

## Fernwartung des Schulservers übers Internet Anleitung ssh - putty – winscp - für Arktur v.4.x -

**Wichtige Vorbemerkung: Da sich die Version 4 noch in der Entwicklung befindet und immer wieder verändert wird, kann diese Anleitung nur Anregungen geben, wie man eine Fernwartung ggf. realisieren kann.**

Die folgende Anleitung beschreibt die Fernwartung des Schulservers z.B. von zu Hause über das Internet. Der Benutzer sollte sich im Klaren sein, dass er den zu wartenden Server durch die Öffnung nach außen potenziell gefährdet. Die Beschreibung orientiert sich daher auch an einer Datenübertragung mittels ssh und des gleichzeitigen Ausschaltens von telnet.

Voraussetzung für die Fernwartung ist natürlich die Kenntnis der z.Zt. gültigen IP-Adresse. Die einfachste Lösung ist das Anlegen eines Accounts bei [www.dyndns.org](http://www.dyndns.org). Die Vorgehensweise hierfür wird im Anhang dieser Anleitung beschrieben.

### 1. Schlüssel generieren:

Die Erstellung eines privaten und öffentlichen Schlüssels ermöglicht, den ssh-Daemon so zu konfigurieren, dass ein Zugriff auf den Server nur dann von außen möglich wird, wenn auf der anderen Seite, also dem Client zu Hause, der entsprechende Part vorhanden ist:

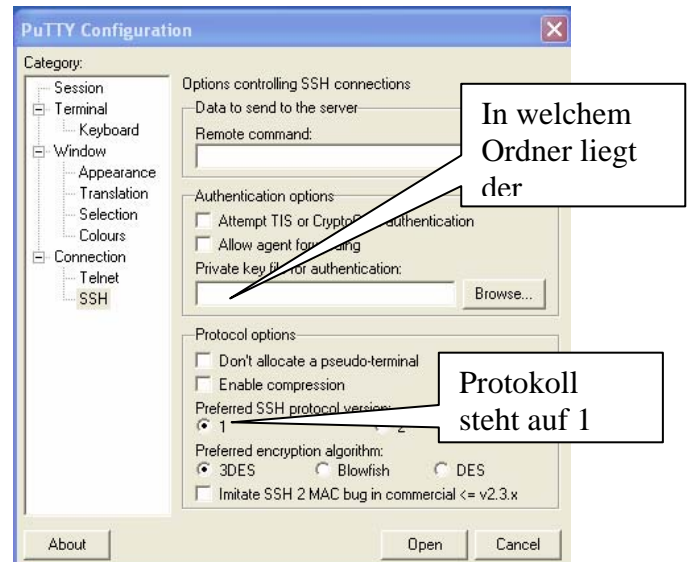
- Als root anmelden und an der Konsole und ausführen: `ssh-keygen -t rsa1`  
Im Ordner `/root/.ssh` befinden sich anschließend zwei Schlüssel: „identity“ und „identity.pub“.

*Anmerkung:* Falls man einem Kollegen ebenfalls Zugriff auf den Server von zu Hause aus geben möchte, etwa zum Hochladen von Arbeitsblättern, muss man dem Kollegen den Shellzugang erlauben (Sysadm-Menü: Anwender verwalten - einzelne Anwender verwalten - Den Shell-Zugang eines Anwenders ändern - Lehrer - Name - Vollzugang mit Prompt; dann Aktivieren nicht vergessen). Nun unter dem Namen des Kollegen anmelden und den o.a. Befehl ausführen. Das Schlüsselpaar findet man dann im /home-Verzeichnis des entsprechenden Users, also unter `/home/Lehrer/[NAME]`. Die weiter Vorgehensweise ist analog zu der hier für root Beschriebenen.

- Schlüssel duplizieren: Den Schlüssel `identity.pub` nach `authorized_keys` kopieren:  
`cp /root/.ssh/identity.pub /root/.ssh/authorized_keys`
- Schlüssel zum Client bringen: Den Schlüssel `identity` in das Verzeichnis des Clients kopieren, auf dem putty installiert ist. Am einfachsten geht das, indem man die Datei `identity` nach `/home/tmp` kopiert und erst einmal die Rechte ändert, so dass man sie anschließen von einem Client im Netz aus auf Diskette kopieren oder sich selbst per E-Mail schicken kann:  
  
`cp /root/.ssh/identity /home/tmp`  
`chmod 666 /home/tmp/identity`
- Man findet die Datei nun auf einem Client im Verzeichnis `t:`. Nach dem Kopieren dann auf jeden Fall löschen!

## 2. Schlüssel putty bekannt geben:

Im Putty-Konfigurations-Menü befindet sich unter connection der Menüpunkt SSH. Dort kann unter Private key file for authentication der Ordner angegeben werden, in dem jetzt die Datei identity abgelegt wurde. Unter SSH Protocol version muss als Version SSH 1 angegeben sein.



## 3. Sicherheitsmaßnahmen

Um sicherzustellen, dass der Anmeldende auch tatsächlich den richtigen Schlüssel besitzt, muss in der /etc/sshd/sshd\_config das Anmeldeverfahren umgestellt werden. Dort sollten folgender Schalter etwas in Zeile 56 gesetzt werden (Raute entfernen):

```
PasswordAuthentication no
```

Anschließend schaltet man noch Telnet ab: in /etc/inetd.conf die Zeile, die mit Telnet beginnt, auskommentieren (etwas Zeile 29).

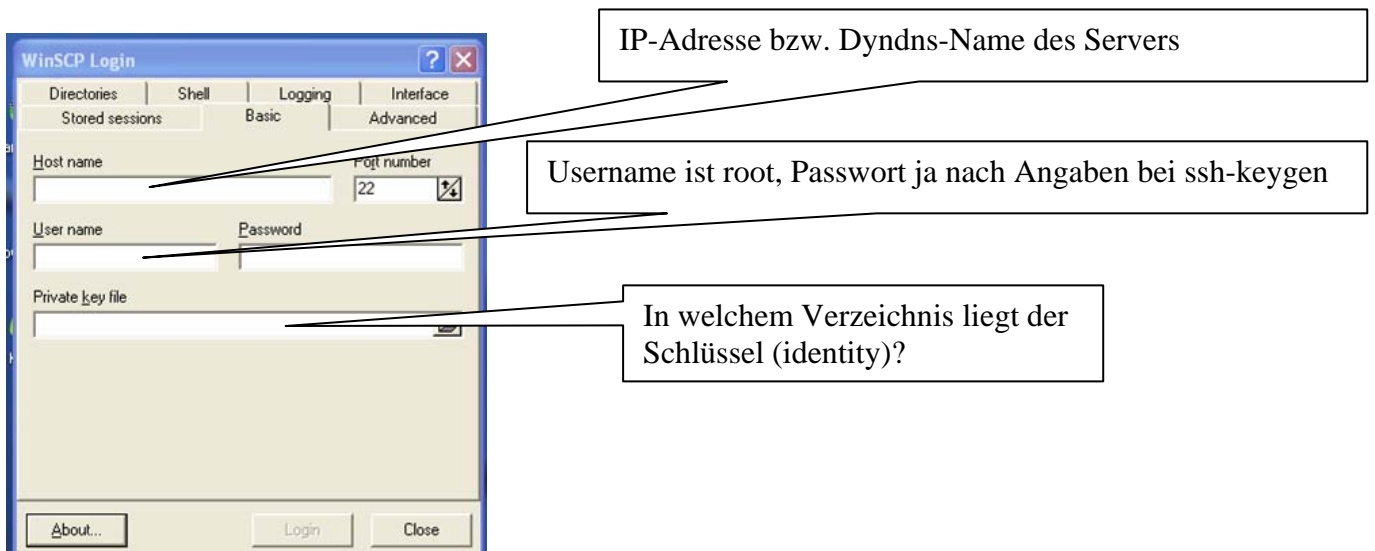
Danach muss der sshd neu gestartet werden:

```
/etc/init.d/sshd stop  
/etc/init.d/sshd start
```

Nun kann man sich nur noch mittels vorhandenem Schlüssel anmelden und so arbeiten, als säße man direkt vor dem Server.

## 4. Mit WINSOCP Dateien kopieren

Mit WinSCP lässt sich von jedem Client-Rechner aus alles auf den Server oder vom Server zum heimischen PC kopieren. Das Programm kann wie putty mit den generierten Schlüsseln umgehen, ist selbsterklärend und dürfte relativ sicher sein. Eine funktionierende Version von WinSCP wird bei der Installation des Servers automatisch nach /home/adm/software/winscp kopiert, von Client aus zu finden unter p:\software\winscp\winscp2.exe. Sie muss nur noch auf einen Client kopiert und ausgeführt werden.



## Anhang 1

### Einrichten eines Accounts bei [www.dyndns.org](http://www.dyndns.org) (Vgl. Anleitung „Webserver“)

Einen professionellen Dienst bietet z.B. [dyndns.org](http://www.dyndns.org) an. Bei der Eingabe einer dort beantragten Internetadresse wie z.B. <http://schulexyz.dyndns.org> sorgt dieses Service für die Weiterleitung an die richtige IP-Adresse. Damit wird der schulische Server auch hier weltweit immer unter derselben Adresse erreichbar.

Die IP-Adresse des schulischen Arkturs ändert sich mit jeder neuen Einwahl. Um also das oben beschriebene Verfahren durchführbar zu machen, muss diesem Dienstleister sofort nach der Einwahl von Arktur ins Internet automatisch die IP-Adresse übermittelt werden, die Arktur gerade zugeteilt bekommen hat. Das erledigt der Aufruf eines Scripts, das in die Datei `/etc/ppp/ip-up` eingebunden wird. Damit Arktur nicht offline geht, reicht ein regelmäßiges ping an irgendeine bekannte Webadresse aus.

Im Folgenden sei beispielhaft das Verfahren bei [dyndns.org](http://www.dyndns.org) beschrieben. Zunächst sichert man sich eine entsprechende Internetadresse, z.B. [schulexyz.dyndns.org](http://schulexyz.dyndns.org). Dazu ruft man die Seite bei [dyndns.org](http://www.dyndns.org) auf, lässt sich dort registrieren und erhält nach wenigen Minuten per Mail den Zugang zur Konfigurationsseite. Damit ist die Registrierung abgeschlossen.

Anschließend muss man nun die Internetadresse definieren, unter der der schulische Arktur erreichbar sein soll - auf der angesprochenen Webseite spricht man von einem Host bzw. man klickt auf **Add New Host**. In der folgenden



Eingabemaske bestimmt man die Internetadresse, hier also z.B. [schulexyz.dyndns.org](http://schulexyz.dyndns.org). Mit der Anmeldung hat man einen Benutzernamen und ein Passwort definieren können, mit denen man sich jederzeit wieder bei [dyndns.org](http://www.dyndns.org) einloggen kann und die man benötigt, wenn man später mittels des bereits erwähnten Scripts Arktur seine IP-Adresse automatisch übermitteln lässt.



Die Datei `dyndnsupdate.tgz` (Zusammenstellung nach einer Vorlage von Thomas Litsch, zu finden unter <http://www.linux-schule.de/downloads/dyndnsupdate.tgz>) kopiert man nun in das Wurzelverzeichnis (!) von Arktur und entpackt es an der Konsole mittels

```
tar xzvf dyndnsupdate.tgz.
```

Beim Auspacken werden einige Dateien in verschiedene Unterverzeichnisse entpackt. Davon muss die Datei `./etc/ppp/ip-up.local.dyndns` noch angepasst werden. Dieses Script übermittelt Arkturs augenblickliche öffentliche IP an [dyndns.org](http://www.dyndns.org). Öffnen Sie dazu die Datei mit `mc` und `F4` und tragen Sie an den ausgewiesenen Stellen den bei [dyndns.org](http://www.dyndns.org) gewählten Benutzernamen, das Passwort und den eben gewählten Hostnamen ein. Wenn Sie nun das Script einmal starten, meldet es Ihnen die erfolgreiche Übermittlung und ab sofort können Sie den schulischen Arktur per <http://schulexyz.dyndns.org> erreichen.

Um diese Verfahren zu automatisieren, muss der Aufruf innerhalb eines anderen Scripts erfolgen, das immer dann abgearbeitet wird, wenn Arktur eine Verbindung ins Internet herstellt. Öffnen Sie dazu die Datei `/etc/ppp/ip-up` ebenfalls mit `mc` und `F4` zum Editieren.

Etwa in der Zeile 44 findet man einen Eintrag `exit 0 ;;`. Vor (!) dieser Zeile fügen Sie eine neue Zeile mit dem Inhalt `/etc/ppp/ip-up.local.dyndns` ein. Bei schnellen Rechnern sollt zusätzlich vor dem Aufruf dieses Scripts noch eine Wartezeit definiert werden, besonders wenn man nur eine ISDN-Verbindung hat. Fügen Sie dazu den Befehl `sleep 30` noch ein.

Um sicher zu stellen, dass Arktur nicht offline geht, muss noch der standardmäßig vorhandene Eintrag `/etc/ppp/inet-off` aus der crontab entfernt werden. Zur Bearbeitung der crontab ruft man an der Konsole `crontab -e` auf.

Will man ein offline bzw. die Zwangstrennung von Arktur durch die Telekom grundsätzlich verhindern, fügt man in die crontab folgende Zeile ein `0-59/5 * * * ping -c1 www.irgendeineAdresse.de > /dev/null`. Damit wird alle fünf Minuten eine ganz kurze Verbindung ins Internet hergestellt.

Jetzt ist Arktur per ssh immer über <http://schulexyz.dyndns.org> erreichbar.

## Anhang 2

Falls die Fernwartung doch noch Probleme macht, beachten Sie bitte folgenden Hinweis, der uns von [gpeter@rs-prohn.de](mailto:gpeter@rs-prohn.de) gemailt wurde:

Hallo,  
ich habe heute die Anleitung zur Fernwartung des Arktur ausprobiert.  
Es klappt auch so weit, nur ihr solltet noch dazuschreiben, wie man die Firewall anpasst, damit der Port 22 auch geöffnet wird. Im "Ur-Zustand" sind alle Ports beim Arktur geschlossen.  
Die Zeile für die IP-Tables hab ich auch gefunden.

Für ISDN heißt die Zeile

```
$IPTABLES_BIN -A INPUT -i ippp0 -p tcp --dport 22 -j ACCEPT
```

Für DSL:

```
$IPTABLES_BIN -A INPUT -i ppp0 -p tcp --dport 22 -j ACCEPT
```

Ich habe das in `/etc/rc.d/ipfilter` eingetragen.  
Danach die `ipfilter` stoppen und starten und dann geht das auch.

MfG Peter

---

Fragen und Rückmeldungen speziell zur Anpassung der Anleitung an die Arktur-Version 4:  
[mahr@medienzentrum-oberberg.de](mailto:mahr@medienzentrum-oberberg.de)