Súborový systém

- Základné pojmy
- Prístupové práva
- Atribúty
- Kvóty
- ACL
- Kryptografia
- Diskové oddiely

Súborový systém

- Poskytuje abstraktný pohľad na súbor ako postupnosť bajtov.
- Transformuje požiadavky na operácie so súbormi na operácie s diskovými blokmi.
- Organizuje:
  - sektory do blokov, bloky do skupín,
  - bloky do súborov (fyzická organizácia),
  - súbory do adresárov (logická organizácia).
- **Riadi prístup k súborom.**
- Spravuje informácie o súboroch.

i-UZOL

- *i*-uzol je dátová štruktúra reprezentujúca súbor (abstrakcia).
- Každému súboru prislúcha práve jeden *i*-uzol.
- Obsahuje odkazy na bloky s dátami súboru.
- Obsahuje všetky metadáta súboru:
  - Prístupové práva (*i_mode* 16 b), vlastníka, skupinu, príznaky,
  - veľkosť, počet blokov, počet liniek,
  - časy modifikácie obsahu súboru, mod. *i*-uzla, prístupu, zmazania, ...
  - Neobsahuje meno súboru.

Výpis obsahu *i*-uzla

- Obsah i-uzla, teda informácie o súbore (nie obsah súboru), je možné zobraziť príkazom:
  - `stat`
  - `stat /; stat .; stat /etc/passwd`
  - `stat -f /`
- Bežne však stačí použiť:
  - `ls -l; ls -id /`
  - `find`

Vlastník a skupina

- Používateľ je v systéme identifikovaný číslom UID a má priradenú skupinu GID.
- Po prihlásení sa spustí shell s UID a GID používateľa, ktorý sa autentifikoval.
- Každý proces má UID a GID (podľa toho, kto ho spustil).
- Každý súbor má vlastníka UID a skupinu GID.
- Pri otvorení súboru sa kontroluje, či proces požadujúci operáciu má k tomu oprávnenie.

Vlastník a skupina – príklad

- Zmenu vlastníka alebo skupiny súboru môže urobiť len 'root'.
- Vlastníka i skupinu je možné zmeniť naraz:
  - `chown`
  - `chown -R 0:0 /root/`
- Zmena vlastniacej skupiny súboru:
  - `chgrp`
  - `chgrp wheel /tmp`

Typy súborov

- Bity 12 – 15 (*i_mode*):
  - 0140000: pomenovaný soket
  - 0120000: symbolická linka
  - 0100000: obyčajný súbor (dáta)
  - 0060000: blokové zariadenie
  - 0040000: adresár
  - 0020000: znakové zariadenie
  - 0010000: dátovod (pipe)
- Abstrakcia súboru zahŕňa nielen používateľské dáta ale aj medziprocesovú komunikáciu a hardvér.

Prístupové práva

- Súbor má povolenia troch druhov prístupov:
  - Čítať obsah súboru (Read), váha 4,
  - Meniť obsah súboru (Write), váha 2,
  - Vykonať súbor, (eXecute), váha 1.
- pre tri skupiny používateľov:
  - bity 6 - 8: pre vlastníka (User),
  - bity 3 - 5: pre skupinu (Group),
  - bity 0 - 2: pre všetkých ostatných (Other).
- Zvyčajne sa udávajú ako číslo v osmičkovej sústave (je to prehľadné).

Prístupové práva – príklad

- Prístupové práva k súborom je možné uvádzať v osmičkovom alebo symbolickom tvare
  - `0664`
  - `u=rw,g=rw,o=r`
- Nastavenie prístupových práv k súboru:
  - `chmod`
  - `chmod +x sync.pl`
  - `chmod 700 ~`
  - `chmod g=r,o-rwx group/file.txt`
  - `chmod 660 file.txt file2.txt`
  - `chmod -R g-rw ~/group/`

Práva nového súboru

- Novovytvorený súbor má spravidla UID a GID procesu, ktorý ho vytvára (*creat, open, mkdir*).
- Prístupové práva sa nastavia podľa požadovanej hodnoty `mode` a nastavenia `umask`.
  - `mode & ~umask`
- Teda bity nastavené v `umask` budú v prístupových právach nového súboru vynechané.
- Typické hodnoty `umask` sú `0022`, `0002`.

Symbolické linky

- Prístupové práva na symbolických linkách sa ignorujú.
- Význam majú len práva nastavené na súbore, ktorý je obsahom linky.
- Napríklad:
  - `ls -l /bin/sh`

Oprávnenia “eXecute/search”

- V prípade obyčajných súborov oprávnenie **X** znamená možnosť vykonať obsah súboru
  - priamo jadrom ak ide o binárne súbory, alebo interpretovať ho ak ide o textové skripty.
- V prípade adresárov toto oprávnenie znamená možnosť “vojsť” do adresára.
  - Prístup k súboru bude zamietnutý, pokiaľ žiadateľ nemá právo vojsť do všetkých adresárov v ceste k tomuto súboru.
  - Adresár ku ktorému nemáme toto oprávnenie nemôžeme zvoliť za pracovný adresár.

Oprávnenia adresárov

- Adresár je súbor, ktorý obsahuje mená súborov v tomto adresári a čísla ich *i*-uzlov.
- Pre adresár ďalej platí:
  - Oprávnenie **R** umožňuje čítať jeho obsah, čiže zoznam súborov, ktoré sa v ňom nachádzajú.
  - Oprávnenie **W** umožňuje meniť zoznam súborov v ňom obsiahnutých:
    - teda vytvárať nové súbory,
    - premenovávať súbory,
    - vymazávať súbory.

Oprávnenia adresárov

- Príklady:
  - Je teda možné, že nemôžeme vykonávať programy z adresára kde nemáme **X**, aj keď na konkrétny program v tomto adresári **X** máme.
  - Je tiež možné vytvoriť adresár, v ktorom môžme vytvárať a mazať súbory, ale nevidíme, čo naozaj obsahuje.
    - Môžme teda so súbormi v ňom normálne manipulovať, ale mená musíme poznať.

Zvláštne oprávnenia

- Bity 9 – 11 (*i_mode*):
  - SetUID (váha 4), `u+s`,
  - SetGID (váha 2), `g+s`,
  - StickyBit (váha 1), `o+t`.
- Napríklad:
  - `ls -l /usr/bin/passwd`
  - `ls -l /bin/mount`
  - `ls -ld /tmp/`

Zvláštne oprávnenia

- *SUID* a *SGID*:
  - Na súbore spôsobia, že program sa bude vykonávať s efektívnymi právami vlastníka, resp. skupiny súboru.
  - Na adresári spôsobia, že nové súbory v ňom vytvárané, budú mať nastaveného vlastníka, resp. skupinu ako tento adresár.
- *Sticky* bit:
  - Na súbore sa väčšinou ignoruje.
  - Na adresári spôsobí, že súbor v ňom môže vymazať len vlastník (používa sa v `/tmp`).

Zvláštne oprávnenia – príklad

- Obmedzenie prístupu (mazanie, premenovanie) k súborom vo verejne zapisovateľnom adresári len pre vlastníka súboru alebo adresára:
  - `chmod o+t /tmp/`
  - `chmod 1777 /tmp/`
- Novovytvorené súbory budú mať GID ako tento adresár, nie ako vytvárajúci proces:
  - `chmod g+s /tmp/shared/`
- Program sa bude spúšťať s UID vlastníka súboru, nie s UID spúšťajúceho procesu:
  - `chmod u+s /bin/ping`

Atribúty súborov

- Atribúty v súborových systémoch založených na *ext2* umožňujú ďalej obmedziť, resp. upraviť, vlastnosti súborov.
- Dostupné atribúty (`man chattr`):
  - a, append only
  - i, immutable
  - j, journalled
  - s, secure delete (N)
  - S, synchronous write
  - t, no tail merging
  - u, undelete (N)

Atribúty súborov – príklady

- Vypísanie/zmena atribútov: `lsattr`, `chattr`.
  - `lsattr ~`
- Môže ich meniť len root
  - `chattr [-R] +-=[AsacDdIijsTtu] files`
  - `chattr +i /boot/{vmlinuz,initrd}*`
  - `chattr +a /var/log/messages`

Kvóty

- Aby neprišlo k zaplneniu súborového systému, je možné nastaviť jednotlivým používateľom limit pre spotrebovaný diskový priestor.
- Hard/soft limit.
- Manipulácia s kvótami:
  - `quota`
  - `edquota`
  - `quotacheck`
  - `quotastats`
  - `quotaon`, `quotaoff`

Zoznamy prístupových práv

- Zoznam prístupových práv (Access Control List).
- Okrem práv pre tri uvedené skupiny, umožňuje toto rozšírenie definovať práva `rwx` samostatne aj pre ďalších vymenovaných používateľov a skupiny.
  - Vlastník **`user::rwx`**
  - Vymenovaný používateľ **`user:name:rwx`**
  - Vlastniaca skupina **`group::rwx`**
  - Vymenovaná skupina **`group:name:rwx`**
  - Maska **`mask::rwx`**
  - Ostatní **`other::rwx`**

Zoznamy prístupových práv

- Zistenie ACL súboru: `getfacl file`
- Nastavenie ACL súboru: `setfacl`
  - `setfacl -m u:charlie:rwx /root`
  - `setfacl -m g:wheel:rx /root`
  - `setfacl -m m::rx /root`
- ACL sú v *Linux*-e implementované pomocou rozšírených atribútov súborov.
- Počet položiek v ACL je v *ext2* aj *ext3* obmedzený na 32.
- Výpis príkazu `ls` naznačuje prítomnosť ACL znakom '+'.

Informácie o kapacite

- Veľkosť diskového priestoru zabraného súbormi alebo adresármi je možné zistiť príkazom
  - `du`
  - `du -sh ~/*`
- Prehľad o zaplnení pripojených súborových systémov
  - `df`
  - `df -h .`

“Loopback” zariadenia

- Pripojenie súboru k zariadeniu 'loop'
  - `losetup`
  - `losetup /dev/loop0 fs.ext3`
  - `losetup -a`
  - `losetup -d /dev/loop0`
- Enkrypcia (nepoužíva sa)
  - `losetup -e blowfish /dev/loop0 en.fs`
- Môže vyžadovať zavedenie modulov do jadra
  - `modprobe cryptoloop`
  - `modprobe blowfish`

Enkrypcia blokových zariadení

- Vytvorenie šifrovaného zariadenia
  - `man cryptsetup`
  - `cryptsetup luksFormat /dev/hda1`
- Aktivovanie/deaktivovanie zariadenia
  - `cryptsetup luksOpen /dev/hda1 encdev`
  - `ls /dev/mapper`
  - `cryptsetup luksClose encdev`
- Podporuje viacero “hesiel” – LUKS.
- Pridanie/zrušenie overovacej frázy
  - `luksAddKey, luksDelKey`

Diskové oddiely

- Vytvorenie, modifikácia, výpis informácií
  - `sfdisk -l`
  - `parted -l, parted -i`
  - `fdisk`
- Vytvorenie súborového systému
  - `mkfs`
  - `tune2fs`
  - `fsck`
- Pripojenie súborového systému
  - `mount, umount`

Pripájanie diskových oddielov

- Automaticky, počas štartu systému
  - `/etc/fstab, man 5 fstab`
- nastavenia – mount options
  - `noexec`
  - `nosuid`
  - `ro, rw`
  - `user, users`
  - `acl, quota, ...`
- VFAT
  - `uid, gid, umask`

Adresárová štruktúra

- Všetky pripojené súborové systémy sú usporiadané do jediného stromu.
- Zvyčajná štruktúra: `man hier`
- Konfiguračné súbory: `/etc/`
- Log-y: `/var/log/`
- Používateľské dáta: `/home/`

Súvisiace témy

- šifrované súborové systémy
  - `cryptsetup`
- zálohovanie a obnova FS alebo jeho časti
  - `dump/restore`, `cpio`, `dd`
- spoľahlivosť, redundancia, rozšíriteľnosť FS
  - `mdadm`, `lvm`, `resize2fs`
- zmena root adresára pre proces
  - `chroot`
- bezpečnostné rozšírenia SELinux
  - `getenforce`, `man selinux`
- iné súborové systémy (ext4, reiserfs, btrfs)

Literatúra a zdroje

- Manuálové stránky
  - http://www.manpages.info
- Design and Implementation of the Ext2fs
  - http://e2fsprogs.sourceforge.net/ext2intro.html
- Security Mechanisms and Policies
  - http://www.st.cs.uni-saarland.de/edu/secdesign/mechanisms.ps
- Linux Partition HOWTO
  - http://tldp.org/HOWTO/Partition/index.html
- Poznámky k súborovému systému EXT2
  - http://www.fiit.stuba.sk/~bernat/ext2fs.pdf