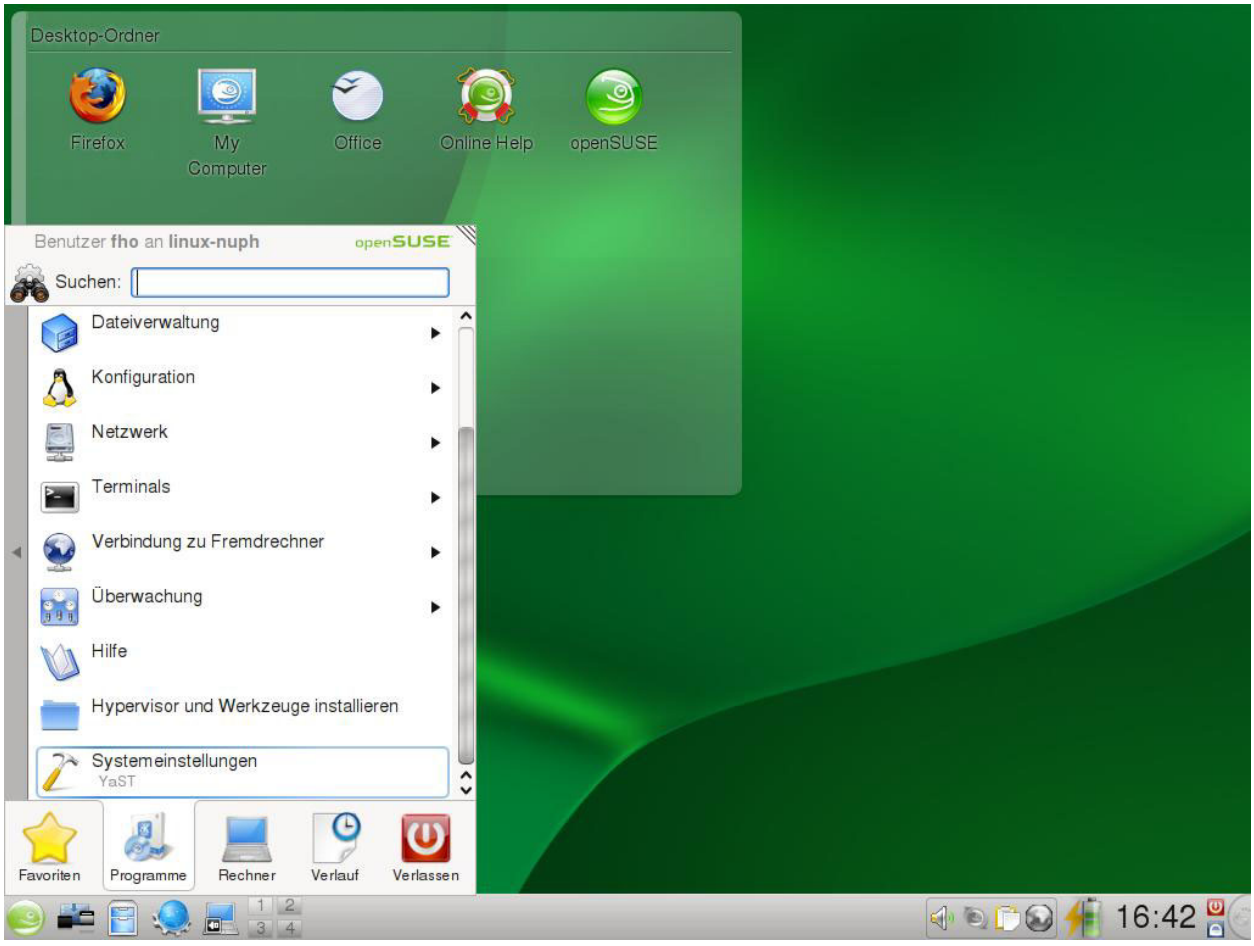
A.NET
Dorfstrasse 68
CH-8126 Zumikon
Tel: +41 (0)44 991 86 30
Fax: +41 (0)44 991 86 34
www.anetgmbh.ch

Installation und Konfiguration von openSuSE 11.1

Eine Schritt-für-Schritt Anleitung für die erfolgreiche Installation und Konfiguration eines File-, Druck, DNS, FTP und Web-Servers.



Inhalt

Installation von OpenSuSE 11.1

Voraussetzungen

- PC ab 256 MB RAM, 512 MB empfohlen
- Pentium 1-4, AMD Duron, Athlon, Athlon XP, MP, Athlon 64 aber keine 80386, 80486, K6
- mind. 500 MB Disk, empfohlen 5 bis 7 GB (je nach Softwareauswahl)
- 1 unterstützter LAN Adapter (fast alle gehen) und/oder ein WLAN-Adapter.

Wenn Sie bereits ein Windows auf der Festplatte haben und genügend ungenutzten Platz auf der Festplatte, installiert sich Linux automatisch in den freien Bereich und den Bootloader GRUB in den Master Boot Record der ersten Festplatte (hda bei einem IDE-System, sda bei SATA oder SCSI-Systemen). Windows wird dann automatisch auf das Bootmenü genommen. Wenn Windows die ganze Platte belegt (dies ist leider Standard), sollten Sie die Windows Partition verkleinern, um Platz für Linux zu schaffen. Linux bietet eine Option "Verkleinern" für Windows NTFS Partitionen (ab Windows NT). Es kann auch ein separates Programm wie PartitionMagic V 8 verwendet werden. Dies geht nicht bei Vista! .

Hinweis: Bei all diesen Veränderungen der Partitionen sollten die Daten vorher gesichert werden!

Falls Sie mehrere Betriebssysteme auf dem gleichen System installieren wollen, haben Sie mehrere Möglichkeiten:

- GRUB einsetzen, wie Linux das vorschlägt. Dies ist geeignet für Windows (dieses am einfachsten als erstes Bestriebssystem installieren) und dann Linux nachinstallieren.
- Verwenden Sie den OS/2 Bootmanager, falls Sie Windows, OS/2 und Linux einsetzen möchten. Der neue Bootmanager von eCS kann von der ganzen Platte booten. Installieren Sie auch hier Windows als erstes, dann den OS/2 Bootmanager. Erstellen Sie dann die Partitionen für Linux (swap und /) mit dem OS/2 LVM und ändern Sie die Partitionen bei der Linux-Installation auf Ext3 oder Reiser. GRUB geht dann in die / Partition.
- Airboot (Freeware) kann alle Betriebssysteme booten und belegt keine Partition. Windows überschreibt zwar auch hier Teile von Airboot bei der Installation, aber Airboot erstellt eine Kopie der Einstellungen in einem nicht überschriebenen Bereich im MBR. So kann Airboot einfach wieder repariert werden. Auch hier installieren Sie GRUB in die / Partition.

Windows Vista enthält selber eine Funktion, seine Partition C: zu verkleinern. Dazu gehen Sie wie folgt vor:

> Start --> Computer --> (rechte Maustaste): Verwalten --> Datenträgerverwaltung
>
> Laufwerk C: markieren --> (rechte Maustaste): Volume verkleinern.

Allerdings kann damit die Partition nur auf ca. 70% verkleinert werden. Das Tool dfsee zeigt an, dass Vista im bereich oberhalb von 53% der Partition Daten anlegt, die nicht verschoben werden. SuSE 10.3 kann die Vista-Partition stärker verkleinern. Allerdings startet Vista dann nicht mehr. Man muss dann ab Vista DVD booten, die Sprache wählen und dann die Installation mit den Computer-Reparatur-Optionen flicken lassen.

Unterschiede zu SuSE 10.1

Die für uns wichtigsten Unterschiede von SuSE 11.x zu 10.1 sind:

- Die Paketauswahl sieht anders aus, sie ist jetzt feiner gegliedert
- Werden Samba-Freigaben mit SWAT konfiguriert, muss bei jeder Freigabe unter „Verschiedene Optionen“ der Parameter Availabe = yes gesetzt werden, sonst ist die Freigabe nicht benutzbar.
- Beim Einbinden von Windows XP-Clients muss *kein* Registry Eintrag mehr geändert

werden.

- Als Mail-Server SMTP fungiert weiterhin Postfix, jedoch wird als POP und IMAP-Server neu Cyrus installiert. Der hält die Daten in einer eigenen Datenbank, ist deshalb stark anders in der Konfiguration, bietet aber wesentlich mehr Funktionen als die alten POP und Imap-Server.

Installation

Wir möchten mehrere Betriebssysteme auf dem gleichen PC starten können. Dazu benutzen wir einen Bootmanager: GRUB (bei Linux enthalten) oder den OS/2 Bootmanager oder AIRboot.

Installation auf einem Windows System

Sorgen Sie für freien Platz auf Platte.

- Bei Windows-Systemen kann direkt bei der SuSE 11.x-Installation die Partition verkleinert werden (es sollten aber immer ein paar GB frei bleiben, damit Windows nicht erstickt!)
- Die Windows-Partition kann auch mit einem separaten Utility wie PartitionMagic V 8 verkleinert werden. Dazu muss der PC ab DOS-Diskette gebootet werden und PQMAGIC.EXE gestartet werden.
- Vista kann via Computer --> (rechte Maustaste) --> Verwalten --> Datenträgerverwaltung auf ca. 70% verkleinert werden. (Partition markieren --> (rechte Maustaste) Verkleinern)
- Schaffen Sie ca. 5-7 GB Platz, das genügt für ein recht umfassendes Linux-System.

Beginn der Installation

1. Open SuSE 11.1 DVD einlegen
2. Booten ab DVD (Einstellung im BIOS notwendig)
3. Auf dem ersten Boot-Bildschirm wählen Sie:
4. [F2] Language --> Deutsch
5. [F3] Weitere Optionen (Other Options) --> [F3] 1024x768 oder 1280x1024 (je nach Bildschirm oder gar 800x600 im Notfall). So sind die Paketinformationen besser darstellbar.
6. Auswahlen auf dem ersten Bildschirm:
   Von Festplatte booten
   --> **Installation**
   Installiertes System reparieren
   Rettungssystem
   Prüfen Installationsmedium (dauert eine Weile)
   Firmwaretest
   Speichertest
   [Enter] (Laden des Linux- Kernels)

   Hinweis: Auf der Eingabezeile können Optionen eingegeben werden. z.B. **vnc=1** Dann kann die Installation ferngesteuert mit einem VNC-Viewer von einem anderen System aus erfolgen.
7. [Weiter] (etwas Geduld, die Hardware-Erkennung läuft nun)
8. Willkommen
   Sprache: [Deutsch]
   Tastaturbelegung: [**Deutsch (Schweiz)**]
   Lizenzvereinbarung
   [Weiter] (Das System wird überprüft)
9. Installationsmodus:

(x) Neuinstallation
( ) Aktualisierung
( ) Reparatur eines installierten Systems

[ ] Zusatzprodukte aus separaten Medien einbinden
[x] Automatische Konfiguration verwenden
[weiter] (Initialisierung)

10. Uhr und Zeitzone
    Wählen Sie links [Europa] und dann rechts [**Schweiz**]
    [ ] Rechneruhr ist auf UTC gestellt (markieren, falls nur Linux auf diesem System läuft)
    (Windows und OS/2 verwenden immer die lokale Zeit)
    [Weiter]
11. Desktop-Auswahl
    Es stehen zwei grafische Oberflächen zur Auswahl. GNOME ist sparsamer mit den Ressourcen und beliebt bei Unix-gewohnten Benutzern, KDE ist umfassender und für Windows-User eher vertraut. Man kann später auch beide installieren und wahlweise benutzen.
    ( ) GNOME
    (x) KDE 4.1
    ( ) weitere
    [Weiter]
12. Partitionierungsvorschlag
    Es wird ein Vorschlag für die Partitionierung gemacht. Dabei sind zu löschende Partitionen **rot** markiert (wenn kein Platz auf dem Disk ist, wird vorgeschlagen Windows zu entfernen!)
    Es werden je eine Partition vorgeschlagen für:
    - swap
    - / (root)
    - /home
    Wir machen die Partitionierung manuell:
    [**Partitionsaufbau erstellen ...**] [Partitionsaufbau bearbeiten...]
13. Vorbereitung der Festplatte: Schritt 1
    ( ) 1: 1. IDE 232 GB /dev/sda
    (x) **Benutzerdefinierte Partitionierung** (für Experten)
    [weiter]
    Dies ist sehr wichtig, vor allem wenn Sie mehrere Betriebssysteme betreiben wollen.
14. Festplatte vorbereiten: Expertenmodus

    Zur Erläuterung: Bezeichnung der Festplatten unter Linux:

HDA	erste IDE/P-ATA-Festplatte (Master)
HDB	zweite IDE/P-ATA-Festplatte (meist Slave)
SDA	erste SATA-Festplatte
SDB	zweite SATA-Festplatte
SCA	erste SCSI-Festplatte (ID=0)
SCB	zweite SCSI-Festplatte (ID=1)
SDA1	erste Partition auf der ersten SATA-Festplatte (A)
SDA2	zweite Partition auf der ersten SATA-Festplatte (A)

    etc.
    Vorbereitung der Festplatte: Schritt 1 (max. sind 4 Partitionen pro Platte möglich, davon *eine* erweiterte mit max. 15 (SCSI) oder 63 (IDE) logischen Laufwerken,). Wir erstellen die **/** (root) und die **swap**, sowie eine **/export**-Partition alle in einer erweiterten Partition.)

    Markieren Sie im linken Fenster die [+] Festplatte (z.B. /dev/sda) und wählen im rechten Fenster den Reiter [**Partitionen**]

    Falls Windows installiert ist, wird dies als erste Partition angezeigt z.B. So:

/dev/sda1 24.4 GB Hidden HPFS/NTFS NTFS XP_X31_3
[Hinzufügen]

( ) Primäre Partition
(x) Erweiterte Partition
[Weiter]

15. Partition auf /dev/sda hinzufügen
Wir erstellen eine erweiterte Partition, die den ganzen freien Plattenplatz belegt:

(x) Maximale Grösse (208.47 GB) (variiert je nach freiem Plattenplatz)
( ) benutzerdefinierte Grösse
( ) benutzerdefinierter Bereich
[Beenden]

16. Wir markieren die neue Extended Partition und erstellen nun die 3 Partitionen:

/dev/sda1 24.4 GB Hidden HPFS/NTFS NTFS XP_X31_3
/dev/sda2 208.47 GB Extended
[Hinzufügen]

17. Partition auf /dev/sda hinzufügen

( ) Maximale Grösse (208.47 GB)
(**x**) benutzerdefinierte Grösse [**1 GB**]
( ) benutzerdefinierter Bereich
[Weiter]

18. Partition auf /dev/sda hinzufügen
(x) Partition formatieren
Dateisystem: [**swap**]
(X) Partition einhängen
Einhängepunkt: [**swap**]
[Beenden]

19. Wir markieren wieder die Extended Partition und erstellen nun die / Partition:

/dev/sda1 24.4 GB Hidden HPFS/NTFS NTFS XP_X31_3
/dev/sda2 208.47 GB Extended
/dev/sda5 1019.75 MB Linux swap swap swap
[Hinzufügen]

20. Partition auf /dev/sda hinzufügen

( ) Maximale Grösse (208.47 GB)
(**x**) benutzerdefinierte Grösse [**7 GB**]
( ) benutzerdefinierter Bereich
[Weiter]

21. Partition auf /dev/sda hinzufügen
(x) Partition formatieren
Dateisystem: [**Ext3**]
(X) Partition einhängen
Einhängepunkt: [**/**]
[Beenden]

22. Wir markieren wieder die Extended Partition und erstellen nun die / export Partition:

/dev/sda1 24.4 GB Hidden HPFS/NTFS NTFS XP_X31_3
/dev/sda2 208.47 GB Extended

/dev/sda5 1019.75 MB Linux swap swap swap
/dev/sda6 6.99 GB Linux native Ext3 /
[Hinzufügen]

23. Partition auf /dev/sda hinzufügen

    ( ) Maximale Grösse (208.47 GB)
    (**x**) benutzerdefinierte Grösse [**50 GB**]
    ( ) benutzerdefinierter Bereich
    [Weiter]

24. Partition auf /dev/sda hinzufügen
    (x) Partition formatieren
    Dateisystem: [**Ext3**]
    (X) Partition einhängen
    Einhängepunkt: [**/export**]
    [Beenden]

25. Damit sind unsere drei Partitionen erstellt. Die genaue Grösse der Partitionen wird automatisch gemacht, da eine Partition immer ganze Spuren umfassen muss. Die genaue Grösse einer Spur ist abhängig von der Disk-Geometrie. Die Partitionen sehen nun wie folgt aus:

Kontrollieren Sie nun folgendes:

- sind die Partitionen mit Ihren bisherigen Betriebssystemen noch da?
- haben Sie eine swap Partition mit ca. 500 bis 1000 MB?
- haben Sie eine / root Partition mit ca. 4 bis 6 GB
- haben Sie eine /export Partition (für die Daten von SAMBA etc.)?

Wenn alles stimmt, schliessen wir die Partitionierung ab. Falls nicht, kann jetzt noch alles

geändert werden (auf dem Disk wurde noch nichts verändert!).
[**Übernehmen**]
[Weiter]

26. Neuen Nutzer erstellen
    Es wird ein erster Benutzer erstellt (man meldet sich auf einem Linux-System *nie* als root an, sondern gibt sich die root-Rechte nur in einem Fenster, wenn wirklich administriert werden soll. Das geht unter Linux/Unix ganz einfach (s. weiter unten).

    Vollständiger Name des Benutzers: [Fritz Hodel]
    Benutzername: [fho]
    Passwort: [xxxxxxxxxxxx]
    Passwort bestaätigen: [xxxxxxxxxxxx]

    [ ] diese Passwort für den Systemadministrator verwenden
    [x] Systemmail empfangen (dies soll der Hauptbenutzer für den Admin werden)
    [ ] Automatische Anmeldung (unbedingt entfernen auf einem Server!)
    [Weiter]

    Hinweis: Wenn Ihr Passwort zu kurz oder zu einfach ist, erscheint eine Warnung.

27. Passwort für den Systemadministrator „root“
    Geben Sie ein starkes Passwort ein, das Sie niemals vergessen dürfen!

    Passwort für Benutzer 'root': [xxxxxxxxxxxxxx]
    Passwort bestätigen: [xxxxxxxxxxxxxx]
    [Weiter]

28. **Installationseinstellungen**
    Es wird die Übersicht der möglichen Einstellungen angezeigt. Die Partitionen sind bereits definiert, es fehlen noch die Angaben zum Bootloader und die Softwareauswahl.

29. Partitionierung
    (die *weiter oben* gewählten Partitionen werden angezeigt)

30. **Konfiguration des Bootloaders -->** (klicken)
    Dieser kann belassen werden, falls nur Linux oder Linux und Windows benutzt wird, überprüfen Sie jedoch die Einstellungen:.

    Konfiguration des Bootloaders:

    Es sollten drei Optionen vorhanden sein:
    [x] openSuSE 11.1
    - Windows (Mit [Bearbeiten] können Sie den genauen Namen der Version anpassen)
    - Failsave
    – openSuSE 11.1

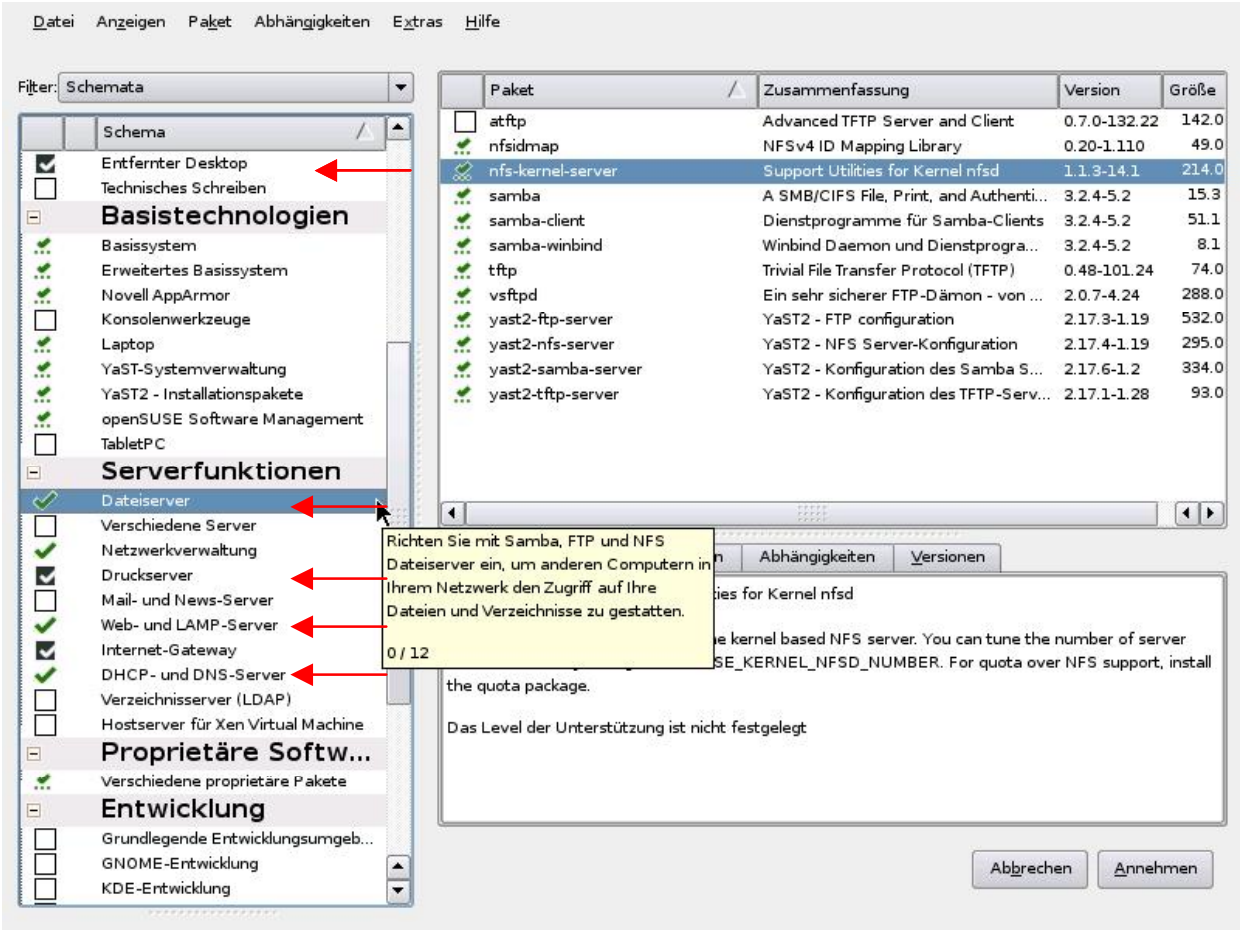
    Wählen sie nun oben rechts den Reiter [**Bootloader-Installation**]

    Prüfen Sie die Optionen des Bootloaders GRUB (Bootloader Installation):
    [ ] Aus Boot-Partition booten
    [ ] Aus erweiterter Partition booten
    [x] **Aus Master Boot Record booten**
    [ ] Aus Root-Partition booten
    [ ] Benutzerdefinierte Bootpartiton

    [OK]

Nur wenn ein anderer Bootmanager benutzt werden soll (z.B. OS/2 Bootmanager oder Airboot) muss die Installation von Grub in die / Partition verschoben werden).

31. **Software -->** (klicken)
    (Hier wählen wir die Pakete für die gewünschten Serverfunktionen. Bei Bedarf kann ein bestimmtes Paket auch gesucht werden: Filter: [Schemata] --> [Suche]). Mit [Details] sieht man die enthaltenen Pakete im Detail.



32. Software Selection and System Tasks
    (Standardmässig werden die Pakete in Gruppen angezeigt (**Schema**)) Die Schemata mit dem **grünen** Hacken sind bereits selektiert. Wir markieren **zusätzlich**:

    [x] Dateiserver (SAMBA, FTP, NFS-Server)
    [x] Netzwerkverwaltung (Kerberos, tcpdump, wireshark etc.)
    [x] Druckserver (sollte bereits markiert sein, CUPS)
    [x] Web- und LAMP-Server (Apache2, MySQL, PHP, Ruby on Rails)
    [x] DHCP- und DNS-Server (Bind9)

    Wir schliessen die Auswahl ab mit:
    [**Annehmen**]

    Hinweis: Wird unten links auf [Details...] gedrückt, sieht man die jeweils enthaltenen Pakete, wie im obigen Beispiel.

33. Automatische Änderungen
    Einzelne Pakete setzen andere Programme voraus, diese werden nun automatisch hinzugefügt.
    [Fortfahren]

34. **Länderspezifische Einstellungen** --> klicken
    Sprache [**de_CH**] ---> [**Details**] (hier klicken)

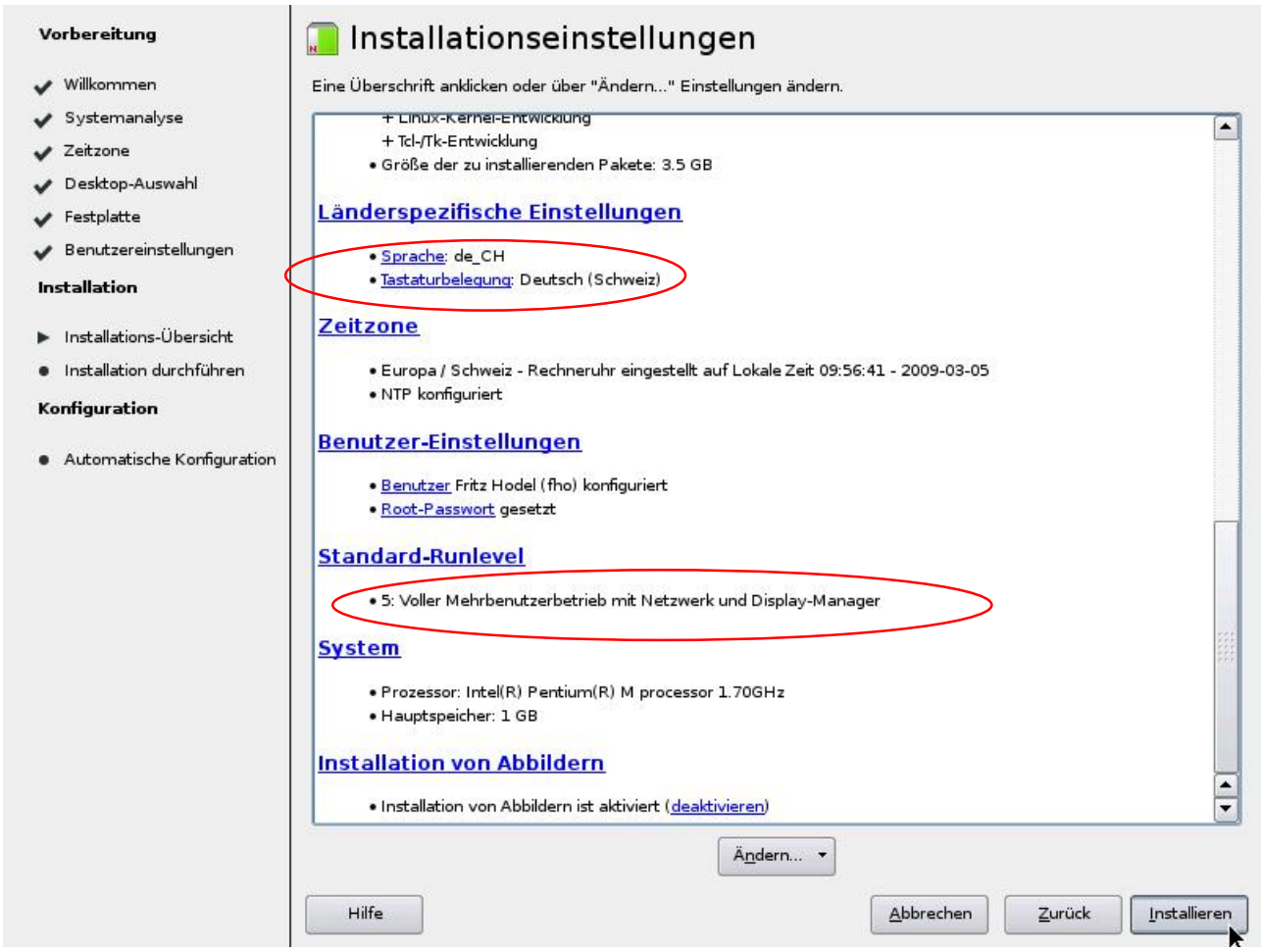
    Detaileinstellungen für die Sprache
    Locale Einstellungen für den Benutzer root:
    [nur ctype]

    [x] UTF-8 als Kodierung verwenden

    Detaillierte Locale Einstellungen:
    [de_CH]
    [OK]

    Sprachen
    [ ] Tastaturbelegung an Deutsch (Schweiz) anpassen
    [ ]Zeitzone an Europa/Schweiz anpassen
    [Übernehmen]

35. Nun sind alle Anpassungen gemacht und wir drücken auf:
    [Installieren]



36. Installation bestätigen

    Hinweis: Wenn hier weitergefahren wird, werden die Partitionen auf der Platte definitiv erstellt/gelöscht (**Point of no return**). Sonst kann jetzt noch abgebrochen werden!
    [Installieren]

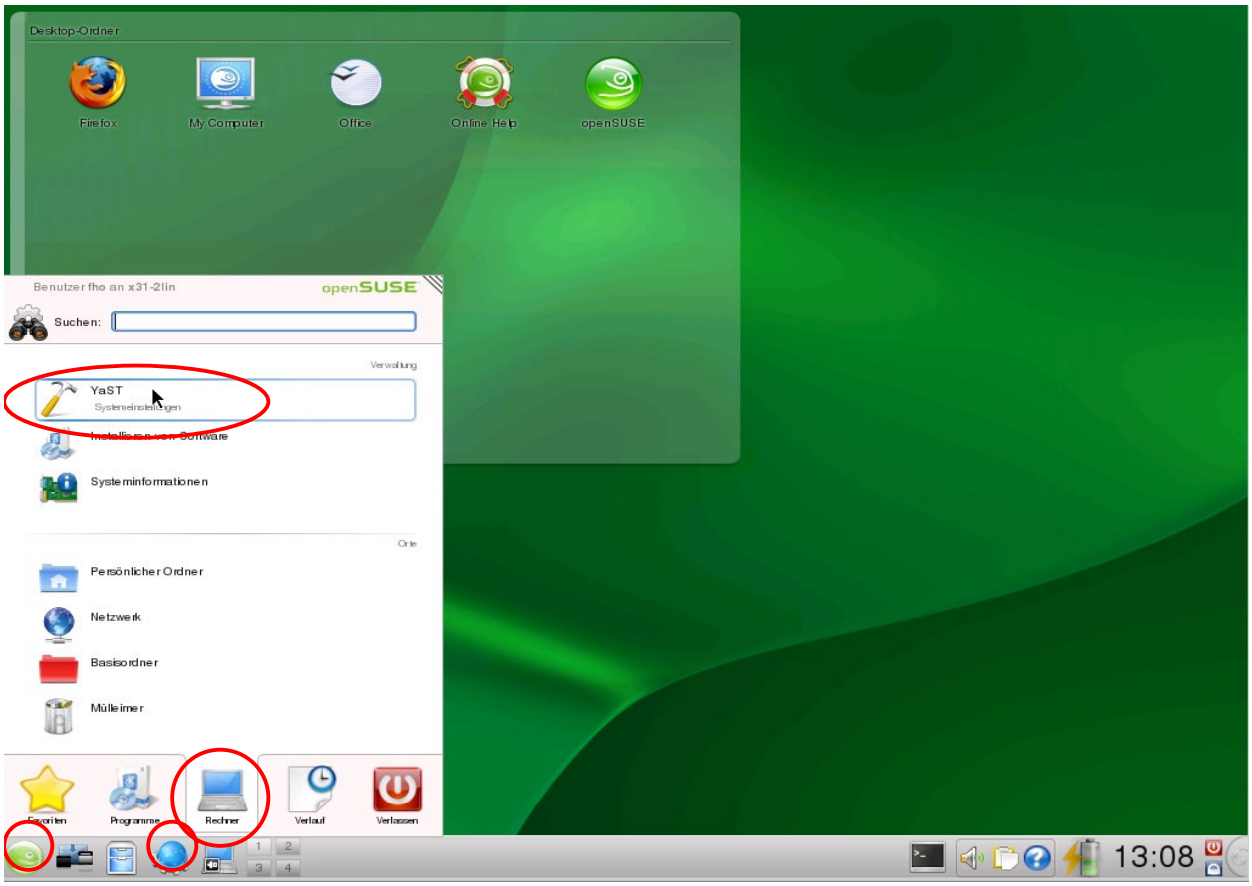
37. Installation durchführen
    Die Installation wird gemäss den gemachten Angeben gemacht. Zuerst werden die Partitionen angelegt, formatiert und dann die Pakete installiert. Dauer (je nach SW-Auswahl und System) ca. 20-40 Minuten. Dann erfolgt ein automatischer Neustart ab Festplatte. Fertig!

Nach dem Kopieren

Gratulation, die Grundinstallation haben Sie geschafft! Es wurde einiges an Software installiert, vieles ist von aussen gesperrt und benötigt noch eine genauere Konfiguration. Ausserdem wehr der Firewall Zugriffe von aussen ab.

Sie können sich nach dem Neustart zum ersten mal am Linux-System anmelden – natürlich **als Benutzer** (den Sie ja bei der Installation bereits eingerichtet haben) und *nicht* als root! Dies wäre ein unnötiges Risiko und schliesslich wollen wir das virenfreie System so behalten.

Zur Orientierung betrachten wir erst einmal den neuen Desktop. Links unten ist ein Chamäleon Symbol, etwa vergleichbar mit dem Start-Knopf von Windows oder dem eCS Symbol von OS/2. Klicken Sie darauf und markieren Sie unten „System“. Dann erscheint oben auf der Liste YaST (Yet another Setup Tool) von SuSE. Starten Sie nun YaST.



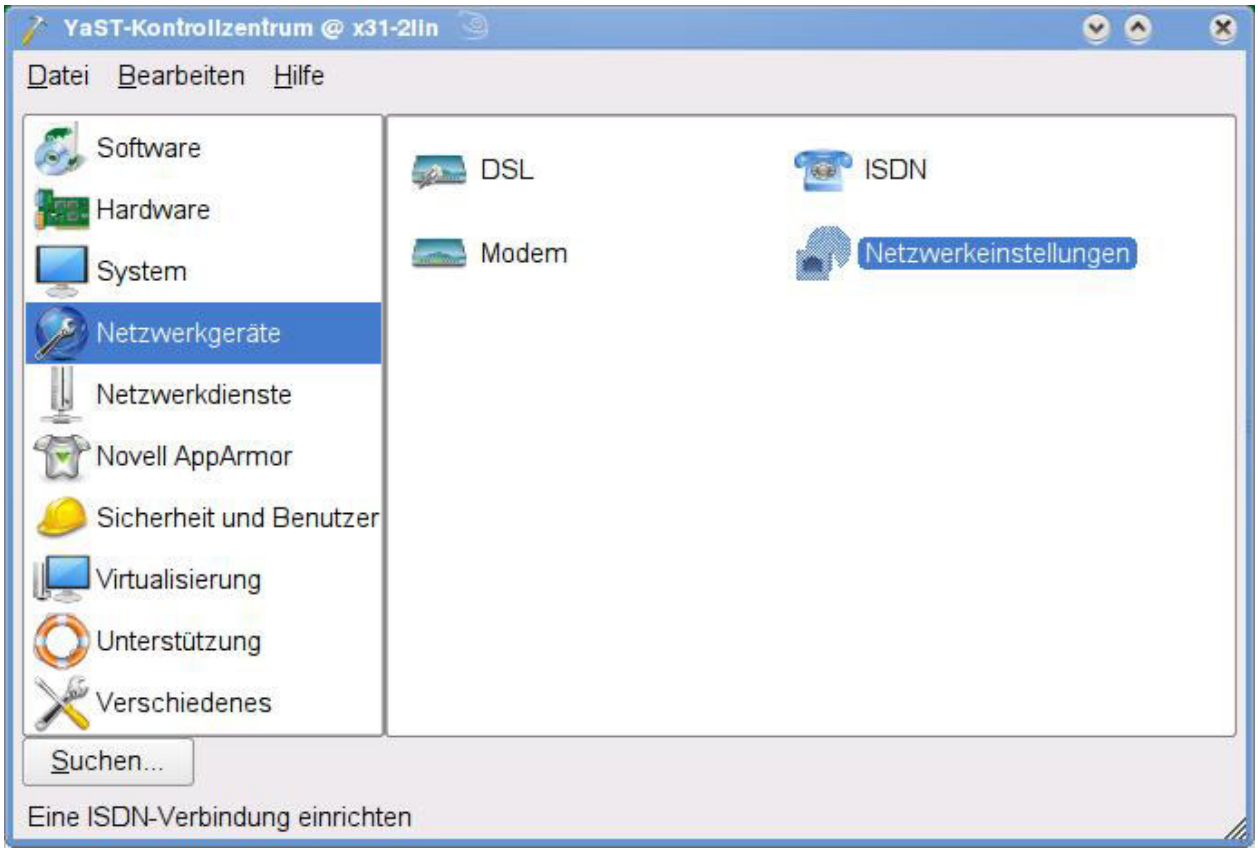
YaST ist ei Tool von SuSE Linux, das eine graphische Oberfläche zum Einstellen von vielen Systemfunktionen und Kommunikationsprogrammen erlaubt. Man kann es auch von der Befehlszeile starten mit „yast2“. Auch „yast“ existiert mit den gleichen Funktionen aber im Textmodus.

Einstellen von Netzwerkadresse und DNS-Name

38. Als erstes legen wir die Netzwerkonfiguration fest. Ein Server wird logischerweise mit einer festen IP-Adresse betrieben:

    “Chamäleon“ --> (unten) Rechner --> (oben auf der Liste) YaST. Im YaST wählen wir nun:

(linke Spalte) **Netzwerkgeräte** --> (rechts) **Netzwerkeinstellungen**
Hinweis: Ein Klick genügt!



Es erscheint eine Warnung, dass das Netzwerk Momentan durch den NetzworkManager gesteuert wird.:
[OK]

Netzwerkeinstellungen
Globale Optionen Übersicht Hostname/DNS Routing

Methode für den Netzwerkaufbau
( ) Benutzergesteuert von NetzworkManager
(x) Traditionelle Methode mit ifup (Wir möchten die manuelle Steuerung)

IPv6 Protokoll-Einstellungen
[ ] IPv6 aktivieren (IP Version 6 wird nicht benötigt und kann bei der Anzeige der Domänen stören. Es wird beim nächsten Neustart deaktiviert.)

(Klick auf den Reiter:) [**Übersicht]**

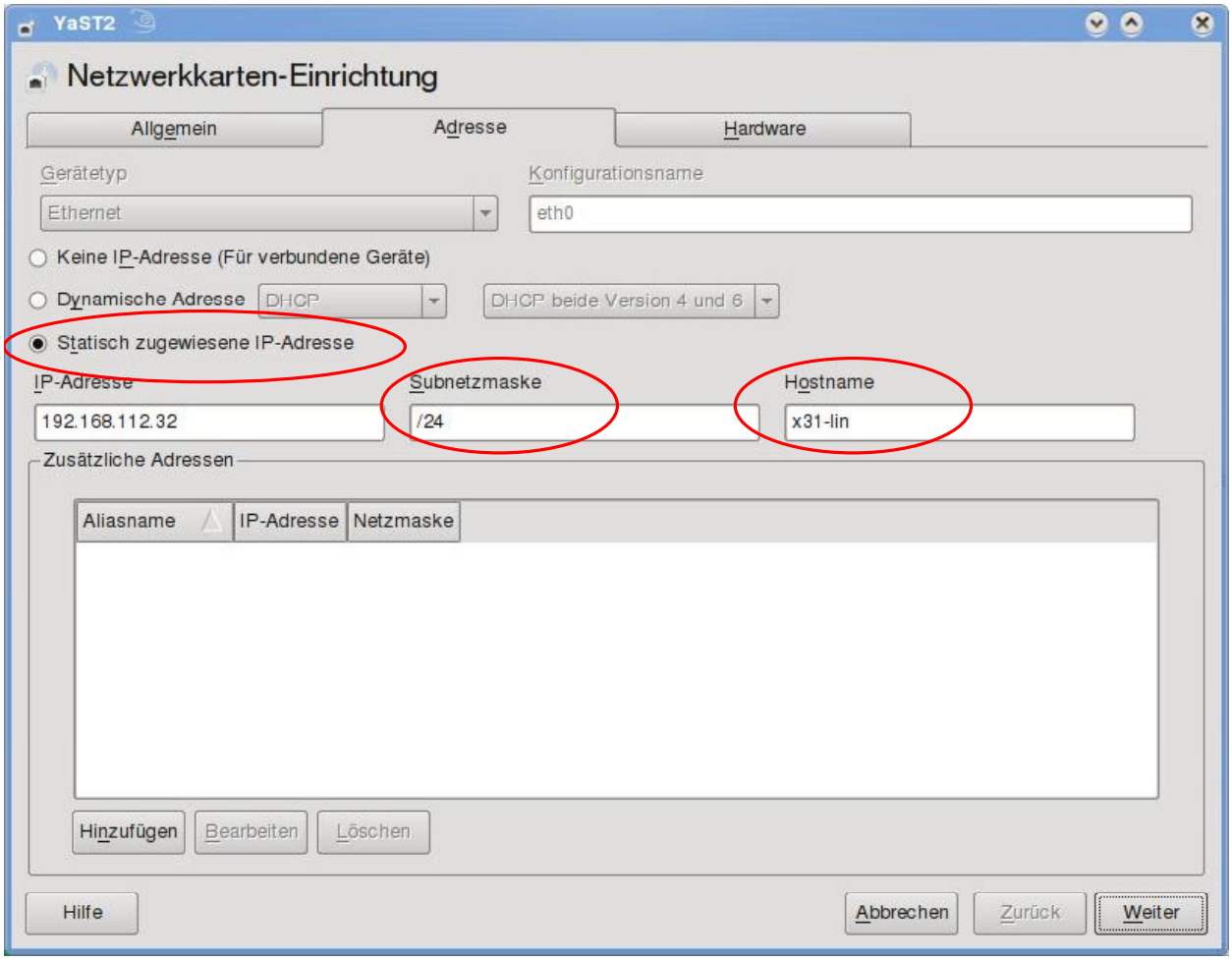
Name: IP-Adresse
8254EP Gigabit Ethernet Controller DHCP (diese Zeile markieren)
[Bearbeiten]

Netzwerkkarten-Einrichtung
Gerätetyp: Konfigurationsname
Ethernet eth0 (= erste Ethernetkarte)
( ) Keine IP-Adresse (Für verbundene Geräte)
( ) Dynamische Adresse

(x) Statisch zugewiesene IP-Adresse

IP-Adresse:	Subnetzmaske	Hostname
192.168.112.32	**/24**	**x31-lin**

(Die Subnetzmaske kann auch mit 255.255.255.0 angegeben werden und *x31-lin* sei der Name des Systems)
[Weiter]



(Klick auf den Reiter:) [**Hostname/DNS**]

Hostname und Domänenname

Hostname:	Domänenname:
x31-lin	anet31.intern

[ ] Hostname über DHCP ändern
[ ] Hostname in /etc/hosts schreiben

DNS-Konfiguration modifizieren
Nameserver und Domänensuchliste:

Nameserver 1	Domänensuche:
192.168.111.32	anet31.intern
Nameserver 2:	
1095.186.1.111	(DNS des Providers)

Hinweis: Wird auf diesem Server auch als DNS-Server aufgesetzt (s. weiter unten), dann sollte er selber als erster DNS eingetragen werden. Damit vorher auch schon ein Zugriff aus Internet möglich ist, geben wir hier als zweiten DNS denjenigen vom Provider ein, hier ein DNS von Bluewin.

(Klick auf den Reiter:) [**Routing**]

Standardgateway:
192.168.112.52 (die IP-Adresse Ihres ADSL/Cable Routers/Firewalls)
[OK] (die Netz-Konfiguration wird gespeichert und aktiviert)

Damit ist die IP-Konfiguration fest eingestellt und – falls ein Netzwerkkabel angeschlossen ist und der Internet-Router/Firewall läuft – kann Ihr System ins Internet gelangen.

SAMBA konfigurieren

Für die Konfiguration des Samba-Servers benützen wir das graphische Hilfsmittel SWAT. Diese ist sehr leistungsfähig und hat den Vorteil, dass es für praktisch alle Distributionen (also nicht nur für SuSE) verfügbar ist. Wir betrachten am Schluss die erzeugte Konfiguration in der Datei /etc/samba/smb.conf. Dort können später Änderungen sehr schnell mit dem Editor gemacht werden.

Wir aktivieren nun via YaST das Programm **SWAT** (Samba Web Administration Tool) um den File- und Print-Server SAMBA zu konfigurieren. Wenn der PC eine Internetverbindung hat, sollte das Paket **samba-doc** nachinstalliert werden (über Rechner --> YaST --> Software --> Software installieren -->Filter: Suche samba-doc [Suchen]). Dann sind in SWAT erläuternde Dokumente verfügbar und für die Parameter steht jeweils direkt ein Hilfetext zur Verfügung.

Swat läuft unter dem xinetd. Der xinetd (eXtended Internet Daemon) ist ein Multi-Server, der auf mehreren IP-Ports horchen kann und erst wenn ein Dienst verlangt wird, startet er den dazugehörigen Dienst. So müssen viele (selten) gebrauchte Dienste nicht dauernd laufen und sind bei Bedarf doch verfügbar.

Wir Planen einen SAMBA-Server als Domänenkontroller mit folgenden Funktionen:

- **NETLOGON** für die Logonscripte
- **DATA** für die Ablage von Benutzerdaten (wie z.B. Dokumente, Tabellen, Bilder etc.)
- **APPS** für Programme, welche die Benutzer von dort laden oder installieren können
- **PUBLIC** als Austauschbox, damit Dateien nicht mehr via Diskette/USB-Stick verteilt werden müssen
- Ein Drucker soll via Netzwerk verfügbar sein
- Unter PRINT$ sollen die Druckertreiber bereitgestellt werden
- Alle Benutzer erhalten ein Home - Verzeichnis, auf welches nur der jeweilige Benutzer Zugriff hat.
- Alle Benutzerstation übernehmen bei der Anmeldung die aktuelle Zeit vom Server

Die einzelnen Schritte der Konfiguration sind wie folgt:

- Verzeichnisse für die Freigaben erstellen
- Server- und Domänennamen konfigurieren
- Benutzer und Samba-Benutzer einrichten
- Freigaben und Zugriffsrechte definieren
- Logonscript definieren und den add machine script
- Clients in die Domäne einbinden und testen

Verzeichnisse für die Freigaben erstellen

39. Wir bereiten die Datenverzeichnisse für den SAMBA-Server vor. Dazu verwenden wir die Befehlszeile mit der Berechtigung als root. Nun bereiten wir die Datenverzeichnisse für den SAMBA-Server vor. Dazu verwenden wir ein Befehlsfenster (Terminal) und verschaffen und darin mit **su -** root-Rechte:
    "Chamäleon" --> Programme --> System --> Terminals --> Terminal (Konsole)
    (es öffnet sich eine Befehlszeile)

    Hinweis: da wir noch öfter mit der Befehlszeile arbeiten werden (schneller als jedes GUI), können wir eine Verknüpfung in der Taskleiste machen. Markieren Sie die Menuposition „Terminals" und drücken Sie die rechte Maustaste --> Zur Kontrollleiste hinzufügen

40. Wir sollten bereits ein Verzeichnis /export haben (da wir dafür eine separate Partition erstellt haben (s. Schritt 24). Falls dem so ist, gibt es beim ersten Befehl eine entsprechende Meldung, andernfalls wird das Verzeichnis jetzt erstellt. Wir geben alles als absoluten Pfad ein):
    Hinweis: Linux (wie Unix) unterscheidet zwischen Gross- und Kleinbuchstaben. Deshalb verwenden wir nur Kleinbuchstaben!

```
su  -                                (es wird das Passwort von root verlangt,
                                     falls erfolgreich ändert der Prompt auf #)
cd  /                                (ins root-Verzeichnis wechseln)
mkdir  /export                       (sollte eigentlich bereits bestehen)
mkdir  /export/samba
mkdir  /export/samba                 (Basisverzeichnis für alle SAMBA-Freigaben
mkdir  /export/samba/netlogon        (für die Logonscripte)
mkdir  /export/samba/data            (für dir Daten der Benutzer)
mkdir   /export/samba/apps           (für Programme, nur Leserecht)
mkdir  /export(samba/public          (Tauschbox)
```

    Wir passen die Berechtigungen an. Im Moment machen wir es uns einfach und schränken den Zugriff mur mit den SAMBA-Freigaben ein. Später kann man die Rechte passenden Gruppen zuteilen (=besser).

```
cd  /export/samba                    (wir gehen in dieses Verzeichnis)
chmod  775  netlogon                 (alle dürfen lesen, Gruppe auch schreiben)
chmod  777  data                     (alle dürfen alles)
chmod  777 apps
chmod  777  public

ls  –l                               (Anzeige zur Kontrolle, sollte so aussehen:)
drwxrwxrwx     2  root  root   4096  Oct  6     09:35  apps
drwxrwxrwx     2  root  root   4096  Oct  6     09:35  data
drwxrwxr-x     2  root  root   4096  Oct  6     09:35  netlogon
drwxrwxrwx     2  root  root   4096  Oct  6     09:35  public
```

41. Windows-Clients vom Tpy Windows NT, 2000, XP und vista benötigen ein Maschinen-Konto, das gleich heisst, wie der Computer, aber mit einem $ angehängt. Also z.B. für den Computer mit dem Namen **PC25** ein Konto **PC25$**). Zusätzlich muss einmal die Gruppe „machines" erstellt werden. OS/2- und Windows 9x-Clients brauchen kein solches Konto.

    Wir erstellen hier die Gruppe „machines" (nicht maschines !) mit der GID 222:

    groupadd –g 222 machines

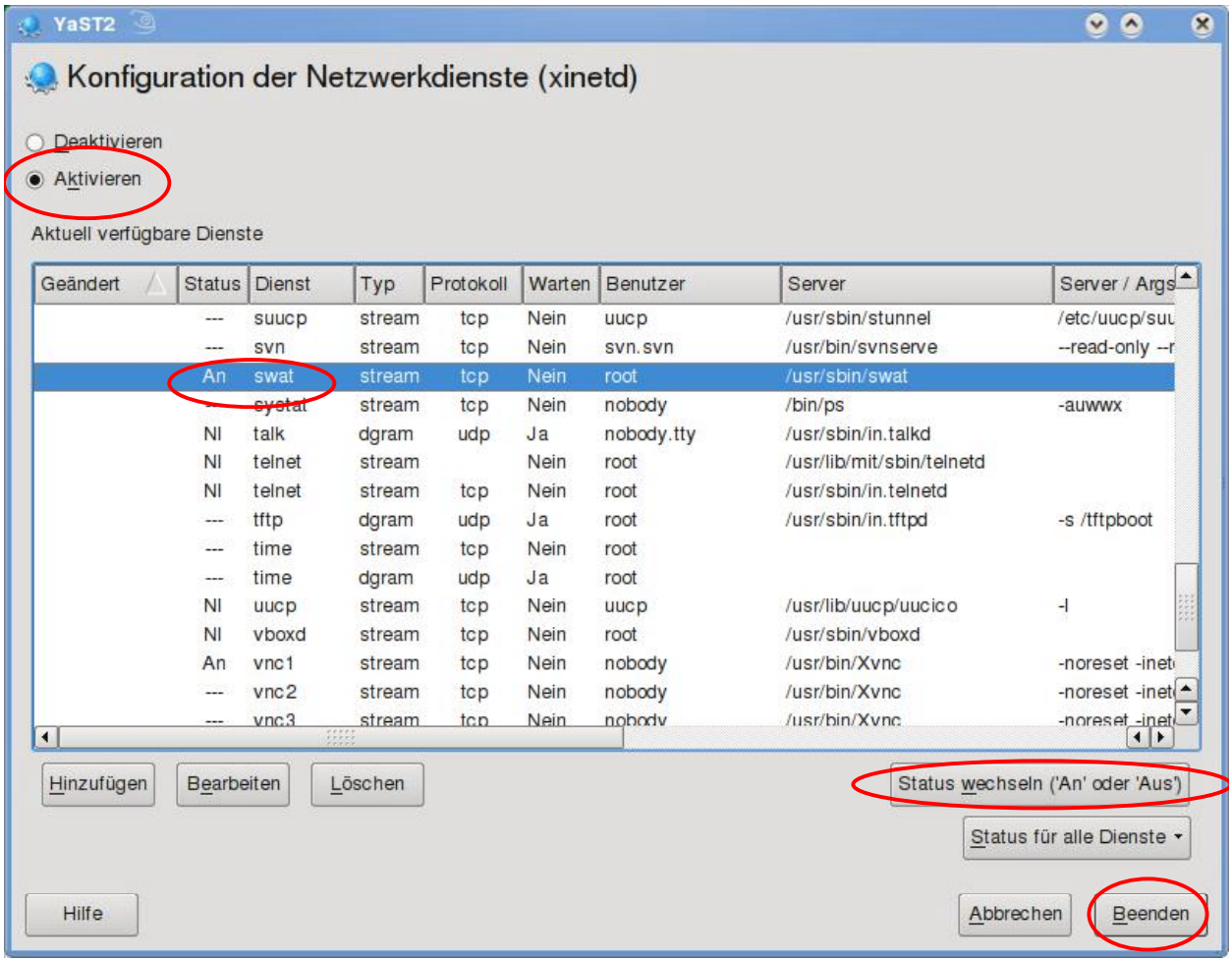
SWAT aktivieren

Zur Konfiguration von SAMBA benutzen SWAT (Samba Web Administration Tool), Dieses muss

erst aktiviert werden.

42. „Chamäleon“ --> (unten) Rechner --> (oben auf der Liste) YaST. Im YaST wählen wir nun:

(linke Spalte) **Netzwerkdienste** --> (rechts) **Netzwerkdienste (xinetd)**



Konfiguration der Netzwerkdienste (xinetd):
( ) Deaktivieren
(x) Aktivieren

(Suche und markieren Sie die Zeile mit SWAT in der alphabetisch sortierten Liste:)

Status	Dienst	Typ	Protokoll	Warten	Benutzer	Server
An	swat	stream	tcp	Nein	root	/usr/sbin/swat

[**Status wechseln (‚An’ oder ‚Aus’)**] (Klicken bis links ‚**An**’ erscheint, s. Bild oben)

[Beenden] (Fortan wird swat automatisch gestartet).

Hinweis 1: Bei einigen älteren SuSE Versionen(9.3, 10.1) wird swat nicht sofort gestartet, Dann geben Sie einfach folgenden Befehl ein**: rcxinetd restart**

Hinweis 2: swat ist standardmässig so eingestellt, dass es *nur von localhost* benutzt werden kann. Soll ein Zugriff übers Netzwerk erlaubt werden, muss dies in der Datei /etc/xinetd.d/swat geändert werden. Bei der 4-te Zeile muss das # Zeichen entfernt werden und die IP-Adressen ergänzt werden, die Zugriff haben sollen:

only_from = 127.0.0.1, 192.168.112.43 (Liste von berechtigten IP’s)

mit *rcxinetd restart* werden die neuen Angaben aktiviert.
Vorsicht: Die Daten gehen unverschlüsselt über das Netzwerk!

Konfiguration mit SWAT

43. Die Bedienung von SWAT erfolgt via Browser auf dem Port 901. Starten Sie dazu den Browser Konqueror (natürlich geht auch der Firefox). Dazu klicken Sie in der Schellstartleiste auf die Ikone mit der blauen Weltkugel mit Achsen.
Als Adresse geben Sie ein:

    localhost:901
    (es erscheint ein Anmeldefenster:)

    Authorisierung:
    Benutzername: **root**
    Passwort: **xxxxxxxxx**

    Melden Sie sich unbedingt an mit **root** und seinem Passwort (Ein Benutzer kann nur den Status abfragen, aber nichts ändern).

    Hinweis: Falls swat nicht läuft, erscheint die Meldung: „Die Aktion lässt sich nicht ausführen“. Gehen Sie in diesem Fall zurück zu vorherigen Schritt und starten Sie swat. Jetzt (ev. *rcxinetd restart* eingeben. Dann probieren Sie es erneut.

44. Es erscheint das Hauptbild von SWAT. Diese umfasst folgende Reiter:

    - **Home** Falls das Paket samba-doc mitinstalliert wurde, stehen ausführliche Hilfetexte und Dokumente zur Verfügung.
    - **Globals** Hier werden Parameter für den ganzen SAMBA gesetzt , z.B. die NetBios-Namen von Server und Domäne
    - **Shares** Definiert die Freigaben
    - **Printers** freigegebene Drucker
    - **Wizzard** benutzen wir nicht
    - **Status** Samba-Server starten/stoppen
    - **View** Anzeige der Konfigurationsdatei /etc/samba/smb.conf
    - **Password** Verwaltung der Samba-Passwörter /etc/samba/smbpasswd

Globale Einstellungen

45. Unter **Globals** definieren wir gleich zwei wichtige Parameter:

- Workgroup	**ANET31**	Dies wird der spätere Domänenname. Wählen Sie ihn *gleich, wie den ersten Teil* der DNS-Domäne
- NetBios name	**X31-LIN**	Dies ist der Servername. Wählen Sie ihn gleich wie den DNS Namen des Systems (s. Schritt 38).

    Hinweis: Beides sind NetBios Namen und werden meist gross geschrieben (an sich unterschiedet NetBios nicht zwischen Gross- und Kleinbuchstaben). Die beiden dürfen nicht gleich sein. Achten Sie darauf, dass es *keine* Windows Domäne gibt, deren Domänenname mit dem gleichen Namen beginnt (z.B. anet31.intern). Ebenso darf *kein* Windows-System den gleichen Computernamen haben! Die Workgroup ist das gleiche, wie eine Domäne: Eine Domäne hat einen Chef – den Domänen-Kontroller -, die Arbeitsgruppe hat keinen Chef.

46. Weitere Einstellungen in Globals
Damit die Änderungen beim Wechseln der Ansicht nicht verloren gehen (es ist eben eine Browser-Anwendung) speichern Sie die gemachten Anpassungen der NetBios Namen:
[**Änderungen speichern**]

Für die nächsten Einstellungen wechseln Sie in die
[Erweiterte Ansicht] Die meisten Einstellungen lassen Sie auf ihren Standards.

47. Blättern Sie zu den „**Sicherheitsoptionen**“
Dort sollten folgende Einstellungen bereits bestehen:

- security	[USER]	(Sicherheits basiert auf dem Benutzer)
- encrypt passwords	[Yes]	(mindestens die Passwörter werden verschlüsselt)

Blättern Sie (etwas) weiter zu:

- admin users	[root, fho]	(Diese Benutzer können Clients in der Domain eintragen)
- read list	[root, fho]	(diese Benutzer könne überall lesen)

- write list [root, fho] (diese Benutzer könne überall schreiben)

Hinweis: Lassen Sie „valid users“ leer (alle Anderen sind sonst invalid!)

48. Blättern Sie etwa 3 mal weiter bis zu den „**Login Options**“:

- add machine script (ergänzen Sie in diesem Feld:)
[**/usr/sbin/useradd -g machines -c “Windows Client“ -d /dev/null -s /bin/false %m\$**]

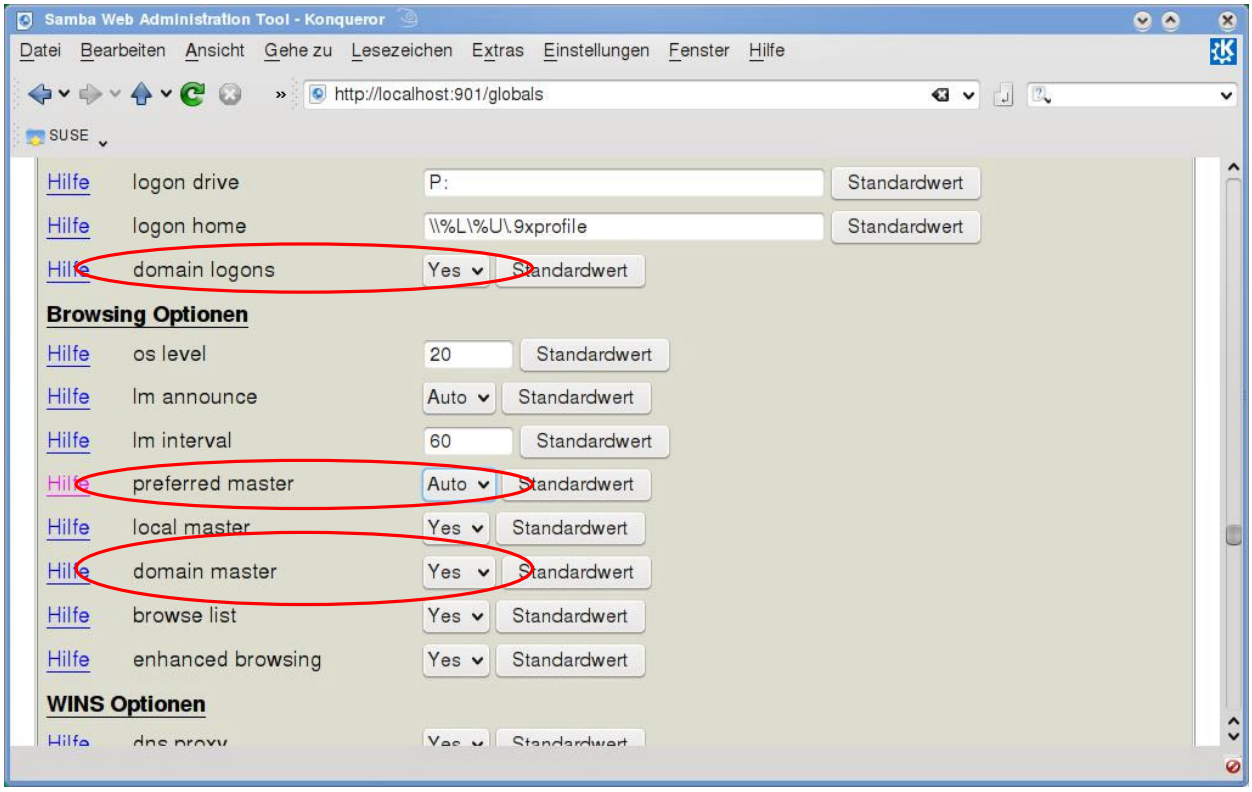
Hinweis 1: Dies erstellt beim Einbuchen von Clients mit Windows NT, 2000, XP, Vista ein Maschinen-Konto, das gleich heisst, wie der Computer, aber mit einem $-Zeichen angehängt. Dieser Befehl erstellt dieses Maschinen-Konto automatisch. Die Gruppe „machines“ haben Sie bereits im Schritt 41 erstellt.

Hinweis 2: Erscheint unter **SuSE 11.2** beim Beitreten zur Domain die Meldung, dass der Benutzername nicht gefunden wurde, sollte der add machine script geändert werden auf:

[**/usr/sbin/useradd -g machines -c “Windows Client“ -d /var/lib/nobody -s /bin/false %m\$**]

Definitionen als Domain Controller

Wir machen nun den SAMBA zum Domaincontroller. Dazu sind die Einträge „domain logons“ Yes und „domain master“ Yes wichtig. Der Eintrag „preferred master“ kann auf Yes gesetzt werden wenn kein anderen Server (SAMBA, Windows etc.) im Netzwerk dies bereits macht. Sonst empfiehlt sich die Einstellung Auto.



49. (kurz darunter:)
logon script [logonscr.cmd] (Dieser Logon-Script wird weiter unten erstellt)

50. (kurz darunter:)
domain logons [**Yes**] Samba funktioniert als Domain-Controller)

51. Blättern Sie weiter zu den „**Browsing Optionen**“
os level [60] Damit gewinnt SAMBA die Auswahl zum

	Masterbrowser gegenüber Windows Systemen. (Kann auch auf 20 belassen werden)
domain master [**Yes**]	SAMBA wird so zum Primary Domain Controller

52. Damit sind alle Globals Definitionen fertig. Sie werden gespeichert mit (ganz oben links): [**Änderungen speichern**]

SAMBA Benutzer und Gruppen definieren

Alle Benutzer von SAMBA müssen *zuerst* als Linux-Benutzer angelegt werden, *erst dann* wird ihnen zusätzlich ein SAMBA-Passwort zugewiesen. Beim Linux-Passwort wird ein Hashwert des Passwortes in der Datei /etc/shadow abgelegt, meist verschlüsselt mit MD5. In der Datei /etc/samba/smbpasswd wird der Hash des SAMBA-Passwortes abgelegt. Dieses ist gleich verschlüsselt, wie es die Windows Systeme machen. Damit kann SAMBA das Passwort der Windows-Clients überprüfen.

Wir definieren ein Paar Benutzer für den Samba und Gruppen für die Berechtigung an den Freigaben. Die Steuerung der Berechtigungen via Gruppen ist wesentlich übersichtlicher als die Vergabe von Berechtigungen an einzelne Benutzer.

Zuerst erstellen wir die Benutzer Hans und Eva, dann eine Gruppe smb-data und smb-apps. Mitglieder dieser Gruppen sollen alle Benutzer sein, welche auf den Freigaben DATA bzw. APPS Schreibrechte haben sollen.

53. Die Benutzer Benutzer hans und eva können per Befehl oder via Yast gemacht werden.
    Chamäleon → Rechner → YaST
    (Es wird das Passwort von root verlangt).

    (links) Sicherheit und Benutzer → (rechts) Benutzer- und Gruppenverwaltung
    (Es erscheint ein Fenster mit dem Benutzer fho, der bereits bei der Installation erstellt wurde.)

    [Hinzufügen] (unten links)

    Vollständiger Name des Benutzers: [Hans Muster]
    Benutzername: [hans] (Kleinbuchstaben)
    Passwort: [xxxxxxxxxx]
    Passwort bestätigen: [xxxxxxxxxx]
    [ ] Systemmail empfangen
    [ ] Benutzername deaktivieren

    [OK]

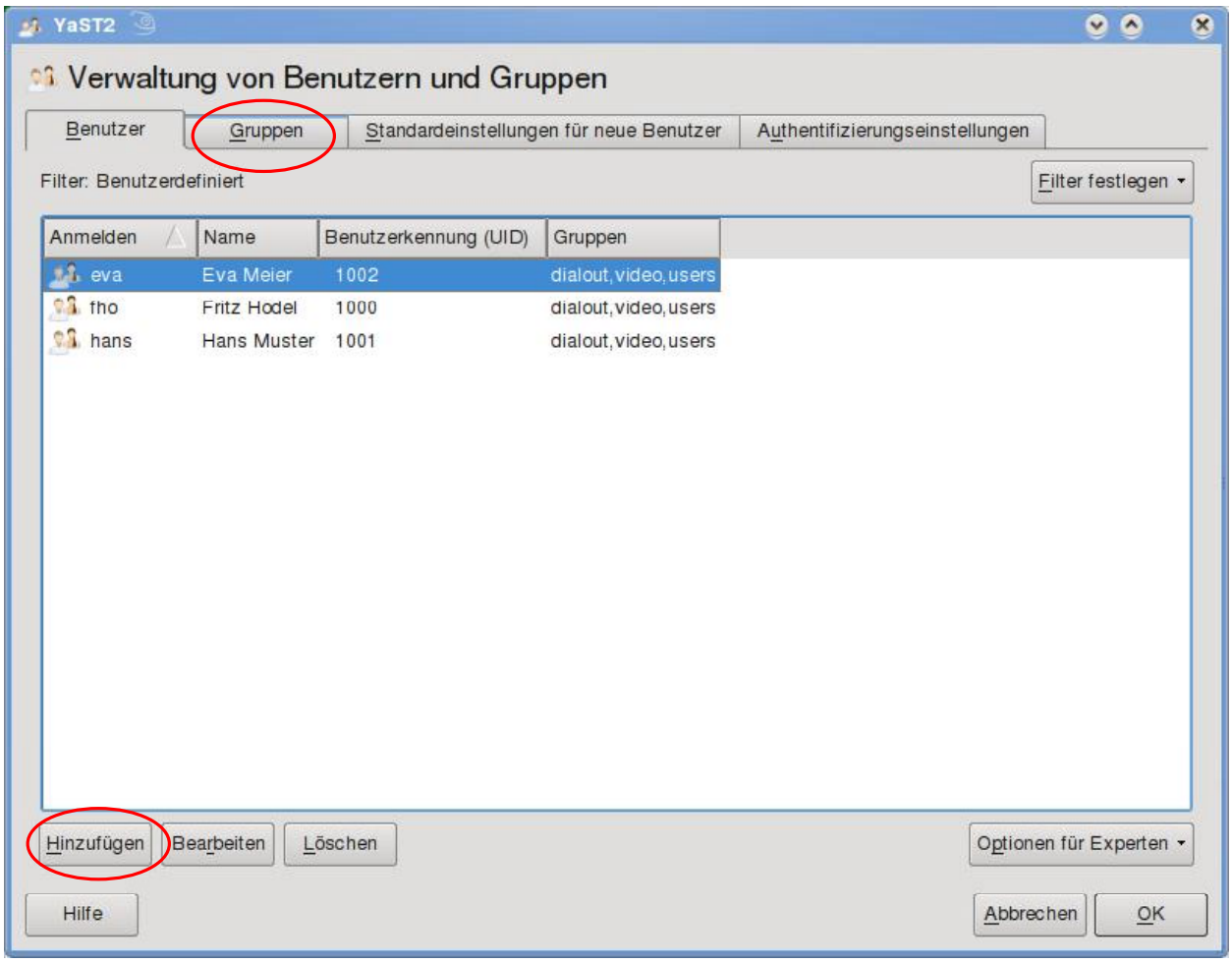
    (erstellen Sie nun den Benutzer eva genau gleich:)

    [Hinzufügen] (unten links)

    Vollständiger Name des Benutzers: [Eva Meier]
    Benutzername: [eva] (Kleinbuchstaben)
    Passwort: [xxxxxxxxxx]
    Passwort bestätigen: [xxxxxxxxxx]
    [ ] Systemmail empfangen
    [ ] Benutzername deaktivieren

    [OK]

    Die beiden Benutzer werden standardmässig Mitglieder der Gruppen dialout, video, audio (falls eine Soundkarte eingebaut ist) und users. Das Bild sollte nun wie im folgenden Beispiel aussehen:



54. Nun werden die Gruppen smb-data und smb-apps erstellt.
In der Benutzerverwaltung klicken Sie auf den Reiter [**Gruppen**]

[Hinzufügen]

Neue lokale Gruppe

Name der Gruppe:	[smb-data	]	
Gruppen-ID (gid):	[1000	]	
Passwort:	[	]	(leer lassen)
Passwort bestätigen:	[	]	(leer lassen)

(dann rechts folgende Benutzer markieren:)

[x]	eva
[x]	fho
[x]	hans

[OK]

Nun wird die Gruppe smb-apps erstellt, hier ist nur fho Mitglied:

[Hinzufügen]

Neue lokale Gruppe

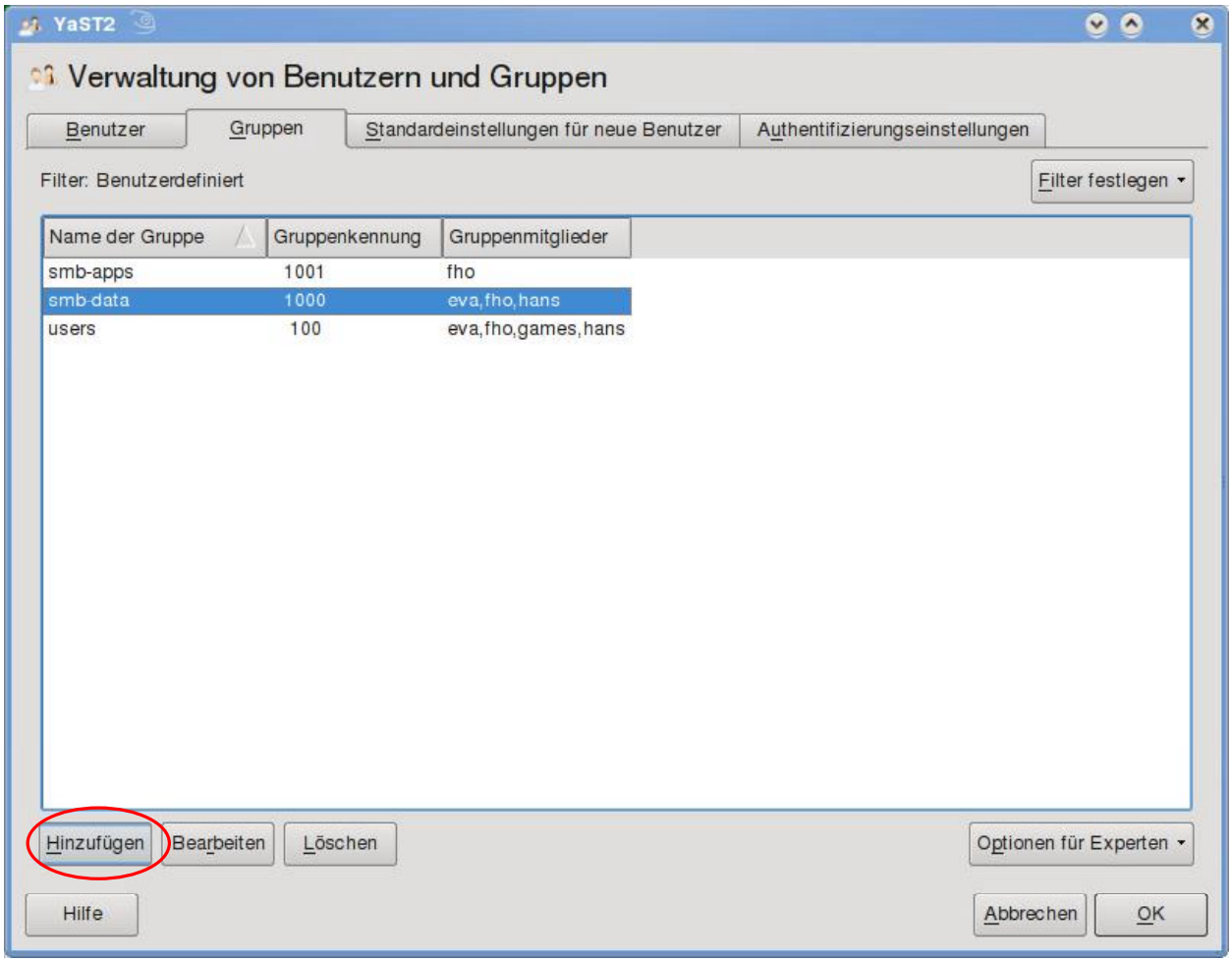
Name der Gruppe:	[smb-apps	]	
Gruppen-ID (gid):	[1001	]	
Passwort:	[	]	(leer lassen)
Passwort bestätigen:	[	]	(leer lassen)

(dann rechts folgenden Benutzer markieren:)

[x] fho

[OK]

Das Bild sollte nun wie im folgenden Beispiel aussehen:



[OK]

55. Die Linux-Benutzer sind erstellt und den Gruppen zugewiesen. Nun müssen Sie noch ein Samba-Passwort bekommen. Dies machen Sie am besten in SWAT:

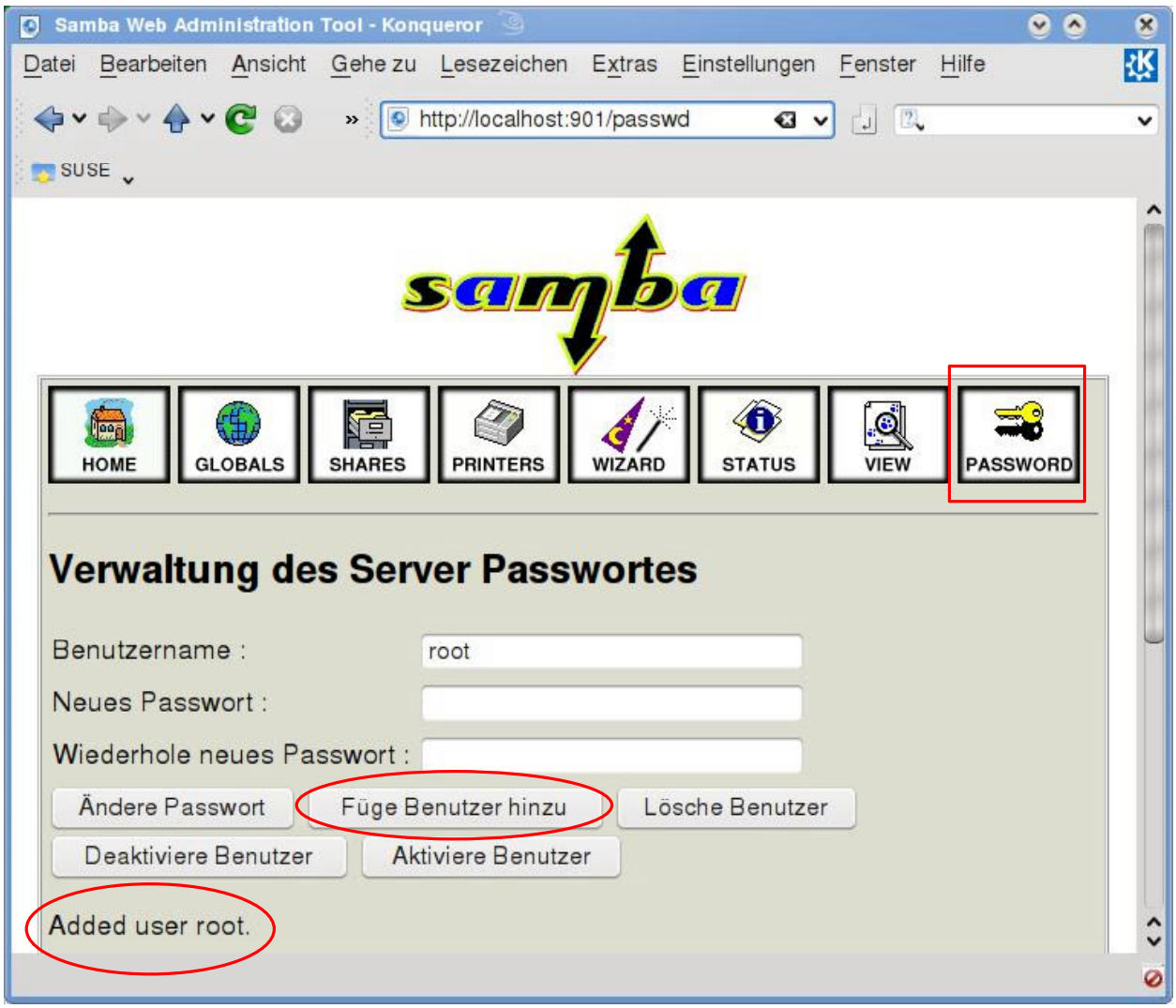
    localhost:901
    (Anmelden als root)

    Reiter [**Password**]

    Benutzername: [root]
    Neues Passwort: [xxxxxxxx] (gleich oder anders als im Linux)
    Wiederhole neues Passwort: [xxxxxxxx]
    [Füge Benutzer hinzu]

    (es erscheint eine Meldung, dass Konqueror das Passwort speichern könne → [Nein]

    Hinweis: Unter den Knöpfen muss nun die Meldung „**added user root**“ erscheinen, sonst ging es nicht.



Genau gleich weisen wir den Benutzern fho, hans und eva ein Samba-Passwort zu.

Benutzername:	[fho	]	
Neues Passwort:	[xxxxxxxx	]	(gleich oder anders als im Linux)
Wiederhole neues Passwort:	[xxxxxxxx	]	
[Füge Benutzer hinzu]			

Benutzername:	[hans	]	
Neues Passwort:	[xxxxxxxx	]	(gleich oder anders als im Linux)
Wiederhole neues Passwort:	[xxxxxxxx	]	
[Füge Benutzer hinzu]			

Benutzername:	[eva	]	
Neues Passwort:	[xxxxxxxx	]	(gleich oder anders als im Linux)
Wiederhole neues Passwort:	[xxxxxxxx	]	
[Füge Benutzer hinzu]			

Kontrollieren Sie immer, ob die Meldung „added user xxxx“ erscheint!

Erster Test von Samba

Wir haben nun die Globalen Einstellungen von SAMBA gemacht und auch ein paar Benutzer definiert. Da bereits einige Freigaben vordefiniert sind, können wir Samba ein erstes Mal testen

56. Klicken Sie im SWAT auf den Reiter [**Status**]

smbd:	aktiv	[Starte smbd]	[**Neustart smbd**]	(hier klicken)
nmbd:	aktiv	[Starte nmbd]	[**Neustart nmbd**]	(hier klicken)
winbindd:	inaktiv	[Starte winbindd]	[Neustart winbindd]	

Am Schluss sollten smbd und nmbd aktiv sein, Der winbindd wird nicht benötigt.

57. Öffnen Sie ein Befehlsfenster (Terminal):
Camäleon → Favoriten → Terminal

su -
(das Passwort von root wird verlangt)

smbclient -L localhost [Enter] (grosses L beachten!)
Enter roots's Password:
(geben Sie das Samba-Passwort von root ein) xxxxxxx

Es erscheint eine Liste der Freigaben und Domänen:

```
Domain=[ANET31] OS=[Unix] Server=[Samba 3.2.4-5.2-1985-SUSE-CODE11]
        Sharename       Type      Comment
        ---------       ----      -------
        profiles        Disk      Network Profiles Service
        users           Disk      All users
        groups          Disk      All groups
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 3.2.4-5.2-1985)
        root            Disk      Home Directories
Domain=[ANET31] OS=[Unix] Server=[Samba 3.2.4-5.2-1985-SUSE-CODE11]
        Server               Comment
        ---------            -------
        X31-LIN              Samba 3.2.4-5.2-1985-SUSE-CODE11

        Workgroup            Master
        ---------            -------
        ANET31               X31-LIN
```

Hinweis 1: Es erschienen die Standradfreigaben für Drucker und zur Verwaltung. Der Name des Server X31-LIN und der Domäne ANET31 werden angezeigt. Erscheinen nur die Freigaben probieren Sie: **smbclient –L 192.168.112.32**
Hinweis 2: Falls nicht benötigt (heute meistens der Fall) kann auch IP Version 6 deaktiviert werden (s. Schritt 38). Dies benötigt einen Neustart.
Hinweis 3: Falls der nmb nicht gestartet werden kann (Anzeige „inaktiv" in SWAT → Status), prüfen Sie, ob ein Netzwerkkabel angeschlossen ist. Nach dem Anschliessen ca. 1 Minute warten und den nmb neu starten mit **rcnmb restart** und den smbclient Befehl erneut probieren.

Freigaben (Shares) einrichten

Die eigenen Freigaben können nun definiert werden und gleich die Berechtigungen gesetzt werden, da wir die Benutzer und Gruppen bereits haben. Für folgende Freigaben sind die Verzeichnisse bereits erstellt worden (s. Schritt 40):

- DATA (alle Benutzer dürfen lesen und schreiben)

- APPS (alle Benutzer dürfen lesen, root und fho auch schreiben)
- PUBLIC (Alle dürfen lesen und schreiben)
- NETLOGON (Alle dürfen Lesen, fho und root auch schreiben)

58. Starten Sie SWAT (falls es nicht mehr läuft):

    localhost:901
    (Anmelden als root)

    Reiter [**Shares**] klicken

59. Freigabe NETLOGON erstellen

    Aktuelle Konfiguration (x) Einfache Ansicht ( ) Erweiterte Ansicht
    [Erstelle Freigabe] **netlogon** (Namen eingeben und [Erstelle Feigabe] klicken)

    Basisoptionen:
    comment: [Logonscripte auf Linux-Server]
    path **[/export/samba/netlogon**] (muss genau dem bereits erstellten Verzeichnis entsprechen!)
    read only [Yes] (nur Lesezugriff)

    Browsing Optionen
    browseable [Yes] (Inhalt kann angezeigt werden)

    Verschiedene Optionen
    availlable [**Yes**] (sonst nicht benutzbar)

    (oben links):
    [**Änderungen speichern**]

    Nun passe wir die Schreibrechte an:
    [Erweiterte Ansicht]

    Sicherheitoptionen
    username (leer lassen)
    invalid users (leer lassen)
    valid users (leer lassen)
    admin users (leer lassen)
    read list [**@users**] (Leszugriff für Gruppe *users*, **@** beachten!)
    write list [**root, fho**] (Schreibzugriff *für root* und *fho*)

    (oben links):
    [**Änderungen speichern**]

    Damit ist die Freigabe Netlogon erstellt. Die Benutzer dürfen lesen, aber nicht schreiben (so könnten schädliche Befehle eingetragen werden).

    Hinweis: Die Freigabe für die Logonscripte *muss* NETLOGON heissen, da die Windows Clients beim Logon an der Domäne genau diesen Namen suchen.

60. Freigabe DATA erstellen:

    [Erstelle Freigabe] **data** (Namen eingeben und [Erstelle Feigabe] klicken)

    Basisoptionen:
    comment: [Dokumente auf Linux-Server]

path **[/export/samba/data**] (muss genau dem bereits erstellten Verzeichnis entsprechen!)
read only [**No**] (=schreiben erlaubt!)

Browsing Optionen
browseable [Yes] (Inhalt kann angezeigt werden)

Verschiedene Optionen
availlable [**Yes**] (sonst nicht benutzbar)

(oben links):
[**Änderungen speichern**]

Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen
username (leer lassen)
invalid users (leer lassen)
valid users (leer lassen)
admin users (leer lassen)
read list [**@users**] (Leszugriff für die Gruppe *users*)
write list [**@smb-data**] (Schreibzugriff für die Gruppe *smb-data*)

(oben links):
[**Änderungen speichern**]

Hinweis: Bei der read und write list können mehrere *Gruppen* und *Benutzer* angegeben werden, jeweils durch Komma getrennt. Bei Gruppennamen muss ein **@** vorangestellt werden! Also z.B. @smb-data, fho, hans.

61. Erstellen der Freigabe APPS:

[Erstelle Freigabe] **apps** (Namen eingeben und [Erstelle Feigabe] klicken)

Basisoptionen:
comment: [Programme auf Linux-Server]
path **[/export/samba/apps**] (muss genau dem bereits erstellten Verzeichnis entsprechen!)
read only [**yes**] (=nur lesen erlaubt!)

Browsing Optionen
browseable [Yes] (Inhalt kann angezeigt werden)

Verschiedene Optionen
availlable [**Yes**] (sonst nicht benutzbar)

(oben links):
[**Änderungen speichern**]

Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen
username (leer lassen)
invalid users (leer lassen)

valid users		(leer lassen)
admin users		(leer lassen)
read list	[**@users**]	(Leszugriff für die Gruppe *users*)
write list	[**@smb-apps**]	(Schreibzugriff für die Gruppe *smb-apps*)

(oben links):
[**Änderungen speichern**]

62. Als letztes folgt die Feigabe PUBLIC als Tauschbox:

[Erstelle Freigabe] **public** (Namen eingeben und [Erstelle Feigabe] klicken)

Basisoptionen:

comment:	[Tauschbox auf Linux-Server]	
path	**[/export/samba/public**]	(muss genau dem bereits erstellten Verzeichnis entsprechen!)
read only	[**No**]	(=schreiben erlaubt!)

Browsing Optionen

browseable	[Yes]	(Inhalt kann angezeigt werden)

Verschiedene Optionen

availlable	[**Yes**]	(sonst nicht benutzbar)

(oben links):
[**Änderungen speichern**]

Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen

username		(leer lassen)
invalid users		(leer lassen)
valid users		(leer lassen)
admin users		(leer lassen)
read list	[**@users**]	(Leszugriff für die Gruppe *users*)
write list	[**@users**]	(Schreibzugriff für die Gruppe *users*)

(oben links):
[**Änderungen speichern**]

Freigaben testen

Nun sind alle Freigaben definiert und wir können sie testen. Wir testen zuerst vom Linux-Server aus, dann von einem Windows-Client.

63. Test vom Linux-Server aus.

Öffnen Sie eine Befehlszeile:

Chamäleon → Favoriten → Terminal

su -
(Passwort von root wird verlangt)

Wir starten den smbd neu, damit die Änderungen übernommen werden:

rcsmb restart [Enter] (oder Neustart via Status im SWAT)

smbclient -L localhost [Enter] (grosses L beachten!)
Enter roots's Password:
(geben Sie das Samba-Passwort von root ein) xxxxxxx

In der Liste sollten nun auch Ihre selber definierten Freigaben erscheinen:
- netlogon
- data
- public
- apps

Falls nicht, wurde möglicherweise unter *Verschiedene Optionen* der Parameter „available Yes" vergessen oder der smbd wurde nicht neu gestartet.

```
Domain=[ANET31] OS=[Unix] Server=[Samba 3.2.4-5.2-1985-SUSE-CODE11]
        Sharename       Type      Comment
        ---------       ----      -------
        profiles        Disk      Network Profiles Service
        users           Disk      All users
        groups          Disk      All groups
        print$          Disk      Printer Drivers
        netlogon        Disk      logonscripte auf Linux-Server
        data            Disk      Dokumente auf Linux-Server
        public          Disk      Tauschbox auf Linux-Server
        apps            Disk      Programme auf Linux-Server
        IPC$            IPC       IPC Service (Samba 3.2.4-5.2-1985)
        root            Disk      Home Directories
Domain=[ANET31] OS=[Unix] Server=[Samba 3.2.4-5.2-1985-SUSE-CODE11]
        Server               Comment
        ---------            -------
        X31-LIN              Samba 3.2.4-5.2-1985-SUSE-CODE11
        Workgroup            Master
        ---------            -------
        ANET31               X31-LIN
```

64. Nun folgt der Test von einem Windows Client aus. Beachten Sie, dass Sie gegenüber einem Server immer nur *EIN* Benutzer für alle Freigaben sein können. Wollen Sie die gleiche Freigabe mit einem anderen Benutzer testen. Müssen Sie alle Freigaben von diesem Server erst abhängen.

    Setzen Sie sich an einen Windows Client (z.B. Windows XP) und öffnen Sie eine Befehlszeile (MS DOS Fenster):

    Start → Ausführen → cmd.exe [Enter]

    net use (zeig die Momentan benutzten Freigaben an. es sollte keine vom Linux-Server dabei sein)

    net view \\x31-lin (zeigt alle Freigaben vom Linux-Server an,
    ausser diejenige, die mit einem $ enden)

    Hinweis: sollten keine Freigaben angezeigt werden, kann dies zwei Ursachen haben:

- Stoppen Sie den Firewall auf dem Server: **rcSuSEfirewall2 stop**
  (Gross-/Kleinschreibung beachten!)
- Sie sind auf dem **Windows-System** als Benutzer angemeldet, der keine Rechte auf dem SAMBA hat.

```
C:\>net view \\x31-lin

Freigegebene Ressourcen auf \\x31-lin
Samba 3.2.4-5.2-1985-SUSE-CODE11
Freigabename  Typ     Verwendet als  Kommentar
-------------------------------------------------------------------
apps          Platte                 Programme auf Linux-Server
data          Platte                 Dokumente auf Linux-Serve
fho           Platte                 Home Directories
groups        Platte                 All groups
netlogon      Platte                 logonscripte auf Linux-Server
profiles      Platte                 Network Profiles Service
public        Platte                 Tauschbox auf Linux-Serve
users         Platte                 All users
Der Befehl wurde erfolgreich ausgeführt.
```

65. Nun hängen wir die Freigabe DATA als Laufwerk X: an:

    net use x: \\x31-lin\data /user:hans *
    (es wird das Samba-Passwort von Hans verlangt)
    Der Befehl wurde erfolgreich ausgeführt

    Nun sollten Sie im Explorer ein Laufwerk x: sehen. Öffnen Sie dieses und testen Sie, ob Sie schreiben und lesen können:

    echo nur ein Test > x:\test.txt (erstellt eine Datei test.txt auf x:)
    Erscheint eine Meldung „Zugriff verweigert“ hat hans kein Schreibrecht auf x:

    dir x: (zeigt die Dateien auf x: an)

66. Nun hängen wir zusätzlich die Freigabe NETLOGON an. Hier darf hans *nicht* schreiben:

    net use y: \\x31-lin\netlogon (wir sind immer noch hans!)
    echo nur ein Test > y:\test.txt
    Zugriff verweigert (hans darf *nicht* schreiben!)

67. Nun hängen wir die Freigaben wieder ab, um sie als anderer Benutzer wieder anzuhängen:

    net use * /d (hängt alle Freigaben ab)
    y (Sicherheitsabfrage bestätigen)

    Nun hängen wir NETLOGON als root an, damit wir den Logonscript dort schreiben dürfen:

    net use z: \\x31-lin\netlogon /user:root *
    (Samba-Passwort von root wird verlangt)

    Nun (als root) sollte das Schreiben auf dem Laufwerk z: möglich sein.

Logonscript erstellen

Der Logonscript muss auf der Freigabe NETLOGN gespeichert werden. Seinen Namen haben wir unter Globals im SWAT bereits definiert:

68. Wir erstellen eine Datei **logonscr.cmd** auf dem Laufwerk z: (Netlogon)
    Öffnen Sie im Explorer das Laufwerk z:

→ drücken Sie die rechte Maustaste → neu → Textdokument

Nennen Sie das neue Dokument **logonscr.cmd** (die Warnung wegen der Änderung auf *.cmd können Sie ignorieren):

Nun wird die Datei logonscr.cmd bearbeitet:

Markieren Sie die Datei **logonscr.cmd** → rechte Maustaste → **Bearbeiten**
Schreiben Sie nun folgende Befehle rein:

```
@echo  off                                  (unterdrückt unnötige Meldungen)
net  use  k:   /d  > nul                    (hängt ein allfälliges k: ab)
net  use  l:   /d  >  nul
net  use  n:  /d  >  nul
net  use  lpt3  /d > nul                    (hängt den Drucker am LPT3 ab)

net  use  k:  \\x31-lin\data    /p:no       (häng DATA als K: an)
net  use  l:   \\x31-lin\apps   /p:no       (hängt APPS als L: an)
net  use  n:  \\x31-lin\public  /p:no       (hängt PUBLIC als N: an)
net  use  lpt3  \\x31-lin\laserjet          (hängt den Drucker an LPT3 an,
                                            diese wird erst weiter unten definiert)
net  time  \\x31-lin  /set  /y              (Client übernimmt Zeit vom Server)

net  use                                    (zeigt die benutzten Freigaben an)
pause                                       (Weiterfahren mit Leertaste)
```

Hinweis 1: Soll der Script auch über Router hinweg funktionieren können Sie den Server-Namen durch die IP-Adresse ersetzen, z.B. :
net use k: \\192.168.112.32\data   /p:no

Hinweis 2: Das /p:no (persistent:no) bewirkt, dass der Windows-Client die Verbindungen *nicht* speichert. So wird verhindert, dass beim Anmelden unterwegs (wenn der Server nicht erreichbar ist) lästige Fehlermeldungen betreffend nicht verfügbarer Laufwerke kommen.

Hinweis 3: Natürlich können Sie den Logon-Script auch auf dem Linux-Server selbst im Verzeichnis /export/samba/netlogon erstellen. Beachten Sie aber, dass Linux am Zeilenende nur ein „Line feed“ Zeichen macht, Windows aber „Carriage return“ *und* „Line feed“ möchte (sonst erscheinen im Windows alle Befehle auf einer langen Zeile). Sie können den Logonscript mit dem Program **kwrite** erstellen/bearbeiten und vor dem Abspeichern den Reiter [Settings] → Configure Editor → Open/Save → End of Line: DOS/Windows angeben. Die Linux-Editoren machen fortan die Zeilenenden in DOS-Manier.

69. Sie können nun den LogonScript testen. Das Laufwerk z: mit NETLOGN ist vom letzten Schritt noch angehängt. Öffnen sie eine Befehlszeile (MS-Dos Fenster):
z: [Enter]
logonscr.cmd [Enter]

Wenn der Script bis zur Pause durchläuft, sollten Sie nun die Laufwerke K:, L: und N: haben.

Gratuliere, der Logonscript funktioniert!

Drucker einrichten

Damit alle Clients drucken können, richten wir noch einen Drucke ein. Dieser wird standardmässig von SAMBA freigegeben. Im LogonScript hängen wir den Drucker LASERJET an den Port LPT3 an. Auf dem Client muss deshalb ein (lokaler) Druckertreiber am Anschluss LPT3 installiert werden.

70. Wir richten einen Drucker mit eingebauter Netzwerkkarte ein, Die IP-Adresse und das Modell müssen bekannt sein:

Chamäleon → Rechner → YaST

(links) Hardware → (rechts) **Drucker** (klicken)

Druckerkonfiguration
Anzeigen [x] Lokal [x] Entfernt
[Hinzufügen] (Druckerdatenbank wird geöffnet, dauert eine Weile...)

Neue Druckerkonfiguration hinzufügen
(rechts oben:) [**Verbindungsassistent**]

Verbindungsassistent
- Direkt verbundenes Gerät
  - Parallel Port
  - USB-Port
  - Bluetooth
  - SCSI
  - HP-Geräte (HPLIP)
- Zugriff auf Netzwerkdrucker
  - **TCP-Port (AppSocket/JetDirect)** ← (hier klicken)
- Via Printserver-Maschine drucken
  - Microsoft Windows/SAMBA (SMB/CIFS)
  - Traditionelle Unix-Server (LPR)
  - CUPS-Server
  - Novell Netware Printserver (IPX)
- Speziell

(Dann rechts eingeben:)

Verbindungseinstellungen
IP-Address or Hostname: [**192.168.112.134**]
TCP-Portnummer: [9100]
[Verbindung testen]
Select the Printer Manufacturer [**HP**]
[OK]

Neue Druckerkonfiguration hinzufügen

Modell	Verbindung	Beschreibung
HP	socket://192.168.112.134	created by the connection wizzard

Treiber festlegen
(passendes Modell markieren)

Namen setzen: [**laserjet**] (alles Kleinbuchstaben!)
[OK]

Hinweis: Fehlt das genaue Druckermodell kann meist ein Vorgängermodell gewählt werden. Auf jeden Fall muss der Drucker dir *gleiche Druckersprache* beherrschen: PS (PostScript), PCL 5, PCL6 etc.

Druckerkonfiguration:

Konfiguration	Name	Beschreibung	
lokal	laserjet	HP LaserJet 13xx	(markieren)

[**Testseite drucken**] (etwas warten, bis Drucker aufgewärmt ist und startet)
[OK]

Standardmässig ist der Drucker bereits unter seinem Namen (hier: laserjet) freigeben. Sie können dies überprüfen mit:

smbclient -L localhost

Der Drucker müsste nun aufgeführt sein und auch im Logonscript müste er als LPT3 angehängt werden (sonst: überprüfen Sie den Freigabenamen im Script).

Hinweis 1: Sie müssen nun auf den Windows-Clients ab CD/Diskette einen passenden Treiber für diesen lokalen Drucker auf den Anschluss LPT3 installieren. Wenn Sie keine Diskette/CD mehr benutzen wollen: (s. folgenden Hinweis).

Hinweis 2: Sie können den Drucker auf einem ersten Windows XP manuell auf den Anschluss LPT3 installieren, die weitern können den Treiber vom SAMBA beziehen. Dazu kopieren Sie alle Treiberdaten in die Freigabe **print**$. Das ist auf dem SAMBA-Server unter:
/var/lib/samba/drivers
Suchen Sie auf dem Windows-Client folgendes Verzeichnis:
\Windows\System32\spool\drivers
Kopieren Sie alle Daten und Verzeichnisse vom Windows Client (je nach Drucker):
- Color (bei Farbdruckern)
- w32x86 (32-bit Treiber)
- w32x83\3 (Version 3 Treiber für Win2000, WinXP, ME)
- w32x86\2 (Version 2 Treber, eigentlich für NT)

Samba automatisch starten

Damit SAMBA fortan automatisch gestartet wir, geben wir dies im Runlevel Editor an. SAMBA benötigt natürlich ein funktionierende Netzwerk. Das ist im Runlevel 3 und 5 gegeben.

71. Starten Sie YaST mit:
Chamäleon → Rechner → YaST
(Passwort von root wird verlangt)
(links) System → (rechts) **Systemdienste (Runlevel)**

Systemdienste (Runlevel): Dienste
( ) Einfacher Modus (x) Expertenmodus (Expertenmodus klicken)

Suchen und makieren Sie nun die Zeilen:
- **nmb** (markieren)
[Anwenden/Zurücksetzen] → [**Dienst aktivieren**] (es sollten 3 5 erscheinen)
- **smb** (markieren)
[Anwenden/Zurücksetzen] → [**Dienst aktivieren**] (es sollten 3 5 erscheinen)
[OK]
[Ja] (Änderungen speichern)

Fortan wir SAMBA beim Einschalten *automatisch* gestartet.

Firewall anpassen

Vergessen Sie nicht, den Firewall zu deaktivieren oder (besser) die Ports 137, 138, 139 und 445 freizuschalten. Dise sind via YaST -->Sicherheit und Benutzer --> Firewall unter „erlaubte Dienste“ mit SAMBA zusammengefasst. Sonst müssen Sie jedes Mal den Firewall manuell stoppen mit *rcSuSEfirewall2 stop*.

72. Starten Sie YaST:

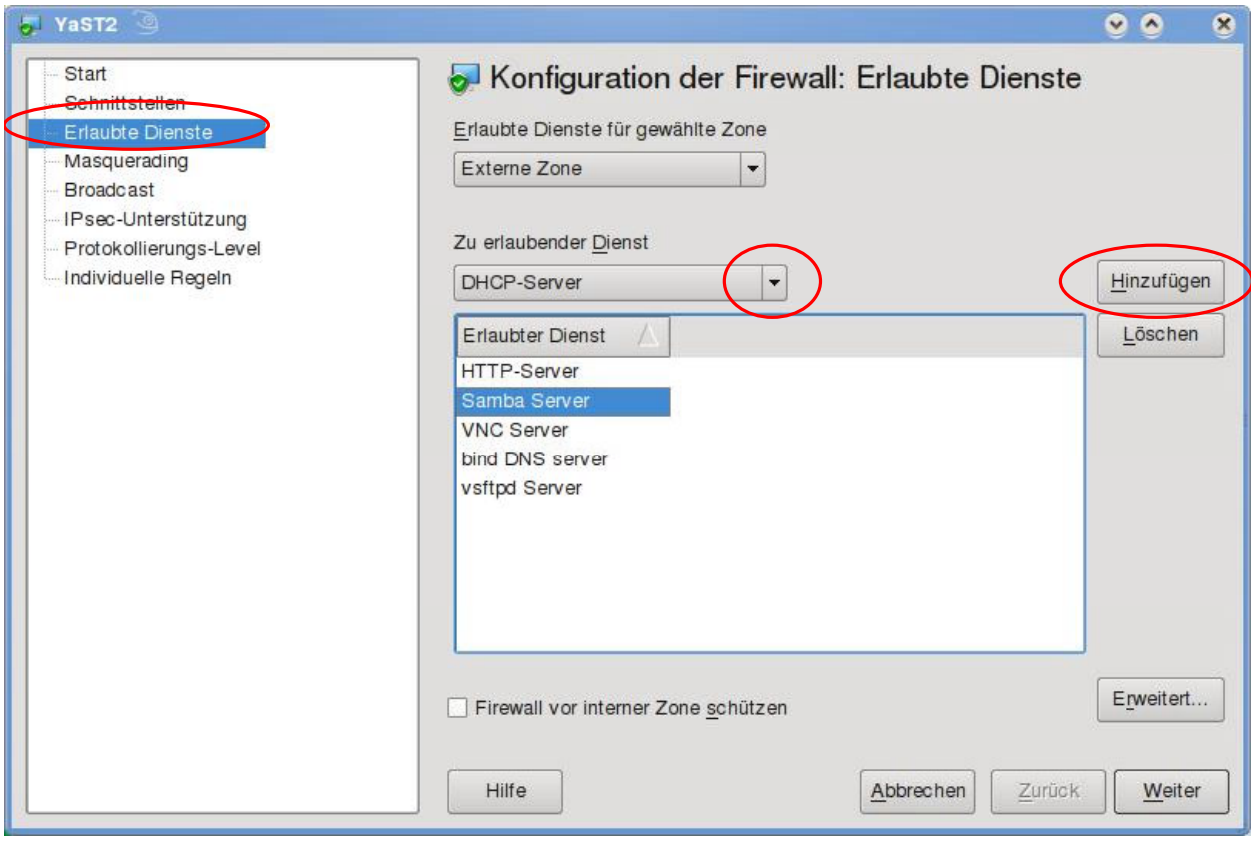
Chamäleon → Rechner →YaST
(Passwort von root wird verlangt)

(links) Sicherheit und Benutzer → (rechts) **Firewall** (klicken)

73. Konfiguration der Firewall: Erlaubte Dienste
(links) Erlaubte Dienste → (rechts) Zu erlaubender Dienst (blättern)

- HTTP-Server	[Hinzufügen]	(für den Apache2)
- Samba Server	[Hinzufügen]	
- VNC-Server	[Hinzufügen]	(zum Fernsteuern)
- bind DNS Server	[Hinzufügen]	(für den Name-Server)
- vsftp-Server	[Hinzufügen]	(für den FTP-Server)

[Weiter]
[Beenden]



Einbinden von Windows-Clients

Clients ab Windows NT benötigen ein Maschinen-Konto, das gleich heisst, wie der Computer, mit eingehängtem $-Zeichen (also z.B. **PC28$** für den PC mit dem N z.B. PC28$ für den PC mit dem Namen PC28). *Im Schritt 48 h*aben wir einen add machine script für das automatische Einbuchen in die Domäne erstellt. Dazu wird die Variable %m verwendet, bei der – ohne Leerzeichen – ein $ angehängt wird. Das macht der Ausdruck **%m\$** (dabei ist der \ das Escape-Zeichen, damit der $ *ohne* Abstand angehängt wird).

OS/2, Windows 9x und DOS-Clients benötigen *kein* Maschinen-Konto.

Einbinden eines Windows 2000 Clients

Ein Windows 2000 Client kann in der Domäne eingebucht werden. Dann kann man sich als irgend ein Benutzer in der SAMBA-domäne anmelden und der LogonScript wird automatisch

ausgeführt.

74. Melden sie sich *lokal* am Client als Administrator an. Dann öffnen sie die Systemsteuerung:
    Start --> Einstellungen --> Systemsteuerung --> System
    (wählen sie den Reiter) [**Netzwerkidentifikation**] --> Eigenschaften

    markieren Sie im Fenster Mitglied von: [x] Domäne : [**anet31**]
    [ok]

    Geben sie als Benutzer root (oder einen anderen Benutzer aus *admin users*) und sein Passwort ein. Nach einiger Zeit erscheint die Meldung:

    Willkommen in der Domäne ANET31

75. Nach einem Reboot können sie sich in der Domäne anmelden. Dabei sollte der LogonScript ausgeführt werden (angehängte Freigaben kontrollieren).

Einbinden eines Windows XP pro und 7 pro Clients

Windows XP/7 pro kann eingebucht werden, Windows XP/7 home Clients können dies aber *nicht* (by design). Auch ein WindowsXP pro Client benötigt ein Maschinenkonto. Windows 7 benötigt zusätzlich noch zwei Registry Einträge:

```
HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
     DWORD DomainCompatibilityMode=1
     DWORD DNSNameResolutionRequired=0
```

76. Melden sie sich *lokal* am XP pro Client als Administrator an. Dann öffnen sie die Systemsteuerung:
    Start --> Systemsteuerung --> Leistung und Wartung --> System
    Reiter [**Computername**]

    (unten rechts): [Ändern]

    Computernamen ändern
    Computername: [wsanet17] (kann bestehen bleiben)
    Mitglied von
    (x) Domäne: [**ANET31**]
    [OK]

77. Geben sie als Benutzer root (oder einen anderen Benutzer den *admin users*) und sein Passwort ein. Nach einiger Zeit erscheint die Meldung:

    Willkommen in der Domäne ANET31

78. Nach einem Reboot können sie sich in der Domäne anmelden:

    Ctrl+Alt+Del

    Benutzer [fho]
    Kennwort [xxxxx]
    >> **Optionen**
    Anmelden an: [anet31]
    [OK]

Hinweis 1: Kann die Maschine nicht in der Domäne eingetragen werden, weil die Domäne nicht gefunden wird, können Sie erst mal folgendes machen:
- den Firewall stoppen: rcSuSEfirewall2 stop
- Server erreichbar: ping 192.168.112.32
- prüfen, ob der Server sichtbar ist: net view \\x31-lin
- eine Freigabe vom Server anhängen: net use z: \\192.168.112.32\netlogon

Hinweis 2: Prüfen Sie, ob in /etc/samba/smb.conf in der Sektion [Globals] folgende Einträge gemacht und korrekt sind:
- workgroup = CHANET17 (= Domänenname)
- domain logons = Yes
- preferred master = Yes oder Auto
- domain master = Yes
- add machine script = /usr/sbin/useradd -g machines -c "Windows Client" -s /bin/false %m\$
- die Gruppe „machines“ exisitiert

Hinweis 3: Erscheint beim Eintragen des Systems die Meldung, dass das Passwort nicht stimme (obwohl Sie es korrekt eingegeben haben), liegt vermutlich ein Fehler im add machine script vor (Leerzeichen vor den – (MinusZeichen), Tippfehler, Gruppe „machines“ fehlt.

Hinweis 4: Beim Anmelden eines Benutzers am Windows Client erscheint die Meldung, dass keine serverbasierten Benutzerprofile gespeichert werden können. Das Verzeichnis /home/fho/.msprofile gehört root (wenn dieser das System eingebucht hat). Deshalb den Besitzer ändern auf den jeweiligen Benutzer z.B. fho:

chown fho:users /home/fho/.msprofile (Punkt bei .msprofile beachten!)

Hinweise zu SAMBA

Auch Policies können via Samba festgelegt werden. Diese Policies können mit dem Programm POLEDIT.EXE auf einem NT-Server erstellt werden und auf NETLOGON abgelegt werden. Es sind zwei Files notwendig:

config.pol (für Windows 9x Clients)

ntconfig.pol (für Windows NT Clients)

Einschränkung: Zur Zeit kann Samba ein Domänenkontroller ähnlich Windows NT sein. Die SAMBA Version 3.0.x kann Mitgliedsserver in einer ActiveDirectory Domain sein, aber selber kein ActiveDirectory begründen. Die Beta-Version 4 soll da bereits noch mehr können.

Muster einer /etc/samba/smb.conf

Die Konfiguration des SAMBA-Servers kann im SWAT unter [**View**] angesehen werden. Im folgenden ist eine (gekürzte) Version der smb.conf dargestellt.

[Globals]

```
[global]
      workgroup = ANET31
      map to guest = Bad User
      printcap name = cups
      add machine script = /usr/sbin/useradd -g machines(nächste Zeile)
            -c "windows NT  200 XP" -d /dev/null -s /bin/false %m\$
      logon script = logonscr.cmd
      logon path = \\%L\profiles\.msprofile
      logon drive = P:
      logon home = \\%L\%U\.9xprofile
      domain logons = Yes
      preferred master = Auto
      domain master = Yes
      ldap ssl = no
```

```
      usershare allow guests = Yes
      admin users = root, fho
      read list = root, fho
      write list = root, fho
      cups options = raw
      include = /etc/samba/dhcp.conf
```

Vordefinierte Freigaben: homes, profiles, users, groups, printers

```
[homes]
      comment = Home Directories
      valid users = %S, %D%w%S
      read only = No
      inherit acls = Yes
      browseable = No

[profiles]
      comment = Network Profiles Service
      path = %H
      read only = No
      create mask = 0600
      directory mask = 0700
      store dos attributes = Yes

[users]
      comment = All users
      path = /home
      read only = No
      inherit acls = Yes
      veto files = /aquota.user/groups/shares/

[groups]
      comment = All groups
      path = /home/groups
      read only = No
      inherit acls = Yes

[printers]
      comment = All Printers
      path = /var/tmp
      create mask = 0600
      printable = Yes
      browseable = No

[print$]
      comment = Printer Drivers
      path = /var/lib/samba/drivers
      write list = @ntadmin, root
      force group = ntadmin
      create mask = 0664
      directory mask = 0775
```

Eigene Freigaben: netlogon, data, public, apps

```
[netlogon]
      comment = logonscripte auf Linux-Server
      path = /export/samba/netlogon

[data]
      comment = Dokumente auf Linux-Serve
      path = /export/samba/data
      admin users =
      read list = @users
      write list = @smb-data
      read only = No
```

```
[public]
      comment = Tauschbox auf Linux-Serve
      path = /export/samba/public
      read list = @users
      write list = @users
      read only = No

[apps]
      comment = Programme auf Linux-Server
      path = /export/samba/apps
      read list = @users
      write list = @smb-apps
      read only = No
```

vi-Editor

Ein Urgestein in der Unix-Welt ist der Editor vi. Sein spartanisches Aussehen täuscht, weil er trotzdem sehr leistungsfähig ist. Die Bedienung will gelernt sein, weicht sie doch von den GUI-Editoren ab. Ein Vorteil ist sicher, dass vi auf jedem Unix/Linux-System vorhanden ist und auch via Textkonsole (Telnet, SSH) bedient werden kann. Für kleine Änderungen an Konfigurationsdateien ist er oft der schnellste Weg.

Lernprogramm vimtutor

Als **Lernprogramm** können Sie in einem Befehlsfenster **vimtutor** eingeben. Das lernprogramm ist in ca. 20 Minuten zu schaffen. Hier kurz das allerwichtigste.

79. Beim Starten des Editors befindet man sich im **Befehlsmodus** (und kann *keinen* Text eingeben!)
    - mit PgUP und PgDN kann man Blättern
    - mit den Pfeil-Tasten (oder mit den Tasten **h j k l** kann man den Cursor nach links, unten, oben und rechts bewegen. hjkl gehen nicht in einer leeren Datei. (Praktisch bei Terminals ohne Cursor-Tasten)
    - mit der Maus kann der Cursor *nicht* bewegt werden!
    - die aktuelle Cursor-Position (Zeile, Spalte) wird unten rechts angezeigt
80. Mit **i** (oder der [Insert]-Taste) gelangt man in den **Einfügemodus** (wird unten angezeigt).
    - Nun kann Text eingefügt oder mit der
    - [Delete]-Taste Buchstaben rechts vom Cursor gelöscht werden
    - mit [←] werden Buchstaben links vom Cursor gelöscht
    - mit [Enter] gelangt man auf eine neue Zeile
81. Mit [Esc] kehrt man in den **Befehlsmodus** zurück (Anzeige „Insert“ unten verschwindet)
    - **dd** löscht die aktuelle
    - **5d [Enter]** löscht 5 Zeilen
    - **u** (undo) bringt die eben gelöschten Zeilen wieder zurück
82. Um vi zu **beenden** hat man verschiedene Optionen:
    - [**Esc**] **:q** (quit)beendet vi, wenn man keine Änderungen gemacht hat
    - [**Esc**] **:q!** beendet vi *ohne* Speichern der Änderungen
    - [**Esc**] **:wq** (write quit) Speichert die Änderungen und beendet vi
    - [**Esc**] **:x** macht das gleiche wie wq. Kleines x (sonst wird die Datei verschlüsselt!)

    Hinweis: Wurde vi aus Versehen beendet, indem einfach das Befehlsfenster geschlossen wurde, bleibt eine Sicherungsdatei bestehen und vi gibt eine Warnungaus, die Datei werde bereits bearbeitet. Ältere vi-Vesionen weigern sich, die Datei erneut zu bearbeiten, neuere lassen eine Verarbeitung erzwingen. Sie können in diesem Fall die Sicherungsdatei *.test.txt.swp* löschen (Punkt zu Beginn beachten).
83. **vi +120 /home/fho/test.txt** öffnet die Datei /home/fho/test.txt und der Cursor ist direkt auf der Zeile 120.

Wir werden vi im Folgenden für die Konfiguration von FTP und DNS-Server verwenden. Natürlich können Sie auch die /etc/samba/smb.conf damit bearbeiten, das geht oft schneller als via SWAT.

DNS-Server

Im Internet lassen sich alle Systeme per Namen finden, etwa www.anetgmbh.ch. In jedem Paket, das diesen Server erreichen soll, muss jedoch die IP-Adresse stehen. Der Browser fragt deshalb zuerst einen Domain Name Service-Server und dieser löst den Namen in die IP-Adresse auf. Umgekehrt kann ein DNS-Server meist auch angeben, welcher Name hinter einer IP-Adresse steht (Reverse Lookup). Hier wird ein DNS aufgesetzt, der für die eigene Zone verwendet werden kann und so auch die ideale Ergänzung zu den name based virtual hosts des Apache 2 bildet. Ein Eintrag in der hosts-Datei ist dann nicht mehr notwendig (sollte sogar entfernt werden).

Erfahrungsgemäss tun sich alle GUI-Programme für die DNS-Konfiguration schwer und produzieren oft fehlerhafte und unschöne Dateien. (Am besten funktioniert noch das GUI bei Windows Server 2003). Deshalb beschreiten wird hier den sicheren Weg mit dem Editor. Der etwas höhere Lernaufwand lohnt sich, sehen doch die Konfigurationsdateien auf allen Systemen fast zu 100% gleich aus. Um die Tipparbeit zu reduzieren, kopieren wir die standardmässig vorhandenen Dateien für die Zone localhost und passen sie an. Als Editor können Sie jeden Editor verwenden, hier benutzen wir **vi** (siehe Beschreibung weiter oben).

Der meistverbreitete DNS-Server ist der **bind** (Berkeley Internet Name Daemon), aktuell in der Version 9.x. Das eigentliche Programm heisst **named** (Name Daemon – Namens-Server) und läuft aus Sicherheitsgründen mit dem speziellen Benutzer named.

Folgende Dateien sind für den DNS wichtig:

/etc/named.conf	Hauptkonfiguration, nennt alle Zonen, für die dieser DNS zuständig ist was gelogt werden soll
/var/lib/named/master	in diesem Verzeichnis sind alle Zonen-Dateien, für die dieser DNS Server der Master ist
/var/lib/named/slave	in dieses Verzeichnis werden alle Zonen-Dateien gestellt, für die dieser DNS Server der Slave ist

Bearbeiten der /etc/named.conf

Wir passen die Haupt-Konfigurationsdatei so an, dass unser Name-Server folgende Funktionen beherrscht:

- Anfragen beantworten für die neue Zone test.intern (als Master)
- Anfragen beantworten für die Zone a-net.ch (als Slave)
- Rückwärts Namens-Auflösung für das Netz 192.168.112.x
- Weiterleitung aller übrigen Anfragen ins Internet (root-Server, Provider)

Allgemeine Optionen

Am Anfang der Datei /etc/named.conf stehen allgemeine Optionen über Speicherort der Zonen-Dateien, zu verwendende Forwarder und Logging Optionen. Diese werden kurz besprochen und kaum geändert.

84. Zur Sicherheit erstellen wir eine Sicherungskopie von named.conf. Öffnen sie dazu eine Befehlszeile:

    Chamäleon → Favoriten → Terminal (oder Chamäleon --> Programme --> System --> Teminals)

    su - Es werden root-Rechte benötigt

(Passwort von root wird verlangt)

cd /etc	Wechsel ins Verzeichnis /etc
cp named.conf named.conf:org	named.conf auf named.conf.org kopieren
vi /etc/named.conf	Datei editieren mit vi

Teil 1: Options

Hier werden allgemeine Optionen für den ganzen Name-Server festgelegt. Wir betrachten die geöffnete Datei (Reine Kommentar-Zeilen wurden entfernt):

```
options {
      directory "/var/lib/named";

      dump-file "/var/log/named_dump.db";
      statistics-file "/var/log/named.stats";

      #forwarders { 192.0.2.1; 192.0.2.2; };

      #forward first;

      #listen-on port 53 { 127.0.0.1; };

      listen-on-v6 { any; };

      #query-source address * port 53;
      #transfer-source * port 53;
      #notify-source * port 53;

      #allow-query { 127.0.0.1; };

      notify no;
};
```

Meistens sind in diesem Bereich *keine* Änderungen notwendig. Falls man die Caching Funktion de DSN vom Provider benutzen möchte, kann allenfalls ein forwarder eingerichtet werden. Einzelne Einträge werde hier lediglich erläutert.

85. direcotry „/var/lib/named“; Unter diesem Pfad werden die Zonen-Dateien gesucht (s. weiter unten). Dieser Pfad mit den Unterverzeichnissen master und slave wurde bei der Installation bereits erstellt. Die Zonen, für welche dieser DNS Master ist, werden im Unterverzeichnis master gespeichert, Zonen für welche er Slave ist im Unterverzeichnis slave.
86. Es folgen zwei Angaben für dump und Statistik-Dateien. Kein Änderung hier.
87. **forwarders {195.186.1.111; };** Hier kann ein DNS von Ihrem Provider eingetragen werden. Dann fragt unser DNS diesen für alle Zonen, für die nicht er selber zuständig ist. Die Chance besteht, dass der DNS viele ortsübliche Namen im Cache hat und deshalb schneller Auskunft geben kann. Wenn Sie dies wollen, entfernen Sie das #-Zeichen am Anfang und tragen Sie den DNS Ihres Providers ein. Beachten Sie den **;** nach der IP-Adresse, es könnten nämlich mehrere DNS eingetragen werden, getrennt durch ;.
88. **forward first;** Falls ein Forwarder oben eingetragen wurde, sollte das #-Zeichen entfernt werden. Dann wird der DNS des Providers zuerst gefragt.
89. #listen-on port 53 { 127.0.0.1 }; Der DNS hört standardmässig auf dem Port 53 (UDP und TCP). Keine Änderung notwendig.
90. listen-on-v6 { any }; Der DNS hört auch auf IPv6 (falls vorhanden). Keine Änderung.
91. #allow-query { 127.0.0.1; }; Der DNS erlaubt standardmässig Zonen-Transfers von allen Systemen aus. Diese können dann auch Slaves einrichten.

92. notify no; Standardmässig fragen die Slaves periodisch den Master nach der aktuellen Serienummer der Zonen-Datei, eine Benachrichtigung der Slaves bei Änderungen ist daher nicht notwendig.

Teil 2: Logging Optionen

Der DNS kann Daten in eine Logdatei schreiben. Standardmässig werden kein Logs geführt. Mann kann aber alle Zugriffe loggen. Dann werden die Log-Dateien schnell sehr gross und der DNS sicher langsamer. Ausserdem ergeben sich Probleme mit dem Datenschutz, da die Anfragen jedes Benutzers ausgewertet werden können. Bei der Fehlersuche können nur Fehlermeldungen geloggt werden. Wir machen hier keine Änderungen.

Teil 3: Vordefinierte Standardzonen

Der DNS hat bereits vordefinierte Zonen, die benutzt werden können. Diese sind:

- Zone localhost (Forward Lookup Zone)
- Zone 0.0.127.in-addr.arpa (Reverse Lookup Zone für 127.0.0.x)
- Zone root.hint (Kennt die root-Server des Internet DNS Systems)

Diese Zonen sollten belassen werden und dienen uns als willkommene Vorlagen für die eigenen Zonendateien. Dir Zone root.hint beschreibt die Zone . (Punkt=root) und enthält die Root-Server im Internet. Diese leiten den DNS für alle Toplevel Domänen zu den zuständigen Servern (z.B. für alle xxxx.ch Zone zu den Server von switch.ch etc.) Damit kann rekursiv jede registrierte Zone im Internet gefunden werden.

Hier sind *keine* Änderungen zu machen.

```
zone "." in {                                   (Zone . mit den root-Servern)
      type hint;
      file "root.hint";
};

zone "localhost" in {                           (Forward-Zone für „localhost")
      type master;
      file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {                (Reverse-Zone für 127.0.0.x)
      type master;
      file "127.0.0.zone";
};
```

Eigene Zonen hinzufügen

Wir fügen nun die eigenen Zonen hinzu. Dazu sind zwei Dinge notwendig:

- Eintragen der Zonen in der named.conf
- Erstellen der zugehörigen Zonen-Dateien

Zuerst machen wir die Einträge in der named.conf für unsere Zonen:

- test.intern (als Master)
- a-net.ch (als Slave)der bestehenden Zone im Internet)
- Reverse-Lookup für das interne Netzwerk 192.168.112.x

Master-Zone test.intern hinzufügen

93. Eintrag für **test.intern** erstellen:

Die Datei named.conf ist noch im **vi** geöffnet (s. oben). Wir entfernen den Eintrag für die vorgesehene Zusatzdatei named.conf.include.

Blättern Sie mit [PgDn] bis ans Ende der Datei. Auf Zeile 128 steht der include-Befehl. Diesen machen wir zum Kommentar mit dem #-Zeichen:

i	(Insert-Modus)
[Home]	(An den Anfang der Zeile 128 gehen)
# include "/etc/named.conf.include";	(# an den Anfang der Zeile schreiben)
(nun zur letzten Zeile 133 gehen)	
[**End**]	(Cursor springt ans Ende der Zeile 133)
[Enter]	
[[Enter]	(eine Leerzeile am Ende)

Nun markieren wir mit der Maus die vier Zeilen der Zone localhost bis und mit **};**
Im Menu oben am Fenster wählen wir:
„Bearbeiten" → „Kopieren".
(Der Cursor steht immer noch am Ende der Datei und Insert wird unten angezeigt)
Wählen Sie im Menu oben am Fenster:
„Bearbeiten" → „Einfügen" (die kopierten Zeilen erscheinen am Ende)

Nun bearbeiten wir diese Zeilen, bis sie wie folgt aussehen:
(immer noch im Insert-Modus mit **i**):

```
zone "test.intern"   in  {
        type  master;
        file  "master/test.intern";
};
```

Damit weiss unser DNS, dass er als Master zuständig ist für die Zone test.intern und dass die Zonendatei unter **/var/lib/named/master/test.intern** zu finden ist. Achten Sie auf die Hochkommata und die **};** am Ende!

Hinweis: es ha sich sehr bewährt, wenn die Zonen-Dateien genau *gleich heissen*, wie die Zonen, die sie beschreiben. Die Zonendatei erstellen wir weiter unten.

Slave-Zone a-net.ch hinzufügen

94. Eintrag für die Zone **a-net.ch** erstellen.

Die Datei /etc/named.conf ist immer noch im **vi** geöffnet (s. oben)

Blättern Sie mit [PgDn] bis ans Ende der Datei.

i	(Insert-Modus)
[PgDn]	(nun zur letzten Zeile gehen)
[**End**]	(Cursor springt ans Ende der Zeile)
[Enter]	
[[Enter]	(eine Leerzeile am Ende)

Nun markieren wir mit der Maus die vier Zeilen der Zone localhost bis und mit **};**
Im Menu oben am Fenster wählen wir:
„Bearbeiten" → „Kopieren".
(Der Cursor steht immer noch am Ende der Datei und Insert wird unten angezeigt)
Wählen Sie im Menu oben am Fenster:
„Bearbeiten" → „Einfügen" (die kopierten Zeilen erscheinen am Ende)

Nun bearbeiten wir diese Zeilen, bis sie wie folgt aussehen:
(immer noch im Insert-Modus mit **i**):

```
zone "a-net.ch"   in  {
        type  slave;
        file  "slave/a-net.ch";
        masters {81.6.49.206; };
};
```

Beachten Sie, dass hier der Typ „slave" ist und die Zonendatei Untervezeichnis /var/lib/named/slave abgelegt werden soll. Ausserdem ist die Zeile „masters" notwendig. Dort wird angegeben, von welchem Master die Zonen-Daten transferiert werden können.

Hinweis: Unter der angegebenen IP-Adresse kann die Zone a-net.ch geholt werden, falls Ihr System ugriff zum Internet hat.

Reverse-Zone 112.168.192.in-addr.arpa hinzufügen

Reverse-Zonen sind immer Class C Netzwerke mit max. 256 Adressen. Der Name der Zone enthält die ersten drei Ziffern der IP-Adresse (allerdings ***rückwärts***) und die Pseudo-Toplevel-Domain **in-addr.arpa**. Wollen sie also das Netzwerk 192.168.112.x beschreiben, *muss* die Zone lauten:
112.168.192.in-addr.arpa.

95. Eintrag für die Zone **112.168 192.in-addr.arpa** erstellen:

Die Datei /etc/named.conf ist immer noch im **vi** geöffnet (s. oben)

Blättern Sie mit [PgDn] bis ans Ende der Datei.

i	(Insert-Modus)
[PgDn]	(nun zur letzten Zeile gehen)
[**End**]	(Cursor springt ans Ende der Zeile)
[Enter]	
[[Enter]	(eine Leerzeile am Ende)

Nun markieren wir mit der Maus die vier Zeilen der Zone **0.0.127.in-addr.arpa** bis und mit **};**
Im Menu oben am Fenster wählen wir:
„Bearbeiten" → „Kopieren".
(Der Cursor steht immer noch am Ende der Datei und Insert wird unten angezeigt)
Wählen Sie im Menu oben am Fenster:
„Bearbeiten" → „Einfügen" (die kopierten Zeilen erscheinen am Ende)

Nun bearbeiten wir diese Zeilen, bis sie wie folgt aussehen:
(immer noch im Insert-Modus mit **i**):

```
zone "112.168.192.in-addr.arpa"   in  {
        type  master;
        file  "master/112.168.192.in-addr.arpa";
};
```

Beachten Sie, dass hier der Typ wieder master ist.

96. Kontrollieren Sie nun die neu hinzugefügten Zonen:

- sind alle Zonen- und Dateinamen zwischen " (Hochkomma)?
- Stimmt das Unterverzeichnis master/ oder slave/?
- haben die Zeilen am Ende einem **;** (Strichpunkt) ?
- ist die letzte Zeile jeweils **};** ?

97. Wenn alles stimmt, speichern Sie die Datei und beenden Sie **vi**:

    [Esc] : wq

    Die Datei /etc/named.conf ist somit fertig und es fehlen noch die beiden Zonen-Dateien für test.intern uns 112.168.192.in-addr.arpa. Die Zonendatei für die Slave-Zone a-net.ch müssen wir *nicht* erstellen, diese wird beim Starten des DNS direkt vom Master transferiert!

Zonendatei für test.intern

Die Zonendatei erstellen wir durch kopieren der Vorlage localhost.zone und passen sie danach an. Die Dateien kommen ins Verzeichnis /var/lib/named/master.

98. Wir kopieren als erstes die Zonen-Datei auf den richtigen Namen und den richtigen Ort:

    Öffnen sie eine Befehlszeile:
    Chamäleon → Favoriten → Terminal

su -	(Wir benötigen root-Rechte)
(Passwort von root wird verlangt)	
cd /var/lib/named	(Standard-Verzeichnis für Zonen-Dateien)
ls -l	(vorhandene Dateien werden angezeigt, darunter localhost.zone)
cp localhost.zone master/test.intern	(Kopieren der Datei ins Unterverzeichnis master)
cd master	(Wechsel ins Unterverzeichnis master)
ls -l	(test.intern sollte dort sein)
vi test.intern	(test.intern anpassen mit **vi**)
i	(Insert-Modus)

    (nun die Datei anpassen, bis sie wie folgt aussieht:)

```
$TTL 2D
@         IN SOA      ns.test.intern. info.test.intern. (
                      2009101400  ; serial
                      4H          ; refresh
                      1H          ; retry
                      1W          ; expiry
                      2D )        ; minimum

          IN NS       ns.test.intern.
          IN MX       10 smtp
ns        IN A        192.168.112.32
www       IN A        192.168.112.32
smtp      IN A        192.168.112.12
router    IN A        192.168.112.1
www2      IN CNAME    www
```

	Wen alles stimmt (z.B. Punkte am Ende eine Namens kontrollieren, sonst wird der Zonen-Name nochmals angehängt)
[Esc] :wq	Datei speichern und vi beenden.

    Hierzu ein paar Erläuterungen zu den einzelnen Zeilen:

1. Zeile:	$TTL 2D	Die minimale „time to live“ ist 2 Tage (grosses **D**!)
2. Zeile:	SOA- Zeile	Source of Authority, meist verteilt auf mehrere Zeilen (s. Runde Klammer)
	ns.test.intern**.**	zuständiger Name-Server (Punkt beachten!)

	info.test.intern.			eMail-Adresse des Zuständigen, (ohne @, da dies den Zonen-Namen bedeutet, Punkt am Ende)
	2009101400			Seriennummer, oft Datum rückwärts und 2 Stellen, maximal 10 Stellen möglich
	4H			Alle 4 Stunden prüfen die Slaves die Seriennummer
	1H			Falls Master nicht erreichbar, Wiederholung nach 1 Stunde. (H gross!)
	1W			Einträge werden nach 1 Woche ohne Masterkontakt ungültig
	2D)			time to live, dann Klammer zu!
3. Zeile	IN NS	ns.test.intern.		zuständiger Name-Server (mehrere NS möglich)
4. Zeile:	IN MX	10 smtp		zuständiger Mail-Server (kann fehlen) da Punkt am Ende fehlt wird Zone ergänzt. er heisst also: smtp.test.intern
5. Zeile:	ns	IN A	192.168.112.32	normale Adress-Zeile für ns.test.intern
6. Zeile:	www	IN A	192.168.112.32	normale Adress-Zeile für www.test.intern
7. Zeile:	smtp	IN A	192.168.112.12	normale Adress-Zeile für smtp.test.intern
8. Zeile:	router	IN A	192.168112.1	normale Adress-Zeile für router.test.intern
9. Zeile:	www2	IN CNAME	www	www2 ist ein Alias (canonical name) für www (=gleiches System für beide)

Damit ist die Zonendatei fertig und kann getestet werden.

Reverse-Zonendatei 192.168.112.x

Reverse-Zonen erlauben es, bei bekannter IP-Adresse den zugehörigen DNS-Namen herauszufinden. Grundsätzlich sollte dies überall funktinieren, aber oft werden die Reverse-Zonen nicht eingerichtet. Dies macht aber auch für Interne Subentze durchaus Sinn, kann man so doch von jedem System aus den Namen eines Gerätes herausfinden. Dies sagt mehr aus als eine Adresse, die man nie alle im Kopf hat.

Wir richten eine Reverse-Zone ein, welche die Adressen im Bereich 192.168.112.x auflösen kann. Wir arbeiten auch hier mit einer Vorlage, der Datei 127.0.0.zone.

Gehen Sie ins richtige Verzeichnis und kopieren Sie die Datei:
(Befehlszeile öffnen)
su - (wir benötigen root-Rechte)
(Passwort von root wird verlangt)

cd /var/lib/named
cp 127.0.0.zone master/112.168.192.in-addr.arpa (IP-Adresse *rückwärts*!)

cd master (ins Unterverzeichnis master)
ls -l (Datei 112.168.192.in-addr.arpa sollte da sein)

vi 112.168.192.in-addr.arpa
i (Insert-Modus)
(nun die Datei anpassen, bis sie wie folgt aussieht:)

```
$TTL 2D
@           IN SOA          ns.test.intern. info.test.intern. (
                        2009101400 ; serial
                        4H         ; refresh
                        1H         ; retry
                        1W         ; expiry
                        2D )       ; minimum

            IN NS       ns.test.intern.       (. Punkt nicht vergessen!)
1           IN PTR      router.test.intern.
```

```
32          IN PTR     ns.test.intern.
12          IN PTR     smtp.test.intern.
```

(Wenn alles stimmt (Punkte am Ende!) schliessen wir die Datei:)
[**Esc**] **:wq**
99. Nun sollte unser DNS-Server z.B. die Adresse 192.168.112.1 auflösen können.

Testen des DNS-Servers

Nun sind alle Definitionen für den DNS-Server gemacht und wir können ihn testen. Dazu gehen wir wie folgt vor:
- Checkliste für die Zonen-Dateien
- probehalber Start des DNS mit Anzeige der Meldungen

100. Mit ein paar Regeln können die Zonendateien überprüft werden:

Checkliste:
- alle Namen müssen am Ende einen **.** (Punkt) haben, ausser es soll der Zonen-Name angehängt werden
- Zeile 1: $TTL Zeile
- Zeile 2: genau eine SOA-Zeile: Name-Server und Mail-Adresse (ohne @)
- Seriennummer **erhöht**? (aber nicht mehr als 10 Stellen lang)
- mindestens eine NS-Zeile
- MX-Zeile(n), falls Mail-Empfang erwünscht
- A-Records (*nur* in Forward-Zonen möglich)
- PRT-Records (*nur* in Reverse-Zonen möglich, alle Namen mit **.** Punkt am Ende)

Nun starten wir den DNS-Server und überprüfen ob er läuft und ob es Fehlermeldungen gibt.
Hinweis: named kann mehrfach gestartet werden, allerdings bekommt nur der erste den Port 53 und gibt Antwort. Deshalb prüfen Sie, dass er nicht zweimal läuft.

rcnamed stop	(named wird - falls er schon läuft – gestoppt)
named –u named –f -g	(named wird so gestartet, dass die Meldungen am Bildschirm erscheinen und nicht in der Log-Datei)

Es erscheinen Meldungen über erfolgreiche und allenfalls nicht erfolgreiche Funktionen. Bei Fehlern ist oft die Zeilennummer angegeben, wo sich der Fehler in der Konfigurationsdatei befindet.
Bei Fehlern kann named mit

[**Ctrl**] + [**C**]

gestoppt werden. Dann die Fehler korrigieren mit

vi +135 /etc/named.conf

(wenn z.B. auf der Zeile 135 in der named.conf ein Fehler angezeigt wird). Dann den named neu starten mit named -u named -f -g.

Wenn keine gravierenden Fehler aufgetreten sind, bleibt der named aktiv mit der Meldung *running* am Schluss.

Beispiel der Meldungen eines Starts:

```
........
18-Oct-2009 12:55:36.468 default max-cache-size (33554432) applies: view
_bind
18-Oct-2009 12:55:36.474 command channel listening on 127.0.0.1#953
18-Oct-2009 12:55:36.474 command channel listening on ::1#953
18-Oct-2009 12:55:36.474 ignoring config file logging statement due to -g
option
18-Oct-2009 12:55:36.478 zone 0.0.127.in-addr.arpa/IN: loaded serial 42
```

```
18-Oct-2009 12:55:36.479 zone 112.168.192.in-addr.arpa/IN: loaded serial
2009101400
18-Oct-2009 12:55:36.482 zone test.intern/IN: loaded serial 2009101400
18-Oct-2009 12:55:36.483 zone localhost/IN: loaded serial 42
18-Oct-2009 12:55:36.488 running
18-Oct-2009 12:55:36.517 zone a-net.ch/IN: Transfer started.
18-Oct-2009 12:55:36.560 transfer of 'a-net.ch/IN' from 81.6.49.206#53:
connected using 192.168.116.32#35856
18-Oct-2009 12:55:36.653 zone a-net.ch/IN: transferred serial 2008100900
```
18-Oct-2009 12:55:36.654 transfer of 'a-net.ch/IN' from 81.6.49.206#53: Transfer completed: 1 messages, 24 records, 597 bytes, 0.093 secs (6419 bytes/sec)

In den Meldungen oben sieht man, dass:
- die Zone test.intern geladen wurde
- die Reverse-Zone 112.168.192.in-addr.arpa geladen wurde
- der named nun läuft (running)
- die Zone a-net.ch vom Master nach dem Start transferiert wurde (die Datei a-net.ch sollte nun im Verzeichnis /var/lib/named/slave vorhanden sein).

Hinweis: Unter **SuSE 11.2** erscheint beim Starten von named eine Fehler-Meldung mit einem Segmentfault. Als momentane Umgehungslösung muss AppArmor deaktiviert werden:

YaST → Novell AppArmor → AppArmor Kontrollfeld
[ ] AppArmor aktivieren (Hacken entfernen)
[OK]

DNS-Server mit nslookup überprüfen

Das Programm nslookup ist auf fast allen Betriebssystemen verfügbar (Linux, Windows ab NT, Mac, OS/2 etc.) und eignet sich zum Überprüfen des DNS-Servers.

101. Wir lassen den named laufen (s. oben) und öffnen ein weiteres Befehlsfenster zum Testen:

Chamäleon --> Favoriten --> Terminal

nslookup [Enter]	(Prompt wechselt auf >)
server 192.168.112.32	(wir fragen unseren neuen DNS-Server)
Default server: 192.168.112.32	
Address: 192.168.112.32#53	
smtp.test.intern [Enter]	(Was ist die IP von www.test.intern?)
Server: 192.168.112.32	
Address: 192.168.112.32#53	
Name: smtp.test.intern	(Antwort)
Address: 192.168.112.12	(Adresse wurde aufgelöst)

(Es können noch weitere Adressen getestet werde, die erfasst wurden)

set q=soa [Enter]	(Abfrage nach Source of Authority)
test.intern [Enter]	(nur noch die Domäne eingeben!)

test.intern
origin = ns.test.intern
mail addr = info.test.intern
serial = 2009101400
refresh = 14400
retry = 3600
expire = 604800

minimum = 172800

Nun testen wir noch den Reverse-Lookup:

set q=a [Enter] (wieder Adressen abfragen)
192.168.112.32 [Enter] (Name diese System ist ?)

Server: 192.168.112.32
Address: 192.168.112.32#53

32.112.168.192.in-addr.arpa name=ns.test.intern. (Antwort)
exit [Ende] (nslookup wir beendet)

102. Damit hat unser DNS die Anfragen beantworten können und funktioniert. Nun können Sie (auch mit nslookup) von einem Client aus den DNS testen. Dazu müssen Sie im nslookup den Befehl server = 192.168.112.32 eingeben, sonst wird der standardmässig konfigurierte DNS gefragt. Wenn unser DNS über eine Internetverbindung verfügt, kann er auch alle Hosts im Internet auflösen.

Automatischer Start des DNS

Nun, da der DNS-Server funktioniert, soll er immer automatisch gestartet werden. Damit es nicht zweimal läuft, stoppen wir unseren Test im Befehlsfenster mit [Ctrl] + [C].

103. Starten Sie YaST mit:
Chamäleon → Rechner → YaST
(Passwort von root wird verlangt)
(links) System → (rechts) **Systemdienste (Runlevel)**

Systemdienste (Runlevel): Dienste
( ) Einfacher Modus (x) Expertenmodus (Expertenmodus klicken)

Suchen und makieren Sie nun die Zeile:
- **named** (markieren)
[Anwenden/Zurücksetzen] → [**Dienst aktivieren**] (es sollten 3 5 erscheinen)
[OK]
[Ja] (Änderungen speichern)

Der named sollte fortan automatisch gestartet werden.

Hinweis: Vergessen Sie bitte folgendes nicht: Wenn Sie Änderungen am Master vornehmen, sind zwei Dinge zu beachten:
- **Seriennummer** im geänderten Zonen-File **erhöhen**
- named neu starten mit: **rcnamed restart**

FTP-Server

Es werden mehrere FTP-Server mitgeliefert, aber natürlich kann nur einer auf Port 21 gestartet werden. Bei SuSE ist vsftpd (Very Secure FTP-Daemon) dabei. Dieser wird neu eigenständig gestartet, kann aber auch als Dienst unter xinetd laufen. Dies steuert der Eintrag „listen=Yes/No“ in vsftpd.conf. Steht er auf Yes (wie hier) läuft der vsftpd als eigener Dienst, bei No wird er bei Bedarf vom xinetd gestartet.

Wir starten den vsftpd so, dass er fortan automatisch als eigener Dienst aktiv wird:

104. Chamäleon --> Rechner --> YaST
(es wird das Passwort für root verlangt)

System (im linken Fenster) --> Systemdienste (Runlevel) (im rechten Fenster)

Systemdienste (Runlevel): Dienste
( ) Einfacher Modus (x) Expertenmodus (Expertenmodus klicken)

Suchen und makieren Sie nun die Zeile:
- **vsftpd** (markieren)
[Anwenden/Zurücksetzen] → [**Dienst aktivieren**] (es sollten 3 5 erscheinen)
[OK]
[Ja] (Änderungen speichern)

Der vsftpd sollte fortan automatisch gestartet werden.
Nun können sich die *anonyme Benutzer* mit FTP anmelden. Geben Sie als Namen einfach anonymous und dann als Passwort irgend eine eMail-Adresse ein (z.B. aa@aa.ch).:

ftp 192.168.112.32
Connected to 192.168.112.32
220 (vsFTPd 2.0.7)
Name: (192.168.112.32:root): **anonymous** (=anonymer Benutzer)
331 Please specify the Password:
Password**: aa@aa.ch** (irgend eine eMail Adresse)
230 Login successful.
Remote system type is UNIX.
Using binarx mode to transfer files.
ftp>**dir** (Anzeige der Dateien, im Moment keine)
quit (abmelden)

Die anonyme Anmeldung ist standardmässig aktiviert. Allerdings können (aus Sicherheitsgründen) nur Dateien heruntergeladen werden, hochladen ist nicht erlaubt. Die Dateien müssen im Verzeichnis **/srv/ftp** sein.

Lokale Benutzer für FTP zulassen

105. Wir passen nun den vsftpd so an, dass die anonymous Anmeldung nicht mehr geht, dafür aber die Linux - Benutzer sich anmelden können. Sie werden standardmässig mit Ihrem Home - Verzeichnis verbunden und können Dateien runter- und hochladen:

vi /etc/**vsftpd.conf** (Konfigurationsdatei in **vi** laden)
i (Insert Modus)
write_enable=YES (Hochladen möglich, Zeile 18 # entfernen)
ftpd_banner="Willkomen beim FTP-Server der A-Net GmbH"
(Begrüssungstext anpassen auf Zeile 32)
local_enable=YES (lokale Benutzer zulassen, Zeile 59 # entfernen)
anonymous_enable=NO (anonymous sperren, Zeile 91)

[**Esc**] **:wq** (vi beenden und sichern)

rcvsftpd restart (FTP-Server neu starten)

Der FTP-Server wurde soch neu gestartet werden, damit die Änderungen wirksam werden.

rcvsftpd restart

vsftpd testen

Der vsftpd sollte nun die anonymous Anmeldung nicht mehr akzeptieren, dafür müssen sich die

lokalen Benutzer anmelden können und Dateien zu/von Ihrem Home -Verzeichnis laden können.

106. Wir testen dies aus. Dazu verwenden wir einen Client im Netzwerk. Der Firewall sollte ftp - Daten zulassen (s. Schritt 73 Firewall --> erlaubte Dienste: vsftpd). Sonst können Sie den Firewall temporär stoppen mit *rcSuSEfirewall2 stop* (Gross-Kleinschreibung beachten!).

    Auf einem Windows-Client öffnen Sie eine Befehlszeile:

    Start --> ausführen --> **cmd.exe** [OK]

cd /	(ins Verzeichnis c:\ wechseln)
ftp 192.168.112.32	
Benutzer: fho	(Als Benutzer anmelden, nicht als root!)
Password: xxxxxxxxx	
dir	(es werden in Ihrem Home-Verzeichnis die Daten und Verzeichnisse angezeigt:)
help	(verfügbare Befehle werden angezeigt)
cd Documents	(Wechsel ins Verzeichnis Documents)
put config.sys config.sys	(Datei config.sys hochladen)
dir	(Datei config,sys sollte da sein)
quit	(abmelden)

    Hinweis 1: Die Benutzer können Dateiein in ihr Homeverzeichnis hochladen und alle Daten, für die Sie Leserechte haben, auch herunterladen (*nicht nur* vom Home-Verzeichnis). Die dazu notwendigen Befehle heissen **put** und **get**. Die Dateiein kommen vom/zum aktuellen Verzeichnis, in dem man vor dem Start des ftp ist.

    Hinweis 2: root (und andere System-Benutzer) dürfen aus Sicherheitsgründen *kein* FTP machen. *Gesperrt* sind die Benutzer in der Datei /etc/ftpusers.

    Hinweis 3: Da auch auf einem Windows-System oft die Befehlszeile schneller zum Ziel führt, können Sie eine Verknüpfung dafür erstellen: (rechte Maustaste auf den Desktop) --> Neu --> Verknüpfung --> cmd.exe [OK]

107. Wir passen den ftp nochmals an, so dass die Benutzer *nur noch* in Ihr eigenes Home-Verzeichnis kommen, alle anderen Verzeichnisse sind für sie unerreichbar.
    Dazu wird die Funktion **chroot** (change root) verwendet. Damit wird beim Logon das Home-Verzeichnis des Benutzer zum root-Verzeichnis gemacht. Ein Wechsel in ein Verzeichnis unter root ist damit nicht möglich, das unterste Verzeichnis (eben /) ist sein Home-Verzeichnis.

vi /etc/**vsftpd.conf**	(Konfigurationsdatei in **vi** laden)
i	(Insert Modus)
chroot_local_users=YES	(nur Homeverzeichnis erreichbar, Zeile 69 # entfernen)
[**Esc**] **:wq**	(vi beenden und sichern)
rcvsftpd restart	(FTP-Server neu starten)

    Der FTP-Server wurde noch neu gestartet werden, damit die Änderungen wirksam werden.

    rcvsftpd restart

108. Wir testen nun, ob der Benutzer wirklich nicht mehr in anderes Verzeichnis kommen kann:

ftp 192.168.112.32
Benutzer: fho (Als Benutzer anmelden, nicht als root!)
Password: xxxxxxxxx
dir (es werden in Ihrem Home-Verzeichnis die Daten und Verzeichnisse angezeigt:)

cd /etc (Wechsel ins Verzeichnis /etc)
550 Failed to change directory (Fehlermeldung, Wechsel abgewiesen)
dir (immer noch im Homeverzeichnis)

quit (abmelden)

109. Mit der Datei /etc/vsftp.chroot_list kann eine Liste von Benutzern angegeben werden, welche trotz chroot-Anweisung in alle Verzeichnisse verzweigen dürfen. Dann muss in der Datei /etc/vsftpd.conf auf der Zeile 75 diese Funktion aktiviert werden und auf der Zeile 79 der Name der Ausnahmeliste angegeben werden.

Apache 2 Webserver

Der Apache2 Web-Server wird automatisch eingerichtet, wenn Sie bei der Installation das Paket "WEB- und LAMP-Server" ausgewählt haben. Der Server braucht nur noch gestartet zu werden und dann kann die Testseite „It works!“ angeschaut werden. .

110. Starten Sie den Apache mit:

Befehlsfenster öffnen:

Chamäleon --> Favoriten --> Terminal
su - (root-Rechte notwendig)
(Passwort von root wird verlangt)

rcapache2 start (apche2 starten oder neustarten mit restart)

(Nun starten Sie einen Browser z.B. den Konqueror mit der Kugel-Icon auf der Taskleiste.)

http.//localhost

(Die Seite „It works!“ sollte angezeigt werden)

111. $$$$$$

112. (**Die Beschreibung des Apche2 folgt später. Siehe Beschreibung von SuSE 10.1**)

113. $$$$$$

Veschiedenes

Nützliche Befehle

Anzeige der Files im aktuellen Verzeichnis	ls -l
Wechseln ins Root-Verzeichnis	cd /
Directory erstellen	mkdir
Directory löschen	rmdir
Kopieren einer Datei	cp
Datei umbenennen	mv

Datei löschen	rm
Diskette mounten als directory /floppy	mount /dev/fd0 /floppy
Diskette formatieren mit 1.44MB	fdformat /dev/fd01440
Diskette freigeben	umount /floppy
CD-ROM mounten als directory /cdrom	mount /dev/cdrom /cdrom
CD-ROM freigeben	umount /cdrom
Text-Editor vi	(Quit mit [ESC] **:q!** oder Save mit [ESC] **:wq**)
IP Adresse testen	ping 192.168.112.17 (beenden mit Ctrl+C)
Erste Netzwerkkarte stoppen	ifconfig eth0 down
Erste Netzwerkkarte starten	ifconfig eth0 up
Abrechen eines Vorganges	Ctrl + z
Eigene IP-Adresse anzeigen	ifconfig
X-Windows starten	startx
KDE X-Windows konfigurieren	sax, sax2
XINETD neu starten	rcxinetd restart
Apache Server neu starten	rcapache2 restart
FTP-Server neu starten	rcvsftpd restart
DNS-Server starten (Test)	named -u named -f -g
Samba Server starten	rcsmb start und rcnmb start
Samba Server stoppen	rcsmb stop und nmb stop
NetBios Namen anzeigen	nmblookup srvanet17 -S
Firewall starten	rcSuSEfirewall2 start
Firewall stoppen	rcSuSEfirewall2 stop
Abmelden	logout
Neuer Befehls-Prompt	Alt]+[Ctrl]+[F1], oder [Alt]+[Ctrl]+[F2] usw, zurück zu KDE mit [Alt]+[Ctrl]+[F7]
Linux herunterfahren	init 0 oder halt
Linux neu starten	init 6 oder reboot
Grafische Oberfläche beenden	init 3
Grafische Oberfläche starten	init 5

Wichtige Dateien

Die Dateien sind neu teilweise in Unterverzeichnissen von /etc (z.B. samba).

Vorsicht: Vor dem Ändern sichern!

Damit Änderungen wirksam werden /sbin/SuSEconfig laufen lassen

/etc/init.d/boot	autostart Scripte, auch um eigene einzubinden
/etc/xinetd.conf	neuer xInetd Superserver (neu für Telnet, SWAT etc.)
/etc/samba/smb.conf	SAMBA Konfiguration
/etc/apache2/httpd.conf	Apache2 Konfiguration (dazu: default-server.conf, listen.conf)

/etc/grub.conf	GRUB Boot-Loader
/etc/postfix/main.cf	postfix Konfiguration (Haupt-Datei)
/etc/sysconfig/mail	postfix (Zugriff von anderen System freischalten)
/etc/ftpusers	Liste für gesperrte FTP-Benutzer (z.B. root)
/etc/vsftpd.conf	Konfiguration für den FTP-Server vsftpd
/var/log/boot.log	Boot-Log etc
/var/log/samba/log.smbd	Log von SAMBA
/var/log/apache2/access.log	Zugriffe auf Apache 2 WEB-Server