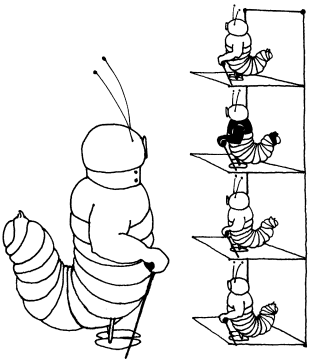
Kapitel 5

Benutzerverwaltung



Wurde im letzten Kapitel gezeigt, wie der Rechner in die einzelnen Runlevel gefahren wird, erfahren Sie hier, wie Benutzer eingerichtet werden und was für die Benutzer eines Linux-Rechners voreingestellt wird. Der Systemverwalter entscheidet letztlich, wer mit dem System arbeiten darf und welche Rechte der Benutzer eingeräumt bekommt. Hier fungiert der Systemverwalter als Statthalter.

5.1 Was passiert beim Anmelden eines Benutzers?

In der Regel wird für die Benutzer unter Linux die grafische Benutzeroberfläche bereitgestellt – zumeist KDE oder GNOME. Als Systemverwalter sollten Sie überlegen, ob Sie wirklich alle Benutzer im Login-Fenster zur Auswahl anzeigen lassen wollen. Sicherer ist ein Anmeldebildschirm, an dem der Benutzer nicht nur sein Passwort, sondern auch seinen Benutzernamen kennen muss. Die Einstellungen hierfür finden Sie unter:

Kontrollzentrum → Systemverwaltung → Anmeldungsmanager

Hier definieren Sie unter der Rubrik **Benutzer**, ob bzw. welche Benutzer angezeigt werden sollen. Nur in Ausnahmefällen sollte man die sog. *Vereinfachungen* wählen, in denen man sogar zulassen kann, dass bestimmte Benutzer sich auch ohne Passwort anmelden dürfen.

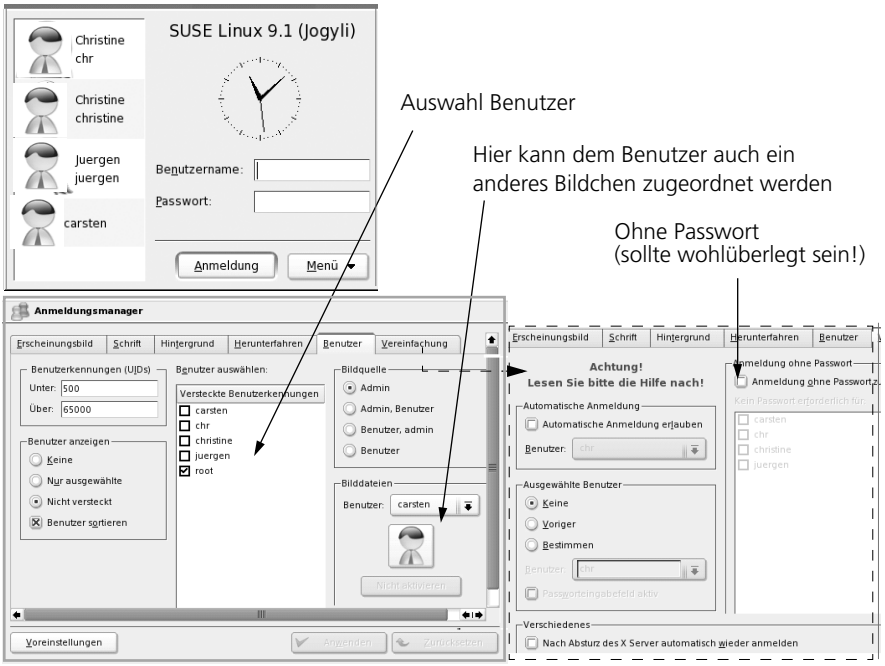


Bild 5-1: Anmeldebildschirm und der Anmeldungsmanager

Der Anmeldebildschirm wird, wie im vorigen Kapitel erwähnt, vom init-Prozess gestartet. Sobald der Benutzer nun versucht sich anzumelden, wird erst in der Datei **/etc/passwd** nach einem Eintrag mit dem angegebenen Namen gesucht und dann das Passwort mit der verschlüsselten Version in der Datei **/etc/shadow** verglichen.

5.1.1 Vorbereiten der Arbeitsumgebung für den Benutzer

Konnte das System den Benutzer beim Login eindeutig zuordnen (Eintrag in der /etc/passwd und richtiges Passwort), wird zunächst die Arbeitsumgebung für den Benutzer vorbereitet. Hierzu gehören eine Reihe von Voreinstellungen wie z. B.:

- Wertzuweisungen für bestimmte Variablen (HOME, PATH, USER, SHELL u. a.)
- Angabe, wie die Zugriffsrechte für neue Dateien und Verzeichnisse gesetzt werden sollen (**umask**, siehe Seite 133)
- Einstellungen für die gewählte Shell (Aliase, Variablen, Optionen)

Bei Anmeldung über KDE oder über eine andere grafische Oberfläche wird dann der Desktop so aufgebaut, wie er das letzte Mal verlassen wurde (evtl. beim Abmelden geöffnete Programme werden wieder gestartet, Farbeinstellungen übernommen etc.). Um alle Voreinstellungen und Zuordnungen durchzuführen, werden bestimmte Dateien nacheinander gelesen. Die zuletzt gelesenen können somit bereits vorgenommene Einstellungen wieder überschreiben. So kann z. B. der Benutzer in seiner eigenen Datei $HOME/.profile die Variable PATH neu zuordnen oder ergänzen (wer zuletzt kommt …).

Die nachfolgende Darstellung zeigt vereinfacht einen Lebenszyklus vom Hochfahren, Anmelden, Abmelden und Herunterfahren bis zum Ausschalten des Rechners. Pro Terminal (grauer Bereich) können sich mehrere Benutzer hintereinander anmelden. Da zur gleichen Zeit mit mehreren Terminals gearbeitet werden kann, können parallel auch mehrere Benutzer zur gleichen Zeit arbeiten.

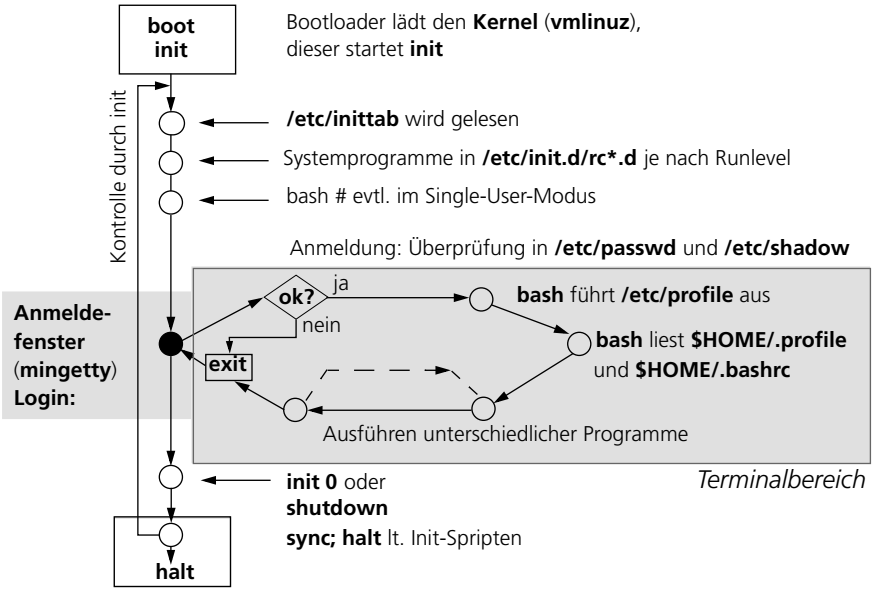


Bild 5-2: Lebenszyklus vom Hochfahren bis zum Ausschalten eines Rechners

Ein Blick in **/etc/profile** zeigt, welche Voreinstellungen für alle Benutzer gesetzt werden. Ein Ausschnitt reicht, um die generelle Funktionsweise zu erkennen, wobei wesentliche Punkte erläutert sind:

/etc/profile – Voreinstellungen für die Benutzerumgebung

```
# /etc/profile for SUSE Linux
#
# PLEASE DO NOT CHANGE /etc/profile. There are chances that your changes
# will be lost during system upgrades. Instead use /etc/profile.local fo
# your local settings, favourite global aliases, VISUAL and EDITOR
# variables, etc ...
# Check which shell is reading this file
#
if test -f /proc/mounts ; then
  case "`/bin/ls -l /proc/$$/exe`" in
    */bash)is=bash ;;
    */*) is=sh   ;;
  esac
else
  is=sh
fi
# Initialize terminal
tty=`tty 2> /dev/null`
test $? -ne 0 && tty=""
if test -O "$tty" -a -n "$PS1"; then
   test -z "${TERM}"&& { TERM=linux; export TERM; }
  ...
fi
...
# The user file-creation mask
umask 022
...
test -z "$USER" && USER=`id -un 2> /dev/null`
test -z "$MAIL" && MAIL=/var/spool/mail/$USER
test -z "$HOST" && HOST=`hostname -s 2> /dev/null`
...
# Do NOT export UID, EUID, USER, MAIL, and LOGNAME
export HOST CPU HOSTNAME HOSTTYPE OSTYPE MACHTYPE
#
# Make path more comfortable

if test -z "$PROFILEREAD" ; then
    PATH=/usr/local/bin:/usr/bin:/usr/X11R6/bin:/bin
    for dir in $HOME/bin/$CPU $HOME/bin ; do
        test -d $dir && PATH=$dir:$PATH
    done
    test "$UID" = 0 && PATH=/sbin:/usr/sbin:/usr/local/sbin:$PATH
...     test -d $dir && PATH=$PATH:$dir
fi
##
HISTSIZE=1000
export HISTSIZE
# And now let's see if there is a local profile
test -s /etc/profile.local && . /etc/profile.local

## System BASH specials, maybe also good for other shells
#
test -r /etc/bash.bashrc && . /etc/bash.bashrc
if test "$is" = "bash" -a -z "$_HOMEBASHRC" ; then
    # loop detection
    readonly _HOMEBASHRC=true
    test -r $HOME/.bashrc  && . $HOME/.bashrc
fi
```

Zuordnung der Shell

Zuordnung des Terminaltyps

Voreinstellung der Zugriffsberechtigung bei Erstellung neuer Dateien/Verzeichnisse hier mit 644 und mit 755 (Näheres in Kapitel 6.5.2)

Zuordnung der Variablen PATH getrennt für Benutzer und für root

Variable HISTSIZE für alle

Spezialeinstellung für die Bash

Ist .bashrc vorhanden, dann wird an dieser Stelle (durch **.** Dateiname) die nachfolgende Datei eingelesen

Fortsetzung nächste Seite

```
#
# KSH specials
#
if test "$is" = "ksh" ; then
    test -r /etc/ksh.kshrc && . /etc/ksh.kshrc
fi
if test "$is" = "ksh"  -a -z "$_HOMEKSHRC";then
    # loop detection
    readonly _HOMEKSHRC=true
    test -r $HOME/.kshrc   && . $HOME/.kshrc
fi
#
# End of /etc/profile
```

Spezialeinstellung für ksh (ähnlich wie für die Bash, hier $/HOME/.kshrc). Dadurch ist die Variable ENV, die sonst für die Korn-Shell gesetzt sein muss, nicht erforderlich.

Bild 5-3: Ausschnitt aus /etc/profile

5.2 Voreinstellungsdateien für den Benutzer

Es gibt eine ganze Reihe von Voreinstellungsdateien, deren Namen in der Regel mit einem Punkt beginnen, also für den normalen Anwender nur dann sichtbar sind, wenn er sie per ›**ls -a**‹ anzeigen lässt bzw. in der grafischen Oberfläche einstellt, dass auch die versteckten Dateien angezeigt werden. Für einige Programme, wie etwa **vi/vim** oder den Acrobat-Reader, werden die Voreinstellungsoptionen und Parameter in diesen Dateien im Home-Verzeichnis (oder einem Unterverzeichnis) des Benutzers abgelegt. Beim Neuanlegen eines Benutzers werden einige dieser Dateien bereits aus dem Vorlagenverzeichnis **/etc/skel** übernommen (siehe auch Seite 91).

Je nachdem, welche Shell der Benutzer verwendet, werden unterschiedliche Voreinstellungsdateien gelesen. Für die Bash und Kornshell u.a. die **.profile**:

```
# Sample .profile for SUSE Linux
# ...
# All other interactive shells will only read .bashrc; this is
# particularly important for language
# settings, see below

test -z "$PROFILEREAD" && . /etc/profile
#...
export PATH=$PATH:~/Befehle
```

Wenn die Variable $PROFILEREAD leer ist (sie wird in /etc/profile gesetzt), dann soll /etc/profile an dieser Stelle gelesen werden.

Erweiterung der Variablen PATH

Bild 5-4: Ausschnitt aus .profile

Wie schon erwähnt, kann der Benutzer in der Datei $HOME/.profile, die beim Login gelesen wird, die Variable PATH mit einem zusätzlichen Verzeichnis ergänzen (siehe Bild 5-4). Dies ist dann sinnvoll, wenn er eigene Kommandos schreibt und sie dann in jenem Verzeichnis ablegt (z.B. $HOME/bin oder $HOME/Befehle). Da der Benutzer unter Linux mehrere Shells gleichzeitig aktivieren kann (z.B. in mehreren Terminalfenstern), wird für die sog. *interaktive Shell* die Datei **~/.bashrc** (~/ steht für das jeweilige Home-Verzeichnis des Benutzers) gelesen. Da in diesem

Buch die Bash nicht mehr speziell behandelt wird, hier nur der Hinweis, dass in **~/**.bashrc z.B. Aliase (Kurznamen für Befehle) und Zuordnung mit entsprechenden Optionen eingetragen werden können. Unter SUSE lassen sich solche Alias-Anweisungen auch in einer zusätzlichen Datei **~/.alias** eintragen (siehe Bild 5-5 zur Einbindung der Datei in den Anmeldungsprozess).

```
# # Sample .bashrc for SUSE Linux
#...
test -f /etc/profile.dos && . /etc/
# ...#
# NOTE: It is recommended to make language settings in ~/.profile rather
# than here, since multilingual X sessions would not work properly if
# LANG is overridden in
# every subshell.
...
test -s ~/.alias && . ~/.alias
alias rm="rm -i"
```

Existiert eine Datei /etc/profile.dos, dann lies sie hier ein. (Eine nette Erleichterung von SUSE für ehemalige DOS-Benutzer)

Existiert eine nicht leere Datei im Home-Verzeichnis mit Namen .alias, soll sie hier eingefügt werden.

Für rm soll immer rm -i verwendet werden.

Bild 5-5: Ausschnitt aus .bashrc

Für die grafische Oberfläche existieren zusätzliche Voreinstellungsdateien wie **.xsession** und **.xinitrc**. Sie sind ähnlich aufgebaut wie /etc/profile. Unter SUSE Linux sind diese Dateien schon so angepasst, dass Sie als Systemverwalter in der Regel kaum etwas daran ändern müssen.

5.3 Das Linux-Einwohnermeldeamt

Bevor ein Benutzer mit dem System arbeiten darf, muss er registriert sein, d.h. einen Account besitzen. Der Account ist ein Eintrag zum Benutzer in /etc/passwd und (zumeist) in /etc/shadow.

Bei der SUSE Linux-Installation wurde als Teil des Installationsdialogs neben root bereits ein weiterer Benutzer eingetragen.

Nur mit gültigem Wohnsitz (sprich Home-Verzeichnis) und der Zutrittskontrolle über das Passwort wird einem Benutzer erlaubt, mit einem Linux-System zu arbeiten. Im Standardfall kann nur der Systemverwalter einen dazu notwendigen Account (neuen Benutzer) anlegen. Sehen wir uns dazu die entsprechenden Dateien im folgenden Abschnitt an.

5.3.1 /etc/passwd, /etc/shadow und /etc/group

Die Datei **/etc/passwd** ist die zentrale Datei zur Benutzerverwaltung. Gleich zu Beginn eine Warnung: Sollte die Datei /etc/passwd versehentlich gelöscht werden oder die 1. Zeile (Root-Eintrag) verstümmelt sein, kann Ihr System nicht mehr korrekt hochfahren. Dann hilft nur noch eine Neuinstallation oder ein Wiederherstellen über ein sogenanntes *Rescue-System* (Rettungssystem z.B. auf der Installa–

tions-CD/DVD). Verändern Sie /etc/passwd deshalb nur, wenn Sie genau wissen, was Sie tun. Um neue Benutzer anzulegen oder vorhandene zu löschen, ist es meist besser, die dafür vorgesehenen Tools einzusetzen. Die Struktur der passwd-Datei können Sie sich auch als normaler Benutzer anschauen. Die /etc/passwd hat sieben Spalten, die durch einen ›:‹ getrennt werden:

Benutzer-name	Passwort Schlüssel	Benutzer-Nr.	Gruppen-Nr.	Kommentar (Vorname, Name)	Login-Verzeichnis	Start-programm

root:x:0:0:root:/root:/bin/bash **Achtung root-Zeile niemals verändern!**

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
chr:x:1000:100:Christine:/home/chr:/bin/bash
christine:x:1001:100:Christine:/home/christine:/bin/bash
juergen:x:1002:100:Juergen:/home/juergen:/bin/bash
carsten:x:1003:100::/home/carsten:/bin/bash
james:x:1004:100:James Cook:/home/james:/bin/bash
+::::::
```

reservierte Nummern für Programme

Bild 5-6: Beispiel einer /etc/passwd

Erläuterungen zu den Spalten:

Benutzername Auf einigen Linux/Unix-Systemen darf der Login-/Benutzername maximal 8 Zeichen enthalten und nur Kleinbuchstaben verwenden. Seit SUSE 8.x sind auch längere Namen möglich und Großbuchstaben zulässig. Manche Programme werten allerdings nur acht Zeichen aus (z.B. who). Der Benutzername sollte keine Umlaute und Sonderzeichen enthalten!

Passwort Ein *x* hier zeigt an, dass das (verschlüsselte) Passwort in der Datei /etc/shadow abgelegt ist.

Benutzer-Nr. Die Standardtools vergeben Benutzernummern automatisch ab der Nummer 1000 (seit SUSE Linux 9.1, davor ab 500). Wird die gleiche Nummer zweimal vergeben, bedeutet dies, dass der Benutzer mit mehreren Benutzernamen Zugriff auf das Home-Verzeichnis und die Dateien hat. In der Anzeige mit ›**ls -l**‹ wird nur der Name angezeigt,

der in der /etc/passwd zuerst vorkommt. Im Dateikopf von Dateien ist jeweils nur diese Benutzernummer eingetragen. Der Befehl **ls** ermittelt daraus den Namen erst über die /etc/passwd. Allerdings wird eine doppelt vorkommende Nummer unter YaST nicht akzeptiert. Das Prüfprogramm **pwck** (*password check*) fragt den Systemverwalter erst, ob der zweite Eintrag gelöscht werden soll. Doppelte Vergabe von Nummern ist sicher nicht empfehlenswert, kann aber unter Umständen bei der Vernetzung mit Windows-Rechnern über Samba sinnvoll sein.

Gruppen-Nr. Hier steht die *primäre Gruppennummer* (*Initial- oder Standardgruppe*) des Benutzers. Diese Gruppennummer wird beim Anlegen von Dateien und Verzeichnissen übernommen. Default ist die Gruppennummer 100 für die Gruppe ›users‹. Ein Benutzer kann jedoch mehreren Gruppen angehören (siehe */etc/group*).

Kommentar Hier werden in der Regel Vorname und Nachname eingetragen. Einige Programme werten dieses Kommentarfeld aus, so u.a. **finger**, das ähnlich wie **who** die aktuell angemeldeten Benutzer anzeigt, jedoch mit mehr Informationen. Mit **chfn** können weitere Informationen wie Abteilung, Telefon etc. mitgegeben werden, die letztlich mit Komma getrennt im Kommentarfeld der /etc/passwd eingetragen werden.

Login-Verzeichnis Das Verzeichnis, das dem Benutzer nach dem Anmelden (Login) automatisch zugewiesen wird. Es ist in der Regel zugleich sein Home-Verzeichnis.

Startprogramm Das hier angegebene Programm wird nach dem Login automatisch gestartet. Unter SUSE Linux ist als Default /bin/bash eingesetzt. Fehlt die Angabe, so wird die Bourne-Shell verwendet (/bin/sh).
Je nach Vorliebe des Benutzers lässt sich hier auch eine andere Shell eintragen (**csh**, **tcsh**, **ksh**, **ash** u.a.). Der Benutzer kann später auch selbst durch das Kommando **chsh** (*change shell*) hier eine Änderung vornehmen.
Wird ein anderes Programm als eine Shell eingetragen, so wird dieses Programm gestartet. Beendet der Benutzer dann das Programm, wird er automatisch abgemeldet. (Doch Vorsicht: Auch die grafische Oberfläche steht dem Benutzer dann nicht zur Verfügung, d.h., um ein grafisches Programm zu starten, müsste ein spezielles Skript geschrieben werden, das dann auch die grafische Oberfläche mit startet).

Um sich mit einem Passwort anzumelden, ist die Datei **/etc/shadow** notwendig. In ihr sind zusätzliche Vorgaben möglich, etwa zur Gültigkeitsdauer des Passworts oder bis zu welchem Datum der Benutzer sich am System anmelden darf (die Berechtigung endet dann zu diesem Datum). Doch auch dafür bieten die Tools zum Anlegen und Ändern von Benutzern Möglichkeiten an. Die Einträge sollten deshalb statt mit einem Editor mit diesen Tools vorgenommen werden. Sie ersparen z.B. die Berechnung des Gültigkeitstermins. Er ist in Tagen ab dem 1.1.1970 anzugeben – dem Beginn des Unix-Zeitalters.

Die Datei **/etc/shadow** ist im Gegensatz zu /etc/passwd nicht allgemein lesbar. Sie enthält für jeden Benutzer im System einen einzeiligen Eintrag in folgendem Format – jeweils durch einen Doppelpunkt getrennt:

Benutzer-name	Passwort	l-Änderung	min	max	warn	inaktiv	Verfall	Flag

```
carsten:lPgyOon.Ol8.s:12561:0:99999:7:::
chr:NzxtljEacipR.:12547:0:99999:7:::
christine:1i1GysUBYcBw.:12548:0:99999:7:::
james:tR10inLLrfYqQ:12607:0:99999:7:::
juergen:FShYpMXX5GxdA:12548:0:99999:7:::
hans:!:12620:0:99999:7:::
otto:eZ2P9qhM1.6NI:12620:0:99999:7:::
+::0:0:0::::
```

Bild 5-7: Ausschnitt aus /etc/shadow

Hierbei ist:

Benutzername Die Kennung, unter der sich der Benutzer am System anmeldet. Sie wird auch als *Account-Name* bezeichnet und stellt die Querverbindung zum korrespondierenden Eintrag in der Datei **/etc/passwd** her.

Passwort An dieser Stelle wird das Passwort des Benutzers in verschlüsselter Form gespeichert. Bei manchen Systemen ist ein leeres Passwort (›::‹) erlaubt. Ab Linux 9.1 wird hier ein Ausrufezeichen eingesetzt (siehe ›hans‹ in Bild 5-7). In diesem Falle erfolgt beim Anmelden keine Passwortabfrage. Ein Passwort, welches nur aus der Return-Taste besteht, ist **kein** leeres Passwort.

l-Änderung Tag der letzten Passwortänderung. Der Tag wird als absolute Differenz in Tagen zum 1. Januar 1970 angegeben.

min Definiert die Anzahl der Tage, die mindestens zwischen zwei Passwortänderungen liegen muss.

max Gibt die maximale Gültigkeit des Passwortes in Tagen vor. Erfolgt eine Anmeldung nach Ablauf dieser Frist, erzwingt das System die Passwortänderung vor dem Beginn der Sitzung.

warn Spezifiziert die Anzahl von Tagen, ab denen der Benutzer vor Ablauf der Gültigkeit des Passwortes diesbezüglich gewarnt wird.

inaktiv Anzahl der maximal akzeptierten Tage ohne Anwesenheit am System. War der Benutzer mehr Tage als angegeben nicht am System, so verfällt die Gültigkeit seines Passwortes, unabhängig von den anderen Gültigkeitskriterien.

Verfall Verfallsdatum. Nach diesem Tag wird der Zugang des Benutzers zum System in jedem Falle verwehrt.

Flag Ein Zeichen zur Identifikation des verwendeten Kodierverfahrens für das Passwort.

Die dritte Datei, **/etc/group**, beinhaltet die Gruppennamen und die dazugehörigen Benutzer. Auch hier reicht ein kleiner Ausschnitt der Datei. Der Aufbau der Gruppendatei ist recht einfach:

Gruppen-name	Gruppen-passwort	Gruppen-Nr.	Benutzer, Benutzer …

```
root:x:0:
...
uucp:x:14:carsten,chr,christine,james,juergen,hans,otto
dialout:x:16:carsten,chr,christine,james,juergen,hans,otto
audio:x:17:carsten,chr,christine,james,juergen,hans,otto
...
video:x:33:carsten,chr,christine,james,juergen,hans,otto
...
users:x:100:
```

Bild 5-8: Ausschnitt aus /etc/group

Hat eine Gruppe mehrere Benutzer, werden diese jeweils durch Komma getrennt. Das Gruppenpasswort ist verschlüsselt abgelegt.

Um der Gruppe ein Passwort zu vergeben, wird das Kommando **passwd -g** aufgerufen. Das verschlüsselte Passwort wird in der Datei **/etc/gshadow** gehalten. Eine Passwortvergabe bei Gruppennamen ist in der Praxis jedoch sehr selten.

Um Dateien/Verzeichnisse mit einer anderen Gruppe anzulegen als die eingetragene Gruppe aus der /etc/passwd, muss der Benutzer das Kommando ›**newgrp** *Gruppenname*‹ aufrufen. Dazu muss sein Name in /etc/group unter dem betreffenden Gruppennamen aufgeführt sein. Falls für die Gruppe ein Passwort vergeben wurde, wird die Eingabe des Passworts verlangt.

5.4 Neue Benutzer anlegen

Müsste man das Home-Verzeichnis mit all seinen Voreinstellungsdateien für jeden neuen Benutzer erst anlegen, so wäre das Einrichten von neuen Benutzern eine recht aufwendige Angelegenheit. Doch mit den YaST-Tools lässt sich dies schnell erledigen.

5.4.1 Anlegen und Ändern von Benutzern über YaST

Das Kontrollzentrum ist zu Beginn zwar einfach zu handhaben, doch nach und nach wissen Sie bereits, welche Menüs Sie direkt mit YaST aufrufen können. Dann empfiehlt es sich, das Icon für YaST (Startmenü: **System** → **YaST**) in die Kontrollleiste zu übernehmen (das Icon aus dem Startmenü einfach in die Kontrollleiste ziehen) und von dort die gewünschte Anwendung zu starten:

YaST → Sicherheit und Benutzer → Benutzer bearbeiten und anlegen

Nach der obligatorischen Eingabe des Root-Passworts werden übersichtlich die bisher angelegten Benutzer angezeigt, wie in Bild 5-9 ① dargestellt. Um einen neuen Benutzer anzulegen, klicken Sie auf die Schaltfläche **Hinzufügen** ②. Über die Maske gibt man zumindest den Benutzernamen und das Passwort an. Die Eingabe des Passworts muss wiederholt werden. Vorname und Name, die im Kommentarfeld der /etc/passwd landen, sind nicht zwingend, gehören aber in eine ›ordentliche‹ /etc/passwd. Über **Details** ④ sehen Sie, dass der Benutzer automatisch noch anderen Gruppen zugeordnet wurde. Es lassen sich hier noch weitere Gruppen vorgeben oder zugewiesene entfernen.

Soll der Benutzer nur einen zeitlich begrenzten Zugang erhalten, so lässt sich unter ›**Passworteinstellungen**‹ ③ das Ablaufdatum eintragen. Der Benutzer erhält dann sieben Tage vor Ablauf eine Warnung, falls in der ersten Zeile die Standardeinstellung nicht verändert wurde.

Für sensible Bereiche lässt sich hier auch vorgeben, dass das Passwort nach einer vorgegebenen Anzahl von Tagen zu ändern ist.

Ein Klick auf **Weiter** ⑤ legt automatisch alle nötigen Verzeichnisse und Dateien an und trägt als Besitzer sämtlicher Dateien im neuen Home-Verzeichnis den neuen Benutzer ein. Möchte man die Account-Daten eines bestehenden Benutzers ändern, so markiert man in der ersten Anzeige die entsprechende Zeile und klickt auf **Bearbeiten** ⑥.

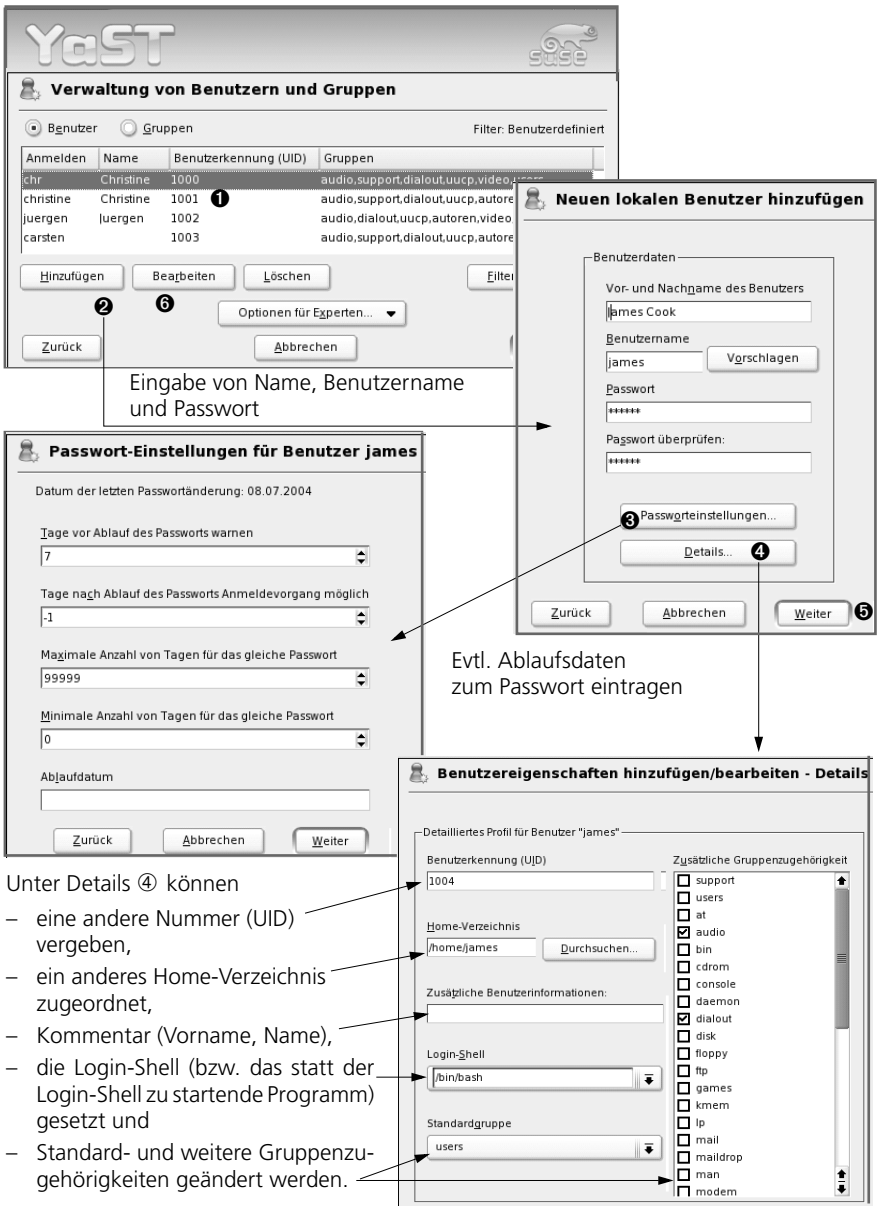


Bild 5-9: Neue Benutzer bearbeiten und anlegen über YaST2

5.4.2 Das Vorlagenverzeichnis /etc/skel

Welche Dateien und Unterverzeichnisse angelegt werden sollen, ist im Verzeichnis **/etc/skel** (abgeleitet von *skeleton*, hier Entwurf, Rahmen) enthalten. Wollen Sie als Systemverwalter, dass neue Benutzer das Kommando rm immer automatisch mit ›**rm -i**‹ aufrufen, dann ergänzen Sie im Verzeichnis /etc/skel die Datei .bashrc um den Aliaseintrag **alias rm="rm -i"**.

Die Datei .exrc beinhaltet die Voreinstellungen für den komfortableren **vim**, der unter Linux statt **vi** verwendet wird.

```
./                  .exrc               .xemacs/
../                 .fonts/             .xim
.Xdefaults          .gnu-emacs          .xinitrc*
.Xmodmap            .kermrc             .xserverrc.secure
.Xresources@        .muttrc             .xsession*
.bash_history       .profile            .xtalkrc
.bashrc             .urlview            Documents/
.dvipsrc            .xcoralrc           public_html/
.emacs
```

Bild 5-10: Liste (ls -Fa) der Standarddateien und Unterverzeichnisse in /etc/skel

5.4.3 Benutzer anlegen per useradd

Die grafische Oberfläche ist, wie Sie gesehen haben, sehr komfortabel – doch was machen Sie, wenn Sie nicht nur einen neuen Benutzer, sondern 100 neue Benutzer anlegen wollen? Dies ist per Kommandozeile wesentlich schneller möglich. Das Kommando hierfür mit den wichtigsten Optionen lautet:

useradd [**-c** *Kommentar*] [**-m**] [**-p** *verschlüsseltes Passwort*] *Benutzername*

Kommando, um Benutzer anzulegen

Die Option **-m** (*mkdir*) bewirkt, dass ein Home-Verzeichnis unter /home mit dem Benutzernamen angelegt wird, falls es nicht bereits existiert. Zusätzlich werden alle Dateien und Unterverzeichnisse aus der /etc/skel in das Home-Verzeichnis kopiert.

Weitere oft verwendete Optionen sind:

-s *shell*	Nur dann notwendig, wenn die Bash **nicht** verwendet und stattdessen ein anderes Programm ausgeführt werden soll.
-d *Home-Verzeichnis*	Erlaubt die Vorgabe eines vom Standard (/home/*benutzername*) abweichenden Home-Verzeichnisses.
-g *Gruppennr./-namen*	Erlaubt die Vorgabe einer vom Standard (100) abweichenden Gruppennummer.

-k *Verzeichnis* Gibt vor, dass statt /etc/skel das angegebene Verzeichnis als Vorlage verwendet werden soll.

Sollen keine Voreinstellungsdateien kopiert werden, lässt man **-m** weg; das Home-Verzeichnis ist dann explizit per **-d** vorzugeben.

Es gibt eine Reihe weiterer Optionen, die auch den Eingabemöglichkeiten unter YaST entsprechen (Passwort-Ablauf etc.). Weitere Hinweise dazu finden Sie per **man useradd** oder in der Online-Hilfe von SUSE.

Wichtig ist nun, mit möglichst wenig Aufwand mehrere Benutzer anzulegen. Das dazu notwendige verschlüsselte Passwort erhält man per

mkpasswd *Passwort*

Kommando, um ein verschlüsseltes Passwort zu erhalten

Dessen Ausgabe sieht dann etwa so aus: EDfoeeWUhPCHU

Unter Umständen muss dieses Kommando erst nachinstalliert werden (Paket whois, siehe auch Seite 348).

Der Aufruf, um einen Benutzer gleich mit Passwort (in nachfolgendem Fall mit dem gleichen Namen und den Ziffern 123) anzulegen, lautet dann:

useradd -m -p $(mkpasswd *hans123*) *hans*

Um mehrere Benutzer anzulegen, ruft man das Kommando über eine Schleife auf:

```
for ben in hans otto helga inge
do useradd -m -p $( mkpasswd ${ben}123 ) $ben; done
```

Die Kommandosequenz legt man vorzugsweise in ein kleines Skript. Statt die Namen einzeln anzuführen, könnte man sie auch mit **$**(**cat liste**) ausgeben. Sind in der Liste Vornamen und Nachnamen enthalten, wäre hier ein Skript mit **awk** besser, das zuerst einen Benutzernamen kreiert und Vor- und Nachnamen per Option **-c** als Kommentar mitgibt. An dem Beispiel wird ersichtlich, dass die Kommandozeile und einige einfache Shell-Skripte dem Systemverwalter viel Zeit sparen können. Das nachfolgende kleine Skript geht davon aus, das die neu einzutragenden Benutzer in einer Datei *benutzer* bereits zeilenweise stehen, und zwar in der Form: *Benutzername Vorname Nachname*

```
#!/bin/bash
cat benutzer | while read name kom1 kom2
      do useradd -m -c" $kom1 $kom2" -p $( mkpasswd ${name}123 ) $name
         echo $name angelegt
      done
```

Bild 5-11: Beispiel eines Skripts, um mehrere Benutzer anzulegen

Um in Skripten das Passwort zu ändern, gibt es seit Version 9.1 auch das Kommando **chpasswd**, das keine interaktive Eingabe des Passworts verlangt. Mit diesem Kommando kann das Passwort auch unverschlüsselt vorgegeben werden. Die Benutzer müssen bereits einen Account besitzen. Das Kommando erwartet als Eingabe entweder ›benutzername:password‹ über die Standardeingabe oder mit der Option -e *Dateiname* entsprechend aufbereitete Zeilen in einer Datei.

5.4.4 Passwortverschlüsselung

Linux bietet mehrere Verschlüsselungsmethoden des Passworts an:

DES — Dies ist die Standardmethode unter Linux. Allerdings werden auch bei längeren Passwörtern nur acht Zeichen übernommen. Es funktioniert dafür in allen Netzwerkumgebungen.

MD5 — Diese Methode lässt auch längere Passwörter zu und ist damit sicherer. Allerdings wird dies nicht von allen Netzwerkprotokollen unterstützt.

Blowfisch — Auch hier werden längere Passwörter verschlüsselt, doch wie bei MD5 können Probleme mit Netzwerkprotokollen auftreten.

Die Passwortverschlüsselung kann pro Benutzer zugeordnet werden:

YaST → Sicherheit und Benutzer
→ Benutzer bearbeiten und anlegen
→ Expertenmodus

5.4.5 Passwort ändern

Das Passwort ist ein wesentlicher Teil des Linux-Sicherheitskonzeptes. Es verhindert, dass sich ein Fremder unerlaubt unter dem Account eines anderen Benutzers anmeldet. Deshalb sollte jeder Benutzer angehalten werden, sein vorläufig vom Systemverwalter vergebenes Passwort so bald wie möglich zu ändern. Dazu muss er ein sicheres Passwort wählen – d.h. ein Passwort, welches nicht leicht erraten oder durch Probieren ermittelt werden kann. Wählt der Benutzer seinen eigenen Benutzernamen als Passwort oder ein Wort mit weniger als sechs Zeichen, so weist das System ihn darauf hin (Meldung: ›*too easy*‹). Bleibt der Benutzer jedoch stur und gibt das schwache Passwort erneut ein, so akzeptiert das System auch einfache Passwörter. Ein Passwort sollte mindestens acht Zeichen lang sein und aus einer Kombination von Buchstaben und Sonderzeichen oder Ziffern bestehen. Das Passwort sollte nicht in einem Lexikon oder Wörterbuch zu finden sein und schon gar nicht ein Eigenname sein. Linux (wie alle Unix-Systeme) unterscheidet dabei zwischen Groß- und Kleinbuchstaben, gleich welche Verschlüsselungsart gewählt wurde.

Vergisst ein Benutzer sein Passwort, kann nur der Systemverwalter ihm mit dem Kommmando

passwd *Benutzer*

Kommando, um ein Passwort zu ändern

ein neues Passwort zuweisen. Der Benutzer kann sich dann wieder anmelden, sollte aber als erstes mit dem Kommando **passwd** das (neue, vorläufige) Passwort ändern. Denken Sie als Systemverwalter daran, dass beim Kommando **passwd** ohne Angabe eines Benutzers immer das eigene Passwort (also in diesem Fall das von root) geändert wird. Wie oft wurde in Systemverwalterkursen so das Passwort für den Systemverwalter irrtümlich geändert!

Vergisst allerdings der Systemverwalter sein Passwort, hilft nur die Installations-CD mit dem Rescue-System oder ein anderes ladbares Linux (z. B. Knoppix). Da es etwas aufwendiger ist, das vergessene Root-Passwort zu ändern, erfahren Sie hierüber mehr im Kapitel 13, Hilfe zur Selbsthilfe.

5.5 Benutzereinstellungen ändern per usermod

Mit dem Kommando **usermod** werden Account-Einstellungen geändert, die mit **useradd** oder mit YaST eingerichtet wurden. Das Kommando hat die gleichen Optionen wie **useradd**. So lässt sich z. B. mit

usermod -p *verschlüsseltes_Passwort Benutzername*

Kommando, um Benutzerdaten zu verändern (*in /etc/passwd und /etc/shadow*)

das Passwort ändern. Dies ist dann nützlich, wenn mehrere Benutzer neue Passwörter erhalten sollen. Es geht schneller, das Passwort muss nicht wiederholt werden, und das Kommando lässt sich in einem Skript verwenden.

5.6 Benutzer löschen per userdel

userdel [**-r**] *Benutzername*(*n*)

Kommando, um Benutzer zu löschen

Es ist ein einfaches und sehr wirksames Kommando. Verwendet man die Option **-r**, wird – ohne Rückfrage – das Home-Verzeichnis des Benutzers mit sämtlichen Dateien und Unterverzeichnissen gelöscht (hoffentlich haben Sie nicht den Verkehrten erwischt …). Vor dem Löschen wird man deshalb eine aktuelle Sicherung anlegen.

5.7 Neue Gruppen anlegen, ändern, löschen

Unter der grafischen Oberfläche werden Gruppen ebenfalls über YaST neu angelegt oder geändert.

Kontrollzentrum → YaST2 Module → Sicherheit und Benutzer → Gruppen bearbeiten und anlegen

Auf der Einstiegsmaske wird gleich oben ausgewählt, ob man Benutzer- oder Gruppenverwaltung vornehmen möchte.

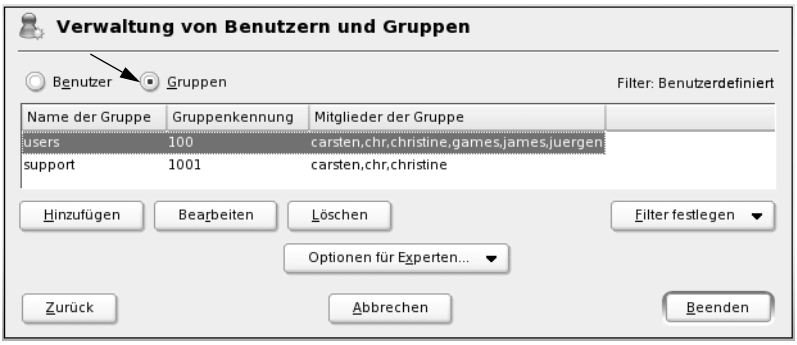


Bild 5-12: Verwalten von Gruppen über YaST

Statt der vorhandenen Benutzer werden dann die bereits eingerichteten Gruppen angezeigt, d.h. nur jene Gruppen, die für Benutzer vorgesehen sind (ab der Gruppennummer 100). Für eine Reihe spezieller Programme und Dienste – z.B. mail – gibt es neben Benutzernamen auch Gruppennamen. Diese sollten nicht verändern werden. Sie sehen sie nur, wenn Sie sich die /etc/group anzeigen lassen (z.B. per **less** oder **more**).

Zum Einrichten einer neuen Gruppe klicken Sie auf **Hinzufügen** und geben den Gruppennamen ein. Über ein Scroll-Feld können Sie all jene Benutzer auswählen, die Mitglied dieser Gruppe sein sollen. Wird ein Gruppenpasswort eingetragen, so müssen die Gruppenmitglieder, bevor sie mit **newgrp** in die Gruppe wechseln, das Passwort angeben.

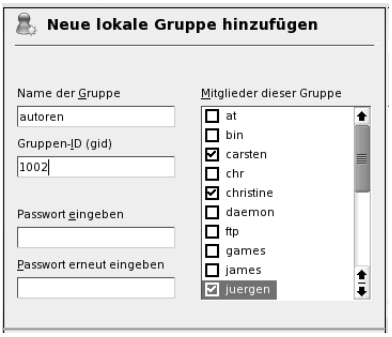


Bild 5-13: Neue Gruppe einrichten mit YaST

Mit **Beenden** werden die Änderungen in /etc/group vorgenommen. Die so angelegten Gruppen erhalten standardmäßig fortlaufende Nummern ab 1001 (seit SUSE Linux 9.1, davor ab 500).

Gleich ob die Neuanlage über YaST oder über Kommandos erfolgt, die /etc/group wird in gleicher Weise verändert. Hier die Ergänzungen der Eingabe von Bild 5-13:

```
users:x:100:
support:x:1001:carsten,chr,christine
autoren:x:1002:carsten,christine,juergen
+:::
```

Die letzte Zeile kennzeichnet das Ende und dient für automatische Folgebearbeitungen.

Für die Eingabe per Kommandozeile oder für Shell-Skripten sind folgende Kommandos für das Anlegen und Ändern für Gruppen vorhanden:

groupadd [**-g** *Gruppennummer*] *Gruppenname*

Kommando, um Gruppen anzulegen

Fehlt die Option **-g**, so wird bei der Neuanlage die nächstfolgende Nummer (ab 1001) automatisch vergeben.

groupmod [**-g** *Gruppennummer*] *Gruppenname*

Kommando, um Gruppen zu ändern

Hier ist es jedoch einfacher, über einen Editor die Datei /etc/group zu bearbeiten.

5.8 Überlegungen zur Benutzerverwaltung

Wie andere administrative Aufgaben verlangt auch die Benutzerverwaltung ein bisschen Planung und Systematik – sobald es über ganz wenige Benutzer hinausgeht. Legen Sie sich deshalb ein Schema für die Vergabe von Benutzernamen (Account-Namen) und Gruppennummer zurecht – angepasst an Ihre Bedürfnisse (bzw. die Ihrer Firma) und an Anzahl und Art Ihrer Benutzer. Dokumentieren Sie dieses Schema!

In einer Firma ist es z.B. sinnvoll, auch Blöcke von Benutzernummern für einzelne Abteilungen zu reservieren – 1000–1099 für das Marketing, 2000–2099 für Verwaltung und Einkauf usw. Überlegen Sie sich auch, nach welchem Schema Sie Gruppennummern vergeben möchten. Im Standardfall vergibt SUSE Linux jedem Benutzer die Gruppennummer 100. Dies ist nicht immer sinnvoll. Über die Gruppe lassen sich die Benutzer zusammenfassen, welche auf bestimmte Daten gemeinsam zugreifen dürfen (z.B. die aktuellen Marketingzahlen). Planen Sie bei einer Firma das Nummernschema auf Expansion – es kostet praktisch nichts.

Scheidet ein Benutzer aus, so sollte seine Benutzernummer zunächst nicht wieder vergeben werden. So lässt sich später einfacher und eindeutiger in Protokollen

und Ähnlichem nachvollziehen, welcher Benutzer gemeint ist. Auch sind alte Dateien mit ihrem Zugriffsschutz so vor dem ungewollten Zugriff des neuen Benutzers geschützt, der zufällig die gleiche Benutzernummer erhalten hat.

Legen Sie die Musterdateien (Standardeinstellungen) in dem Vorlagenverzeichnis **/etc/ske**l sorgfältig an – dies erspart Ihnen als Systemverwalter später einiges an Zeit und Rückfragen der Benutzer. Werden im Marketing z.B. spezielle Programme eingesetzt, die solche Voreinstellungen benötigen, so legen Sie am besten für das Marketing ein spezielles Musterverzeichnis an, in dem auch diese Voreinstellungsdateien vorhanden sind. Benutzen Sie dann dieses Vorlagenverzeichnis als Muster beim Anlegen neuer Accounts für das Marketing.

So wie Benutzerdaten regelmäßig gesichert werden müssen, so müssen auch diese Verwaltungsdaten gesichert werden! Beziehen Sie deshalb das Verzeichnis /etc in Ihre regelmäßige Sicherung ein (siehe hierzu Kapitel 9, Datensicherung).

Bringen Sie Ihren Benutzern bei, dass gut gewählte Passwörter und ein verantwortungsvoller Umgang mit Passwörtern zu ihrem eigenen Nutzen sind und dem Schutz der Firma vor Missbrauch dienen. Zeigen Sie ihnen, wie man sichere Passwörter aufbaut und wie man sie sich merken kann – z.B. über einen gut zu merkenden Schlüsselsatz, bei dem man von jedem Wort den ersten und letzten Buchstaben als Teil des Passworts nimmt und noch ein paar Gemeinheiten (Sonderzeichen) gegen das Cracken einwirft. Benutzer sollten private Passwörter und solche für den Gebrauch in der Firma trennen. Das Passwort bei AOL oder T-Online sollte auf keinen Fall das gleiche sein wie das Zugangspasswort in der Firma![1]

5.9 Kommandos zur Bearbeitung von Benutzern und Gruppen

Rufen Sie das Kommando **man -k user** auf, so erhalten Sie eine Liste von Kommandos, die alle etwas mit user (Benutzer) zu tun haben. Neben den grafischen Tools für die Benutzerverwaltung, die Ihnen zu Beginn alles Wissenswerte über die Benutzer aufzeigen, finden Sie auf der Seite 409 eine Tabelle mit Kommandos, die die Benutzerverwaltung betreffen.

5.10 Dateien und Verzeichnisse für die Benutzerverwaltung

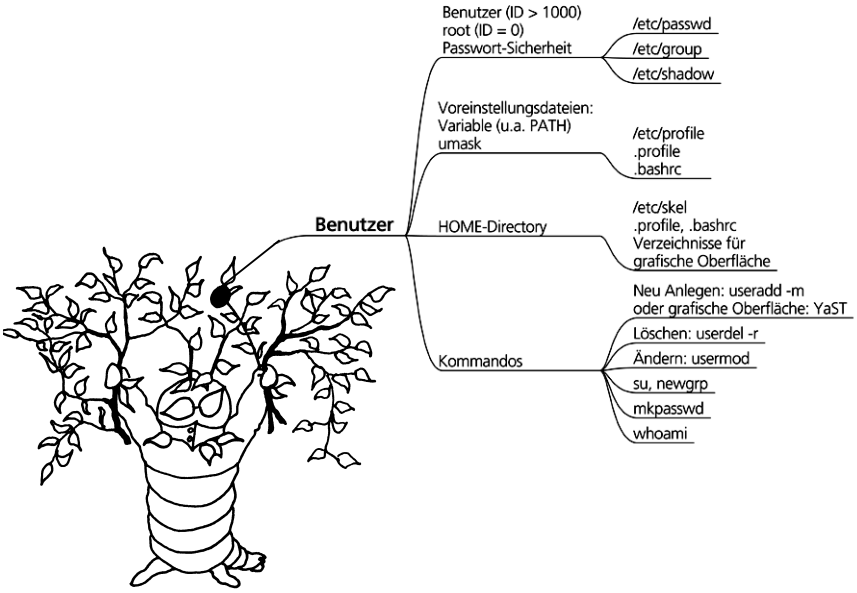
Verzeichnis/Datei	Erläuterung
$HOME/.bashrc	Benutzer-Voreinstellungsdatei für die interaktive Bash
$HOME/.cshrc	Benutzer-Voreinstellungsdatei für die C-Shell

1. Hierzu finden Sie einen guten Artikel in der Online-Dokumentation von ›selflinux‹ unter *file:/usr/share/doc/selflinux/html/passwoerter01.html#d37e69* (nachzuinstallieren von der SUSE-CD oder über Internet [55]).

Verzeichnis/Datei	Erläuterung
$HOME/.profile	Benutzer-Voreinstellungsdatei für das Login (Korn-Shell und Bash)
/etc/group	Systemdatei für die Gruppenzuordnung
/etc/passwd	Systemdatei für die Benutzerverwaltung
/etc/profile	Systemdatei für Voreinstellungen der Benutzer (Variable, Zugriffsrechte etc.)
/etc/shadow	Systemdatei für die Passwörter der Benutzer
/etc/skel	Musterverzeichnis für neue Benutzer

5.11 Rückblick in Stichworten

Die Stichwörter zu dem Thema Benutzer, die in der Einleitung unter dem Wissensbaum für Systemverwalter aufgeführt waren, sollten Ihnen nun die entsprechenden Abläufe und Zusammenhänge in Erinnerung rufen:



http://www.springer.com/978-3-540-20399-5

Linux-Systemadministration
Grundlagen, Konzepte, Anwendung
Wolfinger, C.; Gulbins, J.; Hammer, C.
2005, XIV, 482 S., Hardcover
ISBN: 978-3-540-20399-5