SuSE Linux

Office Server

1. Auflage 2002

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

Autoren: Roman Drahtmüller, Michael Hager, Roland Haidl, Jana Jäger, Jordi Jaen Pallares, Karine Nguyen, Edith Parzefall, Peter Reinhart, Marc Rührschneck, Thomas Schraitle, Martin Sommer

Redaktion: Antje Faber, Dennis Geider, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Marc Rührschneck, Thomas Schraitle, Martin Sommer, Rebecca Walter

Layout: Manuela Piotrowski, Thomas Schraitle

Satz: LaTeX

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

Willkommen

Der SuSE Linux Office Server ist ein ideale Werkzeug für kleine Firmennetzwerke, die für den Betrieb ohne eigenen Systemadministrator konzipiert sind. Dieser Server bietet Ihnen für Ihre Clients Internet und Intranet aus einem Guss: Fileserver, Printserver, Internet-Gateway mit Proxy und Firewall.

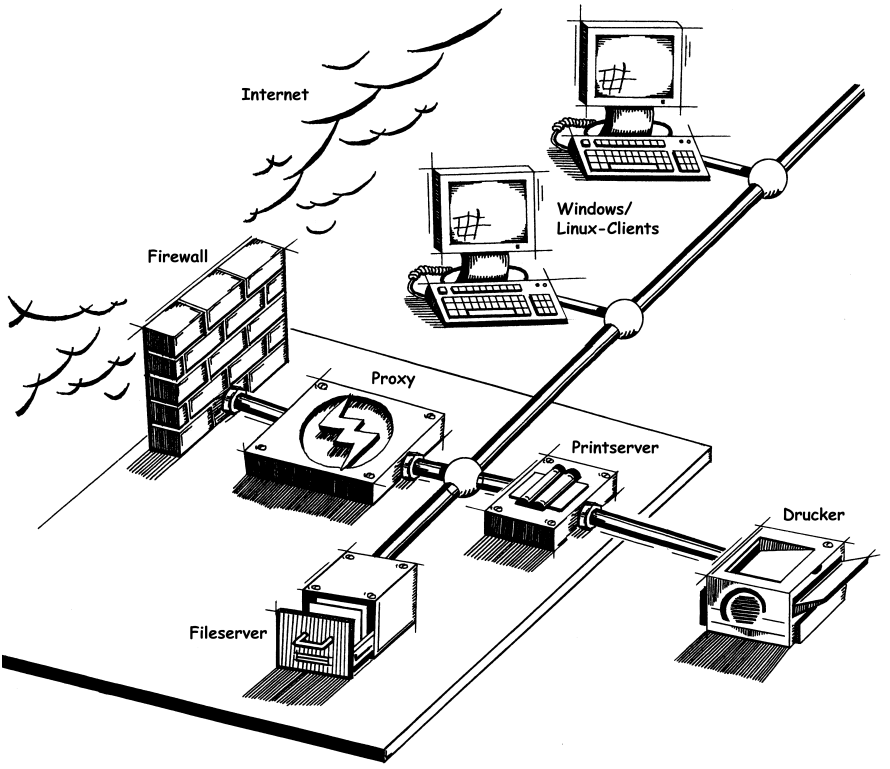
Der SuSE Linux Office Server lässt sich relativ einfach installieren und im laufenden Betrieb unkompliziert betreuen.

Sollten Sie spezielle, über die vorkonfigurierten Einstellungen hinausgehende Anforderungen haben, unterstützt Sie unser professioneller Support.

Der im Vergleich zu anderen Produkten robuste SuSE Linux Office Server verfügt über lange Release-Zyklen. Er kombiniert die erwiesene Stabilität eines Linuxsystems mit permanenter Aktualität: Sie können Online-Updates jederzeit automatisch einspielen. Zudem schont er auch Ihre finanziellen Ressourcen.

SuSE hat den SuSE Linux Office Server konzipiert, um Ihnen zu helfen, im kritischen Bereich Netzwerk Produktivität und Profitabilität Ihres Unternehmens abzusichern, damit Sie sich aufs Wesentliche konzentrieren können.

Ihr SuSE Team


Internet
Windows/
Linux-Clients
Firewall
Proxy
Printserver
Drucker
Fileserver

Inhaltsverzeichnis

Die Installation des SuSE Linux Office Server

Auf den folgenden Seiten wird die Installation des SuSE Linux Office Servers mit YaST2 erklärt.

Systemstart von CD–ROM

Zum Starten der Installation schalten Sie bitte Ihren Rechner ein und legen Sie die erste CD des SuSE Linux Office Server in das Laufwerk ein. Ihr System muss von CD bootbar sein. Ist dies nicht der Fall, müssen Sie möglicherweise die Einstellungen Ihres BIOS' ändern oder, falls SCSI-Systeme verwendet werden, die Boot-Sequenz Ihres SCSI-Controllers. Bitte ziehen Sie für solche Fälle die Dokumentation des Herstellers zu Rate.

Wenn Ihr System nicht von CD booten kann, müssen Sie eine Bootdiskette zum Starten des Installationsvorgangs erstellen. Weitere Informationen darüber finden Sie im Abschnitt *Bootdiskette erstellen* auf Seite 92.

Begrüßungsbildschirm

Ein Bildschirm wie in Abbildung 1.1 zeigt Ihnen, dass Ihr SuSE Linux Office Server startbereit ist. Bei der Standard-Einstellung 'Installation' startet nach einigen Sekunden Wartezeit das graphische Installationsprogramm YaST2 automatisch im SVGA (800x600) Grafikmodus.

Nach Ablauf der Wartezeit wird ein minimales Linux–System in den Hauptspeicher des Rechners geladen. Unter diesem Linux–System läuft der weitere Installationsvorgang ab. Zum Abschluss des Ladevorgangs wird YaST2 gestartet und nach wenigen Sekunden erscheint dessen grafische Oberfläche.

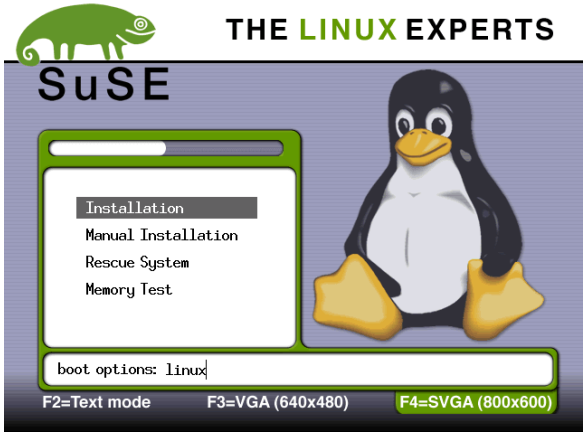


Abbildung 1.1: *Der Startbildschirm von SuSE Linux*

Andere Optionen zur Installation

Wenn Sie vor Ablauf der Wartezeit eine Taste drücken, ist der automatische Start unterbrochen und Sie können in Ruhe andere Optionen wählen. Diese benötigen Sie, wenn es bei der Standard-Einstellung Probleme mit der graphischen Darstellung gibt. Da erst nach einigen Dialogen und expliziter Rückfrage das eigentliche Installieren auf die Festplatte gestartet wird, können Sie bei Problemen jederzeit abbrechen und nach erneutem Booten andere Optionen wählen.

Anderen Grafikmodus für YaST2

Mit den Funktionstasten können Sie den VGA (640x480) Grafikmodus wählen, der mit jeder Grafikkarte funktionieren sollte. Im Notfall steht Ihnen auch der Textmodus zur Verfügung.

Im Text-Modus von YaST2 springen Sie innerhalb eines Bildschirms mit der (Tab) Taste von Menüpunkt zu Menüpunkt und innerhalb eines Menüs erfolgt die Auswahl mit den Tasten (↑) und (↓) und mit der Taste (↵) wechseln Sie zum nächsten Bildschirm.

Andere Installationsoptionen

Mit den Tasten (↑) und (↓) können Sie die anderen Systeme wählen.

- Wenn Sie 'Manual Installation' wählen, haben Sie mehr Eingriffsmöglichkeiten, insbesonders bei der Auswahl der zu installierenden Gerätetreiber. Allerdings werden keine Treiber automatisch geladen. Dies ist i. d. R. nur für Experten sinnvoll.
- Unter 'Rettungssystem' steht ein Rettungssystem zur Verfügung, mit dem Sie Ihren Rechner sicher starten können, falls Probleme auf Ihren System auftreten. Mehr Informationen zum Rettungssystem erhalten sie im Kapitel A auf Seite 99.
- Mit 'Memory Test' kann ein sehr lang andauernder Speichertest gestartet werden, der Speicherfehler wesentlich sicherer finden kann, als der BIOS-Speichertest beim Booten.

Wenn Sie nun (Enter) drücken, dann wird das gewählte System gestartet.

YaST2 übernimmt die Arbeit

Jetzt beginnt die eigentliche Installation von SuSE Linux mit dem Installationsprogramm YaST2. Abbildung 1.2 auf der nächsten Seite zeigt die erste Bildschirmansicht. In dieser Phase wird die vorhandene Hardware Ihres Rechners überprüft und für die Installation vorbereitet. Eine Leiste in der Mitte des Bildschirms zeigt Ihnen den Fortschritt an.

Alle Bildschirmansichten von YaST2 folgen einem einheitlichen Schema. Sie enthalten im linken Bildteil einen Hilfetext, der Sie zum aktuellen Installationsabschnitt informiert. Alle Eingabefelder, Auswahllisten und Buttons der YaST2–Bildschirme können Sie sowohl mit der Maus als auch mit der Tastatur steuern. (Tab) verschiebt den Fokus und aktiviert ein Knopf (dicke Umrandung), Feld usw., (↵) ist äquivalent einem Mausklick. In manchen Elementen können Sie auch die Cursortasten verwenden. Diese Tastenkombinationen sind besonders hilfreich, wenn Ihre Maus nicht automatisch erkannt wurde. Nach dem Bildschirm zur Sprachauswahl erhalten Sie die Möglichkeit, Ihre Maus manuell zu konfigurieren.

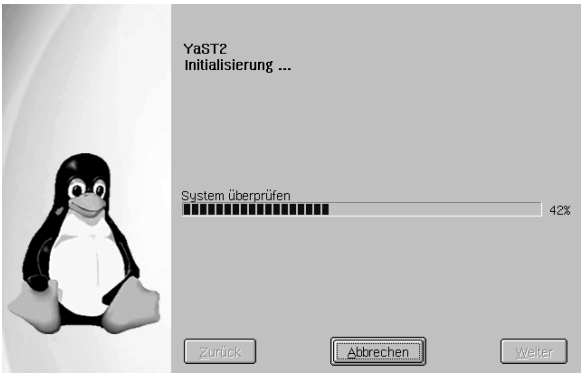


Abbildung 1.2: *Die Hardwareanalyse*

Sprachauswahl

SuSE Linux und YaST2 stellen sich auf die von Ihnen gewünschte Sprache ein. Bei der deutschen Version von SuSE Linux ist Deutsch voreingestellt. Andere Sprachen können individuell ausgewählt werden.

Falls die Maus noch nicht funktioniert, drücken Sie bitte so oft die (Tab)–Taste, bis der Button 'Weiter' voraktiviert ist, und anschließend die (↵)–Taste.

Mauszeiger

Sollte YaST2 die Maus nicht automatisch erkennen können, erscheint die in Abbildung 1.3 auf der nächsten Seite gezeigte Bildschirmmaske. Verwenden Sie zur Auswahl des Maustyps die Tasten (↑) und (↓). Falls Sie eine Dokumentation zu Ihrer Maus besitzen, finden Sie dort eine Beschreibung des Maustyps. Die ersten

drei Maustypen in der Liste sind die gängigsten, die Sie deshalb zuerst ausprobieren sollten, wenn Sie den Maustyp nicht kennen. Insbesondere serielle Mäuse anderer Hersteller sind normalerweise kompatibel zur Microsoft Maus.

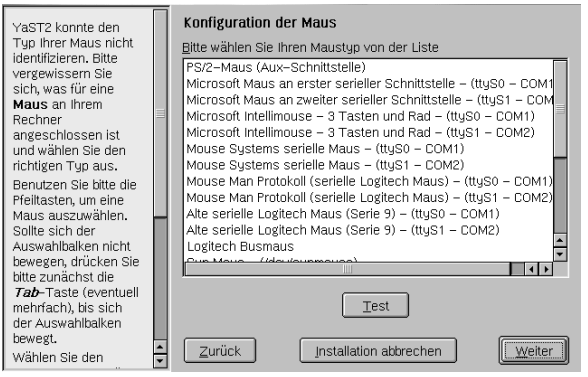


Abbildung 1.3: *Auswählen des Maustyps*

Bestätigen Sie den gewünschten Maustyp entweder durch Drücken der Tastenkombination Alt + T oder von Tab und anschließender Bestätigung mit ↵.

Testen Sie, ob Ihre Maus funktioniert. Falls sich der Zeiger nicht bewegt, wählen Sie einen anderen Maustyp, und wiederholen Sie den Versuch.

Tastatur und Uhrzeit

Im darauf folgenden Schritt (siehe Abb. 1.4 auf der nächsten Seite) erfolgt die Auswahl des Tastaturlayouts und der Zeitzone. Im Feld 'Rechneruhr eingestellt auf' können Sie zwischen `Lokalzeit` und `GMT` wählen. Ihre Auswahl hängt von der Einstellung der Uhr im BIOS Ihres Rechners ab. Sollte diese auf `GMT` stehen, übernimmt SuSE Linux automatisch die Umstellung von Sommer– auf Winterzeit und umgekehrt.

Im nächsten Schritt wählen Sie das gewünschte Tastaturlayout aus. In der Regel entspricht es der gewählten Sprache. In der anderen Spalte wählen Sie die richtige Zeitzone. Um die Tastaturbelegung zu prüfen aktivieren Sie das Testfeld und drücken Sie im Testfeld Y und Z und Umlaute wie Ä oder ß und Sonderzeichen wie @ und |.

Partition auswählen

Nun wählen Sie die Partition. Sie haben die folgenden Möglichkeiten, Ihre Festplatte zu formatieren:

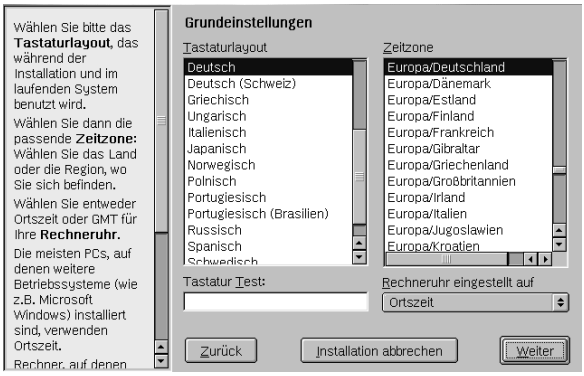


Abbildung 1.4: *Auswählen des Tastaturlayouts und der Zeitzone.*

- Sie überlassen YaST2 die Partitionierung:
  Es empfiehlt sich, den kompletten Festplattenplatz für den Server vorzusehen Im Normalfall wird der SuSE Linux Office Server das einzige System auf dem Rechner sein und auf einer einzigen Festplatte installiert werden. In diesem Fall wählen Sie am einfachsten die Festplatte und dann 'Gesamte Festplatte'. Dann wird YaST2 eine sinnvolle Partitionierung anlegen wobei alle evtl. noch vorhandenen Daten auf der Festplatte verloren gehen, so dass der gesamte Plattenplatz dem SuSE Linux Office Server zur Verfügung steht. Die Abschnitte über Partitionen anlegen, LVM und Kryptofilesystem brauchen Sie dann nicht zu lesen.

- Sie möchten die Partitionen individuell anlegen:
  In diesem Fall lesen Sie weiter in Abschnitt *Partitionen wählen* auf der nächsten Seite.

- Sie möchten den SuSE Linux Office Server mit LVM betreiben:
  Lesen Sie im Abschnitt *Logical Volume Manager (LVM)* auf Seite 9 weiter.

- Sie möchten ein Kryptofilesystem einrichten:
  Beachten Sie die Hinweise im Abschnitt *Kryptofilesystem einrichten* auf Seite 13.

Die Standardpartitionierung umfasst 3 primäre Partitionen: eine Boot-Partition für den Linux-Kernel (ca. `20 MB`) im Startzylinder der Festplatte, eine Swap-Partition, zugeschnitten auf den Umfang Ihres RAM und eine / (oder Root) Partition für alle System- und Benutzerdateien, die den restlichen Festplattenspeicher belegen.

Hinweis

Es werden keine Änderungen an Ihrer Festplatte vorgenommen, bis Sie nicht alle Installationseinstellungen konfiguriert und in einem speziellen Dialogfenster mit 'Ja' bestätigt haben. Sie können während der Installation mit YaST2 jederzeit zu vorherigen Konfigurationsfenstern zurückgehen und Einstellungen ändern mit 'Zurück'.

Hinweis

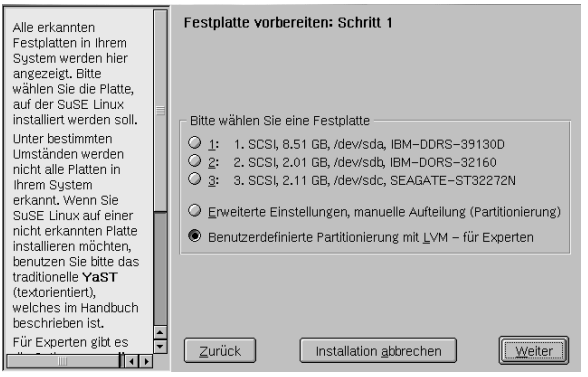


Abbildung 1.5: *Wahl der Festplatte für die Installation von SuSE Linux*

Partitionen wählen

Nachdem Sie die Festplatte gewählt haben, auf der SuSE Linux installiert werden soll, wird YaST2 alle auf der gewählten Festplatte befindlichen Partitionen anzeigen (siehe Abb. 1.6 auf der nächsten Seite). Sie entscheiden, ob Sie für SuSE Linux Office Server die 'Gesamte Festplatte verwenden' oder Partitionen löschen möchten, um Platz für das SuSE Linux System zu schaffen. Folgen Sie den Hilfetexten von YaST2, um mehr über die Wahl der Partitionen zu erfahren.

Möchten Sie weiteres über die Partionierung erfahren, lesen Sie im nächsten Abschnitt weiter (siehe *Anmerkungen zur erweiterten Partitionierung* auf der nächsten Seite), andernfalls im Abschnitt *Bootmanager für den Systemstart* auf Seite 13.

Achtung

Alle Daten auf der für die Installation gewählten Partition gehen verloren. Genauso verlieren Sie alle Festplattendaten, wenn Sie den Menüpunkt 'Gesamte Festplatte verwenden' wählen!

Achtung

Während des Installationsvorgangs überprüft YaST2, ob sich genug Platz auf der Festplatte für die Installation von SuSE Linux befindet. Ist dies nicht der Fall,

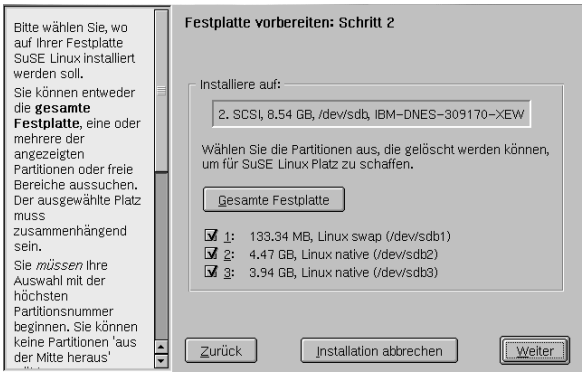


Abbildung 1.6: *Wahl der Partitionen für die Installation von SuSE Linux*

werden Sie aufgefordert, eine andere Auswahl zu treffen. Die Installation von SuSE Linux Office Server benötigt etwa 800 MB Festplattenplatz.

Anmerkungen zur erweiterten Partitionierung

Bitte wählen Sie diese Option nur, wenn Sie mit Begriffen wie Partition, Mountpunkt oder Dateisystem vertraut sind. Die Standardpartitionierung unter YaST2 wurde bereits für Ihre Systemanforderungen konfiguriert. Gehen Sie jedoch trotzdem besonders sorgfältig bei der Partitionierung Ihres Systems vor.

In dieser Maske können Sie Partitionen in Ihrem System 'Anlegen', 'Bearbeiten' oder 'Löschen' (siehe Abb. 1.7). Ein Vorschlag zum Partionieren Ihrer Festplatte wäre z. B.:

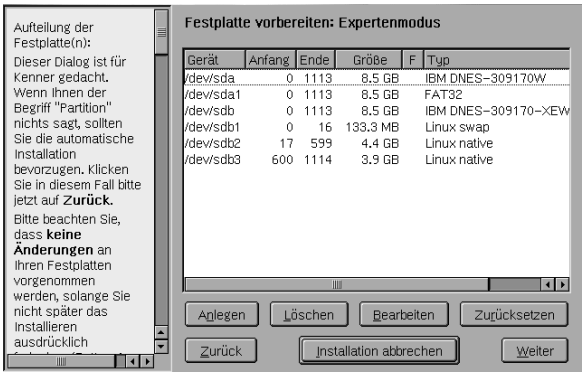


Abbildung 1.7: *Auswählen der Partitionen*

`/`	2 GByte
`swap`	das 2-fache der RAM-Größe, max. 1 GByte
`/home`	Verzeichnisse der Benutzer; besitzen unterhalb von `/home` ihr eigenes Verzeichnis. Pro Benutzer ca. 2 GByte.
`/shared`	Allgemeines Verzeichnis, ist für alle zugänglich.

Falls Sie das `/home` Verzeichnis später vergrößern möchten, können Sie dies mit LVM dynamisch tun (siehe Abschnitt *Logical Volume Manager (LVM)* auf dieser Seite).

Sie müssen die Parameter für die einzelnen Partitionen in Ihrem System manuell festlegen:

- Legen Sie die Größe jeder einzelnen Partition fest. Geben Sie sie entweder direkt in `MBytes` oder in Festplattenzylindern an.
- Entscheiden Sie sich für ein Format. Sie können zwischen `ext2` oder `reiserFS` wählen. Entscheiden Sie sich für `reiserFS`, wenn Sie die Vorteile eines Journaling Filesystems nutzen wollen.
- Bestimmen Sie einen Mountpunkt für die einzelnen Partitionen. Der Mountpunkt ist das Verzeichnis in Ihrem Dateisystem, in dem Sie die Partition mounten (oder „einhängen“). Dies ist möglicherweise dann nützlich, wenn Sie die Verzeichnisse `/home`, `/opt` usw. in getrennten Partitionen unterbringen möchten.

Hinweis

SuSE Linux Office Server verwendet ein gemeinsames Verzeichnis zum Exportieren gemeinsamer Daten für Samba, NFS und netatalk nach allen Netzwerk-Clients im System. Falls Sie eine separate Partition für dieses gemeinsame Verzeichnis verwenden wollen, geben Sie bitte `/shared` als Mountpunkt an.

Hinweis

Logical Volume Manager (LVM)

Der Logical Volume Manager (LVM) verfügt eine logische Ebene zwischen dem physikalischen Medium, d. h. Ihrer Festplatte, und dem Dateisystem, das Ihre Daten enthält.

Das Prinzip besteht darin, physikalische Platten in eine Art Speichereinheiten aufzuteilen. Speichereinheiten von verschiedenen Laufwerken können zu einem Logical Volume zusammengefasst werden, von wo sie Partitionen zugewiesen werden können. Zusätzlich können je nach Speicherbedarf Einheiten zu Partitionen hinzugefügt oder davon entfernt werden.

LVM ermöglicht während des Rechnerbetriebs die Größenänderung von Partitionen. Angenommen, Sie haben nicht mehr genügend Speicher auf einer Ihrer

Festplattenpartitionen, z. B. auf `/home`. Mit LVM können Sie dieses Problem einfach lösen, indem Sie der Partition neue Speichereinheiten zuweisen, entweder von der gleichen Platte oder von anderen Platten auf Ihrem System.

Weitere Informationen über die Konfiguration des „Logical Volume Manager“ (LVM) finden Sie im offiziellen LVM-Howto unter:

`http://www.suse.de/en/support/oracle/docs/lvm_whitepaper.pdf`

oder unter

`/usr/share/doc/howto/en/html/LVM-HOWTO.html`.

Konfiguration von LVM mit YaST2

Unter YaST2 können Sie die Konfiguration von LVM starten, indem Sie während der Startphase der Festplattenvorbereitung, siehe Abbildung 1.5 auf Seite 7, ‘Benutzerdefinierte Partitionierung mit LVM’ wählen.

LVM – Partitionierung

Zuerst erscheint folgender Dialog (siehe Abb. 1.8). Hier können Sie die Partitionierung Ihrer Festplatte ändern. Legen Sie je nach Bedarf Partitionen oder Volumes an.

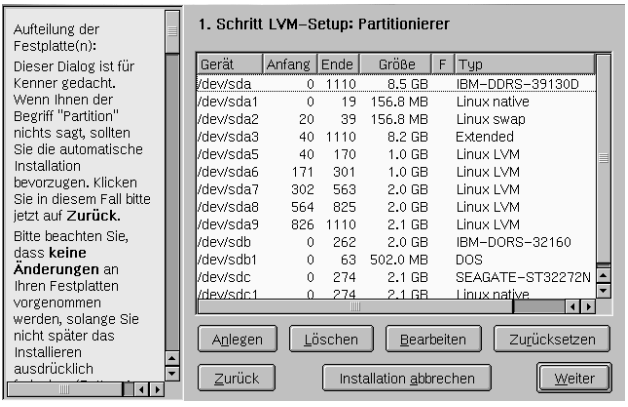


Abbildung 1.8: *YaST2: LVM-Partitionierer*

Nach einem Klick auf ‘Anlegen’ können Sie in der folgenden Maske den LVM-Typ wählen, indem Sie auf ‘Nicht formatieren’ klicken und dann als ‘Dateisystem-ID’ `0x8e Linux LVM` wählen. Die LVM-„Partitionen“ müssen zu diesem Zeitpunkt nicht partitioniert werden. Ignorieren Sie also die Warnung, die beim Klick auf ‘Weiter’ erscheint. Beachten Sie auch, dass Sie noch keinen Mountpunkt angeben müssen. Dies wird später geschehen.

Hinweis

Unter YaST2 muss sich mindestens das **Root**- (oder **/**-)Dateisystem auf einer normalen Partition befinden, z. B. auf einer `ext2` oder `reiserFS`-Partition.

Hinweis

LVM – Einrichten von Physical Volumes

Dieser Dialog behandelt die LVM Volume-Gruppen (Abkz.: „VG“). Falls noch keine Volume-Gruppe in Ihrem System vorhanden ist, werden Sie durch ein Popup-Fenster aufgefordert, eine anzulegen. „System“ bezeichnet den vorgeschlagenen Namen für die Volume-Gruppe. Die „Physical Extent Size“ (oft abgekürzt mit PE-Größe) gibt die maximale Größe eines Physical und Logical Volumes in dieser Volume-Gruppe an. Dieser Wert lieg normalerweise bei 4 Megabytes. Somit ergibt sich eine maximale Größe von 256 Gigabytes für ein Physical und Logical Volume. Sie sollten also nur die Physical Extent Size (z. B. auf 8, 16 oder 32 Megabytes) erhöhen, wenn Sie Logical Volumes mit mehr als 256 Gigabytes benötigen.

Im folgenden Dialog werden alle "Linux LVM"- oder "Linux-eigenen" Partitionstypen aufgelistet. Falls eine Partition bereits einer Volume-Gruppe zugewiesen wurde, erscheint der Name der Volume-Gruppe. Nicht zugewiesene Partitionen tragen das Label "–".

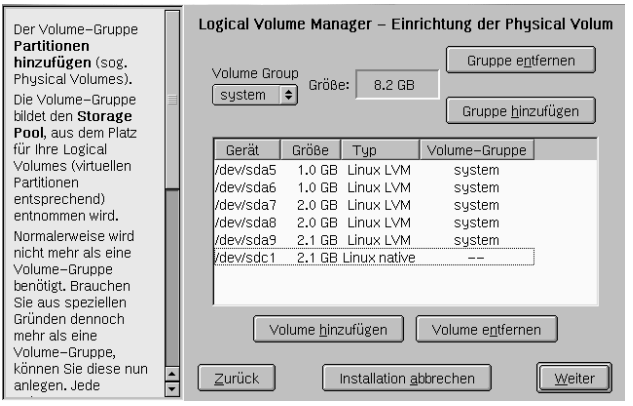


Abbildung 1.9: *YaST2: Überblick über die Partitionen*

Markieren Sie die zu bearbeitende Volume-Gruppe in der Auswahlbox links oben. Mit den Buttons rechts oben, können Sie Volume-Gruppen ‘Hinzufügen’ oder ‘Entfernen’. Jedoch können Sie nur Volume-Gruppen entfernen, denen keine Partitionen zugeordnet sind. Eine Partition, die einer Volume-Gruppe zugeordnet ist, wird auch als Physical Volume (Abkz.: PV) bezeichnet.

Um eine bisher nicht zugewiesene Partition zur gewünschten Volume-Gruppe hinzuzufügen, müssen Sie zunächst die Partition auswählen und dann auf den Button 'Volume hinzufügen' unterhalb der Auswahlliste klicken. Sie können den Dialog erst verlassen, wenn Sie jeder Volume-Gruppe mindestens ein Physical Volume zugewiesen haben.

Logical Volumes

In diesem Dialog können Sie Logical Volumes hinzufügen, bearbeiten oder löschen (siehe Abb. 1.10). Klicken Sie auf 'Hinzufügen', wenn Sie ein Logical Volume anlegen möchten. Geben Sie für das Volume eine Größe, ein Format (z. B. `reiserFS` oder `ext2`) und einen Mountpunkt in Ihrem Dateisystem an.

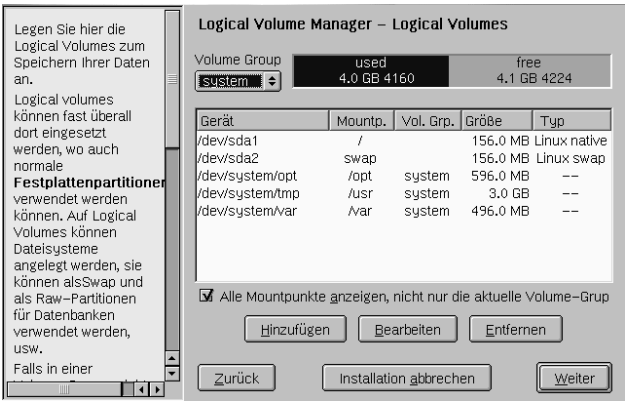


Abbildung 1.10: *YaST2: Umgang mit Logical Volumes*

Wenn Sie mehrere Volume-Gruppen angelegt haben, können Sie zwischen diesen in der Auswahlliste oben links hin- und herschalten.

Achtung

Bitte denken Sie daran, vor dem Einsatz von LVM bzw. vor der Neukonfiguration von Volumes eine Datensicherung vorzunehmen, d. h. Sie sollten nie ohne Backup arbeiten!

Achtung

Kryptofilesystem einrichten

Während der Partitionierung in YaST2 haben Sie die Möglichkeit, eine Partition komplett zu verschlüsseln. Ein Kryptodateisystem macht also nur dann Sinn, wenn der Rechner ausgeschaltet ist (wie z. B. dies bei Laptops der Fall ist).

Beachten Sie bitte: Während die Partition(en) eingebunden („gemountet“) ist/sind, sind die Daten unverschlüsselt und für jeden sichtbar! Wird die Einbindung jedoch gelöst, sind die Daten sicher geschützt. Selbst bei Diebstahl der Festplatte bzw. des Laptops besteht ohne Passwort keine Möglichkeit, die Daten zu entschlüsseln.

Um eine Partition zu verschlüsseln, geben Sie im Dialogfenster zum Anlegen von Partitionen Start- und Endzylinder bzw. als Ende die gewünschte Größe der Partition wie unter dem Feld vorgeschlagen. Den Mountpunkt, auf dem Sie Ihre verschlüsselte Partition erreichen wollen, können Sie frei wählen. Klicken Sie nun rechts den Punkt ‘Dateisystem verschlüsseln’ an und geben Sie ‘OK’.

Im nächsten Dialogfenster werden Sie nun nach dem Passwort gefragt, das Sie zur Bestätigung zweimal eingeben müssen. Es muss mindestens 5 Zeichen lang sein und sollte eine Kombination aus großen und kleinen Buchstaben sowie Zahlen darstellen.

Achtung

Seien Sie hier besonders vorsichtig bei der Passworteingabe. Dieses Passwort ist später nicht mehr veränderbar. Wenn Sie es vergessen, sind Ihre Daten unwiederbringlich verloren!!

Achtung

Ist dies geschehen, erscheint die neue Partition jetzt in der Partitionierungstabelle, wobei in der Spalte ‘F’ nun der Eintrag ‘CF’ für „Kryptofilesystem“ erscheint.

Bootmanager für den Systemstart

Nachdem Sie die Festplatte nach Ihren Wünschen eingerichtet haben, wird in diesem Schritt der so genannte „Bootmanager“ konfiguriert. Damit Linux später überhaupt starten kann, ist ein Bootmechanismus nötig, welcher durch das Programm LILO (engl. *LInux LOader*) vorgenommen wird. Hierzu muss festgelegt werden, an welcher Stelle im System der Bootmanager installiert wird bzw. ob ein anderes Bootkonzept verwendet werden soll.

Im Normalfall ist der SuSE Linux Office Server das einzige System auf Ihrem Rechner; in diesem Fall installieren Sie am einfachsten LILO im Startsektor (MBR) der ersten Festplatte. Möchten Sie LILO auf einem anderen Medium installieren, müssen Sie ‘Andere Konfiguration’ wählen; dann zeigt Ihnen YaST2 die erweiterten Möglichkeiten an (siehe Abb. 1.11 auf der nächsten Seite). Sie brauchen dies allerdings nur, wenn Sie genau wissen was Sie tun.

YaST2 bietet Ihnen vier Möglichkeiten zur Auswahl an:

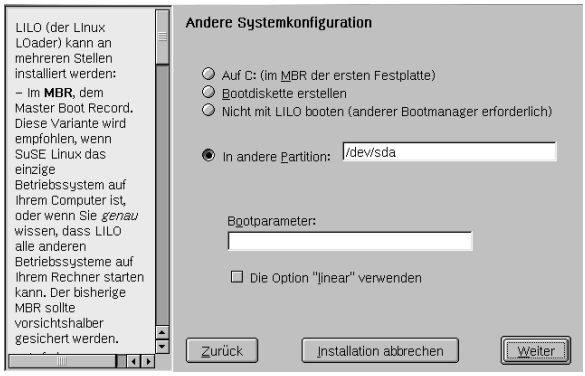


Abbildung 1.11: *LILO Andere Startkonfiguration*

'Auf C: (im MBR der ersten Festplatte)' – Wenn SuSE Linux als alleiniges Betriebssystem installiert werden soll, gehört LILO auf jeden Fall in den MBR (engl. *Master Boot Record*).

LILO im MBR kann auch als Bootmanager für mehrere Betriebssysteme fungieren. Wählen Sie diese Möglichkeit aber nur dann, wenn Sie sich *sicher* sind, dass Ihre bereits installierten Systeme von LILO gebootet werden können – in der Regel ist dies bei Windows 9x/ME der Fall. Sind Sie im Zweifel, entscheiden Sie sich für die Möglichkeit 'Bootdiskette erstellen'.

'Bootdiskette erstellen' – Falls Ihr Rechner mit mehreren Betriebssystemen laufen soll, können Sie für SuSE Linux eine Bootdiskette zu erstellen. So bleibt der bisherige Bootmechanismus völlig unverändert und SuSE Linux kann jederzeit von dieser Diskette gestartet werden.

'LILO nicht installieren (anderer Bootmanager)' – Hiermit können Sie weiterhin Ihren eigenen Bootmanager benutzen. Am MBR (Master Boot Record) wird nichts geändert; LILO wird in der Partition `/boot` eingerichtet. Allerdings müssen Sie in diesem Fall *selbstständig* den vorhandenen Bootmanager neu konfigurieren.

'In andere Partition' – Wählen Sie diese Möglichkeit, wenn Sie eine abweichende Partition angeben wollen oder müssen; vgl. den vorangegangen Punkt.

Die verbleibenden Felder werden nur in ganz bestimmte Fällen benötigt, im Zweifelsfall verwenden Sie bitte die YaST2 Onlinehilfe.

Passwort für den Systemadministrator

Der Benutzer `root` ist der Name für den „Superuser“, den Systemverwalter. Er kann das System verändern, Programme einspielen, Benutzer anlegen sowie

neue Hardware hinzufügen und einrichten. Wenn jemand sein Passwort vergessen hat oder Programme nicht mehr laufen, hat der Administrator die Möglichkeit zu helfen.

Das Passwort muss zur Überprüfung zweimal eingegeben werden (siehe Abb. 1.12). Merken Sie sich das Passwort für den Benutzernamen root *besonders gut*.

Abbildung 1.12: *Passwort für den Benutzer root angeben*

Achtung

Sollten Sie das root-Passwort einmal vergessen, können Sie Ihr System nur mit erheblichem Aufwand wiederherstellen. Bewahren Sie das Passwort nicht an Stellen auf, die Dritten zugänglich sind!

Aus Gründen der Systemsicherheit empfehlen wir, sich *nicht* als Root anzumelden. Benutzen Sie hierzu den Administrator-Account. (siehe Abschnitt *Administrator-Account anlegen* auf dieser Seite).

Achtung

Administrator-Account anlegen

Nachdem Sie das Passwort für Root vergeben haben, müssen Sie in diesem Schritt Ihren Administrator-Account erstellen. Mit diesem erledigen Sie Ihre täglichen Arbeiten. Geben Sie sich dazu einen einprägsamen Loginnamen, der z. B. Ihr Vor- oder Nachname sein könnte. Verwenden Sie jedoch keine Umlaute oder Leerzeichen. Im Anschluss daran bestätigen Sie zweimal Ihr Passwort.

Verwenden Sie für Ihr Passwort eine Kombination aus kleinen und großen Buchstaben sowie Ziffern. Benutzen Sie diesen Account um sich später am System anzumelden.

Der Administrator-Account enthält im Unterschied zu einem normalen Benutzerkonto verschiedenartige Anpassungen, um die Administrierbarkeit des SuSE Linux Office Servers zu vereinfachen.

Jetzt geht's los . . .

Im folgenden Dialog (siehe Abb. 1.13) werden die von Ihnen vorgenommenen Einstellungen nochmals aufgeführt. Sie können hier auch die 'Installation abbrechen'. SuSE Linux wird dann beendet, Ihr System bleibt unverändert. Änderungen können Sie vornehmen, indem Sie so oft auf 'Zurück' klicken bis Sie wieder zu dem Dialog, der geändert werden soll, gelangen. Wenn Sie jedoch auf 'Weiter' klicken, folgt eine Sicherheitsabfrage. Antworten Sie mit 'Ja – installieren', beginnt die Installation. Um die Installationseinstellungen für einen späteren Abruf zu sichern, klicken Sie auf 'Einstellungen auf Diskette speichern'.

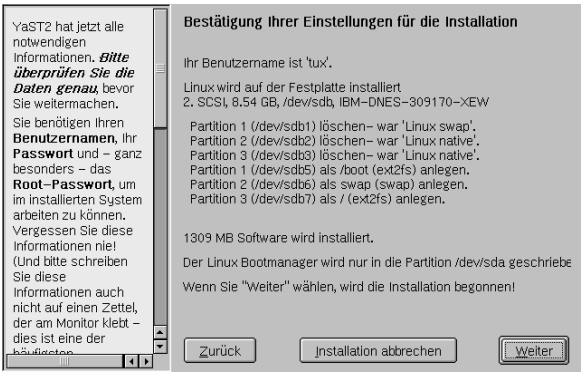


Abbildung 1.13: *Auflistung der vorgenommenen Einstellungen*

Achtung

Alle Daten auf den Partitionen, die Sie für SuSE Linux gewählt haben, werden jetzt unwiderruflich gelöscht. Haben Sie die gesamte Festplatte gewählt, werden auch alle darauf befindlichen Betriebssysteme gelöscht!

Achtung

Vorbereiten der Festplatte

YaST2 beginnt mit der Arbeit, legt die gewählten Partitionen an und formatiert sie. Je nach Systemausstattung kann das einige Zeit in Anspruch nehmen.

Installation der Software-Pakete

Nachdem die Festplatte vorbereitet wurde, werden die Software-Pakete des Linux–Systems von CD kopiert und installiert. Auf dem Bildschirm wird der Fortschritt

der anfallenden Arbeiten angezeigt (siehe Abb. 1.14). Je nach Systemausstattung kann dies einige Zeit in Anspruch nehmen.

Abbildung 1.14: *Installation der Pakete*

Zum Abschluss der Installation der Software-Pakete wird LILO installiert und danach wird ein Linux–Basissystem gestartet. Auf dem Bildschirm erscheinen dabei wieder zahlreiche Meldungen.

Hinweis

Je nach Einstellung, die Sie für die Installation von LILO gewählt haben, können Sie aufgefordert werden, eine Diskette einzulegen, um die Bootdiskette zu erstellen. Beachten Sie bitte, dass dabei alle auf dem Datenträger befindlichen Daten gelöscht werden.

Hinweis

Bildschirm–Einstellungen

Falls der angeschlossene Monitor nicht automatisch erkannt wurde, können Sie das Modell aus der angezeigten Liste auswählen, vgl. Abbildung 1.15 auf der nächsten Seite.

Einige technische Daten des ausgewählten Modells, horizontale (HSync) und vertikale (VSync) Ablenkfrequenz, werden im unteren Teil des Bildschirms eingeblendet. Falls das gewünschte Modell nicht in der Liste verfügbar ist, können Sie die Daten manuell in die Eingabefelder eingeben oder vordefinierte Einstellungen (Vesa–Modi) wählen. Bitte entnehmen Sie die entsprechenden Werte dem Handbuch zu Ihrem Monitor.

Achtung

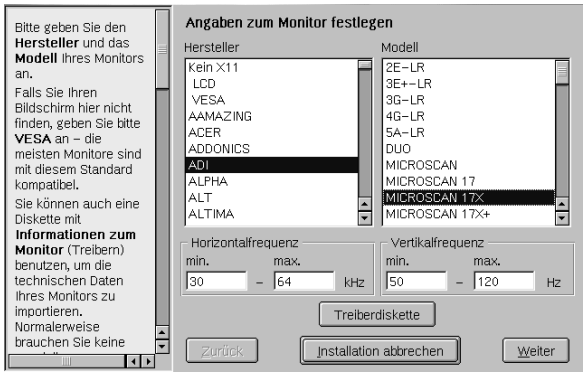


Abbildung 1.15: *Auswählen des Monitor Modells*

Wenn Sie zu hohe Werte (insbesondere bei der Horizontalfrequenz) eintragen, kann Ihr Monitor beschädigt werden (gute Monitore schalten bei zu hohen Werten automatisch ab).

Achtung

Es empfielt sich, bei der Vertikalfrequenz keine zu hohen Werte zuzulassen, auch wenn dies der Monitor ermöglicht, denn ab 90 Hz ist das Bild sicher flimmerfrei aber bei Vertikalfrequenzen am Grenzbereich des Monitors wird das Bild unscharf. Alternativ können Sie auch eine Treiberdiskette verwenden. Dazu klicken Sie auf 'Treiberdiskette'. Legen Sie die Diskette in das Laufwerk ein und bestätigen Sie mit 'OK'. Falls keine Datei gefunden werden konnte oder die Diskette nicht lesbar ist, erhalten Sie einen entsprechenden Hinweis. Bei erfolgreichem Einlesen erscheinen die Monitordaten dann in der Auswahlliste.

In der folgenden Bildschirmansicht (siehe Abb. 1.16 auf der nächsten Seite) können Sie festlegen, ob SuSE Linux zukünftig im 'Textmodus' oder mit einer 'Graphischen Oberfläche' betrieben werden soll. Im Falle des SuSE Linux Office Servers wird der Betrieb von einer grafischen Oberfläche aus Gründen der Benutzerfreundlichkeit empfohlen.

Wenn Sie auf 'Ändern' klicken, haben Sie die Möglichkeit, Einstellungen zur grafischen Oberfläche vorzunehmen. (siehe Abb. 1.17 auf der nächsten Seite).

Hinweis

Falls „3D acceleration“ angezeigt wird, klicken Sie bitte unbedingt auf 'Ändern' und schalten diese ab, da diese zu Problemen führen kann und auf einem Server nicht benötigt wird.

Hinweis

Sie können die Bildschirmauflösung und Farbtiefe für den Grafikmodus einstellen. Auch die Bildwiederholfrequenz kann festgelegt werden. Durch einen Klick

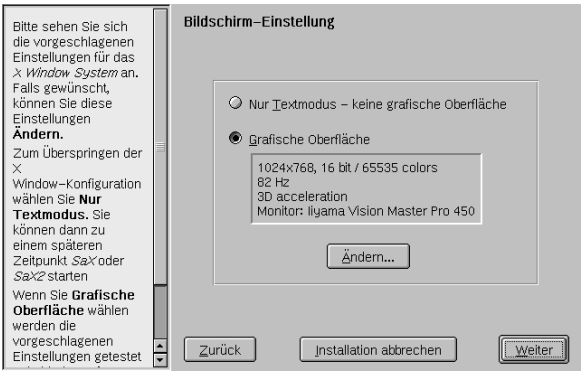


Abbildung 1.16: *Einstellungen zum Bildschirm*

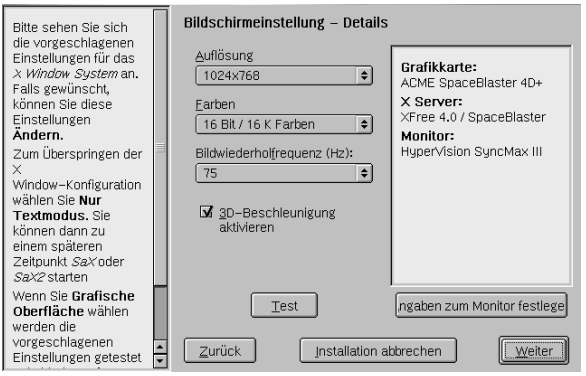


Abbildung 1.17: *Einstellungen zur grafischen Oberfläche ändern*

auf 'Test' wird die gewählte Auflösung getestet. Das Installationsprogramm informiert Sie, dass der Bildschirm nun umgeschaltet wird. Falls Sie kein ruhiges Bild erhalten, brechen Sie den Test bitte umgehend durch Drücken von der Taste (ESC) ab.

Netzwerkkarte

Zur Netzwerkkonfiguration muss man als ersten Schritt die Netzwerkkarte des Servers konfigurieren, die an das *interne Netzwerk* angeschlossen wird. YaST2 erkennt automatisch alle Netzwerkkarten in Ihrem System und zeigt Ihnen eine Liste an (siehe Abb. 1.18 auf der nächsten Seite).

Die Karte, die Sie jetzt auswählen, verbindet Sie mit Ihrem lokalen Netz. Alle Serverdienste werden nur über diesen Anschluss (=eth0, ist die erste Netzwerkkarte

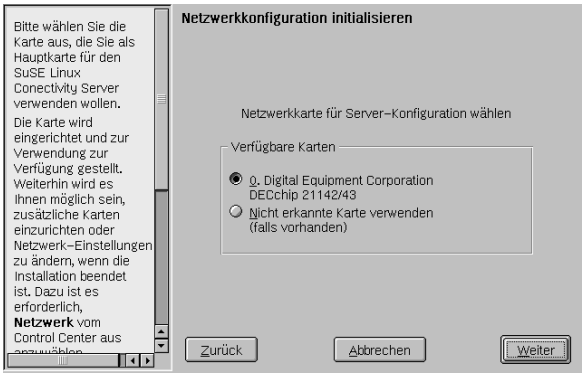


Abbildung 1.18: *Netzwerkkarte wählen*

unter Linux) bereitgestellt.

Tipp

Falls Sie mehr als eine Netzwerkkarte haben, befindet sich diese erste Netzwerkkarte normalerweise im oberen Slot des Rechners, bei Desktop-Computern i. d. R. links außen.

Tipp

Wurde die Netzwerkkarte nicht automatisch durch YaST2 erkannt, können Sie sie immer noch manuell konfigurieren, indem Sie auf 'Nicht erkannte Karte verwenden, falls vorhanden' klicken. YaST2 erlaubt Ihnen die manuelle Eingabe des Treibernamens (oder Kernel-Moduls), der für Ihre Netzwerkkarte benötigt wird. Durch Klicken auf 'Auswahl von Liste', erhalten Sie die Möglichkeit, einen Treiber aus einer Liste zu wählen.

Netzwerkkonfiguration initialisieren

Internet-Gateway

Hier müssen Sie angeben, ob Sie Ihren Server als Internet-Gateway benutzen möchten oder nicht. Wählen Sie 'This server will (probably) be configured as internet gateway …', wenn

- kein Internet-Gateway oder Router in Ihrem Netzwerk vorhanden ist,
- Sie einen existierenden Gateway/Router ersetzen möchten,
- Sie nicht geplant haben, je einen Gateway einzusetzen.

Falls diese Optionen für Sie nicht zutreffen (z. B. weil Sie schon einen Internet Gateway/Router besitzen), wählen Sie 'There is already an internet gateway or router'.

Host- und Domainname

Nachdem Sie den Internet-Gateway eingerichtet haben, gelangen Sie zur Konfiguration des Host- und Domainnamens für Ihren Server. Der Name besteht aus dem eigentlichen Rechnernamen (engl. *hostname*) und dem Domainnamen. Erlaubte Zeichen sind Buchstaben, Ziffern und das Zeichen '-'. Der Domainname setzt sich aus mehreren solchen Teilen zusammen, die durch Punkte getrennt sind.

Rechnername ist der Name, den der Rechner im Netzwerk haben soll, voreingestellt ist `server1`. Der Name sollte nicht mehr als acht Zeichen umfassen und darf im lokalen Netzwerk noch nicht vergeben worden sein.

Die hier gewählte Domain ist eine Bezeichnung für das lokale Netzwerk und mit dem Wert `office` vorbelegt. Zusätzlich gibt es eine NT-Domäne. Diese ist unabhängig von der „normalen" Domain (oder der Internet-Domain bei Anschluss an das Internet), welche standardmäßig `OFFICE` heisst. Durch diese Belegung wird auch die NT-Domäne gesetzt.

Tipp

Möchten Sie die NT-Domäne ändern, starten Sie im später installierten System YaST2 und wählen das Samba-Modul an, welches sich unter 'Netzwerk/Erweitert' befindet. Ändern Sie dies jedoch nur, wenn es unbedingt erforderlich ist.

Tipp

Die lokale Domain dient der Identifizierung der Rechner bei Verwendung des TCP/IP-Protokolls und wird an die am lokalen Netz angeschlossenen Clients automatisch weitergereicht.

Tipp

Wenn Sie keine Domain bei Ihren anderen Computern definiert haben, können sie den Eintrag 'Domainname' unangetastet lassen. Unter 'Hostnamen' können Sie Ihrem Server einen beliebigen Namen geben.

Tipp

Die Internet-Domain dient der Identifizierung eines Netzwerks im Internet und müsste registriert werden. Da es sich hier aber um ein lokales, von aussen (Dank der Firewall) nicht zugängliches Netzwerk handelt, ist die Internet-Domain hier ohne Belang.

Wenn dieser Server Ihr erster Computer im Netzwerk ist, brauchen Sie die vorgeschlagene IP-Adresse und Netzwerkmaske nicht zu verändern. Andernfalls starten Sie auf einem Windows-Client eine DOS-Shell und geben `ipconfig` ein. Der

Befehl zeigt Ihnen die IP-Adresse Ihres Clients an. Wählen Sie diese IP-Adresse aus und geben es im Feld 'IP Adresse' ein, wobei Sie die letzte Ziffer ändern, z. B. wenn `10.10.0.4` auf Ihrem Client angezeigt wird, wählen Sie z. B. `10.10.0.64`.

Bei der Wahl auf 'Weiter' speichert der SuSE Linux Office Server alle Ihre Einstellungen. Beachten Sie, dass es danach keine Möglichkeit gibt, wieder mit 'Zurück' zu den vorherigem Schritt zu gelangen.

Netzwerk-Management

Als Netzwerk-Management wird hier DHCP bezeichnet. YaST2 überprüft, ob sich in Ihrem Netzwerk ein DHCP-Server befindet. Es empfiehlt sich diesen Service zu nutzen, da er normalerweise immer benötigt wird, d. h. YaST2 gibt Ihnen einen Vorschlag, den Sie folgen können.

Wenn bereits ein DHCP-Server in Ihrem Netz vorhanden ist, sollten Sie 'Do not start' anwählen (normalerweise wird dies YaST2 bereits vorselektieren).

Falls YaST2 kein DHCP-Server gefunden hat, sollten Sie einen Server durch YaST2 einrichten lassen. Ein DHCP-Server wird benötigt, damit Ihre Clients

- IP-Adresse,
- Routing Informationen und
- Informationen zum Nameserver

erhalten können. Dadurch vereinfacht sich der Anschluß eines neuen Clients ans Netzwerk; er muß nur noch den DHCP-Server angeben. Nach allen Einstellungen wird die Installation abgeschlossen.

Status der Vorkonfigurierung

Nachdem Sie den Rechner eingerichtet haben, wird Ihnen in diesem Fenster die Liste aller Dienste angezeigt, die automatisch für diesen Server konfiguriert wurden. Alle Dienste, die mit 'OK' gekennzeichnet sind, werden zukünftig nach Wahl auf 'Weiter' gestartet.

Dies gilt nicht für das Internet-Gateway. Dieses müssen Sie im installierten System konfigurieren. Weitere Informationen finden Sie hierzu im Kapitel *Internet-Zugang für Clients* auf Seite 47.

Abschluss der Installation

Nachdem die SuSE Linux Office Server Grundkonfiguration beendet wurde fährt das Linux-System in den endgültigen Betriebszustand hoch. Auf dem Bildschirm erscheinen dabei wieder zahlreiche Meldungen. Zum Abschluss der Installation muss 'SuSEconfig' das installierte SuSE Linux System initialisieren.

Falls während der Installation Fehler augetreten sind, können Sie diese im Protokoll der Installation einsehen.

Achtung

Nachdem Sie die Installation abgeschlossen haben, sind sämtliche Serverdienste aktiv. Falls Sie andere Rechner besitzen, die genau dieselben Dienste anbieten, kann es zu Störungen in Ihrem Netzwerk führen.

Achtung

Grafisches Login

Der SuSE Linux Office Server ist nun installiert und Sie können sich zum ersten Mal an Ihrem System anmelden. Auf Ihrem Monitor erscheint nun das grafische Login. Geben Sie bei 'Benutzername:' den Loginnamen des Administrator-Accounts ein, den Sie in Abschnitt *Administrator-Account anlegen* auf Seite 15 angelegt haben.

Achtung

Aus Sicherheitsgründen raten wir davon ab, die grafische Umgebung als Benutzer `root` zu starten (siehe Kapitel *Passwort für den Systemadministrator* auf Seite 14). Es ist ratsam, sich nur in absolut notwendigen Fällen als `root` anzumelden.

Achtung

Nach dem erfolgreichen Login startet Ihre Desktopumgebung. Ihr Administrator-Account beinhaltet schon verschiedene Icons, die Sie auf Ihrem Desktop finden können.

Wenn Administrationsarbeiten anfallen, klicken Sie auf das Icon 'YaST'. Ein Fenster öffnet sich, in dem Sie das root-Passwort eingeben müssen. Nachdem YaST2 gestartet wurde, können Sie Ihre Konfigurationsaufgaben erledigen.

Sollten Sie weitere Benutzer für Ihr Netzwerk benötigen, können Sie in Abschnitt *Erweiterte Konfiguration* auf Seite 26 weitere Erklärungen finden.

Konfiguration des Fileserver und der Clients unter Windows

In diesem Kapitel zeigen wir Ihnen, wie Sie von Windows-Clients aus auf einen Fileserver zugreifen können. Es wird beschrieben, wie Sie diese konfigurieren müssen, um ein Verzeichnis auf dem Fileserver für mehrere Benutzer zugänglich zu machen.

Serverkonfiguration

Standardkonfiguration

Nachdem Sie erfolgreich die Installation abgeschlossen haben, ist Ihr Fileserver bereits so konfiguriert, dass er ein Verzeichnis `/shared` besitzt, das von Ihren Anwendern benutzt werden kann. Bevor Sie dies testen können, muß Ihr Windows-Client konfiguriert sein. Wie dies geht, erfahren Sie im Abschnitt *Arbeitsplatzkonfiguration allgemein* auf der nächsten Seite. Sind Ihre Arbeitsplatzrechner korrekt eingerichtet, starten Sie unter Windows den Dateimanager und wählen 'Netzwerk' → 'Gesamtes Netzwerk'. Jetzt sollten Sie ein leeres Verzeichnis `/shared` sehen, in dem Sie Dateien hineinkopieren und von anderen Clients bearbeitet werden können.

Erhalten Sie eine Fehlermeldung konsultieren Sie das Kapitel *Fehlerbehebung* auf Seite 91.

Der Vorteil des Verzeichnisses `/shared` ist, dass Sie keine weiteren Einstellungen vornehmen müssen. Jeder kann innerhalb dieses Verzeichnisses lesen, schreiben und löschen. Dies ist aber auch der gravierendste Nachteil. Möchten Sie dies verhindern, müssen Sie private Verzeichnisse einrichten. Diese sind anwenderbezogen und stehen unter der Regie eines Benutzers. Sie werden im nächsten Abschnitt beschrieben.

Erweiterte Konfiguration

Benötigen Sie zusätzlich zu dem `/shared`-Verzeichnis auch private Anwenderverzeichnisse, gehen Sie folgendermaßen dazu vor:

1. Sie benötigen eine zentrale Windowsbenutzerverwaltung (PDC). Standardmäßig ist der SuSE Linux Office Server als PDC vorkonfiguriert und Sie brauchen nichts zu ändern.

   Achtung

   Ist ein anderer PDC in Ihrem Netzwerk bereits vorhanden, *müssen* Sie den SuSE Linux Office Server anders konfigurieren. Starten Sie dazu das YaST2 Kontrollzentrum und rufen Sie das Samba-Modul auf. Im Feld 'Art des Servers' stellen Sie von 'Domäne' auf 'Arbeitsgruppe' um. Vergessen Sie nicht einen geeigneten Namen einzugeben.

   Achtung

2. Richten Sie auf dem SuSE Linux Office Server die potentiellen Benutzer ein, die auf dem Server Ihre privaten Verzeichnisse besitzen können.

   Wählen Sie auf Ihrem Desktop das Piktogramm 'Benutzerverwaltung' an, und geben Sie das Root-Passwort ein.

Sie können bequem einen neuen Benutzer anlegen, in dem Sie auf die Schaltfläche 'Hinzufügen' anklicken und die entsprechenden Eingabefelder ausfüllen; schließen Sie die Eingabe mit 'Anlegen' ab. Der neue Benutzer darf sich nun mit seinem Login-Namen (in unserem Beispiel 'tux') und Passwort auf dem Server anmelden.

Bevor Sie den Benutzer anlegen, können Sie unter 'Details' speziellere Einstellungen vornehmen, an denen Sie nichts verändern sollten, wenn Sie sich nicht auskennen. Dort befindet sich eine Liste an Standardgruppen, aus der Sie den Home-Verzeichnis-Pfad, der hier verändert werden kann, ebenso die Benutzerkennung (ID) und eine Auswahlliste für Login-Shells auswählen können. Im Eingabefeld welches mit 'Zusätzliche Gruppenzugehörigkeit' beschriftet ist, können Sie weitere Gruppen hinzufügen. Diese ermöglichen dem Benutzer weitere Zugriffsrechte. Wenn der neue Benutzer Zugriff auf das Modem haben soll, muss für ihn `dialout` und `uucp` (engl. *unix to unix copy program*) eingetragen sein.

3. Konfigurieren Sie Ihre Windows-Clients. Schlagen Sie hierzu die folgenden Abschnitte zur Arbeitsplatzkonfiguration von Windows 9x/ME oder Windows-XP nach.

Expertenkonfiguration

Feineinstellungen können Sie mit SWAT konfigurieren, welcher standardmäßig Port 901 überprüft. Sie haben dazu folgende Zugriffsmöglichkeiten:

- Am SuSE Linux Office Server: Auf dem Desktop Ihres Administrator-Accounts befindet sich ein Piktogramm mit dem Namen SWAT.

  Hinweis

  Mit SWAT können Sie auch Benutzer anlegen. Beachten Sie jedoch, dass diese Benutzer nur unter Samba verfügbar sind, nicht jedoch als „normale Linux-User". Möchten Sie gewährleisten, dass Benutzer sowohl in Samba als auch über NIS/YP verfügbar sind, legen Sie neue Benutzer stets mit YaST2 an.

  Hinweis

- Vom Client: Starten Sie einen Webbrowser und geben als Adresse `http://server1.office:901` ein. Identifizieren Sie sich als Benutzer `root` mit dem entsprechenden Root-Passwort.

Arbeitsplatzkonfiguration allgemein

Bevor wir auf den nachfolgenden Seiten Ihre Arbeitsplätze Schritt für Schritt für die Nutzung der Fileserver- und Internetfunktionen des SuSE Linux Office Servers einrichten, stellen Sie bitte sicher, dass in jedem Rechner eine Netzwerkkarte

eingebaut und über geeignete Kabel mit dem Server verbunden ist. Nichts ist frustrierender, als stundenlang in Programmen nach Fehlerquellen zu suchen, um dann festzustellen, dass das Netzwerkkabel nicht richtig steckte…

Tipp

Viele Netzwerkkarten signalisieren durch eine Leuchtdiode, dass sie ordnungsgemäß mit dem Netzwerk verbunden sind.

Tipp

Arbeitsplatzkonfiguration für Windows 9x/ME

Standardkonfiguration

Nachdem die Netzwerkkarte dem Rechner nun bekannt sein müsste, stellen wir als nächstes sicher, dass alle Softwarekomponenten vorhanden sind, damit Ihr Windows-System überhaupt in der Lage ist, auf den Server zuzugreifen. Wählen Sie hierzu in der Systemsteuerung den Punkt 'Netzwerk' aus. Es erscheint ein Fenster mit drei Registerkarten und einer Übersicht der installierten Netzwerk-Komponenten (siehe Abb. 2.1 auf der nächsten Seite).

In dieser Liste müssen neben der im Rechner installierten Netzwerkkarte zumindestens der „Client für Microsoft-Netzwerke" und das „TCP/IP-Protokoll" auftauchen. Bei vielen Rechnern sind diese Komponenten bereits vorhanden; falls nicht, müssen Sie sie nachinstallieren: Wählen Sie hierzu 'Hinzufügen' und doppelklicken Sie auf 'Client'; selektieren Sie im nun erscheinenden Fenster `Microsoft` sowie „Client für Microsoft-Netzwerke" und bestätigen Sie Ihre Eingabe mit 'OK'. „TCP/IP" ist unter 'Protokolle' beim Hersteller `Microsoft` gelistet.

Bitte beachten Sie, dass hierzu in aller Regel eine Windows-CD benötigt wird und nach erfolgreicher Installation meist ein Neustart des Systems erforderlich ist.

Weitere Einstellungen sind nicht nötig, diese werden durch DHCP automatisch vom Server übernommen. Nach der Konfiguration der Identifikations-Daten ist ein Neustart von Windows erforderlich.

Falls durch besondere Einstellungen am System diese Daten nicht automatisch von Windows übernommen werden können, stellen Sie bitte sicher, dass für den WINS-, DNS-Server und den Gateway die IP-Nummer desServers eingetragen ist. Standardmäßig wird hier `192.168.0.1` vorgeschlagen.

Sie können die Einstellungen überprüfen, in dem Sie auf dem Desktop des Windows-Clients über dem Piktogramm 'Netzwerkumgebung' ein Kontextmenü öffnen (rechte Maustaste) und den Punkt 'Eigenschaften' anwählen. Dabei sollten folgende Einstellungen angezeigt werden:

IP-Adresse – Eintrag sollte auf 'IP-Adresse automatisch beziehen' stehen

Abbildung 2.1: *Netzwerkkonfiguration unter Windows 9x/ME*

WINS-Konfiguration – Ausgewählt ist 'DHCP für WINS-Auflösung verwenden'

Gateway – leer

DNS-Konfiguration – Ausgewählt ist 'DNS deaktivieren'

Erweiterte Einstellungen

Nach dem Neustart sollten die gerade installierten Protokolle bzw. Dienste zur Verfügung stehen. Falls Sie Zugriff auf ein privates Anwenderverzeichnis erhalten möchten, müssen Sie noch einige Einstellungen vornehmen.

- Doppelklicken Sie dazu wieder in der Systemsteuerung auf 'Netzwerk' und stellen Sie zuerst einmal sicher, dass die „Primäre Netzwerkanmeldung" auf „Client für Microsoft-Netzwerke" steht; wählen Sie danach die Registerkarte 'Identifikation' aus. Hier müssen Sie noch einige Angaben machen. Computername und Beschreibung sind letztendlich egal, bei ersterem muss lediglich darauf geachtet werden, dass der Name aus nicht mehr als 15 Zeichen bestehen und keine Leerzeichen enthalten darf.

Hinweis

Wichtig ist die zu konfigurierende Arbeitsgruppe, die standardmäßig auf `OFFICE` eingestellt ist. Verwenden Server und Client unterschiedliche Arbeitsgruppennamen, kann kein einfacher Zugriff auf den Server erfolgen.

Hinweis

- Ist der SuSE Linux Office Server auf „Domain“ konfiguriert, müssen Sie unter der Registerkarte ‘Zugriffssteuerung’ von ‘Zugriffssteuerung auf Freigabeebene’ auf ‘Zugriffssteuerung auf Benutzerebene’ umschalten und unter ‘Benutzer- und Gruppenliste beziehen von’ den bei der Installation eingestellten Domainnamen eintragen. Der Domainname ergibt sich aus der Netzwerkkonfiguration, Standard ist `office`)

- Damit Ihr Windows-Client korrekt funktionieren kann, benötigt er eine NT-Domäne, diese ist standardmäßig auf `OFFICE` eingestellt. Unter Windows tragen Sie im Menü ‘Client für Microsoft-Netzwerke’ → ‘Eigenschaften’ → ‘NT-Domäne’ die entsprechendne NT-Domäne ein. Die NT-Domäne ergibt sich aus der Samba-Konfiguration.

  Wenn Ihr SuSE Linux Office Server als Domain-Controller konfiguriert wurde (dies ist der voreingestellte Standard), erfolgt die gesamte Benutzerverwaltung auf diesem Server. Jeder angelegte Benutzer ist dann auch den Windows-Clients bekannt.

Ein erster Test

Nachdem der Rechner neu gestartet worden ist, wird Windows Sie nach einem Benutzernamen und Kennwort fragen. Melden Sie sich hier als Benutzer mit denselben Daten an, die Sie im Benutzermodul von YaST2 festgelegt haben.

Klicken Sie nach dem Hochfahren die ‘Netzwerkumgebung’ an. Spätestens nach ein paar Sekunden sollte hier Ihr SuSE Linux Office Server unter dem bei der Installation konfigurierten Namen sichtbar werden. Wenn Sie auf den entsprechenden Namen klicken, sollte sich ein Fenster öffnen, in dem sich Ihr privates Verzeichnis (das auch Ihren Namen trägt) sowie der allgemein verfügbare „Shared Data“-Bereich auftauchen.

Tipp

Sollte die Anmeldung oder der Testzugriff auf den Server nicht funktionieren, liegt wahrscheinlich ein Netzwerk- oder Passwortproblem vor. Zur Änderungen Ihres Passworts steht (neben dem Benutzermodul von YaST2 am Server) unter `https://server1.office/change_password` ein Web-Frontend zur Verfügung, dass Sie auch von einem Client-Rechner aus ausführen können. Ersetzen Sie ggf. die Host- und Domainnamen `server1.office` durch ihren richtigen Wert.

Tipp

Über die URL `https://server1.office/change_password` eingeben, gibt es folgendes zu sagen:

1. Beachten Sie, dass ältere Clients (Windows 95) oft keine Unterstützung für das https-Protokoll bieten, d. h. Sie können dann nicht auf diese Seite zugreifen.
2. Bei der ersten Verbindung wird der Benutzer darauf aufmerksam gemacht, dass dieser Rechner noch unbekannt ist. Normalerweise fragen die Browser dann, ob man diesen Rechner/oder Schlüssel akzeptieren möchte. Diese Vorgehen hängt sehr stark vom Browser ab.

Verwenden Sie eine frühe Version von Windows 95, die noch keine Übertragung von verschlüsselten Passwörtern an Samba unterstützt, so müssen Sie zuerst von `ftp://ftp.microsoft.com/softlib/mslfiles/vrdrupd.exe` ein Update herunterladen und installieren, damit die Anmeldung mit verschlüsselten Passwörtern funktionieren kann.

Laufwerke verknüpfen

Natürlich wäre es recht kompliziert, alle Dateien irgendwo tief in der Netzwerkumgebung abzulegen, aber glücklicherweise gibt er hier eine einfache und sehr komfortable Lösung – die Verknüpfung von Netzlaufwerken des Servers mit Laufwerksbuchstaben.

Wählen Sie unter Windows 9x/ME im Windows-Explorer den Punkt 'Extras' → 'Netzlaufwerk verbinden' an. Im nun erscheinenden Fenster haben Sie die Möglichkeit, das unter „Pfad" zu spezifizierende Verzeichnis mit einem Laufwerksbuchstaben zu verknüpfen. Wenn Sie beispielsweise `\\server1\public` mit `E:` verbinden, steht Ihnen der Inhalt des öffentlichen Verzeichnisses des SuSE Linux Office Server als „virtuelles" Laufwerk `E:` zur Verfügung.

Bitte beachten Sie, dass diese Verknüpfung mit dem Herunterfahren des Rechners entfernt wird und somit beim nächsten Start des Windows-Systems nicht mehr zur Verfügung steht. Wünschen Sie, dass diese Laufwerks-Verknüpfung auch beim nächsten Systemstart wieder funktioniert, aktivieren Sie bitte den Punkt 'Verbindung beim Start wiederherstellen'.

Arbeitsplatzkonfiguration für Windows XP

Standardkonfiguration

Die Einrichtung von Windows XP für den Dateiserver-Dienst des SuSE Linux Office Server unterscheidet sich prinzipiell nicht wesentlich von der Konfiguration, die wir im vorangegangen Kapitel für Windows 9x/ME beschrieben haben. Natürlich kann auch Windows XP nicht ohne funktionierende Netzwerkkarte auf

den SuSE Linux Office Server zugreifen und selbstverständlich ist auch Microsofts Betriebssystem auf bestimmte Protokolle und Einstellungen angewiesen.

Tipp

Bitte beachten Sie, dass Sie unter Windows XP entweder als „Administrator“ oder als ein der Gruppe „Administratoren“ angehörender Benutzer angemeldet sein müssen, um Einstellungen an der Netzwerkkonfiguration vornehmen zu können. Beim ersten Anmelden benötigen Sie den Rootaccount und das Rootpassword vom Server.

Tipp

Die folgenden Schritte werden benötigt, nachdem Sie Windows XP installiert haben und Sie nun sich mit dem SuSE Linux Office Server verbinden möchten:

1. Nach dem Start von Windows XP wählen Sie im Menü ‘Start’ → ‘Einstellung’ → ‘Systemsteuerung’ den Eintrag ‘Netzwerkverbindung’ aus.
2. Im nächsten Schritt wählen Sie ‘Netzwerkaufgaben’ und klicken auf ‘Ein Heim- oder ein kleines Firmennetzwerk einrichten’. Es öffnet sich ein ‘Netzwerkinstall Assistent’. Bestätigen Sie mit ‘Weiter’.
3. Sie sehen nun drei mögliche Auswahlmöglichkeiten. Wählen Sie ‘Diesen Computer stellt eine Internetverbindung über einen anderes Computer Netzwerk oder lokales Gateway her’. Bestätigen Sie mit ‘Weiter’.
4. Windows XP möchte nun Informationen darüber haben, wie Sie Ihren Computer benutzen. Des Weiteren wird ein Name benötigt. Dies kann eine Beschreibung der Funktionalität (Office, Rezeption usw.) oder einfach ein Name eines Benutzers (z. B. David) sein. Geben Sie die benötigten Daten ein und bestätigen Sie mit ‘Weiter’.
5. Überprüfen Sie Ihre Einstellungen und wenn Sie zufrieden damit sind, klicken Sie auf ‘Weiter’.
6. Dieser Schritt benötigt der Name einer Arbeitsgruppe. Geben Sie diesen unter ‘Arbeitsgruppenname’ ein und wählen Sie ‘Weiter’.
7. Überprüfen Sie die Informationen, die Ihnen nun angezeigt werden. Sind Sie zufrieden, dann wählen Sie ‘Weiter’ ansonsten ‘Zurück’.
8. Ihr Computer wird dann die Konfiguration speichern. Ein Fenster öffnet sich (‘Der Vorgang wurde fast abgeschlossen’) und fragt Sie, wie Sie weiterverfahren möchten; es werden Ihnen vier Möglichkeiten angeboten. Windows XP kann Ihnen zusätzlich eine Installationsdiskette erstellen, die Sie benutzen zu können, um andere Microsoft-Produkte im Netzwerk zu installieren. Mit SuSE Linux Office Server ist dies nicht erforderlich; aktivieren Sie den vierten Punkt ‘Nur den Assistenten fertig stellen’ und wählen Sie ‘Weiter’.
9. Wählen Sie ‘Fertig stellen’.

Erweiterte Konfiguration

Mit den folgenden Schritten wird Ihr Windows-Client an einem PDC angemeldet.

1. Melden Sie sich unter Windows XP als Administrator an.
2. Jeder Windows XP Client muß ein einziges Mal am PDC angemeldet werden.
3. In Windows XP hat Microsoft die Netzwerkfunktionen von Windows NT 4 und 2000 übernommen. Leider wurden damit auch einige erweiterte Sicherheitsfunktion aktiviert, die es so in Windows 9x/ME nocht nicht gab. Unglücklicherweise hält Microsoft diese Erweiterungen geheim, so dass Samba damit nicht umgehen kann.

   Um diese erweiterten Sicherheitsfunktionen abzuschalten, müssen Sie die Registry ändern. Hierzu gibt es zwei Möglichkeiten:

   (a) Starten Sie den Explorer und geben als Adresse \\⟨*rechnername*⟩ ein (ersetzen Sie die Variable ⟨*rechnername*⟩ durch den richtigen Namen, standardmäßig ist dieser Wert auf `server1` gesetzt). Öffnen Sie das Verzeichnis `Shared Volume` und klicken Sie auf die Registry-Datei `xpkpdc.reg`. Sie ändert die Einstellungen so, dass Sie sich zukünftig auf dem SuSE Linux Office Server anmelden können. Damit ist die Änderung der Registry abgeschlossen.

   (b) Ist das Verzeichnis momentan nicht verfügbar oder möchten Sie die Einstellungen manuell vornehmen, gehen Sie wie folgt vor:

      i. Starten Sie den Registry-Editor durch Eingabe von `regedit` in der Eingabeaufforderung.
      ii. Wählen Sie im Menü 'Edit' → 'Suchen ...' und geben Sie im Feld 'Suchen nach' die Zeichenfolge `RequireSignOrSeal` ein.
      iii. Nachdem der Suchvorgang den gewünschten Eintrag gefunden hat, wählen Sie 'DisplayType'. Mit der rechten Maustaste öffnen Sie das Kontextmenü und rufen 'Modify' auf.
      iv. Ändern Sie den Wert von `1` nach `0`.
      v. Beenden Sie den Registry-Editor.

4. Nach dem Neustart von Windows XP wählen Sie aus dem Menü 'Start' → 'Systemeigenschaften'. Rufen Sie die Kategorie 'Netzwerk und Internetverbindung' auf, danach 'Netzwerkverbindungen'.
5. Rufen Sie im Menü 'Erweitert' → 'Netzwerk-Identifikation' auf.
6. Wählen Sie den Reiter 'Computername' und dort den Button 'Ändern' an. (siehe Abb. 2.2 auf der nächsten Seite).
7. Ein Fenster öffnet sich. Im Feld 'Computername' können Sie einen beliebigen Namen vergeben; unter 'Domain' tragen Sie die NT-Domäne (standardmäßig ist dies `OFFICE`) ein.

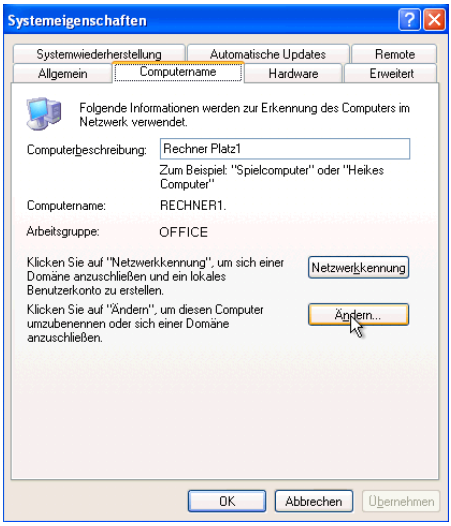


Abbildung 2.2: *Systemeigenschaften bei Windows XP*

Der Test kann beginnen

Um einen ersten Funktionstest durchführen zu können, gehen Sie wie folgt vor:

1. Starten Sie Ihren Rechner neu.
2. Nach dem Start drücken Sie (Strg) + (Alt) + (Entf) und sie gelangen zum Windowsanmeld Dialog.
3. Klicken Sie auf den Button 'Optionen >>'; das Fenster vergrößert sich und zeigt Ihnen einige erweiterte Möglichkeiten an.
4. Wählen Sie die Arbeitsgruppe `OFFICE` im Feld 'Anmelden an:' aus. (siehe Abb. 2.3 auf der nächsten Seite)
5. Melden Sie sich mit dem Benutzernamen und Passwort an (in unserem Beispiel mit `tux`). Sollten Sie noch keine Benutzer angelegt haben, holen Sie dies bitte umgehend nach (siehe Abschnitt *Erweiterte Konfiguration* auf Seite 26) und und melden Sie sich anschließend auf dem Windows XP-Rechner mit den entsprechenden Daten an.

Überprüfen Sie die Netzverbindung wie folgt: Rufen Sie 'Start' → 'Mein Computer' auf. Es öffnet sich ein Fenster. Unter 'Netzlaufwerke' sollten Sie einen entsprechenden Eintrag sehen.

Abbildung 2.3: *Windowsanmeldung*

Fehlerbehebung

Erhalten Sie die Fehlermeldung "Mehrfache Verbindungen . . . sind nicht erlaubt." ("Multiple connections ... are not allowed") überprüfen Sie die folgenden Punkte:

- Ist Ihre Registry korrekt angepasst worden? Wenn nicht, schauen Sie nochmals im Abschnitt *Erweiterte Konfiguration* auf Seite 33 nach und folgen den Einstellungen.
- Ist Ihre Registry wie in Abschnitt *Erweiterte Konfiguration* auf Seite 33 korrekt angepasst, gehen Sie wie folgt vor:

  1. Melden Sie sich in Ihrem Windows XP Client als Administrator an.
  2. Wählen Sie 'Start' → 'Systemeigenschaften'. Rufen Sie 'Netzwerk- und Internetverbindungen' → 'Netzwerkverbindungen' auf.
  3. Im Menü 'Erweitert' wählen Sie den Punkt 'Netzwerk-Identifikation' aus.
  4. Klicken Sie auf den Button 'Ändern' und geben im Feld 'Arbeitsgruppe' eine andere Arbeitsgruppe ein (z. B. `xxxx`).
  5. Ein Dialogfenster erscheint, welches Sie mit 'OK' bestätigen müssen. Starten Sie Ihren Computer neu .
  6. Wiederholen Sie nach dem Start die Schritte 1 bis 4, geben jedoch im Feld 'Arbeitsgruppe' Ihre richtige Arbeitsgruppe ein (standardmäßig ist dies `OFFICE`).
  7. Starten Sie Ihren Computer neu.

- Beim nächsten Start muß in der Login-Maske die Arbeitsgruppe `OFFICE` ausgewählt sein.

Konfiguration von Fileserver und Arbeitsplatz unter Linux

In diesem Kapitel zeigen wir Ihnen, wie Sie von Linux-Clients aus auf einen Dateiserver (engl. *Fileserver*) zugreifen können. Es wird beschrieben, wie Sie Ihre Linux-Clients konfigurieren müssen, um ein Verzeichnis auf dem Fileserver für mehrere Benutzer zugänglich zu machen.

Serverkonfiguration für Linux

Nach der Installation ist Ihr Fileserver so konfiguriert, dass Sie nichts mehr einstellen müssen.

Der Server stellt allen Anwendern einen gemeinsamer Ordner `/shared` zur Verfügung, sowie den geschützten privaten Bereich unter `/home`. Möchten Sie eine genauere Kontrolle über bestimmte Möglichkeiten des Dateiservers erhalten, können Sie die weiteren Einstellungen über das YaST2 Modul 'NFS-Server' vornehmen.

Arbeitsplatzkonfiguration

Nachdem wir uns vorher mit der Einrichtung von diversen Windows-Clients befasst haben, möchten wir Ihnen nun zeigen, wie Sie einen SuSE-Linux-Rechner als Client Ihres SuSE Linux Office Server verwenden können.

Dateiserver-Einstellungen

Im Vergleich zu den angesprochenen Windows-Lösungen lässt sich ein SuSE-Linux-System sehr einfach für den Zugriff auf Ihren SuSE Linux Office Server konfigurieren. Rufen Sie dazu bitte im YaST2-Kontrollzentrum unter 'Netzwerk/Erweitert' den Punkt 'NFS-Client' auf. In dem nun erscheinenden Dialogfenster haben Sie die Möglichkeit, Verzeichnisse Ihres SuSE Linux Office Servers in das Dateisystem des Client-Systems zu integrieren (siehe Abb. 3.1)

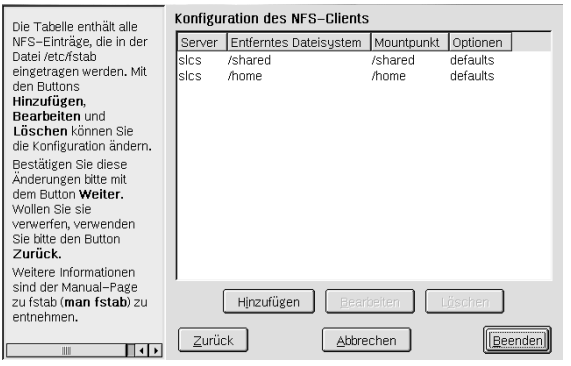


Abbildung 3.1: *YaST2-Modul zur Konfiguration von NFS*

Standardmäßig stehen die Verzeichnisse `/home`, unter dem alle (privaten) Homeverzeichnisse der SuSE Linux Office Server-Benutzer angelegt sind sowie sowie `/shared`, der allgemeine Dateibereich, auf den jeder Zugriff hat, zum Export per NFS zur Verfügung.

Um nun diese beiden Verzeichnisse einzubinden, wählen Sie 'Neu' und tragen Sie als „Rechnername des NFS-Servers" die IP-Adresse Ihres SuSE Linux Office Server ein, in der Regel ist dies `192.168.0.1`. Als 'Entferntes Dateisystem' geben Sie `/home` bzw. `/shared` an. Werden `/home` und `/shared` auf dem Client-Rechner nicht anderweitig benötigt, empfiehlt es sich, diese als Mountpunkte unter 'Mountpunkt (lokal)' einzutragen. Selbstverständlich können Sie auch jedes andere auf dem Client vorhandene Verzeichnis hier angeben. Das Feld 'Optionen' kann getrost ignoriert werden – hier können Experten, falls nötig, Feineinstellungen vornehmen. Nachdem Sie Ihre Einstellungen abgeschlossen haben, bestätigen Sie mit 'Beenden' Ihre Eingaben und bejahen ebenfalls die Frage, ob diese nun gespeichert werden sollen.

Die Datenverzeichnisse Ihres SuSE Linux Office Servers sind nun unter den im Kontrollzentrum konfigurierten Mountpunkten eingebunden.

NIS-Konfiguration

Nach der Einrichtung von NFS ist es empfehlenswert, auch „NIS" zu aktivieren. NIS, das oftmals auch als „Yellow Pages (YP)" bezeichnet wird, sorgt dafür, dass Logins (also Benutzernamen und dazu gehörige Passwörter) des Servers auf jedem Linux-Client innerhalb Ihres Netzwerkes ebenfalls zur Verfügung stehen.

Möchten Sie auf private Dateibereiche Ihres Servers, wie z. B. die Homeverzeichnisse, zugreifen, führt an der Einrichtung von NIS kein Weg vorbei – schließlich sollen ja nur Befugte Zugriff auf diesen privaten Bereich erhalten.

Um NIS zu aktivieren wählen Sie im Kontrollzentrum unter der Kategorie 'Netzwerk/Erweitert' das Modul 'NIS-Client' aus. Aktivieren Sie 'NIS verwenden' und geben Sie bei 'NIS-Domain' die bei der Installation eingestellte Domain, z. B. „tux.net" an. Die 'IP-Adresse des NIS-Servers' ist in aller Regel `192.168.0.1`.

Bestätigen Sie auch hier Ihre Einstellungen mit 'Beenden'. Fertig!

Samba

Normalerweise brauchen Sie hier nichts zu ändern, wenn Sie die Standardwerte übernommen haben. Nach der Installation läuft der SuSE Linux Office Server als primärer NT Domänenserver (primary domain controller, kurz PDC) unter der NT-Domäne `OFFICE`.

Möchten Sie dennoch Werte ändern, so bestimmen Sie zuerst die Grundkonfiguration des Samba-Servers. Wählen Sie hier, ob der Server als Workgroup-Server oder als (primärer) Domain-Controller fungieren soll.

Geben Sie dann den passenden Namen für die Workgroup oder Domain ein. Die beschreibende Zeichenkette erleichtert die Identifikation des Servers beim Browsen durch das Netzwerk.

Abschnitt *Samba* auf Seite 58 liefert Ihnen weitere Details. Weiterführende Informationen können Sie im Samba-Buch nachlesen (siehe `http://www.susepress.de/de/katalog/3_935922_15_9/index.html`, ISBN 3-935922-15-9).

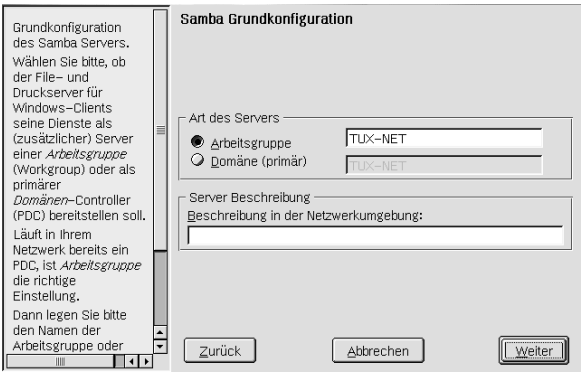


Abbildung 3.2: *Samba Grundkonfiguration*

Intra-Net

Dieses Kapitel beschreibt, wie Sie Informationen in Ihrem Intra-Net ablegen und publizieren können. Des Weiteren erhalten Sie einen kleinen Einblick in den Webserver Apache.

Das öffentliche Verzeichnis public_html

Jeder Benutzer besitzt auf dem SuSE Linux Office Server ein Verzeichnis namens `public_html`. Wenn Sie anderen Benutzern Dateien zur Verfügung stellen möchten, kopieren oder verschieben Sie Ihre Dokumente am besten in dieses Verzeichnis.

Sie können z. B. Ihre eigene Homepage in diesem Verzeichnis erstellen.

Zugriff auf das öffentliche Verzeichnis

Um ein Verzeichnis eines anderen Benutzers anzuzeigen, starten Sie einen Browser und geben als Adresse z. B. ein `http://server1.office/~tux` (`server1.office` ist der Standardwert den Sie ggf. durch Ihre eigene Benennung ersetzen müssen, `tux` der Benutzer, von dem das Verzeichnis `public_html` angezeigt werden soll).

Sind in diesem Verzeichnis Dateien enthalten, werden diese im Browser angezeigt. Existiert dagegen eine Datei `index.html`, wird diese HTML-Datei im Browser formatiert.

Insofern können Sie sich Ihre eigene Homepage aufbauen, die von jedem Benutzer im Netzwerk abgerufen werden kann.

Globale Webseiten im Intra-Net

Möchten Sie eine firmenweite Seite innerhalb Ihres Intra-Nets veröffentlichen, dann legen Sie Ihre HTML-Seiten im Verzeichnis `/usr/local/httpd/htdocs` ab. Damit die Seite allen Benutzern zur Verfügung steht, müssen Sie Apache (dem Webserver) mitteilen, das Verzeichnis neu einzulesen. Geben Sie hierzu als Benutzer `root` den Befehl `rcapache reload` ein.

Apache

Der Webserver Apache ist ein Prestigeprojekt der Open-Source-Szene. Ungefähr 60% aller Webserver auf der ganzen Welt laufen damit.

„Geboren“ wurde der Apache ursprünglich als Notbehelf, als Erweiterung des NSCD 1.3 Webservers um wichtige Verbesserungen und Bugfixes. Daher auch sein Name („A patchy server“), der sich vor allem auf seine „Patchworkstruktur“ bezieht, nicht auf den nordamerikanischen Indianerstamm.

Apache als Intra-Netserver

Der folgende Abschnitt wird Ihnen komprimiert darstellen, wie der auf Ihrem System laufende Apache im Prinzip konfiguriert sein muss, um Ihnen als Intra-Netserver zu dienen. Bitte haben Sie dafür Verständnis, dass an dieser Stelle keine komplette Erörterung seiner Konfigurationsmöglichkeiten und Zusatzmodule erfolgen kann. Hierzu sei auf die Informationsquellen auf Seite 44 verwiesen.

Um aus einem frisch installierten Apache einen kraftvollen Intra-Netserver zu machen, sind im einzelnen folgende Schritte notwendig:

1. Welche Inhalte wollen Sie präsentieren?

   Das Verzeichnis, in dem Apache standardmäßig den zu präsentierenden Inhalt erwartet, ist `/usr/local/httpd/htdocs`. Hier legen Sie alle Dateien ab, die Apache am Ende darstellen soll – und zwar mit Leserechten für andere Benutzer:

   ```
   -rw-r-r- 1 ich meine_gruppe 0 Mar 2010 14:26 meine_datei
   ```

   Verzeichnisse werden dementsprechend so angelegt, dass Sie selber lesend, schreibend und ausführend zugreifen können, Ihre Gruppe und der Rest der Welt höchstens lesend und ausführend. Ihre eigene persönliche Startseite erwartet der SuSE-Apache als `index.html`. Sollten Sie keine eigene Startseite unter diesem Namen verwenden, greift Apache auf eine eigene Default-Starteite zu.

2. Jetzt werden die grundlegendsten Einträge (als `root`) in der `/etc/httpd/httpd.conf` vorgenommen. Zu nennen sind hier:

   ServerRoot – `/usr/local/httpd` hier liegt der Dateibaum, unter dem alle Apache relevanten Dateien platziert sind

   ServerAdmin – die E-Mail-Adresse des Administrators – sollte eine Seite auf dem neuen Server nicht anzeigbar sein, wird unter anderem diese Adresse weitergegeben

   ServerName – voll gültiger Name des Servers

   DocumentRoot – die „DocumentRoot"-Variable ist `/usr/local/httpd/htdocs`, wie in Schritt 1 angegeben

   CustomLog – `/var/log/httpd/access_log`, hier werden standardmäßig die Zugriffe auf Ihren Server mitgeloggt

   ErrorLog – `/var/log/httpd/error_log`, hier werden Fehlermeldungen archiviert

3. Sollen einzelne Verzeichnisse oder gar alle Inhalte des Servers vor unbefugtem „Betreten" geschützt werden, bieten sich mehrere einfache Schutzmechanismen an:

   - Den expliziten Schutz einzelner Verzeichnisse über `.htaccess`. Jedes Verzeichnis, das Sie schützen wollen, erhält eine eigene `.htaccess` Datei, in der (sinngemäß) die folgenden Zeilen zu lesen sein werden:

```
order deny,allow
deny from all
allow from server1
```

Das Verzeichnis (und alle Unterverzeichnisse, in dem diese Datei liegt, ist jetzt vor externen Zugriffen geschützt und erlaubt nur noch die Auslieferung an Rechner aus der internen Domain `server1`. Ebensogut könnten Sie, wenn durch eine Firewall die Verbindung ins restliche Internet voll und ganz dicht ist, dieses Verfahren verwenden, um einzelne Hosts aus der `server1`-Domain auszusperren. Damit die neuangelegte `.htaccess`-Datei auch beim Start des Apachen gelesen wird, muss in der `/etc/httpd/httpd.conf` folgende Option aktiviert sein:

```
#
# This controls which options the .htaccess files in directories
#  can override. Can also be "All", or any combination of
# "Options", "FileInfo", "AuthConfig", and "Limit"
#
    AllowOverride All
```

Ist diese Option nicht aktiviert, werden sämtliche `.htaccess`-Einträge ignoriert.

- Derselbe Effekt wie mit `.htaccess` wird auch erzielt, wenn analoge Einträge in der zentralen `httpd.conf` vorgenommen werden. Entweder man spezifiziert einzelne `>Directory/<`-Einträge oder es wird kategorisch eine Zugangsbeschränkung vorgenommen:

  ```
  #
  # Controls who can get stuff from this server.
  #
      Order deny,allow
      Deny from all
      Allow from slcs.de
  ```

  Diese Maßnahme hat die gleiche Auswirkung, als würden Sie die oberste Verzeichnisebene des Webservers, die DocumentRoot mit allen ihren Unterverzeichnissen via `.htaccess` schützen.

Dieser kleine Einblick ist nur eine Einführung in das Prinzip des Verzeichnisschutzes. Es gibt noch eine große Anzahl beliebig komplizierter Schutzmechanismen, die ein Administrator einsetzen kann, um unliebsamen Besuch abzuschütteln. So lassen sich zum Beispiel auch bestimmte Regionen eines Servers nur von autorisierten Benutzern mit Passwort betreten.

Weitere Informationen zu Apache

Mehr über Apache erfahren Sie auf der Website des Projekts unter `http://httpd.apache.org`. Hier finden Sie sehr ausführliche Informationen zur augenblicklichen Entwicklung, FAQs, Tutorials und eine sehr gute Erläuterung zur Konfiguration.

Sollten Sie an zusätzlichen Modulen für Ihren Webserver interessiert sein, wäre `http://modules.apache.org` ein guter Anfang.

Für wirklich tiefgreifende Fragen und höhere Anforderungen sind inzwischen mehrere Bücher erschienen, wobei hier vor allem das im O'Reilly-Verlag erschienene „Apache: The Definitive Guide" von Ben und Peter Laurie zu nennen wäre.

Mit ApacheWeek (`http://www.apacheweek.org`) existiert ein wöchentlicher Newsletter, der über die neuesten Entwicklungen des Projekts informiert.

Internet-Zugang für Clients

Wenn Sie für Ihre Rechner eine Internetanbindung bereitstellen möchten, dann können Sie in diesem Kapitel die nötigen Hilfestellungen darüber enthalten.

Grundlagen einer Internetverbindung

Das Internet

Alle Rechner im Internet bilden ein einziges großes Netzwerk, in dem unterschiedliche Betriebssysteme auf unterschiedlicher Hardware laufen. Damit dennoch beliebige Rechner miteinander kommunizieren können, muss ein allgemeines, verbindliches Kommunikationsprotokoll verwendet werden, über das die unterschiedlichen Betriebssysteme unabhängig von der jeweiligen Hardware ihre Daten austauschen können. Das leistet das Internet Protocol (IP) zusammen mit dem Transmission Control Protocol (TCP), dem User Datagram Protocol (UDP) und dem Internet Control Message Protocol (ICMP). Diese Protokolle bilden die gemeinsame „Sprache“ aller Rechner im Internet und die Kurzbezeichnung ist TCP/IP.

Die IP-Adresse

Jeder Rechner im Internet hat eine Identifikationsnummer, die so genannte IP-Adresse, und nur über diese Nummer kann er via TCP/IP angesprochen werden. Normalerweise hat ein Rechner auch einen Klartextnamen, mit dem er in Anwendungsprogrammen bezeichnet wird. Um die IP-Adresse zu einem Klartextnamen zu bekommen, gibt es das Domain Name System (DNS). Dies ist ein spezieller Dienst, den so genannte Nameserver bereitstellen. Ein Rechner bzw. ein Programm, das einen Dienst bereitstellt, heißt Server (hier z. B. DNS-Server), ein Rechner oder Programm, das einen Dienst beansprucht, heißt Client.

Hinweise zu allen Arten des Internetzugangs

Personal Firewall

Die Personal Firewall ist insbesondere dafür gedacht, ohne großen Konfigurationsaufwand zu verhindern, dass Rechner aus dem Internet eine Verbindung zu Ihrem eigenen Rechner aufbauen können. Gleichzeitig werden jedoch Verbindungen von Ihrem eigenen Rechner aus zu Rechnern im Internet zugelassen. Somit ist die Personal Firewall für die üblichen Anforderungen gut geeignet und an sich ausreichend. Konfigurierbar ist einzig der Name des Netzwerkinterfaces (`ppp0`, `ippp0`, `eth0`) in der Datei `/etc/rc.config.d/security.rc.config`, auf welchem insbesondere Anfragen zum Aufbau einer Verbindung abgewiesen werden. Dies erledigt YaST2 für Sie, wenn Sie in den entsprechenden Dialogen den Punkt ‘Firewall aktivieren’ anwählen.

Folgendes wird von der Personal Firewall gefiltert:

- Alle TCP-Verbindungsanfragen. Die Sicherheit beruht darauf, dass die Personal Firewall immer das erste ankommende TCP-Paket ablehnt, das einen korrekten TCP-Verbindungsaufbau verhindert. Diejenigen TCP-Pakete, die nicht zu einer bestehenden TCP-Verbindung gehören und keine TCP-Verbindungsanfragen sind, werden nämlich unabhängig von den Filterregeln der Personal Firewall verworfen.
- Alle UDP-Pakete bis auf Pakete von Port 53 von einem der konfigurierten Nameserver (normalerweise nur der Nameserver des Providers, der normalerweise beim Aufbau der Internet-Verbindung automatisch konfiguriert wird; vgl. hierzu „Internetverbindung und lokales Netzwerk“ auf Seite 49).
- Einige eher seltene ICMP-Pakete.

Alle Filterregeln gelten nur für das/die konfigurierte(n) Interface(s). Bei manchen Diensten kann es zu „Nebenwirkungen“ kommen. Dazu zählen IRC (CTCP), FTP (nur der PORT-Modus; passives FTP, was von den üblichen Browsern verwendet wird, funktioniert), printer-services, real-audio, real-video, cucme, napster, icq und wenige andere.

Automatische Einwahl (Dial on Demand)

Wenn Sie in den YaST2-Modulen ‘Dial on demand’ oder ‘Automatische Einwahl’ aktivieren, dann wird z. B. nach der Eingabe einer externen URL im Browser oder beim Senden und Abholen von E-Mail die Internet-Verbindung automatisch aufgebaut. Nur wenn Sie eine so genannte Flatrate (Pauschaltarif) für den Internetzugang haben, ist ‘Dial on demand’ empfehlenswert. Denn durch Prozesse, die im Hintergrund ablaufen (z. B. zum regelmäßigen Abholen von E-Mail), erfolgt eine häufige Einwahl in das Internet und das erhöht die Telefonkosten.

Internetverbindung und lokales Netzwerk

Bei jeder Internetverbindung besteht eine ganz normale TCP/IP-Verbindung zwischen dem lokalen Rechner und einem Rechner beim Internetprovider. Als Nameserver wird normalerweise der DNS-Server des Internetproviders automatisch konfiguriert und das Netzwerk wird gleichflls automatisch so konfiguriert, dass die Verbindung zum Internetprovider für alle TCP/IP-Daten verwendet wird, die nicht für den lokalen Rechner bestimmt sind. Das ist korrekt, denn normalerweise ist der lokale Rechner kein DNS-Server und normalerweise hat der lokale Rechner keine anderen Netzwerkverbindungen, so dass alle nicht lokalen TCP/IP-Daten den Internetzugang betreffen.

Daher sind Netzwerkprobleme mit der TCP/IP-Verbindung zum Internetprovider in der Regel ausgeschlossen, wenn es lokal nur einen Rechner gibt (Ausnahmen gibt es, wenn z. B. eine Firewall so konfiguriert wurde, dass keine Daten übertragen werden können).

T-DSL und ADSL in Deutschland

Um T-DSL bzw. ADSL zu konfigurieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie zuerst Ihre Netzwerkkarte: Starten Sie das entsprechende YaST2-Modul unter 'Netzwerk/Basis' → 'T-DSL' bzw. 'ADSL'.

   Alternativ können Sie im Office-Server Assistenten (siehe Piktogramm auf dem Desktop mit dem Namen `SLOS`) die T-DSL- bzw. ADSL-Piktogramme anklicken und danach 'Netzwerkkonfiguration' aufrufen.

   Wählen Sie in der Netzwerkkonfiguration den Schaltknopf 'Hinzufügen' aus. YaST2 zeigt Ihnen die erkannten Netzwerkkarten an. Wählen Sie Ihre Netzwerkkarte aus. Ein Dialog öffnet sich aus dem Sie den Menüpunkt 'Konfiguration der statischen Adresse' aufrufen und geben Sie eine IP-Adresse aus einem nicht vorhandenen Netz ein (Vorschlag: `192.168.22.1`, Netzmaske `255.255.255.0`). Nameserver und Routingeinträge brauchen nicht verändert zu werden.

   Schließen Sie den Dialog mit 'Beenden' ab.

2. Als nächsten Schritt konfigurieren Sie den DSL-Zugang, welchen im nachfolgenden Text beschrieben ist.

Für Ihre DSL–Konfiguration benötigen Sie folgende Daten: Anschlusskennung, T–Online–Nummer (für T–DSL), Mitbenutzerkennung und Ihr persönliches Kennwort. Entnehmen Sie die Informationen Ihrem T–DSL–Anmeldeschreiben. Das ADSL-Modul ist nur für den PPPoE ADSL-Zugang geeignet, der in Deutschland normalerweise verwendet wird. Der Standard für die Ethernetkarte ist `eth1`. Allgemein empfiehlt es sich, bei mehr als 5 Personen, den Timeout deutlich höher als 60 Sekunden (z. B. auf 360 Sekunden) einzustellen. Der allgemeine Zugriff beschleunigt sich merklich, da nicht mehr für jeden Zugriff die Verbindung erneut aufgebaut werden muß.

T-DSL oder ADSL werden nach der Konfiguration automatisch als Standard zur Interneteinwahl festgelegt. Sie können Ihren DSL–Internetzugang mit kinternet bequem steuern. Wenn Sie noch andere Internetzugänge haben und diese auch nutzen möchten (z. B. ISDN), können Sie in kinternet auswählen, mit welchem Provider Sie ins Internet möchten.

Zusätzlich können Sie in den Konfigurationsmasken zu T-DSL und ADSL durch Anklicken des Buttons 'Firewall aktivieren...' festlegen, ob Sie die Personal Firewall aktivieren möchten. Damit wird Ihr Rechner bei der Einwahl gegen Verbindungen von außen gesperrt und damit vor Angriffen geschützt.

Wenn Sie 'Dial on demand' aktivieren, dann wird z. B. nach der Eingabe einer externen URL im Browser oder beim Senden und Abholen von E–Mail die Internet–Verbindung automatisch aufgebaut. Nur wenn Sie eine so genannte Flatrate (Pauschaltarif) für den Internetzugang haben, ist 'Dial on demand' empfehlenswert. Mit 'Beenden' schließen Sie den Vorgang ab.

Hinweis

Wenn Sie keine Flatrate haben, sollten Sie 'Dial on demand' nicht verwenden, weil sonst durch Prozesse, die im Hintergrund ablaufen (z. B. zum regelmäßigen Abholen von E–Mail), eine häufige Einwahl in das Internet stattfindet und das kann teuer werden.

Hinweis

Um 'Dial on demand' nutzen zu können, müssen Sie bei Einzelplatzsystemen auf jeden Fall DNS (Nameserver) konfigurieren. Die meisten Provider unterstützen heute dynamische DNS-Vergabe, d. h. bei jedem Verbindungsaufbau wird eine andere IP-Adresse der Nameserver übergeben. Dennoch muss in Ihrem Einzelplatzsystem in diesem Dialog ein Platzhalter für einen DNS-Server eingetragen werden. Gut geeignet ist z. B. `192.168.22.99` . Falls Sie den Nameserver nicht dynamisch zugewiesen bekommen, oder Probleme auftreten, müssen Sie hier die IP–Adressen der Nameserver Ihres Providers eintragen.

Hinweis

Dial on demand besitzt drei Stati: 'Abgeschaltet', 'Eingeschaltet' und 'Abgebaut'; es funktioniert nur, wenn dies auf 'Abgebaut' eingestellt wurde.

Nach dem Konfigurieren von KInternet ist der Status auf 'Abgeschaltet'. Mit Kinternet oder unter der URL `http://server1.office/internet` können Sie den Status ändern. Bei Problemen hilft es, die Dial on Demand Verbindung per Hand nochmals einschalten.

Hinweis

ISDN

Wenn Ihre ISDN–Karte automatisch erkannt wurde, erscheint ein Dialog, in dem Sie die 'Auswahl des ISDN–Protokolls' treffen. Hierbei gilt 'Euro-ISDN (EDSS1)' als Standard (vgl. weiter unten Fall 1 und 2a). Bei '1TR6' handelt es sich um ein Protokoll für ältere bzw. große Telefonanlagen (vgl. unten Fall 2b). Für die USA gilt 'NI1'. Falls die automatische Erkennung fehlschlägt, wählen Sie zunächst die richtige ISDN–Karte aus (siehe Abb. 5.1 auf Seite 54). Geben Sie dann das ISDN-Protokoll an und schließen Sie mit 'Weiter' ab. In der nachfolgenden Maske bestimmen Sie Ihr Land und Ihren Provider. Bei den hier aufgelisteten Anbietern handelt es sich um „Call–by–Call"–Provider.

Achtung

Bei „dial on demand“ (d. h. Wählautomatik steht auf ‘automatisch’) ist nur ein Provider auswählbar.

Achtung

Wenn Sie Ihren Provider in der Liste nicht finden, dann finden Sie hinter ‘Neu’ eine Eingabemaske ‘ISP–Parameter’, mit deren Hilfe Sie einem Provider konfigurieren können. Bei ‘ISDN-Typ’ ist ‘ISDN SyncPPP’ der Standard. Bei ‘Name für die Verbindung’ geben Sie den Namen des Providers ein (z. B. T-Online) und dann dessen Telefonnummer. Die Telefonnummer darf keinerlei Trennungen wie Komma oder Leerzeichen enthalten. Geben Sie außerdem den Benutzernamen und das Passwort ein, das Sie von Ihrem Provider erhalten haben.

Hinweis

Da sich Providerdaten relativ schnell ändern, kann es vorkommen, dass die in YaST gespeicherten Daten inzwischen ungültig sind. Probieren Sie einfach verschiedene der angegebenen Provider aus.

Hinweis

Weiter geht es mit den Parametern für eine ISDN-Verbindung. Hier erfordern folgende Situationen unterschiedliche Angaben für die ‘Eigene Telefonnummer’:

1. Die ISDN-Karte ist direkt am NTBA (Telefondose der Telekom) angeschlossen: Es gibt eine so genannte „MSN“ – das ist eine der Telefonnummern (ohne Vorwahl eingeben!), die man von der Telekom für diesen Anschluss bekommen hat.

2. Die ISDN-Karte ist an einer Telefonanlage angeschlossen:

   (a) Das Protokoll der Telefonanlage für die internen Anschlüsse ist bei „kleinen“ Telefonanlagen normalerweise Euro-ISDN/EDSS1. Diese Telefonanlagen haben einen internen S0–Bus und in der Telefonanlage sind MSNs gespeichert. Die Werte sind vom Hersteller abhängig und finden sich in der Dokumentation der Telefonanlage. Irgendeine der gemäß Telefonanlage möglichen MSNs sollte funktionieren, sofern für diese MSN der Zugriff nach außen freigeschaltet ist. Zur Not funktioniert eventuell auch eine einzelne Null.

   (b) Bei „großen“ Telefonanlagen ist das Protokoll für die internen Anschlüsse normalerweise 1TR6. Die MSN heißt hier „EAZ“ und ist üblicherweise die Durchwahl. Für die Linux-Konfiguration ist normalerweise nur die letzte Ziffer der EAZ einzutragen. Eventuell funktioniert auch hier nur eine einzelne Null.

Im Folgenden entscheiden Sie sich für einen Wählmodus: ‘Manuell’, ‘Automatisch’ oder ‘Aus’. Wählen Sie am besten ‘Manuell’, dann können Sie sich später bequem per kinternet in das Internet einwählen. Durch einen Klick auf das

Steckersymbol in der Kontrollleiste unten rechts wählen Sie sich ins Internet ein. Durch einen weiteren Klick beenden Sie die Verbindung.

Alternativ können Sie in der Shell den Befehl aufrufen:

```
/usr/sbin/isdnctrl dial ippp0
```

zur Einwahl und mit

```
/usr/sbin/isdnctrl hangup ippp0
```

legen Sie wieder auf.

Hinweis

Vorsicht mit dem Wählmodus 'Automatisch' – vgl. Hinweis zu 'Dial on demand' auf S. 51.

Hinweis

Ferner können Sie einstellen, nach wie vielen Sekunden „Leerlauf" die Verbindung automatisch getrennt werden soll. 60 Sekunden sind hier ein guter Wert. In diesem Zusammenhang steht auch 'ChargeHUP', welches bei Aktivierung bewirkt, dass dieses automatische Auflegen erst vor der nächsten zu zahlenden Gebühreneinheit erfolgt. Diese Option funktioniert jedoch nicht mit jedem Provider.

Es empfiehlt sich dringend, den Punkt 'ISDN-System beim Booten initialisieren' anzuwählen, damit die benötigten Treiber geladen werden. Dadurch wird noch keine Internet–Verbindung aufgebaut. Zudem haben Sie die Möglichkeit, eine „Firewall" zu aktivieren. Damit lehnt Ihr Rechner Verbindungsanfragen von außen ab, wobei Sie aber das Netzwerk weiterhin wie gewohnt benutzen können. Beachten Sie, dass es zwei unterschiedliche Firewall–Pakete gibt: Die SuSEfirewall und die Personal Firewall. Die Personal Firewall ist im Gegensatz zur SuSEfirewall nicht konfigurierbar – einzig der Name des Netzwerkinterface (`ippp0`, `eth0` usw.), auf welchem ankommende Pakete abgewiesen werden sollen, kann angegeben werden.

Unter 'IP–Einstellungen' sollten Sie die von YaST2 vorgeschlagenen Adressen einfach übernehmen. Die Punkte 'Dynamische IP–Adressenvergabe' und 'Dynamische DNS–Vergabe' sorgen dafür, dass während der Verbindung die vom Provider zugewiesene IP–Adresse und der Name–Server übermittelt werden, was im Normalfall nötig ist. Unter 'Rückruf–Einstellungen' sollte 'Rückruf nicht konfiguriert' angewählt sein. Die anderen Möglichkeiten sind – zumindest bei privatem Gebrauch – nicht relevant.

Mit 'Weiter' bzw. 'Beenden' schließen Sie die Konfiguration ab.

Modem

Normalerweise sind Firmen heute über DSL, ISDN oder eine Standleitung mit dem Internet verbunden. Trotzdem besteht beim SuSE Linux Office Server die

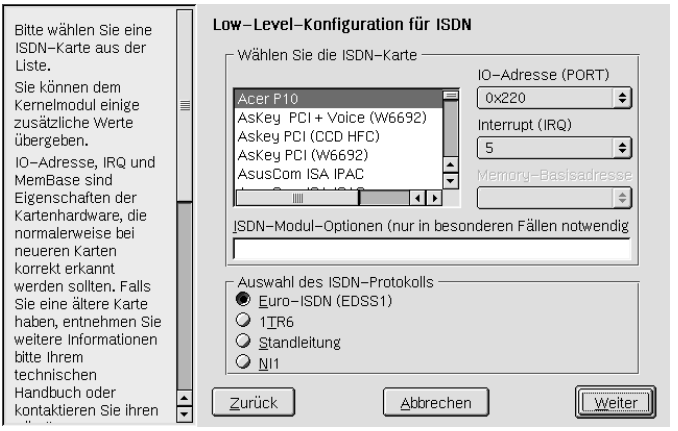


Abbildung 5.1: *YaST2: ISDN–Konfiguration*

Möglichkeit, die Einwahl über ein Modem zu realisieren (Abb. 5.2). Auf die Konfiguration soll hier nicht näher eingegangen werden. Sie ist größtenteils intuitiv und geschieht analog den Einstellungen der ISDN-Konfiguration im Abschnitt *ISDN* auf Seite 51. Nur im Menü 'Details' finden Sie Einstellungen zur Baudrate und Initialisierungs–Strings für das Modem, wo Sie Änderungen vornehmen können, wenn Sie sich damit auskennen. Im Allgemeinen ist dies jedoch nicht nötig. Hier sollten Sie nur dann Änderungen vornehmen, wenn Ihr Modem nicht automatisch erkannt wurde und für die Datenübertragung speziell eingestellt werden muss. Dies ist vor allem bei so genannten „ISDN–Terminaladaptern" der Fall.

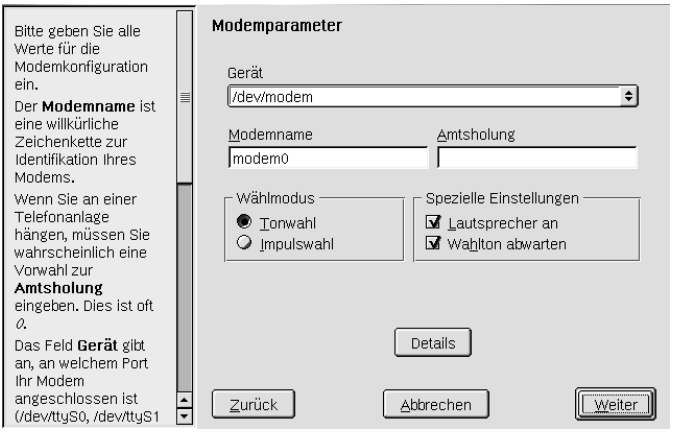


Abbildung 5.2: *YaST2 Modemkonfiguration*

Einrichten eines Printservers

Wie richtet man einen Printserver ein? Welche Dinge muß man beachten? Diese und andere Fragen beantwortet das vorliegende Kapitel.

Die Problematik der GDI-Drucker

Am Markt befinden sich zahlreiche Drucker, die mit der Beschriftung „for Windows“ versehen sind; eine andere häufige Bezeichnung ist „GDI-Drucker“. Derartige Geräte lassen sich oftmals gar nicht oder sind nur eingeschränkt unter Linux benutzen; sehen Sie bitte in der Hardwaredatenbank unter `http://cdb.suse.de/` nach, oder fragen Sie Ihren Händler.

Bei reinen GDI-Druckern verzichtet der Hersteller auf ein Standardprotokoll und spricht den Drucker direkt mit den Steuerimpulsen des speziellen Modells an. Es muss jedoch gesagt werden, dass es Drucker gibt, die zusätzlich zum GDI-Modus eine „richtige“ Druckersprache verstehen.

Drucker einrichten

Sie können mit YaST2 lokale und Netzwerkdrucker hinzufügen und einrichten. Klicken Sie dazu im Startfenster auf ‘Drucker’. YaST2 lädt nun die nötigen Einstellungen für die Druckerkonfiguration (Abb. 6.1).

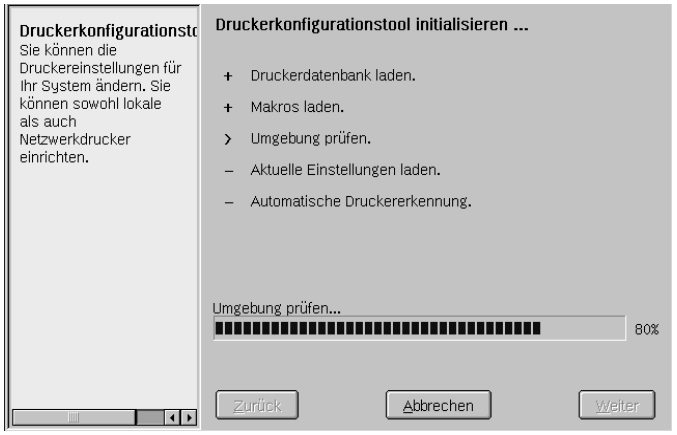


Abbildung 6.1: *YaST2: Initialisieren des Druckerkonfigurationstools*

Danach wird eine Liste der bisher an Ihrem Rechner oder in Ihrem Netzwerk angeschlossenen bzw. verfügbaren Drucker angezeigt. Klicken Sie nun auf ‘Hinzufügen’, können Sie wählen, ob Sie einen lokalen Drucker, einen Drucker aus dem Linux-Netzwerk oder aus einem anderen Netzwerk (Novell oder Samba) installieren möchten (Abb. 6.2 auf der nächsten Seite). Wählen Sie die gewünschte Kategorie und klicken Sie auf ‘weiter’.

Wollen Sie einen Drucker, der in Ihr Netzwerk eingebunden ist, einrichten, müssen Sie einen Druckserver eintragen. Mit Klick auf den Doppelpfeil neben dem

Eingabefeld erhalten Sie eine Liste der verfügbaren Rechner- und Druckernamen. Wenn Sie einen Druckserver bzw. Netzwerkdrucker benutzen wollen, der nicht in der Liste steht, müssen Sie seinen Namen bzw. seine IP-Adresse kennen. Haben Sie einen Drucker ausgewählt oder eingetragen, können Sie mit 'Test' überprüfen, ob es sich überhaupt um einen Drucker bzw. Druckserver handelt und ob dieser auch erreichbar ist. Wurde der Druckserver ordnungsgemäß gefunden, fordert Sie YaST2 im darauf folgenden Fenster auf, einen Namen anzugeben; wurde kein Druckerserver gefunden, erscheint eine entsprechende Fehlermeldung.

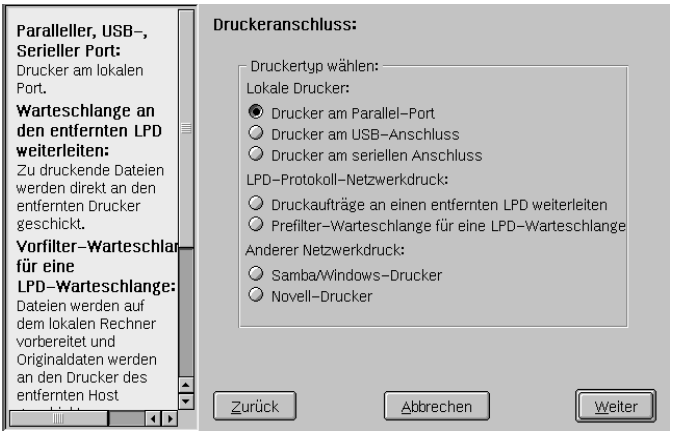


Abbildung 6.2: *YaST2: Auswählen des Druckertyps*

Die Einbindung eines Druckers aus einem Samba- oder einem Novell-Netzwerk funktioniert analog. Sie müssen wieder einen Druckserver angeben oder aus der Liste auswählen. Der Unterschied zum Linux-Netzwerk besteht in der Nutzerkennung, die Sie in diesem Fall kennen und eingeben müssen.

Wollen Sie einen lokalen Drucker an Ihrem Parallelport anschließen, wählen Sie nach 'Hinzufügen' den Punkt 'Drucker am Parallel-Port' und klicken Sie auf 'Weiter'. Jetzt wählen Sie den Parallelport-Anschluss. Mit 'Test' können Sie überprüfen, ob der Drucker ordnungsgemäß angeschlossen ist.

War der Test erfolgreich, erhalten Sie im nächsten Fenster eine Liste zur Zeit im Handel erhältlicher Drucker. Wählen Sie Ihr Modell aus. Zu jedem Drucker erhalten Sie über der 'Info'-Button Informationen über die Unterstützung durch Linux und wo Sie im Falle von GDI-Druckern eventuell Linuxtreiber erhalten. Die Einbindung von lokalen Druckern an einer seriellen oder einer USB-Schnittstelle läuft analog.

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 von Samba benutzte SMB-Protokoll ist ursprünglich eine Entwicklung von Microsoft und wurde auf Initiative von IBM der Öffentlichkeit zugänglich gemacht. Über SMB können auch Rechner anderer Betriebssysteme mit Rechnern in einem Microsoft-Domain-Netz Kontakt kommunizieren. Samba setzt SMB auf das TCP/IP-Protokoll auf, d. h. auf allen Clients im Samba-Netz muss TCP/IP installiert sein.

Linux kann – egal, ob es sich um Filesharing oder Printsharing handelt – sowohl die Client- als auch die Server-Rolle übernehmen. Über Samba können Windows-Rechner auf einen Linux-Fileserver zugreifen und dort Dateien speichern und lesen. Linux-Rechner können dagegen auch von Windows-Servern zur Verfügung gestellte Dateisysteme („Shares“) mounten und darauf lesend und schreibend zugreifen.

Der Vorzug dieser Lösung: Der Linux-Server gibt für alle diese Netzwerkzugriffe vor, selbst ein Windows-Rechner zu sein (genauer gesagt: Er gibt sich auf allen angeschlossenen Microsoft-Rechnern als Windows NT 4.2 Server aus.).

Leistungsumfang

Mit Hilfe von Samba kann ein Linux-Rechner viele Dienste aus der Microsoft-Welt anbieten. Dazu zählen unter anderem:

- Fileserver
- Printserver
- Primary Domain Controller
- Primary WINS Server
- Windows 95/98-Authentifizierung

Auf dem Samba-Server unter Linux gibt es hierfür zwei „Daemonen“ (hintergrundaktive Prozesse):

- smbd verwaltet die Ressourcen (File-, Print- und Browserdienste) und ist für die Benutzerauthentifizierung sowie den Datenaustausch über SMB zuständig
- nmbd ist für die Namensauflösung über von den Windows-Clients ausgehende NetBIOS- und WINS-Namensanfragen zuständig

Als Sambaclient, d. h. als Linux-Maschine, die auf einen Windows-Rechner zugreifen möchte, nutzt ein Linux-Client folgende Programme:

- smbclient ermöglicht den Zugang zu Windows-Dateisystemen
- smbtar dient der Speicherung von SMB-Shares auf Unix-Bandlaufwerke
- nmblookup Namensauflösung der NetBIOS-Namen
- smbpasswd Verwaltung der SMB Benutzerpasswörter
- smbstatus Auskunft über offene SMB-Verbindungen

Alle diese Programme sind Teile der *Samba-Suite* und arbeiten mehr oder weniger im Hintergrund für Sie.

Weitere Informationen

Mittlerweile gibt es zahlreiche Bücher und Webseiten, die sich mit dem Thema Samba befassen – aber auch auf Ihrem System sind eine Fülle nützlicher und interessanter Informationen zum Thema Samba vorhanden, schauen Sie unter `/usr/share/doc/packages/samba/`. Sie werden dort eine „Flut“ von Informationen finden. Unter anderem liegt unter `/usr/share/doc/packages/samba/htmldocs/using_samba/` die vollständige Version des „Using Samba“-Buchs von Robert Eckstein, David Collier-Brown und Peter Kelly.

Aber auch die Webseiten des Samba-Projekts haben einiges zu bieten:

`http://de.samba.org/samba/samba.html` ist der offizielle Mirror der Sambaseiten. Im Unterverzeichnis `http://de.samba.org/samba/docs/` liegt ein Überblick über die wichtigsten (aktuellen) Informationsquellen (inklusive Manpages) zum Thema.

Netzwerkdienste – Hinter die Kulissen geschaut

Dieses Kapitel soll Ihnen einige weitere Informationen über die Netzwerkdienste vermitteln, die im Verborgenen für Sie arbeiten, deren Funktion aber unverzichtbar für das Funktionieren Ihres gesamten Netzes ist.

Grundfunktionen

Dieser Abschnitt geht kurz auf die elementarsten Dienste ein, die Sie zum Arbeiten im Netz benötigen:

Namensauflösung – Der Domain Name Service (DNS) verwaltet Namen und IP-Adresse Ihrer lokalen Rechner und holt Namensinformationen aus dem gesamten Internet

Konfiguration der Netzwerkinterfaces – Die Vergabe von IP-Adressen für Ihre internen Clients wird Ihnen abgenommen – per DHCP (engl. *Dynamic Host Configuration Protocol*)

Verwaltung und Verteilung von Systemdateien – Wichtige Benutzerdaten können in einer zentralen Datenbank verwaltet und gewartet werden. Der Export erfolgt über NIS (engl. *Network Information System*)

Domain Name Service

DNS sorgt dafür, dass Sie sich keine IP-Adressen merken müssen: Mit Hilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden, umgekehrt aber auch eine Name einer IP-Adresse. Unter Linux kann diese Umwandlung üblicherweise von einer speziellen Software namens bind erledigt werden. 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 unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an:

```
     laurent.suse.de
Rechnername.Domain
```

Ein vollständiger Name – „fully qualified domain name“, kurz FQDN – 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, anderswo immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. In der Tabelle 7.1 auf der nächsten Seite sind verschiedene TLDs ohne Anspruch auf Vollständigkeit aufgeführt, um Ihnen einen ersten Eindruck zu geben.

`.com`	(engl. *Commercial*) - Firmen in den USA.
`.edu`	(engl. *Educational*) - Schulen, Universitäten und andere nichtkommerzielle Bildungseinrichtungen der USA.
`.gov`	(engl. *Government*) - Staatliche Einrichtungen und Regierungsstellen der USA.
`.org`	(engl. *Organizational*) - Nichtkommerzielle Organisationen der USA.
`.de`	Rechner in Deutschland.
`.at`	Rechner in Österreich.

Tabelle 7.1: *Verschiedene Top Level Domains*

Wie Sie sehen, erhalten die Rechner in Deutschland üblicherweise de, Rechner in Österreich at und Rechner in der Schweiz die TLD ch.

An der Spitze der Hierarchie befinden sich die so genannten „Root-Nameserver". Diese Root-Nameserver verwalten die Top Level Domains. Die Root-Nameserver werden vom Network Information Center kurz NIC verwaltet. Der Root-Nameserver kennt jeweils die 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 können Sie unter `http://www.internic.net` nachschlagen.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt gemacht werden. Die Konfiguration eines Nameservers können Sie komfortabel mit Hilfe von YaST2 erledigen. Falls Sie eine Einwahl über Modem vornehmen, so kann es sein, dass Sie keinen Nameserver manuell konfigurieren müssen. Das zur Einwahl verwendete Protokoll liefert die Adresse des Nameservers während der Einwahl mit.

Betrieb des Nameservers BIND

Der Nameserver BIND8 ist für Ihren Server bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann.

Mit dem „von Haus aus" mitgelieferten Konfigurationsdateien kennt Ihr Nameserver schon alle Rechner im lokalen Netz. Er kann jedem Rechner im gesamten Netz mitteilen, wie die IP-Adresse oder der volle Name seines „Kollegen" heißt.

Nachdem Sie bei der Installation die IP-Adresse des Nameservers Ihres Providers in YaST2 Maske Konfiguration des Hostnamens & Nameservers eingetragen haben, ist Ihr Nameserver auch in der Lage, die übrigen Adressen des restlichen Internets zügig aufzulösen.

Dass Ihr Nameserver funktioniert, merken Sie daran, dass Sie mit dem Programm host sowohl externe als auch interne Adressen auflösen können.

Weitere Informationen

- Dokumentation zum Paket `bind8`: `file:/usr/share/doc/packages/bind8/html/index.html`.
- Eine Beispielkonfiguration finden Sie unter: `/usr/share/doc/packages/bind8/sample-config`
- Die 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`).

DHCP

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 selbstständig nach den Vorgaben des DHCP-Servers.

Dabei ist es sowohl möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte zu identifizieren und ständig mit denselben Einstellungen zu versorgen, als auch 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, über dem die jeweils aktuelle Uhrzeit abrufbar ist oder ein Printserver.

Schließlich können über das DHCP-Protokoll auch ganze Clients („diskless clients“) ohne Festplatte ihr Betriebssystem und alle Konfigurationsdateien über das Netz beziehen. Allerdings ist das ein Kapitel für sich …

Weitere Informationen

Zusätzliche Informationen zu DHCP finden Sie auf den Webseiten des *Internet Software Consortiums* unter: `http://www.isc.org/products/DHCP`

Hinweise, die in konkreten Situationen Rat bieten, finden Sie auf den entsprechenden Manpages:

- Allgemeines zum DHCP-Server Daemon:
  man dhcpd
- Informationen zu seiner Konfiguration:
  man dhcpd.conf und man dhcpd.leases
- Übergabe-Optionen an die DHCP-Clients:
  man dhcp-options

NIS

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass z. B. Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonieren. Das Netzwerk soll für den Anwender transparent sein. Egal an welchem Rechner er arbeitet, er 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 7 auf der nächsten Seite beschrieben.

NIS (engl. *Network Information Service*) kann als Datenbankdienst verstanden werden, der den Zugriff auf Informationen wichtiger Systemdateien netzwerkweit ermöglicht. Die wichtigsten Einsatzfelder findet NIS bei der Verteilung folgender Dateien:

/etc/passwd – auch wenn diese Datei aus (historischen) Gründen „Passwort" im Namen trägt, werden hier nur Daten über Login, Benutzernummer, Gruppenzugehörigkeit (engl. *Group-ID*), Homeverzeichnis und Standardshell eines Benutzers verwaltet.

/etc/shadow – hier befinden sich die Benutzerpasswörter in verschlüsselter Form. Außerdem ist in dieser Datei festgehalten, wie viele Tage ein Passwort gültig ist.

/etc/group – ist eine Auflistung aller netzweit vorhandenen Gruppen samt „Group-ID" und optional auch Angabe der zugehörigen Benutzer.

Der Vorteil dieser zentralistischen Lösung: Fast alle systemwichtigen Daten müssen nur an einer einzigen Stelle im Netz gewartet werden. Mögliche Änderungen sprechen sich mittels NIS von allein herum, ohne dass sie auf jedem Rechner einzeln aktualisiert werden müssten.

Weitere Informationen zu NIS

Neben den Informationen, die Sie auf Ihrem eigenen System unter `/usr/share/doc/packages/ypbind/` finden, oder den Manpages steht Ihnen das „Linux NIS(YP)/NYS/NIS+ HOWTO“ unter `http://www.linuxdoc.org/HOWTO/NIS-HOWTO-index.html` zur Verfügung.

File– und Print-Service

Zentrale Aufgabe Ihres Servers ist die Verwaltung von Dateien bzw. Verzeichnissen und Druckaufträgen unabhängig vom Betriebssystem der angeschlossenen Clients. Linux-Clients werden über NFS (das „Network File System“) zentral mit Dateien und Verzeichnissen versorgt. Druckaufträge können vom angeschlossenen Netzwerkdrucker bearbeitet werden.

Die Windows-Clients stehen über Samba mit Ihrem Linux-Server in Verbindung, um Dateisysteme („Shares“) zu mounten und den angeschlossenen Netzwerkdrucker zu nutzen.

NFS – verteilte Dateisysteme

Wie bereits in Abschnitt *NIS* auf der vorherigen Seite erwähnt dient NFS neben NIS dazu, ein Netzwerk für Anwender transparent zu machen. Durch NFS ist es möglich, Dateisysteme im Netz zu verteilen. Unabhängig davon, an welchem Rechner im Netz ein Anwender arbeitet, kann er so stets die gleiche Umgebung vorfinden. Die Nutzer Ihres Servers können so per NFS an einem beliebigen Linux-Client in Ihrem Netz Zugang zu ihrem persönlichen Homeverzeichnis haben, ohne dass dieses physikalisch auf der entsprechenden Maschine vorhanden sein müsste.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS-Server und NFS-Clients. Allerdings kann ein Rechner beides sein, d. h. er kann 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

Dateisysteme von einem NFS-Server zu importieren, ist sehr einfach. Einzige Voraussetzung ist, dass der RPC-Portmapper gestartet wurde, was nach der Installation des Servers automatisch der Fall ist. 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

Ein Rechner, der Dateisysteme exportiert, wird als NFS-Server bezeichnet. Auf einem NFS-Server müssen die folgenden Netzwerkserver gestartet werden:

- RPC-Portmapper (portmap)
- 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 Daemonen 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 benötigt, in der steht, welche Rechner wie darauf zugreifen dürfen. Alle Unterverzeichnisse eines exportierten Verzeichnisses werden automatisch ebenfalls 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, so 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.

`ro`	Dateisystem wird nur mit Leserechten exportiert (Vorgabe).
`rw`	Dateisystem wird mit Schreib- und Leserechten exportiert.
`root_squash`	Diese Option bewirkt, dass der Benutzer `root` des angegebenen Rechners keine für `root` 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 `nobody` zugewiesen werden (Vorgabe).

Tabelle 7.2: *Fortsetzung auf der nächsten Seite…*

`no_root_squash`	Rootzugriffe nicht umsetzen; Rootrechte bleiben also erhalten.
`link_relative`	Umsetzen von absoluten, symbolischen Links (solche, die mit `'/'` beginnen) in eine entsprechende Folge von `'../'`. 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 nfsd angewiesen, eine Umsetztabelle für die User-IDs zu erstellen. Voraussetzung dafür ist jedoch die Aktivierung des Daemons ugidd.

Tabelle 7.2: *Zugriffsrechte für exportierte Verzeichnisse*

Die `exports`-Datei kann beispielsweise aussehen wie Datei 1.

```
#
# /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 1: *Die Datei /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
```

Sicherheit

Firewall

Ihr Server ist mittels eines einfach zu handhabenden Paketfilters vor Angriffen aus dem Internet geschützt. Die Personal Firewall arbeitet praktisch wartungsfrei und ist nach einem einzigen Konfigurationsschritt bereits einsatzbereit. Im aktiven Zustand öffnet sie für das interne Netz Verbindungen ins Internet, lässt aber im Gegenzug keinen Verbindungsaufbau von außerhalb zu.

Da der SuSE Linux Office Server als reiner File-/Druckserver in einem privaten Netz konzipiert ist und keinerlei Services (FTP, HTTP etc.) im Internet anbietet, ist er mit dieser Lösung einfach, aber sehr wirkungsvoll geschützt.

Ist Personal Firewall aktiviert, werden alle Datenpakete abgelehnt, die zu einer der drei folgenden Gruppen gehören:

- UDP-Pakete
- versuchte TCP Anfragen von außerhalb
- ICMP Redirect Subtypes (mittels ICMP Redirects könnte Ihr Rechner dazu gebracht werden, seine Routingtabelle zu ändern)

Personal Firewall wird nur über eine einzige Variable konfiguriert, die in der Datei `/etc/rc.config.d/security.rc.config` festgehalten wird.

Die zu konfigurierende Variable heißt `REJECT_ALL_INCOMING_CONNECTIONS`. Sobald hierfür eine sinnvolle Konfigurationsoption gewählt wurde, startet die Firewall nach Abschluss der Konfigurationsarbeiten und Neustart des Netzwerkes automatisch.

Folgende Einstellungen sind möglich:

`no`	Wird "no" gesetzt oder bleibt dieses Feld leer, wird Personal Firewall nicht aktiv. Alle eingehenden Verbindungen werden angenommen. Es findet keine Filterung statt.
`yes`	Personal Firewall wirkt auf alle Interfaces außer "lo", das Loopbackinterface, "localhost". So werden auch Verbindungen geblockt, die aus dem eigenen Netz stammen. Die einzigen Pakete, die angenommen werden, sind solche, die an "localhost" gerichtet sind.
`iface`	Hier werden explizit (und durch Leerzeichen getrennt) diejenigen Interfaces angegeben, auf denen eingehende Verbindungen geblockt werden sollen.

Tabelle 7.3: *Fortsetzung auf der nächsten Seite…*

`masq`	Pakete, die den Rechner erreichen, aber nicht für eines seiner Interfaces bestimmt sind, werden vor der Weiterleitung entsprechend maskiert. Hier wird der Name des Interfaces angegeben, über das Pakete maskiert nach außen gelangen und an dem alle eingehenden Verbindungen abgelehnt werden sollen. (Interface Name und "masq" sind durch Leerzeichen voneinander zu trennen.)

Tabelle 7.3: *Konfiguration der Personal Firewall*

Bei der Einrichtung Ihres Internetzugangs über Modem oder ISDN werden Sie in der YaST2-Maske 'Verbindungsparameter' beziehungsweise 'Parameter für eine ISDN-Verbindung' gefragt, ob die Firewall aktiviert werden soll. Wählen Sie diese Option an, kommt dies einem Eintrag "masq Interface Name" in die Datei `/etc/rc.config.d/security.rc.config` gleich. Per Masquerading werden alle Netzwerkpakete, die von internen Clients für das Internet bestimmt sind, nicht mit der Netzwerkadresse ihres Ursprungs versehen, sondern erscheinen nach außen hin so, als kämen sie von dem im Internet bekannten Netzwerkinterface Ihres Servers. So wird zum einen das interne Netz zusätzlich dadurch geschützt, dass die einzelnen Clients nur lokal bekannt sind, zum anderen wird so Adressraum für Internetadressen eingespart. Sollten Sie die Firewall nicht aktivieren, ist der Netzwerkverkehr über Ihre Internetanbindung völlig ungefiltert (gleichbedeutend mit einem "no" in der Konfigurationsdatei).

Proxy-Server: Squid

In den folgenden Abschnitten wird erläutert, wie das Caching von Webseiten mit Hilfe eines Proxy-Servers funktioniert und welchen Nutzen Squid für Ihr System hat. Squid ist der am weitesten verbreitete Proxy-Cache für Linux/UNIX-Plattformen.

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 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.

Squid und der SuSE Linux Office Server

Squid läuft bereits beim ersten Start Ihres Systems, ohne dass von Ihrer Seite eine Aktion erforderlich wäre. Die Grundfunktionen, die er bereitstellt, ohne dass Sie sich darum kümmern müssten, sind folgende:

Caching von Webseiten – Alle Clients aus dem internen Netz können vom Caching der angeforderten Webseiten profitieren.

Zugangsbeschränkung auf das eigene Netz – die Konfiguration des Squid ist so ausgelegt, dass nur lokale Clients Zugang zu seinen Diensten haben.

Cache Management – Mittels des Programms Cache-Manager können bei gleichzeitig eingerichtetem Webserver Apache auf Ihrem Server jederzeit aktuelle Statistiken darüber angefordert werden, in welcher Größenordnung Squid Speicher zum Caching benötigt.

Sie können diese Grundfunktionalitäten natürlich noch um manch andere nützliche Funktion ergänzen. Dazu verändern Sie die Konfigurationsdatei `/etc/squid.conf` entsprechend. Nützliche Erweiterungen waren z. B. :

Verfeinerte Zugangsregeln zum Internet – mittels ACLs (engl. *Access Control Lists*) können Sie den Internetzugriff für bestimmte Benutzergruppen beispielsweise auf bestimmte Tageszeiten beschränken. Hier ein Beispiel:

```
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 localhost
http_access allow lehrer
http_access allow studenten mittags
http_access deny all
```

Datei 2: *Ausschnitt aus einer* `squid.conf` *mit Zugangsbeschränkung*

Mit dieser Einstellung kann die Benutzergruppe `lehrer` jederzeit uneingeschränkt auf das Internet zugreifen, die Benutzergruppe `studenten` nur um die Mittagszeit und alle anderen Benutzer überhaupt nicht.

Internetzugang nur für authentifizierte Benutzer – Wollen Sie den Internetzugang für Ihre Benutzer nur nach vorheriger Authentifizierung zulassen, sollten Sie ein Authentifizierungsprogramm, beispielsweise pam_auth, einbinden, das jeden Benutzer nach seinem Login und Passwort fragt:

```
authenticate_program /usr/sbin/pam_auth
...
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Datei 3: *Proxy-Authentifizierung in* `squid.conf`

Zusätzlich muss jetzt noch eine ACL aufgestellt werden, damit nur Clients mit gültigem Login surfen dürfen. Alternativ kann auch das `REQUIRED` durch eine Liste von erlaubten Benutzernamen ersetzt werden.

Identitätsabfrage – Die entsprechende Software vorausgesetzt können Sie Squid auch so konfigurieren, dass er per Ident-Abfrage die Identität des jeweils surfenden Benutzers abfragt. Unter Linux können Sie hierzu das Programm pidentd verwenden, für Windows-Clients bekommen Sie die entsprechende Software frei über das Internet.

Sperrung unerwünschter URLs – Über geschickt aufgestellt ACLs und in Verbindung mit Proxy-Authentifizierung können Sie mit einem separaten Programm, z. B. SquidGuard unerwünschte URLs für bestimmte Benutzer sperren. *Inhalte* oder bestimmte in HTML eingebettete *Skriptsprachen* (JavaScript, VBscript) können aber weder von Squid noch von SquidGuard in irgendeiner Weise gefiltert, zensiert oder gesperrt werden.

Finetuning – Mit etwas Erfahrung können Sie die Leistungsfähigkeit Ihres Proxies noch verbessern, indem Sie die gewünschte Cachegröße und die Speicherkapazität Ihres Systems aufeinander abstimmen. Auch durch die Verwendung mehrerer Caches wird Ihr System entlastet, da es dann mit anderen Caches Objekte austauschen kann.

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. Unter anderem finden sich hier Informationen zu den Themen „Verwendung mehrerer Caches“, „Optimierung des Caches“, „Aufstellen von ACLs“ und „Aufbau der Konfigurationsdatei“ (hierzu besonders empfehlenswert: `http://squid.visolve.com/squid24s1/contents.htm` mit ausführlichen Erklärungen zu den einzelnen Konfigurationsoptionen).

Informationen zur Verwendung eines Cache-Managers finden Sie unter: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

In diesem Zusammenhang auch interessant, die Webseite von Calamaris, einem Perl-Skript, das Cache-Berichte in HTML- oder ASCII-Format erzeugen kann: `http://Calamaris.Cord.de`

Sollten Sie Informationen über SquidGuard benötigen, hält die Homepage des Projekts eine Fülle nützlicher Dinge für Sie bereit:

- Generelle Informationen unter:
  `http://www.squidguard.org`
- Beispielkonfigurationen und Erläuterungen unter:
  `http://www.squidguard.org/config/`

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/`

Der Webserver Apache

Weitere Informationen zum Webserver Apache erhalten Sie im Abschnitt **??** auf Seite ??.

Sicherheit ist Vertrauenssache

In diesem Kapitel werden wir Ihnen einige Grundlagen zeigen und die lokale Sicherheit von Netzwerken betrachten. Einige Tipps und Tricks zum Thema Sicherheit finden Sie auch hier.

Grundlagen

Eines der grundlegendsten Leistungsmerkmale eines Linux/Unix-Systems ist der Anspruch, dass mehrere Benutzer (engl. *multi-user*) mehrere Aufgaben zur gleichen Zeit auf demselben Rechner (engl. *multi-tasking*) ausführen können. Wir erwarten von dem Betriebssystem, dass es netzwerktransparent ist, so dass wir gar nicht merken, ob die Daten oder Applikationen, mit denen wir arbeiten, lokal auf dem Rechner vor uns vorgehalten werden oder sich woanders befinden.

Die spezielle Eigenschaft, dass mehrere Benutzer an oder auf einem System arbeiten, führt zu der Notwendigkeit, dass diese Benutzer und ihre Daten auch voneinander getrennt werden können. Da in diesem Zusammenhang verschiedenartigste und nicht zuletzt auch emotionale Aspekte zum Tragen kommen, verlangt das Thema Sicherheit und Schutz von Privatsphäre eine besonders sorgfältige Zuwendung.

Den Begriff Datensicherheit gibt es schon aus der Zeit, als Computer nicht miteinander vernetzt waren. Es war schon damals vorrangig wichtig, dass die Daten bei einem Verlust oder einem Defekt der Datenträger (im Allgemeinen Festplatten) weiterhin verfügbar blieben, 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 erscheint bei nüchterner Betrachtung logisch, dass der Zugriff auf die Daten eines Rechners nur dann möglich ist, wenn die Daten überhaupt erst zur Verfügung gestellt werden. Wenn die Daten nicht einfach in einem Safe sicher geparkt werden sollen, dann geschieht der Zugriff auf unterschiedlichen Wegen:

- Jemand bedient einen Rechner und telefoniert mit dem Nutzer der Daten,
- direkt an der Console eines Rechners (physikalischer Zugriff),
- über eine serielle Schnittstelle, oder
- über ein Netzwerk.

Alle diese Fälle sollten eines gemeinsam haben: Sie sollten sich als Benutzer authentifizieren müssen, bevor Sie Zugriff auf die Ressourcen oder Daten bekommen, oder anders gesagt: Sie sollten einen Nachweis über eine Identität erbracht haben, der der Zugriff auf die angeforderten Ressourcen (Daten oder Kapazitäten) durch eine Zugriffsregel gestattet ist. Ein Webserver mag da anders geartet sein, aber Sie wollen sicherlich nicht, dass der Webserver Ihre persönlichen Daten an Dritte preisgibt. Eine SuSE-Linux Installation ließe sich mit wenigen Handgriffen dazu bringen, Sie nach dem Systemstart direkt und ohne Passwort mit Ihrer Arbeitsoberfläche zu konfrontieren, aber dieser Ansatz erscheint meistens unangemessen. Schließlich dehnen Sie durch das Einloggen Ihre Identität und Ihr Handeln auf den Rechner aus, den Sie steuern wollen. Sie würden nur in Ausnahmefällen wollen, dass jemand anders dies in Ihrem Namen tut.

Der erste Fall in der Liste ist der realischtiste von allen: 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 (die mit Computern, Betriebssystemen und Netzwerken vielleicht weniger zu tun haben) wäre es möglich, durch das geschickte Erwähnen von bruchstückhaften Kenntnissen von Gegebenheiten unterschiedlichster Art oder durch geschickte Rhetorik das Vertrauen eines Trägers von Wissen zu erschleichen, so dass dieser schrittweise mehr und mehr Information weitergibt, womöglich ohne dass das Opfer dies bemerkt. Manche Menschen sind so unvorsichtig mit ihren Äußerungen und unbewusst mit ihren Antworten, dass auch die Antworten, die sie für nicht beantwortet halten, genug Information enthalten, um Fragen immer präziser zu stellen, weil wie in einem Mosaik immer mehr Details bekannt werden. („Nein, der Herr Meier ist im Urlaub und kommt erst in drei Wochen wieder. Und im übrigen ist er nicht mein Chef, zumal er im vierten Stock sitzt und ich im dritten!“) 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 Rechnersystemem 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 herkömmliche, 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 verstaut sein - dazu kann auch eine eventuell vorhandene Netzwerkleitung oder ein Stromkabel gehören. Der Startvorgang muss abgesichert sein, denn allgemein bekannte Tastenkombinationen können den Rechner zu speziellen Reaktionen bringen. Dagegen hilft das Setzen von BIOS- und Bootloaderpasswörtern.

Serielle Schnittstellen mit seriellen Terminals sind heute zwar immer noch verbreitet gebräuchlich, werden aber kaum noch an neuen Arbeitsplätzen installiert. In Bezug auf die Art des Zugriffs ist ein serielles Terminal ein Sonderfall: Es ist keine Netzwerkschnittstelle, da kein Netzwerkprotokoll zur Kommunikation zwischen den Systemeinheiten verwendet wird. Ein simples Kabel (oder eine In-

frarotschnittstelle) 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.

Netzwerke vereinfachen den Zugriff auf Daten mit zum Teil komplexen Kommunikationsprotokollen. Das mag paradox klingen, muss aber so sein. Wenn Sie völlig ortsunabhängig sein wollen und einen Rechner fernsteuern oder Daten von ihm beziehen wollen, dann brauchen Sie abstrakte, modulare Modelle, deren Ebenen weitgehend voneinander unabhängig sind. Im täglichen Umgang mit Computern begegnen Sie ständig solchen Modellen: Modularität ist, wenn Ihr Textverarbeitungsprogramm nicht wissen muss, welche Art von Festplatte Sie haben, und Ihr E-Mail-Programm sollte sich nicht darum kümmern müssen, ob Sie nun ein Modem oder eine Ethernet-Karte haben. Teile Ihres Betriebssystems (in unserem Fall Linux) stellen Ihnen die Funktionalität mittels einer definierten Schnittstelle zur Verfügung und kümmern sich um die Details. So kann einerseits ein Textverarbeitungsprogramm oder ein Mail-User-Agent (MUA) auch auf einem Rechner mit gänzlich unterschiedlicher Hardware funktionieren, und andererseits sorgt diese Modularität dafür, dass Sie dies prinzipiell von jedem Ort der Welt aus tun können.

Aus der Sicht der Daten bedeutet dies für eine Datei und den Zugriff darauf, dass es keinen Unterschied macht, ob Sie die Datei auf der Kommandozeile öffnen oder ob dies ein Webserver macht (etwa Apache) und die Datei über ein Netzwerk auf einem Browser dargestellt wird. In beiden Fällen hat ein Benutzer die Datei mit seiner jeweiligen Berechtigung geöffnet und davon gelesen. Es geht noch weiter: Sie hätten sich auch über ein Netzwerk (etwa mit einem telnet-Programm oder, viel besser, mit einem secure shell Programm (ssh), das den Netzverkehr vollständig verschlüsselt) einloggen können und die Datei lesen können. Dennoch müssten Sie dabei mehrere Hürden überspringen: Erst einmal müssten Sie sich über das Netzwerk mit dem Rechner zu verbinden und sich authentifizieren (Ihre Identität nachweisen), und dann hätten noch die Zugriffsrechte der Datei Ihre Handlungsmöglichkeiten eingeschränkt.

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 sie da markiert, wo Daten in Pakete verschnürt werden müssen, um verschickt und zur Anwendung zu gelangen.

Lokale Sicherheit

Wie bereits erwähnt, beginnt 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. Versetzen Sie sich in die Lage eines Angreifers: So-

lange wir noch von „Lokaler Sicherheit“ sprechen, ist es die Aufgabe, die einzelnen Benutzer voneinander zu trennen, so dass kein Benutzer die Rechte eines anderen Benutzen annehmen kann. Dies gilt allgemein, im speziellen ist natürlich besonders der `root`-Account gemeint, der im System die Allmacht hat. Wenn ein Benutzer `root` wird, kann er sich ohne Passwort zu jedem lokalen Benutzer machen und überdies jede lokale Datei lesen.

Die Liste der Möglichkeiten, ein System anzugreifen, wenn man bereits Zugriff auf lokale Ressourcen mit einer Kommandozeile hat, ist recht lang.

Passwörter

Ihr Linux-System speichert die Passwörter, die Sie vergeben haben, 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 verschlüsselt das System Ihr Passwort, und jedes Mal, wenn Sie ein Passwort eingegeben haben, wird dieses 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 ist der Fall: Man nennt solche Algorithmen „Falltüralgorithmen“, weil sie nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann also 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. Sie können sich leicht ausrechnen, dass dies bei acht Buchstaben pro Passwort beträchtlich viele sind.

Mit ein Argument für die Sicherheit dieser Methode in dem 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, was nach zwei Dingen verlangt: Die verschlüsselten Passwörter dürfen 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 sind leichtes Brot für Knackprogramme, die Wörterbücher zum Raten benutzen. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für Sie eine persönliche Bedeutung haben (aber nicht so wie die Zahlenkombination Ihres Reisekoffers!), etwa die Anfangsbuchstaben der Wörter eines Satzes. Beispiel: Ein Buchtitel, „Der Name der Rose“ von Umberto Eco birgt 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 Sie ein BIOS-Passwort setzen und im BIOS ausschließlich das Booten von Festplatte erlauben.

Linux Systeme starten gewöhnlicherweise mit einem Boot-loader, 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. Verhindern Sie, dass jemand solche Optionen verwendet, während Ihr Rechner startet, indem Sie die Optionen „restricted“ und „password=irgendein_passwort“ in `/etc/lilo.conf` verwenden. Vergessen Sie nicht, das Kommando `lilo` auszuführen, wenn Sie die Datei `/etc/lilo.conf` verändert haben, und achten Sie auf die Ausgaben des Programms! Wenn Sie das Passwort vergessen, müssen Sie das BIOS-Passwort kennen und von CD booten, um den Eintrag in `/etc/lilo.conf` aus einem Rettungssystem heraus zu lesen.

Zugriffsrechte

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für die jeweilige Aufgabe zu arbeiten. Es ist definitiv nicht nötig, seine emails 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 Aktivwerdens 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. Es sei bemerkt, dass ein falsch gesetztes Attribut durchaus nicht nur bedeuten kann, dass Dateien überschrieben oder gelöscht werden könnten, sondern dass die ausgetauschten Dateien ja auch von `root` ausgeführt oder im Fall von Konfigurationsdateien von Programmen als `root` benutzt werden könnten. Damit würde ein Angreifer seine Rechte beträchtlich ausweiten können. Man nennt solche Angriffe dann Kukukseier, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kukuk 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 setuser-ID-bits (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`) von Dateien

festgelegt. Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Änderungen festhalten kann. Die Variable PERMISSION_SECURITY aus der Datei `/etc/rc.config` legt fest, welche der Dateien von den Konfigurationsprogrammen von SuSE für die Vergabe der Rechte benutzt werden soll. Diese Auswahl können Sie auch komfortabel unter dem Menüpunkt 'Sicherheit' ('Security') von YaST2 treffen. Mehr zu diesem Thema erfahren Sie direkt aus der Datei `/etc/permissions` und der manual page des Kommandos `chmod` (`man chmod`).

file race conditions

Ein Programm will eine Datei in einem Verzeichnis anlegen, das für jedermann schreibbar ist (wie `/tmp`). Es überprüft, ob die Datei bereits existiert und erzeugt die Datei, wenn sie noch nicht vorhanden war. Zwischen dem Überprüfen der Existenz und dem Anlegen der Datei vergeht aber eine kurze Zeit, in der ein Angreifer einen symbolischen Link anlegen kann, ein Zeiger auf eine andere Datei. Das Programm verfolgt dann diesen symbolischen Link und überschreibt dabei die Zieldatei mit seinen Privilegien. Dies ist ein Rennen (engl. *race*), weil für den Angreifer nur eine kurze Zeit bleibt, in der er den „symlink" anlegen kann. Dieses Rennen besteht also immer dann, wenn der Vorgang von Überprüfen und Anlegen einer Datei nicht atomisch, also unteilbar ist. Wenn das Rennen stattfindet, dann kann es von einem Angreifer auch gewonnen werden, das ist eine Frage der Wahrscheinlichkeit.

buffer overflows, format string bugs, signed/unsigned 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 manchen 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 Programmierers stehen. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Rechten (Siehe Zugriffsrechte oben) abläuft. „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 geringst möglichen Privilegien (Siehe Abschnitt über Zugriffsrechte!).

Da bei „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 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 geringst möglichen Privilegien, dann sollten Sie eher Schwierigkeiten haben, sich einen Virus unter Linux einzufangen. Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie vom 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 *in* einem Rechner voneinander zu trennen, insbesondere den Benutzer `root`. Im Gegensatz dazu soll bei der Netzwerksicherheit das ganze System gegen Angriffe vom Netzwerk geschützt werden. Obwohl man beim klassischen Einloggen eine Benutzerkennung und ein Passwort eingeben muss, ist Benutzerauthentifizierung eher Gegenstand von lokaler Sicherheit. Speziell beim Einloggen über eine Netzwerkverbindung trennen sich die Sicherheitsaspekte auf in das, was bis zur erfolgten

Authentifizierung passiert (Netzwerksicherheit) und in das, was danach folgt (lokal).

X-Window (X11-Authentifizierung)

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X11, dem Windowing-System von Unix-Systemen, gilt dies besonders eindrücklich! 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. Das Protokoll, welches zwischen der X-Applikation und dem X-Server (der lokale Prozess, der die Fenster auf der Grafikkarte zur Anzeige bringt) zur Kommunikation verwendet wird, ist recht sparsam, was Netzwerkbandbreiten angeht. Das ist durch die in den 80er Jahren, als das System entworfen wurde, zur Verfügung stehenden Bandbreiten bedingt.

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-Window 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-Window-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-Window 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. Der Client öffnet zum Anzeigen dann eine Verbindung zum sshd (secure shell daemon, das serverseitige Programm), der dann die Verbindung an den richtigen, realen X-Server durchschleust. Wenn Sie X-Clients über das Netzwerk anzeigen lassen müssen, dann sollten Sie `ssh` einmal genauer unter die Lupe nehmen. Die Manpage von `ssh` gibt weitere Auskünfte über diese Funktionalität.

Achtung

Wenn Sie den Rechner, auf dem Sie sich einloggen, nicht als sicher betrachten, dann sollten Sie auch keine X-Window-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 unpriviligierten 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 Sicherheitsmailinglisten 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 Source-Code für jedermann erhältlich ist, 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 = enlg. 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 einen 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 („gespooften“) 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 geringst nötigen Privilegien für eine Aufgabe zu benutzen. Das verringert die Chancen für ein Kukuksei 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 Recher 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-Linux-Distribution ab Version 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. Wenn Sie gar keine Dienste auf Ihrem Rechner zur Verfügung stellen wollen, dann verwenden Sie am besten die SuSEpersonal-firewall. Die Konfiguration beschränkt sich auf den Namen des Netzwerkinterface, auf welchem hereinkommende Verbindungen abgelehnt werden sollen. Nähere Informationen finden Sie in der Datei `/sbin/SuSEpersonal-firewall` und in `/etc/rc.config.d/security.rc.config`.
- 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 fingerprin
= 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 Down-

load bereit.

A

Fehlerbehebung

Fehlerbehebung

Falls Sie Probleme besitzen, kann Ihnen das Kapitel vielleicht die nötigen Hintergrundinformationen geben.

Bootdiskette erstellen

Bootdiskette unter DOS erstellen

Voraussetzung

Sie brauchen eine formatierte 3.5-Zoll-HD-Diskette und ein 3.5-Zoll-Disketten-Laufwerk, das auch bootfähig sein muss. Falls Sie unter Windows arbeiten: Starten Sie setup *nicht* in der MS-DOS-Box, sondern im MS-DOS-Modus!

Zusatzinfo

Auf der CD 1 im Verzeichnis `/disks` sind einige Diskettenabbilder (Images) enthalten. Solch ein Image kann mit geeigneten Hilfsprogrammen auf eine Diskette kopiert werden, die Diskette nennt sich dann Bootdiskette.

Auf diesen Diskettenimages sind außerdem noch der „Loader“ Syslinux und das Programm linuxrc drauf; Syslinux erlaubt es Ihnen, während des Bootvorganges den gewünschten Kernel auszuwählen und bei Bedarf Parameter über die verwendete Hardware zu übergeben. – Das Programm linuxrc unterstützt Sie beim Laden der Kernelmodule speziell für Ihre Hardware und startet schließlich die Installation.

Die mitgelieferte SuSE-Bootdiskette können Sie im Normalfall als Bootdiskette einsetzen. Nur bei exotischer Hardware, die vom modularisierten Kernel dieser Diskette nicht unterstützt wird, oder wenn Sie sich ein Disketten-Image aus den Internet von z. B. `ftp://ftp.suse.com` downloaden, müssen Sie eine eigene Bootdiskette erzeugen, wie es hier beschrieben wird.

Mit Setup

Schritt für Schritt...

Gehen Sie so vor, um eine Bootdiskette zu erzeugen:

1. Starten Sie Setup direkt von der CD 1.
2. Wählen Sie die Option ‘Floppy’ und drücken Sie ↵; dann ‘Boot’ und wieder ↵.
3. Jetzt müssen Sie sich eine Diskette mit einem passenden Kernel aussuchen, der z. B. Ihren SCSI-Adapter unterstützt. Setup zeigt Ihnen die wichtigsten Daten zu den Kernel an. Wenn Sie weitere Informationen brauchen, können Sie in der Datei `\disks\readme.dos` nachsehen. Merken Sie sich, wie Ihr Kernel heißt, Sie brauchen den Namen später nochmal. Dann drücken Sie ↵.
4. Jetzt wird die Diskette geschrieben. Legen Sie eine (DOS-formatierte) Diskette in das 3.5-Zoll-Laufwerk und suchen Sie sich die Diskette aus, die Sie erstellen wollen.

- Kümmern Sie sich nur um die Bootdiskette ('Root' wird bei SuSE Linux nicht mehr benötigt!): Setzen Sie den Cursor auf 'Boot' und drücken Sie ↵.
- Setup will bestätigt haben, dass eine Diskette eingelegt ist. Drücken Sie jetzt ↵. Die Diskette wird geschrieben.
- Wenn die Diskette fertig ist, drücken Sie ↵.
- Wählen Sie die Option 'Fertig', um den Bildschirm und Setup zu verlassen.

Mit rawrite

Alternativ können Sie auch das (unter Umständen langsamere) DOS-Programm rawrite.exe (CD 1, Verzeichnis `\dosutils\rawrite`) zum Schreiben der Diskette am DOS-Prompt einsetzen.

Auf der CD 1 im Verzeichnis `/disks` liegen die Standard-Diskettenimages; lesen Sie dort bitte die Dateien `README` bzw. `LIESMICH`. Das Image `bootdisk` ist die Vorlage für die Standarddiskette. Die eigentlichen Kernel sind im Verzeichnis `/suse/images` zu finden (ohne Endung!); lesen Sie auch dort bitte `README` bzw. `LIESMICH`.

Wenn Sie die Standarddiskette benötigen, wird, gehen Sie folgendermaßen vor; es wird vorausgesetzt, dass Sie sich im Hauptverzeichnis der CD befinden:

```
Q:> dosutils\rawrite\rawrite disks\bootdisk
```

Falls Sie eine spezielle Unterstützung, ist anstelle von `bootdisk` ein anderes Diskettenimage zu verwenden; bei Problemen kann als Fallback-Kernel `k_i386` eingesetzt werden.

Bootdiskette unter Unix erstellen

Voraussetzung

Sie können auf ein Unix/Linux-System mit einem funktionstüchtigen CD-ROM-Laufwerk zurückgreifen. Sie brauchen eine geprüfte Diskette (formatiert).

Gehen Sie so vor, um Bootdisketten zu erstellen:

1. Falls Sie die Disketten noch formatieren müssen:

   ```
   erde:~ # fdformat /dev/fd0u1440
   ```

2. Mounten Sie die erste CD (Disk 1); z. B. nach `/cdrom`:

   ```
   erde:~ # mount -tiso9660 /dev/cdrom /cdrom
   ```

3. Wechseln Sie in das Verzeichnis `disks` auf der CD:

```
erde:~ # cd /cdrom/disks
```

4. Erstellen Sie die Bootdiskette mit

   ```
   erde:~ # dd if=/cdrom/disks/bootdisk of=/dev/fd0 bs=8k
   ```

   In der `LIESMICH`- bzw. der `README`-Datei im `disks`-Verzeichnis erfahren Sie, welcher Kernel was kann; diese Dateien können Sie mit `more` oder `less` lesen.

   Falls Sie spezielle Unterstützung benötigen, ist anstelle von `bootdisk` ein anderes Diskettenimage zu verwenden; bei Problemen kann als Fallback-Kernel `k_i386` eingesetzt werden.

Probleme mit LILO

Einige Richtlinien

Zu Beginn ein paar einfache Richtlinien, mit denen die meisten LILO-Probleme von vorneherein vermieden werden können

(entnommen dem LILO-Benutzerhandbuch):

- **Keine Panik!** Wenn etwas nicht geht: versuchen Sie erst, den Fehler und die Ursache zu finden; überprüfen Sie die Diagnose und beginnen Sie erst dann mit Maßnahmen zur Fehlerbehebung.
- Halten Sie stets eine aktuelle und erprobte „Bootdiskette“ bereit.

  SuSE Linux enthält eigenständiges Rettungssystem (siehe Abschnitt *Das SuSE Rettungssystem* auf Seite 99), mit dem Sie an alle Linux-Partit wieder herankommen. Mit enthalten ist genügend Werkzeug, um die allermeisten Probleme mit unzugänglich gewordenen Festplatten zu lösen.
- Lesen Sie die Dokumentation. Vor allem dann, wenn das System nicht tut, was es Ihrer Meinung nach tun sollte.
- *Vor* jedem Aufruf des Map-Installers (`/sbin/lilo`): überprüfen Sie sorgfältig die Konfigurationsdatei `/etc/lilo.conf` .
- Rufen Sie `/sbin/lilo` *jedes Mal* auf, wenn irgendein Bestandteil der LILO-Startmaschinerie oder die LILO-Konfigurationsdatei `/etc/lilo.conf` geändert worden ist.
- Aufmerksamkeit ist bei großen oder bei mehreren Festplatten geboten: Berücksichtigen Sie die 1024-Zylinder-Grenze!
- Probieren Sie es ohne und mit Option linear (meist besser: ohne!).

Fehlerdiagnose: LILO Start-Meldungen

Hier wiederholen wir im Wesentlichen in Übersetzung einen Abschnitt aus [**?**], der LILO-Beschreibung von Werner Almesberger.

Der LILO-Systemstart-Code besteht aus zwei Teilen: der *ersten Stufe* in einem Bootsektor und der *zweiten Stufe* in `/boot/boot.b`. Bei der Installation von LILO wird eine „Map-Datei“ erzeugt (standardmäßig `/boot/map`), in der LILO die nötigen Zeiger (Sektoradressen) auf die Betriebssysteme (Linux-Kernel usw.) findet, die er starten soll.

Wenn LILO geladen wird, zeigt er das Wort `'LILO'` an. Jeder Buchstabe entspricht der Vollendung einer spezifischen Phase. Wenn LILO nicht starten kann, bilden die bereits ausgegebenen Buchstaben einen genaueren Hinweis darauf, in welchem Stadium ein Problem aufgetreten ist.

(nichts) – Kein Teil von LILO wurde geladen. Entweder LILO ist gar nicht installiert, oder es wurde nicht die Partition mit dem LILO-Bootsektor gestartet.

`'L'` ***error*** . . . – Die „erste Stufe“ wurde geladen und gestartet, aber sie konnte die zweite Stufe (`/boot/boot.b`) nicht laden. Dies weist üblicherweise auf einen physikalischen Fehler des Boot-Datenträgers oder eine fehlerhafte Platten-Geometrie hin.

`'LI'` – Die zweite Stufe von LILO wurde geladen, konnte aber nicht gestartet werden. Dies kann verursacht werden durch eine fehlerhafte Platten-Geometrie oder durch Verschieben von `/boot/boot.b` ohne Neuinstallation von LILO.

`'LIL'` – Die zweite Stufe von LILO wurde gestartet, konnte aber die nötigen Daten (Zeiger usw.) nicht aus der Map-Datei laden. Dies wird typischerweise verursacht durch einen physikalischen Fehler des Boot-Datenträgers oder eine fehlerhafte Platten-Geometrie.

`'LIL?'` – Die zweite Stufe von LILO wurde an eine falsche Speicheradresse geladen. Dies wird typischerweise verursacht durch einen subtilen Fehler in der Platten-Geometrie oder durch Verschieben von `/boot/boot.b` ohne Neuinstallation von LILO.

`'LIL-'` – Die Daten in der Map-Datei sind ungültig. Dies wird typischerweise verursacht durch einen Fehler in der Platten-Geometrie oder durch Verschieben von `/boot/boot.b` ohne Neuinstallation von LILO.

`'LILO'` – Alle Teile von LILO wurden erfolgreich geladen.

Fehlerursache beseitigen

Die häufigsten Ursachen für *Geometriefehler* sind nicht physikalische Defekte oder ungültige Partitionstabellen, sondern Fehler bei der Installation von LILO– vor allem die Missachtung der 1024-Zylinder-Grenze (s. den Abschnitt *Die 1024-Zylinder--Grenze* auf Seite 97).

In den meisten Fällen läuft die Abhilfe auf die folgenden drei Maßnahmen hinaus:

1. Die LILO-Daten unterhalb der 1024-Zylinder-Grenze installieren (falls noch nicht geschehen). Das bezieht sich auf die benötigten Linux-Kernel, den Inhalt des Verzeichnisses `/boot` und auch den Bootsektor, der den LILO-Startcode aufnehmen soll.

2. LILO neu installieren mit dem Befehl `lilo` als `root`

   Ein informatives Log liefert `lilo`, wenn Sie die Gesprächigkeit (engl. *verbosity*) erhöhen und Logdateien anlegen lassen. Das geht wie folgt:

   ```
   erde:~ # lilo -v -v -v >/boot/lilo.log 2>/boot/lilo.logerr
   ```

   In `/boot/lilo.logerr` sollte bei einer korrekten Bootkonfiguration gar nichts stehen. In `/boot/lilo.log` können Sie u. a. genau nachlesen, wie LILO sich die Lokationen seiner Dateien merkt, welche BIOS-Gerätenumme LILO für die betroffenen Festplatten verwendet und mehr.

3. Konsistenz der Festplattengeometrie-Informationen prüfen. Tatsächlich sind dazu bis zu vier Stellen von Belang:

   (a) Geometrie, die LILO verwendet. Siehe die oben genannte Logdatei. Beeinflussbar durch die Angabe disk in `lilo.conf`

   (b) Geometrie, die der Linux-Kernel erkannt hat. Siehe die Boot-Meldungen (`/var/log/boot.msg` oder die Ausgabe des Befehls `dmesg`). Beeinflussbar durch: Kernelparameter (in Grenzen).

   (c) Geometrie, die der Partitionstabelle zu Grunde liegt. Siehe die Ausgab von `fdisk -l`. Beeinflussbar durch `fdisk`-Expertenbefehle. Sehr gefährlich für die Daten! Vollbackup vorher dringend empfohlen! Wirklich nur für Experten!

   (d) Geometrie, die das BIOS erkannt hat. Diese Geometrie findet LILO später beim Systemstart vor und muss mit ihr arbeiten. Siehe das BIOS-Setup, eventuell auch das des SCSI-Hostadapters (falls vorhanden). Beeinflussbar durch das BIOS-Setup.

Bei Inkonsistenzen ist für die Entscheidung „Wo anpassen?“ oft der Weg des „geringsten Widerstandes“ die beste Methode.

Zur Problembeseitigung sind also folgende Daten zu erheben:

- `/etc/lilo.conf`
- Ausgabe des Befehls `fdisk -l` (Partitionierung)
- oben genannte Logdateien
- Einstellungen des BIOS und des SCSI-BIOS zu Ihren Festplatten

Die 1024-Zylinder-Grenze

Hinweis

Seit kurzer Zeit sind BIOS-Versionen verfügbar, die es erlauben, Betriebssysteme oberhalb der 1024-Zylinder-Grenze zu starten. Die aktuell Version von LILO kann diese BIOS-Erweiterung nutzen. YaST und YaST2 wird Sie bei der LILO-Konfiguration entsprechend über die Möglichkeiten Ihres BIOS informieren. Sollte Ihr BIOS nicht über diese Erweiterung verfügen, sollten Sie hier unbedingt weiterlesen.

Hinweis

Wie schon mehrfach betont , muss die gesamte LILO-Startmaschinerie, d. h. alle Daten, die LILO zum Starten benötigt, mit BIOS-Routinen allein zugänglich sein. Welche Festplatten-Bereiche demnach dafür in Frage kommen (wir nennen das im Folgenden kurz: *zulässiger Bereich*), haben wir dort bereits ausgeführt.

Welche Möglichkeiten lässt diese Einschränkung nun offen? Eigentlich noch eine ganze Menge, wenn man bedenkt, dass *nur* die Startmaschinerie betroffen ist. Es gibt kein Gesetz, nach dem diese in der Linux-Rootpartition liegen müsste: ja, es ist im Notfall sogar möglich (wenn auch nicht ganz ungefährlich), Dateien der Startmaschinerie auf Partitionen fremder Betriebssysteme unterzubringen, wenn nur Linux Lese- und Schreibzugriff auf deren Dateisysteme hat.

Achtung

Sie müssen sich nur davor hüten, den LILO-Bootsektor in eine fremde Partition zu installieren, weil damit in der Regel deren Dateisystem beschädigt wird!

Achtung

- Die „sauberste Lösung“ besteht auf jeden Fall darin, bei der Linux-Installation eine *primäre Linux-Partition* ganz innerhalb des zulässigen Bereichs anzulegen und die LILO-Daten (einschließlich des LILO-Bootsektors) dort unterzubringen.

  Bei der Installation mit YaST wird dafür eine eigene Partition (`/boot`) vorgesehen, die lediglich groß genug ist, um die folgenden Dateien aufzunehmen:

  - `boot.b`, `map`, `message`,
  - die Linux-Kernel, die LILO booten soll.

  Es genügen also wenige Megabytes. Das ganze übrige System unterliegt hinsichtlich der Lokation auf der/den Festplatte(n) keiner Einschränkung: wenn der Kernel erst einmal läuft, hat er uneingeschränkten Zugriff auf alle Festplatten im System.

Aber was tun, wenn für so eine Partition kein Platz mehr ist? Wenn Sie nicht umpartitionieren wollen oder können, und auch ein Upgrade auf SCSI oder ein modernes BIOS nicht in Frage kommt, gibt es doch noch zwei behelfsmäßige Möglichkeiten:

- An Stelle von LILO auf der Platte eine Bootdiskette oder, wenn Sie MS-DOS betreiben, loadlin verwenden, um Linux zu booten.
- Die LILO-Startmaschinerie auf einer Nicht-Linux-Partition unterbringen, die ganz im zulässigen Bereich liegt, und auf die Linux schreiben kann (z. B. ein FAT/VFAT DOS-Laufwerk). Natürlich können wir den LILO-Bootsektor nicht auch dorthin schreiben! So bleiben dafür nur übrig: der Anfang einer erweiterten Partition auf der ersten Platte – sofern vor Zylinder 1024 – oder der MBR. Nehmen wir an, die betreffende Partition ist unter `/mnt` gemountet. LILO soll in den MBR, etwa `/dev/hda`, und soll zusätzlich DOS von `/dev/hda1` booten. Dann ist das Vorgehen wie folgt:
  - Neues Verzeichnis, z. B. `/mnt/LINUX` anlegen und die eben schon genannten LILO-Dateien aus `/boot` dorthin kopieren: `boot.b`, `map`, `message`, sowie die Chain-Loader für Ihre anderen Betriebssysteme (i. Allg. `chain.b`) und die Linux-Kernel, die LILO booten soll.
  - Legen Sie eine `/mnt/LINUX/lilo.cfg` an, in der alle Pfade nach `/mnt/LINUX` verweisen (Datei 4):

```
# LILO Konfigurations-Datei Fremdverzeichnis
# Start LILO global Section
boot=/dev/hda              # Installationsziel
backup=/mnt/LINUX/hda.xxxx  # backup alter MBR
install=/mnt/LINUX/boot.b  # Natürlich sind LILO und
map=/mnt/LINUX/map         # Map-Datei in /mnt/LINUX!
message=/mnt/LINUX/message # optional
prompt
timeout=100     # Warten am Prompt: 10 s
vga = normal    #
# End LILO global section
#
# Linux bootable partition config begins
image = /mnt/LINUX/Erster_Kernel   #   default
    root = /dev/Ihr_Root_Device    # Root-Partition hierher!
    label = linux
# Linux bootable partition config ends
#
# Systemabschnitte für weitere Kernel hier:
#
# Ende Linux
# DOS bootable partition config begins
other = /dev/hda1      # MSDOS-Systemlaufwerk
```

```
    label = dos
    loader = /mnt/LINUX/chain.b
    table = /dev/hda
# DOS bootable partition config ends
```

Datei 4: *`lilo.cfg` für fremde Partition*

- LILO mit *dieser* `lilo.cfg` installieren:

  ```
  erde:~ # /sbin/lilo -C /mnt/LINUX/lilo.cfg
  ```

  Danach sollte LILO funktionieren. Booten Sie MS-DOS und schützen Sie die LILO-Dateien, so gut es geht, gegen Schreibzugriffe. (Zur Erinnerung: jeder solche setzt LILO außer Funktion!) Zumindest geben Sie allen Dateien in `X:\LINUX` (wo `X:` das eben unter `/mnt` gemountete MS-DOS-Laufwerk ist) die DOS-Attribute *System* und *Versteckt*.

Abschließend möchten wir zum selben Thema noch verweisen auf die zwei HOWTOs `LILO.gz` und `Large-Disk.gz` in `/usr/share/doc/howto/en/mini/`.

Das SuSE Rettungssystem

Das Rettungssystem wird von der SuSE-Bootdiskette bzw. der bootbaren CD 1 Ihres SuSE-Linux gestartet. Die Voraussetzung ist, dass das Disketten- bzw. CD-ROM-Laufwerk bootfähig ist; nötigenfalls müssen Sie im CMOS-Setup die Boot-Reihenfolge ändern.

Nachfolgend die Schritte zum Starten des Rettungssystems:

1. Legen Sie die SuSE-Bootdiskette (`bootdisk`) bzw. die erste CD Ihres SuSE-Linux in das CD-ROM-Laufwerk ein und schalten Sie Ihr System ein.
2. Sie können entweder das System durchbooten lassen oder Sie wählen 'Manual Installation' aus und können dann – falls notwendig – bei den 'boot options' Parameter angeben. Im Folgenden ist es möglich festzulegen, welche Kernel-Module geladen werden sollen.
3. Nehmen Sie im linuxrc die erforderlichen Einstellungen für die Sprache, den Bildschirm und die Tastatur vor.
4. Wählen Sie im Hauptmenü den Punkt 'Installation/System starten'.
5. Wenn Sie mit der *Bootdiskette* gestartet haben, legen Sie nun die Installations-CD oder die Diskette (`rescue`) mit dem komprimierten Abbild des Rettungssystems ein.
6. Wählen Sie im Menü 'Installation/System starten' den Punkt 'Rettungssystem starten' und geben Sie dann das gewünschte Quellmedium an.

   Im Anschluss ein paar Hinweise zu den Auswahlmöglichkeiten:

'CD-ROM' – Beim Laden des Rettungssystems wird der Pfad `/cdrom` exportiert. Eine Installation ist so von *dieser* CD aus möglich.

Hinweis

Sie müssen die notwendigen Werte noch in SuSEconfig eintragen

Hinweis

'Netzwerk (NFS)' – Um das `rescue`-System via NFS aus dem Netz zu laden, ist es erforderlich, dass Sie den Treiber für Ihre Netzwerkkarte zuvor geladen haben.

'Netzwerk (FTP)' – Um das `rescue`-System via FTP aus dem Netz zu laden, ist es erforderlich, dass Sie den Treiber für Ihre Netzwerkkarte parat haben.

'Festplatte' – Laden Sie das `rescue`-System von der Festplatte aus.

'Diskette' – Das `rescue`-System kann auch von Diskette gestartet werden, vor allem wenn der Rechner über wenig Arbeitsspeicher verfügt.

Welches Medium Sie auch gewählt haben, das Rettungssystem wird dekomprimiert und als neues Root-Dateisystem in eine RAM-Disk geladen, gemountet und gestartet. Es ist damit betriebsbereit.

Das Rettungssystem benutzen

Das Rettungssystem stellt Ihnen unter (Alt) + (F1) bis (Alt) + (F3) mindestens drei virtuelle Konsolen zur Verfügung, an denen Sie sich als Benutzer `root` ohne Passwort einloggen können. Mit (Alt) + (F10) kommen Sie zur Systemkonsole mit den Meldungen von Kernel und syslog.

In dem Verzeichnis `/bin` finden Sie die Shell und Utilities (z. B. mount). Wichtige Datei- und Netz-Utilities, z. B. zum Überprüfen und Reparieren von Dateisystemen (e2fsck), liegen im Verzeichnis `/sbin`. Des Weiteren finden Sie in diesem Verzeichnis auch die wichtigsten Binaries für die Systemverwaltung wie fdisk, mkfs, mkswap, init, shutdown, sowie für den Netzwerkbetrieb ifconfig, route und netstat.

Als Editor ist der vi unter `/usr/bin` verfügbar; hier sind auch weitere Tools (grep, find, less etc.) wie auch das Programm telnet zu finden.

Zugriff auf das normale System

Zum Mounten Ihres SuSE Linux-Systems auf der Platte ist der Mountpoint `/mnt` gedacht. Sie können für eigene Zwecke weitere Verzeichnisse erzeugen und als Mountpoints verwenden.

Nehmen wir als Beispiel einmal an, Ihr normales System setzt sich laut `/etc/fstab` wie in der Beispieldatei 5 beschrieben zusammen.

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

Datei 5: *Beispiel* `/etc/fstab`

Achtung

Beachten Sie im folgendem Abschnitt die Reihenfolge, in welcher die einzelnen Geräte zu mounten sind.

Achtung

Um Zugriff auf Ihr gesamtes System zu haben, mounten Sie es Schritt für Schritt unter `/mnt` mit den folgenden Befehlen:

```
erde:/ # mount /dev/sdb3 /mnt
erde:/ # mount /dev/sdb6 /mnt/usr
```

Nun haben Sie Zugriff auf Ihr ganzes System und können z. B. Fehler in Konfigurationsdateien wie `/etc/fstab`, `/etc/passwd`, `/etc/inittab` beheben. Die Konfigurationsdateien befinden sich statt im Verzeichnis `/etc` jetzt im Verzeichnis `/mnt/etc`.

Um selbst komplett verloren gegangene Partitionen mit dem Programm fdisk einfach wieder durch Neu-Anlegen zurückzugewinnen – wenn bekannt war, wo die Partitionen vorher auf der Festplatte lagen – sollten Sie sich einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls

```
erde:~ # fdisk -l /dev/⟨disk⟩
```

machen. Anstelle der Variablen ⟨*disk*⟩ setzen Sie bitte der Reihe nach die Gerätenamen (engl. *devices*) Ihrer Festplatten ein, z. B. `hda`.

Dateisysteme reparieren

Beschädigte Dateisysteme sind ein besonders ernster Anlass für den Griff zum Rettungssystem. Dies kann z. B. nach einem unsauberen Shutdown (wie bei Stromausfall) oder einem Systemabsturz vorkommen. Dateisysteme lassen sich grundsätzlich nicht im laufenden Betrieb reparieren. Bei schwereren Schäden lässt sich unter Umständen nicht einmal das Root-Dateisystem mehr mounten und der Systemstart endet in einer "kernel panic". Da bleibt nur der Weg, die Reparatur „von außen“ unter einem Rettungssystem zu versuchen.

Im SuSE Linux-Rettungssystem sind die Utilities e2fsck und dumpe2fs (zur Diagnose) enthalten. Damit beheben Sie die meisten Probleme. Und da auch im Notfall oft die Manual-Page von e2fsck nicht mehr zugänglich ist, ist sie im Anhang A auf der nächsten Seite ausgedruckt.

Beispiel: Wenn sich ein Dateisystem wegen eines *ungültigen Superblocks* nicht mehr mounten lässt, wird das Programm e2fsck vermutlich zunächst ebenfalls scheitern. Die Lösung ist, die im Dateisystem alle 8192 Blöcke (8193, 16385. . .) angelegt und gepflegten Superblock-Backups zu verwenden. Dies leistet z. B. der Befehl:

```
erde:~ # e2fsck -f -b 8193 /dev/⟨Defekte_Partition⟩
```

Die Option `-f` erzwingt den Dateisystem-Check und kommt damit dem möglichen Irrtum von `e2fsck` zuvor, es sei – angesichts der intakten Superblock-Kopie – alles in Ordnung.

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 sys-
       tem (e2fs).  E2fsck also supports ext2  filesystems  coun-
       taining  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 uuencode(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 1.23 August 2001 3

Support

Das Support-Konzept für den SuSE Linux Office Server besteht aus mehreren Bausteinen:

1. Kostenloser Installations-Support für die grundlegende Server-Installation
2. Erweiterter Installations-Support für die Server-Installation
3. Support für die Windows-Netzwerkeinrichtung

Kostenloser Installations-Support

Sollten Sie weder in der Dokumentation noch in der Supportdatenbank fündig geworden sein, so können Sie Ihre Anfragen auch direkt an uns richten. Im Rahmen des kostenlosen Installations-Supportes geben wir Ihnen Antworten auf Fragen im Bereich:

- Installation auf einem Rechner mit mindestens 64 MB RAM und 2 GB freiem Plattenplatz
- Kernel-Upgrades offizieller SuSE Update-RPMs
- Einspielen von SuSE Bugfixes und Security-Updates mittels YOU oder manuell
- Bootkonfiguration mit LILO im MBR der ersten Platte oder auf Floppy ohne Änderungen am BIOS-Mapping
- Installation von einem lokal angeschlossenen ATAPI/SCSI CD- oder DVD-ROM
- Installation auf die 1. oder 2. Festplatte in einem reinem IDE oder SCSI-System inkl. Analyse von Resourcen-Konflikten

- Einrichten eines Internetzugangs mit unterstützter PCI-ISDN-Karte oder externem seriellen Modem oder DSL (über unterstützte PCI Netzwerkkarte, nur PPPoE)
- Einbindung einer Standard-Tastatur und einer Standard-Maus (ohne Wheel)
- Konfiguration der Grafikkarte bei einem von YaST2 erkannten Monitor ohne 3D mit Hilfe von YaST2

Hinweis

Wir versuchen, Ihnen so schnell und präzise wie möglich zu helfen. Eine gezielte Fragestellung reduziert dabei erheblich den Aufwand und Zeitbedarf.

Hinweis

Deshalb sollten Sie im Vorfeld folgende Punkte klären und bevor Sie zum Hörer greifen nachstehende Informationen unbedingt bereithalten:

- Um welches Programm/Version handelt es sich? Bei welchem Vorgang tritt das Problem auf?
- Was genau ist das Problem? Versuchen Sie, die Fehlerbeschreibung als konkrete Wenn-Dann-Aussage zu formulieren (z. B. wenn man die Schaltfläche 'xy' anklickt, dann . . .)
- Auf welcher Hardware arbeiten Sie (Grafikkarte, Monitor, Drucker, ISDN-Karte etc.).

Weitere Hinweise

1. Der kostenlose Support bezieht sich nur auf die Erstinstallation.
2. Die Unterstützung der Hardware durch SuSE Linux ist natürlich jeweils Voraussetzung dafür, dass wir entsprechenden Support leisten können.
3. Es gibt keine garantierten Reaktionszeiten auf Mail-Anfragen.
4. Um den Support in Anspruch nehmen zu können müssen Sie sich mit Ihrem Support Key zunächst registrieren. Am besten gleich unter `https://support.suse.de/de/register/` oder telefonisch unter 0421-526-2310.
5. Der Support Key wird personalisiert erfasst und ist nicht übertragbar.
6. Zeitraum des Installationssupports Der Installationssupport für den SuSE Linux Office Server erstreckt sich über einen Zeitraum von 60 Tagen ab dem Registrierdatum; maximal jedoch bis 60 Tage nach Erscheinen der Nachfolge-Version.

Kostenloser Installations-Support bei der Server-Installation per E-Mail

Bitte geben Sie bei E-Mail-Anfragen an den Support immer Ihren Support Key, den Sie auf der CD-Hülle finden, mit an!

Schreiben Sie, wie unten aufgezeigt, eine E-Mail direkt an die Adresse `support@suse.de`. Beachten Sie die Groß- und Kleinschreibung bei den Kundendaten. Nur so kann Ihre E-Mail automatisch verarbeitet werden. Lassen Sie Felder wie `FIRMA:` bitte leer, falls Sie sie nicht benötigen. Verwenden Sie keine unnötigen Attachments Visitenkarten im X-VCARD Format und fügen Sie ggf. Konfigurationsdateien im ASCII-Format direkt in die Anfrage ein.

```
VORNAME: Honigtau
NAME: Dr. Bunsenbrenner
FIRMA: Muppetshow (Laboratorium)
STRASSE: Sesamstr. 4711
PLZ: 00815
ORT: Timbuktu
LAND: Deutschland
REGCODE: XXXXXX
EMAIL: bunsen@nowhere.de

Liebes SuSE Support-Team,

ich habe hier in meinem Muppet-Laboratorium ein kleines
Problem.

Nach der Installation des SuSE Linux Office Server kommt nach dem
Booten des Kernels die Fehlermeldung

            "Unable to open an initial console"

Ich habe einen Pentium 400 mit 128 MB RAM und eine 8 GB IDE
Festplatte. Was mache ich falsch?
Mit freundlichen Gruessen
(auch von meinem Assistenten Beeker)

Ihr Dr. Honigtau Bunsenbrenner
<bunsen@nowhere.de>
```

```
... habe ich ein Problem mit Lilo. Hier ist der wichtige
Teil meiner /etc/lilo.conf

---schnipp---
# Linux bootable partition config begins
image = /boot/vmlinuz
root = /dev/sda2
label = linux-2.0.36
# Linux bootable partition config ends
```

Sie erreichen den Installationssupport:

Via	Daten	Bearbeitung
E-Mail	support@suse.de	ganzwöchig
WWW Formular/E-Mail	Online Webformular[a]	ganzwöchig
Fax	Fax-Nummer: 0421-526-2350	ganzwöchig

[a] siehe http://support.suse.de/de/services/anfrage-onlineform.html

Erweiterter Support bei der Office-Server-Installatio

Auch bei Fragen und Problemen, die über den Rahmen des kostenlosen Installationssupports hinaus gehen, lassen wir sie nicht im Regen stehen. Hierfür bieten wir ihnen wie gehabt unseren bewährten Basic Level Support für Privatkunden an. Durch den Erwerb eines "Callpacks"bearbeiten wir nahezu alle Anfragen, die innerhalb eines Zeitrahmens von 30 Minuten liegen. Legen Sie hingegen Wert auf eine möglichst zeitgenaue Abrechnung, möchten wir Ihnen unsere kostenpflichte Telefon Hotline (Deutschland: 1,86 EUR/Minute, Österreich: 1,80 EUR/Minute, Schweiz: 3,13 sFr/Minute) ans Herz legen. Ihr Vorteil: Sie bezahlen wirklich nur für die Zeit, die wir für die Lösung ihrer Anfrage tätsächlich gebraucht haben.

0190 862 801	Internet (Modem, ISDN, DSL, Cable Modem)
0190 862 802	Externe Peripherie (Drucker)
0190 862 804	Grafische Oberfläche X11 (Grafikkarten, Maus, Tastatur, 3D, TV-Out)
0190 862 807	Einfache Administration und LAN (Netzwerkdienste, Benutzerverwaltung, Rechte, kleine Netzwerke) (Ohne Einrichtung des Windows-Netzwerks)

Darüberhinaus können Sie von unserem umfangreichen Support Service für Geschäftskunden profitieren. Das Dienstleistungsspektrum erstreckt sich über die Möglichkeit der Lösung einzelner Anfragen bis hin zum Abschluß von laufzeit- oder projektabhängigen Verträgen.

Support bei Fragen zur Samba und Netzwerkkonfiguration

Bei Fragen zur Samba und Netzwerkkonfiguration können Sie das Supportangebot unserer Professional Services in Anspruch nehmen, das sowohl für Privatkunden als auch für Geschäftskunden preislich attraktive Supportleistungen bereitstellt. Sie können sich auf unserer Homepage unter

`http://www.suse.de/de/services/support/private/basic.html`

für unsere Privatkunden und

`http://www.suse.de/de/services/support/business/index.html`

für unsere Geschäftskunden über unsere Angebote informieren. Wenn Sie ein persönliches Gespräch bevorzugen, stehen wir Ihnen gerne unter der Telefonnummer

0421 / 526 23 30

zur Verfügung.

Feedback

Wir sind Ihnen immer für Hinweise und Problembeschreibungen dankbar und helfen auch gerne weiter, wenn das Problem grundlegender Natur ist oder wir bereits eine Lösung dafür haben. Auf jeden Fall ermöglicht uns Ihr Feedback, das Problem in späteren Versionen zu beseitigen bzw. die Information anderen SuSE Linux-Anwendern z. B. via WWW zur Verfügung zu stellen.

Zum anderen sind wir bemüht, ein SuSE Linux-System aufzubauen, das den Wünschen unser Kunden möglichst nahe kommt. Deshalb haben wir für Kritik an der CD und am Buch, sowie für Anregungen zu künftigen Projekten, immer ein offenes Ohr. Wir denken, dies ist der beste Weg, Fehlentwicklungen frühzeitig zu erkennen und den hohen Qualitätsstandard von Linux zu erhalten. Sie können uns Ihr Feedback jederzeit via Webfrontend (siehe `http://www.suse.de/cgi-bin/feedback.cgi`) schicken.

Index