Open School Server

Administrationshandbuch

4. Auflage 2007

Hinweise und Kommentare richten Sie ggf. an ossinfo@extis.de

Autor(en): Lars Rupp, Péter Varkoly
Redaktion: Peter Grill, Péter Varkoly
Layout: Manuela Piotrowski, Thomas Schraitle
Satz: LaTeX

Inhaltsverzeichnis

Teil I

Inbetriebnahme des Open School Servers

Vorwort

In der Vergangenheit wurden oft Arbeitskreise mit dem Ziel gegründet, eine „easy to install – easy to use“ Linux Distribution speziell für die Bedürfnisse an Schulen zu erstellen. Diese scheiterten jedoch meistens daran, dass weder die dafür notwendige Zeit noch das Know-how vorhanden waren. Auf die dauerhafte Unterstützung von fachkundigen Schülern konnten bzw. können die Lehrer nicht rechnen, da es zu einer enormen Ablenkung von deren eigentlichen Aufgabe führen kann. Auch die Lehrer selbst und evtl. vorhandene ehrenamtliche Helfer stehen nicht ständig für Wartungsaufgaben oder gar die Entwicklung spezieller Software zur Verfügung und haben ganz andere Aufgaben.

Schulen brauchen also eine professionelle Unterstützung. Deshalb entstand eine Initiative des Landkreises Fürth, die Firma SUSE LINUX AG mit der Entwicklung eines speziell auf die Bedürfnisse von Schulen ausgerichteten Servers zu beauftragen.

1.1 Anforderungen an einen Schul-Server

Die Anforderungen an ein Computernetzwerk in einer Schulumgebung, also an ein sogenanntes pädagogisches Netzwerk, sind komplexer als die in einer reinem Büroumgebung. Abgestürzte Arbeitstationen unter Windows müssen in Minutenschnelle – etwa während einer Abschlussprüfung am Rechner oder von einer Unterrichtsstunde zur anderen – und auf Knopfdruck restaurierbar sein.

In bestimmten Unterrichtssituationen ist es wünschenswert, den Zugriff auf das Internet und damit auf diverse Kommunikationsmöglichkeiten wie Email, FTP, SSH etc. auf Knopfdruck ausschalten zu können. Und selbstverständlich müssen alle anderen Anforderungen an ein LAN (Intranet) erfüllt sein. Im einzelnen sind das:

- Sicherheit gegen Zugriff von außen (Firewall)

- Kontrollierter Internetzugang
- Ein eigenes Intranet mit internen WWW–Seiten, FTP–Zugang und Email
- Stabiler Fileserver mit Backup
- Stabiler Printserver
- Einfache, grafische Benutzeradministration (mit der Möglichkeit, Benutzeraccounts automatisiert anzulegen)
- Einfache Netzwerkanalyse
- Problemlose Installation von Updates

Diese Anforderungen kann man durch den Einsatz von einem (oder mehreren) Linux Servern auf hohem Niveau erfüllen. Für Linux sprechen neben seinen günstigen Anschaffungskosten seine hohe Stabilität und Flexibilität. Es existieren schon viele Ansätze für die Verwendung von Linux im schulischen Bereich als Serverplattform, die von Schulen bzw. Schulträgern ausgehen. Zahlreiche Pädagogen, meistens Informatik-, Mathematik- und Physiklehrer haben oft in ihrer Freizeit hervorragende Lösungen auf Basis verschiedener Linux-Distributionen produziert. Es fehlte jedoch bis jetzt ein Linux-Produkt, welches nicht nur den speziellen schulischen Anforderungen genügte sondern auch einen langfristigen und professionellen Support beinhaltet und entsprechend betreut wird.

Die Antwort darauf ist der Open School Server: Durch die Kombination und Anpassung vorhandener SUSE Business Produkte und Technologien, durch die Verwendung des an Schulen gesammelten Know-hows und durch die gezielte Gestaltung der Netzwerktopologie konnten diese Aufgaben effektiv gelöst werden.

Der Open School Server (OSS) ist der Nachfolger des SuSE Linux Schulservers (SLSS). Der SLSS wurde in Zusammenarbeit mit mehreren Schulen auf der Basis von SuSE Linux Businessprodukten entwickelt. Seit dem Erscheinen der Version 1.0 im Jahre 2003 wird der SLSS in einigen hundert Schulen europaweit erfolgreich eingesetzt.

Der OSS zeichnet sich durch folgende Eigenschaften aus:

- Multifunktionale Server-Lösung speziell für Schulen konzipiert
- Internetzugang für Netzwerke (Modem, ISDN, DSL, Standleitung)
- All-in-one IP-Server: Stellt DNS-, DHCP-, E-Mail-, LDAP- und Proxydienste bereit, enthält Firewall-Lösung und Virenscanner (AMAVIS, Clam AntiVirus)
- Multiplattform-Authentikations-, Datei- und -Druckserver

- Transparenter Einsatz in einzelnen Schulen oder Schulverbänden
- Hervorragende Skalierbarkeit
- Intuitiv zu bedienendes Webinterface für Administratoren und Lehrer
- Externer Administrationszugang per HTTPS und/oder ssh möglich
- Zugriff auf Serverdienste (Internet, Drucken, Mail, Groupware) kann individuell für einzelne Räume oder Benutzer konfiguriert werden
- Arbeit in geschüzter Umgebung

Der Schulserver befindet sich in laufender Weiterentwicklung und greift dabei vor allem Anregungen aus der schulischen Praxis auf. Durch seine Flexibilität und den hohen Anpassungsgrad eignet er sich auch für komplexe Szenarien:

Zentrale Administration mehrerer Schulen Skalierung der Schulserver: Auslagern der Mail und Groupware Dienste auf eigene Rechner Einsatz von mehreren Schulservern in einem gemeinsamen Netzwerk

Die Version 2 des Schulservers basiert auf dem SUSE LINUX Enterprise Server. Wesentliche Neuerungen sind Samba 3.0, die verbesserte Unterstützung aktueller Hardwarekomponenten und eine ganze Reihe von Erweiterungen aus administrativer und pädagogischer Sicht.

1.2 Konzeption des Handbuches

Zunächst gibt dieses Buch auf den folgenden Seiten einige Tips für die einzusetzende Hardware und die Netzwerktopologie eines Schulnetzwerkes.

Im dritten Kapitel finden Sie dann die ausführliche Anleitung für die Installation und erste Inbetriebnahme des Open School Servers. Jedem, der schon einmal mit einer aktuellen SUSE LINUX Distribution in Berührung gekommen ist, dürfte die Installation bekannt vorkommen. Nur die Installation des Netzwerks (siehe Abschnitt 3.5.2 auf Seite 26) und die anschließende Grundkonfiguration des Servers (siehe Abschnitt 3.5.5 auf Seite 39) unterscheiden sich von einer normalen SUSE LINUX Installation.

Über die eigentliche Administration im laufenden Betrieb informiert Sie das Kapitel 6 auf Seite 55, das Sie Schritt für Schritt durch die einzelnen Bestandteile der Administrationsoberfläche führt. Hier lernen Sie Benutzer- und Computerkonten anzulegen und zu verwalten und die verschiedenen Serverdienste auf Ihre Bedürfnisse anzupassen.

Im Kapitel 6.3 auf Seite 107 finden Sie die Erläuterungen des Lehrerhandbuchs nochmals in gekürzter Form. So können Sie auch Lehrer und Schüler schnell bei evtl. auftretenden Fragen mit Ihrem Serveraccount helfen.

Wie Ihnen sicherlich schon aufgefallen ist, wird in diesem Buch immer nur die Rede von „Lehrern“ oder „Schülern“ sein – um den Wünschen der besseren Lesbarkeit zu entsprechen, haben wir auf die normalerweise dazu gehörende zusätzliche Nennung des jeweils weiblichen Parts verzichtet. Natürlich soll dadurch niemand diskriminiert werden – aber ständig „Lehrerinnen und Lehrer“ oder „LehrerInnen“ bzw. „Administratorinnen und Administratoren“ oder „AdministratorInnen“ zu schreiben würde dieses Buch nicht nur dicker werden lassen sondern manche Dinge auch unnötig verkomplizieren. Haben Sie, liebe weibliche Kolleginnen, also bitte Mitleid mit den Autoren und richten Sie Ihre Kritik vorwiegend auf die anderen Inhalte dieses Buches.

1.3 Danksagung

Wir möchten uns herzlich bei allen Helfern und Betatestern bedanken: den Lehrern und Schüler der Gymnasien und Realschulen in Franken (u.a. Markus Bölling, Dieter Kroemer, Gerhard Miedaner und Michael Schmidt) und den Mitarbeitern der Firma DoSys (u.a. Markus Klappenbach und Ralf Grevinga).
Ein zusätzlicher Dank geht an die Forschungstelle Recht des DFN Vereins e.V. und Andrea Wardzichowski vom DFN-WiNShuttle-Team für die Kooperation in Fragen des Datenschutzes und für die reibungslose Zusammenarbeit.

Typografische Konventionen

Auszeichnung	Bedeutung
YaST	die Angabe eines Programmnamens
`/etc/passwd`	die Angabe einer Datei oder eines Verzeichnisses
⟨*platzhalter*⟩	die Zeichenfolge `platzhalter` (inkl. Winkelklammern) ist durch den tatsächlichen Wert zu ersetzen
`PATH`	eine Umgebungsvariable mit dem Namen `PATH`
`192.168.1.2`	der Wert einer Variablen
`ls`	die Angabe eines einzugebenden Befehls
`user`	die Angabe eines Benutzers
`client1:~ # ls`	Eingabe von `ls` auf der Shell des Benutzers `root` im Homeverzeichnis auf dem Rechner „Erde“
`tux@client1:~ > ls`	Eingabe von `ls` auf der Shell des Benutzers `tux` (offizieller Name des Linux-Pinguins) im Homeverzeichnis auf dem Rechner „Erde“
Alt	eine zu drückende Taste; nacheinander zu drückende Tasten werden durch Leerzeichen getrennt
Ctrl + Alt + Entf	gleichzeitig zu drückende Tasten werden durch `'+'` miteinander verbunden
"Permission denied"	Meldungen des Systems
‘System updaten’	Menü-Punkte, Buttons
„DMA-Modus“	Namenskonventionen, -definitionen, So genanntes…

Vor der Installation

Mit dem Open School Server besitzen Sie ein leistungsfähiges Produkt auf Basis des SUSE LINUX Enterprise Servers. Stundenlange komplizierte Konfigurationssitzungen bleiben Ihnen erspart, und Sie können schnell einen leistungsfähigen E-Mail-, File-, Print- und Groupware Server, der kaum Wünsche offen lässt, einrichten.

Hinweis

In diesem Handbuch wird an einigen Stellen auf das Handbuch zum SUSE LINUX Enterprise Server (SLES9) sowie auf das Online Handbuch des Open School Server verwiesen. Das SLES9 Handbuch finden Sie zudem auf der CD im Verzeichnis `/doc`. Das Online Handbuch steht Ihnen nach der Installation über die Oberfläche des Open School Servers zur Verfügung. (Siehe *Online–Handbuch* auf Seite 44.)

Hinweis

2.1 Hardwarevoraussetzungen

Die Installation des Open School Servers auf sogenannten x86 Systemen gestaltet sich i.d.R. unproblematisch. Wir empfehlen Ihnen, folgende Randbedingungen einzuhalten:

- Als Hauptspeicher empfehlen wir mindestens 512 MB – besser sind jedoch 1 GB und mehr.
- Eine CPU mit mindestens 1 GHz. Empfohlen: 2 GHz und mehr.
- Festplattenkapazität mindestens 20 GB. Empfohlen: 40 GB und mehr.
- Von SUSE LINUX Enterprise Server unterstützte Netzwerkkarte(n).

- Eine von SUSE LINUX Enterprise Server unterstützte VGA–Karte. Empfohlen wird eine Grafikkarte und ein Monitor mit einer Auflösung von 1024x786 bei mindestens 75 Hz Bildwiederholungsrate.

2.1.1 Besondere Hardwareanforderungen

Beachten Sie bitte, dass ein Server normalerweise 24 Stunden am Tag und 7 Tage in der Woche durchläuft, und ein Ausfall des Servers meist auch den Ausfall des gesamten Systems und damit zumindest des Unterrichts nach sich ziehen kann. Entsprechend hoch sind die an die Hardware gestellten Anforderungen.

- Da ein fehlerhafter Arbeitsspeicher zu unkontrollierbaren und schwer nachvollziehbaren Abstürzen des Servers führen kann, sollten Sie hier zu Markenprodukten greifen und vor der Installation ein Speicherprüfprogramm (wie Memory Test – siehe *Startbildschirm* auf Seite 17) mindestens 24 Stunden laufen lassen.
- SCSI–Platten sind für erhöhte Laufzeiten und für höhere Datendurchsatzt ausgelegt und meist langlebiger als vergleichbare IDE–Festplatten.
- Eine „Unterbrechungsfreie Stromversorgung“ (USV) stellt sicher, dass der Server bei einem plötzlichen Stromausfall noch geöffnete Daten speichern und den Betrieb ordnungsgemäß beenden kann. Außerdem werden zumeist auch schädliche Spannungsschwankungen gefiltert und die Hardware geschont. Achten Sie bitte beim Kauf einer USV darauf, dass der Server mittels Datenleitung vom Status der USV erfahren kann.
- Beachten Sie bitte die Wärmeentwicklung von Prozessor und Festplatten. Ein Wärmestau im Gehäuse sollte unbedingt vermieden werden!
- Bei der Installation in einem größeren Netzwerk sollten Sie über die Anbindung des Servers mit 1 GB–Netzwerkkarten nachdenken. Beachten Sie dabei aber, dass dann auch das Subsystem entsprechend ausgestattet sein sollte (RAID-System, viel RAM) und Ihr Switch über entsprechende Ports verfügt.

2.2 Die Netzwerkstruktur des Open School Servers

Der Open School Server ist nicht nur ein Produkt – er liefert ein fertiges Konzept für die Netzwerkverwaltung in Schulen.

Das Netzwerk wird in logische Segmente unterteilt. Die einzelnen Segmente entsprechen dabei den realen räumlichen Gegebenheiten der betreffenden Schule. Dadurch können die Arbeitsplatzrechner gezielt von den Lehrern kontrolliert werden

Aber nicht nur stationäre Rechner, auch mobile Geräte, externe Laptops und unbekannte Rechner können problemlos im Netzwerk betrieben werden – erhalten aber ohne „Erlaubnis“ des Administrators nur eingeschränkten Zugriff auf die vorhandenen Resourcen.

In der Abbildung 2.1 auf der nächsten Seite ist der grundlegende Netzwerkaufbau dargestellt. Das Schulnetz wird in mehrere logische Teilnetze unterteilt.

- Im ersten Teilnetz („Servernetz“) befinden sich die Server der Schule. Hier können Sie – je nach Wunsch – z. B. auch Netzwerkdrucker über eine entsprechende Subnetzmaske (255.255.255.0) so konfigurieren, dass diese nur noch über Freigaben des Open School Server erreicht werden können.
- Das zweite Teilnetz wird für neue bzw. provisorische Arbeitsplätze reserviert.
- In den weiteren Teilnetzen werden die stationären Arbeitsplätze der Schule geordnet unterbracht. Dazu wird jedem Schulraum ein eigener IP-Adressenbereich zugeordnet. Es ist sinnvoll nicht stationäre Rechner auch einem oder mehreren virtuellen Schulräumen zuzuordnen.

Diese Aufteilung des Netzwerkes ermöglicht einerseits die bequeme raumweise Sperrung der Dienste des Open School Servers, andererseits die Störungen im Netz schnell einzugrenzen.

2.2.1 Dienste des Open School Servers:

Achtung

Der Open School Server wird nach der Installation auch als DHCP– und Nameserver für Ihr Intranet eingerichtet. Sollten Sie schon interne DHCP–Server benutzen, schalten Sie diese bitte aus. Das Vorhandensein von zwei verschiedenen DHCP–Server in einem Netzwerk führt zu Fehlfunktionen.

Achtung

Der Open School Server bekommt nach der Installation vier verschiedene IP–Adressen. Damit kann einerseits der Zugriff auf die verschiedenen vom Open School Server bereitgestellten Dienste besser kontrolliert werden, andererseits lassen sich so bei Bedarf verschiedene Dienste auch auf andere Rechner auslagern. Diesen vier verschiedenen IP–Adressen werden verschiedene (DNS–)Namen zugewiesen, um die Zuordnung der hinter diesen Adressen laufenden Dienste zu erleichtern.

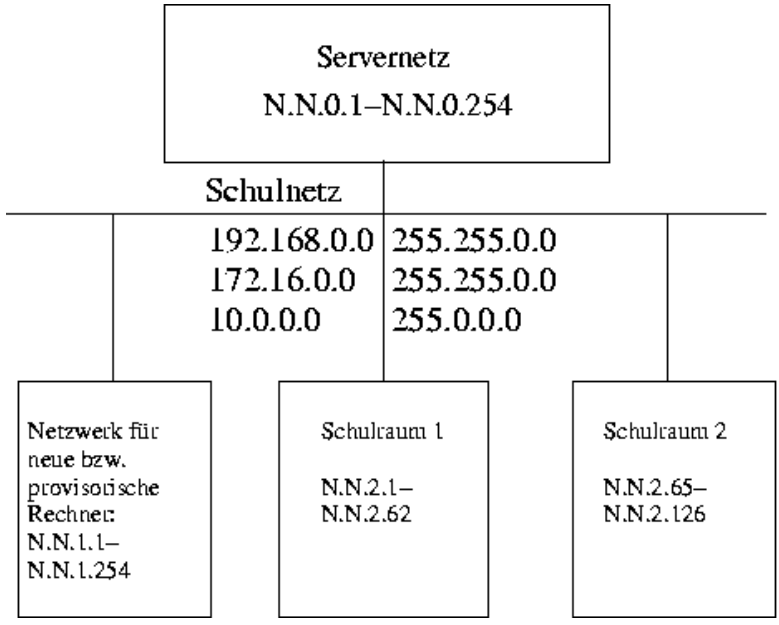

Abbildung 2.1: *Netzwerkstruktur des Open School Servers*

Erster Bereich:

- DNS-Namen: `admin`, `dns`, `nfs`, `ldap`, `samba`, `install`, `PDC-SERVER`
- Webserver für
  - die Selbstverwaltung der Benutzer
  - die Verwaltung des Schul-Servers bzw. –Netzes
  - die Verwaltung der Arbeitsplatzrechner
  - besondere Aktivitäten für Lehrer
- Fileserver (NFS/SAMBA)
- Passwortserver (LDAP/SAMBA)
- DHCP-Server
- Installationsserver für die automatische Installation und Verteilung von Updates von SUSE LINUX Clients
- Backupserver

Zweiter Bereich:

- DNS-Namen: `schulserver`, `mailserver`
- Mailserver (SMTP mit postfix, IMAP/POP3 mit Cyrus)
- Webserver für
  - Webmailer
  - Groupware
  - Zugriff auf die persönlichen Webseiten der Benutzer des Open School Servers

Dritter Bereich:

- DNS-Name: `printserver`
- Druckerserver

Vierter Bereich:

- DNS-Name: `Proxy`
- Proxyserver mit integriertem Filter für die Clients

2.3 Auswahl des Domainnamens

Bitte machen Sie sich vor der Installation Gedanken über den Domainnamen Ihrer Schule. Nach der Installation kann der Domainname nur noch mit großem Aufwand geändert werden. Überlegen Sie sich deshalb schon vor der Installation, wie Sie „Ihren Open School Server “ sinnvoll benennen.

Ein korrekt aufgesetzter Nameservice (DNS) ist für die einwandfreie Funktionsweise eines Mailservers von enormer Bedeutung und erleichtet die Administration des gesamten Systems. Auch wenn Sie keine offizielle Internet-Verbindung besitzen, d. h. nicht direkt vom Internet aus erreichbar sind, sollten Sie Ihrem Intranet einen vernünftigen Domainnamen zuweisen. Namen wie etwa „schulname.lokal“ sind wenig sinnvoll, da eine E-Mail, die mit `benutzer@schulename.lokal` als absender in das Internet geschickt wird, höchstwahrscheinlich von keinem Provider angenommen wird. Wie wäre es also z. B. mit `<schulname_stadt>.de` – auch wenn Sie derzeit noch keinen Email-Verkehr unter diesem Domainnamen haben? Das hat auch den Vorteil, dass einem späteren Internetauftritt nichts mehr im Wege steht.

Achten Sie aber darauf, dass der Name, den Sie verwenden möchten, nicht schon vergeben ist. Sie können mit jedem Webbrowser überprüfen, ob die gewünschte Domain bereits existiert, indem Sie den gewünschten Namen als URL (eventuell mit dem Vorsatz `www.`) eingeben.

Genauere Auskunft erhalten Sie bei einer der zuständigen Datenbanken:

Für `de`-Domains: `http://www.denic.de/index.html`
Für andere Domains: `http://www.internic.com/whois.html`.

Installation

Auf den folgenden Seiten wird die Installation und Grundkonfiguration des Open School Servers mit YaST erklärt. Wenn Sie auch nach der Lektüre dieses Kapitels nicht zum Ziel kommen, wenden Sie sich bitte an unseren Support. *Installations–Support* auf Seite 45

Achtung

Während der Installation werden für verschiedene Dienste des Servers Zertifikate erstellt. Wenn die Systemzeit während der Installation nicht korrekt ist (z. B. in der fernen Zukunft liegt), sind diese Zertifikate u.U. nicht gültig und ein korrekter Betrieb des Servers ist nur sehr schwer zu erreichen! Kontrollieren Sie deshalb bitte vor der Installation die Systemzeit im BIOS.

Achtung

3.1 Systemstart von CD–ROM

Schalten Sie Ihren Rechner ein und legen Sie die CD in das Laufwerk. Open School Server wird nun zur Installation geladen.

3.2 Startbildschirm

Der Startbildschirm zeigt mehrere Auswahlmöglichkeiten für den weiteren Verlauf der Installation. Ganz oben befindet sich die Option 'Boot from Harddisk', die das bereits installierte System bootet. Weil nach erfolgreicher Installation die CD häufig zum Nachinstallieren von Software eingelegt wird, ist diese Option vorgewählt. Für die Installation wählen Sie aber bitte 'Installation' mit den Pfeil–Tasten aus. Danach wird YaST2, das Systemkonfigurationswerkzeug von SUSE LINUX Enterprise Server, geladen und die Installation beginnt.

Die einzelnen Optionen im Startbildschirm bewirken folgendes:

Boot from Harddisk Bootet Ihr System von der Festplatte (jenes, das normalerweise beim Rechnerstart hochfährt). Diese Option ist vorgewählt.

Installation Die *normale* Installation, in der alle modernen Hardware–Funktionen aktiviert werden.

Installation – ACPI Disabled Wenn die normale Installation fehlschlägt, liegt dies möglicherweise daran, dass die System–Hardware mit der Unterstützung von ACPI „Advanced Configuration and Power Interface“ nicht zurecht kommt. Mit dieser Option können Sie in solchen Fällen ohne ACPI–Unterstützung installieren.

Installation – Safe Settings Die DMA–Funktion (für das CD–ROM–Laufwerk) und problematisches Powermanagement werden deaktiviert. Experten können zusätzlich Kernel–Parameter in der Eingabezeile mitgeben oder verändern.

Manual Installation Wenn bestimmte Treiber, die beim Start der Installation automatisch geladen werden, Probleme bereiten, können Sie hiermit *manuell* installieren, das heisst diese Treiber werden dann nicht automatisch geladen. Dies funktioniert allerdings nicht, wenn Sie an Ihrem Rechner eine USB–Tastatur benutzen.

Rescue System Falls Sie keinen Zugriff mehr auf Ihr installiertes Linux–System haben, starten Sie den Rechner mit dem eingelegten Installationsmedium neu und wählen Sie diesen Punkt. Es startet dann ein *Rettungssystem*, ein minimales Linux–System ohne grafische Oberfläche, mit dem Experten Zugriff auf die Festplatten haben und eventuelle Fehler des installierten Systems reparieren können. Wenn Sie sich mit Open School Server bzw. SUSE LINUX Enterprise Server noch nicht so gut auskennen, können Sie alternativ die YaST2–Systemreparatur verwenden. Details hierzu finden Sie im Kapitel *Das Rettungssystem* auf Seite 227.

Memory Test (nur x86–Plattform) Testet den Arbeitsspeicher Ihres Systems durch wiederholtes Beschreiben und Auslesen. Der Test läuft endlos, weil Speicherfehler oft sehr sporadisch auftreten und nur bei sehr vielen Schreib–Lese–Zyklen entdeckt werden können. Wenn Sie den Verdacht haben, dass der Arbeitsspeicher defekt sein könnte, lassen Sie diesen Test einige Stunden laufen; falls nach einiger Zeit keine Fehler gemeldet werden, können Sie davon ausgehen, dass der Speicher intakt ist. Der Test wird durch Neustart des Rechners beendet.

Entsprechend der Funktionstastenleiste am unteren Bildschimrand können Sie mittels der angegebenen F–Tasten verschiedene Einstellungen für die Installation vornehmen.

(F1) Hier erhalten Sie eine kontextsensitive Hilfe zum jeweils aktiven Element des Startbildschirms.

(F2) Auswählen verschiedener Grafik-Modi für die Installation. Sollten bei der grafischen Installation Probleme auftreten, kann hier auch der Text-Modus ausgewählt werden.

(F3) Auswählen verschiedener Installationsquellen. Normalerweise wird vom eingelegten Installationsmedium installiert. Hier können Sie jedoch auch andere Quellen wie zum Beispiel FTP und NFS auswählen. Besondere Erwähnung verdient hier *SLP* (Service Location Protocol). Bei Installation in einem Netzwerk mit SLP-Server können mit dieser Option vor der eigentlichen Installation die auf dem Server verfügbaren Installationsquellen ausgewählt werden. Weitere Informationen zu *SLP* finden Sie im Administrationshadbuch des SUSE LINUX Enterprise Servers im Abschnitt 'Dienste im Netz vermitteln'.

(F4) Hier können Sie die Sprache für die Oberfläche des Startbildschirms einstellen.

(F5) Normalerweise sehen Sie beim Systemstart keine Fortschrittsmeldungen des Linux-Kernels, sondern einen Fortschrittsbalken. Wenn Sie diese Meldungen sehen wollen, wählen Sie hier bitte 'Native', für noch mehr zusätzliche Ausgaben 'Verbose'.

(F6) Wenn Sie für SUSE LINUX eine Treiber-Update-Diskette erhalten haben, können Sie diese hier zur Anwendung bringen. Sie werden dann im Lauf der Installation aufgefordert, das Update-Medium einzulegen.

Bei der Installation lädt SUSE LINUX Enterprise Server einige Sekunden nach dem Startbildschirm ein minimales *Linux-System*, das den weiteren Installationsvorgang kontrolliert. Wenn Sie den Ausgabemode auf 'Native' oder 'Verbose' umgestellt haben, sehen Sie jetzt auf dem Bildschirm zahlreiche Meldungen und Copyright-Hinweise. Zum Abschluss des Ladevorgangs wird das Installationsprogramm YaST2 gestartet und nach wenigen Sekunden sehen Sie die grafische Oberfläche, die Sie durch die Installation führen wird.

3.3 YaST2 übernimmt die Arbeit

Jetzt beginnt die eigentliche Installation mit dem Installationsprogramm YaST2. Die Bildschirmansichten von YaST2 folgen einem einheitlichen Schema: alle Eingabefelder, Auswahllisten und Buttons der YaST2-Bildschirme können Sie mit der Maus steuern.

Bewegt sich der Cursor nicht, wurde Ihre Maus nicht automatisch erkannt. Verwenden Sie in diesem Fall zunächst die Tastatur und bewegen Sie sich bitte mit den Pfeiltasten und der (Tab)-Taste bis zum gewünschten Menüpunkt. Drücken Sie anschließend die (↵)-Taste. Die Einrichtung der Maus finden Sie im Abschnitt 3.4.3 auf der nächsten Seite.

3.3.1 Sprachauswahl

YaST2 stellt sich zur Installation auf die von Ihnen gewünschte Sprache ein. Die Spracheinstellung, die Sie hier wählen, wird auch für Ihr Tastaturlayout übernommen. Außerdem stellt YaST2 eine Standardzeitzone ein, die für Ihre Spracheinstellung wahrscheinlich ist.

3.4 Installationseinstellungen

Nach der Hardwareerkennung (und ggf. der manuellen Mauseinrichtung) erhalten Sie Informationen über die erkannte Hardware und Vorschläge zur Installation und Parti-

tionierung, das sog. Vorschlagsfenster. Wenn Sie ein Modul anklicken und konfigurieren, gelangen Sie anschließend immer wieder in das Vorschlagsfenster mit den jeweils geänderten Werten zurück. Im Folgenden werden die einzelnen Konfigurationseinstellungen, die Sie vornehmen können, beschrieben.

3.4.1 Modus

Dieser Punkt sollte immer auf 'Neuinstallation' stehen. Machen Sie hier bitte keine Änderungen.

3.4.2 Tastaturbelegung

Wählen Sie in dieser Maske das gewünschte Tastaturlayout aus. In der Regel entspricht es der gewählten Sprache. Drücken Sie anschließend im Testfeld die Tasten Ü oder Ä, um deren richtige Darstellung zu prüfen. Werden diese nicht richtig angezeigt, stimmt die Tastaturbelegung nicht.

Mit 'Weiter' gelangen Sie wieder zu den Vorschlägen zurück.

3.4.3 Maus

Sollte YaST2 die Maus nicht automatisch erkannt haben, so bewegen Sie zuerst den Fokus mit der Tab-Taste, bis der Button 'Ändern' markiert ist, drücken dann die Leertaste und anschließend die Pfeiltasten zu dem Menüpunkt 'Maus'.

Verwenden Sie zur Auswahl des Maustyps die Tasten ↑ und ↓. Falls Sie eine Dokumentation zu Ihrer Maus besitzen, finden Sie dort eine Beschreibung 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. Folgt der Mauszeiger am Bildschirm Ihren Bewegungen, war dieser Installationsschritt erfolgreich. Falls sich der Zeiger nicht bewegt, wählen Sie einen anderen Maustyp und wiederholen Sie den Versuch.

Mit 'Übernehmen' werden die Einstellungen gespeichert und Sie gelangen wieder zurück ins Vorschlagsfenster.

3.4.4 Partitionierung

Während der Installation des Open School Servers macht Ihnen der Partitionierer von YaST2 einen Vorschlag, der im allgemeinen eine vernünftige Wahl darstellt und nicht abgeändert werden muss.

Achtung

Beachten Sie, dass der Partitionierer normalerweise *alle* im System installierten Festplatten für die Verwendung mit dem Open School Server einrichtet. Daten, welche sich auf diesen Festplatten befinden, werden bei der Installation gelöscht!

Möchten Sie den Open School Server parallel zu einem anderen System installieren, müssen Sie also die Partitionierung manuell vornehmen!

Achtung

Möchten Sie die Partitionierung selber vornehmen, lesen Sie die nächsten Kapitel, andernfalls können Sie mit dem Kapitel *Software* 3.4.5 auf Seite 24 fortfahren.

Hinweis

Wenn Sie die Imaging-Lösung des Open School Server und/ oder die Autoinstallation nutzen möchten, achten Sie bitte darauf, dass die Partition auf der sich das Verzeichnis `/srv` befindet ausreichend groß ist. Normalerweise handelt es sich dabei im das `/` Verzeichnis.

Sollten Sie von einer dieser Lösungen (Imaging, Autoinstallation) oder gar von beiden Gebrauch machen wollen, kann es sinnvoll sein für das `/srv`-Verzeichnis eine extra Partition zu erstellen.

Als ungefähren Anhaltspunkt für die Größe dieser Partition können Sie für die Autoinstallation ca. 9 GB insgesammt und bei der Imaging-Lösung ca. 2 GB pro Clientimage vorsehen.

Hinweis

Der Partitionierer von YaST2

Wenn Sie die Partitionierung manuell vornehmen, können Sie sie Ihren persönlichen Gegebenheiten anpassen. Wenn Sie z. B. zu Testzwecken verschiedene Versionen oder Betriebssysteme nebeneinander installieren oder später einmal mittels LVM Ihre Partition (auch über die Festplatte hinaus) erweitern möchten, dann werden Sie nicht um eine manuelle Partitionierung herumkommen.

Wenn Sie den Open School Server zu Testzwecken neben einem anderen Betriebssystem auf Ihrer Festplatte installieren wollen, beachten Sie bitte, dass Sie mindestens drei Partitionen anlegen (`swap`; `/(root)` und `/home`) und für `/home` die Fstab-Optionen `acl,usrquota,defaults` nicht vergessen.

Manuelle Partitionierung

Wählen Sie das Modul 'Partitionierung' aus. Nun wird Ihnen angeboten, den Vorschlag von YaST2 abzuändern oder eine eigene Partitionierung anzulegen.

Im Menü ‘Partitionen nach eigenen Vorstellungen anlegen’ werden zunächst alle im System gefundenen Festplatten angezeigt. An dieser Stelle wählen Sie den Menüpunkt ‘Erweiterte Einstellungen, manuelle Aufteilung (Partitionierung)’ um die gefundenen Festplatten manuell zu partitionieren.

YaST2 listet alle vorhandenen Partitionen der gefundenen Festplatten auf (Abbildung 3.1). An dieser Stelle können Sie von Hand Partitionen erstellen, bearbeiten oder löschen. Weiterhin ist es möglich, den LVM (Logical Volume Manager) zu konfigurieren oder ein Software–RAID anzulegen. Lesen Sie bitte dazu die entsprechenden Kapitel des SUSE LINUX Enterprise Server Handbuches. (Kapitel 3.10 bzw. 3.11).

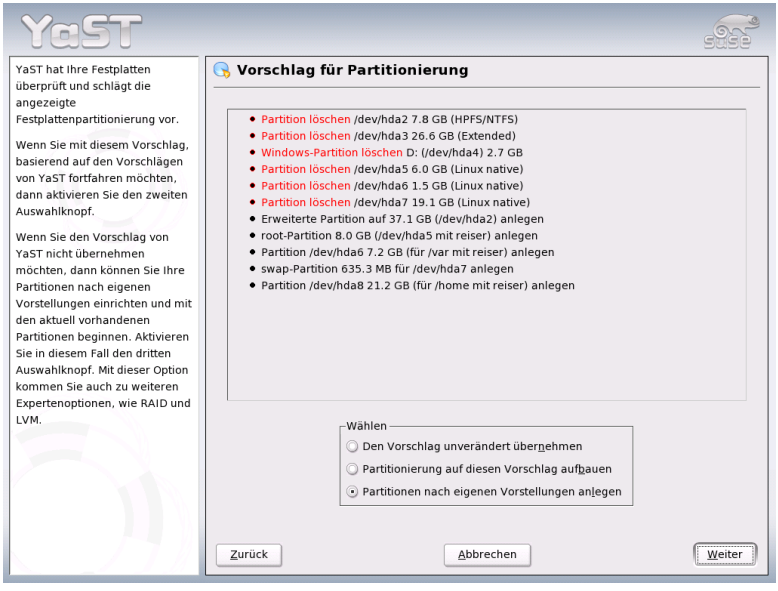

Abbildung 3.1: *Der Partitionierer des Open School Servers*

Partitionstypen

Da der Open School Server im Normalfall nur 4 Partitionen benötigt, können Sie ruhig primäre Partitionen verwenden. Brauchen Sie weitere Partitionen, sollten Sie eine erweiterte Partition zuerst anlegen.

Als Format empfehlen wir das Filesystem `Ext3`.

Sie müssen nun folgende Partitionen mit den hier erläuterten Parametern anlegen und konfigurieren.

swap Diese Partition dient zum zeitweisen Auslagern von RAM-Speicherinhalten. Wählen Sie diesen Bereich so groß wie der Speicher in Ihrem Rechner ist. (siehe Abbildung 3.2)

Abbildung 3.2: *Anlegen einer swap-Partition*

/ Das Wurzelverzeichnis des Systems. Als Größe sollten in normal Fall 4 GB reichen. Weiterhin müssen ggf. die Installations–CDs der aktuellen SUSE LINUX Distribution in ein Unterverzeichnis (`/srv/tftp/akt`) auf dieser Partition kopiert werden, um SUSE LINUX Clients automatisch zu installieren . In diesem Fall müssen Sie noch mit zusätzlich ca. 7 GB rechnen.

/var In diesem Verzeichnis befinden sich vor allem die Spoolverzeichnisse des Drucksystems, die Emails der Benutzer und die Benutzerdatenbank. Deshalb ist es sinnvoll, dieses Verzeichniss auf eine separate Partition zu legen.

Die Größe dieser Partition wird in erster Linie durch die Anzahl und Größe der Mailboxen bestimmt. Sind in Ihrer Schule z. B. 800 Schüler und 80 Lehrer, werden die Mailboxen der Lehrer auf 25 MB und die der Schüler auf 5 MB begrenzt. So sind Sie in unserem Beispiel mit einer Partitiongröße von

```
(800 * 5 MB) + (80 * 25 MB) + 4GB = 10 GB
```

auf der sicheren Seite.

/home Hier werden die Dateien der Benutzer gespeichert. Die Praxis zeigt, dass diese Partition nie groß genug sein kann. Am besten verwendet man dafür aus Performancegründen eine eigene Festplatte.

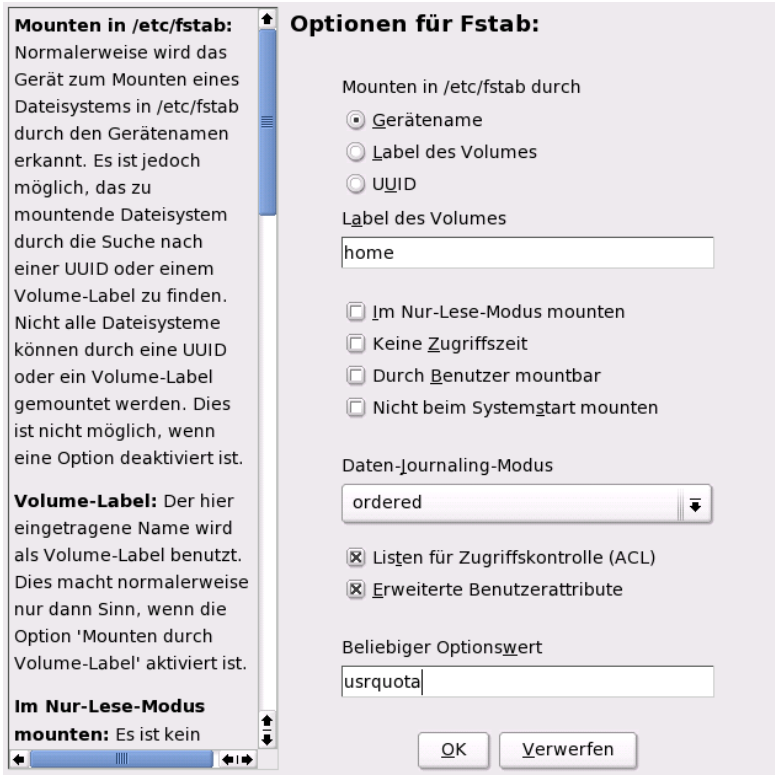

Abbildung 3.3: *Setzten der Filesystemoptionen der /home–Partition*

Hinweis

Für die `/` und `/var` und `/home`–Partitionen müssen die sog. „Fstab Optionen“ ‘Listen für Zugriffskontrolle (ACL)’ bzw. ‘Erweiterte Benutzerattribute’ aktiviert sein. Weiterhin ist es empfehlenswert als ‘Label des Volumes’ `root`, `var` bzw. `home` zu setzen. Für die `/home`–Partition muss im Feld ‘Beliebiger Optionswert’ folgender Wert eingetragen werden: `usrquota`.

Hinweis

In den folgenden Tabellen finden Sie als Beispiel einen Vorschlag zur sinnvollen Partitionierung des Open School Servers:

Partition	Mountpoint	Größe	Format
Beispiel für die Partitionierung einer EIDE Festplatte			
/dev/hda1		1GB	swap
/dev/hda2	/	8GB	Ext3
/dev/hda3	/var	5GB	Ext3
/dev/hda4	/home	Der Rest	Ext3

3.4.5 Software

Da der Open School Server eine fertig konfigurierte Softwareauswahl mitbringt, können hier keine Änderungen gemacht werden. Um die Systemintegrität zu gewährleisten, sollten auf dem Open School Server auch später keine weiteren Pakete installiert werden. Damit Ihr System sicher und stabil läuft werden Sie immer benachrichtigt, wenn evtl. Bugfixes oder Securitypatches einzuspielen sind.

Sie sollten sich speziell für diese Informationen eine eigene Email-Adresse einrichten und diese bei der Registrierung Ihres Open School Servers angeben, damit Sie immer die aktuellsten Meldungen erhalten können.

3.4.6 Systemstart

Hier können Sie spezielle Einstellungen zum Bootloader GRUB vornehmen. Für eine Standardinstallation sind keine Änderungen erforderlich.

Hinweis

Das Ändern des Boot-Modus ist nur Experten zu empfehlen, da der Rechner bei falscher Konfiguration nicht mehr bootet.

Hinweis

3.4.7 Zeitzone

In dieser Maske wählen Sie Ihre Zeitzone und geben die Einstellung der Rechneruhr an. Im Feld 'Rechneruhr einstellen auf' wählen Sie zwischen `Lokalzeit` und `GMT`. Bitte richten Sie sich dabei nach der Uhreinstellung im BIOS Ihres Rechners.

Sollte diese auf `GMT` stehen, übernimmt Open School Server automatisch die Umstellung von Sommer- auf Winterzeit und umgekehrt.

3.4.8 Sprache

Hier können Sie die Sprache auswählen, mit welcher das spätere System installiert wird. Hier ist standardmäßig die von Ihnen beim Einrichten von YaST2 gewählte Sprache voreingestellt.

3.4.9 Installation starten

Mit Klick auf 'Weiter' nehmen Sie den Installationsvorschlag mit allen von Ihnen gemachten Änderungen an und gelangen in eine Bestätigungsmaske. Wenn Sie hier 'Ja' wählen, geht es wirklich los mit der Installation. Die Installation dauert je nach Rechnerleistung meist zwischen 15 und 30 Minuten.

3.5 System konfigurieren

Nachdem die Softwarepakete fertig installiert sind und der Open School Server neu gebootet wurde, müssen Sie noch einige wichtige Einstellungen vornehmen, damit Sie mit dem Server arbeiten können.

3.5.1 Root–Passwort

`Root` ist der Name für den `Administrator` des Systems. Er kann das System verändern, neue Programme für alle Benutzer einspielen oder neue Hardware einrichten. Weiterhin wird das hier eingegebene Passwort für folgende Benutzer, die während der Installation angelegt werden, zugewiesen:

`admin` Administrator des Open School Servers. Dessen Passwort können Sie später mit der Administrationsoberfläche ändern.

`cyrus` Der Administrator des Mailsystemes.

`CA-Administrator` Der Administrator der Zertifikaten.

`rootdn` RootDN oder auch BindDN gennant ist der Hauptadministrator des LDAP-Servers.

Die Templatebenutzer Während der Installation werden sog. „Templatebenutzer" für die Verwaltung von Benutzerprofilen angelegt. Diese Benutzer erhalten auch das Rootpasswort.

Achtung

Der Benutzer `root` hat alle Rechte und darf sämtliche Veränderungen am System vornehmen. Wenn Sie solche Aufgaben durchführen wollen, benötigen Sie das für `root` vergebene spezielle Passwort. Ohne dieses Passwort können Sie keine administrativen Aufgaben mehr durchführen!

Achtung

Im Allgemeinen sollte man als `root` nur für administrative Aufgaben, Wartungs- und Reparaturarbeiten am Rechner angemeldet sein. Für den Alltagsbetrieb ist das zu riskant, da `root` z. B. sämtliche Dateien unwiederbringlich löschen kann.

Bei der Passwortvergabe für `root` muss das Passwort zur Überprüfung zweimal eingegeben werden. Sie sollten hier ein komplexes Passwort verwenden, das sich aus Zahlen, Groß- und Kleinbuchstaben sowie evtl. Sonderzeichen (beachten Sie aber unterschiedliche Tastaturlayouts) zusammensetzt.

Tipp

Verwenden Sie *nie* Passwörter, die Sie auch in einem mehrsprachigen Wörterbuch wiederfinden könnten! Auch persönliche Daten und Namen, die Ihnen bekannte Personen erraten könnten, eignen sich nicht als Passwort.

Tipp

Merken Sie sich das Passwort für den Benutzer `root` besonders gut. Es kann zu einem späteren Zeitpunkt nicht wieder eingesehen werden.

Da es im Schulalltag durchaus vorkommen kann, dass der eigentliche Administrator längere Zeit nicht erreichbar ist oder das System über längere Zeit nicht warten muss (und dabei das Passwort vergisst), haben wir am Ende des Buches einen kleinen „Merkzettel“ abgedruckt (siehe Abschnitt J.2 auf Seite 254), den Sie als Vorlage nutzen sollten, um die wichtigsten Daten und Passwörter Ihres Systems zu notieren.

Hinterlegen Sie diesen – durch einem dicken, verschlossenen Umschlag geschützten – Zettel an einem absolut sicheren Platz in der Schule und informieren Sie auch die Schulleitung über den Lagerort. Im Notfall gibt es dann zumindest eine kleine Hilfe für den z. B. aus der Nachbarschule herbeigerufenen Admin.

Ändern Sie das Passwort für `root` regelmäßig und tragen Sie dieses geänderte Passwort (mit Datum) auch auf diesem Zettel ein. Einerseits haben Sie so eine gute Kontrolle darüber, dass bis dahin niemand den „Notfall-Brief“ geöffnet hat und andererseits verbessern Sie damit die Sicherheit des Systems.

3.5.2 Netzwerkkonfiguration

Die Konfiguration des Netzwerks ist im Falle des Open School Servers wesentlich komplexer als bei einem Arbeitsplatzrechner.

Sollten Sie sich bislang noch keine Gedanken über die Netzwerkstruktur Ihrer Schule gemacht haben, sollten Sie spätestens jetzt damit beginnen! Wir würden Ihnen auf jeden Fall empfehlen, alle Server (auch Netzwerkdrucker gehören dazu) der Schule in einem eigenen Teilnetz zu sammeln, welches durch eine passende Subnetzmaske von den anderen Netzwerkbereichen abgetrennt ist. So können Sie später ganz gezielt den Clients Zugriff auf bestimmte Serverdienste gestatten.

Achtung

Bitte achten Sie darauf, dass Sie während der Installation die korrekten Schnittstellen für das interne Netzwerk und den Zugang zum Internet angeben, da im Anschluß an die Konfiguration automatisch die eingebaute Firewall konfiguriert und gestartet wird, um den Server vor Angriffen aus dem Internet zu schützen.

Achtung

Interne Netzwerkkarte konfigurieren – Schulnetz

Nachdem das Root-Passwort gesetzt ist, gelangen Sie zu dem in Abbildung 3.4 auf der nächsten Seite dargestellten Bildschirm. Hier wählen Sie zunächst diejenige Netzwerkkarte aus, die mit Ihrem internen Schulnetzwerk verbunden ist.

Üblicherweise wird der richtige Treiber für Ihre Netzwerkkarte schon während der Installation von YaST2 konfiguriert. Daher sind manuelle Einstellungen der Hardwareparameter nur nötig, wenn die Netzwerkhardware nicht automatisch erkannt wird. In diesem Fall müssen Sie den Punkt 'Hinzufügen' anwählen, damit ein neues Treibermodul ausgewählt werden kann.

Für das Schulnetz wurden drei Netzwerkmodelle bereits bis ins Detail vorkonfiguriert:

- `10.0.0.0/8`
- `172.16.0.0/16`
- `192.168.0.0/16`

Andere Netzwerkbereiche kann man gleichfalls wählen, diese müssen jedoch manuell eingetragen werden. Akzeptiert man die Standardeinstellungen, muss in diesem Menü lediglich der Domainname der Schule eingetragen werden.

Beachten Sie bitte, dass es sich bei der Vorauswahl um „IP-Nummern für lokale Netze" handelt: Diese IP-Adressen werden nicht im Internet verwendet und auch nicht weitergeleitet. Damit ist sichergestellt, dass es zu keinerlei Adresskonflikten mit „richtigen" IP-Internet-Adressen kommt.

Sollten Sie hier andere Adressbereiche wählen, müssen Sie selbst sicherstellen, dass es bei der Nutzung des Internets weltweit keine anderen Rechner mit derselben IP-Adresse gibt.

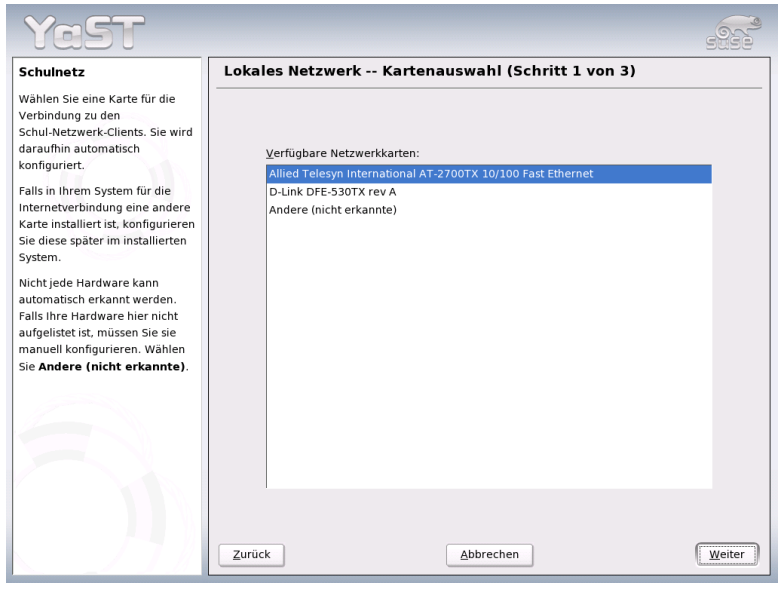

Abbildung 3.4: *Interne Netzwerkkarte auswählen*

Der erste Adressbereich ermöglicht es, ein sehr großes lokales Netz zu bilden (theoretisch mit bis zu 16 Millionen Rechnern). Wenn Sie hier die Subnetzmaske einschränken (z. B. auf 255.255.0.0), so können Sie auch mehrere Schulen miteinander vernetzen, indem Sie jeder Schule einen eigenen Bereich innerhalb dieses verkleinerten Subnetzes zuordnen und dem Hauptserver über eine alle Bereiche umfassende Subnetzmaske wiederum den Zugriff auf diese Teilnetze ermöglichen.

Wenn Sie z. B. die Konfiguration für das 172er Netzwerk übernehmen, wird der Open School Server folgendermassen konfiguriert:

IP-Adresse z. B. `172.16.0.2`;
DNS-Namen: `admin, dns, nfs, ldap, samba, PDC-SERVER, gateway, timeserver`

Subnetzmaske z. B. `255.255.0.0` *Eine engere Netzwerkmaske als 255.255.240.0 wird von dem Open School Server nicht akzeptiert, da sonst keine IP-Adressen für die Schulräume zur Verfügung stehen.*

IP-Adresse des Mailservers z. B. `172.16.0.3`;
DNS-Namen: `schulserver, mailserver, schoolserver`

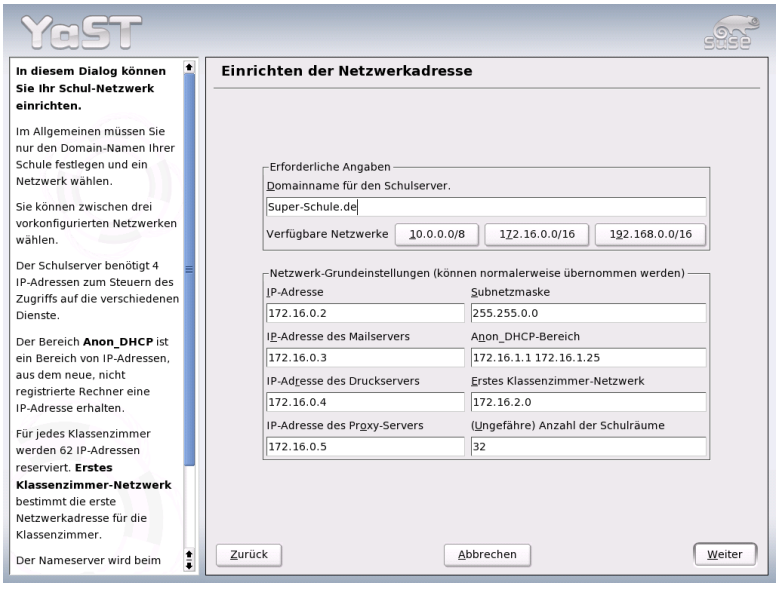

Abbildung 3.5: *Internes Netzwerk konfigurieren*

IP-Adresse des Druckservers z. B. `172.16.0.4`;
DNS-Name: `printserver, install`

IP-Adresse des Proxy-Servers z. B. `172.16.0.5`;
DNS-Name: `proxy`

`Anon_DHCP-Bereich` „DHCP-Bereich für nicht registrierte Rechner“. Aus diesem IP-Adressenbereich bekommen neue bzw. nicht registrierte Rechner ihre IP-Adressen.

Der Standardbereich ist z. B.: `172.16.1.1 bis 172.16.1.25`

Alle Rechner des IP-Adressenbereiches für nicht registrierte Rechner werden in den Nameserver mit folgendem Namen eingetragen:

`dhpc1 - dhcp254.<domainname.der.schule>`.

`Erstes Klassenzimmer` Aus diesem IP-Adressenbereich bekommen registrierte Rechner des ersten Klassenraumes ihre IP-Adressen (z. B. `172.16.2.1 bis 172.16.2.64`).
Weitere Klassenräume werden entsprechend angelegt (siehe Grafik 2.1 auf Seite 12).

(Ungefähre) Anzahl der Schulräume Für jeden Schulraum wird eine sog. DHCP-Gruppe und ein IP-Adressenbereich von 62 IP-Adressen reserviert. Hier geben Sie bitte die ungefähre Anzahl der Schulräume, in denen sich Computer befinden, an. Auch später ist es möglich weitere DHCP-Gruppen bzw. IP-Adressenbereiche über die DHCP-Konfigurationsoberfläche zu reservieren, es erfordert jedoch tiefergehende Kentnisse, deshalb sollten Sie hier lieber großzügiger sein.

Internet Verbindung einrichten

Nun kommen Sie zur Einrichtung des Internet Zugangs . Hier wählen Sie die Art und Weise, wie Sie mit dem Open School Server an das Internet angebunden sind.

In der Abbildung 3.6 auf Seite 32 sehen Sie die 3 Möglichkeiten, wie das Schulnetzwerk mit dem Internet verbunden werden kann.

a) Anbindung über ein Transportnetz mit dem Internet Das ist die sicherste Methode für die Anbindung eines Schulnetzes an das Internet. Sie erhalten alle Kontrollmöglichkeiten, die der Open School Server anbietet. Lediglich die DynDNS-Konfiguration wird nicht verfügbar sein. Viele der gängigen Hardware-Router bieten jedoch heutzutage diesen Dienst selber an.

Sie müssen darauf achten, dass die IP-Adressenbereiche des Transportnetzes und des Schulnetzes sich nicht überschneiden und der Router (Firewall) ausschließlich dem Open School Server einen unbeschränkten Internetzugang bei gleichzeitigem Schutz vor Angriffen gewährleistet.

b) Schulserver ist direkt mit dem Internet verbunden Der Schutz des Schulnetzes wird durch das SuSE Firewallscript gewährleistet. Sie erhalten alle Kontrollmöglichkeiten, die der Open School Server anbietet.

Bitte beachten Sie, dass auch bei einer Internetverbindung via ISDN, DSL oder Modem mit dynamischen IP-Adressen die Gefahr für unerwünschte Zugriffe aus dem Internet besteht. Im Falle einer Standleitung raten wir von einer direkten Internetanbindung auf jeden Fall ab.

c) Internetgateway befindet sich im Schulnetzwerk In diesem Fall ist der Schutz des Schulnetzes davon abhängig, wie gut der Router (Firewall) konfiguriert ist. Sie müssen dafür sorgen, dass die Clients den Internetgateway nur dann erreichen können, wenn Sie es ausdrücklich wünschen. Weiterhin müssen Sie darauf achten, dass der Router (Firewall) dem Schulserver einen unbeschränkten Internetzugang bei gleichzeitigem Schutz vor Angriffen aus dem Internet gewährleistet.

Bei dieser Art von Internetverbindung können Sie folgende Funktionen des Open School Server nicht einsetzen:

- DynDNS-Konfiguration .
- Direkten Internetzugang erlauben/verbieten .

Weiterhin müssen Sie ggf. den externen Zugriff für den Open School Server auf den Internetgateway konfigurieren.

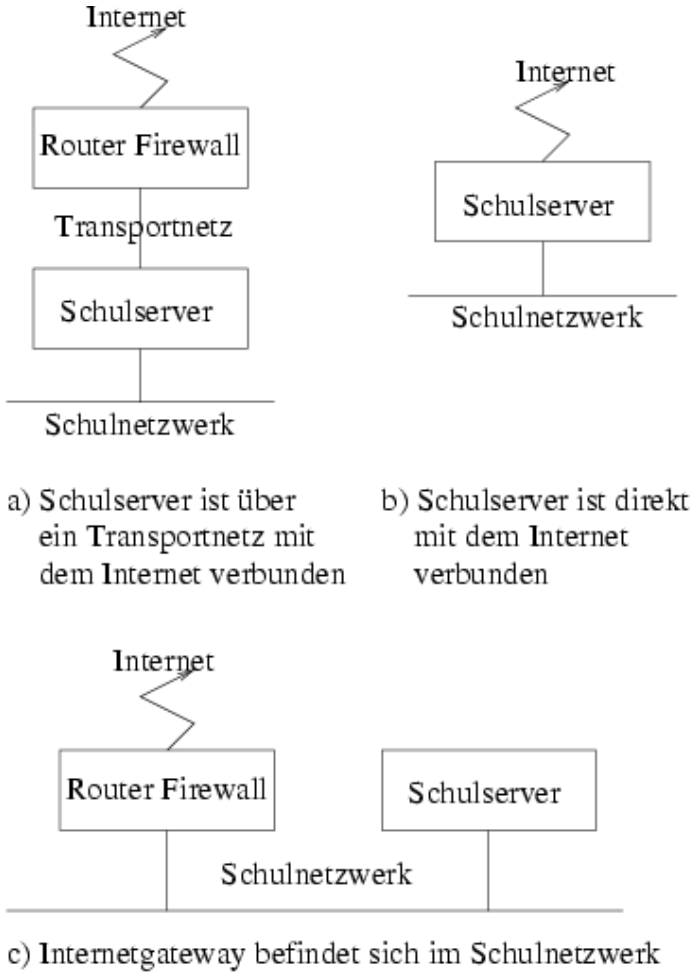

Abbildung 3.6: *Verschiedene Internetanbindungsmöglichkeiten*

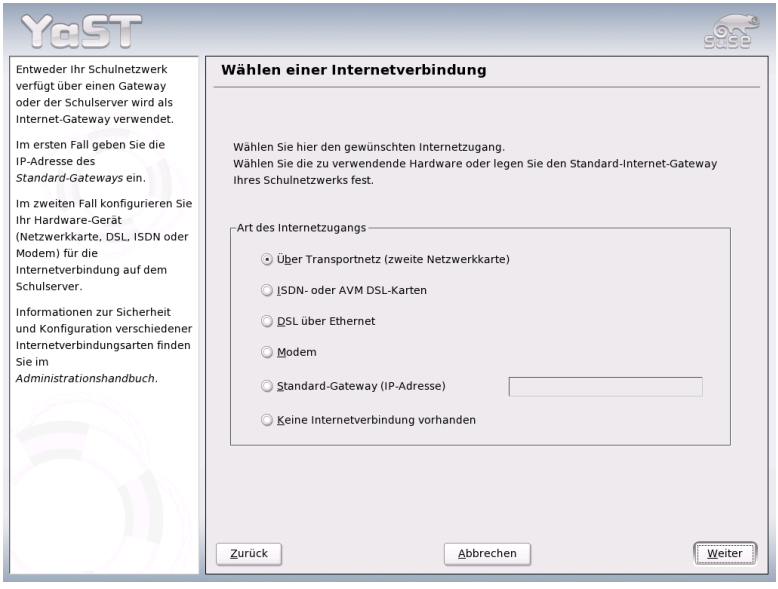

Abbildung 3.7: *Internetverbindung einrichten*

Wählen Sie also die entsprechende Hardware für die Internetverbindung aus oder geben Sie die IP–Adresse des Standard–Gateways in Ihrem Schulnetzwerk ein (siehe Abbildung 3.7 auf der vorherigen Seite).

Über Transportnetz (zweite Netzwerkkarte) Wählen Sie nun die Netzwerkkarte für die Internetverbindung aus und konfigurieren Sie das Transportnetz. Da einige Dienste die externe IP-Adresse des Open School Servers benötigen, ist es nicht möglich, die externe IP-Adresse des Open School Servers über DHCP zu beziehen.

Hinweis

Nachträgliche Änderung fester IP-Adressen

Sollten Sie später einmal die eingegebene „statische“ Adresse ändern wollen, so nutzen Sie hierfür auch wieder das YaST2-Modul ‘Netzwerk’ und ändern dort die IP-Adresse ab. Zusätzlich müssen Sie in der Datei `/etc/rinetd.conf` die alte Adresse gegen die neue austauschen.

Hinweis

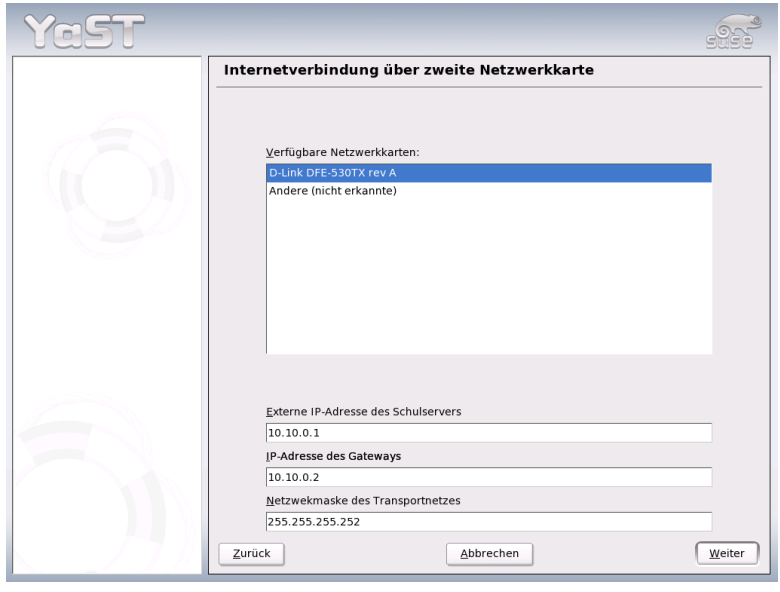

Abbildung 3.8: *Internet Verbindung über Netzwerkkarte*

ISDN– oder AVM DSL–Karten Wenn Sie über eine ISDN–Verbindung oder eine interne AVM DSL–Karte ins Internet gehen, wählen Sie bitte diesen Menüpunkt und folgen Sie den Anweisungen auf dem Bildschirm.

Normalerweise sollte Ihre ISDN–Karte automatisch erkannt werden. Ist dies nicht der Fall, wählen Sie sie bitte im oberen Fenster aus. Informationen für die richtige Konfigurationseinstellungen Ihrer Internetverbindung entnehmen Sie bitte aus dem nächsten Punkt 'DSL'.

DSL Um DSL nutzen zu können, muss eine separate Netzwerkkarte im Open School Server installiert werden. Wählen Sie bitte diesen Menüpunkt und folgen Sie den Anweisungen auf dem Bildschirm. In mehreren Dialogen haben Sie hier die Möglichkeit, die Kenndaten Ihres DSL–Zugangs einzugeben. Mit YaST2 können Sie DSL–Zugänge einrichten, die auf den folgenden Protokollen aufsetzen:

- PPP über Ethernet (PPPoE) – Deutschland
- PPP über ATM (PPPoATM) – England
- CAPI für ADSL (Fritz–Karten)
- Tunnelprotokoll für Point–to–Point (PPTP) – Österreich

Wichtig sind folgende Einstellungen:
Schritt 1:

PPP-Modus Wählen Sie hier bitte den in Ihrem Land üblichen PPP-Modus

Ethernetkarte Wählen Sie hier die Netzwerkkarte aus, die Sie für die DSL-Verbindung verwenden möchten. Beachten Sie bitte, dass die Konfiguration Ihres DSL–Zugangs mit PPPoE und PPTP eine korrekte Konfiguration Ihrer Netzwerkkarte voraussetzt. Mit 'Netzwerkkarten konfigurieren' kommen Sie direkt zum entsprechenden Dialog. Die automatische IP-Adressenvergabe findet bei DSL nicht mit dem DHCP–Protokoll statt. Deshalb dürfen Sie nicht 'Automatische Adressvergabe (mit DHCP)' wählen. Vergeben Sie stattdessen bitte eine statische Dummy–IP–Adresse aus einem anderem Netzwerkbereich als Ihr Schulnetz. (z. B. 192.168.0.1 mit Netzwerkmaske 255.255.255.0 falls Sie das Netzwerkmodell 10.0.0.0 oder 172.16.0.0 gewählt haben).

Geräte-Aktivierung Stellen Sie hier 'Beim Booten' ein.

In den Schritten 2 und 3 stellen Sie Ihre Provider– bzw. Zugangsdaten ein.

Im Schritt 4 stellen Sie bitte folgende Parameter ein:

'Dial-On-Demand'	An
'Während Verbindung DNS Ändern'	Aus
'DNS automatisch abrufen'	Aus
'Firewall aktivieren'	An
'Verbindung abbrechen nach . . . '	1800 (oder mehr)

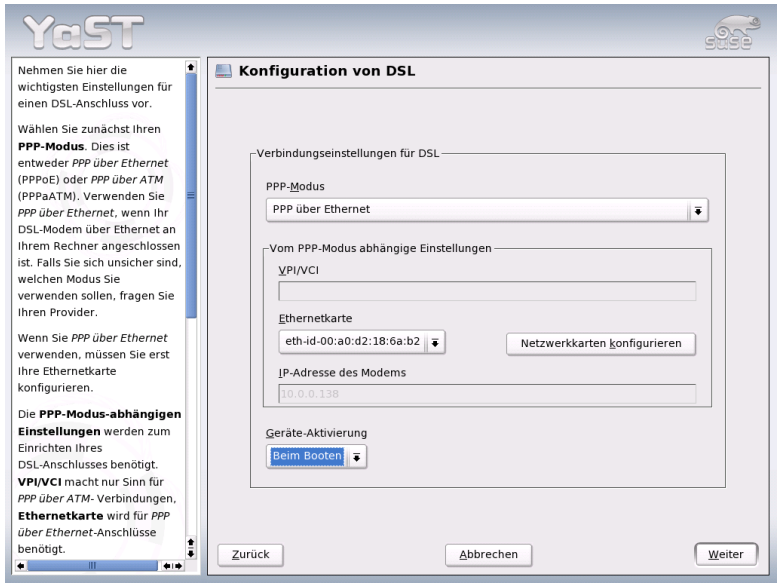

Abbildung 3.9: *Internet Verbindung über DSL Schritt 1*

Hinweis

Wenn Sie die DSL, ISDN oder Modem Einstellungen in dem konfigurierten System ändern, vergessen Sie nicht die Variabeln `REJECT_ALL_INCOMING_CONNECTIONS` in der Datei `/etc/sysconfig/personal-firewall` auf `no` zu setzten.

Hinweis

Die Frage, ob nun das Email-System konfiguriert werden soll, können Sie mit `Nein` beantworten. Der Mailserver des Open School Server wird automatisch konfiguriert.

Modem Hier können Sie ein Modem konfigurieren, das an einer seriellen Schnittstelle angeschlossen ist. Bitte beachten Sie, dass es heute kaum noch Sinn macht, ein Modem in einer größeren Schulumgebung als einzigen Internetzugang zu nutzen.

Default–Gateway Sollten Sie z. B. einen Hardwarerouter für Ihren DSL-Zugang verwenden, welcher über einen Switch oder HUB direkt mit Ihrer Netzwerkkarte für das interne Netzwerk verbunden ist, so geben Sie als Standardgateway hier

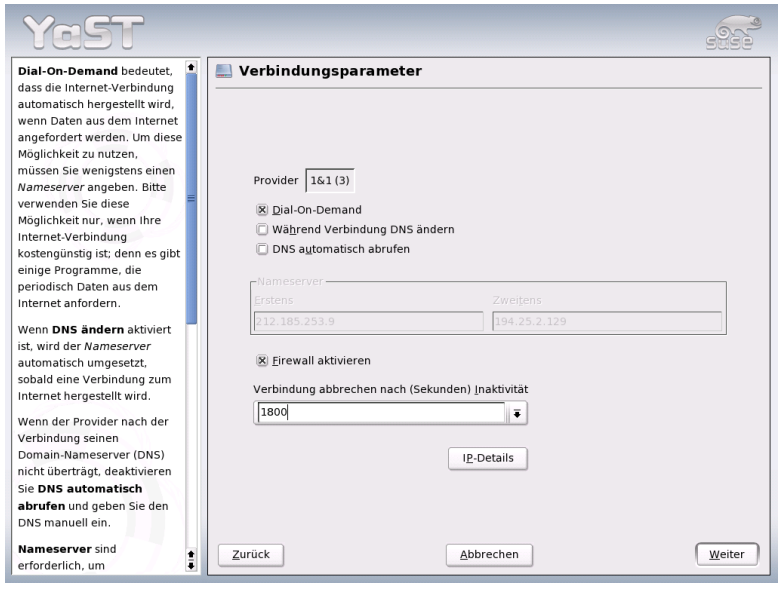

Abbildung 3.10: *Internet Verbindung über DSL Schritt 4*

dessen interne Adresse an.

Bitte beachten Sie, dass Hardwarerouter oftmals einen eingebauten DHCP-Server haben, der sich nicht mit dem im Open School Server integrierten verträgt. Schalten Sie in diesem Fall bitte den DHCP-Server des Hardwarerouters ab.

Kein Internetzugang Wenn der Server nur für den internen Gebrauch bestimmt ist und keine Internetdienste nutzen soll, dann wählen Sie diesen Menüpunkt. Ein Zugriff auf das Internet über den Open School Server ist dann nicht möglich. Die Firewall wird in diesem Fall nicht konfiguriert.

Bitte klicken Sie zum Abschluss auf 'Weiter', um die Installation fortzusetzen. Nun wird zuerst der entsprechende Internetzugang eingerichtet und anschließend die Firewall des Servers so konfiguriert, dass dieser vor Zugriffen von außen einigermaßen geschützt ist.

Achtung

Wir möchten Sie ausdrücklich darauf hinweisen, dass es zwar durchaus möglich, generell aber keine gute Idee ist, den Open School Server direkt an das Internet anzuschließen. Trotz der Firewall sind hier Angriffe von außen möglich. Besser ist in jedem Fall ein separater Internetzugang über einen Router oder eine Firewall (Internetverbindung über Transportnetz).

Achtung

3.5.3 Netzwerkdienste

Nach der Konfiguration der Netzwerkverbindungen gelangen Sie in einen Dialog zur Aktivierung und Konfiguration zweier wichtiger Netzwerkdienste (siehe Abb. 3.11).

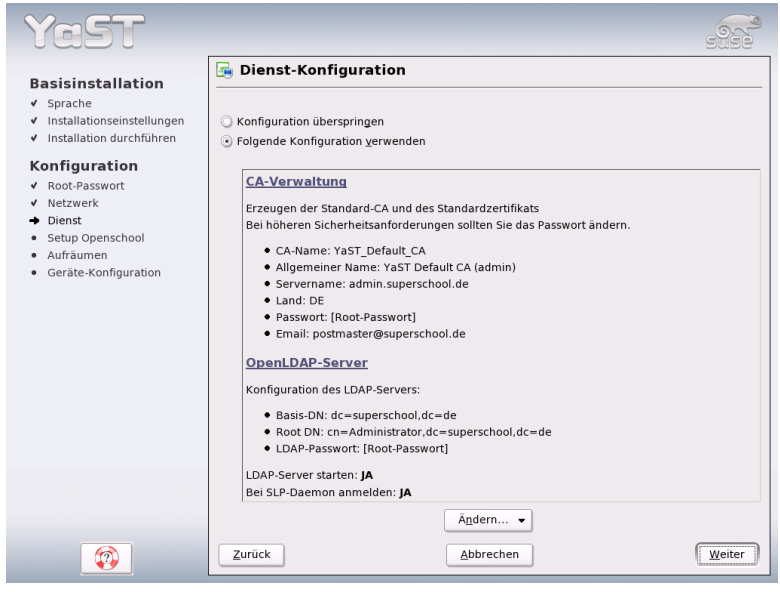

Abbildung 3.11: *Vorschlag: Netzwerkdienste*

CA–Management

Eine CA (Certificate Authority) dient dazu, sicherzustellen, dass alle miteinander kommunizierenden Netzwerkdienste einander vertrauen können. Entscheiden Sie sich ge-

gen die Einrichtung einer CA, muss die Absicherung der Serverkommunikation separat für jeden Dienst einzeln mit SSL/TLS erfolgen. Standardmäßig wird während der Installation eine CA eingerichtet und aktiviert. Details zur Einrichtung einer CA mit YaST2 und Hintergrundinformationen zu dieser Thematik finden Sie in Kapitel 26.1. *X.509-Zertifizierung mit YaST2* des SUSE LINUX Enterprise Server Handbuches.

LDAP–Server

Der LDAP–Server kann auf Ihrem System zur zentralen Verwaltung verschiedener Konfiugarationsdateien eingesetzt werden. Typischerweise verwaltet ein LDAP-Server Benutzerinformationen, er kann unter Open School Server aber auch zur Verwaltung von Mail, DHCP und DNS-Informationen eingesetzt werden. Standardmäßig wird während der Installation ein LDAP-Server eingerichtet. Mehr Details zu LDAP und zur Konfiguration mit YaST2 lesen Sie in Abschnitt 21.8. *LDAP Ein Verzeichnisdienst* des SUSE LINUX Enterprise Server Handbuches.

Hinweis

Bitte übernehmen Sie die hier vorgeschlagenen Werte!

Hinweis

3.5.4 Konfiguration als LDAP–Client

Im nächsten Schritt wird der Server als LDAP–Client konfiguriert (siehe Abbildung 3.12 auf der nächsten Seite). Der Open School Server speichert alle relevanten Daten (Benutzer, Gruppen, DNS, DHCP, Mailrouting, etc.) in LDAP.

Hinweis

Bitte übernehmen Sie die hier vorgeschlagenen Werte!

Hinweis

3.5.5 Schulspezifische Angaben

Als nächstes werden die schulspezifischen Angaben (Name der Schule, Anzahl der Klassen) abgefragt und das System dementsprechend konfiguriert:

In den meisten Schulen heißen die Klassen `4A 4B 4C 5A 5B 5C` usw. Um die Schreibarbeit bei der Installation zu minimieren, gibt es zwei Felder mit vordefinierten Werten in der YaST2–Installationsmaske.

- Das Feld ‘Schulklassen’ enthält den numerischen Teil und

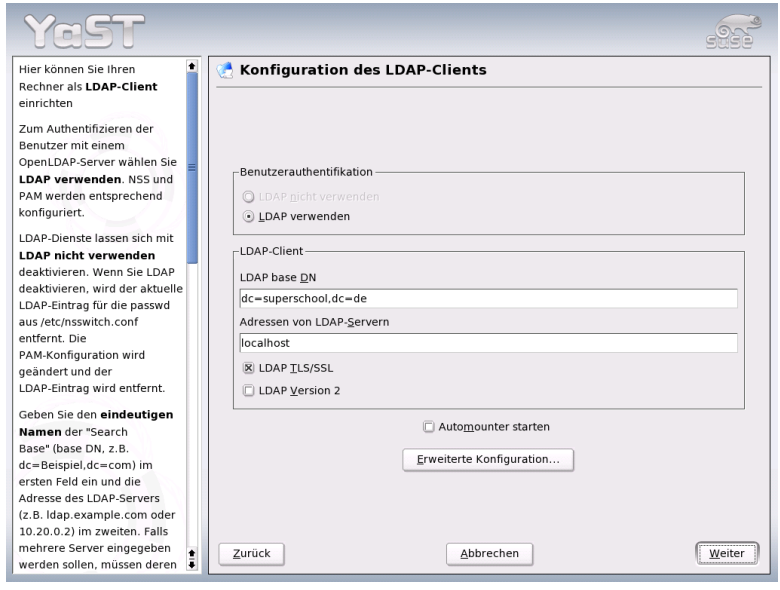

Abbildung 3.12: *Einrichten des Servers als LDAP–Client*

- das Feld 'Parallelklassen' die Buchstaben der Klassennamen.

Steht vor einer Nummer ein `'-'`–Zeichen bedeutet dies, dass es von dieser Klasse keine parallelen Klassen gibt.

Beide Felder können jedoch beliebige alphanumerische Zeichen des *englischen Alphabets* enthalten (Umlaute sind nicht erlaubt). Die Namen müssen durch je ein Leerzeichen getrennt werden.

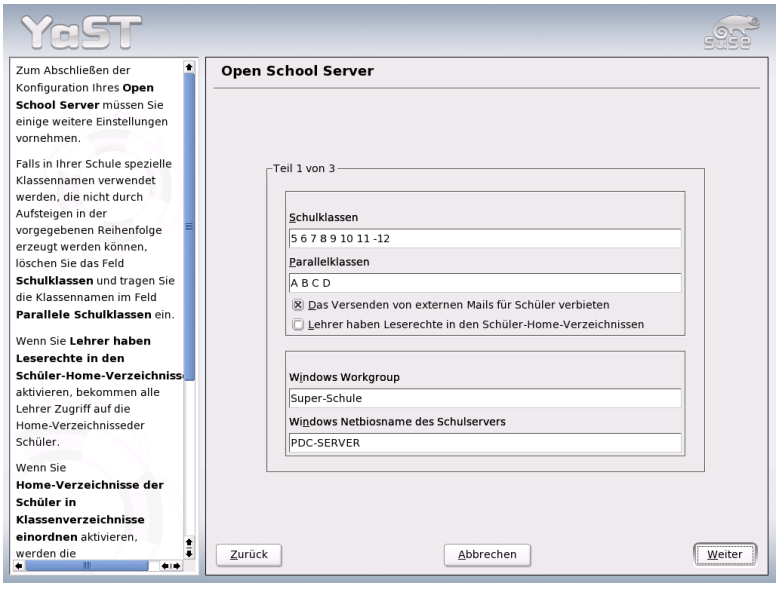

Abbildung 3.13: *Schulspezifische Einstellungen*

Hinweis

Sie müssen während der Installation *nicht* alle Klassen Ihrer Schule anlegen! Sie können auch später zusätzliche Klassen anlegen bzw. vorhandene Klassen löschen. Weiterhin werden während des Importierens der Schülerliste alle Klassen, die in der Liste vorkommen, aber in System nicht existieren, neu angelegt.

Haben Sie ganz spezielle Klassennamen, die nicht einfach durch die Konbination von Jahrgängen und Parallelklassen zu bekommen sind, (das ist in Berufsschulen oft der Fall) tragen Sie in das Feld ‘Schulklassen’ das Zeichen "*" und den Namen mindestens einer Klasse ins Feld ‘Parallelklassen’ ein.

Da Linux grundsätzlich zwischen Groß- und Kleinschreibung unterscheidet, werden die Klassennamen in Großbuchstaben konvertiert, um später Probleme beim Import von Benutzern zu vermeiden.

Hinweis

Der Open School Server wird auch als PDC (engl. *Primary Domain Controller*), File– und Printserver für Windows Rechner eingerichtet.

Der Name der ‘Windows Domäne/Arbeitsgruppe’ wird aus dem DNS–Domainnamen abgeleitet, welchen Sie schon eingegeben haben. Sie können ihn jedoch ändern. Als

NETBIOSNAME für den Open School Server wird `PDC-SERVER` vorgeschlagen. Auch diesen Eintrag können Sie anpassen in dem Feld 'Windows Netbiosname des Schulservers' (siehe Abbildung 3.13 auf der vorherigen Seite).

3.5.6 Schulname, Registrierungscode und Sprachpakete

Geben Sie nun den Namen Ihrer Schule ein und wählen Sie die zu installierenden Spracherweiterungen und Ihr Land aus. Wenn Sie mehrere Spracherweiterungen installieren, können Ihre Benutzer später unter `https://admin/` die von ihnen bevorzugte Sprache einstellen.

Wenn Sie hier Ihren Registrierungscode eintragen, können Sie später bequem über die Administrationswebseite Supportanfragen stellen und Ihr YaST2 Online Update Zugang wird eingerichtet. Sie können Ihren Registrierungscode auch nachträglich in die Variable `SCHOOL_REG_CODE` in der Datei `/etc/sysconfig/schoolserver` eintragen.

3.5.7 Groupware wählen

Sie können hier Ihr gewünschtes Groupwareprogramm auswählen. Die auf dieser CD befindlichen Groupware Lösungen sind frei verfügbare Open Source Pakete. Die Installationspakete wurden so vorkonfiguriert, dass sie ohne Probleme mit dem Open School Server laufen sollten. Ihr Open School Server Support Vertrag beinhaltet keinen Support zu den Groupware Lösungen der über den Standard–Installationssupport hinausgeht. Bitte wenden Sie Sich für weitergehenden Support an die Open Source Community Ihrer ausgewählten Groupware.

3.5.8 Hardwarekonfiguration

Im nächsten Bildschirm können Sie evtl. an die lokalen Anschlüsse des Servers angeschlossene Drucker installieren.

Bitte beachten Sie, dass Sie an externe Printserver angeschlossene Drucker bzw. Netzwerkdrucker erst nächträglich über YaST2 installieren können.

Nach der Installation

Nach Fertigstellung der Konfiguration wird der Open School Server in den endgültigen Betriebszustand hochgefahren. Auf dem Bildschirm erscheinen dabei wieder zahlreiche Meldungen, die Sie über das Starten der einzelnen Dienste des Servers informieren.

Ist das System gestartet, können Sie sich als `admin` am System anmelden. Nachdem Sie sich am Open School Server angemeldet haben, wird die grafische Oberfläche gestartet.

4.1 Links auf der Oberfläche

Um Ihnen die Administration zu erleichtern, werden Links zu den entsprechenden Weboberflächen auf dem Desktop angelegt.

Bitte klicken Sie zunächst auf den Link „Web-Mail, Groupware, Forum“ und versuchen Sie sich als `admin` anzumelden. Dabei sollten Sie eine Warnmeldung erhalten, dass die Authentifizierung des Server–Zertifikats fehlgeschlagen ist. Da dieses Zertifikat gerade erst für Ihre Schule erstellt wurde und deshalb für den Browser unbekannt ist, hat die Meldung ihre Richtigkeit. Sie können daher den Dialog fortsetzen und das Zertifikat dauerhaft annehmen.

Ebenso sollten Sie sich nach einem Klick auf den Link „Administration“ als `admin` auf der Administrationsoberfläche anmelden können – auch hier sollten Sie zuerst wieder eine Warnung zum Zertifikat erhalten.

4.2 Online–Handbuch

Abbildung 4.1: *Online–Hilfe steht auf der Administrationsweboberfläche zur Verfügung*

Die Online–Dokumentation erreichen Sie direkt über das Buchicon in der linken oberen Ecke einer jeden Seite in der Open School Server Administrationsanwendung. Weiterhin bekommen Sie zu jeder Administrationsanwendung Online–Hilfe über das Fragezeichenicon in der rechten oberen Ecke.

4.3 Internetverbindung/Proxy

Um die Internetverbindung zu testen klicken Sie auf den Link „Open School Server“. Jetzt müssten Sie auf die Homepage des Open School Servers gelangen.

Um die Funktionalität des Proxy–Servers und des eingebauten Filters zu testen, müssen Sie zunächst den Proxy in Ihrem Browser richtig konfigurieren. Sie würden ansonsten den Proxy umgehen, da Sie direkt am Server arbeiten.

Öffnen Sie im Konqueror in der Menüleiste das Menü 'Einstellungen' → 'Konqueror einrichten' und klicken Sie dort im linken Bereich auf 'Proxy-Server'. Aktivieren Sie das Feld 'Proxy verwenden' und wählen Sie im darunter liegenden Bereich „Angegebene Skript-Datei“ aus und geben folgenden Pfad ein:

```
http://admin/proxy.pac
```

Anschließend sollten Sie – auch wenn keine Internetverbindung besteht – nach Eingabe der URL `http://www.sex.de/` nach einem Benutzernamen und Passwort gefragt werden. Hier können Sie sich als `admin` anmelden und sollten dann auf die Sperrseite weitergeleitet werden.

4.4 Installations–Support

Um Ihnen einen optimalen Installations–Support gewähren zu können, werden nur Anfragen von registrierten Anwendern beantwortet. In der Verpackun befindet sich der Installations–Registriercode. Dieser Code ist einmalig und dient zur Verifizierung, dass Sie ein originales Open School Server vorliegen und somit Anspruch auf Installations–Support bzw. Maintenance haben.

Der bereits im Kaufpreis des Open School Servers enthaltene Installations–Support erstreckt sich über einen Zeitraum von 30 Tagen ab dem Kaufdatum und umfasst die unten aufgelisteten Dienstleistungen.

Dieser Installations–Support ist als Hilfe zur grundlegenden Installation des Systems gedacht, nicht jedoch als Schulung oder Einführung in Linux. Er kann also nur bei Konfigurationsproblemen, nicht aber bei Verständnisfragen, in Anspruch genommen werden.

4.4.1 Umfang des Installations–Supports

Der Installations–Support umfasst die grundlegende Installation des Open School Server auf vom Basissystem unterstützter Hardware (ein Rechner). In diesem Rahmen unterstützen wir Sie bei der Installation der Basishardware und folgender Geräte mit dem Konfigurationswerkzeug YaST2:

- Grafikkarte (ohne 3D-Unterstützung, ohne TV-in/out)

- bis zu drei Netzwerkkarten (Ethernet) (eine für den Server und zwei für die Firewall)
- DSL (PPP over Ethernet)
- ISDN-Karte oder Modem für die Einwahl beim Provider (IP)
- Einbindung für das Basissystem (SUSE LINUX Enterprise Server) zertifizierte Massenspeicherkomponenten (Festplatten, RAID–Arrays)

Über den Installations-Support erhalten Sie weiterhin Unterstützung bei der Konfiguration folgender Punkte:

- Grundkonfiguration externer E-Mail-Programme
- Unterstützung bei der Einrichtung eines Virenscanners
- Unterstützung bei der Einrichtung eines auf der Dateiendung basierenden Contentfilters (Anhangfilter) für den Mailverkehr, basierend auf Postfix

4.5 Maintenance

Die Maintenance des Open School Servers ist ein aktiver Wartungsvertrag und bietet präventiven Support, der Ihren spezifischen IT–Anforderungen optimal gerecht wird. Sie erhalten folgende Dienstleistungen, die ein Höchstmaß an Aktualität und Anwendungskomfort gewährleisten:

- Produktaktualisierungen zu allen auf dem Installationsmedium enthaltenen Paketen zur Behebung von kritischen Fehlern (Sicherheit, Datenverlust) des Open School Servers.
- Sie werden von dem Open School Server Support Team aktiv per E–Mail zu Sicherheitsrelevanten Updates benachrichtigt.
- Die Patches selbst werden auf einem geschützten Web–Server zum Download zur Verfügung gestellt.

Durch den Kauf des Basisprodukts erhalten Sie automatisch Anspruch auf Open School Server Maintenance für eine Dauer von 12 Monaten. Damit haben Sie jederzeit ein stabiles und getestetes System.

Informationen über weitere Supportangebote erhalten Sie über `http://www.extis.de/oss`.

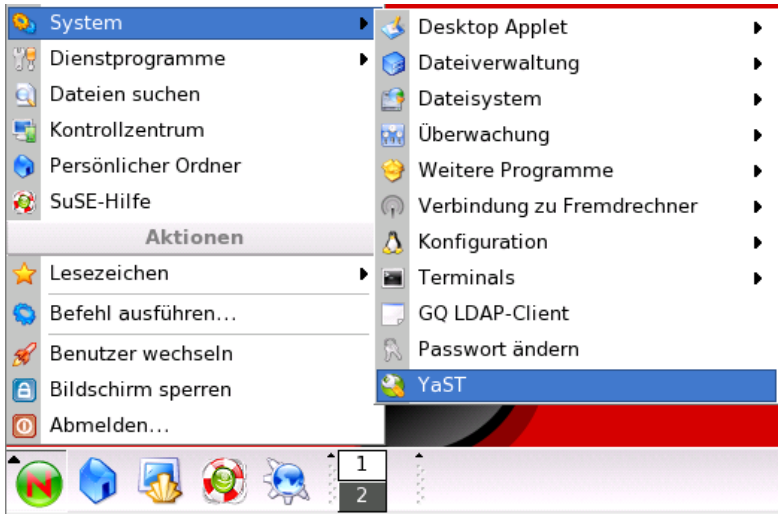

Abbildung 4.2: *YaST2–Kontrollzentrum starten*

4.5.1 Updates Einspielen

Die Online–Updates könne Sie mit dem YaST2 Online Update Programm einsplielen. Melden Sie sich dazu als Benutzer `root` an den Open School Server an, öffnen Sie eine Konsole und starten Sie das Progamn yast. Alternativ können Sie über die Kontrolleiste zuerst das YaST2 Kontrolzentrum und anschließend das Online–Update starten.

4.6 Der schnellste Weg zur Hilfe

In der Weboberfläche des Admins im Menüpunkt 'Hilfsmittel' Untermenü 'Support' können Sie während der Laufzeit ihres Maintenance–Vertrages Anfragen direkt an den Open School Server Support Team stellen. Neben der Beschreibung ihres Problems können Sie die Konfiguration Ihres Systems und die LDAP–Datenbank mitsenden. Bitte beachten Sie dabei folgende Punkte:

- Beschreiben Sie bitte pro Anfrage nur ein Problem!
- Vergessen Sie nicht alle Felder vollständig auszufüllen!
- Aktivieren Sie die Checkbox 'LDAP Datenbank senden' nur dann, wenn der Open School Server Support Team das ausdrücklich verlangt hat!

4.7 Mailinglisten

Haben Sie beim Kauf eine E–Mail–Adresse angegeben, werden Sie automatisch über sicherheitsrelevante Updates benachrichtigt. Weitere Informationen z.B. über die Verfügbarkeit neuer Funktionen im OSS erhalten Sie über verschiedene Mailinglisten, die das OSS Support Team unterhält. Hier können Sie selbst entscheiden wieviele Informationen Sie erhalten möchten indem Sie nur die für Sie interessante Mailingliste abonnieren. Die Mailinglisten finden Sie unter `http://www.extis.de/oss`.

Systemreparatur

SUSE LINUX Enterprise Server bietet neben zahlreichen YaST-Modulen zur Systeminstallation und -konfiguration auch Funktionalität zur Reparatur des installierten Systems. Dieses Kapitel beschreibt die verschiedenen Arten und Stufen der Systemreparatur.

5.1 Starten der YaST-Systemreparatur

Weil im Schadensfall nicht sicher davon ausgegangen werden kann, dass Ihr System überhaupt noch bootet, und weil ein gerade laufendes System ohnehin schlecht repariert werden kann, wird die YaST-Systemreparatur über das Open School Server Installationsmedium gestartet. Nachdem Sie die im Kapitel 3 auf Seite 15 genannten Schritte durchlaufen haben, gelangen Sie in den Dialog zur Auswahl der Installationsart und wählen dort bitte die Option 'Reparatur des installierten Systems'.

Danach wählen Sie aus, wie die Reparatur des Systems durchgeführt werden soll. Folgende Möglichkeiten stehen zur Auswahl und werden nachfolgend beschrieben.

- Automatische Reparatur
- Benutzerdefinierte Reparatur
- Expertenwerkzeuge

5.2 Automatische Reparatur

Bei unklarer Fehlersituation ist diese Methode am besten geeignet, ein beschädigtes System wieder herzustellen. Nach der Auswahl beginnt eine ausführliche Analyse des

installierten Systems, die aufgrund der Vielzahl von Prüfungen und Untersuchungen einige Zeit in Anspruch nimmt. Der Fortschritt dieses Vorgangs wird am unteren Bildschirmrand anhand zweier Fortschrittsbalken dargestellt. Der obere zeigt den Ablauf der aktuell ausgeführten Teilprüfung, während der untere den Fortschritt der gesamten Untersuchung anzeigt. Im Logging-Fenster darüber können Sie verfolgen, welche Aktion gerade stattfindet und welches Ergebnis die jeweilige Prüfung hatte. Die folgenden Testgruppen werden durchgeführt, wobei jede Gruppe noch eine Vielzahl untergeordneter Einzelprüfungen beinhaltet.

Partitionstabellen aller Festplatten Die Gültigkeit und Konsistenz der Partitionstabellen aller gefundenen Festplatten wird geprüft.

Swap–Bereiche Die Swap-Bereiche des installierten Systems werden gesucht, geprüft und ggf. zur Aktivierung angeboten. Sie sollten der Aktivierung zustimmen, weil dadurch die Geschwindigkeit der YaST-Systemreparatur gesteigert wird.

Dateisysteme Für alle gefundenen Dateisysteme wird eine Dateisystem-spezifische Prüfung durchgeführt.

Einträge der Datei /etc/fstab Es wird geprüft, ob die Einträge in der Datei vollständig und konsistent sind. Alle gültigen Partitionen werden eingebunden.

Bootloader-Konfiguration Die Bootloader-Konfiguration des installierten Systems (GRUB oder LILO) wird auf Vollständigkeit und Konsistenz geprüft. Boot- und Root-Device werden untersucht und die Verfügbarkeit der initrd-Module kontrolliert.

Paketdatenbank Es wird geprüft, ob alle Pakete vorhanden sind, die zum Betrieb einer Minimal-Installation notwendig sind. Wahlweise können auch die Basispakete analysiert werden, jedoch dauert diese Untersuchung wegen des großen Umfangs recht lange.

Wenn ein Fehler gefunden wird, stoppt die Analyse und ein Dialog wird geöffnet, der Details anzeigt und Lösungsmöglichkeiten anbietet. Aufgrund der Vielzahl von Prüfungen ist es hier nicht möglich, auf all diese Fälle einzugehen. Bitte lesen Sie die Hinweise am Bildschirm genau und wählen Sie dann aus den angebotenen Optionen die gewünschte aus. In Zweifelsfällen können Sie die vorgeschlagene Reparatur natürlich auch ablehnen. Das System bleibt dann in diesem Punkt unverändert. Es wird in keinem Fall automatisch und ohne Rückfrage repariert.

5.3 Benutzerdefinierte Reparatur

Wenn Sie bereits wissen, welcher Systembereich betroffen ist, können Sie hier die Anzahl der durchgeführten Tests einschränken. Nach Auswahl von ‘Benutzerdefinierte

Reparatur' erhalten Sie eine Auswahl von Testgruppen, die zunächst alle angewählt sind. Der Gesamtumfang der Prüfungen ist damit der gleiche wie bei der automatischen Reparatur. Wenn Sie bereits wissen, wo sich der Fehler sicher nicht befindet, können Sie die entsprechenden Gruppen durch einen Klick auf die zugehörige Checkbox abwählen. Nach einem Klick auf 'Weiter' startet dann eine reduzierte Testprozedur mit gegebenenfalls deutlich kürzerer Laufzeit. Beachten Sie dabei jedoch, dass nicht alle Testgruppen einzeln anwendbar sind. Die Prüfung der fstab-Einträge ist z. B. immer mit einer Prüfung der Dateisysteme einschließlich vorhandener Swap-Bereiche verbunden. Falls nötig, bereinigt YaST solche Abhängigkeiten durch automatische Anwahl der kleinstmöglichen Anzahl von Testgruppen.

5.4 Expertenwerkzeuge

Wenn Sie sich mit Linux gut auskennen und schon eine sehr konkrete Vorstellung davon haben, was in Ihrem System repariert werden muss, können Sie nach Auswahl von 'Expertenwerkzeuge' gezielt jenes Werkzeug anwenden, das Sie für die Reparatur benötigen.

Neuen Bootloader installieren Hier starten Sie das YaST-Bootloader-Konfigurationsmodul. Details hierzu finden Sie im Kapitel 8.6. 'Bootloader-Konfiguration mit YaST' des Handbuches von SUSE LINUX Enterprise Server.

Partitionierer starten Hier starten Sie den YaST-Expertenpartitionierer. Details hierzu finden Sie im Kapitel 1.7.5. 'Experten-Partitionierung mit YaST' des Handbuches von SUSE LINUX Enterprise Server.

Reparatur des Dateisystems Hier können Sie die Dateisysteme Ihres installierten Systems prüfen. Sie erhalten zunächst eine Auswahl aller gefundenen Partionen und können dort jene auswählen, die Sie prüfen möchten.

Verlorene Partitionen wieder herstellen Wenn Partitionstabellen in Ihrem System beschädigt sind, können Sie hier eine Rekonstruktion versuchen. Bei mehreren Festplatten bekommen Sie zunächst Gelegenheit, eine davon auszuwählen. Nach einem Klick auf 'OK' beginnt dann die Prüfung. Dies kann je nach Rechenleistung und Größe der Festplatte einige Zeit dauern.

Systemeinstellungen auf Diskette speichern Mit dieser Option können Sie wichtige Systemdateien auf eine Diskette sichern. Falls dann später einmal eine dieser Dateien beschädigt ist, kann sie von der Diskette wieder restauriert werden.

Installierte Software prüfen Hier wird die Konsistenz der Paketdatenbank getestet und die Verfügbarkeit der wichtigsten Pakete geprüft. Sollten installierte Pakete beschädigt sein, können Sie hier deren Neuinstallation veranlassen.

Teil II

Administration

Die Administrationsoberfläche

6.1 Die Startseite im Browser

Nach der erfolgreichen Installation steht Ihnen nun der Open School Server mit seinen Funktionen zur Verfügung. Öffnen Sie dazu einen Browser auf einem Ihrer Clientrechner[1] und geben Sie die URL

`https://admin`

ein. Sie sollten dann folgende Startseite erhalten (siehe Abbildung 6.1 auf der nächsten Seite).

Achtung

Da das Zertifikat des Open School Server erst bei der Installation speziell für Ihre Schule ausgestellt wird, kennt der Browser dieses Zertifikat nicht und gibt eine entsprechende Warnung aus. Je nach Webbrowser müssen Sie nun diesen Zertifikat auf verschiednen Weise dauerhaft akzeptieren bzw. in die Zertifikat–Managemant aufnehmen

Achtung

Je nach Rolle des angemeldeten Benutzers werden verschiedene Administrationsmöglichkeiten angeboten. Um die unteschiedlichen Rollen besser zum Ausdruck zu bringen, kann man die Administrationsoberfläche je nach Rolle in verschiedenen Farben darstellen. Diesen Eigenschaft kann man einschalten indem man die Sysconfig–Variable `SCHOOL_ADAPT_STYLESHEET` auf `yes` setzt. Die Stylsheets findet man im Verzeichnis `/srv/www/admin/`: `stylesheetAdmin.css`, `stylesheetStudents.css` und `stylesheetTeachers.css`.

[1] Der Clientrechner muss vorher mind. als DHCP–Client (automatischer Bezug der IP-Adresse) konfiguriert werden. Alternativ können Sie sich als Benutzer `admin` direkt an den Open School Server anmelden und auf dem Icon „Administration“ klicken.

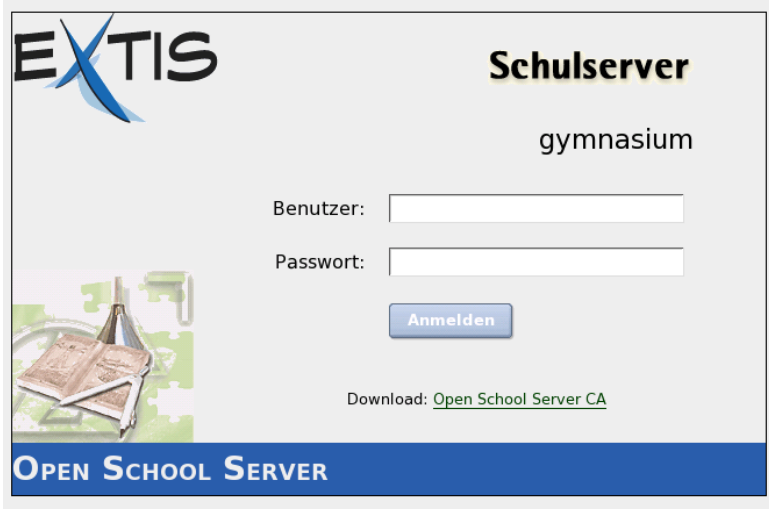

Abbildung 6.1: *Startseite des Open School Servers*

6.2 Administration als Systemadministrator `admin`

Um als Schuladministrator den Open School Server zu verwalten, melden Sie sich mit dem Benutzernamen `admin` und Ihrem Administratorpasswort am „Adminfrontend“ an, indem Sie in einem beliebigen Browser die URL
`https://admin/`
eingeben. Sie können hier nahezu alle Parameter einstellen, mit denen der Open School Server konfiguriert wird.

Die Navigation im Konfigurationsmenü ist bewusst einfach und effizient gehalten: Das Menü besteht aus einer Reiterleiste auf der linken Seite als Hauptmenü und einer bei Bedarf am oberen Rand erscheinenden Leiste als Untermenü (siehe Abbildung 6.2 auf der nächsten Seite).

Links oben über dem Untermenü erscheint der Name des angemeldeten Benutzers, und ggf. der Name des Schulraumes in welchem sein Rechner registriert worden ist.

Wurde mehr als eine Sprachenerweiterung installiert, erscheint rechts oben über dem Untermenü ein Knopf ‘Sprache’ um die Sprache der Weboberfläche zu ändern.

Durch einen Mausklick auf die Hauptleiste wird das entsprechende Untermenü aufgerufen. Das Symbol in der Hauptleiste wird dabei eingefärbt. Durch einen Mausklick auf ein Untermenü erhalten Sie die entsprechende Maske.

Abbildung 6.2: *Administration des Open School Servers für den Benutzer* `admin`

Durch Anklicken des Fragezeichens am rechten oberen Rand der jeweiligen Maske eines Untermenüs erhalten Sie in einem separaten Fenster Hilfe zu den angezeigten Eingabemöglichkeiten.

Mit 'Abmelden' beenden Sie Ihre Sitzung. Sie müssen dann erneut Benutzername und Passwort eingeben.

Hinweis

Webfrontend und YaST2

Bitte beachten Sie: Die grundsätzliche Konfiguration wird über das Webfrontend mit einem Browser gehandhabt.

Um tiefgreifende Änderungen an der Konfiguration des Servers vorzunehmen (z. B. um zusätzliche Hardware einzurichten oder den Internetzugang zu ändern), müssen Sie in manchen Fällen trotzdem das graphische Konfigurationstool YaST2 verwenden.

Verwenden Sie aber *nie* YaST2 um neue Benutzer anzulegen!

Hinweis

6.2.1 Benutzer

Nachdem der Open School Server installiert ist, sollten Sie Benutzer anlegen. Bereits vorhanden sind der Benutzer `admin` (welcher den Open School Server konfiguriert) und die E–Mails an den Administrator lesen kann, sowie sog. „Templatebenutzer“ für die Schüler, Lehrer und Verwaltungspersonal (`tstudents, tteachers, tadministration`).

Benutzer können Sie unter zwei Menüpunkten anlegen:

'Neu' In diesem Fall wird ein einzelner Benutzer angelegt.

'Importieren' Unter diesem Menüpunkt haben Sie die Möglichkeit, Benutzer aus einer Textdatei einzulesen. Wie Sie dies machen wird unter 6.2.1 auf Seite 62 erläutert.

Neu – Anlegen einzelner Benutzer

Wählen Sie im Hauptmenü 'Benutzer', dann im Untermenü 'Neu', um den ersten Benutzer anzulegen (siehe Abbildung 6.3 auf Seite 60).

Folgende Felder müssen beim Anlegen eines neuen Benutzers unbedingt ausgefüllt bzw. gesetzt werden:

'Nachname'

'Vorname'

'Geburtstag'

'Primäre Gruppe' Wählen Sie eine primäre Gruppe, der der neue Benutzer angehören soll. Weitere Gruppen können Sie später über das Menü 'Gruppen/ Ordner' zuordnen. Sofern Sie noch keine Gruppen angelegt haben, können Sie hier nur die Gruppen `Schüler`, `Lehrer`, `Verwaltung` oder `Template Benutzer` wählen.

'Klasse' Benutzer können zu einer beliebigen Anzahl von Klassen gehören. Ist der neu angelegte Benutzer ein Schüler, muss er jedoch mind. einer Klasse zugeordnet werden. Am Ende der Auswahl können Sie auch `all` wählen, um einen Lehrer allen Klassen zuzuordnen.

Wurde keine 'Benutzerkürzel' (UID: User–ID) angegeben, wird diese aus dem Nach- und Vornamen ermittelt. Wie das geschieht, wird durch die Systemvariable `SCHOOL_LOGIN_SCHEME`in der Datei `/etc/sysconfig/schoolserver` gesteuert. Der Standardwert ist`N4V4`.

Achtung

Ändern Sie den Standardwert nachträglich nur dann, wenn Sie *alle* Nutzer neu generieren möchten.

Achtung

Das bedeutet, dass der Login aus den ersten vier Buchstaben des Nachnamens plus der ersten vier Buchstaben des Vornamens gebildet wird. Existiert im System schon ein Benutzer mit derselben UID, wird eine Zahl an die UID angehängt, damit diese eindeutig ist. Sie können auch selbst eine UID für den neuen Benutzer angeben. Bitte beachten Sie dabei, dass die UID aus Kleinbuchstaben bestehen muss, keine Sonderzeichen oder Leerstellen enthalten darf und auf dem System eindeutig sein muss.

Hinweis

Für 'Templatebenutzer' muss immer ein Benutzerkürzel angegeben werden. Ausserdem sollte bei Templatebenutzern das Feld 'Nachname' eine ausführliche Beschreibung des anzulegenden Templates erhalten.

Hinweis

Wenn Sie wollen, dass Ihre Benutzer im Internet einen „sprechenden" Namen für ihre E-Mail-Adresse haben, benutzen Sie einfach den E-Mail-Alias als Adresse. Dieser wird standardmäßig in der Form `Vorname.Nachname@domain.de` angelegt. Weitere Aliase können Sie später über den Menüpunkt 'Bearbeiten' hinzufügen.

Der Administrator muss dem neuen Benutzer ein Passwort zuweisen. Das muss kein besonders sicheres Wort sein, denn der Benutzer sollte bei seinem ersten Login sowieso das Passwort ändern.

Tipp

Passwort-Verschlüsselung

Sie können Art und Stärke der Passwort-Verschlüsselung wählen. Mit der älteren„crypt"-Verschlüsselung ist eine maximale Passwortlänge von acht Zeichenmöglich – längere Passwörter werden einfach abgeschnitten.

Mit „SMD5" sind bis zu 255 Zeichen lange Passwörter möglich.

Tipp

Um Lehrern besondere Rechte auf die Benutzerdaten zu geben, muss der Checkbutton 'Administrationsrechte (ja/nein)' gewählt werden. Schülern kann dieses Recht nicht erteilt werden.

Beachten Sie weiterhin die Werte, die bei 'E-Mail-Quota (in MB)' und 'Festplattenquota (in MB)' eingetragen sind.

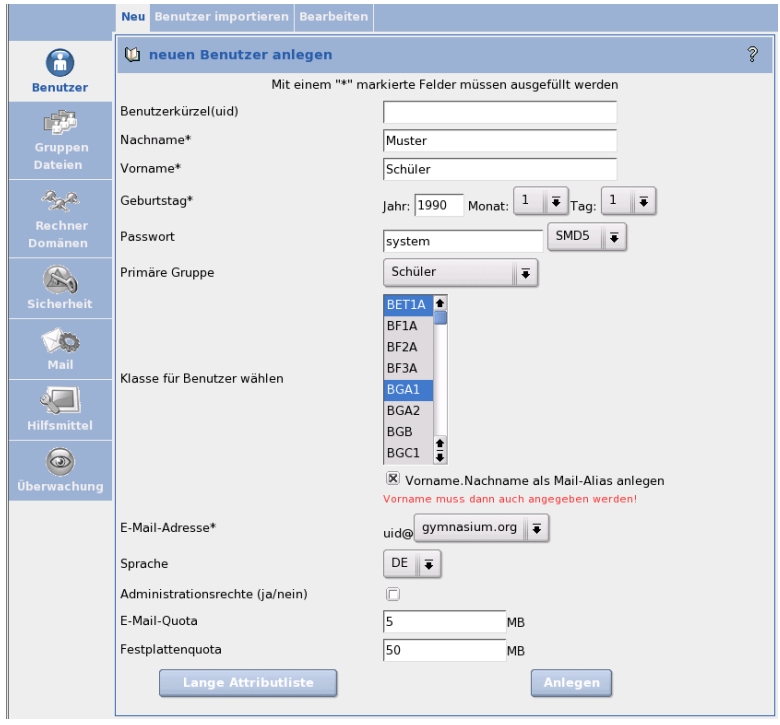

Abbildung 6.3: *Anlegen eines neuen Benutzers*

Diese Werte bezeichnen den Platz, den ein Benutzer maximal für E-Mails in seinen Ordnern bzw. für Dateien auf dem Open School Server zur Verfügung hat. Wenn er den durch 'E-Mail-Quota (in MB)' bestimmten Platz vollständig in Anspruch genommen hat, kann er keine E-Mails mehr empfangen, bis er einige seiner alten E-Mails gelöscht hat, um wieder unter seinen Maximalwert zu gelangen. Auch diesen Wert können Sie noch nachträglich ändern.

Wenn der Benutzer den durch `Festplattenquota (in MB)` bestimmten Platz vollständig in Anspruch genommen hat, kann er keine Dateien mehr auf den Server speichern, bis er genug Daten gelöscht hat, um wieder unter seinen Maximalwert zu gelangen. Dabei ist es wichtig zu wissen, dass bei der Berechnung der benutzten Festplattenkapazität eines Benutzers nicht nur die Dateien, in seinem sog. *Homeverzeichnis*, sondern alle Dateien die der Benutzer auf dem System gespeichert hat (`/home/all`, `/home/groups/<was_auch_immmer>`, ...), berücksichtigt werden.

Die angezeigten Standardwerte (`E-Mail-Quota (in MB)` und `Festplattenquota`

(in MB)) beim Anlegen eines Benutzers können Sie in der Datei /etc/sysconfig/schoolserver durch das Setzen folgender Variable einstellen:

SCHOOL_MAIL_QUOTA Standardwert für E-Mail-Quota (in MB) beim Anlegen eines Schülers. Standard: 5 MB.

SCHOOL_MAIL_TEACHER_QUOTA Standardwert für E-Mail-Quota (in MB) beim Anlegen eines Lehrers. Standard: 25 MB.

SCHOOL_FILE_QUOTA Standardwert für Fesplattenquota (in MB) beim Anlegen eines Schülers. Standard: 50 MB

SCHOOL_FILE_TEACHER_QUOTA Standardwert für Fesplattenquota (in MB) beim Anlegen eines Lehrers. Standard: 250 MB

Wollen Sie weitere persönliche Daten (z. B. Adresse, Telefonnummern, Bild, ...) für den Benutzer eintragen, können Sie sich durch Anklicken des Buttons 'Lange Attributliste' sämtliche möglichen Attribute anzeigen lassen und bearbeiten.

Teilen Sie dem neuen Benutzer sein Benutzerkürzel und sein Passwort mit. Der Benutzer kann sich sofort über einen Browser am Webfrontend des Open School Server anmelden und sollte zuerst sein Passwort ändern. Es besteht keine Notwendigkeit, dass der Administrator das Benutzerpasswort kennt. Der Administrator kann auch ohne Kenntnis des alten Passwortes ein neues vergeben.

Wie oben erwähnt, wird für jeden neuen Benutzer ein eigenes Heimatverzeichnis angelegt. Die Lehrer bekommen ihre Verzeichnisse unterhalb des Verzeichnisses /home/teachers/ und die Schüler unterhalb des Verzeichnisses /home/users. „Verwaltungsnutzer" bekommen ihre Verzeichnisse unterhalb des Verzeichnisses /home/administration.

Folgende Verzeichnisse werden in jedem neu erzeugten Heimatverzeichnis angelegt:

Import: Für Dateien, die von anderen Benutzern in das Heimatverzeichnis kopiert werden. Dies trifft z. B. bei Lehrern zu, die Dateien von Schülern einsammeln.

Export: Für Dateien, welche an andere Benutzer verteilt werden sollen. Wenn ein Schüler z. B. Dateien bearbeitet hat, die nun vom Lehrer eingesammelt werden sollen.

public_html: Für die Veröffentlichung von Dateien im WWW. Anderen Benutzern ist dieses Verzeichnis über die in einem Browser eingegebene URL: https://schulserver/~<login> zugänglich.

Zusätzlich bekommt jeder Benutzer ein Verzeichnis unterhalb von /home/profile für seine Windowsprofile. Hier wird für jede Windows-Version (WinXP, Win2k, Win9x) ein eigenes Unterverzeichnis angelegt.

Benutzer importieren – Einlesen von Benutzerlisten

Da es sehr mühsam wäre, die Schüler bzw. die Lehrer jedes Jahr von Hand einzutragen, bietet der Open School Server die Möglichkeit, die Liste der Schüler (und Lehrer) aus einer Datei zu importieren.

Die Datei sollte dazu folgendes Format haben:

Normale ASCII-Textdatei Hierbei handelt es sich um eine normale Textdatei in der für die Landessprache üblichen Kodierung (in Deutschland und Österreich ist das ISO-Latin-1). Wird UTF-8 verwendet, muss in der ersten Zeile der Datei das Schlüsselwort ÜTF-8ëingetragen werden.

Die Trennzeichen zwischen den einzelnen Feldern sind prinzipiell egal - Hauptsache, Sie ändern sich nicht im Verlauf der Datei. So reicht die bei vielen Schulverwaltungsprogrammen existierende Export-Funktion in eine CSV oder Textdatei meist vollkommen aus.

Sonderformen Einige Schulverwaltungsprogramme beherrschen den Export in eine normale Textdatei nicht. Für diese wurden spezielle Import-Filter geschrieben, um die Schülerdaten dennoch korrekt in den Open School Server zu importieren.

Hierbei handelt es sich u.a. um die Schulverwaltungsprogramme WinSV, Sibank und Schild-NRW.

Unter *Schülerdaten exportieren und importieren* auf Seite 191 finden Sie Anleitungen für den richtigen Export der Daten bei diesen Programmen und und den korrekten Import am Open School Server. Wichtig: Ändern Sie bitte wie dort beschrieben das Importformat für die Dateien unter 'Hilfsmittel' → 'Globale Konfiguration'. Mehr muss dann am Open School Server nicht geändert werden. Benutzen Sie eines dieser Programme, können Sie den nächsten Abschnitt (*Format der CSV-Datei* auf dieser Seite) überspringen.

Format der CSV-Datei

In der ersten Zeile werden die Spalten und das Trennfeld der Datei definiert. Zur Zeit sind folgende Schlüsselwörter erlaubt:

`NAME` *

`VORNAME` *

`GEBURTSTAG` *

`KLASSE` * Wird der Benutzer zu mehr als einer Klasse zugeordnet, müssen diese durch Leerzeichen getrennt werden.

RELIGION

PASSWORT

LOGIN

TELEFONNUMMER

FAXNUMMER

TELEFONNUMMER-PRIVAT

TELEFONNUMMER-MOBIL

SPRACHE

BESCHREIBUNG

STRASSE

PLZ

BUNDESLAND

EMAIL-DOMAIN

UTF-8 Zeigt an, dass die einzulesende Datei den UTF-8 Zeichensatz verwendet.

Die mit '*' gekenzeichneten Felder sind obligatorisch. Ein Benutzer wird also durch die Felder NAME,VORNAME und GEBURTSTAG identifiziert und durch das Feld KLASSE einer Klasse zugeordnet.

Es gibt noch weitere Felder, welche Sie in der Datei verwenden können, die allerdings (noch) nicht übersetzt sind:

maileanbled Dieses Feld kann folgende Werte enthalten:

OK Der Benutzer bekommt ein Mailbox, und darf eMails versenden. Das ist die Standardeinstellung das Fehlen dieses Feldes wird so interpretiert.

NO Für den Benutzer wird kein Mailbox angelegt.

LOCAL_ONLY Der Benutzer bekommt einen Mailbox, darf eMails jedoch nur lokal versenden. Wobei lokal heisst, an die Domains, die in der Datei /etc/postfix/local_domains aufgelistet sind.

reqpwdchange Muss das Passwort beim ersten Anmelden geändert werden?

0 Der Benutzer wird beim ersten Anmelden nicht angefordert das Passwort zu ändern. Dies ist die Standardeinstellung.

1 Der Benutzer wird bei der ersten Anmeldung angefordert das Passwort zu ändern.

Es gibt drei Möglichkeiten, was mit einem Benutzer nach dem Einlesen der Benutzerdatei passiert:

Neuer Benutzer Wird ein Benutzer in der LDAP-Datenbank nicht gefunden, handelt es sich um einen neuen Benutzer. In diesem Fall wird für diesen Benutzer ein neuer eindeutiger Login Name, wie unter *Neu – Anlegen einzelner Benutzer* auf Seite 58 beschrieben, ermittelt und dieser in die LDAP-Datenbank aufgenommen.

Falls vorhanden, wird das Feld `PASSWORT` wie folgt Weise ausgewertet:

`'text' =>` `'text'` wird als Passwort gesetzt.

`'*' =>` Sollten Sie in ein und derselben Textdatei einigen Nutzern ein fest definiertes Passwort über `'text'` zuweisen, für dere jedoch ein zufälliges Passwort generieren lassen wollen, so fügen Sie bei diesen Nutzern den `'*'` ein.

`'kein Inhalt' =>` Sollte anderen Nutzern ein Passwort über die beiden oben angegebenen Möglichkeiten (fest oder zufällig) zugewiesen worden sein, bei einem (oder mehreren) Nutzern in derselben Datei aber *kein* Wert im Passwortfeld enhalten sein, so bekommen diese Nutzer kein Passwort, d.h. sie können sich ohne Passwort am System anmelden.

Ist das Feld `PASSWORT` in der Datei nicht vorhanden wird ein zufälliges Passwort zugewiesen.

Vorhandene Benutzer Ändern Steht ein Benutzer sowohl in der LDAP-Datenbank als auch in der Benutzerliste, handelt es sich um einen alten Benutzer.

Bei vorhandenen Benutzern wird dass Feld `PASSWORT` nicht ausgewertet. Die Benutzer werden lediglich aus der alten Klasse aus- und in die neue Klasse eingetragen.

Benutzer löschen Hinweis: Diese Funktion funktioniert nur, wenn sie *nicht* eine Teilliste einlesen.

Steht ein Benutzer in der LDAP-Datenbank, jedoch nicht in der Benutzerliste, bedeutet das, dass dieser Benutzer die Schule verlassen hat.

Also werden seine Daten aus der Datenbank gelöscht, sein Heimatverzeichnis wird in ein Archiv zusammengefasst und unter `/home/archiv/benutzername-datum.tgz` gespeichert.

Da die Archivierung sehr rechenintensiv ist, wird diese nicht sofort, sondern erst früh am nächsten Tag durchgeführt. Sie können jedoch die Archivierung auch manuell anstoßen.

Melden Sie sich dazu am Open School Server als `root` an und führen Sie auf einer Konsole den Befehl `/usr/sbin/archiv_user` aus.

Hinweis

Wenn Sie eine Liste mit Lehrern anlegen wollen, so beachten Sie, dass Nutzer, welche der Primärgruppe `Lehrer` angehören, *immer* so behandelt werden als würde nur eine Teilliste eingelesen. Sie müssen aus dem Dienst ausgeschiedene Lehrer also immer manuell löschen.

Hinweis

Nach dem Abarbeiten der eingelesenen Datei wird die neue, aktuelle Benutzerliste pro Klasse in der Datei `/home/sysadmins/admin/<datum>.<uhrzeit>/userlist.<KLASSE>.txt` im Homeverzeichniss des Benutzers `admin` gespeichert. In dieser Datei stehen die Passwörter im Klartext, mit dementsprechender Vorsicht muss sie behandelt werden.

Hier ist eine Beispieldatei für das erstes Laden des Systems mit unterschiedlichen Passwort-Vergaben: `GEBURTSTAG:NACHNAME:VORNAME:PASSWORT:KLASSE`

```
11.10.1986:Klein:Aladar:12345:9A
4.08.1986:Micuc:Emil::9A
09.11.1986:Groß:Evelyn:*:9A
17.04.1986:Müller:Helmuth:*:9A 10A:
29.9.1987:Klein:Aladar:*:10A
```

Die resultierenden Dateien `/root/<datum>.<uhrzeit>.userlist.9A.txt` und `/root/<datum>.<uhrzeit>.userlist.10A.txt` sehen folgendermaßen aus, wobei die zufällig ermittelten Passwörter natürlich abweichen können:

```
LOGIN:GEBURTSTAG:NACHNAME:VORNAME:PASSWORT:KLASSE
aladklei:11.10.1986:Klein:Aladar:12345:9A
emilmicu:4.08.1986:Micuc:Emil::9A
evelgros:09.11.1986:Groß:Evelyn:avwbdfwa:9A

LOGIN:GEBURTSTAG:NACHNAME:VORNAME:PASSWORT:KLASSE
helmmuel:17.04.1986:Müller:Helmuth:wghgettr:10A
aladklei1:29.9.1987:Klein:Aladar:oilweqqk:10A
```

Während also Aladar Klein ein fest zugewiesenes Passwort (12345) bekommt, wird für Emil Micuc ein leeres Passwort generiert (er kann sich also ohne Passwort anmelden). Alle anderen Benutzer auf dieser Liste bekommen ein zufällig generiertes Passwort, da

im entsprechenden Feld ein `'*'` steht. Nochmals der Hinweis: wenn Sie allen Nutzern ein zufällig generiertes Passwort zuweisen lassen wollen, dann sollte in der Datei kein Passwort-Feld existieren. (Oder Sie müssen bei jeder Person in diesem Feld ein `'*'` setzen.) Eine Beispieldatei ohne Passwortfeld würde so aussehen:

```
GEBURTSTAG:NACHNAME:VORNAME:KLASSE
11.10.1986:Klein:Aladar:9A
4.08.1986:Micuc:Emil:9A
09.11.1986:Groß:Evelyn:9A
17.04.1986:Müller:Helmuth:10A
29.9.1987:Klein:Aladar:10A
```

Bearbeiten – Verändern der Benutzerdaten

Klicken Sie zunächst auf 'Bearbeiten'. Jetzt müssen Sie auswählen, welche Benutzer angezeigt werden sollen. Haben Sie eine überschaubare Anzahl von Benutzern, dann klicken Sie auf 'Filter anwenden', ohne den Wert `'*'` im Eingabefeld 'Filter' zu verändern. Daraufhin werden alle Benutzer angezeigt. Wählen Sie den zu bearbeitenden Benutzer mit einem Mausklick aus.

Sie können Benutzer nach folgenden Kriterien suchen:

UID, Nachname oder Vorname Tragen Sie das gesuchte Wort oder einen Teil davon mit `'*'` erweitert ins Eingabefeld 'Benutzer' ein. Andere Jokerzeichen wie z. B. `'?'` unterstützt der Open School Server zur Zeit nicht.

Klasse bzw. Gruppe Tragen Sie die Bezeichnung der Klasse oder Gruppe, deren Mitglieder Sie suchen, ins Feld 'Klasse / Gruppe' ein. Auch hier können Sie mit dem Suchstring `'5*'` z. B. alle Schüler des fünften Jahrganges und deren Lehrer auflisten.
Durch die Kombination der Felder 'Klasse' und 'Gruppe' können Sie z. B. alle Schüler des funften Jahrgangs auflisten, die auch Mitglied der (fiktiven) Arbeitsgruppe `EDV` sind.

Die Funktionen

- 'Löschen',
- 'Profile verteilen',
- 'Zugriffstatus',
- 'Anmelden erlauben/verbieten',
- 'Internet erlauben/verbieten' und

- 'Externe Mails Ja/Nein'

lassen sich auch für mehrere Benutzer gleichzeitig anwenden. Wählen Sie dazu einfach mit Hilfe der gedrückten Strg– oder Shift–Taste mehrere Benutzer mit der Maus aus. Die Namen der gewählten Benutzer sind dann farbig markiert.

Am rechten Rand befinden sich Buttons für die einzelnen Funktionen (siehe Abbildung 6.4).

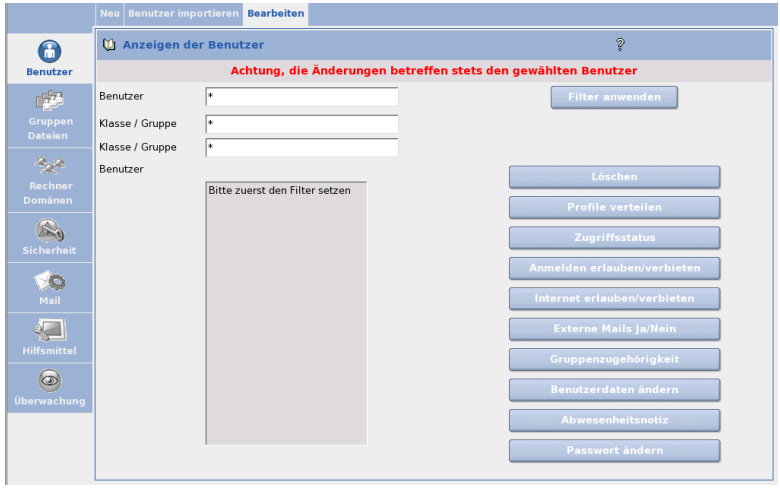

Abbildung 6.4: *Verändern der Benutzerdaten*

'Löschen' Entfernt den ausgewählten Benutzer vom Server. Gehen Sie mit dieser Funktion vorsichtig um: Alle E-Mails dieses Benutzers sind dann unwiederbringlich verloren!

Alle Dateien die der Benutzer erstellt hat (einschließlich seiner Windowsprofile), werden in einem Archiv gesammelt und unter `/home/archiv/<Benutzername>-<Datum>.<Uhrzeit>.tgz` gespeichert.

'Profile verteilen' Unter diesem Menüpunkt können Sie vordefinierte Profile (z. B. Windows und/oder Linux Desktop Einstellungen) an ausgewählte Benutzer verteilen.

Sie müssen zunächst das gewünschte Betriebssystem (entsprechende Windows-Version oder Linux) anklicken. Durch das Aktivieren der Checkbox 'Windowsprofile 'nur lesbar' machen' verhindern Sie Änderungen durch die Benutzer.

'Zugriffsstatus' Unter diesem Menüpunkt werden die aktuellen Zugangsberechtigungen ausgewählter Benutzer angezeigt. Diese können Sie in den weiteren Menüpunkten bearbeiten.

'Anmelden erlauben/verbieten' Hier können Sie einzelnen Benutzern das Anmelden an den Workstations und an der Weboberfläche verbieten bzw. erlauben. (Das LDAP-Attribut `loginDisabled` wird auf den Wert `true` bzw. `false` gesetzt.)

'Internet erlauben/verbieten' Hier können Sie einzelnen Benutzern den Zugang ins Internet über den Proxyserver sperren bzw. wieder freigeben. (Das LDAP-Attribut `internetDisabled` wird auf den Wert `true` bzw. `false` gesetzt.) Dies betrifft allerdings nur das Surfen im Internet – andere Dienste (wie z. B. Email) sind davon nicht betroffen.

'Externe Mails Ja/Nein' Je nachdem, wie Sie den Open School Server installiert haben (Stichwort: 'Das Versenden von externen Mails für Schüler verbieten'), ist das Versenden von externen Mails für Schüler verboten oder erlaubt. Dieses Verhalten wird jedoch nicht an die Gruppe der Schüler gebunden, sondern beim Anlegen jedes einzelnen Benutzers wird die Standardeinstellung diesem Benutzer zugeordnet.

Unter diesem Menüpunkt können Sie einzelnen Benutzern das Versenden von externen Mails auch nachträglich noch erlauben bzw. verbieten.

'Zu Gruppen hinzufügen' Sie können die Benutzer einer oder mehreren (sekundären) Gruppen zuordnen.

'Ändere Benutzerdaten' Sie erhalten nahezu dieselbe Maske, die auch beim Anlegen eines Benutzers erscheint. Hier können Sie alle Werte ändern. Zusätzlich besteht jetzt die Möglichkeit, dem Benutzer „Aliasnamen" zu vergeben.

Dazu können Sie im Feld 'E-Mail-Aliase', durch Leerzeichen getrennt, eine Auflistung der Namen eintragen, mit denen der Benutzer zusätzlich zu seiner UID per E-Mail (in der Hauptmaildomain) erreichbar sein soll.

'Abwesenheitsnotiz' Hier können Sie automatische Abwesenheitsnotizen für Benutzer einrichten (siehe hierzu auch 6.3.5 auf Seite 121).

'Ändere Passwort' In dieser Maske wird ein neues Passwort vergeben.

6.2.2 Gruppen und Dateien

Gruppen Bearbeiten

Hier können Sie neue Gruppen anlegen, vorhandene Gruppen bearbeiten oder löschen sowie die Beschreibung der Gruppe verändern. Wählen Sie eine Gruppe und die

Schaltfläche ‘Bearbeiten’, um die Liste der Mitglieder einzusehen oder zu verändern (siehe Abb. 6.5).

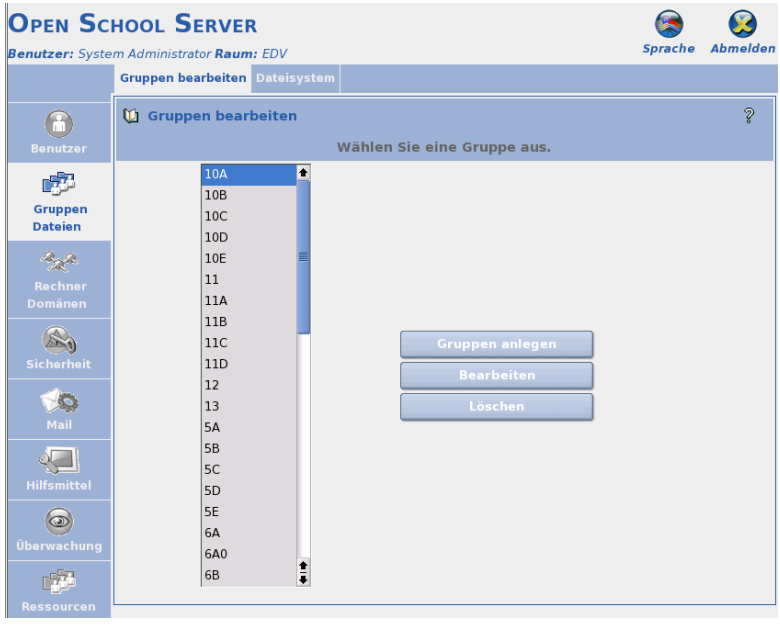

Abbildung 6.5: *Bearbeiten einer Gruppe*

Wählen Sie wieder ‘Filter anwenden’ und Sie erhalten die Liste aller auf dem System vorhandenen User. Bereits dieser Gruppe zugeordnete User sind farbig markiert. Ändern Sie die Zugehörigkeiten nach Ihren Wünschen per Mausklick. Mit ‘Aktualisieren’ schließen Sie die Bearbeitung ab und speichern die Änderungen.

Anlegen einer Gruppe

Mit dem Untermenü ‘Gruppen anlegen’ aus dem Menü ‘Gruppen’ erstellen Sie eine neue Gruppe (siehe Abb. 6.6 auf der nächsten Seite). Wählen Sie einen eindeutigen Gruppennamen aus.

Achtung

Gruppennamen

Verwenden Sie für den Gruppennamen keine Sonderzeichen und auch keine Leerstellen! Die Gruppennamen werden immer in Großbuchstaben konvertiert.

Achtung

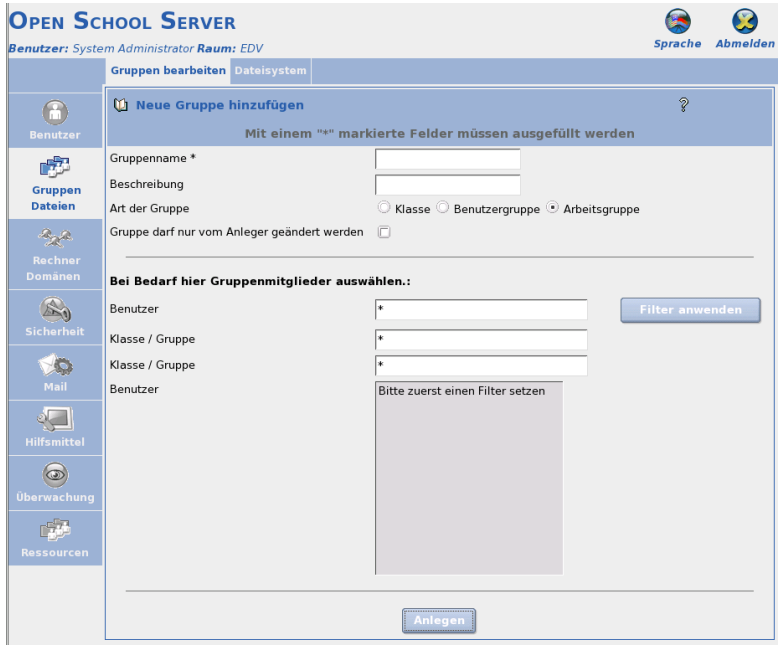

Abbildung 6.6: *Anlegen einer Gruppe*

Geben Sie der Gruppe eine aussagekräftige Beschreibung. Der Schulserver bietet abweichend von anderen Betriebsystemen drei Arten von Gruppen an:

Klasse Diese Gruppen bilden die Realen Schulklassen einer Schule ab, können nur vom Benutzer `admin` oder von Lehrern mit besonderen Administrationsrechten angelegt werden.

Primäre Gruppe Diese Gruppen bestimmen die grundsätzliche Rolle eines Benutzers auf dem System. Nach einer Neuinstallation des Open School Servers sind folgende primäre Gruppen schon verdefiniert „Schüler“, „Lehrer“, „Verwaltung“, „Templatebenutzer“ und „Workstation–Benutzer“.

Arbeitsgruppe Diese Art von Gruppen kann von jeden Lehrer angelegt und/ oder bearbeitet werden, und können z. B. zu Projektarbeiten verwendet werden..

Alle diese Gruppen bekommen eine Mailbox und ein Gruppenverzeichnis und erscheinen auch in der Groupware (z. B. für Terminabsprachen oder Email).

Um der zu erstellenden Gruppe Benutzer zuzuordnen, müssen Sie sich eine Liste der vorhandenen Benutzer anzeigen lassen. Klicken Sie auf ‘Filter anwenden’ ohne den

Wert im Feld ‘Filter’ zu verändern, um eine Liste aller vorhandenen Benutzer anzuzeigen, oder schränken Sie vorher die anzuzeigenden Benutzer mit dem Eingabefeld ‘Filter’ ein.

Wählen Sie dann per Mausklick einen oder mehrere Benutzer aus, die der Gruppe angehören sollen. Ausgewählte Benutzer werden farbig markiert. Mit dem Button ‘Anlegen’ legen Sie die Gruppe mit den gewählten Mitgliedern an.

Tipp

Gruppen verwenden

Sie können auch einer ganzen Gruppe Rechte vergeben. Fassen Sie also nach Möglichkeit Ihre Benutzer in Gruppen zusammen und vergeben Sie dann Rechte für die Gruppen. Damit erleichtern Sie später den Verwaltungsaufwand, wenn Änderungen erforderlich sind.

Tipp

Dateisystem

Wollen Sie anderen Benutzern Zugriff auf bestimmte Dateien und Ornder gestatten, Dateien von ihrem lokalen System in ein Verzeichnis auf dem Server laden oder Dateien vom Server in ein lokales Verzeichnis kopieren, so können Sie dies in diesem Menü tun.

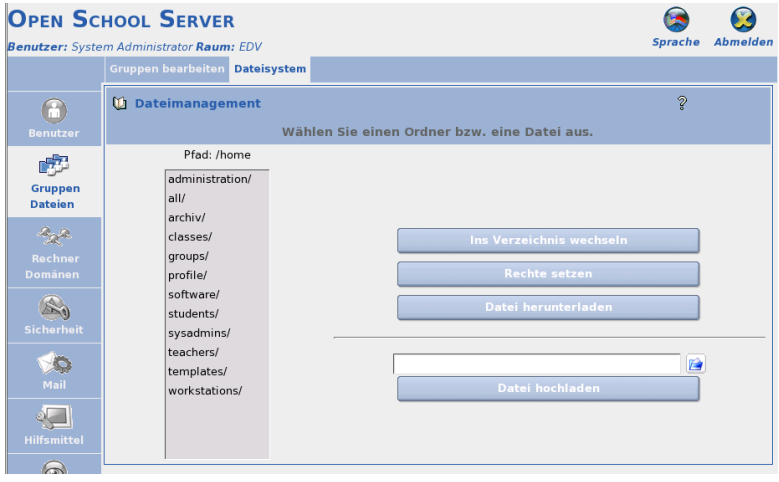

Abbildung 6.7: *Dateimanagement*

Navigation

Markieren Sie dazu zunächst in der linken Auswahlbox das entsprechende Verzeichnis oder die entsprechende Datei. Sollten Sie sich noch nicht im entsprechenden Ordner befinden, so markieren Sie bitte denjenigen Ordner, in welchem sich die gesuchte Datei oder der Unterordner befindet und klicken Sie anschließend auf 'Ins Verzeichnis wechseln'.

Hinweis

Fehlende Zugriffsrechte

Beachten Sie bitte, dass Sie aufgrund der für die jeweiligen Verzeichnisse geltenden Zugriffsbeschränkungen nicht in jedes angezeigte Verzeichnis wechseln können.

Hinweis

Wenn Sie aus einem Unterverzeichnis wieder in das übergeordnete Verzeichnis wechseln wollen, so markieren Sie die „..“ ganz oben in der Liste und klicken auf 'Ins Verzeichnis wechseln'.

Rechte setzen

Markieren Sie die Datei oder das Verzeichnis, für welches Sie die Zugriffsrechte ändern wollen, und klicken Sie auf 'Rechte setzen'. Es öffnet sich eine neue Maske, in welcher Sie die bereits vergebenen Rechte einsehen, ändern und neue Rechte vergeben können.

Tipp

Auswahl korrigieren

Die ausgewählte Datei oder das Verzeichnis wird Ihnen im grau hinterlegten Bereich über dem jeweiligen Abschnitt nochmals mit absolutem Pfad angezeigt. Sollten Sie hier feststellen, dass Sie die falsche Datei oder das falsche Verzeichnis ausgewählt haben, können Sie einfach über den 'Zurück'-Button Ihres Browsers wieder zur Auswahlliste gelangen. Beantworten Sie die dabei gestellte Frage nach dem nochmaligen Senden der Daten mit 'ok', damit Sie sich direkt wieder im vorher ausgewählten Verzeichnis wiederfinden. Sie können auch auf den Menüeintrag 'Dateisystem' klicken, um wieder zurück zur ersten Maske zu gelangen.

Tipp

Im oberen Teil der neuen Maske sehen Sie bereits vergebene Rechte. Hier können Sie schnell allgemeinere Rechte vergeben oder im unteren Teil nach Gruppen oder Benutzern differenzieren.

Tipp

Berechtigungen unter Linux

Basierend auf der Art, wie unter Linux auf Dateien und Verzeichnisse zugegriffen werden kann, unterscheidet der Open School Server drei Rechte pro Benutzer oder Gruppe. Sie werden abkürzend mit r, w oder x bezeichnet. Die einzelnen Rechte sind an die jeweilige Datei oder das Verzeichnis gebunden.

Dabei gilt für Dateien:

r = read Der Benutzer kann den Inhalt der Datei einsehen, d. h. er kann sie am Bildschirm anzeigen lassen, drucken oder kopieren.

w = write Der Benutzer kann die Datei verändern, d.h. unter dem bisherigen Namen speichern oder sogar löschen.

x = execute Die Datei kann als Programm gestartet werden. Dies setzt natürlich voraus, dass die Datei ein Programm ist und funktioniert nur unter Linux.

Für Verzeichnisse gilt:

r = read Der Benutzer kann den Inhalt des Verzeichnisses einsehen, d. h. er kann Dateien in diesem Verzeichnis auflisten und auf diese zugreifen, sofern er dafür die entsprechenden Rechte besitzt.

w = write Der Benutzer kann Dateien und Verzeichnisse in diesem Verzeichnis bearbeiten und löschen. Vorsicht: Löschen gilt auch für Dateien und Verzeichnisse, für welche der Benutzer normalerweise keine Schreibrechte besitzt!

x = execute Der Benutzer kann in das Verzeichnis wechseln und dort auf sämtliche Dateien zugreifen, sofern er die nötigen Rechte dazu besitzt. Zusätzlich kann er auch auf evtl. vorhandene Unterverzeichnisse zugreifen. Sie sollten dieses Recht immer zusammen mit dem Leserecht „r“ vergeben, um evtl. missverständliche Fehlermeldungen zu vermeiden.

Tipp

Die Rechte für den Besitzer der Datei, welche immer zuerst angezeigt werden, brauchen Sie normalerweise nicht zu ändern. Sollten Sie sich selbst hier die Schreibrechte entziehen, können Sie die Datei oder das Verzeichnis auch unter Windows nicht mehr löschen. Sie können als Eigentümer der Datei aber jederzeit wieder die entsprechenden Rechte setzen.

Wenn Sie für Ihre eigene Benutzergruppe – bei Lehrern also allen Mitgliedern der Gruppe `lehrer` oder `teachers`, bei Schülern allen Mitgliedern der Gruppe `schüler` oder `users` – andere Rechte setzen möchten, etwa weil Sie diesen ein Dokument oder

Verzeichnis zugänglich machen wollen, dann können Sie dies recht schnell in der Zeile 'Gruppe' tun. Bitte beachten Sie, dass hier nur diejenige Gruppe angezeigt wird, in welcher Sie sich als Benutzer primär befinden. Wenn Sie also als Lehrer einer bestimmten Klasse ein Verzeichnis zugänglich machen wollen, so müssen Sie diese Klasse erst explizit in der unteren Maske auswählen und ihr dort die entsprechenden Rechte zuweisen.

Wenn Sie ein Dokument oder Verzeichnis für 'Andere' freigeben, beachten Sie bitte, dass dieses Dokument oder Verzeichnis dann wirklich „weltweit" freigegeben ist! Wenn es sich also nicht um Dokumente oder Verzeichnisse handelt, die Sie auch auf einer Webseite im Internet präsentieren würden, sollten Sie hier lieber keine Rechte vergeben und z. B. nur der Gruppe `users` in der unteren Maske die entsprechenden Rechte zuweisen.

Nachdem Sie schon vergebene Rechte verändert oder neuen Benutzern oder Gruppen in der unteren Maske neue Rechte vergeben haben, klicken Sie auf 'Speichern', um die Änderungen anzuwenden. Anschließend können Sie für die entsprechende Datei oder das Verzeichnis weitere Rechte vergeben.

Hinweis

ACL-Maske

Eine Besonderheit stellt der Eintrag 'Maske' dar, welcher die maximalen Rechte der eigenen Benutzergruppe und aller weiteren Benutzer und Gruppen festgelegt. Steht dort z. B. nur 'r' (Lesen), dürfen alle anderen Benutzer und Gruppen auch nur Lesen – egal was für diese zusätzlich eingestellt ist! Aus diesem Grund wird die Maske auch geändert, wenn Sie einem neuen Benutzer Rechte zuweisen, die bislang nicht in der Maske erfasst waren. Ändern Sie nächträglich die Einstellungen der Maske, so werden zwar die Rechte der anderen Nutzer und Gruppen nicht geändert – diese dürfen aber trotzdem maximal das, was ihnen die Maske vorgibt. Ein Benutzer mit Lese und Schreibrecht auf eine Datei kann die Datei dann z. B. nicht mehr verändern, wenn Sie die Maske für diese Datei nachträglich auf „nur-lesen" setzen.

Hinweis

Datei herunterladen

Wenn Sie sich im linken Bereich im Auswahlmenü bis zu einer Datei „vorgearbeitet" haben, können Sie diese mit einen Klick auf 'Datei herunterladen' vom Server auf den Client, an welchem Sie gerade sitzen, herunterladen. Da wir hier aus Sicherheitsgründen auf zusätzliche Skripte verzichten, erscheint im Downloadfenster Ihres Browsers allerdings nicht der ursprüngliche Dateiname sondern der Name der „Webseite", von

welcher der Download gestartet wird (also meist „edit_acl.pl“). Bitte ändern Sie also den Dateinamen in Ihrem Downloadfenster noch in den urspünglichen Dateinamen um oder geben Sie einen neuen Namen ein. Vergessen Sie aber insbesondere bei Windows-Clients nicht, die richtige Endung der Datei beizubehalten.

Datei hochladen

Um eine Datei von Ihrem Client, an welchem Sie gerade arbeiten, in ein Verzeichnis auf den Server hochzuladen, gehen Sie wie folgt vor:

- Navigieren Sie zunächst in das Verzeichnis auf dem Server, in welches die Datei später gespeichert werden soll.
- Drücken Sie nun auf ‘Durchsuchen’ und wählen Sie im sich öffnenden Fenster die entsprechende Datei aus (das genaue Vorgehen ist je nach verwendetem Browser unterschiedlich).
- Die ausgewählte Datei erscheint nun mit der kompletten Pfadangabe im Textfeld. Überprüfen Sie hier sicherheitshalber noch einmal, ob sich nicht eine gleichnamige Datei schon im Verzeichnis befindet – diese wird ohne Nachfrage überschrieben!
- Starten Sie den „Upload“ mit einem Klick auf ‘Datei hochladen’.

Um eine Datei in ein Verzeichnis hochladen zu können, benötigen Sie dafür Schreibrechte im entsprechenden Verzeichnis.

Überwachen der Schüler-Homeverzeichnisse

Wurde vom Administrator während der Installation die Überwachung der Homeverzeichnisse der Schüler durch Lehrkräfte erlaubt, so können Sie sich die Inhalte der Homeverzeichnisse einzelner Schüler ansehen, indem Sie in den Ordner `/home/classes` bzw. unter Windows Laufwerk `O:` wechseln. Hier finden Sie „Verknüpfungen“ zu den Homeverzeichnissen der Schüler, welche sich in der betreffenden Klasse befinden.

Hinweis

Datenschutzhinweis

Es sei hier darauf hingewiesen, dass der Zugriff auf diese Verzeichnisse einen Verstoss gegen das Datenschutzgesetz bedeuten kann. Sie sollten also eine schriftliche Genehmigung aller Eltern und Schüler einholen, "bevor" Sie dieses Feature des Open School Servers nutzen.

Hinweis

6.2.3 Rechner/Domänen

Rechnerverwaltung

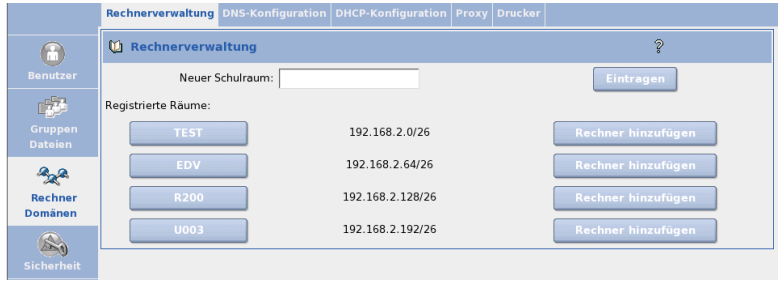

Abbildung 6.8: *Liste der definierten Schulräumen*

Unabhängig von dem Betriebsystem des Clientrechners müssen Clients am Open School Server angemeldet werden, um die Workstations einem Schulraum zuzuordnen und in die DNS– und DHCP–Dienste einzutragen. Diese Anmeldung bzw. Verwaltung der Workstations kann man leicht mit dem Webbrowser erledigen.

Unter dem Menüpunkt 'Rechnerverwaltung' bekommen Sie als erstes eine Liste der definierten Schulräume (siehe Abbildung 6.8).

Direkt nach der Installation ist diese Liste noch leer. Um einen neuen Raum zu definieren tragen Sie den Namen des neuen Raumes ins Feld 'Neuer Schulraum' ein und drücken Sie den Knopf 'Eintragen'

Hinweis

Der Rechnername wird aus dem Schulraumnamen auf folgende Weise gebildet: `<Schulraum>-pc<NN>` (also z. B. `musik1-pc01`). Aufgrund der DNS-Konventionen darf der Name eines Schulraumes nur die Buchstaben des englischen Alphabets, Zahlen und das Zeichen `'-'` enthalten. Da Windows-Betriebssysteme Rechnernamen nur bis zu einer Länge von maximal 15 Zeichen unterstützen, dürfen Schulraumnamen nicht länger als 10 Zeichen sein.

Hinweis

Klicken Sie auf einen Raum, zeigt Ihnen der Open School Server eine Liste der in diesem Raum registrierten Arbeitsplatzrechner an. Nun könnnen Sie hier die Hardwareadresse der einzelnen Rechner ändern oder den Rechner aus dem System entfernen.

Um einen oder mehrere Rechner in einen Raum aufzunehmen, wählen Sie neben dem entsprechenden Eintrag 'Rechner hinzufügen' (siehe Abbildung 6.8).

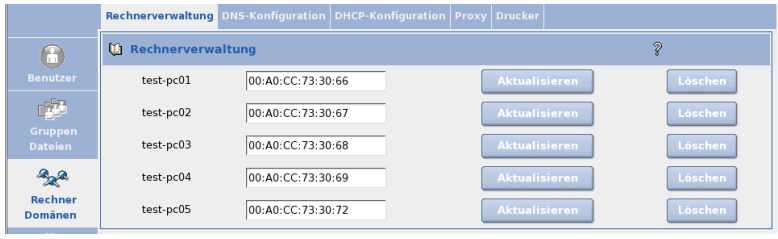

Abbildung 6.9: *Liste der registrierten Rechner*

Führen Sie die Aufnahme direkt vom Client aus durch, so erkennt der Open School Server die Hardwareadresse des zu registrierenden Rechners automatisch und trägt diese in das Feld 'Hardwareadresse:' ein (siehe Abbildung 6.10).

Auf der linken Seite finden Sie die Liste der verfügbaren Rechnernamen des Raumes. Wählen Sie den gewünschten Rechnernamen und klicken Sie auf 'Eintragen'.

Auf der nächsten Seite (Abbildung 6.11 auf der nächsten Seite) erscheint nun das Ergebniss der Registrierung. Der Browser zeigt Ihnen die IP-Adresse, den Hostnamen, die Hardwareadresse und den Netbiosname des Clients an.

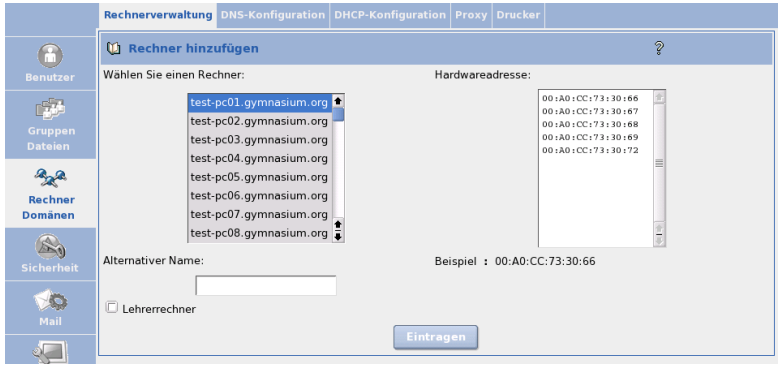

Abbildung 6.10: *Clients an den Open School Server anmelden*

Möchten Sie mehrere Rechner auf einmal registrieren, müssen Sie ins Feld `Hardwareadresse` die Hardware-Adressen sämtlicher Rechner eintragen. Anschließend wählen Sie aus der Liste 'Rechner' den ersten Rechnernamen aus und klicken anschließend auf den Knopf 'Eintragen'.

Während der Registrierung wird weiterhin ein neuer Benutzer angelegt dessen Name und Passwort dem Hostnamen des registrierten Rechners entspricht.

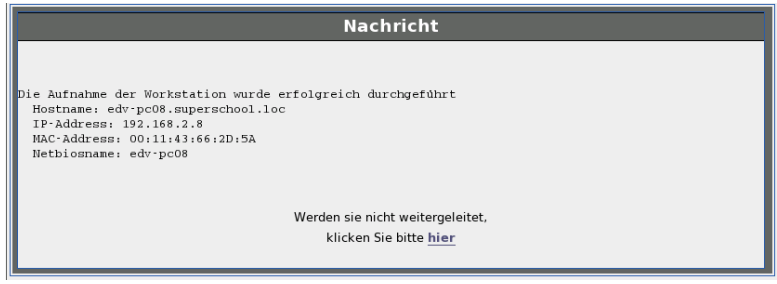

Abbildung 6.11: *Aufnahme eines Clients*

Das sind die sogenannten „Workstationbenutzer“, die sich nur an den ëigenen"Rechner anmelden können. Die Rechte dieser Benutzer sind weitesgehend eingeschränkt: Sie haben Zugriff nur auf ihr eigenes Homeverzeichnis und keinen Email-Account.

Dadurch haben Sie die Möglichkeit, z. B. Klassenarbeiten in einer geschützten Umgebung zu schreiben. In diesem Fall müssen die Schüler sich nicht mit ihrem eigenem Login (UID), sondern mit dem des jeweiligen Rechners an das System anmelden. So haben sie eine Standardumgebung und keinen Zugriff auf ihre eigenen Dateien. Weiteres dazu finden Sie im Abschnitt 6.3.2 auf Seite 114.

Hinweis

Workstationbenutzer

Mit dem Hostname als Loginname und Passwort sollte man sich nur an der Workstation anmelden, deren Hostname identisch mit dem Loginname ist. Für die Windows-Clients und die automatisch installierten SUSE LINUX Clients ist schon eine entsprechende Sperre eingebaut, die es verhindert, dass man sich mit vom Hostname abweichendem Workstationbenutzeraccount an einem Client anmeldet.

Für andere UNIX/Linux-Clients fügen Sie folgende Zeilen in die Datei `/etc/profile.local` auf den Clients zu:

```
# Workstation user may only login on its own workstation
GID=`id -g`
if test $GID -eq 503
then
  test $HOST = $USER || exit 1
fi
```

Datei 1: */etc/profile.local*

Hinweis

Möchten Sie mehrere Rechner auf einmal registrieren, müssen Sie ins Feld 'Hardwareadresse:' deren Hardwareadressen eintragen aus der Liste 'Wählen Sie einen Rechner:' den ersten Rechnernamen auswählen und anschließend auf dem Knopf 'Eintragen' drücken.

Vor der eigentlichen Anmeldung müssen die Clients vorab meist noch richtig konfiguriert ggf. in die Windowsdomäne aufgenommen werden. Wie das geschieht, hängt vom Betriebsystem des Clientsrechners ab und wird ausführlich im im Kapitel 7 auf Seite 125 beschrieben.

DNS Konfiguration

Hier können Sie virtuelle Domains anlegen, Rechnern Namen zuweisen und auch wieder löschen, sowie die Werte für `SOA`, `NS` und `MX` in den Zonendateien ändern.

Hinweis

Sämtliche Änderungen innerhalb dieses Menüpunktes werden erst dann aktiviert, wenn Sie auf die Schaltfläche 'Exportieren' klicken.

Hinweis

Um evtl. Fehler in der Konfiguration des DHCP-Servers zu vermeiden, werden über den Menüpunkt `Neu` aufgenommene Clients in der DNS-Konfiguration nicht aufgelistet. Sie können sich trotzdem einen Überblick über die im Open School Server registrierten Clients verschaffen, wenn Sie in der DHCP-Konfiguration unter dem Menüpunkt 'Hosts verwalten' nachsehen.

Anlegen und Bearbeiten von virtuellen Domains Oft benutzt eine Schule mehrere Domain-Namen, z. B. ist `schule.de` Hauptdomain, virtuelle Domains sind `schule.com`, `meine-schule.de` usw. Häufig haben die zusätzlichen Domains nur einen funktionalen Zweck, um z. B. die Webpräsenz in verschiedenen Sprachen darzustellen. Der Open School Server unterstützt die Verwendung beliebig vieler virtueller Domains und Benutzer, und kann durch diese Erweiterung auch zwischen den Benutzern in den verschiedenen Domains unterscheiden. Dabei werden E-Mails an einen virtuellen Benutzer in einer virtuellen Domain (z. B. `direktor@physik-schule.de`) an einen realen Benutzer in der Hauptdomain (z. B. `direktor@schule.de`) weitergeleitet.

Es ist erlaubt, denselben lokalen Teil einer E-Mail-Adresse (in diesem Beispiel `direktor`) für die Hauptdomain sowie in der virtuellen Domain zu verwenden. Der Open School Server unterscheidet dies anhand der Domain. Bei Bedarf geben Sie dem realen Empfänger als Absendeadresse die virtuelle E-Mail-Adresse. Nach außen haben Sie damit eine domainabhängige Benutzerverwaltung.

Bevor Sie einen virtuellen Benutzer anlegen können, müssen Sie die zugehörige virtuelle Domain erstellen. Klicken Sie auf 'Rechner/Domänen' und dort auf 'DNS-Konfiguration'. Eine neue Domain wird angelegt, indem Sie im Feld hinter 'Neue Domain' den Namen der Domain eingeben und mit 'Hinzufügen' bestätigen (siehe Abbildung 6.12). Auf diese Weise können Sie beliebig viele virtuelle Domains hinzufügen.

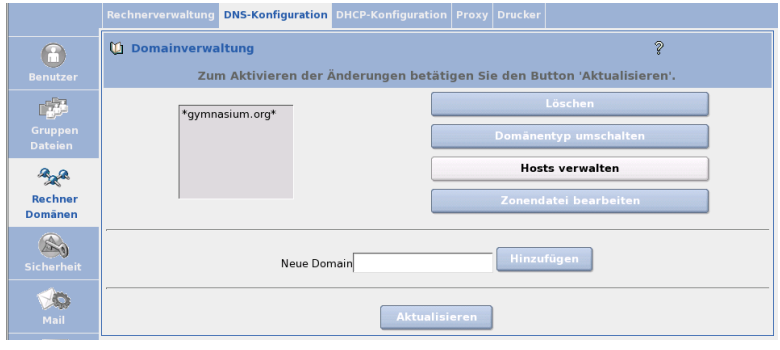

Abbildung 6.12: *Anlegen und Bearbeiten von virtuellen Domains*

Um die bestehenden Domains in die Konfiguration des Nameservice aufzunehmen, klicken Sie auf den Knopf 'Exportieren'. Die neue Domain sollte nun in der Liste im linken, oberen Bereich auftauchen.

Möchten Sie zusätzlich zur automatisch generierten Konfiguration für die Domain des Open School Servers und die virtuellen Domains selbst noch Zonendatenbanken hinzufügen, benutzen Sie einfach Namen, die mit den vom Open School Server generierten nicht übereinstimmen. Die Zonendateien werden nach folgendem Schema benannt:

Für das so genannte „Forward Mapping“: `/var/named/schule.de.zone`. Für das „Reverse Mapping“ wird die „IN-ADDR.ARPA“-Adresse in den Dateinamen abgelegt.

Um eine bestehende Domain zu löschen, wählen Sie sie aus der Liste im oberen, linken Fenster aus und klicken Sie auf `Löschen`. Sie können eine Domain allerdings erst dann löschen, wenn keine virtuellen Email-Adressen mehr für diese Domain definiert sind.

Domänentyp umschalten Der Open School Server unterstützt zwei Arten virtueller Domains. Ihr Verhalten entspricht der Art und Weise, wie diese über LDAP-Anfragen abgebildet („gemappt“) und auf „virtual tables“ von postfix aufgesetztwerden. Details dazu entnehmen Sie der Datei `/etc/postfix/virtual`.

Typ virtual (default) In dieser Art virtueller Domain existiert keine E-Mail-Adresse, solange Sie keine virtuelle Adresse angelegt haben. Lokale Benutzer können unter dieser Domain *keine* Mail empfangen. Wird eine Mail an eine nicht existente Adresse innerhalb dieser Domäne geschickt, wird die Mail vom MTA (postfix) als nicht existent abgewiesen.

Typ local Alle lokalen Benutzer können unter dem Namen der Domain E-Mail empfangen.

Hosts verwalten Um im Nameserver einen neuen DNS-Eintrag hinzuzufügen oder zu löschen, wählen Sie 'Hosts verwalten' aus. Im nächsten Bild sehen Sie im linken Rahmen alle Hosts aufgelistet.

Tipp

Im DHCP eingetragene Hosts

Beachten Sie bitte, dass in dieser Liste die über das Menü 'Neu' hinzugefügten Clients nicht aufgelistet werden. Diese Hosts können Sie nur in der DHCP-Konfiguration sehen und auch löschen.

Damit wird vermieden, dass der DHCP-Server aufgrund eines verwaisten Eintrages nicht startet, wenn in der DNS-Konfiguration ein Client gelöscht wurde, ohne ihn auch im DHCP-Server zu löschen.

Tipp

Klicken Sie nun auf ‘Host anlegen’ und geben Sie den Hostnamen und die IP-Nummer des neuen Rechners ein und bestätigen mit ‘Erstellen’.

Sie können anschließend weitere Hostnamen und deren IP-Nummern angeben oder die Maske durch einen Klick auf ein anderes Menü verlassen.

Um einen Client aus dem lokalen Netzwerk zu entfernen, wählen Sie den entsprechenden Eintrag im linken Bereich aus und dann die Option ‘Host löschen’.

Achtung

Auch wenn sich die IP-Nummer eines Clients geändert hat, muss dieser erst entfernt und anschließend ein neuer Eintrag erstellt werden.

Achtung

DHCP–Konfiguration

Unter ‘Rechner/Domänen’ gelangen Sie zum Dialog der DHCP-Konfiguration. Sie haben die Möglichkeit zum Anlegen und Löschen von Subnetzen, Gruppen und Rechnern bzw. zum Editieren von DHCP–Einträgen.

Hinweis

Normalerweise brauchen Sie hier keine Einstellungen vorzunehemen. Alle nötige Konfigurationen werden während des Registrierens der Rechner vorgenommen. Nur in ganz speziellen Fällen müssen Sie die DHCP–Optionen ändern.

Hinweis

Konfiguration des DHCP-Servers Um einen neuen Eintrag (Subnetz, Gruppe oder Rechner) zur Konfiguration hinzuzufügen, klicken Sie auf die Auswahlbox der entsprechende Schaltfläche (vgl. Abbildung 6.13 auf der nächsten Seite).

Sie sehen in diesem Menü auch die bestehenden Subnetze, Gruppen, Rechner und IP-Pools, die schon während der Installation des Open School Servers angelegt wurden. Unter den jeweiligen Einträgen wählen Sie eine Aktion aus der Auswahlbox und klicken auf ‘Aktion durchführen’.

Zu Pools und Hosts können keine weiteren Einträge hinzugefügt werden, diese können lediglich gelöscht werden.

Achtung

Beim Löschen eines Eintrages werden alle untergeordneten Einträge auch gelöscht.

Achtung

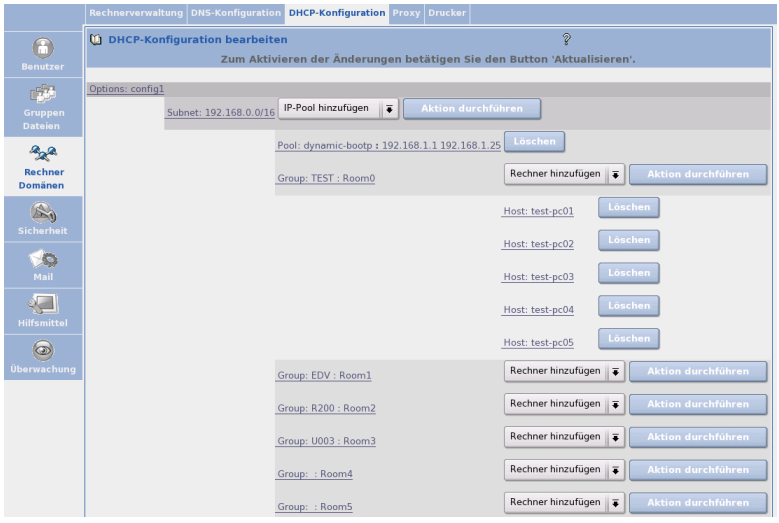

Abbildung 6.13: *DHCP-Konfiguration*

Möchten Sie die DHCP-Optionen oder -Statements in einem Eintrag ändern oder neue hinzufügen, wählen Sie als Aktion 'Bearbeiten' aus. Folgende DHCP-Einträge können angelegt werden:

DHCP-Subnetz Das ist der Grundeintrag für den DHCP-Server. Durch diesen Eintrag wird dem DHCP-Server mitgeteilt, für welche Subnetze mit welcher IP-Adressenmaske er zuständig ist. In ein Subnetz können alle weiteren DHCP-Objekte eingefügt werden.

Gruppe In eine Gruppe werden Rechner(namen) zusammengefasst, die mit gleichen DHCP-Parametern (Optionen, Statements) vom DHCP-Server versorgt werden müssen. Zu einer Gruppe können nur Rechner-Objekte hinzugefügt werden. Eine Gruppe kann sowohl Mitglied der globalen Konfiguration als auch Mitglied eines Subnetzes sein.

IP-Pool Ein Adressenpool definiert einen IP-Adressenbereich, der anders als die übrigen IP-Adressen behandelt werden muss. Beim Anlegen des DHCP-Pools werden die im IP-Pool befindlichen IP-Adressen beim Nameserver eingetragen, und für diese IP-Adressen werden Rechnernamen generiert.

Rechner Um einen Rechner in die DHCP-Konfiguration einzutragen, muss dieser vorher in der DNS-Konfiguration eingetragen werden. Ein Rechner kann zu der

Grundkonfiguration, zu einem DHCP-Subnetz oder zu einer Gruppe hinzugefügt werden.

Hinweis

Bitte beachten Sie, dass mindestens ein Subnetz definiert sein muss, damit der DHCP-Server gestartet werden kann.

Hinweis

Die Änderungen der DHCP-Konfiguration werden vom LDAP-Server gespeichert. Klicken Sie auf 'Exportieren'. Dadurch wird die Konfiguration des DHCP-Servers erstellt und neu geladen.

Eine Gruppe zur DHCP-Konfiguration hinzufügen In diesem Dialog legen Sie eine neue DHCP-Gruppe an. In einer Gruppe werden Rechner(namen) zusammengefasst, die mit gleichen DHCP-Parametern (Optionen, Statements) vom DHCP-Server versorgt werden müssen. Zu einer Gruppe können nur Rechner-Objekte hinzugefügt werden. Eine Gruppe kann sowohl Mitglied der globalen Konfiguration als aucheines Subnetzes sein.

Legt man eine Gruppe im 'Globalen DHCP-Eintrag' an, können die Rechner dieser Gruppe ihre IP-Adressen aus verschiedenen Subnetzen bekommen. Es müssen jedoch in diesem Fall alle Subnetze konfiguriert werden. Legt man eine Gruppe in einem DHCP-Subnet ab, muss dafür Sorge getragen werden, dass die Rechner dieser Gruppe ihre IP-Adressen aus diesem Subnetz bekommen.

Die Bezeichnung einer Gruppe kann frei gewählt werden. Klicken Sie auf 'Bestätigen', um die neue Gruppe in die DHCP-Konfiguration einzutragen. Ändern Sie gegebenenfalls die automatisch erstellten DHCP-Optionen und -Statements für die neu angelegte Gruppe unter 'Experten-Optionen'.

Einen Rechner zur DHCP-Konfiguration hinzufügen Ein Klick auf 'Rechner hinzufügen' führt Sie zum entsprechenden Dialog. Wählen Sie die gewünschte Domain aus und klicken Sie auf 'Weiter'. Selektieren Sie einen Rechner aus der Liste, geben Sie die Hardwareadresse der Netzwerkkarte (MAC) in das entsprechende Feld ein und klicken Sie auf Bestätigen. Sollte sich der Rechner noch nicht in der Liste befinden, muss er zuvor im Dialog 'DNS-Konfiguration' über 'Host anlegen' in einer DNS-Domain angelegt werden. Sind in der gewählten Domain noch keine Rechner angelegt, die in die DHCP-Konfiguration aufgenommen sind, werden Sie automatisch zur 'DNS-Konfiguration' weitergeleitet.

Wurde der Rechner hinzugefügt, können Sie bei Bedarf DHCP-Optionen und Statements für den neu angelegten Rechner definieren. Klicken Sie dazu auf 'Experten-Optionen'.

Hinweis

Wurde ein Rechner zur DHCP-Konfiguration hinzugefügt, kann er nicht aus dem Nameserver entfernt werden. Er wird im Dialog 'DNS-Konfiguration' → 'Hosts verwalten' → 'Host löschen' nicht zur Auswahl angeboten, da das versehentliche Löschen dieses Eintrages die Funktionalität des DHCP-Servers beeinträchtigt. Möchte man einen in der DHCP-Konfiguration eingetragenen Rechner aus dem Nameserver entfernen, muss als erstes dessen DHCP-Hosteintrag gelöscht werden.

Hinweis

Einen IP-Adressenpool zur DHCP-Konfiguration hinzufügen Mit diesem Menüpunkt haben Sie die Möglichkeit zum Anlegen eines neuen IP-Adressenbereiches.

Ein Adressenpool definiert einen IP-Adressenbereich, der anders als die übrigen IP-Adressen behandelt werden muss und dessen Adressen von dem DHCP-Server dynamisch vergeben werden.

Beim Anlegen des DHCP-Pools werden die im IP-Pool befindlichen IP-Adressen in den Nameserver eingetragen, und für diese IP-Adressen werden Rechnernamen generiert. Deshalb müssen Sie als erstes die DNS-Domäne auswählen, in der die neuen Rechnernamen eingetragen werden sollen.

Anschließend müssen Sie eine Bezeichnung für diesen Adressenpool angeben. Dieser Name ist frei wählbar und wird in das Feld 'Bezeichnung' eingetragen.

Die im Feld 'Prefix' für die Hostnamen eingetragene Zeichenkette wird für dieGenerierung der Rechnernamen auf folgende Weise verwendet:

Der Adressenbereich reicht von `192.168.1.10` bis `192.168.1.29`, dasPrefix heißt `dhcpPC-` und die gewählte DNS-Domäne lautet `schule.de`. In diesem Fall werden folgende Rechnernamen und IP-Adressengeneriert und in den Nameserver eingetragen:

```
dhcpPC-01.schule.de -> 192.168.1.10
dhcpPC-02.schule.de -> 192.168.1.11
dhcpPC-03.schule.de -> 192.168.1.12
...
...
...
dhcpPC-18.schule.de -> 192.168.1.27
dhcpPC-19.schule.de -> 192.168.1.28
dhcpPC-20.schule.de -> 192.168.1.29
```

Den gewünschten Adressenbereich tragen Sie bitte in die Felder 'IP-Adressenbereich' ein.

Hinweis

Die so generierten Rechnernamen können nur durch das Löschen des DHCP-IP-Adressenpools aus dem Nameserver entfernt werden. Sie werden unter dem Menüpunkt 'DNS-Konfiguration'/'Host löschen' nicht zur Auswahl angeboten, da das versehentliche Löschen dieser Einträge die Funktionalität des DHCP-Servers beeinträchtigt.

Bitte beachten Sie, dass der DHCP-Server für jede IP-Adresse in einem Pool einen Teil des Hauptspeichers des Rechners reserviert. Wählt man den Adressenbereich zu groß, werden eventuell unnötig viele Ressourcen des Computers in Anspruch genommen; im äußersten Fall kann der DHCP-Server wegen Speichermangels gar nicht gestartet werden.

Hinweis

Klicken Sie auf 'Eintragen', um den neuen IP-Adressenpool in die DHCP-Konfiguration einzutragen. Anschließend können Sie DHCP-Optionen und -Statements für den neu angelegten Pool definieren, indem Sie in dem Browser unter dem Menüpunkt 'DHCP-Konfiguration' auf diesen Pool klicken.

Ein Subnetz zur DHCP-Konfiguration hinzufügen Klicken Sie auf 'Subnetz hinzufügen'. In den Feldern 'Subnetz' definieren Sie die Netzwerkadresse und in dem Feld 'Netzmaske' die Netzmaske des Subnetzes. Die Netzmaske kann sowohlin Bitmaskform (z. B. `24`) als auch in Dezimalform (`255.255.255.0`)angegeben werden.

Durch diesen Eintrag wird dem DHCP-Server mitgeteilt, für welche Subnetze mitwelcher IP-Adressenmaske er zuständig ist. In ein Subnetz können alle weiterenDHCP-Objekte eingefügt werden.

Klicken Sie auf 'Eintragen', um das neue Subnetz in die DHCP-Konfiguration einzutragen. Ändern Sie gegebenenfalls die DHCP-Optionen und -Statements für das neu angelegte Subnetz über 'Experten-Optionen'.

Optionen und Statements eines DHCP-Eintrages Im Dialog 'Experten-Optionen' ändern oder löschen Sie die Optionen und Statements eines DHCP-Eintrages. In der Maske sind die aktuellen Werte des Eintrages dargestellt. Einige Parameter (u.a. Objektklassen, `cn`) sind nur lesbar dargestellt. Um den Wert einer Option oder eines Statements zu ändern, bearbeiten Sie das entsprechende Textfeld und klicken Sie danach auf 'Änderungen speichern'. Um eine Option oder ein Statement zu löschen, klicken Sie auf den Checkbutton rechts neben dem Wert und anschließend auf 'Änderungen

speichern'. Um eine neue Option oder ein neues Statement in den DHCP-Eintrag aufzunehmen, tragen Sie diese in das Feld 'Neu' ein und klicken dann auf 'Änderungen speichern'.

Hinweis

Bei DHCP-Optionen darf das Wort `option` nicht mit eingetragen werden.

Hinweis

Wenn Sie auf das Fragezeichen neben dem Feld 'Neu' klicken, öffnet sich ein Fenster mit der Liste der DHCP-Optionen und -Statements. Wählen Sie den gewünschen Eintrag aus, klicken Sie auf 'DHCP-Parameter wählen' und auf 'Schließen'. Der Eintrag wird in das Feld 'Neu' übernommen und kann gegebenenfalls erweitert werden.

Mit dem Button 'Zurücksetzen' stellen Sie die vorherigen Werte wieder her. Durch Klick auf 'Exportieren' wird die Konfiguration des DHCP-Servers erstellt und neu geladen.

Hinweis

Bitte beachten Sie, dass falsche Einträge in der Konfiguration Fehlfunktionen des DHCP-Servers verursachen können. Ein syntaktischer Fehler führt meist dazu, dass der DHCP-Server nicht neu gestartet werden kann.

Hinweis

Dynamic DNS

Dynamic DNS ist ein Service, mit dem Sie einen oder mehrere Hostnamen für Ihre dynamische IP-Adresse vergeben können. Sobald Sie sich neu ins Internet einwählen und eine neue dynamische IP-Adresse bekommen, wird die neueIP-Adresse einfach beim Namen eingetragen. Auf diese Weise bleiben Sie unter diesem Hostnamen für andere Benutzer erreichbar.

Hinweis

Dieser Menüpunkt ist nur dann sichtbar, wenn Sie während der Installation eine DSL-/ Modem- oder ISDN-Verbindung eingerichtet haben.

Hinweis

Um diesen Dienst zu nutzen, muessen Sie sich zunächst bei einem Anbieter dieser Services anmelden und bekommen dort einen Login-Namen und ein Passwort, mit dem Sie einen oder auch mehrere Hostnamen verwalten können. Die Anbieter stellen Ihre Dienste in unterschiedlichem Umfang zur Verfügung, einige sind kostenlos, andere gegen eine Gebühr erhältlich. Je nach Anbieter können Sie einen Namen aus vorgegebenen Listen von Domains aussuchen oder auch eine eigene Domain registrieren lassen (z.B. Custom-DNS Service bei `www.dyndns.org`).

Bei einigen Anbietern bzw. Services können Sie noch weitere Einstellungen vornehmen, etwa die Benutzung von Wildcards, Angabe eines Mail-Servers oder eines Backup Mail-Servers. Diese zusätzlichen Einstellungen werden nur bei Anbietern angezeigt, die diese auch unterstützen.

Login: Tragen Sie hier den registrierten Benutzernamen ein.

Passwort: Geben Sie Ihr registriertes Passwort ein.

Hostname: Tragen Sie hier den beim Dynamic-DNS Anbieter registrierten Hostnamen oder auch eine mit Komma getrennte Liste von Hostnamen ein. Beim Anbieter `www.dslreports.com` erhalten Sie statt eines Hostnamens eindeutige Nummern, welche Sie bitte in das Feld für Hostnamen eintragen.

Wildcard: Dieser Schalter erlaubt die Benutzung des Dynamic-DNS Hostnamens als eine Art Sub-Domain. Lautet Ihr Hostname `myhostname.dyndns.org`, werden auch die Namen `www.myhostname.dyndns.org` und `ftp.myhostname.dyndns.org` auf `myhostname.dyndns.org` verweisen.

Mail-Server: Hier können Sie den Hostnamen eines Mail- Servers angeben, der E-Mails für Ihren Host entgegen nehmen soll (z. B. Mailserver Ihres Providers). Sie werden dann nicht direkt an Ihren Host zugestellt.

Hinweis

Dieser Mail-Server muss passend konfiguriert sein und E-Mails für Ihren Hostnamen akzeptieren.

Hinweis

Backup Mail-Server Aktivieren Sie die Checkbox 'Backup Mail-Server', wird der unter Mail-Server angegebene Host als Backup Mail-Server verwendet. Als primärer Mail-Server wird Ihr Hostname mit dynamischer IP-Adresse verwendet. In diesem Fall wird zunächst versucht, E-Mails an den Hostnamen mit dynamischer IP zuzustellen, und falls dieser nicht erreichbar ist, an den sekundären Mail-Server.

Falls Sie keinen Mail-Server angeben, sollten Sie den Hostnamen auch als virtuelle Domain in der 'DNS-Konfiguration' anlegen, damit die E-Mails angenommen werden. Dies ist nicht notwendig, wenn Sie den Hostnamen nicht zum Mail-Emfang benutzen.

Achtung

Beachten Sie, dass bei dynamischen IP-Nummern, auch wenn der Rechner offline ist, der Name weiterhin auf die IP-Nummer zeigt. Vergibt der Provider diese IP-Nummer an einen Dritten, bekommt dieser die E-Mails!

Achtung

Update-Typ: DynDNS.org bietet drei Arten von Dynamic-DNS an. Wählen Sie diese passend zum Hostnamen-Typ bei DynDNS.org aus.

dyndns: Dynamic-DNS ist die Standard-Einstellung.

static: Static-DNS ist ähnlich Dynamic-DNS, jedoch mit einer längeren Gültigkeit der IP-Adresse. Interessant wird dies, falls Ihr Provider Ihnen fast immer die gleiche IP-Adresse vergibt, sie sich also nur sehr selten ändert.

custom: Custom-DNS erlaubt Updates für Ihre eigenen (Sub-)Domains, die Sie bei DynDNS.org betreiben.

Proxy

Im Proxy-Dialog ist standardmäßig bereits die IP-Adresse des Proxy Servers (z. B. `192.168.0.5`) und der Port `8080` eingetragen.

Die Größe des Cachespeichers ist auf 1000 MB foreingestellt, kann allerdings je nach bedarf geändert werden.

Der Open School Server liefert einen Jugendschutzfilter für das Aussperren von kritischen Webseiten mit. Das Filtern erledigt das Hilfsprogramm SquidGuard. Die Checkbox 'SquidGuard benutzen' ist aktiviert, kann allerdings hier abgeschaltet werden, wenn Sie SquidGuard nicht benutzen wollen.

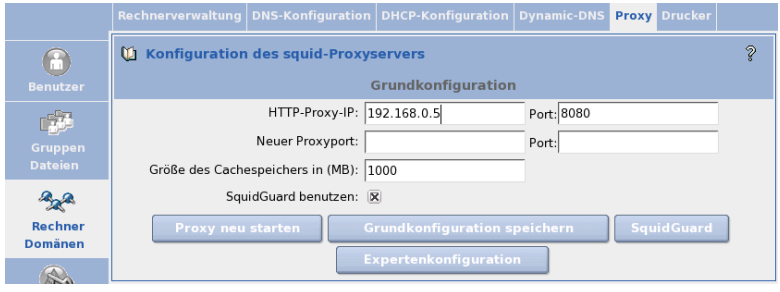

Abbildung 6.14: *Proxy-Konfiguration*

Über die Schaltfläche 'Expertenkonfiguration' gelangen Sie zum ACL–Dialog. Hier definieren Sie neue oder bearbeiten bestehende ACLs (engl. *Access Control Lists*).

Nachdem Sie ACLs definiert haben, klicken Sie auf 'ACLs anordnen', um die Reihenfolge der Abarbeitung festzulegen. Die Regeln werden von oben nach unten abgearbeitet, bis die erste zutrifft. Über die Schaltfläche 'Grundkonfiguration' gelangen Sie zurück zum Proxy-Dialog.

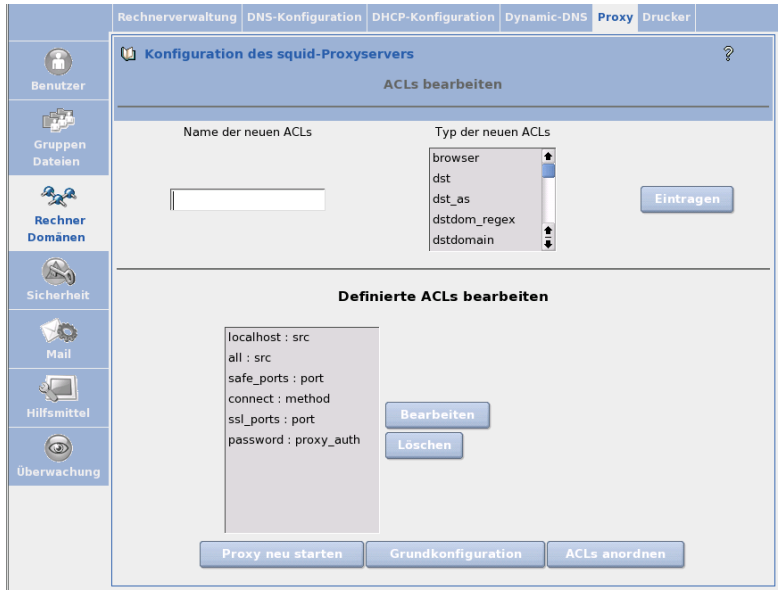

Abbildung 6.15: *ACL-Definition*

ACLs definieren In Abbildung 6.15 sehen Sie den ACL-Dialog. Vergeben Sie zunächst einen Namen für die anzulegende Liste. Als Nächstes wählen Sie einen 'Typ' für Ihre ACL. Folgende Typen stehen zur Verfügung:

browser Angabe von Browsern.

dst (destination) Angabe der Zieladressen.

dstdomain Angabe der Ziel-Domain.

dstdom_regex Angabe der Ziel-Domain unter Verwendung regulärer Ausdrücke.

ident Benutzerauthorisierung über den ident-Dämon. Hier kann man Benutzername(n) oder das `REQUIRED` angeben; dies gilt für alle gültigen Benutzernamen.

maxconn Bestimmung der maximalen Verbindungsanzahl.

method Angabe der Methode wie `CONNECT`, `POST` oder `GET`.

port Angabe des Ports.

proto (protocol) Hier legen Sie die entsprechenden Protokolle fest.

proxy_auth Benutzer-Authentifizierung erfolgt über `squid_ldapauth`

snmp_community Angabe der SNMP-Community (Simple Network Management Protocol). Damit erlauben Sie bestimmten SNMP-Agents den Zugriff auf Squid. Die Voreinstellung für `community` ist `public`, der Wert kann jedoch beliebig geändert werden und dient zur Authorisierung der Agenten. Diese können unter anderem Informationen über Version, Speicher und Festplattenverbrauch vom laufenden Squid abfragen.

src (source) Bestimmung der Quelladressen.

srcdomain Angabe der Quell-Domain.

srcdom_regex Angabe der Quell-Domain unter Verwendung regulärer Ausdrücke.

time Angabe der Zeit.

url_regex Angabe von URL-Adressen unter Verwendung regulärer Ausdrücke.

urlpath_regex Angabe von URL-Pfaden unter Verwendung regulärer Ausdrücke.

Ausführliche Dokumentation (in Englisch) zum Proxy Squid finden Sie unter `http://squid.visolve.com/squid24s1/contents.htm`; genauere Beschreibungen zu den verschiedenen ACLs liefert Ihnen die Seite: `http://squid.visolve.com/squid24s1/access_controls.htm`

Klicken Sie auf 'Eintragen', um eine neue ACL der Liste von bereits angelegten ACLs hinzuzufügen.

Klicken Sie auf 'Bearbeiten', öffnet sich ein Fenster, in dem Sie Werte eintragen bzw. ändern können, die für eine von Ihnen ausgewählte ACL gelten sollen. Sie können im Eingabefeld neue Werte hinzufügen bzw. bestehende Werte editieren oder löschen.

Komplette ACLs entfernen Sie über die Schaltfläche 'Löschen'. Sichern Sie Ihre Änderungen mit dem Button 'Speichern'.

Ein Klick auf 'Zurück' bringt Sie wieder zur Proxy-Konfiguration.

Mit 'ACLs anordnen' gelangen Sie zum Dialog, in dem Sie die Reihenfolge der ACLs festlegen.

ACLs anordnen Die Einstellungen bei 'Definierte ACLs' und 'Definierte ACLs negiert' werden „UND"-verknüpft. Mit dem 'Aktion'-Auswahlfeld wählen Sie zwischen 'allow' zum Erlauben bzw. 'deny' zum Verbieten der Internetzugriffe.

Wählen Sie aus 'Definierte ACLs' eine bereits angelegte Liste, für die Ihre Einstellungen gelten sollen, oder bestimmen Sie über 'ACL-negiert' eine ACL, die negiert eingesetzt werden soll. Erlauben Sie z. B. das Abrufen von Internetseiten (Auswahl bei 'ACL'), die aber nicht über SSL-Ports laufen(Auswahl bei 'ACL-negiert').

Eine neue Regel binden Sie über ‘Eintragen’ ein. Sie wird dann im Listenfeld mit definierten ACLs aufgeführt. Zum Löschen von Regeln wählen Sie die entsprechende aus und klicken auf ‘Löschen’. Mit den Buttons ‘Nach oben’ und ‘Nach unten’ verschieben Sie eine markierte Regel in der Liste.

Achtung

Die Reihenfolge der Regeln im Listenfeld ist sehr wichtig, denn die aufgestellte Liste wird von oben nach unten abgearbeitet. Je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben oder gesperrt.

Achtung

Haben Sie alle Veränderungen vorgenommen, gelangen Sie mit ‘Grundkonfiguration’ wieder zum Proxy-Dialog. Damit Ihre Veränderungen wirksam werden, starten Sie über die Schaltfläche den Proxy neu.

Drucker

Im Drucker-Dialog finden Sie zunächst eine Reihe von Links zum Druckserver. Über diese Links können Sie sich eine Übersicht über die Drucker und die Druckjobs verschaffen oder den Druckserver administrieren.

Zur Übersicht der Drucker Hier finden Sie eine Liste sämtlicher auf dem Open School Server installierten Drucker mit Bezeichnung, Standort und der Anzahl der aktuellen Druckaufträge.

Klickt man auf den Namen eines Druckers, gelangt man zur Liste der aktuellen Druckaufträge (hier werden dann u.a. Eigentümer, Größe und Startzeit angezeigt).

Klickt man auf ‘Zurücksetzen’, werden sämtliche Druckaufträge des Druckers gelöscht und der Drucker wird wieder freigeben.

Zugriffsrechte / Quota In diesem Dialog können Zugriffsrechte auf bestimmte Drucker für einzelne Gruppen oder Benutzer erteilt werden.

Weiterhin können Sie hier festlegen, wie viele Seiten ein Benutzer in einem bestimmten Zeitraum auf einem bestimmten Drucker drucken darf.

Hinweis

Das Setzten von Quotas bzw. Quotaperioden ist für sog. raw-Queues nicht möglich, da in diesem Fall der Printserver keine Information über die Inhalte der Druckaufträge erhält.

Hinweis

Links zum Druckserver Der beim Open School Server verwendete Druckserver CUPS verfügt über ein eigenes Webfrontend zur Administration. Normalerweise brauchen Sie dieses Webfrontend nicht – allerdings können Sie damit Aufgaben zur Wartung von Druckern an andere Benutzer abgeben oder (abhängig vom jeweiligen Druckertyp) z. B. auch einige Standardeinstellungen bezgl. der Druckqualität für alle Benutzer vorgeben.

In diesem Menü finden Sie Links, die Sie auf entsprechende Seiten des CUPS-Webfrontends führen.

Für einige dieser Webseiten (z. B. 'Zu den Einrichtungsaufgaben') benötigen Sie das Passwort für den Drucker-Administrator. Dieses Passwort sollte *nicht* identisch mit dem Passwort des Benutzers `admin` oder des Benutzers `root` sein, da einige Daten unverschlüsselt über das Netzwerk gesendet werden.

Wenn kein Passwort für den Drucker-Administrator vergeben wurde, kann sich diese nicht am Webfrontend anmelden. Vergeben Sie deshalb zunächst ein Passwort für diesen Drucker-Administrator, indem Sie es (im Klartext) in das dafür vorgesehene Feld 'Passwort für den Druckserveradministrator (admin)' eingeben. Das Passwort muss aus mindestens 6 Ziffern und Buchstaben bestehen und darf den Benutzernamen nicht enthalten.

Anschließend können Sie auch administrative Aufgaben (wie z. B. das Installieren von neuen Druckern) über das CUPS-Webfrontend erledigen. Melden Sie sich dazu als Benutzer `admin` mit dem für diesen Benutzer vergebenen Passwort am Webfrontend an, wenn Sie dazu aufgefordert werden.

Tipp

Es ist sinnvoll die Netzwerkdrucker so einzurichten, dass diese eine IP-Adresse aus dem Servernetz bekommen und ihre Netzwerkmaske auf 255.255.255.0 gesetzt wird. Dies können Sie über eine fest IP-Zuordnung am Drucker selbst vornehmen - oder über den Menüpunkt 'DHCP' der MAC-Addresse des Druckers vom DHCP-Server eine feste IP-Addresse in diesem Bereich zuweisen lassen.

Dadurch wird verhindert, dass die Clients die Netzwerkdrucker direkt, unter Umgehung des Printservers, erreichen können.

Tipp

Administration des lokalen Druckservers Hier nehmen Sie Einstellungen zum lokalen Druckserver vor, die Sie nicht über das CUPS-Webfrontend tätigen können.

Geben Sie an, an welche IP-Adressen oder Broadcast-Adressen eines ganzes Netzwerks die Informationen über installierte Drucker geschickt werden sollen. Auch das Zeitintervall für das Versenden der Informationen können Sie hier angeben.

Mit Return oder über das Pfeil-Symbol wird die Eingabe übernommen.

Sie können den Zugriff auf den Druckserver auch auf bestimmte Rechner oder Netzwerke einschränken. Geben Sie dazu im folgenden Feld die IP-Adressen derjenigen Rechner an, die Zugriff erhalten sollen.

Im letzten Feld erteilen Sie bestimmten Rechnern über deren IP-Adressen administrativen Zugriff auf den Druckserver. Andere Rechner können dann zwar noch drucken, aber keine Drucker mehr administrieren.

6.2.4 Sicherheit

Zugangsrechte setzen

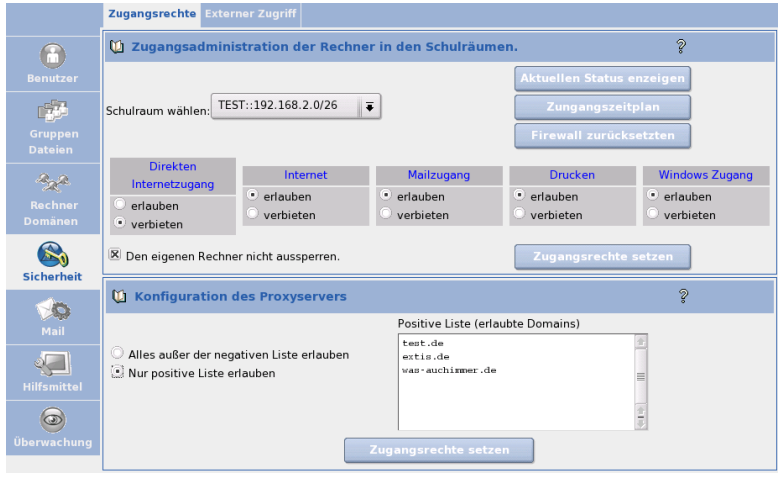

Abbildung 6.16: *Zugangsadministration der Rechner in den Schulräumen*

Haben Sie die Rechner der Schule an den Open School Server angemeldet und Schulräumen zugewiesen, besteht die Möglichkeit, den Rechnern eines Schulraumes bestimmte Dienste zu sperren bzw. zu gestatten.

Dies betrifft folgende Dienste:

- Direkter Internetzugang
- Internetzugang über Proxy
- Zugang zum Mail– und Groupware–Server

- Zugang zu Windowsanmeldung
- Zugang zum Printserver

Diese Möglichkeit besteht jedoch nicht nur für den Hauptadministrator `admin` und Systemadministratoren sondern auch für Lehrkräfte. Während diese die Dienste allerdings nur für den aktuellen Klassenraum ein– und ausschalten können, darf ein Systemadministrator dies für jeden PC-Raum tun.

Zugangszeitplan Unter dem Menüpunkt 'Zugangszeitplan' kann der Hauptadministrator (bzw. Lehrer mit Administrationsrechten) je Schulraum einen Zugangszeitplan erstellen.

Externer Zugriff

Diese Funktion steht Ihnen nur dann zur Verfügung, wenn der Open School Server bei der Installation als Internet Gateway konfiguriert wurde.

Normalerweise blockiert die Firewall des Open School Servers jeden Zugriff aus dem Internet. Hier können Sie den Open School Server so konfigurieren, dass einige Dienste auch über das Internet erreichbar sind. Dies betrifft unter anderem den SSH-Zugang und den Zugriff auf die Administrations- und die Benutzerweboberfläche.

Achtung

Neustart der Firewall

Wenn Sie in diesem Menü Änderungen vornehmen, muss die Firewall neu gestartet werden. Damit werden aber auch alle Zugriffsrechte der einzelnen Klassenräume wieder in den Ausgangszustand versetzt!

Sie sollten also Änderungen hier nur durchführen, wenn niemand mehr mit den Schulrechnern arbeitet.

Achtung

SSH Zugriff Wenn Sie diese Schaltfläche aktivieren, können Sie den Server über eine SSH-Verbindung Fernadministrieren. Hierfür wird in der Firewall der Port 22 für einen externen Zugriff freigeschaltet.

Wenn Sie X-forwarding aktivieren, können Sie aus der Ferne den Open School Server so administrieren, als ob Sie direkt am Rechner selbst sitzen würden. Auch YaST2 z. B. läßt sich so mit der graphischen Oberfläche starten. An einem Linux-Client müssen Sie dazu nur den Befehl `ssh -X -l admin <ip-adresse>` eingeben.

Zugriff auf die Administrationsweboberfläche Wenn Sie einen schnellen Zugriff auf die Weboberfläche für die Administration des Servers haben möchten, aktivieren Sie diese Schaltfläche. Sie können den Server dann aus dem Internet mit jedem beliebigen Webbrowser administrieren, indem Sie in der Adresszeile die URL `https://<extertne-ip-adresse-der-schule>:444/` eingeben. Wichtig ist hierbei die Angabe des richtigen Ports 444 am Ende der Adresse.

Zugriff auf die Mail/Groupwareoberfläche Wenn Sie Ihren Schülern auch während Ihrer Freizeit einen Zugriff auf die Mail- und Groupwareoberfläche Ihres Servers gestatten möchten, dann müssen Sie diese Schaltfläche aktivieren.

Achtung

Datenschutz

Bitte beachten Sie, dass Sie – wenn Sie auch die private Nutzung ausserhalb des Unterrichts genehmigen – dann Teledienstanbieter laut Teledienstedatenschutz- und Telekommunikationsgesetz sind und die entsprechenden Auflagen dieser Gesetze erfüllen müssen. Nähere Informationen hierzu finden Sie u.a. im Kapitel *Datenschutz* auf Seite 183.

Achtung

Jeder am Open School Server exisiterende Nutzer kann sich dann am Server anmelden und z. B. seine Emails lesen – wenn er die Internetadresse des Servers kennt. Sie erreichen die Mail- und Groupwareoberfläche in Ihrem Browser, indem Sie die URL `https://<extertne-ip-adresse-der-schule>/` eingeben.

Hinweis

Beachten Sie bitte, dass der Server hier jedem Nutzer aus dem Internet sein Angebot zur Verfügung stellt. Sollte ein Schüler ein zu schwaches Passwort für seinen Account verwenden, so kann es u.U. zu unschönen Nebenwirkungen kommen, wenn plötzlich bösartige Emails über diesen Account versendet werden …

Hinweis

SMTP Zugriff Verfügt Ihre Schule über eine feste, offizielle IP-Adresse, und soll der Open School Server die E–Mails aus dem Internet direkt empfangen, müssen Sie den SMTP–Port öffnen in der Firewal. In der Grundeinstellung wurde der Mailserver des Open School Servers so konfiguriert, dass dieser nur auf die IP–Adressen `mailserver` und `localhost` hört. Sie müssen nun Postfix so konfigurieren, dass dieser zusätzlich

auf die IP-Adresse des externen Interfaces lauscht. Das wird durch das setzen der Variable `inet_interfaces` in der Datei `/etc/postfix/main.cf`. Diese Variable können Sie mit Hilfe eines Texteditors oder auf der Administrationsweboberfläche setzten. (Siehe *Postfix für Experten* auf der nächsten Seite.)

6.2.5 Mail

Während der Installation des Open School Servers wurde das Mailsystem schon soweit konfiguriert, dass dieses in der Lage ist für Ihre Domaine(n) E–Mails empfangen und versenden kann.

Sämtliche E-Mails (versendete und empfangene) werden auf Viren und SPAM überprüft. Änderungen an diesen Einstellungen müssen Sie deshalb nur dann vornehmen, wenn Sie E-Mails per UUCP erhalten beziehungsweise versenden oder Sie einen so genannten Relay Host für das Versenden von E-Mail einrichten möchten.

Dabei müssen Sie folgende Tatsachen beachten:

- E–Mails können nur dann versendet werden, wenn der Open School Server mit einer offiziellen Domainnamen konfiguriert ist.
- Verfügen Sie über keine feste, ofizielle IP-Adresse (DSL– oder ISDN–Verbindung) ist es empfehlenswert das Versenden von E–Mails über einen „Mailrelay“ abzuwickeln. Nähres dazu finden Sie in den Abschnitten 6.2.5 bzw. 6.2.5.
- Sofern Sie für Ihre Schule eine feste, offizielle IP-Adresse benutzen und Ihr Open School Server für Ihre Domain „verantwortlich“ ist (d. h. es existiert ein „mx-record“ in Ihrem offiziellen Nameserver für Ihre Domain der auf Ihre fest IP-Adresse verweist), werden Ihre E–Mails direkt an Ihren Server geliefert. Dazu müssen Sie jedoch das SMTP–Port auf der Firewall des Open School Servers wie unter 6.2.4 beschrieben freischalten.
- Sofern E–Mail–Konten bei einem Provider abgerufen werden und die E–Mails an lokalen Benutzern gehen soll, müssen Sie je nach verwendeten Protokoll sog. „Fetchmailjobs“ einrichten bzw. das „UUCP“–System konfigurieren. Die Konfiguration fürs Abholen von E–Mails von externen Mailserver über IMAP oder POP3 Protokol können Sie mit dem YaST2 ‘Mail Server’–Modul erledigen. Melden Sie sich dazu als `admin` oder `root` an den Schulserver an und starten Sie YaST2. Das ‘Mail Server’–Modul finden Sie unter Netzwerkdienste.
  Die konfiguration von UUCP wird unter *E-Mail-Empfang über UUCP* auf Seite 99 erklärt.

Unter dem Punkt 'MAIL' kann das gesamte Mailsystem eingerichtet werden. Für den Betrieb des Open School Servers essentielle Daten können hier beeinflusst werden. Bitte ändern Sie Werte nur, wenn Sie sich über die Auswirkungen Ihres Handelns im Klaren sind.

Postfix – Postfix-Grundkonfiguration

Über das Postfix-Interface können Sie folgende Funktionen beeinflussen.

Name des Relayhosts Geben Sie hier das Mail Relay an, das Ihnen der Provider genannt hat. Die Angabe ist in der Regel nötig, wenn der Server nicht mit einer Standleitung an das Internet angebunden ist.

Dial-On-Demand Wenn Sie eine Einwählverbindung zu Ihrem Provider verwenden (z. B. ISDN), können Sie bestimmen, ob der Server bei Bedarf automatisch die Einwahl durchführen darf.

SMTP_AUTH Aktivieren Sie dieses Feld, wenn sich Benutzer über „sicheres SMTP" (authenticated SMTP) anmelden dürfen.

Postfix für Experten

In dieser Maske lassen sich nahezu alle Parameter von Postfix ändern, entfernen oder neu hinzufügen.

Achtung

Das Ändern von Werten in dieser Maske ohne detailliertes Wissen über die Konfiguration von Postfix kann Ihren Server unbrauchbar machen. Ändern Sie hier nur etwas, wenn Sie sich über die Auswirkungen im Klaren sind.

Achtung

IMAP Konfiguration

Hier können Sie einige grundlegende Einstellungen treffen, wie der Open School Server sich gegenüber Clients verhalten soll. Mit dem Feld 'Festlegen der Quota-Default-Größe' geben Sie den Wert vor, der bei der Erstellung eines neuen Benutzers als Quota vorgeschlagen wird. Sie können mit 'Nach Ablauf dieser Zeit werden inaktive IMAP Benutzer automatisch ausgeloggt' festsetzen, nach welcher Zeit sich ein Benutzer neu anmelden muss, wenn er keine Aktionen ausgeführt hat. Automatisches Ausloggen ist z. B. sinnvoll, wenn Benutzer vergessen, sich abzumelden bevor sie ihren Rechner verlassen. Auch für Zugriffe über POP kann das automatische Ausloggen mit dem Wert für 'Nach Ablauf dieser Zeit werden inaktive POP3 Benutzer automatisch ausgeloggt'

geregelt werden. Dadurch werden in erster Linie offene Verbindungen zum Server getrennt. POP-Clients authentifizieren sich in der Regel bei jedem Abruf von E-Mails neu.

Weiterhin können Sie einstellen, was passieren soll, wenn eine E-Mail an einen Benutzer ausgeliefert wird, dessen Quota Limit überschritten ist. Per Default wird diese E-Mail angenommen und es wird über einen Zeitraum von fünf Tagen — sofern der `postfix` Parameter `maximal_queue_lifetime` nicht geändert wurde — immer wieder versucht, die E-Mail auszuliefern. Danach wird die E-Mail verworfen und der Absender bekommt einen Warnhinweis per E-Mail. Wenn Sie den Schalter 'Mail wird sofort abgewiesen, wenn Quotalimit überstiegen ist'auf „Ja" setzen, wird die E-Mail sofort verworfen und dem Absender wird ein Warnhinweis zugestellt.

Außerdem können Sie einen lokalen Benutzer für nicht zustellbare E-Mail festlegen. Im Normalfall werden E-Mails an nicht existierende lokale Adressen abgewiesen und der Absender bekommt eine E-Mail mit einem entsprechenden Hinweis. Wenn Sie in das Feld einen existierenden, lokalen Benutzer eintragen, wird E-Mail an nicht existente Adressen an diesen Benutzer ausgeliefert. Der Absender bekommt dann keinen Hinweis.

Sollten Sie im Menü 'Hilfsmittel' → 'Globale Konfiguration'den Parameter für `drop_undeliverable_mail` auf `true` gesetzt haben,wird jede unzustellbare Email kommentarlos verworfen.

Hinweis

Sie können hier nur lokale Benutzer eintragen, wie z. B. `admin`, d. h. ohne die E-Mail-Domäne.

Hinweis

E-Mail-Empfang über UUCP

Voraussetzungen:

- Benutzername für uucp
- Passwort für uucp
- Adresse des E-Mail-Servers

Tipp

Wenn Sie einen normalen WinShuttle-Account beantragt haben, müssen Sie noch über die Telefon-Hotline von WinShuttle ein eigenes Passwort für UUCP aushandeln. Dieses ist nicht identisch zu einem normalen WinShuttle-Zugangspasswort. WinShuttle richtet dann den uucp-Zugang ein, der i.d.R. am nächsten Tag aktiv und nutzbar ist. Die Adresse des E-Mail-Servers bei WinShuttle-Accounts lautet i.A. mail.KFZ.shuttle.de.

Tipp

Wir haben soweit möglich bereits alle Vorarbeiten für die Konfiguration abgeschlossen. Die nötigen RPM-Pakete sind installiert und auch an der Konfiguration von Postfix braucht nichts geändert zu werden.

Sie müssen lediglich noch vier Konfigurationsdateien anpassen und den Mailaustausch automatisieren.

Konfigurationsdateien anpassen Es müssen folgende Dateien mit den entsprechenden Inhalten im Verzeichnis `/etc/uucp` angelegt werden:

```
shuttle         <winshuttle-benutzername>  <passwort>
```

Datei 2: *Inhalt der Datei call*

```
nodename    <winshuttle-benutzername>
```

Datei 3: *Inhalt der Datei config*

```
port    TCP
type    tcp
```

Datei 4: *Inhalt der Datei port*

```
system          shuttle
call-login      *
call-password   *
time            any
address         <winshuttle-emailserver>
commands        rmail #rnews
port            TCP
```

Datei 5: *Inhalt der Datei sys*

Rechtevergabe Alle Dateien sollten mit dem Befehl:

```
chown uucp:root /etc/uucp/*
```

dem Benutzer uucp zugeordnet werden. Zusätzlich müssen Sie noch

```
chmod o-r /etc/uucp/*
```

eingeben, um allen anderen Nutzern die Leserechte zu entziehen.

E-Mail-Empfang testen Jetzt sollte der E-Mail-Empfang über WinShuttle mit dem Befehl:

```
uucico -S shuttle
```

aktiviert werden können. Liegen E-Mails für auf dem System existierende Nutzer vor, werden diese abgeholt und zugestellt.

Die Protokolldateien liegen nach dem ersten Mailaustausch unter `/var/log/uucp`.

`Stats` für die „Statistiker" mit allg. Informationen zu den übertragenen Datenmengen und das im Fehlerfall wesentlich interessantere `Log` mit Informationen zur (erfolgreichen) Anmeldung und zum Mailaustausch.

E-Mail-Austausch automatisieren Aktivieren Sie dazu in der Datei `/etc/crontab` folgende Zeile:

```
#30 * * * * root /usr/sbin/uucico -S shuttle
```

indem Sie die Raute (#) am Anfang entfernen. Damit wird dann alle halbe Stunde der E-Mailaustausch aktiviert.

E-Mail-Versand über UUCP

Um auch Emails über UUCP versenden zu können, müssen Sie noch Postfix auf die neue Versandart umstellen - da Postfix normalerweise die Emails über SMTP versendet.

Nachdem Sie die entsprechenden Dateien für die UUCP-Verbindung wie unter *E-Mail-Empfang über UUCP* auf Seite 99 beschrieben angelegt haben, wechseln Sie bitte ins Webfrontend unter `https://admin` und melden sich dort als `admin` an. Wechseln Sie nun ins Menü 'Mail' und geben Sie dort im Untermenü 'Postfix' als 'Relayhost' den Wert 'shuttle' ein. Anschließend speichern Sie bitte. Im Menü 'Postfix für Experten' klicken Sie auf den Button 'Parameter hinzufügen', wählen den Parameter 'default_transport' aus und geben als Wert `uucp` ein. Auch hier bitte wieder am Ende der Änderungen 'speichern' nicht vergessen.

6.2.6 Hilfsmittel: Zusätzliche Funktionen

LDAP Browser: Editieren der LDAP-Datenbank

Der Open School Server verwendet intern den Verzeichnisdienst LDAP für die Gruppen- und Benutzerverwaltung (auch unter Samba), Adressverwaltung, Mailrouting, DNS und DHCP.

Möchten Sie über die Konfigurationsmasken dieser Dienste hinaus Änderungen an den Einstellungen vornehmen, können Sie dazu den LDAP-Browser benutzen. Er erlaubt das Ändern, Löschen und Hinzufügen von Attributwerten zu bestehenden Einträgen.

Achtung

Führen Sie hier nur Änderungen durch, wenn Sie sicher wissen, was Sie tun. Sie können hier durch Änderungen den Open School Server unbrauchbar machen.

Achtung

Ein LDAP-Verzeichnis hat baumartige Struktur. Alle Einträge (Objekte genannt) im Verzeichnis haben eine definierte Position innerhalb dieser Hierarchie. Diese Hierarchie wird als *Directory Information Tree* oder kurz DIT bezeichnet.

Der komplette Pfad zum gewünschten Eintrag, der ihn eindeutig identifiziert, wird *Distinguished Name* oder DN genannt.

Die einzelnen Knoten auf dem Weg zu diesem Eintrag werden *Relative Distinguished Name* oder RDN genannt. Objekte können generell zwei verschiedenen Typen zugeordnet werden:

Container Diese Objekte können wiederum andere Objekte enthalten. Solche Objektklassen sind `Root` (Wurzelelement des Verzeichnisbaums, das nicht real existiert), `c` (engl. *country*), `ou` (engl. *OrganizationalUnit*), und `dc` (engl. *domainComponent*).

Vergleichbar ist dieses Modell auch mit Verzeichnissen (Ordnern) im Dateisystem.

Blatt Diese Objekte sitzen am Ende eines Astes. Ihnen sind keine anderen Objekte untergeordnet. Beispiele sind `Person/InetOrgPerson` oder `groupofNames`.

Vergleichbar ist dies mit Dateien im Dateisystem.

Wenn Sie sich ein wenig genauer mit `LDAP` auseinandersetzen möchten, empfehlen wir Ihnen einen Blick ins SUSE LINUX Enterprise Server Handbuch (Kapitel 21.8 ‘LDAP – Ein Verzeichnissdienst’ auf den Seiten 521–523).

Mail an Alle: Nachricht vom Administrator

Es kann vorkommen, dass der Administrator (`admin`) allen angelegten Benutzern eine E–Mail zukommen lassen will.

Beispielsweise wenn der Open School Server wegen Wartungsarbeiten abgeschaltet werden soll.

Geben Sie den Betreff und den Nachrichtentext ein (siehe Abb. 6.17 auf der nächsten Seite). Die E–Mail erreicht jeden vorhandenen Benutzer ohne Rücksicht auf dessen Quota.

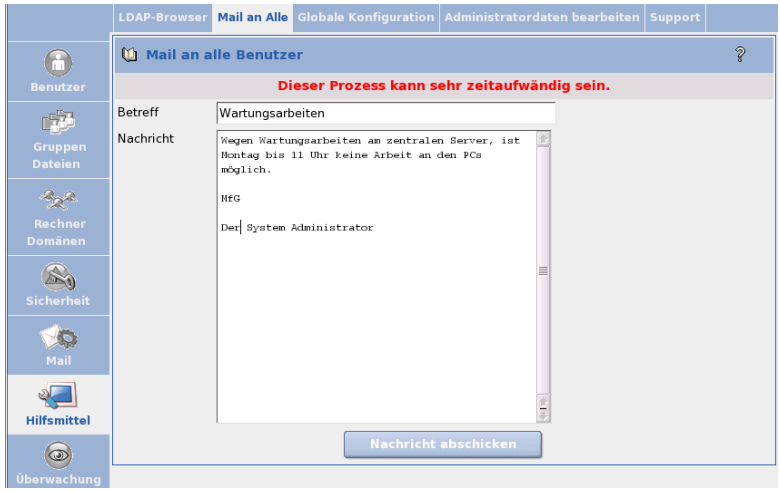

Abbildung 6.17: *Eine Mail vom Administrator*

Globale Konfiguration

Diese Einstellungen beeinflussen die webbasierte Konfiguration und einige Komponenten Ihres Servers. Die Konfigurationsdatei finden Sie auf dem Server unter `/etc/imap/globals.conf`.

GENERAL

ImportFileFormat Wählen Sie hier das Format für die Importlisten von neuen Nutzern aus. Genauere Informationen finden Sie im Abschnitt *Schülerdaten exportieren und importieren* auf Seite 191.

EnableUserSpamFrontend Hier kann das SPAM-Filter-Frontend unter den Filter-Einstellungen für Benutzer an- oder abgeschaltet werden.

EnableSieveEditor Aktivieren/Deaktivieren des SIEVE Filter Editor in den Benutzer-Filtereinstellungen.

MonitorResolveAddr Sollen IP Adressen zu Hostnamen im Online Monitor aufgelöst werden?

NewUserChangePassword Aktivieren Sie diese Funktion, muss der Benutzer standardmäßig nach dem ersten Login, das vom Administrator vergebene Passwort ändern.

UserJpegPhotoMaxHeight Geben Sie die maximale Höhe von Benutzerfotos an. Die Seitenverhältnisse bleiben beim Skalieren erhalten.

UserJpegPhotoMaxWidth Geben Sie die maximale Breite von Benutzerfotos an. Die Seitenverhältnisse bleiben beim Skalieren erhalten.

MonitorServices Geben Sie hier diejenigen Dienste an, welche Ihnen im Menü 'Überwachung' → 'Dienstüberwachung' angezeigt werden sollen. Prinzipiell können Sie hier jeden Dienst eintragen, welcher über eine „rc"-Startdatei verfügt.

SESSIOND

SessionTimeout Hier können Sie den Timeout einstellen, nach dem ein im Webfrontend angemeldeter Benutzer automatisch ausgeloggt wird.

SessionHost; SessionPort; SSL_key_file; SSL_cert_file und SSL_ca_file Diese Optionen werden derzeit noch nicht benötigt. Sie sind für eine eventuelle Auslagerung des administrativen Webfrontends auf einen anderen Rechner vorgesehen.

SECURITY

UseCookie Die Optionen 'UseCookie' und 'CheckClientIP' verhindern, dass die eigene Sitzung „gestohlen" werden kann, indem der Angreifer auf irgendeine Weise an die Sitzungs-ID des jeweiligen Benutzers kommt. 'UseCookie' ist die sicherste der beiden Möglichkeiten. Sie speichert eine weitere ID in einem Cookie im Browser des jeweiligen Benutzers.

CheckClientIP Mittels 'CheckClientIP' wird überprüft, ob die Zugriffe auf das Webfrontend pro Benutzer von einem einzigen Rechner kommt. Somit kann verhindert werden, dass eine Sitzung „gestohlen" wird. Da man IP-Adressen fälschen kann und ein Benutzer evtl. hinter einem Proxy-Cluster sitzt, der wechselnde IP-Adressen benutzt, ist diese Option nicht so geeignet wie die o. g. Methode mittels Cookies.

DefaultPasswordHash Hier können Sie einstellen, mit welcher Methode Benutzerpasswörter standardmäßig verschlüsselt werden sollen.

Administratordaten bearbeiten

In diesem Menüpunkt können Sie die Daten und das Passwort des Hauptadministrators `admin` setzen.

Um das Passwort zu ändern klicken Sie auf 'Passwort setzen'. Sie werden nun zu einer weitern Oberfläche weitergeleitet. Geben Sie das alte Passwort ein und zweimal das neue.

Hinweis

Merken Sie sich das Passwort gut. Ohne Passwort haben Sie keine Administrationsmöglichkeit.

Hier wird nur das Passwort des Benutzers `admin` in der LDAP geändert. Die Passwörter von Benutzern die lokal auf dem System gespeichert sind bleiben davon unberührt. Die wichtigsten davon sind:

- `root`
- `cyrus` IMAP–Administrator passwort.
- Passwort des RootDN–s für LDAP.

Hinweis

Support

Unter diesem Menüpunkt können Sie Supportfragen an die Entwickler des Open School Servers oder an Ihre persönliche Supportstelle richten.

Neben der Beschreibung Ihres Problems können Sie die Konfiguration Ihres Systems und die LDAP–Datenbank mitsenden.

Hinweis

Beachten Sie, dass die LDAP–Datenbank die (verschlüsselten) Passwörter und persönliche Daten Ihrer Benutzer enthält.

Hinweis

6.2.7 Überwachung des Systems

Wer ist online?

Hier erhalten Sie eine Übersicht über die Benutzer, die momentan auf der Administrationsoberfläche angemeldet sind.

Durch einen Klick auf die Benutzer–ID löschen Sie die jeweilige Sitzung des Benutzers. Ihre eigene Sitzung kann nicht gelöscht werden.

Mail–Warteschlange

In dieser Maske sehen Sie die von Postfix zur Zeit bearbeiteten E-Mails. Geben Sie die Aktualisierungsrate in Sekunden ein (z. B. 5 Sekunden) und drücken Sie die Eingabetaste. Die Maske wird dann in diesem Zeitintervall aktualisiert. Um den Refresh abzuschalten, wählen Sie den Menüpunkt 'Mail Queue' erneut an.

In der Regel sollten Sie hier dauerhaft keine E–Mails sehen. Sollte das Postfixsystem jedoch gestoppt werden oder aus irgendwelchen Gründen keine E–Mails zustellen können, erscheinen hier allerdings die noch zuzustellenden E–Mails.

Über den Button 'Queue leeren' veranlassen Sie Postfix, die Bearbeitung der aufgelaufenen E–Mails sofort vorzunehmen. Sie können aufgelaufene E–Mails hier auch entfernen. Klicken Sie dazu auf den QueueID der jeweiligen E–Mail.

Achtung

Die E–Mail geht unwiederbringlich verloren!

Achtung

Mailstatistik

Unter 'Mailstatistik' können Sie sich für einen bestimmten Zeitraum (zwischen den letzten 24 Stunden und dem letzten Jahr) das Mail-Aufkommen in einem Graphen darstellen lassen. In weiteren Graphen sehen Sie die Fehler-Statistik und die Datenmenge dargestellt.

Systemstatistik

Hier erhalten Sie eine Übersicht über die Auslastung Ihres Open School Servers.

Wenn Sie Änderungen an Ihrer Hardware vorgenommen haben, wenn Sie z. B. eine neue Festplatte einbauen, müssen Sie den Systemmonitor neu initialisieren. Rufen Sie dazu die folgenden Kommandos hintereinander auf:

```
/usr/lib/sysMonitor/clearall CLEAR_GRAPHS
/usr/lib/sysMonitor/clearall CLEAR_DATABASES
/usr/lib/sysMonitor/SETUP.pl
/usr/lib/sysMonitor/rrdtimer gv
```

Dienstüberwachung

Dieser Menüpunkt zeigt Ihneneine Übersicht wichtiger Systemdienste und deren aktuelle Zustände (vgl. Abbildung 6.18 auf der nächsten Seite) an.

Welche Eintäge der Open School Server hier anzeigt, legen Sie über den Parameter `MonitorServices` in der Datei `/etc/imap/globals.conf` oder im Administrationsfrontend fest.

Ein Dienst kann aktiviert oder deaktiviert sein. Ist ein Dienst aktiviert, wird er beim Hochfahren des Systems automatisch gestartet.

Weiterhin können Sie einen Dienst starten, stoppen, neu laden und neu starten. Wenn Sie einen Dienst neu starten, wird dieser zunächst gestoppt und danach wieder gestartet. Wenn Sie einen Dienst neu laden, wird dieser nicht beendet, sondern lädt in der

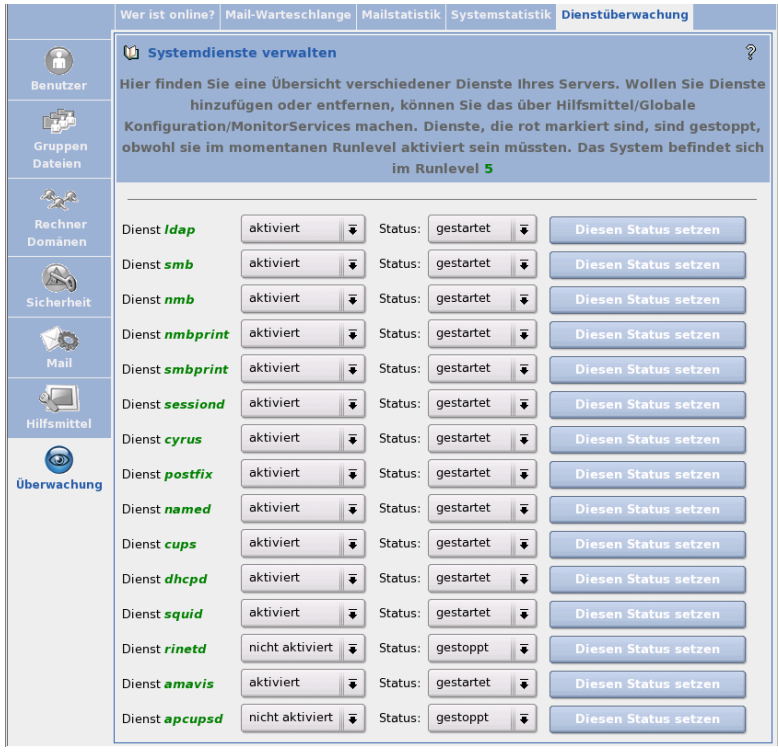

Abbildung 6.18: *Überwachung der Systemdienste*

Regel seine Konfiguration neu oder macht einige Initialisierungen. Nicht alle Dienste unterstützen diese Funktion. Nachdem Sie den Status eines Dienstes geändert haben, klicken Sie auf 'Diesen Status setzen'.

6.3 Administration als Benutzer

Öffnen Sie in einem Browser auf einem Ihrer Clientrechner die URL:

`https://admin.<schule.de>`

Nach der Anmeldung mit Ihrem Benutzernamen erreichen Sie einen Konfigurationsbereich, wo es Ihnen je nach Gruppenzugehörigkeit und durch den Hautpadministrator

Abbildung 6.19: *Administrationsoberfläche für Schüler*

erteilten Rechten verschiedene Administrationsmöglichkeiten zur Verfügung stehen. Die einzelnen Menüpunkte werden in den folgenden Abschnitten erläutert.

Meldet sich ein Schüler an die Administrationsoberfläche des Open School Servers an, kann er

- sein Passwort ändern,
- seine Mailboxen verwalten,
- seinen Mailfilter einstellen bzw. Urlaubsbenachrichtigung erstellen
- und Dateien aus seine Verzeichnissen runterladen.

Meldet sich ein Lehrer an die Administrationsoberfläche des Open School Servers an, sieht er sofort den aktuellen Zugangstatus des Schulraumes in dem er sich befindet. Weiterhin kann er

- sein persönliche Daten ändern,
- seine Schüler verwalten,
- Projektgruppen anlegen bzw. verwalten,
- Dateien verteilen bzw. einsammeln,
- seine Mailboxen verwalten,
- seinen Mailfilter einstellen bzw. Urlaubsbenachrichtigung erstellen

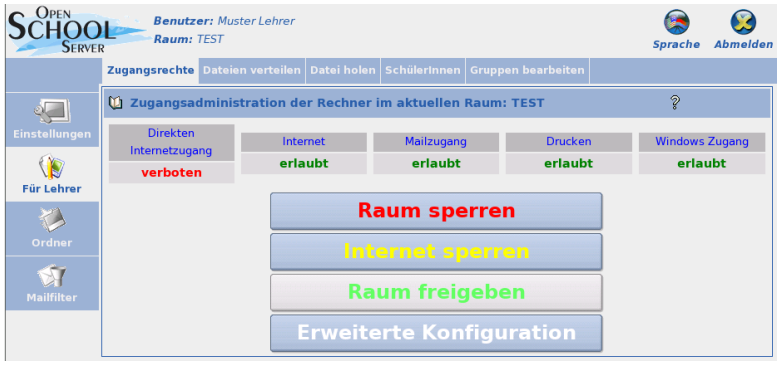

Abbildung 6.20: *Administrationsoberfläche für Lehrer*

- und Dateien aus seine Verzeichnissen runterladen.

Meldet sich ein Lehrer mit zus. Administrationsrechten an die Administrationsoberfläche des Open School Servers an, kann er zusätzlich

- Benutzer anlgen, importieren und ändern,
- Gruppen anlegen und bearbeiten,
- Rechner verwalten,
- den Systemstatus erfragen,
- und den Zugangstatus sämtlicher Schulräumen verwalten.

6.3.1 Einstellungen

Dieses Menü bietet Ihnen die Möglichkeit, Ihre persönlichen Daten (z. B. Adresse und Telefonnummer) und das Passwort zu ändern, sowie einen Überblick der Drucker bzw. Druckjobs zu bekommen.

Eingeben und Ändern der persönlichen Daten

Hier können Sie, je nach Schreibberechtigung, die vom Administrator eingetragenen persönlichen Daten ändern. Falls Sie für ein oder mehrere Felder kein Schreibrecht haben, werden für die betreffenden Felder lediglich die gerade aktuellen Werte angezeigt. Mit dem Button 'Speichern' werden die vorgenommenen Änderungen gespeichert.

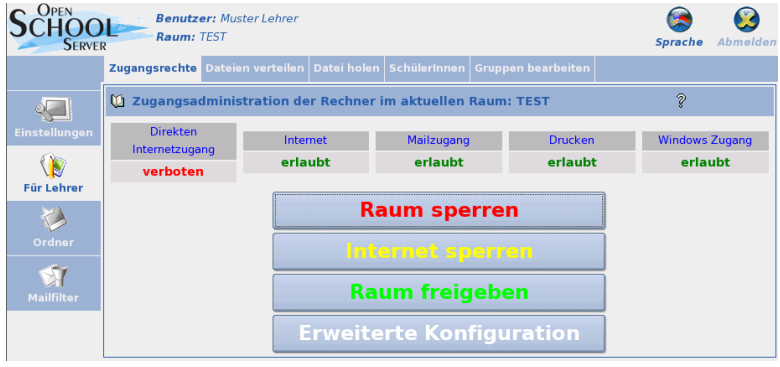

Abbildung 6.21: *Administrationsoberfläche für Lehrer mit zus. Administrationsrechten*

Hinweis

Schüler dürfen normalerweise ihre persönliche Daten nicht ändern. Lediglich auf ihr Passwort haben sie Zugriff. Dies kann aber durch den Administrator geändert werden.

Hinweis

Ändern des Passwortes

Aus Sicherheitsgründen sollten Sie von Zeit zu Zeit Ihr Passwort ändern. Dazu müssen Sie zunächst Ihr altes Passwort und dann zweimal das neue Passwort in die dafür vorgesehenen Felder eingeben. Sie können außerdem wählen, wie das neue Passwort gesichert werden soll. Folgende Methoden sind möglich:

CRYPT: Beim CRYPT-Mechanismus ist das Passwort auf eine maximale Länge von acht Zeichen begrenzt. Dieser Mechanismus ist der Standard für die meisten Unix-Systeme. Längere Passwörter werden einfach nach der 8ten Stelle abgeschnitten.

SMD5: Der SMD5-Mechanismus ermöglicht wesentlich längere Passwörter als der CRYPT-Algorithmus (bis zu 255 Zeichen). Des Weiteren wird die bei diesem Verfahren eingesetzte „Verschlüsselung“ unter Sicherheitsexperten höher eingeschätzt als das bei der `CRYPT`-Methode verwendete Verfahren.

Standardmäßig wird das Verfahren ausgewählt, mit dem bereits das alte Passwort gespeichert wurde.

Haben Sie Ihr Passwort vergessen, können Sie sich an den Administrator wenden. Der Administrator kann jederzeit ein neues Passwort vergeben ohne das alte kennen zu müssen.

Schüler können sich auch an jene Lehrkräfte wenden, welche vom Administrator mit Administrationsrechten ausgestattet wurden (siehe Abschnitt *Administration durch Lehrer* auf Seite 123).

6.3.2 Für Lehrer

Zugangsrechte setzen

Wie der Hauptadministrator `admin` haben die Lehrkräfte auch die Möglichkeit, den Rechnern eines Schulraumes bestimmte Dienste (Internetzugang, Zugang zu den Mail- bzw. Groupwareserver, Zugang zu den Printserver) zu sperren, bzw. zu erlauben (direkter Internetzugang) (siehe 6.2.4 auf Seite 94). Die Lehrkräfte können jedoch den Zugang nur in dem Schulraum kontrollieren, in dem sie sich gerade befinden.

Hinweis

Die Möglichkeit, den Zugang von Rechnern zu den Diensten des Open School Servers und ins Internet zu kontrollieren, ist nur dann gegeben, wenn die Clientrechner registriert sind.

Hinweis

Zunächst bekommt der Lehrer hier einen Übersicht über den aktuellen Zugangstatus des Raumes (siehe *Zugangsrechte setzen* auf der nächsten Seite, und eine einfache Möglichkeit dieses zu ändern:

- den Raum einfach total zu sperren;
- den Internetzugan in dem Raum zu sperren;
- oder den Raum wieder frei zu geben.

Die Sperrungen betreffen den Rechner, an dem die Aktion durchgeführt wird, nicht.

Durch Drücken 'Erweiterte Konfiguration' gelangen Sie zu einer erweiterten Oberfläche. Hier können Sie den Zugangstatus differenzierter einstellen, bzw. nur bestimmte Webseiten für den Raum erreichbar machen.

Um den Rechner, an welchem die Aktion durchgeführt wird, nicht aussperren zu lassen, muss die Checkbox 'Den eigenen Rechner nicht aussperren' angewählt sein (Standardeinstellung).

Abbildung 6.22: *Zugangskontrolle für LehrerInnen*

Direkten Internetzugang erlauben/ verbieten Hier wird für die Rechner des betreffenden Schulraumes Masquerading aktiviert. Dies wird benötigt, wenn Sie z. B. mittels `ftp` direkt Daten mit Servern aus dem Internet austauschen möchten. Wenn Sie also z. B. die Schulhomepage von einem Provider hosten lassen und sie mittels `ftp` aktualisieren möchten, müssen Sie vorher erst das Masquerading aktivieren.

Da der Open School Server den Clients zusammen mit ihrer IP-Adresse noch einige andere Daten über `DHCP` übermittelt, brauchen Sie an den Clients im allgemeinen keine weiteren Einstellungen vornehmen.

Bei FTP-Programmen müssen Sie allerdings den „passiven“ Übertragungsmodus einschalten, da die Clients ansonsten bei „aktivem“ FTP eine Anfrage an den betreffenden FTP-Server stellen und ihn bitten, sie auf einem für die Datenübertragung freien Port „zurückzurufen“. Der FTP-Server sucht sich dann einen bei ihm freien Port aus und versucht über diesen eine Verbindung herzustellen.
Da der Open School Server aber nicht wissen kann, an wen er die betreffende Anfrage von außen weiterleiten soll, lehnt er die Verbindungsaufnahme des FTP-Servers ab. Bei der Verwendung von „passiven“ FTP versuchen die Clients so lange eine Daten–Verbindung zum FTP-Server aufzubauen, bis sie auf einen freien Port am Server treffen. Dies dauert zwar Bruchteile von Sekunden länger – aber dafür gehen die Verbindungen von den Clients aus und der Open School Server kann die entsprechenden Antworten eindeutig zuordnen.

Achtung

Beachten Sie bitte, dass die Clients bei eingeschaltetem Masquerading eine „direkte“ Verbindung zum Internet haben. Die Schutzfunktionen des Open School Servers (wie z. B. der Internetfilter) sind dann nicht mehr wirksam!

Achtung

Internet erlauben/ verbieten Hier können Sie den Zugang für zum Proxyserver freischalten bzw. sperren. Die Sperre bzw. Freigabe des Internets erfolgt dabei raumbezogen, wenn die Clients am Open School Server angemeldet sind. Wenn also ein Lehrer im Computerraum 1 seinen Schülern den Internetzugang freigibt, hat das keine Auswirkungen auf die Rechner in den anderen Räumen.

Beachten Sie bitte, dass die Schüler im allgemeinen nur an der langen Wartezeit und der anschließenden Fehlermeldung im Browser (Seite kann nicht erreicht werden) erkennen können, dass der Internetzugang gesperrt ist – eine besondere Information wird hier nicht an die Clients übertragen.

Mailzugang erlauben/ verbieten Hier können Sie den Zugang zur Groupwareseite unter `https://SchoolServer` bzw. zu den Mailserver gestatten oder verweigern.

Drucken erlauben/ verbieten Wenn die Drucker der Schule über den Printserver des Open School Servers verwaltet werden, können Sie hier den Zugriff auf sämtliche vorhandenen Drucker für den betreffenden Klassenraum sperren. Damit können Sie z. B. ungewollte Ausdrucke verhindern.

Konfiguration des Proxyservers Hier können Sie den Internetzugang für die Clients „feintunen“. Entweder erlauben Sie hier `Alles außer der negativen Liste` des Proxyservers oder Sie erstellen selbst eine sog. „Positive Liste“.

Wenn Sie Ihren Schülern während des Unterrichts nur den Zugriff auf ganz bestimmte Domains erlauben wollen, oder Sie denn Zugang zu Internetseiten, die normaler Weise gesperrt sind, ermöglichen möchten, dann tragen Sie die entsprechenden URLs in das entsprechende Formular ein (siehe Abbildung 6.22 auf der vorherigen Seite und aktivieren die Schaltfläche `Nur positive Liste erlauben`.

Wenn Sie also z. B. nur die Domain `www.extis.de` erlauben möchten, dann tragen Sie sie hier ein, aktivieren die Schaltfläche `Nur positive Liste erlauben` und klicken auf `Zugangsrechte setzen`.

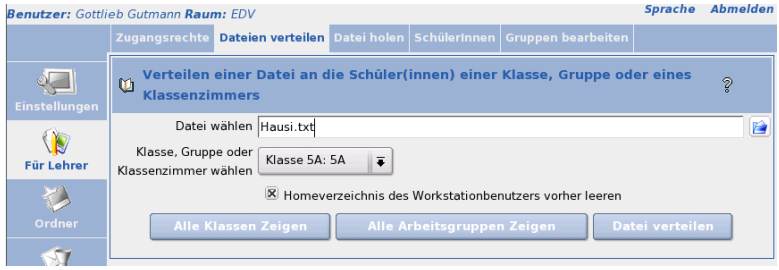

Abbildung 6.23: *Datei verteilen*

Dateien verteilen und Dateien einsammeln

Die Lehrkräfte können mit Hilfe des Open School Servers Dateien an die Schüler einer Klasse verteilen. Dazu müssen Sie zuerst den Menüpunkt 'Für Lehrer' → 'Datei verteilen' (siehe Abb. 6.23) und die gewünschte Datei und Klasse auswählen. Die Datei wird in die persönlichen Importverzeichnisse der Schüler einer Klasse oder der Workstationbenutzer gelegt.

Mit dem Menüpunkt 'Für Lehrer' → 'Datei holen' (siehe 6.24 auf der nächsten Seite) wird der Inhalt der Exportverzeichnisse der Schüler einer Klasse ins Importverzeichnis der Lehrkraft gelegt.

Dabei kann die Lehrkraft durch das de-/aktivieren der Checkbox 'Dateien in Unterverzeichnisse sortieren' entscheiden, wie die Dateien im Importverzeichnis eingeordnet werden sollen:

- Bei aktivierter Checkbox werden (bei Bedarf) für jeden Schüler eigene Verzeichnisse angelegt: `\~<Lehrerlogin>/Import/<Schüler~loginname>/<Dateien>`.
- Wird die Checkbox deaktiviert, wird jeder Datei der entsprechende Loginname des betreffenden Schülers vorangestellt - diese aber nicht in extra Verzeichnisse eingeordnet: `\~<Lehrerlogin>/Import/<Schüler~loginname>-<Datei(en)>`.

Workstationbenutzer - Klausurumgebung Sind die Clientrechner raumweise registriert, besteht die Möglichkeit, Klassenarbeiten in einer geschützten Umgebung durchzuführen. Dazu müssen Sie wie folg vorgehen:

1. Im Menü 'Für Lehrer' → 'Datei verteilen' statt einer Klasse der aktuelle Arbeitsraum ausgewählt werden. Durch Aktivieren der Checkbox 'Homeverzeichnis

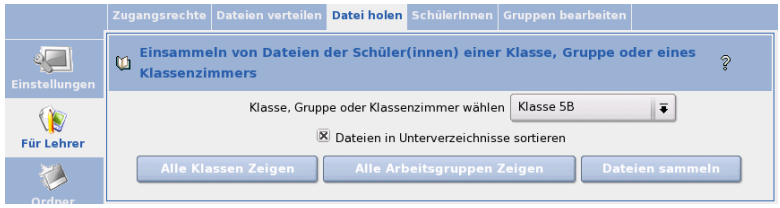

Abbildung 6.24: *Dateien einsammeln*

des Workstationbenutzers vorher leeren' kann man vor dem Verteilen der Datei die Homeverzeichnisse der Workstationbenutzer auf Standardeinstellung bringen.

2. Die Schüler sollten sich nun nicht mit ihrem eigenem Benutzeraccount, sondern mit dem des Arbeitsplatzrechners anmelden. Die Zugangsdaten sind hier:
   - Benutzername = Name der Workstation
   - Passwort = Name der Workstation
3. Nachdem sich alle Schüler angemeldet haben sperren Sie den Raum alle Dienste wir unter *Zugangsrechte setzen* auf Seite 111 beschieben ist.
4. Nach der Anmeldung sollten die Schüler die zuvor ausgeteilten Dateien im Homeverzeichnis im Unterordner `Import` finden. Am Ende der Stunde brauchen die Schüler die bearbeiteten Dateien nur im Verzeichnis `Export` zu speichern, damit Sie anschließend von der Lehrkraft wieder „eingesammelt" werden können.

SchülerInnen

Im Menü 'SchülerInnen' können die Schüler verwalten. Ihnen stehen bisauf 'Löschen' alle Funktionen die dem Hauptadministrator zur Verfügung. Eine genau Beschreibung der Funktionen finden Sie unter *Bearbeiten – Verändern der Benutzerdaten* auf Seite 66.

Hinweis

Lehrer ohne zusätzlichen administrativen Rechten können nur „seiner" Schüler ändern, d.h. derjenigen Schüler, welche sich in seinen Klassen befinden.

Hinweis

Gruppen anlegen/ bearbeiten

Uneter dieser Menüpunkt bekommen Sie in erster Linie eine Liste der Arbeitsgruppen, die Sie selber angelegt haben oder in denen Sie administrative Zugriffsrechte haben. Beim Erstellen einer Arbeitsgruppe (Projektgruppe), wird für diese eine eigene Tauschverzeichnis eigene Email-Adresse `<Grupenname>\@<Domainname>` angelegt. Das Tauschverzeichnis der Gruppe ist `/home/groups/<Gruppenname>` bzw. unter Windows `G:\<ruppenname>` – dort haben alle Mitglieder volle Zugriffsrechte. Weiterhin können Sie für die angelegten Arbeitsgruppen in der Groupware des Open School Server u.v.a Termine erstellen, Projekte anlegen.

Sie können zunächst auch Arbeitsgruppen ohne Mitglieder erstellen und erst später Schüler und/oder Lehrer hinzufügen. Wenn Sie beim Anlegen der Gruppe die Checkbox Gruppe darf nur vom Anleger geändert werden aktiviert haben, kann diese Gruppe nur von Ihnen verwalten werden, und erscheint bei keinem anderem Lehrer in der Liste der Arbeitsgruppen.

Hinweis

Beachten Sie bitte, dass der Arbeitsgruppenname keine Leer– und Sonderzeichen enthalten darf! Sie sollten jedoch immer eine ausführliche Beschreibung der Arbeitsgruppen zuordnen. In der Suchlisten erscheint nämlich nicht der Name sondern die Beschreibung der Arbeitsgruppen, wenn diese vorhanden ist.

Hinweis

Alle Arbeitsgruppen erhalten an den Arbeitsgruppennamen addressierte Emails automatisch in einen Gemainsamen Mailordner. Die Lehrer der Arbeitsgruppe können diese E–Mails lesen und löschen, bzw. können weitere Unterordner ablegen. Schüler haben jedoch nur Leserechte hier.

6.3.3 Ordner

Der Open School Server legt E-Mails in Ordnern ab. Unter dem Menüpunkt 'Ordner' können Sie Ordner anlegen, umbenennen und löschen sowie die Zugriffsrechte von anderen Benutzern auf Ihre Ordner verwalten. Das ist eine der Stärken des IMAP-Protokolls. Mit POP ist keine Verwendung von Ordnern möglich.

Weiterhin bekommt man hier, unter dem Menüpunkt 'Dateisystem' über das gesammte, für den jeweiligen Benutuer zur Verfügung stehendes, Filesystem des Open School Server Zugriff. Es ist also möglich per Webbrowser Dateien hoch– und runterzuladen, bzw. die Zugriffsrechte der Dateien zu ändern.

Beim Open School Server sind die Ordner hierarchisch strukturiert. An der Spitze dieser Hierarchie befindet sich der Ordner `INBOX`. Alle weiteren Ordner sind unterhalb

von INBOX angelegt. Standardmäßig existieren z. B. für jeden Benutzer folgende Ordner:

INBOX: Wenn keine Mailfilter definiert sind, werden alle eingehenden Nachrichten hier abgelegt.

Gesendet: Alle E-Mails, die Sie verschicken, werden hier abgelegt.

Spam: Dieser Ordner wird genutzt, wenn auf Ihrem System der Filter für ungewollte Werbemail (auch SPAM oder Unsolicted Commercial Email) aktiv ist. Hier können Sie automatisch alle vom System als SPAM erkannte E-Mails ablegen lassen (für Details zum SPAM-Filter siehe auch Abschnitt 6.3.5 auf Seite 121).

Papierkorb: Standardmäßig ist das Webmail-Programm so konfiguriert, dass E-Mails, die Sie löschen, zunächst als Sicherheitskopie in diesem Ordner abgelegt werden.

Diese Ordner werden vom System benötigt und sollten nicht gelöscht werden. Das Löschen der kompletten INBOX ist nicht möglich.

Neu: Anlegen eines neuen Ordners

Im Untermenü 'Neu' haben Sie die Möglichkeit, neue Ordner anzulegen. Auf der linken Seite wird eine Liste aller Ordner angezeigt, in welchen Sie E-Mails ablegen können. Wenn Sie einen neuen Ordner hinzufügen wollen, wählen Sie zunächst per Mausklick einen bestehenden Ordner aus, unterhalb dessen der neue Ordner erscheinen soll. Wenn Sie den neuen Ordner auf die oberste Ebene (dort wo INBOX, Spam, Gesendet und Papierkorb liegen) anlegen möchten, wählen Sie INBOX aus. Geben Sie dann den gewünschten Namen des neuen Ordners an.

Durch Betätigen des Buttons 'Neu' wird der Ordner angelegt. Der Name des neuen Ordners ist z. B. Gesendet/Mutti. Sie können auch in diesem Ordner einen Unterordner anlegen, z. B. noch_ein_ordner. Der Ordnername lautet dann Gesendet/Mutti/noch_ein_ordner.

6.3.4 Bearbeiten: Ordnereigenschaften und Rechte

Im Untermenü 'Bearbeiten' können Sie bestehende Ordner umbenennen und löschen, sowie die Zugriffsrechte anderer Benutzer auf diese Ordner bearbeiten. Zum Löschen eines Ordner wählen Sie einfach den entsprechenden Ordner in der Liste auf der linken Seite an und klicken mit der Maus auf dem Button 'Löschen'.

Achtung

Beim Löschen eines Ordners gehen alle darin enthaltenen E-Mails verloren. Ebenso werden alle zugehörigen Unterordner mit deren Inhalt entfernt!

Achtung

Wenn Sie den Namen eines bestehenden Ordners ändern möchten, wählen Sie den entsprechenden Ordner ebenfalls aus der Liste aus. Dann geben Sie den neuen Namen in dem Feld neben 'Umbenennen' ein und klicken Sie auf den Button.

6.3.5 Mailfilter

Mit dem SIEVE-basierten Mailfiltersystem des Open School Server können Sie die Verarbeitung von eingehenden E-Mails automatisieren. Eine detaillierte Beschreibung von SIEVE finden Sie in RFC 3028:

`http://www.ietf.org/rfc/rfc3028.txt`

Mailfilter

Über 'Mailfilter' können Sie Bedingungen festlegen, anhand derer der Open School Server eingehende E-Mails behandelt. So können Sie z. B. E-Mails automatisch in bestimmte Ordner einsortierten lassen oder an eine andere E-Mailadresse weiterleiten.

Wenn Sie den Menüpunkt 'Mailfilter' ausgewählt haben, sehen Sie zunächst eine Übersicht über alle augenblicklich konfigurierten Mailfilter. Diese ist zunächst leer.

Filterregeln erstellen

Um eine neue Filterregel zu erstellen klicken Sie auf den Button 'Filterregel einfügen' Das Erstellen einer Filterregel teilt sich in mehrere Schritte auf. Der erste Schritt ist das Festlegen der Filterbedingungen. Folgende Eigenschaften einer E-Mail können überprüft werden:

Größe: Es kann getestet werden, ob die E-Mail größer oder kleiner als ein bestimmter Wert ist.

Kopfzeilen/Umschlagfelder: Der Inhalt der Kopfzeilen und Umschlagfelder kann überprüft werden. Diese Felder enthalten z. B. Absender, Empfänger und Betreff einer E-Mail.

Im zweiten Schritt wird eine Aktion festgelegt, die ausgeführt wird, wenn die Filterbedingungen zutreffen. Falls mehrere Filterbedingungen für eine Filterregel angegeben werden sollen, kann ausgewählt werden, wie die einzelnen Bedingungen miteinander verknüpft werden.

`UND` bedeutet dabei, das alle Filterbedingungen zutreffen müssen, damit die zugehörige Aktion ausgeführt wird. Bei `ODER` ist es ausreichend, wenn eine Filterbedingung erfüllt ist (siehe Abb. 6.25).

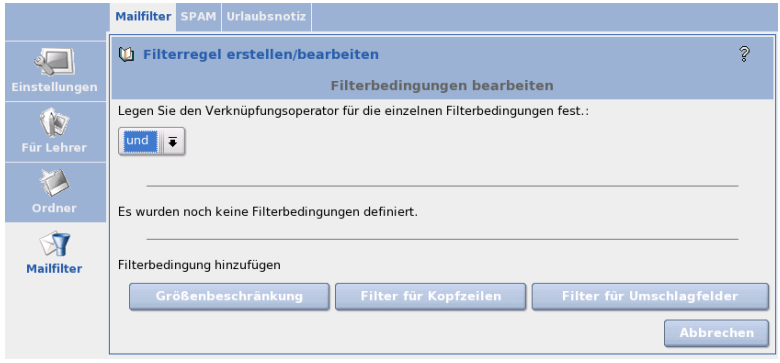

Abbildung 6.25: *Mailfilter*

An folgendem einfachen Beispiel führen wir die Konfiguration des Mailfilters vor: Ein Bekannter sendet Ihnen regelmäßig E-Mails. Sie wollen aber nicht alle dieser E-Mails erhalten. Sie wollen E-Mails aussortieren, die größer als ein Megabyte sind und von `bekannter@domain.de` gesendet werden. Sie wollen die Annahme solcher E-Mails verweigern und dies dem Absender auch mitteilen.

Abbildung 6.26: *Größenbeschränkung definieren*

Wählen Sie 'Filterregel einfügen'. Klicken Sie auf 'Größenbeschränkung' (siehe Abb. 6.26). Geben Sie den gewünschten Wert ein. In unserem Beispiel ist das 'Nachricht ist größer als 5 Megabyte'. Bestätigen Sie mit 'OK'. Wählen Sie dann den 'Filter für Kopfzeilen'. Geben Sie 'From enthält bekannter@domain.de' ein und bestätigen Sie wieder mit 'OK'. Damit haben Sie die Eingabe der Bedingungen abgeschlossen. Mit 'Weiter' kommen Sie in das Menü zur Auswahl einer passenden Aktion.

Wählen Sie 'weise Nachricht zurück mit der Begründung' und geben Sie dann einen aussagefähigen Text ein, z. B. „Ihre E-Mail ist zu groß, bitte senden Sie keine derart umfangreichen E-Mails an mich!" (siehe Abb. 6.27).

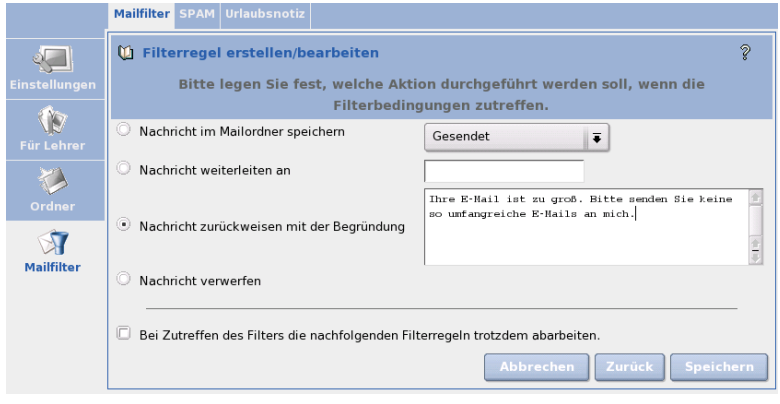

Abbildung 6.27: *Mailfilteraktion definieren*

Wenn Sie einen weiteren Filter auf diese E-Mail anwenden wollen (das ist in diesem Fall eher unwahrscheinlich), aktivieren Sie die Option 'Bei Zutreffen des Filters die nachfolgenden Filterregeln trotzdem abarbeiten.' Speichern Sie die Änderungen. Wenn Sie nun das Untermenü 'Mailfilter' erneut aufrufen, sehen Sie die angelegte Regel als Satz formuliert. Sie haben die Möglichkeit diesen Filter zu verändern (Symbol: Blatt/Bleistift), den Filter außer Kraft zu setzen (oder wieder zu aktivieren) ohne die eingegebenen Daten zu verändern (Symbol: rotes Kreuz/grüner Haken) oder den Filter zu entfernen (Symbol: Mülltonne). Um einen weiteren Filter zu entwerfen, verwenden Sie den Button 'Filterregel einfügen'. Sofern Sie das Feld 'an Position' nicht ändern, wird der neue Filter an die letzte Stelle gesetzt. Sie können aber auch die Position bestimmen. In manchen Fällen kann es wichtig sein, in welcher Reihenfolge die Filter abgearbeitet werden.

SPAM: Filter für ungewollte Werbemail

Der Open School Server ist für die Erkennung und Markierung von so genannter SPAM-Mail konfiguriert, deschalb können Sie hier festlegen, was mit Nachrichten, die als SPAM markiert wurden, gemacht werden soll. Sie haben folgende Möglichkeiten:

Abspeichern in einem Ordner: Wenn dieser Punkt aktiviert ist, kann ein Ordner ausgewählt werden, in dem sämtliche als SPAM markierte E-Mail abgelegt wird.

Löschen: Jede als SPAM erkannte E-Mail sofort löschen.

Achtung

Diese Einstellung sollte mit großer Vorsicht benutzt werden. Es ist unter Umständen möglich das auch E-Mails die kein SPAM sind, aufgrund typischer SPAM-Merkmale als SPAM erkannt werden.

Achtung

Nichts: Kein Sonderbehandlung für Nachrichten, die als SPAM erkannt wurden.

Urlaubsnotiz: Automatisches Antworten bei Abwesenheit

Mit der Urlaubsnotiz können Sie den Open School Server automatisch auf ankommende E-Mails antworten lassen. Klicken Sie auf 'Erstellen', um eine Notiz anzulegen. In der folgenden Maske geben Sie den Betreff und den Text der abzusendenden Nachricht ein (siehe Abb. 6.28 auf der nächsten Seite).

Soll der Betreff aus der zu beantwortenden E-Mail übernommen werden, lassen Sie das Feld 'Betreff' leer.

Im Feld 'Text' können Sie den Text eintragen, den die die automatische Antwort enthalten soll.

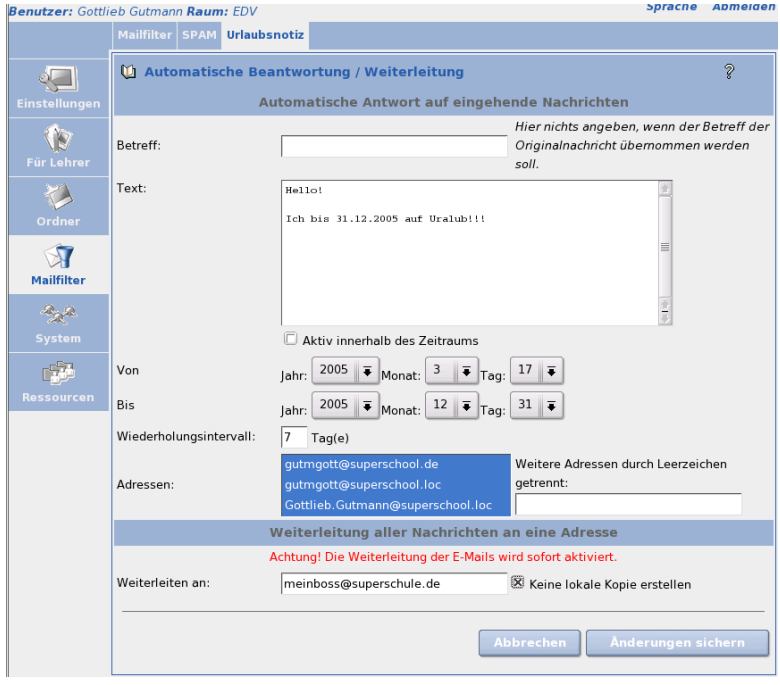

Abbildung 6.28: *Urlaubsnotiz erstellen*

Normalerweise wird die Urlaubsnotiz sofort durch einen Klick auf ‘Änderungen sichern’ aktiviert und Sie können Sie jederzeit wieder löschen.

Wenn Sie jedoch schon im voraus eine Urlaubsnotiz anlegen möchten, so können sie dies durch das Aktivieren der Checkbox ‘Aktiv innerhalb des Zeitraums’ tun. Stellen Sie anschließend über die beiden Pulldown-Menüs hinter ‘von’ bzw. ‘bis’ den entsprechenden Zeitraum ein.

Sendet Ihnen jemand bei aktivierter Urlaubsmeldung eine E-Mail, so erhält er die von Ihnen erstellte Nachricht als Antwort. Der Sender wird dabei in einer Datenbank gespeichert. Sollte der Sender Ihnen innerhalb der im Feld ‘Wiederholungsintervall’ eingetragenen Zeit erneut eine E-Mail schreiben, erhält er keine erneute automatische Antwort.

Zusätzlich können Sie im Feld ‘Weiterleiten an’ eine E-Mail-Adresse angeben, an die Ihre ankommende E-Mail weitergeleitet werden soll. Sie können die E-Mails an eine interne Adresse weiterleiten (z. B. wenn ein anderer Benutzer des Open School Server die Bearbeitung übernehmen soll), sowie an externe E-Mail-Adressen (z. B. ein Mailkonto, welches Sie auch von zu Hause aus erreichen können).

Wenn Sie eine Urlaubsnotiz eingerichtet haben, wird dies beim Aufruf des Untermenüs angezeigt. Sie haben hier die Möglichkeit, die Funktion durch einen Mausklick auf das Symbol rotes Kreuz/grüner Haken zu deaktivieren, bzw. wieder zu aktivieren, ohne die Einstellungen zu verändern.

6.3.6 Administration durch Lehrer

Wurden einer Lehrkraft beim Anlegen oder zu einem späteren Zeitpunkt Administrationsrechte vom Administrator zugewiesen, kann sie einige Systemadministrations selber durchführen.

- Uneingeschränkte Administration von Benutzer: Anlegen, Ändern, Löschen, Imporieren.
- Verwaltung von alle Gruppen: Benuztergruppen, Klassen, Arbeitsgruppen.
- Verwaltung der Arbeitsplatzrechner. (Registration, Löschen)

Hinweis

Beim Importieren der Lehrkräfte aus einer Liste werden den Lehrern keine Administrationsrechte zugeteilt. Hier muss der Administrator zu einem späteren Zeitpunkt manuell die entsprechenden Rechte zuweisen.

Hinweis

Client-Konfigurationen

Um den vollen Funktionsumfang des Open School Servers nutzen zu können, müssen sich die Benutzer an den Client–Rechnern anmelden. Erst nach dem Anmelden bekommen sie Zugang zum privaten Home–Verzeichnis und zu den gemeinsamen Verzeichnissen (Freigaben). Damit die Anmeldung möglich wird, müssen die Windows–Clients in die Windows–Domäne des Open School Servers aufgenommen und UNIX/Linux–Clients als LDAP– bzw. NFS–Clients des Open School Servers konnfiguriert werden.

Zum Schluss dieses Kapitels wird die Einrichtung der Drucker an den Clientrechner beschrieben.

7.1 Konfiguration von UNIX/Linux-Clients

Damit sich UNIX/Linux-Benutzer dem Open School Server gegenüber authentifizieren können und von dort ihre Heimatverzeichnisse mittels „automounter“ erhalten, müssen die Rechner als LDAP– bzw. NFS–Clients konfiguriert werden.

Die, mit der automatischen Installationsumgebung installierten, SUSE-Linux-Clients, müssen lediglich über ‘Rechnerverwaltung’ an den Open School Server angemeldet werden, damit diese Rechner einem Schulraum zugeordnet werden (siehe Kapitel 6.2.3 auf Seite 76).

Die Konfiguration als LDAP bzw. NFS-Client wurde schon während der Installation erledigt. Bei anderen UNIX/Linux Clients müssen noch folgende Konfigurationsschritte durchgeführt werden:

1. Stellen Sie sicher, dass es eine Netzwerkverbindung zwischen dem Open School Server und den Client besteht.

2. Melden Sie sich als Benutzer `root` am Client an.

3. Konfigurieren Sie die Netzwerkkarte des Clients, und stellen Sie sicher, dass dieser alle Netzwerkspeziefische einstellungen (die IP-Adresse, Hostname, Nameserver, Default-Route) vom DHCP erhält.

4. Öffnen Sie in einem Webbrowser die Webseite `https://admin`. Der Browser weist Sie darauf hin, dass ihm das Zertifikat des OSS nicht bekannt ist. Importieren Sie das Zertifikat über den entsprechenden Menüpunkt.

5. Jetzt können Sie den Rechner über die Weboberfläche am Schulserver anmelden. Wählen Sie dazu folgende Menüpunkte:
   ‘Rechner/Domänen’ → ‘Rechnerverwaltung’
   Ggf. müssen Sie über ‘Neuer Schulraum’ einen neuen Raum aufnehmen. Klicken Sie auf den Knopf ‘Rechner hinzufügen’ neben dem gewünschtem Raum. Nun werden Sie auf die nächste Seite weitergeleitet. Da Sie in diesem Fall die Aufnahme direkt vom Client aus ausführen, erkennt der Open School Server die Hardwareadresse des zu registrierenden Rechners und trägt diese in Feld ‘Hardwareadresse:’ ein. Auf der linken Seite finden ist die Liste der verfügbaren Rechnernamen des Raumes. Wählen Sie nun den gewünschten Rechnernamen und klicken Sie auf ‘Eintragen’.

6. Je nach UNIX/Linux-Version können Sie verschiedene Werkzeuge für die NFS- bzw. LDAP-Client-Konfiguration verwenden (bei SUSE ist das der YaST2 LDAP Modul, bei Red Hat muss man dafür Authconfig verwenden), letztendlich werden jedoch folgende Einträge benötigt:

NFS-Client: In der Datei `/etc/fstab` müssen Sie folgenden Eintrag als letzte Zeile einfügen:

```
nfs:/home /home nfs defaults 0 0
```

LDAP-Client: Für die manuelle Konfiguration sind drei Schritte notwendig

Zunächst soll in der Datein '/etc/openldap/ldap.conf' und '/etc/ldap.conf' der zu verwendende LDAP-Server und der Verzeichnissbaum spezifiziert werden:

```
nss_base_passwd ou=people,<LDAPBASE>
nss_base_shadow ou=people,<LDAPBASE>
nss_base_group  ou=group,<LDAPBASE>
host            ldap
base            <LDAPBASE>
ldap_version    3
pam_passwd      crypt
ssl             yes
```

Datei 6: *ldap.conf*

Anschließend ist die Namensauflösung auf LDAP umzustellen. Hierzu editieren Sie die Datei `/etc/nsswitch.conf`:

```
passwd: files ldap
shadow: files ldap
group:  files ldap
```

Datei 7: *nsswitch.conf*

Nur die hier aufgeführten Einträge müssen angefasst werden.

Für die Authentifizierung ist die PAM-Konfiguration zu Ändern. Dazu müssen in der Dateien `login`, `xdm` und `session` folgende Einträge angepasst werden:

```
auth suffizient     /lib/security/pam_ldap.so use_first_pass
password suffizient /lib/security/pam_ldap.so use_authtok
session optional    /lib/security/pam_ldap.so
```

Datei 8: */etc/pamd/{login,xdm,session}*

7.2 Anbindung von Windows-Clients

Um den vollen Funktionsumfang des Open School Servers nutzen zu können, müssen sich die Benutzer an den in die Domäne eingebundenen Client-Rechnern anmelden. Nach der Anmeldung bekommen sie dann Zugang zu Ihrem privaten Home-Verzeichnis und zu den gemeinsamen Verzeichnissen (Freigaben).

Um die Anmeldung zu ermöglichen, müssen die Windows–Clients in die Windows–Domäne des Open School Servers aufgenommen werden. Die Anbindung von Windows–Clients (ab Windows NT) erfolgt in folgenden Schritten:

1. Stellen Sie sicher, dass eine Netzwerkverbindung zwischen dem Open School Server und den Windows–Client besteht.
2. Melden Sie sich als lokaler Benutzer `Administrator` am Windows-Client an und stellen Sie sicher, dass der Rechner nicht der Domäne–Schulserver angehört.
3. Wählen Sie 'Netzwerkeinstellung → TCP-IP → IP-Adresse' automatisch beziehen. Überprüfen Sie ob die Verteilung der IP–Adresse erfolgreich war. Geben Sie dazu in einem DOS–Fenster den Befehl `ipconfig /all` ein. Der Client sollte eine IP–Adresse aus dem Schulnetz (genauer: dem während der Installation festgelegten Bereich für unbekannte Rechner) bekommen haben.
4. Öffnen Sie in einem Webbrowser die Webseite `https://admin`.
5. Jetzt können Sie den Rechner über die Weboberfläche am Schulserver anmelden. Wählen Sie dazu folgende Menüpunkte:
   - Melden Sie sich als Benutzer `admin` an der Administrationsweboberfläche an.
   - 'Rechner/Domänen → Rechnerverwaltung'
   - Ggf. müssen Sie über 'Neuen Raumnamen eintragen' einen neuen Raum aufnehmen.
   - Klicken Sie auf den Knopf 'Rechner hinzufügen' neben dem gewünschtem Raum. Nun werden Sie auf die nächste Seite weitergeleitet.
   - Wenn Sie in diesem Fall die Aufnahme direkt vom Client aus ausführen, erkennt der Open School Server die Hardwareadresse des zu registrierenden Rechners und trägt diese in Feld 'Hardwareadresse:' ein. Auf der linken Seite ist die Liste der verfügbaren Rechnernamen des Raumes.
   - Verlief die Registrierung erfolgreich, zeigt Ihnen der Browser den DNS–Namen, den Netbios–Namen und die IP–Adresse des Clients an. Notieren Sie sich diese Angaben.

6. Sie müssen nun den Netbios–Namen des Clients zu dem vom Open School Server vergebenen ändern. Starten Sie anschließend den Client neu. Ändern Sie den Netbios–Namen eines Windows–Clients wie folgt:

   - 'Start → [Rechte–Maustaste] → Arbeitsplatz → Eigenschaften'
   - '[Reiter–Computername] → Ändern'
   - Tragen Sie jetzt den Computernamen ein und klicken Sie auf 'OK'. Nun müssen Sie den Rechner neu starten.
     WICHTIG! Sie dürfen den Rechner auf keinen Fall sofort in die Domäne aufnehmen: er soll zunächst zu einer Arbeitsgruppe oder einer anderen Domäne gehören. Sie können auch einen fiktiven Arbeitsgruppenamen angeben, der in ihrem Netzwerk nicht existiert.

7. Nach dem Neustart überprüfen Sie nochmals ob der Rechner die richtige IP–Adresse und den richtigen Namen erhalten hat. Dann erst treten Sie mit dem Rechner der Domäne des OSS bei. Dies geschieht im selben Menüpunkt, in welchem Sie auch die Änderung des Netbios–Namens vorgenommen haben. Wenn Sie während der Installation den Namen der Windows–Domäne nicht explizit verändert haben, benutzt der Open School Server den DNS–Domänenamen Ihrer Schule ohne die Toplevel–Domain. (Aus `School.de` wird `School`.)
   Haben Sie die Domäne eingetragen und auf 'OK' geklickt, verlangt Windows nach einem Benutzernamen und Passwort. Geben Sie als Benutzername `root` oder `Administrator` und als Passwort das während der Installation des Open School Server festgelegte Passwort für den Admin an.

8. Nach einem weiteren Neustart ist der Client dann einsatzbereit.

9. Ab Windows–NT ist es möglich, Dateien, die auf Netzwerklaufwerken liegen auch offline zur Verfügung zu stellen. In einem Schulnetzwerk haben die Benutzer meistens keine festen Arbeitsplätze, deshalb würde die Synchronisation der Dateien sehr viel Zeit und Performance bei jeder An– und Abmeldung erfordern. Deshalb ist es ratsam, die Verwendung von Offlinedateien auf den Clients abzuschalten. Bei Win–NT und Win–2000 ist das die Standardeinstellung. Im Falle von Windows–XP Clients ist jedoch die Synchronisierung der sog. `EigeneDateien` standardmäßig eingeschaltet, wenn diese auf einem Netzwerklaufwerk liegen, was beim Open School Server der Fall ist. Die Verwendung von Offlinedateien wird unter 'Arbeitsplatz → Extras → Ordneroptionen...' mit der Checkbox 'Offlinedateien aktivieren' ein– bzw. ausschaltet.

Hinweis

Wächterkarten und Maschinenaccounts

In bestimmten Zeitabständen handeln die Windows-2000 und Windows-XP Clients mit dem Server automatisch neue Passwörter für die Maschinenkonten aus. Sollten Sie zur Absicherung der Clients „Wächterkarten“ (Schutzkarten) einsetzen, werden diese geänderten Passwörter beim nächsten Reboot der Clients wieder zurückgesetzt. Der Server hat sich aber das neue Passwort gemerkt, und so können sich die Clients dann nicht mehr in der Domäne anmelden, da Sie dem Server das falsche (alte) Passwort übermitteln. In diesem speziellen Fall sollten Sie also in der Registry nach dem Schlüssel `DisablePasswordChange` suchen und diesen auf den Wert `1` setzen. Unter Windows 2000 finden Sie diesen Schlüssel meist unter `/hkey_local_machine/system/currentcontrolset/services/netlogon/parameters/`.

Hinweis

7.2.1 Microsoft Windows 95/98/ME

Stellen Sie zunächst sicher, dass alle Softwarekomponenten vorhanden sind, die Windows benötigt, um auf den Server zuzugreifen. Wählen Sie hierzu in der Systemsteuerung den Punkt ‘Netzwerk’ aus. Ein Fenster mit drei Registerkarten und einer Übersicht der installierten Netzwerk-Komponenten erscheint (siehe Abb. 7.1 auf der nächsten Seite).

Netzwerkverbindung zum Server herstellen

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 des Servers eingetragen ist. Standardmäßig wird hier `192.168.0.1` vorgeschlagen.

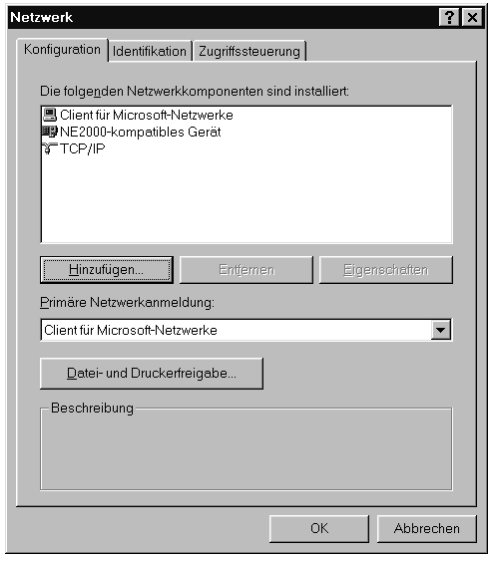

Abbildung 7.1: *Netzwerkkonfiguration unter Windows 95/98/ME*

Sie können die Einstellungen überprüfen, indem 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

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

Gateway leer

DNS-Konfiguration Ausgewählt ist 'DNS deaktivieren'

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.

Anmelden an einer Domäne

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.

Ist der Server als PDC 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.

Damit Ihr Windows-Client korrekt funktionieren kann, benötigt er eine NT-Domäne.

Unter Windows tragen Sie im Menü 'Client für Microsoft-Netzwerke' → 'Eigenschaften' → 'Windows NT-Domäne' die entsprechendne NT-Domäne ein. Diese ergibt sich aus der Samba-Konfiguration.

Beachten Sie, dass Sie das Kästchen 'An Windows NT-Domäne anmelden' anklicken und so mit einem Haken versehen. Wenn der Open School Server als Primary Domain Controller konfiguriert wurde, erfolgt die gesamte Benutzerverwaltung auf diesem Server. Jeder angelegte Benutzer ist dann auch den Windows-Clients bekannt.

Verwenden Sie eine frühe Version von Windows 95, die noch keine Übertragung von verschlüsselten Passwörtern an Samba unterstützt, dann 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.

7.2.2 Template-Benutzer

Der Open School Server bietet Ihnen eine einfache Möglichkeit, die Einstellungen für den Desktop, das Startmenü und einige weitere als `Profile` bezeichneten Vorgaben für neue Nutzer vorzugeben und alten Nutzern auch noch nachträglich zuzuweisen. Das geschiet über sog. „Template-Benutzer“. Die Template-Benutzer sind in erster Linie auch normale Benutzeraccounts. Das heisst, man kann sich mit diesem Accounts an die Clients (sowohl Windows, als auch UNIX/Linux) anmelden. Der Zweck von diesen Accounts ist jedoch nicht, dass man damit Arbeitet, sondern die Zusammenstellung verschiedener Arbeitsumgebungen sog. „Profilen“, die man an den realen Benutzer zuweisen kann. Leider sind die Profilen unter den verschiedenen Betriebsysgtemen nicht miteinander kompatiebel, deshalb müssen diese für alle verwendeten Betriebsystemen extra erstellt werden.

Die Profile der Template-Benutzer können auf zwei Arten den Benutzer zugewiesen werden:

1. Für jede primäre Benutzergruppe existiert ein Template-Benutzer. Beim Anlegen eines Benutzers wird dem Benutzer das Profil des entsprechenden Template-Benutzers zugewiesen, wenn dieses vorhanden ist.

2. Die Lehrer können den Schülern und die Administratoren jedem Benutzer ein beliebiges Profil zuweisen. ('Benutzer' → 'Bearbeiten' 'Profile verteilen')

Die persönliche Windows–Profile der Benutzer befinden sich auf dem Open School Server unter `/home/profile/<Benutzer--UID>/<Windows--Version>`. Auf diese Verzeichnisse haben nur die jeweiligen Eigentümer und die Benutzer `root` und unter Windows `<Windows-Domäne>\Administrator` Zugriff.

Tipp

Weitere Vorlagen anlegen

Sie können beliebig weitere Vorlagen anlegen. (Wie das geht finden Sie unter *Neu – Anlegen einzelner Benutzer* auf Seite 58 Dies kann z.B. für bestimmte Räume oder bestimmte Kurse sinnvoll sein, die von den normalen Vorgaben abweichen. So kann z. B. für einen anders ausgerüsteten Computerraum ein eigenes Profil angelegt werden und den Schülern vor der Nutzung des Raumes zugewiesen werden oder für bestimmte Kurse können die Profile vor Kursbeginn bei allen Kursteilnehmern passend gesetzt werden.

Tipp

7.2.3 Default User Profil

Direkt nach der Installation sind die Profile der Template-Benutzer erst leer, deshalb bekommt jeder Benutzer (auch die Template-Benuzter) beim ersten Anmelden die sog. „Default User" Profile zugewiesen. Diese Profil existiert zur Zeit für Linux Win2000 und WinXP Clients und befinden sich unter:

`/var/lib/samba/netlogon/Win2K/DefaultUser/` für Windows 200

und

`/var/lib/samba/netlogon/WinXP/DefaultUser/` für Windows XP.

Diese Profile erhalten folgende Voreinstellungen:

- Proxy-Einstellungen
- „Eigene Dateien" auf `Z:` (Homeverzeichnis) umleiten
- Die wichtigsten Links (`https://admin`, `https://schulserver` und `http://www.extis.de/oss`) sind auf dem Desktop vorhanden.

Für andere Windows-Versionen (Win9X und WinNT) sind die Verzeichnisse schon angelegt, zur Zeit werden jedoch noch keine default Profile mitgeliefert. Durch die „Default User“ – Profile wird erreicht, dass jeder Benutzer (unabhängig davon ob Schüler oder Lehrer) eine vordefinierte Umgebung auf seinem Windows–Client vorfindet.

7.2.4 Nutzerprofile vorbereiten

In der Grundeinstellung bekommt jeder Benutzer das selbe Windows-Profil, das des „Default Users“ der jeweiligen Windows-Version. Möchte man für die verschiedenen Benutzergruppen unterschiedliche Profile einstellen, muss man dafür die sog. Template-Benutzer verwenden. Die Profile der Template-Benutzer werden auf zwei Arten verwendet:

1. Für jede primäre Benutzergruppe existiert ein Template-Benutzer. Beim Anlegen eines Benutzers wird dem Benutzer das Profil des entsprechenden Template-Benutzers zugewiesen (kopiert), wenn dieses vorhanden ist.
2. Die Lehrer können den Schülern und die Administratoren jedem Benutzer ein beliebiges Profil zuweisen. (‘Benutzer’ → ‘Bearbeiten’ → ‘Profile verteilen’)

Für die Template-Benutzer sind im Auslieferungszustand noch keine Profile angelegt. Wenn man solche braucht, mussi man diese unter WinXP in folgender Weise erstellen:

1. Man melde sich als Template-Benutzer (z.B. „tstudents“, Passwort = admin-Passwort) an einer Windows-Workstation an die Windows-Domäne an, und stelle die gewünschte Umgebung zusammen. Anschließend muss man sich abmelden, damit das Profil auf den Server zurückgeschrieben wird.
2. Das Windows-Profil ist nun einsatzbereit. Allerdings hat zur Zeit nur der Ersteller (der Templatebenutzer) Zugriffsrechte auf dieses Profil. Es gibt 2 Möglichkeiten, anderen Benutzern den Zugriff zu ermöglichen:
   (a) Man gibt Lokal-Administrator Rechte der Benutzergruppe Domain Users auf den Clients.
   (b) Man gibt allen Benutzern Zugriffsrechte auf das Profil.

Lokal-Administrator Rechte der „Domain Users“ Gruppe

1. Melden Sie sich als Domänen-Benutzer `admin` an einem Windows Rechner an.

2. Öffnen Sie die Benutzerverwaltung: 'Start'<93> → 'Systemseuerung' → 'Benutzerkonten<93>'
3. Öffnen Sie die Erweiterte Benutzerverwaltung: Reiter 'Erweitert' → 'Erweitert'
4. Wählen Sie unter Gruppen die Gruppe 'Administratoren'
5. 'Action' → 'Mitglieder hinzufügen' → 'Hinzufügen'
6. Der Name der hinzufügende Gruppe ist <DOMÄNENAME>/Domain Users und kann über 'Erweitert' → 'Jetzt suchen' ausgewählt werden.

Hinweis

Diese Änderung müssen Sie auf allen Windows-Clients vornehmen. Durch diese Änderung werden alle Domänen-Benutzer unbeschränkte Rechte (dies ist bei vielen Schulsoftware-Paketen leider unbedingt erforderlich) auf den Clients bekommen, deshalb müssen Sie für deren Integrität mit Hilfsmitteln (Wächterkarten, Imaging-System) Sorge tragen.

Hinweis

Bearbeitung der Zugriffsrechte der Profile

1. Melden Sie sich als Domänen-Benutzer `Administrator` (Passwort = admin-Passwort) an derselben Windows-Workstation an, auf welcher das Profil vorher erstellt worden ist.
2. Nun speichern Sie das neu erstellte Benutzerprofil in das Profil Verzeichnis des Template-Benutzers:
3. 'Start' → 'Arbeitsplatz' - Rechte Maustaste drücken → 'Eigenschaften'
4. 'Erweitert' → 'Benutzerprofile' → 'Einstellungen' Wählen Sie nun das gewünschte Profil aus `<Domänenname>/tstudents`
5. 'Kopieren'
6. 'Benutzer' → 'Ändern'
7. 'Geben Sie die zu verwendenden Objektnamen ein' → 'Jeder' → 'OK'
8. 'Profil kopieren nach' → `U:\profiles\tstudents\WinXP` Nun ist das Profil einsatzbereit.

Hinweis

Nach jeder Änderung der Profile (wenn man sich als Templatebenutzer anmeldet), muss das Profil durch den Benutzer `Administrator` neu gespeichert werden.

Unter Windows NT und Windows 2000 funktioniert das Erstellen von Templateprofilen in gleicher Weise, nur muss am Ende des Pfades beim Kopieren der entsprechende Name stehen: WinNT bzw. Win2K

Hinweis

Default User Profil ändern Möchte man das „Default User“ Profil ändern, muss man ein vorher erstelltes Benutzerprofil ins entsprechende Verzeichnis kopieren. Dazu muss man sich als Benutzer `Administrator` (Passwort = admin-Passwort) an der Windows-Domäne anmelden. Der Pfad zu dem „Default User“ Profilverzeichniss ist `n:/DefaultUser`. Um zum Beispiel das WinXP-Profil des `tstudents` als „Default User“ Profil zu verwenden müssen Sie folgende Schritte ausführen:

1. Den Inhalt des Verzeichnisses `n:/DefaultUser` löschen.
2. Den Inhalt des Verzeichnisses `u:/profile/tstudents/WinXP` `n:/DefaultUser` kopieren.

7.2.5 Profile übertragen

Sie können schon existierenden Nutzern auch nachträglch noch ein geändertes Profil übertragen, indem Sie diese Benutzer unter ‘Benutzer’ → ‘Bearbeiten’ im Administrationsmenü markieren und auf ‘Profile verteilen’ klicken. Wählen Sie im nachfolgenden Dialog ein Default Profil aus dem Pull-Down-Menü aus und bestätigen Sie Ihre Wahl mit ‘Profil übertragen’ (siehe Abbildung *Profile übertragen* auf dieser Seite).

Abbildung 7.2: *Übertragen eines neuen Profils an existierende Benutzer*

7.2.6 Neue Profile anlegen

Sie können beliebig viele neue Vorlagen für Benutzer anlegen. Legen Sie dazu im Administrationsmenü unter 'Benutzer' → 'Neu' unter 'Primäre Gruppe' den Eintrag `Template Benutzer` aus (siehe Abbildung *Neue Profile anlegen* auf dieser Seite). Ein Template Benutzer benötigt zwingend:

- Ein Benutzerkürzel (uid) - das Benutzerkürzel sollte mit einem kleinen `t` beginnen und nicht mehr als 8 Buchstaben umfassen.
- Einen Nachnamen, der später im Auswahlmenü angeboten wird. Wählen Sie hier also eine aussagekräftige Beschreibung.
- Keinen Geburtstag.

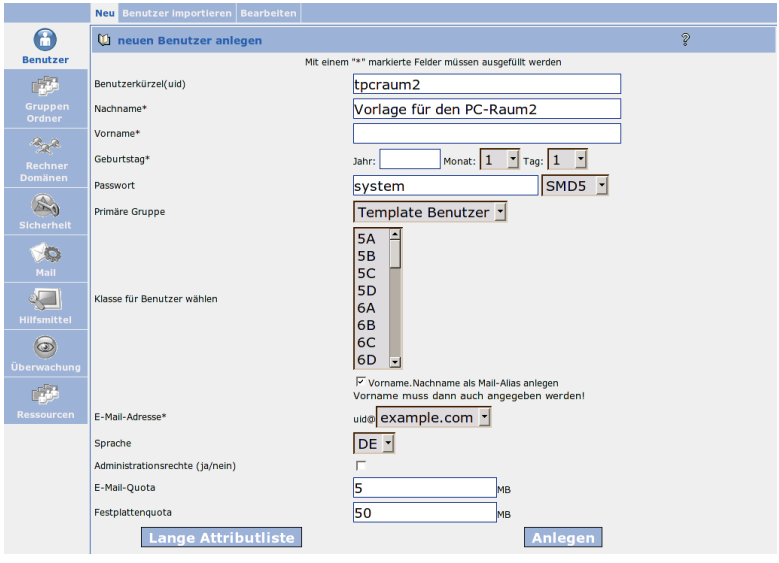

Abbildung 7.3: *Anlegen eines neuen Template-Benutzers*

7.2.7 Hinweise zum Gruppenrichtlinieneditor

Wie die Clients die Serverprofile Verwenden können Sie mit dem Gruppenrichtlinieneditor einstellen. (Diese Einstellingen sind nicht notwendig in bestimmten Fällen jedoch sehr hilfreich.)

Melden Sie sich dazu mit lokalen Administratorrechten an und starten Sie den Gruppenrichtlinieneditor über 'Start' → 'Ausführen' → 'gpedit.msc' (siehe Abbildung *Hinweise zum Gruppenrichtlinieneditor* auf dieser Seite).

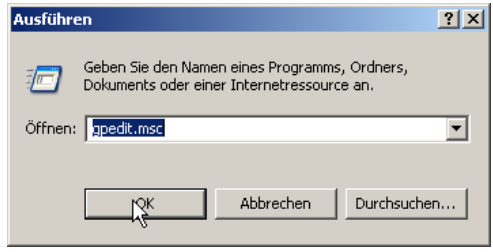

Abbildung 7.4: *Gruppenrichtlinieneditor starten*

Folgende Einstellungen sollte Sie unter 'Richtlinien für Lokaler Computer' → 'Computerkonfiguration' → 'Administrative Vorlagen' → 'System' → 'Benutzerprofile' aktivieren, damit die Anmeldung der Benutzer im Schulnetz sichergestellt ist und die Festplatten der Clients nicht „überlaufen" (siehe Abbildung *Hinweise zum Gruppenrichtlinieneditor* auf der nächsten Seite)

Zwischengespeicherte Kopien von servergespeicherten Profilen löschen Diese Einstellung Aktivieren Sie und legen so fest, dass keine Kopie des servergespeicherten Benutzerprofils auf der Festplatte dieses Computers bei der Benutzerabmeldung gespeichert wird. Damit muss zwar bei jeder Anmeldung das komplette Profil auf den Computer übertragen werden, aber Sie stellen damit einerseits sicher, dass niemand die Festplatte des Clients überfüllen und damit den Client „unbrauchbar" machen kann (Windows verweigert die Anmeldung, wenn die Festplatte voll ist) und andererseits funktioniert nur auf diese Weise das Übertragen von Profilen vom Server aus.

Normalerweise wird eine Kopie des servergespeicherten Benutzerprofils eines Benutzers bei der Benutzerabmeldung auf der Festplatte des Computers gespeichert, damit – falls der Server, auf dem das Hauptprofil gespeichert wurde – beim nächsten Neustart des Computers nicht verfügbar ist sich der Benutzer trotzdem noch am Client anmelden kann.

Durch Aktivieren dieser Einstellung werden sämtliche Kopien des servergespeicherten Benutzerprofils des Benutzers bei der Benutzerabmeldung gelöscht. Das servergespeicherte Benutzerprofil wird aber weiterhin auf dem Server gespeichert.

Remotebenutzerprofil abwarten Lädt die Remotekopie des servergespeicherten Benutzerprofils, auch wenn die Kopie nur langsam geladen wird. Zusätzlich wird

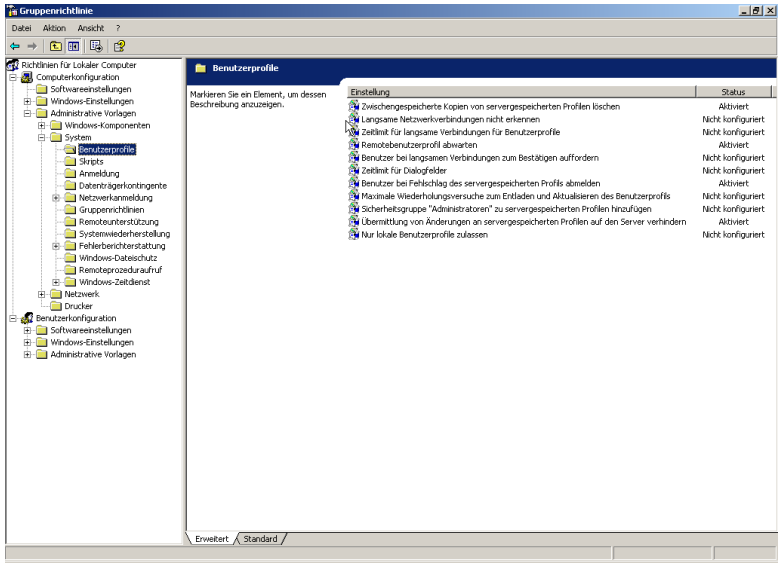

Abbildung 7.5: *Gruppenrichtlinieneditor: Verhalten der Benutzerprofile einstellen*

auf die Remotekopie gewartet, wenn der Benutzer über eine langsame Verbindung benachrichtigt wird, aber nicht innerhalb der zugelassenen Zeit reagiert.

Wenn Sie diese Einstellung aktivieren, wird auch bei einer langsamen Verbindung das servergespeicherte Benutzerprofil geladen.

Es ist sinnvoll, auf das Remoteprofil zu warten, wenn Benutzer häufig zwischen Computern wechseln, da ihre Profile somit nicht aktuell sind.

Benutzer bei Fehlschlag des servergespeicherten Profils abmelden Meldet einen Benutzer automatisch ab, wenn das servergespeicherte Benutzerprofil des Benutzers nicht geladen werden kann.

Diese Einstellung ist hilfreich, wenn ein servergespeichertes Benutzerprofil nicht gefunden werden kann, oder das Profil fehlerhaft ist und daher nicht ordnungsgemäß geladen werden kann.

Wenn Sie diese Einstellung nicht aktivieren wird, falls das Laden des servergespeicherten Profils fehlschlägt, das Standardbenutzerprofil, das unter `\%Systemroot\%\\DokumenteundEinstellungen\\DefaultUser` gespeichert wird, geladen.

Übermittlung von Änderungen an servergespeicherten Profilen auf den Server verhindern Mit dieser Einstellung wird festgelegt, ob die Änderungen, die Benutzer an ihren

servergespeicherten Profilen vornehmen, mit der Serverkopie der entsprechenden Profile zusammengeführt werden.

Wenn sich ein Benutzer mit einem servergespeicherten Profil an einem Computer anmeldet, wird standardmäßig sein servergespeichertes Profil auf den lokalen Computer kopiert. Wenn sich der Benutzer bereits früher an diesem Computer angemeldet hatte, wird das servergespeicherte Profil mit dem lokalen Profil zusammengeführt. Auf ähnliche Weise wird bei der Abmeldung des Benutzers von diesem Computer die lokale Kopie des Profils, einschließlich aller vorgenommenen Änderungen, mit der Serverkopie des Profils zusammengeführt.

Mit dieser Einstellung können Sie verhindern, dass Änderungen, die an einem servergespeicherten Profil auf einem bestimmten Computer vorgenommen wurden, übernommen werden.

Wenn Sie diese Einstellung aktivieren, geschieht am betreffenden Computer Folgendes: Bei der Anmeldung erhält der Benutzer sein servergespeichertes Profil. Alle Änderungen, die ein Benutzer an seinem Profil vornimmt, werden jedoch bei der Abmeldung nicht mit dem servergespeicherten Profil zusammengeführt.

Auf in den weiteren Unterordnern finden Sie sicherlich noch die eine oder andere Option, die in Ihrem Schulnetz geeignet ist.

Wir möchten hier nur noch auf den 'Windows-Zeitdienst' hinweisen, den Sie ebenfalls im Ordner 'System' finden.

So können Sie 'Globale Konfigurationseinstellungen' `Aktivieren` und haben damit grundlegende Einstellungen getroffen, die den Windows-Clients einen Zeitabgleich mit einem Zeitserver ermöglicht.

Wenn Sie sicherstellen möchten, dass die Clients den Zeitserver des Open School Server nutzen, müssen Sie lediglich noch zwei Einstellungen unter 'Zeitanbieter' machen: 'Windows-NTP-Client aktivieren' setzen Sie auf `Aktiviert` und unter 'Windows-NTP-Client konfigurieren' geben Sie unter 'NTP-Server' den Wert `timerserver,0x1` ein und aktivieren auch diese Einstellungen (siehe Abbildung *Hinweise zum Gruppenrichtlinieneditor* auf der nächsten Seite).

7.3 Drucker einrichten

7.3.1 Drucker auf UNIX/Linux Clients einrichten

Um auf den Drucker des Druckerservers von UNIX/Linux Clients zugreifen zu können, muss auf den Clients der CUPS-Client (Common Unix Printing System) installiert sein.

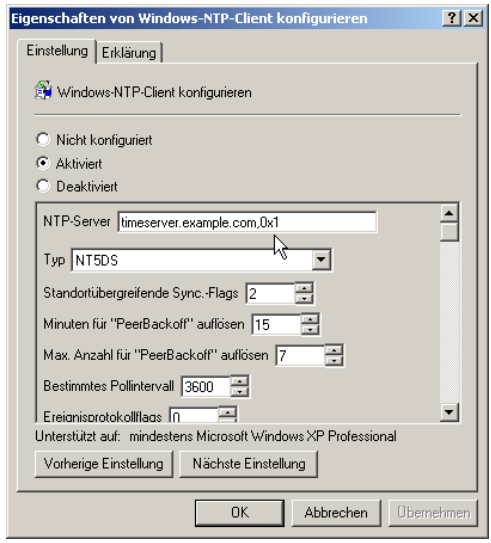

Abbildung 7.6: *Gruppenrichtlinieneditor: Timeserver einstellen*

Zwar ist es möglich, dass der Printserver über Broadcast die verfügbaren Drucker den Clients mitteilt, es ist jedoch empfehlenswert, den Clients dem Druckserver manuell mitzuteilen. Das geschieht durch folgenden Eintrag in der Datei `/etc/cups/client.conf`:

```
ServerName printserver
```

Datei 9: *Eintrag des Druckservers in der Datei path/etc/cups/client.conf*

Auf automatisch installierten (open)SUSE Clients ist dieser Eintrag schon vorhanden.

7.3.2 Drucker auf Windows Clients einrichten

Ab der Version 2000 unterstützt auch Windows das sog. ipp-Protokol (Internet Printing Protocol). Dadurch ist ein direkter Zugriff von Windows-Clients auf den Printserver des Open School Server möglich.

So richtet man einen Drucker, der am Open School Server installiert ist, an einem Windows-Client ein:

1. 'Start' → 'Drucker und Faxgeräte'

2. ‘Drucker hinzufügen’

3. ‘Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist.’

4. ‘Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen:’
   `URL: http://printserver:631/printers/<Druckername>`

5. ‘Druckertreiber Installation.’

Tipp

Drucken über Postscripttreiber

UNIX-änliche Betriebsysteme (UNIX, MacOS, Linux) kennen nur ein einziges Druckerformat: Postscript.

Das bedeutet alle Anwendungen liefern ein Postscript-Dokument dem Druckserver und dieser sorgt dafür, dass dieses auf dem jeweiligen Drucker sauber ausgedruckt wird. Dabei kümmert sich der Drucker selbst um die optimale Aufbereitung des Dokuments und der Client benötigt nur einen „universellen“ Druckertreiber: den Postscript-Treiber, um auf zig verschiedenen Druckern die jeweils besten Resultate zu erzielen.

Unter Windows kann man dieses Verhalten nachahmen, wenn man auf Windows-Clients für alle Drucker den „Generic Postscript“–Treiber installiert und die Umwandlung in das richtige Format dem Printserver überlässt. Als „Generic Postscript“–Treiber hat sich der Treiber für den Apple Laser Writer etabliert, da dieser ein sehr korrektes Postscript-Format liefert und bei Windows immer vorhanden ist.

Dadurch erreicht man einerseits, dass das Layout der Dokumente unabhängig von dem gewählten Drucker ist, andererseits wird dadurch das Accounting der Druckaufträge durch den Printserver ermöglicht.

Ein weiterer Vorteil: fällt einmal der Drucker aus, müssen nicht an allen Clients neue Druckertreiber installiert werden. Die neue Drucker bekommt einfach den Namen des alten Druckers und wird am Open School Server korrekt eingerichtet. Für die Clients ändert sich überhaupt nichts.

Tipp

Imaging von Clients

Der Open School Server bietet eine Lösung zum Installieren, Wiederherstellen, Klonen und Migrieren von PCs. Damit steht neben der vollautomatischen Installation (siehe *Autoinstallation und Booten über Netzwerk* auf Seite 151) und dem damit evtl. verbundenen Betrieb eines zusätzlichen LTSP-Terminalservers (siehe *Externer LTSP-Terminalserver* auf Seite 203) eine weitere effektive Möglichkeit zur Verfügung den Administrationsaufwand eines Schulnetzwerks zu senken.

8.1 Technischer Hintergrund

Die am Open School Server eingesetzte Imaging-Lösung unterscheidet zwischen Hardware- und Software-Konfigurationsobjekten. Anhand dieser beiden Konfigurationsobjekte lassen sich verschiedene Images erstellen, pflegen und den unterschiedlichen Clients zuweisen.

Hardwarekonfiguration In einem Hardwarekonfigurationsobjekt wird die Beschreibung der Clienthardware gespeichert. Dies dient einerseits später der Erstellung von Images, die für die spezielle Hardware geeignet sind, andererseits läßt sich so auf einfache Art und Weise an zentraler Stelle eine Übersicht über die Hardwarekomponenten eines Clients pflegen.

Um eine solche Inventarliste zur Verfügung stellen zu können, werden die entsprechenden Daten zu jedem Client im LDAP-Verzeichnis des Open School Servers gesammelt.

Softwarekonfiguration In einem Softwarekonfigurationsobjekt wird ein installiertes Softwarepaket beschrieben. Dieses beinhaltet nicht nur das bzw. die installierten Betriebssysteme sondern auch die auf dem Client installierten Programme.

Images stellen nun eine Verbindung zwischen verschiedenen Hardware- und Softwarekonfigurationen dar. Für jede Kombination aus eingesetzter Hardware und darauf einzuspielender Software muss also ein eigenes Image erstellt werden. Dieses Image wird dann auf dem Open School Server im Verzeichnis `/srv/itool/images` abgespeichert.

Die Konfiguration für die einzelnen Clientimages wird im Verzeichnis `/srv/itool/config/<hardware-addresse>.inf` abgelegt. Die `hardware-addresse` ist dabei die „MAC-Addresse“ der Netzwerkkarte des Clients.

Das Verzeichnis `/srv/itool` ist über Samba von jedem Windows-Rechner aus unter dem Verzeichnisnamen `itool` für Mitglieder der Gruppen `sysadmins` und `Lehrer` (teachers) erreichbar.

Hinweis

Platz im Verzeichnis /srv

Da die sowohl die Images der Client als auch die SUSE CD-s für die automatische Installation unterhalb des Verzeichnisses `/srv` liegen, ist es angebracht dieses Verzeichnis während der Installation auf eine eigene, große Partition zu legen, wenn man eine oder gar beide Möglichkeiten nutzen will.

Hinweis

8.2 Nutzung der Imaging-Lösung

Zunächst müssen die für das Imaging vorgesehenen Clients für das Booten über PXE konfiguriert werden. Dies geschieht je nach vorhandenem BIOS der Clients und der eingebauten Netzwerkkarten unterschiedlich. Bitte werfen Sie hierfür einen Blick in die entsprechenden Handbücher.

Das weitere Vorgehen läßt sich am einfachsten in Form einer „Schritt für Schritt“-Anleitung beschreiben.

Hinweis

Please shut the sherif!

Bitte beseitigen Sie alle Festplattenschutzmechanismen. Einerseits erübrigen sich diese sowieso durch die Verwendung von iTool, andererseits machen sie die Arbeit von iTool kaputt. Bauen Sie also die Schutzkarten aus den Rechnern aus, bzw. deinstallieren sie die Festplattenschutzprogramme befor Sie mit der Erstellung der Images beginnen.

Hinweis

8.2.1 Vorbereitungen im Adminfrontend des Open School Server

Hardwarekonfiguration Wechseln Sie im Adminfrontend des Open School Server nun in das Menü 'Hardwarekonfiguration'.

Vergeben Sie hier eine 'Beschreibung' für die im Client verbaute Hardware. Sie können bei speziellen Rechnern aber z. B. auch deren Namen verwenden.

Bei 'Festplatte' wählen Sie die Anschlußart der im Client eingebauten Festplatte. Normalerweise verfügen ältere Clients über „ATA"-Festplatten und neuere über „SATA"-Festplatten. „SCSI"-Festplatten sind eher selten - oft bei Servern anzutreffen.

Die Festplatte wird in 3 Partitionen aufgeteilt: Systempartition, Swappartition und Cachepartition. Im Systempartition wird das Betriebsystem des Clients installiert. Die Swappartition wird von Linux benutzt. In der Cachepartition werden die Systemimages gespeichert.

Die 'Größe der Systempartition' sollten Sie mit bedacht wählen: Sie muss so groß sein, dass alle Softwarekonfigurationen, die auf die betroffene Hardware installiert werden sollen, einzeln in diese Partition passen. Es ist durchaus möglich auf einem Client zwischen verschiedenen Softwarekonfigurationen umzuschalten.

Möchten Sie z. B. auf den Clients wahlweise eine 10 GB große WinXP eine 8 GB große openSUSE und eine 5 GB Win2000 Systeminstallation starten, dann müssen Sie hier 10 GB angeben. Weiterhin müssen Sie beachten, dass die Festplatte selbst so groß sein muss, dass die Swappartition und alle 3 Images darauf Platz bekommen.

Die 'Größe der Linux-Swappartition' sollte die Größe des Hauptspeichers der Clients entsprechen.

Bei 'Monitor' stellen Sie die Auflösung und Bildschirmwiederholfrequenz ein, mit welcher der Client später den angeschlossenen Monitor ansteuern soll. Beachten Sie bitte, dass zu hohe Werte ältere Monitore zerstören können!

Der Bereich 'Garantie' kann bleiben wie er ist - wenn Sie die Hardware-Datenbank des Open School Servers auch für die Inventur nutzen möchten, geben Sie hier den Ablauf der Garantiezeit ein.

Unter 'Weitere Angaben' können Sie beliebige weitere Informationen über den Client sammeln. z. B. der Lieferant, Servicehotline uva. Beachten Sie bitte, dass der Schlüsselname keinen Leerzeichen erhalten darf.

Wenn Sie alle Daten eingegeben haben, drücken Sie bitte auf 'Eintragen' und die Daten zu speichern.

Softwarekonfiguration Im Menü 'Sofwarekonfiguration' legen Sie eine Beschreibung für ein Softwarepaket an, welches später auf den Clients installiert werden soll.

Geben Sie unter 'Beschreibung' einen aussagekräftigen Namen für die Software an.

Unter 'ProductID' können Sie die Registrierungsschlüssel hinterlegen, die für einige Betriebssysteme benötigt werden.

Die Angabe des 'OS' (Betriebssystems) ist für einige weitere Stellen in der Konfiguration des Open School Server wichtig.

Images definieren Der vorläufige Abschluss der Vorarbeiten am Open School Server ist die Konfiguration vom Systemimages. Wählen Sie dazu den Menüpunkt 'Systemimages'.

Hier Konfigurieren Sie mit 'Neu' ein neues Image bestehend aus einer vorhandenen Hardware- und Softwarekonfiguration. Zunächst können Sie nur eine Software- und eine Hardwarekonfiguration aus den jeweiligen Drop-Down-Menüs auswählen. Später können Sie auch hier für jedes „Systemimage" weitere Angaben machen.

Wenn Sie ein Image „Read-Only" setzen kann diese nicht geändert werden.

Räume definieren Legen Sie nun im Menü 'Räume' einen neuen Schulraum an. Dies geschieht, indem Sie im Textfeld 'Neuer Schulraum' einen maximal 9 Zeichen langen Namen für den Schulraum eingeben und die im Raum standardmäßig verwendete Softwarekonfiguration auswählen. Klicken Sie anschließend 'Eintragen'

Rechner registrieren Starten Sie hierfür den Client und überprüfen Sie, ob er eine IP-Adresse vom Open School Server bekommt. Sollte der Client noch über kein Betriebssystem verfügen, notieren Sie sich bitte die „MAC-Adresse" der Netzwerkkarte. Diese wird im allgemeinen als zwölf stellige, hexadezimale Zahl während des Bootvorgangs darstellt. Die Darstellung fällt dabei leider unterschiedlich aus - ein Beispiel wäre „08-00-20-ae-fd-7e" oder auch „08:00:20:ae:fd:7e".

Beim registrieren eines Rechners müssen Sie diesem eine Hardwarekonfiguration zuweisen. Weiterhin können Sie angeben, ob der registrierte Client ein Masterrechner seiner Hardwarekonfiguration ist.

Normalerweise bekommen die Rechner die Softwarekonfiguration des Raumes zugewiesen. Möchten Sie jedoch bestimmten Rechner eine ebweichende Softwarekonfiguration (z. B. Lehrerrechner) zuteilen, können Sie das an dieser stelle machen.

Das weitere Vorgehen zur Registrierung entnehmen Sie bitte dem Kapitel *Rechnerverwaltung* auf Seite 76 - geben Sie hier die notierte MAC-Adresse für den am Open School Server zu registrierenden Client ein.

8.2.2 Client vorbereiten

Installieren Sie wie gewohnt das Betriebssystem auf der Festplatte des Clients. Wählen Sie bei Windows Systemen als „Zieldateisystem“ FAT32 (hierfür darf die Partitionsgröße 32 GB nicht überschreiten).

Achtung

FAT32

Das Imaging-Tool des Open School Servers kann derzeit leider nur Partitionen, welche mit „FAT32“ oder „FAT16“ partitioniert sind, sichern. Diese FAT-Partitionen können beim Zurückspielen eines Images bei Bedarf automatisch in „NTFS“-Partitionen umgewandelt werden.

Die Erstellung eines Images muss aber immer auf einer FAT-Partition erfolgen!

Achtung

Richten Sie anschließend den Client ein: installieren Sie die benötigte Software und nehmen Sie ggf. weitere Einstellungen im System vor. Hier unterliegen Sie keinen Beschränkungen.

Wenn Sie den Rechner fertig konfiguriert und ggf. wie unter **??** auf Seite ?? in die Domäne des Open School Servers aufgenommen haben, müssen Sie vor dem Erstellen des Images noch das Tool sysprep ausführen. Dieses befindet sich auf der Windows-CD im Ordner `\SUPPORT\TOOLS\` in der Datei `DEPLOY.CAB`, welche Sie mit den Windows-Bordmitteln installieren können.

Tipp

Das Programm sysprep dient dazu einen komplett installierten PC so vorzubereiten, dass man ein von diesem erstelltes Image anschließend auf andere Computer übertragen kann.

Tipp

Das Programm sysprep läßt sich über eine Konfigurationsdatei namens `sysprep.inf` steuern. Damit dies später auf den geklonten Clients problemlos funktioniert, muss in dieser Datei unter Umständen noch eine Anpassung vorgenommen werden: Im Abschnitt ‘[Unattended]’ sollte der Eintrag `InstallFilesPath` den Wert `C:\sysprep\i386` aufweisen. Bitte kontrollieren Sie dies, indem Sie die Datei mit einem beliebigen Editor wie z. B. dem Programm Notepad.exe öffnen.

Je nach Windows-Version muss anschließend das Programm sysprep mit bestimmten Parametern auf einer Kommandozeile gestartet werden.

Windows 2000 Starten Sie sysprep.exe ohne Parameter. Windows 2000 enthält leider einen Fehler, der unter Umständen verhindert, dass der Computer nach dem

ausführen von sysprep.exe und dem danach erforderlichen Reboot nicht von selbst wieder neu startet. Sollte dies der Fall sein starten Sie den Computer nach ca. 5 Minuten selber neu.

Windows XP Starten Sie sysprep.exe mit den folgenden Parametern:

```
sysprep.exe -pnp -mini -reboot -quiet -reseal -activated
```

Hier noch ein kurzer Überblick über einige mögliche Optionen:

–activated Das System wird als „bereits bei Microsoft registriert“ geführt. Eine erneute Aktivierung ist nicht notwendig.

–quiet Unterdrückt Bestätigungsdialogfelder, die normalerweise auf dem Bildschirm angezeigt werden.

–reboot Startet den Computer am Ende automatisch neu.

–pnp Dieser Parameter erzwingt eine erneute Ausführung der vollständigen PnP-Hardware-Erkennung.

–mini Konfiguriert den PC so, dass beim Reboot anstelle der Windows-Willkommensseite die Miniinstallation verwendet wird.

–reseal Löscht die Protokolle der Ereignisanzeige und bereitet den Computer für das Imaging vor. Beim nächsten Start wird die Windows-Willkommensseite bzw. die Miniinstallation gestartet.

–nosidgen Führt Sysprep aus, ohne neue SIDs zu generieren.

Nachdem das Programm sysprep seine Routinen abgearbeitet hat startet der Computer neu und ist bereit für das Erstellen eines Images.

8.2.3 Image erstellen

Booten Sie den Client über PXE, erscheint zunächst ein Bootmenü, in welchem Sie drei verschiedene Auswahlmöglichkeiten haben: ‘Festplatte’, ‘iTool’ und ‘Autoinstallation Linux’.

Wählen Sie hier mit den Pfeiltasten der Tastatur den Menüpunkt ‘iTool’ (siehe *Image erstellen* auf der nächsten Seite.

Geben Sie im nun folgenden Dialog Ihren Benutzernamen und anschließend Ihr Passwort ein.

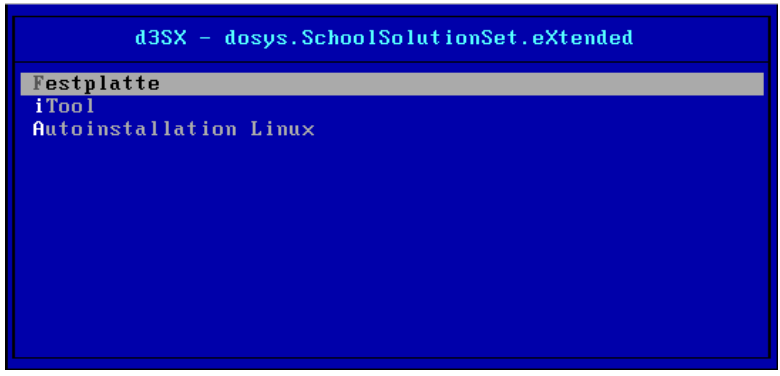

Abbildung 8.1: *Bootmenü-Auswahl mit PXE und iTool*

Hinweis

Imaging-Rechte

Nur Benutzer der Gruppe `sysadmins` - also zunächst nur der Benutzer `admin` - dürfen Images erstellen. Benutzer der Gruppe `Lehrer` (bzw. `teachers`) können nur ein Image wiederherstellen.

Hinweis

Wenn Sie sich korrekt angemeldet haben, erscheint ein Auswahlmenü in welchem Sie zwischen verschiedenen Modi wählen können. Da Sie ein neues Image erstellen möchten, wählen Sie den Punkt 3 'Image erstellen' (siehe *Image erstellen* auf der nächsten Seite).

Nun beginnt das Erstellen des Images. Dieses wird auf dem Open School Server später unterhalb des Verzeichnisses `/srv/itool/images` abgelegt. Dieser Prozess kann je nach Größe der zu sichernden Partition und der enthaltenen Daten einige Zeit dauern.

Abbildung 8.2: *iTool-Auswahlmenü*

Autoinstallation und Booten über Netzwerk

Oftmals erhalten Schulen kostenlos ältere Hardware von Firmen oder die Schule selbst verfügt über ausgemusterte Rechner, die in einem Kellerraum ungenutzt Platz wegnehmen.

Der Open School Server bietet Ihnen nun die Möglichkeit, diese ältere Hardware wieder gewinnbringend im Schulalltag einzusetzen. Dazu können Sie über die automatische Installation einen leistungsfähigen Terminalserver installieren und die ausgemusterten Rechner als ThinClients benutzen.

Während der Installation des Open School Servers wird für diese Zwecke automatisch ein Installationsserver für die Installation der aktuellen Version von SUSE LINUX konfiguriert. Weiterhin wird ein TFTP-Server eingerichtet, um das Booten über Netzwerk mit PXE-Protokoll zu ermöglichen.

Mit diesen beiden Werkzeugen sind Sie so in der Lage, SUSE LINUX völlig automatisch zu installieren. Die automatisch installierten Linux-Clients sind direkt nach der Installation bereit für die Nutzung im Schulalltag. Der Installationsaufwand hält sich also stark in Grenzen und beträgt pro Client ungefähr 30 Minuten - wobei mehrere Installationen parallel ablaufen können und sich die eigentliche Arbeit auf das Einlegen der CD und das Auswählen eines Profils aus einem Menü beschränkt.

Einen Überblick über die Abweichungen im Gegensatz zu einer normalen SUSE LINUX Installation finden sie unter *Die Steuerdateien für einzelne Clients anpassen* auf Seite 155.

9.1 Vorbereitungen zur Installation

Das Rootverzeichnis des TFTP-Servers ist `/srv/tftp`. Unterhalb dieses Verzeichnisses müssen sich einige Dateien befinden, die nachträglich von der ersten CD oder DVD der aktuellen SUSE LINUX Distribution kopiert werden müssen. Bei der Beschreibung der Befehle gehen wir davon aus, dass eine DVD unter dem Pfad `/media/dvd` in das Filesystem eingebunden wird:

`linux` Der zu ladende Linux-Kernel. Er muss von der aktuellen SUSE LINUX-DVD kopiert werden:
`cp /media/dvd/boot/i386/loader/linux /srv/tftp/`

`initrd` Das zu startende Filesystem. Es muss von der aktuellen SUSE LINUX-DVD kopiert werden:
`cp /media/dvd/boot/i386/loader/initrd /srv/tftp/`

`/srv/tftp/menu.lst` Diese Datei beinhaltet das deutschsprachige Bootmenü und ist schon auf dem System vorhanden.

`pxegrub` PXE-Bootimage für den Bootloader Grub - diese Datei sollten Sie nicht verändern!

`pxes` In diesem Verzeichnis befinden sich spezielle Kernel– und Filesystem–Images zum Starten von Linux X-Terminals. Auch hier müssen Sie nichts mehr anpassen.

Die Hauptvorbereitung besteht darin, die CDs oder die DVDs der aktuellen SUSE LINUX Distribution mit folgenden Befehlen in die Verzeichnisse unterhalb von `/srv/tftp/akt/CD1...CD5` kopiert werden (wir gehen hier wieder von der DVD aus, diese muss nur in den Ordner `/srv/tftp/akt/CD1` kopiert werden und wird später als CD1 angesprochen):

```
mount /media/dvd
cd /media/dvd
cp –va . /srv/tftp/akt/CD1
umount /media/dvd
```

Diese Befehle müssen ggf. für alle CDs oder DVDs wiederholt werden. Vergessen Sie bei den CDs bitte nicht, die CD-Nummer zu wechseln.

Startet man einen Rechner mit PXE-Netzwerkboot-Karte oder über die Netzwerk-Boot-CD (siehe Abschnitt *Netzwerk-Boot-CD erstellen* auf der nächsten Seite, erhält man ein Bootmenü mit folgenden Optionen:

Festplatte Das auf der Festplatte des Clients installierte Betriebssystem wird gestartet. So wird verhindert, dass fälschlicherweise eine Installation begonnen wird,

falls Sie einmal eine Boot-CD im Laufwerk vergessen oder das BIOS noch nicht umgestellt haben.

Starte Linux X-Terminal Ein Diskless Linux X-Terminal wird gestartet. Als X-Server wird der `terminalserver` benutzt, welcher vorher installiert sein sollte.

Linux Autoinstallation Die automatische Installation einer SUSE LINUX Workstation wird gestartet.

Linux Autoinstallation mit Windows Partitionen Die Festplatte wird so aufgeteilt, dass Sie nach der automatischen Installation von SUSE LINUX zusätzlich Windows installieren können.

Linux manuelle Installation Es startet die normale Installation einer SUSE LINUX Workstation, wie Sie sie auch aus dem SUSE LINUX-Handbüchern kennen.

Linux ThinClient Autoinstallation Die automatische Installation eines ThinClients wird gestartet. Dieser benötigt zum Betrieb später den Terminalserver - nutzt aber zusätzlich die eingebaute Festplatte.

Terminalserver Autoinstallation Es wird ein Terminalserver installiert. Diese Installation dauert ca. 1 bis 2 Stunden - danach kann der Terminalserver aber sofort benutzt werden.

Hinweis

Direkt nach den Vorbereitungen auf dem Open School Server müssen Sie also nur noch die Clients über PXE-Boot oder mittels der mitgelieferten Boot-CD starten und aus dem Bootmenü den passenden Eintrag für jeden Client auswählen. Nach einer mehr oder weniger ausgiebigen Kaffepause können Sie dann nach einem Neustart die Clients im Schulnetz ohne weitere Arbeiten in Betrieb nehmen.

Hinweis

Wenn Sie schon über Netzwerkkarten mit PXE-Boot-ROM verfügen, brauchen Sie normalerweise die Rechner nur über die Netzwerkkarte zu booten. Dies wird im BIOS des jeweiligen Rechners eingestellt.

9.1.1 Netzwerk-Boot-CD erstellen

Wenn Sie über Hardware ohne PXE-Boot-ROM verfügen, können Sie sich eine bootfähige CD erstellen, die nach dem Bootvorgang automatisch eine Verbindung zum Server aufbaut und Ihnen das Auswahlmenü anbietet.

Das entsprechende ISO-Image finden Sie unter der URL `http://admin/bootcd.iso` auf dem Open School Server.

Laden Sie das Image auf einen PC mit eingebautem CD-Brenner herunter und starten Sie ein Brennprogramm. Alle heute auf dem Markt befindlichen CD-Brennprogramme können das ISO-Image problemlos auf eine CD brennen. Nutzen Sie hierfür die Option 'CD-Image brennen' im jeweiligen Programm und wählen dann die ISO-Datei aus. Mit der erzeugten Boot-CD können Sie nun einen PC booten. Ändern Sie dafür ggf. die Bootreihenfolge im BIOS des Rechners auf 'CD'.

9.2 Detaillierte Erklärungen und Anpassungen zur Autoinstallation

Normalerweise sind keine weiteren Anpassungen oder Ergänzungen für die Automatische Installation nötig. Sie können aber Anpassungen vornehmen, um die Clients noch besser an Ihre persönlichen Befürfnisse anzupassen. Bitte erstellen Sie aber vor Änderungen an der Konfiguration in jedem Fall Sicherheitskopien der zu ändernden Dateien!

9.2.1 Die Steuerdateien für einzelne Clients anpassen

Für die Steuerung der Installation der einzelnen Client-Profile (Linux-Client, Linux-Client mit Windows-Partition, Terminalserver, etc.) werden XML-Dateien genutzt. Diese ermöglichen später die Installation und Konfiguration der Clients ohne eine einzige Nutzerinteraktion.

Die XML-Dateien befinden sich im Verzeichnis `/srv/tftp/xml` und heißen `std+win.xml`, `std.xml`, `thin_client.xml` und `terminalserver.xml`.

Diese XML-Dateien werden auch Kontrolldateien genannt und sind für die Steuerung des gesammten Installationsprozesses (siehe Abbildung *Die Steuerdateien für einzelne Clients anpassen* auf der nächsten Seite) verantwortlich. Sie als Administrator müssen sich also nur noch um die Vorab-Konfiguration und das Erzeugen der Profildatei kümmern. Die restliche Installation - von der Partitionierung der Festplatte über die Konfiguration der Hardware und das Einrichten der System und Netzwerkprofile - wird danach von YaST2 automatisch erledigt.

Sie können diese Dateien bei Bedarf mit einem XML-Editor wie z. B. dem kxmleditor von KDE oder mit dem YaST2-Modul `Automatische Installation` (siehe Abbildung *Die Steuerdateien für einzelne Clients anpassen* auf Seite 156) unter 'YaST2' →

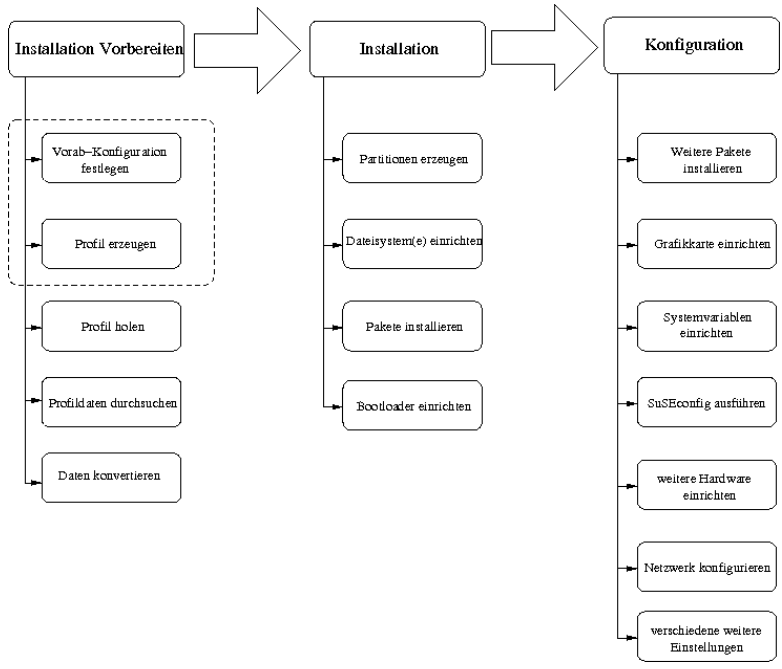

Abbildung 9.1: *Schema des Autoinstallationsprozesses*

'Verschiedenes' bearbeiten. Wenn Sie das YaST2-Modul für die automatische Installation verwenden, können Sie die Dateien als symbolische Links auch im Verzeichnis `/var/lib/autoinstall/repository/` öffnen und bearbeiten.

Tipp

Weitere Informationen zu AutoYaST2 finden Sie auf der Installations-CD vom Open School Server im Verzeichnis `docu` bzw unter `/usr/share/doc/packages/autoyast2/html/` oder im Internet unter der URL `http://www.suse.de/~nashif/autoinstall/`.

Tipp

Achtung

Beachten Sie bitte, dass bei *allen* automatischen Installationen die bisherigen Daten und Partitionen auf den Festplatten der Clients gelöscht werden!

Achtung

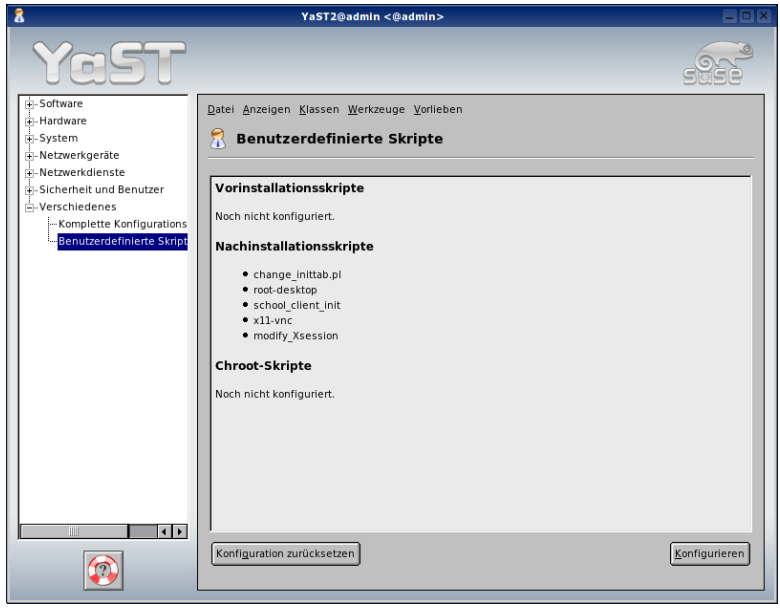

Abbildung 9.2: *Das YaST2-Modul für die automatische Installation*

Die Konfiguration der über die Autoinstallation eingerichteten Clients unterscheidet sich von einer normalen Installation in folgenden Punkten:

- Für den Benutzer `root` wird auf allen Systemen das bei der Installation des Open School Servers eingetragene Administratorpasswort gesetzt und eine passwortfreie ssh-Verbindung für den Benutzer `root` eingerichtet.
- Die Textkonsolen, welche Sie an einem normal eingerichteten Client über die Tastenkombinationen (Strg) (Alt) und (F1) bis (F6) erreichen können, sind deaktiviert.
- Eine speziell eingerichtete Firewall wird aktiviert, die nur noch dem Open School Server direkten Zugriff auf die Clients gewährt.
- Über ein spezielles Skript werden Workstation-Accounts nur an den entsprechenden Workstations akzeptiert und Schüler, welche sich an einem Lehrer-PC anmelden wollen, abgewiesen.
- An den Clients wird ein VNCServer eingerichtet. So kann ein Lehrer später vom Lehrer-PC aus die Bildschirme der Schüler-PCs einsehen und bei Bedarf auch die Kontrolle übernehmen.

- Die Clients werden so konfiguriert, dass Sie während des Bootens automatisch im Verzeichnis `/var/SuSE/update` des Open School Servers nach evtl. vorhandenen Online-Updates suchen. Sind dort Updates vorhanden, werden diese automatisch eingespielt. So bleiben die Clients immer softwaretechnisch auf dem neuesten Stand.
- Sämtliche Werte für die Proxykonfiguration und Anmeldung

All diese Änderungen gegenüber der normalen Installation eines SUSE LINUX-Clients können Sie natürlich auch nachträglich noch an älteren - nicht über die Autoinstallation installierten - Clients vornehmen. Dazu kopieren Sie ggfs. die entsprechenden Dateien von einem über die Autoinstallation eingerichtetem Client in die entsprechenden Verzeichnisse auf den anderen Client. Die Pfad- und genauen Skriptangaben entnehmen Sie bitte den jeweiligen Konfigurationsdateien - Sie finden diese Angaben im `configure`-Abschnitt der jeweiligen Datei. Wir empfehlen jedoch ausdrücklich eine Neuinstallation des betreffenden Clients über die Autoinstallation - so wird garantiert nichts vergessen.

9.2.2 Die Konfigurationsdateien std+win.xml und std.xml

Diese Konfigurationsdateien beeinflussen die automatische Installation einer normalen Workstation. Wie die Dateinamen schon andeuten, wird bei `std+win.xml` ein Rechner mit zusätzlichen Windows-Partitionen installiert; bei `std.xml` wird die gesamte Festplatte für eine Linux Installation vorbereitet.

Bitte beachten Sie, dass für Windows zwei primäre Partitionen eingerichtet werden, so dass Sie auch ältere Windows-Versionen (9x, ME) problemlos dort installieren können. Sie sollten also entweder:

- Vorher mit einem Partitions-Backuptool wie z. B. Partition Image ein Image einer auf dem Client vorhandenen Windows-Installation erstellen und diese auf einem anderen Rechner auslagern. Dann können Sie nach der Autoinstalltion die ersten beiden Partitionen mit einer Windows-Bootdiskette formatieren, für Windows „bootfähig“ machen und dann das Image wieder zurückspielen.
- Windows erst nach der Autoinstallation neu installieren. Richten Sie Windows so ein, wie Sie es möchten und installieren Sie die benötigten Treiber und Software.

Danach müssen Sie mit einer Linux-CD (z. B. der Installations-CD der aktuellen SUSE LINUX) den Rechner booten und über den Menüpunkt ‘Manuelle Installation’ ein Rettungssystem starten, mit welchem Sie den das installierte Linuxsystem starten und von dort aus den Bootloader erneut installieren können.

Nähere Informationen hierzu erhalten Sie in unserer Support-Datenbank. Suchen Sie dazu bitte unter der URL `http://portal.suse.com/PM/page/search.pm?` nach dem Stichwort „Windows“.

Partitionierung: Der gesamte Festplattenbereich wird verwendet und folgendermaßen eingeteilt:
Bei einem Client mit std+win.xml:

	std+win.xml	
Mountpoint	Größe	Dateisystemtyp
	4G	Win95 FAT32
	4G	Win95 FAT32
/boot	30M	Linux
swap	wird automatisch ermittelt	Linux swap
/	Rest	Linux

Bei einem Client mit std.xml:

	std.xml	
Mountpoint	Größe	Dateisystemtyp
/boot	30M	Linux
swap	wird automatisch ermittelt	Linux swap
/	restliche Platte	Linux

Paketauswahl In beiden Installationsvarianten wird die folgende Paketauswahl installiert, welche im Allgemeinen völlig ausreichend sein sollte. Sollten Sie dennoch einzelne Pakete zusätzlich auf den Rechnern installieren wollen, editieren Sie bitte *vor* der Installation der Clients die entsprechende xml-Datei und fügen dort im Abschnitt <packages>den entsprechenden Paketnamen (ohne Versionsnummer) ein. Sie können den hier schon vorhandenen Eintrag für das Paket `syslog-ng` als Vorlage nehmen.

Ausgewählte Paketgruppen:

- default
- Kde
- Kde-Desktop
- Office

Netzwerk Die erste Netzwerkkarte wird als DHCP-Client konfiguriert.

NFS-Client Das Verzeichnis `nfs:/home` vom Open School Server wird mit Standardoptionen nach `/home` gemountet.

LDAP-Client Der Server wird in die LDAP-Authorisierung eingebunden.

Drucken CUPS wird installiert und und so eingerichtet, dass die Clients auf den CUPS-Server mit dem Namen `printserver` lauschen.

Bildschirmauflösung Wenn möglich, wird die 3D-Hardwarebeschleunigung aktiviert. Die Auflösung wird auf 1024x768 bei 75Hz gesetzt.

9.2.3 Die Konfigurationsdatei thin_client.xml

Diese Konfigurationsdatei ist für die Einrichtung von „ThinClients“ zuständig. Diese ThinClients sind selbst nicht mehr in der Lage aktuelle Software schnell genug auszuführen – in Verbindung mit einem Terminalserver, welcher die eigentlichen Berechnungen übernimmt, können Sie aber durchaus bis ans Ende ihrer Tage noch ausreichen. Durch die zusätzliche Verwendung der eigenen Festplatte wird der Terminalserver und das Netzwerk entlastet. Damit können mehr Clients vom Terminalserver bedient werden als bei reinen „Diskless Clients“. Zusätzliche Hardware ist nicht nötig.

Hardwarevoraussetzungen Benötigt werden ältere Clients ab Pentium I mit einer 2 MB Grafikkarte, ca. 32 MB RAM, bootfähiger Netzwerkkarte mit PXE-ROM oder CD-ROM-Laufwerk und einer Festplatte ab 600 MB. Auf der Festplatte wird eine Swap-Partition und ein minimales Betriebssystem zum Starten eines X-Servers eingerichtet, um das Netzwerk im Gegensatz zum reinen Terminalbetrieb zu entlasten.

Partitionierung: Der gesamte Festplattenbereich wird verwendet und folgendermaßen eingeteilt:

Mountpoint	Größe	Dateisystemtyp
`swap`	`wird automatisch ermittelt`	`Linux swap`
/	`max`	`Linux`

Der Bootmanager wird in den MBR geschrieben.

Paketauswahl Basisauswahl: Minimal+X11
Zusätzliche Pakete:

- xdmsc – nützliche Skripte für den Terminalbetrieb.
- nfsserver – damit der Terminalserver auf den Client zugreifen kann.
- mozilla – startet so schneller

Netzwerk Die erste Netzwerkkarte wird als DHCP-Client konfiguriert.

Bildschirmauflösung Wenn möglich, wird die 3D-Hardwarebeschleunigung aktiviert. Die Auflösung wird auf 1024x768 bei 75Hz gesetzt.

sysconfig xdmsc Als Terminalserver wird standardmäßig der DNS-Name `terminalserver` verwendet.

Hinweis

Die ThinClients sollten auch registriert werden. Bitte vergessen Sie dabei nicht, dass das Registrierungstool die Hardwareadresse (MAC-Adresse) der ThinClients nicht ermitteln kann, da aus Sicht des Open School Server nur der Terminalserver arbeitet. Deshalb müssen Sie hier die Hardwareadresse leider per Hand eintragen. Sie können sie ermitteln, indem Sie mit (Alt) (Strg) (F1) auf die Konsole des ThinClients wechseln, sich als `root` einloggen und den Befehl `ip link show eth0` ausführen.

Hinweis

9.2.4 Die Konfigurationsdatei terminalserver.xml

Hier wird die Einrichtung eines Terminalservers konfiguriert. Dieser Rechner stellt später seine gesammte Kapazität den an ihn angeschlossenen Clients zur Verfügung. Die Clients können sämtliche auf dem Server installierte Software nutzen und auch die CD/DVD- und Diskettenlaufwerke sowie zusätzlich am Server angeschlossene Hardware. Beachten Sie bei der Auswahl von Prozessor(en) und RAM das der Terminalserver seine Ressourcen unter den Clients aufteilen muss. Glücklicherweise haben Sie mit SUSE LINUX ein Produkt erworben, welches hervorragend auf unterschiedlichster Hardware skaliert.

Hardwarevoraussetzungen Dieser Rechner sollte unbedingt der neueren Generation angehören und über genügend RAM verfügen (für jeden Client ca. 64 MB + 128 MB für das Serversystem). Da eine Anwendung wie z. B. OpenOffice - wenn Sie mehrfach aufgerufen wird - durch geschicktes Speichermanagement des Kernels nicht jedesmal wieder komplett in den Speicher geladen werden muss, haben Sie bei dieser Rechnung durchaus noch Reserven im Schulalltag.

Partitionierung: Der gesamte Festplattenbereich wird verwendet und wie folgt eingeteilt:

Mountpoint	Größe	Dateisystemtyp
`/boot`	`30M`	`Linux`
`swap`	`wird automatisch ermittelt`	`Linux swap`
`/`	`max`	`Linux`

Der Bootmanager wird in den MBR geschrieben.

Paketauswahl Im Gegensatz zu den normalen Clients wird hier eine große Auswahl an Softwarepaketen installiert, damit jeder Client bei Bedarf seine eigene Arbeitsumgebung bekommen kann. Die Installation des Terminalservers dauert aus diesem Grund aber auch sehr lange. Bei einem 100MB-Netzwerk können Sie ca. 1h veranschlagen.

Ausgewählte Paketgruppen:

- default
- Basis-Devel
- Basis-Sound
- Kde-Desktop
- Kde-Devel
- Kde
- LAMP
- Network
- Office
- SuSE-Documentation
- Tcl-Development
- X11

Zusätzliche Pakete:

- a2ps
- cvs
- emacs
- emacs-x11
- gv
- html2txt
- mozilla
- mutt
- phpMyAdmin

Network Die erste Netzwerkkarte wird als DHCP-Client konfiguriert. Sie müssen nach der Installation den Terminalserver unbedingt als Client im Open School Server registrieren, wie unter 6.2.3 auf Seite 76 beschrieben. Bitte merken Sie sich die vergebene IP-Adresse. Sie werden sie später noch brauchen.

Zusätzlich müssen Sie den Namen `terminalserver` auch im DNS-Server eintragen, da die automatisch installierten ThinClients einen Rechner mit dem DNS-Namen `terminalserver` kontaktieren werden. Dazu müssen Sie, wie im Abschnitt 6.2.3 auf Seite 81 beschrieben, die neue (während der Registrierung erhaltene) IP-Adresse unter dem Menüpunkt 'DNS: Host anlegen' eintragen. [1]

NFS-Client Das Verzeichnis `nfs:/home` vom Open School Server wird mit Standardoptionen nach `/home` gemountet.

LDAP-Client Der Server wird in die LDAP-Authorisierung eingebunden.

Drucken CUPS wird installiert und und so eingerichtet, dass die Clients auf den CUPS-Server mit dem Namen `printserver` lauschen.

Bildschirmauflösung Wenn möglich, wird die 3D-Hardwarebeschleunigung aktiviert. Die Auflösung wird auf 1024x768 bei 75Hz gesetzt.

Tipp

Mehrere Terminalserver

Sie können auch mehrere Terminalserver (z. B. einen Terminalserver pro Klassenraum) installieren. Dazu führen Sie bitte pro Terminalserver folgende Schritte aus:

- Installieren und registrieren Sie einen Terminalserver, nehmen Sie jedoch seine IP-Adresse nicht als `terminalserver` in den DNS auf.
- Tragen Sie den Namen des registrierten Terminalservers in die Autoinstallationskonfigurationsdatei der ThinClients `/var/SuSE/thin\_client.xml` anstelle von `terminalserver` ein.
- Jetzt können Sie die gewünschte Anzahl von ThinClients installieren, und registrieren.

  Bitte beachten Sie dabei, dass die jetzt installierten ThinClients alle den zuletzt installierten Terminalserver kontaktieren.

Tipp

[1] Der neue Eintrag wird nicht sofort in die Konfigurationsdateien übernommen. Um die Konfigurationsdateien zu schreiben, wählen Sie 'Virt. Domaenen' → 'Exportieren'.

9.2.5 Linux X-Terminal

Wenn Sie die Boot-CD in einen Client einlegen und den Eintrag 'Linux X-Terminal' anwählen, wird, nachdem der Kernel geladen und die Netzwerkkarte konfiguriert wurde, eine Verbindung zu einem vorher installierten Terminalserver aufgebaut und ein grafischer Anmeldebildschirm gestartet, über welchen Sie - genau wie bei den ThinClients oder über PXE-Boot - auf dem Terminalserver arbeiten können.

Da bei dieser Startoption die auf den Clients evtl. vorhandene Festplatte nicht genutzt wird, können Sie so einen Client kurzfristig mit Linux booten. Dies eröffnet vielfältige Möglichkeiten - etwa ein rudimentäres Sichern von Windows-Clients über die Boot-CD und einen `tar`- oder `rsync`-Befehl oder die Demonstration von Linux...

Vergessen Sie aber bitte nicht, im BIOS des entsprechenden Clients die Bootreihenfolge wieder so zu ändern, das nicht von CD gebootet werden kann. Ansonsten wären alle weiteren Sicherheitsvorkehrungen am Cient nutzlos.

9.3 Der Open School Server als YOU-Server

Da die Entwickler nicht wissen können, welche LINUX Version auf den Clients installiert ist, hält der Open School Server nach einer Default-Installation noch keine Updates für die Clients bereit. Damit dies nicht so bleibt und die Aktualisierung der Clients zukünftig automatisch abläuft ohne das der Administrator sich noch weiter darum kümmern muss, sind noch zwei Schritte auf dem Open School Server notwenig:

- Der Open School Server muss das Update-Verzeichnis lokal bereitstellen, d.h. er spiegelt dieses Verzeichnis von einem öffentlichen FTP-Server. Dieser Vorgang wird über einen Cron-Job automatisch erfolgen.
- Damit die Clients wissen, ob Sie ein Update durchführen müssen, ist noch ein zusätzlicher Eintrag im LDAP-Server notwendig – auch das läßt sich über einen Cron-Job automatisieren.

Das Vorgehen ist dabei eigentlich recht einfach, weil an den Clients selbst nichts mehr eingestellt werden muss:

- Suchen Sie sich zunächst einen Mirror-Server in ihrer Nähe, welcher YOU-Updates für die auf ihren Clients installierte SUSE LINUX Version anbietet.
- Prüfen Sie, ob das benötigte Verzeichnis über `rsync` (dies schont die Bandbreite und sollte nach Möglichkeit bevorzugt werden) oder nur über `wget` (funktioniert eigentlich immer) gespiegelt werden kann. Beide Optionen sind auf dem Open School Server möglich.

- Wenn der Test erfolgreich verlaufen ist, können Sie den entsprechenden Aufruf als Cronjob automatisch ablaufen lassen.

Anhand des Servers der TU München demonstrieren wir nun das genaue Vorgehen. Dieser Server bietet auch einen rsync-Server an. Zunächst prüfen Sie, ob der Server auch wirklich die benötigten Verzeichnisse über rsync bereitstellt:
`rsync rsync://ftp.leo.org`

Dieser Befehl liefert bei erfolgreicher Ausführung eine Liste mit den zur Verfügung gestellten Software-Archiven. Um nun den genauen Pfad für das benötigte Update herauszufinden, melden Sie sich über FTP am Server an oder nutzen im Falle der TU München einfach die URL `http://archiv.leo.org/`.

Navigieren Sie mit den Befehlen `cd <verzeichnis>` und `ls <verzeichnis>` in das Verzeichnis, in welchem die Updates für die SUSE LINUX-Version Ihrer Clients liegen - im Falle der 9.2 also z. B. ins Verzeichnis:
`suse/i386/update/9.2`

Testen Sie nun zunächst, ob Sie das Verzeichnis über rsync spiegeln können. Mit dem Befehl: `rsync -navz rsync://ftp.leo.org/suse/i386/update/9.2 /tmp` wird nur ein Testlauf durchgeführt - die Übertragung passiert noch nicht wirklich.

Um Platz zu sparen, brauchen Sie keine Source-RPMs herunterladen - diese werden normalerweise an den Clients nicht installiert. Dies wird durch die Option `-exclude=*.src.rpm` erreicht.

Erstellen Sie anschließend das Verzeichnis, welches später die Update-Pakete enthalten wird, mit dem Befehl: `mkdir -p /srv/tftp/update/i386/update/9.2` – dieses Verzeichnis ist sowohl über NFS also auch über FTP von den Clients aus erreichbar.

Spiegeln Sie anschließend die entsprechenden Verzeichnisse und Dateien vom entfernten Server in das soeben erstellte Verzeichnis:

```
rsync -az -stats -delete -exclude=*.src.rpm
rsync://ftp.leo.org/suse/i386/update/9.2/
/srv/tftp/update 1»/var/log/rsync92.log
```

Durch die Option `-stats` erhalten Sie am Ende der Übertragung noch ein wenig zusätzliche Information und durch die Option `-delete` werden auf dem Mirror-Server nicht mehr vorhandene Patches auch lokal gelöscht. Die normale Ausgabe dieses Befehls wird mit der Option `1»/var/log/rsync92.log` in die Datei `rsync92.log` im Verzeichnis `/var/log` umgeleitet. So können Sie auch später noch genau nachvollziehen, was wann vom entfernten Server übertragen wurde.

Nach der ersten erfolgreichen Synchronisation erstellen Sie noch ein Eintrag in der „Crontab“, damit der Datenaustausch zukünftig automatisch und ohne weitere Nutzereingriffe abläuft. Rufen Sie dazu mit dem Befehl: `crontab -e` einen Editor auf und tragen dort die folgende, eine Zeile ein:

```
0 2 * * 4 /usr/bin/rsync -az --stats --delete
          --exclude=*.src.rpm
          rsync://ftp.leo.org/suse/i386/update/9.2/
          /srv/tftp/update
          1>>/var/log/rsync92.log
```

Datei 10: *Beispiel für einen Cron-Eintrag*

Damit wird jeden Donnerstag um 02:00 Uhr nachts der Abgleich durchgeführt. Sollte ein Fehler auftreten, werden Sie per Email informiert.

Teil III

Anhang

Das automatische Backup

Der Open School Server kann automatisch sowohl inkrementelle als auch Vollbackups der wichtigsten Dateien erstellen. So kann der Server bei einem Hardwaredefekt schnell wieder ersetzt werden, ohne dass wichtige Daten verloren gehen.

In diesem Kapitel erfahren Sie, wie das Backup des Open School Servers abläuft und wie Sie es über Variablen beeinflussen können.

A.1 Gedanken zum Thema Datensicherung

Spätestens nach dem ersten unbeabsichtigtem Löschen oder Überschreiben von Dateien, dem ersten Festplattencrash oder anderen Hardware-Schäden, nach einem Diebstahl, etc. wird der Sinn und Zweck einer Datensicherung klar. Für einen Administrator gehört das Erstellen von „Backups“ damit zum Alltag.

Noch vor dem Erstellen eines Backups sollte allerdings klar sein, WAS WIE und WARUM mit WELCHEM Aufwand gesichert werden soll. Denn es gibt verschiedene Arten der Datensicherung und unterschiedliche Motivationen dieses zu tun.

Generell unterscheidet man zwischen differenzieller, inkrementeller und vollständiger Datensicherung.

Bei einem differenziellen Backup werden die seit dem letzten vollständigen Backup geänderten Daten vollständig gespeichert.

Bei der inkrementellen Datensicherung werden nur die Daten gesichert, die sich seit der letzten Datensicherung (meist dem letzten inkrementellen Backup) verändert haben.

Eine vollständige Datensicherung bezeichnet die Sicherung aller Daten unabhängig vom Datum ihrer letzten Sicherung.

Hinweis

Ein Backup-Medium gehört an einen anderen Ort wie die Originaldaten!

Bei einem Brand, einem Wasserschaden, etc. oder einem Diebstahl könnte ansonsten auch das beste Backup zusammen mit den Originaldaten zerstört werden bzw. verloren gehen. Aus diesem Grund ermöglichen RAID-Systeme auch kein Backup. Mit einem RAID-System wird zwar die Ausfallsicherheit eines Systems erhöht - aber vor den oben erwähnten Gefahren kann ein RAID-System nicht schützen.

Hinweis

Der Open School Server ist soweit vorkonfiguriert, dass er Ihnen ein automatisches Backup sämtlicher wichtigen Daten auf anderen, über USB oder Firewire angeschlossenen Datenträgern (kein Bandlaufwerk) oder einen anderen PC anbieten kann.

Bedenken Sie bitte, dass Sie bei der Verwendung eines anderen PCs auch für dessen Absicherung sorgen müssen. Wir empfehlen ihnen die Verwendung von mindestens zwei verschiedenen USB–2.0–Festplatten, deren jeweilige Gesamtkapazität mindestens 10 Prozent über der Größe des Homeverzeichnisses liegt. Sie können eine dieser Festplatten dann direkt am Open School Server angeschlossen lassen und alle anderen an einem anderen, sicheren Ort aufbewahren. Wenn Sie die Platten dann z.B. jede Woche austauschen, verlieren Sie maximal die Daten von zwei Wochen.

A.2 Konfiguration des Backups

Die Konfiguration des automatischen Backups erfolgt über die Administrationswebo-berfläche unter 'Hilfsmittel' → 'Globale Konfiguration'.

Zunächst legen Sie mit vier Variablen den Speicherplatz für das Backup fest:

SCHOOL_BACKUP Mögliche Werte: `yes` oder `no`. Soll überhaupt ein Backup durch-geführt werden?

SCHOOL_BACKUP_FULL_DIR Geben Sie hier den Pfad zum Verzeichnis für das vollständige Backup an.

SCHOOL_BACKUP_INC_DIR Unterhalb dieses Verzeichnisses werden die inkre-mentellen Backups abgelegt. Dabei wird jeden Tag ein neues Unterverzeich-nis mit dem aktuellen Datum erzeugt. Für das vollständige und das inkre-mentelle Backup können Sie auch dieselben Verzeichnisse angeben. Der Open School Server legt für jedes inkrementelle Backup ein neues Unterverzeich-nisse mit der genauen Zeit als Namen an. Deshalb könne beide Verzeichnisse (SCHOOL_BACKUP_FULL_DIR und SCHOOL_BACKUP_INC_DIR) identisch sein.

SCHOOL_BACKUP_CHECK_MOUNT Diese Variable sollten Sie insbesondere bei der Verwendung von externen Festplatten auf `yes` setzen. Dann prüft der Open School Server vor dem Backup, ob das Verzeichnis gemountet ist und führt bei einem negativen Ergebnis kein Backup durch. Sollten Sie also einmal vergessen eine Platte anzuschließen, wird auch kein Backup durchgeführt. Das erspart im Fall der Fälle zwar keinen Datenverlust - aber viele Warn-Emails und eine voll-gelaufene `/`-Partition.

Mit vier weiteren Variablen bestimmen Sie dann den Umfang des Backups:

SCHOOL_BACKUP_HOME Mit `yes` aktivieren Sie das Backup für das `/home`-Verzeichnis.

SCHOOL_BACKUP_DB Mit diesem Eintrag können Sie entscheiden, ob die Daten-bank der jeweiligen Groupware gesichert werden soll. Hier werden je nach ver-wendeter Groupware u.a. die Termine, persönlichen Adressbücher und Foren-Nachrichten gespeichert.

SCHOOL_BACKUP_MAIL Mit `yes` werden sämtliche Emails gesichert.

SCHOOL_BACKUP_LDAP Da sämtliche Benutzerdaten des Open School Servers in der LDAP-Datenbank gespeichert werden, sollten Sie hier generell `yes` eintra-gen.

A.3 Backup auf eine externe USB–Festplatte

Melden Sie sich zunächst als `root` am Open School Server an. Schließen Sie nun eine handelsübliche, externe USB–Festplatte (empfohlen: USB 2.0) an einen USB–Port ihres Rechners. Der SUSE Plugger sollte die Festplatte nun erkennen und ihnen anbieten, diese unter einem bestimmten Mountpoint in das Dateisystem einzuhängen (siehe Abbildung *Backup auf eine externe USB–Festplatte* auf dieser Seite).

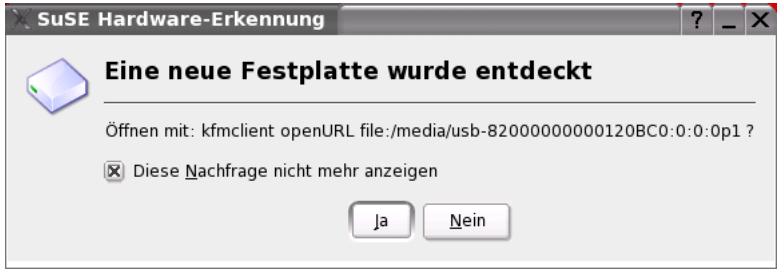

Abbildung A.1: *Meldung des SUSE Plugger beim Einstecken einer USB–Festplatte*

Bestätigen Sie zunächst die Nachfrage und kontrollieren Sie den Inhalt der Festplatte.

A.3.1 Festplatte Formatieren und Partitionieren

Die meisten heute erhältlichen Festplatten sind mit dem `FAT32`- oder `NTFS`-Dateisystem formatiert und bestehen aus einer einzigen, großen Partition. Auf diesen Dateisystemen können nicht alle Linux-Rechte übernommen werden, so dass eine solchermaßen vorbereitete Festplatte erst mit einem anderen Dateisystem formatiert werden muss, bevor sie für ein Backup des Open School Server genutzt werden kann.

Achtung

Durch das Formatieren der USB–Festplatte werden sämtliche Daten auf der entsprechenden Partition gelöscht!

Achtung

Hierzu müssen Sie zunächst die USB–Festplatte aus dem Dateisystem entfernen. Öffnen Sie hierfür eine Konsole und wechseln Sie mit dem Befehl `cd /media` in das Verzeichnis unter welchem die USB–Festplatte mit ihrer Hardware-ID eingehängt ist.

Verschaffen Sie sich einen kurzen Überblick über den Inhalt des `/media`-Verzeichnisses mit dem Befehl `ls`. Geben Sie anschließend den Befehl

`umount /media/usb-` ein und lassen Sie den Open School Server die Hardware-ID vervollständigen, indem Sie die (TAB)-Taste drücken. (Sind auf der USB–Festplatte mehrere Partitionen angelegt, müssen Sie den Vorgang öfter wiederholen - die Partitionen werden am Ende der Hardware-ID dem Verzeichnisnamen hinzugefügt.)

Wenn Sie nun den Befehl `mount` ohne Parameter eingeben, sollte die USB–Festplatte dort nicht mehr aufgeführt werden. Nur so kann der Partitionierer im nächsten Schritt sinnvoll mit der Festplatte arbeiten.

Starten Sie nun YaST2 über die grafische Oberfläche. Wählen Sie 'System' → 'Partitionieren'. Eine Warnmeldung (siehe Abbildung *Festplatte Formatieren und Partitionieren* auf dieser Seite weißt nochmals auf die Gefährlichkeit des Partitionierungs-Tools hin. Bestätigen Sie mit 'Ja', dass Sie sich der Gefahr einer möglichen Datenverlusts bewußt sind.

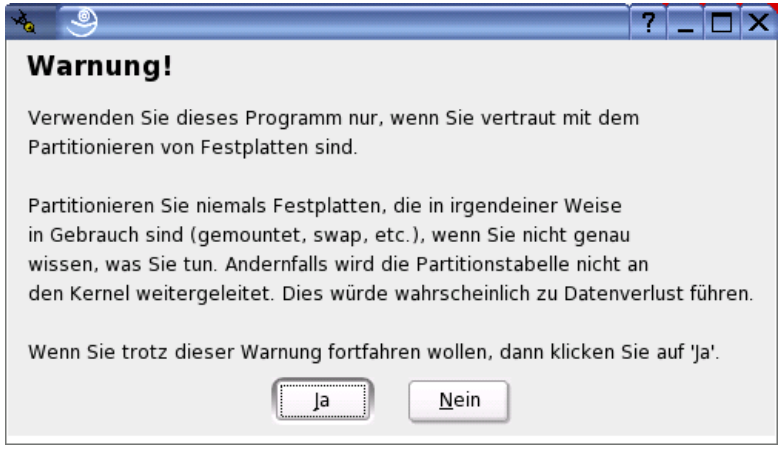

Abbildung A.2: *Warnmeldung des YaST2-Partitionierers*

Den nächsten Dialog kennen Sie schon, wenn Sie während der Installation des Open School Servers eine manuelle Partitionierung vorgenommen haben (siehe Abbildung *Festplatte Formatieren und Partitionieren* auf der nächsten Seite entsprechend gelten die unter *Installation* auf Seite 15 gemachten Anmerkungen auch hier. Im 'Expertenmodus' werden ihnen nun sämtliche Festplatten mitsamt ihren Partitionen angezeigt.

Achtung

Bearbeiten Sie *niemals* ohne Grund die Partitionen für `/`, `swap`, `/var` und `/home`! Auf diesen Partitionen sind sämtliche Daten des Open School Servers gespeichert.

Achtung

Sie können die USB–Festplatte u.a. daran erkennen, dass sie

- Ihr als Mountpoint noch ein Verzeichnis unterhalb von `/media` zugewiesen wird.
- Sie in einem reinen IDE-System als `/dev/sda` (und damit als SCSI-Platte) aufgeführt wird. Wenn Sie schon SCSI-Festplatten im System verwenden, ist die USB–Festplatte meist diejenige, welche als letzte Platte aufgelistet wird.

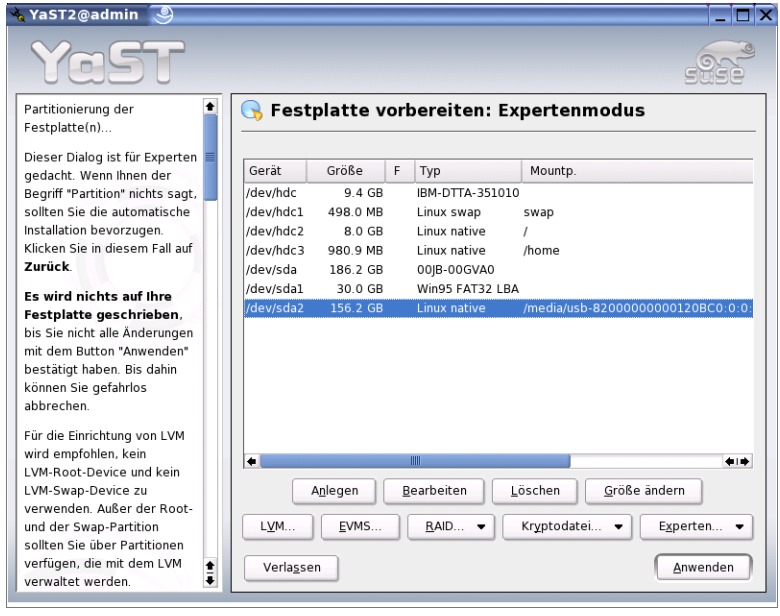

Abbildung A.3: *YaST2-Partitionierer: Übersicht über die Partitionen*

- Markieren Sie nun die Partition der USB–Festplatte, die Sie zukünftig für Backups nutzen wollen und wählen Sie die Option ‘Bearbeiten’.
- Im nächsten Dialog formatieren Sie die bestehende Partition nun mit dem Dateisystem `ext3` (siehe Abbildung A.4 auf der nächsten Seite).
- Wählen Sie nun ‘Fstab-Optionen’ - es öffnet sich ein neuer Dialog (siehe Abbildung A.5 auf Seite 176). Achten Sie darauf, dass die Optionen `Nicht beim Systemstart mounten` und `Listen für Zugriffskontrolle (ACL)` aktiviert ist. Wenn Sie die Festplatte während des laufenden Betriebs an den Server

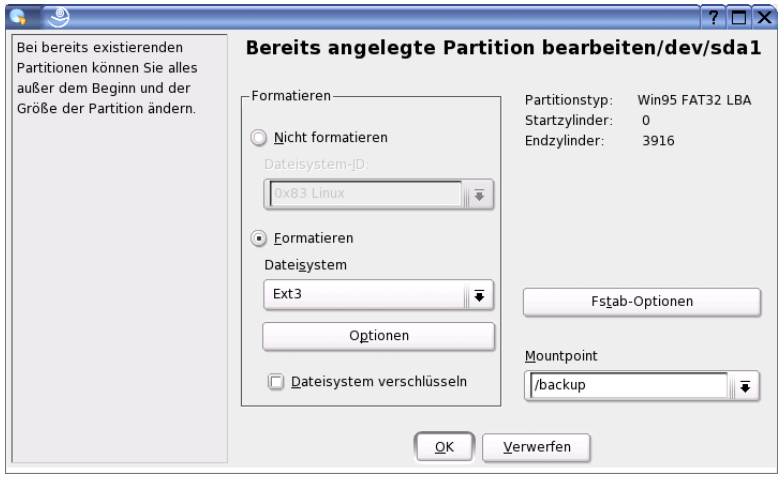

Abbildung A.4: *YaST2-Partitionierer: bereits angelegte Partition bearbeiten*

an- und wieder abstecken (was z. B. bei einer USB–Festplatte der Fall sein sollte), dann achten Sie bitte darauf, dass unter 'Mountpoint' nichts eingetragen wird!

- Nachdem Sie die Dialoge mit `OK` verlassen haben, erhalten Sie noch eine Warnmeldung, die Sie darauf hinweist, dass die Partition zukünftig unter Windows ohne Zusatzprogramme nicht mehr gelesen werden kann (siehe Abbildung A.6 auf Seite 177). Bestätigen Sie hier mit `Ja`.

- Wieder zurück in der Übersicht des Expertenmodus kontrollieren Sie bitte nochmals, ob Sie die richtige Festplatte und Partition gewählt haben. Achten Sie besonders auf die Spalte `F`: ein `F` in dieser Spalte bedeutet, dass die entsprechende Partition neu formatiert wird.

Achtung

Achten Sie bei Wechselmedien darauf, dass bei diesen kein Mountpoint eingetragen ist - ansonsten meldet der Open School Server beim nächsten Bootvorgang einen Fehler, wenn unter diesem Mountpoint kein Gerät existiert.

Achtung

(siehe Abbildung A.7 auf Seite 178).

- Nach einem Klick auf `Anwenden` und der zusätzlichen Bestätigung im nächsten Warnfenster wird die USB–Festplatte nun neu Formatiert und Sie können den

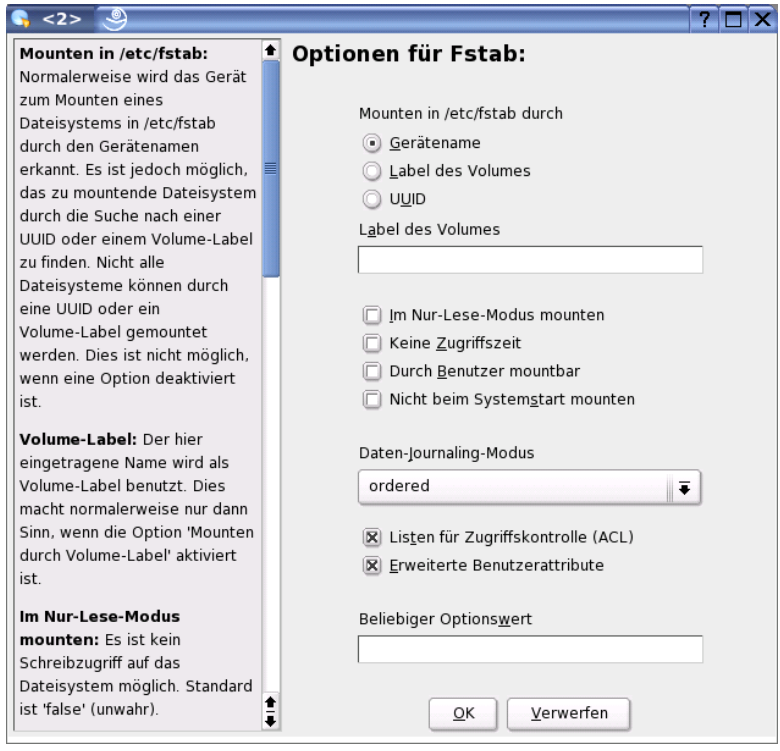

Abbildung A.5: *YaST2-Partitionierer: Fstab-Optionen bearbeiten*

Partitionierer (und YaST2) wieder ‘Verlassen’.

Nachdem Sie nun die Festplatte neu Partitioniert haben, überprüfen Sie nochmals die korrekte Einbindung der Platte, indem Sie den USB–Stecker abziehen und ihn anschließend wieder anstecken. Mit dem Befehl `mount` in einem Konsolenfenster sollte ihnen nun unter `/media` eine mit `ext3` formatierte Festplatte angezeigt werden. Sie können das hier angezeigte Verzeichnis mit der rechten Maustaste markieren. Wenn Sie anschließend im Editor oder über YaST2 → ‘System’ → ‘Editor für /etc/sysconfig-Dateien’ bei der Pfadangabe die mittlere Maustaste drücken, wird die zwischengespeicherte Pfadangabe in das Eingabefeld automatisch eingefügt.

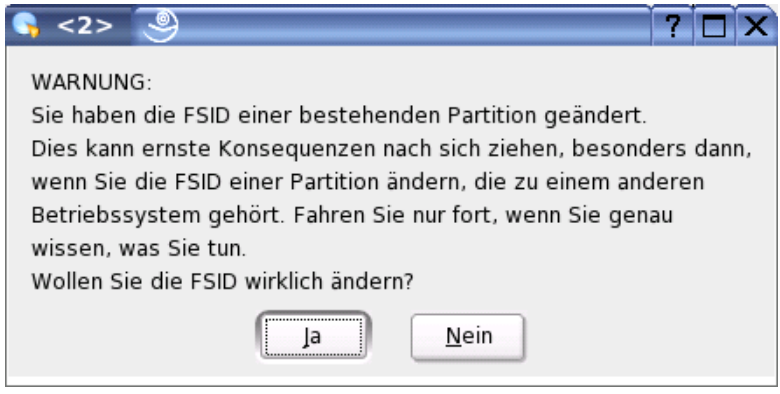

Abbildung A.6: *YaST2-Partitionierer: Warnmeldung aufgrund geänderter FSID*

A.3.2 Backup auf einen entfernten Linux-Rechner

Sie können als Backupziel auch einen anderen Linux-Rechner verwenden, welcher dem Open School Server ein bestimmtes Verzeichnis über NFS zur Verfügung stellt.

Hinweis

Bedenken Sie bei dieser Art von Sicherung, dass dieser „Backup-Rechner“ in seinem Backup-Verzeichnis sämtliche Nutzerdaten (inkl. Passwörter) beherbergt und entsprechend abgesichert werden sollte!

Hinweis

Als Vorbereitung sollten Sie auf dem entfernten Rechner ein bestimmtes Verzeichnis für die Aufnahme des Backups vorbereiten und exportieren (unter SUSE LINUX können Sie hierfür das YaST2-Modul ‘NFS-Server’ verwenden).

Konfigurieren Sie den Open School Server nun über YaST2 → ‘Netzwerkdienste’ → ‘NFS-Client’ als NFS-Client und mounten Sie das entfernte Dateisystem (siehe Abbildung *Backup auf einen entfernten Linux-Rechner* auf Seite 179.

Bitte beachten Sie hierbei, dass der Open School Server nun bei jedem Start versuchen wird, dass entfernte Dateisystem zu mounten. Entsprechend sollte der Backup-Rechner immer zur Verfügung stehen.

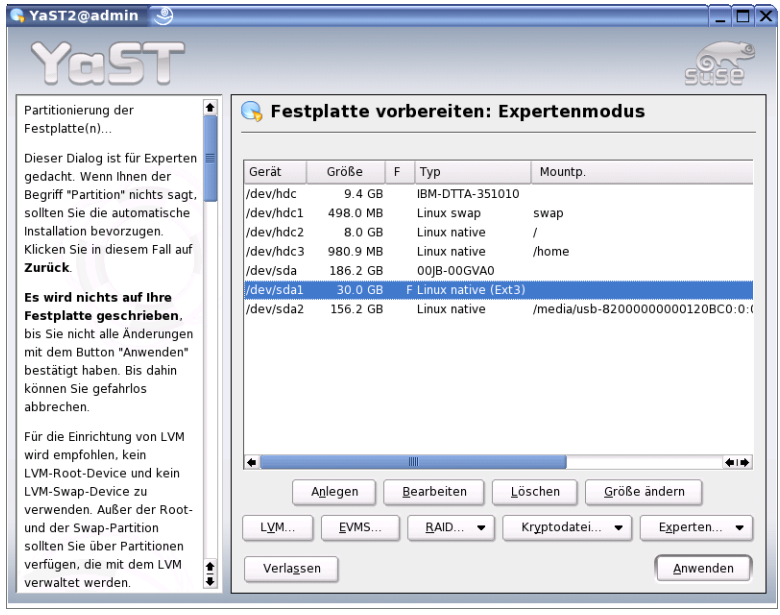

Abbildung A.7: *YaST2-Partitionierer: Übersicht über die geänderte Partitionierung*

A.4 Hintergrundinformationen zum Backup

Das eigentliche Backup wird über einen Cron-Job gesteuert. Dieser ruft einmal täglich die Datei `/etc/cron.daily/oss-backup` auf. Hier wird nun anhand der in der Datei `/etc/sysconfig/schoolserver` eingestellten Variablen das Backup gestartet.

Wenn Sie einmal ohne Zugriff auf ein Backup wissen möchten, wann das letzte Backup gestartet wurde, können Sie in der Datei `/var/adm/backup/LAST_BACKUP` die genaue Zeit finden.

A.5 Zurückspielen der Daten

Für das Zurückspielen der Daten ist das Skript oss_recover.sh verantwortlich, welches die Backup-Daten auf einem installierten Open School Server wieder herstellt. Das Skript wird - zusammen mit einem „readme“ - automatisch in das Verzeichnis kopiert, in welchem sich auch das Vollbackup befindet. Wenn Sie das Skritp mit der Option `-h` aufrufen, bekommen Sie eine kurze Hilfe angezeigt.

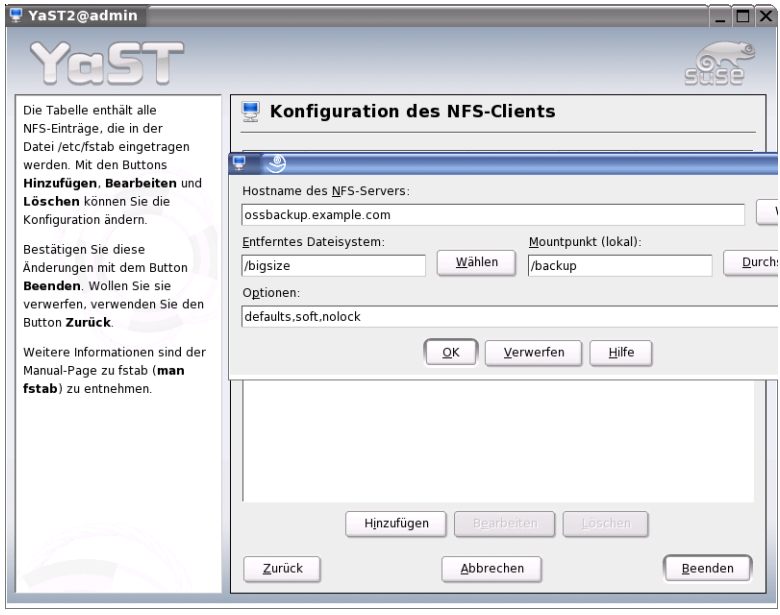

Abbildung A.8: *YaST2-NFS-Client: Mounten eines entfernten Dateisystems*

A.5.1 Vollständiges Zurückspielen des Backups

Wenn Sie das Skrit ohne eine Option aufrufen, werden sämtliche auf dem System vorhandenen Verzeichnisse und Datenbanken automatisch wieder hergestellt.

A.5.2 Partielles Zurückspielen des Backups

Je nachdem, welche Daten Sie gesichert (siehe Abschnitt *Konfiguration des Backups* auf Seite 171) haben, können Sie diese partiell wieder herstellen, indem Sie das Skript oss_recover.sh mit der betreffenden Option aufrufen.

–egroupware Die Datenbank der eGroupware wird wieder hergestellt.

–home Mit dieser Option werden die Daten im Homeverzeichnis mit denen aus dem Vollbackup überschrieben. Alle bis dahin im /home-Verzeichnis vorhandenen Daten gehen dabei verloren!

–joomla Die Joomla-Datenbank wird wieder hergestellt.

–ldap Mit dieser Option wird die LDAP-Datenbank wieder hergestellt.

–mail Mit dieser Option werden die Emails der Benutzer wieder hergestellt.

–moodle Die Moodle-Datenbank und die Dateien für Moodule werden wieder hergestellt.

–openxchange Die Open Xchange Datenbank wird wieder hergestellt.

–proxy Die Proxykonfiguration und die persönlichen Blacklists werden wieder hergestellt.

–samba Die Sambakonfiguration und die Samba-Datenbanken werden wieder hergestellt.

–ssh Die SSH-Keys werden wieder hergestellt.

–ssl Die SSL Zertifikate für den Webserver werden wieder hergestellt.

–tfk Die Filter-Datenbank des „Time 4 Kids“-Internetfilters wird wieder hergestellt.

A.5.3 Grafisches Recovery-Tool

Für den Benutzer `root` steht auch ein grafisches Tool zur Verfügung (siehe *Grafisches Recovery-Tool* auf der nächsten Seite, welches einzelne Teile oder das vollständige Backup zurückspielen kann.

Starten Sie das Tool, indem Sie auf das ‘OSS Recover’ Ikon auf dem Root-Desktop klicken. Das Tool liest die Datei `/etc/sysconfig/schoolserver` aus und warnt Sie ggf. wenn das Backup-Verzeichnis nicht gemountet ist. Anschließend können Sie aus einem Menü auswählen, welche der vorhandenen Daten Sie wieder herstellen möchten.

Abbildung A.9: *OSS Recover: grafische Oberfläche zum Rückspielen eines Backups*

Datenschutz

Die Nutzung und zur Verfügungstellung von Kommunikationstechnischen Anlagen kann für eine Schule weitreichende Folgen haben. Um Ihnen den Umfang der zu beachtenden Gesetze und Vorschriften zu verdeutlichen, soll hier neben einem kurzen Hinweis auf entsprechende Gesetze und Richtlinien ein kurzer Überblick über deren tiefere Bedeutung für die Nutzung des Open School Servers und abschließend ein paar Tipps zu deren praktischen Nutzung und Anwendung gegeben werden.

Achtung

Haftungsausschluß

Die Firma SUSE übernimmt keine Verantwortung für die Richtigkeit der hier gemachten Angaben. Die hier aufgeführten Tipps und Erklärungen entstammen dem Alltag an vielen deutschen Schulen und sind – bis auf ihre Widerlegung durch gerichtliche Entscheidungen – sicherlich ein guter Ausgangspunkt für eigene Entscheidungen. Letzte Gewissheit kann aber nur eine juristische Prüfung an der entsprechenden Schule bringen.

Achtung

B.1 Gesetzliche Grundlagen

Für Schulen relevante Gesetze und Verordnungen:

- das jeweilige Landesdatenschutzgesetz,
- das Bundesdatenschutzgesetz,
- weitere in Schulgesetzen und -verordnungen festgelegte Datenschutzbestimmungen,

- der Mediendienste-Staatsvertrag (MDStV),
- das Teledienstedatenschutzgesetz (TDDSG),
- das Telekommunikationsgesetz (TKG) und die dazugehörige Telekommunikationsdatenschutzverordnung (TDSV),

Die vier letztgenannten (MDStV, TDDSG, TKG & TDSV) greifen an Schulen nur, wenn auch die private Nutzung der schulischen Anlage erlaubt ist. Bei einer rein unterrichtsbezogenen schulischen oder rein dienstlichen Nutzung der Anlage kommen nur die für Schulen bekannten Datenschutzgesetze zur Anwendung.

B.2 Speicherung von Logfiles

Im normalen Betrieb des Open School Servers fallen Logfiles an, deren Inhalt Aufschluss z. B. darüber geben, wer wielange am Rechner eingeloggt war oder wer wann welche Internetseite aufgerufen hat.

Der Gesetzgeber untersagt allerdings generell die Speicherung derartiger Daten.

In Fällen von Missbrauch oder Straftaten möchte aber der Rechnerbetreiber natürlich herausfinden können, wer den Missbrauch/die Straftat verursacht hat, da er sonst unter Umständen selber haftet.

Manchmal genügt auch schon der Hinweis auf solche Logfiles, um das Ansurfen „verbotener“ Webseiten oder das Beschädigen von Hardware zu verhindern.

Die Forschungsstelle Recht des DFN Verein e.V., bei welcher wir uns für die geleistete Arbeit recht herzlich bedanken möchten, trifft zur Speicherung der Daten folgende Aussage:

B.2.1 Einwilligung zur Speicherung von Daten

Mangels gesetzlicher Erlaubnis zur Speicherung solcher Daten kann das Vorhaben nur umgesetzt werden, wenn die betroffenen Schüler bzw. deren gesetzlichen Vertreter einwilligen!

Dabei ist Folgendes unbedingt zu beachten:

- Volljährige Schüler können selbst wirksam einwilligen,
- bei Schülern unter 7 Jahren ist die Einwilligung der Erziehungsberechtigten einzuholen.
- Bei Schülern zwischen 12 und 18 Jahren empfiehlt sich eine Doppeleinwilligung!

Gründe:

1. Solange es sich um Schüler unter 7 Jahren handelt, sind diese nach §104 BGB geschäftsunfähig und noch nicht einsichtsfähig, so dass es alleine auf die Einwilligung aller Erziehungsberechtigten ankommt (i.d.R. Vater und Mutter).

2. Bei Schülern im Alter von 7 bis 18 Jahren (so genannten beschränkt geschäftsfähigen Rechtssubjekten) können nach heutiger Ansicht nur so lange die Erziehungsberechtigten wirksam einwilligen, wie dem Schüler noch die notwendige Einsichtsfähigkeit in sein Handeln abzusprechen ist. Der Zeitpunkt, ab dem Schüler die Konsequenzen der Einwilligung umfassend begreifen können, kann nicht pauschal festgemacht werden. Eine individuelle Abklärung der Lage wäre im Schulbereich natürlich nicht praktikabel und sicher nicht pädagogisch sinnvoll. Im Regelfall ist die Einsichtsfähigkeit bei einem Jugendlichen ab 14 Jahren zu bejahen.

   Wir empfehlen Ihnen „auf Nummer sicher zu gehen“ und bei Jugendlichen ab 12 Jahren von deren Einsichtsfähigkeit auszugehen. Lassen Sie daher bereits bei Schülern ab 12 Jahren den Minderjährigen und deren Erziehungsberechtigte zustimmen.

Wir möchten Ihnen daher empfehlen zu Beginn eines Schuljahres von neu anzulegenden Schülern und deren Erziehungsberechtigten eine entsprechende Erklärung (siehe *Einwilligung zur Speicherung von Daten* auf Seite 255) unterschreiben zu lassen, die dann in den entsprechenden Schülerakten verwahrt wird. Der entstehende Aufwand dürfte sich in Grenzen halten - die daraus entstehende rechtliche Sicherheit ist ihn allemal wert.

Mehr Informationen zum Bereich „Datenschutz und Fernmeldegeheimnis“ erhalten Sie unter `http://www.lehrer-online.de/` im Bereich „datenschutz-fernmeldegeheimnis“.

B.3 Benutzerordnung

Die folgende Benutzerordnung entstand in Zusammenarbeit mit mehreren Schulen und ist dort – manchmal in leicht abgewandelter Form – bis heute im Einsatz.

B.3.1 Vorwort

Diese Nutzerordnung stellt Regelungen bereit, die die Arbeit mit teuren technischen Geräten, die Informationsbeschaffung, die Informationsweitergabe und die Arbeit mit zum Teil komplexer Software betreffen.

In diesem Zusammenhang müssen Hinweise auf Sanktionen gegeben werden, die vom Entzug der Nutzungsberechtigung über sonstige disziplinarische Maßnahmen bis zur Möglichkeit strafrechtlicher Verfolgung reichen. Im Sinne der üblichen Systematik erscheint deshalb die Einbindung in die Schulordnung sinnvoll.

Volljährige Schüler und Schülerinnen sind vor der Benutzung der informationstechnischen Anlagen der Schule über diese Nutzerordnung in Kenntnis zu setzen und haben dies durch eigenhändige Unterschrift zu bestätigen. Bei Schülern und Schülerinnen, welche das 18. Lebensjahr noch nicht vollendet haben, müssen zusätzlich die Erziehungsberechtigten durch Unterschrift bestätigen über diese Nutzerordnung und die durch ihre Nichtbeachtung entstehenden Folgen informiert worden zu sein.

1. **Geltungsbereich und Inkrafttreten** Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Schulordnung und tritt am Tage ihrer Verkündung in Kraft.

2. **Nutzungs- und Weisungsberechtigung** Nutzungsberechtigt sind Lehrerinnen und Lehrer sowie Schülerinnen und Schüler der Schule. Außerhalb des regulären Unterrichts wird der Zugang zu den Computern durch die Schulleitung und den Fachlehrern geregelt. Weisungsberechtigt sind die unterrichts- bzw. aufsichtsführenden Fachlehrer. In Ausnahmefällen kann ein verantwortungsbewusster Schüler von einem Fachlehrer als weisungsberechtigte Aufsicht eingesetzt werden.

3. **Arbeit am Computer** Ein Nutzer hat sich im Schulnetz nur unter dem ihm zugewiesenen Nutzernamen anzumelden. Der Nutzer ist für die Aktivitäten, die unter diesem Nutzernamen ablaufen, verantwortlich. Die Arbeitsstation, an der sich ein Nutzer im Netz angemeldet hat, darf nicht von diesem unbeaufsichtigt gelassen werden.

   Nach dem Beenden der Nutzung hat sich ein Nutzer im Netzwerk abzumelden und ggf. den Rechner herunterzufahren.

   Die während des Bootvorgangs oder der Anmeldung am System automatisch gestarteten Programme dürfen nicht deaktiviert werden.

Das unbefugte Kopieren lizenzpflichtiger Software von den Arbeitsstationen oder aus dem Netz ist verboten. Nutzer, die unbefugte Kopien anfertigen, machen sich strafbar und können rechtlich verfolgt werden. Davon ausgenommen sind Programme, die im Unterricht selbst erstellt wurden und Kopiervorgänge, die bei jedem Programmstart automatisch durchgeführt werden (Programmkopie im Arbeitsspeicher). Lizenzrechtlich zulässige Arbeitskopien und Kopien freier Software können von der zuständigen Lehrkraft bezogen werden.

4. Datenschutz und Datensicherheit Alle im Schulnetz befindlichen Daten unterliegen dem Zugriff der Systemverwalter. Diese können bei dringendem Handlungsbedarf unangemeldet Daten einsehen, löschen oder verändern. Der Nutzer wird von einem solchen Eingriff – notfalls nachträglich – angemessen informiert. Die Namen der Systemverwalter sind über die Schulverwaltung zu erfahren.

Die persönlichen Arbeitsbereiche sind durch sinnvoll gewählte Passwörter gegen unbefugten Zugriff zu sichern. Die Passwörter sind geheim zu halten. Jeder Nutzer ist dafür verantwortlich, dass sie/er nur alleine ihre/seine persönlichen Passwörter kennt, bzw. zugewiesene Passwörter nicht weitergibt.

Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen und sonstiger Authentifizierungsmittel sind wie der Zugriff auf fremde, persönliche Verzeichnisse und Dateien ohne ausdrückliche Zustimmung des Eigentümers unzulässig. Der Einsatz von sog. „Spyware“ (z.B. Sniffern) oder Schadsoftware (z.B. Viren, Würmer) ist im Schulnetz strengstens untersagt. Der unbefugte Einsatz solcher Software hat den sofortigen Verlust der Zugangsberechtigung zur Folge und kann strafrechtlich verfolgt werden. Laborversuche unter Aufsicht einer Lehrkraft sind hiervon ausgenommen.

Ein Rechtsanspruch auf den Schutz persönlicher Daten vor unbefugten Zugriffen besteht gegenüber der Schule nicht. Ein Rechtsanspruch auf die Speicherung und Verfügbarkeit persönlicher Daten besteht gegenüber der Schule nicht.

5. Nutzung des Internets Informationen aus dem Internet können aus technischen Gründen keiner lückenlosen hausinternen Selektion unterworfen werden. Die Schule kommt ihrer Aufsichtspflicht gegenüber Minderjährigen durch regelmäßige Stichprobenkontrollen des Datenverkehrs nach. Dazu ist sie auch berechtigt den Datenverkehr in Protokolldateien zu speichern, aus denen Nutzer, Datum und Art der Nutzung festzustellen sind. Zusätzlich kann sie sogenannte Filtersoftware einsetzen, die jedoch keine lückenlose Sperrung fragwürdiger Seiten ermöglicht.

Es ist verboten Vertragsverhältnisse im Namen der Schule einzugehen (z.B. Bestellung von Artikeln über das Internet) oder kostenpflichtige Dienste im Internet zu nutzen.

Es ist verboten sich Zugang zu Informationen aus dem Internet zu verschaffen, die rechtlichen Grundsätzen in der Bundesrepublik widersprechen. Das gilt insbesondere für Seiten mit gewaltverherrlichendem, pornographischem oder nationalsozialistischem Inhalt. Verstöße hiergegen haben unter anderem den Entzug der Nutzungsberechtigung zur Folge.

Das Internet und sämtliche dort zugänglichen Dienste und Dateien dürfen nur für schulische Zwecke genutzt werden. Downloads und die Nutzung von Kommunikationsdiensten wie E-Mail, News und Chat für private Zwecke sind generell untersagt.

Der Aufbau jeglicher zusätzlicher externer Verbindungen (z.B. über Modem oder ISDN) ist untersagt. Laborversuche unter Aufsicht einer Lehrkraft sind ausgenommen.

6. Informationsübertragung in das Internet Die Schule ist verantwortlich für ihr Internetangebot. Eine Geheimhaltung von Daten, die über das Internet übertragen werden, kann von der Schule nicht gewährleistet werden.

Es ist untersagt den Internetzugang der Schule zur Verbreitung von Informationen zu verwenden, die dazu geeignet sind dem Ansehen der Einrichtung Schaden zuzufügen.

Es ist verboten Informationen zu verschicken die rechtlichen Grundsätzen widersprechen. Dies gilt insbesondere für rassistische, ehrverletzende, beleidigende oder aus anderen Gründen gegen geltendes Recht verstoßende Nachrichten. Die Bestimmungen des Bundesdatenschutzgesetzes sind einzuhalten. Dies gilt insbesondere für die Bekanntgabe von Namen und Adressdaten oder die Veröffentlichung von Fotografien ohne die ausdrückliche Genehmigung der davon betroffenen Personen.

Grundsätze, wie sie beispielhaft in der Netiquette, dem Knigge im Bereich der Datenkommunikation, enthalten sind, sind einzuhalten.

7. Datenvolumen Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (z.B. Grafiken, Videos oder Audiodateien) aus dem Internet ist zu vermeiden. Sollte ein Nutzer unberechtigt größere Datenmengen in seinem Arbeitsbereich ablegen, so sind die Systemverwalter berechtigt diese Daten zu löschen.

8. Verhalten im Computerraum Innerhalb der Räume ist den Anweisungen der aufsichtsführenden Personen Folge zu leisten.

Das Einnehmen von Speisen und Getränken an den Computern ist nicht gestattet.

Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich

untersagt. Schulfremde Hardware (z.B. ein Notebook) darf nur nach ausdrücklicher Erlaubnis der zuständigen, weisungsberechtigten Person und unter Einhaltung der zugeteilten Zugangsdaten an das Datennetz der Schule angeschlossen werden.

Daten, die während der Nutzung einer Arbeitsstation entstehen, können im zugewiesenen Arbeitsbereich abgelegt werden. Das Starten von eigener Software bedarf der Genehmigung durch die aufsichtsführende Person.

Beim Auftreten von Funktionsstörungen ist die aufsichtsführende Person zu verständigen.

Vor dem Verlassen des Raumes ist der Arbeitsplatz aufzuräumen. Die Stühle sollen unter den Tisch gerückt werden.

9. Zuwiderhandlungen Zuwiderhandlungen gegen diese Ordnung oder ein Missbrauch des Internet-Zugangs können neben dem Entzug der Nutzungsberechtigung für das Netz und die Arbeitsstationen disziplinarische Maßnahmen und Geldbußen nach sich ziehen.

Schülerdaten exportieren und importieren

Hier beschreiben wir verschiedene Möglichkeiten, Schülerdaten aus anderen Programmen mit dem Open School Server zu verarbeiten.

Um für jeden Schüler der Schule einen eigenen Account anzulegen, bietet es sich an, die benötigten Daten direkt aus einem Schulverwaltungsprogramm zu importieren. Dies erleichtert die Administration enorm, da so die aktuellen Schülerdaten mit Name, Klasse, etc. nur ein einziges Mal in aktueller Form vorgehalten werden müssen: in der Schulverwaltung.

Sie als Administrator benötigen dann nur noch eine Diskette, auf welcher die Daten möglichst im „CSV-Format“ (eine ASCII-Datei mit bestimmten Trennzeichen zwischen den einzelnen Werten) vorliegen müssen. Das läßt sich heute mit vielen Verwaltungsprogrammen problemlos realisieren.

Hier zeigen wir Ihnen kurz anhand weitverbreiteter Beispiele, wie der Export der Daten aus Schulverwaltungsprogrammen stattfinden kann. Über den Import der Daten in den Open School Server lesen Sie bitte unter *Benutzer importieren – Einlesen von Benutzerlisten* auf Seite 62 nach.

C.1 Schulverwaltungsprogramme, die CSV-Exporte ermöglichen

Wenn das verwendete Schulverwaltungsprogramm den direkten Export einer reinen Textdatei mit Trennzeichen zwischen den einzelnen Feldern (also eine sogenannte „CSV-Datei“) erlaubt, müssen Sie nur noch sicherstellen, dass der Open School Server die einzelnen Felder auch zuordnen kann – also z. B. beim Import nicht den Vornamen mit dem Nachnamen verwechselt.

Exportieren Sie dazu die entsprechenden Daten (wichtig sind: Nachname, Vorname, Geburtstag und Klasse) und öffnen Sie die Datei anschließend mit einem beliebigen Editor. Überprüfen Sie nun, ob in der ersten Zeile schon Überschriften mit diesen Namen vorhanden sind. Sollte dies nicht der Fall sein, tragen Sie bitte die entsprechenden Überschriften ein und verwenden Sie dieselben Trennzeichen zwischen den Feldern, wie in den restlichen Zeilen.

Nun können Sie die Daten wie unter *Benutzer importieren – Einlesen von Benutzerlisten* auf Seite 62 beschrieben importieren.

C.2 WinSV - bayerische Schülerdatei

Zuerst müssen Sie die Schülerdaten aus dem Programm exportieren. Dazu aktivieren Sie das Pflegemenü unter 'Datei' → 'Pflegemenü'. Dieses sollte nun angezeigt werden (siehe Abbildung C.1).

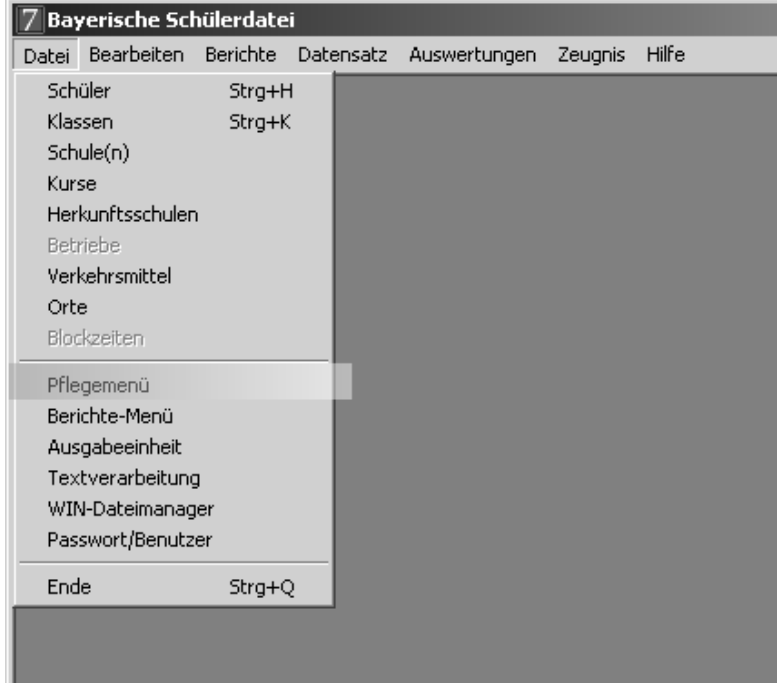

Abbildung C.1: *WinSV: Aufrufen des Pflegemenüs*

Dort wählen Sie nun 'Export - Import von Schülerdaten' → 'Export für eigene Schule' (siehe Abbildung C.2).

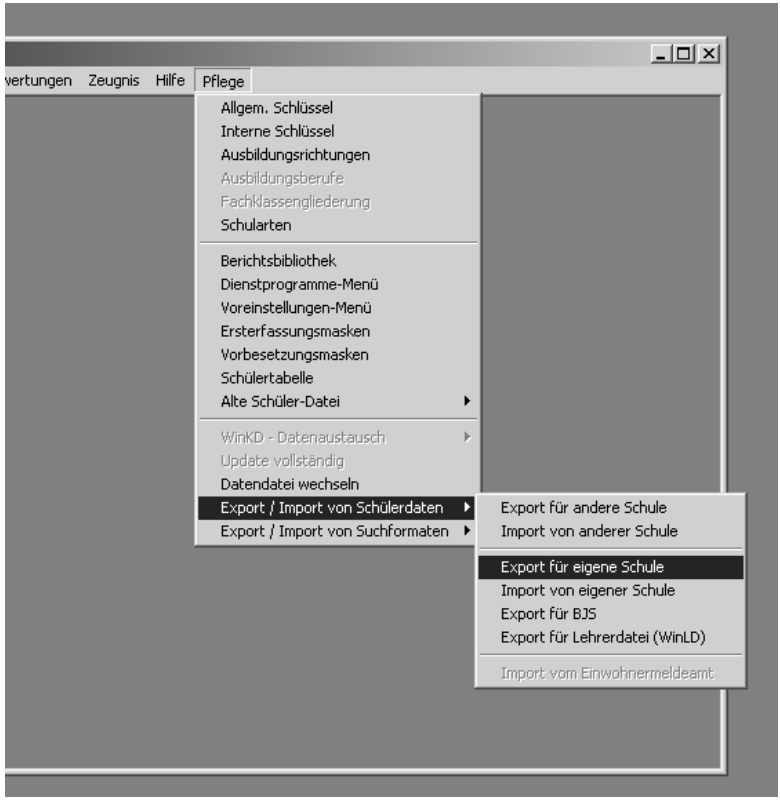

Abbildung C.2: *WinSV: Export der Daten für die eigene Schule*

Nun müssen Sie alle Klassen markieren, die Sie im Open School Server anlegen möchten. Oder wählen Sie `alle Klassen` im unteren Menü.

Achtung

Bei erneutem Einspielen der Liste müssen Sie auch die schon am Open School Server angelegten Klassen auswählen, da diese sonst gelöscht werden!

Für das Anlegen oder Editieren einzelner Schüler sehen Sie bitte im Abschnitt 6.2.1 auf Seite 58 nach.

Achtung

Als Export-Datei geben Sie einen Namen ein (nach Möglichkeit ohne Umlaute - und nicht den Namen `userlist.txt`) und klicken auf (Export starten)

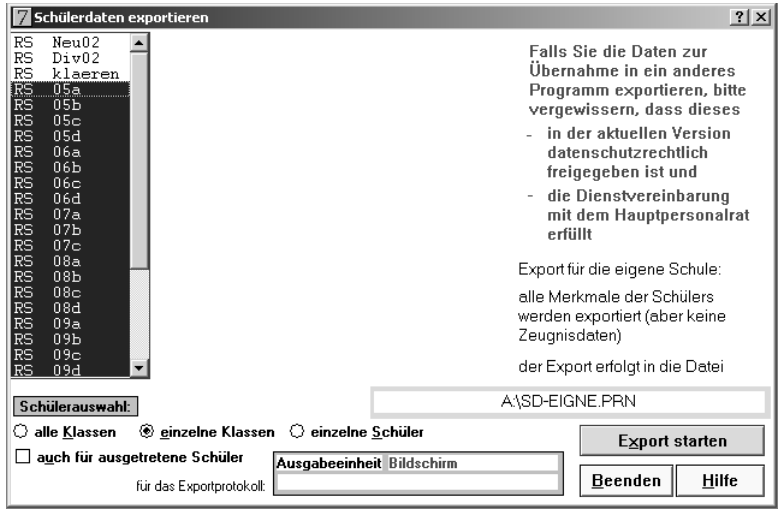

Abbildung C.3: *WinSV: Export starten*

Speichern Sie die Datei auf eine Diskette.

Vor dem Einlesen der Schülerdaten

Um die auf Diskette gespeicherten Daten in den Open School Server einzulesen, müssen diese noch passend formatiert werden. Dies stellen Sie im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' ein, indem Sie unter '

$$GENERAL$$

' → 'SCHOOL_IMPORT_FILE_FORMAT' „WinSV“ auswählen.

C.3 Sibank - niedersächsisches Schulverwaltungsprogramm

Zuerst müssen Sie die Schülerdaten aus dem Verwaltungsprogramm exportieren. Glücklicherweise ermöglicht Sibank den direkten Export in eine ASCII-Datei, so dass die Nacharbeiten nicht allzu umfangreich ausfallen.

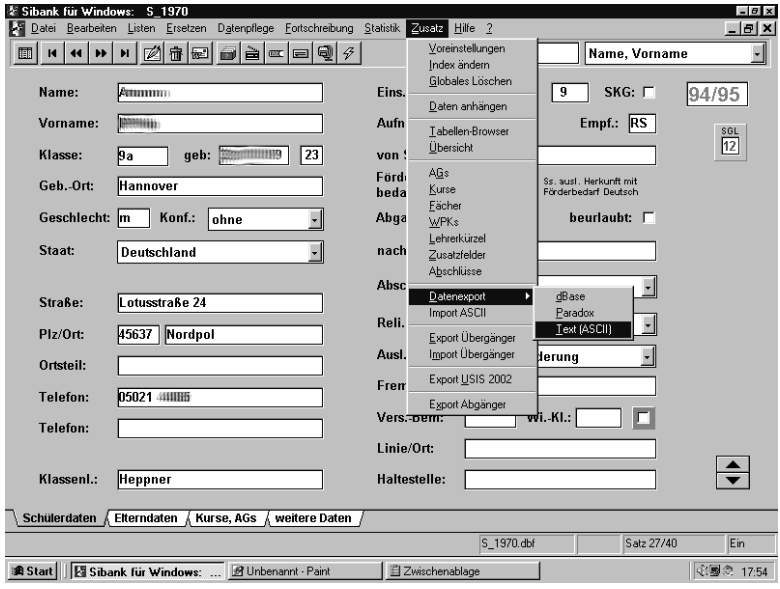

Abbildung C.4: *SiBank: Aufrufen der Exportfunktion*

Zum Exportieren der Schülerdaten wählen Sie im Programm den Menüpunkt 'Zusatz' → 'Datenexport' → 'Text(ASCII)'.

Nun müssen Sie alle Klassen markieren, die Sie im Open School Server anlegen möchten. Oder wählen Sie einfach alle Klassen aus. Der nächste Schritt ist die Bestimmung der zu exportierenden Felder.

Wenn datenschutzrechlich nichts dagegen spricht, können Sie einfach das Feld „alle Datenfelder" markieren und die Daten unter einem aussagekräftigen Namen auf einer Diskette speichern (siehe C.5 auf der nächsten Seite).

Achtung

Bei erneutem Einspielen der Liste müssen Sie auch die schon am Open School Server angelegten Klassen auswählen, da diese sonst gelöscht werden!

Für das Anlegen oder Editieren einzelner Schüler sehen Sie bitte im Abschnitt 6.2.1 auf Seite 58 nach.

Achtung

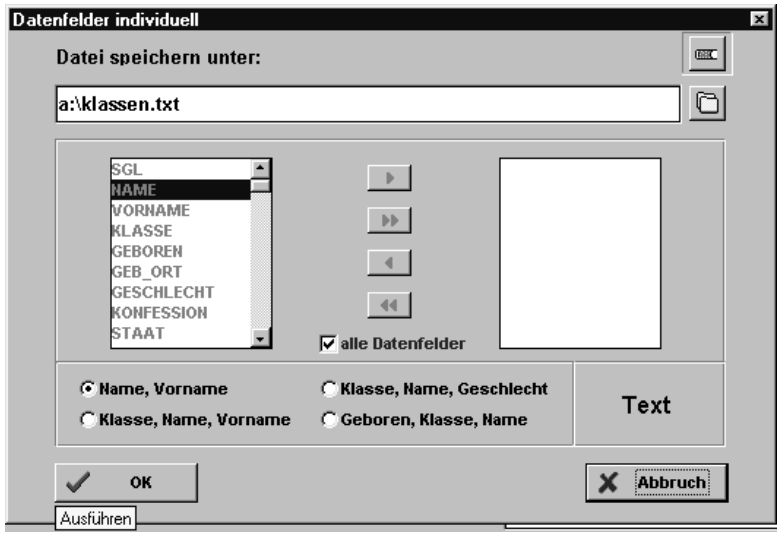

Abbildung C.5: *SiBank: Speichern der Daten auf Diskette*

Vor dem Einlesen der Schülerdaten

Um die auf Diskette gespeicherten Daten in den Open School Server einzulesen, müssen diese noch passend formatiert werden. Dies stellen Sie im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' ein, indem Sie unter '

$$GENERAL$$

' → 'SCHOOL_IMPORT_FILE_FORMAT' „SiBank“ auswählen.

C.4 Schild-NRW - nordrheinwestfälisches Schülerverwaltungsprogramm

Zuerst müssen Sie die Schülerdaten aus dem Programm exportieren. Dazu starten Sie den Datenaustausch über das Menü 'Datenaustausch' → 'Text-Dateien' →Export (siehe Abbildung C.6 auf der nächsten Seite).

Im nächsten Fenster wählen Sie als Datenart 'Schüler' und die Export-Felder:

- Vorname,

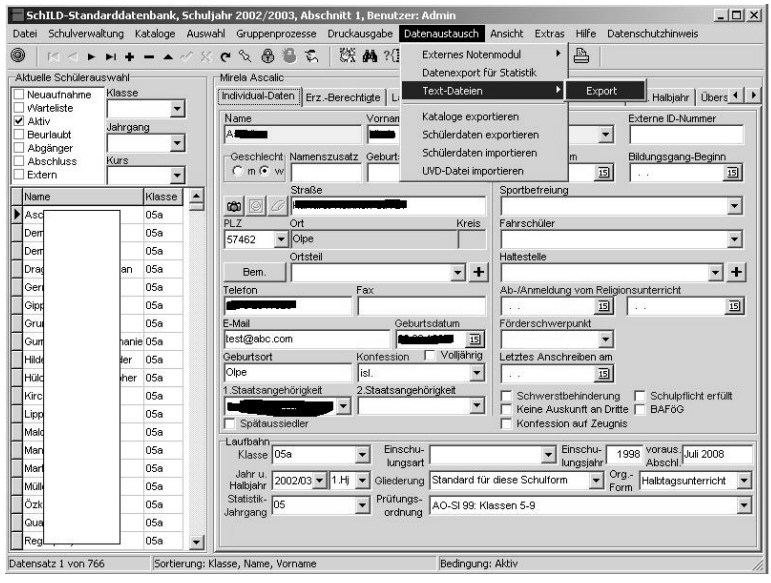

Abbildung C.6: *Schild-NRW: Aufrufen der Exportfunktion*

- Nachname,
- Namenszusatz,
- Geburtsdatum und
- Klasse aus.

Geben Sie im Anschluß einen Namen für die Ausgabe-Datei an (z. B. `slss_export`) und klicken Sie auf 'Export starten' (siehe Abbildung C.7 auf der nächsten Seite).

Die exportierte Datei können Sie direkt mit dem Open School Server einlesen. Stellen Sie dazu im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' sicher, das unter '

$$GENERAL$$

' → 'SCHOOL_IMPORT_FILE_FORMAT' „CSV“ gewählt ist.

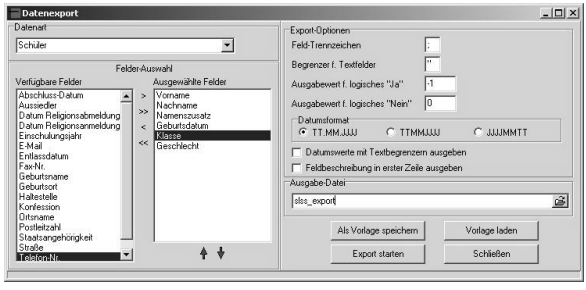

Abbildung C.7: *Schild-NRW: Export starten*

C.4.1 SquidGuard

Das Programm SquidGuard wird am Open School Server als Filterprogramm für Internetseiten verwendet. SquidGuard ist ein „Redirector“, der in der Lage ist, unerwünschte URLs zu sperren, indem er die im Browser eingegebene URLs mit Einträgen aus einer auf dem Server gespeicherten Datenbank vergleicht und bei einer Übereinstimmung die Anfrage des Clients auf eine vorher definierte Webseite umleitet.

Sicherlich kann über den Einsatz einer solchen zensierenden Software immer diskutiert werden – wir möchten Ihnen hier nur einen kurzen, technischen Überblick über die Möglichkeiten geben, damit Sie Ihre Entscheidung für oder gegen den Einsatz dieses Programms auf der Grundlage von fundiertem Wissen treffen können.

Was ist SquidGuard?

SquidGuard ist ein Plugin für den Proxy-Server Squid, das

- Internetseiten aufgrund eines Datenbankeintrages sperren,
- den Nutzer statt auf die angeforderten auf andere Seiten umlenken und
- je nach Tageszeit, Grupenzugehörigkeit oder sogar Nutzer- bzw. Rechnerabhängig die Zugriffsrechte unterschiedlich handhaben kann.

Im Open School Server werden nicht alle diese Funktionalitäten genutzt. Eine Aufteilung nach Tageszeit oder gruppen- oder computerabhängige Zugriffsrechte findet nicht statt.

Nach einer Standardinstallation des Open School Server werden in einer Berkley-Datenbank diverse Internetseiten und IP-Adressen initialisiert, welche für die Verbreitung von „schmutzigen Inhalten“ bekannt sind.

Nach dem Start von Squid wird auch SquidGuard initialisiert und läd die Datenbank. Jede Anfrage eines Clients wird nun von Squid an SquidGuard durchgereicht, wo Sie mit den in der Datenbank enthaltenen Einträgen verglichen wird. Da die Inhalte der Datenbank vorher „kompiliert“ wurden und so sehr schnell abgefragt werden können, merkt der normale Nutzer auch bei mehreren tausend Einträgen in der Datenbank kaum etwas davon.

Die Listen (der Sperrseiten) für die Datenbank befindet sich im Verzeichnis ‘/var/squidGuard/db/blacklist’. Nehmen Sie hier Änderungen vor, müssen Sie mit dem Befehl `squidGuard -c /etc/squid/squidguard.conf -C all` die Datenbanken neu aufbauen und den Proxy squid neu starten.

Findet SquidGuard eine Übereinstimmung mit der Datenbank, wird der Nutzer per default-Einstellung auf ein cgi-Skript auf dem Webserver des Open School Server umgeleitet, welches Ihm mitteilt, dass die Auslieferung der angefragten Seite verweigert wird.

Einsatz von SquidGuard in einer Schulumgebung

Prinzipiell bietet SquidGuard mit seinen Möglichkeiten für Schulen eine gute Möglichkeit, Schüler vor unerlaubten Inhalten des Internets zu schützen. Allerdings wird dieser Schutz (trotz einer zusätzlichen „Stichwortsuche“ in Webseiten) nie endgültig alle Inhalte erfassen können, da sich eben diese Inhalte zu oft und zu schnell ändern.

Eine Einweisung in den verantwortungsvollen Umgang mit dem Internet kann SquidGuard deshalb nicht ersetzen! Während der vorbeugende Einsatz von SquidGuard in Grundschulen wohl noch akzeptabel erscheint, sollten in weiterführenden Schulen also eher pädagogische und soziale Maßnahmen – zumindest begleitend – eingesetzt werden.

Filterlisten aktualisieren

Achtung

Haftungsausschluß

Die Firma EXTIS GmbH übernimmt keine Verantwortung für die korrekte Funktion der zur Verfügung gestellten Filterlisten. Wir lehnen jede Haftung für jegliche Art von Mißbrauch oder Fehlfunktionen in diesem Zusammenhang ab.

Bitte weisen Sie sämtliche Personen, die das Internet nutzen, auf die Verwendung von Filtersoftware hin und sorgen Sie durch eine ausreichende zusätzliche Kontrolle für die Sicherung eines verantwortungsvollen Interneteinsatzes.

Achtung

Im Menü ‘Rechner/ Domänen’ → ‘Proxy’ klicken Sie bitte auf den Button ‘SquidGuard’. Nun wird Ihnen zunächst ein neues Menü angeboten, in welchem Sie zusätziche Einträge in die „Blacklists“ machen oder die Blacklists von externen Servern herunterladen können.

Zusätzliche Einträge

Da die „Blacklists“ aus dem Internet vorwiegend von sogenannten Robots, d.h. selbstständig arbeitenden Programmen, erzeugt werden, können durchaus einmal erlaubte Seiten auf einer solchen Blacklist landen und werden dann gesperrt. Dies ist z. B. mit der Suchseite Google schon häufiger passiert.

Genauso kann es aber auch passieren, dass diese Robots eine der zig Millionen fragwürdigen Internetseiten nicht finden – wohl aber Ihre Schüler. Aus diesem Grund können Sie in diesem Menü zwei „Eigene Listen“ pflegen. Tragen Sie in die entsprechenden Listen bitte pro Zeile nur eine Seite ein.

Abbildung C.8: *Filterlisten des Proxyservers aktualisieren*

Fälschlicherweise gesperrte Seiten freigeben Wurde fälschlicherweise einmal eine Webseite eingetragen, auf die Sie den Zugriff gewähren möchten, dann tragen Sie diese Seite bitte in das entsprechende Textfeld ein. Damit wird die eingetragene Domain von der Sperrung ausgenommen.

Zusätzliche Seiten sperren Wenn einmal eine Seite nicht gesperrt ist, können Sie diese hier eintragen. Damit wird der Zugriff auf diese Seite gesperrt. Wenn Sie auch anderen Schulen dabei helfen wollen, diese Seiten zu sperren, dann melden Sie die entsprechende URL bitte an eine der entsprechenden Stellen weiter.

Über den Button 'Änderungen anwenden' speichern Sie Ihre Änderungen in den Listen und die Änderungen stehen sofort zur Verfügung.

Externer LTSP-Terminalserver

Um neben dem Open School Server einen LTSP-Terminalserver in Betrieb zu nehmen, ist ein wenig „Handarbeit“ gefordert. Vielen Dank an Dieter Kroemer (`http://www.linux-in-der-schule.de`), welcher an der staatlichen Realschule Schesslitz unterrichtet und dort „nebenbei“ das Netzwerk betreut, für Unterlagen zu diesem Thema, welche er uns überlassen hat und welche nun Eingang in dieses Handbuch gefunden haben.

Um einen LTSP-Terminalserver in Betrieb nehmen zu können, bedarf es folgender Voraussetzung:

- Ein mit SuSE 10.1 oder 10.2 installierter PC mit dem zusätzlichen Paket: Netzwerk/Server. Am einfachsten ist ein per Autoinstallation installierter Terminalserver.
- Der Rechner ist am Open School Server angemeldet und erhält seine IP-Adresse über `DHCP`.
- Eingerichteter `LDAP- und NFS-Client` - wie unter 7 auf Seite 125 beschrieben.
- Die Diskless-Clients benötigen entweder eine PXE-fähige Netzwerkkarte oder die Möglichkeit mittels Etherboot (z.B. über eine Etherboot-Diskette oder ein Etherboot-PROM auf der Netzwerkkarte - siehe z. B. `http://marl.linuxfreunde.de/kmLinuxTSE`) zu booten.

Pakete, die unbedingt installiert sein sollten (bitte mit YaST2 überprüfen):

dhcp-server Der DHCP-Server. Dieser wird nach der Grundkonfiguration wieder abgeschaltet, wird aber von ltspadmin benötigt.

tftp Ein einfacher FTP-Server.

nfs-utils Wird benötigt, um an die LTSP-Clients das Root-Dateisystem über NFS auszuliefern.

xntp Dieser Dienst lauscht als Stellvertreter an bestimmten Netzwerkports und startet z. B. den tftpd nur bei Bedarf.

D.1 LTSP-Terminalserver einrichten

Für die weitere Arbeit benötigen Sie `root`-Rechte - melden Sie sich deshalb z. B. unter KDE als solcher am zukünftigen Terminalserver an und laden Sie von der Webseite

`http://www.ltsp.org/`

folgendes Paket in das Verzeichnis `/root/Desktop` herunter: `ltsp-utils-<version>.noarch.rpm`. Sie können hierbei ruhig das Ret-Hat oder das Mandriva RPM benutzen.

Wenn Sie mit Konqueror auf das Paket klicken, können Sie es gleich installieren. Ansonsten öffnen Sie ein Terminalfenster und installieren das Paket „von Hand“.

Machen Sie dazu bitte folgende Eingaben:

```
cd /root/Desktop/
rpm -Uhv ltsp-utils-*.noarch.rpm
```

Datei 11: *Eingaben zur Installation des LTSP*

Nun können Sie mit dem Tool ltspadmin weitere Pakete herunterladen. Starten Sie dazu das Tool in einem Terminalfenster mit den Befehl `ltspadmin` als `root`.

- Im ersten Schritt müssen Sie einige Einstellungen für den Installer machen. Die Frage ‘Where to retrieve packages from?’ sollten Sie mit Enter übernehmen - oder Sie geben z. B. mit `file://home/install/ltsp/ltsp-4.2/` den Pfad zu einem lokalen Repository an.
- Auch die Frage ‘In which directory would you like to place the LTSP client tree?’ können Sie mit Enter übernehmen. Wenn Sie mit verschiedenen Versionen von LTSP herumspielen möchten, können Sie aber auch hier andere Eingaben machen und so z. B. `/opt/ltsp-4.2` eingeben (und später mit `ln -s /opt/ltsp-4.2 /opt/ltsp` einen Symlink anlegen.

- Da sich der Terminalserver aller Voraussicht nach hinter dem Open School Server befindet, sollten Sie zum Zeitpunkt des Downloads den 'Direkten Internetzugang' für den Raum des Terminalservers erlauben. Dann können Sie auch die dritte Frage 'If you want to use an HTTP proxy, enter it here' mit (Enter) überspringen.
- Dasselbe gilt für die Frage 'If you want to use an FTP proxy, enter it here'.
- Zum Abschluß der Konfiguration werden Sie gefragt, ob die eingegebenen Werte korrekt sind. Dies beantworten Sie mit `y` und (Enter).

Damit wäre die Grundkonfiguration erledigt und Sie können die ersten Pakete aus dem Internet herunterladen. Wählen Sie nun 'Install/Update LTSP Packages' im Menü aus, indem Sie mit den Pfeiltasten auf den entsprechenden Menüpunkt navigieren und dann (Enter) drücken.

Im darauf folgenden Dialog wählen Sie einfach mit (A) alle Pakete zur Installation aus und starten den Download mit (Q).

Wählen Sie zum Schluß im Hauptmenü den Punkt 'Configure LTSP' aus. Nach einem kurzen Check können Sie mit (Enter) in ein neues Menü wechseln, in welchem Sie sich zunächst mit (S) ('Show the status of all services') den aktuellen Status ansehen können.

Im zweiten Schritt lassen Sie nun ltspadmin Ihr System einmal grundlegend konfigurieren. Wechseln Sie dazu mit (Enter) wieder zum vorherigen Menü und wählen Sie nun mit (C) ('Configure the services manually').

Wenn Sie sich nicht sicher sind, welche Einstellungen Sie hier machen müssen, dann wählen Sie der Reihe nach die Menüpunkte 1 bis 11 an und beantworten Sie die entsprechenden Fragen (meist reicht auch hier ein einfaches (Enter)). Verlassen Sie das Konfigurationsmenü über die Taste (Q) und wählen Sie dann 'Quit the administration program'.

Nachdem die Grundlegenden Einstellungen gemacht worden sind, können Sie das Konfigurationsprogramm verlassen – nun geht es zunächst mit YaST2 weiter:

- Starten Sie den Runlevel-Editor über 'System' → 'Runlevel-Editor öffnen' → 'Runlevel-Eigenschaften'
- Wählen Sie hier `nfsserver` → `Starten/Anhalten/Aktualisieren: Jetzt starten` und bestätigen Sie die Meldungen mit `OK`:
- Markieren Sie die Checkboxen unter `Der Dienst wird in folgenden Runleveln gestartet: [X] 3 [X] 5`

- Den DHCP-Server müssen Sie jetzt über `Starten/Anhalten/Akualisieren: Jetzt anhalten` anhalten und dafür sorgen, dass er auch zukünftig nicht mehr gestartet wird. Das geschieht, indem Sie unter `Der Dienst wird in folgenden Runleveln gestartet:` alle `[X]` wegklicken.
- Ebenso verfahren Sie mit dem NSCD. Auch dieser darf auf dem Terminalserver nicht gestartet werden.
- Über `Beenden` werden alle Eingaben gespeichert und und der Runlevel-Editor geschlossen.

Tipp

Damit nicht jeder Schüler mit seinem Client den Terminalserver ausschalten/herunterfahren kann, sollten Sie als `root` das 'Kontrollzentrum' von KDE starten und dort über 'Systemverwaltung' → 'Anmeldemanager' →Sitzungen →Konsole folgende Einstellungen im Bereich 'Herunterfahren erlauben' machen:

'nur Konsole': Nur Systemverwalter

'vom Fremdrechner': Niemand

Tipp

D.1.1 Keyboard, Server-IP und NFS-Server einstellen

Um an den Clients des Terminalservers kompfortabel arbeiten zu können, müssen noch Änderungen in einigen Konfigurationsdateien vorgenommen werden. Bearbeiten Sie die Dateien einfach mit Ihrem bevorzugten Editor.

Wir gehen im weiteren davon aus, dass Sie ein 192er Netzwerk benutzen. Bitte ändern Sie ggf. die angegebenen IP-Addressen und Netzwerkbereiche entsprechend Ihren eigenen Netzwerkeinstellungen ab.

Deutsche Tastatur und XServer

Editieren Sie die Datei `/opt/ltsp/i386/etc/lts.conf` und ändern Sie unterhalb von [Default] den Wert:

```
SERVER = 192.168.<IP >[1]
```

und fügen Sie folgende Werte zusätzlich ein:

```
XkbModel = pc104
XkbLayout = de
```

Öffnen Sie anschließend eine Konsole und geben Sie dort folgende Befehlszeile ein:

```
/sbin/ldconfig -r /opt/ltsp/i386
```

[1] <IP >muss durch die vom Open School Server vergebene IP ersetzt werden.

Einstellungen für den Nummernblock

Sollte am Nummernblock das `','` nicht funktionieren und anstattdessen ein `'.'` ausgegeben werden, fügen Sie bitte folgende Zeile in die Datei `/etc/X11/Xmodmap.remote` ein:

```
keycode 91 = KP_Separator
```

Datei /etc/exports anpassen

In der Datei `/etc/exports` müssen Sie noch die Subnetzmaske folgendermaßen abändern:

```
/opt/ltsp/i386 192.168.0.0/255.255.0.0(ro,no_root_squash,sync)
/var/opt/ltsp/swapfiles 192.168.0.0/255.255.0.0(rw,no_root_squash,async)
```

Verbesserte Namensauflösung duch Einträge in /etc/hosts

In der Datei `/etc/hosts` des Terminalservers sollte man einmalig für jeden Client eine neue Zeile nach diesem Schema hinzufügen:

```
IP  kompletter Rechnername  Rechnername
```

also z. B.:

```
192.168.4.2  cr04-pc02.suse.de  cr04-pc02
192.168.4.3  cr04-pc03.suse.de  cr04-pc03
192.168.4.4  cr04-pc04.suse.de  cr04-pc04
...
```

(Wobei `suse.de` die jeweilige Domain des Open School Servers ist.)

Nach einem Neustart sollte der Terminalserver nun bald seinen Dienst aufnehmen können.

D.2 Einstellungen am Open School Server

Um einen zusätzlichen Terminalserver in Betrieb nehmen zu können, bedarf es einiger Änderungen am Open School Server. Sicherheitshalber sollten Sie ein Backup aller geänderten Daten machen – bevor es nachher zu spät ist.

Hinweis

Bei Änderungen an der LDAP-Konfiguration sollten Sie ganz genau wissen, was Sie da tun! Ein fehlerhaft konfigurierter LDAP-Server kann den gesamten Betrieb des Open School Servers negativ beeinflussen.

Hinweis

D.2.1 DHCP-Server konfigurieren

Wenn man nur einen Terminalserver verwendet, schreibt man die folgende Einträge in den Abschnitt 'Options Global' im 'ADMIN-Menü' → 'Rechner/Domänen' → 'DHCP-Konfiguration' (siehe Abbildung D.1:

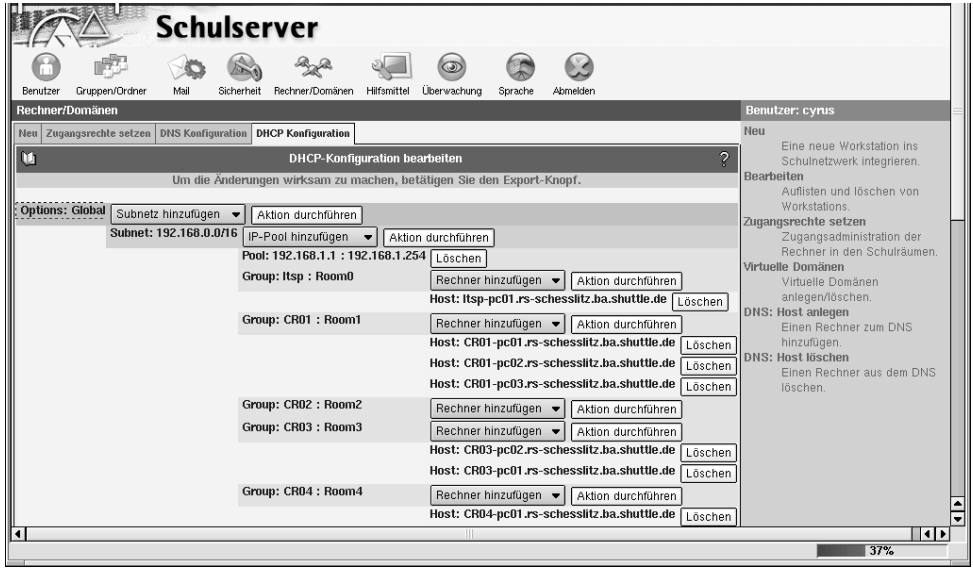

Abbildung D.1: *DHCP-Server-Einstellungen im Webfrontend*

dhcpStatement: if (Der nachfolgende Text ist eine Zeile bzw. ein Statement!)

```
if substring (option vendor-class-identifier, 0, 9) =
"PXEClient" { filename "/lts/pxelinux.0"; } else if substring
(option vendor-class-identifier, 0, 9) = "Etherboot" { filename
"/lts/vmlinuz-2.4.22-ltsp-1"; }#
```

dhcp-Option: root-path (Wiederum nur eine Zeile bzw. ein Statement.)

```
root-path "192.168.<IP >/opt/ltsp/i386"
```

(wobei natürlich 192.168.<IP >durch die IP des Terminalservers ersetzt werden muss.)

Die Einträge abschließend 'Speichern' und 'Exportieren' (siehe Buttons ganz unten auf der Seite).

Verwendet man mehrere LTSP-Server, so muss der Eintrag

```
root path "192.168.<IP >:/opt/ltsp/i386"
```

in der dhcp-Konfiguration des jeweiligen Klassenraums erstellt werden, in dem sich die Terminals befinden, welche auf den dort eingetragenen Terminalserver zugreifen sollen. (Das if-Statement kann in Options-Globals stehen bleiben.)

D.2.2 Dateien/Ordner kopieren

Im Abschnitt D.1 auf Seite 204 wurde u.a. auch das Archiv `ltsp_kernel-3.0.11-i386.tgz` am Terminalserver entpackt und installiert. Folgende der installierten Dateien/Ordner müssen nun von dort ins (neu zu erstellende) Verzeichnis `/srv/tftpboot/lts` des Open School Servers kopiert werden (Anm.: mit einem dos-formatierten USB-Stick kann das Herüberkopieren zu Problemen führen):

- `/tftpboot/lts/2.4.22-ltsp-1/bzImage-2.4.22-ltsp-1`
- `/tftpboot/lts/2.4.22-ltsp-1/pxelinux.0`
- `/tftpboot/lts/2.4.22-ltsp-1/initrd-2.4.22-ltsp-1.gz`
- `/tftpboot/lts/2.4.22-ltsp-1/pxelinux.cfg`

Das waren die Dateien um das booten mittels pxe zu ermöglichen.
Zum Schluss muss noch die Datei für das etherboot-image

`/tftpboot/lts/vmlinuz-2.4.22-ltsp-1`

vom Terminalserver ebenfalls in das Verzeichnis:

`/srv/tftpboot/lts` auf den Open School Server kopiert werden.

D.2.3 Clients anmelden

Damit neue Clients booten können, müssen diese auch am Open School Server angemeldet werden – ohne Anmeldung gelangen die Clients sonst zwar in das pxe-Menü des Open School Servers, welches aber für LTSP nicht eingerichtet ist. Die MAC-Adresse der Clients erhält man z. B., indem man den Client bootet und beim Erscheinen der MAC-Adresse auf (Pause) drückt.

D.3 Weitere (Fein-)Einstellungen beim LTSP

Prozesse von Usern nach deren Ausloggen automatisch stoppen: Es kann vorkommen, dass einige Prozesse von Usern unkontrolliert weiterlaufen, auch wenn sich diese ausgeloggt haben. Dadurch werden natürlich Ressourcen des Servers unnötigt verschwendet. Das folgende kleine Script kann die häufigsten dieser Probleme automatisch beheben, indem es nach jedem Xreset (z. B. nach Abmelden oder einem Xserver-Crash) alle laufenden Applicationen des jeweiligen Users beendet:

Erstellen Sie dazu folgende Datei `/usr/bin/suicide` mit einem Editor:

```
#!/bin/sh
#Suicide!
#this is GPL software, read the license at www.gnu.org
#by Carlos Urbieta Cabrera
#a change suggested by John et al
if [ $USER != root ]; then
  kill -9 `ps aux | grep $USER | awk 'print $2'`
fi
```

Datei 12: *Suicide: Prozesse von Usern automatisch stoppen*

Und machen Sie mit `chmod 0750 /usr/bin/suicide` ausführbar. Ergänzen Sie weiterhin in der Datei `/etc/X11/xdm/Xreset` die entsprechende Zeile mit „suicide“:

```
...
#
case "$DISPLAY" in
    :0|:0.0)
        # Only for display :0  we have to reset the
        # owner ship and permissions of the
        # /dev/xconsole FIFO and the current
        # virtual console /dev/tty0.
```

```
        $XDMDIR/TakeDevices

        # Shut down xconsole started in Xsetup
        # for display :0
        /sbin/killproc    $xconsole
        ;;
    *)
esac
/usr/bin/suicide
```

Datei 13: *Xreset für xdm - Ergänzt um den Aufruf der Datei suicide*

Sollten Sie KDE bevorzugen, so ergänzen Sie ebenfalls die Datei `/opt/kde3/share/config/kdm/Xreset` um die entsprechende Zeile mit „suicide“:

```
#! /bin/sh
# Xreset - run as root after session exits

# Reassign ownership of the console to root, this should
# disallow assignment of console output to any random
# users's xterm. See Xstartup.
#
#chown root /dev/console
#chmod 622 /dev/console

exec sessreg -d -l $DISPLAY $USER
/usr/bin/suicide
```

Datei 14: *Xreset für kdm - Ergänzt um den Aufruf der Datei suicide*

D.3.1 Weitere TrueType-Fonts für OpenOffice.org

Bei der Verwendung von OpenOffice.org sind standardmäßig für die Clients nur sehr wenige Fonts vorhanden. Wenn Sie folgendermaßen vorgehen, können Sie auch an den Clients „vernünftige“ Schriftarten nutzen:

- Als root einloggen.
- In ein beliebiges Verzeichnis die gewünschten TrueType-Fonts (z.B. würden auch die TrueType-Fonts eines Windows-Rechners funktionieren) kopieren.

- Das Programm spadmin von OpenOffice.org mit `/opt/OpenOffice.org/programm/./spadmin` starten.
- In diesem Programm den Button (Schriften) betätigen, danach den Button (Hinzufügen) drücken.
- Dort das oben genannte Verzeichnis mit den TrueType-Fonts suchen und den Button (auswählen) betätigen.
- Schließlich noch den Button (Alle markieren) betätigen und mit (OK) die Schriften zu OpenOffice.org hinzufügen.

Jetzt müssten Ihnen in OpenOffice.org diese TrueType-Fonts zur Verfügung stehen.

D.3.2 Nutzung lokaler Diskettenlaufwerke

Die meisten Informationen hierzu finden Sie unter `http://www.ltsp.org/documentation/floppyd.html`. Im Allgemeinen genügt es, das Archiv Paket `ltsp_floppyd-3.0.tar.gz` von `http://www.ltsp.org/` herunterzuladen und nach Anleitung zu installieren.

Bitte überprüfen Sie mit YaST2, ob das Paket `MToolsFM` schon installiert ist, ansonsten installieren Sie es von der SUSE CD nach.

In der Datei `lts.conf` kann der Wert `RCFILE_01 = floppyd` in 'default' eingetragen werden.

D.3.3 Anleitung zum Erstellen einer Etherboot-Diskette

Für diejenigen, deren Diskless-Clients keine PXE-fähigen Netzwerkkarten besitzen, oder die das Ganze zuerst mit einem anderen Rechner ausprobieren möchten, besteht die Möglichkeit, die Clients mit Hilfe einer „Etherboot-Diskette“ zu booten.

Wir erläutern einmal Stichpunktartig die Erstellung einer solchen Diskette unter Windows9x:

- Die MS-DOS Eingabeaufforderung öffnen
- In den Ordner mit rawrite.exe gehen
- Rawrite.exe starten
- Netzwerkkartendatei auswählen
- formatierte Diskette einlegen

- Client mit dieser Diskette starten

Zusätzliche Netzwerkkarten-Dateien finden Sie unter:

`http://www.rom-o-matic.com/`

Logfiles und Fehlersuche

E.1 Logfiles des Servers

Fast jeder Dienst, welcher auf dem Open School Server eingesetzt wird, bietet die Möglichkeit umfangreiche Logfiles zu erzeugen. Die Art und der Umfang der mitgeloggten Daten ist je nach eingesetztem Dienst und dessen Konfiguration unterschiedlich. So können Sie oft – durch das Setzen eines sog. Debug- oder Log-Levels in der Konfigurationsdatei – den Umfang der ins Logfile geschriebenen Meldungen beeinflussen. Dies bietet sich z. B. bei der Fehlersuche an.

Nachfolgend erhalten Sie einen kurze Erklärung zu einigen Logfiles, welche auf dem Open School Server automatisch eingerichtet und von den verschiedenen Diensten genutzt werden. Wir beschränken uns hier allerdings auf die während des Betriebs des Servers interessanten Dienste. Diese Logfiles befinden sich – soweit nicht anders angegeben – im Verzeichnis `/var/log` bzw. in einem Unterverzeichnis desselben.

Logfiles sind meist reine Textdateien, welche Sie mit jedem beliebigen Editor durchstöbern können. Oft sind nur die gerade aktuellen Meldungen wichtig – dann hilft der Befehl `tail` weiter. Geben Sie z. B. den Befehl `tail -f /var/log/mesages` ein, um einen Live-Mittschnitt dieser Datei am Bildschirm angezeigt zu bekommen. Immer dann, wenn ein Dienst oder der Kernel selbst eine Meldung in diese Datei schreibt, verändert sich auch die Bildschirmausgabe. Reichen die angezeigten 10 Zeilen nicht aus, können Sie mit der Option `-n X` X Zeilen anzeigen lassen. Wenn Sie also die letzten 25 Zeilen sehen möchten, geben Sie `tail -f -n 25 /var/log/messages` ein. Um die Anzeige wieder abzuschalten, brechen Sie den Befehl mit der Tastenkombination (Strg) und (C) ab.

boot.msg Hier werden Meldungen gespeichert, welche der Kernel während des Bootvorgangs ausgibt. Diese Meldungen können Sie auch während des Betriebs mit dem Befehl `dmesg` anschauen. Zur Analyse des Bootvorgangs und bei Hardwareproblemen ist diese Datei also sehr hilfreich. In `boot.omsg` werden übrigens die Meldungen des letzten Bootvorgangs gespeichert.

faillog Jeder fehlgeschlagene Versuch, sich am Server anzumelden wird in dieser Datei gespeichert. Bei dieser Datei handelt es sich ausnahmsweise nicht um eine Textdatei. Informationen aus dieser Datei bekommen Sie deshalb mit dem Befehl `faillog`.

lastlog Hier handelt es sich nicht um eine Textdatei: Sie können sich durch den Befehl `lastlog` anzeigen lassen, welche Benutzer sich am jeweiligen Rechner von wo aus eingeloggt haben. Ein weiterer Befehl, welcher in dieser Hinsicht hilfreich ist, ist der Befehl `last`, der nur die letzten erfolgreichen Anmeldungen (welche in der Datei `wtmp` gespeichert werden) auflistet. Viele Rootkits oder Hacker löschen oder verändern übrigens die Dateien `lastlog` und `wtmp`, um ihre Spuren zu verwischen.

localmessages Diese Datei dient dazu, Meldungen, die den Status „local“ haben, aufzunehmen. Damit wird die Datei `messages` entlastet. Beim Open School Server können hier z. B. die Meldungen des `slapd` geschrieben werden, wenn in dessen Konfigurationsdatei `/etc/openldap/slapd.conf` der Loglevel entsprechend höher gesetzt wird. Wie Sie einzelne Meldungen von solchen Diensten in andere Dateien umleiten können, erfahren Sie im Abschnitt *Der Syslog-Daemon* auf Seite 218.

mail Diese Datei nutzt der Emailserver Postfix, um Informationen über seine Tätigkeiten zu hinterlassen. Hier werden sowohl reine Informationensmeldungen über erfolgreich verschickte Emails als auch Fehler- und Warnmeldungen eingetragen. Sollten Sie also Probleme mit dem Emailsystem haben, ist diese Datei eine gute Anlaufstelle.

messages *Die* Hauptanlaufstelle für alle Administratoren die wissen möchten, was auf Ihrem Server so alles passiert. Hier werden Meldungen des Kernels, Statusberichte und Warnungen einzelner Dienste und natürlich auch Fehlermeldungen protokolliert. Es ist also meist eine gute Idee, bei Problemen erst einmal hier mit den Nachforschungen zu beginnen...

warn Ebenso wie die Datei `messages` eine sehr wichtige Datei: Warnmeldungen von Diensten - etwa der Firewall - werden hier eingetragen, damit der Administrator sich nicht erst durch andere Logfiles wühlen muss, um möglichen Problemen auf die Spur zu kommen.

apache2/access_log Der Webserver Apache führt hier genau Buch über jede an Clients ausgelieferte Webseite. Neben einem Zeitstempel wird also auch die IP-Adresse des Clients und die angeforderte Datei protokolliert.

apache2/error_log Sollten Fehler in Skripten (sogenannten „CGI“-Skripten) auftauchen, die dynamische Seiten generieren; unauthorisierte Zugriffe auf Webseiten

erfolgen oder falsche Seiten angefordert werden, so werden diese hier protokolliert. Wenn Sie also einmal genau wissen wollen, was hinter einem „Error 500 - Server Error!“ steckt, der in einem Browserfenster angezeigt wird, finden Sie in dieser Datei etwas aussagekräftigere Hinweise.

cups/access_log Hier werden vom Druckerserver CUPS sämtliche an ihn gerichteten Anfragen protokolliert.

cups/error_log Wenn es zu Fehlern oder möglichen Problemen in Zusammenhang mit dem Druckserver CUPS kommt, kann ein Blick in diese Datei schnell Klarheit verschaffen: hier meldet der Server Fehler und Warnungen.

samba/log.nmdb Der Wins–Server, welcher als NetBIOS–Nameserver für Windows-Clients fungiert, teilt hier Informationen über seine Arbeit mit.

samba/log.smbd In diesem Logfile notiert der Samba–Server, welcher als Fileserver und Primary Domain Controller für Windows–Rechner fungiert, alle Zugriffe und Fehlermeldungen. Wenn Sie also z. B. Anmeldeprobleme mit Windows–Clients haben, sollten Sie unbedingt einen Blick in diese Datei werfen!

Hier finden Sie für den jeweiligen Client Einträge, die z. B. auf fehlgeschlagene LDAP–Authentifizierungen hinweisen: ein Hinweis, dass der Rechner noch nicht am Open School Server registriert wurde.

squid/access.log Der Proxyserver Squid trägt hier jede vom Client angeforderte Webseite inkl. des Datums, der IP–Adresse des Clients und dem Namen des Benutzers ein. Hier haben Sie als Administrator also einen vollständigen Einblick, wer wann und wo welche Internetseite aufgerufen hat. Zusätzlich führt Squid auch noch auf, ob die angeforderte Seite schon im Cache vorhanden war oder neu aus dem Internet heruntergeladen werden musste.

squid/store.log Hier führt der Proxyserver Squid ein „lesbares“ Logbuch über seinen eigenen Cache, in welchem er einmal angeforderte Webseiten zwischenspeichert, um sie bei einer erneuten Anfrage nicht erneut aus dem Internet holen zu müssen. Sollten

squid/rcsquid.log Wenn der Proxyserver gestartet wird, prüft er u.a. die Syntax in seiner Konfigurationsdatei. Sollte er dort Fehler finden, die ihn nicht vom eigentlichen Start abhalten, so werden diese hier festgehalten. Wenn Sie also die Datei `/etc/squid/squid.conf` verändern, indem Sie z. B. eine neue Regel für Squid über das Webinterface erstellen, diese Regel aber anscheinend nicht angewendet wird, so dürften Sie hier mit ziemlicher Sicherheit einen Hinweis auf den Grund dafür finden.

sysMonitor/* In diesem Verzeichnis speichert der System Monitor, welchen Sie im Webinterface aufrufen können, Informationen. Normalerweise sollte hier aber alles funktionieren, so dass wir uns eine genaue Erläuterung hier ersparen.

uucp/Log Sollten Sie den Server so konfiguriert haben, dass er seine Emails über UUCP austauscht, dann finden Sie hier das entsprechende Logfile, welches über die Verbindungsaufnahme zum UUCP–Server, die ausgetausche Email und evtl. aufgetretene Fehler informiert.

/var/log/squidGuard/squidGuard.log Der „Jugendschutzfilter“ SquidGuard, welcher beim Start von Squid automatisch mitgestartet wird und alle angeforderten Seiten prüft, schreibt in dieses Logfile Informationen über die hoffentlich erfolgreiche Einbindung seiner Datenbanken. Nach einem Update dieser Datenbanken sollte hier ebenfalls eine entsprechende Meldung auftauchen.

/var/log/squidGuard/blocked.log Wenn Sie die entsprechenden Veränderungen in der Konfigurationsdatei von SquidGuard vorgenommen haben (siehe Abschnitt *SquidGuard* auf Seite 199), so loggt SquidGuard jeden geblockten Aufruf einer Internetseite inkl. der Zeit, der IP-Adresse des Clients und des Namens des Benutzers hier mit.

/var/log/squidGuard/get_blacklist.log Hier wird das Update der Blacklists von verschiedenen, im Internet verfügbaren Servern protokolliert. Je nach Konfiguration finden Sie hier nur normale Meldungen über das Herunterladen und Einbinden der Listen oder ausführliche Informationen über jeden einzelnen Schritt des Programms.

E.2 Der Syslog-Daemon

Der Syslog-Daemon ist ein eigenständiges Programm und nimmt Meldungen von anderen Programmen als „zentrale Sammelstelle“ über lokale Sockets oder über das Netzwerk entgegen. Diese schreibt er je nach Konfiguration in verschiedene Logfiles oder schickt sie wiederum an andere Syslog-Daemons weiter.

Die Konfigurationsdatei `/etc/syslogd.conf` steuert dabei, wie Syslog mit den Meldungen der Programme verfährt und hat folgendes Schema:

Facility | Klasse Zuerst wird die Herkunft der Nachricht eingeordnet. Jedes Programm kann dabei die Herkunft seiner Meldungen selbst klassifizieren. Es gibt viele verschiedene Klassen, die leider nicht alle genormt sind. Entsprechend groß ist hier die Anzahl an möglichen Einträgen. Jeder Programm sollte aber irgendwo in seiner Konfiguration Aufschluß darüber geben, an welche Klasse(n) Nachrichten gesendet werden können.

Priorität Die Priorität oder Wichtigkeit einer Meldung unterliegt einer fest vorgegebenen Rangfolge. Dabei haben Meldungen mit der Priorität 0 die höchste Gewichtung. Die niedrigste Gewichtung haben Meldungen mit der Priorität 7. Um besser lesbare Konfigurationen zu bekommen, hat man den Prioritätsstufen zusätzlich noch sprechendere Namen gegeben:

emerg (0) Ein nicht behebbarer Fehler ist aufgetreten. Diese Meldungen haben die allerhöchste Priorität und werden immer protokolliert. (Vergleichbar mit dem „blue screen“ eines bekannten Betriebssystems.)

alert (1) Ein schwerer Fehler ist aufgetreten. Der sofortige Eingriff des Administrators ist notwendig.

crit (2) Eine kritische Situation: das Programm läuft zwar noch, aber irgend ein unvorhergesehenes Ereignis hat einen Fehler produziert.

err (3) Es ist ein Fehler im Programm aufgetreten. Das Programm läuft aber weiter.

warning (4) Das Programm läuft vorläufig weiter, allerdings ist eine Situation aufgetreten, die so nicht geplant war.

notice (5) Ein besonderes Ereignis ist eingetreten. Ein Fehler liegt allerdings nicht vor.

info (6) Normale Routinemeldungen. Das Programm läuft normal.

debug (7) Im Normalbetrieb unwichtige Debuginformationen, die aber für eine Fehlersuche durchaus interessant sein können.

Aktion Hier wird im allgemeinen der Pfad zur Datei angegeben, in welche die entsprechende Meldung geschrieben werden soll. Als weitere Optionen stehen hier noch die Adresse eines anderen Rechners, eine Named Pipe oder ein Sternchen zur Verfügung.

- Eine Logdatei, ein Terminal oder ein Device sollten immer absolut angegeben werden.
- Nach einem Klammeraffen () wird ein anderer Rechner angegeben, an welchen die Nachricht weitergeleitet werden soll.
- Nach einem Pipesymbol (|) folgt der Angabe eines (Datei-)Namens. Daten die in diese Datei geschrieben werden, können nur sequentiell in der gleichen Reihenfolge – dafür aber auch von anderen Prozessen – wieder gelesen werden. Diese Form wird oft für die Kommunikation mit dem Programm xconsole verwendet, um Logmeldungen in einem grafischen Fenster anzeigen zu können.
- Ein Sternchen (*) als Adresse bewirkt eine Ausgabe der Meldungen auf allen TTYs, an welchem gerade Benutzer angemeldet sind.

Folgendes Beispiel für eine Konfigurationsdatei `/etc/syslogd.conf` soll die verschiedenen Möglichkeiten illustrieren:

```
# Alle Meldungen (mit Ausnahme von debug und info) des
# Email-Systems an den Rechner loghost.example.com
# weiterleiten
mail.notice  @loghost.example.com

# Alle Warnungen, Fehler und noch wichtigere Meldungen
# an den Rechner 10.10.0.10 weiterleiten, Meldungen des
# Mailsystems ausgenommen
*.warning;mail.none   @10.10.0.10

# Kernelmeldungen auf der Textkonsole /dev/tty10
# (erreichbar über [Alt]+[F10]) ausgeben
kern.*  /dev/tty10

# Alle Meldungen nach /var/log/messages schreiben -
# dabei vor dem Schreiben erst eine Weile im RAM puffern,
# im das System zu entlasten
*.*    -/var/log/messages

# Meldungen mit der höchsten Fehlerstufe sofort allen
# angemeldeten Benutzern senden
*.emerg  *
```

Datei 15: *Beispiel einer `/etc/syslogd.conf`*

Damit der Syslog-Daemon auch Meldungen von einem anderen System entgegen nimmt, muss er erst entsprechend konfiguriert werden. Dies geschieht durch hinzufügen der Option `-r` in der Variablen `SYSLOGD_PARAMS=`in der Datei `/var/sysconfig/syslog`.

Allerdings nimmt der Syslog-Daemon anschließend Meldungen von *allen* Rechnern entgegen, die ihm solche Nachrichten schicken. Eine Zugriffskontrolle muss über entsprechende Firewall-Regeln realisiert werden.

Server Upgrade

Sollte einmal eine Zeit gekommen sein, in welcher die aktuelle Serverhardware durch ein neues System ersetzt werden soll, stellt sich natürlich die Frage, wie man die bisherigen Daten erhalten – aber trotzdem die neueste Version des Open School Server installieren kann.

Hinweis

Die hier gemachten Angaben sollen bei der Übernahme der alten Daten auf einen neu installiertes System helfen - allerdings können wir keine Verantwortung dafür übernehmen, dass evtl. zusätzliche Veränderungen des Systems durch diese Maßnahmen auch berücksichtigt werden. Bitte stellen Sie also in jedem Fall *vor* der Neuinstallation ein Backup ihres bisherigen Systems her!

Wenn man die Liste mit den jeweils zu stoppenden Diensten betrachtet könnte man auch auf die Idee kommen, den Server einfach in den Runlevel 1 zu fahren, da dort diese Dienste ebenfalls gestoppt werden. Allerdings funktionieren dann die weiter unten beschriebenen Verfahren nicht mehr.

Hinweis

F.1 Daten sichern

Nachfolgend nun eine kurze Übersicht über die einzelnen Arbeitsschritte:

Dienste abschalten Bevor Sie mit der Sicherung beginnen, sollten Sie dafür sorgen, dass niemand mehr auf den Server zugreift. Sie sollten deshalb einige wichtige Dienste anhalten:

- `rcsuad stop`

- `rcdhcpd stop`
- `rccron stop`
- `rcfetchd stop`
- `rcsmprint stop`
- `rcnfsserver stop`
- `rcpostfix stop`
- `rcsmb stop`
- `rcxntp stop`
- `rccups stop`
- `rcldap stop`
- `rcmysql stop`
- `rcnamed stop`
- `rcquota stop`
- `rcrinetd stop`
- `rcsessiond stop`
- `rccyrus stop`
- `rcnmb stop`
- `rcportmap stop`
- `rcsaslauthd stop`
- `rcatalk stop`

/home-Verzeichnis Sichern Sie in jedem Fall das gesammte Homeverzeichnis! Dies können Sie z. B. durch den Befehl `cp -a /home/* <Ziel>` machen. Die Option „-a“ sorgt dafür, dass sämtliche eingestellten Benutzerrechte erhalten bleiben. Das Ziel sollte nach Möglichkeit ein per NFS gemountetes Verzeichnis eines anderen Rechners (z. B. des schon neu aufgesetzten Servers) oder eine andere Festplatte sein. Beachten Sie bitte, dass für eine korrekte Sicherung auf der anderen Platte deren Filesystem auch „ACLs“ unterstützen muss. Wenn Sie sich unsicher sind, dann kopieren Sie *vor* dem Mounten die entsprechende Zeile aus der alten Datei `/etc/fstab`. Anschließend können Sie die Platte wie gewohnt mounten und die Daten kopieren.

/etc-Verzeichnis Im Verzeichnis `/etc` befinden sich die Systemeinstellungen. Dieses Verzeichnis sollten Sie ebenso wie das Homeverzeichnis komplett kopieren. (Hier sind normalerweise ACLs nicht aktiviert.)

LDAP-Datenbank Da in der Datenbank sämtliche Benutzerrechte und Passwörter gespeichert werden, ist Sie genauso wichtig, wie das Systemverzeichnis. Da der LDAP-Server schon gestoppt ist, brauchen Sie nur noch einen sogenannten „Dump“ anzufertigen. Dies geschieht mit dem Befehl `slapcat > LDAP-Backupdatei.ldif`. Damit werden alle Einträge der Datenbank in einer Datei „LDAP-Backupdatei“ (eine Textdatei) gespeichert. Sichern Sie sicherheitshalber trotzdem noch das betreffende Verzeichnis `/var/lib/ldap` mit dem Befehl `cp -a /var/lib/ldap/* <Ziel>`.

Mailboxen Um die Mailbox-Datenbanken der Benutzer zu sichern, geben Sie die folgenden Befehle ein:

- `rcldap start`
- `su - cyrus`
- `ctl_mboxlist -d > /tmp/mboxlist.dump`
- `exit`
- `cp /tmp/mboxlist.dump <Ziel>`

Damit wird auch hier (ähnlich wie beim LDAP-Server) der Inhalt der Mailboxen in einer Datei „mboxlist.dump“ gesichert. Sollten Sie Ihre Email über UUCP austauschen, so sichern Sie bitte auch noch das Verzeichnis `/var/spool/uucp` mit dem Befehl `cp -a /var/spool/uucp/* <Ziel>`.

Nun kommen noch sämtliche IMAP-Daten hinzu:
`cp -a /var/spool/imap/* <Ziel>`

MySQL-Datenbank(en) Hier sichern wir einfach sämtliche Datenbanken und damit auch die Daten der Groupware (wenn noch keine Daten dort eingetragen wurden, können Sie diesen Schritt auch auslassen). Geben Sie dazu die folgenden Befehle ein:

- `rcmysql stop`
- `cp -a /var/lib/mysql/* <Ziel>`

Tipp

rsync nutzen

Wenn Sie auf dem Server rsync installiert haben, können Sie auch dieses Programm anstelle von cp nutzen. Dies wird insbesondere später bei ständigen Sicherungen interessant, da rsync nur diejenigen Datenblöcke überträgt, die auch wirklich geändert wurden. Dies spart Bandbreite und beschleunigt den Backup-Vorgang. Zusätzlich läßt sich die Datenübertragung mit rsync auch verschlüsseln und zusätzlich komprimieren. Ein Beispiel:
`rsync -e ssh -azP /home/* backupserver.example.com:/backup/home`
Wenn vorher die SSH-Schlüssel zwischen den Servern ausgetauscht wurden können Sie so sogar ein Backup über das Internet machen.

Tipp

F.2 Daten wiederherstellen

Um die Daten auf einem neuen System wieder einzuspielen, gehen Sie folgendermaßen vor:

Dienste abschalten Auch hier sollten Sie wieder die betreffenden Dienste temporär abschalten. Ebenso sollten Sie sicherstellen, dass für die `/home`-Partition sowohl Quota- als auch ACL-Support eingeschaltet ist.

MySQL-Datenbanken Geben Sie für die Datenbanken die Befehle:

- `rcmysql stop`
- `rm -r /var/lib/mysql/*`
- `cp -a <Quelle> /var/lib/mysql`

ein.

Mailboxen Geben Sie bitte die folgenden Befehle ein:

- `rcldap start`
- `cp mboxlist.dump /tmp`
- `su - cyrus`
- `ctl_mboxlist -u < /tmp/mboxlist.dump`
- `exit`
- `cp -af <Quelle> /var/spool/imap/`

- (Bei Bedarf auch noch `cp -af <Quelle> /var/spool/uucp` für die UUCP-Transferdaten.)

LDAP-Datenbank Stellen Sie bitte zunächst sicher, dass der LDAP-Server nicht mehr läuft: `rcldap stop` und sicherheitshalber noch `killall -9 slapd`.

Anschließend werden die bisherigen Datenbankdateien entfernt und das Backup eingespielt:

- `rm /var/lib/ldap/*`
- `slapadd -l LDAP-Backupdatei.ldif`

Nun können Sie den LDAP-Server mit dem Befehl `rcldap start` wieder starten.

System- und Homeverzeichnis Das System- und das Homeverzeichnis stellen Sie wieder her, indem Sie den Befehl `cp -af <Quelle> <Ziel>` eingeben. Als Quelle wählen Sie das Backupverzeichnis und als Ziel das Verzeichnis `/etc` bzw. `/home`. Denken Sie hier bitte wieder an die ACLs, mit welchen die entsprechende Partition gemountet sein muss.

Dienste wieder starten Zuletzt werden sicherheitshalber alle weiter oben angehaltenen Dienste wieder in der richtigen Reihenfolge gestartet. Wir führen hier auch diejenigen Dienste auf, welche in den einzelnen Abschnitten schon gestartet wurden - ausser einem entsprechenden Hinweis, dass dieser Dienst schon gestartet ist werden Sie aber keinen Fehler erhalten, wenn Sie diese Dienste nochmal starten.

- `rccyrus start`
- `rcnmb start`
- `rcportmap start`
- `rcsaslauthd start`
- `rcldap start`
- `rcmysql start`
- `rcnamed start`
- `rcquota start`
- `rcrinetd start`
- `rcsessiond start`
- `rccups start`
- `rcnfsserver start`
- `rcpostfix start`

- `rcsmb start`
- `rcxntpd start`
- `rcfetchd start`
- `rcsmbprint start`
- `rccron start`
- `rcdhcpd start`
- `rcsuad start`

Das Rettungssystem

Der Open School Server enthält ein Rettungssystem, mit dessen Hilfe Sie in Notfällen von außen an Ihre Linux-Partitionen auf den Festplatten kommen können: das *„Rescue"–System*, das Sie von Ihrer Installations-CD starten können.

Zum Rettungssystem gehören verschiedene Hilfsprogramme, mit denen Sie Probleme mit unzugänglich gewordenen Festplatten, fehlerhaften Konfigurationsdateien usw. beheben können.

G.1 Das Rettungssystem starten

Nachfolgend die Schritte zum Starten des Rettungssystems:

1. Schalten Sie Ihren Rechner ein und legen Sie die Installations–CD von Open School Server in das Laufwerk.
2. Wählen Sie 'Rescue System' aus und geben Sie – falls notwendig – bei den 'boot options' Parameter an.
3. Nehmen Sie im linuxrc die erforderlichen Einstellungen für die Sprache und die Tastatur vor.
4. Das Rettungssystem wird dekomprimiert, als neues Root-Dateisystem in eine RAM-Disk geladen, gemountet und gestartet. Es ist damit betriebsbereit.

G.2 Das Rettungssystem benutzen

Das Rettungssystem stellt Ihnen unter (Alt) + (F1) bis (Alt) + (F6) sechs virtuelle Konsolen zur Verfügung, an denen Sie sich als Benutzer `root` ohne Passwort einloggen können.

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.

G.2.1 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 16 beschrieben zusammen.

```
/dev/hda1            swap                 swap       defaults
/dev/hda2            /                    ext3       acl,user_xattr
/dev/hda3            /data1               ext3       acl,user_xattr
/dev/hda4            /home                ext3       acl,user_xattr,usrquot
```

Datei 16: *Beispiel /etc/fstab*

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

```
client1:/ #  mkdir /mnt/home
client1:/ #  mkdir /mnt/var
client1:/ #  mount /dev/hda2 /mnt/
client1:/ #  mount /dev/hda3 /mnt/home
client1:/ #  mount /dev/hda4 /mnt/var
```

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, sollten Sie sich einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls

```
client1:~ #  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`.

G.2.2 Passwort zurücksetzen

Sollten Sie sich einmal komplett aus Ihrem normalen System ausgesperrt haben und sich nicht mehr anmelden können, so besteht noch eine Hoffnung auf Rettung: Sie können das entsprechende Passwort zurücksetzen, sofern es sich dabei um einen normalen Account auf dem Rechner handelt.

Hinweis

Passwörter von Nutzern, die in einer LDAP–Datenbank eingetragen sind lassen sich auf die beschriebene Art und Weise nicht ändern. Ebenso wenig können wir hier sämtliche möglichen Orte berücksichtigen, in welchen Programme ein Passwort speichern.

Verwenden Sie diese Möglichkeit also nur, wenn Sie ganz genau wissen, was Sie da tun!

Hinweis

Wir gehen hier davon aus, dass Sie das Passwort des Benutzers `root` vergessen haben und ein neues vergeben möchten.

- Mounten Sie zunächst diejenige Partition Ihres normalen Systems, welche den Pfad `/etc` enthält (siehe G.2.1 auf der vorherigen Seite).
- Wechseln Sie anschließend in das gemountete Verzeichnis und bearbeiten Sie die Datei `shadow` mit dem `vi` (Eine Anleitung finden Sie im Anhang unter **??** auf Seite ??).
- Suchen Sie zunächst die Zeile, welche die Daten des Benutzers `root` enthält. In diese Zeile stehen – durch Doppelpunkte getrennt –
  der Benutzername : sein verschlüsseltes Passwort : Zeit seit der letzten Passwortänderung : minimale und : maximale Zeit zwischen möglichen Passwortänderungen : Zeit, wann zu einer Änderung des Passworts aufgefordert wird, bevor es abläuft : Information, ob das Konto inaktiv ist : Zeit bis zum Ablauf des Kontos : Evtl. ein spezielles „Flag“
- Entfernen Sie nun das verschlüsselte Passwort (zweite Spalte), bis nur noch die beiden Doppelpunkte aneinander stehen, und speichern Sie die Datei.

Anschließend sollten Sie das System neu starten und sich als Benutzer `root` ohne die Eingabe eines Passworts anmelden können. Ändern Sie jetzt z. B. mit dem Befehl `passwd` das Passwort.

SSH: Verschlüsselte Verbindungen

Der Open School Server ermöglicht Ihnen u.a. auch die Fernwartung des Servers über verschlüsselte Verbindungen. Wir wollen nun einmal zeigen, welche Möglichkeiten und zusätzliche Absicherungsmaßnahmen sich speziell durch die Nutzung von SSH-Verbindungen ergeben.

H.1 SSH-Server und SSH Programm

Zunächst einmal sollten Sie wissen, dass es sowohl einen SSH-Server (welcher im Allgemeinen vom Benutzer `root` gestartet wird) wie auch ein SSH-Programm gibt, welches jeder Nutzer einsetzen kann. Der Serverdienst sshd wird normalerweise immer gestartet. Er wird durch die Datei `sshd_config` im Verzeichnis `/etc/ssh` konfiguriert. Wir werden später auf diese Datei zurückkommen.

Zusätzlich gibt es noch einen sicheren „FTP-Server“, welcher eine verschlüsselte Datenübertragung ermöglicht. Dieser wird über den SSH-Server bei Bedarf gestartet und nennt sich `sftp-server`.

Das Programm, welches Sie unter Linux nutzen um eine verschlüsselte Verbindung aufzubauen, wird mit dem Befehl ssh aufgerufen. Zusätzlich wird als Parameter noch der Rechnername erwartet. Weitere Parameter wie z. B. der Nutzername auf dem fremden System, bestimmte Portnummern, Kompression oder X-forwarding sind optional.

Besonders bei der verwendeten Kompressionsstärke sollten Sie später einen Kompromiss zwischen der verfügbaren Bandbreite und der Rechenleistung der beteiligten Computer finden. Heutige Computer sind aber meist so leistungsstark, dass die zusätzliche Belastung durch Kompression meist unerheblich ist - die eingesparte Bandbreite während der Übertragung kann aber durchaus nützlich sein.

Auch hier gibt es noch zusätzliche Programme wie etwa sftp – den sicheren FTP-Client – oder scp – das „secure copy“. Hiermit können Sie – ähnlich wie mit dem normalen cp-Befehl – Dateien und sogar ganze Verzeichnisse geschützt auf ein anderes System kopieren.

H.2 Das Clientprogramm SSH

Wir wollen nun erst einmal eine verschlüsselte Verbindung zu unserem Server aufbauen. Wir gehen dabei davon aus, dass Sie den Server schon über das Webfrontend so eingerichtet haben, dass er seine aktuelle IP-Adresse über DynDNS bekannt macht (siehe *Dynamic DNS* auf Seite 87) und der SSH-Port geöffnet ist (siehe *Externer Zugriff* auf Seite 95).

Für einen einfachen Verbindungsaufbau genügt dann von einem Linux-Client aus der Befehl `ssh root@myip.dyndns.org`.

Tipp

Verbindungsaufbau

Der eigentliche Verbindungsaufbau findet dann zunächst über asymmetrische Verschlüsselung statt. Jeder SSH-Server benötigt zu seinem Betrieb ein solches Schlüsselpaar, welches aus einem öffentlichen und einem privaten Schlüssel besteht. Dieses Schlüsselpaar wird beim Open School Server automatisch erzeugt.

Tipp

Empfängt der SSH-Server eine Verbindungsanfrage, dann sendet er seinen öffentlichen Schlüssel an den Client. Hat dieser noch keinen Schlüssel vom Server erhalten wird der Nutzer gefragt, ob der öffentliche Schlüssel gespeichert werden soll (siehe *Das Clientprogramm SSH*).

```
The authenticity of host 'ssh-server.example.com
(10.10.0.14)' can't be established.
RSA key fingerprint is
c7:08:14:35:c0:86:7b:a5:b1:b6:4f:1c:e4:73:bc:0f.
Are you sure you want to continue connecting (yes/no)?
```

Datei 17: *Anfrage zur Speicherung des öffentlichen Serverschlüssels*

Wenn Sie sicher sind, dass der übertagene, öffentliche Schlüssel wirklich der Schlüssel des angewählten Servers ist, dann bestätigen Sie die Frage mit einem ausgeschriebenen *yes* - andere Eingaben führen hier zum Abbruch der Verbindung. Wenn Sie unsicher sind, sollten Sie den angegebenen Fingerprint mit der Ausgabe des am Server eingegebenen Befehls `ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub` überprüfen. Diese müssen identisch sein.

Nun wird der öffentliche Schlüssel des Servers auf dem Client im Heimatverzeichnis des Benutzers unter `.ssh/known_hosts` gespeichert. Bei allen späteren Verbindungen wird der ssh-Client nur noch überprüfen, ob sich der Schlüssel geändert hat und Sie ggf. mit einer Warnmeldung darauf hinweisen.

Achtung

Man-in-the-middle Angriff

Sollten Sie eine solche Warnung beim Versuch eines Verbindungsaufbaus erhalten, dann sollten Sie zunächst sicherstellen, dass sich das Schlüsselpaar des Servers geändert hat und dann ggf. den zu diesem Server gehörenden Eintrag in der Datei `.ssh/known_hosts` löschen. Vorher ist aus Sicherheitsgründen keine Verbindungsaufnahme möglich, da hier ein sogenannter „man in the middle"-Angriff stattfinden könnte, bei welchem sich ein anderer Rechner als der eigentlich angewählte Server ausgibt. Wenn sich wirklich das Schlüsselpaar des Servers geändert haben sollte, müssen Sie nach dem Löschen der entsprechenden Zeile den öffentlichen Schlüssel erneut importieren, wie unter *Das Clientprogramm SSH* auf Seite 232 beschrieben

Achtung

Tipp

Verschlüsselungsmechanismus

Nachdem der Client nun dem Server vertraut, verschlüsselt er zur endgültigen Einrichtung der Verbindung nun eine große Zufallszahl mit dem öffentlichen Schlüssel des Servers und schickt diese verschlüsselte Datei dann an den Server zurück. Dieser entschlüsselt die Datei mit seinem privaten Schlüssel – was nur der original Server tun kann – und damit wird auch zukünftig die Authentizität des Servers gegenüber dem Client sichergestellt. Alle weiteren Daten werden nun symetrisch verschlüsselt, wobei die vom Client erzeugte Zufallszahl als Schlüssel genutzt wird.

Tipp

Sie sollten also nach dem einmaligen Austausch des Schlüssels zukünftig nur noch nach dem Passwort für `root` gefragt werden, da Sie durch das vorangestellte „root@" dem Server mitgeteilt haben, dass Sie sich mit diesem Nutzernamen am System anmelden möchten. Dasselbe Verhalten erreichen Sie übrigens auch, wenn Sie den folgenden Befehl aufrufen: `ssh -l root myip.dyndns.org`. Wenn Sie den Benutzernamen weglassen, wird der Client versuchen, Sie mit dem Nutzernamen des aktuellen Systems anzumelden. Nun können Sie auf der Konsole des Servers arbeiten.

Im zweiten Schritt möchten wir aber auch mal ein grafisches Programm starten, um z.B. im Konqueror die Homeverzeichnisse zu kontrollieren oder ein wenig zu surfen. Geben Sie dazu auf Ihrem heimischen System den Befehl `ssh -X root@myip.dyndns.org` ein. Durch das `-X` wird X11-Forwarding aktiviert. Damit erzeugt das Programm ssh ein Pseudo-Terminal auf dem Zielrechner und setzt die Umgebungsvariable DISPLAY entsprechend. Die graphischen Ausgaben eines Pro-

gramms werden dann von ssh verschlüsselt weitergeleitet und erscheinen auf dem Clientrechner.

Nach der nun schon bekannten Eingabe des Passworts können Sie nun also auch grafische Programme starten – z. B. den Konqueror mit dem Befehl `konqueror`. Erwarten Sie aber bitte keinen Geschwindigkeitsrausch - besonders nicht bei Wählverbindungen!

Die Geschwindigkeit können Sie aber durch Kompression erhöhen. Hierbei wird ein ähnlicher Algorithmus wie für gezipte Dateien verwendet. Ähnlich dem dortigen Verfahren können Sie auch hier den Grad der Kompression angeben. Wiederholen Sie also die vorherige Anmeldung – nur schalten Sie diesmal mit dem zusätzlichen Parameter „-C“ die Kompression ein: `ssh -C -X root@myip.dyndns.org`. Vergleichen Sie die Geschwindigkeit, mit der der Konqueror nun startet und arbeitet.

Tipp

Einen anderen Port verwenden

Wenn Sie – z. B. aus Sicherheitsgründen – einmal den Port auf dem der SSH-Server auf Anfragen lauscht geändert haben, müssen Sie diese Veränderung dem SSH-Programm bei der Verbindungsaufnahme auch mitteilen. Normalerweise versucht das Programm eine Verbindung auf Port 22 des Zielsystems herzustellen. Wenn nun aber der SSH-Server auf einem anderen Port läuft, können Sie dies wiederum dem Programm mit einem zusätzlichen Parameter einstellen: `ssh -p 222222 -C -X root@myip.dyndns.org`. Hier also Port 222222.

Tipp

Wenn Sie eine stabile Verbindung eingerichtet haben, können Sie die Einstellungen in einer Konfigurationsdatei ablegen und müssen so nicht bei jeder erneuten Verbindung wieder alle Optionen eingeben. Jeder Nutzer kann so in seinem Heimatverzeichnis im Unterverzeichnis `.ssh` eine Datei `config` anlegen und dort entweder für einzelne Rechner, ganze Netzwerke oder global die Optionen für eine Verbindung einstellen.

So könnte eine `config`-Datei einige globale Optionen konfigurieren, so dass z. B. X11-Forwarding aktiviert ist, als Protokoll das sicherere Protokoll 2 verwendet wird, der Nutzernamen auf dem fremden System vorgeben oder Kompression aktiviert wird.

```
Host *
    StrictHostKeyChecking ask
    ForwardX11 yes
    UseRsh no
    FallBackToRsh no
    Compression yes
    BatchMode no
```

```
KeepAlive yes
User root
Protocol 2
```

Datei 18: *Beispiel einer Datei .ssh/config mit globalen Vorgaben für alle Verbindungen*

Mehr Informationen zum Programm ssh erhalten Sie mit `man ssh`. Zur Konfigurationsdatei erhalten Sie mit dem Befehl `man ssh_config` weitere Informationen.

H.2.1 Secure Copy

Das Programm scp ist eine Mischung aus SSH und CP. Wollen Sie also z. B. Datei `test.txt` von daheim auf den Server kopieren, dann geben Sie den folgenden Befehl ein `scp test.txt root@myip.dnydns.org:/root/` Damit kopieren Sie die Datei in das Heimatverzeichnis von `root`. Sie können auch mit Wildcards arbeiten: `scp te*.txt root@myip.dnydns.org:/root/` kopiert alle Dateien, welche mit „te“ anfangen und mit „.txt“ aufhören, ins Heimatverzeichnis von `root`. Beachten Sie aber bitte, dass vorhandene Dateien überschrieben werden! Prüfen Sie also vorher auf dem anderen Rechner, ob nicht fälschlicherweise Dateien überschrieben werden können.

Auch scp bietet Möglichkeiten zur Komprimierung der Daten oder zur Verwendung eines anderen Ports (normalerweise wird auch hier immer Port 22 genutzt). Mit `scp -C -P 222222 test.txt root@myip.dyndns.org:/root/` kopieren Sie also die Datei `test.txt` verschlüsselt und komprimiert über den Port 222222 auf den Server ins Heimatverzeichnis von `root`.

Mehr Informationen zum Programm scp erhalten Sie mit dem Befehl `man scp`.

H.2.2 Secure FTP

Das Programm sftp dient als sicherer Ersatz für FTP. Wie bei einer normalen FTP-Verbindung können Sie verschiedene Dateien und Verzeichnisse zwischen den beiden Zielsystemen hin- und herkopieren, löschen oder verschieben. Die Daten werden dabei ebenfalls über die verschlüsselte Verbindung übertragen und auf Wunsch auch während der Übertragung komprimiert. Mit SFTP-fähigen Clients können Sie also wie mit einem üblichen FTP-Client arbeiten – nur sind hier die Daten und Passörter im Gegensatz zu normalen FTP geschützt.

Mit dem Befehl `sftp -C root@myip.dyndns.org` starten Sie eine verschlüsselte und komprimierte FTP-Sitzung, die Sie mit dem Befehl `quit` wieder verlassen können.

Auch hier liefert der Befehl `man sftp` weitere Informationen zur Benutzung des Programms. Hier werden auch die einzelnen Befehle beschrieben, die während einer SFTP-Sitzung genutzt werden können.

H.3 Der SSH-Server

Wir wollen uns hier nur mit den für den Alltag relevanten Konfigurationsmöglichkeiten des SSH-Servers beschäftigen. Weitere Informationen zu den einzelnen Optionen entnehmen Sie bitte der Manpage zur Konfigurationsdatei (`man sshd_config`). Alle Einstellungen nehmen Sie in der Datei `/etc/ssh/sshd_config` vor.

Hinweis

Bitte erstellen Sie vor Änderungen immer eine Sicherheitskopie der laufenden Konfiguration!

Hinweis

Zusätzlich sollten Sie sich ganz genau überlegen, ob Sie sich wirklich über SSH auf dem Server anmelden sollen, wenn Sie die Konfiguration dieses Servers bearbeiten. Der Server muss nach jeder Änderung in der Konfigurationsdatei die Konfiguration neu laden. Dies betrifft zwar keine laufenden Sitzungen - aber im schlimmsten Fall „sägen Sie sich genau den Ast ab, auf welchem Sie gerade sitzen“.

Editieren Sie die Datei mit einem beliebigen Editor ihrer Wahl, z. B. kate oder dem vi. Zunächst können Sie den Server ein wenig absichern, indem Sie die Zeile `#Protocol2,1` editieren. Indem Sie die # und die 1 entfernen nimmt der Server zukünftig nur noch Verbindungsanfragen von Clients entgegen, welche das sichere Protokoll 2 verwenden. Die Zeile sieht anschließend so aus: `Protocol2`

Wenn Sie eine statische IP-Adresse besitzen sollten können Sie sogar noch weitere Einschränkungen vornehmen und hier die Adresse eintragen von welcher der Server zukünftig nur noch Verbindungen akzeptieren soll.

Weiter unten in der Datei `sshd_config` können Sie von der Passwort-Authentifizierung auf eine Authentifizierung mit PublicKey, Kerberos oder anderen Verfahren umstellen. Damit entfällt für Hacker die Möglichkeit eines Wörterbuchangriffs auf den Server. Im weiteren Verlauf dieser Beschreibung wird die Umstellung auf das PublicKey-Verfahren beschrieben. Für andere Verfahren lesen Sie bitte die Manpage mit dem Befehl `man sshd_config`.

Dazu muss aber zunächst einmal sichergestellt sein, dass die anvisierte Authentifizierungsmethode auch funktioniert. Für die Authentifizierung mit PublicKey-Verfahren benötigt zunächst jeder Benutzer, welcher sich später auf den Server anmelden können soll, ein Schlüsselpaar.

H.4 PublicKey Schlüssel erzeugen und nutzen

H.4.1 ssh-keygen - Schlüsselpaar erzeugen

Das mit ssh-keygen erzeugte Schlüsselpaar dient später als einzige Authorisierungsquelle. Sie sollten also die erzeugten Schlüssel sicher verwahren und niemanden Zugriff darauf gestatten!

Erzeugen Sie mit dem Befehl `ssh-keygen -t rsa -b 2048` ein 2048 Bit langes RSA-Schlüsselpaar. Sie müssen anschließend den Pfad für die späteren Schlüsseldateien angeben `Enter file in which to save the key (/home/hugo/.ssh/id_rsa):`. Sie können hier die Vorgabe verwenden oder sich auch einen sprechenden Namen für Ihr Schlüsselpaar überlegen. Geben Sie dann aber den vollen Pfad zur Datei an. Für das Beispiel werden die Vorgabe einfach übernommen indem (Enter) gedrückt wird.

Nun werden Sie zweimal nach einer „passphrase“ gefragt. Wenn Sie an dieser Stelle einfach (Enter) drücken, wird ein Schlüssel ohne Passwort generiert - dies sollten Sie aus Sicherheitsgründen nicht tun, sondern sich wirklich ein langes Passwort überlegen. Zur Sicherheit müssen Sie diese Passphrase erneut eingeben, bevor das Schlüsselpaar erzeugt wird.

Als Ergebnis sollten Sie zwei Dateien erhalten: `id_rsa` und `id_rsa.pub`. Die Datei mit der Endung „pub“ dürfen Sie an alle weitergeben.

Hinweis

Den privaten Schlüssel `id_rsa` sollten Sie - auch wenn er durch die Passphrase geschützt ist - nicht aus der Hand geben.

Hinweis

Hinterlegt man nun den eigenen öffentlichen Schlüssel auf dem Server in der Datei `~/.ssh/authorized_keys`, so ist es möglich, sich mittels des PublicKey-Verfahrens am Server anzumelden.

H.4.2 Schlüssel hinterlegen

Wenn Sie sich zukünftig als `root` am Server anmelden und dabei das PublicKey-Verfahren nutzen möchten, müssen Sie nun Ihren öffentlichen Schlüssel in die Datei `authorized_keys` im Unterverzeichnis `.ssh` des Heimatverzeichnisses von `root` kopieren.

Kopieren Sie dazu den öffentlichen Schlüssel auf eine Diskette, die Sie dann am Server mounten oder nutzen Sie den Befehl `scp`, um den Schlüssel direkt auf

den Server zu kopieren. Das Einfügen in die Datei `authorized_keys` (die Datei existiert am Anfang noch nicht) geschieht am elegantesten mit dem Befehl `cat id_rsa.pub » /root/.ssh/authorized_keys` – wenn sich der öffentlichen Schlüssel im aktuellen Verzeichnis befindet.

Eine weitere, elegant Möglichkeit bietet der Befehl `ssh-copy-id`. Bei diesem Befehl handelt es sich um ein Shell-Skript, welches den öffentlichen Schlüssel auf einem fremden Rechner hinterlegt und damit genau das tut, was wir im Absatz vorher per Hand gemacht haben. (Da der Befehl allerdings nicht unter allen Systemen verfügbar ist, ist die manuelle Methode sicherlich auch nicht schlechter.)

Um also den Schlüssel `id_rsa.pub` in der Datei `.ssh/authorized_keys` des Benutzers `root` auf dem Server `myip.dyndns.org` zu hinterlegen, geben Sie als normaler Nutzer den folgenden Befehl ein:

```
ssh-copy-id -i  /.ssh/id_rsa.pub root@myip.dyndns.org
```

Geben Sie anschließend das Passwort des Benutzers `root` ein und das Skript ssh-copy-id nimmt ihnen die weitere Arbeit ab.

Um Sicherheitslücken zu vermeiden, sollten Sie darauf achten, dass die Datei `authorized_keys` nur vom jeweiligen Benutzer lesbar ist. (Der SSH-Server achtet übrigens auch darauf und schaltet auf Passwortanmeldung um, wenn die Rechte dieser Datei nicht stimmen! Wenn der Serveradmin dann eine Anmeldung mit Passwort nicht zuläßt stehen Sie vor einem verschlossenem System - ohne Schlüssel.) Dies stellen Sie mit dem Befehl sicher: `chmod 600 authorized_keys`

Nun sollten Sie sich über das PublicKey-Verfahren am Server anmelden können (siehe *Das Clientprogramm SSH* auf Seite 232).

Hierfür sind die folgenden normalerweise auskommentierten Werte (dies sind die Standardwerte) in der Datei `/etc/ssh/sshd_config` verantwortlich:

```
#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
```

RSA-Authentifizierung mittels PublicKey-Verfahren ist also aktiviert (und steht in der Datei noch vor der Passwort-Authentifizierung) und der SSH-Server sucht die öffentlichen Schlüssel im Homeverzeichnis des entsprechenden Nutzers in der Datei `.ssh/authorized_keys`.

Sie sollten also nach einem `ssh -X -C root@myip.dyndns.org` nach Ihrer Passphrase und nicht mehr nach dem Passwort von `root` gefragt werden.

Nun kann am SSH-Server auch die Authentifizierung mittels Passwort abgeschaltet werden. Hierzu muss in der Datei `/etc/ssh/sshd_config` die Zeile

```
#PasswordAuthentication yes
```

geändert werden in

```
PasswordAuthentication no.
```

Anschließend sollte der SSH-Server noch von dieser Änderung durch den Befehl `rcsshd reload` erfahren. Nun werden Benutzer ohne PublicKey zwar immer noch nach dem Passwort gefragt - aber anmelden kann man sich auch mit dem korrekten Passwort eines Nutzers nicht mehr. Nur noch Nutzer mit einem auf dem System hinterlegten PublicKey haben Zugang zum Server.

H.5 SSH-Verbindungen unter Windows

Für eine SSH-Verbindung von Windows zum Open School Server benötigen Sie die beiden Programme Putty und Puttygen, welche Sie unter den angegebenen URLs herunterladen können:

- `http://the.earth.li/~Esgtatham/putty/latest/x86/putty.exe`
- `http://the.earth.li/~Esgtatham/putty/latest/x86/puttygen.exe`

H.5.1 Schlüsseldatei für Putty nutzbar machen

Um die Schlüsseldatei `id_dsa` mit Putty überhaupt nutzen zu können, benötigen Sie das Programm Puttygen.

Nach dem Start drücken Sie auf (Load) um die Datei `id_dsa` zu laden (siehe Abbildung *Schlüsseldatei für Putty nutzbar machen* auf der nächsten Seite).

Anschließend geht es weiter mit der Suche nach der Datei. Sie sollten die Datei auf Diskette, USB-Stick oder CD speichern und auf das Speichermedium gut Acht geben!

Im nächsten Schritt erzeugen Sie jetzt aus der Datei einen Schlüssel, welchen Putty verwenden kann. Das geschieht mit einem Klick auf (OK).

Jetzt müssen Sie die neu erzeugte Datei für Putty nur noch abspeichern. Dazu wählen Sie im Hauptfenster 'Save private-key' und als Speicherort z. B. wieder das transportable Speichermedium auf welchem sich auch schon die andere Schlüsseldatei befindet. Die Parameter können Sie ignorieren, da Puttygen nur den schon vorhandenden Schlüssel angepaßt und keinen neuen generiert hat.

Jetzt können Sie den neuen Schlüssel abspeichern. Eine Passphrase kann hier zusätzlich angegeben werden.

Geben Sie anschließend einen Namen für die neue Datei an (siehe Abbildung *Schlüsseldatei für Putty nutzbar machen* auf Seite 243)

Und Sie sind mit den Vorarbeiten fertig.

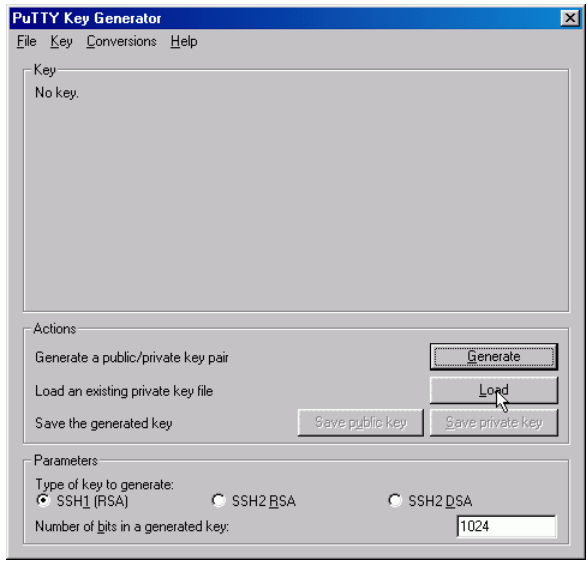

Abbildung H.1: *PuttyGen: Laden des öffentlichen RSA-Schlüssels*

H.5.2 Putty konfigurieren

Nun müssen Sie das Programm Putty noch für die Verwendung des Schlüssels konfigurieren. Geben Sie den Speicherort der Schlüsseldatei angeben. Dies geschieht unter 'Connection' → 'SSH' → 'Auth' → 'Private key file for authentication' (siehe Abbildung *Putty konfigurieren* auf Seite 244).

Ausserdem können Sie auch den Nutzernamen für den Server angeben. Diesen stellen Sie unter 'Connection' → 'SSH' → 'Auth' → 'Auto-Login Username' ein. Geben Sie hier `root` ein. Um sicherzustellen, dass Putty und der Server die Verbindung mit der besseren SSH-Verschlüsselung (Version 2) verschlüsseln, weisen Sie Putty entsprechend unter 'Connection' → 'SSH'.

Nun sollten Sie die Einstellungen abspeichern, damit Sie sie nicht jedes Mal wieder eingeben müssen. Geben Sie vorher noch die richtige IP-Adresse des Servers und den Port in die dafür vorgesehenen Felder ein. Dann brauchen Sie sich wieder nur einen aussagekräftigen Namen zu überlegen und auf (Save) zu drücken (siehe Abbildung *Putty konfigurieren* auf Seite 245. Achten Sie allerdings bei dynamischer IP-Vergabe darauf, dass Sie bei zukünftigen Sitzungen die IP wieder anpassen müssen! (Wenn Sie statt dessen den DynDNS-Namen des Servers verwenden ist dies nicht nötig.) Um eine Verbindung aufzubauen wählen Sie die gespeicherte Sitzung, drücken Sie auf (Load) und ändern Sie dann einfach nur die IP-Nummer.

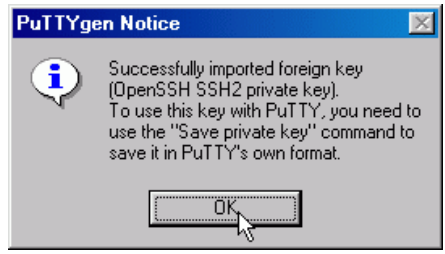

Abbildung H.2: *PuttyGen: Schlüsseldatei importieren und konvertieren*

Jetzt fehlt nur noch eine passende Verknüpfung auf dem Desktop und dem automatisierten Anmelden steht nichts mehr im Wege. Wenn Sie unter den 'Eigenschaften' der Verknüpfung hinter einem @ noch den gespeicherten Namen der Verbindung angeben, dann nimmt Putty diese Werte automatisch beim Start als Parameter an und es genügt ein Doppelklick auf das Icon zum Aufbau der Verbindung.

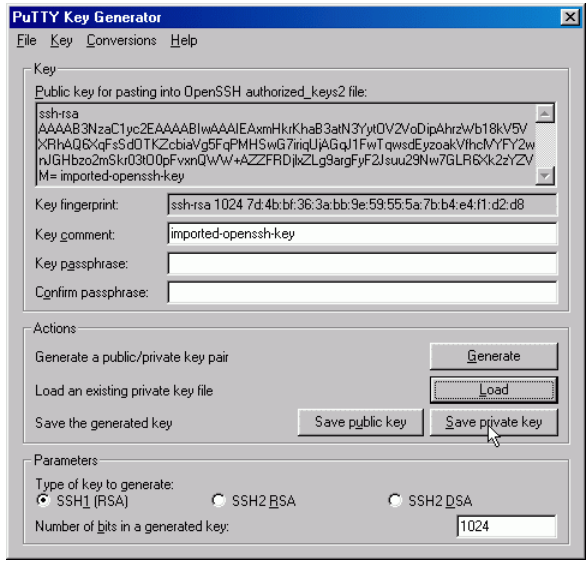

Abbildung H.3: *PuttyGen: Parameter für den neuen Schlüssel*

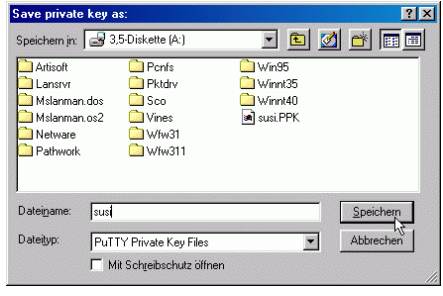

Abbildung H.4: *PuttyGen: neue Datei speichern*

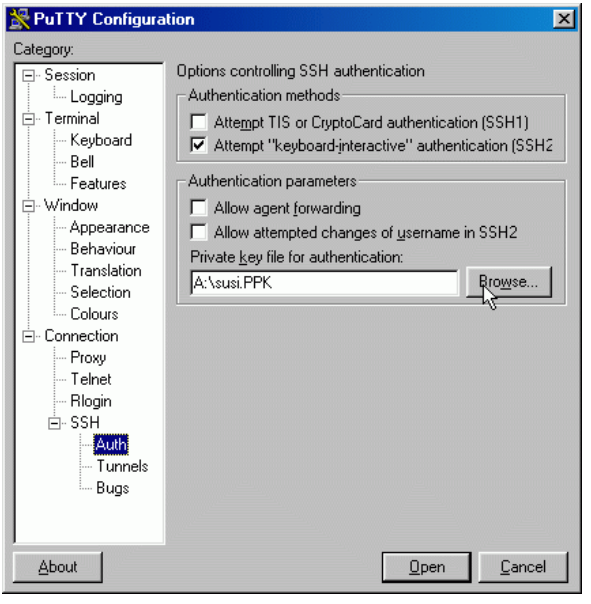

Abbildung H.5: *Putty: Speicherort der Schlüsseldatei angeben*

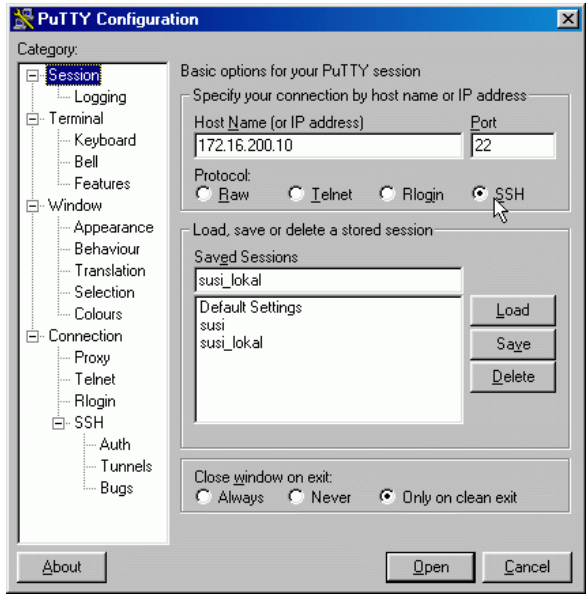

Abbildung H.6: *Putty-Hauptseite: IP-Adresse, Protokoll und Namen eingeben*

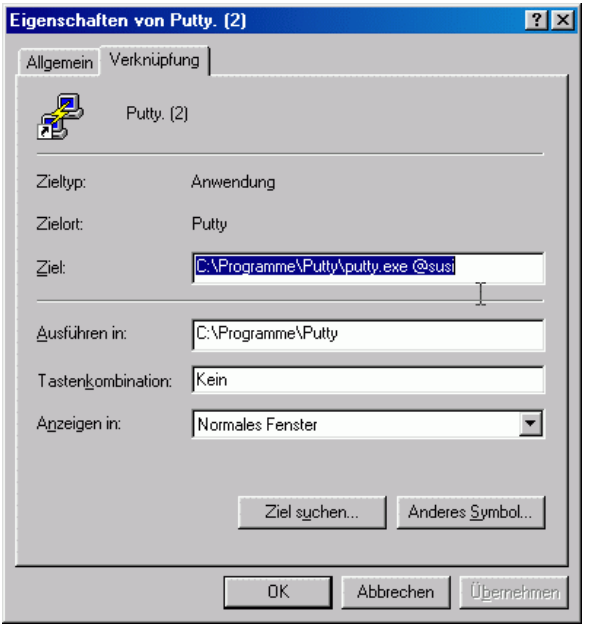

Abbildung H.7: *Putty: automatisierte Anmeldung einrichten*

Glossar

CA (engl. *Certification Authority*)
Eine Certification Authority ist berechtigt, Zertifikate für Server und Clients auszustellen. An Hand der Zertifikate kann geprüft werden, ob Server und Clients diejenigen sind, die sie behaupten zu sein.
Der Open School Server beinhaltet eine solche CA.

Um einem Client außerhalb des lokalen Netzes einen sicheren Zugang zum Server zu gewähren, muss dieser seine Echtheit durch ein Zertifikat nachweisen. Zur Überprüfung muss das Zertifikat der CA auf dem Client gespeichert sein. Hat wiederum der Server kein Zertifikat, zweifeln manche Clients die Echtheit an und verweigern den Verbindungsaufbau.

CSV (engl. *Character Separated Values*)
Eine CSV-Datei ist eine tabellarisch strukturierte ASCII-Text-Datei (Tabelle), deren Elemente (Felder) durch ein bestimmtes Trennzeichen getrennt werden.

Das Trennzeichen darf nicht in Datenelementen vorkommen, oder es muss durch ein Maskierungszeichen als normales Zeichen gekennzeichnet werden. Das Trennzeichen muss nicht (wie meist) ein Komma sein, auch Semikolon, Doppelpunkt, Tabulator und andere Zeichen sind üblich.

Einzelne Datensätze werden in der Regel durch einen Zeilenumbruch (bei Windows: CR LF = carriage return, line feed - ASCII 13 und 10; bei Unix: nur LF - ASCII 10; bei MacOS: nur CR - ASCII 13) getrennt. Wie dieses Trennzeichen und der Zeilenumbruch realisiert wird, ist für den Import der Nutzerdaten beim Open School Server egal. Hauptsache in der ersten Zeile stehen die Feldnamen.

CSV-Dateien tragen auch oft die Dateiendung .txt, statt .csv und können auch in jedem Texteditor erstellt und bearbeitet werden.

DNS (engl. *Domain Name Service*)
siehe ‘Nameserver’, S. 248

Filter
Filter werden zur eingeschränkten Auflistung von Einträgen verwendet.

Im einfachsten Fall ist der Filtereintrag ein `'*'` (Stern) als universeller Platzhalter für ein oder mehrere beliebige Zeichen. So würde bspw. als Filter die Eingabe von `sch*` alle Namen auflisten, die mit der Buchstabenkombination „sch“ beginnen; `*sch*` alle Namen, die „sch“ enthalten.

Gruppen
Eine Gruppe beinhaltet verschiedene Benutzer, die für einen bestimmten Zweck dieselben Rechte oder Eigenschaften erhalten. Die Benutzer verschiedener Gruppen teilen sich so Rechte auf Dateien oder Ordner.
Ein Benutzer gehört immer mindestens einer Gruppe an. Im Open School Server ist dies in erster Linie die primäre Gruppe `students` oder `teachers`. Jeder Benutzer kann weiteren Gruppen angehören, die als sekundäre Gruppen bezeichnet werden.

LDAP (engl. *Lightweight Directory Access Protocol*)
Der Open School Server verwendet eine Datenbank, um nahezu alle Benutzerinformationen zu speichern. Auf diese Datenbank wird mittels LDAP zugegriffen. Externe Clients können über Port `389` Kontakt mit dem Server aufnehmen. Die BaseDN (engl. *Base Distinguished Name*) ist dabei „die oberste Ebene“ der hierarchisch aufgebauten Verzeichnisstruktur. So wäre dies z. B. für die Domain `firma.de`: dc=firma, dc=de.
Weitere Erläuterungen finden Sie unter `http://www.openldap.org/`

Nameserver (DNS)
Ein Nameserver dient zum Auflösen von Rechnernamen in IP-Adressen und umgekehrt. Der Open School Server hat einen eigenen Nameservice zur Verwaltung seiner Domains. Dazu wird BIND8 verwendet, dessen Konfigurationsdateien unter `/var/named/` sowie `/etc/named.conf` zu finden sind. Diese Dateien werden bei der Installation sowie beim Anlegen von virtuellen Domains automatisch generiert (‘Exportieren’). Für eine manuelle Bearbeitung verwenden Sie bitte die Vorlagedatei `/etc/named.conf.in`.

Soll Ihr Open School Server den Nameservice offiziell im Internet delegieren, so benötigen Sie einen weiteren Nameserver und sollten ebenfalls einen Mailserver als „Backup–Mailserver“ eintragen. Dafür sind weitere NS (engl. *Name Service*)– und MX (engl. *MaileXchanger*)–Einträge nötig. Klicken Sie dazu auf ‘System’ → ‘LDAP Browser’ und wählen Sie ‘Suche starten’. Anschließend klicken Sie auf das Kreuz vor ‘o=DNS’ und wählen den Link mit Namen ‘relativeDomainName=@’. In dem folgenden Dialog können zusätzliche NS– oder MX–Einträge hinzugefügt werden, indem Sie unter ‘Neu’ in das Eingabefeld z. B. mXRecord sowie als Wert im Feld daneben die Priorität und den Namen des Mailservers

eintragen. Um diese Änderungen wirksam zu machen, klicken Sie im Hauptmenü auf 'Virt. Benutzer' → 'Virt. Domains' → 'Exportieren'.

Ordner

Ordner sind im Prinzip Postfächer, in denen Mails abgelegt werden können. Jeder Benutzer hat einen sog. „privaten" Ordner (`INBOX`). Ein Benutzer kann durch die Rechtevergabe für seine `INBOX` diesen zu einem gemeinsamen Ordner freigeben. So können verschiedene Benutzer diesen auf unterschiedliche Art (lesend, schreibend) nutzen. Allerdings ist es sinnvoller, einen Unterordner wie den schon standardmäßig vorhandenen Ordner `INBOX.public` als gemeinsamen Ordner mit anderen Benutzern zu teilen.

Quota

Der den Benutzern zur Verfügung gestellte Speicherplatz kann mit Hilfe von Quota begrenzt werden. Dies wird empfohlen, da mit wachsender Anzahl an Benutzern und aufbewahrten Mails der Platz auf der Festplatte schrumpft. So beträgt bei 200 Benutzer mit durchschnittlich 5 MB Platzbedarf der Speicherplatzbedarf der Festplatte bereits 1000 MB.

UID (engl. *User Identification*)

Dies ist der Login-Name, mit dem sich ein Benutzer am Server anmeldet. Er darf maximal acht Zeichen lang sein und keine Sonderzeichen oder Leerstellen enthalten, nur aus Kleinbuchstaben bestehen und muss eindeutig sein. Für davon abweichende E-Mail-Adressen müssen Aliase verwendet werden.

Zertifikat

Ein Zertifikat ist der „Personalausweis" für einen Benutzer, der ihm gestattet, bestimmte Dienste auf dem Open School Server zu verwenden. Das Benutzerzertifikat wird lokal auf dem jeweiligen Client gespeichert und sollte anderen Benutzern nicht zugänglich sein. Beispielsweise kann es ausschließlich Benutzern mit Zertifikat erlaubt sein, eine sichere Verbindung zum Server aufzubauen (siehe auch 'CA', S. 247)

Merkzettel

J.1 Hardwareinformationen

Versuchen Sie hier möglichst umfangreiche Angaben zur Hardware des Servers zu sammeln.

REGCODE: (Produktregistrierungscode)			
Prozessor(en):		Grafikkarte:	
Mainboard:		Arbeitsspeicher (RAM):	
SCSI– oder Raid–Controller	Hersteller,Serie	Treiber	
Festplatte(n)	Hersteller,Serie		
Netzwerkkarten			
Adresse eth0	Typ,Treiber	Netzmaske	MAC-Adr.
Adresse eth1	Typ,Treiber	Netzmaske	MAC-Adr.

Adresse eth2	Typ,Treiber	Netzmaske	MAC-Adr.
ISDN-Karte	Hersteller, Treiber		

J.1.1 Partitionierungsdaten der Festplatte(n)

Sollte einmal eine Festplatte ausfallen oder Sie versehentlich die Partitionstabelle zerstören, können die hier angegebenen Daten manchmal noch weiterhelfen. Tragen Sie einfach die Werte ein, die Sie dem Partitionierer von YaST2 entnehmen können.

Gerät	Größe	Typ	Mountpoint	Start-	Endzylinder	Raid

J.2 Passwörter

Auch wenn es aus Sicherheitsgründen sicher eine schlechte Idee ist, die Passwörter des Servers zu notieren: Im Falle der Abwesenheit des Administrators kann ein solcher Zettel – wenn er unter Verschluss aufbewahrt wird – im Notfall die Rettung sein.

Achtung

Bewahren Sie die hier notierten Passwörter in einem versiegelten, undurchsichtigen Umschlag auf und hinterlegen Sie ihn an einem sicheren Ort.

Vor einer Öffnung sollte in jedem Fall der Administrator informiert werden!

Achtung

Bereich	**Account**	**Passwort**	**Bemerkung**
`Internet`			Providerdaten
`Server-BIOS`			
`Server-Root`	`root`		
`Administrator`	`admin`		

J.3 Einwilligung zur Speicherung von Daten

Hinweis

Bei den unten aufgeführten Dokumenten handelt es sich um Vorlagen, welche wir kostenlos für die Erstellung eigener Ausfertigungen zur Verfügung stellen. Die Firma SUSE lehnt jegliche Verantwortung für die Richtigkeit und rechtlichen Korrektheit dieser Vorlagen ab. Insbesondere eine Überprüfung, ob die hier geforderten Aussagen auch dem jeweils geltenden Schulrecht im betreffenden Bundesland entsprechen, obliegt einzig und allein der jeweiligen Schulleitung.

Hinweis

J.3.1 Elternbrief

An die Eltern
Name der Schule

Datum:

Name des Schulleiters

Liebe Eltern/Erziehungsberechtigten!

Unsere Schule bietet Ihrem Kind neben einem persönlichen Zugang zum schuleigenen Computersystem einen Internetzugang und eine persönliche E-Mail Adresse.
Der Interneteinsatz und die Verwendung von E-Mails dient der Ausbildung von IKT-Fertigkeiten (Informations-/Kommunikationstechnologie) des Kindes.

Bitte lesen Sie die Regelungen für zulässigen und verantwortungsvollen Gebrauch der informationstechnischen Anlage (IT-Anlage) und des Interneteinsatzes (Benutzerordnung - siehe Anhang 1) und unterschreiben Sie das Zustimmungsformular (Anhang 2) damit Ihr Kind das Internet und die IT-Anlage in der Schule verwenden kann.

Da es einige Bedenken bezüglich Zugang zu unerwünschten Materialien im Internet gegeben hat, hat die Schule Regeln erstellt und Filtersoftware installiert, um diese Risiken so gering wie möglich zu halten. Dennoch bitten wir Sie, folgende Punkte zur Kenntnis zu nehmen:

Die Schule hat jede mögliche Vorkehrung getroffen, um die Schüler vor ungeeigneten Materialien zu schützen, Sie kann aber nicht für die Art oder den Inhalt von Materialien im Internet verantwortlich gemacht werden.
Die Schule ist nicht haftbar für Beeinträchtigungen, die das Kind von der Benutzung des Internets davongetragen hat.
Wenn Sie Kommentare zu diesen Regeln anbringen möchten oder Vorschläge für zusätzliche Regeln haben, dann vereinbaren Sie bitte telefonisch einen Termin oder schicken Sie uns eine E-Mail.

Hochachtungsvoll

Name

Anlagen:
1x Benutzerordnung
1x Zustimmungserklärung (Eltern/ Erziehungsberechtigte)
1x Zustimmungserklärung (Schüler)

J.3.2 Zustimmung zur Benutzerordnung für die informationstechnische Anlage, den Internetzugang und zur Internetveröffentlichung von Arbeiten und Fotos (Schüler)

Nichtzutreffendes bitte streichen.

Name des Schülers:

Klasse:

Datum:

Ich habe die Benutzerordnung für den Umgang mit der informationstechnischen Anlage (IT-Anlage) und dem Internetzugang der Schule gelesen und verstanden.

Ich werde das Computersystem und das Internet verantwortungsvoll benutzen und die Regeln jederzeit beachten.

Ich bin mir bewusst, dass nach einer bestimmten Anzahl an vorsätzlichen Verletzungen dieser Regeln, die Schule automatisch meinen Zugang löscht und/oder Maßnahmen einleitet, die wie ein Verstoß gegen die Schulordnung behandelt und entsprechend geahndet werden.

Ich bin darüber informiert worden, dass über meine Tätigkeiten und die von mir aufgerufenen Internetseiten Logdateien geführt werden und diese für eine spätere Auswertung gespeichert werden.

Ich bin mir bewusst, dass die Administratoren des Systems Einblick in die von mir gespeicherten Daten nehmen und diese unter besonderen Umständen auch löschen.

Ich bin mir ebenso bewusst, dass für die Sicherheit der von mir gespeicherten Daten nicht garantiert werden kann und ich von wichtigen Daten zusätzliche Sicherheitskopien anfertigen muss.

Ich bin damit einverstanden, dass meine Arbeiten auf der schuleigenen Webseite präsentiert werden dürfen.

Ich bin außerdem einverstanden, dass Fotos, die mich zeigen, gemäß den Regeln der Schule (es werden keine Namen verwendet) veröffentlicht werden.

Ort, Datum Unterschrift des Schülers

J.3.3 Zustimmung zur Benutzerordnung für die informationstechnische Anlage, den Internetzugang und zur Internetveröffentlichung von Schülerarbeiten und Fotos (Eltern/ Erziehungsberechtigte)

Nichtzutreffendes bitte streichen.

Ich habe die Benutzerordnung für den Umgang mit der informationstechnischen Anlage (IT-Anlage) und dem Internetzugang der Schule gelesen und verstanden und erlaube meinem Kind, die IT-Anlage und den Internetzugang zu verwenden.

Ich weiss, dass die Schule alle nötigen Vorkehrungen trifft, die Schüler vor ungeeigneten Materialien zu schützen und fernzuhalten.

Ich stimme zu, dass die Schule nicht verantwortlich ist für die Art und den Inhalt von Internetmaterialien und für Beeinträchtigungen, die aus dem Internetgebrauch entstehen, nicht haftbar gemacht werden kann.

Ich bin darüber informiert worden, dass die Schule Logdateien speichert, welche Aufschluss über die an der IT-Anlage ausgeführten Tätigkeiten und die aufgerufenen Internetseiten für jeden Benutzeraccount geben.

Ich bin auch darüber informiert worden, dass die Administratoren der Schule die Möglichkeit haben Einblick in die auf der Anlage gespeicherten Dateien meines Kindes zu nehmen und für die Sicherheit dieser Daten nicht garantieren können.

Ich bin damit einverstanden, dass die Arbeiten meines Kindes auf der schuleigenen Webseite präsentiert werden dürfen.

Ich bin außerdem einverstanden, dass Fotos, die mein Kind zeigen, gemäß den Regeln der Schule (es werden keine Namen verwendet) veröffentlicht werden.

Ort, Datum Unterschrift

Name des/der Unterzeichners/Unterzeichnenden in Blockbuchstaben: