# SSH

 **Tento návod je určen pro pokročilé uživatele**

 **SSH** poskytuje zabezpečený vzdálený přístup příkazovou řádkou, vzdáleného spouštění grafických aplikací, bezpečného přesunu souborů pomocí protokolů zabezpečeného kopírování (SCP) a zabezpečeného FTP. Dodatečně může také sloužit jako šifrovací tunel pro ostatní aplikace za pomoci přesměrování portů.

**SSH** nahrazuje starší, nezabezpečené aplikace jako *telnet*, *rlogin* a *FTP*. Tyto aplikace přenášely hesla po internetu bez šifrování, čímž mohla být hesla snadno odposlechnuta a ukradena. Použitím šifrování SSH těmto problémům předchází.

# Instalace SSH serveru

 Pokud se chcete bezpečně spojit s vaším počítačem z jiného počítače, musíte si nainstalovat server, který toto spojení dovolí. Poté se můžete připojit i z počítače běžícím na MS Windows (klient), například pomocí programu **Putty**. Ubuntu používá openssh-server, který můžete nainstalovat jako balík openssh-server.

# Vzdálený přenos souborů s použitím SSH

## Graficky (z prostředí GNOME)

 Správce souborů Nautilus umí přistupovat na vzdálené počítače pomocí SSH, procházet a přenášet soubory. Klikněte na **Místa → Připojit se k serveru**. Vyberte **SSH** v poli **Typ služby**, do pole **Server** napište jméno nebo IP adresu počítače na který se hodláte připojovat, do pole **Jméno uživatele** zadejte uživatelské jméno, pod kterým se chcete přihlásit a do pole **Název, který pro spojení používat** zadejte libovolný název spojení.

Soubory mohou být kopírovány přetažením mezi nově otevřeným a jiným oknem Nautilu. Funkce Drag&Drop.

 Další informace můžete nalézt v článku Připojení vzdálených zdrojů.

# Graficky (z prostředí KDE)

 Konqueror umí také přistupovat na vzdálené počítače pomocí SSH, procházet a přenášet soubory. Otevřete Konqueror a do adresního řádku napište:

```
fish://uživatelské_jméno@adresa_serveru
```

Soubory mohou být kopírovány přetažením mezi nově otevřeným a jiným oknem, mezi tímto oknem a záložkou nebo mezi záložkami Konqueroru.

 Další informace můžete nalézt v článku Připojení vzdálených zdrojů.

# Graficky (ze systému MS Windows)

 Pro přenos souborů mezi počítačem s Windows a počítačem s Ubuntu můžete použít program WinSCP, který můžete (zdarma) stáhnout z http://winscp.net.

# Použitím příkazové řádky

 Pro kopírování souborů z vašeho počítače do jiného se spuštěným SSH serverem, budete potřebovat zabezpečené kopírování (secure copy) - příkaz **scp**. Použití příkazu by mělo vypadat asi takto:

```
scp <soubor> <uživatelské_jméno>@<IP_adresa_nebo_název_PC>:<cílový_adresář>
```

Příklad: Kopírování souboru `testování.txt` z lokálního počítače do adresáře `/home/jirka/stahování` na vzdáleném počítači `192.168.1.103` s uživatelem `jirka`:

```
scp testování.txt jirka@192.168.1.103:stahování/
```

Jiný příklad:

```
scp "Nový dokument.odt" jirka@laptop:"/home/jirka/Léto 2005"
```

Takže do příkazu musíte zahrnout `<název souboru>`, `<uživatelské jméno>` na počítači ke kterému se přihlašujete a `<cílový adresář>` do kterého hodláte soubory přesouvat. Cestu `<cílový adresář>` je možné zadat absolutně, nebo relativně vzhledem k domovskému adresáři.

Pro kopírování souborů ze vzdáleného počítače na místní disk použijte příkaz:

```
scp franta@192.168.1.103:/home/franta/jinýsoubor.txt .
```

Znak „`.`“ znamená, že se soubor bude kopírovat do aktuálního adresáře. Místo „`.`“ můžete napsat název souboru (např. `můjsoubor.txt`) a soubor se při kopírování současně přejmenuje na zadaný název.

Dva užitečné parametry příkazu **scp** jsou `-r` a `-C`. `-r` umožňuje rekurzivní kopírování, to je vhodné v případě, že chcete zkopírovat celý strom (strukturu) adresářů (tzn. včetně všech podadresářů). `-C` povolí kompresi, což může vést ke zvýšení přenosové rychlosti na internetových linkách (na místní síti je doporučené kompresi nezapínat). Parametr `-C` je také možno použít s příkazy ssh a sftp.

Upozornění: Nemůžete přenášet soubory pomocí **scp** mezi dvěma vzdálenými počítači. Buď zdrojový nebo cílový soubor musí být na lokálním počítači. Pokud chcete přenášet soubory mezi dvěma vzdálenými počítači, musíte se na jeden z nich připojit pomocí **ssh**.

Poznámka: Pokud je vaše místní přihlašovací jméno stejné jako vaše přihlašovací jméno na vzdáleném počítači, poté můžete část před zavináčem „uživatelské_jméno@“ vynechat. Pokud je vynechaný vzdálený adresář, pak je standardně použit domovský adresář.

```
scp 192.168.1.103:soubor.txt .
```

Zkopíruje soubor `soubor.txt` z domovského adresáře aktuálního uživatele na vzdáleném počítači 192.168.1.103 do aktuálního adresáře.

# Přihlášení na vzdálené počítače přes SSH


Pro připojení na vzdálený počítač s běžícím ssh-serverem byste měli zadat:

```
ssh <uživatelské_jméno>@<jméno_počítače nebo IP adresa>
```

příklad:

```
ssh joe@laptop
```

další příklad:

```
ssh franta@192.168.1.103
```

# Ověření veřejného klíče


Kdysi všichni používali k prokazování identity klasické uživatelské jméno a heslo. Nicméně pokud někdo uhodl nebo odposlechl vaše heslo, tak bylo veškeré zabezpečení pryč. Proto SSH nabízí **ověření veřejného klíče**. To využívá privátní a veřejné klíče namísto jednoduchých hesel.

Pokud ještě nemáte privátní klíč, tak byste si měli jeden udělat. Napište:

```
ssh-keygen -t dsa
```

Poté budete dotázáni, kam má být privátní klíč uložen (pouze potvrďte standardní umístění) a k určení vstupní fráze. Vstupní fráze je použita k zašifrování vašeho privátního klíče. Každý, kdo se dostane k vašemu (nezašifrovanému) privátnímu klíči bude mít vaše práva na jiných počítačích. Na chvíli se zastavte a zapřemýšlejte nad opravdu dobrým heslem. Pokud si nevíte rady, podívejte se na stránku o výběru bezpečného hesla .

Pro získání přístupu do vzdálených počítačů musí tyto počítače vašemu veřejnému klíčí **důvěřovat**. Váš veřejný klíč byl vytvořen společně s novým privátním klíčem. Obvykle bývá umístěn v:

```
~/.ssh/id_dsa.pub
```

Cílový uživatel musí mít tento klíč (je to řádek ASCII znaků) ve svém souboru autorizovaných klíčů umístěného v:

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

na cílovém počítači. Takže buď zkopírujte a vložte tento řádek do souboru s autorizovanými klíči a nebo použijte příkaz `ssh-copy-id`:

```
ssh-copy-id -i ~/.ssh/id_dsa.pub pepa@maxipesfik
```

Budete dotázáni na pepovo heslo na cílovém počítači. Pokud je ověřování pomocí hesla vypnuté, pak musíte zkopírovat a vložit váš klíč za použití jiného média. Poté, co bude váš veřejný klíč přidán, se stanete pro tento počítač důvěryhodní.

Pro použití ssh-copy-id potřebujete mít vaši vstupní frázi uloženou v ssh-agentovi ssh-add (viz. níže).

Spusťte:

```
ssh pepa@maxipesfik
```

a dotaz už by neměl být na heslo ale na **vstupní frázi**. Prosím všimněte si, že heslo a vstupní fráze dělají rozdílné věci. Heslo je uloženo v `/etc/passwd` cílového systému. Vstupní fráze je použita pro dešifrování vašeho privátního klíče na vašem (lokálním) systému.

Pro zopakování: lepší ochrana při použití ověřování veřejného klíče oproti ověřování pomocí hesla je v tom, že pro získání přístupu potřebujete dvě věci:

- váš (zašifrovaný) privátní klíč
- vaši vstupní frázi (která je potřebná pro dešifrování privátního klíče)

Takže pokud nebudete používat vůbec žádné heslo (což je možné - viz. další kapitola), budete mít ještě méně bezpečnosti než při použití hesla samotného.

Ověřování pomocí hesla je standardně v Ubuntu zapnuto. Pokud chcete zabránit uživatelům ve vzdáleném přihlašování pomocí hesla, tak v souboru `/etc/ssh/sshd_config` změňte `PasswordAuthentication no`. Nezapomeňte restartovat váš ssh server po změně konfigurace pomocí příkazu(sudo /etc/init.d/ssh restart) nebo nověji od verze Ubuntu 8.10 sudo service ssh

restart).

# Omezení SSH přístupu

 Při použití SSH ověřování veřejných klíčů je zde další užitečná vlastnost. Cílový server může omezit příkazy, které budou povoleny. Pokud spravujete CVS zdroj, můžete použít řádek podobný tomuto v souboru `authorized_keys`:

```
command="/usr/bin/cvs server" ssh-dss AAAAB3N....
```

Toto vám umožní spustit pouze tento příkaz. Nic jiného.

# Automatický přístup v dávkovém skriptu

Ověřování veřejného klíče (viz. výše) může být také použito pro zautomatizování úkolů, které obvykle vyžadují psaní hesla. Představte si, že chcete zkopírovat soubor ze vzdáleného počítače každý den o půlnoci. Vše co potřebujete udělat je vytvořit „důvěru“ mezi těmito dvěma počítači. Vytvořte servisní účet na jednom počítači, vytvořte dvojici klíčů (ssh-keyge -t dsa) a až budete dotázáni na vstupní frázi, tak pouze stiskněte 'ENTER'. To nechá váš klíč nezašifrovaný. Přidejte veřejný klíč do „souboru autorized_keys2“ na druhém počítači (ssh-copy-id). Nyní se můžete připojit k tomuto počítači pomocí SSH bez toho, aniž abyste byli dotázáni na vstupní frázi. Přidejte toto SSH volání do vaší cron tabulky a je hotovo.

 **Buďte opatrní!** Mít nezašifrovaný privátní klíč může být velké bezpečnostní riziko. Hackerovi bude stačit dostat se k tomuto privátnímu klíči a může získat přístup na vzdálený počítač, který tomuto klíči důvěřuje.

# Použití ssh-agenta

Pokud často kopírujete soubory přes SSH nebo přistupujete na ostatní počítače ve vaší síti (což bývá obvyklá činnost administrátora), tak možná přemýšlíte, jestli neexistuje nějaká snadnější cesta pro zadávání vstupní fráze. A skutečně existuje - je to volání **SSH agenta**. Vy pouze jednou zadáte vaši vstupní frázi za použití příkazu „ssh-add“ a všechno co zadáte jako podproces SSH agenta si tuto frázi bude pamatovat.

Příliš mnoho teorie? V podstatě se nemusíte věcmi okolo agenta trápit. Vaše X sezení totiž automaticky běží v sezení ssh-agenta. Vše co potřebujete je spustit příkaz „ssh-add“ a napsat vaši vstupní frázi. Příště, až použijete **SSH** pro přístup k jinému počítači, už nebudete muset vaši vstupní frázi znovu zadávat. Hezké, ne? 🙂

 Měli byste zamknout vaši plochu pokud odcházíte od počítače. Jiní lidé mohou přes váš počítač získat přístup ke vzdáleným počítačům pomocí ssh i bez znalosti vaší vstupní fráze.

Pokud chcete být znovu dotázáni na vaši vstupní frázi po každém přihlášení do Ubuntu, můžete si přidat volání „ssh-add“ takto, přidejte `ssh-add` do aplikací spouštěných při startu systému:

 **Systém → Volby → Sezení → Programy po přihlášení → Přidat**

Při příštím přihlášení byste měli být dotázáni na vaši vstupní frázi.

 Uživatelé KDE mohou ssh-add využít také.

Spusťte příkaz

```
ln -s /usr/bin/ssh-add .kde/Autostart
```

Odhlaste se z KDE sezení a přihlaste se zpět. Vyskočí nabídka s dotazem na vaši vstupní frázi.

# Bezpečnost

 Přihlášení uživatelů a ostatní data jsou uložena v souboru `/var/log/auth.log` (a `auth.log.0`, atd.). Pokud chcete vědět, zda se někdo pokoušel přihlásit na váš systém, můžete prozkoumat protokoly. Příkaz

```
awk '/Invalid user/ {print $8}' /var/log/auth.log{,.0} | sort | uniq -c
```

vám ukáže, kdo se (nejspíš automatický útok) snažil přihlásit s neplatným uživatelským jménem a počet pokusů o přihlášení s tímto jménem.

Pro seznam uživatelů a kam se přihlásili slouží příkaz „last“; „lastb“ (last bad - poslední špatný) vám dovolí udělat rychlou kontrolu.

Pro zvýšení bezpečnosti se podívejte na sekci *Pokročilé nastavení* níže.

# Pokročilé nastavení

Podívejte se na stránku Pokročilé OpenSSH pro pokročilá nastavení a extra zabezpečení.

# GPG & OpenSSH

Podívejte se na stránku GPG podepisování pro SSH pro použití GPG pro podepsání SSH klíčů.

# OpenSSH 4.3 VPN

OpenSSH verze 4.3 přidala schopnost vytvořit tunely; podívejte se na stránku SSH VPN pro informace, jak nastavit VPN (virtuální privátní síť) za použití této vlastnosti.

# Odkazy

- SCP - bezpečné kopírování
- SSH: Best Practices