

SSH

Co je to?

SSH je univerzální komunikační protokol umožňující **šifrované** a **oboustranně ověřené** připojení k serveru. Nejčastěji se používá pro zpřístupnění vzdáleného terminálu (příkazové řádky) nebo přenosu souborů. Pokud se chcete připojit ke svému serveru a provádět na něm jakékoliv administrátorské zásahy, budete potřebovat správně nakonfigurované SSH.

Konfigurace

```
/etc/ssh/sshd_config
```

Měli bychom dodržovat zásadu, že co není povoleno, je zakázáno.

Přihlášení jen pro některé uživatele

```
AllowUsers petr karel
```

v systému můžeme mít mnoho uživatelů a někteří mohou mít slabé heslo apod., tímto nastavením umožníme přihlásit se jen explicitně uvedeným uživatelům

za jméno můžeme přidat i omezení na IP adresu:

```
AllowUsers petr karel@8.8.8.8
```

Zakázání roota s heslem

```
PermitRootLogin without-password
```

Zakáz přihlašování heslem

```
PasswordAuthentication no
```

Restrikce připojení dle IP

```
vim /etc/hosts.deny
SSHD: all
```

```
vim /etc/hosts.allow
SSHD: 8.8.8.8 8.8.4.4 ..... # dalsi ip adresy ze kterych umoznime spojeni na SSH
```

Přihlášení pomocí klíčů

Nejprve je potřeba si vygenerovat soukromý a veřejný klíč pomocí PuTTYgen. Vygenerujeme si SSH-2 RS 1024 bitové klíče. Nyní vyplníme údaje o klíči (komentář a passphrase) a uložíme si soukromý klíč do pc.

V Linuxu použijeme řádkovou utilitu:

```
ssh-keygen -t rsa -b 2048 -C uzivatel@stanice
```

Na serveru si vytvoříme složku s právy 700:

```
mkdir ~/.ssh
chmod 700 ~/.ssh
```

Vygenerovaný klíč so vložíme v domovském adresáři na serveru do souboru

```
~/.ssh/authorized_keys
```

Nesmíme zapomenou nastavit práva k souboru:

```
chmod 600 ~/.ssh/authorized_keys
```

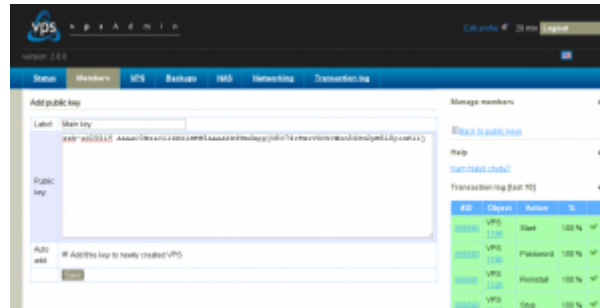
Nyní se můžeme přihlásit pomocí PuTTY a soukromého klíče, který zadáme v sekci SSH → Auth.

Pokud chceme zakázat přihlašování pomocí hesla přes SSH, změníme konfiguraci v souboru `/etc/ssh/sshd_config`:

```
[...]
Protocol 2
PasswordAuthentication no
UsePAM no
[...]
```

Automatické vložení klíčů

vpsAdmin umí do nově vytvořeného VPS vložit klíče automaticky. Nejprve mu je musíme předat. To uděláme po přihlášení v Edit profile → Public keys → vpravo v panelu Add public key.



U každého klíče si můžeme vybrat, jestli se má do nových/reinstalovaných VPS nahrávat automaticky. Klíče můžeme kdykoliv do běžícího VPS také nahrát pomocí formuláře v detailech VPS, hned pod formulářem na nastavení hesla.

Deploy public key to /root/.ssh/authorized_keys

Public keys can be registered in [profile settings](#).

Public key:



Go >>

From:

<https://kb.vpsfree.cz/> - Znalostní Báze

Permanent link:

<https://kb.vpsfree.cz/navody/server/ssh>

Last update: **2016/11/28 13:38**