# Zugriff zum Datenaustausch per scponly

## Warum scponly?

In der Grundkonfiguration der Musterlösung ist es notwendig, dass ein Benutzer, der die Möglichkeit haben soll von außen Dateien mit dem Server auszutauschen, einen Zugriff auf Shellebene benötigt. Das bedeutet, der Benutzer kann sich am Server anmelden und unter Linux dort Befehle ausführen, was die Systemsicherheit beeinträchtigen kann.

Mit scponly kann man

- Dataiaustausch von außen machen
- Der Benutzer hat keinen Shellzugang
- Wenn man möchte: Der Benutzer kann sein Heimatverzeichnis nicht verlassen

Aus dem letzten Punkt folgt auch ein kleiner Nachteil: Die Tauschverzeichnisse sind von Zuhause nicht erreichbar, und Linux Clients sind nicht mehr einsetzbar.

## **Etwas Theorie**

Die hier vorgestellte Möglichkeit besteht aus zwei Komponenten:

 Der Zugang wird nicht mehr mit einer Shell wie der in Linux übliche bash realisiert, sondern mit einer Shell namens scponly, die nur noch Befehle zur Verfügung stellt, die zum Dataiaustausch per scp notwendig sind. Der Beutzer darf aber auch mit dieser Shell immer noch in alle von System erlaubten Verzeichnisse wechseln und kann somit alle für seine Benutzerkennung lesbaren Dateien auch nach Hause kopieren. Sollten irgendwelche Zugriffsrechte nicht korrekt gesetzt sein, kann auf diese Weise auf sensible Informationen zugegriffen werden.

Man kann an dieser Stelle aufhören und hat bereits ein erhebliches Sicherheitsplus gegenüber dem für gewöhnlich notwendigen Schellzugang gewonnen.

2. Wenn man nun das Programm scponly und alle von ihm benötigten Teile (Bilbliotheken u.ä.) innerhalb jedes Homeverzeichnisses installiert, kann man den Zugang so konfigurieren, dass der Benutzer als Stammverzeichnis sein Heimatverzeichnis sieht – er kann also nicht in Verzeichnisse unterhalb seines Heimatverzeichnisses wechseln.

Nachteile: Speicherplatzbedarf (Kann man durch Hardlinks vermeiden) und kein Zugriff auf die Tauschverzeichnisse.

## Installation

Um die Übungen durchzuführen, muss es auf dem System den im ersten Teil der Fortbildung angelegten Benutzer *remote* geben. sollte dieser nicht existieren, legen Sie ihn bitte an oder übertragen Sie die Anweisungen auf einen Testbenutzer ihrer Wahl.

#### Übung und Schritt 1: scponly auf dem Server installieren

Laden Sie die Datei lml22-scponly-0.1.tgz von <u>http://www.gtr-wiki.de/</u> herunter. Packen sie die Datei mit dem Befehl tar xPzvf lml22-scponly-0.1.tgz aus.

Damit der Benutzer nur noch Zugang per scponly hat, muss man ihm in der Datei /etc/passwd als Shell das Programm /usr/local/bin/scponly zuweisen. Vor allen Änderungen an der Passwort- Datei empfiehlt es sich diese zu sichern, z.B. mit der Anweisung

cp /etc/passwd /etc/passwd.scponly

Jede Zeile der Passwortdatei folgt demselben Schema:

remote:x:1000:100::/home/remote:/bin/bash

Durch Doppelpunkte getrennt finden sich Benutzername:UserID:GruppenID:Bemerkungen:Heimatverzeichnis:Shell

Beachten Sie, dass die Bemerkungen in diesem Fall leer sind – es folgen zwei Doppelpunkte direkt aufeinander. Ändern Sie bitte den Eintrag für die Shell (am Zeilenende) beim Benutzer *remote* in /usr/local/bin/scponly

Nun muss die Shelländerung dem System noch mitgeteilt werden, dazu führen Sie bitte den Befehl

/etc/init.d/nscd restart

aus. Dies muss nach jeder Änderung an der Passwort Datei geschehen.



Versuchen Sie dann sich von einem Client- PC aus per putty als Benutzer remote am Server anzumelden. Sie sollten ein Ergebnis wie das im Screenshot dargestellte erhalten, wenn Sie nach der Anmeldung mit Passwort die Return Taste drücken. Sie haben also keine Kommandozeile zur Verfügung.

### **Testen mit WinSCP**

Laden Sie sich die Anwendung WinSCP von <u>http://winscp.net/eng/download.php</u> herunter. Wenn Sie das Paket "Standalone Application" wählen. muss das Programm nicht installiert werden, liegt aber auf Englisch vor. Für zu hause empfiehlt sich die

Installierbare Version auf Deutsch.

Diese Beschreibung bezieht sich auf die nicht installierbare Standalone Version des Programms. Durch einen Doppelklick startet es, sie werden aufgefordert, die Daten zu Zielserver und Konto einzugeben.

Host name: Hier kommt der DNS-Name oder die IP-Adresse des Servers rein

Port number: 22 (ssh)

User name: Benutzername...

Password: Ebendas...

Beim Protocol können Sie die Voreinstellung SFTP(allow SCP fallback) belassen.

Wenn Sie alles richtig gemacht haben und das Passwort zum Benutzer passt, erscheint zunächst eine Sicherheitswarnung, die man abnickt, bevor sich der Hauptbildschirm öffnet.

Warning						×		
<u>.</u>	The server's host key was not found it the cache. You have no guarantee that the server is the computer you think it is. The server's rea? key lineernint is:							
	ssh-rsa 1024 81:4e:f5	5:22.ba:2c:c3:b2:af:2e:3	5:da:24:d8:a9:5	ь				
	If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.							
	Continue connecting and add host key to the cache?							
		Yes	<u>N</u> o	Cancel	Help			

Wichtig ist, zu erkennen, dass man immer noch in alle für den Unix-Benutzer *remote* erlaubten Verzeichnisse wechseln darf. Im Screenshot befindet sich der Testbenutzer im Verzeichnis /etc/ und könnte sich problemlos die Passwortdatei

herunterladen, da diese für jeden Benutzer lesbar ist.

**Zwischenbilanz:** Die Benutzer können sich zwar nicht mehr direkt am Server anmelden, dennoch Dateien autauschen, aber mit Hilfe von WinSCP noch immer in Bereiche vordringen, von denen man sie möglicherweise gerne fernhalten würde.

📲 etc - scponly@albert.selfip.net - WinSCP 📃						
Local Mark Files Command	ls Session (	Options Remote I	Help			
🌘 🕞 🕐 • 🔐 🗳 ·	🔁 💷 🎤		🗑 🧔 Default	- 0	<b>5</b> •	
$\fbox{\begin{tabular}{c} $$ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $ $	1 🖾 🕅	🖞 🕑 🔄 🔓	🔁 etc 💌 🖙 ⇒	•	🕼 🙆 🔁 🐮	
C\Dokumente und Einstellungen\Frank\Eigene Dateien /etc						
Name /	Size	Туре 🔺	Name 🛆	Size	Changed 🔺	
<b>E</b>		Parent director	nntpserver	5	20.10.2000 19	
📇 Eigene Bilder		Dateiordner	🖬 nscd.conf	1.157	27.03.2003 17	
Eigene eBooks		Dateiordner	🖬 nsswitch.conf	1.342	04.05.2005 09	
🔂 Eigene Musik		Dateiordner	🖬 🖬 pam_smb.conf	30	19.02.2003 10	
🚞 schooldoc		Dateiordner	🖬 passwd	3.078	29.01.2006 18	
🖬 12M4-M-05=2F06.pdb	4.700	PDB-Datei	🖬 passwd-	3.021	29.01.2006 18	
🔁 Datenblatt_MA111.pdf	355.885	Adobe Acrobal	🖬 passwd.alt	2.194	25.10.2005 14	
🔁 Datenblatt_MA301.pdf	99.610	Adobe Acrobal	i permissions	20.259	25.09.2003 17	
🔁 Datenblatt_WAG311.pdf	185.877	Adobe Acrobal	🖬 permissions.easy	5.250	18.07.2000 00	
🔁 Datenblatt_WG111.pdf	151.578	Adobe Acrobal	permissions.local	565	20.10.2000 20	
📑 desktop.ini	78	Konfigurations	🖬 permissions.paranoid	19.209	29.06.2000 15	
	11.100	A dala A		[ 007	17 07 000 01	
0 B of 13.648 KB in 0 of 16			0 B of 1.828 KB in 0 of 255			
🚦 🖉 F2 Rename 📑 F4 Edit 🛽	🔓 F5 Copy 🛛	🔓 F6 Move 💣 F	7 Create Directory 🔀 F8 Delei	te 📑 F9 Prop	erties »	
36.872 B 571	B 🧕	) 🧖 🔒 aes	SFTP (v3)	0:01:10	1.	



### Übung und Schritt 2: Die Changeroot Umgebung

Laden Sie die Datei <u>lm122-scponly-changeroot-env-0.1.tgz</u> von <u>http://www.gtr-</u> <u>wiki.de/</u> herunter. Diese Datei enthält alle für die Changeroot- Umgebung nötigen Bestandteile. Wenn sie die Datei mit tar xPzvf lm122-scponly-changeroot-env-0.1.tgz entpacken, wird die Changeroot- Umgebung nach /home/scponly entpackt, es sollte keinen Benutzer mit diesem Namen auf dem System geben!

Wechseln Sie nach dem Auspacken in das Verzeichnis /home/scponly/ Sie finden die Unterverzeichnisse etc/ usr/ bin/ und lib/

### Von Hand einrichten

Um die Changeroot Umgebung für einen Benutzer "von Hand" einzurichten, muss man folgendes tun (Übung: Machen Sie es am Inselserver!)

- Im Verzeichnis des Benutzers alle Dateien und Verzeichnisse mit Ausnahme des windows-Verzeichnisses löschen (Achtung: Kollision mit Linux Clients!)
- Alle Unterverzeichnisse der Changeroot- Vorlage aus /home/scponly in das Home des Benutzers kopieren. Kontrollieren Sie anschließend, dass alle

000	haegar@sven:	/home/haegar 🦳
albert:/home/remote # ls total 16	-la	
drwxr-xr-x 3 remote	users 4096	Jan 30 16:29 .
drwxr-xr-x 11 root	root 4096	Jan 30 15:50
-rw 1 remote	users 29	Jan 29 19:08 .bash_history
lrwxrwxrwx 1 remote	users 30	Jan 29 17:41 austeilen -> /home/remot
e/windows/austeilen		
lrwxrwxrwx 1 remote	users 20	Jan 29 17:41 cdrom -> /usr/local/samb
a/cds		
lrwxrwxrwx 1 remote	users 31	Jan 29 17:41 einsammeln -> /home/remo
te/windows/einsammeln		
lrwxrwxrwx 1 remote	users 32	Jan 29 17:41 public_html -> /home/rem
ote/windows/public_html		
lrwxrwxrwx 1 remote	users 21	Jan 29 17:41 tausch_schueler -> /home
/tausch/schueler		
drwxr-xr-x 5 remote	users 4096	Jan 29 17:41 windows
albert:/home/remote # rm ml tausch_schueler	-rf .bash_history	austeilen cdrom einsammeln public_ht

000		haega	ar@sven: /home/haegar	Θ
albert:/home albert:/home albert:/home total 28 drwxr-xr-x drwxr-xr-x drwxr-xr-x drwxr-xr-x drwxr-xr-x drwxr-xr-x drwxr-xr-x	<pre>/remote # ls //remote # cp //remote # ls 7 remote 11 root 2 root 2 root 2 root 4 root 5 remote</pre>	-ar /home -la root root root root root users	e/scponly/* . 4096 Jan 30 16:33 . 4096 Jan 30 15:50 4096 Mar 15 2005 bin 4096 Mar 15 2005 etc 4096 Mar 15 2005 usr 4096 Jan 29 17:41 windows	

Unterverzeichnisse mit Ausnhame von windows root gehören, wenn nicht muss das mittels chmod angepasst werden.

3. Die zum Benutzer gehörige Zeile aus der Datei /etc/passwd muss in die Datei /home/<benutzer>/etc/passwd kopiert werden, sonst darf die Passwortdatei in

der Changeroot Umgebung leer sein. Außerdem muss als Shell jetzt in beiden Passwort Dateien /usr/local/sbin/scponlyc stehen, das "c" steht für die Changeroot Version.

Jetzt nochmals mit

/etc/init.d/nscd restart

die Änderungen wirksam werden lassen. Das wars, nun kann man dass funktionieren testen, indem man sich mit WinSCP am Server anmeldet, man sollte nicht mehr aus seinem Homeverzeichnis herauswechseln können. Man sieht auch am Bildschirmfoto, dass der Benutzer in seinem Heimatverzeichnis ist, dort die Dateien der Changeroot Umgebung und sein Windows Homeverzeichnis sieht, WinSCP aber als aktuelles Verzeichnis /<root> anzeigt. Man kann im Verzeichnisbaum nicht mehr nach oben wechseln.



### Automatik

Das mitgelieferte Shellskript /usr/local/sbin/addscpacces.sh erledigt die Schritte oben automatisch für den Benutzer der als Argument übergeben wird:

addscpaccess.sh hallo

richtet einen Changeroot- SCP-Zugang für den Benutzer *hallo* ein. Außerdem kopiert das Skript die Dateien der Changeroot Umgebung nicht sondern legt harte Links an, was den Platzbedarf reduziert, da die Dateien so nur einmal vorgehalten werden müssen.

Bemerkung zum Skript: Ich habe mich um Sorgfalt bemüht, die passwd- Datei wird auch gesichert, aber Garantien für das Skript gebe ich keine.