



SuSE Linux Desktop

Referenz

System- und
Netzwerkkonfiguration

Auflage 2003

Copyright ©

Dieses Werk ist geistiges Eigentum der SuSE Linux AG.

Es darf als Ganzes oder in Auszügen kopiert werden, vorausgesetzt, dass sich dieser Copyrightvermerk auf jeder Kopie befindet.

Alle in diesem Buch enthaltenen Informationen wurden mit größter Sorgfalt zusammengestellt. Dennoch können fehlerhafte Angaben nicht völlig ausgeschlossen werden. Die SuSE Linux AG, die Autoren und die Übersetzer haften nicht für eventuelle Fehler und deren Folgen.

Die in diesem Buch verwendeten Soft- und Hardwarebezeichnungen sind in vielen Fällen auch eingetragene Warenzeichen; sie werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Die SuSE Linux AG richtet sich im Wesentlichen nach den Schreibweisen der Hersteller. Die Wiedergabe von Waren- und Handelsnamen usw. in diesem Buch (auch ohne besondere Kennzeichnung) berechtigt nicht zu der Annahme, dass solche Namen (im Sinne der Warenzeichen und Markenschutz-Gesetzgebung) als frei zu betrachten sind.

Hinweise und Kommentare richten Sie ggf. an documentation@suse.de

| | |
|-------------------|--|
| <i>Autoren:</i> | Frank Bodammer, Stefan Dirsch, Roman Drahtmüller, Karl Eichwalder, Werner Fink, Dennis Geider, Carsten Groß, Olaf Hering, Andreas Jaeger, Jana Jaeger, Klaus Kämpf, Olaf Kirch, Hubert Mantel, Michael Matz, Johannes Meixner, Lars Müller, Anas Nashif, Susanne Oberhauser, Edith Parzefall, Peter Poeml, Marc Rührschneck, Marcus Schaefer, Klaus Singvogel, Andreas Schwab, Martin Sommer, Klaus G. Wagner, Christian Zoz |
| <i>Redaktion:</i> | Antje Faber, Dennis Geider, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Marc Rührschneck, Thomas Schraitle, Martin Sommer, Rebecca Walter |
| <i>Layout:</i> | Manuela Piotrowski, Thomas Schraitle |
| <i>Satz:</i> | L ^A T _E X |

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

Inhaltsverzeichnis

| | | |
|----------|---|----------|
| I | System | 1 |
| 1 | AutoYast2: Automatische Installation und Konfiguration | 3 |
| | Einführung | 4 |
| | Zusammenstellung der Information | 5 |
| | Das Control File | 5 |
| | Format | 6 |
| | Struktur | 8 |
| | Die XML Document Type Definition (DTD) | 11 |
| | Erstellung eines neuen Control Files | 13 |
| | Benutzung des Configuration Management Systems | 13 |
| | Manuelle Erstellung und Bearbeitung eines Control Files | 18 |
| | Profilressourcen unter der Lupe | 18 |
| | Die Quelle der Installationsdaten festlegen | 40 |
| | Automatische Installation eines Einzelplatzrechners | 40 |
| | Netzwerkinstallationen | 40 |
| | Verwaltung des Bootvorgangs | 43 |
| | Booten des Zielsystems | 43 |
| | Booten des Clients | 43 |
| | Auslösen der automatischen Installation | 49 |
| | Starten der automatischen Installation | 54 |
| | Der Autoinstallationsprozess | 54 |
| | Systemkonfiguration | 55 |
| | Postinstallation und Systemkonfiguration | 56 |
| | Systemanpassung | 56 |

| | | |
|----------|---|------------|
| 2 | Das X Window System | 57 |
| | Geschichtlicher Hintergrund | 58 |
| | Die Version 4.x von XFree86 | 59 |
| | Konfiguration mit xf86config | 60 |
| | Installation des X Window System optimieren | 70 |
| | Zusätzliche (TrueType-)Fonts einbinden | 76 |
| | Konfiguration von OpenGL/3D | 80 |
| 3 | Booten und Bootmanager | 85 |
| | Der Bootvorgang auf dem PC | 86 |
| | Bootkonzepte | 87 |
| | Map Files, GRUB und LILO | 88 |
| | Booten mit GRUB | 89 |
| | Das Menü | 89 |
| | Namen für BIOS-Geräte | 91 |
| | Installation mit der GRUB-Shell | 91 |
| | Weiterführende Informationen | 92 |
| | Booten mit LILO | 92 |
| | Grundlagen | 93 |
| | LILO-Konfiguration | 94 |
| | Der Aufbau der Datei lilo.conf | 94 |
| | Installation und Deinstallation von LILO | 98 |
| | Bei Bootproblemen: Boot-CD erstellen | 100 |
| | Boot-CD mit ISOLINUX | 100 |
| 4 | Hotplug | 103 |
| | Realisierung von Hotplug in Linux | 104 |
| | Hotplug starten und Coldplug | 104 |
| | USB | 105 |
| | PCI und PCMCIA | 106 |
| | Netzwerk | 107 |
| | Firewire (IEEE1394) | 108 |
| | Sonstige Geräte und weitere Entwicklung | 109 |

| | |
|---|------------|
| 5 Konfiguration und mobiles Arbeiten mit Notebooks | 111 |
| PCMCIA | 112 |
| Die Hardware | 112 |
| Die Software | 112 |
| Die Konfiguration | 114 |
| Konfigurationen zum Umschalten – SCPM | 116 |
| Wenn's trotzdem nicht geht | 117 |
| Installation via PCMCIA | 121 |
| Weitere Hilfsprogramme | 122 |
| Kernel oder PCMCIA Paket aktualisieren | 123 |
| Weiterführende Informationen | 123 |
| SCPM – System Configuration Profile Management | 123 |
| Grundbegriffe und Grundlagen | 124 |
| SCPM YaST2 Modul und weiterführende Dokumentation | 125 |
| SCPM einrichten | 125 |
| Profile anlegen und verwalten | 126 |
| Zwischen Konfigurationsprofilen umschalten | 127 |
| Erweiterte Profileinstellungen | 128 |
| Profilauswahl beim Booten | 129 |
| APM und ACPI – Powermanagement | 131 |
| Stromsparfunktionen | 131 |
| APM | 133 |
| Weitere Befehle | 135 |
| ACPI | 135 |
| Pause für die Festplatte | 136 |
| IrDA – Infrared Data Association | 138 |
| Software | 138 |
| Konfiguration | 139 |
| Verwendung | 139 |
| Troubleshooting | 140 |

| | | |
|-----------|--|------------|
| 6 | Der Kernel | 141 |
| | Die Kernelquellen | 141 |
| | Kernel-Module | 141 |
| 7 | Systemmerkmale | 145 |
| | Hinweise zu speziellen Softwarepaketen | 146 |
| | Paket bash und /etc/profile | 146 |
| | Paket cron | 146 |
| | Protokoll-Dateien – das Paket logrotate | 147 |
| | Manual-Pages | 148 |
| | Der Befehl ulimit | 149 |
| | Der Befehl free | 150 |
| | Die /etc/resolv.conf | 150 |
| | Virtuelle Konsolen | 151 |
| | Tastaturbelegung | 151 |
| | Lokale Anpassungen – I18N/L10N | 152 |
| 8 | Das Bootkonzept | 157 |
| | Das init-Programm | 158 |
| | Die Runlevels | 158 |
| | Wechsel des Runlevels | 160 |
| | Die Init-Skripten | 161 |
| | Der YaST2 Runlevel-Editor | 164 |
| | SuSEconfig, /etc/sysconfig und /etc/rc.config | 165 |
| | Systemkonfiguration mit dem YaST2 Sysconfig-Editor | 167 |
| | Skripte und Variablen – Konfiguration des Systems | 167 |
| II | Netzwerk | 199 |
| 9 | Grundlagen der Vernetzung | 201 |
| | TCP/IP - Das von Linux verwendete Protokoll | 202 |
| | Schichtenmodell | 203 |
| | IP-Adressen und Routing | 206 |

| | |
|--|-----|
| Domain Name System | 209 |
| IPv6 – Internet der nächsten Generation | 210 |
| Warum ein neues Internet-Protokoll? | 210 |
| Aufbau einer IPv6-Adresse | 212 |
| IPv6-Netzmasken | 214 |
| Weiterführende Literatur und Links zu IPv6 | 215 |
| Die Einbindung ins Netzwerk | 216 |
| Vorbereitungen | 216 |
| Konfiguration mit YaST2 | 216 |
| PCMCIA | 218 |
| Konfiguration von IPv6 | 218 |
| Manuelle Netzwerkkonfiguration | 219 |
| Konfigurationsdateien | 219 |
| Startup-Skripten | 225 |
| Routing unter SuSE Linux Desktop | 225 |
| DNS – Domain Name Service | 227 |
| Nameserver BIND starten | 227 |
| Die Konfigurationsdatei /etc/named.conf | 229 |
| Weitere Informationen | 236 |
| NIS – Network Information Service | 237 |
| NIS-Master- und -Slave-Server | 237 |
| Das NIS-Client-Modul im YaST2 | 239 |
| Manuelles Einrichten eines NIS-Clients | 240 |
| NFS – verteilte Dateisysteme | 242 |
| Importieren von Dateisystemen mit YaST2 | 242 |
| Manuelles Importieren von Dateisystemen | 243 |
| Exportieren von Dateisystemen mit YaST2 | 243 |
| Manuelles Exportieren von Dateisystemen | 243 |
| DHCP | 247 |
| Das DHCP-Protokoll | 247 |
| DHCP-Softwarepakete | 247 |
| Der DHCP-Server dhcpd | 248 |
| Rechner mit fester IP-Adresse | 250 |
| Weitere Informationen | 251 |

| | |
|--|------------|
| 10 Heterogene Netzwerke | 253 |
| Samba | 254 |
| Installation und Konfiguration des Servers | 255 |
| Samba als Anmelde-Server | 259 |
| Installation der Clients | 260 |
| Optimierung | 261 |
| Netatalk | 262 |
| Konfiguration des Fileservers | 263 |
| Konfiguration des Druckservers | 266 |
| Starten des Servers | 267 |
| 11 Internet | 269 |
| Konfiguration eines ADSL / T-DSL Anschlusses | 270 |
| Standardkonfiguration | 270 |
| DSL Verbindung per Dial-on-Demand | 270 |
| Proxy-Server: Squid | 271 |
| Was ist ein Proxy-Cache? | 272 |
| Informationen zu Proxy-Cache | 272 |
| Systemanforderungen | 274 |
| Squid starten | 276 |
| Die Konfigurationsdatei /etc/squid.conf | 277 |
| Transparente Proxy-Konfiguration | 283 |
| Squid und andere Programme | 285 |
| Weitere Informationen zu Squid | 290 |
| 12 Sicherheit im Netzwerk | 291 |
| Masquerading und Firewall | 292 |
| Grundlagen des Masquerading | 292 |
| Grundlagen Firewalling | 294 |
| SuSEfirewall2 | 295 |
| SSH – secure shell, die sichere Alternative | 297 |
| Das OpenSSH-Paket | 298 |
| Das ssh-Programm | 298 |

| | |
|---|------------|
| scp – sicheres Kopieren | 299 |
| sftp - sicherere Dateiübertragung | 299 |
| Der SSH Daemon (sshd) – die Serverseite | 300 |
| SSH-Authentifizierungsmechanismen | 301 |
| X-, Authentifizierungs- und sonstige Weiterleitung | 302 |
| Netzwerkauthentifizierung — Kerberos | 303 |
| Kerberos-Terminologie | 304 |
| Wie funktioniert es? | 306 |
| Auswirkungen von Kerberos für den Benutzer | 309 |
| Weitere Informationen über Kerberos | 310 |
| Installation und Administration von Kerberos | 311 |
| Festlegung der Kerberos-Realms | 311 |
| Einrichtung der KDC-Hardware | 311 |
| Zeitsynchronisation | 313 |
| Konfiguration der Protokollfunktion | 313 |
| Installation des KDC | 314 |
| Konfiguration von Kerberos-Clients | 317 |
| Verwaltung von Principals | 320 |
| Aktivierung der PAM-Unterstützung für Kerberos | 321 |
| Einrichtung der Netzwerkserver für Kerberos | 325 |
| Konfiguration von sshd für die Kerberos-Authentifizierung | 326 |
| Benutzung von LDAP und Kerberos | 326 |
| Sicherheit ist Vertrauenssache | 327 |
| Grundlagen | 327 |
| Lokale Sicherheit und Netzwerksicherheit | 328 |
| Tipps und Tricks: Allgemeine Hinweise | 337 |
| Zentrale Meldung von neuen Sicherheitsproblemen | 339 |
| A Manual-Page von e2fsck | 341 |
| B Deutsche Übersetzung der GNU General Public License | 347 |
| Literaturverzeichnis | 359 |

Teil I

System

AutoYaST2: Automatische Installation und Konfiguration

Zur Vereinfachung und Automatisierung der Installation von Linux bietet SuSE das Programm AutoYaST2 an. AutoYaST2 ermöglicht es dem Benutzer, eine Konfiguration für ein zu installierendes System zu erstellen, und führt die Installation automatisch durch, falls die Konfiguration während der Installation bereitgestellt wird.

| | |
|---|----|
| Einführung | 4 |
| Zusammenstellung der Information | 5 |
| Das Control File | 5 |
| Erstellung eines neuen Control Files | 13 |
| Die Quelle der Installationsdaten festlegen | 40 |
| Verwaltung des Bootvorgangs | 43 |
| Starten der automatischen Installation | 54 |
| Systemkonfiguration | 55 |

Einführung

AutoYaST2 kann benutzt werden, um mehrere Systeme mit der gleichen Systemumgebung und ähnlicher Hardware parallel zu installieren. Eine Konfigurationsdatei (das „Control File“) wird anhand von existierenden Konfigurationsressourcen erstellt und kann leicht spezifischen Bedingungen angepasst werden.

Dieses Kapitel führt Sie durch die drei Schritte der automatischen Installation:

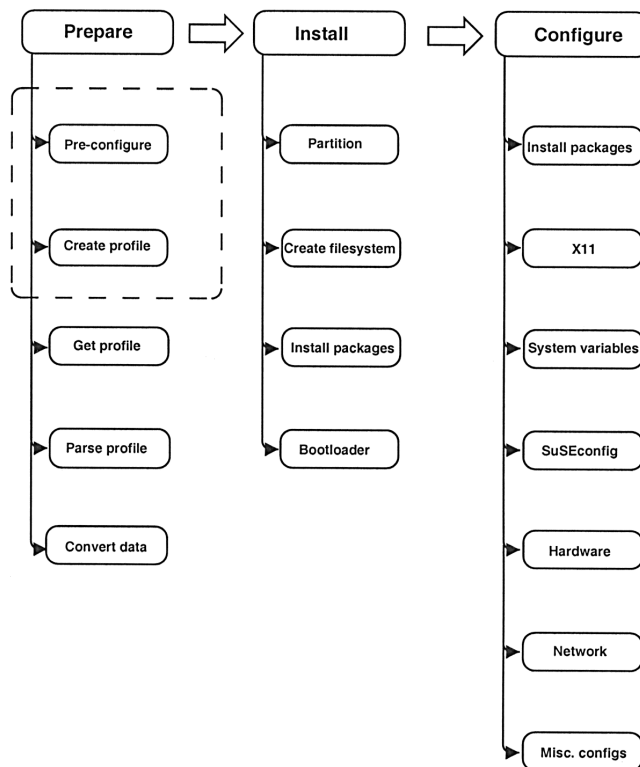


Abbildung 1.1: Die automatische Installation

Vorbereitung Alle wichtige Informationen über das Zielsystem werden zusammengestellt und in entsprechende Direktiven des Control Files über-

setzt. Das Control File wird auf das Zielsystem übertragen und deren Direktiven werden geparkt und in YaST2-konforme Daten umgewandelt.

Installation YaST2 folgt den Anweisungen des Control Files und installiert ein Basissystem.

Konfiguration YaST2 und einige benutzerdefinierte Postinstall-Skripten schließen die Systemkonfiguration ab.

Tipp

Bei der automatischen Installation mit AutoYaST2 wird sich eine gute Kenntnis des YaST2-Installationsvorgangs und grundlegende Kenntnisse von XML als nützlich erweisen. Eine ausführliche Beschreibung der XML-Syntax und zahlreiche Beispiele sind unter `/usr/share/doc/packages/autoyast2` erhältlich.

Tipp

Zusammenstellung der Information

Sie müssen die Information über die zu installierenden Rechner vorab zusammenstellen. Dies betrifft sowohl Hardwaredaten als auch Netzwerkinformationen. Sorgen Sie dafür, dass die folgenden Daten der zu installierenden Rechner zur Verfügung stehen:

- Festplattentypen und -größen
- Grafikkarte und angeschlossener Monitor (falls zutreffend)
- Netzwerkkarte und MAC-Adresse sofern bekannt (was bei der Benutzung von DHCP der Fall ist)

Mit diesen Parametern können Sie nun ein Profil Ihrer Systeme erstellen, um die automatische Installation zu steuern.

Das Control File

Das Control File ist eine hostspezifische Konfigurationsbeschreibung. Es besteht aus einer Reihe von Ressourcen mit den dazugehörigen Eigenschaften die durch

komplex strukturierte Beschreibungen wie Listen, Einträge, Baumstrukturen und große eingebettete oder referenzierte Objekte dargestellt werden.

Das Control File kann man am einfachsten mit einem XML-Editor bearbeiten. Benutzen Sie einen der vielen XML-Editoren oder Ihren bevorzugten Text-Editor mit XML-Unterstützung (z.B. Emacs, Vim). Es ist jedoch nicht zu empfehlen, ein Control File für große Installationen manuell zu erstellen. Stattdessen soll die manuelle Bearbeitung nur als Zugang zum Verständniss des Autoinstallationsmoduls und des Configuration Management Systems (CMS) angesehen werden.

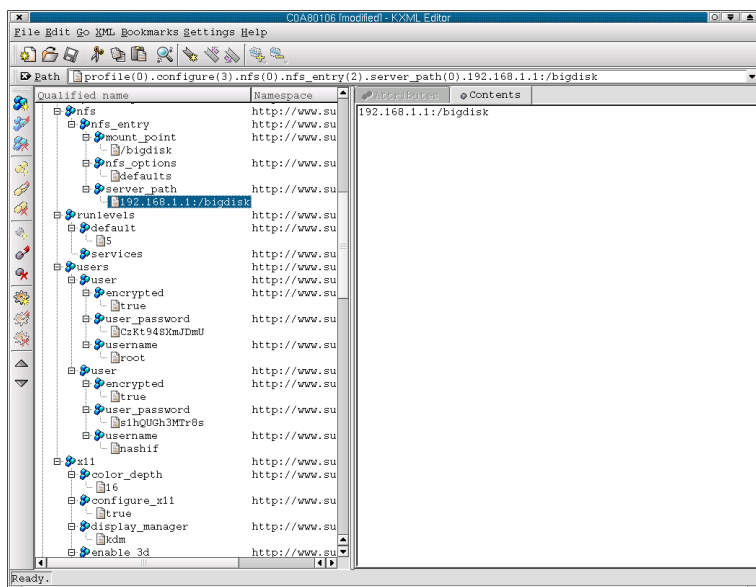


Abbildung 1.2: Bearbeitung des Control Files mit kxmledit

Format

Das XML-Konfigurationsformat bietet eine konsistente Datenstruktur, die leicht erlernbar ist und an die man sich leicht erinnert, wenn man ein neues System konfigurieren möchte. Mit XML erübrigt sich das Parsen und die Fehlerbereinigung des Control Files (fast) vollständig — dies kann durch einen externen XML-Parser erledigt werden (besonders wenn es sich um einen validierenden Parser handelt). Um sicherzustellen, dass das Control File "well-formed" (=

wohlgeformt) und die Syntax "valid" (= gültig) ist, lassen Sie das Control File durch einen validierenden Parser laufen, bevor es für die automatische Installation eingesetzt wird. Dies ist besonders dann wichtig, falls Sie vorziehen, das Profil manuell zu bearbeiten.

Das folgende Beispiel zeigt ein Control File in XML-Format:

```
<?xml version="1.0"?>
<![CDATA[
<!DOCTYPE control_file SYSTEM
"/usr/lib/YaST2/include/control-file.dtd">
<profile
xmlns="http://www.suse.de/1.0/cfns"
xmlns:cfg="http://www.suse.de/1.0/cfgns">
<install>
  <partitioning config:type="list">
    <drive>
      <device>/dev/hda</device>
      <partition>
        <filesystem>ext2</filesystem>
        <size>520Mb</size>
        <mount>/</mount>
      </partition>
      <partition>
        <filesystem>reiser</filesystem>
        <size>1200Mb</size>
        <mount>/data</mount>
      </partition>
    </drive>
  </partitioning>
</install>
<configure>
  <scripts>
    <pre-scripts>
      <script>
        <interpreter>shell</interpreter>
        <filename>start.sh</filename>
        <source>
          <![CDATA[
            #!/bin/sh
            echo "Starting installation"
            exit 0
          ]]>
        </source>
      </script>
    </pre-scripts>
  </scripts>
</configure>
</profile>
</control_file>
]]>
```

```

        </source>
    </script>
</pre-scripts>
</scripts>
</configure>
</profile>
]]>

```

Ausgabe 1: XML Control File (Profil)

Struktur

Das folgende Beispiel zeigt einen grundlegenden Control File Container, dessen eigentlicher Inhalt später in diesem Kapitel erläutert wird.

```

<?xml version="1.0"?>
<!DOCTYPE control_file SYSTEM
    "/usr/lib/YaST2/include/control-file.dtd">
<profile
    xmlns="http://www.suse.de/1.0/cfns"
    xmlns:config="http://www.suse.de/1.0/cfgns">

<!-- RESOURCES -->
</profile>

```

Ausgabe 2: Control File Container

Das Profilelement (Root-Element) enthält ein oder mehrere unterschiedliche Ressourcenelemente. Die zulässigen Ressourcenelemente werden in der DTD spezifiziert.

Das Root-Element im Control File kann beispielsweise die folgenden Subvariablen enthalten:

Installation (*<install>*-Tag)

- Lilo-Konfiguration: Lilo-Gerät, Lilo-Typ (*<bootloader>*-Tag)
- Partitionierung: Übersicht über Laufwerke und Partitionen (*<partitioning>*-Tag)

- Allgemein: Installationshinweise, einschl. aller Client-bezogenen Variablen wie Display, Sprachen, Tastatur usw. (*<general>*-Tag)

Netzwerk Netzwerkkonfiguration für den Client und die Server, die für den Zielclient Dienste bereitstellen (*<networking>*-Tag)

Benutzer Benutzeradministration, einschl. erstem Benutzer und Root (Tag *<users>*)

Benutzerskripten: Vorkonfiguration (*<pre-scripts>*-Tag)

Benutzerskripten: Nachkonfiguration (*<post-scripts>*-Tag)

Ressourcen und Eigenschaften

Ein Ressourcenelement kann entweder mehrere unterschiedliche Eigenschafts- und Ressourcenelemente oder mehrere Instanzen des gleichen Ressourcenelements enthalten oder leer sein. Der zulässige Inhalt eines Ressourcenelements wird in der DTD spezifiziert.

Ein Eigenschaftselement kann entweder leer sein oder einen buchstäblichen Wert enthalten. Die zulässigen Eigenschaftselemente und -werte in jedem Ressourcenelement sind in der DTD spezifiziert.

Ein Element kann entweder ein Container sein, der andere Elemente enthält (eine Ressource) oder einen buchstäblichen Wert (ein Eigenschaft) enthalten, niemals beides zugleich. Diese Beschränkung ist in der DTD spezifiziert. Eine Konfigurationskomponente mit mehr als einem Wert muss entweder als eine eingebettete Liste in einem Eigenschaftswert oder als verschachtelte Ressource dargestellt werden.

Verschachtelte Ressourcen

Verschachtelte Ressourcenelemente ermöglichen den Aufbau einer baumartigen Struktur von Konfigurationselementen.

```
...
<drive>
  <device>/dev/hda</device>
  <partitions>
    <partition>
      <size>1000</size>
      <mount>/</mount>
    </partition>
    <partition>
      <size>250</size>
```

```

        <mount>/tmp</mount>
    </partition>
</partitions>
</drive>
....

```

Ausgabe 3: Verschachtelte Ressourcen

Im obigen Beispiel besteht die Plattenressource aus einer Geräteeigenschaft und einer Partitionsressource. Die Partitionsressource enthält mehrere Instanzen der Partitionsressource. Jede Partitionsressource enthält eine Size-Eigenschaft (Größe) und eine Mount-Eigenschaft (Einbindung ins Dateisystem).

Obwohl in der DTD spezifiziert ist, dass die Partitionsressourcen mehrere Instanzen enthalten, muss dies trotzdem angegeben werden, um die Zuweisung verkehrter Datentypen zu vermeiden. Nehmen wir bei dem obigen Beispiel an, wir hätten ein Laufwerk mit nur einer Partition. Dies würde zur Folge haben, dass die Partitionsressource als Eigenschaft interpretiert wird. Um dies zu vermeiden, muss die folgende Syntax benutzt werden, wenn mehrere Instanzen definiert werden. Weitere Informationen über die Typattribute werden im folgenden Abschnitt behandelt.

```

...
<drive>
  <device>/dev/hda</device>
  <partitions config:type="list">
    <partition>
      <size>1000</size>
      <mount>/</mount>
    </partition>
    <partition>
      <size>250</size>
      <mount>/tmp</mount>
    </partition>
  </partitions>
</drive>
....

```

Ausgabe 4: Verschachtelte Ressourcen mit Typattributen

Attribute

Globale Profilattribute werden benutzt, um Metadaten auf Ressourcen und Eigenschaften zu definieren. Attribute werden benutzt, um Zeitstempel, Zugangskontrolle, dynamische Werte und Kontextwechsel zu definieren. Sie werden

auch benutzt, um Eigenschaften Namen und Typen zuzuweisen, wie in den obigen Abschnitten gezeigt.

Tipp

Profilattribute befinden sich in einem getrennten Namensraum und brauchen nicht als reservierte Wörter im Default-Namensraum behandelt werden. Neue Attribute können hinzugefügt werden, ohne existierende Profile wesentlich zu verändern.

Tipp

Profilattribute sind im Konfigurations-Namensraum definiert und müssen immer mit dem Präfix `config:` versehen werden. Alle Profilattribute sind optional. Die meisten können sowohl mit Ressourcen- als auch mit Eigenschaftselementen benutzt werden. Manche können allerdings nur mit dem Elementtyp benutzt werden, der in der DTD festgelegt ist.

Es gibt keine Einschränkungen für die Reihenfolge der Attribute, und die Reihenfolge ist nicht von Bedeutung.

Attributname Der Name eines Ressourcen- oder Eigenschaftselements wird für die Adressierung und Unterscheidung mehrerer Instanzen des gleichen Elements benutzt. Der Name eines Elements kann mit dem Attribut `config:name` definiert werden. Standardmäßig ist bei einzelnen Instanzelementen der Name mit dem Elementtyp identisch. Standardmäßig ist bei mehreren Instanzelementen ist der Name die Indexpositionsnummer. Ein Element kann nur anhand des

Attributtyps adressiert werden. Der Typ eines Elements wird mit dem Attribut `config:type` definiert. Der Typ eines Ressourcenelements ist immer `RESOURCE`, obgleich dies auch mit Hilfe dieses Attributs explizit definiert werden kann (um die richtige Identifizierung eines leeren Elements zu gewährleisten, z.B. wenn es keine DTD gibt, auf die Bezug genommen werden kann). Ein Ressourcenelement kann kein anderer Typ sein, und diese Beschränkung wird in der DTD spezifiziert. Der Typ eines Eigenschaftselements bestimmt die Auswertung seines buchstäblichen Wertes. Der Typ eines Eigenschaftselements wird standardmäßig auf `STRING` gesetzt, wie in der DTD spezifiziert. Die vollständige Palette der zulässigen Typen ist in der DTD spezifiziert.

Die XML Document Type Definition (DTD)

Einführung

Der Zweck einer DTD ist die Definition von zulässigen Bauteilen eines XML-Dokuments. Sie definiert die Dokumentenstruktur mit einer Liste von zulässi-

gen Elementen. Eine DTD kann innerhalb des XML-Dokuments oder als externe Referenz bestimmt werden.

XML benutzt einen von der Anwendung unabhängigen Ansatz zur Bereitstellung von Daten. Eine Anwendung kann eine Standard-DTD benutzen, um sicherzustellen, dass die vom Benutzer bereitgestellten Daten gültig sind. Ein gültiges XML-Dokument ist ein „well-formed“ XML-Dokument, dass den Regeln einer Document Type Definition (DTD) entspricht.

AutoYaST2 verfügt über eine DTD, die es Benutzern ermöglicht, die Control Files zu validieren, bevor der Installationsprozess gestartet wird. Die DTD kann auch im Zusammenhang mit XML-Editoren benutzt werden, während das Control File editiert wird, um zu vermeiden, dass sich Fehler einschleichen.

Eine Beispiel-DTD

- Eine *<drive>*-Ressource, die eine *<device>*-Eigenschaft und eine als verschachtelte Ressource dargestellte *<partitions>*-Eigenschaft enthält.
- Eine *<partitions>*-Ressource, die mehrere Instanzen der als verschachtelte Ressource dargestellten *<partition>*-Eigenschaft enthält.
- Eine *<partition>*-Ressource, die eine *<size>*-Eigenschaft und eine *<mount>*-Eigenschaft enthält.

Im Folgenden sehen Sie ein XML-Beispiel für ein Profil, das den oben beschriebenen Baum abbildet. Es enthält die DTD, die notwendig ist, um es zu validieren.

```
<?xml version="1.0"?>
<!DOCTYPE profile [
<!ELEMENT profile (install)>
<!ELEMENT install (partitioning)>
<!ELEMENT install (drive+)>
<!ELEMENT drive (name,partitions)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT partitions (partition*)>
<!ELEMENT partition (size,mount)>
<!ELEMENT size (#PCDATA)>
<!ELEMENT mount (#PCDATA)>
]>
<profile>
.....
  <install>
    <partitioning config:type="list">
      <drive>
        <device>
```

```
        /dev/hda
    </device>
    <partitions>
        <partition>
            <size>1000mb</size>
            <mount>/</mount>
        </partition>
        <partition>
            <size>250mb</size>
            <mount>/tmp</mount>
        </partition>
    </partitions>
</drive>
</partitioning>
</install>
.....
</profile>
```

Ausgabe 5: Eine Beispiel-DTD

Erstellung eines neuen Control Files

Um ein Control File zu erstellen, können Sie entweder das Configuration Management System, das die meisten Eigenschaften des Autoinstallationssystems abdeckt, oder einen Editor Ihrer Wahl benutzen. In manchen Fällen mag es notwendig sein, einige Informationen manuell hinzuzufügen, nachdem das Control File mit dem Configuration Management System erstellt wurde.

Sorgen Sie dafür, dass das Configuration Management System (Paket `autoyast2`) installiert ist und rufen Sie es vom YaST2-Kontrollzentrum aus. Sie können es auch als `root` mit dem Befehl `/sbin/yast2 autoyast` direkt starten (die `DISPLAY`-Variable muss korrekt gesetzt sein, um die grafische Oberfläche und nicht die textbasierte Oberfläche zu starten).

Benutzung des Configuration Management Systems

Das Control File für ein bestimmtes System kann mit Hilfe eines YaST2-basierten Systems erstellt werden. Dieses System greift auf die installierten YaST2 Module zurück. Das Configuration Management System ermöglicht Ihnen, Control Files zu erstellen und kann außerdem zur Verwaltung von Konfigurationen mehrerer Clients benutzt werden.

Bis auf wenige Ausnahmen können die Ressourcen des Control Files mit Hilfe des Configuration Management Systems konfiguriert werden. Dieses System

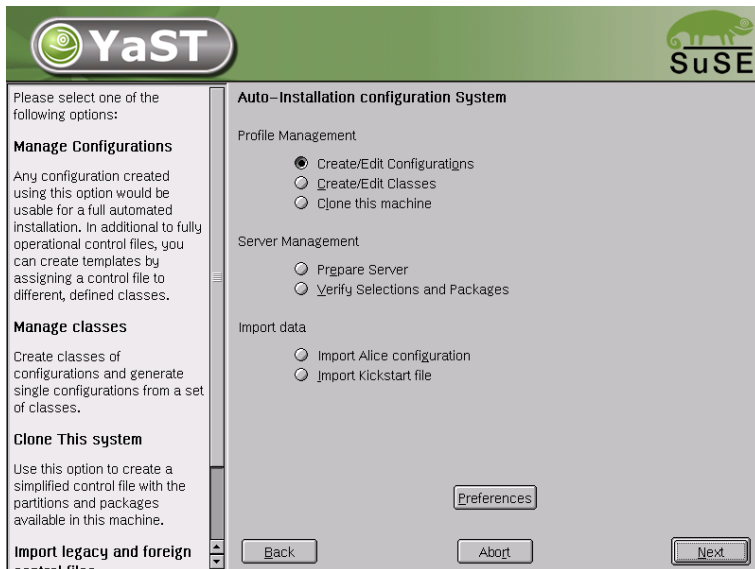


Abbildung 1.3: Das Configuration Management System

ist sehr flexibel. Viele der Ressourcen werden mit den gleichen YaST2-Modulen konfiguriert wie bei der normalen Systemkonfiguration. Für spezielle und komplexe Konfigurationsressourcen wurden neue Interfaces wie `Partitioning` and `General Options` erstellt, um den Zugang zur Information zu erleichtern.

Bei Benutzung des Configuration Management Systems kann man sicher sein, dass das generierte Control File gültig ist und unmittelbar benutzt werden kann, um eine automatisierte Installation zu starten.

Schritt für Schritt durch das Configuration Management System

Um eine neue Konfiguration zu erstellen, wählen Sie die entsprechende Option aus dem Hauptmenü des Configuration Management Systems. Dies öffnet das Menü 'File Management', in dem Sie eine neue Konfiguration starten oder eine existierende Konfiguration ändern können. Die Dateien, die standardmäßig angezeigt werden, sind vollständige Konfigurationen, die ohne Änderungen für die automatische Installation benutzt werden könne. Diese Dateien werden im Hauptkonfigurationsrepository gespeichert. Falls Sie Klassen benutzen, um Ihre Konfiguration zu erstellen, wechseln Sie bitte in die Ansicht 'Templates'

(Vorlagen werden im Verzeichnis `templates` unterhalb des Konfigurationsrepositoriums gespeichert).

Um mit der Konfiguration zu starten, wählen Sie eine existierende Datei mit 'Edit' oder generieren Sie eine neue Konfiguration mit 'New'. Wenn Sie 'New' auswählen werden Sie in einem Dialog nach dem Namen der neuen Datei gefragt. Dies führt direkt zu den Konfigurationsoptionen, die in beliebiger Reihenfolge bearbeitet werden können. Sie brauchen nur genau die Ressourcen zu konfigurieren, die Sie benötigen.

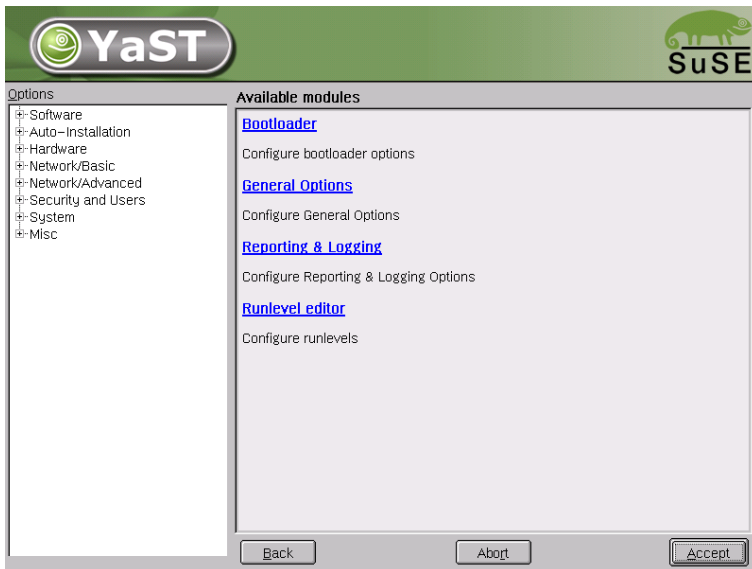


Abbildung 1.4: Konfigurationsoptionen

Klicken Sie auf eine Konfigurationsoption, um eine Zusammenfassung der aktuellen Konfiguration zu sehen. Eine Konfigurationsressource kann jederzeit auf den default Wert zurückgesetzt werden. Klicken Sie auf 'Configure', um eine Ressource zu konfigurieren.

Benutzung von Klassen

Das Configuration Management System kann zur Definition von neuen Klassen benutzt werden. Die Klassendefinition besteht aus den folgenden Variablen für jede Klasse:

- Name: Name der Klasse

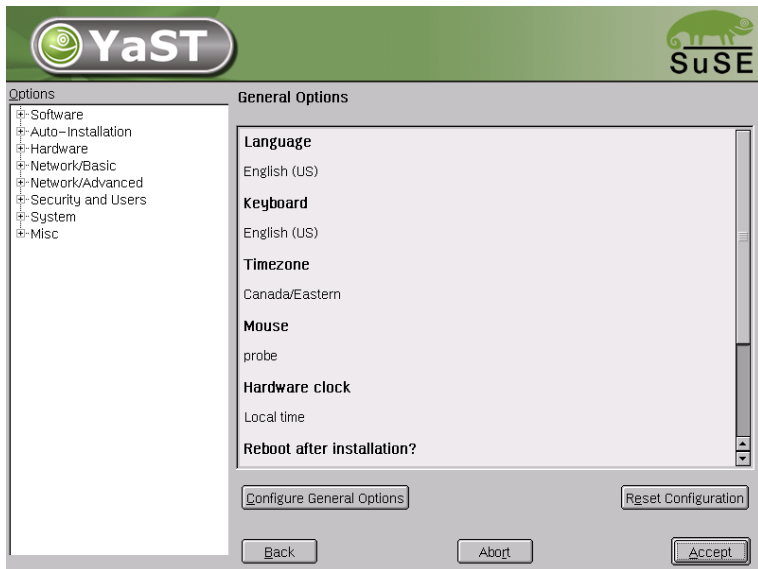


Abbildung 1.5: General Options

- Descriptions: Beschreibung der Klasse
- Order: Reihenfolge (oder Priorität) der Klasse im Migrationsstapel

Generieren Sie so viele Klassen, wie Sie benötigen. Es ist jedoch zu empfehlen, die Anzahl der Klassen möglichst klein zu halten, um die Übersichtlichkeit im Configuration Management System zu wahren. Beispielsweise könnte man die folgende Gruppe von Klassen zu benutzen:

- site: Klasse, die eine physische Stelle oder einen Standort der Rechner beschreiben.
- machine: Klasse, die einen Rechnertyp oder Hersteller beschreiben.
- role: Klasse, die die Funktion des zu installierenden Rechners beschreiben.
- group: Klasse, die eine Abteilung/Gruppe an einer Stelle oder an einem Standort beschreiben.

Eine Datei, die in einer Klasse definiert wird, kann die gleiche Syntax und das gleiche Format haben, wie die XML-Datei, die das Hauptprofil enthält, und

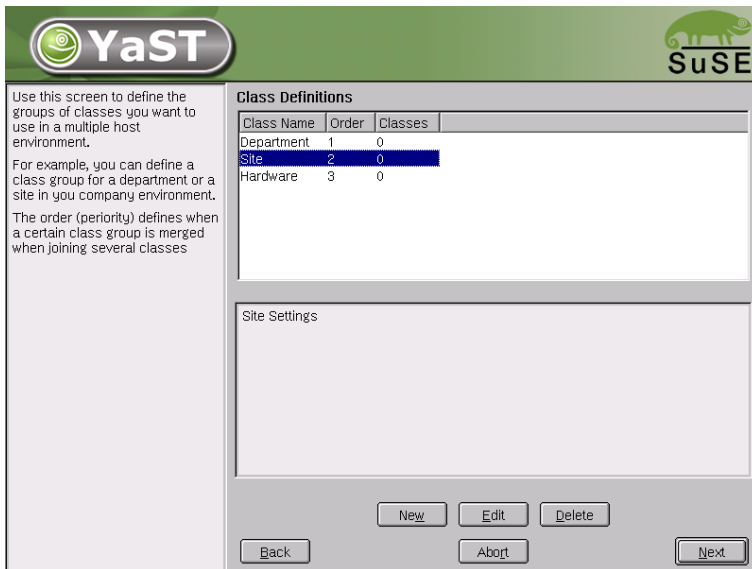


Abbildung 1.6: Definition von Klassen

stellt eine Untergruppe der Konfiguration dar. Um beispielsweise ein neues Profil für einen besonderen Rechner mit einer spezifischen Netzwerkkarte zu erstellen, wird nur die Ressource im Profil gebraucht, die für die Konfiguration des Netzwerkes zuständig ist. Bei verschiedenen Netzwerktypen können Sie den Typ, der für eine bestimmte Hardware gebraucht wird, mit anderen Klassendateien zusammenführen, um ein neues Control File zu erstellen, das den definierten Klassen entspricht.

Benutzung von Vorlagen

Vorlagen (Templates) sind Control Files, die keinen vollständigen Inhalt haben und einer oder mehreren Klassen angehören. Um eine Vorlage installierbar zu machen, muss sie einen Prozess durchlaufen, der alle benötigten Werte gemäß den Daten setzt, die in den Konfigurationen der Klassen vorhanden sind.

Wenn Sie mit Hilfe des Configuration Management Systems im Control File Klassen definieren, wird die Datei nicht im Repository, sondern im Verzeichnis `templates` des Repositories gespeichert.

Manuelle Erstellung und Bearbeitung eines Control Files

Wenn Sie das Control File manuell bearbeiten, achten Sie bitte darauf, dass die Syntax in Ordnung ist. Der SuSE Linux Enterprise Server enthält einige Tools zur Überprüfung der Syntax. Um zum Beispiel zu überprüfen, ob die Datei „well-formed“ ist, können Sie die Utility `xmllint` benutzen, welches im Paket `libxml2` enthalten ist (`xmllint <control file>`).

Falls das Control File nicht „well-formed“ ist (z.B. falls ein Tag nicht geschlossen ist), wird `xmllint` die Fehler berichten. Bevor Sie mit der automatischen Installation fortfahren, korrigieren Sie bitte die Fehler, die bei der Überprüfung gefunden werden. Die automatische Installation kann mit ungültigen Control Files nicht durchgeführt werden.

Profilressourcen unter der Lupe

Dieser Abschnitt behandelt die wichtigsten Teile eines Control Files für Standardzwecke. Für Information über andere verfügbaren Optionen sehen Sie bitte in der XML-Dokumentation nach und benutzen Sie das Configuration Management System.

Allgemeine Optionen

Der Abschnitt `general` ist ein Abschnitt des Profils, der alle Einstellungen enthält, die im Zusammenhang mit dem Installationsprozess und der Umgebung des installierten Systems stehen. Dieser Abschnitt ist zwingend erforderlich. Die Ressourcen enthalten die folgenden vier Eigenschaften, die für alle Installationen benötigt werden: `language` (Sprache), `keyboard` (Tastatur), `time zone` (Zeitzone) und `mouse` (Maus). Falls dieser Abschnitt nicht konfiguriert wird, werden Standardwerte benutzt, die mit dem zu installierenden System vermutlich nicht kompatibel sind.

```
<install>
...
  <general>
    <language>de_DE</language>
    <keyboard>
      <keymap>german</keymap>
      <rate>24</rate>
      <delay>24</delay>
      <numlock>on</numlock> <!-- on|off|bios -->
      <scrolllock>on</scrolllock> <!-- on|off -->
      <capslock>on</capslock> <!-- on|off|disables -->
    </keyboard>
```

```
<clock>
  <timezone>US/Eastern</timezone>
  <utc config:type="boolean">true</utc>
  <ntp_servers config:type="list">
    <ntp_server>ntp.example.com</ntp_server>
  </ntp_servers>
</clock>
<mouse>
  <id>ps0</id>
  <device>/dev/psaux</device>
  <gpm>
    <protocol>ps2</protocol>
    <parameters></parameters>
  </gpm>
  <wheels config:type="integer">1</wheels>
  <buttons config:type="integer">1</buttons>
  <xemu3 config:type="boolean">true</xemu3>
</mouse>
<mode>
  <installation config:type="boolean">true</installation>
  <upgrade config:type="boolean">false</upgrade>
  <confirm config:type="boolean">false</confirm>
  <interactive_boot config:type="boolean">false</interactive_boot>
  <reboot config:type="boolean">false</reboot>
</mode>

</general>
...
</install>
```

Ausgabe 6: Allgemeine Optionen

Die Eigenschaft `reboot` in der Ressource `mode` wird gebraucht, um nach der ersten Systemeinrichtung und vor dem ersten Systemstart einen Neustart zu erzwingen.

Standardmäßig muss der automatische Installationsprozess vom Benutzer bestätigt werden. Die Bestätigung sollte deaktiviert werden, falls eine vollständig unbeaufsichtigte Installation erwünscht ist. Diese Option wird benötigt, um die Einstellungen auf einem Zielsystem zu steuern, bevor irgendwelche Änderungen vorgenommen werden, und kann zum Debuggen benutzt werden. Standardmäßig wird der Wert auf `true` gesetzt, um eine rekursive Installation zu vermeiden, wenn das System aufgrund eines Kernelwechsels neu startet oder wenn das Control File einen Neustart erfordert.

Meldungen

Die Ressource `report` verwaltet drei Arten von Pop-Up-Meldungen, die während der Installation angezeigt werden können.

- Pop-Up-Meldungen (überwiegend nichtkritische, informative Meldungen)
- Warnmeldungen (falls etwas schiefgehen könnte)
- Fehlermeldungen (wenn ein Fehler geschieht)

```
<install>
...
  <report>
    <messages>
      <show>true</show>
      <timeout>10</timeout>
      <log>true</log>
    </messages>
    <errors>
      <show>true</show>
      <timeout>10</timeout>
      <log>true</log>
    </errors>
    <warnings>
      <show>true</show>
      <timeout>10</timeout>
      <log>true</log>
    </warnings>
  </report>
...
</install>
```

Ausgabe 7: Meldungsverhalten

Je nach Ihrer Erfahrung können Sie diese Meldungen übergehen, protokollieren und anzeigen lassen (mit Timeout). Es ist empfehlenswert, alle Meldungen mit Timeout anzeigen zu lassen. Einige Warnmeldungen können übergangen werden, sollten jedoch nicht ignoriert werden. Die Standardeinstellung im automatischen Installationsmodus ist die Anzeige aller Meldungen ohne Protokollierung und mit einem Timeout von 10 Sekunden.

Hinweis

Kritische Systemmeldungen

Nicht alle Meldungen während der Installation werden von der `Resource report` gesteuert. Einige kritische Meldungen bezüglich der Paketinstallation und der Partitionierung werden auch ungeachtet Ihrer Einstellungen im Abschnitt `report` angezeigt.

Hinweis

Der Bootloader

Falls Sie keinen Bootloader installieren möchten, können Sie dies mit der Eigenschaft `write_bootloader` spezifizieren (Boolscher Wert). Wenn kein Bootloader installiert wird, sollten Sie eine Startdiskette oder eine andere Möglichkeit haben, um Ihr System zu starten (zum Beispiel einen externen Bootloader). Standardmäßig wird der Bootloader installiert.

Falls Sie einen Bootloader installieren möchten, müssen Sie bestimmen, wo er installiert werden soll (im MBR oder im ersten Sektor der Partition `/boot`). Installieren Sie den Bootloader im MBR, falls Sie ihn als Ihren Bootloader verwenden möchten. Wenn Sie einen anderen Bootloader verwenden, installieren Sie Linux im ersten Sektor der Partition `/boot` und konfigurieren Sie den anderen Bootloader so, dass er SuSE Linux Desktop startet.

Falls der Kernel für den Systemstart irgendwelche speziellen Parameter benötigt, können Sie diese unter dem Tag `Kernelparameter` eingeben. Außerdem können Sie zwischen dem `linearen` Modus und der erzwungenen Verwendung des `lba32`-Modus wählen.

Partitionierung

Automatische Partitionierung Die Durchführung der automatischen Partitionierung erfordert lediglich die Angabe der Größen und Mount-Punkte der Partitionen. Allen anderen Daten, die für eine erfolgreiche Partitionierung erforderlich sind, können automatisch berechnet werden.

Falls keine Partitionen definiert werden und das spezifizierte Laufwerk das Laufwerk ist, in dem die Root-Partition sich befinden soll, werden die folgenden Partitionen automatisch angelegt:

/boot Die Größe von `/boot` ist abhängig von der Architektur des Zielsystems.

swap Die Größe der swap-Partitionen ist davon abhängig, wieviel Speicher auf dem System verfügbar ist.

/ (Root-Partition) Die Größe von / (Root-Partition) ist der Platz, der nach der Erstellung von swap und /boot noch verfügbar ist.

Je nachdem, wie der anfängliche Status des Laufwerks ist und wie es vorher partitioniert war, können die default-Partitionen wie folgt angelegt werden:

Use free space Falls das Laufwerk bereits partitioniert ist, können die neuen Partitionen in dem freien Platz auf dem Laufwerk angelegt werden. Dies ist nur möglich, wenn für alle ausgewählten Pakete und swap genügend Platz vorhanden ist.

'Reuse all available space' Diese Option führt zur Löschung aller vorhandenen Partitionen.

'Reuse all available Linux partitions' Diese Option führt zur Löschung der vorhandenen Linux-Partitionen. Alle anderen Partitionen (z.B. Windows-Partitionen) werden beibehalten.

'Reuse only specified partitions' Diese Option führt zur Löschung der angegebenen Partitionen. Die Auswahl der zu löschenden Partitionen sollte von der letzten verfügbaren Partition an beginnen.

Falls das Zielsystem mehrere Laufwerke hat, sollten alle Laufwerke anhand ihrer Gerätebezeichnungen und zusätzlicher Informationen im Zusammenhang mit dem oben genannten Verhalten identifiziert werden.

Partitionsgrößen können in Gigabyte oder Megabyte angegeben werden oder mit den Variablen `auto` und `max` als flexible Werte gesetzt werden. `max` wird benutzt, um eine Partition anzulegen, die den gesamten freien Platz auf einem Laufwerk ausfüllt. Dies bedeutet, dass die Partition die letzte auf dem Laufwerk ist. `auto` kann benutzt werden, um die Größe der swap- oder boot-Partitionen in Abhängigkeit des Speichers und des Systemtyps zu ermitteln.

Um eine feste Größe zu bestimmen, benutzen Sie bitte das Format der folgenden Beispiele. `1gb` legt eine Partition von 1 GB an, `1500mb` legt eine Partition von 1,5 GB an.

Logical Volume Manager (LVM) Um LVM zu konfigurieren, muss zunächst ein Physical Volume mit der normalen, oben beschriebenen Partitionierungsmethode angelegt werden.

Das folgende Beispiel zeigt, wie man die Ressource `partitioning` für LVM vorbereiten kann:


```
....  
<partitioning config:type="list">  
  <drive>  
    <device>/dev/sda</device>  
    <use>all</use>  
    <partitions config:type="list">  
      <partition>  
        <size>auto</size>  
        <lvm_group>system</lvm_group>  
      </partition>  
    </partitions>  
  </drive>  
</partitioning>  
.....
```

Aufgabe 8: Anlegen von LVM Physical Volumes

Das letzte Beispiel legt auf dem Gerät `/dev/sda1` eine unformatierte Partition vom Typ LVM mit der Volume Group `system` an. Die angelegte Partition wird den gesamten verfügbaren Platz auf diesem Laufwerk benutzen.

Die Logical Volumes sollten in der Ressource `lvm` definiert werden. Zur Zeit ist es nicht möglich, LVM mit dem Configuration Management System zu konfigurieren. Stattdessen muss die Ressource manuell hinzugefügt werden, wie in dem folgenden Beispiel beschrieben.

```
....  
<lvm config:type="list">  
  <lvm_group>  
    <lvm_name>system</lvm_name>  
    <pesize>4M</pesize>  
    <logical_volumes config:type="list">  
      <lv>  
        <lv_name>usr</lv_name>  
        <lv_size>500mb</lv_size>  
        <lv_fs>reiser</lv_fs>  
        <lv_mount>/usr</lv_mount>  
      </lv>  
    </logical_volumes>  
  </lvm_group>  
</lvm>
```

```

    <lv_name>optlv</lv_name>
    <lv_size>1500mb</lv_size>
    <lv_fs>reiser</lv_fs>
    <lv_mount>/opt</lv_mount>
</lv>
<lv>
    <lv_name>varlv</lv_name>
    <lv_size>200mb</lv_size>
    <lv_fs>reiser</lv_fs>
    <lv_mount>/var</lv_mount>
</lv>
</logical_volumes>
</lvm_group>
</lvm>
...

```

Ausgabe 9: LVM Logical Volumes

Software RAID

AutoYaST2 ermöglicht die Konfiguration von Software RAID Geräten. Die folgenden RAID-Levels werden unterstützt:

RAID 0 Dieses Level verbessert die Leistung Ihrer Festplatte. In diesem Modus gibt es *keine* Redundanz. Falls eines der Laufwerke abstürzen sollte, ist keine Wiederherstellung der Daten möglich.

RAID 1 Dieser Modus hat die beste Redundanz. Er kann mit zwei oder mehr Festplatten benutzt werden. Dieser Modus speichert eine genaue Kopie aller Daten auf allen Laufwerken. Datenverluste sind ausgeschlossen, solange noch mindestens ein Laufwerk funktioniert. Die Partitionen, die für diese Art RAID benutzt werden, sollten ungefähr gleich groß sein.

RAID 5 Dieser Modus integriert die Verwaltung einer größeren Anzahl von Festplatten und bietet in beschränktem Umfang Redundanz. Falls eine Festplatte ausfällt, sind alle Daten noch vorhanden. Falls zwei Festplatten gleichzeitig ausfallen, sind alle Daten verloren.

Multipath Dieser Modus ermöglicht den Zugang zum gleichen physikalischen Gerät über mehrere Controller, um Redundanz gegen Störungen in der Controller-Karte zu gewährleisten. Dieser Modus kann mit mindestens zwei Geräten benutzt werden.

Ähnlich wie bei LVM müssen Sie auch bei RAID zunächst die RAID-Partitionen anlegen und die Partitionen dem RAID-Gerät zuweisen, dass Sie anlegen möchten. Außerdem müssen Sie spezifizieren, ob eine Partition oder ein Gerät im RAID oder als Ersatzgerät konfiguriert werden soll.

Das folgende Beispiel zeigt eine einfache RAID 1 Konfiguration:

```
....
  <partitioning config:type="list">
    <drive>
      <device>/dev/hdc</device>
      <partitions config:type="list">
        <partition>
          <filesystem_id config:type="integer">253</filesystem_id>
          <format config:type="boolean">>false</format>
          <raid_name>/dev/md0</raid_name>
          <size>4gb</size>
        </partition>

        <!-- Here come the regular parti-
ons, i.e. / and swap -->

      </partitions>
      <use>all</use>
    </drive>
    <drive>
      <device>/dev/sda</device>
      <use>all</use>
      <partitions config:type="list">
        <partition>
          <filesystem_id config:type="integer">253</filesystem_id>
          <format config:type="boolean">>false</format>
          <raid_name>/dev/md0</raid_name>
          <raid_type>raid</raid_type>
          <size>4gb</size>
        </partition>
      </partitions>
    </drive>
  </partitioning>

  <raid config:type="list">
    <device>
      <raid config:type="integer">md0</raid>
      <parity_algorithm>left-asymmetric</parity_algorithm>
      <persistent_superblock>true</persistent_superblock>
```

```

        <raid_type>raid1</raid_type>
        <filesystem_id config:type="integer">131</filesystem_id>
        <chunk_size config:type="integer">4</chunk_size>
    </device>
</raid>
....

```

Ausgabe 10: Beispielskonfiguration für RAID 1

Software

Paketselektionen Sie haben die Wahl zwischen drei Arten von Paketselektionen:

- Vordefinierte Paketselektionen wie `default`, `development` oder `default+office` und mehrere Add-on-Selektionen.
- Benutzerdefinierte Auswahl von Paketen — Paketauswahl in einem existierenden System mit dem `rpm`-Befehl oder ähnlichen Tools.
- Zusätzliche lokale Pakete (nicht-SuSE-Pakete) und Pakete, die für die Einrichtung und Konfiguration des Systems benötigt werden.

Im Control File werden Pakete und Paketauswahlen wie folgt beschrieben:

```

....
<software>
  <base>Minimal</base>
  <addons config:type="list">
    <addon>Kde</addon>
  </addons>
  <packages config:type="list">
    <package>apache</package>
    <package>sendmail</package>
  </packages>
</software>
....

```

Ausgabe 11: Softwareauswahl in der Control File

Eine Liste der verfügbaren vordefinierten Selektionen ist auf der ersten CD-ROM im Verzeichnis `/suse/setup/descr` erhältlich. Sie können auch eine der Grundselektionen und eine oder mehrere zusätzliche Selektionen installieren.

Benutzerdefinierte Paketselektionen Zusätzlich zu den vordefinierten Selektionen können Sie benutzerdefinierte Selektionen erstellen, indem Sie im Selektionsverzeichnis eine benutzerdefinierte Selektionsdatei bereitstellen. Die Selektionsdateien haben ein spezielles Format, welches auch für zusätzliche Selektionsdateien benutzt werden muss, da Yast2 sonst nicht in der Lage sein wird, sie zu lesen.

Mehr Information über die Selektionsdatei ist in der Dokumentation der des Paketes `yast2-package-manager-devel` erhältlich.

Nachdem eine Selektionsdatei erstellt wurde, fügen Sie sie der Konfiguration hinzu, wie oben beschrieben.

```
....
<software>
  <base>My</base>

</software>
....
```

Ausgabe 12: Benutzerdefinierte Softwareauswahl

Die Datei `My.sel` sollte das folgende Format haben:

```
# SuSE-Linux-Package-Selection 3.0 -- (c) 2002 SuSE Linux AG
# generated on Sat Aug 10 17:55:42 UTC 2002

=Ver: 3.0

# name version release
=Sel: Kde-Desktop <version>

# size in bytes (pkgsize instsize)
=Siz: 123456 1234567

# Summary
...
=Sum.de: KDE Desktop-Umgebung
=Sum.en: KDE Desktop Environment
=Sum.es: Entorno Grafico KDE
=Sum.fr: Environnement de bureau KDE
=Sum.gl: KDE Desktop Environment
=Sum.hu: KDE grafikus munkakrnyezet
```

```

=Sum.it: Ambiente Desktop KDE
=Sum.tr: KDE Desktop Environment
...

# selections required for installation
=Req: X11 Basis-Sound
# conflicting selections
=Con: Minimal
# category, add-on or base
=Cat: addon

# visibility of selection (for user interface)
=Vis: true

# list of packages to install
+Ins:
SDL
aalib
alsa

...
smpppd
unixODBC
wvdial
-In:

# list of packages to install if given language is active

+Ins.cs:
kde3-i18n-cs
-In.cs:

+Ins.da:
kde3-i18n-da
-In.da:

+Ins.de:
kde3-i18n-de
-In.de:

...

```

Ausgabe 13: Paketselektionsdatei

Installation zusätzlicher und angepasster Pakete Außer den auf den CDs vorhandenen Paketen können Sie auch Fremdpakete und Fremdkernel installieren. Angepasste Kernelpakete müssen mit den SuSE-Paketen kompatibel sein und die Kerneldateien an den gleichen Stellen installieren.

Im Gegensatz zu früheren Versionen erfordert die Installation benutzerdefinierter und externer Pakete keine spezielle Ressource im Control File.

Stattdessen müssen Sie die Paketdatenbank neu generieren und mit etwaigen neuen Paketen oder neuen Paketversionen aus dem Quellrepository aktualisieren.

Für diese Aufgabe wird ein Skript mitgeliefert, welches die im Repository verfügbaren Pakete abfragt und die erforderliche Paketdatenbank erstellt.

Der Vorteil dieser Methode ist, dass Sie auf diese Weise ein aktuelles Repository mit gefixten und aktualisierten Paketen unterhalten können (vom SuSE FTP-Server). Außerdem vereinfacht diese Methode die Erstellung benutzerdefinierter CDs.

Dienste und Runlevels

Die Runlevel-Ressource dient der Festsetzung des Default-Runlevels sowie der Bestimmung der Systemdienste, die in den jeweiligen Runlevels gestartet werden.

Die Eigenschaft `default` spezifiziert den Default-Runlevel des Systems. Änderungen des Default-Runlevels werden beim nächsten Start des Zielsystems wirksam. Nachdem die Installation vollendet ist, hat das System den Runlevel 5, d.h. vollen Multiuserbetrieb mit Netzwerk und `xdm`. Falls Sie ein System ohne X11 konfiguriert haben, ist es empfehlenswert das System nach der ersten Stufe mit der Eigenschaft `reboot` in der Ressource `general` neu zu starten.

Bestimmen Sie die Runlevels, in denen ein Dienst aktiv sein soll, in dem Sie eine durch Leerzeichen getrennte Liste der Runlevel angeben, wie in dem folgenden Beispiel gezeigt wird.

```
<configure>
....
<runlevels>
  <default>3</default>
  <services config:type="list" >

    <service>
      <service_name>at</service_name>
      <service_start>3 5</service_start>
      <service_stop>2 3 5</service_stop>
    </service>
    <service>
      <service_name>portmap</service_name>
      <service_start>3 5</service_start>
      <service_stop>2 3 5</service_stop>
```

```

    </service>
  </services>
</runlevels>
....
</configure>

```

Ausgabe 14: Die Konfiguration der Runlevel

Konfiguration des Netzwerkes

Netzwerkgeräte, DNS und Routing Die Netzwerkkonfiguration wird benötigt, um einen alleinstehenden SuSE Linux Desktop-Arbeitsplatzrechner in ein Ethernet-basiertes LAN einzubinden oder Einwahlverbindungen zu konfigurieren. Kompliziertere Konfigurationen (mehrere Netzwerkkarten, Routing usw.) sind auch möglich. Dieses Modul ermöglicht die Konfiguration von Ethernet-Controllern und Token-Ring-Controllern. Um Netzwerkeinstellungen zu konfigurieren und das Netzwerk automatisch zu aktivieren, wird eine globale Übersicht benutzt, um die gesamte Netzwerkkonfiguration zu speichern.

```

<configure>
....
  <networking>
    <dns>
      <dhcp_hostname config:type="boolean">true</dhcp_hostname>
      <dhcp_resolv config:type="boolean">true</dhcp_resolv>
      <domain>local</domain>
      <hostname>linux</hostname>
    </dns>
    <interfaces config:type="list">
      <interface>
        <bootproto>dhcp</bootproto>
        <device>eth0</device>
        <module>tulip</module>
        <options>options=0</options>
        <startmode>onboot</startmode>
      </interface>
    </interfaces>
    <routing>
      <ip_forwarding config:type="boolean">false</ip_forwarding>
      <routes config:type="list">
        <route>
          <destination>default</destination>
          <device>-</device>
          <gateway>192.168.1.240</gateway>

```



```

        <netmask>--</netmask>
    </route>
</routes>
</routing>
</networking>
....
</configure>

```

Ausgabe 15: Netzwerkkonfiguration

NIS Der Zielrechner kann als NIS-Client aufgesetzt werden. Mehrere Server können mit dem Attribut `list` angegeben werden (`config:type="list"`).

```

<configure>
...
<nis>
  <nis_broadcast config:type="boolean">true</nis_broadcast>
  <nis_broken_server config:type="boolean">true</nis_broken_server>
  <nis_domain>test.com</nis_domain>
  <nis_local_only config:type="boolean">true</nis_local_only>
  <nis_servers config:type="list">
    <nis_server>192.168.1.1</nis_server>
  </nis_servers>
  <start_autofs config:type="boolean">true</start_autofs>
  <start_nis config:type="boolean">true</start_nis>
</nis>
...
</configure>

```

Ausgabe 16: Netzwerkkonfiguration: NIS

NIS+ Falls Sie NIS+ aktivieren, werden die Daten des NIS+ -Servers `/etc/hosts` hinzugefügt. `KeyServ` und der NIS+ Cache Manager werden gestartet und die NSS- und PAM-Konfiguration wird modifiziert, um NIS+ zu benutzen und den geheimen Schlüssel des Benutzers zu setzen.

```

<configure>
...
  <nisplus>
    <start_nisplus>true</start_nisplus>
    <nisplus_domain>Domain</nisplus_domain>
    <nisplus_address>Address</nisplus_address>
  </nisplus>

```

```

        <start_autofs>true</start_autofs>
    </nisplus>
...
</configure>

```

Ausgabe 17: Netzwerkkonfiguration: NIS+

LDAP-Client Der installierte Rechner kann als LDAP-Client aufgesetzt werden, um Benutzer an einem OpenLDAP-Server zu authentifizieren. Erforderliche Daten sind der Name der Search Base (Basis-DN, z.B. `dc=mydomain,dc=com`) und die IP-Adresse des LDAP-Servers (z.B. `10.20.0.2`). Wenn LDAP aktiviert wird, werden NSS und PAM dementsprechend konfiguriert, um LDAP für die Benutzerauthentifizierung zu benutzen.

```

<configure>
...
    <ldap>
        <start_ldapclient>false</start_ldapclient>
        <ldap_domain>domain</ldap_domain>
        <ldap_address>192.168.1.1</ldap_address>
    </ldap>
...
</configure>

```

Ausgabe 18: Netzwerkkonfiguration: LDAP-Client

NFS Die Stapelverarbeitung des NFS-Client-Moduls ist noch nicht verfügbar (`nfs_write` mit Optionen), aber die Routine `nfs_client_save` kann für die automatische Installation und die Konfiguration von `/etc/fstab` benutzt werden.

```

<configure>
...
    <nfs config:type="list">
        <entry>
            <server_path>server:/space</server_path>
            <mount_point>/space</mount_point>
            <options>default</options>
        </entry>
    </nfs config:type="list">

```

```

        </entry>
    </nfs>
...
</configure>

```

Ausgabe 19: Netzwerkkonfiguration: NFS

Mailkonfiguration (Sendmail oder Postfix) Das existierende Modul für die Mailkonfiguration im laufenden System wird für die Mailkonfiguration des Clients benutzt. Dieses Modul ermöglicht sehr komplexe Mailkonfigurationen und sollte der manuellen Bearbeitung der Mail-Ressource vorgezogen werden.

```

<configure>
...
<mail>
  <mta>sendmail</mta>
  <connection_type>permanent</connection_type>
  <local_domains config:type="list"></local_domains>
  <outgoing_mail_server></outgoing_mail_server>
  <from_header ></from_header>
  <masquerade_other_domains config:type="list"></masquerade_other_domains>
  <masquerade_users config:type="list"></masquerade_users>
  <fetchmail config:type="list"></fetchmail>
  <aliases config:type="list"></aliases>
  <merge_aliases></merge_aliases>
  <virtual_users config:type="list"></virtual_users>
</mail>
...
</configure>

```

Ausgabe 20: Mailkonfiguration

Sicherheitseinstellungen

Dieses Modul dient der Konfiguration von lokalen Sicherheitseinstellungen wie der Boot-Konfiguration, Login-Einstellungen, Passwordeinstellungen, einige Einstellungen zum Anlegen von Benutzern und Dateiberechtigungen auf dem Zielsystem.

Die automatische Konfiguration der Sicherheitseinstellungen entspricht dem Menü 'Custom Settings' im Sicherheitsmodul des laufenden Systems, welches Ihnen ermöglicht, eine benutzerdefinierte Konfiguration zu erstellen.

Password Setting Options Dient der Änderung von verschiedenen Passwort-einstellungen. Diese Einstellungen werden hauptsächlich in der Datei `/etc/login.defs` gespeichert.

Benutzen Sie diese Ressource, um eine der encryption-Methoden (Verschlüsselungsmethoden) zu aktivieren, die zur Zeit unterstützt werden. Falls nichts spezifiziert wird, wird DES konfiguriert.

DES, die Standardmethode in Linux, funktioniert in allen Netzwerkkumgebungen, erlaubt jedoch nur Passwörter bis zu einer maximalen Länge von acht Zeichen. MD5 ermöglicht längere Passwörter und ist sicherer, wird jedoch nicht von allen Netzwerkprotokollen unterstützt, was zu Problemen mit NIS führen könnte. Blowfish wird auch unterstützt.

Das System kann so konfiguriert werden, dass die Länge und Sicherheit der Passwörter überprüft wird.

Boot settings Verschieden Boot-Einstellungen können mit der Ressource `security` verändert werden.

- **How to interpret `(Ctrl) + (Alt) + (Del)`** Wenn man an der Konsole die Tastenkombination `(Ctrl) + (Alt) + (Entf)` drückt, führt dies normalerweise zu einem Neustart des Systems. In manchen Fällen mag es wünschenswert sein, diese Kombination zu ignorieren, beispielsweise wenn das System sowohl als Arbeitsplatzrechner als auch als Server benutzt wird.
- **Shutdown behavior of KDM** Hier kann festgelegt werden, wer den Rechner von KDM aus herunterfahren darf.

Login settings Dient der Festlegung verschiedener Einstellungen für die Anmeldung. Diese Einstellungen werden hauptsächlich in der Datei `/etc/login.defs` gespeichert.

New user settings (useradd settings) Hier können Sie die kleinste und größte zulässige Benutzer-ID sowie die kleinste und größte zulässige Gruppen-ID festlegen.

Benutzer

Der Benutzer Root und mindestens ein normaler Benutzer können während der Installation anhand der Daten im Control File angelegt werden. Die Benutzerdaten und Passwörter (verschlüsselt oder Klartext) sind Teil der Ressource `configure` in der Control File.

Während der automatischen Installation sollte zumindest der Benutzer Root angelegt werden, um sicherzustellen, dass Sie sich nach vollendeter Installation

anmelden können, und zu vermeiden, dass sich andere am System anmelden können (falls kein Passwort gesetzt wurde).

Die beiden Benutzer im folgenden Beispiel werden während der Konfiguration des Systems angelegt.

```
<configure>
...
  <users config:type="list">
    <user>
      <username>root</username>
      <user_password>password</user_password>
      <encrypted>true</encrypted>
      <forename/>
      <surname/>
    </user>
    <user>
      <username>nashif</username>
      <user_password>password</user_password>
      <encrypted>true</encrypted>
      <forename>Anas</forename>
      <surname>Nashif</surname>
    </user>
  </users>
...
</configure>
```

Ausgabe 21: User Configuration

Das letzte Beispiel zeigt die minimale Information an, die für das Anlegen von Benutzern benötigt wird. Für eine spezialisiertere Verwaltung der Benutzerkonten sind zusätzliche Optionen verfügbar. Die Daten in `/etc/default/useradd` werden benutzt, um das Homeverzeichnis des Benutzers anzulegen und andere Parameter zu definieren. In der Ressourcenreferenz werden weitere Optionen erläutert.

Benutzerdefinierte Skripten

Durch das Hinzufügen von Skripten zum automatischen Installationsprozess können Sie die Installation Ihren Bedürfnissen anpassen und die verschiedenen Stufen der Installation steuern.

Im automatischen Installationsprozess können drei Arten von Skripten ausgeführt werden:

Preinstall-Skripten Diese Skripten werden ausgeführt, bevor YaST2 irgendwelche Änderungen am System vornimmt (vor der Partitionierung und der Installation der Pakete)

Postinstall-Skripten Diese Skripten werden ausgeführt, nachdem YaST2 die Installation abgeschlossen und das System zum ersten Mal gestartet hat.

Postinstall-Skripten für die Chroot-Umgebung Chroot-Skripten werden in der chroot-Umgebung ausgeführt, bevor YaST2 zum ersten Mal bootet und der Bootloader installiert wird.

Alle Skripten außer den Preinstall-Skripten können in der Shell-Sprache oder in der Perl-Skriptsprache geschrieben werden. Wenn diese dem control File manuell hinzugefügt werden, müssen die Skripten in ein CDATA-Element eingebunden werden, um eine Verwechslung mit der Dateisyntax und anderen Tags zu vermeiden, die in der Control File definiert werden.

Weitere Optionen werden in der Ressourcenreferenz erläutert.

```
<post-scripts config:type="list" >
  <script>
    <filename>post.sh</filename>
    <interpreter>shell</interpreter>
    <source>
]]>
<![CDATA[
#!/bin/sh
echo "Do something useful"

]]>
<![CDATA[
    </source>
  </script>
</post-scripts>
```

Ausgabe 22: Konfiguration von Postinstall-Skripten

Nachdem die Installation abgeschlossen ist, befinden sich die Skripten und Ausgabeprotokolle im Verzeichnis `/var/adm/autoinstall`. Die Skripten befinden sich im Verzeichnis `scripts` und die Ausgangsprotokolle der Skripten im Verzeichnis `log`.

Das Protokoll ist die Ausgabe, die generiert wird, wenn die Shell-Skripten mit dem folgenden Befehl ausgeführt werden:

```
/bin/sh -x <script_name> 2&> /var/adm/autoinstall/logs/<script_name>.log
```

Systemvariablen (sysconfig)

Die Ressource `sysconfig` wird benutzt, um Konfigurationsvariablen direkt im `sysconfig-Repository (/etc/sysconfig)` zu definieren. Mit den `sysconfig`-Variablen können viele Systemkomponenten und Umgebungsvariablen genau auf Ihre Bedürfnisse abgestimmt werden.

Das Administrationshandbuch behandelt viele weitere Einzelheiten über die verschiedenen Konfigurationsoptionen in `/etc/sysconfig`.

Das folgende Beispiel zeigt, wie eine Variable mit der Ressource `sysconfig` festgelegt werden kann. Um eine Variable in einer `sysconfig`-Datei zu konfigurieren, wird die folgende Syntax benutzt:

```
<sysconfig config:type="list" >
  <sysconfig_entry>
    <sysconfig_key>XNTPD_INITIAL_NTPDATE</sysconfig_key>
    <sysconfig_path>xntp</sysconfig_path>
    <sysconfig_value>ntp.host.com</sysconfig_value>
  </sysconfig_entry>
  <sysconfig_entry>
    <sysconfig_key>HTTP_PROXY</sysconfig_key>
    <sysconfig_path>proxy</sysconfig_path>
    <sysconfig_value>proxy.host.com:3128</sysconfig_value>
  </sysconfig_entry>
  <sysconfig_entry>
    <sysconfig_key>FTP_PROXY</sysconfig_key>
    <sysconfig_path>proxy</sysconfig_path>
    <sysconfig_value>proxy.host.com:3128</sysconfig_value>
  </sysconfig_entry>
</sysconfig>
```

Ausgabe 23: Die Konfiguration von sysconfig

Hinzufügen von kompletten Konfigurationen

Für viele Anwendungen und Dienste haben Sie unter Umständen eine Konfigurationsdatei angelegt, die nun vollständig an einen bestimmten Ort im installierten System kopiert werden soll. Dies trifft beispielsweise zu, wenn Sie einen Webserver installieren und eine betriebsfertige `httpd.conf`-Datei haben.

Mit dieser Ressource können Sie die Datei in das Control File einbetten, indem Sie den endgültigen Pfad auf dem installierten System angeben. YaST2 wird diese Datei an die angegebene Stelle kopieren.

```

<files config:type="list">
  <config_file>
    <file_path>/etc/httpd/httpd.conf</file_path>
    <file_contents>
  ]]>
<![CDATA[
some content
]]>
<![CDATA[
  </file_contents>
</config_file>
</files>
]]>

```

Ausgabe 24: Dateien in das installierte System übertragen

Verschiedene Hardware- und Systemkomponenten

Zusätzlich zu der Konfiguration der Kernkomponenten wie der Netzwerkauthentifizierung und der Sicherheit ermöglicht AutoYaST2 eine breite Palette von Hardware- und Systemkonfigurationen, die standardmäßig auf jedem manuell installierten System interaktiv verfügbar sind. So ist es beispielsweise möglich, Drucker, Soundkarten, TV-Karten und andere Hardwarekomponenten zu konfigurieren, für die YaST2 über ein Modul verfügt.

Drucker Obwohl es möglich ist, die Druckerkonfiguration manuell vorzunehmen (wie bei anderen Konfigurationen), ist es empfehlenswert, für solche Konfigurationen das Configuration Management System zu benutzen, da diese Module sehr komplex sind und viele Optionen anbieten.

Bei Gebrauch des Configuration Management Systems wird dafür gesorgt, dass die bereitgestellten Optionen konsistent sind. Das folgende Beispiel zeigt einen Abschnitt einer Konfiguration, die mit dem Configuration Management System erstellt wurde.

```

<configure>
...
  <printer>
    <default>lp</default>
    <printcap config:type="list">
      <printcap_entry>
        <cups-state>void</cups-state>
        <ff config:type="boolean">true</ff>
        <info></info>

```



```

        <location></location>
        <lprng-state>changed</lprng-state>
        <name>lp</name>
        <options>
            <job-sheets>none,none</job-sheets>
        </options>
        <raw config:type="boolean">true</raw>
        <type>yast2</type>
        <uri>parallel:/dev/lp0</uri>
    </printcap_entry>
</printcap>
</printer>
....
</configure>

```

Ausgabe 25: Konfiguration des Druckers

Soundkarten Das folgende Beispiel zeigt eine Soundkonfiguration, die mit dem Configuration Management System erstellt wurde.

```

<configure>
....
  <sound>
    <autoinstall config:type="boolean">true</autoinstall>
    <modules_conf config:type="list">
      <module_conf>
        <alias>snd-card-0</alias>
        <model>M5451, ALI</model>
        <module>snd-ali5451</module>
        <options>
          <snd_enable>1</snd_enable>
          <snd_index>0</snd_index>
          <snd_pcm_channels>32</snd_pcm_channels>
        </options>
        <unique_key>uniq.virtual</unique_key>
      </module_conf>
    </modules_conf>
    <volume_settings config:type="list">
      <listentry>
        <Master config:type="integer">75</Master>
      </listentry>
    </volume_settings>
  </sound>
....
</configure>

```

Ausgabe 26: Soundkonfiguration

Die Quelle der Installationsdaten festlegen

Automatische Installation eines Einzelplatzrechners

Der beste Weg, ein System ohne irgendeine Netzwerkverbindung automatisch zu installieren, ist der Einsatz der Standard-CDs, die in der SuSE Linux Desktop-Box enthalten sind. Wenn Sie die CDs in Verbindung mit einer Diskette benutzen, können Sie AutoYaST2 schnell starten, ohne viel Zeit mit der Konfiguration der Server- und Netzwerkkumgebung zu verlieren.

Wie in den folgenden Abschnitten beschrieben wird, müssen Sie eine Diskette mit einer Profildatei erstellen, die sämtliche Daten enthält, die YaST2 benötigt, um die automatische Installation durchzuführen.

Erstellen Sie das Control File wie oben beschrieben und nennen Sie sie `autoinst.xml`. Kopieren Sie `autoinst.xml` auf die Diskette, indem Sie die Diskette mounten oder `mtools` benutzen.

```
mcopy autoinst.xml a:
```

Netzwerkinstallationen

Der Umfang der erforderlichen Eingriffe durch den Benutzer ist davon abhängig, wie die Serverseite einer Netzwerkinstallation vorbereitet ist. In einer vollständigen Netzwerkinstallation ist es ausreichend, dass der Benutzer den Client anschaltet, um die automatische Installation zu starten. Auch dies kann mit verschiedenen Technologien wie Remote Power Management oder Wake-on-LAN (WOL) automatisiert werden. Zusätzliche Information über WOL ist unter <http://www.scyld.com/expert/wake-on-lan.html> erhältlich.

Einrichtung eines Installationsrepositorys

Der Server kann als Konfigurationsrepository benutzt werden. Die Clients müssen Zugang zu den Serverressourcen haben, um zu booten, Pakete zu installieren usw. Um dies zu bewerkstelligen, müssen verschiedene Netzwerkdienste richtig eingerichtet werden.

Der Installationsserver exportiert die Dateien der SuSE Linux Desktop Distribution via NFS. Legen Sie in einem Dateisystem ein Verzeichnis mit ausreichend viel Platz (mehrere Gigabyte) an und kopieren den Inhalt der CDs in dieses Verzeichnis. Dieses Verzeichnis wird dann mit NFS exportiert (durch einen geeigneten Eintrag in `/etc/exports`). Die folgenden Schritte beschreiben, wie ein Installationsrepository erstellt wird.

Melden Sie sich an dem Rechner an, der als Installationsserver bestimmt wurde, und legen Sie ein Verzeichnis für die Dateien der SuSE Linux Desktop Distribution an, zum Beispiel `/usr/local/SuSE/current`. In unserem Beispiel ist `/usr/local/SuSE/current` das Basisverzeichnis für die SuSE Linux Desktop Distribution. Die Position dieses Verzeichnisses kann in der Datei `info` spezifiziert werden oder auf der Befehlszeile des Kernels (siehe unten) mit der Variable `install` angegeben werden (in der Form `install=nfs://192.168.1.1/usr/local/SuSE/current`).

Dann kopieren Sie die Dateien aller CDs oder der CDs, die für die Installation benötigt werden, in das Verzeichnis `current`. Sorgen Sie dafür, dass alle Pakete kopiert werden, die für die Installation benötigt werden. Achten Sie darauf, dass die versteckten Dateien (`.<dateiname>`) auf der CD-ROM auch kopiert werden, da diese zur Identifizierung des Datenträgers benötigt werden. Benutzen Sie die folgenden Befehle, um die CDs zu kopieren.

```
mount /cdrom
cd /cdrom && cp -va . /usr/local/SuSE/current ; cd -
umount /cdrom
```

Wiederholen Sie diesen Vorgang für alle weiteren CDs. Für die Installation sind zwei verschiedene Verzeichnisstrukturen möglich:

- Der Inhalt aller CDs wird in ein Verzeichnis kopiert; es wird eine einzige Verzeichnisstruktur mit einem Unterverzeichnis `suse` erstellt, dass alle Paketgruppen enthält. Dieser Strukturtyp wird empfohlen, da er einfacher zu verwalten ist und ein einziges Installationsmedium darstellt.

Um das Verzeichnis für den Client als einzigen Datenträger erscheinen zu lassen, muss die auf den CDs enthaltene Paketdatenbank modifiziert werden, indem der Verweis auf die verschiedenen CDs auf eine einzige CD abgeändert wird, in unserem Fall auf CD 1.

Benutzen Sie den folgenden Befehl, um den Installationspfad in der textbasierten Paketdatenbank im Verzeichnis `suse/setup/descr` abzuändern:

```
cd /usr/local/SuSE/current/suse/setup/descr
perl -pi -e 's/InstPath:\t0[2|3|4|5|6|7]/InstPath:\t01/' common.pkd
cd -
```

- Kopieren Sie die CDs in Unterverzeichnisse, die nach der CD-Nummer benannt werden (CD1, CD2 usw.). Auch diese Struktur ermöglicht die Installation via NFS, aber die einzelnen Verzeichnisse werden als getrennte Datenträger behandelt.

Nachdem Sie die CDs in das Installationsverzeichnis kopiert haben, sorgen Sie dafür, dass es via NFS exportiert wird. Sie können dies mit dem NFS-Server-Modul in YaST2 bewerkstelligen.

Außerdem modifizieren Sie bitte die folgenden Dienste so, dass sie bei jedem Systemstart gestartet werden.

- `nfsserver`
- `portmap`

Anlegen eines Konfigurationsrepositorys

Ein Konfigurationsrepository enthält das Control File für mehrere Rechner. Control Files können beliebige Dateinamen haben, die dann jeweils beim Starten eines Clients angegeben werden müssen. Um nicht den Profilnamen für jeden Client gesondert angeben zu müssen, definieren Sie einfach das Verzeichnis, in dem sich das Control File befindet. Wenn ein Verzeichnis angegeben ist, wird der Client versuchen, eine Datei zu laden, deren Name seiner hexadezimalen IP-Adresse entspricht. (Siehe *Über HTTP abrufbares Control File* in Abschnitt [Auflösen der automatischen Installation](#) auf Seite 49.) Dies hat den Vorteil, dass Sie es mit konsistenten Dateinamen und nicht mit IPs als Dateinamen zu tun haben, was eher verwirrend wäre.

Das Konfigurationrepository ist das gleiche Verzeichnis, das angegeben wird, wenn Sie für die Erstellung von Control Files das Configuration Management System benutzen.

HTTP-Repository Um das HTTP-Protokoll zum Abrufen der Control File für die automatische Installation benutzen zu können, brauchen Sie auf der Serverseite einen funktionierenden HTTP-Server. Installieren Sie Apache oder einen Webserver Ihrer Wahl und aktivieren Sie ihn mit YaST2. Normalerweise befindet sich das Wurzelverzeichnis des Webserver in `/usr/local/httpd/htdocs`. Legen Sie im Wurzelverzeichnis des Webserver ein Unterverzeichnis an, das Sie als Konfigurationsrepository benutzen können.

NFS-Repository Legen Sie ein Verzeichnis an und machen Sie es via NFS für die Clients verfügbar, indem Sie es exportieren. Dieses Verzeichnis kann sich beispielsweise an der gleichen Stelle befinden, wohin Sie bereits die CDs kopiert haben (`/usr/local/SuSE`).

TFTP-Repository Standardmäßig befindet sich das TFTP-Verzeichnis unter `/tftpboot` und kann auch Boot-Images enthalten, falls Sie über das

Netzwerk booten. Vergessen Sie nicht, `tftp` in der Konfigurationsdatei des `inetd` (`/etc/inetd.conf`) zu aktivieren. Der `inetd` kann mit `Yast2` konfiguriert werden.

Verwaltung des Bootvorgangs

Booten des Zielsystems

Es gibt verschiedene Möglichkeiten, das Zielsystem zu booten. Das Booten des Rechners und die Initialisierung der automatischen Installation ist so wichtig wie die eigentliche Installation. Je nachdem wie viele Zielsysteme zu installieren sind, werden die folgenden Methoden unterstützt:

Diskette Nicht zu empfehlen für komplexe Netzwerkkumgebungen. Eine Diskette kann nicht die gesamte Information fassen, die benötigt wird, um einen Rechner für die Installation vorzubereiten. Daher sollte man nur in sehr speziellen Fällen eine Diskette benutzen. In diesem Fall müssen die Standardkomponenten der SuSE-Startdiskette Ihren Bedürfnissen genau angepasst werden. Eine Diskette kann jedoch benutzt werden, um das Control File und andere Informationen zu speichern, die für die Installation benötigt werden.

CD-ROM Benutzen Sie die Original-CDs von SuSE zusammen mit einem anderen Datenträger, zum Beispiel mit einer Diskette für das Control File, oder mit einem Netzwerk, aus dem das Control File abgerufen werden kann. Es ist auch möglich, angepasste CD-ROMs zu erstellen, die außer dem Control File nur die benötigten Pakete enthält. Dieser Ansatz erfordert jedes Mal, wenn sich die Konfiguration ändert, die Erstellung neuer CD-ROMs.

Netzwerk Der Gebrauch des Netzwerks zum Booten des Zielsystems ist der praktischste Weg für die automatische Installation. Das Booten vom Netzwerk und die Bereitstellung eines Repositories für Control Files auf einem erreichbaren Server kann sehr flexibel sein, besonders wenn verschiedene Systemtypen mit unterschiedlichen Aufgaben und Hardwarekomponenten konfiguriert werden müssen.

Booten des Clients

Es gibt verschiedene Möglichkeiten, den Client zu booten. Der Computer kann über seine Netzwerkkarte (NIC) booten, um die Boot-Images via DHCP oder

TFTP abzurufen, oder ein geeigneter Kernel und ein initrd-Abbild kann von einer Diskette oder einer angepassten bootfähigen CD-ROM geladen werden.

Booten von Diskette

Für Test- und Rettungszwecke oder falls die NIC keinen PROM oder PXE hat, erstellen Sie eine Startdiskette zum Gebrauch mit AutoYaST2. Der Gebrauchsfähigkeit einer Diskette für die Initialisierung einer automatischen Installation ist beschränkt, da eine Diskette nur über einen begrenzten Speicherplatz verfügt. Es ist jedoch möglich, für die automatische Installation eines unabhängigen Einzelplatzrechners Disketten zu benutzen.

Disketten sind geeignet, um das Control File zu speichern, besonders wenn die Original-CDs von SuSE benutzt werden sollen. Mit Hilfe der Befehlszeile des Kernels kann der Benutzer angeben, wo sich das Control File auf der Diskette befindet. (Siehe *Control File auf einer Diskette* in Abschnitt *Auslösen der automatischen Installation* auf Seite 49).

Selbst ohne die spezielle Befehlszeilenoption `autoyast` ist es möglich, die automatische Installation zu initialisieren, indem man ein Control File mit einem speziellen Namen (`autoinst.xml`) auf einer Diskette speichert. Beim Systemstart prüft YaST2, ob eine Datei namens `autoinst.xml` vorhanden ist. Falls dies der Fall ist, wechselt YaST2 vom interaktiven Modus zur automatisierten Installation.

Booten von einer Netzwerkkarte

Für administrative Zwecke ist es praktischer, von einer Netzwerkkarte (NIC) zu booten als von einer Diskette. Um diese Bootmethode nutzen zu können, braucht die NIC des Clients ein Boot-PROM, das mit einem DHCP-Server kommunizieren kann, um kommunikationsspezifische Konfigurationsparameter (z.B. Netzwerkadressen) zu erhalten, und der mit einem TFTP-Server kommunizieren kann, um ein Boot-Image abzurufen.

Etherboot und Netboot Etherboot und Netboot können eine PROM-Binary (die aber immer noch auf ein PROM programmiert werden müssen) und ein entsprechendes „tagged“ TFTP-Boot-Image erstellen, das einen Kernel und eine Initial Ramdisk umfasst. Es gibt Tools, mit denen man ein PROM-Boot-Image testen kann. Die Utilities von Ethernet und Netboot sind fast identisch.

<http://etherboot.sourceforge.net/>

<http://www.han.de/~gero/netboot.html>

Gebrauch von PXE zum Booten von PROMs Eine weitere Alternative zu Etherboot und Netboot ist der Gebrauch eines PXE-fähigen Boot-PROMs. PXE (Preboot Execution Environment) ist ein von Intel entworfenes Protokoll für das Booten von Computern über das Netzwerk. PXE wird im ROM der neuen Generationen von Netzwerkkarten gespeichert. Wenn der Computer gestartet wird, lädt das BIOS das PXE in den Speicher und führt es aus. Ein Menü wird angezeigt, in dem die Möglichkeit angeboten wird, den Computer mit einem Betriebssystem zu booten, das über das Netzwerk geladen wird.

<http://developer.intel.com/ial/WfM/Wfmspecs.htm>

Um einen Client mit einem Pre-Boot Execution Environment (PXE) zu installieren, benötigen Sie keinen PXE-Server. PXE benutzt eine BOOTP-Anfrage, um eine IP-Adresse und andere Netzwerkinformationen sowie eine Bootloader-Programme an den Client zu übertragen. Sie können dies entweder mit einem BOOTP-Server oder mit einem DHCP- und einem TFTP-Server tun.

In den folgenden Abschnitten wird beschrieben, wie DHCP und TFTP eingerichtet werden müssen, um PXE-Installationen zu ermöglichen.

- **DHCP** Installieren Sie den DHCP-Server von ISC (<http://www.isc.org/>); das entsprechende Paket ist in der SuSE Distribution enthalten. Konfigurieren Sie die Parameter des DHCP-Servers in `/etc/sysconfig/dhcpd` und sorgen Sie dafür, dass Sie eine funktionierende Konfigurationsdatei `/etc/dhcpd.conf` haben.
- **PXE-Bootloader** PXE kann ein Programm in den Speicher des Clients laden und starten. Dann lädt der Bootloader seine Konfigurationsdatei via TFTP von dem Server, der in `next-server` definiert ist (wie in der obigen Musterdatei `dhcpd.conf`).

Die Konfigurationsdatei des Bootloaders legt fest, ob ein Client von der lokalen Festplatte oder über das Netzwerk gebootet wird.

```
default linux
serial 0,9600n8
label linux
kernel linux
append console=ttyS0,9800
console=tty0 load_ramdisk=1
```

```
initrd=initrd
autoyast=nfs://nfsserv/file.xml
```

Ausgabe 27: Konfigurationsdatei für das Booten über das Netzwerk mit PXELINUX

Bitte beachten Sie, dass der Ausdruck „append console ... file.xml“ in eine Zeile geschrieben werden muss.

Booten von der lokalen Festplatte (Dateiname default):

```
default linux
label linux
localboot 0
```

Ausgabe 28: Konfigurationsdatei für das lokale Booten mit PXELINUX

pxelinux.0 versucht, verschiedene Konfigurationsdateien zu lesen. Es benutzt die erste Konfigurationsdatei, die es findet. Die Dateinamen, nach denen es sucht, werden von der IP-Adresse des Clients bestimmt, auf dem es läuft. Es konvertiert die vier dezimalen Teile einer IP-Adresse (durch Punkte getrennt) in hexadezimale Zahlen und verknüpft sie. Beispiel: Die IP-Adresse 192.168.0.11 wird in C0 A8 00 0B konvertiert (ohne Leerstellen).

Die Dateisuche beginnt bei C0A8000B und fährt fort, indem eine Ziffer von rechts entfernt wird (Rest C0A8000) und so weiter. Wenn alle Ziffern entfernt sind, wird als letztes der Dateiname *default* versucht. Auf Ihrem TFTP-Server kann dieser Algorithmus benutzt werden, um jedem einzelnen Rechner mitzuteilen, wie gebootet werden soll:

```
/tftpboot/pxelinux.cfg/
C0A8000B -> default.netboot-8.0
C0A8000C -> default.netboot-8.1
default.netboot-8.0
default.netboot-8.1
default
```

Ausgabe 29: PXELINUX-Konfiguration

Dies ist wichtig, falls Sie viele Rechner gleichzeitig installieren. Sie können die syslog-Datei auf Ihrem TFTP-Server beobachten und

immer, wenn ein Client seine Initial Ramdisk bekommen hat, den Symlink für diesen Rechner aus dem Verzeichnis `pxelinux.cfg` entfernen. Dies zwingt den Client, die Standardkonfiguration zu laden, die besagt, dass von der lokalen Festplatte gebootet wird, wenn nach der Beendigung von AutoYaST neu gestartet wird.

- **TFTP PXE** erfordert einen speziellen TFTP-Server. Einzelheiten werden in `pxelinux.doc` im oben erwähnten `syslinux`-Paket beschrieben.

Der `inetd`-basierte TFTP-Server ist nicht in Lage, mehr als 64 Clients gleichzeitig zuverlässig zu bedienen. Falls die Anzahl der Clients größer ist, werden einige keine Antwort von Ihrem TFTP-Server erhalten und Sie werden `syslog`-Meldungen erhalten, die wie folgt aussehen:

```
tftpd: read: Connection refused.
```

Um dieses Problem zu beseitigen, können Sie `atftp` benutzen, das als Paket verfügbar ist. Dieser TFTP-Server kann als unabhängiger Daemon laufen.

Das Verzeichnis `/tftpboot` auf dem TFTP-Server sollte wie folgt aussehen:

```
/tftpboot/initrd
pxelinux.0
linux
```

Ausgabe 30: Inhalt des Verzeichnisses `tftpboot`

Der nächste Abschnitt beschreibt, wie Sie die Dateien `linux` und `initrd` beschaffen.

- **Kernel und Initial Ramdisk** Für das Booten vom Netzwerk und andere Konfigurationen wird empfohlen, die Images zu verwenden, die sich auf jeder SuSE CD-ROM im Verzeichnis `/suse/images/boot` befinden. Die Initial Ramdisk (`initrd`) enthält alle Kernelmodule, die für eine erfolgreiche Installation erforderlich sind. In speziellen Fällen mag es nötig sein, einen eigenen Kernel zu kompilieren oder spezielle Kernel zu verwenden, die auf der CD-ROM verfügbar sind.

BOOTP- DHCP-Optionen Eine andere DHCP-Option kann benutzt werden, um die Angabe des Quellmediums zu ermöglichen, wenn über das Netzwerk gebootet wird. Diese Option `root-path` wird im folgenden Beispiel gezeigt.

```
subnet 192.168.1.0 netmask 255.255.255.0

    range dynamic-bootp 192.168.1.100 192.168.1.110;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    filename "vmlinuz.nbi";
    option root-path "/tftpboot/CDs";

next-server 192.168.1.1;
```

Ausgabe 31: /etc/dhcpd.conf mit der Option root-path

Das nächste Beispiel zeigt, wie der DHCP-Server in Abhängigkeit von dem anfordernden Client (PXE oder Etherboot) ein Image an den Client senden kann.

```
ddns-update-style none;
allow bootp;
allow booting;

subnet 192.168.1.0 netmask 255.255.255.0
    range dynamic-bootp 192.168.1.100 192.168.1.110;
    option domain-name "cluster.suse.de";
    option routers 192.168.1.240;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    filename "vmlinuz-node.nbi";
    option root-path "/local/CD1";

group
    next-server 192.168.1.240;
    use-host-decl-names on;

    host n1
        hardware ethernet 00:00:1c:b5:6e:71;
        fixed-address n1;
        if substring (option vendor-class-identifier, 0, 9) = "PXEClient"
```

```
        filename "/tulip.lzpxe";
    else if substring (option vendor-class-identifier, 0, 9) = "Ether
boot"
        filename "/vmlinuz-node.nbi";

    host n2
        hardware ethernet 00:00:1c:b5:72:ea;
        fixed-address n2;
        if substring (option vendor-class-identifier, 0, 9) = "PXEClient"
            filename "pxelinux.0";
        else if substring (option vendor-class-identifier, 0, 9) = "Ether
boot"
            filename "/vmlinuz-node.nbi";
```

Ausgabe 32: Konfiguration des DHCP-Servers mit PXE- und Etherboot-Optionen

Auslösen der automatischen Installation

Das Hinzufügen der Befehlszeilenvariable `autoyast` lässt `linuxrc` im automatisierten Modus starten. `linuxrc` sucht nach einer Konfigurationsdatei, die sich an den folgenden Stellen vom zentralen Control File unterscheiden sollte:

- Im Wurzelverzeichnis der Initial Ramdisk, die Sie benutzen, um das System zu booten
- Im Wurzelverzeichnis der Diskette

Das Control File für `linuxrc` kann die Variablen enthalten, die in Tabelle 1.1 auf der nächsten Seite aufgeführt sind.

| Variable | Wert |
|-------------------------|---|
| <code>netdevice</code> | Das Netzwerkgerät, dass für die Einrichtung des Netzwerks benutzt werden soll (das Gerät, das für BOOTP- oder DHCP-Anfragen benutzt wird) |
| <code>server</code> | Welcher Server für das Wurzelverzeichnis angesprochen werden muss (NFS-Server) |
| <code>serverdir</code> | Verzeichnis auf dem NFS-Server |
| <code>ip</code> | Falls leer, sendet der Client eine BOOTP-Anfrage; andernfalls wird der Client mit der angegebenen IP-Konfiguration konfiguriert |
| <code>netmask</code> | Netzwerkmaske |
| <code>gateway</code> | Gateway |
| <code>nameserver</code> | Nameserver |
| <code>insmod</code> | Zu ladende Kernelmodule |
| <code>autoyast</code> | Position des Rechnerprofils, das für die automatische Installation benutzt werden soll (z.B. <code>autoyast=http://192.168.2.1/profiles/</code>) |
| <code>install</code> | Position des Installationsverzeichnisses (z.B. <code>install=nfs://192.168.2.1/CDs/</code>) |
| <code>instmode</code> | Installationsmodus (nfs, http usw.); wird nicht benötigt, wenn <code>install</code> gesetzt ist |

Tabelle 1.1: Variablen für `linuxrc`

Diese Variablen und Stichwörter bringen das System bis zu dem Punkt, an dem Y_oST2 den Vorgang mit dem zentralen Control File übernehmen kann. Da das Quellmedium automatisch festgestellt wird, ist es manchmal möglich, die automatische Installation ohne irgendwelche Anweisungen an `linuxrc` zu starten.

Die traditionelle Konfigurationsdatei (`info`) von `linuxrc` sollte nur in der Vorbereitungsphase benutzt werden. Sie hat die Aufgabe, dem Client genügend Information über den Installationsserver und die Position der Quellen mitzuteilen. In den meisten Fällen wird diese Datei nicht benötigt. Sie wird jedoch in manchen speziellen Netzwerkumgebungen benötigt, in denen DHCP und BOOTP nicht benutzt werden oder spezielle Kernelmodule geladen werden müssen.

Anstatt die erwähnten Variablen im Control File festzulegen, kann man sie auch mit Hilfe der Kernelbefehlszeile an `linuxrc` weitergeben. Alle Kombinationen von Schlüsseln und Variablen können jetzt in dieser Weise mitgeteilt werden. Die Befehlszeile kann beispielsweise auch benutzt werden, wenn Images erstellt werden, die über das Netzwerk gebootet werden können, oder an den Kernel

weitergegeben werden, wenn ein speziell konfigurierter DHCP-Server in Verbindung mit Etherboot oder PXE benutzt wird. Das Format der speziellen Befehlszeilenvariable `autoyast` kann benutzt werden, wie in Tabelle 1.2 gezeigt wird.

| Befehlszeilenvariable | Beschreibung |
|--|---|
| <code>autoyast=default</code> | Standardoption für die automatische Installation |
| <code>autoyast=file://<path></code> | Sucht in dem angegebenen Pfad (relativ zum Wurzelverzeichnis des Quellmediums, z.b. <code>file://autoinst.xml</code> falls es sich um das oberste Verzeichnis einer CD-ROM handelt) nach dem Control File |
| <code>autoyast=floppy://<path></code> | Sucht auf der Diskette nach dem Control File (nützlich, wenn von CD gebootet wird) |
| <code>autoyast=nfs://<server>:<path></code> | Sucht auf <server> nach dem Control File |
| <code>autoyast=http://<server>/<path></code> | Abrufen des Control Files von einem Webserver mit dem HTTP-Protokoll |
| <code>autoyast=tftp://<server>:<path></code> | Abrufen des Control Files mit TFTP |

Tabelle 1.2: Befehlszeilenvariablen für AutoYaST2

Bei Gebrauch von verschiedenen Arten von Infrastrukturen und Quellmedien sind verschiedene Szenarien für die automatische Installation möglich. Der einfachste Weg ist der Gebrauch der Quellmedien aus der SuSE-Box. In diesem Fall hat der Benutzer entweder eine DVD mit allen SuSE-Paketen oder einen Satz CDs. Um die automatische Installation zu initialisieren, sollte jedoch die Befehlszeilenvariable für die automatische Installation beim Systemstart eingegeben werden und das Control File sollte für YaST2 zugänglich sein. Die folgende Liste von Szenarien zeigt, wie das Control File bereitgestellt werden kann und wie das Setup sein muss, damit die automatische Installation erfolgreich ist.

- Benutzung der Original-CDs aus der SuSE Linux Desktop Box: Bei Benutzung der Original-CDs benötigt der Benutzer einen Datenträger mit

dem Control File. Das Control File kann sich an den folgenden Positionen befinden:

1. *Diskette*: Der Zugang zum Control File wird durch die Option `autoyast=floppy` ermöglicht. Beim Start sucht YaST2 nach einer Datei namens `autoinst.xml`. Wenn eine solche Datei gefunden wird, wechselt YaST2 in den Autoinstallationsmodus, auch wenn keine speziellen Befehlszeilenvariablen mitgeteilt wurden. Um diese Option zu benutzen, erstellen Sie das Control File, speichern sie auf eine vorformatierte Diskette und starten die Installation wie gewöhnlich.
2. *Netzwerk*: Der Zugang zum Control File wird durch die Optionen `autoyast=nfs://..`, `autoyast=http://..` oder `autoyast=tftp://..` ermöglicht.

■ Benutzung von „selbstgemachten“ CDs:

In diesem Fall kann der Benutzer das Control File auf der CD-ROM abspeichern, um den Zugang zu vereinfachen (im Zusammenhang mit der Option `autoyast=file://`), oder eine der obenerwähnten Methoden anwenden, die bei Gebrauch der Original-CDs von SuSE zur Verfügung stehen.

■ Benutzung von NFS und Diskette, Netzwerk oder CD-ROM für den Systemstart. Dies ist die wichtigste Option, da die Installation von PC-Farmen normalerweise über NFS-Server und andere Netzwerkdienste wie BOOTP und DHCP erfolgt. Das Control File kann sich an den folgenden Stellen befinden:

1. *Diskette oder CD-ROM*: Zugang zum Control File über die Option `autoyast=file://...`
2. *Netzwerk*: Zugang zum Control File über die Optionen `autoyast=http://...`, `autoyast=nfs://..` oder `autoyast=tftp://...`

Standardverhalten

Wenn `autoyast=default` gesetzt ist, sucht YaST2 an den folgenden drei Positionen nach einer Datei namens `autoinst.xml`:

1. Das Wurzelverzeichnis der Diskette
2. Das Wurzelverzeichnis des Installationsmediums

3. Das Wurzelverzeichnis der Initial Ramdisk, die benutzt wird, um das System zu booten.

Dies ist der Standard, der auch dem Verhalten von `linuxrc` in früheren Versionen von SuSE Linux Desktop entspricht.

Control File auf dem Bootmedium

Legen Sie die Position des Control Filea mit der Option `file` fest, die anzeigt, wo sich das Control File befindet. Je nachdem, welche Bootmethode benutzt wird, sucht Yast2 im angegebenen Pfad des Wurzelverzeichnisses der Initial Ramdisk (`initrd`) nach dem Control File.

Control File auf einer Diskette

Yast2 sucht im angegebenen Verzeichnis nach der Control File. Dies ist besonders nützlich, wenn zum Booten eine CD-ROM benutzt wird (Original-CDs von SuSE).

Über HTTP abrufbare Control File

Um HTTP zu benutzen, setzen Sie die Befehlszeilenvariable `autoyast` zusammen mit der Position des Control Files, wie in Tabelle 1.2 auf Seite 51 beschrieben. Die Position des Control Files kann mit den folgenden Methoden angegeben werden:

1. Angabe der genauen Position des Control Files:
`autoyast=http://192.168.1.1/control-files/client01.xml`
2. Angabe eines Verzeichnisses, in dem sich mehrere Control Files befinden:
`autoyast=http://192.168.1.1/control-files/`

In diesem Fall wird das relevante Control File anhand der hexadezimalen Bezeichnung der IP-Adresse abgerufen, wie unten beschrieben.

Wenn nur die Pfadpräfixvariable definiert ist, holt sich Yast2 wie folgt das Control File vom HTTP-Server:

1. Zunächst wird nach dem Control File gesucht, indem die eigene IP-Adresse in hexadezimaler Form in Großbuchstaben benutzt wird. Beispiel: 192.0.2.91 entspricht C000025B.

2. Falls diese Datei nicht gefunden wird, wird eine hexadezimale Stelle entfernt und ein erneuter Versuch gestartet. Dies geht weiter, bis die Datei mit dem richtigen Namen gefunden wird. Zuletzt wird nach einer Datei namens `default` (in Kleinbuchstaben) gesucht.

Beim Beispiel `192.0.2.91` sucht der HTTP-Client der Reihe nach nach `C000025B`, `C000025`, `C00002`, `C0000`, `C000`, `C00`, `C0`, `C` und `default`.

Um die hexadezimale Darstellung der IP-Adresse des Clients zu ermitteln, können Sie die Utility `/usr/sbin/gethostip` benutzen, die im Paket `syslinux` enthalten ist.

```
myhost # /usr/sbin/gethostip 10.10.0.1
10.10.0.1 10.10.0.1 0A0A0001
```

Über TFTP abrufbares Control File

Diese Option entspricht dem Gebrauch von HTTP.

Control File auf einem NFS-Server

YoST2 sucht auf dem NFS-Server, der auf der Befehlszeile angegeben wird, nach dem Control File. In diesem Fall wird `linuxrc` das Netzwerkgerät automatisch erkennen und DHCP benutzen, um das Ethernetgerät zu konfigurieren. Das gleiche Verhalten im Zusammenhang mit hexadezimalen IP-Adressen steht auch hier zur Verfügung (wie bei TFTP und HTTP).

Starten der automatischen Installation

Der Autoinstallationsprozess

Nachdem das System gestartet und das Control File abgerufen wurde, konfiguriert YoST2 das System gemäß den Informationen in der Control File. Die Konfiguration wird standardmäßig in einem Fenster zusammengefasst. Diese Funktion sollte deaktiviert werden, falls eine vollautomatische Installation erwünscht wird.

Bevor die Zusammenfassung der Konfiguration angezeigt wird, hat YoST2 nur die Hardware erkannt und das System für die automatische Installation vorbereitet. Es sind noch keine Änderungen am System vorgenommen worden, so dass der Prozess abgebrochen werden kann, falls ein Fehler aufgetreten ist.

Ein System sollte auch ohne Grafikkarte oder Monitor automatisch installierbar sein. Der Anschluss eines Monitors wird empfohlen, um den Vorgang zu überwachen und Feedback über etwaige Fehler zu bekommen. Man kann zwischen dem Qt- und dem Ncurses-Interface wählen. Bei Clients ohne Monitor können die Systemmeldungen über die serielle Konsole verfolgt werden.

Das X11-Interface

Dies ist das Standardinterface für die automatische Installation. Es sind keine speziellen Variablen erforderlich, um diesen Modus zu aktivieren.

Serielle Konsole

Sie können die Systeminstallation mit der seriellen Konsole starten, indem Sie die Variable `console` der Befehlszeile des Kernels hinzufügen (zum Beispiel `console=ttyS0`). Dies führt dazu, dass `linuxrc` im Konsolenmodus gestartet wird. Im weiteren Verlauf wird auch YaST2 im seriellen Konsolenmodus gestartet.

Textbasierte Installation mit YaST2

Diese Option kann auch auf der Befehlszeile aktiviert werden. Dies startet YaST2 im Ncurses-Modus. Um YaST2 im Textmodus zu starten, geben Sie auf der Befehlszeile `textmode=1` ein.

Es wird empfohlen, YaST2 im Textmodus zu starten, wenn ein Client mit weniger als 64 MB oder gänzlich ohne X11 (besonders Rechner ohne Monitore) installiert werden soll.

Systemkonfiguration

Die Systemkonfiguration kann als wichtigste Stufe der gesamten automatischen Installation angesehen werden. Mehr als die eigentliche Installation ist die Anpassung eines Systems an Ihre Bedürfnisse das, was ein Autoinstallationssystem attraktiv macht.

Wie Sie in den vorhergehenden Kapitel gesehen haben, können fast alle Parameter auf dem Zielsystem automatisch konfiguriert werden. Außer den vordefinierten Direktiven können Sie Postskripten benutzen, um andere Dinge im System zu ändern. Sie können alle Systemvariablen ändern oder komplette Konfigurationsdateien zum Zielsystem kopieren.

Postinstallation und Systemkonfiguration

Die Postinstallation und die Systemkonfiguration werden sofort initialisiert, nachdem das letzte Paket auf dem Zielsystem installiert wurde und werden wiederaufgenommen, nachdem das System zum ersten Mal gebootet wurde.

Bevor das System zum ersten Mal gebootet wird, schreibt YaST2 alle Daten, die während der Installation gesammelt wurden, zum System und installiert zuletzt den Bootloader an der angegebenen Position. Außer diesen Routinemaßnahmen, welche auch im Verlauf einer normalen Installation durchgeführt werden, führt YaST2 die chroot-Skripten aus, die im Control File spezifiziert werden. Diese Skripten werden ausgeführt, bevor das System gemountet wird.

Falls ein anderer Kernel als der Standardkernel installiert wird, ist ein Systemneustart erforderlich. Ein Neustart kann auch unabhängig vom installierten Kernel während der automatischen Installation erzwungen werden. Dies kann mit Hilfe der Eigenschaft `reboot` in der Ressource `general` erreicht werden. (Siehe *Allgemeine Optionen* in Abschnitt [Profilressourcen unter der Lupe](#) auf Seite 18).

Systemanpassung

Die Systemanpassung erfolgt größtenteils während der zweiten Phase der Installation. YaST2 bietet die meisten relevanten Ressourcen, die benötigt werden, um das System in einen allgemein gebrauchsfähigen Zustand zu versetzen. Es könnte jedoch sein, dass Sie spezielle Anforderungen an das installierte System haben. Falls die erforderlichen Anpassungen mit YaST2-Ressourcen durchgeführt werden können, kann dies mit Hilfe der Postinstall-Skripten geschehen. Definieren Sie im Control File eine unbegrenzte Anzahl von benutzerdefinierten Skripten, indem Sie das Control File modifizieren oder das Configuration Management System benutzen.

Das X Window System

Das X Window System stellt unter Unix einen Quasi-Standard für grafische Benutzeroberflächen dar. Das X Window System, das auch als X11 bezeichnet wird, ist noch viel mehr: es ist ein netzwerkbasiertes System. Anwendungen, die auf dem Rechner *er*de laufen, können ihre Ausgaben auf dem Rechner *son*nne darstellen, sofern die Maschinen durch ein Netzwerk verbunden sind. Dieses Netz kann ein LAN sein, die Geräte können aber auch tausende Kilometer voneinander entfernt stehen und über das Internet miteinander kommunizieren.

Im Folgenden stellen wir Ihnen u. a. das Programm `xf86config` vor, mit dem Sie alternativ zu `SxX2` Monitor, Grafikkarte, Tastatur und Maus einrichten können. Ein weiterer Schwerpunkt ist die OpenGL/3D-Konfiguration. Für YcST2 Modulbeschreibungen siehe [\[SuS02b\]](#).

| | |
|---|----|
| Geschichtlicher Hintergrund | 58 |
| Die Version 4.x von XFree86 | 59 |
| Konfiguration mit <code>xf86config</code> | 60 |
| Installation des X Window System optimieren | 70 |
| Konfiguration von OpenGL/3D | 80 |

Geschichtlicher Hintergrund

X11 entstand als Gemeinschaftsproduktion von DEC (Digital Equipment Corporation) und dem Projekt Athena am MIT (Massachusetts Institute of Technology). Die erste Version (X11R1) wurde im September 1987 freigegeben. Seit Release 6 hat das X Consortium, Inc., ab 1996 The Open Group die Entwicklung des X Window System übernommen.

XFree86™ ist eine frei verfügbare Implementierung von X-Servern für PC-Unix-Systeme (vgl. <http://www.XFree86.org>). XFree86 wurde und wird auch weiterhin – verstreut über die ganze Welt – von Programmierern entwickelt, die sich 1992 zum XFree86-Team zusammengeschlossen haben. Daraus entstand die 1994 gegründete Firma The XFree86 Project, Inc., deren Ziel es ist, XFree86™ einer breiten Öffentlichkeit zur Verfügung zu stellen und sowohl forschend als auch entwickelnd an der Zukunft des X Window System mitzuarbeiten. Seit März 2000 steht die gründlich überarbeitete Major-Release XFree86 4.0 zum Download von <http://www.XFree86.org> zur Verfügung. Bei SuSE Linux Desktop wird standardmäßig XFree86 4.x verwendet. Eine nähere Erläuterung zu den Merkmalen dieser Version folgt gleich im Anschluss.

Die folgenden Abschnitte behandeln die Konfiguration des X-Servers. Zu diesem Zweck wird das Programm `xf86config` besprochen, mit dem alternativ zu `SoX2` ebenfalls eine Konfiguration des X Window System möglich ist.

Um die zur Verfügung stehende Hardware (Maus, Grafikkarte, Monitor, Tastatur) optimal nutzen zu können, besteht die Möglichkeit, die Konfiguration manuell zu optimieren. Auf einige Aspekte der Optimierung wird eingegangen, andere werden nicht gesondert behandelt. Detaillierte Informationen zur Konfiguration des X Window System finden sich in verschiedenen Dateien im Verzeichnis `/usr/share/doc/packages/xf86` sowie natürlich in der Manual-Page von `XF86Config` (`man XF86Config`).

Achtung

Bei der Konfiguration des X Window Systems sollte besonders sorgsam vorgegangen werden! Auf keinen Fall sollte X gestartet werden, bevor die Konfiguration abgeschlossen wurde. Ein falsch eingestelltes System kann zu irreparablen Schäden an der Hardware führen; besonders gefährdet sind Festfrequenz-Monitore. Die Autoren dieses Buches und die SuSE Linux AG lehnen jede Verantwortung für eventuell entstehende Schäden ab. Der vorliegende Text wurde mit größtmöglicher Sorgfalt erstellt. Dennoch kann nicht absolut garantiert werden, dass die hier vorgestellten Methoden korrekt sind und Ihrer Hardware keinen Schaden zufügen.

Achtung

Die Version 4.x von XFree86

Diese Version von SuSE Linux Desktop enthält die Version 4.x von XFree86, die sich in einigen Punkten von der auf den früheren Distributionen enthaltenen Version 3.3 unterscheidet. Insgesamt ergeben sich für den Anwender bei der Bedienung der grafischen Oberfläche kaum Unterschiede, die Applikationen wie zum Beispiel der grafische Desktop KDE oder GNOME verhalten sich auch weiterhin wie bei der früher verwendeten Version 3.3.6.

Welche Vorteile bietet diese Version?

Der neue X-Server ist kein monolithisches Programm mehr, sondern nur noch ein relativ kleines Grundgerüst, zu dem die nötigen Programmmodule bei Bedarf nachgeladen werden können. Es gibt also beispielsweise keine extra X-Server mehr für verschiedene Grafikkarten wie in der bisherigen Version, sondern nur noch ein ausführbares Programm namens XFree86, das Sie im Verzeichnis `/usr/X11R6/bin` finden. Dies ist dann auch der eigentliche X-Server. Der Grafiktreiber, der dann die Ansteuerung der Grafikkarte übernimmt, ist ein ladbares Modul.

Ähnlich wird auch bei der Unterstützung verschiedener Eingabegeräte, Fonts oder X-Protokolle verfahren: Hierbei handelt es sich wieder um einzelne Module, die vom X-Server nachgeladen werden können. Sie müssen sich allerdings in der Regel keine Gedanken über diese Module machen, die Konfiguration der zum Betrieb der grafischen Oberfläche auf Ihrem Computer erforderlichen Module wird weitestgehend von `SoX2` erledigt.

Durch das Modulkonzept ist es für die Hersteller leicht, einen Treiber für spezielle Hardware wie zum Beispiel Touchscreens oder brandneue Grafikkarten zu implementieren. Die Entwickler haben sogar dafür gesorgt, dass die nötigen Module für verschiedene Betriebssysteme nur einmal zur Verfügung gestellt werden müssen, das heißt, ein Grafiktreibermodul, das beispielsweise unter FreeBSD kompiliert wurde, kann auch unter Linux verwendet werden und umgekehrt. Allerdings ist diese Portabilität natürlich auf eine Hardwareplattform beschränkt: ein Modul, das für Linux auf PowerPCs kompiliert wurde, kann nicht auf einem Intel-PC verwendet werden.

Außerdem ist die Unterstützung der Maus deutlich verbessert. Vor allem bei hoher Last ist die Reaktion der Maus auf Mausbewegungen wesentlich schneller und direkter als bei dem bisherigen XFree86 X-Server. Generell hat sich die Ausgabegeschwindigkeit verbessert, Grafikoperationen werden in der Regel schneller ausgeführt als auf dem alten X-Server, was vor allem an der nochmals neu überarbeiteten XAA (engl. *XFree86 Acceleration Architecture*) liegt.

Die Konfigurationsdatei besitzt ein gegenüber XFree86 3.3.x etwas verändertes Format. Falls Sie Ihren X-Server „feintunen“ oder spezielle Einstellungen vornehmen wollen, finden Sie im Abschnitt [Installation des X Window System optimieren](#) auf Seite 70 ausführliche Informationen zum Aufbau und zur Funktionsweise der mittlerweile in `/etc/X11/XF86Config` befindlichen XFree86 Konfigurationsdatei. Auch das Fehlerlogging hat sich verbessert: der X-Server erzeugt ein sehr ausführliches Logfile, das Sie nach dem Start immer in der Datei `/var/log/XFree86.0.log` finden.

Zu weiteren Features dieser Version gehört auch noch die Unterstützung spezieller Optionen wie z. B. True-Type-Fonts, die Bereitstellung der 3D-Protokollerweiterung `glx`, Gamma-Korrektur des Bildschirms und die Unterstützung mehrerer Grafikkarten für Multihead Konfigurationen. Näheres hierzu finden Sie in Abschnitt [Installation des X Window System optimieren](#) auf Seite 70.

Was ändert sich?

Natürlich baut XFree86 4.x auf der bisherigen Version 3.3.x auf. Da manche Grafiktreiber sehr komplex sind, konnten leider nicht alle auf die neue XAA-Architektur portiert werden.

Im Einzelnen handelt es sich hierbei um Grafikkarten, die bisher mit den folgenden X-Servern betrieben wurden: `XF86_S3`, `XF86_Mach8`, `XF86_Mach32` und `XF86_8514`. Für den S3-Server bedeutet dies, dass alle S3-Karten, die den S3-Server benötigen, nicht von XFree86 4.x unterstützt werden. S3-Karten die vom bisherigen SVGA-Server unterstützt waren, laufen also auch mit XFree86 4.x. Im Wesentlichen sind das Grafikkarten mit S3 Trio3D-, Savage4-, Savage3D- und Savage2000-Chips und fast alle S3 Virge-Karten.

Die Grafikkarten, die die oben aufgeführten X-Server (Mach8, Mach32 und 8514) zum Betrieb benötigen, dürften nicht mehr sehr weit verbreitet sein.

Konfiguration mit `xf86config`

In den meisten Fällen ist `SaX` als Konfigurations-Werkzeug dem Programm `xf86config` bei der einfachen Konfiguration des X Window System überlegen. In den wenigen Fällen aber, in denen eine Konfiguration mittels `SaX` fehlschlägt, gelingt diese in der Regel mit `xf86config`.

XFree86 4.x bringt ein ähnliches, wiederum textbasiertes `xf86config` Programm mit. Dieses hat an manchen Stellen etwas veränderte Dialoge und schreibt die Konfigurationsdatei natürlich nach `/etc/X11/XF86Config`. In der folgenden

Beschreibung wird daher nur auf das `xf86config` Programm von XFree86 3.3.x eingegangen.

Unter XFree86 4.x ist die Verwendung von `xf86config` zumeist nicht erforderlich, da hier „problematische“ Grafikkarten auch mit dem `Framebuffer` oder dem `vga` Modul konfiguriert werden können.

Zur Konfiguration müssen folgende Daten bekannt sein:

- Maus-Typ und Port, an den die Maus angeschlossen wurde, sowie die Baudrate, mit der die Maus betrieben wird (letzteres ist in der Regel optional).
- Spezifikation der Grafikkarte.
- Monitordaten (Frequenzen etc.).

Sind diese Daten bekannt bzw. liegen Monitor- und Kartenbeschreibung in greifbarer Nähe, so kann mit der Konfiguration begonnen werden. Diese kann nur vom Benutzer `root` vorgenommen werden!

Gestartet wird die Konfiguration mit:

```
erde:/root # xf86config
```

Maus

Nach der Begrüßungsseite wird im ersten Menü nach dem Maustyp gefragt. Es erscheint die folgende Auswahl:

1. Microsoft compatible (2-button protocol)
2. Mouse Systems (3-button protocol)
3. Bus Mouse
4. PS/2 Mouse
5. Logitech Mouse (serial, old type, Logitech protocol)
6. Logitech MouseMan (Microsoft compatible)
7. MM Series
8. MM HitTablet

Ausgabe 33: Auswahl der Maus für X

Bei der Festlegung des Maustyps ist zu beachten, dass viele der neueren Logitech-Mäuse Microsoft-kompatibel sind oder das MouseMan-Protocol verwenden. Die Auswahl `Bus Mouse` bezeichnet alle Typen von Busmäusen, auch Logitech!

Der passende Maustyp wird durch Angabe der davor stehenden Nummer ausgewählt. Es folgt evtl. (z. B. bei Auswahl von Typ 1) die Abfrage, ob ChordMiddle aktiviert werden soll. Dies ist bei manchen Logitech Mäusen bzw. Trackballs notwendig, um die mittlere Maustaste zu aktivieren:

```
Please answer the following question with either 'y' or 'n'.
Do you want to enable ChordMiddle?
```

Wird eine Maus mit zwei Tasten verwendet, so kann durch Beantwortung der nächsten Frage mit 'y' die Emulation eines dritten Knopfes eingeschaltet werden:

```
Please answer the following question with either 'y' or 'n'.
Do you want to enable Emulate3Buttons?
```

Zur Emulation der mittleren Maustaste muss man gleichzeitig die rechte und linke Taste drücken.

Als Nächstes wird nach der Schnittstelle gefragt, an der die Maus angeschlossen ist:

```
Now give the full device name that the mouse is connected to, for
example /dev/tty00. Just pressing enter will use the default,
/dev/mouse. Mouse device:
```

Wurde bereits bei der Systeminstallation ein Port für die Maus angegeben, so sollte hier die Vorgabe (/dev/mouse) übernommen werden.

Tastatur

Nun wird gefragt, ob der linken **(Alt)**-Taste der Wert Meta (ESC) und der rechten **(Alt)**-Taste der Wert ModeShift (AltGr) zugeordnet werden soll:

```
Please answer the following question with either 'y' or 'n'.
Do you want to enable these bindings for the Alt keys?
```

Hier sollte 'y' gewählt werden, damit die über **(Alt Gr)** erreichbaren Zeichen der deutschen Tastatur eingegeben werden können, und die linke **(Alt)**-Taste als Meta-Taste — besonders vorteilhaft bei der Arbeit mit Emacs — verwendet werden kann.

Monitor

Als Nächstes muss der Monitor spezifiziert werden. Kritisch sind die Vertikal- und die Horizontal-Frequenzen. Diese sind in der Regel im Monitorhandbuch angegeben.

Achtung

Eine Angabe von falschen Frequenzbereichen kann zur irreparablen Zerstörung des Monitors führen! Das X Window System spricht nur Video-Modi an, die den Monitor in den angegebenen Frequenzbereichen betreiben. Die Angabe von Frequenzen, für die der Monitor nicht spezifiziert ist, kann diesen überlasten!

Achtung

Für einige Monitore können auch in `/usr/X11R6/lib/X11/doc/Monitors` die Werte nachgesehen werden (ohne Gewähr).

Zur Angabe der Horizontalfrequenz wird folgende Auswahl präsentiert:

```
hsync in kHz; monitor type with characteristic modes
1 31.5;                Standard VGA, 640x480 @ 60 Hz
2 31.5 - 35.1;         Super VGA, 800x600 @ 56 Hz
3 31.5, 35.5;          8514 Compatible, 1024x768 @ 87 Hz interl.
                      (no 800x600)
4 31.5, 35.15, 35.5;   Super VGA, 1024x768 @ 87 Hz il.,
                      800x600 @ 56 Hz
5 31.5 - 37.9;         Extended Super VGA, 800x600 @ 60 Hz,
                      640x480 @ 72 Hz
6 31.5 - 48.5;         Non-Interlaced SVGA, 1024x768 @ 60 Hz,
                      800x600 @ 72 Hz
7 31.5 - 57.0;         High Frequency SVGA, 1024x768 @ 70 Hz
8 31.5 - 64.3;         Monitor that can do 1280x1024 @ 60 Hz
9 31.5 - 79.0;         Monitor that can do 1280x1024 @ 74 Hz
10 Enter your own horizontal sync range
Enter your choice (1-10):
```

Ausgabe 34: *Eingabe der Horizontalfrequenzen des Monitors*

Nur wenn die genauen Monitordaten nicht bekannt sind, sollte eine der Vorgaben übernommen werden. Mit Auswahl '10' können die genauen Frequenzen angegeben werden.

Nach Angabe der Horizontalfrequenzen werden die Vertikalfrequenzen abgefragt. Auch hier wird wieder eine Auswahl vorgegeben:

```
1 50-70
2 50-90
3 50-100
4 40-150
5 Enter your own vertical sync range
Enter your choice (1-5):
```

Ausgabe 35: *Detaillierte Vertikalfrequenzen*

Wieder sollte die Angabe der genauen Werte der Übernahme eines der Punkte '1' bis '4' vorgezogen werden.

Es wird dann die Eingabe eines Namens für die Monitorbeschreibung,

Enter an identifier for your monitor definition:

die Angabe des Herstellers,

Enter the vendor name of your monitor:

und die Modellbezeichnung

Enter the model name of your monitor:

verlangt. Hier können Sie einen entsprechenden Namen eingeben oder aber mit **(Enter)** die Vorgabewerte direkt übernehmen. Die Spezifikation des Monitors ist damit beendet.

Grafikkarte/X-Server

Weiter geht es mit der Spezifikation der verwendeten Grafikkarte:

Do you want to look at the card database?

Bei Eingabe von 'y' wird eine Auswahl von vorkonfigurierten Grafikkarten präsentiert.

Aus dieser Liste kann durch Angabe der entsprechenden Nummer eine Kartendefinition ausgewählt werden. Es sollte jedoch nicht blind eine Definition übernommen werden, da es selbst bei Karten gleichen Typs zu Variationen in Clock-Chip und RAMDAC (engl. **R**andom **A**ccess **M**emory **D**igital-to-**A**nalogue **C**onverter) kommen kann!

Aus diesem Grund wird, obwohl eine Definition ausgewählt wurde, an späteren Punkten der Konfiguration wieder nach Clock-Chip, RAMDAC, etc. gefragt. Es wird dann allerdings eine aus der Kartendefinition stammende Vorgabe als zusätzliche Option präsentiert.

Die Kartendefinitionen beinhalten Informationen zu Clock-Chip, RAMDAC und dem zu verwendenden X-Server. Außerdem werden ggf. wertvolle Hinweise zum Umgang mit der Karte in die Device-Section der Datei `XF86Config` geschrieben.

Falls die gesuchte Karte nicht aufgeführt ist, so ist das kein Grund zur Beunruhigung. In diesem Fall kann mit 'q' zur normalen Konfiguration zurückgekehrt werden. Es ist dabei zu beachten, dass eine Grafikkarte nur dann ausgewählt werden sollte, wenn diese genau mit der verwendeten Karte übereinstimmt! Die Auswahl einer Karte mit einer ähnlichen Bezeichnung ist nicht zu empfehlen. Ähnliche Namen bedeuten noch lange nicht ähnliche Hardware...

Weitere Informationen zur Konfiguration der Grafikkarte werden in Abschnitt *Installation des X Window System optimieren* auf Seite 70 beschrieben.

Nach der Spezifikation der Karte folgt die Auswahl des X-Servers:

- 1 The XF86_Mono server. This a monochrome server that should work on any VGA-compatible card, in 640x480 (more on some SVGA chipsets).
- 2 The XF86_VGA16 server. This is a 16-color VGA server that should work on any VGA-compatible card.
- 3 The XF86_SVGA server. This is a 256 color SVGA server that supports a number of SVGA chipsets. It is accelerated on some Cirrus and WD chipsets; it supports 16/32-bit color on certain Cirrus configurations.
- 4 The accelerated servers. These include XF86_S3, XF86_Mach32, XF86_Mach8, XF86_8514, XF86_P9000, XF86_AGX, XF86_W32 and XF86_Mach64.

These four server types correspond to the four different "Screen" sections in XF86Config (vga2, vga16, svga, accel).

- 5 Choose the server from the card definition, XF86_S3.

Which one of these four screen types do you intend to run by default (1-4)?

Ausgabe 36: Auswahl des X-Servers

- 1 Ein Server für monochrome (Schwarz/Weiß) Monitore. Sollte mit jeder VGA kompatiblen Grafikkarte funktionieren und zumindest eine Auflösung von 640x480 Punkten liefern.
- 2 Der 16-Farb-Server XF86_VGA16. Sollte mit jeder VGA kompatiblen Grafikkarte funktionieren.
- 3 Der SVGA-Server XF86_SVGA. Dieser 256-Farb-Server unterstützt eine große Anzahl von SVGA-Karten. Bei einigen Cirrus- und WD-Karten wird die Grafikkbeschleunigung ausgenutzt. Bei manchen Cirrus-Karten kann auch der 16- bzw. 32-Bit Farbmodus aktiviert werden.
- 4 Server für beschleunigte Grafikkarten. Hier stehen mehrere Server zur Auswahl (s. u.)
- 5 Diesen Punkt gibt es nur dann, wenn in der vorhergehenden Auswahl eine Kartendefinition ausgewählt wurde. Es wird hier der Server vorgeschlagen, der zu der ausgewählten Karte passt.

Wurde ein Server ausgewählt, so folgt die Frage, ob ein symbolischer Link vom ausgewählten Server nach `/usr/X11R6/bin/X` gemacht werden soll. Wird diese Frage mit 'y' beantwortet, so wird noch nachgefragt, ob der Link in `/var/X11R6/bin` angelegt werden soll:

```
Do you want to set it in /var/X11R6/bin?
```

Diese Frage ist unbedingt zu bejahen, da auf den `/usr`-Baum nicht unbedingt in jedem Fall geschrieben werden kann.

Anschließend erscheint ggf. (wenn in obiger Auswahl '4' angegeben wurde) ein Menü mit den verfügbaren X-Servern für beschleunigte Grafikkarten:

```
Select an accel server:
```

- 1 XF86_S3
- 2 XF86_Mach32
- 3 XF86_Mach8
- 4 XF86_8514
- 5 XF86_P9000
- 6 XF86_AGX
- 7 XF86_W32
- 8 XF86_MACH64

```
Which accel server:
```

Diese Server unterstützen jeweils die entsprechende Karte. Das Anlegen des Links setzt voraus, dass der passende Server bereits installiert wurde, d. h., dass bei der Installation des X Window System bereits der richtige Server ausgewählt wurde.


Nach der Auswahl des X-Servers muss die Grafikkarte noch näher spezifiziert werden. Als Erstes wird nach der Größe des vorhandenen Videospeichers gefragt:

```
How much video memory do you have on your video card:
```

- 1 256K
- 2 512K
- 3 1024K
- 4 2048K
- 5 4096K
- 6 Other

```
Enter your choice:
```

Ausgabe 37: Angabe des Grafikspeichers

Anschließend wird nach Name, Hersteller und Typ der Karte gefragt. Falls eine Grafikkarte ausgewählt wurde, genügt es,  zu drücken.

Enter an identifier for your video card definition:

Enter the vendor name of your video card:

Enter the model (board) name of your video card:

Wenn als X-Server ein Server für beschleunigte Grafikkarten ausgewählt wurde, wird jetzt nach dem RAMDAC-Setting gefragt. Diese sind nur für S3 und AGX Server relevant:

| | | |
|----|-----------------------------------|------------|
| 1 | AT&T 20C490 (S3 server) | att20c490 |
| 2 | AT&T 20C498/21C498/22C498 (S3) | att20c498 |
| 3 | AT&T 20C505 (S3) | att20c505 |
| 4 | BrookTree BT481 (AGX) | bt481 |
| 5 | BrookTree BT482 (AGX) | bt482 |
| 6 | BrookTree BT485/9485 (S3) | bt485 |
| 7 | Sierra SC15025 (S3, AGX) | sc15025 |
| 8 | S3 GenDAC (86C708) (autodetected) | s3gendac |
| 9 | S3 SDAC (86C716) (autodetected) | s3_sdac |
| 10 | STG-1700 (S3) | stgl1700 |
| 11 | TI 3020 (S3) | ti3020 |
| 12 | TI 3025 (S3) | ti3025 |
| 13 | TI 3020 (S3, autodetected) | ti3020 |
| 14 | TI 3025 (S3, autodetected) | ti3025 |
| 15 | TI 3026 (S3, autodetected) | ti3026 |
| 16 | IBM RGB 514 (S3, autodetected) | ibm_rgb514 |
| 17 | IBM RGB 524 (S3, autodetected) | ibm_rgb524 |
| 18 | IBM RGB 525 (S3, autodetected) | ibm_rgb525 |
| 19 | IBM RGB 526 (S3) | ibm_rgb526 |
| 20 | IBM RGB 528 (S3, autodetected) | ibm_rgb528 |
| 21 | ICS5342 (S3, ARK) | ics5342 |
| 22 | ICS5341 (W32) | ics5341 |
| 23 | IC Works w30C516 ZoomDac (ARK) | zoomdac |
| 24 | Normal DAC | normal |

Ausgabe 38: Angabe des RAMDACs

In den meisten Fällen ist es am Besten, die Eingabetaste zu drücken und keine Auswahl vorzunehmen. Wenn eine Grafikkarte ausgewählt wurde, die ein bestimmtes RAMDAC-Setting unterstützt, so wird dies angezeigt und sollte ausgewählt werden.

Nachdem diese Fragen beantwortet wurden, kann für beschleunigte Karten der Clock-Chip, sofern vorhanden, ausgewählt werden. Durch Auswahl eines Clock-Chips werden keine Clocks-Zeilen mehr benötigt, da die benötigten Clocks programmiert werden können:

| | | |
|---|--|----------|
| 1 | Chrontel 8391 | ch8391 |
| 2 | ICD2061A and compatibles (ICS9161A, DCS2824) | icd2061a |

| | | |
|----|--|------------|
| 3 | ICS2595 | ics2595 |
| 4 | ICS5342 (similar to SDAC, but not completely compatible) | ics5342 |
| 5 | ICS5341 | ics5341 |
| 6 | S3 GenDAC (86C708) and ICS5300 (autodetected) | s3gendac |
| 7 | S3 SDAC (86C716) | s3_sdac |
| 8 | STG 1703 (autodetected) | stg1703 |
| 9 | Sierra SC11412 | sc11412 |
| 10 | TI 3025 (autodetected) | ti3025 |
| 11 | TI 3026 (autodetected) | ti3026 |
| 12 | IBM RGB 51x/52x (autodetected) | ibm_rgb5xx |

Ausgabe 39: Angabe des Clockchips

Wird eine Grafikkarte ohne Clock-Chip eingesetzt, so genügt es, die Eingabetaste zu drücken, um keinen Clock-Chip auszuwählen. Wenn eine Grafikkarte im Auswahlménú ausgewählt wurde, wird der Clock-Chip, falls vorhanden, automatisch angezeigt.

Wurde kein Clock-Chip ausgewählt, schlägt xf86config vor, X -probeonly zu starten, um die von der Karte unterstützten Clock-Timings zu ermitteln. Diese werden dann automatisch in eine Clocks-Zeile in der Datei XF86Config eingetragen.

An dieser Stelle muss klar gesagt werden, warum die automatisch ermittelten und eingetragenen Clock-Timings **sehr gefährlich** sein können: Hat die Grafikkarte einen programmierbaren Clock-Chip, dann kann der X-Server beim Proben nicht zwischen den verschiedenen Clocks der Karte umschalten und erkennt deshalb nur die Clocks 0, 1 und gelegentlich 2. Alle anderen Werte sind mehr oder weniger zufällig (in der Regel wiederholen sich die Clocks 0, 1 und 2 und werden daher durch Nullen ersetzt).

Alle Clocks außer 0 und 1 hängen aber stark von der Vorprogrammierung des Clock-Chips ab, also kann Clock 2 beim Proben einen anderen Wert gehabt haben (der in die XF86Config eingetragen wurde) als bei einem späteren Start des X-Servers. Dann sind natürlich alle Timings falsch und der Monitor könnte beschädigt werden.

Ein guter Hinweis auf einen programmierbaren Clock-Chip und die damit verbundenen Probleme sind viele Nullen oder sich immer wiederholende Timing-Werte. Solche Werte dürfen keinesfalls in die Datei XF86Config übernommen werden!

Verwenden Sie also beim Ermitteln der Clock-Chips oder des Clock-Timings folgende Strategie:

- Am Besten ist es, einen vorhandenen **programmierbaren Clock-Chip** anzugeben (wenn einer vorhanden ist). Er wird dann passend programmiert, die XF86Config enthält keine Clock-Angaben. Sie können auch

die Chips auf der Karte mit den im Menü angebotenen Clock-Chips vergleichen und so den richtigen Chip herausfinden. Fast alle modernen S3-Karten haben einen programmierbaren Clock-Chip.

- Wenn Sie **keinen programmierbaren Clock-Chip** auf der Grafikkarte haben, starten Sie am Besten `X -probeonly` und vergleichen Sie die (bei unbelastetem Rechner) ermittelten Clock-Werte mit denen im Handbuch der Grafikkarte. Stimmen die Werte annähernd überein (± 2), tragen Sie diese in die Datei `XF86Config` ein.

Falls im Handbuch nichts angeführt wird, können Sie die Timing-Werte mit `X -probeonly` ermitteln lassen (am Besten auf einem unbelasteten Rechner). Prüfen Sie die ermittelten Werte auf Gültigkeit, da sich bei einigen Karten die Clock-Werte nicht auslesen lassen (viele Nullen oder sich immer wiederholende Werte deuten auf ungültige Werte). Tragen Sie gültige Werte danach selbst in die Datei `XF86Config` ein. Aber lassen sie keine Werte weg, versuchen sie nicht, Werte umzuordnen oder sonst irgendwie zu verändern. Die Werte müssen exakt in der gleichen Reihenfolge eingetragen werden.

Wird der P9000-Server benutzt, so muss einfach in beliebiger Reihenfolge für jeden Mode die gewünschte Clock in der `Clocks`-Zeile angegeben werden.

- Generell gilt: Bei programmierbaren Clock-Chips darf es keine `Clocks`-Zeile in der `XF86Config` geben (Ausnahme: P9000).

Bei Karten ohne programmierbare Clock-Chips sollte es eine „*Clocks*-Zeile“ in der `XF86Config` geben. Dadurch wird das lästige und unter Umständen gefährliche automatische Ermitteln der Clocks bei jedem Start des X Window System vermieden. Außerdem gibt es dann bei Karten mit nicht lesbaren Clocks keine falschen Werte und kein Risiko für den Monitor.

Soll jetzt (und in Kenntnis der voranstehenden Absätze) versucht werden, die Clocks automatisch zu erkennen, muss auf die Frage:

Do you want me to run 'X -probeonly' now?

mit 'y' geantwortet werden. Der Bildschirm wird dann kurz schwarz, anschließend erscheint eine Liste der erkannten Clocks oder eine Meldung, dass keine Clocks erkannt wurden. Falls ein Clock-Chip ausgewählt wurde, erscheint die Frage, ob X -probeonly gestartet werden soll, nicht, da die Clocks dann automatisch programmiert werden. In diesem Fall wird direkt zum nächsten Konfigurationspunkt gesprungen.

Achtung

Wurde die letzte Frage mit 'y' beantwortet und bleibt der Bildschirm dann länger als ca. 30 Sekunden dunkel, so sollte der Testvorgang unbedingt mit **(Strg)+(Alt)+(←)** bzw. **(Strg)+(C)** abgebrochen werden! Notfalls müssen Rechner und Monitor abgeschaltet werden, um die Hardware nicht zu gefährden!

Achtung

Abspeichern der Konfiguration

Die Konfiguration ist damit abgeschlossen. Die Konfigurationsdatei muss jedoch noch gespeichert werden. Es empfiehlt sich, die X-Window-Konfigurationsdatei `XF86Config` im Verzeichnis `/etc` zu speichern. So ist sichergestellt, dass auch im Netzwerk jeder Rechner eine „eigene“ Konfiguration hat, selbst wenn sich mehrere Rechner das `/usr`-Dateisystem teilen.

An dieser Stelle muss `/etc/XF86Config` übernommen werden! – Damit ist das Programm `xf86config` und die Konfiguration des X Window System beendet.

Installation des X Window System optimieren

Im Folgenden soll der Aufbau der Konfigurationsdatei `/etc/X11/XF86Config` vorgestellt werden. Diese Datei ist in Abschnitte (engl. *Sections*) aufgeteilt, die jeweils mit dem Schlüsselwort `Section` "bezeichner" eingeleitet werden und mit `EndSection` beendet werden. Es folgt ein grober Abriss der wichtigsten Abschnitte.

Im Anschluss erfahren Sie, wie Sie zusätzliche Fonts einbinden können, wie Sie die Eingabegeräte konfigurieren und wie die 3D-Beschleunigung realisiert wird. Dies wird natürlich auch in bestimmten Abschnitten der `XF86Config` Datei erledigt, allerdings erfordert insbesondere die Einbindung eines zusätzlichen Fonts die Hilfe externer Programme, die aber bei SuSE Linux Desktop mitgeliefert werden bzw. zur Default-Installation dazugehören. Die hier angesprochenen Vorgehensweisen sollen Ihnen die prinzipiellen Möglichkeiten verdeutlichen und als Anregung dienen und erhebt keinesfalls den Anspruch auf Vollständigkeit.

Die Programme `SaX2` und `xf86config` (für XFree86 4.x) erstellen die Datei `XF86Config`, standardmäßig in `/etc/X11`. Dies ist die primäre Konfigurationsdatei

für das X Window System. Hier finden sich die gemachten Angaben zu Maus, Monitor und Grafikkarte.

XF86Config setzt sich – wie gesagt – aus mehreren Abschnitten zusammen (den sog. „Sections“) zusammen, die sich mit jeweils einem Aspekt der Konfiguration beschäftigen. Eine Section hat stets die Form:

```
Section <Abschnittsbezeichnung>
    eintrag 1
    eintrag 2
    eintrag n
EndSection
```

Es existieren folgende Typen von Sections:

| Typ | Bedeutung |
|-------------|--|
| Files | Dieser Abschnitt beschreibt die verwendeten Pfade für Zeichensätze und die RGB-Farbtabelle. |
| ServerFlags | Hier werden allgemeine Schalter angegeben. |
| InputDevice | Über diesen Abschnitt werden die Eingabegeräte konfiguriert. Im Gegensatz zu XFree86 3.3 werden sowohl Tastaturen und Mäuse als auch spezielle Eingabegeräte (Touchtablett, Joysticks usw.) über diesen Abschnitt konfiguriert. Wichtige Bezeichner sind hier <code>Driver</code> und die Optionen, die <code>Protocol</code> und <code>Device</code> festlegen. |
| Monitor | Beschreibt den verwendeten Monitor. Elemente dieses Abschnittes sind ein Name, auf den später bei der Definition des Screens verwiesen wird, sowie die Beschreibung der Bandbreite (<code>Bandwidth</code>) und der zulässigen Synchronisationsfrequenzen (<code>HorizSync</code> und <code>VertRefresh</code>). Die Angaben erfolgen in MHz, kHz bzw. Hz. Grundsätzlich lehnt der Server jede Modeline ab, die nicht der Spezifikation des Monitors entspricht. Damit soll verhindert werden, dass durch Experimente an den Modelines versehentlich zu hohe Frequenzen an den Monitor geschickt werden. |

Tabelle 2.1: Fortsetzung auf der nächsten Seite...

| | |
|--------------|---|
| Modes | Hier werden die Darstellungsparameter der einzelnen Bildschirmauflösungen festgelegt. Diese Parameter können von <code>SqX2</code> aufgrund der vom Benutzer vorgegebenen Werte berechnet werden und müssen im Regelfall nicht verändert werden. Manuell eingreifen können Sie an dieser Stelle aber beispielsweise, wenn Sie einen Festfrequenzbildschirm anschließen möchten. Eine genaue Erläuterung der einzelnen Parameter würde den Rahmen dieses Buches sprengen, Sie finden allerdings eine detaillierte Erläuterung der Bedeutung der einzelnen Zahlenwerte in der HOWTO Datei <code>/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz</code> . |
| Device | Dieser Abschnitt definiert eine bestimmte Grafikkarte. Diese wird durch den angegebenen Namen referenziert. |
| Screen | Diese Section schließlich fügt einen Monitor und ein Device zusammen und es ergeben sich daraus die notwendigen Angaben für XFree86. Der Unterabschnitt <code>Display</code> erlaubt die Angabe der virtuellen Bildschirmgröße (<code>Virtual</code>), des <code>ViewPort</code> und der verwendeten Modes mit diesem Screen. |
| ServerLayout | Dieser Abschnitt legt das Layout einer Single- oder Multiheadkonfiguration fest. Hier werden die Eingabegeräte <code>InputDevice</code> und die Anzeigegeräte <code>Screen</code> zu einem Ganzen zusammengefasst. |

Tabelle 2.1: Abschnitte (sog. sections) in `/etc/X11/XF86Config`

Näher betrachtet werden die Sections `Monitor`, `Device` und `Screen`. In der Manual-Page von XFree86 (`man XFree86`) und Manual-Page von XF86Config (`man XF86Config`) finden sich weitere Informationen zu den verbleibenden Sections.

In XF86Config können mehrere `Monitor`- und `Device`-Abschnitte vorkommen. Auch mehrere `Screen`-Abschnitte sind möglich; welcher davon verwendet wird, hängt dann vom nachfolgenden Abschnitt `ServerLayout` ab.

Screen-Section

Zunächst soll die `Screen`-Section näher betrachtet werden. Diese bringt, wie gesagt, eine `Monitor`- mit einer `Device`-Section zusammen und bestimmt, welche Auflösungen mit welcher Farbtiefe bereitgestellt werden sollen.

Eine Screen-Section kann beispielsweise wie in Datei 1 aussehen.

```
Section "Screen"
    DefaultDepth 16
    SubSection "Display"
        Depth 16
        Modes "1152x864" "1024x768" "800x600"
        Virtual 1152x864
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"
    Monitor "Monitor[0]"
EndSection
```

Datei 1: Die Screen-Section der Datei /etc/X11/XF86Config

Die Zeile `Identifier` (hier `Screen[0]`) gibt diesem Abschnitt eine eindeutige Bezeichnung, durch die er dann im darauf folgenden Abschnitt `ServerLayout` eindeutig referenziert werden kann. Über die Zeilen `Device` und `Monitor` werden dem `Screen` eindeutig die schon weiter oben in der Datei definierte Grafikkarte und der Monitor zugeordnet. Dies sind nichts weiter als Verweise auf die `Device`- und `Monitor`-Sections mit den entsprechenden Namen bzw. „Identifiern“. Auf diese Sections wird weiter unten noch näher eingegangen.

Mittels der `DefaultColorDepth`-Angabe kann ausgewählt werden, in welcher Farbtiefe der Server startet, wenn er ohne eine explizite Angabe der Farbtiefe gestartet wird. Es folgt für jede Farbtiefe eine `Display`-Subsection. Die Farbtiefe, für die die Subsection gilt, wird durch das Schlüsselwort `Depth` festgelegt. Mögliche Werte für `Depth` sind 8, 15, 16, 24 und 32. Nicht alle X-Server-Module unterstützen jeden der Werte, 24 und 32 bpp ergeben die gleiche Farbtiefe, wobei allerdings 24 für den packed-pixel 24 bpp Modus und 32 den padded-pixel 24 bpp Modus auswählt.

Nach der Farbtiefe wird mit `Modes` eine Liste von Auflösungen festgelegt. Diese Liste wird vom X-Server von links nach rechts durchlaufen. Für jede Auflösung

wird in der Modes-Section in Abhängigkeit von der Monitor-Section eine passende Modeline gesucht, die vom Monitor und der Grafikkarte dargestellt werden kann.

Die erste in diesem Sinne passende Auflösung ist die, in der der X-Server startet (der sog. Default-Mode). Mit den Tasten (Strg) + (Alt) + (Grau +) kann in der Liste nach rechts, mit (Strg) + (Alt) + (Grau -) nach Links gewandert werden. So kann die Bildschirmauflösung zur Laufzeit des X Window Systems variiert werden.

Die letzte Zeile der Subsection Display mit Depth 16 bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe des virtuellen Bildschirms hängt vom Speicherausbau der Videokarte und der gewünschten Farbtiefe ab, nicht aber von der maximalen Auflösung des Monitors. Da moderne Grafikkarten sehr viel Grafikspeicher anbieten können Sie sehr große virtuelle Desktops anlegen. Beachten Sie dann aber bitte dass Sie evtl. keine 3D-Funktionalität mehr nutzen können wenn Sie praktisch den gesamten Grafikspeicher mit einem virtuellen Desktop füllen. Hat die Karte z. B. 16 MB Video-RAM, so kann, bei 8 Bit Farbtiefe, der virtuelle Bildschirm bis zu 4096x4096(!) Pixel groß sein. Speziell bei den beschleunigten Servern empfiehlt es sich jedoch nachdrücklich, nicht den gesamten Speicher der Videokarte für den virtuellen Bildschirm zu verwenden, da der nicht verwendete Speicherbereich auf der Videokarte von diesen Servern für verschiedene Caches für Zeichensätze und Grafikbereiche verwendet wird.

Device-Section

Eine Device-Section beschreibt eine bestimmte Grafikkarte. Es können beliebig viele Device-Sections in XF86Config enthalten sein, solange sich ihr Name, der mit dem Schlüsselwort Identifier angegeben wird, unterscheidet. In der Regel werden – falls Sie mehrere Grafikkarten eingebaut haben – die Sections einfach durchnummeriert, die erste wird dann mit Device[0], die zweite mit Device[1] bezeichnet usw. In folgenden Datei sehen Sie den Ausschnitt aus der Device Section eines Computers in dem eine Matrox Millennium PCI Grafikkarte eingebaut ist:

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"
    Driver         "mga"
    Identifier      "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

Wenn Sie `Sx2` zur Konfiguration verwenden, dann dürfte die `Device-Section` ungefähr so wie oben abgebildet aussehen. Insbesondere `Driver` und `BusID` sind natürlich von der in Ihrem Computer eingebauten Hardware abhängig und werden von `Sx2` automatisch bestimmt. Die `BusID` bestimmt den PCI- bzw. AGP-Steckplatz in den die Grafikkarte eingesteckt ist. Diese stimmt mit der vom Kommando `lspci` ausgegebenen ID überein. Beachten Sie, dass der X-Server die Angaben in dezimaler, das Programm `lspci` hingegen in hexadezimaler Schreibweise ausgibt!

Über den Parameter `Driver` legen Sie den zu verwendenden Treiber für diese Grafikkarte fest. Im Falle der Matrox Millennium heißt das Treibermodul `mga`. Diese werden vom X-Server über den im Abschnitt `Files` definierten `ModulePath` im Unterverzeichnis `drivers` gesucht. In einer Standardinstallation ist dies das Verzeichnis `/usr/X11R6/lib/modules/drivers`. Hierzu wird an den Namen einfach `_drv.o` angehängt, im Falle des `mga` Treibers wird als die Treiberdatei `mga_drv.o` geladen.

Über zusätzliche Optionen kann das Verhalten des X-Servers bzw. des Treibers beeinflusst werden. In der `Device Section` ist hier exemplarisch die Option `sw_cursor` gesetzt worden. Dies deaktiviert den Hardwaremauscursor und stellt den Mauszeiger in Software dar. Je nach Treibermodul stehen ihnen verschiedene Optionen zur Verfügung, diese sind in den Beschreibungsdateien zu den Treibermodulen im Verzeichnis `/usr/X11R6/lib/X11/doc` zu finden. Allgemein gültige Optionen finden Sie auch in der `Manual-Page` von `XF86Config` (`man XF86Config`) und `Manual-Page` von `XFree86` (`man XFree86`).

Monitor- und Modes-Section

Die `Monitor-Sections` und die `Modes Section` beschreiben, analog zu den `Device-Sections`, jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/XF86Config` kann wieder beliebig viele, unterschiedlich benannte `Monitor-Sections` enthalten. In der `ServerLayout-Section` wird dann festgelegt, welche `Monitor-Section` ausschlaggebend ist.

Für die Monitordefinition gilt, noch mehr als für die Beschreibung der Grafikkarte, dass das Erstellen einer `Monitor-Section` und insbesondere der `Modes-Section` nur von erfahrenen Benutzern gemacht werden sollte. Der wesentliche Bestandteil der `Modes-Section` sind die sog. `Modelines`, in denen Horizontal- und Vertikal-Timings für die jeweilige Auflösung angegeben werden. In der `Monitor-Section` werden die Eigenschaften des Monitors, insbesondere die zulässigen Ablenkfrequenzen, festgehalten.

Achtung

Ohne ein grundlegendes Verständnis der Funktionsweise von Monitor und Grafikkarte sollte an den Modelines nichts verändert werden, da dies u. U. zur Zerstörung des Monitors führen kann!

Achtung

Diejenigen, die sich (zu)trauen, eigene Monitorbeschreibungen zu entwickeln, sollten mit der Dokumentation im Verzeichnis `/usr/X11/lib/X11/doc` vertraut sein. Besonders zu erwähnen ist [FCR93], wo die Funktion der Hardware und das Erstellen von Modelines detailliert beschrieben wird. Eine deutsche Einführung in dieses Thema findet sich im XFree86-Kapitel in [HHMK96].

Glücklicherweise ist mittlerweile die manuelle Erstellung von Modelines oder Monitordefinitionen fast nie mehr nötig. Wenn Sie einen modernen Multisync-Monitor verwenden, können die zulässigen Frequenzbereiche und optimalen Auflösungen in der Regel, wie im `SxX2` Konfigurationsabschnitt erwähnt, direkt via DDC vom X-Server aus dem Monitor gelesen werden. Sollte dies nicht möglich sein, können Sie auch einen der eingebauten VESA-Modi des X-Servers verwenden. Diese sollten auf praktisch allen Grafikkarten/Monitorkombinationen einwandfrei funktionieren.

Zusätzliche (TrueType-)Fonts einbinden

Zu einer normalen X11R6 X-Server-Installation gehört auch eine gute Anzahl Fonts. Diese finden Sie im Verzeichnis `/usr/X11R6/lib/X11/fonts` jeweils in logisch zusammengehörigen Gruppen in Unterverzeichnissen. Beachten Sie, dass nur Unterverzeichnisse vom X-Server beachtet werden, die

- im Abschnitt `Files` der Datei `/etc/X11/XF86Config` als `FontPath` eingetragen sind.
- eine gültige `fonts.dir` Datei besitzen.
- nicht zur Laufzeit des X-Servers mit Hilfe des Kommandos `xset -fp` abgemeldet wurden.
- bzw. zur Laufzeit des X-Server mit Hilfe des Kommandos `xset +fp` eingebunden wurden.

Seit der Version 4.0 versteht XFree86 nicht nur das eigene Format `Type1` (ein PostScript-Format) für skalierbare- und `pcf` für Bitmapzeichensätze, sondern auch das `ttf` (engl. *true type font*) Dateiformat. Diese Unterstützung wird, wie

in Abschnitt *Die Version 4.x von XFree86* auf Seite 59 beschrieben, natürlich über ladbare Module des X-Servers realisiert. Sie können also auch Verzeichnisse, die TrueType-Fonts enthalten, mit dem X-Server verwenden. Hierzu sind mittlerweile praktisch keine Vorarbeiten vonnöten.

Ein großer Vorteil der meisten TrueType-Fonts, neben der sehr guten Skalierbarkeit, liegt darin, dass diese Fonts praktisch immer wesentlich mehr als die normalen 255 Zeichen des in „iso-8859-1“ kodierten Zeichensatzes für Westeuropa enthalten. Mit diesen Zeichensätzen können Sie ohne weiteres auch Kyrlisch, Griechisch oder osteuropäische Sprachen darstellen, mit spezieller Software auch asiatische Sprachen. In dieser Beschreibung soll im Wesentlichen auf die Verwendung der Zeichensätze als 8-Bit-Zeichensätze eingegangen werden. Falls Sie Zeichen asiatischer Sprachen (Japanisch, Chinesisch usw.) eingeben möchten, können Sie spezielle Editoren verwenden, die Ihnen unter SuSE Linux Desktop auch zur Verfügung stehen.

Ein 8-Bit-Zeichensatz umfasst 256 Zeichen und besteht im Wesentlichen darin, den US ASCII-Zeichensatz, der nur die ersten 128 von 256 möglichen Zeichen definiert, um weitere Zeichen zu erweitern. Ein Textzeichen belegt im Computerspeicher also 8 Bit. Da 128 Zeichen bei weitem nicht ausreichen, um die Sonderzeichen beispielsweise aller europäischen Sprachen aufzunehmen, werden die verschiedenen Sprachen in Gruppen zusammengefasst, und diese Gruppe wird dann mit einer Kurzbezeichnung bezeichnet. Der dazugehörige Zeichensatz wird nach der dazugehörigen Norm als „iso-8859-x“ Zeichensatz bezeichnet, wobei das 'x' eine Ziffer zwischen 1 und 15 ist. Die genaue Anordnung der Zeichen im Zeichensatz iso-8859-1 bzw. iso-8859-15 können Sie der Manual-Page von iso-8859-1 (man iso-8859-1) bzw. Manual-Page von iso-8859-15 (man iso-8859-15) entnehmen.

Die bekannteren Kodierungen sind in Tabelle 2.2 auf der nächsten Seite aufgeführt, weitere können Sie der oben genannten Manual-Page entnehmen.

Zeichensatz Unterstützte Regionen, enthält Sonderzeichen

| | |
|------------|--|
| iso-8859-1 | Westeuropäische Sprachen: Spanisch, Deutsch, Schwedisch, Dänisch u. a.; für Finnisch und Französisch ist nunmehr iso-8859-15 besser geeignet |
| iso-8859-2 | Zentral- und Osteuropa: Ungarisch, Tschechisch, Rumänisch, Polnisch, Deutsch u. a. |
| iso-8859-5 | Kyrillische Zeichen für Russisch |
| iso-8859-7 | Griechische Zeichen für Griechisch |

Tabelle 2.2: Fortsetzung auf der nächsten Seite...

| | |
|-------------|--|
| iso-8859-9 | Zeichen für Türkisch |
| iso-8859-15 | Weitgehend wie iso-8859-1, aber z. B. mit dem Eurozeichen und besserer Unterstützung für Finnisch und Französisch. |

Tabelle 2.2: Wichtige Zeichensatzkodierungen

Der Benutzer muss dann – je nach verwendeter Sprache – die passende Kodierung auswählen. Insbesondere bei der Übertragung von Texten zwischen verschiedenen Rechnern muss die verwendete Kodierung mitübertragen werden. Der Vorteil des Verfahrens liegt auf der Hand: Um Unterstützung für die regionalen Sonderzeichen zu erhalten, brauchen Sie nur die richtige Kodierung zu wählen und sofort können (fast) alle Programme diese Sonderzeichen darstellen, da fast alle Programme einen 8-Bit-Wert (ein Byte) zur Darstellung eines Textzeichens verwenden. Wird die falsche Kodierung gewählt, werden die Sonderzeichen allerdings falsch dargestellt. Bei den meisten X-Applikationen und auch beim KDE-Desktop können Sie die Kodierung des Zeichensatzes auswählen, meist zusammen mit der Konfiguration des zu verwendenden Zeichensatzes. In den X-Applikationen wird die Kodierung meist mit *Encoding* bezeichnet.

Der Nachteil dieser Lösung ist, dass manche Sprachkombinationen unmöglich sind: Sie können z. B. nicht ohne weiteres einen deutschen Text mit Umlauten verfassen, in dem Sie russische Ortsnamen in Kyrillisch erwähnen. Dieses Dilemma kann erst durch einen anderen Ansatz, die Verwendung von Unicode gelöst werden. Unicode kodiert Zeichen – anders als ASCII – nicht mit einem, sondern mit 2 oder noch mehr Bytes, wodurch wesentlich mehr Zeichen dargestellt werden können. Erst durch die Verwendung von Unicode können Sie auch asiatische Sprachen mit mehr als 127 Zeichen wie Chinesisch, Japanisch oder Koreanisch auf dem Rechner darstellen. Der Nachteil dieser Lösung ist, dass der Großteil der existierenden Software nicht auf den Umgang mit diesen Zeichen vorbereitet ist und Sie nur mit spezieller Software Texte mit Unicode-Zeichen lesen oder selber schreiben können. Weitere Informationen zur Verwendung von Unicode-Fonts unter Linux finden sie u. a. unter <http://www.unicode.org>. Es ist davon auszugehen, dass zukünftig mehr und mehr Programme Unicode-Zeichen unterstützen werden. Unter SuSE Linux Desktop gibt es den Editor *yudit*, um Texte in Unicode einzugeben. Sie finden es im Paket *yudit* bzw. nach der Installation über das SuSE-Menü, unter *Geschäftliches/Office* und dort unter *Editoren*.

Nach diesen Vorbetrachtungen hier nun eine Schritt-für-Schritt-Beschreibung der Installation von zusätzlichen Zeichensätzen, hier am Beispiel von TrueType-

Fonts. Machen Sie die Fonts ausfindig, die Sie in Ihrem X Window System installieren wollen. Falls Sie lizenzierte TrueType-Fonts auf Ihrem System haben, können Sie diese einfach nutzen. Mounten Sie die Partition, die diese Fonts enthält, und wechseln Sie in ein Fontverzeichnis. SuSE Linux Desktop hat schon ein Verzeichnis mit dem Namen `/usr/X11R6/lib/X11/fonts/truetype` vorbereitet, hier können Sie die betreffenden Fonts hinkopieren.

```
erde:/root # cd /usr/X11R6/lib/X11/fonts/truetype
```

Legen Sie symbolische Links auf die `ttf`-Dateien an. Setzen Sie statt `<pfad/zu/den/fonts>` den entsprechenden Pfad ein, unter dem Ihnen diese Fonts zur Verfügung stehen. Rufen Sie dann `SuSEconfig` auf, das die erforderlichen Einträge in der Datei `fonts.dir` erzeugt.

```
erde:/usr/X11R6/lib/X11/fonts/truetype #
ln -s <pfad/zu/den/fonts>/*.ttf .
```

```
erde:/usr/X11R6/lib/X11/fonts/truetype #
SuSEconfig -module fonts
```

Wenn der X-Server schon läuft, können Sie jetzt die Fonts dynamisch zur Verfügung stellen. Geben Sie hierzu ein:

```
erde:~ # xset fp rehash
```

Tipp

Das `xset`-Kommando greift über das X-Protokoll auf den X-Server zu. Es muss daher Zugriffsrechte auf den laufenden X-Server haben. Dies ist beispielsweise der Fall, wenn es sich bei `tux` um den Benutzer handelt, der den X-Server gestartet hat. Mehr hierzu finden Sie in der Manual-Page von `xauth` (`man xauth`).

Tipp

Testen Sie, ob die Fonts richtig eingerichtet wurden. Hierzu können Sie das Kommando `xlsfonts` verwenden. Wenn die Zeichensätze richtig installiert sind, so wird die Liste aller installierten Fonts inklusive der neu installierten TrueType-Fonts ausgegeben. Sie können auch den KDE-Fontmanager verwenden, der die installierten Fonts mit Beispieltext ausgibt – zu starten über das Control Center von KDE.

```
erde:~ # xlsfonts
```

Diese so eingebundenen Fonts können Sie dann in allen X-Applikationen verwenden.

| OpenGL-Treiber | Unterstützte Hardware |
|---|--|
| Mesa Software Rendering (sehr langsam) | für alle von XFree86 unterstützten Karten |
| nVidia-GLX / XFree86 4.x | nVidia Chips: alle ausser Riva 128(ZX) |
| DRI / XFree86 4.x | 3Dfx Voodoo Banshee 3Dfx Voodoo-3/4/5 Intel i810/i815/i830 Matrox G200/G400/G450/G550 ATI Rage 128(Pro)/Radeon ATI FireGL 1/2/3/4 ATI FireGL 8700/8800 SiS 300/540/630/730 3Dlabs Glint MX/Gamma |
| Mesa/Glide | 3Dfx Voodoo Graphics 3Dfx Voodoo II |

Tabelle 2.3: Unterstützte 3D-Hardware

Konfiguration von OpenGL/3D

Als 3D-Schnittstellen sind unter Linux die OpenGL- und die GLIDE-Schnittstelle für 3Dfx Voodoo-Karten bekannt. Alle aktuellen 3D-Programme verwenden inzwischen nahezu ausschließlich die OpenGL-Schnittstelle, so dass die 3D-Hardwarebeschleunigung auch bei 3Dfx Voodoo-Karten über die OpenGL-Schnittstelle realisiert werden muss. Nur ältere Programme verwenden noch die GLIDE-Schnittstelle direkt. Auch der OpenGL-Treiber für 3Dfx Voodoo-Karten macht dies. Direct3D von Microsoft steht unter Linux nicht zur Verfügung.

Hardwareunterstützung

SuSE Linux Desktop beinhaltet für die 3D-Hardwareunterstützung diverse OpenGL-Treiber. Eine Übersicht finden Sie in der Tabelle [2.3](#).

Bei einer Neuinstallation mit YoST2 kann bereits während der Installation die 3D-Unterstützung aktiviert werden, wenn eine entsprechende Unterstützung von YoST2 erkannt wird. Eine Ausnahme sind jedoch Grafikchips von nVidia.

Hier muss noch der mitgelieferte „Dummy“-Treiber durch den offiziellen Treiber von nVidia ausgetauscht werden. Verwenden Sie dazu bitte YOU (YaST Online Update) für ein Update der Pakete `NVIDIA_GLX` sowie `NVIDIA_kernel`. Sollte ein Update mit YOU nicht möglich sein, laden Sie bitte die passenden RPM-Pakete `NVIDIA_GLX` und `NVIDIA_kernel` vom nVidia-Webserver (<http://www.nvidia.com>) herunter und installieren diese mit YaST2. Aus Lizenzgründen können wir nur „Dummy“ Pakete des nVidia-Treibers mitliefern. Beachten Sie bitte weiterhin, dass bei SiS Grafikchips der Grafikspeicher im BIOS Setup auf mindestens 32 MB gesetzt werden muss, und der generische Framebuffer Support im Kernel deaktiviert werden muss.

Sollte ein Update eingespielt worden sein oder eine 3Dfx Addon Grafikkarte (Voodoo Graphics/Voodoo-2) konfiguriert werden, muss der 3D-Hardwaresupport anderweitig eingerichtet werden. Die Vorgehensweise hängt dabei vom zu verwendenden OpenGL-Treiber ab und wird im folgenden Abschnitt genauer erklärt.

OpenGL-Treiber

Mesa Software Rendering

Dieser OpenGL Treiber findet immer dann Verwendung, wenn während der Installation kein 3D-Support eingerichtet wurde oder wenn es für die Karte unter Linux keinen 3D-Support gibt.

Mesa Software Rendering sollte auch dann verwendet werden, wenn der 3D-Treiber Probleme macht (Darstellungsfehler, mangelnde Stabilität). Achten Sie bitte darauf, dass das Paket `mesa-soft` installiert ist und rufen Sie dann das Skript `switch2mesa-soft` auf. Falls Sie eine nVidia-Karte haben, sollten Sie zusätzlich noch das Skript `switch2nv` aufrufen, damit statt des `nvidia`-Treibers der `nv`-Treiber für XFree86 verwendet wird. Mit dem Kommando `3Ddiag --mesa-soft` können Sie überprüfen, ob Mesa Software Rendering korrekt konfiguriert ist.

nVidia-GLX und DRI

Diese OpenGL-Treiber können sehr komfortabel mit SaX2 eingerichtet werden. Beachten Sie bitte, dass SaX2 bei nVidia Karten noch die SuSE „Dummy“-Pakete des Treibers durch die offiziellen Pakete des Treibers vom nVidia Server mit Hilfe eines Online Updates ersetzen muss, falls dies nicht bereits geschehen ist. Mit dem Kommando `3Ddiag` können Sie überprüfen, ob die Konfiguration für nVidia-GLX bzw. DRI korrekt ist.

Aus Sicherheitsgründen dürfen nur die Benutzer der Gruppe `video` auf die 3D-Hardware zugreifen. Stellen Sie deshalb sicher, dass alle Benutzer, die auf

der Maschine lokal arbeiten, in der Gruppe `video` eingetragen sind. Ansonsten wird für OpenGL-Programme der sehr langsame *Software Rendering Fallback* des OpenGL-Treibers verwendet. Mit dem Kommando `id` können Sie überprüfen, ob der aktuelle Benutzer der Gruppe `video` angehört. Ist dies nicht der Fall, kann er mittels `Yast2` zu dieser Gruppe hinzugefügt werden.

Mesa/Glide

Dieser OpenGL-Treiber kann nur manuell mit Hilfe der Information, die das Kommando `3Ddiag -mesaglide` liefert, konfiguriert werden. Details dazu finden Sie im Abschnitt [Diagnose-Tool 3Ddiag](#) auf dieser Seite. Beachten Sie bitte, dass Sie beim Mesa/Glide-Treiber OpenGL-starten müssen, da nur dieser Zugriff auf die Hardware hat. Dazu muss der gerade eingeloggte Benutzer sein (`DISPLAY`) für `root` freigeben. Dies können Sie mit dem Kommando `xhost localhost` erreichen. Des Weiteren muss die Auflösung, die das OpenGL Programm verwendet, von GLIDE unterstützt werden (unterstützte Auflösungen: 640×480 und 800×600). Anderenfalls kommt es zum sehr langsamen *Software Rendering Fallback* des OpenGL-Treibers.

Diagnose-Tool 3Ddiag

Um die 3D-Konfiguration unter SuSE Linux Desktop überprüfen zu können, steht das Diagnosetool `3Ddiag` zur Verfügung. Beachten Sie bitte, dass es sich dabei um ein Kommandozeilentool handelt, das Sie in einem Terminal aufrufen müssen.

Das Programm überprüft dabei beispielsweise die XFree86-Konfiguration, ob die entsprechenden Pakete für 3D-Support installiert sind, und ob die korrekte OpenGL-Bibliothek sowie GLX Extension verwendet wird. Befolgen Sie bitte die Anweisungen von `3Ddiag`, wenn es zu "failed" Meldungen kommt. Im Erfolgsfall werden ausschließlich "done" Meldungen auf dem Bildschirm ausgegeben. Für den Mesa/Glide OpenGL-Treiber kann die 3D-Konfiguration über diese Diagnose nur relativ mühsam eingerichtet werden, wenn der 3D-Support nicht bereits während der Installation aktiviert wurde.

Mit `3Ddiag -h` lassen sich zulässige Optionen für `3Ddiag` ermitteln.

OpenGL-Testprogramme

Als OpenGL-Testprogramme eignen sich neben `gears` und `glxinfo` Spiele wie `tuxracer` und `armagetron` (gleichnamige Pakete). Bei aktiviertem 3D-Support sollten sich diese auf einem halbwegs aktuellen Rechner flüssig spielen lassen. Mit Mesa Software Rendering ist dies nicht möglich bzw. nicht zumutbar (Diashow-Effekt).

Troubleshooting

Sollte sich der OpenGL 3D-Test als negativ herausstellen (kein flüssiges Spielen möglich), sollte erst mit 3Ddiag überprüft werden, ob keine Fehlkonfiguration vorliegt ("failed" Meldungen) und diese ggf. behoben werden. Hilft auch das nicht oder lagen keine failed Meldungen vor, hilft oft nur noch ein Blick in die Logdateien von XFree86. Oft findet man hier in `/var/log/XFree86.0.log` von XFree86 4.x die Zeile "DRI is disabled". Dafür kann es mehrere Ursachen geben, die sich jedoch nur mit genauem Studium der Logdatei finden lassen, womit der Laie in aller Regel überfordert ist.

In diesen Fällen liegt in der Regel kein Konfigurationsfehler vor, da dieser bereits von 3Ddiag erkannt worden wäre. Somit bleibt ohnehin nur der Mesa Software Rendering OpenGL-Treiber, der jedoch keinerlei 3D-Hardware-Support bietet. Man sollte ebenfalls auf die Verwendung von Mesa Software Rendering zurückgreifen und somit auf 3D-Hardwarebeschleunigung verzichten, wenn sich OpenGL Darstellungsfehler oder gar Stabilitätsprobleme ergeben sollten.

Installationssupport

Abgesehen von Mesa Software Rendering befinden sich unter Linux alle OpenGL-Treiber im Entwicklungsstadium und sind deshalb zum Teil noch als experimentell anzusehen. Wir haben uns dennoch entschlossen, die Treiber auf der Distribution mitzuliefern, da die Nachfrage nach 3D-Hardwarebeschleunigung unter Linux sehr groß ist. Aufgrund des z. T. experimentellen Stadiums der OpenGL-Treiber können wir im Rahmen des Installationsupports jedoch nicht auf das Einrichten von 3D-Hardwarebeschleunigung eingehen und bei diesbezüglichen Problemen nicht weiterhelfen. Das grundlegende Einrichten der grafischen Benutzeroberfläche X11 beinhaltet also keinesfalls auch das Einrichten von 3D-Hardwarebeschleunigung.

Wir hoffen jedoch, dass dieses Kapitel viele Fragen zu diesem Thema beantwortet. Bei Problemen mit dem 3D-Hardwaresupport empfehlen wir Ihnen im Zweifelsfall die Verwendung von Mesa Software Rendering, wie bereits im Abschnitt *Mesa Software Rendering* auf Seite 81 beschrieben.

Weiterführende Online Dokumentation

- nVidia-GLX: `/usr/share/doc/packages/nv_glx/`,
`/usr/src/kernel-modules/nv_glx/README` (Pakete `NVIDIA_GLX`
und `NVIDIA_kernel` vom nVidia Server)

- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (Paket `xf86`)
- Mesa/Glide: `/usr/share/doc/packages/mesa3dfx/` (Paket `mesa3dfx`)
- Mesa allgemein: `/usr/share/doc/packages/mesa/` (Paket `mesa`)

Booten und Bootmanager

Im Folgenden werden verschiedene Methoden vorgestellt, wie sich das fertig installierte System booten lässt. Um das Verständnis der einzelnen Methoden zu erleichtern, werden zunächst einige technische Details des Bootprozesses erläutert. Im Anschluss daran folgen Erläuterungen zu den beiden Bootmanagern GRUB und LILO.

Wenn Sie ein Update von einer früheren Version durchführen, die LILO benutzte, wird auch wieder LILO eingerichtet. Bei einer Neuinstallation wird dagegen GRUB verwendet, außer die Root-Partition wird auf einem Raidsystem oder LVM installiert.

| | |
|--|-----|
| Der Bootvorgang auf dem PC | 86 |
| Bootkonzepte | 87 |
| Map Files, GRUB und LILO | 88 |
| Booten mit GRUB | 89 |
| Booten mit LILO | 92 |
| Bei Bootproblemen: Boot-CD erstellen | 100 |

Der Bootvorgang auf dem PC

Nach dem Einschalten des Rechners werden vom BIOS (engl. *Basic Input Output System*) Bildschirm und Tastatur initialisiert sowie der Hauptspeicher getestet. Bis zu diesem Zeitpunkt verfügt der Rechner über keine Massenspeichermedien.

Anschließend werden Informationen über aktuelles Datum, Zeit und die wichtigsten Peripherie-Geräte aus den CMOS-Werten (*CMOS setup*) ausgelesen. Da nun die erste Festplatte einschließlich ihrer Geometrie bekannt sein sollte, kann das Laden des Betriebssystems von dort beginnen.

Dazu wird von der ersten Festplatte der physikalisch erste Datensektor von 512 Byte Größe in den Speicher geladen und die Kontrolle geht auf das Programm zu Beginn dieses Sektors über. Die Abfolge der auf diese Weise ausgeführten Anweisungen bestimmt den weiteren Ablauf des Bootvorgangs. Die ersten 512 Byte auf der ersten Festplatte werden deshalb auch als *Master Boot Record* (MBR) bezeichnet.

Bis zu diesem Zeitpunkt (Laden des MBR) läuft der Bootvorgang völlig unabhängig vom installierten System auf jedem PC immer gleich ab und der Computer hat bis dahin für den Zugriff auf die Peripherie lediglich die im BIOS gespeicherten Routinen (Treiber) zur Verfügung.

Master Boot Record

Die Struktur des MBR ist durch eine betriebssystemübergreifende Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen. Ohne die Partitionstabelle gibt es keine Dateisysteme, d. h. die Festplatte ist praktisch nicht zu verwenden. Die letzten 2 Byte müssen eine feste „magische Zahl“ (AA55) enthalten: ein MBR, der dort etwas anderes stehen hat, wird vom BIOS und von allen PC-Betriebssystemen als ungültig angesehen.

Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplatten-Partitionen, außer bei der erweiterten Partition, die nur ein „Behälter“ für andere Partitionen ist. Diese Bootsektoren bieten 512 Byte Platz und sind dazu gedacht, Code aufzunehmen, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Grunddaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen – auch nach der Anlage

eines Dateisystems – von Hause aus erst einmal leer! Eine Linux-Partition ist daher *nicht von selbst startbar*, auch wenn sie einen Kernel und ein gültiges Root-Dateisystem enthält.

Ein Bootsektor mit gültigem Systemstart-Code trägt in den letzten 2 Byte dieselbe „magische“ Kennung wie der MBR (AA55).

Booten von DOS oder Windows 95/98

Im DOS-MBR der ersten Festplatte ist ein Partitionseintrag als *aktiv* (engl. *bootable*) gekennzeichnet, was bedeutet, dass dort nach dem zu ladenden System gesucht werden soll. Deshalb muss DOS zwingend auf der ersten Festplatte installiert sein. Der DOS-Programmcode im MBR ist die erste Stufe des Bootloaders (engl. *first stage bootloader*) und überprüft, ob auf der angegebenen Partition ein gültiger Bootsektor vorhanden ist.

Falls dies der Fall ist, kann der Code in diesem Bootsektor als „zweite Stufe“ des Bootloaders (engl. *secondary stage loader*) nachgestartet werden. Dieser lädt nun die Systemprogramme, und schließlich erscheint der gewohnte DOS-Prompt bzw. es startet die Windows 95/98-Oberfläche.

Unter DOS lässt sich nur eine einzige primäre Partition als aktiv markieren. Folglich kann das DOS-System nicht auf logischen Laufwerken in einer erweiterten Partition untergebracht werden.

Bootkonzepte

Das einfachste „Bootkonzept“ betrifft einen Rechner mit einem einzigen Betriebssystem. Die Abläufe in der Startphase in diesem Fall haben wir soeben geschildert. Ein solcher Bootvorgang ist auch für einen Nur-Linux-Rechner denkbar. Dann kann theoretisch auf die Installation von GRUB oder LILO verzichtet werden, allerdings wäre es so nicht möglich, dem Kernel während des Startens eine Kommandozeile (mit Spezialwünschen zum Startvorgang, zusätzlichen Hardware-Informationen usw.) mitzugeben. Sobald mehr als ein Betriebssystem auf einem Rechner installiert ist, bieten sich verschiedene Bootkonzepte an:

Zusätzliche Systeme von Diskette booten Ein Betriebssystem wird von Platte geladen, mit Hilfe von Boot-Disketten können alternativ weitere Betriebssysteme vom Disketten-Laufwerk aus gestartet werden.

- *Bedingung:* Ein bootfähiges Diskettenlaufwerk ist vorhanden.

- *Beispiel:* Sie installieren Linux zusätzlich zu Ihrem Windows-System und starten Linux stets von Bootdiskette.
- *Vorteil:* Sie ersparen sich die Bootloader-Installation.
- *Nachteile:* Sie müssen *sehr* darauf bedacht sein, einen Sicherheitsvorrat funktionierender Bootdisketten zu haben und der Start dauert länger.
- Dass Ihr Linux ohne Bootdiskette nicht starten kann, mag je nach beabsichtigtem Einsatz Ihres Rechners ein Vor- oder Nachteil sein.

Installation eines Bootmanagers Ein Bootmanager erlaubt, mehrere Systeme gleichzeitig auf einem Rechner zu halten und sie abwechselnd zu nutzen. Der Benutzer wählt das zu ladende System bereits während des Bootvorgangs aus; ein Wechsel erfordert den Neustart des Rechners. Bedingung ist dabei, dass der gewählte Bootmanager mit allen Betriebssystemen „harmoniert“.

Map Files, GRUB und LILO

Das größte Problem beim Booten eines Betriebssystems besteht darin, dass der Kernel eine Datei auf einem Dateisystem auf einer Partition auf einer Festplatte ist. Für das BIOS allerdings sind Dateisysteme und Partitionen völlig unbekannte Konzepte.

Um dieses Problem zu umgehen, wurden so genannte „Maps“ und „Map Files“ eingeführt. In den Maps werden die physikalischen Blöcke auf der Festplatte notiert, die von den logischen Dateien belegt sind. Wenn so eine Map verarbeitet wird, lädt das BIOS die physikalischen Blöcke in der Reihenfolge, wie sie in der Map-Datei angegeben ist, und baut so die logische Datei im Speicher auf.

Der Hauptunterschied zwischen LILO und GRUB besteht nun darin, dass LILO sich fast vollständig auf Maps verlässt, während GRUB versucht, sich so bald als möglich während des Bootens von den festen Maps zu lösen. Dies erreicht GRUB durch *File System Code*, der es ermöglicht, auf Dateien durch die Pfadangabe zuzugreifen und nicht mehr durch die Blocknummern.

Dieser Unterschied hat historische Gründe. In den frühen Tagen von Linux kämpften viele verschiedenen Dateisysteme um die Vorherrschaft. Werner Almesberger entwickelte einen Bootloader (LILO), der nicht wissen musste, auf welchem Filesystem der zu bootende Kernel angelegt war. Die Idee hinter GRUB geht sogar noch weiter zurück in die Tage des traditionellen Unix und BSD. Diese hatten sich gewöhnlich auf ein Dateisystem festgelegt und am Anfang desselben einen bestimmten Platz für den Bootloader reserviert. Dieser Bootloader

kannte die Struktur des Dateisystems, in das er eingebunden war, und fand dort die Kernel mit ihren Namen im root-Verzeichnis.

Ein weiterer fundamentaler Unterschied besteht darin, dass der LILO Bootcode in 16-bit Assembler geschrieben ist, während GRUB weitestgehend in 32-bit portablen C-Code implementiert ist. Die Auswirkungen zu beschreiben, übersteigt allerdings den Rahmen dieses Buches.

Der folgende Abschnitt beschreibt die Installation und Konfiguration eines Bootmanagers am Beispiel von GRUB. Im Anschluss wird auf die Unterschiede bei der Verwendung von LILO eingegangen. Eine vollständige Beschreibung von LILO finden Sie in [Alm96]. Diese Anleitung finden Sie unter: `/usr/share/doc/packages/lilo/user.dvi`. Lesen Sie den Text am Bildschirm mit Programmen wie `xdvi` oder drucken Sie den Text mit dem Befehl: `lpr /usr/share/doc/packages/lilo/user.dvi`

Booten mit GRUB

Wie auch LILO besteht GRUB auch aus zwei Stufen — eine erste 512-Byte-Stufe, die in den MBR oder einen Partitions-Boot-Block geschrieben wird, und eine größere zweite Stufe („stage2“), die durch eine Map-Datei gefunden wird. Ab diesem Punkt jedoch unterscheidet sich GRUB von LILO. stage2 kann auf Dateisysteme zugreifen. Derzeit werden ext2, ext3, reiser FS, jfs, xfs, minix und das von Windows verwendete DOS FAT FS unterstützt. Die Dateien eines solchen Dateisystems auf einem unterstützten BIOS-Disk-Device (Floppy oder vom BIOS erkannte Festplatten) können angezeigt, als Befehl oder Menüdatei verwendet oder als Kernel oder `initrd` in den Speicher geladen werden, lediglich durch Ausführung des entsprechenden Befehls, gefolgt vom BIOS-Device und einem Pfad.

Der größte Unterschied zu LILO besteht darin, dass, wenn GRUB einmal installiert ist, Kernel- und Menüeinträge ohne weiteres Zutun hinzugefügt oder geändert werden können. GRUB wird beim Booten dynamisch die Inhalte der Dateien finden und erneut einlesen.

Das Menü

Nach erfolgter Installation ist die Menüdatei die wichtigste GRUB-Datei für den Anwender. Diese befindet sich standardmäßig unter `/boot/grub/menu.lst`. Sie enthält alle Informationen zu anderen Partitionen oder Betriebssystemen, die mithilfe des Menüs gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder erfolgten Änderung an der Datei zu aktualisieren — verwenden Sie einfach YaST2 oder Ihren favorisierten Editor.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen vor dem ersten Parameter. Kommentare werden durch einen Hash (`'#'`) eingeleitet.

Zur Erkennung der Menüeinträge in der Menüübersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als selektierbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrages ausgeführt.

Einfachster Fall ist das Verzweigen zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Boot-Block einer anderen Partition in GRUBs „Block-Notation“, zum Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen unter GRUB werden in Abschnitt [Namen für BIOS-Geräte](#) auf der nächsten Seite erklärt. Obiges Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Kommando `kernel` wird ein Kernel-Image spezifiziert. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel auf der Kommandozeile übergeben.

Wenn der Kernel nicht die erforderlichen Treiber für den Zugriff auf die `root`-Partition einkompiliert hat, dann muss `initrd` angegeben werden. Hierbei handelt es sich um einen separaten GRUB-Befehl, der den Pfad zur `initrd`-Datei als einziges Argument hat. Da die Ladeadresse der `initrd` in das bereits geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den `kernel`-Befehl folgen.

Der Befehl `root` vereinfacht die Spezifikation der Kernel- und `initrd`-Dateien. `root` hat als einziges Argument entweder ein GRUB-Device oder eine Partition auf einem solchen. Allen Kernel-, `initrd`- oder anderen Dateipfaden, bei denen nicht explizit ein Device angegeben wird, wird bis zum nächsten `root`-Befehl das Device vorangestellt. Dieser Befehl kommt in einer während der Installation generierten `menu.lst` nicht vor.

Am Ende jeden Menüeintrags steht implizit das `boot`-Kommando, so dass dieses nicht in die Menüdatei geschrieben werden muss. Sollten Sie jedoch in die Situation kommen, GRUB interaktiv zum Booten zu benutzen, müssen Sie am

Ende das `boot`-Kommando eingeben. `boot` hat keine Argumente, es führt lediglich das geladene Kernel-Image oder den angegebenen Chain Loader aus. Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Andernfalls wird der erste (Eintrag 0) verwendet. Sie haben auch die Möglichkeit, einen Timeout in Sekunden anzugeben, nach dem dies geschehen soll. `timeout` und `default` werden üblicherweise vor die Menüeinträge geschrieben.

Namen für BIOS-Geräte

Die Herkunft von GRUB zeigt sich in der Weise, wie es Namen an BIOS-Devices vergibt. Es wird ein BSD-ähnliches Schema verwendet: die Diskettenlaufwerke `0x00`, `0x01` werden `fd0` und `fd1` genannt und alle Festplatten (`0x80`, `0x81`, `0x82`), die vom BIOS oder durch Zusatz-Controller erkannt werden, werden als `hd0`, `hd1` etc. bezeichnet, unabhängig vom Typ des Controllers. Das Problem, dass Linux-Device-Namen nicht eindeutig zu BIOS-Device-Namen zugeordnet werden können, besteht für sowohl LILU als auch GRUB. Beide benutzen vergleichbare Algorithmen, um diese Zuordnung zu generieren. Jedoch speichert GRUB diese Zuordnung in einer Datei (`device.map`), die bearbeitet werden kann.

Hinweis

Die Zählung der Partitionen in GRUB beginnt bei Null. (`hd0,0`) entspricht der ersten Partition auf der ersten Festplatte; in einem gewöhnlichen Desktop-Rechner mit einer Platte als „Primary Master“ angeschlossen lautet der Device-Name `/dev/hda1`.

Hinweis

Festplattenpartitionen werden durch Anhängen eines Kommas und der Partitionsnummer spezifiziert. Ein kompletter GRUB-Pfad besteht aus einem Device-Namen, der in Klammern geschrieben wird sowie dem Pfad der Datei in dem Dateisystem auf der angegebenen Partition. Der Pfad wird durch einen Slash eingeleitet. Als Beispiel, auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition, könnte der bootbare Kernel wie folgt aussehen

```
(hd0,0)/boot/vmlinuz
```

Installation mit der GRUB-Shell

GRUB existiert in zwei Versionen. Einmal als Bootloader und einmal als normales Linux-Programm. Dieses Programm wird als *GRUB shell* bezeichnet. Die

Funktionalität, GRUB als Bootloader auf eine Festplatte oder Diskette zu installieren, ist direkt in GRUB integriert in Form der Kommandos `install` oder `setup`. Damit ist sie in der GRUB shell verfügbar, wenn Linux läuft und GRUB beim Booten geladen wurde. Dadurch vereinfacht sich die Rettung eines defekten Systems.

Nur wenn es als Linux-Programm läuft, kommt der Zuordnungsalgorithmus ins Spiel. Das Programm liest die Datei `device.map`, welche aus Zeilen besteht, die jeweils GRUB-Device und Linux-Device-Namen enthalten. Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der `device.map` festzulegen. Sollten Sie Probleme beim Booten haben, kontrollieren Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht. Die Datei befindet sich im GRUB-Verzeichnis `/boot/grub/`.

Weiterführende Informationen

Auf der Webseite <http://www.gnu.org/software/grub/> finden Sie ausführliche Informationen zu GRUB in den Sprachen Deutsch, Englisch und Japanisch. Das Online-Handbuch existiert allerdings nur in Englisch.

Wenn `texinfo` auf dem Rechner installiert ist, können Sie sich in der Shell mit `info grub` die Info-Seiten zu GRUB anzeigen lassen. Suchen Sie auch in der Support-Datenbank sdb.suse.de nach dem Stichwort GRUB, um Informationen zu speziellen Themen zu erhalten.

Booten mit LILO

Der Linux-Bootloader LILO ist für die Installation im MBR geeignet. LILO hat Zugriff auf beide im Real-Modus bekannten Festplatten und ist bereits von seiner Installation her in der Lage, alle benötigten Daten auf den „rohen“ Festplatten, ohne Informationen zur Partitionierung, zu finden. Deshalb lassen sich auch Betriebssysteme von der zweiten Festplatte booten. Die Einträge in der Partitionstabelle werden im Gegensatz zum DOS-Bootvorgang ignoriert.

Der Hauptunterschied zum DOS-Bootvorgang besteht in der Möglichkeit, beim Booten zwischen dem Laden verschiedener installierter Betriebssysteme wählen zu können. Nach dem Laden des MBR in den Speicher wird LILO gestartet; LILO bietet nun dem Benutzer die Auswahl aus einer Liste vorinstallierter Systeme an. Er kann beim Systemstart Bootsektoren von Partitionen laden, um ein Betriebssystem von dieser Partition zu starten, oder den Linux-Kernel laden und

Linux starten. Zudem bietet er die wichtige Gelegenheit, dem Linux-Kernel eine Kommandozeile mitzugeben. Zu Sicherheitszwecken können die LILO-Dienste ganz oder teilweise passwortgeschützt werden.

Grundlagen

Die LILO-Startmaschinerie umfasst die folgenden Bestandteile:

- *LILO-Bootsektor* mit einem Anfangsstück („erste Stufe“) des LILO-Codes, das den eigentlichen LILO beim Systemstart aktiviert.
- LILO-Maschinencode, standardmäßig in `/boot/boot-menu.b`
- *Map-Datei* (`/boot/map`), in der LILO bei seiner Installation einträgt, wo die Linux-Kernel und sonstigen Daten, die er braucht, zu finden sind.
- optional: die *Message-Datei* `/boot/message`, die standardmäßig eine graphische LILO-Bootauswahl erzeugt.
- die verschiedenen Linux-Kernel und Bootsektoren, die LILO zum Starten anbieten soll.

Achtung

Jeder Schreibzugriff (auch durch Dateiverschiebung) auf einen dieser Bestandteile macht die Map-Datei ungültig und daher eine *Neu-Installation von LILO* erforderlich (siehe auf Seite 98)! Dies betrifft vor allem den Wechsel zu einem neuen Linux-Kernel.

Achtung

Für den LILO-Bootsektor stehen folgende Installationsziele zur Auswahl:

Auf einer Diskette Dies ist die einfachste, aber auch langsamste Methode, mit LILO zu booten. Wählen Sie diese Methode, wenn Sie den bestehenden Bootsektor nicht überschreiben wollen.

Im Bootsektor einer primären Linux-Partition der ersten Festplatte
Diese Variante lässt den MBR unberührt. Vor dem Booten muss diese Partition mit `fdisk` als aktiv markiert werden. Rufen Sie dazu als `root` `fdisk -s <Partition>` auf. `fdisk` fragt Sie nun nach einer Eingabe. `'m'` gibt Ihnen eine Liste der möglichen Eingaben und mit `'a'` können Sie die angegebene Partition startbar machen.

Im Master Boot Record Diese Variante bietet die größte Flexibilität. Insbesondere ist dies die einzige Möglichkeit, Linux von Festplatte aus zu booten, wenn sämtliche Linux-Partitionen auf der zweiten Festplatte liegen und auf der ersten keine erweiterte Partition zur Verfügung steht. Eine Veränderung des MBR birgt aber bei unsachgemäßer Installation auch gewisse Risiken.

Wenn Sie bisher einen anderen Bootmanager verwendet haben... ... und ihn weiterverwenden wollen, gibt es, je nach dessen Fähigkeiten, noch weitere Möglichkeiten. Ein häufiger Fall: Sie haben eine primäre Linux-Partition auf der zweiten Platte, von der aus Sie Linux starten wollen. Ihr anderer Bootmanager wäre imstande, diese Partition über den Bootsektor zu starten. Dann können Sie diese Partition startbar machen, indem Sie LILO in deren Bootsektor installieren und sie dem anderen Bootmanager als startbar melden.

LILO-Konfiguration

Als flexibler Bootmanager bietet LILO zahlreiche Möglichkeiten, seine Konfiguration den individuellen Erfordernissen anzupassen. Die wichtigsten Optionen und ihre Bedeutung werden im Folgenden erläutert. Für eine umfassende Beschreibung sei auf [Alm96] verwiesen.

Die Konfiguration von LILO wird in der Datei `/etc/lilo.conf` eingetragen. Es ist ratsam, die bei der letzten LILO-Installation verwendete Konfigurationsdatei sorgfältig aufzubewahren und vor jeder Änderung eine Sicherheitskopie herzustellen. Eine Änderung wird erst wirksam, indem Sie LILO mit der neuesten Fassung der Konfigurationsdatei neu installieren (Abschnitt [Installation und Deinstallation von LILO](#) auf Seite 98)!

Der Aufbau der Datei lilo.conf

Die `/etc/lilo.conf` beginnt mit einem *globalen Abschnitt* (engl. *global options section*) mit allgemeinen Einstellungen, gefolgt von einem oder mehreren *System-Abschnitten* (engl. *image sections*) für die einzelnen Betriebssysteme, die LILO starten soll. Ein neuer Systemabschnitt wird jeweils eingeleitet durch eine Zeile mit der Option `image` oder `other`.

Die Reihenfolge der einzelnen Betriebssysteme in der `lilo.conf` ist nur insofern von Bedeutung, als das *zuerst* in der Liste aufgeführte System automatisch gebootet wird, wenn keine Benutzereingabe erfolgt – gegebenenfalls nach Ablauf einer vorkonfigurierten Wartezeit (s. u. die Optionen `delay` und `timeout`).

Datei 2 zeigt eine Beispielkonfiguration auf einem Rechner mit Linux und Windows. Beim Booten sollen zur Auswahl stehen: ein neuer Kernel (/boot/vmlinuz) und ein Linux-Kernel als Fallback (/boot/vmlinuz.shipped, so wie Windows auf /dev/hda1 und das Programm Memtest86.

```
### LILO global section
boot      = /dev/hda          # LILO installation target: MBR
backup    = /boot/MBR.hda.990428 # backup file for the old MBR
                                   # 1999-04-28
vga       = normal           # normal text mode (80x25 chars)
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32     # Use BIOS to ignore
                                   # 1024 cylinder limit

prompt
password = q99iwr4           # LILO password (example)
timeout = 80                 # Wait at prompt for 8 s before
                                   # default is booted
message = /boot/message      # LILO's greeting

### LILO Linux section (default)
image = /boot/vmlinuz        # Default
label = linux
root   = /dev/hda7           # Root partition for the kernel
initrd = /boot/initrd

### LILO Linux section (fallback)
image = /boot/vmlinuz.shipped
label = Failsafe
root   = /dev/hda7
initrd = /boot/initrd.suse
optional

### LILO other system section (Windows)
other = /dev/hda1           # Windows partition
label = windows

### LILO Memory Test
image = /boot/memtest.bin
label = memtest86
```

Datei 2: Beispielkonfiguration in /etc/lilo.conf

In /etc/lilo.conf ist alles von einem # bis zum Zeilenende Kommentar. Er wird – ebenso wie Zwischenraum – von LILLO ignoriert und kann zur Verbesserung der Lesbarkeit verwendet werden. Zunächst werden die unbedingt notwendigen Einträge besprochen, die weiteren Optionen sind im anschließenden Abschnitt *Der Aufbau der Datei lilo.conf* auf der vorherigen Seite beschrieben.

■ Globaler Abschnitt (Parameterteil)

▷ `boot=<bootdevice>`

Device auf dessen erstem Sektor der LILO-Bootsektor installiert werden soll (das Installationsziel).

`<bootdevice>` kann sein: ein Diskettenlaufwerk (`/dev/fd0`), eine Partition (z. B. `/dev/hdb3`), oder eine ganze Platte (z. B. `/dev/hda`): letzteres bedeutet die Installation im MBR.

Voreinstellung: Fehlt diese Angabe, wird LILO auf der gegenwärtigen Linux-Rootpartition installiert.

▷ `lba32`

Diese Option umgeht die 1024-Zylinder-Grenze von LILO. Dies funktioniert natürlich nur, wenn das BIOS Ihres Rechners dies auch unterstützt.

▷ `prompt`

Erzwingt das Erscheinen der LILO-Eingabeaufforderung (Prompt). Die Voreinstellung ist: kein Prompt! (Vgl. Abschnitt *Der Aufbau der Datei lilo.conf* auf Seite 94, Option `delay`.)

Empfohlen, sobald LILO mehr als nur ein System starten soll. Zusammen damit sollte auch die `timeout`-Option gesetzt werden, damit ein automatischer Reboot möglich ist, wenn keine Eingabe erfolgt.

▷ `timeout=<zehntelsekunden>`

Setzt eine Auszeit für die Wahl des zu startenden Systems und ermöglicht dadurch das automatische Booten, wenn nicht rechtzeitig eine Auswahl erfolgt. `<zehntelsekunden>` ist dabei die verbleibende Zeit in Zehntelsekunden für eine Eingabe. Durch Drücken von (↑) wird diese Funktion außer Kraft gesetzt und der Rechner wartet auf Ihre Eingabe. Die Voreinstellung ist 80.

■ Linux-Abschnitt

▷ `image=<kernelimage>`

Hier muss der Name des zu bootenden Kernel-Images stehen. Dies wird in der Regel `/boot/vmlinuz` sein.

▷ `label=<name>`

Innerhalb der `/etc/lilo.conf` eindeutiger, aber sonst frei wählbarer Name für das System (z. B. `Linux`). Maximale Länge 15 Zeichen: möglichst nur Buchstaben, Ziffern und Unterstrich – keine Leerzeichen, Sonderzeichen wie deutsche Umlaute u. Ä. Die

genauen Regeln für erlaubte Zeichen finden Sie in [Alm96], Abschnitt 3.2.1. Voreinstellung: der Dateiname des Kernel-Images (z. B. `/boot/vmlinuz`).

Unter diesem Namen wählen Sie beim Systemstart das gewünschte Betriebssystem aus. Bei mehreren Systemen empfiehlt es sich, eine nähere Beschreibung der Namen und Systeme in einer message-Datei (siehe Abschnitt *Der Aufbau der Datei `lilo.conf`* auf Seite 94, Option `message`) bereitzustellen.

▷ `root=<rootdevice>`

Damit gibt LILO dem Kernel die Rootpartition (z. B. `/dev/hda2`) des Linux-Systems an. Zur Sicherheit empfohlen! Wird diese Option weggelassen, nimmt der Kernel die in ihm selbst eingetragene Rootpartition `<kernelimage>`.

■ Linux-Abschnitt (Linux – Safe Settings)

Auch wenn ein eigener Kernel installiert wurde, ist es immer möglich, auf diesen Kernel zurückzugreifen und das System zu starten.

▷ `optional`

Sollte `/boot/vmlinuz.shipped` gelöscht werden (*nicht* empfehlenswert!), wird bei der LILO-Installation dieser Abschnitt ohne Fehlermeldung übergangen.

■ Anderes System

▷ `other=<partition>`

Mit `other` werden LILO Startpartitionen anderer Systeme zum Booten bekannt gemacht (z. B. `/dev/hda1`).

▷ `label=<name>`

Wählen Sie hier einen Name für dieses System. Die Voreinstellung – der bloße Device-Name der Partition – ist beim Booten nicht sehr aussagekräftig.

■ Memory Test

Hier ist nur das Programm zum Testen des Speichers eingetragen.

Im diesem Abschnitt wurden nur die in `/etc/lilo.conf` minimal nötigen Einträge besprochen. Weitere nützliche Einstellungen entnehmen Sie bitte der Manual-Page von `lilo.conf`, die Sie mit dem Befehl `man lilo.conf` erhalten.

Installation und Deinstallation von LILO

Achtung

Vergewissern Sie sich vor der Installation von LILO *auf jeden Fall*, dass Sie eventuell vorhandene andere Betriebssysteme von Diskette booten können (funktioniert nicht bei Windows XP/2000/NT)! Vor allem fdisk muss zur Verfügung stehen. SuSE Linux kann gegebenenfalls auch von der Installations-CD bzw. -DVD gebootet werden.

Achtung

Installation nach Änderung der Konfiguration

Wenn sich an den LILO-Komponenten etwas geändert hat oder wenn Sie Ihre Konfiguration in `/etc/lilo.conf` modifiziert haben, müssen Sie LILO neu installieren. Dies geschieht durch einfachen Aufruf des sog. *Map-Installers*:

```
erde:~ # /sbin/lilo
```

LILO legt daraufhin ein Backup des Ziel-(Boot-)Sektors an, schreibt seine „erste Stufe“ in diesen Sektor und erzeugt eine neue Map-Datei (siehe auf Seite 93). LILO meldet nacheinander die installierten Systeme – z. B. im Fall unser obigen Beispielkonfiguration:

```
Added linux *
Added suse
Added windows
Added memtest86
```

Nach abgeschlossener Installation kann der Rechner neu gestartet werden:

```
erde:~ # shutdown -r now
```

Nachdem das BIOS seinen Systemtest ausgeführt hat, meldet sich LILO mit seiner Eingabeaufforderung, an der Sie LILO Parameter für den Kernel übergeben und das gewünschte Bootimage auswählen können. Mit Tab lassen sich die Bezeichnungen der installierten Konfigurationen auflisten.

Entfernen von LILO

Um LILO zu deinstallieren, wird der Bootsektor, in dem LILO installiert worden ist, mit seinem früheren Inhalt überschrieben. Unter Linux ist das kein Problem, *wenn* ein gültiges Backup vorhanden ist (vgl. Abschnitt [Der Aufbau der Datei](#)

lilo.conf auf Seite 94, Option `backup`). Auch YaST2 kann Sie in diesem Fall unterstützen.

Achtung

Ein Bootsektor-Backup wird ungültig, wenn die betreffende Partition ein neues Dateisystem erhalten hat. Die Partitionstabelle in einem MBR-Backup wird ungültig, wenn die betreffende Festplatte zwischenzeitlich anders partitioniert worden ist. Solche Backups sind „Zeitbomben“: am Besten sofort löschen!

Achtung

Ursprünglichen Windows-MBR wiederherstellen

Einen DOS- oder Windows-MBR stellt man mit dem folgenden MS-DOS-Befehl (verfügbar ab DOS-Version 5.0) wieder her:

```
C:\> fdisk /MBR
```

Oder unter OS/2 mit dem Befehl:

```
C:\> fdisk /newmbr
```

Diese Befehle schreiben nur die 446 ersten Bytes (den Boot-Code) in den MBR zurück und lassen die gegenwärtige Partitionstabelle unangetastet. Außer, wenn der MBR (siehe auf Seite 86) wegen einer falschen „magischen Zahl“ als im ganzen ungültig behandelt wird: dann wird die Partitionstabelle genullt! *Nicht vergessen:* Mit `fdisk` die von jetzt an gewünschte Startpartition wieder als *aktiv* (engl. *bootable*) kennzeichnen; die MBR-Routinen von DOS, Windows, OS/2 brauchen das!

Ansonsten legen Sie zunächst von dem fraglichen LILO-Sektor ein weiteres frisches Backup an – sicher ist sicher. Dann prüfen Sie, ob Ihre alte Backup-Datei die richtige ist und ob sie genau 512 Byte groß ist. Schließlich spielen Sie diese mit den folgenden Befehlen zurück:

- Wenn LILO in Partition `yyyy` (z. B. `hda1`, `hda2`, ...) residiert:

```
erde:~ # dd if=/dev/yyyy of=Neue-Datei bs=512 count=1
erde:~ # dd if=Backup-Datei of=/dev/yyyy
```

- Wenn LILO im MBR der Platte `zzz` (z. B. `hda`, `sda`) residiert:

```
erde:~ # dd if=/dev/zzz of=Neue-Datei bs=512 count=1
erde:~ # dd if=Backup-Datei of=/dev/zzz bs=446 count=1
```

Der letzte Befehl ist „vorsichtig“ und schreibt gleichfalls nicht in die Partitionstabelle. Auch hier *nicht vergessen*: Mit `fdisk` anschließend die von jetzt an gewünschte Startpartition wieder als *aktiv* (engl. *bootable*) kennzeichnen.

Windows XP MBR wiederherstellen

Booten Sie von der Windows XP CD, drücken Sie im Setup die Taste **(R)**, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows XP Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

Windows 2000 MBR wiederherstellen

Booten Sie von der Windows 2000 CD, drücken Sie im Setup die Taste **(R)**, sowie im darauf folgenden Menü die Taste **(K)**, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows 2000 Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

Bei Bootproblemen: Boot-CD erstellen

Falls Sie Probleme haben, Ihr installiertes System über einen Bootmanager zu booten oder Lilo oder Grub nicht in den MBR Ihrer Festplatte, noch auf eine Diskette installieren wollen oder können, ist es auch möglich, eine bootfähige CD zu erstellen, auf die Sie die Linux Startdateien brennen. Voraussetzung hierfür ist natürlich, dass ein Brenner in Ihrem System vorhanden und eingerichtet ist.

Boot-CD mit ISOLINUX

Um eine bootfähige CD zu erstellen, ist es am einfachsten, den Bootmanager Isolinux zu verwenden. Auch die SuSE Installations-CDs werden übrigens per Verwendung von Isolinux bootfähig gemacht.

- Booten Sie Ihr installiertes System zunächst auf folgendem Umweg: Legen Sie die Installations-CD oder -DVD und booten Sie von dieser wie bei der Installation. Wählen Sie dann im Bootmenü die Option 'Installation' aus und im nächsten Menu den Punkt 'Installiertes System booten'. Dabei wird die root-Partition automatisch erkannt, sodass von dieser das System gebootet werden kann.
- Installieren Sie mit Hilfe von YaST2 das Paket `syslinux`.
- Öffnen Sie eine Root-Shell. Mit Hilfe der folgenden Aufrufe wird für die Boot-CD ein temporäres Verzeichnis erstellt und die zum Booten des Linux Systems notwendigen Dateien (der Bootloader Isolinux sowie der Kernel und die Initrd) hineinkopiert.

```
erde:~ # mkdir /tmp/CDroot
erde:~ # cp /usr/share/syslinux/isolinux.bin /tmp/CDroot/
erde:~ # cp /boot/vmlinuz /tmp/CDroot/linux
erde:~ # cp /boot/initrd /tmp/CDroot
```

- Mit Ihrem Lieblingstexteditor erstellen Sie nun die Bootloader-Konfigurationsdatei `/tmp/CDroot/isolinux.cfg`. Wenn Sie z. B. `pico` verwenden wollen, lautet der entsprechende Aufruf

```
pico /tmp/CDroot/isolinux.cfg
```

Tragen Sie folgenden Inhalt ein:

```
DEFAULT linux
LABEL linux
    KERNEL linux
    APPEND initrd=initrd root=/dev/hdXY [bootparameter]
```

Für den Parameter `root=/dev/hdXY` tragen Sie bitte Ihre root-Partition ein. Wenn Sie sich nicht sicher sind, welche Partitionsbezeichnung diese hat, schauen Sie einfach in der Datei `/etc/fstab` nach. Für den Wert `[bootparameter]` können Sie zusätzliche Optionen eingeben, die beim Booten verwendet werden sollen. Die Konfigurationsdatei könnte z. B. folgendermaßen aussehen:

```
DEFAULT linux LABEL linux KERNEL linux APPEND initrd=initrd
root=/dev/hda7 hdd=ide-scsi
```

- Anschließend wird mit folgendem Aufruf aus den Dateien ein ISO9660-Dateisystem für die CD erstellt (schreiben Sie das folgende Kommando in eine Zeile):

```
mkisofs -o /tmp/bootcd.iso -b isolinux.bin -c boot.cat  
-no-emul-boot -boot-load-size 4  
-boot-info-table /tmp/CDroot
```

- Dann kann die Datei `/tmp/bootcd.iso` auf CD gebrannt werden, entweder mit graphischen Brennprogrammen wie K3b oder einfach von der Kommandozeile:

```
cdrecord -v speed=2 dev=0,0,0 /tmp/bootcd.iso -eject
```

Evtl. muss der Parameter `dev=0,0,0` an die SCSI-ID des Brenners angepasst werden (diese erfahren Sie durch Eingabe des Aufrufs `cdrecord -scanbus`, vgl. auch Manual-Page von `cdrecord` (`man cdrecord`)).

- Probieren Sie die Boot-CD aus! Rebooten Sie dazu den Computer und überprüfen Sie ob Ihr Linux-System korrekt von der CD gestartet wird.

Hotplug

Mittlerweile werden in vielen Computern Hardwarekomponenten verwendet, die zur Laufzeit des Systems angeschlossen und wieder abgenommen werden können. Neben USB, als bekanntestes Beispiel für diese Komponenten, gibt es auch noch PCI, PCMCIA, Firewire, SCSI und andere Schnittstellen.

Hotplug-Systeme haben die Aufgabe, neue angeschlossene bzw. eingebaute Hardware zu erkennen und diese automatisch betriebsbereit einzurichten. Des Weiteren müssen Komponenten, die wieder entnommen werden sollen, auf diese Entnahme vorbereitet werden bzw. Ressourcen wieder frei gegeben werden, wenn Komponenten ohne Vorwarnung entfernt wurden.

| | |
|---|-----|
| Realisierung von Hotplug in Linux | 104 |
| Hotplug starten und Coldplug | 104 |
| USB | 105 |
| PCI und PCMCIA | 106 |
| Netzwerk | 107 |
| Firewire (IEEE1394) | 108 |
| Sonstige Geräte und weitere Entwicklung | 109 |

Realisierung von Hotplug in Linux

Für gewöhnlich überwachen so genannte Daemons Teile eines Systems auf externe Ereignisse, so überwacht z. B. der `inetd` eingehende Netzwerkankfragen. Der Daemon bei Hotplug ist der Kernel selbst. Dazu müssen die Treiber eines Busses in der Lage sein, neue Geräte zu erkennen und diese auf einheitlichen Weg dem System mitzuteilen. Im Kernel 2.4 sind USB, PCMCIA, Firewire, teilweise PCI und das Netzwerksystem dazu in der Lage. Dieser Teil von Hotplug ist in den jeweiligen Modulen fest eingebaut und lässt sich ohne Kerneländerung nicht weiter beeinflussen.

Hinweis

PCMCIA-Geräte werden nur dann von Hotplug behandelt, wenn diese CardBus-Karten sind und das Kernel PCMCIA-System gewählt wurde. Sie erscheinen dann als PCI-Geräte. Genauere Information finden Sie dazu im Abschnitt über PCMCIA.

Hinweis

Der zweite Teil von Hotplug leitet die notwendigen Schritte zum Einbinden von Geräten bzw. deren Herauslösen ein und ist eine Sammlung von Skripten im Verzeichnis `/etc/hotplug` mit dem zentralen Skript `/sbin/hotplug`. Dieses Skript ist die Schnittstelle zwischen dem Kernel und der Hotplug-Skriptensammlung.

Im weiteren Verlauf des Kapitels werden wir mit „Hotplug-System“ diese Skripte bezeichnen.

Wenn ein hotplugfähiges Gerät angeschlossen oder entfernt wird, ruft der Kernel das Skript `/sbin/hotplug` auf und übergibt zusätzliche Informationen über die entsprechende Hardwarekomponente. Dieses Skript verteilt die Arbeit – je nach Art der Hardware – an weitere Skripte. Diese laden bzw. entladen die Kernelmodule und rufen wiederum weitere Programme zur Konfiguration der Komponenten auf. Die Programme liegen in `/etc/hotplug` und enden immer mit `.agent`.

Hotplug starten und Coldplug

Obwohl der Kernel immer Hotplugereignisse an `/sbin/hotplug` weitergibt, muss das Hotplug-System erst einmal gestartet werden. Solange Hotplug nicht gestartet ist, werden alle entsprechenden Ereignisse verworfen.

Außerdem gibt es Komponenten, die vom Kernel schon erkannt werden bevor überhaupt ein Zugriff auf das Dateisystem möglich ist. Diese Ereignisse gehen

einfach verloren. Deshalb wird in den Skripten `/etc/hotplug/*.rc` versucht, für bereits vorhandene Hardware diese Ereignisse künstlich zu erzeugen. In diesem Zusammenhang wird auch von „Coldplug“ gesprochen.

Falls zu diesem Zeitpunkt die USB-Basismodule noch nicht geladen sind, werden diese geladen und das USB-Gerätedateisystem (`usbdevfs`) eingehängt.

Wird Hotplug durch einen Aufruf von `rchotplug stop` angehalten, werden keine weiteren Ereignisse mehr ausgewertet. Wer nie während des Betriebs seine Hardware verändert, kann Hotplug auch vollständig deaktivieren. Allerdings muss dann auf andere Art und Weise für die Einrichtung von USB- oder PCMCIA-Geräten gesorgt werden.

Im Verzeichnis `/etc/sysconfig/hotplug` gibt es einige Variablen, die das Verhalten von Hotplug steuern. So kann z. B. mit der Variable `<HOTPLUG_DEBUG>` die „Gesprächigkeit“ von Hotplug beeinflusst werden. Über die Variablen `<HOTPLUG_START_USB>`, `<HOTPLUG_START_PCI>` und `<HOTPLUG_START_NET>` kann eingestellt werden, dass nur Ereignisse bestimmten Typs verarbeitet werden. Alle weiteren Variablen sind in den entsprechenden Unterabschnitten näher erläutert.

Alle Meldungen von Hotplug werden immer in der Datei (`/var/log/messages`) (Systemlog) protokolliert.

USB

Wenn ein neues USB-Gerät angeschlossen wird, ermittelt das Skript `/etc/hotplug/usb.agent` einen geeigneten Treiber und stellt sicher, dass dieser geladen ist. Dieser Treiber muss nicht unbedingt ein Kernelmodul sein, so werden viele USB Kameras direkt von Anwendungsprogrammen angesprochen.

Die Zuordnung von Treibern zur Hardware ist mehrstufig: Als Erstes wird in der Datei `/etc/hotplug/usb.usermap` nachgesehen, ob diese Hardware von einem Anwendungsprogramm bzw. einem speziellen Initialisierungsskript bedient werden soll. Falls das nicht zutrifft, wird in `/etc/hotplug/usb.handmap` nach einer individuellen Zuordnung zu einem Kernelmodul gesucht. Wenn auch dort nichts gefunden wurde (was in den meisten Fällen zutrifft), wird letztendlich die Zuordnungstabelle des Kernels `/lib/modules/<kernelversion>/modules.usbmap` befragt. Des Weiteren wird hier nochmal ein USB-Hardwarescan durchgeführt, der bei der Verwendung von KDE als grafische Oberfläche weitere Aktionen auslöst. Zum Beispiel wird für Geräte, die zum ersten Mal verwendet werden, ein geeignetes YaST-Modul zur Konfiguration angeboten oder Applikationen zur Verwendung mit dem neuen Gerät werden gestartet. Dieser Mechanismus läuft parallel zu den anderen Aktionen, die von `/etc/hotplug/usb.agent` ausgelöst werden.

USB-Geräte werden vom `usb.agent` je nach Typ unterschiedlich behandelt:

Speichergeräte wie z. B. Festplatten werden vom Skript `path/usr/sbin/checkhotmounts` behandelt, sobald die erforderlichen Treiber geladen sind.

Netzwerkgeräte erzeugen ein eigenes Hotplugereignis im Kernel, sobald diese registriert werden. Der `usb.agent` hinterlegt lediglich Hardwareinformationen, die später vom Netzwerkereignis verwendet werden. Dies ist nur eine vorübergehende Lösung für den Kernel 2.4 und versagt, wenn mehrere USB-Netzwerkgeräte verwendet werden. Dies kommt jedoch nur sehr selten vor.

Kameras werden über den `Hardwarescan/KDE`-Mechanismus angesprochen. Dazu werden allerdings noch via `/etc/hotplug/usb/usbcam` die Zugriffsrechte der Gerätedatei für den eingeloggten Benutzer gesetzt, damit dieser unter KDE darauf zugreifen kann.

Mäuse benötigen nur ein geladenes Modul, welches hier geladen wird, um sofort verwendet zu werden.

Tastaturen werden schon beim Bootvorgang benötigt und werden deshalb nicht von Hotplug behandelt.

ISDN/Modem wird derzeit noch nicht automatisch eingerichtet.

Es gibt noch einige USB-spezifische Variablen in `/etc/sysconfig/hotplug`. In `<HOTPLUG_USB_HOSTCONTROLLER_LIST>` stehen die Treiber für den USB-Controller in der Reihenfolge, wie sie zu laden versucht werden. Wird ein Treiber erfolgreich geladen, werden in `<HOTPLUG_USB_MODULES_TO_UNLOAD>` die Module eingetragen, die beim Entfernen der Komponente wieder entladen werden sollen. Alle nachfolgenden Module für USB werden nicht entladen, weil nicht sicher entschieden werden kann, ob sie noch von einem Gerät benötigt werden. Die Variable `<HOTPLUG_USB_NET_MODULES>` enthält die Namen der Module, die ein Netzwerkinterface zur Verfügung stellen. Sobald eines dieser Module geladen wird, wird eine Hardwarebeschreibung zur späteren Verwendung beim Netzwerkereignis abgelegt. Dieser Vorgang wird im Systemlog protokolliert.

PCI und PCMCIA

Bei PCMCIA-Karten muss sorgfältig unterschieden werden, da außer CardBus-Karten keine PC-Carten von Hotplug behandelt werden; diese wiederum auch

nur dann, wenn das Kernel PCMCIA-System aktiv ist. Dieser Sachverhalt wird im PCMCIA-Kapitel im Abschnitt Software (xxPCMCIA-SOFTWARExx) genauer erklärt.

CardBus-Karten sind technisch gesehen beinahe PCI-Geräte. Deshalb werden beide von demselben Hotplug-Skript `/etc/hotplug/pci.agent` behandelt. Dort wird im Wesentlichen ein Treiber für die Karte ermittelt und geladen. Außerdem wird eine Information darüber, wo die neue Karte angeschlossen wurde (PCI-Bus/PCMCIA-Slots und die Slotnummer) abgelegt, damit ein nachfolgendes Hotplug-Netzwerk-Ereignis diese Information lesen und die richtige Konfiguration auswählen kann.

Die Treiberzuordnung ist hier zweistufig: Zuerst wird in der Datei `/etc/hotplug/pci.handmap` nach individuellen Einstellungen gesucht und falls nichts gefunden wurde, wird in der PCI-Treibertabelle des Kernels `/lib/modules/⟨kernelversion⟩/modules.pcimap` gesucht. Wer also die Treiberzuordnung verändern möchte, sollte dazu `/etc/hotplug/pci.handmap` anpassen, da die andere Tabelle bei einem Kernelupdate überschrieben wird.

Anders als bei USB werden keine besonderen Aktionen je nach Art der PCI- oder CardBus-Karte ausgeführt. Bei Netzwerkkarten erzeugt der Kernel ein Hotplug-Netzwerkereignis, das die Einrichtung des Interfaces veranlasst. Bei allen anderen Karten müssen weitere Aktionen manuell ausgeführt werden. Das Hotplug-System wird aber diesbezüglich noch erweitert.

Sobald die Karte entfernt wird, werden auch die verwendeten Module wieder entladen. Falls das Entfernen bei bestimmten Modulen zu Problemen führt, kann dies verhindert werden, indem die Modulnamen in `/etc/sysconfig/hotplug` in die Variable `⟨HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD⟩` geschrieben werden.

Netzwerk

Sobald im Kernel ein neues Netzwerkinterface an- oder abgemeldet wird, erzeugt dieser ein Hotplug-Netzwerkereignis. Dieses wird von `/etc/hotplug/net.agent` ausgewertet. Gegenwärtig werden dort nur Ethernet-, Tokenring- und WirelessLAN-Interfaces berücksichtigt. Für alle anderen Arten von Netzwerken wie Modem oder ISDN gibt es andere Mechanismen. Auch Netzwerkinterfaces, die von PCMCIA-Karten bereitgestellt werden und nicht von Hotplug, sondern vom Cardmanager behandelt werden, werden hier nicht behandelt. Es erscheint dann eine entsprechende Meldung im Systemlog.

Zuerst wird zu ermitteln versucht, welche Hardware das Interface bereitstellt. Da der Kernel 2.4 solche Information nicht liefern kann, wird eine Information

verwendet, die bei dem vorangegangenen USB- oder PCI-Hotplug-Ereignis bereitgestellt wurde. Obwohl dies in den meisten Fällen gut funktioniert, ist es als vorübergehende Notlösung zu betrachten. Es dürfen deswegen nämlich nicht zwei Netzwerkkarten gleichzeitig angeschlossen werden. Sollten Sie mehrere hotplugfähige Netzwerkkarten verwenden, dann verbinden Sie diese bitte nacheinander mit dem Computer. Ein zeitlicher Abstand von wenigen Sekunden genügt. Diese Informationsübermittlung wird in `/var/log/messages` protokolliert.

Mit dieser Information über die zugrunde liegende Hardware wird dann das Skript `/sbin/ifup` (bzw. `ifdown`) aufgerufen. `ifup` ist so in der Lage, einer bestimmten Karte immer die richtige Konfiguration zuzuweisen, auch wenn das Interface einen anderen Namen hat. Interfacenamen werden vom Kernel nämlich nicht gezielt zugeordnet.

Weitere individuelle Aktionen, die Sie ausführen lassen möchten, nachdem ein neues Netzwerkinterface angelegt wurde, können Sie in `/sbin/ifup` einhängen. Details dazu finden sich in der Manpage zu Manual-Page von `ifup` (`man ifup`). Es ist auch möglich, je nach angeschlossener Hardware unterschiedliche Defaulttrouten zu verwenden; siehe dazu Manual-Page von `route` (`man route`).

Falls die automatische Ermittlung der Hardware hinter dem Interface fehlschlägt (z. B. bei Firewire) und nur ein hotplugfähiges Netzwerkgerät verwendet wird, dann kann die Beschreibung der Netzwerkhardware in `/etc/sysconfig/hotplug` in die Variable `<HOTPLUG_NET_DEFAULT_HARDWARE>` geschrieben werden. Diese Zeichenkette muss dem entsprechen, was von `/sbin/ifup` zur Zuordnung der richtigen Konfiguration verwendet werden soll. In der Variable `<HOTPLUG_NET_TIMEOUT>` wird festgelegt, wie lange `net.agent` auf eine dynamisch erzeugte Hardwarebeschreibung wartet.

Firewire (IEEE1394)

Für Firewire-Geräte werden derzeit nur die Treibermodule geladen. Um einen Überblick zu bekommen, wie stark Firewire-Hardware unter unseren Kunden verbreitet ist, können Sie uns über unser Feedback-Webfrontend <http://www.suse.de/feedback> kontaktieren.

Sonstige Geräte und weitere Entwicklung

Alle hier nicht beschriebenen Arten von hotplugfähiger Hardware werden gegenwärtig (noch) nicht behandelt. Hotplug unterliegt aber zur Zeit einer starken Entwicklung, die jedoch sehr von den Fähigkeiten des Kernels abhängt. Es ist zu erwarten, dass zusammen mit dem nächsten Kernel 2.6 wesentlich bessere Möglichkeiten geboten werden.

Konfiguration und mobiles Arbeiten mit Notebooks

An Notebooks werden besondere Anforderungen gestellt. Hierzu zählen unter anderem Power Management (APM/ACPI), Infrarot-Schnittstellen (IrDA) und PC-Karten (PCMCIA). Gelegentlich sind auch in Desktop-Rechnern solche Komponenten zu finden; sie unterscheiden sich nur unwesentlich von den in Notebooks verwendeten Spezifika – deshalb wird deren Verwendung und Konfiguration in diesem Kapitel zusammengefasst.

| | |
|--|-----|
| PCMCIA | 112 |
| SCPM – System Configuration Profile Management | 123 |
| APM und ACPI – Powermanagement | 131 |
| IrDA – Infrared Data Association | 138 |

PCMCIA

PCMCIA steht für „Personal Computer Memory Card International Association“ und wird als Sammelbegriff für sämtliche damit zusammenhängende Hard- und Software verwendet.

Die Hardware

Die wesentliche Komponente ist die PCMCIA-Karte; hierbei unterscheidet man zwei Typen:

PC-Karten Das sind die derzeit noch am häufigsten vorkommenden Karten. Sie verwenden einen 16 Bit breiten Bus zur Datenübertragung, sind meist relativ günstig und werden i. d. R. problemlos und stabil unterstützt.

CardBus-Karten Dies ist ein neuerer Standard. Sie verwenden einen 32 Bit breiten Bus, sind dadurch schneller, aber auch teurer. Da die Datenübertragungsrate aber häufig an anderer Stelle eingeschränkt wird, lohnt sich der Aufwand häufig nicht. Es gibt mittlerweile auch für diese Karten etliche Treiber, wobei manche immer noch instabil sind – abhängig auch vom vorhandenen PCMCIA-Controller.

Welche Karte eingeschoben ist, sagt bei aktivem PCMCIA-Dienst das Kommando `cardctl ident`. Eine Liste von unterstützten Karten findet man in `SUPPORTED/_CARDS` in `/usr/share/doc/packages/pcmcia`. Dort gibt es auch die jeweils aktuelle Version des PCMCIA-HOWTO.

Die zweite notwendige Komponente ist der PCMCIA-Controller, oder auch die PC-Card/CardBus-Bridge. Diese stellt die Verbindung zwischen der Karte und dem PCI-Bus her, in älteren Geräten auch die Verbindung zum ISA-Bus. Diese Controller sind fast immer zu dem Intel-Chip i82365 kompatibel; es werden alle gängigen Modelle unterstützt. Der Typ des Controllers lässt sich mit dem Kommando `probe` ermitteln. Falls es ein PCI-Gerät ist, liefert auch das Kommando `lspci -vt` interessante Informationen.

Die Software

Unterschiede zwischen den beiden existierenden PCMCIA-Systemen

Gegenwärtig gibt es zwei PCMCIA Systeme, externes PCMCIA und Kernel-PCMCIA. Das externe PCMCIA System von David Hinds ist das ältere, somit auch besser erprobte und wird immer noch weiterentwickelt. Die Quellen der

verwendeten Module sind nicht in die Kernelquellen integriert, deshalb „externes“ System. Seit Kernel 2.4 gibt es alternative Module in den Kernelquellen. Diese bilden das Kernel PCMCIA System. Die Basismodule wurden von Linus Torvalds geschrieben und unterstützen vor allem neuere CardBus Bridges besser.

Leider sind diese beiden Systeme zueinander inkompatibel. Außerdem gibt es in beiden Systemen unterschiedliche Sätze von Kartentreibern. Deswegen kommt je nach verwendeter Hardware nur ein System in Frage. Die Voreinstellung in SuSE Linux Desktop ist das neuere Kernel PCMCIA. Es ist jedoch möglich, das System zu wechseln. Dazu muss in der Datei `/etc/sysconfig/pcmcia` der Variablen `(PCMCIA_SYSTEM)` entweder `external` oder `kernel` zugewiesen und PCMCIA mit `rcpcmcia restart` neu gestartet werden. Für vorübergehende Wechsel können Sie auch `rcpcmcia [re]start external, kernel` verwenden. Detailinformationen dazu befindet sich in `/usr/share/doc/packages/pcmcia/LIESMICH.SuSE`.

Die Basismodule

Die Kernelmodule für beide Systeme befinden sich in den Kernelpaketen. Zusätzlich werden noch die Paket `pcmcia` und `hotplug` benötigt.

Beim Start von PCMCIA werden die Module `pcmcia_core`, `i82365` (externes PCMCIA) oder `yenta_socket` (Kernel-PCMCIA) und `ds` geladen. In sehr seltenen Fällen wird alternativ zu `i82365` bzw. `yenta_socket` das Modul `tcic` benötigt. Sie initialisieren die vorhandenen PCMCIA-Controller und stellen Basisfunktionen zur Verfügung.

Der Cardmanager

Da PCMCIA-Karten zur Laufzeit gewechselt werden können, muss es einen Daemonen geben, der die Aktivitäten in den Steckplätzen überwacht. Diese Aufgabe erledigen je nach gewähltem PCMCIA System und verwendeter Hardware der Cardmanager oder das Hotplug System des Kernels. Bei externem PCMCIA kommt nur der Cardmanager zum Einsatz. Bei Kernel-PCMCIA handelt der Cardmanager nur die PC-Card Karten, wohingegen CardBus Karten von Hotplug behandelt werden. Der Cardmanager wird vom PCMCIA Startskript nach dem Laden der Basismodule gestartet. Da Hotplug neben PCMCIA auch noch andere Subsysteme bedient, gibt es hierfür ein eigenes Startskript. (Siehe auch Kapitel [Hotplug](#) auf Seite 103).

Ist eine Karte eingeschoben, ermittelt der Cardmanager bzw. Hotplug Typ und Funktion und lädt die passenden Module. Wurden diese erfolgreich geladen,

startet der Cardmanager bzw. Hotplug je nach Funktion der Karte bestimmte Initialisierungsskripten, die ihrerseits die Netzwerkverbindung aufbauen, Partitionen von externen SCSI-Platten einhängen (mounten) oder andere hardware-spezifische Aktionen ausführen. Die Skripte des Cardmanager befinden sich in `/etc/pcmcia`. Die Skripte für Hotplug sind in `/etc/hotplug` zu finden. Wenn die Karte wieder entfernt wird, beendet der Cardmanager bzw. Hotplug mit den selben Skripten die diversen Kartenaktivitäten. Anschließend werden die nicht mehr benötigten Module wieder entladen.

Sowohl der Startvorgang von PCMCIA als auch die Kartenereignisse werden im Systemlog (`/var/log/messages`) protokolliert. Dort wird festgehalten, welches PCMCIA System gerade verwendet wird und welcher Daemon welche Skripte zur Einrichtung verwendet hat. Theoretisch kann eine PCMCIA Karte einfach entnommen werden. Dies funktioniert auch hervorragend für Netzwerk-, Modem- oder ISDN-Karten, solange keine aktiven Netzwerkverbindungen mehr bestehen. Es funktioniert nicht im Zusammenhang mit eingehängten Partitionen einer externen Platte oder mit NFS-Verzeichnissen. Hier müssen Sie dafür sorgen, dass die Einheiten synchronisiert und sauber ausgehängt werden (unmounten). Das ist natürlich nicht mehr möglich, wenn die Karte bereits gezogen wurde. Im Zweifelsfall hilft ein

```
cardctl eject
```

Dieser Befehl deaktiviert alle Karten, die sich noch im Notebook befinden. Um nur eine der Karten zu deaktivieren, können Sie zusätzlich die Slotnummer angeben, z. B. `cardctl eject 0`.

Die Konfiguration

Ob PCMCIA bzw. Hotplug beim Booten gestartet wird, lässt sich mit dem YaST2 Runleveleditor oder auf der Kommandozeile mittels `chkconfig` einstellen .

In `/etc/sysconfig/pcmcia` befinden sich vier Variablen:

⟨`PCMCIA_SYSTEM`⟩ bestimmt, welches PCMCIA System verwendet wird.

⟨`PCMCIA_PCIC`⟩ enthält den Namen des Moduls, das den PCMCIA-Controller ansteuert. Im Normalfall ermittelt das Startskript diesen Namen selbstständig. Nur wenn dies fehlschlägt, kann das Modul hier eingetragen werden. Ansonsten sollte diese Variable leer bleiben.

⟨`PCMCIA_CORE_OPTS`⟩ ist für Parameter für das Modul `pcmcia_core` gedacht; sie werden aber nur selten benötigt. Diese Optionen sind in Manual-Page von `pcmcia_core` (`man pcmcia_core`) beschrieben.

`(PCMCIA_PCIC_OPTS)` nimmt Parameter für das Modul `i82365` auf. Auch hierzu gibt es eine Manpage Manual-Page von `i82365` (`man i82365`). Falls `yenta_socket` verwendet wird, werden diese Optionen ignoriert, da `yenta_socket` keine Optionen kennt.

Die Zuordnung von Treibern zu PCMCIA Karten für den Cardmanager befindet sich in den Dateien `/etc/pcmcia/config` und `/etc/pcmcia/*.conf`. Zuerst wird `config` gelesen und dann die `/*.conf` in alphabetischer Reihenfolge. Der zuletzt gefundene Eintrag für eine Karte ist ausschlaggebend. Details über die Syntax dieser Dateien befinden sich in der Manual-Page von `pcmcia` (`man pcmcia`).

Die Zuordnung von Treibern zu PCMCIA Karten für Hotplug wird im Kapitel über Hotplug beschrieben (siehe [Hotplug](#) auf Seite 103).

Netzwerkkarten (Ethernet, Wireless LAN und TokenRing)

Diese lassen sich wie gewöhnliche Netzwerkkarten mit YaST2 einrichten. Dort muss lediglich 'PCMCIA' als Kartentyp ausgewählt werden. Alle weiteren Details zur Netzwerkeinrichtung befinden sich im Netzwerkkapitel. Beachten Sie dort die Hinweise zu hotplugfähigen Karten.

ISDN

Auch bei ISDN-PC-Karten erfolgt die Konfiguration größtenteils wie bei sonstigen ISDN-Karten mit YaST2. Es spielt keine Rolle welche der dort angebotenen PCMCIA ISDN-Karten ausgewählt wird; wichtig ist nur, dass es eine PCMCIA Karte ist. Bei der Einrichtung der Hardware und der Provider ist darauf zu achten, dass der Betriebsmodus immer auf `hotplug`, nicht auf `onboot` steht.

So genannte ISDN-Modems gibt es auch bei PCMCIA-Karten. Dies sind, Modem- oder Multifunktionskarten mit einem zusätzlichen ISDN-Connection-Kit und werden wie ein Modem behandelt.

Modem

Bei Modem-PC-Karten gibt es im Normalfall keine PCMCIA-spezifischen Einstellungen. Sobald ein Modem eingeschoben wird, steht dieses unter `/dev/modem` zur Verfügung.

Es gibt auch bei PCMCIA Karten so genannte Softmodems. Diese werden i. d. R. nicht unterstützt. Falls es irgendwelche Treiber gibt, müssen diese individuell ins System eingebunden werden.

SCSI und IDE

Das passende Treibermodul wird vom Cardmanager oder Hotplug geladen. Sobald also eine SCSI- oder IDE-Karte eingeschoben wird, stehen die daran angeschlossenen Geräte zur Verfügung. Die Gerätenamen werden dynamisch ermittelt. Informationen über vorhandene SCSI- bzw. IDE- Geräte sind unter `/proc/scsi` bzw. unter `/proc/ide` zu finden.

Externe Festplatten, CD-ROM-Laufwerke und ähnliche Geräte müssen eingeschaltet sein, bevor die PCMCIA-Karte in den Steckplatz eingeschoben wird. SCSI-Geräte müssen aktiv terminiert werden.

Hinweis

Bevor eine SCSI- oder IDE-Karte entnommen wird, müssen sämtliche Partitionen der daran angeschlossenen Geräte ausgehängt werden. Wurde dies vergessen, kann erst nach einem Reboot des Systems erneut auf diese Geräte zugegriffen werden, auch wenn der Rest des Systems durchaus stabil weiterläuft.

Hinweis

Sie können Linux auch vollständig auf solchen externen Platten installieren. Allerdings gestaltet sich dann der Bootvorgang etwas komplizierter. Es wird auf alle Fälle eine Bootdisk benötigt, die den Kernel und eine Init-Ramdisk (`initrd`) enthält. Die `initrd` enthält ein virtuelles Dateisystem, das alle benötigten PCMCIA-Module und -Programme enthält. Die Bootdisk bzw. die Bootdisk-Images sind ebenso aufgebaut, damit könnten Sie Ihre externe Installation immer booten. Es ist jedoch umständlich, jedes Mal die PCMCIA-Unterstützung von Hand zu laden. Fortgeschrittene Anwender können sich eine auf das jeweilige System zugeschnittene Bootdiskette selbst erstellen. Hinweise finden Sie dazu in dem englischsprachigem PCMCIA-HOWTO in Abschnitt 5.3 *Bootting from a PCMCIA device*.

Konfigurationen zum Umschalten – SCPM

Häufig benötigt man bei mobilen Computern verschiedene Konfigurationsprofile, für Firma oder für zu Hause. Mit PCMCIA-Geräten war dies dank der PCMCIA Schemata noch nie ein Problem. Da jedoch auch Betreiber von fest eingebauten Netzwerkkarten oder USB/FireWire Geräten verschiedene Profile für die Systemkonfiguration verwenden möchten, gibt es seit SuSE Linux 8.0 das Paket SCPM (System Configuration Profile Management). Deshalb unterstützt SuSE die PCMCIA Schemata nicht mehr. Wer diese dennoch verwenden möchte, muss die Konfiguration unter `/etc/pcmcia` von Hand anpassen. Wir

empfehlen jedoch einen Umstieg auf SCPM, da sich damit beliebige Teile der Systemkonfiguration verwalten lassen, nicht nur PCMCIA bezogene.

Die Dokumentation zu SCPM befindet sich im Abschnitt *SCPM – System Configuration Profile Management* auf Seite 123.

Wenn's trotzdem nicht geht

Bisweilen kommt es bei der Verwendung von PCMCIA auf manchen Notebooks oder mit manchen Karten zu Problemen. Die meisten Schwierigkeiten lassen sich mit wenig Aufwand bewältigen, solange man die Sache systematisch angeht.

Achtung

Da es in SuSE Linux sowohl externes als auch Kernel PCMCIA nebeneinander gibt, muss beim manuellen Laden von Modulen eine Besonderheit beachtet werden. Die beiden PCMCIA Systeme verwenden Module gleichen Namens und sind in unterschiedlichen Unterverzeichnissen unter `/lib/modules/<kernelversion>` untergebracht. Diese Unterverzeichnisse heißen `pcmcia` für Kernel-PCMCIA und `pcmcia-external` für externes PCMCIA. Deshalb muss beim manuellen Laden von Modulen dieses Unterverzeichnis angegeben werden, entweder mittels `insmod /lib/modules/<kernelversion>/<Unterverzeichnis>/<dateiname des Moduls>` oder mit `modprobe -t <Unterverzeichnis> <modulname>`.

Achtung

Zuerst ist herauszufinden, ob das Problem mit einer Karte zusammenhängt, oder ob ein Problem des PCMCIA-Basissystems vorliegt. Deshalb sollten Sie in jedem Fall den Computer zunächst ohne eingeschobene Karten starten. Erst wenn das Basissystem einwandfrei zu funktionieren scheint, wird die Karte eingeschoben. Alle aufschlussreichen Meldungen werden in `/var/log/messages` protokolliert. Deshalb sollte die Datei mit

```
tail -f /var/log/messages
```

während der notwendigen Tests beobachtet werden. So lässt sich der Fehler auf einen der beiden folgenden Fälle einschränken.

Das PCMCIA-Basissystem funktioniert nicht

Wenn das System beim Booten bereits bei der Meldung PCMCIA: "Starting services" stehen bleibt oder andere merkwürdige Dinge geschehen, kann das Starten von PCMCIA beim nächsten Booten durch die Eingabe von `NOPCMCIA=yes`

am Bootprompt verhindert werden. Um den Fehler weiter einzugrenzen, werden nun die drei Basismodule des verwendeten PCMCIA Systems von Hand nacheinander geladen.

Dazu dienen die Kommandos

```
erde:~ # modprobe -t <dir> pcmcia_core
erde:~ # modprobe -t pcmcia-external i82365 (bei externem PCMCIA)
      bzw.
```

```
erde:~ # modprobe -t pcmcia yenta_socket (bei kernel PCMCIA)
```

bzw. – in sehr seltenen Fällen –

```
erde:~ # modprobe -t <dir> tcic
```

und

```
erde:~ # modprobe -t <dir> ds
```

Die kritischen Module sind die beiden ersten.

Tritt der Fehler beim Laden von `pcmcia_core` auf, hilft die Manpage zu `pcmcia_core` weiter. Die darin beschriebenen Optionen können zunächst zusammen mit dem Kommando `modprobe` getestet werden. Als Beispiel können wir die APM Unterstützung der PCMCIA-Module abschalten; in wenigen Fällen kann es damit Probleme geben. Dafür gibt es die Option `doapm`; mit `do_apm=0` wird das Powermanagement deaktiviert:

```
modprobe -t <dir> pcmcia_core do_apm=0
```

Führt die gewählte Option zum Erfolg, wird sie in der Datei `/etc/sysconfig/pcmcia` in die Variable `<PCMCIA_CORE_OPTS>` geschrieben:

```
PCMCIA_CORE_OPTS="do_apm=0"
```

Vereinzelte kann das Prüfen freier IO-Bereiche Ärger machen, wenn sich dadurch andere Hardwarekomponenten gestört fühlen. Das umgeht man dann mit `probe_io=0`. Sollen mehrere Optionen verwendet werden, müssen sie durch Leerzeichen getrennt werden:

```
PCMCIA_CORE_OPTS="do_apm=0 probe_io=0"
```

Wenn es beim Laden des Moduls `i82365` zu Fehlern kommt, hilft die Manpage zu Manual-Page von `i82365` (`man i82365`).

Ein Problem in diesem Zusammenhang ist ein Ressourcenkonflikt, ein Interrupt, IO-Port oder Speicherbereich wird doppelt belegt. Das Modul `i82365` prüft zwar diese Ressourcen, bevor sie für eine Karte zur Verfügung gestellt

werden, jedoch führt manchmal genau diese Prüfung zum Problem. So führt das Prüfen des Interrupt 12 (PS/2-Geräte) bei manchen Computern zum Blockieren von Maus und/oder Tastatur. In diesem Fall hilft der Parameter `irq_list=`*ListevonIRQs*. Die Liste soll alle IRQs enthalten, die verwendet werden dürfen. Also

```
modprobe i82365 irq_list=5,7,9,10
```

oder dauerhaft in `/etc/sysconfig/pcmcia`:

```
PCMCIA_PCIC_OPTS="irq_list=5,7,9,10"
```

Weiterhin gibt es `/etc/pcmcia/config` und `/etc/pcmcia/config.opts`. Diese Dateien werden vom Cardmanager ausgewertet. Die darin gemachten Einstellungen sind erst für das Laden der Treiber-Module für die PCMCIA-Karten relevant.

In `/etc/pcmcia/config.opts` können auch IRQs, IO-Ports und Speicherbereiche ein- oder ausgeschlossen werden. Der Unterschied zur Option `irqlist` ist, dass die in `config.opts` ausgeschlossenen Ressourcen zwar nicht für eine PCMCIA-Karte verwendet, aber dennoch vom Basis-Modul `i82365` geprüft werden.

Die PCMCIA-Karte funktioniert nicht (richtig)

Hier gibt es im Wesentlichen drei Varianten: Die Karte wird nicht erkannt, der Treiber kann nicht geladen werden oder das Interface, das vom Treiber bereitgestellt wird, wird falsch eingerichtet.

Man sollte beachten, ob die Karte vom Cardmanager oder von `hotplug` behandelt wird. Nochmal zur Erinnerung: Bei externem PCMCIA regiert immer der Cardmanager, bei Kernel PCMCIA behandelt der Cardmanager PC-Card Karten und `Hotplug` behandelt CardBUS Karten. Hier wird nur der Cardmanager besprochen. `Hotplug` Probleme werden im `Hotplug` Kapitel behandelt (siehe Kapitel [Hotplug](#) auf Seite 103).

■ Die Karte wird nicht erkannt.

Wenn die Karte nicht erkannt wird, erscheint in `/var/log/messages` die Meldung "unsupported Card in Slot x". Diese Meldung besagt lediglich, dass der Cardmanager der Karte keinen Treiber zuordnen kann. Zu dieser Zuordnung wird `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` benötigt. Diese Dateien sind sozusagen die Treiberdatenbank. Diese Treiberdatenbank lässt sich am leichtesten erweitern, wenn man vorhandene Einträge als Vorlage nimmt. Sie können mit dem Kommando `cardctl ident` herausfinden, wie die Karte sich identifiziert. Weitere

Informationen dazu befinden sich im PCMCIA-HOWTO Abschnitt 6 und in der Manual-Page von `pcmcia` (`man pcmcia`). Nach der Änderung von `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` muss die Treiberzuordnung neu geladen werden; dazu genügt ein `rcpcmcia reload`.

■ Treiber wird nicht geladen

Eine Ursache hierfür besteht darin, dass in der Treiberdatenbank eine falsche Zuordnung gespeichert ist. Das kann z. B. daher kommen, dass ein Hersteller in ein äußerlich unverändertes Kartenmodell einen anderen Chip einbaut. Manchmal gibt es auch alternative Treiber, die bei bestimmten Modellen besser (oder überhaupt erst) funktionieren als der voreingestellte Treiber. In diesen Fällen werden genaue Informationen über die Karte benötigt. Hier hilft auch, eine Mailingliste oder den Advanced Support Service zu fragen.

Eine weitere Ursache ist ein Ressourcenkonflikt. Bei den meisten PCMCIA-Karten ist es nicht relevant, mit welchem IRQ, IO-Port oder Speicherbereich sie betrieben werden, aber es gibt auch Ausnahmen. Dann sollte man zuerst immer nur eine Karte testen und evtl. auch andere Systemkomponenten wie z. B. Soundkarte, IrDA, Modem oder Drucker vorübergehend abschalten. Die Ressourcenverteilung des Systems kann man mit `lsdev` einsehen (Es ist durchaus normal, dass mehrere PCI Geräte denselben IRQ verwenden).

Eine Lösungsmöglichkeit wäre, eine geeignete Option für das Modul `i82365` zu verwenden (siehe oben `PCMCIA_PCIC_OPTS`). Es gibt jedoch auch für manche Kartentreibermodule Optionen. Diese lassen sich mit `modinfo /lib/modules/<richtiges_pcmcia_Verzeichnis>/<treiber>.o` herausfinden (der vollständige Pfad ist hier wieder nötig, um den Treiber vom richtigen PCMCIA System anzusprechen). Für die meisten Module gibt es auch eine Manpage. Tipp: `rpm -ql pcmcia | grep man` listet alle im `pcmcia` enthaltene Manual-Pages auf. Zum Testen der Optionen können die Kartentreiber auch von Hand entladen werden. Hierbei ist wieder zu beachten, dass das Modul des gerade verwendeten PCMCIA Systems zu verwenden. Siehe die Warnung weiter oben.

Wenn eine Lösung gefunden wurde, kann in `/etc/pcmcia/config.opts` die Verwendung einer bestimmten Ressource allgemein erlaubt bzw. verboten werden. Auch die Optionen für Kartentreiber finden hier Platz Soll z. B. das Modul `pcnet_cs` ausschließlich mit dem IRQ 5 betrieben werden, wird folgender Eintrag benötigt:

```
module pcnet_cs opts irq_list=5
```

Ein Problem, das manchmal mit 10/100-MBit-Netzwerkkarten auftritt:

Die Übertragungsart wird nicht automatisch richtig erkannt. Hier hilft das Kommando `ifport` oder `mii_tool`. Damit lässt sich die eingestellte Übertragungsart anzeigen und verändern. Um diese Kommandos automatisch ausführen zu lassen, muss das Script `/etc/pcmcia/network` individuell angepasst werden.

■ Interface wird falsch konfiguriert

In diesem Fall ist es empfehlenswert, die Konfiguration des Interfaces nochmal genau zu überprüfen, um seltene Konfigurationsfehler auszuschließen. Bei Netzwerkkarten kann außerdem die Dialograte der Netzwerkskripten erhöht werden, in dem man in `/etc/sysconfig/network/config` der Variable `DEBUG=yes` zuweist. Bei anderen Karten, oder wenn das noch nicht hilft, gibt es noch die Möglichkeit, in das vom Cardmanager aufgerufene Script (siehe `/var/log/messages`) eine Zeile `set -x` einzubauen. Dadurch wird jedes einzelne Kommando des Scripts im Systemlog protokolliert. Hat man die kritische Stelle in einem Script gefunden, können die entsprechenden Kommandos auch in einem Terminal eingegeben und getestet werden.

Installation via PCMCIA

In manchen Fällen wird PCMCIA bereits zum Installieren benötigt, wenn man über Netzwerk installieren möchte oder das CD-ROM via PCMCIA betrieben wird. Dazu muss man mit einer Bootdiskette starten. Des weiteren wird eine der Moduldisketten benötigt.

Nach dem Booten von Diskette (oder auch nach der Auswahl 'manuelle Installation' beim Booten von CD) wird das Programm `linuxrc` gestartet. Dort muss unter dem Menüpunkt 'Kernel-Module (Hardware-Treiber)' der Punkt 'Lade PCMCIA Module' ausgewählt werden. Zuerst erscheinen zwei Eingabefelder, in denen man Optionen für die Module `pcmcia_core` und `i82365` eingeben kann. Im Normalfall bleiben diese Felder jedoch leer. Die Man-Pages für `pcmcia_core` und `i82365` befinden sich als Textdateien auf der ersten CD im Verzeichnis `docu`.

Nach dem aktuellen Stand der Entwicklung wird bei SuSE Linux 8.1 nach wie vor mit dem externen PCMCIA System installiert. Sollte sich dies nach Fertigstellung des Buches noch ändern, erkennen Sie das daran, dass keine Moduloptionen für `i82365` erfragt werden und stattdessen das Modul `yenta_socket` verwendet wird. Während der Installation werden Systemmeldungen auf verschiedenen virtuellen Konsolen ausgegeben, auf die man mit (Alt) + (Funktionstaste) umschalten kann. Später, wenn bereits eine grafische Oberfläche aktiv ist, muss man (Ctrl) + (Alt) + (Funktionstaste) verwenden.

Es gibt auch schon während der Installation Terminals, auf denen Kommandos ausgeführt werden können. Solange `linuxrc` läuft, ist das die Konsole 9 (eine sehr spartanisch ausgestattete Shell); sobald das Installationssystem geladen ist (YaST2 wurde gestartet) gibt es auf Konsole 2 eine `bash` und viele gängige Systemtools.

Wenn während der Installation ein falsches Treibermodul für eine PCMCIA Karte geladen wird, muss die Bootdiskette von Hand angepasst werden. Dazu benötigt man jedoch fortgeschrittene Linuxkenntnisse. Wenn der erste Teil der Installation abgeschlossen ist, wird das System teilweise oder ganz neu gestartet. Dabei kann in seltenen Fällen beim Starten von PCMCIA das System stehen bleiben. Zu diesem Zeitpunkt ist die Installation aber schon weit genug fortgeschritten, so dass mit der Boot-Option `NOPCMIA=yes` Linux ohne PCMCIA gestartet werden kann, zumindest im Textmodus. Hier hilft der Abschnitt *Wenn's trotzdem nicht geht* auf Seite 117 weiter. Evtl. kann man schon vor Abschluss des ersten Teils der Installation auf Konsole 2 einige Einstellungen am System verändern, so dass der Neustart erfolgreich verläuft.

Weitere Hilfsprogramme

Das Programm `cardctl` wurde schon mehrfach erwähnt. `cardctl` ist das wesentliche Werkzeug, um Informationen von PCMCIA zu erhalten, bzw. bestimmte Aktionen auszuführen. In der `cardctl` finden Sie Details; oder Sie geben `cardctl` ein und erhalten eine Liste der gültigen Kommandos.

Zu diesem Programm gibt es auch ein graphisches Frontend `cardinfo` (vgl. Abb. 5.1), mit dem die wichtigsten Dinge kontrollierbar sind. Dazu muss jedoch das Paket `pcmcia-cardinfo` installiert sein.

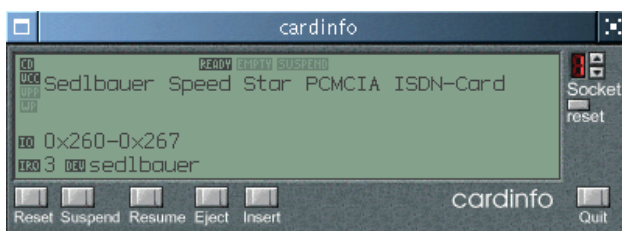


Abbildung 5.1: Das Programm `cardinfo`

Weitere Helfer aus dem `pcmcia` Paket sind `ifport`, `ifuser`, `probe` und `rcpcmcia`. Diese werden aber nicht immer benötigt. Um genau zu erfahren, was alles im Paket `pcmcia` steckt, verwendet man den Befehl `rpm -ql pcmcia`.

Kernel oder PCMCIA Paket aktualisieren

Wenn Sie den Kernel aktualisieren möchten, sollten Sie die von SuSE bereitgestellte Kernelpakete verwenden. Ist es notwendig, einen eigenen Kernel zu kompilieren, dann müssen auch die PCMCIA-Module neu kompiliert werden. Wichtig ist, dass während der Neuübersetzung bereits der richtige Kernel läuft, da aus diesem einige Informationen extrahiert werden. Das pcmcia Paket sollte bereits installiert, aber nicht gestartet sein; im Zweifelsfall also noch ein `rcpcmcia stop` ausführen. Dann installiert man das PCMCIA-Quellpaket mit und gibt anschließend ein:

```
rpm -ba /usr/src/packages/SPECS/pcmcia.spec
```

Danach liegen unter `/usr/src/packages/RPMS` neue Pakete. Das Paket `pcmcia-modules` enthält die PCMCIA Module für externes PCMCIA. Dieses Paket muss mit `rpm -force` installiert werden, da die Moduldateien offiziell zum Kernel-Paket gehören.

Weiterführende Informationen

Wer an Erfahrungen mit bestimmten Notebooks interessiert ist, sollte auf alle Fälle die Linux Laptop Homepage unter <http://linux-laptop.net> besuchen. Eine weitere gute Informationsquelle ist die Moblix-Homepage unter <http://mobilix.org/> (MobiliX – Mobile Computers and Unix). Dort findet man neben viele interessanten Informationen auch ein Laptop-Howto und ein IrDA-Howto. Außerdem gibt es in der Supportdatenbank den Artikel Laptops und Notebooks (PCMCIA) unter Linux <http://sdb.suse.de/de/sdb/html/laptop.html> (oder lokal unter `file:/usr/share/doc/sdb/de/html/laptop.html`).

SCPM – System Configuration Profile Management

Es gibt Situationen, in denen eine veränderte Konfiguration des Computersystems benötigt wird. Am häufigsten wird dies wohl auf mobile Computer zutreffen, die an verschiedenen Standorten betrieben werden. Es kann aber auch sein, dass man auf einem Desktopsystem zeitweilig andere Hardwarekomponenten verwendet. Oder aber man möchte einfach mal etwas ausprobieren. In jedem Fall sollte eine Rückkehr zum ursprünglichen System einfach sein. Noch besser ist es, wenn diese Umkonfiguration auch noch einfach reproduzierbar ist.

Eine Lösung für dieses Problem gab es bisher nur für PCMCIA Hardware. Dort konnte man verschiedene Konfigurationen in bestimmten Schemata ablegen. Ausgehend davon haben wir SCPM entwickelt, das die Beschränkung auf PCMCIA aufhebt. Mit dem „System Configuration Profile Management“ lässt sich ein frei wählbarer Teil der Systemkonfiguration festlegen, von dem verschiedene Zustände in eigenen Konfigurationsprofilen festgehalten werden können. Etwas freier ausgedrückt ist das, als ob man Schnappschüsse von seiner Systemkonfiguration macht, die man jederzeit wiederherstellen kann. Und der Bildauschnitt ist frei wählbar.

Das Hauptanwendungsgebiet wird vermutlich bei der Netzwerkkonfiguration von Laptops liegen. Aber bei unterschiedlichen Netzwerkeinstellungen verändern sich meist auch noch andere Elemente, z. B. die Einstellungen für E-Mail oder Proxies. Hierzu kommen unterschiedliche Drucker zuhause und in der Firma oder die gesonderte XFree86-Konfiguration für den Beamer bei Vorträgen, extra sparsame Stromverbrauchseinstellungen für unterwegs oder die andere Zeitzone in der Auslandsniederlassung.

Mit steigendem Einsatz dieses Werkzeugs werden immer wieder neue Anforderungen sichtbar. Wenn Sie selbst Anregungen und Kritik zu SCPM haben, dann nehmen Sie mit uns Kontakt auf. Wir sind sehr an Rückmeldungen interessiert. Wir haben versucht, SCPM auf ein flexibles Grundgerüst zu stellen, so dass z. B. auch ein serverbasiertes Profil Management möglich ist. Bitte teilen Sie uns Ihre Wünsche, Anregungen und Fehlerbeschreibungen über unser Webfrontend <http://www.suse.de/feedback> mit.

Grundbegriffe und Grundlagen

Vorab sollen einige Grundbegriffe festgelegt werden, die auch in der restlichen Dokumentation zu SCPM und im YaST2 Modul so verwendet werden.

- Unter *Systemkonfiguration* verstehen wir die gesamte Konfiguration des Computers. Alle grundlegenden Einstellungen, wie die z. B. Verwendung von Festplattenpartitionen oder Netzwerkeinstellungen, Zeitzonenauswahl oder Tastatureinstellung.
- Ein *Profil* oder auch *Konfigurationsprofil* ist ein Zustand der Systemkonfiguration, der festgehalten wurde und der bei Bedarf einfach wiederhergestellt werden kann.
- Als *aktives Profil* wird immer das Profil bezeichnet, in das zuletzt geschaltet wurde. Das heißt nicht, dass die aktuelle Systemkonfiguration exakt diesem Profil entspricht, denn die Konfiguration kann jederzeit individuell verändert werden.

- *Resource* im Sinne von SCPM sind alle Elemente, die zur Systemkonfiguration beitragen. Das kann eine Datei oder ein Softlink einschließlich ihrer Metadaten, wie Benutzer, Rechte, oder Zugriffszeit sein. Das kann aber auch ein Systemdienst sein, der einmal läuft und in einem anderen Profil ausgeschaltet ist.
- Für die häufigsten Anwendungsfälle gibt es vordefinierte *Resourcesets*. Durch die Auswahl eines solchen Resourcesets kann man einfach festlegen, welche Elemente der Systemkonfiguration von SCPM berücksichtigt werden. Bei Bedarf können auch eigene Resourcesets definiert werden. In der gegenwärtigen Entwicklungsstufe von SCPM verwenden alle Profile dasselbe Set. Eine Weiterentwicklung hin zu Profilen, die unterschiedliche Ressourcen behandeln, ist jedoch bereits bedacht.

SCPM YaST2 Modul und weiterführende Dokumentation

Als grafisches Frontend zu SCPM gibt es ein YaST2 Modul als Alternative zu dem Kommandozeilen-Frontend. Da die Funktionalität beider Frontends im wesentlichen dieselbe ist und die Kenntnis des Kommandozeilen-Frontends für viele Zwecke interessant ist, wird hier nur das letztere beschrieben. Die Bedienung des SCPM YaST2 Moduls ist danach zusammen mit den dort angebotenen Hilfetexten sehr leicht. Die wenigen Besonderheiten des YaST2 Moduls werden an passender Stelle erwähnt.

Die aktuellste Dokumentation wird immer in den Infoseiten zu SCPM zu finden sein. Diese kann mit Werkzeugen wie Konqueror oder Emacs eingesehen werden (`konqueror info:scpm`). In der Konsole verwendet man `info` oder `pinfo`. Technische Dokumentation für Leute, die selbst Hand an SCPM legen möchten, gibt es unter `/usr/share/doc/packages/scpm`.

Der Aufruf von `scpm` ohne weitere Argumente gibt eine Kommandoübersicht aus.

SCPM einrichten

Bevor mit SCPM gearbeitet werden kann, muss es erst einmal eingeschaltet werden. Es ist jedoch sehr empfehlenswert, zuerst ein Resourceset aus `/lib/scpm/resource_sets/` auszuwählen. Das ausgewählte Set wird in `/etc/scpm.conf` in die Variable `(RESOURCE_SET)` eingetragen. Wird kein Resourceset eingetragen, versucht SCPM aus verschiedenen Informationsquellen eine sinnvolle Menge von behandelten Ressourcen zusammenzustellen. Diese ist jedoch für viele Anwendungsfälle zu umfangreich.

Um seinen eigenen Anforderungen am besten gerecht zu werden, können unter `/var/lib/scpm/resource_sets` eigene Resourcesets angelegt werden. Es gilt dabei keineswegs der Grundsatz „Viel hilft viel“. Jede Änderung, die für alle Profile gelten soll, an einer Datei, die von SCPM behandelt wird, muss dann sofort durchgeführt werden, wie es Profile gibt. Deshalb ist die gesamte Konfiguration aller Profile um so komplexer, je größer ein Resourceset ist. Die Wahl des Resourcesets kann jederzeit geändert werden, wobei jedoch nur der Wechsel von kleineren Sets zu größeren immer problemlos ist. Beim Verkleinern des verwendeten Resourcesets muss nämlich immer bedacht werden, welche Version einer Resource (aus welchem Profil) behalten und welche verworfen wird.

Mit dem Aufruf von `scpm enable` wird SCPM eingeschaltet. Beim ersten Einschalten wird SCPM initialisiert, was einige Sekunden in Anspruch nimmt. SCPM kann mit `scpm disable` jederzeit ausgeschaltet werden, um unbeabsichtigte Profilumschaltungen zu vermeiden. Beim anschließenden Wiedereinschalten wird die Initialisierung einfach fortgesetzt.

Profile anlegen und verwalten

Nachdem SCPM eingeschaltet wurde, gibt es bereits ein Profil namens `default`. Eine Liste aller verfügbaren Profile gibt das Kommando `scpm list` aus. Dieses bisher einzige Profil ist zwangsläufig auch das aktive Profile. Das erfährt man mit `scpm active`. Das Profil `default` ist als Grundkonfiguration gedacht, von der die anderen Profile abgeleitet werden. Deshalb sollten zuerst alle Einstellungen, die in allen Profilen einheitlich sein sollen, vorgenommen werden. Mit `scpm reload` werden diese Änderungen dann im aktiven Profil gespeichert. Das Profil `default` kann dennoch beliebig verwendet, umbenannt oder gelöscht werden.

Es gibt zwei Möglichkeiten, ein neues Profil hinzuzufügen. Wenn das neue Profil (hier mit Namen `work`) z. B. auf dem Profil `default` basieren soll, geschieht dies mit `scpm copy default work`. Danach kann man mit `scpm switch work` in das neue Profil umschalten und es dann konfigurieren. Manchmal hat man aber auch die Systemkonfiguration schon für bestimmte Zwecke verändert und möchte diese danach in einem neuen Profil festhalten. Das erledigt der Aufruf von `scpm add work`. Jetzt ist die aktuelle Systemkonfiguration im Profil `work` gesichert und das neue Profil als aktiv markiert; d. h. ein `scpm reload` sichert Änderungen jetzt im Profil `work`.

Selbstverständlich können Profile auch umbenannt oder gelöscht werden. Dafür gibt es die Kommandos `scpm rename x y` und `scpm delete x`. Um z. B. `work` nach `arbeit` umzubenennen und es hinterher zu löschen, gibt man `scpm rename work arbeit` und dann `scpm delete arbeit` ein. Nur das aktive Profil kann nicht gelöscht werden.

Nochmal die einzelnen Kommandos:

`scpm list` gibt alle verfügbaren Profile aus

`scpm active` gibt das aktive Profile aus

`scpm add` *<name>* speichert die gegenwärtige Systemkonfiguration in einem neuen Profil und macht dieses zum aktiven

`scpm copy` *<quellname>* *<zielname>* kopiert ein Profil

`scpm rename` *<quellname>* *<zielname>* benennt ein Profil um

`scpm delete` *<name>* löscht ein Profil

Hinweis zum YoST2 Modul: Hier gibt es nur den Knopf 'Add'. Es erscheint dann aber die Frage, ob man ein existierendes Profil kopieren oder die gegenwärtige Systemkonfiguration sichern möchte. Zum Umbenennen verwende man dort den Knopf 'Edit'.

Zwischen Konfigurationsprofilen umschalten

Das Umschalten zu einem anderen Profil (hier `work`) wird mit dem Kommando `scpm switch work` ausgelöst. Es ist zulässig, zum gerade aktiven Profile umzuschalten um geänderte Einstellungen an der Systemkonfiguration zu sichern. Alternativ kann dafür aber auch das Kommando `scpm reload` verwendet werden.

Um den Umschaltvorgang und die dabei evtl. auftretenden Fragen besser zu verstehen, soll dieser hier näher erläutert werden.

Zuerst prüft SCPM, welche Ressourcen des aktiven Profils seit dem letzten Umschalten verändert wurden. Für alle veränderten Ressourcen wird dann nachgefragt, ob die Änderung an dieser Resource in das immer noch aktive Profil übernommen oder verworfen werden soll. Diese Fragen betreffen insofern nur das Profil, das man gerade verlassen möchte.

Danach vergleicht SCPM die aktuelle Systemkonfiguration mit dem neuen Profil, in das umgeschaltet werden soll. Dabei wird ermittelt, welche Systemdienste aufgrund von Konfigurationsänderungen oder wegen gegenseitiger Abhängigkeiten angehalten bzw. (wieder) gestartet werden müssen. Das kann man sich wie einen teilweisen Systemreboot vorstellen, nur dass eben nur ein kleiner Teil des Systems betroffen ist und der Rest unverändert weiterarbeitet.

Erst jetzt werden die

1. Systemdienste angehalten,
2. alle veränderten Ressourcen (i. a. Konfigurationsdateien) geschrieben und die
3. Systemdienste (wieder) gestartet.

Erweiterte Profileinstellungen

Sie können für jedes Profil eine Beschreibung eingeben, die dann bei `scpm list` mit ausgegeben wird. Eingeben kann man diese Beschreibung für das gerade aktive Profil mit dem Kommando `scpm set description "text"`. Für nicht aktive Profile muss noch das Profil angegeben werden, also `scpm set description "text" work`. Manchmal kommt es vor, dass beim Umschalten in ein anderes Profil zusätzliche Aktionen ausgeführt werden sollen, die in SCPM (noch) nicht vorgesehen sind. Dafür können für jedes Profil vier ausführbare Programme oder Scripte eingehängt werden, die zu verschiedenen Zeitpunkten während das Umschaltens ausgeführt werden. Diese Zeitpunkte sind:

prestop vor dem Anhalten von Diensten beim Verlassen des Profils

poststop nach dem Anhalten von Diensten beim Verlassen des Profils

prestart vor dem Starten von Diensten beim Aktivieren des Profils

poststart nach dem Starten von Diensten beim Aktivieren des Profils

Das Umschalten von Profil `work` zu Profil `home` läuft dann folgendermaßen ab:

1. Prestop-Aktion des Profils `work` wird ausgeführt.
2. Anhalten von Diensten
3. Poststop-Aktion des Profils `work` wird ausgeführt
4. Verändern der Systemkonfiguration
5. Prestart-Aktion des Profils `home` wird ausgeführt.
6. Starten von Diensten
7. Poststart-Aktion des Profils `home` wird ausgeführt.

Diese Aktionen werden auch mit dem `set` Kommando eingehängt, nämlich mit `scpm set prestop <dateiname>`, `scpm set poststop <dateiname>`, `scpm set prestart <dateiname>` oder `scpm set poststart <dateiname>`. Es muss sich dabei um ein ausführbares Programm handeln, d. h. Scripte müssen den richtigen Interpreter beinhalten und zumindest für den Superuser ausführbar sein.

Alle Zusatzeinstellungen, die mit `set` eingegeben wurden, lassen sich mit `get` abfragen. Zum Beispiel liefert `scpm get poststart` den Namen des Poststartprogramms oder einfach keine Information, wenn nichts eingehängt wurde. Gelöscht werden solche Einstellungen durch Überschreiben mit `" "`; d. h. ein `scpm set prestop ""` hängt das Poststop-Programm wieder aus.

Genau wie beim Anlegen der Beschreibung können alle `set` und `get` Kommandos für ein beliebiges Profil angewandt werden. Dazu wird zuletzt noch der Name des Profils angegeben. Zum Beispiel `scpm get prestop <dateiname> work` oder `scpm get prestop work`.

Achtung

Da diese Skripte oder Programme mit den Rechten des Superusers ausgeführt werden sollten sie nicht von beliebigen Anwendern änderbar sein. Da in Scripten durchaus vertrauliche Informationen enthalten sein können, ist es sogar angeraten, dass diese nur vom Superuser lesbar sind. Am besten versieht man diese Programme mit den Rechten `-rwx---- root root`.

`(chmod 700 <dateiname> und chown root.root <dateiname>)`

Achtung

Profilauswahl beim Booten

Es ist möglich, schon vor dem Booten ein Profil auszuwählen. Dazu muss lediglich der Bootparameter `PROFILE=<Name des Profils>` am Bootprompt eingegeben werden.

Bei der Option `title` verwendet man dann ebenfalls den Namen des Profils. Standardmäßig wird GRUB als Bootloader verwendet. Eine ausführlichere Beschreibung finden Sie Abschnitt [Booten mit GRUB](#) auf Seite 89; alternativ geben Sie `info grub` ein. Die Konfiguration von GRUB sieht dann z. B. wie folgt aus:

```
gfxmenu (hd0,5)/boot/message
color white/green black/light-gray
```

```

default 0
timeout 8

title work
    kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=work
    initrd (hd0,5)/boot/initrd-2.4.19-4GB

title home
    kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=home
    initrd (hd0,5)/boot/initrd-2.4.19-4GB

title road
    kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=road
    initrd (hd0,5)/boot/initrd-2.4.19-4GB

```

Datei 3: Die Datei /boot/grub/menu.lst

Für Systeme, die noch den Bootloader LILO verwenden, kann die Datei [4](#) verwendet werden.

```

boot      = /dev/hda
change-rules
reset
read-only
menu-scheme = Wg:kw:Wg:Wg
prompt
timeout = 80
message = /boot/message

    image = /boot/vmlinuz
    label = home
    root = /dev/hda6
    initrd = /boot/initrd
    append = "vga=0x317 hde=ide-scsi PROFILE=home"

    image = /boot/vmlinuz
    label = work
    root = /dev/hda6
    initrd = /boot/initrd
    append = "vga=0x317 hde=ide-scsi PROFILE=work"

    image = /boot/vmlinuz

```

```
label    = road
root     = /dev/hda6
initrd   = /boot/initrd
append   = "vga=0x317 hde=ide-scsi PROFILE=road"
```

Datei 4: Datei /etc/lilo.conf

Jetzt kann beim Booten sehr einfach das gewünschte Profil ausgewählt werden.

APM und ACPI – Powermanagement

Powermanagement setzt eine dafür ausgelegte Hardware und passende BIOS-Routinen voraus. Die meisten Notebooks und viele moderne Desktops bringen diese Voraussetzungen mit. Bisher wurde dazu meist der APM Standard verwendet (engl. *Advanced Power Management*). Dies sind im wesentlichen Funktionen, die im BIOS des Computers implementiert sind. Deshalb funktioniert Powermanagement nicht auf allen Geräten gleich gut. Wenn Sie ein Notebook mit funktionierender APM Implementierung haben, dann tun Sie gegenwärtig gut daran, diese zu verwenden. Es gibt nämlich seit einiger Zeit Hersteller, die sich APM sparen und vollständig auf den neueren Standard ACPI (engl. *Advanced Configuration and Power Interface*) setzen. ACPI ist aber schon konzeptionell schwieriger und setzt gute Zusammenarbeit von Hardwareherstellern, BIOS-Programmieren und den Betriebssystemexperten voraus. Außerdem ist die ACPI Implementierung im Linux Kernel ist noch nicht fertig und deswegen nur teilweise nutzbar. Erst mit dem Kernel 2.6 ist hier eine wesentliche Besserung in Sicht.

Stromsparfunktionen

Viele dieser Funktionen sind von allgemeinem Interesse, aber so richtig wichtig sind diese aber erst im mobilen Einsatz. Im Folgenden werden diese Funktionen beschrieben und erklärt von welchem System diese ausgeführt werden können.

Stand-by In dieser Betriebsart wird nur das Display ausgeschaltet und bei manchen Geräten die Prozessorleistung gedrosselt. Nicht jedes APM stellt diese Funktion zur Verfügung. Bei ACPI entspricht das dem Zustand S2.

Suspend (to memory) Hier wird der gesamte Systemzustand in den Arbeitsspeicher geschrieben und außer diesem das gesamte System schlafen gelegt. In diesem Zustand braucht der Computer nur sehr wenig Strom,

sodass man damit je nach Gerät von 12 Stunden bis mehrere Tage mit Batterie überbrücken kann. Der Vorteil dieses Zustands ist, dass man innerhalb weniger Sekunden wieder an derselben Stelle weiterarbeiten kann, ohne erst booten und benötigte Programme neu laden zu müssen. Bei den meisten modernen Geräten genügt es, den Deckel zu schließen, um zu suspendieren, und ihn zum Weiterarbeiten einfach wieder zu öffnen und es kann sofort weitergehen. Bei ACPI entspricht das dem Zustand S3.

Hibernation (Suspend to disk) In dieser Betriebsart hält es der Computer länger als einen Winter aus (Hibernation bedeutet Überwinterung), denn der Systemzustand wird vollständig auf der Festplatte gespeichert und das System danach ausgeschaltet. Die Rückkehr aus dem Winterschlaf dauert zwischen 30 - 90 Sekunden und auch hier wird der Zustand vor dem Suspend genau wiederhergestellt. Einige Hersteller bieten in ihrem APM sinnvolle Mischformen davon an (z. B. RediSafe bei IBM Thinkpads). Hibernation entspricht bei ACPI dem Zustand S4. Es gibt für Linux auch eine reine Softwarelösung, die in SuSE Linux aber nicht enthalten ist. Wer dies Verwenden möchte muß selbst die Ärmel hochkrempeln: <http://falcon.sch.bme.hu/~seasons/linux/swsusp.html>

Kontrolle des Akkuzustands Neben der reinen Information über den Ladezustand, ist es auch wichtig, daß etwas unternommen wird, wenn die Energiereserven knapp werden. Auch das wird meist von den APM BIOSroutinen erledigt. Alternativ kann dazu auch der `apmd/acpid` oder `klaptopdaemon` verwendet werden.

Automatisches Ausschalten Nach einem Shutdown wird der Computer vollständig ausgeschaltet. Das ist vor allem von Bedeutung, wenn ein automatischer Shutdown ausgeführt wird, kurz bevor der Akku leer ist.

Abschalten von Systemkomponenten Die wesentliche Komponente um Energie zu sparen ist die Festplatte. Je nach Zuverlässigkeit des gesamten Systems kann diese mehr oder weniger lang schlafen gelegt werden. Allerdings steigt das Risiko eines Datenverlusts mit der Länge der Ruhepausen der Platte. Andere Komponenten können via ACPI/footnotezumindest theoretisch oder dauerhaft im BIOSsetup deaktiviert werden. Vor allem der Infrarotport sollte möglichst ausgeschaltet bleiben, solange man diesen nicht benötigt (siehe xxxIRDAxxx).

Kontrolle der Prozessorleistung Zusammen mit APM gibt es meist nur die Möglichkeit im BIOSsetup verschiedene Einstellungen zu wählen. Kontrollieren läßt sich die Prozessorfrequenz mit dem Programm `procspeed` aus dem Paket `apmd`.

APM

Einige der Stromsparfunktionen führt das APM-BIOS alleine aus. Stand-by und Suspend kann man auf vielen Notebooks mit Tastenkombinationen oder mit Schließen des Deckels aktivieren. Dazu ist erstmal keinerlei Funktion seitens des Betriebssystems nötig. Wer diese Betriebsarten jedoch per Kommando einleiten möchte, darauf angewiesen ist, dass vor dem Suspend noch bestimmte Aktionen ausgeführt werden, oder einfach nur den Ladezustand der Batterie angezeigt bekommen möchte, muss entsprechende Pakete und einen geeigneten Kernel installiert haben.

Bei den fertigen Kernen von SuSE Linux ist der APM Support fest eingebaut und wird automatisch aktiviert, sobald beim Booten ein APM-BIOS gefunden wird. Um den APM Support auszuschalten kann am Bootprompt `apm=off` verwendet werden. Ob APM aktiviert wurde lässt sich leicht mit dem Kommando `cat /proc/apm` nachprüfen. Wenn hier eine Zeile mit diversen Zahlen erscheint, ist alles okay. Jetzt sollte ein `shutdown -h` zum Ausschalten des Computers führen.

Da manche BIOS-Implementierungen sich nicht exakt an Standards halten, kommt es manchmal zu merkwürdigem Verhalten. Manche Probleme kann man mit speziellen Bootparametern umgehen (früher waren dies Kernelkonfigurationsoptionen). Alle Parameter werden am Bootprompt in der Form `apm=<parameter>` eingegeben:

on/off APM Support ein/ausschalten

(no-)allow-ints Während dem Ausführen von BIOS Funktionen Interrupts zulassen

(no-)broken-psr BIOS hat eine kaputte „GetPowerStatus“ Funktion

(no-)realmode-power-off Den Prozessor vor dem Shutdown in den Real Mode zurückschalten

(no-)debug APM Ereignisse im Syslog protokollieren

(no-)power-off Nach dem Shutdown das System ausschalten

bounce-interval=<n> Zeit in 1/100 Sekunden, in der nach einem Suspendereignis weitere Suspendereignisse ignoriert werden

idle-threshold=<n> Prozentsatz der Systeminaktivität, ab der die BIOS Funktion `idle` aufgerufen wird (0=immer, 100=nie)

idle-period=<n> Zeit in 1/100 Sekunden, über der die System(in)aktivität ermittelt wird

Der APM-Daemon (apmd)

Der Daemon `apmd` dient zur Überwachung der Batterie und kann bestimmte Aktionen auslösen, wenn ein Stand-by oder Suspend Ereignis eintritt. Er befindet sich im Paket `apmd`. Er ist nicht unbedingt zum Betrieb notwendig, kann jedoch bei manchen Problemen recht nützlich sein.

Der `apmd` wird nicht automatisch beim Booten gestartet. Ist dies jedoch erforderlich, kann man mit dem YaST2 Runlevel-Modul die Einstellungen zu den Systemdiensten verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Manuell kann er mit dem Kommando `rcapmd start` gestartet werden.

Zur Konfiguration gibt es in `/etc/sysconfig/powermanagement` einige Variablen. Die Datei ist mit Kommentaren versehen, deshalb werden hier nur einige Hinweise gegeben.

APMD_ADJUST_DISK_PERF Damit wird veranlasst, daß das Verhalten der Festplatte an den Zustand der Stromversorgung angepasst wird. Dazu gibt es eine Reihe weiterer Variablen, die entweder mit `APMD_BATTERY` oder `APMD_AC` beginnen. Die ersteren enthalten die Einstellungen für den Batteriebetrieb, die letzteren die für den Betrieb mit externer Stromversorgung.

APMD_BATTERY/AC_DISK_TIMEOUT Nach welcher Zeit Platteninaktivität wird diese angehalten. Die möglichen Werte sind im Abschnitt *[Pause für die Festplatte](#)* auf Seite 136 oder in der Manpage zu `hdparm` Option `-S` beschrieben.

APMD_BATTERY/AC_KUPDATED_INTERVAL Die Zeit zwischen zwei Läufen des Kernel Update Deamons.

APMD_BATTERY/AC_DATA_TIMEOUT Das maximale Alter gepufferter Daten.

APMD_BATTERY/AC_FILL_LEVEL Der maximale Füllstand des Festplattenpuffers.

APMD_PCMCIA_EJECT_ON_SUSPEND Obwohl PCMCIA bei mit APM-Unterstützung übersetzt ist, gibt es hier manchmal Schwierigkeiten. Einige der Kartentreiber kehren von einem Suspend nicht ordentlich zurück (`xirc2ps_cs`). Deshalb kann der `apmd` das PCMCIA-System vor dem Suspend deaktivieren und danach wieder aktivieren. Dazu wird die Variable `APMD_PCMCIA_EJECT_ON_SUSPEND` auf `yes` gesetzt.

APMD_INTERFACES_TO_STOP Hier können Netzwerkinterfaces eingetragen werden, die vor dem Suspendieren angehalten und danach wieder gestartet werden sollen.

APMD_INTERFACES_TO_UNLOAD Wenn außerdem noch die Teribermodule dieser Interfaces entladen werden müssen, ist diese Variable zu verwenden.

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND Manchmal kommt es auch vor, daß das Wiederaufwachen nach einem Suspend nicht funktioniert, wenn ein IDE Gerät (Festplatte) noch im DMA Modus ist.

Es gibt noch weitere Möglichkeiten, wie z. B. Tastaturwiederholrate oder die Uhrzeit nach einem Suspend zu korrigieren oder den Laptop automatisch herunterzufahren, wenn die das APM-BIOS ein „Batterie kritisch“-Ereignis sendet. Wer noch speziellere Aktionen ausführen möchte, der kann das Script `/usr/sbin/apmd_proxy`, das die oben aufgeführten Jobs ausführt, an seine Bedürfnisse anpassen.

Weitere Befehle

Im `apmd` sind noch einige nützliche Programme enthalten. Mit `apm` kann die aktuelle Batteriekapazität abgefragt werden und das System in Stand-by (`apm -s`) oder Suspend (`apm -s`) geschickt werden; vgl. die Manual-Page von `apm` (`man apm`).

Das Kommando `apmsleep` suspendiert das System für eine vorgegebene Zeit; vgl. `apmsleep`.

Wer eine Logdatei beobachten möchte, ohne die Festplatte ständig am Laufen zu halten, der kann `tailf` als Ersatz für `tail -f` verwenden.

Natürlich gibt es auch hier Tools für das X Window System. Ebenfalls im `apmd` findet man `xapm`, was den Ladezustand der Batterie grafisch anzeigt. Wer den KDE-Desktop verwendet – oder zumindest `kpanel` –, kann sich auch von `kbatmon` den Ladestand des Akkus anzeigen lassen und das System suspendieren. Als Alternative ist auch `xosview` interessant.

ACPI

Um ACPI verwenden zu können, darf APM nicht aktiviert werden. Wenn der Kernel kein APM-BIOS erkennt, geschieht dies automatisch. Ansonsten kann am Bootprompt der Parameter `apm=off` verwendet werden. Natürlich muß der

Computer ACPI 2.0 oder neuer unterstützen. Ob ACPI aktiviert wurde, kann in den Bootmeldungen des Kernels in `/var/log/boot.msg` nachgesehen werden.

Danach müssen jedoch noch eine Reihe von Modulen für das OSPM (Operating System Power Management) geladen werden. Diese werden vom Startscript des ACPI-Daemons geladen. Wenn eines dieser Module Probleme bereitet, kann es in `/etc/sysconfig/powermanagement` vom Laden ausgeschlossen werden.

Jetzt findet man unter `/proc/acpi` eine Reihe von Dateien, die über den Systemzustand informieren oder über die Aktionen wie Suspend ausgelöst werden können. Allerdings funktioniert hier noch längst nicht alles, weil es sich noch in der Entwicklung befindet. Was funktioniert und was nicht, ist jedoch auch stark vom verwendeten Computer abhängig. Hier hilft nur ausprobieren.

Der ACPI-Daemon (acpid)

Ähnlich wie der APM Daemon verarbeitet der ACPI Daemon bestimmte ACPI Ereignisse. Diese sind zur Zeit lediglich die Ereignisse, daß bestimmte Schalter, wie der Ein-/Aus-Schalter oder der Deckelkontakt, betätigt wurden. Alle Ereignisse werden im Systemlog protokolliert. In `/etc/sysconfig/powermanagement` kann in den Variablen `ACPI_BUTTON_POWER` und `ACPI_BUTTON_LID` festgelegt werden, was bei diesen Ereignissen geschehen soll. Wem das nicht genügt, der kann das Script `/usr/sbin/acpid_proxy` anpassen oder die Konfiguration des `acpid` unter `/etc/acpi/` verändern.

Pause für die Festplatte

Man kann unter Linux die Festplatte abschalten, wenn sie nicht benötigt wird. Dazu dient das Programm `hdparm`, mit dem man diverse Einstellungen an den Festplatten vornehmen kann. Mit der Option `-y` wird die Platte sofort in den Stand-by-Modus geschickt, mit `-Y` (Vorsicht!) wird sie vollständig abgeschaltet. Mit `hdparm -S <x>` wird erreicht, dass die Platte nach einer bestimmten Zeit Inaktivität abgeschaltet wird. Der Platzhalter `<x>` hat leicht unterschiedliche Bedeutung: 0 schaltet diesen Mechanismus aus, die Platte läuft immer. Werte von 1 bis 240 werden mit 5 Sekunden multipliziert. 241 bis 251 entsprechen 1 bis 11 mal 30 Minuten.

Häufig ist es aber nicht ganz so einfach, denn es gibt unter Linux eine Vielzahl von Prozessen, die Daten auf die Platte schreiben und dadurch die Platte wieder aufwecken. Deshalb ist es an dieser Stelle wichtig zu verstehen wie Linux mit Daten umgeht, die auf die Platte geschrieben werden sollen.

Alle Daten werden zuerst in einen Puffer im Arbeitsspeicher geschrieben. Dieser Puffer wird vom „Kernel Update Daemon“ (`kupdated`) überwacht. Immer

wenn Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem gewissen Grad gefüllt ist, wird der Puffer geleert und die Daten der Festplatte übergeben. Die Größe des Puffers ist übrigens dynamisch und hängt von der Speichergröße und der Systemauslastung ab. Da das vorrangige Ziel Datensicherheit ist, ist der `kupdated` standardmäßig auf kleine Zeitintervalle eingestellt. Er prüft den Puffer alle 5 Sekunden und benachrichtigt `bdfush`-Daemon, wenn Daten älter als 30 Sekunden sind oder der Puffer zu 30% gefüllt ist. Der `bdfush`-Daemon schreibt dann die Daten auf die Platte. Er schreibt auch unabhängig vom `kupdated` wenn z. B. der Puffer voll ist. Wer ein stabiles System hat kann diese Einstellungen nun verändern. Man muß sich jedoch immer darüber im klaren sein, daß dies auf Kosten der Datensicherheit geht.

Die Einstellungen findet man mit `cat /proc/sys/vm/bdfush`. Der erste Wert ist der Füllgrad des Puffers ab dem der Puffer geleert wird. Der sechste Wert ist das maximale Alter von Daten im Puffer in 1/100 Sekunden. Der fünfte Wert ist das Intervall in dem `kupdated` den Puffer prüft auch in 1/100 Sekunden. Um z. B. das `kupdated`-Intervall auf 1 Minute zu vergrößern schreibt man neue Zahlen in diese Datei mit

```
echo 30 500 0 0 6000 > /proc/sys/vm/bdfush
```

Die Werte vor dem zu verändernden Wert werden dabei einfach abgeschrieben, die Werte danach kann man weglassen. So ändert

```
echo 60 > /proc/sys/vm/bdfush
```

den auslösenden Füllgrad des Puffers auf 60%. Die restlichen Werte sind in den Kernelquellen in der Datei `Documentation/filesystems/proc.txt` beschrieben.

Vorsicht: Änderungen an den Einstellungen des Kernel Update Daemon beeinflussen die Datensicherheit. Wer sich unsicher ist, läßt lieber die Finger davon.

Die Einstellungen für den Festplattentimeout, den `kupdated`-Intervall, den Füllgrad des Puffers und das Alter der Daten können in `/etc/sysconfig/powermanagement` zweifach abgelegt werden: einmal für den Batteriebetrieb und einmal für den Betrieb mit externer Stromversorgung. Die Variablen sind im Abschnitt über den `apmd` und in der Datei selbst beschrieben.

Neben all diesen Vorgängen schreiben sogenannte „Journaling Dateisysteme“ wie z. B. ReiserFS oder Ext3 unabhängig von `bdfush` ihre Metadaten auf die Festplatte, was natürlich auch ein Einschlafen der Platte verhindert. Zur Zeit der Dokumentationserstellung, respektieren Ext3/JBD den 5. Wert in `/proc/sys/vm/bdfush` und schreiben dann auch seltener ihre Metadaten, wenn dieser Wert erhöht wurde. Für ReiserFS wird das gerade implementiert. Voraussichtlich soll also auch dieses Filesystem ein Suspendieren nicht mehr

verhindern. Im Zweifelsfall ist es das beste, auf das gute alte Ext2-Dateisystem zurückzugreifen.

Weiterhin ist natürlich zu beachten, wie sich die Programme verhalten, die man gerade verwendet. Zum Beispiel schreiben gute Texteditoren regelmäßig versteckte Sicherungen der gerade geänderten Datei auf die Platte. Das weckt dann die Platte immer wieder auf. Solche Eigenschaften von Programmen können auch abgeschaltet werden, aber auch hier wieder auf Kosten der Datensicherheit.

In diesem Zusammenhang gibt es für den Maildaemon `postfix` eine Variable `POSTFIX_LAPTOP`. Wenn diese auf `yes` gesetzt wird greift `postfix` wesentlich seltener auf die Festplatte zu. Das ist jedoch nicht von Bedeutung, wenn das Intervall für den `kupdated` verlängert wurde.

IrDA – Infrared Data Association

IrDA („Infrared Data Association“) ist ein Industriestandard für drahtlose Kommunikation über Infrarotlicht. Viele heute ausgelieferte Laptops sind mit einem IrDA-kompatiblen Sender/Empfänger ausgestattet, der die Kommunikation mit anderen Geräten wie Druckern, Modems, LAN oder anderen Laptops ermöglicht. Die Übertragungsrate reicht von 2400 bps bis hin zu 4 Mbps.

Es gibt zwei Betriebsmodi für IrDA. Im Standardmodus SIR wird der Infrarotport über eine serielle Schnittstelle angesprochen. Dieser Modus funktioniert auf fast allen Geräten und genügt für viele Anforderungen. Der schnellere Modus FIR benötigt einen speziellen Treiber für den IrDA Chip. Es gibt aber nicht für alle Chips solche Treiber. Außerdem muss der gewünschte Modus im BIOS Setup des Computers eingestellt werden. Dort erfährt man meist auch, welche serielle Schnittstelle für den SIR Modus verwendet wird.

Informationen zu IrDA finden Sie im IrDA-Howto von Werner Heuser unter <http://mobilix.org/Infrared-HOWTO/Infrared-HOWTO.html> und auf der Homepage des Linux IrDA Projekts <http://irda.sourceforge.net/>.

Software

Die notwendigen Kernelmodule sind im Kernelpaket enthalten. Das Paket `irda` stellt die nötigen Hilfsprogramme zur Unterstützung der Infrarotschnittstelle bereit. Nach der Installation des Paketes findet man die Dokumentation unter `/usr/share/doc/packages/irda/README`.

Konfiguration

Der IrDA Systemdienst wird nicht automatisch beim Booten gestartet. Verwenden Sie das YaST2 Runlevel-Modul um die Einstellungen zu den Systemdiensten zu verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Leider benötigt IrDA merklich mehr (Batterie-)Strom, da alle paar Sekunden ein Discovery-Paket verschickt wird, um andere Peripheriegeräte automatisch zu erkennen. Deshalb sollte man, wenn man auf Batteriestrom angewiesen ist, IrDA am besten nur bei Bedarf starten, Mit dem Kommando

```
rcirda start
```

können Sie die Schnittstelle jederzeit manuell aktivieren bzw. deaktivieren (mit dem Parameter `stop`). Beim Aktivieren der Schnittstelle werden die notwendigen Kernel-Module automatisch geladen.

In der Datei `/etc/sysconfig/irda` gibt es nur eine Variable `IRDA_PORT`. Dort können Sie einstellen welche Schnittstelle im SIR Modus verwendet wird; dies wird über das Skript `/etc/irda/drivers` beim Start der Infrarotunterstützung eingestellt.

Verwendung

Will man nun über Infrarot drucken, kann man dazu über die Gerätedatei `/dev/ir1pt0` die Daten schicken. Die Gerätedatei `/dev/ir1pt0` verhält sich wie die normale drahtgebundene Schnittstelle `/dev/lp0`, nur dass die Druckdaten drahtlos über infrarotes Licht verschickt werden.

Einen Drucker, der über die Infrarotschnittstelle betrieben wird, können Sie wie einen Drucker am Parallelport oder an der seriellen Schnittstelle über einrichten. Beachten Sie bitte beim Drucken, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wird.

Will man über die Infrarotschnittstelle mit anderen Rechnern, mit Handys oder ähnlichen Geräten kommunizieren, so kann man dies über die Gerätedatei `/dev/ircomm0` erledigen. Mit dem Siemens S25 Handy beispielsweise kann man sich über das Programm `wvdial` mittels Infrarot drahtlos ins Internet einwählen. Auch ein Datenabgleich mit dem Palm Pilot ist so möglich, dazu muss im entsprechenden Programm als Gerät einfach `/dev/ircomm0` eingegeben werden.

Beachten Sie bitte auch, dass Sie ohne weiteres nur Geräte ansprechen können, die die Protokolle Printer oder IrCOMM unterstützen. Mit speziellen Programmen (`irobexpalm3`, `irobexreceive`, bitte beachten Sie hierzu die Beschrei-

bung im IR-HOWTO) können Sie auch Geräte ansprechen, die das IROBEX-Protokoll verwenden (3Com Palm Pilot). Die vom Gerät unterstützten Protokolle werden bei der Ausgabe von irdadump nach dem Gerätenamen in eckigen Klammern angegeben. Die Unterstützung des IrLAN-Protokolls ist „work in progress“ – es ist leider zur Zeit noch nicht stabil, wird aber sicher in naher Zukunft auch unter Linux zur Verfügung stehen.

Troubleshooting

Falls Geräte am Infrarotport nicht reagieren, können Sie als Benutzer root mit dem Kommando irdadump überprüfen, ob das andere Gerät vom Computer erkannt wird:

```
irdadump
```

Bei einem Canon BJC-80 Drucker in Sichtweite des Computers erscheint dann eine Ausgabe ähnlich der folgenden in regelmäßiger Wiederholung (vgl. Ausgabe 40).

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [ Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* erde
                        hint=0500 [ PnP Computer ] (21)
```

Ausgabe 40: IrDA: irdadump

Sollte überhaupt keine Ausgabe erfolgen oder das andere Gerät sich nicht zurückmelden, so überprüfen Sie bitte die Konfiguration der Schnittstelle. Verwenden Sie überhaupt die richtige Schnittstelle? Manchmal ist die Infrarotschnittstelle auch unter /dev/ttyS2 oder /dev/ttyS3 zu finden oder ein anderer Interrupt als Interrupt 3 wird verwendet. Diese Einstellungen können Sie aber bei fast jedem Laptop im BIOS-Setup konfigurieren.

Mit einer einfachen Video-Kamera können Sie auch überprüfen, ob die Infrarot-LED überhaupt aufleuchtet – im Gegensatz zum menschlichen Auge können die meisten Videokameras Infrarotlicht sehen.

Der Kernel

Der SuSE Standard-Kernel, der während der Installation auf die Festplatte geschrieben wird ist so konfiguriert, dass er ein möglichst breites Spektrum von Hardware unterstützt.

Die Kernelquellen

Um die Kernelquellen zu übersetzen, müssen folgende Pakete installiert sein: die Kernelquellen (Paket `kernel-source`), der C-Compiler (Paket `gcc`), die GNU Binutils (Paket `binutils`) und die Include-Dateien für den C-Compiler (Paket `glibc-devel`). Generell ist die Installation des C-Compilers dringend anzuraten, da die Programmiersprache C untrennbar mit dem Betriebssystem Linux verbunden ist.

Kernel-Module

Viele Treiber und Features des Linux-Kernels müssen nicht fest zum Kernel hinzugebunden werden, sondern können zur Laufzeit als Kernel-Modul (engl. *kernel module*) geladen werden. Welche Treiber fest zum Kernel gebunden und welche als Module realisiert werden, wird bei der Konfiguration des Kernels festgelegt.

Die Kernelmodule werden im Verzeichnis `/lib/modules/<Version>` abgelegt, wobei `<Version>` der derzeitigen Version des Kernels entspricht.

Umgang mit Modulen

Folgende Befehle zum Umgang mit Modulen stehen zur Verfügung:

- **insmod**
Mit dem Befehl `insmod` wird das angegebene Modul geladen. Das Modul wird in einem Unterverzeichnis von `/lib/modules/<Version>` gesucht. Zugunsten von `modprobe` (s. u.) sollte `insmod` *nicht* mehr verwendet werden.
- **rmmod**
Entlädt das angegebene Modul. Dies ist natürlich nur dann möglich, wenn die entsprechende Funktionalität des Kernels nicht mehr verwendet wird. So ist es nicht möglich, das Modul `isofs` zu entladen, wenn noch eine CD gemountet ist.
- **depmod**
Dieser Befehl erzeugt eine Datei mit dem Namen `modules.dep` im Verzeichnis `/lib/modules/<Version>`, in der die Abhängigkeiten der einzelnen Module untereinander verzeichnet sind. Damit stellt man sicher, dass beim Laden eines Modules alle davon abhängigen Module ebenfalls automatisch geladen werden. Ist die Variable `START_KERNELD` in der Datei `/etc/rc.config` gesetzt, wird die Datei mit den Modul-Abhängigkeiten beim Start des Systems automatisch generiert.
- **modprobe**
Lädt bzw. entlädt ein Modul unter Berücksichtigung der Abhängigkeiten zu anderen Modulen. Dieser Befehl ist sehr mächtig und kann für eine Reihe weiterer Zwecke eingesetzt werden (etwa Durchprobieren aller Module eines bestimmten Typs, bis eines erfolgreich geladen werden kann). Im Gegensatz zu `insmod` wertet `modprobe` die Datei `/etc/modules.conf` aus und sollte daher generell zum Laden von Modulen verwendet werden. Eine ausführliche Erklärung sämtlicher Möglichkeiten finden Sie in den zugehörigen Manual-Pages.
- **lsmod**
Zeigt an, welche Module gegenwärtig geladen sind und von wie vielen anderen Modulen sie verwendet werden. Module, die vom Kernel-Daemon geladen wurden, sind durch ein nachfolgendes `autoclean` gekennzeichnet, so dass diese Module automatisch wieder entfernt werden, wenn sie eine bestimmte Zeit nicht benutzt wurden.

/etc/modules.conf

Das Laden von Modulen wird über die Datei `/etc/modules.conf` beeinflusst; vgl. Manual-Page von `depmod` (`man depmod`).

Insbesondere können in dieser Datei die Parameter für solche Module eingetragen werden, die direkt auf die Hardware zugreifen und daher auf das spezifische System eingestellt werden müssen (z. B. CD-ROM-Treiber oder Netzwerktreiber). Die hier eingetragenen Parameter sind im Prinzip identisch mit denen, die am Bootprompt des Kernels übergeben werden können, jedoch weichen in vielen Fällen die Namen von denen ab, die am Bootprompt zum Einsatz kommen.

Wenn das Laden eines Moduls nicht erfolgreich ist, versuchen Sie, in dieser Datei die Hardware zu spezifizieren und verwenden Sie zum Laden des Moduls `modprobe` anstelle von `insmod`.

Systemmerkmale

Dieses Kapitel enthält wichtige Hinweise zu einigen Softwarepaketen sowie Systemeigenschaften des SuSE Linux Desktop.

| | |
|--|-----|
| Hinweise zu speziellen Softwarepaketen | 146 |
| Virtuelle Konsolen | 151 |
| Tastaturbelegung | 151 |
| Lokale Anpassungen – I18N/L10N | 152 |

Hinweise zu speziellen Softwarepaketen

Paket bash und /etc/profile

In dieser Reihenfolge wertet die bash die Initialisierungsdateien aus, wenn sie als Loginshell aufgerufen wird:

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

Eigene Einträge können Benutzer in ~/.profile bzw. ~/.bashrc vornehmen. Um ordnungsgemäßes Abarbeiten dieser Dateien zu gewährleisten, ist es erforderlich, dass die aktuellen Grundeinstellungen von /etc/skel/.profile bzw. /etc/skel/.bashrc in das Benutzerverzeichnis übernommen werden. Nach einem Update empfiehlt sich deshalb die Einstellungen aus /etc/skel zu übernehmen; um keine eigenen Anpassungen zu verlieren, führen Sie bitte die folgenden Shellbefehle aus:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Danach sind die eigenen Anpassungen aus den Dateien *.old zurückzuschreiben.

Paket cron

Die cron-Tabellen liegen unter /var/spool/cron/tabs. Als systemweite Tabelle wird die Datei /etc/crontab eingerichtet. In der Datei /etc/crontab muss zusätzlich nach der Zeitangabe eingetragen werden, unter welchem Benutzer der jeweilige Auftrag ausgeführt werden soll (vgl. Datei 5 auf der nächsten Seite, dort ist root angegeben); dem gleichen Format folgen paket-spezifische Tabellen, die in /etc/cron.d liegen – vgl. Manual-Page von cron (man 8 cron).

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Datei 5: Beispiel eines Eintrags in /etc/crontab

/etc/crontab kann *nicht* mit `crontab -e` bearbeitet werden, sondern muss direkt in einen Editor geladen, bearbeitet und schließlich gespeichert werden.

Einige Pakete installieren in den Verzeichnissen `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly` Shellskripten, deren Abarbeitung von `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupt-Tabelle (`/etc/crontab`) aufgerufen; so wird sichergestellt, dass eventuell versäumte Läufe rechtzeitig nachgeholt werden. Wundern Sie sich also bitte nicht, wenn kurz nach dem Booten der Benutzer `nobody` in der Prozess-Tabelle mit regen Aktivitäten auftaucht; `nobody` aktualisiert wahrscheinlich dann gerade die `locate`-Datenbank (vgl. Abschnitt *Einstellungen in den Dateien in /etc/sysconfig* auf Seite 182).

Die täglichen Wartungsarbeiten am System sind aus Gründen der Übersichtlichkeit auf mehrere Skripten verteilt worden (Paket `aaa_base`). In `/etc/cron.daily` gibt es also neben `aaa_base` z. B. die Komponenten `backup-rpmdb`, `clean-tmp` oder `clean-vi`.

Protokoll-Dateien – das Paket `logrotate`

Zahlreiche System-Dienste („Daemons“) und auch der Kernel selber protokollieren regelmäßig Systemzustände oder besondere Vorkommnisse in Protokoll-Dateien (engl. *logfiles*). So kann der Administrator zuverlässig feststellen, in welchem Zustand sich das System zu einem bestimmten Zeitpunkt befand, Fehler oder Fehlfunktionen erkennen und gezielt beheben. Diese Protokoll-Dateien werden in der Regel gemäß FHS unter `/var/log` abgelegt und werden von Tag zu Tag größer. Mit Hilfe von Paket `logrotate` ist es möglich, das Wachsen der Protokoll-Dateien zu steuern.

Konfiguration

In der Konfigurationsdatei `/etc/logrotate.conf` wird das generelle Verhalten festgelegt. Mit der `include`-Angabe wird insbesondere konfiguriert, welche weiteren Dateien ausgewertet werden sollen; bei SuSE Linux Desktop ist vorgesehen, dass die einzelnen Pakete in `/etc/logrotate.d` Dateien installieren (beispielsweise `syslog` oder `yast`).

```
# see "man logrotate" for details
# rotate log files weekly
weekly
```

```
# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#     monthly
#     create 0664 root utmp
#     rotate 1
#}

# system-specific logs may be also be configured here.
```

Datei 6: Beispiel für /etc/logrotate.conf

logrotate selbst wird über cron gesteuert; es wird einmal täglich von /etc/cron.daily/logrotate angestoßen.

Hinweis

Die Option `create` liest etwaige Einstellungen ein, die Sie als Administrator in den Dateien `/etc/permissions*` vorgenommen haben könnten. Stellen Sie bitte sicher, dass es bei eigenen Anpassungen zu keinen Konflikten kommt.

Hinweis

Manual-Pages

Für einige GNU-Programme (z. B. `tar`) werden die Manual-Pages nicht mehr weiter gepflegt. An ihre Stelle treten als Schnellübersicht die `--help`-Ausgabe sowie als ausführliche Manuals die Info-Dateien. Info (`info`) ist GNUs Hypertext-System. Mit `info info` erhält man erste Hilfe zur Benutzung; `info` kann entweder über Emacs `emacs -f info` aufgerufen werden, oder standalone: `info`.

Der Befehl ulimit

Mit dem Befehl `ulimit` (engl. *user limits*) ist es möglich, Limits für die Nutzung von Systemressourcen zu setzen, bzw. sich diese anzeigen zu lassen. Insbesondere ist `ulimit` dazu geeignet, den zur Verfügung stehenden Speicher für Anwendungen zu begrenzen. Dadurch kann verhindert werden, dass eine Anwendung übermäßig viel (allen) Speicherplatz für sich beschlagnahmt und dass das System so zum Stillstand kommen könnte.

Der Aufruf von `ulimit` kann mit verschiedenen Optionen geschehen. Um den Speicherverbrauch zu begrenzen, sind z. B. die Optionen in Tabelle 7.1 tauglich.

- m max. Größe des physikalischen Speichers
- v max. Größe des virtuellen Speichers (Swap)
- s max. Größe des Stacks
- c max. Größe der Core-Dateien
- a Anzeige der gesetzten Limits

Tabelle 7.1: `ulimit`: Ressourcen für den Anwender einstellen

Systemweit können die Einstellungen in `/etc/profile` vorgenommen werden. Dort muss beispielsweise das Erzeugen von Core-Dateien freigeschaltet werden, die Programmierer zum „Debuggen“ benötigen. Als Anwender kann man die vom Systemadministrator in `/etc/profile` vorgegebenen Werte nicht erhöhen, aber man kann spezielle Einstellung in die eigene `~/ .bashrc` eintragen.

```
# Begrenzung des realen Speichers:
ulimit -m 98304
```

```
# Begrenzung des virtuellen Speichers:
ulimit -v 98304
```

Datei 7: `ulimit`-Einstellungen in `~/ .bashrc`

Die Speicherangaben müssen in KB gemacht werden. Für detailliertere Informationen werfen Sie bitte einen Blick in die Manual-Page von `bash` (`man bash`).

Hinweis

Nicht alle Shells unterstützen `ulimit`-Angaben. Wenn Sie auf übergreifende Einstellungen für derartige Beschränkungen angewiesen sind, dann bietet PAM (z. B. `pam_limits`) weitgehende Einstellmöglichkeiten.

Hinweis

Der Befehl `free`

Der Befehl `free` ist etwas irreführend, wenn es darum geht herauszufinden, wie der Arbeitsspeicher gerade verwendet wird...

Die nützlichen Informationen findet man in `/proc/meminfo`. Heutzutage sollte sich eigentlich kein Anwender darum Gedanken machen, dem ein modernes Betriebssystem wie Linux zur Verfügung steht. Das Konzept vom „freien Arbeitsspeicher“ datiert von der Zeit her, als es noch keine vereinheitlichte Speicherverwaltung (engl. *unified memory management*) gab – unter Linux gilt das Motto: *freier Speicher ist schlechter Speicher* (engl. *free memory is bad memory*). Infolgedessen ist Linux immer bestrebt, verschiedene Caches auszubalancieren, nie aber wirklich freien (= ungenutzten) Speicher zuzulassen.

Der Kernel weiß im Grunde nichts direkt von Programmen oder Benutzerdaten; er verwaltet Programme und Benutzerdaten im so genannten „Page Cache“. Wenn der Speicher knapp wird, werden Teile davon entweder in den Swapbereich oder in die Dateien geschrieben, aus denen sie ursprünglich mit Hilfe des Systemaufrufs `mmap` gelesen wurden; vgl. Manual-Page von `mmap` (`man 2 mmap`).

Des Weiteren hält der Kernel auch noch andere Zwischenspeicher, wie den „slab cache“, der z. B. die für den Netzwerkzugriff benutzten Puffer enthält. Dadurch werden eventuelle Differenzen zwischen den Zählern in `/proc/meminfo` erklärt. Die meisten, aber nicht alle, sind über `/proc/slabinfo` abfragbar.

Die `/etc/resolv.conf`

Die Namensauflösung wird über die Datei `/etc/resolv.conf` geregelt; vgl. Abschnitt [DNS – Domain Name Service](#) auf Seite 227.

Diese Datei wird stets nur von dem Skript `/sbin/modify_resolvconf` aktualisiert. Es ist keinem Programm erlaubt, `/etc/resolv.conf` direkt zu manipulieren. Nur wenn diese Regel beachtet wird, kann sichergestellt werden, dass die Netzwerkkonfiguration und zugehörigen Daten konsistent gehalten werden.

Virtuelle Konsolen

Linux ist multitasking- und multiuserfähig. Auch bei einem Ein-Benutzer-PC-System werden Sie die Vorteile, die diese Fähigkeiten mitbringen, schätzen lernen:

Im Textmodus stehen 6 virtuelle Konsolen zur Verfügung, zwischen denen Sie durch die Tastenkombinationen **(Alt) + (F1)** bis **(Alt) + (F6)** wechseln können. Die siebte Konsole ist für X11 reserviert. Durch Modifikation der Datei `/etc/inittab` können auch weitere oder weniger Konsolen zur Verfügung gestellt werden.

Wenn Sie von X11 aus auf eine Textkonsole zurückschalten möchten, ohne X11 zu beenden, verwenden Sie **(Ctrl) + (Alt) + (F1)** bis **(Ctrl) + (Alt) + (F6)**. Mit **(Alt) + (F7)** kommen Sie zu X11 zurück.

Tastaturbelegung

Um die Tastaturbelegung von Programmen zu vereinheitlichen, wurden Änderungen an den folgenden Dateien vorgenommen:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/⟨VERSION⟩/site-lisp/term/*.el
/usr/lib/joerc
```

Diese Änderungen wirken sich nur auf die Applikationen aus, die die `terminfo`-Einträge auslesen, bzw. deren Konfigurationsdateien direkt verändert wurden (`vi`, `less` etc.). Andere nicht-SuSE-Applikationen sollten an diese Vorgaben angepasst werden.

Unter X ist die Compose-Taste („Multi_key“) über die Tastenkombination **(Ctrl) + (↑)** (rechts) zu erreichen; vgl. den Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Lokale Anpassungen – I18N/L10N

SuSE Linux Desktop ist sehr weitgehend internationalisiert und kann flexibel auf lokale Gegebenheiten abgestimmt werden; anders gesagt: die Internationalisierung („I18N“) erlaubt spezielle Lokalisierungen („L10N“). Die Abkürzungen I18N und L10N stehen für *internationalization* und *localization*: jeweils Anfangs- und Endbuchstabe und dazwischen die Anzahl der ausgelassenen Buchstaben.

Die Einstellungen werden über LC_*-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dabei geht es nicht nur um die Einstellung der Sprache für die Programmoberfläche und -meldungen (engl. *native language support*), sondern im Einzelnen um die Kategorien für *Nachrichten* (Sprache), *Zeichenklassen*, *Sortierreihenfolge*, *Datum und Uhrzeit*, *Zahlen* und *Geld*. Jede dieser Kategorien kann entweder gezielt über eine eigene Variable oder indirekt über eine übergeordnete Variable in der Datei `language` festgelegt werden (vgl. Manual-Page von `locale` (`man 5 locale`)):

1. `RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`: Diese Variablen werden ohne den `RC_`-Vorsatz an die Shell weitergereicht und bestimmen die o. g. Kategorien; die betroffenen Dateien werden im Folgenden aufgezählt.

Die aktuelle Einstellung kann mit dem Befehl `locale` abgefragt werden.

2. `RC_LC_ALL`: Diese Variable überschreibt, falls gesetzt, die Werte der in Punkt 1 genannten Variablen.
3. `RC_LANG`: Wenn keine der o. g. Variablen gesetzt ist, ist diese der „Fall-back“. SuSE Linux Desktop setzt standardmäßig nur `RC_LANG`; dadurch kann der Anwender leichter eigene Werte eintragen.
4. `ROOT_USES_LANG`: Eine `yes/no`-Variable. Ist sie auf `no` gesetzt, dann arbeitet `root` immer in der POSIX-Umgebung.

Die Variablen sind über den `sysconfig`-Editor zu setzen.

Der Wert einer solchen Variablen setzt sich aus Sprachangabe (engl. *language code*), Land oder Territorium (engl. *country code*), Zeichensatz (engl. *encoding*) und Option (engl. *modifier*) zusammen. Die einzelnen Angaben werden mit Spezialzeichen verbunden:

```
LANG=<language>[_<COUNTRY>].Encoding[@Modifier]
```

Einige Beispiele

Bitte setzen Sie die Sprach- und die Länderangabe immer zusammen. Die Angabe der Sprache folgt dem Standard ISO 639 (<http://www.evertype.com/standards/iso639/iso639-en.html> und <http://www.loc.gov/standards/iso639-2/>), die Ländercodes sind in ISO 3166 (http://www.din.de/gremien/nas/nabd/iso3166ma/codlstpl/en_listpl.html) festgelegt. Sinnvollerweise dürfen aber nur die Werte gewählt werden, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Weitere Beschreibungsdateien lassen sich mit Hilfe von `localedef` aus den Dateien in `/usr/share/i18n` erzeugen. Eine Beschreibungsdatei für `de_DE@euro.UTF-8` wird so erzeugt mit:

```
erde:~ # localedef -i de_DE@euro -f UTF-8 de_DE@euro.UTF-8
```

LANG=de_DE.ISO-8859-1

So stellt man deutsche Sprache in Deutschland mit Zeichensatz ISO-8859-1 ein. Dieser Zeichensatz enthält nicht das Euro-Zeichen; man benötigt diesen Zeichensatz bisweilen noch, wenn ein Programm noch nicht an ISO-8859-15 angepasst ist.

Die Angabe des Zeichensatzes (hier ISO-8859-1) wertet z. B. der Emacs aus.

LANG=de_DE@euro

Dies ist ein Beispiel für das Setzen einer Option (`euro`). Die Einstellung `de_DE@euro` ist die Vorgabe für eine Standardinstallation in deutscher Sprache.

LANG=de_DE.UTF-8

Wenn man in einem Unicode-xterm arbeitet, ist die Angabe UTF-8 zu machen. Um ein xterm für UTF-8 zu starten, sollte man sich ein einfaches Shell-Skript etwa unter dem Namen `uxterm` anlegen; vgl. Datei 8.

```
#!/bin/bash
export LANG=de_DE.UTF-8
xterm -fn \
-Misc-Fixed-Medium-R-Normal--18-120-100-100-C-90-ISO10646-1 \
-T 'xterm UTF-8' $*
```

Datei 8: uxterm zum Starten eines Unicode-xterm

SuSEconfig liest die Variablen aus `/etc/sysconfig/language` aus und schreibt die Angaben nach `/etc/SuSEconfig/profile` und `/etc/`

SuSEconfig/csh.cshrc. /etc/SuSEconfig/profile wird von /etc/profile eingelesen („gesourcet“) und /etc/SuSEconfig/csh.cshrc von /etc/csh.cshrc. Somit stehen die Einstellungen systemweit zur Verfügung. Die Benutzer können die Systemvorgaben in ~/.bashrc überschreiben. Wenn also die Systemvorgabe de_DE ist, kann der Benutzer, falls er mit deutschen Programmierungen nicht zufrieden ist, so auf englische Ausgaben umschalten:

```
LC_MESSAGES=en_US
```

Anpassung für Sprachunterstützung

Hinweisend ist zu sagen, dass die Dateien der Kategorie *Nachrichten* in der Regel nur im Sprachverzeichnis (z. B. de) abgelegt werden, um ein Fallback zu haben. Wenn man also LANG auf de_AT setzt und die „Message“-Datei unter /usr/share/locale/de_AT/LC_MESSAGES nicht vorhanden ist, dann wird auf /usr/share/locale/de/LC_MESSAGES zurückgegriffen.

Auch kann man mit LANGUAGE eine Fallbackkaskade festlegen; z. B. für bretonisch → französisch oder für galizisch → spanisch → portugiesisch:

```
LANGUAGE="br_FR:fr_FR"  
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Oder um – je nach Vorliebe – auf die norwegischen Variaten „nynorsk“ bzw. „bokmål“ auszuweichen (mit zusätzlichem Rückfall auf no):

```
LANG="nn_NO"  
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"  
LANGUAGE="nb_NO:nn_NO:no"
```

Bei Norwegisch ist auch zu beachten, dass LC_TIME unterschiedlich behandelt wird.

Mögliche Probleme

- Der Tausenderpunkt wird nicht erkannt. Wahrscheinlich steht LANG beispielsweise auf de. Da die Beschreibung, auf die die glibc zurückgreift, in /usr/share/locale/de_DE/LC_NUMERIC zu finden ist, muss beispielsweise LC_NUMERIC auf de_DE gesetzt werden.

Weitere Informationen:

- *The GNU C Library Reference Manual*, Kap. "Locales and Internationalization"; enthalten im Paket `glibc-info`.
- Jochen Hein [[Hei96](#)], unter dem Stichwort "NLS".
- *German-Howto* von Winfried Trümper <file:/usr/share/doc/howto/en/html/German-HOWTO.html>
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, aktuell unter <http://www.cl.cam.ac.uk/~mgk25/unicode.html>.
- *Unicode-Howto* von Bruno Haible
<file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html>.

Das Bootkonzept

Das Booten und die Initialisierung eines Unix-Systems sind selbst für einem erfahrenen System-Administrator keineswegs trivial. Dieses Kapitel gibt eine kurze Einführung in das Bootkonzept von SuSE Linux Desktop. Die vorliegende Implementierung setzt den LSB (engl. *Linux Standard Base*) in Version 1.2 um.

| | |
|--|-----|
| Das init-Programm | 158 |
| Die Runlevels | 158 |
| Wechsel des Runlevels | 160 |
| Die Init-Skripten | 161 |
| Der YaST2 Runlevel-Editor | 164 |
| SuSEconfig, /etc/sysconfig und /etc/rc.config | 165 |
| Systemkonfiguration mit dem YaST2 Sysconfig-Editor | 167 |
| Skripte und Variablen – Konfiguration des Systems | 167 |

Mit den lapidaren Worten "Uncompressing Linux..." übernimmt der Kernel die Kontrolle über die gesamte Hardware des Systems. Er prüft und setzt die Konsole – oder genauer: die BIOS-Register der Graphikkarte und das Ausgabeformat auf den Bildschirm –, um danach die Einstellungen im BIOS zu lesen und die elementaren Schnittstellen des Mainboards zu initialisieren. In den nächsten Schritten „proben“ die einzelnen Treiber – die ja Bestandteil des Kernels sind – die vorhandene Hardware, um sie gegebenenfalls zu initialisieren. Nach dem Überprüfen der Partitionen und dem Mounten des Root-Dateisystems startet der Kernel das Programm `init`. Durch `init` wird das eigentliche System „hochgefahren“ (Unix-Jargon) und die vielen Dienstprogramme und deren Konfiguration werden so gestartet. Der Kernel verwaltet dann das gesamte System; er überwacht Rechenzeit für die einzelnen Programme, er stellt Speicher zur Verfügung und steuert Hardware-Zugriffe.

Das `init`-Programm

Das Programm `init` ist der für die korrekte Initialisierung des Systems zuständige Prozess; es ist sozusagen der „Vater aller Prozesse“ im System.

Unter allen Programmen nimmt `init` eine Sonderrolle ein: `init` wird direkt vom Kernel gestartet und ist immun gegen das Signal 9, mit dem normalerweise jeder Prozess „gekillt“ werden kann. Alle weiteren Prozesse werden entweder von `init` selbst oder von einem seiner „Kindprozesse“ gestartet.

Konfiguriert wird `init` zentral über die Datei `/etc/inittab`; hier werden die so genannten „Runlevels“ definiert (mehr dazu im nächsten Abschnitt [Die Runlevels](#) auf dieser Seite) und es wird festgelegt, welche Dienste und Daemons in den einzelnen Levels zur Verfügung stehen sollen. Abhängig von den Einträgen in `/etc/inittab` ruft `init` verschiedene Skripten auf, die aus Gründen der Übersichtlichkeit im Verzeichnis `/etc/init.d` zusammengefasst sind.

Der gesamte Hochlauf des Systems – und natürlich auch das Herunterfahren – wird somit einzig und allein vom `init`-Prozess gesteuert; insofern lässt sich der Kernel quasi als „Hintergrundprozess“ betrachten, dessen Aufgabe darin besteht, die gestarteten Prozesse zu verwalten, ihnen Rechenzeit zuzuteilen und den Zugriff auf die Hardware zu ermöglichen und zu kontrollieren.

Die Runlevels

Unter Linux existieren verschiedene *Runlevels*, die den jeweiligen Zustand des Systems definieren. Der Standard-Runlevel, in dem das System beim Booten

hochfährt, ist in der Datei `/etc/inittab` durch den Eintrag `initdefault` festgelegt. Für gewöhnlich ist dies 3 oder 5 (siehe Tabelle 8.1 auf der nächsten Seite). Alternativ kann der gewünschte Runlevel beim Booten (z. B. am Boot-Prompt) angegeben werden; der Kernel reicht die Parameter, die er nicht selbst auswertet, unverändert an den `init`-Prozess weiter.

Um zu einem späteren Zeitpunkt in einen anderen Runlevel zu wechseln, kann man `init` mit der Nummer des zugehörigen Runlevels aufrufen; das Wechseln des Runlevels kann nur vom Systemadministrator veranlasst werden.

Beispielsweise gelangt man durch das Kommando

```
root@erde:/ > init 1
```

in den *Einzelbenutzerbetrieb* (engl. *Single user mode*), der der Pflege und Administration des Systems dient. Nachdem der Systemadministrator seine Arbeit beendet hat, kann er durch

```
root@erde:/ > init 3
```

das System wieder in den normalen Runlevel hochfahren lassen, in dem alle für den Betrieb erforderlichen Programme laufen und sich die einzelnen Benutzer beim System anmelden können.

Die Tabelle 8.1 auf der nächsten Seite gibt einen Überblick über die zur Verfügung stehenden Runlevel. Runlevel 2 sollte auf einem System, dessen `/usr`-Partition via NFS gemountet ist, nicht verwendet werden!

Daraus folgt insbesondere, dass Sie das System auch durch

```
root@erde:/ > init 0
```

anhalten, bzw. durch

```
root@erde:/ > init 6
```

zu einem Neustart veranlassen können.

Bei einer Standardinstallation von SuSE Linux Desktop wird normalerweise Runlevel 5 als Standard eingerichtet, so dass sich die Benutzer direkt an der grafischen Oberfläche beim System anmelden können. Sollte die Einrichtung von Runlevel 5 durch manuellen Eingriff verhindert worden sein, so kann man nun nachträglich eine Umkonfiguration vornehmen.

Wenn Sie den Runlevel von 3 auf 5 setzen wollen, muss sichergestellt sein, dass das X Window System bereits korrekt konfiguriert ist; (Kapitel [Das X Window System](#) auf Seite 57). Ob das System so wie von Ihnen gewünscht funktioniert, testen Sie danach durch Eingabe von:

| Runlevel | Bedeutung |
|----------|---|
| 0 | Systemhalt (engl. <i>System halt</i>) |
| S | Einzelbenutzerbetrieb (engl. <i>Single user mode</i>); vom Bootprompt aus mit US-Tastaturbelegung |
| 1 | Einzelbenutzerbetrieb (engl. <i>Single user mode</i>) |
| 2 | Lokaler Multiuserbetrieb ohne entferntes Netzwerk (engl. <i>Local multiuser without remote network (e. g. NFS)</i>) |
| 3 | Voller Multiuserbetrieb mit Netzwerk (engl. <i>Full multiuser with network</i>) |
| 4 | Frei (engl. <i>Not used</i>) |
| 5 | Voller Multiuserbetrieb mit Netzwerk und KDM (Standard), GDM oder XDM (engl. <i>Full multiuser with network and xdm</i>) |
| 6 | Systemneustart (engl. <i>System reboot</i>) |

Tabelle 8.1: Liste der gültigen Runlevels unter Linux

```
root@erde:/ > init 5
```

Ist dies der Fall, können Sie den Standard-Runlevel über YdST2 auf 5 ändern.

Tipp

Eigene Änderungen an `/etc/inittab`

Eine zerstörte `/etc/inittab` kann dazu führen, dass das System nicht mehr korrekt hochgefahren wird. Gehen Sie bei Veränderungen dieser Datei deshalb mit besonderer Sorgfalt vor und behalten Sie immer eine Kopie einer intakten Datei. Zur Behebung des Schadens können Sie versuchen, am Boot-Prompt den Parameter `init=/bin/sh` zu übergeben, um direkt in eine Shell zu booten und von dort aus die Datei wiederherzustellen: `boot: linux init=/bin/sh`

Nach dem Booten spielen Sie mittels `cp` die Backupkopie wieder ein.

Tipp

Wechsel des Runlevels

Generell passieren bei einem Wechsel des Runlevels folgende Dinge: Die *Stopp-Skripten* des gegenwärtigen Runlevels werden ausgeführt – dabei werden typischerweise verschiedene, in diesem Level laufende Programme beendet – und

die *Start-Skripten* des neuen Runlevels werden ausgeführt. Während eines solchen Vorgangs werden in den meisten Fällen einige Programme gestartet.

Um dies zu verdeutlichen, betrachten wir an einem Beispiel den Wechsel von Runlevel 3 nach Runlevel 5:

- Der Administrator (`root`) teilt dem `init`-Prozess mit, dass der Runlevel gewechselt werden soll:

```
root@erde:/ > init 5
```

- `init` konsultiert die Konfigurationsdatei `/etc/inittab` und stellt fest, dass das Skript `/etc/init.d/rc` mit dem neuen Runlevel als Parameter aufgerufen werden muss.
- Nun ruft `rc` alle Stopp-Skripten des gegenwärtigen Runlevels auf, für die im neuen Runlevel kein Start-Skript existiert; in unserem Beispiel sind das alle Skripte, die sich im Verzeichnis `/etc/init.d/rc3.d` befinden (der alte Runlevel war 3) und mit einem `'K'` beginnen. Die nach dem `'K'` folgende Zahl gewährleistet, dass hierbei eine bestimmte Reihenfolge eingehalten wird, da unter Umständen manche Programme von anderen abhängig sind.

Hinweis

Die Namen der Stopp-Skripten beginnen immer mit `'K'` (engl. *kill*), die der Start-Skripten mit `'S'` (engl. *start*).

Hinweis

- Als Letztes werden die Start-Skripten des neuen Runlevels aufgerufen; diese liegen in unserem Beispiel unter `/etc/init.d/rc5.d` und beginnen mit einem `'S'`. Auch hierbei wird eine bestimmte Reihenfolge eingehalten, die durch die dem `'S'` folgende Zahl festgelegt ist.

Wenn Sie in denselben Runlevel wechseln, in dem Sie sich bereits befinden, liest `init` nur die `/etc/inittab` ein, prüft sie auf Veränderungen und nimmt bei Bedarf die entsprechenden Maßnahmen vor, etwa das Starten eines `getty` auf einer weiteren Schnittstelle.

Die Init-Skripten

Die Skripten unter `/etc/init.d` unterteilen sich in zwei Kategorien:

| Option | Bedeutung |
|--------------|--|
| start | Dienst starten |
| stop | Dienst stoppen |
| restart | Dienst stoppen und erneut starten, wenn der Dienst bereits lief; andernfalls den Dienst starten |
| reload | Konfiguration des Dienstes erneut einlesen, ohne den Dienst zu stoppen und neu zu starten |
| force-reload | Konfiguration des Dienstes erneut einlesen, wenn der Dienst dies unterstützt; andernfalls wie <code>restart</code> |
| status | aktuellen Status anzeigen |

Tabelle 8.2: Übersicht der Optionen der init-Skripten

- Skripte, die direkt von `init` aufgerufen werden: Dies ist nur beim Booten der Fall sowie bei einem sofortigen Herunterfahren des Systems (bei Stromausfall oder durch Drücken der Tastenkombination `(Ctrl) + (Alt) + (Entf)` durch den Anwender).
- Skripte, die indirekt von `init` aufgerufen werden: Das geschieht bei einem Wechsel des Runlevels; es wird generell das übergeordnete Skript `/etc/init.d/rc` ausgeführt, das dafür sorgt, dass die relevanten Skripten in der korrekten Reihenfolge aufgerufen werden.

Alle Skripten befinden sich unter `/etc/init.d`. Die Skripten für das Wechseln des Runlevels befinden sich ebenfalls in diesem Verzeichnis, werden jedoch grundsätzlich als symbolischer Link aus einem der Unterverzeichnisse `/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d` aufgerufen. Dies dient der Übersichtlichkeit und vermeidet, dass Skripten mehrfach vorhanden sein müssen, etwa weil sie in verschiedenen Runlevels verwendet werden sollen. Da jedes dieser Skripten sowohl als Start- wie auch als Stopp-Skript aufgerufen werden kann, müssen sie alle die beiden möglichen Parameter `start` und `stop` verstehen. Zusätzlich verstehen die Skripten die Optionen `restart`, `reload`, `force-reload` und `status`; die Bedeutung aller Optionen ist in [Tabelle 8.2](#) aufgelistet.

Beim Verlassen des Runlevels 3 wird `/etc/init.d/rc3.d/K40network` aufgerufen; `/etc/init.d/rc` ruft das Skript `/etc/init.d/network` mit dem Parameter `stop` auf. Beim Eintritt in Runlevel 5 wird letztlich das gleiche Skript gestartet, diesmal jedoch mit dem Parameter `start`.

Die Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen dienen somit also nur dazu, eine Zuordnung der einzelnen Skripten zu bestimmten

Runlevels zu ermöglichen.

Die Anlage und das Entfernen der notwendigen Links geschieht mit `insserv` (bzw. dem Link `/usr/lib/lsb/install_initd`) beim Installieren oder Deinstallieren des jeweiligen Paketes; vgl. Manual-Page von `insserv` (`man 8 insserv`).

Im Folgenden finden Sie eine kurze Beschreibung der ersten Boot- und der letzten Shutdown-Skripten sowie des Steuerskripts:

boot Wird beim Start des Systems ausgeführt und direkt von `init` gestartet. Es ist unabhängig vom gewünschten Default-Runlevel und wird nur genau ein einziges Mal ausgeführt: Im Wesentlichen werden `proc`- und `devpts`-Dateisystem eingehängt („gemountet“), der `blogd` (engl. *Boot Logging Daemon*) wird aktiert und – nach einer Erstinstallation oder einem Update des Systems – wird eine Grundkonfiguration angestoßen.

Diesem Skript ist des Weiteren das Verzeichnis `/etc/init.d/boot.d` zugeordnet; alle in diesem Verzeichnis gefundenen Skripte, die mit `'S'` beginnen, werden automatisch beim Hochlauf des Systems ausgeführt. Es werden die Dateisysteme geprüft, etwaige überflüssige Dateien unter `/var/lock` gelöscht und das Netzwerk für das Loopback-Device konfiguriert, sofern dies vorgesehen ist. Weiterhin wird die Systemzeit gesetzt.

Tritt beim Prüfen und automatischen Reparieren der Dateisysteme ein schwerer Fehler auf, hat der Systemadministrator nach Eingabe des Root-Passwortes die Möglichkeit, manuell eine Lösung des Problems herbeizuführen.

Schließlich wird das Skript `boot.local` ausgeführt.

boot.local Hier können weitere Dinge eingetragen werden, die beim Start geschehen sollen, bevor das System in einen der Runlevels eintritt; es kann von seiner Funktion her mit der vielleicht von DOS her gewohnten `AUTOEXEC.BAT` verglichen werden.

boot.setup Grundlegende Einstellungen, die beim Übergang vom Einzelnutzerbetrieb in irgendeinen Runlevel vorgenommen werden müssen.

Hier werden die Tastaturbelegung und die Konsolenkonfiguration geladen.

halt Dieses Skript wird nur beim Eintritt in den Runlevel 0 oder 6 ausgeführt. Dabei wird es entweder unter dem Namen `halt` oder dem Namen `reboot` aufgerufen. Abhängig davon, wie `halt` aufgerufen wurde, wird das System neu gestartet oder ganz heruntergefahren.

rc Das übergeordnete Skript, das bei jedem Wechsel des Runlevels aufgerufen wird. Es führt die Stopp-Skripten des gegenwärtigen Runlevels aus und danach die Start-Skripten des neuen.

Eigene Skripten lassen sich anhand dieses Konzepts hinzufügen. Ein Gerüst ist in `/etc/init.d/skeleton` vorbereitet. Das genaue Format ist im Entwurf des LSB beschrieben; dort wird insbesondere festgelegt, in welcher Reihenfolge und in welchen Levels das jeweilige Skript abgearbeitet werden muss. Nun sind Links mit `insserv` von dem jeweiligen `rc`-Verzeichnis auf das neue Skript anzulegen, damit das Skript – wie oben beschrieben – beim Wechsel des Runlevels ausgeführt wird; die Namensgebung für die Links wird ebendort beleuchtet. Die technischen Details werden in der Manual-Page von `init.d` (`man 7 init.d`) und Manual-Page von `insserv` (`man 8 insserv`) dargestellt. Als grafisches Konfigurationswerkzeug zum Anlegen der Links steht der Runlevel-Editor von YaST2 zur Verfügung; vgl. Abschnitt [Der YaST2 Runlevel-Editor](#) auf dieser Seite.

Achtung

Erstellung eigener init-Skripten

Fehlerhafte `init`-Skripten können das gesamte System „aufhängen“. Erstellen Sie eigene Skripte mit äußerster Sorgfalt und testen Sie sie – soweit möglich – vor dem Ernstfall in der Multiuserumgebung. Grundlageninformation zum Umgang mit Runleveln/`init`-Skripten finden Sie im Abschnitt [Die Runlevels](#) auf Seite 158.

Achtung

Der YaST2 Runlevel-Editor

Nach dem Start wird dieses Experten-Modul zunächst initialisiert. Im nächsten Dialog wird der aktuelle Standard-Runlevel angezeigt. Dieser „Betriebsmodus“ wird nach dem Booten Ihres Systems hochgefahren. Bei SuSE Linux Desktop ist dies üblicherweise Runlevel 5 (voller Multiuserbetrieb mit Netzwerk und KDM, dem grafischen Login). Geeignet wäre z. B. auch Runlevel 3 (voller Multiuserbetrieb mit Netzwerk). An dieser Stelle lässt sich mit Hilfe von YaST2 ein anderer Default-Runlevel einstellen; vgl. Tabelle 8.1 auf Seite 160.

Mit ‘Bearbeiten’ gelangen Sie zu einer Übersicht aller Dienste und Daemonen mit der Information, ob diese in Ihrem System aktiv geschaltet sind und für welche Runlevels dies gilt. Wenn Sie eine Zeile per Mausklick markieren, haben Sie die Möglichkeit, die Checkboxes für die Runlevels ‘0’, ‘1’, ‘2’, ‘3’, ‘5’, ‘6’ und ‘S’ zu aktivieren und damit festzulegen, für welche Runlevels der entsprechende

Dienst bzw. Daemon aktiv werden soll. Runlevel 4 ist nicht definiert – dieser ist stets frei für benutzereigene Einstellungen.

Mit 'Starten' und 'Anhalten' entscheiden Sie, ob ein Dienst eingesetzt werden soll. Mit 'Aktualisieren' sind Sie in der Lage, den aktuellen Status zu prüfen, falls dies nicht automatisch geschieht. 'Auf Standardwert zurücksetzen' dient der Wiederherstellung der Standardeinstellungen, das ist der Zustand nach der Installation. 'Dienst aktivieren' erscheint nur, wenn der Dienst derzeit deaktiviert ist. 'Alle Dienste auf Standardwert zurücksetzen' versetzt alle Dienste in den ursprünglichen Zustand, wie er nach der Installation ist. Mit 'Beenden' speichern Sie die Systemkonfiguration.

Achtung

Editieren der Runlevel-Einstellungen

Fehlerhafte Einstellungen von Systemdiensten und Runleveln können Ihr System unbrauchbar machen. Informieren Sie sich vor einer Änderung dieser Einstellungen über die möglichen Folgen, um die Funktionsfähigkeit Ihres Systems zu gewährleisten.

Achtung

SuSEconfig, /etc/sysconfig und /etc/rc.config

Die wesentliche Konfiguration von SuSE Linux Desktop nehmen Sie über die Konfigurationsdateien unter `/etc/sysconfig` vor. Die Datei `/etc/rc.config`, die bisher 8.0 für die Systemkonfiguration genutzt wurde, wird „leer“ beibehalten, damit Ihren selbsterstellten Skripten Ihre eigenen Einstellungen nicht verlorengehen und weiterhin global ausgewertet werden können.

Auf die Dateien in `/etc/sysconfig` wird nur gezielt von einzelnen Skripten zugegriffen; dadurch wird gewährleistet, dass die Netzwerkeinstellungen auch nur von dem Netzwerk-Skripten ausgewertet werden müssen.

Darüber hinaus werden viele weitere Konfigurationsdateien des Systems in Abhängigkeit von den Dateien in `/etc/sysconfig` generiert; diese Aufgabe erledigt SuSEconfig. So wird beispielsweise nach einer Änderung der Netzwerkkonfiguration die Datei `/etc/host.conf` neu erzeugt, da sie abhängig von der Art der Konfiguration ist.

Wenn Sie Änderungen an den genannten Dateien vornehmen, müssen Sie nachfolgend immer SuSEconfig aufrufen, so dass die neuen Einstellungen auch an

allen relevanten Stellen wirksam werden. Verändern Sie die Konfiguration mit YaST2, brauchen Sie sich darum nicht explizit zu kümmern; YaST2 startet automatisch SuSEconfig, wodurch die betroffenen Dateien auf den aktuellen Stand gebracht werden.

Dieses Konzept ermöglicht es, grundlegende Änderungen an der Konfiguration des Rechners vornehmen zu können, ohne die Maschine neu booten zu müssen. Da manche Einstellungen sehr tiefgreifend sind, müssen jedoch unter Umständen einige Programme neu gestartet werden, um die Änderungen wirksam werden zu lassen.

Durch Verwendung der Kommandos

```
erde:~ # rcnetwork stop
erde:~ # rcnetwork start
```

wird erreicht, dass die von der Änderung betroffenen Netzwerk-Programme neu gestartet werden. Wie Sie sehen, können die Init-Skripten auch von Hand aufgerufen werden.

Generell ist für das Konfigurieren des Systems folgender Weg zu empfehlen:

- Bringen Sie das System in den „single user mode“ (Runlevel 1):

```
erde:~ # init 1
```

- Nehmen Sie die gewünschten Änderungen an den Konfigurationsdateien vor. Dies entweder kann mit einem Texteditor geschehen oder besser mit dem Sysconfig-Editor von YaST2; vgl. in Abschnitt [Systemkonfiguration mit dem YaST2 Sysconfig-Editor](#) auf der nächsten Seite.
- Führen Sie SuSEconfig aus, um die Änderungen in die verschiedenen weiteren Konfigurationsdateien eintragen zu lassen. Dies geschieht automatisch, wenn Sie YaST2 verwendet haben, um den Runlevel zu setzen.
- Bringen Sie das System in den vorherigen Runlevel zurück (hier im Beispiel 3):

```
erde:~ # init 3
```

Diese Vorgehensweise ist natürlich nur bei sehr weitreichenden Änderungen an den Einstellungen des Systems erforderlich (z. B. Netzwerkkonfiguration); bei einfachen Aufgaben ist es nicht erforderlich, für die Administration in den „single user mode“ zu wechseln; jedoch stellen Sie damit sicher, dass auch wirklich alle von der Änderung betroffenen Programme neu gestartet werden.

Tipp

Sie können die automatische Konfiguration via SuSEconfig *global* abschalten, indem Sie die Variable `(ENABLE_SUSECONFIG)` in `/etc/sysconfig/suseconfig` auf `no` setzen. Wollen Sie den Installationssupport in Anspruch nehmen, muss `(ENABLE_SUSECONFIG)` allerdings auf `yes` gesetzt sein. Einzelne Teile der Autokonfiguration können auch gezielt deaktiviert werden.

Tipp

Systemkonfiguration mit dem YaST2 Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig` sind die Dateien mit den wichtigsten Einstellungen für SuSE Linux Desktop hinterlegt (ehemals in der Datei `/etc/rc.config` zentral verwaltet). Der YaST2 Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Editieren allerdings nicht notwendig, da bei der Installation eines Paketes oder beim Einrichten eines Dienstes etc. die Dateien automatisch angepasst werden.

Achtung**Änderungen in den `/etc/sysconfig/*`-Dateien**

Ihre Änderungen in `/etc/sysconfig/*` haben tiefgreifende Folgen für Ihr gesamtes System. Bitte informieren Sie sich vor jeder Änderung ausreichend über die möglichen Folgen. So stellen Sie sicher, dass Ihr System funktionsfähig bleibt.

Achtung

Skripte und Variablen

Im Folgenden werden die einzelnen Parameter des Systems und ihre Einstellungen *in Auswahl* kurz beschrieben. Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` *nicht* mit YaST bearbeiten, achten Sie darauf, dass Sie einen leeren Parameter als zwei aufeinander folgende Anführungszeichen schreiben

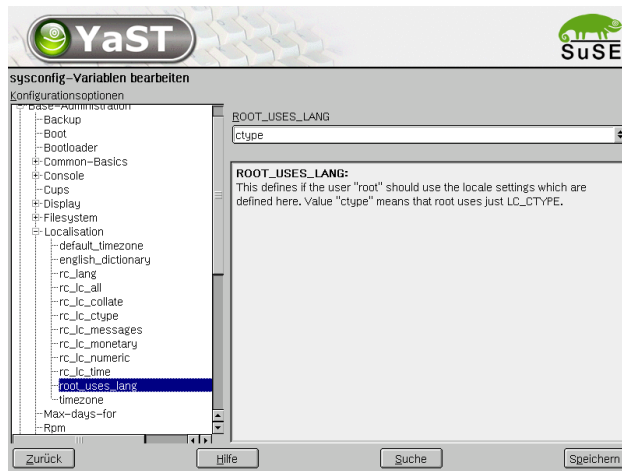


Abbildung 8.1: YaST2: Konfiguration des sysconfig-Editors

(z. B. `<KEYTABLE="">`) und Parameter, die Leerzeichen enthalten, in Anführungsstriche einschließen. Bei Variablen, die nur aus einem Wort bestehen, sind die Anführungszeichen nicht notwendig.

Hinweis

Plattformspezifische Variablen in `/etc/sysconfig`

Die hier vorgestellten Variablen und Dateien in `/etc/sysconfig` sind als der kleinste gemeinsame Nenner aller unterstützten Plattformen konzipiert. Unter Umständen finden Sie hier Variablen, die es auf Ihrer Plattform nicht gibt. Andere Variablen, die nur auf bestimmten Plattformen vorkommen, fehlen möglicherweise. Hier verweisen wir auf die Dokumentation innerhalb der `/etc/sysconfig` Dateien.

Hinweis

Einstellungen in den Dateien in `/etc/sysconfig`

3ddiag Für 3Ddiag.

SCRIPT_3D="switch2mesasoft"

Skript festlegen, das die notwendigen symbolischen Links für die richtigen OpenGL-Bibliotheken und -Erweiterungen anlegt. Mögliche Werte für die in `/usr/X11R6/bin` befindlichen Skripte sind:

no – Kein Skript ausführen
 switch2mesasoft – Emulation der Mesa-Software (funktioniert mit allen Grafikkarten)
 switch2mesa3dfx – Mesa/Glide
 switch2nvidia_glx – XFree86 4.x/NVIDIA_GLX (NVIDIA_GLX/NVIDIA_kernel)
 switch2xf86_glx – XFree86 4.x/DRI
 Mit 3Ddiag lässt sich die richtige Einstellung herausfinden .

SuSEfirewall12 Firewall-Aktivierung; vgl. die Beschreibung in Paket SuSEfirewall12.

amavis Aktivierung des AMaViS Virenschanners in Sendmail oder Postfix.

USE_AMAVIS="yes"

Hier aktivieren Sie AMaViS. SuSEconfig wird eine passende Sendmail oder Postfix Konfiguration erstellen. Mehr Details lesen Sie im README . SuSE des AMaViS Pakets.

apache Konfiguration des Apache Webservers. Diese Aufstellung umfasst lediglich solche Einstellungen, die standardmässig gesetzt oder für das Verständnis des Apache unerlässlich sind. Für alle anderen Variablen bzw. Module und deren Funktionssweisen verweisen wir auf die Apache Dokumentation, die Sie mit YaST2 als Paket apache-doc installieren können oder im WWW unter den folgenden URLs finden:

<http://httpd.apache.org/docs/> und <http://modules.apache.org>

HTTPD_PERFORMANCE="slim"

Hier legen Sie fest, wieviele Clients von Ihrem Server bedient werden können. Sie haben die Auswahl aus den Klassen „slim“, „mid“, „thick“ und „enterprise“. SuSEconfig stimmt die MinSpareServers, MaxSpareServers, StartServers und MaxClients in der Apache-Konfiguration entsprechend /sbin/conf.d/SuSEconfig.apache.

HTTPD_START_TIMEOUT="2"

Hier setzen Sie den Zeitrahmen (in Sekunden), innerhalb dessen das Startskript feststellt, ob der http Prozess fehlerfrei gestartet werden konnte. Für den Fall, dass Sie mod_ssl verwenden und Ihr SSL-Zertifikat passwortgeschützt ist, erhöhen Sie diesen Wert.

HTTPD_SEC_ACCESS_SERVERINFO="no"

Diese Einstellung aktiviert die Module mod_status und mod_info, die jeweils über den Status, die Performance und die Konfiguration Ihres Servers Auskunft geben.

HTTPD_SEC_SAY_FULLNAME="no"

Welche Informationen sollen über den Server nach aussen in Form einer Fußzeile bei servergenerierten Dokumenten (z. B. Fehlermeldungen) weitergegeben werden? Sie haben die Wahl zwischen *yes* für Versionsnummer und Servernamen, *no* für keine Information und *email* für Versionsnummer, Name und *mailto*:-Anweisung an den Administrator des Servers. Diese Variable korreliert mit der *ServerSignature* Direktive des Apache.

HTTPD_SEC_SERVERADMIN=""

Bitte tragen Sie an dieser Stelle die E-Mailadresse des Serveradministrators ein. Haben Sie *<HTTPD_SEC_SAY_FULLNAME>* auf *yes* gesetzt, wird diese Angabe nach aussen weitergeleitet. Bleibt dieser Eintrag leer, wird als Mailadresse standardmässig *webmaster@\$HOSTNAME* verwendet. *<HOSTNAME>* (der vollständige Hostname des Servers) wird in der Datei */etc/HOSTNAME* festgelegt. *<HTTPD_SEC_SERVERADMIN>* entspricht der *ServerAdmin* Direktive des Apachen. *ServerAdmin* Direktiven in den *VirtualHost* Statements werden durch Ihren Eintrag an dieser Stelle nicht verändert – ebenso wenig wie der Eintrag des *SSL Virtual Hosts*.

HTTPD_SEC_PUBLIC_HTML="yes"

Sollen *public_html* Verzeichnisse im Homeverzeichnis der Benutzer zugänglich gemacht werden? Beantworten Sie diese Frage mit *yes*, so können Sie die weiteren Einstellungen in */etc/httpd/suse_public_html.conf* vornehmen.

HTTPD_CONF_INCLUDE_FILES=""

Durch Leerzeichen voneinander getrennt, geben Sie hier Dateien an, die von */etc/httpd/httpd.conf* übernommen werden sollen. Auf diese Weise können Sie z. B. *VirtualHost* Statements neu anlegen, ohne extra */etc/httpd/httpd.conf* ändern zu müssen. Solange *SuSEconfig* über den MD5-Summen Mechanismus keine Änderung von */etc/httpd/httpd.conf* feststellt, wird diese Datei bei der Apache Konfiguration nicht angerührt werden müssen.

HTTPD_AWSTATS_COMBINED_LOG="yes"

Soll Apache ein extra Logfile anlegen, das von *awstats* (engl. *Advanced Web Statistics*) ausgewertet wird?

HTTPD_DDT="yes"

Das *DDT Admin CGI* wird aktiviert. Sie können es verwenden, um auf einem lokalen *DDT* (engl. *Dynamic DNS Tools*) *Server Accounts* anzulegen und zu verwalten.

MAILMAN_APACHE="yes"

Soll das *Mailman* Webfrontend zur Verwaltung von Mailinglisten akti-

viert werden?

HTTPD_SEC_MOD_MIDGARD="yes"

Aktivieren des midgard Moduls. Midgard ist ein Open Source Content Management System.

HTTPD_SEC_MOD_PERL="yes"

Aktivieren des mod_perl Moduls

HTTPD_SEC_MOD_PHP="yes"

Aktivieren des mod_php Moduls

HTTPD_SEC_MOD_PYTHON="yes"

Wollen Sie das Python-Modul des Apache aktivieren? yes ist hier die Voreinstellung.

HTTPD_SEC_NAGIOS="yes"

Erlauben Sie den Zugang zum Nagios Webinterface. Sie konfigurieren es unter `/etc/httpd/nagios.conf`.

HTTPD_SEC_MOD_SSL="no"

Hier aktivieren Sie das SSL Modul. Die Voreinstellung ist no, da Sie einige Vorarbeiten leisten müssen, bevor SSL fehlerfrei verwendbar ist.

Erstellen Sie ein Serverzertifikat. Ein Testzertifikat legen Sie an, indem Sie folgende Befehle in dieser Reihenfolge als root ausführen:

```
cd /usr/share/doc/packages/mod_ssl
./certificate.sh
```

Setzen Sie `<ServerName>` im VirtualHost `_default_:443` der `httpd.conf` auf den vollständigen Servernamen (engl. *Fully Qualified Domain Name*) (siehe `<HOSTNAME>` `/etc/HOSTNAME`).

Erhöhen Sie `<HTTPD_START_TIMEOUT>`, wenn Ihr Serverzertifikat passwortgeschützt ist (siehe oben).

ZOPE_PCGI="no"

Sollen Anfragen von Zope über das PCGI-Interface von Apache abgewickelt werden? Belassen Sie diese Variable auf der Voreinstellung no, startet Zope als Standalone Webserver. Setzen Sie hier yes, müssen Sie Apache installiert haben, um PCGI verwenden zu können. Mehr Optionen liegen in `/etc/sysconfig/zope`.

ZOPE_KEEP_HOMES="yes"

Sollten Zope-Anfragen über apache-pcgi abgewickelt werden und `<ZOPE_KEEP_HOMES>` auf yes gesetzt sein, werden die Homeverzeichnisse der Benutzer von Apache gehandhabt.

argoups Die Konfiguration für argoups. Dieses Paket bietet die Möglichkeit, das System über einen speziellen Daemon kontrolliert herunterfahren zu

können, falls die USV (Unterbrechungsfreie Stromversorgung) einen Stromausfall meldet.

ARGO_TYPE="local"

Geben Sie hier den Verbindungstyp zum zu überwachenden System ein. Wenn Sie ein System „fernüberwachen“ möchten, tragen Sie dessen Namen bei `<ARGO_REMOTESERVER>` ein.

ARGO_REMOTESERVER=""

ARGO_TTY="/dev/ttyS0"

Über welchen seriellen Port besteht die Verbindung zu ArgoUPS?

ARGO_USERTIME="2"

Wie lang (in Minuten) nach dem Stromausfall soll das Skript aus `<ARGO_USERFILE>` ausgeführt werden?

ARGO_USERFILE="/usr/sbin/argoblackout"

ARGO_SHUTDOWN="8"

Wann soll danach der Shutdown eingeleitet werden?

argus Server für Argus (Netzwerkmonitor).

ARGUS_INTERFACE="eth0"

Das von Argus zu überwachende Interface.

ARGUS_LOGFILE="/var/log/argus.log"

Die Argus-Logdatei. Diese Datei kann sehr groß werden!

autofs Mit diesem Daemon ist es möglich, sowohl über NFS erreichbare Verzeichnisse als auch lokale Verzeichnisse (CD-ROM-Laufwerke, Disketten etc.) automatisch zu mounten.

AUTOFS_OPTIONS=""

Optionen für autofs, z. B. `--timeout 60`. Die `-timeout` Option legt fest, nach welchem Zeitraum (in Sekunden) Verzeichnisse automatisch wieder ausgehängt werden sollen (engl. *unmount*).

autoinstall AutoYaST2 der Auto-Installer von YaST2.

REPOSITORY="/var/lib/autoinstall/repository"

Ablage für alle „Profiles“. Dies sind die Kontrolldateien, die die Konfigurationsbeschreibungen für die zu installierenden Hosts beinhalten.

CLASS_DIR="/var/lib/autoinstall/classes"

Sie können bei der Erstellung von Profilen/Kontrolldateien für komplexe Installationsszenarien mit vielen Hosts zur Vereinfachung Klassen definieren, die verschiedene Hosttypen und -gruppen abbilden. YaST2 legt diese unter `/var/lib/autoinstall/classes` ab.

PACKAGE_REPOSITORY=""

Dieses Verzeichnis enthält die Installationsdaten/Pakete für SuSE Linux Desktop.

backup Kopien der RPM-Datenbank.

RPMDB_BACKUP_DIR="/var/adm/backup/rpmdb"

Legt fest, wohin cron.daily Backups der RPM-Datenbank schreiben soll; wenn keine Backups gewünscht werden, diese Variable auf "" setzen.

MAX_RPMDB_BACKUPS="5"

Legt die Anzahl der Backups der RPM-Datenbank fest.

RCCONFIG_BACKUP_DIR="/var/adm/backup/rpmdb"

In das hier angegebene Verzeichnis legt cron.daily die Backups von Ihrer /etc/rc.config und den Dateien unter etc/sysconfig/ ab. Wann immer diese Dateien geändert werden, wird der nächste cron.daily-Lauf Backups erzeugen. Wünschen Sie keine Backups, setzen Sie diese Variable auf "" .

MAX_RCCONFIG_BACKUPS="5"

Hier legen Sie fest, wieviele Backups von den Dateien unter /etc/sysconfig und von /etc/rc.config vorgehalten werden.

clock Zeiteinstellungen.

GMT=""

Wenn Ihre Hardware-Uhr auf GMT (*Greenwich Mean Time*) eingestellt ist, setzen Sie diese Variable auf -u, anderenfalls setzen Sie die Variable auf --localtime. Diese Einstellung ist relevant für das automatische Umstellen von Sommer- auf Winterzeit und umgekehrt.

TIMEZONE=""

Die Zeitzone, in der Sie wohnen bzw. den Rechner betreiben. Diese Einstellung ist auch wichtig für die automatische Umstellung von Sommer- auf Winterzeit und umgekehrt. Damit wird /usr/lib/zoneinfo/localtime gesetzt.

console Einstellungen für die Konsole.

FB_MODULES=""

Wollen Sie Framebuffer-Treibermodule zu Ihrem Kernel hinzuladen? Vor einer Entscheidung für das Laden der Module sollten Sie bedenken, dass Ihre Einstellungen nicht funktionieren, wenn vesafb bereits aktiv ist. Weiterhin ist es vorteilhaft, Framebufferunterstützung direkt in den Kernel hineinkompiliert zu haben. Schließlich haben manche XFree86-Treiber (insbesondere der XFree86-4.x Serie) im Framebuffer Textmodus Probleme.

FBSET_PARAMS=""

Bietet Ihr Kernel Framebufferunterstützung (oder wird diese als Modul geladen), werden Sie die Auflösung oder andere Parameter ändern wollen. Geben Sie fbset die entsprechenden Parameter mit (Details: man fbset und/oder fbset -h).

Achtung

Einstellen der Framebuffer Parameter

Die möglichen Einstellungen sind stark von Ihrer speziellen Hard- und Software abhängig. Falsche Entscheidungen können unter Umständen Ihren Monitor beschädigen. Bitte beachten Sie daher Folgendes:

vesafb bietet (noch) keine Unterstützung für den Wechsel des Displaymodus.

Wählen Sie keine Displaymodi, die von Ihrem Monitor nicht unterstützt werden.

Achtung

CONSOLE_FONT=""

Der Font, der für die Konsole beim Booten geladen wird. Nicht alle Fonts unterstützen z. B. die deutschen Umlaute oder andere 8-Bit-Zeichen! Zusatzeinstellungen sind: `<CONSOLE_SCREENMAP>`, `<CONSOLE_UNICODEMAP>` und `<CONSOLE_MAGIC>`.

CONSOLE_UNICODEMAP=""

Manche Fonts haben keine eigene Unicode Map. Geben Sie hier explizit das von Ihnen gewünschte Unicode Mapping an. Sie finden diese Dateien unter `/usr/share/kbd/unimaps/`. Im Normalfall wird diese Option allerdings nicht benötigt.

CONSOLE_SCREENMAP=""

Muss der von Ihnen verwendete Font in Unicode-Zeichensatz umgesetzt werden? Geben Sie hier die passende Screenmap an. Screenmaps finden Sie unter `/usr/share/kbd/consoletrans/`.

CONSOLE_MAGIC=""

Die Konsole muss je nach verwendetem Font unter Umständen mit `<CONSOLE_MAGIC>` initialisiert werden. Im Normalfall müssen Sie hier keine Änderungen vornehmen.

SVGATEXTMODE="80x25"

Das zugehörige Paket `svgatext` erlaubt die Einstellung höherer Textauflösungen (bis zu 160x60) mit VGA-Karten. Diese Variable enthält einen gültigen Wert aus `/etc/TextConfig`. Bitte passen Sie diese Datei den

Gegebenheiten Ihrer Grafikkarte entsprechend an. Wie dies zu erreichen ist, erfahren Sie unter `/usr/share/doc/packages/svgatext`. Standardeinstellung für `(SVGATEXTMODE)` ist „80x25“. SVGATextMode Auflösungen werden in den Runlevels 1,2,3 und 5 verwendet.

cron Tägliche Wartungsarbeiten am System.

Der Cron-Daemon startet zu vorgegebenen Zeiten automatisch gewisse Programme. Seine Aktivierung ist auf Rechnern, die rund um die Uhr laufen, dringend zu empfehlen. Eine Alternative bzw. Ergänzung ist der AT-Daemon.

Hinweis

Es gibt eine Reihe von Systemeinstellungen, die es erfordern, dass regelmäßig bestimmte Programme gestartet werden. Daher sollte auf jedem System der Cron-Daemon aktiviert werden.

Hinweis

MAX_DAYS_IN_TMP="0"

Es wird täglich geprüft, ob es in den tmp-Verzeichnissen (vgl. `(TMP_DIRS_TO_CLEAR)`) Dateien gibt, auf die länger als angegeben nicht zugegriffen wurde (in Tagen). Wurde auf eine Datei in einem dieser Verzeichnisse länger als angegeben nicht mehr zugegriffen, wird sie gelöscht.

Dieser Mechanismus kann mit "" oder 0 (Vorgabe) abgeschaltet werden. Diese Variable sollte gesetzt werden, wenn mehrere Benutzer das System verwenden, um ein Überlaufen der tmp-Verzeichnisse zu verhindern.

TMP_DIRS_TO_CLEAR="/tmp /var/tmp"

Angabe derjenigen Verzeichnisse, die täglich nach „alten“ Dateien durchsucht werden sollen; vgl. `(MAX_DAYS_IN_TMP)`.

OWNER_TO_KEEP_IN_TMP="root"

Die Dateien der hier angegebenen Systembenutzer sollen auch dann nicht aus den tmp-Verzeichnissen gelöscht werden (vgl. `(TMP_DIRS_TO_CLEAR)`), wenn auf sie länger als angegeben nicht mehr zugegriffen wurde.

Achtung: Wenn `(CLEAR_TMP_DIRS_AT_BOOTUP)` auf *yes* steht, wird dieser Eintrag hier *nicht* beachtet!

CLEAR_TMP_DIRS_AT_BOOTUP="no"

Setzen Sie diese Variable auf *yes*, wenn alle Dateien und Unterverzeichnisse in den temporären Verzeichnissen, die in `(TMP_DIRS_TO_CLEAR)`

genannt sind, gelöscht werden sollen (`rm -fr`).

Achtung: Wenn diese Variable auf `yes` gesetzt wird, werden die Einträge in `<OWNER_TO_KEEP_IN_TMP>` *nicht* beachtet; alle Dateien werden ausnahmslos gelöscht!

DELETE_OLD_CORE="no"

Corefiles sind Abbilder der Speicherbelegung von Programmen, die wegen einer Speicherschutzverletzung abgebrochen wurden; diese Abbilder dienen der Fehlersuche. Hier können Sie einstellen, dass regelmäßig nach etwaigen alten Corefiles gesucht wird und diese automatisch gelöscht werden. Gleichzeitig muss das Paket `findutils-locate` installiert und `<RUN_UPDATEDB>` auf `yes` gesetzt sein.

MAX_DAYS_FOR_CORE="7"

Legt fest, wie alt Corefiles maximal werden dürfen (in Tagen), bevor sie automatisch gelöscht werden.

REINIT_MANDB="yes"

Wenn die Manpage-Datenbanken (`mandb` und `whatis`) von `cron.daily` täglich neu angelegt werden sollen.

DELETE_OLD_CATMAN="yes"

Sollen veraltete vorformatierte Manual-Pages in `/var/catman` gelöscht werden?

CATMAN_ETIME="7"

Wie lang (in Tagen) sollen vorformatierte Manual-Pages aufgehoben werden, bevor sie gelöscht werden?

dhcpcd Konfiguration des DHCP-Servers

DHCPD_INTERFACE="eth0"

Interface/s, auf dem/denen der DHCP-Server lauschen soll.

DHCPD_RUN_CHROOTED="yes"

Soll `dhcpcd` in einem „chroot jail“ betrieben werden? Lesen Sie hierzu bitte das `README.SuSE` zu `dhcpcd` unter `/usr/share/doc/packages/dhcpcd/README.SuSE`.

DHCPD_CONF_INCLUDE_FILES=""

Die Datei `dhcpcd.conf` kann `include`-Statements enthalten. Geben Sie unter `<DHCPD_CONF_INCLUDE_FILES>` alle Dateien an, die Sie inkludieren wollen. Auf diese Weise werden *alle* Ihre `.conf` Dateien ebenso wie `/etc/dhcpcd.conf` in das Chroot-Verzeichnis (`\$chroot/etc/`) kopiert.

DHCPD_RUN_AS="nobody"

Legen Sie fest, als welcher Benutzer `dhcpcd` gestartet wird. Bleibt diese Variable leer oder geben Sie `root` an, wird `dhcpcd` als `root` gestartet. Mit `nobody` startet er als `nobody` der Gruppe `nogroup`.

DHCPD_OTHER_ARGS=""

Hier geben Sie dhcpd weitere Argumente mit (siehe man dhcpd).

dhcrelay Konfiguration des DHCP-Relay-Agents. Er dient als „Vermittler“ zwischen Subnetzen mit und ohne eigenem DHCP-Server. DHCP- (und Bootp-) Anfragen aus einem Subnetz ohne eigenen Server leitet er an einen oder mehrere DHCP-Server im Netz weiter und übermittelt deren Antworten.

DHCRELAY_INTERFACES=""

Interfaces, auf denen der DHCP-Relay-Agent lauschen soll. Bitte trennen Sie die Einträge durch Leerzeichen.

DHCRELAY_SERVERS=""

An welche DHCP-Server kann sich der DHCP-Relay-Agent wenden? Tragen Sie hier einen oder mehrere Server durch Leerzeichen getrennt ein.

displaymanager Displaymanager konfigurieren.

DISPLAYMANAGER=""

Diese Variable legt fest, welcher Displaymanager zum Anmelden („Login“) verwendet werden soll. Mögliche Werte sind `console`, `xdm` (traditioneller Displaymanager des X Window System), `kdm` (Displaymanager von KDE), `gdm` (Displaymanager von GNOME) oder `wdm` (der „WINGs Display Manager“).

DISPLAYMANAGER_REMOTE_ACCESS="no"

Wollen Sie einen Remotezugriff auf Ihren Displaymanager erlauben? Die Standardeinstellung ist `no`.

DISPLAYMANAGER_STARTS_XSERVER="yes"

Soll der Displaymanager einen lokalen X-Server starten? Erlauben Sie ausschliesslich Remotezugriff, ist diese Variable auf `no` zu setzen.

KDM_SHUTDOWN="auto"

Hier legen Sie fest, von wem das System in kdm heruntergefahren werden darf. Mögliche Werte sind `root`, `all`, `none`, `local` und `auto`.

KDM_USERS=""

Tragen Sie, durch Leerzeichen getrennt, die Liste der Benutzer ein, für die in kdm Icons angezeigt werden sollen. Nehmen Sie hier keine eigenen Einträge vor, werden die Standardeinstellungen des Systems verwendet.

KDM_BACKGROUND=""

Hier lässt sich ein Hintergrund für kdm angeben.

KDM_GREETSTRING=""

Wünschen Sie eine besondere Begrüßung durch kdm?

dracd Einstellungen für den dracd Daemon und das Mail-Relaying durch „POP-before SMTP.“

DRACD_RELAYTIME="5"

Postfix hält auf dem POP-Server für eine bestimmte Zeitspanne die IP-Adresse eines authentifizierten Hosts vor und erlaubt das Versenden von Mails von eben diesem Host. Nach dieser Zeit wird der Eintrag gelöscht und eine neue Authentifizierung erforderlich. Die Angabe erfolgt in Minuten.

DRACD_DRACDB="/etc/postfix/dracd.db"

Hier ist die dracdb zu finden.

dvb DVB-Karte

DVB_SOUND_CHIP="ti"

Soundchip auf der DVB-Karte festlegen; ti oder crystal.

hardware Hardware-Einstellungen.

DEVICES_FORCE_IDE_DMA_ON=""

DMA bei den genannten Geräten einschalten.

DEVICES_FORCE_IDE_DMA_OFF=""

DMA bei den genannten Geräten abschalten.

hotplug Einstellungen zu Hotplug.

HOTPLUG_DEBUG="default"

Mit dieser Variable kontrollieren Sie die Menge an (Fehler-)Meldungen, die der hotplug Service an syslog meldet. default, " " , oder no bewirken eine moderate Menge an Meldungen, off lässt hotplug „verstummen“ und verbose oder yes geben einige zusätzliche Debugmeldungen weiter. max führt dazu, dass syslog mit Meldungen „überschwemmt“ wird.

HOTPLUG_START_USB="yes"

Hier starten oder stoppen Sie USB Hotplug.

Hinweis

USB Hotplug deaktivieren

Sollten Sie USB Hotplug deaktivieren und die USB-Eingabegeräte als Modul geladen haben, wird Ihre Tastatur nicht mehr reagieren, da Sie die Tastaturunterstützung auf diese Weise mit deaktivieren.

Hinweis

HOTPLUG_USB_HOSTCONTROLLER_LIST="usb-uhci uhci usb-ohci ehci-hcd"

Hier legen Sie die „Probing“-Reihenfolge der Hostcontroller-Treiber fest.

HOTPLUG_USB_MODULES_TO_UNLOAD="scanner"

Diese Module werden bei einem USB „remove“ entfernt. Für manche Hardware ist eine Reinitialisierung durchaus sinnvoll.

HOTPLUG_USB_NET_MODULES="pegasus usbnet catc kaweth CDCether"

Wird eines dieser Module in/aus dem Speicher geladen, nimmt das System an, dass es sich hierbei um ein Netzwerkgerät handelt und erstellt eine Hardwarebeschreibung für das folgende „net event“.

HOTPLUG_START_NET="yes"

Aktivieren/Deaktivieren Sie NET Hotplug Event Handling.

HOTPLUG_NET_DEFAULT_HARDWARE=""

Bis hotplug selbständig erkennt, welcher Typ Hardware sich hinter einem Netzwerkinterface verbirgt, werden bei USB oder PCI Hotplug Events Hardwarebeschreibungen erstellt, die zum NET Event ausgelesen werden. Gleichzeitiges Hinzufügen mehrerer Hotplug Geräte kann Race Conditions auslösen. Sollte die automatische Erkennung neuer Geräte nicht funktionieren, wird beim Aufruf von `if{up,down}` der Inhalt von `<HOTPLUG_NET_DEFAULT_HARDWARE>` ausgewertet. Tragen Sie hier ein, was Sie als NIC (engl. *Network Interface Card*) verwenden: `pcmcia`, `usb` oder `firewire`.

HOTPLUG_NET_TIMEOUT="8"

Geben Sie hier einen Wert an, wie lange (in Sekunden) auf eine Hardwarebeschreibung von einem USB oder PCI Hotplug Event gewartet werden soll. Nimmt diese Variable den Wert 0 an, wird automatisch `<HOTPLUG_NET_DEFAULT_HARDWARE>` ausgewertet. Die Voreinstellung von acht Sekunden berücksichtigt den Zeitbedarf mancher PCMCIA Netzwerkkarten.

HOTPLUG_START_PCI="yes"

Aktivieren/Deaktivieren des PCI Hotplug Event Handlings.

HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD=""

Die folgenden Module sollen beim „PCI remove Event“ nicht aus dem Speicher geladen werden.

intermezzo Einstellungen zum Intermezzo-Filesystem.

EXCLUDE_GID="63"

Geben Sie hier an, welche Gruppe von der Replikation ausgenommen werden soll.

irda IrDA ist die Infrarot-Schnittstelle, die bei Notebooks häufig anzustellen ist.

IRDA_PORT="/dev/ttyS1"

Momentan wird nur der serielle Modus (UART [SIR]) in der Standard-Konfiguration unterstützt. Im BIOS-Setup ist der verwendete serielle Port nachzusehen. Sollten Sie einen unterstützten FIR Chipsatz haben, legen Sie das entsprechende Kernelmodul (z. B. `toshoboe`) fest. FIR muss zuerst in den BIOS-Einstellungen aktiviert werden. In einzelnen Fällen, kann es nötig sein, den seriellen Port via `setserial /dev/ttyS<x> uart none` zu deaktivieren.

isdn/ Alle wichtigen Skripte zu ISDN.

ispell Überprüfung der Rechtschreibung.

ENGLISH_DICTIONARY="system american british"

SuSEconfig.ispell verwaltet einen symbolischen Link vom „englischen“ Wörterbuch auf eines der beiden von `american` oder `british`. Ist sowohl `ispell-american` als auch `ispell-british` installiert, greift `<ENGLISH_DICTIONARY>`. Der Wert `system` verweist auf die Standardsprache des Systems (festgelegt in `/etc/sysconfig/language` unter `<RC_LANG>`), so diese eine der beiden englischen Sprachen ist. Andernfalls hat `system` keinen Effekt. Ein symbolischer Link wird auf das erste installierte Wörterbuch dieser Liste gesetzt.

java Einstellungen zur Java-Konfiguration

CREATE_JAVALINK="yes"

SuSEconfig kann für Sie die `/usr/lib/java` und `/usr/lib/jre` Links zum passenden JDK (engl. *Java Development Kit*) und JRE (engl. *Java Runtime Environment*) anlegen, wenn Sie den Wert dieser Variable auf `yes` setzen. Ziehen Sie die manuelle Konfiguration vor, setzen Sie `<CREATE_JAVALINK>` auf `no`.

JAVA_JRE_THREADS_TYPE="green"

Konfiguration des `java-jre` Pakets. Wenn Sie *echtes* Multithreading wünschen, setzen Sie diese Variable auf `native`. Dies macht z. B. in Kombination mit SMP Systemen Sinn.

joystick Einstellungen zur Joystick-Konfiguration.

GAMEPORT_MODULE_0=""

Name des Gameport-Moduls, z. B. `ns558` für einen betagten Gameport.

JOYSTICK_MODULE_0=""

Normalerweise `analog`.

JOYSTICK_MODULE_OPTION_0=""

Zum Beispiel "js=gameport" für analog.

JOYSTICK_CONTROL_0=""

Zum Beispiel yes.

JOYSTICK_CONTROL_PORT_0=""

Soundkarten wie ens1371 benötigen hier eine Port-Adresse; üblicherweise 0x200.

kernel Kernel.

INITRD_MODULES=""

Die Namen der Module, die per `mk_initrd` zur Initial Ramdisk hinzugefügt werden müssen. (z. B. Treiber für SCSI-Controller, LVM oder ReiserFS).

SHMFS=""

Hier übergeben Sie den Größenparameter für das Mounten des shmfs Filesystems. Standardmäßig verwendet der Kernel hier 50% des verfügbaren Speichers. Dies kann, abhängig vom individuellen Setup, manchmal nicht ausreichend sein.

keyboard Einstellungen für die Tastatur.

KEYTABLE="de-latin1-nodeadkeys"

Definiert die Tastaturbelegung. Bei Verwendung einer US-Tastatur kann diese Variable leer bleiben.

KBD_RATE="24.0"

Bestimmt die Geschwindigkeit der automatischen Tastaturwiederholung. Mögliche Eingaben sind von zweimal bis zu 30 mal pro Sekunde. Damit diese Einstellung wirkt, muss gleichfalls die Dauer der Verzögerung (vgl. `<KBD_DELAY>`) festgelegt werden!

KBD_DELAY="500"

Mögliche Werte: 250, 500, 750 und 1000. Hier können Sie die Verzögerung einstellen, nach der die automatische Wiederholungsfunktion einsetzt. Der Wert ist in Millisekunden, das Raster ist jedoch nicht sehr genau. Sie müssen auch `<KBD_RATE>` einstellen!

KBD_NUMLOCK="bios"

Bei `no` wird `(NumLock)` beim Booten nicht eingeschaltet. Weitere mögliche Einstellungen sind `yes`, `" "` oder `bios` für BIOS-Einstellung.

KBD_SCRLOCK="no"

`(ScrollLock)` einschalten?

KBD_CAPSLOCK="no"

`(CapsLock)` beim Booten nicht einschalten.

KBD_DISABLE_CAPS_LOCK="no"

Soll **(CapsLock)** abgeschaltet werden und sich wie eine normale **(Shift)** Taste verhalten?

KBD_TTY="tty1 tty2 tty3 tty4 tty5 tty6"

(NumLock), **(CapsLock)** und **(ScrollLock)** kann auf bestimmte TTYs beschränkt werden; "" steht für alle TTYs.

COMPOSETABLE="clear winkeys shiftctrl latin1.add"

Hier legen Sie die zu ladende „Compose Table“ fest. Mittels „Compose-table“ ist es Ihnen möglich, Sonderzeichen (Akzente, Währungssymbole etc.), die nicht direkt auf die Tastatur gelegt sind, dennoch über spezielle Tastenkombinationen einzugeben. Eine detaillierte Erklärung finden Sie unter `/usr/share/doc/packages/kbd/README.SuSE`.

language Einstellungen zu Sprache und Standort (Lokale).

RC_LANG="de_DE@euro"

Setzt `LANG` für `locale`; hiermit kann für die lokalen Benutzer eine Vorgabe eingestellt werden. Dieser Wert kommt solange zum Tragen, wie keine speziellen `(RC_LC_*)`-Variablen benutzt werden.

Die einschlägigen `sysconfig`-Variablen lauten: `(RC_LC_ALL)` (hiermit kann man die `LC_*` wie auch `LANG` überschreiben!), `(RC_LC_MESSAGES)`, `(RC_LC_CTYPE)`, `(RC_LC_MONETARY)`, `(RC_LC_NUMERIC)`, `(RC_LC_TIME)` und `(RC_LC_COLLATE)`.
Vgl. Abschnitt *Lokale Anpassungen – I18N/L10N* auf Seite 152.

ROOT_USES_LANG="ctype"

Sollen auch für `root` die `locale`-Einstellungen verwendet werden? `ctype` bedeutet, dass hier der Wert von `(LC_CTYPE)` verwendet wird.

locate Die `locate`-Datenbank dient dem schnellen Auffinden von Dateien im System. – Diese Aktualisierung wird möglicherweise kurz nach dem Booten durchgeführt, wenn Sie den Rechner *nicht* ununterbrochen laufen haben; vgl. Abschnitt *Paket cron* auf Seite 146.

RUN_UPDATEDB="no"

Einmal täglich soll die Datenbank für `locate` (`locate`) aktualisiert werden. Eine Detailkonfiguration des Programms `updatedb` kann über die folgenden Variablen erreicht werden (vgl. die Kommentare dort).

RUN_UPDATEDB_AS="nobody"

Der Benutzer, unter dessen Identität `updatedb` ausgeführt werden soll. Die Standardeinstellung ist hier aus Sicherheitsgründen `nobody`.

UPDATEDB_NETPATHS=""

`updatedb` durchsucht von sich aus nur lokale Verzeichnisse. Sie können aber selbst zu durchsuchende Netzwerkverzeichnisse festlegen.


```
UPDATEDB_PRUNEPATHS="/mnt /media/cdrom /tmp /usr/tmp
/var/tmp /var/spool /proc /media"
```

Alle Verzeichnisse, die hier eingetragen werden, ignoriert updatedb bei seiner Suche.

```
UPDATEDB_NETUSER=""
```

Siehe oben; hier legen Sie den Benutzer fest, unter dessen Identität Netzpfade durchsucht werden sollen. nobody ist ein Beispiel.

```
UPDATEDB_PRUNEFS=""
```

updatedb kann nicht nur bestimmte Verzeichnisse ignorieren; auch Dateisystemtypen können von der Suche ausgenommen werden.

lvm Der Logical Volume Manager.

mail Einstellungen bezüglich E-Mail.

```
FROM_HEADER=""
```

From:-Zeile systemweit vorgeben. Wenn "", wird der FQDN verwendet; vgl. *Domain Name System* auf Seite 209.

```
MAIL_CREATE_CONFIG="yes"
```

SuSEconfig wird eine `/etc/sendmail.cf` aus den Angaben zusammenstellen, die Sie unter `sendmail` machen. Bevorzugen Sie die manuelle Konfiguration, setzen Sie diese Variable auf `no`.

```
NULLCLIENT=""
```

Ein „Nullclient“ ist eine Maschine, die ausschließlich Mail versenden kann. Sie erhält keinerlei Mail aus dem Netz und kann auch lokal keine Mail zustellen. Typischerweise verwendet ein „Nullclient“ POP oder NFS für den Mailbox-Zugriff.

```
SMTPD_LISTEN_REMOTE="no"
```

`yes` wird gesetzt, sobald Mails von extern angenommen werden sollen. Für einen Mailserver ist diese Einstellung ein „Muss“.

mouse Maus-Einstellungen.

```
MOUSE=""
```

Die Schnittstelle, an der die Maus angeschlossen ist (z. B. `/dev/ttyS0`). Von YaST2 bzw. SuSEconfig wird ein Link von `/dev/mouse` auf das angegebene Device angelegt.

```
GPM_PROTOCOL=""
```

Das GPM-Protokoll für das unter `<MOUSE>` eingetragene Device. Diesen Wert legt YaST2 fest.

```
GPM_PARAM=" -t $GPM_PROTOCOL -m $MOUSE"
```

Die Startparameter für den `gpm`.

network Verzeichnis für Netzwerkkonfigurationen.

network/config Generelle Einstellungen zur Netzwerkkonfiguration.

DEFAULT_BROADCAST="+"

⟨DEFAULT_BROADCAST⟩ wird ausgewertet, wenn keine andere BROADCAST Angabe gesetzt wurde. Sie können zwischen " " für keine Broadcastadresse, - für die ⟨IPADDR⟩ ohne Host Bits und + für die volle Angabe der ⟨IPADDR⟩ mit allen Host Bits wählen.

CHECK_FOR_MASTER="yes"

Dieser Eintrag bewirkt, dass ein „Master“-Interface bereits aktiviert sein muss, bevor Alias-Adressen („labelled address“) aufgesetzt werden können. Technisch hat dieser Eintrag keinerlei Konsequenz, aber Benutzer von ifconfig profitieren davon.

CHECK_DUPLICATE_IP="yes"

yes bewirkt, dass das ifup-Skript prüft, ob eine IP-Adresse bereits benutzt wird. Bitte stellen Sie sicher, dass der Kernel Packet-Sockets unterstützt (⟨CONFIG_PACKET⟩), um die ARP Funktionalität, von der dieses Feature abhängt, zu gewährleisten. Diese Prüfung dauert eine Sekunde pro Interface, was sich bei einer großen Anzahl IP-Adressen bemerkbar machen kann.

DEBUG="no"

Generelles An-/ Ausschalten von Debug-Meldungen für alle Netzwerkskripte. Selbst bei no können Sie mit der Option -o debug die Debug-Meldungen einzelner Skripte wieder aktivieren.

USE_SYSLOG="yes"

Sollen Fehlermeldungen der Konfigurationsskripte nach syslog ausgegeben werden?

MODIFY_RESOLV_CONF_DYNAMICALY="yes"

Manche Dienste wie ppp, ipp, dhcp-client, pcmcia und hotplug wollen zu bestimmten Zeiten /etc/resolv.conf verändern. Der Standardwert ist yes.

MODIFY_NAMED_CONF_DYNAMICALY="no"

Siehe ⟨MODIFY_RESOLV_CONF_DYNAMICALY⟩. Sollten Sie sich hier unsicher sein, belassen Sie es bei der Standardeinstellung no.

network/dhcp Einstellungen zu DHCP (engl. *Dynamic Host Configuration Protocol*).

Hinweis

Um die Konfiguration eines oder mehrerer Interfaces über DHCP zu ermöglichen, muss `<BOOTPROTO>` in `/etc/sysconfig/network/ifcfg-<interface>` den Wert `dhcp` annehmen. Eventuell muss `<STARTMODE>` den Wert `onboot` zugewiesen bekommen.

Hinweis

Die meisten dieser Optionen werden nur von `dhcpcd` verwendet, der ISC `dhclient` verwendet eine eigene Konfigurationsdatei. Manche Optionen werden auch durch die Einstellungen in den `ifcfg-*`-Dateien beschrieben.

DHCLIENT_BIN=""

Welcher DHCP-Client soll verwendet werden? `dhcpcd` für den DHCP Client Daemon oder `dhclient` für den ISC `dhclient`? Ein leerer Eintrag bewirkt, dass zuerst versucht wird, `dhcpcd` zu starten. Bleibt dies ohne Erfolg, wird `dhclient` versucht.

DHCLIENT_DEBUG="no"

Soll DHCP Client im Debug-Modus gestartet werden? Für DHCP Client Daemon liegen die Logdateien unter `/var/log/messagesfordhcpcd`, für ISC `dhclient` unter `/var/log/dhclient-script`.

DHCLIENT_SET_HOSTNAME="no"

Soll der DHCP Client den Hostnamen setzen? Achten Sie bei der Einstellung `yes` darauf, dass Sie sich nicht gerade in einer laufenden X-Session befinden, wenn der Hostname neu gesetzt wird. Andernfalls kann ihre `<DISPLAY>`-Variable nicht korrekt ausgewertet werden und Sie können keine neuen Fenster mehr starten.

DHCLIENT_MODIFY_RESOLV_CONF="yes"

Darf der DHCP Client Ihre `/etc/resolv.conf` ändern? Die Standardeinstellung ist `yes`. Setzen Sie hier `no` oder enthält `<MODIFY_RESOLV_CONF_DYNAMICALY>` in `/etc/sysconfig/network/config` den Wert `no`, wird die Datei `/etc/resolv.conf` nicht angerührt.

DHCLIENT_SET_DEFAULT_ROUTE="yes"

Soll der DHCP Client den Default Gateway bestimmen? Sollten mehrere `dhcpcd` Prozesse laufen, sollte dies nur einer von ihnen tun dürfen.

DHCLIENT_MODIFY_NTP_CONF="no"

Soll der DHCP Client die NTP Konfiguration (`/etc/ntp.conf`) verändern können?

DHCLIENT_MODIFY_NIS_CONF="no"

Soll der DHCP Client die NIS Konfiguration (/etc/yp.conf) verändern können?

DHCLIENT_SET_DOMAINNAME="yes"

Soll der DHCP Client den NIS Domain Namen setzen? (Nur sinnvoll, wenn der Server die nis-domain Option anbietet.)

DHCLIENT_KEEP_SEARCHLIST="no"

Soll der DHCP Client, wenn er eine neue /etc/resolv.conf schreibt, die bereits existierende Domain-Suchliste beibehalten und zu derjenigen hinzufügen, die er vom DHCP Server erhält?

DHCLIENT_LEASE_TIME=""

Hier können Sie (in Sekunden) angeben, für welchen Zeitraum der DHCP Server dem Client eine dynamische IP überlässt („least“).

DHCLIENT_TIMEOUT="999999"

Sie können einen „Timeout“ setzen, nach dem der Client automatisch abbricht, wenn er keine Antwort vom Server bekommt. Diese Einstellung betrifft nur dhcpcd.

DHCLIENT_REBOOT_TIMEOUT=""

Diese Option legt fest, wie lang dhcpcd versucht einen früheren „Lease“ wiederzubekommen (im Init-Reboot-Zustand), bevor ein neuer „Lease“ verwendet wird.

DHCLIENT_HOSTNAME_OPTION="AUTO"

Sie können einen bestimmten Hostnamen festlegen, den dhcpcd für DHCP Messages verwendet. Die Voreinstellung AUTO bewirkt, dass automatisch der Hostname gesendet wird.

DHCLIENT_CLIENT_ID=""

Hier legen Sie eine Zeichenkette fest, die als Client-ID gesendet wird. Nehmen Sie hier keinen Eintrag vor, wird die Hardware-Adresse der Netzwerkkarte gesendet.

DHCLIENT_VENDOR_CLASS_ID=""

Legt den „Vendor Class Identifier“ fest.

DHCLIENT_RELEASE_BEFORE_QUIT="no"

Soll der Client den Server benachrichtigen, wenn er eine Adresse nicht mehr benötigt, so dass diese wieder zum allgemeinen Gebrauch freigegeben werden kann? Diese Option unterstützt nur dhcpcd.

DHCLIENT_SLEEP="0"

Manche Interfaces brauchen eine bestimmte Zeit, bis sie korrekt initialisiert werden. Sie können hier eine Latenzzeit in Sekunden angeben, während der der DHCP Client die Initialisierung abwartet. Allerdings sollten

solche Einstellungen separat für die einzelnen Interfaces vorgenommen werden.

network/ifcfg-eth0 Konfiguration der ersten Netzwerkkarte. Die folgenden Einstellungen lassen sich komfortabel mit YaST2 vornehmen.

STARTMODE=" "

Wann wird das Interface aktiviert? `onboot` besagt, dass das Interface zur Bootzeit gestartet wird, `manual`, dass `ifup` manuell gestartet werden muss und `hotplug` ermöglicht die Aktivierung per Hotplug oder PCMCIA.

BOOTPROTO=" "

Wählen Sie zwischen statische IP-Konfiguration oder dynamischer Adressvergabe mit DHCP (`dhcp`).

IPADDR=" "

Hier tragen Sie die IP-Adresse für die erste Netzwerkkarte ein.

NETMASK=" "

Hier tragen Sie die Netzmaske Ihres Netzes ein.

BROADCAST=" "

Geben Sie die Broadcastadresse für Ihr Netzwerk an.

PREFIXLEN=" "

Geben Sie die Länge des Prefix an.

NETWORK=" "

Die Adresse Ihres Netzwerks.

network/ifcfg-lo Die Konfiguration des Loopback-Device.

network/wireless Die Konfiguration für Wireless LAN. Bitte verwenden Sie YaST2 zur Konfiguration.

news Einstellungen für den Zugriff auf den NNTP-Server.

ORGANIZATION=" "

Der hier eingetragene Text erscheint in jedem News-Posting, das von dem betreffenden Rechner abgeschickt wird. Beispiel:

Duesentrieb, Entenhausen

NNTPSERVER="news"

Die Adresse des News-Servers; beziehen Sie Ihre News per UUCP und werden diese lokal gespeichert, sollten Sie hier `localhost` eintragen.

nfs NFS-Server. Gleichzeitig werden die Daemonen `rpc.nfsd` und `rpc.mountd` gestartet. Für eine weitergehende Beschreibung eines NFS-Servers (zum Beispiel die Festlegung der zu exportierenden Verzeichnisse) lesen Sie bitte Abschnitt *NFS – verteilte Dateisysteme* auf Seite 242.

REEXPORT_NFS="no"

Setzen Sie die Variable auf **yes**, um gemountete NFS-Verzeichnisse oder NetWare-Volumes zu re-exportieren.

onlineupdate Einstellungen für YaST2-Online-Update.

YAST2_LOADFTPSEVER="yes"

Beim Starten von YOU („YaST2-Online-Update“) die Liste der FTP-Server mit **wget** von <http://www.suse.de> aktualisieren. Diese Liste wird in `/etc/suseservers` eingetragen. Diese Variable ist auf **no** zu setzen, wenn die Liste nicht aktualisiert werden soll.

PROXY_USER=""

Benutzer des verwendeten Proxy.

PROXY_PASSWORD=""

Passwort für den verwendeten Proxy.

pcmcia PCMCIA-System/PC-Cards.

PCMCIA_SYSTEM="kernel"

Wählen Sie eines der beiden PCMCIA-Systeme aus: **external** oder **kernel**. Wenn nur eines der beiden Systeme installiert ist, wird der Inhalt dieser Variable ignoriert.

PCMCIA_PCIC=""

Dient der Festlegung des Socket-Treibers (Chipsets); gültige Werte sind **i82365** oder **tcic**, wenn das „externe“ PCMCIA-System verwendet wird (vgl. `(PCMCIA_SYSTEM)`) und **yenta_socket**, **i82365** oder **tcic** bei Verwendung des Systems **kernel**. Wenn die Variable leer ist (""), versucht das Skript selbstständig den richtigen Treiber herauszufinden; die Variable muss also nur gesetzt werden, wenn die automatische Erkennungen fehlschlägt.

PCMCIA_PCIC_OPTS=""

Festlegung der Sockettreiber-Timingparameter. Sie finden eine nähere Beschreibung unter `man i82365` oder `man tcic` und im PCMCIA-HOWTO (`/usr/share/doc/packages/pcmcia`) unter „PCIC_OPTS“.

PCMCIA_CORE_OPTS=""

Hier legen Sie die „pcmcia_core“ Optionen fest. Eine Beschreibung finden Sie unter `/usr/share/doc/packages/pcmcia` bei „CORE_OPTS“. Diese Optionen sind für beide PCMCIA-Typen gültig.

postfix Die Konfiguration der Postfix Variablen. Benutzen Sie hierfür bitte das `mail` Modul von YaST2.

postgresql PostgreSQL.

POSTGRES_DATADIR="/~postgres/data"

In welchem Verzeichnis soll die PostgreSQL Datenbank zu finden sein?

POSTGRES_OPTIONS=""

Die hier spezifizierten Optionen werden dem „PostgreSQL Master Daemon“ beim Start übergeben. Bitte informieren Sie sich über Details auf den Manpages für `postmaster` und `postgresql`. Bitte verwenden Sie die Option `-D datadir` an dieser Stelle nicht; das Startup-Skript setzt diesen Wert ausgehend von `(POSTGRES_DATADIR)`.

powermanagement apmd.

APMD_WARN_LEVEL="10"

Wollen Sie gewarnt werden, sobald die Batteriekapazität ein bestimmtes Niveau (Angabe in Prozent) unterschreitet? Die Standardeinstellung ist 10; mit 0 deaktivieren Sie diese und die drei folgenden Optionen. Mehr zu `apmd` unter `man 8 apmd` oder im zugehörigen Init-Skript `/etc/init.d/apmd`.

APMD_WARN_ALL="no"

Sollen die `apmd`-Warnungen an alle Terminals gesendet werden? Dann wählen Sie `yes`, andernfalls werden sie in der `Syslog`-Datei erfasst. Die Standardeinstellung ist `no`.

APMD_WARN_STEP="0"

Die Warnmeldungen werden wiederholt, sobald die maximale Batteriekapazität um eine bestimmte Größe (`(APMD_WARN_STEP)`) abnimmt. 0 deaktiviert diese Einstellung.

APMD_CHECK_TIME="0"

`apmd` überprüft standardmässig den Batteriestatus, wann immer es vom BIOS ein Event gemeldet bekommt. Soll diese Überprüfung öfter stattfinden, setzen Sie den Wert dieser Variable auf einen Wert größer als 0 Sekunden. Allerdings wird Ihre Festplatte dann bei jeder Überprüfung wieder angefahren. Die Standardeinstellung ist 0.

APMD_DEBUG="no"

`apmd` und das `apmd_proxy` Skript können „gesprächiger“ gemacht werden. Bei `yes` werden Sie darüber informiert, wann und wie `apmd_proxy` aufgerufen wird. Wenn Sie alles sehen wollen, was innerhalb von `apmd_proxy` auf `stdout` und `stderr` ausgegeben wird, wählen Sie `error`. Mit `all` entgeht Ihnen nichts. Standardeinstellung ist `no`.

APMD_ADJUST_DISK_PERF="no"

Um Energie zu sparen, sollte Ihre Festplatte nach einer bestimmten „Idle Time“ heruntergefahren werden. Wenn Sie allerdings Prozesse betreiben, die in regelmäßigen Abständen und häufig auf die Platte schreiben, wird

diese Option wenig ausrichten. Per Voreinstellung ist diese Option inaktiv.

APMD_BATTERY_DISK_TIMEOUT="12"

Setzen Sie den „Timeout“ fest, nach dem die Festplatte heruntergefahren werden soll. Allerdings bemisst sich der Wert dieser Variable nicht in Minuten oder Sekunden. Bitte lesen Sie für Details die Manpage von `hdparm`. Natürlich macht diese Einstellung nur Sinn, wenn Sie zuvor `<ADJUST_DISK_PERF>` auf `yes` gesetzt haben.

APMD_AC_DISK_TIMEOUT="0"

Soll die Festplatte auch heruntergefahren werden, wenn der Rechner am Stromnetz hängt? Wenn ja, wann (siehe oben)? Diese Option ist per Voreinstellung inaktiv.

APMD_BATTERY_LOW_SHUTDOWN="0"

Manche Laptop BIOSe senden nach Unterschreiten einer bestimmten Batteriekapazität eine „battery low“ Meldung. Ihr System kann automatisch eine bestimmte Zeit nach diesem Ereignis heruntergefahren werden. Geben Sie einen Wert in Minuten an. 1 ist das Minimum, 0 deaktiviert dieses Verhalten.

APMD_SET_CLOCK_ON_RESUME="no"

Sollten Ihre Zeiteinstellungen nach einem Standby oder Suspend aus dem Tritt geraten, setzen Sie diese Variable auf `yes`. Dann wird die Kernelzeit automatisch auf den Wert gesetzt, der in der GMT-Variable gesetzt wurde. Diese Option ist per Voreinstellung inaktiv.

APMD_SUSPEND_ON_AC="yes"

Ihr System wird auch dann heruntergefahren, wenn es an das Stromnetz angeschlossen ist. Mit `no` schalten Sie dieses Verhalten ab.

APMD_PCMCIA_SUSPEND_ON_SUSPEND="no"

Sollte Ihr PCMCIA keine APM-Unterstützung bieten, veranlassen Sie `apmd` dazu, Ihre Karten vor dem Suspend des Gesamtsystems in den Suspend-Modus zu bringen.

APMD_PCMCIA_EJECT_ON_SUSPEND="no"

Manche PCMCIA-Karten (insbesondere SCSI-Karten) reagieren nicht angemessen auf ein Suspend-Ereignis. Deshalb kann es notwendig werden, sie per `cardctl eject` zu deaktivieren.

APMD_INTERFACES_TO_STOP=" "

Sollte das Setup Ihrer integrierten Netzwerkkarte mit dem Suspend/Resume-Zyklus nicht richtig zurechtkommen, setzen Sie hier den Interface Namen. Das angegebene Interface wird jetzt bei einem Suspend korrekt heruntergefahren und wieder hochgefahren, sobald der Suspend-Modus aufgehoben wird.

APMD_INTERFACES_TO_UNLOAD=""

Sollte Ihr Netzwerk-Interface auch nach Auswertung von `<APMD_INTERFACES_TO_STOP>` nicht korrekt heruntergefahren werden können, tragen Sie hier das Treibermodul Ihres Netzwerk-Interfaces ein. Es wird dann beim Suspend aus dem Speicher geladen und bei einem Resume wieder eingelesen.

APMD_LEAVE_X_BEFORE_SUSPEND="no"

Abhängig von Ihrer Grafikkarte kann die Rückkehr in den Grafikmodus nach dem Suspend nicht korrekt funktionieren. Sie können vor dem Suspend auf die Textkonsole wechseln und nach dem Resume wieder auf die X-Console zurückkehren. Die Standardeinstellung ist 0.

APMD_LEAVE_X_BEFORE_STANDBY="no"

Siehe `<APMD_LEAVE_X_BEFORE_SUSPEND>`. Auch die Rückkehr nach einem Standby kann erschwert sein. Die Standardeinstellung ist 0.

APMD_LOCK_X_ON_SUSPEND="no"

Soll `opmd` Ihr Display „locken“? Wenn nur ein X-Server auf Ihrem System läuft und niemand über ein virtuelles Terminal Zugriff auf Ihr System hat, kann dieser Zustand als „sicher“ angesehen werden. Zusätzlich bietet eine verschlüsselte Datenpartition einen sehr guten Schutz, wenn Ihr Laptop gestohlen werden sollte. Die Standardeinstellung ist 0.

APMD_STOP_SOUND_BEFORE_SUSPEND="no"

Auch Soundmodule überleben unter Umständen einen Suspend/Resume-Zyklus nicht. Sie können hier die Soundmodule angeben, die vor dem Suspend aus dem Speicher entfernt werden sollen und bei einem Resume wieder geladen werden. Vor dem Suspend schließen Sie bitte alle Soundapplikationen. Je nach verwendetem Soundsystem weisen Sie dieser Variable die Werte `alsa`, `oss` oder `kernel` zu. Mit `no` wird kein „Unload“ der Soundmodule durchgeführt.

APMD_KBD_RATE=""

Unter Umständen muss auch die Tastaturwiederholungsrate und -verzögerung wieder neu gesetzt werden. Tragen Sie einen möglichen numerischen Wert ein oder lassen Sie diese beiden Variablen leer, wenn Sie dieses Verhalten nicht wünschen.

APMD_KBD_DELAY=""**APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND=""**

Manche Notebooks kehren nicht korrekt in den normalen Betriebsmodus zurück, wenn die Festplatte zuvor im DMA-Modus war. Tragen Sie alle Platten hier ein, die einen Stop des DMA-Modus benötigen, um in den normalen Betriebsmodus zurückzukehren.

printer Drucker.

DEFAULT_PRINTER="lp"

Name des Standarddruckers, wenn beim lpr-Aufruf kein Drucker mit -P angegeben ist.

proxy Proxy-Einstellungen.

HTTP_PROXY=""

Einige Programme (z. B. lynx, arena oder wget) können Proxy-Server benutzen, wenn diese Umgebungsvariable entsprechend gesetzt ist; SuSEconfig kann diese in /etc/SuSEconfig/* setzen (vgl. in der SDB file:///usr/share/doc/sdb/de/html/lynx_proxy.html). Beispiel: "http://proxy.provider.de:3128/" .

FTP_PROXY=""

Proxy für FTP. Beispiel: "http://proxy.provider.de:3128/" .

NO_PROXY="localhost"

Mittels dieser Variable lassen sich (Sub-)Domains vom Proxy ausschließen. Beispiel: "www.me.de, do.main, localhost" .

security Einstellungen zur Systemsicherheit.

CHECK_PERMISSIONS="set"

Legt fest, ob die Datei-Rechte anhand der Datei /etc/permissions überprüft werden sollen. Mit set werden falsche Einstellungen berichtigt, mit warn werden nur „Warnungen“ hergestellt, no wird dieses Merkmal abgestellt.

PERMISSION_SECURITY="easy local"

In /etc/permissions.paranoid, /etc/permissions.secure und /etc/permissions.easy sind drei Sicherheitsstufen vorbereitet. Tragen Sie hier easy, secure oder paranoid ein; eigene Einstellungen können Sie z. B. in /etc/permissions.local vornehmen und dann die Erweiterung local als Wert hinzufügen.

Beachten Sie, dass bei Auswahl der Option paranoid einige Systemdienste möglicherweise nicht mehr so zur Verfügung stehen, wie Sie das wünschen; dies bedeutet, dass Sie gezielt die Dienste „freischalten“ müssen, die Sie benötigen!

Achtung: Wenn Sie Angaben in /etc/permissions.local vornehmen, kontrollieren Sie bitte, dass diese in keinem Konflikt zu Vorgaben des Rotationsmechanismus (Paket logrotate) stehen. logrotate überschreibt Angaben von /etc/permissions.local; vgl. Abschnitt [Protokoll-Dateien – das Paket logrotate](#) auf Seite 147.

sendmail Die sendmail-Variablen; verwenden Sie das mail-Modul von YaST2 zur Konfiguration.

sound Angaben zur Soundkonfiguration**LOAD_SEQUENCER="yes"**

Sollen die ALSA Sequencer Module beim Boot-up geladen werden? Diese Module benötigen Sie nur, wenn Sie mit MIDI Devices arbeiten. Sollten Sie kein MIDI benötigen, deaktivieren Sie diese Option. Die Module können auch automatisch nachgeladen werden.

ssh „Secure Shell Daemon“; stellen Sie vor dem Starten sicher, dass ein „host key“ existiert – vgl. dazu die Dokumentation unter `/usr/share/doc/packages/ssh` sowie die Manual-Pages.

SSHD_OPTS=""**suseconfig** Grundeinstellungen für SuSEconfig.**ENABLE_SUSECONFIG="yes"**

Legt fest, ob SuSEconfig die Konfiguration durchführen soll. Bitte auf keinen Fall ausschalten, falls Sie Installationssupport in Anspruch nehmen wollen.

MAIL_REPORTS_TO="root"

Festlegen, an wen SuSEconfig Berichte per E-Mail schicken soll, die während der automatischen System-Administration erzeugt werden.

MAIL_LEVEL="warn"

Zwei Stufen sind möglich: bei `warn` werden nur die wichtigen Meldungen verschickt; bei `all` auch die Protokoll-Dateien („Logs“).

CREATE_INFO_DIR="yes"

Legt fest, ob automatisch die Datei `/usr/share/info/dir` mit einem Perl-Skript erstellt werden soll, die einen Index für alle vorhandenen Info-Seiten bildet.

CHECK_ETC_HOSTS="yes"

Legt fest, ob SuSEconfig die Datei `/etc/hosts` überprüfen und ggf. ändern soll.

BEAUTIFY_ETC_HOSTS="no"

Falls `/etc/hosts` sortiert werden soll.

SORT_PASSWD_BY_UID="no"

`/etc/passwd` und `/etc/group` nach „UID“ bzw. „GID“ sortieren.

CWD_IN_ROOT_PATH="no"

Aktuelles Verzeichnis (engl. *current working directory*) im Pfad von `root`; davon wird aus Sicherheitsgründen abgeraten. Diese Einstellung betrifft alle Benutzer mit einer UID unter 100 (engl. *system users*).

CWD_IN_USER_PATH="yes"

Soll das aktuelle Verzeichnis (engl. *current working directory*) im Pfad der normalen Benutzer liegen?

CREATE_PERLLOCAL_POD="yes"

yes erlaubt es SuSEconfig, die Datei `perllocal.pod` zu verändern. In `perllocal.pod` sind die Installationsspezifika einzelner Perl-Module enthalten.

UPDATE_GROFF_CONF="yes"

DESC aktualisieren, um die Blattgröße korrekt einzustellen.

GROFF_PAGESIZE=""

Wenn die Blattgröße aus der `/etc/printcap` nicht hervorgeht, ist die Einstellung hier vorzunehmen. `letter`, `legal`, `a4` und `a5` werden von `groff` und `ghostscript` unterstützt.

sysctl System auf Kernellevel kontrollieren.

IP_DYNIP="no"

Den „dynamic IP patch“ beim Booten aktivieren; bei `yes` gibt das Skript `/etc/init.d/boot.proc` diesen Patch durch einen Eintrag in das `/proc`-Dateisystem frei.

IP_TCP_SYNCOOKIES="yes"

Schutz vor „Syn Flooding“ (engl. *syn flood protection*) aktivieren; vgl. `/usr/src/linux/Documentation/Configure.help`.

IP_FORWARD="no"

Wenn der Rechner über zwei Netzwerk-Interfaces weiterleiten soll, ist `<IP_FORWARD>` auf `yes` zu setzen; dies ist bei einem „Router“ der Fall.

ENABLE_SYSRQ="no"

Interna des Kernels betrachten. Vor Anwendungen bitte unbedingt `/usr/src/linux/Documentation/sysrq.txt` lesen!

DISABLE_ECN="yes"

Mit `yes` wird ECN (engl. *early congestion notification*) zur Bootzeit abgeschaltet; nützlich wenn es Verbindungsschwierigkeiten zur anderen Rechnern im Internet gibt, die aufgrund einer eigenartigen Firewallkonfiguration Netzwerkpakete verwerfen und diese Verbindungen zuvor mit dem Linux-Kernel 2.2 funktioniert hatten.

BOOT_SPLASH="yes"

Den „Splashscreen“ zur Bootzeit abschalten.

syslog Syslog-Daemon konfigurieren.

KERNEL_LOGLEVEL="/var/lib/dhcp/dev/log"

Zusätzlicher Eintrag, der vom dhcp-server Paket generiert wurde. Der hier eingetragene Dateiname wird mittels `-a <Dateiname>` als zusätzlicher Socket über `<SYSLOGD_PARAMS>` automatisch hinzugefügt, sobald syslogd gestartet wird. Dies ist nötig, um einem „chrooted“ betriebenen dhcpd nach einem Neustart des syslogd weiteres Logging zu ermöglichen.

KERNEL_LOGLEVEL="1"

Loglevel für klogd.

SYSLOGD_PARAMS=""

Parameter für den syslogd; z. B. `"-r -s my.dom.ain"`.

syslog-ng Syslog-ng konfigurieren.

SYSLOG_NG_REPLACE="yes"

Soll syslog-ng den „alten“ syslogd ersetzen? Wird diese Variable auf `no` gesetzt, starten beide Programme.

SYSLOG_NG_PARAMS=""

Parameterübergabe an syslog-ng. Bitte entnehmen Sie `man 8 syslog-ng` die nötigen Details.

tetex T_EX/L_AT_EX.

CLEAR_TEXMF_FONTS="no"

Im Rahmen der automatischen Fontgenerierung für das TeX/LaTeX-System werden Bitmap-Fonts im Verzeichnis `/var/cache/fonts/` abgelegt. Setzen Sie diese Variable auf `yes` werden in diesem Verzeichnis regelmäßig alle Fonts gelöscht, die länger als 20 Tage nicht verwendet wurden.

windowmanager Windowmanager.

DEFAULT_WM="kde"

Mögliche Einstellungen: `kde`, `gnome`, `fvwm` etc.

INSTALL_DESKTOP_EXTENSIONS="yes"

SuSE-Erweiterungen für neu angelegte Benutzer installieren. Dabei handelt es sich um „Themes“ und zusätzliche Funktionen, die das System benutzerfreundlich gestalten.

KDE_USE_FAM="no"

fam-Daemon vorverwenden; nur sinnvoll bei Verzeichnissen, die über NFS eingehängt werden.

KDE_USE_FAST_MALLOC="yes"

Das verbesserte malloc verwenden.

SUSEWM_UPDATE="yes"

Legt fest, ob SuSEconfig die systemweiten Konfigurationsdateien für die Windowmanager in Abhängigkeit von den installierten Software-Paketen anpassen soll.

SUSEWM_WM="all"

Liste der Windowmanager, für die Konfigurationsdateien erzeugt werden sollen; mögliche Werte: fvwm, fvwm2, fvwm95, bowman, mwm, ctwm, kwm sowie all (für alle).

SUSEWM_XPM="yes"

Das Paket 3dpixms muss installiert sein, damit beim fvwm/fvwm95 Pix-maps in den Menüs erscheinen; wenn der Windowmanager dadurch für den Benutzer zu langsam wird, ist diese Variable auf no zu setzen.

xdmisc Zum Betrieb von X-Terminals.

START_RX="no"

Bevor Sie diese Variable verändern, editieren Sie bitte zuerst die Datei /etc/inittab und entfernen Sie dort die Zeile mit /sbin/init.d/rx. Ausserdem müssen die Variablen $\langle RX_XDMCP \rangle$ und $\langle RX_RHOST \rangle$ gesetzt. Dann setzen Sie diese Variable auf yes, um ein X-Terminal zu bekommen.

RX_XDMCP="broadcast"

Konfiguration der XDMCP (engl. *XDM Control Protocol*) Requests. query – bei einem XDM-Server um ein Login-Fenster anfragen, indirect – bei einem XDM-Server um ein Chooser-Menü anfragen und broadcast – bei allen im Netz befindlichen XDM-Servern um ein Login-Fenster anfragen, der Erste gewinnt. Für die beiden Optionen query und indirect muss $\langle RX_HOST \rangle$ gesetzt sein.

RX_RHOST=""

Name des XDM-Hosts.

RX_DSP=""

Hier können Sie optional die Displaynummer festlegen. Die Standardeinstellung ist : 0.

RX_BPP=""

Farbtiefe des lokalen X-Servers. Diese Angabe ist optional.

RX_CLASS=""

xntp Startet den „Network Time Protocol (NTP) Daemon“ aus dem Paket xntp; die Konfiguration selbst geschieht über die Datei /etc/ntp.conf.

XNTPD_INITIAL_NTPDATE="AUTO-2"

Mit Leerzeichen abgeteilte Liste der NTP-Server, von denen die Zeit geholt werden kann, bevor der lokale Server gestartet wird; z. B.

"sonne.kosmos.all".

Es ist auch möglich `AUTO` einzutragen, dann werden alle Server und Peers abgefragt, die in `/etc/ntp.conf` konfiguriert sind. Zudem kann man die Gesamtzahl der abzufragenden Server durch anhängen einer Zahl einschränken; Vorgabe ist `AUTO-2`.

Funkuhren haben Adressen in der Form `127.127.T.U`; dabei steht `T` für den Typ der Uhr und `U` ist die „unit number“ im Bereich von 0 bis 3. – Die meisten dieser Uhren benötigen eine serielle Schnittstelle oder einen speziellen Bus. Die dafür vorgesehene Gerätedatei (Device) wird normalerweise durch einen symbolischen Link `/dev/device-U` auf die tatsächliche Hardware angegeben; dabei hat `U` mit der zuvor erwähnten „unit number“ übereinzustimmen. Vgl. auch </usr/share/doc/packages/xntp/html/refclock.htm>.

Beispiel: Wer eine Funkuhr hat, die an eine serielle Schnittstelle angeschlossen ist, der benötigt auch einen entsprechenden Symlink. Wie der zu heißen hat, erfährt man über `refclock.htm`. – Für die üblichen DCF77-Empfänger, ist der „PARSE“-Treiber zuständig:

```
## Type 8 Generic Reference Driver (PARSE)
## Address:      127.127.8.u
## Serial Port:  /dev/refclock-u
```

Wer also über einen `ntp.conf`-Eintrag den `server 127.127.8.0` wählt, der braucht auch einen Symlink von `/dev/refclock-0` auf `ttysx` – dabei steht `x` für die Schnittstelle, an die die Funkuhr angeschlossen ist.

ypbind Konfiguration eines NIS-Client. Zusätzliche Informationen: Der Domainname steht direkt in `/etc/defaultdomain`. Server wird bei der Konfiguration mit `Yast2` direkt in `/etc/yp.conf` eingetragen; vgl. Abschnitt *NIS – Network Information Service* auf Seite 237.

YPBIND_OPTIONS=""

Optionen.

YPBIND_LOCAL_ONLY="no"

Setzen Sie diese Option auf `yes`, verbindet sich `ypbind` nur mit dem lokalen Loopback Interface. Andere Hosts können es nicht abfragen.

YPBIND_BROADCAST="no"

Wird diese Option auf `yes` gesetzt, ignoriert `ypbind` die Datei `/etc/yp.conf` und versucht, über einen Broadcast-Call einen verfügbaren NIS-Server im lokalen Subnetz zu finden. Bitte vermeiden Sie diese Option, da sie ein großes Sicherheitsloch darstellt.

YPBIND_BROKEN_SERVER="no"

Sollten Sie in Ihrem Netz einen NIS-Server haben, der sich nur mit höheren Ports als 1024 verbindet, ist diese Option auf **yes** zu setzen. Allerdings stellt dies ein Sicherheitsrisiko dar – Sie sollten die Verwendung einer anderen NIS-Server Implementation in Betracht ziehen.

ypserv Einstellungen zur Konfiguration eines NIS-Servers

YPPWD_SRCDIR="/etc"

Falls Sie ein von **/etc** abweichendes Verzeichnis für die Quelldateien für **passwd**, **shadow** und **group** festlegen wollen, geben Sie es hier an.

YPPWD_CHFN="no"

Darf der Benutzer mittels **ypchfn** sein GECOS-Feld (mit zusätzlichen Informationen wie Telefonnummern etc.) ändern?

YPPWD_CHSH="no"

Darf der Benutzer mittels **ypchsh** sein Standard-Login ändern?

zope Konfiguration eines ZOPE-Systems.

ZOPE_FTP="yes"

Soll Zope einen FTP-Zugang bieten?

ZOPE_FTP_PORT="8021"

Über welchen Port soll der Zugang möglich sein?

ZOPE_HTTP_PORT="8080"

Falls Zope als Standalone Webserver fungieren soll, müssen Sie den Port festlegen, den er belegen soll.

Teil II

Netzwerk

Grundlagen der Vernetzung

Linux, ein wahres Kind des Internets, bietet Ihnen alle Voraussetzungen und notwendigen Netzwerktools zur Einbindung in diverse Netzwerkstrukturen. Im folgenden erhalten Sie eine Einführung in das normalerweise von Linux verwendete Protokoll TCP/IP, dessen Dienstleistungen und auch besonderen Eigenschaften. Anschließend zeigen wir Ihnen die Einrichtung eines Netzwerkzugangs mit einer Netzwerkkarte unter SuSE Linux Desktop mit Hilfe von YAST2. Es werden die zentralen Konfigurationsdateien besprochen und einige der wichtigsten Tools aufgeführt.

Da die Konfiguration eines Netzwerks beliebig komplex sein kann, werden in diesem Kapitel nur die grundlegenden Mechanismen dargestellt.

| | |
|---|-----|
| TCP/IP - Das von Linux verwendete Protokoll | 202 |
| IPv6 – Internet der nächsten Generation | 210 |
| Die Einbindung ins Netzwerk | 216 |
| Manuelle Netzwerkkonfiguration | 219 |
| Routing unter SuSE Linux Desktop | 225 |
| DNS – Domain Name Service | 227 |
| NIS – Network Information Service | 237 |
| NFS – verteilte Dateisysteme | 242 |
| DHCP | 247 |

TCP/IP - Das von Linux verwendete Protokoll

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Genau genommen handelt es sich um eine Protokollfamilie, die ganz unterschiedliche Dienstleistungen bietet. TCP/IP wurde aus einer militärischen Anwendung heraus entwickelt und in der heute verwendeten Form ca. 1981 in einem so genannten RFC festgelegt. Bei RFC (engl. *Request for comments*) handelt es sich um Dokumente, die die verschiedenen Internetprotokolle und die Vorgehensweise bei der Implementierung des Betriebssystems und von Applikationen beschreiben. Auf diese RFC-Dokumente können Sie direkt über das Web zugreifen, die URL lautet <http://www.ietf.org/>. In der Zwischenzeit sind einige Verfeinerungen am TCP/IP Protokoll vorgenommen worden, am grundlegenden Protokoll hat sich seit 1981 aber nichts geändert.

Tipp

Die RFC Dokumente beschreiben den Aufbau der Internet Protokolle. Falls Sie Ihr Know-how über ein bestimmtes Protokoll vertiefen wollen, ist das passende RFC Dokument die richtige Anlaufstelle:

<http://www.ietf.org/rfc.html>

Tipp

Die in Tabelle 9.1 auf der nächsten Seite genannten Dienste stehen zur Verfügung, um Daten zwischen zwei Linuxrechnern über TCP/IP auszutauschen:

| Protokoll | Beschreibung |
|-----------|--|
| TCP | (engl. <i>Transmission control protocol</i>) Ein verbindungsorientiertes, gesichertes Protokoll. Die zu übertragenden Daten werden aus der Sicht der Applikation als Datenstrom verschickt und vom Betriebssystem selbst in das passende Übertragungsformat gebracht. Die Daten kommen bei der Zielapplikation auf dem Zielrechner als exakt der Datenstrom an, als der sie abgeschickt wurden. TCP stellt sicher, dass unterwegs keine Daten verloren gehen und nichts durcheinander kommt. TCP wird dort verwendet, wo die Reihenfolge der Daten wichtig ist und der Begriff Verbindung Sinn macht. |

Tabelle 9.1: Fortsetzung auf der nächsten Seite...

| | |
|------|---|
| UDP | (engl. <i>User Datagram protocol</i>) Ein verbindungsloses, ungesichertes Protokoll. Die zu übertragenden Daten werden paketorientiert verschickt, die Datenpakete werden dabei schon von der Applikation erzeugt. Die Reihenfolge der Daten beim Empfänger ist nicht garantiert, ebenso kann es passieren, dass einzelne Datenpakete verloren gehen. UDP eignet sich für datensatzorientierte Applikationen und bietet kleinere Latenzzeiten als TCP. |
| ICMP | (engl. <i>Internet control message protocol</i>) Im Wesentlichen ist das kein für den Benutzer verwendbares Protokoll, sondern ein spezielles Steuerprotokoll, das Fehlerzustände übermittelt und das Verhalten der an der TCP/IP-Datenübertragung beteiligten Rechner steuern kann. Zusätzlich wird durch ICMP noch ein spezieller Echo-Modus bereitgestellt, den man mit dem Programm ping prüfen kann. |
| IGMP | (engl. <i>Internet group management protocol</i>) Dieses Protokoll steuert das Verhalten von Rechnern bei der Verwendung von IP-Multicast. Leider kann IP-Multicasting in diesem Rahmen nicht vorgestellt werden. |

Tabelle 9.1: Verschiedene Protokolle der TCP/IP Protokollfamilie

Fast alle Hardwareprotokolle arbeiten paketorientiert. Die zu übertragenden Daten müssen in kleine „Päckchen“ gepackt werden und können nicht „in einem Rutsch“ verschickt werden. Deshalb arbeitet auch TCP/IP mit kleinen Datenpaketen. Die Maximalgröße eines TCP/IP Paketes ist knapp 64 Kilobyte. In der Praxis sind die Pakete normalerweise viel kleiner, da die Netzwerkhardware der limitierende Faktor ist. So ist die zulässige Maximalgröße eines Datenpaketes auf dem Ethernet ca. 1500 Byte. Dementsprechend wird die Paketgröße des TCP/IP Pakets begrenzt, wenn die Daten über ein Ethernet geschickt werden. Will man mehr Daten übertragen, müssen vom Betriebssystem entsprechend mehr Datenpakete verschickt werden.

Schichtenmodell

Über IP (engl. *Internet protocol*) findet eine ungesicherte Datenübertragung statt. TCP (engl. *Transmission control protocol*) ist gewissermaßen nur ein Aufsatz auf das darunter liegende IP, um eine gesicherte Übertragung der Daten zu garan-

tieren. IP selbst ist wiederum ein Aufsatz auf das darunter liegende, hardware-abhängige Protokoll, zum Beispiel Ethernet. Kenner sprechen hier vom „Schichtenmodell“. Vergleichen Sie hierzu die Abbildung 9.1.

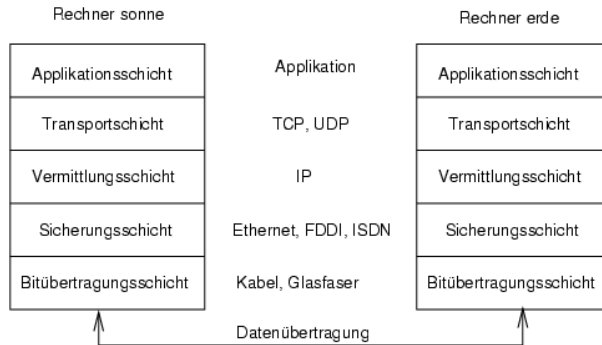


Abbildung 9.1: Vereinfachtes Schichtenmodell für TCP/IP

In der Abbildung sind jeweils ein oder zwei Beispiele für die jeweilige Schicht erwähnt. Wie Sie sehen, sind die Schichten nach „Abstraktionsebenen“ geordnet, die unterste Schicht ist sehr nah an der Hardware. Die oberste Schicht hingegen abstrahiert die darunter liegende Hardware nahezu vollständig. Jede der Schichten hat eine ganz spezielle Funktion, die zum Großteil schon aus der Bezeichnung hervorgeht. So wird das verwendete Netzwerk (z. B. Ethernet) durch die Bitübertragungsschicht und die Sicherungsschicht verkörpert.

- Während sich Schicht 1 mit solchen Dingen wie Kabeltypen, Signalformen, Signalkodierung und ähnlichem beschäftigt ist Schicht 2 für das Zugriffsverfahren (Welcher Rechner darf wann Daten schicken?) und eine Fehlerkorrektur (Datensicherung - deshalb Sicherungsschicht) zuständig. Die Schicht 1 nennt man die Bitübertragungsschicht.
- Schicht 3 wiederum, die Vermittlungsschicht ist für die Datenübertragung über weite Strecken verantwortlich. Die Vermittlungsschicht stellt sicher, dass die Daten auch über weite Strecken beim richtigen Empfänger ankommen und zugestellt werden können.
- Schicht 4, die Transportschicht, ist für die Daten der Applikation verantwortlich und stellt sicher, dass die Daten in der richtigen Reihenfolge ankommen und nicht verloren gehen. Die Sicherungsschicht ist nur dafür verantwortlich, dass die ankommenden Daten korrekt sind. Gegen das „Verlieren“ von Daten schützt die Transportschicht.

- Schicht 5 schließlich ist die Datenverarbeitung durch die Applikation selbst.

Damit jede der Schichten die ihr zugeteilte Aufgabe erfüllen kann, müssen zusätzliche Informationen der jeweiligen Schicht im Datenpaket im Header, dem Kopf des Datenpakets, gespeichert werden. Jede der Schichten fügt einen kleinen Datenblock, den sog. „Protokollkopf“ (engl. *Protocol header*), an das im Entstehen begriffene Paket vorne dran. Schauen wir uns also einmal ein beliebiges TCP/IP-Datenpaket an, das auf einem Ethernetkabel unterwegs ist, so setzt sich dieses wie in Bild 9.2 abgebildet zusammen.

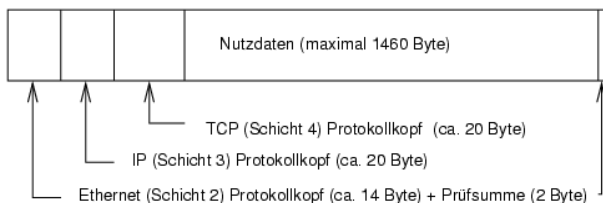


Abbildung 9.2: TCP/IP Paket im Ethernet

Wie Sie sehen, ist die Welt nicht perfekt und ohne Ausnahme. Die Prüfsumme der Sicherungsschicht befindet sich am Ende des Pakets und nicht am Anfang. Dies bringt aber für die Netzwerkhardware eine Vereinfachung. Die maximal mögliche Menge der Nutzdaten in einem Paket beträgt im Ethernet-Netzwerk 1460 Byte.

Möchte eine Applikation also Daten über das Netzwerk verschicken, durchlaufen die Daten die einzelnen Schichtebenen, die alle im Linuxkernel (Ausnahme Schicht 1: Netzwerkkarte) implementiert sind. Jede der Schichten ist dafür verantwortlich, die Daten so aufzubereiten, dass sie an die jeweils darunter liegende Schicht weitergereicht werden können. Die unterste Schicht ist schließlich für den eigentlichen Datenversand zuständig. Beim Empfang läuft das ganze nun umgekehrt ab. Wie bei den Schalen einer Zwiebel werden von jeder Schicht die Protokollköpfe von den Nutzdaten entfernt. Schicht 4 ist dann letztendlich dafür verantwortlich, die Daten für die Applikation auf dem Zielrechner bereitzustellen. Dabei kommuniziert eine Schicht immer nur mit der Schicht direkt über oder unter ihr. Für eine Applikation ist es also irrelevant, ob die Daten über ein 100-MBit/s-FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Umgekehrt ist es für die Datenübertragungsleitung egal, welche Daten eigentlich verschickt werden, solange sie richtig verpackt sind.

| | | | | |
|-----------------------|----------|----------|----------|----------|
| IP-Adresse (binär): | 11000000 | 10101000 | 00000000 | 00010100 |
| IP-Adresse (dezimal): | 192. | 168. | 0. | 20 |

Tabelle 9.2: Schreibweise einer IP-Adresse

IP-Adressen und Routing

IP-Adressen

Jeder Computer im Internet hat eine eindeutige 32-Bit-Adresse. Diese 32 Bit bzw. 4 Byte werden normalerweise wie in Tabelle 9.2 in der zweiten Zeile abgebildet geschrieben.

Die vier Bytes werden also im dezimalen Zahlensystem durch einen Punkt getrennt nebeneinander geschrieben. Die IP-Adresse ist einem Rechner bzw. einer Netzwerkschnittstelle zugeordnet, sie kann also nicht woanders auf der Welt nochmals verwendet werden. Ausnahmen von diesen Regeln gibt es zwar, spielen aber bei der folgenden Betrachtung erst einmal keine Rolle.

Auch die Ethernetkarte besitzt selbst eine eindeutige Adresse, die so genannte MAC (engl. *Media access control*) Adresse. Diese ist 48 Bit lang, weltweit eindeutig und wird vom Hersteller der Netzwerkkarte fest in der Hardware gespeichert. Durch die Vergabe der Adresse vom Hersteller ergibt sich aber ein fataler Nachteil: Die MAC-Adressen bilden kein hierarchisches System, sondern sind mehr oder weniger zufällig verteilt. Sie können daher nicht zur Adressierung eines weit entfernten Rechners verwendet werden. Die MAC-Adresse spielt aber bei der Kommunikation von Rechnern in einem lokalen Netz eine entscheidende Rolle (und ist der Hauptbestandteil des Protokollkopfes von Schicht 2).

Zurück zu den IP-Adressen: Die Punkte deuten schon an, dass die IP-Adressen ein hierarchisches System bilden. Bis Mitte der 90er Jahre waren die IP-Adressen fest in Klassen eingeteilt. Dieses System erwies sich aber als zu unflexibel und daher wurde diese Aufteilung aufgegeben. Man verwendet nun „klassenloses Routing“ (CIDR (engl. *classless inter domain routing*)).

Netzmasken und Routing

Da der Rechner mit der IP-Adresse 192.168.0.20 erst einmal nicht wissen kann, wo sich der Rechner mit der IP-Adresse 192.168.0.1 befindet, wurden die Netzmasken erdacht.

Vereinfacht gesagt definiert die (Sub-)Netzmaske auf einem Rechner mit IP-Adresse, was „drinnen“ und was „draußen“ ist. Rechner, die sich „drinnen“ (Profis sagen: „im gleichen Subnetz“) befinden, können direkt angesprochen

| | | | | |
|--------------------------|----------|----------|----------|----------|
| IP-Adresse: 192.168.0.20 | 11000000 | 10101000 | 00000000 | 00010100 |
| Netzmaske: 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |
| Ergebnis binär | 11000000 | 10101000 | 00000000 | 00000000 |
| Ergebnis dezimal | 192. | 168. | 0. | 0 |

| | | | | |
|---------------------------|----------|----------|----------|----------|
| IP-Adresse: 213.95.15.200 | 11010101 | 10111111 | 00001111 | 11001000 |
| Netzmaske: 255.255.255.0 | 11111111 | 11111111 | 11111111 | 00000000 |
| Ergebnis binär | 11010101 | 10111111 | 00001111 | 00000000 |
| Ergebnis dezimal | 213. | 95. | 15. | 0 |

Tabelle 9.3: Verknüpfung der IP-Adressen mit der Netzmaske

werden. Rechner, die sich „draußen“ („nicht im gleichen Subnetz“) befinden, müssen über ein so genanntes Gateway oder Router angesprochen werden. Da jedes Netzwerkinterface eine eigene IP-Adresse bekommen kann, ahnen Sie schon, dass es schnell beliebig kompliziert wird.

Bevor ein Netzwerkpaket auf die Reise geschickt wird, läuft folgendes im Rechner ab: Die Zieladresse wird mit der Netzmaske bitweise UND verknüpft. Daraufhin wird auch die Absendeadresse bitweise mit der Netzmaske UND verknüpft (siehe Tabelle 9.3). Stehen mehrere Netzwerkinterfaces zur Verfügung, werden in der Regel alle möglichen Absendeadressen überprüft.

Die Ergebnisse der UND-Verknüpfungen werden verglichen. Ergibt sich zwischen den Ergebnissen eine exakte Übereinstimmung, so befindet sich der Zielrechner im gleichen Subnetz. Ansonsten muss er über ein Gateway angesprochen werden. Das heißt, je mehr „1“ Bits sich in der Netzmaske befinden, desto weniger Rechner können direkt, sondern nur über ein Gateway angesprochen werden. Zur Veranschaulichung sind in Tabelle 9.3 mehrere Beispiele aufgeführt.

Die Netzmaske wird wieder – wie schon die IP-Adresse – in Form von durch Punkte getrennten Dezimalzahlen geschrieben. Da die Netzmaske auch ein 32-Bit-Wert ist, werden vier Zahlenwerte nebeneinander geschrieben. Welche Rechner Gateway sind oder welche Adressbereiche über welche Netzwerkschnittstelle erreichbar sind, muss vom Benutzer konfiguriert werden.

Um wieder ein Beispiel zu geben: Alle Rechner, die am gleichen Ethernetkabel angeschlossen sind, befinden sich in der Regel *im gleichen Subnetz* und sind direkt erreichbar. Auch wenn das Ethernet über Switches oder Bridges unterteilt ist, sind diese Rechner immer noch direkt erreichbar.

Wollen Sie eine längere Strecke überbrücken, ist das preiswerte Ethernet dafür nicht mehr geeignet. Sie müssen dann die IP-Pakete auf andere Hardware (z. B.

FDDI oder ISDN) weiterleiten. Solche Geräte heißen Router bzw. Gateway. Ein Linuxrechner kann diese Aufgabe selbstverständlich auch erledigen, die entsprechende Option wird mit `ip_forwarding` bezeichnet.

Ist ein Gateway konfiguriert, wird das IP-Paket an das passende Gateway geschickt. Dieses versucht, das Paket dann wiederum nach dem gleichen Schema weiterzuleiten. Das wiederholt sich auf jedem weiteren Rechner sooft, bis das Paket entweder den Zielrechner erreicht hat oder die „Lebenszeit“ TTL (engl. *time to live*) des Paketes verbraucht ist.

| Adressart | Beschreibung |
|----------------------------|--|
| Die Netzwerkbasisisadresse | Das ist die Netzmaske UND eine beliebige Adresse aus dem Netz, also das was in Tabelle 9.3 auf der vorherigen Seite unter Ergebnis abgebildet ist. Diese Adresse kann keinem Rechner zugewiesen werden. |
| Die Broadcastadresse | Sie heißt soviel wie: „Sprich alle Rechner in diesem Subnetz an“. Um sie zu erzeugen wird die Netzmaske binär invertiert und mit der Netzwerkbasisisadresse ODER verknüpft. Obiges Beispiel ergibt also 192.168.0.255. Natürlich kann auch diese Adresse keinem Rechner zugewiesen werden. |
| Der Localhost | Die Adresse 127.0.0.1 ist auf jedem Rechner fest dem so genannten „Loopbackdevice“ zugewiesen. Über diese Adresse kann man eine Verbindung auf den eigenen Rechner aufbauen. |

Tabelle 9.4: Spezielle Adressen

Da die IP-Adressen aber weltweit eindeutig sein müssen, können Sie natürlich nicht beliebige Adressen erfinden. Damit Sie aber trotzdem ein auf IP basierendes Netzwerk aufbauen können gibt es drei Adressbereiche, die Sie ohne weiteres verwenden können. Mit diesen können Sie allerdings nicht so ohne weiteres Verbindungen in das Internet aufbauen, da diese Adressen im Internet nicht weitergeleitet werden.

Dabei handelt es sich um diese Adressbereiche die in RFC 1597 definiert sind:

| Netzwerk, Netzmaske | Bereich |
|--------------------------|-------------------------|
| 10.0.0.0, 255.0.0.0 | 10.x.x.x |
| 172.16.0.0, 255.240.0.0 | 172.16.x.x - 172.31.x.x |
| 192.168.0.0, 255.255.0.0 | 192.168.x.x |

Tabelle 9.5: Private IP-Adressbereiche

Domain Name System

DNS

DNS sorgt dafür, dass Sie sich nicht zwingend irgendwelche IP-Adressen merken müssen: Mit Hilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch eine Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise von einer speziellen Software namens `bind`. Der Rechner, der diese Umwandlung dann erledigt, nennt sich `Nameserver`. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an, z. B.

`laurent.suse.de` geschrieben im Format `Rechnername.Domain`. Ein vollständiger Name – Experten sagen „fully qualified domain name“ oder kurz `FQDN` dazu – besteht aus einem Rechnernamen und einem Domainteil. Dabei wird der Domainteil aus einem frei wählbaren Anteil – im obigen Beispiel `suse` – und der so genannten `Top level domain`, `TLD` gebildet.

Aus historischen Gründen ist die Zuteilung der `TLDs` etwas verwirrend. So werden in den USA dreibuchstabige `TLDs` verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen.

In der Frühzeit des Internets (vor 1990) gab es hierzu eine Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge von am Internet angeschlossener Rechner als unpraktikabel. Deshalb wurde eine dezentrale Datenbank entworfen, die die Rechnernamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte `Nameserver`, hält also nicht die Daten aller Rechner im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere `Nameserver` weiterdelegieren.

An der Spitze der Hierarchie befinden sich die „Root-Nameserver“, die die `Top level domains` verwalten. Die `Root-Nameserver` werden vom `Network Information Center` (`NIC`) verwaltet. Der `Root-Nameserver` kennt die jeweils für

eine Top level domain zuständigen Nameserver. Im Falle der deutschen Top level domain de ist das DE-NIC für die Domains zuständig, die mit der TLD de aufhören. Mehr Informationen zum DE-NIC erhalten Sie auf der Website <http://www.denic.de>, mehr Informationen zum Top level domain NIC erfahren Sie unter <http://www.internic.net>.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Nameservers erledigen Sie komfortabel mit Hilfe von Yast2. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass das zur Einwahl verwendete Protokoll die Adresse des Nameservers während der Einwahl mitliefert.

Aber nicht nur Rechnernamen können über DNS aufgelöst werden, DNS kann noch mehr. Zum Beispiel „weiß“ der Nameserver auch, welcher Rechner für eine ganze Domain E-Mails annimmt, der so genannte Mail exchanger (MX).

Die Konfiguration des Nameserverzugriffs unter SuSE Linux Desktop ist im Abschnitt *DNS – Domain Name Service* auf Seite 227 beschrieben.

whois

Eng verwandt mit DNS ist das Protokoll whois. Mit dem gleichnamigen Programm whois können Sie schnell herauskriegen, wer für eine bestimmte Domain verantwortlich ist.

IPv6 – Internet der nächsten Generation

Warum ein neues Internet-Protokoll?

Bedingt durch die Erfindung des WWW (engl. *World Wide Web*) ist das Internet und damit die Anzahl der Rechner, die TCP/IP „sprechen“, in den letzten zehn Jahren explosionsartig gewachsen. Seit der Erfindung des WWW durch Tim Berners-Lee 1990 am CERN (<http://public.web.cern.ch/>) ist die Zahl der Internet-Hosts von wenigen tausend auf mittlerweile ca. 100 Millionen gewachsen.

Wie Sie wissen, besteht eine IP-Adresse „nur“ aus 32 Bit. Viele IP-Adressen können durch organisatorische Bedingtheiten gar nicht verwendet werden, sie gehen verloren. Zur Erinnerung: Das Internet wird in Subnetze, also Teilnetze unterteilt. Diese bestehen immer aus einer Zweierpotenz minus zwei nutzbaren IP-Adressen. Ein Subnetz besteht also beispielsweise aus 2, 6, 14, 30 usw. IP-Adressen. Möchten Sie beispielsweise 128 Rechner an das Internet anbinden,

so benötigen Sie ein „Class C“ Subnetz mit 256 IP-Adressen, von denen nur 254 nutzbar sind. Wie Sie oben gesehen haben, entfallen zwei der IP-Adressen aus einem Subnetz, nämlich die Broadcastadresse und die Netzwerkbasissadresse.

Die Konfiguration eines Rechners im TCP/IP-Netzwerk ist relativ kompliziert. Wie Sie oben schon gesehen haben, müssen Sie auf Ihrem Rechner folgende Dinge konfigurieren: Die eigene IP-Adresse, Subnetzmaske, Gatewayadresse (falls vorhanden) und einen Nameserver. Diese Daten müssen Sie alle „wissen“ bzw. von Ihrem Provider bekommen, sie können nicht irgendwoher abgeleitet werden. In jedem IP-Paket ist eine Prüfsumme enthalten, die bei jedem Routingvorgang überprüft und neu berechnet werden muss. Deshalb benötigen sehr schnelle Router leider sehr viel Rechenleistung, was diese Router verteuert.

Einige Dienste werden bisher mit Broadcasts realisiert (zum Beispiel das Windows Netzwerkprotokoll SMB). Rechner, die nicht an diesem Dienst interessiert sind, sind trotzdem gezwungen, die Pakete zu verarbeiten um sie dann anschließend zu ignorieren. In sehr schnellen Netzwerken kann das durchaus ein Problem werden.

Der Nachfolger des bisherigen IP, IPv6, löst all diese Probleme. Das primäre Ziel bei der Entwicklung war, den beschränkten Adressraum stark zu erweitern und die Konfiguration von Arbeitsstationen zu vereinfachen, wenn möglich zu automatisieren. In diesem Abschnitt wird von IPv4 oder IP die Rede sein, wenn das bisher verwendete und verbreitete Internet-Protokoll gemeint ist, und von IPv6, wenn es um die neue Version 6 geht.

IPv6 ist in RFC 1752 näher erläutert. IPv6 verwendet 128-Bit-Adressen, bietet also viele Milliarden IP-Adressen, genug auch bei großzügiger Verteilung der Adressen. Diese enorme Menge an IPv6-Adressen erlaubt den Luxus, das kleinste Subnetz 48 Bit „groß“ zu machen.

Dies erlaubt dann nämlich auch, die oben erläuterte MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration der Rechner sehr. In Wirklichkeit werden sogar die ersten 64 Bit zu einem so genannten EUI-64-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen, die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (PPP- und ISDN-Verbindungen!) ein EUI-64-Token zuzuweisen.

Zusätzlich gibt es in IPv6 eine neue Erfindung: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines davon kann mit Hilfe der MAC-Adresse und einem bekannten Präfix zu einem vollautomatisch konfigurierten Netz zusammengestellt werden, und ohne weitere Konfigurations-

arbeiten sind damit direkt nach dem Starten von IPv6 alle Rechner im lokalen Netz erreichbar (sog. „Link-local-Adresse“).

Aber auch die restliche Konfiguration einer Arbeitsstation kann weitgehend automatisch erfolgen. Hierzu gibt es ein spezielles Protokoll, mit dem Arbeitsstationen von einem Router eine IP-Adresse bekommen können.

Zwingend vorgeschrieben für alle IPv6 unterstützenden Rechner ist die Unterstützung von „Multicast“. Mit Hilfe von Multicast kann eine Gruppe von Rechnern auf einmal angesprochen werden, also nicht alle auf einmal („broadcast“), oder nur einer („unicast“), sondern eben ein paar. Welche das sind, hängt von der Anwendung ab. Es gibt aber auch ein paar wohldefinierte Multicastgruppen, beispielsweise „alle Nameserver“ (engl. *all nameservers multicast group*), oder „alle Router“ (engl. *all routers multicast group*).

Da eine plötzliche Umstellung aller Rechner im Internet von IPv4 auf IPv6 nicht denkbar ist, gibt es einen Kompatibilitätsmodus. Dieser bildet die bisherigen Adressen auf IPv6-Adressen ab. Gleichzeitig gibt es Mechanismen wie „Tunneling“. Hierbei werden IPv6-Pakete in IPv4-Paketen verpackt verschickt. Natürlich sind auch Umsetzungen von IPv6 auf IPv4 und umgekehrt möglich. Um einen IPv6-Rechner von einem IPv4-Rechner aus erreichen zu können, ist es allerdings nötig, dass der IPv6-Rechner eine IPv4-Kompatibilitätsadresse hat.

Aufbau einer IPv6-Adresse

Sie können sich sicher vorstellen, dass eine IPv6-Adresse, bedingt durch die 128 Bit, wesentlich länger wird als eine IPv4-Adresse mit Ihren 32 Bit. Immerhin ist eine IPv6-Adresse damit 16 Byte lang. Verursacht durch die Größe werden die neuen IPv6-Adressen in einer anderen Schreibweise geschrieben als die bisher verwendeten IPv4-Adressen. Schauen wir uns einmal die Beispiele in Tabelle 9.6 auf der nächsten Seite an.

Wie Sie der Tabelle entnehmen, werden IPv6-Adressen mit Hilfe von Hexadezimalzahlen dargestellt. Die Hexadezimalzahlen werden immer zu je zwei Byte gruppiert zusammengefasst und durch `:` getrennt dargestellt. Es gibt daher maximal acht Gruppen und sieben Doppelpunkte in einer Adresse. Führende Null-Bytes in einer Gruppe dürfen weggelassen werden, nicht aber inmitten oder am Ende einer Gruppe. Mehr als vier Null-Bytes direkt hintereinander kann man durch das Auslassungszeichen `::` überspringen. Allerdings ist nur ein Auslassungszeichen in einer Adresse erlaubt. Dieser Vorgang des Auslassens wird in Englisch mit „collapsing“ bezeichnet. Eine Spezialdarstellung sind IPv4-Kompatibilitätsadressen: Hier wird die IPv4-Adresse einfach an den festgelegten Präfix für IPv4-Kompatibilitätsadressen angehängt.

| Bezeichnung | Adresswert |
|------------------------------|--|
| Localhost | ::1 |
| IPv4 kompatible IPv6-Adresse | ::10.10.11.102 (IPv6 wird unterstützt) |
| IPv4 gemappte IPv6-Adresse | ::ffff:10.10.11.102 (IPv6 wird nicht unterstützt) |
| beliebige Adresse | 3ffe:400:10:100:200:c0ff:fed0:a4c3 |
| Link-local-Adresse | fe80::10:1000:1a4 |
| Site-local-Adresse | fec0:1:1:0:210:10ff:fe00:1a4 |
| Multicastgruppe | ff02:0:0:0:0:0:0:2 |
| „alle link-lokalen Router“ | |

Tabelle 9.6: Darstellung verschiedener IPv6 Adressen

Jeder Teil einer IPv6-Adresse hat eine definierte Bedeutung. Die ersten Bytes bilden einen Präfix und geben den Typ der Adresse an. Der Mittelteil adressiert ein Netzwerk oder ist bedeutungslos und den Schluss der Adresse bildet der Hostteil.

Tabelle 9.7 auf der nächsten Seite veranschaulicht die Bedeutung einiger häufiger Präfixe.

| Präfix(hexadez.) | Verwendung |
|-----------------------|--|
| 00 | IPv4 und IPv4 über IPv6-Kompatibilitätsadressen. Es handelt sich um eine zu IPv4 kompatible Adresse. Ein geeigneter Router muss das IPv6-Paket noch in IPv4 verwandeln. Weitere Spezialadressen (z. B. Loopback Device) sind ebenfalls mit diesem Präfix ausgestattet. |
| erste Ziffer 2 oder 3 | (engl. <i>provider-based-unicast</i>) Provider basierte Unicast-Adressen. Wie bisher auch können Sie bei IPv6 von einem Provider Teilnetze zugewiesen bekommen. |
| fe80 bis febf | (engl. <i>link-local</i>) Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden. |
| fec0 bis feff | (engl. <i>site-local</i>) Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb einer Organisation. Damit entsprechen diese Adressen den bisherigen „privaten“ Netzen (beispielsweise 10.x.x.x). |
| ff | (engl. <i>multicast</i>) IPv6-Adressen die mit ff anfangen sind Multicastadressen. |

Tabelle 9.7: verschiedene IPv6-Präfixe

Wie Sie oben schon sehen, sind speziell Unicastadressen sehr lang. Diese kann man sich praktisch nicht mehr merken. Ein funktionierender Nameserver ist für IPv6 daher noch wichtiger als bei IPv4. Der Nameserver ist so wichtig, dass es ein spezielles Autokonfigurationsprotokoll für Nameserver gibt.

IPv6-Netzmasken

Netzmasken werden in IPv6 etwas anders dargestellt. Da schon von Anfang an klassenloses Routing verwendet wird und schon das kleine Subnetz praktisch beliebig viele Rechner aufnehmen kann, macht die Unterteilung der Netze in Klassen keinen Sinn. Da die Netzmasken in der Darstellung sehr lang wären, werden diese nun ganz anders geschrieben. Die Schreibweise

`fec0:1:1:0:210:10ff:fe00:1a4/64`

bedeutet, dass die letzten 64 Bit den Hostteil und die vorderen 64 Bit den Netzwerkteil der Adresse bilden.

Anders gesagt bedeutet die 64, dass von links her die Netzmaske mit 1 Bits aufgefüllt wird. Es gibt in der Netzmaske also 64 1 Bits. Wie bei IPv4 wird durch eine UND-Verknüpfung der Netzmaske mit der IP-Adresse bestimmt, ob sich ein Rechner im gleichen oder in einem anderen Subnetz befindet.

Weiterführende Literatur und Links zu IPv6

Natürlich kann und will der obige Überblick keine vollständige Einführung zum sehr umfangreichen Thema IPv6 sein. Zum tieferen Einstieg in IPv6 können Sie die folgende Onlineliteratur und Bücher zu Rate ziehen:

<http://www.bieringer.de/linux/IPv6/> Linux-IPv6-HOWTO und viele Links.

<http://www.6bone.de/> Anschluss an das IPv6 über einen Tunnel bekommen.

<http://www.ipv6.org/> Alles rund um IPv6.

RFC 1725 Das einführende RFC zum Thema IPv6.

Die Einbindung ins Netzwerk

TCP/IP ist inzwischen das Standard-Netzwerkprotokoll, über das alle modernen Betriebssysteme mit TCP/IP kommunizieren können. Dennoch unterstützt Linux auch noch andere Netzwerkprotokolle, beispielsweise das (früher) von Novell Netware verwendete IPX oder das von Macintosh-Rechnern verwendete Appletalk. In diesem Rahmen besprechen wir nur die Integration eines Linux-Rechners in ein TCP/IP-Netzwerk. Wenn Sie „exotische“ Arcnet, Token-Ring oder FDDI-Netzwerkkarten einbinden wollen, finden Sie weiterführende Hilfe hierzu in den Kernelquellen `/usr/src/linux/Documentation`. Änderungen in der Netzwerk-Konfiguration seit SuSE Linux Desktop 8.0 sind in folgender Datei dokumentiert: `/usr/share/doc/packages/sysconfig/README`.

Vorbereitungen

Der Rechner muss über eine unterstützte Netzwerkkarte verfügen. Üblicherweise wird die Netzwerkkarte schon bei der Installation erkannt und der passende Treiber eingebunden. Ob Ihre Karte korrekt eingebunden wurde, können Sie unter anderem daran sehen, dass die Ausgabe des Kommandos `ifstatus eth0` das Netzwerk-Device `eth0` anzeigt.

Wenn der Kernel-Support für die Netzwerkkarte als Modul realisiert wird – so wie es beim SuSE-Kernel standardmäßig der Fall ist –, dann muss der Name des Moduls als Alias in der `/etc/modules.conf` eingetragen werden. Für die erste Ethernet-Karte z. B. in dieser Art: `alias eth0 tulip`. Dies geschieht automatisch, wenn im `linuxrc` während der Erstinstallation der Treiber-Support für die Netzwerkkarte geladen wird. Nachträglich lässt sich diese Aufgabe von YaST2 aus erledigen.

Konfiguration mit YaST2

Die Konfiguration der Netzwerkkarte lässt sich mit YaST2 schnell durchführen. Wählen Sie im Kontrollzentrum den Punkt 'Netzwerk/Basis' und anschließend 'Konfiguration der Netzwerkkarte'. In diesem Dialog integrieren Sie mit 'Hinzufügen' eine Netzwerkkarte, mit 'Entfernen' wird die entsprechende Karte aus der Konfiguration gelöscht und mit 'Bearbeiten' können die Einstellungen zu einer Netzwerkkarte geändert werden.

Aktivieren Sie den Punkt 'Hardware', um die Hardwaredaten einer schon eingerichteten Netzwerkkarte mit 'Bearbeiten' zu verändern. Sie gelangen in das Menü zur Konfiguration der Hardwaredaten Ihrer Netzwerkkarte; vgl. Abbildung 9.3 auf der nächsten Seite.

Üblicherweise wird der richtige Treiber für Ihre Netzwerkkarte schon während der Installation von YaST2 konfiguriert und die Netzwerkkarte aktiviert. Daher sind manuelle Einstellungen der Hardwareparameter nur nötig, wenn Sie mehr als eine Netzwerkkarte einsetzen oder die Netzwerkhardware nicht automatisch erkannt wird. In diesem Fall müssen Sie den Punkt 'Hinzufügen' anwählen, damit ein neues Treibermodul ausgewählt werden kann.

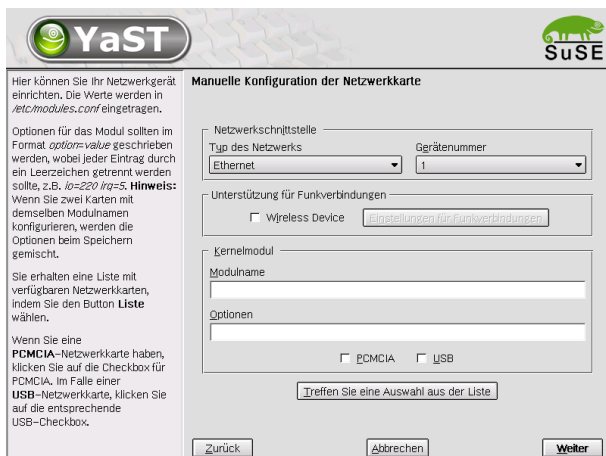


Abbildung 9.3: Konfiguration der Hardwareparameter

In diesem Dialog können Sie den Typ der Netzwerkkarte und im Falle von ISA-Karten auch den zu verwendenden Interrupt und die IO-Adresse einstellen. Manchen Netzwerktreibern können Sie auch spezielle Parameter wie die zu verwendende Schnittstelle mitgeben, ob Sie beispielsweise den RJ-45- oder BNC-Anschluss auf der Karte verwenden wollen. Beachten Sie hierzu die Dokumentation des Treibermoduls.

Nach der Eingabe der Hardwareparameter konfigurieren Sie die weiteren Daten der Netzwerkschnittstelle. Wählen Sie im Dialog 'Grundlegende Netzwerkkonfiguration' den Punkt 'Schnittstelle' aus, um die soeben einrichtete Netzwerkkarte zu aktivieren und dieser Netzwerkkarte eine IP-Adresse zuzuweisen. Wählen Sie dann die Kartenummer aus und klicken Sie auf 'Bearbeiten'. Es erscheint ein neuer Dialog, in dem Sie die IP-Adresse und die weiteren Daten des IP-Netzwerks auswählen können. Falls Sie selbst ein eigenes Netzwerk aufbauen, können Sie sich bei der Vergabe der Adressen am Abschnitt 9 auf Seite 202 bzw. der Tabelle 9.5 auf Seite 209 orientieren. Ansonsten tragen Sie bitte die von Ihrem Netzwerkadministrator zugewiesenen Adressen in die vorgesehenen Felder ein.

Vergessen Sie nicht, einen Nameserver unter 'Rechnername und Nameserver' einzustellen, damit die Namensauflösung wie in Abschnitt 9 auf Seite 227 beschrieben funktionieren kann. Über den Punkt 'Routing' können Sie das Routing einstellen. Wählen Sie den Punkt 'Konfiguration für Experten', um fortgeschrittene Einstellungen vorzunehmen.

Damit ist die Netzwerkconfiguration abgeschlossen. YcST2 ruft abschließend SuSEconfig auf und trägt Ihre Angaben in die entsprechenden Dateien ein. Damit die Einstellungen wirksam werden, müssen die betroffenen Programme neu konfiguriert und die entsprechenden Daemonen neu gestartet werden. Dies erreichen Sie, indem Sie folgenden Befehl eingeben:

```
erde:~ # rcnetwork restart
```

PCMCIA

Eine Sonderstellung nehmen PCMCIA-Netzwerkkarten ein. Im Gegensatz zu festeingebauten Netzwerkkarten, die eine gleich bleibende Gerätebezeichnung erhalten, beispielsweise `eth0`, wird PCMCIA-Karten dynamisch bei Bedarf eine freie Gerätebezeichnung zugewiesen. Um Konflikte mit eventuell fest eingebauten Karten zu vermeiden wird PCMCIA beim Booten auch erst nach dem Netzwerk gestartet.

Für PCMCIA liegen die Konfigurations- und Startskripte im Verzeichnis `/etc/sysconfig/pcmcia`. Diese Skripte werden ausgeführt, sobald `cardmgr`, der so genannte „PCMCIA Device Manager“, eine angeschlossene PCMCIA-Karte entdeckt. Deshalb ist es nicht notwendig, dass PCMCIA vor dem Netzwerk gestartet wird.

Ausführliche Informationen zu PCMCIA finden Sie im Referenz-Handbuch.

Konfiguration von IPv6

Falls Sie die Verwendung von IPv6 konfigurieren möchten, müssen Sie in der Regel keine Konfiguration auf den Arbeitsstationen durchführen. Allerdings muss die IPv6-Unterstützung geladen werden. Dies können Sie am einfachsten mit dem Kommando

```
erde:~ # modprobe ipv6
```

erledigen. Aufgrund der Autokonfigurationsphilosophie von IPv6 wird dann der Netzwerkkarte eine Adresse im `link-local` Netz zugewiesen. Normalerweise wird auf einer Arbeitsstation keine Routingtabelle gepflegt. Die Router im

Netz können über das Router Advertisement Protocol von der Arbeitsstation darüber befragt werden, welches Präfix und welche Gateways zu verwenden sind. Um einen IPv6-Router aufzusetzen, können Sie das Programm `radvd` aus Paket `radvd`, Serie `n` (Netzwerk) verwenden. Dieses Programm teilt den Arbeitsstationen das zu verwendende Präfix für IPv6-Adressen und den/die Router mit.

Um einer Arbeitsstation eine IPv6-Adresse bequem zuweisen zu können, ist es also ratsam, einen Router mit dem Programm `radvd` zu installieren und zu konfigurieren. Die Arbeitsstationen bekommen die IPv6-Adresse dann automatisch zugewiesen.

Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte stets die zweite Wahl sein. Wir empfehlen, `YaST2` zu benutzen.

Konfigurationsdateien

Dieser Abschnitt gibt eine Übersicht über die Netzwerkkonfigurationsdateien und erklärt ihre Funktion sowie das verwendete Format.

`/etc/hosts`

In dieser Datei (siehe Datei 9) werden Rechnernamen IP-Adressen zugeordnet. Wird kein Nameserver verwendet, müssen hier alle Rechner aufgeführt werden, zu denen eine IP-Verbindung aufgebaut werden soll. Je Rechner wird eine Zeile bestehend aus IP-Adresse, dem voll qualifizierten Hostnamen und dem Rechnernamen (z. B. `erde`) in die Datei eingetragen. Die IP-Adresse muss am Anfang der Zeile stehen, die Einträge werden durch Leerzeichen bzw. Tabulatoren getrennt. Kommentare werden durch `#` eingeleitet.

```
127.0.0.1 localhost
192.168.0.1 sonne.kosmos.all sonne
192.168.0.20 erde.kosmos.all erde
```

Datei 9: `/etc/hosts`

`/etc/networks`

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen (siehe Datei 10).

```

loopback      127.0.0.0
localnet      192.168.0.0

```

Datei 10: `/etc/networks`

`/etc/host.conf`

Das Auflösen von Namen – d. h. das Übersetzen von Rechner- bzw. Netzwerknamen über die *resolver*-Bibliothek – wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die gegen die `libc4` oder die `libc5` gelinkt sind; für aktuelle `glibc`-Programme vgl. die Einstellungen in `/etc/nsswitch.conf`! Ein Parameter muss in einer eigenen Zeile stehen, Kommentare werden durch ``#'` eingeleitet. Die möglichen Parameter zeigt Tabelle 9.8.

| | |
|--|---|
| <code>order hosts, bind</code> | Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente sind (durch Leerzeichen oder Kommata voneinander getrennt): <i>hosts</i> : Durchsuchen der Datei <code>/etc/hosts</code> <i>bind</i> : Ansprechen eines Nameservers <i>nis</i> : Über NIS |
| <code>multi on/off</code> | Bestimmt, ob ein in <code>/etc/hosts</code> eingetragener Rechner mehrere IP-Adressen haben darf. |
| <code>nospoof on</code> <code>alert on/off</code> | Diese Parameter beeinflussen das <i>spoofing</i> des Nameservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration. |
| <code>trim</code> <code><domainname></code> | Der angegebene Domainname wird vor dem Auflösen des Rechnernamens von diesem abgeschnitten (insofern der Rechnername diesen Domainnamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei <code>/etc/hosts</code> nur Namen aus der lokalen Domain stehen, diese aber auch mit angehängtem Domainnamen erkannt werden sollen. |

Tabelle 9.8: Parameter für `/etc/host.conf`

Ein Beispiel für `/etc/host.conf` zeigt Datei 11.

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

Datei 11: `/etc/host.conf`

`/etc/nsswitch.conf`

Mit der GNU C Library 2.0 hat der „Name Service Switch“ (NSS) Einzug gehalten (vgl. Manual-Page von `nsswitch.conf` (`man 5 nsswitch.conf`), sowie ausführlicher *The GNU C Library Reference Manual*, Kap. "System Databases and Name Service Switch"; vgl. Paket `libcinfo`, Serie `doc`).

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` zeigt Datei 12. Kommentare werden durch '#' eingeleitet. Dort bedeutet z. B. der Eintrag bei der „Datenbank“ `hosts`, dass nach `/etc/hosts` (files) eine Anfrage über DNS (vgl. Abschnitt 9 auf Seite 227) losgeschickt wird.

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

Datei 12: `/etc/nsswitch.conf`

Die über NSS verfügbaren „Datenbanken“ sind in Tabelle 9.9 auf der nächsten Seite genannt. Zusätzlich sind in Zukunft `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten.

| | |
|-----------|--|
| aliases | Mail-Aliase, von sendmail(8) verwendet; vgl. Manual-Page von aliases (man 5 aliases). |
| ethers | Ethernet-Adressen. |
| group | Für Benutzergruppen, von getgrent(3) verwendet; vgl. Manual-Page von group (man 5 group). |
| hosts | Für Hostnamen und IP-Adressen, von gethostbyname(3) und ähnlichen Funktionen verwendet. |
| netgroup | Im Netzwerk gültige Liste von Hosts und Benutzern, um Zugriffsrechte zu steuern; vgl. Manual-Page von netgroup (man 5 netgroup). |
| networks | Netzwerknamen und -adressen, von getnetent(3) verwendet. |
| passwd | Benutzerpasswörter, von getpwent(3) verwendet; vgl. Manual-Page von passwd (man 5 passwd). |
| protocols | Netzwerk-Protokolle, von getprotoent(3) verwendet; vgl. Manual-Page von protocols (man 5 protocols). |
| rpc | „Remote Procedure Call“-Namen und -Adressen, von getrpcbyname(3) und ähnlichen Funktionen verwendet. |
| services | Netzwerkdienste, von getservent(3) verwendet. |
| shadow | „Shadow“-Passwörter der Benutzer, von getspnam(3) verwendet; vgl. Manual-Page von shadow (man 5 shadow). |

Tabelle 9.9: Über /etc/nsswitch.conf verfügbare Datenbanken

Die Konfigurationsmöglichkeiten der NSS-„Datenbanken“ stehen in Tabelle 9.10 auf der nächsten Seite.

| | |
|---------|--|
| files | direkt auf Dateien zugreifen, z. B. auf /etc/aliases. |
| db | über eine Datenbank zugreifen. |
| nis | NIS, vgl. Abschnitt 9 auf Seite 237. |
| nisplus | |
| dns | Nur bei hosts und networks als Erweiterung verwendbar. |

Tabelle 9.10: Fortsetzung auf der nächsten Seite...

| | |
|------------|--|
| compat | Nur bei passwd, shadow und group als Erweiterung verwendbar. |
| zusätzlich | ist es möglich, unterschiedliche Reaktionen bei bestimmten Lookup-Ergebnissen auszulösen; Details sind der Manual-Page von <code>nsswitch.conf</code> (<code>man 5 nsswitch.conf</code>) zu entnehmen. |

Tabelle 9.10: Konfigurationsmöglichkeiten der NSS-„Datenbanken“

/etc/nscd.conf

Über diese Datei wird der `nscd` (engl. *Name Service Cache Daemon*) konfiguriert (vgl. Manual-Page von `nscd` (`man 8 nscd`) und Manual-Page von `nscd.conf` (`man 5 nscd.conf`)). Betroffen sind die Informationen von `passwd` und `groups`. `hosts` wird nicht eingelesen, damit der Daemon nicht neu gestartet werden muss, wenn z. B. die Namensauflösung (DNS) durch Änderung der `/etc/resolv.conf` umgestellt wird.

Wenn beispielsweise das Caching für `passwd` aktiviert ist, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten des `nscd` kann diese Wartezeit verkürzt werden:

```
erde:~ # rcnscd restart
```

/etc/resolv.conf

Wie bereits die Datei `/etc/host.conf`, so spielt auch diese Datei in Bezug auf Auflösung von Rechnernamen durch die *resolver*-Bibliothek eine Rolle.

In dieser Datei wird angegeben, welcher Domain der Rechner angehört (Schlüsselwort `search`) und wie die Adresse des Nameservers ist (Schlüsselwort `nameserver`), der angesprochen werden soll. Es können mehrere Domainnamen angegeben werden. Beim Auflösen eines nicht voll qualifizierten Namens wird versucht, durch Anhängen der einzelnen Einträge in `search` einen gültigen, voll qualifizierten Namen zu erzeugen. Mehrere Nameserver können durch mehrere Zeilen, die mit `nameserver` beginnen, bekannt gemacht werden. Kommentare werden wieder mit ``#'` eingeleitet.

Ein Beispiel für `/etc/resolv.conf` zeigt Datei [13](#).

```
# Our domain
```

```
search kosmos.all
#
# We use sonne (192.168.0.1) as nameserver
nameserver 192.168.0.1
```

Datei 13: /etc/resolv.conf

YaST trägt hier den angegebenen Nameserver ein!

Einige Dienste wie pppd (wvdial), ipppd (isdn), dhcp (dhcpcd und dhclient), pcmcia und hotplug modifizieren die Datei /etc/resolv.conf über das Skript `modify_resolvconf`.

Wenn die Datei /etc/resolv.conf durch dieses Skript vorübergehend modifiziert wurde, enthält sie einen definierten Kommentar, der Auskunft darüber gibt, welcher Dienst sie modifiziert hat, wo die ursprüngliche Datei gesichert ist und wie man die automatischen Modifikationen abstellen kann.

Wenn /etc/resolv.conf mehrmals modifiziert wird, wird diese Verschachtelung von Modifikationen auch dann wieder sauber abgebaut, wenn sie in einer anderen Reihenfolge zurückgenommen werden; dies kann bei isdn, pcmcia und hotplug durchaus vorkommen.

Wenn ein Dienst nicht sauber beendet wurde, kann mit Hilfe des Skripts `modify_resolvconf` der Ursprungszustand wiederhergestellt werden. Beim Booten wird geprüft, ob eine modifizierte `resolv.conf` stehen geblieben ist (z. B. wegen Systemabsturz). Dann wird die ursprüngliche (unmodifizierte) `resolv.conf` wiederhergestellt.

YaST findet mittels `modify_resolvconf check` heraus, ob `resolv.conf` modifiziert wurde, und dann den Benutzer warnen, dass seine Änderungen nach der Restauration wieder verloren sein werden. Ansonsten verwendet YaST `modify_resolvconf` nicht, das heißt eine Änderung der Datei `resolv.conf` mittels YaST und eine manuelle Änderung sind äquivalent. Beides entspricht einer gezielten und dauerhaften Änderung, während eine Änderung durch einen der genannten Dienste nur vorübergehend ist.

/etc/HOSTNAME

Hier steht der Name des Rechners, also nur der Hostname ohne den Domainnamen. Diese Datei wird von verschiedenen Skripten während des Starts des Rechners gelesen. Sie darf nur eine Zeile enthalten, in der der Rechnername steht!

Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die während des Hochfahrens des Rechners die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Multiuser-Runlevel* übergeht (vgl. Tabelle 9.11).

| | |
|------------------------------------|---|
| <code>/etc/init.d/network</code> | Dieses Skript übernimmt die Konfiguration der Netzwerk Hard- und Software während der Startphase des Systems. |
| <code>/etc/init.d/inetd</code> | Startet den <code>inetd</code> . Dies ist beispielsweise dann nötig, wenn Sie sich vom Netzwerk aus auf diese Maschine einloggen möchten. |
| <code>/etc/init.d/portmap</code> | Startet den Portmapper, der benötigt wird, um RPC-Server verwenden zu können, wie z. B. einen NFS-Server. |
| <code>/etc/init.d/nfsserver</code> | Startet den NFS-Server. |
| <code>/etc/init.d/sendmail</code> | Kontrolliert den <code>sendmail</code> -Prozess. |
| <code>/etc/init.d/ypserv</code> | Startet den NIS-Server. |
| <code>/etc/init.d/ypbind</code> | Startet den NIS-Client. |

Tabelle 9.11: Einige Startup-Skripten der Netzwerkprogramme

Routing unter SuSE Linux Desktop

Ab SuSE Linux Desktop 8.0 wird die Routing-Tabelle in den Konfigurationsdateien `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*` eingestellt.

In der Datei `/etc/sysconfig/network/routes` können alle statischen Routen eingetragen werden, die für die verschiedenen Aufgaben eines Systems benötigt werden könnten: Route zu einem Rechner, Route zu einem Rechner über ein Gateway und Route zu einem Netzwerk.

Für alle Interfaces, die individuelles Routing benötigen, kann dies jeweils in einer eigenen Datei pro Interface definiert werden: `/etc/sysconfig/network/ifroute-*`. Für das Zeichen ``*`` muss die Interface-Bezeichnung eingesetzt werden. Die Einträge können folgendermaßen aussehen:

```
DESTINATION      GATEWAY NETMASK  INTERFACE [ TYPE ] [ OPTIONS ]
```

```

DESTINATION          GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -          INTERFACE [ TYPE ] [ OPTIONS ]

```

Falls GATEWAY, NETMASK, PREFIXLEN oder INTERFACE nicht angegeben werden, muss an ihrer Stelle das Zeichen '-' gesetzt werden. Die Einträge TYPE und OPTIONS können schlicht entfallen.

- In der ersten Spalte steht das Ziel einer Route. Dabei kann dort die IP-Adresse eines Netzes oder Rechners oder bei *erreichbaren* Nameservern auch der voll qualifizierte Name eines Netzes oder eines Rechners stehen.
- Die zweite Spalte enthält entweder das Default-Gateway oder ein Gateway, hinter dem ein Rechner oder Netzwerk erreichbar ist.
- Die dritte Spalte enthält die Netzmaske für Netzwerke oder Rechner hinter einem Gateway. Für Rechner hinter einem Gateway lautet die Maske z. B. 255.255.255.255.
- Die letzte Spalte ist nur für die am lokalen Rechner angeschlossenen Netzwerke (Loopback, Ethernet, ISDN, PPP, ...) wichtig. Hier muss der Name des Devices eingetragen werden.

Folgende Skripten im Verzeichnis `/etc/sysconfig/network/scripts/` erleichtern den Umgang mit Routen:

ifup-route setzt eine Route,

ifdown-route deaktiviert eine Route,

ifstatus-route gibt den Status der konfigurierten Routen an.

DNS – Domain Name Service

DNS (engl. *Domain Name Service*) wird benötigt, um die Domain- und Rechnernamen in IP-Adressen aufzulösen. Bevor Sie einen eigenen Nameserver einrichten, sollten Sie die allgemeinen Informationen zu DNS im Abschnitt 9 auf Seite 209 lesen.

Nameserver BIND starten

Der Nameserver BIND ist auf SuSE Linux bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann.

Hat man bereits eine funktionsfähige Internetverbindung und trägt in der `/etc/resolv.conf` als Nameserver 127.0.0.1 für localhost ein, hat man in der Regel schon eine funktionierende Namensauflösung, ohne dass man den DNS des Providers kennt. BIND führt so die Namensauflösung über die Root-Nameserver durch, was aber merklich langsamer ist. Normalerweise sollte man den DNS des Providers mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` eintragen, um eine effektive und sichere Namensauflösung zu erhalten. Funktioniert das soweit, läuft der Nameserver als reiner „Caching-only“-Nameserver. Erst wenn man ihm eigene Zonen bereitstellt, wird er ein richtiger DNS werden. Ein einfaches Beispiel dafür, findet man im Doku-Verzeichnis: `/usr/share/doc/packages/bind8/sample-config`.

Man sollte allerdings keine offizielle Domain aufsetzen, solange man diese nicht von der zuständigen Institution – für '.de' ist das die DENIC eG – zugewiesen bekommen hat. Auch wenn man eine eigene Domain hat, diese aber vom Provider verwaltet wird, sollte man diese besser nicht verwenden, da BIND sonst keine Anfragen für diese Domain mehr forwarden würde und so z. B. der Webserver beim Provider für die eigene Domain nicht mehr erreichbar wäre.

Um den Nameserver zu starten gibt man auf der Kommandozeile (als root)

```
rcnamed start
```

ein. Erscheint rechts in grün „done“, ist der named, so heißt der Nameserver-Prozess, erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit des Nameservers sofort testen, indem man die Programme `host` oder `dig` verwendet. Als Default Server muss localhost mit der Adresse 127.0.0.1 angezeigt werden. Sollte das nicht der Fall sein, steht wahrscheinlich in der `/etc/resolv.conf` ein falscher Nameserver oder diese Datei existiert gar nicht. Für einen ersten Test gibt man `host 127.0.0.1` ein, das sollte immer

funktionieren; erhält man eine Fehlermeldung, sollte man mit folgendem Kommando überprüfen, ob der `named` überhaupt läuft

```
rcnamed status
```

Falls der Nameserver nicht startet oder ein fehlerhaftes Verhalten zeigt, findet man die Ursache in den meisten Fällen in „`/var/log/messages`“ protokolliert.

Hat man eine Wählverbindung, muss man beachten, dass BIND8 beim Starten die Root-Nameserver überprüfen will. Gelingt ihm das nicht, weil keine Internetverbindung zustande kommt, kann das dazu führen, dass überhaupt keine DNS-Anfragen außer für lokal definierte Zonen aufgelöst werden können. BIND9 verhält sich da anders, benötigt aber ein Mehrfaches an Ressourcen im Vergleich zu BIND8.

Um den Nameserver des Providers, oder einen eigenen, den man schon im eigenen Netz laufen hat, als „`forwarder`“ zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt `options` unter `forwarders` ein; vgl. Beispiel 14.

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.0.99; };
    allow-query { 127/8; 192.168.0/24; };
    notify no;
};
```

Datei 14: Forwarding-Optionen in `named.conf`

Die im Beispiel verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten eingetragen werden.

Nach den `options` folgen dann die Einträge für die Zonen, die Einträge für „`localhost`“, „`0.0.127.in-addr.arpa`“, sowie „`;`“ vom „`type hint`“ sollten mindestens immer vorhanden sein. Die zugehörigen Dateien müssen nicht verändert werden, da sie so funktionieren wie sie sind. Beachten muss man auch, dass nach jedem Eintrag ein „`;`“ steht und die geschweiften Klammern korrekt gesetzt sind. Hat man nun Änderungen an der Konfigurationsdatei `/etc/named.conf` oder an den Zonen-Dateien vorgenommen, muss man BIND dazu bringen diese neu einzulesen. Das gelingt mit dem Kommando `rcnamed reload`. Alternativ kann man den Nameserver auch komplett neu starten, durch den Befehl `rcnamed restart`. Fehlt nur noch das Kommando, um den Nameserver wieder zu beenden: `rcnamed stop`.

Die Konfigurationsdatei `/etc/named.conf`

Alle Einstellungen zum Nameserver BIND8 bzw. BIND9 sind in der Datei `/etc/named.conf` vorzunehmen. Die Zonendaten selbst, die Rechnernamen, IP-Adressen usw. für die zu verwaltenden Domains, sind in separaten Dateien im Verzeichnis `/var/lib/named` abzulegen, dazu aber unten mehr.

Die `/etc/named.conf` unterteilt sich grob in zwei Bereiche, zum einen der Abschnitt `options` für allgemeine Einstellungen und zum anderen die `zone`-Einträge für die einzelnen Domains. Außerdem kann man noch einen Bereich `logging`, sowie Einträge vom Typ `acl` definieren. Kommentarzeilen beginnen mit einem ``#'`-Zeichen, alternativ ist ``//'` auch erlaubt.

Eine minimalistische `/etc/named.conf` stellt Beispiel 15 dar.

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};
```

Datei 15: Minimalistische Datei `/etc/named.conf`

Dieses Beispiel funktioniert für Bind8 und Bind9 gleichermaßen, da keine speziellen Optionen verwendet werden, die nur von einer Version verstanden werden. Bind9 akzeptiert alle Bind8-Konfigurationen und vermerkt allenfalls beim Start, wenn eine Option nicht implementiert ist. Spezielle Bind9-Optionen werden vom Bind8 aber nicht unterstützt.

Die wichtigsten Konfigurationsoptionen im Abschnitt `options`

directory "/var/lib/named"; gibt das Verzeichnis an, in dem der BIND die Dateien mit den Zonendaten findet,

forwarders { 10.0.0.1; }; verwendet man, um den oder die Nameserver (meist des Providers) anzugeben, an den oder die DNS-Anfragen weitergereicht werden, die nicht direkt beantwortet werden können.

forward first; bewirkt, dass die DNS-Anfragen zu erst geforwarded werden, bevor versucht wird diese über die Root-Nameserver aufzulösen. Anstelle von `forward first` kann man auch `forward only` schreiben, dann werden alle Anfragen weitergeleitet und die Root-Nameserver werden gar nicht mehr angesprochen. Das kann für Firewall-Konfigurationen sinnvoll sein.

listen-on port 53 { 127.0.0.1; 192.168.0.1; }; sagt dem BIND, auf welchen Netzwerkinterfaces und welchem Port er auf Anfragen der Clients horcht. Die Angabe `port 53` kann man sich dabei sparen, da 53 ohnehin der Standardport ist. Lässt man diesen Eintrag komplett weg, werden standardmäßig alle Interfaces verwendet

query-source address * port 53; Dieser Eintrag kann notwendig sein, wenn eine Firewall die externen DNS-Abfragen blockiert. So wird BIND dazu gebracht, Anfragen nach außen von Port 53 aus und nicht von den hohen Ports > 1024 zu stellen.

allow-query { 127.0.0.1; 192.168.1/24; }; bestimmt die Netze aus denen Clients DNS-Anfragen stellen dürfen. Das /24 ist dabei eine Kurzschreibweise für die Netzmaske, in diesem Fall 255.255.255.0.

allow-transfer { ! *; }; regelt welche Rechner Zonentransfers anfordern dürfen, dieses Beispiel unterbindet sie, aufgrund des ! * komplett. Ohne diesen Eintrag können Zonentransfers ohne Einschränkungen von überall angefordert werden.

statistics-interval 0; Ohne diesen Eintrag produziert Bind8 stündlich mehrere Zeilen Statistikmeldungen in `/var/log/messages`. Die Angabe von 0 bewirkt, dass diese komplett unterdrückt werden, ansonsten kann man hier die Zeit in Minuten angeben.

cleaning-interval 720; Diese Option legt fest, in welchem Zeitabstand Bind8 seinen Cache aufräumt. Die Aktivität führt jedes Mal zu einem Eintrag in `/var/log/messages`. Die Zeitangabe erfolgt in Minuten. Voreingestellt sind 60 Minuten.

interface-interval 0; Bind8 durchsucht regelmäßig die Netzwerkschnittstellen nach neuen oder nicht mehr vorhandenen Interfaces. Setzt man diesen Wert auf 0, so wird darauf verzichtet und Bind8 lauscht nur auf den beim Start gefundenen Interfaces. Alternativ kann man das Intervall in Minuten angeben. Voreingestellt sind 60 Minuten.

notify no; Das no bewirkt, dass keine anderen Nameserver benachrichtigt werden, wenn an den Zonendaten Änderungen vorgenommen werden oder der Nameserver neu gestartet wird.

Der Konfigurationsabschnitt Logging

Was und wie wohin mitprotokolliert wird, kann man beim Bind8 recht vielseitig konfigurieren. Normalerweise sollte man mit den Voreinstellungen zufrieden sein können. Beispiel 16 zeigt die einfachste Form so eines Eintrages und unterdrückt das „Logging“ komplett

```
logging {  
    category default { null; };  
};
```

Datei 16: Logging wird unterdrückt

Aufbau der Zonen-Einträge

Nach zone wird der Name der zu verwaltenden Domain angegeben, hier willkürlich meine-domain.de gefolgt von einem in und einem in geschweiften Klammern gesetzten Block zugehöriger Optionen; vgl. Datei 17.

```
zone "meine-domain.de" in {  
    type master;  
    file "meine-domain.zone";  
    notify no;  
};
```

Datei 17: Zone-Eintrag für meine-domain.de

Will man eine „Slave-Zone“ definieren, ändert sich nur der `type` auf `slave` und es muss ein Nameserver angegeben werden, der diese Zone als `master` verwaltet (kann aber auch ein „slave“ sein); vgl. Datei 18.

```
zone "andere-domain.de" in {  
    type slave;  
    file "slave/andere-domain.zone";  
    masters { 10.0.0.1; };  
};
```

Datei 18: Zone-Eintrag für andere-domain.de

Die Optionen:

type master; Das `master` legt fest, dass diese Zone auf diesem Nameserver verwaltet wird. Das setzt eine sauber erstellte Zonendatei voraus.

type slave; Diese Zone wird von einem anderen Nameserver transferiert. Muss zusammen mit `masters` verwendet werden.

type hint; Die Zone `.` vom Typ `hint` wird für die Angabe der Root-Nameserver verwendet. Diese Zonendefinition kann man unverändert lassen.

file „meine-domain.zone“ oder file „slave/andere-domain.zone“; Dieser Eintrag gibt die Datei an, in der die Zonendaten für die Domain eingetragen sind. Bei einem `slave` braucht die Datei nicht zu existieren, da ihr Inhalt von einem anderen Nameserver geholt wird. Um Master- und Slave-Dateien auseinander zu halten, gibt man für die Slave-Dateien das Verzeichnis `slave` an.

masters { 10.0.0.1; }; Diesen Eintrag braucht man nur für Slave-Zonen und er gibt an, von welchem Nameserver die Zonendatei transferiert werden soll.

allow-update { ! *; }; diese Option regelt den Schreibzugriff von extern auf die Zonendaten. Damit wäre es Clients möglich, sich selbst im DNS einzutragen, was aus Sicherheitsgründen nicht wünschenswert ist. Ohne diesen Eintrag, sind Zonen-Updates generell untersagt, dieses Beispiel würde daran auch nichts ändern, da `! *` ebenfalls alles verbietet.

Aufbau der Zonendateien

Man benötigt zwei Arten von Zonen-Dateien, die einen dienen dazu, einem Rechnernamen die IP-Adresse zu zuordnen und die anderen gehen den umgekehrten Weg und liefern zu einer gegebenen IP-Adresse den Rechnernamen.

Eine wichtige Bedeutung hat der '.' in den Zonendateien. Werden Rechnernamen, ohne abschließenden '.' angegeben, wird immer die Zone ergänzt. Man muss also komplette Rechnernamen, die bereits mit vollständiger Domain angegeben wurden, mit einem '.' abschließen, damit die Domain nicht noch einmal dran gehängt wird. Ein fehlender Punkt oder einer an der falschen Stelle, dürfte die häufigste Fehlerursache bei der Konfiguration von Nameservern sein.

Den ersten Fall betrachten wir an der Zonen-Datei `welt.zone`, die für die Domain `welt.all` zuständig ist; vgl. Datei 19.

```

1. $TTL 2D
2.  welt.all.      IN SOA      gateway root.welt.all. (
3.                  2001040901 ; serial
4.                  1D        ; refresh
5.                  2H        ; retry
6.                  1W        ; expiry
7.                  2D )      ; minimum
8.
9.                  IN NS      gateway
10.                 IN MX      10 sonne
11.
12. gateway        IN A        192.168.0.1
13.                IN A        192.168.1.1
14. sonne           IN A        192.168.0.2
15. mond            IN A        192.168.0.3
16. erde            IN A        192.168.1.2
17. mars            IN A        192.168.1.3

```

Datei 19: Datei `/var/lib/named/welt.zone`

Zeile 1: `$TTL` definiert die Standard-TTL, die für alle Einträge in dieser Datei gilt, hier 2 Tage (2D = 2 days). TTL bedeutet hier „time to live“, zu deutsch Gültigkeitsdauer.

Zeile 2: Hier beginnt der SOA control record:

- An erster Stelle steht hier der Name der zu verwaltenden Domain `welt.all`, diese ist mit einem '.' abgeschlossen, da ansonsten die

Zone noch einmal angehängt würde. Alternativ kann man hier ein '@' schreiben, dann wird die Zone dem zugehörigen Eintrag in der /etc/named.conf entnommen.

- Nach dem IN SOA steht der Name des Nameservers, der als Master für diese Zone zuständig ist. In diesem Fall wird der Name gateway zu gateway.welt.all ergänzt, da er nicht mit einem '.' abgeschlossen ist.
- Danach folgt eine E-Mail-Adresse, der für diesen Nameserver zuständigen Person. Da das '@'-Zeichen bereits eine besondere Bedeutung hat, ist hier stattdessen einfach ein '.' einzutragen, für root@welt.all schreibt man hier folglich root.welt.all.. Den '.' am Ende darf man hier nicht vergessen, da sonst die Zone noch angehängt würde.
- Am Ende folgt eine '(' , um die folgenden Zeilen, bis zur ')' mit in den SOA-Record einzuschließen.

Zeile 3: Die serial number ist eine willkürliche Zahl, die bei jeder Änderung an dieser Datei erhöht werden sollte. Sie wird benötigt, um sekundäre Nameserver (Slave-Server) über Änderungen zu informieren. Eingebürgert hat sich dafür eine zehnstellige Zahl aus Datum und fortlaufender Nummer in der Form JJJJMMTTNN.

Zeile 4: Die refresh rate gibt das Zeitintervall an, in dem Sekundär-Nameserver die serial number der Zone überprüfen. In diesem Fall 1 Tag (1D = 1 day).

Zeile 5: Die retry rate gibt den Zeitabstand an, in dem ein sekundärer Nameserver, im Fehlerfall versucht den primären Server erneut zu kontaktieren. Hier 2 Stunden (2H = 2 hours).

Zeile 6: Die expiration time gibt den Zeitraum an, nachdem ein sekundärer Nameserver die gecachelten Daten verwirft, wenn er keinen Kontakt zum primären Server mehr bekommen hat. Hier ist das eine Woche (1W = 1 week).

Zeile 7: Die minimum time to live sagt aus, wie lange die Ergebnisse von DNS-Anfragen von anderen Servern gecached werden dürfen, bevor sie ihre Gültigkeit verlieren und neu angefragt werden müssen.

Zeile 9: Das IN NS gibt den Nameserver an, der für diese Domain zuständig ist. Auch hier gilt, dass gateway wieder zu gateway.welt.all ergänzt wird, weil es nicht mit einem '.' abgeschlossen ist. Es kann

mehrere Zeilen dieser Art geben, eine für den primären und jeweils eine für jeden sekundären Nameserver. Ist für diese Zone `notify` in der `/etc/named.conf` nicht auf `no` gesetzt, werden alle hier aufgeführten Nameserver über Änderungen der Zonendaten informiert.

Zeile 10: Der MX-Record gibt den Mailserver an, der für die Domain `welt.all` die Mails annimmt und weiterverarbeitet oder weiterleitet. In diesem Beispiel ist das der Rechner `sonne.welt.all`. Die Zahl vor dem Rechnernamen ist der Präferenz-Wert, gibt es mehrere MX-Einträge, wird zuerst der Mailserver mit dem kleinsten Wert genommen und falls die Auslieferung an diesen scheitert, wird der mit dem nächst höheren Wert versucht.

Zeile 12-17: Das sind jetzt die eigentlichen Adress-Records, in denen den Rechnernamen eine oder mehrere IP-Adressen zugeordnet werden. Die Namen stehen hier ohne abschließenden `.`, da sie ohne angehängte Domain eingetragen sind und alle um `welt.all` ergänzt werden dürfen. Dem Rechner `gateway` sind zwei IP-Adressen zugeordnet, da er über zwei Netzwerkkarten verfügt.

Für die Rückwärts-Auflösung (reverse lookup) von IP-Adressen in Rechnernamen wird die Pseudo-Domain `in-addr.arpa` zu Hilfe genommen. Diese wird dazu an den in umgedrehter Reihenfolge geschriebenen Netzanteil angehängt. Aus `192.168.1` wird dann `1.168.192.in-addr.arpa`; vgl. 20.

```

1. $TTL 2D
2. 1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
3.                               2001040901      ; serial
4.                               1D              ; refresh
5.                               2H              ; retry
6.                               1W              ; expiry
7.                               2D )            ; minimum
8.
9.                               IN NS          gateway.welt.all.
10.
11. 1                             IN PTR        gateway.welt.all.
12. 2                             IN PTR        erde.welt.all.
13. 3                             IN PTR        mars.welt.all.
```

Datei 20: Umgekehrte Adress-Auflösung

Zeile 1: `$TTL` definiert die Standard-TTL, die hier für alle Einträge gilt.

Zeile 2: Der 'revers lookup' soll mit dieser Datei für das Netz 192.168.1.0 ermöglicht werden. Da die Zone hier '1.168.192.in-addr.arpa' heißt, will man dies natürlich nicht an die Rechnernamen anhängen, deshalb sind diese alle komplett mit Domain und abschließendem '.' eingetragen. Der Rest entspricht dem, was im vorangegangenen Beispiel für "welt.all", bereits beschrieben wurde.

Zeile 3-7: Siehe vorangegangenes Beispiel für "welt.all".

Zeile 9: Diese Zeile gibt auch hier wieder den Nameserver an, der für diese Zone zuständig ist, diesmal wird aber der Name komplett mit Domain und abschließendem '.' hier eingetragen.

Zeile 11-13: Das sind die Pointer-Records, die zu einer IP-Adresse auf den zugehörigen Rechnernamen zeigen. Hier steht am Anfang der Zeile nur die letzte Stelle der IP-Adresse, ohne abschließenden '.'. Wird jetzt die Zone daran angehängt und man denkt sich das '.in-addr.arpa' weg, hat man die komplette IP-Adresse in verdrehter Reihenfolge.

Die Zonendateien sind in dieser Form für Bind8 und Bind9 gleichermaßen verwendbar. Auch Zonentransfers zwischen den verschiedenen Versionen sollten normalerweise kein Problem darstellen.

Weitere Informationen

- Dokumentation zum Paket bind8: `file:/usr/share/doc/packages/bind8/html/index.html`.
- Eine Beispielkonfiguration findet man unter:
`/usr/share/doc/packages/bind8/sample-config`
- Manual-Page von named (man 8 named), in der die einschlägigen RFCs genannt werden, sowie besonders die Manual-Page von named.conf (man 5 named.conf).

NIS – Network Information Service

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonisieren. Das Netzwerk soll für den Anwender transparent sein. Egal welcher Rechner, der Anwender findet immer die gleiche Umgebung vor. Möglich wird dies durch die Dienste NIS und NFS. NFS dient der Verteilung von Dateisystemen im Netz und wird in Abschnitt *NFS – verteilte Dateisysteme* auf Seite 242 beschrieben.

NIS (engl. *Network Information Service*) kann als Datenbankdienst verstanden werden, der Zugriff auf Informationen aus den Dateien `/etc/passwd`, `/etc/shadow` oder `/etc/group` netzwerkweit ermöglicht. NIS kann auch für weitergehende Aufgaben eingesetzt werden (z. B. für `/etc/hosts` oder `/etc/services`). Darauf soll hier jedoch nicht im Detail eingegangen werden. Für NIS wird vielfach synonym der Begriff 'YP' verwendet. Dieser leitet sich ab von den *yellow pages*, also den *gelben Seiten* im Netz.

NIS-Master- und -Slave-Server

Zur Installation wählen Sie in YaST2 'Netzwerk/Erweitert' und dort 'NIS-Server konfigurieren'.

Wenn in Ihrem Netzwerk bisher noch kein NIS-Server existiert, müssen Sie in der nächsten Maske den Punkt 'NIS Master Server einrichten' aktivieren. Falls Sie schon einen NIS-Server (also einen „Master“) haben, können Sie (z. B. wenn Sie ein neues Subnetz einrichten) einen NIS Slave Server hinzufügen. Als Erstes wird die Konfiguration des Master-Servers erläutert. In der ersten Konfigurationsmaske (Abb. 9.4 auf der nächsten Seite) geben Sie oben den Domainnamen ein. In der Checkbox darunter können Sie festlegen, ob der Rechner auch ein NIS-Client werden soll, also ob sich darauf auch User einloggen können, die dann ebenfalls die Daten von dem NIS-Server erhalten.

Wollen Sie später weitere NIS-Server („Slave-Server“) in Ihrem Netzwerk einrichten, müssen Sie die Box 'Aktiver Slave-Server für NIS vorhanden' aktivieren. Zusätzlich sollten Sie dann auch die 'Schnelle Map-Verteilung' aktivieren, die bewirkt, dass die Datenbankeinträge sehr schnell vom Master auf die Slave-Server übertragen werden.

Wollen Sie den Nutzern in Ihrem Netzwerk erlauben, dass sie Ihre Passwörter ändern können (mit dem Befehl `yppasswd`, also nicht nur die lokalen, sondern die, die auf dem NIS-Server abgelegt sind), können Sie das hier ebenfalls aktivieren. Dann werden auch die Checkboxes 'Ändern des GECOS-Eintrags zulassen' und 'Ändern des SHELL-Eintrags zulassen' aktiv. „GECOS“ bedeutet,

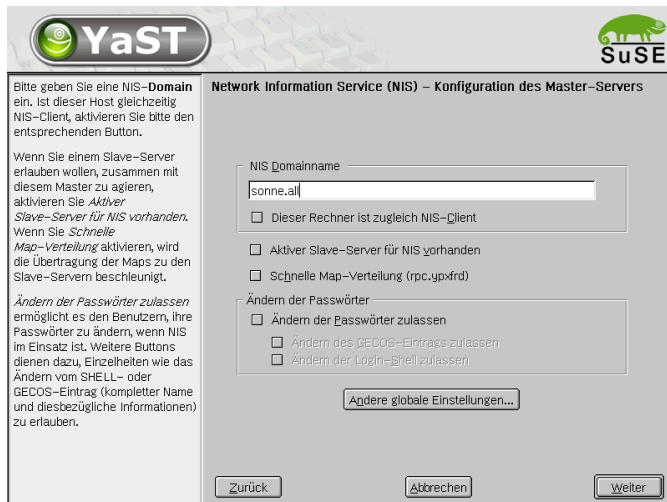


Abbildung 9.4: YaST2: NIS-Server Konfigurationstool

der User kann auch seine Namens- und Adresseinstellungen ändern (mit dem Befehl `ypchfn`). „SHELL“ heißt, er darf auch seine standardmäßig eingetragene Shell ändern (mit dem Befehl `ypchsh`, z. B. von `bash` zu `sh`).

Unter 'Ändere globale Einstellungen...' erscheint ein Menü (Abb. 9.5 auf der nächsten Seite), in dem man das Standardverzeichnis (`/etc`) ändern kann. Zusätzlich kann man hier noch Passwörter und Gruppen zusammenführen. Die Einstellung sollte man auf 'Ja' belassen, damit die jeweiligen Dateien (`/etc/passwd` und `/etc/shadow` bzw. `/etc/group` und `/etc/gshadow`) aufeinander abgestimmt werden. Zusätzlich kann noch die jeweils kleinste Benutzer- und Gruppenkennung festgelegt werden. Mit 'OK' kommen Sie wieder in die vorige Maske zurück. Klicken Sie nun auf 'Weiter'.

Haben Sie vorher 'Aktiver Slave-Server für NIS vorhanden' aktiviert, müssen Sie nun die Namen der Rechner angeben, die als Slaves fungieren sollen. Legen Sie die Namen fest und gehen Sie auf 'Weiter'. Das folgende Menü erreichen Sie auch direkt, wenn Sie vorher die Einstellung für die Slave-Server nicht aktiviert haben. Nun können die „Maps“, d. h. die Teildatenbanken, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die Voreinstellungen hier sind für die meisten Fälle sehr sinnvoll. Daher sollten Sie im Normalfall hier nichts ändern. Falls Sie hier doch Änderungen vornehmen wollen, sollten Sie sich in der Materie sehr gut auskennen.

Mit 'Weiter' kommen Sie in den letzten Dialog, in dem festgelegt werden kann,

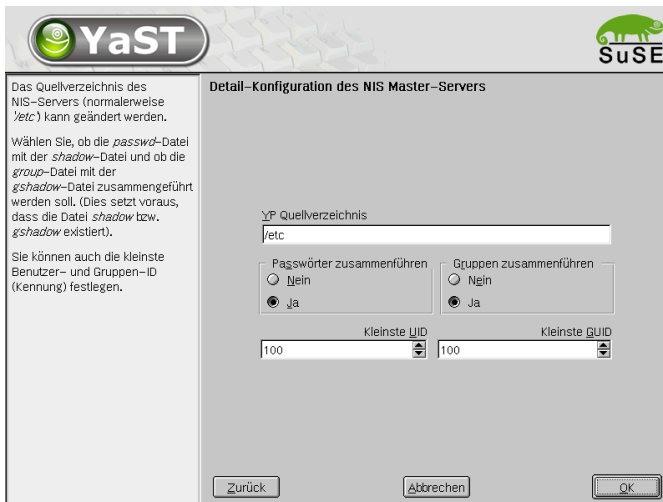


Abbildung 9.5: YaST2: NIS-Server: Verzeichnis ändern und Dateien synchronisieren

welche Netzwerke Anfragen an den NIS-Server stellen dürfen (siehe Abb. 9.6 auf der nächsten Seite). Normalerweise wird das Ihr Firmennetzwerk sein. Dann sollten die beiden Eintragungen

```
255.0.0.0 127.0.0.0
0.0.0.0 0.0.0.0
```

hier stehen. Die erste erlaubt Verbindungen vom eigenen Rechner, die zweite ermöglicht allen Rechnern, die Zugriff auf das Netzwerk haben, Anfragen an den Server.

Das NIS-Client-Modul im YaST2

Mit diesem Modul können Sie sehr einfach den NIS-Client konfigurieren. Im Startfenster geben Sie an, dass Sie NIS benutzen möchten. Im folgenden Dialog können Sie dann die NIS-Domain und die IP-Nummer des NIS-Servers angeben. Mit der 'Broadcast'-Checkbox ermöglichen Sie die Suche nach einem NIS-Server im Netzwerk, wenn der angegebene Server nicht antwortet. Sie haben auch die Möglichkeit, multiple Domains mit einer Default-Domain anzugeben. Für die einzelnen Domains können Sie wiederum mit 'Hinzufügen' mehrere Server einschließlich Broadcast-Funktion angeben.

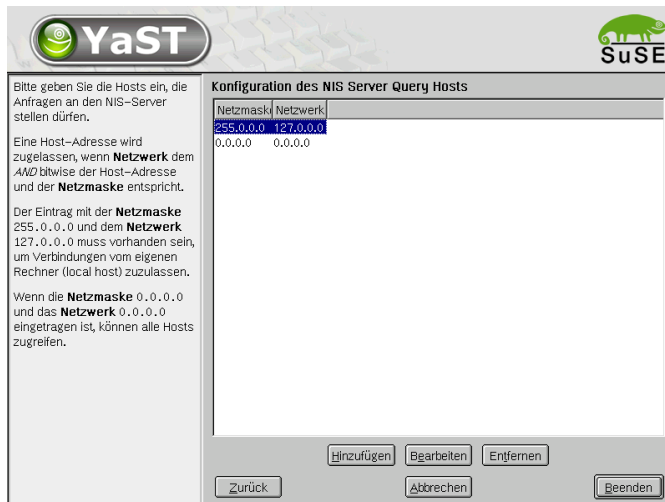


Abbildung 9.6: YaST2: NIS-Server: Festlegung der Anfrageerlaubnis

Manuelles Einrichten eines NIS-Clients

Im Paket `ypbind`, befinden sich alle notwendigen Programme zum Einrichten eines NIS-Clients. Folgende Schritte sind notwendig:

- Setzen Sie die NIS-Domain in der Datei `/etc/defaultdomain` Der NIS-Domainname ist nicht zu verwechseln mit dem DNS-Domainnamen. Diese können gleich lauten, haben jedoch grundsätzlich nichts miteinander zu tun!
- Der Name des NIS-Server wird in der Datei `/etc/yp.conf` eingetragen:

```
ypserver 192.168.0.1
```
- Der Name des NIS-Servers (z. B. `sonne.kosmos.all`) muss über `/etc/hosts` auflösbar sein.
- NIS wird über RPC (engl. *Remote Procedure Calls*) realisiert, deshalb ist es Bedingung, dass der RPC-Portmapper läuft. Gestartet wird dieser Server vom Skript `/etc/init.d/portmap`.

- Ergänzen der Einträge in `/etc/passwd` und `/etc/group`. Damit nach dem Durchsuchen der lokalen Dateien eine Anfrage beim NIS-Server gemacht wird, müssen die entsprechenden Dateien durch eine Zeile, die mit einem Pluszeichen ('+') beginnt, ergänzt werden.
- NIS erlaubt es, eine Menge weiterer Optionen in der Datei `/etc/sysconfig/ypbind` zu aktivieren.
- Der letzte Schritt des Aufsetzens des NIS-Clients besteht aus dem Start des Programmes `ypbind` und damit des eigentlichen NIS-Clients.
- Entweder muss nun das System neu gestartet werden oder die benötigten Dienste werden durch folgende Befehle neu gestartet:

```
erde: # rcnetwork restart
erde: # rcypbind restart
```

NFS – verteilte Dateisysteme

Wie bereits in Abschnitt *NIS – Network Information Service* auf Seite 237 erwähnt, dient NFS neben NIS dazu, ein Netzwerk für Anwender transparent zu machen. Durch NFS lassen sich Dateisysteme im Netz verteilen. Unabhängig davon, an welchem Rechner im Netz ein Anwender arbeitet, findet er so stets die gleiche Umgebung vor.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS-Server und NFS-Clients. Allerdings kann ein Rechner beides sein, d. h. gleichzeitig Dateisysteme dem Netz zur Verfügung stellen („exportieren“) und Dateisysteme anderer Rechner mounten („importieren“). Im Regelfall jedoch benutzt man dafür Server mit großer Festplattenkapazität, deren Dateisysteme von Clients gemountet werden.

Importieren von Dateisystemen mit YaST2

Jeder Benutzer (der die Rechte dazu erteilt bekommt), kann NFS-Verzeichnisse von NFS-Servern in seinen eigenen Dateibaum einhängen. Dies lässt sich am einfachsten mit dem Modul ‘NFS-Client’ in YaST2 erledigen. Dort muss lediglich der Hostname des als NFS-Server fungierenden Rechners eingetragen werden, das Verzeichnis, das von dem Server exportiert wird und den Mountpunkt, unter dem es auf dem eigenen Computer eingehängt werden soll. Wählen Sie dazu im ersten Dialogfenster ‘Hinzufügen’ und tragen Sie dann die genannten Angaben ein (s. Abb. 9.7).



Hostname des NFS-Servers:
server.mylan.de Wählen

Entferntes Dateisystem: /homedirs
Mountpunkt (lokal): /myhome Durchsuchen

Optionen:
defaults

OK Verwerfen Hilfe

Abbildung 9.7: Konfiguration des NFS-Clients

Manuelles Importieren von Dateisystemen

Dateisysteme von einem NFS-Server zu importieren, ist sehr einfach. Einzige Voraussetzung ist, dass der RPC-Portmapper gestartet wurde. Das Starten dieses Servers wurde bereits im Zusammenhang mit NIS besprochen (siehe Abschnitt *Manuelles Einrichten eines NIS-Clients* auf Seite 240). Ist diese Voraussetzung erfüllt, können fremde Dateisysteme, sofern sie von den entsprechenden Maschinen exportiert werden, analog zu lokalen Platten mit dem Befehl `mount` in das Dateisystem eingebunden werden. Die Syntax ist wie folgt:

```
mount -t nfs <Rechner>:<Remote-Pfad> <Lokaler-Pfad>
```

Sollen also z. B. die Benutzerverzeichnisse vom Rechner `sonne` importiert werden, so kann dies mit folgendem Befehl erreicht werden:

```
erde:~ # mount -t nfs sonne:/home /home
```

Exportieren von Dateisystemen mit YaST2

Mit YaST2 können Sie sehr schnell einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Das ist ein Server, der Verzeichnisse und Dateien für alle Rechner, denen Sie Zugang gewähren, bereitstellt. Viele Anwendungsprogramme können so z. B. für Mitarbeiter zur Verfügung gestellt werden, ohne dass sie lokal auf deren Rechnern installiert werden müssen.

Zur Installation wählen Sie in YaST2 'Netzwerk/Erweitert' und dort 'NFS-Server' (Abb. 9.8 auf der nächsten Seite).

Im nächsten Schritt aktivieren Sie 'NFS-Server starten' und klicken auf 'Weiter'

Jetzt ist nur noch ein Schritt zu tun: Sie müssen im oberen Feld die Verzeichnisse eintragen, die exportiert werden sollen und im unteren die Rechner Ihres Netzwerks, die darauf Zugriff erhalten (Abb. 9.9 auf Seite 245). Zu den Rechnern sind jeweils vier Optionen einstellbar, *<single host>*, *<netgroups>*, *<wildcards>* und *<IP networks>*. Nähere Erläuterungen zu diesen Optionen finden Sie in den manpages zu Paket `exports` (`man exports`).

Mit 'Beenden' schließen Sie die Konfiguration ab.

Manuelles Exportieren von Dateisystemen

Auf einem NFS-Server müssen die folgenden Netzwerkserver gestartet werden:

- RPC-Portmapper (`portmap`)

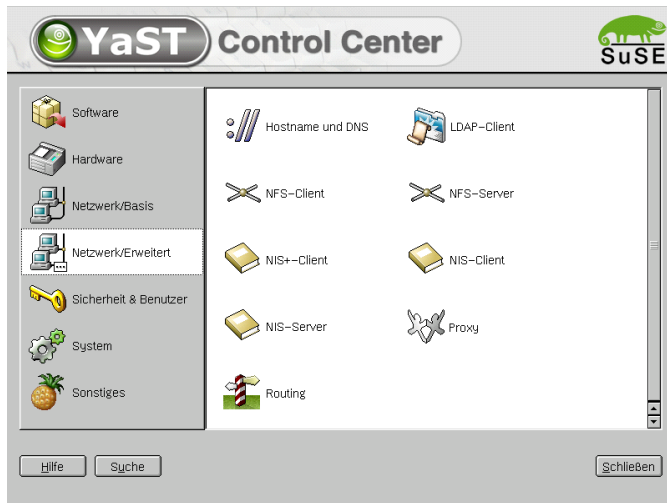


Abbildung 9.8: YaST2: NFS-Server Konfigurationstool

- RPC-Mount-Daemon (`rpc.mountd`)
- RPC-NFS-Daemon (`rpc.nfsd`)

Diese werden beim Hochfahren des Systems von den Skripten `/etc/init.d/portmap` und `/etc/init.d/nfsserver` gestartet.

Neben dem Start dieser Daemons muss noch festgelegt werden, welche Dateisysteme an welche Rechner exportiert werden sollen. Dies geschieht in der Datei `/etc/exports`.

Je Verzeichnis, das exportiert werden soll, wird eine Zeile für die Information benötigt, welche Rechner wie darauf zugreifen dürfen. Alle Unterverzeichnisse eines exportierten Verzeichnisses werden ebenfalls automatisch exportiert. Die berechtigten Rechner werden üblicherweise mit ihren Namen (inklusive Domainname) angegeben, es ist aber auch möglich, mit den Jokerzeichen ``*`` und ``?`` zu arbeiten, die die aus der `bash` bekannte Funktion haben. Wird kein Rechnername angegeben, hat jeder Rechner die Erlaubnis, auf dieses Verzeichnis (mit den angegebenen Rechten) zuzugreifen.

Die Rechte, mit denen das Verzeichnis exportiert wird, werden in einer von Klammern umgebenen Liste nach dem Rechnernamen angegeben. Die wichtigsten Optionen für die Zugriffsrechte sind in der folgenden Tabelle beschrieben.

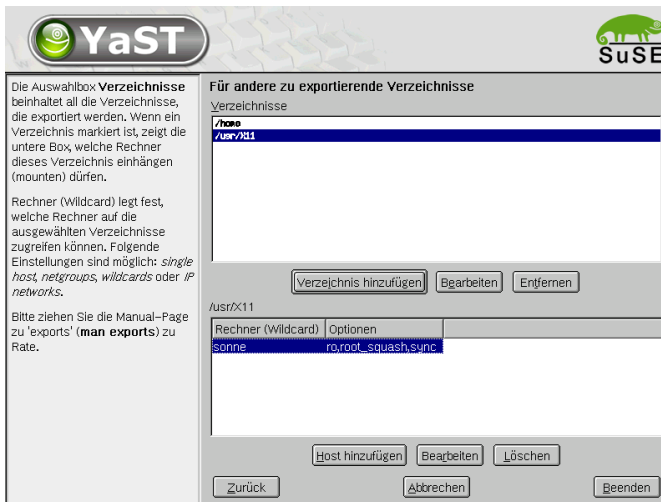


Abbildung 9.9: YaST2: NFS-Server: Exportverzeichnisse und Hosts eintragen

| Optionen | Bedeutung |
|----------------|--|
| ro | Dateisystem wird nur mit Leserechten exportiert (Vorgabe). |
| rw | Dateisystem wird mit Schreib- und Leserechten exportiert. |
| root_squash | Diese Option bewirkt, dass der Benutzer <code>root</code> des angegebenen Rechners keine für <code>root</code> typischen Sonderrechte auf diesem Dateisystem hat. Erreicht wird dies, indem Zugriffe mit der User-ID 0 auf die User-ID 65534 (-2) umgesetzt werden. Diese User-ID sollte dem Benutzer <code>nobody</code> zugewiesen werden (Vorgabe). |
| no_root_squash | Rootzugriffe nicht umsetzen; Rootrechte bleiben also erhalten. |

Tabelle 9.12: Fortsetzung auf der nächsten Seite...

| | |
|---------------|---|
| link_relative | Umsetzen von absoluten, symbolischen Links (solche, die mit <code>'/'</code> beginnen) in eine entsprechende Folge von <code>'../'</code> . Diese Option ist nur dann sinnvoll, wenn das gesamte Dateisystem eines Rechners gemountet wird (Vorgabe). |
| link_absolute | Symbolische Links bleiben unverändert. |
| map_identity | Auf dem Client werden die gleichen User-IDs wie auf dem Server verwendet (Vorgabe). |
| map_daemon | Client und Server haben keine übereinstimmenden User-IDs. Durch diese Option wird der <code>nfsd</code> angewiesen, eine Umsetztabelle für die User-IDs zu erstellen. Voraussetzung dafür ist jedoch die Aktivierung des Daemons <code>ugidd</code> . |

Tabelle 9.12: Zugriffsrechte für exportierte Verzeichnisse

Die `exports`-Datei kann beispielsweise aussehen wie Datei 21.

```
#
# /etc/exports
#
/home          sonne(rw)    venus(rw)
/usr/X11       sonne(ro)    venus(ro)
/usr/lib/texmf sonne(ro)    venus(rw)
/              erde(ro,root_squash)
/home/ftp      (ro)
# End of exports
```

Datei 21: `/etc/exports`

Die Datei `/etc/exports` wird von `mountd` und `nfsd` gelesen. Wird also eine Änderung daran vorgenommen, so müssen `mountd` und `nfsd` neu gestartet werden, damit diese Änderung berücksichtigt wird! Erreicht wird dies am einfachsten mit dem Befehl:

```
erde:~ # rcnfsserver restart
```


DHCP

Das DHCP-Protokoll

Das so genannte „Dynamic Host Configuration Protocol“ dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zu vergeben, statt diese dezentral an einzelnen Arbeitsplatzrechnern zu konfigurieren. Ein mit DHCP konfigurierter Client verfügt selbst nicht über statische Adressen, sondern konfiguriert sich voll und ganz selbstständig nach den Vorgaben des DHCP-Servers.

Dabei ist es möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte zu identifizieren und ständig mit denselben Einstellungen zu versorgen, sowie Adressen aus einem dafür bestimmten Pool „dynamisch“ an jeden „interessierten“ Rechner zu vergeben. In diesem Fall wird sich der DHCP-Server bemühen, jedem Client bei jeder Anforderung (auch über längere Zeiträume hinweg) dieselbe Adresse zuzuweisen – dies funktioniert natürlich nicht, wenn es mehr Rechner im Netz als Adressen gibt.

Ein Systemadministrator kann somit gleich in zweierlei Hinsicht von DHCP profitieren. Einerseits ist es möglich, selbst umfangreiche Änderungen der Netzwerk-Adressen oder der Konfiguration komfortabel in der Konfigurationsdatei des DHCP-Servers zentral vorzunehmen, ohne dass eine Vielzahl von Clients einzeln konfiguriert werden müssen. Andererseits können vor allem neue Rechner sehr einfach ins Netzwerk integriert werden, indem sie aus dem Adress-Pool eine IP-Nummer zugewiesen bekommen. Auch für Laptops, die regelmäßig in verschiedenen Netzen betrieben werden, ist die Möglichkeit, von einem DHCP-Server jeweils passende Netzwerkeinstellungen zu beziehen, sicherlich interessant.

Neben IP-Adresse und Netzmaske werden der Rechner- und Domain-Name, der zu verwendende Gateway und Nameserver-Adressen dem Client mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Timeserver, von dem die jeweils aktuelle Uhrzeit abrufbar ist oder ein Printserver. Im Folgenden möchten wir Ihnen nun einen kurzen Einblick in die Welt von DHCP geben. Wir möchten Ihnen anhand des DHCP-Servers `dhcpcd` zeigen, wie einfach auch in Ihrem Netzwerk die gesamte Netzwerkkonfiguration zentral per DHCP erledigt werden kann.

DHCP-Softwarepakete

Bei SuSE Linux sind drei für DHCP relevante Pakete enthalten.

Einerseits gibt es den vom Internet Software Consortium herausgegebenen DHCP-Server `dhcpd`, der im Netzwerk die entsprechenden Einstellungen vergibt und verwaltet. Doch während bei SuSE Linux normalerweise nur `dhcpd` als Server in Frage kommt, stehen als DHCP-Clients zwei Alternativen zur Auswahl. Einerseits ist hier der ebenfalls von ISC herausgegebene `dhclient` zu nennen, andererseits der so genannte „DHCP Client Daemon“ im Paket `dhcpd`.

Der bei SuSE Linux standardmäßig installierte `dhcpd` ist sehr einfach zu handhaben und wird beim Starten des Rechners automatisch gestartet, um nach einem DHCP-Server zu suchen. Er kommt ohne eine Konfigurationsdatei aus und sollte im Normalfall ohne weitere Konfiguration funktionieren.

Für komplexere Situationen kann man auf den ISC `dhclient` zurückgreifen, der sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt. Egal ob eine zusätzliche Domain in die Suchliste aufgenommen oder gar das Verhalten eines Microsoft DHCP-Clients emuliert werden soll – dem technisch versierten Anwender stehen unzählige Möglichkeiten zur Verfügung, das Verhalten des `dhclient` bis ins Detail seinen Bedürfnissen entsprechend anzupassen.

Der DHCP-Server `dhcpd`

Der *Dynamic Host Configuration Protocol Daemon* ist das Herz eines DHCP-Systems. Er „vermietet“ Adressen und wacht über deren Nutzung, wie in der Konfigurationsdatei `/etc/dhcpd.conf` festgelegt. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des DHCP nach seinen Wünschen zu beeinflussen.

Ein Beispiel für eine einfache `/etc/dhcpd.conf`-Datei:

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "kosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}
```

Datei 22: Die Konfigurationsdatei /etc/dhcpd.conf

Diese einfache Konfigurationsdatei reicht bereits aus, damit DHCP in Ihrem Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Strichpunkte am Ende jeder Zeile, ohne die dhcpd nicht starten wird!

Wie Sie sehen, lässt sich obige Beispieldatei in drei Blöcke unterteilen:

Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Rechner „vermietet“ wird, bevor sich dieser um eine Verlängerung bemühen sollte (`default-lease-time`). Auch wird hier angegeben, wie lange ein Rechner maximal eine vom DHCP-Server vergebene IP-Nummer behalten darf, ohne für diese eine Verlängerung zu beantragen (`max-lease-time`).

Im zweiten Block werden nun einige grundsätzliche Netzwerk-Parameter global festgesetzt:

- Mit `option domain-name` wird die Default-Domain Ihres Netzwerks definiert.
- Bei `option domain-name-servers` können bis zu drei DNS-Server angegeben werden, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollte auf Ihrem System bzw. innerhalb Ihres Netzwerks ein Nameserver bereits in Betrieb sein, der auch für dynamische Adressen jeweils einen Hostnamen und umgekehrt bereit hält. Mehr über die Einrichtung eines eigenen Nameservers erfahren Sie in Abschnitt 9 auf Seite 227.
- `option broadcast-address` legt fest, welche Broadcast-Adresse der anfragende Rechner verwenden soll.
- `option routers` definiert, wohin Datenpakete geschickt werden können, die (aufgrund der Adresse von Quell- und Zielhost sowie Subnetz-Maske) nicht im lokalen Netz zugestellt werden können. Gerade bei kleineren Netzen ist dieser Router auch meist der Übergang zum Internet.
- `option subnet-mask` gibt die an den Client zu übergebende Netzmaske an.

Unterhalb dieser allgemeinen Einstellungen wird nun noch ein Netzwerk samt Subnet Mask definiert. Abschließend muss noch ein Bereich gewählt werden, aus dem der DHCP-Daemon Adressen an anfragende Clients vergeben darf. Im Beispiel stehen alle Adressen zwischen `192.168.1.10` und `192.168.1.20` bzw. `192.168.1.100` und `192.168.1.200` zur Verfügung.

Nach diesen wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Kommando `redhcpd start` zu aktivieren, der sogleich zur Verfügung steht. Auch könnten Sie mit `redhcpd syntax-check` eine kurze, formale Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten und der Server mit einem Fehler abbrechen und nicht mit einem „done“ starten, finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (**Ctrl** + **Alt** + **F10**).

Rechner mit fester IP-Adresse

Nachdem wir es nun geschafft haben, den Server für die Vergabe von dynamischen Adressen zu konfigurieren, sollten wir uns die Vergabe *statischer* Adressen einmal genauer ansehen. Wie eingangs bereits erwähnt, kann mit DHCP auch an ein- und denselben Rechner bei jeder Anfrage eine ganz bestimmte, definierte Adresse vergeben werden.

Selbstverständlich haben solche expliziten Adresszuweisungen Vorrang vor solchen aus dem Pool der dynamischen Adressen. Im Gegensatz zu diesen verfallen die festen Adressinformationen in keinem Fall, wie es bei den dynamischen der Fall ist, wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung erforderlich ist.

Zur Identifizierung eines mit einer *statischen* Adresse definierten Systems, bedient sich der DHCPD der so genannten Hardwareadresse. Dies ist eine weltweit i. d. R. einmalige, fest definierte Nummer aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:00:45:12:EE:F4`.

Wird nun die Konfigurationsdatei aus Datei 22 auf Seite 248 um einen entsprechenden Eintrag wie in Datei 23 ergänzt, wird DHCPD unter allen Umständen dieselben Daten an den entsprechenden Rechner ausliefern.

```
host erde
  hardware ethernet 00:00:45:12:EE:F4;
  fixed-address 192.168.1.21;
```

Datei 23: Ergänzungen zur Konfigurationsdatei

Der Aufbau dieser Zeilen ist nahezu selbsterklärend:

Zuerst wird der DNS-Name des zu definierenden Rechners eingetragen (`host hostname`) und in der folgenden Zeile die MAC-Adresse definiert. Diese Adresse kann bei Linux-Rechnern mit dem Befehl `ifstatus` plus Netzwerkdevice (z. B. `eth0`) festgestellt werden. Gegebenenfalls müssen Sie zuvor die Karte aktivieren: `ifup eth0`. Sie erhalten dann eine Ausgabe wie: `"link/ether 00:00:45:12:EE:F4"`.

In unserem Beispiel wird also dem Rechner, dessen Netzwerkkarte die MAC-Adresse 00:00:45:12:EE:F4 hat, die IP-Adresse 192.168.1.21 sowie der Rechnername *erde* zugewiesen.

Als Hardware-Typ wird heutzutage in aller Regel ethernet zum Einsatz kommen, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende token-ring unterstützt wird.

Weitere Informationen

Wenn Sie an zusätzlichen Informationen interessiert sind, bietet sich z. B. die Seite des *Internet Software Consortium* an, auf der detaillierte Informationen zu DHCP verfügbar sind: <http://www.isc.org/products/DHCP/>.

Auch die neue Version 3 des Protokolls, die sich im Moment im Beta-Test befindet, wird dort dokumentiert. Im Übrigen stehen Ihnen selbstverständlich auch die Manpages zur Verfügung, dies sind insbesondere `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` und `man dhcp-options`. Auf dem Markt sind bisweilen einige Bücher erschienen, die sich umfassend mit den Möglichkeiten des *Dynamic Host Name Configuration Protocol* auseinander setzen.

Übrigens, `dhcpd` kann sogar anfragenden Rechnern eine in der Konfigurationsdatei mit dem `filename`-Parameter definierte Datei anbieten, die einen bootbaren Betriebssystemkern enthält. Damit lassen sich Clients aufbauen, die über keine Festplatte verfügen und sowohl ihr Betriebssystem wie auch ihre Daten ausschließlich über das Netzwerk laden (*diskless clients*). Dies kann sowohl aus Kosten- als auch aus Sicherheitsgründen interessant sein.

Heterogene Netzwerke

Linux kann nicht nur mit anderen Linux-Rechnern kommunizieren, sondern auch mit Windows und Macintoshs. Dieses Kapitel zeigt Ihnen, welche Einstellungen Sie vornehmen müssen.

| | |
|--------------------|-----|
| Samba | 254 |
| Netatalk | 262 |

Samba

Mit dem Programmpaket Samba kann ein beliebiger Unix-Rechner zu einem leistungsfähigen File- und Printserver für DOS-, Windows- und OS/2 Rechner ausgebaut werden. Das Samba-Projekt wird vom Samba Team betreut und wurde ursprünglich von dem Australier Andrew Tridgell entwickelt.

Samba ist inzwischen ein sehr umfassendes Produkt, so dass wir an dieser Stelle lediglich einen Einblick in seine Funktionalität liefern können. Jedoch kommt die Software mit umfassender digitaler Dokumentation. Diese besteht einerseits aus Handbuchseiten — zwecks Umfang rufen Sie bitte `apropos samba` auf der Kommandozeile auf — und andererseits aus Dokumenten und Beispielen, die Sie bei installiertem Samba auf Ihrem System unter `/usr/share/doc/packages/samba` finden. Dort finden Sie im Unterverzeichnis `examples` auch die kommentierte Beispielkonfiguration `smb.conf.SuSE`.

Samba benutzt das SMB-Protokoll (Server Message Block) der Firma Microsoft, das auf den NetBIOS Diensten aufgesetzt ist. Auf Drängen der Firma IBM gab die Firma Microsoft das Protokoll frei, sodass auch andere Software-Hersteller Anbindungen an ein Microsoft-Domain-Netz finden konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das Protokoll TCP/IP installiert sein. Wir empfehlen die ausschließliche Verwendung von TCP/IP auf den Clients.

NetBIOS

NetBIOS ist eine Softwareschnittstelle (API), die zur Rechnerkommunikation entworfen wurde. Dabei wird ein Namensdienst (engl. *name service*) bereitgestellt, der zur gegenseitigen Identifikation der Rechner dient. Für die Namensvergabe gibt es keine zentrale Instanz, die Rechte vergeben oder überprüfen könnte. Jeder Rechner am Netz kann beliebig Namen für sich reservieren, sofern diese noch nicht vergeben sind. Die NetBIOS-Schnittstelle kann auf unterschiedlichen Netzarchitekturen implementiert werden. Eine Implementation erfolgt relativ „dicht“ an der Netzwerkhardware und nennt sich NetBEUI. NetBEUI wird häufig als NetBIOS bezeichnet. Netzwerkprotokolle, mit denen NetBIOS implementiert wurde, sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die NetBIOS-Namen, die auch bei der Implementation von NetBIOS mittels TCP/IP vergeben werden, haben zunächst einmal nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun, NetBIOS ist ein vollständig eigener Namensraum. Es empfiehlt sich jedoch zwecks vereinfachter Administration, zumindest für die Server NetBIOS-Namen zu vergeben, die ihrem DNS-Hostnamen entsprechen. Samba macht dies als Voreinstellung.

Clients

Alle gängigen Betriebssysteme wie DOS, Windows und OS/2 unterstützen das SMB-Protokoll. Auf den Rechnern muss das TCP/IP Protokoll installiert sein. Für die verschiedenen UNIX Versionen kann man ebenfalls Samba einsetzen.

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben, so genannten „Shares“ zur Verfügung. Dabei umfasst ein Share ein Verzeichnis mit allen Unterverzeichnissen auf dem Server. Es wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Dabei kann der Sharename frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem exportierten Drucker ein Name zugeordnet, unter dem Clients darauf zugreifen können.

Installation und Konfiguration des Servers

Zunächst sollte das Paket `samba` installiert sein. Manuell startet man die Dienste mit `rcsmb start`; mit `rcsmb stop` kann man die Dienste beenden.

Die zentrale Konfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Grundsätzlich ist die Datei in zwei Sektionen aufgeteilt. In der so genannten `[global]`-Sektion werden zentrale und übergreifende Einstellungen vorgenommen. Die zweite Sektion ist die `[share]`-Sektion. Hier werden die einzelnen Datei- und Drucker-Freigaben definiert. Dabei können Details der Freigaben unterschiedlich oder in der `[global]`-Sektion übergreifend gesetzt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei. Da im Betrieb häufig auf diese Datei zugegriffen wird, sorgt eine kurze und kommentarfreie Konfigurationsdatei für ein besseres Antwortverhalten des Samba-Servers.

Anschließend werden ausgewählte Parameter näher erläutert.

global-Section anhand der Beispielkonfiguration

Die folgenden Parameter der `global`-Sektion sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server im Windows-Netz von anderen Systemen per SMB erreichbar ist.

workgroup = TUX-NET Der Samba-Server wird mittels dieser Zeile einer Arbeitsgruppe zugeordnet. Zum Betrieb passen Sie `TUX-NET` an die bei Ihnen vorhandene Arbeitsgruppe an oder konfigurieren Ihren Clients auf den hier gewählten Wert. Ihr Samba-Server erscheint bei dieser Konfiguration mit seinem DNS-Namen in der gewählten Arbeitsgruppe, insoweit der Name noch nicht vergeben ist.

Sollte der Name bereits vergeben sein, kann er mit `netbiosname=MEINNAME` abweichend vom DNS-Namen gesetzt werden. Details zu diesem Parameter sind per `man smb.conf` verfügbar.

os level = 2 Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (engl. *Local Master Browser*) für seine Arbeitsgruppe zu werden. Der im Beispiel genutzte Wert ist bewusst niedrig gewählt, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Details zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

Wird nicht bereits ein SMB-Server — z. B. Windows NT, 2000 Server — betrieben und soll der Samba-Server im lokalen Netz die Namen der verfügbaren Systeme vorhalten, so erhöhen Sie den `os level` auf einen höheren Wert (z. B. 65), um die Wahl zum LMB zu gewinnen.

Bei der Änderung dieses Wertes sollten Sie besonders vorsichtig sein, da Sie den Betrieb eines vorhandenen Windows-Netzes stören können. Reden Sie mit Ihrem Administrator, testen Sie Änderungen zuerst in einem isolierten Netz oder zu unkritischen Zeiten.

wins support und wins server Sie wollen den Samba-Server in ein vorhandenes Windows-Netz integrieren, in dem bereits ein WINS-Server betrieben wird: Dazu müssen Sie den Parameter `wins server` durch Entfernen des Semikolon aktivieren und die IP-Adresse auf Ihre Gegebenheiten anpassen.

Ihre Windows-Systeme werden in getrennten Sub-Netzen betrieben, sollen sich gegenseitig sehen, in Ihrem Windows-Netz ist *kein* WINS-Server vorhanden und Ihr Samba-Server soll der WINS-Server werden: Aktivieren Sie dazu die Zeile mit `wins support = yes`. Achten Sie unbedingt darauf, dass Sie diesen Parameter ausschliesslich bei einem Samba-Server aktivieren. Zudem darf in dieser Konstellation `wins server` nicht aktiviert werden.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer, `homes` für SMB-Clients freigegeben.

CD-ROM

```
[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = no
```

Datei 24: CD-ROM-Freigabe

Um die versehentliche Freigabe einer CD-ROM zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe deaktiviert.

- `[cdrom]` und `comment` Der Eintrag `[cdrom]` ist der den SMB-Clients sichtbare Freigabename. Mittels `comment` kann den Clients eine aussagekräftigere Bezeichnung der Freigabe mitgeteilt werden.
- `path = /media/cdrom` Mit `path` wird das Verzeichnis `/media/cdrom` exportiert.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Nutzer verfügbar. Soll die Freigabe für jedermann bereitgestellt werden, ermöglicht man dies mit der zusätzlichen Zeile `guest ok = yes`. Aufgrund der sich daraus ergebenden Lesemöglichkeit für jedermann, sollte man mit dieser Einstellung sehr vorsichtig umgehen und sie allein auf ausgesuchte Freigaben anwenden. Für die Verwendung in der `[global]`-Section gilt besondere Vorsicht.

[homes]

Eine besondere Stellung nimmt die sogenannte `[homes]`-Freigabe ein. Hat der Benutzer auf dem Linux-File-Server einen gültigen Account und ein eigenes Home-Verzeichnis, so kann sich sein Client bei gültiger Nutzerkennung und Passwort mit diesem verbinden.

```
[homes]
      comment = Home Directories
      valid users = %S
      browseable = no
      writeable = yes
      create mask = 0640
      directory mask = 0750
```

Datei 25: Freigabe homes

- `[homes]` Insofern keine ausdrückliche Freigabe mit dem Freigabenamen des sich verbindenden Nutzers existiert, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Nutzernamen.
- `valid users = %S %S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabenamen ersetzt. Da dies bei der `[homes]`-Freigabe immer mit dem Nutzernamen identisch ist, werden die zulässigen Nutzer auf den Eigentümer des Nutzerverzeichnisses beschränkt. Dies ist eine Möglichkeit, um den Zugriff allein dem Eigentümer zugestatten.
- `browseable = no` Durch diese Einstellung ist die `[homes]`-Freigabe nicht in der Liste der Freigaben sichtbar.
- `writeable = yes` Samba verbietet in der Voreinstellung den Schreibzugriff auf exportierte Freigaben, `read only = yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss man den Wert `writeable = yes` setzen. Bei Nutzerverzeichnissen ist dies in der Regel erwünscht.
- `create mask = 0640` Windows-Rechner kennen das Konzept der Unix-Zugriffsrechte nicht. Daher können sie bei der Erstellung von Dateien auch nicht angeben, mit welchen Zugriffsrechten dies zu geschehen hat.
Der Parameter `create mask` legt fest, mit welchen Zugriffsrechten Dateien angelegt werden. Dieses gilt nur für schreibbare Shares. Konkret wird hier dem Eigentümer das Lesen und Schreiben und Mitgliedern der gleichen Gruppe das Lesen erlaubt. Bitte beachten Sie, dass `valid users = %S` selbst den lesenden Zugriff der Gruppenmitglieder verhindert.

Security Level

Das SMB-Protokoll kommt aus der DOS/Windows-Welt und berücksichtigt die Sicherheitsproblematik direkt. Jeder Zugang zu einem Share kann mit einem Passwort geschützt werden. SMB kennt drei verschiedene Möglichkeiten, dies zu bewerkstelligen:

- **Share Level Security:** Bei der Share Level Security wird einem Share ein Passwort fest zugeordnet. Jeder, der dieses Passwort kennt, hat Zugriff auf das Share.
- **User Level Security:** Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort

anmelden. Nach der Authentifizierung kann der Server dann, abhängig vom Benutzernamen, Zugang zu den einzelnen, exportierten Shares gewähren.

- **Server Level Security:** Samba behauptet gegenüber den Clients, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server =`).

Die Unterscheidung zwischen Share, User und Server Level Security gilt für den gesamten Server. Es ist nicht möglich, einzelne Shares per Share Level Security und andere per User Level Security zu exportieren.

Weitere Infos zu diesem Thema finden Sie in der Datei `textdocs/security_level.txt`.

Tipp

Für die einfache Administration des Samba-Servers gibt es noch das Programm `swat`. Es stellt ein einfaches Webinterface zur Verfügung, mit dem Sie bequem den Samba-Server konfigurieren können. Rufen Sie in einem Webbrowser `http://localhost:901` auf und loggen Sie sich als Benutzer `root` ein. Bitte beachten Sie, dass `swat` auch in den Dateien `/etc/inetd.conf` und `/etc/services` aktiviert ist. Weitere Informationen zu `swat` finden Sie in der Manual-Page von `swat` (`man swat`).

Tipp

Samba als Anmelde-Server

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich die Benutzer nur mit gültigem Account und Passwort anmelden dürfen. Dies kann mit Hilfe eines Samba-Servers realisiert werden. In einem reinen Windows-Netzwerk übernimmt ein Windows-NT-Server diese Aufgabe, dieser ist als so genannter Primary Domain Controller (PDC) konfiguriert. Es müssen Einträge in die `[global]`-Section der `smb.conf` vorgenommen werden wie in Beispiel 26 auf der nächsten Seite.

```
[global]
workgroup = TUX-NET
domain logons = yes
domain master = yes%
```

Datei 26: Global-Section in smb.conf

Werden verschlüsselte Passwörter zur Verifizierung genutzt, muss der Samba Server damit umgehen können. Der Eintrag `encrypt passwords = yes` in der `[global]`-Section ermöglicht dies. Außerdem müssen die Benutzeraccounts bzw. die Passwörter in eine Windows konforme Verschlüsselungsform gebracht werden. Das geschieht mit dem Befehl `smbpasswd -a name`. Da nach dem Windows NT Domänenkonzept auch die Rechner selbst einen Domänen-Account benötigen, wird dieser mit den folgenden Befehlen angelegt:

```
useradd -m rechnername
smbpasswd -a -m rechnername
```

Datei 27: Anlegen eines Maschinenaccounts

Bei dem Befehl `useradd` wurde ein Dollarzeichen, maskiert durch den Backslash hinzugefügt. Der Befehl `smbpasswd` fügt diesen bei der Verwendung des Parameters `-m` selbst hinzu.

In der kommentierten Beispielskonfiguration sind Einstellungen vorgesehen, die diese Arbeiten automatisieren.

```
add user script = /usr/sbin/useradd -g machines \
                  -c "NT Machine Account" -d
/dev/null -s /bin/false %m$
```

Datei 28: Automatisiertes Anlegen eines Maschinenaccounts

Installation der Clients

Zunächst sei erwähnt, dass die Clients den Samba-Server nur über TCP/IP erreichen können. NetBEUI oder NetBIOS über IPX sind mit Samba momentan nicht verwendbar. Da TCP/IP überall, sogar bei Novell und Microsoft, auf dem Vormarsch ist, ist es fraglich, ob sich dies jemals ändern wird.

Windows 9x/ME

Windows 9x/ME bringt die Unterstützung für TCP/IP bereits mit. Wie bei Windows for Workgroups wird sie jedoch in der Standardinstallation nicht mitinstalliert. Um TCP/IP nachzuinstallieren, wählt man im Netzwerk-Applet der Systemsteuerung 'Hinzufügen...' unter 'Protokolle' TCP/IP von Microsoft. Bitte achten Sie auf die korrekte Angabe Ihrer Netzwerkadresse und der Netzwerkmaske! Nach einem Neustart des Windows-Rechners können Sie den richtig konfigurierten Samba-Server in der Netzwerkkumgebung wiederfinden (Doppelklick auf das entsprechende Icon auf dem Desktop).

Tipp

Um einen Drucker auf dem Samba-Server zu nutzen, sollte man den allgemeinen oder den Apple PostScript-Druckertreiber von der jeweiligen Windows-Version installieren; am besten verbindet man dann mit der Linux Drucker-Queue, die die automatische aspfiler-Erkennung beinhaltet.

Tipp

Optimierung

Eine Möglichkeit der Optimierung bietet `socket options`. Die Voreinstellung in der mitgelieferten Beispielkonfiguration orientiert sich an einem lokalen Ethernet-Netzwerk. Weitere Details finden Sie in der Manual-Page von `smb.conf` (`man smb.conf`) im Abschnitt `socket options` und zu Manual-Page von `socket(7)` (`man socket(7)`). Weitere Ansätze werden in `textdocs/Speed.txt` und `textdocs/Speed2.txt` beschrieben.

Die Standardkonfiguration in `/etc/samba/smb.conf` versucht weitestgehend sinnvolle Werte vorzuschlagen und verzichtet dabei auf alle Einstellungen, die den Voreinstellungen des Samba-Teams entsprechen. Dies ist jedoch insbesondere hinsichtlich der Netzwerkkonfiguration und des Arbeitsgruppennamens nur sehr schwer oder nicht möglich. In der kommentierten Beispielkonfiguration `examples/smb.conf`. SuSE finden Sie zahlreiche weiterführenden Hinweise, die bei der Anpassung an lokale Gegebenheiten hilfreich sind.

Tipp

Das Samba-Team liefert mit `textdocs/DIAGNOSIS.txt` eine Schritt-für-Schritt-Anleitung zum Überprüfen der Konfiguration.

Tipp

Netatalk

Mit dem Paket `netatalk` können Sie einen leistungsfähigen File- und Druckserver für Mac OS-Clients realisieren. Es ist möglich, von einem Macintosh aus auf Daten des Linux-Rechners zuzugreifen oder auf einem angeschlossenen Drucker zu drucken.

Netatalk ist eine Suite von Unix-Programmen, die auf dem im Kernel implementierten DDP (Datagram Delivery Protocol) aufsetzen und die AppleTalk-Protokoll-Familie (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP und PAP) implementieren.

AppleTalk ist im Prinzip ein Äquivalent zum wesentlich weiter verbreiteten TCP (Transmission Control Protocol). Viele auf TCP/IP aufsetzende Dienste, z. B. zur Auflösung von Hostnamen und Zeitsynchronisation, finden ihre Entsprechung unter AppleTalk. Beispielsweise wird an Stelle von `ping` (ICMP ECHO_REQUEST, Internet Control Message Protocol) der Befehl `aecho` (AEP, AppleTalk Echo Protocol) verwendet.

Folgende drei Daemonen werden normalerweise auf dem Server gestartet:

- Der `atalkd` („AppleTalk-Netzwerk-Manager“), der quasi den Programmen `ifconfig` und `routed` entspricht;
- `afpd` (AppleTalk Filing Protocol daemon), der für Macintosh-Clients ein Interface zu Unix-Dateisystemen zur Verfügung stellt;
- `papd` (Printer Access Protocol daemon), der Drucker im (AppleTalk-) Netz bereitstellt.

Sie können ohne weiteres – und in heterogenen Netzwerkumgebungen ist dies sehr nützlich – Verzeichnisse auf dem Server nicht nur über Netatalk, sondern gleichzeitig über Samba (für Windows-Clients, siehe voriges Kapitel) und über NFS (siehe 9 auf Seite 242), exportieren. Datensicherung und die Verwaltung der Nutzerrechte können zentral auf dem Linux-Server erfolgen.

Beachten Sie bitte:

- Wegen einer Einschränkung der Macintosh-Clients dürfen die Passwörter der Benutzer auf dem Server maximal 8 Zeichen lang sein.
- Auf Unix-Dateien mit Namen länger als 31 Zeichen können Macintosh-Clients nicht zugreifen.
- Dateinamen dürfen keine Doppelpunkte (‘ : ’) enthalten, weil diese unter Mac OS als Separator in Pfadnamen dienen.

Zu installieren ist das Paket `netatalk`.

Konfiguration des Fileservers

In der Standardkonfiguration ist Netatalk als Fileserver für die auf dem Linux-System eingetragenen Benutzer schon voll funktionsfähig. Um die weitergehenden Features zu nutzen, müssen Sie einige Einstellungen in den Konfigurationsdateien vornehmen. Diese befinden sich im Verzeichnis `/etc/atalk`.

Alle Konfigurationsdateien sind reine Textdateien. Text, der hinter einer Raute ``#'` steht, wird ignoriert („Kommentare“), leere Zeilen ebenso.

Netz konfigurieren – `atalkd.conf`

In `/etc/atalk/atalkd.conf` legt man fest, über welche Interfaces die Dienste angeboten werden. Meist ist dies `eth0`, und es genügt, wenn hier als einziger Wert

```
eth0
```

eingetragen ist (dies ist in der Beispieldatei der Fall). Hier tragen Sie weitere Interfaces ein, wenn Sie z. B. mehrere Netzwerkkarten gleichzeitig verwenden. Wird der Server gestartet, sucht er im Netzwerk nach bereits vorhandenen Zonen und Servern und verändert die entsprechende Zeile, indem er die konfigurierten AppleTalk-Netzwerk-Adressen einträgt. Sie finden dann eine Zeile wie

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

am Ende der Datei. Sollten Sie komplexere Konfigurationen vornehmen wollen, finden Sie in der Konfigurationsdatei Beispiele. Dokumentation über weitere Optionen können Sie außerdem der Manual-Page zum `afpd` entnehmen.

Fileserver definieren – `afpd.conf`

In der Datei `afpd.conf` wird festgelegt, wie Ihr Fileserver auf Mac-OS-Rechnern in der 'Auswahl' erscheint. Wie die anderen Konfigurationsdateien enthält auch diese ausführliche Kommentare, die die vielfältigen Optionen erklären.

Ändern Sie hier nichts, wird einfach der Default-Server gestartet und in der 'Auswahl' mit dem Hostnamen angezeigt. Sie müssen also hier nicht unbedingt etwas eintragen, allerdings ist es auch möglich, Fileserver mit verschiedenen Namen und Optionen zu definieren, um z. B. einen speziellen „Guest Server“ anzubieten, auf dem man als „Gast“ Dateien ablegen kann:

```
"Guest server" -uamlist uams_guest.so
```

Oder Sie können einen Server definieren, der keinen Gastzugang erlaubt, sondern nur für Benutzer zugänglich ist, die auf dem Linux-System existieren:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Dieses Verhalten wird gesteuert durch die Option `uamlist` gefolgt von einer durch Kommata getrennten Liste der zu verwendenden Authentifizierungsmodule. Default ist, dass alle Verfahren aktiv sind.

Ein AppleShare-Server stellt seine Dienste standardmäßig nicht nur über AppleTalk, sondern auch („encapsulated“) über TCP/IP zur Verfügung. Der Default-Port ist 548. Für zusätzliche AppleShare-Server (auf dem gleichen Rechner) müssen Sie, wenn diese ebenfalls auch über TCP laufen sollen, dedizierte Ports zuweisen. Die Bereitstellung des Dienstes über TCP/IP ermöglicht den Zugriff auf den Server auch über nicht AppleTalk-Netze wie zum Beispiel das Internet.

Die Syntax wäre dann z. B.:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Der AppleShare-Server erscheint hier im Netz mit dem Namen „Font Server“, erlaubt keinen Zugriff für Gäste und ist auf den Port 12 000 eingestellt. Damit ist er auch über TCP/IP-Router hinweg erreichbar.

Welche (auf dem Server liegenden) Verzeichnisse der jeweilige AppleShare-Server dann als Netz-„Volumes“ bereitstellt, wird in der Datei `AppleVolumes.default` definiert (die weiter unten näher erläutert wird). Mit der `-defaultvol` Option können Sie für einen einzelnen AppleShare-Server auch eine andere Datei festlegen, in der abweichende Vorgaben gemacht werden, z. B. (in einer Zeile):

```
"Guest server" -uamlist uams_guest.so -defaultvol  
/etc/atalk/AppleVolumes.guest
```

Weitere Optionen sind in der Datei `afpd.conf` selbst erklärt.

Verzeichnisse und Zugriffsrechte – AppleVolumes.default

Hier legen Sie Verzeichnisse fest, die exportiert werden sollen. Die Zugriffsrechte werden dabei durch die unter Unix üblichen Benutzer- und Gruppen-Rechte festgelegt.

Dies wird in der Datei `AppleVolumes.default` eingerichtet.

Hinweis

Hier hat sich die Syntax teilweise geändert. Bitte berücksichtigen Sie dies, wenn Sie von einer älteren Version updaten; z. B. heißt es statt `access=` jetzt `allow:` (ein charakteristisches Symptom wäre, wenn Sie auf den Mac-Clients unter AppleTalk statt der Laufwerksbezeichnung deren Optionen angezeigt bekommen.) Da bei einem Update die neuen Dateien mit der Endung `.rpmnew` angelegt werden, kann es sein, dass Ihre alten Einstellungen unter Umständen wegen der geänderten Syntax nicht mehr funktionieren.

Wir empfehlen Ihnen, ein Backup von Ihren Konfigurationsdateien zu machen, aus diesen Ihre alten Einstellungen in die neuen Dateien zu übernehmen und diese dann umzubenennen. So profitieren Sie auch von den aktuellen ausführlichen Kommentaren, die zur Erklärung der diversen Optionen in den Konfigurationsdateien enthalten sind.

Hinweis

Neben `AppleVolumes.default` können zusätzliche Dateien angelegt werden, z. B. `AppleVolumes.guest`, die von bestimmten Servern benutzt werden (indem in der Datei `afpd.conf` die `-defaultvol`-Option benutzt wird – siehe voriger Abschnitt).

Die Syntax ist denkbar einfach:

```
/usr/local/psfonts "PostScript Fonts"
```

bedeutet, dass das in dem Rootverzeichnis liegende Linux-Verzeichnis `/usr/local/psfonts` als AppleShare-Volume mit dem Namen „PostScript Fonts“ freigegeben wird.

Optionen werden, durch Leerzeichen getrennt, an die Zeile angehängt. Eine sehr nützliche Option ist die Zugriffsbeschränkung:

```
/usr/local/psfonts "PostScript Fonts" allow:User1,@gruppe0
```

was den Zugriff auf das Volume „PostScript Fonts“ auf den Benutzer „User1“ und alle Mitglieder der Gruppe „gruppe0“ beschränkt. Diese müssen natürlich dem Server bekannt sein. Entsprechend können Sie mit `deny:User2` auch explizit Nutzer ausschließen.

Bitte berücksichtigen Sie, dass diese Einschränkungen für den Zugriff über AppleTalk gelten und nichts mit den Rechten zu tun haben, die der User hat, wenn er sich auf dem Server selber einloggen kann.

Netatalk legt zur Abbildung der Mac-OS-typischen Ressource-Fork von Dateien im Linux-Dateisystem `.AppleDouble`-Verzeichnisse an. Mit der Option `noadouble` können Sie bestimmen, dass diese Verzeichnisse erst dann angelegt werden, wenn sie tatsächlich benötigt werden. Syntax:

```
/usr/local/guests "Guests" options:noadouble
```

Weitere Optionen und Möglichkeiten entnehmen Sie bitte den Erklärungen in der Datei selbst.

Übrigens: In dieser Konfigurationsdatei finden Sie ebenfalls eine kleine unschuldige Tilde (``~``). Diese Tilde steht für das Homeverzeichnis eines jeden Benutzers auf dem Server. Dadurch kann jedem Benutzer automatisch sein Homeverzeichnis bereitgestellt werden, ohne dass jedes einzelne hier explizit angegeben werden müsste. Die installierte Beispieldatei enthält bereits eine Tilde, weshalb Netatalk standardmäßig die Homeverzeichnisse bereitstellt, wenn Sie an dieser Datei nichts ändern.

Der `afpd` sucht außerdem im Homeverzeichnis eines angemeldeten Benutzers nach einer Datei `AppleVolumes` oder `.AppleVolumes`. Einträge in dieser Datei ergänzen die Einträge in den Serverdateien `AppleVolumes.system` und `AppleVolumes.default`, um weitere individuelle `type/creator`-Zuordnungen zu ermöglichen und auf Dateisysteme zuzugreifen. Diese Einträge sind Ergänzungen und ermöglichen keine Zugriffe, die nicht von Serverseite für diesen Benutzer erlaubt sind.

Die Datei `netatalk.pamd` dient der Authentifizierung über PAM (Pluggable Authentication Modules), was in unserem Rahmen hier ohne Bedeutung ist.

Dateizuordnungen – `AppleVolumes.system`

In der Datei `AppleVolumes.system` legen Sie fest, welche (Mac-OS-typischen) `Type`- und `Creator`-Zuordnungen zu bestimmten Dateiendungen erfolgen soll. Eine ganze Reihe von Standardwerten sind schon vorgegeben. Wenn eine Datei mit einem generischen weißen Icon angezeigt wird, ist in diesem Fall noch kein Eintrag vorhanden. Sollten Sie Probleme haben, eine Textdatei eines anderen Systems unter Mac OS korrekt öffnen zu können, bzw. das umgekehrte Problem, kontrollieren Sie dort die Einträge.

Konfiguration des Druckservers

Über die Datei `papd.conf` konfigurierbar wird ein Laserwriter-Dienst zur Verfügung gestellt. Der Drucker muss lokal schon mit dem `lpd` funktionieren.

Wenn Sie mit dem Kommando `lpr datei.txt` lokal drucken können, ist der erste Schritt erfolgreich getan.

Sie müssen in `papd.conf` nichts eingeben, wenn unter Linux ein lokaler Drucker eingerichtet ist, da ohne weitere Angaben Druckaufträge einfach an den Druck-Daemon `lpd` weitergegeben werden. Der Drucker meldet sich im AppleTalk-Netz als Laserwriter. Sie können aber auch bestimmte Drucker wie folgt eintragen:

```
Drucker_Empfang:pr=lp:pd=/etc/atalk/kyocera.ppd
```

Dies lässt den Drucker mit dem Namen `Drucker_Empfang` in der Auswahl erscheinen. Die entsprechende Druckerbeschreibungsdatei gibt es gewöhnlich beim Hersteller. Ansonsten nehmen Sie einfach die Datei `Laserwriter` aus dem Ordner 'Systemerweiterungen'; allerdings können Sie dann meist nicht alle Features benutzen.

Starten des Servers

Der Server wird per „Init-Skript“ beim Systemstart gestartet oder per Hand mit: `rcatalk start`. Das Init-Skript befindet sich in `/etc/init.d/atalc`. Den Start erledigt das Startskript im Hintergrund; es dauert ca. eine Minute, bis die AppleTalk-Interfaces konfiguriert und erreichbar sind. Sie können mit einer Statusabfrage sehen, ob es soweit ist (erkennbar daran, dass dreimal OK ausgegeben wird):

```
erde:~ # rcatalk status
```

"Checking for service atalk:OKOKOK"

Gehen Sie nun an einen Mac, der unter Mac OS läuft. Kontrollieren Sie, dass AppleTalk aktiviert ist, wählen Sie 'Filesharing', doppelklicken Sie 'Appleshare'; in dem Fenster sollten Sie nun den Namen Ihres Servers sehen. Doppelklicken Sie ihn und melden sie sich an. Wählen Sie das Laufwerk und – voilà – hier ist Ihr Netzlaufwerk unter Mac OS.

Mit Servern, die nur über TCP und nicht über DDP laufen, können Sie sich verbinden, indem Sie in der 'Auswahl' auf 'Server IP-Adresse' klicken und die entsprechende IP-Adresse, gegebenenfalls gefolgt von einem Doppelpunkt und der Portnummer, eingeben.

Weiterführende Informationen

Um alle Möglichkeiten, die das Paket `netatalk` bietet, voll auszuschöpfen, empfiehlt es sich, in den entsprechenden Manual-Pages zu stöbern. Diese finden Sie mit dem Befehl: `rpm -qd netatalk` Noch ein Hinweis: Die Datei `/etc/atalk/netatalk.conf` wird in unserer Version von `netatalk` nicht verwendet, Sie können sie einfach ignorieren. Hilfreiche URLs:

- <http://netatalk.sourceforge.net/>
- <http://www.umich.edu/~rsug/netatalk/>
- <http://www.anders.com/projects/netatalk/>
- <http://cgi.zettabyte.net/fom-serve/netatalk/cache/1.html>

Und wie sieht es eigentlich „andersherum“ aus? Kann ich unter Linux ein AppleShare-Laufwerk erreichen? Die ehrlichste Antwort ist: Besser nicht, da das entsprechende Paket, sich in einem Prä-Alpha-Stadium befindet. Tapfere Experimentatoren finden es unter: <http://www.panix.com/~dfoster/afpfs/>

Internet

Dieses Kapitel gibt Ihnen detaillierte Informationen zur Konfiguration des Proxy-Server Squid. Dieser Server-Dienst hilft Ihnen, den Zugriff auf das World-WideWeb zu beschleunigen.

Des Weiteren erhalten Sie in diesem Kapitel Informationen zur manuellen Konfiguration eines ADSL-Zuganges, falls es bei der Einrichtung mit YaST2 Probleme geben sollte.

| | |
|--|-----|
| Konfiguration eines ADSL / T-DSL Anschlusses | 270 |
| Proxy-Server: Squid | 271 |

Konfiguration eines ADSL / T-DSL Anschlusses

Standardkonfiguration

Momentan werden von SuSE Linux DSL-Zugänge unterstützt, die mit dem Point-to-Point-over-Ethernet-Protokoll (PPPoE) arbeiten. Dieses Protokoll wird von allen großen Anbietern benutzt. Sollten Sie sich nicht sicher sein, welches Protokoll Ihr Provider verwendet, gibt dieser sicherlich gerne Auskunft.

1. Die Pakete `ppp` und `smpppd` müssen installiert werden. Verwenden Sie dazu am besten YaST2.
2. Konfigurieren Sie ihre Netzwerkkarte mit YaST2. Verwenden Sie nicht `dhcp`, sondern vergeben Sie eine statische IP Adresse, zum Beispiel `192.168.2.22`.
3. Die Parameter, die Sie mit dem YaST2 T/ADSL-Modul bearbeiten, werden in der Datei `/etc/sysconfig/network/providers/dsl-provider0` abgespeichert. Zusätzlich gibt es noch Konfigurationsdateien für den SuSE Meta-PPP-Daemon und seine Frontends `kinternet` und `cinternet`. Bitte beachten Sie dazu Manual-Page von `smpppd` (`man smpppd`).
4. Starten Sie das Netzwerk ggf. mit dem Befehl `rcnetwork start`.
5. Mit den Befehlen `cinternet -start` und `cinternet -stop` können Sie auf einem System ohne graphischer Oberfläche eine Verbindung herstellen bzw. abbrechen. Auf einer graphischen Benutzer-Oberfläche können Sie dazu `kinternet` benutzen, das automatisch gestartet wurde, falls Sie DSL mit YaST2 eingerichtet haben. Klicken Sie auf das Zahnrad-Icon in der Buttonleiste. Wählen Sie 'Kommunikation/Internet' → 'Internet Tools' → 'kinternet'. Nun erscheint in der Buttonleiste das Steckersymbol. Ein Klick darauf startet die Verbindung und ein zweiter Klick beendet sie wieder.

DSL Verbindung per Dial-on-Demand

Dial-on-Demand bedeutet, dass die Verbindung automatisch aufgebaut wird, sobald ein User auf das Internet zugreift, z. B. indem er eine Webseite mit einem Browser anwählt oder E-Mails verschickt. Nach einer bestimmten Zeit (Idle-time), in der keine Daten gesendet oder empfangen werden, wird die Verbindung wieder getrennt. Da die Einwahl mit PPPoE, dem Protokoll für ADSL,

sehr schnell geht, entsteht fast der Eindruck, als hätte man eine Standleitung in das Internet.

Dies ist aber nur sinnvoll, wenn Sie eine so genannte Flatrate besitzen. Wird Ihr Zugang zeitabhängig abgerechnet, müssen Sie darauf achten, dass kein periodischer Prozess, z. B. ein cronjob, immer wieder eine Verbindung aufbaut. Das könnte sehr teuer werden.

Obwohl mit einer DSL-Flatrate auch eine permanente Einwahl möglich wäre, sprechen doch einige Punkte für eine Verbindung, die nur kurz und nach Bedarf besteht:

- Die meisten Provider trennen die Verbindung nach einer gewissen Zeit.
- Eine permanente Verbindung kann als Ressourcenverschwendung betrachtet werden (z. B. IP-Adressen).
- Vor allem ist es ein enormes Sicherheitsrisiko permanent online zu sein, da ein Angreifer das System auf Schwachstellen absuchen kann. Ein System, das nur bei Bedarf im Internet erreichbar ist und immer wieder eine andere IP-Adresse hat, ist viel schwieriger zu attackieren.

Dial-on-Demand können Sie mit YaST2 aktivieren (siehe auch das Benutzer-Handbuch) oder Sie richten es manuell ein. Setzen Sie in der Datei `/etc/sysconfig/network/providers/dsl-provider0` den Parameter `DEMAND=` auf „yes“ und definieren Sie eine Idlezeit mit der Variable: `IDLETIME="60"`. Damit wird eine unbenutzte Verbindung nach 60 Sekunden beendet.

Zur Einrichtung eines DSL-Gateways für private Netzwerke empfehlen wir folgenden Artikel in unserer Supportdatenbank: <http://sdb.suse.de/de/sdb/html/masq80.html>

Proxy-Server: Squid

Squid ist der am weitesten verbreitete Proxy-Cache für Linux/UNIX-Plattformen. Wir werden beschreiben, wie er zu konfigurieren ist, welche Systemanforderungen bestehen, wie das eigene System konfiguriert sein muss, um transparentes Proxying durchzuführen, wie man Statistiken über den Nutzen des Cache mithilfe von Programmen wie Calamaris und cachemgr erhält oder wie man Web-Inhalte mit squidgrd filtert.

Was ist ein Proxy-Cache?

Squid fungiert als Proxy-Cache. Es verhält sich wie ein Makler, der Anfragen von Clients erhält (in diesem Fall Web-Browser) und an den zuständigen Server-Provider weiterleitet. Wenn die angeforderten Objekte beim Vermittler ankommen, behält er eine Kopie davon in einem Festplatten-Cache.

Der Vorteil zeigt sich, wenn mehrere Clients dasselbe Objekt anfordern: Sie können nun direkt aus dem Festplatten-Cache bedient werden, also wesentlich schneller als aus dem Internet. Dies spart gleichzeitig eine Menge Systembandbreite.

Tipp

Squid bietet ein großes Spektrum an Features, z. B. die Festlegung von Hierarchien für die Proxy-Server zum Verteilen der Systemlast, Aufstellen fester Zugriffsregeln an alle Clients, die auf den Proxy zugreifen wollen, Erteilen oder Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen oder die Ausgabe von Statistiken der meistbesuchten Webseiten, wie z. B. das Surfverhalten der Benutzer u. v. m.

Tipp

Squid ist kein generischer Proxy. Normalerweise vermittelt er nur zwischen HTTP-Verbindungen. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, jedoch keine anderen Internet-Protokolle wie Real Audio, News oder Videokonferenzen. Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Aus diesem Grund werden auch andere Multimedia-Programme nicht unterstützt.

Informationen zu Proxy-Cache

Squid und Sicherheit

Man kann Squid zusammen mit einer Firewall verwenden, um interne Netzwerke durch den Einsatz von Proxy-Cache nach außen zu schützen. Die Firewall verweigert mit Ausnahme von Squid alle externen Dienste, alle WWW-Verbindungen müssen durch den Proxy aufgebaut werden.

Im Falle einer Firewall-Konfiguration mit einem DMZ würden wir dort unseren Proxy setzen. In diesem Fall ist es wichtig, dass alle Rechner im DMZ ihre Protokolldateien an Rechner innerhalb des gesicherten Netzwerks senden.

Ein Möglichkeit der Implementierung dieser Features mit Hilfe eines so genannten „transparenten“ Proxy wird in Abschnitt [Transparente Proxy-Konfiguration](#) auf Seite 283 behandelt.

Mehrere Caches

Man kann mehrere Caches so konfigurieren, dass Objekte zwischen ihnen ausgetauscht werden können, um die Systemlast zu reduzieren und die Möglichkeit zu steigern, ein bereits im lokalen Netzwerk vorhandenes Objekt zu finden. Möglich sind auch Cache-Hierarchien, so dass ein Cache in der Lage ist, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle herunterzuladen.

Die Wahl der richtigen Topologie für die Cache-Hierarchie ist sehr wichtig, da Netzwerkverkehr insgesamt nicht erhöht werden soll. In einem großen Netzwerk z. B. ist es möglich, für jedes Subnetz einen Proxy-Server zu konfigurieren und diesen dann mit einem übergeordneten Proxy zu verbinden, der wiederum an den Proxy-Cache vom ISP angeschlossen wird.

Die gesamte Kommunikation wird vom ICP (engl. *Internet Cache Protocol*) gesteuert, das auf dem UDP-Protokoll aufgesetzt ist. Der Datenaustausch zwischen Caches geschieht mittels HTTP (engl. *Hyper Text Transmission Protocol*) basierend auf TCP. Allerdings sollten für solche Verbindungen schnellere und einfachere Protokolle verwendet werden, die innerhalb von maximal einer oder zwei Sekunden auf eingehende Anfragen reagieren können.

Um den besten Server für die gewünschten Objekte zu finden, schickt ein Cache an alle Proxies der gleichen Hierarchie eine ICP-Anfrage. Die Proxies werden mittels ICP-Antworten mit dem Code „HIT“ auf die Anfragen reagieren, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Falle mehrerer HIT-Antworten wird der Proxy-Server einen Server für das Herunterladen bestimmen. Diese Entscheidung wird unter anderem dadurch bestimmt, welcher Cache die schnellste Antwort sendet oder welcher näher ist. Bei einer nicht zufrieden stellenden Antwort gesendet wurde, wird die Anfrage an den übergeordneten Cache geschickt.

Tipp

Zur Vermeidung von mehrfacher Speicherung von Objekten in verschiedenen Caches unseres Netzwerks werden andere ICP-Protokolle verwendet, wie z. B. CARP (engl. *Cache Array Routing Protocol*) oder HTCP (engl. *Hyper-Text Cache Protocol*).

Je mehr Objekte sich im Netzwerk befinden, desto leichter wird es, das Gesuchte zu finden.

Tipp

Zwischenspeichern von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es existieren viele dynamisch generierte CGI-Seiten, Zugriffszähler oder verschlüsselte SSL-Dokumente für eine höhere Sicherheit. Aus diesem Grund werden solche Objekte nicht im Cache gehalten: Bei jedem neuen Zugriff hat sich das Objekt bereits wieder verändert.

Für alle anderen im Cache befindlichen Objekte stellt sich jedoch die Frage, wie lange sie dort bleiben sollen. Für diese Entscheidung werden alle Objekte im Cache drei verschiedenen Stadien zugeordnet:

Durch Header wie `Last modified` („zuletzt geändert“) oder `Expires` („läuft ab“) und dem entsprechenden Datum informieren sich Web- und Proxy-Server über den Status eines Objekts. Es werden auch andere Header verwendet, die z. B. anzeigen, dass ein Objekt nicht zwischengespeichert werden muss.

Objekte im Cache werden normalerweise aufgrund fehlenden Speichers ersetzt, und zwar durch Algorithmen wie LRU (engl. *Last Recently Used*), die zum Ersetzen von Cache-Objekten entwickelt wurden. Das Prinzip besteht im Wesentlichen darin, zuerst die am seltensten gewünschten Objekte zu ersetzen.

Systemanforderungen

Zuerst sollte die maximale Systemlast bestimmt werden. Es ist wichtig, den Systemspitzen besondere Aufmerksamkeit zu schenken, da diese mehr als viermal so hoch wie der Tagesdurchschnitt sein können. Im Zweifelsfall ist es besser, die Systemanforderungen zu überschätzen, vorausgesetzt, dass ein am Limit arbeitender Squid zu einem ernsthaften Qualitätsverlust des Dienstes führen kann.

Geordnet nach Wichtigkeit werden in den folgenden Abschnitten die verschiedenen Systemfaktoren aufgezeigt.

Festplatte

Für das Zwischenspeichern spielt Geschwindigkeit eine hohe Rolle. Man sollte sich also um diesen Faktor besonders kümmern. Bei Festplatten ist dieser Parameter als „zufällige Positionierzeit“ in Millisekunden beschrieben. Als Faustregel gilt: Je niedriger dieser Wert, desto besser. Für eine hohe Geschwindigkeit empfiehlt es sich, schnelle Festplatten zu wählen.

Größe des Festplatten-Cache

In einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (das gewünschte Objekt befindet sich bereits dort) sehr gering, da der Cache schnell gefüllt sein

wird. In diesem Fall werden die selten gewünschten Objekte durch neue ersetzt. Steht jedoch 1 GB für den Cache zur Verfügung und die Benutzer benötigen nur 10 MB pro Tag zum Surfen, dann dauert es mehr als hundert Tage, bis der Cache voll ist.

Am leichtesten lässt sich die Größe des Cache durch die maximale Übertragungsrate der Verbindung bestimmen. Mit einer Verbindung von 1 MB/Sek wird die maximale Übertragungsrate bei 125 KB/Sek liegen. Landet der gesamte Datenverkehr im Cache, kommen innerhalb einer Stunde 450 MB zusammen. Wenn man nun annimmt, dass der gesamte Datenverkehr lediglich während acht Arbeitsstunden erzeugt wird, erreicht man innerhalb eines Tages 3,6 GB. Da die Verbindung nicht bis zur Kapazitätsgrenze ausgeschöpft wurde, konnten wir davon ausgehen, dass die gesamte Datenmenge, die durch den Cache geht, bei ungefähr 2 GB liegt. In unserem Beispiel werden 2 GB Speicher für Squid benötigt, um die Daten aller aufgerufenen Seiten *eines* Tages im Cache zu halten.

Zusammenfassend lässt sich sagen, dass Squid dazu tendiert, kleinere Datenblöcke von der Festplatte zu lesen oder darauf zu schreiben, so dass es wichtiger ist, wie schnell er diese Objekte auf der Festplatte findet, als eine Festplatte mit hohem Durchsatz zu haben.

RAM

Der von Squid benötigte Speicher ist abhängig von der Anzahl der im Cache zugewiesenen Objekte. Squid speichert Cache-Objektverweise und häufig angeforderte Objekte zusätzlich im Speicher, damit diese Daten schneller abgefragt werden können. Der Speicher ist eine Million mal schneller als eine Festplatte!

Squid hält auch andere Daten im Speicher, z. B. eine Tabelle mit allen vergebenen IP-Adressen, einen genau festgelegten Domainnamen-Cache, die am häufigsten gewünschten Objekte, Puffer, Zugriffskontrolllisten, etc.

Es ist sehr wichtig, dass ausreichend Speicher für den Squid-Prozess zur Verfügung steht. Sollte er auf Festplatte ausgelagert werden müssen, wird sich die Systemleistung nämlich drastisch reduzieren. Für die Cache-Speicherverwaltung wird das Tool `cachemgr.cgi` verwendet. Es wird im Abschnitt [cachemgr.cgi](#) auf Seite 286 erläutert.

CPU

Das Programm Squid benötigt nicht viel CPU. Nur beim Start und während der Überprüfung des Cache-Inhalts ist die Prozessorlast höher. Der Einsatz eines Multiprozessorrechners steigert nicht die Systemleistung. Zur Effektivitätssteigerung ist es besser, schnellere Festplatten zu verwenden oder mehr Speicher hinzuzufügen.

Einige Beispiele von konfigurierten Systemen, auf denen Squid läuft, finden sich unter <http://wwwcache.ja.net/servers/squids.html>.

Squid starten

Der Squid auf SuSE Linux Desktop ist bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Als Voraussetzung für einen reibungslosen Start sollte das Netzwerk soweit konfiguriert sein, dass mindestens ein Nameserver und sinnvollerweise auch das Internet erreichbar sind. Probleme kann es bereiten, wenn man eine Wählverbindung mit dynamischer DNS-Konfiguration verwendet. In so einem Fall sollte mindestens der Nameserver fest eingetragen sein, da Squid erst gar nicht startet, wenn er in der `/etc/resolv.conf` keinen DNS findet.

Um Squid zu starten, gibt man auf der Kommandozeile (als `root`)

```
rcsquid start
```

ein. Beim ersten Mal wird zunächst die Verzeichnisstruktur in `/var/squid/cache` angelegt. Dies wird vom Startskript `/etc/init.d/squid` automatisch durchgeführt und kann ein paar Sekunden bis Minuten dauern. Erscheint rechts in grün `done`, wurde Squid erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit von Squid sofort testen, indem man im Browser als Proxy `localhost` und Port `3128` einträgt. Um den Zugriff auf Squid und somit das Internet für alle zu ermöglichen, braucht man in der Konfigurationsdatei `/etc/squid.conf` lediglich den Eintrag `http_access deny all` auf `http_access allow all` zu ändern. Allerdings sollte man dabei bedenken, dass man den Squid damit komplett für jedermann öffnet. Von daher sollte man unbedingt ACLs definieren, die den Zugriff auf den Proxy regeln. Dazu mehr im Abschnitt *Optionen zur Zugriffskontrolle* auf Seite 280.

Hat man Änderungen an der Konfigurationsdatei `/etc/squid.conf` vorgenommen, muss man Squid dazu bringen, diese neu einzulesen. Das gelingt mit:

```
rcsquid reload
```

Alternativ kann man Squid auch komplett neu starten:

```
rcsquid restart
```

Wichtig ist noch folgendes Kommando:

```
rcsquid status
```

 Damit kann man feststellen, ob der Proxy läuft und mit

```
rcsquid stop
```

wird Squid beendet. Letzteres kann eine Weile dauern, da Squid bis zu einer

halben Minute (Option `shutdown_lifetime` in `/etc/squid.conf`) wartet, bevor die Verbindungen zu den Clients unterbrochen werden und er dann noch seine Daten auf Platte schreiben muss. Beendet man Squid mit einem `kill` oder `killall`, kann das einen zerstörten Cache zur Folge haben, den man dann löschen muss, um Squid wieder starten zu können.

Beendet sich Squid nach kurzer Zeit, obwohl er scheinbar erfolgreich gestartet wurde, kann das an einem fehlerhaften Nameserver-Eintrag oder einer fehlenden `/etc/resolv.conf` liegen. Den Grund für einen gescheiterten Start protokolliert Squid dabei in der Datei `/var/squid/logs/cache.log`. Soll Squid bereits beim Booten automatisch gestartet werden, muss im Yast2 Runlevel-Editor Squid für bestimmte Runlevel aktiviert werden.

Bei einer Deinstallation von Squid werden weder Cache noch Log-Dateien entfernt. Man muss das Verzeichnis `/var/cache/squid` manuell löschen.

Lokaler DNS-Server

Einen lokalen DNS-Server wie BIND-8 oder BIND-9 aufzusetzen, ist durchaus sinnvoll, auch wenn er keine eigene Domain verwaltet. Er fungiert dann lediglich als „Caching-only DNS“ und kann ohne spezielle Konfiguration DNS-Anfragen über die Root-Nameserver auflösen. Trägt man diesen in der `/etc/resolv.conf` mit der IP-Adresse `127.0.0.1` für `localhost` ein, findet Squid beim Starten immer einen gültigen Nameserver. Es reicht aus, das Paket zu installieren und BIND zu starten. Den Nameserver des Providers sollte man in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` mit seiner IP-Adresse eintragen. Falls man eine Firewall laufen hat, und sei es nur die Personal-Firewall, muss man aber darauf achten, dass die DNS-Anfragen auch durchgelassen werden.

Die Konfigurationsdatei `/etc/squid.conf`

Alle Einstellungen zum Squid Proxyserver sind in der Datei `/etc/squid.conf` vorzunehmen. Um Squid erstmalig starten zu können, sind darin keine Änderungen erforderlich, der Zugriff von externen Clients ist jedoch erst einmal gesperrt. Für `localhost` ist der Proxy freigegeben und als Port wird standardmäßig 3128 verwendet. Die Optionen sind ausführlich und mit vielen Beispielen in der vorinstallierten `/etc/squid.conf` dokumentiert. Annähernd alle Einträge sind am Zeilenanfang durch ein `#`-Zeichen auskommentiert; am Zeilenende befinden sich die relevanten Spezifikationen. Die angegebenen Werte entsprechen fast immer den voreingestellten Werten, so dass das Entfernen des Kommentarzeichens, ohne den Parameter der Option zu ändern, bis auf wenige Ausnahmen keine Wirkung hat. Besser ist es, das Beispiel stehen zu lassen

und die Option mit dem geänderten Parameter in der Zeile darunter neu einzufügen. So kann man die voreingestellten Werte und Änderungen problemlos nachvollziehen.

Hat man ein Update von einer älteren Squid-Version durchgeführt, ist es unbedingt zu empfehlen, die neue `/etc/squid.conf` zu verwenden und nur die Änderungen von der ursprünglichen Datei zu übernehmen. Versucht man die alte `squid.conf` weiter zu verwenden, läuft man Gefahr, dass die Konfiguration nicht mehr funktioniert, da Optionen immer wieder geändert werden und neue hinzukommen.

Allgemeine Konfigurations-Optionen

http_port 3128 Das ist der Port, auf dem Squid auf Anfragen der Clients lauscht. Voreingestellt ist 3128, gebräuchlich ist auch 8080. Es ist möglich, hier mehrere Portnummern, durch Leerzeichen getrennt, anzugeben.

cache_peer <hostname> <type> <proxy-port> <icp-port> Hier kann man einen übergeordneten Proxy als „Parent“ eintragen, z. B. wenn man den des Providers nutzen will oder muss. Als <hostname> trägt man den Namen bzw. die IP-Adresse des zu verwendenden Proxies und als <type> `parent` ein. Für <proxy-port> trägt man die Portnummer ein, die der Betreiber des Parent auch zur Verwendung im Browser angibt, meist 8080. Den <icp-port> kann man auf 7 oder 0 setzen, wenn man den ICP-Port des Parent nicht kennt und die Benutzung dieses mit dem Provider nicht vereinbart wurde. Zusätzlich sollte man dann noch `default` und `no-query` nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxy des Providers wie ein normaler Browser.

cache_mem 8 MB Dieser Eintrag gibt an, wie viel Arbeitsspeicher von Squid für das Cachen maximal verwendet wird. Voreingestellt sind 8 MB.

cache_dir ufs /var/cache/squid 100 16 256 Der Eintrag `cache_dir` gibt das Verzeichnis an, in dem alle Objekte auf Platte abgelegt werden. Die Zahlen dahinter geben den maximal zu verwendenden Plattenplatz in MB und die Anzahl der Verzeichnisse in erster und zweiter Ebene an. Den Parameter `ufs` sollte man unverändert lassen. Voreingestellt sind 100 MB Plattenplatz im Verzeichnis `/var/cache/squid` zu belegen und darin 16 Unterverzeichnisse anzulegen, die jeweils wiederum 256 Verzeichnisse enthalten. Bei Angabe des zu verwendenden Plattenplatzes sollte man genügend Reserven lassen, sinnvoll sind Werte zwischen 50 und maximal 80 Prozent des verfügbaren Platzes. Die beiden letzten Zahlen für die Anzahl

der Verzeichnisse sollte man nur mit Vorsicht vergrößern, da zu viele Verzeichnisse auch wieder auf Kosten der Performance gehen können. Hat man mehrere Platten, auf die der Cache verteilt werden soll, kann man entsprechend viele `cache_dir`-Zeilen eintragen.

cache_access_log /var/squid/logs/access.log Pfadangabe für Log-Dateien.

cache_log /var/squid/logs/cache.log Pfadangabe für Log-Dateien.

cache_store_log /var/squid/logs/store.log Pfadangabe für Log-Dateien.

Diese drei Einträge geben den Pfad zur Protokolldatei von Squid an. Normalerweise wird man daran nichts ändern. Wird der Squid stark beansprucht, kann es sinnvoll sein, den Cache und die Log-Dateien auf verschiedene Platten zu legen.

emulate_htpdd_log off Ändert man diesen Eintrag auf `on`, erhält man lesbare Log-Dateien. Allerdings kommen manche Auswerteprogramme damit nicht zurecht.

client_netmask 255.255.255.255 Mit diesem Eintrag kann man die protokollierten IP-Adressen in den Log-Dateien maskieren, um die Identität der Clients zu verbergen. Trägt man hier `255.255.255.0` ein, wird die letzte Stelle der IP-Adresse auf Null gesetzt.

ftp_user Squid@do.main Hiermit kann man das Passwort setzen, welches Squid für den anonymen FTP-Login verwenden soll. Es kann aber sinnvoll sein, hier eine gültige E-Mail-Adresse in der eigenen Domain anzugeben, da einige FTP-Server diese auf Gültigkeit überprüfen.

cache_mgr webmaster Eine E-Mail-Adresse, an die Squid eine Nachricht schickt, wenn er unerwartet abstürzt. Voreingestellt ist `webmaster`.

logfile_rotate 0 Squid ist in der Lage, die gesicherten Log-Dateien zu rotieren, wenn man `squid -k rotate` aufruft. Die Dateien werden dabei, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Dieser Wert steht standardmäßig auf 0, weil das Archivieren und Löschen der Log-Dateien bei SuSE Linux Desktop von einem eigenen Cronjob durchgeführt wird, dessen Konfiguration man in der Datei `/etc/logrotate/syslog` findet. Der Zeitraum, nach dem die Dateien gelöscht werden, wird in der Datei `/etc/sysconfig/aaa_base` mit dem Eintrag `MAX_DAYS_FOR_LOG_FILES` festgelegt.

append_domain <domain> Mit `append_domain` kann man angeben, welche Domain automatisch angehängt wird, wenn keine angegeben wurde.

Meist wird man hier die eigene Domain eintragen, dann genügt es, im Browser `www` einzugeben, um auf den eigenen Webserver zu gelangen.

forwarded_for on Setzt man diesen Eintrag auf `off`, entfernt Squid die IP-Adresse bzw. den Systemnamen des Clients aus den HTTP-Anfragen.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes Normalerweise braucht man diese Werte nicht zu verändern. Hat man aber eine Wählleitung, kann es vorkommen, dass das Internet zeitweilig nicht erreichbar ist. Squid merkt sich dann die erfolglosen Anfragen und weigert sich, diese neu anzufragen, obwohl die Verbindung in das Internet wieder steht. Für diesen Fall sollte man die `minutes` in `seconds` ändern, dann führt auch ein Reload im Browser, wenige Sekunden nach der Einwahl, wieder zum Erfolg.

never_direct allow <acl_name> Will man verhindern, dass Squid Anfragen direkt aus dem Internet fordert, kann man hiermit die Verwendung eines anderen Proxies erzwingen. Diesen muss man zuvor unter `cache_peer` eingetragen haben. Gibt man als `<acl_name>` `all` an, erzwingt man, dass sämtliche Anfragen direkt an den `parent` weitergegeben werden. Das kann zum Beispiel nötig sein, wenn man einen Provider verwendet, der die Verwendung seines Proxies zwingend vorschreibt oder die Firewall keinen direkten Zugriff auf das Internet durchlässt.

Optionen zur Zugriffskontrolle

Squid bietet ein ausgeklügeltes System, um den Zugriff auf den Proxy zu steuern. Durch die Verwendung von ACLs ist es einfach und vielseitig konfigurierbar. Dabei handelt es sich um Listen mit Regeln, die der Reihe nach abgearbeitet werden. ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs wie `all` und `localhost` sind bereits vorhanden. Das Festlegen einer ACL an sich bewirkt aber noch gar nichts. Erst wenn sie tatsächlich eingesetzt wird, z. B. in Verbindung mit `http_access`, werden die definierten Regeln abgearbeitet.

acl <acl_name> <type> <data> Eine ACL benötigt zur Definition mindestens drei Angaben. Der Name `<acl_name>` kann frei gewählt werden. Für `<type>` kann man aus einer Vielzahl unterschiedlicher Möglichkeiten auswählen, die man im Abschnitt `ACCESS CONTROLS` in der `/etc/squid.conf` nachlesen kann. Was für `<data>` anzugeben ist, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, z. B. mit Rechnernamen, IP-Adressen oder URLs eingelesen werden. Im folgenden einige einfache Beispiele:

```
acl meinesurfer srcdomain .meine-domain.com
acl lehrer src 192.168.1.0/255.255.255.0
acl studenten src 192.168.7.0-192.168.9.0/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

http_access allow <acl_name> Mit `http_access` wird festgelegt, wer den Proxy verwenden darf und auf was er im Internet zugreifen darf. Dabei sind ACLs anzugeben, `localhost` und `all` sind weiter oben bereits definiert, die mit `deny` oder `allow` den Zugriff sperren oder freigeben. Man kann hier eine Liste mit vielen `http_access`-Einträgen erstellen, die von oben nach unten abgearbeitet werden; je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben oder gesperrt. Als letzter Eintrag sollte immer `http_access deny all` stehen. Im folgenden Beispiel hat `localhost`, also der lokale Rechner, freien Zugriff auf alles, während er für alle anderen komplett gesperrt ist:

```
http_access allow localhost
http_access deny all
```

Noch ein Beispiel, in dem die zuvor definierten ACLs verwendet werden: Die Gruppe `lehrer` hat jederzeit Zugriff auf das Internet, während die Gruppe `studenten` nur Montags bis Freitags, und da nur `mittags`, surfen darf:

```
http_access deny localhost
http_access allow lehrer
http_access allow studenten mittags
http_access deny all
```

Die Liste mit den eigenen `http_access`-Einträgen sollte man der Übersichtlichkeit halber nur an der dafür vorgesehenen Stelle in der `/etc/squid.conf` eintragen. Das bedeutet zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

und dem abschließenden

```
http_access deny all
```

redirect_program /usr/bin/squidGuard Mit dieser Option kann man einen „Redirector“, wie z. B. SquidGuard angeben, der in der Lage ist, unerwünschte URLs zu sperren. In Verbindung mit Proxy-Authentifizierung und den passenden ACLs kann man so den Zugriff auf das Internet für verschiedene Benutzergruppen sehr differenziert steuern. SquidGuard ist ein eigenes Paket, das separat zu installieren und konfigurieren ist.

authenticate_program /usr/sbin/pam_auth Sollen sich die Benutzer am Proxy authentifizieren müssen, kann man hier ein entsprechendes Programm wie z. B. pam_auth angeben. Bei der Verwendung von pam_auth öffnet sich für den Anwender beim ersten Zugriff ein Loginfenster, in dem er Benutzername und Passwort eingeben muss. Zusätzlich ist noch eine ACL erforderlich, damit nur Clients mit gültigem Login surfen können:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Das REQUIRED nach proxy_auth kann man auch durch eine Liste von erlaubten Benutzernamen oder einen Pfad zu solch einer Liste ersetzen.

ident_lookup_access allow <acl_name> Hiermit erreicht man, dass auf alle durch die ACL definierten Clients eine Ident-Anfrage ausgeführt wird, um die Identität des jeweiligen Benutzers zu ermitteln. Setzt man für <acl_name> all ein, erfolgt dies generell für alle Clients. Auf den Clients muss dazu ein Ident-Daemon laufen, bei Linux kann man dafür das Paket pidentd installieren, für Windows gibt es freie Software, die man sich aus dem Internet besorgen kann. Damit nur Clients mit erfolgreichem Ident-Lookup zugelassen werden, ist auch hier wieder eine entsprechende ACL zu definieren:

```
acl identhsts ident REQUIRED

http_access allow identhsts
http_access deny all
```

Auch hier kann man das REQUIRED wieder durch eine Liste erlaubter Benutzernamen ersetzen. Die Verwendung von Ident kann den Zugriff merklich verlangsamen, da die Ident-Lookups durchaus für jede Anfrage wiederholt werden.

Transparente Proxy-Konfiguration

Normalerweise schickt der Web-Browser an einen bestimmten Port des Proxy-Servers Anfragen und der Proxy stellt die angeforderten Objekte zur Verfügung, ob sie nun im Cache sind oder nicht. Innerhalb eines echten Netzwerks können verschiedene Situationen auftreten:

- Aus Sicherheitsgründen ist es besser, wenn alle Clients zum Surfen im Internet einen Proxy verwenden.
- Es ist notwendig, dass alle Clients einen Proxy verwenden, egal ob sie sich dessen bewusst sind oder nicht.
- In großen Netzwerken, die bereits einen Proxy verwenden, ist es möglich, veränderte Konfigurationen der einzelnen Rechner zu speichern, falls sich Änderungen am System ergeben.

In jedem dieser Fälle kann ein transparenter Proxy eingesetzt werden. Das Prinzip ist denkbar einfach: Der Proxy nimmt die Anfragen des Web-Browsers entgegen und bearbeitet sie, sodass der Web-Browser die angeforderten Seiten erhält ohne zu wissen, woher sie kommen. Der gesamte Prozess wird transparent ausgeführt, daher der Name für den Vorgang.

Konfigurationsoptionen in `/etc/squid.conf`

Folgende Optionen in der Datei `/etc/squid.conf` müssen aktiviert werden, um einen transparenten Proxy aufzusetzen:

- `httpd_accel_host virtual`
- `httpd_accel_port 80` # Port, auf dem sich der tatsächliche HTTP-Server befindet.
- `httpd_accel_with_proxy on`
- `httpd_accel_uses_host_header on`

Firewall-Konfiguration mit SuSEfirewall2

Alle durch die Firewall eingehenden Anfragen müssen mithilfe einer Port-Weiterleitungsregel an den Squid-Port weitergeleitet werden.

Dafür eignet sich das SuSE-eigene Tool SuSEfirewall2. Dessen Konfigurationsdatei findet man in der Datei `/etc/sysconfig/scripts/SuSEfirewall2-custom`. Die Konfigurationsdatei wiederum setzt sich aus

gut dokumentierten Einträgen zusammen. Auch wenn wir nur einen transparenten Proxy einrichten wollen, müssen wir einige Firewall-Optionen konfigurieren. Beispielsweise:

- Gerät zeigt auf Internet: `FW_DEV_WORLD="eth1"`
- Gerät zeigt auf Netzwerk: `FW_DEV_INT="eth0"`

Auf Ports und Dienste (siehe `/etc/exports`) in der Firewall wird von nicht vertrauenswürdigen Netzwerken also dem Internet zugegriffen. In diesem Beispiel bieten wir lediglich Web-Dienste nach außen hin an:

```
FW_SERVICES_EXTERNAL_TCP="www"
```

Auf Ports/Dienste (siehe `/etc/exports`) in der Firewall wird vom sicheren Netzwerk, sowohl TCP und UDP, zugegriffen.

```
FW_SERVICES_INTERNAL_TCP="domain www 3128"
```

```
FW_SERVICES_INTERNAL_UDP="domain"
```

Wir greifen auf Web-Dienste und Squid (dessen Standardport ist 3128) zu. Der oben beschriebene Dienst „Domain“ steht für DNS oder Domain Name Server. Es ist üblich, diesen Dienst zu nutzen. Andernfalls entfernen wir ihn einfach aus obigem Eintrag und setzen folgende Option auf `no`:

```
FW_SERVICE_DNS="yes"
```

Die wichtigste Option ist die Ziffer 15:

```
#
# 15.)
# Welcher Zugriff auf die einzelnen Dienste soll an einen lokalen
# Port auf dem Firewall-Rechner umgeleitet werden?
#
# Damit können alle internen Benutzer gezwungen werden, über den
# Squid-Proxy zu surfen oder es kann eingehender Webverkehr
# transparent an einen sicheren Web-Server umgeleitet werden.
#
# Wahl: keinen Eintrag vornehmen oder folgend erklärte Syntax von
# Umleitungsregeln, getrennt durch Leerzeichen, verwenden.
```

```
# Eine Umleitungsregel besteht aus 1) Quelle IP/Netz, 2) Ziel
# IP/Netz, 3) ursprünglicher Zielpport und 4) lokaler Port, an den
# der Verkehr umgeleitet werden soll, getrennt durch Kommata, z.B.:
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

Datei 29: Option 15 der Firewallkonfiguration

Im obigen Kommentar wird die einzuhaltende Syntax gezeigt. Zuerst greifen die IP-Adresse und die Netzwerkmaske der „internen Netzwerke“ auf die Proxy-Firewall zu. Dann die IP-Adresse und die Netzwerkmaske, an die Anfragen von den Clients „gesendet“ werden. Im Fall von Web-Browsern wählt man die Netzwerke 0/0. Dies ist eine Wildcard und bedeutet „überallhin“. Danach kommt der „ursprüngliche“ Port, an den diese Anfragen geschickt wurden und schließlich folgt der Port, an den die Anfragen „umgeleitet“ wurden.

Da Squid mehr Protokolle unterstützt als nur HTTP, können auch Anfragen von anderen Ports an den Proxy umgeleitet werden, so zum Beispiel FTP (Port 21), HTTPS oder SSL (Port 443).

Im konkreten Fall werden Web-Dienste (Port 80) auf den Proxy-Port (hier 3128) umgeleitet. Falls mehrere Netzwerke oder Dienste hinzugefügt werden sollen, müssen diese durch ein Leerzeichen im entsprechenden Eintrag getrennt werden.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

```
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

Zum Starten der Firewall und der neuen Konfiguration muss man einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall12` editieren. Der Eintrag `START_FW` muss auf "yes" gesetzt werden:

Starten Sie Squid wie in Abschnitt [Squid starten](#) auf Seite 276 beschrieben. Anhand der Protokolldateien in `/var/log/squid/access.log` kann überprüft werden, ob alles richtig funktioniert. Um zu überprüfen, ob alle Ports korrekt konfiguriert wurden, kann von jedem beliebigen Rechner außerhalb unserer Netzwerke auf dem Rechner ein Portscan ausgeführt werden. Nur der Web-Dienst-Port (80) sollte offen sein. Der Portscan führt über `nmap`:

```
nmap -O IP_address
```

Squid und andere Programme

In diesem Abschnitt wird gezeigt, wie andere Applikationen mit Squid interagieren.

cachemgr.cgi ermöglicht dem Systemadministrator, den benötigten Speicher für das Zwischenspeichern von Objekten zu überprüfen. Squidgrd filtert Webseiten, und calamaris ist ein Berichtsgenerator für Squid.

cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den benötigten Speicher des laufenden Squid-Prozesses. Im Gegensatz zum Protokollieren erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken.

Einrichten

Zuerst wird ein lauffähiger Web-Server auf dem System benötigt. Als Benutzer root gibt man Folgendes ein, um herauszufinden, ob Apache bereits läuft: `rcapache status`.

Erscheint eine Nachricht wie diese:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

dann läuft Apache auf unserem Rechner. Andernfalls müssen Sie Folgendes eingeben: `rcapache start`

So wird Apache mit den SuSE Linux-Standardeinstellungen gestartet. Weitere Details zu Apache finden sich in diesem Handbuch.

Als letzten Schritt muss man die Datei `cachemgr.cgi` in das Verzeichnis `cgi-bin` von Apache kopieren:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/usr/local/httpd/cgi-bin
```

Cache-Manager ACLs in `/etc/squid.conf`

Folgende Standardeinstellungen sind für den Cache-Manager erforderlich:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln sollten enthalten sein:

```
http_access allow manager localhost
http_access deny manager
```


Die erste ACL ist am wichtigsten, da der Cache-Manager versucht, mit dem Squid über das `cache_object`-Protokoll zu kommunizieren. Die folgenden Regeln setzen voraus, dass der Web-Server und Squid auf demselben Rechner laufen. Die Kommunikation zwischen dem Cache-Manager und Squid entsteht beim Web-Server, nicht beim Browser. Befindet sich der Web-Server also auf einem anderen Rechner, müssen Sie extra eine ACL wie in der Beispieldatei 30 hinzufügen.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP Webserver
```

Datei 30: Zugriffsregeln

Dann werden noch folgende Regeln aus Datei 31 benötigt.

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Datei 31: Zugriffsregeln

Es ist auch möglich, ein Passwort für den Manager zu konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie z. B. Schließen des Cache von Remote oder Anzeigen weiterer Informationen über den Cache. Dann müssen Sie den Eintrag `cachemgr_passwd` und die Optionenliste, die angezeigt werden soll, mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragskommentare in `/etc/squid.conf`.

Immer wenn sich die Konfigurationsdatei geändert hat, muss Squid mit der Option `-k reconfigure` neu gestartet werden.

Statistiken anzeigen

Gehen Sie zur entsprechenden Web-Seite, z. B.:

<http://webserver.example.org/cgi-bin/cachemgr.cgi>

Drücken Sie auf 'continue' und lassen Sie sich die verschiedenen Statistiken anzeigen. Weitere Informationen über die einzelnen Einträge, die vom Cache-Manager ausgegeben werden, finden sich in den FAQs zu Squid: <http://www.squid-cache.org/Doc/FAQ/FAQ-9.html>

SquidGuard

Dieses Kapitel soll lediglich eine Einführung zur Konfiguration von SquidGuard sowie ein paar Ratschläge zu dessen Einsatz geben. Auf eine umfangreiche Erklärung wird an dieser Stelle verzichtet. Tiefer gehende Informationen finden sich auf den Webseiten zu SquidGuard: <http://www.squidguard.org>

SquidGuard ist ein freier (GPL), flexibler und ultraschneller Filter, ein Umleiter und „Zugriffs-Controller-PlugIn“ für Squid. Er ermöglicht das Festlegen einer Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen für einen Squid-Cache. SquidGuard verwendet die Standardschnittstelle von Squid zum Umleiten.

squidGuard kann u. a. für Folgendes verwendet werden:

- Beschränkung des Internetzugriffs für einige Benutzer auf bestimmte akzeptierte/bekannte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf bestimmte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf URLs, die bestimmte reguläre Ausdrücke oder Wörter enthalten.
- Umleiten gesperrter URLs an eine „intelligente“ CGI-basierte Infoseite.
- Umleiten nicht registrierter Benutzer an ein Registrierungsformular.
- Umleiten von Bannern an ein leeres GIF.
- Unterschiedliche Zugriffsregeln abhängig von der Uhrzeit, dem Wochentag, dem Datum etc.
- Unterschiedliche Regeln für die einzelnen Benutzergruppen.

Weder mit squidGuard noch mit Squid ist Folgendes möglich:

- Text innerhalb von Dokumenten filtern, zensieren oder editieren.
- In HTML eingebettete Skriptsprachen wie JavaScript oder VBscript filtern, zensieren oder editieren.

Verwendung von SquidGuard

Installieren Sie das Paket `squidgrd`. Editieren Sie die Konfigurationsdatei `/etc/squidguard.conf`. Es gibt zahlreiche andere Konfigurationsbeispiele unter <http://www.squidguard.org/config/>. Sie können später mit komplizierteren Konfigurationseinstellungen experimentieren.

Der nächste Schritt besteht darin, eine Dummy-Seite „Zugriff verweigert“ oder eine mehr oder weniger intelligente CGI-Seite zu erzeugen, um Squid umzuleiten, falls der Client eine verbotene Webseite anfordert. Der Einsatz von Apache wird auch hier wieder empfohlen.

Nun müssen wir Squid sagen, dass er SquidGuard benutzen soll. Dafür verwenden wir folgende Einträge in der Datei `/etc/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine andere Option namens `redirect_children` konfiguriert die Anzahl der verschiedenen auf dem Rechner laufenden „redirect“, also Umleitungsprozesse (in diesem Fall SquidGuard). SquidGuard ist schnell genug, um eine Vielzahl von Anfragen (SquidGuard ist wirklich schnell: 100.000 Anfragen innerhalb von 10 Sekunden auf einem 500MHz Pentium mit 5900 Domains, 7880 URLs, gesamt 13780) zu bearbeiten. Es wird daher nicht empfohlen, mehr als 4 Prozesse festzusetzen, da die Zuweisung dieser Prozesse unnötig viel Speicher braucht.

```
redirect_children 4
```

Als Letztes senden Sie ein HUP-Signal zum Squid, damit die neue Konfiguration eingelesen wird:

```
squid -k reconfigure
```

Nun können Sie Ihre Einstellungen in einem Browser testen.

Erzeugen von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, das zur Erzeugung von Aktivitätsberichten des Cache im ASCII- oder HTML-Format verwendet wird. Es arbeitet mit Squid-eigenen Zugriffsprotokolldateien. Die Homepage zu Calamaris befindet sich unter: <http://Calamaris.Cord.de/>

Das Programm ist einfach zu verwenden. Melden Sie sich als `root` an und geben Sie Folgendes ein:

```
cat access.log.files | calamaris [options] > reportfile
```

Beim Verketteten mehrerer Protokolldateien ist die Beachtung der chronologischen Reihenfolge wichtig, d. h. ältere Dateien kommen zuerst.

Die verschiedenen Optionen:

- a wird normalerweise zur Ausgabe aller verfügbaren Berichte verwendet, mit
- w erhält man einen HTML-Bericht und mit
- l eine Nachricht oder ein Logo im Header des Berichts.

Weitere Informationen über die verschiedenen Optionen finden Sie in der Manual Page zu calamaris: `man calamaris`

Ein übliches Beispiel:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \  
>/usr/local/httpd/htdocs/Squid/squidreport.html
```

Der Bericht wird im Verzeichnis des Web-Servers abgelegt. Wieder wird Apache benötigt, um die Berichte anzeigen zu können.

Ein weiteres, leistungsstarkes Tool zum Erzeugen von Cache-Berichten ist SARG (Squid Analysis Report Generator). Weitere Informationen dazu gibt es auf der entsprechenden Internetseite unter: <http://web.onda.com.br/orso/>

Weitere Informationen zu Squid

Besuchen Sie die Homepage von Squid: <http://www.squid-cache.org/>. Hier finden Sie den Squid User Guide und eine sehr umfangreiche Sammlung von FAQs zu Squid.

Das Mini-Howto zu einem transparenten Proxy im Paket howtoen, unter: `/usr/share/doc/howto/en/mini/TransparentProxy.gz`

Des Weiteren gibt es Mailinglisten für Squid unter: squid-users@squid-cache.org.

Das Archiv dazu befindet sich unter: <http://www.squid-cache.org/mail-archive/squid-users/>

Sicherheit im Netzwerk

Masquerading, Firewall und Kerberos bilden die Grundlagen für ein sicheres Netzwerk, welche für einen kontrollierten Datenverkehr sorgen. Die Secure Shell (SSH) gibt dem Benutzer die Möglichkeit, über eine verschlüsselte Verbindung auf entfernten Rechner sich anzumelden.

| | |
|--|-----|
| Masquerading und Firewall | 292 |
| SSH – secure shell, die sichere Alternative | 297 |
| Netzwerkauthentifizierung — Kerberos | 303 |
| Installation und Administration von Kerberos | 311 |
| Sicherheit ist Vertrauenssache | 327 |

Masquerading und Firewall

Wegen seiner herausragenden Netzwerkfähigkeiten wird Linux immer häufiger als Router für Wählleitungen oder auch Standleitungen verwendet. Der Begriff „Router“ bezieht sich hierbei auf einen Rechner, der mehr als ein Netzwerkinterface hat und der Pakete, die nicht für eines seiner eigenen Netzwerkinterfaces bestimmt sind, an seine jeweiligen Kommunikationspartner weiterleitet. Ein Router wird häufig auch „gateway“ genannt. Die im Linux-Kernel vorhandenen Paketfilter ermöglichen eine präzise Steuerung dafür, welche Pakete des Datenverkehrs nun passieren dürfen und welche nicht.

Das Festlegen der genauen Filterregeln für diesen Paketfilter erfordert in der Regel etwas Erfahrung seitens des Administrators. SuSE Linux hält für den weniger erfahrenen Benutzer ein Paket `SuSEfirewall2` bereit, das das Einstellen dieser Regeln erleichtert.

Die `SuSEfirewall2` ist sehr flexibel konfigurierbar und eignet sich deswegen auch zum Aufbau von komplexeren Paketfilterkonstrukten. Das Paketfilter-Paket erlaubt es, einen Linux-Rechner mittels Masquerading als Router zur Anbindung eines internen Netzwerks mit nur einer einzigen von außen sichtbaren IP-Adresse zu betreiben. Masquerading wird also mit Hilfe von Regeln eines Paketfilters realisiert.

Achtung

Die hier vorgestellten Verfahren gelten als Standard und funktionieren in der Regel. Es gibt jedoch keine Garantie dafür, dass sich nicht doch in diesem Buch oder woanders ein Fehler eingeschlichen hat. Sollten Cracker trotz umfassender korrekter Schutzmaßnahmen Ihrerseits in Ihr System eindringen, dann machen Sie bitte nicht die Buchautoren verantwortlich. Auch wenn Sie nicht direkt eine Antwort erhalten, können Sie sicher sein, dass wir für Kritik und Anregungen dankbar sind und Verbesserungen einbringen werden.

Achtung

Grundlagen des Masquerading

Masquerading ist der Linux-Spezialfall von NAT (engl. *Network Address Translation*) der Übersetzung von Netzwerkadressen. Das Prinzip dahinter ist nicht sonderlich kompliziert: Ihr Router hat mehr als ein Netzwerkinterface, typischerweise sind das eine Netzkarte und eine Schnittstelle zum Internet (z.B. ein ISDN-Interface). Eines dieser Interfaces wird Sie nach außen anbinden, eines

oder mehrere andere verbinden Ihren Rechner mit den weiteren Rechnern in Ihrem Netz. In einem Beispiel soll nun per ISDN nach außen eingewählt werden, das äußere Netzwerkinterface ist `ipp0`. Sie haben mehrere Rechner im lokalen Netz mit der Netzwerkkarte Ihres Linux-Routers verbunden, die in diesem Beispiel `eth0` heißt. Die Rechner im Netz senden alle Pakete, die nicht für das eigene Netz bestimmt sind, an den Default-Router oder das Default-Gateway.

Hinweis

Achten Sie beim Konfigurieren Ihres Netzwerks immer auf übereinstimmende broadcast-Adressen und Netzwerkmasken!

Hinweis

Wird nun einer der Rechner in Ihrem Netz ein Paket fürs Internet abschicken, dann landet es beim Default-Router. Dieser muss so konfiguriert sein, dass er solche Pakete auch weiterleitet. Aus Sicherheitsgründen wird eine SuSE-Linux Installation dies nicht tun! Ändern Sie die Variable `IP_FORWARD` in der Datei `/etc/sysconfig/network/options` auf `IP_FORWARD=yes`. Nach einem Reboot oder dem folgenden Kommando ist das Weiterleiten aktiviert:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Der Zielrechner der Verbindung kennt nur Ihren Router, nicht aber den eigentlichen Absender-Rechner in Ihrem inneren Netzwerk, der hinter Ihrem Router versteckt ist. Daher kommt der Begriff „Masquerading“. Die Zieladresse für Antwortpakete ist wegen der Adressübersetzung wieder unser Router. Dieser muss die Pakete erkennen und die Zieladresse so umschreiben, dass sie zum richtigen Rechner im lokalen Netz gelangen.

Diese Erkennung von Paketen, die zu Verbindungen gehören, die durch Masquerading durch den Router entstanden sind, geschieht mit Hilfe einer Tabelle, die direkt im Kernel Ihres Routers gehalten wird, solange die dazugehörigen Verbindungen aktiv sind. Diese Tabelle kann der Superuser (`root`) sogar mit den Kommandos `ipchains` oder `iptables` einsehen. Bitte konsultieren Sie die Manpages dieser Kommandos für genauere Anleitungen. Für die Identifizierung einzelner Masquerade Verbindungen sind neben Absender- und Zieladresse auch Port-Nummern und die beteiligten Protokolle an sich relevant. Damit ist es möglich, dass Ihr Router für jeden einzelnen Ihrer lokalen Rechner viele Tausend Verbindungen gleichzeitig „verstecken“ kann.

Da der Weg der Pakete von außen nach innen von der Masquerading-Tabelle abhängt, gibt es keine Möglichkeit, von außen eine Verbindung nach innen zu öffnen. Für diese Verbindung gäbe es keinen Eintrag in der Tabelle. Eine etablierte Verbindung hat darüber hinaus in der Tabelle einen zugeordneten Status, so dass dieser Tabelleneintrag nicht von einer zweiten Verbindung genutzt werden kann.

In der Folge ergeben sich nun Probleme mit manchen Anwendungen, zum Beispiel ICQ, cucme, IRC (DCC, CTCP), Quake und FTP (im PORT-Mode). Netscape, das Standard-FTP-Programm und viele andere benutzen den PASV-Modus, der im Zusammenhang mit Paketfiltern und Masquerading weit weniger problembehaftet ist.

Grundlagen Firewalling

„Firewall“ ist wohl der am weitesten verbreitete Begriff für einen Mechanismus, der zwei Netze miteinander verbindet, aber für möglichst kontrollierten Datenverkehr sorgt. Es gibt verschiedene Bauarten von Firewalls, die sich hauptsächlich in der logisch-abstrakten Ebene unterscheiden, auf der sie den Datenverkehr untersuchen und regulieren. Die Methode, die wir hier vorstellen, müsste sich eigentlich genauer „Paketfilter“ nennen. Ein Paketfilter regelt den Durchlass anhand von Kriterien wie Protokoll, Port und IP-Adresse. Auf diese Weise können Sie also Pakete abfangen, die aufgrund ihrer Adressierung nicht in Ihr Netz durchdringen sollen. Beispielsweise sollten Sie Pakete abfangen, die den telnet-Dienst Ihrer Rechner auf port 23 zum Ziel haben. Wenn Sie beispielsweise Zugriffe auf Ihren Webserver zulassen wollen, müssen Sie den dazugehörigen Port freischalten. Der Inhalt dieser Pakete, falls sie legitim adressiert sind (also beispielsweise mit Ihrem Webserver als Ziel), wird nicht untersucht. Das Paket könnte insofern einen Angriff auf ein CGI-Programm auf Ihrem Webserver enthalten und wird vom Paketfilter durchgelassen.

Ein wirksames — wenn auch komplexeres — Konstrukt ist die Kombination von mehreren Bauarten, beispielsweise ein Paketfilter mit zusätzlichem Application Gateway/Proxy. Der Paketfilter wehrt Pakete ab, die zum Beispiel an nicht freigeschaltete Ports gerichtet sind. Nur Pakete für ein Application Gateway sollen durchgelassen werden. Dieses Proxy tut nun so, als wäre es der eigentliche Kommunikationspartner des Servers, der mit uns eine Verbindung herstellt. In diesem Sinne kann ein solches Proxy als eine Masquerading-Maschine auf der Ebene des Protokolls der jeweiligen Anwendung angesehen werden. Ein Beispiel für solch ein Proxy ist Squid, ein HTTP Proxy Server, für den Sie Ihren Browser so konfigurieren müssen, dass Anfragen für HTML-Seiten zuerst an den Speicher des Proxy gehen und nur, wenn dort die Seite nicht zu finden ist, in das Internet geschickt werden. Die SuSE proxy suite (das Paket `proxy-suite`) enthält übrigens einen Proxy-Server für das FTP-Protokoll.

Im Folgenden wollen wir uns auf das Paketfilter-Paket bei SuSE-Linux konzentrieren. Für mehr Informationen und weitere Links zum Thema Firewall lesen Sie bitte das Firewall-HOWTO, enthalten im Paket `howtode`. Es lässt sich mit dem Kommando

`less /usr/share/doc/howto/de/DE-Firewall-HOWTO.txt.gz` lesen, wenn das Paket `howtode` installiert ist.

SuSEfirewall2

Die Konfiguration der SuSEfirewall2 erfordert einiges an Wissen und Erfahrung. Unter `/usr/share/doc/packages/SuSEfirewall12` finden Sie Dokumentation zur SuSEfirewall2.

Die Konfiguration lässt sich entweder mit Yast2 vornehmen ('Sicherheit' → 'Firewall') oder kann direkt in der Datei `/etc/sysconfig/SuSEfirewall12` erfolgen, die ausführliche englische Kommentare enthält. Wir werden Ihnen nun Schritt für Schritt eine erfolgreiche Konfiguration vorführen. Es ist bei jedem Punkt angeführt, ob er für Masquerading oder Firewall gilt. In der Konfigurationsdatei ist auch von einer DMZ („Demilitarisierte Zone“) die Rede, auf die an dieser Stelle nicht näher eingegangen wird.

Falls Sie wirklich nicht mehr als Masquerading brauchen, füllen Sie nur die mit *Masquerading* bezeichneten Zeilen aus.

- Aktivieren Sie zunächst mit dem Yast2 Runlevel Editor die SuSEfirewall2 für Ihren Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die `SuSEfirewall2_*` Skripten in den Verzeichnissen `/etc/init.d/rc?.d/` angelegt.
- `FW_DEV_WORLD` (Firewall, Masquerading): Zum Beispiel `eth0`, als Device, das ins Internet führt. Bei ISDN ist es z. B. `ipp0`.
- `FW_DEV_INT` (Firewall, Masquerading): Geben Sie hier das Device an, das ins innere, „private“ Netz zeigt. Falls kein inneres Netz vorhanden ist, einfach leer lassen.
- `FW_ROUTE` (Firewall, Masquerading): Wenn Sie Masquerading brauchen, müssen Sie hier auf jeden Fall `yes` eintragen. Ihre internen Rechner sind nicht von außen sichtbar, da diese private Netzwerkadressen (z. B. `192.168.x.x`) haben, die im Internet gar nicht geroutet werden.
Bei einer Firewall ohne Masquerading wählen Sie hier nur dann `yes`, wenn Sie Zugang zum internen Netz erlauben wollen. Dazu müssen die internen Rechner offiziell zugewiesene IP-Adressen haben. Im Normalfall sollten Sie allerdings den Zugang von außen auf die internen Rechner *nicht* erlauben!
- `FW_MASQUERADE` (Masquerading): Wenn Sie Masquerading brauchen, müssen Sie hier `yes` eintragen. Beachten Sie, dass es sicherer ist, wenn die Rechner des internen Netzes über Proxy-Server auf das Internet zugreifen.

- `FW_MASQ_NETS` (Masquerading): Tragen Sie hier die Rechner oder Netzwerke ein, für die Masquerading vorgenommen werden soll. Trennen Sie die einzelnen Einträge durch Leerzeichen. Zum Beispiel: `FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"`
- `FW_PROTECT_FROM_INTERNAL` (Firewall): Tragen Sie hier `yes` ein, wenn Sie den Firewall-Rechner auch durch Angriffe vom inneren Netz schützen wollen. Dann müssen Sie die Services, die für das innere Netz verfügbar sind, explizit freigeben. Siehe auch `FW_SERVICES_INTERNAL_TCP` und `FW_SERVICES_INTERNAL_UDP`.
- `FW_AUTOPROTECT_GLOBAL_SERVICES` (Firewall): Im Normalfall auf `yes` lassen.
- `FW_SERVICES_EXTERNAL_TCP` (Firewall): Tragen Sie hier die Services ein, auf die zugegriffen werden soll; z. B. `"www smtp ftp domain 443"` – für den Rechner zu Hause, der keine Dienste anbieten soll, tragen Sie meist nichts ein.
- `FW_SERVICES_EXTERNAL_UDP` (Firewall): Wenn Sie nicht gerade einen Nameserver betreiben, auf den von außen zugegriffen werden soll, lassen Sie dieses Feld leer. Ansonsten fügen Sie hier die benötigten Ports ein.
- `FW_SERVICES_INTERNAL_TCP` (Firewall): Hier werden die für das innere Netz zur Verfügung stehenden Dienste deklariert. Die Angaben sind analog zu denen unter `FW_SERVICES_EXTERNAL_TCP`, beziehen sich hier aber auf das *interne* Netz.
- `FW_SERVICES_INTERNAL_UDP` (Firewall): Siehe oben.
- `FW_TRUSTED_NETS` (Firewall): Hier tragen Sie die Rechner ein, denen Sie *wirklich* vertrauen können („Trusted Hosts“). Beachten Sie zudem, dass auch diese Rechner vor Eindringlingen geschützt sein müssen. `"172.20.0.0/16 172.30.4.2"` bedeutet, dass alle Rechner, deren IP-Adresse mit `172.20.x.x` beginnt, sowie der Rechner mit der IP-Adresse `172.30.4.2` durch die Firewall hindurch können.
- `FW_SERVICES_TRUSTED_TCP` (Firewall): Hier legen Sie die TCP-Portadressen fest, die von den „Trusted Hosts“ benutzt werden können. Geben Sie z. B. `1:65535` ein, wenn die vertrauenswürdigen Rechner auf alle Services zugreifen dürfen. Normalerweise sollte es reichen, wenn man hier als Service `ssh` eingibt.
- `FW_SERVICES_TRUSTED_UDP` (Firewall): Wie oben, nur auf UDP bezogen.

- `FW_ALLOW_INCOMING_HIGHPORTS_TCP` (Firewall): Wenn Sie mit normalem (aktivem) FTP arbeiten wollen, so tragen Sie hier `ftp-data` ein.
- `FW_ALLOW_INCOMING_HIGHPORTS_UDP` (Firewall): Tragen Sie hier `dns` ein, damit Sie die in `/etc/resolv.conf` eingetragenen Nameserver verwenden können. Mit `yes` geben Sie alle hohen Portnummern frei.
- `FW_SERVICE_DNS` (Firewall): Falls bei Ihnen ein Nameserver läuft, auf den von außen zugegriffen werden soll, tragen Sie hier `yes` ein; in `FW_TCP_SERVICES_*` muss zugleich der Port 53 freigeschaltet sein.
- `FW_SERVICE_DHCLIENT` (Firewall): Wenn Sie `dhclient` benutzen, um Ihre IP-Adresse zu beziehen, so müssen Sie hier `yes` eintragen.
- `FW_LOG_*`: Stellen Sie hier ein, was Sie mitloggen wollen. Für den laufenden Betrieb reicht `yes` bei `FW_LOG_DENY_CRIT`.
- `FW_STOP_KEEP_ROUTING_STATE` (Firewall): Falls Sie automatisch per `cidld` oder über ISDN (dial on demand) ins Internet gehen, so tragen Sie hier `yes` ein.

Damit ist die Konfiguration abgeschlossen. Vergessen Sie nicht, die Firewall zu testen (z. B. `telnet` von außen); Sie sollten dann in `/var/log/messages` in etwa folgende Einträge sehen:

```
Feb  7 01:54:14 www kernel: Packet log: input DENY eth0
PROTO=6 129.27.43.9:1427 195.58.178.210:23 L=60 S=0x00
I=36981 F=0x4000 T=59 SYN (#119)
```

SSH – secure shell, die sichere Alternative

In unserer Zeit der immer stärkeren Vernetzung werden auch Zugriffe auf entfernte Systeme immer häufiger. Dabei muss immer eine Authentifikation der Person erfolgen.

In der Regel sollten Nutzer heutzutage verinnerlicht haben, dass ihr Benutzername und ihr Kennwort lediglich für sie allein gedacht sind. Eine entsprechende Vereinbarung zwischen Arbeitgeber, Rechenzentrum oder Serviceanbieter über die Personengebundenheit dieser Daten ist Standard.

Erschreckend ist demgegenüber die weitgehende Praxis, dass Authentifizierung und Datenübertragung weiterhin in Form von Klartextdaten erfolgt. Die ist beispielsweise der Fall, wenn mit `Post Office Protocol (POP)` E-Mail

abgeholt wird oder man sich mit `telnet` auf einem entfernten System anmeldet. Hierbei gehen die in den Nutzungsbedingungen als sensibel eingestuften Nutzerinformationen und Daten, z. B. der Inhalt eines Briefes, oder ein per `talk`-Kommando geführtes Gespräch, ohne jeden Schutz offen über das Netzwerk. Dies beeinträchtigt einerseits die Privatsphäre des Nutzers und eröffnet andererseits die Möglichkeit zum Missbrauch eines Zugangs. Insbesondere werden solche Zugänge gern benutzt, um von dort aus andere Systeme anzugreifen, oder Administrator- bzw. Rootrechte auf diesem System zu erlangen.

Jedes an der Weiterleitung der Daten beteiligte oder im gleichen lokalen Netz betriebene Gerät wie Firewall, Router, Switch, Mailserver, Arbeitsplatzrechner, etc., kann die Daten zusätzlich einsehen. Grundsätzlich untersagen zwar die geltenden rechtlichen Regelungen ein solches Vorgehen, stellen es sogar unter Strafe, jedoch sind derartige Angriffe oder unberechtigte Einsichtnahmen nur schwer festzustellen und nachzuweisen.

Die SSH-Software liefert hier den gewünschten Schutz. Die komplette Authentifizierung, in der Regel Benutzername und Passwort, und die Kommunikation erfolgen hier verschlüsselt. Zwar ist auch hier weiterhin das Mitschneiden der übertragenen Daten möglich, doch kann der Inhalt mangels fehlendem Schlüssels durch einen Unwissenden nicht wieder entschlüsselt werden. So wird sichere Kommunikation über unsichere Netze wie das Internet möglich. SuSE Linux Desktop bietet das Paket `openssh` an.

Das OpenSSH-Paket

Per Default wird unter SuSE Linux das Paket OpenSSH installiert. Es stehen Ihnen daher die Programme `ssh`, `scp` und `sftp` als Alternative für `telnet`, `rlogin`, `rsh`, `rcp` und `ftp` zur Verfügung.

Das ssh-Programm

Mit dem `ssh`-Programm können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ist somit gleichermaßen ein Ersatz für `telnet` und `rlogin`. Aufgrund der Verwandtschaft zu `rlogin` zeigt der zusätzliche symbolische Name `slogin` ebenfalls auf `ssh`. Zum Beispiel kann man sich mit dem Befehl `ssh sonne` auf dem Rechner `sonne` anmelden. Anschließend wird man nach seinem Passwort auf dem System `sonne` gefragt.

Nach erfolgreicher Authentifizierung kann dort auf der Kommandozeile oder interaktiv, z. B. mit dem SuSE- Administrationsprogramm YaST, gearbeitet werden. Sollten sich der lokale Benutzername und der auf dem entfernten System unterscheiden, kann ein abweichender Name angegeben werden, z. B. `ssh -l august sonne` oder `ssh august@sonne`.

Darüber hinaus bietet ssh die von rsh bekannte Möglichkeit, Kommandos auf einem anderen System auszuführen. Im nachfolgenden Beispiel wird das Kommando `uptime` auf dem Rechner `sonne` ausgeführt und ein Verzeichnis mit dem Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Rechners `erde`.

```
tux@erde:~ > ssh sonne "uptime; mkdir tmp"
tux@sonne's password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

Anführungszeichen sind hier zum Zusammenfassen der beiden Anweisungen in einem Kommando erforderlich. Nur so wird auch der zweite Befehl auf dem Rechner `sonne` ausgeführt.

scp – sicheres Kopieren

Mittels `scp` kopieren Sie Dateien auf einen entfernten Rechner. `scp` ist der sichere, verschlüsselte Ersatz für `rcp`. Zum Beispiel kopiert `scp MeinBrief.tex sonne:` die Datei `MeinBrief.tex` vom Rechner `erde` auf den Rechner `sonne`. Insoweit sich die beteiligten Nutzernamen auf `erde` und `sonne` unterscheiden, geben Sie bei `scp` die Schreibweise `Nutzername@Rechnername` an. Eine Option `-l` existiert nicht.

Nachdem das Passwort eingegeben wurde, beginnt `scp` mit der Datenübertragung und zeigt dabei den Fortschritt anhand eines von links nach rechts anwachsenden Balkens aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (engl. *estimated time of arrival*) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

`scp` bietet neben dem Kopieren einzelner Dateien ein rekursives Verfahren zum Übertragen ganzer Verzeichnisse: `scp -r src/ sonne:backup/`

kopiert den kompletten Inhalt des Verzeichnisses `src/` inklusive aller Unterverzeichnisse auf den Rechner `sonne` und dort in das Unterverzeichnis `backup/`. Dieses wird automatisch angelegt wenn es fehlt.

Mittels der Option `-p` kann `scp` die Zeitstempel der Dateien erhalten. `-C` sorgt für eine komprimierte Übertragung. Dadurch wird einerseits das zu übertragende Datenvolumen minimiert, andererseits aber ein höherer Rechenaufwand erforderlich.

sftp - sicherere Dateiübertragung

Alternativ kann man zur sicheren Datenübertragung `sftp` verwenden. `sftp` bietet innerhalb der Sitzung viele der von `ftp` bekannten Kommandos. Gegenüber `scp`

mag es vor allem beim Übertragen von Daten, deren Dateinamen unbekannt sind, von Vorteil sein.

Der SSH Daemon (sshd) – die Serverseite

Damit ssh und scp, die Clientprogramme des SSH-Paketes, eingesetzt werden können, muss im Hintergrund der SSH-Daemon, ein Server, laufen. Dieser erwartet seine Verbindungen auf TCP/IP Port 22.

Während des ersten Starts generiert der Daemon drei Schlüsselpaare. Die Schlüsselpaare bestehen aus einem privaten und einem öffentlichen (engl. *public*) Teil. Deshalb bezeichnet man dies als ein public-key basiertes Verfahren. Um die Sicherheit der Kommunikation mittels SSH zu gewährleisten, darf ausschließlich der Systemadministrator die Dateien der privaten Schlüssel einsehen können. Die Dateirechte werden per Voreinstellung entsprechend restriktiv gesetzt. Die privaten Schlüssel werden lediglich lokal vom SSH-Daemon benötigt und dürfen an niemanden weitergegeben werden. Demgegenüber werden die öffentlichen Schlüsselbestandteile (an der Namensendung *.pub* erkennbar) an Kommunikationspartner weitergegeben und sind entsprechend für alle Benutzer lesbar.

Eine Verbindung wird vom SSH-Client eingeleitet. Der wartende SSH-Daemon und der anfragende SSH-Client tauschen Identifikationsdaten aus, um die Protokoll- und Softwareversion abzugleichen und die Verbindung zu einem falschen Port auszuschließen. Da ein Kindprozess des ursprünglichen SSH-Daemons antwortet, sind gleichzeitig viele SSH-Verbindungen möglich.

Zur Kommunikation zwischen SSH-Server und SSH-Client steht das SSH Protokoll in Version 1 und 2 zur Verfügung.

Bei Verwendung der SSH Protokoll Version 1 sendet der Server sodann seinen öffentlichen *host key* und einen stündlich vom SSH-Daemon neu generierten *server key*. Mittels beider verschlüsselt (engl. *encrypt*) der SSH-Client einen von ihm frei gewählten Sitzungsschlüssel (engl. *session key*) und sendet ihn an den SSH-Server. Er teilt dem Server zudem die gewählte Verschlüsselungsmethode (engl. *cipher*) mit.

Die SSH Protokoll Version 2 kommt ohne den *server key* aus. Stattdessen wird ein Algorithmus nach Diffie-Hellman verwendet, um die Schlüssel auszutauschen.

Die zur Entschlüsselung des Sitzungsschlüssels zwingend erforderlichen privaten *host* und *server keys*, können nicht aus den öffentlichen Teilen abgeleitet werden. Somit kann allein der kontaktierte SSH-Daemon mit seinen privaten Schlüsseln den Sitzungsschlüssel entziffern (vgl. */usr/share/doc/*

`packages/openssh/RFC.nroff`). Diese einleitende Phase der Verbindung kann man mittels der Fehlersuchoption `-v` des SSH-Clientprogramms gut nachvollziehen. Per Default wird SSH Protokoll Version 2 verwendet, man kann jedoch mit dem Parameter `-1` auch die SSH Protokoll Version 1 erzwingen. Indem der Client alle öffentlichen host keys nach der ersten Kontaktaufnahme in `~/.ssh/known_hosts` ablegt, können so genannte „man-in-the-middle“-Angriffe unterbunden werden. SSH-Server, die versuchen, Name und IP-Adresse eines anderen vorzutäuschen, werden durch einen deutlichen Hinweis enttarnt. Sie fallen entweder durch einen gegenüber `~/.ssh/known_hosts` abweichenden host-Schlüssel auf, oder können mangels passendem privaten Gegenstück den vereinbarten Sitzungsschlüssel nicht entschlüsseln.

Es empfiehlt sich, die in `/etc/ssh/` abgelegten privaten und öffentlichen Schlüssel extern und gut geschützt zu archivieren. So können Änderungen der Schlüssel festgestellt und nach einer Neuinstallation die alten wieder eingespielt werden. Dies erspart den Benutzern die beunruhigende Warnung. Ist es sichergestellt, dass es sich trotz der Warnung um den korrekten SSH-Server handelt, muss der vorhandene Eintrag zu diesem System aus `~/.ssh/known_hosts` entfernt werden.

SSH-Authentifizierungsmechanismen

Jetzt erfolgt die eigentliche Authentifizierung, die in ihrer einfachsten Weise aus der Eingabe eines Passwortes besteht, wie es in den oben aufgezeigten Beispielen erfolgte. Ziel von SSH war die Einführung einer sicheren, aber zugleich einfach zu nutzenden Software. Wie bei den abzulösenden Programmen `rsh` und `rlogin` muss deshalb auch SSH eine im Alltag einfach zu nutzende Authentifizierungsmethode bieten. SSH realisiert dies mittels eines weiteren hier vom Nutzer erzeugten Schlüsselpaares. Dazu liefert das SSH-Paket das Hilfsprogramm `ssh-keygen` mit. Nach der Eingabe von `ssh-keygen -t rsa` oder `ssh-keygen -t dsa` wird das Schlüsselpaar generiert und der Basisdateiname zur Ablage der Schlüssel erfragt:

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Bestätigen Sie die Voreinstellung und beantworten Sie die Frage nach einer Passphrase. Auch wenn die Software eine leere Passphrase nahelegt, sollte bei der hier vorgeschlagenen Vorgehensweise ein Text von zehn bis 30 Zeichen Länge gewählt werden. Verwenden Sie möglichst keine kurzen und einfachen Worte oder Sätze. Nach erfolgter Eingabe wird zur Bestätigung eine Wiederholung der Eingabe verlangt. Anschließend wird der Ablageort des privaten und öffentlichen Schlüssels, in unserem Beispiel der Dateien `id_rsa` und `id_rsa.pub`, ausgegeben.

```
Enter same passphrase again:
Your identification has been saved in /home/tux/.ssh/id_rsa
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@sonne
```

Verwenden Sie `ssh-keygen -p -t rsa` bzw. `ssh-keygen -p -t dsa`, um Ihre alte Passphrase zu ändern. Kopieren Sie den öffentlichen Teil des Schlüssels (in unserem Beispiel `id_rsa.pub`) auf den entfernten Rechner und legen Sie ihn dort als `~/.ssh/authorized_keys2` ab. Zur Authentifizierung werden Sie beim nächsten Verbindungsaufbau nach Ihrer Passphrase gefragt. Sollte dies nicht der Fall sein, überprüfen Sie bitte Ort und Inhalt der zuvor erwähnten Dateien.

Auf Dauer ist diese Vorgehensweise mühsamer, als die Eingabe eines Passwortes. Entsprechend liefert das SSH-Paket ein weiteres Hilfsprogramm, den `ssh-agent`, der für die Dauer einer „X-session“ private Schlüssel bereit hält. Dazu wird das gesamte X als Kindprozess des `ssh-agent`s gestartet. Sie erreichen dies am einfachsten, indem Sie am Anfang der Datei `.xsession` die Variable `usessh` auf `yes` setzen und sich über einen Displaymanager, z. B. KDM oder XDM, anmelden. Alternativ können Sie `ssh-agent startx` verwenden.

Nun können Sie wie gewohnt `ssh` oder `scp` nutzen. Insoweit Sie Ihren öffentlichen Schlüssel wie zuvor verteilt haben, sollten Sie jetzt nicht mehr nach dem Passwort gefragt werden. Achten Sie beim Verlassen Ihres Rechners darauf, dass Sie Ihre X-session beenden oder mittels einer passwortgeschützten Bildschirmsperre, z. B. `xlock`, verriegeln.

Alle wichtigen Änderungen die sich mit der Einführung von SSH Protokoll Version 2 ergeben haben, wurden auch in der Datei `/usr/share/doc/packages/openssh/README.SuSE` noch einmal dokumentiert.

X-, Authentifizierungs- und sonstige Weiterleitung

Über die bisher beschriebenen sicherheitsrelevanten Verbesserungen hinaus erleichtert `ssh` auch die Verwendung von entfernten X-Anwendungen. Insoweit Sie `ssh` mit der Option `-X` aufrufen, wird auf dem entfernten System automatisch die `DISPLAY`-Variable gesetzt und alle X-Ausgaben werden durch die bestehende `ssh`-Verbindung auf den Ausgangsrechner weitergeleitet. Diese bequeme Funktion unterbindet gleichzeitig die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch die gesetzte Option `-A` wird der `ssh-agent`-Authentifizierungsmechanismus auf den nächsten Rechner mit übernommen. Man kann so von

einem Rechner zum anderen gehen, ohne ein Passwort eingeben zu müssen. Allerdings nur, wenn man zuvor seinen öffentlichen Schlüssel auf die beteiligten Zielrechner verteilt und korrekt abgelegt hat.

Beide Mechanismen sind vorsichtshalber in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config` oder der nutzeigenen `~/.ssh/config` permanent eingeschaltet werden.

Man kann `ssh` auch zur beliebigen Umleitung von TCP/IP-Verbindungen benutzen. Als Beispiel sei hier die Weiterleitung des SMTP- und POP3-Ports aufgeführt: `ssh -L 25:sonne:25 sonne` Hier wird jede Verbindung zu „erde Port 25“, SMTP auf den SMTP-Port von `sonne` über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere für Nutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Fähigkeiten von Nutzen. Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den „heimischen“ Mailserver übertragen werden.

Analog leitet `ssh -L 110:sonne:110 sonne` alle Port 110, POP3-Anfragen an `erde` auf den POP3-Port von `sonne` weiter.

Beide Beispiele müssen Sie als Nutzer `root` ausführen, da auf privilegierte lokale Ports verbunden wird. Bei bestehender SSH-Verbindung wird die Post wie gewohnt als normaler Nutzer versandt und abgeholt. Der SMTP- und POP3-Host muss dabei auf `localhost` konfiguriert werden.

Zusätzliche Informationen können den Manualpages der einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh` entnehmen werden.

Netzwerkauthentifizierung — Kerberos

Ein offenes Netzwerk bietet außer den gewöhnlichen Passwortmechanismen — die von Natur aus unsicher sind — keinerlei Möglichkeit, um sicherzustellen, dass ein Arbeitsplatzrechner seine Benutzer eindeutig identifizieren kann. Das bedeutet, dass eine beliebige Person unter der Vorgabe einer anderen Identität dessen e-Mails abholen, auf dessen private Dateien zugreifen oder einen Dienst starten könnte. Ihre Netzwerkumgebung muss daher die folgenden Anforderungen erfüllen, um wirklich sicher zu sein:

- Lassen Sie alle Benutzer für jeden gewünschten Dienst ihre Identität nachweisen und stellen Sie sicher, dass niemand die Identität eines anderen Benutzers annehmen kann.

- Stellen Sie außerdem sicher, dass jeder Netzwerkserver seine Identität nachweist. Falls Sie dies nicht tun, könnte es einem Angreifer gelingen, sich als der von ihnen angefragte Server auszugeben und vertrauliche Informationen abfangen, die Sie dem Server senden. Dieser Vorgang wird als „Mutual Authentication“ (gegenseitige Authentifizierung) bezeichnet, weil sich der Client beim Server und der Server beim Client authentifiziert.

Durch stark verschlüsselte Authentifizierung hilft Ihnen Kerberos, die o.g. Anforderungen zu erfüllen. Die folgenden Abschnitte zeigen Ihnen, wie dies erreicht wird. Bitte beachten Sie, dass hier nur die grundlegende Arbeitsweise von Kerberos dargelegt wird. Ausführlichere technische Anweisungen sind in der mit Ihrer Kerberos-Implementierung mitgelieferten Dokumentation enthalten.

Hinweis

Das ursprüngliche Kerberos wurde am MIT entwickelt. Neben MIT Kerberos existieren noch verschiedene andere Implementierungen von Kerberos. SuSE Linux Desktop enthält eine freie Implementierung von Kerberos 5, das sogenannte Heimdal Kerberos 5 von KTH. Da sich der folgende Text auf gemeinsame Eigenschaften aller Kerberi bezieht, bezeichnen wir das Programm als Kerberos, es sei denn, es handelt sich um spezifische Information über Heimdal.

Hinweis

Kerberos-Terminologie

Bevor wir auf die Einzelheiten von Kerberos eingehen, wollen wir einen Blick auf das folgende Glossar werfen, das Ihnen helfen wird, mit der Kerberos-Terminologie zurechtzukommen.

Credential Benutzer oder Clients müssen Credentials (Berechtigungsnachweise) vorweisen können, die sie berechtigen, Dienste anzufordern. Kerberos kennt zwei Arten von Berechtigungsnachweisen — Tickets und Authenticators.

Ticket Ein Ticket ist ein serverbezogener Berechtigungsnachweis, den ein Client benutzt, um sich bei einem Server zu authentifizieren, von dem er einen Dienst anfordert. Es enthält den Namen des Servers, den Namen des Clients, die Internetadresse des Clients, einen Zeitstempel (engl. *timestamp*), eine Lebensdauer und einen zufällig generierten Session Key. Alle diese Daten werden mit dem Schlüssel des Servers verschlüsselt.

Authenticator In Verbindung mit dem Ticket wird ein Authenticator benutzt, um zu beweisen, dass der Client, der ein Ticket vorlegt, tatsächlich derjenige ist, der er zu sein vorgibt. Ein Authenticator wird anhand des Namens des Clients, der IP-Adresse des Arbeitsplatzrechners und der aktuellen Uhrzeit am Arbeitsplatzrechner erstellt — verschlüsselt mit dem Session Key, der nur dem Client und dem Server, von dem er einen Dienst anfordert, bekannt ist. Im Gegensatz zu einem Ticket kann ein Authenticator nur einmal benutzt werden. Ein Client kann selber einen Authenticator erzeugen.

Principal Ein Kerberos-Principal ist eine unverwechselbare Einheit (ein Benutzer oder ein Dienst), der ein Ticket zugewiesen werden kann. Ein Principal setzt sich aus den folgenden Bestandteilen zusammen:

- **Primary** – Der erste Teil des Principals, der im Falle eines Benutzers mit dem Benutzernamen identisch sein kann.
- **Instance** – Optionelle Information, die den Primary beschreibt. Diese Zeichenkette ist durch ein ` / ` vom Primary getrennt.
- **Realm** – Der Realm legt Ihren Kerberos-Bereich fest. Normalerweise ist Ihr Realm Ihr Domainname in Großbuchstaben.

Mutual Authentication Kerberos sorgt dafür, dass sich sowohl der Client als auch der Server über die Identität der jeweiligen Gegenpartei sicher sein können. Sie teilen sich einen Session Key, mit dem sie sicher kommunizieren können.

Session Key Session Keys (Sitzungsschlüssel) sind temporäre private Schlüssel, die von Kerberos generiert werden. Sie sind dem Client bekannt und werden zur Verschlüsselung der Kommunikation zwischen dem Client und dem Server benutzt, von dem der Client ein Ticket angefordert und bekommen hat.

Replay Fast alle Nachrichten, die in einem Netzwerk versendet werden, können abgehört, entwendet und erneut versendet werden. Im Zusammenhang mit Kerberos könnte dies äußerst gefährlich sein, falls es einem Angreifer gelingen sollte, Ihre Anforderung für einen Dienst abzufangen, die Ihr Ticket und Ihren Authenticator enthält. Er könnte daraufhin versuchen, sie erneut zu versenden („Replay“) und sich als Sie ausgeben. Allerdings implementiert Kerberos verschiedene Mechanismen, um diesem Problem vorzubeugen.

Server oder Service „Service“ (Dienst) wird benutzt, wenn eine bestimmte Aktion durchgeführt werden soll. Der zugrundeliegende Prozess wird als „Server“ bezeichnet.

Wie funktioniert es?

Kerberos wird oft als „Trusted Third Party“-Authentifizierungsdienst bezeichnet, was ausdrückt, dass sich alle Clients im Hinblick auf die Identität eines anderen Clients auf die Einschätzung von Kerberos verlassen. Kerberos unterhält eine Datenbank über alle Benutzer und ihre privaten Schlüssel.

Um sicherzustellen, dass Kerberos das in ihn gesetzte Vertrauen auch wirklich verdient, müssen Authentifizierungsserver und Ticket-Granting Server auf einer dedizierten Maschine laufen. Sorgen Sie dafür, dass nur der Administrator physisch und über das Netzwerk Zugang zu dieser Maschine hat und beschränken Sie die (Netzwerk-)Dienste, die auf diesem Server laufen, auf das absolute Minimum — lassen Sie nicht einmal sshd laufen.

Erste Kontaktaufnahme Ihr erster Kontakt mit Kerberos ähnelt dem gewöhnlichen Einloggen an einem normalen Netzwerksystem. Geben Sie Ihren Benutzernamen ein. Diese Information und der Name des Ticket-Granting Services werden dem Authentifizierungsserver (Kerberos) zugesendet. Falls der Authentifizierungsserver von Ihrer Existenz weiß, generiert er einen (zufälligen) Session Key für den weiteren Gebrauch zwischen Ihrem Client und dem Ticket-Granting Server. Nun wird der Authentifizierungsserver ein Ticket für den Ticket-Granting Server erstellen. Das Ticket enthält die folgenden Informationen — die alle mit einem Session Key verschlüsselt sind, den nur der Authentifizierungsserver und der Ticket-Granting Server kennen:

- die Namen des Clients und des Ticket-Granting Servers
- die aktuelle Uhrzeit
- die Lebensdauer, die diesem Ticket zugewiesen wurde
- die IP-Adresse des Clients
- den neu generierten Session Key

Dann wird das Ticket zusammen mit dem Session Key nochmals in verschlüsselter Form dem Client zurückgesendet, jedoch unter Benutzung des privaten Schlüssels des Clients. Dieser private Schlüssel ist nur Kerberos und dem Client bekannt, da er von Ihrem Benutzerpasswort abgeleitet ist. Sobald der Client diese Antwort erhält, werden Sie nach Ihrem Passwort gefragt. Dieses Passwort wird in den Schlüssel konvertiert, welcher das vom Authentifizierungsserver gesendete Paket entschlüsseln kann. Das Paket wird „entpackt“ und das Passwort und der Schlüssel werden aus dem Arbeitsspeicher des Arbeitsplatzrechners gelöscht. Ihr Arbeitsplatzrechner kann Ihre Identität nachweisen, bis die Lebensdauer des Ticket-Granting Tickets erlischt.

Anforderung eines Dienstes Um von einem beliebigen Server im Netzwerk einen Dienst anfordern zu können, muss die Client-Anwendung dem Server ihre Identität nachweisen. Daher generiert die Anwendung einen Authenticator. Ein Authenticator setzt sich aus den folgenden Bestandteilen zusammen:

- dem Principal des Clients
- der IP-Adresse des Clients
- der aktuellen Uhrzeit
- einer Prüfsumme (bestimmt durch den Client)

Alle diese Informationen werden mit dem Session Key, den der Client bereits für diesen speziellen Server empfangen hat, verschlüsselt. Der Authenticator und das Ticket für den Server werden an den Server gesendet. Der Server benutzt seine Kopie des Session Keys, um den Authenticator zu entschlüsseln, der ihm sämtliche benötigte Informationen über den Client liefert, der seinen Dienst anfordert. Diese Informationen können mit denen verglichen werden, die im Ticket enthalten sind. Gäbe es auf der Serverseite keine Sicherheitsmaßnahmen, so wäre diese Stufe das ideale Ziel für Replay-Attacken. Jemand mit schlechten Absichten könnte versuchen, eine vorher aus dem Netz gestohlene Anforderung erneut zu versenden. Um dies zu verhindern, nimmt der Server keine Anforderungen an, die mit einem Zeitstempel und einem Ticket versehen sind, die ihm schon vorher zugesendet worden waren. Außerdem können Anforderungen abgelehnt werden, deren Zeitstempel in Bezug auf den Zeitpunkt, an dem die Anforderung empfangen wurde, zu sehr abweichen (in die Zukunft und in die Vergangenheit).

Gegenseitige Authentifizierung Die Kerberos-Authentifizierung kann in beide Richtungen benutzt werden. Es geht nicht nur darum, ob der Client wirklich derjenige ist, der er zu sein vorgibt; auch der Server sollte in der Lage sein, sich gegenüber dem Client zu authentifizieren, der seinen Dienst anfordert. Daher versendet er selber auch eine Art Authenticator. Er addiert der Prüfsumme, die er im Authenticator des Clients erhalten hat, eins hinzu und verschlüsselt sie mit dem Session Key, den er mit dem Client teilt. Der Client betrachtet diese Antwort als Nachweis für die Echtheit des Servers, wonach die Zusammenarbeit zwischen dem Client und dem Server beginnen kann.

Ticket-Granting — Kontaktaufnahme mit allen Servern Tickets sind für den Gebrauch für jeweils einen Server bestimmt. Das bedeutet, dass Sie ein neues Ticket brauchen, sobald Sie einen anderen Dienst anfordern.

Kerberos implementiert einen Mechanismus zur Beschaffung von Tickets für einzelne Server. Dieser Dienst wird als „Ticket-Granting Service“ (Dienst zur Ausstellung von Tickets) bezeichnet. Der Ticket-Granting Service ist ein Dienst wie jeder andere und unterliegt daher den gleichen Zugriffsprotokollen, die bereits erwähnt wurden. Jedes Mal, wenn eine Anwendung ein Ticket benötigt, das noch nicht angefordert wurde, nimmt sie mit dem Ticket-Granting Server Kontakt auf. Diese Anforderung setzt sich aus den folgenden Bestandteilen zusammen:

- dem angeforderten Principal
- dem Ticket-Granting Ticket
- dem Authenticator

Ähnlich wie bei jedem anderen Server überprüft der Ticket-Granting Server das Ticket-Granting Ticket sowie den Authenticator. Falls sie als gültig anerkannt werden, erstellt der Ticket-Granting Server einen neuen Session Key zur Benutzung durch den ursprünglichen Client und den neuen Server. Dann wird das Ticket für den neuen Server mit den folgenden Informationen erstellt:

- dem Principal des Clients
- dem Principal des Servers
- der aktuellen Uhrzeit
- der IP-Adresse des Clients
- dem neu generierten Session Key

Dem neuen Ticket wird eine Lebensdauer zugewiesen, die der verbleibenden Lebensdauer des Ticket-Granting Tickets oder dem Standardwert für den Dienst entspricht, je nachdem, was kürzer ist. Dieses Ticket und der Session Key werden dem Client vom Ticket-Granting Service zugesendet. Dieses Mal ist die Antwort jedoch mit dem Session Key verschlüsselt, der mit dem ursprünglichen Ticket-Granting Ticket empfangen wurde. Wenn ein neuer Dienst angefordert wird, kann der Client nun die Antwort entschlüsseln, ohne das Benutzerpasswort erneut anzufordern. So kann Kerberos für den Client ein Ticket nach dem anderen erlangen, ohne den Benutzer mehr als einmal beim Login zu belästigen.

Kompatibilität mit Windows 2000 Windows 2000 enthält eine Microsoft-Implementierung von Kerberos 5. Da SuSE Linux Desktop die Heimdal-Implementierung von Kerberos 5 benutzt, werden Sie in der Heimdal-Dokumentation bestimmt einige nützliche Informationen und Anleitungen finden; siehe [Weitere Informationen über Kerberos](#) auf Seite 310.

Auswirkungen von Kerberos für den Benutzer

Im Idealfall kommt ein Benutzer ausschließlich beim Login an seinem Arbeitsplatzrechner mit Kerberos in Kontakt. Beim Einloggen wird ein Ticket-Granting Ticket erlangt. Beim Ausloggen werden die Kerberos-Tickets des Benutzers automatisch vernichtet, wodurch verhindert wird, dass sich ein anderer Benutzer als dieser spezielle Benutzer ausgibt, wenn dieser nicht eingeloggt ist. Die automatische Vernichtung von Tickets führt zu einer schwierigen Situation, wenn die Sitzung des Benutzers länger dauert als die Höchstlebensdauer, die dem Ticket-Granting Ticket zugewiesen wird (10 Stunden ist ein vernünftiger Wert). Der Benutzer kann sich jedoch ein neues Ticket-Granting Ticket besorgen, indem er kinit startet. Er braucht nur sein Passwort erneut einzugeben — Kerberos wird dafür sorgen, dass er zu jedem gewünschten Dienst Zugang hat, ohne nochmals eine Authentifizierung zu verlangen. Diejenigen, die an einer Liste aller Tickets interessiert sind, die durch Kerberos im Hintergrund für sie erworben wurden, können diese mit klist abrufen.

Es folgt eine Auswahl von Anwendungen, die sich die Kerberos-Authentifizierung zunutze machen. Diese Anwendungen befinden sich unter `/usr/lib/heimdal/bin`. Sie alle bieten die volle Funktionalität ihrer gewöhnlichen UNIX/Linux-Geschwister sowie den zusätzlichen Vorteil einer transparenten Authentifizierung mit Hilfe von Kerberos:

- telnet/telnetd
- rlogin
- rsh, rcp, rshd
- popper/push
- ftp/ftpd
- su
- imapd
- pine

Wie Sie sehen werden, brauchen Sie Ihr Passwort nicht einzugeben, um diese Anwendungen benutzen zu können, da Kerberos Ihre Identität bereits nachgewiesen hat. ssh — sofern mit Kerberos-Unterstützung kompiliert — kann sogar alle Tickets, die Sie für einen Arbeitsplatzrechner erworben haben, an einen anderen Arbeitsplatz weiterleiten. Wenn Sie ssh benutzen, um sich auf

einem anderen Arbeitsplatzrechner einzuloggen, sorgt ssh dafür, dass die verschlüsselten Inhalte der Tickets der neuen Situation angepasst werden. Es ist nicht ausreichend, die Tickets einfach von einem Arbeitsplatzrechner auf einen anderen zu kopieren, da das Ticket spezifische Information über den Arbeitsplatzrechner enthält (die IP-Adresse). XDM und KDM bieten ebenfalls Kerberos-Unterstützung. Lesen Sie im *Kerberos V5 UNIX User's Guide* unter http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html mehr über die Kerberos-Netzwerkanwendungen.

Weitere Informationen über Kerberos

SuSE Linux Desktop enthält eine freie Implementierung von Kerberos, die als Heimdal bezeichnet wird. Die entsprechende Dokumentation wird zusammen mit dem Paket heimdal unter `/usr/share/doc/packages/heimdal/doc/heimdal.info` installiert. Die Dokumentation ist auch auf der Internetseite des Projekts unter <http://www.pdc.kth.se/heimdal/> erhältlich.

Auf der offiziellen Website der Kerberos-Implementierung des MIT finden Sie Links zu anderen relevanten Ressourcen im Zusammenhang mit Kerberos:

<http://web.mit.edu/kerberos/www/>

Ein „klassischer“ Dialog, der die Arbeitsweise von Kerberos erläutert. Nicht allzu technisch, aber trotzdem hochinteressant:

<http://web.mit.edu/kerberos/www/dialogue.html>

Dieses Papier vermittelt ein umfangreiches Verständnis über die grundlegende Arbeitsweise von Kerberos, ist jedoch nicht übermäßig schwer zu verstehen. Es bietet außerdem eine Menge Möglichkeiten für weitere Nachforschungen zu Kerberos:

<ftp://athena-dist.mit.edu/kerberos/doc/usenix.PS>

Diese Links bieten eine kurze Einführung in Kerberos sowie Antworten auf viele Fragen im Zusammenhang mit der Installation, Konfiguration und Administration von Kerberos:

http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/user-guide_toc.html

http://www.lns.cornell.edu/public/COMP/krb5/install/install_toc.html

http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.5/doc/admin_toc.html

Das offizielle Kerberos-FAQ:

<http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>

Tung, Brian: *Kerberos — A Network Authentication System*. Addison Wesley, 1999. - (ISBN 0-201-37924-4)

Installation und Administration von Kerberos

Dieser Abschnitt erläutert die Installation des Heimdal Kerberos sowie einige Aspekte der Administration. Es wird vorausgesetzt, dass Sie mit den Grundlagen von Kerberos vertraut sind (siehe auch Abschnitt [Netzwerkauthentifizierung — Kerberos](#) auf Seite 303).

Festlegung der Kerberos-Realms

Die „Domain“ einer Kerberos-Installation wird als Realm bezeichnet und hat einen Namen wie `FOOBAR.COM` oder einfach nur `ACCOUNTING`. Da Kerberos Groß-/Kleinbuchstaben unterscheidet, ist `foobar.com` ein anderer Realm als `FOOBAR.COM`. Die Wahl von Groß-/Kleinbuchstaben ist Ihnen überlassen. Es ist jedoch üblich, für Realm-Namen Großbuchstaben zu benutzen.

Es ist empfehlenswert, Ihren DNS-Domainnamen (oder eine Subdomain wie `ACCOUNTING.FOOBAR.COM`) zu benutzen. Wie Sie später sehen werden, haben Sie es als Administrator viel leichter, wenn Sie Ihre Kerberos-Clients so konfigurieren, dass das KDC und andere Kerberos-Dienste via DNS ansprechbar sind. Um dies zu ermöglichen, ist es sinnvoll, wenn der Realm-Name eine Subdomain Ihres DNS-Domainnamens ist.

Im Gegensatz zum DNS-Namensraum ist Kerberos nicht hierarchisch gegliedert. Sie können nicht einen Realm namens `FOOBAR.COM` aufsetzen, darunter zwei „Subrealms“ namens `DEVELOPMENT` und `ACCOUNTING` erstellen und erwarten, dass die beiden untergeordneten Realms irgendwie Principals von `FOOBAR.COM` übernehmen. Stattdessen hätten Sie drei getrennte Realms, für die Sie „Crossrealm“-Authentifizierung konfigurieren müssten, um Benutzern eines Realms zu ermöglichen, mit Servern oder Benutzern eines anderen Realms zu interagieren. Die Einrichtung der Crossrealm-Authentifizierung wird beispielsweise in [Tun99] beschrieben.

Der Einfachheit halber nehmen wir an, dass Sie für Ihre gesamte Organisation nur einen Realm anlegen. Im restlichen Teil dieses Abschnittes wird der Realm-Name `SAMPLE.COM` für alle Beispiele benutzt.

Einrichtung der KDC-Hardware

Wenn Sie Kerberos benutzen möchten, brauchen Sie zunächst einen Rechner, der als Key Distribution Center (KDC) eingesetzt wird. Auf diesem Rechner befindet sich die gesamte Kerberos-Benutzerdatenbank mit den Passwörtern und allen Informationen.

Das KDC ist der wichtigste Teil Ihrer Sicherheitsinfrastruktur — wenn jemand hier eindringt, sind alle Benutzerkonten und die gesamte Infrastruktur, die durch Kerberos geschützt wird, offengelegt. Ein Angreifer, der Zugang zur Kerberos-Datenbank hat, kann ein beliebiges Principal in der Datenbank verkörpern! Sorgen Sie dafür, dass die Sicherheitsvorkehrungen für diesen Rechner so strikt wie möglich sind:

- Stellen Sie den Server an einem physikalisch sicheren Standort auf, zum Beispiel in einem abgeschlossenen Serverraum, zu dem nur ein begrenzter Personenkreis Zugang hat.
- Lassen Sie außer dem KDC keine anderen Netzwerkanwendungen auf dem Rechner laufen. Dies gilt sowohl für Server- als auch für Clientanwendungen. Das KDC sollte beispielsweise keine Dateisysteme über NFS importieren oder DHCP benutzen, um seine Netzwerkkonfiguration abzurufen.

Ein guter Ansatz wäre, zunächst nur ein Minimalsystem zu installieren und dann die Liste aller installierten Pakete zu überprüfen und eventuelle unnötige Pakete zu löschen. Dies schließt Server wie `inetd`, `portmap` und `cups` sowie alles ein, was mit X11 zu tun hat. Selbst die Installation eines SSH-Servers stellt ein potentielles Sicherheitsrisiko dar.

Auf diesem Rechner gibt es kein grafisches Login, da auch ein X-Server ein potentielles Sicherheitsrisiko darstellt. Kerberos hat jedoch ein eigenes Administrationsinterface.

- Konfigurieren Sie `/etc/nsswitch.conf` so, dass nur in lokalen Dateien nach Benutzern und Gruppen gesucht wird. Ändern Sie die Zeilen für `passwd` und `group` wie folgt:

```
passwd:      files
group:       files
```

Editieren Sie die Dateien `passwd`, `group`, `shadow` und `gshadow` in `/etc` und entfernen Sie die Zeilen, die mit einem Pluszeichen anfangen (diese werden für NIS-Anfragen benutzt).

Sie sollten sich auch überlegen, DNS-Anfragen zu deaktivieren, da dies einen Risikofaktor darstellt. Falls in der DNS Resolver Library eine Sicherheitslücke ist, könnte ein Angreifer das KDC überlisten, eine DNS-Anfrage durchzuführen, die diese Lücke ausnutzt. Um DNS-Anfragen zu deaktivieren, löschen Sie einfach `/etc/resolv.conf`.

- Deaktivieren Sie alle Benutzerkonten außer dem von Root, indem Sie `/etc/shadow` editieren und die gehashten Passwörter durch Sternchen oder Ausrufezeichen ersetzen.

Zeitsynchronisation

Um Kerberos erfolgreich einsetzen zu können, müssen alle Systemuhren in Ihrer Organisation in einem bestimmten Bereich synchronisiert werden. Der Grund hierfür ist, dass Kerberos versuchen wird, Sie vor erneut versendeten Credentials (Replay) zu schützen. Es könnte einem Angreifer gelingen, Kerberos-Credentials im Netzwerk zu beobachten und diese zu benutzen, um den Server anzugreifen. Kerberos setzt verschiedene Verteidigungsmechanismen ein, um dies zu verhindern. Einer dieser Mechanismen sieht vor, dass die Tickets mit Zeitstempeln versehen werden. Ein Server, der ein Ticket mit einem nicht aktuellen Zeitstempel erhält, wird das Ticket zurückweisen.

Natürlich erlaubt Kerberos beim Vergleichen von Zeitstempeln einen gewissen Spielraum. Computeruhren können jedoch äußerst ungenau sein — es ist nicht ungewöhnlich, das PC-Uhren im Laufe einer Woche eine halbe Stunde vor- oder zurückgehen. Sie sollten daher alle Hosts im Netzwerk so konfigurieren, dass ihre Uhren mit einer zentralen Zeitquelle synchronisiert werden.

Sie können dies sehr einfach bewerkstelligen, indem Sie auf einem Rechner einen NTP-Zeitserver installieren und alle Clients ihre Uhren mit diesem Server synchronisieren lassen. Dies kann erreicht werden, indem Sie einen NTP-Daemon im Client-Modus auf allen Rechnern laufen lassen oder `ntpdate` einmal am Tag von allen Clients ausführen lassen (diese Lösung funktioniert wahrscheinlich nur bei einer kleineren Anzahl von Clients).

Das KDC selber muss auch mit der gemeinsamen Zeitquelle synchronisiert werden. Da ein NTP-Daemon auf diesem Rechner ein Sicherheitsrisiko darstellen würde, ist es wahrscheinlich das Beste, `ntpdate` via einen Croneintrag auszuführen.

Eine Beschreibung der Konfiguration von NTP würde über den Rahmen dieses Abschnittes hinausgehen. Weitergehende Information ist in der NTP-Dokumentation auf Ihrem installierten System unter `/usr/share/doc/packages/xntp-doc` erhältlich.

Konfiguration der Protokollfunktion

Standardmäßig protokollieren die auf dem KDC-Host laufenden Kerberos-Daemons ihre Information zum `syslog`-Daemon. Falls Sie die Aktivitäten Ihres KDC beobachten möchten, ist es vielleicht nützlich, diese Protokolldateien

regelmäßig zu verarbeiten und auf ungewöhnliche Ereignisse oder potentielle Probleme zu untersuchen.

Um dies zu erreichen, kann man auf dem KDC-Host ein Protokollscannerskript laufen lassen oder diese Protokolldaten via rsync vom KDC auf einen anderen Host kopieren und die Protokollanalyse dort durchführen. Es wird davon abgeraten, die gesamte Protokollausgabe über die Weiterleitungsfunktion von syslogd weiterzuleiten, da die Information in unverschlüsselter Form im Netzwerk übertragen wird.

Installation des KDC

Dieser Abschnitt erläutert die Erstinstallation des KDC, einschließlich der Einrichtung eines administrativen Principals.

Installation der RPMs

Bevor Sie anfangen können, müssen Sie die Kerberos-Software installieren. Installieren Sie die RPMs `heimdal` und `heimdal-lib` auf dem KDC:

```
erde:~ # rpm -ivh heimdal-0*.rpm heimdal-lib-0*.rpm
```

Editieren von `krb5.conf`

Dann editieren Sie die Konfigurationsdatei `/etc/krb5.conf`. Die Datei, die standardmäßig installiert wird, enthält verschiedene Mustereinträge. Sorgen Sie dafür, dass all diese Einträge gelöscht werden, bevor Sie anfangen.

`krb5.conf` besteht aus mehreren Abschnitten, die jeweils durch den Namen des Abschnittes eingeleitet werden. Dies sieht `[so]` aus. Der einzige Abschnitt, den wir uns jetzt vornehmen, ist `[libdefaults]`, welcher wie folgt aussehen sollte:

```
[libdefaults]
    default_realm = SAMPLE.COM
    clockskew = 300
```

Die Zeile `default_realm` setzt den Default-Realm für Kerberos-Anwendungen fest. `clock_skew` definiert die Toleranz für die Annahme von Tickets, deren Zeitstempel nicht genau der Uhrzeit des KDC-Hosts entsprechen. Normalerweise wird die maximale Diskrepanz auf 300 Sekunden, also 5 Minuten eingestellt. Das bedeutet, dass ein Ticket einen Zeitstempel haben kann, der aus der Sicht des Server 5 Minuten zurück oder 5 Minuten in der Zukunft liegt. Wenn NTP benutzt wird, um alle Hosts zu synchronisieren, kann dieser Wert auf etwa eine Minute reduziert werden.

Setzen des Master Keys

Der nächste Schritt ist die Initialisierung der Datenbank, in der Kerberos sämtliche Informationen über die Principals speichert. Zuerst muss der Master Key der Datenbank gesetzt werden, der benötigt wird, um die Datenbank vor unbeabsichtigter Offenlegung zu schützen, besonders wenn diese auf ein Band gesichert wird.

Der Master Key wird aus einer Passphrase generiert und in einer Datei gespeichert, die als Stash File bezeichnet wird. Daher brauchen Sie nicht jedes Mal, wenn das KDC neu gestartet wird, das Passwort einzugeben. Wählen Sie eine gute Passphrase, beispielsweise einen Satz aus einem Buch, das Sie an einer zufälligen Stelle aufschlagen.

Wenn Sie die Kerberos-Datenbank auf Band sichern (`/var/heimdal/heimdal.db`), sichern Sie bitte nicht die stash Datei (in `/var/heimdal/m-key`). Ansonsten könnte jeder, der das Band lesen kann, die Datenbank entschlüsseln. Aus diesem Grunde ist es empfehlenswert, eine Kopie der Passphrase in einem Safe oder an einem anderen sicheren Ort aufzubewahren, da Sie diese benötigen, wenn Sie nach einem Absturz Ihre Datenbank von Band wiederherstellen.

Um den Master Key zu setzen, starten Sie die Utility `kstash` ohne zusätzliche Argumente und geben die Passphrase zweimal ein:

```
erde:~ # kstash
```

```
Master key:<enter pass phrase>
```

```
Verifying password - Master key:<enter pass phrase again>
```

Anlegen des Realms

Zuletzt müssen die Einträge für Ihren Realm in der Kerberos-Datenbank erstellt werden. Starten Sie die Utility `kadmin` mit der Option `-l`. Diese Option veranlasst `kadmin`, auf die lokale Datenbank zuzugreifen. Standardmäßig versucht `kadmin`, den Kerberos-Administrationsdienst über das Netzwerk zu erreichen. In diesem Stadium würde dies nicht funktionieren, da dieser Dienst noch nicht läuft.

Nun weisen Sie `kadmin` an, Ihren Realm zu initialisieren. `kadmin` wird eine Reihe von Fragen stellen. Zunächst ist es das Beste, die von `kadmin` angebotenen Defaults anzunehmen:

```
erde:~ # kadmin -l
```

```
kadmin> init SAMPLE.COM
Realm max ticket life [unlimited]: <press return>
Realm max renewable ticket life [unlimited]: <press return>
```

Um zu prüfen, ob etwas geschehen ist, benutzen Sie den Befehl `list`:

```
kadmin> list *
default@SAMPLE.COM
kadmin/admin@SAMPLE.COM
kadmin/hprop@SAMPLE.COM
kadmin/changepw@SAMPLE.COM
krbtgt/SAMPLE.COM@SAMPLE.COM
changepw/kerberos@SAMPLE.COM
```

Dies zeigt, dass es jetzt in der Datenbank eine Reihe von Principals gibt, die alle für den internen Gebrauch durch Kerberos bestimmt sind.

Erstellung eines Principals

Nun schaffen Sie zwei Kerberos-Principals für sich selbst — ein „normales“ Principal für Ihre tägliche Arbeit und eines für administrative Aufgaben im Zusammenhang mit Kerberos. Verfahren Sie wie folgt, um den Login-Namen `newbie` einzurichten:

```
erde:~ # kadmin -l

kadmin> add newbie
Max ticket life [1 day]: <press return>
Max renewable life [1 week]: <press return>
Principal expiration time [never]: <press return>
Password expiration time [never]: <press return>
Attributes []: <press return>
newbie@SAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Sie können die Standardwerte mit **(Enter)** bestätigen. Wählen Sie ein geeignetes Passwort.

Dann erstellen Sie ein anderes Principal namens `newbie/admin` durch Eingabe von `add newbie/admin` am `kadmin`-Prompt. Der Suffix `admin` hinter dem Benutzernamen bezeichnet die Rolle. Später werden Sie diese administrative Rolle benutzen, um die Kerberos-Datenbank zu administrieren.

Einrichtung der Fernadministration

Um der Kerberos-Datenbank Principals hinzufügen bzw. löschen zu können, ohne direkten Zugang zur Konsole des KDC zu haben, teilen Sie dem Kerberos-Adminserver mit, welche Principals hierzu berechtigt sind.

Sie können dies erreichen, indem Sie die Datei `/var/heimdal/kadmind.acl` editieren (ACL ist die Abkürzung von Access Control List). Die ACL-Datei ermöglicht eine Spezifizierung der Vorrechte und die Feineinstellung des Kontrollgrads. Nähere Informationen sind unter Manual-Page von `kadmind` (`man 8 kadmind`) erhältlich.

Erlauben Sie sich nun, mit der Datenbank alles zu tun, was Sie möchten, indem Sie der Datei die folgende Zeile hinzufügen:

```
newbie/admin                                all
```

Ersetzen Sie den Benutzernamen `newbie` mit Ihrem eigenen Benutzernamen.

Starten des KDC

Starten Sie die KDC-Daemons. Dies schließt den eigentlichen `kdc` (der Daemon, der für die Benutzerauthentifizierung und Ticketanfragen zuständig ist), `kadmind` (der Server für die Fernadministration) sowie `kpasswd` (zuständig für Passwortänderungsanfragen von Benutzern) ein. Um den Daemon manuell zu starten, geben Sie Folgendes ein:

```
erde:~ # rckdc start
```

```
Starting kdc                                done
```

Sorgen Sie dafür, dass das KDC standardmäßig gestartet wird, wenn der Server neu gestartet wird. Dies wird mit Hilfe des Befehls `insserv kdc` bewerkstelligt.

Konfiguration von Kerberos-Clients

Die Konfiguration von Kerberos kann grundsätzlich auf zweierlei Weise erfolgen — über eine statische Konfiguration mit der Datei `/etc/krb5.conf` oder über eine dynamische Konfiguration via DNS. Bei der DNS-Konfiguration versuchen Kerberos-Anwendungen, die KDC-Dienste durch DNS-Einträge zu finden. Bei der statischen Konfiguration müssen Sie die Hostnamen Ihres KDC-Servers in der Datei `krb5.conf` eintragen (und die Datei aktualisieren, wenn

das KDC „umzieht“ oder Sie Ihren Realm in irgendeiner anderen Weise neu konfigurieren).

Die DNS-basierte Konfiguration ist gewöhnlich viel flexibler und der Konfigurationsaufwand pro Rechner viel geringer. Dieser Ansatz erfordert jedoch, dass Ihr Realm-Name mit Ihrer DNS-Domain identisch ist oder eine Subdomain hiervon ist.

Außerdem verursacht die Konfiguration von Kerberos via DNS ein kleines Sicherheitsproblem, denn ein Angreifer kann Ihre Infrastruktur durch Ihren DNS erheblich stören (durch Abschuss des Nameservers, Verfälschung (Spoofing) von DNS-Einträgen usw.). Im schlimmsten Fall führt dies jedoch zu einem DoS. Ein ähnliches Szenario kann auch bei der statischen Konfiguration auftreten, es sei denn, Sie geben in `krb5.conf` IP-Adressen anstelle von Hostnamen ein.

Statische Konfiguration

Für die statische Konfiguration fügen Sie bitte den folgenden Abschnitt in `krb5.conf` ein (wobei `kdc.sample.com` der Hostname des KDCs ist):

```
[realms]
    SAMPLE.COM = {
        kdc = kdc.sample.com
        kpasswd_server = kdc.sample.com
        admin_server = kdc.sample.com
    }
```

Falls Sie mehrere Realms haben, fügen Sie einfach dem Abschnitt `[realms]` einen weiteren Ausdruck hinzu.

Fügen Sie dieser Datei auch einen Ausdruck hinzu, der besagt, wie Anwendungen Hostnamen zu Realms zuordnen müssen. Wenn man beispielsweise eine Verbindung zu einem entfernten Host aufbaut, muss die Kerberos-Library wissen, in welchem Realm sich dieser Host befindet. Dies muss in dem Abschnitt `[domain_realms]` konfiguriert werden:

```
[domain_realm]
    .sample.com = SAMPLE.COM
    www.foobar.com = SAMPLE.COM
```

Dieser Eintrag teilt der Library mit, dass sich alle Hosts in den `sample.com` DNS-Domains in dem Kerberos-REALM `SAMPLE.COM` befinden. Außerdem sollte auch ein externer Host namens `www.foobar.com` als Angehöriger des Realms `SAMPLE.COM` betrachtet werden.

DNS-basierte Konfiguration

Die DNS-basierte Kerberos-Konfiguration macht intensiven Gebrauch von SRV-Einträgen (Siehe (RFC2052) *A DNS RR for specifying the location of services* unter <http://www.ietf.org>). Diese Einträge wurden in früheren Implementierungen des BIND-Nameservers noch nicht unterstützt. Deshalb ist BIND Version 8 (oder spätere Versionen) erforderlich.

Was Kerberos betrifft, ist der Name eines SRV-Eintrags immer wie folgt aufgebaut: `_service._proto.realm`, wobei `realm` der Kerberos-Realm ist. Beachten Sie, dass Domainnamen in DNS keine Groß-/Kleinbuchstaben unterscheiden, so dass Kerberos-Realms, die Groß-/Kleinschreibung unterscheiden, bei dieser Konfigurationsmethode hinfällig werden. `_service` ist der Name eines Dienstes (verschieden Namen werden benutzt, wenn beispielsweise eine Verbindung zum KDC oder zum Passwortdienst aufgebaut wird). `_proto` kann entweder `_udp` oder `_tcp` sein, aber nicht alle Dienste unterstützen beide Protokolle.

Der Datenteil der SRV Resource Records besteht aus einem Prioritätswert, einer Gewichtung, einer Portnummer und einem Hostnamen. Die Priorität definiert die Reihenfolge, in welcher Hosts versucht werden sollen (kleinere Werte stellen eine höhere Priorität dar). Die Gewichtung wird benutzt, um ein gewisses Load-Balancing zwischen Servern gleicher Priorität zu unterstützen. Diese Funktion wird kaum gebraucht, so dass Sie diese auf Null setzen können.

Bei der Suche nach Diensten sucht Heimdal Kerberos zur Zeit nach den folgenden Namen:

`_kerberos` Definiert die Lokalisierung des KDC-Daemons (der Authentifizierungs- und Ticket-Granting-Server). Typischerweise sehen die Einträge wie folgt aus:

```
_kerberos._udp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
_kerberos._tcp.SAMPLE.COM.  IN  SRV    0 0 88 kdc.sample.com.
```

`_kpasswd` Beschreibt die Lokalisierung des Servers für Passwortänderungen. Typischerweise sehen die Einträge wie folgt aus:

```
_kpasswd._udp.SAMPLE.COM.  IN  SRV    0 0 464 kdc.sample.com.
```

Da `kpasswd` TCP nicht unterstützt, sollte es keinen `_tcp` Eintrag geben.

`_kerberos-adm` Beschreibt die Lokalisierung des Fernadministrationsservers. Typischerweise sehen die Einträge wie folgt aus:

```
_kerberos-adm._tcp.SAMPLE.COM. IN  SRV    0 0 749 kdc.sample.com.
```

Da `kodmind` UDP nicht unterstützt, sollte es keinen `_udp` Eintrag geben.

Wie bei der statischen Konfigurationsdatei gibt es einen Mechanismus, der Clients darüber informiert, dass ein bestimmter Host sich in dem Realm `SAMPLE.COM` befindet, selbst wenn er kein Teil der DNS-Domain `sample.com` ist. Dies kann erreicht werden, indem man `_kerberos.hostname` einen TXT-Eintrag hinzufügt:

```
_kerberos.www.foobar.com. IN TXT "SAMPLE.COM"
```

Verwaltung von Principals

Die Fernadministration von Kerberos sollte nun mit Hilfe des Tools `kadmin` möglich sein. Zunächst brauchen Sie ein Ticket für Ihr Admin-Principal. Dieses Ticket wird gebraucht, wenn Sie eine Verbindung zum `kadmin`-Server herstellen:

```
erde:newbie # kinit newbie/admin
```

```
newbie/admin@SAMPLE.COM's Password: <enter password>
```

```
erde:newbie # /usr/sbin/kadmin
```

```
kadmin> privs
change-password, list, delete, modify, add, get
```

Mit dem Befehl `privs` können Sie überprüfen, welche Vorrechte Sie haben. Die obige Liste führt sämtliche Vorrechte auf.

Zum Beispiel können Sie das Principal `newbie` modifizieren:

```
kadmin> mod newbie
Max ticket life [1 day]:2 days
Max renewable life [1 week]:
Principal expiration time [never]:2003-01-01
Password expiration time [never]:
Attributes []:
```

Dies ändert die maximale Lebensdauer des Tickets auf zwei Tage und setzt das Auslaufdatum auf den 01.01.2003.

Die grundlegenden Befehle von `kadmin` sind:

add *<principal>* Fügt ein neues Principal hinzu.

modify *<principal>* Editieren verschiedener Attribute eines Principals wie der maximalen Lebensdauer der Tickets und das Auslaufdatum des Kontos/Accounts.

delete *<principal>* Entfernt ein Principal aus der Datenbank.

rename *<principal>* *<neuename>* benennt ein Principal in *<neuename>* um.

list *<pattern>* Listet alle Principals auf, die dem angegebenen Pattern (Muster) entsprechen. Patterns funktionieren ähnlich wie die Shell Globbing Patterns: `list newbie*` würde in unserem Beispiel `newbie` und `newbie/admin` auflisten.

get *<principal>* Zeigt Detailinformation über das Principal an.

passwd *<principal>* Ändert das Passwort eines Principals.

Hilfe ist zu jeder Zeit durch Eingabe von `(?)` und `(Enter)` erhältlich, auch an Prompts, die von Befehlen wie `modify` und `add` ausgegeben werden.

Der Befehl `init`, der benutzt wird, wenn der Realm erstmals erstellt wird (sowie bei einigen anderen), ist im Remote-Modus nicht verfügbar. Um einen neuen Realm zu erstellen, gehen Sie an die Konsole des KDCs und benutzen `kadmin` im lokalen Modus (mit der Befehlszeilenoption `-l`).

Aktivierung der PAM-Unterstützung für Kerberos

SuSE Linux Desktop wird mit einem PAM-Modul namens `pam_krb5` ausgeliefert, welches die Anmeldung via Kerberos und die Passwortaktualisierung unterstützt. Dieses Modul kann von Anwendungen wie dem Konsole-Login, su und grafischen Anwendungen wie KDM gebraucht werden, in denen der Benutzer ein Passwort eingibt und den Authentifizierungsmechanismus benutzen möchte, um ein erstes Kerberos-Ticket zu erhalten. Um Benutzern zu ermöglichen, ihr Kerberos-Passwort mit Hilfe der normalen `passwd`-Utility transparent zu aktualisieren (statt das Programm `kpasswd` zu starten), fügen Sie `pam_krb5` auch der PAM-Konfiguration von `passwd` hinzu.

Das Modul `pam_krb5` war ursprünglich **nicht** für Netzwerkdienste bestimmt, die Kerberos-Tickets als Teil der Benutzerauthentifizierung annehmen — dies ist eine vollständig andere Geschichte.

In allen Fällen editieren Sie die PAM-Konfigurationsdateien der Dienste, denen Kerberos-Unterstützung hinzugefügt werden soll. Die folgenden Anwendungen benutzen `pam_krb5`. Ihre entsprechenden PAM-Konfigurationsdateien sind auch aufgelistet.

| | |
|---------------|-------------------|
| login | /etc/pam.d/login |
| su | /etc/pam.d/su |
| kdm, gdm, xdm | /etc/pam.d/xdm |
| xlock | /etc/pam.d/xlock |
| passwd | /etc/pam.d/passwd |

Benutzung von pam_krb5

Sie können pam_krb5 auf zweierlei Weise benutzen, je nachdem, ob Sie KDC zur primären Authentifizierungsmethode machen möchten und Passwörter der konventionellen Passwortdatenbanken nur als Fallback benutzen möchten oder aber die konventionellen Datenbanken als primäre Quelle beibehalten und pam_krb5 nur zur Anforderung von Kerberos-Tickets für die Benutzer anwenden möchten, die in dem KDC Principals haben. Der zweite Ansatz ist besonders sinnvoll, wenn man von einem anderen Authentifizierungsmechanismus auf Kerberos umsteigt.

Da Kerberos nur die Authentifizierung durchführt, brauchen Sie immer noch einen Mechanismus, der die restliche Kontoinformationen wie die UID und das Homeverzeichnis verteilt. LDAP ist ein solcher Mechanismus. Der Gebrauch von NIS ist nicht möglich, da Linux zur Zeit über keine Kerberos-Sicherheitsmechanismen für RPC-Netzwerkdienste verfügt.

Sekundäre Authentifizierung mit pam_krb5

In diesem Modus wird die primäre Authentifizierung über das existierende Authentifizierungssystem durchgeführt (Benutzereinträge in der Datei /etc/passwd oder eine NIS-Datenbank). Der einzige Unterschied ist, dass dem Benutzer zusätzlich ein Kerberos-Principal zugeordnet wird und pam_krb5 versuchen wird, mit dem eingegebenen Passwort ein Ticket für den Benutzer abzuholen.

Betrachten Sie beispielsweise die PAM-Konfigurationsdatei für su, welche die folgenden Zeilen für den auth-Dienst enthält:

| | | | |
|------|------------|---------------|--------|
| auth | sufficient | pam_rootok.so | |
| auth | required | pam_unix.so | nullok |

Diese beiden Zeilen teilen der PAM-Library mit, dass zunächst das Modul pam_rootok aufgerufen werden soll, wenn ein Benutzer authentifiziert wird. Wenn dieses Modul Erfolg meldet (was der Fall ist, wenn der anfragende Benutzer der Benutzer Root ist), sollte die su-Anfrage ohne weitere Authentifizierungsaufforderungen angenommen werden. Wenn dies nicht der Fall ist, ruft

PAM das Modul `pam_unix` auf, welches die „traditionelle“ Authentifizierung durchführt, indem es den Benutzer nach einem Passwort fragt, dieses hasht und es mit dem gehashten Passwort des Zielbenutzerkontos vergleicht.

Um optionelle Kerberos-Unterstützung zu implementieren, fügen Sie hiernach eine weitere Zeile ein, die wie folgt aussieht:

```
auth      optional      pam_krb5.so      try_first_pass \
                                missing_keytab_ok \
                                ccache=SAFE \
                                putenv_direct
```

Dies startet das Modul `pam_krb5` und ignoriert eventuelle Fehler, die hiervon angezeigt werden (zum Beispiel falls es nicht in der Lage war, ein Ticket für den Benutzer zu erlangen). Bei dieser Konfiguration wird das Passwort immer mit den Passworteinträgen des ursprünglichen Authentifizierungssystems verglichen.

Bei anderen Diensten sind die Änderungen, die in der PAM-Konfigurationsdatei vorgenommen werden müssen, ähnlich. Es ist gewöhnlich empfehlenswert, `pam_krb5`-Zeile nach der Zeile einzufügen, die `pam_unix` oder `pam_unix2` aufruft.

Primäre Authentifizierung mit `pam_krb5`

Falls Sie alle Benutzer auf Kerberos umgestellt haben, können Sie `pam_krb5` als primären Authentifizierungsmechanismus benutzen und die lokale Passwortdatei als Ausweichlösung benutzen, falls ein Fehler passiert, zum Beispiel weil es für diesen Benutzer kein Principal gibt oder das KDC ausgeschaltet ist. Bei dieser Konfiguration sind alle Benutzerkonten standardmäßig in der Kerberos-Datenbank erfasst und der Fallback zur lokalen Passwortdatei existiert nur für Konten wie Root.

Das folgende Beispiel zeigt, wie `/etc/pam.d/su` geändert werden muss, um dies zu erreichen (beachten Sie das zusätzliche Argument `use_first_pass` für das Modul `pam_unix`):

```
auth      sufficient      pam_rootok.so
auth      sufficient      pam_krb5.so      missing_keytab_ok \
                                ccache=SAFE \
                                putenv_direct
auth      required      pam_unix.so      use_first_pass nullok
```

Diese Änderung fügt `pam_krb5` vor dem Modul `pam_unix` ein und erklärt es für ausreichend, was bedeutet, dass PAM an dieser Stelle abbricht und `pam_unix` überspringt, wenn `pam_krb5` erfolgreich ist. Wenn es jedoch fehlschlägt, wird es fortfahren und auf `pam_unix.so` zurückgreifen.

Nicht alle Anwendungen können jedoch so leicht modifiziert werden wie `su`. Die PAM-Datei für `login` (bzw. die paar Zeilen, die mit der Authentifizierung zu tun haben) sieht wie folgt aus:

```
auth    requisite      pam_unix2.so    nullok
auth    required       pam_securetty.so
auth    required       pam_nologin.so
auth    required       pam_env.so
auth    required       pam_mail.so
```

Fügen Sie eine Zeile für `pam_krb5` vor `pam_unix2` ein. Falls die Authentifizierung mit `pam_krb5` erfolgreich ist, soll `pam_unix2` übersprungen werden, aber es soll mit den anderen Modulen weitergemacht werden. Dies ist etwas komplizierter, wie hier gezeigt wird:

```
auth    [success=1 default=ignore] \
                                pam_krb5.so    missing_keytab_ok \
                                                ccache=SAFE \
                                                putenv_direct
auth    requisite      pam_unix2.so    nullok
... rest as above ...
```

Dies veranlasst, dass PAM ein Modul (`pam_unix2`) überspringt, falls `pam_krb5` Erfolg meldet. Andere Rückmeldungen werden ignoriert und `pam_unix2` wird aufgerufen, wie es vorher der Fall war.

Passwortaktualisierungen mit `pam_krb5`

Bei Benutzung von Kerberos gibt es gewöhnlich zwei Möglichkeiten, wie Benutzer ihre Passwörter aktualisieren können — über die Utility `kpasswd` (nur für Kerberos-Passwörter) oder dadurch, dass der Systemadministrator das Modul `pam_krb5` der `passwd`-Konfiguration hinzufügt.

Um dies zu erreichen, ändern Sie `/etc/pam.d/passwd` wie folgt:

```
auth    required      pam_krb5.so
account required      pam_unix2.so
password required     pam_pwcheck.so    nullok
password required     pam_krb5.so
password required     pam_unix2.so    nullok use_first_pass use_authtok
session required      pam_unix2.so
```

Falls Sie einen Verzeichnisdienst wie LDAP benutzen, die Benutzerpasswörter jedoch nicht mehr in LDAP speichern (es ist nicht empfehlenswert, diese Passwörter in LDAP zu speichern, wenn Sie Kerberos haben), ändern Sie die PAM-Konfiguration von passwd wie folgt:

| | | | |
|----------|----------|----------------|----------------|
| auth | required | pam_krb5.so | |
| account | required | pam_unix2.so | |
| password | required | pam_pwcheck.so | nullok |
| password | required | pam_krb5.so | nopasswdverify |
| session | required | pam_unix2.so | |

Einrichtung der Netzwerkeserver für Kerberos

Bis jetzt wurden nur Benutzer-Credentials behandelt. Auch die Netzwerkeserver, die Kerberos benutzen, müssen sich jedoch gegenüber den Client-Benutzern authentifizieren. Natürlich können sie die Kerberos-Tickets nicht wie normale Benutzer anwenden, da es für den Systemadministrator ziemlich unpraktisch wäre, ungefähr alle acht Stunden für jeden Dienst neue Tickets zu besorgen.

Stattdessen speichern Netzwerkeserver Ihre Kerberos-Keys in Keytabs und besorgen sich bei Bedarf automatisch neue Keys.

Normalerweise brauchen Sie mindestens ein Principal für jeden Host, auf dem Sie einen Netzwerkdienst laufen lassen, der Kerberos benutzt. Dieses Principal wird als `host/machine.sample.com@SAMPLE.COM` bezeichnet, wobei `machine.sample.com` der kanonische Hostname des Servers ist.

Erstellen Sie zunächst das Principal. Sorgen Sie dafür, dass Sie gültige Administrator-Credentials haben, und fügen dann das neue Principal hinzu:

```
erde:~ # kinit newbie/admin
```

```
newbie/admin@SAMPLE.COM's Password: <type password>
```

```
erde:~ # kadmin add -r host/machine.sample.com
```

```
Max ticket life [1 day]:
Max renewable life [1 week]:
Principal expiration time [never]:
Password expiration time [never]:
Attributes []:
```

Statt ein Passwort für das neue Principal zu setzen, weist die Option `-r kadmin` an, einen zufälligen Key zu generieren. Der Grund hierfür ist, dass wir für dieses Principal keine Benutzeraktivität wünschen, da es sich um ein Serverkonto für den Rechner handelt.

Abschließend extrahieren Sie den Key und speichern ihn in der lokalen Keytab-Datei `/etc/krb5.keytab`. Diese Datei gehört dem Superuser, weshalb Sie Root sein müssen, um den folgenden Befehl ausführen zu können:

```
erde:~ # ktutil get host/machine.sample.com
```

Danach sorgen Sie bitte dafür, dass Sie das Admin-Ticket mit `kdestroy` vernichten, das Sie via `kinit` erhalten haben, wie oben beschrieben.

Konfiguration von sshd für die Kerberos-Authentifizierung

Um `sshd` mit der Kerberos-Authentifizierung zu benutzen, editieren Sie `/etc/ssh/sshd_config` und setzen die beiden folgenden Optionen:

```
KerberosAuthentication yes
KerberosTgtPassing yes
```

Dann benutzen Sie den Befehl `rcsshd restart`, um Ihren SSH-Daemon neu zu starten.

Nun sollten Sie in der Lage sein, eine Verbindung mit Kerberos-Authentifizierung aufzubauen. Kerberos wird zur Zeit nur unterstützt, wenn Sie SSH Protokollversion 1 benutzen. Deshalb muss der Client dieses Protokoll wählen, indem die Option `-1` an der Befehlszeile übergeben wird:

```
erde:newbie # ssh -1 earth.sample.com
```

```
Last login: Fri Aug  9 14:12:50 2002 from zamboni.sample.com
Have a lot of fun...
```

```
erde:newbie #
```

Benutzung von LDAP und Kerberos

Um die Zuordnung von Kerberos zum OpenLDAP-Server zu ermöglichen, erstellen Sie das Principal `ldap/earth.sample.com` und fügen es der Keytab hinzu:


```
erde:~ # kadmin add -r ldap/earth.sample.com
erde:~ # ktutil get ldap/earth.sample.com
```

Nach dem Neustart des LDAP-Servers mit `rcldap restart` sollten Sie in der Lage sein, Tools wie `ldapsearch` automatisch mit Kerberos-Authentifizierung zu benutzen.

```
erde:~ # ldapsearch -b ou=People,dc=suse,dc=de '(uid=newbie)'

SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
[...]

# newbie, People, suse.de
dn: uid=newbie,ou=People,dc=suse,dc=de
uid: newbie
cn: Olaf Kirch
[...]
```

Achten Sie darauf, dass `ldapsearch` bei der Ausgabe der SASL/GSSAPI-Meldung Kerberos benutzt. GSSAPI (General Security Services API) ist ein Programmierinterface, welches die Details der verschiedenen Authentifizierungsmechanismen von der Anwendung fernhält. SASL ist ein Netzwerkprotokoll, das benutzt wird, um Authentifizierungsinformation vom Client zum Server und umgekehrt zu übertragen.

Sicherheit ist Vertrauenssache

Grundlagen

Eines der grundlegendsten Leistungsmerkmale eines Linux/Unix-Systems ist, dass mehrere Benutzer (multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben Rechner (multi-tasking) ausführen können. Das Betriebssystem ist darüber hinaus netzwerktransparent, sodass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Applikationen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bezogen werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt verwaltet werden können. Hier geht es

unter anderem auch um Sicherheit und den Schutz der Privatsphäre. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten weiterhin verfügbar sein, auch wenn solche Defekte womöglich den vorübergehenden Ausfall einer größeren Infrastruktur zur Folge hatten.

Auch wenn sich dieses Kapitel des SuSE-Handbuchs in der Hauptsache mit der Vertraulichkeit der Daten und dem Schutz der Privatsphäre der Benutzer beschäftigt, sei betont, dass ein umfassendes Sicherheitskonzept als integralen Bestandteil immer ein regelmäßiges, funktionierendes und überprüftes Backup beinhaltet. Ohne dieses Backup der Daten wird es nicht nur im Fall eines Hardware-Defekts schwierig sein, weiterhin auf die Daten zuzugreifen, sondern insbesondere auch dann, wenn nur der Verdacht besteht, dass jemand sich unbefugterweise an den Daten zu schaffen gemacht hat.

Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- Persönliche Kommunikation mit jemand, der über die gewünschten Informationen verfügt bzw. Zugang zu bestimmten Daten auf einem Computer hat,
- direkt an der Konsole eines Rechners (physikalischer Zugriff),
- über eine serielle Schnittstelle oder
- über ein Netzwerk.

Alle diese Fälle sollten eine Gemeinsamkeit haben: Sie sollten sich als Benutzer authentifizieren müssen, bevor Sie Zugriff auf die Ressourcen oder Daten bekommen. Ein Webserver mag da anders geartet sein, aber Sie wollen sicherlich nicht, dass der Webserver Ihre persönlichen Daten an Surfer preisgibt.

Der erste Fall der oben genannten ist der menschlichste von allen: Etwa bei einer Bank müssen Sie einem Angestellten beweisen, dass Ihnen der Zugriff auf Ihre Konten gestattet ist, indem Sie mit Ihrer Unterschrift, einer PIN oder mit einem Passwort beweisen, dass Sie derjenige sind, für den Sie sich ausgeben. In manchen Fällen kann es gelingen, durch das Erwähnen von Kenntnissen oder durch geschickte Rhetorik das Vertrauen eines Wissensträgers zu erschleichen, so dass dieser weitere Information preisgibt, womöglich ohne dass das Opfer dies bemerkt. Man nennt dies in Hackerkreisen „Social Engineering“. Gegen diese Art von Angriff hilft nur Aufklärung und ein bewusster Umgang mit

Information und Sprache. Einbrüchen auf Rechnersystemen geht oft eine Art Social-Engineering-Angriff, etwa auf das Empfangspersonal, Dienstleister in der Firma oder auch Familienmitglieder, voraus, der erst viel später bemerkt wird. Jemand, der (unbefugt) Zugriff auf Daten erlangen will, könnte auch die traditionellste Methode benutzen, denn die Hardware selbst ist ein Angriffspunkt. Der Rechner muss gegen Entnahme, Austausch und Sabotage von Teilen und Gesamteinheit (und dem Backup der Daten!) sicher verstaubt sein - dazu kann auch eine eventuell vorhandene Netzwerkleitung oder ein Stromkabel gehören. Außerdem muss der Startvorgang abgesichert sein, denn allgemein bekannte Tastenkombinationen können den Rechner zu speziellen Reaktionen veranlassen. Dagegen hilft das Setzen von BIOS- und Bootloaderpasswörtern. Serielle Schnittstellen mit seriellen Terminals sind heute zwar immer noch gebräuchlich, werden aber kaum noch an neuen Arbeitsplätzen installiert. Ein serielles Terminal stellt eine besondere Art des Zugriffs dar: Es ist keine Netzwerkschnittstelle, da kein Netzwerkprotokoll zur Kommunikation zwischen den Systemeinheiten verwendet wird. Ein simples Kabel (oder eine Infrarotschnittstelle) wird als Übertragungsmedium für einfache Zeichen verwendet. Das Kabel selbst ist dabei der einfachste Angriffspunkt: Man muss nur einen alten Drucker daran anschließen und kann die Kommunikation aufzeichnen. Was mit einem Drucker möglich ist, geht selbstverständlich mit beliebigem Aufwand auch anders.

Da das Öffnen einer Datei auf einem Rechner anderen Zugriffsbeschränkungen unterliegt als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem Rechner, ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie ist da markiert, wo Daten in Pakete verschnürt werden müssen, um verschickt zu werden und zur Anwendung zu gelangen.

Lokale Sicherheit

Lokale Sicherheit mit den physikalischen Gegebenheiten, in denen der Rechner aufgestellt ist. Wir gehen davon aus, dass Sie Ihren Rechner so aufgebaut haben, dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt. In Bezug auf „Lokale Sicherheit“ besteht die Aufgabe darin, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder die Identität eines anderen Benutzers annehmen kann. Dies gilt im Allgemeinen, im Speziellen sind natürlich besonders `root`-Rechte gemeint, da der Benutzer `root` im System Allmacht hat; er kann unter anderem ohne Passwort zu jedem lokalen Benutzer werden und jede lokale Datei lesen.

Passwörter

Ihr Linux-System speichert Passwörter nicht etwa im Klartext ab und vergleicht ein eingegebenes Passwort mit dem, was gespeichert ist. Bei einem Diebstahl

der Datei, in der die Passwörter stehen, wären dann ja alle Accounts auf Ihrem System kompromittiert. Stattdessen wird Ihr Passwort verschlüsselt abgelegt und jedes Mal, wenn Sie das Passwort eingegeben haben, wird dieses wieder verschlüsselt und das Ergebnis verglichen mit dem, was als verschlüsseltes Passwort abgespeichert ist. Dies macht natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht das Klartextpasswort errechnen kann. Dies erreicht man durch so genannte „Falltüralgorithmen“, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach zurückrechnen und das Passwort sehen, sondern er muss alle möglichen Buchstabenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie Ihres. Bei acht Buchstaben pro Passwort gibt es beträchtlich viele Kombinationen.

Mit ein Argument für die Sicherheit dieser Methode in den 70er Jahren war, dass der verwendete Algorithmus recht langsam ist und Zeit im Sekundenbereich für das Verschlüsseln von einem Passwort brauchte. Heutige PCs schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund dürfen verschlüsselte Passwörter nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar), und die Passwörter dürfen nicht leicht zu erraten sein, für den Fall, dass die verschlüsselten Passwörter wegen eines Fehlers eben doch sichtbar werden. Ein Passwort wie „Phantasie“ umzuschreiben in „Ph@nt@s13“ hilft nicht viel: Solche Vertauschungsregeln können von Knackprogrammen, die Wörterbücher zum Raten benutzen, sehr leicht aufgelöst werden. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für den Benutzer eine persönliche Bedeutung haben, etwa die Anfangsbuchstaben der Wörter eines Satzes, oder nehmen Sie zum Beispiel einen Buchtitel wie „Der Name der Rose“ von Umberto Eco. Daraus gewinnen Sie ein gutes Passwort: „DNdRvUE9“. Ein Passwort wie „Bierjunge“ oder „Jasmin76“ würde schon jemand erraten können, der Sie oberflächlich gut kennt.

Der Bootvorgang

Verhindern Sie, dass mit einer Diskette oder einer CD-ROM gebootet werden kann, indem Sie die Laufwerke ausbauen oder indem Sie ein BIOS-Passwort setzen und im BIOS ausschließlich das Booten von Festplatte erlauben.

Linux Systeme starten gewöhnlicherweise mit einem Bootloader, der es erlaubt, zusätzliche Optionen an den zu startenden Kernel weiterzugeben. Solche Optionen sind im hohem Maße sicherheitskritisch, weil der Kernel ja nicht nur mit `root`-Rechten läuft, sondern die `root`-Rechte von Anfang an vergibt. Wenn Sie LILO als Bootloader verwenden, können Sie dies durch Vergabe eines weiteren Passwortes in `/etc/lilo.conf` verhindern (siehe [Booten und Bootmanager](#) auf Seite 85).

Zugriffsrechte

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für eine jeweilige Aufgabe zu arbeiten. Es ist definitiv nicht nötig, seine E-Mails als `root` zu lesen und zu schreiben. Wenn das Mailprogramm (MUA = Mail User Agent), mit dem Sie arbeiten, einen Fehler hat, dann wirkt sich dieser Fehler mit genau den Rechten aus, die Sie zum Zeitpunkt des des Angriffs hatten. Hier geht es also auch um Schadensminimierung.

Die einzelnen Rechte der weit über 200.000 Dateien einer SuSE-Distribution sind sorgfältig vergeben. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien nur unter größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Rechte der Dateien achten. Erfahrene und sicherheitsbewusste Admins verwenden bei dem Kommando `ls` stets die Option `-l` für eine ausführliche Liste der Dateien mitsamt den Zugriffsrechten, so dass sie eventuell falsch gesetzte Dateirechte gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können, sondern auch dass die veränderten Dateien von `root` ausgeführt oder im Fall von Konfigurationsdateien von Programmen als `root` benutzt werden können. Damit könnte ein Angreifer seine Rechte beträchtlich ausweiten. Man nennt solche Angriffe dann Kuckuckseier, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kuckuck seine Eier von fremden Vögeln ausbrüten lässt.

SuSE-Systeme verfügen über die Dateien `permissions`, `permissions.easy`, `permissions.secure` und `permissions.paranoid` im Verzeichnis `/etc`. In diesen Dateien werden besondere Rechte wie etwa welt-schreibbare Verzeichnisse oder für Dateien `setuser-ID-bits` festgelegt, d. h. das Programm läuft dann nicht mit der Berechtigung des Eigentümers des Prozesses, der es gestartet hat, sondern mit der Berechtigung des Eigentümers der Datei, und das ist in der Regel `root`. Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Änderungen festhalten kann.

Die Auswahl, welche der Dateien für Konfigurationsprogramme von SuSE zur Vergabe der Rechte benutzt werden sollen, können Sie auch komfortabel mit YaST2 unter dem Menüpunkt 'Sicherheit' treffen. Mehr zu diesem Thema erfahren Sie direkt aus der Datei `/etc/permissions` und der Manpage des Kommandos `chmod` (man `chmod`).

Buffer overflows, format string bugs

Wann immer ein Programm Daten verarbeitet, die in beliebiger Form unter Einfluss eines Benutzers stehen oder standen, ist besondere Vorsicht geboten. Diese Vorsicht gilt in der Hauptsache für den Programmierer der Anwendung: Er muss sicherstellen, dass die Daten durch das Programm richtig interpretiert

werden, dass die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind und dass er die Daten in konsistenter Art und Weise durch sein eigenes Programm und die dafür definierten Schnittstellen weiterreicht.

Ein „Buffer Overflow“ passiert dann, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer eigentlich ist. Es könnte sein, dass die Daten (die vom Benutzer kamen) etwas mehr Platz verlangen, als im Puffer zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenze hinaus ist es unter Umständen möglich, dass ein Programm aufgrund der Daten, die er eigentlich nur verarbeiten soll, Programmsequenzen ausführt, die unter dem Einfluss des Users und nicht des Programmiers stehen. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Rechten abläuft (siehe Abschnitt [Zugriffsrechte](#) auf der vorherigen Seite). „Format String Bugs“ funktionieren etwas anders, verwenden aber wieder user-input, um das Programm von seinem eigentlichen Weg abzubringen.

Diese Programmierfehler werden normalerweise bei Programmen ausgebeutet (engl. *exploit*), die mit gehobenen Privilegien ausgeführt werden, also `setuid`- und `setgid`-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte von den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe Abschnitt [Zugriffsrechte](#) auf der vorherigen Seite).

Da „Buffer Overflows“ und „Format String Bugs“ Fehler bei der Behandlung von Benutzerdaten sind, sind sie nicht notwendigerweise nur ausbeutbar, wenn man bereits Zugriff auf ein lokales „login“ hat. Viele der bekannt gewordenen Fehler können über eine Netzwerkverbindung ausgenutzt werden. Deswegen sind „Buffer Overflows“ und „Format String Bugs“ nicht direkt auf den lokalen Rechner oder das Netzwerk klassifizierbar.

Viren

Entgegen andersartiger Verlautbarungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als „Proof-of-Concept“ geschrieben worden, als Beweis, dass die Technik funktioniert. Allerdings ist noch keiner dieser Viren in „freier Wildbahn“ beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt, ohne den sie nicht überlebensfähig sind. Dieser Wirt ist ein Programm oder ein wichtiger Speicherbereich für das System, etwa der Master-Boot-Record, und er muss für den Programmcode des Virus beschreibbar sein. Linux hat aufgrund seiner Multi-User Fähigkeiten die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, also insbesondere Systemdateien. Wenn Sie als `root` arbeiten, erhöhen Sie also die Wahrscheinlichkeit, dass Ihr System von solch einem Virus infiziert wird. Berücksichtigen

Sie aber die Regel der geringstmöglichen Privilegien, ist es Schwierigkeiten unter Linux einen Virus zu bekommen. Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie aus dem Internet bezogen haben und dessen genaue Herkunft Sie nicht kennen. SuSE-rpm Pakete sind kryptographisch signiert und tragen mit dieser digitalen Unterschrift das Markenzeichen der Sorgfalt beim Bau der Pakete bei SuSE. Viren sind klassische Symptome dafür, dass auch ein hochsicheres System unsicher wird, wenn der Administrator oder auch der Benutzer ein mangelndes Sicherheitsbewusstsein hat.

Viren sind nicht mit Würmern zu verwechseln, die Phänomene auch der Netzwerksicherheit sind und keinen Wirt brauchen, um sich zu verbreiten.

Netzwerksicherheit

Bei der lokalen Sicherheit war es die Aufgabe, die Benutzer, die an demselben Rechner arbeiten, voneinander zu trennen, insbesondere den Benutzer `root`. Im Gegensatz dazu soll bei der Netzwerksicherheit das ganze System gegen Angriffe über das Netzwerk geschützt werden. Benutzerauthentifizierung beim klassischen Einloggen durch Benutzerkennung und Passwort gehört zur lokalen Sicherheit. Beim Einloggen über eine Netzwerkverbindung muss man differenzieren zwischen beiden Sicherheitsaspekten: bis zur erfolgten Authentifizierung spricht man von Netzwerksicherheit, nach dem Login geht es um lokale Sicherheit.

X-Windows (X11-Authentifizierung)

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X11, dem Windowing-System von Unix, gilt dies in besonderem Maße! Sie können sich ohne Weiteres auf einem entfernten Rechner einloggen und dort ein Programm starten, welches dann über das Netzwerk auf Ihrem Rechner angezeigt wird.

Wenn nun ein X-Client über das Netzwerk bei unserem X-Server angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (das Display), gegen unberechtigte Zugriffe schützen. Konkret heißt das hier, dass das Client-Programm Rechte bekommen muss. Bei X-Windows geschieht dies auf zwei verschiedene Arten: Host-basierte und cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Rechners, auf dem das Client-Programm laufen soll und wird mit dem Programm `xhost` kontrolliert. Das Programm `xhost` trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank im X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Es könnte noch ein zweiter Benutzer auf dem Rechner mit dem Client-Programm aktiv sein, und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server. Deswegen soll hier

auch nicht näher auf diese Methoden eingegangen werden. Die Manpage des `xhost`-Kommandos gibt mehr Aufschluss über die Funktionsweise (und enthält ebenfalls die Warnung!).

Bei „cookie“-basierter Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der legitim eingeloggte Benutzer kennen, als einem Passwort ähnliches Ausweismittel verwendet. Dieses „cookie“ (das englische Wort *cookie* bedeutet Keks und meint hier die chinesischen *fortune cookies*, die einen Spruch enthalten) wird in der Datei `.xauthority` im `home`-Verzeichnis des Benutzers beim login abgespeichert und steht somit jedem X-Windows-client, der ein Fenster beim X-Server zur Anzeige bringen will, zur Verfügung. Das Programm `xauth` gibt dem Benutzer das Werkzeug, die Datei `.xauthority` zu untersuchen. Wenn Sie `.xauthority` aus Ihrem `home`-Verzeichnis löschen oder umbenennen, dann können Sie keine weiteren Fenster von neuen X-Clients mehr öffnen. Näheres über Sicherheitsaspekte von X-Windows erfahren Sie in der manpage von `Xsecurity` (`man Xsecurity`).

`ssh` (secure shell) kann über eine vollständig verschlüsselte Netzverbindung für einen Benutzer transparent (also nicht direkt sichtbar) die Verbindung zu einem X-Server weiterleiten. Man spricht von „X11-forwarding“. Dabei wird auf der Server-Seite ein X-Server simuliert und bei der Shell auf der remote-Seite die `DISPLAY`-Variable gesetzt.

Achtung

Wenn Sie den Rechner, auf dem Sie sich einloggen, nicht als sicher betrachten, dann sollten Sie auch keine X-Windows-Verbindungen weiterleiten lassen. Mit eingeschaltetem „X11-forwarding“ könnten sich auch Angreifer über Ihre `ssh`-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatur belauschen.

Achtung

Buffer Overflows und Format String Bugs

Nicht direkt klassifizierbar in lokal und remote gilt das im Abschnitt „Lokale Sicherheit“ über „Buffer Overflows“ und „Format String Bugs“ Gesagte äquivalent für Netzwerksicherheit. Wie auch bei den lokalen Varianten dieser Programmierfehler führen Buffer Overflows bei Netzwerkdiensten meistens zu `root`-Rechten. Sollte dies nicht der Fall sein, dann könnte sich der Angreifer zumindest Zugang zu einem unprivilegierten lokalen Account verschaffen, mit dem er dann weitere (lokale) Sicherheitsprobleme ausnutzen kann, falls diese vorhanden sind.

Über das Netzwerk ausbeutbare Buffer Overflows und Format String Bugs sind wohl die häufigsten Varianten von remote-Angriffen überhaupt. Auf Sicher-

heitsmailinglisten werden so genannte „exploits“ herumgereicht, d. h. Programme, die die frisch gefundenen Lücken ausnutzen. Auch jemand, der nicht die genauen Details der Lücke kennt, kann damit die Lücke ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von „exploitcodes“ generell die Sicherheit von Betriebssystemen erhöht hat, was sicherlich daran liegt, dass Betriebssystemhersteller dazu gezwungen waren, die Probleme in ihrer Software zu beseitigen. Da bei freier Software der Sourcecode für jedermann erhältlich ist (SuSE-Linux liefert alle verfügbaren Quellen mit), kann jemand, der eine Lücke mitsamt „exploitcode“ findet, auch gleichzeitig noch einen Reparaturvorschlag für das Problem anbieten.

DoS — Denial of Service

Ziel dieser Art von Angriff ist das Einstellen des Dienstes (oder gleich des ganzen Systems). Dies kann auf verschiedenste Arten passieren: Durch Überlastung, durch Beschäftigung mit unsinnigen Paketen oder durch Ausnutzen von „Remote Buffer Overflows“, die nicht direkt zum Ausführen von Programmen auf der remote-Seite ausbeutbar sind.

Der Zweck eines DoS mag meistens darin begründet sein, dass der Dienst einfach nicht mehr verfügbar ist. Dass ein Dienst fehlt, kann aber weitere Konsequenzen haben. Siehe „man in the middle: sniffing, tcp connection hijacking, spoofing“ und „DNS poisoning“.

man in the middle: sniffing, tcp connection hijacking, spoofing

Ganz allgemein gilt: Ein Angriff vom Netzwerk, bei der der Angreifer eine Position zwischen zwei Kommunikationspartnern einnimmt, nennt sich „man in the middle attack“. Sie haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar: Der Angreifer nimmt die Verbindung entgegen und stellt, damit das Opfer nichts merkt, selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Rechner geöffnet, weil dieser sich als das Ziel ausgibt. Der einfachste „man in the middle attack“ ist ein „sniffer“. Er belauscht einfach nur die Netzverbindungen, die an ihm vorüber geführt werden (sniffing = engl. schnüffeln). Komplexer wird es, wenn der Angreifer in der Mitte versucht, eine etablierte, bestehende Verbindung zu übernehmen (entführen = engl. hijacking). Dafür muss der Angreifer die Pakete, die an ihm vorbeigeführt werden, eine Weile lang analysiert haben, damit er die richtigen TCP-Sequenznummern der TCP-Verbindung vorhersagen kann. Wenn er dann die Rolle des Ziels der Verbindung übernimmt, merkt das das Opfer, weil auf der Seite des Opfers die Verbindung als ungültig terminiert wird.

Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen „hijacking“ gesichert sind und bei denen zu Beginn der Verbindung eine Authentifizierung stattfindet. „Spoofing“ nennt sich das Verschicken von Paketen mit modifizierten Absenderdaten, also hauptsächlich der IP Adresse. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`root`) darf.

Viele der Angriffsmöglichkeiten kommen in Kombination mit einem DoS vor. Gibt es eine Möglichkeit, einen Rechner schlagartig vom Netzwerk zu trennen (wenn auch nur für kurze Zeit), dann wirkt sich das förderlich auf einen aktiven Angriff aus, weil keine Störungen mehr erwartet werden müssen.

DNS poisoning

Der Angreifer versucht, mit gefälschten („gespoofen“) DNS-Antwortpaketen den cache eines DNS-Servers zu vergiften (engl. *poisoning*), so dass dieser die gewünschte Information an ein Opfer weitergibt, das danach fragt. Um einem DNS-Server solche falschen Informationen glaubhaft zuschieben zu können, muss der Angreifer normalerweise einige Pakete des Servers bekommen und analysieren. Weil viele Server ein Vertrauensverhältnis zu anderen Rechnern aufgrund ihrer IP Adresse oder ihres Hostnamens konfiguriert haben, kann ein solcher Angriff trotz eines gehörigen Aufwands recht schnell Früchte tragen. Voraussetzung ist allerdings eine gute Kenntnis der Vertrauensstruktur zwischen diesen Rechnern. Ein zeitlich genau abgestimmter DoS gegen einen DNS-Server, dessen Daten gefälscht werden sollen, ist aus Sicht des Angreifers meistens nicht vermeidbar.

Abhilfe schafft wieder eine kryptographisch verschlüsselte Verbindung, die die Identität des Ziels der Verbindung verifizieren kann.

Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied: Ein Wurm muss keinerlei Wirtsprogramm infizieren, und er ist darauf spezialisiert, sich möglichst schnell im Netzwerk zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen wohlbekannte Sicherheitslücken von Serverprogrammen wie `bind8` oder `lprNG`. Man kann sich relativ einfach gegen Würmer schützen, weil zwischen dem Zeitpunkt des Bekanntwerdens der ausgenutzten Lücken bis zum Auftauchen des Wurms normalerweise einige Tage vergehen, so dass update-Pakete vorhanden sind. Natürlich setzt dies voraus, dass der Administrator die Security-updates auch in seine Systeme einspielt.

Tipps und Tricks: Allgemeine Hinweise

Information: Für einen effizienten Umgang mit dem Bereich Sicherheit ist es nötig, mit den Entwicklungen Schritt zu halten und auf dem Laufenden zu sein, was die neuesten Sicherheitsprobleme angeht. Ein sehr guter Schutz gegen Fehler aller Art ist das schnellstmögliche Einspielen von update-Paketen, die von einem Security-Announcement angekündigt werden. Die SuSE-security-Announcements werden über eine Mailingliste verbreitet, in die Sie sich, den Links unter <http://www.suse.de/security> folgend, eintragen können. suse-security-announce@suse.de ist die erste Informationsquelle für update-Pakete, die vom Security-Team mit neuen Informationen beliefert wird.

Die Mailingliste suse-security@suse.de ist ein lehrreiches Diskussionsforum für den Bereich Sicherheit. Sie können sich auf der gleichen URL wie für suse-security-announce@suse.de für die Liste anmelden.

Eine der bekanntesten Sicherheitsmailinglisten der Welt ist die Liste bugtraq@securityfocus.com. Die Lektüre dieser Liste bei durchschnittlich 15-20 Postings am Tag kann mit gutem Gewissen empfohlen werden. Mehr Information finden Sie auf <http://www.securityfocus.com>.

Einige Grundregeln, die zu kennen nützlich sein kann, sind nachstehend aufgeführt:

- Vermeiden Sie es, als `root` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu benutzen. Das verringert die Chancen für ein Kuckucksei oder einen Virus, und überdies für Fehler Ihrerseits.
- Benutzen Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten remote auszuführen. „ssh“ (secure shell) ist Standard, vermeiden Sie `telnet`, `ftp`, `rsh` und `rlogin`.
- Benutzen Sie keine Authentifizierungsmethoden, die alleine auf der IP-Adresse aufgebaut sind.
- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die Mailinglisten für Announcements der jeweiligen Software (z. B. Beispiel `bind`, `sendmail`, `ssh`). Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.
- Optimieren Sie die Zugriffsrechte auf sicherheitskritische Dateien im System, indem Sie die `/etc/permissions`-Datei Ihrer Wahl an Ihre Bedürfnisse anpassen. Ein `setuid`-Programm, welches kein `setuid`-bit mehr hat, mag zwar nicht mehr wirklich seine Aufgabe erledigen können, aber es

ist in der Regel kein Sicherheitsproblem mehr. Mit einer ähnlichen Vorgehensweise können Sie auf welt-schreibbare Dateien und Verzeichnisse losgehen.

- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer, und es verhindert, dass Ihre Benutzer sich an einen Dienst gewöhnen, den Sie nie absichtlich freigegeben haben (legacy-Problem). Offene Ports (mit socket-Zustand LISTEN) finden Sie mit dem Programm `netstat`. Als Optionen bietet sich an, `netstat -ap` oder `netstat -anp` zu verwenden. Mit der `-p`-Option können Sie gleich sehen, welcher Prozess mit welchem Namen den Port belegt.

Vergleichen Sie die Ergebnisse, die Sie haben, mit einem vollständigen Portscan Ihres Rechners von außen. Das Programm `nmap` ist dafür hervorragend geeignet. Es klopft jeden einzelnen Port ab und kann anhand der Antwort Ihres Rechners Schlüsse über einen hinter dem Port wartenden Dienst ziehen. Scannen Sie niemals einen Rechner ohne das direkte Einverständnis des Administrators, denn dies könnte als aggressiver Akt aufgefasst werden. Denken Sie daran, dass Sie nicht nur TCP-Ports scannen sollten, sondern auf jeden Fall auch UDP-Ports (Optionen `-sS` und `-sU`).

- Zur zuverlässigen Integritätsprüfung der Dateien in Ihrem System sollten Sie `tripwire` benutzen und die Datenbank verschlüsseln, um sie gegen manipulative Zugriffe zu schützen. Darüber hinaus brauchen Sie auf jeden Fall ein Backup dieser Datenbank außerhalb der Maschine auf einem eigenen Datenträger, der nicht über einen Rechner mit einem Netzwerk verbunden ist.
- Seien Sie vorsichtig beim Installieren von Fremdsoftware. Es gab schon Fälle, wo ein Angreifer tar-Archive einer Sicherheitssoftware mit einem trojanischen Pferd versehen hat. Zum Glück wurde dies schnell bemerkt. Wenn Sie ein binäres Paket installieren, sollten Sie sicher sein, woher das Paket kommt.

SuSE rpm-Pakete werden gpg-signiert ausgeliefert. Der Schlüssel, den wir zum Signieren verwenden, ist

ID:9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>

Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

Das Kommando `rpm -checksig paket.rpm` zeigt an, ob die Prüfsumme und die Signatur des (nicht installierten!) Pakets stimmen. Sie finden

den Schlüssel auf der ersten CD einer SuSE-Distribution ab SuSE-7.1 und auf den meisten Keyservern der Welt.

- Überprüfen Sie regelmäßig Ihr Backup der Daten und des Systems. Ohne eine zuverlässige Aussage über die Funktion des Backups ist das Backup unter Umständen wertlos.
- Überwachen Sie Ihre „Logfiles“. Nach Möglichkeit sollten Sie sich ein kleines Script schreiben, welches Ihre Logfiles nach ungewöhnlichen Einträgen absucht. Diese Aufgabe ist alles andere als trivial, denn nur Sie wissen, was ungewöhnlich ist und was nicht.
- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Rechners auf die IP-Adressen einzuschränken, denen der Zugriff auf einen bestimmten Dienst explizit gestattet ist. Nähere Information zu den `tcp_wrappern` finden Sie in der `manual page` von `tcpd(8)` und `hosts_access` (`man tcpd`, `man hosts_access`).
- Als zusätzlichen Schutz zu dem `tcpd` (`tcp_wrapper`) könnten Sie die SuSEfirewall verwenden.
- Legen Sie Ihr Sicherheitsdenken redundant aus: Eine Meldung, die zweimal eintrifft, ist besser als eine, die Sie nie sehen. Dies gilt genauso für Gespräche mit Kollegen.

Zentrale Meldung von neuen Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie die zur Verfügung stehenden update-Pakete), dann wenden Sie sich bitte vertrauensvoll an die E-Mail-Adresse security@suse.de. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. Wir werden uns bemühen, Ihnen so schnell wie möglich zu antworten. Eine pgp Verschlüsselung Ihrer E-Mail ist erwünscht. Unser pgp key ist:

ID:3D25D3D9 1999-03-06 SuSE Security Team <security@suse.de>

Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5

Der Schlüssel liegt auch unter <http://www.suse.de/security> zum Download bereit.

Manual-Page von e2fsck

E2FSCK(8)

E2FSCK(8)

NAME

e2fsck - check a Linux second extended file system

SYNOPSIS

```
e2fsck [ -pacnyrdfvstFSV ] [ -b superblock ] [ -B block-size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j external-journal ] [ device
```

DESCRIPTION

e2fsck is used to check a Linux second extended file system (e2fs). E2fsck also supports ext2 filesystems containing a journal, which are also sometimes known as ext3 filesystems.

device is the special file corresponding to the device (e.g /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock

Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the `mke2fs` program using the `-n` option to print out where the superblocks were created. The `-b` option to `mke2fs`, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, `e2fsck` will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize

Normally, `e2fsck` will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces `e2fsck` to only try locating the superblock at a particular blocksize. If the superblock is not found, `e2fsck` will terminate with a fatal error.

-c This option causes `e2fsck` to run the `badblocks(8)` program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode.

-C This option causes `e2fsck` to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by programs which are running `e2fsck`. If the file descriptor specified is 0, `e2fsck` will print a completion bar as it goes about its business. This requires that `e2fsck` is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging `e2fsck`).

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing `e2fsck` time trials.

-j external-journal

Set the pathname where the external-journal for this filesystem can be found.

-l filename

Add the blocks listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program.

- L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)
- n Open the filesystem read-only, and assume an answer of 'no' to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)
- p Automatically repair ("preen") the file system without any questions.
- r This option does nothing at all; it is provided only for backwards compatibility.
- s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesystem is already in the standard byte-order, e2fsck will take no action.
- S This option will byte-swap the filesystem, regardless of its current byte-order.
- t Print timing statistics for e2fsck. If this option is used twice, additional timing statistics are printed on a pass by pass basis.
- v Verbose mode.
- V Print version information and exit.
- y Assume an answer of 'yes' to all questions; allows e2fsck to be used non-interactively.

EXIT CODE

The exit code returned by e2fsck is the sum of the following conditions:

- 0 - No errors
- 1 - File system errors corrected
- 2 - File system errors corrected, system should be rebooted if file system was mounted

- 4 - File system errors left uncorrected
- 8 - Operational error
- 16 - Usage or syntax error
- 128 - Shared library error

SIGNALS

The following signals have the following effect when sent to e2fsck.

SIGUSR1

This signal causes e2fsck to start displaying a completion bar. (See discussion of the -C option.)

SIGUSR2

This signal causes e2fsck to stop displaying a completion bar.

REPORTING BUGS

Almost any piece of software will have bugs. If you manage to find a filesystem which causes e2fsck to crash, or which e2fsck is unable to repair, please report it to the author.

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trouble, try running the debugfs(8) command and send the output of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuen code(1).

Always include the full version string which e2fsck displays when it is run, so I know which version you are running.

AUTHOR

This version of e2fsck was written by Theodore Ts'o <tytso@mit.edu>.

SEE ALSO

mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.25

September 2001

E2FSCK(8)

Deutsche Übersetzung der GNU General Public License

Der folgende Text folgt im Wesentlichen der inoffiziellen Übersetzung von Katja Lachmann und der Überarbeitung von Peter Gerwinski (31. Oktober 1996, 4. Juni 2000).

Diese Übersetzung wird mit der Absicht angeboten, das Verständnis der *GNU General Public License* (GNU-GPL) zu erleichtern. Es handelt sich jedoch nicht um eine offizielle oder im rechtlichen Sinne anerkannte Übersetzung.

Die *Free Software Foundation* (FSF) ist nicht der Herausgeber dieser Übersetzung, und sie hat diese Übersetzung auch nicht als rechtskräftigen Ersatz für die Original-GNU-GPL (siehe <http://www.gnu.org/copyleft/gpl.html>) anerkannt. Da die Übersetzung nicht sorgfältig von Anwälten überprüft wurde, können die Übersetzer nicht garantieren, dass die Übersetzung die rechtlichen Aussagen der GNU-GPL exakt wiedergibt. Wenn Sie sichergehen wollen, dass von Ihnen geplante Aktivitäten im Sinne der GNU-GPL gestattet sind, halten Sie sich bitte an die englischsprachige Originalversion.

Die *Free Software Foundation* möchte Sie darum bitten, diese Übersetzung nicht als offizielle Lizenzbedingungen für von Ihnen geschriebene Programme zu verwenden. Bitte benutzen Sie hierfür stattdessen die von der *Free Software Foundation* herausgegebene englischsprachige Originalversion.

This is a translation of the GNU General Public License into German. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License. The translation has not been reviewed carefully by lawyers, and therefore the translator cannot be sure that it exactly represents the legal meaning of the GNU General Public License. If

you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to the authentic English version.

The Free Software Foundation strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the Free Software Foundation.

GNU General Public License

Deutsche Übersetzung der Version 2, Juni 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Es ist jedermann gestattet, diese Lizenzurkunde zu vervielfältigen und unveränderte Kopien zu verbreiten; Änderungen sind jedoch nicht erlaubt.

Diese Übersetzung ist kein rechtskräftiger Ersatz für die englischsprachige Originalversion!

Vorwort

Die meisten Softwarelizenzen sind daraufhin entworfen worden, Ihnen die Freiheit zu nehmen, die Software weiterzugeben und zu verändern. Im Gegensatz dazu soll Ihnen die *GNU General Public License*, die Allgemeine Öffentliche GNU-Lizenz, ebendiese Freiheit garantieren. Sie soll sicherstellen, dass die Software für alle Benutzer frei ist. Diese Lizenz gilt für den Großteil der von der *Free Software Foundation* herausgegebenen Software und für alle anderen Programme, deren Autoren ihr Datenwerk dieser Lizenz unterstellt haben. Auch Sie können diese Möglichkeit der Lizenzierung für Ihre Programme anwenden. (Ein anderer Teil der Software der *Free Software Foundation* unterliegt stattdessen der *GNU Library General Public License*, der Allgemeinen Öffentlichen GNU-Lizenz für Bibliotheken.)¹

Die Bezeichnung „freie“ Software bezieht sich auf Freiheit, nicht auf den Preis. Unsere Lizenzen sollen Ihnen die Freiheit garantieren, Kopien freier Software zu verbreiten (und etwas für diesen Service zu berechnen, wenn Sie möchten), die Möglichkeit, die Software im Quelltext zu erhalten oder den Quelltext auf Wunsch zu bekommen. Die Lizenzen sollen garantieren, dass Sie die Software ändern oder Teile davon in neuen freien Programmen verwenden dürfen – und dass Sie wissen, dass Sie dies alles tun dürfen.

Um Ihre Rechte zu schützen, müssen wir Einschränkungen machen, die es jedem verbieten, Ihnen diese Rechte zu verweigern oder Sie aufzufordern, auf

¹Mittlerweile wurde die GNU Library Public License von der GNU Lesser Public License abgelöst.

diese Rechte zu verzichten. Aus diesen Einschränkungen folgen bestimmte Verantwortlichkeiten für Sie, wenn Sie Kopien der Software verbreiten oder sie verändern.

Beispielsweise müssen Sie den Empfängern alle Rechte gewähren, die Sie selbst haben, wenn Sie – kostenlos oder gegen Bezahlung – Kopien eines solchen Programms verbreiten. Sie müssen sicherstellen, dass auch die Empfänger den Quelltext erhalten bzw. erhalten können. Und Sie müssen ihnen diese Bedingungen zeigen, damit sie ihre Rechte kennen.

Wir schützen Ihre Rechte in zwei Schritten: (1) Wir stellen die Software unter ein Urheberrecht (Copyright), und (2) wir bieten Ihnen diese Lizenz an, die Ihnen das Recht gibt, die Software zu vervielfältigen, zu verbreiten und/oder zu verändern.

Um die Autoren und uns zu schützen, wollen wir darüberhinaus sicherstellen, dass jeder erfährt, dass für diese freie Software keinerlei Garantie besteht. Wenn die Software von jemand anderem modifiziert und weitergegeben wird, möchten wir, dass die Empfänger wissen, dass sie nicht das Original erhalten haben, damit irgendwelche von anderen verursachte Probleme nicht den Ruf des ursprünglichen Autors schädigen.

Schließlich und endlich ist jedes freie Programm permanent durch Software-Patente bedroht. Wir möchten die Gefahr ausschließen, dass Distributoren eines freien Programms individuell Patente lizenzieren – mit dem Ergebnis, dass das Programm proprietär würde. Um dies zu verhindern, haben wir klargestellt, dass jedes Patent entweder für freie Benutzung durch jedermann lizenziert werden muss oder überhaupt nicht lizenziert werden darf.

Es folgen die genauen Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung:

Allgemeine Öffentliche GNU-Lizenz

Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung

0. Diese Lizenz gilt für jedes Programm und jedes andere Datenwerk, in dem ein entsprechender Vermerk des Copyright-Inhabers darauf hinweist, dass das Datenwerk unter den Bestimmungen dieser *General Public License* verbreitet werden darf. Im Folgenden wird jedes derartige Programm oder Datenwerk als „das Programm“ bezeichnet; die Formulierung „auf dem Programm basierendes Datenwerk“ bezeichnet das Programm sowie jegliche Bearbeitung des Programms im urheberrechtlichen Sinne, also ein Datenwerk, welches das Programm, auch auszugsweise, sei es unverändert oder verändert und/oder in eine andere Sprache übersetzt, enthält. (Im Folgenden wird die Übersetzung ohne Einschränkung als „Bearbeitung“ eingestuft.) Jeder Lizenznehmer wird im Folgenden als „Sie“ angesprochen.

Andere Handlungen als Vervielfältigung, Verbreitung und Bearbeitung werden von dieser Lizenz nicht berührt; sie fallen nicht in ihren Anwendungsbereich. Der Vorgang der Ausführung des Programms wird nicht eingeschränkt, und die Ausgaben des Programms unterliegen dieser Lizenz nur, wenn der Inhalt ein auf dem Programm basierendes Datenwerk darstellt (unabhängig davon, dass die Ausgabe durch die Ausführung des Programmes erfolgte). Ob dies zutrifft, hängt von den Funktionen des Programms ab.

1. Sie dürfen auf beliebigen Medien unveränderte Kopien des Quelltextes des Programms, wie sie ihn erhalten haben, anfertigen und verbreiten. Voraussetzung hierfür ist, dass Sie mit jeder Kopie einen entsprechenden Copyright-Vermerk sowie einen Haftungsausschluss veröffentlichen, alle Vermerke, die sich auf diese Lizenz und das Fehlen einer Garantie beziehen, unverändert lassen und desweiteren allen anderen Empfängern des Programms zusammen mit dem Programm eine Kopie dieser Lizenz zukommen lassen.

Sie dürfen für den eigentlichen Kopiervorgang eine Gebühr verlangen. Wenn Sie es wünschen, dürfen Sie auch gegen Entgelt eine Garantie für das Programm anbieten.

2. Sie dürfen Ihre Kopie(n) des Programms oder einen Teil davon verändern, wodurch ein auf dem Programm basierendes Datenwerk entsteht; Sie dürfen derartige Bearbeitungen unter den Bestimmungen von Paragraph 1 vervielfältigen und verbreiten, vorausgesetzt, dass zusätzlich alle im Folgenden genannten Bedingungen erfüllt werden:

- a) Sie müssen die veränderten Dateien mit einem auffälligen Vermerk versehen, der auf die von Ihnen vorgenommene Modifizierung und das Datum jeder Änderung hinweist.
- b) Sie müssen dafür sorgen, dass jede von Ihnen verbreitete oder veröffentlichte Arbeit, die ganz oder teilweise von dem Programm oder Teilen davon abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.
- c) Wenn das veränderte Programm normalerweise bei der Ausführung interaktiv Kommandos einliest, müssen Sie dafür sorgen, dass es, wenn es auf dem üblichsten Wege für solche interaktive Nutzung gestartet wird, eine Meldung ausgibt oder ausdruckt, die einen geeigneten Copyright-Vermerk enthält sowie einen Hinweis, dass es keine Gewährleistung gibt (oder anderenfalls, dass Sie Garantie leisten), und dass die Benutzer das Programm unter diesen Bedingungen weiter verbreiten dürfen. Auch

muss der Benutzer darauf hingewiesen werden, wie er eine Kopie dieser Lizenz ansehen kann. (Ausnahme: Wenn das Programm selbst interaktiv arbeitet, aber normalerweise keine derartige Meldung ausgibt, muss Ihr auf dem Programm basierendes Datenwerk auch keine solche Meldung ausgeben.)

Diese Anforderungen gelten für das bearbeitete Datenwerk als Ganzes. Wenn identifizierbare Teile des Datenwerkes nicht von dem Programm abgeleitet sind und vernünftigerweise als unabhängige und eigenständige Datenwerke für sich selbst zu betrachten sind, dann gelten diese Lizenz und ihre Bedingungen nicht für die betroffenen Teile, wenn Sie diese als eigenständige Datenwerke weitergeben. Wenn Sie jedoch dieselben Abschnitte als Teil eines Ganzen weitergeben, das ein auf dem Programm basierendes Datenwerk darstellt, dann muss die Weitergabe des Ganzen nach den Bedingungen dieser Lizenz erfolgen, deren Bedingungen für weitere Lizenznehmer somit auf das gesamte Ganze ausgedehnt werden – und somit auf jeden einzelnen Teil, unabhängig vom jeweiligen Autor.

Somit ist es nicht die Absicht dieses Abschnittes, Rechte für Datenwerke in Anspruch zu nehmen oder Ihnen die Rechte für Datenwerke streitig zu machen, die komplett von Ihnen geschrieben wurden; vielmehr ist es die Absicht, die Rechte zur Kontrolle der Verbreitung von Datenwerken, die auf dem Programm basieren oder unter seiner auszugswweisen Verwendung zusammengestellt worden sind, auszuüben.

Ferner bringt auch das einfache Zusammenlegen eines anderen Datenwerkes, das nicht auf dem Programm basiert, mit dem Programm oder einem auf dem Programm basierenden Datenwerk auf ein- und demselben Speicher- oder Vertriebsmedium dieses andere Datenwerk nicht in den Anwendungsbereich dieser Lizenz.

3. Sie dürfen das Programm (oder ein darauf basierendes Datenwerk gemäß Paragraph 2) als Objectcode oder in ausführbarer Form unter den Bedingungen der Paragraphen 1 und 2 kopieren und weitergeben – vorausgesetzt, dass Sie außerdem eine der folgenden Leistungen erbringen:

- a) Liefern Sie das Programm zusammen mit dem vollständigen zugehörigen maschinenlesbaren Quelltext auf einem für den Datenaustausch üblichen Medium aus, wobei die Verteilung unter den Bedingungen der Paragraphen 1 und 2 erfolgen muss. Oder:
- b) Liefern Sie das Programm zusammen mit einem mindestens drei Jahre lang gültigen schriftlichen Angebot aus, jedem Dritten eine vollständige

maschinenlesbare Kopie des Quelltextes zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen –, wobei der Quelltext unter den Bedingungen der Paragraphen 1 und 2 auf einem für den Datenaustausch üblichen Medium weitergegeben wird. Oder:

- c) Liefern Sie das Programm zusammen mit dem schriftlichen Angebot der Zurverfügungstellung des Quelltextes aus, das Sie selbst erhalten haben. (Diese Alternative ist nur für nicht-kommerzielle Verbreitung zulässig und nur, wenn Sie das Programm als Objectcode oder in ausführbarer Form mit einem entsprechenden Angebot gemäß Absatz b erhalten haben.)

Unter dem Quelltext eines Datenwerkes wird diejenige Form des Datenwerkes verstanden, die für Bearbeitungen vorzugsweise verwendet wird. Für ein ausführbares Programm bedeutet „der komplette Quelltext“: Der Quelltext aller im Programm enthaltenen Module einschließlich aller zugehörigen Modulschnittstellen-Definitionsdateien sowie der zur Kompilation und Installation verwendeten Skripte. Als besondere Ausnahme jedoch braucht der verteilte Quelltext nichts von dem zu enthalten, was üblicherweise (entweder als Quelltext oder in binärer Form) zusammen mit den Hauptkomponenten des Betriebssystems (Kernel, Compiler usw.) geliefert wird, unter dem das Programm läuft – es sei denn, diese Komponente selbst gehört zum ausführbaren Programm.

Wenn die Verbreitung eines ausführbaren Programms oder von Objectcode dadurch erfolgt, dass der Kopierzugriff auf eine dafür vorgesehene Stelle gewährt wird, so gilt die Gewährung eines gleichwertigen Zugriffs auf den Quelltext als Verbreitung des Quelltextes, auch wenn Dritte nicht dazu gezwungen sind, den Quelltext zusammen mit dem Objectcode zu kopieren.

4. Sie dürfen das Programm nicht vervielfältigen, verändern, weiter lizenzieren oder verbreiten, sofern es nicht durch diese Lizenz ausdrücklich gestattet ist. Jeder anderweitige Versuch der Vervielfältigung, Modifizierung, Weiterlizenzierung und Verbreitung ist nichtig und beendet automatisch Ihre Rechte unter dieser Lizenz. Jedoch werden die Lizenzen Dritter, die von Ihnen Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese die Lizenz voll anerkennen und befolgen.

5. Sie sind nicht verpflichtet, diese Lizenz anzunehmen, da Sie sie nicht unterzeichnet haben. Jedoch gibt Ihnen nichts anderes die Erlaubnis, das Programm oder von ihm abgeleitete Datenwerke zu verändern oder zu verbreiten. Diese Handlungen sind gesetzlich verboten, wenn Sie diese Lizenz nicht anerkennen.

Indem Sie das Programm (oder ein darauf basierendes Datenwerk) verändern oder verbreiten, erklären Sie Ihr Einverständnis mit dieser Lizenz und mit allen ihren Bedingungen bezüglich der Vervielfältigung, Verbreitung und Veränderung des Programms oder eines darauf basierenden Datenwerks.

6. Jedes Mal, wenn Sie das Programm (oder ein auf dem Programm basierendes Datenwerk) weitergeben, erhält der Empfänger automatisch vom ursprünglichen Lizenzgeber die Lizenz, das Programm entsprechend den hier festgelegten Bestimmungen zu vervielfältigen, zu verbreiten und zu verändern. Sie dürfen keine weiteren Einschränkungen der Durchsetzung der hierin zugestandenen Rechte des Empfängers vornehmen. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

7. Sollten Ihnen infolge eines Gerichtsurteils, des Vorwurfs einer Patentverletzung oder aus einem anderen Grunde (nicht auf Patentfragen begrenzt) Bedingungen (durch Gerichtsbeschluss, Vergleich oder anderweitig) auferlegt werden, die den Bedingungen dieser Lizenz widersprechen, so befreien Sie diese Umstände nicht von den Bestimmungen dieser Lizenz. Wenn es Ihnen nicht möglich ist, das Programm unter gleichzeitiger Beachtung der Bedingungen in dieser Lizenz und Ihrer anderweitigen Verpflichtungen zu verbreiten, dann dürfen Sie als Folge das Programm überhaupt nicht verbreiten. Wenn zum Beispiel ein Patent nicht die gebührenfreie Weiterverbreitung des Programms durch diejenigen erlaubt, die das Programm direkt oder indirekt von Ihnen erhalten haben, dann besteht der einzige Weg, sowohl das Patentrecht als auch diese Lizenz zu befolgen, darin, ganz auf die Verbreitung des Programms zu verzichten.

Sollte sich ein Teil dieses Paragraphen als ungültig oder unter bestimmten Umständen nicht durchsetzbar erweisen, so soll dieser Paragraph seinem Sinne nach angewandt werden; im übrigen soll dieser Paragraph als Ganzes gelten.

Zweck dieses Paragraphen ist nicht, Sie dazu zu bringen, irgendwelche Patente oder andere Eigentumsansprüche zu verletzen oder die Gültigkeit solcher Ansprüche zu bestreiten; dieser Paragraph hat einzig den Zweck, die Integrität des Verbreitungssystems der freien Software zu schützen, das durch die Praxis öffentlicher Lizenzen verwirklicht wird. Viele Leute haben großzügige Beiträge zu dem großen Angebot der mit diesem System verbreiteten Software im Vertrauen auf die konsistente Anwendung dieses Systems geleistet; es liegt am Autor/Geber, zu entscheiden, ob er die Software mittels irgendeines anderen Systems verbreiten will; ein Lizenznehmer hat auf diese Entscheidung keinen Einfluss.

Dieser Paragraph ist dazu gedacht, deutlich klarzustellen, was als Konsequenz aus dem Rest dieser Lizenz betrachtet wird.

8. Wenn die Verbreitung und/oder die Benutzung des Programms in bestimmten Staaten entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann der Urheberrechtsinhaber, der das Programm unter diese Lizenz gestellt hat, eine explizite geographische Begrenzung der Verbreitung angeben, in der diese Staaten ausgeschlossen werden, so dass die Verbreitung nur innerhalb und zwischen den Staaten erlaubt ist, die nicht ausgeschlossen sind. In einem solchen Fall beinhaltet diese Lizenz die Beschränkung, als wäre sie in diesem Text niedergeschrieben.

9. Die *Free Software Foundation* kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der *General Public License* veröffentlichen. Solche neuen Versionen werden vom Grundprinzip her der gegenwärtigen entsprechen, können aber im Detail abweichen, um neuen Problemen und Anforderungen gerecht zu werden.

Jede Version dieser Lizenz hat eine eindeutige Versionsnummer. Wenn in einem Programm angegeben wird, dass es dieser Lizenz in einer bestimmten Versionsnummer oder „jeder späteren Version“ (*„any later version“*) unterliegt, so haben Sie die Wahl, entweder den Bestimmungen der genannten Version zu folgen oder denen jeder beliebigen späteren Version, die von der *Free Software Foundation* veröffentlicht wurde. Wenn das Programm keine Versionsnummer angibt, können Sie eine beliebige Version wählen, die je von der *Free Software Foundation* veröffentlicht wurde.

10. Wenn Sie den Wunsch haben, Teile des Programms in anderen freien Programmen zu verwenden, deren Bedingungen für die Verbreitung anders sind, schreiben Sie an den Autor, um ihn um die Erlaubnis zu bitten. Für Software, die unter dem Copyright der *Free Software Foundation* steht, schreiben Sie an die *Free Software Foundation*; wir machen zu diesem Zweck gelegentlich Ausnahmen. Unsere Entscheidung wird von den beiden Zielen geleitet werden, zum einen den freien Status aller von unserer freien Software abgeleiteten Datenwerke zu erhalten und zum anderen das gemeinschaftliche Nutzen und Wiederverwenden von Software im allgemeinen zu fördern.

Keine Gewährleistung

11. Da das Programm ohne jegliche Kosten lizenziert wird, besteht keinerlei Gewährleistung für das Programm, soweit dies gesetzlich zulässig ist. Sofern nicht anderweitig schriftlich bestätigt, stellen die Copyright-Inhaber und/oder Dritte das Programm so zur Verfügung, „wie es ist“, ohne irgendeine Gewährleistung, weder ausdrücklich noch implizit, einschließlich – aber nicht begrenzt auf – Marktreife oder Verwendbarkeit für einen bestimmten

Zweck. Das volle Risiko bezüglich Qualität und Leistungsfähigkeit des Programms liegt bei Ihnen. Sollte sich das Programm als fehlerhaft herausstellen, liegen die Kosten für notwendigen Service, Reparatur oder Korrektur bei Ihnen.

12. In keinem Fall, außer wenn durch geltendes Recht gefordert oder schriftlich zugesichert, ist irgendein Copyright-Inhaber oder irgendein Dritter, der das Programm wie oben erlaubt modifiziert oder verbreitet hat, Ihnen gegenüber für irgendwelche Schäden haftbar, einschließlich jeglicher allgemeiner oder spezieller Schäden, Schäden durch Seiteneffekte (Nebenwirkungen) oder Folgeschäden, die aus der Benutzung des Programms oder der Unbenutzbarkeit des Programms folgen (einschließlich – aber nicht beschränkt auf – Datenverluste, fehlerhafte Verarbeitung von Daten, Verluste, die von Ihnen oder anderen getragen werden müssen, oder dem Unvermögen des Programms, mit irgendeinem anderen Programm zusammenzuarbeiten), selbst wenn ein Copyright-Inhaber oder Dritter über die Möglichkeit solcher Schäden unterrichtet worden war.

Ende der Bedingungen

Anhang: Wie Sie diese Bedingungen auf Ihre eigenen, neuen Programme anwenden können

Wenn Sie ein neues Programm entwickeln und wollen, dass es vom größtmöglichen Nutzen für die Allgemeinheit ist, dann erreichen Sie das am besten, indem Sie es zu freier Software machen, die jeder unter diesen Bestimmungen weiterverbreiten und verändern kann.

Um dies zu erreichen, fügen Sie die folgenden Vermerke zu Ihrem Programm hinzu. Am sichersten ist es, sie an den Anfang einer jeden Quelldatei zu stellen, um den Gewährleistungsausschluss möglichst deutlich darzustellen; zumindest aber sollte jede Datei eine Copyright-Zeile besitzen sowie einen kurzen Hinweis darauf, wo die vollständigen Vermerke zu finden sind.

eine Zeile mit dem Programmnamen und einer kurzen Beschreibung
Copyright (C) 19yy Name des Autors

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty

of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Auf Deutsch:

eine Zeile mit dem Programmnamen und einer kurzen Beschreibung
Copyright (C) 19jj *Name des Autors*

Dieses Programm ist freie Software. Sie können es unter den Bedingungen der GNU General Public License, wie von der Free Software Foundation veröffentlicht, weitergeben und/oder modifizieren, entweder gemäß Version 2 der Lizenz oder (nach Ihrer Option) jeder späteren Version.

Die Veröffentlichung dieses Programms erfolgt in der Hoffnung, dass es Ihnen von Nutzen sein wird, aber OHNE IRGEND EINE GARANTIE, sogar ohne die implizite Garantie der MARKTREIFE oder der VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. Details finden Sie in der GNU General Public License.

Sie sollten eine Kopie der GNU General Public License zusammen mit diesem Programm erhalten haben. Falls nicht, schreiben Sie an die Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Fügen Sie auch einen kurzen Hinweis hinzu, wie Sie elektronisch und per Brief erreichbar sind.

Wenn Ihr Programm interaktiv ist, sorgen Sie dafür, dass es nach dem Start einen kurzen Vermerk ausgibt:

Gnomovision version 69, Copyright (C) 19yy *Name des Autors*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

Auf Deutsch:

Gnomovision Version 69, Copyright (C) 19jj *Name des Autors*

Für Gnomovision besteht KEINERLEI GARANTIE; geben Sie 'show w' für Details ein. Gnomovision ist freie Software, die Sie unter bestimmten Bedingungen weitergeben dürfen; geben Sie 'show c' für Details ein.

Die hypothetischen Kommandos `show w` und `show c` sollten die entsprechenden Teile der GNU-GPL anzeigen. Natürlich können die von Ihnen verwendeten Kommandos anders heißen als `show w` und `show c`; es könnten auch Mausklicks oder Menüpunkte sein – was immer am besten in Ihr Programm passt.

Soweit vorhanden, sollten Sie auch Ihren Arbeitgeber (wenn Sie als Programmierer arbeiten) oder Ihre Schule einen Copyright-Verzicht für das Programm unterschreiben lassen. Hier ein Beispiel. Die Namen müssen Sie natürlich ändern.

Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

Unterschrift von Ty Coon, 1 April 1989

Ty Coon, President of Vice

Auf Deutsch:

Die Yoyodyne GmbH erhebt keinen urheberrechtlichen Anspruch auf das von James Hacker geschriebene Programm , Gnomovision' (einem Schrittmacher für Compiler).

Unterschrift von Ty Coon, 1. April 1989

Ty Coon, Vizepräsident

Diese *General Public License* gestattet nicht die Einbindung des Programms in proprietäre Programme. Ist Ihr Programm eine Funktionsbibliothek, so kann es sinnvoller sein, das Binden proprietärer Programme mit dieser Bibliothek zu gestatten. Wenn Sie dies tun wollen, sollten Sie die GNU Library General Public License anstelle dieser Lizenz verwenden.

Literaturverzeichnis

- [Alm96] ALMESBERGER, Werner: *LILO User's guide*, 1996. – (siehe Datei `/usr/share/doc/lilo/user.dvi`)
- [Bai97] BAILEY, Edward C.: *Maximum RPM*. Red Hat, 1997. – (ISBN 1-888172-78-9)
- [BBD⁺97] BECK, Michael; BÖHME, Harald; DZIADZKA, Mirko; KUNITZ, Ulrich; MAGNUS, Robert ; VERWORNER, Dirk: *Linux-Kernel-Programmierung*. 4. Aufl. Addison Wesley GmbH, 1997. – (ISBN 3-8273-1144-6)
- [BD98] BORKNER-DELCARLO, Olaf: *Linux im kommerziellen Einsatz*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19465-7)
- [BD99] BORKNER-DELCARLO, Olaf: *Das Samba-Buch*. SuSE PRESS, 1999. – (ISBN 3-930419-93-9)
- [CAR93] COSTALES, Bryan; ALLMAN, Eric ; RICKERT, Neil: *sendmail*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-056-2)
- [CB96] CHESWICK, William R.; BELLOVIN, Steven M.: *Firewalls und Sicherheit im Internet*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-875-x)
- [CZ96] CHAPMAN, Brent; ZWICKY, Elisabeth D.: *Einrichten von Internet Firewalls. Sicherheit im Internet gewährleisten..* O'Reilly & Associates, Inc., 1996. – (ISBN 3-930673312)
- [DR99] DAWSON, Terry; RUBINI, Alessandro: *NET3-4 HOWTO*, v1.5, August 1999. – (siehe Datei `/usr/share/doc/howto/en/NET3-4-HOWTO.gz`)
- [EH98] ECKEL, George; HARE, Chris: *Linux – Internet Server*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19044-9)

- [FCR93] FANG, Chin; CROSSON, Bob ; RAYMOND, Eric S.: *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*, 1993. – (siehe Datei /usr/x11/lib/x11/doc/VideoModes.doc)
- [Fis00] FISCHER, Thorsten: *GUI-Programmierung mit GTK+ (Handbuch und Referenz)*. SuSE PRESS, 2000. – ISBN (3-934678-42-4)
- [Fri93] FRISCH, Aileen: *Essential System Administration*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-80-3)
- [Gil92] GILLY, Daniel: *UNIX in a nutshell: System V Edition*. O'Reilly & Associates, Inc., 1992. – (ISBN 1-56592-001-5)
- [GMR97] GOOSSENS, Michel; MITTELBACH, Frank ; RAHTZ, Sebastian: *The L^AT_EX Graphics Companion*. Addison Wesley Longman, 1997. – (ISBN 0-201-85469-4)
- [GMS94] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *The L^AT_EX Companion*. Addison Wesley GmbH, 1994. – (ISBN 0-201-54199-8)
- [GMS96] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *Der L^AT_EX-Begleiter*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-646-3)
- [GR99] GOOSSENS, Michel; RAHTZ, Sebastian: *The L^AT_EX Web Companion*. Addison Wesley Longman, 1999. – (ISBN 0-201-43322-7)
- [GS93] GARFINKEL, Simson; SPAFFORD, Gene: *Practical UNIX Security*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-72-2)
- [Hei96] HEIN, Jochen: *Linux-Companion zur Systemadministration*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-869-5)
- [Her92] HEROLD, H.: *UNIX Grundlagen*. Addison Wesley GmbH, 1992. – (ISBN 3-89319-542-8)
- [HHMK96] HETZE, Sebastian; HOHNDEL, Dirk; MÜLLER, Martin ; KIRCH, Olaf: *Linux Anwenderhandbuch*. 6. Aufl. LunetIX Softfair, 1996. – (ISBN 3-929764-05-9)
- [Hof97] HOFFMANN, Erwin: EMail-Gateway mit qmail. In: *iX* 12 (1997), S. 108ff.
- [HR98] HÖLZER, Matthias; RÖHRIG, Bernhard: *KDE – Das K Desktop Environment*. Computer & Literatur, 1998. – (ISBN 3-932311-50-7)

- [Hun95] HUNT, Craig: *TCP/IP Netzwerk Administration*. O'Reilly & Associates, Inc., 1995. – (ISBN 3-930673-02-9)
- [JT98] JOHNSON, Michael K.; TROAN, Erik W.: *Anwendungen entwickeln unter Linux*. Addison Wesley GmbH, 1998. – (ISBN 3-8273-1449-6)
- [Kie95] KIENLE, Micheal: TIS: Toolkit für anwendungsorientierte Firewall-Systeme. In: *iX* 8 (1995), S. 140ff.
- [Kir95] KIRCH, Olaf: *LINUX Network Administrator's Guide*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-087-2)
- [Kof99] KOFLER, Michael: *Linux – Installation, Konfiguration, Anwendung*. 4. Aufl. Addison Wesley GmbH, 1999. – (ISBN 3-8273-1475-5)
- [Kop94] KOPKA, Helmut: *L^AT_EX-Einführung*. Addison Wesley GmbH, 1994. – (ISBN 3-89319-664-1)
- [Kopff] KOPKA, Helmut: *L^AT_EX*. Addison Wesley GmbH, 1996 ff. – 3 Bde. (ISBN 3-8273-1025-3; 3-8273-1229-9; 3-89319-666-8)
- [Kun95] KUNITZ, Ulrich: Sicherheit fast kostenlos: Einrichtung eines kostenlosen Firewall-Systems. In: *iX* 9 (1995), S. 176ff.
- [Lam90] LAMB, Linda: *Learning the vi Editor*. O'Reilly & Associates, Inc., 1990. – (ISBN 0-937175-67-6)
- [Lef96] LEFFLER, Sam: *HylaFAX Home Page*, 1996
- [Meg98] MEGGINSON, David: *Structuring XML Documents*. Prentice-Hall, 1998. – ISBN (0-13-642299-3)
- [Moh98] MOHR, James: *UNIX-Windows-Integration*. International Thomson Publishing, 1998. – (ISBN 3-8266-4032-2)
- [OT92] O'REILLY, Tim; TODINO, Grace: *Managing UUCP and Usenet*. O'Reilly & Associates, Inc., 1992. – (ISBN 0-937175-93-5)
- [POL97] PEEK, Jerry; O'REILLY, Tim ; LOUKIDES, Mike: *Unix Power Tools*. 2. Aufl. Sebastopol : O'Reilly & Associates, Inc., 1997
- [Rub98] RUBINI, Alessandro: *Linux-Gerätetreiber*. O'Reilly & Associates, Inc., 1998. – (ISBN 3-89721-122-X)
- [Sch98] SCHEIDERER, Jürgen: Sicherheit Kostenlos - Firewall mit Linux. In: *iX* 12 (1998)

- [Sto98] STOLL, Clifford: *Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer-TB.-Vlg., 1998. – (ISBN 3596139848)
- [SuS02a] *SuSE Linux. Basis*. 1. Nürnberg : SuSE Linux AG, 2002
- [SuS02b] *SuSE Linux. Benutzerhandbuch*. 1. Nürnberg : SuSE Linux AG, 2002
- [SuS02c] *SuSE Linux. Die Programme*. 1. Nürnberg : SuSE Linux AG, 2002
- [The96] THE XFREE86™-TEAM: *XF86Config(4/5) – Configuration File for Xfree86™*, 1996. – Manual-Page zu XFree86™
- [TSP93] TODINO, Grace; STRANG, John ; PEEK, Jerry: *Learning the UNIX operating system*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-060-0)
- [Tun99] TUNG, Brian: *Kerberos: A Network Authentication System*. Fischer-TB.-Vlg., 1999. – (ISBN 0-201-37924-4)
- [Wel94] WELSH, Matt: *Linux Installation and Getting Started*. 2. Aufl. SuSE GmbH, 1994. – (ISBN 3-930419-03-3)
- [WK95] WELSH, Matt; KAUFMAN, Lars: *Running Linux*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-100-3)
- [WK98] WELSH, Matt; KAUFMAN, Lars: *Linux – Wegweiser zur Installation & Konfiguration*. 2. Aufl. O'Reilly & Associates, Inc., 1998. – (ISBN 3-930673-58-4)
- [WM99] WALSH, Norman; MUELLNER, Leonard: *DocBook. The Definitive Guide*. O'Reilly & Associates, Inc., 1999. – ISBN (1-56592-580-7)

Index

Symbole

| | |
|-------------------------|---------------------------------|
| /etc/conf.modules | 143 |
| /etc/hosts | 193 |
| /etc/inittab | 158 |
| /etc/lilo.conf | 94 |
| /etc/modules.conf | 143 |
| /etc/profile | <i>siehe</i> bash, /etc/profile |
| /etc/resolv.conf | 150 |
| xdm | 177 |
| 3D | <i>siehe</i> OpenGL/3D |

A

| | |
|---------------------------------|------|
| ACPI | 131 |
| Adressen | |
| - IP | 206 |
| - MAC | 206 |
| Advanced Powermanagement | 189 |
| AMaViS | 169 |
| Apache | |
| - Squid | 286 |
| APM | 131 |
| Apple | |
| - Netatalk | 262 |
| autoexec.bat | 163 |
| autofs | 172 |
| automatische Installation | 3 |
| AutoYaST2 | 3–56 |

B

| | |
|---------------------------|-----|
| bash | |
| - /etc/profile | 146 |
| Befehl | |
| - ulimit | 149 |
| Benutzer anlegen | |
| - Schwierigkeiten | 223 |
| Bildschirmauflösung | 74 |

| | |
|---------------------|--------------|
| BIND | 227 |
| - BIND8 | 229 |
| - BIND9 | 229 |
| Bootdiskette | 87, 93 |
| Booten | 85, 157, 341 |
| - Ablauf | 86 |
| - Bootmanager | 88 |
| - GRUB | 89–92 |
| - Konzept | 157 |
| - Konzepte | 87 |
| Bootkonzepte | 87 |
| Bootloader | |
| - GRUB | 85, 89 |
| - LILO | 85 |
| Bootmanager | 85 |
| - boot.sys | 88 |
| - LILO | 88 |
| - Windows NT | 88 |
| Bootsektor | 86 |
| Bootvorgang | 86 |
| Busmaus | 61 |

C

| | |
|--|----------|
| Check | 341 |
| Clock-Chip | 64 |
| command not found | 193 |
| Compose ... <i>siehe</i> Tastaturbelegung, Compose | |
| conf.modules | 143 |
| configuration files | |
| - squid.conf | 286 |
| Core-Dateien | 149 |
| Crash | 341 |
| cron | 146, 175 |

D

| | |
|-------------------|-----|
| Dateirechte | 192 |
|-------------------|-----|

| | |
|---------------------------------|----------|
| Dateisysteme | |
| - Intermezzo | 179 |
| DCF77 | 197 |
| Deinstallation | |
| - Linux | 98 |
| - Squid | 277 |
| DENIC | 227 |
| depmod | 142 |
| DHCP | |
| - Clientkonfiguration | 184 |
| - Relay Agent | 177 |
| - Serverkonfiguration | 176 |
| Diskette | |
| - Booten von | 87 |
| DMA | |
| - abschalten | 178 |
| - einschalten | 178 |
| DNS | 209, 227 |
| - Forwarding | 228 |
| - Logging | 231 |
| - Mail Exchanger | 210 |
| - NIC | 209 |
| - Optionen | 230 |
| - Problemanalyse | 228 |
| - Squid und | 277 |
| - Starten | 227 |
| - top level domain | 209 |
| - Zondateien | 233 |
| - Zonen | 231 |
| DNS-Domain | 240 |
| DNS:umgekehrte Adress-Auflösung | 235 |
| Domain | 223 |
| Domain Name Service | 227 |
| DVB | 178 |
| Dynamische IP-Adresse | 194 |
| E | |
| 2fsck | 341 |
| exportieren | 243, 244 |
| F | |
| Farbtiefe | 74 |
| fdisk | |
| - mbr | 99 |
| Firewall | 292 |
| - Aktivieren | 169 |
| - Squid | 283 |
| - SuSEfirewall2 | 292 |
| Firewire | 108 |
| Framebuffer | 173 |
| free | 150 |
| Funkuhr | 197 |

| | |
|--------------------|--------|
| G | |
| GPL | 347 |
| Grafik | |
| - 3D | 168 |
| group | 241 |
| GRUB | 85, 89 |
| H | |
| Hardware | |
| - Drucker | 191 |
| - Hotplug | 178 |
| - Joystick | 180 |
| - Laptop | 111 |
| - Notebook | 111 |
| Hochverfügbarkeit | |
| - ArgoUPS | 171 |
| Horizontalfrequenz | 63 |
| hosts | 219 |
| Hotplug | 103 |
| - Firewire | 108 |
| - Kameras | 106 |
| - Mäuse | 106 |
| - Netzwerkgeräte | 106 |
| - PCI | 106 |
| - PCMCIA | 106 |
| - Speichergeräte | 106 |
| - Tastaturen | 106 |
| - unter Linux | 104 |
| - USB | 105 |
| httpd | 169 |
| I | |
| I18N | 152 |
| Identifier | 75 |
| importieren | 242 |
| Info (info) | 148 |
| init | 158 |
| - Skripte | 161 |
| initrd | 181 |
| inittab | 158 |
| insmod | 142 |
| Installation | |
| - Autoinstallation | 172 |
| - PCMCIA | 121 |
| Intermezzo | 179 |
| IP-Adresse | |
| - dynamisch | 194 |
| IP-Adressen | 206 |
| - IPv6 | 210 |
| - Aufbau | 212 |
| - Netzmasken | 214 |
| - Präfixe | 213 |
| - Netzmasken | 206 |

| | |
|----------------------------------|-----|
| - Netzwerkklassen | 206 |
| - privat | 208 |
| IP-Forwarding | 194 |
| IrDA | 138 |
| - Schnittstelle einstellen | 180 |
| iso-8859 | 78 |
| ispell | 180 |

J

| | |
|------------|-----|
| Java | 180 |
|------------|-----|

K

| | |
|-----------------------------|----------|
| Kernel | 141 |
| - Debugging | 194 |
| - Module | 141 |
| - Sysrq | 194 |
| Kernel Module | |
| - Netzwerkkarten | 216 |
| Konfiguration | |
| - Ändern | 165 |
| - IPv6 | 218 |
| - LILO | 94 |
| - manuell | 19 |
| - Netzzeit | 196 |
| - Squid | 277 |
| - X11 | 60 |
| - YaST2 | 216 |
| Konfigurationsdatei | 167 |
| Konfigurationsdateien | 219 |
| - exports | 245 |
| - host.conf | 220 |
| - HOSTNAME | 224 |
| - ifroute-* | 225 |
| - menu.lst | 89 |
| - named.conf | 229 |
| - Netzwerk | 219 |
| - nscd.conf | 223 |
| - nsswitch.conf | 221 |
| - resolv.conf | 223 |
| - routes | 225 |
| - squid.conf | 277, 283 |
| - squidguard.conf | 289 |
| Konsole | 173, 177 |
| - virtuell | 151 |

L

| | |
|---------------|-----|
| L10N | 152 |
| Löschen | |
| - LILO | 98 |
| - Linux | 98 |
| LAN | 216 |
| Laptop | 111 |
| LILO | 85 |

| | |
|------------------------|----|
| - Deinstallation | 98 |
| - Entfernen | 98 |
| - Grundlagen | 93 |
| - Installation | 98 |
| - Konfiguration | 94 |

Linux

| | |
|--------------------------|--------------------------------|
| - Deinstallieren | 98 |
| - Löschen | 98 |
| Lizenz | 347 |
| Local Area Network | <i>siehe</i> LAN |
| locate | 182 |
| Logdateien | <i>siehe</i> Protokoll-Dateien |
| Login | 177 |
| Logitech | 61 |
| lsmod | 142 |

M

| | |
|-------------------------------|---|
| Mac OS | 262 |
| Mail | |
| - Postfix | 178 |
| Manpages | <i>siehe</i> Manual-Pages |
| Manual-Pages | 148 |
| - Datenbank anlegen | 176 |
| Masquerading | 292 |
| - IP-Forwarding | 194 |
| Maus | 183 |
| - Bus | 61 |
| - HiTablet | 61 |
| - Logitech | 61 |
| - Logitech (MouseMan) | 61 |
| - Microsoft | 61 |
| - MM-Serie | 61 |
| - Mouse Systems | 61 |
| - PS/2 | 61 |
| Maustasten | 62 |
| Maustyp | 61 |
| MBR | 86, 94, <i>siehe</i> Master Boot Record |
| Mesa Software Rendering | 82 |
| Modeline | 76 |
| modprobe | 142 |
| Module | 141 |
| - Umgang | 142 |
| modules.conf | 143 |
| Monitors | 62 |
| mount | 243 |
| mountd | 244 |
| Multi_key .. | <i>siehe</i> Tastaturbelegung, Compose |

N

| | |
|---------------------------------|----------|
| Name Service Switch | 221 |
| Name Service Cache Daemon | 223 |
| Namensdienst | 254 |
| Nameserver | 223, 227 |

| | |
|-------------------------------------|------------------|
| - BIND | 227 |
| Netatalk | 262 |
| NetBIOS | 254 |
| Network File System | <i>siehe</i> NFS |
| Network Information Service | <i>siehe</i> NIS |
| Netzwerk | |
| - Authentifizierung | |
| · Kerberos | 303 |
| - Broadcastadresse | 208 |
| - DHCP Relay | 177 |
| - DNS | 209 |
| - E-Mail | 183 |
| - Grundkonfiguration | 184 |
| - IP-Adressen | 206 |
| - Konfiguration | 216 |
| · IPv6 | 218 |
| - Konfiguration DHCP Server | 176 |
| - Konfigurationsdateien | 219 |
| - Localhost | 208 |
| - Monitorsoftware | 172 |
| - Netzwerkbas Adresse | 208 |
| - Netzwerkkarte konfigurieren | 187 |
| - NFS | 187 |
| - Routing | 206 |
| - Zope | 198 |
| Netzwerke | 201 |
| - Netzmasken | 206 |
| Netzwerkkarte | |
| - Test | 216 |
| NFS | 242 |
| NFS-Client | 242 |
| NFS-Server | 242 |
| nfsd | 244 |
| NIS | 237 |
| - Client | 240 |
| NIS-Domain | 240 |
| NIS-Server | 240 |
| NNTP-Server | 187 |
| Notebook | 111 |
| - ACPI | 131 |
| - APM | 131 |
| - IrDA | 138 |
| - PCMCIA | 188 |
| - Powermanagement | 131 |
| - SCPM | 123 |
| Notebooks | |
| - PCMCIA | 218 |
| NSS | 221 |
| - Datenbanken | 221 |
| O | |
| OpenGL/3D | 80 |
| OpenSSH | <i>siehe</i> SSH |

P

Paket

| | |
|--------------------------|--------------------|
| - 3dpixms | 196 |
| - aaa_base | 147 |
| - apmd | 132 |
| - bind8 | 236 |
| - binutils | 141 |
| - dhcpcd | 248 |
| - exports | 244 |
| - findutils-locate | 176 |
| - gcc | 141 |
| - glibc-devel | 141 |
| - glibc-info | 155 |
| - howtode | 294, 295 |
| - howtoen | 290 |
| - irda | 138 |
| - kernel-source | 141 |
| - libcinfo | 221 |
| - logrotate | 147, 192 |
| - mesa | 84 |
| - mesa3dfx | 84 |
| - mesasoft | 82 |
| - netatalk | 262, 268 |
| - openssh | 298 |
| - pcmcia | 113 |
| - pcmcia-cardinfo | 122 |
| - pcmcia-modules | 123 |
| - pcmcia | 122 |
| - proxy-suite | 294 |
| - radvd | 219 |
| - samba | 255 |
| - squidgrd | 289 |
| - SuSEfirewall2 | 169, 292 |
| - syslinux | 100 |
| - xf86 | 84 |
| - xntp | 196 |
| - yudit | 79 |
| Paketfilter | 292 |
| Partitionstabelle | 86 |
| passwd | 241 |
| PC-Cards | 188 |
| PCI | 106 |
| PCMCIA | 106, 112, 188, 218 |
| - Cardmanager | 113 |
| - Fehlerbehebung | 117 |
| - Hilfsprogramme | 122 |
| - Installation | 121 |
| - IrDA | 138 |
| - ISDN | 115 |
| - Konfiguration | 114 |
| - Modem | 115 |
| - Netzwerkkarten | 115 |

| | |
|-------------------------|-----|
| - SCPM | 116 |
| - SCSI | 116 |
| Permissions | 192 |
| portmap | 244 |
| Ports | |
| - Scannen | 285 |
| Postfix | |
| - Mail-Relaying | 178 |
| Powermanagement | 131 |
| Programmieren | |
| - Core-Dateien | 149 |
| Protokoll-Dateien | 147 |
| Protokolle | |
| - ICMP | 203 |
| - IGMP | 203 |
| - TCP/IP | 202 |
| - UDP | 203 |
| Proxy | |
| - FTP | 192 |
| - HTTP | 192 |
| - Squid | 271 |
| - transparent | 283 |
| - Vorteile | 272 |

R

| | |
|-------------------------|-------------------------------|
| Ramdac | 64 |
| Ramdisk | |
| - Initial Ramdisk | 181 |
| Reboot | 177 |
| Rechte | 192 |
| - Dateirechte | 148 |
| resolv.conf | <i>siehe /etc/resolv.conf</i> |
| rmmmod | 142 |
| Router | |
| - IP-Forwarding | 194 |
| Routing | 206, 225 |
| - Netzmasken | 206 |
| - routes | 225 |
| - statisch | 225 |
| RPC-Mount-Daemon | 244 |
| RPC-NFS-Daemon | 244 |
| RPC-Portmapper | 242, 244 |
| RPM | |
| - Datenbank | 173 |
| Runlevel | 158 |
| - wechseln | 160 |
| Runlevel-Editor | 164 |

S

| | |
|------------------------|----------|
| Samba | 254 |
| - Security Level | 258 |
| SCPM | 116, 123 |
| - Einrichten | 125 |

| | |
|-----------------------------|-----|
| - Profile verwalten | 126 |
| secure shell | 297 |
| Secure Shell Daemon | 193 |
| Security Level | |
| - Samba | 258 |
| Serie | |
| - doc | 221 |
| - n | 219 |
| Share | 255 |
| Shutdown | 177 |
| Sicherheit | 327 |
| - Firewall | 292 |
| - Squid | 272 |
| - SSH | 297 |
| - SSH) | 303 |
| Skript | |
| - init.d | |
| · inetd | 225 |
| · network | 225 |
| · nfsserver | 225 |
| · portmap | 225 |
| · sendmail | 225 |
| · ypbind | 225 |
| · ypserv | 225 |
| - init.d/squid | 276 |
| - modify_resolvconf | 224 |
| SMB | 254 |
| Speicher | |
| - Arbeitsspeicher | 150 |
| Squid | 271 |
| - Access controls | 286 |
| - Apache | 286 |
| - Cache-Größe | 274 |
| - cachemgr.cgi | 286 |
| - Caches | 273 |
| - Calamaris | 289 |
| - CPU | 275 |
| - DNS | 277 |
| - Eigenschaften | 272 |
| - Festplatte | 274 |
| - Firewall | 283 |
| - Konfiguration | 277 |
| - Logdatei | 277 |
| - Objekte speichern | 274 |
| - Proxy-Cache | 272 |
| - RAM | 275 |
| - Rechte | 280 |
| - SARG | 290 |
| - Sicherheit | 272 |
| - SquidGuard | 288 |
| - Starten | 276 |
| - Statistik | 286 |
| - transparenter Proxy | 283 |

| | |
|-----------------------------|----------------------------|
| - Verzeichnisse | 276 |
| - Zugriffskontrolle | 280 |
| SSH | 297–303 |
| - Authentifizierung | 301 |
| - scp | 299 |
| - sftp | 299 |
| - ssh-agent | 302 |
| - sshd | 300 |
| Startup-Skripte | |
| - init.d | 225 |
| SuSE | 145 |
| SuSEconfig | 193 |
| SuSEconfig | 165 |
| SuSEConfig | 165 |
| SuSE Linux Desktop | 145 |
| - Besondere Merkmale | 145 |
| - Tastaturbelegung | 151 |
| switch2mesasoft | 82 |
| switch2nv | 82 |
| Syn Flood Protection | 194 |
| /etc/sysconfig | 165 |
| Syslog-Daemon | |
| - konfigurieren | 194 |
| - syslog-ng | 195 |
| Sysrq | <i>siehe</i> Kernel, Sysrq |
| Systemkonfiguration | 167 |
| Systemzeit | 173 |
| T | |
| Tastatur | |
| - Belegung | 181 |
| - CapsLock | 181 |
| - NumLock | 181 |
| - ScrLock | 181 |
| - Verzögerung | 181 |
| - Wiederholung | 181 |
| Tastaturbelegung | 151 |
| - Compose | 151 |
| TCP/IP | 202 |
| - Dienste | 202 |
| - ICMP | 203 |
| - IGMP | 203 |
| - packets | 203, 205 |
| - Schichtenmodell | 203 |
| - TCP | 202 |
| - UDP | 203 |
| Temporäre Dateien | |
| - Beim Booten löschen | 175 |
| - Löschen | 175 |
| TeX | 195 |
| Texinfo | 148 |
| Textkonsole | 177 |
| Tkinfo (tkinfo) | 148 |

True Type *siehe* X11, True Type

U

| | |
|----------------------------------|------------------|
| UDP | <i>siehe</i> TCP |
| ugidd | 246 |
| ulimit | 149 |
| Umgebungsvariable | |
| - ACPI_BUTTON_LID | 136 |
| - ACPI_BUTTON_POWER | 136 |
| - APMD_AC | 134 |
| - APMD_BATTERY | 134 |
| - APMD_PCMCIA_EJECT_ON_SUSPEND . | 134 |
| - LANG | 182 |
| - LC_* | 182 |
| - POSTFIX_LAPTOP | 138 |
| Unicode | 79 |
| USB | 105 |

V

| | |
|-----------------------------|-----|
| Vernetzung | 201 |
| Vertikalfrequenz | 62 |
| Virtuelle Konsolen | 151 |
| virtueller Bildschirm | 74 |

W

| | |
|---------------------|-----|
| whois | 210 |
| Windowmanager | 195 |
| Windows | |
| - SMB | 254 |
| Windows | 254 |
| Windows NT | |
| - Bootmanager | 88 |

X

| | |
|------------------------|------------------|
| X | <i>siehe</i> X11 |
| X Window System | 57 |
| X-Terminal | 196 |
| X11 | 57 |
| - Displaymanager | 177 |
| - Font | 77 |
| - Grafikkarten | 64 |
| - Konfiguration | 60 |
| - Mäuse | 61 |
| - Monitore | 62 |
| - Tastatur | 62 |
| - X-Server | 64 |
| - mkfontdir | 77 |
| - Optimierung | 70 |
| - Treiber | 75 |
| - TrueType-Font | 77 |
| - ttmkfdir | 77 |
| - Zeichensatz | 77 |

| | |
|----------------------|------------|
| X11R6.4 | 58 |
| xf86config | 60 |
| XF86Config | 60 |
| - Clocks | 74 |
| - Depth | 74 |
| - Device | 72, 74, 75 |
| - Files | 72 |
| - InputDevice | 72 |
| - modeline | 74 |
| - Modeline | 72 |
| - Modes | 72, 74, 76 |
| - Monitor | 72, 74, 76 |
| - Screen | 73 |
| - ServerFlags | 72 |
| - ServerLayout | 73 |
| - Subsection | |
| · Display | 74 |
| - Virtual | 75 |
| XFree86 | 58 |
| - Geschichte | 58 |

| | |
|---------------------|-----|
| XInfo (xinfo) | 148 |
|---------------------|-----|

Y

| | |
|-----------------------------------|------------------|
| YaST2 | |
| - automatische Installation | 3 |
| - AutoYaST2 | 3 |
| - rc.config | 167 |
| - Runlevel-Editor | 164 |
| - Sysconfig-Editor | 167 |
| - YOU | 188 |
| Yellow Pages | <i>siehe</i> NIS |
| YP | |
| - Optionen | 197 |
| yudit | 79 |

Z

| | |
|-----------------------|-----|
| Zeit einstellen | 196 |
| Zeitzone | 173 |
| Zope | 198 |

