

Aug 07, 17 18:05

putty-anmeldung-ohne-passwort-HOWTO.txt

Page 1/3

HOWTO zur schlüsselbasierten SSH-Anmeldung per Putty unter Windows

(C) 2012-2017 T.Birnthaler/H.Gottschalk <howtos(at)ostc.de>
 OSTC Open Source Training and Consulting GmbH
<http://www.ostc.de>

```
$Id: putty-anmeldung-ohne-passwort-HOWTO.txt,v 1.11 2017/08/07 16:05:05 tsbirn Exp $
```

Dieses Dokument beschreibt die Einrichtung einer schlüsselbasierten sicheren Verbindung zwischen Putty-Client auf einem Windows-Rechner und SSH-Dienst auf eine UNIX/Linux-Rechner.

INHALTSVERZEICHNIS

- 0) Installation
- 1) Schlüsselpaar für Authentifizierung erzeugen
- 2) Öffentlichen Schlüsselteil auf Ziel-Rechner eintragen
- 3) Verbindung zum Ziel-Rechner aufnehmen
- 4) Probleme bei der Verbindungsaufnahme lösen
- 5) Passwortbasierte Authentifizierung abschalten
- 6) Weitere Informationen

0) Installation

Das Installationspaket "putty-0.XX-installer.exe" von der ORIGINAL-Webseite

<http://www.chiark.greenend.org.uk/~sgtatham/putty>

holen und installieren (NICHT von einer anderen Webseite!)

1) Schlüsselpaar für Authentifizierung erzeugen

Das Programm "PuttyGen" aus Start --> Programme --> Putty aufrufen und ein Schlüsselpaar erzeugen: Dazu Button "Generate" drücken und die Maus solange beliebig bewegen, bis genügend Zufall zur Schlüsselgenerierung erzeugt ist. Der grüne Balken signalisiert den Fortschritt bei der Schlüsselgenerierung (läuft 2x durch).

2) Öffentlichen Schlüsselteil auf Ziel-Rechner eintragen

Den im Textfeld oben von "PuttyGen" angezeigten (langen) öffentlichen Schlüssel (public key) "ssh-rsa AAAA... == rsa-key-20140409" kopieren (ACHTUNG: wirklich ALLE Zeichen, z.B. per "Rechte Maustaste --> Alles auswählen" + "Rechte Maustaste --> Kopieren") und auf dem Ziel-Rechner bei einem Benutzer (z.B. "kurs") in die Datei "~/ssh/authorized_keys" eintragen (EINE Zeile!).

```
/home/kurs/.ssh/authorized_keys # Benutzer "kurs"
```

ACHTUNG: Ein mit "PuttyGen" gespeicherter öffentliche Schlüssel (Button "Save Public Key") ist leider nicht unter UNIX/Linux verwendbar (hat falsches Format).

Falls auf dem Ziel-Rechner im Heimatverz. "/home/kurs" von Benutzer "kurs" das Verz. ".ssh" oder die Datei ".ssh/authorized_keys" nicht existiert, diese anlegen + verrecken:

```
mkdir ~/.ssh # Verstecktes Verz. (wg. führendem Punkt)
touch ~/.ssh/authorized_keys # Tippfehler vermeiden
chown -R kurs.kurs ~/.ssh # Besitzer (Gruppe) (-R=Rekursiv)
chmod 755 ~/.ssh # Zugriffsrechte (--> rwxr-xr-x)
chmod 644 ~/.ssh/authorized_keys # Zugriffsrechte (--> rw-r--r--)
```

ACHTUNG: Den Namen der Datei "authorized_keys" ohne Tippfehler schreiben und die Verreckung des Verz. "~/ssh" und der Datei "authorized_keys" kontrollieren, d.h.:

```
ls -ld ~/.ssh ~/.ssh/authorized_keys # -l=long, -d=directory only
```

MUSS folgende Ausgabe liefern:

```
rwxr-xr-x kurs kurs ... /home/kurs/.ssh
rwxr--r-- kurs kurs ... /home/kurs/.ssh/authorized_keys
```

ACHTUNG: Beim Kopieren des öffentlichen Schlüssels aus dem Fenster von "PuttyGen" kein Zeichen vorne oder hinten vergessen, der Schlüssel funktioniert sonst nicht. Das korrekte Format sieht so aus:

```

      Je ein Leerzeichen
      +-----+
      |         |
      v         v
ssh-rsa AAAA...== rsa-key-20140409 # Zeile in "authorized_keys"
  ^         ^         ^
  |         |         |
KEYTYP     SCHLUESSEL KOMMENTAR (endet auf YYYYMMDD)
              (beginnt mit "AAAA" und endet mit "==")

```

ACHTUNG: Wird der "vi" zum Editieren der Datei "authorized_keys" benutzt, VOR dem Einfügen des Schlüssels per Maus in den INSERT-Modus schalten (z.B. per "i" oder "I" oder "o")! Sonst wird das 1. Zeichen "s" des kopierten Schlüsseltextes als "substitute"-Befehl des vi interpretiert und beim folgenden Einfügen des Schlüssels im kopierten Text unterschlagen!

ACHTUNG: Die letzte Zeile in "authorized_keys" MUSS mit einem Zeilenvorschub abgeschlossen werden (sonst Meldung "missing EOL at last line").

```

ssh-rsa AAAA...== rsa-key-20140409 # OK (Typ + Key + Kommentar)
sh-rsa AAAA...== rsa-key-20140409 # Falsch (Typ sh-rsa am Anfang falsch)
AAAA...== rsa-key-20140409       # Falsch (Typ ssh-rsa am Anfang fehlt)
ssh-rsa AAAA...                  # Falsch (...== am Keyende fehlt)

```

ACHTUNG: Das Kopieren per Maus ist NICHT SICHER, da es über Netzwerk erfolgt! Besser wäre ein Transport über einen 2. Weg (z.B. als Datei per USB-Stick). Zumindest sollte dann der Fingerprint des Originalschlüssels (vorlesen lassen) mit dem Fingerprint der Kopie auf Identität überprüft werden.

Den privaten Teil des erzeugten Schlüssels (private key) auf dem Windows-Rechner per Button "Save private key" abspeichern.

Die Passphrase kann leer gelassen werden, allerdings ist der private Schlüssel dann im Klartext auf der Windows-Maschine abgelegt und kann von anderen evtl. gelesen werden, die Zugriff auf diesen Rechner haben.

Besser ist es daher, eine Passphrase für den privaten Schlüssel zu vergeben. Diese ist dann bei jeder Verbindungsaufnahme per Putty zum Entsperren des privaten Schlüssels einzutippen oder kann mit dem Programm "Pageant" (Putty-Agent) automatisch zur Verfügung gestellt werden.

3) Verbindung zum Ziel-Rechner aufnehmen

Putty starten, eine Session zum Ziel-Rechner (hier "192.168.0.201") für den obigen Benutzer (hier "kurs") neu anlegen oder per "Load" einlesen:

```
kurs@192.168.0.201
```

Im Konfigurationsteil "Connection --> SSH --> Auth" der Sitzung den Pfad zur Datei mit dem gerade gespeicherten privaten Schlüssel eintragen

```
"Private key file for authentication:" [...] "Browse..."
```

Die Sitzung ordentlich BENENNEN + SPEICHERN nicht vergessen (dazu wieder im Konfigurationsteil auf "Session" positionieren und "Save" drücken")

Nun sollte eine schlüsselbasierte Verbindung mit dem Ziel-Rechner (ohne Passwort) möglich sein (aber evtl. mit Eingabe der Passphrase).

ACHTUNG: Bei der 1. Verbindungsaufnahme zum Ziel-Rechner erscheint eine Meldung, dass dieser Rechner noch nie besucht wurde und ein Fingerprint wird angezeigt. Dieser Fingerprint ist mit dem des Zielrechners manuell zu vergleichen und die Meldung ist zu bestätigen.

4) Probleme bei der Verbindungsaufnahme lösen

Bei Problemen mit der Verbindungsaufnahme auf dem Ziel-Rechner die Meldungen des SSH-Dämons "sshd" währenddessen in der Log-Datei beobachten:

```
sudo tail -f /var/log/auth.log
```

Typische Probleme sind:

- * Falsche Verreichtung des Verz./der Datei "~/ssh/authorized_keys" (z.B. Schreibrecht gesetzt für alle oder fehlendes x-Recht für alle)
- * Fehler beim Kopieren des Schlüssels nach "~/ssh/authorized_keys" (z.B. Windows-Format, Schlüssel nicht vollständig kopiert, "==" am Ende fehlt)
- * Falscher Name von Verz./Datei (z.B. "~/ssh/autorized-key")

Um mehr Log-Informationen zu erhalten, den Log-Level in "/etc/ssh/sshd_config"

erhöhen (nicht vergessen, den SSH-Server danach neu zu starten):

```
LogLevel DEBUG          # statt INFO
```

ACHTUNG: Nach der Fehlersuche den Log-Level wieder auf "INFO" zurücksetzen (und den SSH-Server neu starten), damit die Menge an Logdaten nicht zu stark wächst.

5) Passwortbasierte Authentifizierung abschalten

Sobald die schlüsselbasierte Anmeldung funktioniert, kann die passwortbasierte Anmeldung abgeschaltet werden (erhöhte Sicherheit). Dazu auf dem Zielrechner in der Konfigurations-Datei "/etc/ssh/sshd_config" des SSH-Daemons den Eintrag

```
PasswordAuthentication yes
```

gegen

```
PasswordAuthentication no
```

austauschen und den SSH-Daemon neu starten:

```
sudo /etc/init.d/ssh restart # SysV
sudo systemctl ssh restart  # Upstart
```

6) Weitere Informationen

Die öffentlichen Schlüssel der Hosts, mit denen man sich verbindet, landen in der Windows-Registry. Ebenso die Putty-Konfigurations- und Sitzungsdaten:

```
[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\*]
[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys]
```

Bei WinSCP landen Sie an folgender Stelle in der Windows-Registry:

```
[HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Configuration\*]
[HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Session\*]
[HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\SshHostKeys]
```

Weitere Hinweise zur Konfiguration von Putty sind zu finden unter:

--> [putty-konfiguration-HOWTO.txt](#)