

MO15. Správa souborů na disku, souborové systémy

1 Správa souborů

1.1 Souborový systém

Souborový systém (*filesystem*) je označení pro způsob organizace informací ve formě souborů tak, aby bylo možné je snadné najít a přistupovat k nim. Zabývá se umístováním a organizací souborů na nosiči, přiděluje jim atributy a přístupová práva, řídí a kontroluje přístup k datům

Může poskytovat přístup:

- > ke klasickým paměťovým médiům (pevný disk, CD...)
- > k datům uloženým na serveru (síťové souborové systémy, např. NFS, SMB nebo 9P)
- > k virtuálním datům (např. procfs v Linuxu)

Umožňuje ukládat data do souborů, které jsou označeny názvy. Obvykle také umožňuje vytvářet adresáře, pomocí kterých lze soubory organizovat do stromové struktury.

1.2 Organizace dat na disku

Pevné disky jsou obvykle logicky rozděleny na **oddíly (partition)**, takže souborový systém se rozkládá jen na konkrétním oddílu a ne na celém disku. To umožňuje mít na pevném disku **více nezávislých souborových systémů**, které mohou být různého typu.

Informace uložené v systému souborů se dělí na metadata a data:

- metadata** - popisují strukturu systému souborů a obsahují služební a doplňující informace (*velikost souboru, čas poslední změny, čas posledního přístupu, vlastník souboru, přístupová práva...*)
- data** - vlastní obsah souboru, který je možný číst, po otevření souboru

Software, který realizuje souborový systém, bývá součástí operačního systému.

1.3 Žurnálování

Žurnálování vytváří podrobné záznamy o změnách, které mají být v systému souborů provedeny. Jeho účelem je ochránit data na pevném disku v případě neočekávaných havárií (výpadek napájení, pád systému atd).

Pokud dojde v kterémkoliv okamžiku k přerušení, je možné pomocí dat uvedených v žurnálu uvést systém souborů do konzistentního stavu buď návratem zpět ke stavu před započítím transakce nebo dokončením přerušené transakce.

Žurnálování umožňuje po havárii rychlou opravu nekonzistentních dat.

Žurnálovací souborové systémy: např. NTFS, HFS+, ext3, ReiserFS

1.4 Síťové souborové systémy

Síťové souborové systémy (*network filesystem*) je označení pro systémy souborů, které jsou dostupné prostřednictvím počítačové sítě.

Soubory a adresáře leží na jiném počítači a přistupujeme k nim pomocí speciálních síťových volání služeb. Na vzdáleném počítači jsou pak soubory a adresáře fyzicky uloženy v podobě klasického systému souborů.

Síťové souborové systémy: např. NFS, SMB, CODA

1.5 Některé souborové systémy

Operační systémy podporují tyto souborové systémy:

DOS - FAT

Windows - FAT, NTFS

Linux - ext2, ext3, ReiserFS, JFS, XFS, FAT, NTFS a mnoho dalších

Solaris - UFS, ZFS a mnoho dalších

Souborový systém ISO 9660 pro ukládání souborů na CD/DVD podporuje většina OS.

1.5.1 FAT (File Allocation Table)

- jednoduchý souborový systém, je podporován téměř všemi operačními systémy

- FAT16** - používá 16 bitů na adresaci clusteru
 - maximální možná velikost logického disku 2GB
- FAT32** - používá 32 bitů na adresaci clusteru
 - limit disku 128 GB
 - maximální velikost souboru 4 GB

1.5.2 NTFS (New Technology File System)

- vyvinut firmou Microsoft a IBM pro operační systém Windows NT

- podporuje:

- > žurnálování
- > access control list - podpora pro přidělování práv k souborům
- > šifrování - šifrování a dešifrování dat při jejich zápisu na disk a opětovném čtení
- > dlouhá jména souborů
- > ...

- používá 64 bitů na adresaci clusterů

1.5.3 ext3

- open-source souborový systém, používá se především v Linuxu

- vychází a navazuje na předchozí **ext2**, rozšířen o žurnálování

1.5.4 reiserFS

- vyvinut firmou Namesys, podporován především Linuxem

- u mnoha distribucí nastaven jako výchozí systém

- žurnálování

- dosahuje vysokého výkonu s mnoha malými soubory

2 Soubory

2.1 Soubor, adresář

Soubor - pojmenovaná posloupnost záznamů, se kterou lze manipulovat jako s celkem

- slouží k trvalému uložení informace
- nacházejí se na vnějších paměťových nosičích (pevný disk, CD...)

Adresář - organizační jednotka v souborovém systému

- může obsahovat soubory a podadresáře
- slouží ke zpřehlednění, tvoří stromovou strukturu

2.2 Typy souborů

- **řádné(regular)** - **textové** – data, které lze přímo tisknout, speciální případ binárních
- **binární** – sekvence bajtů
- **knihovny(directory)** - slouží k vytvoření struktury souborového systému
- **speciální znakové soubory** - pro sériový vstup/výstup

Každý soubor má svůj název, délku a případně další atributy požadované operačním systémem. Obsahem souboru mohou být různá data, textová a binární.

Datové soubory

Obecně jakýkoli soubor, který obsahuje údaje s informační hodnotou.

Binární soubory

Označení pro soubor obsahující kromě běžných znaků i speciální (řídící) symboly z celého rozsahu ASCII. Soubory s touto vlastností se označují jako binární právě z důvodu využití kompletní sady znaků, tedy vnitřně z posloupnosti nul a jedniček uspořádaných ve správném pořadí bez jakýchkoli dalších omezení (např. bez zakázaných znaků).

Binární soubor je nečitelný pro běžného uživatele (na rozdíl od textového souboru). Strukturu souboru v binárním tvaru dokáže rozpoznat a číst samotný systém (v případě spustitelných programů), nebo speciální aplikace (např. pro zobrazování obsahu grafických souborů).

2.3 Přípona souboru

Přípona názvu souboru (*file name extension*) je část na konci názvu souboru oddělená tečkou . od vlastního názvu souboru. Přípona názvu souboru má zpravidla délku 2 až 4 znaky. Pomocí přípony na konci souboru pozná operační systém, o jaký typ souboru se jedná.

2.4 Hierarchická struktura souborů

Způsob organizace souborů v operačním systému umožňující jejich hierarchické členění do struktury adresářů a podadresářů (složek). Celá souborová struktura začíná na disku kořenovým adresářem (root directory), který může obsahovat další adresáře (složky) a soubory, ale není podadresářem žádného jiného adresáře. Pro libovolné další adresáře pak platí, že mohou opět obsahovat soubory a podadresáře, a navíc má každý z nich jednoznačně přiřazen nadřazený adresář. Uživatel může podle svých potřeb vytvářet nebo rušit libovolné adresáře a soubory.

Výhoda hierarchického souborového systému spočívá v jeho přehledném členění do menších oblastí a podoblastí, v nichž se uživatel dobře orientuje.

3 Defragmentace, skenování disku

Defragmentace disku je systémový nástroj určený pro analýzu místních svazků a vyhledání a sloučení fragmentovaných souborů a složek.

Defragmentace je proces, který uspořádává soubory na trvalém paměťovém médiu tak, že jsou konzistentní, tvořeny jediným souvislým sledem sektorů. Při defragmentaci lze soubory i třídit podle určitých kritérií.

Diskeeper, Windows Disk Defragmenter, PerfectDisk

Skenování disku je nástroj pro kontrolu disku, skenuje obsah disku a hledá nějakým způsobem poškozené soubory nebo oblasti disku.

4 Komprimace

Komprimační programy slouží ke zmenšení velikosti souborů, tzn. místa potřebného k uložení těchto souborů na disk.

Tyto soubory ovšem není možné bez dekomprimace opět spustit či měnit a vůbec s nimi jakkoli manipulovat (pouze celým tzv. archivem).

- **Ztrátová komprese** – při kompresi jsou některé informace nenávratně ztraceny a nelze je zpět rekonstruovat. Používá se tam, kde je možné ztrátu některých informací tolerovat a kde nevýhoda určitého zkreslení je bohatě vyvážena velmi významným zmenšením souboru. Používá se pro kompresi zvuku a obrazu (videa)
- **Bezeztrátová komprese** – obvykle není tak účinná jako ztrátová komprese dat. Velkou výhodou je, že komprimovaný soubor lze opačným postupem rekonstruovat do původní podoby.

Tyto programy používají různých komprimačních metod. Z nejznámějších jsou ARJ, RAR, PKZIP, LHARC, ZOO, atd. Komprimační programy jsou zahrnuty i v některých diskových manažerech.

5 Zálohování. zabezpečení

Zálohování

Záloha či záložní kopie je kopie dat uložená ještě na jiném nosiči či místě pro případ ztráty v původním úložišti.

Jako prevence před ztrátou dat se data nepravdělně či pravidelně ukládají z pracovního místa (např. disky serverů) na záložní média.

V případě ztráty či poškození dat na původním místě lze soubory obnovit ze záložní kopie.

U větších systémů pak bývá speciální zálohovací zařízení se zvláštním softwarem, které umožňuje ukládat velké množství dat z různých serverů v síti i s dalšími údaji (přístupová práva, umístění) velkou rychlostí na speciální výměnná média, většinou pásy. Zálohovací zařízení dokáže také data při zálohování komprimovat.

Zabezpečení

Dokumenty je možné ochránit proti jejich otevření nebo přepsání jeho obsahu:

- **Heslo pro otevření** – dokument po uzamčení není možné bez znalosti hesla otevřít. Používá se u dokumentů, které mají být přístupné pouze některým uživatelům.
- **Heslo pro zápis** – v dokumentu není možné bez znalosti hesla provedené úpravy uložit, změněný dokument je ale možné uložit pod jiným názvem. Heslo pro zápis používáme například u dokumentů, které umístíme na síťový disk a chceme zabránit jejich přepsání jinými uživateli.

Dobré heslo musí splňovat alespoň tyto podmínky:

- obsahuje malá a velká písmena, číslice a jiné znaky
- dostatečná délka
- nepředstavuje smysluplná slova

6 Viry, antiviry

6.1 Viry

Virus - program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů..

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů). Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji.

Červ (worm) - počítačový červ je zvláštním typem počítačového viru. Šíří se v podobě infikovaných souborů nebo paketů počítačové sítě. Úspěšně infikovaný systém červ využije k odeslání své kopie na další systémy v síti Internet a velmi rychle se tak rozšiřuje. Dominový efekt může mít za následek až zahlcení počítačové sítě.

Červ se na rozdíl od viru dokáže šířit sám, bez závislosti na přenosu hostitele

Dělení virů podle hledisek:

- Podle hostitele:
 - Spustitelné soubory (.COM, EXE v DOSu, EXE ve Win, ELF soubory v UNIXu...)
 - Boot sektory disket a diskových oddílů.
 - Master boot sektor (MBR) pevného disku
 - Dávkové soubory a skripty (BAT v DOSu, shellovské skripty na UNIXech...)
 - Dokumenty, které mohou obsahovat makra
 - Specializované skripty některých konkrétních aplikací.
- Podle způsobu činnosti:
 - Nerezidentní
 - vir se ve chvíli spuštění hostitele rozšíří do nalezených nenakažených souborů
 - Rezidentní
 - při spuštění se pouze uloží do operační paměti počítače, ve které zůstane až do doby vypnutí počítače, a mezitím infikuje soubory (nebo např. diskety), se kterými uživatel pracuje
 - Stealth viry
 - snaží se zamaskovat svou přítomnost v souboru tím, že se zachytí na přerušení, kudy prochází veškeré požadavky na čtení dat ze souboru (tedy i požadavky antiviru). Vir si pak kontroluje, zda se požadavek týká i infikovaného souboru, v tomto případě pak vrátí aplikaci data původního neinfikovaného souboru.

6.2 Antivirové programy

Antivir - počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného záškodného software (malware).

K zajištění této úlohy používají dvě techniky:

- Prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.
- Detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Dělení antivirů

➤ **On-demand skenery** - spouštějí se přes rozhraní OS DOS a jsou určeny pro případ, že systém není z důvodu poškození schopen nastartovat běžným způsobem.

➤ **Jednoúčelové antiviry** - jde o antivirové programy, které jsou zaměřeny na detekci, popřípadě i odstranění jednoho konkrétního viru, popřípadě menší skupiny virů. Tyto antiviry vznikají většinou k likvidaci rozšířeného viru v dané době.

➤ **Antivirové systémy** - jde o komplexní antivirové řešení, které má za úkol ochránit počítač před červy šířící se poštou, škodlivými skripty, případně zabránit stažení infikovaných souborů. Komplexní nástroj může mít ve výbavě firewall a další specializované nástroje.

Některé antiviry: AVG, Norton AntiVirus, NOD32, avast!, Spyware Doctor...