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 11.4

Eine Schritt-für-Schritt Anleitung für die erfolgreiche Konfiguration eines File- und Druck-Servers mit SAMBA.

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 oder Sie die SuSE 11.4 DVD haben, 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

1. Wir bereiten die Datenverzeichnisse für den SAMBA-Server vor. Dazu verwenden wir die Befehlszeile. Wir öffnen 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

2. Wir sollten bereits ein Verzeichnis /export haben (da wir dafür bei der Installation 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, beginnend mit einem /):
   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                 (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)
   ```

   Hinweis: Der letzte Befehl kann jeweils mit Pfeil nach oben (Cursor up) wieder hervorgeholt und angepasst werden. Das spart Tipp-Arbeit.

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

   ```
   cd  /export/samba                    (wir gehen in dieses Verzeichnis)
   ls  -l                               (zeigt die erstellten Verzeichnisse zu Kontrolle an)
   chmod  775  netlogon                 (Besitzer und Gruppe dürfen schreiben,
                                        alle Andern nur lesen)
   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
   ```

3. Windows-Clients vom Tpy Windows NT, 2000, XP, Vist und Windows 7 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:

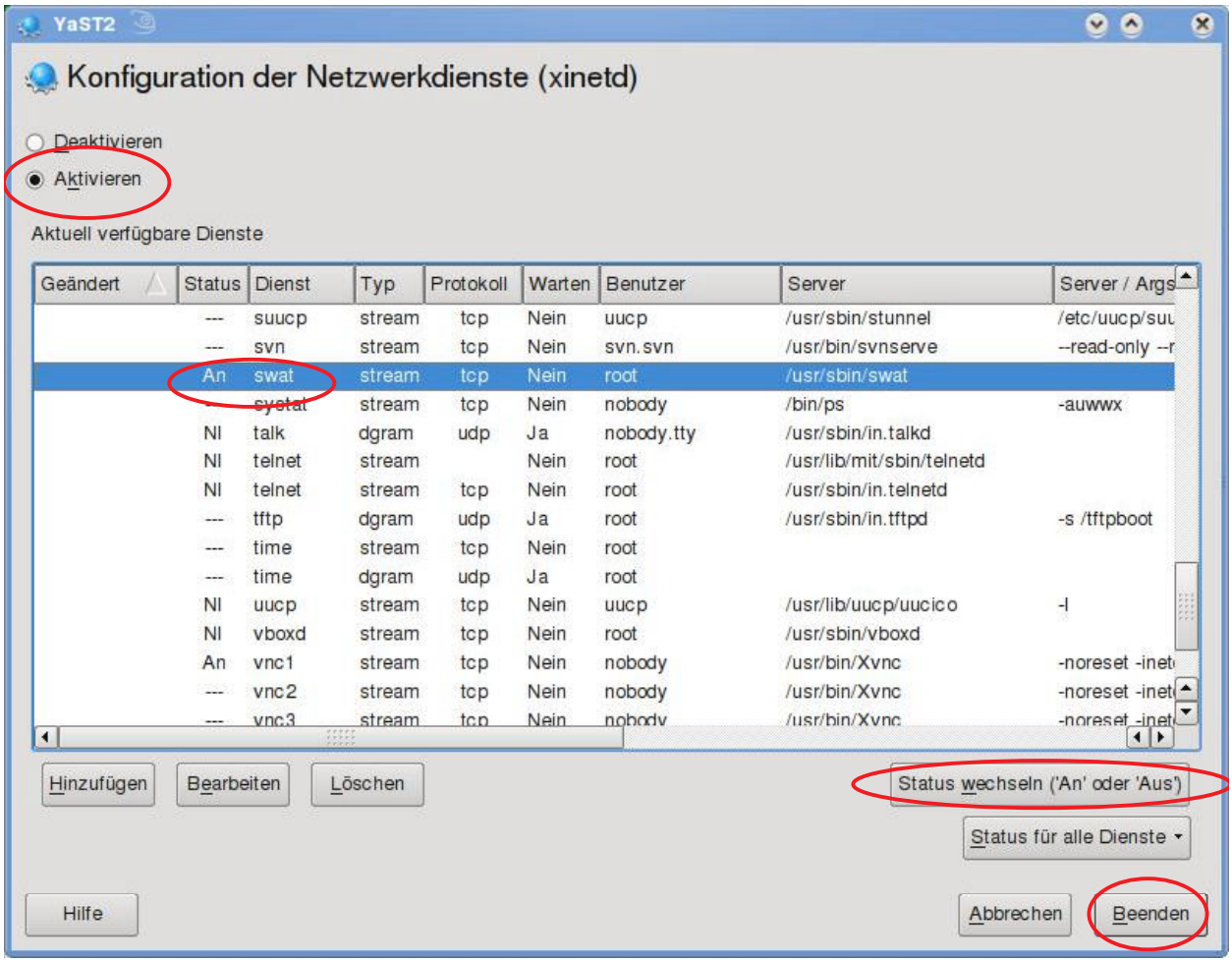
groupadd –g 222 machines

SWAT aktivieren

Zur Konfiguration von SAMBA benutzen SWAT (Samba Web Administration Tool), Dieses muss erst aktiviert werden.

4. „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

5. Die Bedienung von SWAT erfolgt via Browser auf dem Port 901. Starten Sie dazu den Browser Firefox. Dazu klicken Sie in der Schellstartleiste auf die Ikone mit der blauen Weltkugel mit dem Fuchs.
   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.

6. 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

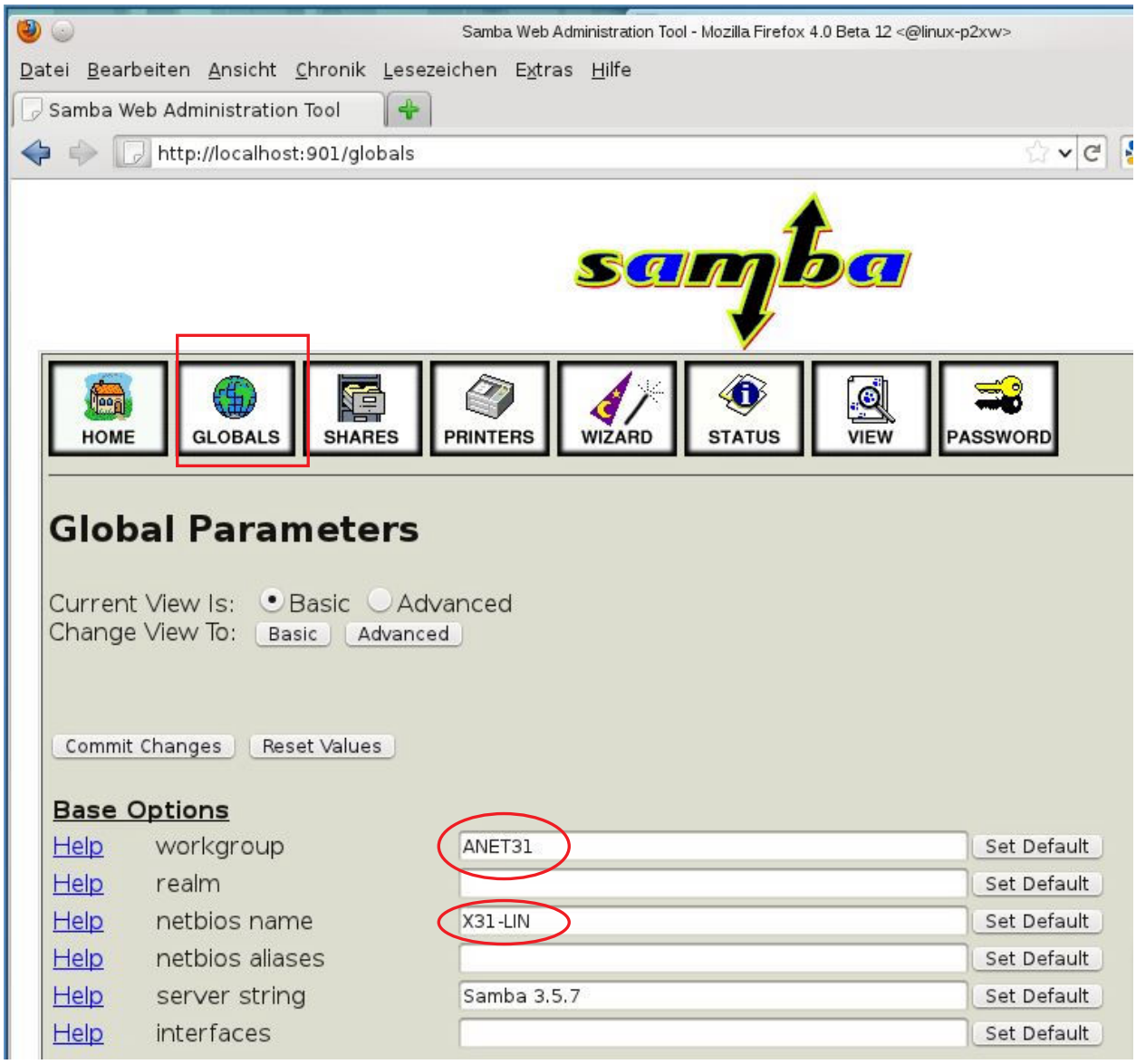
Globale Einstellungen

7. 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.



8. Weitere Einstellungen in Globals (Global Parametes)
   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**] (Commit Changes)

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

9. Blättern Sie zu den „**Sicherheitsoptionen**“ (Security Options)
   Dort sollten folgende Einstellungen bereits bestehen:

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

   Blättern Sie (etwas) weiter zu:

   - admin users [root, zli] (Diese Benutzer können Clients in der Domain eintragen)

- read list [root, zli] (diese Benutzer könne überall lesen)
- write list [root, zli] (diese Benutzer könne überall schreiben)

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

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

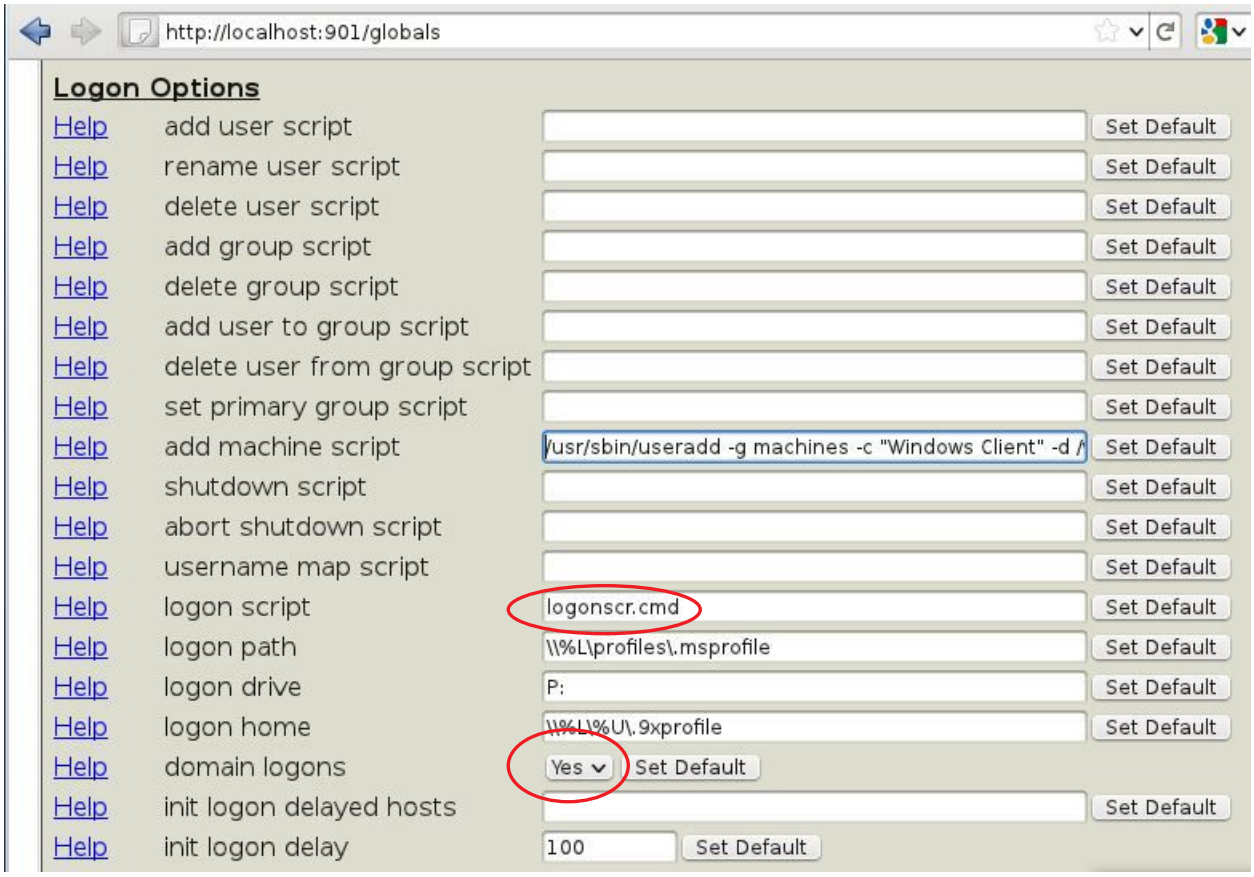
    - add machine script (ergänzen Sie in diesem Feld:)
    [**/usr/sbin/useradd -g machines -c “Windows Client“ -d /var/lib/nobody -s /bin/false %m\$**]

    Hinweis 1: Dies erstellt beim Einbuchen von Clients mit Windows NT, 2000, XP, Vista und Windows 7 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 3 erstellt mit: **groupadd –g 222 machines**

Definitionen als Domain Controller

11. 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.

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



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

13. (kurz darunter:)
    domain logons [**Yes**] Samba funktioniert als Domain-Controller)
14. Blättern Sie weiter zu den „**Browsing Optionen**“ (Browse Options)
    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
15. Damit sind alle Globals Definitionen fertig. Sie werden gespeichert mit (ganz oben links): [**Änderungen speichern**] (Commit Changes)

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.

16. 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]

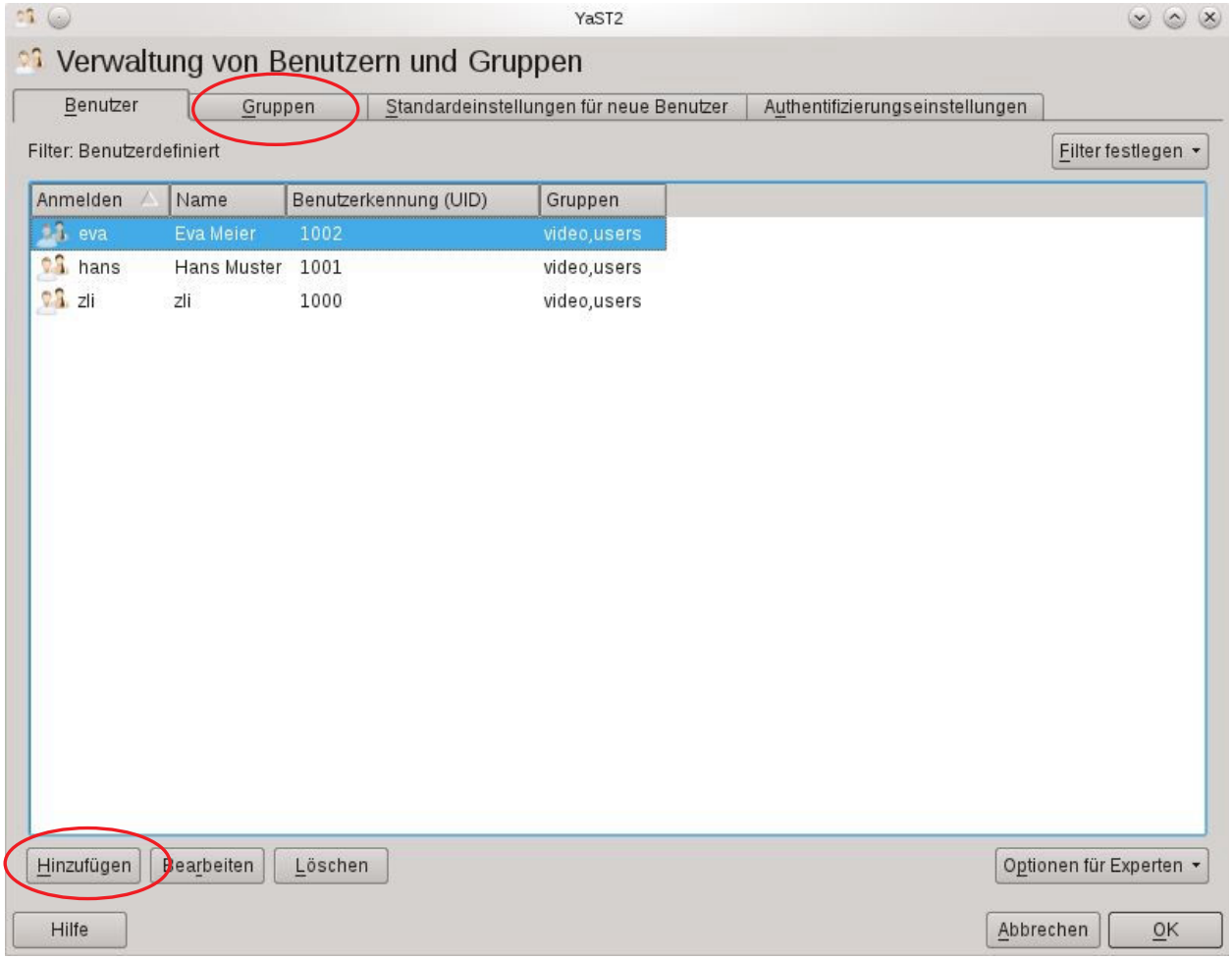
    (erstellen Sie nun den Benutzer eva genau gleich:)

    [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:



17. 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]

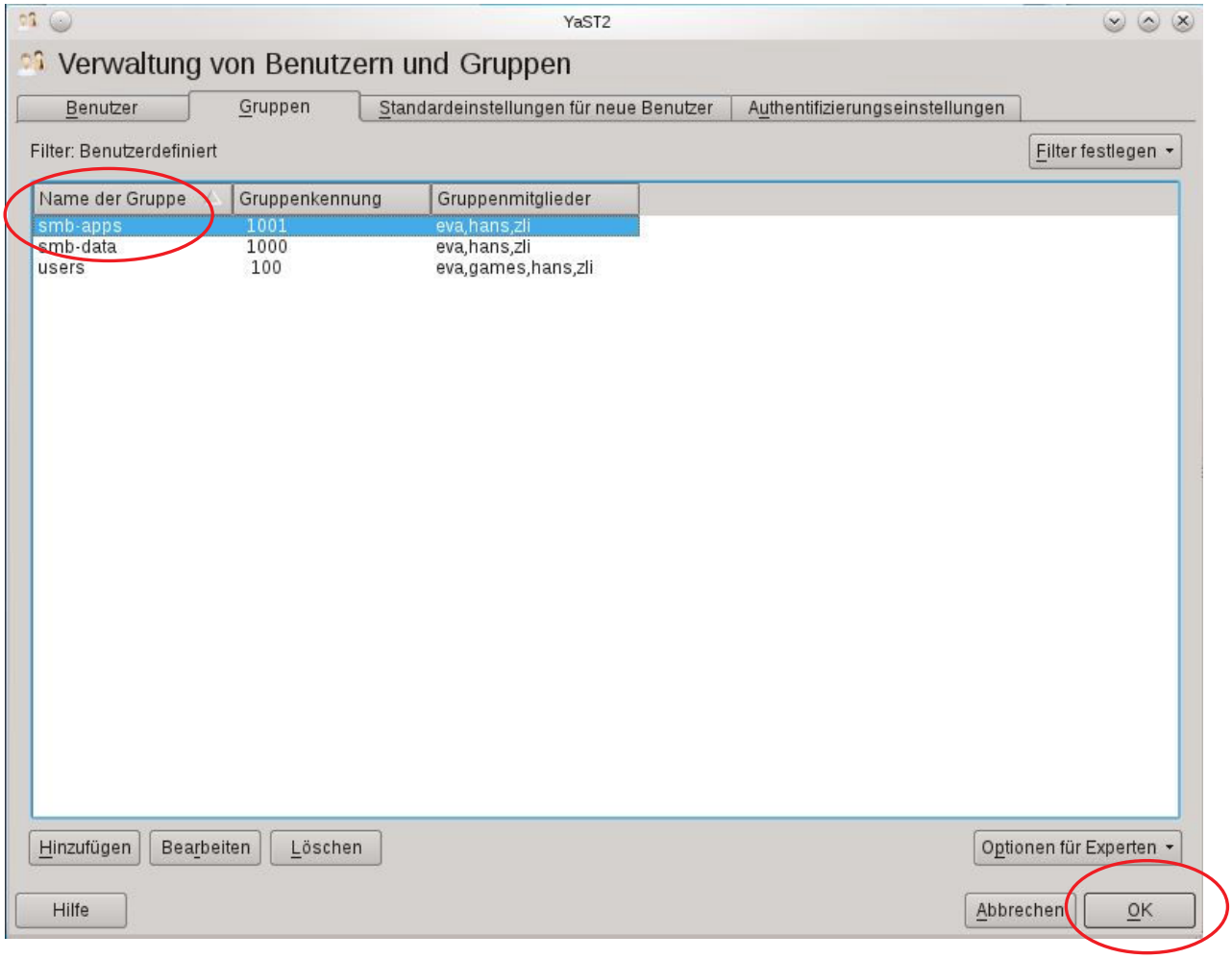
    Nun wird die Gruppe smb-apps erstellt, hier ist nur fho Mitglied:

    [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]

18. 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] (Add New User)

(es erscheint eine Meldung, dass Firefox 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!

19. Zur Kontrolle zeigen wir die Samba-Benutzer an:

pdbedit -L (zeigt die Samba-Benutzer an)

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

20. 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.

Hinweis: . Ob smbd läuft sehen Sie im SWAT unter [Status]. Falls der smbd nicht gestartet werden kann, liegt dies vermutlich am AppArmor Dienst. Falls dies so ist, deaktivieren Sie AppArmor:

YaST → Novell App Armor → AppArmor Kontrollfeld

[ ] AppArmor aktivieren (Hacken entfernen)
[Fertig]

Nun sollte sich der smbd starten lassen.

21. Öffnen Sie ein Befehlsfenster (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 oder lassen Sie es leer

Es erscheint eine Liste der Freigaben und Domänen:

```
zli : bash <@linux-p2xw>
Datei  Bearbeiten  Ansicht  Lesezeichen  Einstellungen  Hilfe
linux-p2xw:/export/samba # smbclient -L localhost
Enter root's password:
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        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 3.5.7)
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        Server               Comment
        ---------            -------
        X31-LIN              Samba 3.5.7

        Workgroup            Master
        ---------            -------
        ANET31               X31-LIN
linux-p2xw:/export/samba #
```

Hinweis 1: Es erscheinen die Standardfreigaben 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.
Hinweis 4: Dauert es lange nach der Passworteingabe und dann kann keine Session aufgebaut werden, muss ev. mehrmals rcsmb restart und rcnmb restart gemacht werden (beobachtet bei openSuSE 12.2). Die beiden laufen korrekt, wenn die PIDs (Prozess IDs) angezeigt werden mit: ll /var/run/samba/

```
#   ll  /var/run/samba/
   total 8
   -rw-r--r-- 1 root root 5 Oct 31 08:50 nmbd.pid
   -rw-r--r-- 1 root root 5 Oct 31 08:50 smbd.pid
```

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)

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

    localhost:901
    (Anmelden als root)

    Reiter [**Shares**] klicken

23. 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)	

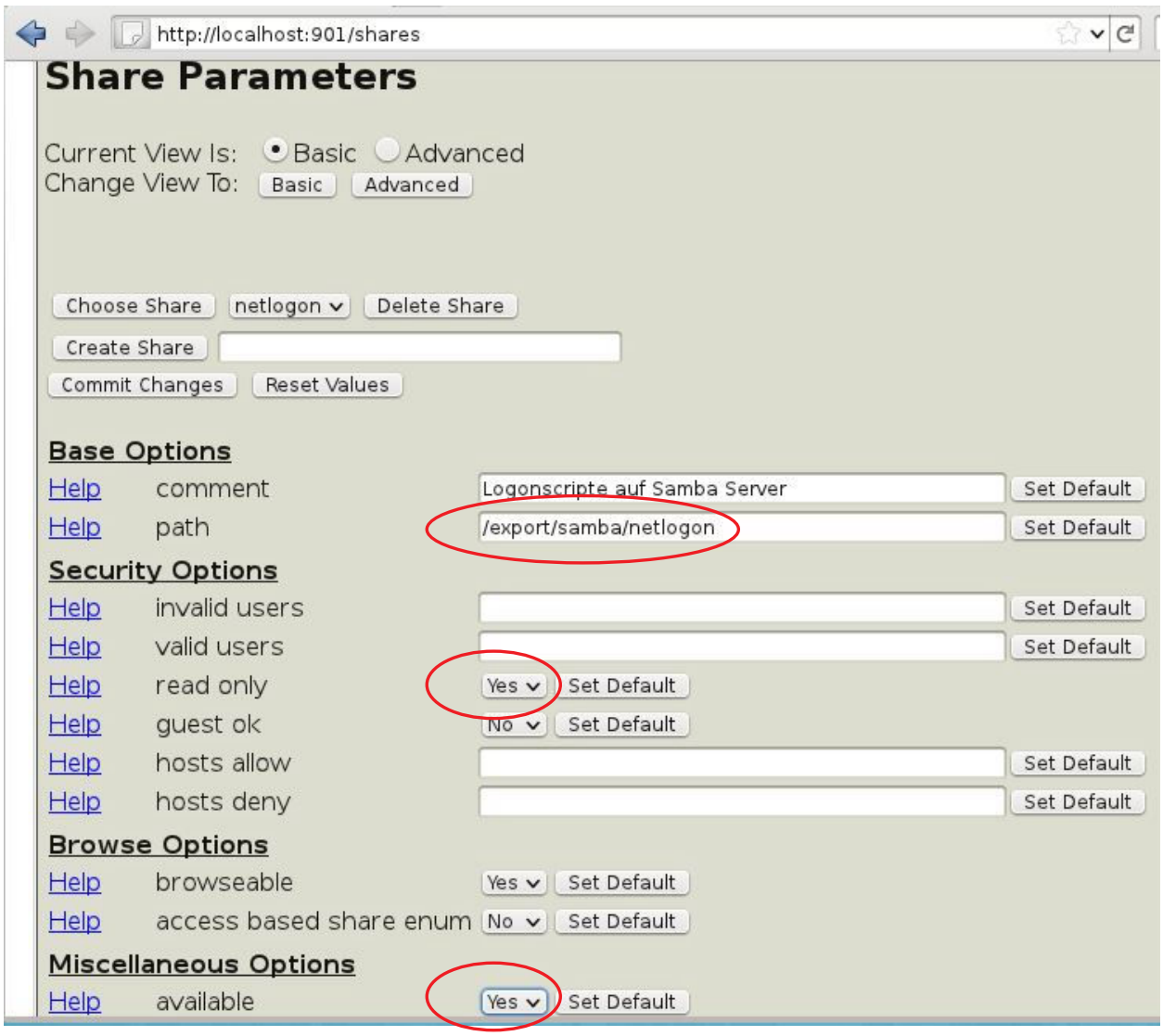
    Browsing Optionen

browseable	[Yes]	(Inhalt kann angezeigt werden)

    Verschiedene Optionen (Miscellaneous Options)

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

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



Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitoptionen (Security Options)

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.

24. 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!)	

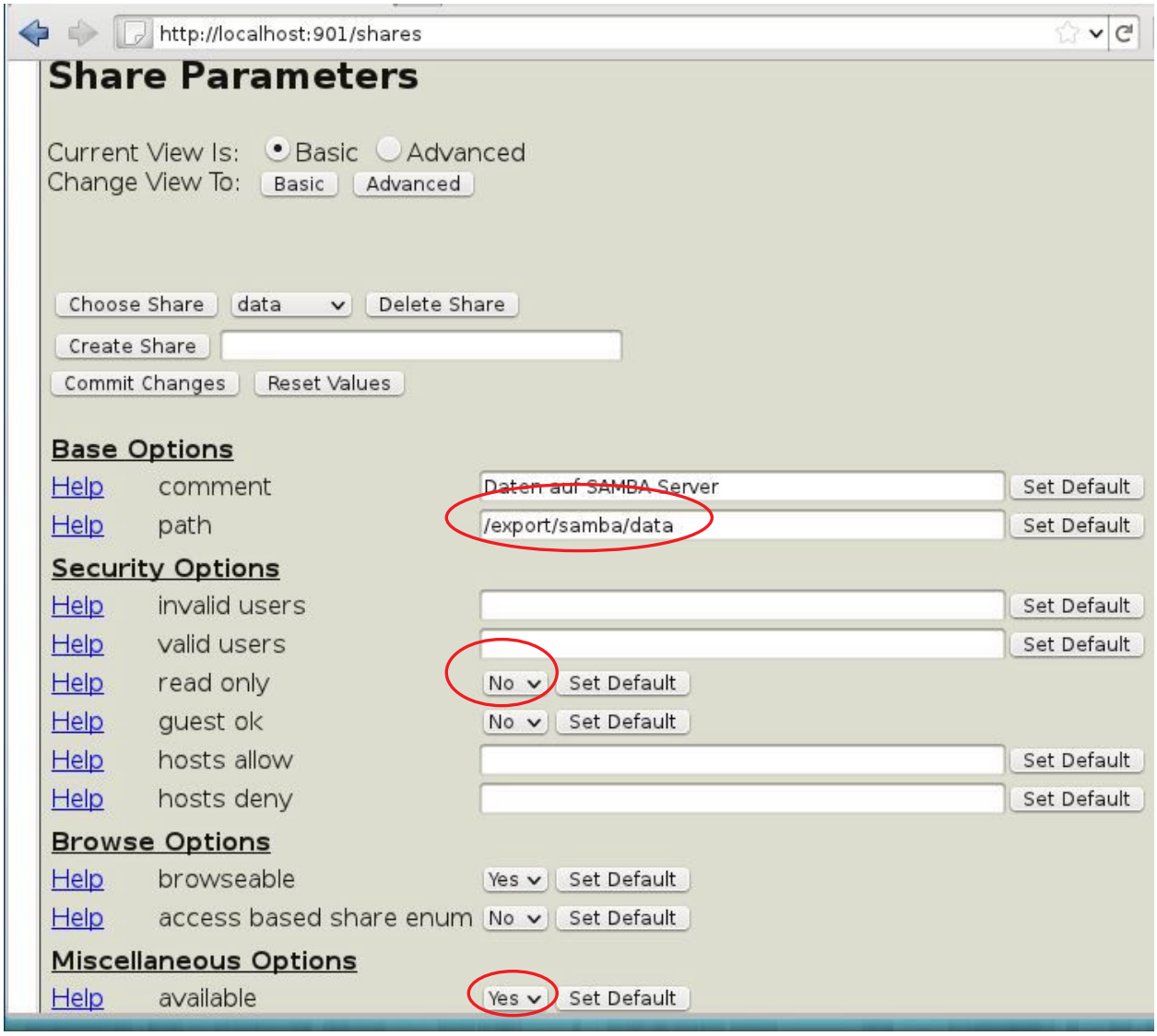
Browsing Optionen

browseable	[Yes]	(Inhalt kann angezeigt werden)

Verschiedene Optionen (Miscellaneous Options)

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

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

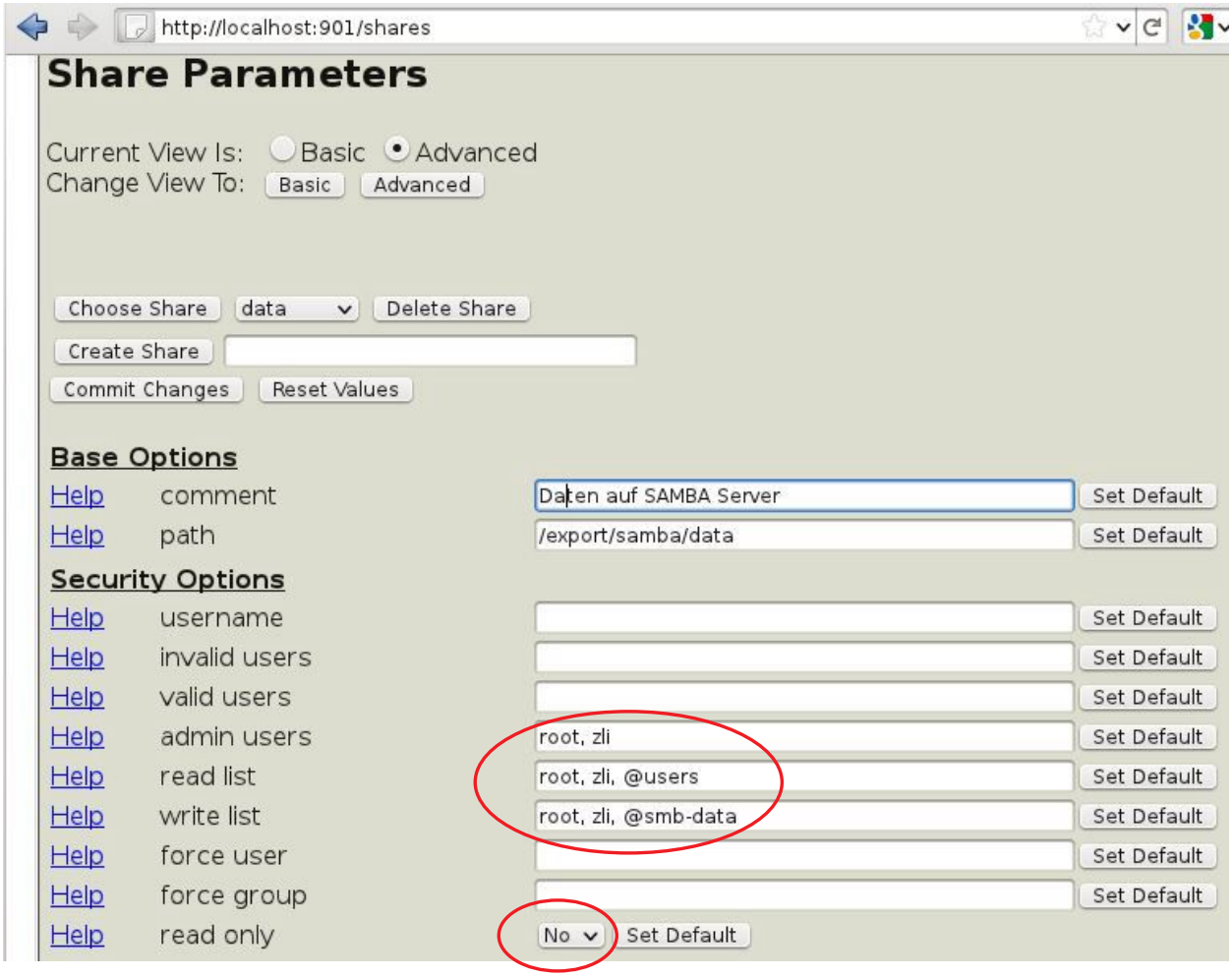


Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen (Security Options)

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**] (Commit Changes)



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.

25. 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**] (Commit Changes)

Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen (Security Options)

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**] (Commit Changes)

26. 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 (Miscellaneous Options)
availlable [**Yes**] (sonst nicht benutzbar)

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

Nun passe wir die Schreibrechte an:
[Erweiterte Ansicht]

Sicherheitsoptionen (Security Options)

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.

27. 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.

```
zli : bash <@linux-p2xw>
Datei  Bearbeiten  Ansicht  Lesezeichen  Einstellungen  Hilfe
linux-p2xw:/export/samba # rcsmb restart
Shutting down Samba SMB daemon                                   done
Starting Samba SMB daemon                                        done
linux-p2xw:/export/samba # smbclient -L localhost
Enter root's password:
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        Sharename       Type      Comment
        ---------       ----      -------
        profiles        Disk      Network Profiles Service
        users           Disk      All users
        groups          Disk      All groups
        print$          Disk      Printer Drivers
        netlogon        Disk      Logonscripte auf Samba Server
        data            Disk      Daten auf SAMBA Server
        apps            Disk      Programme auf SAMBA Server
        public          Disk      Tauschbox auf SAMBA Server
        IPC$            IPC       IPC Service (Samba 3.5.7)
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        Server               Comment
        ---------            -------
        X31-LIN              Samba 3.5.7

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

28. 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.
```

29. 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)

30. 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!)

31. 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:

32. 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\optra-c540n       (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.

33. Sie können nun den LogonScript testen. Das Laufwerk z: mit NETLOGON 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!

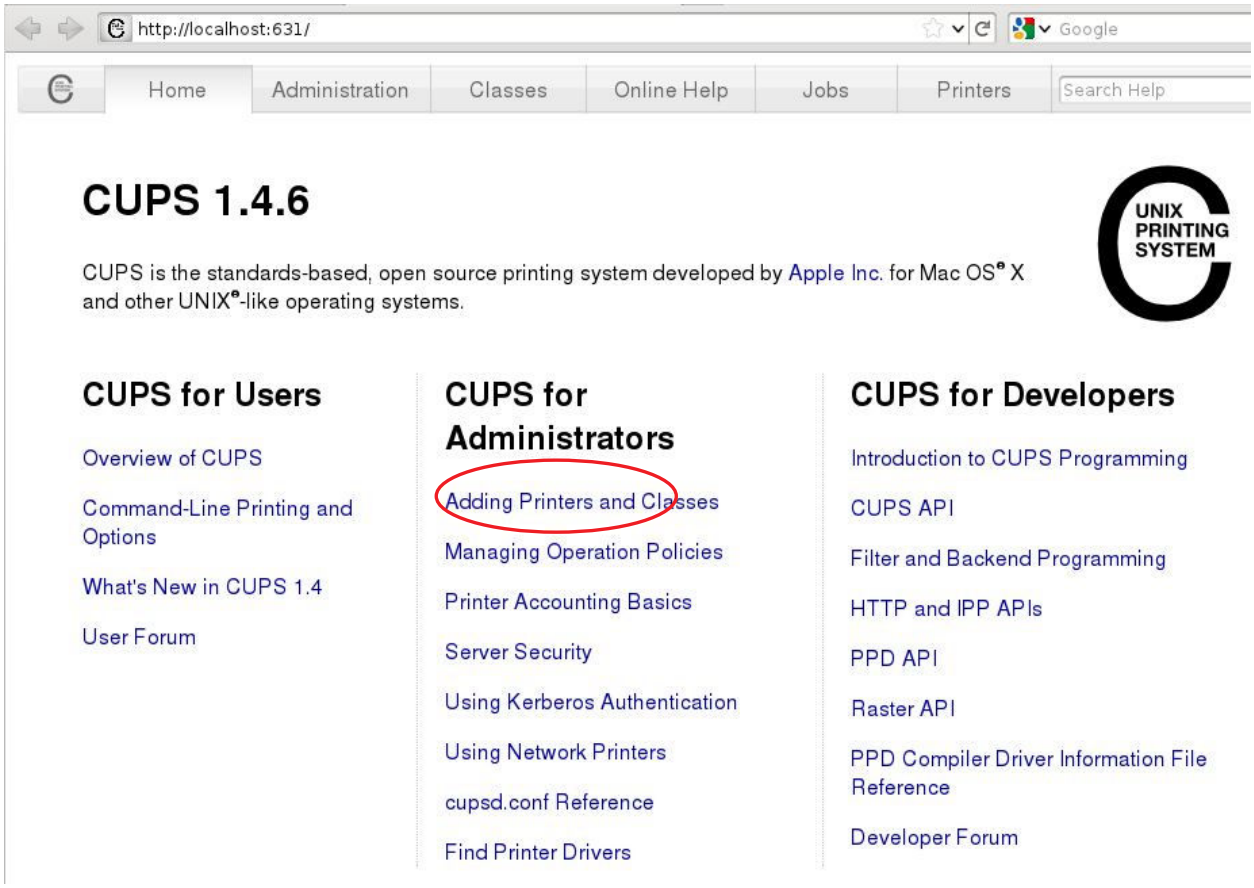
Drucker einrichten

Damit alle Clients drucken können, richten wir noch einen Drucker ein. Dieser wird standardmässig von SAMBA freigegeben. Im LogonScript hängen wir den Drucker optra-c540n an den Port LPT3 an. Auf dem Client muss deshalb ein (lokaler) Druckertreiber am Anschluss LPT3 installiert werden. Man kann den Drucker via YaST → Hardware → Drucker einrichten oder – eleganter – via CUPS (Common Unix Printing System).

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

35. Wir starten die Verwaltungsseite von CUPS:

    Im Firefox geben wir folgende URL ein**: localhost:631** [Enter]

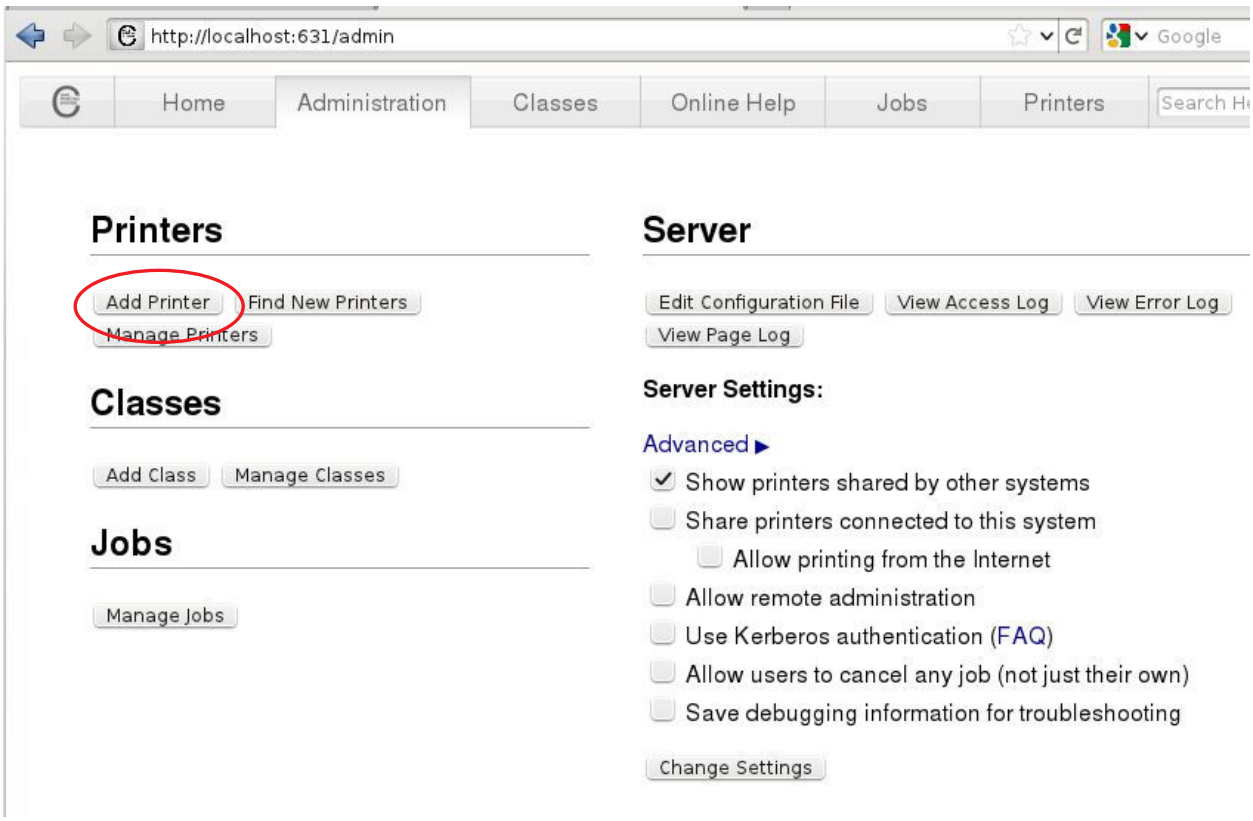


Nun wählen wir [**Adding Printers and Classes**].

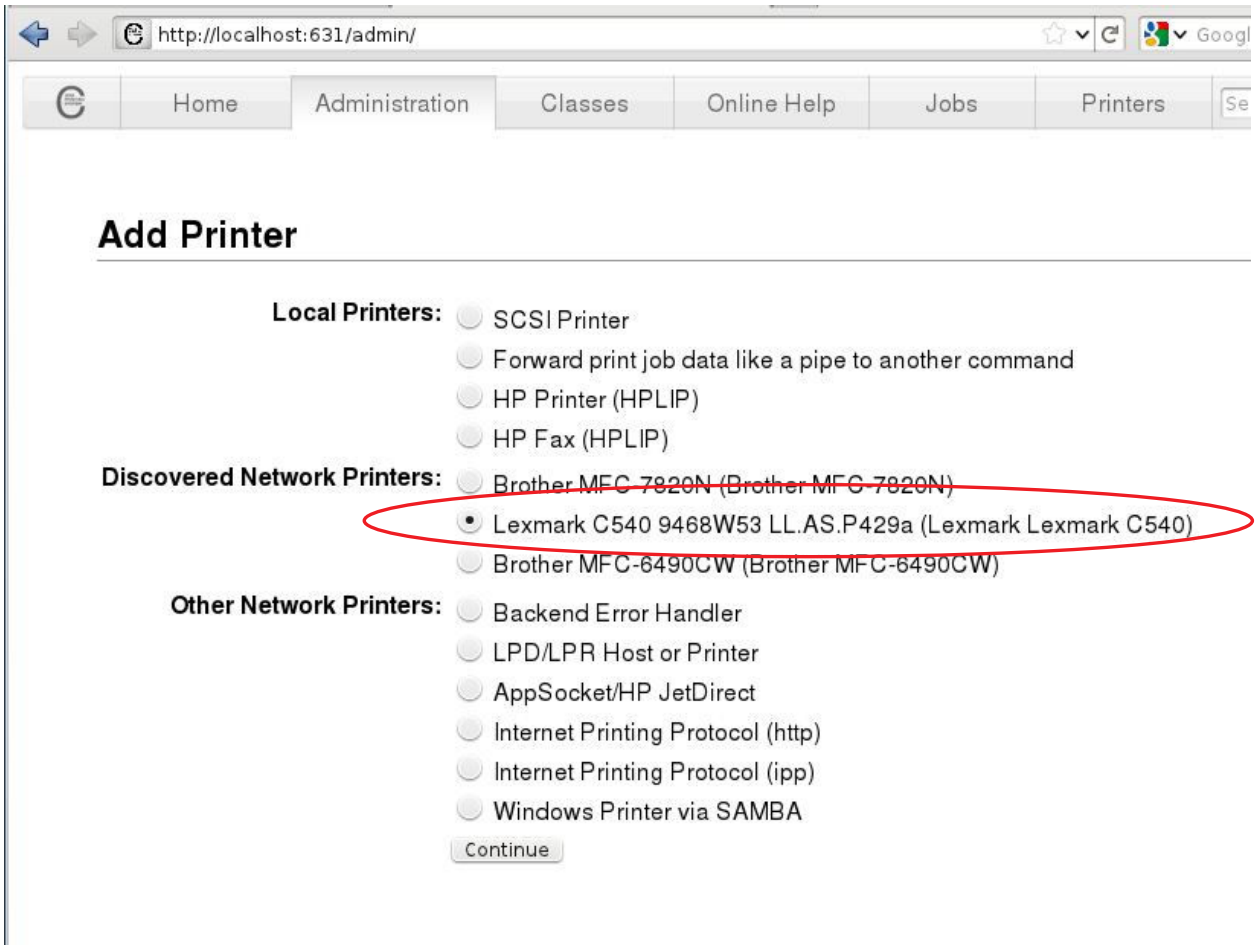
36. Wir fügen nun den Drucker hinzu. Schalten Sie den Drucker ein. Auf dem folgenden Bild drüken Sie auf [**Add Printer**]

    Es erscheint ein Anmelde-Bild:

    Benutzer: **root**
    Passwort: xxxxxxxxx



37. Falls der Drucker im gleichen Subnet und eingeschaltet, wird er automatisch angezeigt:

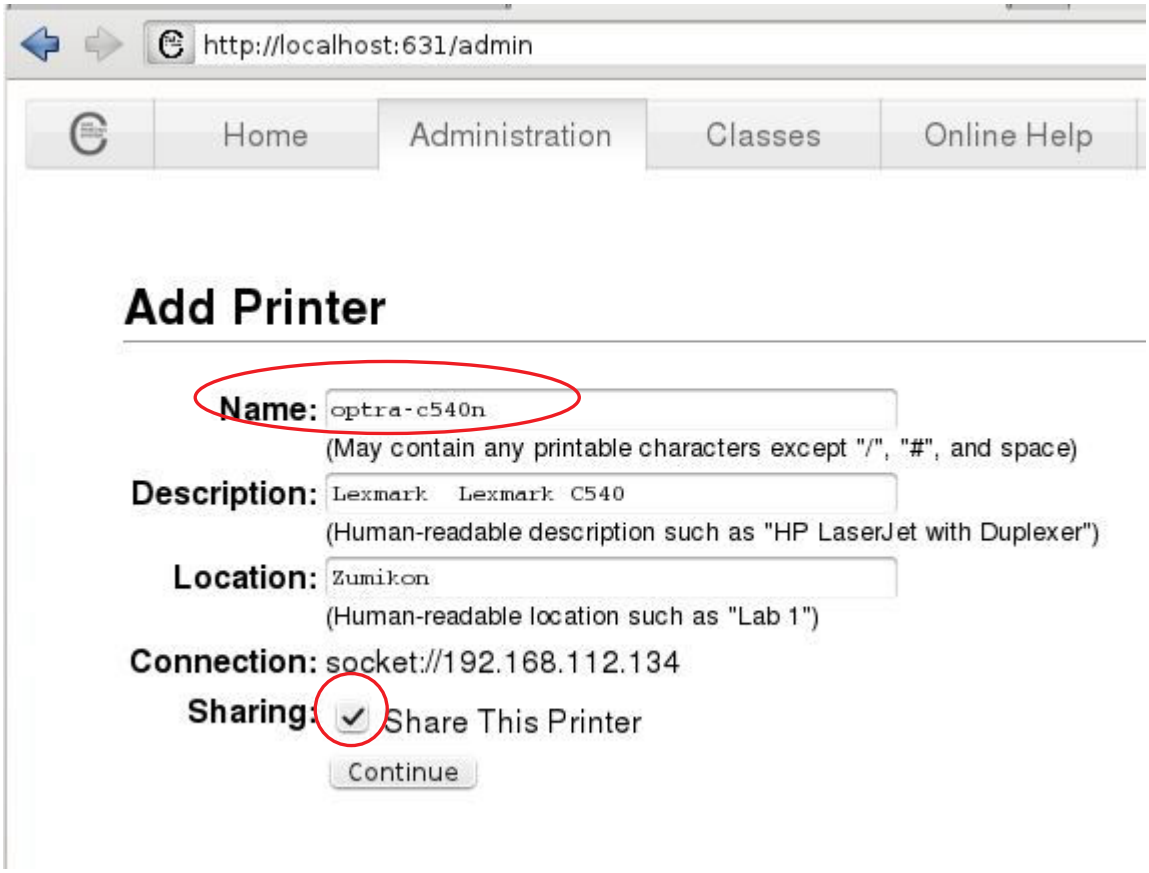


Wir wählen den gefundenen Lexmark C540.

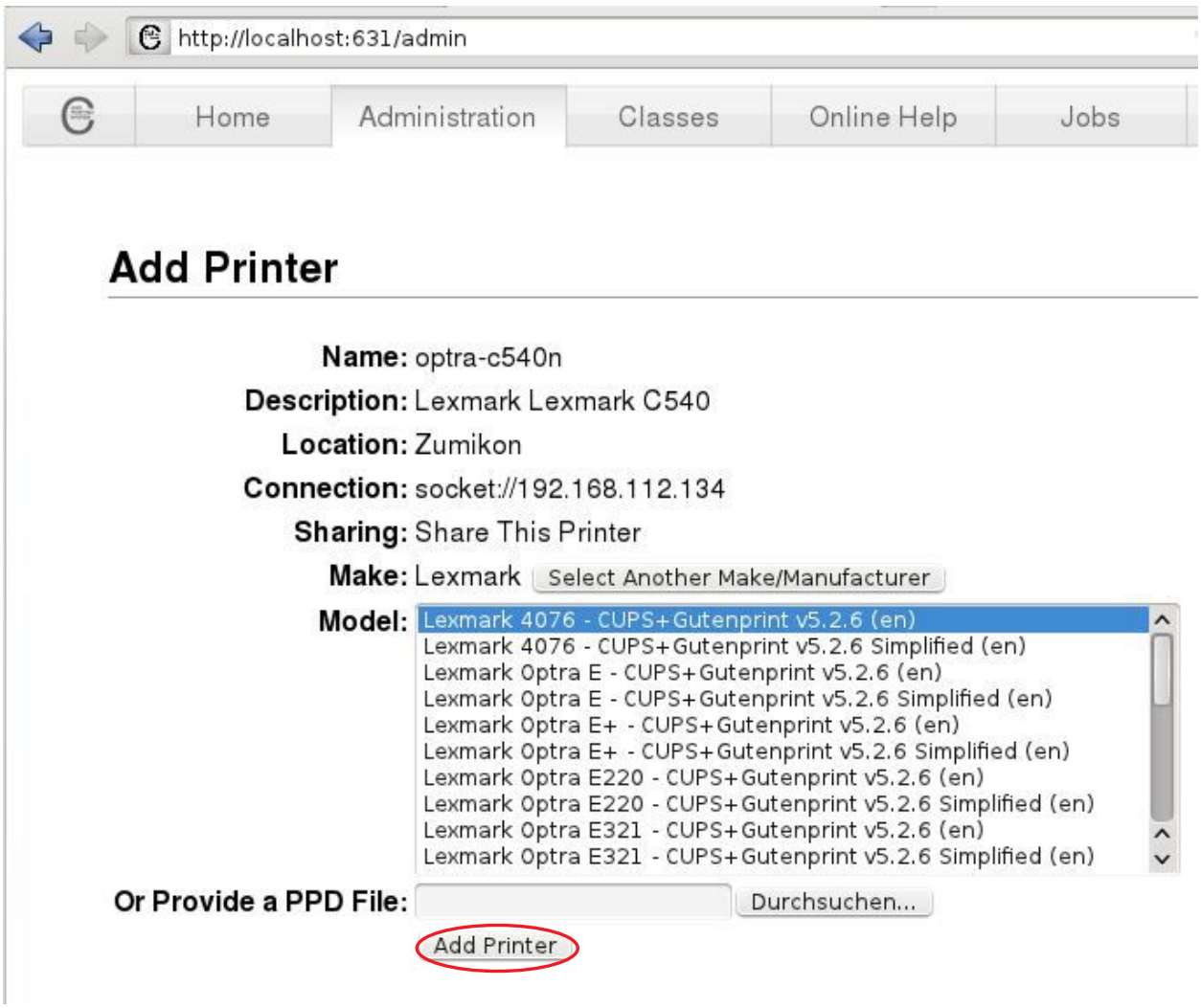
Hinweis: Falls der Drucker nicht gefunden wird, wählen Sie [AppSocket/HP JetDirect und geben dann die IP-Adresse des Drucker an.

38. Geben sie dem Drucker einen (kürzeren) Namen. Dieser Name ist dann auch gleich der Freigabe-Name und dieser sollte **nicht länger als 15 Zeichen** sein und **keine Leerzeichen** enthalten, sonst können nicht alle Systeme den Drucker benutzen.

    Durch Markieren von [**x**] „Share This Printer“ wird dieser gleich freigegeben.

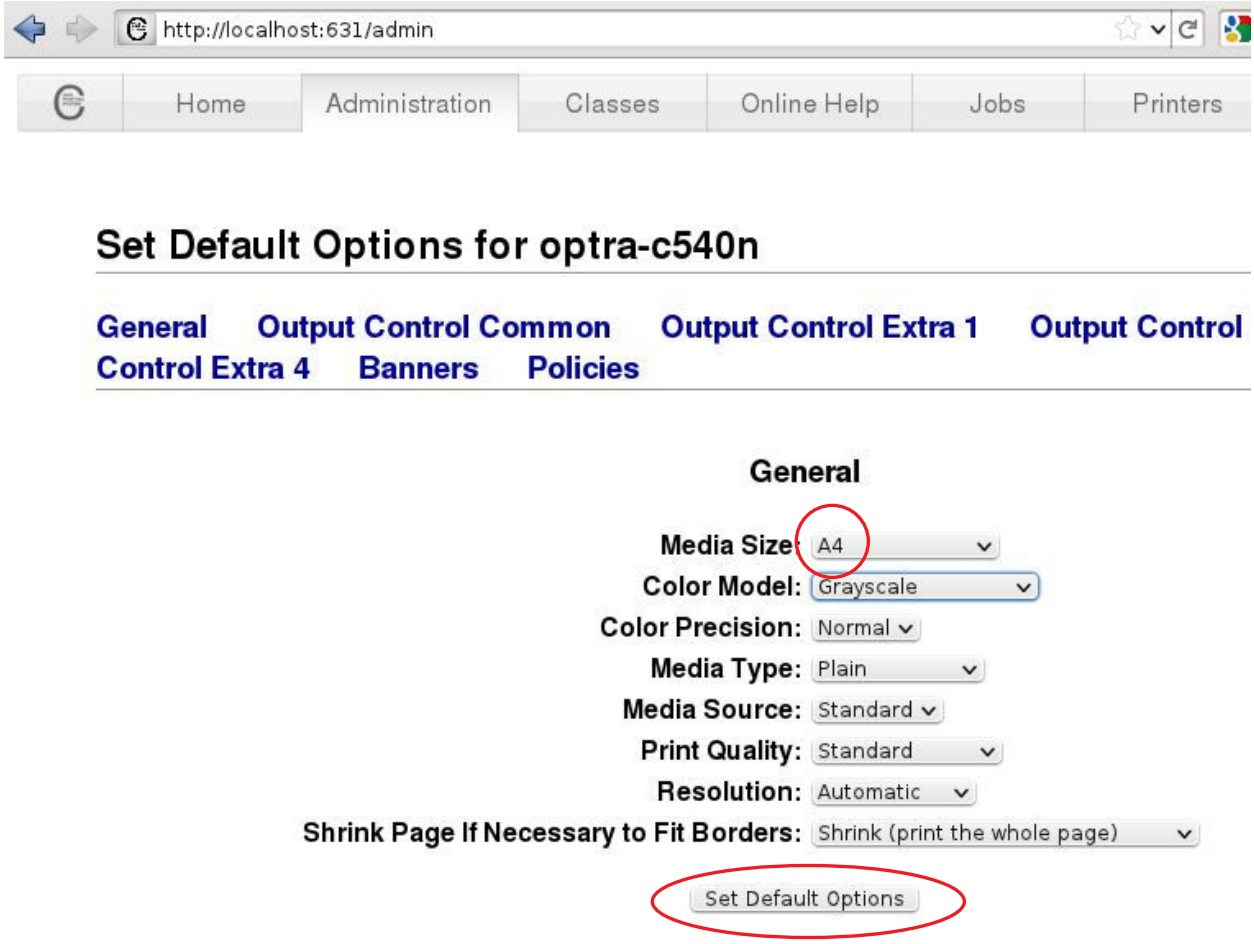


Drücken sie auf [Continue]. Nun wird die Liste der Druckertreiber aufbereitet und angezeigt, Dies dauert – vor allem beim ersten Mal - einige Zeit!



Der vorgeschlagene Treiber sollte passen. Drücken Sie auf [**Add Printer**]

39. Legen Sie das bei uns übliche **A4** Format fest. Dann drücken Sie auf [**Set Default Options**]



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

    Standardmässig ist der Drucker bereits unter seinem Namen (hier: optra-c540n) freigeben.
    Sie könnendies überprüfen mit:

    rcsmb restart (smbd neu starten)

    smbclient -L localhost

```
zli : bash <@linux-p2xw>
Datei  Bearbeiten  Ansicht  Lesezeichen  Einstellungen  Hilfe
linux-p2xw:/export/samba # smbclient -L localhost
Enter root's password:
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        Sharename       Type      Comment
        ---------       ----      -------
        profiles        Disk      Network Profiles Service
        users           Disk      All users
        groups          Disk      All groups
        print$          Disk      Printer Drivers
        netlogon        Disk      Logonscripte auf Samba Server
        data            Disk      Daten auf SAMBA Server
        apps            Disk      Programme auf SAMBA Server
        public          Disk      Tauschbox auf SAMBA Server
        IPC$            IPC       IPC Service (Samba 3.5.7)
        optra-c540n     Printer   Lexmark  Lexmark C540
Anonymous login successful
Domain=[ANET31] OS=[Unix] Server=[Samba 3.5.7-1.17.1-2505-SUSE-SL11.4-i386]

        Server               Comment
        ---------            -------
        X31-LIN              Samba 3.5.7

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

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 Treiber, 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.

41. 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

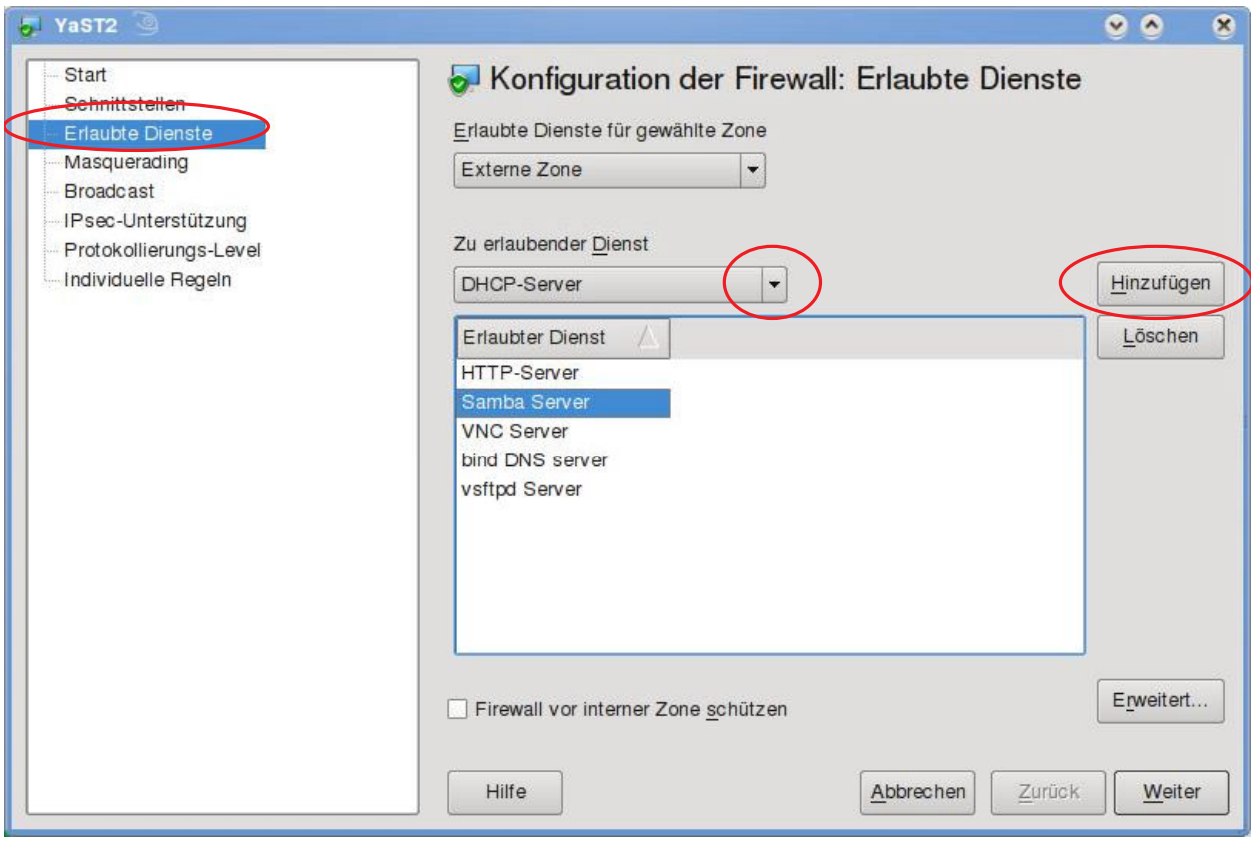
Vergessen Sie nicht, den Firewall zu deaktivieren oder (besser) die Ports 137, 138, 139 und 445 freizuschalten. Dise sind via YaST -->Sicherheit und Benutzer --> Firewall unter „erlaubte Dienste“ mit SAMBA zusammengefasst. Sonst müssen Sie jedes Mal den Firewall manuell stoppen mit *rcSuSEfirewall2 stop*.

42. Starten Sie YaST:

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

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

43. 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 11 ha*ben 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.

44. 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
45. 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
```

46. 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]
47. 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

48. 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" -d /var/lib/nobody -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
        server string = Samba 3.5.7
        map to guest = Bad User
        printcap name = cups
        add machine script = /usr/sbin/useradd -g machines -c "Windows
Client" -d /var/lib/nobody -s /bin/false %m\$
        logon script = logonscr.cmd
        logon path = \\%L\profiles\.msprofile
        logon drive = P:
        logon home = \\%L\%U\.9xprofile
        domain logons = Yes
        usershare allow guests = Yes
        admin users = root, zli
        read list = root, zli
        write list = root, zli
        cups options = raw
```

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, apps, public

```
[netlogon]
        comment = Logonscripte auf Samba Server
        path = /export/samba/netlogon
        read list = root, zli, @users

[data]
        comment = Daten auf SAMBA Server
        path = /export/samba/data
        read list = root, zli, @users
        write list = root, zli, @smb-data
        read only = No

[apps]
        comment = Programme auf SAMBA Server
        path = /export/samba/apps
        read list = root, zli, @users
        write list = root, zli, @smb-apps

[public]
        comment = Tauschbox auf SAMBA Server
        path = /export/samba/public
```

```
read list = root, zli, @users
write list = root, zli, @users
read only = No
```