NTFS元文件

NTFS 包含若干用于定义和组织文件系统的文件。总体来说，这些文件中的绝大多数结构和其它用户文件类似（“$Volume”是最特殊的），但不能被文件系统客户端直接访问。这些元文件用于定义文件、备份文件系统关键数据、缓存文件系统的更改、管理空闲空间的分配、满足 [BIOS](http://zh.wikipedia.org/zh-cn/BIOS) 的要求、跟踪坏[扇区](http://zh.wikipedia.org/zh-cn/%E6%89%87%E5%8C%BA" \t "_blank)单元，以及储存安全信息和磁盘空间使用情况。

|  |  |  |
| --- | --- | --- |
| 区段编号 | 文件名 | 作用 |
| 0 | $MFT | 描述卷上的所有文件，包括文件名、时间戳、流名称和数据流所在的簇的编号列表、索引、安全标识符，以及文件属性（如“只读”、“压缩”、“加密”等）。 |
| 1 | $MFTMirr | $MFT 的最开始的几个关键项的副本，通常是 4 项（4[KiB](http://zh.wikipedia.org/zh-cn/Kibibyte)）。 |
| 2 | $LogFile | 包含文件系统更改的事务日志，以保护元数据的稳定性。 |
| 3 | $Volume | 包含卷的相关信息，如卷对象标识符、[卷标](http://zh.wikipedia.org/w/index.php?title=%E5%8D%B7%E6%A0%87&action=edit&redlink=1" \t "_blank)、文件系统版本，以及卷标志（加载、需要扫描、需要调整 $LogFile 大小、在 NT4 上加载、正在更新卷序列号、需要升级结构）。卷序列号储存在 $Boot 文件中。 |
| 4 | $AttrDef | 使用的 NTFS 属性的表，包含名称、编号和描述。 |
| 5 | . | [根目录](http://zh.wikipedia.org/zh-cn/%E6%A0%B9%E7%9B%AE%E5%BD%95)。 |
| 6 | $Bitmap | 一个位图，用于指示卷上的指定簇正在被使用或空闲。 |
| 7 | $Boot | [卷引导记录](http://zh.wikipedia.org/w/index.php?title=%E5%8D%B7%E5%BC%95%E5%AF%BC%E8%AE%B0%E5%BD%95&action=edit&redlink=1)，该文件位于卷的第一个簇，其中包含引导代码（用于定位并启动 [NTLDR](http://zh.wikipedia.org/w/index.php?title=NTLDR&action=edit&redlink=1)／[BOOTMGR](http://zh.wikipedia.org/w/index.php?title=Windows_Vista_%E5%90%AF%E5%8A%A8%E8%BF%87%E7%A8%8B&action=edit&redlink=1" \t "_blank)）、一个 [BIOS 参数区块](http://zh.wikipedia.org/w/index.php?title=BIOS_%E5%8F%82%E6%95%B0%E5%8C%BA%E5%9D%97&action=edit&redlink=1)（其中包含[卷序列号](http://zh.wikipedia.org/w/index.php?title=%E5%8D%B7%E5%BA%8F%E5%88%97%E5%8F%B7&action=edit&redlink=1)），以及 $MFT 和 $MFTMirr 所在的簇编号。 |
| 8 | $BadClus | 包含所有标记为“有[坏扇区](http://zh.wikipedia.org/w/index.php?title=%E5%9D%8F%E6%89%87%E5%8C%BA&action=edit&redlink=1" \t "_blank)”的簇的一个文件。该文件用于为 chksdk（磁盘扫描）工具简化簇的管理，用于放置新发现的坏扇区，以及标识未被引用的簇。 |
| 9 | $Secure | [访问控制列表](http://zh.wikipedia.org/w/index.php?title=%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6%E5%88%97%E8%A1%A8&action=edit&redlink=1)（ACL）数据库，统一将 ACL 存储于该数据库中而非每个文件存储各自的 ACL 以减少总体代价。包含两个索引：$SII——可能是[[来源请求]](http://zh.wikipedia.org/zh-cn/Wikipedia:%E5%88%97%E6%98%8E%E6%9D%A5%E6%BA%90" \t "_blank)*安全 ID 索引*，以及 $SDH——*安全描述符哈希*，用于索引包含实际 ACL 列表的称为 $SDS 的流的位置。[[1]](http://zh.wikipedia.org/zh-cn/NTFS" \l "_note-insidewin2kntfs-0" \t "_blank) |
| 10 | $UpCase | 一个 [Unicode](http://zh.wikipedia.org/zh-cn/Unicode) 大写字母表，用于确保在 Win32 和 DOS 命名空间下大小写不敏感。 |
| 11 | $Extend | 一个文件系统目录，包含若干不定的可选扩展，如 $Quota、$ObjId、$Reparse、$UsnJrnl 等。 |
| 12 ... 23 | 保留。 | |
| 通常是 24 | $Extend\$Quota | 包含关于磁盘限额的信息。 |
| 通常是 25 | $Extend\$ObjId | 包含用于[分布链接跟踪](http://zh.wikipedia.org/w/index.php?title=%E5%88%86%E5%B8%83%E9%93%BE%E6%8E%A5%E8%B7%9F%E8%B8%AA&action=edit&redlink=1)的信息。 |
| 通常是 26 | $Extend\$Reparse | 包含对卷上所有[重解析点](http://zh.wikipedia.org/w/index.php?title=%E9%87%8D%E8%A7%A3%E6%9E%90%E7%82%B9&action=edit&redlink=1)（如[符号链接](http://zh.wikipedia.org/zh-cn/%E7%AC%A6%E5%8F%B7%E9%93%BE%E6%8E%A5)）的反引用。 |
| *27 ...* | *file.ext* | 常规文件项的开始位置。 |

这些元文件会被 NTFS 专门处理，很难直接查看。需要使用专门为此设计的工具完成实现该功能。