SSH nejen pro vzdálenou správu Linuxu

Petr Krčmář

6. října 2019

Uvedené dílo (s výjimkou obrázků) podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O mně

- linuxák od roku 1998
- správce serverů
- školitel
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz

Prezentace už teď na webu

https://www.petrkrcmar.cz

Obsah přednášky

1. Správa na dálku
2. Heslo nebo klíč
3. Vylepšení terminálu
4. Přenos souborů
5. Omezení uživatele
6. Tunely

Správa na dálku

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

ROOT.CZ vpsFree.cz

Sériová linka

- když se něco rozbije a není dálkový přístup
- je třeba mít zapnuté `getty` na sériové lince

/etc/inittab

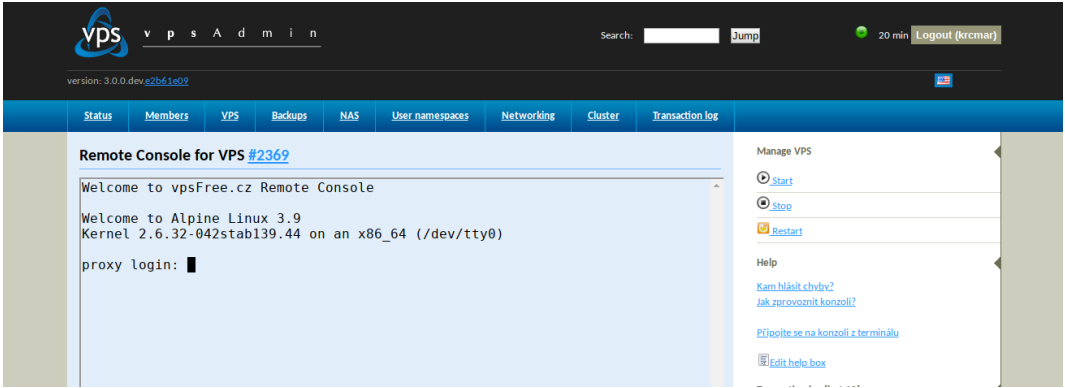
```
1:2345:respawn:/sbin/getty 38400 tty0
```

- systemd zapíná automaticky podle `systemd-getty-generator`

manuální zavedení se systemd

```
# less /lib/systemd/system/serial-getty@.service
# systemctl enable serial-getty@ttyS1.service
# systemctl start serial-getty@ttyS1.service
```

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

Heslo nebo klíč

Přihlášení pomocí hesla

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

ROOT.CZ vpsFree.cz

Bezpečněji = přihlašování klíčem

- klíče se nedají hádat
- volitelně můžeme vypnout přihlašování heslem
- nemusíme se zdržovat zadáváním složitého hesla
- systém nás může přihlašovat automaticky
- klíče nemusíme mít na disku
  - smart karty, tokeny…

Vygenerování a použití klíče

- na klientovi vygenerujeme pár klíčů
- uloží se do `~/.ssh/`

Generujeme

```
$ ssh-keygen -t ecdsa -b 384 -C popis_klice
```

- 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

ROOT.CZ vpsFree.cz

SSH agent

- hesla jsou na disku zašifrovaná
  - při použití se zadává heslo
- opakované zadávání lze obejít použitím SSH agenta
- klíčenka v paměti, která nevydává privátní klíče
- přidání klíčů pomocí `ssh-add`
  - parametr `-c` vynutí potvrzení před použitím
- automatické přidání klíče `AddKeysToAgent confirm`
- socket lze tunelovat pomocí `ssh -A` nebo `ForwardAgent yes`
  - správce serveru má k socketu přístup

Deaktivace přihlašování heslem

/etc/ssh/sshd_config

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

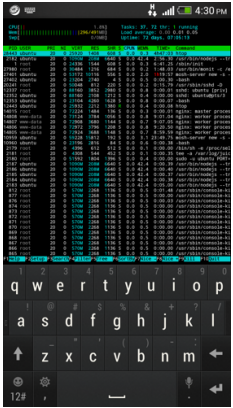
- nutno restartovat démona
- možno ověřit pomocí parametru

Vynucení použití hesla

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

Klienti

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



Vylepšení terminálu

Jednoduchá vylepšení

- uživatelská konfigurace je v souboru `~/.ssh/config`
- obrázek RandomArt `VisualHostKey yes`
- delší udržení spojení `ServerAliveInterval 10`
- ukončení mrtvého spojení pomocí `Enter ~.`
- napovídání jmen z `known_hosts` pomocí `bash-completion`
  - vyžaduje nehašovaná jména `HashKnownHosts no`

Sdílené spojení

- multiplexování více nezávislých relací jedním SSH spojením
- realizováno pomocí řídicího soketu
  - *master* naváže spojení a vytvoří UNIX soket
  - *slave* komunikuje se soketem
- autentizaci provádí pouze *master*

Konfigurace sdílení spojení

```
ControlMaster auto
ControlPath ~/.ssh/controlsock-%h-%p-%r
ControlPersist  30
```

Lepší terminál s Mosh

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

Použití Mosh

```
$ mosh root@ssh.server.cz
```

Terminálové multiplexery

- terminálový multiplexer – Tmux nebo Screen
- virtuální plochy v terminálu – více otevřených „oken“
- možné spouštět víc úloh
- možnost odpojit se a zavřít spojení
  - úlohy stále běží
  - můžeme se znovu připojit

Přenos souborů

Přenos souborů

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

Terminálové scp

```
$ scp prednaska.pdf server.nekde.cz:/tmp/
```

- klientů je spousta
  - CLI: sftp, lftp
  - GUI: FileZilla, WinSCP, gFTP...

ROOT.CZ vpsFree.cz

OpenSSH HPN patche

- OpenSSH není optimalizováno na výkon
- pomalé při vyšší latenci kvůli malé a fixní velikosti bufferů
- velké buffery zase zabíjejí interaktivitu (*Bufferbloat*)
- problém řeší sada patchů označených jako HPN
  - dynamická velikost bufferu podle TCP okna
  - možnost nulového šifrování
  - možnost paralelizace některých procesů

Omezení uživatele

Omezení uživatelů

- ve výchozím stavu může SSH uživatel využívat všech možností
  - chceme to? potřebuje to uživatel?
- můžeme blokovat jednotlivé uživatel či skupiny
- můžeme omezovat přihlášení na IP adresy
- můžeme omezovat, co který uživatel (skupina) může dělat
- například: může jen k souborům, nemůže terminál ani tunely

Omezení přihlášení

- v souboru `/etc/ssh/sshd_config`
- zákaz podle jména, skupiny, IP
- možno kombinovat, možno používat wildcard
- v pořadí: DenyUsers, AllowUsers, DenyGroups a AllowGroups

Příklad blokace

```
DenyUsers jirka franta skoleni*
AllowUser skoleni-test admin@192.168.1.*
DenyGroups studenti
```

Omezení uživatelů v adresáři

- můžeme uživatele uzamknout v adresáři
  - OpenSSH od 4.8 (2008) umí přímo vytvořit chroot
- nedostane se ven = ani do systému
- zároveň mu můžeme odebrat terminál
  - vynutíme použití interního SFTP serveru
- výsledkem je bezpečný kanál pro přenos souborů
- výhodná náhrada za FTP
  - WinSCP, FileZilla, TotalCommander…
  - mohou používat klíče

Nastavení na serveru

V souboru /etc/ssh/sshd_config

```
Subsystem   sftp    internal-sftp

Match group sftpusers
    ChrootDirectory     /sftp/%u
    ForceCommand        internal-sftp
    X11Forwarding       no
    AllowTcpForwarding  no
```

- uživatelův adresář **musí vlastnit root**
- uživatel do něj **nesmí mít právo zápisu** (755)

Tunely

SSH tunely

- lokální – otevřený konec se otevře na klientovi

```
$ ssh -L 8080:server.nekde.cz:80
```

- vzdálený – otevřený konec na serveru, provoz jde ke klientovi
  - výchozí jen localhost, možno změnit s `GatewayPorts`

```
$ ssh -R 2222:server.doma.cz:22
```

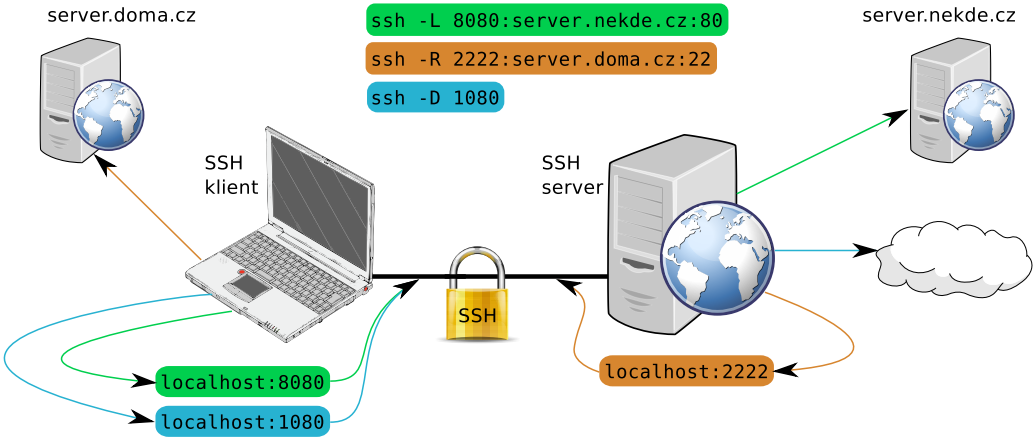
- dynamický – socks proxy pro univerzální použití

```
$ ssh -D 1080
```

- pokud nechceme terminál, přidáme `-N`

ROOT.CZ vpsFree.cz

Schéma tunelování



Děkuji za pozornost

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ vpsFree.cz