

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

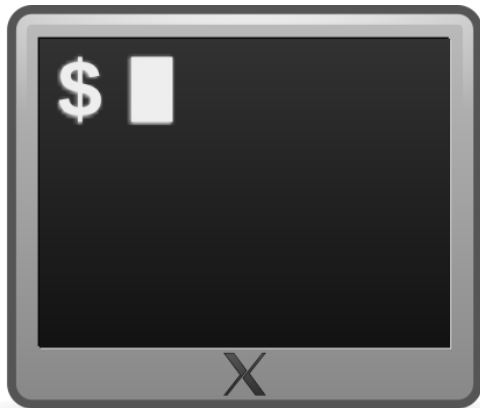
<https://www.petrkrcmar.cz>

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



- 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
- 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

The screenshot displays the vpsAdmin web interface. At the top, there is a search bar and a 'Jump' button. The main navigation menu includes links for Status, Members, VPS, Backups, NAS, User namespaces, Networking, Cluster, and Transaction log. The central area shows a 'Remote Console for VPS #2369' with the following terminal output:

```
Welcome to vpsFree.cz Remote Console
Welcome to Alpine Linux 3.9
Kernel 2.6.32-042stab139.44 on an x86_64 (/dev/tty0)
proxy login: █
```

On the right side, there is a 'Manage VPS' sidebar with buttons for Start, Stop, and Restart, along with a 'Help' section containing links for reporting errors, managing the console, and connecting via terminal.

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

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 nezadááme

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).
```


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

```
tasky 87.72 thr: 1 running
Load average: 0.00 0.01 0.05
up: 1 day, 07:08:13

USER      PID     PPID  STAT   VSZ    RSS   TTY      TIME    CMD
root      20      1      S      1024   1200  pts/0    0:00.00 sshd: [root@root]
sshd      20      1      Ss     1024   1200  pts/0    0:00.00 sshd: [root@root]
root      21      20     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      22      21     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      23      22     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      24      23     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      25      24     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      26      25     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      27      26     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      28      27     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      29      28     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      30      29     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      31      30     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      32      31     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      33      32     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      34      33     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      35      34     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      36      35     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      37      36     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      38      37     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      39      38     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      40      39     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      41      40     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      42      41     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      43      42     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      44      43     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      45      44     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      46      45     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      47      46     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      48      47     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      49      48     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      50      49     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      51      50     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      52      51     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      53      52     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      54      53     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      55      54     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      56      55     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      57      56     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      58      57     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      59      58     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      60      59     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      61      60     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      62      61     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      63      62     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      64      63     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      65      64     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      66      65     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      67      66     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      68      67     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      69      68     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      70      69     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      71      70     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      72      71     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      73      72     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      74      73     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      75      74     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      76      75     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      77      76     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      78      77     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      79      78     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      80      79     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      81      80     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      82      81     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      83      82     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      84      83     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      85      84     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      86      85     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      87      86     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      88      87     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      89      88     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      90      89     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      91      90     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      92      91     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      93      92     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      94      93     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      95      94     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      96      95     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      97      96     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      98      97     S      1024   1200  pts/0    0:00.00 ssh: root@root
root      99      98     S      1024   1200  pts/0    0:00.00 ssh: root@root
root     100      99     S      1024   1200  pts/0    0:00.00 ssh: root@root
```

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 socketu
 - *master* naváže spojení a vytvoří UNIX socket
 - *slave* komunikuje se socketem
- 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 nepadne
- 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...

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 uživatele 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

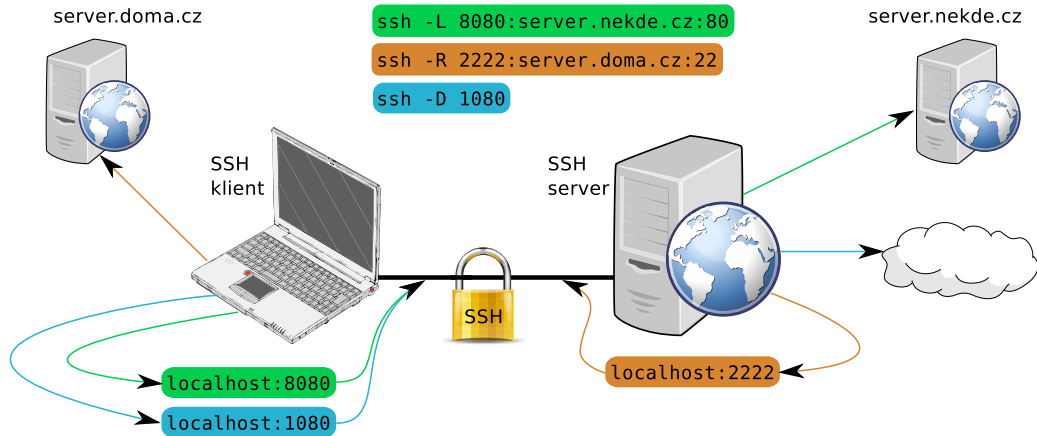
```
$ ssh -R 2222:server.doma.cz:22
```

- dynamický – socks proxy pro univerzální použití

```
$ ssh -D 1080
```

- pokud nechceme terminál, přidáme -N

Schéma tunelování



Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz