FTP-Server

Details zum Server

IP-Adresse: 188.166.161.116

FQDN: ftp.go-solution.cloud

Servername: VSFTPD-01

Neuer Benutzer erstellen

Um einen neuen Benutzer auf dem FTP-Server zu erstellen, müssen folgende Befehle ausgeführt werden:

```
#create user and enble ftp access
sudo useradd -s /bin/bash -m -p $(perl -e 'print crypt("Mu$TrFTPuSr", "password")' "Mu$TrFTPuSr") muster
echo 'muster:Mu$TrFTPuSr' | chpasswd
sudo mkdir /home/muster/ftp
sudo chown nobody:nogroup /home/muster/ftp
sudo chmod a-w /home/muster/ftp

#create directory for new files (folder for new files)
sudo mkdir /home/muster/ftp/files
sudo chown muster:muster /home/muster/ftp/files

#create directory for processed files (folder for pcrocessed files)
sudo mkdir /home/muster/ftp/files_processed
sudo chown muster:muster /home/muster/ftp/files_processed
```

Der folgende Befehl löscht den Benutzer wieder

```
deluser --remove-home muster
```

Installationsanleitung

Installation mit folgenden Befehlen:

```
#update package list
sudo apt update

#install vsftpd daemon & service
sudo apt install vsftpd

#copy original configuration file
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

#configure firewall
sudo ufw allow 20,21,22,990/tcp
sudo ufw allow 40000:50000/tcp
sudo ufw enable
```

Konfigurationsdateien

Die Konfigurationsdatei ist unter dem Pfad "/etc/vsftpd.conf" verfügbar.

Um die Datei zu bearbeiten kann folgender Befehl genutzt werden:

```
nano /etc/vsftpd.conf
```

Nach einer Anpassung der Konfiguration muss der Service neu gestartet werden. Der folgende Befehl startet den Service neu:

```
sudo systemctl restart vsftpd
```

Das Konfigurationsfile für unseren Server ist:

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
```

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# 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=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=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
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
```

```
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# 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.
# Note that the default log file location is /var/log/xferlog in this case.
#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
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
```

```
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# 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/empty
#
```

```
# This string is the name of the PAM service vsftpd will use.
pam_service_name=fm-gateway-sync-center
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#ssl_enable=NO

# Paths to your letsencrypt files
rsa_cert_file=/etc/letsencrypt/live/ftp.go-solution.cloud/fullchain.pem
rsa_private_key_file=/etc/letsencrypt/live/ftp.go-solution.cloud/privkey.pem
ssl_enable=YES
allow_anon_ssl=NO

# Options to force all communications over SSL - why would you want to
# allow clear these days? Comment them out if you don't want to force
# SSL though
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

require_ssl_reuse=NO
ssl_ciphers=HIGH

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

# custom
user_sub_token=$USER
local_root=/home/$USER/ftp

pasv_min_port=40000
pasv_max_port=50000
```

SSL-Zertifikat

Für das SSL-Zertifikat wird Certbot im Zusammenhang mit Apache genutz.

Installation:

```
sudo apt-get update

sudo apt-get install apache2

sudo snap install --classic certbot

sudo ln -s /snap/bin/certbot /usr/bin/certbot

sudo certbot certonly --apache
```

In der Crontabelle ist eine monatliche Erneuerung des Zertifikats hinterlegt

```
0 0 1 * * sudo certbot renew --dry-run
```