SSH: dálková správa serveru

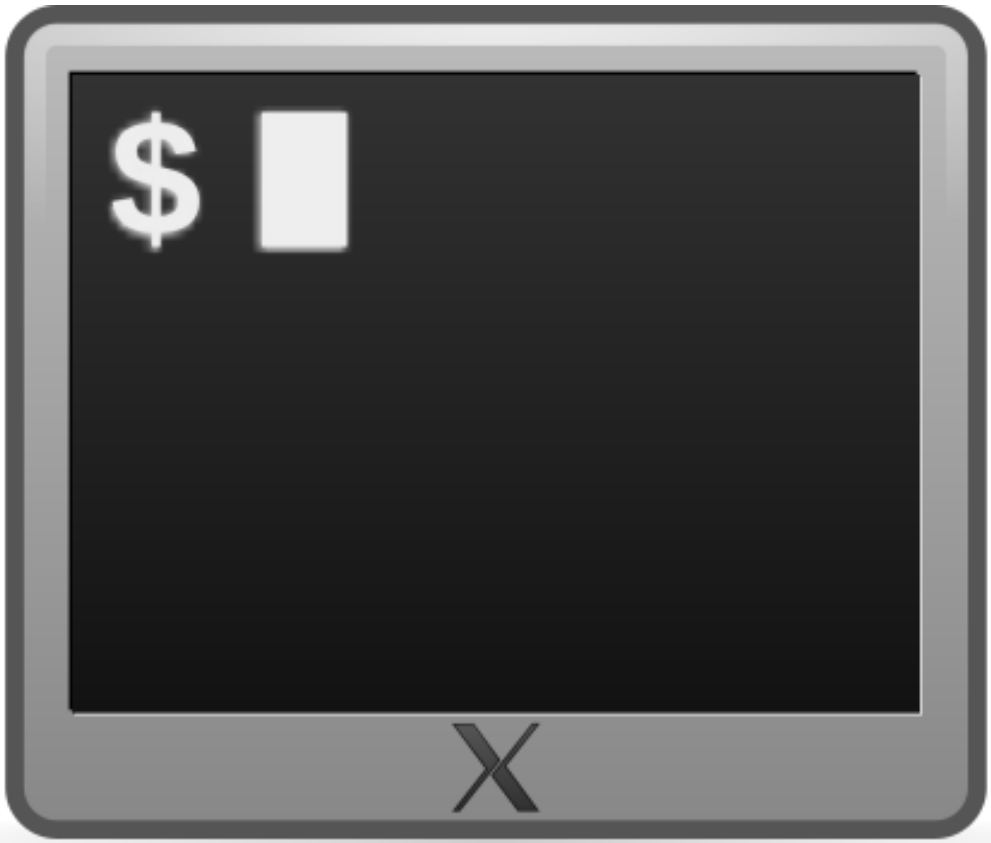
Petr Krčmář

8. března 2015

Obsah přednášky

- Správa na dálku
- SSH není jen šifrovaný telnet
- Bezpečné použití SSH s klíči
- Klienti pro jiné systémy
- Přenos souborů
- Tipy: Mosh a Tmux
- Prostor na otázky

Dálková správa = SSH



Správa na dálku

- u VPS nemáme fyzický přístup
- jedinou možností dálková správa
- buď virtuální terminál po sériové lince
- nebo lépe odkudkoliv po SSH
  - SSH velmi univerzální
  - možné i přenášet soubory
  - velmi bezpečné

Sériová linka

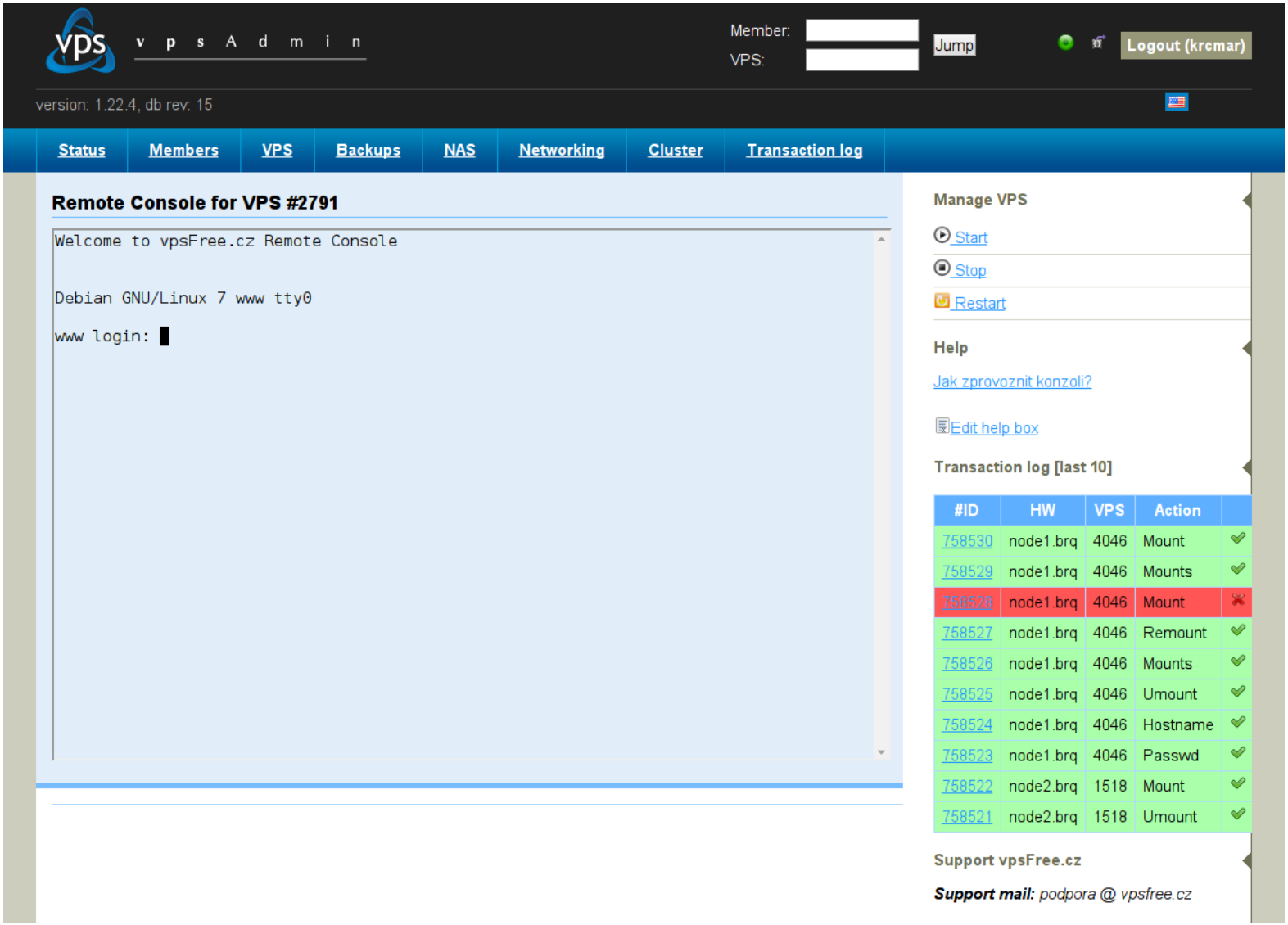
- když se něco rozbije a není dálkový přístup
- vypadné démon/zablokujeme firewall
- ovládací rozhraní vpsAdmin
- je třeba mít zapnuté (v šablonách automaticky)

/etc/inittab

```
1:2345:respawn:/sbin/getty 38400 tty0
```

- podrobně na kb.vpsfree.cz

Ukázka sériové konzole



Obrázek: Konzole ve vpsAdminu

SSH = správná cesta

- původní náhrada za otevřený telnet
- běží na TCP portu 22
- ale zdaleka **není jen terminál**
- velmi bezpečné – autentizace, šifrování, klíče
- součástí všech unixů (obvykle OpenSSH)
- klienti pro všechny platformy

Přihlášení pomocí hesla

- zadáme jméno a heslo (a port)
- potvrdíme pravost otisků veřejného klíče
- (uloží se do `~/.ssh/known_hosts`)
- zadáme přihlašovací heslo
- spustí se shell a jsme tam
- pozor na heslo, SSH je nejčastější cesta dovnitř

Bezpečněji = přihlašování klíčem

- klíče se nedají hádat
- volitelně můžeme vypnout přihlašování heslem
- nemusíme se zdržovat zadáváním složitého hesla
- systém nás může přihlašovat automaticky
- klíče můžeme mít na smart kartě

Vygenerování a použití klíče

- vygenerujeme klíč

Generujeme

```
$ ssh-keygen -t rsa -b 4096 -C petr@masina
```

- nahrajeme na serveru do `~/.ssh/authorized_keys`

Nahrajeme

```
$ ssh-copy-id petr@server.nekde.cz
```

- naposledy zadáme heslo, klíč se přenese
- při příštím přihlášení už heslo nezadáváme

SSH agent

- hesla jsou na disku zašifrovaná
- při použití se zadává heslo
- lze obejít použitím SSH agenta
- ten drží klíče v paměti a umí je používat
- autostart v Debianu:

/etc/X11/Xsession.options

```
use-ssh-agent
```

- `/etc/X11/Xsession.d/90x11-common_ssh-agent`
- doporučuji připsat `-c` pro vyvolání dialogu

Deaktivace přihlašování heslem

/etc/ssh/sshd_config

```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile %h/.ssh/authorized_keys
ChallengeResponseAuthentication no
PasswordAuthentication no
```

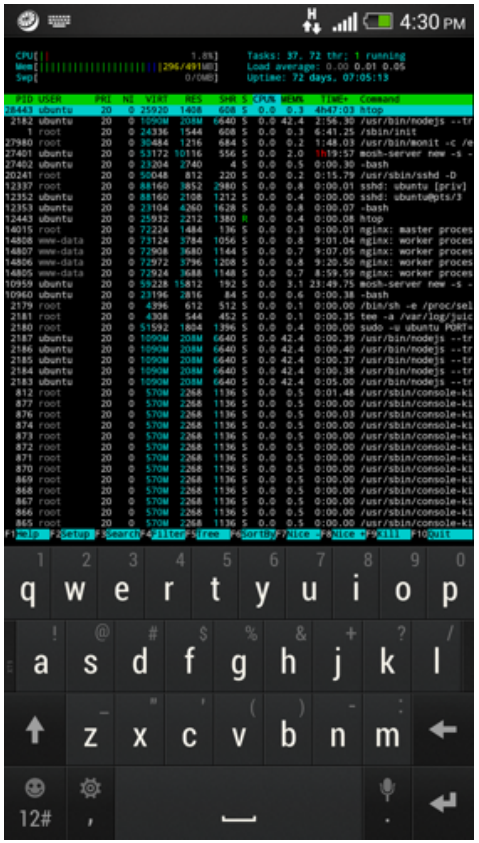
- nutno restartovat démona
- možno ověřit pomocí parametru

Vynucení použití hesla

```
$ ssh -o PubkeyAuthentication=no petr@server.nekde.cz
Permission denied (publickey).
```

Klienti

- Linux: ssh z balíčku OpenSSH
- Windows: Putty
- OS X: Terminal.app
- Android: JuiceSSH, ConnectBot



ROOT.CZ vpsFree.cz

Přenos souborů

- SFTP vs. SCP – často se zaměňuje
- SCP – jednoduchý, neumí ani listovat soubory
- k tomu se musí volat příazy (fish v MC)
- SFTP – komplexní jako FTP, ale mladší
- používá se stejný protokol – bezpečnost, klíče…

Terminálové scp

```
$ scp prednaska.pdf server.nekde.cz:/home/petr/prednasky/
```

- GUI aplikace: FileZilla, WinSCP, gFTP…
- často součástí správců souborů: Nautilus, MC…

Tipy: Mosh a Tmux

Mosh

- pro pomalá/špatná spojení se hodí Mosh
- SSH po UDP – neexistující spojení nespadne
- přežije uspání počítače i změnu IP adresy
- používá se stejně jako SSH, včetně klíčů

Tmux/Screen

- terminálový multiplexer – Tmux nebo Screen
- virtuální plochy v terminálu – více otevřených „oken“
- možné spouštět víc úloh

Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz