SOUBOROVÝ SYSTÉM NTFS A ÚDRŽBA OS WINDOWS

- **Charakteristika NTFS**
- **Vnitřní struktura NTFS**
- **Porovnání s FAT**
- **Metasoubory a jejich funkce**
- **Struktura logického disku NTFS**
- **Registr Windows**
- **Bod obnovení**
- **Defragmentace disku**
    - **Programy pro údržbu OS**
- **Bezpečné odstraňování dat**

Charakteristika NTFS

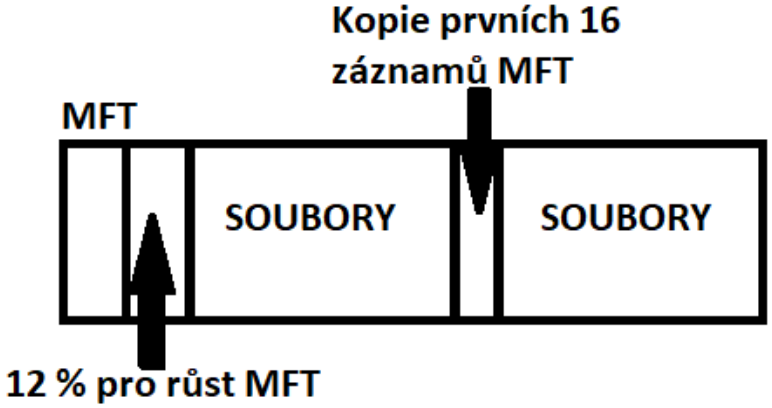
- Zkratka NTFS znamená New Technology File Systém
- Jedná se o souborový systém
    - Souborový systém je sada pravidel, podle kterých OS organizuje data na logickém disku
- Při své práci využívá transakce
    - Transakce je několik dílčích akcí
        - Zápis na disk je rozdělen na
            - Přenos dat do řadiče
            - Vyhledání volného místa na disku
            - Vlastní zápis dat
            - Uložení informaci o poloze zapsaných dat do tabulky logické struktury
    - Podstata transakce spočívá v tom, že se buď provede, nebo se neprovede vůbec
        - Pokud by došlo k havárii některého z kroků, neprovede se nic
        - Nemůže tedy dojít ke ztrátě clusteru jako u FAT
- Výhody NTFS
    - Žurnalování
        - Všechny zápisy na disk se zároveň zaznamenávají do speciálního souboru = žurnálu ($LOGFILE)
        - Pokud uprostřed zápisu systém havaruje, je následně možné podle záznamu všechny rozpracované operace dokončit, nebo zrušit
    - Přemapování clusterů při zápisu
    - Komprese dat je zapracována přímo NTFS
    - Oprávnění pro složky a soubory
        - Popisují co muže nebo nemůže uživatel provádět s daty ve složky (práva uživatelů)
    - Diskové kvóty
    - Šifrování dat – přímo na úrovni souborového systému
    - Vylepšená správa dat
        - Není omezen počet složek v ROOTu
        - Svazky do velikosti 2 TB u MBR, u GPT větší
        - Při vyhledávání je minimalizován počet přístupu na disk
    - Celý systém je řešen jako velká databáze, kde jeden záznam odpovídá souboru
    - Základ tvoří 11 systémových souborů = METADAT (vznikají po naformátování svazku)

NTFS vs. FAT

- FAT je kompatibilní se všemi OS, zatímco NTFS nemusí pracovat s Linuxem nebo Mac OS
- FAT je starší
- NTFS využívá transakce, tudíž nedojde ke ztrátě clusteru, protože transakce se buď provede celá úplně, nebo vůbec
- NTFS zálohování dat do speciálního souboru = žurnálu, tomuto procesu se říká žurnálování
- NTFS umí nastavit přístupová práva k souborům
- U NTFS může mít diskový oddíl větší maximální kapacitu než u FAT

Vnitřní struktura NTFS

- Prostor NTFS je rozdělen na dvě části
    - MFT +12% rezerva pro růst MFT (aby nemusela být fragmentována)
    - Soubory
        - Uprostřed kopie prvních 16 záznamů MFT a pak opět soubory
- MFT se nachází hned za boot sektorem
    - Bootovací záznam NTFS disku obsahuje pozici MFT i její kopii



Metasoubory

- Jde o prvních 16 záznamů na disku
- V metasouborech je zaznamenána organizace dat v clusterech
- MFT = Master File Table
    - je to sám o sobě souborem
    - Je základním souborem celé struktury NTFS – má stejný význam jako FAT tabulka
    - V MFT jsou uloženy všechny informace o souborech
        - Jméno, velikost, poloha fragmentu, atributy
- MFT je tvořena jednotlivými záznamy pevné délky a každý z nich koresponduje s nějakým souborem na disku
    - Prvních 16 záznamů je určeno pro vnitřní potřebu systému = metasoubory, mají fixní umístění na disku hned za boot recordem NTFS disku
    - Prvním záznamem v MFT je info o samotné MFT
    - Kopie prvních 16 záznamů je kvůli spolehlivosti uložena ve středu disku ($MFTMirr)
- Metasoubory jsou uloženy v kořenové složce a začínají $, ale nejsou viditelná
    - $MFT = Master File Table
    - $MFTMirr = kopie prvních 16 záznamů MFT, umístěná ve středu disku
    - $LOGFILE = transakční logovací soubor
    - $VOLUME = sériové číslo svazku, čas vytvoření
    - $ATTRDEF = definice atributů
    - $BITMAP = obsahuje mapu použití clusterů (1 – použité, 0 – volno)
    - . = kořenový adresář disku
    - $BOOT = boot record jednotky
    - $BADCLUS = seznam vadných clusterů na disku
    - $QUOTA = obsahuje info o uživatelských kvótách
    - $UPCASE = přidělení velkých znaků malým

Registr Windows

- V registru jsou uloženy veškeré údaje o HW PC, uživatelích, instalovaném SW, konfiguraci
- Jedná se o obrovskou databázi
- Počet záznamů se pohybuje kolem 50 000 – 100 000
- Registry jsou členěny do klíčů a podklíčů
- Struktura je hierarchická (stromová) rozdělená do 5 základních větví (klíčů)
- Klíče registru
    - Hkey_Classes_Root
        - Popisuje nastavení programů
    - Hkey_Current_User
        - Popisuje nastavení uživatele, který je právě přihlášen
    - Hkey_Local_Machine
        - Konfigurační údaje místního PC (info o ovladačích, připojení k síti, modemech, SW)
    - Hkey_Users
        - Údaje o uživatelích, kteří se mohou přihlásit
    - Hkey_Current_Config
        - Informace o aktuální konfiguraci HW
- Registry si lze prohlédnout v Editoru registrů pod Windows
- Odstranit chyby v registru lze pomocí programu, např. TuneUp, Norton Utilities

Bod obnovení

- Bod obnovení obsahuje informace o změnách v souborech, které byly provedeny od posledního pořízení snímku svazku
- Standardně jsou automaticky body obnovení vytvářeny každých 7 dní
- Dále jsou vytvářeny automaticky před započetím následujících úkonu
    - Instalace SW, aktualizaci OS, zálohování
- Obnovení systému do původní podoby lze provést, pokud jsme nainstalovali program, který dělá potíže, nefunguje správně, nebo jsme naistalovali ovladače, které narušují výkon, anebo pokud PC vykazuje problémy se stabilitou bez zjevné příčiny

Fragmentace

- Fragmentovaný soubor je takový, který není uložený do řetězce clusterů následujících za sebou – je rozházený po disku (leží na několika různých cylindrech)
- Takový soubor bude z disku načítán pomaleji
- Program pro záchranu dat má menší šanci opravit případné chyby vznikající při zápisu správně
- Fragmentace vzniká častým mazáním a zápisem nových souborů, které jsou delší než uvolněné místo po těch vymazaných

Defragmentace

- Defragmentace znamená, že program spojí jednotlivé fragmenty souboru do jednoho celku tím, že jej přesune na místo, kam se soubor vleze celý
- Defragmentační programy:
  - V OS je to defragmentace
  - O&O Defrag
  - Diskeeper

Mazání souborů z disku (platí pro FAT)

- Je rozdíl mezi vhozením do koše a skutečným vymazáním souboru a bezpečným odstraněním souborů z disku
  - Vhození do koše pouze přesun souboru do složky KOŠ
  - Vymazání souborů znamená v OS přesání prvního znaku názvu souboru v adresáři znakem E5h, OS dále přepíše celý řetězec záznamů ve FAT tabulce číslem 0 – pro OS to znamená, že tyto clustry muže použít pro zápis, ale obsah souboru nadále zůstává v clustrech (v datové oblasti), dokud nedojde k jeho přepsání daty nově uloženého souboru
- Bezpečné odstranění dat – skartování
  - Neprovádí jej OS, ale specializované programy
    - WipeInfo, DiskWipe, Tune Up Shredder
  - Dojde nejen k vymazání prvního znaku názvu souboru, ale taky k odstranění celého záznamu názvu v adresáři a také k přepsání obsahu souboru novým obsahem

- KECY V KLECI, ale zní to pěkně a honosně :D
    - Tím, že ve Windows vysypete koš, nepřestanou smazaná data existovat. Ta z pevného disku fyzicky zmizí až v okamžiku, kdy dojde k jejich přepisu. Na jednu stranu tuto vlastnost oceníte při nechtěném smazání některého ze souborů, naopak v případě citlivých dat jako fotek tvojí staré či nekvalitního porna, se jich většinou chcete zbavit nadobro. Podobně lze postupovat třeba při prodeji notebooku, kde nechcete zanechat obnovitelná data jako fotky tvojí staré. S tím pomohou specializované nástroje.
    - Jejich princip je jednoduchý – přepis smazaných souborů náhodnými daty. Ať už se jedná o soubor s citlivým dokumentem nebo celý diskový oddíl, způsob zůstane stejný. Liší se pouze úroveň přepisu, na němž závisí možnost obnovení dat.
    - Tou nejrychlejší a nejsnadnější možností je jeden přepis. Ačkoliv bude ve většině případů dostačovat, teoretická šance na obnovení zde stále bude existovat. Potom tedy přichází na řadu důkladnější přepis dat.
    - Jeden ze standardů amerického ministerstva obrany je označován jako NEVIM a spočívá v sedmi postupných přepisech. Nejbezpečnější je potom Gutmannova metoda, která disk přepíše celkem 35×. Po tomto zásahu data neobnoví ani ten nejlepší technik jako Hrnčiar.

Klasicky obecné souvislosti na závěr ☺ (aka vše souvisí se vším)

- Master Boot Record (způsob rozdělení disku na oddíly) používá adresování CHS
- Guid Partiton Table neboli GPT (způsob rozdělení disku na oddíly) používá adresování LBA
- Pokud máme základní desku s BIOSem, lze použit pouze Master Boot Record
- Pokud máme základní desku s UEFI, používáme GPT
- UEFI podporuje pouze souborový systém FAT32, nikoliv NTFS
- BIOS podporuje jak souborový systém FAT, tak i NTFS