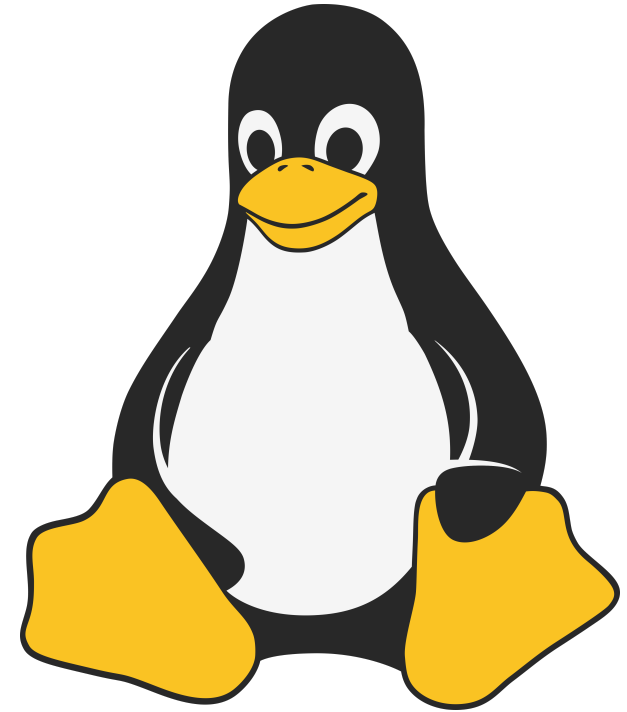


Passwortloses SSH-Login von Windows zu `debsrv` und `debian`



Inhaltsverzeichnis

- [Voraussetzung](#)
- [Vorgehen](#)
- [Schlüsselpaar erzeugen unter Windows](#)
- [Schlüsselpaar übertragen auf](#) `debsrv`

Voraussetzung

Wir können uns von `debian` zu `debsrv` und umgekehrt ohne Passwort einloggen.

Das `ssh`-Login von Windows auf die Linux-Systeme erfordert jedes Mal die Passwort-Authentifizierung.

Ziel: Wir wollen auch von Windows aus ohne Passwort-Authentifizierung auf die Linux-Systeme zugreifen.

Vorgehen

- Grundsätzlich ist das Vorgehen das gleiche wie bei der Einrichtung des schlüssel-basierten `ssh`-Logins zwischen den Linux-Systemen.
- Zum Erzeugen des Schlüsselpaars kann wie unter Linux das Kommando `ssh-keygen` verwendet werden.
- Das Kommando `ssh-copy-id` steht unter Windows **NICHT** zur Verfügung. Wir müssen den öffentlichen Schlüssel manuell (mit dem Kommando `scp`) auf die Linux-Systeme kopieren und dort ans Ende der Datei `~/.ssh/authorized_keys` anhängen.

Schlüsselpaar erzeugen unter Windows

```
C:\Users\hermann> ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\hermann/.ssh/id_rsa):
Created directory 'C:\\Users\\hermann/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\hermann/.ssh/id_rsa
Your public key has been saved in C:\Users\hermann/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ixITwf00PZcFKgDY1CDkfrx8L9BB85rXdNVYKYQ4Xhg hermann@tuxp14-win11
The key's randomart image is:
+---[RSA 4096]-----+
|o==o      E=.o.+..|
|o.. +=.   = o.+ o |
| .  o++oo oo. .  |
| . .  oooooo.    |
| . o+ + So.      |
|  o..* o o       |
|  oo.o .        |
|  .o.           |
|  .             |
+-----[SHA256]-----+
```

Schlüsselpaar übertragen auf `debsrv`

- Öffentlichen Schlüssel `id_rsa.pub` kopieren mit `scp` auf `debsrv`
- `ssh`-Login auf `debsrv` mit Passwort (wir erhalten eine Linux-Shell)
- Öffentlichen Schlüssel an die Datei `~/.ssh/authorized_keys` anhängen mit `cat id_rsa.pub >> ~/.ssh/authorized_keys`
- Öffentlichen Schlüssel-Datei `id_rsa.pub` löschen mit `rm id_rsa.pub`
- Abmelden von `debsrv` mit `exit`
- `ssh`-Login auf `debsrv` funktioniert jetzt ohne Passwort.

Beachten Sie:

- Beim Befehl `scp .ssh/id_rsa.pub hermann@debsrv.mshome.net:` in der 2. Zeile muss ganz am Ende ein `:` (Doppelpunkt) stehen.
- Beim Befehl `cat id_rsa.pub >> ~/.ssh/authorized_keys` in der 10. Zeile wird die Ausgabe des `cat`-Befehls umgelenkt und an die Datei `~/.ssh/authorized_keys` angehängt. Das Symbol zum Umlenken der Ausgabe ist `>>`. (Zwischen den beiden `>`-Zeichen darf kein Leerzeichen stehen.)

```
C:\Users\hermann> rem transfer the public key to remote host **WITH** password
C:\Users\hermann> scp .ssh\id_rsa.pub hermann@debsrv.mshome.net:
hermann@debsrv.mshome.net's password:
id_rsa.pub                                100% 747    364.8KB/s   00:00
C:\Users\hermann> rem last login to the remote host **WITH** password
C:\Users\hermann> ssh hermann@debsrv.mshome.net
hermann@debsrv.mshome.net's password:
...
hermann@debsrv:~$ # append the public key to the authorized_keys file
hermann@debsrv:~$ cat id_rsa.pub >> ~/.ssh/authorized_keys
hermann@debsrv:~$ rm id_rsa.pub # file no longer needed; remove it
hermann@debsrv:~$ exit
Abgemeldet
Connection to debsrv.mshome.net closed.
C:\Users\hermann> rem login to the remote host **WITHOUT** password
C:\Users\hermann> ssh hermann@debsrv.mshome.net
...
```


Durch Alkohol bringt man sich auf Stufen der Kultur zurück, die man überwunden hat.

-- Friedrich Wilhelm Nietzsche

```
hermann@debsrv:~$ date
```

```
So 16. Mär 20:21:08 CET 2025
```

```
hermann@debsrv:~$
```

Gezeigt wurde die Einrichtung des schlüssel-basierten `ssh`-Logins auf `debsrv`.

Das Vorgehen für `debian` ist analog.