Installation und Nutzung von SSH

ITS-Net-Lin

Sebastian Meisel

7. Dezember 2024

Open Secure Shell (OSS) ist eine kostenlose und offene Implementierung des Secure Shell-Protokolls. Es bietet sichere Remote-Zugriff auf Ihren Server oder Arbeitsplatz, der es ermöglicht, von überall aus mit SSH-Clients wie PuTTY auf Windows zu verbinden.

1 Open Secure Shell installieren

System aktualisieren Bringen Sie zunächst die Systemquellen und das gesamte System auf den aktuellsten Stand:

```
sudo apt update && sudo apt full-upgrade -y
```

OSS-Paket holen Installieren Sie das OSS-Paket mit dem folgenden Befehl:

```
sudo apt install openssh-server -y
```

Das `-y` am Ende besagt, dass wir zustimmen, alle vorgeschlagenen Paket zu installieren. Ohne diese Option, müssen Sie später noch die Installation der benötigten Abhängigkeiten bestätigen.

2 Verbindung mit SSH von Windows aus mittels Powershell

Powershell öffnen Starte die PowerShell-Anwendung auf Ihrem Windows-Rechner.

Verbindung herstellen Geben Sie den folgenden Befehl ein, um eine Verbindung herzustellen:

```
ssh username@openssh-server-ip-address -p 22
```

Ersetzen Sie `username` durch Ihren Benutzernamen unter Linux und `openssh-server-ip-address` durch die IP-Adresse die Linuxrechners.

2.1 Config Datei

Ein bequemerer Weg SSH zu nutzen, ist es für jeden Host, mit dem Sie sich verbinden wollen, einen Eintrag in der config-Datei von OSS zu machen.
Dafür brauchen wir zunächst das Verzeichnis `.ssh` im Nutzer Verzeichnis. Dies erstellen wir unter Windows in der Powershell oder unter Linux in der Bash mit demselben Befehl:

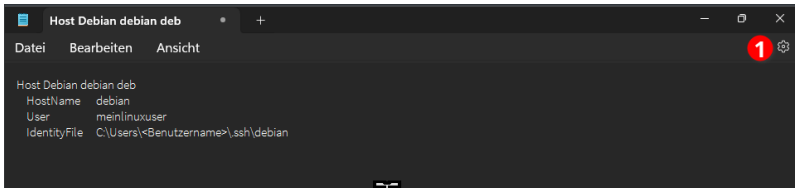
```
mkdir .ssh
cd .ssh
```

Mit dem zweiten Befehl wechseln Sie in das Verzeichnis. Nun müssen wir config-Datei erstellen. Unter Windows, geht dies am einfachsten mit dem Editor. Erstellen Sie eine Datei mit folgendem Inhalt

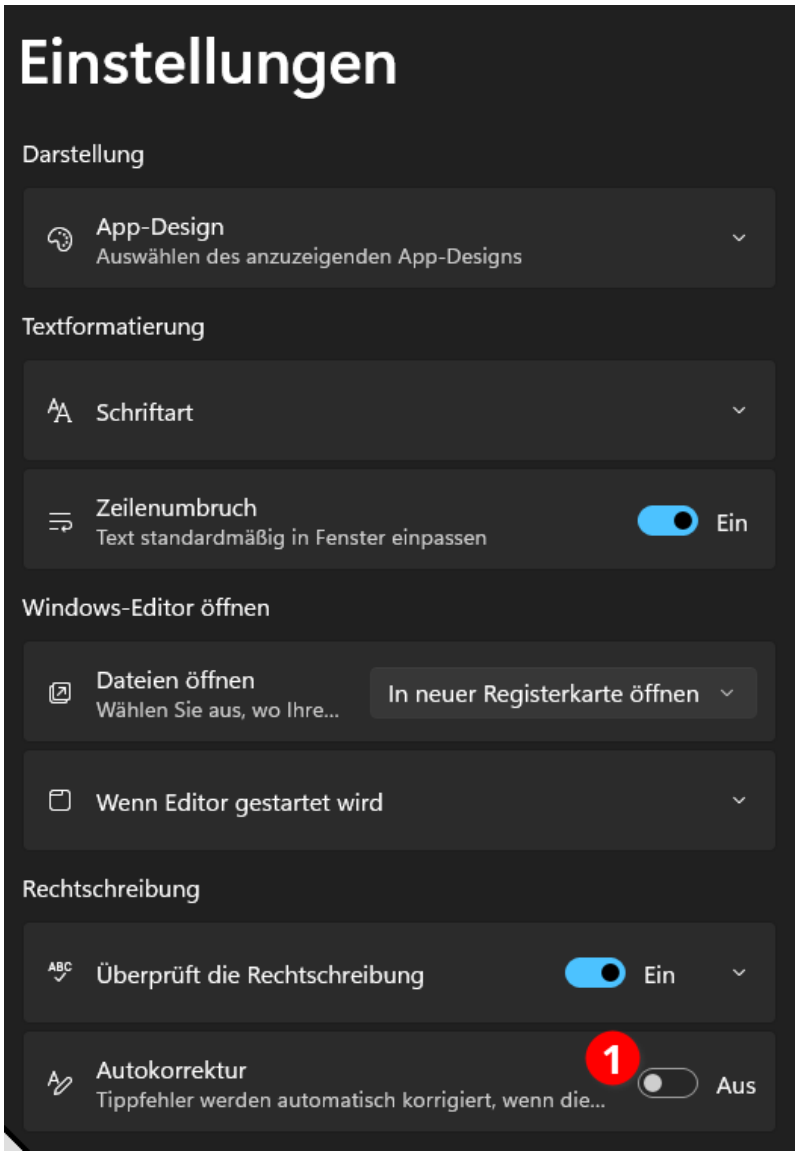
```
Host Debian debian deb
    HostName  debian
    User  meinlinuxuser
```

Ersetzen Sie dabei `meinlinuxuser` durch Ihren Benutzernamen unter Linux.

Tipp: Deaktivieren Sie Autokorrektur im Editor.



Klicken Sie dazu auf das Zahnrad (1) …



und deaktivieren Sie dann die Autokorrektur.

Speichern Sie nun die Datei -> Speichern unter im Verzeichnis `C:\Benutzer\<Nutzername>\.ssh\config.txt`.
Nun müssen Sie die Datei in der Powershell kopieren:

```
cp .\config.txt .\config
```

Achten Sie darauf, dass Sie im Verzeichnis `.ssh` sind. Nun können Sie sich mit einem der Namen, die Sie unter Host angegeben haben, per `ssh` mit dem Host verbinden.

```
ssh debian
```

2.2 Datenübertragung mit SCP

SCP-Befehl Geben Sie den folgenden Befehl ein, um eine Datei von Ihrem lokalen Rechner auf den entfernten Server zu kopieren:

```
scp C:\Path\ToLocalFile.txt debian:/remote/path/
```

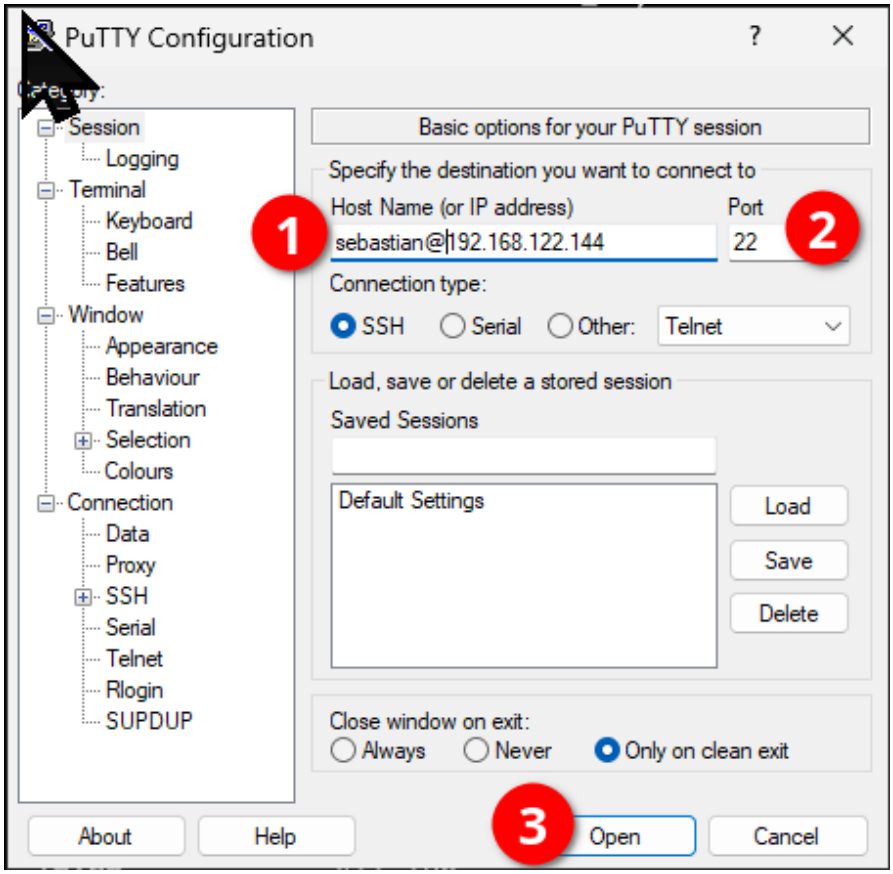
Ersetzen Sie wieder `username` durch Ihren Benutzernamen unter Linux und `debian` durch den Hostnamen Ihres Linuxrechners, wie Sie ihn in der config-Datei definiert haben.

SCP-Befehl (Gegenrichtung) Um eine Datei von dem entfernten Server auf Ihren lokalen Rechner zu kopieren:

```
scp username@openssh-server-ip-address:/remote/file.txt C:\Path\ToLocalFile.txt
```

Ersetzen Sie auch diesmal `username` durch Ihren Benutzernamen unter Linux und `openssh-server-ip-address` durch die IP-Adresse die Linuxrechners.

3 Verbindung mit SSH von Windows aus mittels PuTTY



Tragen Sie …

1. … `username@openssh-server-ip-address` ein und ersetzen Sie dabei `username` durch Ihren Benutzernamen unter Linux und `openssh-server-ip-address` durch die IP-Adresse die Linuxrechners.
2. … den Port 22 ein.
3. Bestätigen Sie mit OK.

4 Tipps und Fehlerbehebung

Stellen Sie sicher, dass SSH-Verbindungen auf Ihrem OpenSecureShell-Server aktiviert sind. Überprüfen Sie, ob Ihr Windows-Clients die notwendigen Abhängigkeiten installiert hat (z.B. PuTTY oder OpenSSL). Wenn Sie Verbindungsausnahmen begegnen, überprüfen Sie Ihre Firewall-Einstellungen und stellen Sie sicher, dass Port 22 offen ist.