



Willkommen

zum Vortrag Linux im Serverbetrieb

von

Maik Gischel und Michael Thieme

im Rahmen der Linux- Installations- Party 2008



DHCP

SSH

Domain

Timeserver

Terminal server

DNS

SAMBA/ NFS

POP3

Groupwareserver

WWW

FTP

Proxy-Server

SMTP

VPN

Backupserver



SSH



Einleitung

SSH dient zum Herstellen einer sicheren Verbindung zu einem entfernten Computer. Die IANA (Internet Assigned Numbers Authority) hat dem SSH-Protokoll den TCP-Port 22 vergeben.

SSH steht dabei als Abkürzung für „Secure Shell“ und ist eine Sammlung von Programmen.

Unter ihnen gibt es z.B. den SSH-Client und den SSH-Server. Nachdem SSH unter einer kommerziellen Lizenz angeboten wurde, nahmen sich die Entwickler von OpenBSD des Quellcodes an und entwickelten eine freie Version namens „OpenSSH“.

Diese ist in fast allen Linux- / UNIX Distributionen verfügbar und soll Teil dieses Vortrages sein.



SSH

Installation

SSH-Client:

- ist bereits verfügbar und muss nicht nachinstalliert werden

SSH-Server:

```
sudo apt-get install openssh-server
```

Konfiguration

SSH-Client:

~/.ssh/config (Einstellungen für jeden Benutzer)
/etc/ssh/ssh_config (Globale Einstellungen für alle Nutzer)

SSH-Server:

```
/etc/ssh/sshd_config
```



SSH

Verbindungsaufbau

ssh IP-Adresse
ssh servername

z.B. ssh 192.169.0.1

Befehle automatisch ausführen:

ssh servername befehl

z.B.: ssh servername cat /etc/issue

Verbindung mit anderen Benutzernamen:

ssh -l Benutzername servername
ssh Benutzername@servername
ssh -o User=Benutzername servername

z.B.: ssh -l Benutzer1 192.168.0.1

Verbindung über anderen Port:

ssh servername -p Port

z.B.: ssh 192.168.0.1 -p 2233



SSH

Config-Datei-Client

Host servername

HostName 192.168.0.1

Port 2233

User Benutzer1

Protocol 2

ForwardAgent yes

StrictHostkeyChecking ask

ForwardX11 yes

Compression yes

Cipher 3des

CheckHostIP no

EscapeChar ~

#IP-Adresse des Servers

#geänderter Port

#Benutzername

#Protokollversion

#Überprüfung der Schlüssel

#GUI weiterleiten

#Kompression einschalten

#verwendete Verschlüsselung

#Abbruch Zeichen



SSH

Auszug Config-Datei-Server

Port 2233

PermitRootLogin no

PermitEmptyPasswords no

X11Forwarding yes

PasswordAuthentication yes

UsePAM yes

PrintLastLog yes

TCPKeepAlive yes

#Standard Port ändern

#Benutzer root verweigern

#leere Passwörter ablehnen

#GUI Weiterleiten zulassen

#Einloggen per Passwort zulassen

#Einloggen per Passwort zulassen

#letzten Login anzeigen

#Verbindung aufrecht halten



SSH

Sicherheit

Authentifizierung:

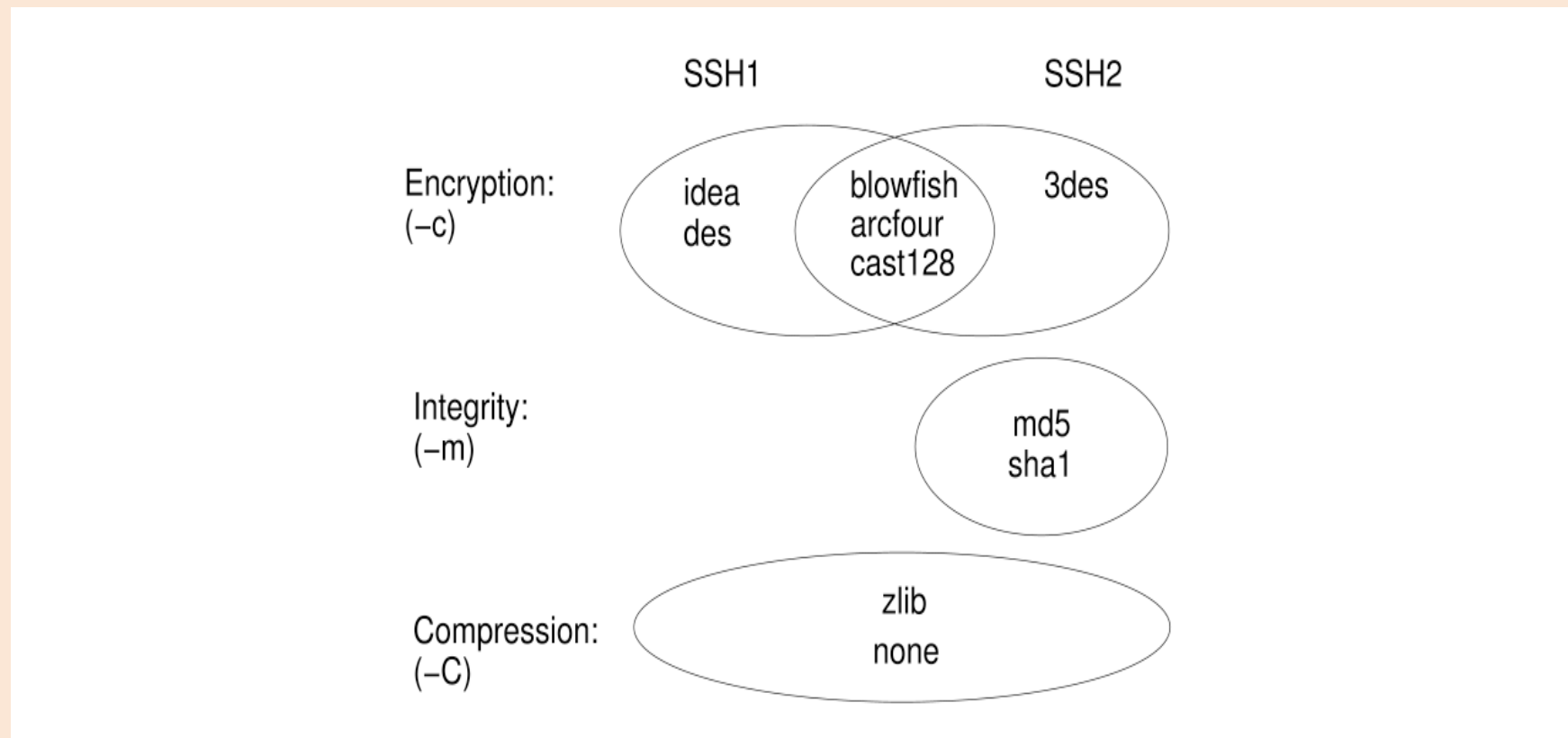
- Server: RSA-Zertifikat
- Client: Kennwort Authentifizierung (Standard Einstellung)
- Client: „Public-Key-Authentifizierung“ (öffentlicher Schlüssel wird auf dem Server hinterlegt)

Verschlüsselung:

- nach Authentifizierung -> Erzeugung eines geheimen Schlüssels; Gültigkeit: Dauer der Sitzung
- SSH2 Standard: AES 128-Bit-Schlüssellänge
- weitere mögliche Verfahren: 3DES, Blowfish, Twofish, CAST, IDEA, Arcfour, SEED, AES verschiedener Schlüssellängen (3DES: besonders sicher -> viel Rechenzeit; Blowfish: besonders schnell)



SSH





SSH

Authentifizierung über Public-Keys

Schlüssel erzeugen:

```
ssh-keygen -t dsa
```

Hinweis: alle Fragen mit Enter bestätigen; Passwort vergeben!

Schlüssel in Server einbinden:

```
ssh-copy-id -i ~/.ssh/id_dsa.pub servername
```

Schlüssel entfernen:

```
ssh-keygen -R servername
```

Schlüssel für eine Sitzung speichern:

```
ssh-add
```

Hinweis: Speicherung nur bis zum Ausloggen aus dem Computer



SSH

X-Forwarding

- grafische Programme anderer Computer werden auf eigenen Computer angezeigt
- Voraussetzung: Paket „xauth“ auf Server installiert;
„X11Forwarding yes“ in Config-Datei-Server

Aufruf:

ssh -X servername

z.B.: ssh -X servername firefox &

Hinweis: „ssh -Y servername“ öffnet den Tunnel in beide Richtungen!



SSH

Dateitransfer

FUSE (Filesystem in USErspace) über SSH:

```
sudo apt-get install sshfs (universe Quellen)
mkdir ~/mp3_server
sudo adduser Benutzername fuse
```

Einbinden:

```
sshfs Benutzername@servername:/Pfad_auf_dem_Server/ /Pfad_auf_den_Client
```

z.B.: `sshfs -C servername:/home/user/mp3 ~/mp3_server`

Aushängen:

```
fusermount -u /Pfad_auf_den_Client
```

z.B.: `fusermount -u ~/mp3_server`



Datenbanksysteme unter Linux

- es stehen sehr viele Datenbank- Management- Systeme zur Verfügung

- Beispiele:

1. MySQL
2. PostgreSQL
3. Oracle
4. usw.



- Betrachten wir zwei der Beispiele näher:

- MySQL
- PostgreSQL





Datenbanksysteme unter Linux

- MySQL
 - wird von vielen Webanwendungen benutzt zum Beispiel:
 - Joomla (CMS)
 - phpBB (Forum)
 - sehr schnelles und einfaches Datenbanksystem
 - weiterhin stehen die unter Windows bekannten grafischen Konfigurationstools auch unter Linux zur Verfügung, zum Beispiel phpMyAdmin in Verbindung mit einem Webserver
 - die Konfiguration kann aber auch per Hand in der Datei `/etc/mysql/my.cnf` vorgenommen werden
 - die Datei `my.cnf` unterteilt sich in verschiedene Blöcke:
 - `[client]` Einstellungen für den MySQL- Client (Portnummer, usw.)
 - `[mysqld]` Einstellung des Serverdienstes (Basis- Einstellungen)
 - und andere



Datenbanksysteme unter Linux

- Auszüge aus der Datei my.cnf:

```
[mysqld]
user= mysql
pid-file= /var/run/mysqld/mysqld.pid
socket= /var/run/mysqld/mysqld.sock
port= 3306
basedir= /usr
datadir= /var/lib/mysql
tmpdir= /tmp
language= /usr/share/mysql/english
skip-external-locking
key_buffer= 16M
max_allowed_packet= 16M
thread_stack= 128K
thread_cache_size= 8
```

Angabe verschiedener Parameter wie
zum Beispiel:
user = Standard- Benutzer
port = Serverport



Datenbanksysteme unter Linux

- PostgreSQL
 - eine der Leistungsstärksten Open Source Datenbanken
 - Universell einsetzbar zum Beispiel für Werbeanwendungen
 - für die Einstellung stehen auch verschiedene Tools zur Verfügung die Bekanntesten sind:
 - PgAdmin III Plattformübergreifende Development und Administrationssoftware
 - phpPgAdmin PHP- basierte Verwaltungssoftware Analog zu phpMyAdmin
 - Manuelle Konfiguration über die Konfigurationsdateien im Verzeichnis /etc/postgresql/8.3/main/ (der Pfad kann sich bei einer anderen Version ändern hier Version 8.3)



Datenbanksysteme unter Linux

- Auszüge aus der Konfigurationsdatei postgresql.conf

```
data_directory = '/var/lib/postgresql/8.3/main'  
port = 5432  
max_connections = 100  
ssl = true
```

Einstellen des
Datenverzeichnisses, des Ports,
der Anzahl der maximal
erlaubten Verbindungen und
Anschalten von SSL

- in der Konfigurationsdatei pg_hba.conf legt man fest wer Zugriff auf die Datenbank hat speziell Hosts, User usw.
- in der Konfigurationsdatei pg_ident.conf kann man Systembenutzern Postgresql- benutzernamen zuweisen
- mit der Konfigurationsdatei start.conf legt man die Startoptionen der Datenbank fest
 - auto automatisches Starten und Stoppen unter Verwendung der Init- Scripte
 - manual manuelles Starten und Stoppen ohne Verwendung der Init- Scripte mit dem Befehl pg_ctlcluster
 - disabled auto und manual Start Deaktiviert



Samba/ NFS



- Samba ist ein Serverapplikation die es ermöglicht Linux- Systeme in bestehende Windowsnetzwerke einzubinden
- Weiter besteht die Möglichkeit Linux Ressourcen Windowsrechner zur Verfügung zustellen
 - zum Beispiel Drucker oder Dateien und Ordner
- Samba unterstützt weiterhin auch die NetBIOS- Namensgebung von Windowssysteme und kann auch als NetBIOS – Name – Server verwendet werden
- der Samba- Daemon „smbd“ stellt die Datei- und Druckerfreigaben für die SMB- Clients (Windows und Unix/Linux) bereicht
- die Konfiguration von Samba kann mit Hilfe verschiedener Tools vorgenommen werden Beispiele hierfür sind:
 - SWAT – Samba eigenes browserbasiertes Tool
 - Webmin – browserbasiertes Konfigurationstool
 - GSAMBAD – C/GTK+ – basiertes Tool
 - Smb4K – KDE basiertes Programm
- die Konfiguration kann auch hier wieder Manuell durchgeführt werden



Samba/ NFS

- die Manuelle Samba- Konfiguration
 - die Konfigurationsdatei befindet sich in `/etc/samba/smb.conf`
 - die Datei unterteilt sich in verschiedene Blöcke, die Wichtigsten sind:
 - **[Global]** globale Einstellungen
 - **[Homes]** Freigabe der Homeverzeichnisse
 - **[Printers]** Freigabe von Druckern
 - die Vergabe von Zugriffsrechten für Freigaben ist in Samba elementar
 - Samba stellt hierfür eine Reihe von Möglichkeiten zur Verfügung
 - globale Sicherheitsoptionen im [Global] teil der smb.conf:
 - der Parameter „`security= [wert]`“, hat folgende Optionen
 - **user** Benutzername und Passwort werden Abgefragt
 - **share** der Freigabe wird ein Passwort zugeordnet
 - **server** die Authentifikation wird von einem User Level Mode Server übernommen



Samba/ NFS

- Sicherheitsoptionen für einzelne Freigaben
 - **create mask= [wert]**
 - **directory mask= [wert]**
 - die Werte für diese Optionen setzen sich aus Oktalzahlen wie folgt zusammen:

Oktal	Bitmaske	Rechte
750	111 101 000	user: rwx, group: rx, other: --
544	101 100 100	user: rx, group: r, other: r
775	111 111 101	user: rwx, group: rwx, other: rx

- Beispiele für eine minimale Konfiguration



Samba/ NFS

[global]

netbios name = LIPSERVER

server string = SAMBA

workgroup = LIP2007

wins support = yes

interfaces = xxxx/24

encrypt passwords = true

security = user

domain logons = no

Angabe des Servernamens, der Arbeitsgruppe und der globalen Sicherheitsoptionen

[homes]

comment = Home Directories

writeable = yes

create mask = 0700

directory mask = 0700

valid users = %s

Freigabe der Homeverzeichnisse und Angabe der Rechte für die Freigabe in diesem fall nur der Eigentümer (user) darf zugreifen



Samba/ NFS

```
[public]
path = /media/public/
browseable = yes
read only = yes
guest ok = yes
create mask = 0644
directory mask = 0755
force user = YOUR_USERNAME
force group = YOUR_USERGROUP
```

Öffentliches Read- Only Verzeichnis





Linux als Backupserver

- unter Linux gibt es eine Vielzahl von Programmen zur Datensicherung
 - Beispiele sind:
 - rsync
 - rsnapshot
 - tar
 - buffer
 - partimage
 - es stehen alle Backupmedien zur Verfügung (Tape, CD, DVD, HDD usw.)
 - Backup mit dem Programm rsync
 - rsync vergleicht Dateien und Verzeichnisse auf einem Quell- und einem Ziellaufwerk miteinander, gibt es Unterschiede werden die Verzeichnisse bzw. die Dateien mit einander synchronisiert dabei werden nur die Unterschiede übertragen
 - Befehl:

```
rsync [OPTIONEN] <Quelle> <Ziel>
```





Linux als Backupserver

- Automatisches Backup mit Hilfe eines Skriptes welches als Cron- Job gespeichert werden kann

```
#!/bin/sh
cd ~Directory
{
echo
date
dest=~/.backup/`date +%A`
mkdir $dest.new
find . -xdev -type f \( -mtime 0 -or -mtime 1 \) -exec cp -aPv "{}"
$dest.new \;
cnt=`find $dest.new -type f | wc -l`
if [ $cnt -gt 0 ]; then
  rm -rf $dest
  mv $dest.new $dest
fi
rm -rf $dest.new
rsync -Cavze ssh . samba:backup
}>> ~/.backup/backup.log 2>&1
```




FTP- Server

Einleitung

Ein FTP-Server ist ein Computer, welcher es ermöglicht Daten über ein Netzwerk auszutauschen. FTP steht dabei als Abkürzung für „File Transfer Protocol“.

Das Programm ProFTPD ist ein weit verbreiteter FTP-Server für Linux.

Dieser ist in vielen Distributionen schon in den Quellen verfügbar.

Installation

```
sudo apt-get install proftpd #(universe Quellen)
```

Konfiguration

```
sudo vi /etc/proftpd/proftpd.conf
```

Einen Anonymous FTP-Zugang einrichten

am Ordner /home/ftp/ die benötigten Zugangsrechte anpassen:

```
sudo chmod 777 -R /home/ftp/
```



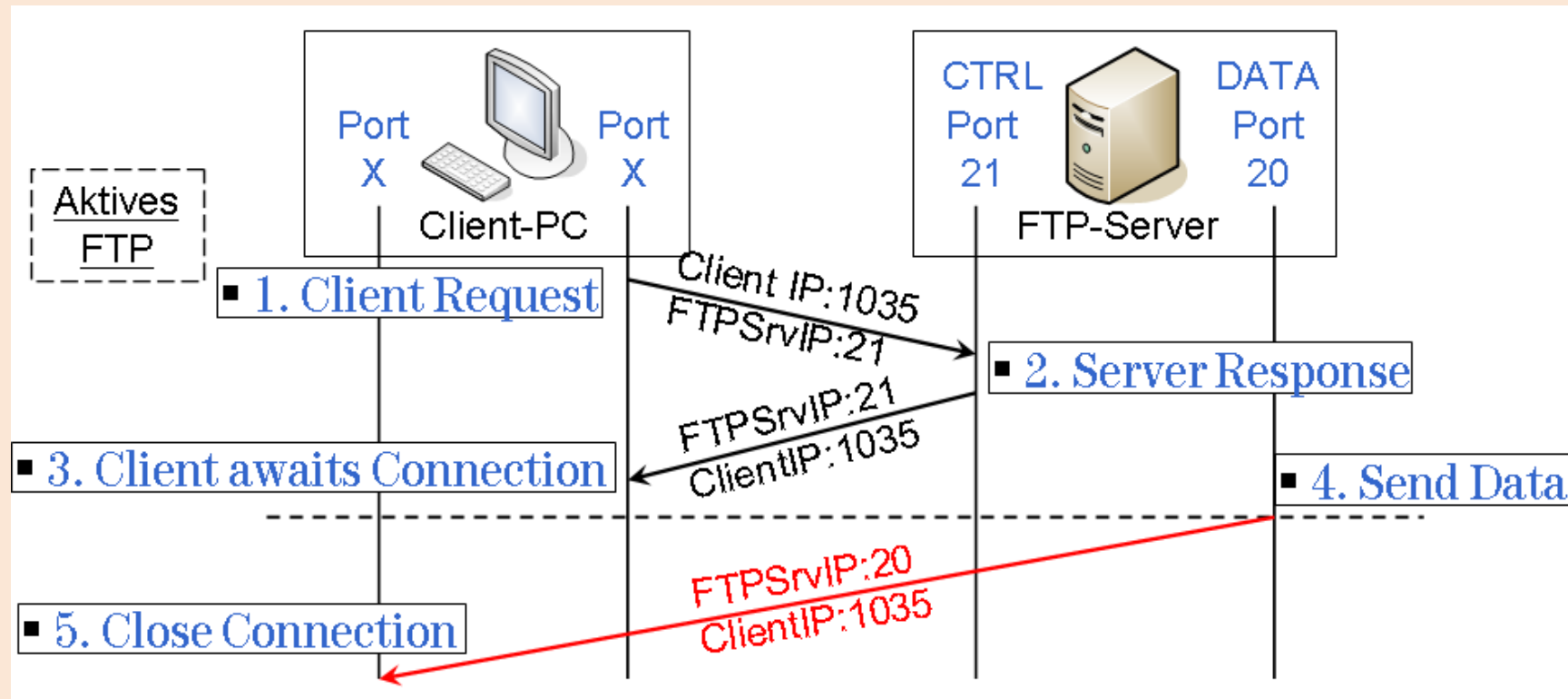
FTP- Server

- an das Ende der proftpd.conf schreiben (Lese- aber keine Schreibrechte):

```
<Anonymous ~ftp>
  User          ftp
  Group         nogroup
  UserAlias     anonymous ftp
  DirFakeUser  on ftp
  DirFakeGroup on ftp
  RequireValidShell  off
  MaxClients   10
  DisplayLogin  welcome.msg
  DisplayFirstChdir  .message
  <Directory *>
    <Limit WRITE>
      DenyAll
    </Limit>
  </Directory>
</Anonymous>
```



FTP- Server





FTP- Server

Benutzer anlegen

-alle Benutzer des Systems haben FTP Zugang, damit allerdings auch z.B. einen SSH-Zugang mit einer Shell

virtuelle Benutzer anlegen (haben keine weiteren Rechte im System)

- die Datei `/etc/proftpd/proftpd.conf` bearbeiten

DefaultRoot ~

AuthUserFile `/etc/proftpd/ftpd.passwd`

AuthPAM off

RequireValidShell off

- in das Verzeichnis `/etc/proftpd/` wechseln

```
sudo ftpasswd --passwd --name benutzername --uid 500 --home /pfad/zum/userdir --shell /bin/false
```



FTP- Server

Resume erlauben

in die Datei proftpd.conf eintragen:

AllowOverwrite on
AllowRetrieveRestart on
AllowStoreRestart on

Hinweis: "hiddenstor" darf nicht aktiviert sein

ProFTPD neu starten

```
sudo /etc/init.d/proftpd restart
```



FTP- Server

verbundene Benutzer anzeigen

ftpwho -v

ab ProFTPD 1.2.7 mittels Tool (dauerhafte Anzeige):

ftptop

Benutzer in ein Verzeichnis "einsperren"

- "defaultroot" in der proftpd.conf
- es kann ein Verzeichnis oder der Platzhalter "~" (Home-Verzeichnis) angegeben werden

Beispiel:

Benutzer in das Verzeichnis /home/ftp einschließen:

- defaultroot /home/ftp

Benutzer in ihr Home-Verzeichnis einschließen:

- defaultroot ~



Web- Server

- als Web- Server wird Linux sehr oft eingesetzt
- die bekannteste Web- Server- Software ist Apache, dieser lässt sich ohne großen Aufwand, mit Hilfe von APT-Get Installieren
 - Nachteil hierbei ist das wichtige Zusatzpakete wie zum Beispiel php auch einzeln nachinstalliert werden müssen
- besser eignet sich hier XAMPP (früher LAMPP)
 - XAMPP besteht aus folgenden Paketen:
 - Apache
 - MySQL
 - Perl
 - PHP
 - ProFTPd
 - OpenSSL
 -
 - das XAMPP Paket ist eigenständig und verwaltet die Config Daten in eigenen Ordnern die von System unabhängig sind
 - Nachteil hier an der Grundinstallation müssen noch einige Einstellungen hinsichtlich der Sicherheit des System getätigt werden



Postfix



Einleitung

Postfix ist ein Mail Transfer Agent (MTA) für Linux- und Unix-Derivate.

Der Klassiker dieser Programme wäre zwar sendmail, jedoch ist sendmail sehr umständlich einstellbar.

Postfix hingegen ist sicher, schnell, einfach zu administrieren, hat einen modularen Programmaufbau,

Änderungen der Konfiguration können zur Laufzeit erfolgen und Postfix ist Aufrufkompartible zu sendmail.

Diese Kompatibilität erleichtert sendmail Nutzern den Umstieg.

Postfix steht unter der „IBM Public License“ und ist somit freie Software.



Postfix

Installation

```
sudo apt-get install postfix
```

```
sudo apt-get install libsasl2-modules #notwendig bei Authentifizierung  
am Smarthost
```

```
sudo apt-get install mailx #optional – Versenden von mails über die Console
```



Postfix

Authentifizierung am Smarthost

- ist notwendig, da fast alle mail-Server mails von Dialin Zugängen nicht akzeptieren
- mails müssen demzufolge über externe mail-Anbieter geleitet werden

Config-Datei vorbereiten:

```
sudo vi /etc/postfix/main.cf
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noplaintext noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

Zugangsdaten eintragen:

```
sudo vi /etc/postfix/sasl_password
smtp.mailanbieter.de Loginname:Passwort_des_Nutzers
```

```
sudo postmap /etc/postfix/sasl_password
```



Postfix

Absenderinformation angeben:

```
sudo vi /etc/postfix/sender_canonical  
Benutzername email.adresse@stud.fh-sm.de  
www-data webserver@was_auch_immer.net
```

```
sudo postmap /etc/postfix/sender_canonical
```

Postfix neu starten:

```
sudo /etc/init.d/postfix restart
```



Postfix

Funktionstest

mail versenden:

```
mail -s "Text der Betreffzeile" email@mailanbieter.de < textdatei_mit_Inhalt.txt
```

Kontrolle:

```
vi /var/log/mail.log
```

```
...from=<email.adresse@stud.fh-sm.de>...
```

```
...to=<email@mailanbieter.de>,... status=sent... Message accepted
```



Quellen

<http://www.jfranken.de/homepages/johannes/vortraege/ssh1.de.html>

<http://wiki.ubuntuusers.de/ssh>

<http://de.wikipedia.org/wiki/Ssh>

<http://openssh.org/de/index.html>

<http://wiki.ubuntuusers.de/ProFTPD>

<http://www.proftpd.de/>

http://de.wikipedia.org/wiki/File_Transfer_Protocol

<http://wiki.ubuntuusers.de/Postfix>

[http://de.wikipedia.org/wiki/Postfix \(Mail Transfer Agent\)](http://de.wikipedia.org/wiki/Postfix_(Mail_Transfer_Agent))

<http://www.mysql.de>

<http://www.postgresql.org>

<http://wiki.ubuntuusers.de/rsync>

<http://de.wikipedia.org/wiki/Rsync>

<http://www.apachefriends.org/de/xampp.html>

<http://wiki.ubuntuusers.de/Sicherheit>



Quellen Bilder

<http://www.jfranken.de/homepages/johannes/vortraege/ssh/protokolle.png>

<http://openssh.org/images/openssh.gif>

<http://upload.wikimedia.org/wikipedia/de/8/89/AktivesFTP.png>

<http://www.postfix.org/mysza.gif>

<http://thehostconnection.ch/web1/Pics/logoMysql.gif>

http://www.alleventsgroup.com/mhrcongress/images/oracle_logo3.jpg

<http://pgfoundry.org/docman/view.php/1000089/72/100x58.zip>

http://upload.wikimedia.org/wikipedia/de/b/bd/Logo_Samba_Software.svg

<http://www.daten-bunker.de/images/backup-tape.jpg>



Danke für die Aufmerksamkeit

???? FRAGEN ????

ENDE