文章编号: 1672 - 058X(2009)04 - 0346 - 04

浅析 NTFS管理磁盘数据的基本结构

杨 华, 高福兵, 王旭辉
(重庆通信学院 研究生管理大队,重庆 400035)

摘 要:鉴于 NTFS文件系统的广泛应用,从物理扇区组织、磁盘空间规划以及数据组织模式等方面分析了 NTFS文件系统管理磁盘数据的基本结构,为基于 NTFS文件系统的数据恢复、计算机取证等技术提供了一定的指导作用。

关键词: NTFS文件系统;磁盘规划;元数据文件;主文件表
中图分类号: TP3 **文献标志码**: A

NTFS(New Technology File System),是微软公司为 Windows NT/2000/XP/2003/2008/Vista设计的一种高性能、自恢复的标准文件系统。与早期的 FAT文件系统相比,NTFS文件系统能够支持和管理更大的磁盘空间和磁盘文件,拥有更高的磁盘空间利用率和数据管理性能,具备更强的安全性和可靠性,并提供了诸如加密文件系统、事务日志记录、磁盘压缩、磁盘配额以及 RAID存储方案等多种扩展功能。NTFS文件系统所体现的优越性能离不开其底层采用的特定磁盘规划和相应的数据组织模式,这也是 NTFS文件系统区别于其他类型文件系统的根本所在。从整体磁盘规划和内部数据组织的角度剖析 NTFS文件系统管理磁盘数据的基本结构,对研究基于 NTFS文件系统的数据恢复、数据彻底删除、计算机取证,甚至开发自己的文件系统都具有重要的实际意义。

1 NTFS文件系统的磁盘规划

NTFS文件系统组织和管理磁盘数据的基本架构由磁盘分区格式化软件负责构建。磁盘分区格式化软件在格式化 NTFS分区时主要执行以下两个操作:一是根据用户指定的或默认的簇大小来组织分区内的物理扇区;二是在磁盘分区上为 NTFS文件系统的执行创建必须的系统管理数据。上述两个操作将形成 NTFS文件系统管理磁盘数据所独有的磁盘规划。

1.1 分区的物理组织

NTFS文件系统以簇为基本单元来组织和管理分区内的物理扇区[1]。簇是磁盘上若干个连续物理扇区的组合。在 NTFS文件系统中,簇的划分从分区所属的第一个物理扇区开始 (即 DBR扇区),默认大小为 4 kB。NTFS分区上的所有簇在物理上前后相连,构成一个连续不断的线性簇链。为了方便簇的管理和定位,NTFS文件系统按照簇在物理上排列的先后顺序,从 0开始对其进行顺序编号,即所谓的逻辑簇号 (Logical Cluster Number, LCN),如图 1所示。

收稿日期: 2009 - 04 - 28;**修回日期**: 2009 - 05 - 25。
作者简介:杨华 (1971 -),男,四川省乐山市人,讲师,硕士,从事数据安全与数据恢复、嵌入式系统开发研究。

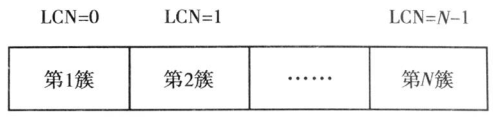

图 1　簇的 LCN编号

1.2　分区的逻辑组织

NTFS文件系统把分区内存储的所有数据看作是各种不同文件的组合,文件是 NTFS文件系统组织和管理磁盘数据的基本对象[2]。因此,在 NTFS分区上已分配的每一个扇区或簇都属于某个特定的文件,包括分区引导扇区 DBR在内。

从文件系统的角度来看, NTFS分区内的文件可分为两类:元数据文件和用户数据文件。其中,元数据文件由磁盘分区格式化软件在执行分区格式化时创建,是 NTFS文件系统用于组织、架构和管理 NTFS分区所必须的系统文件,这些文件的命名统一以“$”开头。

在 NTFS文件系统中,与磁盘规划直接相关的元数据文件主要有以下 3个:

(1) $Boot。 $Boot文件一般占用 NTFS分区最初的 16个扇区,主要由 DBR扇区和操作系统引导代码构成。与 FAT文件系统不同, NTFS分区的 DBR不再是一个独立的磁盘区域,它从属于 $Boot文件,其内部的 BIOS参数块包含有识别和挂载 NTFS文件系统所必须的基本信息,如分区类型、扇区大小、簇大小、文件记录大小、索引分配大小以及定位 NTFS文件系统中最关键的元数据文件 $MFT和 $MFTMirr所需要的起始簇号等等。

从某种程度上看, DBR不仅是引导操作系统的起点,也是 NTFS文件系统的入口。鉴于 DBR在系统启动中的重要作用, NTFS文件系统在该分区的最后一个扇区中保留了 DBR的一个备份。

此外,由于 DBR的物理位置是系统预设的(必须是分区的第一扇区),因此 $Boot就成为 NTFS文件系统中惟一一个位置固定且不能移动的文件。

(2) $MFT。 $MFT文件,即主文件表 (Master File Table, MFT),以文件记录的形式描述了 NTFS分区内所有元数据文件和用户数据文件的相关信息,可由此访问和操作 NTFS分区上的任何文件。 $MFT可由 DBR定位,是继 $Boot之后被访问的第一个 NTFS元数据文件,是组织和架构 NTFS文件系统的基础。

从 $MFT文件的内部结构上看,首先记录的是 NTFS文件系统的元数据文件,紧接着是为后续功能扩展而保留的文件记录空间,然后才是用户数据文件的记录。其中, $MFT的第一个文件记录描述的就是 $MFT文件本身,其后的文件记录依次描述了 $MFTMirr、$LogFile、$Volume等文件。

为了尽量保证 $MFT占用空间的连续性,防止因过多的文件碎片而影响文件系统的整体性能, NTFS默认在分区上为 $MFT预留了 12.5%的独占空间,称之为 MFT区域,而余下的 87.5%的空间则被用于存储文件数据。一般情况下,除非分区缺乏足够的数据存储空间,否则不会占用 MFT的预留空间。

(3) $MFTMirr。 $MFTMirr是 $MFT的镜像文件,它备份了 $MFT文件中的前几个关键文件记录,目的是确保在 $MFT出错的情况下仍能正常访问由这些文件记录所指向的关键元数据文件。 $MFTMirr文件备份的文件记录的多少因簇的大小而异,但至少会备份 $MFT中的前 4个文件记录。

$MFTMirr文件一般被安排在 NTFS分区的中部,其起始簇号保存在 DBR的 BIOS参数块中。可用图 2来描述 NTFS文件系统的磁盘空间布局[3]:

除了上述 3个元数据文件外, $Bitmap和 $BadClus文件也与磁盘空间的分配和管理密切相关:前者以位串的形式记录了 NTFS分区中每个簇的使用情况,后者则记录了 NTFS分区内的所有坏簇[4]。

至于其他的元数据文件,基本不涉及 NTFS分区的磁盘空间规划,仅为 NTFS文件系统提供各种扩展功能。

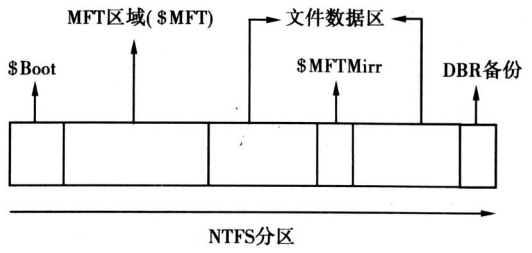

图 2 NTFS文件系统的磁盘空间布局

2 NTFS文件系统的数据组织

NTFS文件系统通过元数据文件来组织和管理用户数据文件,其中 $MFT文件扮演着主要角色。如前所述, $MFT文件的基本组成单元和管理对象是文件记录,它们描述了用户数据文件在 NTFS文件系统中的存储状态。掌握了文件记录的基本结构以及文件记录彼此之间的内在联系,就能理清 NTFS文件系统组织和管理磁盘数据的脉络。

2.1 文件记录的位置号

在 NTFS文件系统中,文件记录的大小固定为 1 KB,且所有的文件记录在 $MFT文件中连续排列,并由前至后从 0开始顺序编号,称之为文件记录的 MFT位置号,并被记录在对应的文件记录中。通过 MFT位置号可以唯一确定 $MFT中的文件记录,因此 MFT位置号就成为文件记录的标识以及关联文件记录的纽带。

2.2 文件记录的内部结构

NTFS文件系统把每个文件看作是一套属性的集合,文件的各个组成元素,如文件名、文件的安全信息,甚至文件中包含的数据都属于文件的属性。相应地,文件记录的主体就是关于这些文件属性的描述,其结构如图 3所示。

文件记录的头部主要描述了文件记录的基本信息,如文件记录的大小、类型、MFT位置号以及本文件记录与其他文件记录之间的关联等等,且始终以十六进制数据“46 49 4C 45”(即 ASCII码“FILE”)开始。

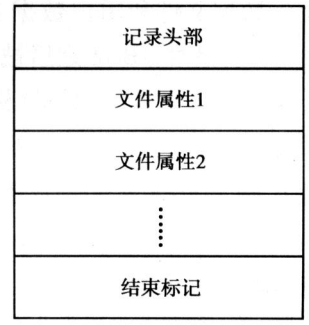

图 3 文件记录的内部结构

文件属性又可划分为属性头部和属性值两个部分:属性头部是对属性的一般性描述,如属性的类型、大小、名称以及驻留状态等等;属性值则是文件属性所包含的具体内容,取决于属性的类型。

NTFS文件系统将文件的常用属性类型及其标准命名定义在 $AttrDef元数据文件中,可直接在文件记录中用相应的属性 ID表示。如果文件属性采用在 $AttrDef文件中定义的标准属性名,则称其为未命名属性。反之,如果文件属性使用自定义的名称,则称其为命名属性。

如果文件属性能整个被包含在固定大小为 1 KB的文件记录中,则称其为常驻属性;如果需要在文件记录之外为文件属性分配额外的存储空间,则称其为非常驻属性。非常驻属性的属性头仍然位于文件记录中,但其属性值部分却不再包含具体的属性内容,而是记录了 NTFS文件系统在文件数据区为该属性内容所分配的额外存储空间的信息 (包括存储空间的起始逻辑簇号和簇数),称为数据运行 (Data Run)。如果分配的存储空间不连续,则非常驻属性可能拥有多个依次排列的数据运行。

此外,为了方便管理非常驻数据,NTFS文件系统把分配给它的数据运行所包含的簇按顺序从 0开始依次编号,并将该信息记录在非常驻属性的头部,称之为虚拟簇号 (Virtual Cluster Number, VCN)。VCN不同于 LCN,前者针对特定的空间分配,且不要求在物理上连续,而后者则针对整个 NTFS分区,且在物理上连续。

文件记录的结束标记始终为十六进制数据“FF FF FF FF”。

2.3 文件记录的类型

NTFS的文件记录可分为文件和目录两种类型,该类型信息记录在文件记录的头部。文件包含了实际的用户数据,而 NTFS文件系统则通过其文件记录的数据属性来定位和访问文件所含的用户数据。NTFS文件系统支持文件的多数据属性,即单个文件除了包含一个必须的未命名数据属性外,还可以创建多个可选的命名数据属性,分别用于描述文件所包含的不同数据。其中,NTFS文件系统将把未命名的数据属性当作文件的默认数据属性,而其他的命名数据属性则必须通过特殊的语法才能访问,且这些命名数据属性的大小不会计入文件的容量。

目录是一种特殊的文件,主要用于组织和管理 NTFS文件系统的命名空间。NTFS文件系统的命名空间采用由顶而下的树形目录结构,其根目录是定义在 $MFT文件中的元数据文件“.”。与目录关联的文件记录并不包含具体的用户数据,仅仅是列举了该目录下所有文件名和目录名的索引信息,以供 NTFS文件系统在列举目录和查询文件时使用。小目录的所有索引信息通常保存在目录的索引根属性中,并驻留在目录的文件记录内。大目录则必须在文件数据区开辟专门的存储空间来保存索引信息,并将空间分配情况以数据运行的形式记录在目录的索引分配属性中,而且大目录的索引信息将以 B+树结构进行组织,能最大限度地提高 NTFS文件系统的搜索效率。至于索引空间的分配大小可从 DBR的 BIOS参数块中获取,一般是 4 KB。

3 结束语

根据上面的分析,可以看出 NTFS文件系统与 FAT文件系统采用了截然不同的磁盘数据管理方式:FAT文件系统采用“FAT+FDT”的管理方式,而 NTFS文件系统则采用元数据文件驱动的模式。正是基于元数据文件及元数据文件中创建的各种基本数据管理结构,才使 NTFS文件系统具有比 FAT文件系统更高的性能,并依此提供了多种增强功能,从而使 NTFS文件系统更适应于多种需求环境。

参考文献:

[1] 黄步根. NTFS系统存储介质上文件操作痕迹分析 [J]. 计算机工程, 2007, 33(23): 281 - 283
[2] 戴士剑,涂彦辉. 数据恢复技术 (2版) [M]. 北京:电子工业出版社, 2005
[3] 赵双峰,费金龙,刘楠,等. Windows NTFS下数据恢复的研究与实现 [J]. 计算机工程与设计, 2008, 29(2): 306 - 308, 332
[4] 居锦武,王兰英. NTFS文件系统剖析 [J]. 计算机工程与设计, 2007, 28(22): 5437 - 5439, 5460

Analyzing the basic structure of managing disk data on NTFS volume

YANG Hua, GAO Fu-bing, WANG Xu-hui

(Graduate Management Team, Chongqing Communication College, Chongqing 400035, China)

Abstract: Because of the extensive use of NTFS, this paper analyzed the basic structure of managing disk data on NTFS volume from the organization of disk physical sectors, the layout of disk space and the mode of organizing disk data in detail. This paper can supply some guidance for the data recovery technology and Computer Forensics technology based on NTFS.

Key words: NTFS file system; disk layout; metadata file; master file table

责任编辑:李翠薇