在，Windows Server 2019 就拒绝该用户访问相应的资源。

1. 标准权限

利用文件权限可以控制用户对特定的文件和文件夹进行访问和修改，Windows Server 2008 提供读、读和运行、写、修改、列出文件夹内容和完全控制 6 种标准的文件权限。

（1）读取：可以读取文件或文件夹的内容，查看文件或文件夹的属性，但不修改文件内容。

（2）读取和执行：包含读取能够执行的所有操作，并能运行应用程序和可执行文件。

（3）写入：包含读取和执行的所有操作，可修改文件或文件夹属性和内容，在文件夹中创建文件和文件夹，但不能删除文件。

（4）修改：包含写权限能够执行的所有操作，可以删除文件。

（5）列出文件夹内容：仅对文件夹有此权限，查看此文件夹中的文件和子文件夹的属性和权限，读取文件夹中的文件内容。

（6）完全控制：对文件的最高权力，除在拥有上述其他所有的权限外，还可以修改文件权限以及替换文件所有者。

（7）特殊权限：是对文件或文件夹权限更为详细的设置。

2. 特殊权限

（1）完全控制。对文件的最高权力，在拥有上述其他权限的所有权限以外，还可以修改文件权限以及替换文件所有者。

（2）遍历文件夹/执行文件。“遍历文件夹”可以让用户即使在无权访问某个文件夹的情况下，仍然可以切换到该文件夹内。这个权限设置只适用于文件夹，不适用于文件。只有当组或用户在“组策略”中没有赋予“绕过遍历检查”用户权力时，对文件夹的遍历才会生效。默认情况下，Everyone 组具有“绕过遍历检查”的用户权力，所以此处的“遍历文件夹”权限设置不起作用。“执行文件”让用户可以运行程序文件，该权限设置只适用于文件，不适用于文件夹。

（3）列出文件夹/读取数据。“列出文件夹”让用户可以查看该文件夹内的文件名称与子文件夹的名称。“读取数据”让用户可以查看文件内的数据。

（4）读取属性。该权限让用户可以查看文件夹或文件的属性，例如只读、隐藏等属性。

（5）读取扩展属性。该权限让用户可以查看文件夹或文件的扩展属性。扩展属性是由应用程序自行定义的，不同的应用程序可能有不同的设置。

（6）创建文件/写入数据。“创建文件”让用户可以在文件夹内创建文件；“写入数据”让用户能够更改文件内的数据。

(7) 创建文件夹/附加数据。“创建文件夹”让用户可以在文件夹内创建子文件夹；“附加数据”让用户可以在文件的后面添加数据，但是无法更改、删除、覆盖原有的数据。

(8) 写入属性。该权限让用户可以更改文件夹或文件的属性，例如只读、隐藏等属性。

(9) 写入扩展属性。该权限让用户可以更改文件夹或文件的扩展属性。扩展属性是由应用程序自行定义的，不同的应用程序可能有不同的设置。

(10) 删除子文件夹及文件。该权限让用户可以删除该文件夹内的子文件夹与文件，即使用户对这个子文件夹或文件没有“删除”的权限，也可以将其删除。

(11) 删除。该权限让用户可以删除该文件夹与文件。即使用户对该文件夹或文件没有“删除”的权限，但是只要他对其父文件夹具有“删除子文件夹及文件”的权限，他还是可以删除该文件夹或文件。

(12) 读取权限。该权限让用户可以读取文件夹或文件的权限设置。

(13) 更改权限。该权限让用户可以更改文件夹或文件的权限设置。

(14) 取得所有权。该权限让用户可以夺取文件夹或文件的所有权。文件夹或文件的所有者，无论该文件夹或文件权限是什么，他永远具有更改该文件夹或文件权限的能力。

注意：尽管“列出文件夹内容”和“读取及执行”看起来有相同的特殊权限，但是这些权限在继承时却有所不同。“列出文件夹内容”可以被文件夹继承而不能被文件继承，并且它只在查看文件夹权限时才会显示。“读取及执行”可以被文件和文件夹继承，并且在查看文件和文件夹权限时始终出现。

3.1.3　文件权限的有效性

由于文件权限只能在特定分区设置，且可以分别给用户和组指派文件权限，再者要涉及文件和文件夹两种资源，因此针对某一资源的最终权限需要仔细考虑。

1. 资源权限发生重叠时

(1) 权限的累加性。用户对某个资源的有效权限是所有权限的来源的总和。假设现在 zhang 用户既属于 A 用户组，也属于 B 用户组，它在 A 用户组的权限是“读取”，在 B 用户组中的权限是“写入”，那么根据累加原则，zhang 用户的实际权限将会是“读取+写入”两种。

(2) “拒绝”权限会覆盖所有其他权限。虽然用户的有效权限是所有权限的来源的总和。但是只要其中有个权限是被设为拒绝访问，则用户最后的有效权限将是无法访问此资源。例如，zhang 这个用户既属于 zhangs 用户组，也属于 wangs 用户组，当对 wangs 组中某个资源进行“写入”权限的集中分配(即针对用户组进行)时，这个时候该组中 zhang 帐户将自动拥有“写入”的权限。而在 zhangs 组中同样也对 zhang 用户进行了针对这个资源的权限设置，但设置的权限是“拒绝写入”。基于“拒绝优于允许”的原则，zhang 在 zhangs 组中被“拒绝写入”的权限将优先 wangs 组中被赋予的允许“写入”权限被执行。因此，在实际操作中，zhang 用户无法对这个资源进行“写入”操作。

(3) 文件会覆盖文件夹的权限。如果针对某个文件夹设置了权限，同时也对该文件夹内的文件设置了权限。则以文件的权限设置为优先。以 C:\test\readme.txt 为例来说明，若用户 A 对 C:\test 文件夹不具有任何的权限，但是却对其中的 readme.txt 文件具有“读

取”的权限，则仍然可以读取该文件。

（4）权限继承性原则。权限继承性原则是指下级文件夹或文件可以继承父级的权限。假设现在有个 DOC 目录，在这个目录中有 DOC01、DOC02、DOC03 等子目录，现在需要对 DOC 目录及其下的子目录均设置 shyzhong 用户有“写入”权限。因为有继承性原则，所以只需对 DOC 目录设置 shyzhong 用户有“写入”权限，其下的所有子目录将自动继承这个权限的设置。

2. 资源复制或移动时权限的变化与处理

在权限的应用中，不可避免地会遇到设置了权限后的资源需要复制或移动的情况，那么这个时候资源相应的权限会发生怎样的变化呢？

（1）复制资源时。在复制资源时，原资源的权限不会发生变化，而新生成的资源将继承其目标位置父级资源的权限。

（2）移动资源时。在移动资源时，一般会遇到两种情况：一是如果资源的移动发生在同一驱动器内，那么对象保留本身原有的权限不变（包括资源本身权限及原先从父级资源中继承的权限）；二是如果资源的移动发生在不同的驱动器之间，那么不仅对象本身的权限会丢失，而且原先从父级资源中继承的权限也会被从目标位置的父级资源继承的权限所替代。实际上，移动操作就是首先进行资源的复制，然后从原有位置删除资源的操作。

（3）非 NTFS、ReFS 分区。如果将资源复制或移动到非 NTFS、ReFS 分区（如 FAT16/FAT32 分区）上，那么所有的权限均会自动全部丢失。

3.1.4 设置文件权限

将某个磁盘格式化为 NTFS 或 ReFS 后，系统默认的权限设置为 Everyone 的权限都是完全控制，为了该磁盘内的文件与文件夹的安全性，应该改变这个默认值，也就是重新改变用户的访问权限。

1. 查看文件权限

如果用户需要查看文件或文件夹的属性，具体方法如下。

步骤 1：在文件资源管理器中，右击选定的文件或文件夹，在弹出的快捷菜单中选择“属性”命令。

步骤 2：在打开的文件或文件夹的属性对话框中单击“安全”选项卡，如图 3-1 所示，在“组或用户名”列表框中列出了对选定的文件或文件夹具有访问许可权限的组和用户。当选定某个组或用户后，该组或用户所具有的各种权限将显示在权限列表框中。

2. 修改文件权限

当用户需要修改文件或文件夹的权限的时候，必须具有对它的更改权限或拥有权。具体方法如下。

步骤 1：打开图 3-1 所示的文件或文件夹的属性对话框，在“安全”选项卡中单击“编辑”按钮，打开权限设置对话框。

步骤 2：在如图 3-2 所示的对话框中，可以在“组或用户名”列表中选择要设置的用户和组，然后在下面的权限列表中简单地选中相关权限后的复选框即可。

图 3-1　查看文件权限

图 3-2　修改文件权限

步骤 3：如果要修改文件或文件夹的“特殊权限”，单击如图 3-1 所示属性对话框“安全”选项卡中的“高级”按钮，将打开如图 3-3 所示的高级安全设置对话框，在此可以看查该文件或文件夹的所有者、文件权限、审核权限、共享权限（若是共享文件夹）及最终有效访问权限等。

图 3-3　查看高级安全设置

步骤 4：选择“权限”选项卡，单击“添加”按钮，打开如图 3-4 所示的对话框。

图 3-4　修改高级权限

步骤 5：单击图 3-4 所示的对话框中的“选择主体”链接，在出现的“选择用户和组”对话框中输入或选择用户后，单击“确定”按钮。然后图 3-4 将变为相应用户的对话框，在此就可以选中基本权限；也可以单击右侧的“显示高级权限”链接，将显示如图 3-5 所示的高级权限，在此选中相应选项后，单击“确定”按钮即可。

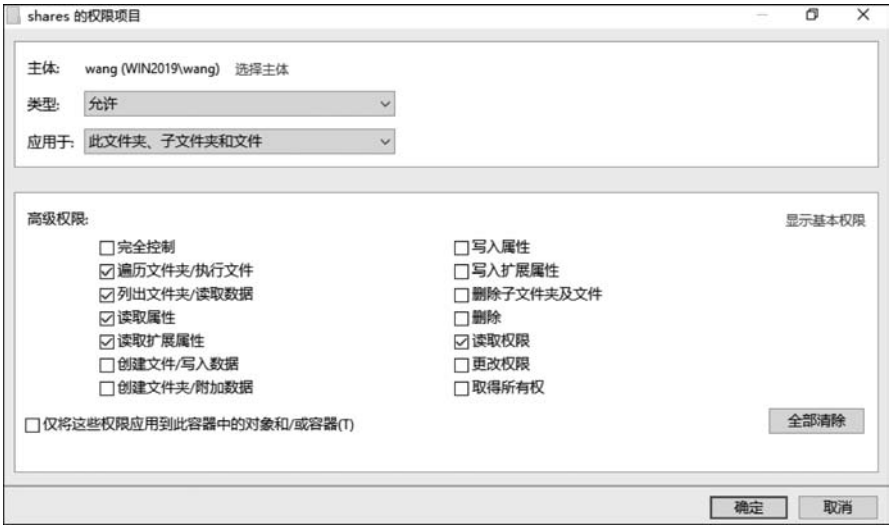

图 3-5　修改特殊权限

3. 取消继承权限

如果不希望继承父项的权限，可以阻断上下目录的继承关系，例如不希望“C:\试题”内的“A 卷”文件继承父项(C:\试题)权限，可执行如下步骤。

步骤 1：打开 A 卷文件的安全属性对话框，如图 3-6 所示，灰色对钩表示这些权限是继承下来的。

步骤 2：单击“高级”按钮，打开如图 3-3 所示的高级安全设置对话框，然后单击“禁用继承”按钮，弹出如图 3-7 所示的提示对话框。如果单击“将已继承的权限转换为此对象的显式权限。”链接，将保留原来从父项对象所继承来的权限；如果单击“从此对象中删除所有已继承的权限。”链接，将清除原来从父项对象所继承的权限。

图 3-6　安全属性

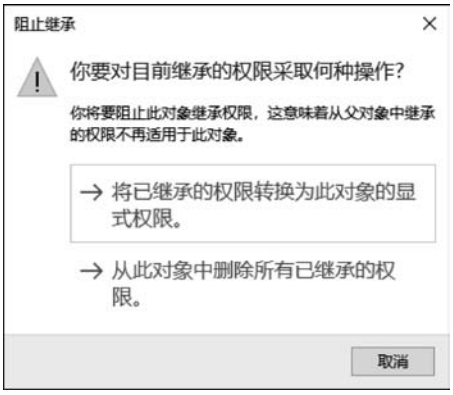

图 3-7　保留或删除继承权限

4. 取得所有权

很多用户都有过这样的经验：在计算机中病毒之后，当用户试图删除某个文件(夹)时，系统会提示磁盘空间不足或该文件拒绝访问，不能删除此文件，这是由于病毒程序对此文件(夹)设置了访问权限。所以用户在系统中试图删除文件夹时由于没有相应的权限，就会被拒绝访问。此时，只要用户夺回这个文件(夹)的控制权，那么就可以删除它了。但是当打开文件(夹)的属性对话框中的“高级”选项卡，却发现所有内容都是灰色的，无法做任何设置，这是因为文件的所有权不属于当前用户。

每个文件与文件夹都有其“所有者”，系统默认是建立文件或文件夹的用户，就是该文件或文件夹的所有者，所有者永远具有更改该文件或文件夹的权限能力。文件或文件夹的所有者是可以转移的，不过不是由所有者来执行转移的，而是由其他用户自行来夺取所有权实现转移的。Windows 的文件转移者必须具有以下权限。

(1) 拥有“取得所有权”的特殊权限。

(2) 具有“更改权限”的特殊权限。

(3) 拥有“完全控制”的标准权限。

(4) 任何一位具有 Administrator 权限的用户，无论对该文件或文件夹拥有哪种权限，