3 Benutzerverwaltung

Systemadministratoren verbringen viel Zeit mit dem Verwalten der Benutzer und den entsprechenden Benutzerkonten.

Typische Arbeiten sind das

- Anlegen und Löschen von Benutzerkonten,
- Prüfen der Qualität von Passwörtern (siehe Kapitel 15),
- Ändern von Passwörtern, welche die Benutzer vergessen haben sowie
- das Überwachen des von Nutzern belegten Speicherplatzes.

Wegen ihrer Überlastung benötigen Systembetreuer in vielen Organisationen mehrere Tage, bis sie neuen Mitarbeitern vollen Systemzugang eingerichtet haben und oft noch länger, bis sie ausscheidenden Mitarbeitern alle Zugänge entzogen haben.

Viele Benutzer neigen dazu, leicht zu erratende Passwörter zu wählen. Da dies die Sicherheit des Systems gefährdet, sollten Systemverwalter die Qualität der Passwörter regelmäßig überprüfen.

Viele Anwender müssen sich mehrere Dutzend Passwörter merken. Da kann es schon passieren, dass sie sich nach einem richtig erholsamen Urlaub nicht mehr an alle erinnern.

Großzügig bemessener Speicherplatz verleitet Benutzer leicht zu einer chaotischen Datenorganisation. Wenn ein Verzeichnis unübersichtlich wird, dann legen sie einfach ein neues an, ohne das alte zu löschen, da sie ja eine der darin enthaltenen Dateien vielleicht irgendwann noch gebrauchen könnten.

Für all diese Systemarbeiten gibt es freie und kommerzielle Produkte. Sparsame Systemverwalter setzen u. a.

- das freie Tool *Webmin* ein, das Sie unter `http://www.webmin.com/webmin/` finden, oder
- eine freie Version des Lightweight Directory Access Protocol (*LDAP*).

Systemverwalter mit großem Budget und Liebe zu kommerziellen Produkten ziehen vielleicht

- die NDS für Linux von Novell (`http://www.novell.de`) oder Volution von Caldera (`http://www.caldera.com`).

vor. Viele Tools sollten nur erfahrene Systemadministratoren installieren und konfigurieren.

3.1 Überblick

Die Autoren stellen Ihnen in diesem Kapitel eine eigene Tool-Sammlung vor, die deutschsprachig, leicht konfigurierbar und über das Netz bedienbar ist. Diese Tools erfordern nur einen geringen Installationsaufwand und nehmen keine weiteren Veränderungen am System vor. Sie unterstützen das Arbeiten mit *Changed-Root-Umgebungen* (siehe Kapitel 7) und den Umgang mit *Disk-Quotas* (siehe unten). Weiterhin unterstützen die Tools das Arbeiten mit verschlüsselten Passwörtern, deren Bedeutung Sie in Kapitel 9 kennen lernen werden. Neu seit der vierten Auflage dieses Buches ist der Abschnitt 3.5.1 zur Benutzerverwaltung mit LDAP.

3.2 Benutzerverwaltung mit YaST

Die Benutzerverwaltung von Linux mit *useradd* ist nicht besonders komfortabel. Etwas einfacher haben Sie es, wenn Sie für das Anlegen von neuen Benutzern YaST benutzen.

Im YaST-Kontrollzentrum finden Sie unter *Sicherheit und Benutzer* • *Benutzer bearbeiten und anlegen* ein Menü für das Verwalten der Benutzer.

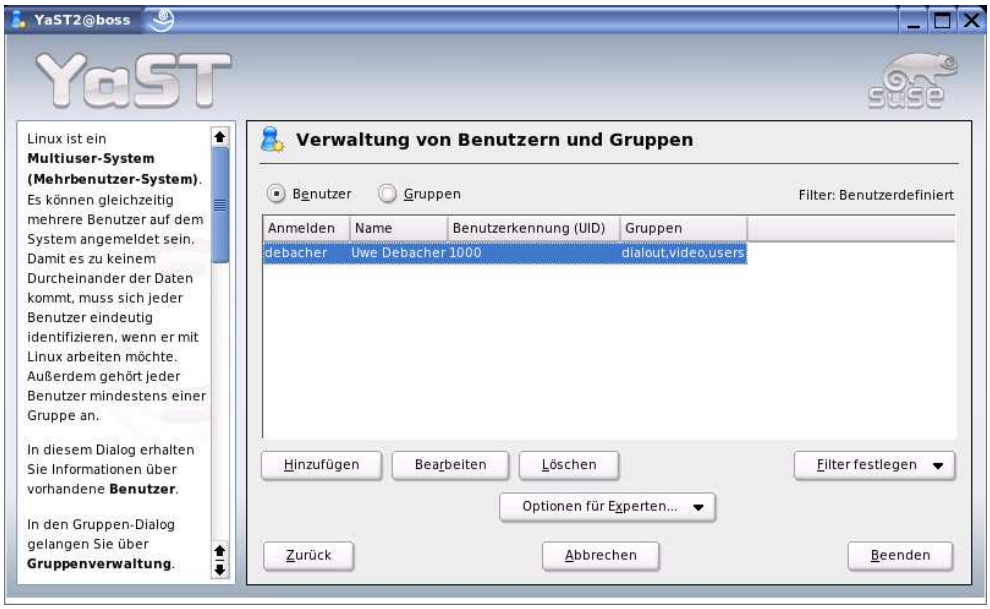

Abbildung 3.1: Benutzerverwaltung mit YaST

In der Benutzer-Liste finden Sie nur den Benutzer, den Sie bei der Grundinstallation angelegt haben. Diesen Account können Sie über *Bearbeiten* verändern oder über *Löschen* entfernen.

Mit der Funktion *Hinzufügen* richten Sie weitere Benutzer ein.

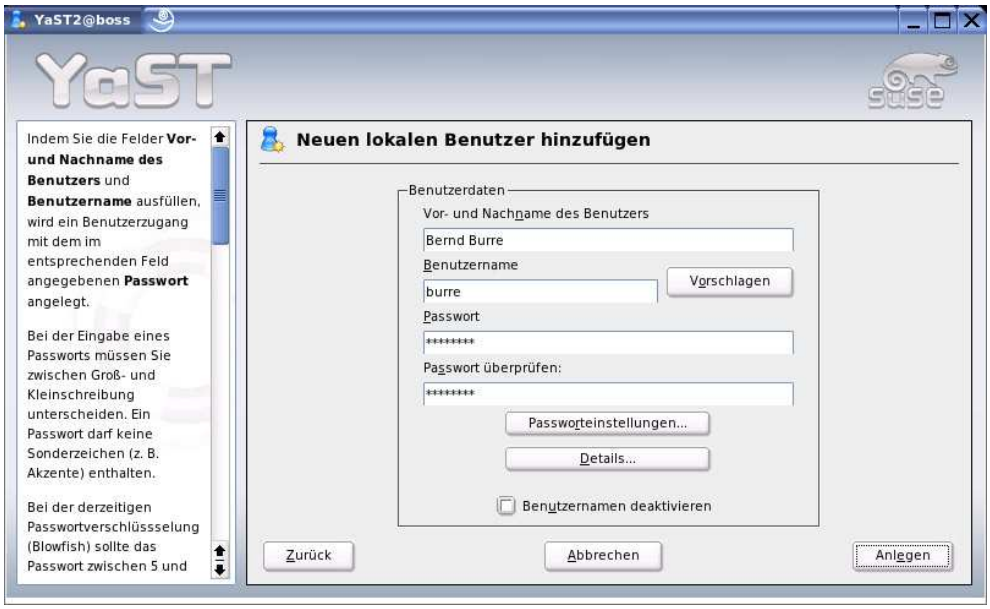

Abbildung 3.2: ***Benutzer Hinzufügen*** **mit YaST**

Wenn Sie in diesem Menü alle Daten eingegeben haben, reicht ein Klick auf die Schaltfläche *Anlegen*, um den neuen Benutzer-Account endgültig einzurichten. Falls Sie besondere Arbeitsumgebungen konfigurieren wollen, z. B. einen anderen Pfad für das Home-Verzeichnis, müssen Sie dafür vorher noch über die Schaltfläche *Details* ein Formular aufrufen und nutzen.

3.3 Disk-Quotas

Einzelne speicherhungrige Benutzer können die Arbeit auf Linux-Systemen blockieren:

- Wenn die Systemverwalter für die Home-Verzeichnisse keine eigene Partition angelegt haben, können sie die gesamte(n) Server-Festplatte(n) füllen und dadurch die Funktionsfähigkeit des Linux-Systems erheblich einschränken.
- Liegen die Home-Verzeichnisse in eigenen Partitionen, so können Vielspeicherer zumindest die Home-Partition so weit mit Daten füllen, dass dies die Arbeit aller Anwender blockiert.

Ein Schutz vor derartigen Problemen besteht darin, für jeden Benutzer eine Obergrenze (*Quota*) für die Nutzung der Festplatten festzulegen. Während man für kommerzielle Betriebssysteme Quota-Software zusätzlich erwerben muss, enthalten die meisten Linux-Distributionen freie und oft für bestimmte Nutzungsarten kostenlose Quota-Software.

Die von SuSE gelieferte Version der Quota-Software kommt mit allen wichtigen Linux-Partitionstypen wie `ext2`, `ext3` als auch `reiserfs` zurecht. Die Software erlaubt Quotas sowohl für Benutzer, als auch für Gruppen. Die Beschränkungen gelten jeweils für eine einzelne Partition.

Gruppenquotas geben die Summe des Speicherplatzes an, den alle Mitglieder dieser Gruppe gemeinsam belegen dürfen. Diese Werte müssen Sie bei vielen Benutzern daher recht hoch ansetzen.

Mit der Software kann man die individuelle Festplattenkapazität der Benutzer über zwei Angaben einschränken:

- Speicherplatz in Bytes und
- Zahl der Dateien über die Inodes.

Die Beispiele in diesem Kapitel beschränken jeweils den Speicherplatz in Bytes, nicht aber die Zahl der Dateien.

Bei beiden Möglichkeiten können Sie zwei unterschiedliche Grenzen setzen:

- Hard-Limits können Benutzer auf keinen Fall überschreiten,
- Soft-Limits dürfen Benutzer eine bestimmte Zeit (meist eine Woche) lang überschreiten, aber nur bis zum Hard-Limit. Sie bestimmen auch
- die Dauer, für die ein Benutzer das Soft-Limit überschreiten darf.

Bei SuSE finden Sie die Quota-Software im Paket `quota` der Selektion `Netzwerk/Server` bzw. in der rpm-Datei auf der `CD4`.

Bevor Sie die Quotas konfigurieren können, müssen Sie noch Module nachinstallieren. Das Quota-System benötigt Unterstützung durch den Kernel. Diese Unterstützung hat SuSE zwar eingebaut, aber als Modul. Genau dieses Modul müssen Sie noch laden lassen.

1. Gehen Sie dazu im YaST-Kontrollzentrum auf *System • Editor für /etc/sysconfig-Dateien* und dort auf *System • Kernel,* und erweitern Sie dort die Variable *INITRD_MODULES*. Normalerweise steht dort *reiserfs*, eventuell sogar einige Einträge mehr. Zu den Einträgen gehören jeweils Module, die der Kernel gleich beim Systemstart laden muss, und zwar vor der eigentlichen Modulverwaltung. Hier finden Sie also die Module für bestimmte Festplatten-Hardware, z. B. *SCSI* und besondere Partitionstypen, z. B. *reiserfs*.
2. Ergänzen Sie die Zeile um die Angabe `quota_v2`, und lassen Sie bitte zwischen den bisherigen Einträgen und Ihrer Eingabe ein Leerzeichen. Abschließend müssen Sie noch die *initrd*-Datei neu erzeugen lassen, die die Module für den Systemstart enthält.

```
mk_initrd
```

Normalerweise installiert SuSE bei der Standardinstallation den Boot-Manager *Grub*, der die Veränderungen automatisch registriert. Falls Sie jedoch noch *lilo* als Boot-Manager benutzen, müssen Sie nun *lilo* noch einmal von der Konsole aus aufrufen, damit der Boot-Manager die veränderte *initrd* übernimmt.

Nach einem Reboot ist dann die Änderung aktiv und das Modul für das Quota-System geladen. Statt den PC zu rebooten, kann man das Modul auch manuell mit `modprobe` laden:

```
modprobe -v quota_v2
```

Um die Quota-Unterstützung für eine Partition zu aktivieren, müssen Sie die Datei `/etc/fstab` erweitern, die alle Dateisysteme enthält, die das Linux-System beim Hochfahren automatisch mounten soll.

Die Datei können Sie entweder direkt mit Ihrem Lieblingseditor bearbeiten oder etwas sicherer vom YaST-Kontrollzentrum aus über *System • Partitionieren*. Die Warnung von YaST *»Verwenden Sie das Programm nur, wenn Sie mit dem Partitionieren von Festplatten vertraut sind.«* sollten Sie auf alle Fälle ernst nehmen.

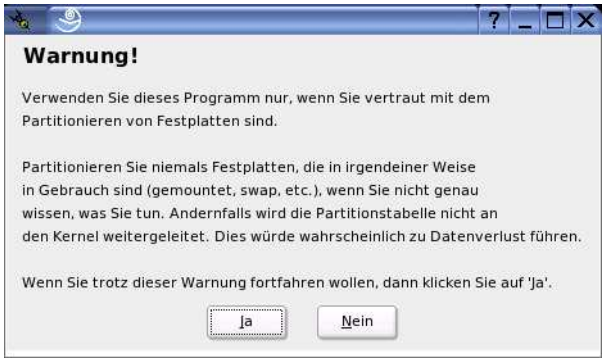

Abbildung 3.3: Partitionieren • Warnung

Wenn Sie sicher sind, dass Sie Partitionen verändern wollen, klicken Sie auf *Ja*. YaST öffnet eine Liste aller vorhandenen Partitionen, aus der Sie die Home-Partition (`/dev/hda9`) auswählen. In dem folgenden Formular ist in diesem Zusammenhang nur ein Button wichtig.

Sie sollten hier nichts anderes einstellen, sondern nur auf *Fstab-Optionen* klicken. Die benötigte Einstellung können Sie in dem dann folgenden Formular unterbringen.

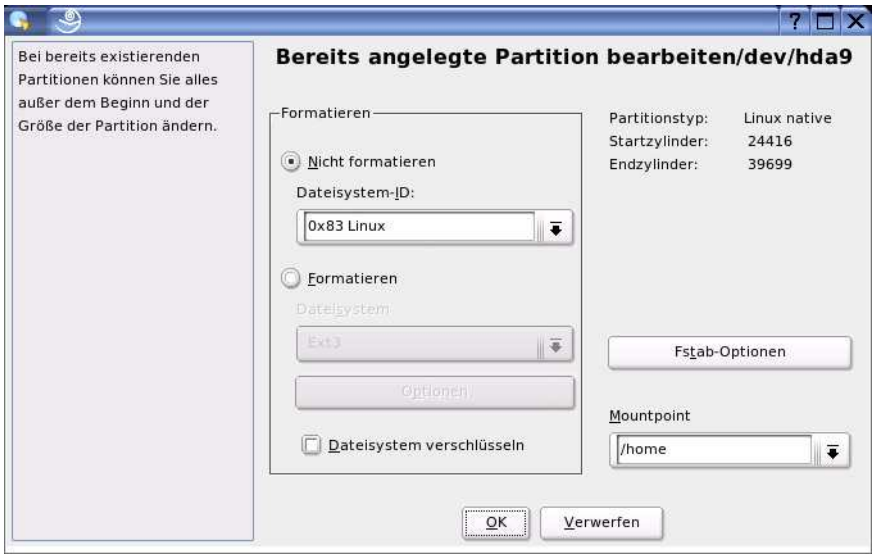

Abbildung 3.4: ***Partitionieren • Home-Partition***

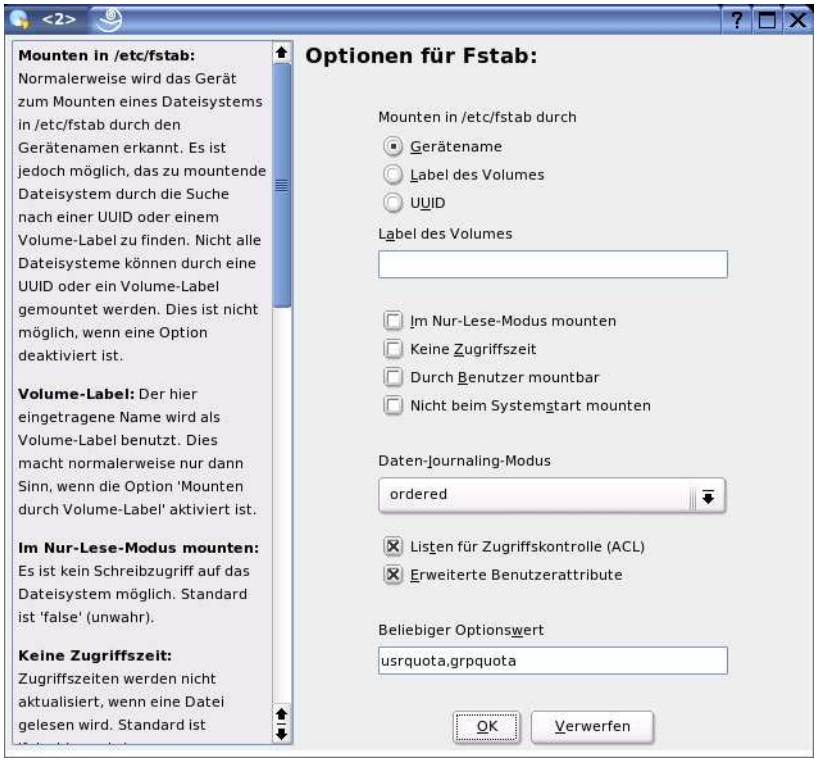

Abbildung 3.5: ***Partitionieren • Optionen***

Entscheidend ist hier das Feld *Beliebiger Optionswert*. Dieses Feld enthält normalerweise keinen Eintrag. Tragen Sie hier also ein

```
usrquota,grpquota
```

Damit aktivieren Sie für diese Partition sowohl Benutzerquota als auch Gruppenquota.

Tipp: Bei der Aufzählung `usrquota,grpquota` dürfen keine Leerzeichen zwischen diesen Parametern stehen!

Wenn Sie dann auf *Ok* klicken und das Partitionierungsmenü verlassen, ändert YaST die Datei `/etc/fstab`, nachdem es Sie vorher noch einmal gewarnt hat.

Bei einer Installation mit der hier im Kapitel 2 vorgeschlagenen Partitionierung hat diese Datei den folgenden Inhalt:

```
/dev/hda6   /              ext3    acl,user_xattr          1 1
/dev/hda9   /home          ext3    acl,user_xattr          1 2
/dev/hda7   /tmp           ext3    acl,user_xattr          1 2
/dev/hda8   /var           ext3    acl,user_xattr          1 2
/dev/hda5   swap           swap    pri=42                  0 0
devpts      /dev/pts       devpts  mode=0620,gid=5         0 0
proc        /proc          proc    defaults                0 0
usbfs       /proc/bus/usb  usbfs   noauto                  0 0
sysfs       /sys           sysfs   noauto                  0 0
/dev/cdrom  /media/cdrom   subfs   fs=cdfss,ro,procuid,
                                  ↵ nosuid,nodev,exec,
                                  ↵ iocharset=utf8        0 0
/dev/fd0    /media/floppy  subfs    fs=floppyfss,procuid,
                                  ↵ nodev,nosuid,sync     0 0
```

Um die Nutzung von Partitionen zu beschränken, müssen Sie das Schlüsselwort `usrquota` für Beschränkungen auf Benutzerebene oder `grpquota` für Beschränkungen auf Gruppenebene hinzufügen. Sie können auch beide Beschränkungen gleichzeitig aktivieren.

```
/dev/hda6   /              ext3    acl,user_xattr          1 1
/dev/hda9   /home          ext3    acl,user_xattr,
                                  ↵ usrquota,grpquota     1 2
/dev/hda7   /tmp           ext3    acl,user_xattr          1 2
/dev/hda8   /var           ext3    acl,user_xattr          1 2
/dev/hda5   swap           swap    pri=42                  0 0
devpts      /dev/pts       devpts  mode=0620,gid=5         0 0
proc        /proc          proc    defaults                0 0
usbfs       /proc/bus/usb  usbfs   noauto                  0 0
sysfs       /sys           sysfs   noauto                  0 0
```

```
/dev/cdrom  /media/cdrom   subfs   fs=cdfss,ro,procuid,
                                  ↵ nosuid,nodev,exec,
                                  ↵ iocharset=utf8      0 0
/dev/fd0    /media/floppy  subfs   fs=floppyfss,procuid,
                                  ↵ nodev,nosuid,sync   0 0
```

Da Sie das Dateisystem geändert haben, müssen Sie es neu mounten, am einfachsten durch Booten des Linux-Servers.

Tipp: Beschränken Systemverwalter den Speicherplatz nur für ganze Benutzergruppen mit Gruppenquotas, verhindert dies nicht, dass ein einzelner Benutzer den gesamten zulässigen Speicherplatz belegt und damit die Arbeit der anderen Benutzer blockiert. Benutzerquotas sind auf alle Fälle zum Sicherstellen eines geordneten IT-Betriebes geeigneter als Gruppenquotas.

Nach dem Neustart des Linux-Servers können Sie die Quota-Software den momentanen Belegungsstand der Festplatte erfassen lassen. Dazu geben Sie ein:

```
quotacheck  -vagu
```

Der Parameter `v` bewirkt eine ausführliche Ausgabe, mit dem Parameter `a` überprüft das Programm alle Partitionen, für die in der Datei `/etc/fstab` eine Quota-Unterstützung angegeben ist. Den Schalter `g` benötigen Sie für Gruppen-Quotas und den Schalter `u` für User-Quotas.

Sollte die Partition aktiv sein, so verweigert `quotacheck` seinen Dienst. Sie können dann entweder dafür sorgen, dass die Partition nicht aktiv ist oder zusätzlich den Schalter `m` mit angeben.

Das Untersuchen der Festplatte kann je nach Belegungsgrad einige Minuten dauern. Danach hat das Programm für jede quotierte Partition die Belegungsdaten in die Dateien `aquota.user` und `aquota.group` im Wurzelverzeichnis der jeweiligen Partition geschrieben.

Nach diesen Vorbereitungen können Sie die Quotas scharf schalten.

1. Dazu starten Sie das YaST-Kontrollzentrum, gehen dort in das Menü *System* • *Runlevel-Editor* • *Runlevel -Eigenschaften* und aktivieren hier den Dienst *boot.quota* für die Run-Level B (Start beim Booten), indem Sie den Leuchtbalken auf die Zeile mit *quota* bringen und dann das mit *B* beschriftete Kästchen anklicken.
2. Anschließend können Sie den Dienst auch gleich starten. Klicken Sie dazu auf *Starten/Anhalten/Aktualisieren,* und wählen Sie dann *Starten*. Damit ist der Dienst aktiv.

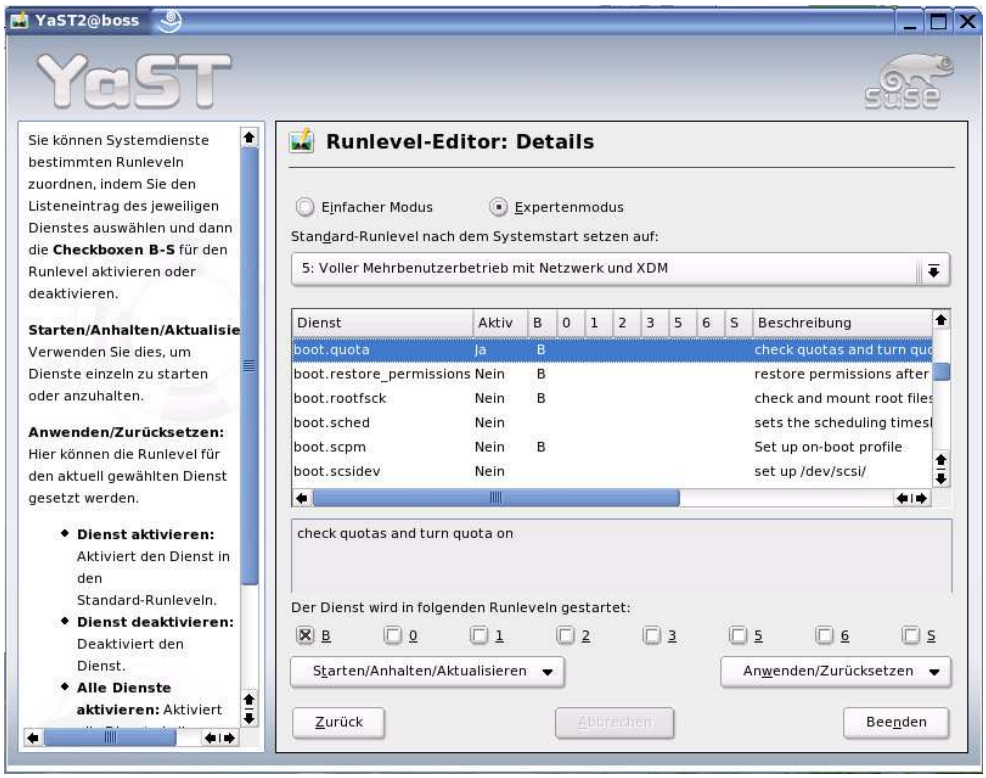

Abbildung 3.6: 6: Run-Level-Editor *QUOTA*

Sie sollten anschließend auch gleich den Dienst *quotad* für die Run-Level 3 und 5 aktivieren, der Quotas auf Laufwerken verwaltet, die Sie von anderen Rechnern per NFS gemountet haben. Dieser Dienst startet nur, wenn Sie Laufwerke von anderen Rechner eingebunden haben.

Um die Funktion Ihrer Quotas zu testen, richten Sie (als `root`) für einen Ihrer Benutzer eine Beschränkung ein:

```
edquota  -u  debacher
```

Daraufhin startet der von Ihnen eingestellte Editor mit folgendem Text:

```
Disk quotas for user debacher (uid 1000):
  Filesystem   blocks    soft    hard   inodes   soft   hard
  /dev/hda9      1028       0       0      167      0      0
```

Der Benutzer belegt 1.028 KByte Speicherplatz auf dem System mit 167 Dateien. Verändern Sie die Einstellungen zu

```
Disk quotas for user debacher (uid 1000):
  Filesystem   blocks    soft    hard   inodes   soft   hard
  /dev/hda9      1028    4000    5000      167      0      0
```

Damit erlauben Sie dem Benutzer, maximal 5.000 KByte Speicherplatz zu belegen.

Der Wert 0 bedeutet hier immer: keine Beschränkung. Ein Hard-Limit können Benutzer auf keinen Fall überschreiten, ein Soft-Limit (hier 4.000) nur für eine einstellbare Dauer. Diesen Zeitrahmen konfiguriert man mit `edquota -t`.

Melden Sie sich nun mit dem Benutzernamen an, für den Sie soeben die Beschränkungen erstellt haben. Jeder Benutzer kann seine eigenen Werte abfragen mit:

```
quota
```

Das erzeugt die folgende Ausgabe:

```
Disk quotas for user debacher (uid 1000):
 Filesystem blocks quota limit grace files quota limit grace
  /dev/hda9   1028  4000  5000         167     0     0
```

Der Benutzer belegt momentan mit 167 Dateien 1.028 KByte Speicherplatz. Er darf beliebig viele Dateien anlegen, aber maximal 5.000 KByte verbrauchen.

Das Soft-Limit ist nicht erreicht, damit entfällt auch die Angabe einer Gnadenfrist (*grace*) für das noch erlaubte Überschreiten dieses Limits.

Versuchen Sie nun, das Limit zu überschreiten, indem Sie große Dateien erstellen oder kopieren. Im einfachsten Fall geht das mit folgendem Befehl:

```
dd  if=/dev/zero  of=/home/debacher/test
```

Damit kopieren Sie von dem Gerät, das ständig Nullen liefert, in eine beliebige Datei, hier `/home/debacher/test`. Dieser Kopiervorgang läuft so lange, bis die Beschränkung erreicht oder die Festplatte voll ist.

Nach kurzer Zeit sollten Sie eine Fehlermeldung erhalten:

```
hda9: warning, user block quota exceeded.
hda9: write failed, user block limit reached.

dd: Schreiben in /home/debacher/test:
Der zugewiesene Plattenplatz (Quota) ist überschritten
7529+0 Datensätze ein
7528+0 Datensätze aus
```

Ein erneuter Aufruf von `quota` liefert jetzt als Ausgabe:

```
Disk quotas for user debacher (uid 1000):
 Filesystem blocks quota limit grace files quota limit   grace
  /dev/hda9   5000* 4000  5000         194     0     0
```

Die Datei `test` hat eine Größe von etwa 5 MB angenommen, danach hat die Quota-Begrenzung den Kopiervorgang abgebrochen.

Die Quota-Begrenzung ist damit funktionsfähig und kann eingesetzt werden.

Leider bietet die in der SuSE Distribution enthaltene Quota-Software keine Möglichkeit, einen Standardwert für alle Benutzer festzulegen. Dies kann in der betrieblichen Praxis auch sinnvoll sein, wenn Sie den Vorstand Ihres Unternehmens nicht zu sehr gängeln wollen. Daher müssen Systemverwalter die Userquotas für jeden Benutzer einzeln festlegen oder ggf. mit dem Befehl `edquota vervielfältigen`.

Um die für einen Benutzer (hier *debacher*) definierte Quotas auf den Benutzer *schultz* zu übernehmen, geben Sie den Befehl ein:

```
edquota  -p  debacher  schultz
```

3.4 Die Linuxbu.ch/Tools

Die *Linuxbu.ch/Tools* sind eine bewährte Sammlung einfacher Administrationsprogramme mit Browser-Schnittstelle.

Sie arbeiten mit drei Benutzergruppen, denen Sie unterschiedliche Rechte zuordnen können:

- *ntadmin*
- *leiter*
- *mitarbeiter*

Jede der drei Gruppen hat unterschiedliche Zugriffsrechte auf die Funktionen. *mitarbeiter* können mit den Tools lediglich ihr eigenes Passwort verändern, *leiter* können zusätzliche *mitarbeiter*-Accounts einrichten und die Internet-Verbindung aktivieren sowie Gruppen einrichten. Die Update-Funktion können hingegen nur Angehörige der Gruppe *ntadmin* nutzen.

Hinweis: In den bisherigen Versionen haben die *Linuxbu.ch/Tools* statt der Gruppe *ntadmin* einfach *admin* benutzt. In gemischten Umgebungen benötigen Windows-Rechner für Administrationszwecke unbedingt die Gruppe *ntadmin*.

Die Tools bieten momentan folgende Funktionen:

- Eigenes Passwort ändern (alle Benutzer),
- Gruppenverwaltung (*ntadmin*),
- Benutzerverwaltung (*ntadmin* und *leiter*),
- Internet-Verbindung auf- und abbauen (*ntadmin* und *leiter*),
- Software-Update (*ntadmin*).

Die *Linuxbu.ch/Tools* ändern an keiner Stelle die Konfiguration Ihres Rechners oder der Software. Verwalter können sie einfach erweitern und anpassen und müssen lediglich den Web-Server Apache so konfigurieren, dass er die Programme aus dem Verzeichnis `/srv/www/htdocs/tools` ausführt.

Hinweis: Da SuSE den Web-Server in der Standardinstallation nicht mehr einrichtet, müssen Sie den Apache Web-Server zuerst installiert haben. Eine ausführliche Beschreibung dazu lesen Sie im Kapitel 6 dieses Buches.

Sie können die Software vom Server zum Buch (`www.linuxbu.ch`) beziehen und kostenlos nutzen. Installieren Sie sie in drei Schritten:

- Auspacken des Archivs `tools4_2.tgz` und Initialisieren der Programme,
- Erweitern der Apache-Konfigurationsdatei und
- Einrichten von Administratoren-Account und Tools-Gruppen.

3.4.1 Auspacken des Archivs und Initialisieren der Programme

Laden Sie die Datei `tools4_2.tgz` vom Server `www.linuxbu.ch`, und speichern Sie sie im Verzeichnis `/srv/www/htdocs`. Wechseln Sie in dieses Verzeichnis, und entpacken Sie die Datei mit:

```
tar  xvfz  tools4_2.tgz
```

Dabei entsteht ein Verzeichnis `tools`, in das Sie nun hineinwechseln:

```
cd  tools
```

Der größte Teil der Tools besteht aus Programmen in der Programmiersprache Perl. Diese Programme erkennen Sie an der Endung `.pl`. Für viele Funktionen benötigen die *Linuxbu.ch/Tools* die besonderen Rechte des Benutzers `root`. Diese Rechte geben Sie den Perl-Programmen, indem Sie als Benutzer `root` folgenden Befehl eingeben (Sie müssen dazu im Verzeichnis `tools` sein):

```
./makecgi
```

`makecgi` erstellt nach einer Sicherheitsabfrage zu jedem Programm mit der Endung `.pl` ein C-Programm mit der Endung `.cgi`, das diese besonderen Rechte besitzt.

Sollten Sie beim Aufruf des Programmes Fehlermeldungen der Art

```
./makecgi: line 30: gcc: command not found
```

bekommen, dann ist auf Ihrem Rechner der C-Compiler *ggc* noch nicht eingerichtet. Sie müssen dann das Paket *gcc* nachträglich installieren. Sie finden das Paket in der Selektion *C/C++ Compiler und Werkzeuge*, die Sie ruhig komplett installieren können, indem Sie die Checkbox vor der Selektionsgruppe aktivieren. Sie finden die notwendigen Pakete übrigens auf den Datenträgern der Professional-Version, nicht aber auf der CD der Evaluations-Version zum Buch.

Sofern der C-Compiler vorhanden, ist kann *makecgi* seiner Arbeit nachgehen.

```
makecgi - erstellt die .cgi Dateien.

Grundlage ist die Datei source/setroot.c
Alle bestehenden .cgi Dateien werden ueberschrieben.

Sind Sie sich sicher, dass Sie fortfahren moechten ? [J/Y/N] j
Mache admin/internet/index.cgi
Mache admin/index.cgi
Mache admin/passwd/index.cgi
Mache admin/passwd/chpasswd.cgi
Mache admin/gruppen/shgroupdata.cgi
Mache admin/gruppen/shgrouplist.cgi
Mache admin/gruppen/newgroup.cgi
Mache admin/gruppen/addgroup.cgi
Mache admin/gruppen/delgroup.cgi
Mache admin/update/index.cgi
Mache admin/benutzer/shuserdata.cgi
Mache admin/benutzer/shuserlist.cgi
Mache admin/benutzer/newuser.cgi
Mache admin/benutzer/deluser.cgi
Mache admin/benutzer/multiadd.cgi
Mache admin/benutzer/chuserdata.cgi
Mache admin/benutzer/adduser.cgi
Mache admin/benutzer/shuser.cgi
```

Damit sind die Tools einsatzbereit, und Sie können diese in die Konfiguration des Web-Servers einbinden.

3.4.2 Erweitern der Apache-Konfigurationsdatei

Im Verzeichnis `/srv/www/htdocs/tools/` finden Sie die Datei `httpd.conf.erg` mit den notwendigen Ergänzungen für die Konfigurationsdatei des Apache-Servers.

```
#
# Erweiterung fuer die Linuxbu.ch/Tools
# einfach ueber YaST->Editor fuer
#/etc/sysconfig->Network->WWW->Apache2
# den vollen Pfad zu dieser Datei in die
# sysconfig aufnehmen:
#
# APACHE_CONF_INCLUDE_FILES="/srv/www/htdocs/tools/
# httpd.conf.erg"
#
# anschliessend den Apache neu starten
#
#

<Directory /srv/www/htdocs/tools/admin>
Addtype application/x-httpd-cgi .cgi

Options Indexes FollowSymLinks EXECcgi
authType Basic
authuserFile /etc/apache2/yfh.pwd
authName LinuxBuchTools
require valid-user
</Directory>

<Directory /srv/www/htdocs/tools>
Addtype application/x-httpd-cgi .cgi
Options Indexes FollowSymLinks EXECcgi
</Directory>
```

Zum Aktivieren dieser Änderung müssen Sie anschließend im YaST-Kontrollzentrum unter *System • Editor für /etc/sysconfig-Daten • Network • WWW • Apache2* für die Variable *APACHE_CONF_INCLUDE_FILES* den Wert */srv/www/htdocs/tools/httpd.conf.erg* angeben und damit die Erweiterung in die Konfiguration des Web-Servers einbinden.

Damit binden Sie die mit den Tools mitgelieferte Konfigurationsdatei in die Konfigurationsdatei des Web-Servers ein, ohne diese selber bearbeiten zu müssen. Genauere Informationen über den Web-Server finden Sie im Kapitel 6.

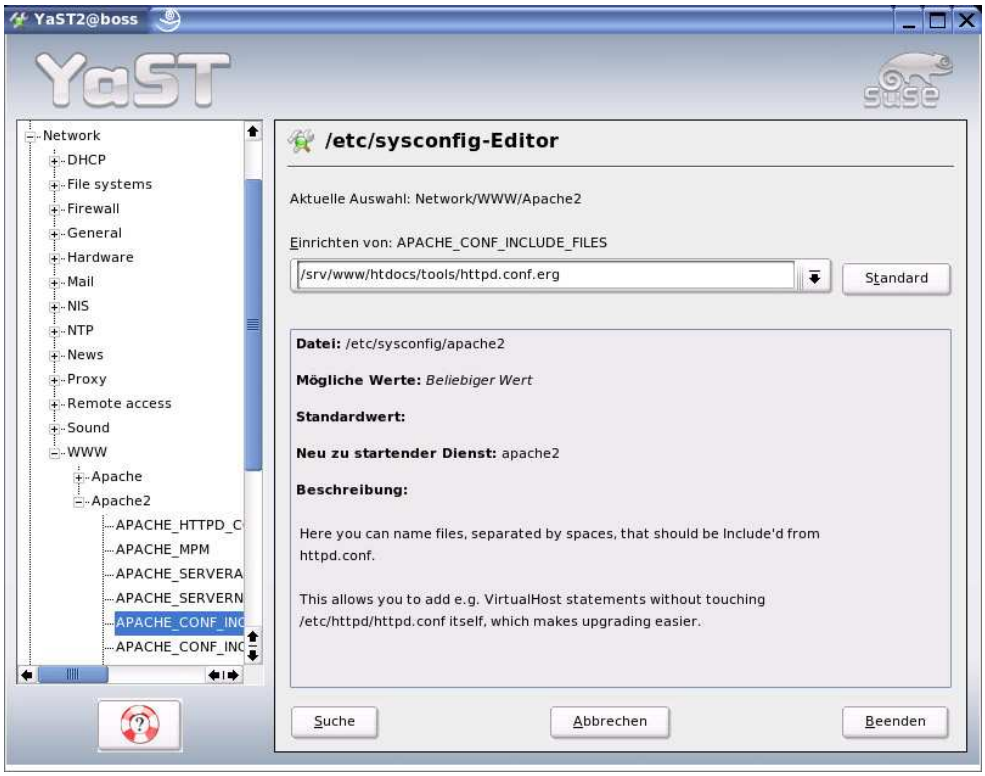

Abbildung 3.7: Eigene Konfigurationsdatei einbinden

Durch diese Ergänzungen führt Apache die Programme im Verzeichnis `tools` aus und authentifiziert Benutzer für alle Zugriffe auf die *Linuxbu.ch/Tools*.

Nach diesen Änderungen müssen Sie den Apache neu starten:

```
rcapache restart
```

3.4.3 Einrichten von Administratoren-Accounts und Tools-Gruppen

Für die Nutzung der Tools müssen Sie die zwei Gruppen

- *leiter*
- *mitarbeiter*

anlegen und mindestens einen Administratoren-Account einrichten.

Um die Verwaltungsfunktionen leiten zu können, sollten Sie sich selbst mit Ihrem persönlichen Account (nicht `root`) in die Gruppe *ntadmin* aufnehmen.

Am einfachsten geht das mit dem `usermod`-Befehl wie hier im Beispiel:

```
usermod -G ntadmin debacher
```

Im YaST-Kontrollzentrum gehen Sie dafür auf *Sicherheit und Benutzer* • *Gruppen bearbeiten und anlegen*. Um alle Gruppen sehen zu können, klicken Sie hier auf *Filter festlegen* • *Systemgruppen*. Dann wählen Sie die Gruppe *ntadmin* aus und klicken auf *Bearbeiten*. Hier müssen Sie nun die Checkbox vor Ihrem Benutzer-Account aktivieren und sodann die Konfiguration mit *Weiter* beenden.

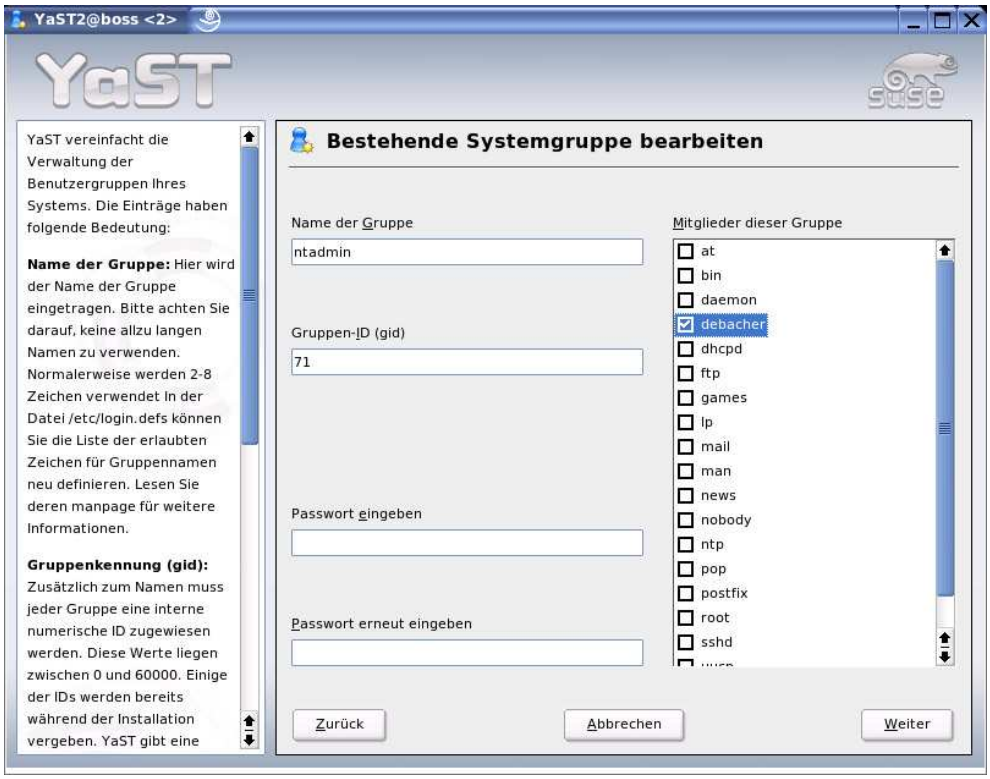

Abbildung 3.8: YaST: Hinzufügen zur Gruppenverwaltung

Starten Sie dann auf einem über das Netz angeschlossenen Rechner einen Browser, und rufen Sie die URL `/tools/` auf dem Linux-Server auf, auf dem Sie die Tools ausführen, hier `http://192.168.1.2/tools/` (auch der letzte Slash ist wichtig).

Im Dialogfenster geben Sie Ihren Benutzernamen und Ihr Passwort ein. Danach steht Ihnen das Hauptmenü zur Verfügung.

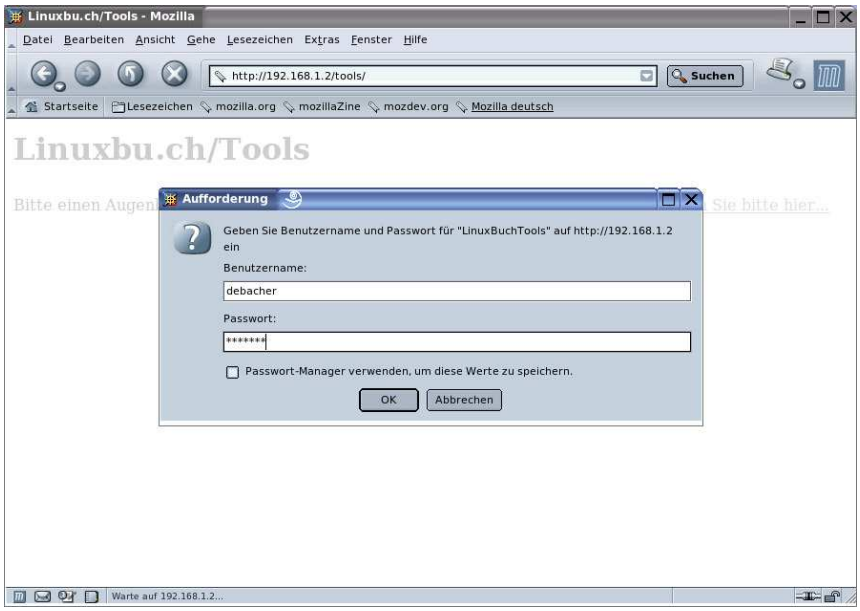

Abbildung 3.9: Tools: Anmeldung

Abbildung 3.10: Tools: Hauptmenü

Dort gehen Sie zunächst auf *Gruppenverwaltung* und dann auf *Neue Gruppe anlegen*. Hier können Sie nacheinander die Gruppen *leiter* und *mitarbeiter* anlegen.

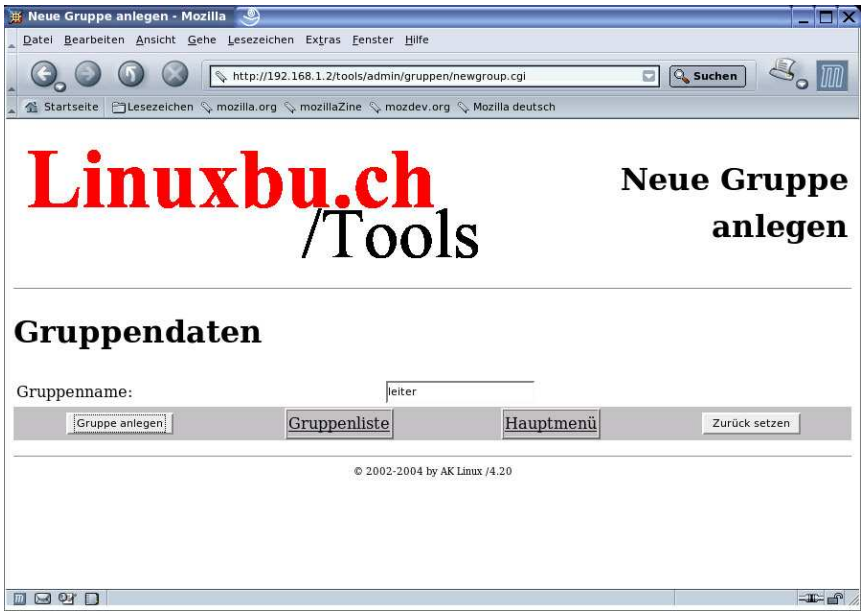

Abbildung 3.11: Tools: Neue Gruppe anlegen

Nach dem Anlegen dieser beiden Gruppen sollte die Gruppenliste wie im nächsten Fenster aussehen:

Abbildung 3.12: Tools: Gruppenliste

Um abschließend die Angaben für Ihren eigenen Account zu vervollständigen, gehen Sie auf *Benutzerverwaltung*, dort auf *Benutzerliste,* und klicken dort Ihren Benutzer-Account an.

Sie sollten vor allem darauf achten, dass Sie auch für sich eine Abteilung und Ihren vollen Namen angeben, da die Tools Ihren Namen bei allen Benutzern eintragen, die Sie mit den *Linuxbu.ch/Tools* anlegen.

Abbildung 3.13: Tools: Daten ändern

Wenn Sie die Daten eingegeben haben, klicken Sie auf *Daten ändern*, worauf das Programm bestätigt, dass es die Daten übernommen hat.

Abbildung 3.14: Tools: Daten geändert

Damit sind die *Linuxbu.ch/Tools* installiert und einsatzbereit.

3.4.4 Anlegen von Benutzern mit den Tools

Alle Administratoren und die Leiter können mit den Tools jetzt Benutzer einrichten. Nur Administratoren können Leiter einrichten. Die Administratoren haben vollen Zugriff auf alle Benutzer und können deren Daten sowie Passwörter ändern. Die Leiter können nur die Daten (einschließlich Passwort) der Mitarbeiter ändern, die sie selbst eingerichtet haben.

Legen Sie zuerst die Abteilungsleiter an, im Beispiel *Klaus Sparsam*. Gehen Sie dazu auf *Benutzerverwaltung* • *Benutzer anlegen*, und füllen Sie das Formular nach dem Muster wie in der Abbildung 3.15 aus.

Zwingend erforderlich ist nur die Angabe der Abteilung und des vollständigen Namens. Wenn Sie keine weiteren Daten angeben, erzeugen die Tools den Login-Namen aus den Initialen und einer laufenden Nummer, in diesem Fall also `ks1001`. Als Anfangspasswort stellen die Tools den Vornamen `klaus` ein. Wenn Sie andere

Login-Namen und Passwörter für Ihre Benutzer haben möchten, müssen Sie diese in die dafür vorgesehenen Felder eintragen.

Abbildung 3.15: Benutzer anlegen, hier Abteilungsleiter

Wenn Sie die Eingaben für einen Benutzer abgeschlossen haben, startet ein Klick auf *Benutzer anlegen* das Erstellen des Benutzer-Accounts.

Die Tools legen auch das Home-Verzeichnis des Benutzers an, in diesem Fall wäre das `/home/ksparsam`. Zusätzlich können die Tools auch Quotas für die neuen Benutzer anlegen. Dazu müssen Sie für einen Beispiel-Account die Quotas sorgfältig konfigurieren und den Tools diesen Account als Muster nennen. Die Einstellungen des Musters übernimmt das Programm dann für alle neuen Benutzer.

Um die Quota-Unterstützung zu aktivieren, müssen Sie die Konfigurationsdatei `/srv/www/htdocs/tools/config.pl` bearbeiten.

Die Quota-Untersützung aktivieren Sie, indem Sie in der drittletzten Zeile das Kommentarzeichen # entfernen und den Benutzernamen `beispiel` durch einen passenden Benutzer ersetzen.

`/srv/www/htdocs/tools/config.pl` (Auszug, Ende der Datei):

```
# $FIRST_CH_UID gibt die UserID an, ab der Benutzer zum Aendern
# angezeigt werden. Wenn man das Veraendern/Loeschen des
# root-Account verhindern moechte, sollte man diesen Wert
# entsprechend hoch setzen.
$FIRST_CH_UID = 1000;
```

```
# $LAST_CH_UID gibt die letzte UID an, nach der Benutzer zum
# Aendern nicht mehr angezeigt werden. (nobody hat 65534)
$LAST_CH_UID = 10000;

# $FIRST_NEW_UID gibt die erste UID an, die fuer neue Benutzer
# vergeben wird.
$FIRST_NEW_UID = 1000;

# $FIRST_CH_GID gibt die GruppenID an, ab der Gruppen verwendet
# werden duerfen. Zum Aendern der Gruppendaten, oder zum
# Aendern von Benutzerdaten.
$FIRST_CH_GID = 70;

# $LAST_CH_GID gibt die Letzte GruppenID an, bis zu der
# Gruppendaten veraendert werden duerfen, oder Gruppendaten fuer
# Benutzer verwendet werden duerfen.
$LAST_CH_GID = 10000;

# $NEWUSER_SHELL gibt an, welche Shell ein Neuer Benutzer
# standardmaessig bekommt.
$NEWUSER_SHELL = "/usr/bin/passwd";

# $USERADMINPFAD gibt den Pfad zum Benutzerverwaltungsmodul an.
$USERADMINPFAD = "benutzer/";

# $QUOTAUSER gibt den Benutzer an, dessen Quotas kopiert werden
$QUOTAUSER="beispiel";

# $INTERFACE gibt an, ueber welches Geraet die
# Internetverbindung laeuft
$INTERFACE="ippp0";
```

Machen Sie sich ruhig auch mit den anderen Konfigurationseinstellungen in dieser Datei vertraut, sie ist ausführlich kommentiert.

3.4.5 Internet Start/Stop

Mit den *Linuxbu.ch/Tools* kann man festlegen, welche Benutzer über das lokale Netz das Internet anwählen können. In der Grundeinstellung können diese Funktion alle Mitglieder der Gruppen *ntadmin* und *leiter* aufrufen.

Abbildung 3.16: Tools: Internet-Verbindung

Wollen Sie dies erweitern oder einschränken, so müssen Sie die Datei `modinfo.dat` im Verzeichnis der jeweiligen Funktion, hier `/srv/www/htdocs/tools/admin/internet/modinfo.dat`, bearbeiten:

```
index.cgi
Internet Start/Stop
Starten/Stoppen der Internet-Verbindung
1
1
0
0
0
/htmldoc/mods/internet.html
# Ende der Datei
```

Der Aufbau dieser Konfigurationdatei ist immer gleich:

1. Zeile: Startprogramm des Moduls
2. Zeile: Kurztext für das Menü
3. Zeile: Langtext für die Statuszeile im Menü
4. Zeile: Ausführungsrechte für ntadmin `0` = nein, `1` = ja
5. Zeile: Ausführungsrechte für leiter `0` = nein, `1` = ja
6. Zeile: Ausführungsrechte für mitarbeiter `0` = nein, `1` = ja

7. Zeile: Logging für Aktionen `0` = nein, `1` = ja

8. Zeile: Logging für Fehler `0` = nein, `1` = ja

9. Zeile: frei

10.Zeile: Hilfetext (spätere Erweiterung)

Entscheidend für das Vergeben von Rechten sind die Zeilen 4, 5 und 6. Hier stehen die Werte `1` und `0`. Damit verbieten Sie nur den Mitgliedern der Gruppe *mitarbeiter*, eine Verbindung aufzubauen. Wollen Sie erlauben, dass auch diese die Funktion nutzen, so müssen Sie die erste `0` durch eine `1` ersetzen.

Die Internet-Einwahl kann sehr unterschiedlich erfolgen, per Modem, ISDN oder DSL. Die *Linuxbu.ch/Tools* erwarten daher, dass Sie in der Konfigurationsdatei das Interface korrekt angegeben haben.

`/srv/www/htdocs/tools/config.pl` (Auszug, Ende der Datei):

```
# $INTERFACE gibt an, über welches Geraet die
# Internetverbindung laeuft
$INTERFACE="ippp0";
```

Die Tools benutzen für die Steuerung der Internet-Verbindung das Programm *cinternet*, das Sie im Kapitel 10 kennen lernen werden.

Die *Linuxbu.ch/Tools* können Sie relativ leicht um weitere Module erweitern. Eventuell finden sich ja Leser, die bereit sind eigene Entwicklungen beizutragen.

3.5 Benutzerverwaltung in großen Netzen

Wenn Sie Linux-PCs im Netz betreiben, werden Sie nicht alle Administrationsaufgaben der Benutzerverwaltung auf allen Rechnern wiederholen wollen.

Das noch vor Jahren hierfür meist eingesetzte Network Information System (*NIS*), (*Yellow Pages*) entspricht seit langem nicht mehr den heutigen Sicherheitsanforderungen und ist weder hinreichend flexibel noch erweiterbar. Deshalb setzten sich hier hierarchische Datenbanken durch. Von der X.500-Protokollfamilie, die einen umfangreichen Verzeichnisdienst definiert, stammt das Lightweight Directory Access Protocol (*LDAP*) ab. *Directory* bezeichnet im englischen Sprachgebrauch *Verzeichnis*. LDAP ist lese-optimiert. Daher eignet es sich besonders für Aufgaben wie das Authentifizieren von Benutzern und Adressbüchern, bei denen Abfragen überwiegen.

LDAP ist nicht ursprünglich als Benutzerverwaltung entwickelt worden. Sie können darin weit mehr als die Daten und Passwörter Ihrer Benutzer ablegen. So könnten Sie beispielsweise Mitarbeitern ihre Fotos zuordnen, zusätzliche Telefonnummern speichern oder die URL ihrer Homepage hinterlegen. Sie sind hier nicht

an Vorgaben gebunden, die Sie vielleicht bei NIS als einschränkend empfunden haben. LDAP ist kein Linux/Unix-Spezifikum. Microsoft verwendet seine eigene Version davon seit Windows 2000-Server unter dem Namen Active Directory (*AD*). Dieses macht nichts anderes als eine LDAP-Datenbank: Es verwaltet insbesondere Benutzer- und Maschinendaten.

Damit Sie die Benutzer Ihrer Organisation mit LDAP verwalten können, benötigen Sie neben der Datenbank weitere Komponenten.

- LDAP selbst stellt lediglich die Funktionen zur Datenverwaltung bereit. Es speichert die Informationen und gibt sie bei Bedarf an Berechtigte heraus. LDAP läuft als Server-Prozess auf einem der Linux-Server. Alternativ zu einem Linux-Server kann man auch ein Active Directory eines Windows 2000/2003-Servers verwenden.
- Weiterhin benötigen Sie einen Name Service Switch (*NSS*). Dieser macht auf ihren Linux-PCs die Benutzer gegenüber dem System bekannt. Die PCs selbst verfügen über keine oder über nur sehr wenige Benutzerdaten. Diese können Sie sogar miteinander verknüpfen und gemeinsam nutzen. Der Name Service Switch kümmert sich nicht selbst um den Zugang zu den PCs, sondern überlässt dies den Pluggable Authentication Modules.
- Diese Pluggable Authentication Modules (*PAM*) sind ein Plugin der zentralen C-Bibliothek Ihres Linux-Systems. Sie bewachen die Zugänge zu Ihrem PC. Bei Bedarf können sie das Neusetzen der Passwörter koordinieren und weitere Routinen für den Zugang zu PCs anbieten. So könnte beispielsweise eine PAM-Komponente ein im Samba liegendes Home-Verzeichnis einbinden. Das ist deshalb sinnvoll, da dieser Vorgang Benutzername und Passwort benötigt. So müssen Systemverwalter ihre Benutzer nicht zweimal nach diesen Daten befragen.
- Der Name Service Caching Daemon (*NSCD*) merkt sich für eine bestimmte Zeit Zuordnungen, beispielsweise zwischen numerischen UserIDs und den Namen von Accounts, damit Ihr Linux-PC nicht bei jedem Aufruf von *ls* den LDAP-Server fragen muss.

Die nächsten Abschnitte beschreiben, wie Sie diese Komponenten zu einer flexiblen, sicheren und leicht erweiterbaren Benutzerverwaltung zusammenführen.

3.5.1 Kurzeinführung in LDAP

LDAP ist eine hierarchische Datenbank. Anders als relationale Datenbanken legt sie ihre Daten nicht in miteinander verknüpften Tabellen, sondern in einer Baumstruktur ab. LDAP eignet sich dadurch für sehr kompaktes Speichern von Benutzerinformationen jeder Art. Die Datenbasis lässt sich sogar so erweitern, dass LDAP Aufgaben für einen Samba-PDC oder BDC übernehmen kann. Lesen Sie hierzu Kapitel 9.

LDAP arbeitet objektorientiert. Jeder Directory-Eintrag beschreibt ein Objekt, das eine Person, eine Verwaltungseinheit oder auch ein Server, ein Drucker usw. sein kann. Jeder Eintrag kann weitere Attribute besitzen, die einen Typ und einen bzw. mehrere Werte haben. Im hierarchischen Verzeichnis gibt es immer eine einzige Wurzel `root`, ähnlich wie beim UNIX/Linux-Verzeichnisbaum. Die Baumwurzel lässt sich hier wie dort weder verschieben noch im Betrieb verändern.

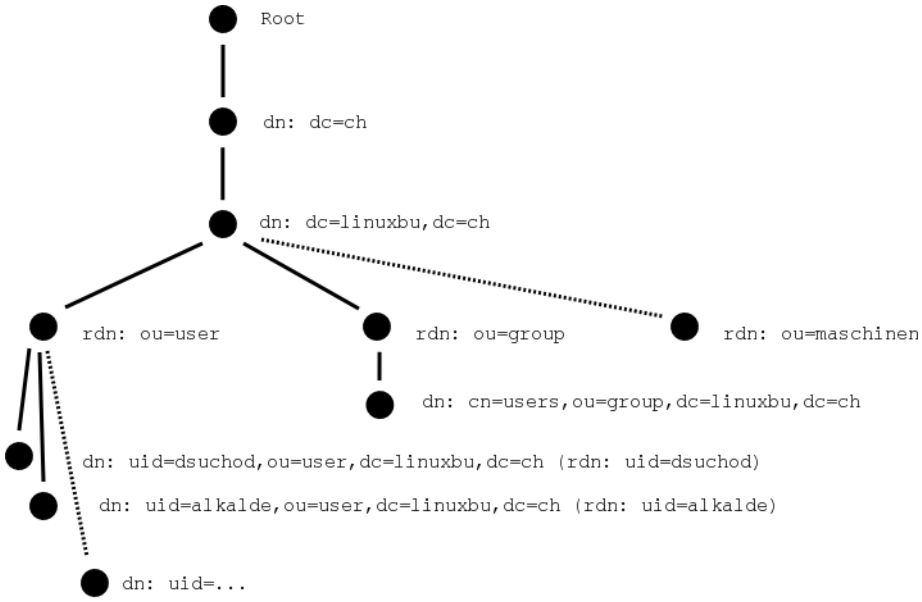

Abbildung 3.17: Eine LDAP-Beispielhierarchie

Clients müssen später Datensätze eindeutig identifizieren. Deswegen besitzt jedes Objekt im Verzeichnis einen eindeutigen Namen, den *Distinguished Name* (dn). Dieser setzt sich von der Wurzel aus gelesen aus den bisherigen Distinguished Names zusammen. Je tiefer Sie in die Baumhierarchie hinabsteigen, desto länger wird er. Es gibt mehrere Möglichkeiten, eindeutige Namen zu erreichen.

- *Domain Components* (dc) oder
- *Country* (c), *Organization* (o)

Domain Components setzt beispielsweise Microsoft in seinen Active Directories ein. Sie stellen auf eine sehr leicht verständliche Weise sicher, dass die Objekte auf jeder Hierarchieebene eindeutig sind. Die Wurzel bezeichnet man beginnend mit der Top-Level-Domain einer Site, in den darunter liegenden Hierarchien folgen Second-Level-Domain- und falls erforderlich Sublevel-Domain-Namen. Ab dann verwenden Sie meistens andere Bezeichner, wie *Organizational Unit* (ou). Sie kön-

nen alternativ die Top-Level-Objekte Country und Organization einsetzen. Das ist das traditionelle Verfahren. In den folgenden Beispielen

Einträge zu einem Objekt heißen Attribute. Der *Common Name* (cn) ist ein allgemeiner Bezeichner, ein für Menschen gut lesbares und merkbares Attribut, ähnlich einem Rechnernamen. An den Baumenden ist häufig dieses Attribut Bestandteil des *dn*. In den folgenden Beispielen ist die UserID *uid* Bestandteil des *dn*, da sie auf jeden Fall eindeutig ist.

Für viele Standarddaten sind bereits Klassen vordefiniert. Diese können voneinander Eigenschaften und definierte Attribute erben. So ist die üblicherweise für Personendaten verwendete Klasse *InetOrgPerson* von *OrganizationalPerson* und diese wieder von *Person* (person) abgeleitet. Zu einer Person gehören zwingend als so genannte MUST-Attribute die Objektklasse *objectClass* selbst, der Nachname *sn* und der *commonName*, üblicherweise Vor- und Nachname. Zusätzlich gibt es mit MAY gekennzeichnet optionale Attribute, wie eine beliebige Beschreibung *description*, Verweise auf ein anderes Objekt *seeAlso*, eine Telefonnummer *telephoneNumber* oder ein Passwort *userPassword*. Da mit einer Person häufig noch weitere Eigenschaften verknüpft sind, gibt es die abgeleitete Objektklasse *organizationalPerson*. Diese erbt die Eigenschaften von *person* und definiert darüber hinaus optionale Eigenschaften.

```
dn: uid=alkalde,ou=user,dc=linuxbu,dc=ch
uid: alkalde
cn: Anna Alkalde
sn: Alkalde
title: Dr.
mail: aa@linuxbu.ch
employeeNumber: 22
telephoneNumber: 0321-123456
mobile: 0171-1234567
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uidNumber: 1005
gidNumber: 100
homeDirectory: /home/alkalde
loginShell: /bin/bash
```

Das Beispiel zeigt einen typischen LDAP-Eintrag einer Person. Die Objektklasse ist *InetOrgPerson*. Sie hat von *Person* die zwingenden Attribute *sn* und *cn* geerbt und weitere Attribute wie *employeeNumber* erlaubt. Kombiniert ist *InetOrgPerson* mit *posixAccount* und *shadowAccount*. Diese Objektklassen liefern weitere Felder, wie *uidNumber* oder *homeDirectory*.

3.5.2 Benutzerverwaltung mit LDAP

Für eine einfache Benutzerverwaltung benötigt ein Linux-System

- einen Common Name als Bezeichner des tatsächlichen Namens einer Person,
- eine eindeutige Zeichenfolge als UserID,
- eine eindeutige Benutzer- und Gruppennummer,
- ein Heimatverzeichnis,
- eine Loginshell und
- eventuell ein Benutzerpasswort.

Soll die Datenbank die Einheitlichkeit der Adressbücher der Mitarbeiter sicher stellen, sollten Sie außerdem Daten wie Telefonnummer, E-Mail-Adresse, persönliche Web-Seite usw. speichern.

LDAP bietet Administratoren viel Freiheit beim Organisieren der Datensätze. So lange sie sich an die LDAP-Standards halten, können sie die Benutzerdaten in der Datenbank in sehr verschiedener Weise ablegen:

- Sie könnten auf einer Hierarchieebene verschiedene Unterbäume für einzelne Abteilungen anlegen und diesen Abteilungen die Benutzer zuordnen.
- Viele Administratoren ordnen alle Mitarbeiter in einem einzigen Baum an und vermerken in einem weiteren Attribut die Abteilung des Mitarbeiters. Dieses Modell erleichtert das Aktualisieren der Datenbank nach einem Wechsel der Abteilung.

Die Design-Entscheidung hat später Einfluss auf die Angabe des Suchfilters für die LDAP-Client-Konfiguration. Für den Anfang bieten die YaST2-Komponenten von SuSE einen guten Einstieg. Lesen Sie zunächst hier darüber, bevor es danach tiefer in Details geht.

3.5.3 Aufsetzen eines OpenLDAP-Servers

Wenn in Ihrem Netz schon ein LDAP-Server arbeitet und Sie diesen benutzen möchten oder sollen, überspringen Sie bitte diesen Abschnitt.

OpenLDAP2 ist eine freie Implementierung der Version 3 des LDAP-Standards. Es ist Bestandteil der meisten großen Linux-Distributionen. Bei SuSE 9.2 können Sie den Server mit Tools und Hilfsprogrammen aus der Selektion *LDAP Server und Werkzeuge* auswählen oder in der Paketauswahl nach *ldap* suchen.

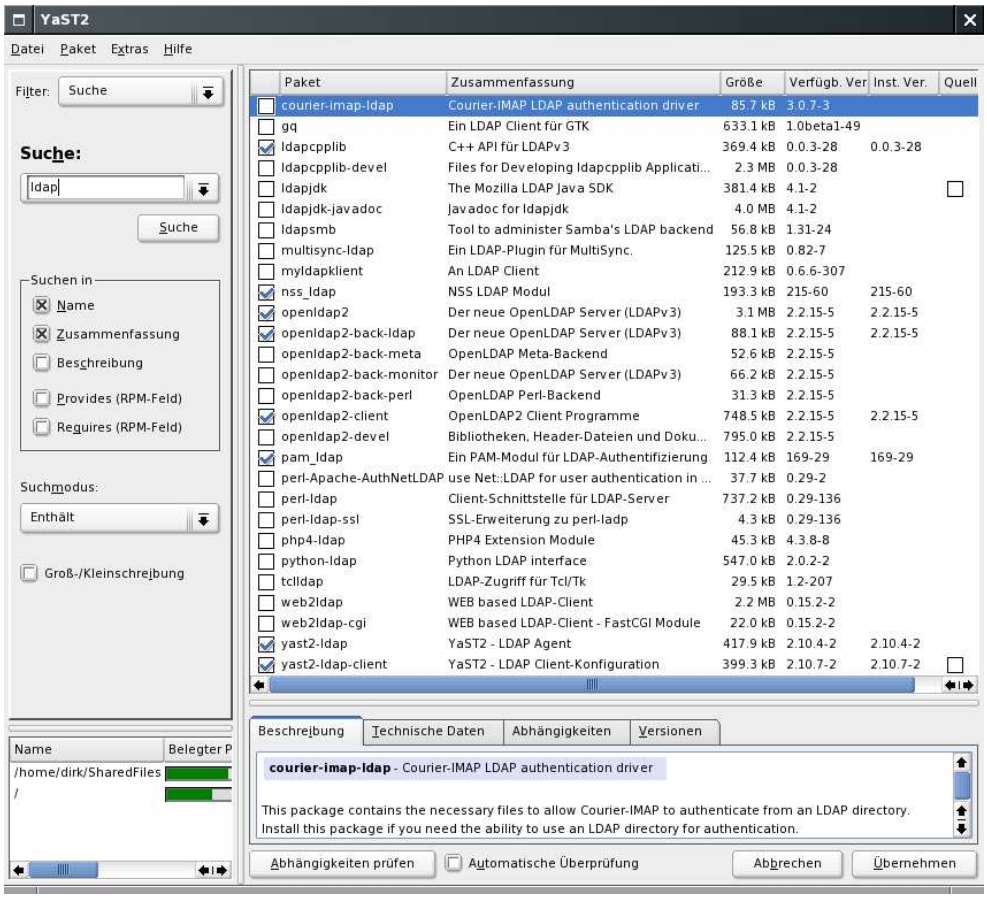

Abbildung 3.18: Auswahl einiger LDAPv3-Komponenten

Meist benötigt man folgende Pakete:

- *openldap2* – den OpenLDAP2-Server,
- *openldap2-back-ldap* – das Standard- Backend für den Server,
- *openldap2-client* – ist meist bereits installiert,
- *nss_ldap* – LDAPv3-Modul des NSS für die LDAP-Benutzer-Identifikation
- *pam_ldap* – LDAPv3-Modul für PAM für die LDAP-Benutzer-Authentifizierung
- *yast2-ldap und yast2-ldapclient* – zur LDAP-Konfiguration via YaST2-Modul

Die Installation legt einige Verzeichnisse und Konfigurationsdateien für OpenLDAP an. Der LDAP-Server erwartet seine Konfigurationdatei `slapd.conf` unterhalb von `/etc/openldap`. Die Dateien der laufenden Datenbank landen üblicher-

weise im Verzeichnis `/var/lib/ldap`. Dieses Verzeichnis können Sie in der Konfigurationsdatei wie voreingestellt verwenden oder anders angegeben.

Zusammen mit dem LDAP-Paket installiert YaST2 etliche Kommandozeilenprogramme. Die Werkzeuge `ldapsearch`, `ldapadd`, `ldapdelete` und `ldapmodify` für Operationen auf der LDAP-Datenbank stehen im Verzeichnis `/usr/bin`.

Bevor Sie mit Ihrem frisch installierten Server jetzt Daten erfassen, richten Sie ihn durch Anpassen der Konfigurationsdatei ein. Hierzu öffnen Sie mit Ihrem Lieblingseditor die Datei `/etc/openldap/slapd.conf`:

```
...
#######################################################################
# BDB database definitions
#######################################################################

database        bdb
checkpoint      1024    5
cachesize       10000
suffix          "dc=mydomain,dc=site"
rootdn          "cn=Manager,dc=mydomain,dc=site"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          Geheim
# The database directory MUST exist prior to running slapd
# AND should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap
...
```

Das Listing zeigt nur den für diesen Schritt wesentlichen Ausschnitt der Datei. Sie passen den `suffix` an Ihre Domain an. Entsprechend setzen Sie auch den *rootdn*. Das Beispiel geht von der privaten Domain `mydomain.site` aus. `rootdn` bezeichnet den Directory-Administrator. Dieser Benutzer erhält zusammen mit dem Passwort `rootpw` immer alle Rechte auf der LDAP-Datenbank. Im Beispiel ist nur ein einfaches Passwort gewählt. Setzen Sie hier bitte eins, das Ihre Sicherheitsanforderungen erfüllt. Das Kommando `slappasswd` fragt Sie interaktiv nach einem Passwort und gibt dieses dann verschlüsselt aus. Die Ausgabe kopieren Sie anschließend in die `slapd.conf` an die Stelle, an der oben `Geheim` steht.

```
linux:/etc/openldap # slappasswd
New password:
Re-enter new password:
{SSHA}7mTMFTNjV1BnND7SeZvg/lKOTAvSB4tL
```

Nach diesen Anpassungen können Sie Ihren LDAP-Server starten. Hierzu gibt es das Run-Level-Skript `rcldap`, das wie gewohnt mindestens die Argumente `start`, `stop`, `restart` kennt.

```
linux:/etc/openldap # rcldap start
Starting ldap-server                                        done
linux:/etc/openldap # ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
```

Nach dem Start des Dienstes erfolgt ein kleiner Test, ob der Server antwortet. Er müsste antworten, kann aber noch keine Informationen ausgeben, da er noch keine bekommen hat. Mit der folgenden Kommandozeile prüfen Sie, ob der Directory-Administrator sich erfolgreich nach Eingabe seines Passwortes verbinden darf.

```
ldapsearch -x -D "cn=Manager,dc=mydomain,dc=site" -W
```

Wenn Sie dieselbe Ausgabe wie beim ersten Test sehen, ist alles erfolgreich verlaufen. Die Kommandozeilenschalter gelten für die meisten OpenLDAP-Tools. Sie haben folgende Bedeutung:

- `x` – *simple Authentication*, sollte eigentlich immer angegeben werden.
- `D` – *Distinguished Name* des Datenbankadministrators oder eines anderen Benutzers, unter dessen ID Sie auf die Datenbank zugreifen wollen.
- `W` – Fragt interaktiv nach einem Passwort, meistens zusammen mit `-D`. Mit `w` können Sie das Passwort direkt angeben, z. B.: `-w Geheim`.
- `f` – Lesen aus einer Datei mit anschließender Angabe des Dateinamens. Spielt bei `ldapadd` oder `ldapmodify` eine Rolle.
- `h` – Gibt den Rechnernamen oder die IP des LDAP-Servers an, z. B. `-h 127.0.0.1`.
- `H` – Gibt den Unified Resource Indicator (*URI*) für eine LDAP-Quelle an. Für eine verschlüsselte Verbindung auf den Server `ldap.mydomain.site` sieht die Angabe so aus: `-H ldaps://ldap.mydomain.site:636`. Den Port müssen Sie nicht angeben, wenn Sie den Standard-Port für verschlüsselte Verbindungen `636` wählen. Der Standard-Port für unverschlüsselte Verbindungen lautet `389`. Diesen Parameter benötigen Sie nur, wenn Sie oder YaST2 die LDAP-Quelle nicht in der `/etc/openldap/ldap.conf` konfiguriert haben.

- `b` – Setzt den obersten Knoten für die Suche auf dem LDAP-Baum. So können Sie die Suche einschränken und dadurch beschleunigen. Suchen Sie beispielsweise nur Benutzer, ist die folgende Angabe sinnvoll: `-b ou=user,dc=mydomain,dc=site`. Sie müssen ebenfalls einen Startknoten für allgemeines Suchen angeben, wenn dieser nicht in der `ldap.conf` definiert ist, da Ihr Suchergebnis sonst leer bleiben könnte.
- `d` – Legt den Debug level fest.

Nun wird es Zeit, Daten zu erfassen. Hierzu stehen Ihnen viele Wege offen. Ein Weg führt über die YaST2-LDAP-Client-Einstellung. Leider kommt dieser nicht mit einer komplett leeren Datenbank klar. Daher muss man zumindest die Wurzel initialisieren, indem man die nachfolgenden Datei `init.ldif` lädt:

```
dn: dc=mydomain, dc=site
objectClass: dcObject
objectClass: top
objectClass: namedObject
dc: mydomain
```

Diese Datei hat das so genannte Lightwight Directory Interchange Format (*LDIF*). Diese Datei liest man mit dem LDAP-Tool `ldapadd` in die Datenbank ein.

```
ldapadd -x -D "cn=Manager,dc=mydomain,dc=site" -W -f init.ldif
```

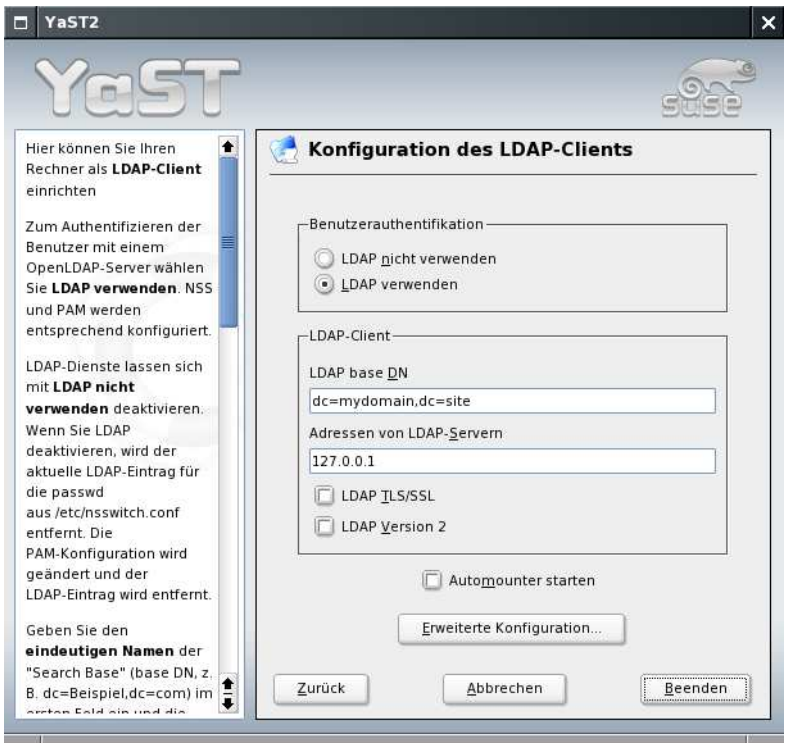

Abbildung 3.19: Das erste Konfigurationsfenster

Anschließend wählen Sie in YaST2 im Hauptmenü *Netzwerkdienste* • *LDAP-Client* aus.

Als Erstes aktivieren Sie im Bereich *Benutzerauthentifikation: LDAP verwenden*. Dann tragen Sie Ihren LDAP-Base-DN ein: `dc=mydomain,dc=site` und schalten die verschlüsselte Übertragung zum Server aus. Bisher startet der neu konfigurierte Server lediglich auf dem lokalen Interface `127.0.0.1`. Dann geht es über *Erweiterte Konfiguration* zum nächsten Dialog.

Abbildung 3.20: Die erweiterte Konfiguration mit einigen Basiseinstellungen

Die meisten Felder hat YaST2 bereits automatisch mit Einträgen gefüllt. Sie müssen noch den Administrator-DN festlegen, so wie Sie ihn in der `slapd.conf` erfasst haben. Die hier eingetragenen Daten finden Sie nach dem Speichern in `/etc/sysconfig/ldap` wieder. Sie können die Standardkonfigurationsobjekte durch Anklicken automatisch erzeugen lassen. Anschließend geht es weiter mit der Schaltfläche *Einstellungen für die Benutzerverwaltung konfigurieren*... Beim Zugriff auf diese Maske fragt YaST2 nach dem Kennwort des Directory-Administrators. Die Authentifizierung benötigt es, um in der Datenbank Daten einzutragen. Das Fenster *Konfiguration von Modulen* legt Konfigurationsgruppen an.

Um einen neuen Abschnitt des LDAP-Baums zu erzeugen, in dem LDAP Gruppen ablegen soll, hier `group`, klicken Sie auf *Neu*.

Anschließend legen Sie mit *Neu* den Knoten für die Benutzerverwaltungswerkzeuge an, hier `user` genannt. In beiden Fällen können Sie durch *Vorlage konfigurieren* weitere *Details* einstellen.

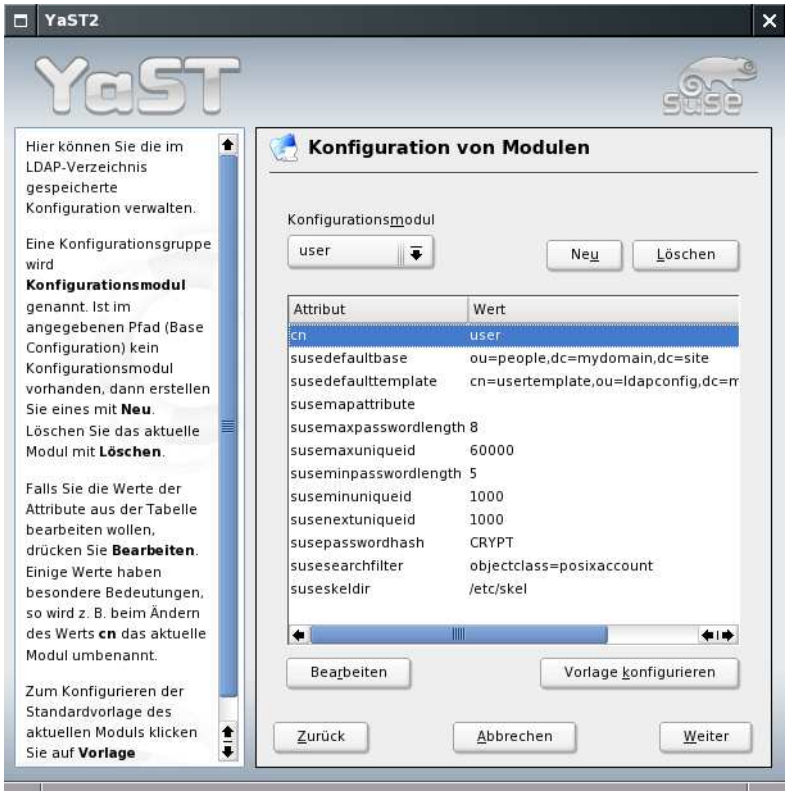

Abbildung 3.21: Anlegen und Konfiguration von Modulen

Schließen Sie dann mit *Weiter* und *Beenden* ab. Die Datenbank enthält nun schon mehrere Einträge. Diese zeigt Ihnen `ldapsearch -x` an. Jedoch kennt Ihre Datenbank immer noch keine Benutzer. Diese fügen Sie in YaST2 in *Sicherheit und Benutzer* mit dem Unterpunkt *Benutzer bearbeiten und anlegen* hinzu.

Abbildung 3.22: Die Startseite der Benutzerverwaltung zeigt alle konfigurierten User-Accounts

Wenn die Konfiguration des LDAP-Clients erfolgreich war, zeigt Ihnen das Konfigurations-Interface einen Butten für *LDAP-Optionen*... Um diese müssen Sie sich nicht kümmern, da Sie den Client bereits konfiguriert haben. In der Tabelle der Benutzer sehen Sie erst einmal nur alle angelegten lokalen Accounts, da im LDAP noch keine Accounts eingetragen sind. Über *Filter festlegen* • *LDAP-Benutzer* erhalten Sie eine neue Sicht der Tabelle. Unter Umständen fragt Sie YaST2, ob Sie die fehlenden Knoten für Benutzer und Gruppen im LDAP ergänzen wollen. Dieses bestätigen Sie einfach mit *OK*.

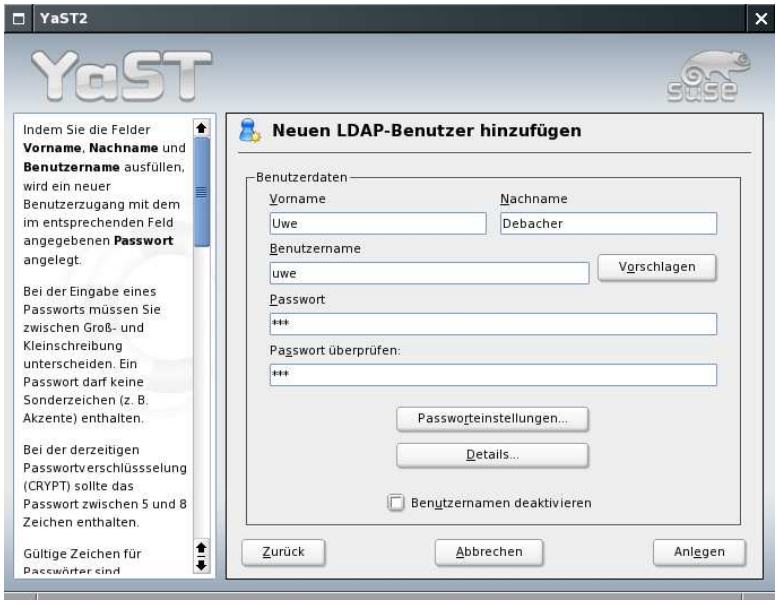

Abbildung 3.23: Einen neuen Benutzer im LDAP hinzufügen

Wenn Sie nun über *Filter festlegen* • *Benutzerdefinierte Filtereinstellung*... die LDAP-Benutzer aktivieren, listet eine Tabelle sowohl lokale als auch LDAP-Accounts auf. Mit *Beenden* aktivieren Sie Ihre Einstellungen. Mit dem Befehl

```
linux:~ # id uwe
uid=1001(uwe) gid=100(users) Gruppen=100(users)
```

können Sie nachsehen, ob Ihr neu angelegter Benutzer dem System bekannt ist. Nun sollte sich dieser Nutzer auch an einer Konsole oder mit *ssh* an dem PC anmelden können. Noch hat der Nutzer kein Home-Verzeichnis, da YaST es nicht automatisch anlegt. Dieses importieren Sie vermutlich von einem anderen PC, z. B. mit NFS in Kombination mit dem Automounter. NFS ist in diesem Buch im Kapitel 8 beschrieben.

3.5.4 Mit OpenLDAP direkt arbeiten

Bisher waren Sie mit den Komponenten LDAP, NSS und PAM nicht direkt konfrontiert. Die Einstellungen erledigten die YaST2-Module. Wenn Sie viele Benutzer gleichzeitig anlegen wollen, möchten Sie das vielleicht nicht interaktiv vornehmen. Wollen Sie Ihre Benutzerverwaltung selbst im LDAP anlegen, erweitern Sie die im vorherigen Abschnitt gezeigte LDIF-Datei wie folgt:

```
# LDIF-Datei für ein Beispielnutzer: alkalde
dn: dc=mydomain, dc=site
objectClass: dcObject
objectClass: top
objectClass: namedObject
dc: mydomain

# zusätzliche Einträge
dn: ou=user, dc=mydomain, dc=site
objectclass: organizationalUnit
ou: user

dn: ou=group, dc=mydomain, dc=site
objectclass: organizationalUnit
ou: group

dn: cn=users, ou=group, dc=mydomain, dc=site
objectClass: posixGroup
objectClass: top
objectClass: namedObject
cn: users
gidNumber: 100
userPassword: group-pw
```

```
dn: uid=alkalde, ou=user, dc=mydomain, dc=site
uid: alkalde
cn: Anna Alkalde
sn: Alkalde
objectclass: person
objectclass: posixAccount
objectclass: shadowAccount
objectclass: top
userPassword: aa-pw
uidNumber: 1002
gidNumber: 100
homeDirectory: /home/alkalde
loginShell: /bin/bash
mail: aa@linuxbu.ch
```

Die Beispieleinträge entsprechen nicht ganz dem, was YaST2 eintragen würde. Für die darauf zugreifenden Applikationen und Dienste ist nur wichtig, dass die entscheidenden Attribute identisch sind. Das Kommando `ldapadd` zum Einfügen von Objekten in die Datenbank wie im folgenden Listing kennen Sie schon vom vorherigen Abschnitt.

```
linux:~/ldap # ldapadd -x -c -D "cn=Manager,dc=mydomain,
  ↵ dc=site" -W -f init.ldif
Enter LDAP Password:
adding new entry "dc=mydomain, dc=site"
adding new entry "ou=user, dc=mydomain, dc=site"
adding new entry "ou=group, dc=mydomain, dc=site"
adding new entry "cn=users, ou=group, dc=mydomain, dc=site"
adding new entry "uid=alkalde, ou=user, dc=mydomain, dc=site"
```

Der Kommandozeilenschalter `-c` sorgt dafür, dass das Kommando nicht abbricht, wenn schon Daten eingetragen sind. So können Sie Ihr LDIF einfach erweitern und erneut laden, um einen oder mehrere weitere Accounts hinzuzufügen. Hier im Beispiel legen Sie nacheinander den Root-Knoten und dann die zwei Unterknoten für Benutzer (`user`) und Gruppen (`group`) in einer leeren Datenbank an. Anschließend generieren Sie unterhalb der Gruppen eine Gruppe `users` und unterhalb der Benutzer einen Account `alkalde`. Für weitere Nutzer duplizieren Sie das Beispiel für `alkalde`. Für weitere Gruppen nehmen Sie den Eintrag darüber als Vorlage.

Sind Sie mit einem Eintrag nicht einverstanden, können Sie diesen mit `ldapdelete` wieder entfernen:

```
ldapdelete -x -D "cn=Manager,dc=mydomain,dc=site" -
W "uid=dsuchod,ou=user,dc=mydomain,dc=site"
```

Sie können jedoch keine Knoten entfernen, in denen noch Einträge vorhanden sind. Der Versuch, den Baum `ou=user,dc=mydomain,dc=site` zu löschen, schlägt fehl, wenn darunter noch ein einziger Benutzer in der Datenbank steht. Um den Inhalt einer kompletten Datenbank zu löschen, können Sie den Dienst stoppen und dann alle Dateien im Verzeichnis `/var/lib/ldap` entfernen.

```
rclinux:~/ldap # ldap stop
rclinux:~/ldap # rm /var/lib/ldap/*
rclinux:~/ldap # rcldap start
```

In der Standardeinstellung startet der LDAP-Server mit dem oben angegebenen Befehl nur auf der IP `127.0.0.1`. In dieser Einstellung arbeitet OpenLDAP nur unverschlüsselt. Möchten Sie den Server über das Netzwerk von entfernten Rechnern aus ansprechen, editieren Sie die Datei `/etc/sysconfig/openldap`. In dieser Datei können Sie mit `OPENLDAP_START_LDAPS=yes` festlegen, dass der Server mit Verschlüsselung arbeiten soll. Hierzu sind zusätzliche Einträge in der Konfigurationsdatei `/etc/openldap/slapd.conf` notwendig. Sie benötigen dann ein Server- und ein CA-Zertifikat. Mit `OPENLDAP_LDAP_INTERFACES` können Sie festlegen, dass der Server auf weiteren IP-Adressen und Ports gestartet wird. Ein Eintrag von `192.168.75.128:389 127.0.0.1:389` bewirkt, dass der Server-Prozess `slapd` auf den Interfaces mit den IP-Nummern `192.168.75.128` und `127.0.0.1` auf ankommende Verbindungen lauscht. Wenn alles soweit funktioniert, können Sie den Dienst durch das Run-Level-System automatisch beim Hochfahren Ihres Servers starten lassen. Dann steht OpenLDAP automatisch in den Run-Levels 3 und 5 zur Verfügung:

```
insserv ldap
```

Fehler beim Versuch, Daten in LDAP einzufügen, können verschiedenste Ursachen haben. Diese sind manchmal nicht auf den ersten Blick sichtbar. Die folgenden Tipps helfen Ihnen hoffentlich bei der Fehlersuche:

- In der aktuellen Version des OpenLDAPs muss das Attribut, das zum Aufbau des Distinguished Names verwendet wird, noch einmal in der Attributliste auftauchen. Weiterhin ist es erforderlich, immer die Objektklasse *top* anzugeben. Dieses ist eine generelle Klasse, die keine eigenen MUST-Attribute definiert. MUST-Attribute sind kumulativ: Mindestens eine Klasse ist neben *top* erforderlich. Werden mehrere Objektklassen angegeben, müssen alle MUSTs dieser Objektklassen gemeinsam erfüllt sein.
- Man kann nur leere Knoten löschen. Entfernen Sie alle Einträge nacheinander, ausgehend von denen, die am weitesten von der Wurzel weg sind zu dieser hin. Den Inhalt der gesamten Datenbank löschen Sie einfacher direkt wie oben gezeigt.

Zwei Dateien spielen für LDAP-Clients eine Rolle. Sie können das Verhalten eines LDAP-Clients mit den DNS-Einstellungen Ihres Linux-Systems vergleichen. Anders als bei NIS starten Sie für den LDAP-Client keinen eigenen Dienst. Die LDAP-Programme können die Daten zur Verbindung auf den Server aus der Datei `/etc/openldap/ldap.conf` lesen:

```
#BASE   dc=example, dc=com
#URI    ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
TLS_REQCERT     allow
host    127.0.0.1
base    dc=mydomain,dc=site
```

Einige Parameter können Sie direkt auf der Kommandozeile angeben. Lesen Sie hierzu die Liste der Kommandozeilenschalter im Abschnitt zum OpenLDAP-Server.

Die beiden Erweiterungen der C-Bibliothek für die Benutzeranmeldung und -zuordnung PAM und NSS greifen ihrerseits auf die Datei `/etc/ldap.conf` zu. Diese Datei ist zur Erleichterung Ihrer Anpassungen ausführlich kommentiert.

3.5.5 PAM im Einsatz

Im vorletzten Abschnitt hatten Sie die YaST2-Unterstüztung zur Verwendung von LDAP zur Benutzerverwaltung kennen gelernt. Nun möchten Sie vielleicht mehrere Linux-Maschinen mit LDAP-Authentifizierung einrichten und nicht jedes Mal die grafische Oberfläche verwenden. Sie möchten ebenfalls verstehen, was sich hinter den Kulissen abspielt.

PAM alleine genügt nicht zum Einbinden von LDAP-Benutzern. Damit Ihr Linux-Rechner mit diesen Nutzern umgehen kann, nachdem diese sich angemeldet haben, muss auch der Name Service Switch eingerichtet sein. Hierzu passen Sie die Datei `/etc/nsswitch.conf` an. Diese definiert die Quellen, aus denen die zentrale C-Bibliothek beispielsweise aus einer im Dateisystem gespeicherten numerischen UserID den Account-Namen ermittelt:

```
# /etc/nsswitch.conf
[ ... ]
passwd: files ldap nis
group:  files ldap nis
[ ... ]
```

In diesem Beispiel befragt NSS zuerst die lokalen Dateien `/etc/passwd` oder `/etc/group` nach Benutzer- oder Gruppenzuordnungen. Anschließend nutzt sie hierzu LDAP. Zur Demonstration, dass Sie weitere Quellen angeben können, steht hier noch das alte NIS. So können Sie schrittweise von NIS zu LDAP migrieren. Der NSCD speichert Anfragen an verschiedene Datenquellen zwischen (*Caching*). Wenn der `nscd` diesen Nutzer noch im Negativ-Cache und diesen Eintrag noch nicht vergessen hat, ist ein Benutzer nach dem Hinzufügen einer neuen Datenquelle dem System nicht sofort bekannt.

Ein Aufruf von

```
rcnscd restart
```

löscht den Cache und ermöglicht damit den sofortigen Zugriff auf den Benutzer-Account.

LDAP ist nur eines der Beispiele einer netzwerkbasierten gemeinsamen Benutzerverwaltung. Während früher NIS eingesetzt wurde, wird zukünftig vielleicht Kerberos diese Rolle übernehmen. Damit die zentrale C-Bibliothek eines Systems und Applikationen nicht bei jeder Änderung angepasst werden müssen, wählt PAM einen völlig neuen Ansatz. Die einzelnen Anwendungen benutzen zur Benutzeranmeldung Funktionen aus einer Bibliothek, die PAM bereitstellt. Die Funktionen benutzen ihrerseits passende PAM-Module zum Authentifizieren.

PAM kann jedoch noch mehr. Neben dem *Authentication Management* kann es sich ebenfalls um die Aufgaben *Account Management*, *Session Management* und *Password Management* kümmern. Jedes PAM-Modul muss mindestens einen, kann aber auch mehrere dieser Jobs abdecken.

Diese Aufteilung findet sich in den Konfigurationsdateien wieder: Für jede Aufgabe finden Sie keinen, einen oder mehrere Einträge.

Für einige Anwendungen ist es ein Problem, dass PAM rein passiv ist und stets von einer Applikation aufgerufen werden muss. Wenn Sie automatisch nach dem Durchziehen Ihrer Chipkarte oder dem Auflegen Ihres Fingers auf einem biometrischen Leser eingeloggt werden wollen, muss eine Applikation regelmäßige pollen und die Authentifizierung anstoßen.

Die schematische Darstellung zeigt den Kommunikationsfluss zwischen den Applikationen und PAM. Die PAM-Bibliothek wird zur Laufzeit eines Programms mit Benutzeranmeldung geladen. Das PAM-Modul kommuniziert zum einen mit der PAM-Bibliothek, um seine Parameter auszulesen. Zum anderen tauscht es Daten mit der Applikation aus, um an die Benutzerdaten wie Account-Namen und Passwort zu gelangen.

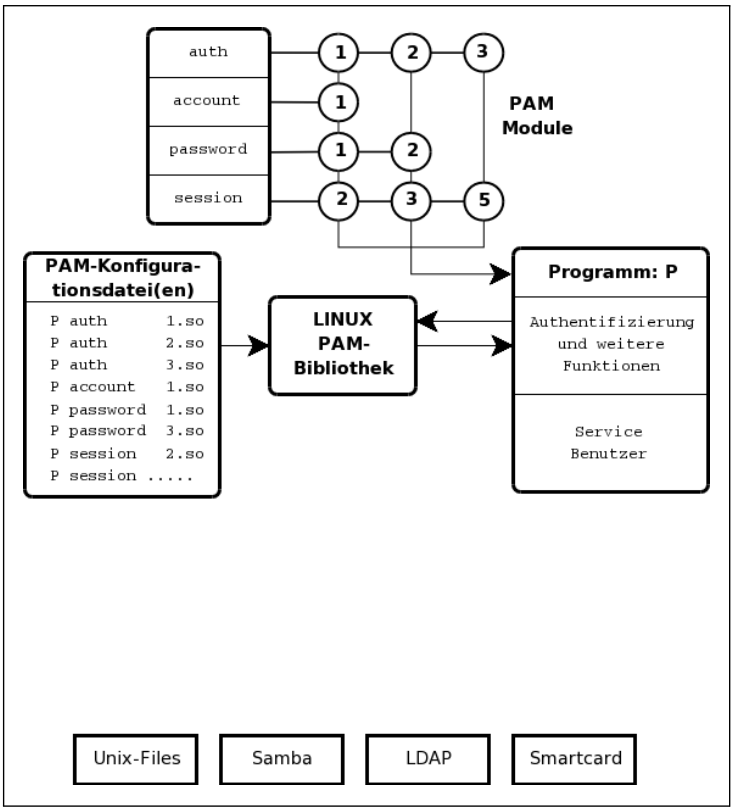

Abbildung 3.24: Die Funktionsweise von PAM

Die PAM-Bibliothek ist bei SuSE ein eigenes RPM (*pam und pam-modules*). Spezielle Module, die weitere Bibliotheken benötigen, wie etwa das LDAP-Modul, finden sich in separaten Paketen, die Sie bei Bedarf zusätzlich installieren. Bei der Installation legt PAM drei Verzeichnisse an:

- `/lib/security`
- `/etc/security`
- `/etc/pam.d`

`/lib/security` nimmt die Bibliotheksdateien auf. Dieses Verzeichnis enthält alle aktuell auf einem System installierten Standard-PAM-Module:

```
pam_access.so      pam_localuser.so    pam_shells.so
pam_chroot.so      pam_mail.so         pam_smbpass.so
pam_cracklib.so    pam_make.so         pam_stress.so
pam_debug.so       pam_mkhomedir.so    pam_succeed_if.so
pam_deny.so        pam_mktemp.so       pam_tally.so
pam_devperm.so     pam_motd.so         pam_time.so
pam_env.so         pam_nologin.so      pam_unix2.so
```

```
pam_filter          pam_opensc.so        pam_unix_acct.so
pam_filter.so       pam_passwdqc.so      pam_unix_auth.so
pam_ftp.so          pam_permit.so        pam_unix_passwd.so
pam_group.so        pam_pwcheck.so       pam_unix_session.so
pam_homecheck.so    pam_resmgr.so        pam_unix.so
pam_issue.so        pam_rhosts_auth.so   pam_userdb.so
pam_lastlog.so      pam_rootok.so        pam_userpass.so
pam_ldap.so         pam_rpasswd.so       pam_warn.so
pam_limits.so       pam_securetty.so     pam_wheel.so
pam_listfile.so     pam_selinux.so       pam_xauth.so
```

Einige Module verfügen über eigene Konfigurationsdateien, die ihr generelles Verhalten unabhängig von der aufrufenden Applikation steuern. Diese finden Sie im Verzeichnis `/etc/security`. Für die Konfiguration der PAM-Bibliotheken zu den einzelnen Diensten gibt es eine eigene Konfigurationsdatei unterhalb von `/etc/pam.d`.

```
chage   cups   passwd   samba   su       xdm      xscreensaver
chfn    login  ppp      shadow  sudo     xdm-np
chsh    other  rpasswd  sshd    useradd  xlock
```

Die Menge der Dateien in diesem Verzeichnis leitet sich aus der Zahl der PAM-fähigen Dienste ab, die Sie auf dem PC installiert haben. Für die meisten Dienste gibt es eine eigene Konfigurationsdatei, damit Login feststellen kann, ob sich der Systemadministrator von einem sicheren Terminal aus anmeldet. Bei der Benutzung von SSH ist dies nicht sinnvoll, zumal in der SSH-Konfiguration festgelegt wird, ob sich `root` überhaupt auf diesem Wege einloggen darf.

Beim Start legt jedes Programm in einer meist gleichnamigen Konfigurationsdatei seine Parameter fest, z. B. `xdm`. Leider stimmt das nicht immer, sodass es Netzwerkdienste gibt, bei denen das abschließende '`d`' fehlt, wie bei `ppp` oder die abweichend bezeichnet sind, wie `samba`. Falls PAM keine passende Konfigurationsdatei findet, verwendet es die Datei `/etc/pam.d/other`. Wenn man nicht genau weiß, welcher Dienst diese Datei benutzt, sollte man sie wie im folgenden Beispiel möglichst restriktiv einstellen.

Generell sind alle Konfigurationsdateien einheitlich strukturiert.

```
#modultyp   modulsteuerung  modulpfad       argumente
auth        sufficient      pam_unix2.so    nullok
auth        required        pam_ldap.so     use_first_pass
account     required        pam_unix2.so
password    required        pam_unix2.so
session     required        pam_unix2.so
session     required        pam_env.so
session     required        pam_devperm.so
```

Der *modultyp* legt die Management-Funktion eines Eintrags fest. Es gibt vier Modultypen:

- *auth* – Module in dieser Kategorie dienen der Benutzeridentifizierung durch klassische Abfragen von Benutzernamen/Passwort durch biometrische Verfahren, Smartcard mit PIN oder Ähnliches. Voraussetzung sind Schnittstellen der angeschlossenen Geräte, wie Smartcard-Leser. In diesen Bereich fallen auch spezielle Module, die Benutzerkennung und Passwort abgreifen, um sie für einen authentifizierten Mount-Prozess des Home-Verzeichnisses z. B. von einem Samba-Server einzusetzen, oder damit ein AFS-Token zu holen. Das Andrew Filesystem (*AFS*) setzt Kerberos zur Benutzerauthentifizierung ein. Einige Institutionen verwenden dieses ursprünglich von IBM entwickelte Dateisystem für die Benutzer-Home-Verzeichnisse.
- *account* – Diese Module verwalten den Zugriff auf Accounts nach der Anmeldeprozedur, um den Zugriff auf einen Dienst abhängig von der Uhrzeit oder dem Wochentag zu steuern.
- *password* – Diese Module steuern das Aktualisieren von Passwörtern oder Tokens. Verwendet das `passwd`-Kommando die PAM-Bibliotheken, lässt sich festlegen, welche Passwörter das Programm ändert und akzeptiert. Gleichzeitig können Sie dadurch ein Passwort netzwerktransparent ändern.
- *session* – Module diesen Typs verwalten Einstellungen für die Sitzung des Benutzers. Hiermit kann man die im System verbrachte Zeit abrechnen. Ebenso fällt in diese Kategorie das Setzen von Limits oder Zugriffsberechtigungen auf Unix-Devices sowie das Mounten von Verzeichnissen. Benötigen Sie für Letzteres ein Passwort, sollte dieser Vorgang im *auth*-Modul erfolgen. Das wäre bei Heimatverzeichnissen von einem Samba-Server der Fall.

In der Spalte *modulsteuerung* legen Sie fest, wie PAM auf Erfolgs- oder Fehlermeldungen der einzelnen Module reagiert. Die Standardbedingungen kann man bei Bedarf verfeinert aufgliedern. Um PAM-Module aufeinander zu stapeln. Diese *stacking* genannten PAM-Stapel arbeitet es in Reihenfolge ihrer Auflistung ab. Unter bestimmten Bedingungen können weiter unten stehende Module nicht erreicht werden. Das aufrufende Programm erfährt von diesem Vorgang der Abarbeitung das zusammengefasste Endergebnis als Statusbericht über Erfolg *(success)* oder Misserfolg *(fail)*.

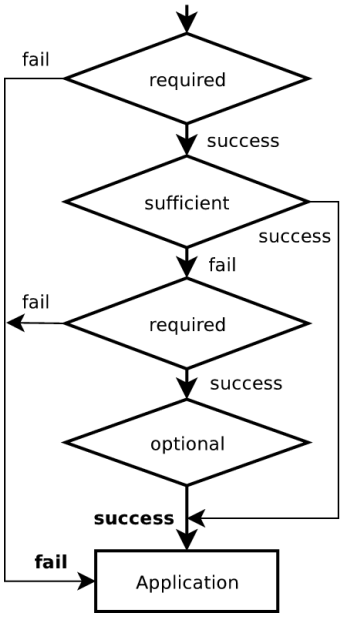

Abbildung 3.25: Die Funktion der Modulsteuerung

Für den Gesamterfolg eines PAM-Stapels kommt es auf die Einzelergebnisse an. Diese können mit unterschiedlichen Auswirkungen in die Gesamtwertung eingehen.

- *required* – Dieses Moduls muss mit dem Status *success* beendet werden, damit das zusammengefasste Ergebnis aller Module dieses Typs erfolgreich sein kann. Ein Misserfolg dieses Moduls zeigt sich erst, nachdem alle Module dieser Kategorie durchlaufen wurden.
- *requisite* – Verhält sich ähnlich wie *required*, gibt jedoch die Kontrolle sofort an die Anwendung zurück. Der Rückgabewert ist der des ersten fehlgeschlagenen Moduls mit *required*- oder *requisite*-Steuerung.
- *sufficient* – Liefert dieses Modul die Statusmeldung *success* zurück, genügt dieses für PAM zur positiven Gesamtmeldung, wenn nicht zuvor ein vorher eingetragenes Module mit *required* oder *requisite* fehlgeschlagen ist. Anschließend ruft PAM keine weiteren Module dieses Typs mehr auf. Das Ende der Prozedur wird zum Problem, wenn ein folgendes Modul mit dem User-Passwort ein Mount ausführen soll. Liefert ein Modul mit *sufficient*-Steuerung keine Erfolgsmeldung, ruft PAM die nachfolgenden Module auf. Der Misserfolg eines *sufficient*-Moduls bedeutet nicht das Fehlschlagen der Gesamtfunktion.
- *optional* – Bei diesem Modul entscheiden Erfolg oder Misserfolg nicht über den Gesamtrückgabewert. Ausnahmsweise geschieht dieses nur, wenn alle anderen Module im Stapel keinen definitiven Erfolg oder Misserfolg meldeten. Das Modul sollten Sie mit Vorsicht einsetzen, weil Sie Ihre Maschine unbedacht öffnen

oder komplett absperren könnten. Die Beispiele weiter unten demonstrieren diese Risiken.

Je nach Art des Programms oder Dienst ruft dieses bei Bedarf einen der vier Modul-Typen auf. Die PAM-Bibliothek geht nun alle Module, die in der Konfigurationsdatei zur dieser Kategorie vermerkt sind, nacheinander durch. Nach Erreichen des letzten Moduls oder dem vorzeitigen erfolgreichen Abbruch bei *sufficient* liefert sie den Gesamtstatus an die aufrufende Applikation zurück.

Der Modulpfad in der darauf folgenden Dateispalte legt fest, wo ein Modul installiert ist. Standardmäßig erwartet PAM seine Module in `/lib/security`. In diesem Fall reicht die Angabe des Modul-Namens. Andernfalls gilt wie sonst bei Unix Pfadnamen mit/beginnend werden als absolute Pfade interpretiert. Fehlt `/`, nimmt es einen Pfad relativ zu `/lib/security` an. So unterscheiden Sie selbst hinzugefügte Module von den üblicherweise installierten.

Die letzte Spalte *Argumente* ist optional und enthält nur bei einigen Modulen einen Eintrag. Argumente werden als Liste angegeben und dort durch Leerzeichen getrennt. Es gibt einfache Flags, wie *nullok* oder *use_first_pass* und Zuweisungen, z. B. *strict=false*. Es gibt von fast allen Modulen verstandene Argumente: *debug* liefert Diagnosemeldungen an den Systemlog-Dienst, *no_warn* unterdrückt diese. Authentifizierungs- und Passwortmodule kennen darüber hinaus *use_first_pass*. Sie versuchen dann, das Passwort des vorhergehenden *auth*-Moduls zu verwenden. Schlägt es fehl, meldet das Modul den Status *fail* zurück. Ähnlich wirkt für Authentifizierungsmodule *try_first_pass*. Das Modul versucht dann, das Passwort des vorhergehenden Moduls zu verwenden. Wenn dies fehlschlägt, fordert es Benutzer auf, ihr Passwort erneut einzugeben.

Inzwischen gibt es für PAM fast alle erdenklichen Module. Ein großer Teil ist bereits im Standard-RPM dabei. Spezifische Module wie für die LDAP-Authentifizierung (*pam_ldap*) installieren Sie bei Bedarf zusätzlich. Das haben Sie vermutlich bereits zusammen mit der OpenLDAP-Installation erledigt.

Die nachstehende Datei `/etc/pam.d/xdm` zeigt ein typisches Beispiel einer PAM-Konfiguration mit drei hintereinander geschalteten Authentifizierungsmodulen:

- Das erste Modul überprüft, wenn die UserID ungleich Null ist, ob eine Datei `/etc/nologin` existiert. Es unterbindet in diesem Fall eine weitere Anmeldung, da das Fehlschlagen eines *required*-Moduls zum Gesamtergebnis *fail* führt.
- Mit der nächsten Zeile versucht PAM, sich anmeldende Benutzer gegen die Standard-Unix-Dateien zu authentifizieren. Gelingt dieses, arbeitet es keine weiteren Module mehr ab.
- Schlägt dieser Schritt fehl, verwendet es das nächste Modul im Stapel.

Klappt die Anmeldung des Benutzers gegen den LDAP-Server, ist der Rückmeldewert *success*.

```
#%PAM-1.0
auth     required       pam_nologin.so
auth     sufficient     pam_unix2.so
auth     required       pam_ldap.so     use_first_pass
account  required       pam_unix2.so
password required       pam_unix2.so    #strict=false
session  required       pam_unix2.so    debug # trace or none
session  required       pam_devperm.so
session  required       pam_resmgr.so
```

Diese Konfiguration eignet sich für Umgebungen, in denen es bis auf den Administrator keine lokal eingetragenen Benutzer gibt. Zuerst schaut PAM, ob eine Authentifizierung gegenüber den klassischen Unix-Dateien Erfolg hat. Dieses trifft nur bei `root` ein. Da der Root-Benutzer nicht im LDAP gespeichert ist und kein zentrales Home-Verzeichnis hat, darf er auch nicht mehr bei den auf `pam_unix2` folgenden Modulen vorbeikommen. Das ist durch *sufficient* unterbunden.

`pam_unix2` ist zusätzlich als Account-, Passwortänderungs- und Session-Modul eingesetzt. Die Accounting-Funktion dieses Moduls prüft anhand der Felder in der Shadow-Datei, ob der Account noch gültig ist. Ebenfalls testet es, ob das Passwort abgelaufen ist. In diesem Fall kann es die Authentifizierung verschieben, bis der Benutzer sein Passwort aktualisiert hat. Es kann ebenfalls eine Warnung an den Benutzer ausgeben, dass er sein Passwort ändern sollte. Als Session-Modul zeichnet es einfach nur den Benutzernamen und den Diensttyp über den Syslog-Dienst auf. Das Modul `pam_env.so` setzt Umgebungsvariablen, die in `/etc/security/pam_env.conf` stehen. `pam_mail.so` ist als *optional* eingetragen, darf also ohne Konsequenzen fehlschlagen. Es teilt lediglich Benutzern mit, ob neue Mail für sie vorliegt. Da dieses jedoch nur für lokal erreichbare Mailfolder klappt, ist dieses Modul eher selten einsetzbar.

Bei fehlkonfiguriertem PAM können sich Benutzer möglicherweise auch ohne ausreichende Authentifizierung anmelden. Das demonstriert das folgende Beispiel:

```
auth     required   pam_nologin.so
auth     optional   pam_unix2.so     set_secrpc
auth     optional   pam_ldap.so      use_first_pass
[ ... ]
```

Drei Module sind hintereinander geschaltet: Das erste Modul testet auf die Existenz der `/etc/nologin`. Gibt es diese Datei nicht, liefert es den Status *success*. Selbst wenn nun alle drei folgenden Module fehlschlagen, meldet PAM als Gesamtergebnis *success*. So könnte ein Benutzer auch mit falschem Passwort ins System gelangen. Wenn Sie es noch einfacher haben wollen, setzen Sie auf *pam_permit*. Dieses garantiert den Erfolg der Anmeldung, wenn Sie irgendeinen existierenden Benutzer beim Login angegeben haben.

Umgekehrt können Sie durch eine Fehlkonfiguration Ihre Maschine für jegliches Login (auch `root`) sperren:

```
auth     required   pam_nologin.so
auth     required   pam_unix2.so     set_secrpc
auth     required   pam_ldap.so      use_first_pass
```

Die Kontrolleinstellung *required* sorgt dafür, dass ein Benutzer sowohl in den Unix-Dateien `passwd` und `shadow` als auch im LDAP bekannt sein muss. In verteilten Authentifizierungsarchitekturen liegt dieses oft nicht vor: Der Systemadministrator ist immer nur lokal eingetragen, normale Benutzer sinnvollerweise nie. Die Aussperrung von der Maschine ist perfekt. Deshalb veranstalten Sie solche Tests am besten auf einem unkritischen Dienst (z. B. xdm). Anschließend übertragen Sie die erfolgreich getestete Kombination auf die gewünschten anderen. Dabei müssen Sie nicht für alle Dienste eine einheitliche Einstellung haben: Vielleicht dürfen sich Benutzer an Ihrem Server nur per SSH anmelden aber nicht per FTP. Dann tragen Sie das LDAP-Moduls nur in der `/etc/pam.d/sshd` ein.

Wenn Sie PAM für Netzwerkdienste verwenden, wie für die FTP-Authentifizierung, sollten Sie beachten, dass PAM selbst die Übertragung von Passwörtern nicht schützen kann. Dieses ist immer Aufgabe der Applikation selbst.

Für alle PAM-Dateien und -Verzeichnisse dürfen nur Systemadministratoren Schreibrechte haben. Nur sie dürfen die Verzeichnisse `/lib/security`, `/etc/security` und `/etc/pam.d` und die darin befindlichen Dateien besitzen. Außerdem sollte man keine PAM-Module verwenden, die von Benutzern schreibbare Programmbibliotheken verwenden, da dies Angreifern erleichtert, an verschiedenen Stellen vom PAM ihre Schwachstellen zu finden. Weiter sollte man ein Fallback für unkonfigurierte Dienste definieren.

```
auth      required       pam_warn.so
auth      required       pam_unix2.so
account   required       pam_warn.so
account   required       pam_unix2.so
password  required       pam_warn.so
password  required       pam_cracklib.so
password  required       pam_unix2.so      use_first_pass
session   required       pam_warn.so
session   required       pam_unix2.so
```

3.5.6 Weitere Einsatzgebiete der LDAP-Datenbank

Mit einer LDAP-Datenbank können Sie die Benutzer nicht nur besser und sicherer verwalten, sondern ihnen auch weitere Daten wie (E-Mail-)Adressbücher zuordnen. Deshalb zeigt dieser Abschnitt, wie Sie Ihr KDE- und Windows-Adressbuch so einrichten, dass diese den frisch aufgesetzten LDAP-Server als Quelle benutzen.

Das KDE-Adressbuch (Kommando `kaddressbook` oder über die Startleiste von KDE) ist eine mächtige Applikation zum Verwalten von Kontaktdaten. Damit Ihre Benutzer auf in LDAP gespeicherten Daten zugreifen können, müssen Sie diese als Datenquelle angeben.

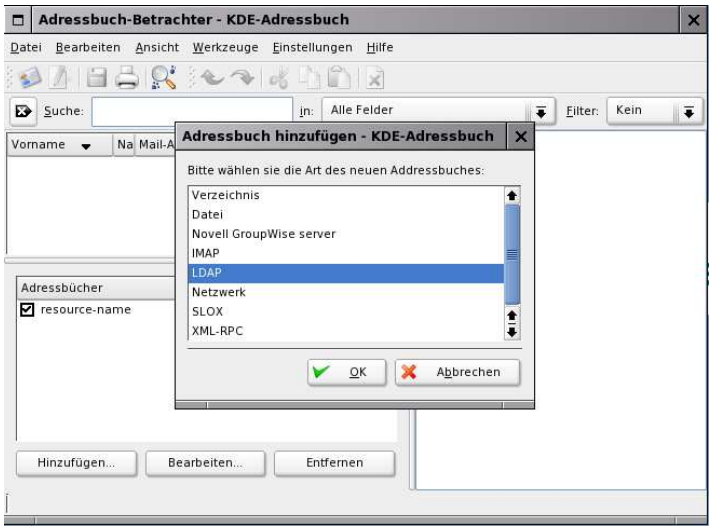

Abbildung 3.26: Die KDE-Kontaktdatenverwaltung – Aufnahme einer neuen Datenquelle

1. Dazu klicken Sie links unten im Hauptfenster auf *Hinzufügen*. Das Adressbuch öffnet ein kleines Auswahlfenster (wie in Abbildung 3.26 gezeigt). Hier wählen Sie als Art des Adressbuchs *LDAP* aus. Das führt Sie zu einem weiteren Dialogfenster:

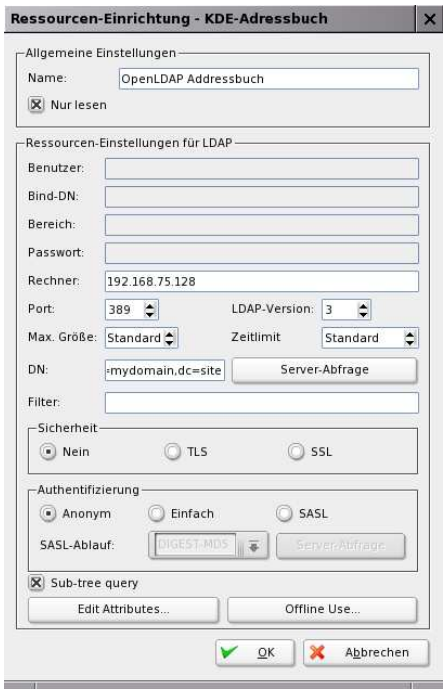

Abbildung 3.27: Einrichten der LDAP-Datenquelle im KDE-Adressbuch

2. Im Bereich *Allgemeine Einstellungen* legen Sie fest, unter welchem Namen die LDAP-Quelle im Hauptfenster der Adressbuch-Applikation erscheint. Für normale Benutzer genügt ein ausschließlich lesender Zugriff auf die Datenbank. Deshalb müssen Sie nur noch die IP-Adresse oder den Namen des Rechners ergänzen, auf dem Ihr LDAP-Server im Netz läuft. Den Port müssen Sie nur anpassen, wenn Sie einen vom Standard abweichenden gewählt haben. Den *DN* ermitteln Sie einfach durch einen Klick auf *Server-Abfrage*. Dann sehen Sie auch, ob das `kaddressbook` Ihren Server kontaktieren kann. Sicherheit und Authentifizierung müssen Sie nur dann anzupassen, wenn Sie mit verschlüsselten Verbindungen arbeiten.

3. Am Ende des Formulars klicken Sie auf den Button *Edit Attributes*:

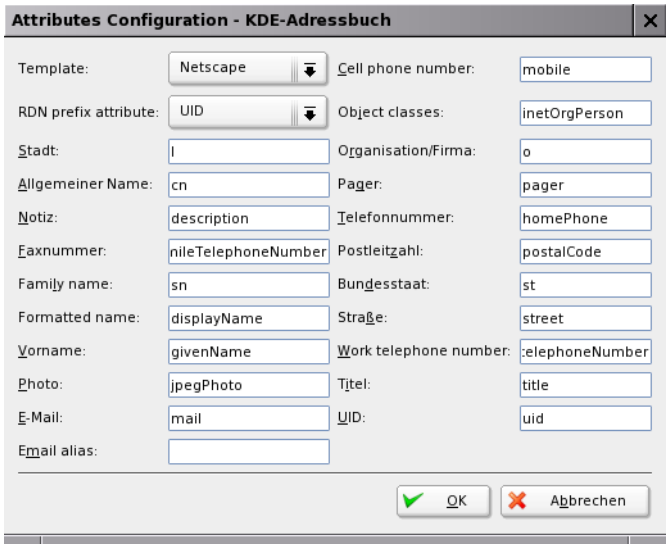

Abbildung 3.28: Anpassen des RDN für Ihre LDAP-Einstellungen

In diesem Formular schalten Sie das *RDN prefix attribute* von *CN* auf *UID* um. In Beispielen zum LDAP-Server wurde der Distinguished Name eines Eintrags mit der UserID (*UID*) und nicht dem Common Name (*CN*) gebildet. Anschließend können Sie im Hauptfenster des KDE-Adressbuches nach einem LDAP-Benutzer suchen.

Das Adressbuch von Windows XP ist eine recht einfache Anwendung. Sie genügt hier, um den Zugriff auf eine OpenLDAP-Datenquelle unter Windows zu zeigen.

1. Das Adressbuch finden Sie unter *Start* • *Alle Programme* • *Zubehör*. Im Adressbuch wählen Sie über das Menü *Extras* den Punkt *Konten...* aus. Dieser öffnet ein Dialogfeld für *Internetkonten*. Mit *Hinfügen* tragen Sie Ihren OpenLDAP-Server als Datenquelle ein:

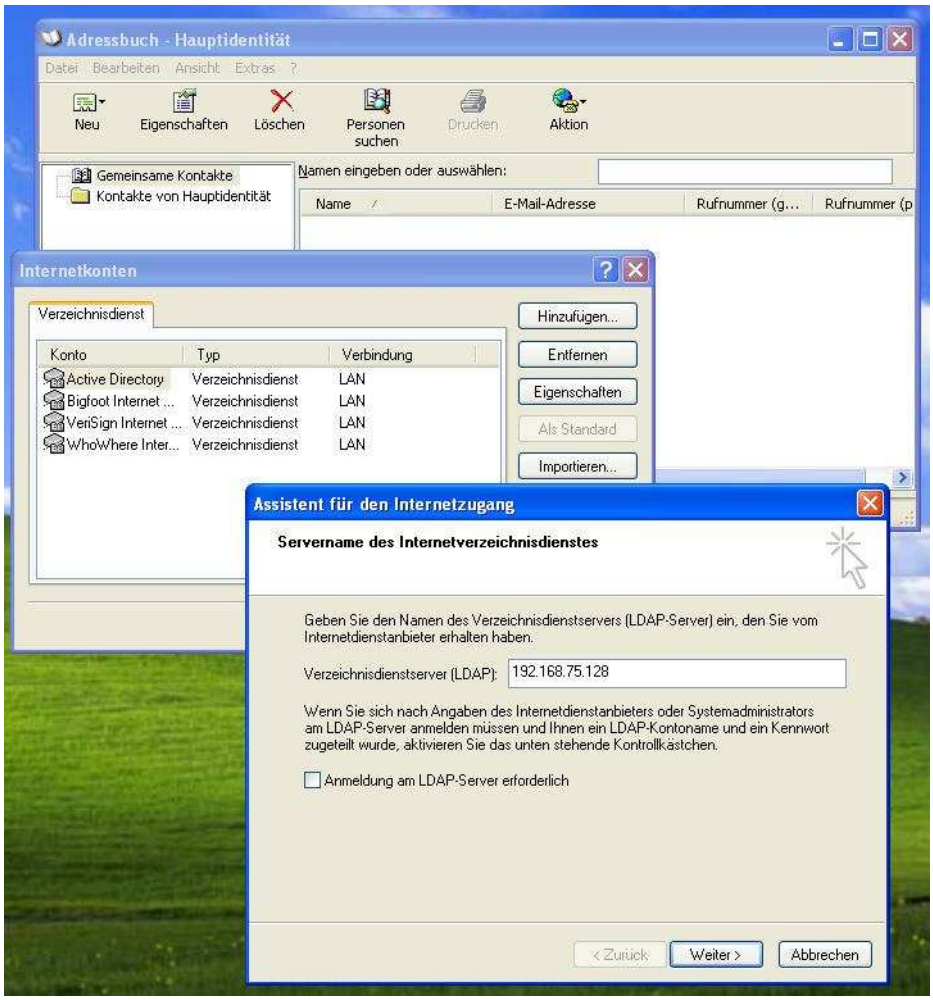

Abbildung 3.29: Eintragen einer OpenLDAP-Datenquelle im WindowsXP-*Adressbuch*

2. Sie beenden dann diesen Assistenten und markieren den neuen Eintrag in *Internetkonten*. Über den Button *Einstellungen* richten Sie in der Registerkarte *Erweitert* Parameter für die Suchbasis ein. In dieser Karte würden Sie die Verschlüsselung einschalten, wenn Sie einen Server mit Verschlüsselung aufgesetzt hätten.

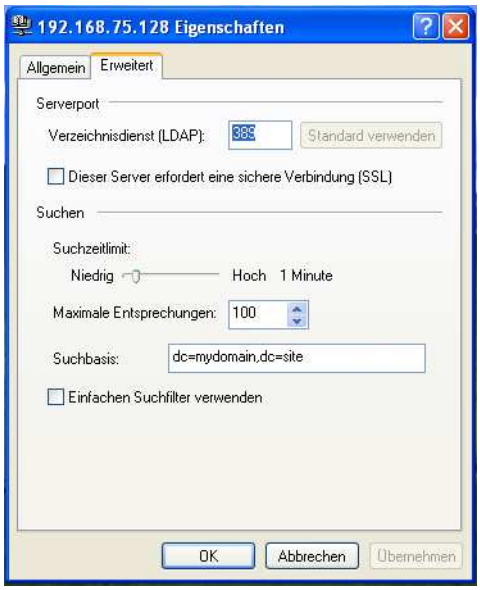

Abbildung 3.30: Eintragung der Suchbasis im *Eigenschaften*-Dialog

3. Nach Abschluss der Konfiguration können Sie einen Benutzer im LDAP suchen. Diesen Vorgang können Sie dann im Logfile `/var/log/messages` auf Ihrem Server nachvollziehen.

```
Dec 30 06:20:49 linux slapd[4482]: conn=17 fd=12 ACCEPT from
  ↵ IP=192.168.75.1:1039 (IP=192.168.75.128:389)
Dec 30 06:20:49 linux slapd[4482]: conn=17 op=0 BIND dn=""
  ↵ method=128
Dec 30 06:20:49 linux slapd[4482]: conn=17 op=0 RESULT tag=97
  ↵ err=0 text=
Dec 30 06:20:49 linux slapd[4482]: conn=17 op=1 SRCH base="
  ↵ dc=mydomain,dc=site"
scope=2 deref=3 filter="(mail=*dsuchod*)"
Dec 30 06:20:49 linux slapd[4482]: conn=17 op=1 SRCH attr=
display-name cn common Name mail otherMailbox givenName sn surname
st c co organizationName o ou organizationalUnitName URL homePhone
facsimileTelephoneNumber otherFacsimileTelephoneNumber OfficeFax
mobile otherPager OfficePager pager info title telephoneNumber l
homePostalAddress postalAddress streetAddress street department
comment postalCode physicalDeliveryOfficeName initials
conferenceInformation userCertificate;binary
userSMIMECertificate;binary labeledURI Manager Reports IPPhone
Dec 30 06:20:49 linux slapd[4482]: <= bdb_substring_candidates:
(mail) index_param failed (18)
```

```
Dec 30 06:20:49 linux slapd[4482]: conn=17 op=1 SEARCH RESULT
  ↵ tag=101 err=0 nentries=1 text=
Dec 30 06:20:50 linux slapd[4482]: conn=17 op=2 UNBIND
Dec 30 06:20:50 linux slapd[4482]: conn=17 fd=12 closed
```

Im Logfile sehen Sie die anfragende IP-Nummer des Windows-PCs (hier `192.168.75.1`). Die Verbindung erfolgte anonym – der *BIND dn* ist leer. Die Suchbasis entspricht dem Eintrag in den erweiterten Einstellungen. Der Filter sucht nach einem Eintrag im Mail-Attribut, der den String `alkalde` enthält.

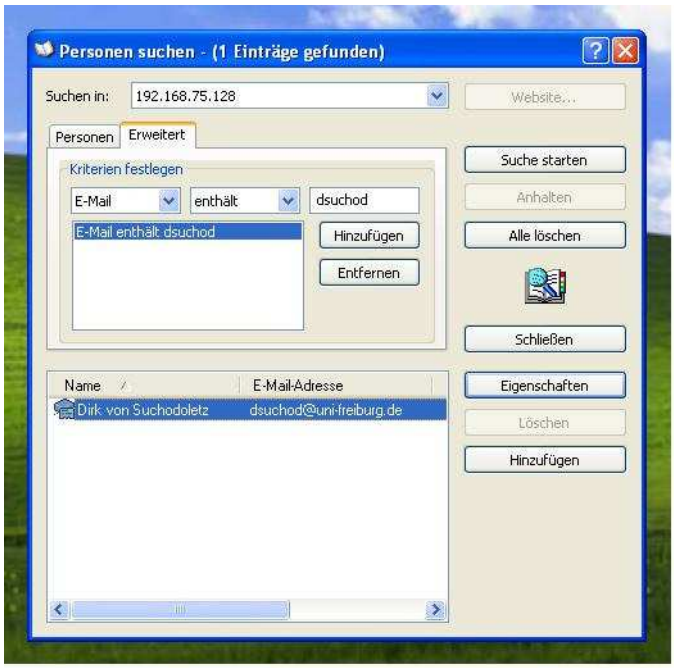

Abbildung 3.31: Erfolgreiche Suche nach einem Eintrag mit der Mail-Adresse *dsuchod*

Einige Programme können nicht direkt auf einen LDAP-Server zugreifen. Sie unterstützen jedoch häufig den Datenimport aus LDIF-Dateien. Wenn Sie eine User-Liste als LDIF speichern wollen, können Sie das beispielsweise mit

```
ldapsearch -x -b "ou=user,dc=mydomain,dc=site" > user.ldif
```

vornehmen. Das Beispiel schränkt die Suchbasis auf den Teil des LDAP-Baumes ein, in dem alle Benutzer eingetragen sind. Die Datei `user.ldif` können Sie anschließend in Adressbücher, Mozilla etc. importieren.