# Step by Step
## vsftpd unter SuSe Linux

**von Christian Bartl**

# vsftpd unter SuSe Linux

## Installation

1. Als erstes sollte (für Server die im Produktiveinsatz sind und immer erreichbar sein sollen zwingend erforderlich) die Netzwerkkarte mit einer fixen IP-Adresse konfiguriert werden. Dies erledigen Sie unter SuSe am komfortabelsten mit Hilfe von Yast. Gehen Sie dazu unter Yast auf netzwerkgeräte und dort auf Netzwerkkarte. Klicken Sie hier entweder im bereich bereits konfigurierte Netzwerkkarten oder im Bereich zu konfigurierende Netzwerkkarten (je nachdem wo die von ihnen gewünschte Karte aufscheint) auf ändern. Wählen Sie im nächsten Dialog die Netzwerkkarte aus der Sie die Adresse zuweisen wollen. Klicken Sie auf Bearbeiten. Nun stellen Sie hier die Konfiguration auf statische Adresse um, geben Sie die IP-Adresse und Subnetmask ein. Im Punkt Hostname vergeben Sie einen Namen für ihren Server. Unter Routing geben Sie falls notwendig ein Defaultgateway an (in dieser Übung aber nicht notwendig).

   Konfigurationsdaten für diese Übung:

   IP-Adresse: 10.0.0.7
   Subnetmask: 255.255.255.0
   Rechnername: B19

2. Als nächstes muss der vsftpd in die Konfiguration des inetd-Dienstes eingetragen werden. Dies erfolgt wiederum am einfachsten per Yast. Gehen Sie dazu unter Netzwerkdienste und dort unter „Netzwerkdienste (xinetd)“. Aktivieren Sie die Option Aktivieren, suchen Sie den Dienst ftp (Achtung: bei Server muss der Eintrag „/usr/bin/vsftpd“ lauten) und klicken Sie auf den Button „Status wechseln (An oder Aus)“ um den Dienst in die Konfigurationsdatei von xinted einzutragen. Beenden Sie den Dialog mit der gleichnamigen Schaltfläche um die Konfiguration zu Speichern.

3. Als nächstes muss die AccessControl-Liste bearbeitet werden um allen IP-Adressen den Zugriff auf den Server zu garantieren. Wechseln Sie dafür in die Konsole (als Superuser). Begeben Sie sich in das Verzeichnis „/etc“ und öffnen Sie die Datei „hosts.allow“:

   ```
   #mcedit hosts.allow
   ```

   Fügen Sie am Ende der Datei folgende Zeile ein:

   ```
   vsftpd: ALL
   ```

   Speichern Sie die Änderung mit F2 und beenden Sie den Editor mit F10.

4. Um den Server allerdings wirklich von außen zugänglich zu machen, muss die Firewall noch konfiguriert werden. Dies erledigen Sie wieder über Yast. Gehen Sie dort unter Sicherheit und Benutzer dann unter Firewall. Gehen Sie dort auf den Punkt „Erlaubte Dienste“ unter Erweitert und geben Sie bei TCP-Ports „21“ ein. Bestätigen Sie mit OK und gehen Sie auf den Punt Start wo Sie auf „Einstellungen speichern und Firewall nun neu starten“ klicken.

5. Nun muss der Dienst „xinetd“ (fasst alle Netzwerkdienste zusammen) noch in die „chkconfig“-Datei eingetragen werden. Dadurch wird dieser dann bei jedem Systemstart automatisch mitgestartet. Gehen Sie dazu in die Konsole und geben Sie folgenden Befehl ein

   ```
   #chkconfig –add xinetd
   ```

Starten Sie den Server nun manuell um ihn zu testen.

```
#/etc/init.d/xinetd start
```

6. Bevor Sie den Server jetzt endgültig konfigurieren, testen Sie diesen. Standardmäßig ist der Anonymous-Account bereits konfiguriert. Um den Server also zu testen reicht es sich kurz bei Anonymous einzuloggen. Zuvor überprüfen wir jedoch ob der Dienst überhaupt gestartet wurde. Geben Sie dazu folgenden Befehl ein:

   ```
   #netstat –a | grep ftp
   ```

   Hier sollte dann eine Zeile in dem der FTP-Server aufscheint ausgegeben werden. Testen Sie nun den Zugriff mit Hilfe des Konsolen-ftp-Programms:

   ```
   #ftp
   ftp>open 127.0.0.1
   Einloggen mit anonymous und keinem Passwort
   Beenden Sie die Verbindung mit ftp>quit
   ```

7. Um den FTP-Server jetzt endgültig zu kunfigurieren beenden Sie diesen zuerst mit folgendem Befehl:

   ```
   #/etc/init.d/xinetd stop
   ```

8. Jetzt öffnen Sie den Konfigurationsfile des Servers. Gehen Sie dazu in das Verzeichnis „/etc“ und rufen Sie mit folgendem Befehl die Datei „vsftp.conf“ auf:

   ```
   #mcedit vsftp.conf
   ```

   Die nachfolgende Auflistung enthält nur jene Punkt die geändert wurden oder jene bei denen die Auskommentierung gelöscht wurde (in der Reihenfolge wie sie im Config-File enthalten sind). Für nähere Details zu den einzelnen Punkte lesen Sie die Kommentare in der Konfigurationsdatei bzw. weiter unten im Dokument den Punkt Theorie.

   ```
   General Settings
       write_enable=YES
       ftpd_banner="Welcome to my FTP service."
       deny_email_enable=YES
       banned_email_file=/etc/vsftpd.banned_emails

   Local FTP user Settings
       local_enable=YES

   Anonymous FTP user Settings
       anon_upload_enable=NO
       anon_max_rate=7200
   ```

9. Jetzt muss noch die Datei „vsftpd.banned_emails“ erzeugt werden.

   ```
   #mcedit vsftp.conf
   ```

   Fügen Sie folgende Zeilen ein:

   ```
   #denied E-mail Adresses
   @gmx.at
   ```

10. Zu Schluss starten Sie den Serverdienst wieder und testen Sie die Einstellung durch Anmeldung am Server und erstellen bzw. downloaden von Dateien.

    ```
    #/etc/init.d/xinetd start
    ```

# Theorie

## Allgemeines

Very Secure im Namen des FTP-Servers unterstreicht das Anliegen der Entwickler, bei Design und Implementierung die Sicherheit zum obersten Prinzip zu erheben. Der Einsatz des Servers ist zwar keine Garantie für absolute Sicherheit. Bislang jedoch sind keine gravierenden Sicherheitslücken des Vsftpd bekannt geworden.
Das recht einfache Aufsetzen des Servers und nicht zuletzt seine gute Skalierbarkeit und Geschwindigkeit prädistenieren den Server für den Einsatz als FTP-Server in kleinen und mittleren Netzwerken.

## Konfiguration

Die allgemeine Konfiguration des Daemons erfolgt in der Datei /etc/vsftpd.conf. Belange der Sicherheit werden bei Verwendung von Pluggable Authentication Modules in der Datei /etc/pam.d/vsftpd eingestellt.
Die Datei /etc/vsftpd.conf
Mit dem Doppelkreuz beginnende Zeilen der Konfigurationsdatei sind Kommentare. Einträge besitzen stets die Form: <Option>=<Wert>

Boolsche Optionen kennen den Status YES (aktiviert) und NO (deaktiviert). Ist eine solche Option nicht explizit aufgeführt, gilt ihr voreingestellter Wert.
Folgende boolsche Optionen (Auswahl) kennt vsftpd; die Voreinstellung ist in Klammern angegeben:

**anon_mkdir_write_enable (NO)**
Gestattet dem anonymen Zugang das Anlegen neuer Verzeichnisse. Hierzu müssen sowohl write_enable aktiviert als auch die entsprechenden Rechte im übergeordneten Verzeichnis entsprechend gesetzt sein.

**anon_other_write_enable (NO)**
Umbenennen und Löschen von Dateien/Verzeichnissen ist auch den anonymen Benutzern möglich.

**anon_upload_enable (NO)**
Gestattet dem anonymen Zugang das Hochladen neuer Dateien. Hierzu müssen sowohl write_enable aktiviert als auch die entsprechenden Rechte im übergeordneten Verzeichnis entsprechend gesetzt sein.

**anon_world_readable_only (YES)**
Anonyme Benutzer dürfen nurDateien runterladen, auf die »Leserechte für alle« bestehen.

**anonymous_enable (NO)**
Ist diese Option gesetzt, ist der anonyme FTP-Zugang zugelassen.

**chown_uploads (NO)**
Hochgeladene Dateien gehören in edr Voreinstellung dem Benutzer, der das Hochladen vornahm. Bei YES wird stattdessen der unter chown_username angebene Benutzer zum neuen Eigentümer.

**chroot_list_enable (NO)**
Bei Aktivierung werden lokale Benutzer, die in einer Datei /etc/vsftp.chroot_list aufgeführt sind, vom chroot-Wechsel in ihr Heimatverzeichnis ausgenommen (in Verbindung mit der Option chroot_local_usr sinnvoll). Die zu verwendende Konfigurationsdatei kann mittels der Option chroot_list_file geändert werden.

**chroot_local_user (NO)**
Steht die Option auf YES, landen lokale Benutzer nach der Anmeldung via chroot in ihrem Homeverzeichnis. In der Voreinstellung verfügen die Benutzer den vollen Zugriff auf das Dateisystem analog zur lokalen Anmeldung.

**dirmessage_enable (NO)**
Ist die Option aktiv, erhalten die Benutzer beim erstmaligen Wechsel in ein Verzeichnis den Inhalt der Datei .message aus dem Verzeichnis (falls vorhanden) angezeigt. Der Name der anzuzeigenden Datei ist über die Option message_file konfigurierbar.

**guest_enable (NO)**
Anonyme Anmeldungen werden bei aktivierter Option auf den in guest_username benannten Zugang gemappt.

**listen (NO)**
Die Option ist zu Setzen, wenn der FTP-Daemon nicht über einen der Internet-Daemonen inetd oder xinetd gestartet wird. Erst somit überwacht er selbstständig die Ports auf eintreffende Verbindungen.

**local_enable (NO)**
Erst bei Aktivierung dürfen sich lokale Benutzer (mit Zugang in der Datei /etc/passwd) via FTP anmelden.

**log_ftp_protocol (NO)**
Bei aktiver Option werden alle FTP-Anforderungen und -Antworten protokolliert.

**port_enable (YES)**

**text_userdb_names (NO)**
Eigentümer/Gruppen werden beim Dateilisting als Namen anstatt als numerische ID's dargestellt.

**userlist_deny (YES)**
Die Option ist nur bei gesetzem userlist_enable relevant. Dann wird lokalen Benutzern das Anmelden nur ermöglicht, wenn sie explizit in der in userlist_file benannten Datei aufgeführt sind.

**userlist_enable (NO)**
Bei Aktivierung ist das Anmelden nur für die localen Benutzer möglich, die in der in userlist_file benannten Datei aufgeführt sind.

**write_enable (NO)**
Bei Aktivierung sind FTP-Kommandos, die Änderungen am Dateisystem vornehmen, gestattet.

**xferlog_enable (NO)**
Ermöglicht die detaillierte Protokollierung von Downloads und Uploads. Die Daten landen in der in xferlog_file benannten Datei (Voreinstellung /var/log/vsftpd.log).
Numerische Optionen konfigurieren im Wesentlichen das Timeout-Verhalten und die zu verwendenden Ports (Auswahl):

**accept_timeout (60)**
Nach so vielen Sekunden nach Aufbau der Verbindung wird diese abgebrochen, falls der Client sich noch nicht authentifiziert hat.

**anon_max_rate (0)**
Anzahl Bytes pro Sekunde, mit denen Daten vom/zum anonymen Clients erfolgen. 0 bedeutet keine Einschränkung der Transfergeschwindigkeit.

**connect_timeout (60)**
Nach dieser Zeitspanne wird die Verbindung zu einem Client gekappt, falls keine Kommunikation stattfand.

**data_connection_timeout (300)**
Werden laufende Datenübertragungen unterbrochen, wird ein Client nach Ablauf dieser Zeitspanne automatisch rausgeworfen.

**ftp_data_port (20)**
Der Datenport für die Datenübertragung.

**idle_session_timeout (300)**
Nach Ablauf dieser Zeit ohne jeglicher Kommunikation zwischen Server und Client wird die Verbindung zum Client geschlossen.

**local_max_rate (0)**
Analog zu annon_max_rate nur für lokale Benutzer.

**max_clients (0)**
Maximale Anzahl gleichzeitig akzeptierter Verbindungen. Nur im Stand-alone-Modus relevant. 0 bedeutet »unbegrenzt«.
Des Weiteren existieren eine Fülle von Zeichenkettenoptionen (Auswahl):

**anon_root (none)**
Bei anonymen Zugang erfolgt eine Wechsel in das angegebene Verzeichnis (via chroot).

**banner_file (none)**
Wenn gesetzt, wird der Text der angegebenen Datei beim ersten Anmelden einen Clients angezeigt. Ist die Option nicht aktiv, wird der unter ftpd_banner stehende Text zur Anzeige verwendet.

**chown_username (root)**
Der Eigentümer, dem hochgeladene Dateien anonymer Benutzer zugeordnet werden, insofern auch die Option chown_uploads gesetzt ist.
chroot_list_file (/etc/vsftpd.chroot_list)

Existiert die angegebene Datei und sind die Optionen chroot_list_enable aktiv bzw. chroot_local_user nicht aktiv, so werden die in der Datei benannten lokalen Benutzer via chroot bei Anmeldung in ihr Heimatverzeichnis verbannt.

**guest_username (ftp)**
Der Benutzername für den anonymen Zugang, falls dieser auf ein spezielles »Gastlogin« gemappt ist. Die Option wird nur betrachtet, wenn guest_enable gesetzt ist.

**ftp_username (ftp)**
Der Benutzername für den anonymen Zugang. Das Heimatverzeichnis ist i.d.R. ein spezielles FTP-Verzeichnis, das mittels eines chroot-Umgebung betreten wird. Der Unterschied zum Gast-Zugang (vergleiche guest_username) ist im Wesentlichen, das letzterer nicht zwingend in einer chroot-Umgebung gefangen ist.

**ftpd_banner (none)**
Der Begrüßungstext bei erstmaligem FTP-Zugang. Ist die Option nicht gesetzt, wird ein Vsftpd-eigener Text angezeigt.

**listen_address (none)**
Bei Rechnern mit mehreren Schnittstellen kann der Vsftpd engeweisen werden, eine andere als die erste Schnittstelle auf einkommende Verbindungen zu überwachen. Einzutragen ist hier die numerische IP-Adresse der zu überwachenden Schnittstelle.

**local_root (none)**
Wenn gesetzt, landen lokale Benutzer nach erfolgreicher Anmeldung in diesem Verzeichnis (sonst in ihrem Heimatverzeichnis).

**message_file (.message)**
Der Inhalt dieser Datei wird angezeigt, wenn ein Verzeichnis erstmals betreten wird und eine solche Datei dort existiert. Des Weiterin muss dirmessage_enable gesetzt sein.

**pam_service_name (ftp)**
Bezeichner, den der Vsftpd bei Verwendung der Pluggable Authentication Modules wählt.

**user_config_dir (none)**
Ermöglicht eine Benutzer abhängige Konfiguration. Existiert im angegebenen Verzeichnis eine gleichnamige Datei wie ein sich anmeldender Benutzer(name), so gelten für dessen Zugang neben den allgemein gesetzten alle darin aufgeführten Optionen. Die Benutzer spezifischen Optionen überschreiben ggf. die globalen!

**userlist_file (/etc/vsftpd.user_list)**
Siehe userlist_enable.

**xferlog_file (/var/log/vsftpd.log)**
Protokolldatei für die Transferstatistik.

## Beispielkonfiguration

Eine typische Konfigurationsdatei für einen einfachen Server könnte folgende Optionen enthalten:

```
user@sonne> cat /etc/vsftpd.conf
# Beispielkonfiguration /etc/vsftpd.conf
#
# Anonymes FTP gestatten
anonymous_enable=YES
#
# Lokale Anmeldung gestatten
local_enable=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 (beide Optionen sind in der
Voreinstellung auf NO gesetzt; wir führen sie hier nur zur Demonstration explizit auf)
anon_upload_enable=NO
anon_mkdir_write_enable=NO
#
# 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 dem Linuxfibel-FTP-Server
#
# Als PAM-Dienst verwenden wir nicht die Standard-FTP-Konfiguration
pam_service_name=vsftpd
```

## Start des Servers

In den meisten Anwendungsfällen wird ein FTP-Server nur sporadisch benötigt, sodass sich dessen Start erst bei Bedarf, also über einen der Internet-Daemons inetd oder xinetd anbietet.
Start via inetd

```
root@sonne> vi /etc/inetd.conf
...
# These are standard services.
#
# ftp   stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd
```

```
ftp   stream  tcp     nowait  root    /usr/sbin/tcpd  vsftpd
...
```

Der im Beispiel zwischen geschaltete TCP-Wrapper ist nicht zwingend notwendig. Zumindest bei Authentifizierung mittels Pluggable Authentication Modules ist der zusätzlich Gewinn an Sicherheit gleich Null.
Vergessen Sie nach Änderungen in der Konfigurationsdatei nicht, den inetd neu zu starten!
Start via xinetd

```
root@sonne> vi /etc/xinetd.conf
...
service ftp
  {
  socket_type = stream
  wait        = no
  user        = root
  server      = /usr/sbin/vsftpd
  server_flags = -a
  log_on_success += DURATION
  instance    = 4
  }
```

Nach Modifikation ist der xinetd neu zu starten.
Start als eigenständiger Server
Der Vsftpd ist nicht für den Stand-Alone-Betrieb vorgesehen. Versuchten Sie dennoch den Start, ernten Sie eine Abfuhr:

```
root@sonne> vsftpd
500 OOPS: vsftpd: does not run standalone, must be started from inetd
```

## Problemberichte und Anmerkungen

**Problembericht 1**

Es ist das Problem aufgetreten, dass das Einloggen als Anonymous mittels dem Konsolen-Ftp-Programms nicht möglich war (Allerdings erst nachdem dem Anlegen der „vsftpd.banned_emails“ Datei und dem Aktivieren des Punktes „deny_email_enable=YES“) . Wurde der Server mittels Browser (IE-Explorer, Konqueror) war dies allerdings kein Problem.

Eine mögliche Ursache dürfte sein, dass bei der Anmeldung mittels Konsole keine E-Mailadresse mitgesendet wird und die Option „deny_email_enable=YES“ zur Überprüfung jetzt aber immer eine E-Mailadresse erwartet. Eine Lösung zu dem Problem wurde allerdings nicht gefunden, außer sich mittels Browser oder eines FTP-Clients eines Drittanbieters zu verbinden.

**Anmerkung 1**

Es gibt zwei Möglichkeiten den vsftpd zu Starten und zu Stoppen:

1. /etc/init.d/xinetd start/stop
2. service vsftpd start/stop/restart

Dabei sollte immer die 1. Variante benutz werden da damit alle Netzwerkdienste neu gestartet werden.

**Anmerkung 2**

Unter Suse liegt das Verzeichnis des Anonymous-Users des FTP-Servers bzw. generell das Standardverzeichnis des FTP-Servers unter „/srv/ftp“.