FTP Server installieren für Paperless

Kann aber auch für andere Sachen verwendet werden

```
#### Paperless NGX - Nextcloud - Scanner Workflow ####

## FTP-Server installieren ##
apt-get install proftpd

## config bearbeitren ##
mv /etc/proftpd/proftpd.conf /etc/proftpd/proftpd.conf.old

nano /etc/proftpd/proftpd.conf


########################################## paste
######################################

# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
#UseIPv6                on
# If set on you can experience a longer connection delay in many cases.
#IdentLookups           off

ServerName              "myserver.com"
# Set to inetd only if you would run proftpd by inetd/xinetd.
# Read README.Debian for more information on proper configuration.
```

```
ServerType                    standalone
DeferWelcome              off
MultilineRFC2228          on
DefaultServer            on
ShowSymlinks             on
TimeoutNoTransfer         600
TimeoutStalled           600
TimeoutIdle             1200
DisplayLogin             welcome.msg
DisplayChdir             .message true
ListOptions           "-l"


DenyFilter            \*.*/


# Use this to jail all users in their homes
 DefaultRoot              ~


# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell        off


# Port 21 is the standard FTP port.
Port                    21


# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
# PassivePorts          49152 65534


# If your host was NATted, this option is useful in order to
# allow passive tranfers to work. You have to use your public
# address and opening the passive ports used on your firewall as well.
# MasqueradeAddress          1.2.3.4


# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours


# DynMasqRefresh 28800


# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
```

at once, simply increase this value. Note that this ONLY works

in standalone mode, in inetd mode you should use an inetd server

that allows you to limit maximum number of processes per service

(such as xinetd)

MaxInstances   30

Set the user and group that the server normally runs at.

User   proftpd

Group   nogroup

Umask 022 is a good standard umask to prevent new files and dirs

(second parm) from being group and world writable.

Umask   022 022

Normally, we want files to be overwriteable.

AllowOverwrite   on

Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:

PersistentPasswd   off

This is required to use both PAM-based authentication and local passwords

AuthOrder   mod_auth_pam.c* mod_auth_unix.c

Be warned: use of this directive impacts CPU average load!

Uncomment this if you like to see progress and transfer rate with ftpwho

in downloads. That is not needed for uploads rates.

#

UseSendFile   off

TransferLog /var/log/proftpd/xferlog

SystemLog   /var/log/proftpd/proftpd.log

Logging onto /var/log/lastlog is enabled but set to off by default

#UseLastlog on

In order to keep log file dates consistent after chroot, use timezone info

from /etc/localtime. If this is not set, and proftpd is configured to

chroot (e.g. DefaultRoot or), it will use the non-daylight

savings timezone regardless of whether DST is in effect.

#SetEnv TZ :/etc/localtime

QuotaEngine off

Ratios off

```
# Delay engine reduces impact of the so-called Timing Attack described in
# http://www.securityfocus.com/bid/11430/discuss
# It is on by default.

DelayEngine on

ControlsEngine        off
ControlsMaxClients    2
ControlsLog           /var/log/proftpd/controls.log
ControlsInterval      5
ControlsSocket        /var/run/proftpd/proftpd.sock

AdminControlsEngine off

#
# Alternative authentication frameworks
#
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf

#
# This is used for FTPS connections
#
#Include /etc/proftpd/tls.conf

#
# Useful to keep VirtualHost/VirtualRoot directives separated
#
#Include /etc/proftpd/virtuals.conf

# A basic anonymous configuration, no upload directories.

#
#   User                      ftp
#   Group                     nogroup
#   # We want clients to be able to login with "anonymous" as well as "ftp"
#   UserAlias                 anonymous ftp
#   # Cosmetic changes, all files belongs to ftp user
#   DirFakeUser on ftp
#   DirFakeGroup on ftp
```

```
#
#   RequireValidShell            off
#
#   # Limit the maximum number of anonymous logins
#   MaxClients                   10
#
#   # We want 'welcome.msg' displayed at login, and '.message' displayed
#   # in each newly chdired directory.
#   DisplayLogin                 welcome.msg
#   DisplayChdir                 .message
#
#   # Limit WRITE everywhere in the anonymous chroot
#
#
#       DenyAll
#
#
#
#   # Uncomment this if you're brave.
#   #
#   #   # Umask 022 is a good standard umask to prevent new files and dirs
#   #   # (second parm) from being group and world writable.
#   #   Umask                    022  022
#   #
#   #           DenyAll
#   #
#   #
#   #           AllowAll
#   #
#   #
#
#
```

Include other custom configuration files
Include /etc/proftpd/conf.d/

FTP-Server neu starten
systemctl restart proftpd

Verzeichnisse

PDF-Input - /consume

PDF-Output - /media/documents/archive

Revision #1
Created 21 March 2023 08:03:21 by Hermann
Updated 21 March 2023 08:03:39 by Hermann