
Caldera Systems

OpenLinux eServer 2.3
Handbuch für
Systemadministratoren

Caldera Systems
240 West Center Street
Orem, UT 84057

KAPITEL 1

Einführung in OpenLinux eServer 7

- Welche Funktionen bietet Ihnen
OpenLinux eServer? 7
- Wer ist Caldera Systems? 9
- Technischer Support 9
- Über dieses Handbuch 11
- Wenn Sie Fehler in dieser Dokumentation finden 12

KAPITEL 2

Installieren von OpenLinux eServer 13

- Auswählen einer Installationsmethode 14
 - Die Standardinstallation 14*
 - Unbeaufsichtigte Installation mit Hilfe des Lizard 14*
- Erstellen der Installationsdisketten 14
 - Erstellen der Installations-/Bootdiskette 14*
 - Erstellen der Moduldiskette 15*
- Durchführen einer unbeaufsichtigten Installation 16
 - Erstellen eines Installationsservers 16*
 - Verwenden der unbeaufsichtigten Installation mit dem Lizard 17*
- Installieren von OpenLinux eServer 19
 - Abrufen von Hilfe während der Installation 19*
 - Mauskonfiguration 19*
 - Konfigurieren des Grafiksystems 20*
 - Auswählen der Partition für die Installation 25*
 - Vorbereiten einer Festplatte mit der Option Benutzerdefiniert 27*
 - Auswählen einer Festplatte für OpenLinux eServer 29*
 - Definieren des OpenLinux eServer Dateisystems 30*
 - Vorbereiten der OpenLinux eServer Partitionen 31*
 - Auswählen der zu installierenden Komponenten 33*
 - Testen der Soundkarte 34*
 - Erstellen von Benutzer-Accounts 35*
 - Festlegen der Netzwerkeinstellungen 38*
 - Installieren des Bootloaders 40*
- Abschließen der Installation 42
 - Konfigurieren von Webmin 45*

KAPITEL 3

Starten und Stoppen von OpenLinux eServer 47

Booten von Linux 47

Systeminitialisierung 48

*Verwenden von Webmin für das Steuern der
Systeminitialisierung 49*

Verwenden von LILO 55

Modifizieren des aktuellen Kernels 56

Erstellen eines neuen Bootkernels 57

Ändern der globalen Bootoptionen 58

Analysieren von /etc/lilo.conf 60

KAPITEL 4

Verwalten des Kernels 63

Neukompilieren des Kernels 63

Verwenden von Kernelmodulen 65

Manuelles Laden von Kernelmodulen 66

Automatisches Laden von Kernelmodulen 67

KAPITEL 5

Systemkonfiguration und -administration 69

Verwalten von Benutzern und Gruppen 69

Verwalten von Benutzern und Gruppen mit Webmin 70

Zentrales Verwalten von Benutzern und Gruppen
mit NIS 73

*Konfigurieren von OpenLinux eServer als
NIS-Client 75*

*Konfigurieren von OpenLinux eServer als
NIS-Server 76*

Webmin Tools zur Systemadministration 78

Verwalten von Cron-Jobs 78

Verwalten von Festplattenpartitionen 81

Verwalten von Dateisystemen 83

Prozesssteuerung 86

Software-Paketmanagement 90

Fortgeschrittene Webmin-Konfiguration 92

KAPITEL 6

Tools zur Netzwerküberwachung 97

- Verwenden von Sniffit 97
- Verwenden von Netwatch 102
- Verwenden von tcpdump 104
- Verwenden von Cheops 108
- Verwenden von Ntop 108
- Verwenden von Scotty 109
- Zusätzliche Ressourcen 110
 - Webseiten 110*
 - Linux Documentation Project 110*
 - Bücher 111*

KAPITEL 7

Verwenden von KDE 113

- Speicherort von KDE-Dateien 113
- KDE-Funktionen 114
 - Anpassen des KDE-Desktops 116*
- Zusätzliche Ressourcen 117

KAPITEL 8

Konfigurieren von Internet- und Intranetdiensten 119

- Konfigurieren eines Mailservers 120
 - Mail Aliases 121*
 - Local Domains 122*
 - Domain Masquerading 122*
 - Trusted Users 123*
 - Domain Routing 124*
 - Relay Domains 124*
 - Mail Queue 125*
- Einrichten eines Webservers 125
 - Apache-Konfiguration unter Verwendung von Webmin 126*
- Einrichten eines FTP-Servers 127
- Einrichten eines Domain Name Servers 129
- Konfigurieren eines PPP-Einwahlservers 133

Einrichten eines BOOTP/DHCP-Servers 135

Allgemeine Parameter 136

Die subnet-Anweisung 136

Die shared-network-Anweisung 137

Verwenden von BOOTP mit DHCP 137

Zusätzliche Ressourcen 138

Webseiten 138

Linux Documentation Project 138

Books 139

KAPITEL 9

Konfigurieren eines Druckservers 141

Konfigurieren eines Druckservers 141

KAPITEL 10

Konfigurieren von MySQL 145

Die Standardkonfiguration 145

Verbinden mit einem MySQL-Server 147

Hinzufügen von Benutzern zu einem
MySQL-Server 148

Erstellen einer neuen MySQL-Datenbank 149

Zusätzliche Ressourcen 150

Bücher 150

Websites 150

KAPITEL 11

Sicherheit 151

Herstellen der physischen Sicherheit 151

Herstellen der Netzwerksicherheit 152

Kennwortsicherheit 152

Einschränken von Berechtigungen und Zugriff 152

Überwachen des Systems 153

Firewall und Paketfilter 153

Kernelunterstützung für Paketfilter 154

Konfigurieren eines Paketfilters 154

Speichern des Paketfilters 155

IP-Masquerading – Kurzübersicht	156
Geläufige Firewall-Setups	156
<i>Privates Netzwerk Traditionelle Proxies</i>	157
<i>Privates Netzwerk Transparente Proxies</i>	157
<i>Privates Netzwerk Masquerading</i>	158
<i>Öffentliches Netzwerk</i>	159
TCP-Wrapper	159
Secure Shell (SSH)	161
Secure Socket Layer (SSL)	161
Pretty Good Privacy (PGP)	161
Zusätzliche Informationen	162
<i>Linux Documentation Project</i>	162
<i>Websites</i>	162
<i>Bücher</i>	162
Index	163

KAPITEL 1

Einführung in OpenLinux eServer

Willkommen bei OpenLinux eServer von Caldera Systems, dem fortschrittlichsten Linux-Betriebssystem auf dem Markt! Caldera genießt einen hervorragenden Ruf als Anbieter einer Distribution, die für E-Business bestens geeignet ist, und hat OpenLinux eServer von Grund auf als schnelle, sichere und einfach zu administrierende Serverplattform entwickelt und konfiguriert.

Dieses Handbuch begleitet Sie durch den grafischen Installationsvorgang von OpenLinux eServer und unterstützt Sie bei der Feinabstimmung Ihrer Linux-Konfiguration, damit Sie ein System erhalten, das genau auf die besonderen Anforderungen Ihrer Rechnerumgebung abgestimmt ist. Aber zunächst möchten Sie sicher etwas mehr über OpenLinux eServer erfahren.

Welche Funktionen bietet Ihnen OpenLinux eServer?

OpenLinux eServer wurde als Serverplattform konzipiert. Um diesem Anspruch gerecht zu werden, wurden folgende Funktionen implementiert:



- Konfigurierbare Kernelparameter ermöglichen die Berücksichtigung spezieller Serveranforderungen.
- RAID-Unterstützung auf Hardware- und Softwareebene wurde in den Kernel kompiliert.
- Disk Quota Unterstützung ist standardmäßig aktiviert.
- Fast alle Pakete in OpenLinux eServer wurden für Pentium II oder bessere Prozessoren kompiliert und optimiert.
- Zusätzliche PAM-Module (Pluggable Authentication Modules) stehen zur Verfügung, um die Sicherheit des Systems noch weiter zu erhöhen.
- Der Kernel wurde modifiziert, um bis zu 4 GB physikalischen Hauptspeicher (RAM) zu unterstützen.
- Die standardmäßigen Einstellungen für die Systemsicherheit gewährleisten einen konsequenteren Schutz Ihres Systems als bei anderen Linux-Distributionen.

OpenLinux eServer wird mit zahlreichen Anwendungen weiterer Anbieter ausgeliefert, mit deren Hilfe Sie Ihr System als optimale Serverplattform nutzen können. Eine Liste mit einigen dieser Anwendungen finden Sie in Tabelle 1:

TABELLE 1. Anwendungen weiterer Anbieter im Lieferumfang von OpenLinux eServer

Anwendung	Beschreibung
AppWatch	Anwendungsüberwachung
Ethereal	Netzwerküberwachung
Scotty	Grafische Darstellung von Netzwerkinformationen
OpenLDAP	Open Source LDAP-Implementierung
Cheops	SNMP Management-Tool
PHP3	Tool zum dynamischen Erstellen von Apache-kompatiblen Webseiten
Squid	Web-Proxyserver und Cache-Manager
Webmin	Leistungsfähiges und benutzerfreundliches Administrationstool, das über den Webbrowser bedient wird

Wer ist Caldera Systems?

Caldera Systems ist einer der ältesten Linux-Anbieter. Caldera Systems wurde im Jahr 1994 unter der Bezeichnung Caldera, Inc. gegründet und ist seitdem ein führender Anbieter von Linux-Technologie für den geschäftlichen und privaten Bereich. Caldera Systems bietet die folgenden Dienstleistungen und Produkte an:

- Zwei Linux-Distributionen auf der Grundlage eines von Caldera gepflegten Quellcodes. Neben OpenLinux für den Desktopbereich bietet Caldera auch OpenLinux eServer an, zwei Produkte, die den höchsten Qualitätsansprüchen genügen können, die an kommerzielle Software gestellt werden.
- Das erste umfassende weltweite Vertriebsnetz mit Beratungsdienstleistungen im Linux-Bereich
- Schulungen und technische Ausbildungsprogramme
- Technischer Support in Form einzelner Supportleistungen oder auf Vertragsbasis

Der Hauptsitz von Caldera Systems befindet sich in Orem, Utah (USA). Die europäische Niederlassung hat ihren Sitz in Erlangen (Deutschland).

Technischer Support

Durch den Kauf von OpenLinux eServer haben Sie Anspruch auf technischen Support über Internet erworben. Die Supportleistungen unterstützen Sie bei der Installation des Betriebssystems und stellen sicher, dass die Standardkonfiguration von OpenLinux eServer erfolgreich auf Ihrem System eingerichtet werden kann und Sie somit eine sichere und stabile Serverumgebung erhalten. Dieser Installationssupport umfasst 90 Tage mit maximal fünf Beratungseinheiten (Incidents).

Wenn Sie technischen Support benötigen, sollten Sie sich zuerst informieren, ob in der Knowledge Base auf der Website von Caldera Systems unter <http://support.calderasystems.com/> bereits eine Antwort auf Ihre Frage enthalten ist. Wenn Sie in der Knowledge Base keine Lösung finden, können Sie eine E-Mail an die Experten für technischen Support von Caldera senden. Hierzu steht Ihnen der Abschnitt Personal Assistance in der Knowledge Base zur Verfügung. Bitte geben Sie bei Ihrer Frage die Seriennummer Ihrer Kopie von OpenLinux eServer an, um sicherzustellen, dass Ihre Anfrage rasch bearbeitet werden kann.

Ab erfolgter Registration erhalten Sie 30 Tage lang kostenlosen telefonischen Support oder 90 Tage lang kostenlosen Support per E-Mail. In Tabelle 1 sind die Telefonnummern, die Zeiten sowie die E-Mail-Adressen für den Support aufgelistet.

TABELLE 2. Internationaler Technischer Support

Ort	Support- Telefonnummer	E-Mail-Adresse für den Support	Telefonische Support-Zeiten
USA	801-443-1000	support@calderasystems.com	Montag bis Freitag 7.00–19.00 Uhr (Mountain US-Zeit)
Deutschland	030-726238-88	support@caldera.de	Montag bis Freitag 10.00–17.00 Uhr
Irland	61-702033	europe.support@calderasystems.com	Montag bis Freitag 8.30–17.30 Uhr
Europa (außer Deutschland)	353-61-702033	europe.support@calderasystems.com	
Japan	03-3797-9050	support@openlinux.ne.jp	Montag bis Freitag von 10.00–12.00 Uhr und 13.00–18.00 Uhr
Korea	2-569-1999	service@calderasystems.co.kr	Montag bis Freitag von 9.00–12.00 Uhr und 13.00–18.00 Uhr

Sehen Sie bitte regelmäßig unter: <http://www.calderasystems.com/support/> nach den aktuellen örtlichen Support-Telefonnummern

Der Installationssupport ist für folgende Bereiche verfügbar:

- CD-Installation von OpenLinux eServer auf unterstützter Hardware (weitere Informationen finden Sie in Anhang A in diesem Handbuch und in der Hardware-Kompatibilitätsliste unter <http://www.calderasystems.com/support/hardware.html>).
- Grundlegende Konfiguration der grafischen Benutzeroberfläche (Xfree86)
- Grundlegende Netzwerkkonfiguration, einschließlich TCP/IP, IPX und NetWare-Client
- Grundlegende Konfiguration eines E-Mail-Clients
- Grundlegende Konfiguration eines FTP-Servers
- Grundlegende Konfiguration eines Webserver
- Grundlegende Konfiguration eines Druckserver

Wenn Sie telefonische Supportleistungen auf Einzelfallbasis erwerben oder einen längerfristigen Supportvertrag abschließen möchten, sollten Sie die Website von

Caldera Systems unter <http://www.calderasystems.com/support/index.html> besuchen. Dort finden Sie nähere Informationen und Preisangaben.

Über dieses Handbuch

Dieses Handbuch für Systemadministratoren soll Ihnen beim Installieren und Konfigurieren Ihres OpenLinux eServer Systems helfen. In Kapitel 1, das Sie gerade lesen, erhalten Sie Informationen über die wichtigsten Funktionen von OpenLinux eServer. Kapitel 2 leitet Sie durch den grafischen Installationsvorgang für OpenLinux eServer und beschreibt die Konfiguration von Webmin, dem browsergestützten Tool zur Systemadministration. In Kapitel 3 werden dann die Abläufe bei der Systeminitialisierung und beim Booten von Linux beschrieben. Kapitel 4 wiederum enthält grundlegende Informationen zum Verwalten des Kernels, einschließlich dem Neukompilieren des Kernels und Verwenden ladbarer Kernel-module.

Kapitel 5 befasst sich mit verschiedenen Tätigkeiten im Rahmen der Systemadministration wie der Verwaltung von Benutzern und Gruppen. Sie erfahren in diesem Kapitel auch, wie Sie die zahlreichen Tools von Webmin zum System- und Netzwerkmanagement verwenden können. In Kapitel 6 werden dann die Netzwerküberwachungstools näher besprochen, die im Lieferumfang von OpenLinux eServer enthalten sind, darunter Sniffit, Netwatch und tcpdump. Nach einer kurzen Einführung in KDE in Kapitel 7 führt Sie Kapitel 8 in die Konfiguration einer ganzen Reihe von Internet- und Intranetdiensten ein. Im Einzelnen werden die folgenden Themen behandelt:

- Einrichten eines Mailservers
- Einrichten eines Webservers
- Einrichten eines FTP-Servers
- Einrichten eines Domain Name Servers
- Einrichten eines Einwahlservers (PPP)
- Einrichten eines BOOTP- und DHCP-Servers

In Kapitel 9 lernen Sie, wie Sie mit OpenLinux eServer Datei- und Druckdienste in heterogenen Umgebungen mit mehreren Plattformen zur Verfügung stellen können. Für das Bereitstellen von netzwerkweiten Druckdiensten wird LPR verwendet, während SAMBA für die Integration von Windows 9x, Windows NT und Windows 2000-Systemen in Ihr Linux-Netzwerk eingesetzt wird. Darüber hinaus erfahren Sie in diesem Kapitel, wie Sie NFS konfigurieren müssen, um im gesamten Netzwerk Dateien zur Verfügung stellen zu können.

OpenLinux eServer ist eine hervorragende Plattform für das Bereitstellen von Datenbankdiensten in Ihrem Netzwerk. In Kapitel 10 wird erläutert, wie die relationale Datenbank MySQL eingerichtet wird.

Beim Konfigurieren eines Servers sollten Sicherheitsüberlegungen im Mittelpunkt stehen, insbesondere dann, wenn dieser mit dem Internet verbunden ist. Kapitel 11 enthält daher wichtige Informationen zum Sichern Ihres Servers gegen Angriffe durch Hacker. Obwohl bei der standardmäßigen Installation von OpenLinux eServer bereits ein sicheres System eingerichtet wird, sollten die Systemadministratoren die Sicherheit durch Feinabstimmen der Konfiguration noch weiter erhöhen. Sie erfahren hierzu, welche grundlegenden Regeln Sie für das Sichern Ihres Systems beachten sollten und wie Sie diese dann mit Hilfe von Firewalls, Proxydiensten, TCP-Wrappern und verschiedenen Verschlüsselungstools in der Praxis umsetzen können.

Anhang A dieses Handbuchs enthält eine Liste mit Hardwarekomponenten, die mit OpenLinux eServer von Caldera Systems kompatibel sind.

Wenn Sie Fehler in dieser Dokumentation finden

Wir haben uns bemüht, beim Abfassen dieses Handbuchs Fehler zu vermeiden. Allerdings können wir nicht vollständig ausschließen, dass uns dennoch einzelne Fehler unterlaufen sind oder bei bestimmten Themen noch gewisse Unklarheiten bestehen. Wenn Sie also der Meinung sind, dass die vorliegende Dokumentation noch verbessert werden könnte, sollten Sie die folgende Internetadresse aufrufen, um die aktuellsten Informationen zu Ihrem Produkt abzurufen:

`http://www.calderasystems.com/support/docs/`

Wir würden uns auch über Vorschläge und Kommentare zu unseren Handbüchern freuen. Bitte senden Sie uns Ihre E-Mails an `docs@calderasystems.com`.

KAPITEL 2

Installieren von OpenLinux eServer

In diesem Kapitel wird beschrieben, wie OpenLinux eServer mit Hilfe des Installationsprogramms, des so genannten Linux Installation Wizard (LIZARD), installiert wird. Um OpenLinux eServer installieren zu können, müssen Sie mindestens über eine Partition verfügen, die ausschließlich von Linux genutzt wird. Wenn diese Partition noch nicht existiert, können Sie diese während der Installation mit Hilfe des in LIZARD enthaltenen Partitionierungstools erstellen. In diesem Kapitel werden drei Installationsmethoden behandelt:

- Verwenden der standardmäßigen Installationsmethode für das Installieren von OpenLinux eServer auf einem einzelnen Server über ein CD-ROM-Laufwerk
- Durchführen einer unbeaufsichtigten Installation
- Installieren von einem Installationsserver aus

Auswählen einer Installationsmethode

Die Standardinstallation

Die meisten Benutzer werden vermutlich die standardmäßige Methode für das Installieren von OpenLinux eServer verwenden, bei der OpenLinux eServer auf einem einzelnen System über die CD-ROM installiert wird. Sie können hierbei entweder direkt von CD-ROM (falls Ihr System über ein bootfähiges CD-ROM-Laufwerk verfügt und diese Bootoption aktiviert ist) oder von Diskette booten. Wenn Sie die Installation mit Hilfe einer Installationsdiskette starten möchten, finden Sie im Abschnitt "Erstellen der Installationsdisketten" weitere Anweisungen.

Unbeaufsichtigte Installation mit Hilfe des Lizard

Bei der unbeaufsichtigten Installation mit Hilfe des Lizard ist es möglich, den Installationsvorgang automatisch und ohne Eingriffe durch den Benutzer ablaufen zu lassen. Dabei werden die zu aktualisierenden Pakete berücksichtigt und alle erforderlichen Aktionen zum Abstimmen und Konfigurieren des Systems nach erfolgter Installation ausgeführt. Die unbeaufsichtigte Installation kann mit einer Installationsdiskette oder über ein Netzwerk und einen Installationsserver durchgeführt werden.

Erstellen der Installationsdisketten

Um die standardmäßige Installation mit Installationsdisketten durchführen zu können, müssen Sie eine Installations-/Bootdiskette und eine Moduldiskette erstellen. Die Moduldiskette ist möglicherweise nicht erforderlich. Das Installationsprogramm LIZARD wird Sie zum Einlegen der Moduldiskette auffordern, falls diese benötigt werden sollte. Wenn Sie keine Installationsdisketten erstellen müssen, können Sie gleich im Abschnitt Installieren von OpenLinux eServer weiterlesen.

Erstellen der Installations-/Bootdiskette

Gehen Sie wie folgt vor, um die Installations-/Bootdiskette auf einem DOS- oder Windows-System zu erstellen:

1. Legen Sie eine leere 3½ Zoll-Diskette in Ihr Diskettenlaufwerk ein.
2. Wechseln Sie in einem Fenster mit einer MSDOS-Eingabeaufforderung in das Verzeichnis `\COL\LAUNCH\FLOPPY`.

3. Geben Sie `\COL\TOOLS\RAWRITE\RAWRITE3.COM` ein.
4. Geben Sie `INSTALL.144` ein.
5. Geben Sie den Laufwerksbuchstaben Ihres Diskettenlaufwerks ein, und drücken Sie die Eingabetaste.
6. Drücken Sie die Eingabetaste, um fortzufahren.
7. Schließen Sie `RAWRITE3`.

Gehen Sie wie folgt vor, um die Installations-/Bootdiskette unter Linux zu erstellen:

1. Legen Sie eine leere 3½ Zoll-Diskette in Ihr Diskettenlaufwerk ein.
2. Mounten Sie Ihr CD-ROM-Laufwerk.
3. Wechseln Sie in das Verzeichnis `col/launch/floppy` auf der CD.
4. Geben Sie `dd if=./install.144 of=/dev/fd0` ein, wobei `/dev/fd0` die Bezeichnung Ihres Diskettenlaufwerks unter Linux ist.

Erstellen der Moduldiskette

Gehen Sie wie folgt vor, um die Moduldiskette auf einem DOS- oder Windows-System zu erstellen:

1. Legen Sie eine leere 3½ Zoll-Diskette in Ihr Diskettenlaufwerk ein.
2. Wechseln Sie in einem Fenster mit einer MSDOS-Eingabeaufforderung in das Verzeichnis `\COL\LAUNCH\FLOPPY`.
3. Geben Sie `\COL\TOOLS\RAWRITE\RAWRITE3.COM` ein.
4. Geben Sie `MODULES.144` ein.
5. Geben Sie den Laufwerksbuchstaben Ihres Diskettenlaufwerks ein, und drücken Sie die Eingabetaste.
6. Drücken Sie die Eingabetaste, um fortzufahren.
7. Schließen Sie `RAWRITE3`.

Gehen Sie wie folgt vor, um die Moduldiskette unter Linux zu erstellen:

1. Legen Sie eine leere 3½ Zoll-Diskette in Ihr Diskettenlaufwerk ein.
2. Mounten Sie Ihr CD-ROM-Laufwerk.
3. Wechseln Sie in das Verzeichnis `col/launch/floppy` auf der CD.
4. Geben Sie `dd if=./modules.144 of=/dev/fd0` ein, wobei `/dev/fd0` die Bezeichnung Ihres Diskettenlaufwerks unter Linux ist.

Durchführen einer unbeaufsichtigten Installation

Bevor Sie eine unbeaufsichtigte Installation durchführen können, müssen Sie erst einen Installationsserver erstellen. Im nächsten Abschnitt mit der Bezeichnung Erstellen eines Installationsservers wird dieser Vorgang näher beschrieben. Nachdem Sie einen Installationsserver erstellt haben, können Sie diesen für eine unbeaufsichtigte Installation von CD-ROM oder für eine serverbasierte Installation verwenden.

Erstellen eines Installationsservers

Bei Verwendung eines Installationsservers können Sie OpenLinux eServer auf jedem Computer in Ihrem LAN über das Netzwerk installieren. Leider steht diese Funktion aus Copyright-Gründen jedoch nicht für kommerzielle Anwendungen zur Verfügung. Hier ist ein Überblick über den gesamten Vorgang:

- Kopieren Sie den Inhalt der Installations-CD auf den Installationsserver.
- Konfigurieren Sie den Installationsserver als NFS-Server.
- Konfigurieren Sie den Installationsserver als DHCP-Server.
- Erstellen Sie ein individuelles Installationsprofil, falls erforderlich.
- Booten Sie die Clients, auf denen Linux installiert werden soll, mit Hilfe einer Installationsdiskette.

Das Erstellen und Konfigurieren eines Installationsservers wird im Folgenden ausführlich erläutert.

1. Erstellen Sie auf dem Installationsserver zwei Verzeichnisse mit den Namen `/install/cd1` und `/install/cd2`. Geben Sie hierzu folgende Befehle ein

```
# mkdir /install/cd1
# mkdir /install/cd2
```
2. Kopieren Sie den gesamten Inhalt der OpenLinux eServer Kernel und Installations-CD-ROM in `/install/cd1`. Wenn Sie serverbasierte Installationen unter Verwendung des Quellcodes ermöglichen möchten, kopieren Sie analog den Inhalt der OpenLinux eServer Quellcode-CD-ROM in `/install/cd2`. Nach dem Mounten der CD-ROM können Sie mit dem folgenden Befehl den Kernel und die Installations-CD-ROM auf die Festplatte kopieren:

```
# cp -r -v /mnt/cdrom/* /install/cd1
```
3. Exportieren Sie das Installationsverzeichnis unter Verwendung von NFS, um allen Benutzern Zugriff darauf zu ermöglichen. Wenn Ihr Domänenname `bigbiz.com` lautet, müssen Sie die folgende Zeile in die Datei `/etc/exports` auf

dem Installationsserver einfügen (möglicherweise müssen Sie diese Datei erst erstellen):

```
/install *.scary.org(ro,no_root_squash)
```

4. Starten Sie den NFS-Dämon (`nfsd`) neu, damit das exportierte Verzeichnis berücksichtigt wird.
5. Fügen Sie einen Eintrag in `/etc/dhcp.conf` für jeden Client ein, auf dem Sie Linux installieren möchten. Ein Eintrag könnte beispielsweise wie folgt aufgebaut sein:

```
host phantom {  
    hardware ethernet 00:01:E3:FB:34:35;  
    fixed-address 192.168.1.3;  
    options host-name "phantom.scary.org";  
    next-server 192.168.1.1;  
    filename "/install/cd1";  
}
```

Mit diesem Eintrag werden die Einstellungen für einen Clienthost mit der Bezeichnung `maple` vorgenommen. Die MAC-Adresse lautet `00:01:E3:FB:34:35`. Dem Client wird die Adresse `192.168.1.3` zugewiesen. Der vollständige Domänenname lautet `maple.bigbiz.com`. Der Eintrag `next-server` gibt die Adresse des Installationsservers (`192.168.1.1`) an, und die Optionen unter `filename` enthalten die Angabe zum Speicherort des Inhalts der CD-ROM (`/install/cd1`).

6. Starten Sie den DHCP-Serverdämon neu (`dhcpcd`), um die neuen Einträge in `/etc/dhcp.conf` zu aktivieren.

Wenn ein in `/etc/dhcp.conf` aufgeführter Client von einer Installationsdiskette bootet, erkennt er unter Verwendung von DHCP den Installationsserver und das Quellenverzeichnis, so dass die Installation fortgeführt werden kann.

Verwenden der unbeaufsichtigten Installation mit dem Lizard

Die Verwendung eines Installationsservers, wie sie im letzten Abschnitt beschrieben wurde, empfiehlt sich vor allem dann, wenn Sie mehrere Installationen in Ihrem Netzwerk durchführen müssen. Wenn Sie die unbeaufsichtigte Installationsmethode mit dem Lizard verwenden, können Sie darüber hinaus noch auf komfortable Weise Konfigurationseinstellungen vorher festlegen, so dass der Installationsvorgang nicht überwacht werden muss. Zu diesem Zweck müssen Sie eine Datei mit Regeln erstellen, die bei der Installation berücksichtigt werden sollen. Zuerst müssen Sie den Installationsserver auf die im vorherigen Abschnitt beschriebene Weise erstellen. Als nächstes müssen Sie folgende Schritte durchführen:

- Konfigurieren des Installationsservers für das Ausführen einer unbeaufsichtigten Installation mit dem Lizard
- Erstellen einer Datei mit Regeln und eines Installationsprofils
- Testen der Installation durch Vornehmen einer Installation auf einem Client

In den folgenden Schritten wird die unbeaufsichtigte Installation unter Verwendung des Lizard detailliert beschrieben:

1. Legen Sie auf dem Installationsserver ein Verzeichnis mit der Bezeichnung `lizard` an. Dieses Verzeichnis muss sich im gleichen Verzeichnis wie die beiden Unterverzeichnisse `cd1` und `cd2` befinden. Wenn wir das Beispiel aus dem vorherigen Abschnitt fortführen, müssten Sie folgenden Befehl eingeben:

```
# mkdir /install/lizard
```
2. Erstellen Sie die folgenden Verzeichnisse und Dateien im gerade angelegten Verzeichnis `lizard`:
 - `rules`
 - `profile`
 - `etc/XF86Config`
 - `etc/pkgs.sel`
 - `bin/finish.sh`
 - `bin/start.sh`
 - `bin/instpkg`

In unserem Beispiel müssen Sie hierzu die folgenden Befehle ausführen:

```
# mkdir /install/lizard/rules
# mkdir /install/lizard/profile
# mkdir /install/lizard/etc
# touch /install/lizard/etc/XF86Config
# touch /install/lizard/etc/pkgs.sel
# mkdir /install/lizard/bin
# touch /install/lizard/bin/finish.sh
# touch /install/lizard/bin/start.sh
# touch /install/lizard/bin/instpkg
```

Installieren von OpenLinux eServer

Wenn die Installation beginnt, wird auf dem Bildschirm unter einer grafischen Oberfläche angezeigt, dass der Linux-Kernel vorbereitet wird und eine Überprüfung Ihres Systems stattfindet. Im Startbildschirm wird die Information ausgegeben, dass das Installationsprogramm LIZARD versucht, Informationen über die Hardware Ihres Computers abzurufen, um den Installationsvorgang entsprechend anpassen zu können. Insbesondere versucht das Installationsprogramm, das Medium zu ermitteln, das für die Installation verwendet werden soll. Die folgenden Quellen werden hierzu in der angegebenen Reihenfolge untersucht:

- Wenn die OpenLinux eServer Installations-CD-ROM bei der automatischen Hardwareerkennung gefunden wird, geht das Installationsprogramm davon aus, dass die Installation von CD-ROM erfolgen soll.
- Wenn die Installations-CD-ROM nicht gefunden wird, geht das Installationsprogramm davon aus, dass Sie die Installation über einen mittels NFS eingebundenen Installationsserver durchführen möchten. Daher versucht das Installationsprogramm, diesen Server im Netzwerk aufzufinden zu machen.

Nachdem das Installationsprogramm diesen Vorgang abgeschlossen hat, der einige Minuten in Anspruch nehmen kann, wird der Startbildschirm von LIZARD wie in Abbildung 1 angezeigt. Somit kann die Installation beginnen.

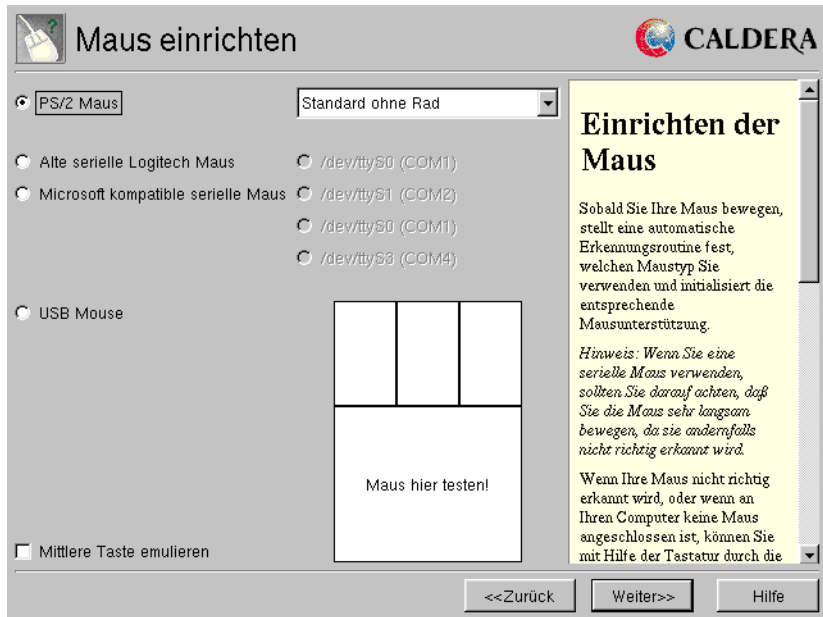
Abrufen von Hilfe während der Installation

Bei Verwendung des Installationsprogramms müssen Sie lediglich auf die Schaltfläche Hilfe klicken, um Informationen über die aktuell auf dem Bildschirm angezeigten Optionen zu erhalten. Die Schaltfläche Hilfe befindet sich in der unteren rechten Ecke in jedem Bildschirm des Installationsprogramms.

Mauskonfiguration

Mit dem Bildschirm zur Mauskonfiguration können Sie die Einstellungen für die Mauskonfiguration ändern oder die Maus manuell konfigurieren, falls diese nicht automatisch erkannt wurde. Ein geeignetes Mausprotokoll (PS/2, Microsoft, Logitech oder USB) und Gerät für die Maus (beispielsweise der verwendete serielle Port) sollten bereits ausgewählt sein. Um die angezeigte Einstellung zu ändern, wählen Sie die gewünschte Option in der Dropdown-Liste aus, die sich an der Oberseite des Bildschirms in der Mitte befindet. Aktivieren Sie das Kontrollkästchen Mittlere Taste emulieren links unten im Bildschirm, wenn Sie eine Maus mit zwei Tasten verwenden. Abbildung 1 zeigt Ihnen, wie dieser Bildschirm aussieht.

ABBILDUNG 1. Mauskonfiguration

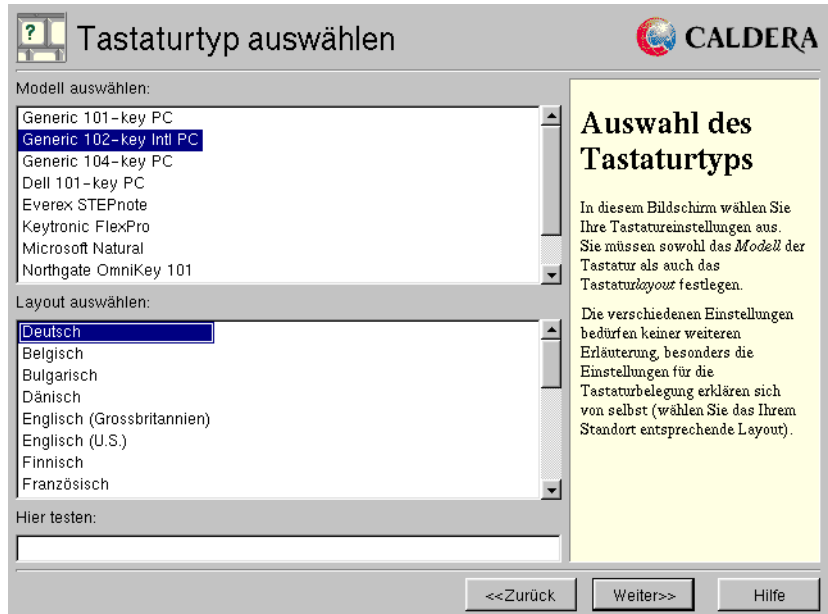


Wenn Probleme bei der Verwendung der Maus auftreten, können Sie mit Tabulatortaste, Pfeiltasten und Eingabetaste in diesem Bildschirm navigieren (und auch in allen anderen Bildschirmen, falls dies erforderlich sein sollte).

Konfigurieren des Grafiksystems

Mit Hilfe der nächsten Bildschirme wird das X Window Grafiksystem konfiguriert. Mit dem ersten Bildschirm (siehe Abbildung 2) können Sie Ihre Tastatur konfigurieren.

ABBILDUNG 2. X Server Tastaturkonfiguration



1. Wählen Sie aus, welches Tastaturmodell Sie verwenden.
2. Wählen Sie die Sprache und die Tastaturbelegung aus.
3. (Optional) Klicken Sie in das Textfeld Hier testen, um zu Testzwecken Sonderzeichen einzugeben, die nur in Ihrer Sprache vorkommen.
4. Klicken Sie zum Fortfahren auf Weiter.

Im nächsten Bildschirm (siehe Abbildung 3) können Sie Ihre Grafikkarte auswählen. In den meisten Fällen werden bei der Installation automatisch die richtigen Einstellungen ausgewählt, so dass Ihr Grafiksystem bereits ordnungsgemäß konfiguriert ist. Die Programme XF86Setup oder `lizardx` können nach der Installation verwendet werden, um das X Window System neu zu konfigurieren, falls bei der automatischen Erkennung Ihre Grafikhardware nicht richtig ermittelt wurde.

ABBILDUNG 3. Auswählen der Grafikkarte für den X Server

Grafikkarte auswählen

Kartentyp: Matrox MGA G200 AGP rev 3

Ihre Grafikkarte wurde erkannt. Die Analyse der Hardware-Details sollte risikolos möglich sein.

Details:

Video-RAM: 8192 KB

Taktrate: ☒ Programmierbar bis zu (MHz): 250

☐ Feste Frequenzen (MHz):

Analysieren

Sie können die Details für Ihre Karte hier eingeben oder die Werte durch Analysieren ermitteln lassen. Bitte beachten Sie, daß sich Ihr System beim Analysieren aufhängen kann.

Auswahl der Grafikkarte

OpenLinux eServer sollte das Fabrikat und Modell Ihrer Grafikkarte automatisch erkannt haben.

Wählen Sie die Schaltfläche "Analysieren" aus, um RAM und Taktrate der Karte automatisch ermitteln zu lassen.

ACHTUNG: Die Analyse kann Ihren Computer zum Absturz bringen!

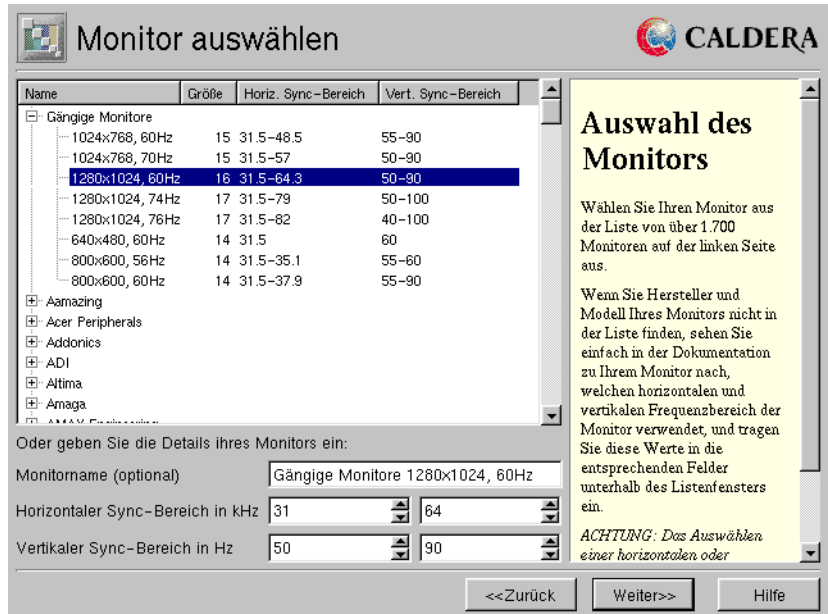
Falls die automatische Erkennung kein befriedigendes Ergebnis ermittelt, können Sie Ihre Karte manuell konfigurieren.

<<Zurück Weiter>> Hilfe

1. Klicken Sie auf die Schaltfläche Analysieren, um die Angaben zur Grafikkarte näher zu bestimmen, die für Ihr System angezeigt werden. Wenn die richtige Grafikkarte bereits angezeigt wird, klicken Sie ebenfalls auf die Schaltfläche Analysieren, zur genauen Bestimmung des Grafikspeichers.
2. Der Bildschirm wird kurzzeitig schwarz, bevor wieder derselbe Bildschirm wie zuvor angezeigt wird. Eine Meldung informiert Sie darüber, dass die Erkennung erfolgreich durchgeführt werden konnte.
3. Wenn bei der automatischen Erkennung nicht die richtige Größe des Grafikspeichers ermittelt werden kann, müssen Sie diesen Wert selbst eingeben.
4. Klicken Sie im Meldungsfeld auf OK.
5. Klicken Sie zum Fortfahren auf Weiter.

Im nächsten Bildschirm (siehe Abbildung 4) können Sie Ihre Monitoreinstellungen vornehmen. Es ist besonders wichtig, dass Sie hier die richtigen Werte angeben. Falls Sie eine Monitoreinstellung auswählen, die die tatsächliche Leistungsfähigkeit Ihres Monitors übersteigt, besteht nämlich die Gefahr einer Beschädigung Ihres Monitors.

ABBILDUNG 4. X Server Monitorkonfiguration



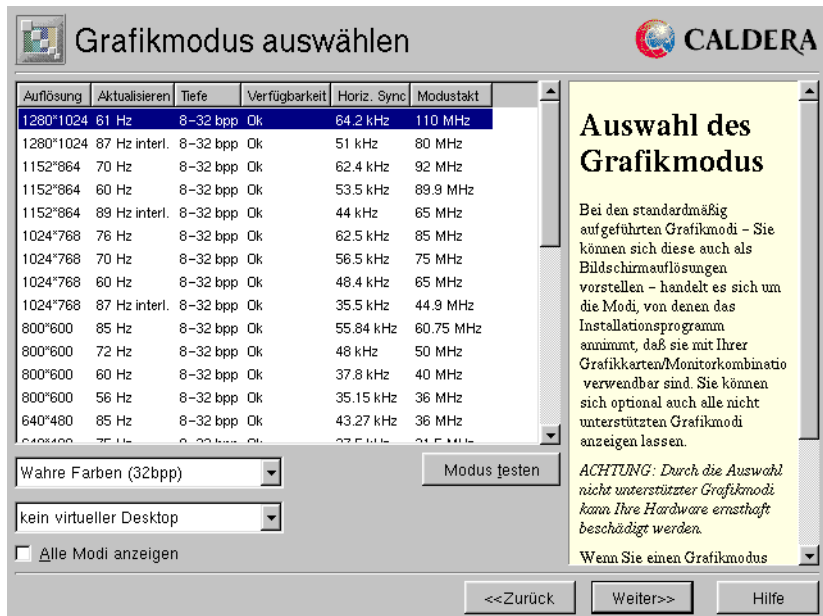
So konfigurieren Sie Ihren Monitor:

1. Blättern Sie in der Liste mit Monitoren, bis Sie den Markennamen Ihres Monitors finden.
2. Klicken Sie auf das Pluszeichen neben dem Markennamen, um eine Liste mit verschiedenen Modellen dieses Herstellers anzuzeigen.
3. Klicken Sie auf den Eintrag für das Monitormodell, das Sie verwenden.
4. In den Feldern unterhalb der Liste werden die Detailinformationen zum jeweils ausgewählten Monitor angezeigt.
5. Wenn Ihr Monitor nicht in der Liste enthalten ist, blättern Sie zum Anfang der Liste und wählen in der Liste mit typischen Monitoren den Eintrag aus, der den Fähigkeiten Ihres Monitors am besten entspricht. Wenn Sie die Dokumentation zu Ihrem Monitor zur Hand haben, sollten Sie die Werte für die vertikale und horizontale Bildwiederholfrequenz nachschlagen und mit Hilfe der Pfeiltasten in den entsprechenden Feldern des Bildschirms einstellen.
6. Klicken Sie zum Fortfahren auf Weiter.

Im nächsten Bildschirm (siehe Abbildung 5) können Sie einen Grafikmodus auswählen, der sich nach den Fähigkeiten Ihrer Grafikkarte und Ihres Monitors richten sollte. Der Grafikmodus legt folgende Einstellungen fest:

- Bildschirmauflösung
- Bildwiederholfrequenz (höhere Wiederholffrequenzen verringern das Flimmern des Monitors und reduzieren die Belastung der Augen)
- Farbtiefe (in Bit, wird weiter hinten beschrieben)
- Verfügbarkeit (wenn das Installationsprogramm berechnet, dass der Modus auf Ihrem System problemlos funktionieren sollte)

ABBILDUNG 5. Auswählen des Grafikmodus für den X Server



So legen Sie den Grafikmodus fest:

1. Klicken Sie auf den Grafikmodus, den Sie als Standardeinstellung verwenden möchten. Es werden nur Modi angezeigt, die von Ihrem Grafiksysteem unterstützt werden. Wenn Sie alle verfügbaren Modi anzeigen möchten, aktivieren Sie das Kontrollkästchen Alle Modi anzeigen.
2. Wählen Sie in der Dropdown-Liste eine Farbtiefe aus. Die meisten Benutzer wählen die höchste verfügbare Auflösung mit der jeweils höchsten Bildwieder-

holrate, die für die gewünschte Farbtiefe zur Verfügung steht. Die Anzahl der verfügbaren Farben hängt von der eingestellten Auflösung ab. Falls Ihre Grafikkarte nicht über ausreichend Speicher verfügt, müssen Sie sich entscheiden, ob Ihnen eine höhere Auflösung oder eine größere Farbtiefe wichtiger ist.

3. Wählen Sie in der Dropdown-Liste die Größe des virtuellen Desktops aus, oder legen Sie fest, dass Sie keinen virtuellen Desktop verwenden möchten. Die meisten Benutzer verwenden keinen virtuellen Desktop.

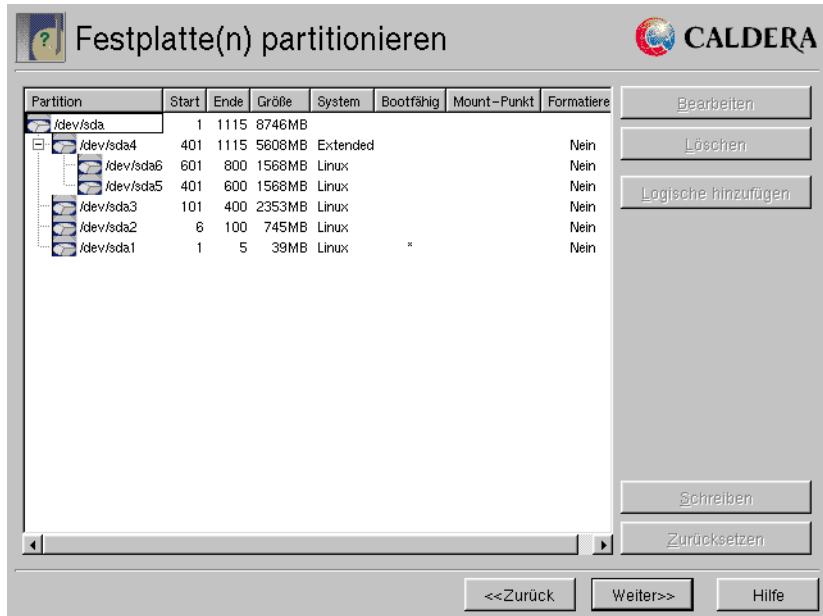
HINWEIS: Bei einem *virtuellen Desktop* handelt es sich um einen Desktop, dessen Größe den Bereich übersteigt, den Ihr Monitor vollständig darstellen kann. Um die nicht angezeigten Bereiche einzublenden, bewegen Sie die Maus in Richtung des ausgeblendeten Bereichs. Daraufhin wird die Bildschirmanzeige automatisch gescrollt, um diese Bereiche anzuzeigen.

4. Klicken Sie auf die Schaltfläche Modus testen, um den ausgewählten Modus für einen Zeitraum von 10 Sekunden zu testen.
5. Wenn der Test kein befriedigendes Ergebnis liefert oder die Bildschirmanzeige schwer zu erkennen ist, wählen Sie einen anderen Grafikmodus aus und testen diesen.
6. Klicken Sie zum Fortfahren auf Weiter.

Auswählen der Partition für die Installation

Mit Hilfe des nächsten Installationsbildschirms (siehe Abbildung 6) können Sie festlegen, wo OpenLinux auf Ihrer Festplatte installiert werden soll. Bevor eine der verfügbaren Optionen automatisch ausgewählt wird, durchsucht das Installationsprogramm Ihre Festplatten, um festzustellen, welche Partitionen erstellt wurden. Während dieses Suchvorgangs werden keine Daten auf Ihre Festplatte geschrieben.

ABBILDUNG 6. Auswählen der Partition für die Installation



- Wenn eine Linux-Partition gefunden wurde, wird die Option Vorbereitete Partition(en) automatisch ausgewählt.
- Wenn Sie lediglich über eine Linux-Partition verfügen, können Sie durch Klicken auf die Schaltfläche Weiter mit der Installation unter Verwendung der Option Vorbereitete Partition(en) fortfahren.
- Wenn das Installationsprogramm keine Linux-Partitionen findet, wird die Option Gesamte Festplatte ausgewählt. Sie können diese Option beibehalten, falls Sie Ihre gesamte Festplatte für die Installation von Linux verwenden möchten. Wenn Sie selbst festlegen möchten, wo OpenLinux installiert werden soll, sollten Sie hingegen die Option Benutzerdefiniert verwenden.
- Mit der Option Benutzerdefiniert können Sie auswählen, welche Partitionen auf welche Weise von OpenLinux verwendet werden sollen. Um diese Option verwenden zu können, sind gewisse Kenntnisse über Festplattenpartitionen und Gerätenamen unter Linux erforderlich. Im nächsten Abschnitt, Vorbereiten einer Festplatte mit der Option Benutzerdefiniert, wird die Verwendung des Bildschirms zum benutzerdefinierten Einrichten der Festplatte beschrieben. Dieser Bildschirm wird angezeigt, wenn Sie die Option Benutzerdefiniert auswählen und auf die Schaltfläche Weiter klicken.

ACHTUNG: Fast während des gesamten Installationsvorgangs können Sie mit Hilfe der Schaltfläche Zurück zu den vorherigen Bildschirmen des Installationsprogramms zurückkehren, um Ihre Einstellungen zu überprüfen oder zu ändern. Wenn Sie jedoch Ihre Festplatte bereits formatiert haben, können Sie durch Klicken auf die Schaltfläche Zurück das Formatieren *nicht* rückgängig machen.

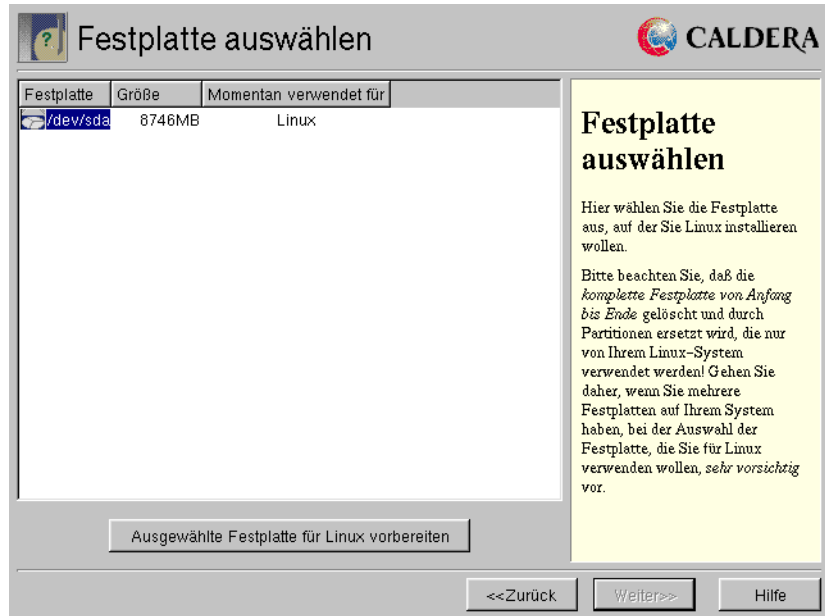
Die weitere Vorgehensweise richtet sich jetzt danach, welche Option Sie in diesem Bildschirm ausgewählt haben:

- Wenn Sie Benutzerdefiniert ausgewählt haben, sollten Sie sich den nächsten Abschnitt mit der Bezeichnung Vorbereiten einer Festplatte mit der Option Benutzerdefiniert durchlesen und dann mit dem Abschnitt Vorbereiten der Partitionen für OpenLinux eServer fortfahren.
- Wenn Sie die Option Gesamte Festplatte gewählt haben, können Sie gleich im Abschnitt Auswählen einer Festplatte für OpenLinux eServer weiterlesen und dann mit dem Abschnitt Definieren des OpenLinux eServer Dateisystems fortfahren.
- Wenn Sie die Option Vorbereitete Partition(en) ausgewählt haben, lesen Sie im Abschnitt Definieren des OpenLinux eServer Dateisystems weiter und fahren dann mit dem folgenden Abschnitt Vorbereiten der OpenLinux eServer Partitionen fort.

Vorbereiten einer Festplatte mit der Option Benutzerdefiniert

Die Option zum benutzerdefinierten Konfigurieren stellt Ihnen Tools zum Erstellen und Bearbeiten von Partitionen auf Ihrem System zur Verfügung. Verwenden Sie diesen Bildschirm (siehe Abbildung 7) für das Definieren der Partitionen auf Ihren Festplatten. Der Partitionstyp wird im Feld System angezeigt. Sie können jede Partition in Ihrem System auswählen und dann mit Hilfe der Schaltflächen Bearbeiten oder Löschen die aktuellen Einstellungen für diese Partition ändern.

ABBILDUNG 7. Benutzerdefiniertes Partitionieren



ACHTUNG: Vor der Verwendung des Tools zum benutzerdefinierten Partitionieren sollten Sie eine Sicherungskopie wichtiger Daten auf Ihrer Festplatte erstellen.

Bevor Sie durch Klicken auf Weiter zum nächsten Bildschirm wechseln, sollten Sie mit Hilfe der Schaltflächen Logische Partition hinzufügen und Bearbeiten die folgenden Partitionen erstellen:

- Eine Linux-Partition, auf der mindestens ausreichend Platz für die von Ihnen ausgewählte Installationsoption für OpenLinux eServer verfügbar ist. In Abhängigkeit von der ausgewählten Installationsoption sind hierfür zwischen 160 MB und 1,4 GB erforderlich.
- Eine Linux-Swap-Partition. Generell lässt sich feststellen, dass die Swap-Partition doppelt so groß wie der physikalisch vorhandene Hauptspeicher (RAM) Ihres Systems sein sollte.

Wenn Sie mit Linux-Dateisystemen vertraut sind, können Sie weitere Mountpoints für zusätzliche Linux-Partitionen auf Ihrer Festplatte definieren. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie eine Partition aus.

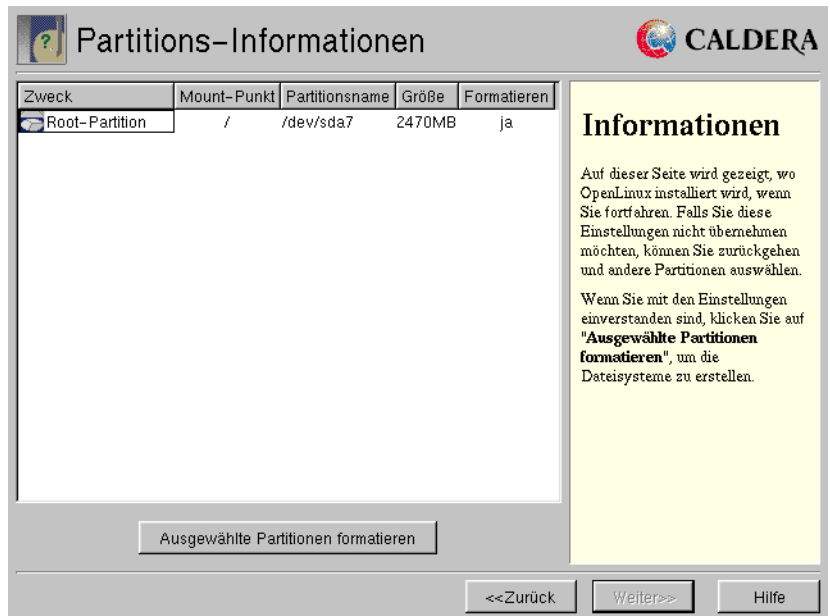
2. Klicken Sie auf Bearbeiten.
3. Wählen Sie einen Mountpoint in der Dropdown-Liste aus.

Wenn Sie einen Mountpoint verwenden möchten, der nicht in der Dropdown-Liste enthalten ist, können Sie diesen erst nach der Installation von OpenLinux definieren.

Auswählen einer Festplatte für OpenLinux eServer

Wenn Sie die Option Gesamte Festplatte ausgewählt und dann auf Weiter geklickt haben, können Sie im nächsten Bildschirm (siehe Abbildung 8) den Gerätenamen der Festplatte auswählen, auf der OpenLinux installiert werden soll.

ABBILDUNG 8. Auswählen einer Rootpartition



Im Feld Gerätename werden die Festplatten in Ihrem System unter Verwendung der unter Linux üblichen Gerätebezeichnungen aufgeführt. In Tabelle 3 erhalten Sie einen Überblick über die Gerätenamen bei Linux:

TABELLE 3. Gerätenamen für Festplatten unter Linux

Gerätename	Beschreibung
/dev/hda	Erste IDE-Festplatte
/dev/hdb	Zweite IDE-Festplatte
/dev/hdc	Dritte IDE-Festplatte (erstes IDE-Gerät am zweiten IDE-Controller, häufig für ein CD-ROM-Laufwerk verwendet)
/dev/hdd	Vierte IDE-Festplatte
/dev/sda	Erste SCSI-Festplatte
/dev/sdb	Zweite SCSI-Festplatte

ACHTUNG: Bitte beachten Sie, dass bei Verwendung der Option **Gesamte Festplatte** die Festplatte beim Formatieren vollständig gelöscht wird, bevor die Installation von OpenLinux erfolgt!

Sie können erst dann auf **Weiter** klicken und mit dem nächsten Bildschirm fortfahren, wenn Sie eine Linux Rootpartition und eine Swap-Partition erstellt haben. Die folgenden Schritte beschreiben, wie Sie mit diesem Bildschirm die benötigten Partitionen erstellen können:

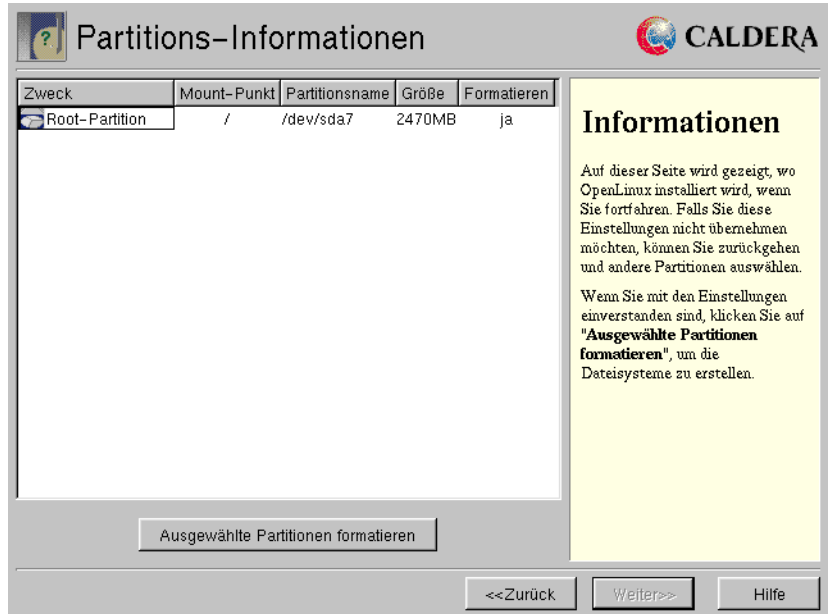
1. Klicken Sie auf den Gerätenamen der Festplatte, auf der OpenLinux eServer installiert werden soll.
2. Klicken Sie auf die Schaltfläche **Ausgewählte Festplatte für Linux vorbereiten**.
3. Die ausgewählte Festplatte wird partitioniert. Eine Linux-Partition und eine Linux Swap-Partition werden erstellt.
4. Klicken Sie zum Fortfahren auf **Weiter**.
5. Lesen Sie im nächsten Abschnitt mit der Bezeichnung **Definieren des OpenLinux eServer Dateisystems** weiter.

Definieren des OpenLinux eServer Dateisystems

Nachdem Sie die Festplattenpartitionen vorbereitet haben, müssen Sie jetzt die Rootpartition für Ihr neues Linux-Dateisystem festlegen. In diesem Bildschirm (siehe Abbildung 9) definieren Sie, welche Partition für Ihr OpenLinux Dateisystem verwendet werden soll. Sie können auch noch weitere Partitionen angeben, die von Linux genutzt werden sollen. Besonders wichtig ist in diesem Zusammen-

hang, dass die in der Spalte Verwendet als als Rootpartition bezeichnete Partition formatiert und OpenLinux in dieser Partition installiert wird.

ABBILDUNG 9. Definieren des Dateisystems

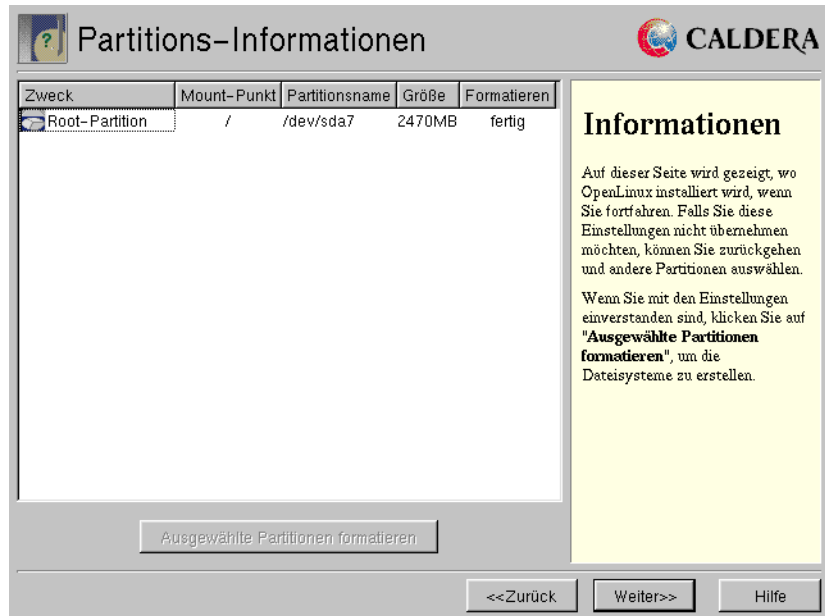


Wenn Sie auf Ihrem System über mehrere Linux-Partitionen verfügen, werden diese ebenfalls aufgelistet. Falls Sie eine andere Partition oder Festplatte für die OpenLinux Rootpartition verwenden möchten, klicken Sie auf den Namen der gewünschten Partition. Sobald Sie die richtige Partition ausgewählt haben, klicken Sie zum Fortfahren auf die Schaltfläche Weiter.

Vorbereiten der OpenLinux eServer Partitionen

In diesem Bildschirm (siehe Abbildung 10) werden die Partitionen aufgelistet, auf denen OpenLinux installiert wird. Sie können zugleich sehen, welche Partitionen formatiert werden. Diese Liste besteht mindestens aus einer Zeile mit einem Eintrag für eine Rootpartition mit dem Mountpoint /.

ABBILDUNG 10. Vorbereiten der Partitionen für die Installation



Mit Hilfe des Bildschirms mit den Zielpartitionen müssen Sie nun die ausgewählten Partitionen formatieren, bevor Sie fortfahren können. In der Spalte Formatierung wird bei allen Partitionen, die formatiert werden müssen, der Eintrag Ja angezeigt.

1. Bevor Sie mit der Installation fortfahren können, müssen Sie auf die Schaltfläche **Ausgewählte Partitionen formatieren** klicken.
2. Nach dem Klicken auf diese Schaltfläche wird das Feld **Formatierung** ständig aktualisiert und zeigt an, welche Partition gerade formatiert wird. Wenn das Formatieren abgeschlossen ist, werden Sie im Feld **Formatierung** hierüber informiert. Sie können dann auch auf die Schaltfläche **Weiter** klicken, die zuvor abgeblendet dargestellt wurde. (Neben der Partition für den virtuellen Speicher sollte ein Häkchen angezeigt werden, um zu bestätigen, dass diese Partition als Swap-Bereich verwendet werden kann.)
3. Klicken Sie zum Fortfahren auf **Weiter**.

Auswählen der zu installierenden Komponenten

Im Dialogfeld Installation auswählen können Sie zwischen sechs verschiedenen Optionen für die Installation wählen, die in Tabelle 4 aufgeführt werden. Der Bildschirm wird in Abbildung 11 dargestellt.

ABBILDUNG 11. Auswählen eines Installationsprofils



WARNUNG: Wenn die von Ihnen für OpenLinux eServer erstellten und formatierten Partitionen für eine der Installationsoptionen nicht die ausreichende Speicherkapazität aufweisen, wird diese Option (beispielsweise Alle Pakete) abgeblendet dargestellt und kann nicht ausgewählt werden.

TABELLE 4. OpenLinux eServer Installationsprofile

Option	Beschreibung
Webserver	
Datei und Druckserver	
Netzwerkserver	

TABELLE 4. OpenLinux eServer Installationsprofile

Option	Beschreibung
Minimaler Server	
Alle Pakete	
Benutzer-definierte Auswahl (Diskette)	Wie bereits zuvor erläutert, können Sie bei der benutzerdefinierten Installation eine zuvor festgelegte Auswahl an Paketen installieren.

Beachten Sie bitte in diesem Zusammenhang, dass Sie nach erfolgter Installation jederzeit Softwarepakete installieren oder entfernen können. Wenn Sie das X Window System installiert haben, können Sie zu diesem Zweck KPackage verwenden, ein grafisches Tool zum Verwalten von Paketen. Falls Sie sich für eine Installationsoption entschieden haben, bei der das X Window System nicht installiert wird, können Sie stattdessen das Programm `coastool` verwenden. Wählen Sie eine der Installationsoptionen aus, die in der vorangegangenen Tabelle aufgeführt wurden.

4. Klicken Sie zum Fortfahren auf Weiter.

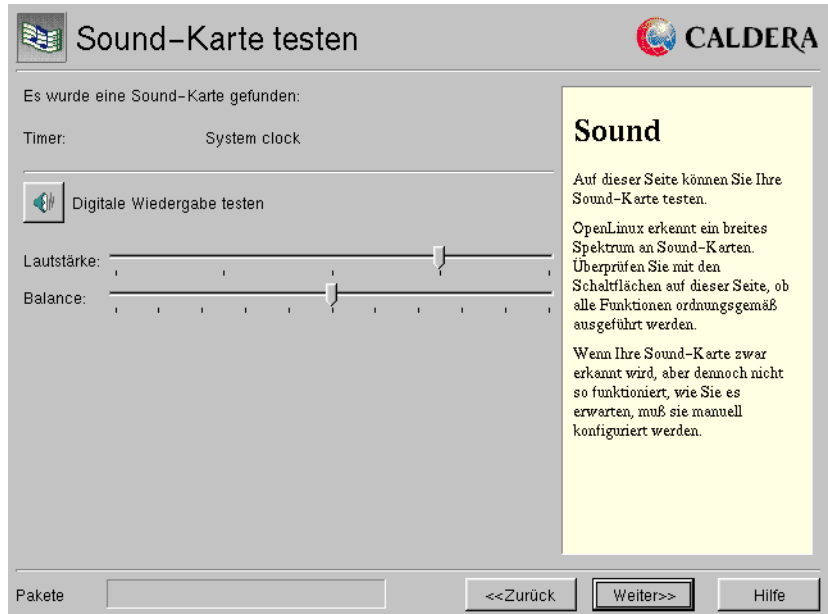
Die Installation der Pakete erfolgt im Hintergrund, so dass Sie gleichzeitig mit dem Konfigurieren Ihres Systems fortfahren können.

Testen der Soundkarte

Während die ausgewählten Pakete installiert werden, können Sie im nächsten Bildschirm (siehe Abbildung 12) Ihre Soundkarte testen, falls eine Soundkarte in Ihrem System gefunden wurde. Sie können dann die folgenden Einstellungen testen oder konfigurieren:

- Digitale Wiedergabe testen – Wenn Ihre Karte die digitale Klangwiedergabe unterstützt, sollten Sie nach dem Klicken auf diese Schaltfläche Musik hören.
- MIDI-Wiedergabe testen – Wenn Ihre Karte MIDI-Wiedergabe unterstützt, wird nach dem Klicken auf diese Schaltfläche Musik abgespielt.
- Lautstärke und Balance-Regler – Mit Hilfe dieser beiden Schieberegler können Sie mit der Maus die Lautstärke und Balance einstellen.

ABBILDUNG 12. Konfigurieren und Testen der Soundkarte



Erstellen von Benutzer-Accounts

Auf jedem Linux-System ist ein spezieller Benutzer mit der Bezeichnung root vorhanden. Dabei handelt es sich um den superuser, der unter Linux uneingeschränkte Rechte besitzt und das System sogar zerstören kann. In diesem Bildschirm (siehe Abbildung 13) können Sie ein Kennwort für den Rootbenutzer Ihres neuen OpenLinux eServer Systems festlegen. Sie sollten dieses Kennwort mit großer Sorgfalt auswählen, da jede Person, die im Besitz dieses Kennworts ist, alle Systemeinstellungen ändern, Dateien löschen und jede Menge Unheil in Ihrem System anrichten kann.

Gute Kennwörter erfüllen folgende Eigenschaften:

- Ihre Länge beträgt mindestens fünf Zeichen (die Verwendung von acht Zeichen gewährleistet noch mehr Sicherheit)
- Die Kennwörter enthalten Zahlen oder Sonderzeichen. So bietet es sich oft an, den Buchstaben O durch eine 0 (Null) und den Buchstaben L durch eine 1 (Eins) zu ersetzen.

- Die Kennwörter sind in keinem Wörterbuch enthalten und können auch nicht durch einfaches Verändern eines Wortes in einem Wörterbuch gebildet werden (beispielsweise durch Umkehren der Reihenfolge der Buchstaben).

ABBILDUNG 13. Festlegen des Kennworts für Root

Root-Kennwort einrichten

Root-Kennwort:

Kennwort erneut eingeben:

Root-Account

Es gibt einen standardmäßig erstellten Account, der für die Durchführung von Verwaltungsarbeiten auf Ihrem Linux-System verwendet werden sollte: der **Root**-Account.

Dieser Account ermöglicht systemweit einen "Superuser"-Zugriff auf das gesamte System. Der Benutzer, der sich mit diesem Account anmeldet, kann alle Dateien, alle Dienste, schlicht *alles* auf Ihrem System ändern, konfigurieren oder sogar zerstören.

Pakete 2% <<Zurück Weiter>> Hilfe

So legen Sie das Kennwort für Root fest:

1. Geben Sie ein Kennwort in das Feld Root-Kennwort ein.
2. Für jedes eingegebene Zeichen wird ein Sternchen angezeigt.
3. Drücken Sie die Tabulatortaste, oder klicken Sie in das Feld Kennwort bestätigen, um das Kennwort nochmals einzugeben.
4. Auf diese Weise kann das Installationsprogramm überprüfen, ob Sie das Kennwort richtig eingegeben haben.
5. Wenn Sie in beide Felder das gleiche Kennwort eingegeben haben, können Sie auf die Schaltfläche Weiter klicken, die zuvor abgeblendet dargestellt wurde.
6. Klicken Sie zum Fortfahren auf Weiter.

Als nächstes können Sie weitere Benutzer für Ihr OpenLinux System festlegen, die über keine Administratorrechte verfügen. Dieser Bildschirm wird in Abbildung 14

dargestellt. Da Sie Ihr System unbeabsichtigt beschädigen können, wenn Sie als Root angemeldet sind, sollten Sie normalerweise unter Ihrem persönlichen Benutzer-Account mit dem System arbeiten und nur zum Ausführen bestimmter Verwaltungstätigkeiten, für die Administratorrechte erforderlich sind, zu Ihrem Root-Account wechseln. Da Sie sich für das alltägliche Arbeiten mit dem System nicht als Root anmelden sollten, müssen Sie mindestens einen normalen Benutzer-Account erstellen.

ABBILDUNG 14. Erstellen weiterer Benutzer

Benutzer einrichten

Voller Name:

Login-Name:

Kennwort: Kennwort bestätigen:

Login-Shell: ☒ bash ☐ tcsh ☐ zsh

Diese Benutzer werden hinzugefügt:

Anmeldung	Voller Name	Shell	Kennwort
col	Caldera Systems	OpenLinux/bin/bash	Nicht gezeigt

Benutzer hinzufügen

Linux ist ein Multiuser-/Multitasking-Betriebssystem. Die Fähigkeit, mehrere Benutzer zur gleichen Zeit denselben Computer benutzen zu lassen, macht es erforderlich, für jeden Benutzer einen Login-Account einzurichten.

Wenn Sie nicht wenigstens einen Anmeldenamen (Login) eingerichtet haben, können Sie sich nur als **Root** (der Systemverwalter) bei Ihrem Rechner anmelden. Da der Root-Account für Systemverwaltungsaufgaben reserviert ist, müssen Sie

Pakete 12%

So erstellen Sie einen neuen Benutzer-Account:

1. Löschen Sie den Beispielttext im Feld Voller Name, geben Sie den vollständigen Namen des Benutzers ein, und drücken Sie die Eingabetaste.
2. Löschen Sie den Beispielttext im Feld Anmeldenamen (falls erforderlich), geben Sie einen Anmeldenamen ein, und drücken Sie die Eingabetaste. Der Anmelde-name besteht oft aus dem ersten Buchstaben des Vornamens und dem Nachnamen oder aus dem Vornamen und dem ersten Buchstaben des Nachnamens. Der Anmelde-name sollte nicht länger als acht Zeichen sein. Wenn der Name länger ist, wird er vom System automatisch auf acht Zeichen gekürzt.

3. Geben Sie für diesen neuen Benutzer-Account ein Kennwort in das Feld Kennwort ein, und drücken Sie die Eingabetaste.
4. Wiederholen Sie das gleiche Kennwort im Feld Kennwort bestätigen, und drücken Sie die Eingabetaste.
5. Wenn Sie das gleiche Kennwort in beide Felder eingegeben haben, können Sie auf die Schaltfläche Benutzer hinzufügen klicken, die zuvor abgeblendet dargestellt wurde.
6. Wenn Sie die standardmäßig verwendete Shell für diesen Benutzer ändern möchten, wählen Sie `tcsh` oder `zsh` aus. Die Standardshell für Linux-Systeme ist `bash`.
7. Klicken Sie auf die Schaltfläche Benutzer hinzufügen. Der neue Benutzer wird daraufhin in der Liste in der unteren Hälfte des Dialogfelds angezeigt.
8. Wiederholen Sie diese Schritte für jeden weiteren Benutzer, den Sie hinzufügen möchten.
9. Wenn Sie alle benötigten Benutzer-Accounts erstellt haben, klicken Sie auf Weiter, um mit der Installation fortzufahren. Die Schaltfläche Weiter wird erst dann aktiviert, wenn Sie mindestens einen normalen Benutzer-Account erstellt haben.

Festlegen der Netzwerkeinstellungen

Mit Hilfe dieses Bildschirms (siehe Abbildung 15) können Sie die Netzwerkeinstellungen für Ihr OpenLinux eServer System konfigurieren. Wenn Sie lediglich über ein Modem mit einem Internet-Dienstanbieter verbunden sind, müssen Sie in diesem Bildschirm keine Netzwerkinformationen eingeben. Wählen Sie daher das erste Optionsfeld mit der Bezeichnung Kein Ethernet, und klicken Sie auf Weiter.

ABBILDUNG 15. Festlegen der Netzwerkeinstellungen

Netzwerk einrichten

☐ Kein Netzwerk
☐ Netzwerk über DHCP konfigurieren
☒ Netzwerk statisch konfigurieren

IP Adresse: 192.168.1.1 DNS-Server: 192.168.1.1
 Netzmaske: 255.255.255.0 Backup #1: 192.168.1.254
 Gateway: 192.168.1.2 NIS-Domain:

Hostname: noname.nodomain.nowhere

Dieses Dialogfeld dient ausschließlich der Konfiguration eines TCP/IP-Netzwerks für Ethernet-Geräte vorbehalten. Bitte konfigurieren Sie andere Netzwerktypen, beispielsweise DFÜ-Netzwerke, nach der Installation.
 Wenn Sie keine Ethernet-Karte besitzen oder das Netzwerk erst zu einem späteren Zeitpunkt konfigurieren wollen, wählen Sie die Option **Kein Netzwerk** aus, und gehen Sie zum nächsten Bildschirm.
 Verwenden Sie die Option

Pakete 25% <<Zurück Weiter>> Hilfe

- Wenn Sie keine Verbindung mit einem lokalen Netzwerk über eine Ethernetkarte oder eine ähnliche Netzwerkkarte herstellen möchten, wählen Sie die Option **Kein Ethernet**.
- Wenn Sie die Netzwerkinformationen über einen DHCP-Server (Dynamic Host Configuration Protocol) in Ihrem Netzwerk beziehen, wählen Sie die zweite Option. Wenn Sie sich für diese Option entscheiden, müssen Sie die weiteren Felder in diesem Bildschirm nicht ausfüllen. Alle Netzwerkeinstellungen werden vom Installationsprogramm vom DHCP-Server in Ihrem Netzwerk bezogen.
- Wenn Sie einen üblichen Netzwerkclient einrichten oder Ihr OpenLinux eServer System als Server verwenden möchten, wählen Sie die dritte Option, um statische Netzwerkeinstellungen festzulegen.

Auch bei Verwendung statischer Netzwerkeinstellungen ist es möglich, dass einige Felder mit Netzwerkinformationen bereits ausgefüllt sind, weil das Installationsprogramm Informationen über Ihr Netzwerk abrufen konnte. Die Netzwerkinformationen wurden gegebenenfalls bereits automatisch vom Installationsprogramm durch Abfragen des Netzwerks ermittelt oder müssen manuell in die entsprechenden Felder eingetragen werden.

Wenn Sie statische Netzwerkeinstellungen verwenden, müssen Sie alle Felder auf der linken Seite des Bildschirms unter Verwendung des standardmäßigen IP-Adressenformats ausfüllen: vier Zahlenblöcke, jeweils zwischen 0 bis 255, getrennt durch Punkte. Um von einem numerischen Feld zum nächsten zu wechseln, können Sie in das Feld klicken oder die Tabulatortaste drücken.

So legen Sie die Netzwerkinformationen fest:

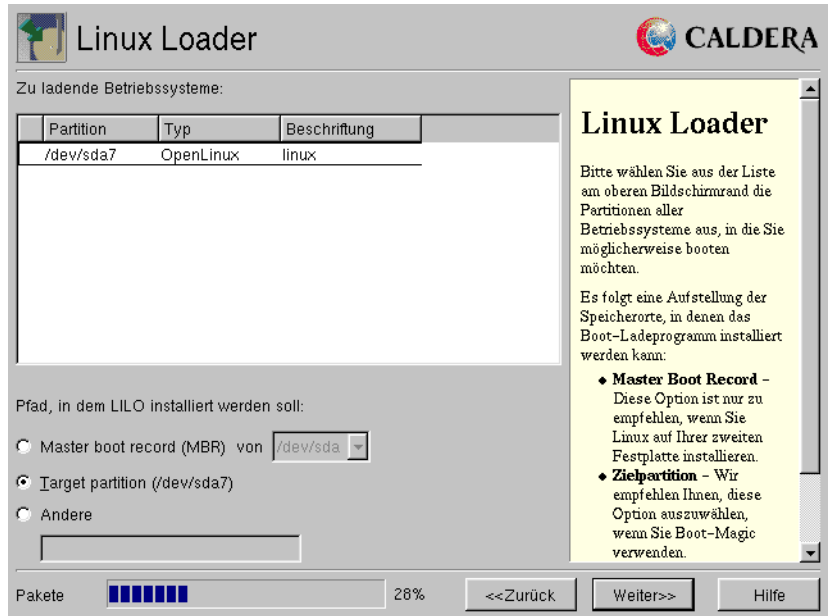
1. Geben Sie im Feld IP-Adresse die vier Zahlen für die IP-Adresse ein, die Ihrem System zugewiesen wurde. Diese Adresse wurde von Ihrem Internet-Dienstanbieter oder dem Systemadministrator für Ihr Netzwerk festgelegt. Wenn Sie eine zufällig ausgewählte Nummer angeben, kann Ihr System unter Umständen nicht mit den anderen vernetzten Computern zusammenarbeiten oder es treten Probleme beim Benutzer des Rechners auf, dem die von Ihnen eingegebene Adresse bereits zuvor zugewiesen wurde.
2. Geben Sie die Netzwerkmaske für Ihr lokales Netzwerk ein.
3. Geben Sie die IP-Adresse für Ihr Gateway ein.
4. Geben Sie die IP-Adresse Ihres DNS-Nameservers in das Feld Namensserver ein.
5. Wenn Sie über einen sekundären Nameserver verfügen, geben Sie dessen IP-Adresse in das Feld Backup 1 ein.
6. Wenn Sie NIS in Ihrem Netzwerk verwenden, geben Sie die NIS-Domäne in das hierfür vorgesehene Feld ein. Wenn Sie NIS nicht verwenden, müssen Sie im Feld NIS-Domäne nichts eintragen.
7. Unabhängig von der ausgewählten Netzwerkoption (kein Ethernet, DHCP oder statisch) sollten Sie einen vollständigen Hostnamen für Ihr OpenLinux System im Feld Hostname eingeben. Der Hostname besteht aus dem Rechnernamen Ihres Computers, den Sie selbst auswählen können, sowie dem Domännennamen Ihres lokalen Netzwerks. Im folgenden erhalten Sie zwei Beispiele für vollständige Hostnamen. Der Hostname für Ihr System wird natürlich anders lauten:
 - rocky.calderasystems.com
 - tripoli.cs.utah.edu
8. Wenn Sie Ihren Hostnamen eingegeben haben, können Sie durch Klicken auf Weiter mit der Installation fortfahren.

Installieren des Bootloaders

Mit dem nächsten Konfigurationsbildschirm wird LILO installiert, der Linux LOader. Die Hauptfunktion von LILO besteht im Booten von Linux. Wenn Sie auf

Ihrem System mehrere Betriebssysteme installiert haben, können Sie mit LILO auswählen, welches Betriebssystem beim Booten Ihres Computers gestartet werden soll. Der Bildschirm zum Konfigurieren von LILO ist in Abbildung 16 dargestellt.

ABBILDUNG 16. Installieren des LILO-Bootloaders



In diesem Bildschirm werden alle vom Installationsprogramm erkannten bootfähigen Partitionen aufgelistet, jeweils versehen mit Informationen zum Partitionstyp und der zugewiesenen Kennung. Bei der Kennung handelt es sich um die Bezeichnung einer bootfähigen Partition, die Sie beim Starten des Systems eingeben müssen, um das gewünschte Betriebssystem zu starten. Klicken Sie auf den Eintrag für die Partition, die Sie als Standardpartition verwenden möchten. Diese Partition wird beim Booten des Systems nach einigen Sekunden gestartet, wenn Sie am LILO Prompt keine Eingabe vornehmen.

Als nächstes müssen Sie festlegen, wo LILO installiert werden soll. Folgende Optionen stehen hierfür zur Auswahl:

- **Master Boot Record (MBR):** Verwenden Sie diese Option, wenn OpenLinux eServer als einziges Betriebssystem auf Ihrem Rechner verwendet wird, oder wenn OpenLinux eServer auf einer zweiten Festplatte installiert ist.

- Zielpartition: Bei Wahl dieser Option wird LILO in der von OpenLinux verwendeten Partition installiert. Diese Einstellung wird empfohlen, wenn auf Ihrem System neben OpenLinux noch ein weiteres Betriebssystem installiert ist, oder falls Sie bereits einen anderen Bootloader wie Boot Magic oder System Commander im MBR installiert haben.
- Andere: Diese Option sollte nur von erfahrenen Benutzern verwendet werden, die LILO in einem anderen Bereich installieren möchten.

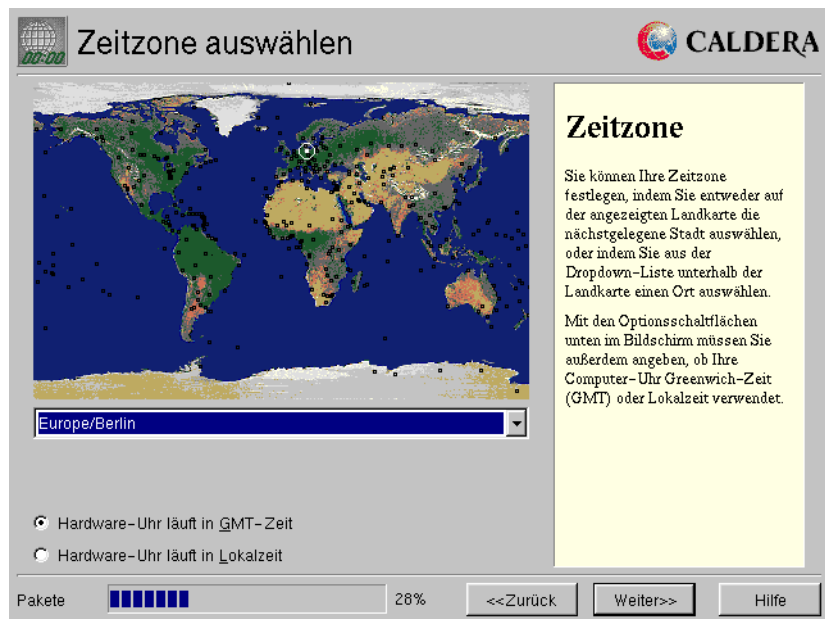
So wird LILO installiert:

1. Wählen Sie aus, wo LILO installiert werden soll.
2. Klicken Sie zum Fortfahren auf Weiter.

Abschließen der Installation

Mit dem nächsten Installationsbildschirm können Sie die Zeitzone auswählen, in der sich Ihr Computer befindet (siehe Abbildung 17).

ABBILDUNG 17. Konfigurieren der Zeitzone



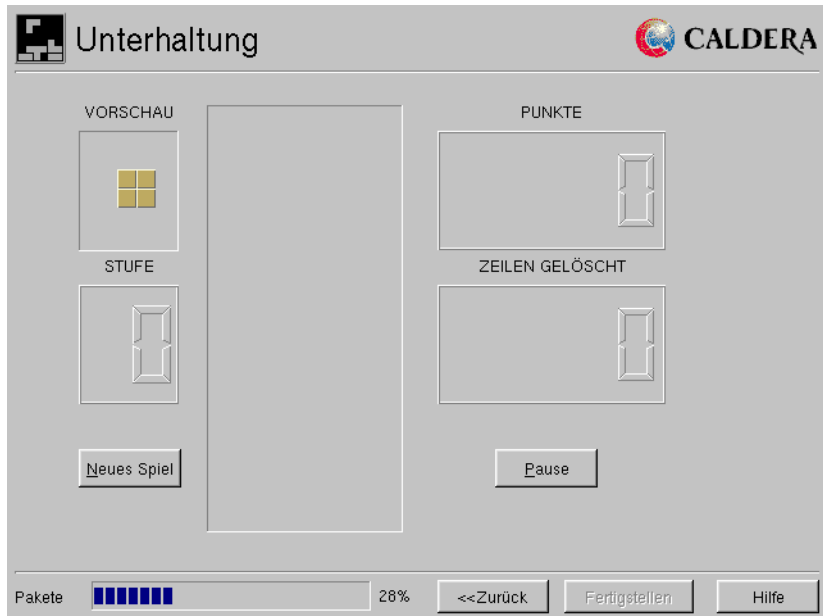
So wählen Sie Ihre Zeitzone aus:

1. Blättern Sie in der Dropdown-Liste, bis Sie die richtige Zeitzone für Ihren Aufenthaltsort ausfindig gemacht haben, oder klicken Sie auf die Karte, um dort Ihre Zeitzone auszuwählen. In den meisten Fällen können Sie Ihre Zeitzone am einfachsten dadurch auswählen, dass Sie nach dem Eintrag für Ihr Land suchen, auf das Pluszeichen klicken und dann die richtige Zone in diesem Land auswählen.
2. Klicken Sie auf die richtige Einstellung für die Hardwareuhr Ihres Computers.
3. Wenn Sie auf Ihrem System sowohl Windows als auch OpenLinux verwenden, wählen Sie die Option zur Verwendung lokaler Zeit.
4. Wenn auf Ihrem System lediglich OpenLinux verwendet wird, wählen Sie GMT (Universal Coordinated Time in Greenwich).
5. Klicken Sie auf die Schaltfläche Weiter, um mit der Installation fortzufahren.

In Abhängigkeit von der Geschwindigkeit Ihres Computers und der von Ihnen ausgewählten Installationsoption werden zum jetzigen Zeitpunkt möglicherweise noch Pakete installiert. Der Verlauf der Installation wird an der Unterseite mit Hilfe einer Fortschrittsanzeige dargestellt.

Im nächsten Bildschirm können Sie sich mit einem Spiel die Zeit vertreiben, das ein wenig an Tetris (siehe Abbildung 18) erinnert, während die verbleibenden Pakete installiert werden. Wenn alle Pakete installiert und konfiguriert wurden, können Sie auf die Schaltfläche Fertigstellen im unteren Bildschirmbereich klicken. Dadurch wird die Installation abgeschlossen und Ihr gerade eben installiertes OpenLinux eServer System gebootet. Nach wenigen Augenblicken wird dann der Startbildschirm von OpenLinux angezeigt.

ABBILDUNG 18. Während die Installation im Hintergrund abgeschlossen



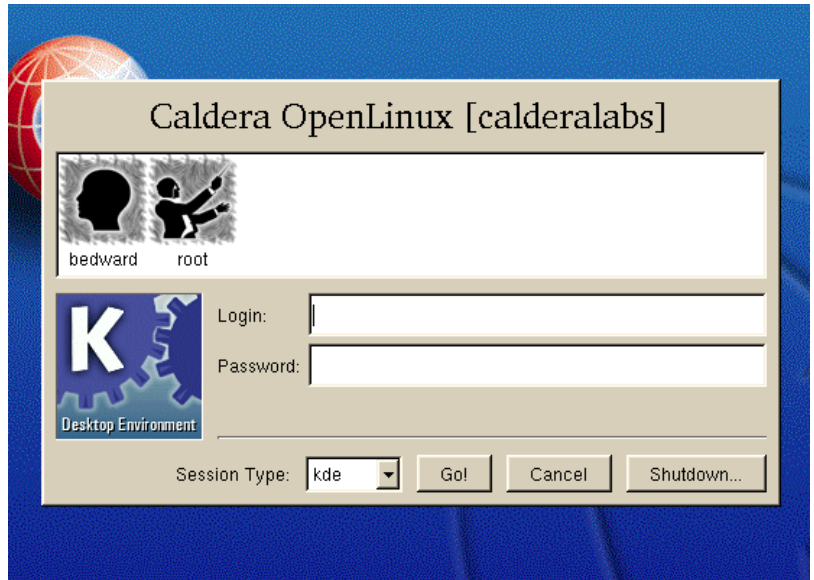
wird, ist für Unterhaltung gesorgt

HINWEIS: Bevor Sie Ihr OpenLinux System neu starten, müssen Sie die OpenLinux CD-ROM und/oder die Installationsdiskette (falls verwendet) aus den Laufwerken Ihres Computers herausnehmen.

Nachdem der Kernel gestartet wurde, wird eine Reihe von Meldungen auf dem Bildschirm angezeigt. Diese Meldungen weisen auf folgende Vorgänge hin:

- Der Kernel untersucht Ihre Hardware.
- OpenLinux wird gestartet.
- Ihr System wechselt sofort in den grafischen Modus.
- Die grafische Anmeldeaufforderung wird angezeigt (siehe Abbildung 19).

ABBILDUNG 19. Die grafische Anmeldeaufforderung von KDM



Melden Sie sich jetzt am System an. Hierfür sollten Sie Ihren Root-Account verwenden, da Sie gegebenenfalls noch Software weiterer Anbieter oder kommerzielle Software installieren möchten und hierfür über Administratorrechte verfügen müssen. Im Hintergrund führt OpenLinux eServer gleichzeitig noch Setup-Programme aus, um die Konfiguration Ihres Systems abzuschließen. Warten Sie daher mindestens zehn Minuten, bevor Sie den Server neu starten. Informationen über das richtige Herunterfahren Ihres OpenLinux Systems finden Sie in Kapitel 4.

Konfigurieren von Webmin

Nach erfolgreicher Installation hat das Installationsprogramm LIZARD das Tool Webmin mit dem gewählten Hostnamen und dem verschlüsselten Rootkennwort konfiguriert. Außerdem wurde für den standardmäßigen Port von Webmin die Einstellung 1000 (und nicht 10000) festgelegt. Daher erfolgt der Zugriff auf Webmin über den Port 1000 über Ihren Root-Account und mit dem Kennwort, das Sie bei der Installation in LIZARD eingegeben haben.

KAPITEL 3

Starten und Stoppen von OpenLinux eServer

In diesem Kapitel wird erläutert, wie Ihr OpenLinux eServer System gestartet und gestoppt wird und welche Vorgänge bei der Systeminitialisierung ablaufen. Wenn Sie über Grundlagenwissen zu diesen Themen verfügen, können Sie die entsprechenden Abläufe bei Ihrem System individuell konfigurieren und Probleme beheben.

Booten von Linux

Nachdem der Linux-Kernel durch LILO gestartet wurde, werden durch den Kernel die folgenden Schritte ausgeführt:

1. Der Kernel initialisiert seine eigenen internen Systeme.
2. Das Programm `init` wird gestartet.
3. `init` liest die Datei `/etc/inittab`, um festzustellen, wie das System zum angegebenen Runlevel hochgefahren werden soll.

4. `init` liest die Datei `/etc/rc.d/rc.modules`, um festzustellen, welche Module automatisch geladen werden müssen.
5. `init` führt `/etc/rc.d/rc.boot` aus, um weitere wichtige Systeminformationen zu laden und zu verarbeiten, so z.B. den Hostnamen des Systems.
6. In Abhängigkeit vom *Runlevel*, also dem Betriebszustand, den das System nach dem Starten erreichen soll (normalerweise 3 oder 5), werden alle Dienste gelesen und ausgeführt, die im entsprechenden Verzeichnis aufgelistet werden (`/etc/rc.d/rc3.d` oder `/etc/rc.d/rc5.d`). Dadurch befindet sich das System nach der Initialisierung im gewünschten Runlevel. Die Skripten, die mit dem Buchstaben *S* beginnen, werden gestartet, während alle Skripten, die mit dem Buchstaben *K* beginnen, gestoppt werden.
7. Das Programm `getty` wird für jede der in `/etc/inittab` definierten virtuellen Konsolen gestartet. Bei `getty` handelt es sich um den Prozess, der das Starten von Terminals verwaltet und den Anmeldeprozess startet.

Eine detailliertere Erklärung von Schritt 6 erhalten Sie im nächsten Abschnitt mit der Bezeichnung Systeminitialisierung.

Systeminitialisierung

Im Verzeichnis `/etc/rc.d` befinden sich mehrere Unterverzeichnisse, und zwar eines für jeden Runlevel, `rc0.d` - `rc6.d` und `init.d`. Jedes dieser Unterverzeichnisse enthält zahlreiche symbolische Verknüpfungen mit den tatsächlichen Initialisierungsskripten, die im Master-Init-Verzeichnis, `init.d`, gespeichert werden. Alle Skripten beginnen mit einem *S* oder einem *K*, gefolgt von einer zweistelligen Zahl, und akzeptieren die Argumente `start` oder `stop` und mitunter auch `reload` oder `restart`. Jedes Skript steuert einen einzelnen Dämon oder Dienst im System. Dadurch ist es für den Systemadministrator problemlos möglich, Dämonen oder Dienste von der Befehlszeile aus zu starten, zu stoppen oder neu zu starten.

Wenn nicht direkt von der Befehlszeile aus Anweisungen übergeben werden, d.h. wenn das System gestartet, heruntergefahren oder in einen anderen Runlevel gebracht wird, steuert das Skript `/etc/rc.d/rc` in Abhängigkeit vom aktuellen und vorherigen Runlevel, welche Dämonen und Dienste auf welche Weise ausgeführt werden müssen. Angenommen, Sie booten in Runlevel 3. Das Skript `rc` führt alle Skripten im Verzeichnis `/etc/rc3.d` aus. Zuerst werden die Skripten ausgeführt, die mit dem Buchstaben *K* beginnen (in aufsteigender Reihenfolge), wodurch alle Prozesse gestoppt werden, die in Runlevel 3 nicht ausgeführt werden sollen.

Dann startet das Skript `rc` alle Skripten, die mit einem `S` beginnen (und auch das wiederum in aufsteigender Reihenfolge).

Wenn das System heruntergefahren wird, wechselt es entweder bei einem Neustart in Runlevel 6 oder beim Anhalten des Systems in Runlevel 0. Auch hier müssen alle Dienste in der richtigen Reihenfolge heruntergefahren werden. Zu diesem Zweck werden wiederum die Skripten mit `K` am Anfang in aufsteigender Reihenfolge ausgeführt, gefolgt von den Skripten mit `S` am Anfang, die in diesem Fall die Skripten zum Neustarten oder Anhalten des Systems "starten".

Wenn Sie neue Prozesse hinzufügen möchten, die beim Booten oder Anhalten des Systems gestartet bzw. beendet werden sollen, stehen Ihnen zwei Optionen zur Verfügung. Die einfachste Methode besteht darin, den zu startenden Prozess in die Datei `/etc/rc.d/rc.local` einzufügen. Er wird dann automatisch beendet, wenn das System angehalten oder neu gestartet wird.

Alternativ können Sie auch ein Skript in `/etc/rc.d/init.d` erstellen, mit dessen Hilfe der entsprechende Prozess gestartet oder gestoppt wird. Glücklicherweise müssen Sie das Skript nicht von Grund auf neu schreiben. Statt dessen können Sie die Vorlage mit der Bezeichnung `/etc/rc.d/init.d/skeleton` verwenden, in der Sie das Wort `daemon` in der Zeile

```
NAME=daemon
```

durch die Bezeichnung des gewünschten Programms ersetzen müssen. Als nächstes müssen Sie festlegen, zu welchem Zeitpunkt das Programm beim Booten oder Herunterfahren des Systems gestartet und gestoppt werden muss. Erstellen Sie schließlich noch in den entsprechenden Unterverzeichnissen in `rcX.d` in `/etc/rc.d` eine symbolische Verknüpfung, die mit einem `K` oder einem `S` beginnt, gefolgt von einer zweistelligen Zahl, die noch nicht verwendet wird und festlegt, zu welchem Zeitpunkt das Skript in `/etc/rc.d/init.d` ausgeführt wird.

Verwenden von Webmin für das Steuern der Systeminitialisierung

In diesem Abschnitt wird beschrieben, wie Sie Webmin für das Steuern der Systeminitialisierung verwenden können und wie Webmin gestartet wird.

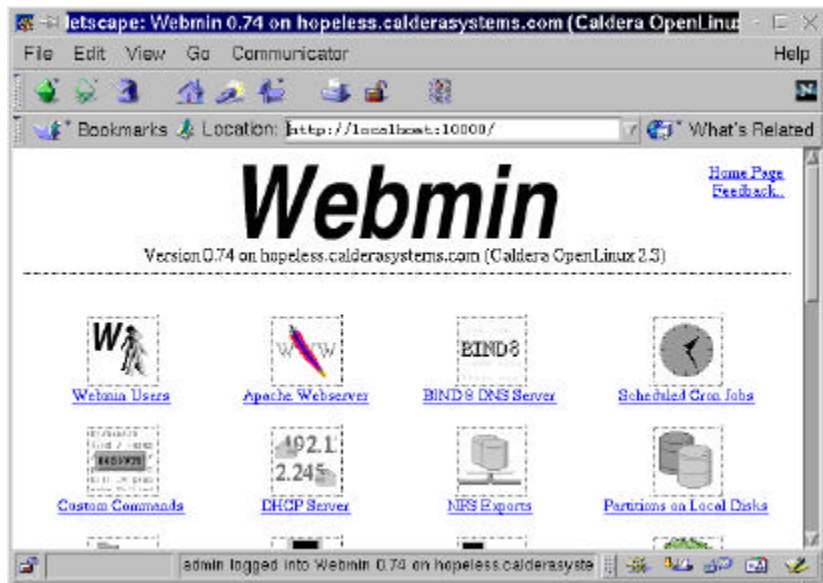
Um Webmin aufzurufen, starten Sie den Netscape-Browser durch Klicken auf dessen Symbol in der Kontrolleiste (siehe Abbildung 22) oder über das KMenü->Internet->Communicator. Um die Verbindung mit dem Webmin-Server herzustellen, geben Sie `localhost:1000` in das Textfeld Location des Browsers ein und drücken dann die Eingabetaste. Daraufhin wird der Anmeldebildschirm von Webmin angezeigt (siehe Abbildung 20). Geben Sie den Benutzernamen und das Kennwort ein, das Sie gegen Ende von Kapitel 2 festgelegt

haben, und klicken Sie auf OK. Dadurch wird der Hauptbildschirm von Webmin angezeigt, der in Abbildung 21 dargestellt wird.

ABBILDUNG 20. Das Symbol für Netscape in der Kontrolleiste von KDE



ABBILDUNG 21. Der Hauptbildschirm von Webmin

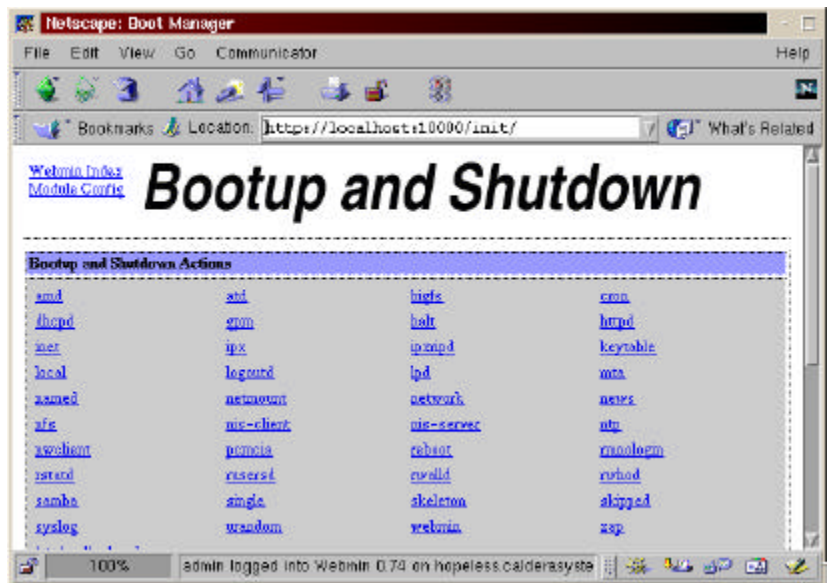


Um mit Hilfe der Benutzeroberfläche von Webmin die Einstellungen zur Systeminitialisierung zu ändern, klicken Sie auf das Symbol Bootup and Shutdown Actions (siehe Abbildung 22). Abbildung 23 zeigt den anschließend angezeigten Bildschirm.

ABBILDUNG 22. Das Symbol Bootup and Shutdown Actions in Webmin

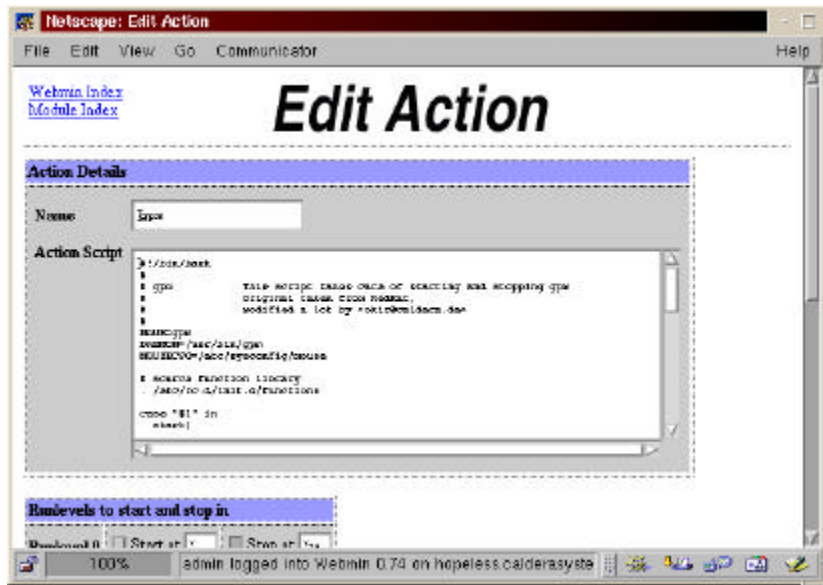


ABBILDUNG 23. Das Modul Bootup and Shutdown



In diesem Fenster werden im Wesentlichen alle aktuell definierten Initialisierungsskripten (die Skripten befinden sich in `/etc/rc.d/init.d`) und das spezielle Skript `/etc/rc.d/rc.local` angezeigt. Um eines der Skripten zu bearbeiten, klicken Sie auf dessen Namen. Angenommen, Sie möchten verhindern, dass der Maustreiber für die Konsole, `gpm`, beim Booten in Runlevel 5 geladen wird. Klicken Sie hierzu auf die Verknüpfung `gpm`, worauf der in Abbildung 24 dargestellte Bildschirm angezeigt wird.

ABBILDUNG 24. Der Konfigurationsbildschirm für gpm



In der oberen Hälfte des Bildschirms wird das tatsächliche Initialisierungsskript angezeigt, das Sie hier direkt bearbeiten können. In der unteren Bildschirmhälfte können Sie hingegen festlegen, in welchen Runlevels `gpm` gestartet und gestoppt wird. Wie Sie erkennen können, ist `gpm` momentan so konfiguriert, dass der Konsolenmaustreiber in den Runlevels 3, 4 und 5 gestartet und in den Runlevels 0, 1, 2 und 6 gestoppt wird. Die Zahlen 75 und 25 legen fest, in welcher Reihenfolge der Dämon jeweils gestartet bzw. gestoppt wird. So wird `gpm` in Runlevel 5 deaktiviert:

1. Deaktivieren Sie das Kontrollkästchen Start at für Runlevel 5.
2. Klicken Sie auf die Schaltfläche Stop Now, um den Dämon anzuhalten (falls er gerade ausgeführt wird).
3. Klicken Sie auf die Verknüpfung Return to action im folgenden Bildschirm.
4. Klicken Sie auf die Schaltfläche Save.

Nachdem Sie auf Save geklickt haben, kehren Sie zum Bildschirm Bootup and Shutdown Actions von vorhin zurück. Um zu überprüfen, ob `gpm` jetzt in Runlevel 5 nicht mehr gestartet wird, klicken Sie auf die Verknüpfung `gpm`. Sie werden daraufhin feststellen, dass Ihre Änderungen gespeichert wurden.

Mit Hilfe des Hauptbildschirms von Bootup and Shutdown Actions können Sie auch neue Aktionen für das Booten und Herunterfahren des Systems festlegen. Gehen Sie hierzu wie folgt vor:

1. Klicken Sie auf die Verknüpfung Create a new bootup or shutdown action.
2. Füllen Sie die Eingabemaske Create Action aus (siehe Abbildung 27).
3. Schreiben Sie das eigentliche Skript mit Hilfe der Eingabemaske Action Details. Webmin erstellt das Skript automatisch und verwendet dabei die von Ihnen hier eingegebenen Informationen. Die erforderlichen Elemente werden in Tabelle 5 aufgelistet.
4. Legen Sie die Runlevels fest, in denen das neue Skript gestartet und gestoppt werden soll. Geben Sie zudem die Zahlenwerte an, mit denen die Reihenfolge für die Ausführung festgelegt wird. Üblicherweise werden Bootaktionen in den Runlevels 3, 4 und 5 gestartet und in den Runlevels 0, 1, 2 und 6 gestoppt. HINWEIS: Wenn Sie versehentlich einen Skriptnamen auswählen, der bereits verwendet wird, speichert Webmin die neue Aktion nicht.
5. Klicken Sie auf die Schaltfläche Create.

Ein Beispiel für das Erstellen eines neuen Initialisierungsskripts wird in Abbildung 25 dargestellt.

ABBILDUNG 25. Erstellen eines neuen Initialisierungsskripts

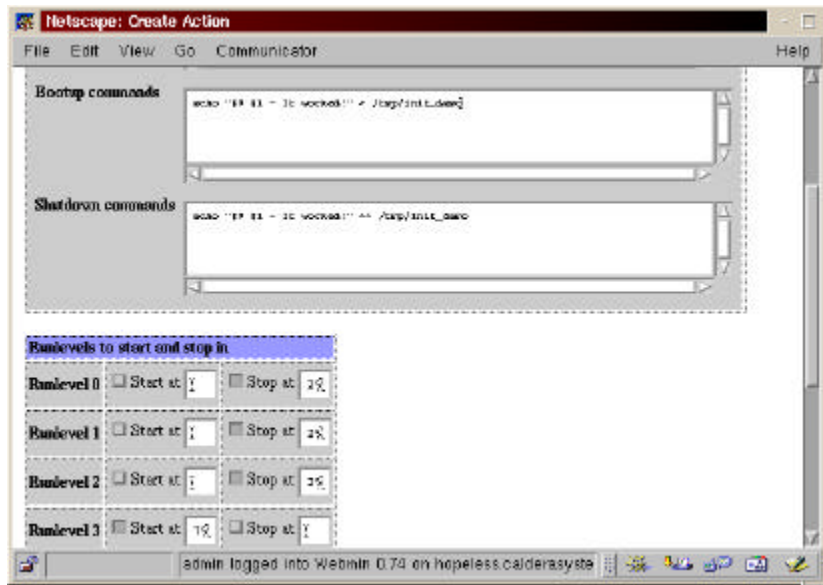


TABELLE 5. Die Felder in Action Details

Feld	Beschreibung
<i>Name</i>	Name des Skripts
<i>Beschreibung</i>	Kurze Beschreibung des Skripts
<i>Befehle zum Starten</i>	Die Befehle, die zum Starten des Dämons oder Programms ausgeführt werden, einschließlich möglicher Argumente oder Optionen
<i>Befehle zum Beenden</i>	Die Befehle, die zum Beenden des Dämons oder Programms ausgeführt werden, einschließlich möglicherweise erforderlicher Argumente oder Optionen

Um ein Skript zum Starten oder Beenden von Dämonen oder Diensten zu löschen, klicken Sie zuerst auf die Verknüpfung für dieses Skript im Hauptfenster Bootup and Shutdown und dann auf die Schaltfläche Delete unten rechts im Bildschirm.

Verwenden von LILO

In diesem Abschnitt erhalten Sie grundlegende Informationen über die Konfiguration und Verwendung von LILO. Dadurch erwerben Sie das nötige Vorwissen für den nächsten Abschnitt, in dem die Vorgehensweise zum Booten mehrerer Kernel erläutert wird. Das Modul von Webmin für das Bearbeiten von LILO und der Datei `/etc/lilo.conf` (durch die das Verhalten von LILO festgelegt wird) wird durch Klicken auf das Symbol Linux Bootup Configuration aufgerufen (siehe Abbildung 26). Dadurch wird der Bildschirm in Abbildung 27 mit der Bezeichnung Linux Bootup Configuration angezeigt.

ABBILDUNG 26. Das Symbol Linux Bootup Configuration



ABBILDUNG 27. Das Modul Linux Bootup Configuration



Über diesen Bildschirm können Sie mehrere Aktivitäten vornehmen:

- Modifizieren der Bootoptionen des aktuellen Kernels
- Erstellen eines neuen Bootkernels
- Erstellen einer neuen Bootpartition
- Bearbeiten der LILO-Optionen, die für alle Kernel gelten
- Aktivieren aller vorgenommenen Änderungen

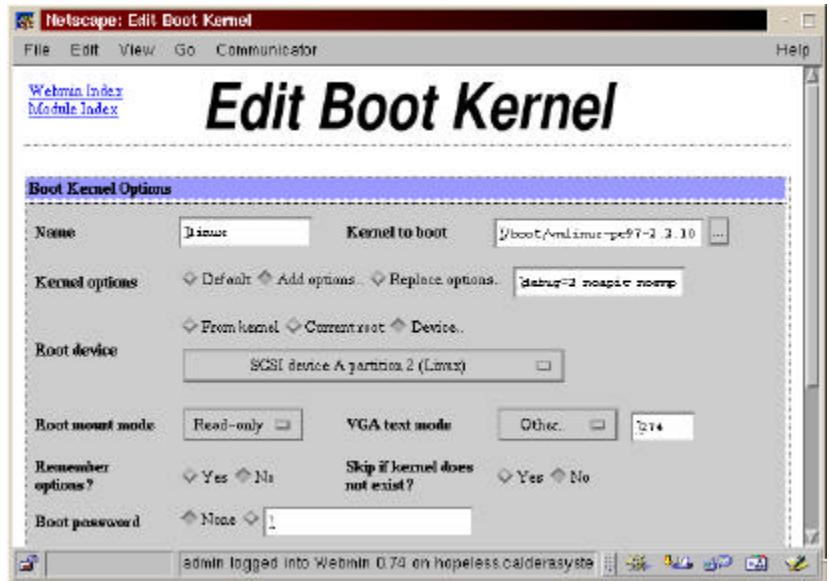
Modifizieren des aktuellen Kernels

Um die Bootoptionen des aktuellen Kernels zu ändern, klicken Sie auf eines der Symbole in der oberen Bildschirmhälfte. In Abbildung 28 wurde beispielsweise das Symbol mit der Bezeichnung `linux` gewählt. Abbildung 29 zeigt den Bildschirm, der daraufhin erscheint. Tabelle 6 beschreibt die einzelnen Felder.

TABELLE 6. Beschreibung der Felder in der Maske Boot Options

Feld	Beschreibung
Name	Die Kennung, die am Bootprompt von LILO eingegeben wird.
Kernel to boot	Vollständiger Pfad für das zu bootende Kernel-Image.
Kernel options	Parameter, die beim Booten an den Kernel unter Verwendung der Option <code>append</code> übergeben werden.
Root device	Das Gerät, auf dem sich das Rootdateisystem befindet.
Root mount mode	Das Rootgerät sollte beim Booten immer im Lesemodus (also ohne Schreibzugriff) gemountet werden.
VGA text mode	Der standardmäßige Grafikmodus. Entspricht der <code>vga</code> -Option von LILO.
Remember options?	Wählen Sie Yes, wenn die Kerneloptionen in den Kernel geschrieben werden sollen.
Skip if kernel does not exist?	Wählen Sie Yes, wenn LILO diesen Bereich übergehen soll, falls der angegebene Kernel nicht existiert.
Boot password	Vor dem Booten des angegebenen Kernels erwartet LILO die Eingabe dieses Kennworts.
Password needed for	Legt die Bedingungen fest, unter denen ein Kennwort angegeben werden muss.

ABBILDUNG 28. Der Bildschirm Edit Boot Kernel



Nachdem Sie diese Optionen geändert haben, klicken Sie auf die Schaltfläche Save, um Ihre Änderungen zu speichern. Klicken Sie dann auf die Schaltfläche Apply Configuration, damit Ihre Änderungen übernommen werden. Wenn Sie Ihre Änderungen hingegen wieder rückgängig machen möchten, klicken Sie auf die Verknüpfung Return to kernels and partitions.

Erstellen eines neuen Bootkernels

Ihr OpenLinux eServer System kann für die Verwendung mehrerer Kernel konfiguriert werden. Diese Funktion bietet sich an, wenn Sie spezielle Hardwarekonfigurationen unterstützen oder bestimmte Dienste zur Verfügung stellen möchten oder einen neu kompilierten Kernel testen wollen. Vor allem beim Testen eines neuen Kernels ist es besonders wichtig, mehrere Kernel booten zu können, da der neue Kernel möglicherweise nicht stabil ist oder nicht über alle gewünschten Funktionen verfügt. Beachten Sie bitte, dass Sie vor dem Erstellen eines neuen Kernels den alten Kernel sichern müssen und auch ein Eintrag für den alten Kernel in Ihrer Bootkonfigurationsdatei, /etc/lilo.conf, erhalten bleiben sollte. Die für das Neukompilieren des Kernels erforderlichen Schritte werden in Kapitel 4, Verwalten des Kernels, näher erläutert.

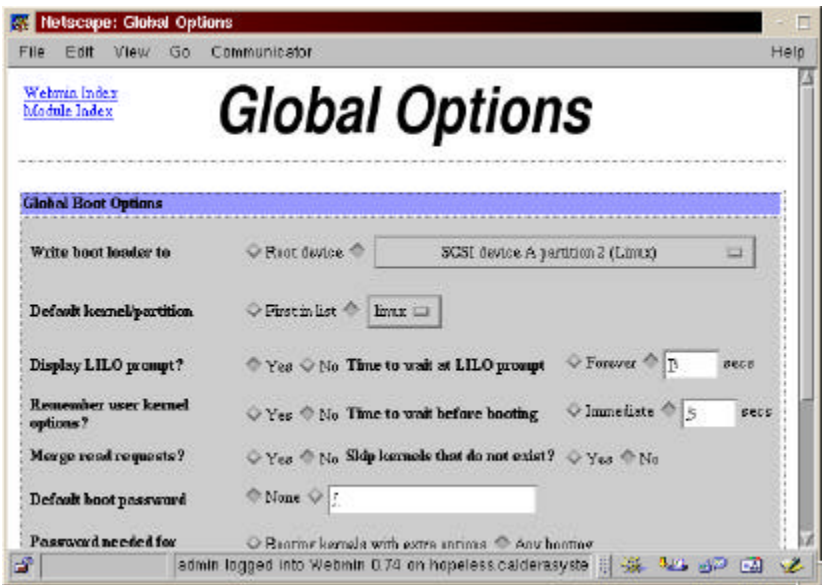
Um von mehreren Kernen booten zu können (nur ein Kernel kann jeweils gleichzeitig geladen und ausgeführt werden), benötigt OpenLinux eServer Informationen zum Speicherort und zu den Ladeoptionen für jeden Kernel. LILO (Linux LOader) übergibt diese Informationen über den auszuführenden Kernel an den Computer. Webmin erleichtert das Konfigurieren Ihres Systems zum Booten mehrerer Kernel ganz beträchtlich. Klicken Sie zuerst auf die Verknüpfung *Create a new boot kernel*. Der daraufhin angezeigte Bildschirm sieht ähnlich wie in Abbildung 28 aus, allerdings müssen Sie noch alle Felder ausfüllen. Klicken Sie auf die Schaltfläche *Save*, wenn Sie mit dem Ausfüllen fertig sind. Nachdem Sie wieder in den Bildschirm *Linux Bootup Configuration* zurückgekehrt sind, klicken Sie auf die Schaltfläche *Apply Configuration*, um Ihre Änderungen zu aktivieren.

Um einen Bootkernel zu löschen, wählen Sie dessen Symbol aus und klicken dann auf die Schaltfläche *Delete*, die sich in der unteren rechten Ecke des Bildschirms *Edit Boot Kernel* befindet.

Ändern der globalen Bootoptionen

Im ersten Abschnitt der Konfigurationsdatei zu LILO, `/etc/lilo.conf`, wird eine Reihe von Optionen für alle Kernel und das allgemeine Verhalten von LILO festgelegt. Wenn Sie diese Optionen anzeigen, erweitern oder ändern möchten, klicken Sie auf die Schaltfläche *Edit Global Options*. Der entsprechende Bildschirm wird in Abbildung 29 dargestellt.

ABBILDUNG 29. Der Bildschirm LILO Global Options von Webmin



In Abbildung 29 hat Webmin die bereits in der Datei `/etc/lilo.conf` vorhandenen globalen Optionen eingelesen. Die wichtigsten Optionen werden in Tabelle 7 behandelt.

TABELLE 7. Globale Optionen in LILO

Feld	Beschreibung
Write boot loader to	Gibt den Ort für die Installation des Bootloaders an.
Display LILO prompt?	Soll das Prompt "boot:" angezeigt werden oder nicht?
Time to wait at LILO prompt	Für welchen Zeitraum soll das Bootprompt angezeigt werden, bevor das Booten fortgesetzt wird?
Time to wait before booting	Wie lang soll LILO warten, bevor der standardmäßige Kernel gebootet wird, falls keine Alternative angegeben wird?

Die weiteren Felder wurden in Tabelle 5 aufgelistet und erläutert. Nachdem Sie die gewünschten Änderungen vorgenommen haben, können Sie diese durch Klicken auf die Schaltfläche **Save** speichern. Klicken Sie dann wie im vorigen Abschnitt auf die Schaltfläche **Apply Configuration**, um Ihre Änderungen zu aktivieren.

Analysieren von /etc/lilo.conf

Im vorherigen Abschnitt wurde erläutert, wie Webmin für das Konfigurieren von LILO verwendet wird. In diesem Abschnitt wird nun am Beispiel einer konkreten LILO-Konfigurationsdatei erklärt, wie diese Datei aufgebaut ist und was sie im System bewirkt. In der folgenden Auflistung sehen Sie zunächst den Inhalt der vollständigen Datei. Danach wird die Datei Zeile für Zeile detailliert untersucht, und die Verwendung der einzelnen Befehle und Optionen wird erläutert. Zeilen, die mit dem Gatterzeichen # beginnen, enthalten Kommentare, die von LILO ignoriert werden.

```
# /etc/lilo.conf
# Beispiel für eine LILO Konfigurationsdatei
```

```
boot = /dev/hda
install = /boot/boot.b
prompt
delay = 50
timeout = 50
message = /boot/message
default = linux-2.2.13

image = /boot/vmlinuz-2.3.25
    label = new-kernel
    root  = /dev/hda3
    via   = 274
    read-only
    append = "debug=2 noapic nosmp"

other = /dev/hda2
    label = win
```

```
boot = /dev/hda
install = /boot/boot.b
```

Das Schlüsselwort `boot` gibt das Laufwerk an, von dem der Computer bootet. Das Schlüsselwort `install` übergibt an den Computer Informationen zur Geometrie des Bootlaufwerks und zum genauen Speicherort des Kernels auf der Festplatte.

```
prompt
delay = 50
timeout = 50
message = /boot/message
```

default = linux-2.2.13

In diesem Abschnitt der Konfigurationsdatei werden die Optionen für das Booten aufgelistet. Der Eintrag `prompt` gibt beispielsweise an, dass ein Bootprompt angezeigt werden soll. Die Option `delay` weist den Computer an, den angegebenen Zeitraum (in Zehntelsekunden) zu warten, bevor der standardmäßige Kernel gebootet wird. Das Schlüsselwort `default` enthält den Namen des Kernels, der geladen werden soll, falls vor dem Ablauf der voreingestellten Zeitspanne am Bootprompt keine alternative Kennung eingegeben wird. Die Option `timeout` übergibt dem Computer die Information, wie lang dieser warten soll, bevor die weiteren Standardeinstellungen für das Booten verwendet werden. Die Angaben unter `message` enthalten den Speicherort von Meldungen, die Sie den Benutzern anzeigen möchten.

```
image = /boot/vmlinuz-2.3.25
label = new-kernel
root  = /dev/hda3
vga   = 274
read-only
append = "debug=2 noapic nosmp"
```

Dabei handelt es sich um den ersten Abschnitt, der in englischen Fachtexten häufig auch als *Stanza* bezeichnet wird und Anweisungen für das Laden eines speziellen Kernels enthält. Das Schlüsselwort `image` gibt an, welches Kernel-Image geladen werden soll, wie der Name dieses Images lautet und wo dieser in Bezug auf die Rootpartition gespeichert ist, in der Linux installiert ist. `label` ist ein Name oder Alias für das angegebene Kernel-Image. Bei dieser Kennung ("label") handelt es sich um den Begriff, den der Benutzer am Bootprompt eingeben muss. `root` wiederum legt fest, welche Partition auf dem Bootlaufwerk die Rootpartition enthält.

Die Einträge unterhalb dem Schlüsselwort `root` in jedem Stanza enthalten zusätzliche Parameter, die Sie an den Kernel vor dem Booten übergeben möchten. `vga` bezieht sich auf den Grafikmodus, in dem das Betriebssystem gestartet wird. Bei der Einstellung 274 in unserem Beispiel handelt es sich um den speziellen LIZARD Bootmodus. Das Schlüsselwort `read-only` weist den Kernel an, die Rootpartition beim Booten im Lesemodus zu mounten. Der Prozess `init` mountet das Rootdateisystem dann nach dem Booten des Kernels neu und ermöglicht dadurch auch Schreibzugriffe. Bei der Option in der Zeile `append` handelt es sich um eine von doppelten Anführungszeichen umschlossene Zeichenkette mit zusätzlichen Parametern, die beim Booten an den Kernel übergeben werden müssen. Diese Parameter unterstützen den Kernel beim Erkennen von Hardware und vermeiden dadurch beispielsweise Probleme, die durch das fehlerhafte Erkennen der tatsächlichen Hardwarekonfiguration entstehen könnten. Außerdem legen diese Parameter fest, welche Module geladen oder nicht geladen werden sollen u.ä.

```
other = /dev/hda2  
label = win
```

Dieses Stanza enthält Anweisungen für das Laden von anderen Betriebssystemen als Linux, was durch das Schlüsselwort `other` bereits angedeutet wird. In diesem Beispiel verweist diese Zeile auf die zweite primäre Partition auf der ersten IDE-Festplatte. Für die Kennung ("label") können Sie einen beliebigen Begriff festlegen. Es empfiehlt sich jedoch, einen Begriff auszuwählen, aus dem klar hervorgeht, welches Betriebssystem durch das Stanza geladen werden soll.

Alle Änderungen an der Datei `/etc/lilo.conf` müssen in den Master Boot Record (falls Sie nur LILO verwenden) oder in den Bootsektor Ihrer Linux-Partition geschrieben werden, falls Sie einen Bootloader eines anderen Anbieters wie System Commander oder BootMagic verwenden. Um die Änderungen zu aktivieren, führen Sie den Befehl `/sbin/lilo -v` aus. LILO zeigt dann die hinzugefügten neuen Kernel an.

KAPITEL 4

Verwalten des Kernels

Neukompilieren des Kernels

Die Administratoren von OpenLinux eServer Systemen entscheiden sich häufig dazu, die verwendeten Kernel neu zu kompilieren. Hierfür gibt es eine Reihe von Gründen: So kann auf diese Weise die Größe des Kernels verringert oder dieser an bestimmte Hardwarekomponenten angepasst werden. Es ist auch möglich, die Unterstützung für Geräte oder Funktionen bereitzustellen, die noch nicht im Kernel enthalten sind, oder nicht benötigte Funktionen zu entfernen. Der Kernel von OpenLinux eServer (und auch die meisten Anwendungen) wurde bereits für Pentium Pro oder bessere Prozessoren optimiert. Wenn Sie aber dennoch Ihren Kernel neu kompilieren möchten, erfahren Sie in diesem Abschnitt, wie Sie hierzu vorgehen müssen.

Am einfachsten erfolgt das Neukompilieren des OpenLinux eServer Kernels dadurch, dass Sie ein neues RPM-Paket erstellen und installieren, in dem alle gewünschten Anpassungen berücksichtigt werden. Gehen Sie hierzu wie folgt vor:

1. Überprüfen Sie zuerst, ob der Kernel Quellcode installiert ist. Falls dies nicht der Fall ist, müssen Sie die Installation nachholen. Sie benötigen mindestens die Dateien `linux-source-common-2.2.14` und `linux-source-i386-2.2.14`. Außerdem muss auf Ihrem Rechner eine geeignete

Entwicklungsumgebung installiert sein. Mit dem ersten Befehl werden die installierten Kernelpakete aufgelistet (falls diese vorhanden sind). Mit dem zweiten und dem dritten Befehl werden die Pakete installiert, die für das Neukompilieren des Kernels mindestens erforderlich sind:

```
# rpm -qa | grep linux
# rpm -ivh linux-source-common-2.2.14-1.i386.rpm
# rpm -ivh linux-source-i386-2.2.14-1.i386.rpm
```

2. Installieren Sie das RPM-Paket mit dem Linux-Quellcode (SRPM). Dieses Paket trägt die Bezeichnung `linux-2.2.13-1.src.rpm`:

```
rpm -ivh linux-2.2.13-1.src.rpm
```

3. Kopieren Sie als nächstes die standardmäßige Kernelkonfigurationsdatei für OpenLinux eServer in der beschriebenen Form in das Verzeichnis für den Kernel Quellcode:

```
# /usr/src/OpenLinux/SOURCES
# cp linux.defconfig.i386.modular /usr/src/linux/.config
```

4. Wechseln Sie in das Verzeichnis mit dem Kernel Quellcode, und verwenden Sie den Befehl `make` in Verbindung mit den üblichen Optionen für das Konfigurieren des Kernels:

```
# cd /usr/src/linux
# make [config | menuconfig | xconfig]
```

5. Nach dem Konfigurieren des Kernels kopieren Sie die neue Konfigurationsdatei, `/usr/src/linux/.config`, zurück in das Quellverzeichnis von OpenLinux:

```
# cd /usr/src/OpenLinux/SOURCES
# cp /usr/src/linux/.config linux.defconfig.i386.modular
```

6. Sie müssen die Schritte 4 und 5 für jede Architektur durchführen, für die Sie einen Kernel erstellen möchten. Standardmäßig werden i386 und i586 kompiliert, und so müssen Sie diese Schritte für die i586-Konfiguration wie folgt wiederholen:

```
# cd /usr/src/OpenLinux/SOURCES
# cp linux.defconfig.i586.modular /usr/src/linux/.config
# cd /usr/src/linux
# make [config | menuconfig | xconfig]
# cd /usr/src/OpenLinux/SOURCES
# cp /usr/src/linux/.config linux.defconfig.i586.modular
```

7. Damit ist der schwierige Teil auch schon abgeschlossen. Als nächstes müssen Sie die Spezifikationsdatei für das RPM-Paket bearbeiten und die Zeile `Release :` in eine Angabe ändern, die Ihren Anpassungen Rechnung trägt (das Zeichen `-` kann jedoch nicht verwendet werden). Die standardmäßige Spezifi-

kationsdatei, `/usr/src/OpenLinux/SPECS/linux.spec`, wird vermutlich wie folgt aussehen:

```
Name : linux
Version : 2.2.14
Release : 1
Group : System/Kernel
```

Angenommen, Sie haben Unterstützung für die Funktion IP-Masquerading hinzugefügt. In diesem Fall sollten Sie die Zeile `Release :` wie folgt ändern:

```
Release : ip_masq
```

8. Erstellen Sie nun das RPM-Paket. Wenn Sie nur das binäre RPM-Paket benötigen, verwenden Sie hierfür folgenden Befehl:

```
# rpm -bb /usr/src/OpenLinux/SPECS/linux.spec
```

Wenn Sie sowohl RPM-Pakete mit Binärcode als auch Quellcode benötigen, verwenden Sie hierfür die Option `-ba` von RPM:

```
# rpm -ba /usr/src/OpenLinux/SPECS/linux.spec
```

Mit dem ersten RPM-Befehl wird ein RPM-Paket mit dem Binärcode und der Bezeichnung `/usr/src/OpenLinux/RPMS/i386/linux-kernel-binary-2.2.14-ip_masq.i386.rpm` erstellt. Mit dem zweiten Befehl wird neben dem Binärpaket zusätzlich noch ein RPM-Paket mit dem Quellcode und der Bezeichnung `/usr/src/OpenLinux/SRPMS/i386/linux-kernel-binary-2.2.14-ip_masq.src.rpm` erstellt.

9. Geben Sie zum Installieren des RPM-Pakets mit dem Binärcode den folgenden Befehl ein:

```
# cd /usr/src/OpenLinux/RPMS/i386/
# rpm -ivh linux-kernel-binary-2.2.14-ip_masq.i386.rpm
```

10. Schließlich müssen Sie LILO nochmals ausführen, um dem Bootloader die Information über den geänderten Kernel zu übergeben:

```
# /sbin/lilo -v
```

Wenn Sie Ihr OpenLinux eServer System zum nächsten Mal booten, wird dabei der neu erstellte Kernel geladen.

Verwenden von Kernelmodulen

Bei Kernelmodulen handelt es sich um Code, der dem Kernel dynamisch hinzugefügt bzw. aus diesem entfernt werden kann. Dieser Code wird häufig verwendet, um bestimmte Hardwaregeräte zu unterstützen oder bestimmte Funktionen wie IP-Masquerading oder BSD-Prozessverwaltung zu aktivieren. Da diese Module

dynamisch geladen und entfernt werden können, ist der Kernel dadurch insgesamt kleiner und schneller.

Ihr OpenLinux eServer System verwendet standardmäßig einen modularen Kernel. Die Module können manuell oder automatisch geladen werden. Im ersten Abschnitt wird kurz das manuelle Laden von Modulen erläutert, bevor dann das von OpenLinux zum automatischen Laden von Modulen beim Booten verwendete System beschrieben wird.

Manuelles Laden von Kernelmodulen

- Um Module manuell laden zu können, müssen Sie die folgenden drei Befehle kennen:
- `insmod` – Fügt Module in den aktuell ausgeführten Kernel ein.
- `rmmod` – Entfernt Module aus dem aktuell ausgeführten Kernel
- `lsmod` – Listet alle Module auf, die in den aktuell ausgeführten Kernel geladen wurden

Die Syntax der einzelnen Befehle ist ziemlich einfach. Um alle aktuell geladenen Module anzuzeigen, verwenden Sie den Befehl `lsmod` wie folgt:

```
# lsmod
Module  Size Used by
isofs   17176 1 (autoclean)
nfs     30168 0 (autoclean)
lockd   31720 0 (autoclean) [nfs]
sunrpc   53924 0 (autoclean) [nfs lockd]
nls_iso8859-1 2020 2 (autoclean)
nls_cp437 3548 1 (autoclean)
vfat    11292 1 (autoclean)
fat      25504 1 (autoclean) [vfat]
```

Aus Platzgründen wurde die Ausgabe des Befehls hier gekürzt.

Um ein Modul zu entfernen, verwenden Sie `rmmod`. Da das Entfernen (und Einfügen) von Modulen Rootberechtigung erfordert, müssen Sie sich als Root angemeldet haben. Bei der Reihenfolge, in der Module entfernt werden, muss zudem berücksichtigt werden, dass manche Module von bestimmten anderen Modulen abhängig sind. Daher müssen diese Module zuerst entfernt werden.

```
# rmmod fat
rmmod: fat is in use
# rmmod vfat
```

```
# rmmod fat
```

Verwenden Sie den Befehl `insmod`, um Module einzufügen. Wenn Sie die Option `-v` (verbose, d.h. erläuternd) in Verbindung mit `insmod` verwenden, geben manche Module zusätzliche Informationen aus, die nützlich sind, falls beim Laden der Module Fehler auftreten.

```
# insmod fat
```

```
# insmod vfat
```

Da das Modul `vfat` vom Modul `fat` abhängt, müssen Sie das Modul `fat` zuerst laden. Wenn Sie sich nicht sicher sind, welche Modulabhängigkeiten existieren, können Sie diese mit dem Befehl `modprobe` in Verbindung mit der Option `-v` auf dem Bildschirm anzeigen. Außerdem bietet Ihnen `modprobe` den Vorteil, dass es die Module durch Aufrufen von `insmod` lädt:

```
# modprobe -v /lib/modules/2.2.12/fs/vfat.o
```

```
/sbin/insmod -L /lib/modules/2.2.12/fs/fat.o
```

```
/sbin/insmod -L /lib/modules/2.2.12/fs/vfat.o
```

Automatisches Laden von Kernelmodulen

Bei der Installation erstellt OpenLinux eServer eine Datei mit der Bezeichnung `/etc/modules/default`, die eine Liste mit den Modulen enthält, die beim Booten automatisch geladen werden sollen. Wenn Ihr System eine initiale RAM-Disk erfordert (`initrd`), wurde auch eine Datei mit der Bezeichnung `/etc/modules/rootfs` angelegt, in der eine Liste mit allen Modulen enthalten ist, die für das Booten des Systems und Mounten des Rootdateisystems erforderlich ist. Die meisten SCSI-Systeme müssen beispielsweise diese Methode nutzen, um SCSI-Treiber laden zu können.

Um automatisch ein neues Modul zu laden, das für das Booten nicht unbedingt erforderlich ist, müssen Sie dieses in die Datei `/etc/modules/default` einfügen. Wenn ein Modul für das Booten hingegen unverzichtbar ist, fügen Sie dieses in `/etc/modules/rootfs` ein. Beachten Sie bitte in diesem Zusammenhang, dass die Reihenfolge von großer Bedeutung sein kann, in der die Module geladen werden. Dies gilt vor allem für den Fall, dass wie im bereits erwähnten Beispiel mit `fat` und `vfat` einzelne Module voneinander abhängig sind.

KAPITEL 5

System- konfiguration und -administration

In diesem Kapitel erhalten Sie grundlegende Informationen über das Ausführen grundlegender Administrationstätigkeiten auf Ihrem OpenLinux eServer System. Da Webmin beim Administrieren Ihres Systems eine besondere Rolle zukommt, wird im folgenden vor allem die Frage behandelt, *wie* Sie mit Webmin eine bestimmte Aktion ausführen und nicht, *weshalb* eine Administratortätigkeit in der beschriebenen Weise vorgenommen werden muss. Nähere Informationen zu dieser Thematik finden Sie in Büchern, Artikel und den HOWTO-Dokumenten, die im Abschnitt "Zusätzliche Ressourcen" am Ende des Kapitels aufgeführt werden. Zusätzliche Informationen stehen auch auf der Website von Caldera Systems in Form von technischen Dokumentationen zur Verfügung.

Verwalten von Benutzern und Gruppen

In diesem Abschnitt lernen Sie, wie Sie unter Ihrem OpenLinux eServer System mit Hilfe des mitgelieferten Tools zur Systemadministration, Webmin, Benutzer

hinzufügen, bearbeiten und löschen können. Sie erhalten zudem Informationen über NIS, das Network Information System, und dessen Konfiguration und Benutzung.

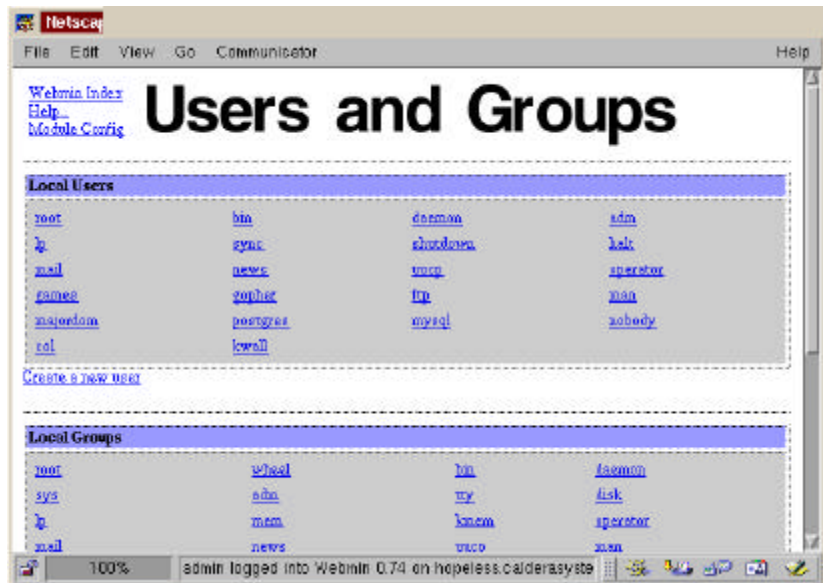
Verwalten von Benutzern und Gruppen mit Webmin

Um mit Webmin Benutzer und Gruppen zu verwalten, starten Sie zunächst Webmin und klicken dann auf das Symbol Users and Groups (siehe Abbildung 30). Der daraufhin angezeigte Hauptbildschirm sieht so ähnlich aus wie in Abbildung 31.

ABBILDUNG 30. Das Symbol Users and Groups in Webmin



ABBILDUNG 31. Der Hauptbildschirm Users and Groups von Webmin



Um einen neuen Benutzer hinzuzufügen, klicken Sie auf die Verknüpfung Create a new user. Analog klicken Sie auf die Verknüpfung Create a new group, um eine

neue Gruppe hinzuzufügen. Die Abbildung 32 zeigt den Bildschirm Create User, nachdem er für das Erstellen eines Benutzers mit der Bezeichnung `gnu_user` ausgefüllt wurde.

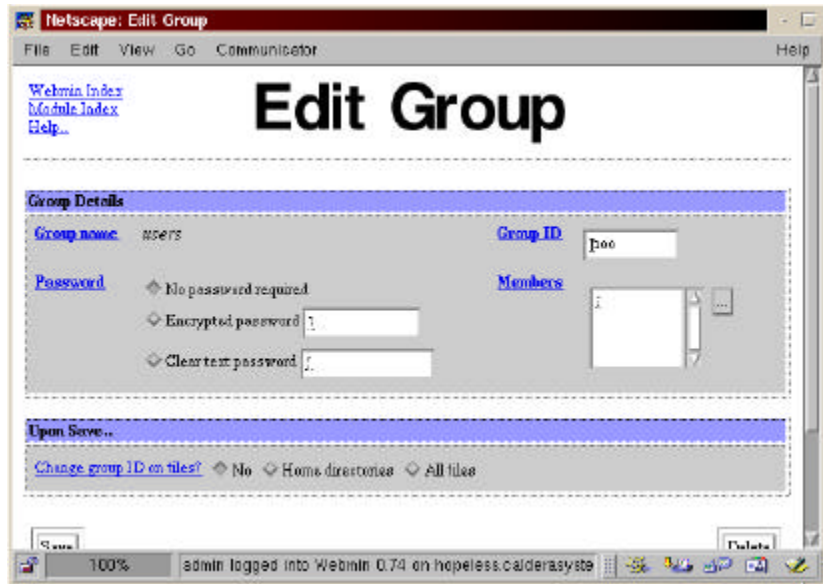
ABBILDUNG 32. Der Bildschirm Create User von Webmin



Bitte beachten Sie in diesem Zusammenhang, dass Webmin standardmäßig keine Informationen über ablaufende Benutzer-Accounts ausgibt. Sollten diese Informationen für Ihr System erforderlich sein, müssen Sie diese selbst erstellen. Sie sollten auch berücksichtigen, dass Ihr OpenLinux eServer System Shadow-Kennwörter verwendet und daher das Optionsfeld "Encrypted password" auswählen. Geben Sie dann den Namen des neuen Benutzers in das entsprechende Textfeld ein. Nachdem Sie alle erforderlichen Informationen eingegeben haben, klicken Sie auf die Schaltfläche Create.

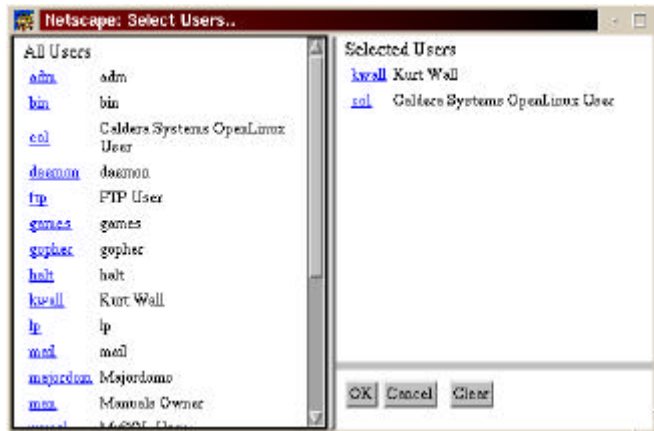
Um die Angaben zu Benutzern oder Gruppen zu bearbeiten, klicken Sie auf einen der aufgeführten Namen von Benutzern oder Gruppen. Abbildung 33 zeigt den Bildschirm Edit Group für die Gruppe `users`.

ABBILDUNG 33. Der Bildschirm Edit Group von Webmin



Um Benutzer in eine Gruppe einzufügen, klicken Sie auf die Schaltfläche mit dem Auslassungszeichen (den drei Punkten). Dadurch wird ein Dialogfeld angezeigt, das eine Liste mit Benutzernamen enthält. Um einen Benutzernamen in eine Gruppe einzufügen, klicken Sie auf diesen wie in Abbildung 34. Nachdem Sie alle erforderlichen Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche Save im unteren Bildschirmbereich, um die Änderungen zu speichern.

ABBILDUNG 34. Hinzufügen von Benutzern in eine Gruppe



Zentrales Verwalten von Benutzern und Gruppen mit NIS

NIS steht für Network Information System¹ und bezeichnet eine Methode zum zentralen Steuern, Administrieren und Verteilen von wichtigen Dateien mit Systemeinstellungen wie beispielsweise Datenbanken mit Kennwörtern oder Dateien zur Netzwerkkonfiguration. *NIS* konvertiert Dateien, die üblicherweise im jeweiligen Verzeichnis `/etc` der einzelnen Rechner gespeichert werden, in Datenbanken mit der Bezeichnung *NIS Maps*. Diese Datenbanken werden an einem zentralen Ort gespeichert (auf dem *NIS-Server*) und mit bestimmten Befehlen aktualisiert. Die Informationen in diesen Maps stehen den *NIS-Clients* auf Anforderung zur Verfügung. Die Zusammenstellung aus einem *NIS-Server* (oder mehreren Servern, falls in einem lokalen Netzwerk mehrere *NIS-Domänen* vorhanden sind) und *NIS-Clients* ergibt eine *NIS-Domäne*.

-
1. *NIS* war früher unter der Bezeichnung *Yellow Pages* bekannt. Auch wenn der Name inzwischen geändert wurde, beginnen die Befehle für die Administration und Interaktion mit *NIS* weiterhin mit `yp`.

Die von NIS ersetzten Dateien werden in Tabelle 8 aufgelistet:

TABELLE 8. Von NIS ersetzte Dateien

Datei	Beschreibung
<u>/etc/ethers</u>	Verwendet vom RARP-System
<u>/etc/hosts</u>	Weist Hostnamen den entsprechenden IP-Adressen zu
<u>/etc/networks</u>	Wird nicht mehr verwendet; ersetzt durch DNS (Domain Name System)
<u>/etc/protocols</u>	Beschreibt die verschiedenen Protokolle, die das TCP/IP-Subsystem zur Verfügung stellt
<u>/etc/services</u>	Weist Namen für Internetdienste, die im Klartext vorliegen, Portnummern und Protokolltypen zu
<u>/etc/aliases</u>	Wird von sendmail verwendet, um gültige Benutzernamen in einen oder mehrere Aliasnamen umzuwandeln und umgekehrt
<u>/etc/passwd</u>	Die Kennwortdatei des Systems
<u>/etc/group</u>	Die Gruppendatei des Systems

Der Vorteil von NIS besteht darin, dass nur eine einzige Fassung dieser Dateien auf einem einzelnen Server gewartet werden muss, wodurch die Verwaltung des Systems durch den System- oder Netzwerkadministrator entscheidend vereinfacht und übersichtlicher gestaltet wird. Obwohl diese Informationen zentral gespeichert werden, können sie von allen Remote-Clients abgerufen werden. Der Hauptnachteil von NIS besteht in gewissen Sicherheitsproblemen. NIS geht nämlich davon aus, dass es sich bei allen Hosts im Netzwerk um vertrauenswürdige Hosts handelt. Daher sollte dieser Dienst *unter keinen Umständen* jemals bei direkter Anbindung an das Internet verwendet werden. Wenn NIS in einem lokalen Netzwerk verwendet wird, muss dieses durch eine wirkungsvolle Firewall geschützt werden.

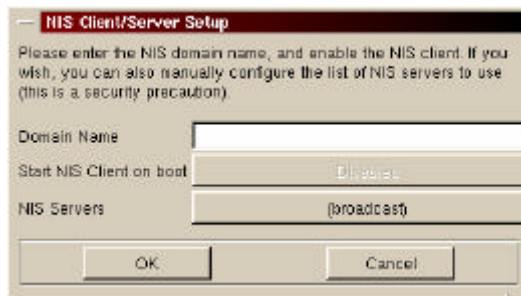
Der erste Schritt bei der Implementierung von NIS besteht darin, dass Sie entscheiden müssen, ob Ihr OpenLinux eServer System als NIS-Masterserver, Slaveserver oder Client genutzt werden soll. Bei einem NIS-*Server* handelt es sich um ein System, auf dem die von NIS verwalteten Informationen zentral gespeichert werden. Ein *Masterserver* ist gewissermaßen die Ausgabestelle für diese Informationen, während so genannte *Slaveserver* immer dann neue Kopien der NIS-Datenbanken vom Masterserver erhalten, wenn die Datenbanken auf dem Masterserver geändert werden. Die Aufgabe von Slaveservern besteht darin, das Funktionieren des NIS-Systems auch dann noch zu gewährleisten, wenn der Masterserver überlastet ist oder aus verschiedenen Gründen nicht zur Verfügung steht. NIS-*Clients* kommunizieren mit den Master- oder Slaveservern, um die Informationen aus den dort gespeicherten NIS-Datenbanken abzurufen.

Konfigurieren von OpenLinux eServer als NIS-Client

Das Konfigurieren Ihres OpenLinux eServer Systems als NIS-Client stellt den einfachsten Fall dar, da bei dieser Konfiguration davon ausgegangen wird, dass in Ihrem Netzwerk bereits ein NIS-Server existiert. Sie müssen den Namen der NIS-Domäne kennen, an die Ihr OpenLinux eServer System angeschlossen wird. Die entsprechenden Informationen erhalten Sie bei Ihrem Systemadministrator. Sobald Sie Ihren NIS-Domänennamen kennen, gehen Sie wie folgt vor:

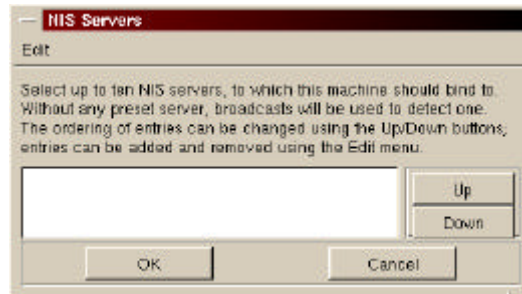
1. Klicken Sie auf die Schaltfläche für das KMenü, und wählen Sie COAS -> Netzwerk -> TCP/IP -> NIS. Daraufhin wird das Dialogfeld wie in Abbildung 35 angezeigt.

ABBILDUNG 35. Dialogfeld NIS Client/Server Setup



2. Geben Sie im Textfeld Domain Name den Domänennamen ein, und drücken Sie die Eingabetaste. Dadurch wird die Schaltfläche neben Start NIS Client on boot aktiviert, die zuvor abgeblendet angezeigt wurde. Klicken Sie auf diese Schaltfläche, oder drücken Sie die Eingabetaste, so dass die Schaltfläche jetzt die Beschriftung Enabled anzeigt.
3. Klicken Sie auf die Schaltfläche neben NIS Servers, um die IP-Adresse von mindestens einem und höchstens zehn NIS-Servern einzugeben. Die Verwendung der Option Broadcast wird nicht empfohlen, da auf diese Weise jeder Benutzer im LAN einen NIS-Server erstellen kann. Wenn Sie hingegen die IP-Adressen Ihrer NIS-Server angeben, erhöhen Sie die Systemsicherheit.
4. Wenn Sie auf die Schaltfläche neben NIS Servers klicken, wird das Dialogfeld NIS Servers wie in Abbildung 36 angezeigt. Klicken Sie in diesem Dialogfeld zunächst in das Textfeld unter Edit. Klicken Sie dann auf die Schaltfläche Add, geben Sie die IP-Adresse ein, und klicken Sie dann auf OK. Wenn Sie alle NIS-Server auf diese Weise hinzugefügt haben, klicken Sie nochmals auf OK.

ABBILDUNG 36. Auswählen von NIS-Servern



5. Klicken Sie im Dialogfeld NIS Client/Server Setup auf OK, um den NIS-Client zu aktivieren. COAS fragt Sie daraufhin, ob Sie die geänderten Informationen speichern möchten. Klicken Sie auf die Schaltfläche Save, um dies zu tun. Im nächsten Dialogfeld werden Sie darüber informiert, dass COAS den NFS-Client neu startet.
6. Um zu überprüfen, ob der Client tatsächlich ausgeführt wird, können Sie einen der folgenden beiden Befehle eingeben:
 \$ rpcinfo -u localhost ypbind
 \$ ps aux | grep ypbind

Die Ausgabe der Befehle sollte so ähnlich wie folgt aussehen:

```
$ rpcinfo -u localhost ypbind
program 10007 version 2 ready and waiting
$ ps aux | grep ypbind
root 2111 0.0 0.4 1252 528 ? S 18:48 0:00 ypbind (master)
root 2113 0.0 0.4 1272 600 ? S 18:48 0:00 ypbind (slave)
```

Konfigurieren von OpenLinux eServer als NIS-Server

Das Einrichten Ihres OpenLinux eServer Systems als NIS-Server ist etwas komplizierter als das Konfigurieren als NIS-Client. Zuerst müssen Sie sich entscheiden, ob Sie Ihren Server als Masterserver, Slaveserver oder als Kombination aus beidem verwenden möchten. Wie bereits zuvor erwähnt, werden auf einem Slaveserver Kopien der NIS-Datenbanken auf dem Masterserver gespeichert und stets aktualisiert, wenn Änderungen am Masterserver vorgenommen werden. Dadurch wird eine gewisse Redundanz gewährleistet, falls der Masterserver überlastet ist oder ausfällt. Beim Masterserver handelt es sich um die Ausgabestelle für die NIS-Datenbanken.

Wenn Sie die RPM-Pakete für `nis-server` und `nis-client` noch nicht installiert haben, müssen Sie dies jetzt nachholen. Falls Ihr CD-ROM-Laufwerk unter `/mnt/cdrom` gemountet wurde, können Sie mit dem folgenden Befehl beide Pakete installieren (für die meisten der folgenden Schritte ist Rootzugriff erforderlich).

```
# rpm -ivh /mnt/cdrom/col/Packages/RPMS/nis-*
```

1. Legen Sie einen Namen für die NIS-Domäne fest. Für den NIS-Domänennamen muss nicht ein weltweit nur einmal vorkommender Name verwendet werden, es ist ausreichend, wenn sich die Namen angrenzender Domänen nicht überschneiden.
2. Erstellen Sie ein Verzeichnis mit der Bezeichnung `/etc/nis/$NISDOMAIN`, in dem die Ressourcenmaps gespeichert werden. Wenn der Name Ihrer NIS-Domäne beispielsweise `nistest` lautet, müssen Sie hierfür folgenden Befehl eingeben

```
# mkdir /etc/nis/nistest
```
3. Legen Sie den NIS-Domänennamen mit COAS fest, aber nur für eine primäre Domäne, die auch den Server enthält. Für alle weiteren Domänen müssen Sie lediglich die Verzeichnisse in `/etc/nis` erstellen. In den entsprechenden Abbildungen werden die Konfigurationsbildschirme von COAS für NIS angezeigt.
4. Kopieren Sie alle Dateien, die Sie für das lokale Netzwerk freigeben möchten, in das in Schritt 3 erstellte Verzeichnis. Die Dateien `/etc/passwd` und `/etc/shadow` dürfen jedoch nicht in dieses Verzeichnis kopiert werden. Ein Fehler im Remote-Prozeduraufruf (RPC) zum Ändern von Kennwörtern erlaubt es nicht, die Masterkennwortdateien für mehrere Domänen auf dem gleichen Server zu speichern. Kopieren Sie `/etc/passwd` und `/etc/shadow` direkt in das Verzeichnis `/etc/nis`.

```
# cp /etc/aliases /etc/nis/nistest
# cp /etc/group /etc/nis/nistest
# cp /etc/passwd /etc/nis
# cp /etc/shadow /etc/nis
```
5. Erstellen Sie symbolische Verknüpfungen mit `/etc/nis/passwd` und `/etc/nis/shadow` in dem bei Schritt 1 erstellten Verzeichnis für die primäre NIS-Domäne. Unter Verwendung des in Schritt 3 vorgeschlagenen Domänennamens müssen hierfür folgende Befehle ausgeführt werden:

```
# ln -s /etc/nis/passwd /etc/nis/nistest/passwd
# ln -s /etc/nis/shadow /etc/nis/nistest/shadow
```
6. Kopieren Sie `/etc/nis/.nisupdate.conf.sample` in das bei Schritt 1 erstellte Verzeichnis für die primäre NIS-Domäne. Bearbeiten Sie die Konfigu-

rationsdateien für die freizugebenden Maps, indem Sie die Kommentarzeichen bei den Regeln für die Maps entfernen, die Sie verwenden möchten. Geben Sie hierzu folgenden Befehl ein:

```
# cp /etc/nis/nisupdate.conf.sample /etc/nis/nistest/nisuate.conf
```

7. Führen Sie `/etc/nis/nis_update` aus. Dies ist immer dann erforderlich, wenn eine der Dateien geändert wurde. In diesem Skript finden Sie auch Beispiele, welche Dateien ebenfalls in das NIS-Verzeichnis kopiert werden müssen. Die Ausgabe dieses Befehls sollte wie folgt aussehen:

```
# /etc/nis/nis_update
Processing domain nistest
Updating nistest/aliases
Updating nis/group
```

8. Führen Sie `/etc/rc.d/init.d/nis-server start` aus. Dieser Schritt wird normalerweise beim Booten automatisch vorgenommen, muss aber nach der erstmaligen Installation manuell ausgeführt werden.
9. Führen Sie den Befehl `ypwhich` aus, um zu überprüfen, ob Ihre NIS-Serverkonfiguration ordnungsgemäß eingerichtet wurde. Falls dies der Fall ist, gibt `ypwhich` den vollständigen Domänennamen des NIS-Servers aus.

Webmin Tools zur Systemadministration

In diesem Abschnitt wird die Verwendung einer Reihe von Tools in Webmin zur Systemadministration erläutert. Zu den behandelten Themen zählen:

- Verwalten von Cron-Jobs
- Verwenden des Tools zur Partitionierung
- Verwalten des Dateisystems
- Prozesssteuerung
- Paketverwaltung
- Fortgeschrittene Systemkonfiguration mit Webmin

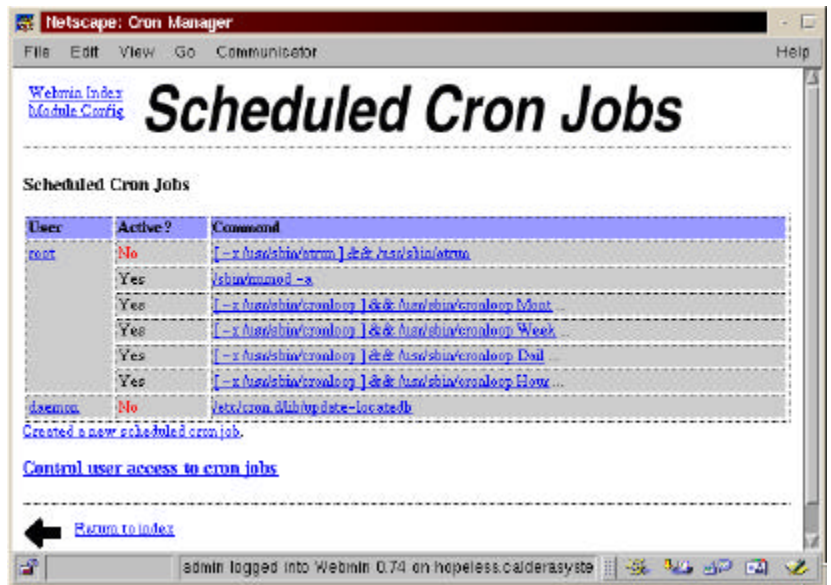
Verwalten von Cron-Jobs

Mit Webmin können Sie die Cron-Jobs in Ihrem System verwalten (die in der Datei `/etc/crontab` aufgelistet werden) und festlegen, welche normalen Benutzer mit welchen Rechten auf cron zugreifen dürfen. Klicken Sie hierzu zuerst auf das Symbol Scheduled Cron Jobs, das in Abbildung 37 dargestellt wird. Webmin zeigt daraufhin einen Bildschirm an, der so ähnlich wie in Abbildung 38 aussehen sollte.

ABBILDUNG 37. Das Symbol Scheduled Cron Jobs

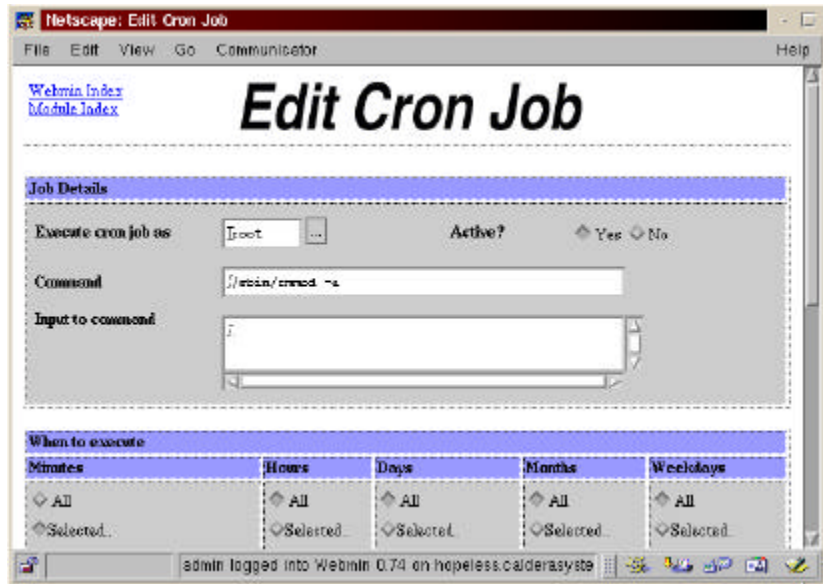


ABBILDUNG 38. Das Symbol Scheduled Cron Jobs



Wie Sie in Abbildung 38 erkennen können, werden in der oberen Hälfte des Bildschirms alle Cron-Jobs aufgelistet, jeweils mit Angaben zum Status (aktiv oder inaktiv) und dem auszuführenden Befehl. Um einen vorhandenen Cron-Job zu bearbeiten, klicken Sie auf den Befehl neben dem entsprechenden Eintrag für diesen Job. Webmin zeigt daraufhin einen Bildschirm mit einer einfachen und intuitiven Benutzeroberfläche an, mit dem Sie diesen Cron-Job bearbeiten können. Abbildung 39 zeigt diesen Bildschirm zum Bearbeiten für einen der in Abbildung 38 aufgelisteten Cron-Jobs.

ABBILDUNG 39. Der Bildschirm Edit Cron Job



In der Eingabemaske Job Details können Sie den Namen des Benutzers, der diesen Job besitzt, und den auszuführenden Befehl ändern. Im Feld Input to command können Sie zudem zusätzliche Eingabedateien angeben. Um den Job zu deaktivieren (dieser wird zu diesem Zweck in der Datei `/etc/crontab` auskommentiert), wählen Sie das Optionsfeld No neben dem Prompt Active?. Im unteren Bereich des Bildschirms können Sie die Zeiten festlegen, zu denen der Job ausgeführt werden soll. Wenn Sie alle Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche Save, um Ihre Änderungen zu speichern. Das Erstellen neuer Cron-Jobs ähnelt in weiten Teilen dem Bearbeiten vorhandener Jobs. Der wesentliche Unterschied besteht darin, dass Sie alle Angaben in den Bereichen Job Details und When to execute selbst eintragen müssen.

Beachten Sie bitte, dass es sich bei allen von Ihnen hier erstellten oder bearbeiteten Cron-Jobs um *System-Cron-Jobs* handelt. Um persönliche crontabs zu erstellen, müssen Sie den Befehl `crontab` verwenden.

Um den Zugriff von normalen Benutzern auf cron einzuschränken, klicken Sie auf die Verknüpfung Control user access to cron jobs. Abbildung 40 zeigt den Bildschirm Control Cron Access von Webmin.

ABBILDUNG 40. Der Bildschirm Control Cron Access von Webmin



Die verfügbaren Optionen sind einfach zu verstehen. Standardmäßig ist cron so konfiguriert, dass alle Benutzer Zugriff erhalten. Um allen Benutzern mit Ausnahme einiger weniger autorisierter Benutzer den Zugriff zu verwehren, wählen Sie das Optionsfeld **Allow only listed users**. Geben Sie dann entweder die Namen der zugelassenen Benutzer ein, oder wählen Sie deren Benutzernamen in einem Dialogfeld aus, das beim Klicken auf die Schaltfläche mit dem Auslassungszeichen angezeigt wird. Um hingegen prinzipiell allen Benutzern mit Ausnahme einiger weniger Benutzer den Zugriff auf cron zu *erlauben*, wählen Sie das Optionsfeld **Deny only listed users** und geben dann die Namen der Benutzer ein, die cron nicht verwenden dürfen. Klicken Sie auf die Schaltfläche **Save**, wenn Sie fertig sind.

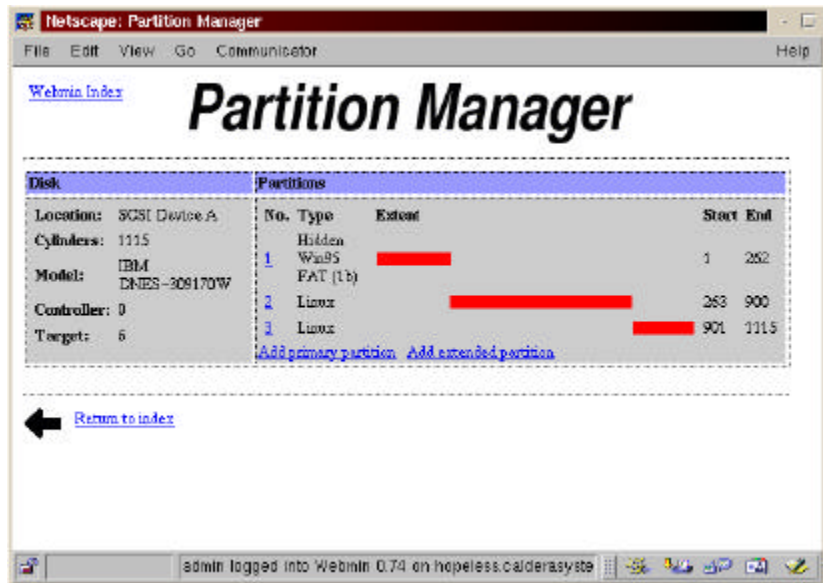
Verwalten von Festplattenpartitionen

Mit Webmin können Sie die Partitionen auf Ihren lokalen Festplatten verwalten. Klicken Sie zunächst auf das Symbol **Partitions on Local Disks** (siehe Abbildung 41). Abbildung 42 verdeutlicht, wie Webmin die Festplattenpartitionen auf Ihrem System anzeigt.

ABBILDUNG 41. Das Symbol Partitions on Local Disks



ABBILDUNG 42. Der Bildschirm Partition Manager



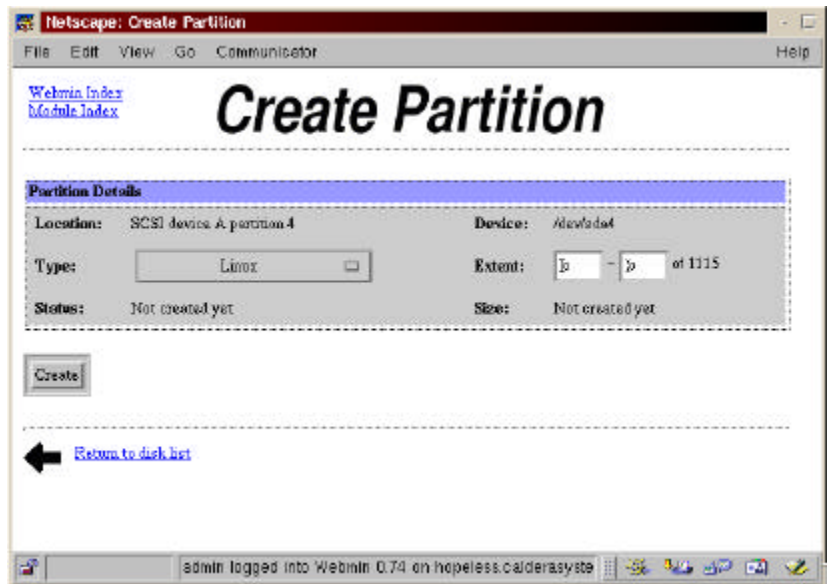
Auf der linken Seite des Bildschirms listet Webmin den Gerätenamen, Informationen zur Geometrie und die Modellbezeichnung der Festplatte auf. Auf der rechten Seite werden die Partitionen grafisch angezeigt. Wie Sie in Abbildung 42 sehen können, sind auf dem System in unserem Beispiel eine Windows-Partition, eine Linux-Swap-Partition und eine primäre Linux-Partition vorhanden, die (in dieser Reihenfolge) den Gerätenamen `/dev/hda1`, `/dev/hda2` und `/dev/hda3` entsprechen.

Um eine Partition zu bearbeiten, klicken Sie auf deren Nummer, nehmen die erforderlichen Änderungen vor und klicken dann auf die Schaltfläche **Change**. Um eine Partition zu löschen, wählen Sie analog deren Partitionsnummer aus und klicken auf die Schaltfläche **Delete** in der unteren linken Ecke des Bildschirms. **HINWEIS:** Wenn Sie eine Partition ändern oder löschen möchten, muss diese zuvor

ungemountet werden und darf momentan nicht in Gebrauch sein. Andernfalls sperrt Webmin den Zugriff auf diese Partition.

Auch das Hinzufügen von Partitionen ist einfach. Klicken Sie hierzu auf die Verknüpfung Add primary partitions im Bildschirm Partition Manager. Der anschließend angezeigte Bildschirm sollte in etwa dem in Abbildung 43 entsprechen.

ABBILDUNG 43. Der Bildschirm Create Partition von Webmin



Wenn Sie nur über eine einzelne Festplatte verfügen, ist der Eintrag für Location bereits vorgegeben. Mit Hilfe der Dropdown-Liste können Sie den Partitionstyp und das Gerät auswählen. Wenn Sie die Größe ändern möchten, können Sie in den beiden Textfeldern neben Extent den Anfangs- und/oder Endzylinder bearbeiten. Wenn Sie damit fertig sind, klicken Sie auf die Schaltfläche Create, um die Partition zu erstellen. Der für das Erstellen einer erweiterten Partition erforderliche Vorgang ist weitgehend ähnlich. Sie müssen in diesem Fall allerdings auf die Verknüpfung Add extended partition klicken.

Verwalten von Dateisystemen

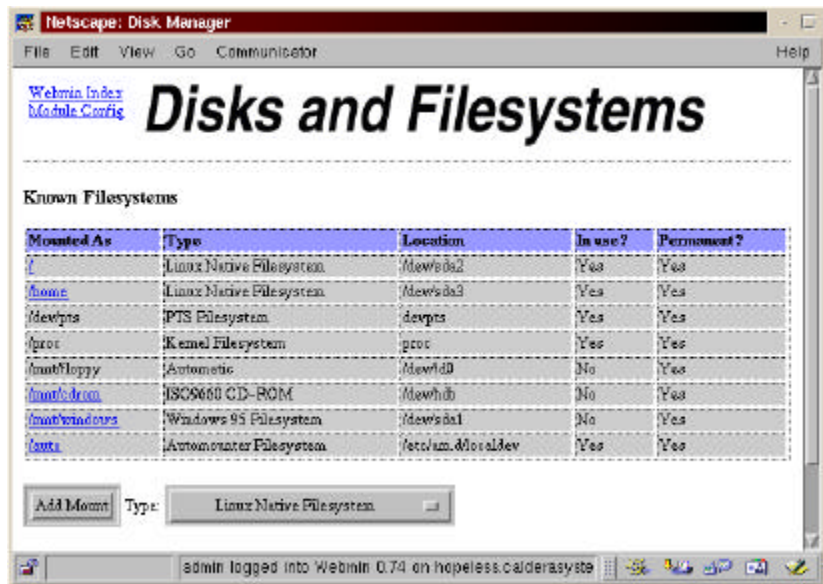
Mit Hilfe des Managers für das Dateisystem von Webmin können Sie 14 verschiedene Dateisysteme mounten, unmounten, erstellen, bearbeiten und löschen.

Klicken Sie zunächst auf die Verknüpfung Disk and Network Filesystems, die in Abbildung 44 abgebildet ist. Dadurch wird der Bildschirm Disks and Filesystem geöffnet, den Sie in Abbildung 45 sehen.

ABBILDUNG 44. Das Symbol Disk and Network Filesystems

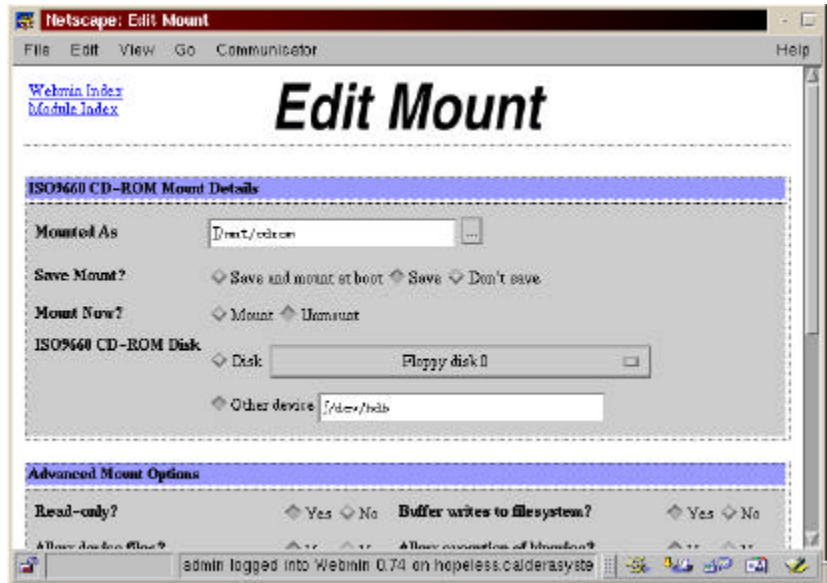


ABBILDUNG 45. Der Bildschirm Disks and Filesystems



Nach dem Aufrufen des Bildschirms zeigt Webmin alle auf Ihrem System verfügbaren Dateisysteme an, unabhängig davon, ob diese aktiv bzw. gemountet sind oder nicht. Sie sehen im Einzelnen den Mountpoint, den Typ des Dateisystems, den Gerätenamen oder Speicherort sowie die Angabe, ob ein Dateisystem gemountet ist oder in `/etc/fstab` aufgelistet wird. Um eines der aufgelisteten Dateisysteme zu bearbeiten, klicken Sie auf dessen Mountpoint, der in der ersten Spalte aufgeführt wird. Je nach ausgewähltem Dateisystem ändert sich die Anzeige auf dem Bildschirm geringfügig. Abbildung 46 zeigt den Bildschirm zum Bearbeiten für `/mnt/cdrom`, dessen Eintrag in Abbildung 45 aufgelistet ist.

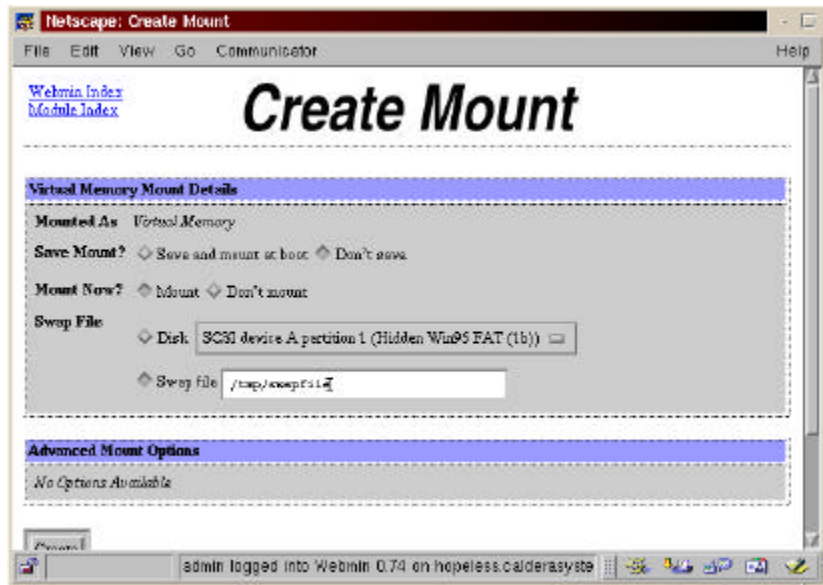
ABBILDUNG 46. Beispiel für den Bildschirm Edit Mount



Die Bedeutung der meisten Felder sollte problemlos verständlich sein. Wenn Sie einen Mountpoint im Feld Mounted As angeben, der noch nicht existiert, wird dieser von Webmin erstellt. Die Standardangaben in der Eingabemaske Advanced Mount Options sollten für die meisten Fälle geeignet sein, können aber natürlich bei Bedarf geändert werden. Nachdem Sie die Änderungen abgeschlossen haben, klicken Sie auf die Schaltfläche Apply, um die Datei `/etc/fstab` zu aktualisieren und die neuen Einstellungen zu aktivieren.

Wenn Sie ein neues Dateisystem hinzufügen möchten, wählen Sie zuerst den Typ des zu erstellenden Dateisystems in der Dropdown-Liste im unteren Bildschirmbereich aus und klicken dann auf die Schaltfläche Add. Wie Sie bereits bei anderen Webmin-Modulen gesehen haben, ist der Bildschirm zum Erstellen üblicherweise dem Bildschirm zum Bearbeiten sehr ähnlich, nur mit dem Unterschied, dass Sie beim Erstellen alle Eingaben selbst vornehmen müssen. Dies gilt auch für die Bildschirme Create Mount und Edit Mount. Bitte beachten Sie in diesem Zusammenhang, dass die verfügbaren Optionen vom Typ des zu erstellenden Dateisystems abhängen. Abbildung 47 zeigt das Erstellen einer Swap-Datei.

ABBILDUNG 47. Erstellen einer Swap-Datei



Da Swap-Dateien nur temporär verwendet werden, wurde das Optionsfeld Don't Save ausgewählt, wodurch kein Eintrag für die Swap-Datei in `/etc/fstab` angelegt wird. Die Swap-Datei erhält in unserem Beispiel die Bezeichnung `/tmp/swapfile`. Klicken Sie auf die Schaltfläche Create, um Ihre Änderungen zu aktivieren. Je nach Typ des von Ihnen erstellten Dateisystems wird noch ein weiterer Bildschirm angezeigt oder die Eingabe zusätzlicher Informationen verlangt, bevor Webmin das Dateisystem erstellt.

Prozesssteuerung

Beim Prozessmanager von Webmin handelt es sich im Prinzip um eine browserbasierte Version des bekannten Tools `top`, die Ihnen aber im Gegensatz zu `top` auch das Ausführen von beliebigen Befehlen ermöglicht. Durch Klicken auf das Symbol Running Processes (siehe Abbildung 48) wird der Bildschirm Process Manager aufgerufen, der in Abbildung 49 dargestellt wird.

ABBILDUNG 48. Das Symbol Running Processes



ABBILDUNG 49. Der Bildschirm Process Manager von Webmin



Standardmäßig werden die Prozesse in der Anzeige nach der PID (Prozess-ID) sortiert. Sie können die Anzeige aber auch nach Benutzernamen, benötigtem Speicher und benötigter CPU-Zeit anordnen lassen, Hierzu müssen Sie (in dieser Reihenfolge) auf die Verknüpfungen User, Memory und CPU an der Oberseite des Bildschirms klicken.

Um einen bestimmten Prozess ausfindig zu machen, klicken Sie auf die Verknüpfung Search. Sie können eines der in Tabelle 9 aufgelisteten Suchkriterien auswählen, indem Sie das Optionsfeld neben der Kategorie wählen, Ihr Kriterium eingeben und auf die Schaltfläche Search klicken. Für jeden Prozess werden PID, Besitzer,

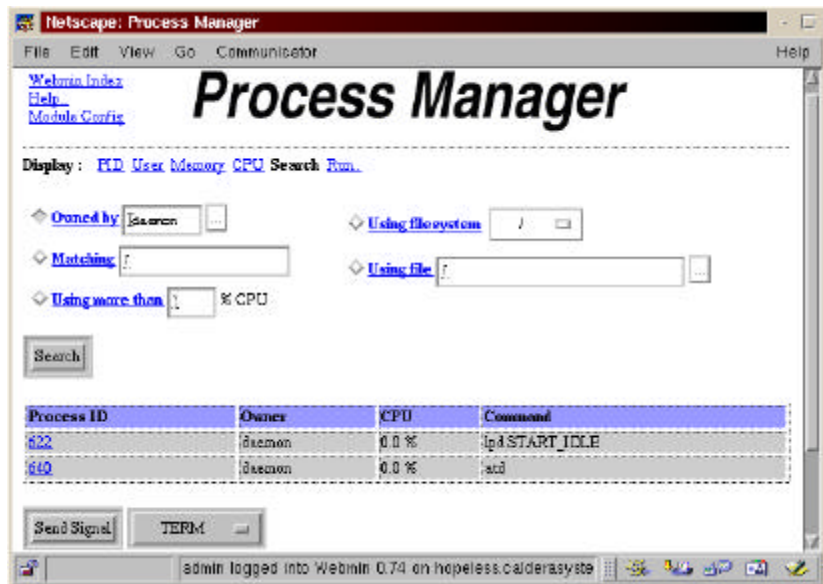
CPU-Nutzung und Befehl angezeigt. Klicken Sie auf die PID eines Prozesses, um weitere Informationen über diesen abzurufen.

TABELLE 9. Suchkriterien im Prozessmanager

Kriterium	Beschreibung
Owned by	Geben Sie den Namen eines Benutzers ein, oder wählen Sie einen Namen im Popup-Fenster aus
Matching	Geben Sie eine Zeichenfolge ein
Using more than % CPU	Geben Sie einen Zahlenwert zwischen 0 und 100 ein
Using filesystem	Wählen Sie ein Dateisystem in der Dropdown-Liste aus
Using file	Geben Sie einen Dateinamen ein

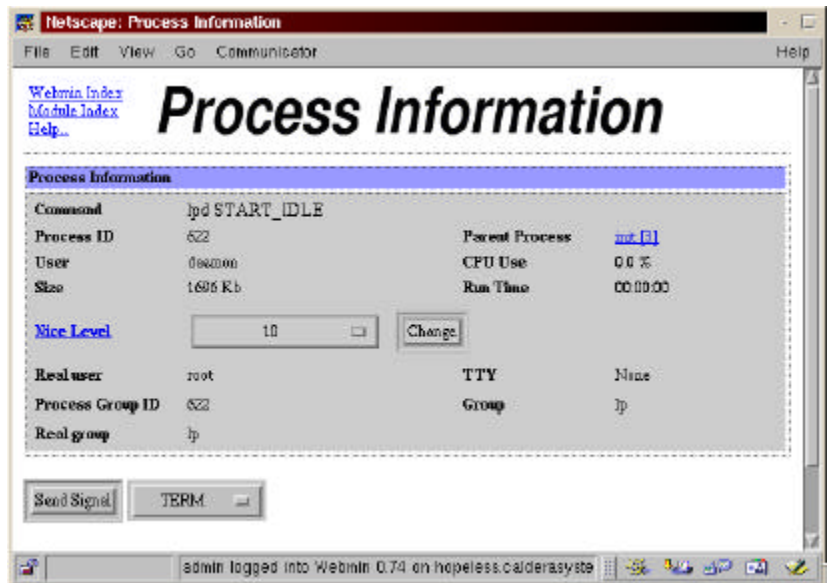
In Abbildung 50 sehen Sie, welches Ergebnis bei einer Suche nach allen Prozessen im Besitz des Benutzers daemon angezeigt wird.

ABBILDUNG 50. Suche nach Prozessen im Besitz des Benutzers daemon



Sie können den Prozessmanager auch verwenden, um die Priorität eines Prozesses zu ändern. Klicken Sie im Hauptfenster oder dem Suchfenster auf eine PID. Wählen Sie dann im daraufhin angezeigten Bildschirm, der Abbildung 51 ähnelt, eine neue Priorität (auch als *nice level* bezeichnet) in der Dropdown-Liste aus, und klicken Sie dann auf die Schaltfläche Change. Beachten Sie in diesem Zusammenhang, dass mit zunehmenden Zahlenwerten der jeweilige Nice Level sinkt.

ABBILDUNG 51. Ändern der Priorität von Prozessen mit dem Prozessmanager von Webmin



Vom gleichen Bildschirm wie in Abbildung 53 können Sie auch ein Signal an einen Prozess senden. Tabelle 10 listet die gebräuchlichsten Signale und deren Funktion auf.

TABELLE 10. Gebräuchliche Prozesssignale

Signal	Beschreibung
INT	Sendet einen Tastaturinterrupt (Strg+C). Beendet den Prozess.
QUIT	Beendet den Prozess.
ABRT	Beendet den Prozess und erstellt einen Speicherauszug (Coredatei).
KILL	Beendet den Prozess. Kann nicht ignoriert werden.
HUP	Beendet den Prozess, fall dieser SIGHUP nicht unterstützt.
TERM	Beendet den Prozess.
STOP	Hält den Prozess an, beendet ihn aber nicht vollständig.
CONT	Setzt die Ausführung eines angehaltenen Prozesses wieder fort.

Wenn Sie also beispielsweise einen Prozess endgültig beenden möchten, wählen Sie in der Dropdown-Liste den Befehl KILL im unteren Bildschirmbereich Process Information aus und klicken auf die Schaltfläche Send Signal.

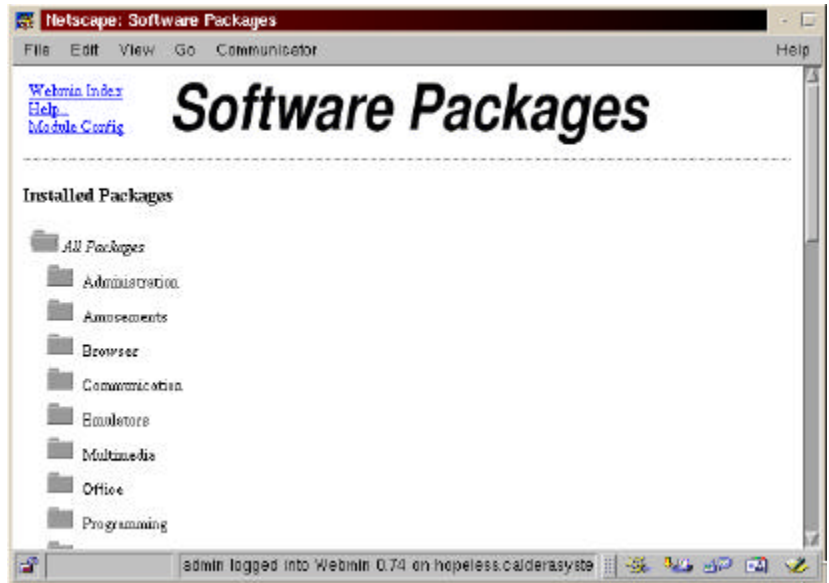
Software-Paketmanagement

Durch Klicken auf das Symbol Software Packages (siehe Abbildung 52) wird die Benutzeroberfläche von Webmin zum Verwalten der Pakete von OpenLinux eServer angezeigt. Der Hauptbildschirm des Paketmanagers wird in Abbildung 53 dargestellt.

ABBILDUNG 52. Das Symbol Software Packages

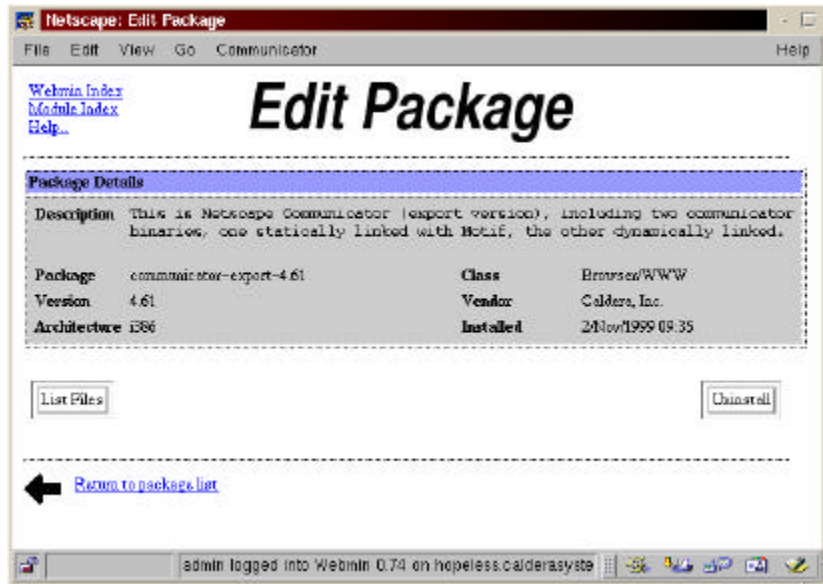


ABBILDUNG 53. Der Bildschirm Package Manager



In der Bildschirmanzeige in Abbildung 53 sind verschiedene Paketgruppen wie Administration, Applications, Browser usw. zu sehen. Wenn Sie auf einen Ordner klicken, werden die darin enthaltenen Unterkategorien angezeigt, die wiederum Listen mit den installierten Paketen wie in der Abbildung enthalten. Wenn Sie auf einen Paketnamen klicken, können Sie detaillierte Informationen zu diesem Paket abrufen, die darin enthaltenen Dateien auflisten oder das Paket deinstallieren. Der Bildschirm Edit Package für das Paket sniffit wird in Abbildung 54 dargestellt.

ABBILDUNG 54. Der Bildschirm Edit Package von Webmin



Fortgeschrittene Webmin-Konfiguration

Wie Sie wohl schon erwartet haben, erfolgt auch die Verwaltung von Webmin selbst über die gleiche browserbasierte Oberfläche, die auch für die Systemadministration Verwendung findet. Nachdem Sie auf das Symbol Webmin Users geklickt haben, das in Abbildung 55 zu sehen ist, können Sie die Liste mit den autorisierten Webmin-Benutzern bearbeiten und Benutzer hinzufügen, löschen oder modifizieren. Durch Klicken auf das Symbol Webmin Configuration (siehe Abbildung 56) wird ein Bildschirm aufgerufen, mit dem das Verhalten von Webmin konfiguriert werden kann.

ABBILDUNG 55. Das Symbol Webmin Users



ABBILDUNG 56. Das Symbol Webmin Configuration



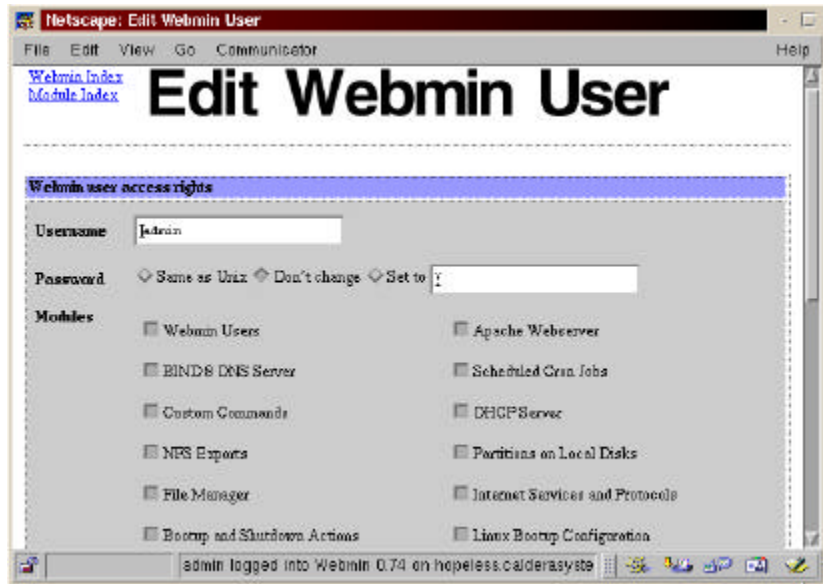
Wenn Sie auf das Symbol Webmin Users klicken, wird ein Bildschirm angezeigt, der so ähnlich wie in Abbildung 57 aussieht. In der ersten Spalte wird ein Benutzername angezeigt, während in der zweiten Spalte die Module aufgelistet werden, auf die der Benutzer zugreifen kann.

ABBILDUNG 57. Der Bildschirm Webmin Users



Klicken Sie auf den Benutzernamen, um die Liste mit Modulen zu ändern, auf die der Benutzer zugreifen darf. Aktivieren oder deaktivieren Sie hierzu einfach die Kontrollkästchen neben den verschiedenen Modulen wie in Abbildung 58.

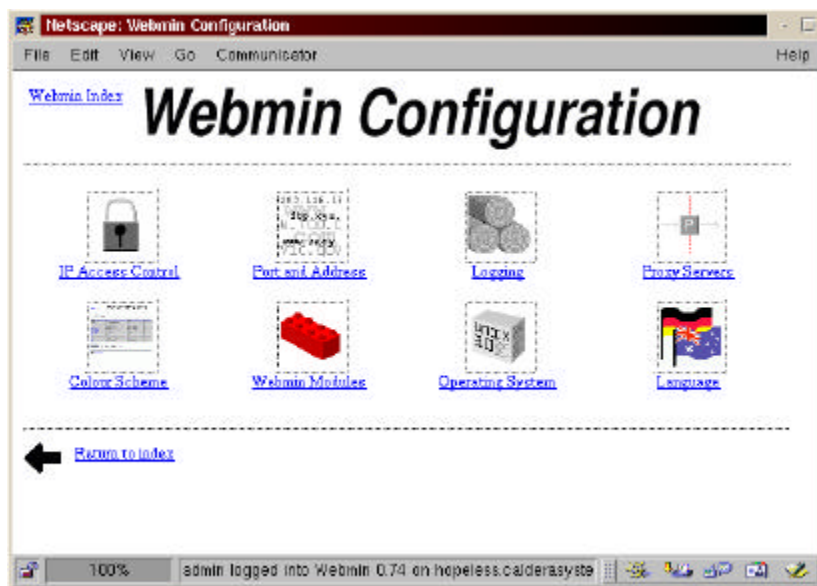
ABBILDUNG 58. Der Bildschirm Edit Webmin Users



Jedes Modul verfügt über eigene Konfigurationsoptionen, die durch Klicken auf die Modulnamen in der zweiten Spalte angezeigt werden können. Schon allein aus Platzgründen wäre es nicht möglich, alle Optionen hier zu beschreiben. In allen Konfigurationsoptionen kann jedoch festgelegt werden, dass ein bestimmter Benutzer das Recht zum Bearbeiten der Modulkonfiguration erhält. Die meisten Module verfügen über detaillierte Hilfebildschirme, über die Sie weitergehende Informationen über die Konfiguration der Module abrufen können. Die Standardkonfiguration sollte aber in den allermeisten Fällen völlig ausreichend sein.

Nachdem Sie auf das Symbol Webmin Configuration geklickt haben, wird ein Bildschirm wie in Abbildung 59 angezeigt. Von diesem Bildschirm aus können Sie festlegen, wie der Zugriff auf Webmin erfolgen soll, wie die standardmäßigen Einstellungen für Port und Adresse lauten usw. Sie sollten diese Einstellungen allerdings erst dann ändern, wenn Sie sich mit der Verwendung von Webmin vertraut gemacht haben.

ABBILDUNG 59. Der Bildschirm Webmin Configuration



KAPITEL 6

Tools zur Netzwerk- überwachung

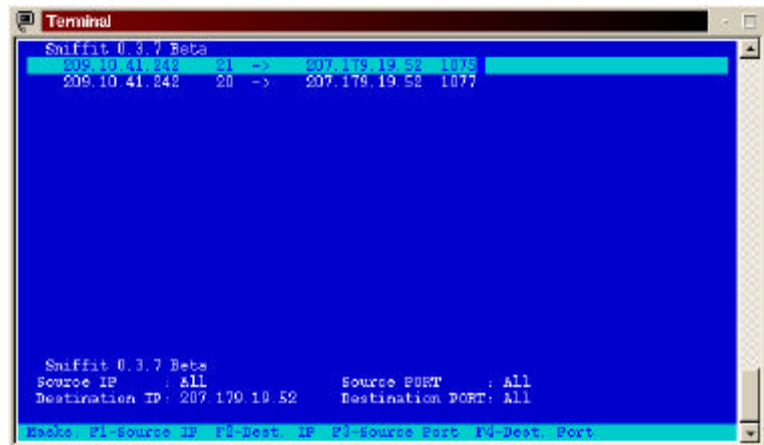
Dieses Kapitel beschreibt einige Tools zur Netzwerküberwachung. Dazu gehören Sniffit, Netwatch und tcpdump. Mit diesen Tools können Sie die Arten und den Umfang des Datenverkehrs im Netzwerk aufzeichnen, wodurch sich wiederum potentielle Sicherheitsprobleme und Leistungsengpässe erkennen lassen.

Verwenden von Sniffit

Dieser Abschnitt beschreibt die Konfiguration von Sniffit. Sniffit ist ein Paketüberwachungsprogramm für TCP/IP-Netzwerke. Es überwacht den Netzwerkverkehr auf der Paketebene, einschließlich IP, TCP, UDP und ICMP-Pakete. Das Tool lässt sich für die Protokollierung aller eingehenden Pakete sowie für die Filterung und Aufzeichnung von Paketen eines bestimmten Typs oder auf einem bestimmten Port konfigurieren. Sniffit kann auch im interaktiven Modus ausgeführt werden, wodurch eine Überwachung des Netzwerkverkehrs in Echtzeit möglich ist.

Wenn Sie Sniffit im interaktiven Modus ausführen, wird seine Ausgabe in einer auf ncurses basierenden grafischen Benutzeroberfläche angezeigt. Starten Sie dazu Sniffit mit der Option `-i` oder `-I`. Im interaktiven Modus können Sie die Quelle und das Ziel aller im Netzwerk übertragenen Pakete sehen. Die Abbildungen 60 und 61 illustrieren den grafischen Modus von Sniffit.

ABBILDUNG 60. Ausführung von Sniffit im interaktiven Modus



In Abbildung 62 zeigen die ersten beiden Spalten die Ausgangs-IP-Adresse sowie den Ausgangsport der Pakete. Die Pfeile in der dritten Spalte zeigen die Richtung, in der die Pakete übertragen werden. Die vierte und fünfte Spalte enthalten die Ziel-IP-Adressen und Ports. In der letzten Spalte wird der Datentyp aufgeführt, den die Pakete enthalten (falls bekannt).

Die erste Zeile zeigt, dass der Host mit der IP-Adresse 209.10.41.242, Port 21, FTP-Daten an die Adresse 207.179.19.52, Port 1075 sendet. In diesem Fall hat das Zielsystem die Kernelsource von der Adresse ftp.kernel.org heruntergeladen.

Abbildung 61 zeigt die gleichen Informationen wie 60, mit der Ausnahme, dass ein kleineres Fenster die kumulative Statistik für den Netzwerkdatenverkehr enthält. Sie können diese Anzeige durch Drücken von `n` wechseln.

ABBILDUNG 61. Anzeigen von kumulativen Statistiken des Netzwerkdatenverkehrs

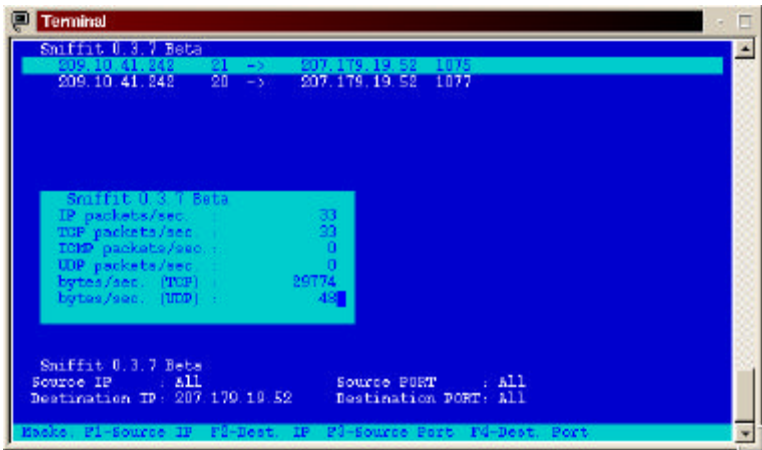


Tabelle 11 enthält eine Liste der Tastatureingaben, die im interaktiven Modus von Sniffit verfügbar sind.

TABELLE 11. Sniffit-Tastatureingaben

Tastatureingabe	Beschreibung
NACH OBEN-TASTE, k	Zur vorherigen Zeile wechseln
NACH UNTEN-TASTE, j	Zur nächsten Zeile wechseln
F1, 1	Die Adresse des überwachten Ausgangshosts ändern
F2, 2	Die Adresse des überwachten Zielhosts ändern
F3,3	Die auf dem Ausgangshost zu überwachende Portnummer ändern
F4, 4	Die auf dem Zielhost zu überwachende Portnummer ändern
n	Die Anzeige der Netzwerkstatistik ändern
q	Beenden

Wenn der interaktive Modus von Sniffit für die Echtzeitüberwachung auch durchaus nützlich ist, wird das Tool häufiger für die Filterung bestimmter Paket- oder Hosttypen und zur Protokollierung in eine oder mehrere Protokolldateien konfigu-

riert. Mit den Befehlszeilenparametern in Tabelle 12 können Sie die Funktionsweise von Sniffit anpassen.

TABELLE 12. Befehlszeilenoptionen für den Batchmodus von Sniffit

Option	Argument	Beschreibung
-v	<ohne>	Version anzeigen und beenden
-t	{ <i>IP-Adresse</i> }	Pakete mit Ziel { <i>IP-Adresse</i> } überwachen
-s	{ <i>IP-Adresse</i> }	Pakete mit Ursprung { <i>IP-Adresse</i> } überwachen
-c	{ <i>Datei</i> }	Konfigurationsinformationen aus <i>Datei</i> lesen
-d	<ohne>	Rawpakete als Bytesequenzen im Hexadezimalformat ausgeben
-a	<ohne>	Rawpakete als Bytesequenzen im ASCII-Format ausgeben
-p	<i>N</i>	Portnummer <i>N</i> überwachen, 0 = alle Ports
-L	{ <i>Protokollparam</i> }	Protokollierungsebene auf <i>Protokollparam</i> einstellen

Die Optionen `-s` und `-t` erkennen das Schlüsselwort `all`, das bewirkt, dass Sniffit den Datenverkehr im gesamten Subnetz eines Systems überwacht, sowie das Platzhalterzeichen `@`. Beispiel:

```
# sniffit -s 192.68.9@
```

überwacht alle Pakete mit den Ausgangs-IP-Adressen 192.68.90.0 bis 192.68.99.255. Analog dazu:

```
# sniffit -t 192.68.90.@
```

überwacht alle Pakete mit den Ziel-IP-Adressen im Bereich 192.68.90.0 bis 192.68.99.255.

Mit der Option `-p` können Sie bestimmte Ports überwachen. Wenn Sie beispielsweise die Daten überwachen möchten, die an den Telnetport eines Systems gesendet werden, verwenden Sie die Option `-p 23` wie folgt:

```
# sniffit -p 23 -t 192.68.90.234
```

Mit den Optionen `-d` und `-a` wird Sniffit veranlasst, die Rawpakete im Hexadezimal- bzw. ASCII-Format anzuzeigen, anstatt diese zu interpretieren. Wie in Tabelle 10 erwähnt, zeichnet die Option `all` alle Pakete auf, die an oder von beliebigen IP-Adressen im Subnetz von Sniffit gesendet werden.

-L ermöglicht die Protokollierung mit einer durch *Protokollparam* angegebenen Protokollierungsebene. Dabei handelt es sich um eine Zusammensetzung eines oder mehrerer der folgenden Begriffe.

- raw – Rawebene
- norm – Normale Ebene
- telnet – Kennwörter am Telnetport (23) protokollieren
- ftp – Kennwörter am Ftp-Port (21) protokollieren
- mail – Mailinfo auf dem SMTP-Port (25) protokollieren

Bei der Protokollierung muss die Option -c verwendet werden. Die Standardprotokolldatei heißt sniffit.log. Es kann in der Konfigurationsdatei auch eine andere Protokolldatei angegeben werden. Mit der nachfolgenden Befehlszeile wird die normale Protokollierung auf dem SMTP-Port aktiviert. Die Konfigurationsinformationen werden aus der Datei sniffit.conf im aktuellen Arbeitsverzeichnis gelesen.

```
# sniffit -L mailnorm -c ./sniffit.conf
```

Die Konfigurationsdatei besteht aus einer Reihe von Zeilen im folgenden Format:

```
{Feld1} {Feld2} {Feld3} {Feld4} [Feld5]
```

Feld1 kann einen der folgenden Einträge enthalten:

- select – Pakete an/von Host in *Feld3* und *Feld4* aufzeichnen
- deselect – Pakete an/von Host in *Feld3* und *Feld4* ignorieren.
- logfile – Name der Protokolldatei in den Wert im *Feld2* umändern

Feld2 kann einen der folgenden Einträge enthalten:

- from – Von Host in *Feld3* und *Feld4* gesendete Pakete berücksichtigen
- to – An Host in *Feld3* und *Feld4* gesendete Pakete berücksichtigen
- both – Kombiniert from- und to-Operationen
- *Dateiname* – Falls logfile in *Feld1* angegeben ist

Feld3 kann einen der folgenden Einträge enthalten:

- host – Ein Rechnername
- port – Eine Portnummer
- mhosts – Mehrere Hosts, die mit einer partiellen IP-Adressennotation beschrieben werden

Je nach Wert von *Feld3* ist *Feld4* ein Rechnername, eine Portnummer oder ein Dienstname (wie z.B. `ftp` oder `telnet`), oder eine Reihe mehrerer IP-Adressen, die partielle IP-Adressennotation verwenden. *Feld5* ist optional, kann aber eine Portnummer sein, falls *Feld3* entweder `host` oder `mhosts` ist. Das folgende Beispiel soll das Dateiformat verdeutlichen. Nehmen wir folgende Konfigurationsdatei:

```
select from host 198.62.73.4
select to host www.forbidden.com
select both mhosts 198.62.73.
deselect both port 80
```

Diese Funktion führt folgende Aktionen aus:

1. Alle von der IP-Adresse 198.62.73.4. gesendeten Pakete aufzeichnen.
2. Alle an den Rechnernamen www.forbidden.com gesendeten Pakete aufzeichnen
3. Alle Pakete, die an oder von allen Hosts im IP-Adressenbereich 198.62.73.0 bis 198.62.73.255 gesendet wurden, aufzeichnen.
4. Pakete an oder von einem Webserver ignorieren (Port 80 ist der Standardport für das HTTP-Protokoll).
5. Alle Daten werden in die Datei `sniffit.log` protokolliert.

Verwenden von Netwatch

Netwatch ist ein Überwachungsprogramm für das IP-Protokoll. Es überwacht und untersucht den Paketdatenverkehr in einem Ethernet und zeigt die Datenverkehrstatistik in einer auf ncurses basierenden grafischen Benutzeroberfläche im Zeichenmodus an. Das Programm kann nur von einem Benutzer mit Rootberechtigung ausgeführt werden. Geben Sie zum Starten von Netwatch folgenden Befehl ein:

```
# netwatch
```

Eine Beispielanzeige sehen Sie in Abbildung 62.

ABBILDUNG 62. Die grafische Benutzeroberfläche von Netwatch

LINE	HOST	LOCAL NETWORK (PKTS)	K	B	HOST	REMOTE NETWORK (PKTS)	K	B
0	207 179.19.255	0	60		>ALL-ROUTERS HEAST NET	0	3	
1	lga.caldersystems.com	160	164		zeus.kernel.org	6894	4096	
2	dhcp244.caldersystems.com	16	16		calhcast.caldersystems.com	0	79	
3	dhcp242.caldersystems.com	12	22		pietra.caldersystems.com	31	0	
4	dhcp238.caldersystems.com	16	16		207 179.18.51	27	0	
5	dhcp233.caldersystems.com	12	22		alcagon.caldersystems.com	3	0	
6	dhcp232.caldersystems.com	16	16		warf.caldersystems.com	11	0	
7	dhcp227.caldersystems.com	12	22		phoenix.caldersystems.com	120	95	
8	dhcp226.caldersystems.com	16	16		calhcast.com	3	0	
9	dhcp225.caldersystems.com	16	16					
10	dhcp223.caldersystems.com	16	16					
11	dhcp222.caldersystems.com	16	16					
12	dhcp220.caldersystems.com	12	22					
13	dhcp214.caldersystems.com	16	16					
14	dhcp210.caldersystems.com	12	22					
15	dhcp207.caldersystems.com	16	16					
16	dhcp205.caldersystems.com	16	16					
17	dhcp204.caldersystems.com	16	16					
18	dhcp200.caldersystems.com	54	22					
ROUTER				0.106 Mbits/sec	Eth: 16102			

Wie Sie in Abbildung 62 sehen können, ist die Anzeige von Netwatch in zwei Bereiche unterteilt. Der linke Bereich zeigt den Datenverkehr im lokalen Netzwerk an und der rechte Bereich den Datenverkehr im Remote-Netzwerk. Jeder Eintrag wird farblich hervorgehoben (auf Terminals, die Farbe unterstützen), um die Aktivität im Netzwerk über einen bestimmten Zeitraum hinweg anzuzeigen. Es wird folgendes Farbschema verwendet:

- Rot: Statistikdaten, die weniger als eine Minute alt sind
- Gelb: Statistikdaten, die weniger als 5 Minuten alt sind
- Grün: Statistikdaten, die weniger als 30 Minuten alt sind
- Blau: Alle anderen Statistikdaten

Der Monitor enthält auch Statistiken mit folgenden Informationen:

- Die Anzahl der empfangenen und übertragenen Pakete
- Die Anzahl der empfangenen und übertragenen Byte
- IP-Adresse des letzten Kommunikationspartners
- Die Fähigkeit, alle Statistiken in eine Textdatei zu protokollieren

Der Bildschirm wird jede Sekunde aktualisiert. Der Rechnername oder die IP-Adresse wird in der ersten Spalte angezeigt und die Anzahl der übertragenen und empfangenen Pakete in der zweiten bzw. dritten Spalte. Abbildung 64 zeigt die Anzahl der Pakete an. Wenn Sie die übertragenen und empfangenen Byte aufzeich-

nen möchten, drücken Sie die linke Maustaste. Wenn Sie eine Protokolldatei erstellen möchten, geben Sie **L** ein.

Tabelle 13 enthält eine Liste der Tastatureingaben, die in Netwatch möglich sind.

TABELLE 13. Netwatch-Tastatureingaben

Tastatureingabe	Beschreibung
Tabulatortaste	Wechselt zwischen den lokalen und Remotebildschirmbereichen
Rechte Pfeiltaste	Zur nächsten Anzeigeoption gehen
Linke Pfeiltaste	Zurück zur vorherigen Anzeigeoption gehen
Pfeiltaste nach oben	Zurück zur vorherigen Seite im aktuellen Bildschirmbereich gehen
c	Alle Zähler auf null setzen
Pfeiltaste nach unten	Weiter zur nächsten Seite im aktuellen Bildschirmbereich gehen
n	Alle Hostlisten zurücksetzen
d	Aufzeichnen von Remote-Domainhosts aktivieren/deaktivieren
b	Anzeige "alter" Hosts (blau gekennzeichnet) aktivieren/deaktivieren

Netwatch unterstützt eine einfache Protokollierungsfunktion mit Hilfe des Befehls **l**. Statistiken werden in die Datei `/etc/netwatch.stats` protokolliert. Achten Sie jedoch auf Ihren Festplattenspeicher, da diese Datei sehr schnell an Größe zunehmen kann.

Verwenden von tcpdump

Bei `tcpdump` handelt es sich um ein weiteres Paketüberwachungsprogramm. Im Gegensatz zu `Sniffit` und `Netwatch` gibt es jedoch die Header von Paketen an einer Netzwerkschnittstelle in Echtzeit aus, anstatt Statistiken über einen bestimmten Zeitraum anzusammeln und Zusammenfassungsinformationen anzuzeigen. Darüber hinaus bietet `tcpdump` größere Kontrolle über die ausgewählten Pakete und die angezeigten Informationen als `Sniffit` oder `Netwatch`.

Geben Sie zur Verwendung von `tcpdump` folgenden Befehl ein:

```
# tcpdump [-i Schnittstelle] [Ausdruck]
```

Schnittstelle bezeichnet dabei eine beliebige aktive Ethernet-Netzwerkschnittstelle in Ihrem System. Wenn Sie keine Schnittstelle angeben, verwendet `tcpdump` die aktive Schnittstelle mit der niedrigsten Nummer. So wird z.B. `eth0` anstelle von `eth1` überwacht, wenn beide aktiv sind.

Ausdruck ist ein boolescher Filter, der den Host, den Typ, die Richtung und das Protokoll, die Sie überwachen möchten, angibt. Die Filtersprache von `tcpdump` ist sehr umfangreich, weshalb in diesem Handbuch nur die grundlegende Nutzung angesprochen wird. Eine Beschreibung der vollständigen Filtersyntax finden Sie auf der Manpage von `tcpdump`.

Um anzugeben, dass Sie nur den Datenverkehr auf einem bestimmten Host überwachen möchten, verwenden Sie das Schlüsselwort `host`, gefolgt vom Rechnernamen, wie im nachfolgenden Beispiel:

```
# tcpdump host queenbee
```

Diese Anweisung zeigt alle an und vom Host namens `queenbee` gesendeten Pakete an. Die nächste Anweisung beschränkt die Anzeige auf alle von `queenbee` gesendeten Pakete:

```
# tcpdump src host queenbee
```

Verwenden Sie analog dazu den Modifizierer `dst` (für *destination*, Ziel) anstelle von `src`, um nur die Pakete anzuzeigen, die an den angegebenen Host gesendet werden. Die nächste Anweisung zeigt den Datenverkehr zwischen den Hosts `queenbee` und `hive` an:

```
# tcpdump host queenbee and hive
```

Mit den Modifizierern `src` und `dst` können Sie weiterhin festlegen, welche Art von Datenverkehr angezeigt werden soll. Beachten Sie, dass dieser Filterausdruck `and` verwendet, um `tcpdump` anzuweisen, sowohl Pakete von `queenbee` als auch von `hive` anzuzeigen. Mit `or` und `not` sowie Klammern haben Sie weiterhin die Möglichkeit, komplexere Filterausdrücke zu erstellen.

Angenommen, Sie möchten den FTP-Datenverkehr überwachen, der über Ihr Internetgateway läuft. Verwenden Sie zunächst das Schlüsselwort `gateway` anstelle von `host`. Dies ist deshalb nötig, da die IP-Adresse des Quell- oder Zielhosts nicht identisch mit der Quell- oder Zieladresse des Ethernet ist. Um nur FTP-Pakete aufzuzeichnen, verwenden Sie das Schlüsselwort `port`, um die angezeigten Pakete auf diejenigen zu begrenzen, die als Ziel oder Ursprung einen FTP-Port haben. Angenommen, Ihr Gateway hat die Bezeichnung `netmonster`. Verwenden Sie die folgende Anweisung, um den FTP-Datenverkehr aufzuzeichnen.

```
# tcpdump 'gateway netmonster and (port ftp or ftp-data)'
```

Bei diesem Filter schützen die einzelnen Anführungszeichen den Ausdruck vor einer Fehlinterpretation durch die Shell.

Wie bereits erwähnt, bietet die Filtersyntax von `tcpdump` wesentlich mehr Optionen, als in diesem Handbuch behandelt werden. Allgemein lässt sich sagen, dass Sie spezifische Protokolle filtern können sowie spezifische Pakettypen, die von einem bestimmten Protokoll transportiert werden. Kurzum: `tcpdump` ist ein leistungsfähiges Tool, weshalb Ihnen dringend empfohlen wird, die Dokumentation zu lesen und zu experimentieren. Tabelle 14 enthält einige nützliche Befehlszeilenoptionen, die in `tcpdump` möglich sind.

TABELLE 14. Befehlszeilenoptionen von `tcpdump`

Option	Beschreibung
<code>-c Anzahl</code>	Nach Empfang von <i>Anzahl</i> von Paketen beenden
<code>-F Datei</code>	Filterausdruck aus <i>Datei</i> lesen
<code>-i Schnittstelle</code>	Pakete auf <i>Schnittstelle</i> ausgeben
<code>-n</code>	Adressen nicht in Namen konvertieren
<code>-t</code>	Keinen Zeitstempel für jede Ausgabezeile ausgeben
<code>-w Datei</code>	Rawpakete in <i>Datei</i> schreiben, anstatt diese anzuzeigen

Die Ausgabe von `tcpdump` ist je nach Protokoll unterschiedlich. Es folgt eine kurze Besprechung des Formats im Umgang mit TCP-Paketen. Hierbei seien Sie wiederum auf die Manpage verwiesen, die eine umfassende Erklärung des Ausgabeformats jedes Protokolls, komplett mit Beispielen, enthält.

Nehmen wir den folgenden `tcpdump`-Befehl:

```
# tcpdump -N -c 10 -n -t host dhcp236 and phoenix
```

Mit diesem Befehl wird die Anzeige der nächsten zehn Pakete (`-c 10`) angefordert, die zwischen den Hosts `dhcp236` und `phoenix` übertragen werden. Folgende Parameter machen die Ausgabe lesbarer: `-t` unterdrückt den Zeitstempel, und `-N` unterdrückt schließlich die Ausgabe vollständiger Domainnamen. Es werden nur Rechnernamen gedruckt. Die Ausgabe wird im folgenden Listing wiedergegeben:

```
dhcp236.bootpc > phoenix.bootps: xid:0xc1a5022d secs:5 C:dhcp236 [|bootp]
dhcp236.1527 > phoenix.pop3: S 1385763770:1385763770(0) win 16060 <mss
1460,sackOK,timestamp \ 1575411[|tcp]> (DF)
phoenix.pop3 > dhcp236.1527: S 2788306362:2788306362(0) ack 1385763771 win 16352 <mss 1460>
dhcp236.1527 > phoenix.pop3: . ack 1 win 16060 (DF)
```

```
phoenix.pop3 > dhcp236.1527: P 1:57(56) ack 1 win 16352 (DF)
dhcp236.1527 > phoenix.pop3: . ack 57 win 16060 (DF)
dhcp236.1527 > phoenix.pop3: P 1:13(12) ack 57 win 16060 (DF)
phoenix.pop3 > dhcp236.1527: P 57:98(41) ack 13 win 16352 (DF)
dhcp236.1527 > phoenix.pop3: P 13:27(14) ack 98 win 16060 (DF)
phoenix.pop3 > dhcp236.1527: . ack 27 win 16338 (DF)
```

Die Ausgabe, die über eine Zeile läuft, wird durch ein \ angezeigt. Das allgemeine Format einer TCP-Protokollzeile lautet:

```
src > dst: flags sequence-num ack window urgent options
```

`src` und `dst` sind die Quell- und Zielhosts. Wie aus dem Listing zu ersehen ist, wechselt sich die Ausgabe für den Quell- und Zielhost ab. Jeder Rechnername wird von einer Portnummer gefolgt, die dann bei Bekanntwerden in einen Dienstnamen konvertiert wird. Beispiel: `phoenix.pop3` würde als `phoenix.110` ausgegeben, falls im Beispiel der Parameter `-n` zur Unterdrückung der Konvertierung von Nummen in Namen verwendet werden würde.

Das `S` in der zweiten Zeile gibt an, dass die Flag `SYN` gesetzt wurde. Andere Flags sind `F` (`FIN`), `P` (`PUSH`), `R` (`RST`) oder `.`, was bedeutet, dass keine Flags gesetzt wurden. `sequence-num` ist die Sequenznummer dieses Pakets relativ zu anderen Paketen sowie die Anzahl der Datenbyte, die in diesem Paket enthalten sind. Die Notation lautet *erstes:letztes(Anzahl_Bytes)*, also bedeutet z.B. `1385763770:1385763770(0)`, dass diese Sequenz keine Datenbyte enthielt, und `1:57(56)` in der fünften Zeile, dass Byte 1-57 insgesamt 56 Datenbyte enthielten.

`Ack` gibt die nächste Sequenznummer an, die erwartet wird. In der sechsten Zeile gibt `ack 57` an, dass `dhcp236` als nächstes das Datenbyte erwartet. In der achten Zeile ist zu erkennen, dass `phoenix` seine Übertragung tatsächlich mit dem 57sten Byte beginnt. (`57:98(41)`). Der Wert nach `win` bezeichnet die Größe des Empfangspuffers am anderen Ende der Verbindung. Wie in Zeile 9 zu erkennen ist, bedeutet `win 16060`, dass `dhcp236` 16060 Bytes Empfangspufferplatz zugewiesen hat.

`urg` bezeichnet, dass das Paket dringende Daten enthält. Das letzte Feld enthält alle TCP-Optionen, die im Paket gesetzt wurden. Beispiel: Das dritte Paket (dritte Zeile) forderte eine maximale Segmentgröße von 1024 Byte an.

Wenn Sie jetzt glauben, dass Sie einen Einblick in die Funktionsweise des TCP-Protokolls benötigen, um die Ausgabe von `tcpdump` verstehen zu können, haben Sie Recht. Leider kann in diesem Handbuch nicht annähernd darauf eingegangen werden. Im Abschnitt "Zusätzliche Ressourcen" am Ende des Kapitels erhalten Sie eine Liste empfohlener Referenzquellen.

Verwenden von Cheops

Cheops ist ein grafisches Programm (basierend auf X Windows), das alle Computer im Netzwerk, einschließlich IP-Adresse, DNS-Name, installiertes Betriebssystem sowie andere relevante Informationen erkennt. Es überwacht auch einen spezifischen Computer auf der Basis der von Ihnen festgelegten Konfigurationen.

Cheops kann einen Portscan in einem beliebigen System des Netzwerks durchführen, und identifizieren, welche Ports geöffnet sind, welche Funktionsweise Ports haben (falls definiert) usw. *Portscans* decken auf, welche Dienste ausgeführt werden, ein grundlegendes Element für die Sicherheit Ihres Netzwerks. Die Ausführung eines Portscans in Systemen Ihres Netzwerks ist eventuell nicht sehr wichtig, wenn Sie allen Benutzern im Netzwerk vertrauen. Jedoch ist die Ausführung eines Portscans auf Ihrer Firewall von großer Bedeutung, damit Sie wissen, welche Dienste in das interne Netzwerk gelassen werden. Weitere Informationen zur Sicherheit und zu Portscans finden Sie in Kapitel 11, Sicherheit.

Mit Cheops haben Sie weiterhin die Möglichkeit, die Verfügbarkeit eines Servers und seiner Dienste zu überwachen. Dadurch können Sie benachrichtigt werden, wenn ein Server oder ein Dienst unerwartet ausfällt. Wenn Sie mehrere Domains verwalten, ist es möglich, mit Cheops alle zu überwachen. Cheops funktioniert auch innerhalb einfacher IP-Adressenbereiche.

Verwenden von Ntop

Ntop ist die Netzwerkversion des bewährten Utilitys `top`. Es liefert Informationen darüber, wie viele Daten im Netzwerk gesendet und empfangen werden und ob es sich um TCP oder UDP handelt. Tabelle 15 enthält die Befehlszeilenoptionen von `ntop`, und Tabelle 16 die Tastaturbefehle, die in `ntop` möglich sind. Bei Ausführung im interaktiven Modus

TABELLE 15. Befehlszeilenoptionen von `tcpdump`

Option	Argument	Beschreibung
-r	<Aktualisierungszeit>	Häufigkeit der Aktualisierung in Sekunden
-i	<Schnittstelle>	Zu überwachende Netzwerkschnittstelle (eg, eth0)
-f	<Datenverkehr-Ausgabedatei>	Dateiname der Ausgabedatei

TABELLE 15. Befehlszeilenoptionen von tcpdump

Option	Argument	Beschreibung
-n	<IP-Adressen>	Zu überwachende IP-Adressen (nur interaktiver Modus)
-p	<Protokolle >	Liste der zu überwachenden IP-Protokolle
-w	<Port>	Zu überwachende Portnummer
-e	<Max. Anzahl der Zeilen>	(nur in Verbindung mit -w zu verwenden)
-d	nicht verfügbar	Im Dämonmodus ausführen (nur in Verbindung mit -w zu verwenden)
-m	<lokale Adressen>	
-l	<Protokollierungs-zeitraum>	Der Zeitraum (in Sekunden), in dem Datenverkehrstatistiken protokolliert werden
-b	<Client:Port>	Der zu überwachende Internetclient und Port
<Filter-ausdruck>	nicht verfügbar	Siehe Manpage

TABELLE 16. Ntop-Tastaturbefehle

Taste	Aktion
q	ntop beenden
r	Statistiken zurücksetzen
n	Adressformat wechseln
p	Datenverkehrswerte wechseln
'l'	Hostanzeige wechseln
d	In Leerlauf wechseln
t	Sortierung wechseln
y	Spaltensortierung wechseln
h	Diese Hilfe anzeigen

Verwenden von Scotty

Bei Scotty handelt es sich um einen Tcl-Interpreter, der darauf ausgelegt ist, Status- und Konfigurationsinformationen über Ihr Netzwerk abzurufen. Es unterstützt die

folgenden Protokolle: SNMP, ICMP, DNS, HTTP, SUN RPC, NTP, & UDP. Das Tool ermöglicht die Überwachung und/oder Steuerung von Prozeduren, deren Ausführung für bestimmte Zeiten geplant ist, die Protokollierung über syslog sowie die Fähigkeit, auf die lokale Netzwerkdatenbank zuzugreifen. Am besten informieren Sie sich über Scotty, indem Sie seine spezifische Dokumentation lesen und sich seine Beispielskripts ansehen. Einige Beispielskripts sowie die Dokumentation für verschiedene Scotty-Erweiterungen finden Sie unter <http://www-home.cs.utwente.nl/~schoenw/scotty/>.

Zusätzliche Ressourcen

Webseiten

NIS

- <http://www.suse.de/~kukuk/nis-howto/index.html>
- <http://www.suse.de/~kukuk/nis/index.html>

Scotty

- <http://wwwhome.cs.utwente.nl/~schoenw/scotty/>

Ntop

- <http://www-serra.unipi.it/~ntop/>

Cheops

- <http://www.marko.net/cheops/>

Kernel-Dokumentation

Linux Documentation Project

- <http://www.linuxdoc.org/HOWTO/Ethernet-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/NIS-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/Networking-Overview-HOWTO.html>

Bücher

- *TCP/IP Network Administration*, 2nd Edition, Craig Hunt (O'Reilly and Associates, 1997)
- *Managing NFS and NIS*, Hal Stern (O'Reilly and Associates, 1991)
- *Essential System Administration*, 2nd Edition, Aileen Frisch (O'Reilly and Associates, 1995)

KAPITEL 7

Verwenden von KDE

Dieses Kapitel erklärt das Layout der Dateien, die KDE unterstützen und bietet eine kurze Einführung in die Grundfunktionen von KDE. Beachten Sie, dass die von OpenLinux eServer unterstützten Installationsoptionen KDE nicht installieren.

Speicherort von KDE-Dateien

Die meisten KDE-Dateien werden im Verzeichnis `/opt/kde` abgelegt. Die persönlichen Dateien von Benutzern, wie die Konfigurationsinformationen, werden in den Unterverzeichnissen `.kde` und `Desktop` ihres Home-Verzeichnisses abgelegt.

Die Tabelle 17 enthält wichtige Verzeichnisse und die darin gespeicherten Dateitypen.

TABELLE 17. KDE-Verzeichnisse

Verzeichnis	Funktion
<u>/opt/kde/bin</u>	KDE-Programmdateien für KDE-Anwendungen
<u>/opt/kde/cgi-bin/</u>	Enthält Skripts, die vom KDE-Hilfesystem verwendet werden.
<u>/opt/kde/lib</u>	Primärer Speicherort für KDE-relevante Bibliotheken
<u>/opt/kde/share/applnk</u>	Enthält Verknüpfungen mit KDE-Anwendungen auf dem KDE-Hauptmenü.
<u>/opt/kde/share/apps</u>	Enthält anwendungsspezifische Konfigurationsinformationen und temporären Speicherplatz.
<u>/opt/kde/share/mimelnk</u>	Der zentrale Speicherbereich für alle MIME-Typdefinitionen von KDE.
<u>share/config</u>	Enthält die primären Konfigurationsdateien für jede KDE-Anwendung. Die hier gespeicherten Informationen werden von benutzerspezifischen Informationen überschrieben.
<u>/opt/kde/share/icons</u>	Der Standardspeicherort von Symbolen für KDE-Anwendungen sowie Fensterdekorationen.
<u>\$HOME/Desktop</u>	Enthält KDE-Verknüpfungsdateien für alle Symbole auf dem Desktop eines Benutzers
<u>\$HOME/.kde</u>	Speichert benutzerspezifische Anpassungs- und Konfigurationsinformationen.

Die Informationen in `$HOME/.kde/share` spiegeln die Struktur und die Verwendung der Informationen in `/opt/kde/share` wieder, mit der Ausnahme, dass diese benutzerspezifisch sind. In der Datei `$HOME/.kderc`, die im Home-Verzeichnis jedes Benutzers vorhanden ist, werden Informationen über die bevorzugte Sprache des Benutzers, den Status von geöffneten Fenstern am Ende der letzten KDE-Sitzung sowie Tastatureinstellungen gespeichert.

KDE-Funktionen

Für KDE stehen eine enorme Vielfalt an Anwendungen, Applets und Dienstprogramme zur Verfügung, und jede Woche kommen neue hinzu. Es wäre daher

schwierig, alle davon zu besprechen. Stattdessen konzentriert sich dieser Abschnitt auf die geläufigsten und wichtigsten Anwendungen, die in Ihrem OpenLinux eServer-System installiert werden, welche Funktionen sie haben und wie sie gestartet und beendet werden.

Sie werden eventuell auch Tabelle 18 nützlich finden, in der die für KDE-Anwendungen geläufigen KDE-Tastenkombinationen aufgelistet werden. Beachten Sie, dass für alle Anwendungen die folgenden Tastenkombinationen gelten:

- ALT+<unterstrichener Buchstabe> eines Menübefehls öffnet das Menü.
- Mit den Pfeiltasten können Sie zwischen Menüs und Menübefehlen wechseln.
- TABULATOR-TASTE wechselt zum nächsten Element in einem Dialogfeld.
- UMSCHALT+TABULATOR-TASTE wechselt zum vorherigen Element in einem Dialogfeld.

TABELLE 18. Geläufige KDE-Tastatureingaben

Tastatureingabe	Beschreibung
<u>ALT+F1</u>	Öffnet das Hauptmenü
<u>ALT+ESC</u>	Blendet eine Liste geöffneter Fenster und Anwendungen ein.
<u>ALT+TAB</u>	Wechselt zum nächsten geöffneten Fenster
<u>ALT+UMSCHALT+TABULATOR-TASTE</u>	Wechselt zum vorherigen geöffneten Fenster
<u>STRG+TABULATOR-TASTE</u>	Wechselt zwischen KDE-Desktops.
<u>ALT+F2</u>	Blendet ein Fenster zur Ausführung einer einzelnen Befehlszeile ein.
<u>ALT+F3</u>	Öffnet das Systemmenü des aktuellen Fensters.
<u>ALT+F4</u>	Schließt das aktuelle Fenster.
<u>STRG+F[1-8]</u>	Wechselt zwischen den KDE-Desktops 1 bis 8.
<u>STRG+C</u>	Kopiert den aktuell markierten Text in die Zwischenablage.
STRG+V	Fügt den Text aus der Zwischenablage an der Cursorposition ein.
<u>STRG+X</u>	Löscht den aktuell markierten Text.
<u>STRG+A</u>	Markiert den gesamten Text.

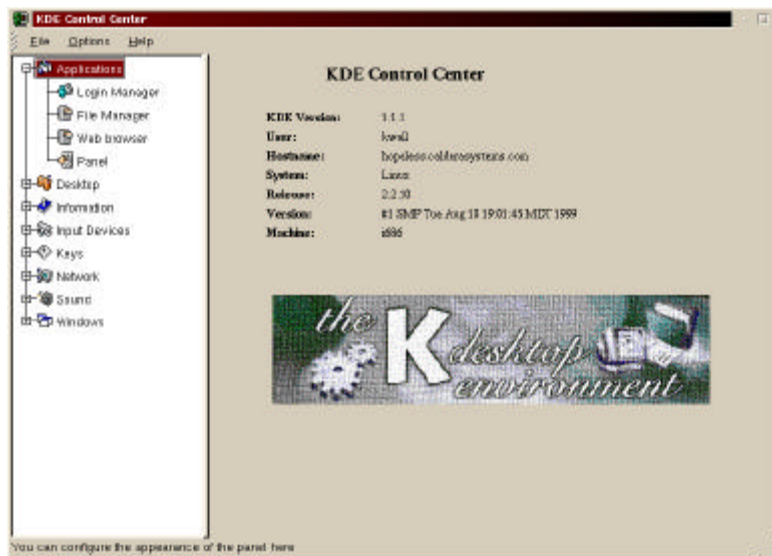
Anpassen des KDE-Desktops

Der KDE-Desktop wird hauptsächlich über das KDE-Steuerzentrum angepasst. Sie können entweder das Symbol KDE-Steuerzentrum im KPanel verwenden (siehe Abbildung 63, oder indem Sie im Kmenu den Befehl KDE-Steuerzentrum auswählen. Abbildung 64 zeigt den Hauptbildschirm des KDE-Steuerzentrums.

ABBILDUNG 63. Das Symbol KDE-Steuerzentrum



ABBILDUNG 64. Der Hauptbildschirm des KDE-Steuerzentrums



Jeder Untereintrag in Abbildung 66 entspricht einer Gruppe von KDE-Konfigurationsoptionen. Mit der Option Application können Sie z.B. den Login Manager (KDM), den File Manager (KFM), den Webbrowser und das Kpanel konfigurieren. Eine ausführliche Beschreibung von KDE sprengt den Rahmen dieses Handbuchs. Der Abschnitt Zusätzliche Ressourcen am Ende dieses Kapitels enthält eine Liste hervorragender Referenzquellen.

Zusätzliche Ressourcen

KDE-Homepage

- <http://www.kde.org/>

Koffice-Homepage

- <http://koffice.kde.org/>

Bücher

- *Teach Yourself KDE 1.1 in 24 Hours*, Nicholas D. Wells (Sams Publishing, 1999)

KAPITEL 8

Konfigurieren von Internet- und Intranetdiensten

Dieses Kapitel beschreibt die Einrichtung einer Reihe von Internetdiensten in Ihrem OpenLinux eServer-System. Die Installation liefert eine Standardkonfiguration für die meisten dieser Dienste. Dieses Kapitel konzentriert sich auf die Anpassung der Konfiguration auf Ihre speziellen Bedürfnisse. Sie werden folgende Dienste konfigurieren:

- Den Sendmail-Mailserver
- Den Apache-Webserver
- Den WUFTP-Dämon
- Den Domain Name Service
- Einwahl-Unterstützung
- BOOTP und DHCP

Konfigurieren eines Mailservers

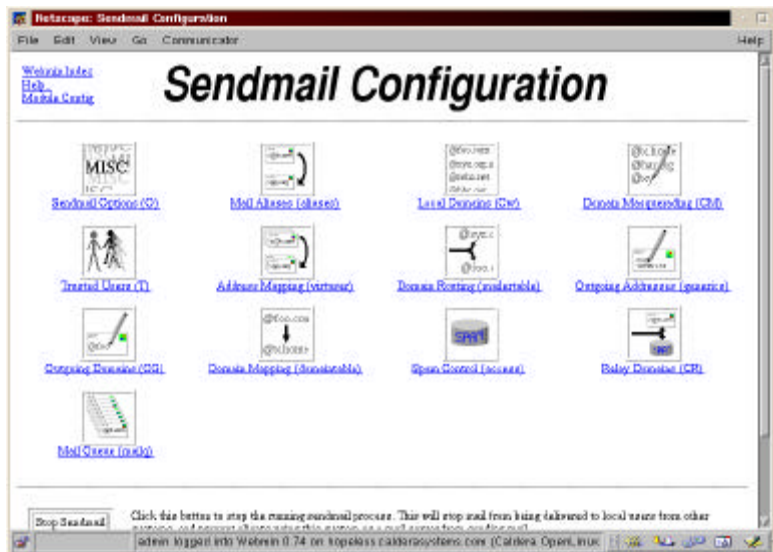
Wie bei den anderen, in Open Linux eServer enthaltenen Internetdiensten, wird auch ein Standard-Mailserver, der Sendmail Mail Transfer Agent, oder *MTA*, installiert und vorkonfiguriert. Die Konfigurationssyntax von Sendmail ist äußerst kompliziert, jedoch wird durch die Webmin-Oberfläche zur Konfiguration von Sendmail der Großteil dieser Komplexität verborgen. Dieser Abschnitt beschreibt die Konfiguration von `sendmail` für eine häufig auftretende Situation: Ein einzelnes System verarbeitet die gesamte ein- und ausgehende E-Mail für ein gesamtes Netzwerk.

Klicken Sie zunächst auf das Symbol Sendmail Configuration (siehe Abbildung 65), wodurch der Hauptbildschirm von Sendmail Configuration angezeigt wird (siehe Abbildung 66).

ABBILDUNG 65. Das Symbol Sendmail Configuration



ABBILDUNG 66. Der Hauptbildschirm Sendmail Configuration



Die Hauptseite zeigt eine Anzahl von Symbolen, mit denen sich unterschiedliche Funktionen von Sendmail konfigurieren lassen. Wenn auch eine ausführliche Beschreibung aller Optionen über den Rahmen dieses Handbuchs hinausgeht, werden dennoch die wichtigsten Funktionen erläutert. Zusätzliche Informationen und Referenzquellen erhalten Sie im Abschnitt "Zusätzliche Ressourcen" am Ende dieses Kapitels.

HINWEIS: Die Standard-Sendmail-Konfiguration von OpenLinux eServer unterstützt nicht Address Mapping, Outgoing Addresses, Domain Mapping, Outgoing Domains oder Spam Control. Wenn Sie versuchen, diese Webmin-Bildschirme zu verwenden, erhalten Sie eine Meldung, dass die Sendmail-Konfigurationsdatei (`/etc/sendmail.cf`) nicht die erforderlichen Direktiven enthält.

Mail Aliases

Der Bildschirm Mail Aliases ermöglicht die Umleitung von E-Mail an eine andere Adresse. Die Zieladresse kann einen anderer Benutzer, eine Adresse in einem anderen System, eine Datei oder sogar ein Programm sein. Beachten Sie jedoch, dass Aliase für *alle* Domänen gelten, für die Ihr System Mail empfängt. Angenommen, Sie nehmen E-Mail für die Domänen `bugcorp.com` und `bigbiz.com` entgegen. Ein Alias für die Adresse `hostmeister` würde folglich an die Adressen `hostmeister@bugcorp.com` und `hostmeister@bigbiz.com` umgeleitet werden.

ABBILDUNG 67. Der Bildschirm Mail Aliases

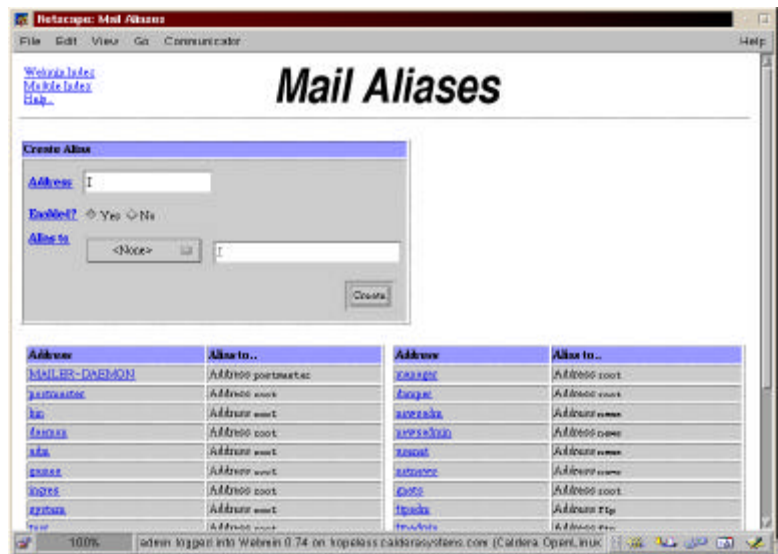


Abbildung 67 zeigt den Konfigurationsbildschirm Mail Aliases. Wenn Sie einen vorhandenen Alias ändern oder löschen möchten, klicken Sie auf seine entsprechende Adresse. Um einen neuen Alias zu erstellen, füllen Sie das Formular am oberen Bildschirmrand aus, wählen Sie in der Dropdown-Liste den Aliastyp aus (in der Regel eine E-Mail-Adresse), und klicken Sie auf die Schaltfläche Create.

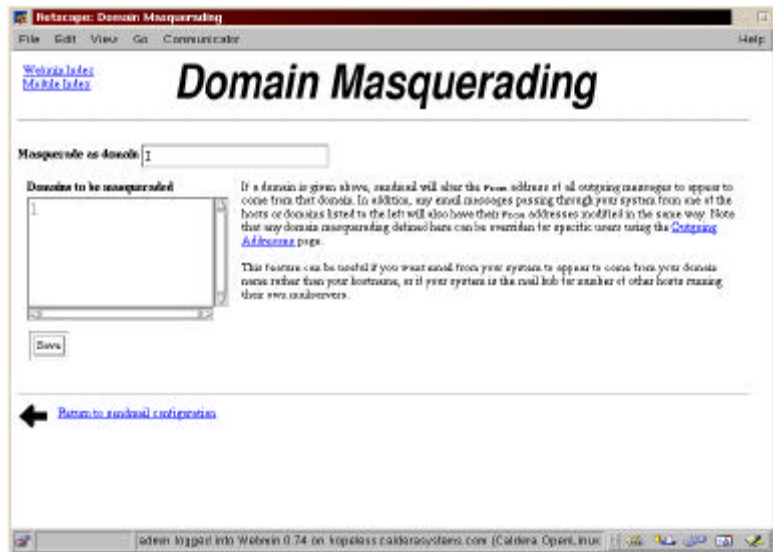
Local Domains

Der Bildschirm Local Domains ermöglicht das Hinzufügen der Namen aller Hosts, für die Sie E-Mail entgegennehmen. Die Liste der Hosts wird in der Datei `/etc/sendmail.cw` gespeichert. Fügen Sie einfach die Domäne zur Liste hinzu, und klicken Sie auf die Schaltfläche Save. Voraussetzung dafür ist, dass ein DNS-Eintrag für die Domäne existiert, und Ihr OpenLinux eServer-System als Mailexchanger für die angegebene Domäne aufgelistet ist.

Domain Masquerading

Abbildung 68 zeigt den Bildschirm Domain Masquerading.

ABBILDUNG 68. Der Bildschirm Domain Masquerading



Mit Hilfe von Domain-Masquerading können Sie die Absenderadresse (From:) von E-Mail, die aus Ihrem System stammt oder dieses durchläuft, dahingehend

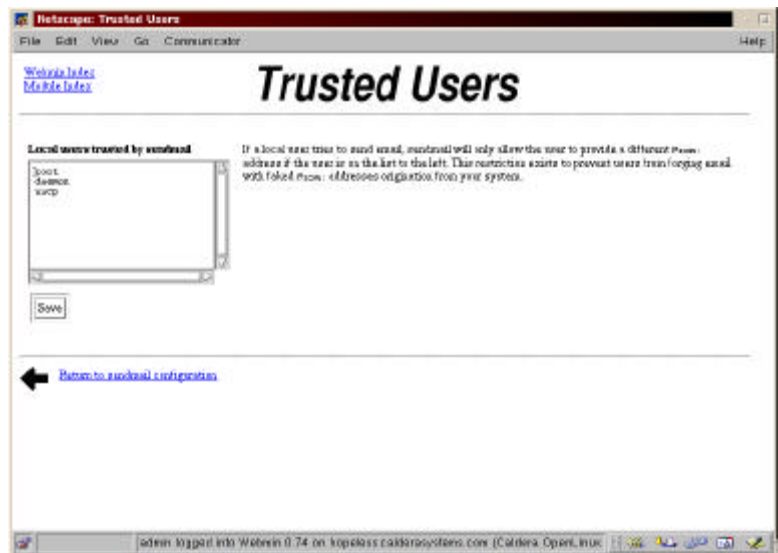
ändern, dass diese scheinbar von der angegebenen Domäne stammt. Die Verwendung dieser Funktion ist auch denkbar, wenn E-Mail von Ihrem Domänennamen anstelle von Ihrem System-Rechnernamen stammen soll. Beispiel: Falls Ihr Mailserver `mailbeast.bigisp.com` heisst, hat die gesamte E-Mail die Absenderadresse `benutzer@mailbeast.bigisp.com`. Damit als Absenderadresse nur `bigisp.com` erscheint, geben Sie `bigisp.com` in das Eingabefeld "Masquerade as domain" ein, und klicken Sie auf die Schaltfläche `Save`.

Falls Ihr System als Host für mehrere Domänen dient, die maskiert werden müssen, geben Sie ihre Namen (eine pro Zeile) in das Listenfeld "Domains to be masqueraded" ein, und klicken Sie auf die Schaltfläche `Save`.

Trusted Users

Bei *vertrauenswürdigen Benutzern* handelt es sich um lokale Benutzer, für die Sendmail die Verwendung einer anderen Absenderadresse (From:) als der regulären zulässt (siehe Abbildung 69). *Gehen Sie extrem vorsichtig mit dieser Option um, da diese E-Mail-Benutzern die Fälschung ihrer E-Mail-Adressen ermöglicht!* Vertrauenswürdige Benutzer werden jeweils auf einer eigenen Zeile aufgelistet. Wenn Sie Änderungen, neue Einträge oder Löschungen speichern möchten, klicken Sie auf `Save`.

ABBILDUNG 69. Der Konfigurationsbildschirm Trusted Users

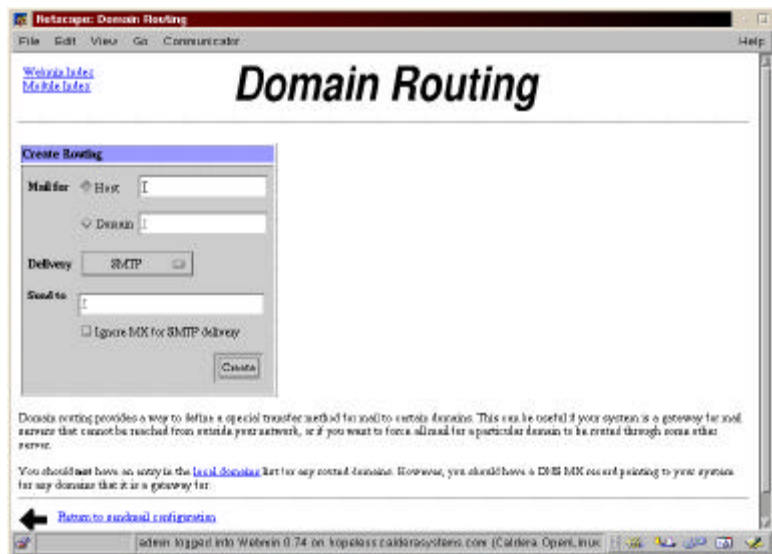


Domain Routing

Das Domänenrouting ermöglicht die Angabe einer speziellen Weiterleitungsmethode für E-Mail, die an bestimmte Domains oder Hosts gerichtet ist. Eine korrekte Funktionsweise setzt voraus, dass Ihr System der Mailexchanger für diese Systeme ist. Um diese Funktion einzurichten, geben Sie den Host- oder Domänennamen für den weitergeleiteten Host oder die Domäne ein, wählen Sie die korrekte Übermittlungsmethode im Dropdown-Listenfeld Delivery aus, und fügen Sie den Namen des Zielsystems ein, an das die E-Mail gesendet werden soll.

In Abbildung 70, wird an `bugcorp.com` gerichtete E-Mail, unter Verwendung des Standard-SMTP-Protokolls, an `mailbeast.bigisp.com` weitergeleitet.

ABBILDUNG 70. Beispiel-Domänenrouting für bugcorp.com

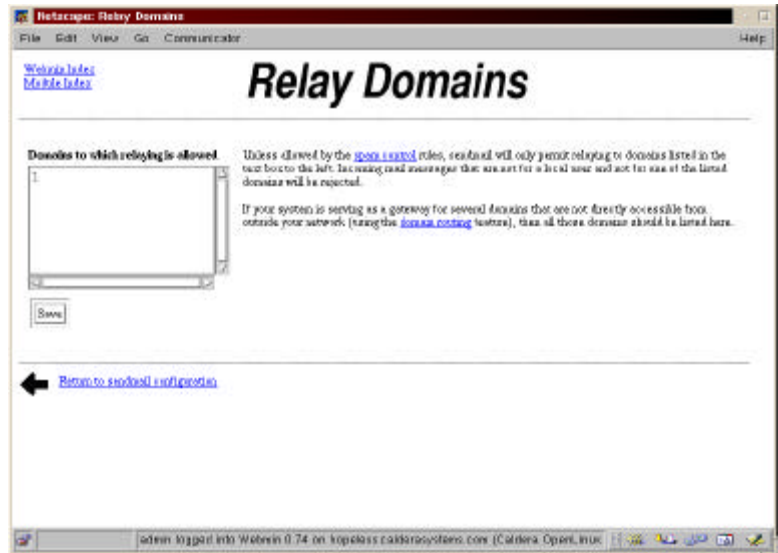


Relay Domains

Falls Sie das Domänenrouting konfiguriert haben, müssen Sie für diese Domänen auch die Weitervermittlung freigeben. Hierbei handelt es sich um eine Kontrollmaßnahme, die Versender von unaufgeforderten Werbemails davon abhält, Ihr System als offene E-Mail-Vermittlungsstelle zu verwenden. Darüber hinaus weist sendmail alle eingehenden Mailnachrichten ab, die nicht für lokale Benutzer und nicht für eine aufgelistete Domäne bestimmt sind, wodurch Ihr System weiter gegen Versender von unaufgeforderter Werbemails geschützt ist.

Um die Weitervermittlung z.B. an eine Domäne mit der Bezeichnung bugcorp.com zuzulassen, geben Sie ihren Namen das Listenfeld ein, und klicken Sie auf die Schaltfläche Save (siehe Abbildung 71).

ABBILDUNG 71. Der Konfigurationsbildschirm Relay Domain



Mail Queue

Der Bildschirm Mail Queue zeigt sowohl eingehende als auch ausgehende E-Mail, die Sendmail in die Warteschlange eingereiht hat. Über diesen Bildschirm können Sie die E-Mail-Warteschlange bearbeiten, unzustellbare Nachrichten löschen und andere Sendestatusinformationen abfragen. Es dient als exzellentes Tool, wenn Sie versuchen, eine fehlerhafte Sendmail-Konfiguration zu debuggen.

Einrichten eines Webservers

Bei der Installation von OpenLinux eServer wurde der Apache Webserver automatisch eingerichtet und installiert. Verwenden Sie den folgenden Befehl, um seine Installation zu überprüfen.

```
$ rpm -q apache
```

Apache ist installiert, wenn in etwa folgende Ausgabe angezeigt wird.

```
apache-1.3.4-4
```

Wenn Sie überprüfen möchten, dass der Server aktiv ist, führen Sie den folgenden Befehl aus:

```
$ ps aux | grep httpd
```

Falls der Server aktiv ist, werden mehrere Zeilen Ausgabe angezeigt, die in etwa der folgenden entsprechen:

```
root 648 0.0 0.1 2284 236 ? S Oct12 0:00 httpd -f /etc/httpd
nobody 652 0.0 0.1 2320 236 ? S Oct12 0:00 httpd -f /etc/httpd
nobody 653 0.0 0.1 2324 232 ? S Oct12 0:00 httpd -f /etc/httpd
nobody 654 0.0 0.1 2324 232 ? S Oct12 0:00 httpd -f /etc/httpd
nobody 655 0.0 0.1 2324 232 ? S Oct12 0:00 httpd -f /etc/httpd
```

Bei dem `httpd`-Programm handelt es sich um den Webserver-Dämon. Falls der Server nicht aktiv ist, melden Sie sich als Rootbenutzer an, und verwenden Sie den folgenden Befehl, um ihn zu starten. Laden Sie anschließend den vorgehenden `ps`-Befehl, um zu überprüfen, ob dieser gestartet wurde.

```
# /etc/rc.d/init.d/httpd start
```

Apache-Konfiguration unter Verwendung von Webmin

Sie starten das Apache-Konfigurationsmodell von Webmin, indem Sie auf das Symbol Apache Webserver klicken (siehe Abbildung 72). Abbildung 73 zeigt den Hauptbildschirm für die Apache Konfiguration

ABBILDUNG 72. Das Symbol Apache Webserver

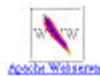
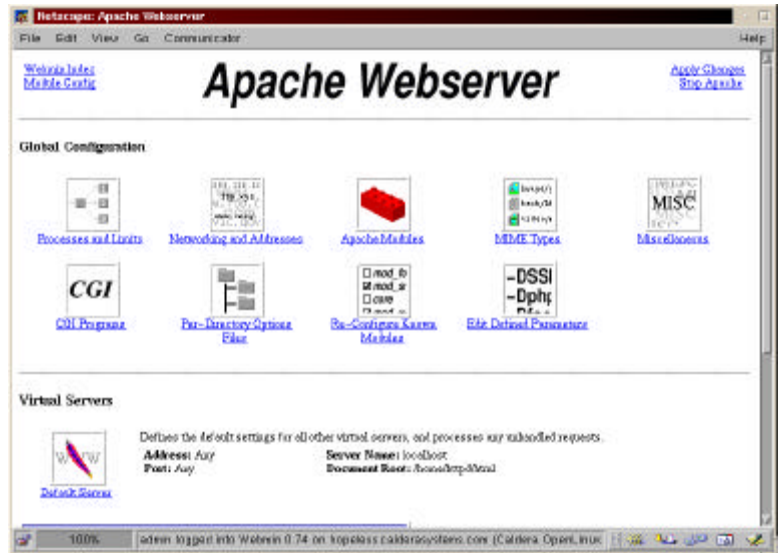


ABBILDUNG 73. Der Konfigurationsbildschirm Apache Webserver



Der obere Teil des Bildschirms ermöglicht Ihnen die Steuerung vieler Konfigurationsaspekte von Apache. Der untere Teil des Bildschirms betrifft die Konfiguration virtueller Server, ein Thema, das nicht im Rahmen dieses Handbuches behandelt werden kann.

Das Symbol Process and Limits ermöglicht die Steuerung der Systemressourcen, die Apache in Anspruch nimmt. Für die meisten Fälle sollte die Standardeinstellung ausreichend sein.

Einrichten eines FTP-Servers

Die Standardkonfiguration des FTP-Servers bietet ein vernünftiges Maß an Sicherheit. Wir empfehlen Ihnen deshalb dringend, die in diesem Abschnitt besprochenen Konfigurationsdateien zu untersuchen, und an Ihre Situation anzupassen. So entscheiden Sie sich z.B. dafür, keinen FTP-Zugriff von außerhalb Ihres Netzwerks, oder nur den Zugriff von bestimmten Domänen aus zuzulassen. Folgende Konfigurationsdateien sind für den FTP-Server relevant:

- `/etc/inetd.conf`: Definiert die Art und Weise, wie das Paket TCP Wrapper FTP-Verbindungsanforderungen verarbeitet.
- `/etc/hosts.allow` und `/etc/hosts.deny`: Legt fest, wer Zugriff auf den FTP-Server erhält.
- `/etc/ftpusers`: Legt fest, welche regulären Benutzer Ihres OpenLinux eServer-System *nicht* zur Verwendung von FTP berechtigt sind.
- `/etc/ftpaccess`: Legt die Zugriffsregeln für alle Konten fest, einschließlich den anonymous Benutzer.
- `/var/log/xferlog`: Protokolliert alle Dateiübertragungen.

Das Paket TCP Wrapper wird ausführlicher in Kapitel 11 besprochen, weshalb hier nicht darauf eingegangen wird. Der Zugriff auf den FTP-Server in Ihren Systemen wird mit einer der folgenden Methoden kontrolliert:

- Ist ein Benutzer-Account unter `/etc/ftpusers` aufgeführt, wird diesem Account die Zugriffsberechtigung auf den FTP-Server verweigert.
- Wird ein Benutzer-Account aus `/etc/passwd` entfernt oder darin herauskommentiert, wird diesem Account die Zugriffsberechtigung auf den FTP-Server verweigert.
- Ist ein Benutzer nicht in `/etc/hosts.allow`, jedoch in `/etc/hosts.deny` aufgeführt, wird diesem Account die Zugriffsberechtigung auf den FTP-Server verweigert.
- Falls ein Eintrag in der Datei `/etc/ftpaccess`, die den Betrieb des FTP-Servers konfiguriert (`ftpd`), diese Klasse von Benutzer entfernt, wird der Zugriff auf den FTP-Server verweigert.

Zur Aktivierung von anonymous FTP, muss der FTP-Benutzer-Account in der Datei `/etc/passwd` und *nicht* in der Datei `/etc/ftpusers` vorhanden sein. Darüber hinaus muss der `in.ftpd`-Dienst in `/etc/inetd.conf` aktiviert sein. In der Standardinstallation von OpenLinux eServer ist anonymous FTP aktiviert. Der Eintrag sieht wie folgt aus:

```
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
```

Die Option `-l` bewirkt eine Protokollierung von FTP-Sitzungen mit Hilfe der Systemprotokollierungsfunktion; `-a` ermöglicht die Verwendung der Datei `/etc/ftpaccess`, um die Funktionsweise von `ftpd` zu steuern.

Jeder der Einträge in `/etc/ftpaccess` steuert, welche Benutzer Zugriff auf den FTP-Server haben und zu was diese nach einer Verbindung berechtigt sind. Wenn Sie den Verdacht haben, dass Angriffe auf Ihr System über FTP erfolgen, können Sie eine oder beide der folgenden Zeilen zur Datei `/etc/ftpaccess` hinzufügen, um weitere Informationen zu erhalten.

```
log commands real,anonymous inbound,outbound
```

```
log security real,anonymous
```

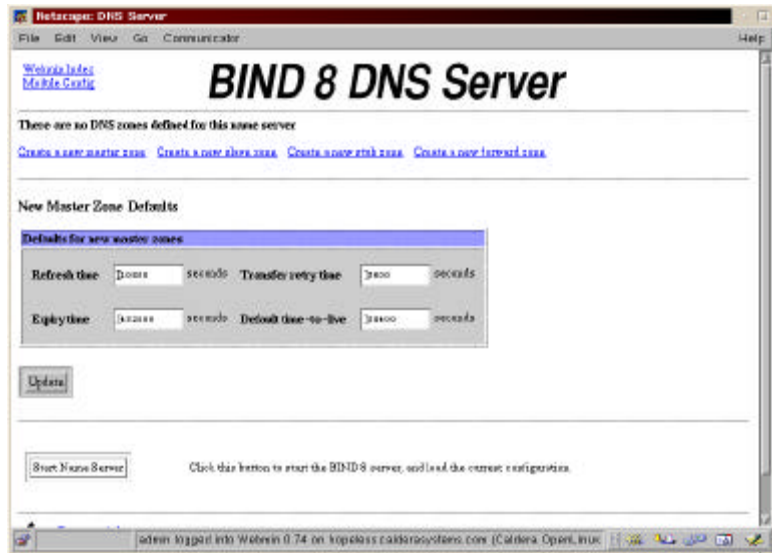
Die erste Zeile zeichnet alle Befehle im Systemprotokoll auf, die während einer FTP-Sitzung von anonymous oder tatsächlichen Benutzern ausgeführt wurden. Die zweite protokolliert Sicherheitsverletzungen durch diese Benutzer. Alternativ dazu könnten Sie einfach FTP deaktivieren, indem Sie den entsprechenden Eintrag in der Datei `/etc/inetd.conf` herauskommentieren, und den `inetd`-Dämon neu starten.

Einrichten eines Domain Name Servers

Die Einrichtung eines Domain Name Servers, auch als DNS bekannt, wird hinsichtlich Komplexität und frustrationsbedingtem Haarausfall nur noch von Sendmail übertroffen. Aufgrund seiner Komplexität wird DNS in diesem Abschnitt nicht ausführlich beschrieben. Stattdessen wird gezeigt, wie Sie zwei geläufige DNS-Schemas konfigurieren, wobei die erforderlichen Begriffe und Konzepte bei Bedarf erklärt werden.

Klicken Sie auf das Symbol BIND 8 DNS Server, um mit der Konfiguration des Namenservers zu beginnen. Da der Namenserver noch nicht konfiguriert wurde, wird zunächst der Bildschirm in Abbildung 74 angezeigt. An dieser Stelle müssen Sie entscheiden, welche Art von Namenserver Sie konfigurieren möchten.

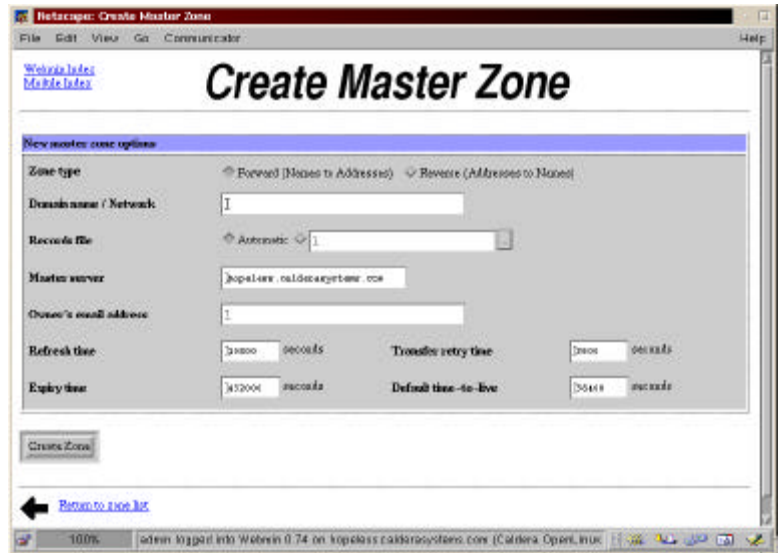
ABBILDUNG 74. Anfangsbildschirm für die DNS-Konfiguration



Falls Ihr Server nicht mit dem Internet verbunden wird, wählen Sie die erste Optionsschaltfläche aus, "Setup nameserver for internal non-internet use only." Die zweiten und dritten Optionen, die für einen Namenserver gelten, der *tatsächlich* mit dem Internet verbunden wird, sind im wesentlichen identisch, mit der Ausnahme, dass die zweite nur funktioniert, wenn bereits eine Internetverbindung besteht. Wählen Sie die entsprechende Option aus, und klicken Sie auf die Schaltfläche am unteren Bildschirmrand, um eine Basiskonfigurationsdatei zu erstellen. Starten Sie anschließend den Namenserver.

Der nächste Schritt besteht in der Erstellung einer Masterzonendatei für Forward- und Reverse-DNS-Lookups. Diese Datei konfiguriert den Namenserver entsprechend, um DNS-Lookups bezüglich Ihrer Domäne beantworten zu können. *Forward Lookups* vergleichen Namen mit IP-Adressen, während *Reverse Lookups* umgekehrt IP-Adressen mit Namen vergleichen. Beide werden für die korrekte Konfiguration des Namensservers vorausgesetzt. Klicken Sie auf die Verknüpfung "Create a new master zone", um zu beginnen. Abbildung 75 zeigt den anschließend angezeigten Bildschirm.

ABBILDUNG 75. Erstellen einer neuen Masterzonendatei



Geben Sie im Feld Domain name/Network den Namen Ihrer Domäne ein. Das Feld "Records file" ermöglicht die Angabe der Datei, die eine Beschreibung Ihrer Domäne enthält. Verwenden Sie den Standarddateinamen, indem Sie die Optionsschaltfläche "Automatic" auswählen. Im Feld "Master Server" geben Sie den Namen oder die IP-Adresse des Systems an, auf dem der Namensserver ausgeführt wird. Webmin geht standardmäßig davon aus, dass es sich hierbei um den lokalen Computer handelt.

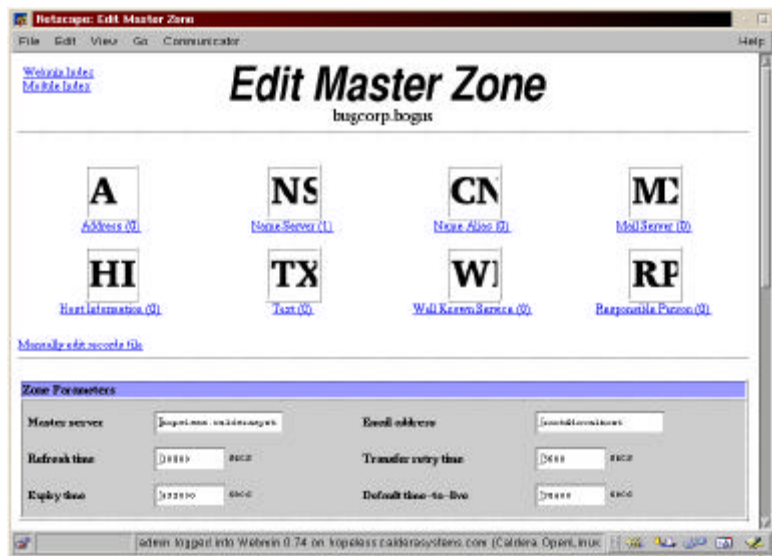
Geben Sie im Feld "Owner's email address" die E-mail-Adresse der Person ein, die E-Mail bezüglich dieses Namensservers erhalten soll. Wenn Sie keinen Grund zum Ändern der anderen Werte haben, klicken Sie auf die Schaltfläche "Create Zone". Sie werden bemerken, dass Webmin ein Symbol für die neue Zone hinzugefügt hat. Klicken Sie zur Aktivierung der neuen Zone auf die Schaltfläche "Apply Changes", und starten Sie den Namensserver erneut.

Beachten Sie, dass Sie sowohl Forward- als auch Reverse-Lookups konfiguriert haben müssen. Erstellen Sie also eine weitere Masterzonendatei, aber wählen Sie dieses Mal die Optionsschaltfläche "Reverse (Addresses to Names)" aus. Verwenden Sie dieselben Werte für die anderen Felder, wie bei der Erstellung der Forward-Zone, klicken Sie auf die Schaltfläche "Create", und anschließend auf die Schaltfläche "Apply Changes". *Voila!* Sie verfügen jetzt über einen einfachen funktionierenden DNS-Server!

Nach der Konfiguration des Basisservers, können Sie nach Bedarf noch die Feinabstimmung vornehmen. So müssen Sie z.B. für jeden Host im Netzwerk, dem eine IP-Adresse zugeordnet ist, einen Adressdatensatz anlegen. Darüber hinaus ist es erforderlich, einen Namenserverdatensatz für den Backupnamenserver (falls vorhanden, empfohlen) zu erstellen sowie einen Mailserverdatensatz, damit die an Ihre Domäne gesendete Mail tatsächlich ankommt.

Die Erstellung dieser Datensätze ist sehr einfach. Klicken Sie dazu auf das Symbol der soeben erstellten Master-Forward-Zonendatei. Der anschließend angezeigte Bildschirm sollte in etwa Abbildung 76 entsprechen. Der Bildschirm enthält Symbole für die unterschiedlichen Arten von Ressourcendatensätzen, die DNS unterstützt. Das folgende Beispiel zeigt, wie Sie einen Adressdatensatz hinzufügen. Der Vorgang ist für alle Typen im wesentlichen gleich.

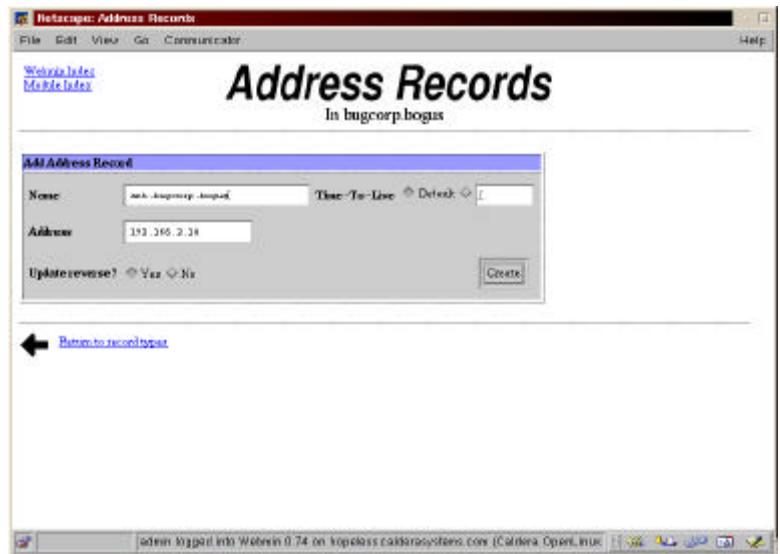
ABBILDUNG 76. Eine Beispiel-Masterzonendatei.



Wenn Sie einen Adressdatensatz hinzufügen möchten, der einen Rechnernamen mit einer IP-Adresse verknüpft, klicken Sie auf das Symbol "Address", und füllen Sie das nachfolgende Formular aus. Das Feld "Name" enthält den vollständigen Domännennamen des hinzuzufügenden Hosts, z.B. ant.bugcorp.com, und "Address" enthält die IP-Adresse, die Sie diesem Host zuordnen, z.B. 192.168.1.13. Die Felder "Time-To-Live" und "Update reverse?" sollten nicht verändert werden. Die Aktualisierung der Reverse-Zonendatei ist besonders wichtig, damit die neue IP-Adresse korrekt in einen vordefinierten Rechnernamen aufgelöst werden kann.

Klicken Sie nach Durchführung der Änderungen auf die Schaltfläche Create, und der neue Datensatz wird unter dem Dateneingabeformular angezeigt. Wenn Sie mit dem Hinzufügen von Datensätzen fertig sind, klicken Sie auf die Verknüpfung "Return to record types" und anschließend auf die Schaltfläche "Save". Um die Datensätze zu aktivieren, klicken Sie abschließend auf die Schaltfläche "Apply Changes". Ein Beispiel eines neuen Adressendatsatzes finden Sie in Abbildung 77.

ABBILDUNG 77. Beispiel-Adressdatensatz



Konfigurieren eines PPP-Einwahlservers

Stellen Sie zunächst sicher, dass Sie das Paket `mgetty` installiert haben.

```
# rpm -q mgetty
```

Falls die Ausgabe `package mgetty is not installed` lautet, müssen Sie es installieren, bevor Sie fortfahren. Bearbeiten Sie nach der Installation des Pakets die Datei `/etc/mgetty+sendfax/mgetty.config`. Sie müssen einen Abschnitt für den Port hinzufügen (oder einen vorhandenen bearbeiten), den Sie für Einwahlzwecke verwenden. Der Abschnitt ist in etwa dem folgenden Listing ähnlich:

```
port ttyS1
init-chat "" AT&F&C1&D2
speed 115200
```

Dieser Abschnitt weist `mgetty` an, die Initialisierungszeichenfolge `AT&F&C1&D2` an das Modem an Port `ttyS1` bei jeder Initialisierung der Leitung zu senden und stellt die Anschlussgeschwindigkeit auf 115000 bps ein, die korrekte Geschwindigkeit für ein 56K-Modem.

Der nächste Schritt ist die Aktivierung von AutoPPP. Bearbeiten Sie die Datei `/etc/mgetty+sendfax/login.config`, entfernen Sie das Kommentarzeichen für die AutoPPP-Zeile, und ändern Sie diese wie folgt:

```
/AutoPPP/ - @ /usr/sbin/ppd file options.server
```

Diese Änderungen weisen `mgetty` an, eingehende PPP-Verbindungen wie folgt zu bearbeiten:

- Keine spezifische Benutzer-ID für den Anruf festlegen (-)
- Den Benutzernamen des Anrufers bei allen `who`-Abfragen anzeigen (@)
- Befehl `/usr/sbin/pppd` ausführen und PPP-Optionen aus der Datei `/etc/ppp/options.server` lesen.

Nun müssen Sie natürlich die Datei `/etc/ppp/options.server` erstellen, und die folgenden Zeilen einfügen:

```
modem
/dev/ttyS0 115200
crtscts
ms-dns <IP des bevorzugten DNS-Servers>
-detach
+pap
-chap
login
```

`modem` gibt dem PPP-Protokoll die Verwendung von Modem-Steuerungsleitungen vor, und `crtscts` gibt die Verwendung der Hardware-Datenflusskontrolle vor. Die zweite Zeile gibt das zu verwendende Gerät vor, `/dev/ttyS0`, sowie die Anschlussgeschwindigkeit, 115200 bps. Falls es sich bei dem PPP-Prozess um einen Server für Microsoft Windows-Clients handelt, ermöglicht der Eintrag `ms-dns` diesem, ein oder zwei Adressen den Clients zur Verfügung zu stellen. `-detach` stellt sicher, dass der aufgespaltene Prozess `pppd` im Hintergrund ausgeführt wird.

+pap zwingt PPP zur Verwendung der PAP-Authentifizierung (Password Authentication Protocol), während die login-Direktive angibt, dass der Name und das Kennwort des Anrufers dem Benutzernamen und dem Kennwort aus der Datei /etc/passwd entsprechen sollte. Fügen Sie zur Ermöglichung der PAP-Authentifizierung die Zeile * * " " * in die Datei /etc/ppp/pap-secrets ein.

Fügen Sie die folgende Zeile zur Datei /etc/inittab hinzu, um den mgetty-Prozess in dem Modem zu starten, das zur Einwahl verwendet wird:

```
S1:2345:respawn:/usr/sbin/mgetty ttyS1
```

Wenn Sie einen unterschiedlichen Anschluss verwenden, müssen Sie diese Zeile entsprechend anpassen. Stellen Sie weiterhin sicher, dass Sie die Kennung am Zeilenanfang ändern, S1. Sie sollte den letzten beiden Zeichen des Anschlusses entsprechen, den Sie zur Einwahl verwenden, also erfordert z.B. ttyS0 die Kennung S0. Außerdem sollten Sie alle anderen Zeilen deaktivieren, die einen mgetty- oder getty-Prozess auf diesem Anschluss ausführen.

Als letzter Schritt werden diese Änderungen an initd weitergegeben. Mit dem Befehl

```
# init q
```

oder

```
# init Q
```

wird initd zum erneuten Einlesen der Datei /etc/inittab veranlasst. Die PPP-Einwahl ist jetzt aktiviert, wobei die PAP-Authentifizierung im Modem am Anschluss /dev/ttyS1 verwendet wird. Das PAP-Kennwort und der PAP-Name des Benutzers entspricht dem Benutzernamen und dem Kennwort in der Datei /etc/passwd.

Einrichten eines BOOTP/DHCP-Servers

DHCP ist vor allem in dynamischen, sich schnell ändernden Umgebungen nützlich. Wenn die an Ihr Netzwerk angeschlossenen Hosts ziemlich schnell wechseln, wenn sich die Netzwerkadressen bei einem Wechsel des Internetdienstanbieters ändern oder wenn Sie nur eine begrenzte Anzahl von IP-Adressen zur Verfügung haben, um eine große Anzahl von Hosts zu bedienen, die jeweils nur zeitlich begrenzt mit Ihrem Netzwerk verbunden sind, dann ist DHCP, das *Dynamic Host Configuration Protocol*, wahrscheinlich eine gute Lösung für Sie. Es ist wesentlich einfacher, ein paar Server zu ändern, als z.B. 150 Clientworkstations.

Einfache DHCP-Installationen lassen sich problemlos konfigurieren, obwohl aufgrund der Flexibilität von DHCP auch komplexe Installationen möglich sind. Dieses Kapitel konzentriert sich nur auf eine kleine und einfache DHCP-Konfiguration.

Die Konfigurationsdatei des DHCP-Servers lautet `/etc/dhcpd.conf`. Sie besteht aus einem allgemeinen Abschnitt, der für das gesamte Netzwerk gilt und anderen Abschnitten, die für Subnetze, Sammlungen von Hosts (werden manchmal auch *Gruppen* bezeichnet) oder spezifische Hosts relevant sind. Die Syntax der Konfigurationsdatei erinnert entfernt an die Programmiersprache C, da geschweifte Klammern `{` und `}` zum Einsatz kommen, um Abschnitte der Datei zu gruppieren und Semikolons, `;`, um Konfigurationsbefehle zu beenden. Stringdaten, wie z.B. ein vollständiger Domänenname, müssen in Anführungszeichen gesetzt werden.

Allgemeine Parameter

Das nachfolgende Listing ist ein Beispiel für einen allgemeinen Abschnitt einer DHCP-Konfigurationsdatei.

```
server-identifizier queen.bugcorp.com;  
option domain-name "bugcorp.com";  
option domain-name-server "queen.bugcorp.com";  
option subnet-mask 255.255.255.0;  
option broadcast-address 192.168.10.255;  
default-lease-time 7200;  
max-lease-time 86400;
```

Die erste Zeile gibt den Namen des DHCP-Servers an, `queen.bugcorp.com`, der eine einzelne IP-Adresse auflösen muss. Die vier `option`-Zeilen erklären sich von selbst. Die Parameter `default-lease-time` und `max-lease-time` werden in Sekunden angegeben. `default-lease-time` gibt die Standardleasedauer an, falls der Client keine bestimmte Leasedauer festlegt, während `max-lease-time` die maximale Leasedauer angibt, die überhaupt möglich.

Die subnet-Anweisung

Jeder DHCP-Server muss über eine `subnet`-Anweisung verfügen, um zu definieren, welches Subnetz er bedient und den Bereich der verleasten IP-Adressen festzulegen. Nehmen wir die folgende `subnet`-Anweisung:

```
subnet 192.168.10.0 netmask 255.255.255.0 {  
    range 192.168.10.1 192.168.10.50;  
    default-lease-time 28800;
```

```
        max-lease-time 144000;  
    }
```

Diese `subnet`-Anweisung definiert das Subnetz, für das der Server verantwortlich ist. Die drei Zeilen innerhalb der geschweiften Klammern geben Optionen an, die für dieses bestimmte Subnetz gelten. Die `range`-Deklaration gibt an, dass der Server einen Pool von 50 IP-Adressen hat, die er in diesem Subnetz vergeben kann. Beachten Sie, dass die allgemeinen Optionen gelten, es sei denn, Sie werden explizit überschrieben, wie dies hier bei `default-lease-time` und `max-lease-time` der Fall ist.

Die shared-network-Anweisung

Angenommen, Sie verfügen über zwei Subnetze, die von demselben DHCP-Server bedient werden sollen. Dies kann über die `shared-network`-Anweisung erreicht werden.

```
shared-network INSECT-NET {  
    subnet 192.168.10.0 netmask 255.255.255.224 {  
        range 192.168.10.3 192.168.10.30;  
        option routers 192.168.10.2;  
    }  
    subnet 192.168.10.32 netmask 255.255.255.224 {  
        range 192.168.10.35 192.168.10.60;  
        option routers 192.168.10.3;  
    }  
}
```

Dieser Abschnitt erstellt ein freigegebenes Netzwerk aus zwei Subnetzen, 192.168.10.0 und 192.168.10.32, die aus den, in den `subnet`-Anweisungen aufgelisteten IP-Adressenbereichen bestehen. Die `Optionrouters` stellt in diesem Fall zwei Ethernetschnittstellen in demselben Host dar, die die Verbindung zwischen den beiden Subnetzen ermöglichen.

Verwenden von BOOTP mit DHCP

Sie können DHCP auch für die Beantwortung von DHCP-Anfragen konfigurieren. Dazu benötigen Sie die MAC-Adresse der Netzwerkschnittstellenkarte, die die BOOTP-Anfrage durchführt. Sie müssen dabei einen Eintrag für alle Clients erstellen, die BOOTP verwenden.

```
group {  
    filename bootimage;
```

```
next-server queen.bugcorp.com;
host fire_ant {
    hardware ethernet 00:C0:C3:11:90:23;
}
host red_ant {
    hardware ethernet 00:D4:H9:49:2B:57;
}
}
```

Diese Listing verwendet die `group`-Anweisung zur Erstellung einer logischen Gruppe von BOOTP-Clients. Die `group`-Anweisung selbst hat keine Parameter, da sie ausschließlich vom DHCP-Server verwendet wird, um einen oder mehrere Parameter auf dieselbe Gruppe von Deklarationen anzuwenden. In diesem Fall lesen die beiden BOOTP-Hosts, `fire_ant` und `red_ant` ihr Bootimage aus der Datei, die mit der Deklaration `filename` als `bootimage` bezeichnet wird, und mounten ihr Root-Dateisystem vom Server aus, der in der Deklaration `next-server` als `queen.bugcorp.com` bezeichnet wird.

Die `host`-Anweisungen deklarieren zwei Hosts, `fire_ant` und `red_ant`, die ihre IP-Adresse über BOOTP abrufen. Die `hardware`-Anweisungen sind für das Booten der BOOTP-Clients erforderlich, da dadurch die Hardware (MAC)-Adressen an den Rechnernamen gebunden werden, der als Parameter zur `host`-Anweisung angegeben wird.

Zusätzliche Ressourcen

Webseiten

- <http://axion.physics.ubc.ca/ppp-linux.html>
- <http://www.calderasystems.com/support/>

Linux Documentation Project

- <http://www.linuxdoc.org/HOWTO/mini/DHCP.html>
- <http://www.linuxdoc.org/HOWTO/Diskless-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/DNS-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/Mail-Administrator-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/PPP-HOWTO.html>

- <http://www.linuxdoc.org/HOWTO/WWW-HOWTO.html>

Books

- *Apache: The Definitive Guide, 2nd Edition*, Ben Laurie and Peter Laurie (O'Reilly, 1999)
- *DNS and BIND, 3rd Edition*, Paul Albitz and Cricket Liu (O'Reilly, 1998)

KAPITEL 9

Konfigurieren eines Druckservers

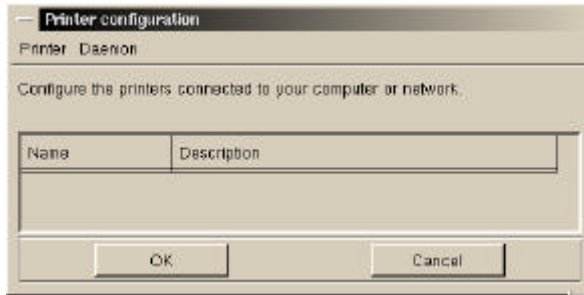
OpenLinux eServer eignet sich hervorragend als Plattform zur Bereitstellung von Datei- und Druckdiensten für andere Linux- und UNIX-Systeme sowie für Windows-Systeme in Ihrem Netzwerk. Dieses Kapitel behandelt die Verwendung von Webmin zur Konfiguration von Druckern.

Konfigurieren eines Druckservers

Webmin enthält derzeit kein eigenes Modul zur Druckerkonfiguration. Jedoch ist das Hinzufügen und Verwalten von Druckern mit COAS-Tool von Caldera ziemlich einfach. Wenn Sie einen Drucker einrichten, der direkt mit einem System verbunden ist, wird diese als lokaler Drucker (des Systems) angesehen, und an eine der parallelen Schnittstellen der Systeme angeschlossen. Drucker mit eigenen Netzwerkkarten (wie z.B. die Hewlett Packard JetDirect-Karten) werden als Remote-drucker angesehen, selbst wenn ein System das Druckspooling dafür übernimmt. Die Konfiguration ist immer gleich, unabhängig davon, ob es sich um einen lokalen oder Remotedrucker handelt.

Wählen Sie zu Beginn im KMenu den Befehl COAS->Peripherals->Printer aus. Abbildung 78 zeigt das anschließend angezeigte Dialogfeld.

ABBILDUNG 78. Das Dialogfeld Druckerkonfiguration von COAS



Klicken Sie als nächstes auf den Befehl Printer->Add, und wählen Sie einen Drucker im Listenfeld aus (siehe Abbildung 79). Die Liste enthält über 120 Drucker. Falls Sie Ihr genaues Druckermodell nicht finden, können Sie jederzeit eines der "generischen" Geräte am Listenanfang auswählen. Weisen Sie nach Auswahl des Druckers seiner Druckerwarteschlange einen Namen zu (siehe Abbildung 80).

ABBILDUNG 79. Auswählen eines Druckers

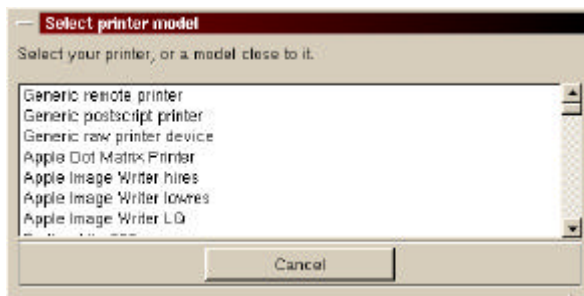
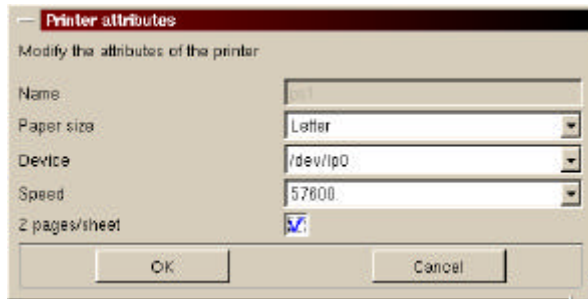


ABBILDUNG 80. Einstellen der Druckereigenschaften

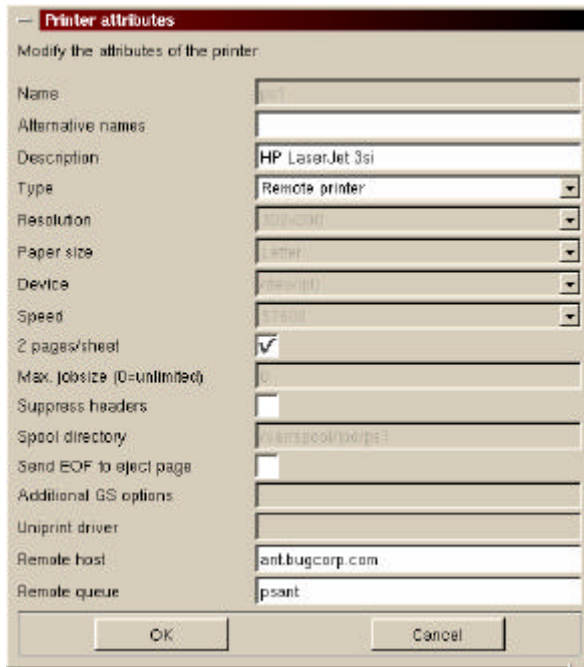


Führen Sie schließlich die gewünschten Änderungen der Druckereigenschaften durch, wie z.B. Duplexdruck, und klicken Sie anschließend auf die Schaltfläche "OK", um die Änderungen zu übernehmen. Klicken Sie auf die Schaltfläche "Save", um die Datei `/etc/printcap` zu aktualisieren, und dann (erneut) auf "OK", wodurch COAS zur Erstellung einer Druckerwarteschlange veranlasst wird. Danach wird erneut das Dialogfeld in Abbildung 80 angezeigt, mit der Ausnahme, dass der soeben konfigurierte Drucker zur Liste hinzugefügt wurde.

Verwenden Sie das gleiche Verfahren für Remotedrucker, und bearbeiten Sie anschließend die Druckerdefinition, um anzugeben, dass es sich um einen Remote-drucker handelt. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie auf den Namen der Warteschlange.
2. Wählen Sie den Menübefehl Printer->Edit aus. Der anschließend angezeigte Bildschirm sollte in etwa Abbildung 81 entsprechen.

ABBILDUNG 81. Bearbeiten der Druckereigenschaften



3. Wählen Sie im Dropdown-Listenfeld "Type" den Eintrag "Remote Printer" aus.
4. Geben Sie im Eingabefeld "Remote host" am unteren Rand des Dialogfeldes den Namen des Systems an, das diesen Drucker bedient.
5. Geben Sie im Eingabefeld "Remote queue" den Namen der Warteschlange ein.
6. Klicken Sie auf "OK".
7. Klicken Sie auf "Speichern".

Wenn Sie nach der Konfiguration aller Drucker im Hauptdialogfeld auf "OK" klicken, sind Sie bereit zum Drucken.

KAPITEL 10

Konfigurieren von MySQL

MySQL ist ein qualitativ hochwertiger Mehrbenutzer-SQL-Datenbankserver mit Multithreading (SQL, Structured Query Language, strukturierte Abfragesprache). Dieses Kapitel beschreibt kurz die Standardkonfiguration von MySQL auf Ihrem neu installierten OpenLinux eServer-System. Außerdem erlernen Sie die folgenden Aufgaben:

- Verbinden mit einem MySQL-Datenbankserver
- Hinzufügen von Benutzern zu einem MySQL-Datenbankserver
- Erstellen einer neuen MySQL-Datenbank

In den zusätzlichen Ressourcen am Ende des Kapitels erhalten Sie Verweise auf zusätzliche Informationsquellen zur allgemeinen Datenbanktheorie, zu SQL und zu MySQL im Besonderen.

Die Standardkonfiguration

Das nachfolgende Listing zeigt die komplette Konfigurationsdatei, `/etc/my.cnf`, für den MySQL-Datenbankserver. Die einzelnen Abschnitte der

Konfigurationsdatei werden im Anschluss besprochen. Beachten Sie, dass diese Konfigurationsdatei alle MySQL-Server betrifft. Falls Sie die Konfigurationsinformationen für einzelne Server festlegen möchten, speichern Sie die Konfigurationsdateien in den Verzeichnissen mit den einzelnen Datenbanken. Wenn Sie analog dazu Serveroptionen für einzelne Benutzer definieren möchten, legen Sie für jeden Benutzer eine eigene Kopie der MySQL-Konfigurationsdatei an. Wenn Sie eine umfassende Liste der Konfigurationsoptionen von MySQL anzeigen möchten, führen Sie folgenden Befehl aus:

```
# mysql --help

# Beispiel mysql-Konfig-Datei.
#
[client]
#password      = my_password
port           = 3306
socket         = /var/lib/mysql/mysql.sock
```

Der erste Abschnitt gilt für alle MySQL-Clients. Wäre die `password`-Option nicht herauskommentiert, würdem `my_password` an alle MySQL-Clients gesendet werden. Diese Option wird in der Regel in der persönlichen Konfigurationsdatei von Benutzern verwendet. Die Option `port` gibt die von MySQL verwendete Portnummer an – 3306 ist der Standardport von MySQL. Die Option `socket` gibt den vollständigen Pfadnamen des Sockets an, den MySQL für seinen Betrieb verwendet.

Die nächsten Abschnitte der Datei definieren Konfigurationsoptionen für bestimmte Programme, wie z.B. den Serverdämon, `mysqld`, und einen Dump-client, `mysqldump`. Der Programmname steht in eckigen Klammern

```
# Der MySQL-Server
[mysqld]
port           = 3306
socket         = /var/lib/mysql/mysql.sock
set-variable   = key_buffer=16M
set-variable   = max_allowed_packet=1M
set-variable   = thread_stack=128K
```

Die Optionen `port` und `socket` wurden bereits besprochen. Die drei `set_variable`-Anweisungen legen Optimierungsparameter für die MySQL-Datenbankengine fest. `key_buffer` gibt an, wieviel Arbeitsspeicher für Indizes verwendet wird; `max_allowed_packet` legt die Obergrenze für Netzwerkpakete fest, die MySQL lesen kann; `thread_stack` reserviert den angegebenen

Speicherplatz im Stack für threadrelevante Operationen. Solange Sie noch den Umgang mit MySQL erlernen, sollten Sie diese Werte unverändert lassen.

```
[mysql]  
no-auto-rehash
```

`mysql` ist ein Befehlszeilenclient für die Kommunikation mit dem Server, vor allem zur Durchführung von Abfragen der Datenbank und zur Statusabfrage der Datenbank und des Servers selbst. `no_auto_rehash` weist `mysql` an, die bisher eingegebenen Befehle nicht neu zu sortieren.

```
[mysqldump]  
set-variable      = max_allowed_packet=16M
```

```
[isamchk]  
set-variable= key_buffer=16M
```

`max_allowed_packet` und `key_buffer` wurden bereits besprochen. Bei `mysqldump` handelt es sich um ein Dienstprogramm, das eine Datenbank als Serie von SQL-Anweisungen oder als tabulatorgetrennte Textdatei exportiert. `isamchk` ist ein weiteres Dienstprogramm, das zum Beschreiben, Überprüfen, Optimieren und Reparieren von MySQL-Tabellen dient.

Verbinden mit einem MySQL-Server

Bevor Sie sich mit einer MySQL-Datenbank verbinden können, muss der Server aktiv sein. Durchsuchen Sie die Prozesstabelle nach einem Programm mit der Bezeichnung `mysqld`. Falls Sie das Programm nicht sehen, starten Sie den Server mit dem folgenden Befehl:

```
# /etc/rc.d/init.d/mysql start
```

Sobald der Server aktiv ist, geben Sie `mysql` an der Befehlszeile ein. Die Ausgabe sollte in etwa wie folgt aussehen:

```
# mysql -u root mysql  
Welcome to the MySQL monitor.  Commands end with ; or \q.  
Your MySQL connection id is 1 to server version 3.22.25-log
```

Type 'help' for help.

```
mysql>
```

Der Schalter `-u` muss von einem Benutzernamen gefolgt sein, in diesem Fall `root`. Das letzte Argument gibt den Namen der Datenbank an, mit der Sie eine Verbindung herstellen möchten. An dieser Stelle ist der Server zur Entgegennahme von Befehlen bereit. Natürlich kennen Sie noch keine, und es existiert auch noch keine Datenbank. Wir werden auf diese Aspekte in den nächsten beiden Abschnitten eingehen. Um den Client zu beenden, geben Sie `quit` ein, und drücken Sie die Eingabetaste.

Hinzufügen von Benutzern zu einem MySQL-Server

Der LIZARD-Installer erstellt einen Standardbenutzer, `root`, sowie eine Standarddatenbank, `mysql`. Da das Kennwort von `root` anfangs leer ist, besteht der erste Schritt darin, ein Kennwort zum Schutz vor unberechtigtem Zugriff festzulegen.

1. Starten Sie den `mysql`-Client, wie im vorhergehenden Abschnitt beschrieben wurde.
2. Führen Sie den folgenden SQL-Befehl aus:

```
mysql> UPDATE user SET Password=PASSWORD('new_password')
      > WHERE user='root';
Query OK, 2 rows affected (0.02 sec)
Rows matched: 2  Changed: 2  Warnings: 0
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)
mysql>
```

Zeilen, denen `mysql>` nicht vorausgeht, weisen auf eine Ausgabe der Datenbankengine hin. Ersetzen Sie `new_password` mit dem von Ihnen gewählten Kennwort. Beachten Sie, dass Befehle mit einem `;` beendet werden *müssen*. Nach Festlegung des Kennworts müssen Sie es eingeben, um auf die Datenbank als Benutzer mit der Bezeichnung `root` zugreifen zu können. Danach müssen Sie beim Starten die Option `-p` (password) verwenden, um sich anzumelden.

Nachdem Sie nun die Datenbank gesichert haben, können Sie Benutzer hinzufügen und Privilegien (Zugriffsrechte) mit Hilfe der `GRANT`-Anweisung bearbeiten. Angenommen, Sie haben einen Benutzer mit dem Namen `dbhack`, der Zugriff auf die Datenbank von einem Host mit der Bezeichnung `localhost` aus und dem Kennwort `stupid` wünscht. Führen Sie die folgende SQL-Anweisung aus:

```
GRANT SELECT, INSERT, UPDATE, DELETE
      ON mysql
      TO dbhack@localhost
```

IDENTIFIED by 'stupid';

Diese Anweisung ermöglicht `dbhack` das Anzeigen, Bearbeiten und Löschen von Einträgen in der Datenbank `mysql`.

Erstellen einer neuen MySQL-Datenbank

Dieser Abschnitt zeigt, wie Sie eine neue Datenbank in MySQL und eine neue Tabelle in der Datenbank erstellen.

- Erstellen einer neuen MySQL-Datenbank
- Erstellen einer Tabelle

Angenommen, der Benutzer `dbhack` möchte eine Datenbank mit der Bezeichnung `mylib` erstellen, um seine Bibliothek zu verwalten. Die Erstellung der Datenbank ist ein zweistufiger Prozess. Zunächst muss der MySQL-Administrator die Datenbank erstellen und dem Benutzer dafür `dbhack` Rechte zuweisen. Anschließend erstellt `dbhack` die Datenbanktabellen und füllt diese mit Daten aus.

Wie bereits erwähnt, muss der Administrator die Datenbank erstellen. Folglich startet `root` den `mysql`-Client, und führt die folgenden SQL-Befehle aus:

```
$ mysql -u root mysql -p
mysql> CREATE DATABASE mylib;
mysql> GRANT ALL ON mylib TO dhack@localhost;
```

Die erste SQL-Anweisung erstellt die Datenbank. Die zweite verleiht `dbhack`, bei Verbindung über `localhost`, administrative Rechte über die Datenbank. Um zu prüfen, ob die Datenbank erstellt wurde, verwenden Sie die SQL-Anweisung `SHOW DATABASES ;`.

Nachdem der MySQL-Administrator die Datenbank erstellt hat, muss `dbhack` seine innere Struktur erstellen und diese mit Daten füllen. Zunächst wird die Verbindung hergestellt:

```
$ mysql -u dbhack mylib -p
```

Die Ausführung des Befehls `SHOW TABLES` zeigt an, dass noch keine Tabellen existieren:

```
mysql> SHOW TABLES;
Empty set (0.00 sec)
mysql>
```

Aus Gründen der Übersichtlichkeit möchte dbhack die Bücher nur nach Titel, Autor und Veröffentlichungsjahr verwalten. Der SQL-Befehl dafür wird im Anschluss gezeigt:

```
mysql> CREATE TABLE book
      (title VARCHAR(50),
       author VARCHAR (20),
       pubyr YEAR);
```

Query OK, 0 rows affected (0.00 sec)

```
mysql> SHOW TABLES;
```

```
+-----+
| Tables in mylib |
+-----+
| book            |
+-----+
1 row in set (0.00 sec)
```

Jetzt, da die Tabelle existiert, kann diese mit Daten ausgefüllt werden. MySQL unterstützt eine große Teilmenge der Standard-SQL-Anweisungen, deshalb seien Sie auf eines der SQL-Lernprogramme verwiesen, das im Abschnitt *Zusätzliche Ressourcen* erwähnt wird.

Zusätzliche Ressourcen

Bücher

- *MySQL and mSQL*, Randy Jay Yarger, George Reese, and Tim King (O'Reilly, 1999)

Websites

- <http://www.mysql.org/>

KAPITEL 11

Sicherheit

Die Erhaltung eines sicheren Systems ist eine der Hauptaufgaben eines Systemadministrators. Die Erstellung eines absolut sicheren Systems ist praktisch unmöglich, es sei denn, man will dieses in einen versiegelten Tresorraum stellen, zu dem niemand den Schlüssel oder die Kombination hat. In der Praxis wird auf die meisten Systeme von mehreren Personen zugegriffen, entweder physisch oder per Remotezugang. Als Folge dessen ist es notwendig, Sicherheitsrichtlinien zu erstellen und diese zu befolgen. Bei der Erstellung von Sicherheitsrichtlinien gibt es viele Faktoren zu beachten. Dazu gehören Aspekte wie Vernetzung, Möglichkeit des physischen Zugriffs, Zugriff auf den Server über das Internet, verfügbare Intranetdienste sowie Kennwörter.

Herstellen der physischen Sicherheit

Die einfachste Art und Weise für jemanden, die Sicherheit Ihres Systems zu gefährden, besteht darin, allen Personen den physischen Zugriff zu gewähren. Falls Sie über ein Diskettenlaufwerk, ein CD-ROM-Laufwerk oder eine Festplatte verfügen, dann ist Ihr System nicht sicher. Falls ein Eindringling über eine Diskette, ein bootfähiges CD-ROM-Laufwerk oder sogar eine eigene Festplatte verfügt, können diese Geräte zum Booten Ihres Servers verwendet werden, wodurch diese vollen Zugriff auf die Informationen auf Ihrem Laufwerk erhalten.

Herstellen der Netzwerksicherheit

Nachdem die physische Sicherheit des Systems gewährleistet ist, muss als nächstes die Sicherheit des Netzwerks berücksichtigt werden. Die meisten Computer sind heute für den Informationsaustausch mit anderen Systemen miteinander vernetzt. Sogar die meisten privaten Systeme sind über Modems und das Internet vernetzt. Im nächsten Abschnitt wird die Netzwerksicherheit erläutert.

Kennwortsicherheit

Der erste Aspekt, den es zu berücksichtigen gibt, sind Kennwörter. Wenn Sie über ein schwaches Kennwort verfügen, wie z.B. eines, das auf einem regulären Wort aus einem Wörterbuch basiert, z.B. "Schlaf", würde ein Eindringling nur wenige Sekunden benötigen, um Ihr Kennwort herauszufinden. Wenn Sie dies vermeiden möchten, verwenden Sie Groß- und Kleinbuchstaben, Zahlen, Satzzeichen und andere Sonderzeichen, wie Sternchen (*) oder Zirkumflexzeichen (^). So können Sie z.B. ein Kennwort wie "DiTn%#6M" erstellen, das viel schwerer zu erraten ist.

Es ist jedoch nicht so schwierig, wie Sie denken, sich ein solches Kennwort zu merken. Sie könnten sich z.B. ein Kennwort wie D&v\$MA5 wie folgt merken:

- D Ihr Vorname ist "Dieter",
- ^ Ihr Geburtstag liegt im sechsten Monat (Umschalt+6 ergibt &),
- v Ihre Frau heisst "Vicky", und der Kleinbuchstabe erinnert Sie daran, dass sie klein ist.
- \$ Die erste Nummer von Vickys Sozialversicherungsnummer ist 4 (Umschalt+4 ergibt \$).
- MA Der Name Ihrer Tochter lautet "Marie-Ann"
- 5 Marie-Ann wurde um 05.00 Uhr geboren.

Hierbei handelt es sich um ein starkes Kennwort, das sich trotzdem leicht merken lässt. Kennwörter sollten häufig geändert werden, da sich fast alle durch einfache maschinelle Berechnungen knacken lassen.

Einschränken von Berechtigungen und Zugriff

Wenn Sie einen sicheren Computer in eine Netzwerkumgebung einbinden möchten, dann sind die ersten Überlegungen die Software, die Sie ausführen und die Berechtigungen, die Sie anderen Benutzern geben. Eine gute Daumenregel besteht darin, das Prinzip der *minimalen Berechtigung* anzuwenden. Dies bedeutet, dass Sie Benutzern nur Zugriff auf die Dateien und Programme geben, die sie für ihre

Arbeit benötigen. So benötigt z.B. ein normaler Benutzer, der nur in der Lage sein muss, E-Mail zu lesen und senden, im Internet zu surfen und Dokumente auszu-drucken, keinen Zugriff auf eine private Datenbank.

Überwachen des Systems

Wie können Sie erkennen, ob die Sicherheit Ihres Systems gefährdet wurde? Führen Sie eine häufige Überprüfung der Protokolle durch. Im Verzeichnis `/var/log` befinden sich eine Vielzahl von Protokollen, die die Systemaktivität aufzeichnen. `/var/log/secure` zeichnet z.B. alle zugriffs- und kennwort-spezifischen Aktivitäten auf, und bietet Ihnen somit eine Überwachungsliste darüber, wer zu welcher Zeit auf Ihr System zugegriffen hat.

Obwohl Systemprotokolle nützlich sind, gibt es zusätzliche Tools, die Sie verwenden können, wie z.B.:

- SAINT Security Administrator's Integrated Network Tool
- SARA Security Auditor's Research Assistant
- SATAN Security Administrator Tool for Analyzing Networks

Diese Programme helfen Ihnen bei der Ermittlung zusätzlicher Informationen so beim Überprüfen Ihres Netzwerks auf eine Vielzahl von Schwachstellen.

Als weitere wichtige Komponente der Systemsicherheit sollten Sie sicherstellen, dass keine der in Ihrem System installierten Software bekannte Sicherheits-schwachstellen hat. Es gibt eine Organisation, CERT (*Computer Emergency Response Team*), die solche Software-Schwachstellen (eng. Vulnerability) sammelt und dokumentiert. Geben Sie in Ihrem Webbrowser die Adresse <http://www.cert.org/> ein. Caldera Systems stellt auf seiner Website unter der Adresse <http://www.calderasystems.com/support/security/> ebenfalls eine Liste mit Sicherheitsupdates zur Verfügung.

Firewall und Paketfilter

Dieser Abschnitt erläutert die Erstellung einer Firewall zwischen Ihrem Server und anderen Systemen (in der Regel das Internet) sowie die Zugriffssteuerung auf Ihr internes Netzwerk mit Hilfe von Paketfiltern. *Firewalls* bieten einen Schutzwall zwischen dem Internet oder anderen externen Systemen und Ihrem internen Netzwerk. *Paketfilter* ermöglichen eine ähnliche Funktion, indem sie den Zugriff auf Ihr Netzwerk durch Untersuchen des Netzwerkverkehrs auf der Paketebene einschränken und nur solche Paketen durchlassen, die bestimmte Informationen enthalten.

Kernelunterstützung für Paketfilter

Zunächst benötigen Sie einen Kernel, in den IP-Firewallchains kompiliert wurden. Sie können überprüfen, ob der aktuell von Ihnen ausgeführte Kernel diese Funktion hat, indem Sie nach der Datei `/proc/net/ip_fwchains` suchen. Falls die Datei vorhanden ist, unterstützt der Kernel die IP-Firewallfunktion. Falls nicht, müssen Sie einen Kernel erstellen, der über IP-Firewallchains verfügt.

HINWEIS: In den OpenLinux eServerl-Kernels ist die IP-Firewallfunktion standardmäßig aktiviert. Sollten Sie sich entschließen, den Kernel aus den ursprünglichen Quelldateien erneut zu erstellen, müssen Sie die nachfolgenden Konfigurationsoptionen einstellen, damit der Kernel IP-Firewallchains unterstützt.

```
CONFIG_FIREWALL=y  
CONFIG_IP_FIREWALL=y
```

Konfigurieren eines Paketfilters

Das Tool `ipchains` kommuniziert mit dem Kernel und gibt an, welche Pakete zu filtern sind. `ipchains` erstellt und löscht Regeln im intern verwalteten Paketfilterabschnitt des Kernels. Die nachfolgenden Regeln implementieren also die folgenden Sicherheitsrichtlinien:

- Benutzer davon abhalten, sichere HTTP-Verbindungen mit dem Internet herzustellen – die Benutzer sollen arbeiten und nicht mit ihrer Kreditkarte einkaufen.

```
ipchains -a input -s localnet ! 443 -d 0/0 -i eth(outside) -j ACCEPT
```

- Benutzer außerhalb der Firewall den Zugriff auf DNS, Mail, POP-3, ssh und Ports mit hohen Nummern gestatten.

```
ipchains -A input -p all -s 0/0 -d eth(local) 53 -j ACCEPT
```

```
ipchains -A input -p all -s 0/0 -d eth(outside) 53 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(local) 22 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(outside) 22 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(inside) 1024:20000 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(outside) 1024:20000 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(incide) 25 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(outside) 25 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(inside) 110 -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d eth(outside) 110 -j ACCEPT
```

- Benutzern außerhalb der Firewall Zugriff auf alle anderen Funktionen verweigern.

```
ipchains -P input DENY
```

- IP-Routing durch die Firewall hindurch aktivieren.

`ipchains -P forward ACCEPT`

Speichern des Paketfilters

`ipchains` macht nichts anderes, als Regeln in die interne Routingtabelle des Kernels einzufügen, zu löschen und zu aktualisieren. Folglich gehen alle Regeln, die Sie einrichten, beim Neustart verloren. Verwenden Sie zum Speichern dieser Regeln die Skripts `ipchains-save` und `ipchains-restore`.

1. Führen Sie nach dem Einrichten der Regeln den folgenden Befehl (als Root-Benutzer) aus:

```
# ipchains-save > /etc/ipchains.rules
```

2. Erstellen Sie anschließend das folgende Skript, und speichern Sie es unter `/etc/rc.d/init.d/packetfilter`.

```
#!/bin/sh
# packetfilter - Skript zur Steuerung der Paketfilterung.
# Falls keine Regeln vorhanden, nichts tun
[ -f /etc/ipchains.rules ] || exit 0
case "$1" in
    start)
        echo -n "Paketfilterung aktivieren:"
        /sbin/ipchains-restore < /etc/ipchains.rules || exit 1
        echo 1 > /proc/sys/net/ipv4/ip_forward
        echo "."
        ;;
    stop)
        echo -n "Paketfilterung deaktivieren:"
        echo 0 > /proc/sys/net/ipv4/ip_forward
        /sbin/ipchains -X
        /sbin/ipchains -F
        /sbin/ipchains -P input ACCEPT
        /sbin/ipchains -P output ACCEPT
        /sbin/ipchains -P forward ACCEPT
        echo "."
        ;;
    *)
        echo "Verwendung: /etc/init.d/packetfilter {start|stop}"
        exit 1
        ;;
esac
```

exit 0

Dieses Skript sollte früh innerhalb des Startvorgangs ausgeführt werden. Verwenden Sie das Webmin-Modul "Bootup and Shutdown Actions", um dieses Skript zu konfigurieren. Wenn Sie alternativ dazu die Änderung manuell durchführen und direkt in das grafische System booten, können Sie eine symbolische Verknüpfung mit der Bezeichnung `S39packetfilter` im Verzeichnis `/etc/rc.d/rc5.d` erstellen. Falls Sie in das Runlevel 3 booten, der nicht grafischen Anmeldung, erstellen die symbolische Verknüpfung im Verzeichnis `/etc/rc.d/rc3.d`.

IP-Masquerading – Kurzübersicht

Neben der Paketfilterung des Kernels steuert `ipchains` auch das IP-Masquerading und das transparente Proxying. Leider werden in der aktuellen Linux-Implementierung diese beiden Begriffe irrtümlicherweise miteinander vermischt. Masquerading und Proxying sind nicht miteinander verwandt.

Der nachfolgende Abschnitt setzt voraus, das Ihre externe Schnittstelle, die mit dem Internet kommuniziert, die Bezeichnung `eth0` hat. Ist dies nicht der Fall, passen Sie die folgenden Befehle entsprechend an.

```
# ipchains -P forward DENY
# ipchains -A forward -i eth0 -j MASQ
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Geläufige Firewall-Setups

Dieser Abschnitt beschreibt unterschiedliche Firewall-Setups, mit denen Sie das interne Netzwerk vor potentiellen Angreifern aus dem Internet schützen können, und gleichzeitig den LAN-Zugriff auf das Internet ermöglichen. Jedes Setup setzt das folgende, sehr geläufige Szenario voraus:

Sie verwalten das Netzwerk von `bugcorp.com`. Das Unternehmen verfügt über ein LAN auf TCP/IP Ethernet-Basis mit IP-Adressen aus einem der privaten Adressbereiche:

Netzwerk der Klasse A - 10.0.0.0 - 10.255.255.255

Netzwerk der Klasse B - 172.16.0.0 - 172.31.255.255

Netzwerk der Klasse C - 192.168.0.0 - 192.168.255.255

bugcorp.com verfügt über eine zugewiesene IP-Adresse, 1.2.3.4., bei der es sich um den Rechner mit der Bezeichnung firewall.bugcorp.com handelt. Entscheidend ist, dass das private Netzwerk mit dem Internet über einen einzigen T1-Anschluss verbunden ist.

Privates Netzwerk Traditionelle Proxies

Dieses Setup verhindert, dass Pakete aus dem privaten Netzwerk direkt in das Internet übertragen werden. Die einzige Möglichkeit für Rechner, eine Internetverbindung herzustellen, ist über die Firewall. Die Firewall ist der einzige Rechner in beiden Netzwerken, der sowohl mit dem Internet als auch dem privaten Netzwerk verbunden ist. Programme, die in der Firewall ausgeführt werden, sogenannte Proxies, bieten Zugriff auf FTP, das World Wide Web, Telnet, RealAudio, Usenet-News und andere Dienste. Umgekehrt müssen alle Dienste, die Sie eingehenden Verbindungen aus dem Internet zur Verfügung stellen möchten, in der Firewall ausgeführt werden.

So ermöglichen Sie den Webzugriff vom privaten Netzwerk auf das Internet:

1. Ein Webproxy (Squid, Teil von OpenLinux eServer) wird auf der Firewall installiert und konfiguriert, die auf dem Standardport 8080 ausgeführt wird.
2. Netscape-Browser im privaten Netzwerk müssen für die Verwendung des Firewallports 8080 als Proxy für HTTP konfiguriert werden.
3. Domain Name Services (DNS) brauchen im privaten Netzwerk nicht konfiguriert werden.
4. DNS muss in der Firewall konfiguriert werden.
5. Das private Netzwerk benötigt keine Standardroute, häufig auch Gateway genannt.

Privates Netzwerk Transparente Proxies

Transparente Proxies funktionieren ähnlich wie traditionelle Proxies.

- Pakete aus dem privaten Netzwerk durchqueren niemals das Internet.
- Pakete aus dem Internet durchqueren niemals das private Netzwerk.
- Alle Verbindungen mit dem Internet erfolgen durch die Firewall.
- Proxyprogramme innerhalb der Firewall ermöglichen den Internetzugriff für alle Rechner im privaten Netzwerk.

- Alle Dienste, auf die vom Internet aus zugegriffen wird, müssen sich in der Firewall befinden.

Der einzige faktische Unterschied zwischen traditionellen und transparenten Proxies besteht darin, dass Clientprogramme, wie z.B. Webbrowser, speziell für die Verwendung von Proxydiensten konfiguriert werden müssen, während in einer traditionellen Proxyumgebung Clients von der Existenz eines Proxys nicht zu wissen brauchen. Die Konfigurationen sind jedoch leicht unterschiedlich, wie im Anschluss gezeigt:

1. Auf der Firewall muss ein transparenter Webproxy, wie z.B. `transproxy` installiert und konfiguriert sein.
2. Verwenden Sie `ipchains` zur Konfiguration des Kernels, um Verbindungen mit Port 80 an den Proxy umzuleiten.
3. Internetclients im privaten Netzwerk benötigen keine spezielle Konfiguration. Sie können Standard-Portnummern verwenden.
4. Ein DNS-Server muss sowohl im privaten Netzwerk als auch in der Firewall ausgeführt werden.
5. Eine Standardroute oder Gateway muss im privaten Netzwerk konfiguriert werden, um Pakete an die Firewall senden zu können.

Privates Netzwerk Masquerading

In diesem Szenario werden Pakete, die zwischen dem privaten Netzwerk und dem Internet übertragen werden, speziell behandelt. Anstelle eines Proxys wird eine spezielle Kernelfunktion, das sogenannte Masquerading, verwendet. *Beim Masquerading* werden die Headerinformationen von Paketen beim Durchlaufen der Firewall umgeschrieben, wodurch es den Anschein hat, dass diese aus der Firewall selbst stammen. Die Firewall schreibt wiederum die Antwortpakete um, so dass es den Anschein hat, dass diese an den korrekten internen Empfänger gesendet werden. Alle Dienste, auf die vom Internet aus zugegriffen wird, müssen sich in der Firewall befinden.

So ermöglichen Sie den Webzugriff vom privaten Netzwerk auf das Internet:

1. Konfigurieren Sie die Firewall für das Masquerading aller Pakete, die aus dem privaten Netzwerk stammen und an Port 80 auf einem Internethost übertragen werden.
2. Die meisten Webbrowser können für eine direkte Verbindung konfiguriert werden.
3. DNS muss im privaten Netzwerk konfiguriert werden.

4. Die Firewall ist die Standardroute/Gateway des privaten Netzwerks.

Öffentliches Netzwerk

In diesem Szenario ist Ihr persönliches Netzwerk Teil des Internets: Pakete können ohne Änderung zwischen beiden Netzwerken übertragen werden. Die IP-Adressen des internen Netzwerks müssen durch Beantragung eines IP-Adressenblocks zugewiesen werden, damit der Rest des Netzwerks Pakete an Sie übertragen kann. Dies setzt eine permanente Verbindung voraus.

In dieser Rolle dient die Paketfilterung der Einschränkung der Pakete, die zwischen Ihrem Netzwerk und dem Rest des Internets weitergeleitet werden können, z.B. um dem Internet nur den Zugriff auf interne Webserver zu ermöglichen.

So ermöglichen Sie den netzwerkinternen Webzugriff auf das Internet:

1. Den Systemen im internen Netzwerk werden IP-Adressen von den registrierten Adressenblöcken zugewiesen.
2. Die Firewall lässt das Eindringen des gesamten Datenverkehrs in Ihr privates Netzwerk zu.
3. Die meisten Webbrowser müssen für eine direkte Verbindung konfiguriert werden.
4. DNS muss für Ihr internes Netzwerk konfiguriert werden.
5. Das private Netzwerk verwendet die Firewall als Standardroute/Gateway.

TCP-Wrapper

Viele Internet-Clientprogramme `ftp` und `telnet` können für die Verwendung von TCP-Wrapper konfiguriert werden, die den Zugriff auf Ihre Systeme enger einschränken und somit die Sicherheit verbessern. Viele der Dienste, die in der Datei `/etc/inetd.conf` aufgelistet sind, wie z.B. `FTP`, `telnet`, `IMAP`, `finger`, verwenden TCP-Wrapper. *TCP-Wrapper* sind Programme, die eine sehr kontrollierte Umgebung für die Ausführung von Programmen, wie z.B. `telnet` bieten. Durch Steuerung der Ausführungsumgebung können Sie einschränken, auf welche Teile Ihres Systems mit welchen Berechtigungen zugegriffen werden kann, usw.

Wenn nur bestimmte Personen ein Programm verwenden sollen, fügen Sie Ihre Benutzernamen in die Datei `/etc/hosts.allow` ein, um diesen expliziten Zugriff zu erlauben. Dieser Vorgang ist auch für bestimmte IP-Adressen oder

IP-Adressenbereiche oder sogar für ganze Domänen möglich. Analog gibt die Datei `/etc/hosts.deny` mit derselben Syntax wie `/etc/hosts.allow` an, wer auf Dienste zugreifen kann, die von TCP-Wrapper kontrolliert werden. In der Praxis wird häufig zunächst allen Benutzern der Zugriff auf Dienste in der Datei `/etc/hosts.deny` verweigert. Anschließend werden die berechtigten Benutzer (oder IP-Adressen bzw. Domännennamen) selektiv in die Datei `/etc/hosts.allow` eingefügt.

Beispiel: Die folgende Datei `/etc/hosts.deny` verweigert allen Benutzern den Zugriff auf alle Dienste:

```
# /etc/hosts.deny
# service : person
ALL : ALL
```

Um dem Benutzer `john@bugcorp.com`, einer beliebigen IP-Adresse im Bereich `192.168.0.0 - 192.168.255.255` und allen Benutzern aus der Toplevel-Domäne `edu` Zugriff auf Ihr System zu erlauben, sollte die Datei `/etc/hosts.allow` in etwa wie folgt aussehen.

```
# /etc/hosts.allow
# service : person
ALL : john@bugcorp.com
ALL : 192.168.*.*
ALL : *.*.edu
```

Beachten Sie, dass es sich bei dem Sternchen um kein globales Platzhalterzeichen handelt. `*.edu` ist nicht identisch mit `*.*.edu`. In dieser Schreibweise entsprechen nur Rechnernamen im Format *beliebiger.rechner.edu* dieser Regel.

Die Standardsicherheitsregel für OpenLinux eServer lautet `ALL : ALL : ALLOW`. Diese Regel lässt alle Verbindungen zu Dämonen zu, die herauskommentiert oder nicht in der Datei `/etc/hosts.allow` enthalten sind. Dabei besteht eine Ähnlichkeit mit den Sicherheitsrichtlinien von OpenLinux 2.3. Um jedoch diese Standardeinstellung mit anderen Regeln in dieser Datei konform zu machen, wird empfohlen, dass die Zeile 132 herauskommentiert und das Kommentarzeichen in Zeile 136 entfernt wird (`ALL : localhost YOUR_subnet KNOWN : ALLOW`). Dadurch stehen Standardverbindungen nur dem `localhost`, `localnet` und bekannten Hosts zur Verfügung, d.h. Rechnernamen, die bekannte Adressen auflösen.

Secure Shell (SSH)

Telnet ist kein sehr sicheres Programm, da der Benutzername und das Kennwort im Klartext übertragen werden. Auf diese Weise können alle Benutzer ein Paketüberwachungsprogramms (wie z.B. Sniffit) das Kennwort und den Benutzernamen ermitteln. Es gibt jedoch eine Option, die die gesamte Funktionalität von Telnet ohne die Sicherheitsrisiken zulässt: SSH. Mit SSH wird der Benutzername und das Kennwort verschlüsselt, wodurch deren Ermittlung wesentlich erschwert wird (es würde sehr viel Zeit und Rechenaufwand erfordern).

Secure Socket Layer (SSL)

Wenn Sie Kreditkartennummern, Kennwörter oder Bankdaten online erhalten, sollte ihre Website maximale Sicherheit bieten. Dies kann durch Programme wie "Websphere" oder "Secure Apache" erreicht werden. Diese Programme verwenden SSL oder Secure Socket Layer. Sie können dieses Protokoll im Web beziehen, oder die dazugehörige Verschlüsselungssoftware erwerben. Viele Leute verwenden OpenSSL zur Ausführung von "Secure Apache". Dieses Programm bietet Verschlüsselungsfunktionen für Ihre Website, um eine sichere Übertragung von Informationen zu gewährleisten (wie bei SSH).

Pretty Good Privacy (PGP)

SSH und SSL sind Methoden zur Verschlüsselung von Daten, die im Internet übertragen werden. Aber was passiert, wenn jemand ihren tragbaren Computer stiehlt, der streng geheime Daten enthält? PGP bietet eine Möglichkeit, Ihre wichtigen Daten vor dem Zugriff anderer zu schützen. Mit PGP können Sie alles von einer Datei bis zu einem gesamten Laufwerk verschlüsseln. Bei der Verwendung von PGP wird empfohlen, ein Kennwort für Ihre verschlüsselten Daten und ein anderes für die Anmeldung festzulegen. Wenn die Daten eine Verschlüsselung rechtfertigen, sollten Sie auch daran denken, ein starkes Kennwort zu verwenden.

Zusätzliche Informationen

Linux Documentation Project

- <http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html>
- <http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html>

Websites

- <http://www.cert.org/>
- <http://www.networkassociates.com/>

Bücher

- Building Internet Firewalls, D. Brent Chapman and Elizabeth D. Zwicky (O'Reilly, 1995)
- Practical UNIX and Internet Security, 2nd Edition, Simson Garfinkel and Gene Spafford (O'Reilly, 1996)

Index

A

Analysieren 22
Ändern der globalen Bootoptionen 58
Apache 119
Apache-Konfiguration unter Verwendung von Webmin 126
AppWatch 8
Auswählen der Zeitzone 43
Auswählen einer Rootpartition 29
Auswählen von NIS-Servern 76
Automatisches Laden von Kernelmodulen 67

B

Benutzerdefiniertes Partitionieren 27
Berechtigungen und Zugriff 152
Bildschirm Edit Boot Kernel 57
Booten von Linux 47
BOOTP 119
BOOTP/DHCP Server 135

C

Caldera Systems 7
Caldera Systems, Wer ist 9
Cheops 8, 108
cron 78

D

Dateisysteme 83
Der Bildschirm Edit Group von Webmin 72
Der Bildschirm LILO Global Options von Webmin 59
DHCP 39, 119
Disk Quota Unterstützung 8
Disketten 14
Domain Masquerading 122
Domain Name Server 129
Domain Name Service 119
Domain Routing 124
Druckserver 141
Dynamic Host Configuration Protocol 39

E

Einrichten eines BOOTP/DHCP-Servers 135
Einrichten eines Domain Name Servers 129
Einrichten eines FTP-Servers 127
Einrichten eines Webserver 125
Einwahl-Unterstützung 119
Erstellen der Installationsdisketten 14
Erstellen eines neuen Benutzer-Accounts 37
Erstellen von Benutzer-Accounts 35
Ethereal 8
Ethernet 39

F

Farbtiefe 24
Festlegen des Grafikmodus 24
Festplatte 29
Festplattenpartitionen 81
Firewall und Paketfilter 153
Firewall-Setups, geläufige Beispiele 156
Fortgeschrittene Webmin-Konfiguration 92
FTP-Server 127
Funktionen von OpenLinux eServer 7

G

GMT 43
gpm-Konfigurationsbildschirm 52

H

Handbuch für Systemadministratoren 11
Herstellen der physischen Sicherheit 151
Hilfe während der Installation 19
Hinzufügen von Benutzern in eine Gruppe 73
HOWTO-Dokumente 69

I

Installationsserver 13
Installationsdisketten 14
Installationsserver 16
Installationssupport 10
Installieren des Bootloaders 40
Installieren von OpenLinux eServer 19
Internet 119
Intranet 119
IP-Adresse 40
IP-Masquerading – Kurzübersicht 156

K

- KDE 113
- KDE-Desktop, anpassen 116
- KDE-Funktionen 114
- KDM 45
- Kennwortsicherheit 152
- Kernel 8
- Konfigurieren des Grafiksystems 20
- Konfigurieren des Monitors 23
- Konfigurieren eines Druckservers 141
- Konfigurieren eines Mailservers 120
- Konfigurieren eines PPP-Einwahlservers 133
- Konfigurieren von MySQL 145
- Konfigurieren von OpenLinux eServer als NIS-Client 75
- Konfigurieren von OpenLinux eServer als NIS-Server 76
- Konfigurieren von Webmin 45

L

- LILO 40
- LILO-Bootvorgang 47
- Linux Bootup Configuration Modul 55
- Linux for eBusiness 7
- Linux Installationsprogramm 13
- LIZARD 13

M

- Mail Queue 125
- Manuelles Laden von Kernelmodulen 66
- Masquerading 122
- Master Boot Record 41
- Mauskonfiguration 19
- MBR 41
- Modifizieren des aktuellen Kernels 56
- Modul Bootup and Shutdown 51
- Moduldiskette 14, 15
- MySQL 11, 145
- MySQL Server, verbinden 147
- MySQL-Datenbank, neu erstellen 149
- MySQL-Server, Benutzer hinzufügen 148

N

Netscape 50
Netwatch 102
Netzwerkeinstellungen 38
Neues Initialisierungsskript 54
Neukompilieren des Kernels 63
Nicelevel 89
NIS 73
Ntop 108

O

OpenLDAP 8
OpenLinux eServer 7

P

Paketfilter 153
Paketverwaltung 90
Pentium II 8
PHP3 8
Physische Sicherheit 151
PPP-Einwahlserver 133
Pretty Good Privacy (PGP) 161
Prozesssteuerung 86

R

RAID 8
Relay Domains 124
Rootkennwort 36

S

Scotty 8, 109
Secure Shell (SSH) 161
Secure Socket Layer (SSL) 161
selbst betreut 9
Sendmail 119
Sicherheit 12, 151
Sniffit 97
Software-Paketmanagement 90
Speicherort von KDE-Dateien 113
Sprachauswahl 19
Squid 8
Standardinstallation 13, 14
Systeminitialisierung 48, 49
Systemkonfiguration und -administration 69

T

tcpdump 104
TCP-Wrappers 159
Technischer Support 9
Tetris 43
Tools zur Netzwerküberwachung 97
Trusted Users 123

U

Überwachen des Systems 153
unbeaufsichtigte Installation mit Hilfe des Lizard 14, 17
unbeaufsichtigte Installation 16
unbeaufsichtigte Installation 13
Universal Coordinated Time 43

V

Verwalten des Kernels 63
Verwenden von Kernelmodulen 65
Verwenden von LILO 55

W

Webmin 8
Webmin Hauptbildschirm 50
Webmin Tools zur Systemadministration 78
Webserver 125
Website für Support 10
Website für Support durch Caldera Systems 10
WUFTP 119

X

X Window Grafiksystem 20

Y

Yellow Pages 73

Z

Zentrales Verwalten von Benutzern und Gruppen mit NIS 73