# madapez

IT, Linux, Web und Kreatives aus der Sicht eines verrückten Affen

## Howto: Chroot SFTP Zugang mit openssh ohne shell (ssh) Zugang

Posted by Daniel on 12. April 2011 — Go to comments — Leave a comment (6)

Hallo Besucher, schön dass du hier hergefunden hast. Ich hoffe dir gefällt was du hier liest und schaust ab sofort öfter vorbei. Viel Spass! Daniel
Manchmal kann es sinnvoll sein Prozesse via SFTP zu automatisieren oder man möchte anderen Usern die Möglichkeit geben Dateien abzulegen. Um zu verhindern, dass sie das ganze Dateisystem durchbrowsen können müssen wir eine **Chroot**-Umgebung für diese Benutzer etablieren. Ich zeige Dir wie.

Benötigt wird hierzu ein Ubuntu oder Debian System (bei anderen Distributionen mag der Lösungsweg identisch sein) und openssh ab Version *4.9p1*. Ab dieser Version hat **openssh** bordeigene Mittel um die **Chroot**-Umgebung umzusetzen.

### openssh konfigurieren

Zu allererst müssen wir **openssh** mitteilen, dass es den **SFTP Zugang** für Benutzer der Gruppe "**sftp**" anders behandeln soll, als den Zugang anderer User. Hierzu nehmen wir in der Datei */etc/ssh/sshd_config* 2 Einstellungen vor:

```
#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp

Match Group sftp
        ChrootDirectory %h
        ForceCommand internal-sftp
        AllowTcpForwarding no
```

Die erste Konfigurationsanweisung ändert das **SFTP**-Subsystem auf den internen **SFTP**-Server der für das **Chroot**ing besser funktioniert. Hierbei entfällt auch das Installieren bestimmter Bibliotheken im **Chroot**-Verzeichnis.

Die zweite Anweisung greift jedes mal wenn sich ein Benutzer der Gruppe **sftp** authentifiziert. Er wird in sein Home-Directory (%h) eingesperrt und es wird nochmal explizit der internal-sftp geforced. TCP-Forwarding wollen wir auch deaktiviert wissen.

### Usereinstellungen für den Chroot-SFTP-Zugang

Um das ganze nun zu testen legen wir den User "sftptest" an. Es soll sein Home-Dir automatisch angelegt werden (-m), er soll keinen Shell-Zugang bekommen (-s /bin/false) und er soll der Gruppe sftp angehören (-G sftp):

```
addgroup sftp
useradd -m -s /bin/false -G sftp sftptest
```

Ein Passwort sollte der User sftptest auch bekommen:

```
passwd sftptest
```

Es folgt ein Prompt bei dem ein Passwort angegeben werden muss. Anschließend muss das Passwort nochmal bestätigt werden.

Hast Du bereits einen User angelegt und möchtest diesem sftp-Zugang gewähren führst Du folgendes aus:

```
usermod -G sftp sftptest
usermod -s /bin/false sftptest
```

### Das Home-Dir

Hier müssen wir noch eine Änderung durchführen, die untypisch für das Home-Dir ist. Wir müssen dem root-User den Besitz über das Home-Dir übertragen, andernfalls wird ein Login nicht möglich sein:

```
chown root:root /home/sftptest/
chmod 0755 /home/sftptest/
```

RSS Feed

### Recent Posts

- Howto: MySQL 5.1 auf Debian lenny installieren
- Howto: Chroot SFTP Zugang mit openssh ohne shell (ssh) Zugang
- Howto: Domain-Usern Zugriff auf Internetseiten sperren
- Howto: Automatische Konfiguration des Cisco IP Communicator in einer Windows-Domäne
- long time no see

### Search by Tags!

blackberry chroot cisco darmstadt debian domÃ¤ne drupal e-mail ffmpeg hessen hosting howto indoorspielplatz Kurzgeschichte lame Linux Linux Befehl der Woche mail mplayer mysql schlaflos seo sftp ssh test virtualbox vm web windows

### Archives

- April 2011
- Juli 2010
- April 2010
- Januar 2010
- Dezember 2009
- November 2009
- Oktober 2009
- September 2009

### Links

- Lapinot
- Beetlebum
- Hosting

### Meta

- Registrieren
- Anmelden

Damit der User Dateien samt Ordnern hochladen kann, müssen wir ihm noch ein Verzeichnis anlegen das ihm gehört.

```
mkdir /home/sftptest/upload
chown sftptest:sftptest /home/sftptest/upload
```

Das wars. Nun kannst Du die Logindaten ohne Probleme weitergeben.

Viel Spass beim konfigurieren!

Fragen, Kritik oder Anregungen bitte in die Kommentare!

**Beiträge die für dich ebenfalls interessant sein können:**

- Howto: ssh ohne Passwort
- Howto Virtualbox: Virtuelle Maschine ohne GUI (Shell) erstellen
- Howto: Linux Mint 7 in einer Windows Domäne
- Howto: Automatische Konfiguration des Cisco IP Communicator in einer Windows-Domäne
- Howto: Abaqus 6.9.1 auf Linux Mint 7 installieren

Linux chroot, howto, sftp, ssh

← Howto: Domain-Usern Zugriff auf Internetseiten sperren

Howto: MySQL 5.1 auf Debian lenny installieren →

Leave a comment ? 6 Comments.

**Karl** 11. Juli 2012 um 16:13

Hey,

danke für das Howto!
Es hat mir sehr geholfen.

Weiter so & Gruß
Karl

**Ben** 10. August 2012 um 16:24

Hi,

super Artikel! Hat genauso funktioniert. Allerdings habe ich Probleme beim Hinzufügen eines zweiten Benutzers bei SFTP. Ich arbeite in der sshd_config mit Match User und wenn ich darunter ein zweites Match User hinzufüge, funktioniert das nicht. Ich verstehe nicht warum?! Braucht man einen Closing-Tag bei Match oder geht nur jeweils ein Match User? Also Einloggen funktioniert zwar mit dem neuen Benutzer, aber keine der Einstellungen bei Match User greift: Ich kann alles im System durchklicken und das Homeverzeichnis wird auch falsch gesetzt. Hast du eine Idee? Danke und LG.

**Ben** 10. August 2012 um 16:26

P.S.: Ich glaube bei
mkdir /home/sftptest/upload
chown sftptest:sftptest /home/sftptest/upload
müsste es doch chown sftptest:sftp /… heißen oder?

**Falk** 20. August 2012 um 18:58

Hallo,

die Anleitung finde ich sehr gut. Vielleicht solltest du noch erwähnen, dass alles ab der Zeile Match Group… am Ende der sshd_config stehen muss.

Grüße,
Falk

**Chris** 20. Oktober 2012 um 11:29

gibt es eigentlich auch eine Möglichkeit zusätzlich zum SFTP-Force bei Login ein gesondertes Script im Hintergrund zu starten?

Ziel ist es in meinem Fall, ein Whitelisting auf iptables-basis anzustoßen, welches dazu sorgt, dass der User nicht nach einer gewissen Anzahl von Logins gebannt wird (SFTP baut ja an mancher Stelle parallel mehrere Verbindungen auf, was dann zum sofortigen Ban führen kann).

Daher muss ich bei der erfolgreichen Anmeldung ein Script starten, welches dann IP ausliest und temporär im IP-Filter als whitelisting vermerkt und somit keine Probleme entstehen können.

Grüße Chris

## Leave a Comment

NAME

EMAIL

Website URL

NOTE - You can use these HTML tags and attributes:

```
<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote
cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike>
<strong> <pre lang="" line="" escaped="">
```

SUBMIT

## Trackbacks and Pingbacks:

- Chrooted SFTP Without Shell Access | Black-Pixel - Pingback on 2012/05/21/ 16:06