

# FEDORA 16



**Linux-Mailserver als Basis für webbasierte Groupwarelösung**

Thomas Hürlimann  
thomas@netcult.ch

## Inhaltsverzeichnis

1	Einleitung .....	3
1.1	Warum .....	3
1.2	Beschreibung .....	3
1.3	Hardware .....	3
1.4	Applikationsübersicht .....	3
2	Fedora 16 .....	4
2.1	Download .....	4
2.2	OS Installation .....	4
2.2.1	Installationsablauf .....	4
2.2.2	Server - Pakete .....	7
2.2.3	Root-Benutzer für den GNOME Display Manager .....	9
2.2.4	Deaktivieren von SELinux .....	10
2.2.5	Deaktivieren der Firewall .....	10
2.2.6	Installieren von Webmin .....	10
2.2.7	Installieren von Usermin .....	10
2.2.8	Services permanent aktivieren .....	11
2.2.9	Mail Client und Linux Updates .....	11
3	Applikationen .....	12
3.1	Sendmail .....	12
3.2	Procmail .....	14
3.3	SpamAssassin .....	15
3.4	Dovecot .....	16
3.5	Mail - Funktionstests .....	19
3.6	MySQL .....	21
3.7	Horde Groupware Webmail Edition .....	21
4	Benutzerdaten Migration .....	29
4.1	Benutzerdaten Backup vom alten Mailserver .....	29
4.2	Benutzerdaten Restore auf neuen Mailserver .....	29
4.3	Backup und Restore von weiteren Services .....	29
5	Weitere Services .....	30
5.1.1	Samba Windows Fileserver .....	30
5.1.2	BIND9 DNS Server .....	30
5.1.3	Online Backup .....	32
5.1.3.1	Filesystem .....	32
5.1.3.2	MySQL Dump .....	32
5.1.3.3	Status Monitor .....	33
5.1.3.4	Crontab Jobs .....	34
6	Abschluss .....	34

# 1 Einleitung

## 1.1 Warum

Die Dokumentation ist an alle Personen gerichtet, die auf der Suche nach einem stabilen und wartungsfreundlichen Mailserver auf OpenSource Basis sind, der sich vom Funktionsumfang her nicht fürchten braucht, einfach zu sichern ist, sich unkompliziert in die bestene Landschaft integrieren lässt, jahrelangen stabilen Betrieb garantiert und sich obendrein im ISP Umfeld bereits bestätigt hat.

## 1.2 Beschreibung

In diesem Dokument wird beschrieben, wie ein Mailserver auf Fedora 16 Basis mit folgenden Funktionen installiert wird:

- Sendmail SMTP Mailverkehr mit TLS/SSL Unterstützung auf TCP Port 25
- Dovecot POP3 Mailverkehr mit TLS/SSL Unterstützung auf TCP Port 110 / 995
- Dovecot IMAP Mailverkehr mit TLS/SSL Unterstützung auf TCP Port 143
- Apache/Horde HTTP Webmail mit SSL Verschlüsselung auf TCP Port 80 / 443
- Webmin/Usermin zur Accountverwaltung
- Spamassassin/Procmail Mailfilter lokal installiert
- MySQL Datenbankserver lokal installiert
- Ggf. BIND9 DNS Server

## 1.3 Hardware

4GB RAM auf 100 User, schneller Intel XEON CPU (2.8 GHz/2MB oder schneller). 500 GB Mailpeicher auf 100 Benutzer sind sehr komfortabel. 1 Gbit/s Anschluss im LAN, möglichst schnell im WAN.

Hardware Compatibility List: <http://fedoraproject.org/wiki/HCL>

## 1.4 Applikationsübersicht

Software	Funktion	Download
Fedora 16, Kernel 3.1.2-1	Basisbetriebssystem	<a href="http://www.fedoraproject.org">www.fedoraproject.org</a>
Sendmail	MTA Server	Im Basissystem
Procmail	Regelbasiertes Mail Filtering	Im Basissystem
Spamassassin	Anti Spam Server	Im Basissystem
Dovecot	IMAP/POP/NNTP Server	Im Basissystem
MySQL	SQL Datenbank Server	Im Basissystem
Apache	HTTP Server	Im Basissystem
OpenSSL	SSL Zertifikate	Im Basissystem
Webmin/Usermin	Remote Management	<a href="http://www.webmin.com">www.webmin.com</a>
HORDE Groupware	Webmail	<a href="http://www.horde.org">www.horde.org</a>

## 2 Fedora 16

### 2.1 Download

Die Installation wird mit der 32bit Version von Fedora dokumentiert, die Downloads finden sie unter folgenden URLs:

x86: <http://download.fedoraproject.org/pub/fedora/linux/releases/16/Fedora/i386/iso/Fedora-16-i386-DVD.iso>

64bit: [http://download.fedoraproject.org/pub/fedora/linux/releases/16/Fedora/x86\\_64/iso/Fedora-16-x86\\_64-DVD.iso](http://download.fedoraproject.org/pub/fedora/linux/releases/16/Fedora/x86_64/iso/Fedora-16-x86_64-DVD.iso)

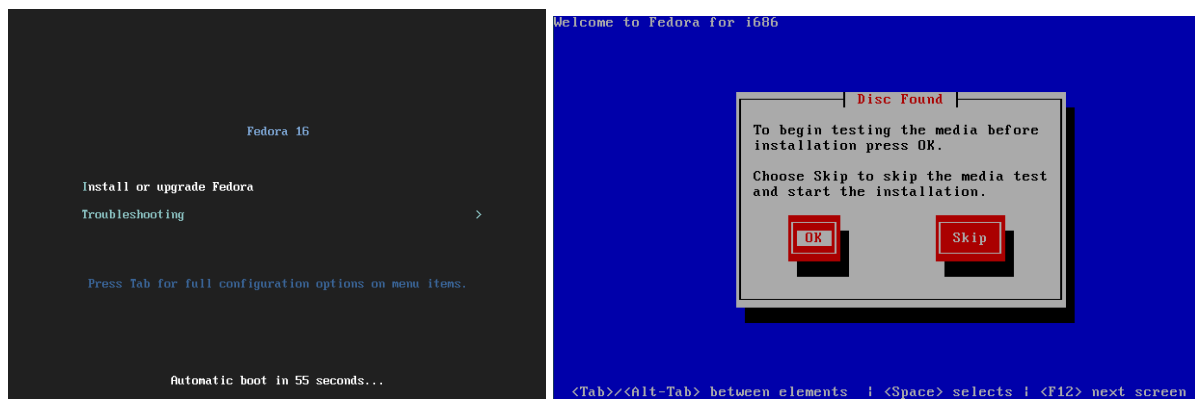
Die gesamte Fedora-Downloadübersicht finden Sie unter folgender URL:

OS: [http://fedoraproject.org/de\\_CH/get-fedora-all](http://fedoraproject.org/de_CH/get-fedora-all)

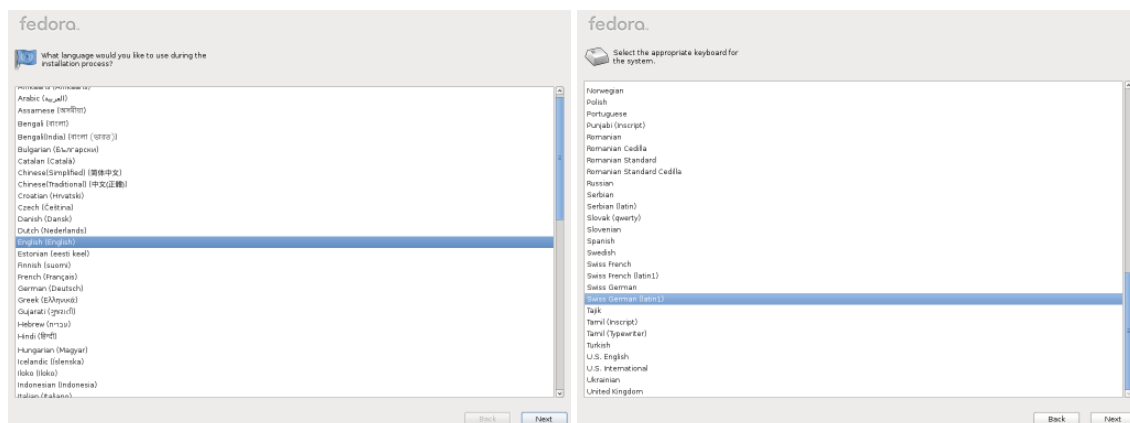
### 2.2 OS Installation

In meiner Dokumentation installiere ich das OS in einem virtuellen System unter Verwendung des VMWare Players 4.0.1. Das Installationsimage werde ich anschliessend auf einen VMWare Server kopieren und final starten.

#### 2.2.1 Installationsablauf



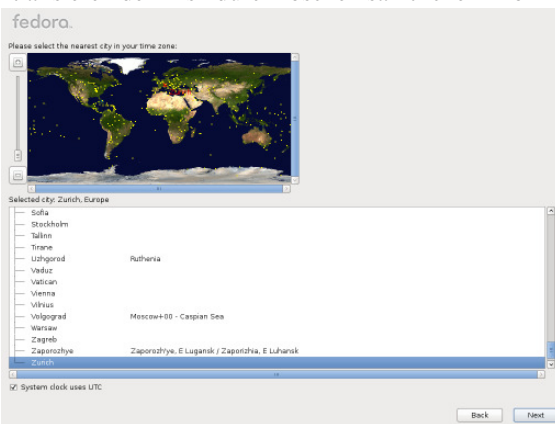
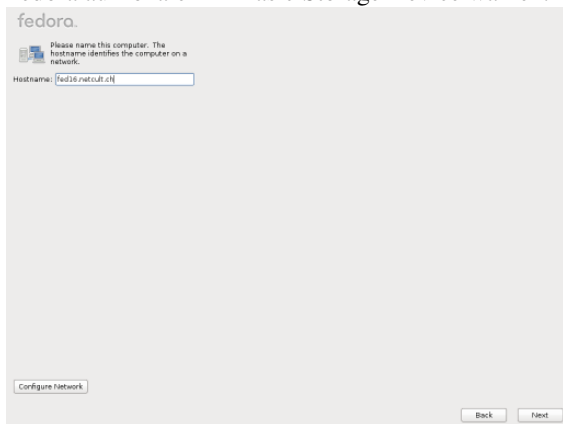
Starten Sie das System von DVD und wählen Sie *install or update Fedora*. Testen Sie das Installationsmedium auf Integrität.



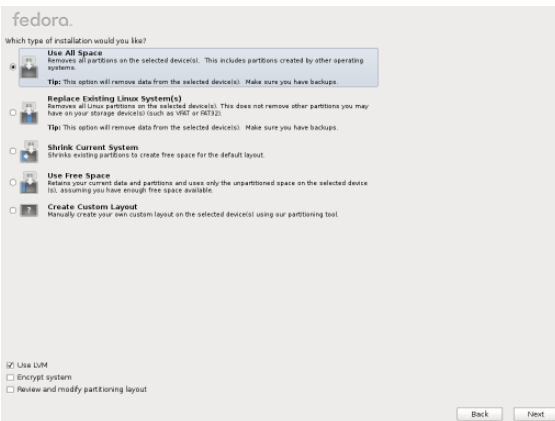
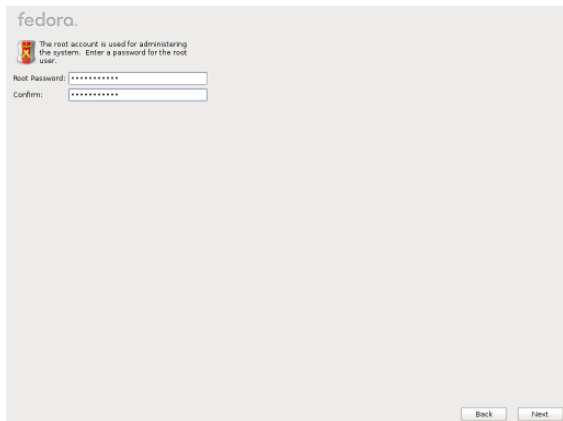
Als Installationsprache *English (english)*. Als Keyboard-Layout entsprechend passendes.



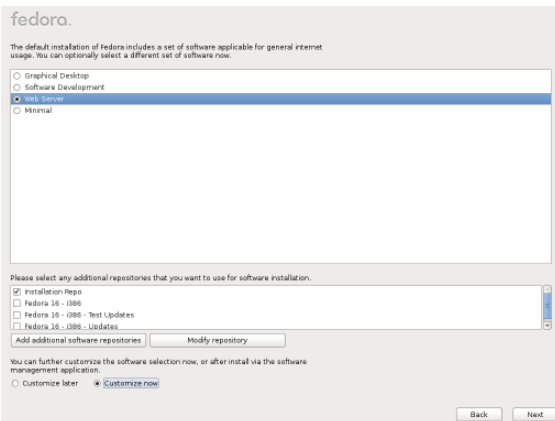
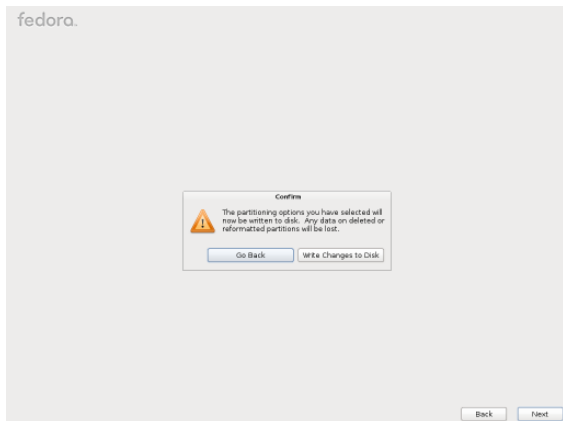
Fedora auf lokale HD Basic Storage Device wählen. Initialisieren der Disk durch löschen sämtlicher Informationen.



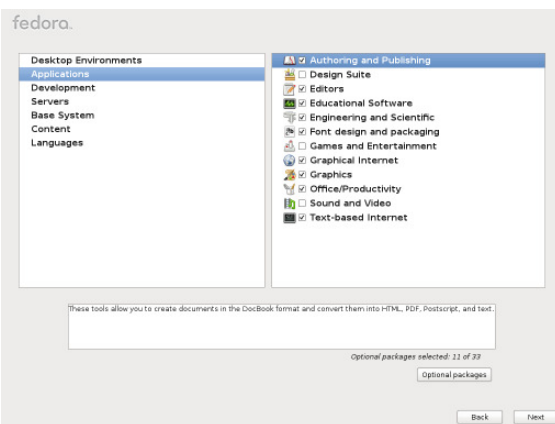
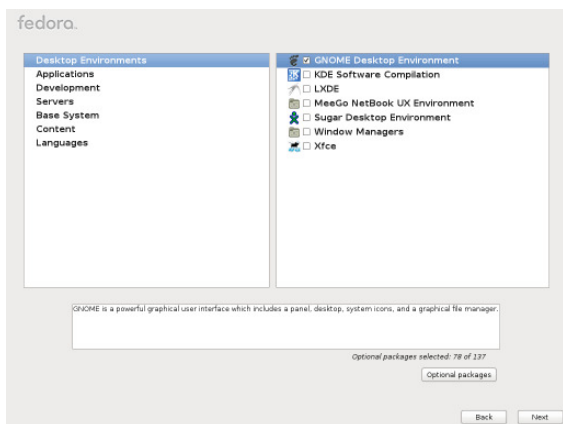
Setzen Sie Hostname und Zeitzone.



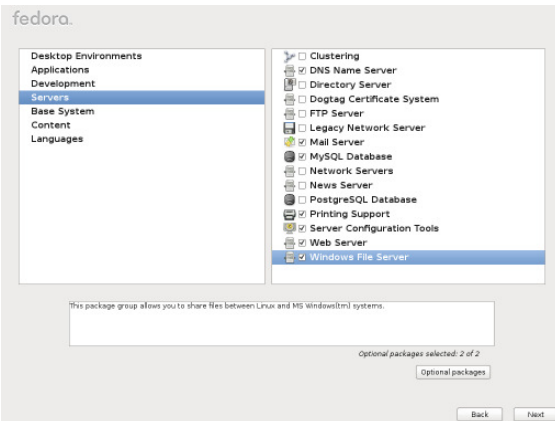
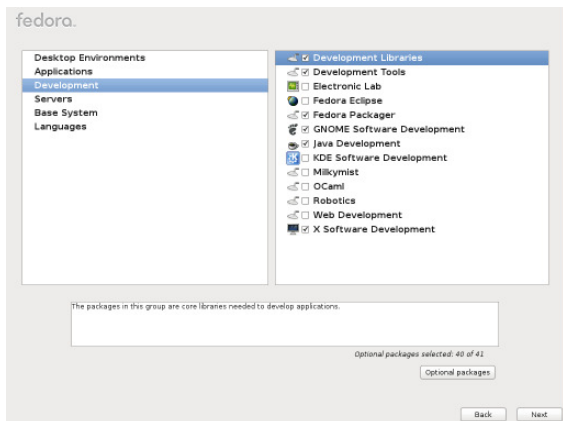
Setzen Sie ein Passwort für den Benutzer root. Nutzen Sie allen verfügbaren Speicherplatz für die Fedora Installation.



Dieser Schritt löscht sämtliche Daten auf der HD. Wählen Sie Webserver und wählen Sie *Customize now*.

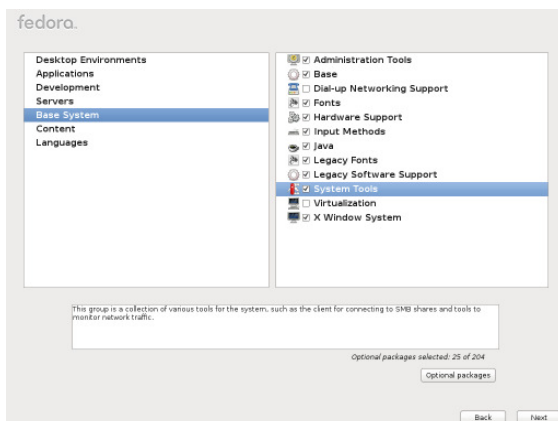
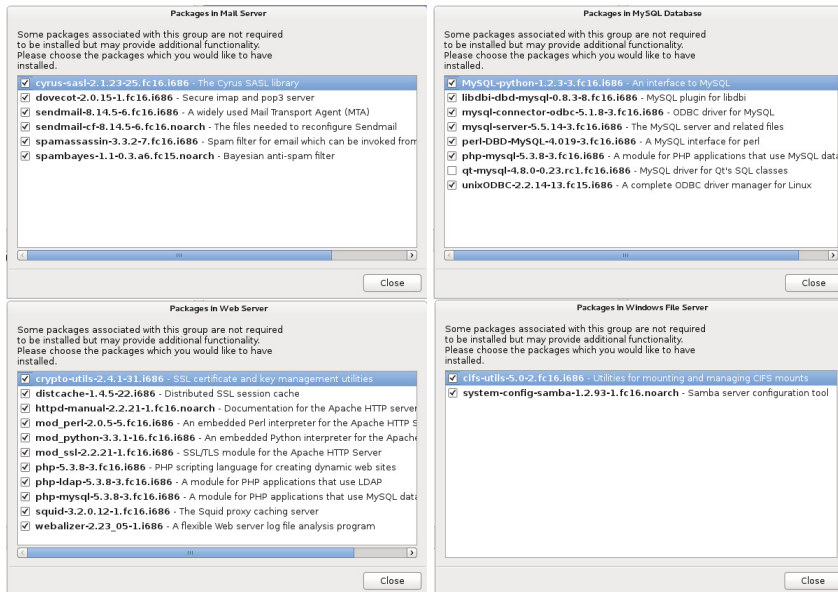


Wählen Sie Ihren bevorzugten Desktop. Wählen Sie bevorzugte Applikationen.

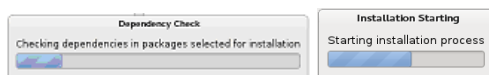


Wählen Sie gem. Abbildungen aus der Entwicklung an. Selektieren Sie *DNS Name Server*, *Mail Server*, *MySQL Database*, *Server Configuration Tools*, *Printing Support*, *Web Server* und *Windows Fileserver*.

## 2.2.2 Server - Pakete



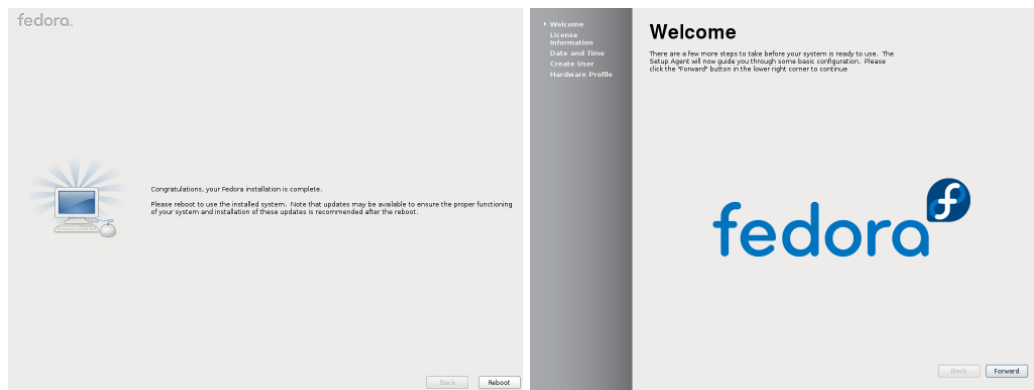
Installieren Sie die abgebildeten Komponenten vom Basis-System. Wenn erforderlich, wählen Sie weiteren Sprachsupport in der Gruppe *Languages*.



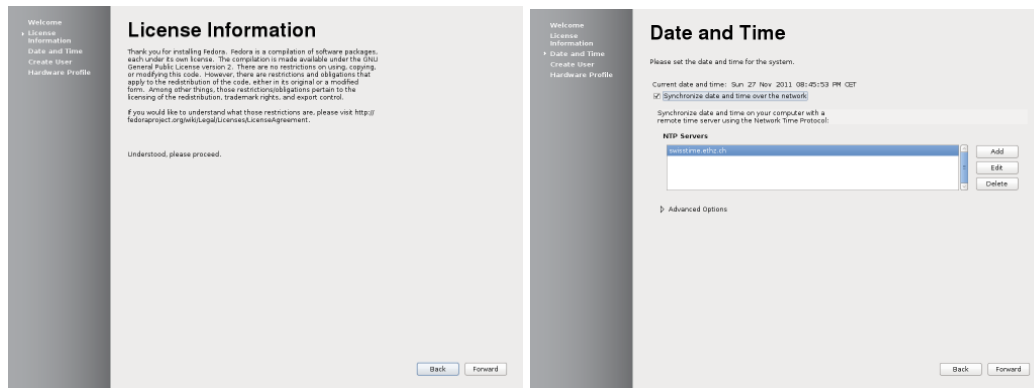
Abhängigkeiten werden geprüft.



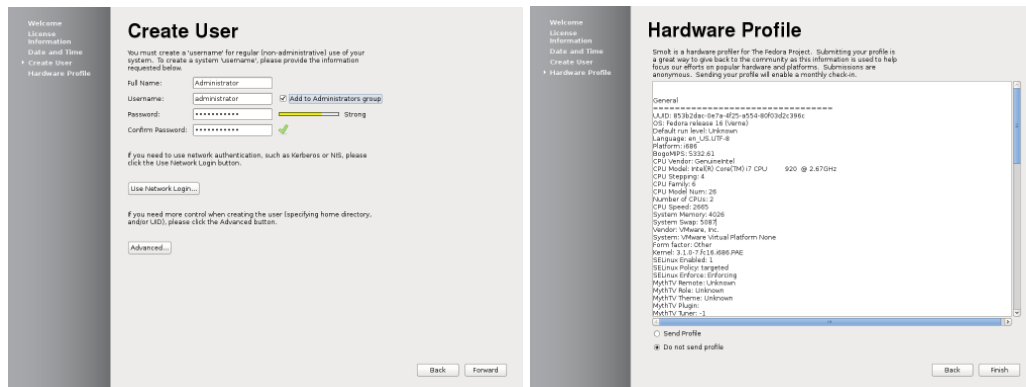
Installation beginnt.



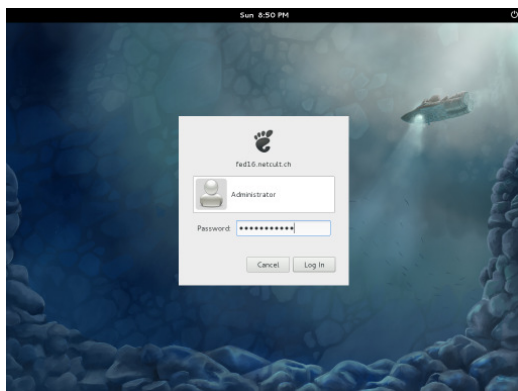
Zum Abschluss wird neu gestartet.



Verstehen Sie die Lizenzinformationen und nutzen Sie einen NTP Server.



Erstellen Sie einen Administrator und reichen Sie Ihr Profil nicht ein.



Melden Sie sich mit zuvor erstelltem Administrator an.

### 2.2.3 Root-Benutzer für den GNOME Display Manager

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Editieren Sie die Konfigurationsdatei:

```
su -c 'vi /etc/pam.d/gdm'
```

2. Finden Sie die Zeile mit folgendem Inhalt:

```
auth required pam_succeed_if.so user != root quiet
```

3. Kommentieren Sie die Zeile durch setzten des Prefix aus (#):

```
# auth required pam_succeed_if.so user != root quiet
```

4. Speichern Sie und schliessen Sie den Editor

Ab Fedora 11 muss ebenfalls die Datei `/etc/pam.d/gdm-password`, anhand derselben Schritte editiert werden.

## 2.2.4 Deaktivieren von SELinux

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Editieren Sie die Konfigurationsdatei:

```
su -c 'vi /etc/selinux/config'
```

2. Finden Sie die Zeile mit folgendem Inhalt und setzen Sie SELINIUX auf disabled:

```
SELINUX=disabled
```

3. Speichern Sie und schliessen Sie den Editor.

## 2.2.5 Deaktivieren der Firewall

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Führen Sie folgenden Befehl aus.

```
systemctl stop iptables.service
```

2. Deaktivieren Sie die Firewall auf mit folgendem Befehl:

```
systemctl disable iptables.service
```

## 2.2.6 Installieren von Webmin

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Führen Sie folgenden Befehl aus.

```
su -c 'rpm -ihv /  
http://downloads.sourceforge.net/project/webadmin/webmin/1.570/ /  
webmin-1.570-1.noarch.rpm'
```

```
Retrieving http://downloads.sourceforge.net/project/webadmin/webmin/1.570/webmin  
-1.570-1.noarch.rpm  
warning: /var/tmp/rpm-tmp.oMpPUk: Header V3 DSA/SHA1 Signature, key ID 11f63c51:  
NOKEY  
Preparing... ##### [100%]  
Operating system is Redhat Linux  
 1:webmin ##### [100%]  
Webmin install complete. You can now login to https://fed16.netcult.ch:10000/  
as root with your root password.
```

## 2.2.7 Installieren von Usermin

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Führen Sie folgenden Befehl aus.

```
su -c 'rpm -ihv /  
http://downloads.sourceforge.net/project/webadmin/usermin/1.490/ /  
usermin-1.490-1.noarch.rpm'
```

```
Operating system is Redhat Linux  
 1:usermin ##### [100%]  
Usermin install complete. You can now login to https://fed16.netcult.ch:20000/  
as any user on your system.
```

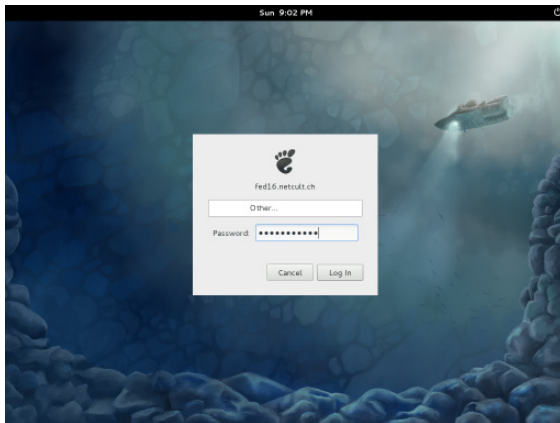
## 2.2.8 Services permanent aktivieren

1. Melden Sie sich als regulären Benutzer an und öffnen Sie das Terminal (command line). Führen Sie folgenden Befehl aus.

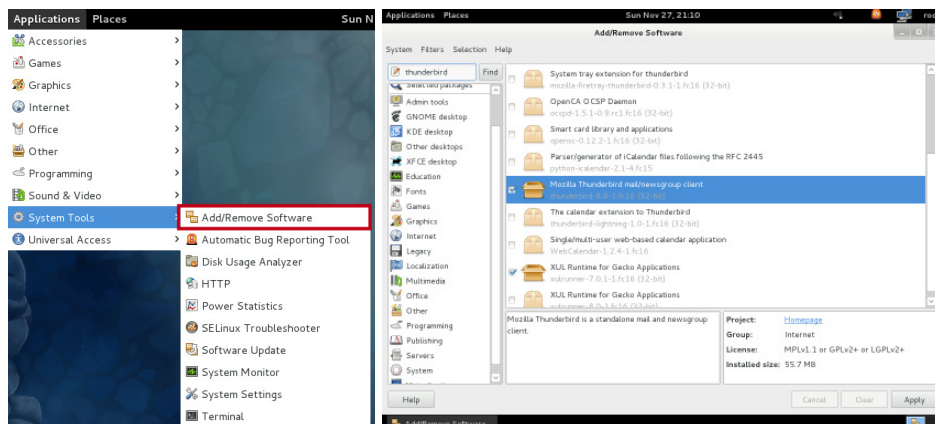
```
su -c 'systemctl enable httpd.service'  
su -c 'systemctl enable dovecot.service'  
su -c 'systemctl enable sendmail.service'  
su -c 'systemctl enable smb.service'  
su -c 'systemctl enable spamassassin.service'  
su -c 'systemctl enable saslauthd.service'  
su -c 'systemctl enable webmin.service'  
su -c 'systemctl enable usermin.service'
```

2. Starten Sie das System neu.

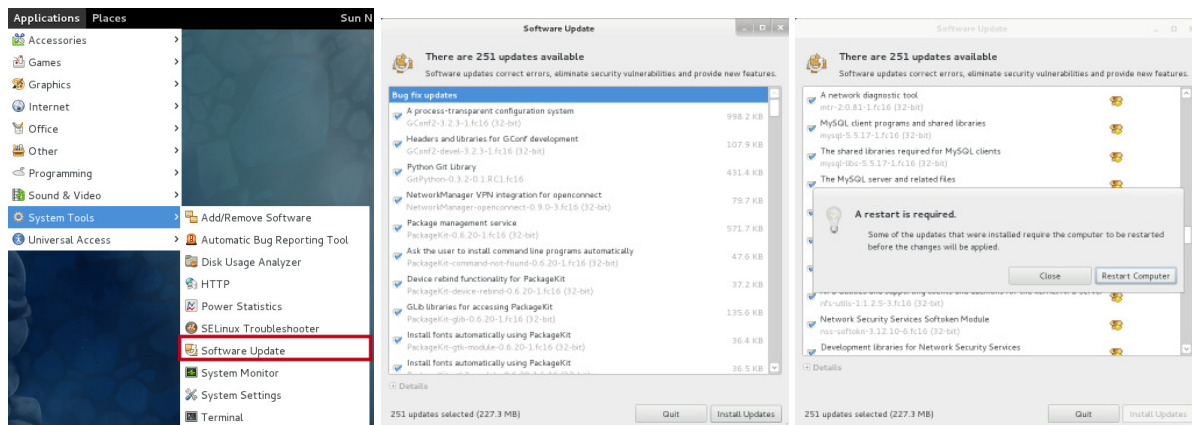
## 2.2.9 Mail Client und Linux Updates



Melden Sie sich mit zuvor erstelltem Root-Benutzer an.



Wählen Sie Applications | System Tools | Add/Remove Software  
Installieren Sie den Mozilla Thunderbird Mailclient.



Wählen Sie *Applications | System Tools | Software Update* oder führen Sie

```
yum update
```

aus. Installation aller verfügbaren Updates. Anschliessend: Starten Sie Ihr System neu.

## 3 Applikationen

### 3.1 Sendmail

1. Öffnen Sie die Sendmail Konfigurationsdatei:

```
su
vi /etc/mail/sendmail.mc
```

2. Aktivieren Sie Sendmail auf allen Netzwerkinterfaces:

```
/etc/mail/sendmail.mc

dnl # The following causes sendmail to only listen on the IPv4
dnl # loopback address 127.0.0.1 and not on any other network
dnl # devices. Remove the loopback address restriction to accept
dnl # email from the internet or // intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
```

3. Erhöhen Sie den Loglevel auf den Wert 14, falls es notwendig sein sollte:

```
/etc/mail/sendmail.mc

dnl # default logging level is 9, you might want to set it higher to
dnl # debug the configuration.
dnl #
define(`confLOG_LEVEL', `14')dnl
```

4. Setzen der Authentifizierungsoptionen und -mechanismen:

```
/etc/mail/sendmail.mc
```

```

define(`confAUTH_OPTIONS', `A')dnl

dnl # PLAIN is the preferred plaintext authentication method and
dnl # used by Mozilla Mail and Evolution, though Outlook Express and
dnl # other MUAs do use LOGIN. Other mechanisms should be used if
dnl # the connection is not guaranteed secure.
dnl # Please remember that saslauthd needs to be running for AUTH.
dnl #
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

```

## 5. Aktivieren der SSL Zertifikate und SSL Dienste:

```

/etc/mail/sendmail.mc

dnl # Rudimentary information on creating certificates for sendmail TLS:
dnl # cd /etc/pki/tls/certs; make sendmail.pem
dnl # Complete usage:
dnl # make -C /etc/pki/tls/certs usage
dnl #
define(`confCRL', `/etc/pki/tls/certs/revocation.list')dnl
define(`confCACERT_PATH', `/etc/pki/tls/certs')dnl
define(`confCACERT', `/etc/pki/tls/certs/sendmail-ca.crt')dnl
define(`confSERVER_CERT', `/etc/pki/tls/certs/sendmail.pem')dnl
define(`confSERVER_KEY', `/etc/pki/tls/certs/sendmail.pem')dnl

dnl # For this to work your OpenSSL certificates must be configured.
dnl #
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl

```

## 6. Falls gewünscht, fügen Sie DNS-Blacklisten Checks gegen Spamsender ein:

```

/etc/mail/sendmail.mc

dnl # Add some dns blacklist checks
dnl #
dnl # Used blackist sites
FEATURE(`dnsbl', `sbl-xbl.spamhaus.org')dnl
FEATURE(`dnsbl', `bl.spamcop.net')dnl
FEATURE(`dnsbl', `cbl.abuseat.org')dnl
dnl # Unused blackist sites
dnl # FEATURE(`dnsbl', `zen.spamhaus.org')dnl
dnl # FEATURE(`dnsbl', `dnsbl.sorbs.net')dnl
dnl # FEATURE(`dnsbl', `relays.ordb.org')dnl

```

## 7. Stellen Sie sicher, dass die MAILER-Optionen korrekt gesetzt sind (diese müssen sich ganz am Ende der Datei befinden):

```

/etc/mail/sendmail.mc

MAILER(smtp)dnl
MAILER(procmail)dnl
dnl MAILER(cyrusv2)dnl

```

## 8. Erstellen der SSL Zertifikate:

**Wechseln Sie in den Ordner** `cd /etc/pki/tls/certs/` **und erstellen Sie Zertifikate:**

```
openssl req -newkey rsa:2048 -nodes -out sendmail-req.pem -keyout /
sendmail-key.pem
openssl rsa -in sendmail-key.pem -out sendmail-plainkey.pem

openssl x509 -in sendmail-req.pem -out sendmail-ca.crt -req -signkey /
sendmail-plainkey.pem -days 3650

cp sendmail-plainkey.pem sendmail.pem
rm -f sendmail-plainkey.pem
cat sendmail-ca.crt >> sendmail.pem
touch revocation.list

chown root:mail sendmail.pem
chown root:mail sendmail-ca.crt
chown root:mail revocation.list
chmod 600 sendmail.pem
chmod 644 sendmail-ca.crt
chmod 600 revocation.list
```

**9. Erstellen Sie eine neue sendmail.cf Datei:**

```
/etc/mail/make
```

**10. Wer Root's E-Mail erhalten soll:**

```
tail -f /etc/aliases
(..)
Person who should get root's mail
root: administrator
```

**11. Starten Sie Sendmail neu:**

```
systemctl restart sendmail.service
```

## **3.2 Procmail**

**1. Öffnen Sie die Procmail Konfigurationsdatei:**

```
su
vi /etc/procmailrc
```

**2. Fügen Sie folgenden Inhalt hinzu:**

```
/etc/procmailrc

# /etc/procmailrc
# Procmail Configfile by Netcult.ch

# Set variables
LOGFILE=/var/log/procmail.log
SPAMASSASSIN=/usr/bin/spamc
LOCKFILESPAMC=$HOME/.spamclock
LOCKFILEPROCMAIL=$HOME/.proclock
DROPPRIVS=yes
```

```

# Pass emails through SpamAssassin and set X-Spam-Status flag by spamc
:0fw: $LOCKFILESPAMC
| $SPAMASSASSIN

# Pick emails with X-Spam-Status flag and move it over to users spamfolder
:0: $LOCKFILEPROCMAIL
* ^X-Spam-Status: Yes
$HOME/mail/Spam

```

3. Nach Konfiguration von Webmin/Usermin sind die Benutzer über ein Webinterface in der Lage weitere eigene Regeln in der Datei `~/.procmailrc` vorzunehmen.

### 3.3 SpamAssassin

1. Öffnen Sie die globale SpamAssassin Konfigurationsdatei:

```
vi /etc/mail/spamassassin/local.cf
```

2. Folgende Einstellungen im Produktivbetrieb getestet:

```

/etc/mail/spamassassin/local.cf

# How many hits before a message is considered spam.
required_score      3.5

# Change the subject of suspected spam
rewrite_header      subject  *SPAM*:

# Encapsulate spam in an attachment (0=no, 1=yes, 2=safe)
report_safe         1

# Enable the Bayes system
use_bayes           1

# Enable Bayes auto-learning
bayes_auto_learn    1

# Enable or disable network checks
skip_rbl_checks     0
use_razor2          1
use_dcc             1
use_pyzor           1

# Mail using languages used in these country codes will not be marked
# as being possibly spam in a foreign language.
# - english german
ok_languages        en de

# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_locales          en

```

3. Nach Konfiguration von Webmin/Usermin sind die Benutzer über ein Webinterface in der Lage weitere eigene Regeln in der Datei `~/.spamassassin/user_prefs.cf` vorzunehmen.
4. Aktivieren Sie die älteren SpamAssassins Plugins indem Sie die Remarks (#) entfernen.

```
vi /etc/mail/spamassassin/v310.pre
vi /etc/mail/spamassassin/v320.pre
vi /etc/mail/spamassassin/v312.pre
vi /etc/mail/spamassassin/v330.pre
```

### 5. Starten Sie SpamAssassin neu:

```
systemctl enable spamassassin.service
```

## 3.4 Dovecot

### 1. Erstellen der SSL Zertifikate:

Wechseln Sie in den Ordner `cd /etc/pki/tls/certs/` und führen Sie folgende Befehle aus:

```
openssl req -newkey rsa:2048 -nodes -out dovecot-req.pem -keyout dovecot-key.pem
openssl rsa -in dovecot-key.pem -out dovecot-plainkey.pem
openssl x509 -in dovecot-req.pem -out dovecot-ca.crt -req -signkey /
dovecot-plainkey.pem -days 3650
```

```
cp dovecot-plainkey.pem dovecot.pem
rm -f dovecot-plainkey.pem
cat dovecot-ca.crt >> dovecot.pem
chown root:root dovecot.pem
chown root:root dovecot-ca.crt
chown root:root dovecot-key.pem
```

### 2. Öffnen Sie die Dovecot Konfigurationsdatei:

```
vi /etc/dovecot/dovecot.conf
```

### 3. Service Konfiguration:

```
/etc/dovecot.conf

# Protocols we want to be serving: imap imaps pop3 pop3s managesieve
# If you only want to use dovecot-auth, you can set this to "none".
# protocols = imap imaps pop3 pop3s
protocols = imap imaps pop3

# A space separated list of IP or host addresses where to listen in for
# connections. "*" listens in all IPv4 interfaces. "[::]" listens in all IPv6
# interfaces. Use "*", "[::]" for listening both IPv4 and IPv6.
#
# If you want to specify ports for each service, you will need to configure
# these settings inside the protocol imap/pop3/managesieve { ... } section,
# so you can specify different ports for IMAP/POP3/MANAGESIEVE. For example:
#   protocol imap {
#     listen = *:10143
#     ssl_listen = *:10943
#     ..
#   }
#   protocol pop3 {
#     listen = *:10100
#     ..
#   }
```

```
# protocol managesieve {
#     listen = *:12000
#     ..
# }

listen = *, ::

# Access for Dovecot process to home directories.
mail_privileged_group = mail
mail_access_groups = mail
```

#### 4. Öffnen Sie die Dovecot SSL Konfigurationsdatei:

```
vi /etc/dovecot/conf.d/10-ssl.conf
```

#### 5. SSL Konfiguration

```
/etc/dovecot/conf.d/10-ssl.conf

##
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf

ssl_cert = </etc/pki/tls/certs/dovecot.pem
ssl_key = </etc/pki/tls/certs/dovecot-key.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path.
#ssl_key_password =

# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = /etc/pki/dovecot/certs/ca.pem)
ssl_ca = </etc/pki/tls/certs/dovecot-ca.crt

# Request client to send a certificate. If you also want to require it, set
# auth_ssl_require_client_cert=yes in auth section.
#ssl_verify_client_cert = no

# Which field from certificate to use for username. commonName and
# x500UniqueIdentifier are the usual choices. You'll also need to set
# auth_ssl_username_from_cert=yes.
#ssl_cert_username_field = commonName

# How often to regenerate the SSL parameters file. Generation is quite CPU
# intensive operation. The value is in hours, 0 disables regeneration
# entirely.
```

```
ssl_parameters_regenerate = 168

# SSL ciphers to use
ssl_cipher_list = ALL:!LOW:!SSLv2:!EXP:!aNULL
```

## 6. Öffnen Sie die Dovecot Auth-Konfigurationsdatei:

```
vi /etc/dovecot/conf.d/10-auth.conf
```

## 7. Auth Konfiguration

```
/etc/dovecot/conf.d/10-auth.conf

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
disable_plaintext_auth = no
```

## 8. Dovecot erstellt an der konfigurierten `mail_location` Standardmässig eine `inbox` Datei. Traditionell speichert Sendmail die Maildaten unter `/var/spool/mail/`.

Dovecot sucht aber die Daten standardmässig unter:

```
/home/thomas/Maildir
/home/thomas/mail
/home/thomas/Mail
```

Um die traditionelle Struktur zu verwenden muss die `mail_location` Option korrekt gesetzt sein.

## 9. Öffnen Sie die Dovecot Mailbox-Konfigurationsdatei:

```
vi /etc/dovecot/conf.d/10-mail.conf
```

## 10. Mailbox Konfiguration

```
/etc/dovecot/conf.d/10-mail.conf

##
## Mailbox locations and namespaces
##

# Location for users' mailboxes. This is the same as the old default_mail_env
# setting. The default is empty, which means that Dovecot tries to find the
# mailboxes automatically. This won't work if the user doesn't have any mail
# yet, so you should explicitly tell Dovecot the full location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
```

```

#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
# mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%ln/%n:INDEX=/var/indexes/%d/%ln/%n
#
# <doc/wiki/MailLocation.txt>
# mail_location = mbox:/var/spool/mail/%u
mail_location = mbox:~/mail:INBOX=/var/mail/%u

```

Um von der traditionellen Struktur auf eine zentralisierte mail-Ablage im Benutzer-Home-Verzeichnis umzustellen, verwenden Sie: `mbox:~/mail:INBOX:~/mail/inbox`.

Bei Umstellung: Beachten Sie, dass Sie auch die globale Mail-Home Variable für Procmail anpassen müssen.

```
vi /etc/procmailrc
```

Fügen Sie markierte Zeile hinzu:

```

/etc/procmailrc
# /etc/procmailrc
# Procmail Configfile by Netcult.ch
# Set variables
DEFAULT=$HOME/mail/inbox
LOGFILE=/var/log/procmail.log
SPAMASSASSIN=/usr/bin/spamc
(..)

```

## 11. Setzen Sie den Benutzer Administrator in die Linux-User Gruppe, ID = 100.

```

vi /etc/passwd
administrator:x:1000:100:Administrator:/home/administrator:/bin/bash

chown -R :users /var/mail/
chown -R :users /home/

```

Als Abschluss starten Sie Dovecot und sasl neu:

```

systemctl restart dovecot.service
systemctl restart saslauthd.service

```

## 3.5 Mail - Funktionstests

Senden Sie eine Testnachricht an den zuvor erstellten Administrator-Benutzer und prüfen Sie ob die E-Mail zugestellt wurde.

```
su administrator
cat /etc/redhat-release | mail -s "Fedora Release" /
administrator@fed16.netcult.ch
tail -f /var/mail/administrator
```

```
Date: Mon, 28 Nov 2011 19:13:43 +0100
To: administrator@fed16.netcult.ch
Subject: Fedora Release
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

Fedora release 16 (Verne)

Öffnen Sie Mozilla Thunderbird und Konfigurieren Sie das lokale Mailkonto für den Benutzer administrator.

The image displays a series of screenshots from a Linux desktop environment. The top-left screenshot shows the 'Mail Account Setup' dialog box with fields for 'Your name' (Administrator), 'Email address' (administrator@fed16.netcult.ch), and 'Password'. The top-right screenshot shows the 'Mail Account Setup' dialog box with the 'Remember password' checkbox checked. The middle-left screenshot shows the 'Mail account setup' dialog box with server settings for IMAP and SMTP. The middle-right screenshot shows a 'Secure Connection Failed' error dialog box with the message 'fed16.netcult.ch:143 uses an invalid security certificate.' The bottom-left screenshot shows the Mozilla Thunderbird interface with the 'Inbox' folder selected and a message titled 'Fedora Release' from Administrator. The bottom-right screenshot shows the 'Write: Re: Fedora Release' dialog box with the subject 'Re: Fedora Release' and the body text 'Outgoing test'.

Wenn alles korrekt funktioniert, können Sie hier Ihre Mailbox mit dem zuvor gesendeten Mail einsehen. Versuchen Sie ebenfalls eine E-Mail via SMTP zu beantworten.

The image shows a 'SMTP Server' configuration window. It has two main sections: 'Settings' and 'Security and Authentication'. In the 'Settings' section, there are three input fields: 'Description' with the value 'Test SMTP Server', 'Server Name' with 'fed16.netcult.ch', and 'Port' with '25' (and a 'Default: 25' label). The 'Security and Authentication' section has two dropdown menus: 'Connection security' set to 'STARTTLS' and 'Authentication method' set to 'Normal password'. Below these is a 'User Name' field containing 'administrator'. At the bottom of the window are 'Cancel' and 'OK' buttons.

Beispiel für unsere Installation.

### 3.6 MySQL

Melden Sie sich als root Benutzer an und öffnen Sie das Terminal (command line). Führe Sie folgenden Befehl aus.

```
systemctl enable mysqld.service
systemctl start mysqld.service
```

### 3.7 Horde Groupware Webmail Edition

Melden Sie sich als root an und starten Sie Add/Remove Software.

Öffnen Sie das Terminal (command line). Führe Sie folgende Befehle aus.

```
yum install php-xml
yum install gettext
yum list php-xml
yum list gettext

wget http://pear.php.net/go-pear.phar
php go-pear.phar

1. Installation base ($prefix)           : /usr
2. Temporary directory for processing    : /tmp/pear/install
3. Temporary directory for downloads     : /tmp/pear/install
4. Binaries directory                   : /usr/bin
5. PHP code directory ($php_dir)        : /usr/share/pear
6. Documentation directory               : /usr/docs
7. Data directory                       : /usr/data
8. User-modifiable configuration files directory : /usr/cfg
9. Public Web Files directory           : /var/www
10. Tests directory                     : /usr/tests
11. Name of configuration file           : /etc/pear.conf

/usr/bin/pear channel-discover pear.horde.org

# Adding Channel "pear.horde.org" succeeded
# Discovery of channel "pear.horde.org" succeeded
```

Als nächstes definieren Sie die sogenannte Role. Die Role entspricht dem Installationsverzeichnis (zb. /var/www/groupware). Dies wird einmalig pro System gesetzt.

```

mkdir /var/www/webmail
/usr/bin/pear install horde/horde_role
/usr/bin/pear run-scripts horde/horde_role

# Filesystem location for the base Horde application : /var/www/webmail
# Configuration successfully saved to PEAR config.
# Install scripts complete

/usr/bin/pear install -a -B horde/webmail

cp /var/www/webmail/config/conf.php.dist /var/www/webmail/config/conf.php

touch /etc/httpd/conf.d/webmail.conf
vi /etc/httpd/conf.d/webmail.conf

```

```
/etc/httpd/conf.d/webmail.conf
```

```

#
# This configuration file allows the manual to be accessed at
# http://localhost/webmail
#
AliasMatch ^/webmail(?:/(?:de|en|fr|ja|ko|ru))?(/.*)?$ "/var/www/webmail$1"

<Directory "/var/www/webmail">
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

```

```

mysqladmin -u root -p create horde4
mysql -h localhost -u root
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('password');
CREATE USER 'horde'@'localhost' IDENTIFIED BY 'password';
GRANT ALL ON *.* TO 'horde'@'localhost' IDENTIFIED BY 'password';
/or/ GRANT ALL ON horde4.* TO horde@localhost; /orend/
EXIT

```

```
webmail-install
```

```

What database backend should we use? Mysql
Request persistent connections? Yes
Username to connect to the database as: horde
Password to connect with: password
How should we connect to the database? Unix
Location of UNIX socket: /var/lib/mysql/mysql.sock
Database to use: horde4
Internally used charset: utf-8
Use SSL to connect to the server? No, 0
Certificate Authority to use for SSL connections: - empty -
Split reads to different servers? disabled, false
Specify an existing mail user who you want to give administrator
Permissions (optional): administrator

```

Test über Website: <http://localhost/webmail/test.php>

```

chown root:apache /var/www/webmail/config/*
find /var/www/webmail/config/ -type f -exec chmod 0440 '{}' \;

```

```
/var/www/webmail/config/conf.php
```

```
<?php
/* CONFIG START. DO NOT CHANGE ANYTHING IN OR AFTER THIS LINE. */
// $Id: 00eb7df9811bb5a1c8030994913451b671e50390 $
$conf['vhosts'] = false;
$conf['debug_level'] = E_ALL & ~E_NOTICE;
$conf['max_exec_time'] = 0;
$conf['compress_pages'] = true;
$conf['secret_key'] = '4e20347a-413c-49b2-b4d3-2780ee5bbdde';
$conf['umask'] = 077;
$conf['testdisable'] = true;
$conf['use_ssl'] = 2;
$conf['server']['name'] = $_SERVER['SERVER_NAME'];
$conf['urls']['token_lifetime'] = 30;
$conf['urls']['hmac_lifetime'] = 30;
$conf['urls']['pretty'] = false;
$conf['safe_ips'] = array();
$conf['session']['name'] = 'Horde';
$conf['session']['use_only_cookies'] = true;
$conf['session']['cache_limiter'] = 'nocache';
$conf['session']['timeout'] = 0;
$conf['cookie']['domain'] = $_SERVER['SERVER_NAME'];
$conf['cookie']['path'] = '/';
$conf['sql']['persistent'] = true;
$conf['sql']['username'] = 'horde';
$conf['sql']['password'] = 'secret_password';
$conf['sql']['socket'] = '/var/lib/mysql/mysql.sock';
$conf['sql']['protocol'] = 'unix';
$conf['sql']['database'] = 'horde4';
$conf['sql']['charset'] = 'utf-8';
$conf['sql']['ssl'] = false;
$conf['sql']['splitread'] = false;
$conf['sql']['phptype'] = 'mysql';
$conf['ldap']['useldap'] = false;
$conf['auth']['admins'] = array('administrator');
$conf['auth']['checkip'] = true;
$conf['auth']['checkbrowser'] = true;
$conf['auth']['resetpassword'] = true;
$conf['auth']['alternate_login'] = false;
$conf['auth']['redirect_on_logout'] = false;
$conf['auth']['list_users'] = 'list';
$conf['auth']['params']['app'] = 'imp';
$conf['auth']['driver'] = 'application';
$conf['auth']['params']['count_bad_logins'] = false;
$conf['auth']['params']['login_block'] = false;
$conf['auth']['params']['login_block_count'] = 5;
$conf['auth']['params']['login_block_time'] = 5;
$conf['signup']['allow'] = false;
$conf['log']['priority'] = 'CRIT';
$conf['log']['ident'] = 'HORDE';
$conf['log']['name'] = LOG_USER;
$conf['log']['type'] = 'syslog';
$conf['log']['enabled'] = true;
$conf['log_accesskeys'] = false;
$conf['prefs']['params']['driverconfig'] = 'horde';
$conf['prefs']['driver'] = 'Sql';
$conf['alarms']['params']['driverconfig'] = 'horde';
$conf['alarms']['params']['ttl'] = 300;
$conf['alarms']['driver'] = 'Sql';
$conf['datatree']['driver'] = 'null';
$conf['group']['driverconfig'] = 'horde';
$conf['group']['driver'] = 'Sql';
$conf['group']['cache'] = false;
$conf['perms']['driverconfig'] = 'horde';
$conf['perms']['driver'] = 'Sql';
```

```
$conf['share']['no_sharing'] = false;
$conf['share']['auto_create'] = true;
$conf['share']['world'] = true;
$conf['share']['any_group'] = false;
$conf['share']['hidden'] = false;
$conf['share']['cache'] = false;
$conf['share']['driver'] = 'Sqlng';
$conf['cache']['default_lifetime'] = 86400;
$conf['cache']['params']['sub'] = 0;
$conf['cache']['driver'] = 'File';
$conf['cache']['compress'] = true;
$conf['cache']['use_memorycache'] = '';
$conf['cachecssparams']['driver'] = 'horde_cache';
$conf['cachecssparams']['lifetime'] = 86400;
$conf['cachecssparams']['compress'] = 'php';
$conf['cachecss'] = true;
$conf['cachejsparams']['driver'] = 'horde_cache';
$conf['cachejsparams']['compress'] = 'php';
$conf['cachejsparams']['lifetime'] = 86400;
$conf['cachejs'] = true;
$conf['cachethemes'] = false;
$conf['lock']['params']['driverconfig'] = 'horde';
$conf['lock']['driver'] = 'Sql';
$conf['token']['params']['driverconfig'] = 'horde';
$conf['token']['driver'] = 'Sql';
$conf['mailer']['params']['sendmail_path'] = '/usr/lib/sendmail';
$conf['mailer']['params']['sendmail_args'] = '-oi';
$conf['mailer']['type'] = 'sendmail';
$conf['mailformat']['brokenrfc2231'] = false;
$conf['vfs']['params']['driverconfig'] = 'horde';
$conf['vfs']['type'] = 'Sql';
$conf['sessionhandler']['type'] = 'Builtin';
$conf['sessionhandler']['memcache'] = false;
$conf['spell']['driver'] = '';
$conf['gnupg']['keyserver'] = array('pgp.mit.edu');
$conf['gnupg']['timeout'] = 10;
$conf['openssl']['cafile'] = '/etc/ssl/certs';
$conf['openssl']['path'] = '/usr/bin/openssl';
$conf['nobase64_img'] = false;
$conf['image']['convert'] = '/usr/bin/convert';
$conf['image']['identify'] = '/usr/bin/identify';
$conf['image']['driver'] = 'Im';
$conf['exif']['driver'] = 'Bundled';
$conf['problems']['email'] = 'support@netcult.ch';
$conf['problems']['maildomain'] = 'netcult.ch';
$conf['problems']['tickets'] = false;
$conf['problems']['attachments'] = true;
$conf['menu']['apps'] = array('imp', 'ingo', 'kronolith', 'mmemo', 'nag', 'turba');
$conf['menu']['always'] = false;
$conf['menu']['links']['help'] = 'all';
$conf['menu']['links']['prefs'] = 'authenticated';
$conf['menu']['links']['problem'] = 'all';
$conf['menu']['links']['login'] = 'all';
$conf['menu']['links']['logout'] = 'authenticated';
$conf['portal']['fixed_blocks'] = array();
$conf['accounts']['driver'] = 'null';
$conf['user']['verify_from_addr'] = false;
$conf['user']['select_view'] = true;
$conf['facebook']['enabled'] = false;
$conf['twitter']['enabled'] = false;
$conf['urlshortener'] = false;
$conf['weather']['provider'] = false;
$conf['imsp']['enabled'] = false;
$conf['kolab']['enabled'] = false;
```

```

$conf['memcache']['enabled'] = false;
$conf['activesync']['state']['params']['devicetable'] = 'horde_activesync_device';
$conf['activesync']['state']['params']['statetable'] = 'horde_activesync_state';
$conf['activesync']['state']['params']['mactable'] = 'horde_activesync_map';
$conf['activesync']['state']['params']['userstable'] =
'horde_activesync_device_users';
$conf['activesync']['logging']['type'] = 'horde';
$conf['activesync']['ping']['heartbeatmin'] = 60;
$conf['activesync']['ping']['heartbeatmax'] = 2700;
$conf['activesync']['ping']['heartbeatdefault'] = 480;
$conf['activesync']['ping']['deviceping'] = true;
$conf['activesync']['ping']['waitinterval'] = 5;
$conf['activesync']['securitypolicies']['provisioning'] = false;
$conf['activesync']['enabled'] = true;
/* CONFIG END. DO NOT CHANGE ANYTHING IN OR BEFORE THIS LINE. */

```

```

/var/www/webmail/config/backend.php

```

```

/* Example configurations: */

```

```

$servers['imap'] = array(
    // ENABLED by default
    'disabled' => false,
    'name' => 'IMAP Server',
    'hostspect' => 'localhost',
    'hordeauth' => false,
    'protocol' => 'imap',
    'port' => 143,
    // Plaintext logins are disabled by default on IMAP servers (see RFC 3501
    // [6.2.3])
    'secure' => 'tls',
    'maildomain' => 'netcult.ch',
    // 'smtp host' => 'smtp.example.com',
    // 'smtp port' => 25,
    'cache' => false,
);

$servers['advanced'] = array(
    // Disabled by default
    'disabled' => true,
    'name' => 'Advanced IMAP Server',
    'hostspect' => 'localhost',
    'hordeauth' => false,
    'protocol' => 'imap',
    'port' => 143,
    'secure' => false,
    'maildomain' => '',
    // 'smtp host' => 'smtp.example.com',
    // 'smtp port' => 25,
    // 'admin' => array(
    //     'params' => array(
    //         'admin_user' => 'cyrus',
    //         'admin_password' => 'cyrus_pass',
    //         'userhierarchy' => 'user.'
    //     ),
    // ),
    'quota' => array(
        'driver' => 'imap',
        'params' => array(
            'hide_when_unlimited' => true,
            'unit' => 'MB'
        )
    ),
),

```

```

        'acl' => true,
        'cache' => false,
    );

$servers['pop'] = array(
    // Disabled by default
    'disabled' => true,
    'name' => 'POP3 Server',
    'hostspect' => 'localhost',
    'hordeauth' => false,
    'protocol' => 'pop3',
    'port' => 110,
    'secure' => false,
    'maildomain' => '',
    // 'smtp host' => 'smtp.example.com',
    // 'smtp port' => 25,
    'cache' => false,
);

$servers['secure-imap'] = array(
    // Disabled by default
    'disabled' => true,
    'name' => 'Secure IMAP Server',
    'hostspect' => 'localhost',
    'hordeauth' => false,
    'protocol' => 'imap',
    'port' => 143,
    'secure' => 'tls',
    'maildomain' => '',
    // 'smtp host' => 'smtp.example.com',
    // 'smtp port' => 25,
    'acl' => false,
    'cache' => false,
);

```

### Setzen Sie Horde Berechtigungen.

```

chown -R apache:apache /var/www/webmail
chmod -R o-rwx /var/www/webmail
chmod -R +rwx /var/www/webmail/config

```

```

yum install ImageMagick

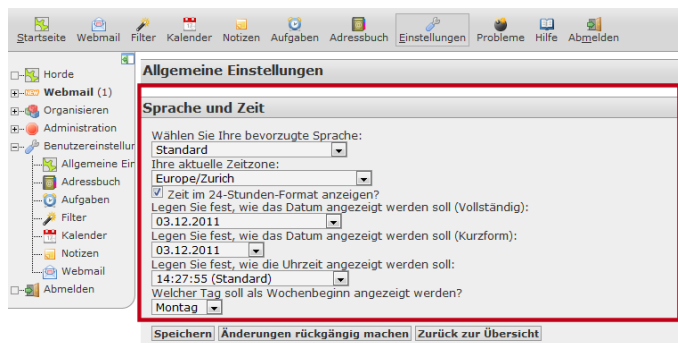
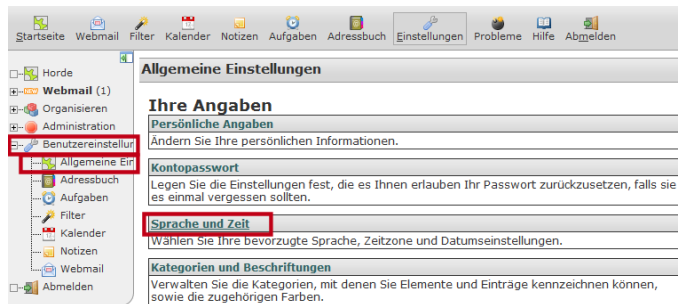
```

**Wenn Ihre Mailbox nicht aufgelistet werden kann, setzen Sie Sprach- und Zeiteinstellungen.  
Wenn Sie den Loglevel von Horde auf DEBUG erhöhen, finden Sie entsprechende Fehlermeldungen:**

```

tail -f /var/log/messages
Dec 1 23:14:43 fed16 HORDE: [horde] PHP ERROR: strftime(): It is not safe to
rely on the system's timezone settings. You are *required* to use the
date.timezone setting or the date_default_timezone_set() function. In case you
used any of those methods and you are still getting this warning, you most
likely misspelled the timezone identifier. We selected 'Europe/Berlin' for
'CET/1,0/no DST' instead [pid 24661 on line 395 of
"/var/www/webmail/config/prefs.php"]

```



## PHP File Upload Unterstützung:

```
vi /etc/php.ini

file_uploads = On
upload_max_filesize = 100M
```

## Zusätzliche Ordner für Benutzer Administrator erstellen:

```
touch /home/administrator/mail/Spam
touch /home/administrator/mail/Draft
touch /home/administrator/mail/Trash
touch /home/administrator/mail/Templates

cd /home/administrator/mail/

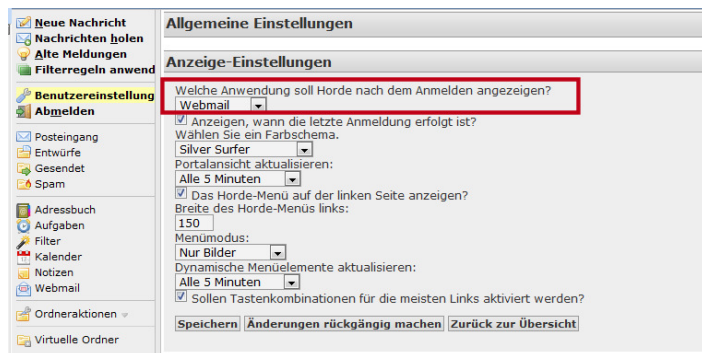
chown --reference /var/mail/administrator Spam
chown --reference /var/mail/administrator Draft
chown --reference /var/mail/administrator Trash
chown --reference /var/mail/administrator Templates

chmod --reference /var/mail/administrator Spam
chmod --reference /var/mail/administrator Draft
chmod --reference /var/mail/administrator Trash
chmod --reference /var/mail/administrator Templates
```

Aktualisieren Sie Ihre Horde Webmail Appliation im Browser und setzen Sie die Maileigenschaften von Adminstrator auf die entsprechend erstellten Ordner.

Ggf. erlauben Sie der Adressbuch-Applikationen einen Export/Import Link anzuzeigen.

Ggf. Benutzereinstellungen -> Anzeige-Einstellungen auf Webmail als Applikation nach dem Anmelden setzen (siehe nachfolgenden Screenshot).



Zusätzlich nachfolgende imp-config setzen. Die Einstellung: “Welche Anwendung soll Horde nach dem Anmelden angezeigt? Webmail,“, macht nur in kombination mit der `apps_iframe` Setting Sinn welche in der der `imp/config/conf.php` Datei aktiviert wird.

```

/var/www/webmail/imp/config/conf.php

<?php
/* CONFIG START. DO NOT CHANGE ANYTHING IN OR AFTER THIS LINE. */
// $Id: 31981bdcd485f0af81362cbffbc3cc334540cba1 $
$conf['user']['autocreate_special'] = true;
$conf['user']['select_sentmail_folder'] = true;
$conf['user']['allow_folders'] = true;
$conf['user']['allow_view_source'] = true;
$conf['server']['server_list'] = 'none';
$conf['server']['fixed_folders'] = array();
$conf['msgsettings']['filtering']['words'] = './config/filter.txt';
$conf['msgsettings']['filtering']['replacement'] = '****';
$conf['spam']['reporting'] = false;
$conf['notspam']['reporting'] = false;
$conf['print']['add_printedby'] = false;
$conf['compose']['use_vfs'] = true;
$conf['compose']['link_all_attachments'] = false;
$conf['compose']['link_attachments_notify'] = true;
$conf['compose']['link_attachments'] = true;
$conf['compose']['attach_size_limit'] = 0;
$conf['compose']['attach_count_limit'] = 0;
$conf['compose']['convert_to_related'] = true;
$conf['compose']['reply_limit'] = 200000;
$conf['compose']['ac_browser'] = 50;
$conf['compose']['ac_threshold'] = 3;
$conf['maillog']['use_maillog'] = true;
$conf['sentmail']['params']['threshold'] = 60;
$conf['sentmail']['params']['limit_period'] = 24;
$conf['sentmail']['params']['table'] = 'imp_sentmail';
$conf['sentmail']['params']['driverconfig'] = 'horde';
$conf['sentmail']['driver'] = 'Sql';
$conf['tasklist']['use_tasklist'] = true;
$conf['notepad']['use_notepad'] = false;
$conf['dimp']['viewport']['buffer_pages'] = 10;
$conf['dimp']['viewport']['viewport_wait'] = 10;
$conf['menu']['apps'] = array();
$conf['menu']['apps_iframe'] = true;
/* CONFIG END. DO NOT CHANGE ANYTHING IN OR BEFORE THIS LINE. */

```

## 4 Benutzerdaten Migration

### 4.1 Benutzerdaten Backup vom alten Mailserver

Erstelle tar ball Archive vom alten Linux System.

```
mkdir /root/move/
```

Setzen vom UID Filterlimit und beginnen mit auslesen der Config-Files.

```
export UGIDLIMIT=500

awk -v LIMIT=$UGIDLIMIT -F: '($3>=LIMIT) && ($3!=65534)' /etc/passwd > /
/root/move/passwd.mig

awk -v LIMIT=$UGIDLIMIT -F: '($3>=LIMIT) && ($3!=65534)' /etc/group > /
/root/move/group.mig

awk -v LIMIT=$UGIDLIMIT -F: '($3>=LIMIT) && ($3!=65534) {print $1}' /
/etc/passwd | tee - | egrep -f - /etc/shadow > /root/move/shadow.mig

cp /etc/gshadow /root/move/gshadow.mig

tar -zcvpf /root/move/home.tar.gz /home
tar -zcvpf /root/move/mail.tar.gz /var/spool/mail
```

Transfer des Backups auf das neue System

```
scp -r /root/move/* user@new.linuxserver.com:/tmp
```

### 4.2 Benutzerdaten Restore auf neuen Mailserver

```
mkdir /root/newsusers.bak
cp /etc/passwd /etc/shadow /etc/group /etc/gshadow /root/newsusers.bak

cd /tmp
cat passwd.mig >> /etc/passwd
cat group.mig >> /etc/group
cat shadow.mig >> /etc/shadow
cp gshadow.mig /etc/gshadow

cd /home
tar -zxvf /tmp/home.tar.gz
cd /var/mail
tar -zxvf /tmp/mail.tar.gz

shutdown -r now
```

### 4.3 Backup und Restore von weiteren Services

Um die Webmin & Usermin - Konfiguration zu sichern und wiederhezustellen – oder aber auch jeden anderen beliebigen Service - folgen Sie der Anleitung von Jamie Cameron:

<http://doxfer.webmin.com/Webmin/BackupConfigurationFiles>

Weitere Backup/Restore Möglichkeiten zu einzelnen Services werden ab Kapitel 5 beschrieben.

## 5 Weitere Services

### 5.1.1 Samba Windows Fileserver

```
/etc/samba/smb.conf

[global]
    log file = /var/log/samba/log.%m
    load printers = yes
    force group = root
    passdb backend = tdbsam
    cups options = raw
    netbios name = fed16.netcult.ch
    netbios aliases = fed16
    wide links = no
    delete readonly = yes
    server string = Samba Server Version %v
    workgroup = netcult
    force user = root
    os level = 20
    security = user
    preferred master = no
    max log size = 50
(...)

[homes]
    comment = Home Directories
    browseable = no
    writable = yes

[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
    guest ok = no
    writable = no
    printable = yes

[c$]
    wide links = no
    delete readonly = yes
    writeable = yes
    path = /
    force group = root
    force user = root
    comment = Root of mail.netcult.ch
```

Fügen Sie den Benutzer Administrator der Samba Benutzerdb hinzu um damit auf den c\$ Share zugreifen können:

```
smbpasswd -a administrator
```

Starten Sie den Samba Service neu:

```
systemctl restart smb.service
```

### 5.1.2 BIND9 DNS Server

Wichtige Konfigfiles für den Nameserver:

```
/var/named/chroot/etc/named.conf
/var/named/chroot/var/named/*.hosts
/var/named/chroot/var/named/slaves/*.hosts
```

Beispiele einer `/var/named/chroot/etc/named.conf` für eine Master und eine Slave Zone:

### Masterzone

```
zone "netcult.ch" {
    type master;
    file "/var/named/netcult.ch.hosts";
};
```

### Slavezone

```
zone "netcult.ch" {
    type slave;
    masters {
        10.0.1.31;
    };
    file "/var/named/slaves/netcult.ch.hosts";
};
```

### Zonenfile

<code>/var/named/slaves/netcult.ch.hosts</code>			
<code>\$ORIGIN .</code>			
<code>\$TTL 3600</code>		<code>; 1 hour</code>	
<code>netcult.ch</code>	<code>IN SOA</code>	<code>dns1.netcult.ch. support.netcult.ch. (</code>	
		<code>2009190107 ; serial</code>	
		<code>900 ; refresh (15 minutes)</code>	
		<code>600 ; retry (10 minutes)</code>	
		<code>86400 ; expire (1 day)</code>	
		<code>3600 ; minimum (1 hour)</code>	
		<code>)</code>	
	<code>NS</code>	<code>dns1.netcult.ch.</code>	
	<code>NS</code>	<code>dns2.netcult.ch.</code>	
	<code>A</code>	<code>84.253.16.62</code>	
	<code>MX</code>	<code>10 mail.netcult.ch.</code>	
	<code>MX</code>	<code>20 mail2.netcult.ch.</code>	
<code>\$ORIGIN netcult.ch.</code>			
<code>blog</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>collab</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>dns1</code>	<code>A</code>	<code>84.253.16.61</code>	
<code>dns2</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>ftp</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>ge</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>mail</code>	<code>A</code>	<code>84.253.16.61</code>	
<code>mail2</code>	<code>A</code>	<code>86.61.70.58</code>	
<code>mysupport</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>photoblog</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>schmedi</code>	<code>A</code>	<code>84.253.16.62</code>	
<code>www</code>	<code>A</code>	<code>84.253.16.62</code>	

## 5.1.3 Online Backup

### 5.1.3.1 Filesystem

CIFS oder NFS Online Backup-Share einrichten, CIFS Share im Beispiel:

```
vi /etc/fstab
\\10.0.1.31\backup /bkp cifs password=pass,uid=0,gid=0,username=user 0 0
mount -all
```

<pre>/etc/webmin/fsdump/169941317761948.dump follow= remount=0 beforefok= rsh= notape=0 file=/bkp/FedoraCore10/filesystem/backup-%m.tar reverify=0 dir=/var/spool/mail /home /etc /var/named mins=10 email= after= xdev=1 id=169941317761948 extra= gzip=0 fs=tar enabled=1 links=1 before= tabs=1 hours=23 pass=pass subject= days=* weekdays=* multi=0 afterfok= label=MAIL update=1 months=* exclude=</pre>
<pre>/etc/webmin/fsdump/169941317761948.11467.status pid=11467 status=tape start=1320444602 tapeid=11527 tapecount=1</pre>

### 5.1.3.2 MySQL Dump

Ich nutze die Scripts von Webmin um die MySQL Datenbank auf einen Online-Share zu dumpen:

```
/etc/webmin/mysql/config
```

```

date_subs=0
max_text=1000
perpage=25
stop_cmd=/etc/rc.d/init.d/mysql stop
mysqldump=/usr/bin/mysqldump
nodbi=0
mysql_libs=
max_dbs=50
start_cmd=/etc/rc.d/init.d/mysql start
pass=pass
mysql_data=/var/lib/mysql
mysqlimport=/usr/bin/mysqlimport
access=: *
style=0
my_cnf=/etc/my.cnf
login=root
mysqlshow=/usr/bin/mysqlshow
mysql=/usr/bin/mysql
nopwd=0
add_mode=1
passwd_mode=0
blob_mode=0
mysqladmin=/usr/bin/mysqladmin
backup_cmode_=1
backup_drop_=0
backup_before_=
backup_compress_=1
backup_single_=0
backup_compatible_=
backup_mkdir_=
backup_=/bkp/FedoraCore10/mysql
backup_charset_=
backup_tables_=
backup_options_=
backup_after_=
backup_where_=

```

```

touch /etc/webmin/mysql/backup.pl
chmod +x /etc/webmin/mysql/backup.pl

```

#### **/etc/webmin/mysql/backup.pl**

```

#!/usr/bin/perl
open(CONF, "/etc/webmin/miniserv.conf");
while(<CONF>) {
    $root = $1 if (/^root=(.*)/);
}
close(CONF);
$ENV{'PERLLIB'} = "$root";
$ENV{'WEBMIN_CONFIG'} = "/etc/webmin";
$ENV{'WEBMIN_VAR'} = "/var/webmin";
chdir("$root/mysql");
exec("$root/mysql/backup.pl", @ARGV) || die "Failed to run $root/mysql/backup.pl :
$!";

```

### **5.1.3.3 Status Monitor**

Backup/Restoren Sie das Webmin Status Verzeichnis, falls es sich um eine Migration handelt:

```

/etc/webmin/status/config
/etc/webmin/status/services/*

```

Bei einer Neuinstallation legen Sie die Monitore über Webmin an, indem Sie auf „Others“ und dann auf „System and Server Status“ navigieren.

#### 5.1.3.4 Usermin Login

Weisen Sie der Benutzergruppe `users` ausschliesslich Usermin-Module zu, welche die eigene Benutzerverwaltung betreffen:

```
tail -f /etc/usermin/usermin.mods
@users::language changepass theme filter forward mailbox schedule spam updown

tail -f /etc/usermin/updown/config
home_only=1
upload=1
background=1
fetch=1
download=1

tail -f /etc/usermin/webmin.acl
user: at changepass chfn commands cron cshrc fetchmail file filter forward gnupg
htaccess-htpasswd htaccess language mailbox mailcap man mysql plan postgresql
proc procmail quota schedule shell spam ssh telnet theme tunnel updown usermount
```

#### 5.1.3.5 Crontab Jobs

Erstellen eine Crontab für root und stellen Sie sicher, dass die Backupjobs ausgeführt werden:

```
tail -f /root/crontab.mailserver
# Webmin Status Monitor
0,10,20,30,40,50 * * * * /etc/webmin/status/monitor.pl
# Online Backup
10 23 * * * /etc/webmin/fsdump/backup.pl 169941317761948
12 0,3,6,9,12,15,18,21 * * * /etc/webmin/mysql/backup.pl --all

crontab < /root/crontab.mailserver

crontab -l
# Webmin Status Monitor
0,10,20,30,40,50 * * * * /etc/webmin/status/monitor.pl
# Online Backup
10 23 * * * /etc/webmin/fsdump/backup.pl 169941317761948
12 0,3,6,9,12,15,18,21 * * * /etc/webmin/mysql/backup.pl --all
```

## 6 Abschluss

Starten Sie den Server neu, indem Sie `shutdown -r now` ausführen. Prüfen Sie anschliessend alle Services auf alle Funktionalitäten.