Souborový systém

Souborový systém (anglicky *filesystem*) je označení pro způsob organizace informací (ve formě souborů) tak, aby bylo možné je snadné najít a přistupovat k nim.

Souborové systémy mohou používat paměťová média jako pevný disk nebo CD, mohou poskytovat přístup k datům uloženým na serveru (síťové souborové systémy, např. NFS, SMB nebo 9P) nebo mohou poskytovat přístup k čistě virtuálním datům (např. procfs v Linuxu).

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

1 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.

Infomace uložené v systému souborů dělíme na **metadata** a **data**.

Metadata popisují strukturu systému souborů a nesou další služební a doplňující informace, jako je velikost souboru, čas poslední změny souboru, čas posledního přístupu k souboru, vlastník souboru, přístupová práva k souboru, seznam bloků dat, které tvoří vlastní soubor atd.

Pojmem **data** pak míníme vlastní obsah souboru, který můžeme přečíst, když soubor otevřeme.

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

Většina operačních systémů podporuje několik různých souborových systémů.

V Microsoft Windows nalezneme podporu pro souborové systémy FAT a NTFS a ISO 9660 pro ukládání souborů na CD a DVD.

V Linuxu nalezneme kromě již zmíněných také ext2, ext3, ReiserFS, JFS, XFS a mnoho dalších.

DOS podporuje systémy FAT, po instalaci CD/DVD driveru také ISO 9660.

Solaris podporuje především UFS a ZFS, ale i mnoho dalších.

2 Defragmentace a skenování disku

Soubory jsou uložené na pevném disku v sektorech o určité velikosti, přičemž větší soubory zabírají na disku více než jeden sektor. Jak se disk zaplňuje, stává se postupně pro systém nemožné vyčlenit pro větší soubory sektory ležící na disku vedle sebe. Přístup k datům v souboru, který je takto "rozkouskován" různě po disku, je pak značně pomalejší. Pro snadnou představu lze použít analogii s knihovnou, kde svazek knih o 7 dílech najdeme rychleji, leží-li všechny knihy v jedné poličce vedle sebe, než když leží každá kniha v jiném regálu. Podstatou defragmentace je pak fyzické přeskupení souborů na disku tak, aby soubory byly uloženy v sektorech tvořících na disku kompaktní celky. Při defragmentaci zůstává samozřejmě plně zachována původní adresářová struktura.

Defragmentace disku je časově poměrně náročná operace, která naštěstí nevyžaduje přítomnost uživatele. Konkrétní doba defragmentace závisí na velikosti disku, volném místu na disku, použitém programu, stavu disku před defragmentací atd. Jedinou podmínkou pro spuštění defragmentace je určité procento volného místa na disku (pro nástroj ve Windows XP je to 15%, pro PerfectDisk 5%). Před samotnou defragmentací doporučuji uvolnit na disku co nejvíce místa nad minimální hranici. Tím defragmentaci podstatně urychlíte a také zvýšíte její účinnost.

Defragmentaci můžete provést přímo systémovým nástrojem ve Windows nebo v některém z mnoha dostupných programů, které se liší množstvím funkcí, rychlostí a kvalitou defragmentace. Lepší programy umí pracovat i s disky na

vzdálených počítačích. V průběhu defragmentace můžete s počítačem normálně pracovat, ale musíte počítat s tím, že nepoběží příliš rychle. Proto jistě uvítáte možnost některých programů, naplánovat si defragmentaci předem na noční hodiny.

PerfectDisk, Diskeeper, O&O Defrag

Skenování disku (kontrolu integrity file systému) je vhodné spustit po nekorektním ukončení chodu počítače. Úkolem je zkontrolovat integritu souborového systému. Nedokáže opravit poškozená/ztracená data, neslouží jako náhrada za systémy pro obnovu souborů. Scandisk dokáže zjistit/opravit:

- Vadné sektory - Vytvoří záznam o vadných sektorech, které se nebudou používat
- Ztracené clustery - Ukládá nalezené položky do kořenového adresáře jako soubory s příponou ".chk"
- Opravuje nesprávně uvedená data (vytvoření/změny)
- Počítá volné místo a zapisuje jej do tabulky pro budoucí použití (výpočet volného místa je poměrně zdlouhavý, proto se provádí pouze někdy)

3 Komprimace

Při ukládání souboru (dat) se provede vynechání redundantních informací podle zvoleného (použitého) kompresního algoritmu.

3.1 Kompresní poměr

Kompresní poměr je podíl velikosti původních dat ku velikosti komprimovaných dat. Například při kompresi 10MB souboru do 2MB je poměr 10/2 = 5 (tj. 5 : 1 – pět ku jedné, pětkrát zmenšeno). Kompresní poměr je ovlivněn volbou kompresního algoritmu i typem komprimovaných dat. Úspora místa je vyjádřena jako 1 − opačný poměr, v našem příkladě 1 − 2/10 = 0,8 (tj. 80% úspora).

Například nekomprimované skladby na Audio CD mají datový tok přibližně 1,35 Mb/s, zatímco komprimované zvukové soubory (např. moderní formát AAC podporovaný přehrávačem Apple iPod či všeobecně známý formát mp3) mají typicky 128 Kb/s. Kompresní poměr je tedy asi 11 a úspora datového toku přibližně 90 %. Jedná se pochopitelně o ztrátovou kompresi, pro bezeztrátovou kompresi jsou (pro stejný typ dat) typické poměry do 2 : 1.

3.2 Huffmanovo kódování

Huffmanovo kódování je algoritmus využívaný pro bezeztrátovou kompresi dat[1]. Konvertuje znaky vstupního souboru do bitových řetězců různé délky. Znaky, které se ve vstupním souboru vyskytují nejčastěji, jsou konvertovány do bitových řetězců s nejkratší délkou (nejfrekventovanější znak tak může být konvertován do jediného bitu), znaky, které se vyskytují velmi zřídka, jsou konvertovány do delších řetězců (mohou být i delší než 8 bitů).

Nejjednodušší metoda komprese touto metodou probíhá ve dvou fázích. Prvni projde soubor a vytvoří statistiku četností každého znaku. Ve druhé fázi se využije této statistiky pro vytvoření binárního stromu a k následné kompresi vstupních dat.

Dekomprese naopak pomocí rekonstruovaného binárního stromu dekoduje řetězce proměnlivé délky.

3.2.1 Algoritmus

Uvažujme příklad, kdy je cílem zakódovat text skládající se ze čtyřech různých symbolů (s1, s2, s3, s4), jejichž četnosti výskytu v textu jsou (0,08; 0,7; 0,1; 0,12).

- Zdrojové znaky se uspořádají postupně podle pravděpodobnostního výskytu p (s2, s4, s3, s1).
- Sečteme poslední dvě pravděpodobnosti (s3 + s1 = 0,18) a výsledek zařadíme podle velikosti mezi ostatní pravděpodobnosti – redukce (s2, s13, s4).
- Znovu sečteme poslední dvě pravděpodobnosti (s13 + s4 = 0,3) a výsledek opět zařadíme podle velikosti (s2, s134).
- Sčítání pravděpodobností provádíme tak dlouho, až dojdeme k součtu 1 (s2 + s134).
- Posledním dvěma znakům přiřadíme kódové znaky 1 (s2, znak s vyšší pravděpodobností) a 0 (s134).
- Zpětným postupem přiřazujeme jednotlivým sčítancům vždy kódové znaky 1 a 0, dokud nepřiřadíme kódové znaky všem zdrojovým znakům.

- Výsledný kód znaku je sestaven ze znaků 1 a 0 podle toho, jak se daný znak seskupoval s ostatními znaky. (s134 = 0 → s13 = s1341 = 01; s4 = s1340 = 00 → s3 = s131 = 011; s1 = s130 = 010)

4 Zálohování

Jako prevence před ztrátou dat se data nepravidelně či pravidelně ukládají z pracovního místa (např. disky serverů) na záložní média. V domácnostech se mohou data z pevného disku kopírovat na diskety nebo vypalovat na CD. V případě ztráty či poškození dat na původním místě v důsledku například hardwarové poruchy, útoku viru či neúmyslného smazání 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 pásky. Zálohovací zařízení dokáže také data při zálohování komprimovat.

4.1 Typy záloh

- Úplná záloha - ukládá se kopie všech určených dat
- Rozdílová (diferenciální) záloha - ukládá se kopie jen těch souborů, které se změnily od poslední úplné záložní kopie
- Přírůstková (inkrementální) záloha - ukládá se kopie jen těch souborů, které se změnily od posledního zálohování (ať už úplného nebo i inkrementálního)

Při obnovování dat se pak musí provést kopie z úplné zálohy a poslední diferenciální zálohy nebo z úplné zálohy a všech přírůstkových záloh od poslední úplné zálohy.

5 Viry, antiviry

5.1 Malware

Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému.
Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware. V právní terminologii je malware někdy nazýván počítačová nečistota (angl. „computer contaminant“), například v zákonech států Kalifornie, Západní Virginie a několika dalších členských států USA. Malware je někdy pejorativně nazýván scumware. Jako malware by neměl být označován software, který sice obsahuje chyby, ale byl napsán pro legitimní účely.

V průběhu let autoři psali zákeřný software z různých důvodů. Mnoho dřívějších nakažlivých programů, mezi které patří internetoví červi a velký počet virů napsaných pro operační systém MS-DOS, vzniklo jako experiment nebo žert a většinou se záměrem vůbec neškodit nebo pouze obtěžovat. Mladí programátoři, kteří studovali možnosti virů a techniky jejich psaní, vytvářeli takové programy, aby ukázali, že to dovedou, nebo aby viděli, jak dalece se mohou jejich výtvory rozšířit.

Větší hrozbu představují programy navržené tak, aby poškozovaly nebo zcela mazaly data. Mnoho virů pro DOS bylo napsáno tak, aby smazaly soubory na pevném disku nebo aby poškodily souborový systém zapsáním nesmyslných dat. Síťoví červi, jako například Code Red nebo Ramen, také patří do této kategorie, protože byly napsány, aby vandalizovaly webové stránky.

Motivem pro vznik zákeřného softwaru bývá někdy pomsta. Programátor nebo správce systému, který byl propuštěn ze zaměstnání, může v systému zanechat zadní vrátka (angl. „backdoors“) nebo softwarovou „časovanou bombu“, která mu umožní poškodit v budoucnu systémy bývalého zaměstnavatele nebo zničit jeho vlastní dřívější práci.

S rozšířením širokopásmového internetového připojení vzniklo velké množství škodlivého softwaru zaměřeného čistě na zisk. Například v roce 2003 byla většina nejrozšířenějších virů a červů navržena tak, aby získala kontrolu nad napadeným počítačem pro jeho pozdější podloudné zneužití. Nakažené počítače jsou zneužity pro rozesílání spamu, šíření nezákonného obsahu, kterým je například dětská pornografie, nebo jsou zapojeny v distribuovaných útocích způsobujících nefunkčnost jiných systémů (DDoS, angl. „Distributed Denial of Service“) jako nové formě vyděračství.

Další kategorií malwaru psaného výhradně za účelem zisku je spyware, tedy programy, které monitorují uživatelem navštívené webové stránky, zobrazují nevyžádané reklamy a přinášejí tak autorovi spywaru podíl na zisku. Spyware se

nešíří způsobem obdobným počítačovým virům, obvykle se instalují zneužitím bezpečnostních chyb prohlížeče nebo jako trojské koně při instalaci jiného softwaru.

5.2 Antivir

Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se 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.

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Aktuální virové databáze se dnes nejčastěji stahují z Internetu.

5.2.1 Metody

5.2.1.1 Virové slovníky/databáze

Při kontrole souboru antivirový program zjišťuje, zda se nějaká jeho část neshoduje s některým ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má program tyto možnosti:

- pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)
- umístit soubor do karantény (virus se dále nemůže šířit, protože ho nelze dále používat)
- smazat infikovaný soubor (i s virem)

K dosažení trvalého úspěchu ve středním a dlouhém období vyžaduje virová databáze pravidelné aktualizace, které obsahují informace o nových virech. Pokud je antivirový program neaktualizovaný, představují viry přinejmenším stejné nebezpečí, jako kdyby antivir v počítači vůbec nebyl! Uživatelé mohou sami zaslat svůj infikovaný soubor výrobcům antivirových programů, kteří informaci o novém viru začlení do databáze virů.

Antivirový program fungující na platformě databáze virů kontrolují soubory v momentě, kdy je operační systém počítače vytvoří, otevře, zavře nebo je zasílá/přijímá emailem. V takovém případě je virus možné zjistit ihned po přijmutí souboru. Nutno podotknout, že uživatel může naplánovat kontrolu celého systému (pravidelně, nebo na určitý čas). Lze tedy plánovat opakované kontroly všech/části souborů, které se na jednotlivých discích nacházejí. Velmi často je antivirová kontrola naplánována ihned po startu počítače.

Ačkoli lze při kontrole za pomoci virových databází virus spolehlivě zničit, tvůrci virů se vždy snaží být o krok napřed v psaní virových softwarů pomocí "oligomorfních", "polymorfních" a stále častěji "metamorfních" virů, které šifrují část sami sebe nebo jinak upravují vlastní kód jako metodu zamaskování před rozpoznáním virovými databázemi. Dalo by se říci, že jde o jakési dynamické mutace klasických virů, které není vždy jednoduché rozpoznat.

5.2.1.2 Nebezpečné chování

Metoda zjištění nebezpečného chování se oproti virovým databázím nesnaží najít známé viry, namísto toho sleduje chování všech programů. Pokud se takový program pokusí zapsat data do spustitelného programu, antivirus například označí toto nebezpečné chování a upozorní uživatele, který je antivirovým programem vyzván k výběru dalšího postupu.

Výhodu má tento postup zjištění nových virů v tom, že ačkoli je virus zcela nový, neznámý ve virových databázích, může ho snadno odhalit. Nicméně i tato metoda má své nevýhody. Stává se, že antivirový program hlásí spoustu falešných "nálezů" viru. To může mít za výsledek, že uživatel postupem času přestane vnímat ty "pravé" varování. Pokud tedy uživatel automaticky povolí pokračování programu, je jasné, že v takovém případě antivirus neplní dále svoji funkci varovat uživatele před možným nebezpečím. Z tohoto důvodu tento postup stále více moderních antivirových programů využívá méně a méně.

5.2.1.3 Další metody

Určité antivirové programy používají další typy heuristických analýz. Například se může pokusit napodobit začátek kódu každého nového spustitelného souboru tak, že ho systém vyvolá ještě před přenosem do tohoto souboru. Pokud se program chová tak, že použije "samo-modifikační" kód nebo se jeví jako virus (pokud například začne hledat další

spustitelné soubory), můžeme předpokládat, že virus nakazil další spustitelné soubory. Nicméně i tato metoda může hlásit falešné pozitivní nálezy.

Další metoda detekce virů se týká užití tzv. sandboxu. Sandbox, neboli pískoviště, napodobuje systém a spouští .exe soubory v jakési simulaci. Po ukončení programu software analyzuje sandbox, aby zjistil nějaké změny, ty mohou ukázat právě přítomnost virů. Tato metoda může taky selhat a to pokud jsou viry nedeterministické a výsledek nastane za různých akcí nebo akce nenastanou při běhu - to způsobí, že je nemožné detekovat virus pouze z jednoho spuštění.

Existují také antiviry, které varují uživatele před viry na základě toho, jakého typu soubor je.

Perspektivní metoda, která si obvykle poradí s malware je tzv. "whitelisting". Spíše než vyhledávání jen známého zákeřného softwaru tato technika předchází spouštění všech kódů kromě těch, které byly již dříve označeny jako důvěryhodný administrátorem (uživatelem). Navíc aplikace v počítači, které jsou označeny jako malware, mají automaticky zakázáno spouštění, jakmile nejsou na "whitelist", tedy seznamu povolených programů. Dnes již existuje velké množství aplikací vytvořených velkými organizacemi, které jsou široce používané a "whitelist" je tedy tvořen především administrátory, kteří software rozpoznávají. Možné provedení této techniky zahrnuje nástroje pro automatické zálohy a whitelist procesy údržby.

6 Žurnálování v systému souborů

Zápis dat a metadat do systému souborů probíhá v několika **krocích**.

Proto nejsou data a metadata v každém okamžiku **konzistentní**.

Dojde-li v takové chvíli k havárii počítače (např. výpadek elektrického proudu, chyba hardware, software a podobně), zůstane systém souborů v nekonzistentním stavu.

Z tohoto důvodu je při dalším startu operačního systému vhodné, aby byla provedena **kontrola** a nekonzistentní data byla opravena.

K tomu může dojít **automaticky** (např. v Linuxu nebo ve Windows 95 a novějších systémech) nebo je nutné spustit kontrolu **ručně** (systémy DOS).

Celková kontrola systému souborů a všech vazeb mezi daty a metadaty je **časově velmi náročná operace**, při které navíc může dojít ke zbytečné ztrátě již částečně zapsaných informací.

Proto jsou moderní systémy souborů rozšířeny o **žurnálování**, které umožňuje po havárii rychlou opravu eventuálních nekonzistencí.

Principem techniky je uchovávání chronologického záznamu prováděných operací, do kterého se zapisují všechny prováděné činnosti.

Pokud dojde např. k výpadku napájení, je po restartu nekonzistence **opravena návratem** do předchozího zaznamenaného stavu za pomoci **záznamů z žurnálu**.

Mezi žurnálovací souborové systémy **patří** např. NTFS, HFS+, ext3 nebo ReiserFS.

7 Kvóty

Kvóty (anglicky *quota*) jsou limity nastavené správcem systému, které určitým způsobem omezují použití souborového systému.

Nejčastěji se kvóty **používají** na omezení následujících věcí:

velikosti využitého místa (*usage* nebo *block quota*)

počtu souborů (file nebo *inode* quota)

Dále může administrátor systému nastavit **varování**, tzv. *soft quota*, které uživatele informuje v případě, že se blíží ke svému limitu (který je pak nazýván *hard quota*).

Často se také nastavuje tzv. *grace interval*, který v případě potřeby umožňuje krátkodobé mírné překročení kvóty.

8 Síťové souborové systémy

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

Ve skutečnosti leží soubory a adresáře na jiném počítači a přistupujeme k nim pomocí speciálních síťových volání služeb (např. SMB, NFS, CODA apod.).

Na vzdáleném počítači jsou pak soubory a adresáře fyzicky uloženy v podobě klasického systému souborů.

Speciálními síťovými systémy souborů jsou **distribuované souborové systémy** (např. GFS v Linuxu), které se mohou rozkládat na několika počítačích, které jsou navzájem propojeny pomocí počítačové sítě.

9 Databázové souborové systémy

V poslední době se začínají objevovat souborové systémy, které se **odklánějí** od klasické **hierarchické struktury** souborů a přiklánějí se více k **databázovému pojetí** reprezentace dat založené na jejich charakteristikách, tj. například na typu souboru, datumu vytvoření, autoru a jiných metadat.

10 Soubory

10.1 Soubor

Je **pojmenovaná** uspořádaná kolekce dat uložená na nějakém datovém médiu (viz např. pevný disk, disketa, CD).

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

10.2 Přípona

Přípona souboru nebo správněji **přípona názvu souboru** (angl. file name extension) je část názvu souboru, zpravidla oddělená tečkou (.) od vlastního názvu souboru.

Přípona názvu souboru má zpravidla délku 2 až 4 znaky.

Její význam je v určení typu a obsahu souboru

11 NTFS

11.1 Vlastnosti

NTFS byl navržen jako nativní souborový systém pro Windows NT a (zejména oproti zastaralému filesystému FAT) obsahoval spoustu novinek:

žurnálování – všechny zápisy na disk se zároveň zaznamenávají do speciálního souboru, tzv. žurnálu. Pokud uprostřed zápisu systém havaruje, je následně možné podle záznamů všechny rozpracované operace dokončit nebo anulovat a tím systém souborů opět uvést do konzistentního stavu.

Access control list – podpora pro přidělování práv k souborům

kompresi na úrovni souborového systému

šifrování

kvóty

dlouhá jména souborů (ve FAT původně nebyla a ve Windows 95 je bylo třeba doplňovat značně komplikovaným způsobem)

hardlinky, symlinky – odkazy na soubory na úrovni filesystémů, známé z operačních systému UNIX. Windows pro editaci tohoto typu odkazů nemají standardní uživatelské rozhraní, ale umí je interpretovat a také je používají (Distribuovaný systém souborů na Windows server 2003 apod.).

11.2 Struktura NTFS

NTFS používá **64bitové adresy clusterů**, takže diskový oddíl může být větší než u FAT (která ve své poslední verzi používala efektivně 28bitové adresování) a to konkrétně až 16 EB (což odpovídá přibližně 17 × 10^9 TB).

Celý systém je řešen jako obří **databáze**, jejíž jeden záznam odpovídá souboru.

Základ tvoří **12 systémových souborů**, tzv. metadat, které vznikají bezprostředně po naformátování svazku.

11.3 Adresáře

Adresáře jsou v NTFS pojaty jako **speciální druh souborů**; používají jiné druhy atributů.

Na disk jsou vkládány jako **B-stromy** (což zrychluje vyhledávání) se jmény souborů a odkazy na jejich záznamy v MFT.

12 RaiserFS

ReiserFS je souborový systém vyvinutý firmou **Namesys** (vedenou a vlastněnou Hansem Reiserem).

V současné době je podporován operačním systémem Linux, ale vzhledem k otevřenosti kódu může být podpora zabudována i **dalších systémů** (existuje již implementace pro Windows).

ReiserFS byl vůbec **první** žurnálovací souborový systém, který byl přidán do jádra Linuxu (ve verzi 2.4.1).

V té době nejvyzdvihovanější výhodou před v té době nejpoužívanějším ext2 byly žurnálovací fukce na záznam změn v struktuře souborů. To umožnilo snadnou obnovu bezchybného stavu systému souborů po nenadálém výpadku (jako je pád systému nebo hardwarový reboot).

Žurnálování rovněž snižuje nebezpečí chybných záznamů a nutnost provádění zdlouhavých testů integrity).

ReiserFS používá strukturu vyváženého stromu (B+ Tree), která umožňuje rychlou správu velkého množství malých souborů.

Po uvedení souborového systému Reiser4 se ReiserFS občas nazývá Reiser3.

Nevýhodou tohoto filesystému například oproti ext3 je dlouhá doba „mountování“ a dlouhé prodlevy čtení/zápis u velkých datových kapacit (více jak 200GB).

12.1 Rozšíření

Pro jeho výhody mnoho distribucí Linuxu (například SUSE, Xandros, Yoper, Linspire/Lindows, FTOSX a Libranet) jej mají jako výchozí souborový systém.

Na přelomu roku 2006/07 společnost Novell, jež ho využívá ve svém SUSE Linuxu, oznámila, že od tohoto filesystému ustoupí a začne používat filesystém typu ext3.

12.2 Zacházení s vadnými bloky disku

Do verze 3.6.12 neexistovaly nástroje pro práci s poškozenými bloky disku. I nyní ReiserFS s nimi umí zacházet, jen když jsou v datové oblasti, v systémové oblasti mohou způsobit nestabilitu systému.