

Installation

```
sudo apt-get install vsftpd openssl
```

SSL-Schlüssel erstellen

```
sudo openssl req -x509 -nodes -days 730 -newkey rsa:1024 -keyout  
/etc/vsftpd.pem -out /etc/vsftpd.pem  
chmod 600 /etc/vsftpd.pem
```

Bei der Zertifikatserstellung werden folgende Fragen gestellt. Zur Identifikation ist es nötig, die richtigen Dinge einzutragen

```
Country Name (2 letter code) [GB]: Land (z.B. DE)  
State or Province Name (full name) [Berkshire]: Bundesland (z.B. Bayern)  
Locality Name (eg, city) [Newbury]: Stadt (z.B. München)  
Organization Name (eg, company) [My Company Ltd]: eigener Name  
Organizational Unit Name (eg, section) []: Bezeichnung des Dienstes (z.B.  
FTP-Server)  
Common Name (eg, your name or your server's hostname) []: Name, unter dem  
der Rechner zu erreichen ist (z.B. www.microsoft.de)  
Email Address []: eMail-Adresse
```

Datei mit Accounts erstellen, die sich nicht am FTP anmelden können

```
sudo -s  
cat /etc/passwd | cut -d":" -f1 > /etc/vsftpd.user_deny
```

Aus der entstandenen Liste (es sind alle Benutzer enthalten) müssen die alle FTP-Nutzer herausgelöscht werden

Logfile für alle lesend setzen

```
sudo chmod go+r /var/log/vsftpd.log
```

Konfigurationsdateien

/etc/vsftpd.conf

```
<filebash vsftpd.conf> # daemon started from an initscript. listen=YES # Allow anonymous FTP?  
(Beware - allowed by default if you comment this out). anonymous_enable=NO # Schalter, um  
Account aus einer Liste zugriff zu verbieten userlist_enable=YES # Liste mit zugriffsberechtigten usern  
userlist_file=/etc/vsftpd.user_deny # Uncomment this to allow local users to log in. local_enable=YES  
# Uncomment this to enable any form of FTP write command. write_enable=YES # Default umask for  
local users is 077. You may wish to change this to 022, # if your users expect that (022 is used by  
most other ftpd's) local_umask=022 # Uncomment this to allow the anonymous FTP user to upload
```

files. This only # has an effect if the above global write enable is activated. Also, you will # obviously need to create a directory writable by the FTP user. anon_upload_enable=NO # Uncomment this if you want the anonymous FTP user to be able to create # new directories.

anon_mkdir_write_enable=NO # Activate directory messages - messages given to remote users when they # go into a certain directory. dirmessage_enable=YES # Activate logging of uploads/downloads. xferlog_enable=YES # Make sure PORT transfer connections originate from port 20 (ftp-data). connect_from_port_20=YES # You may override where the log file goes if you like. The default is shown # below. xferlog_file=/var/log/vsftpd.log # If you want, you can have your log file in standard ftpd xferlog format xferlog_std_format=YES # You may change the default value for timing out an idle session. idle_session_timeout=600 # You may change the default value for timing out a data connection. data_connection_timeout=120 # You may fully customise the login banner string: ftpd_banner=Welcome to da-checka's FTP. chroot_local_user=YES # This option should be the name of a directory which is empty. Also, the # directory should not be writable by the ftp user. This directory is used # as a secure chroot() jail at times vsftpd does not require filesystem # access. secure_chroot_dir=/var/run/vsftpd # This string is the name of the PAM service vsftpd will use. pam_service_name=vsftpd # Einstellungen fuer ssl-verschluesselung ssl_enable=YES allow_anon_ssl=NO force_local_data_ssl=NO force_local_logins_ssl=NO

ssl_tlsv1=YES ssl_sslv2=NO ssl_sslv3=NO

This option specifies the location of the RSA certificate to use for SSL # encrypted connections. rsa_cert_file=/etc/vsftpd.pem

Diese Option gibt an, dass die Lokale Systemzeit und nicht GMT genutzt wird use_localtime=YES

Einstellungen fuer den SSL-verschluesselten Datenverkehr von aussen # Die angegebenen Ports muessen in der FritzBox weitergeleitet werden #pasv_addr_resolve=yes #pasv_address=da-checka.ath.cx pasv_min_port=22000 pasv_max_port=22015 pasv_promiscuous=YES setproctitle_enable=YES session_support=YES </file>

Skript zur erstellung eines FTP-Benutzers

In /usr/local/bin ein Skript mit folgendem Inhalt erstellen

[ftpuser_create](#)

```
# Kleines Programm zum erstellen eines ftp-Nutzers mit mount des
Verzeichnisses fuer alle

# Prüfen, ob das Script als root aufgerufen wurde
if [ `id -u` -ne "0" ]
then
    echo "You must be root"
    exit 1
fi

if [ $# = "1" ]
then
    user=$1
    # Prüft, ob der eingegeben User schon existiert
```

```

if ! id $user>/dev/null 2>&1
then
    #User wird angelegt
    if sudo useradd -d /home/$user -m -s /bin/false $user
    then
        echo "Nutzer $user angelegt"
        # Passwort generieren
        password=`cat /dev/urandom | tr -cd 'a-z0-9' |
head -c8`
        # Abfrage, ob generiertes Passwort verwendet
        werden soll
        echo -e "Wollen Sie das Passwort $password
verwende? [J] \c"
        read fragepasswd
        case $fragepasswd in
            j|J|"")
                printf "%s\n%s" $password $password >
$passwordfile
                sudo passwd $user < $passwordfile >
                sudo rm $passwordfile
                ;;
            *)
                sudo passwd $user
        esac
        # Abfrage, ob Passwort gespeichert werden soll
        echo -e "Wollen Sie das Passwort speichern? [J]
\c"
        read fragespeicher
        case $fragespeicher in
            j|J|"")
                printf "%s\t%s\n" $user $password >>
$speicherpfad
                ;;
            *)
        esac
        # Verzeichnis wird für den Mountpoint angelegt
        sudo mkdir /home/$user/fuer_alle
        # Anlegen des oeffentl. Verzeichnisses fuer
        Apache
        sudo mkdir /home/$user/public_html
        sudo chown $user.$user /home/$user/public_html
        # Eintrag in die fstab wird geschrieben,
        # damit automatisch gemountet wird
        echo -e
"/home/fuer_alle\t/home/$user/fuer_alle\ttext3\tbind\t0\t0" >>
/etc/fstab
        # Mountpoint einhängen
        /bin/mount -a

```

```
        fi
    else
        echo -e "Nutzer gibt es schon"
    fi
else
    echo -e "Falsche Parameter"
fi
```

Script zum löschen eines FTP-Benutzers

in /usr/local/bin ein Skript mit folgendem Inhalt erstellen

`ftpuser_del`

```
#!/bin/bash

user=$1

#Pruefen, ob das Programm als root gestartet wurde
if [ ! `id -u` = "0" ]
then
    echo "You must be root"
    exit 1
fi

#Pruefen, ob Benutzer existiert
if ! id -u $user>/dev/null 2>&1
then
    echo -e "$user existiert nicht\nProgramm beendet"
    exit 1
fi

#Mountpunkt umounten, damit beim loeschen nicht fuer_alle geloescht
wird
if ! umount /home/$user/fuer_alle>/dev/null 2>&1
then
    echo -e "umount nicht erfolgreich\nProgramm beendet"
    exit 1
fi

#Nutzer wird mit home-Verzeichnis geloescht
if ! userdel -r $user
then
    echo -e "userdel nicht erfolgreich\nProgramm beendet"
    exit 1
fi

#Eintrag fuer den Nutzer aus der fstab loeschen
```

```

cp /etc/fstab /etc/fstab.orig
if ! grep -v "/home/$user/fuer_alle" /etc/fstab > /etc/fstab.neu
then
    echo -e "schreiben der fstab.neu fehlgeschlagen\nProgramm
beendet"
    exit 1
fi

mv /etc/fstab.neu /etc/fstab

```

ftptwho für vsftpd

ftptwho-Skript nach /usr/local/bin schreiben

ftptwho

```

#!/bin/bash

#Funktion, um eine Linie zu zeichnen
function linie(){
echo "-----"
}

#setzen des Separators, damit das Array befüllt werden kann
IFS=$'\n'

#Einlesen der Daten in ein Array "Daten"
Daten=( `ps -C vsftpd -o user,pid,stime,cmd | grep "vsftpd:" | egrep -v
'root|nobody' | tr -s ' ' ' '` )

# Zeichnen der ersten Tabellenspalte
echo -e "\nftptwho for vsftpd\n"
linie
printf "| %-15s| %-5s | %-17s| %-10s| %-60s|\n" User Start IP Up/Down
File
linie
#echo "Ausgabe des Arrays"
for (( i=0 ; $i<${#Daten[*]} ; i=i+1 ))
do

    IFS=$' '
    #Befüllen des Zweiten Arrays, das für jede Zeile zuständig ist
    Zeile=( ${Daten[$i]} )

    #      Testschleife, um das Array Zeile[] auszugeben
    #      for (( zaehler=0 ; $zaehler<${#Zeile[*]} ; zaehler=zaehler+1 ))

```

```

#      do
#          echo Zeile $zaehler: ${Zeile[$zaehler]}
#      done

#Wenn nicht der Username sondern die UID ausgegeben wird, wird
dies behoben
    case ${Zeile[0]:0:1} in
        0|1|2|3|4|5|6|7|8|9)
            user=`grep :${Zeile[0]}: /etc/passwd | cut -
d":" -f1`
            ;;
        *)
            user=${Zeile[0]}
    esac

    #Zeit und IP aus dem Array in Variablen schreiben
    zeit=${Zeile[2]}
    ip=${Zeile[4]%%/*:}
    # Umwandeln der Worte STOR in "Upload", RETR in "Download" und
IDLE in "-"
    case ${Zeile[5]} in
        STOR)
            updown="Upload"
            ;;
        RETR)
            updown="Download"
            ;;
        IDLE)
            updown="-"
            ;;
        *)
    esac

    what=''
    for (( z=6 ; $z<${#Zeile[*]} ; z=z+1))
    do
#          echo $z
#          what=$what\ ${Zeile[$z]}
#      echo $what
    done
    # Setzen des Seperierungszeichens, damit die Ausgabe richtig
formatiert wird
    IFS=$' '
    # Ausgabe der jeweiligen ArrayZeile
    printf "| %-15s| %-5s | %-17s| %-10s| %-60s|\n" $user $zeit $ip
$updown $what;

done

if [ ! $i = "0" ]

```

```
then  
    linie  
fi  
echo
```

From:

<https://wiki.da-checka.de/> - PSwiki

Permanent link:

<https://wiki.da-checka.de/doku.php/wiki/dienste/vsftpd?rev=1298463911>

Last update: **2011/02/23 13:25**

