SFTP Server mit Chroot und Usermapping (www-data)

Diese Anleitung wurde zuletzt mit Debian Stretch getestet. Der standard openssh-Dämon kann SFTP zwar schon länger. Chroot ist dabei ein ziemlich nervig einzurichten. Ein Mapping auf einen anderen Benutzer ist damit auch nicht möglich (das ist vor allem beim Zugriff auf /var/www nützlich, wo z.B. der SFTP-Benutzer ein anderer ist, als der mit dem der Webserver läuft).

Mit MySecureShell läßt sich das aber alles sehr bequem erledigen. Die Installation erfolgt einfach über: `apt-get install mysecureshell`

Danach wird die Konfigurationsdatei angepasst:

/etc/ssh/sftp_config

```
## MySecureShell Configuration File ##
# To get more informations on all possible options, please look at the doc:
# http://mysecureshell.readthedocs.org

#Default rules for everybody
<Default>
 GlobalDownload  0 #total speed download for all clients
     # o -> bytes   k -> kilo bytes   m -> mega bytes
 GlobalUpload  0 #total speed download for all clients (0 for unlimited)
 Download   0 #limit speed download for each connection
 Upload    0 #unlimit speed upload for each connection
 StayAtHome  true #limit client to his home
 VirtualChroot  true #fake a chroot to the home account
 LimitConnection  10 #max connection for the server sftp
 LimitConnectionByUser 5 #max connection for the account
 LimitConnectionByIP 5 #max connection by ip for the account
 Home   /home/$USER #overrite home of the user but if you want you can use
      # environment variable (ie: Home /home/$USER)
 IdleTimeOut  5m #(in second) deconnect client is idle too long time
 ResolveIP  true #resolve ip to dns
 IgnoreHidden  false #treat all hidden files as if they don't exist
 DirFakeUser  false #Hide real file/directory owner (just change displayed permissions)
 DirFakeGroup  false #Hide real file/directory group (just change displayed permissions)
 HideNoAccess  false #Hide file/directory which user has no access
 DefaultRights  0640 0750 #Set default rights for new file and new directory
 MinimumRights  0400 0700 #Set minimum rights for files and dirs
 ShowLinksAsLinks false #show links as their destinations
</Default>

<User sftp-www1>
 Home   /var/www
 ForceUser  www-data
 ForceGroup  www-data
</User>
```

Das mysecureshell Binary braucht noch das suid-Bit, um das Usermapping verwenden zu können: `chmod 4755 /usr/bin/mysecureshell`

Der User sftp-www1 wird dann wie folgt angelegt: `useradd -G www-data -s /usr/bin/mysecureshell sftp-www1`

Der User bekommt nun entweder einen SSH-Key in sein Home gelegt (/home/sftp-www, nicht /var/www) oder ein Passwort gesetzt und ist nach dem Einloggen in /var/www gebunden. Dateien, die der Benutzer hochlädt, werden

dem Benutzer www-data zugeordnet.

Revision #1
Created 2021-05-31 12:26:34 UTC by magenbrot
Updated 2021-05-31 12:26:51 UTC by magenbrot