VSFTPD (File Transfer Protocol)

- Kurzakte –

Server:

Installation	
• Paket vsftpd in der Selektion Netzwerk/Server	
Konfiguration Normalzugang	
/etc/services	• Kommentarzeichen entfernen vor Zeilen: ▪ ftp 20/tcp # (Datenkanal) ▪ ftp 21/tcp # (Kommandokanal)
/etc/xinetd.d/vsftpd	• Freischalten von FTP in der Konfig-Datei des xinetd-Daemons: • Entfernen der Zeile disable = yes • oder Aktivieren im YaST-Kontrollzentrum unter *Netzwerkdienste* → *Netzwerkdienste (inetd)* mit *Status wechseln*
/etc/passwd /etc/shadow	• für nicht anonym zugreifende Benutzer einen Account einrichten: *useradd –s /bin/false username* und *passwd username*
/etc/vsftpd.conf	• Haupt-Konfigurationsdatei *local_enable=YES* gestattet FTP-Zugriff von Linuxbenutzern auf das gesamte Dateisystem *write_enable=YES* gestattet schreibenden Zugriff
/etc/ftpusers	• Eintrag aller User mit ftp-Verbot (root, news usw.)
/etc/ftpgroups	• analog ftpusers, wenn von PAM unterstützt
/etc/hosts	• Zuordnung von Hostnamen zur IP-Adresse • ermöglicht Aufruf *ftp <Hostname>*
Konfiguration Zugang Anonymus	
/etc/pam.d/vsftp	• Kommentarzeichen entfernen vor: auth sufficient ...
Start durch xinetd	
/usr/sbin/vsftpd	• Vsftpd ist nicht für den Stand-Alone-Betrieb vorgesehen 500 OOPS: vsftpd: does not run standalone, must be started from inetd
/etc/init.d/xinetd rcxinetd (S.u.S.E.)	• *start* | *stop* | *restart* | *reload* | *status* - Skript startet/stoppt xinetd manuell (dieser startet bei Bedarf /usr/sbin/vsftpd) • auch mit *kill –HUP `cat /var/run/xinetd.pid`* • Kontrolle mit *ps ax | grep xinetd*
/etc/init.d/rc5.d insserv xinetd	• automatischer Start von xinetd durch Anlegen von Symlinks als Start- und Stopp-Skript in die entsprechenden Runlevel-Verzeichnisse • alternativ im YaST-Kontrollzentrum mit Runlevel-Editor
Logdateien	
/var/log/vsftpd.log	• Logdatei für Serverzugriffe und übertragene Daten • mit *log_ftp_protocol=YES* werden auch alle Kommandos protokolliert • Auswertung mit webalizer erfordert *xferlog_std_format=YES*
Dokumentation	
man: vsftpd (8), vsftpd.conf(5), ftpusers (5), ftp (1)	

Clients:

- Problem: das Passwort sowie alle Daten werden unverschlüsselt übertragen! (Sniffer!)

Linux
• für Linux-Stationen Installation der Client-Programme ftp und/oder xftp, auch Webbrowser • Sicherheitsrisiko durch Nutzung der Datei ~/.netrc (Server, User, Passw.)
Windows
• ftp (auf Konsole),CuteFTP, WS FTP PRO, SmartFTP, FTP Voyager • Internet-Explorer: Eingabe in Adresszeile ftp://username@FTP-Server

Erstellt von Dr. Jörg Meese

wichtige FTP-Befehle des Clients (Aufruf auf der Konsole mit "ftp")

Befehl	Erläuterung
ls, dir	Anzeige des Inhaltsverzeichnisses auf dem FTP-Server
!ls	Programm ls auf der lokalen Maschine ausführen
cd <Zielverzeichnis>	Verzeichniswechsel auf dem Server
lcd <Zielverzeichnis>	Verzeichniswechsel auf dem Client
ascii, asc	ASCII-Übertragungsmodus einschalten, wichtig für die Lesbarkeit von Textdateien über die Betriebssystemgrenzen hinweg
binary	Binären Übertragungsmodus einschalten
get <Datei>	Angegebene Datei vom Server laden.
mget <Datei(en)>	Mehrere Dateien vom Server holen, Wildcards * und ? erlaubt.
put <Datei>	Datei zum Server übertragen.
put <Datei(en)>	Mehrere Dateien zum Server übertragen, Wildcards * und ? erlaubt.
quit	Programm beenden.

Beispielhafte Konfigurationsdatei

```
notebook:~> cat /etc/vsftpd.conf
```

```
# Beispielkonfiguration /etc/vsftpd.conf
#
# Anonymes FTP gestatten, das Datenverzeichnis liegt unter /srv/ftp (SUSE)
anonymous_enable=YES
#
# Lokale Anmeldung gestatten
local_enable=YES
#
# lokale Benutzer dürfen ihr Heimatverzeichnis nicht verlassen
chroot_local_user=YES
#
# Veränderungen am Dateisystem prinzipiell zulassen
write_enable=YES
#
# Maske für Rechte auf hoch geladene Dateien und neu angelegte Verzeichnisse setzen
local_umask=022
#
# Anonyme Benutzer dürfen nichts am Dateisystem ädern
anon_upload_enable=NO
anon_mkdir_write_enable=NO
#
# Verstecken der Identitäten der Dateibesitzer
hide_ids=YES
#
# Verzeichnis-Nachrichten aktivieren
dirmessage_enable=YES
#
# Den Datentransfer protokollieren
xferlog_enable=YES
#
# Zur Datenübertragung muss der Port 20 frei geschaltet werden
connect_from_port_20=YES
#
# Die Begrüßungstext
ftpd_banner=Willkommen auf unserem FTP-Server
#
# Als PAM-Dienst verwenden wir nicht die Standard-FTP-Konfiguration
pam_service_name=vsftpd
```

Konfiguration des Authentifizierungsprozesses

notebook:~> `cat /etc/pam.d/vsftpd`

```
#%PAM-1.0

#
# Die Anmeldung bedarf der Existenz des PAM-Moduls »pam_listfile.so«
# Die weiteren Einträge auf der Zeile steuern das Vorgehen des Moduls:
#   Ist der anmeldende Benutzer (item=user)
#   nicht (sense=deny)
#   in der angegebenen Datei (file=/etc/ftpusers)
#   fahre dennoch mit der Authentifizierung fort (onerr=succeed)
auth       required     pam_listfile.so item=user sense=deny
file=/etc/ftpusers onerr=succeed
#   Anonymous ftp wird zugelassen
#   Ist die folgende Authentifizierung erfolgreich, werden nachfolgende Regeln nicht mehr beachtet (sufficient)
auth       sufficient   pam_ftp.so
# Für lokales Login werden die weiteren Regeln befolgt
auth       required     pam_unix.so
auth       required     pam_shells.so
account    required     pam_unix.so
password   required     pam_unix.so
session    required     pam_unix.so
```