Architektura systému GNU/Linux

Bohdan Milar
bohdan.milar@liberix.cz

Úvod

- Liberix, o.p.s.
- Nestátní nezisková organizace
- Založena na jaře 2005
- Hlavní cíl - Podpora a propagace svobodných informačních technologií
- Vize: „Umožnit všem uživatelům ICT nezávislost na proprietárním softwaru.“
- Spolupráce s UP
- Projekty k realizaci
- Kontakty: www.liberix.cz

Organizace předmětu

- Zaměření předmětu - úvod do administrace operačního systému, nikoli programování
- 10 přednášek v LS 2007/2008
- Hodnocení:
  - referát k určenému tématu
  - docházka
  - aktivita

Obsah přednášky

- Bootování Linuxu
- Jádro a jeho moduly
- Služby na pozadí: daemoni a servery
- Uživatelská rozhraní: konzole vs. X
- Řízení přístupu:
  - systém souborů
  - uživatelé a skupiny
  - SE Linux

Bootování Linuxu

- BIOS
- Boot Manager - výběr OS
- Kernel - jádro (vlastní Linux) + ovladače
- Init - praotec všech procesů
- Daemons - služby na pozadí
- Consoles - 6 textových konzolí
- X Window System - grafika

Jádro a jeho moduly

- Jedno velké jádro ovládá celý systém (opak mikrojádra, např. Hurd)
- Binární podoba jádra v samorozbalovacím archivu na boot partition
- Stará se o obsluhu hardwaru, takže všechna systémová volání HW jdou přes jádro
- Ovladače HW lze kompilovat jako integrální součást (monolit) nebo samostatně (moduly)
- Zdrojové kódy = 300 MB, 23 000 souborů
- Číslování verzí (aktuálně 2.6.24.2)

Daemoni - procesy na pozadí

- Daemoni zajišťují činnosti, které musí být dostupné po celou dobu běhu systému.
- Daemoni zpravidla nemají uživatelské rozhraní, jejich činnost využívají jiné procesy, jádro nebo uživatelé přihlášení vzdáleně.
- Typickým použitím daemonů jsou síťové servery: HTTP, FTP, SQL, SSH, Mail, ...
- Příklady dalsích daemonů: CUPS, Syslogd, Cron, Atd, XFS, Hal, kjournald, ...
- Řízení daemonů: service, /etc/init.d

Základy textového prostředí

- Termíny: konzole, terminál, interpretr (CLI)
- Výhody práce v textovém prostředí:
  - nižší nároky na hardware
  - snadnější vzdálený přístup
  - větší rychlost zkušených uživatelů
  - jednodušší skriptovatelnost
  - dostupná historie příkazů

Práce s příkazovými interpretry

- Terminály v X, virtuální konzole, přihlašování
- Prompt, řádek, kurzor, historie
- Obecná syntaxe příkazů
- Doplňování pomocí Tab
- Rolování obrazu (Shift + PgUp / PgDn)
- Prohledávání v historii (Ctrl + r, Ctrl + s)
- Aliasy
- Manuálové stránky
- Proměnné

Správa a ovládání procesů

- Násilné přerušení procesu: Ctrl + c
- Spouštění procesů na pozadí: &
- Přesunutí procesu na pozadí: Ctrl + z, bg
- Vrácení procesu na popředí: fg
- Výpis seznamu běžících procesů: ps, jobs
- Posílání signálů procesům: kill, killall
- Priorita procesu: nice, renice
- Přesměrování vstupu a výstupu, roury

X Window System

- Architektura klient/server:
  - server = vlastní grafické prostředí (XFree86, X.org), knihovny a ovladače grafické karty
  - klienti = uživatelské prostředí a aplikace
  - klienti se serverem komunikují síťově
- Přihlašovací obrazovka (xdm, kdm, gdm)
- Knihovny (Qt, Gtk+, Motif, ...)
- Správci oken (kwin, Metacity, Compiz, ...)
- Prostředí pracovní plochy (KDE, Gnome)

Adresářová struktura v Linuxu

- Princip jediného stromu
- Lomítko vs. obrácené lomítko
- Kořenový adresář (root vs. /root)
- Přípojné body
- Domovské adresáře uživatelů
- Absolutní vs. relativní cesta
- Proměnná PATH
- FS Hierarchy Standard (FHS)

Virtuální systémy souborů

- Příklady virtuálních FS:
  - /dev
  - /proc
  - /sys
- Zajímavá místa v /proc a /sys:
  - CPU: /proc/stat, /proc/loadavg, /proc/cpuinfo
  - RAM: /proc/meminfo
  - disky: /proc/scsi/
  - síť: /proc/net/, /proc/sys/net/
  - napájení: /sys/power/state, /proc/acpi/battery/
  - info o zařízeních: /proc/sys/dev/

Monitorování zátěže systému

- Grafické nástroje - gkrellm
- CPU, RAM - top, uptime, free
- síť: ntop, MRTG, Cacti
- disky: df, du, fuser
- uživatelé: who, w, last

Správa uživatelů a skupin

- Každý soubor má UID a GID
- Změna práv, uživatel root: su, sudo
- Uživatelé, procesy a logy
- Definice uživatelů v /etc/passwd
- Ukládání hesel do /etc/shadow
- Skupiny - /etc/passwd a /etc/group
- Správa uživatelů: useradd, userdel, passwd
- Nastavení uživatelů: chown, chgrp

Přístupová práva v Linuxu

- Přístupová práva k souborům: rwx rwx rwx
- Převod na čísla:
  - binárně: 000 000 000 - 111 111 111
  - dekadicky: 421 421 421
- Speciální bity (suid, sticky, ...)
- Nástroje: chmod, install, umask
- Pokud nefunguje přístup tam, kde jsou správně nastavena základní práva, může za to pravděpodobně SE Linux.

Bezpečnostní vrstva SE Linux

- vyvinula BSA, součástí jádra od verze 2.6
- bezpečnostní kontext:
  - identita - obdoba uživatelského jména
  - role - určuje, které domény jsou dostupné
  - doména - rozsah přístupu k procesům
  - typ - rozsah přístupu k souborům, socketům, ...
- ovládání:
  - modifikované příkazy: ls -Z, ps -Z, id
  - newrole - přepne roli daného uživatele
  - chcon - mění bezpečnostní kontext souborů
  - ...