

# Windows 文件管理高级手册

我们之前介绍的文件和文件夹的管理和操作都是基于文件系统来实现的，是文件系统中文件管理的一些基础操作。Windows 10 支持多种类型的文件系统，我们本章主要学习 Windows 10 的基于文件系统的高级管理操作。

## X.1 文件系统简介

文件系统是操作系统用于明确存储设备（常见的是磁盘，也有基于 NAND Flash 的固态硬盘）或分区上的文件的方法和数据结构；即在存储设备上组织文件的方法。操作系统中负责管理和存储文件信息的软件机构称为文件管理系统，简称文件系统。文件系统由三部分组成：文件系统的接口，对对象操纵和管理的软件集合，对象及属性。从系统角度来看，文件系统是对文件存储设备的空间进行组织和分配，负责文件存储并对存入的文件进行保护和检索的系统。具体地说，它负责为用户建立文件，存入、读出、修改、转储文件，控制文件的存取，当用户不再使用时撤销文件等。下面介绍几种在 Windows 操作系统中常用的文件系统。

### FAT 文件系统

FAT 是 File Allocation Table 的简称，是微软在 Dos/Windows 系列操作系统中共使用的一种文件系统的总称。它几乎被所有的操作系统所支持。

FAT 文件系统又分为 3 种，分别是 FAT16、FAT32 和不太常见的 FAT12。

- **FAT12:**

这是伴随着 Dos 诞生的“老”文件系统了。它采用 12 位文件分配表，并因此而得名。而以后的 FAT 系统都按照这样的方式在命名。在 DOS3.0 以前使用。但是在现在，我们都还能找得到这个文件系统：用于软盘驱动器。当然，其他地方的确基本上不使用这个文件系统了。Fat12 可以管理的磁盘容量是 8M。这在当时，没有硬盘的情况下，这个磁盘管理能力是非常大的。

- **FAT16:**

在 Dos2.0 的使用过程中，对更大的磁盘的管理能力的需求已经出现了，所以在 Dos3.0 中，微软推出了新的文件系统 Fat16。除了采用了 16 位字长的分区表之外，Fat16 和 Fat12 在其他地方都非常的相似。实际上，随着字长增加 4 位，可以使用的簇的总数增加到了 65536。在总的簇数在 4096 之下的时候，应用的还是 Fat12 的分区表，当实际需要超过 4096 簇的时候，应用的是 Fat16 的分区表。刚推出的 Fat16 文件系统管理磁盘的能力实际上是 32M。这在当时是看来是足够大的。1987 年，硬盘的发展推动了文件系统的发展，Dos4.0 之后的 Fat16 可以管理 128M 的磁盘。然后这个数字不断的发展，一直到 2G。在整整的 10 年中，2G 的磁盘管理能力都是大大的多于了实际的需要。需要指出的是，在 windows95 系统中，采用了一种比较独特的技术，叫做 VFat 来解决长文件名等问题。

FAT16 分区格式存在严重的缺点：大容量磁盘利用效率低。在微软的 DOS 和 Windows 系列中，磁盘文件的分配以簇为单位，一个簇只分配给一个文件使用，不管这个文件占用整个簇容量的多少。这样，即使一个很小的文件也要占用一个簇，剩余的簇空间便全部闲置，造成磁盘空间的浪费。由于分区表容

量的限制，FAT16 分区创建的越大，磁盘上每个簇的容量也越大，从而造成的浪费也越大。所以，为了解决这个问题，微软推出了一种全新的磁盘分区格式 FAT32，并在 Windows 95 OSR2 及以后的 Windows 版本中提供支持。

● **FAT32:**

Fat32 文件系统将是 Fat 系列文件系统的最后一个产品。和它的前辈一样，这种格式采用 32 位的文件分配表，磁盘的管理能力大大增强，突破了 FAT16 2GB 的分区容量的限制。由于现在的硬盘生产成本下降，其容量越来越大，运用 FAT32 的分区格式后，我们可以将一个大硬盘定义成一个分区，这大大方便了对磁盘的管理。

FAT32 推出时，主流硬盘空间并不大，所以微软设计在一个不超过 8GB 的分区中，FAT32 分区格式的每个簇都固定为 4KB，与 FAT16 相比，大大减少了磁盘空间的浪费，这就提高了磁盘的利用率。

FAT16 和 FAT32 文件系统的优点是兼容性高，可以被绝大部分操作系统识别和使用。但是由于出现的较早，它们也有很多不足的地方：

单文件最大的尺寸：**FAT32** 系统支持到 **4GB**，**FAT16** 系统只支持到 **2GB**，在现在高清视频逐渐普及的今天，单个视频的文件以及远远超出了 **4GB** 的容量。

FAT16 和 FAT32 文件系统都不支持对文件进行高级管理，比如加密、压缩存储、磁盘配额等功能。

**NTFS 文件系统**

为了解决 FAT16/FAT32 文件系统安全性差、容易产生碎片、难以恢复等缺点，微软在 Windows NT 操作系统和之后的基于 NT 内核的操作系统中使用了新的 NTFS 文件系统。Windows 10 中提供的高级文件管理功能都是基于 NTFS 文件系统来实现的。如图 X-1 所示，这个磁盘使用的就是 NTFS 文件系统。



图 X-1

## NTFS 文件系统结构总览：

当用户将硬盘的一个分区格式化成 NTFS 分区时，就建立了一个 NTFS 文件系统结构。NTFS 文件系统与 FAT 文件系统一样，也是用簇为基本单位对磁盘空间和文件存储进行管理的。一个文件总是占有若干个簇，即使在最后一个簇没有完全放满的情况下，也是占用了整个簇的空间，这也是造成磁盘空间浪费的主要原因。文件系统通过簇来管理磁盘管理，并不需要知道磁盘扇区的大小，这样就使 NTFS 保持了与磁盘扇区大小的独立性，从而使不同大小的磁盘选择合适的簇。

NTFS 分区也被称为 NTFS 卷，卷上簇的大小，又称为卷因子，其大小是用户在创建 NTFS 卷时确定的。和 FAT 文件系统一样，卷因子的大小和文件系统的性能有着非常直接的关系。当一样簇占用的空间太小时，会出现太多的磁盘碎片，这样的空间和文件访问时间上会造成浪费；而相反的当一个簇占用的空间太大时，直接造成了磁盘空间的浪费。因此，最大限度地优化系统对文件的访问速度和最大限度地减少磁盘空间的浪费是确定簇的大小的主要因素。簇的大小一定是扇区大小的整数倍，通常是 2（n 为整数）。

NTFS 文件系统使用了逻辑簇号（LCN）和虚拟簇号（VCN）对卷进行管理。其中 LCN 是对卷的第一个簇到最后一个簇进行编号，只要知道 LCN 号和簇的大小以及 NTFS 卷在物理磁盘中的起始扇区就可以对簇进行定位，而这些信息在 NTFS 卷的引导扇区中可以找到，在系统底层也是用这种方法对文件的簇进行定位的。找到簇在磁盘中的物理位置的计算公式是：

每簇扇区数\*簇号+卷的隐含扇区数（卷之前的扇区总数）=簇的起始绝对扇区号

而虚拟簇号则是将特定文件的簇从头到尾进行编号，这样做的原因是方便系统对文件中的数据进行引用，VCN 并不要求在物理上是连续的，要确定 VCN 的磁盘上的定位需先将其转换为 LCN。

NTFS 文件系统的主文件表中还记录了一些非常重要的系统数据，这些数据被称为元数据文件，简称为“元文件”，其中包括了用于文件定位和恢复数据结构、引导程序数据及整个卷的分配位图等信息。NTFS 文件系统将这些数据都当做文件进行管理，这些文件用户是不能访问的，它们的文件名的第一个字符都是“\$”，表示该文件是隐藏的。在 NTFS 文件系统中这样的文件主要有 16 个，包括 MFT 本身（\$MFT）、MFT 镜像、日志文件、卷文件、属性定义表、根目录、位图文件、引导文件、坏簇文件、安全文件、大写文件、扩展元数据文件、重解析点文件、变更日志文件、配额管理文件、对象 ID 文件等，这 16 个元数据文件总是占据着 MFT 的前 16 项纪录，在 16 项以后就是用户建立的文件和文件夹的记录了。

每个文件记录在主文件表中占据的磁盘空间一般为 1KB，也就是两个扇区，NTFS 文件系统分配给主文件表的区域大约占据了磁盘空间的 12.5%，剩余的磁盘空间用来存放其他元文件和用户的文件。

## NTFS 文件系统具有以下优点：

- 更安全的文件保障，提供文件加密，能够大大提高信息的安全性。
- 更好的磁盘压缩功能。
- 支持最大达 2TB 的大硬盘，并且随着磁盘容量的增大，NTFS 的性能不像 FAT 那样随之降低。
- 可以赋予单个文件和文件夹权限。对同一个文件或者文件夹为不同用户可以指定不同的权限。在 NTFS 文件系统中，可以为单个用户设置权限。
- NTFS 文件系统中设计的恢复能力无需用户在 NTFS 卷中运行磁盘修复程序。在系统崩溃事件中，NTFS 文件系统使用日志文件和复查点信息自动恢复文件系统的一致性。
- NTFS 文件夹的 B-Tree 结构使得用户在访问较大文件夹中的文件时，速度甚至比访问卷中较小的文件夹

中的文件还快。

- 可以在 NTFS 卷中压缩单个文件和文件夹。NTFS 系统的压缩机制可以让用户直接读写压缩文件，而不需要使用解压软件将这些文件展开。
- 支持活动目录和域。此特性可以帮助用户方便灵活地查看和控制网络资源。
- 支持稀疏文件。稀疏文件是应用程序生成的一种特殊文件，文件尺寸非常大，但实际上只需要很少的磁盘空间，也就是说，NTFS 只需要为这种文件实际写入的数据分配磁盘存储空间。
- 支持磁盘配额。磁盘配额可以管理和控制每个用户所能使用的最大磁盘空间。

## exFAT 文件系统

由于 NTFS 系统是针对机械硬盘设计的，对于闪存来说不太实用。为了解决这个问题，出现了 exFAT 文件系统。exFAT（Extended File Allocation Table File System，扩展 FAT，也称作 FAT64，即扩展文件分配表）是 Microsoft 在 Windows Embedded 5.0 以上（包括 Windows CE 5.0、6.0、Windows Mobile 5、6、6.1）中引入的一种适合于闪存的文件系统，为了解决 FAT32 等不支持 4G 及其更大的文件而推出。

相对 FAT 文件系统，exFAT 有如下好处：

- 增强了台式电脑与移动设备的互操作能力
- 单文件大小大大超过了 4GB 的限制。最大可达 16EB
- 簇大小可高达 32MB
- 采用了剩余空间分配表，剩余空间分配性能改进
- 同一目录下最大文件数可达 2,796,202 个
- 支持访问控制
- 支持 Apple MAC 系统

## X.2 转换文件系统

使用 NTFS 文件系统，可以更好的管理磁盘及提高系统的安全性；硬盘为 NTFS 格式时，碎片整理也很快。当我们从旧的系统升级到新系统时，旧的磁盘格式可能为 FAT 格式，这时候我们可以用下面的办法来把它转换成 NTFS 文件系统。

### 通过格式化磁盘转换

如果磁盘中的数据我们不再需要或者我们已经进行过备份，格式化是比较快捷的方式。下面介绍下如何操作。

步骤 1：右键单击要格式化的磁盘，在弹出的快捷菜单中单击“格式化”，如图 X-2 所示。

步骤 2：在弹出的格式化窗口中，点击下拉列表选择 NTFS 格式，然后点击“开始”按钮，如图 X-3 所示，然后等待格式化完成即可。



图 X-2



图 X-3

## 通过 Convert 命令转换

如果我们的磁盘上内容很多，而且不想格式化。那么我们可以使用 Windows 10 自带的 Convert 命令来进行格式的转换。Convert 命令只能将 FAT 格式转换为 NTFS 格式，但是不能反向转换。操作方法如下：

步骤 1：同时按下键盘上的 Win 键和 R 键，在弹出的运行窗口中，输入 cmd，然后回车，如图 X-4 所示。

步骤 2：我们以 I 盘为例，来进行说明。在弹出的窗口中，输入 “Convert I: /fs:ntfs”，然后按下回车键，等待命令完成即可，如图 X-5 所示。

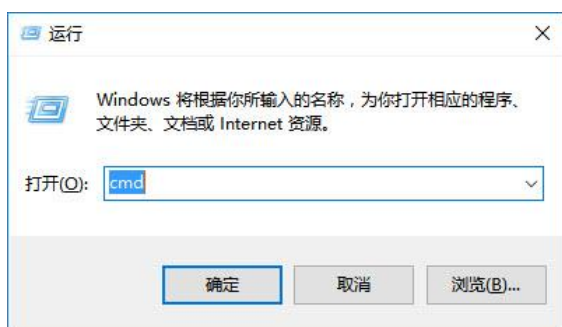


图 X-4

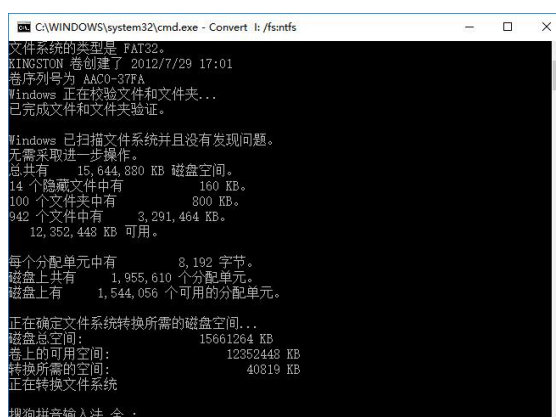


图 X-5

## X.3 设置文件访问权限

如果我们工作中使用的计算机内有比较重要的文件，只能特定的人才可以查看，那么我们应该如何保

护它不被其他用户查看呢。设置对文件的访问权限以及访问级别，可以防止电脑中的其他用户查看或修改重要的文件内容，从而保护电脑中资源。

## 什么是权限

权限是指访问电脑中的文件或文件夹及共享资源的协议。权限确定是否可以访问某个对象，以及对该对象可执行的操作范围。

## NTFS 权限

NTFS 权限就是其实就是访问控制列表的内容。NTFS 分区通过为每个文件和文件夹设定访问控制列表的方法来控制相关的权限。访问控制列表中包括可以访问该文件或文件夹的用户账户，用户组和访问类型。在访问控制列表中，每个用户账户或者用户组都对应一组访问控制项。访问控制项用来存储用户账户或者用户组的访问类型。

当用户访问文件或文件夹时，NTFS 文件系统会首先检查该用户的帐户或者所属的用户组是否存在于此文件或文件夹的访问控制列表中。如果存在列表中，则进一步检查访问类型来确定用户访问权限。如果用户不在访问控制列表中，则直接拒绝用户访问此文件或文件夹。

## Windows 用户帐户和用户组

大部分人提起 Windows 用户账户都会想到登录系统时所需要输入密码的那个用户。Windows 10 中还有许多用于系统管理的帐户，下面逐一为大家说明。

Windows 10 包含 4 种默认的内置用户，如图 X-6 所示。分别如下：

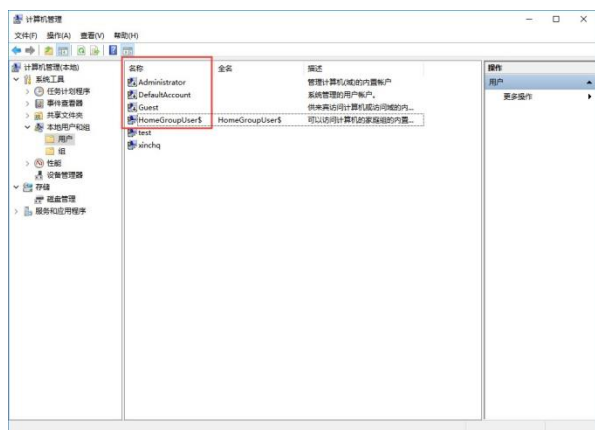


图 X-6

- **Administrator 账户：**超级管理员账户，默认情况下是禁用的。该账户拥有最多的权限，包括以管理员身份运行任何程序，完全控制计算机，访问计算机上的任何数据，已经更改计算机的设置。由于该账户权限过高，如果开启后被其他用户盗用，进行破坏操作后，可能造成系统崩溃，所以不建议启用此账户。
- **DefaultAccount 账户：**系统管理的用户账户，是微软为了防止 OOBE 出现问题准备的。
- **Guest 账户：**来宾账户，适合在公用计算机上为客人准备的账户，此账户受限制较多，不能更改计算机的设置。
- **HomeGroupUser\$ 账户：**家庭组用户账户，用于实现家庭组简化，安全共享的功能。

Windows 10 包含十几种内置的用户组，如图 X-7 所示。我们只介绍最常用到的几种，分别如下：

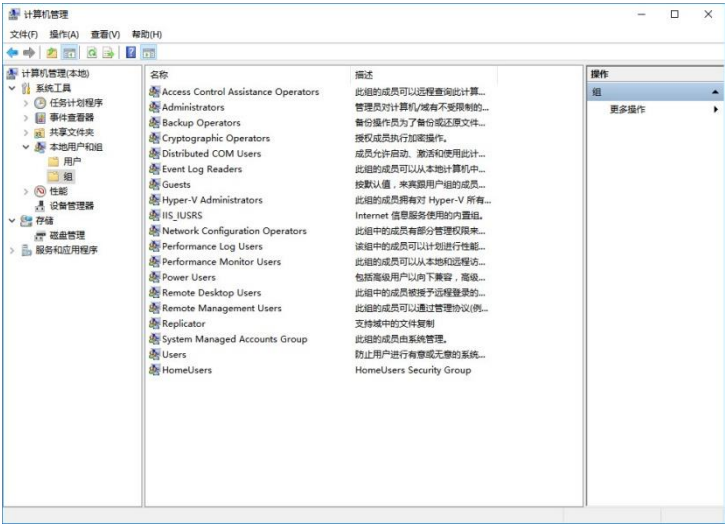


图 X-7

- **Administrators 用户组:** Administrators 组的成员就是系统管理员,如果将用户加入到这个用户组中,用户就会拥有管理员权限。
- **Users 用户组:** 所有的用户账户都属于 Users 组,通常使用 Users 组对用户的权限设置进行分配。
- **Homeusers 用户组:** Homeusers 用户组成员包括所有的家庭组账户。
- **Authenticated 用户组:** 这个用户组包括在计算机或者域中所有通过身份验证的账户,不包括来宾用户。
- **Everyone 用户组:** 所有用户的集合。

## 文件和文件夹的权限

对于 NTFS 分区中的数据,管理员可以为不同的用户账户设置访问权限。NTFS 权限主要分为基本权限和高级权限。

基本权限包括对文件和文件夹的修改、读取和运行、列出文件夹目录、读取、写入等基本操作。

高级权限包括遍历文件夹,运行文件、列出文件夹,读取数据、创建文件,写入数据、创建文件夹,附加数据、读取属性、读取扩展属性、写入属性、删除子文件夹及文件、删除或更改权限、取得所有权等操作。

对于普通用户而言,只需了解基本权限的使用.对于管理员用户,最好详细了解各种高级权限的作用,以便根据实际需要组合出特定的权限分配方案。

### 1.基本权限:

基本权限的内容如图 X-8 所示。





图 X-8

- 完全控制：该权限给予了用户完全控制文件或文件夹的能力，用户可以任意读取，写入或者删除文件夹。
- 修改：该权限允许用户对文件进行修改。
- 读取和执行：该权限允许用户读取文件和执行程序，但不可以进行除此之外的其他操作。如修改，删除等。
- 读取：允许用户查看该文件夹中的文件和子文件夹。
- 写入：该权限允许用户在文件夹中写入新的文件和文件夹。
- 列出文件夹内容：允许用户查看文件夹中的子文件夹和文件名称，但不允许访问文件夹内的文件。

## 2.高级权限：

高级权限的内容如图 X-9 所示。



图 X-9



- 完全控制：和基本权限一致，用户可以随意删除和修改文件。
- 遍历文件夹/执行文件：遍历文件夹允许用户即使没有访问这个文件夹的权限，但是可以移动此文件夹到其他文件夹。执行文件的功能及用户可以运行文件夹内的可执行文件。
- 列出文件夹/读取数据：允许用户查看文件夹中的文件名称，子文件夹名称和查看文件中的数据。
- 读取属性：允许用户读取文件或文件夹的属性。
- 读取扩展属性：允许用户查看文件或文件夹的扩展属性。
- 创建文件/写入数据：允许用户在文件夹内创建新的文件，同时允许用户将数据写入现有文件。
- 创建文件夹/附加数据：允许用户添加新的文件夹，并可以在文件的末尾附加数据，但是不能修改此前已经存在的数据。
- 写入属性：允许用户改变文件或文件夹的属性。
- 写入扩展属性：允许用户改变文件或文件夹的扩展属性
- 删除：允许用户删除此文件夹内的文件和文件夹。
- 读取权限：允许用户读取此文件或文件夹的权限列表。
- 更改权限：允许用户更改文件或文件夹的权限列表。
- 取得所有权：允许用户取得文件和文件夹的所有权。
- 删除子文件夹及文件：允许用户删除文件夹内的子文件夹和文件，但是不能删除该文件夹。

## 权限配置原则

在 Windows 中，针对权限的管理有四项基本原则，即拒绝优于允许原则、权限最小化原则、累加原则和权限继承性原则。这四项基本原则对于权限的设置来说，将会起到非常重要的作用，下面就来了解一下：

### 1.拒绝优于允许原则

“拒绝优于允许”原则是一条非常重要且基础性的原则，它可以非常完美地处理好因用户在用户组的归属方面引起的权限“纠纷”，例如，“test”这个用户既属于“a”用户组，也属于“b”用户组，当我们对“b”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，这个时候该组中的“test”账户将自动拥有“写入”的权限。

但令人奇怪的是，“test”账户明明拥有对这个资源的“写入”权限，为什么实际作中却无法执行呢？原来，在“a”组中同样也对“test”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，“test”在“a”组中被“拒绝写入”的权限将优先于“b”组中被赋予的允许“写入”权限被执行。因此，在实际作中，“test”用户无法对这个资源进行“写入”作。

## 2.权限最小化原则

Windows 将“保持用户最小的权限”作为一个基本原则进行执行，这一点是非常有必要的。这条原则可以确保资源得到最大的安全保障。这条原则可以尽量让用户不能访问或不必要访问的资源得到有效的权限赋予限制。

基于这条原则，在实际的权限赋予作中，我们就必须为资源明确赋予允许或拒绝作的权限。例如系统中新建的受限用户“test”在默认状态下对“DOC”目录是没有任何权限的，现在需要为这个用户赋予对“DOC”目录有“读取”的权限，那么就必须在“DOC”目录的权限列表中为“test”用户添加“读取”权限。

## 3.权限继承性原则

权限继承性原则可以让资源的权限设置变得更加简单。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“test”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“test”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。

## 4.累加原则

这个原则比较好理解，假设现在“test”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，“test”用户的实际权限将会是“读取+写入”两种。

显然，“拒绝优于允许”原则是用于解决权限设置上的冲突问题的；“权限最小化”原则是用于保障资源安全的；“权限继承性”原则是用于“自动化”执行权限设置的；而“累加原则”则是让权限的设置更加灵活多变。几个原则各有所用，缺少哪一项都会给权限的设置带来很多麻烦！

### TIPS

在 Windows 中，“Administrators”组的全部成员都拥有“取得所有者身份”(Take Ownership)的权力，也就是管理员组的成员可以从其他用户手中“夺取”其身份的权力，例如受限用户“test”建立了一个 DOC 目录，并只赋予自己拥有读取权力，这看似周到的权限设置，实际上，“Administrators”组的全部成员将通过“夺取所有权”等方法获得这个权限。

## 获取文件权限

经常看到有人问文件删不掉怎么办，其实 windows 系统中文件删不掉的主要原因有两个：一是文件正在使用中或者已经被打开，二是用户没有权限。对于第一种原因，解决办法就是关闭正在使用或已经打开的文件，之后就可以正常删除了。由于第二种原因导致无法删除的文件或文件夹，我们只要获得此文件（或文件夹）的最高权限即可删除。

下面为大家介绍下具体步骤：

步骤 1：右键单击要删除的文件或文件夹，然后在弹出的快捷菜单中点击“属性”，然后点击“安全”，切

换到安全选项卡，在选项卡内点击“高级”按钮，如图 X-10 所示。

步骤 2：在弹出的对话框中，单击“更改”按钮，如图 X-11 所示。

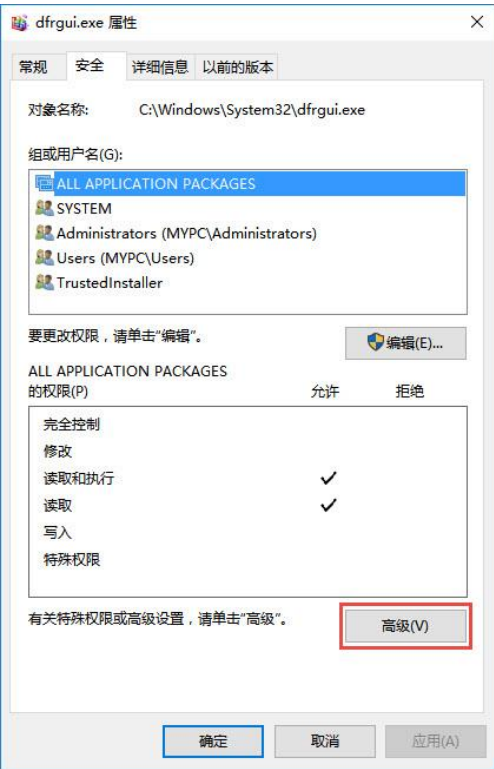


图 X-10

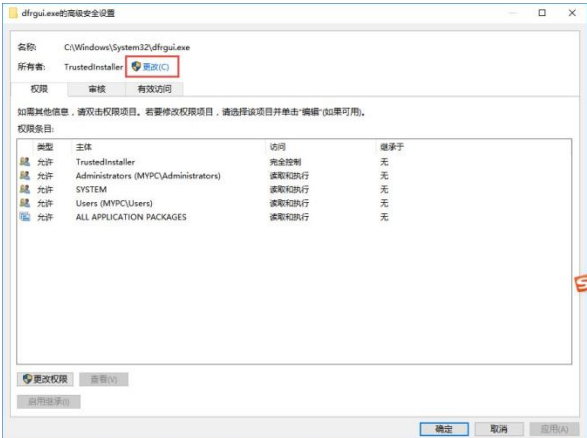


图 X-11

步骤 3：在弹出的对话框中，点击“高级”按钮，如图 X-12 所示。

步骤 4：在弹出的窗口中，点击“立即查找”按钮，在搜索结果内，选择要更换的账户，然后点击“确定”按钮，如图 X-13 所示。

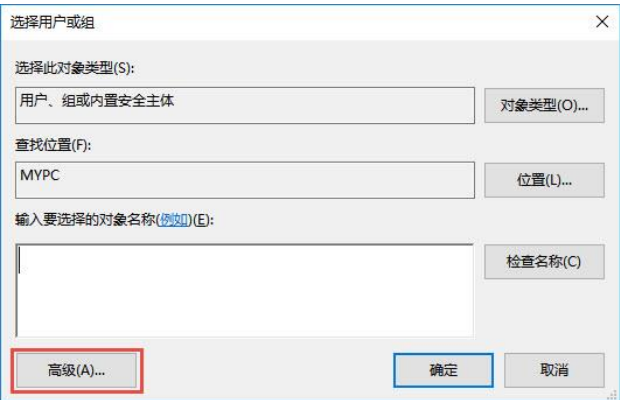


图 X-12

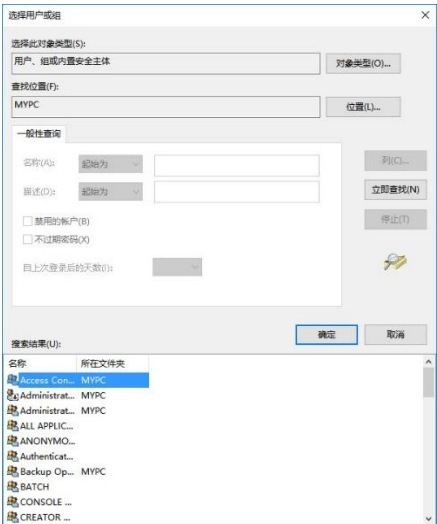


图 X-13

步骤 5：然后在返回的窗口中再次点击“确定”按钮，如图 X-14 所示。

步骤 6: 我们看到文件的所有者已经被更改, 我们点击“确定”按钮, 返回上一步。如图 X-15 所示。



图 X-14

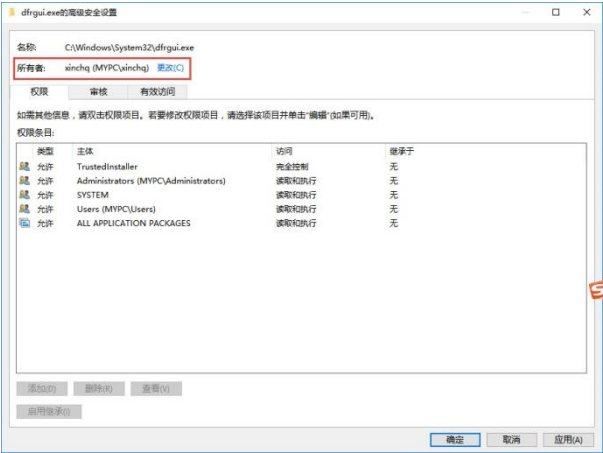


图 X-15

步骤 7: 在返回的窗口中, 点击“编辑”按钮, 为我们添加的用户赋予删除权限, 如图 X-16 所示。  
步骤 8: 在弹出的窗口中, 点击选中要修改权限的账户, 然后, 勾选下方的允许权限, 如图 X-17 所示。

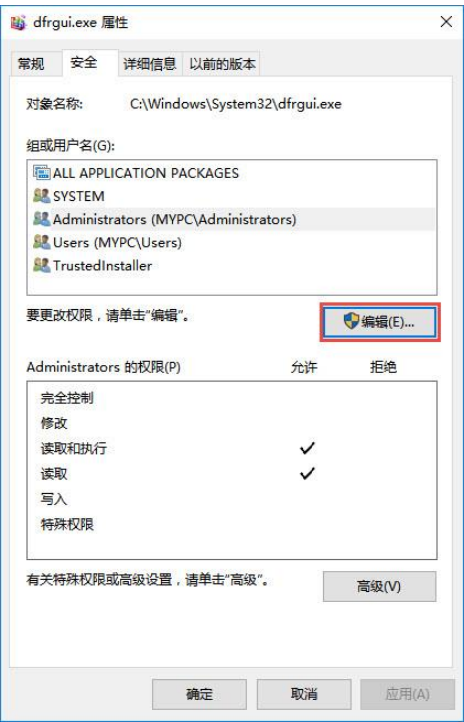


图 X-16

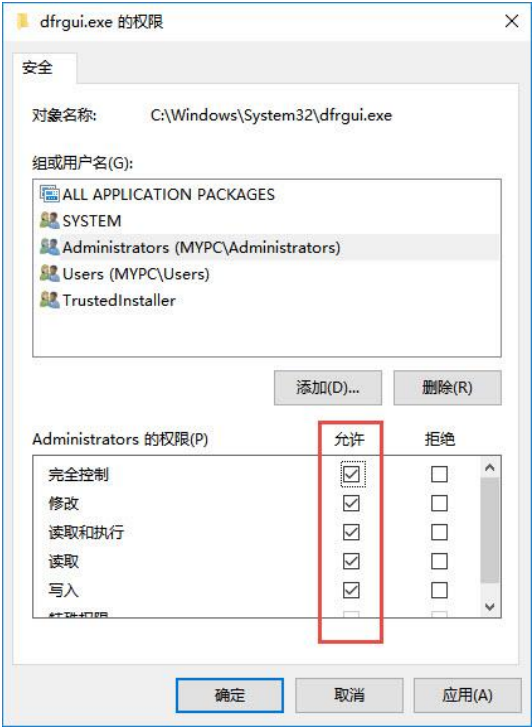


图 X-17

这时候我们已经取得文件的完全控制权, 可以删除文件了。

恢复原有权限配置

有时候 Windows 下的文件夹/文件的权限设置会弄得乱七八糟的, 连自己都不知道哪些文件有特殊权限了, 这时候我们可以通过 Windows 自带的 `icacls` 命令来恢复原有的默认权限设置。以我们刚才修改的文件

的权限为例。

同时按下键盘上的 Win 键和 R 键，然后输入 cmd 并回车，进入命令提示符。然后输入：icacls “c:\Windows\System32\dfrgui.exe” /reset

然后等待系统操作完成即可。如图 X-18 所示。

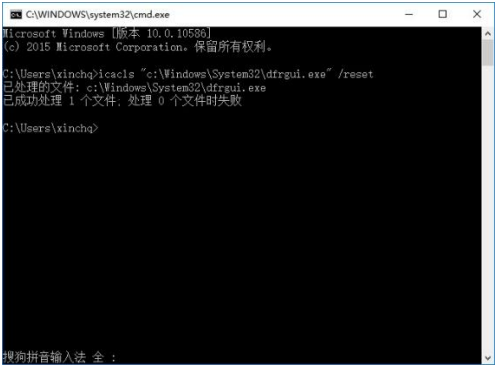


图 X-18

## 设置文件权限

设置对文件的访问权限以及访问级别，可以防止电脑中的其他用户查看或修改重要的文件内容，从而保护电脑中资源。步骤如下：

步骤 1：右键单击要设置权限的文件或文件夹，在弹出的快捷菜单中点击“属性”，然后在弹出的窗口中，点击“安全”选项卡，然后点击“编辑”按钮，如图 X-19 所示。

步骤 2：在弹出的窗口中，选中上方的用户，如果要删除这个用户的权限，则可以点击下方的“删除”按钮，如果我们要添加用户账户，则点击下方的“添加”按钮。如图 X-20 所示。

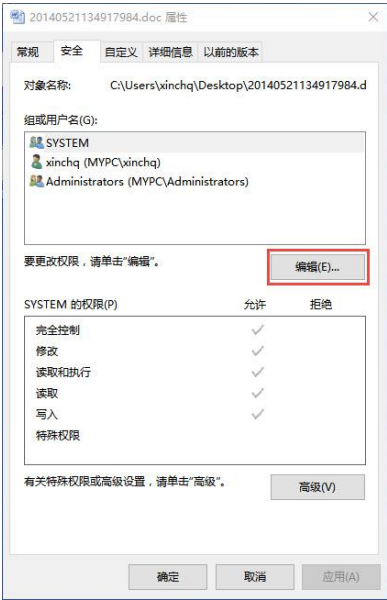


图 X-19

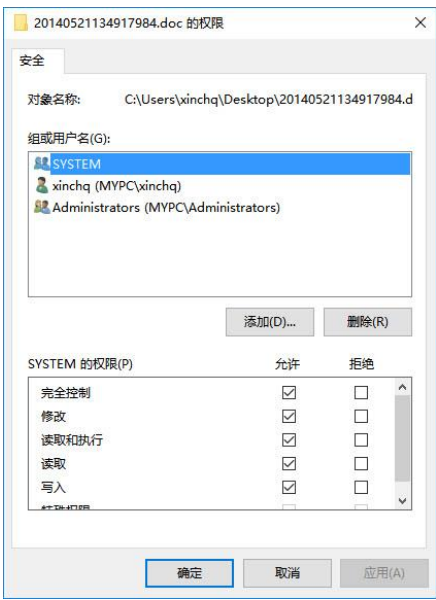


图 X-20

步骤 3：如果我们要添加用户，则可以在点击“添加”按钮弹出的窗口中，添加需要的账户，然后点击确定，然后选择要添加的权限即可。

## 设置文件的高级权限

上节的操作只能添加基本的 6 种权限，如果我们要设置复杂的权限，则可以使用高级权限设置。步骤如下：

**步骤 1:** 在图 X-19 的界面中，点击下方的“高级”按钮，在弹出的窗口中点击“添加”按钮，如图 X-21 所示。

步骤 2: 在弹出的窗口中, 点击“选择主体”, 选择要添加的用户账户, 如图 X-22 所示。

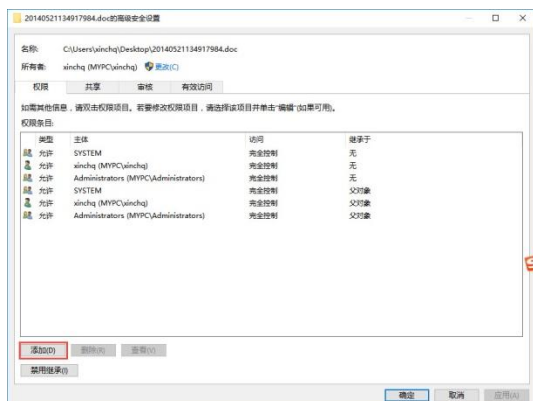


图 X-21

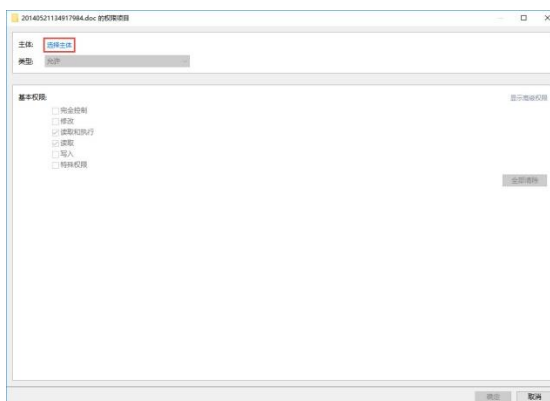


图 X-22

**步骤 3:** 然后点击右侧的“显示高级权限”，如图 X-23 所示。

**步骤 4:** 然后勾选要设置的权限，如图 X-24 所示。

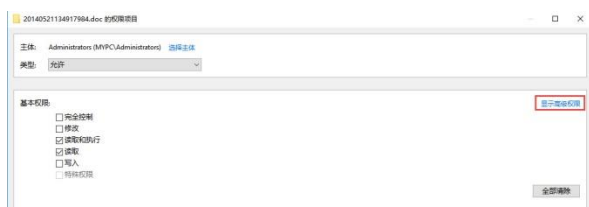


图 X-23

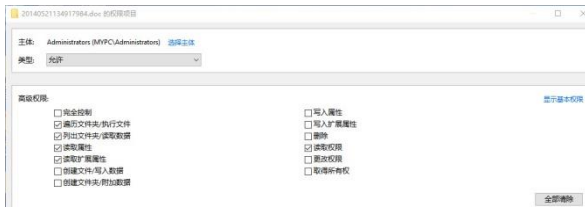


图 X-24

## X.4 使用文件加密功能（文件加密系统 EFS）

对很多电脑用户来说，如何给保存在电脑磁盘中的一些重要文件加密已成为急需了解的常识，由于复杂的电脑使用环境极易引起个人数据的外泄，所以为了防患於未然，每一位电脑用户都应该学会有效保护个人数据。无论是文件或文件夹加密其核心都在于保护个人数据安全，不让其他人未经允许就打开查看，但是要做到这一点我们该如何操作呢？

## 什么是 EFS

Windows 10 系统提供了一种 EFS 加密文件系统来保护用户数据，使用这个加密文件系统可以将文件进行加密然后存储起来。EFS 文件加密系统基于 NTFS 文件系统来进行实现。而且不是所有版本的 Windows 10 提供 EFS 加密功能。只有 Windows 10 专业版和 Windows 10 企业版支持该项功能。

EFS 加密是基于公钥策略的。然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，。如果你登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。

EFS 加密解密都是透明完成，如果用户加密了一些数据，那么其对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问加密过的数据时，就会收到“拒绝访问”的错误提示。

### 1.EFS 加密的优点：

首先，EFS 加密机制和操作系统紧密结合，因此我们不必为了加密数据安装额外的加密软件，这节约了我们的使用成本。

其次，EFS 加密系统对用户是透明的。如果你用 EFS 加密了一些数据，那么你对这些数据的访问将是完全允许的，并不会受到任何限制。而其他非授权用户试图访问 EFS 加密过的数据时，就会收到“访问拒绝”的错误提示。EFS 加密的用户验证过程是在登录 Windows 时进行的，只要登录到 Windows，就可以打开任何一个被授权的加密文件。所以这就是为什么 EFS 加密后的文件夹或文件您看不到加密效果的原因。

### 2.EFS 加密的缺点：

- 如果在重装系统前没有备份加密证书，重装系统后 EFS 加密的文件夹里面的文件将无法打开。
- 如果证书丢失，EFS 加密的文件夹里面的文件也无法打不开。
- 如果系统出现错误，即使有加密证书，EFS 加密的文件夹里面的文件打开后可能会出现乱码的情况。

## 加密与解密文件

下面介绍下如何使用 EFS 对文件进行加密和解密操作。

加密步骤如下：

步骤 1：右键单击要加密的文件或文件夹，在弹出的快捷菜单中点击“属性”，然后在弹出的窗口中点击“高级”按钮，如图 X-25 所示。

步骤 2：在弹出的“高级属性”窗口中，勾选“加密内容以便保护数据”，然后点击确定即可。如图 X-26 所示。

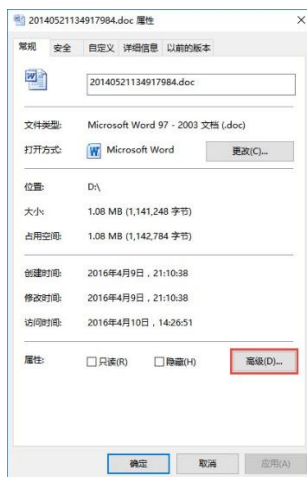


图 X-25

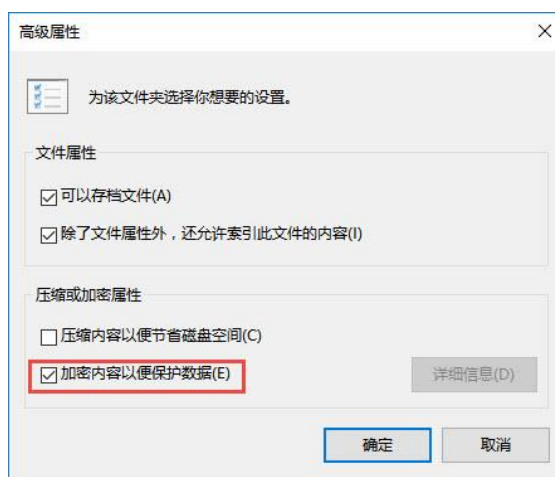


图 X-26

这样文件的加密就完成了。

解密文件时只需要打开文件的高级属性窗口，然后取消勾选“加密内容以便保护数据”，然后点击确定即可。

## EFS 证书导出与导入

文件加密后如果其他用户想要查看文件或者需要在其他计算机上查看文件，用户可以导出含有密钥的



证书。此外，如果用户重新安装了操作系统，则必须使用含有密钥的证书才可以打开原来的文件。因此建议大家在加密文件后，应该第一时间备份文件的加密证书和密钥。

1.证书的导出：

步骤 1：第一次使用 EFS 加密文件后，Windows 会提示用户备份文件加密证书和密钥，然后我们点击“现在备份（推荐）”。如图 X-27 所示。

步骤 2：然后会弹出“证书导出向导”对话框，我们点击“下一步”按钮，如图 X-28 所示。



图 X-27

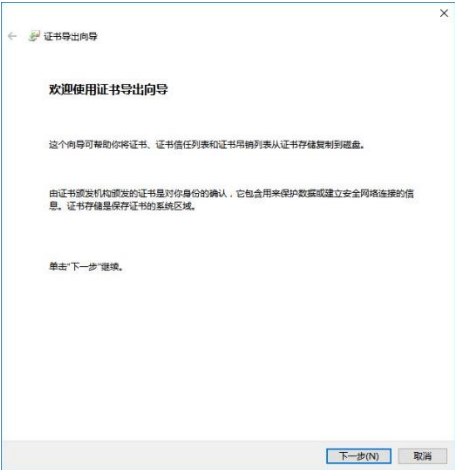


图 X-28

步骤 3：然后会弹出选择导出文件格式窗口，我们保持默认选项不变，点击“下一步”按钮，如图 X-29 所示。

步骤 4：然后在导出证书的安全设置窗口中，为导出的证书设置密码，然后点击下一步。如图 X-30 所示。



图 X-29

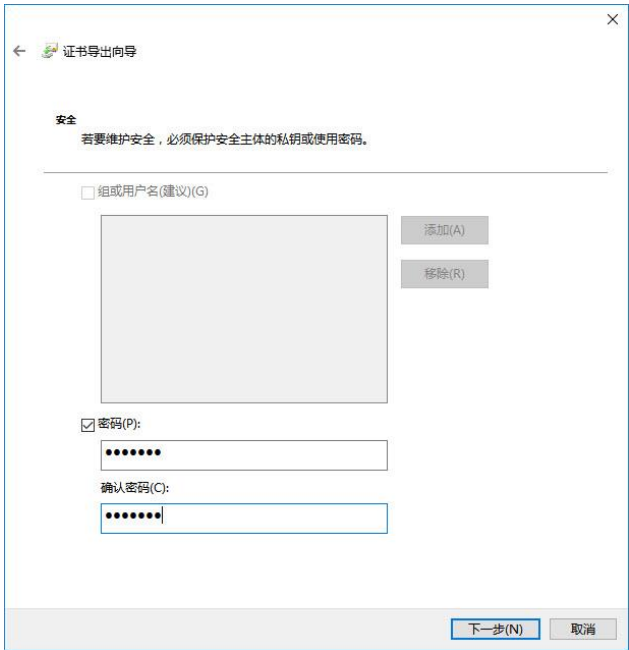


图 X-30

步骤 5：在弹出的窗口中，点击右侧的“浏览”按钮，选择要保存证书的位置。然后点击“下一步”按钮，如图 X-31 所示。

步骤 6 在弹出的窗口中，显示了导出证书的信息，我们点击“完成”按钮，就可以完成对证书的导出了。如图 X-32 所示。

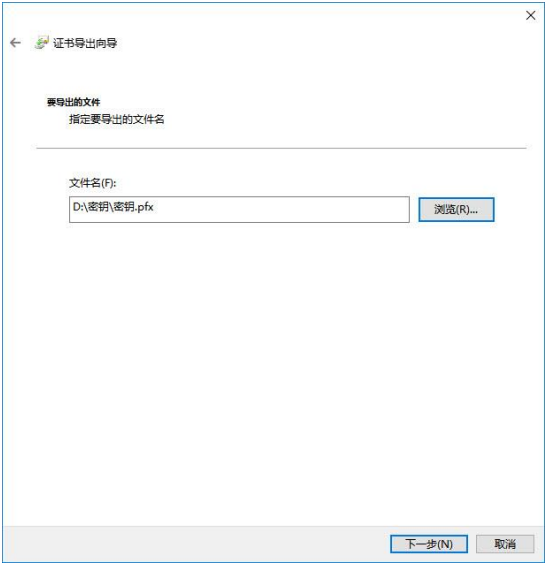


图 X-31

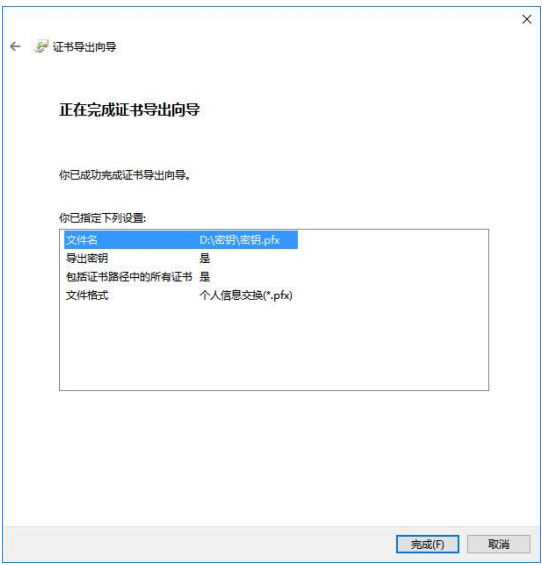


图 X-32

## 2.证书的导入:

当其他用户需要打开文件或者我们需要在其他计算机上打开加密的文件时，这时候需要先将证书导入。下面介绍下如何操作。

步骤 1: 双击要导入的证书文件，然后会弹出“证书导入向导”对话框，我们选择要存储的位置，然后点击“下一步”按钮。如图 X-33 所示。存储位置为“当前用户”时，只有当前用户可以使用密钥打开文件，当存储位置为“本地计算机”时，本地计算机上的所有用户都可以使用密钥打开文件。

步骤 2: 然后会弹出对话框，此时可以选择单个证书导入，或者导入整个文件夹的证书。选择完成后，点击“下一步”按钮，如图 X-34 所示。



图 X-33

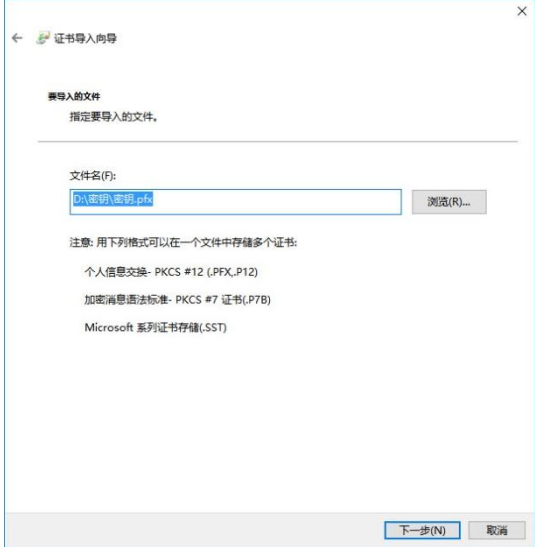


图 X-34

步骤 3: 在弹出的窗口中, 输入此密钥的密码, 然后勾选要导入的选项, 点击“下一步”按钮, 如图 X-35 所示。

步骤 4: 在弹出的窗口中, 选择证书存储的位置, 保持默认即可, 点击“下一步”按钮, 如图 X-36 所示。



图 X-35

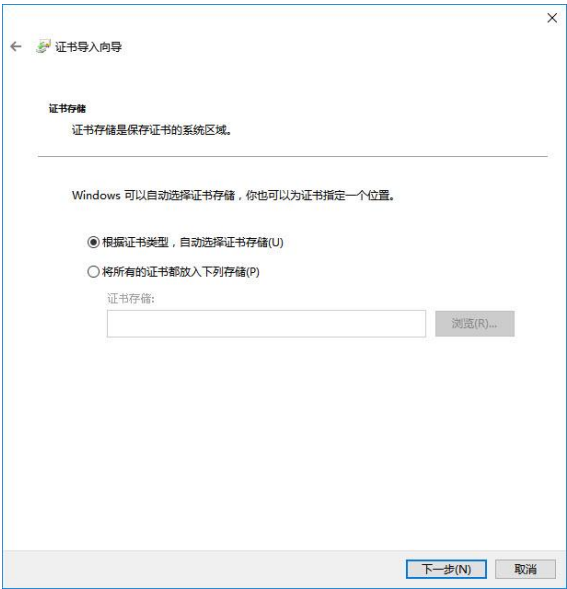


图 X-36

步骤 5: 最后在弹出的对话框中, 点击“完成”按钮, 如图 X-37 所示。此时证书导入就算是完成了。

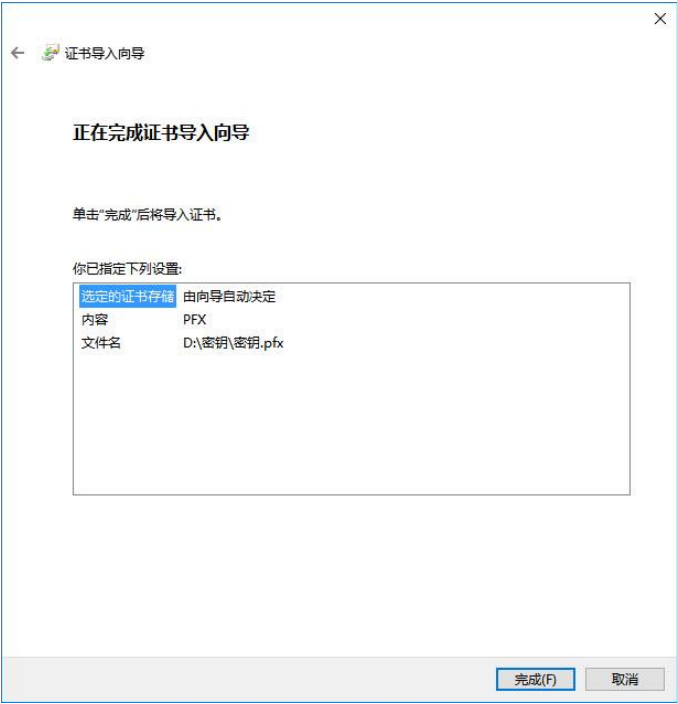


图 X-37

# 停用 EFS

在 Windows 10 专业版和 Windows 10 企业版中，EFS 加密功能是默认启用的。如果不想启用此功能，我们可以关闭 EFS 加密功能。下面介绍下如何操作。

步骤 1：点击开始菜单，然后输入文字“本地安全策略”，然后点击搜索结果中的“本地安全策略”，打开组策略管理器，如图 X-38 所示。

步骤 2：在弹出的“本地安全策略”窗口中，展开“公钥策略”栏，然后选中“加密文件系统”文件夹，右键单击此文件夹，然后在弹出的快捷菜单中点击“属性”，如图 X-39 所示。

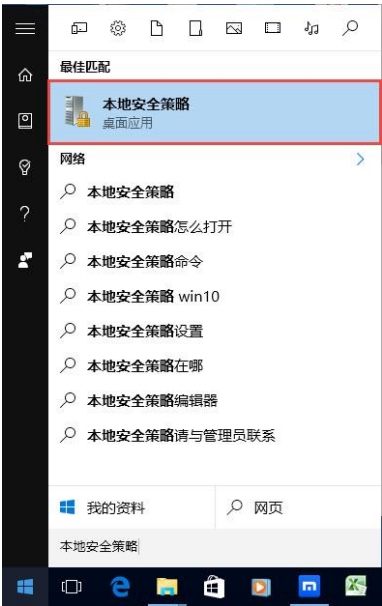


图 X-38

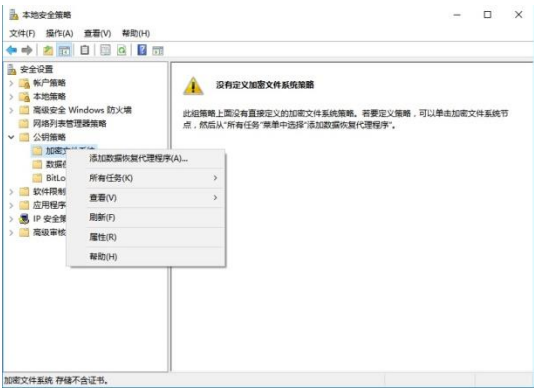


图 X-39

步骤 3：在弹出的窗口中，在“使用加密文件系统（EFS）的文件加密”项上选中“不允许”，然后点击“确定”按钮，如图 X-40 所示。

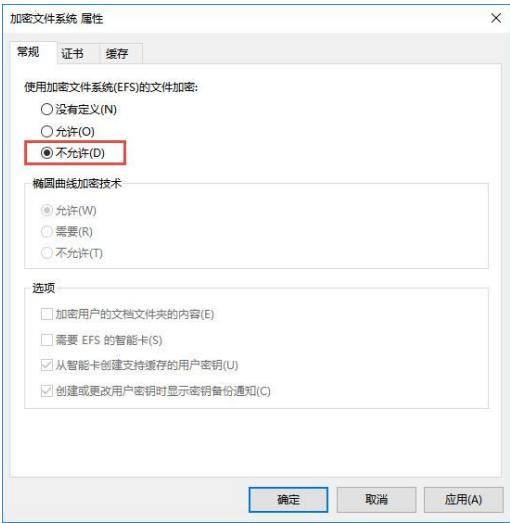


图 X-40

## X.5 文件压缩

随着使用时间的增加，我们的磁盘空间会越来越满。我们一般会使用压缩软件来压缩一些文件来节约磁盘空间。NTFS 文件系统也提供了一种基于操作系统层级的压缩功能。

### 文件压缩概述

NTFS 的压缩作为 NTFS 优秀特性之一，不仅能节约硬盘空间，还能大幅度提升读取性能。压缩提升的性能和压缩比例有关，最高能实现 50% 的提升，因为压缩后的文件排放，位置得到优化，体积减小，所以读取更快。

NTFS 压缩文件使用多种 LZ77 算法。在 4KB 的簇大小下，文件将以 64KB 为区块大小进行压缩。如果压缩后区块尺寸从 64KB 减小到了 60KB 或者更小，则 NTFS 就认为多余的 4KB 是空白的稀疏文件簇，也即认为它们没有内容。因此，这种模式将会有效的提升随机访问的速度。但是在随即写入的时候，大文件可能会被分区成非常多的小片段，片段之间会有许多很小的空隙。

压缩文件最适用于很少写入、平常顺序访问、本身没有被压缩的文件。压缩小于 4KB 或者本身已经被压缩过(如 .zip、.jpg 或者 .avi 格式)的文件可能会导致文件比原来更大并且显著降低速度。应该尽量避免压缩可执行文件，如 .EXE 和 .DLL 文件，因为他们可能内部也会使用 4KB 的大小对内容进行分页。决不要压缩引导系统是需要的系统文件，例如驱动程序，或者 NTDLR、winload.exe 或者 BOOTMGR。

压缩高压缩比的文件，例如 HTML 或者文本文件，可能会增加对他们的访问速度，因为解压缩所需的时间要小于读取完整数据所花费的时间。

通常情况下对于文件的读写是透明的，但并非所有情况下都始终如此。[29] Microsoft 建议避免在保存远程配置文件的服务器系统或者网络共享位置上使用压缩，因为这会显著地增加让处理器的负担。

硬盘空间受限的单用户操作系统可以有效地利用 NTFS 压缩。由于在计算机中速度最慢的访问不是 CPU 而是硬盘，因此 NTFS 压缩可以同时提高受限制的、慢速储存空间的空间和速度利用率。

当某个程序(如下载管理器)无法创建没有内容的稀疏文件的时候，NTFS 压缩也可以作为稀疏文件的替代实现方式。

可是压缩是个双刃剑，如何选择合适的內容区进行压缩。微软文档认为，NTFS 更适用于客户端，比如经常读，写入较少的文件，不适合频繁写入的应用比如服务器，因为会增加 cpu 负担，对于服务器这种 cpu 饥渴性应用，还是不要的好。

### 文件压缩启用与关闭

在 Windows 10 中如何打开和关闭 NTFS 文件压缩功能呢？下面给大家介绍一下：

对文件或文件夹来说，只要右键单击该文件或文件夹，然后在弹出的快捷菜单上点击“属性”，在弹出的窗口中，点击“高级”按钮，如图 X-41 所示。

然后在弹出的“高级属性”窗口中，“压缩内容以便节省磁盘空间”这个选项如果勾选了，就表示启用了 NTFS 文件压缩功能，如果这个选择没有被勾选，则表示关闭了 NTFS 文件压缩功能。如图 X-42 所示。



图 X-41

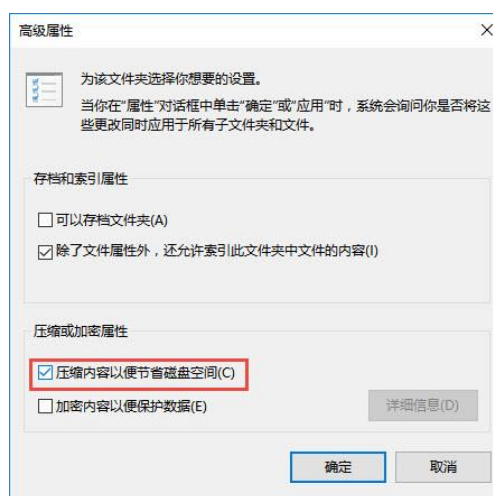


图 X-42

## X.6 文件链接

文件链接的概念最初是由 Linux 操作系统上提出的。自 Windows 2000 开始，微软开始部分支持文件链接功能。随着操作系统版本的更新，对文件链接的支持越来越完善。

文件链接简单来说就是同一个文件或目录，我们可以以多个路径来表示。而不需要占用额外的存储空间。Windows 10 中的文件链接功能包含 3 种方式，分别是：硬链接、软链接、符号链接。

### 硬链接

硬链接就是让多个不在或者同在一个目录下的文件名，同时能够修改同一个文件，其中一个修改后，所有与其有硬链接的文件都一起修改了。但是删除任意一个文件名下的文件，对另外的文件名没有影响。

需要注意的是硬链接只可以链接非空文件，不可以链接文件夹。硬链接是不能跨卷的，只有在同一文件系统中的文件之间才能创建链接。

## 软 链 接

软链接也被称作联接。软链接文件只是其源文件的一个标记，当删除了源文件后，链接文件不能独立存在，虽然仍保留文件名，但却不能查看软链接文件的内容了。删除软链接也不会影响源文件。

## 符 号 链 接

符号链接在功能上和快捷方式有些类似。符号链接在创建的时候可以使用相对路径和绝对路径。

路径可以是任意文件或目录，可以链接不同文件系统的文件。（链接文件可以链接不存在的文件，这就产生一般称之为”断链”的现象），链接文件甚至可以循环链接自己（类似于编程中的递归）。在对符号文件进行读或写操作的时候，系统会自动把该操作转换为对源文件的操作，但删除链接文件时，系统仅仅删除链接文件，而不删除源文件本身。符号链接的操作是透明的：对符号链接文件进行读写的程序会表现得直接对目标文件进行操作。某些需要特别处理符号链接的程序（如备份程序）可能会识别并直接对其进行操作。一个符号链接文件仅包含有一个文本字符串，其被操作系统解释为一条指向另一个文件或者目录的路径。它是一个独立文件，其存在并不依赖于目标文件。如果删除一个符号链接，它指向的目标文件不受影响。如果目标文件被移动、重命名或者删除，任何指向它的符号链接仍然存在，但是它们将会指向一个不复存在的文件。这种情况被有时被称为被遗弃。