UFS, vlastnosti FS, `syslog`

Úvod do administrace operačních systémů

Jan Žďárek

České vysoké učení technické v Praze
FEL, katedra počítačů

(Program STM – kód Y36UAD)

Úvod

Motivace:

1. Doplnit některé chybějící pojmy z oblasti FS.
2. Transakční žurnál.
3. Opravy FS.
4. `syslog`.

Systémy souborů

- Diskové
  - s5, minix, ext;
  - UFS, BSD Fast Filesystem, ext2;
  - vxfs, ext3, . . .
  - ZFS, ext4 (?), . . .
- Síťové
  - NFS, SambaFS, . . .
- PseudoFS
  - procfs, fdfs, . . .
  - tmpfs, . . .

Vytváření a připojování FS II.

Zajímavostí některých UNIXů je podpora práce se souborem jako s logickým diskem.
Příkazy `mount`, `umount`, `mkfs`.
Nutná podpora *loop* zařízení v jádře.

```
mount -o loop
```

ISO 9660, ale lze použít pro libovolné FS podporované jádrem.

Žurnálování FS

Pro zvýšení spolehlivosti některé FS podporují transakční žurnál, obdoba transakcí v databázích.

$ext3 \rightarrow ext2$ pouhým nastavením příznaku FS.

- Žurnál lze zapnout při připojování FS.
- Změny vyžadující více přístupů jsou atomické: otevření nového souboru, `unlink; mkdir; rmdir`.
- Na disku je vyhrazená oblast pro žurnál, záznamy o změnách metadat FS.
- V případě pádu systému je po rebootu každá operace (*transakce*) buď dokončena a potvrzena (*commit*), nebo odvolána a změny zrušeny (*rollback*).
- Proto nemůže nastat problém s hodnotou čítače linků, nevznikají alokované ale neodkazované i-nody, neodkazované datové bloky, atd.

Kontrola a opravy FS

Přes všechna opatření se může stát, že dojde k poškození FS. Výpadek napájení, nahodilý reset – neohrozí konsistenci žurnálovacích FS.

Žurnálovací FS nemůže zachránit data! Nezapsaná data v cache jsou nenávratně ztracena, na disku bude v nejlepším případě stará verze dat.

Existují i chyby, proti nimž není obrany – chyby v jádře: nejen v ovladači FS, ale v libovolném kódu jádra (neotestované moduly!). Chybná manipulace s datovými strukturami jádra.

`fsck`

`fsck.ext2; fsck.vfat; ...`

`fsck` (1)

Pokud `fsck` ze superbloku zjistí, že FS byl čistě odpojen (bit *clean*), kontrolu neprovede.

`fsck -f`

Co `fsck` hledá a umí opravit:

- obsazené, ale neodkazované i-nody,
- realitě neodpovídající čítače odkazů (LC),
- nepoužité datové bloky chybějící v mapách volných bloků,
- datové bloky označené jako volné, ale použité pro data,
- nesprávné hodnoty pomocných informací v superbloku.

`fsck` (2)

Co `fsck` hledá a neumí sám opravit:

- bloky odkazované ze dvou souborů,
- odkazy na bloky mimo FS,
- nižší než skutečný počet odkazů v LC,
- neevidované bloky,
- adresář odkazující na nealokovaný i-node,
- chyby v položkách i-nodů (formát).

Každý logický disk (UFS, ext2, . . .): adresář `lost+found`.

`syslog` (1)

Logovací nástroj, mnoho variant.

- Jednotná logovací politika.
- Usnadnění programování.
- Řízení logování.

Součásti:

- `openlog`(3), `closelog`(3).
- `syslogd`(8).
- `logger`(1).

syslog (2)

Log. adresáře: `/var/log`, `/var/adm`
Konfigurační soubor: `/etc/syslog.conf`
Typické soubory ve `/var/log`:

`messages`	vše/téměř vše
`syslog`	vše/téměř vše
`auth.log`	autorizační zprávy
`wtmp`	přihlašování (`login`)
`lastlog`	řídký binární soubor indexovaný dle UID (`login`)

`/proc/kmsg` → `dmesg`
`/proc/kmsg` → `klogd`
Závažnost zpráv na terminálu: `dmesg -n 1` pouze kritické

`logrotate`; `syslog-ng`

syslog (3)

Formát `/etc/syslog.conf`.

selektor akce

služba.priorita akce

(*facility.priority_level action*)

Selektor v C: hodnoty `LOG_` v `/usr/include/syslog.h`.

Služba: `auth, authpriv, cron, ..., user` = nespecifikovaná.

`*` = všechny služby kromě `mark`.

Priorita: `emerg, alert, crit, err, warning, notice, info, debug`

Složený selektor povolen (`kern.info;kern.!err`), pouze jedna akce, ev. více řádek.

Akce: `soubor, -soubor, |pojmenovaná roura, @host, @ip, user1, *`

syslog (4)

/etc/rsyslogd.conf

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                                  /var/log/maillog
# Log cron stuff
cron.*                                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                                 *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler
# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log
# All kernel messages that come with priorities
# from info up to warning in the file /var/adm/kernel-info.
# Everything from err and higher is excluded.
kern.info;kern.!err                                  /var/adm/kernel-info
```

syslog (5)

Příklady SW používajícího `syslog`

Program	Služba	Priorita	Popis
cron	cron	info	Plánování úloh
ftpd	ftp	debug–crit	wu-ftpd
imapd	mail	info–alert	IMAP daemon
inetd	daemon	err, warning	Inet superdaemon
login	authpriv	info–err	Přihlašování
lpd	lpr	info–err	Tiskové služby
named	daemon	info–err	Jmenná služba DNS
passwd	auth	notice, warning	Nastavování hesel
sendmail	mail	debug–alert	Poštovní daemon
shutdown	auth	notice	Zastavení systému
su	auth	notice	Přepínání UID
sudo	local2	notice, alert	Omezené su
syslogd	syslog, mark	info–err	Interní chyby, časové značky
tcpd	local7	debug–err	Pomocný program `inetd`
vmlinuz	kern	debug–emerg	Linux (jádro)
xinetd	*conf*	info *conf*	Rozšířený `inetd`

syslog (6)

Akce: `@host, @ip`

`syslog -r` remote logging

`syslog -h` remote logging forwarding

UDP: 514 (`/etc/services`)

Některé `syslog` i TCP (akce `@host, @ip`): TCP 200.

Čas zprávy v logu: dle log serveru.

Logování na terminál?

`logcheck, swatch`

```
kill -HUP ‘cat /var/run/syslogd.pid‘

logger -p local3.notice ”Test no.1”
```