

LA-Server 9.2-Beta.

Mag. Dr. Klaus Misof & MMag. Rene Schwarzinger

Inhaltsverzeichnis

I. Vorbemerkung	2
II. LinuxAdvanced Server	3
1. Allgemeine Beschreibung	3
2. Installation	4
3. Allgemeine Konfiguration	4
3.1. Grundkonfiguration	4
3.1.1. Netzwerkkarten	5
3.1.2. DHCP und DNS mit dnsmasq	7
3.2. Dienste Starten	8
3.3. Firewall	8
3.4. Internet-Filter	9
3.5. DATENBANK-NEU-ANLEGEN	10
3.6. Raum-Verwaltung	10
4. File- und Account-Server	12
4.1. User-Verwaltung	12
4.2. Userprofil-Verwaltung	15
4.3. Web-Kontrolle	16
4.4. Zentrale Client-Verwaltung	18
4.4.1. Synchronisation der Clients	19

Tabellenverzeichnis

5. E-Mail-Server	20
5.1. Allgemeines	20
5.2. Konfiguration	20
5.3. SPAM- und Virenfiler	22
5.4. IMAPS und Certificaterstellung	23
5.5. E-Mail-Account-Verwaltung	24

Abbildungsverzeichnis

1. Die Server-Verwaltung mittels menu.sh	5
2. Netzwerkkartenkonfiguration	6
3. Firewall Einstellungen	9
4. Web-Filter	10
5. Raumstruktur	11
6. User-Verwaltung	14
7. Profile-Verwaltung	16
8. Web-Kontrolle	17
9. Remote-Client-Verwaltung	19
10. EMAIL-Konfiguration	21
11. POSTFIX-Konfiguration	22
12. SPAM-Filter-Einstellungen	23
13. IMAPS, HTTPS, CA	24
14. EMAIL-Admin	25

Tabellenverzeichnis

Teil I. Vorbemerkung

Dieses Skriptum beschreibt, wie man mittels der Distribution LinuxAdvanced (LA) ein Schulnetzwerk rasch aufbauen kann. LinuxAdvanced basiert auf GNU/Debian. Es gibt jede Menge von GNU/Linux Distributionen für den Desktop Einsatz. Es gibt mittlerweile auch eine große Anzahl von verschiedenen Server-Entwicklungen für schulische Netzwerke (Arktur-Server, Slixs-Server, Open School Server, ...).

Teil II.

LinuxAdvanced Server

1. Allgemeine Beschreibung

Der LA-Server ist konzipiert für kleine bis mittlere Netzwerke. Der LA-Server kann sehr schnell konfiguriert werden und deckt die meisten in Schulen notwendigen Dienste ab. Folgende Aufgaben können sofort vom Server übernommen werden:

- DHCP-Server
- lokaler DNS-Server
- Authentifizierungs-Server (über MySQL oder LDAP)
- File-Server
- Web-Server
- E-Mail-Server
- MySQL-Datenbank-Server

Alle Dienste sind bereits vorkonfiguriert und nur die notwendigen individuellen Einstellungen werden mittels Dialog geführter Skripte durchgeführt. Die Wartung des LA-Servers ist sehr einfach und deshalb auch zeitsparend. Der LA-Server ist abgestimmt auf den LA-Desktop. Der LA-Server ist nicht für Windows-Clients vorkonfiguriert. Will man Windows-Clients mit dem LA-Server verwalten, dann müssen noch einige Dienste (SAMBAs) konfiguriert werden. Es ist aber möglich, auch einen PDC auf den LA-Server aufzubauen. Da der Server ebenfalls wie der LA-Desktop auf Debian Lenny basiert, sind alle Erweiterungen von Debian jederzeit integrierbar.

Die User-Verwaltung, Raum-Verwaltung, Remote-Client-Verwaltung und Web-Kontrolle basiert auf einer MySQL-Datenbank. Die einzelnen Skripte greifen zunächst auf die MySQL-Datenbank zu und aktualisieren diese. Dann werden aus diesen MySQL-Daten die notwendigen Konfigurationsdateien erzeugt bzw. aktualisiert. Auch die MySQL-Datenbank ist zunächst bereits vorkonfiguriert, kann aber durch ein Skript auch komplett neu erstellt werden. Versierte Anwender können natürlich auch direkt mit der MySQL-Datenbank arbeiten (z.B. mit phpmyadmin). Die User-Datenbank vom MySQL-Server wird automatisch auch in eine LDAP-Datenbank übertragen. Somit kann die Authentifizierung entweder direkt über die MySQL-Datenbank oder die LDAP-Datenbank laufen. Darum sollte man für die Bearbeitung der USER nicht direkt mit der MySQL-Datenbank arbeiten, sondern die LA-Skripts verwenden. Nur so bleiben beide Datenbanken synchron. Die LDAP-Datenbank ermöglicht somit auch eine Anbindung anderer Dienste, wie z.B. Moodle.

3. Allgemeine Konfiguration

2. Installation

Die Installation des LA-Servers unterscheidet sich nicht von der Installation des LA-Desktops. Voraussetzung ist, dass der User- und File-Server den Namen "fileserv" erhält. Der E-Mail, Web und MySQL-Server kann aber auch auf anderen Maschinen installiert werden und auch andere Namen bekommen. Diese Restriktion der Nomenklatur wird aber demnächst beseitigt.

3. Allgemeine Konfiguration

3.1. Grundkonfiguration

Alle Einstellungen und Skripte zur Konfiguration findet man unter

```
/server
```

Man öffnet ein Terminalfenster und wechselt in den Root-Modus (***** steht für das Rootpasswort):

```
su  
*****
```

Dann startet man das Menü:

```
menu . sh
```

Nun kann man die Konfiguration des LA-Servers starten. Man beginnt mit der Netzwerkkonfiguration und muss anschließend alle benötigten Dienste starten. Eine genaue Beschreibung folgt in den nächsten Abschnitten.

3. Allgemeine Konfiguration

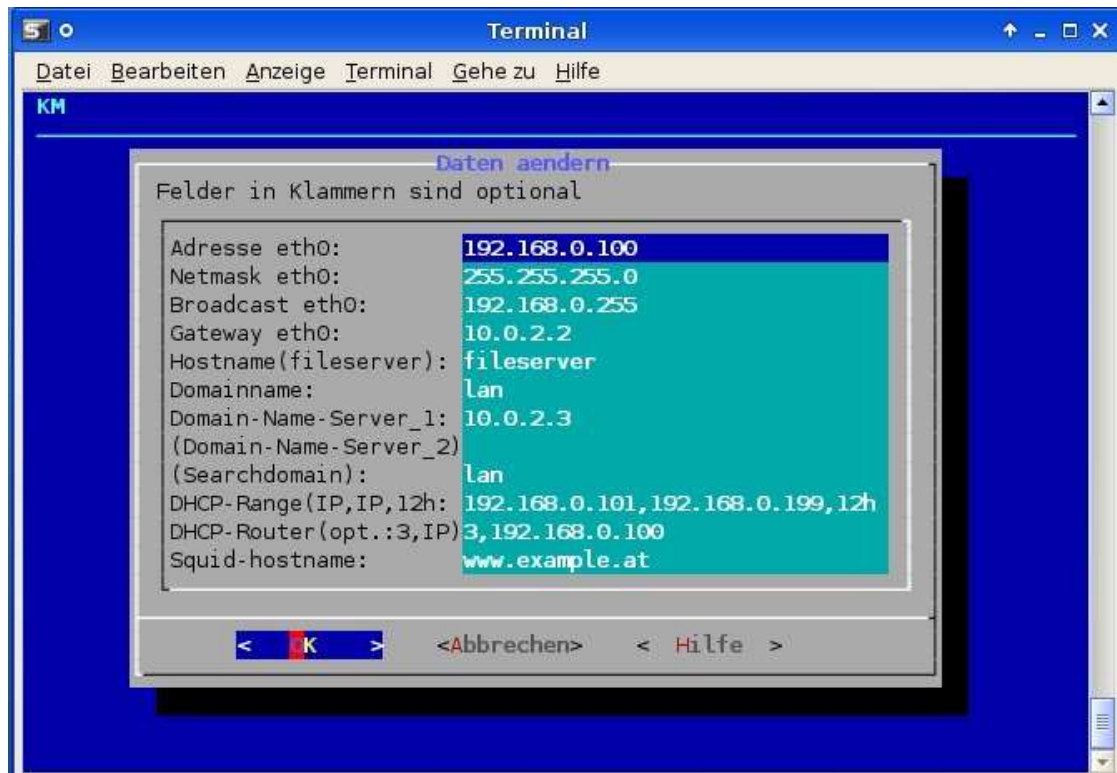


Abbildung 2: Netzwerkkartenkonfiguration

Das folgende Listing zeigt die Manualpage zum Skript: netconfig.sh

```
NAME          netconfig.sh — Erstellt alle Netzwerkgrundkonfigurationen.
DESCRIPTION   Beispiel-Konfiguration:
               Adresse eth0: 192.168.0.100
               Netmask eth0: 255.255.255.0
               Broadcast eth0:192.168.0.255
               Gateway eth0: 192.168.0.1 (<-IP Nummer deines Gateways)
               Hostname  : fileserver (<- muss fileserver lauten !!!)
               DNS1     : 192.168.0.100 (<- fileserver ist auch DNS Server)
               DNS2     : xxx.xxx.xxx.xxx (<- IP des DNS deines Providers)
               Searchdomain: schule (<- Deine locale domain)
               DHCP-Range  : 192.168.0.101,192.168.0.199 (<- Adressbereich
               fuer dynamische Adressenvergabe)
               Squid-hostname: www.schule.at (<- beliebiger Name waelhbar fur
               den eigenen Proxyserver)
AUTOR         script erstellt von KM          Dies ist freie Software (GPL)
version 0.1   December 2007                  netconfig.sh(1)
```

Das Skript bearbeitet schließlich die folgenden Dateien:

- `/etc/network/interfaces` # Netzwerkkonfiguration
- `/etc/hostname` # Name des Servers
- `/etc/hosts` # IP Adresse und Name des Servers

- `/etc/dnsmasq` # Konfigurationsdatei für den DNS- und DHCP-Server
- `/etc/resolv.conf` # Routingtabelle für den Server
- `/etc/mysql/my.conf` # Einstellungen für den MySQL-Server

Versierte Anwender können natürlich auch manuell diese Dateien verändern.

3.1.2. DHCP und DNS mit dnsmasq

Der *dnsmasq*-Dämon ist ein Dienst, der einen relativ einfach konfigurierbaren DHCP- und lokalen DNS-Server zur Verfügung stellt. Er ist viel einfacher zu konfigurieren, als der bekannte *bind*-Dämon. Für kleine bis mittlere Netzwerke ist der *dnsmasq*-Dämon sehr funktionell und gut einsetzbar. Die Konfigurationsdatei findet man unter `/etc/dnsmasq.conf`. Das Skript `/server/netconfig.sh`, welches man unter dem Menüpunkt Grundkonfiguration/Netzwerkkonfiguration aufrufen kann, erstellt bereits die wichtigsten Einträge in dieser Konfigurationsdatei.

Eine besondere Bedeutung haben die Dateien `/etc/ethers` und `/etc/hosts` für den *dnsmasq*-Dämon. Beide Dateien zusammen steuern eine feste Bindung zwischen MAC-Adressen und IP-Adressen bzw. IP-Adressen und Hostnamen. Diese beiden Dateien werden durch das Skript `/server/mysql_webkontrolle.sh` aus den Daten der MySQL-Datenbank neu erzeugt. In der MySQL-Datenbank werden die Client-MAC-Adressen gespeichert und eine Beziehung zwischen MAC-Adresse und IP-Adresse und Client-Name hergestellt. Ein manueller Eingriff in die `/etc/ethers` bzw. `/etc/hosts` Datei ist deshalb nicht sinnvoll.

Standardmäßig übergibt der *dnsmasq*-Dämon an die Clients das Gateway und die DNS-Konfiguration des Hostsystems. Will man spezielle Funktionen übergeben, so muss man die Datei `/etc/dnsmasq` manuell editieren. Alle relevanten DNS-Funktionen kann man sich in einer Konsole durch den Befehl `dnsmasq -dhcp-help` anzeigen lassen.

Beispieldatei `/etc/dnsmasq.conf`:

```
expand-hosts
domain=schule
dhcp-range=192.168.0.101,192.168.0.199,12h
read-ethers
#dhcp-option=3,192.168.0.100 # spezieller DNS Eintrag, normalerweise nicht notwendig
```

Beispielkonfiguration der `/etc/hosts`:

```
127.0.0.1 localhost # The following lines are
desirable for IPv6 capable hosts # (added automatically
by netbase upgrade) ::1 ip6-localhost ip6-
loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
192.168.0.100 fileserv fileserv.schule
192.168.0.101 pc01
192.168.0.102 pc02
```

Beispieldatei `/etc/ethers`:

3. Allgemeine Konfiguration

```
00:17:a4:eb:27:fe 192.168.0.101  
00:38:a5:ec:38:ab 192.168.0.102
```

3.2. Dienste Starten

Der Menüpunkt Dienste starten _stoppen ermöglicht es in einfacher Form, notwendige Dienste einmal zu starten oder zu stoppen. Es wird aber kein automatischer Start beim Hochfahren eingetragen. Hierfür ist der Menüpunkt Dienste _automatisch _starten vorgesehen. Nach der Installation sind die meisten Dienste noch nicht gestartet. Man sollte also nun genau überlegen, welche Dienste man auf dem Server benötigt. Man kann auch manche Dienste auf verschiedenen Maschinen laufen lassen. Besonders gut geeignet ist es, den Web- und E-Mail-Server vom Daten- und File-Server zu trennen. Anfänger sollten aber lieber mit einem Server arbeiten, denn die Konfiguration ist so einfacher. Notwendige Skripte:

- `mysql_dienste_staten_stoppen.sh`

- `mysql_dienste_automatisch_starten_stoppen.sh`

3.3. Firewall

Der Menüpunkt Firewall liefert die Möglichkeit, eine einfache Firewall einzuschalten und zu steuern. Man kann mit dem Menüpunkt Firewall _Befehl _eingeben auch direkt einen Firewall-Befehl eingeben. Die Arbeit leisten dahinter die `ufw` (Ubuntu-Firewall-Skripte). Die erste Spalte gibt die Portnummern an. Die zweite Spalte zeigt den Protokollnamen. Manche Protokolle können aber auch auf andere Ports umgelegt werden! Es wird aber empfohlen, zwischen dem ADSL-Router und dem LA-Server eine eigene Firewall einzurichten. Nach der Installation ist die Firewall zu nächst nicht aktiv! Anfänger sollten die Firewall erst zum Schluss aktivieren, da man dann sicher gehen kann, dass bei Problemen nicht eventuell die Firewall einen Dienst blockiert. Die Firewall lässt sich in einem Terminalfenster mit Root-Rechten durch den Befehl `ufw disable` stoppen. Alle Firewall-Einstellungen werden unter `/etc/ufw/*` gespeichert. Spezielle Anweisungen kann man dort auch direkt eintragen (nur für Fortgeschrittene!!).

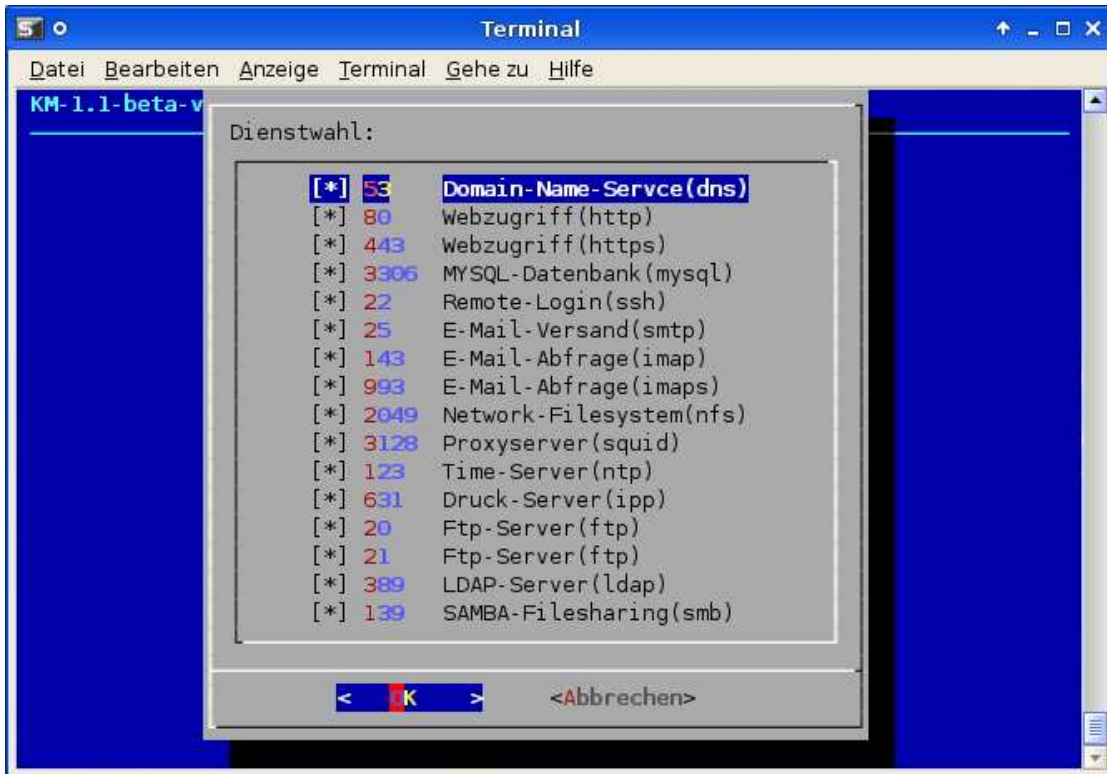


Abbildung 3: Firewall Einstellungen

3.4. Internet-Filter

Unter dem Menüpunkt `Web-Filterliste_konfigurieren` kann man festlegen, welche Listen für die Internetfilterung herangezogen werden sollen. Dieser Dienst beruht auf den Programmen Squid und SquidGuard. Die Listen werden unter `/var/lib/squidguard/db` gespeichert. Man kann aktuelle Listen immer wieder vom Internet beziehen. Man wird aber nie alle ungewollten Seiten sperren können!

Mit dem Menüpunkt `Single-Domain_sperren_öffnen` kann man auch ganz bestimmte Domänen sperren oder freischalten. Fortgeschrittene User können natürlich auch direkt die Datenbank `/var/lib/SquidGuard/db/*` und die Datei `/etc/squid/squidGuard.conf` bearbeiten. Man sollte dann aber die Skripte nicht mehr verwenden, da sonst die Einstellungen in diesen Konfigurationsdateien wieder überschrieben werden.

3. Allgemeine Konfiguration

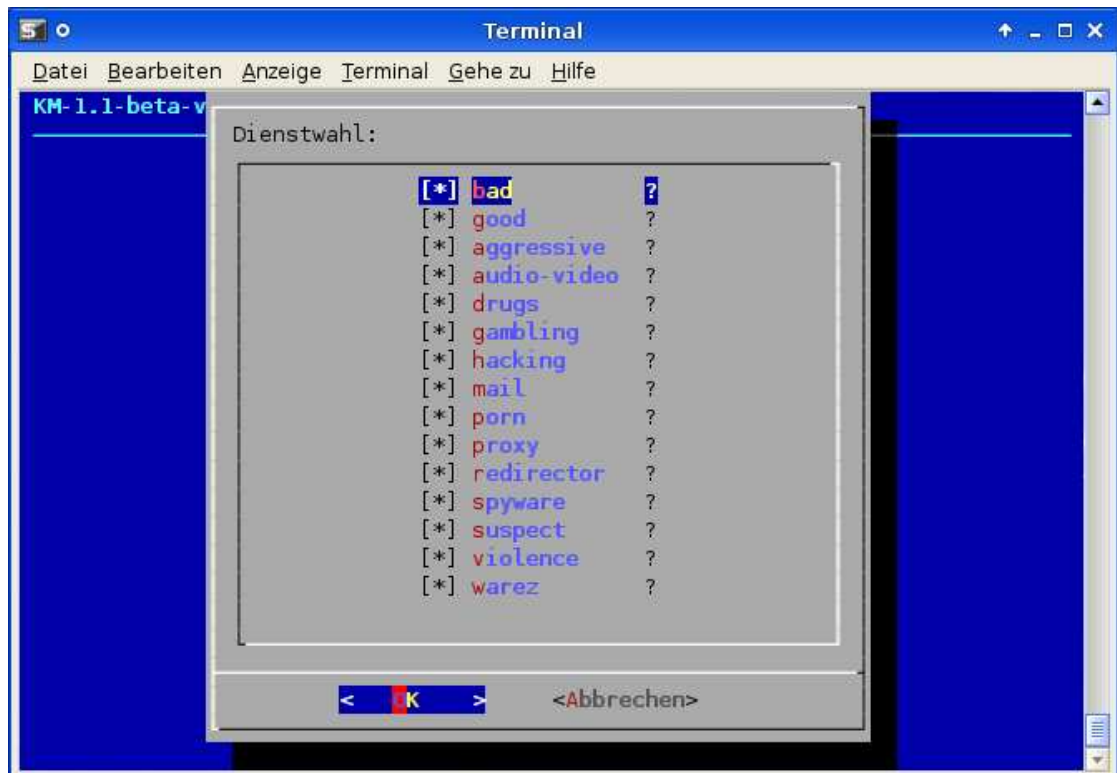


Abbildung 4: Web-Filter

3.5. DATENBANK-NEU-ANLEGEN

Der Menüpunkt `DATENBANK_KOMPLETT_NEU_ANLEGEN` ist mit großer Vorsicht zu verwenden. Es werden die MySQL- und die LDAP-Datenbank irreversibel gelöscht und eine komplett neue Datenbank angelegt. Dieser Menüpunkt sollte also nur dann verwendet werden, wenn man ganz bewusst einen LA-Server neu einrichten möchte. Nach der Installation ist die MySQL- und die LDAP-Datenbank schon initialisiert und man muss diesen Menüpunkt nicht verwenden.

3.6. Raum-Verwaltung

Um eine Web-Kontrolle sowie eine Remote-Client-Verwaltung durchführen zu können, müssen die Clients einem jeweiligen Raum zugeordnet werden. Weiters müssen dem LA-Server die MAC-Adressen der Clients bekannt sein. Um dies zu erreichen muss zunächst eine Raumstruktur angelegt werden. Unter dem Menüpunkt Remote-Client-Admin findet man die notwendigen Skripte. Die Skripte

- `raum_anlegen.sh`
- `raum_anzeigen.sh`

4. File- und Account-Server

raum_name diesen erneut korrekt in die Tabelle eintragen. Dieser Vorgang ist also immer notwendig, wenn ein Client von einem Raum in einen anderen umgesiedelt wird.

Nach Änderungen in der Raumstruktur, Eintragung oder Löschung von Clients muss der Menüpunkt *Raum_Client_aktualisieren* aufgerufen werden. Erst dann werden aus der MySQL-Datenbank die neuen Einstellungen für den DHCP und DNS Dienst übernommen.

4. File- und Account-Server

4.1. User-Verwaltung

Die User-Verwaltung ist eine der zentralen Schnittstellen des LA-Servers. Vorweg ist es ganz wichtig zu beachten, dass in Usernamen keine Sonderzeichen oder Umlaute verwendet werden dürfen. Auch das ß ist durch ss zu ersetzen. Eine Schule hat normalerweise eine große Anzahl von Schülern und Lehrern im System zu integrieren. Beim LA-Server werden standardmäßig drei verschiedene Usertypen verwaltet:

- *schueler*
- *lehrer*
- *admin*

Für die meisten Netzwerke genügt die Unterscheidung zwischen Schülern und Lehrern. Die konkreten Namen der drei verschiedenen Gruppen wird in der globalen Konfigurationsdatei */server/shells/globals.sh* gespeichert und kann eventuell dort auch geändert werden. Listing der Datei */server/shells/globals.sh*:

```
#!/bin/bash #globale variable
#mysql-datenbank-variable
gb_db="nss_mysql"
gb_mysqlpassword="schule "
gb_mysqlroot="root "
gb_mysqlnsspassword="schule"
gb_mysqlshadow="schuleadmin "
gb_shell="/bin/bash"
gb_homedir="/home"
gb_min_uid="5000"
gb_min_gid="5000"
#standard gruppen
gb_group_anzahl="15"
gb_group1="disk:6"
gb_group2="lp:7"
gb_group3="dialout:20"
gb_group4="voice:22"
gb_group5="cdrom:24"
gb_group6="floppy:25"
gb_group7="audio:29"
gb_group8="dip:30"
gb_group9="video:44"
gb_group10="plugdev:46"
gb_group11="games:60"
gb_group12="lpadmin:109"
gb_group13="saned:113"
```

4.1. User-Verwaltung

```
gb_group14="fuse:117"
gb_group15="vboxusers:115"

# dialog
gb_dia="dialog"
gb_author="—backtitle KM-1.0-beta-version"
#vorgabegruppen
gb_gruppe1="schueler"
gb_gruppe2="lehrer"
gb_gruppe3="admin"
gb_klasse="schueler"
gb_vererbung="true" # true or false : admin gehoert auch lehrer und schueler an, lehrer auch schueler # k
gb_klassensuche='[1-9][a-z][1-9]?$'
#installverzeichnis f(ull path) gb_dir=/server
# deleteng users gb_homedir_delete="true" # true or false
# in-out-system
gruppenverz="in-out"
eingang="IN"  ausgang="OUT"
```

Die gesamte User-Verwaltung wird durch die Skripte

- *mysql_add_user.sh*
- *mysql_del_user.sh*
- *mysql_add_group.sh*
- *mysql_del_group.sh*
- *mysql_change_primarygoup.sh*
- *mysql_add_to_group.sh*
- *mysql_del_from_group.sh*

verwaltet.

Man ruft diese Skripte wieder aus dem Hauptmenü auf.

test4 , passwort3 , schueler , 2 a

Alle Gruppennamen insbesondere die Klassennamen müssen schon vorher angelegt werden. Das Skript gibt keine Fehlermeldung aus, wenn eine Klasse oder Gruppe nicht existiert.

Das Skript legt zunächst alle User, die in der MySQL-Datenbank nicht vorkommen, an. User, die bereits vorhanden sind, werden nur auf ihre Klassenzugehörigkeit überprüft und eventuell korrigiert. Alle Schüler, die in der CSV-Datei nicht vorhanden sind, aber in der Datenbank schon, werden zum Löschen vorgeschlagen. Es handelt sich normalerweise um Schüler, die die Schule verlassen haben und deshalb aus der Datenbank gelöscht werden. Man kann jedoch gewisse Schüler auch von der Löschung ausschließen, wenn einzelne Schüler doch noch an der Schule angemeldet sind. Wenn Lehrer nicht mehr an der Schule sind, müssen diese jedoch manuell aus der Datenbank gelöscht werden. Dies kann man mit dem Menüeintrag "User löschen" durchführen.

Es ist also mit diesem Skript möglich, aus der Schüstadatenbank zunächst eine CSV-Datei zu exportieren, diese mit Passwörtern zu versehen und in die User-Datenbank einzuspielen. Bereits existierende User werden automatisch der richtigen Klasse wieder zugewiesen. Somit kann die Userdatenbank relativ einfach am aktuellen Schülerstand gehalten werden.

4.2. Userprofil-Verwaltung

Ein wichtiger Punkt ist die zentrale Profile-Verwaltung. Man möchte jedem User ein bestimmtes Profil zuweisen. Die einfachste Lösung ist es, zunächst einen typischen User anzulegen und alle notwendigen Profileinstellungen durchzuführen. Danach kann man dieses Profil als Vorgabeprofil definieren und dann für eine bestimmte Gruppe (schueler, lehrer, oder admin) anwenden. Diese Aufgaben können mittels der Skripte

- *mysql_profile_vorgabe.sh*

- *mysql_profile_anwenden.sh*

durchgeführt werden.

Das Skript *mysql_profile_anwenden.sh* zeigt alle User einer ausgewählten Gruppe an. Man kann nun noch einzelne User von der Profilübertragung ausschließen.

4. File- und Account-Server

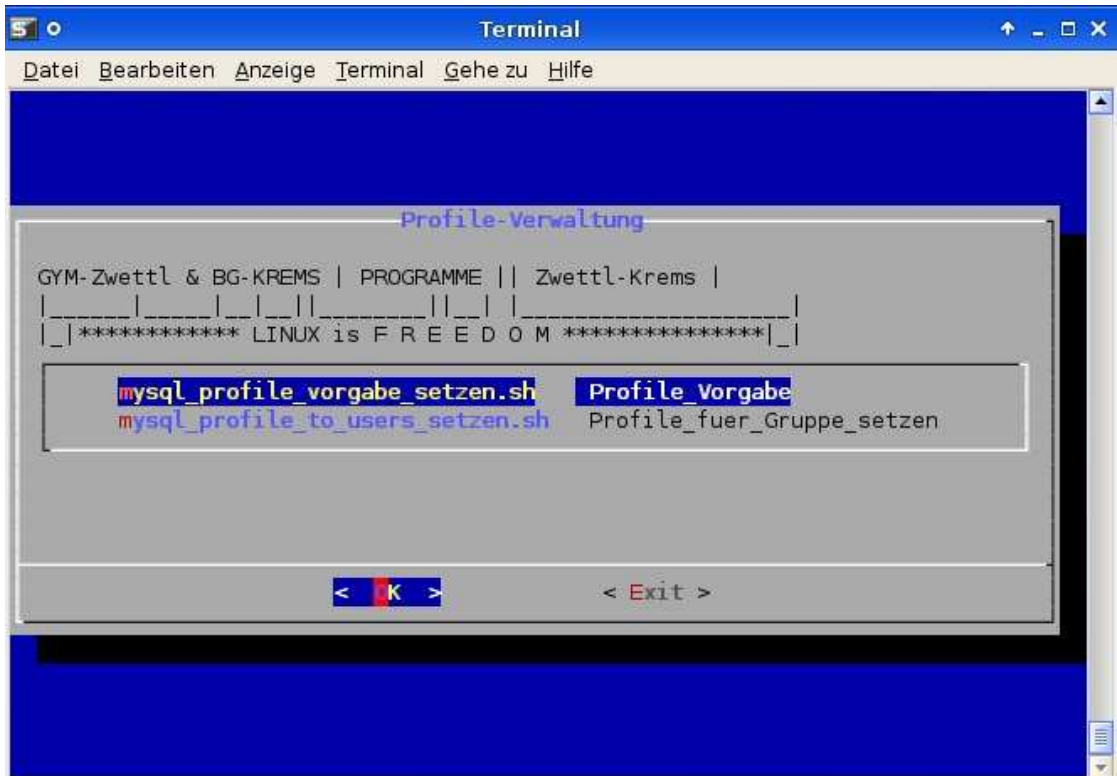


Abbildung 7: Profile-Verwaltung

Tipp: Die Einstellungen für den Webbrowser bzw. den E-Mail-Client werden in der Datei `/home/user_name/.mozilla` bzw. `/home/user_name/.mozilla-thunderbird` gespeichert. Will man diese nicht bei den Usern überschreiben, dann sollte man diese, bevor man das Profil auf andere User überträgt, im Verzeichnis `/etc/skel` löschen.

4.3. Web-Kontrolle

Im täglichen Unterricht ist es immer wieder angenehm, den Internetzugang für bestimmte Phasen des Unterrichts zu sperren bzw. wieder frei zu schalten. Diese Aufgabe kann mit dem LA-Server durchgeführt werden. Voraussetzung ist eine richtig angelegte Raumstruktur und eine Anmeldung aller Clients am LA-Server. Mit Hilfe der Skripte

- `mysql_web_anzeige.sh`
- `mysql_web_kontrolle.sh`
- `mysql_web_aktualisierung.sh`

kann man diese Aufgaben erledigen.

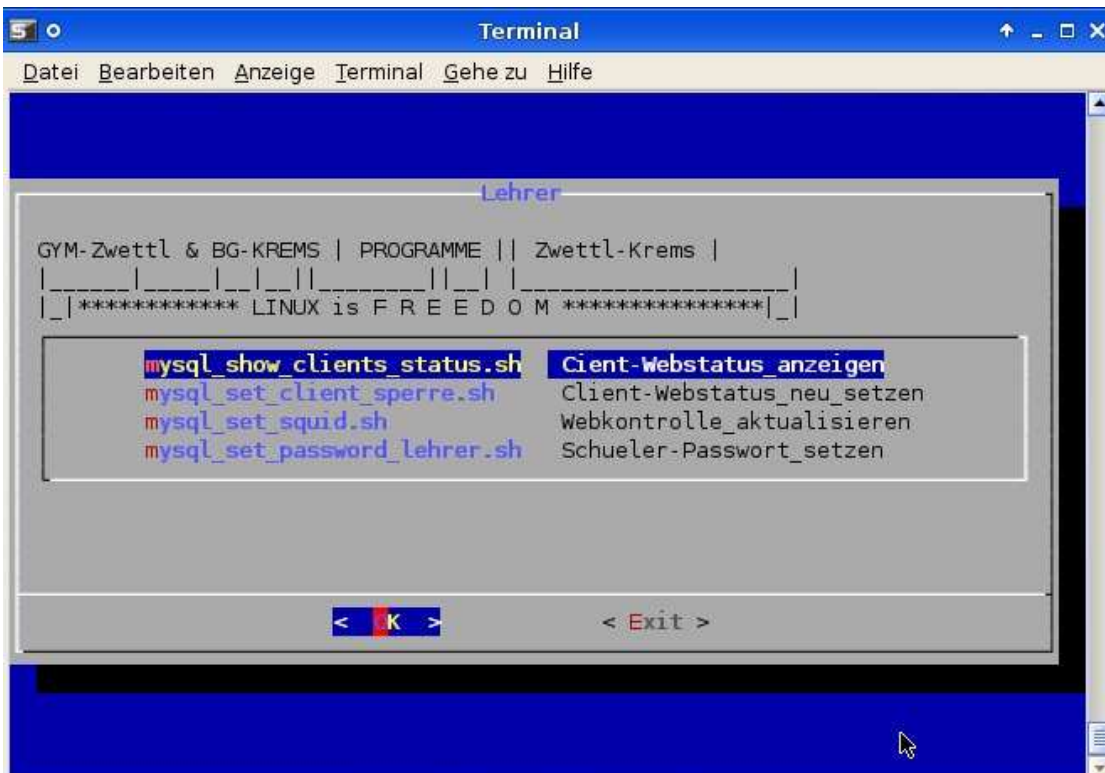


Abbildung 8: Web-Kontrolle

Jeder Lehrer kann sich mit dem Befehl `ssh fileserver` in einem Terminal auf den LA-Server verbinden und dann dort auf dem Server den Befehl `menu.sh` eingeben. Nun erhält der Lehrer die Möglichkeit die Web-Kontrolle zu steuern. Wichtig ist, dass nach Änderung der Web-Kontrolle der Menüpunkt `Webkontrolle_aktualisieren` ausgeführt wird. Erst dann werden die neuen Einstellungen wirksam. Es wird mit dem zuletzt aufgerufenem Befehl der Proxy neu konfiguriert damit dieser die neuen, aktuellen Daten aus der MySQL-Datenbank erhält.

Die Web-Kontrolle basiert natürlich auf einem vorkonfigurierten Proxy-Server (= `squid`). Alle Webanfragen auf dem Port 80 sollte man für die Clients sperren. Der Port 3128 muss freigegeben werden. Der Squid lauscht auf diesem Port und kann dann die Anfrage weiterleiten oder auch sperren. Die Clients müssen also im Webbrowser einen Proxy einstellen, damit ein Internetzugang überhaupt möglich wird. Natürlich könnte man auch einen transparenten Proxy einrichten, aber manche Internetseiten würden dann nicht funktionieren, insbesondere gibt es Probleme bei https-Seiten. In der Konfiguration des squid genügt der Eintrag `http_port 3128 transparent` (siehe `/etc/squid/squid.conf`). Die automatische Umleitung müsste man in den Firewall-Regeln aktivieren (`etc/ufw/*`).

4. File- und Account-Server

4.4. Zentrale Client-Verwaltung

Ein ganz wichtiger Punkt ist die zentrale Client-Verwaltung im Schulnetz. Damit diese klappt muss nach der Installation eines Clients noch einmal manuell Hand angelegt werden. Die Grundidee basiert auf einem passwortlosen ssh login des Root-Users vom Server auf die Clients.

Folgendes muss man aber zunächst für diesen Vorgang einmalig auf jedem Client nach der Clientinstallation durchführen.

```
su
*****
rm -r /root/.ssh
ln -s /scripts/.ssh/ /root/.ssh
```

Obige Befehle löschen auf dem Client das .ssh Verzeichnis des Root-Users. Danach wird eine Verknüpfung auf das vom LA-Server freigegebene Verzeichnis scripts/.ssh eingerichtet. Dieses kann nur vom Root gelesen werden. In einem nächsten Schritt erzeugt man nun ein Public/Private-Key Paar und kopiert den Public-Key an die richtige Stelle: Folgenden Befehl führt man wieder am LA-Server im Rootmodus aus:

```
ssh-keygen
```

Die Passwortabfrage lässt man leer und somit wird ein passwortloses Keypair geschaffen. Dieses wird durch ausschließliche Leserechte für den Root-User geschützt. Der Public-Key wird nun in *authorized_keys* im Verzeichnis */scripts/.ssh* kopiert.

```
cat /root/id_rsa.pub >>/scripts/.ssh/authorized_keys
```

Nun ist damit der Public-Key allen Root-Usern auf den Clients bekannt. Nun kann sich der Root-User vom LA-Server passwortlos auf den Clients mit ssh anmelden.

Alle Skripte zur Remote-Verwaltung der Clients basieren auf dieser Vorarbeit.

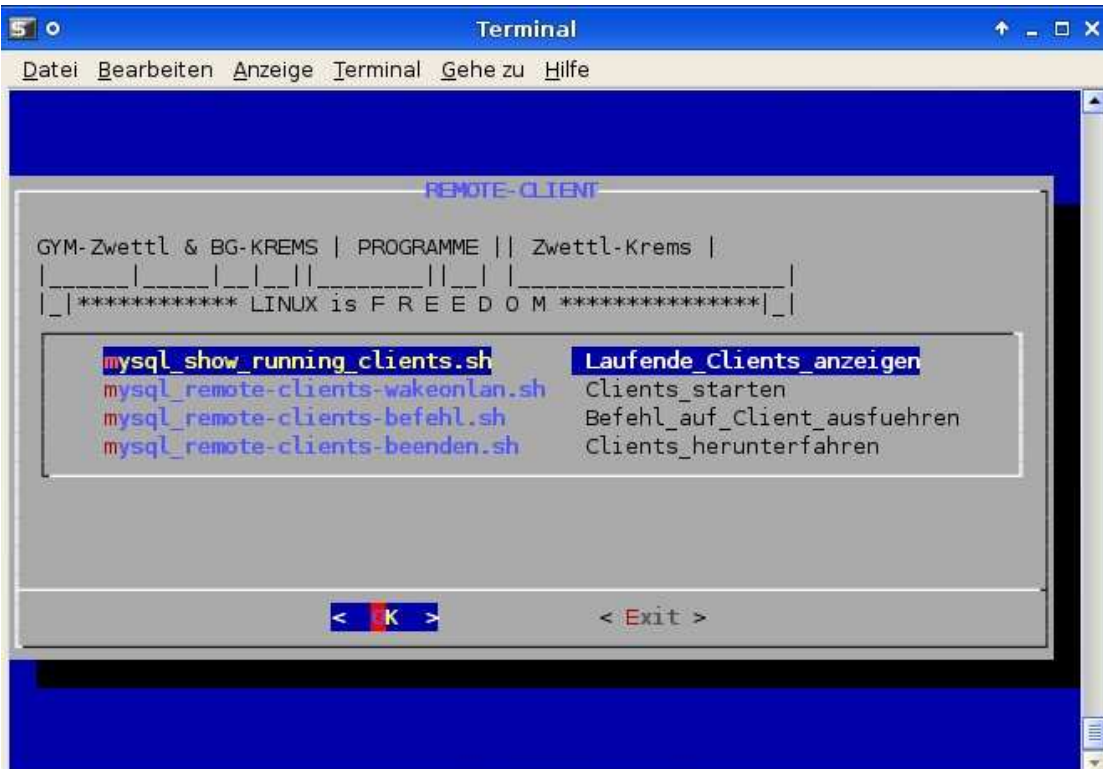


Abbildung 9: Remote-Client-Verwaltung

4.4.1. Synchronisation der Clients

Es ist auch relativ einfach Clients zu synchronisieren. Auf einem Client führt man folgenden Befehl aus:

```
su
*****
rsync -avH --delete / root@client_name:/ --exclude=/proc --exclude=/sys --exclude=
```

Mit dem rsync-Befehl wird der eigene Client als Quelle verwendet und der Client mit dem "client_name" als Ziel mit dem eigenen Client synchronisiert. Die Verzeichnisse /proc, /sys und /tmp werden immer ausgeschlossen. Die Verzeichnisse /scripts und /home sind Verzeichnisse am LA-Server und werden deshalb auch ausgeschlossen.

Diese Synchronisation geht sehr rasch und funktioniert bei gleicher Hardware der Clients. Ist die Hardware unterschiedlich, so muss man zusätzlich folgende Verzeichnisse und Dateien von der Synchronisation ausschließen: /etc/X11/xorg.conf, /etc/fstab, /boot/grub/menu.sh.

Will man die Synchronisation auf allen Rechnern automatisch durchführen, so muss man erreichen, dass jeder Root-User auf einem Client sich auch ohne Passwort auf einen anderen Client anmelden kann. Das ist natürlich ein gewisses Sicherheitsrisiko. Aber nur durch diese Maßnahme lässt sich eine einfache skriptgesteuerte Verwaltung der Clients durchführen.

Zur Vorbereitung führt man folgende Befehle auf einem Client aus:

5. E-Mail-Server

```
su
*****
ssh-keygen
```

Nun wird ein Private/Public-Key Paar auf einem Client erzeugt. Die Frage nach dem Passwort lässt man leer. Der Public-Key wird nun in die *authorized_keys* datei eingetragen:

```
cat /root/.ssh/id_rsa.pub >>/root/.ssh/authorized_keys
```

Da ja alle Clients bereits eine Verknüpfung von */root/.ssh* auf das gleiche Verzeichnis am LA-Server */scripts/.ssh/* haben, ist nun jedem Client der Publickey bekannt. Ab nun kann sich der Root-User von jedem Client auf einen beliebigen anderen Client passwortlos anmelden.

Am LA-Server kann man nun im Menü in die Remote-Client-Verwaltung wechseln und dort das Skript *Clients_synchronisieren* starten.

5. E-Mail-Server

5.1. Allgemeines

Der Betrieb eines eigenen E-Mail-Servers sollte gut überlegt sein. Oft ist es einfacher, diesen Dienst auszulagern. Der LA-Server bietet aber eine Möglichkeit, relativ einfach einen sicheren E-Mail-Server aufzubauen.

Der E-Mail-Server ist aus Sicherheitsgründen von den User-Accounts in der MySQL- bzw. LDAP-Datenbank völlig entkoppelt. Der E-Mail-Server kann auch auf einer eigenen Server-Maschine installiert werden.

Die Zugangsdaten werden in der Datei */etc/sasldb* gespeichert. Auf diese haben der MTA (cyrus2.2) und der SMTP (postfix) Zugriff. Zu den E-Mail-Accounts existiert somit kein gültiges Login und somit kann ein gehacktes Passwort eines E-Mail-Accounts keine Rechte am Server selbst erlangen. Nachteil dieser Struktur ist es, dass jeder E-Mail-Account extra unabhängig von den User-Accounts angelegt werden muss. Auch sollten sich die Namen der User-Accounts und E-Mail-Accounts nicht überschneiden, wenn der E-Mail-Server auf der gleichen Maschine wie der File-Server läuft. Die vorgefertigte Menüstruktur für die Verwaltung des E-Mail-Servers hilft aber beim Anlegen der E-Mail-Accounts. Diese können auch wieder durch ein Batchfile angelegt werden. Natürlich ist der E-Mail-Server auch mit einem SPAM- und Virenfiler ausgerüstet (amavis-new, clamav, clamav-freshclam, dspam, spam-learn).

5.2. Konfiguration

Alle notwendigen Aufgaben bei der Einrichtung des E-Mail-Servers findet man unter dem Menüeintrag EMAIL-Admin

5. E-Mail-Server

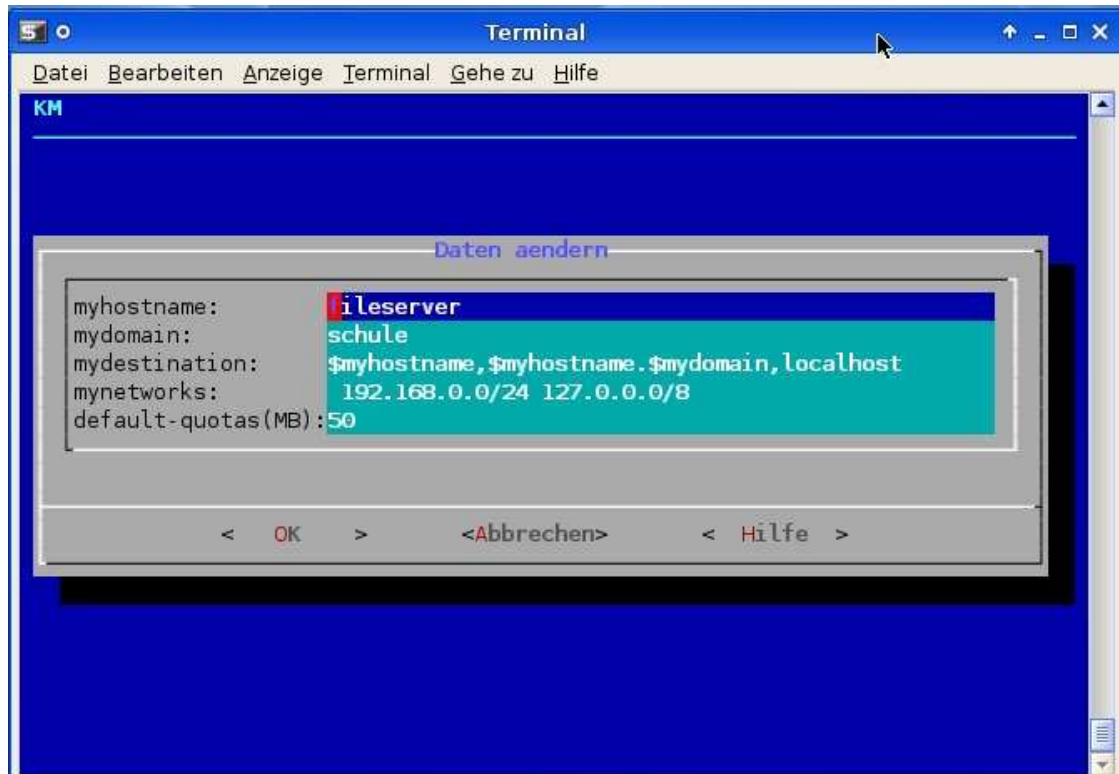


Abbildung 11: POSTFIX-Konfiguration

Im wesentlichen muss normalerweise nur der Servername und das Netzwerk eingestellt werden. Die anderen Parameter bleiben unverändert. Nach dem Betätigen der Einstellungen, zweigt das Skript den Inhalt der Konfigurationsdatei von postfix an (/etc/postfix/main). Der fortgeschrittene Admin kann natürlich diese Datei auch manuell bearbeiten.

5.3. SPAM- und Virentfilter

Ein E-Mail-Server ohne SPAM- und Virentfilter ist heutzutage nicht mehr sinnvoll. Der LA-Server verwendet hierzu die Pakete *amavis-new*, *clamav*, *clam-refresh* und *spam-learn*. Alle Dienste sind bereits vorkonfiguriert und müssen nur gestartet werden. Man kann aber auch insbesondere die SPAM-Einstellungen verändern. (/etc/amavis/conf.d/*).

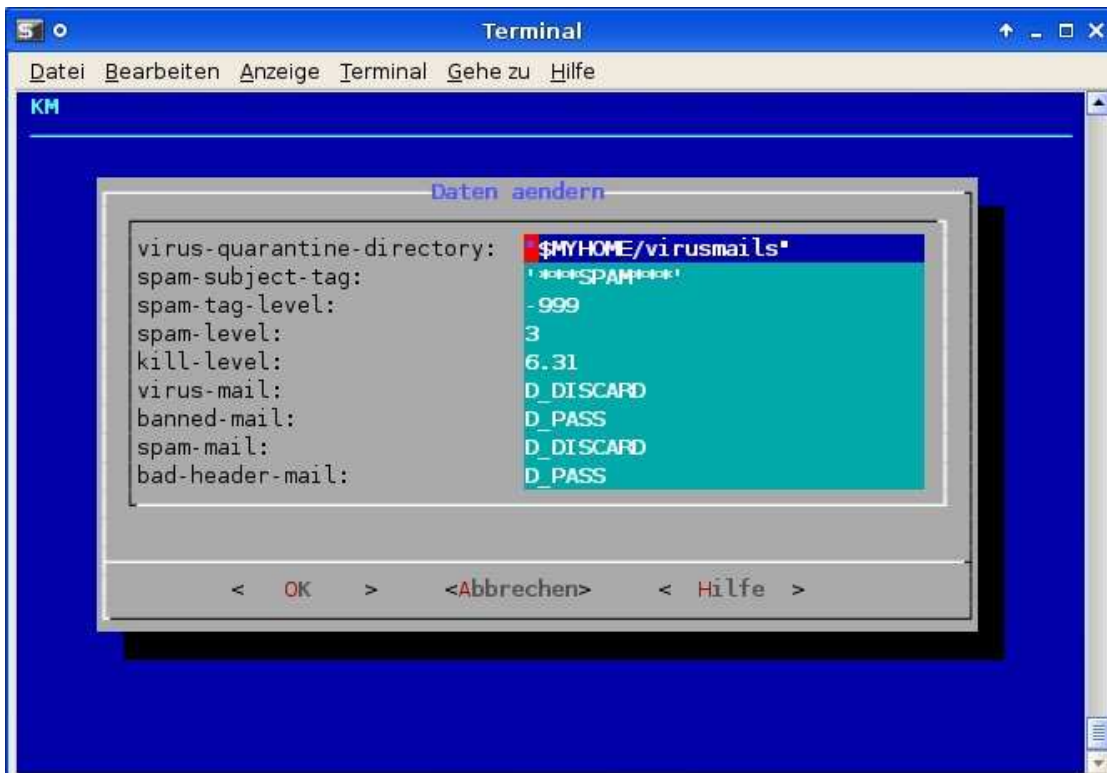


Abbildung 12: SPAM-Filter-Einstellungen

5.4. IMAPS und Certificaterstellung

Für die erhöhte Sicherheit ist eine verschlüsselte Verbindung zum E-Mail-Server zu empfehlen. Für Schulen ist meist ein offizielles Zertifikat nicht notwendig. Der LA-Server bietet eine einfache Möglichkeit, selbst eine eigene CA zu erzeugen und ein eigenes Schlüsselpaar damit selbst zu zertifizieren. Nun kann man mit diesem Schlüssel und mit dem Paket *stunnel4* sehr einfach eine IMAPS Verbindung aufbauen. Mit dem gleichen Schlüssel und dem Stunnelverfahren lässt sich auch eine HTTPS Verbindung einrichten. Das Skript erzeugt einen Schlüssel, der für 10 Jahre gültig ist. So braucht man nicht jedes Jahr wieder einen neuen Schlüssel konfigurieren. Nach der Erstellung des eigenen Schlüsselpaares muss nur noch der Dienst *stunnel* gestartet werden. Ab nun kann man *https* und *imaps* anbieten. In der Firewall sollte man dann *http* und *imap* sperren.

5. E-Mail-Server

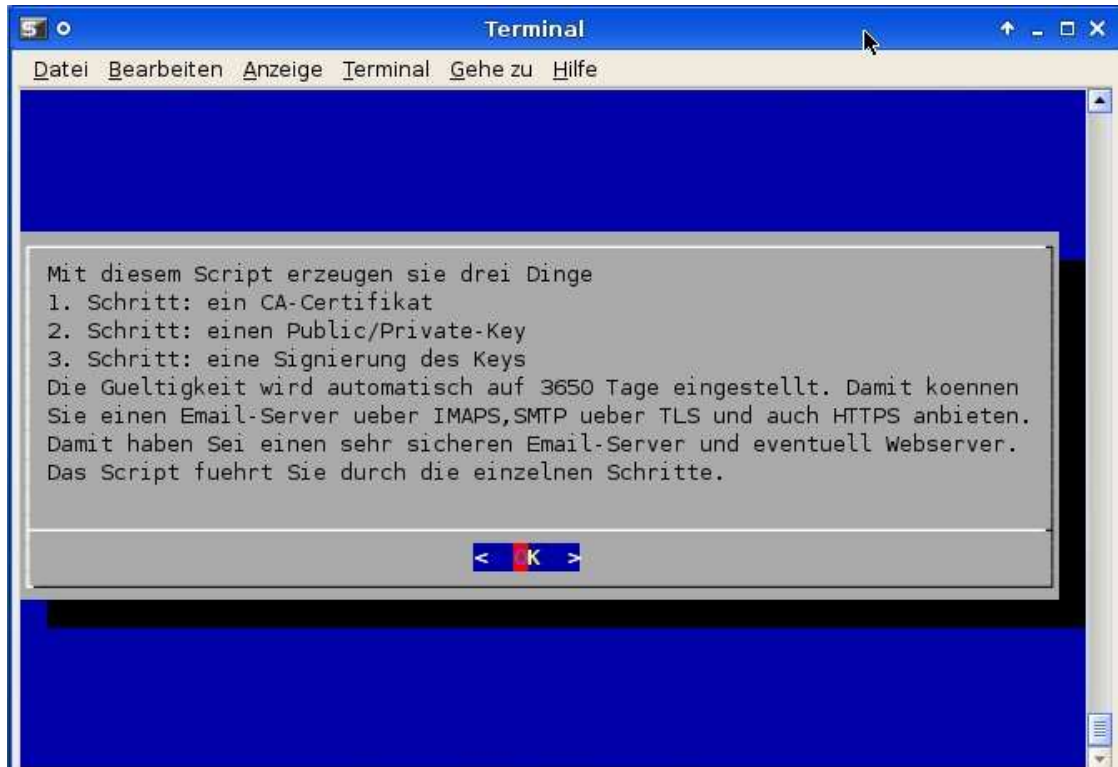


Abbildung 13: IMAPS, HTTPS, CA

5.5. E-Mail-Account-Verwaltung

Die E-Mail-Account-Verwaltung findet man ebenfalls im Menü E-Mail-Admin. Die Menüpunkte sind großteils selbsterklärend. Fortgeschrittene Admins können den E-Mail-Server auch als Groupware-Server ausbauen.

Literatur

- [1] H. Jurzik, "Debian, GNU/Linux; Das Praxisbuch", Galileo Press, 1. Auflage Bonn 2006
- [2] M. Gutmann, D. Lannert, "Linux im Netzwerk; Der Praxisleitfaden für kleine und mittlere Umgebungen", Addison-Wesley 2007
- [3] M. Kofler, "Ubuntu 6.06; Dapper Drake", Addison-Wesley 2006
- [4] R. Hattenhauer, "Linux-Livesysteme", Galileo Press, Bonn 2006
- [5] K. Deutsch, "Suse Linux; System und Anwendungen im Überblick", Nicolaus Millin, Erlangen 2005
- [6] K. Deutsch, "Linux für Windows-Administratoren", Francis, Lavis 2006
- [7] M. Kofler, "Linux; Installation, Konfiguration, Anwendungen", Addison-Wesley, 7. Auflage, München 2006
- [8] F. Ronneburg, "Debian GNU/Linux; Anwenderhandbuch für Einsteiger, Umsteiger und Fortgeschrittene", Addison-Wesley, München 2005
- [9] A. Niemann, "Knoppix; Linux ohne Risiken und Nebenwirkungen", moderne Industrie Buch, Landsberg 2004
- [10] H. Herold, "Linux/Unix-Grundlagenreferenz", Addison-Wesley, München 2004
- [11] F. Ayaz, D. Koch, "Linux-Intern konfigurieren und administrieren", DATA BECKER, Düsseldorf 2006
- [12] K. Sarnow, "Linux in der Schule", SUSE Press, Nürnberg 2000