## Inhaltsverzeichnis

OpenSSH Server insta	llieren und einrichten (Debian)	 1
Terminalbefehl: sshfs		 1
ssh KevGen		2



# OpenSSH Server installieren und einrichten (Debian)

```
# Installation des ssh servers
apt-get install openssh-server

# Die Konfiguration des SSH-Servers lässt sich unter folgender Datei
anpassen.
# nano ist hier der Textedtor
nano /etc/ssh/sshd_config # Achtung! Beachte das 'd' in sshd_config

# Jede Änderung wir erst wirksam nachdem der ssh Server neue gestartet
wurde.
restart ssh
```

Eine genau Anleitung wie OpenSSH-Server unter Debian einzurichten ist.

OpenSSH-Server ist auch unter Windows 10 verfügbar. Hier finden Sie eine Installationsanleitung.

CCC

## Terminalbefehl: sshfs

Über einen SSH-Dienst (openssh, ssh) werden verschlüsselte Verbindungen zum entfernten Linux-System hergestellt. Üblicherweise wird dies über ein Terminalprogramm (PuTTY) erstellt um das entfernte System zu warten und Software zu installieren.

Auf diese Weise lassen sich mit den Programm sshfs auch eine permanente Verbindung zum entfernten System erstellen. Dabei wird die Übertragen verschlüsselt durchgeführt.

Folgende Befehle müssen über das Terminal ausgeführt werden. Siehe auch die Ausführungen unter DigitalOcean.

Mit sshfs lassen sich auch Remote-Ordner von externen Servern einbinden. Dazu muss ein ssh Zugriff ohne Passwort eingerichtet werden. Manchmal möchte man, dass ein eingens dafür eingerichteter User benutzt werden soll. Vorher möchte aber vieleicht noch wissen welche User im System (Linux) eingerichtet sind. Zudem möchte man, um z.B. einen Useraccount zu testen, sich am System als diesen User einloggen bzw ausgeben.

```
    sudo apt-get install sshfs
        Installation von SSHFS.
    sudo modprobe fuse
        (sshfs) in den Kernel laden.
    sudo addgroup fuse
        fuse erstellen (falls notwendig).
```

```
4. sudo adduser $USER fuse
                                                                 # Den
   aktuelle User zur Gruppe fuse hinzufügen.
 5. sudo chown root:fuse /dev/fuse
                                                                 # Rechte
   für den root-user einrichten.
 6. sudo chmod +x /dev/fuse
                                                                 # Rechte
   für den Ordner einrichten.
 7.
 8. sudo mkdir /mnt/remoteserver
                                                                 #
   Mountordner erstellen.
 9.
10. #Zugriff auf den Remoteserver mit ssh testen. (Zertifikat abgelaufen?)
11. ssh user@xxx.xxx.xxx.xxx
12.
                                                                 \# x=IP
   Adresse, Rootpasswort notwendig.
13. sudo sshfs -p 22 root@xxx.xxx.xxx:/ /mnt/remoteserver -o
   follow symlinks
14.
                                                                 # Der
   Zugriff kann auch über den DNS Name möglich...
15. sudo sshfs -p 22 client@server1.net:/home/client/exchange/
   /home/user/remote/server1/ -o follow symlinks
16.
17. ls -al /mnt/remoteserver
                                                                 # Listet
   Details über die Dateien im Remoteserver auf.
18. # Entfernen
19. fusermount -u /mnt/remoteserver
                                                                 # Mit
   diesem Befehl lässt sich der Mount (Ordner)
20.
                                                                 # wieder
   entfernen.
```

Um nun vom Terminal auf einen entfernten Server über ssh zugreifen zu können müssen Sie diesem mit folgendem Behfehl mounten. (Hier mit Beispieldaten)

```
sshfs -p 22 root@185.245.96.84:/ /mnt/remoteserver -o follow_symlinks
```

Damit wir auf das root Verzeichnis zugegriffen.

#### ssh KeyGen

Falls sich der Key auf dem Server ändert bzw. der Klient noch den alten Key besitzt und erneut versucht wird sich über ssh einzulogen wird folgende Fehlermeldung angezeigt.

#### 

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

SHA256:Xze72Yz7ceudcdxEpHpvdfgdfgrtzjkkliowqwe

Please contact your system administrator.

Add correct host key in C:\\Users\\jmz/.ssh/known\_hosts to get rid of this message.

Offending ECDSA key in C:\\Users\\jmz/.ssh/known hosts:8

ECDSA host key for 192.168.xxx.yyy has changed and you have requested strict checking.

Host key verification failed.

Mit folgendem Befehl kann der Klient Key gelöscht werden (Windows 10 Window PowerShell).

PS C:\Windows\system32> ssh-keygen -R 192.168.xxx.yyy

From

https://jmz-elektronik.ch/dokuwiki/ - Bücher & Dokumente

Permanent link:

https://jmz-elektronik.ch/dokuwiki/doku.php?id=start:linux:filesystem:sshfs&rev=1617030306

Last update: 2021/03/29 17:05

