FOTO: WESTEND61/GETTY IMAGES

Dálkové ovládání Windows přes SSH

Bezpečný vzdálený přístup

SSH server OpenSSH umožňuje bezpečné ovládání systému Windows na dálku. Můžete také přenášet šifrované soubory a používat na dálku PowerShell. Jediné, co musíte udělat, je aktivovat si server.

ANDREAS DUMONT, RADEK KUBEŠ

Přístup k počítači prostřednictvím šifrovaného připojení a provádění administrativních úkonů přes terminál je ve světě Linuxu běžnou součástí života uživatelů. Systém Windows ale takovou možnost dlouho nenabízel, protože v něm nebyl implementován Secure Shell (SSH). Nicméně od doby, kdy byl OpenSSH portován pro Windows 10 a 11, je možné ovládat Windows i na dálku. Potřebný SSH server ale není ve výchozím nastavení k dispozici – musíte jej sami aktivovat. Spolu s rozhraním SSH získáte také nástroje SCP a SFTP založené na SSH pro bezpečný přenos souborů.

Jakmile bude vytvořeno bezpečné připojení, budete moci přistupovat k příkazovému řádku vzdáleného počítače a používat jej ke spouštění všech příkazů přes SSH. Můžete tak například vytvářet zabezpečené zálohy. Jedna z výhod SSH spočívá v tom, že protokol funguje ve všech operačních systémech a ve výchozím nastavení je implementován v distribucích Linuxu i systému macOS.

Jak na to

Ukážeme vám, jak aktivovat OpenSSH server ve volitelných funkcích systému Windows, jak jej nainstalovat a nakonfigurovat i jak navázat spojení na dálku.

1. Aktivování SSH serveru

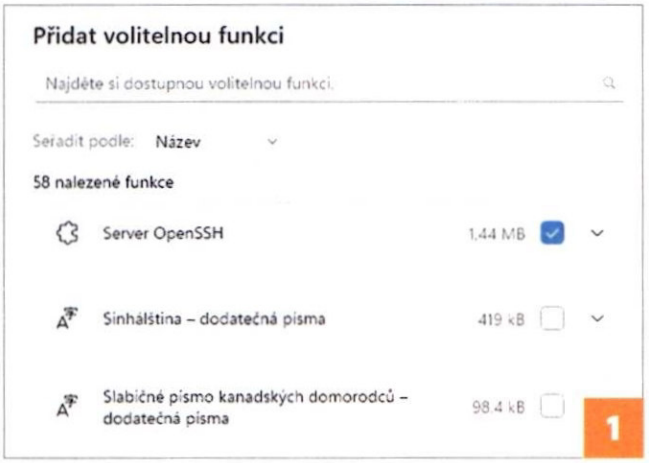
Například prostřednictvím nabídky „Start" otevřete „Nastavení" a přejděte na „Aplikace | Volitelné součásti". Pak klikněte na tlačítko „Zobrazit funkce" u položky „Přidat volitelnou funkci" a v nově otevřeném okně vyhledejte položku „Server OpenSSH". Stejným způsobem můžete postupovat ve Windows 10 i 11.

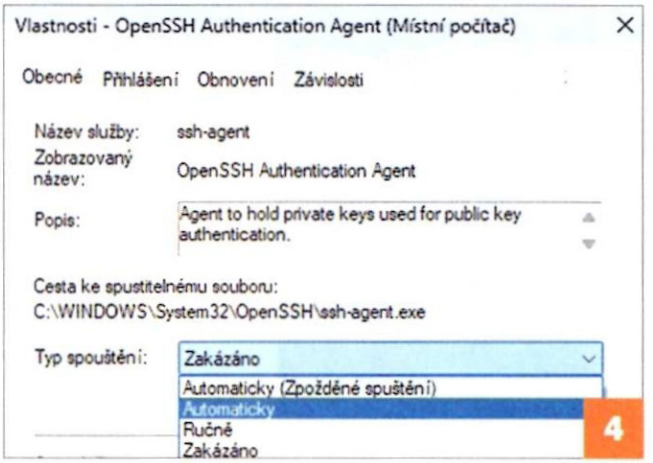
2. Instalace SSH serveru

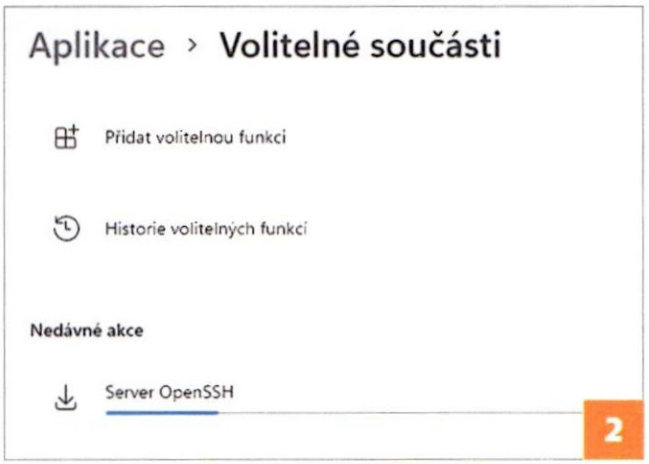
Klinutím na „Instalovat" nebo na „Další | Nainstalovat" ve Windows 11 stáhnete a nainstalujte server OpenSSH. Instalační adresář je „%WINDIR%\System32\OpenSSH". Po prvním spuštění serveru najdete konfigurační soubory v adresáři „%ProgramData%\ssh".

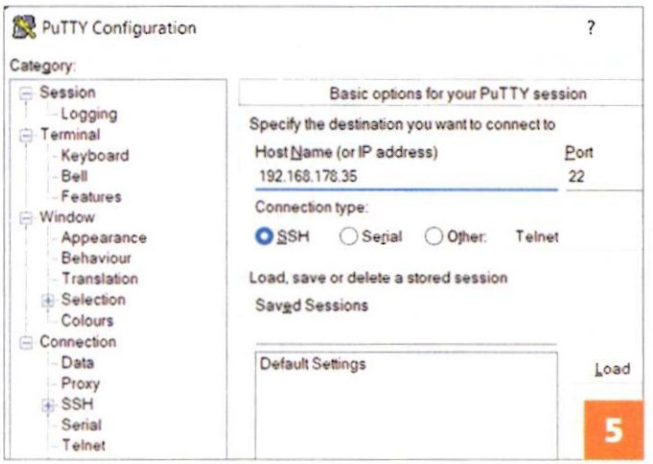
3. Kontrola nastavení firewallu

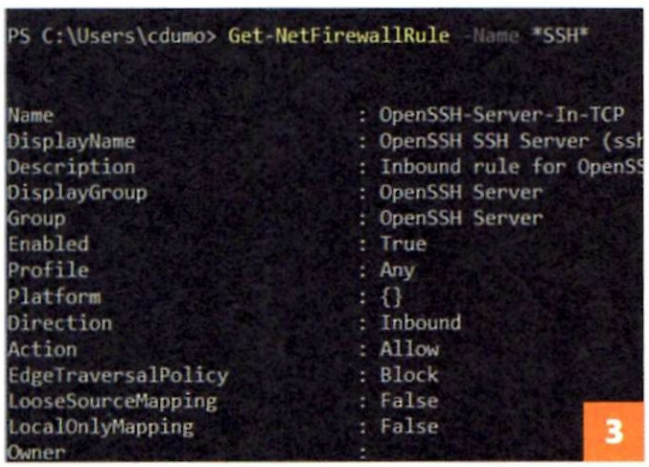
Nyní byste měli zkontrolovat, jestli je ve firewallu správně nastavené pravidlo pro příchozí připojení přes SSH. Za tímto účelem otevřete PowerShell a spusťte příkaz „Get-NetFirewallRule

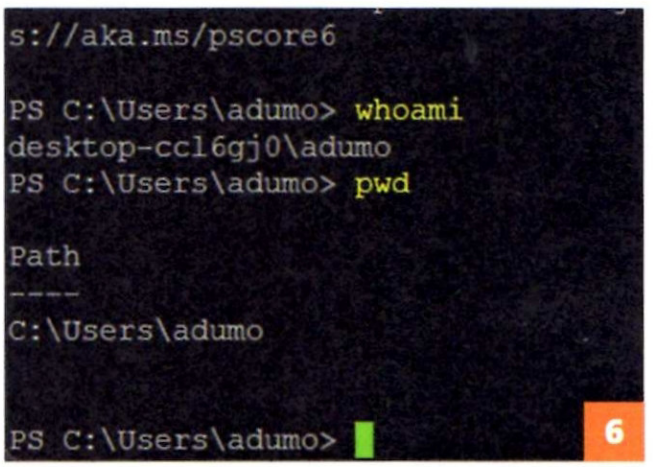












-Name *SSH*". Pokud je na řádku „DisplayName" přítomna položka „OpenSSH SSH Server (sshd)", znamená to, že je vše v pořádku.

4. Konfigurace služeb

Server OpenSSH se skládá z následujících dvou služeb: „OpenSSH Authentication Agent" a „OpenSSH Server". Ani jedna ze služeb nebude ve výchozím nastavení spuštěna a jejich typy spuštění budou buď „Ručně", nebo „Zakázáno". Stisknutím klávesové zkratky [Windows] + [R] vyvolejte dialogové okno „Spustit" a zadejte „services.msc". V okně „Služby" pak u obou zmíněných služeb nastavte typ spuštění na „Automaticky". Server SSH bude díky tomu v provozu i po restartování systému.

5. Navázání spojení

Chcete-li navázat spojení mezi počítačem se systémem Windows nebo Linux a serverem SSH, zadejte do příkazového řádku „ssh name@IP address", tedy jméno uživatelského účtu a IP adresu vzdáleného počítače, jako například „ssh adumo@192.168.178.35". Jako SSH klienta lze v systému Windows použít například program PuTTY. Při prvním navázání SSH spojení budete dotázáni, zda chcete přijmout otisk klíče hostitele. Ten je uložen v souboru „known_hosts". Odpovězte „yes" a následně zadejte heslo ke svému účtu Microsoft. Alternativně můžete také, jak je zvykem v Linuxu, nastavit ověřování pomocí veřejného klíče.

6. Vzdálené ovládání počítače

Nyní se ocitnete v příkazovém řádku vzdáleného počítače, kde budete mít všechny obvyklé možnosti ovládání. V případě potřeby můžete také na dálku přistupovat k prostředí PowerShell.

autor@chip.cz