اساس (اصول) NTFS

سیستم پرونده NT مجموعه ای از عملکرد ، قابلیت اعتماد و سازگاری را مهیا می کند که در سیستم پرونده FAT یافت نمی شود . این سیستم طوری طراحی شده که اعمال پوشه استاندارد از جمله خواندن ، نوشتن و جستجوی و حتی اعمال پیشرفته ای چون بهبود سیستم پوشه را بر روی فضای زیادی از دیسک به سرعت انجام می دهد .

با فرمت کردن یک نسخه با سیستم پرونده NTFS و چندین پوشه دیگر و یک جدول پوشه اصلی (MFT) ایجاد می شود که شامل اطلاعاتی راجع به تمام فایل ها و پوشه های موجود در نسخهٔ NTFS می باشد . اولین اطلاعات بر روی نسخهٔ NTFS ، بخش راه اندازی سیستم است که از 0 شروع شده و می تواند تا 16 نیز ادامه یابد . اولین پوشه بر روی نسخهٔ NTFS ، جدول پوشه اصلی است (MFT) . شکل زیر طرحی از یک نسخهٔ NTFS را نشان می دهد در زمانی که فرمت کردن به پایان رسیده.

این بخش اطلاعاتی راجع به NTFS را در بر دارد . عناوین مورد بحث شامل عناوین زیر است :

- بخش راه اندازی سیستم NTFS
- جدول پرونده اصلی NTFS (MFT)
- انواع پرونده های NTFS
- ویژگی های فایل NTFS
- فایل های سیستم NTFS
- چندین جریان دادهٔ NTFS
- فایل های فشرده NTFS
- فایل های رفرشده NTFS ، EFS
- استفاده از EFS
- دستور اینترنال EFS
- ویژگی EFS

ـ پی آمدهای EFS

ـ فایل های یدکی NTFS

ـ قابلیت بازیافت و تمامیت دادهٔ NTFS

سیستم پرونده NTFS شامل ویژگی های امنیتی مورد نیاز برای سرورهای فایل و کامپیوترهـای شخصـی گـران قیمت در یک محیط متحد است . سیستم پرونده NTFS همچنین کنترل دستیابی به داده و امتیاز مالکیت را که برای تمامیت داده های مهم بسیار حائز اهمیت است را حمایت می کند . هنگـامی کـه پوشـه هـای بـه اشـتراک گذاشته بر روی یک کامپیوتر با ویندوز NT دارای مجوزهای خاص هستند ، فایل ها و پوشه های NTFS بـدون به اشتراک گذاشتن می توانند مجوز داشته باشند . NTFS تنها فایل بر روی ویندوز NT است که بـه شـما ایـن امکان را می دهد که مجوز ها را برای فایل های اختصاصی تعیین کنید.

سیستم پرونده NTFS یک طرح ساده اما در عین حال قدرتمند دارد . اساساً ، هر چیزی بر روی نسخهٔ یک فایل است و هر چیزی در یک فایل ، یک ویژگی است ، از ویژگی داده ، تا ویژگی امنیتی و ویژگی نام فایل . هر بخـش در نسخه NTFS که اختصاص یافته باشد به یک فایل متعلق است . حتی سیستم پرونده متادیتا (اطلاعاتی کـه به تنهایی سیستم پرونده را توصیف می کند) نیز بخشی از یک فایل است .

تازه های **NTFS5** (**WINDOWS 2000**)

رمزگذاری ـ سیستم رمزگذاری فایل (EFS) ، فن آوری رمزگذاری فایل هسته ای را مهیا مـی کنـد کـه فایـل های رفر گذاری شده را بر روی نسخه های NTFS ذخیره می کنند . EFS فایل ها را از دسترس مزاحمان دور نگه می دارد ، کسانی که ممکن است دسترسی غیر مجاز به داده های ذخیره شده نفوذ پذیر را پیدا کنند .

سهمیه های دیسک ـ ویندوز 2000 از سهمیه های دیسک برای نسخه های NTFS پشتیبانی می کند . شما می توانید از سهمیه های دیسک برای بازبینی و محدود کردن فضای دیسک استفاده کنید .

مراحل تجزیه دوباره ـ مراحل تجزیه دوباره ؛ موارد جدیدی در NTFS هستند که می توانند بـرای فایـل هـا و پوشه های NTFS به کار برده شوند . یک فایل یا پوشه که شامل مرحلهٔ تجزیه دوبـاره اسـت نیـاز بـه رفتارهـای

اضافی دارد که در سیستم پرونده اصلی وجود ندارد . مراحل تجزیه دوباره فایل توسط بسیاری از ویژگی های انبار جدید در ویندوز 2000 مورد استفاده قرار می گیرد که شامل مراحل تنظیم نسخه است .

مراحل تنظیم نسخه ـ مراحل تنظیم نسخه ، موارد جدیدی از NTFS هستند . بر اساس مراحل تجزیه دوباره ، مراحل تنظیم نسخه اجازه پیدا می کنند که دستیابی به ریشهٔ یک نسخه محلی را به ساختار پروندهٔ یک نسخهٔ محلی دیگر پیوند دهند .

فایل های یدکی ـ فایل های یدکی به برنامه ها امکان ایجاد فایل های بسیار بزرگتر را می دهند اما فضای دیسک را فقط به حدی که لازم است مصرف می کنند .

ردیابی لینک توزیع شده ـ NTFS یک سرویس ردیابی لینک را مهیا می کند که از میان برهای فایل به خوبی لینک های OLE در پوشه های مرکب نگهداری می کند .

بخش راه اندازی سیستم

جدول 1-5 بخش راه اندازی یک نسخهٔ فرمت شده با NTFS را نشان می دهد . زمانی که شما یک نسخهٔ NTFS را فرمت می کنید ، برنامهٔ فرمت اولین 16 بخش را به بخش راه اندازی و بخش خود راه انداز اختصاص می دهد .

جدول 1-5 بخش راه اندازی **NTFS**

بر روی نسخه های NTFS فیلدهای داده که از BPB پیروی می کنند BPB توسعه یافته را شکل می دهند . داده بر روی این فیلدها Ntldr را قادر به پیدا کردن جدول فایل اصلی می کند . در شروع ویندوز .

بر روی نسخه های NTFS ، MFT در بخش از پیش تعریف شده واقع نشده ، همچون نسخه های FAT32 ، FAT16 . به همین خاطر ، MFT می تواند انتقال داده شود ، اگر یک بخش بد در این محل نرمال وجود داشته باشد . با این وجود اگر داده معیوب باشد ، MFT نمی تواند تعیین مکان کند و ویندوز NT / 2000 وانمود می کند که نسخه فرمت نشده است .

مثال های زیر بخش راه اندازی یک نسخهٔ فرمت شده NTFS را در حین اجرای ویندوز 2000 نشان مـی دهد .

نتیجه چاپی در این سه بخش فرمت شده است :

ـ بایت های 0×0A-0×00 هدایت پردازنده به بخش دیگر برنامه و OEM ID هستند .

ـ بایت های 0×53-0×0B ، BPB ، BPB توسعه یافته هستند .

ـ کد باقیمانده ، کد خود راه انداز و انتهای نشان گر بخش است .

جدول زیر فیلدهای موجود در BPB ، BPB توسعه یافته بر روی نسخه های NTFS نشان مـی دهـد . فیلـدها در0×B ، 0×0D ،0×15، 0×18 ، 0×1A ، 0×1C آغاز می شـوند و بـر روی نسـخه هـای FAT16 ، FAT32 هماهنگ می شوند . نسخه های ساده با داده های این مثال مطابقت می کنند .

نام فیلد (رشته)

بایت در بخش

هر بخش در هر دسته

بخش های ذخیره شده

همیشه 0

توسط NTFS استفاده نمی شود

توصیف گررسانه

هر بخش در هر مسیر

تعداد شبکه

بخش های نهان

توسط NTFS استفاده نمی شود

توسط NTFS استفاده نمی شود

بخش های کلی

تعداد دسته های اصلی برای پوشه

MFT

تعداد دسته های اصلی برای پوشه

MFT Mirr

هر دسته در هر بخش ثبت فایل

هر دسته در هر گروه فهرست

شماره سریال نسخه

حفاظت از بخش راه انداز

به خاطر این که یک سیستم عمل کننده برای دستیابی به یک نسخه به بخش راه انداز تکیه می کنـد ، پیشـنهاد می شود شما ابزارهای اسکن دیسک همچون chkdsk را مرتب اجرا نمایید . علاوه بر تهیه کپی پشتیبانی از تمام فایل ها برای حفاظت در برابر از دست دادن داده ها ، اگر نمی توانید به یک نسخه دست یابید .

جدول پوشه اصلی (MFT) NTFS

هر فایلی بر روی نسخهٔ NTFS توسط یک مدرک (رکورد) در یک فایل خـاص بـه نـام جـدول پوشـه اصـلی (MFT) نمایش داده می شود .NTFS ، اولین 16 ثبت از جدول را برای اطلاعات خاص ذخیره می کنـد . اولین ثبت از این جدول خود جدول فایل اصلی را شرح می دهد که با یک ثبت کپی MFT دنبال می شود . اگـر اولین ثبت MFT خراب شد ، NTFS برای پیدا کردن فایل کپی ، همانی که اولین ثبت هماننـد اولـین ثبـت از MFT است ، اولین ثبت را می خواند . محل قرار گرفتن بخش های داده برای هر دو فایل کپـی MFT ، MFT در بخش راه انداز ثبت شده است . یک کپی از بخش راه انداز در مرکز اصلی دیسک قرار می گیرد . سومین ثبـت از MFT فایل ثبت است (Log) که برای بازیافت فایل مورد استفاده قرار می گیرد . هفدهمین ثبت و ثبت های زیر از جدول فایل اصلی برای هر فایل و فهرستی هستند .

مثالی ساده از ساختار MFT

جدول فایل اصلی مقدار شخصی از فضا را برای هر ثبت فایل در نظر می گیرد . ویژگی های هر فایل در بخش مشخص شده در MFT نوشته می شود . فایل ها و فهرست های کوچک (به ویژه 1500 بایت یا کوچکتر) مثل فایلی که در شکل بعد نشان داده شده می توانند در درون ثبت جدول فایل اصلی قرار بگیرند .

شکل 2-5 ثبت MFT برای فهرست یا فایل های کوچک

این طرح به دسترسی فایل سرعت می بخشد ، در نظر بگیرید ، برای مثال ، سیستم پرونده FAT را که برای فهرست کردن نام ها و آدرس های هر فایل از جدول تعیین فایل استفاده می کند . ورودی فهرست FAT شامل یک فهرست به جدول تعیین فایل است .

زمانی که شما بخواهید یک فایل را مشاهده کنید ، ابتدا FAT جدول اختصاصی فایل را می خواند و مطمئن می شود که چنین جدولی وجود دارد . سپس FAT ، فایل را با استفاده از جستجوی زنجیر اتحادهای اختصاصی که برای فایل در نظر گرفته شده ، باز می یابد . با NTFS به سرعت فایل را پیدا می کند، فایل برای استفادهٔ شما آماده است .

مدارک فهرست درست مثل ثبت فایل درداخل جدول پوشه اصلی واقع شده اند . به جای داده ها ، فهرست ها شامل اطلاعات فهرست می باشند.مدارک فهرست کوچک در ساختار MFT جای دارند . فهرست های بزرگتر به شاخه های B سازمان دهی شده اند ، در حالی که دارای ثبت هایی با اشاره گر به دسته های خارجی هستند که شامل ورودی فهرست هایی است که نمی توانند در ساختار MFT جای گیرند .

انواع فایل های NTFS

- ویژگی های فایل NTFS
- فایل های سیستم NTFS
- چندین جریان دارهٔ NTFS
- فایل های فشرده NTFS
- فایل های رفرشده NTFS
- استفاده از EFS

ـ دستور EFS

ـ ویژگی EFS

ـ پی آمدهای EFS

ـ فایل های یدکی NTFS

ویژگی های فایل NTFS

سیستم فایل NTFS هر فایل یا پوشه را همچون یک مجموعه از ویژگی های فایل مشاهده می کند . عناصری مثل نام فایل اطلاعات امنیتی آن و حتی داده های آن فایل ، همه ویژگی های فایل هستند . هر ویژگی توسط یک کد نوع ویژگی و نام ویژگی مشخص می شود .

زمانی که ویژگی های یک فایل می توانناددرثبت MFT جای گیرند . آنها ویژگی های مستقر دارند . برای مثال اطلاعاتی مثل نام فایل و نشان زمان همیشه در ثبت فایل MFT جای دارند . زمانی که تمام اطلاعات یک فایل برای جای گرفتن در ثبت فایل MFT بسیار بزرگ هستند ، بعضی از ویژگی های آن مستقر نمی شوند . ویژگی های غیر حاضر یک یا بیشتر دسته های فضای دیسک را در هر جایی بر روی نسخه تعیین می کنند . NTFS برای توصیف محل تمام ثبت ویژگی ها ، یک لیست ویژگی (مشخصات) را ایجاد می کند .

جدول 3 ـ5 تمام مشخصات فایل را توسط سیستم فایل NTFS فهرست می کند . این فهرست توسعه پذیر است ، به این معنی که دیگر خصوصیات فایل ها می توانند در آینده تعریف شوند .

جدول 3-5 خصوصیات فایل تعریف شده توسط NTFS

نوع ویژگی	توضیح
اطلاعات استاندارد	شامل اطلاعاتی مثل نشانه زمان و شمارش لینک می باشد .
لیست خصوصیات	مکان تمام ویژگی های ثبت شده ای را که در ثبت MFT جای نگرفته اند فهرست می کند .
	یک ویژگی تکرار پذیر برای اسامی کوتاه و بلند فایل . اسم یک فایل طولانی

نام فایل	می تواند تا 255 علامت باشد . نام کوتاه 3 تا 8 حرف است . نام های اضافی یا لینک های سخت که مورد نیاز POSIX هستند ، می توانند به عنوان خصوصیات نام فایل اضافی شامل شوند .
توصیف گرافیکی	اینکه چه کسی مالک فایل است و چه کسی به آن دست می یابد را شرح می دهد .
داده	حاوی دادهٔ فایل است . NTFS این امکان را می دهد که چندین داده در هر فایل پخش شود . هر فایل یک ویژگی بدون نام دارد . یک فایل می تواند یک یا چند ویژگی داده نام دار داده باشد که هر یک از معنای خاص استفاده می کند.
شناسه متغیر	یک معرف فایل نسخه منحصر به فرد ، که توسط سرویس ردیابی لینک توزیع شده مورد استفاده قرار می گیرد . تمام فایل ها معرف متغیر ندارند .

جریان ابزار ثبت شده شبیه جریان داده هاست اما عملیات درست مثل تغییرات داده های NTFS در فایل ثبت NTFS ، ضبط می شوند . این توسط EFS مورد استفاده قرار می گیرد .

مرحله تجزیه دوباره	برای مراحل تنظیم نسخه استفاده می شود . همچنین توسط راه انداز فیلتر سیستم فایل قابل نصب مورد استفاده قرار می گیرد تا فایل های مشخص را به عنوان فایل های خاص به آن درایور نشان دهد .
ریشه فهرست	برای پرونده های اجرایی و دیگر فهرست ها مورد استفاده قرار می گیرد.
تخصیص فهرست	برای پرونده های اجرایی و دیگر فهرست ها مورد استفاده قرار می گیرد.
نوشتار	برای پرونده های اجرایی ودیگر فهرست ها مورد استفاده قرار می گیرد.
اطلاعات نسخه	فقط در فایل سیستم نسخه مورد استفاده قرار می گیرد .

نام جلد (نسخه)	فقط در فایل سیستم مورد استفاده قرار می گیرد . برچسب جلد را در بردارد .

فایل های سیستم NTFS

NTFS شامل چندین فایل سیستم است . تمام آنهایی که بر روی حجم NTFS از دید پنهان هستند . یک فایل سیستم ، فایلی است که توسط برای ذخیره داده های آن و اجرای سیستم فایل استفاده می شود . فایل های سیستم بر روی حجمی واقع شده اند .

جدول 4-5 داده های ذخیره شده در جدول فایل اصلی

فایل سیستم	نام فایل	ثبت MFT	هدف فایل
جدول فایل اصلی	—	—	برای هر فایل و پرونده بر روی حجم NTFS داری یک فایل اصلی است . اگر اطلاعات تخصیص یک فایل یا پرونده برای جای گیری در یک ثبت مجزا خیلی زیاد باشند،دیگر مدارک فایل اختصاص یافته می شوند .
جدول فایل اصلی 2	—	—	یک کپی از اولین چهار ثبت MFT . این فایل در هنگام شکست یک بخش مجزا ، دسترس به MFT را ضمانت می کند .
فایل ثبت	—	—	لیستی از مراحل بهنگام سازی فایل را داراست که برای قابلیت بازیافت NTFS استفاده می شود . سایز فایل ثبت ، به اندازهٔ حجم بستگی دارد و می تواند به بزرگی 4 مگابایت باشد . ویندوز NT / 2000 بعد از یک شکست سیستم برای بازگرداندن وضعیت اولیه سازگاری به NTFS از آن استفاده می کند .
حجم	—	—	اطلاعاتی راجع به حجم از جمله برچسب حجم و نسخهٔ حجم را در بر دارد .

تعاریف خصوصیات	ـــــ	ـــــ	یک جدول از توصیفات ، اعداد و نام های خصوصیات فایل .
فهرست نام فایل اصلی	ـــــ	ـــــ	پرونده ریشه .
گروه نوشتار	ـــــ	ـــــ	یک نمایش از حجم که نشان می دهد کدام گروه ها در دست استفاده هستند .
بخش راه انداز	ـــــ	ـــــ	شامل BPB است که برای تنظیم حجم و کدبارگیر خود راه انداز استفاده می شود اگر حجم قابل راه اندازی باشد .
فایل امنیتی	ـــــ	ـــــ	شامل توصیف گر های امنیتی برای تمام فایل های داخل حجم (نسخه) است .
جدول حروف بزرگ	ـــــ	ـــــ	حروف کوچک را برای سازگاری به حروف بزرگ تبدیل می کند .
فایل توسعه NTFS	ـــــ	ـــــ	برای توسعه های اختیاری مختلف از جمله سهمیه ها ، مراحل تجزیه دوباره داده و معرف متغییر استفاده می شود .

چندین جریان داده NTFS

NTFS چندین جریان داده را پشتیبانی می کند ، جایی که نام جریان یک ویژگی جدید داده را بر روی فایل مشخص می کند . یک دستگیره می تواند به روی هر یک از جریان داده ها باز شود . پس یک جریان داده مجموعه ای از خصوصیات فایل است . این ویژگی به شما این امکان را می دهد که داده را به عنوان یک واحد مجزا مدیریت کنید . مثال زیر یک جریان متفاوت است :

یک مجموعه از فایل ها ممکن است در جایی وجود داشته باشند که در آنجا فایل ها به عنوان جریان های متفاوت تعریف شده باشند .

مانند مثال زیر :

یک فایل می تواند همزمان با بیشتر از یک برنامه کاربردی همراه شود مانند : مایکروسافت ورد و مایکروسافت ورد پد .

برای مثال : ساختار یک فایل مانند نمونه زیر یک همکاری فایل را نشان می دهد اما نه برای چندین فایل :

برای ایجاد یک جریان داده متفاوت ، در اعلان دستور می توانید دستوری چون مثال زیر را تایپ کنید .

Echo . text > program : sowrce – file

More < program : sowrce – file

مهم

هنگامی که شما یک فایل NTFS را به یک حجم FAT کپی می کنید مثل فلاپی ، جریان داده و دیگر ویژگی ها که توسط FAT پشتیبانی نشده اند از دست می روند .

فایل های فشرده NTFS

ویندوز NT / 2000 ، فشرده سازی را بر روی فایل های فردی ، پرونده ها و کل حجم NTFS حمایت می کند . فایل هایی که بر روی یک حجم NTFS فشرده می شوند ، می توانند توسط هر برنامه کاربردی ویندوز خوانده و نوشته شوند . بدون این که اول توسط یک برنامه دیگر ناهم فشرده شوند .

زمانی که یک فایل خوانده می شود ناهم فشرده سازی به طور خود کار رخ می دهد وقتی که فایل بسته یا ذخیره می شود دوباره فشرده می شود . فایل ها و پرونده های فشرده زمانی که در ویندوز اکسپلورر مشاهده می شوند ویژگی C را دارند . تنها NTFS می تواند شکل فشرده ی دیتا را بخواند زمانی که یک فایل کاربردی مثل Microsoft word یادستور اجرایی سیستم مثل copy درخواست دسترس به فایل را می کند ، راه انداز فیلتر فشرده قبل از این که آن را در دسترس بگذارد آن را ناهم فشرده می کند . برای مثال اگر شما یک فایل فشرده ویندوزNT /2000 دیگر را به یک پرونده فشرده بر روی دیسک خود کپی کنید ، فایل زمانی که خوانده می شود ، از حالت فشرده خارج می شود ، کپی می شود و سپس هنگام ذخیره دوباره فشرده می شود . این فشرده سازی بسیار شبیه عمل کاربردی ویندوز 98 است با یک تفاوت مهم ـ عملکرد محدود شده نخستین حجم یا حجم اصلی را فشرده سازی در NTFS برای حمایت از اندازۀ دسته های تا اندازۀ 4KB است . زمانی که سایز دسته بیشتر از 4 کیلو بایت است ، هیچ از عملکردهای فشرده سازی

NTFS در دسترس نیست . هر جریان داده NTFS شامل اطلاعاتی است که نشان می دهد آیا هیچ یک از بخش ها فشرده شده است یا خیر .

با فرم های فشرده شده منحصر به فرد توسط مجراها تشخیص داده می شوند . اگر مجرایی وجود نداشته باشد ، NTFS برای پیدا کردن و پر کردن مجرا به طور خود کار قبلی را فشرده می کند .

سیستم رمز گذاری فایل ـ EFS . پرونده های و پوشه های رمز گذاری شده .

سیستم رمزگذاری فایل فن آوری رمز گذاری فایل هسته ای را مهیا می کند که برای ذخیره سازی فایل های موجود در حجم NTFS استفاده می شوند . کاربران همانطور که به هر فایل و پروندۀ دیگری کار می کنند با فایل ها و پوشه های رمز گذاری شده نیز کار می کنند . رمز گزاری برای کاربری که فایل را رمز داده است ، ناپیدا نیست . تیم زمانی که کاربردسترسی به فایل داردبه طورخود کار فایل یا پرونده را کشف رمز می کند . زمانی که فایل ذخیره شد ، رمز گذاری اجرا می شود . کاربرانی که مجاز به دستیابی به فایل ها و پرونده های رمز گذاری شده نیستند ، به طور پنهانی پیغام " دستیابی ممنوع شد " را دریافت می کنند . اگر سعی در بازکردن ، کپی ، انتقال یا تغییر نام فایل رمز گذاری شده داشته باشند . پیغام دقیق ممکن است بستگی به برنامه کاربری داشته باشد که سعی در دستیابی به فایل دارد زیرا این به حق کاربر برای فایل مربوط نیست بلکه به توانایی EFS در کشف رمز فایل با استفاده از رمز اختصاصی کاربر بستگی دارد .

EFS مزیت های زیر را داراست :

1 ـ برای کاربر و هر برنامه کاربردی پنهان است . در فراموش کردن رمز گذاری فایل و ترک داده بدون محافظت ، هیچ خطری برای کاربر وجود ندارد . یک فایل یا پرونده که رمز گذاری شده ، در پشت زمینه بدون کشف متقابل با کاربر رمز گذاری می شود . کاربر لازم نیست که برای کشف رمز فایل ها ، رمز را به خاطر بسپارد .

2 ـ امنیت اصلی قوی : در مغایرت با دیگر راه حل ها ، زمانی که کلیدها بر اساس حروفی هستند که کاربر وارد می کند ، EFS کلیدهای تولید می کند که با دیکشنری هماهنگ است .

3 ـ تمام فرآیندهای فشرده سازی و نا هم فشرده سازی در حالت شالوده اجرا می شوند ، به استثنای خط رها کردن کلید در صفحه بندی فایل از جایی که می توانسته احتمالاً استخراج شود .

4 ـ EFS مکانیسم بازیافت داده را فراهم می کند که در تجارت با ارزش است ، برای ذخیره داده ها موقعیتی به آن می دهد اگر کسی که آن را رمز گذاری کرده ، شرکت را ترک کرده باشد .

EFS ـ سیستم رمز گذاری فایل : فایل ها و پرونده های رمز گذاری شده

Using EFS

کاربر می تواند خصوصیات EFS را از طریق ویندوز اکسپلورر و یا با استفاده از خط دستور که ciphn . exe نـام دارد ، درخواست نماید . برای استفاده از ویندوز اکسپلورر برای رمز گذاری فایل ، مشخصه فایل را با راست کلیک کردن بر روی نام فایل باز کنید . بر روی دکمهٔ Advance کلیک کرده ، خصوصیات Advance باز خواهد شد که به شما این امکان را می دهد که فایل را به عنوان یک فایل رمزگذاری شده علامت بزنید .

قبل از ذخیرهٔ تنظیمات جدید ویندوز به کاربر این امکان را می دهد که فقط فایل یا کل پرونده را رمزگذاری کنـد . کـه پیامد مهمی را به دنبال دارد . زمانی که فایل به تنهایی می تواند حفاظت شود، برنامه کاربردی که فایل را باز مـی کنـد ممکن است در زمان کار با پوشه کپی های موقت از فایل را ایجاد کند .

EFS - Encrypting File System. Encrypted Files and Folders (NTFS5 only)

EFS uses symmetric key encryption in combination with public key technology to protect files

اعمال درونی EFS

EFS برای حفاظت از فایل ها درترکیب با فن آوری کلید عمومی از رمز گذاری متناسب کلیدی استفاده می کند . دادهٔ فایل با الگوی متناسب رمزگذاری شده است . کلیدی که در رمزگذاری متناسب استفاده شده کلید رمز فایل نـام دارد (FEK). FEK در چرخش خودش با یک الگوریتم کلید اختصاصی/عمومی رمزگذاری شده و همراه فایل ذخیره شـده .

علت استفاده از دو الگوی متفاوت سرعت رمزگذاری است . گنجایش عمل یک الگوریتم متناسب برای رمزگـذاری مقـدار زیادی اطلاعات بسیار زیاد است . الگوریتم متناسب برای رمزگذاری حجم زیادی از اطلاعات 1000 بار سریع تر است .

به عنوان گام اول در رمزگذاری فایل ، NTFS یک فایل ثبت را به نام EFSO ایجاد می کند . که به عنوان یـک فایـل رمزگذاری شده در پرونده اطلاعات حجم سیستم بر روی همان درایو قرار دارد . پس EFS نیاز به دستیابی به محتویات Cryploapl دارد که از مهیا کننده رمز نویس اصلی مایکروسافت استفاده می کند. با بـاز شـدن محتویـات رمـز EFS کلید رمزگذاری فایل را تولید می کند (FEK) .

گام بعدی گرفتن جفت کلید اختصاصی است ، اگر آن در این مرحله وجود نداشته باشد ، EFS یک جفت جدید را تولید می کند . EFS برای رمزگذاری FEK از الگوریتم 1024-bitRSA استفاده می کند .

پس EFS برای کاربر رایج ، فیلد رمزگشایی داده را ایجاد می کند (DDS) که جایی که FEK را قرار داده و آن را بـا کلید عمومی رمزگذاری می کند . اگر عامل بازیافت توسط قوانین سیستم تعریف شده باشد EFS همچنین فیلد بازیافت داده (DRF) را ایجاد می کند و FEK رمزگذاری شده را با کلید عمومی عامل بازیافت در آنجا قرار می دهد . برای هر عامل بازیافت تعریف شده یک DRA جدا ایجاد می شود . لطفاً توجه کنید که در ویـنـدوز XP ، هـیچ عامـل بازیـافتی تعریف نشده بنابراین این مرحله حذف می شود .

حالا یک فایل موقت EFSO.tmp در همان پرونده به عنوان فایلی که قبلاً رمزگذاری شده ایجاد می شود .

محتویات فایل اصلی بعد از آنکه فایل اصلی با داده رمزگذاری شده دوباره نوشته می شود ، به فایل موقت کپی می شود .

به طور پیش فرض ، EFS برای رمزگذاری داده فایل از الگوریتم DESX به همراه کلیه 128 بایت استفاده می کند اما ویندوز نیز می تواند برای استفاده از الگوریتم 3DES قویتر به همراه کلید 168 بایت پیکربنـدی شـود . در ایـن مـورد استفاده از الگوریتم های موافق باید با قوانین LSA مطابقت کند .

تصویر

EFS بـرای تشـخیص اینکـه از DESX اسـتفاده مـی شـود یـا از 3DES ، از پایگـاه داده اسـتفاده مـی کنـد . اگـر HKLMXSYSTEM\Current\Control set\Control\LSA\EipsAlgorithmPolicy=1 پس از 3DES استفاده می شود . اگر نه EFS .

HKLM\Software\Microsoft\Windows NT\Currentversioul EFS\Algorithm ID

را چک می کند ، اگر حضور داشت ، CAIG-3DES یا CAIG-DESX را دارد ، در غیر این صورت از DESX باید استفاده شود . پس از اینکه رمزگذاری انجام شد ، فایل های موقت و ثبت حذف می شوند .

تصویر

پس از رمزگذاری فایل تنها کاربرانی که DDE یا DRF وابسته را دارند می توانند به فایل دسترسی پیدا کنند . این مکانیسم از معنی امنیتی رایج جداست . فایل باید به همراه کلید عمومی کاربر ، FEK رمزگذاری شده را نیز داشته باشد . تنها کاربرانی که با استفاده از کلید اختصاصی خود توان رمزگذاری FEK را داشته باشند می توانند به فایل دست یابند . نتیجه این است که کاربر که به فایل دسترسی پیدا می کند می تواند آن را رمزگذاری کند و بنابراین مانع از دسترسی صاحب آن می شود . در ابتدا برای کاربری که فایل را رمزگذاری کرده ، تنها یک DDF ایجاد می شود اما بعداً می تواند به حلقهٔ کلیدها کاربران دیگر را هم اضافه کند . در این مورد EFS می تواند به آسانی FEK را با استفاده از کلید اختصاصی کاربری که می خواهد به فایل کاربر دیگر دسترسی پیدا کند ، رمزگشایی کند . فرایند رمزگشایی برخلاف رمزگذاری است : ...

تصویر

در ابتدا این مورد را کنترل می کند که آیا کاربر کلید اختصاصی دارد که با EFS استفاده شود یا نه . اگر دارد ، آن کلید ویژگی های EFS را می خواند و در میان حلقه DDE به دنبال DDE می گردد برای کاربر رایج . اگر DDE پیدا شد ، کلید اختصاصی کاربر برای رمزگشایی FEK استخراج شده از DDE استفاده می شود . با استفاده از FEK رمزگشایی شده ، EFS داده فایل را رمزگشایی می کند . باید به این مورد توجه شود که هرگز تمام فایل رمزگشایی نمی شود اما نسبتاً توسط بخش هایی از آن است که مدل بالاتر بخش خاصی را درخواست می کند .

فرایند بازیافت شبیه رمزگشایی است به جز این مورد که برای رمزگشایی FEK از کلید اختصاصی عامل بازیافت در DRE استفاده می کند نه در DDF .

قوانین DRA برای ویندوز 2000 و ویندوز XP متفاوت عمل می کند . به طور پیش فرض در ویندوز 2000 بر روی کامپیوتر ها کنترل کننده سیستم به قوانین کلید عمومی به عنوان عامل بازیافت داده های رمزگشایی شده اضافه می

شود . بنابراین زمانی که کاربر فایل را رمزگذاری می کند ، هر دو زمینه DRF و DDF ایجاد می شود . اگر DRA آخر نیز حذف شود ، تمام عملکرد EFS پایان می یابد و دیگر امکان رمزگذاری فایل وجود ندارد .

EFS - Encrypting File System. Encrypted Files and Folders (NTFS5 only)

ویژگی EFS

زمانی که NTFS فایل را رمزگذاری می کند ، کدها را نیز رمزگذاری کرده برای فایل و ویژگی EFS را بـرای فایـل در جایی که DDFS و DDRS را ذخیره می کند ، ایجاد می کند . این ویژگـی در NTFS خصوصـیت IO=0×100 را دارد و می تواند بر اساس تعداد DDES و DRFS هنگام کپی کردن از 0.5K تا چندین کیلـو بایـت ، بسـیار طـولانی شود .

اینجا نمونه ای از ویژگی EFS با جزئیات بیشتر شرح داده شده :

ـ اندازه ویژگی EFS

ـ SID کامپیوتر و شماره کاربر که پرونده را که در آن EFS تأییدیه را ذخیره می کند مشخص می کند . برای گرفتن نام پرونده ، EFS بعضی مشابهت را به وجود می آورد :

داده در EFS ذخیره شده 5A56

ذخیره شده

به دهدهی تبدیل می شود

پیشوند SID اضافه می شود

بنابراین پوشه خواهد بود :

%User Profile % \ Applicatin Data\ Microsoft \Crypto\RSA\S-1-5-21-2025018970-693384732-167712168-12321

ـ اثر شست کلید عمومی

ـ راهنمای کلید اختصاصی (همچنین به عنوان نام محافظ استفاده می شود) . اگر در ویژگی EFS فقط یـک DDF وجود داشته باشد ، نام محافظ می تواند EFS نشان داده شود ، اما به محض اینکه کاربران بیشتری به فایل اضافه شوند ، راهنمای PK برای تمام آنها ذخیره نشده و باید بر اساس اثر کلید عمومی از انبار تأییدیه دوباره بازیافت شود .

ـ نام مهیا کننده رمزساز = مهیا کننده رمزساز مایکروسافت V.I.O

ـ FEK رمزگذاری شده . معمولاً FEK در 128 بایت طول می کشد اما از زمانی کـه بـا 1024 بایـت کلیـد RSA رمزگذاری شده ، طول رمزگذاری نیز 1024 بایت است .

EFS - Encrypting File System. Encrypted Files and Folders (NTFS5 only)

نتایج همراه با EFS

فایل موقت پاک نشده است . زمانی که EFS فایل را رمزگذاری می کند ، محتویاتش را به فایل مخفـی موقـت بـه نـام EFSO.tmp در همان پرونده ، به عنوان فایل رمزگذاری شده، کپی می تواند . پس EFS مـتن سـاده را بـا بـلاک هـا رمزگذاری کرده و داده ها رابه فایل اصلی می نویسد . پس ازاینکه فرایند انجام شد ، فایل موقت حذف می شود . مشکل اینجاست که EFS به آسانی آن را بدون پاک کردن محتویاتش پاک می کند . که دستیابی به داده حفاظـت نشـده را از طریق

Low-Level data recovery software like Active @ Undelete

آسان می کند . راه حل آن نیز ـ پاک کردن فضای خالی دیسک است . حتی اگر متن سـاده دوبـاره نوشـته شـده و اثـر مغناطیسی کوچک قابل آشکار سازی باقی بماند ، بنابراین شانس خواندن داده های پاک شده را با تجهیـزات درسـت بـه آن می دهد . برای به حداقل رساندن این امکان ، از نرم افزار در دسترس تجاری بـرای تهیـه ZDelete.net یـا data erasing algorithm like active@eraer پیشرفته استفاده کنید .

در پرونده رمزگذاری شده اسامی فایل حفاظت نشده است . در واقع رمزگذاری محتویات پوشه بـه معنـای بـه کـارگیری خودکار رمزگذاری برای تمام فایل ها در پرونده است نه رمزگذاری فهرست داده ها به تنهایی . از زمانی که فایل می تواند اطلاعات حساس رادربرمی گیرد ، می تواند در امنیت یک قانون شکنی به حساب آید .

یکی از راه حل ها استفاده از آرشیو Zip رمزگذاری شده به جای پرونده هاست که با ویندور XP تقریباً همانـند پرونـده ها رفتار می کند . بنابراین ، فقط یکی از فایل ها برای رمزگذاری لازم است و خود داده های آرشـیو شـده بـرای شـکاف برداشتن سخت ترند . ویندوز از تمام کلیدهای اختصاصی محافظت می کند با رمزگذاری آنها از طریـق سـرویس مخـزن حفاظت شده . مخزن خفاظت شده تمام کلیدهای اختصاصی را رمزگذاری کرده ، از کلید اصلی 512 بایت استنتاج کرده و آنها را در

%User profile % \Application Data\Microsoft\Crypto\RSA\UserSID

ذخیره می کند . کلید اصلی توسط کلید رمزگذاری کلید اصلی که از رمز کاربر توسط استفاده از رمـز وابسـته بـه نقـش استخراج کلید استنتاج شده ، رمزگذاری می شود و در

%User profile % \Application Data\Microsoft\Protect\UserSID

ذخیره می شود . برخلاف تلاشها ویندوز از کلیدها محافظت می کند . این واقعیت که تمام اطلاعات در کامپیوتر محلـی ذخیره شده ، به مهاجمی که قصد دستیابی به درایو را دارد ، شانس نمایش کلیدها و استفاده از آنها در رمزگشـایی داده های حفاظت شده را می دهد . امنیت کلی می تواند توسط رمزگذاری کلیدهای اختصاصی به همراه کلید سیستم عمدتاً افزایش یابد .

برنامه سودمند Syskey.exe می تواند برای ذخیره کلید سیستم بـر روی فلاپـی و پـاک کـردن آن از کـامپیوتر مـورد استفاده واقع شود . در این مورد کاربر باید از زمانی که سیستم بالا می آید ، یک دیسکت را با کلید سیسـتم وارد کنـد . اگر چه که این روش باید با احتیاط انجام شود زیرا اگر دیسکت گم شود ، راهی برای دستیابی به کامپیوتر وجود ندارد .

فایل های یدکی NTFS

یک فایل یدکی ویژگی دارد که باعث می شود زیر سیستم I/O تنها به داده های معنی دار اختصاص یابد . دادهٔ غیر صفر بر روی دیسک اختصاص دارد ولی دادهٔ بی معنی این طور نیست . زمانی که فایل یدکی خوانده می شود ، دادهٔ اختصاص یافته همانطور که ذخیره شده بود باز می گردد . دادهٔ اختصاص نیافته باز می گردد ، به طور پیش فرض به عنوان 0 .

NTFS جریان دادهٔ یدکی را باز می ستاند و فقط دیگر داده ها را به عنوان اختصاص یافته نگه می دارد . زمانی که یک برنامه به یک فایل یدکی دست می یابد ، سیستم پرونده ها ، دادهٔ اختصاص یافته را به عنوان داده واقعی جاری می کند و داده ها به عنوان صفر باز می ستاند .

NTFS شامل حمایت کامل فایل یدکی برای هر دو فایل فشرده و غیر فشرده می باشد . NTFS اعمال روی فایل های یدکی را از طریق برگرداندن دادهٔ اختصاص یافته و دادهٔ یدکی ، می خواند . اگر چه که NTFS کل مجموعه داده هـا را به طور پیش فرض بر می گرداند اما این امکان وجود دارد که یک فایل یدکی را به عنوان دادهٔ اختصاص یافته و گروهـی از داده ها خواند ، بدون بازیافت کل مجموعهٔ داده ها .

با مجموعه ویژگی های فایل های یدکی ، سیستم پرونده ها می تواند داده از هر جایی در فایل بازستاند و زمانی که یـک برنامه کاربردی در حال اجراست ، دادهٔ صفر را به جای ذخیره کردن و بازگرداندن آن به دادهٔ واقعی ، واگذار مـی کنـد . وجه مشترک برنامه کاربردی سیستم پرونده ها به فایل این امکان را می دهد که به عنوان بایت واقعی کپی یا برگردانـده شود . نتیجه ویژه دستیابی مؤثر مخزن سیستم پرونده هاست . شکل بعد نشان می دهد که چطور داده یا بدون مجموعه ویژگی فایل یدکی ذخیره می شود .

تصویر

مهم

اگر شما یک فایل یدکی را به سیستم FAT و یا یک حجم NTFS بدون ویندوز 2000 کپی یا انقال دهید ، فایـل بـه سایز مشخص اصلی خود ساخته می شود . اگر فضای مورد نیاز در دسترس نباشد ، برنامه کاربردی آن را کامل نمی کند .

قابلیت بازیافت و تمامیت داده با NTFS

NTFS یک سیستم پرونده قابل بازیافت است که پایداری یک نسخه را با اسـتفاده از فـن آوری بازیافـت و ورودی داده استاندارد تضمین می کند . در زمان توقف یک دیسک ، NTFS ثبات را با استفاده از اجرای یک روش بازیافـت کـه بـه اطلاعات ذخیره شده در یک فایل ثبت دست پیدا می کند ، ذخیره می کند .

روش باز یافت NTFS درست است . در حالی که این موضوع را که نسخه به یک مکان پایدار ذخیره شده را تضمین می کند . ورودی داده نیازمند حجم کوچکی از منابع است .

NTFS همچنین برای به حداقل رساندن تأثیرات یک بخش بد بر روی نسخه NTFS ، از تکنیکی به نام مسیر دهی دوباره گروهی استفاده می کند .

مهم

اگر ثبت راه انداز اصلی (MBR) یا بخش راه انداز خراب شد ، شما ممکن است قادر به دستیابی به اطلاعات روی نسخه نباشید .

بازیافت داده با استفاده از NTFS

NTFS هر عمل کاربردی I/O را یک فایل را روی نسخه NTFS اصلاح می کند ، به عنوان یک تبادل اطلاعات می بینید و با هر یک از آنها به عنوان یک واحد درست رفتار می کند .

NTFS برای اطمینان از اینکه یک تبادل اطلاعات می تواند کامل شود یا به وضعیت قبلی برگردد ، برنامه های کاربردی یک تبادل اطلاعات را قبل از اینکه به دیسک نوشته شوند در یک فایل ثبت ، ضبط می کند . زمانی که یک تبادل کامل در فایل ثبت ضبط شد ، NTFS برنامه های کاربردی تبادل را بر روی مخزن نسخه انجام می دهد . پس از اینکه NTFS مخزن را به روز کرد ، تبادل را از طریق ضبط آن در یک فایل ثبت انجام می دهد .

زمانی که تبادل انجام شد ، NTFS مطمئن می شود که تمام تبادل بر روی نسخه ظاهر می شود . حتی اگر دیسک متوقف شود . در طول عمل بازیافت ، NTFS هر یک از تبادلات انجام شده ای را که در فایل ثبت یافت می شود دوباره انجام می شود دوباره انجام می دهد . پس NTFS تبادلی را در فایل ثبت تعیین محل می کند که در زمان توقف سیستم انجام نشده است . اصطلاحات تکمیل نشده از ورود به نسخه منع شده اند .

NTFS برای ورود تمام اطلاعات انجام نشده یا دوباره انجام شده برای یک تبادل از سرویس فایل ثبت استفاده می کند . NTFS از اطلاعات دوباره انجام شده برای تکرار تبادل استفاده می کند . اطلاعات انجام نشده NTFS را قادر می سازند که تبادلی را که ناتمام است و یا خطا دارد را انجام ندهد .

مهم

NTFS برای تضمین این موضوع که ساختار نسخه ایرادی ندارد ، از بازیافت و ورودی داده های تبلولی استفاده می کند . به همین خاطر پس از توقف سیستم ، تمام فایل های سیستم در دسترس باقی می مانند . با این وجود به خاطر توقف سیستم و یا یک کد بخش بد ، داده های کاربر می تواند از دست بروند .

مسیر دهی دوباره گروه

در هنگام خطای یک بخش بد ، NTFS فن آوری بازیافتی به نام مسیر دهی دوباره گروه را به کارمی برد. زمانی که ویندوز 2000 یک بخش بد را تشخیص می دهد ، NTFS به طور دینامیکی گروهی را که شامل بخش خراب هستند مسیر دهی دوباره کرده و گروه جدیدی را برای داده ها تعیین می کند . اگر در هنگام خواندن خطایی رخ داد ، NTFS خطایی را به برنامه در حال اجرا بر می گرداند و داده از بین می رود . اگر خطا در حین نوشتن روی دهد ، NTFS داده را در یک گروه جدید می نویسد و داده از بین نمی رود .

NTFS آدرس گروهی را که حاوی بخش معیوب است در فایل گروه معیوب قرار داده و بنابراین بخش معیوب دوباره استفاده نمی شود .

مهم

مسیر دهی دوباره به گروه یک پشتیبانی متفاوت نیست . زمانی که خطا تشخیص داده شد ، دیسک باید از نزدیک بازبینی شود و اگر فهرست تشخیص رشد کند باید دوباره جایگزین شود . این نوع خطا در ثبت رویداد نشان داده شده است .

65536	4194304	تقریباً نا محدود	تقریباً نا محدود	بیشترین فایلها بر روی نسخه
2GB(فقط توسط) اندازه نسخه محدود می شود	4GB minus 2 Byte	فقط توسط اندازه نسخه محدود می شود	فقط توسط اندازه نسخه محدود می شود	بیشترین اندازه فایل

65520	4177918	تقریباً نا محدود	تقریباً نا محدود	بیشترین تعداد گروه ها
استاندارد 3_8 توسعه یافته ، بیشتر از 255	بیشتر از 255	بیشتر از 255	بیشتر از 255	بیشترین اندازه نام فایل

ویژگی های سیستم پرونده

مجموعه حروف سیستم	مجموعه حروف سیستم	مجموعه حرف سیستم	مجموعه حروف	مجموعه حروف اینکد	اسامی فایل های اینکد
دومین کپی از FAT	دومین کپی از FAT	دومین کپی از FAT	فایل بازیافت FAT	فایل بازیافت FAT	بازتاب مدارک سیستم
اولین بخش	اولین بخش	اولین بخش و کپی در بخش b	اولین و آخرین بخش	اولین و آخرین بخش	محل بخش راه انداز
مجموعه استاندارد	مجموعه استاندارد	مجموعه استاندارد	استاندارد ورایج	استاندارد و رایج	ویژگی های فایل
خیر	خیر	خیر	بلی	بلی	جریانات متفاوت
خیر	خیر	خیر	بلی	بلی	فشار
خیر	خیر	خیر	خیر	بلی	رمزگذاری
خیر	خیر	خیر	بلی	بلی	مجوز متغییر
خیر	خیر	خیر	خیر	بلی	سهمیه دیسک
خیر	خیر	خیر	خیر	بلی	فایلهای یدکی
خیر	خیر	خیر	خیر	بلی	مراحل تجزیه

					مجدد
خیر	خیر	خیر	خیر	بلی	مراحل تنظیم نسخه
خیر	اجرای کلی خیر	خیر	بلی	بلی	ساخت در امنیت
خیر	خیر	خیر	بلی	بلی	قابلیت باز یافت
بالا	بر روی نسخه های کوچک بالا و بر روی نسخه های بزرگ پایین	بر روی نسخه های کوچک بالا و بر روی نسخه های بزرگ پایین	بر روی نسخه های کوچک پایین و بر روی نسخه های بزرگ بالا	بر روی نسخه های کوچک پایین و بر روی نسخه های بزرگ بالا	کارایی
زیاد	بر روی نسخه های بزرگ کم	متوسط	زیاد	زیاد	صرفه جویی در فضای دیسک
متوسط	متوسط	کم	زیاد	زیاد	مقاوت عیب