9 Linux als File- und Print-Server für Windows-Clients

In mehrschichtigen Client-Server- oder Thin Client-Umgebungen lassen sich

- die Benutzerschicht,
- die Verarbeitungsschicht und
- die Ebene der Datenhaltung

unterscheiden.

In reinen Linux-Umgebungen ist es üblich, das Network File System (*NFS*) zum Dateiaustausch zu verwenden, soweit man nicht per FTP auf andere Linux-Server zugreift. NFS ist für den Multi User-Betrieb unter Unix ausgelegt. Die Server-Komponente von NFS ist Bestandteil des SuSE Linux-Kernels. Für den Windows-PC gibt es bisher wohl keine geeignete freie Client-Software, jedoch etliche kommerzielle NFS-Clients wie z. B. Hummingbird Exceed (`http://www.hummingbird.com`).

Wenn Sie ohne kommerzielle Software Daten zwischen einem Linux-Server und einem Windows-PC austauschen wollen, können Sie Samba verwenden.

Samba ist eine freie Version eines Server Message Block-Servers. Das Server Message Block (*SMB*-)Protokoll basiert auf der Software-Schnittstelle NetBIOS. Es bietet PCs mit Microsoft Windows-Versionen über das Transport-Protokoll TCP/IP die gewünschten Datei- und Druckdienste. Zudem können Linux-Server anderen PCs ihre Druckdienste zur Verfügung stellen.

Dieses Kapitel beschreibt, wie Sie mit Samba einen Linux-Server im Netz zu einem Datei- und Druck-Server für Windows-PCs gestalten.

Mit Linux und Samba gewinnt man im Vergleich zu proprietären Servern mit Microsofts Server-Betriebssystemen Windows NT-Server, Windows 2000-Server oder Windows Server-2003 mehr Stabilität und höhere Datensicherheit und spart obendrein Lizenzkosten. Auch unterwirft man sich weder Update-Zwängen noch knebelnden Verträgen.

Dieses Kapitel befasst sich ausführlich mit den folgenden Arbeitsschritten:

- Vorarbeiten (9.1),
- Passwortverschlüsselung (9.3),
- Samba-Passwörter (9.4),
- Konfiguration des Samba-Servers (9.5),

- Freigaben (9.6),
- Drucken von Windows-Clients (9.7),
- Domain-Logons (9.8),
- Samba-Server als Mitglied einer Windows NT/2000/2003 -Domain (9.9),
- Informationsquellen (9.10).

9.1 Vorarbeiten

9.1.1 Samba auf dem Linux-Server nachinstallieren

Die Standardkonfiguration von SuSE 9.2 enthält das Paket `samba`. Sollte es fehlen, lässt es sich mit YaST schnell nachinstallieren.

Nach der Installation müssen Sie Ihren Samba-Server konfigurieren und an die Infrastruktur Ihres lokalen Netzes anpassen. Seine Konfigurationsdatei `/etc/samba/smb.conf` ist ähnliche wie eine ini-Datei von Windows aufgebaut.

```
[global]
   workgroup = TUX-NET
   os level = 2
```

Die Datei gliedert sich in unterschiedliche Abschnitte, die jeweils mit einem Bezeichner beginnen, der in eckigen Klammen gesetzt ist. Der angegebene Ausschnitt zeigt den Anfang des Abschnitts *global*. Danach kommt dann jeweils eine Option (z. B. *workgroup*) und nach einem Gleichheitszeichen der zugehörige Wert (hier *TUX-NET*). Sowohl die Optionen als auch die Werte dürfen Leerzeichen beinhalten.

Die folgenden Abschnitte führen Sie schrittweise in die Samba-Konfiguration ein.

9.1.2 Automatischer Start der Server-Programme

Damit die zugehörigen Server-Programme (*Dämonen*) `smbd` (*server message block daemon*) und `nmbd` (*Netbios nameser daemon*, Name-Server für Windows-Rechnernamen) beim Booten des Servers mit starten,

- sollte man entweder mit dem `YaST-Runlevel-Editor` die Dienste `smb` und `nmb` aktivieren
- oder in der Konsole als `root` eingeben:

```
insserv smb
insserv nmb
```

Nach diesen Schritten starten Sie den Samba-Server von Hand mit

```
rcsmb start
rcnmb start
```

9.1.3 Installation der Windows-PCs prüfen

Außer TCP/IP muss auf den Windows-PCs zum Nutzen von Samba der Client für Microsoft-Netzwerke installiert sein.

Um zu überprüfen, ob beides installiert ist, gehen Sie auf einem Windows 9x-PC in der *Systemsteuerung* zu *Netzwerk* und vergewissern sich in der Registerkarte *Konfiguration,*

- dass der Client für Microsoft-Netzwerke installiert ist und
- dann in den *Eigenschaften von TCP/IP* in der Karteikarte *Bindungen,* dass der Client für Microsoft-Netzwerke ausgewählt ist.

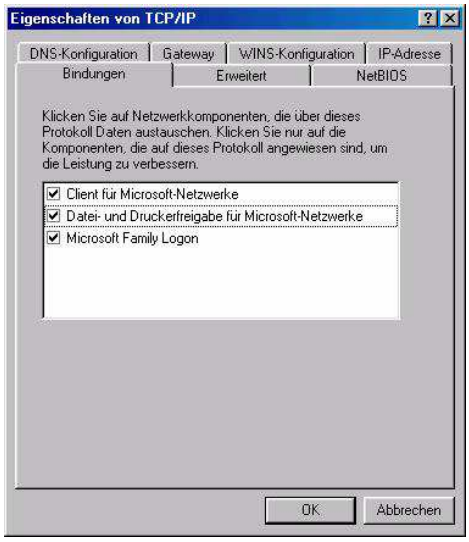

Abbildung 9.1: Bindungen

9.1.4 Arbeitsgruppe der Windows-PCs

Damit Windows-PCs auf Samba-Server zugreifen können, müssen sie alle derselben Arbeitsgruppe angehören und verschiedene Namen haben.

Überprüfen und korrigieren Sie auf den Windows-PCs die Einträge in der Karteikarte *Identifikation* des Dialogs *Netzwerk*, den Sie ja oben schon über *Start* • *Einstellungen* • *Systemsteuerung* aufgesucht haben.

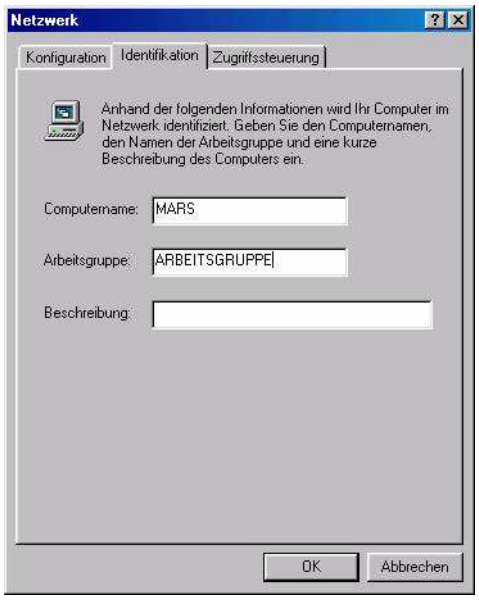

Abbildung 9.2: Identifikation

SuSEs Samba-Konfiguration ist für eine Arbeitsgruppe namens `TUX-NET` voreingestellt. Wenn Sie für Samba das NT-Domänensicherheitsmodell wählen, tragen Sie hier am besten den Namen der NT-Domäne ein. Die folgenden Ausführungen nutzen eine Arbeitsgruppe namens `ARBEITSGRUPPE`.

Sofern Samba bereits gestartet ist sehen Sie jetzt schon in der Netzwerkumgebung des Windows-PCs den oder die Linux-Server. Wenn nicht, hilft es häufig, den Windows-PC neu zu starten oder mit der Suchfunktion von Windows nach ihnen zu suchen, eventuell auch über die IP-Adresse. Da der Windows-PC, der die Liste aller in der Arbeitsgruppe vorhandenen Rechner verwaltet, diese Liste in Intervallen aktualisiert, kann dies bis zu 15 Minuten dauern.

Sollte auch nach einer angemessenen Wartezeit kein Zugriff auf den Samba-Server möglich sein, dann hilft ein Blick in die Log-Dateien meist weiter. Die Log-Datei für den smbd finden Sie unter `/var/log/samba/log.smbd`, die für den nmbd unter `/var/log/samba/log.nmbd`. Eventuelle Fehler in der Konfigurationsdatei können Sie mittels

```
testparm
```

überprüfen. Das kleine Hilfsprogramm überprüft die Konfigurationsdatei für Sie und zeigt die ermittelten Einstellungen und Freigaben an.

9.2 Planen von Linux-Servern für Datei- und Druckdienste

Daten sind das wertvollste Gut aller Einrichtungen, sie sind wertvoller als Anwendungen. Ein Verlust der Daten kann das Überleben einer Firma gefährden. Dem sicheren Speichern von Daten muss man also viel Sorgfalt widmen.

Bei der Server-Hardware für die Datenhaltung sollte man am wenigsten sparen; SCSI-Systeme mit RAID-Controllern und im laufenden Betrieb auswechselbaren Netzteilen und Festplatten und sofort verfügbaren Reserveplatten sind für wertvolle Daten genauso wichtig wie Systeme zur Datensicherung.

Beim Planen der Installation sollten Sie darauf achten, dass Benutzer das System nicht absichtlich oder versehentlich in die Knie zwingen können. Dazu gehört sorgfältiges Planen der Dateisysteme.

Zumindest sollten Sie das Root-System nicht zur Datenhaltung zur Verfügung stellen. Böswillige oder unvorsichtige Benutzer könnten sonst die Root-Partition vollschreiben und damit das System zum Stillstand bringen.

Disk-Quotas (siehe Kapitel 3) sorgen dafür, dass Benutzer keine zu großen Teile der Festplatten mit Beschlag belegen können.

9.2.1 Die Identitäten von Samba

Samba stellt Freigaben (*Shares*) bereit und kann mit verschiedenen Identitäten beeinflussen, wer wann und wie prüft, ob ein Windows-Client auf eine Freigabe auf einem Linux-Server zugreifen darf.

Diese kann man global oder individuell oder durch einen eigenen Samba-Server regeln. Die Einstellung erfolgt jeweils über den Eintrag `security=` in der zentralen Samba-Konfigurationsdatei `/etc/smb.conf`. Für `security=` stehen Ihnen die folgenden Werte zur Verfügung:

- `share`,
- `user`,
- `server`,
- `domain` und
- `ads`.

Im einfachsten Fall

```
security = share
```

gliedert sich Samba in einem Windows 9x-Peer-to-Peer-Netzwerk als weiterer Rechner einer Arbeitsgruppe ein. Dort verhält er sich bei der Zugriffskontrolle wie

ein Windows 9x-PC, bei dem auf der Registerkarte *Zugriffssteuerung* der Netzwerkeigenschaften die Option *Zugriffssteuerung auf Freigabeebene* aktiv ist.

Beim Aufbau der Verbindung zwischen der Freigabe auf dem Linux-Server und dem Windows-PC schickt der Windows-PC lediglich ein Passwort an Samba. Um die Sicherheitsregeln bei Linux nicht zu verletzen, bei denen Benutzer eine Kombination aus Benutzernamen und Passwort angeben müssen, versucht Samba so lange, ein solches Paar zu finden, bis es entweder den Zugriff gewährt oder aber verhindert.

Eine weitere Variante der Zugriffskontrolle ist der Zugriff auf Benutzerebene durch den Eintrag

```
security = user
```

in der Datei `smb.conf`, der Voreinstellung für Samba ab Version 2.0. Hierbei vergleicht Samba das beim Verbindungsaufbau vom einem Benutzer angegebene Paar aus Benutzername und Passwort mit Einträgen einer lokalen Benutzerdatenbank auf dem Linux-Server, d. h. Samba überprüft die Daten auf der Maschine, auf der sich die Freigabe befindet. Wenn sich mehrere SMB-Server in einem Netzwerk befinden, muss man dann mühselig die Benutzerkonten auf jedem Samba-Server einrichten und pflegen.

Ein eigener Samba-Server kann als dritte Variante zentral alle Zugriffsanfragen der anderen Server entgegennehmen, um diese zentral zu authentifizieren. Dies erreicht man durch die Einträge:

```
security = server
password server = name1, name2
```

wobei man zusätzlich zum geänderten Eintrag bei `security` auch den Netbios-Namen eines oder mehrerer Samba-Server (hier im Beispiel `name1`, `name2`) angeben muss, der bzw. die die Authentifizierung durchführen.

Als vierte Variante kann man den Samba-Server zu einem vollwertigen Mitglied einer Windows NT-Domäne anlegen. Hierzu muss man in `smb.conf` drei zentrale Parameter einstellen:

```
security = domain
password server = pdc, bdc
workgroup = nt-domain-name
```

Der Eintrag `security` erhält den Wert `domain` und der Eintrag `password-server` die Namen des Primären NT-Domänencontrollers (*PDC*) und, falls im Netzwerk vorhanden, den/die Namen eines oder mehrerer Backup-Domänencontroller (*BDCs*). Man kann den Eintrag `password-server` auch weglassen. In diesem Fall nimmt Samba die Standardeinstellung `password-server = *` und sucht selbst den zuständigen Server. Der in der SuSE-Distribution auf `TUX-NET` voreingestellte Eintrag `workgroup` muss den Namen der Windows NT-Domäne erhalten. In dieser Variante nimmt der Samba-Server an den Vertrauensbeziehungen in-

nerhalb des Windows NT-Netzwerkes so teil, als ob er ein NT-Server wäre. Der Samba-Server authentifiziert hierbei nicht mehr selbst, sondern delegiert dies an den Windows NT-Domänen-Controller. Abschnitt 9.9 beschreibt die hierzu auf dem Domänen-Controller und auf dem Linux-Server erforderlichen Vorbereitungen.

Die letzte Variante `security = ads` ermöglicht es, die Benutzer über das Kerberos-Protokoll zu authentifizieren. Diese hier nicht besprochene Variante setzt ein installiertes und konfiguriertes Kerberos-System voraus.

Wählen Sie in der Praxis das Sicherheitsmodell, das den Sicherheitsanforderungen des bereits bestehenden oder von Ihnen einzurichtenden Netzwerks am besten entspricht. Weitere Informationen, die Ihnen bei der Entscheidung helfen, finden Sie in den folgenden Abschnitten.

9.3 Passwort-Verschlüsselung

9.3.1 Anmeldeprobleme

Die ersten Windows-Versionen haben die Anmeldedaten unverschlüsselt im Netz übertragen. Erst mit den späteren Versionen kam die Möglichkeit der Verschlüsselung hinzu. Aus Kompatibilitätsgründen bieten daher Samba und auch die Server-Versionen von Windows beide Möglichkeiten an.

Will man auf den Linux-Rechner in der Netzwerkumgebung mit einem

- Windows 98–Rechner oder
- einem Rechner mit einer neueren Windows 95-Version oder
- einem Windows NT-Rechner ab Servicepack 3 oder aber
- einem Windows 2000- bzw. Windows XP-Rechner

zugreifen, so fragt der Windows-Rechner nach einem Passwort.

Hierbei kann es geschehen, dass der Anmeldedialog auf dem Windows-PC das angegebene Passwort ablehnt, da diese Windows-Versionen voreingestellt verschlüsselte Passwörter verwenden, der Samba-Server die Passwörter aber eventuell im Klartext erwartet.

Auf eins von beiden muss man sich daher einigen:

Entweder schaltet man auf den Clients das Verschlüsseln der Passwörter aus oder auf allen Servern ein. Wofür Sie sich entscheiden, sollten Sie von Ihrem Sicherheitsbedürfnis abhängig machen. Beachten Sie, dass unverschlüsselt übertragene Passwörter abgehört werden können. Wenn Sie einen Samba-Server in eine Windows NT-Domäne integrieren, sollten Sie verschlüsselte Passwörter verwenden, da dies die Voreinstellung des Domänen-Controllers ist.

9.3.2 Passwortverschlüsselung am Client ausschalten

Um das Verschlüsseln von Passwörtern auf der Client-Seite auszuschalten, gibt es mehrere Möglichkeiten:

- Entweder kann man die Datei `/usr/doc/packages/samba/<Betriebssystem>_Plain Password.reg` auf dem Umweg über eine Diskette vom Linux-Server auf den Windows-PC kopieren. Diese Datei führt man anschließend durch Anklicken auf dem Windows-PC aus. Nach einem Reboot sendet Windows Passwörter im Klartext.
- Auf einem Windows 98-Rechner installiert man von der Windows 98-CD die Datei `\tools\mtsutil\ptxt_on.inf`. Rechtsklicken Sie dazu im Explorer auf die Datei, und wählen Sie dann *Installieren*. Nach einem Windows-Neustart sollten Sie Ihr Ziel erreichen.
- Bei Windows 2000/XP-Rechnern kann man in der Systemsteuerung unter *Verwaltung* den Eintrag *lokale Sicherheitsrichtlinie •Llokale Richtlinien • Sicherheitsoptionen • Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden* aktivieren und dann den Windows-PCs neu starten.

9.3.3 Passwortverschlüsselung am Linux-Server einschalten

Auf dem Linux-Server kann man stattdessen das Verschlüsseln von Passwörtern durch den folgenden Eintrag in der `/etc/samba/smb.conf` einschalten:

```
encrypt passwords = yes
```

Die Autoren empfehlen dieses Vorgehen, da Rechner mit Windows 2000 und Windows XP Professional nur mit dieser Einstellung eine Domänenanmeldung an einem Samba-Server vornehmen können.

9.4 Samba-Passwörter

Um auf dem Linux-Server, der nicht an der Sicherheitsüberprüfung einer Windows-NT Domäne teilnimmt, verschlüsselte Passwörter zu aktivieren, muss man zusätzlich zur System-Passwort-Datei des Linux-Systems eine eigene Samba-Passwortdatei `/etc/samba/smbpasswd` führen. Mit dem Befehl `smbpasswd -a <loginname>` (Beispiel: `smbpasswd -a uwe`) fügt man einen neuen Benutzer in diese Datei ein und legt sein Passwort für das Samba-System fest. Dieser Benutzer muss bereits als Unix-Benutzer vorhanden sein.

In die `/etc/samba/smb.conf` muss man hierfür im Abschnitt `[global]` einfügen:

```
encrypt passwords = Yes
```

Passwortdateien synchronisieren

Wenn nun ein Benutzer sein Passwort ändert, dann muss sicher gestellt sein, dass diese Änderung sowohl in der Samba-Passwortdatei als auch der System-Passwortdatei erfolgt, die Passwort-Dateien also synchron bleiben. Bei SuSE 9.2 erreichen Sie eine automatische Synchronisierung mit folgenden Zeilen in der Datei `/etc/samba/smb.conf`:

```
passwd program = /usr/bin/passwd %u
pam password change = yes
unix password sync = Yes
```

9.5 Samba-Server konfigurieren

Den Samba-Server konfigurieren Sie komplett über die Datei `/etc/samba/smb.conf`.

Sie können diese Datei entweder direkt auf dem Linux-Server mit einem Editor oder von einem beliebigen PC im Netzwerk mit dem Programm `swat` (*samba web administration tool*) bearbeiten.

9.5.1 Editor oder swat

`swat` ist Bestandteil des Samba-Paketes und damit inzwischen auf Ihrem Server installiert. Bevor Sie im Netzt mit `swat` arbeiten können, müssen Sie den Dienst `swat` mit YaST unter *Netzwerkdienste* • *Netzwerkdienste (inetd)* freischalten. Dazu müssen Sie in der Datei `/etc/xinetd.d/samba` den Eintrag

```
only_from       = 127.0.0.1
```

mit dem Zeichen # auskommentieren.

```
# only_from       = 127.0.0.1
```

Der Befehl

```
rcxinetd  restart
```

sorgt dafür, dass die Änderung wirksam wird.

Das anfängerfreundliche `swat` startet man dann über einen beliebigen Browser. Geben Sie in der Adressleiste eines Web-Browsers auf einem Windows- oder Linux-PC ein:

```
http://<IP-Adresse des Linux-Servers>:901/
```

(Beispiel: `http://192.168.1.2:901/`). Im Anmeldefenster sollte man sich als `root` anmelden, denn dann kann man vom Browser aus Änderungen vornehmen, ohne die Konfigurationsdatei direkt bearbeiten zu müssen.

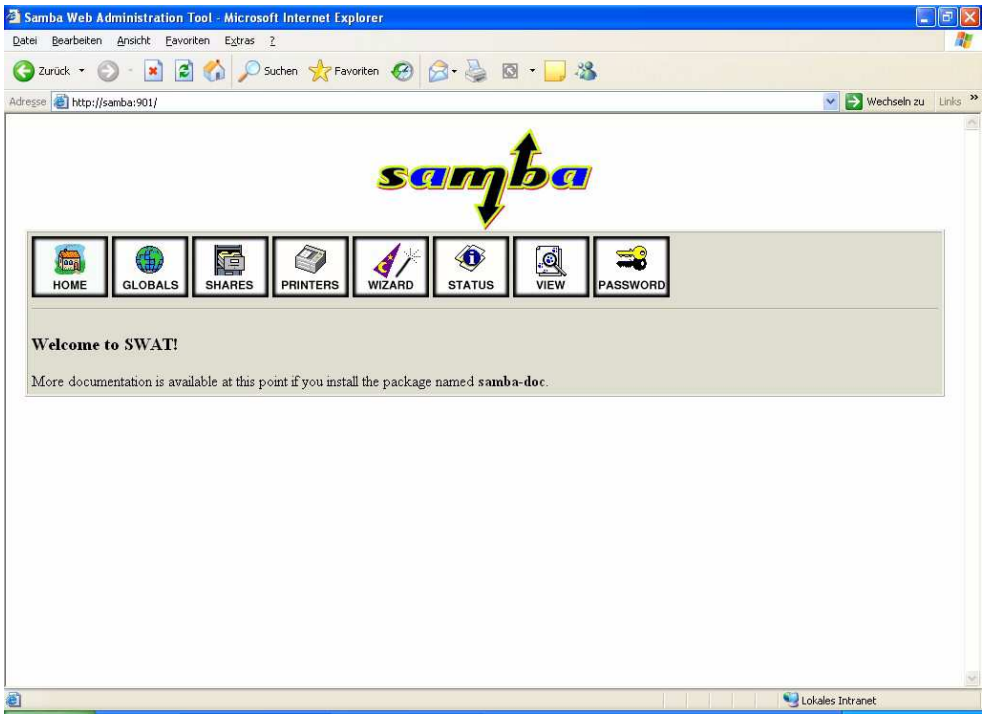

Abbildung 9.3: Startbildschirm von swat im Fenster eines Browsers

9.5.2 SuSE-Konfigurationsdatei

Die von SuSE mitgelieferte `/etc/samba/smb.conf` ist wenig kommentiert, dafür aber recht übersichtlich. Eine ausführlicher kommentierte Version der Datei finden Sie unter `/usr/share/doc/packages/samba/examples/smb.conf.SuSE`, wenn Sie das Paket samba-doc installiert haben.

Die folgenden Abschnitte erklären dann die wichtigsten Parameter der Konfigurationsdatei `/etc/samba/smb.conf`.

Der Parameter

```
include=/etc/samba/dhcp.conf
```

ist überflüssig und sollte auskommentiert oder gelöscht werden.

9.6 Freigaben

```
# smb.conf is the main Samba configuration file. You find a full
# commented version at /usr/share/doc/packages/samba/examples/
# smb.conf.SUSE if the samba-doc package is installed.
# Date: 2004-12-17
[global]
   workgroup = ARBEITSGRUPPE
   printing = cups
   printcap name = cups
   printcap cache time = 750
   cups options = raw
   printer admin = @ntadmin, root, administrator
   username map = /etc/samba/smbusers
   map to guest = Bad User
   include = /etc/samba/dhcp.conf
   logon path = \\%L\profiles\.msprofile
   logon home = \\%L\%U\.9xprofile
   logon drive = P:
[homes]
   comment = Home Directories
   valid users = %S
   browseable = No
   read only = No
   inherit acls = Yes
[profiles]
   comment = Network Profiles Service
   path = %H
   read only = No
   store dos attributes = Yes
   create mask = 0600
   directory mask = 0700
[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
```

```
   printable = Yes
   create mask = 0600
   browseable = No
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/drivers
   write list = @ntadmin root
   force group = ntadmin
   create mask = 0664
   directory mask = 0775
```

Damit alle Benutzer oder Benutzergruppen Verzeichnisse des Linux-Servers über Samba nutzen können, muss man diese gezielt freigeben.

Dies bewirken in der Konfigurationsdatei von SuSE die Einträge `[homes]` bzw. `[printers]`. Der Abschnitt 9.7 (*Drucken von Windows-Clients*) erklärt die Freigabe `printers`. Die Freigabe `homes` gibt das Home-Verzeichnis jedes Benutzers für diesen Benutzer frei. In der von SuSE mitgelieferten Konfigurationsdatei befinden sich zwei weitere Freigaben. Die Freigabe `users` zeigt alle (Home-)Verzeichnisse unterhalb des Pfades `/home` an, die Freigabe `groups` soll dazu dienen, unterhalb von `/home/groups` Verzeichnisse zur Verfügung zu stellen. Dazu muss aber zunächst das Verzeichnis `/home/groups` erstellt werden.

Lesen Sie hier zuerst grundsätzliche Arbeitsschritte, um Freigaben einzurichten und danach Details über Freigaben für alle Benutzer und für einzelne Gruppen.

9.6.1 Grundsätzliches

Um eine neue Freigabe einzurichten, klicken Sie in swat auf *SHARES*. Geben Sie in das Feld hinter dem Button *Create Share* `pub` ein.

Ein Klick auf den Button *Create Share* fügt Folgendes an die Datei `smb.conf` an:

```
[pub]
```

Sobald Sie in swat auf den Button *Commit Changes* drücken, steht in der Konfigurationsdatei:

```
[pub]
          path = /tmp
```

Dies ist ein Beispiel für eine sehr einfache Netzfreigabe. In der Netzwerkumgebung ist sie jetzt sichtbar.

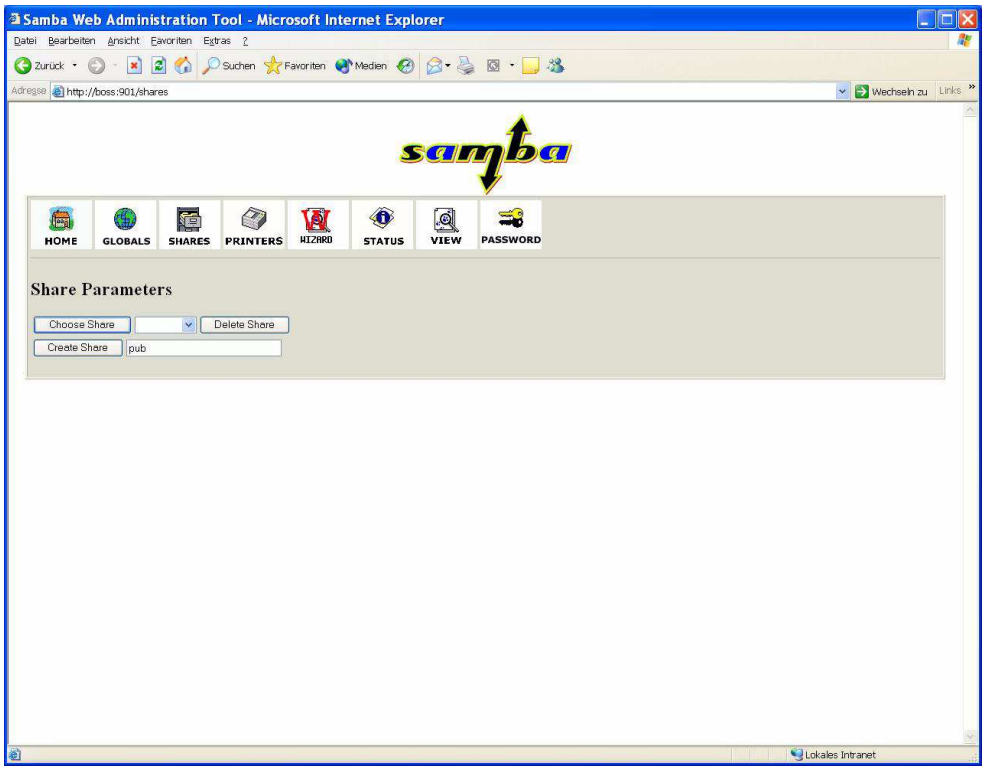

Abbildung 9.4: Dialog in swat

9.6.2 Freigaben für Alle

Auf einem Linux-System können Sie eine Freigabe für ein Verzeichnis so einzustellen, dass dort jeder Benutzer lesen, schreiben, verändern und löschen darf. Dies sollte man nur vornehmen, wenn ein solches Verzeichnis auf einer eigenen Partition der Festplatte liegt, damit Benutzer dem System nicht durch zu große Datenmengen in diesem Verzeichnis die gesamte Festplattenkapazität wegnehmen können.

Um so eine Freigabe einzurichten, erzeugen Sie zunächst am Linux-Prompt das Verzeichnis, auf das die Benutzer über das Netz zugreifen dürfen.

```
mkdir /tmp/fuer_alle
```

Ändern Sie dann die Rechte für dieses Verzeichnis so, dass alle Benutzer in das Verzeichnis wechseln dürfen (`x`), eine Datei anlegen dürfen (`w`) und das Inhaltsverzeichnis lesen dürfen (`r`):

```
chmod a+rwx /tmp/fuer_alle
```

Wählen Sie in swat unter *SHARES* noch einmal die Freigabe `pub`, klicken Sie auf *Advanced View,* und ändern Sie die Variablen so, dass der Abschnitt `pub` in der Datei `smb.conf` wie folgt aussieht:

```
[pub]
          path = /tmp/fuer_alle
          read only = No
          create mask = 0666
          force create mode = 0666
          directory mask = 0777
          force directory mode = 0777
```

9.6.3 Linux- und Samba-Rechte

`path` gibt den Pfad zum freigegebenen Verzeichnis an. Mit `read only = no` dürfen Benutzer auch über den Samba-Server in das Verzeichnis schreiben.

Es gibt dabei immer zwei Arten von Rechten:

- Die Rechte, die der Samba-Server erlaubt und
- die Rechte des Linux-Dateisystems.

Um schreiben zu können, müssen Benutzer auch die Schreibrechte des Linux-Dateisystems besitzen, wenn der Samba-Server das Schreiben erlaubt.

Mit den Parametern `create mask = 0666` und `force create mode = 0666` erreicht man, dass alle Benutzer alle Dateien lesen und ändern können. In der Oktalschreibweise der Dateirechte setzt sich jeder Wert zusammen aus `4` (lesen) + `2` (schreiben) + `1` (ausführen). Die erste `6` gilt für den Besitzer der Datei, die zweite `6` für die Mitglieder der Gruppe und die dritte `6` für alle anderen Benutzer. Für Verzeichnisse erreicht man mit den Parametern

```
directory mask = 0777
```

und

```
force directory mode = 0777
```

dasselbe Ziel. Für Dateien, die auf dem Linux-Server gespeichert werden, ist es nicht notwendig, dass man sie auch unter Linux ausführen kann. Bei Verzeichnissen setzen sich die Werte für die Dateirechte zusammen aus `4` (Dateien aus dem Verzeichnis lesen), `2` (Dateien im Verzeichnis ändern oder neu anlegen) und `1` (in das Verzeichnis wechseln).

9.6.4 Freigabe für Benutzergruppen

Während Sie im letzten Abschnitt lesen konnten, wie man Verzeichnisse für alle Benutzer freigibt, soll hier eine Freigabe nur bestimmten Benutzern Schreibrechte geben. Das Beispiel benutzt die Gruppe `einkauf`, die Sie auf Ihrem Server eingerichtet haben müssen, wenn Sie das Beispiel so nachvollziehen wollen.

```
[einkauf]
          path = /home/einkauf
          write list = @einkauf
          force group = einkauf
          create mask = 0774
          force create mode = 0774
          directory mask = 0775
          force directory mode = 0775
```

Der Eintrag `write list = @einkauf` erreicht, dass nur die Mitglieder der Gruppe `einkauf` Schreibrecht in dieser Freigabe haben. Der Eintrag `force group = einkauf` ordnet neu angelegte Dateien nicht der primären Gruppe des Benutzers, sondern der Gruppe `einkauf` zu.

Um eine Freigabe `buchhalt` zu erzeugen, auf die nur Benutzer der Gruppe `buchhalt` zugreifen, gehen Sie so vor:

```
[buchhalt]
          path = /home/buchhaltung
          valid users = @buchhalt
          force group = buchhalt
          read only = No
          create mask = 0774
          force create mode = 0774
          directory mask = 0775
          force directory mode = 0775
          browseable = No
```

Nur Mitglieder der Gruppe `buchhalt` (`valid users = @buchhalt`) können auf die Freigabe zugreifen. Für sie ist die Freigabe nicht schreibgeschützt (`read only = No`). Die Freigabe ist nicht in der Netzwerkumgebung sichtbar (`browseable = No`).

9.7 Drucken von Windows-Clients

Trotz Web und schönster Arbeitsumgebungen steigt der Papierverbrauch im EDV-Bereich stetig. Damit Anwender über Druckdienste eines Linux-Servers drucken können, kann man Samba als Drucker-Server einrichten.

Dieser Abschnitt zeigt das Verwenden der Druckdienste von Samba.

9.7.1 Samba-Drucker

Die von SuSE als Beispiel gelieferte Konfigurationsdatei enthält im Abschnitt `[global]` die Zeilen:

```
   printing = cups
   printcap name = cups
```

Die Einträge bedeuten: Samba verwendet das `cups`-Drucker-Spool-System, und der Linux-Server stellt den Clients alle Drucker, die dort definiert sind, zur Verfügung und zeigt sie in der Netzwerkumgebung im Abschnitt `[printers]` an.

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

Der Eintrag `printable = Yes` sagt dem Linux-System, dass es sich hier um eine Druckerfreigabe handelt. Dieser Eintrag erlaubt Anwendern dieser Freigabe, ihre Druckdateien in der Druckerwarteschlange abzulegen, die das Linux-System dann an den Drucker weiterleitet.

9.7.2 Vorarbeiten auf dem Linux-Server

Um überhaupt über den Linux-Server drucken zu können, müssen Sie zunächst unter Linux mit YaST Ihren Drucker anlegen. Den Eintrag für die Druckerkonfiguration finden Sie im Punkt *Hardware* von YaST. Anschließend müssen Sie den smbd-Server mit `rcsmb restart` neu starten, damit er die geänderte Druckerkonfiguration einliest.

9.7.3 Windows-Druckertreiber einrichten

Um von den Windows-Clients auf einem Drucker, der am Linux-Server angeschlossen ist, drucken zu können, müssen Sie

- auf jedem Windows 9x-Rechner den Windows-Druckertreiber des freigegebenen Druckers installieren und den Drucker mit dem Linux-Rechner verbinden (z. B. `\\<servername>\lp`) und
- bei den Betriebssystemen Windows NT/2000/XP in der Netzwerkumgebung mit einem Doppelklick auf die *Druckerfreigabe* klicken, um die Druckertreiber zu installieren. Lassen Sie sich hierbei nicht von der Ausgabe `Zugriff verweigert` des Windows- Rechners irritieren.

  `<servername>` ist dabei der Name des Linux-Rechners.

Abbildung 9.5: Windows-Druckertreiber mit dem Linux-Drucker verbinden

9.8 Domain-Logons

Die für die tägliche Arbeit wichtigsten Funktionen von NT-Domainen-Controllern kann man Linux-Servern überlassen. So kann man im Netzwerk völlig auf Windows NT-Server verzichten. Dies ist auch deswegen ratsam, weil Microsoft angekündigt hat, den Support für Windows NT einzustellen.

Das folgende Beispiel einer Konfigurationsdatei bewirkt, dass sich Windows-Rechner am Linux-Server wie an einer Windows NT-Domäne anmelden können. Der Linux-Rechner verhält sich dann wie ein NT-Domänen-Controller; stellt allerdings nicht die volle Funktionalität eines Windows 2000-Servers bereit. Speziell das unter Windows 2000 vorhandene Active Directory steht bisher nicht zur Verfügung.

Abbildung 9.6: Domain-Logons

Die in den vorigen Abschnitten erstellten Freigaben sind hier ebenfalls vorhanden. Wenn sich ein Windows95/98-PC an einer Domäne anmelden soll, muss man dort in *Eigenschaften des Client für Microsoft Netzwerke* die Eigenschaften der Netzwerkumgebung einstellen.

Um einem Linux-Server die Aufgabe eine NT-Domänen-Controllers zu übertragen, muss man die Samba-Konfigurationsdatei bearbeiten. Diese ist nach diesem Absatz abgedruckt und in den darauf folgenden Abschnitten erläutert.

Die Samba-Konfigurationsdatei

```
[global]
  workgroup = ARBEITSGRUPPE
  server string = %L
  os level = 65

   username map   = /etc/samba/smbusers
  username level = 5
  min passwd length = 3

  log level = 1
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 10000

  time server = Yes

  interfaces = 127.0.0.1  eth0
```

```
   bind interfaces only = true

   printing = cups
   printcap name = cups
   cups options = raw
   printer admin = @ntadmin, root, administrator

   wins support = Yes

# default: passdb backend = smbpasswd
#  passdb backend = ldapsam:ldap://localhost
#  passdb backend = ldapsam:ldaps://localhost
#  passdb backend = smbpasswd
#  passdb backend = tdbsam
#  passdb backend = plugin:/path/to/plugin.so:pluging args
# needed for one the nua-backends

   local master = Yes
   domain master = Yes
   domain logons = Yes
   preferred master = Yes
   security = user
   encrypt passwords = Yes

   logon script = scripts\default.bat

   logon path = \\%L\profiles\.msprofile
   logon drive = z:
   logon home = \\%L\%U\.9xprofile

    add machine script = /usr/sbin/useradd -G "" ↵
      -d /home/machine -s /bin/false %u
    add user script = /usr/sbin/useradd -m %u
    add group script = /usr/sbin/groupadd  "%g"
add user to group script = /usr/sbin/groupmod -A "%u" "%g"
delete user from group script = /usr/sbin/groupmod -R "%u" "%g"

   set primary group script = /usr/sbin/usermod -g "%g" "%u"

   unix password sync = True
   passwd program = /usr/bin/passwd %u
   pam password change = True

   deadtime = 15
   profile acls = Yes

[homes]
   comment = Home Directories
```

```
   valid users = %S
   browseable= No
   read only = No
   inherit permissions = Yes
   guest ok = No
   wide links = no


[users]
   comment = All users
   path = /home
   writeable = No
   inherit permissions = Yes
   veto files = /aquota.user/groups/shares/

[groups]
   comment = All groups
   path = /home/groups
   writeable = Yes
   inherit permissions = Yes

[pdf]
   comment = PDF creator
   path = /var/tmp
   printable = Yes
   print command = /usr/bin/smbprngenpdf -J '%J' -c %c -s %s
   ↵ -u '%u' -z %z
   create mask = 0600



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

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

[netlogon]
      path = /home/netlogon
```

```
      read only = yes
      write list = @ntadmin root
      force group = ntadmin
   create mask = 0664
      directory mask = 0775

[profiles]
   path = %H
   read only = no
   inherit permissions = Yes
   store dos attributes = Yes
   create mask = 0600
   directory mask = 0700

  [pub]
          path = /tmp/fuer_alle
          read only = No
          create mask = 0777
          force create mode = 0777
          directory mask = 0777
          force directory mode = 0777
  [einkauf]
          path = /home/einkauf
          write list = @einkauf
          force group = einkauf
          create mask = 0774
          force create mode = 0774
          directory mask = 0775
          force directory mode = 0775

  [buchhalt]
          path = /home/buchhaltung
          valid users = @buchhalt
          force group = buchhalt
          read only = No
          create mask = 0774
          force create mode = 0774
          directory mask = 0775
          force directory mode = 0775
          browseable = No
```

Achten Sie darauf, in dem Namen der Domäne (in unserem Beispiel `ARBEITS-GRUPPE`) nur alphanumerische Zeichen zu verwenden, da Windows-Rechner sonst Probleme bereiten.

Die Freigabe `netlogon` muss zwingend vorhanden sein.

Wenn die Clients sich per Domain-Logon anmelden, kann man nach der Anmeldung auf dem Client eine Batch-Datei ausführen lassen, die Einstellungen auf dem Client-Rechner vornimmt. Die folgende Zeile der Datei `/etc/smb.conf` legt die Lage und den Namen eines solchen Anmeldeskripts fest:

```
logon script = scripts\default.bat
```

Die obige Pfadangabe muss relativ zur `netlogon`-Freigabe sein. Der Pfad zur Freigabe `netlogon` ist hier im Beispiel:

```
/home/netlogon
```

Der Pfad zum Anmeldeskript lautet dann:

```
/home/netlogon/scripts/default.bat
```

Da sich bei Textdateien unter Windows und Linux die Zeilenschaltungen unterscheiden (siehe Abschnitt 7.2), sollte man die Anmeldedatei auf dem Windows-PC mit einem ASCII-Editor wie *Notepad* bearbeiten und anschließend in das richtige Verzeichnis auf dem Linux-Server (im Beispiel: `/home/netlogon/scripts`) kopieren. Die Anmeldedatei ordnet zum Beispiel den Freigaben Laufwerksbuchstaben zu.

Hier kommt ein kurzes Beispiel für ein solches Logon-Skript:

```
Net use u: \\boss\homes
Net use w: \\boss\buchhalt
```

Der Linux-Server heißt in diesem Beispiel *boss*. Hilfen zum Net-Befehl erhalten Sie, wenn Sie an der Eingabeaufforderung eines Windows-PCs `net /?` eingeben.

Damit der Linux-Server die Änderungen berücksichtigt, müssen Sie die Samba-Server neu starten.

Die verschiedenen Abarten der Windows-Familie erfordern unterschiedliche Einträge:

Für Windows NT/2000/XP bestimmt die Zeile

```
logon path = \\%L\profiles\.msprofile
```

den Speicherort für die Profildaten (`USER.DAT`, Eigene Dateien, etc.) eines Benutzers. Der Parameter `%L` steht dabei für den `netbios`-Namen des Rechners und `%U` für den Anmeldenamen des Benutzers. Bei Windows 9x ist für denselben Zweck die Zeile

```
logon home = \\%L\%U\.9xprofile
```

zuständig ist.

Hier im Beispiel liegen die Profile in einem Unterverzeichnis des Home-Verzeichnisses auf dem Linux-Server. Die Freigabe `profiles` ist wie folgt definiert:

```
[profiles]
   path = %H
   read only = no
   inherit permissions = Yes
   store dos attributes = Yes
   create mask = 0600
   directory mask = 0700
```

Der Parameter `username map` gibt den Pfad zu einer Datei an, die Linux-Benutzer auf Windows-Benutzer abbilden kann.

```
username map = /etc/samba/smbusers
```

In der Datei `/etc/samba/smbusers` steht in unserer Redaktion:

```
root = administrator
```

Dies bedeutet: Der Windows-Benutzer `administrator` ist auf den Linux-Benutzer `root` abgebildet. Den Benutzer `administrator` sollte es daher auf dem Linux-Rechner nicht geben. Wenn sich jemand als `administrator` am Windows-Rechner anmeldet und sich mit dem Linux-Server verbindet, so erfolgt das als (Linux-)Benutzer `root`. Zuvor müssen Sie den Benutzer `root` mit dem Befehl `smbpasswd -a root` in die Samba-Benutzerdatenbank aufnehmen.

Damit sich auch Windows NT-Rechner am Linux-Server wie an einem NT-Domänen-Controller anmelden können, muss Samba verschlüsselte Passwörter akzeptieren.

Jeder Windows NT/2000/XP-Rechner, der sich am Samba-Server anmelden können soll, muss als Systembenutzer und als Samba-Benutzer (sog. *Maschinen-Account*) vorhanden sein. Diese legt Samba durch den Eintrag

```
add machine script = /usr/sbin/useradd -G ""
  ↵ -d /home/machine -s /bin/false %u
```

automatisch an. Der obige Eintrag ist eine Zeile in der `/etc/samba/smb.conf`.

Mit dem Befehl

```
mkdir /home/machine
```

legen Sie das dafür notwendige Home-Verzeichnis an.

Falls Sie einen Rechner per Hand in die Domäne aufnehmen wollen, sind dazu auf dem Linux-Server die Befehle des folgenden Listings notwendig. Im Beispiel heißt der NT-Rechner `HHS01`, das $-Zeichen am Ende des Rechnernamens zeigt Samba den Maschinen-Account an.

```
useradd -G "" -d /home/machine -s /bin/false hhs01$
smbpasswd -a -m hhs01$
```

Damit sich auch Benutzer an Windows 2000/XP-Rechnern per Domain-Logon am Samba-Server anmelden können, müssen Sie auch den Benutzer `root` in die Passwortdatenbank von Samba aufnehmen:

```
smbpasswd -a root
```

Außerdem sollten die primären Unix-Gruppen aller Benutzer, die sich an dem Samba-Server anmelden, zu Domain-Gruppen gemappt werden. Der Befehl `net groupmap list` zeigt die vorhandenen Gruppen und ihre Zuordnungen an:

```
System Operators (S-1-5-32-549) -> -1
Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Users (S-1-5-21-2351660384-2028355313-418873532-513) -> -1
Domain Admins (S-1-5-21-2351660384-2028355313-418873532-512) -> -1
Domain Guests (S-1-5-21-2351660384-2028355313-418873532-514) -> -1
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Account Operators (S-1-5-32-548) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
```

Mit den folgenden Befehlen ordnet man die NT-Gruppe `Domain Users` der Unix-Gruppe `users` und die NT-Gruppe `Domain Admins` der Unix-Gruppe `ntadmin` zu.

```
net groupmap modify ntgroup="Domain Users" unixgroup=users
net groupmap modify ntgroup="Domain Admins" unixgroup=ntadmin
```

Mit dem Befehl

```
net groupmap add unixgroup=root
```

erzeugt man die NT-Gruppe `root`.

Der Befehl `net groupmap list` gibt Folgendes aus:

```
System Operators (S-1-5-32-549) -> -1
root (S-1-5-21-2351660384-2028355313-418873532-1001) -> root
Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Users (S-1-5-21-2351660384-2028355313-418873532-513)
  ↵ -> users
Domain Admins (S-1-5-21-2351660384-2028355313-418873532-512)
  ↵ -> ntadmin
```

```
Domain Guests (S-1-5-21-2351660384-2028355313-418873532-514)
  ↵ -> -1
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Account Operators (S-1-5-32-548) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
```

Falls Sie PCs mit Windows XP Professional (oder Windows 2000 Professional) einsetzen, verfolgen Sie bitte die weiteren Schritte zum Einfügen dieser PCs in die Domain:

1. Öffnen Sie im Startmenü oder auf dem Desktop das Kontextmenü von *Arbeitsplatz*, und wählen Sie den Menüpunkt *Eigenschaften*, wie in einem der nächsten beiden Bildern gezeigt.

Abbildung 9.7: *Eigenschaften* von Arbeitsplatz

Abbildung 9.8: *Eigenschaften* von Arbeitsplatz (*klassisch*)

2. Um den Windows XP-PC der Samba-Domain hinzuzufügen, wählen Sie in den *Systemeigenschaften* die Registerkarte *Computername* und klicken auf die Schaltfläche *Ändern*.

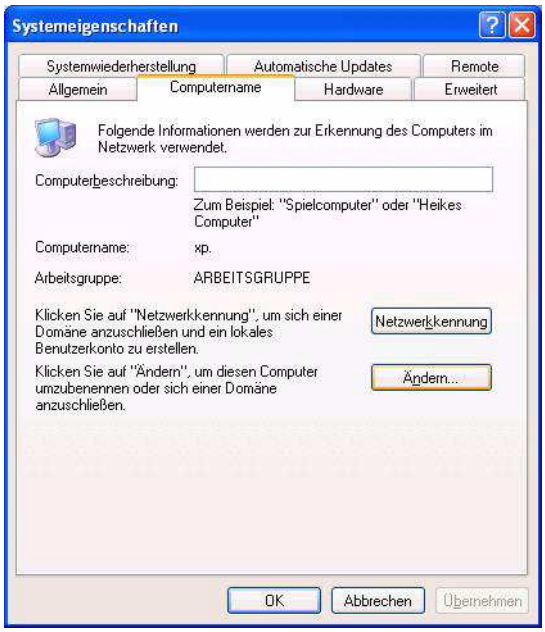

Abbildung 9.9: Computername

3. Im Dialog *Computername ändern* klicken Sie an, dass der Computer Mitglied einer *Domäne* ist, und tragen den Namen der Domäne ein.

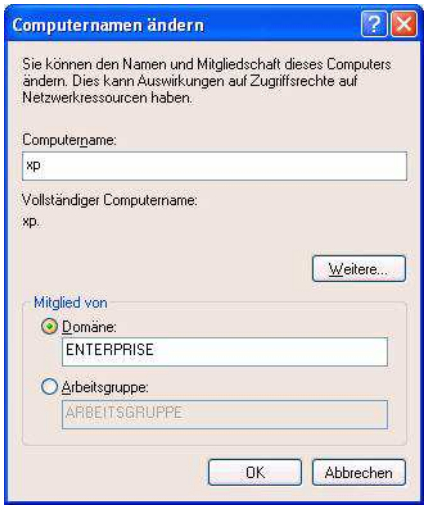

Abbildung 9.10: Domäne

4. Nach einem Klick auf *OK* müssen Sie in einem Dialogfeld einen Domänenbenutzer auswählen, der die Domänenmitglieder verwaltet, und dessen Kennwort eintragen:

Abbildung 9.11: Konto mit der Berechtigung, der Domäne beizutreten

Geben Sie dort als Benutzer `root` sowie das (Samba-) Passwort von `root` ein. Nach einiger Zeit begrüßt Sie dann die Domäne wie im folgenden Bild:

Abbildung 9.12: Willkommen in der Domäne!

Bitte überprüfen Sie vor diesen Schritten nochmals die gesamte `[global]`-Sektion der Datei `/etc/samba/smb.conf`:

```
[global]
   workgroup = ARBEITSGRUPPE
   server string = %L
   os level = 65

    username map   = /etc/samba/smbusers
   username level = 5
   min passwd length = 3

   log level = 1
         syslog = 0
         log file = /var/log/samba/log.%m
         max log size = 10000
```

```
   time server = Yes

   interfaces = 127.0.0.1  eth0
    bind interfaces only = true

   printing = cups
   printcap name = cups
   cups options = raw
   printer admin = @ntadmin, root, administrator

   wins support = Yes

# default: passdb backend = smbpasswd
#  passdb backend = ldapsam:ldap://localhost
#  passdb backend = ldapsam:ldaps://localhost
#  passdb backend = smbpasswd
#  passdb backend = tdbsam
#  passdb backend = plugin:/path/to/plugin.so:pluging args
# needed for one the nua-backends

   local master = Yes
   domain master = Yes
   domain logons = Yes
   preferred master = Yes
   security = user
   encrypt passwords = Yes

   logon script = scripts\default.bat

   logon path = \\%L\profiles\.msprofile
   logon drive = z:
   logon home = \\%L\%U\.9xprofile

    add machine script = /usr/sbin/useradd -G "" ↵
      -d /home/machine -s /bin/false %u
    add user script = /usr/sbin/useradd -m %u
   add group script = /usr/sbin/groupadd  "%g"
add user to group script = /usr/sbin/groupmod -A "%u" "%g"
delete user from group script = /usr/sbin/groupmod -R "%u" "%g"

   set primary group script = /usr/sbin/usermod -g "%g" "%u"

   unix password sync = True
   passwd program = /usr/bin/passwd %u
   pam password change = True

   deadtime = 15
   profile acls = Yes
```

9.9 Samba-Server als Mitglied einer Windows NT/2000-Domäne

In manchen Netzen sind immer noch Windows-Server als zentrale Anmelde-Server vorhanden. Auch in ein solches Umfeld können Sie Ihren Linux-Server einbinden.

1. Als Erstes sollten Sie das Paket `samba-winbind` installieren. Nun stoppen Sie Samba und sorgen dafür, dass auch der Dienst `winbind` beim nächsten Boot startet:

```
rcnmb stop
rcnmbrcsmb stop
insserv winbind
```

2. Danach starten Sie YaST und wählen *Netzwerkdienste* • *Samba-Client*.

Abbildung 9.13: YaST: *Netzwerkdienste*

3. Im nachfolgen Dialog geben Sie den Namen der Arbeitsgruppe an und setzen das Kreuz bei *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden*.

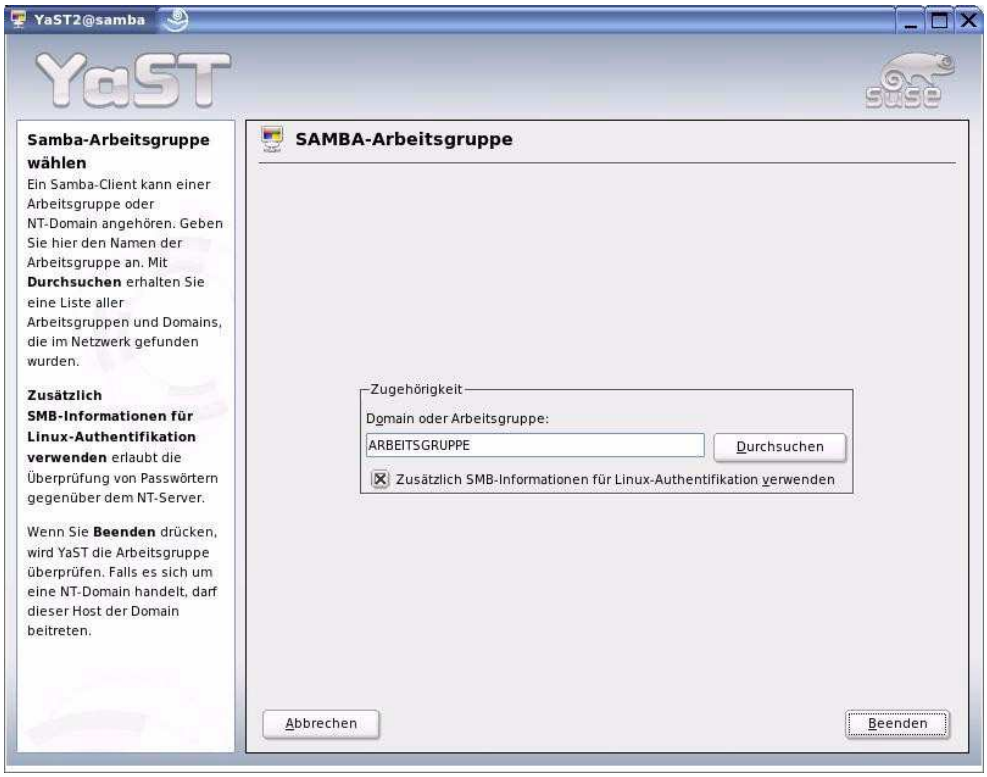

Abbildung 9.14: Samba- Arbeitsgruppe.

Beantworten Sie die Frage nach dem Domänen-Beitritt mit *Ja*, und geben Sie im nachfolgenden Dialog das Administrator-Passwort ein.

Abbildung 9.15: Der Domäne beitreten?

Geben Sie im nachfolgenden Dialog das Administrator-Passwort ein.

Abbildung 9.16: Administrator-Passwort eingeben

Rebooten Sie den Linux-Server, nachdem die Erfolgsmeldung erschienen ist.

Abbildung 9.17: In die Domäne aufgenommen!

Rebooten Sie nun den Linux-Server.

Hier ist zum Vergleich der Abschnitt `[global]` der Datei `/etc/samba/smb.conf`:

```
[global]
   workgroup = ARBEITSGRUPPE
   printing = cups
   printcap name = cups
   printcap cache time = 750
   cups options = raw
   printer admin = @ntadmin, root, administrator
   username map = /etc/samba/smbusers
   map to guest = Bad User
   logon path = \\%L\profiles\.msprofile
   logon home = \\%L\%U\.9xprofile
   logon drive = P:
   security = domain
   encrypt passwords = yes
   idmap uid = 10000-20000
   idmap gid = 10000-20000
```

9.10 Weitere Informationsquellen

Weitere Informationen zu diesem komplexen Thema finden Sie z. B. in

- der Manpage von `smb.conf`,
- der Dokumentation unterhalb von `/usr/share/doc/packages/samba`
- den Web-Seiten des Samba-Projektes: `http://de.samba.org/`