3 Benutzerverwaltung

Systemadministratoren verbringen viel Zeit mit dem Verwalten der Benutzer und Ihrer Konten.

Typische Arbeiten sind das

- Anlegen und Löschen von Benutzerkonten,
- Prüfen der Qualität von Passwörtern (siehe Kapitel 17),
- Ändern von Passwörtern, welche die Benutzer vergessen haben sowie
- Überwachen des von Nutzern belegten Speicherplatzes.

Wegen ihrer Überlastung brauchen Systembetreuer in vielen Organisationen mehrere Tage, bis sie neuen Mitarbeitern vollen System-Zugang 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 brauchen 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 fettem 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 im Kapitel 9 kennen lernen werden. Neu in dieser vierten Auflage ist der Abschnitt 3.5 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 gesamten Server-Festplatten füllen, wenn Sie für die Home-Verzeichnisse keine eigene Partition angelegt haben. Das kann dann die Funktionsfähigkeit des Linux-Systems erheblich einschränken. Liegen die Home-Verzeichnisse in eigenen Partitionen, so können Viel-Speicherer zumindest die Home-Partition so weit mit Daten füllen, dass dies die Arbeit aller anderen 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 zurecht: Sie können Quotas sowohl auf Dateisystemen mit ext2, ext3, als auch reiserfs einsetzen.

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 können Sie die 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 und machen keine Einschränkungen für die Zahl der Dateien.

Bei beiden Möglichkeiten können Sie zwei unterschiedliche Grenzen setzen:

- Ihre Hard-Limits können Benutzer auf keinen Fall überschreiten,
- ihre Soft-Limit 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 `CD2`.

Bevor Sie die Quotas konfigurieren können, müssen Sie noch ein bisschen nachinstallieren. Das Quota-System benötigt Unterstützung durch den Kernel. Diese Unterstützung hat SuSE zwar eingebaut, aber als Modul und genau dieses Modul müssen Sie noch laden lassen. Gehen Sie dazu im YaST-Kontrollzentrum auf *System • Editor für /etc/sysconfig-Dateien* und dort auf *System • Kernel* und erweitern 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, vor der eigentlichen Modulverwaltung. Hier finden Sie also die Module für bestimmte Festplattenhardware, z. B. *SCSI* und besondere Partitionstypen, z. B. *reiserfs*.

Ergänzen Sie die Zeile um die Angabe *quota_v2* und lassen zwischen den bisherigen Einträgen und Ihrer Eingabe bitte ein Leerzeichen. Abschließend müssen Sie noch die *Initrd*-Datei neu erzeugen lassen, welche die Module für den Systemstart enthält.

```
mk_initrd
```

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

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 mit modprobe per Hand 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, welche 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.

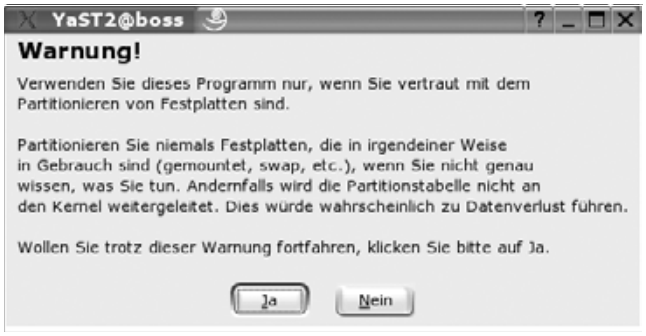

Abbildung 3.3: Partitionieren • Warnung

Wenn Sie sicher sind, dass Sie die Veränderungen durchführen wollen, dann klicken Sie auf *Ja*. Es erscheint 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.

Abbildung 3.4: Partitionieren • Home-Partition

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

Abbildung 3.5: Partitionieren • Optionen

Entscheidend ist hier das Feld *Beliebiger Optionswert*. In diesem Feld finden Sie zunächst nur den Eintrag *defaults*. Bitte ergänzen Sie diesen Wert zu

```
defaults,usrquota,grpquota
```

Damit aktivieren Sie für diese Partition sowohl Userquota, als auch Gruppenquota.

Tipp: Bei der Aufzählung `defaults,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`.

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

```
/dev/hda5  swap          swap      pri=42              0   0
/dev/hda6  /             ext2      defaults            1   1
/dev/hda7  /tmp          ext2      defaults            1   2
/dev/hda8  /var          ext2      defaults            1   2
/dev/hda2  /boot         ext2      defaults            1   2
/dev/hda9  /home         ext2      defaults            1   2

devpts     /dev/pts      devpts    mode=0620,gid=5     0   0
proc       /proc         proc      defaults            0   0
usbdevfs   /proc/bus/usb usbdevfs  noauto              0   0
/dev/cdrom /media/cdrom  auto      ro,noauto,user,exec 0   0
/dev/fd0   /media/floppy auto      noauto,user,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/hda5  swap          swap      pri=42              0   0
/dev/hda6  /             ext2      defaults            1   1
/dev/hda7  /tmp          ext2      defaults            1   2
/dev/hda8  /var          ext2      defaults            1   2
/dev/hda2  /boot         ext2      defaults            1   2
/dev/hda9  /home         ext2      defaults,usrquota,grpquota
                                                   ↵ 1   2

devpts     /dev/pts      devpts    mode=0620,gid=5     0   0
```

```
proc       /proc         proc      defaults            0   0
usbdevfs   /proc/bus/usb usbdevfs  noauto              0   0
/dev/cdrom /media/cdrom  auto      ro,noauto,user,exec 0   0
/dev/fd0   /media/floppy auto      noauto,user,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-Betriebs 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.

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. Dazu starten Sie das YaST-Kontrollzentrum, gehen dort in das Menü *System* • *Runlevel-Editor* • *Runlevel -Eigenschaften* und aktivieren hier den Dienst *quota* für die Runlevel 3 und 5, indem Sie den Leuchtbalken auf die Zeile mit *quota* bringen und dann die mit *3* bzw. *5* beschrifteten Kästchen anklicken. Anschließend können Sie den Dienst auch gleich starten, klicken Sie dazu auf *Starten/Anhalten/Aktualisieren* und wählen dann *Starten*. Anschließend ist der Dienst aktiv.

Sie sollten anschließend auch gleich den Dienst *quotad* für die Runlevel 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.

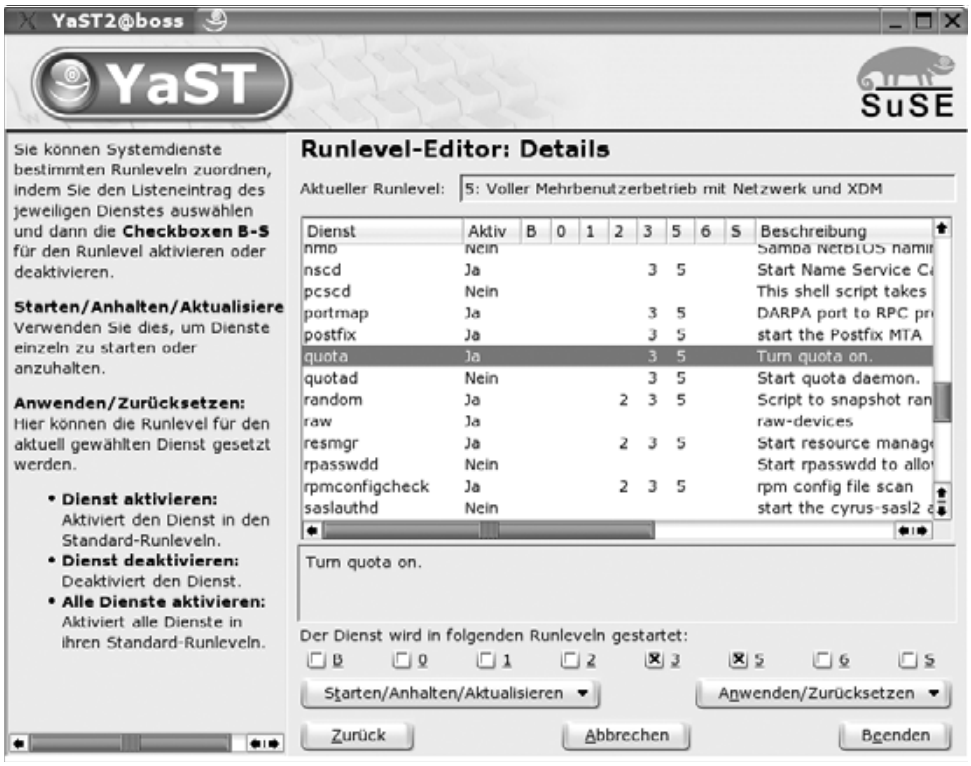

Abbildung 3.6: Runlevel-Editor QUOTA

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 500):
  Filesystem    blocks     soft     hard     inodes     soft
  /dev/hda9     3812       0        0        447        0
```

Der Benutzer belegt 3812 KByte Speicherplatz auf dem System mit 447 Dateien. Verändern Sie die Einstellungen zu

```
Disk quotas for user debacher (uid 500):
  Filesystem    blocks     soft     hard     inodes     soft
  /dev/hda9     3812       4000     5000     447        0
```

Damit erlauben Sie dem Benutzer, maximal 5000 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 4000) 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 500):
Filesystem blocks quota limit   grace   files   quota   limit
↵ grace
/dev/hda3    3812  4000  5000              447       0       0
```

Der Benutzer belegt momentan mit 447 Dateien 3812 KByte Speicherplatz. Er darf beliebig viele Dateien anlegen, aber maximal 5000 KBytes 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, welches 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:

```
ide0(3,9): warning, user block quota exceeded.
ide0(3,9): write failed, user block limit reached.

dd: Schreiben in »/home/debacher/test«:
↵ Der zugewiesene Plattenplatz (Quota) ist überschritten
2369+0 Records ein
2368+0 Records aus
```

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

```
Disk quotas for user debacher (uid 500):
Filesystem  blocks   quota   limit   grace   files quota limit
↵ grace
/dev/hda3    5000*    4000    5000   6days     448     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. Daher müssen Systemverwalter die Userquotas für jeden Benutzer einzeln festlegen oder mit dem Befehl `edquota vervielfältigen`.

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

```
edquota  -p  debacher  schultz
```

3.4 Die Linuxbu.ch/Tools

Die Linuxbu.ch/Tools sind eine Sammlung von Administrations-Programmen 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 Windowsrechner für Administrationszwecke unbedingt die Gruppe ntadmin.

Die Tools bieten momentan folgende Funktionen:

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

Die Linuxbu.ch/Tools kann man einfach erweitern und anpassen. Sie ändern an keiner Stelle die Konfiguration Ihres Rechners oder der Software. Sie brauchen lediglich den Webservers Apache so zu konfigurieren, dass er die Programme aus dem Verzeichnis `/srv/www/htdocs/tools` ausführt.

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

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.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.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.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 24: gcc: command not found
```

bekommen, dann ist auf Ihrem Rechner der C-Compiler *ggc* nicht vorhanden. 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 Selektions-Gruppe aktivieren. Sie finden die notwendigen Pakete übrigens auf *CD1* der Professional Version aber nicht 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 sie in die Konfiguration des Webservers 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
# bei SuSE 8.2 einfach über YaST
# den vollen Pfad zu dieser Datei in die sysconfig
# aufnehmen:
#
# HTTPD_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/httpd/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* • *Apache* für die Variable *HTTPD_CONF_INCLUDE_FILES* den Wert */srv/www/htdocs/tools/httpd.conf.erg* angeben und damit die Erweiterung in die Konfiguration des Webservers einbinden.

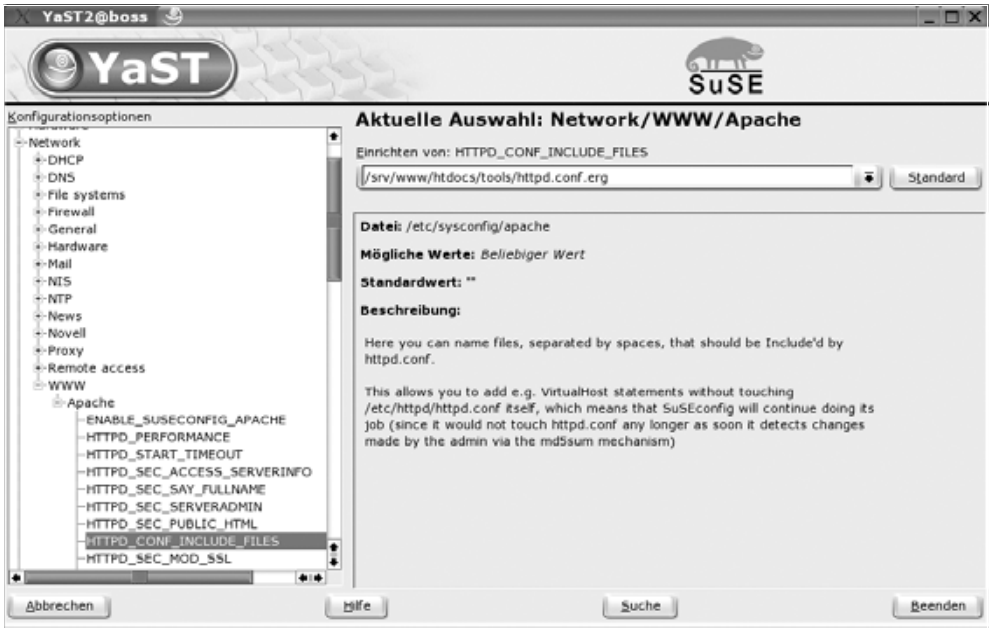

Abbildung 3.7: Eigene Konfigurationsdatei einbinden

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

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-Account und Tools-Gruppen

Für die Nutzung der Tools müssen Sie die zwei Gruppen

- leiter
- mitarbeiter

anlegen und mindestens einen Administratoren-Account einrichten.

Um die Verwaltungs-Funktionen 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
```

Abbildung 3.8: YaST: Hinzufügen zur Gruppenverwaltung

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

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).

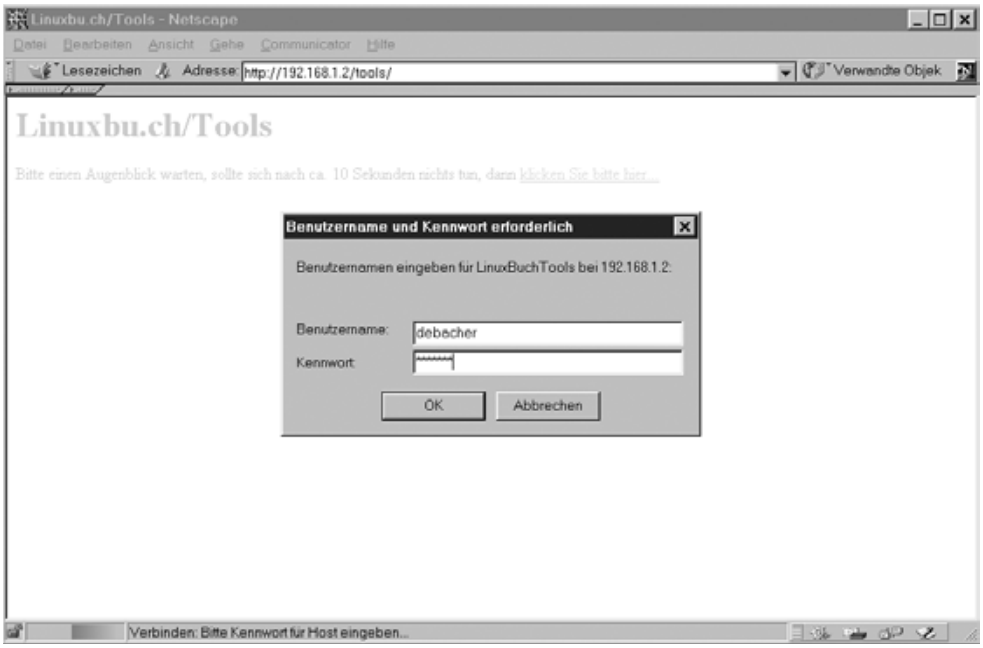

Abbildung 3.9: Tools: Anmeldung

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

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

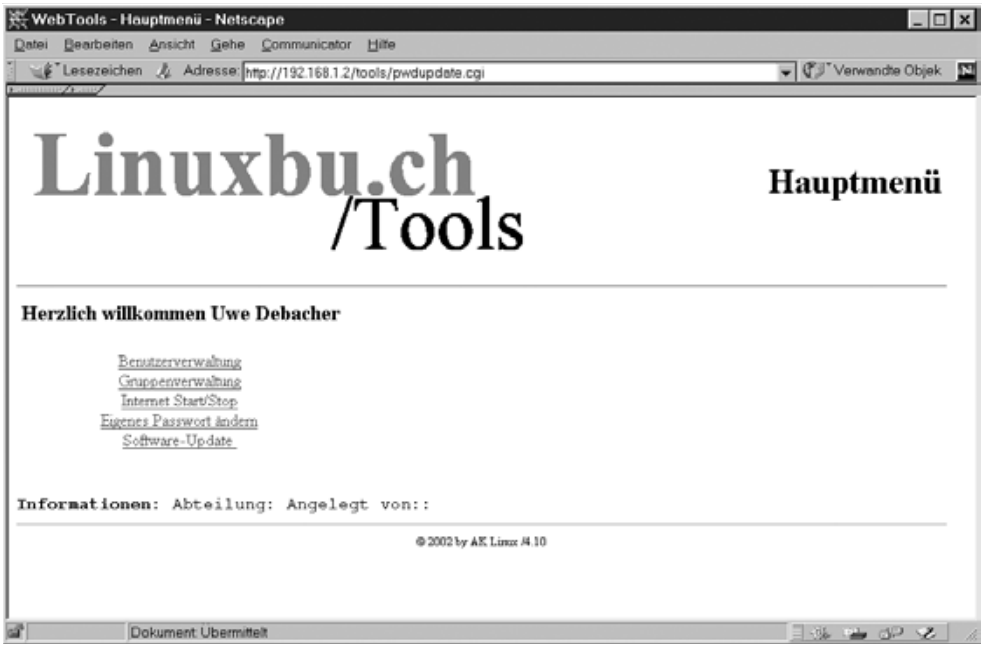

Abbildung 3.10: Tools: Hauptmenü

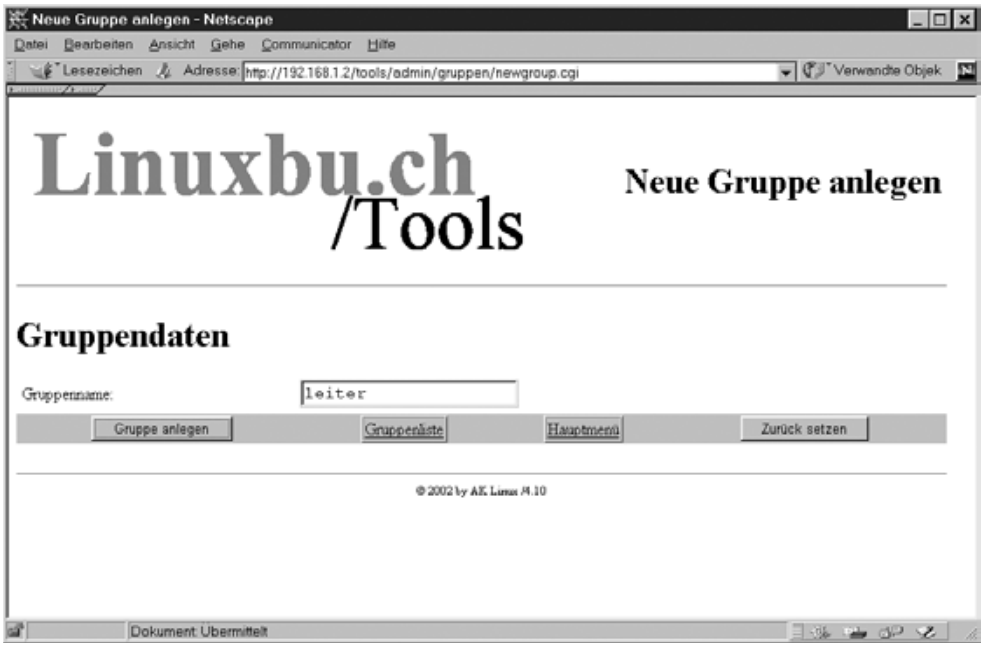

Abbildung 3.11: Tools: Neue Gruppe anlegen

Nach dem Anlegen dieser beiden Gruppen sollte die Gruppenliste folgendermaßen aussehen:

Abbildung 3.12: Tools: Gruppenliste

Abschließend sollten Sie die Angaben für Ihren eigenen Account vervollständigen. Gehen Sie dazu auf *Benutzerverwaltung*, dort auf *Benutzerliste*, und klicken Sie dort Ihren Benutzer-Account an.

Abbildung 3.13: Tools: Daten ändern

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.

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 selber eingerichtet haben.

Legen Sie zuerst die Abteilungsleiter an, im Beispiel den *Klaus Sparsam*. Gehen Sie dazu auf *Benutzerverwaltung* • *Benutzer anlegen* und füllen 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 Anfangs-Passwort 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.

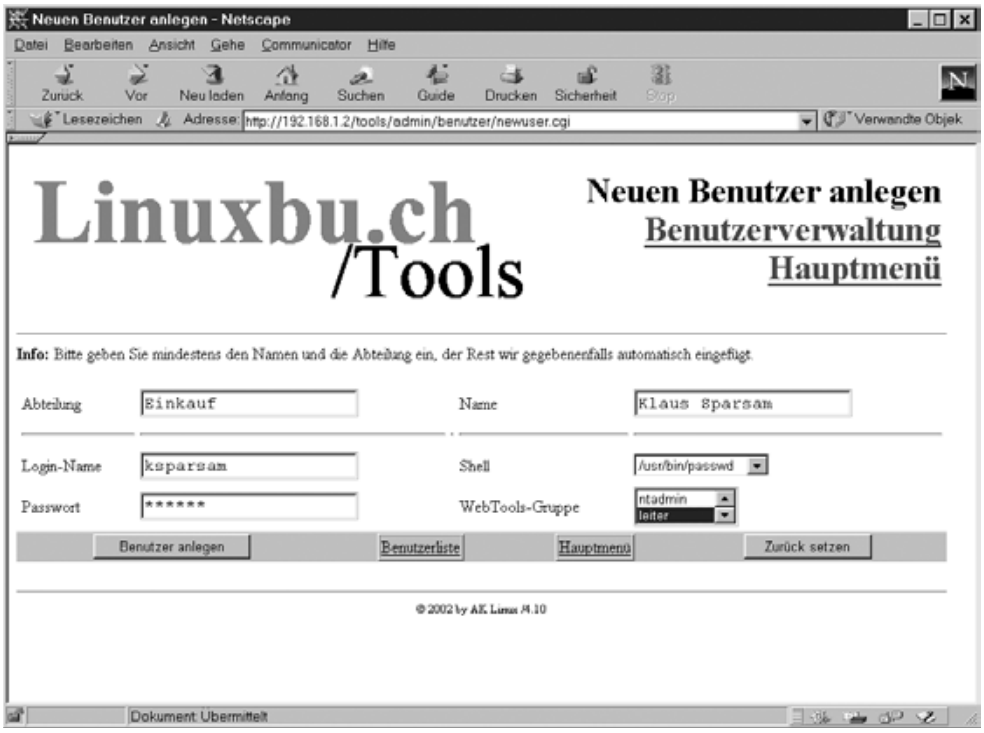

Abbildung 3.15: Tools: Benutzer anlegen, hier Abteilungsleiter

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 diesen Account den Tools 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-Unterstützung 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
# die Tools Benutzerdaten anzeigen
# werden. Wenn man das Verändern/Löschen
# des root-Account verhindern möchte,
# sollte man diesen Wert entsprechend hoch setzen.
$FIRST_CH_UID = 500;
# $LAST_CH_UID gibt die letzte UID an,
# nach der Benutzer nicht mehr
# angezeigt werden.
$LAST_CH_UID = 10000;

# $FIRST_NEW_UID gibt die erste UID an,
# die für neue Benutzer vergeben wird.
$FIRST_NEW_UID = 500;

# $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 ver-
# aendert werden duerfen,
# oder Gruppendaten fuer Benutzer verwendet werden
# duerfen.
$LAST_CH_GID = 10000;
# $NEWUSER_SHELL gibt an, welche Shell ein
# Neuer Benutzer als Voreinstellung bekommt.
$NEWUSER_SHELL = "/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, über welches Gerät die Internetverbindung
# läuft
$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 =j a
9. Zeile: frei
10. Zeile: Hilfetext (spätere Erweiterung)

Entscheidend für die Rechtevergabe 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 T-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 Gerät die Internetverbindung
# läuft
$INTERFACE="ippp0";
```

Die Tools benutzen für die Steuerung der Internetverbindung das Programm *cinternet*, welches Sie im Kapitel 12 kennenlernen 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 mehr als einen Linux-PC im Netz betreiben, werden sie nicht alle Administrationsaufgaben der Benutzerverwaltung auf allen Rechnern wiederholen wollen. Das noch vor Jahren populäre Network Information System (*NIS*), (Yellow Pages) entspricht jedoch 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, welche einen umfangreichen Verzeichnisdienst definiert, stammt das Lightweight Directory Access Protocol (*LDAP*) ab. "Directory" bezeichnet im englischen Sprachgebrauch "Verzeichnis", also so etwas wie ein Telefonbuch, ein Katalog oder ein Gewerberegister. Da LDAP lese-optimiert ist, eignet es sich besonders für Aufgaben wie das Authentifizieren von Benutzern, bei denen Abfragen überwiegen.

3.5.1 Kurzeinführung in LDAP

Wie der Name des Protokolls schon sagt, legt LDAP seine Daten hierarchisch in einem Verzeichnis ab. Es gibt immer nur eine einzige Wurzel "root" eines Directories, die sich weder verschieben noch verändern lässt. Sogenannte »Domain Components« stellen sicher, dass die Elemente jeder Hierarchieebene eindeutig sind. Die Wurzel bezeichnet man beginnend mit der Toplevel-Domain einer Site; in den darunterliegenden Hierarchien folgen Second-Level-Domain- und falls erforderlich Sublevel-Domain-Namen.

Jedes Objekt im Verzeichnis muss einen eindeutigen Namen, den "Distinguished Name" 'dn' haben. Der 'dn' setzt sich aus den distinguished names 'dn' von der Wurzel aus zusammen. Einträge in einem Objekt heißen Attribute. Der Common Name ist ein »allgemeiner Bezeichner«, ein für Menschen gut lesbares und merkbares Attribut, ähnlich einem Rechnernamen. Auf der höchsten Ebene ist dieses Attribut häufig Bestandteil des 'dn'.

Wenn der Common Name den Realnamen einer Person oder Dienstes bezeichnet, benötigt ein Linux-System für eine einfache Benutzerverwaltung noch eine eindeutige Zeichenfolge (User-ID), eine eindeutige Benutzer- und Gruppennummer, ein Home-Verzeichnis, eine Loginshell und eventuell ein Passwort.

Soll die Datenbank auch die Einheitlichkeit der Adressbücher der Mitarbeiter sicherstellen, sollte man außerdem Kontakt-Daten wie Telefonnummer, eMail-Adresse und persönliche Webseite speichern.

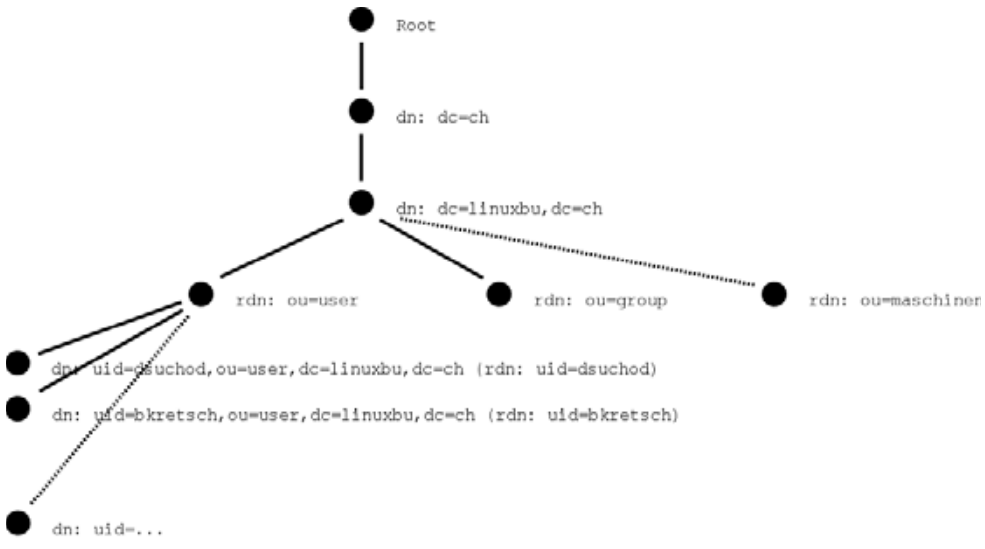

Abbildung 3.17: LDAP-Baumstruktur

LDAP arbeitet objektorientiert. Jeder Directory-Eintrag beschreibt ein Objekt, welches eine Person, eine Verwaltungseinheit oder auch ein Server, ein Drucker usw. sein kann. Jeder Eintrag hat einen ausgezeichneten bzw. herausgestellten Namen, den 'distinguished name'. Jeder Eintrag kann weitere Attribute besitzen, die einen Typ und einen bzw. mehrere Werte haben.

Für viele Standarddaten sind Klassen definiert. Diese können voneinander erben. So ist die üblicherweise für Personendaten verwendete Klasse »InetOrgPerson« von »OrganizationalPerson« und diese wieder von »Person« abgeleitet. Zu einer Person ("person") gehören zwingend (sogenannte MUST-Attribute) objectClass (die Objektklasse selbst), sn (der Nachname) und cn (commonName, etwa: üblicher Name, hier wird üblicherweise Vor- und Nachname verwendet). Zusätzlich gibt es optionale Attribute (mit MAY gekennzeichnet), die man nicht unbedingt angeben muss, wie description (beliebige Beschreibung), seeAlso (verweist auf ein anderes Objekt), telephoneNumber (Telefonnummer), userPassword (ein Passwort). Da mit einer Person häufig noch weitere Eigenschaften verknüpft sind, gibt es die abgeleitete Objektklasse organizationalPerson. Diese erbt die Eigenschaften von »person« und definiert darüberhinaus optionale Eigenschaften, wie Felder der Adresse oder eine Fax-Nummer. »InetOrgPerson« ist die um wichtige Internetattribute, wie Mail, URL und Zertifikate erweiterte OrganisationalPerson.

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

Ein naheliegendes System wäre, auf einer Hierarchieebene verschiedene Unterbäume für einzelne Abteilungen anzulegen und diesen Abteilungen ihre jeweiligen Benutzer zuzuordnen.

Viele Administratoren ordnen alle Mitarbeiter in einem einzigen Baum an und vermerken die Abteilungszugehörigkeit eines Mitarbeiters in einem geeigneten Attribut. Wechseln Mitarbeiter ihre Abteilung, lässt sich die Datenbank bei diesem Modell leichter aktualisieren.

Die Designentscheidung hat später Einfluss auf Suchfilter für die LDAP-Client-Konfiguration.

3.5.2 Linux-LDAP Server und Client

Aus der großen Auswahl von LDAP-Produkten stellt dieses Kapitel die Version 2.1.X von OpenLDAP vor, die unter der GPL frei verfügbar ist. Um LDAP zur Benutzerverwaltung zu verwenden, muss man etliche Pakete installieren.

Mindestens erforderlich sind folgende RPMs

- openldap2
- openldap2-client
- nss_ldap
- pam_ldap
- yast2_ldap_client

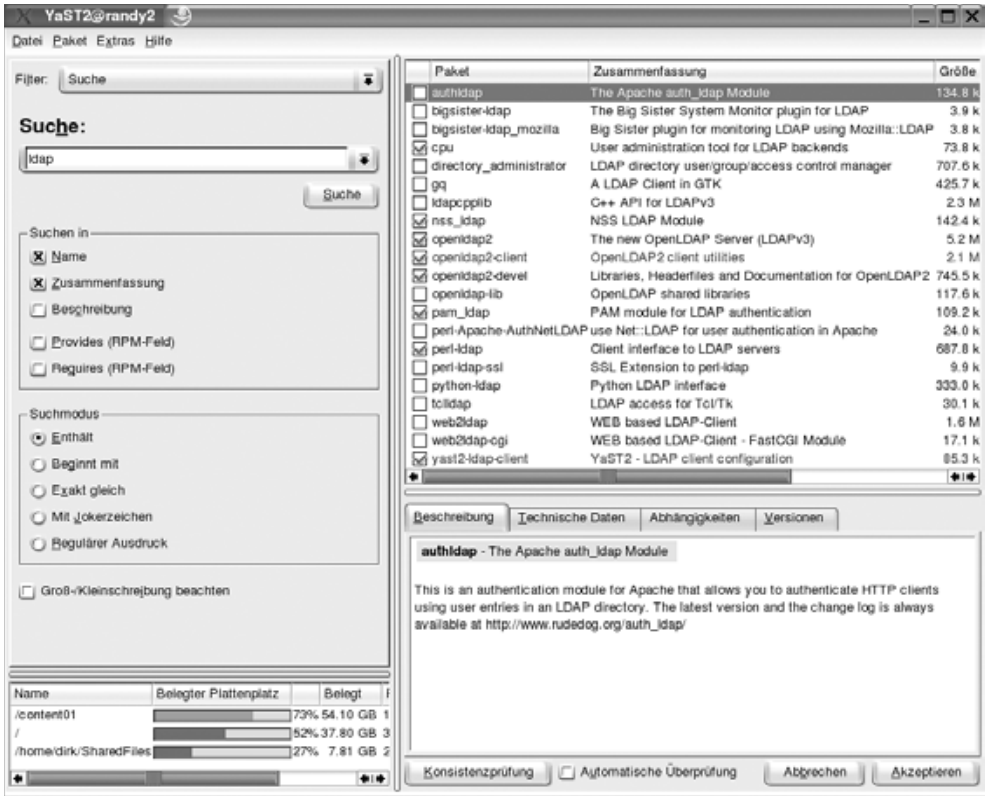

Abbildung 3.18: Installation von OpenLdap

Der Serverdienst slapd findet seine Dateien unterhalb des Dienste-Verzeichnisses `/usr/sbin`. Der LDAP-Server legt seine Konfigurationdatei `slapd.conf` unterhalb von `/etc/openldap` an. Die Dateien der laufenden Datenbank landen üblicherweise im Verzeichnis `/var/lib/ldap`. Diesen Pfad können Sie in der Konfigurationsdatei wie voreingestellt belassen oder dort ändern.

Zusammen mit dem LDAP-Paket installiert YaST etliche kleine Werkzeuge zur Verwaltung auf der Kommandozeile. Die Werkzeuge ldapsearch, ldapadd, ldapdelete und ldapmodify für Operationen auf der LDAP-Datenbank schreibt YaST in das Verzeichnis `/usr/bin`.

Die Pluggable Authentication Modules (PAM) erlauben auch für Linux flexible Authentifizierungsmethoden. Deren Konfigurationsdateien liegen in `/etc/pam.d`:

```
randy2:/etc/pam.d # ls
.          chage     chsh           gdm       login
..         passwd    rpasswd            shadow      su
useradd    xdm       xscreensaver   chfn      cups  gdm-
autologin        other              ppp       samba
sshd       sudo  webmin             xlock     zebra
```

Für jeden Login-Dienst oder jedes Programm, welches diese Authentifizierung benutzt, kann man Regeln definieren. SuSE installiert die zu PAM gehörenden Bilbliotheken unterhalb von `/lib/security`. Das pam_ldap-RPM richtet in diesem Verzeichnis pam_ldap.so ein. Lesen Sie im folgenden Unterkapitel, wie bei eingeschalteter LDAP-Authentifizierung alle dafür konfigurierten Dienste auf diese Bibliothek zugreifen.

Lesen Sie hier bitte zuerst, wie Sie einen LDAP-Servers in einer einfachen ungesicherten Form einrichten, und danach, wie Sie ihn mit SSL/TLS sichern können.

Im Beispiel gilt es, die beiden Benutzer »alcalde« und »dsuchod« mit Linux-LDAP zu verwalten.

Die Serverkonfigurationsdatei `/etc/openldap/slapd.conf` können Sie weitestgehend von SuSE übernehmen und für Ihre Ansprüche anpassen. Die geänderten oder hinzugefügten Teile sind hier im Buch hervorgehoben. Wenn von Ihnen benutzte Objekte und Attribute nicht im Core-Schema enthalten sind, müssen Sie die Standardeinstellungen zum Laden der Schema-Dateien zu Beginn der Konfiguration um weitere Schemabeschreibungen erweitern. Die ersten vier Zeilen der Beispielkonfiguration binden zusätzliche Konfigurationsdateien ein, welche die vier Standardschematypen definieren. Das Core-Schema enthält das bereits das oben genannte Personen-Objekt und das abgeleitete OrganizationalPerson-Object, sowie die Attribut-Beschreibungen, z. B. für den CommonName. inetorgperson. schema erweitert die Beschreibung dieser Objekte. Die Datei nis.schema enthält neben anderen das Objekt »posixAccount«, welches eine Zusammenfassung der Daten von Unix-Accounts beschreibt und die notwendigen Argumente definiert.

Die Lage der zum Start des Servers verwendeten Argumentdatei und der PID-Datei können Sie wie im Beispiel übernehmen. Durch »allow bind_v2« gestatten Sie älteren Client-Programmen den Zugriff auf Datenbanken, die in ihrer Voreinstellung nicht die LDAP-Protokoll-Version 3 sprechen. Hierzu zählt z. B. das Yast-LDAP-Modul.

```
 # LDAP-Serverkonfigurationsdatei
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/inetorgperson.schema

argsfile        /var/run/slapd/slapd.args
pidfile         /var/run/slapd/slapd.pid

allow           bind_v2
database        ldbm
directory       /var/lib/ldap
suffix          "dc=linuxbu,dc=ch"
rootdn          "cn=Manager,dc=linuxbu,dc=ch"
rootpw          <strenggeheim>

access to attr=userpassword
    by anonymous auth
    by self write

access to \ attr=objectclass,entry,mail,cn,sn,loginShell,
↵userPassword
   by self write
   by * read

access to \ attr=objectclass,entry,uid,mail,cn,sn,uidNumber,
↵gidNumber,homeDirectory,loginShell
   by * read

access to *
   by users read
   by anonymous auth
```

»suffix« beschreibt den Wurzelbaum des eingerichteten Servers. »rootdn« und »rootpw« definieren den Datenbankadministrator. Diese Variablen müssen Sie der Konfiguration Ihrer Site anpassen. Die folgenden Zeilen beschreiben Access Control Lists (ACLs) für den Zugriff auf die Datenbankeinträge.

LDAP kennt globale, backend- und datenbank-spezifische Konfigurationsinformationen:

Die globalen Anweisungen stehen zu Beginn der slapd.conf, gefolgt von den Informationen für einen bestimmten Backend Typ. Am Ende der Datei stehen Information für ein bestimmtes Datenbankmodul, welches LDAP zur Organisation der abgelegten Dateien verwendet. Dabei gilt folgende Abhängigkeit: Datenbankdirektiven überschreiben alle eventuell vorher definierten Werte, backend-spezifische Einstellungen eventuell vorher getroffene globale Festlegungen. Mit dem Doppelkreuz # beginnende Kommentarzeilen können Sie an jeder Stelle einfügen.

Tipp: Beim Editieren der LDAP-Serverkonfiguration muss man sehr exakt arbeiten, da unsichtbare Leerzeichen und falsche Zeilenumbrüche zu schwer nachvollziehbaren Fehlern führen können.

Nachdem Sie die Konfigurationsdatei editiert und die Existenz des Datenverzeichnisses und dessen Rechte überprüft haben, können Sie den Dienst für einen ersten Test per Hand starten:

```
/usr/lib/openldap/slapd -f /etc/openldap/slapd.conf -h
↵ ldap://127.0.0.1:389 -u ldap -g ldap
```

Der Kommandozeilenschalter `f` definiert die einzulesende Konfigurationsdatei, `h` das Protokoll, die IP-Adresse, an der der Server lauscht sowie den Port. Damit der LDAP-Server später nicht mit Root-Rechten läuft, können Sie Nutzer und Gruppe festgelegen. Dieses macht später auch das Init-Skript (/etc/init.d/ldap), welches YaST mit dem Server-RPM installiert. Damit der LDAP-Server mehr Meldungen ausgibt, kann man mit dem Parameter `-d N`, den Loglevel `N` bestimmen. SuSE speichert die Startparameter des LDAP-Dämon für das Init-Skript in der Datei `/etc/sysconfig/openldap`.

Die Log-Datei `/var/log/message` zeigt den Erfolg des Tests. Hier landen Meldungen zu Fehlern in der Konfigurationsdatei. Geht nichts schief, findet man folgenden Eintrag:

```
Aug 20 22:44:48 hermes slapd[19451]: bdb_initialize:
↵ Sleepycat Software: Berkeley DB 4.0.14: (March 13, 2003)
Aug 20 22:44:48 hermes slapd[19455]: slapd starting
```

Die LDAP-Kommandozeilenprogramme, das LDAP-PAM- und das Yast-LDAP-Modul greifen auf die Datei /etc/openldap/ldap.conf zu, um von ihr u. a. die IP-Adresse, den Port des Servers und die Wurzel der Datenbank zu beziehen.

```
# LDAP Client Konfigurationsdatei: /etc/openldap/ldap.conf
BASE    dc=linux,dc=ch
URI     ldap://127.0.0.1:389
```

BASE legt fest, in welchem Unterbaum ldap bei der Authentifizierung und beim Systembetrieb suchen soll. Organisieren Sie die Datensätze nach Abteilungen, muss die BASE alle Abteilungen enthalten, damit ldap alle Benutzer finden kann. Fasst man hingegen alle Benutzer in einem einzigen Baum zusammen, kann man BASE auf diesen Baum beschränken. Da diese Strategie für das System unwichtige Daten aus anderen Bäumen mit anderer Bedeutung ignoriert, wird die Suche performanter.

Nun verbindet sich das Suchkommando `ldapsearch -x` schon mit der Datenbank. Es liefert jedoch noch keine Daten, solange Sie die Datenbank noch nicht »befüllt« haben. Um LDAP mit Daten zu bestücken, kann man webbasierte oder grafische LDAP-Administrationsprogramme verwenden oder wie hier sogleich gezeigt für den schnellen Start eine LDIF-Datei bereitstellen:

```
# LDIF-Datei zur Definition von zwei Beispielnutzern: user.ldif
dn: dc=mydomain, dc=local
objectClass: organization
o: mydomain

dn: ou=user, dc=mydomain, dc=local
ou: user
objectclass: organizationalUnit

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

dn: cn=user, ou=group, dc=linuxbu, dc=ch
objectClass: posixGroup
objectClass: top
cn: user
gidNumber: 100
userPassword: group-pw


dn: uid=alcalde, ou=user, dc=linuxbu, dc=ch
uid: alcalde
cn: Anna Alcalde
sn: Alcalde
objectclass: person
objectclass: posixAccount
objectclass: shadowAccount
objectclass: top
userPassword: bks-pw
uidNumber: 1001
gidNumber: 100
homeDirectory: /home/alcalde
loginShell: /bin/ksh
loginShell: /bin/bash
mail: anna@alcal.de

dn: uid=dsuchod, ou=user, dc=mydomain, dc=local
uid: dsuchod
cn: Dirk von Suchodoletz
sn: Suchodoletz
```

```
objectclass: person
objectclass: posixAccount
objectclass: shadowAccount
objectclass: top
userPassword: dvs-pw
uidNumber: 1002
gidNumber: 100
homeDirectory: /home/dsuchod
loginShell: /bin/bash
mail: dsuchod@rz.uni-freiburg.de
```

In Ihre frisch angelegte Datenbank bringen Sie diese Daten mit dem Befehl:

```
ldapadd -c -x -D "cn=Manager,dc=mydomain,dc=local"
↵ -W -f user.ldif
```

Hier finden Sie den oben definierten Datenbank-Manager-Account wieder, den Sie zuvor in der Serverkonfigurationsdatei angegeben haben. Geben Sie hier das Passwort an, welches Sie in der openldap.conf für den Datenbankadministrator definiert haben.

Fehler beim Einfügen der Daten können verschiedenste, nicht sofort auf den ersten Blick sichtbare Ursachen haben. Die folgenden Tipps helfen Ihnen hoffentlich bei der Fehlersuche:

- In der aktuellen Version des OpenLDAPs muss das Attribut, welches zum Aufbau des Distinguished Name 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: Werden mehrere Objektklassen angegeben, wobei mindestens eine Klasse neben "top" erforderlich ist, müssen alle "MUSTs" dieser Objektklassen gemeinsam erfüllt sein.
- Wichtig ist die Reihenfolge des Anlegens der Objekthierarchien: Die Objekte der Root-Klasse müssen in der Datenbank eingefügt sein, bevor man darunter Knoten anlegen kann. Dabei soll das in der Konfigurationsdatei angegebene Suffix mit der Root-Klasse übereinstimmen.

Nach der erfolgreichen Erstbestückung der Datenbank liefert das "ldapsearch -x" bereits mehr Informationen. Zu sehen sind nur für den anonymen Zugriff freigegebene Daten. Um den vollständige Datensatz mit Passwort zu sehen, müssen Sie Benutzername und Passwort des Datenbank-Managers angeben:

```
ldapsearch -x -D "cn=Manager,dc=linuxbu,dc=ch" -W
```

ldapsearch gibt dann Daten im bereits bekannten LDIF-Format aus.

Im nächsten Schritt müssen Sie die PAM-Authentifizierung gegen die frisch eingerichtete LDAP-Datenbank definieren. Fügen Sie dazu bitte wie hier im Beispiel in das PAM-Modul (`/etc/pam.d/sshd`) für den SSH-Login die markierten Zeilen ein.

```
#%PAM-1.0
auth     required      pam_nologin.so
auth     sufficient    pam_ldap.so
auth     required      pam_unix2.so      use_first_pass
# set_secrpc
account  required      pam_unix2.so
password required      pam_pwcheck.so
password required      pam_ldap.so      use_authtok
password required      pam_unix2.so      use_first_pass use_
↵ authtok
session  required      pam_unix2.so
session  required      pam_limits.so
session  required      pam_env.so
session  optional      pam_mail.so
```

Damit das System mit LDAP-Benutzern umgehen kann, nachdem diese sich angemeldet haben, müssen Sie anschließend die Datei `nsswitch.conf` anpassen. Diese Datei definiert den Name-Service-Switch, z. B. das Verfahren, wie die zentrale C-Bibliothek aus einer im Dateisystem gespeicherten numerischen UserID den Accountnamen ermittelt:

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

Im hier gezeigten Ausschnitt aus der Datei sorgt der Systemadministrator dafür, dass das Linux-System zuerst die klassischen Unix-Dateien passwd und group und dann den LDAP-Server befragt. Anschließend startet der Administrator den Name Service Caching Daemon (nscd) neu und versucht als einfachen Test ein Login per SSH. Die Liste der mittels LDAP zur Verfügung gestellten Benutzer-Kennungen sehen Sie durch `getent` an. Die Einträge erscheinen nach den Daten aus der /etc/passwd.

Jetzt wird es Zeit, YaST so zu konfigurieren, dass Sie es zu Administration der LDAP-User verwenden können.

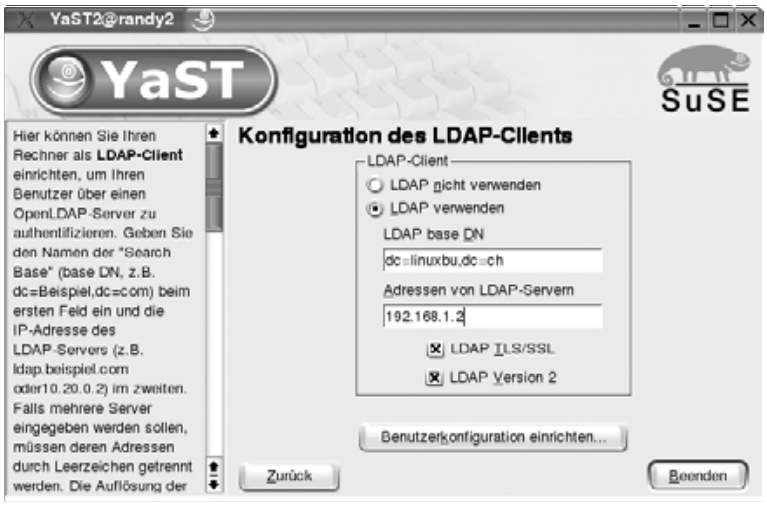

Abbildung 3.19: YaST neu konfigurieren

Wenn Sie im YaST-Kontrollzentrum unter *Netzwerkdienste* den LDAP-Client auswählen, sehen Sie den obigen Dialog. In diesem geben Sie die nun schon mehrfach genannte Datenbankwurzel und die IP-Adresse des Servers ein. Durch Häkchen können Sie eine verschlüsselte Verbindung auf Port 636 statt der unverschlüsselten Verbindung auf Port 389 wählen. Die Schaltfläche *Benutzerkonfiguration einrichten* bringt Sie zum nächsten Dialog:

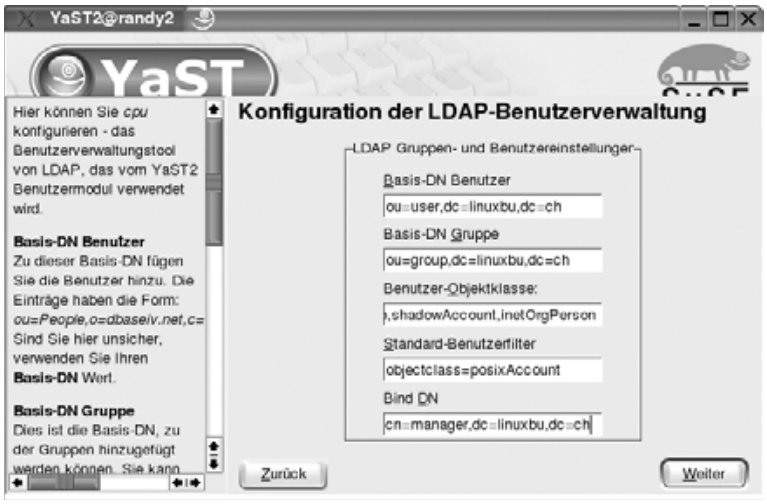

Abbildung 3.20: YaST-Dialog zum Eintragen der User- und Group-Base

Hier tragen Sie statt der Daten des voreingestellten Beispiels Ihre eigene User- und Group-Base ein.

Passen Sie bitte außerdem den Namen des Datenbankmanagers (rootdn) an. Danach können Sie sich wieder in den Bereich der Benutzerverwaltung begeben. Dort schalten Sie in den *Benutzerdefinierten Filtereinstellungen* mindestens die `LDAP-Benutzer` an:

Abbildung 3.21: LDAP-Benutzer anschalten

Anschließend zeigt Ihnen YaST neben den Benutzern aus der `/etc/passwd` alle im LDAP eingetragenen Accounts an.

Abbildung 3.22: YaST zeigt auch LDAP-Accounts

Wenn der LDAP-Client mit dem Server über das Loopback-Interface direkt auf der Maschine selbst kommuniziert, ist die Sicherheit der übertragenen Daten ausreichend gewährleistet. Anders sieht es aus, wenn LDAP-Pakete über ein Ethernet ge-

hen. Deshalb können Sie für eine LDAP-Verbindung analog zu einer HTTP-Verbindung den Secure-Socket-Layer (SSL) verwenden. Das Erstellen und Verwalten der notwendigen Zertifikate und Schlüssel ist etwas aufwändiger. Das Erstellen eines Serverzertifikates ist hier im Buch im Kapitel 6.7 beschrieben. Entweder kopieren Sie anschließend die Zertifikate in ein Unterverzeichnis der LDAP-Konfiguration, wie z. B. /etc/openldap/certificates oder passen den tatsächlichen Pfad zu diesen Dateien anders als im Beispiel unten gezeigt an.

Die Zertifikate binden Sie in Ihre LDAP-Konfigurationsdatei ein, indem Sie Ihrer LDAP-Server-Konfigurationsdatei `/etc/pam.d/sshd` die folgenden drei Zeilen voranstellen:

```
TLSCertificateFile    /etc/openldap/certificates/servercrt.pem
TLSCertificateKeyFile /etc/openldap/certificates/serverkey.pem
TLSCACertificateFile  /etc/openldap/certificates/cacert.pem
```

Zum Testen rufen Sie nun den LDAP-Server-Prozess wie folgt auf:

```
/usr/lib/openldap/slapd -f /etc/openldap/slapd.conf -h "
↵ ldaps://192.168.1.2:636 ldap://localhost:389" -u ldap -g ldap
```

Durch die Angabe von `ldaps://192.168.1.2:636` wählen Sie das abgesicherte Protokoll aus und außerdem stellen Sie nun den Server für die netzweite Benutzung zur Verfügung. Weiterhin steht nach wie vor der unverschlüsselte Zugang zur Datenbank auf dem Loopback-Interface zur Verfügung. Probieren Sie mit dem folgenden Befehl aus, ob der Server nun mit SSL korrekt arbeitet:

```
openssl s_client -connect 192.168.1.2:636--port-- -showcerts
↵ -state -CAfile pfad-zum/cacert.pem
```

Damit wie eingangs gezeigt die LDAP-Client-Programme wieder bequem funktionieren, müssen Sie noch die Datei `ldap.conf` anpassen:

```
BASE    ou=user,dc=mydomain,dc=local
URI     ldaps://10.8.4.254:636
ssl     start_tls
sasl_secprops noactive
tls hard
tls_reqcert allow
tls_checkpeer no
```

Wenn Sie jetzt die Kommandos `ldapsearch -x` oder `getent passwd` aufrufen, sehen Sie wieder die eingangs gezeigten Ausgaben.

Wenn Sie die Dateien `/etc/openldap/ldap.conf` und `/etc/nsswitch.conf` entsprechend einrichten, können Sie ldap von jeder beliebigen Maschine in Ihrem Netzwerk verwalten und mit anderen Anwendungen wie Apache, MySQL,... nutzen.