

2 – Síťové služby, textové editory

PIN1 cvičení

Matěj Klíma, David Fridrich

FJFI ČVUT v Praze, Katedra fyzikální elektroniky

4. března 2016

Obsah

- Archivace souborů, tar, gzip
- SSH - vzdálené připojení, připojení klíčem
- Další síťové služby (ping, nslookup, mail)
- Textové editory - úvod (nano, vim, emacs)

Archivace souborů pomocí tar

- Tape archiver - původně pro archivaci na pásku
- Zachovává atributy, adresářové struktury
- Dnes umí i kompresní algoritmy (gzip)
- Nejčastější parametry - xzf, czf

```
tar -czf <archiv> <soubor/adresář>  
tar -xzf <archiv> <kam>
```

- Pokud "-" místo názvu archivu, použije std. výstup

Archivace souborů - formáty

compress	.Z	LZW	1975, původní UNIX, patentovaný algoritmus
gzip, gunzip	.gz	LZ77	1992, velmi používaný, GNU GPL
bzip2, bunzip2	.bz2	BZW, MTF, Huffman	1992, velmi používaný, BSD
pkzip	.zip	různé (LZ77)	defacto standard pro Windows, iOS
winrar	.rar	?	proprietární formát
xz, 7z	.xz, .7z	hlavně LZMA	moderní alternativy, paměťově náročnější, velká komprese, rychlá dekomprese
freearc	.arc	adaptivně LZMA, PPMD, TrueAudio	2006, velmi efektivní, malá podpora

Vzdálené připojení přes síť

- telnet – 1968, virtuální terminál, nezabezpečený
- ssh – **Secure SHell**
- Primárně pro vzdálený přístup k jinému počítači (příkaz ssh login@stroj.domena)
- Odhlášení logout
- Často se používá pro bezpečné "tunelování" jiných služeb:

```
ssh -N -x -L 1712:skiritf.ics.muni.cz:1712 \  
-L 1713:skiritf.ics.muni.cz:1713 \  
username@newton.fjfi.cvut.cz
```

Vzdálený přenos souborů

- ftp – nezabezpečený
- scp – vzdálené kopírování přes SSH
- sftp – zabezpečená alternativa ftp
- Grafické klienty – např. [FileZilla](#), mc
- FUSE (Filesystem in USErspace) – např. sshfs

Konfigurace sítě KFE

- E-mail funguje na počítači newton.
- SSH je otevřeno mimo ČVUT pouze pro newton, raman.
- Ostatní počítače přístupné pouze v rámci ČVUT.
- Funguje zde web server - adresář ~/public_html je přístupný jako <http://kfe.fjfi.cvut.cz/~uzivatel/>.

Autentizace pomocí veřejného klíče

- U SSH standardně přihlášení pomocí hesla - nevýhody (otrava, menší zabezpečení)
- Místo toho můžeme využít asymetrickou kryptografii:
 - 1 Vygenerujeme pár klíčů na našem stroji
 - 2 Předáme přihlašovacímu procesu soukromý klíč
 - 3 Na vzdálený stroj zkopírujeme veřejný klíč
 - 4 Zajistíme, aby sshd na vzdáleném počítači uznával veřejný klíč

Veřejný klíč - instalace

Zjednodušený postup - pouze mezi KFE počítači

```
ssh-keygen -t dsa  
cd ~/.ssh  
cp id_dsa.pub authorized_keys  
ssh-add id_dsa
```

- Protože na KFE používáte stejný home adresář, může se nastavení udělat na jednom stroji.
- Bude fungovat ale pouze mezi KFE počítači.
- ssh-add se nespustí automaticky, musíme nastavit v GNOME, ~/.bash_profile nebo ~/.tcsh_rc

Veřejný klíč - instalace

Úplný postup - lokální stroj

```
ssh-keygen -t dsa  
scp ~/.ssh/id_dsa.pub uzivatel@newton.fjfi.cvut.cz:~  
ssh-add ~/.ssh/id_dsa
```

Úplný postup - vzdálený stroj

```
mv ~/id_dsa.pub ~/.ssh/authorized_keys  
nebo pro více identit:  
cat ~/id_dsa.pub >> ~/.ssh/authorized_keys  
rm ~/id_dsa.pub  
a nakonec:  
chmod 600 ~/.ssh/authorized_keys
```

Další síťové služby

- Příkaz `ping <adresa>` - testování odezvy
- Příkaz `nslookup <jmeno>` - dotaz na nameserver
- Příkaz `talk` - chatovací klient (zde nefunguje)
- Příkaz `traceroute <adresa>` - výpis cesty paketu
- Příkaz `ifconfig` - výpis nastavení sítě
- Příkaz `ip addr show` - výpis nastavení sítě

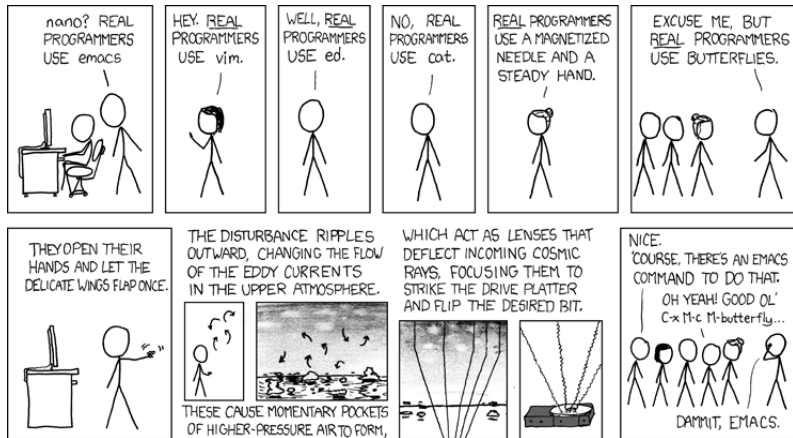
E-mail

- Původně služba pro posílání vzkazů mezi uživateli.
- Pozor, standardně se po síti pohybují bez šifrování!
- Adresa `uzivatel@pocitac.domena`.
- Uživatelsky - příkaz `mail -s "predmet<<adresa>`
- Soubor `~/ .forward` - seznam aliasů, kam se doručují maily pro daného uživatele.
- Grafické klienty `pine`, `alpine`.

Textové editory

- Textový editor je základní nástroj pro psaní souborů v konzoli, ale i v grafickém rozhraní.
- Dnes často překonán specializovaným software (Office pro dokumenty, různá IDE pro programování).
- Pro univerzální použití stále nenahraditelný.
- `vi`, `emacs` - nejobsáhlejší editory, nejstarší stále používané komplexní programy.
- Optimalizované pro co nejrychlejší práci bez myši.
- Který je lepší je předmětem sporů geeků dodnes.
- "lehčí" alternativy - `nano`, `pico`, `mcedit`, případně grafické `gedit` pro GNOME, `kate` u KDE ...

Textové editory



Zdroj: xkcd.com/378/

- [vi:aj] – původní editor pro UNIX, název vzniknul ze zkratky pro mód "visual" editoru ex.
- Původně proprietární, existuje mnoho otevřených modifikací (vim, gvim).
- Základním paradigmatem je příkazový vs. editační mód.

vi - příkazový mód

- Po spuštění editor přijímá příkazy.
- i/a – vložení textu před/za kurzor
- I/A – vložení textu na začátek/konec řádky
- R – přepisování textu
- x/dd – smazání znaku/řádky
- yy,p uložit řádek do schránky, vložit ze schránky za aktuální řádek

vi - příkazový mód

- Editační mód opustíme klávesou Esc.
- Pohyb kurzoru po obrazovce `h j k l`
- `s/text/TEXT/` nahrazení textu.
- `:` zapíná rozšířený příkazový mód
- `w` zapsat do souboru, `q` ukončit.

emacs

- Velmi variabilní, rozšiřovatelný, "editor macros", vytvořil R. Stallman v r. 1976.
- Na rozdíl od vi editování v "reálném čase".
- Má dokonce vlastní programovací jazyk pro psaní nových příkazů – EMACS LISP.
- Byla mu vytýkána přílišná komplikovanost, má přes 2000 klávesových zkratek a příkazů.
- Dnes má ale grafické rozhraní a obsáhlou nápovědu, takže začít není obtížné.

emacs

emacs byl původně navržen pro jiné rozložení klávesnice. Klávesa Meta byla nahrazena Alt, ale v nápovědě se používá stále zkratka "M-" . . .



Zdroj: wikipedia.org