SUSE LINUX

School Server

Benutzer– und Administrationshandbuch

1. Auflage 2004

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

Autoren: Ralf Haferkamp, Carsten Höger, Jana Jaeger, Lars Rupp, Thomas Siedentopf, Robert Simai, Péter Varkoly
Redaktion: Roland Haidl, Edith Parzefall
Layout: Manuela Piotrowski, Thomas Schraitle
Satz: LaTeX

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

Inhaltsverzeichnis

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.

Konzeption des Handbuches

Da die zukünftigen Administratoren des SUSE LINUX School Servers nach unserer Erfahrung oft über sehr geringe Kenntnisse im Umgang mit Computern und speziell mit Linux-basierten Systemen verfügen, versucht dieses Buch diesem Umstand mit einer ausführlichen Darstellung der für die normale Administration notwendigen Handgriffe Rechnung zu tragen.

Wer tiefer in die entsprechenden Grundlagen des SUSE LINUX School Servers einsteigen möchte, den möchten wir an dieser Stelle auf die vielen Handbücher (z.B. von SuSE PRESS siehe `http://www.susepress.de/`) und Informationsmöglichkeiten im Internet verweisen. Für die normalen Anforderungen, die an den Server im Schulalltag gestellt werden, sollten Sie jedoch mit diesem Handbuch gut gerüstet sein.

Fortgeschrittene Anwender können durch das umfangreiche Inhaltsverzeichnis oder das Glossar am Ende des Buches schnell die für sie relevanten Themen nachschlagen.

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 SUSE LINUX 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 auf Seite 39) und die anschließende Grundkonfiguration des Servers (siehe Abschnitt 3 auf Seite 49) unterscheiden sich von einer normalen SuSE Linux Installation.

Über die eigentliche Administration im laufenden Betrieb informiert Sie das Kapitel 4 auf Seite 57, 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 A auf Seite 221 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.

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 SUSE LINUX 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.

Unser Ziel war und bleibt es, ein Produkt zu entwickeln, das die Bedürfnisse der Schulen weitestgehend abdeckt. Da die Größe der Schulen recht unterschiedlich sein kann, haben wir einen sehr hohen Wert auf die Skalierbarkeit unseres Produkts gelegt.

Informationen zum SuSE Linux Enterprise Server sowie den Basisprodukten finden Sie auf der SUSE LINUX School Server CD im Verzeichnis `doku`.

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

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

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
`erde:~ # ls`	Eingabe von `ls` auf der Shell des Benutzers `root` im Homeverzeichnis auf dem Rechner „Erde“
`tux@erde:~ > ls`	Eingabe von `ls` auf der Shell des Benutzers `tux` (offizieller Name des Linux-Pinguins) im Homeverzeichnis auf dem Rechner „Erde“
`C:\> fdisk`	DOS-Prompt mit der Befehlseingabe `fdisk`
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 SUSE LINUX 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.

Dennoch sollten Sie nicht einfach die CD in das Laufwerk schieben und „losinstallieren“. Auch wenn alles sehr schnell geht, sind die einzelnen Schritte sehr komplex. Viele Teilelemente müssen bedacht und aufeinander abgestimmt werden.

Sie sollten sich vor der eigentlichen Installation ein paar Gedanken zum Einsatz des SUSE LINUX School Servers machen und dies auch schriftlich festhalten – das erspart Ihnen mit Sicherheit später eine Menge Arbeit.

Im Anhang J auf Seite 287 finden Sie einen kleinen Merkzettel, den Sie dazu nutzen sollten. Je genauer Sie hier die Informationen über Ihren SUSE LINUX School Server aufschreiben, desto leichter fällt später die Wartung und Pflege des Systems.

Hardwarevoraussetzungen

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

- Als Hauptspeicher empfehlen wir mindestens 256 MB – besser sind jedoch 512 MB und mehr.
- Eine CPU mit mindestens 400 MHz (K6, Celeron, Pentium II). Empfohlen: 1 GHz (Athlon, PIII) und mehr.
- Festplattenkapazität mindestens 20 GB. Empfohlen: 40 GB und mehr.
- Von SuSE Linux unterstützte Netzwerkkarte(n). Wenn Sie den Server ohne eine Internetanbindung oder nur über ISDN oder Modem betreiben möchten, reicht eine Netzwerkkarte aus. In allen andern Fällen empfehlen wir Ihnen mindestens 2 separate (unterschiedliche) Netzwerkkarten.
- Eine von SuSE Linux unterstützte VGA–Karte. Empfohlen wird eine Grafikkarte und ein Monitor mit einer Auflösung von 1024x786 bei mindestens 75 Hz Bildwiederholungsrate.

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 Memtest – siehe *Weitere Optionen* auf Seite 20) mindestens 24 Stunden laufen lassen.
- SCSI-Platten sind für erhöhte Laufzeiten ausgelegt und damit meist langlebiger als vergleichbare IDE–Festplatten.
- Beachten Sie bitte die Wärmeentwicklung von Prozessor und Festplatten. Ein Wärmestau im Gehäuse sollte unbedingt vermieden werden!

- Es hat sich als vorteilhaft herausgestellt, Netzwerkkarten von unterschiedlichen Herstellern zu verwenden. Dies verhindert, dass für die gleiche Hardware derselbe Treiber zuständig ist und somit später die Zuordnung zu einzelnen Netzwerkbereichen schwer nachvollziehbar sein kann.
- 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.
- 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.
- Die Firmware bzw. das BIOS ist für die Initialisierung der Rechnerhardware zuständig. Sie hat entscheidenden Einfluss auf die Stabilität des Systems. Sollten Hardwareprobleme auftreten, so überprüfen Sie, ob sich die Probleme mit einem BIOS–Update beseitigen lassen.
- Bitte stellen Sie den Server nicht an einem öffentlich zugänglichen Platz auf. Unbeabsichtigte Stöße wären hier noch das kleinste Übel: Ein offen zugänglicher Server stellt ein großes Sicherheitsloch dar! Ein Server (und auch die Netzwerkhardware) gehört in einen geschützten Bereich, zu welchem nur berechtigte Personen Zutritt haben. Sollten Sie keinen eigenen Raum für die Hardware zur Verfügung haben, reicht oft auch schon ein abschließbarer Schrank, welcher „um eine Steckdose herumgebaut“ wird und in welchem auch noch Platz für den Internet–Anschluß und die Netzwerkverkabelung ist.

Die Netzwerkstruktur des SUSE LINUX School Server

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 SUSE LINUX School Server erreicht werden können.

- Das zweite Teilnetz wird für neue, provisorische oder nicht stationäre Arbeitsplätze reserviert.
- In den weiteren Teilnetzen werden die stationären Arbeitsplätze der Schule geordnet unterbracht. Dazu wird jedem Schulraum ein eigener IP-Adressenbereich zugeordnet.

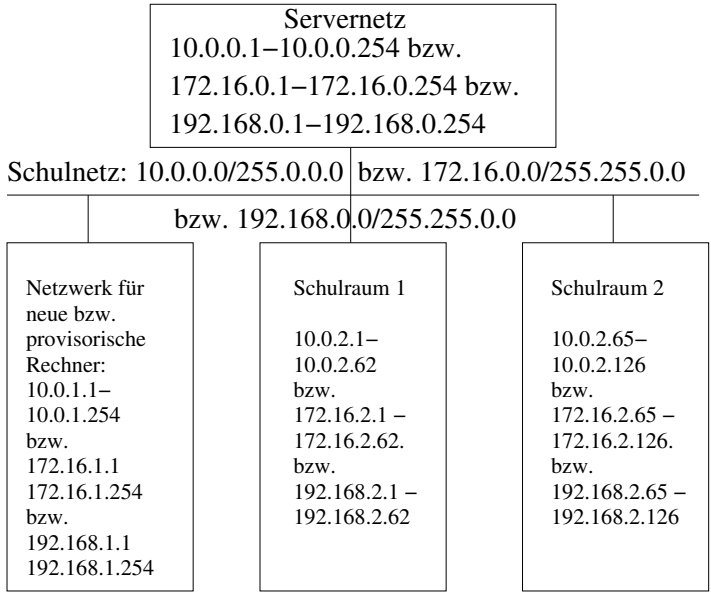


Abbildung 2.1: *Netzwerkstruktur des SUSE LINUX School Servers*

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

Dienste des SUSE LINUX School Server:

Der SUSE LINUX School Server bekommt nach der Installation vier verschiedene IP-Adressen.

Damit kann einerseits der Zugriff auf die verschiedenen vom SUSE LINUX 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.

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/Netatalk)
- 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
  - Webmailclient
  - Terminkalender
  - Foren
  - evtl. für weitere verschiedene Groupwareprogramme
  - Zugriff auf die persönlichen Webseiten der Benutzer des SUSE LINUX School Servers

Dritter Bereich:

- DNS-Name: `printserver`
- Druckerserver

Vierter Bereich:

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

Wie schon erwähnt ermöglicht der SUSE LINUX School Server die Auslagerung dieser Bereiche oder auch einzelner Dienste auf andere Rechner, um die Gesamtperformance des Systems zu steigern. Die gute Skalierbarkeit des SUSE LINUX School Server wirkt sich hier positiv aus.

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 SUSE LINUX School Server " sinnvoll benennen.

Achtung

Der SUSE LINUX School Server wird nach der Installation auch als DHCP- und Nameserver für Ihr Intranet eingerichtet. Sollten Sie schon interne DHCP- und/ oder Nameserver benutzen, schalten Sie diese bitte aus. Ansonsten können Sie die volle Funktionalität des SUSE LINUX School Servers nicht vernünftig nutzen.

Achtung

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` in das Internet geschickt wird, niemals zu Ihnen zurückkommen wird. Wie wäre es also z. B. mit `<schulname>.de` – auch

wenn Sie derzeit noch keinen Email-Verkehr unter diesen 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 SUSE LINUX School Servers mit YaST erklärt. Bitte schalten Sie für eine vollständige Installation sämtliche Hardwarekomponenten wie z. B. Drucker oder externe Laufwerke ein. Natürlich können Sie die Installation dieser Geräte auch später noch vornehmen. Falls Probleme auftreten sollten, helfen die in diesem Abschnitt gegebenen Hinweise über die meisten Hürden hinweg. Wenn Sie auch nach der Lektüre dieses Kapitels nicht zum Ziel kommen, wenden Sie sich bitte an unseren Support.

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.

Achtung

Systemstart von CD–ROM

Schalten Sie Ihren Rechner ein und legen Sie die CD in das Laufwerk. SuSE Linux wird nun zur Installation geladen.

Probleme beim Start

Sollte der Rechner nicht von CD–ROM booten, müssen Sie die Einstellungen im BIOS (Basic Input Output System) des Rechners ändern. Gehen Sie dazu wie folgt vor:

BIOS–Einstellungen ändern

Beim Neustart des Rechners wird dessen Hardware vom BIOS initialisiert. Unter anderem wird der Arbeitsspeicher getestet. Das erkennen Sie am Hochzählen des Systemspeichers. Währenddessen können Sie das BIOS–Setup aufrufen. Am unteren Bildschirmrand wird angezeigt, mit welcher Taste Sie das BIOS–Setup aufrufen können. Üblicherweise sind das die Tasten (Entf) oder (F1). Drücken Sie die entsprechende Taste und das BIOS–Setup wird angezeigt.

Ist Ihr Rechner mit einem AWARD–BIOS ausgestattet, heißt der gesuchte Eintrag BIOS FEATURES SETUP. Andere Hersteller verwenden ähnliche Einträge, z. B. ADVANCED CMOS SETUP. Wählen Sie den entsprechenden Eintrag aus und bestätigen Sie mit (↵).

Für Sie ist der zumeist als 'Boot Sequence' bezeichnete Unterpunkt zur Startreihenfolge der Laufwerke wichtig. Die Voreinstellung ist oftmals C, A oder A, C. Im ersten Fall sucht der Rechner beim Booten das Betriebssystem zuerst auf der Festplatte (C) und dann im Diskettenlaufwerk (A). Wählen Sie 'Boot Sequence' und drücken Sie dann solange die Taste (Bild ↑) bzw. (Bild ↓) oder entsprechende

Tasten, bis eine Sequenz angezeigt wird, die für Ihre Konfiguration passt, z. B. `A, CDROM, C`. Anschließend verlassen Sie diese Einstellungen durch Drücken von (Esc).

Um die Änderungen zu speichern, wählen Sie 'SAVE AND EXIT SETUP' oder drücken Sie (F10). Daraufhin werden Sie gefragt, ob Sie das BIOS–Setup verlassen und die neuen Einstellungen speichern möchten.

Hinweis

Ohne Betriebssystem haben Rechner normalerweise eine amerikanische Tastaturbelegung geladen, d. h. ohne Umlaute und mit einem (Y) an der Stelle, an der bei deutschen Tastaturen das (Z) steht. Drücken Sie also auf einer deutschen Tastatur die Taste (Z) für „yes".

Hinweis

Sie haben ein EIDE (ATAPI) CD–ROM–Laufwerk

Stellen Sie bitte die Bootreihenfolge im BIOS Ihres Rechners auf `CDROM, C, A` oder einen anderen Wert, bei welchem an das CD–ROM-Laufwerk an erster Stelle steht. Sehen Sie dazu unter 3 auf der vorherigen Seite nach.

Sie haben ein SCSI CD–ROM–Laufwerk

Bitte stellen Sie zunächst im BIOS Ihres Rechners wie unter 3 auf der vorherigen Seite beschrieben die Bootreihenfolge `SCSI, CDROM, A` oder eine ähnliche, bei welcher an erster Stelle der SCSI-Adapter steht, ein.

Nach dem Booten des Rechners wird zunächst das BIOS des Rechners selbst aktiv. Danach wird auch der SCSI–Hostadapter initialisiert, welcher über ein eigenes BIOS verfügt. Während dieser Initialisierung (die meist durch eine besondere Meldung angezeigt wird) können Sie dessen BIOS mit der angezeigten Tastenkombination aufrufen. Bei einem Adaptec Hostadapter können Sie dessen BIOS normalerweise mit (Ctrl) + (A) aufrufen. Bei einem Adapter der Firma Tekram etwa mit der Taste (F2) oder (F6).

Wählen Sie die 'Disk Utilities' aus; das System prüft und zeigt die angeschlossene Hardware an. Notieren Sie die SCSI-ID für Ihr CD-ROM-Laufwerk. Das Menü verlassen Sie mit (Esc), um anschließend 'Configure Adapter Settings' zu öffnen. Unter 'Additional Options' finden Sie 'Boot Device Options'. Wählen Sie dieses Menü aus und drücken Sie (↵). Geben Sie nun die zuvor notierte ID des CD–ROM–Laufwerks ein und drücken Sie wieder (↵). Durch zweimaliges Drücken von (Esc) kehren Sie zum Startbildschirm des SCSI–BIOS zurück, den Sie nach der Bestätigung mit 'Yes' verlassen, um den Rechner neu zu booten.

Rechner bootet nicht von CD–ROM

Bootet der Rechner nicht von CD–ROM, muss er mit einer Bootdiskette gestartet werden. Weitere Informationen hierzu finden Sie in der Support–Datenbank:

```
http://sdb.suse.de/de/sdb/html/swiegra_bootdiskette80.html
```

Startbildschirm

Während der Startbildschirm erscheint, bereitet YaST2 die Installation vor. Der Startbildschirm zeigt mehrere Auswahlmöglichkeiten für den weiteren Verlauf der Installation.

Wenn Sie vor Ablauf der Wartezeit eine andere als die (↵)-Taste drücken, wird nicht mehr automatisch die Installation gestartet, und Sie können in Ruhe andere Optionen wählen.

Sollten Sie ältere oder für bestimmte Funktionen nicht optimierte Hardware besitzen, können in seltenen Fällen Probleme bei der Installation auftreten. Solche Schwierigkeiten hängen meist mit dem Powermanagement-Modus oder mit der DMA-Fähigkeit der Laufwerke zusammen. Diese Probleme sind vorab nicht prüfbar und treten sporadisch während der Installation auf. Sollte so etwas passieren, also das System nicht durchinstallieren, starten Sie den Rechner neu und wählen Sie im Startbildschirm den Punkt 'Installation – Safe Settings'. In diesem Modus werden einige der "moderneren" Hardware-Eigenschaften nicht verwendet, was in problematischen Fällen meist dennoch eine korrekte Installation ermöglicht.

Anderer Grafikmodus für YaST2

Sie können bei der Installation zwischen verschiedenen grafischen Auflösungen und einer textbasierten Variante wählen. Mit den Funktionstasten (F3) bis (F5) können Sie unterschiedliche Auflösungen für den grafischen Installationsmodus auswählen, wobei der `VGA Grafikmodus (640x480)` mit jeder Grafikkarte funktionieren sollte.

Im Notfall können Sie mit (F2) auch den reinen Textmodus wählen.Im Text-Modus von YaST2 springen Sie innerhalb eines Bildschirms mit der (Tab) Taste von Menüpunkt zu Menüpunkt; innerhalb eines Menüs erfolgt die Auswahl mit den Tasten (↑) und (↓), mit der Taste (↵) springen Sie zum nächsten Bildschirm.

Kernelparameter

Im Feld `boot options` können Sie spezielle Kernelparameter eingeben, die aber nur bei sehr spezieller Hardware nötig sind.

Weitere Optionen

Die einzelnen Optionen im Startbildschirm bewirken:

Installation: Die normale Installation, in der alle modernen Hardware-Funktionen aktiviert werden.

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

Installation - APIC Enabled: Wird bei Rechnern mit APIC-Unterstützung (engl. *Advanced Programable Interrupt Controller*) benötigt, falls die Standardinstallation fehlschlägt.

Manual Installation: Wenn bestimmte Treiber, die beim Start der Installation automatisch geladen werden, Probleme bereiten, können Sie hier manuell installieren, d. h. diese Treiber werden dann nicht automatisch geladen. Dies funktioniert allerdings nicht, wenn Sie an Ihrem Rechner eine USB-Tastatur benutzen.

Der Rechner startet dann den Text-Modus von YaST, wo Sie die benötigten Treiber angeben können.

Rescue System: Falls Sie keinen Zugriff mehr auf Ihr installiertes Linux-System haben, starten Sie den Rechner mit der eingelegten DVD/CD1 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.

Näheres hierzu finden Sie im Abschnitt E auf Seite 247.

Memory Test: 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.

Boot Installed OS: Bootet Ihr System von der Festplatte (jenes, das normalerweise beim Rechnerstart hochfährt).

Bei der Installation lädt der SUSE LINUX School Server einige Sekunden nach dem Startbildschirm ein minimales Linux-System, das den weiteren Installationsvorgang kontrolliert. Auf dem Bildschirm erscheinen nun 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.

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 auf der nächsten Seite.

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.

Installationseinstellungen

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

Modus

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

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.

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.

Partitionierung

Während der Installation können Sie den verfügbaren Plattenplatz in mehrere Bereiche (Partitionen) unterteilen. Diesen Vorgang bezeichnet man als Partitionierung. Die von YaST2 vorgeschlagene Partitionierung können Sie hier bei Bedarf ändern.

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

Beachten Sie daher die weiteren Kapitel für die manuelle Partitionierung, die Einrichtung eines LVM- oder Softraidsystems nicht weiter, wenn Sie mit diesen Informationen nichts anfangen können, lesen Sie gleich unter 3 auf Seite 36 weiter.

Achtung

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

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

Achtung

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 SUSE LINUX 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 gefundene 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.

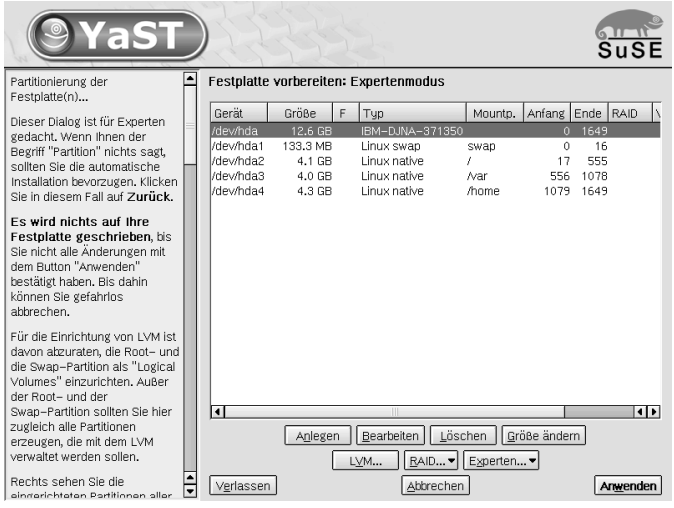


Abbildung 3.1: *Der Partitionierer des SUSE LINUX School Servers*

Prüfen Sie bitte, ob noch genügend freier Festplattenspeicher für die Installation des SUSE LINUX School Servers zur Verfügung steht (mindestens 20GB). Ansonsten müssen Sie evtl. vorhandene Festplattenpartitionen löschen oder verkleinern.

Partitionstypen

Jede Festplatte enthält eine Partitionstabelle, die Platz für vier Einträge hat. Jeder Eintrag in der Partitionstabelle kann entweder für eine primäre Partition oder für eine erweiterte Partition stehen, wobei maximal *eine* erweiterte Partition möglich ist.

Primäre Partitionen haben einen einfachen Aufbau: Sie sind ein durchgehender Bereich von Plattenzylindern (physische Bereiche auf der Platte), der einem Betriebssystem zugeordnet ist. Mit primären Partitionen könnte man pro Festplatte maximal vier Partitionen einrichten.

Werden mehr Partitionen benötigt, muss eine erweiterte Partition angelegt werden. Die erweiterte Partition ist ebenfalls ein durchgehender Bereich von Plattenzylindern. Sie kann in *logische Partitionen* unterteilt werden, die selbst keinen

Eintrag in der Partitionstabelle belegen. Die erweiterte Partition ist sozusagen ein Container, der die logischen Partitionen enthält.

Wenn Sie mehr als vier Partitionen benötigen, müssen Sie also beim Partitionieren nur darauf achten, dass Sie spätestens die vierte Partition als erweiterte Partition vorsehen und ihr den gesamten freien Zylinderbereich zuordnen. Darin können Sie dann beliebig viele logische Partitionen einrichten (das Maximum liegt bei 15 Partitionen für SCSI-Platten und bei 63 Partitionen für (E)IDE-Platten).

Für die Installation des SUSE LINUX School Servers sind beide Arten von Partitionen (primär und logisch) gleich gut geeignet.

Da der SUSE LINUX 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 ReiserFS.

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 Systemes. Als Größe sollten 4-6 GB reichen. (siehe Abbildung 3.3)

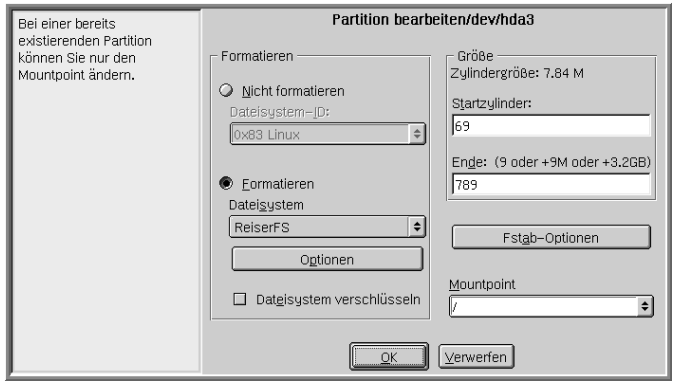


Abbildung 3.3: *Anlegen der* `/`-Partition

`/var` In diesem Verzeichnis befinden sich vor allem die Spoolverzeichnisse des Drucksystems, die Emails der Benutzer und die Benutzerdatenbank.

Weiterhin müssen ggfs. die Installations–CDs der aktuellen SuSE Linux Distribution in ein Unterverzeichnis (`/var/SuSE/akt`) auf dieser Partition kopiert werden, um SuSE Linux Clients automatisch zu installieren (siehe Kapitel 6 auf Seite 145).

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, und die Mailboxen der Lehrer werden auf 25 MB und die der Schüler auf 5 MB begrenzt, so rechnet man noch die etwa 4,5 GB im Verzeichniss `/var/SuSE/akt` und eine Reserve für die Logfiles des Systems dazu.

So sind Sie in unserem Beispiel mit einer Partitiongröße von

```
(800 Schüler * 5MB) + (80 Lehrer
 * 25MB) + 2GB + 4,5GB = 12,5GB
```

auf der sicheren Seite.

Weiterhin müssen unter dem Menüpunkt ‘Fstab-Optionen’ für diese Partition folgende Werte im Feld ‘Beliebiger Optionswert’ eingetragen werden: `defaults,data=writeback,noatime`

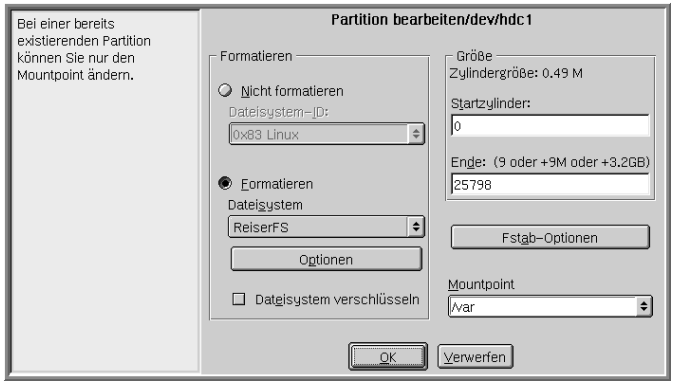


Abbildung 3.4: *Anlegen der /var-Partition*

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

Weiterhin müssen unter dem Menüpunkt 'Fstab-Optionen' für diese Partition folgende Werte im Feld 'Beliebiger Optionswert' eingetragen werden: `defaults,acl,usrquota` (siehe Abbildung 3.5).

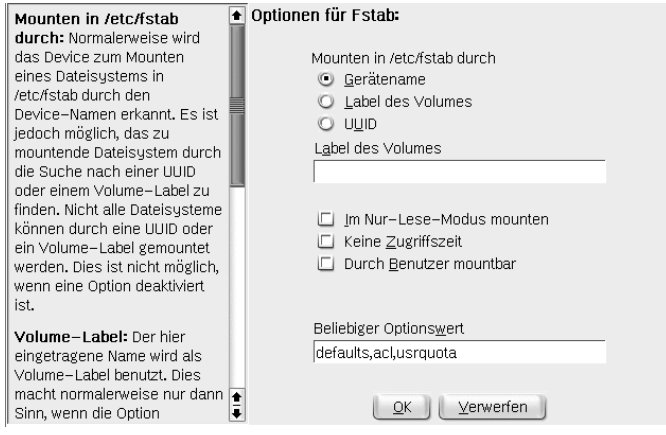


Abbildung 3.5: *Setzten der Filesystemoptionen der /home-Partition*

In den folgenden Tabellen finden Sie als Beispiel zwei Vorschläge zur sinnvollen Partitionierung des SUSE LINUX School Servers:

Partition	Mountpoint	Größe	Format
Beispiel für die Partitionierung einer EIDE Festplatte			
/dev/hda1		256MB	swap
/dev/hda2	/	4GB	ReiserFS
/dev/hda3	/var	5GB	ReiserFS
/dev/hda4	/home	10GB (bzw. der Rest)	ReiserFS
Beispiel für die Aufteilung des Systems auf 2 SCSI Festplatten			
/dev/sda1		256MB	swap
/dev/sda2	/	6GB	ReiserFS
/dev/sda2	/var	10GB (bzw. der Rest)	ReiserFS
/dev/sdb1	/home	24GB (bzw. die Plattengöße)	ReiserFS

Soft-RAID

Der Sinn von RAID (engl. *Redundant Array of Independent Disks*) ist es, mehrere Festplattenpartitionen zu einer großen virtuellen Festplatte zu vereinen, um Performance und Datensicherheit zu optimieren. Dabei geht das eine jedoch auf Kosten des anderen. Der so genannte RAID–Level definiert den Zusammenschluss und die gemeinsame Ansteuerung der Festplatten, die von einem RAID-Controller vorgenommen wird.

Statt eines RAID-Controllers, der unter Umständen sehr teuer sein kann, ist auch Soft-RAID in der Lage, diese Aufgaben zu übernehmen. Der SUSE LINUX School Server bietet Ihnen die Möglichkeit, mit Hilfe von YaST mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu Hardware-RAID, die allerdings auch zusätzliche Rechenkapazität vom Prozessor verlangt.

Gängige RAID-Level

RAID 0 Dieser Level verbessert die Performance Ihres Datenzugriffs. Im Grunde ist dies gar kein RAID, da es keine Datensicherung gibt, doch die Bezeichnung „RAID 0“ hat sich für diese Art von System eingebürgert. Bei

RAID 0 schließt man mindestens zwei Festplatten zusammen. Die Performance ist sehr gut – jedoch ist das RAID-System zerstört und Ihre Daten sind verloren, wenn auch nur eine von noch so vielen Festplatten ausfällt.

RAID 1 Dieser Level bietet eine zufriedenstellende Sicherheit für die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies nennt man „Festplattenspiegelung" – ist eine Platte zerstört, liegt eine Kopie deren Inhalts auf einer anderen. Es dürfen alle bis auf eine der Festplatten fehlerhaft sein, ohne Daten verloren zu haben. Die Schreibperformance leidet durch den Kopiervorgang ein wenig bei einer Verwendung von RAID 1 (10-20 % langsamer), dafür geht der Lesezugriff deutlich schneller im Vergleich zu einer einzelnen normalen physikalischen Festplatte, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können.

RAID 5 RAID 5 ist ein optimierter Kompromiss aus den beiden anderen Levels in Hinblick auf Performance und Redundanz. Das Festplattenpotential entspricht der Anzahl der eingesetzten Platten minus einer. Die Daten werden wie bei RAID 0 über die Festplatten verteilt. Für die Sicherheit sorgen die „Paritätsblöcke", die bei RAID 5 auf einer der Partitionen angelegt werden. Diese werden mit XOR miteinander verknüpft – somit lässt sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt nach XOR rekonstruieren. Bei RAID 5 ist zu beachten, dass nicht mehr als eine Festplatte gleichzeitig ausfallen darf. Ist eine zerstört, muss sie schnellstmöglichst ausgetauscht werden, damit die Daten nicht verloren gehen.

Soft-RAID-Konfiguration mit YaST

1. Schritt: Partitionieren

Zunächst sehen Sie unter 'Experten-Einstellungen' im Partitionierungs-Tool Ihre Partitionen aufgelistet. Wenn Sie bereits Soft-RAID-Partitionen angelegt haben, erscheinen diese hier. Andernfalls müssen Sie neue anlegen. Bei RAID 0 und RAID 1 benötigen Sie mindestens zwei Partitionen – bei RAID 1 sind das im Normalfall genau zwei. Für eine Verwendung von RAID 5 hingegen sind mindestens drei Partitionen nötig. Es ist zu empfehlen, nur Partitionen gleicher Größe zu nehmen.

Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlustes durch den Defekt einer Festplatte bei RAID 1 und 5 verhindert wird bzw. die Performance bei RAID 0 optimiert wird.

2. Schritt: RAID anlegen

Wenn Sie auf 'RAID' klicken, erscheint der Dialog, in dem Sie den RAID-Level 0, 1 oder 5 auswählen. In der nächsten Maske haben Sie die Möglichkeit, die Partitionen dem neuen RAID zuzuordnen. Hinter 'Experten-Optionen' finden Sie Einstellmöglichkeiten für die „chunk-size" – hier können Sie Fein-Tuning für die Performance vornehmen. Die Aktivierung der Checkbox 'Persistent superblock' sorgt dafür, dass RAID-Partitionen gleich beim Booten als solche erkannt werden.

Nach Beendigung der Konfiguration sehen Sie auf der Experten-Seite im Partitionierungs-Modul dann das Device `/dev/md0` (etc.) als „RAID" gekennzeichnet.

Tipp

Raid und LVM

Natürlich können Sie auch auf einem RAID-System ein LVM-System konfigurieren. LVM bietet dafür über Striping Arrays sogar eigene Funktionen. Bedenken Sie jedoch die bei der Verwendung von Softraid und LVM entstehende zusätzliche Belastung des Systems und die erhöhte Gefahr von Datenverlusten.

Tipp

Logical Volume Manager (LVM)

Der Logical Volume Manager (LVM) ermöglicht Ihnen eine flexible Verteilung des Festplattenplatzes auf die verschiedenen Filesysteme. Da die Partitionen in einem laufenden System nur mit relativ großem Aufwand geändert werden können, wurde der LVM entwickelt: Er stellt einen virtuellen Pool (Volume Group – kurz VG) an Speicherplatz zur Verfügung, aus dem logische Volumes (LV) nach Bedarf erzeugt werden. Das Betriebssystem greift dann auf diese statt auf die physikalischen Partitionen zu.

Achtung

Der Einsatz des LVM ist ggf. mit erhöhten Risiken wie z. B. Datenverlust verbunden. Mögliche Gefahren sind Programmabstürze, Stromausfälle oder fehlerhafte Kommandos.

Sichern Sie bitte Ihre Daten, bevor Sie LVM einsetzen oder Volumes umkonfigurieren – arbeiten Sie also nie ohne Backup!

Achtung

Besonderheiten:

- Mehrere Festplatten/Partitionen können zu einer großen logischen Partition zusammengefügt werden.
- Neigt sich bei einem LV (z. B. `/usr`) der freie Platz dem Ende zu, können Sie diese bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie sogar im laufenden System Festplatten oder LVs ergänzen. Voraussetzung ist allerdings hotswapfähige Hardware, die für solche Eingriffe geeignet ist.
- Mehrere Festplatten können im RAID 0 (striping) Modus mit entsprechend verbesserter Performance verwendet werden.
- Das „snapshot"-Feature ermöglicht vor allem bei Servern konsistente Backups während dem laufenden System.

Der Einsatz von LVM lohnt bereits bei kleinen Servern. Hier ist es z. B. möglich, Filesysteme zu haben, die größer sind als eine physikalische Festplatte. Ein weiterer Vorteil des LVM ist, dass bis zu 256 LVs angelegt werden können. Beachten Sie jedoch bitte, dass sich die Arbeit mit dem LVM sehr von der mit konventionellen Partitionen unterscheidet.

Achtung

Root–Filesystem

Zumindest das Root–Filesystem muss in YaST auf einer normalen Partition liegen. Wählen Sie diese Partition aus der Liste aus und legen Sie sie mit dem Button 'Bearbeiten' als Root–Filesystem fest.

Achtung

Elemente des LVM

Physical Volumes Die physikalischen Speichermedien (PV: physical volumes) bilden die unterste Ebene einer dreischichtigen Architektur. Ob diese Speichermedien nun Festplatten oder andere blockorientierte Geräte sind, hat im weiteren Verlauf keine großen Auswirkungen. Wir meinen hier Festplatten, wenn wir im weiteren Verlauf von PVs reden.

Volume Groups Ein oder mehrere PVs werden zu virtuellen Platten (VG: volume groups) zusammengefasst. Die VGs sind (abzüglich eines kleinen Verwaltungsanteils) so groß, wie die gesamte Speicherkapazität aller ihnen zugeteilten PVs.

Logical Volumes Die virtuellen Partitionen (LV: logical volumes) bilden die oberste Schicht und werden vom Betriebssystem wie reguläre Blockgerätedateien angesprochen. Die LVs können dabei – wie normale Partitionen auch – beliebige Dateisysteme enthalten.

Ebenso wie normale Partitionen erhalten auch PVs beim Neuanlegen einen Namen zugewiesen, der in einem Unterverzeichnis der jeweiligen VGs im Verzeichnis `/dev` erscheint.

Konfiguration des LVM mit YaST

Die LVM-Konfiguration von YaST wird vorbereitet, indem Sie während der Installation eine LVM-Partition anlegen.

Tipp

Um zu vermeiden, dass versehentlich bereits benutze Partitionen bei der Erstellung von VGs überschrieben werden, muss zuerst eine Partition per fdisk auf den für LVM reservierten Typ „0x8E“ gesetzt (bzw. erstellt) werden.

Tipp

Dazu wählen Sie ‘Anlegen’ → (‘Festplatte’ →) ‘primäre Partition’ und dort unter ‘Nicht formatieren’ die Dateisystem-ID ‘0x8E Linux LVM’.

Die weitere Partitionierung mit LVM sollten Sie direkt im Anschluss vornehmen, indem Sie im Partitionierer die LVM-Partition markieren und dann auf ‘LVM...’ klicken.

LVM – Partitionierer

Im Dialog ‘LVM’ werden die „virtuellen Platten“ (VGs) verwaltet. Wenn auf Ihrem System noch keine VG existiert, werden Sie in einem Popup-Fenster aufgefordert, eine anzulegen. Als Name für die erste VG wird `system` vorgeschlagen.

Die so genannte Physical Extent Size (oft abgekürzt mit PE-Size) bestimmt die maximale Größe eines Physical und Logical Volumes in dieser VG. Dieser Wert wird normalerweise auf 4 Megabyte festgelegt. Dies lässt eine Maximalgröße für ein Physical und Logical Volume von 256 Gigabyte zu. Sie sollten die Physical Extent Size also nur dann erhöhen (z. B. auf 8, 16 oder 32 Megabyte), wenn Sie größere Logical Volumes als 256 Gigabyte benötigen.

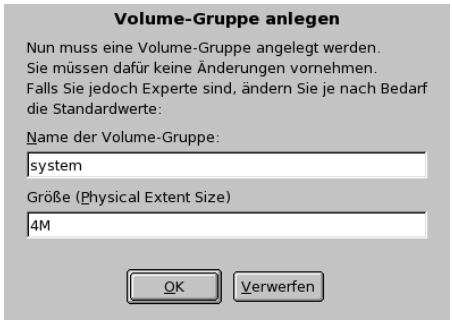


Abbildung 3.6: *YaST: Volume Group anlegen*

Tipp

Umpartitionieren von Logical Volumes

Falls auf Ihrem System bereits eine gültige LVM-Konfiguration existiert, wird diese bei Beginn der LVM-Konfiguration automatisch aktiviert. Ist diese Aktivierung erfolgt, kann die Partitionierung aller Platten, die eine Partition enthalten, welche zu einer aktivierten Volume Group gehört, nicht mehr verändert werden.

Am Anfang der PVs werden Informationen über das Volume in die Partition geschrieben. So „weiss“ eine PV, zu welcher Volume Group sie gehört. Wenn Sie neu partitionieren möchten, ist es empfehlenswert, den Anfang dieser Volumes zu löschen. Bei einer Volume Group „system“ und einem Physical Volume „/dev/sda2“ geht das z. B. mit dem Befehl

```
dd if=/dev/zero of=/dev/sda2 bs=512 count=1
```

Tipp

LVM – Einrichtung der Physical Volumes

In dem folgenden Dialog sind alle Partitionen aufgelistet, die entweder den Typ "Linux LVM" oder "Linux native" haben. Es werden also keine Swap- und DOS-Partitionen angezeigt.

Wenn eine Partition bereits einer VG zugeordnet ist, wird der Name der VG in der Liste angezeigt. Nicht zugeordnete Partitionen enthalten die Kennung "--".

Die gegenwärtig bearbeitete VG kann in der Auswahlbox links oben geändert werden. Mit den Buttons rechts oben ist es möglich, zusätzliche VGs anzulegen

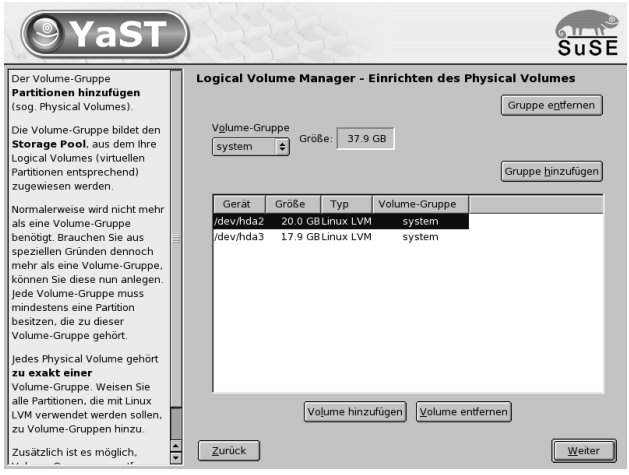


Abbildung 3.7: *YaST: Übersicht über die Partitionen*

und bestehende VGs zu löschen. Es können allerdings nur solche VGs gelöscht werden, denen keine Partitionen mehr zugeordnet sind (siehe Abbildung 3.7).

Tipp

Für ein normal installiertes System ist es nicht nötig, mehr als eine VG anzulegen.

Tipp

Um eine bisher nicht zugeordnete Partition der angewählten VG hinzuzufügen, wählen Sie zuerst die Partition an und aktivieren dann den Button 'Volume hinzufügen' unterhalb der Auswahlliste.

Daraufhin wird der Name der VG bei der angewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen haben, einer VG zuordnen, sonst bleibt der Platz auf der Partition ungenutzt.

Bevor Sie den Dialog verlassen können, muss jeder VG mindestens ein Physical Volume (also eine reale Partition einer Festplatte) zugeordnet sein.

Wenn Sie alle Partitionen Ihrer VG zugeordnet haben, klicken Sie bitte auf 'weiter'. Sie gelangen so zur Verwaltung der virtuellen Partitionen (LV).

Logical Volumes

Im diesem Dialog werden die virtuellen Partitionen (LV) verwaltet.

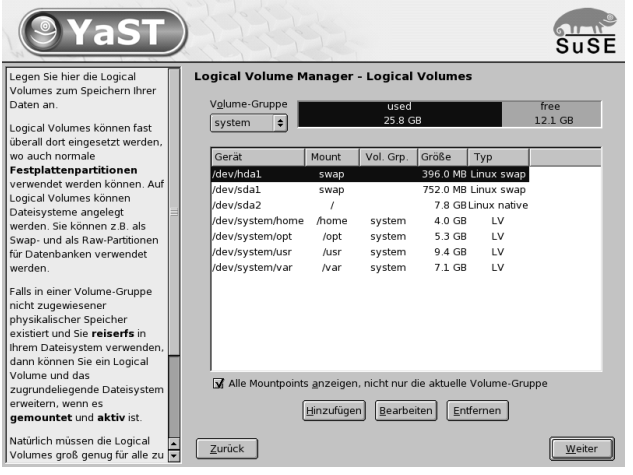


Abbildung 3.8: *YaST: Verwaltung der Logical Volumes*

Virtuelle Partitionen sind jeweils einer Volume Group zugeordnet und haben eine bestimmte Größe.

Normalerweise wird auf einem LV ein Filesystem (z. B. ReiserFS) angelegt und ihm ein Mountpunkt zugeordnet. Unter diesem Mountpunkt sind dann im installierten System die Dateien zu finden, die auf diesem Logical Volume gespeichert sind. In der Liste sind alle normalen Linux-Partitionen (denen ein Mountpunkt zugeordnet ist), alle Swap-Partitionen und alle bereits existierenden Logical Volumes eingetragen.

Wenn Sie erstmalig auf einem System LVM konfigurieren, existieren in dieser Maske noch keine Logical Volumes und Sie müssen für jeden Mountpunkt ein Logical Volume erzeugen (mit dem Button ‘Hinzufügen’) und die Größe, den Filesystem-Typ (z. B. reiserfs) und den Mountpunkt (z. B. `/var`, `/home`) mit den entsprechenden `fstab`-Optionen (siehe Abbildung 3.5 auf Seite 27) festlegen.

Wenn Sie mehrere VGs angelegt haben, können Sie in der Auswahlliste links oben zwischen den einzelnen VGs wechseln. Die angelegten Logical Volumes liegen jeweils in der links oben anzeigten VG. Haben Sie alle Logical Volumes so angelegt, wie sie benötigt werden, ist die LVM-Konfiguration beendet. Sie können den Dialog verlassen und mit der Software-Auswahl fortfahren.

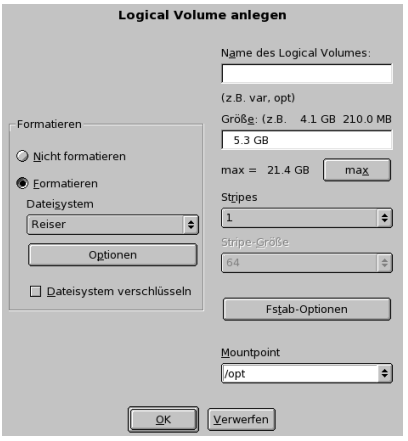


Abbildung 3.9: *YaST: Logical Volumes anlegen*

Software

Da der SUSE LINUX School Server eine fertig konfigurierte Softwareauswahl mitbringt, können hier keine Änderungen gemacht werden. Um die Systemintegrität zu gewährleisten, sollten auf dem SUSE LINUX School Server auch später keine weiteren Pakete installiert werden. Die SuSE Linux AG sorgt dafür, dass Ihr System immer stabil läuft. Deshalb 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 SUSE LINUX School Servers angeben, damit Sie immer die aktuellsten Meldungen erhalten können.

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

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 SuSE Linux automatisch die Umstellung von Sommer- auf Winterzeit und umgekehrt.

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.

Installation starten

Mit Klick auf 'Weiter' nehmen Sie den Installationsvorschlag mit allen von Ihnen gemachten Änderungen an und gelangen in eine grüne 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. Während der Installation sehen Sie Informationen über die SuSE Linux AG und einige Ihrer Produkte. Sie können auch 'Details' anklicken, um sich genauer über den Fortschritt der Installation zu informieren.

System konfigurieren

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

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.

Wenn ein Benutzer sein Passwort vergessen hat oder Programme nicht mehr laufen, hat `root` die Möglichkeit zu helfen.

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, eigenen 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 auf Seite 290), 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 auch die Sicherheit des Systems.

Bildschirm-Einstellungen

Hier werden Grafikkarte und Bildschirm mit einer zumeist sinnvollen Voreinstellung angezeigt. In den meisten Fällen können Sie diesen Vorschlag übernehmen. Sie können Farbtiefe, Auflösung und Bildwiederholfrequenz manuell einstellen und damit Ihren speziellen Anforderungen anpassen.

Wenn Sie auf ‘Ändern’ klicken, haben Sie die Möglichkeit, Einstellungen zur grafischen Oberfläche vorzunehmen. Dazu startet an dieser Stelle das Programm SaX2.

Sofern der Vorschlag geändert wurde, werden die Einstellungen getestet, bevor die Konfiguration auf der Festplatte gesichert wird.

Netzwerkkonfiguration

Die Konfiguration des Netzwerks ist im Falle des SUSE LINUX 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

Nachdem die Grafikkarte konfiguriert wurde, gelangen Sie zu dem in Abbildung 3.10 auf der nächsten Seite dargestellten Bildschirm. Hier wählen Sie zunächst diejenige Netzwerkkarte aus, die mit Ihrem internen Schulnetzwerk verbunden ist.

Tipp

Linux richtet für die Netzwerkkarten „Aliase“ ein, die auf den Namen `eth` hören. Ähnlich wie bei Festplatten dient auch hier wieder eine Zahl hinter dem Alias zur genaueren Definition. `eth0` ist die erste Netzwerkkarte im System, `eth1` die zweite. Für den SUSE LINUX School Server werden auf der ersten Netzwerkkarte zusätzliche, virtuelle Netzwerkkarten angelegt. Diese bekommen die Nummern `eth0:0` bis `eth0:2`.

Tipp

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.

In diesem Dialog können Sie dann den Typ der Netzwerkkarte und im Falle von ISA-Karten auch den zu verwendenden Interrupt und die IO-Adresse einstellen. Manchen Netzwerktreibern können Sie auch spezielle Parameter wie die zu verwendende Schnittstelle mitgeben, ob Sie beispielsweise den RJ-45- oder BNC-Anschluss auf der Karte verwenden wollen. Beachten Sie hierzu die Dokumentation des Treibermoduls.

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

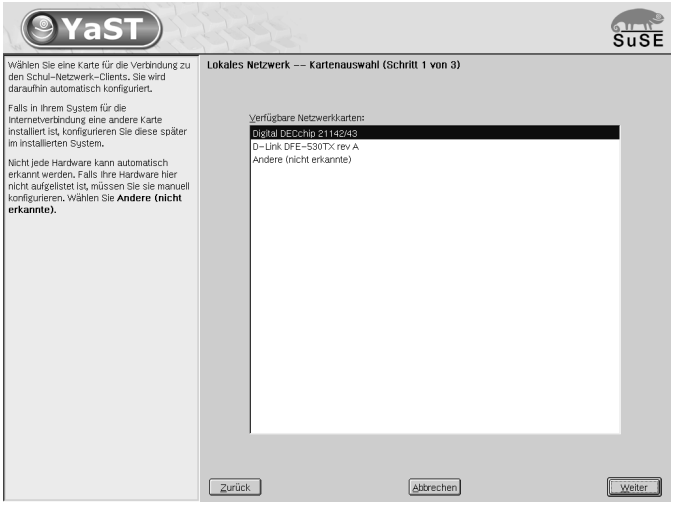


Abbildung 3.10: *Interne Netzwerkkarte auswählen*

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.

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.

Die beiden anderen Bereiche sind bislang schon oft für SUSE LINUX School Server Installationen verwendet worden und ermöglichen immerhin noch über 65.000 Rechner[1].

Wenn Sie z. B. die Konfiguration für das 192er Netzwerk übernehmen, wird der SUSE LINUX School Server folgendermassen konfiguriert:

[1] So verwenden z. B. die in Deutschland relativ bekannten SUSE LINUX School Server „GEE-Server“ und „Arktur“ die Adressbereiche 172.16.xxx.yyy und 192.168.xxx.yyy – wir haben die Adressbereiche dieser beiden Linux-Server so in die Konfiguration aufgenommen, dass sowohl ein Parallelbetrieb mit dem SUSE LINUX School Server als auch eine Migration möglich sein sollte.

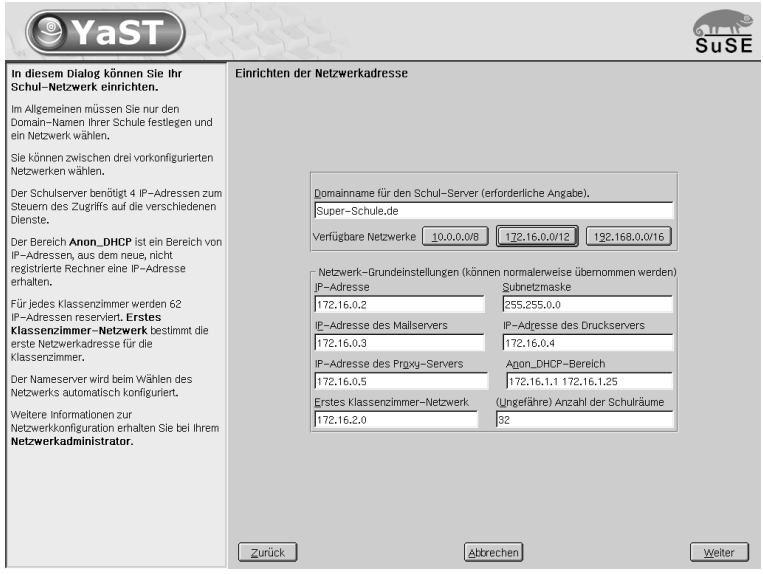


Abbildung 3.11: *Internes Netzwerk konfigurieren*

IP-Adresse z. B. `192.168.0.2`;
DNS-Namen: `admin, dns, nfs, ldap, samba, install, PDC-SERVER, gateway, timeserver`

Subnetzmaske z. B. `255.255.0.0`

IP-Adresse des Mailservers z. B. `192.168.0.3`;
DNS-Namen: `schulserver, mailserver, schoolserver`

IP-Adresse des Druckservers z. B. `192.168.0.4`;
DNS-Name: `printserver`

IP-Adresse des Proxy-Servers z. B. `192.168.0.5`;
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.: `192.168.1.1 bis 192.168.1.254`

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. `192.168.2.1 bis 192.168.2.64`).
Weitere Klassenräume werden entsprechend angelegt (siehe Grafik 2.1 auf Seite 10).

`(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 deren 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 SUSE LINUX School Server an das Internet angebunden sind.

In der Abbildung 3.13 auf Seite 45 sehen Sie die 3 Möglichkeiten, wie das Schulnetzwerk mit dem Internet verbunden werden kann.

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 SUSE LINUX School Server nicht einsetzen:

- DynDNS-Konfiguration (siehe Kapitel 4 auf Seite 104).
- Externer Zugriff (siehe Kapitel 4 auf Seite 89).
- Direkten Internetzugang erlauben/verbieten (siehe Kapitel 8 auf Seite 190).

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

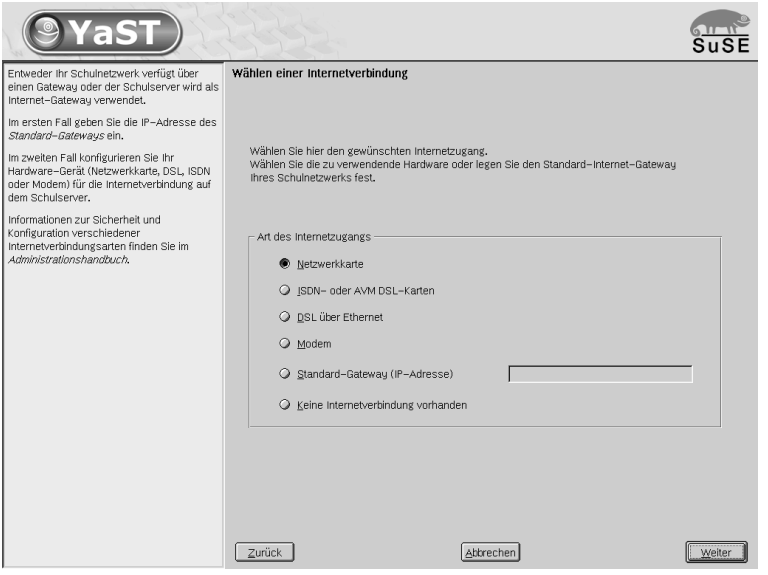
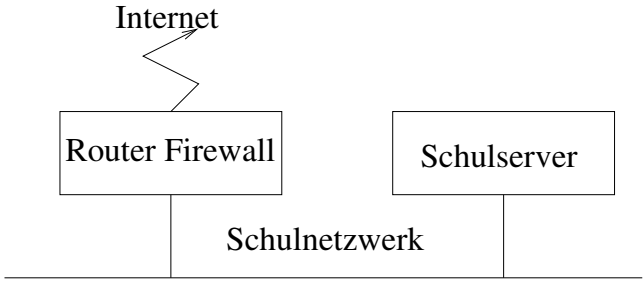


Abbildung 3.12: *Internetverbindung einrichten*

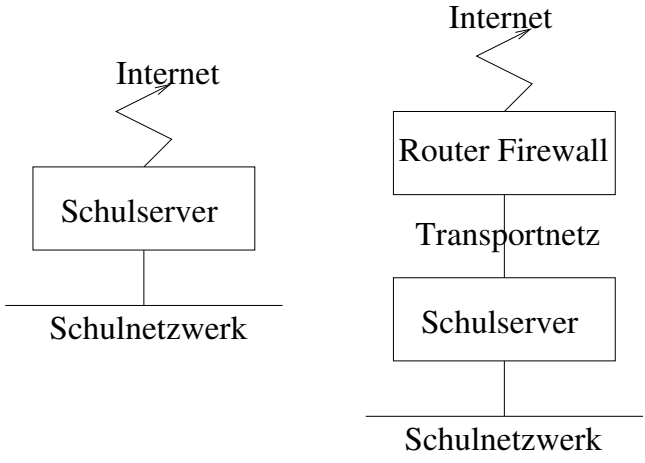
Bei einer Internetverbindung via ISDN, DSL oder Modem mit dynamischen IP-Adressen ist die Gefahr aus dem Internet noch vertretbar, aber im Falle einer Standleitung raten wir von einer direkten Internetanbindung auf jeden Fall ab.

Der Schulserver ist über ein Transportnetz mit dem Internet verbunden Das ist die sicherste Methode für die Anbindung eines Schulnetzes an das Internet. Sie erhalten alle Kontrollmöglichkeiten, die der SUSE LINUX School Server anbietet. Lediglich die DynDNS-Konfiguration (siehe in Kapitel 4 auf Seite 104) wird nicht verfügbar sein.

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



a) Internetgateway befindet sich im Schulnetzwerk



b) Schulserver ist direkt mit dem Internet verbunden

c) Schulserver ist über ein Transportnetz mit dem Internet verbunden

Abbildung 3.13: *Verschiedene Internetanbindungsmöglichkeiten*

Geben Sie also die entsprechende Hardware an oder geben Sie die IP-Adresse des Standard-Gateways in Ihrem Schulnetzwerk ein (siehe Abbildung 3.12 auf Seite 44).

Netzwerkkarte Sollten Sie über eine Standleitung oder einen Router bzw. eine separate Firewall (wie z. B. die „SuSE Firewall on CD“) an das Internet angeschlossen sein, sollten Sie im Server eine separate Netzwerkkarte für diese Anbindung installieren.

Bei einer Standleitung wählen Sie dann diese Netzwerkkarte aus und geben Sie in den Konfigurationseinstellungen für die Netzwerkkarte diejenigen Daten ein, die Sie von Ihrem Provider bekommen haben.

Sollten Sie hier eine feste IP-Adresse bekommen, markieren Sie im Menü die betreffende Netzwerkkarte und wählen Sie ‘Konfigurieren...’. Im nächsten Bildschirm wählen Sie dann ‘Konfiguration der statischen Adresse’ und geben die entsprechenden Werte ein.

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 aber noch in der Datei `/etc/rinetd.conf` die alte Adresse gegen die neue austauschen,

Hinweis

Über den Punkt ‘Routing’ müssen Sie den Standardgateway einstellen. Wählen Sie den Punkt ‘Konfiguration für Experten’, um erweiterte Einstellungen vorzunehmen.

Bitte geben Sie die von Ihrem Provider genannten Nameserver *nicht* in diesem Menü ein, sondern ändern Sie nach der Installation des SUSE LINUX School Servers in der Datei `/etc/named.conf` die entsprechenden Adressen hinter der Option `forwarders`!

Ebenso sollten Sie diese Methode einer separaten Netzwerkkarte wählen, wenn Sie über einen Hardwarerouter oder eine separate Firewall verfügen.

Verbinden Sie dann die beiden Geräte (den SUSE LINUX School Server und z. B. die Firewall) über die Netzwerkkarten miteinander (evtl. mit Cross-over-Kabeln) und richten Sie ggf. auf der Firewall oder (was oft der Fall ist) am Hardware-Router den DHCP-Server ein. Dann kann der SUSE

LINUX School Server mit „dynamischer Adresse“ für diese Netzwerkkarte konfiguriert werden und Sie brauchen hier keine weiteren Einstellungen vornehmen.

Hinweis

DHCP-Server

Achten sie bitte darauf, dass keine Konflikte zwischen dem DHCP-Server des Routers und dem DHCP-Server des SUSE LINUX School Servers entstehen. Der DHCP-Server des Routers sollte also auch andere IP-Adressen vergeben als der DHCP-Server des SUSE LINUX School Servers!

Hinweis

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. Belassen Sie den Startmodus auf ‘OnBoot’, wenn Sie später eine automatische Auswahl einrichten möchten.

DSL-Konfiguration Um DSL nutzen zu können, muss eine separate Netzwerkkarte im SUSE LINUX School Server installiert werden.

Momentan werden vom SUSE LINUX School Server DSL-Zugänge unterstützt, die mit dem Point-to-Point-over-Ethernet-Protokoll (PPPoE) arbeiten. Dieses Protokoll wird von allen großen Anbietern benutzt. Sollten Sie sich nicht sicher sein, welches Protokoll Ihr Provider verwendet, gibt dieser sicherlich gerne Auskunft.

Dial-on-Demand bedeutet, dass die Verbindung automatisch aufgebaut wird, sobald ein User auf das Internet zugreift, z. B. indem er eine Webseite mit einem Browser anwählt oder E-Mails verschickt. Nach einer bestimmten Zeit (Idletime), in der keine Daten gesendet oder empfangen werden, wird die Verbindung wieder getrennt. Da die Einwahl mit PPPoE, dem Protokoll für ADSL, sehr schnell geht, entsteht fast der Eindruck, als hätte man eine Standleitung in das Internet.

Obwohl mit einer DSL-Flatrate auch eine permanente Einwahl möglich wäre, sprechen doch einige Punkte für eine Verbindung, die nur kurz und nach Bedarf besteht:

- Die meisten Provider trennen die Verbindung nach einer gewissen Zeit sowieso.

- Eine permanente Verbindung kann als Ressourcenverschwendung betrachtet werden (z. B. hat der Provider immer weniger IP-Adressen zur Verfügung).
- Vor allem aber stellt es ein enormes Sicherheitsrisiko dar, permanent online zu sein, da ein Angreifer das System auf Schwachstellen absuchen kann. Ein System, das nur bei Bedarf im Internet erreichbar ist und immer wieder eine andere IP-Adresse hat, ist viel schwieriger zu attackieren.

Dial-on-Demand können Sie auch später noch mit YaST2 aktivieren oder Sie richten es manuell ein. Setzen Sie dazu in der Datei `/etc/sysconfig/network/providers/dsl-provider0` den Parameter DEMAND= auf „yes“ und definieren Sie eine Idletime mit der Variable: IDLETIME="60". Damit wird eine unbenutzte Verbindung nach 60 Sekunden beendet.

Beachten Sie bitte, dass Sie einen Nameserver angeben müssen, wenn Sie Dial-On-Demand aktivieren. Hier können Sie einfach die interne IP-Adresse `127.0.0.1` angeben, da der SUSE LINUX School Server über einen eigenen Nameserver verfügt, welcher die Namensauflösung übernimmt und den Server ggf. zur Einwahl ins Internet veranlasst.

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 dessen interne Adresse an.

Bitte beachten Sie, dass Hardwarerouter oftmals einen eingebauten DHCP-Server haben, der sich nicht mit dem im SUSE LINUX 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 SUSE LINUX 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 anschlie-

ßend 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 SUSE LINUX 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.

Achtung

Grundkonfiguration

Jetzt werden die schulspezifische Angaben (Administratorpasswort, Name der Schule, Anzahl der Klassen) abgefragt und das System dementsprechend konfiguriert:

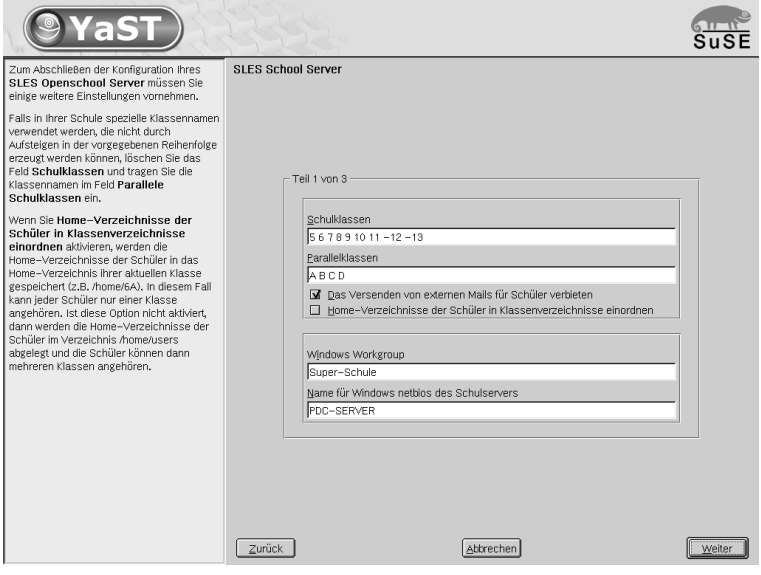


Abbildung 3.14: *Konfiguration des Schulservers: Workgroup und Klassen einrichten*

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
- 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. Haben Sie ganz spezielle Klassennamen, die nicht einfach durch Permutation zu bekommen sind, tragen Sie in das Feld 'Schulklassen' das Zeichen "*" und die Namen der Klassen ins Feld 'Parallelklassen' ein.

Hinweis

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

Hinweis

Für jede Klasse werden Benutzergruppen[2] angelegt. Die Klassen bekommen weiterhin einen gemeinsamen Mail- bzw. Dateisystemordner: `<klassenname>@<domainname.der.schule>` bzw. `/home/groups/<klassenname>`.

Die Mitglieder einer Klasse können die Gruppenmails in dem Gruppenmailkonto lesen. Dieses Verhalten kann nachträglich noch geändert werden. Die Zustellung der Gruppenmails der SchülerInnen in die privaten Mailkonten kann jedoch ein enormes Mailaufkommen verursachen, deshalb sollte man lieber bei der Grundeinstellung bleiben.

[2] Wobei für die gidNumber der Klassen gilt: `gidNumber > 999`

Tipp

Unübliche Klassenbezeichnungen

In machen Schulen gibt es Klassenbezeichnungen, die nicht durch die obige Systematik erfassbar sind. Für diesen Fall empfehlen wir das folgende Vorgehen:

- Tragen Sie in das Feld 'Parallelklassen' genau einen Klassennamen ein, den Sie später *nicht* als normale Klasse benutzen wollen - dieser Klassenname sollte also der Name einer „Testklasse" sein.
- Tragen Sie in das Feld 'Schulklassen' das Zeichen "*" ein.
- Installieren Sie den Schulserver nun wie angegeben.
- Erzeugen Sie mit dem Schulverwaltungsprogramm eine Export-Datei, in welcher u.a. die Namen der jeweiligen Klassen enthalten sind. Importieren Sie diese Datei wie unter *Schülerdaten exportieren und importieren* auf Seite 207 beschrieben.

Tipp

Die Schüler haben in den Klassenmailboxen nur Lesezugriff, deshalb besteht die Gefahr eines zufälligen Löschens durch Schüler nicht. Lehrer jedoch haben vollen Zugriff auf die Klassenmailboxen, deshalb besteht die Gefahr bzw. Möglichkeit, dass ein Lehrer eMails eines anderen Lehrers löscht.

Es werden drei Hauptbenutzergruppen angelegt:

`users; gidNumber = 100` Hauptgruppe der SchülerInnen

`teachers; gidNumber = 102` Hauptgruppe der Lehrkraft

`administration; gidNumber = 104` Hauptgruppe der Arbeitskraft in der Schulverwaltung

Die Gruppe `teachers` und `administration` bekommen einen gemeinsamen Mailaccount und Dateisystemordner:

`lehrer@<domainname.der.schule>` bzw.
`teachers@<domainname.der.schule>` und
`administration@<domainname.der.schule>` bzw.
`verwaltung@<domainname.der.schule>`

`/home/groups/teachers`
`/home/groups/administration`

Die Lehrer und die Verwaltung bekommen alle Gruppenemails in ihre privaten Mailkonten. Dieses Verhalten kann jedoch nachträglich geändert werden.

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

Der 'Windows Workgroup' bzw. Domainname wird aus dem DNS-Domainnamen abgeleitet, welchen Sie schon eingegeben haben. Sie können ihn jedoch ändern. Als NETBIOSNAME für den SUSE LINUX School Server wird „PDC-SERVER" vorgeschlagen. Auch diesen Eintrag können Sie anpassen in dem Feld 'Windows Netbiosname des Schulservers' (siehe Abbildung 3.14 auf Seite 49).

LDAP-Einstellungen und Adminpasswort

Im nächsten Schritt geben Sie nun die Passwörter für die „Schuladmins" ein, welche später die Hauptarbeit am Server erledigen (siehe Abbildung 3.15).

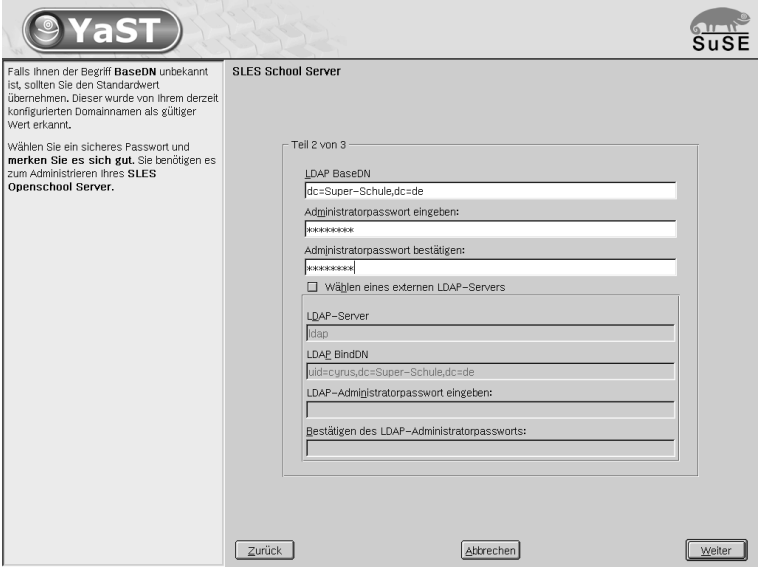


Abbildung 3.15: *Konfiguration des Schulservers: LDAP-Einstellungen und Adminpasswort.*

Den Wert für 'LDAP BaseDN' belassen Sie bitte bei der Voreinstellung – es sei denn, Sie wissen wirklich ganz genau was Sie da tun. Die Voreinstellung ist der Domainname, den Sie bei der Netzwerk-Konfiguration eingetragen haben.

Das Passwort für den Administrator muss hier *nicht* identisch mit dem `root`-Passwort für den Systemadministrator sein, welches schon vorher eingege-

ben wurde! Hier geht es um den Administrator für die spätere Konfiguration des schulischen Teils des Systems des SUSE LINUX School Servers und den Mail-Administrator. Diese Administratoren heißen `admin` und `mailadmin`, für beide wird dasselbe Passwort gesetzt. Auch der Windowsadministrator (`Administrator`) bekommt dasselbe Passwort. Sie können dieses Passwort später über die Weboberfläche ändern.

Möchten Sie einen schon vorhandenen LDAP-Server verwenden, müssen Sie den Menüknopf 'Externen LDAP-Server verwenden' aktivieren und die nötigen Angaben eintragen. Diese Möglichkeit sollten Sie nur dann nutzen, wenn Sie sich wirklich im Klaren darüber sind, welche Auswirkungen das auf Ihr System hat. Bitte beachten Sie, dass der externe LDAP-Server in diesem Fall schon soweit vorkonfiguriert sein sollte, dass der Hauptadministrator Ihres neu installierten SUSE LINUX School Server (`admin`) auf dem gesamten LDAP-Subbaum über komplette Schreibberechtigung verfügt.

Schulname 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.

Nachdem Sie auf 'Beenden' geklickt haben, wird die SUSE LINUX School Server Grundkonfiguration erstellt. Es müssen noch die ausgewählten Spracherweiterungspakete nachinstalliert werden. Legen Sie die entsprechenden CDs ein, sobald Sie dazu aufgefordert werden.

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 SUSE LINUX 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 `root` am System anmelden.

Achtung

Arbeiten als root

Wir möchten Sie noch einmal ausdrücklich darauf aufmerksam machen, dass es immer riskant ist, als Benutzer `root` zu arbeiten!

Leicht kann hier durch irrtümliche Befehle ein großer Schaden am System entstehen. Sie sollten also entsprechende Vorsicht walten lassen, wenn Sie administrative Aufgaben wahrnehmen. Ein guter Tip unter vielen ist sicherlich das Anfertigen von Sicherheitskopien vor der Arbeit am System.

Achtung

Testen des installierten Systems

Nachdem Sie sich am SUSE LINUX School Server angemeldet haben, wird die grafische Oberfläche gestartet. Sie sollten noch einige Tests vornehmen, bevor Sie den Server offiziell in Betrieb nehmen, um sicherzustellen, dass alles zu Ihrer Zufriedenheit funktioniert.

Links auf der Oberfläche

Um Ihnen die Administration zu erleichtern, werden bei der Installation Links zu den entsprechenden Weboberflächen auf dem Desktop von `root` angelegt.

Bitte klicken Sie zunächst auf den Link „Web-Mail, Groupware, Forum“ und versuchen Sie sich als `mailadmin` 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, hat die Meldung ihre Richtigkeit, und Sie können 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 erhalten.

Dienstüberwachung

Bitte überprüfen Sie in der Weboberfläche des Admins im Menüpunkt ‘Überwachung’ → ‘Dienstüberwachung’, ob die entsprechenden Dienste alle den Status

„grün“ haben. Sollte dies nicht der Fall sein, ändern Sie bitte den entsprechenden Eintrag des Dienstes auf „aktiviert“ und starten Sie sicherheitshalber den Server noch einmal neu.

Wird der entsprechende Dienst nun immer noch nicht als „aktiviert“ gemeldet, liegt ein Fehler vor.

Hinweis

Nicht aktivierte Dienste

Vorsorglich wurden in der Dienstüberwachung auch Dienste eingetragen, die nur unter bestimmten Umständen aktiviert werden sollten:

- Der Dienst `atalk` wird nur benötigt, wenn Sie auch „Mac-Rechner“ am SUSE LINUX School Server betreiben.
- Beim Dienst `amavis` handelt es sich um ein Virenscanner-Modul, welches als Mittler zwischen einem Virenscanner und bestimmten Diensten (wie z. B. Email) fungiert. Nähere Informationen erhalten Sie im Verzeichnis `/usr/share/doc/packages/amavisd-postfix`.
- Wenn Sie für Ihrem Server eine USV und diese über ein entsprechendes Kabel mit dem SUSE LINUX School Server verbunden haben, dann können Sie den Dienst `apcupsd` aktivieren, um den Status der USV zu überprüfen und den Server bei einem Stromausfall sicher herunterfahren zu lassen.

Hinweis

Proxy

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

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:

```
/srv/www/htdocs/proxy.pac
```

(Natürlich können Sie auch nach der Datei `proxy.pac` im Verzeichnis `/srv/www/htdocs/` suchen.)

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 `mailadmin` anmelden und sollten dann auf die Sperrseite weitergeleitet werden.

Konfiguration des Archivierungsprogrammes Sesam2000

Die Firma SEP-AG `http://www.sep.de` stellt für den SUSE LINUX School Server eine kostenlose Version ihres Produktes Sesam2000 zur Verfügung. Sie können damit den SUSE LINUX School Server auf ein Single-Band Laufwerk oder eine (separate) Festplatte archivieren.

Hinweis

Bitte beachten Sie, dass die Firma das Produkt zwar für Schulen kostenlos zur Verfügung stellt, dass Sie sich jedoch auf der Webseite der Firma registrieren müssen, wenn Sie es an Ihrer Schule nutzen möchten.

Hinweis

Dieses Programmpaket wird während der Installation ebenfalls installiert, Sie müssen lediglich ein Konfigurationsskript ausführen. Melden Sie sich dazu als Benutzer `root` am System an, starten Sie eine Konsole und führen Sie den Befehl `/opt/sesam/bin/sesam_serv_setup` aus. Es dauert ziemlich lange, bis alle Konfigurationsschritte durchgeführt sind. Unterbrechen Sie bitte deshalb die Ausführung nicht.

Weitere Informationen zur Handhabung dieses Produktes finden Sie in den Onlinedokumentationen oder unter der URL `http://www.sep.de`.

Die Administrationsoberfläche

Die Startseite im Browser

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

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

ein. Sie sollten dann folgende Startseite erhalten (siehe Abbildung 4.1 auf der nächsten Seite).

Achtung

Da das Zertifikat des SUSE LINUX School Server erst bei der Installation speziell für Ihre Schule ausgestellt wird, kennt der Browser dieses Zertifikat natürlich nicht und gibt eine entsprechende Warnung aus.

Achtung

Der Systemadministrator `admin`

Um als Schuladministrator den SUSE LINUX School Server zu verwalten, loggen Sie sich mit dem Benutzernamen `admin` und Ihrem Administratorpasswort in das Konfigurationsmenü ein. Sie können hier nahezu alle Parameter einstellen, mit denen der SUSE LINUX School Server konfiguriert wird.

Die Navigation im Konfigurationsmenü ist bewusst einfach und effizient gehalten. Das Menü besteht aus einer ersten Reiterleiste als Hauptmenü und einer bei Bedarf erscheinenden zweiten Leiste als Untermenü (siehe Abbildung 4.2 auf Seite 59).

Abbildung 4.1: *Startseite des SUSE LINUX School Servers*

Durch einen Mausklick auf die Hauptleiste wird die entsprechende Unterleiste aufgerufen. Das Symbol in der Hauptleiste wird dabei eingefärbt. Durch einen Mausklick auf ein Untermenü erhalten Sie die entsprechende Maske. Wollen Sie die Sprache ändern, klicken Sie auf das Symbol mit dem Untertitel 'Sprache'.

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, um weitere Änderungen vornehmen zu können.

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, müssen Sie in manchen Fällen trotzdem das graphische Konfigurationstool YaST2 verwenden.

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

Hinweis

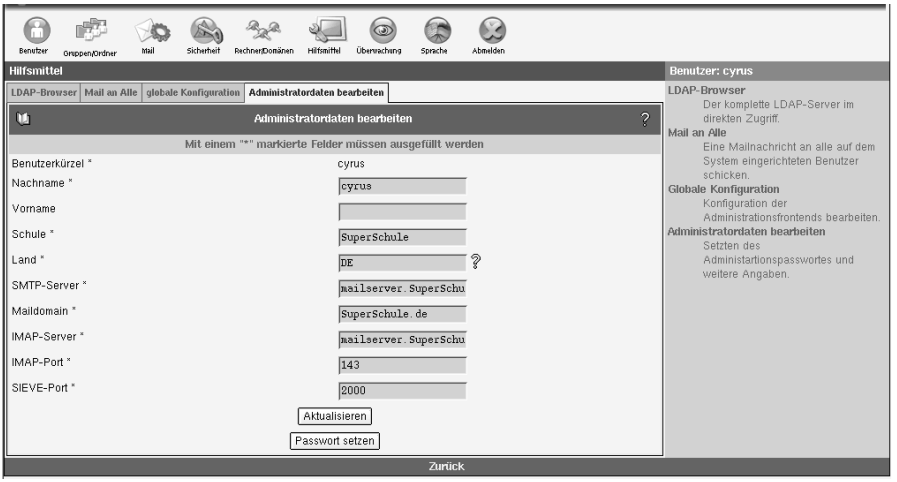


Abbildung 4.2: *Administration des SUSE LINUX School Servers für den Benutzer* `admin`

Benutzer-Verwaltung

Nachdem Sie Ihren SUSE LINUX School Server installiert haben, müssen Sie die Benutzer anlegen. Bereits vorhanden sind der Benutzer `admin` (der den School Server konfiguriert) sowie der Benutzer `mailadmin`, der die E-Mails an den Administrator lesen kann.

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 erläutern wir genauer unter 4 auf Seite 63.

Anlegen einzelner Benutzer

Wählen Sie im Hauptmenü 'Benutzer', dann im Untermenü 'Neu', um den ersten Benutzer anzulegen (siehe Abbildung 4.3 auf Seite 61).

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

- Nachname
- Vorname
- Primäre Gruppe: Schüler, Lehrer oder Verwaltung
- Klasse. Ist der neu angelegte Benutzer ein Schüler, muss er einer (aber auch nur einer!) Klasse zugeordnet werden. Ein Lehrer kann zu einer beliebigen Anzahl von Klassen gehören oder auch zu keiner. Am Ende der Auswahl können Sie auch `all` wählen, um einen Lehrer allen Klassen zuzuordnen.
- Geburtstag

Wurde keine Benutzer-ID (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`.

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.

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

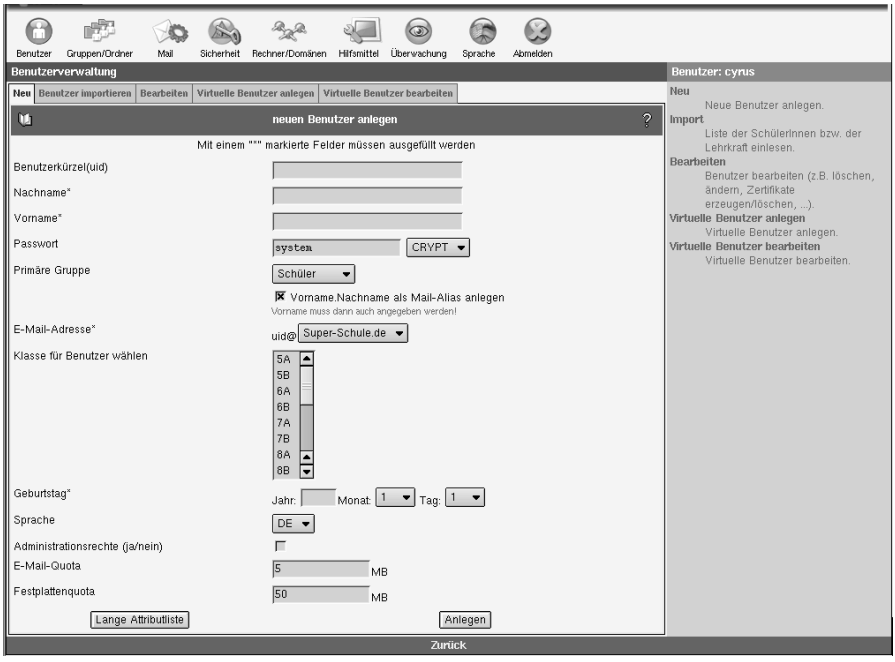


Abbildung 4.3: *Anlegen eines neuen Benutzers*

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` oder `Verwaltung`wählen.

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.

Diese Werte bezeichnen den Platz, den ein Benutzer maximal für E-Mails in seinen Ordnern bzw. für Dateien auf dem SUSE LINUX 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 Variabeln 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 und Telefonnummern) 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 SUSE LINUX 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 Homeverzeichnisse unterhalb des Verzeichnisses `/home/teachers/` und die Schüler unterhalb des Verzeichnisses `/home/<Klasse>` bzw. `/home/users` – je nachdem, was Sie bei der Installation gewählt haben.

Folgende Verzeichnisse werden in jedem neuen Homeverzeichnis angelegt:

Import: für die einkommenden Dateien

Export: für ausgehende Dateien

public_html: für die Veröffentlichung von Dateien. Der Zugriff auf dieses Verzeichnis ist per default über die URL `https://SchoolServer/~<login>` auch mit einem Webbrowser möglich.

Weiterhin bekommt jeder Benutzer ein Verzeichnis in `/home/profile` für seine Windowsprofile.

Benutzer importieren

Da es sehr mühsam wäre, die Schüler bzw. die Lehrer jedes Jahr per Hand einzutragen, gibt es die Möglichkeit, die Liste der Schüler (und Lehrer) aus einer Datei zu importieren. Die Datei sollte dazu folgendes Format haben:

- Format: Normale ASCII-Textdatei. 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.

  Für einige Schulverwaltungsprogramme haben wir unter *Schülerdaten exportieren und importieren* auf Seite 207 eine kleine Anleitung beigefügt. Wenn Sie diese Programme nutzen, ändern Sie bitte wie dort beschrieben das Importformat für die Dateien unter ‘Hilfsmittel’ → ‘Globale Konfiguration’.

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

  NACHNAME *

  VORNAME *

  GEBURTSTAG *

  KLASSE *

  PASSWORT

  LOGIN

  TELEFONNUMMER

  FAXNUMMER

  TELEFONNUMMER-PRIVAT

  TELEFONNUMMER-MOBIL

  SPRACHE

BESCHREIBUNG

STRASSE

PLZ

BUNDESLAND

EMAIL-DOMAIN

- Die mit `'*'` gekenzeichneten Felder sind obligatorisch.
- Durch die Felder NAME, VORNAME und GEBURSTAG wird ein Benutzer identifiziert.
- Es gibt drei Möglichkeiten für einen Eintrag in der Benutzerdatei:

Neuer Benutzer Der Benutzer wird in der LDAP-Datenbank nicht gefunden. In diesem Fall wird für diesen Benutzer ein neuer eindeutiger Login, wie unter *Anlegen einzelner Benutzer* auf Seite 59 beschrieben, ermittelt und in die LDAP-Datenbank aufgenommen.

Falls vorhanden, wird das Feld PASSWORT in folgender 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 andere 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 ermittelt.

Benutzer löschen 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.

Seine Daten werden aus der Datenbank gelöscht, sein Heimatverzeichniss wird in ein Tararchiv zusammengefasst und ins Verzeichnis `/home/archiv` gespeichert. Da die Archivierung sehr rechenintensiv ist, wird diese nicht sofort, sondern erst am nächsten Tag um

2 Uhr früh durchgeführt. Sie können jedoch die Archivierung auch manuell anstoßen. Melden Sie sich dazu am SUSE LINUX 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

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

Bei alten Benutzern wird dass Feld PASSWORT nicht ausgewertet. Die Benutzer werden lediglich aus der alten Klasse aus- und in die neue Klasse eingetragen, ihre Heimatverzeichnisse ziehen um. Ggf. werden ihre Daten nicht geändert, wenn neue und alte Klasse identisch sind.

- Nach dem Abarbeiten der eingelesenen Datei wird die neue, aktuelle Benutzerliste pro Klasse in der Datei `/root/<datum>.<uhrzeit>.userlist.<KLASSE>.txt` im Homeverzeichniss des Benutzers `root` gespeichert. In dieser Datei stehen die Passwörter im Klartext, mit dementsprechender Sicherheit und Diskretion 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:*: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
```

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 oder Nachname oder Vorname Tragen Sie das gesuchte Wort oder einen Teil davon mit `'*'` erweitert ins Eingabefeld 'Filter' ein. Andere Jokerzeichen wie z. B. `'?'` funktionieren hier leider nicht.

Klasse bzw. Gruppe Tragen Sie die Bezeichnung der Klasse oder Gruppe, deren Mitglieder Sie suchen, ins Feld 'Klasse' ein. Auch hier können Sie mit dem Suchstring `'5*'` z. B. alle Schüler des fünften Jahrganges und deren Lehrer auflisten.

Die Funktionen

- 'Löschen',
- 'Externe Mails Ja/Nein' und
- 'Zugriffsrechte bearbeiten'

lassen sich auch für mehrere Benutzer gleichzeitig durchführen. Wählen Sie dazu einfach mit Hilfe der gedrückten Strg- oder Shift-Taste mehrere Benutzer mit der Maus aus.

Die Namen der gewählten Benutzer werden farbig markiert. Am rechten Rand befinden sich Buttons für die einzelnen Funktionen (siehe Abbildung 4.4).

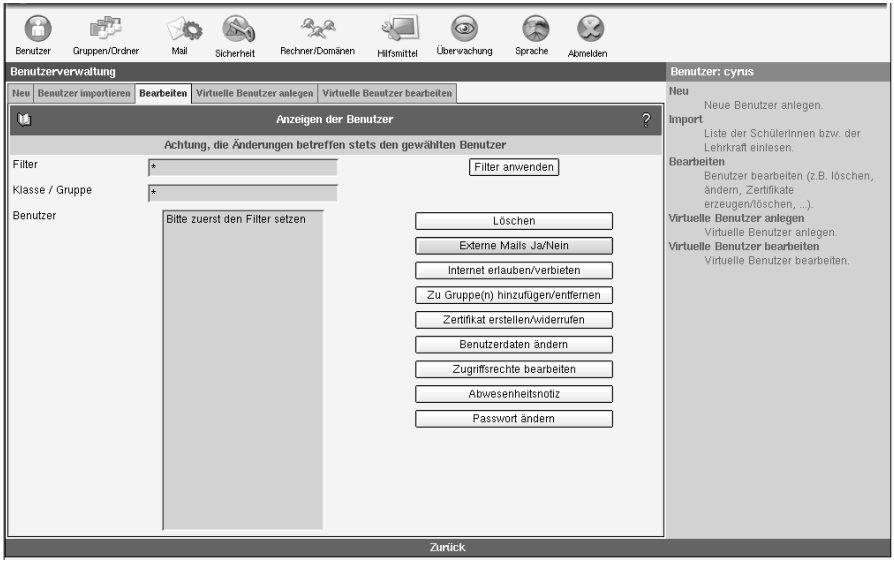


Abbildung 4.4: *Verändern der Benutzerdaten*

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

'Externe Mails Ja/Nein' Je nachdem, wie Sie den SUSE LINUX 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 Benutzer wird das LDAP-Attribut `mailEnabled` auf den Wert `OK` oder `locale_only` gesetzt. Unter diesem Menüpunkt können Sie einzelnen Benutzer das Versenden von externe Mails erlauben bzw. verbieten.

Wenn Sie die Grundeinstellung nachträglich verändern möchten, dann verändern Sie in der Datei `/etc/sysconfig/schoolserver` die Variable `SCHOOL_NO_EXTERN_MAIL` mit einem Editor Ihrer Wahl. Die geänderte Einstellung gilt allerdings nur für neu angelegte Benutzer.

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

'Zertifikat erstellen/widerrufen' Hiermit erstellen Sie ein Zertifikat für diesen Benutzer. Das funktioniert allerdings erst, wenn Sie eine „CA" (engl. *Certification Authority*) aufgesetzt haben. Die Erstellung verläuft ähnlich wie das Anlegen des Serverzertifikats (siehe 4 auf Seite 88).

Sie müssen in der Konfigurationsmaske zuerst das Passwort eingeben, welches Sie für die Erstellung der CA vergeben haben, danach in den beiden folgenden Feldern zweimal das Passwort für das neue Client-Zertifikat.

Bestätigen Sie die Eingaben mit 'signieren'.

'Zu Gruppen hinzufügen' Sie können die Benutzer einer oder mehreren (sekundären) Gruppen zuordnen. Markieren Sie per Mausklick (und evtl. gedrückt gehaltener Shift- oder Strg-Taste) eine oder mehrere der verfügbaren Gruppen und bestätigen Sie die Änderungen.

'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 erreichbar sein soll.

'Zugriffsrechte bearbeiten' In dieser Maske ist es möglich, den Schreibzugriff, den ein Benutzer auf seine persönlichen Daten hat, einzuschränken. Sie erhalten eine Übersicht, die alle verfügbaren Felder anzeigt. Sie können hier diejenigen Felder auswählen, die der Benutzer bearbeiten darf.

'Abwesenheitsnotiz' Hier können Sie automatische Abwesenheitsnotizen für Benutzer einrichten (siehe hierzu auch 8 auf Seite 188).

'Ändere Passwort' In dieser Maske wird ein neues Passwort vergeben, wenn z. B. der Benutzer sein eigenes Passwort vergessen hat.

Anlegen eines virtuellen Benutzers

Nachdem Sie mindestens eine virtuelle Domain angelegt haben, können Sie über 'Neu' virtuelle Benutzer anlegen (siehe Abbildung 4.5). Klicken Sie auf 'Filter anwenden', um eine Liste der auf dem System verfügbaren Benutzer zu erhalten, oder schränken Sie vorher die Suche über das Eingabefeld 'Filter' ein.

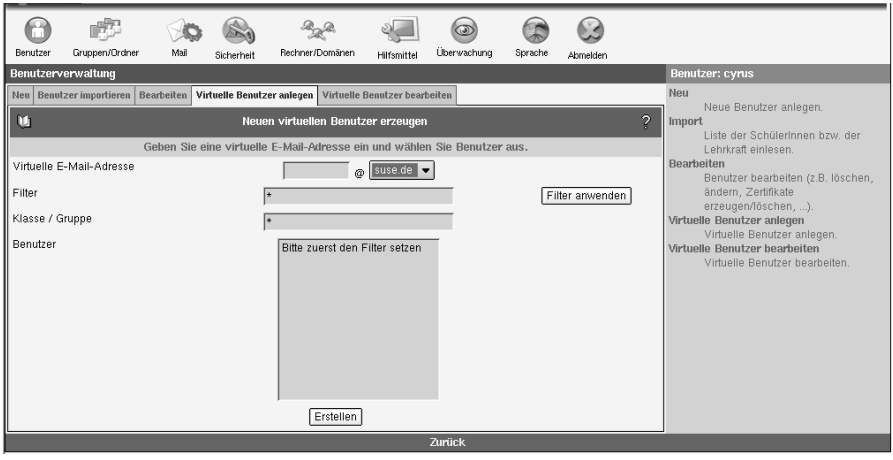


Abbildung 4.5: *Anlegen eines virtuellen Benutzers*

Geben Sie eine virtuelle E-Mailadresse ein und wählen Sie aus den virtuellen Domains eine aus. Markieren Sie einen oder mehrere Benutzer und klicken Sie auf 'Erstellen'. Ab sofort erhalten die festgelegten Benutzer alle E-Mails, die an die virtuelle Adresse gesendet werden.

Bearbeiten der virtuellen Benutzer

Um die Adresse eines virtuellen Benutzers zu ändern, klicken Sie auf 'Bearbeiten' und wählen die zu bearbeitende Adresse aus. Sie können dieser die Adresse eines anderen (realen) Empfängers zuweisen oder die virtuelle Adresse löschen.

Gruppen und Ordner

Sie können Ihren Benutzern Gruppen zuordnen, um z. B. die Rechtevergabe für Ordner zu vereinfachen oder eine Mailingliste zu erstellen. Weiterhin können Sie gemeinsame Ordner für mehrere Benutzer oder Gruppen anlegen. Zusätzlich ist es möglich, durch das Feature 'Direkte Mailzustellung' E-Mails auch an Benutzer zu verteilen, die nicht IMAP sondern POP verwenden und somit keinen Zugriff auf geteilte Ordner haben.

Mit dieser Funktionalität kann auch sehr einfach eine Mailingliste aufgebaut werden.

Anlegen einer Gruppe

Mit dem Untermenü 'Gruppen anlegen' aus dem Menü 'Gruppen' erstellen Sie eine neue Gruppe (siehe Abb. 4.6 auf der nächsten Seite). Wählen Sie einen eindeutigen Gruppennamen aus.

Achtung

Gruppennamen

Verwenden Sie für den Gruppennamen nur Kleinbuchstaben, keine Sonderzeichen und auch keine Leerstellen!

Achtung

Geben Sie der Gruppe eine aussagekräftige Beschreibung. Wir haben für Sie schon drei verschiedene Möglichkeiten vorkonfiguriert:

Klasse Hier sollten alle Schüler einer Klasse enthalten sein. Sie können hier also leicht einen gemeinsamen Ordner und/ oder eine Mailingliste für eine ganze Klasse anlegen.

Benutzergruppe Hier wird nach den verschiedenen Benutzergruppen unterschieden. Nach einer Neuinstallation des SUSE LINUX School Servers wären das z. B. die Benutzergruppen „Schüler“, „Lehrer“ und „Verwaltung“.

Arbeitsgruppe Diese Art von Gruppe kann von Lehrern mit entsprechenden Administratorrechten angelegt und/ oder bearbeitet werden.

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

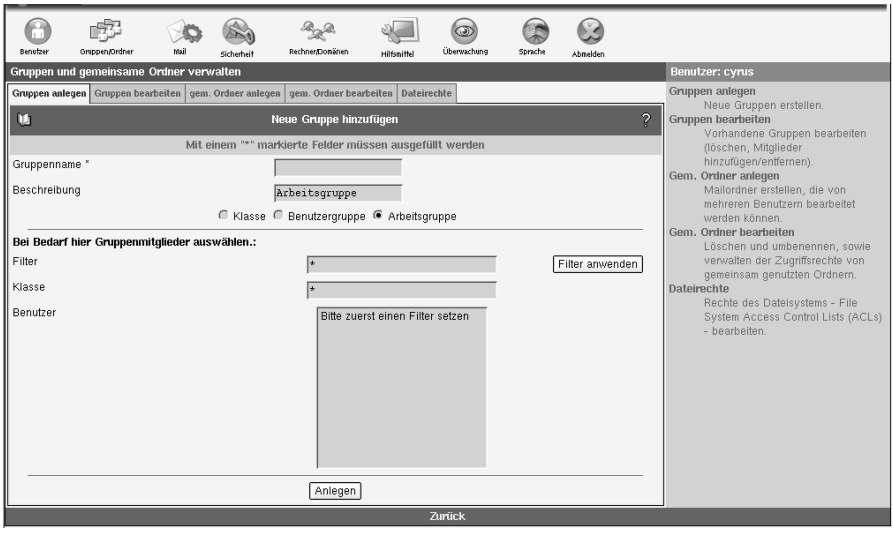


Abbildung 4.6: *Anlegen einer Gruppe*

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.

Bearbeiten von Gruppen

Sie können 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. 4.7 auf der nächsten Seite).

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.

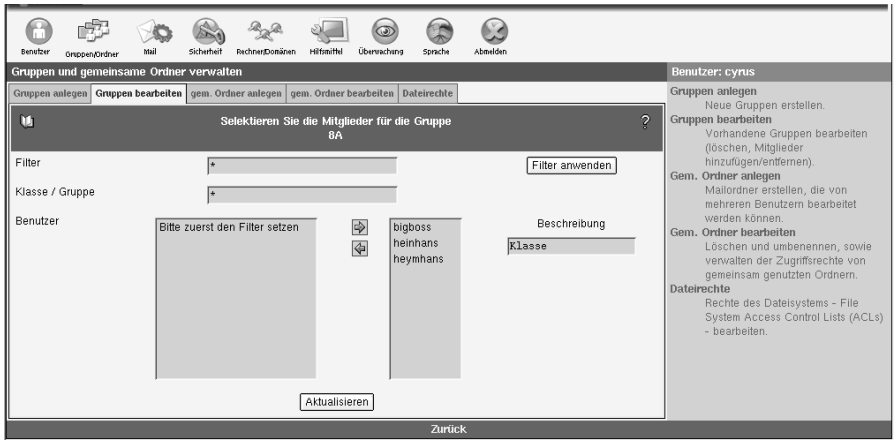


Abbildung 4.7: *Bearbeiten einer Gruppe*

Anlegen eines Ordners

Um einen neuen Ordner anzulegen, wählen Sie im Menü ‘gem. Ordner anlegen’ aus und geben einen Ordnernamen ein.

Achtung

Ordnernamen

Verwenden Sie für Ordnernamen nur Kleinbuchstaben, keine Sonderzeichen und keine Leerzeichen.

Achtung

Geben Sie dann eine aussagekräftige Beschreibung für den zu erstellenden Ordner ein. Soll der Ordner eine E-Mail-Adresse erhalten, lassen Sie die entsprechende Option aktiviert.

Wenn Sie ‘Anlegen’ wählen, werden Sie in einer neuen Maske aufgefordert Rechte für diesen Ordner zu vergeben.

Rechtevergabe für Ordner

Im oberen Teil der Maske sehen Sie bereits vergebene Rechte. Grundsätzlich hat der Eigentümer alle Rechte an diesem Ordner. Diese Einstellung sollten Sie nicht verändern. Um nun Rechte an Dritte zu vergeben, müssen Sie wieder eine Liste der vorhandenen Benutzer anzeigen lassen.

Klicken Sie auf 'Filter anwenden' oder schränken Sie die Anzeige mit dem Eingabefeld 'Filter' vorher ein. Jetzt können Sie einen Benutzer auswählen.

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

Wenn Sie Ihre Auswahl mit 'Speichern' abschließen, wird die erstellte Rechtevergabe im oberen Bereich der Maske hinzugefügt und Sie können mit der Vergabe weiterer Rechte fortfahren oder die Maske verlassen.

Folgende Rechte stehen zur Verfügung:

(l)ookup Der Ordner ist sichtbar, d. h. er kann aufgelistet werden.

(r)ead Der Ordner und dort abgelegte E-Mail kann eingesehen werden.

(s)tore Bewahre den Status neu und gelesen über verschiedene Sitzungen.

(w)rite Verändern von Nachrichten-Flags (neu, beantwortet oder Entwurf) ist gestattet.

(i)nsert Einfügen von Nachrichten ist erlaubt.

(p)ost Senden einer Nachricht an die Empfangsadresse des Ordners ist möglich.

(c)reate Löschen von Ordnern unterhalb dieses Ordners ist möglich.

(d)elete Löschen von Nachrichten ist möglich.

(a)dminister Administrieren des Ordners ist erlaubt (Rechtevergabe).

Folgende Kombinationen haben sich in der Praxis bewährt:

Lesen (lrs) Auflisten von Ordnern und Lesen des Inhaltes.

Hinzufügen (lrsip) Zusätzlich ist das Hinzufügen neuer Nachrichten gestattet.

Schreiben (lrswipcd) Zusätzlich ist Erstellen und Löschen von Unterordnern oder des betreffenden Ordners selbst gestattet.

Administrieren (lrswipcda) Dies beinhaltet alle Rechte einschließlich der Vergabe von Zugriffsrechten an andere Benutzer oder Gruppen.

Bearbeiten von Ordnern und Rechten

Hier können Sie auch im später noch die Attribute der bestehenden Ordner verändern. Wählen Sie zunächst einen Ordner per Mausklick aus. Der ausgewählte Ordner wird farbig hinterlegt. Klicken Sie dann auf 'gem. Ordner bearbeiten', um die Beschreibung oder die Option des Ordners „Mails empfangen" zu verändern. Wählen Sie 'Rechte setzen', um die Rechtevergabe zu ändern.

Mit 'Löschen' wird der gewählte Ordner mitsamt allen enthaltenen E-Mails unwiederbringlich gelöscht.

Direkte Mailzustellung, Mailinglisten mit Ordnern

Eine Besonderheit bei den Ordnern nimmt die „Direkte Mailzustellung" ein. Wählen Sie 'Direkte Mailzustellung für Benutzer', um E-Mails, die an diesen Ordner gesendet werden, auch in der Inbox des jeweiligen Benutzers abzulegen.

Tipp

Direkte Mailzustellung

Das ist notwendig, wenn der Benutzer mittels POP (d.h. einem externem E-Mail-Programm) auf den Server zugreift, da mit POP keine Verwendung von Ordnern möglich ist.

Tipp

Zeigen Sie mit 'Filter anwenden' die Liste aller Benutzer auf dem System an oder schränken Sie die Anzeige zuvor mit dem Eingabefeld 'Filter' ein.

Bereits ausgewählte Benutzer sind farbig markiert. Ändern Sie per Mausklick auf die Namen die Zuordnung und schließen die Eingabe mit 'Änderungen speichern' ab. Mit 'Zurücksetzen' können Sie den Stand vor dem Bearbeiten der Liste wiederherstellen. Mit 'Zurück zur Ordnerauswahl' können Sie einen anderen Ordner zum Bearbeiten auswählen. Ebenso funktioniert die 'Direkte Mailzustellung für Gruppen'. Die Besonderheit dabei: Alle Mitglieder der Gruppe erhalten eine Kopie der eingehenden E-Mails. Mit dieser Funktion können Sie rasch eine Mailingliste erstellen, indem Sie alle Mitglieder der Mailingliste einer dafür vorgesehenen Gruppe zuordnen und einen entsprechenden Ordner mit Mailempfang anlegen, der dann seine E-Mails an diese Gruppe sendet.

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.

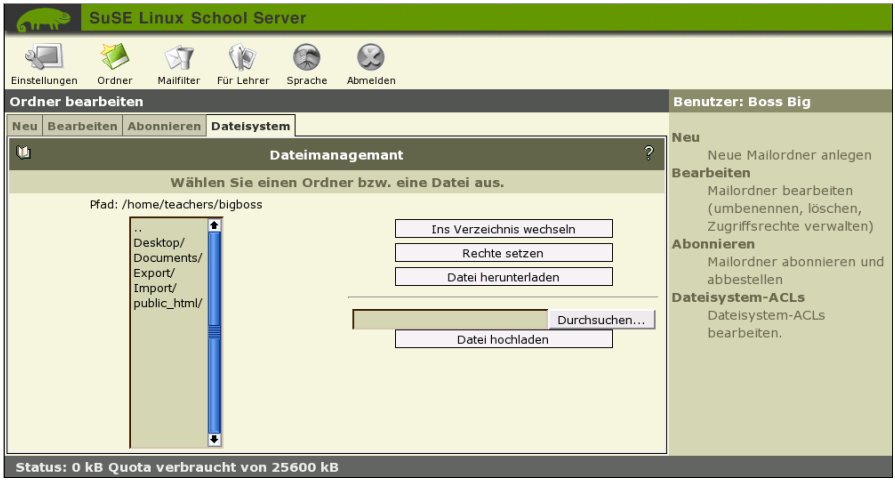


Abbildung 4.8: Dateimanagement

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 SUSE LINUX 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.

Mail

Unter dem Punkt ‘MAIL’ kann das gesamte Mailsystem eingerichtet werden. Für den Betrieb des SUSE LINUX 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: Basisfunktionalität

Über das Postfix-Interface können Sie folgende Funktionen beeinflussen (siehe Abbildung 4.9 auf der nächsten Seite):

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.

TLS diese Option ist nur sichtbar, wenn Sie eine „CA“ aufgesetzt haben. Aktivieren Sie diese, um verschlüsselte Übertragung der E-Mails sowie zertifikat-basiertes Relaying zu verwenden.

SPAM Filter Wenn Sie diese Option anschalten, wird jede per SMTP eingehende E-Mail dahingehend untersucht, ob es sich um eine unerwünschte Werbemail handelt. Hierzu wird jede E-Mail getagged. Das bedeutet, es werden einige Informationen an den Kopf (engl. *Header*) jeder E-Mail angehängt. Weiter wird zunächst nichts gemacht. Jeder Benutzer kann jetzt entscheiden, was er mit einer als SPAM gekennzeichneten E-Mail machen will.

Postfix für Experten

In dieser Maske lassen sich nahezu alle Parameter von Postfix ändern, entfernen oder neu hinzufügen (siehe Abbildung 4.10 auf Seite 82).

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

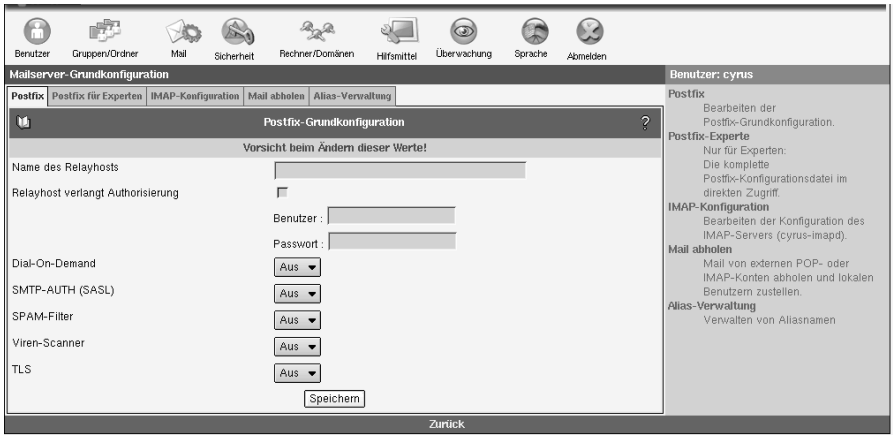


Abbildung 4.9: *Postfix Grundkonfiguration*

IMAP Konfiguration

Hier können Sie einige grundlegende Einstellungen treffen, wie der SUSE LINUX 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.

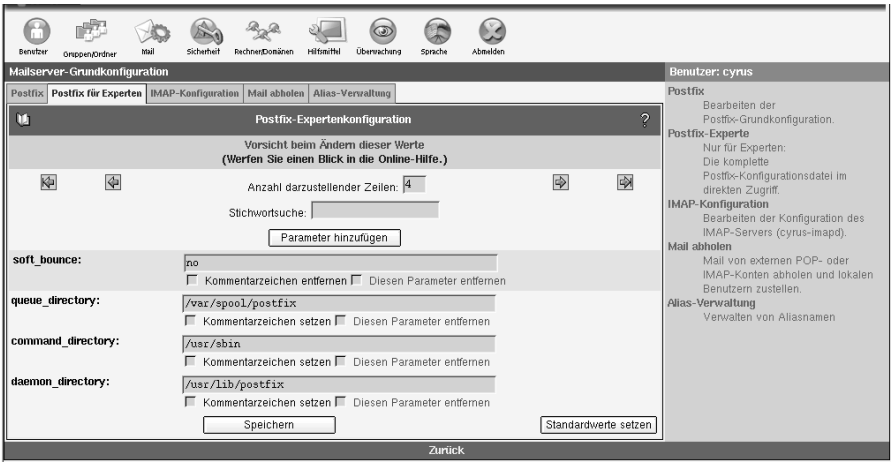


Abbildung 4.10: *Postfix Experten-Konfiguration*

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. `mailadmin`, d. h. ohne die E-Mail-Domäne.

Hinweis

Mail abholen

Sofern Sie für Ihren Server eine feste, offizielle IP-Adresse benutzen und Ihr Mailserver für Ihre Domain „verantwortlich“ ist (d. h. es existiert ein „mx-record“ in einem offiziellen Nameserver), werden Sie diese Funktionalität nicht benötigen.

Sie benötigen 'Mail abholen', sofern E-Mail-Konten bei einem Provider abgerufen werden und die E-Mail an einen der lokalen Benutzer gehen soll. Wählen Sie

'Neu' um einen neuen Eintrag hinzuzufügen und 'Editieren', um einen existierenden Eintrag zu bearbeiten (siehe Abbildung 4.11).

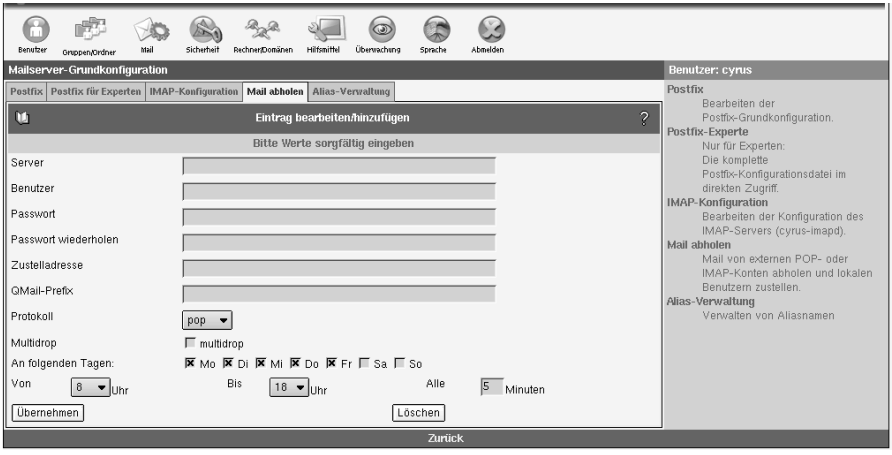


Abbildung 4.11: *Mail abholen*

Geben Sie hier die nötigen Daten für das Login auf dem fernen Mailserver an. Als „Zustelladresse" geben Sie die vollständige E-Mail-Adresse eines Ihrer lokalen Benutzer an. Dieser erhält alle von diesem Konto abgerufenen E-Mails.

Beim „Protokoll" können Sie zwischen POP und IMAP wählen. In der Regel bieten Provider POP an. Ob IMAP möglich ist, müssen Sie evtl. erfragen. Sofern es sich um ein Multidrop Konto handelt (E-Mail an verschiedene Benutzer mit derselben Domain wird in nur einem Konto abgelegt), aktivieren Sie diese Schaltfläche. Sie müssen in diesem Fall keine Zustelladresse angeben, da der SUSE LINUX School Server die Verteilung der E-Mails eigenständig vornimmt. Hier hat auch das „QMail Prefix" Bedeutung. Wenn Ihr Provider auf seinem System QMail verwendet (und nur dann), gibt es eine Besonderheit bei den Empfängeradressen. Jemand sendet beispielsweise eine E-Mail an Ihre Schule, genauer an `user@schule.de`. Der QMail-Server des Providers schreibt z. B. Folgendes in den Mailheader: „Delivered-To: multidrop-user@schule.de". Das QMail-Prefix wäre in diesem Beispiel „multidrop-". Wie das genaue Prefix lautet, hängt von den Einstellungen ab, die Ihr Provider auf seinem System vorgenommen hat (fragen Sie bitte nach).

Mit den Schaltflächen 'An folgenden Tagen' können Sie den Abruf auf bestimmte Tage beschränken. Mit der Angabe „Mo Di Mi Do Fr, von 8 bis 18 Uhr, alle 15 Minuten" können Sie das Abrufen auf Ihre Kernarbeitszeit beschränken. Das Intervall für den Abruf spielt vor allem bei „Dial on Demand"-Verbindungen

(z. B. mit ISDN) eine große Rolle. Um Kosten zu sparen, können Sie die Intervalldauer verlängern, da sich der SUSE LINUX School Server für jeden Abruf eigens bei Ihrem Provider einwählen muss.

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 1: *Inhalt der Datei call*

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

Datei 2: *Inhalt der Datei config*

```
port    TCP
type    tcp
```

Datei 3: *Inhalt der Datei port*

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

Datei 4: *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 84 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.

Alias-Verwaltung

Dieses Frontend erleichtert Ihnen die Verwaltung sogenannter „Mail-Aliase". Jedem Mail-Empfänger können beliebig viele Aliase zugeordnet werden. Auf der Oberfläche sehen Sie links die vergebenen Aliase, daneben die ihnen zugeordneten Benutzernamen. Die Alias-Felder können direkt editiert werden. Klicken Sie anschließen auf 'Speichern.'

Wollen Sie einen Alias entfernen oder weitere Benutzer zu einem Alias hinzufügen, klicken Sie rechts auf 'Hinzufügen/Entfernen'. Sie werden zu einer weiteren Maske geleitet, in der Sie mit Hilfe der Pfeiltasten vorhandene Benutzer zum Alias hinzufügen oder entfernen können. Entfernen Sie alle Benutzer, so wird auch der selektierte Alias entfernt.

In diesem Dialog können keine Aliase neu angelegt werden, gehen Sie dazu nach'Benutzer' → 'Bearbeiten'. Wählen Sie den Benutzer aus,dem ein neuer Alias zugewiesen werden soll, und klicken Sie auf 'Benutzerdaten ändern'. Tragen Sie hier einen oder mehrere durch Leerzeichengetrennte E-Mail-Aliase ein und klicken Sie auf 'Aktualisieren'. Wenn Siezurück zur 'Alias-Verwaltung' gehen, erscheint dann auch dieser Benutzermit entsprechendem Alias in der Liste.

Sicherheit

Hinweis

Sichere Grundkonfiguration

Hier können Sie einige Einstellungen ändern, welche die Sicherheit einiger Serverdienste betreffen. Normalerweise brauchen Sie hier keine Änderungen vorzunehmen, da alle Dienste schon mit einer sicheren Vorabkonfiguration gestartet werden.

Hinweis

SSL-Konfiguration

Der Dialog zur SSL-Konfiguration gliedert sich in drei Bereiche (vgl. Abbildung 4.12). Sie konfigurieren hier SSL für Apache, für den Cyrus IMAPD und für OpenLDAP.

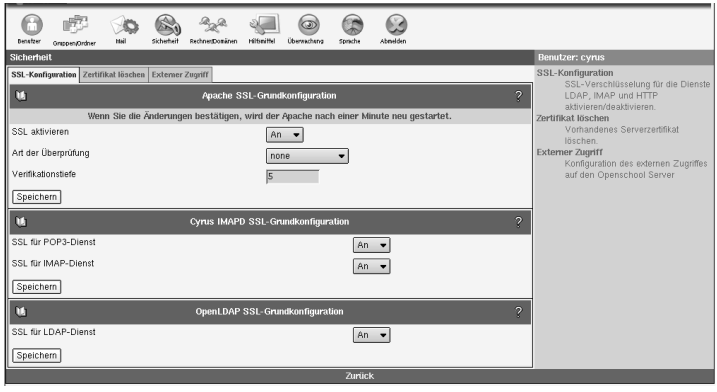


Abbildung 4.12: *SSL-Konfiguration*

Apache SSL Grundkonfiguration

Mit dem Button 'SSL Aktivieren' ermöglichen Sie eine sichere Verbindung Ihrer Clients zum Server. Der Button ist nur wählbar, wenn Sie eine CA (engl. *Certificate Authority*) und ein Server-Zertifikat erstellt haben. Wählen Sie anschließend die Art der Überprüfung:

none Es findet keine Überprüfung auf ein gültiges Zertifikat statt.

optional Das Vorhandensein eines Zertifikats wird geprüft, auch ohne Zertifikat wird der Zugang gewährt.

require Zugang ist nur mit gültigem Zertifikat möglich.

optional_no_ca Es wird auf ein vorhandenes Zertifikat geprüft, dieses muss aber nicht gültig sein.

CAs können hierarchisch sein. Das heißt, eine CA kann durch eine andere CA validiert werden. Die Gültigkeit dieser kann wiederum durch eine „höhere" CA bestätigt werden usw. Mit 'Verifikationstiefe' wird festgelegt, wie tief (wie viele Stufen zurück) der Apache Webserver die Gültigkeit von CAs zurückverfolgen soll, bis sie abgelehnt werden. Die Voreinstellung ist '10'.

Cyrus IMAPD SSL Grundkonfiguration

Aktivieren Sie SSL für IMAP und POP3. Beachten Sie bitte, dass der POP3/IMAP Server bei jeder Aktivierung oder Deaktivierung neu gestartet werden muss. Es kommt also zu Verbindungsabbrüchen bei allen Mailclients, die den Server aktuell benutzen.

OpenLDAP SSL Grundkonfiguration

Aktivieren Sie SSL für den LDAP-Dienst. Beachten Sie auch hier, dass bei jeder-Änderung der LDAP-Server neu gestartet werden muss.

Zertifikatverwaltung

Im Dialog der Zertifikatverwaltung können Sie Ihr bestehendes Server-Zertifikat löschen. Dazu benötigen Sie das CA-Passwort, das Ihrem admin-Passwort entspricht. Ist das Zertifikat entfernt, erhalten Sie die Möglichkeit, ein neues zu erstellen oder ein Zertifikat zu importieren. Bei Neuerstellung können Sie die bestehende CA nutzen oder diese auch neu aufsetzen.

Hinweis

Wenn Sie Ihre CA entfernen oder neu aufsetzen, verlieren bereits erstellte Client-Zertifikate ihre Gültigkeit.

Hinweis

Sie können eine eigene CA (engl. *Certificate Authority*) erstellen oder ein voneinem „Trustcenter“ unterzeichnetes Zertifikat importieren. Letzteres istkostenpflichtig und für die einwandfreie Funktion Ihres SUSE LINUX School Servers nicht notwendig.

Erstellen Sie ein eigenes Zertifikat, um den SUSE LINUX School Server als CA zu nutzen. Füllen Sie die nötigen Felder aus. Das „Passwort für die CA“ benötigen Sie später, um für Ihre Clients Zertifikate erstellen zu können. Das Passwort kann nachträglich nicht geändert werden.

In der nächsten Maske erzeugen Sie jetzt das Server-Zertifikat, das von der CA signiert wird. Vergeben Sie hier möglichst ein anderes Passwort. Mit ‘Rechnername des Webservers’ ist der Name Ihres SUSE LINUX School Servers gemeint. Wenn der im Server-Zertifikat gespeicherte Name nicht diesem Namen entspricht, werden einige Browser wie Netscape bei jeder sicheren Verbindung zu Ihrem SUSE LINUX School Server das Zertifikat anzweifeln. Nachdem Sie das Server-Zertifikat erzeugt haben, können Sie für einzelne Benutzer Zertifikate erzeugen. Außerdem können Sie jetzt die SSL-Funktion von Apache und Postfix aktivieren.

Externer Zugriff

Normalerweise blockiert die Firewall des SUSE LINUX School Servers jeden Zugriff vom externen Interface. Hier können Sie den SUSE LINUX School Server so konfigurieren, dass einige Dienste auch über das Internet erreichbar sind.

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 SUSE LINUX School Server so administrieren, als ob Sie direkt am Rechner selbst säßen. 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://<ip-adresse>: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 199.

Achtung

Jeder am SUSE LINUX School Server exisiterende Nutzer (mit Ausnahme von `admin`) 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://<ip-adresse>/` 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

Rechner/Domänen

Neue Clients anmelden

Unabhängig von dem Betriebsystem des Clientrechners müssen Clients am SUSE LINUX School Server angemeldet werden, um die Workstations einem Schulraum zuzuordnen und entsprechende DNS- und DHCP-Dienste einzutragen.

Vor der eigentlichen Anmeldung müssen die Clients vorab meist noch richtig konfiguriert werden. Wir wollen Ihnen hier nur eine kurze Stichwortliste für die einzelnen Clientarten anbieten. Ausführlichere Erläuterungen hierzu finden Sie im Kapitel 5 auf Seite 119.

SuSE Linux Clients mit Autoinstallation

- Installieren Sie die Clients über die Autoinstallationsfunktion des SUSE LINUX School Servers wie im Kapitel 6 auf Seite 145 beschrieben.
- Starten Sie einen Webbrowser und registrieren Sie den Client wie im weiteren Verlauf dieses Kapitels beschrieben.
- Starten Sie zur Sicherheit die Netzwerkdienste des Clients (mit `rcnetwork restart` neu oder rebooten Sie den Client.

Anbinden vorhandener Linux Clients

- Konfigurieren Sie die Netzwerkkarte des Clients so, dass er seine IP-Adresse und seinen Namen über `DHCP` erhält, und starten Sie bei Bedarf die Netzwerkdienste neu.
- Konfigurieren Sie den Client über YaST2 als `LDAP-Client`.
- Konfigurieren Sie den Client über YaST2 als `NFS-Client`.
- Starten Sie einen Webbrowser und registrieren Sie den Client wie im weiteren Verlauf dieses Kapitels beschrieben.
- Starten Sie zur Sicherheit die Netzwerkdienste des Clients (mit `rcnetwork restart` neu oder rebooten Sie den Client.

Windows Clients

- Konfigurieren Sie die Netzwerkkarte des Clients so, dass er seine IP-Adresse über `DHCP` erhält und starten Sie den Rechner neu.
- Starten Sie einen Webbrowser und registrieren Sie den Client wie im weiteren Verlauf dieses Kapitels beschrieben.

- Ändern Sie anschließend den Namen des Clients in den Netzwerkeigenschaften so ab, dass er mit dem über `DHCP` vergebenen übereinstimmt und starten Sie den Rechner neu.
- Nehmen Sie den Client bei Bedarf in die Domäne auf, wie unter 5 auf Seite 122 beschrieben, und starten Sie den Rechner neu.

Mac-Clients

- Starten Sie zunächst den `Netatalk-Dienst` auf dem Server, indem Sie in den Administrationsseiten des SUSE LINUX School Servers unter 'Überwachung' → 'Dienstüberwachung' den Dienst `Netatalk` aktivieren und starten.
- Konfigurieren Sie die Netzwerkkarte des Clients so, dass er seine IP-Adresse über `DHCP` erhält.
- Starten Sie einen Webbrowser und registrieren Sie den Client wie im weiteren Verlauf dieses Kapitels beschrieben.
- Binden Sie die benötigten Laufwerke des Servers am Client über das Menü 'Auswahl' ein.

Um einen Client am Server anzumelden, starten Sie einen Browser (Konqueror, Netscape, Opera oder den Internet Explorer) und gehen Sie auf die Administrationsseiten des SUSE LINUX School Servers: `https://admin` Melden Sie sich dort als `admin` an und klicken Sie auf 'Rechner/Domänen'. Dort klicken Sie auf 'Neu' (siehe Abbildung 4.13 auf der nächsten Seite).

Sie können jetzt aus dem Menüpunkt 'Liste der registrierten Schulräume' den gewünschten Schulraum auswählen oder den Rechner einem neuen, noch nicht registrierten Raum zuordnen ('Neuen Schulraum eintragen:'). Damit wird der neue Schulraum nach einer erfolgreichen Registrierung des Clients in die 'Liste der registrierten Schulräume' aufgenommen.

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 hier nicht länger als 10 Zeichen sein.

Hinweis

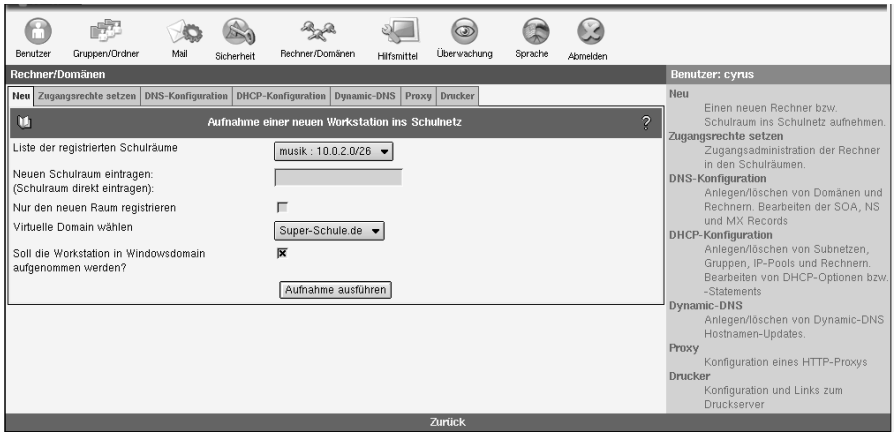


Abbildung 4.13: *Clients an den SUSE LINUX School Server anmelden*

Abbildung 4.14: *Aufnahme eines Clients*

Haben Sie eine oder mehrere virtuelle Domains für den SUSE LINUX School Server angelegt, können Sie im Menüpunkt 'Virtuelle Domain wählen' den gewünschten Domainnamen auswählen.

Möchten Sie einen Windows-Rechner ins Schulnetz aufnehmen, müssen Sie den Menüpunkt 'Soll die Workstation in Windowsdomain aufgenommen werden?' anwählen. Anschließend klicken Sie auf 'Aufnahme durchführen'. Jetzt sollte das Ergebnis der Aufnahme des Clients, d.h. IP-Adresse, Hostname, Hardwareadresse und ggf. Netbiosname,dargestellt werden (siehe Abbildung 4.14). Während der Registrierung wird weiterhin ein neuer Benutzer angelegt dessen Name und Passwort der Hostname des registrierten Rechners ist. (sog. Workstationbenutzer .) Dadurch bekommt man die Möglichkeit, z. B. Klassenarbeiten in einer geschützten Umgebung machen zu lassen. In diesem Fall müssen die Schüler sich nicht mit ihrem eigenem Login (UID), sondern mit dem des Rechners an das System anmelden. So haben sie eine Standardumgebung und keinen

Zugriff auf ihre eigenen Dateien. Weiteres dazu finden Sie im Abschnitt A auf Seite 222.

Hinweis

Workstationbenutzer

Mit dem Hostname als Loginname und Passwort sollte man sich nur an den Workstation anmelden dessen Hostname identisch mit dem Loginname ist. Für die Windows-Clients und die automatisch installierten SuSE Linux Clients ist schon eine Sperre eingebaut die es verhindert, dass man sich mit vom Hostname abweichendem Workstationbenutzeraccount an einem Client anmeldet. Für Mac-Clients gibt es zur Zeit keine solche Beschränkung. Für andere 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 103
then
test $HOST = $USER || exit 1
fi
```

Datei 5: */etc/profile.local*

Hinweis

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

Nun ist Ihr Clientrechner ins Schulnetz integriert. Handelt es sich um einen Windows-Rechner, können Sie ihn als nächstes an Ihrer Domäne anmelden (siehe 5 auf Seite 122).

Im Falle eines MAC OS 9.X Clients sind alle Aufgaben erfüllt.

Linux-Clients bedürfen auch keiner weiteren Konfiguration, wenn diese mit dem mitgelieferten Autoinstallationstool installiert worden sind – ansonsten sehen Sie bitte im Abschnitt 5 auf Seite 120 nach.

Tipp

Clientinformation ändern

Wenn sich die Hardwareadresse eines Clients (z. B. aufgrund einer neuen Netzwerkkarte) geändert hat, müssen Sie den entsprechenden Clienteintrag zuerst löschen und anschließend neu anlegen.

Tipp

Löschen eines Clienteintrags vom Server

Wenn Sie den Eintrag für einen Client am Server löschen wollen, müssen Sie seinen Eintrag aus dem DHCP-Server entfernen.

Wählen Sie dazu den Menüpunkt 'DHCP-Konfiguration' im Abschnitt 'Rechner/Domänen' aus. Suchen Sie nun in der entsprechenden Gruppe nach dem betreffenden Hostnamen und klicken Sie auf die dahinter liegende Schaltfläche (Löschen). Um die Änderung zu Aktivieren, betätigen Sie anschließend noch die Schaltfläche (Exportieren)ganz unten auf der Seite.

Zugangsrechte setzen

Haben Sie die Rechner der Schule an den SUSE LINUX School Server angemeldet und Schulräumen zugewiesen, besteht die Möglichkeit, den Rechnern eines Schulraumes bestimmte Dienste (Internetzugang, Zugang zu den Mail- bzw. Groupwareserver, Zugang zu den Printserver) zu sperren bzw. zu gestatten. Der Zugang zum Hauptserver (`https://admin`) kann jedoch nicht gesperrt werden, da dieser Dienste anbietet (`DNS`, `DHCP`, `nfs`, `samba`), auf die nicht verzichtet werden kann.

Diese Möglichkeit besteht jedoch nicht nur für den Hauptadministrator `admin` sondern auch für Lehrer. Diese können die Dienste allerding nur für den aktuellen Klassenraum setzen. Der Hauptadministrator `admin` hat die Kontrolle über sämtliche registrierten Schulräume.

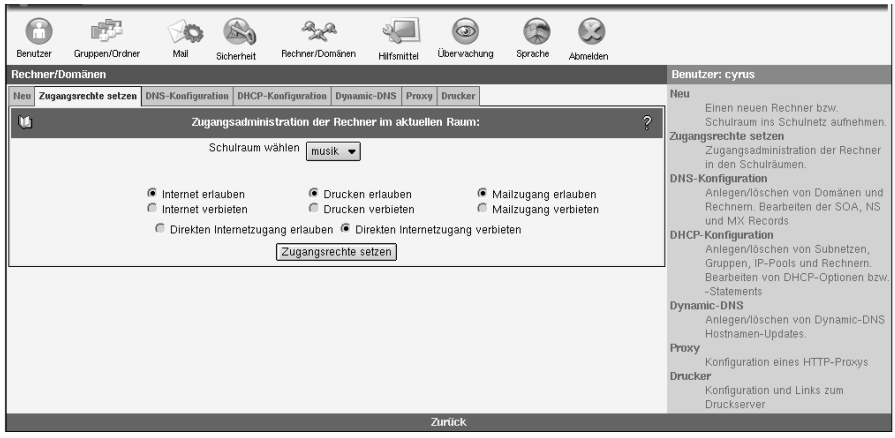


Abbildung 4.15: *Zugangsadministration der Rechner in den Schulräumen*

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 SUSE LINUX 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 SUSE LINUX 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 SUSE LINUX 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 4.16). Auf diese Weise können Sie beliebig viele virtuelle Domains hinzufügen.

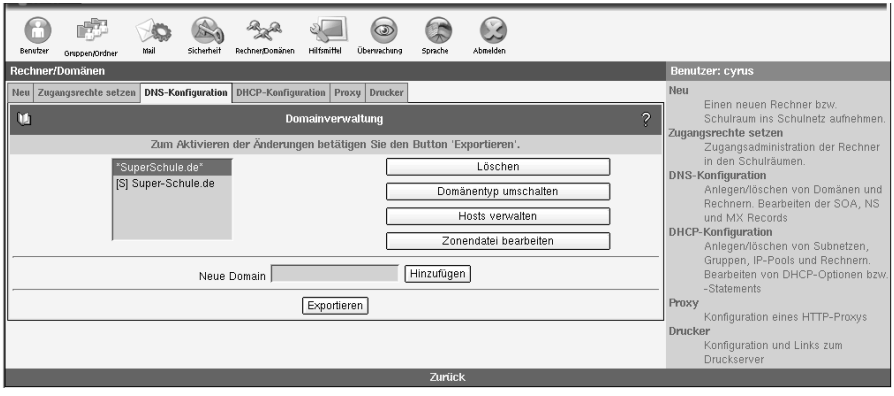


Abbildung 4.16: *Anlegen und Bearbeiten von virtuellen Domains*

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 SUSE LINUX School Servers und die virtuellen Domains selbst noch Zonendatenbanken hinzufügen, benutzen Sie einfach Namen, die mit den vom SUSE LINUX 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 SUSE LINUX 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 S (default) Alle lokalen Benutzer können unter dem Namen der Domain E-Mail empfangen. Zusätzlich können weitere „virtuelle“ Adressen angelegt werden, die an bestimmte lokale Benutzer gebunden sind. Diese Art virtueller Domain wurde auch schon vom SuSE Linux Openexchange Server 4 verwendet. In der postfix-Dokumentation wird dies als `SENDMAIL-STYLE VIRTUAL DOMAIN` bezeichnet.

Typ P 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. Die postfix-Dokumentation bezeichnet diesen Typ als `POSTFIX-STYLE VIRTUAL DOMAIN`.

Wir möchten Ihnen empfehlen, die Einstellung vom Typ `P` zu verwenden. Dies erkennen Sie an einem vorangestellten `[P]` vor dem Domainnamen.

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.

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 4.17 auf der nächsten Seite).

Sie sehen in diesem Menü auch die bestehenden Subnetze, Gruppen, Rechner und IP-Pools, die schon während der Installation des SUSE LINUX 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.

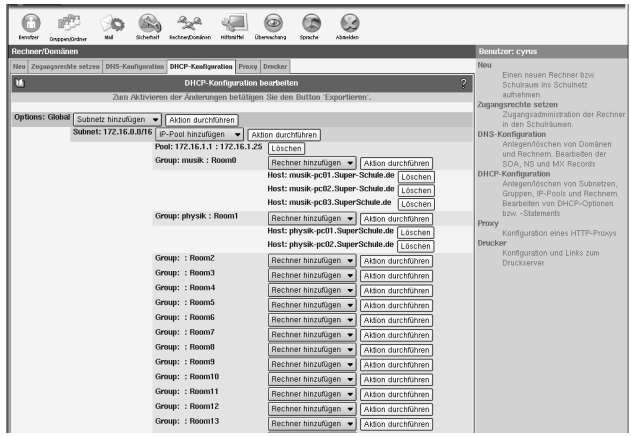


Abbildung 4.17: *DHCP-Konfiguration*

Achtung

Beim Löschen eines Eintrages werden alle untergeordneten Einträge auch gelöscht.

Achtung

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 die-Generierung 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 Cache ist voreingestellt auf 500 MB, kann allerdings geändert werden. Die Checkbox 'SquidGuard benutzen' ist aktiviert, kann allerdings hier abgeschaltet werden, wenn Sie SquidGuard nicht benutzen wollen.

Mehr Informationen zum Programm SquidGuard finden Sie im Anhang unter B auf Seite 229.

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

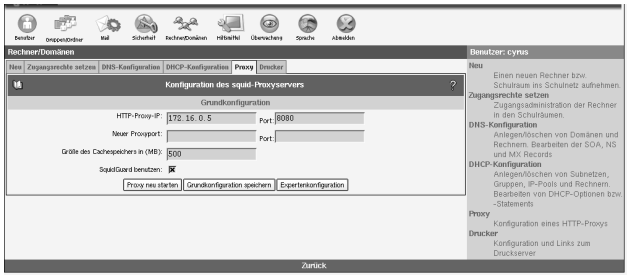


Abbildung 4.18: *Proxy-Konfiguration*

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.

ACLs definieren

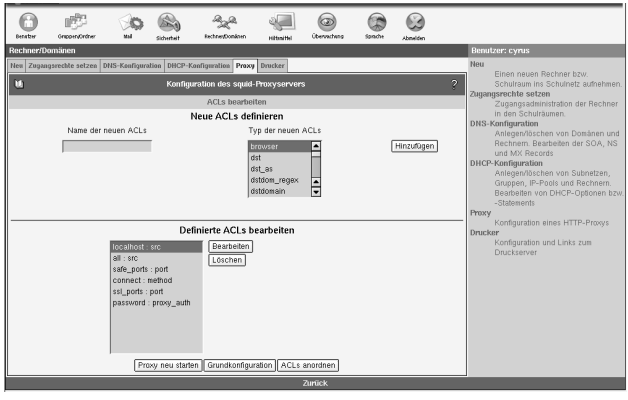


Abbildung 4.19: *ACL-Definition*

In Abbildung 4.19 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 Beschreibungenzu den verschiedenen ACLs liefert Ihnen die Seite: `http://squid.visolve.com/squid24s1/access_controls.htm`

Klicken Sie auf ‘Hinzufügen’, 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 ‘Hinzufügen’ 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 (vgl. Abbildung 4.20 auf der nächsten Seite) 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. Wenn Sie auf 'Administration' klicken, müssen Sie sich als Benutzer `root` mit dem Administrator-Passwort (identisch mit dem `admin`-Passwort) einloggen. Unter 'Help' finden Sie ausführliche Anleitungen zu allen Konfigurationsmöglichkeiten.

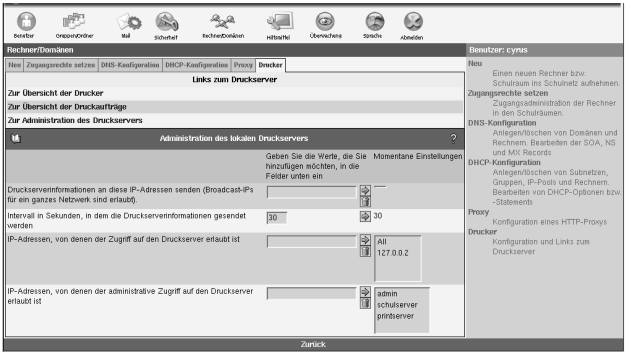


Abbildung 4.20: *Drucker-Verwaltung*

Im unteren Teil des Druckerdialogs nehmen Sie Einstellungen zum lokalen Druckserver vor. Geben Sie an, an welche IP-Adressen oder Broadcast-IPs für ein ganzes Netzwerk an, die Druckserver-Informationen geschickt werden sollen. Mit Return oder über das Pfeil-Symbol wird die Eingabe zu den aktuellen Einstellungen übernommen. Stellen Sie anschließend das Intervall ein, innerhalb dessen die Informationen versendet werden. Im folgenden Feld geben Sie die IP-Adressen aller Rechner an, die Zugriff auf den Druckserver erhalten, und im letzten Feld erteilen Sie bestimmten Rechnern über deren IP-Adressen administrativen Zugriff auf den Druckserver.

Hilfsmittel: Zusätzliche Funktionen

LDAP Browser: Editieren der LDAP-Datenbank

Der SUSE LINUX 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 kleinste Änderungen an den Einstellungen vornehmen, nutzen Sie den LDAP-Browser zum Ändern, Löschen und Hinzufügen von Attributwerten zu bestehenden Einträgen (vgl. Abbildung 4.22).

Abbildung 4.21: *Baumstruktur des LDAP-Browsers*

Achtung

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

Achtung

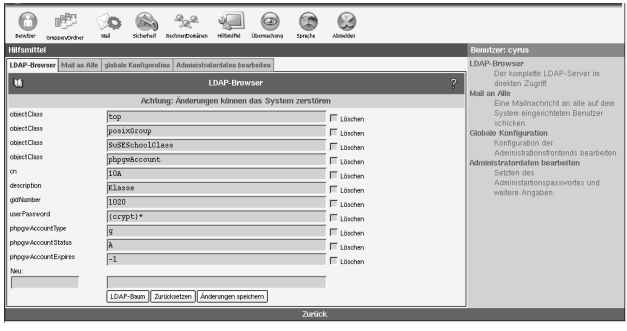


Abbildung 4.22: *Bearbeiten eines LDAP-Eintrages*

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 wieder 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`.

Wenn Sie sich ein wenig genauer mit `LDAP` auseinandersetzen möchten, empfehlen wir Ihnen einen Blick in den Anhang unter G auf Seite 259.

Mail an Alle: Nachricht vom Administrator

Es kann vorkommen, dass der Mailadministrator (`mailadmin`) allen angelegten Benutzern eine E-Mail zukommen lassen will. Beispielsweise soll der SUSE LINUX School Server wegen Wartungsarbeiten abgeschaltet werden. Geben Sie hier den Betreff und den Nachrichtentext ein (siehe Abb. 4.23). Die E-Mail erreicht jeden vorhandenen Benutzer ohne Rücksicht auf dessen Quota.

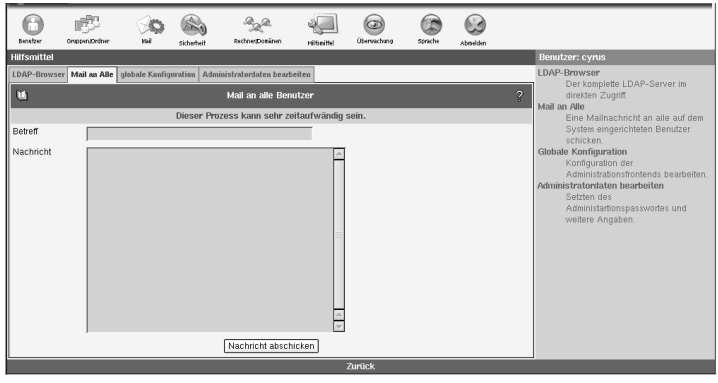


Abbildung 4.23: *Eine Mail vom Administrator*

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 207.

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.

EnableDynDns Aktivieren Sie Dynamic DNS

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.

als

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.

FETCHD

debug Setzen Sie diese Option auf einen Wert größer 0 und starten den „fetchd" mittels `rcfetchd restart` neu, erhalten Sie Debuginformationen.

keeponserver Wenn Sie diese Option aktivieren, werden die E-Mails auf dem Server nicht gelöscht, nachdem sie abgeholt wurden. Sie sollten diese Option nicht aktiviert lassen, da dann grundsätzlich immer wieder alle E-Mails erneut abgeholt werden.

unixsocket Über diesen Socket findet die Kommunikation vom Webclient mit dem fetchd statt.

ldaphost Hier können Sie den Rechnernamen oder die IP-Adresse des LDAP Servers eingeben, in dem der fetchd die Daten der Benutzerpostfächer speichern soll.

ldap_reconnect_interval Der fetchd hält eine permanente Verbindung zum LDAP Server offen. Sollte diese Verbindung einmal geschlossen oder ungültig sein, wird innerhalb des hier angegebenen Intervalles (in Sekunden) eine neue Verbindung aufgebaut.

ldap_max_reconnect Hier können Sie einstellen, wie viele Versuche fetchd maximal machen soll, eine unterbrochene Verbindung zum LDAP Server neu aufzubauen.

mailadmin Der Name des lokalen Ordneres, in welchem administrative Nachrichten gespeichert werden.

append_fetch_header Soll an jede E-Mail, die mittels fetchd abgeholt wurde, ein spezieller Header angefügt werden?

drop_undeliverable_mail Unzustellbare Mail wird kommentarlos verworfen, wenn Sie diese Option auf `true` setzen.

thread_max Der fetchd beeinhaltet einen rudimentären Scheduler, der maximal so viele Prozesse gleichzeitig startet, wie hier angegeben wird. Sie sollten den Wert nicht zu hoch setzen, da ein solcher Prozess u.U. viel Speicher verbrauchen kann.

priority_granularity Dieser Wert sollte immer mindestens doppelt so groß sein wie der Wert von 'thread_max'.

SQUID

squid_conf_file Geben Sie hier die Konfigurationsdatei für Squid an.

Administratordaten bearbeiten

In dem Menüpunkt 'Administratordaten bearbeiten' können Sie die Daten und das Passwort von dem Hauptadministrator `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 (siehe Abbildung 4.24) ein.

Hinweis

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

Hinweis

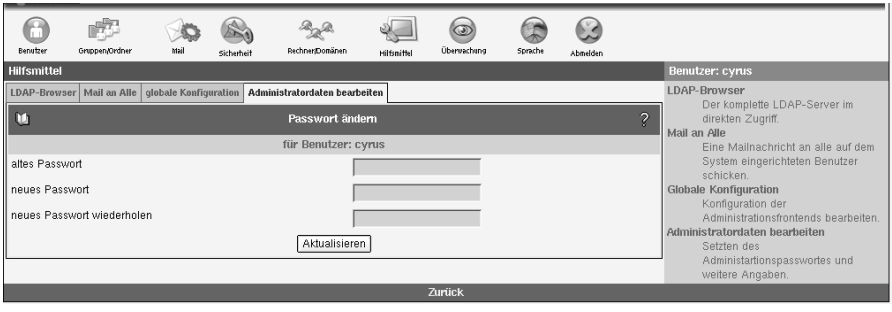


Abbildung 4.24: *Passwort des Administrator ändern*

Überwachung des Systems

Wer ist online?

Hier erhalten Sie eine Übersicht über die Benutzer, die momentan per Webfrontend online sind. Es handelt sich nur um die internen Sitzungen am SUSE LINUX School Server POP bzw. IMAP Verbindungen werden hier nicht gelistet. Durch einen Klick auf die Benutzer ID löschen Sie die jeweilige Sitzung des Benutzers. Ihre eigene Sitzung kann nicht gelöscht werden.

Abbildung 4.25: *Wer ist online?*

Mail-Warteschlange

In dieser Maske sehen Sie die von Postfix zur Zeit bearbeiteten E-Mails. Geben Sie die Refreshrate 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 werden hier dauerhaft keine E-Mails angezeigt. Sollte das Postfixsystem gestoppt werden oder aus irgendwelchen Gründen keine E-Mails zustellen können, werden zuzustellende E-Mails hier erscheinen.

Mit dem Button 'Queue leeren' wird Postfix veranlasst, 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!

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 SUSE LINUX School Servers.

Hinweis

Wenn Sie Änderungen an Ihrer Hardware vorgenommen haben, z. B. wenn Sie eine Festplatte umpartitionieren, 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
```

Hinweis

Dienstüberwachung

Hier erhalten Sie eine Übersicht wichtiger Systemdienste und deren aktuelle Zustände (vgl. Abbildung 4.26 auf der nächsten Seite). Sie sehen alle Dienste, die aktuell hinter dem Parameter `MonitorServices` in `/etc/imap/globals.conf` aufgelistet werden.

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 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'.

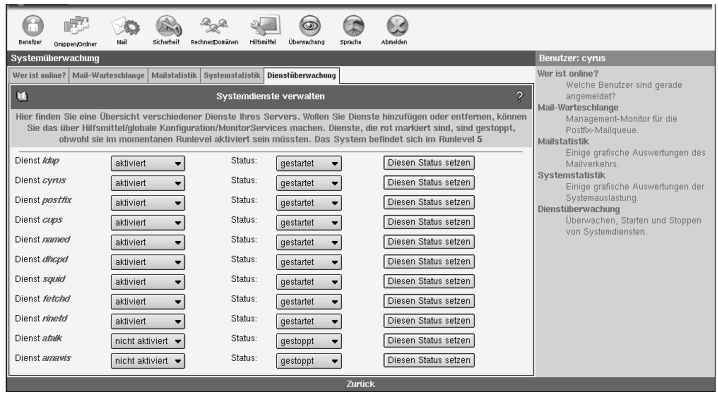


Abbildung 4.26: *Überwachung der Systemdienste*

Sprache

Wählen Sie hier Ihre bevorzugte Sprache für das Webfrontend und klicken Sie anschließend auf den Knopf `Sprache wählen`.

Client-Konfigurationen

Der SUSE LINUX School Server ist nicht nur für die Kommunikation mit Linux Clients sondern auch mit Windows-Rechnern vorkonfiguriert. Dieses Kapitel zeigt Ihnen, worauf Sie dabei achten müssen und wie Sie entsprechende heterogene Netzwerke konfigurieren.

Konfiguration von Linux Clients

Damit sich SuSE Linux Benutzer dem SUSE LINUX School Server gegenüber authentifizieren können und von dort ihre Heimatverzeichnisse mittels „automounter“ erhalten, müssen die Rechner als LDAP-Clients konfiguriert werden.

Wenn die Clients über das mitgelieferte Autoinstallationstool installiert worden sind, ist das nicht mehr nötig.

Tipp

Unter Umständen müssen dazu zunächst noch einige RPM-Pakete auf den Clients nachinstalliert werden. Sie können diese benötigten Pakete über das YaST Modul ‘Software installieren oder löschen’ nachinstallieren.

Ändern Sie dazu den Filter auf „Paketgruppen“ und markieren Sie im Zweig `Produktivität/Netzwerk/LDAP/Client` die Pakete:

- `nss_ldap`
- `pam_ldap`
- `openldap2-client`

sowie im Zweig `System/YaST` das Paket:

- `yast2-ldap-client`

Tipp

Rufen Sie das YaST Modul ‘LDAP-Client’ auf (vgl. Abbildung 5.1 auf der nächsten Seite).

Aktivieren Sie die Checkbox ‘LDAP verwenden’ und tragen Sie die ‘LDAP base DN’ ein. Im zweiten Feld geben Sie den SUSE LINUX School Server als LDAP-Server an. Wenn auf dem SUSE LINUX School Server SSL für LDAP aktiviert ist, aktivieren Sie auch auf Client-Seite die TLS/SSL-Verschlüsselung für die Kommunikation mit dem Server. Bestätigen Sie Ihre Eingaben mit ‘Beenden’.

Unter ‘Netzwerkgeräte’ → ‘Netzwerkkarte’ können Sie die Netzwerkkarte folgendermaßen konfigurieren:

- Wählen Sie zunächst „Automatische Adressvergabe (mit DHCP)“.
- Unter ‘Rechnername und Nameserver’ die Checkboxen „Hostnamen über DHCP ändern“ und „Nameserver und Suchliste über DHCP aktualisieren“ aktivieren.

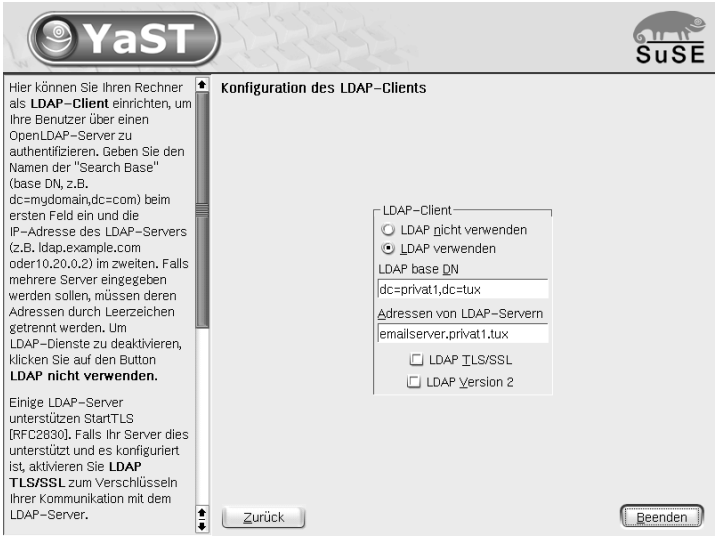


Abbildung 5.1: *LDAP Client-Konfiguration*

Das vereinfacht die Wartung des Netzwerkes - allerdings müssen Sie den Client dann auch mit seinem richtigen Namen am SUSE LINUX School Server anmelden (siehe 4 auf Seite 91).

Damit ist die Konfiguration des SuSE Linux Desktops als Client für den SUSE LINUX School Server konfiguriert.

Hier noch einmal alle Werte, die Sie evtl. zur Konfiguration benötigen:

- NFS-Client (sollte normalerweise über den Automounter automatisch erledigt werden):

  Hostname des NFS-Server: `nfs`

  Entferntes Dateisystem: `/home`

  Mountpunkt (lokal): `/home`

  Optionen: `defaults,rsize=8192,wsize=8192,soft`

- LDAP-Client

  LDAP nicht verwenden `aus`

  LDAP verwenden `an`

LDAP base DN Ihr „ldapbase“ steht auf dem SUSE LINUX School Server in der Datei `/etc/openldap/ldap.conf`.

Adressen von LDAP-Servern `ldap`

LDAP TLS/SSL `aus`

LDAP Version 2 `aus`

Windows-Clients einrichten

Falls Sie den SUSE LINUX School Server als PDC betreiben, sollten Sie zur Nutzung der Vorteile einer zentralen Nutzerverwaltung Ihre Microsoft Windows Systeme in die vom SUSE LINUX School Server betriebene Domäne integrieren. Dadurch erleichtern Sie Ihren Benutzern den Zugriff auf die vom SUSE LINUX School Server verwalteten Daten und Drucker, da nach der Anmeldung des Nutzers gegenüber dem PDC keine weitere Authentifizierung erforderlich ist.

Um den SUSE LINUX School Server als PDC für Ihre vorhandenen Microsoft Windows Clients zu benutzen, müssen Sie die jeweiligen Rechner am System anmelden. Dafür wird vom SUSE LINUX School Server automatisch ein „Maschinen-Account“ pro Workstation angelegt. Auf dem SUSE LINUX School Server sind dazu keine weiteren Schritte erforderlich. Im folgenden werden die auf den unterschiedlichen Microsoft Windows Versionen erforderlichen Schritte kurz beschrieben

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

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. 5.2 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.

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.

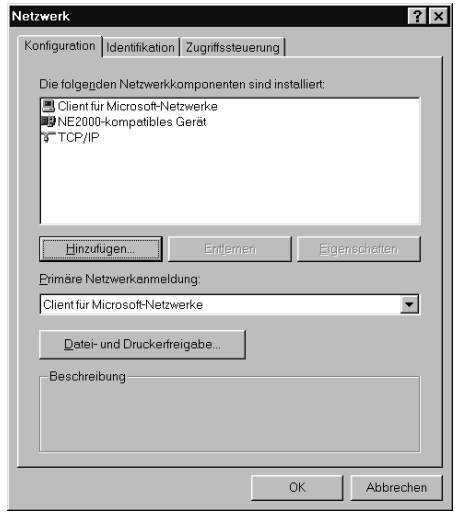


Abbildung 5.2: *Netzwerkkonfiguration unter Windows 95/98/ME*

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 SUSE LINUX 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.

Microsoft Windows NT 4

Klicken Sie mit der rechten Maustaste auf das Symbol 'Netzwerkumgebung' auf dem Desktop. Sollte das Symbol nicht vorhanden sein, öffnen Sie die Systemsteuerung 'Start' → 'Einstellungen' → 'Systemsteuerung' und führen Sie einen Doppelklick auf das Symbol 'Netzwerk' aus.

Aktivieren Sie den Reiter 'Identifikation' und klicken Sie auf den Knopf 'Ändern...' Wählen Sie 'Domäne' im Bereich 'Mitglied von' und geben Sie im Eingabefeld rechts daneben den Namen der vom SUSE LINUX School Server betriebenen Microsoft Windows Domäne an.

Aktivieren Sie die Checkbox 'Computerkonto in der Domäne erstellen' und geben Sie in den entsprechenden Feldern den Benutzernamen `Administrator` mit dem Passwort des SUSE LINUX School Server-Administrators an. Klicken Sie auf 'Ok', um die Änderungen vorzunehmen.

Windows 2000

Klicken Sie mit der rechten Maustaste auf das Symbol 'Arbeitsplatz' auf Ihrem Desktop und gehen Sie auf 'Eigenschaften'. Aktivieren Sie den Reiter 'Netzwerkidentifikation' und klicken Sie auf 'Eigenschaften' (siehe Abbildung 5.3 auf der nächsten Seite).

Im neuen Fenster aktivieren Sie den Knopf 'Domäne' unterhalb von 'Mitglied von' und geben Sie in das freie Feld den Namen Ihrer Windows Domäne in Großbuchstaben ein (siehe Abbildung 5.4 auf Seite 127).

Nachdem Sie auf 'OK' geklickt haben, werden Sie nach einem Benutzer gefragt, der berechtigt ist, ein Konto zu Ihrer Domäne hinzuzufügen. Geben Sie hier `Administrator` ein und das Passwort, das Sie während der Installation auch für den Administrator `admin` verwendet haben. Nach einem Neustart sollten Sie sich jetzt als einer der Benutzer anmelden können, die Sie auf dem SUSE LINUX School Server angelegt haben.

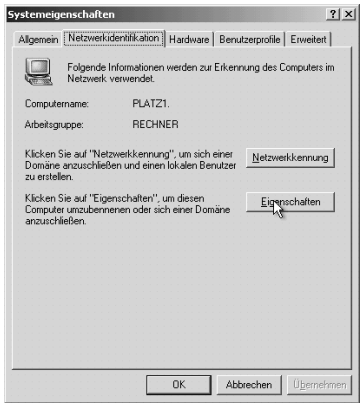


Abbildung 5.3: *Netzwerkeigenschaften unter Windows 2000*

Windows XP

Unter Windows XP müssen Sie entweder als Administrator oder als ein der Gruppe „Administratoren“ zugehöriger Benutzer angemeldet sein, um Einstellungen an der Netzwerkkonfiguration vornehmen zu können. Gehen Sie folgendermaßen vor, um den XP-Client mit dem SUSE LINUX School Server zu verbinden:

Bevor Sie fortfahren, müssen Sie sicherstellen, dass Sie keine Verbindungen von Ihrem Windows-XP-Client zu Ihrem SUSE LINUX School Server offen haben.

Öffnen Sie dazu notfalls eine Kommandozeile und geben Sie dort den Befehl `net use * /delete` ein. Damit werden alle noch offenen Netzwerkverbindungen gelöscht.

Öffnen Sie mit der linken Maustaste das ‘Startmenü’ und klicken Sie mit der rechten Maustaste auf ‘Arbeitsplatz’ und dann auf ‘Eigenschaften’ (siehe Abbildung 5.5 auf der nächsten Seite).

Aktivieren Sie im folgenden Fenster den Reiter ‘Computername’ und klicken Sie dort auf ‘Ändern’.

Im neuen Fenster aktivieren Sie den Knopf ‘Domäne’ unterhalb von ‘Mitglied von’ und geben Sie in das freie Feld den Namen Ihrer Windows Domäne ein (siehe Abbildung 5.6 auf Seite 128).

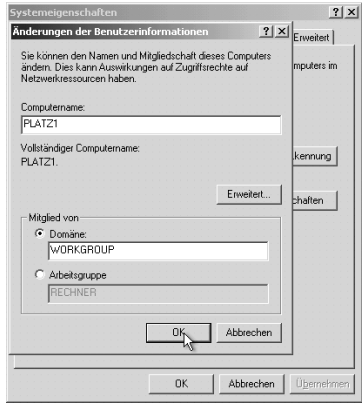


Abbildung 5.4: *Domänen-Namen ändern unter Windows 2000*

Abbildung 5.5: *Windows XP Startmenü*

Abbildung 5.6: *Domänen-Namen ändern unter Windows XP*

Nachdem Sie auf 'OK' geklickt haben, werden Sie nach einem Benutzer gefragt, der berechtigt ist, Ihrer Domäne ein Konto hinzuzufügen. Geben Sie hier `Administrator` ein und das Passwort, welches Sie während der Installation auch für den Administrator `admin` verwendet haben. Nach einem Neustart sollten Sie sich jetzt als ein Benutzer anmelden können, den Sie auf Ihrem SUSE LINUX School Server erstellt haben.

Serverbasierte Profile mit Windows-Clients

Während Linux-Clients einfach das betreffende Homeverzeichnis eines Nutzers mounten und in diesem Homeverzeichnis alle benutzerrelevanten Daten ablegen (welche somit netzwerkweit zur Verfügung gestellt werden können), ist bei Windows-Clients – je nach Version – ein wenig mehr Arbeit vonnöten, um denselben Kompfort zu genießen.

Wir wollen Ihnen in diesem Kapitel einen Einblick in die Konfiguration von serverbasierten Profilen für Windows-Clients geben. Profile beinhalten hierbei alle für den Benutzer relevanten Einstellungen einer Windowsumgebung.

Bitte beachten Sie, dass wie immer 1000 Wege zum Ziel führen und dies kein Windows-Handbuch sein soll. Erwarten Sie hier also bitte keinen Königsweg zur Administration von windowsbasierten Rechnern.

Sollten Sie einmal bei der Konfiguration nicht weiterkommen, so wenden Sie sich bitte vertrauensvoll an Ihren Windows-Händler.

Eine Kombination verschiedener Versionen von Windows-Clients im selben Netzwerk ist im übrigen nur sehr schwer zu administrieren. Wir gehen bei unseren Beschreibungen davon aus, dass sie nur identische Versionen in Ihrem Netzwerk benutzen.

Serverbasierte Profile mit Microsoft Windows 9x/ ME

Die veralteten Windows-Versionen waren eigentlich nicht für den Einsatz im Netzwerk gedacht. Deshalb ist die Konfiguration hier ein wenig komplizierter als bei späteren Versionen.

Beachten Sie bitte, dass diese älteren Versionen über keine vernünftigen Schutzfunktionen verfügen, so dass wir beim Einsatz dieser Betriebssysteme dringend zu „Schutzkarten“ raten, welche die Rechner bei jedem Neustart in einen definierten Zustand zurückversetzen.

Voraussetzungen

Um überhaupt server-basierte Profile einsetzen zu können, müssen sich die Clients am SUSE LINUX School Server anmelden. Lesen Sie hierzu bitte das Kapitel 5 auf Seite 122.

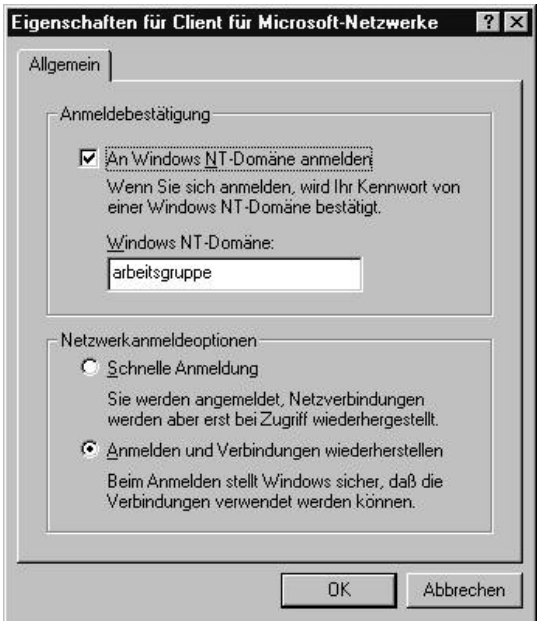


Abbildung 5.7: *Anmeldung am Server aktivieren*

Benutzerprofile aktivieren

Um unter Windows 9x/ ME mit Benutzerprofilen arbeiten zu können, müssen Sie diese zunächst aktivieren.

Unter Windows 95 wählen Sie dafür 'Start' → 'Einstellungen' → 'Systemsteuerung' → 'Kennwörter' und aktivieren Sie den Button 'Benutzerprofile'.

Jetzt haben Sie im oberen Bereich zwei Optionen zur Auswahl: Hier wählen Sie die Option „Benutzer können die Vorgaben und Desktop Einstellungen ..." (siehe Abbildung 5.8 auf der nächsten Seite). Danach schliessen Sie das Menu und starten den Rechner neu.

Unter Windows 98 und Windows ME wählen Sie stattdessen 'Start' → 'Einstellungen' → 'Systemsteuerung' → 'Benutzer'. Hier sollte Sie ein Assistent durch die einzelnen Punkte führen. Auch hier sollten Sie anschließend den Rechner neu starten.

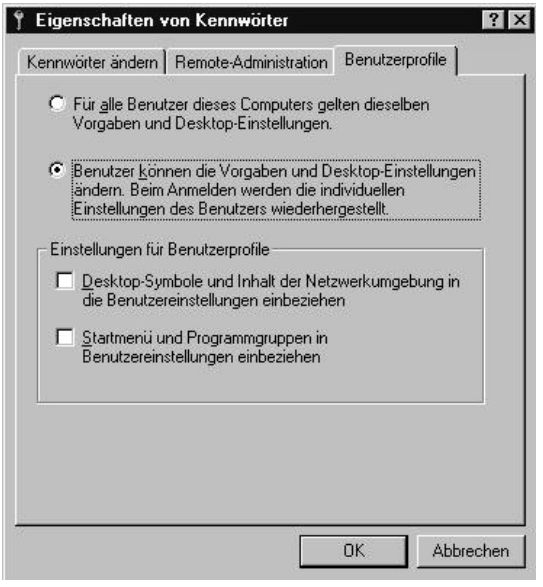


Abbildung 5.8: *Benutzerprofile aktivieren*

Verbindliche Profile

Nachdem Sie die Benutzerprofile aktiviert haben, speichert Windows die benutzerspezifischen Einstellungen in der Datei „user.dat“ im Profilverzeichnis des Benutzers ab. (Die Systemspezifischen Daten werden in der Datei „system.dat“ und – unter Windows ME – der Datei „classes.dat“ gespeichert.)

Hinweis

Sie könnten nun jedem Benutzer ein „mandatory profile“, ein verbindliches Profil, zuweisen, indem Sie die Datei `user.dat` in `user.man` umbenennen.

Hinweis

Damit wird das Profil des Benutzers beim Abmelden vor dem Überschreiben geschützt, es wird also für den Benutzer verbindlich (mandatory). Beim nächsten Anmelden wird wieder das gleiche Profil geladen wie zuvor.

Sie müssen also nur noch einen Musterbenutzer einrichten, der alle benötigten Einstellungen erhält, dieses Profil danach an alle anderen Benutzer verteilen und durch die Umbenennung in `user.man` zu einem verbindlichen Profil machen.

Dies sollte bei kleineren Netzwerken schon ausreichen. Wenn Sie allerdings Wert auf erhöhten Kompfort legen oder eine größere Nutzer- und Computerzahl mit unterschiedlichen Rechten und installierten Programmen zu pflegen haben, sollten Sie mit System- und Grouppolicies arbeiten.

Das Programm Poledit

Fast alle wichtigen Informationen des Windows-Betriebssystems werden in der Registry gespeichert. Die Registry ist der zentrale Ort zum Hinterlegen und Abfragen von Einstellungen eines Windows-Rechners und seiner Komponenten.

Hinweis

Als Administrator müssen Sie direkt in der Registry arbeiten. Sie sollten nur beachten, dass es für das System gefährlich sein kann, wenn Sie falsche Werte eintragen oder richtige löschen oder verändern.

Hinweis

Das Programm Poledit bietet die komfortable Möglichkeit, einen Teil der Registry zu editieren, Poledit kann aber noch viel mehr: Teile der Registry können in serverbasierten Netzen auf dem Server in das Verzeichnis `Netlogon` ausgelagert und erst bei der Anmeldung eines Nutzers von dort auf den lokalen Rechner heruntergeladen werden. Damit läßt sich z. B. erreichen, dass der Administrator an einem Windows-Arbeitsplatz alles darf, der normale Benutzer (ohne böswillige Tricks) aber nicht. Weiterhin können so die Daten der Nutzer auf dem Server gespeichert und müssen nicht lokal vorgehalten werden.

Sie finden den Systemrichtlinieneditor `Poledit.exe` entweder auf Ihren Windows-CDs (bei Windows 95 z. B. im Verzeichnis `admin/apptool/poledit` oder bei Windows 98 im Verzeichnis `\tools\reskit\netadmin\poledit`) oder Sie laden sich die jeweils aktuellste Version für Ihr Betriebssystem aus dem Internet herunter.

Tipp

Eine speziell an die Bedürfnisse von Schulen angepasste Vorlagendatei für Poledit finden Sie unter `ftp://ftp.suse.com/pub/people/lrupp/schoolserver/win/` mit dem Namen des jeweiligen Betriebssystems.

Tipp

Eine gute Anlaufstelle sind hier die WWW-Seiten des Heise–Verlags, welcher in seiner „c't Tipp-Datenbank“ auch einige zusätzliche Vorlagendateien für die entsprechende Windows-Version bereithält: `http://www.heise.de/ct/tipps/adms.shtml`

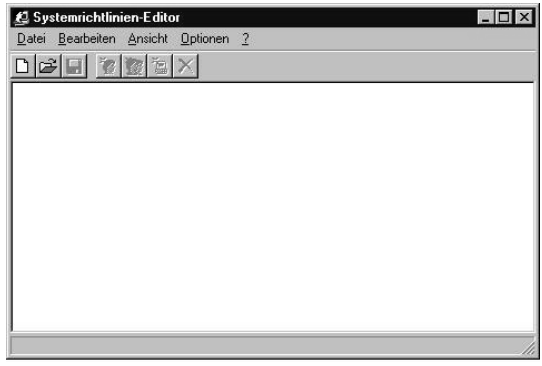


Abbildung 5.9: *Das Programm Poledit*

Achtung

Das Programm Poledit.exe sollte aufgrund seiner Möglichkeiten nur dem Systemverwalter zur Verfügung stehen!

Achtung

Es bietet sich es sich an, das Programm (inkl. aller Dateien im Ordner) im Homeverzeichnis des Admins zu installieren – dazu braucht das entsprechende Verzeichnis (im Allgemeinen `C:\\Programme\Ork\Poledit`) mit dem Programm nach der eigentlichen Installation nur dorthin kopiert werden.

Mit dem Programm Poledit.exe kann man auf drei Ebenen arbeiten:

lokale Registrierungsdatei bearbeiten ‘Datei’ → ‘Registrierung öffnen’ – Hier arbeiten Sie direkt an der Registry des lokalen Rechners.

Richtliniendatei erstellen/ändern ‘Datei’ → ‘Neu’ oder ‘Datei’ → ‘Öffnen’ – Mit diesem Punkt befassen wir uns in den nachfolgenden Abschnitten.

Remote-Zugriff Falls am betreffenden Client der Remote-Zugriff erlaubt wurde, kann man von einem beliebigen Rechner aus die Registry eines Clients bearbeiten.

Der erste Start

Starten Sie Poledit (falls Sie nach einer Vorlagendatei gefragt werden, dann geben Sie entweder die vorgeschlagene Datei `admin.adm` oder verwenden Sie eine heruntergeladene Vorlagendatei.).

Noch ist das Fenster leer. Wählen Sie nun 'Datei' → 'Neu': jetzt befinden sich zwei neue Icons auf der Oberfläche.

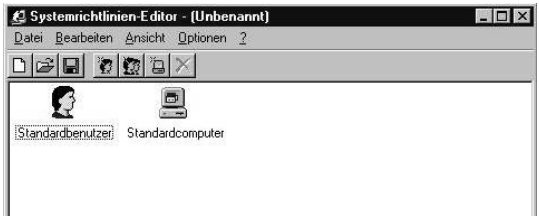


Abbildung 5.10: *Poledit – neue Richtliniendatei erstellen*

Ein Icon steht für den Standardbenutzer, das andere für den Standardcomputer. Als Standardbenutzer wird jeder Benutzer betrachtet, für den es hier kein eigenes Icon gibt.

Systemrichtlinien für den Administrator

Fügen Sie sofort einen Benutzer `admin` über den Menüpunkt 'Bearbeiten' → 'Benutzer hinzufügen' hinzu.

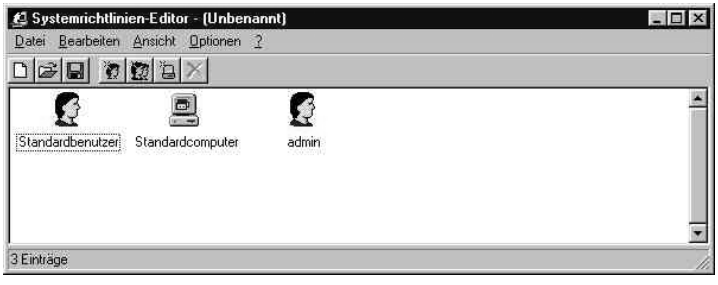


Abbildung 5.11: *Poledit – neuen Benutzer erstellen*

Geben Sie diesem Benutzer alle Rechte im System, indem Sie auf sein Icon doppelklicken und im neuen Fenster alle Kästchen demarkieren.

Zur Erläuterung:

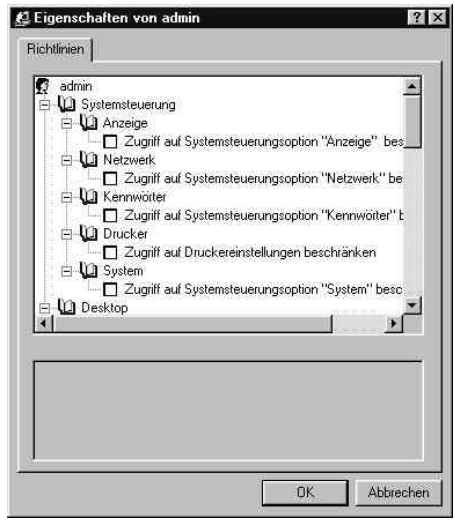


Abbildung 5.12: *Poledit – Administratorrechte zuweisen*

- Bei einem weißen Kästchen wird die betreffende Funktion nicht aktiviert.
- Bei einem Kästchen mit Haken wird die Funktion bzw. Beschränkung aktiviert.
- Bei einem grau hinterlegten Kästchen bleibt die lokale Einstellung erhalten. Diese Einstellung empfehlen wir nicht, da dann ein normaler Nutzer erweiterte Rechte bekommen könnte, wenn sich vor ihm ein Nutzer mit mehr Rechten am Computer angemeldet hatte.

Speichern Sie abschließend Ihre Einstellungen mit einem Klick auf (OK).

Wenn Sie weitere Nutzer in Poledit anlegen, bekommen diese zunächst alle Einstellungen des Standardnutzers zugewiesen. Wenn Sie einen weiteren Administrator–Nutzer einrichten wollen, kopieren Sie einfach dessen Profil, indem Sie sein Icon anklicken und im Menü 'Bearbeiten' → 'Kopieren' wählen. Jetzt brauchen Sie nur noch den neuen Nutzer zu markieren und Ihm über 'Bearbeiten' → 'Einfügen' die neuen Rechte zuweisen.

Systemrichtlinien für den Standardbenutzer

Für den Standardbenutzer sollten Sie sinnvolle Einschränkungen vornehmen.

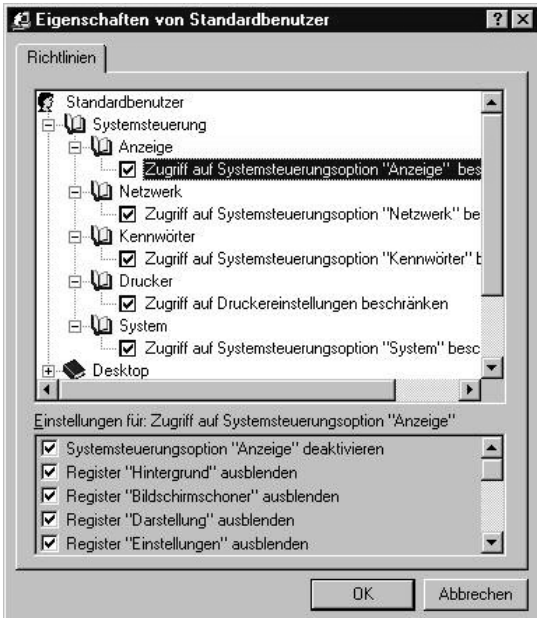


Abbildung 5.13: *Poledit – Benutzerrechte zuweisen*

Was dabei genau eingeschränkt werden soll ist sicherlich Geschmackssache, deshalb hier nur ein paar Vorschläge, die Sie Ihren Gegenheiten anpassen können:

Systemsteuerung Hier sollten alle Beschränkungen aktiviert sein.

Desktop Wird z. B. als Hintergundbild „none“ vorgegeben wird kein Hintergrundbild geladen, da diese Datei nicht existiert. Sollte sich ein Benutzer über die Option ‘als Hintergrund speichern’ in einem Programm ein Hintergrundbild erzeugen, so wird dieses beim nächsten Anmelden nicht mehr angezeigt.

Netzwerk Hier wird wieder alles beschränkt.

Shell Im Bereich ‘Benutzerdefinierte Ordner’ sollten Sie einige Anpassungen vornehmen, auf die wir weiter unten genauer eingehen.

Zugriffsbeschränkungen Hier sollten Sie vor allem alle Programme zum Bearbeiten der Registry verbieten (Haken setzen). Auch über den Zugang zur Eingabeaufforderung von MS-DOS können die Sicherungsmaßnahmen umgangen werden. Beachten Sie hier jedoch, dass einige Programme, welche noch unter MS-DOS geschrieben wurden, dann auch nicht mehr laufen.

Um die Daten der Nutzer auf dem Server zu speichern, sollten Sie im Menüpunkt 'Shell' → 'Benutzerdefinierte Ordner' Anpassungen vornehmen.

Achtung

Legen Sie die entsprechenden Unterverzeichnisse an, bevor Sie sie in Poledit angeben! Ansonsten kann der Rechner u.U. abstürzen!

Achtung

So können Sie das Startmenü und die Desktop-Symbole z. B. auf einem Serverlaufwerk ablegen, welches nur von Lehrern beschreibbar ist. Dann können Schüler nichts mehr verändern und der Desktop und das Startmenü sieht überall gleich aus.

Oder legen Sie die Pfade für diese Ordner ins Homeverzeichnis, so kann sich jeder Benutzer seine eigene Arbeitsumgebung so einrichten, wie es Ihm gefällt – was sich oftmals als sehr motivierend für die SchülerInnen herausgestellt hat.

Die Pfade für den Ordner `Eigene Dateien` sollten Sie auf das Homeverzeichnis der Nutzer zeigen lassen. Günstig wäre hier die Angabe des kompletten Pfades (`\\<server>\<homes>\profile\Eigene Dateien`) – allerdings wird dies nicht von allen Programmen akzeptiert, so dass Sie im Allgemeinen ein Unterverzeichnis im Laufwerk `H:` verwenden sollten.

Beim Anmelden werden vom Server weitere Laufwerke für serverbasierte Software (`S:`), Gruppenverzeichnisse (`M:`) und zum Austausch untereinander (`P:`) angelegt.

Sie können die Speicherorte der benutzerdefinierten Ordner also fast beliebig festlegen. Achten Sie aber darauf, dass die entsprechenden Ordner wirklich existieren und u.U. auch die entsprechenden Daten schon beinhalten müssen!

Systemrichtlinien für den Standardcomputer

Hier können einen speziellen Computer hinzufügen und ihn damit zu einem speziellen Lehrerarbeitsplatz machen. Als Grundlage für die Zuordnung dient der jeweilige NetBIOS-Name des Rechners.

So können Sie hier z. B. die Rechner eines anderen, kleineren Kabinetts angeben und diesen etwas andere Einstellungen verpassen als dem Rest.

Sollten Sie mehrere Computerkabinette verwenden, so hat sich eine etwas andere Vorgehensweise bewährt, weil sie es ermöglicht, die Kabinette später problemlos in die Obhut anderer Administratoren zu geben.

Nutzen Sie dazu einfach unterschiedlich benannte Policy-Dateien für die verschiedenen Kabinette und geben Sie diese einmalig gezielt bei jedem Rechner an.

Dann brauchen Sie sich fortan als Administrator eines Raumes immer nur um den `Standardcomputer` kümmern.

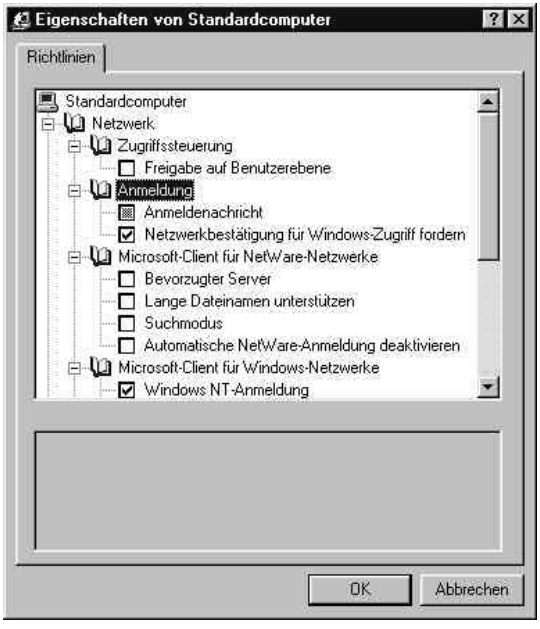


Abbildung 5.14: *Poledit – Standardcomputer einrichten*

Hier wieder einige Beispielangaben:

Zugriffssteuerung Wenn diese komplett deaktiviert wird, sind überhaupt keine Freigaben mehr möglich. Dies sollte insbesondere für Klausurumgebungen gemacht werden.

Anmeldung Wenn Sie den Nutzern direkt nach der Anmeldung eine Nachricht zukommen lassen möchten, setzen Sie einen Haken vor 'Anmeldenachricht' und geben Sie im unteren Fenster die betreffende Nachricht ein.

Netzwerkbestätigung für Windows-Zugriff fordern Hierdurch werden nur Nutzer zugelassen, die sich auch am Server angemeldet haben - ein Drücken auf 'Abbrechen' bei der Anmeldung ist dann nicht mehr möglich. Dies gilt auch dann, wenn der Client keine Netzwerkverbindung zum Server aufbauen kann.

Sollten Sie den Client später einmal wieder als Einzelplatz-PC nutzen wollen, müssen Sie Ihm also zuerst eine lokale Policy-Datei (z. B. config.pol) erstellen und zuweisen.

Achtung

Wichtig ist der Eintrag `Remote-Update` im Abschnitt 'Netzwerk': nur wenn hier der Haken gesetzt ist, wird die Policy-Datei vom Server überhaupt ausgewertet!

Achtung

Im unteren Teil können Sie entweder die Default-Einstellungen so belassen, oder – wenn Sie mehrere Policy-Dateien verwenden wollen – hier entsprechende Anpassungen vornehmen.

Geben Sie als Pfadangabe im Menüpunkt 'Pfad für interaktives Update:' am besten die IP-Nummer des Servers und den Pfad `netlogon` zusammen mit dem vollständigen Dateinamen an. Beachten Sie dabei die Groß- und Kleinschreibung. Ein Beispiel könnte so aussehen:

```
\\192.168.0.2\netlogon\raum1.pol
```

Nachdem Sie das Fenster mit (OK) verlassen haben, können Sie die zukünftige Policy-Datei speichern und in das Verzeichis

```
/var/lib/samba/netlogon
```

auf dem Server verschieben. Achten Sie darauf, dass Sie mit

```
chmod 644/var/lib/samba/netlogon/raum1.pol
```

(um in unserem Beispiel zu bleiben) die richtigen Rechte für die Datei setzen.

Systemrichtlinien aktivieren

Nachdem Sie nun die Vorarbeiten abgeschlossen und die Policy-Datei auf dem Server gespeichert haben, müssen Sie noch den Clients mitteilen, dass diese zukünftig alle Vorgaben vom Server beziehen sollen.

Dazu sollten Sie auf den Clients die folgende Datei (welche Sie auf unserem FTP-Server im Verzeichnis `ftp://ftp.suse.com/pub/people/lrupp/schoolserver/win/<version>` unter dem Namen `remote_update_aktivieren.reg` finden) ausführen und damit in die Registry eintragen.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Update]
"NetworkPath"=""
"UpdateMode"=dword:00000001
"Verbose"=dword:00000001
"LoadBalance"=dword:00000001
```

Datei 6: *Die Datei remote_update_aktivieren.reg*

Sollten Sie einen anderen Dateinamen als den Standardwert (für Windows9x: `config.pol`; für WindowsNT, 2000 und XP: `ntconfig.pol`) vergeben haben, so setzen Sie den korrekten Pfad zur Datei hinter `NetworkPath`.

Serverbasierte Profile mit Microsoft Windows 2000 und XP

Im Gegensatz zu Windows 9x und ME wurde bei Windows 2000 und Windows XP (jeweils in der Professional-Version) wie schon bei Windows NT auf die Mehrbenutzerfähigkeit geachtet.

Hinweis

Microsoft Windows XP in der Home Edition eignet sich nicht für den Netzwerkbetrieb. Eine Aufnahme der Arbeitsstation in die Domäne ist leider nicht möglich.

Sie können zwar über das Tool `TweakUI`, das Sie sich aus dem Internet herunterladen können, einen Standardbenutzer für den Domänenbetrieb vorgeben – eine richtige Nutzung im Mehrbenutzerbetrieb ist jedoch nicht möglich.

Hinweis

Grundlagen zum Einsatz von Profilen

Unter Windows 2000 und Windows XP verfügt jeder Nutzer über ein eigenes Profil. Dort werden alle Daten und Einstellungen gespeichert, die nur diesen Nutzer betreffen. Der Standardspeicherort für diese Profile ist auf einer Workstation `C:\DokumenteundEinstellungen\<Benutzername>`.

Einzelplatzbetrieb

Existiert ein Benutzer auf einem Client noch nicht, und ist dieser Client noch nicht in eine Domäne integriert, so wird beim ersten erfolgreichen Einloggen des Nutzers ein Profil erstellt.

Dafür wird das „Default User"–Profile aus dem gleichnamigen Ordner als Vorlage genommen. Anschließend werden noch die Zugriffsberechtigungen für das neu erstellte Profil geändert.

Hinweis

Unterschiedliche Zugriffsrechte machen ein einfaches Kopieren von Profilen für andere Benutzer unmöglich. Dies muss über 'Arbeitsplatz' → 'Eigenschaften' → 'Benutzerprofile' geschehen.

Hinweis

Es gibt jedoch noch ein Profil mit dem Namen `All Users`. Unter diesem Profil sind die allgemeinen Einstellungen gespeichert, welche für alle Nutzer gelten. Installiert der Administrator ein Programm, welches allen Nutzern auf dieser Workstation zur Verfügung stehen soll, so werden dort die entsprechenden Verknüpfungen angelegt.

Hinweis

Die Arbeitsumgebung ist also immer eine Mischung aus dem eigentlichen Nutzerprofil und dem Profil für alle Benutzer.

Hinweis

Netzwerkbetrieb

Ist der Client in eine Domäne integriert, so verläuft der Anmeldeprozess ohne besondere Eingriffe des Administrators bei einem neuen Benutzer ein wenig anders als bei einem Einzelplatzsystem:

- Zunächst überprüft der Client, ob im Share `netlogon` (auf dem Server unter `/var/lib/samba/netlogon` zu finden) ein Verzeichnis `Default User` existiert, welches er als Vorlage verwenden kann.

- Existiert ein solches Verzeichnis, legt der Client das persönliche Benutzerverzeichnis lokal an und kopiert dorthin das `DefaultUser`–Profil aus dem Netz.
- Gibt es auf dem Server kein entsprechendes Verzeichnis, dient das lokale `Default User`–Profil als Vorlage.

Nach dem Abmelden wird das lokale Benutzerprofil auf den Server kopiert.

Meldet sich der Benutzer nun erneut am Client an, wird das noch lokal vorhandene Profil mit dem auf dem Server vorhandenen abgeglichen und ggfs. werden alte Dateien durch neuere ersetzt.

Achtung

Die Uhrzeiten aller Rechner im Netz müssen synchron laufen, um dem Benutzer auch wirklich immer das aktuellste Profil zur Verfügung zu stellen.

Achtung

Policy- oder Gruppenrichtlinien?

Microsoft stellt dem Administrator zwei grundlegend verschiedene Mechanismen zur Administration von Clients im Netzwerk zur Verfügung:

Policyeditor Mittels Poledit werden weiterhin nutzerabhängige Rechte im Netzwerk vergeben. Dies kann bei vielen verschiedenen Profilen und unterschiedlichen Computern einen hohen Aufwand bedeuten.

Gruppenrichtlinien Über Gruppenrichtlinien wird ein einzelner Computer im Netzwerk konfiguriert. Die hier gemachten Einstellungen gelten deshalb grundsätzlich für *alle* Benutzer dieses Computers. Auch der Administrator selbst kann hier – durch falsche Einstellungen – an der weiteren Administration eines Rechners gehindert werden.

Hinweis

Sie sollten sich bei der Administration Ihrer Clients für eines der beiden Systeme entscheiden. Ein Mischbetrieb ist zwar möglich, kann u.U. die Administration der Gesamtanlage aber erschweren.

Hinweis

Während der Gruppenrichtlinieneditor bei jeder Windowsversion ab Windows 2000 standardmäßig installiert ist und mit dem Befehl `gpedit.msc` auf einer

Kommandozeile (oder über 'Start' → 'Ausführen' → 'gpedit.msc') gestartet werden kann, muß das Programm Poledit erst noch nachinstalliert werden.

Wir würden Ihnen trotzdem zur Nutzung von Poledit raten, da sich damit sämtliche Computer bequem aus der Ferne warten lassen, für jeden Benutzer bei Bedarf eigene Richtlinien definieren lassen und schließlich auch mehrere Vorlagendateien gleichzeitig geladen und somit miteinander kombiniert werden können.

Die Installation und Bedienung von Poledit finden Sie im Abschnitt 5 auf Seite 133.

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 SUSE LINUX 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 SUSE LINUX School Servers wird für diese Zwecke zusätzlich 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 fertig für die Nutzung im Schulalltag. Der Installationsaufwand hält sich also stark in Grenzen. Einen Überblick über die automatisch gemachten Änderungen im Gegensatz zu einer normalen SuSE Linux Installation finden sie unter *Vorbereitungen zur Installation* auf Seite 147.

Vorbereitungen zur Installation

Das Rootverzeichnis des TFTP-Servers ist `/srv/tftpboot`. In diesem Verzeichnis 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/loader/linux /srv/tftpboot`

`initrd` Das zu startende Filesystem. Es muss von der aktuellen SuSE Linux-DVD kopiert werden:
`cp /media/dvd/boot/loader/initrd /srv/tftpboot`

`menu.lst` Diese Datei beinhaltet das Bootmenü.

`pxegrub` PXE-Bootimage für den Bootloader Grub.

`pxes` In diesem Verzeichnis befinden sich spezielle Kernel– und Filesystem–Images zum Starten von Linux X-Terminals.

Weiterhin müssen die CDs oder die DVDs der aktuellen SuSE Linux Distribution mit folgenden Befehlen in das Verzeichnis `/var/SuSE/akt/` kopiert werden (wir gehen hier wieder von der DVD aus):

```
mount /media/dvd
cd /media/dvd
cp -va . /var/SuSE/akt
umount /media/dvd
```

Diese Befehle müssen ggf. für alle CDs oder DVDs wiederholt werden.

Tipp

DVD direkt verwenden

Alternativ können Sie die DVD der aktuellen SuSE Linux Distribution in das Verzeichnis `/var/SuSE/akt/` mounten (`mount /dev/dvd/ /var/SuSE/akt/`). Entfernen Sie in diesem Fall bitte das Kommentarzeichen „#“ in der Datei `/etc/exports` vor dem Eintrag `/var/SuSE/akt/` und aktualisieren Sie den NFS-Server mit dem Befehl `rcnfsserver reload`. Aus Performance-Gründen ist dieses Verfahren jedoch nur für Testzwecke empfohlen.

Tipp

Startet man einen Rechner mit PXE-Netzwerkboot-Karte oder über die Netzwerk-BootCD (siehe Abschnitt *Installation über das Netzwerk* auf Seite 155, erhält man ein Bootmenü mit folgenden Optionen:

Linux X-Terminal Ein Diskless Linux X-Terminal wird gestartet. Als X-Server wird der `terminalserver` benutzt.

SuSE Workstation automatische Installation Die automatische Installation einer SuSE Linux Workstation wird gestartet.

SuSE Workstation automatische Installation mit Windows-Partitionen Die automatische Installation einer SuSE Linux Workstation mit zusätzlichen Windows-Partitionen wird gestartet.

SuSE Professional Workstation manuelle Installation Die manuelle Installation einer SuSE Linux Workstation wird gestartet.

SuSE ThinClient automatische Installation Die automatische Installation eines SuSE Linux ThinClients wird gestartet.

SuSE Terminalserver automatische Installation Die manuelle Installation eines SuSE Linux Terminalservers wird gestartet.

Die Konfigurationsdateien der Autoinstallation befinden sich im Verzeichnis `/var/SuSE` und heißen `std+win.xml`, `std.xml`, `thin_client.xml` und `terminalserver.xml`. Sie können diese Dateien bei Bedarf mit einem XML-Editor wie z. B. dem kxmleditor von KDE (siehe Abbildung 6.1 auf der nächsten Seite) oder mit dem YaST2-Modul `autoyast` auf einem aktuellen Client bearbeiten. Weitere Informationen zu AutoYaST2 finden Sie auf der Installations-CD vom SUSE LINUX School Server im Verzeichnis `docu` bzw unter `/usr/share/doc/packages/autoyast2/html/`.

Für die automatische Installation sind schon die folgenden Konfigurationsdateien angelegt worden, die die meisten Szenarien an Schulen abdecken sollten.

Achtung

Beachten Sie bitte, dass bei *allen* automatischen Installationen die bisherigen Daten und Partitionen auf den Festplatten der Clients gelöscht werden!

Achtung

Die Konfiguration der über die Autoinstallation eingerichteten Clients unterscheidet sich von einer normalen Installation in folgenden Punkten:

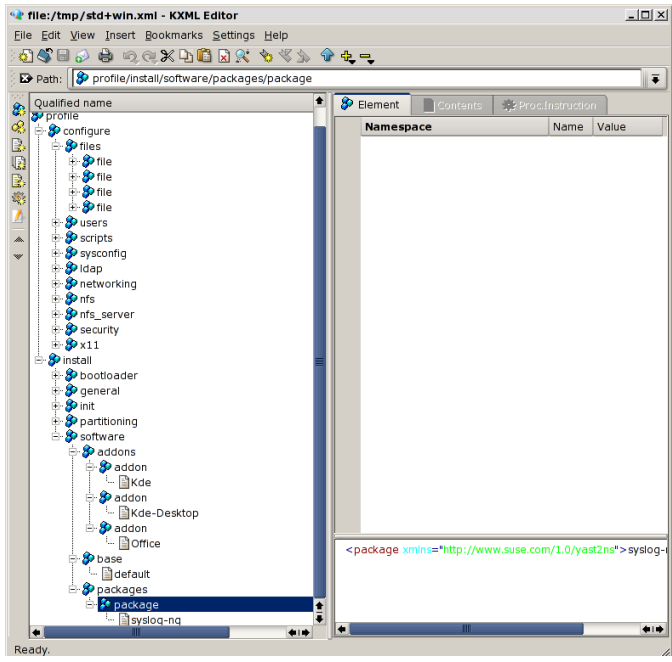


Abbildung 6.1: *XML-Datei mit dem kxmleditor bearbeiten*

- Für den Benutzer `root` wird auf allen Systemen das bei der Installation des SUSE LINUX 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 SUSE LINUX 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 SUSE LINUX 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.

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 SUSE LINUX 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.

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 SUSE LINUX 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

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 SUSE LINUX School Server registrieren, wie unter 4 auf Seite 91 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 4 auf Seite 98 beschrieben, die neue (während der Registrierung erhaltene) IP-Adresse unter dem Menüpunkt 'DNS: Host anlegen' eintragen. [1]

NFS-Client Das Verzeichnis `nfs:/home` vom SUSE LINUX 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.

[1] Der neue Eintrag wird nicht sofort in die Konfigurationsdateien übernommen. Um die Konfigurationsdateien zu schreiben, wählen Sie 'Virt. Domaenen' → 'Exportieren'.

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

Installation über das Netzwerk

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.

Wenn Sie einen SuSE Linux Client über den SUSE LINUX School Server installieren oder bei älterer Hardware erst ausprobieren möchten, ob sie sich für eine Installation als Thin-Client oder Diskless-Client eignet, können Sie sich eine bootfähige CD erstellen, die nach dem Bootvorgang automatisch eine Verbindung zum Server aufbaut und Ihnen das Auswahlmenü anbietet. Das ISO-Image finden Sie unter der URL `http://admin/bootcd.iso`.

Linux X-Terminal

Wenn Sie die erstellte Boot-CD in einen Client einlegen und den ersten Eintrag 'Linux X-Terminal' anwählen, wird, nachdem der Kernel geladen und die Netzwerkkarte konfiguriert wurde, eine Verbindung zu einem vorher installiertem

Terminalserver aufgebaut und von dort aus ein X-Bildschirm 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 nutzlos.

Groupware

Der SUSE LINUX School Server besitzt neben der administrativen Oberfläche auch eine Groupware Komponente. Diese beinhaltet alle Komponenten, die zu einer erfolgreichen Gruppenarbeit nötig sind, wie z.B. Mail und Kalender, und bietet Zugriff auf das zentrale Addressbuch sowie Schüler- und Lehrerforen. Im folgenden Kapitel erfahren Sie, wie Sie die Groupware des SUSE LINUX School Server effektiv nutzen können.

Übersicht über die Groupware Oberfläche

Die Groupware erreichen Sie von der SUSE LINUX School Server Arbeitsoberfläche über das 'Web-Mail, Groupware, Forum' Icon oder innerhalb des Schulnetzes über einen beliebigen Browser, indem Sie in der Adresszeile die URL `https://Schulserver` eingeben (wobei https für eine verschlüsselte Verbindung steht).

Tipp

Externer Login

Ausserhalb des Schulnetzes können Sie die Groupware Oberfläche ggf. über eine verschlüsselte Verbindung (Port 443) erreichen, d.h. wenn Ihre Schule unter www.schule.de registriert ist und der Administrator die Groupware für einen Zugriff von ausserhalb freigeschaltet hat, müssen Sie die folgende Adresse in Ihrem Browser eingeben: `https://www.schule.de`

Tipp

Nachdem Sie sich mit Ihren Benutzerdaten am SUSE LINUX School Server angemeldet haben, erscheint die Groupware Oberfläche (siehe 7.1 auf der nächsten Seite) mit Ihrem persönlichen Kalender.
Die Groupware Oberfläche enthält für Schüler die folgenden Menüpunkte:

- Home
- E-Mail
- Kalender
- Adressbuch
- Forum

Die entsprechenden Funktionen können Sie durch einen Klick auf das jeweilige Icon erreichen. Für Lehrkräfte steht zudem noch ein 'Lehrerforum' und ein Menü zur 'Administration' bereit.

Der Kalender

Ansichtsmodi

Der Kalender zeigt in der Grundeinstellung den aktuellen Monat (gross, in der Mitte), den vergangenen, sowie den kommenden Monat an (links und rechts

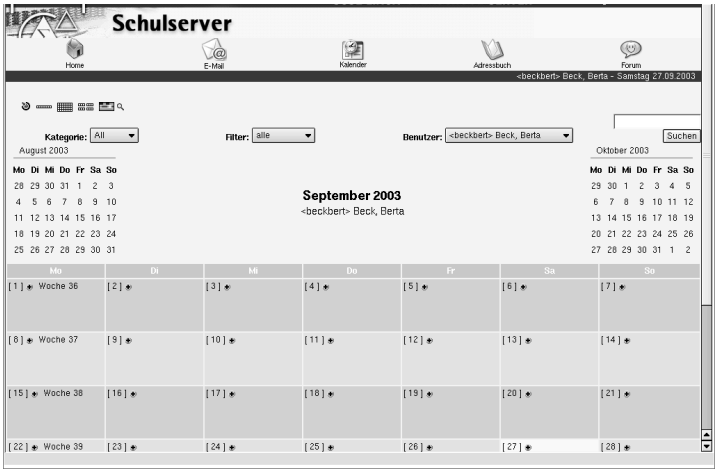


Abbildung 7.1: *Die Kalenderansicht der Benutzeroberfläche des SUSE LINUX School Server*

klein). Darüber befindet sich ein Button für die Suchfunktion sowie drei Pull-Down Menüs mit folgenden Funktionen:

Kategorie: Mit diesem Pull-Down Menü können Sie die auf dem Kalender sichtbaren Ereignisse und Termine in bestimmte Kategorien einordnen. In der Grundeinstellung sind noch keine Kategorien vorhanden, deshalb ist im Menü nur der Eintrag 'All' vorhanden. Wenn Sie eine bestimmte Kategorie auswählen, zeigt der Kalender nur die Termine an, die zur jeweiligen Kategorie gehören. Wie Sie Kategorien anlegen und bearbeiten können, lesen Sie im Abschnitt 7 auf Seite 163.

Filter: Termine und Ereignisse können privat oder öffentlich sein. Hier können Sie einstellen, ob Sie alle Termine/Ereignisse oder nur private sehen möchten.

Benutzer: Hier können Sie auswählen, ob Sie nur Ihren eigenen Kalender, oder denjenigen der Klasse, respektive der übrigen Schüler oder Lehrkräfte sehen möchten. Sofern nicht als privat deklariert, gelten Termine von Schülern für die ganze Klasse und Termine von Lehrkräften für die gesammte Lehrerschaft, das heisst Lehrkräfte haben Lesezugriff auf die Kalender der übrigen Lehrkräfte, sowie auf den Kalender der eigenen Klasse. Die Schüler wiederum haben Lesezugriff auf die Kalender aller Mitschüler und Mitschülerinnen. Diese Einstellungen können unter 'Einstellungen' →

'Kalender' 'Zugriff gewähren' geändert werden. Für Termine und Ereignisse, über die andere nichts wissen sollten ist es in jedem Fall angeraten die 'Privat' Checkbox anzuwählen.

Achtung

Damit ein Benutzer überhaupt in der Liste erscheint, muss er sich schon einmal auf der Web-Benutzeroberfläche eingeloggt haben. Erst dann werden nämlich die benötigten Datenbankeinträge generiert.

Achtung

Die Ansicht des Kalenders (Tag, Monat usw.) können Sie mit Hilfe der sechs kleinen Symbole in der linken oberen Ecke wechseln. Die folgenden Ansichten stehen zur Verfügung (von links nach rechts):

- Heute → Zeigt nur den aktuellen Tag an. Nützlich, sollten an einem Tag mehrere Termine anstehen und um einen neuen Termin gleich zum richtigen Zeitpunkt anzulegen.
- Diese Woche → Zeigt die aktuelle, oder eine ausgewählte Woche an. Nebst der Woche werden auch die drei Monate vor, während und nach der Woche dargestellt.
- Dieser Monat → Die Grundansicht des Kalenders.
- Dieses Jahr → Alle zwölf Monate im Überblick.
- Planer → Hier können Sie mehrere Wochen auf einer Zeitachse nacheinander überblicken. Wenn Sie unter 'Benutzer:' zum Beispiel den Eintrag 'Schüler,users' auswählen, können Sie die Termine der einzelnen Schüler auf Konflikte hin überprüfen.
- Matrix-Ansicht des Tages → Die unter 'Planer' beschriebene Ansicht lässt sich auch für einen bestimmten Tag einstellen. Dazu wählen Sie einfach dieses Symbol an.

Sollte es an Ihrer Schule bald so viele Ereignisse und Treffen geben, dass Sie trotz verschiedener Ansichtsmodi kaum mehr den Überblick behalten können, kann Ihnen die in der rechten oberen Ecke des Kalenders befindliche Suchfunktion weiterhelfen. Geben Sie einfach das gesuchte Stichwort im Eingabefeld an und drücken Sie anschliessend auf den 'Suchen' Button.

Kalendereinträge anlegen und verwalten

Kalendereinträge können Sie grundsätzlich nur in Ihrem eigenen Kalender anlegen, es sei denn jemand hat Ihnen explizit Schreibzugriff auf seinen Kalender ermöglicht. Bevor Sie also versuchen ein neues Treffen zu vereinbaren, wählen Sie unter 'Benutzer' lieber Ihren eigenen Eintrag aus.

Das Erstellen von neuen Einträgen erfolgt über eine einheitliche Maske. Um die Eingabemaske zu erreichen sind allerdings je nach Ansichtsmodus verschiedene Schritte notwendig. Bei der *Wochen-* und der voreingestellten *Monatsansicht* müssen Sie auf das kleine Plus-Zeichen neben dem Kalendertag klicken, um die Eingabemaske für einen neuen Termin zu erreichen. Bei diesem Vorgehen wird dem Ereignis kein genauer Zeitpunkt zugeordet, deshalb ist es in erster Linie für ganztägige Ereignise geeignet. Sie können aber auch hier nachträglich eine bestimmte Uhrzeit angeben.

Entscheiden Sie sich für die *Tagesansicht*, klicken Sie einfach auf einen entsprechenden Zeiteintrag am Ende des schraffierten Feldes. Es erscheint die Eingabemaske für den neuen Termin, wobei die von Ihnen angewählte Zeit als Start- und Enddatum eingetragen ist. Sollte sich daraufhin keine Eingabemaske öffnen, überprüfen Sie bitte, ob sich die Farbe des Zeiteintrages in Orange ändert, wenn Sie den Mauszeiger darüber halten. Wenn nicht, haben sie vermutlich kein Schreibzugriff auf den Kalender, und sie müssen aus dem 'Benutzer:' Pull-Down Menü einen anderen Benutzer auswählen.

Das Vorgehen bei der 'Monatsansicht' ist identisch, nur dass Sie hier zuerst den entsprechenden Tag auswählen müssen, um an die Tagesansicht zu gelangen.

Auch bei *Planer-* und bei *Matrix*ansicht können Sie neue Termine anlegen. Hier müssen Sie nur einmal auf den entsprechenden Tag (Planer), oder die entsprechende Uhrzeit klicken (Matrix), schon erscheint die benötigte Eingabemaske.

Die 'Kalendereintrag hinzufügen' Maske

Wenn Sie alles richtig gemacht haben, sollten Sie jetzt die auf der Abbildung 7.2 auf der nächsten Seite zu sehende 'Kalendereintrag hinzufügen' Maske sehen. Geben Sie hier zuerst den 'TITEL' des Ereignisses an, sowie eine 'vollständige Beschreibung' dazu. Unter 'Kategorie:' können Sie einen entsprechenden Themenkreis auswählen (lesen Sie mehr darüber im folgenden Abschnitt). 'Ort' ist im Normalfall ein Besprechungszimmer, kann aber natürlich auch eine genaue Adresse sein. Das 'Startdatum' wird beim Anlegen des Termines automatisch auf den ausgewählten Tag eingestell, das 'Enddatum' ebenfalls. Die 'Startzeit' und 'Endzeit' Einträge sind jenachdem, wie Sie den Termin angelegt haben leer (d.h. 00:00 Uhr) oder auf eine bestimmte Uhrzeit eingestellt.

Abbildung 7.2: *Die Kalenderansicht der Benutzeroberfläche des SUSE LINUX School Server*

Unter 'Privat' können Sie ankreuzen ob der Termin nur für Sie persönlich oder auch für andere lesbar sein soll. Auch wenn Sie sich für privat entscheiden, kann der Termin von anderen abgefragt werden, allerdings ist nur ersichtlich, dass Sie an diesem Tag einen privaten Termin haben. Dies kann verhindern, dass z.B. ein Kollege von Ihnen eine Besprechung an einem Tag plant, der von Ihnen privat schon besetzt ist.

Unter 'Teilnehmer' können Sie beliebige Personen zum Termin einladen, resp. sie darüber benachrichtigen. Sie haben die Auswahl zwischen einzelnen Schüler/Lehrer (u=users), sowie Gruppen und Klassen (g=group). Um mehrere Einträge hinzuzufügen, halten Sie die Strg Taste gedrückt, während Sie die einzelnen Einträge mit der Maus anklicken. Alle von Ihnen ausgewählten Teilnehmer erhalten eine E-Mail über den Termin und finden den Termineintrag in ihrem eigenen Kalender wieder. In der Grundeinstellung sind Sie automatisch zu jedem von Ihnen erstellten Termin eingeladen. Wenn Sie das nicht möchten (weil Sie z.B. im Sekretariat arbeiten und häufig Termine für die Schulleitung planen müssen), klicken Sie einmal auf die '<login> Name, Vorname nimmt Teil:' Checkbox, um die Auswahl zu entfernen.

Im unteren Teil der Eingabemaske können Sie 'Informationen zu sich wiederholenden Ereignissen' angeben. Das können z. B. fakultative Fächer, Elternstammtische oder Feiertage sein. Wählen Sie dazu erst unter 'Wiederholungstyp' die entsprechende Häufigkeit des Ereignisses aus, und geben Sie dann mit Hilfe der

Checkboxen an, bis wann die Wiederholung stattfinden soll ('Enddatum') und an welchen Tagen (falls wöchentlich).

Um den Termin anzulegen klicken Sie auf 'Absenden'. Um einen bereits angelegten Termin zu löschen wählen Sie 'Löschen', und wenn Sie den Termin doch nicht anlegen möchten, drücken Sie auf 'Abbruch'. Das System speichert nun den Eintrag in Ihrem (und den ausgewählten) Kalender(n), und der SUSE LINUX School Server sendet an alle Eingeladenen eine E-Mail (siehe dazu den Abschnitt 7 auf Seite 173).

Kategorien

Um bei einem überfüllten Kalender nicht die Übersicht zu verlieren ist es sinnvoll, die einzelnen Termine verschiedenen Kategorien zuzuordnen. Um eine neue Kategorie anzulegen wählen Sie ganz oben den Punkt 'Einstellungen' an (neben 'Abmelden'), dann 'Kalender' → 'Kategorien editieren'. Als Lehrkraft können sie wahlweise auch den Punkt 'Administration' → 'Globale Kategorien' anwählen.

Tipp

Da die angelegten Kategorien sowohl von allen Schülern als auch von allen Lehrkräften benutzt werden können, ist es sinnvoll, schon vor Inbetriebnahme des SUSE LINUX School Server einige für die Schule wichtige Kategorien anzulegen.

Tipp

Nachdem Sie den entsprechenden Punkt angewählt haben, klicken Sie bitte auf 'Hinzufügen' um eine neue Kategorie anzulegen. Sofern Sie bereits Kategorien angelegt haben, sehen Sie diese aufgelistet und können mit Hilfe des 'Untergeordnete hizufügen' Menüpunktes eine neue Unterkategorie anlegen. Wenn Sie bereits auf 'Hinzufügen' gedrückt haben, wählen Sie einfach die entsprechende Kategorie aus dem Pull-Down Menü 'Übergeordete Kategorie' aus (siehe Abbildung 7.4 auf der nächsten Seite). Geben Sie der Kategorie einen aussagekräftigen Namen und eine möchlichst konkrete Beschreibung, das erleichtert Ihnen später die Orientierung. Falls Sie nicht möchte, dass die Kategorie auch für andere sichtbar ist, wählen Sie die 'Privat' Checkbox an (bei neuen Terminen müssen Sie aber weiterhin die Privat checkbox anwählen, damit der Termin auch wirklich privat bleibt!).

Um die Kategorie anzulegen drücken Sie bitte auf den 'Speichern' Button. Es erscheint darauf eine Meldung *Kategorie XY wurde hinzugefügt !* Wenn Sie noch weitere Kategorien anlegen möchten, können Sie dies nun durch eine erneute Eingabe tun. Sind Sie fertig, drücken Sie auf den gleichnamigen Button (vorher

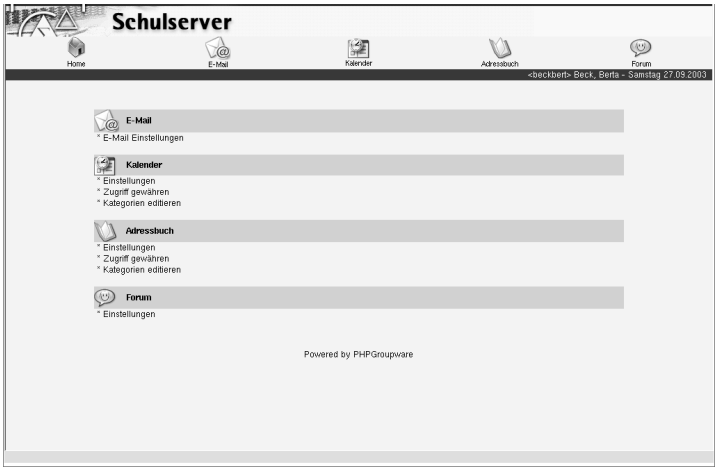


Abbildung 7.3: *Einstellungsmöglichkeiten für Schüler*

speichern nicht vergessen). Sie sehen nun eine Übersicht über die von Ihnen angelegten Kategorien, die Ihnen ab sofort im Kalender beim Anlegen neuer Termine zur Verfügung stehen.

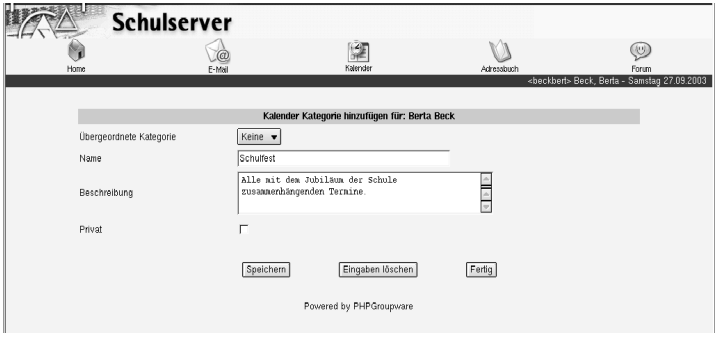


Abbildung 7.4: *Neue Kalender-Kategorie anlegen*

E-Mail

Übersicht über die Mail Komponente

Den Web-E-Mail Client des SUSE LINUX School Server erreichen Sie über das E-Mail Symbol. Bitte beachten Sie, dass das Programm aus (sicherheits-) technischen Gründen nur innerhalb des Schulnetzes erreichbar ist. Wenn Sie von zuhause aus an Ihre E-Mails gelangen möchten, können Sie dazu einen beliebigen Mail Client benutzen, wie z.B KMail, Evolution oder Outlook.

Der Mail Client des SUSE LINUX School Server zeigt in der Grundeinstellung die vorhandenen Ordner an und wieviele neue/gelesene Mails sich in den einzelnen Ordner befinden. Zu dieser Ordneransicht kommen Sie jederzeit zurück, indem sie auf das 'Ordner' Symbol klicken. Um eine neue Mail zu schreiben wählen sie das 'Verfassen' Symbol an.

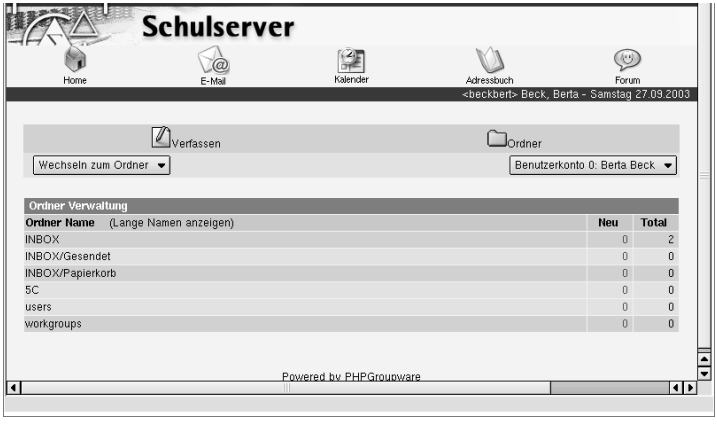


Abbildung 7.5: *Das Mail-Programm des SUSE LINUX School Server*

Verfassen von E-Mails

Um eine neue Mail zu schreiben, klicken Sie auf das 'Verfassen' Symbol. Darauf erscheint die auf Abbildung 7.6 auf der nächsten Seite sichtbare Eingabemaske zum Erstellen einer neuen E-Mail. Hier müssen Sie zunächst unter 'An:' einen Addressaten eingeben. Das können Sie von Hand, oder mit Hilfe des Adressbuch Symbols erledigen (siehe nächsten Abschnitt). Ihre Mails können Sie auch als 'Kopie' oder 'Blindkopie' versenden. Im ersten Fall sieht der Empfänger, wer

die Mail noch erhalten hat; bei der Blindkopie ist nicht ersichtlich, wer die E-Mail noch erhalten hat. Unter 'Betreff' können Sie das Thema oder den Zweck der E-Mail angeben. Da es nicht üblich ist, E-Mails ohne Betreff zu senden, und da die Betreff-Zeile den Überblick über die E-Mails erleichtert, sollten Sie dieses Feld nach Möglichkeit ausfüllen.

Abbildung 7.6: *Erstellen einer neuen E-Mail*

Möchten Sie darüber informiert werden, dass der/die Empfänger/in den Brief erhalten hat, kreuzen Sie die 'Benachrichtigung bei Auslieferung' Checkbox an. Beachten Sie bitte, das diese Funktion nicht von allen Mail-Programmen unterstützt wird. Zusammen mit Ihrer E-Mail können Sie auch beliebig viele Dateien versenden. Klicken Sie dazu auf die Überschrift 'Datei anhängen' und wählen Sie die Datei mit einem weiteren Klick auf 'Durchsuchen...' aus. Nachdem Sie sich für eine Datei entschieden haben, müssen Sie 'Datei anhängen' wählen, um die Datei auf den SUSE LINUX School Server zu verschieben. Allenfalls erscheint eine Meldung, die Sie darauf hinweist, dass die Dateien von Ihrem Rechner auf einen anderen Rechner verschoben werden; dies hängt vom verwendeten Browser ab. Da sich der SUSE LINUX School Server des geschützten `https` Protokolls bedient, können Sie hier beruhigt weiterfahren. Auf dieselbe Art können Sie weitere Dateien anhängen. Bevor Sie nun mit 'Fertig' das Dialogfenster schliessen, müssen Sie zuerst noch jede anzuhängende Datei in der entsprechenden Checkbox ankreuzen.

Schliesslich müssen Sie noch den Text der E-Mail verfassen. Dazu dient das grosse Textfeld am unteren Rande. Sind Sie mit Ihrer Mail fertig, klicken Sie ein-

fach auf 'Senden', und schon leitet der SUSE LINUX School Server Ihre Mail an den/die entsprechenden Empfänger weiter.

Achtung

Bitte beachten Sie, dass das Senden von E-Mails allenfalls auf die schulinternen Adressen beschränkt ist. Bitte wenden Sie sich in diesem Fall an den Systemadministrator.

Achtung

Benutzen des Adressbuches

Niemand kann sich 1000 E-Mail Adressen merken. Aus diesem Grund gibt es auch im SUSE LINUX School Server ein zentrales Adressbuch, das u. A. auch alle E-Mail Adressen beinhaltet. Grundsätzlich haben alle Lehrkräfte und alle Schüler Lesezugriff auf das zentrale Adressbuch. Um die einzelnen Einträge zu sehen, wählen Sie unter der Web-Oberfläche den 'Adressbuch' Hauptmenüpunkt aus. Daraufhin erscheint die Adressbuch-Übersicht (siehe Abbildung 7.7).

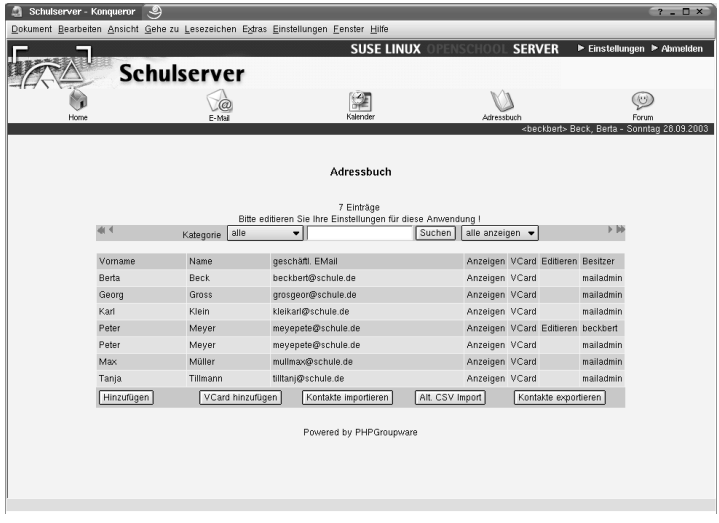


Abbildung 7.7: *Übersicht über das Adressbuch*

Hier können Sie entweder mit Hilfe der Pfeiltasten im Adressbuch blättern, oder die Suchfunktion benutzen, um nach einem bestimmten Eintrag zu suchen.

Schreiben Sie dazu das gesuchte Stichwort ins Eingabefeld und drücken Sie dann auf den 'Suchen' Button. Wenn Sie nur in bestimmten Kategorien suchen möchten, können Sie das mit Hilfe der 'Kategorie' Pull-Down Liste tun. Um z.B alle Schüler-Einträge der Klasse 5B zu sehen, wählen Sie die (voreingestellte) Kategorie Schüler aus, schreiben ins Eingabefeld `5B` (Klein-/Grossschreibung nicht verwechseln) und drücken dann anschließend den 'Suchen' Knopf.

Um Ihrem Adressbuch einen neuen Eintrag hinzuzufügen, drücken Sie auf 'Hinzufügen'. Es erscheint eine ziemlich umfangreiche Eingabemaske, eingeteilt in die drei Bereiche persönlich, geschäftlich und privat (home), wo Sie wenigstens die Felder 'Name' und 'Vorname' ausfüllen müssen. Die übrigen Felder können Sie nach eigenem Ermessen ausfüllen. Um die Suche nach einem bestimmten Eintrag leichter zu gestalten empfiehlt es sich, auch die Rubriken 'Privat' und 'Kategorie' auszufüllen. Sind Sie mit dem Eintrag fertig, klicken Sie bitte auf 'OK'. Es erscheint dann eine Übersicht, in der Sie die Möglichkeit haben, den Eintrag zu editieren, zu kopieren oder als VCard zu exportieren. Mit einem Klick auf 'Fertig' beenden Sie die Eingabe und gelangen zurück zur Adressbuch-Übersicht.

Bestehende Einträge in der Mail Komponente auswählen

Um an die Einträge im Adressbuch heranzukommen, klicken Sie beim Erstellen einer neuen Mail auf den 'Adressbuch' Eintrag. Daraufhin erscheint das auf Abbildung 7.8 auf der nächsten Seite sichtbare Fenster.

Hier sehen Sie je nach Einstellung 10-20 Einträge. Bei mehr als 20 Einträgen können Sie zum Navigieren die grünen Pfeiltasten oben rechts und links verwenden. Um eine Adresse hinzuzufügen, müssen Sie auf die sich unter den einzelnen Einträgen befindenden 'To', 'Cc' oder 'Bcc' Buttons klicken:

To: Der Addressat der Mail. Anders als bei konventionellen Briefen können Sie eine E-Mail gleichzeitig mehreren Adressaten zusenden. Drücken Sie dazu einfach bei den entsprechenden Adress-Einträgen auf den 'To' Button.

Cc: Die über diesen Button angewählten Personen erhalten die Mail nicht als direkt Adressierte, sondern als Kopie. Das können Sie z. B. brauchen, wenn Sie Eltern eine Kopie einer E-Mail von Schüler zustellen möchten oder wenn Sie beim Organisieren einer Party nicht nur diejenigen benachrichtigen möchte, die die Party organisieren, sondern auch die Schulleitung.

Bcc: Die über diesen Button ausgewählten Adressen bekommen die E-Mail als geheime Kopie, d.h. der Empfänger weiss nicht, dass die Mail auch an andere AdressatInnen versendet wurde. Da Blindkopien nicht gerade

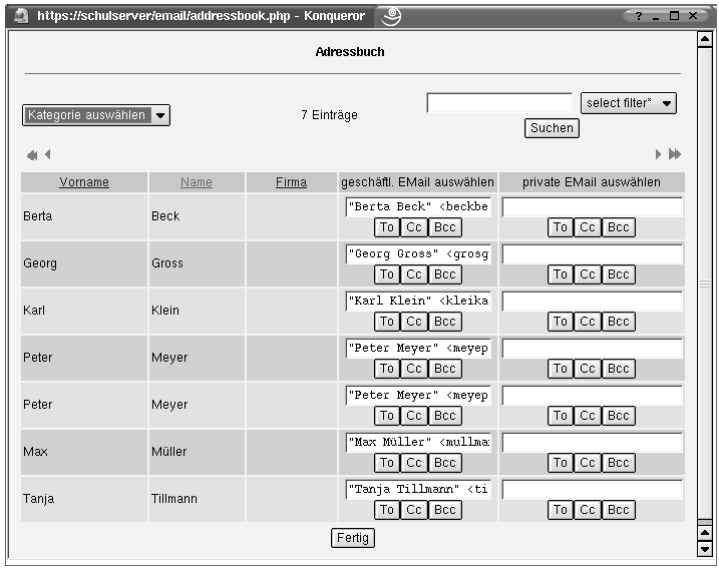


Abbildung 7.8: *Adressen aus dem Adressbuch einfügen*

Vertrauenserweckend sind (der Empfänger kann nicht feststellen an wen die Mail (noch) gesendet wurde), sollte man sie wenn möglich vermeiden.

Während Sie die einzelnen Buttons anwählen fügt das Mail-Programm die Adressen automatisch an der richtigen Stelle in der neuen Mail ein. Haben Sie alle Adressen eingefügt, klicken Sie auf ‘Fertig’. Die einzelnen Adressen sind nun in der Eigabemaske mit Kommatas getrennt sichtbar. Wenn Sie wollen, können Sie der Liste von Hand noch weitere Einträge beifügen.

E-Mails lesen

Jetzt, wo Sie problemlos neuen E-Mails schreiben können, möchten Sie natürlich auch die entsprechenden Antwortbriefe lesen können. Um E-mails zu lesen, gibt es grundsätzlich zwei Möglichkeiten:

- Sie klicken in der Ordnerübersicht auf den entsprechenden Ordnernamen. Das geht beim Starten der Mail Komponente am schnellsten. Um später wieder zur Ordnerübersicht zu gelangen wählen Sie einfach den 'Ordner' Punkt an.
- Sie wählen den entsprechenden Ordner aus der 'Wechseln zum Ordner' Pull-down Liste aus. Mit Hilfe dieser Methode können Sie jederzeit zum entsprechenden Ordner wechseln, ohne den Umweg über die Ordnerübersicht zu machen.

Die INBOX

Solange Sie keine zusätzlichen Mail-Filter eingerichtet haben (siehe Kapitel 8 auf Seite 185), werden alle an Sie adressierten Mails im Ordner 'INBOX' (Briefkasten) abgelegt. Nachdem Sie diesen Ordner angewählt haben, sollten Sie eine zu Abbildung 7.9 ähnliches Fenster sehen.

Abbildung 7.9: *Die INBOX Übersicht von Berta Beck*

Über der INBOX haben Sie oben die gleichen Bedienelemente wie bei der Ordnerübersicht. Darunter sind links und rechts je zwei Pfeilsymbole zu sehen. Mit Hilfe dieser Pfeilsymbole können Sie in der INBOX blättern, falls Ihre Mails mehr als eine Seite benötigen. Darunter befindet sich ein grüner Balken mit

wichtigen Informationen zur INBOX, z.B wieviele neue und wieviele ungelesene Mail Sie haben. Die INBOX selbst besteht aus sechs Spalten.

In der ersten Spalte gibt es vor jeder Mail eine Checkbox, um die Mail zu markieren. Sie können dann die markierten Mails verschieben, löschen oder in den Papierkorb werfen. Um alle Mails auf der Seite auf einmal zu markieren, klicken Sie auf das blaue Häkchen unter den Checkboxen. Um die markierte(n) Mail(s) daraufhin in den Papierkorb zu werfen klicken Sie einfach auf 'Löschen'. Die Mails werden daraufhin in den Ordner 'INBOX/Papierkorb' verschoben. Um die Mails endgültig zu löschen, müssen Sie in diesen Ordner wechseln und dort das Löschen wiederholen. Wenn Sie die Mails nicht in den Papierkorb, sonder in einen anderen Ordner verschieben möchten, dann klicken Sie nach Auswahl der entsprechenden Mail(s) auf das 'Verschiebe ausgewählte Nachrichten nach' Pull-down Menü und wählen dann den entsprechenden Ordner aus.

In der nächsten Spalte sehen Sie, ob eine Nachricht nur aus Text besteht oder ob Sie zur Nachricht auch noch ein Anhang (Attachment) bekommen haben. Falls die entsprechende Mail einen Anhang enthält, wird dies in dieser Spalte durch eine Büroklammer markiert.

Die dritte Spalte (mit 'Von' beschriftet) gibt Auskunft darüber, von wem Sie die Nachricht erhalten haben. Ist der Absender mit fetten Buchstaben gedruckt, bedeutet das, dass Sie die Mail nocht nicht gelesen haben. Möchten Sie die erhaltenen Nachrichten nach dem Sender sortieren, klicken Sie einfach einmal auf die 'Von' Überschrift. Die entsprechende Überschrift wird dann mit zwei Sternen markiert. In der Grundeinstellung werden die eingehenden Nachrichten nach dem Eingangs-(Datum) geordnet.

In der nächsten Spalte ('Betreff') können Sie eine Kurzinfo zur Nachricht sehen. Beginnt eine Kurzinfo mit 'Re:' handelt es sich dabei um ein Antwortschreiben. Diese Kurzinfo verbirgt auch den Zugang zur Mail selbst. Klicken Sie einfach auf den entsprechenden Betreff, und schon erscheint die ganze Nachricht. Auch hier können Sie die Sortier-Funktion benutzen, wenn Sie in der Kopfzeile auf den 'Betreff' Eintrag klicken.

In der nächsten Spalte ('Datum') sehen Sie, wann die Mail abgeschickt wurde. Ist die Nachricht noch keinen Tag alt, wird die aktuelle Uhrzeit angezeigt, sonst, das Absendedatum.

In der letzten Spalte schließlich können Sie die Größe der Nachricht ansehen. Mails die nur Text enthalten sind in der Regel höchsten ein paar Kilobyte gross. Bei 50 k oder größer wurde der Mail vermutlich ein Anhang beigefügt

Nachrichten beantworten und weiterleiten

Nachdem Sie in der entsprechenden Zeile auf den Betreff Eintrag geklickt haben, können Sie die Mail endlich lesen :-). Im oberen Bereich der Leseansicht

finden Sie die bekannten Elemente zum Navigieren. Darunter wiederum ein grüner Balken mit Pfeil-Icons zum blättern (ganz rechts) und vier weiteren Symbolen mit folgender Bedeutung:

Umschlag mit rotem Pfeil nach links – Mail beantworten Mit Hilfe dieses Symbols können Sie die Mail beantworten. Es erscheint ein neues Fenster zum Erstellen von Mails, das den Empfänger und die ursprüngliche Nachricht bereits enthält. Sie brauchen nur noch den neuen Text zu schreiben. Allfällige Anhänge werden nicht mitgesendet, Sie können aber neue Anhänge hinzufügen.

Umschlag mit zwei roten Pfeilen nach links – Allen antworten Die Funktion ist mit der oben geschilderten identisch, nur dass hier nicht nur dem Absender, sondern auch allen Mitadressierten geantwortet wird. Praktisch, wenn Sie zu dritt oder viert per Mail etwas besprechen wollen.

Umschlag mit blauem Pfeil nach rechts – Mail weiterleiten Wollen Sie die Mail nicht beantworten, sondern (zur Ansicht oder mit Kommentar) an jemanden weiterleiten, können Sie das mit Hilfe dieses Symbols tun. Es erscheint ebenfalls das Fenster zum Erstellen einer Mail, in dem Sie nur noch den/die Adressierten auswählen müssen.

Papierkorb – Mail löschen Wenn Sie auf dieses Symbol drücken, wird die Mail ohne Nachfrage in den Papierkorb verschoben. Im Mailfenster erscheint darauf die nächste Mail im Ordner. Die so gelöschten Mails können Sie immer noch im Ordner 'INBOX/Papierkorb' erreichen. Um eine Mail endgültig zu löschen, müssen Sie zuerst dorthin wechseln und dort die Löschung wiederholen.

Die eigentliche Nachricht finden Sie unter 'Nachricht:'. Sollten Sie mit der Nachricht auch einen Anhang bekommen haben, befindet der sich unter 'Sektion: 2'. Je nachdem, ob es sich beim Anhang um einen bekannten Filetyp handelt, wird der Anhang dargestellt (z.B. Bilder) oder kann per Mausklick gespeichert werden.

Neue Ordner anlegen

Auf der Groupware Oberfläche können leider keine neuen Unterordner angelegt werden. Um einen neuen Mailordner anzulegen, müssen Sie sich auf die Administrations-Oberfläche einloggen und dort unter 'Ordner' → 'Neu' einen neuen Unterordner anlegen. Danach müssen Sie sich von neuem auf der Groupware Oberfläche anmelden.

Abbildung 7.10: *Eine Mail lesen und beantworten*

E-Mails des Kalenders bearbeiten

Eine besondere Stellung unter den eingehenden Nachrichten nehmen die internen Mails des Kalenders ein. Sie sind am ‘Kalender Aktualisierung ()’ Betreff zu erkennen (siehe Abbildung 7.9 auf Seite 170). Haben Sie eine solche Mail erhalten, wurden Sie mit ziemlich grosser Sicherheit zu einem gemeinsamen Termin/Treffen eingeladen. Wie bei mündlichen Besprechungen haben Sie auch hier mehrere Möglichkeiten auf die Einladung zu reagieren (siehe Abbildung 7.11 auf der nächsten Seite).

In der Nachricht sehen Sie zunächst eine Übersicht über den Tag des Treffens. Sollten Sie an diesem Tag weitere Verabredungen haben, erscheinen diese ebenfalls auf der Zeitachse, so wissen Sie, ob der geplante Zeitpunkt noch frei ist. Unter der Zeitachse können Sie Titel und Beschreibung des Treffens, sowie dessen wichtigste Parameter sehen (Ort, Dauer, Teilnehmer, wer organisiert das Treffen etc.).

Sind Sie im Bilde, können Sie mit Hilfe der fünf Buttons am unteren Fensterrand Ihre Entscheidung treffen. Sind Sie sicher, dass Sie an der geplanten Verabredung teilnehmen können, drücken Sie den ‘Zusagen’ Button. Sind Sie sicher, dass Sie am Treffen nicht teilnehmen werden können, klicken Sie auf ‘Absagen’. Sind Sie sich noch nicht ganz sicher, planen aber am Treffen teilzunehmen, wählen Sie ‘Vorläufige Zusage’. Falls Sie sich jetzt noch nicht entscheiden können, ist ‘Keine Antwort’ eine gute Wahl. So können Sie später jederzeit zu dieser Mail

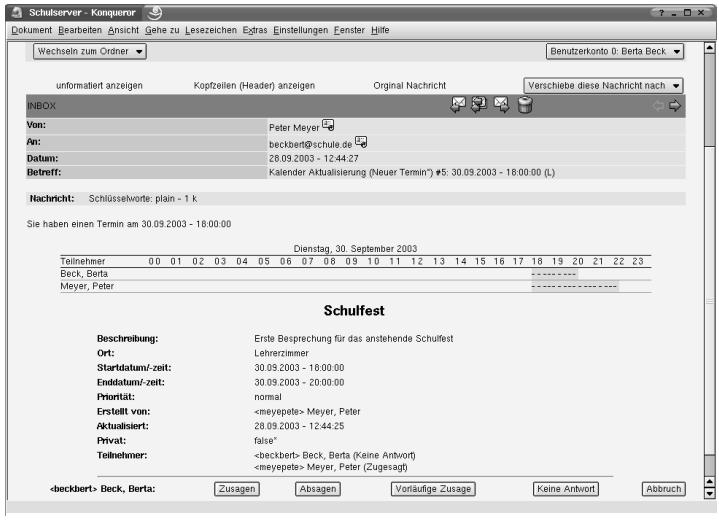


Abbildung 7.11: *Gemeinsame Treffen per Mail organisieren*

zurückkehren und sich definitiv entscheiden. Mit 'Abbruch' kommen sie zu Ihrem Kalender, in dem Sie z.B einen Gegenvorschlag organisieren oder ein zur gleichen Zeit stattfindendes Treffen umorganisieren können.

Sobald Sie Ihre Entscheidung getroffen haben, wird über den SUSE LINUX School Server eine entsprechende Mail versendet, die automatisch die Kalendereinträge der übrigen Teilnehmer aktualisiert. Wenn Sie z.B. zugesagt haben, wechseln Sie zu Ihrem Kalender (das geschieht bei Zusage automatisch) und wählen dort den Termin an. Hinter Ihrem Namen sollte jetzt '(Zugesagt)' stehen.

Foren

Einrichten der Foren

Bevor Sie in Ihrer Schule die SUSE LINUX School Server Foren sinnvoll nutzen können, müssen Sie diese zuerst einrichten. Das Einrichten von Foren ist den Lehrkräften vorbehalten. Loggen Sie sich dazu auf der Web-Benutzeroberfläche ein und wählen Sie den 'Administration' → '(Lehrer-)Forum Administration' Menüpunkt aus. Da die Einstellung der allgemeinen und des Lehrerforums gleich verläuft, beschränken wir uns in diesem Kapitel auf die Einstellung des

allgemeinen Forums. Nachdem Sie den entsprechenden Punkt ausgewählt haben, sollten Sie den auf Abbildung 7.12 sichtbaren Screen sehen.

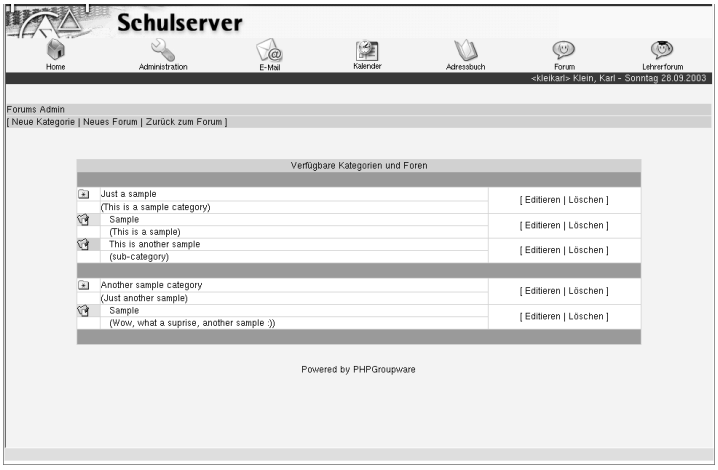


Abbildung 7.12: *Erstes Einrichten der Schüler- und Lehrerforen*

Unter 'Verfügbare Kategorien und Foren' können Sie die bereits eingestellten Beispiel-Kategorien und die dazugehörenden Foren sehen. In einem ersten Schritt ist es am einfachsten, diese zu editieren. Klicken Sie dazu hinter 'Just a sample' (engl. *nur ein Beispiel*) auf 'Editieren', und geben Sie der Kategorie im erscheinenden Dialogfenster einen neuen Namen und eine kurze Beschreibung. Um die Änderungen zu übernehmen und den Dialog zu verlassen, klicken Sie bitte auf 'Kategorie updaten'. Legen Sie hier z.B. die Kategorie Linux an.

Die zur Kategorie gehörenden Foren (Ordner Symbol mit Merkzettel und Reisnagel) heissen jetzt noch 'Sample' und 'This is another sample'. Wiederholen Sie die obigen Schritte auch für diese beiden Einträge und legen Sie so z.B. die Foren SuSE und Knoppix an. Ändern Sie nun auch die 'Another sample category' Einträge nach obigem Muster. Möchten Sie noch weitere Kategorien anlegen, können Sie das über den 'Neue Kategorie' Menüpunkt tun. Um ein neues Forum anzulegen wählen Sie den 'Neues Forum' Eintrag. Da Sie sich beim Anlegen des Forums für eine bereits bestehende Kategorie entscheiden müssen, müssen Sie diese allenfalls im Voraus anlegen. Sind Sie fertig, sollte Ihr Bildschirm etwa wie auf Abbildung 7.13 auf der nächsten Seite aussehen.

Abbildung 7.13: *Nach dem erfolgreichen Anlegen des Forums*

Dieselben Schritte müssen Sie nun auch für die Lehrerforen wiederholen. Sind Ihnen die Einstellungen zu (wenig) bunt, können Sie als `root` die unter `/srv/phpwg/phpgwapi/themes` befindliche `default.theme` Datei editieren oder sie durch eine der dort befindlichen Themendateien ersetzen.

Achtung

Bitte beachten Sie, dass sich das Ändern der Themendatei nicht nur auf die Foren, sondern auf die gesamte Web-Benutzeroberfläche bezieht. Erstellen Sie deshalb gegebenfalls eine Sicherheitskopie der bestehenden `default.theme` Datei.

Achtung

Benutzen des Lehrer- und Schülerforums

Nach dem Einstellen der Foren können Schüler und Lehrer diese benutzen. Lehrer haben Zugriff auf beide Foren, SchülerInnen können nur auf dem Schülerforum lesen und schreiben. Auf der Startseite (siehe Abbildung 7.14 auf der nächsten Seite) können Sie die eingestellten Kategorien, die dazugehörenden Kurzbeschreibungen, das Erstelldatum, sowie die Anzahl der Beiträge sehen.

Wählen Sie den Namen der entsprechenden Kategorie an, erscheinen die dazugehörenden Foren mit denselben Informationen wie oben. Ein erneuter Klick

Abbildung 7.14: *Einstiegseite auf einem Schülerforum*

auf den entsprechenden Namen bringt Sie zur Themenübersicht. Hier können Sie entweder ein neues Thema eröffnen ('Neues Thema' Überschrift) oder zu einem bestehenden Thema einen Beitrag hinzufügen. Sollten Sie sich für ein neues Thema entscheiden, können Sie auch gleich einen ersten Beitrag schreiben. Da einmal angelegte Themen nicht gelöscht werden können, sollten Sie sich Ihr Thema gut überlegen. Um bei einem bestehenden Thema mitzusprechen, müssen Sie die entsprechende Themenüberschrift anwählen. Je nach Schriftverkehr des Themas müssen Sie sich zunächst mal durch einige Beiträge hindurchlesen, bevor Sie am Ende der Seite das entsprechende Eingabefeld für Ihren Beitrag finden.

Möchten Sie dies verhindern, wählen Sie auf der Themenübersicht neben 'Neues Thema' den 'Alle Beiträge sichtbar' Punkt an. So können Sie den Beitrag, den Sie beantworten möchten, direkt anwählen. Die Antwort-Beiträge werden automatisch mit der Vorsilbe `Re:` (engl. *Reply*) versehen. Wenn Sie also einen Beitrag nicht beantworten, sondern z. B. ergänzen möchten, können Sie an dessen Stelle auch einen aussagekräftigeren Betreff wählen.

Achtung

Lehrer können zwar Foren und Kategorien anlegen und löschen, einzelne Beiträge können allerdings nicht moderiert werden.

Achtung

Administration als Benutzer

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

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

Achtung

Da das Zertifikat des SUSE LINUX School Server erst bei der Installation speziell für Ihre Schule ausgestellt wurde, kennt der Browser dieses Zertifikat natürlich nicht und gibt eine entsprechende Warnung aus.

Achtung

Nach der Anmeldung mit Ihrem Benutzernamen erreichen Sie einen Konfigurationsbereich, in dem Sie persönliche Einstellungen vornehmen können. Die einzelnen Menüpunkte werden in den folgenden Abschnitten erläutert.

Einstellungen

Dieses Menü bietet Ihnen die Möglichkeit, Ihre persönlichen Daten (z. B. Adresse und Telefonnummer) und das Passwort zu ändern, sowie ein für Sie erstelltes Zertifikat herunterzuladen.

Eingeben und Ändern der persönlichen Daten

Hier können Sie, je nach Schreibberechtigung, die vom Administrator eingetragenen persönlichen Daten (siehe Abb. 8.1 auf der nächsten Seite) des zentralen Adressbuchs 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.

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

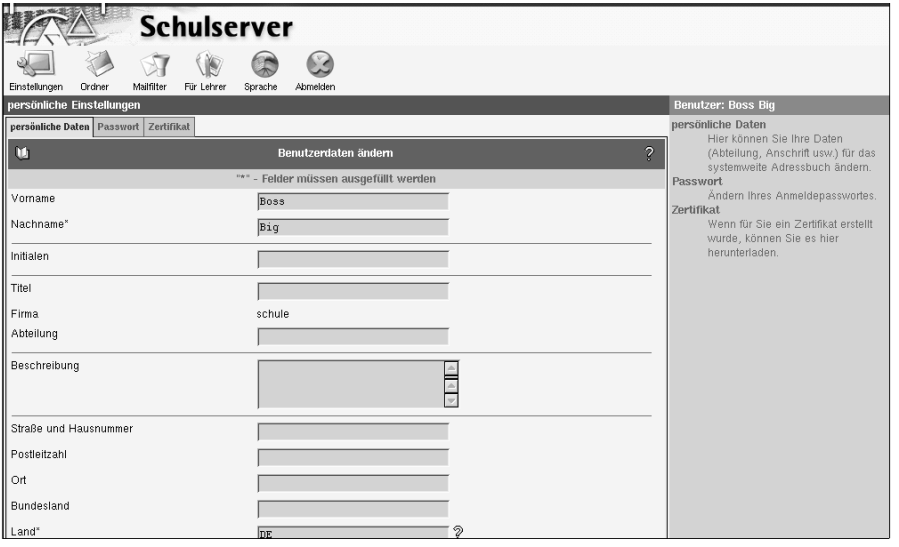


Abbildung 8.1: *Persönliche Daten des Benutzers*

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 (siehe Abb. 8.2 auf der nächsten Seite). 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.

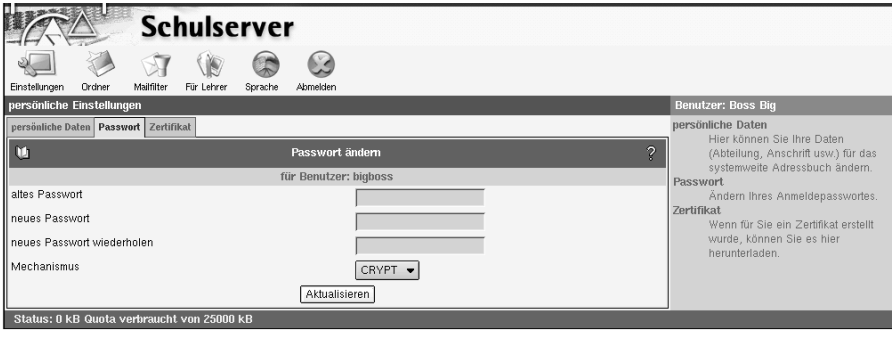


Abbildung 8.2: *Passwort des Benutzers ändern*

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 195). Im Allgemeinen sollten dies die Klassenlehrer sein - das hängt aber vom Administrator ab.

Zertifikat: Herunterladen eines Zertifikates

Wenn Ihr Administrator ein Zertifikat für Sie erzeugt hat, können Sie dieses über ‘Zertifikat’ herunterladen und mit Ihrem Browser importieren. Informationen darüber, wie Sie mit Ihrem Browser ein Zertifikat importieren, entnehmen Sie bitte der Dokumentation Ihres Browsers.

Ordner

Der SUSE LINUX 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.

Beim SUSE LINUX 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.

`INBOX.drafts`: In diesem Ordner können Sie Entwürfe von E-Mails ablegen, die Sie noch nicht verschickt haben.

`INBOX.sent-mail`: Alle E-Mails, die Sie verschicken, werden hier abgelegt.

`INBOX.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 8 auf Seite 188).

`INBOX.trash`: 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 (z. B. `INBOX`). Geben Sie dann den gewünschten Namen des neuen Ordners an (siehe Abb. 8.3 auf der nächsten Seite).

Abbildung 8.3: *Neuen Ordner anlegen*

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

Hinweis

Eine besondere Bedeutung hat der Punkt in Ordnernamen. Ein Punkt wird als „Hierarchie Separator" benutzt, vergleichbar mit dem "/"(Slash) bei Verzeichnissen. Legen Sie z. B. einen Ordner namens `lehrer.mathe` an, haben Sie sinngemäß ein Verzeichnis `lehrer` mit einer Datei `mathe` erstellt. Legen Sie jetzt noch einen Ordner namens `lehrer.musik` an, haben Sie ein Verzeichnis mit zwei Dateien.

Haben Sie den Ordner `lehrer` vorher nicht einzeln angelegt, kann in diesem keine E-Mail abgelegt werden!

Hinweis

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 (siehe Abb. 8.4).

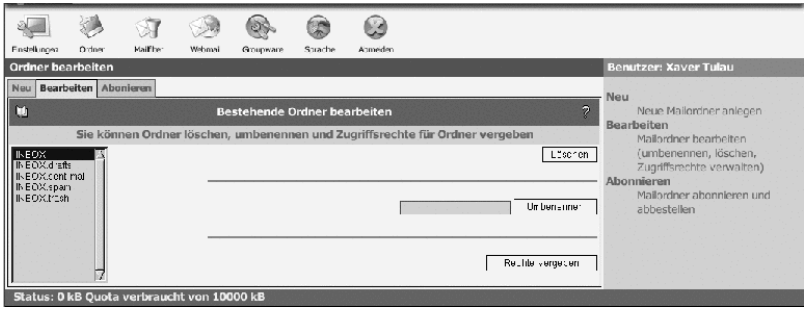


Abbildung 8.4: *Ordner bearbeiten*

Wie auch für die gemeinsamen Ordner können Sie Rechte für die Benutzer-Ordner vergeben. Mit dem Button 'Rechte vergeben' erhalten Sie die schon von der Erstellung gemeinsamer Ordner bekannte Maske. Als Eigentümer des Ordners haben Sie prinzipiell alle Rechte an dem Ordner. Sie sollten diese Einstellung auch nicht verändern.

SIEVE: Der Mailfilter

Mit dem SIEVE-basierten Mailfiltersystem des SUSE LINUX 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 SUSE LINUX 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. 8.5 auf der nächsten Seite).

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 8.5: *Mailfilter*

Abbildung 8.6: *Größenbeschränkung definieren*

Wählen Sie ‘Filterregel einfügen’. Klicken Sie auf ‘Größenbeschränkung’ (siehe Abb. 8.6). 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. 8.7 auf der nächsten Seite).

Abbildung 8.7: *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

Wenn das System für die Erkennung und Markierung von so genannter SPAM-Mail konfiguriert ist, 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 SUSE LINUX School Server automatisch auf ankommende E-Mails antworten lassen. Klicken Sie auf 'Erstellen', um eine

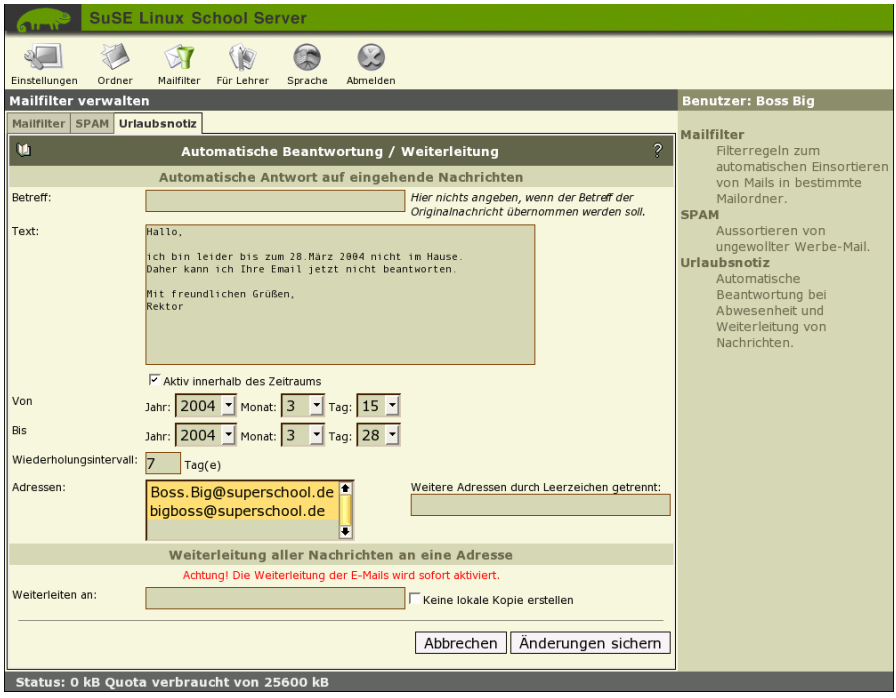


Abbildung 8.8: *Urlaubsnotiz erstellen*

Notiz anzulegen. In der folgenden Maske geben Sie den Betreff und den Text der abzusendenden Nachricht ein (siehe Abb. 8.8).

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.

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 SUSE LINUX 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.

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 4 auf Seite 95). 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 SUSE LINUX School Servers und ins Internet zu kontrollieren, ist nur dann gegeben, wenn die Clientrechner registriert sind.

Hinweis

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

Internet erlauben/ verbieten

Durch die Aktivierung dieser Checkbox schalten Sie den Zugang für die registrierten Clients zum Proxyserver frei. Damit können die Schüler Internetseiten ansurfen.

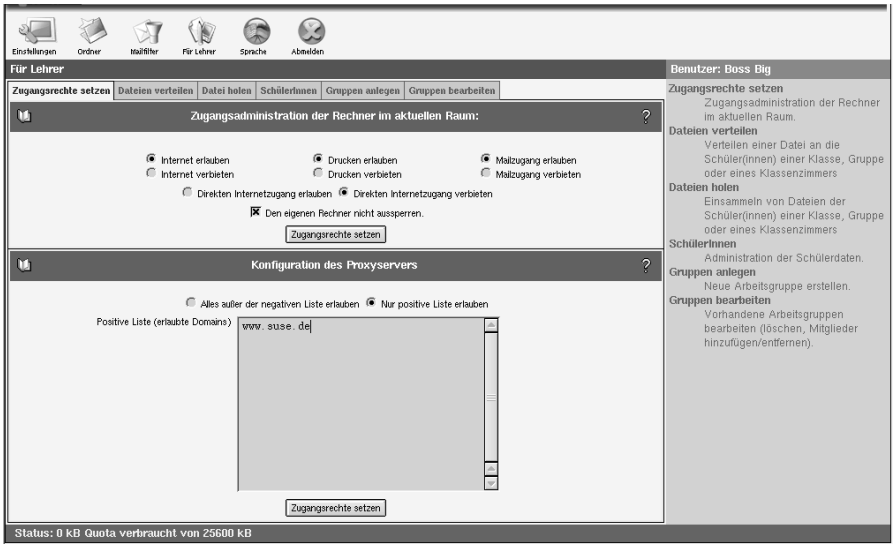


Abbildung 8.9: *Zugangskontrolle für LehrerInnen*

Die Sperre bzw. Freigabe des Internets erfolgt dabei raumbezogen, wenn die Clients am SUSE LINUX 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.

Ausserdem kann es zu Fehlermeldungen kommen, wenn ein Schüler vor der Freischaltung versucht hat eine bestimmte Seite aufzurufen und diese Seite nach der Freischaltung sofort nochmals angefordert wird. Eine Pause von fünf Sekunden zwischen den Anforderungen oder das Aufrufen einer anderen Webseite behebt hier das Problem.

Drucken erlauben/ verbieten

Wenn die Drucker der Schule über den Printserver des SUSE LINUX 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.

Mailzugang erlauben/ verbieten

Hier können Sie den Zugang zur Groupwareseite unter `https://SchoolServer` gestatten oder verweigern.

Direkten Internetzugang erlauben/ verbieten

Hier wird für die Rechner des betreffenden Schulraumes Masquerading aktiviert.

Dies wird benötigt, wenn Sie z. B. mittels `ftp, smtp, imap` oder `pop` 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 oder Sie mit einem Email-Client Emails eines anderen Providers bearbeiten möchten, müssen Sie vorher erst das Masquerading aktivieren.

Tipp

Masquerading

Beim Masquerading erstellt der SUSE LINUX School Server sozusagen eine Tabelle mit den internen IP-Adressen der Clients, welche im Internet nicht weitergeleitet werden. Stellt ein Client eine Anfrage, trägt der Server dessen IP-Nummer (und den entsprechenden Port) in seiner Tabelle ein und vertauscht die Absenderaddresse des „Anfragepakets“ mit seiner eigenen, öffentlichen IP-Adresse (wobei er einen anderen Port verwendet, den er später wieder zuordnen kann). Bekommt er die entsprechende Antwort von einem Server aus dem Internet (auf dem entsprechenden Port) überprüft er das Paket, ordnet es anhand seiner Tabelle dem richtigen Client zu und leitet es an ihn weiter, nachdem er wieder die richtige Empfängeraddresse eingetragen hat.

Normalerweise merken sowohl die Clients als auch die Server im Internet nichts von diesem heimlichen Austausch: beide meinen, direkt miteinander verbunden zu sein. Allerdings funktioniert dieser „Schwindel“ nicht mit jedem Programm.

Tipp

Da der SUSE LINUX 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 SUSE LINUX 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 SUSE LINUX 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 SUSE LINUX School Servers (wie z. B. der Internetfilter) sind dann nicht mehr wirksam!

Achtung

Konfiguration des Proxyservers

Hier können Sie den Internetzugang für die Clients „feintunen“. Entweder erlauben Sie hier `Alles außer der negativen Liste` des Proxyservers (siehe Anhang B auf Seite 229) oder Sie erstellen selbst eine sog. „Positive Liste“.

Wenn Sie Ihren Schülern während des Unterrichts nur den Zugriff auf ganz bestimmte Domains erlauben wollen, dann tragen Sie die entsprechenden URLs in das entsprechende Formular ein (siehe Abbildung 8.9 auf Seite 191 und aktivieren die Schaltfläche `Nur positive Liste erlauben`.

Wenn Sie also z. B. nur die Domain `http://www.suse.de/` erlauben möchten, dann tragen Sie sie hier ein, aktivieren die Schaltfläche `Nur positive Liste erlauben` und klicken auf `Zugangsrechte setzen` (nachdem Sie vorher auch die Schaltfläche `Internet erlauben` aktiviert haben).

Dateien verteilen und Dateien einsammeln

Die Lehrkräfte können mit Hilfe des SUSE LINUX School Servers Dateien an die Schüler einer Klasse verteilen. Dazu müssen Sie zuerst den Menüpunkt ‘Für Lehrer’ → ‘Datei verteilen’ (siehe Abb. 8.10 auf der nächsten Seite) und die gewünschte Datei und Klasse auswählen. Die Datei wird in die persönlichen Importverzeichnisse der Schüler einer Klasse oder der Workstationbenutzer gelegt.

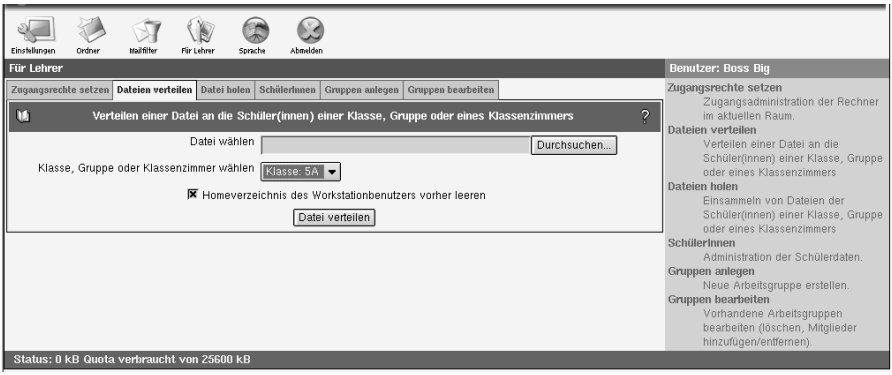


Abbildung 8.10: *Datei verteilen*

Mit dem Menüpunkt 'Für Lehrer' → 'Datei holen' (siehe A.2 auf Seite 222) 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: `/home/teacher/<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: `/home/teacher/<Lehrerlogin>/Import/<Schüler~loginname>-<Datei(en)>`.

Workstationbenutzer - Klausurumgebung

Sind die Clientrechner raumweise registriert, besteht die Möglichkeit, Klassenarbeiten in einer geschützten Umgebung durchzuführen. Dazu muss im Menü 'Für Lehrer' → 'Datei verteilen' statt einer Klasse der aktuelle Arbeitsraum ausgewählt werden.

Durch Aktivieren der Checkbox 'Homeverzeichnis des Workstationbenutzers vorher leeren' kann man vor dem Verteilen der Datei die Homeverzeichnisse

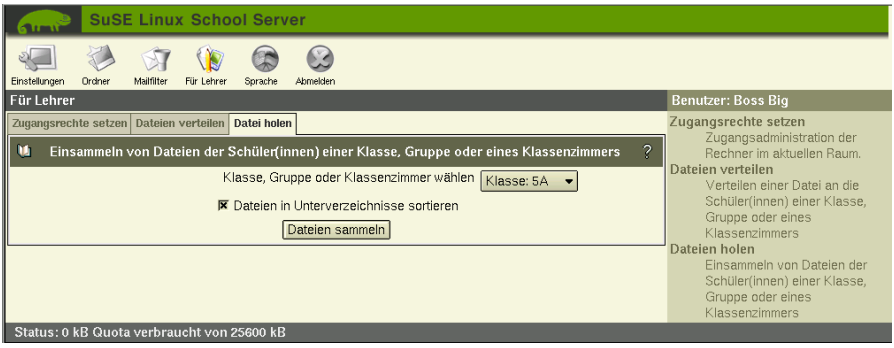


Abbildung 8.11: *Dateien einsammeln*

der Workstationbenutzer auf Standardeinstellung bringen. In diesem Fall dürfen sich die Schüler jedoch erst nach dem Verteilen der Datei anmelden.

Tipp

Vergessen Sie im Falle einer Klassenarbeit nicht, vorher auch die Zugriffsrechte für den Klassenraum entsprechend einzustellen (siehe Abschnitt 8 auf Seite 190).

Workstationaccounts haben keinen Internetzugang und auch keinen Zugang zur Groupware (und damit Email).

Tipp

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

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.

Administration durch Lehrer

Wurden einer Lehrkraft beim Anlegen oder zu einem späteren Zeitpunkt Administrationsrechte vom Administrator zugewiesen, darf sie die Passwörter und

Zugangsrechte der Schüler ändern, sowie neue Benutzergruppen anlegen.

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

Schüler

Im Menü 'SchülerInnen' müssen Sie zuerst 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, die Sie bearbeiten können.

Hinweis

Jeder Lehrer mit administrativen Rechten kann nur Passwörter „seiner" Schüler ändern, d.h. derjenigen Schüler, welche sich in seinen Klassen befinden.

Hinweis

Wählen Sie den zu bearbeitenden Benutzer mit einem Mausklick aus.

Sie können Benutzer auch nach folgenden Kriterien suchen:

UID oder Nachname oder Vorname Tragen Sie das gesuchte Wort oder einen Teil davon mit `'*'` erweitert ins Eingabefeld 'Filter' ein. Andere Jokerzeichen wie z. B. `'?'` funktionieren hier leider nicht.

Klasse bzw. Gruppe Tragen Sie die Bezeichnung der Klasse oder Gruppe, deren Mitglieder Sie suchen, ins Feld 'Klasse' ein. Auch hier können Sie mit dem Suchstring `'5*'` z. B. alle Schüler des fünften Jahrganges auflisten.

Die Funktionen

Externe Mails Ja/Nein Hier können Sie den Schülern gestatten, Emails auch außerhalb der Schule zu versenden. Normalerweise dürfen Schüler sich nur innerhalb der eigenen Schuldomain Emails schreiben - Emails an externe Email-Adressen werden nicht weitergeleitet.

Internet erlauben/ verbieten Sollte ein Schüler den Internetzugang mißbrauchen, können Sie Ihm hier im Rahmen einer „erzieherischen Maßnahme“ den Internetzugang sperren. Der Schüler kann sich dann normal an einem Client anmelden und sämtliche anderen Arbeiten am SUSE LINUX School Server durchführen – wenn er sich jedoch am Proxyserver anmelden will, wird Ihm der Zugriff auf das Internet verweigert.

Zu Gruppe(n) hinzufügen/ entfernen Wenn Sie eigene Gruppen angelegt haben, können Sie hier den oder die betreffenden Schüler in diese Gruppen aufnehmen.

lassen sich auch für mehrere Benutzer gleichzeitig durchführen. Wählen Sie dazu einfach mit Hilfe der gedrückten (Strg)- oder(Shift)-Taste mehrere Benutzer mit der Maus aus.

Die Namen der gewählten Benutzer werden farbig markiert. Am rechten Rand befinden sich Buttons für die einzelnen Funktionen (siehe Abbildung 8.12).

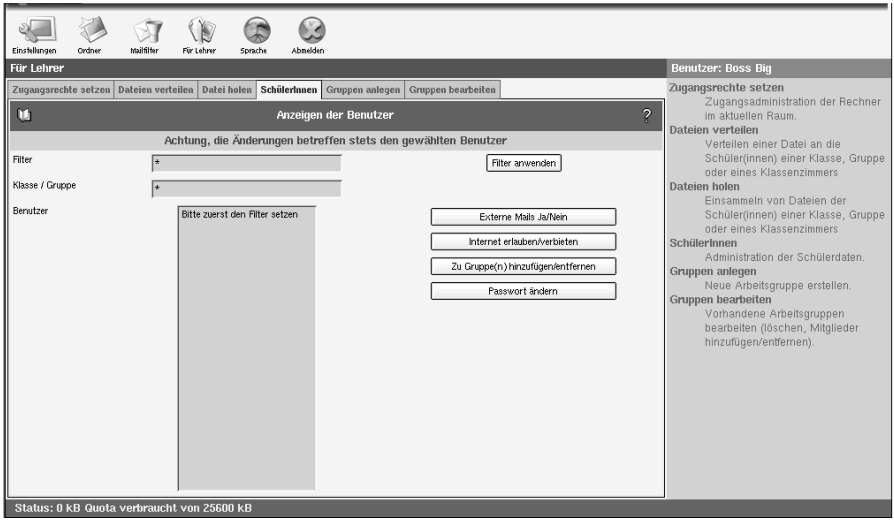


Abbildung 8.12: *Lehreradministration: Verändern der Benutzerdaten*

Unter ‘Passwort ändern’ können Sie das Passwort eines Schülers ändern, wenn dieser sein eigenes vergessen haben sollte. Dazu brauchen Sie verständlicherweise das alte Passwort des Schülers nicht zu wissen.

Unter dem Menüpunkt ‘Mechanismus’ können Sie Art und Stärke der Passwort-Verschlüsselung wählen. Mit der älteren„crypt“-Verschlüsselung ist

eine maximale Passwortlänge von acht Zeichen möglich – längere Passwörter werden einfach abgeschnitten.

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

Wenn der Schüler das Passwort direkt nach dem ersten Anmelden ändern soll (was wir empfehlen), aktivieren Sie noch die entsprechende Checkbox, bevor Sie auf ‘Aktualisieren’ klicken.

Gruppen anlegen/ bearbeiten

Hier können Sie eigene Arbeitsgruppen erstellen, die über eigene Ordner für die gemeinsame Arbeit und eine eigene Email-Adresse unter dem Arbeitsgruppennamen verfügen.

Hinweis

Beachten Sie bitte, dass der Arbeitsgruppenname keine Leer- und Sonderzeichen enthalten darf!

Hinweis

Sie können zunächst auch Arbeitsgruppen ohne Mitglieder erstellen und erst später Schüler und/oder Lehrer hinzufügen.

Alle Mitglieder der Arbeitsgruppe erhalten an den Arbeitsgruppennamen addressierte Emails automatisch in einen Unterordner mit den Namen `workgroups/<Arbeitsgruppennamen>` zugestellt.

Der gemeinsame Ordner befindet sich im Unterverzeichnis `/home/groups/<Arbeitsgruppenname>` – dort haben alle Mitglieder volle Zugriffsrechte.

Sprache ändern

Unter dem Menüpunkt ‘Sprache’ können Sie Ihre bevorzugte Sprache umschalten. Wählen Sie einfach die Sprache und klicken Sie dann zum Speichern den Button ‘Sprache setzen’.

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 SUSE LINUX 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

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.

Speicherung von Logfiles

Im normalen Betrieb des SUSE LINUX 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:

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 291) 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“.

Benutzerordnung

Die folgende Benutzerordnung entstand in Zusammenarbeit mit mehreren Schulen und ist dort – manchmal in leicht abgewandelter Form – bis heute im Einsatz.

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 SUSE LINUX 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 SUSE LINUX School Server lesen Sie bitte unter *Benutzer importieren* auf Seite 63 nach.

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 SUSE LINUX 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* auf Seite 63 beschrieben importieren.

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 10.1 auf der nächsten Seite).

Dort wählen Sie nun ‘Export - Import von Schülerdaten’ → ‘Export für eigene Schule’ (siehe Abbildung 10.2 auf Seite 210).

Nun müssen Sie alle Klassen markieren, die Sie im SUSE LINUX School Server anlegen möchten. Oder wählen Sie `alle Klassen` im unteren Menü.

Achtung

Bei erneutem Einspielen der Liste müssen Sie auch die schon am SUSE LINUX School Server angelegten Klassen auswählen, da diese sonst gelöscht werden!

Für das Anlegen oder Editieren einzelner Schüler sehen Sie bitte im Abschnitt 4 auf Seite 59 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)

Speichern Sie die Datei auf eine Diskette.

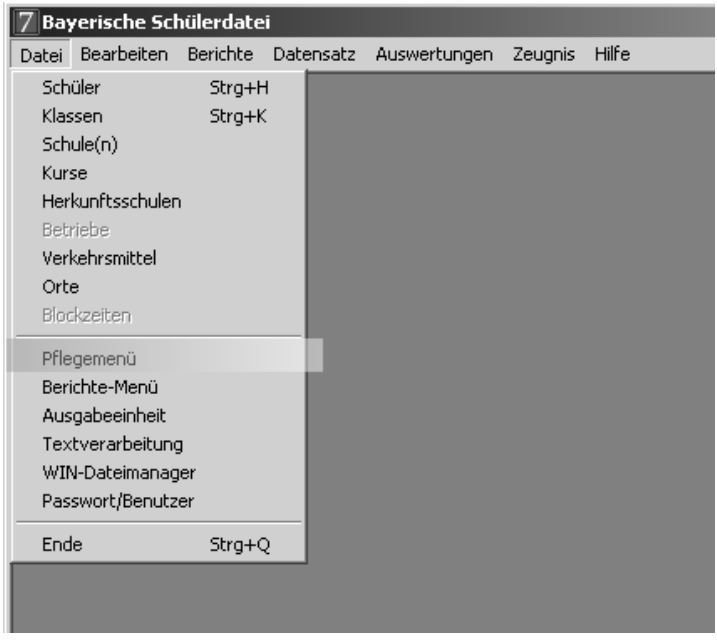


Abbildung 10.1: *WinSV: Aufrufen des Pflegemenüs*

Vor dem Einlesen der Schülerdaten

Um die auf Diskette gespeicherten Daten in den SUSE LINUX School Server einzulesen, müssen diese noch passend formatiert werden. Dies stellen Sie im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' ein, indem Sie unter 'ImportFileFormat' „WinSV“ auswählen.

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.

Zum Exportieren der Schülerdaten wählen Sie im Programm den Menüpunkt 'Zusatz' → 'Datenexport' → 'Text(ASCII)'.

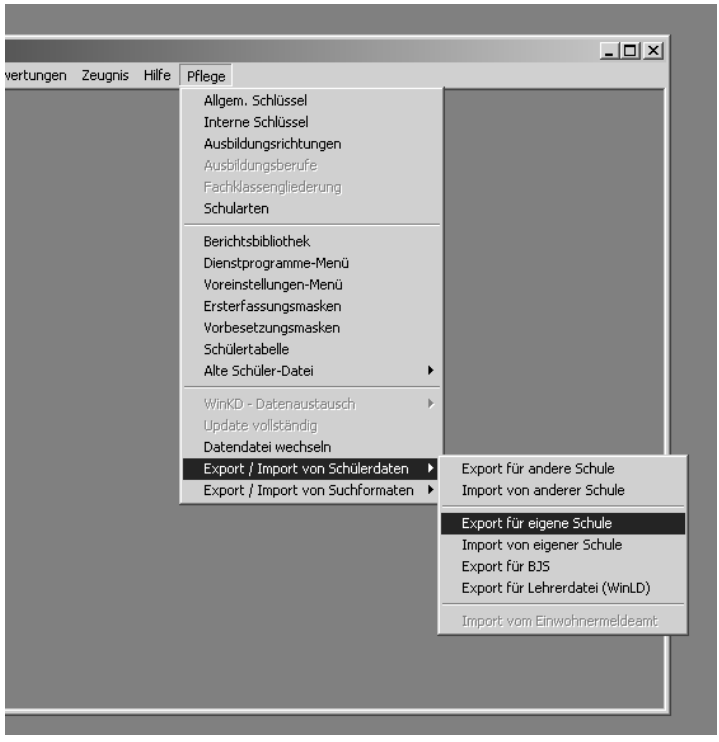


Abbildung 10.2: *WinSV: Export der Daten für die eigene Schule*

Nun müssen Sie alle Klassen markieren, die Sie im SUSE LINUX 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 10.5 auf Seite 213).

Achtung

Bei erneutem Einspielen der Liste müssen Sie auch die schon am SUSE LINUX School Server angelegten Klassen auswählen, da diese sonst gelöscht werden!

Für das Anlegen oder Editieren einzelner Schüler sehen Sie bitte im Abschnitt 4 auf Seite 59 nach.

Achtung

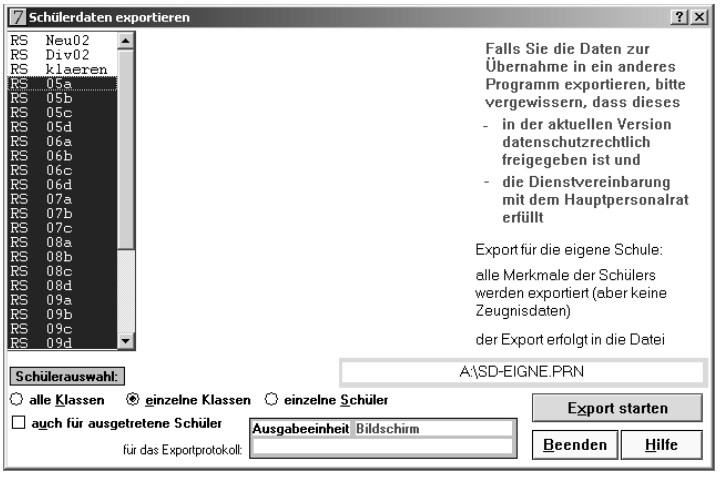


Abbildung 10.3: *WinSV: Export starten*

Vor dem Einlesen der Schülerdaten

Um die auf Diskette gespeicherten Daten in den SUSE LINUX School Server einzulesen, müssen diese noch passend formatiert werden. Dies stellen Sie im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' ein, indem Sie unter 'ImportFileFormat' „SiBank“ auswählen.

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 10.6 auf Seite 213).

Im nächsten Fenster wählen Sie als Datenart 'Schüler' und die Export-Felder:

- Vorname,
- Nachname,
- Namenszusatz,
- Geburtsdatum und

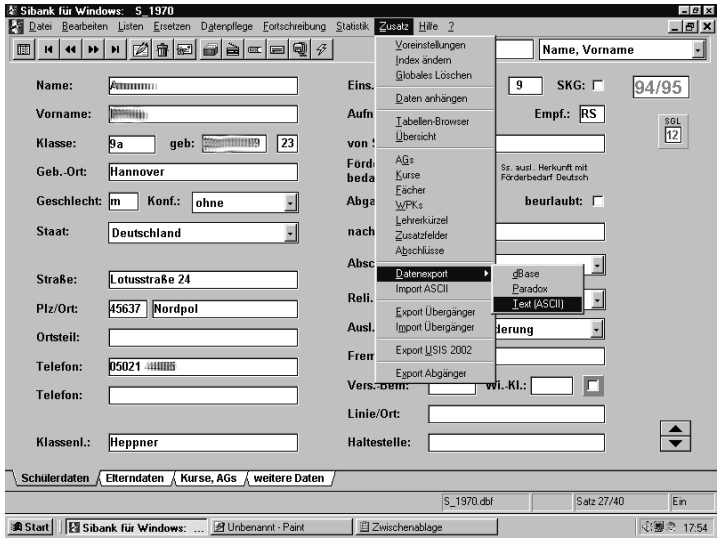


Abbildung 10.4: *SiBank: Aufrufen der Exportfunktion*

- 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 10.7 auf Seite 214).

Die exportierte Datei können Sie direkt mit dem SUSE LINUX School Server einlesen. Stellen Sie dazu im Administrationsmenü des Schulservers unter 'Hilfsmittel' → 'Globale Konfiguration' sicher, das unter 'ImportFileFormat' „CSV“ gewählt ist.

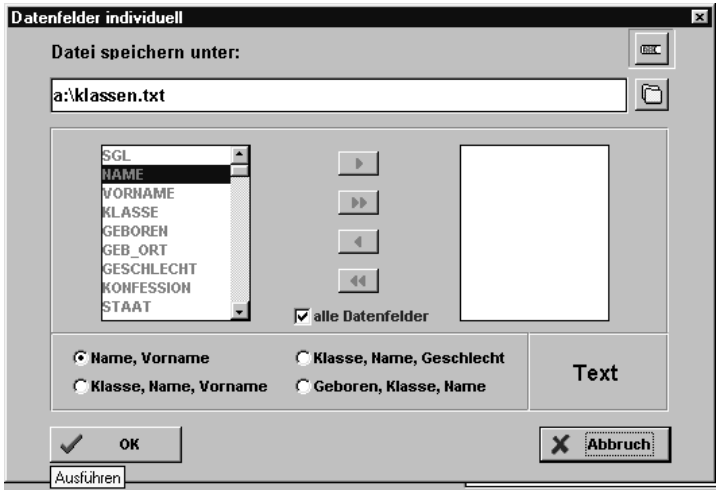


Abbildung 10.5: *SiBank: Speichern der Daten auf Diskette*

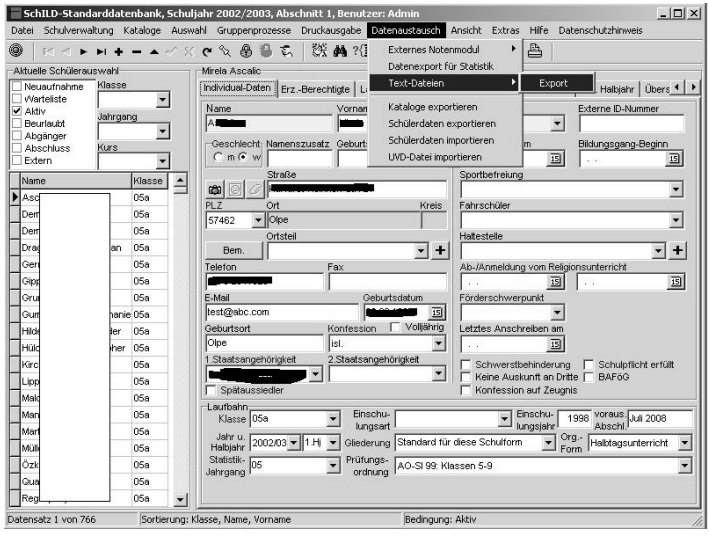


Abbildung 10.6: *Schild-NRW: Aufrufen der Exportfunktion*

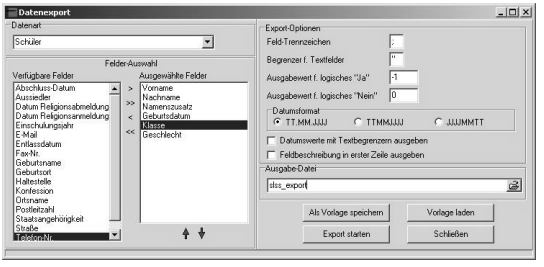


Abbildung 10.7: *Schild-NRW: Export starten*

Korrekturen zum gedruckten Handbuch

Dial-On-Demand

Siehe Handbuch Seite: 45ff.

Wenn Sie sich bei der Internetverbindung für Dial-On-Demand entscheiden, stellen Sie ca. 300 min für die „IDLE-Time“ ein. Dann wird die Verbindung fortwährend offen gehalten und bei evtl. Störungen (Provider trennt die Verbindung) kann die Verbindung automatisch wieder aufgebaut werden.

Alternativ können Sie den Auf- und Abbau der Internetverbindung über je einen Crontab-Eintrag steuern.

Dateisystem

Siehe Handbuch Seite: 72ff

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.

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

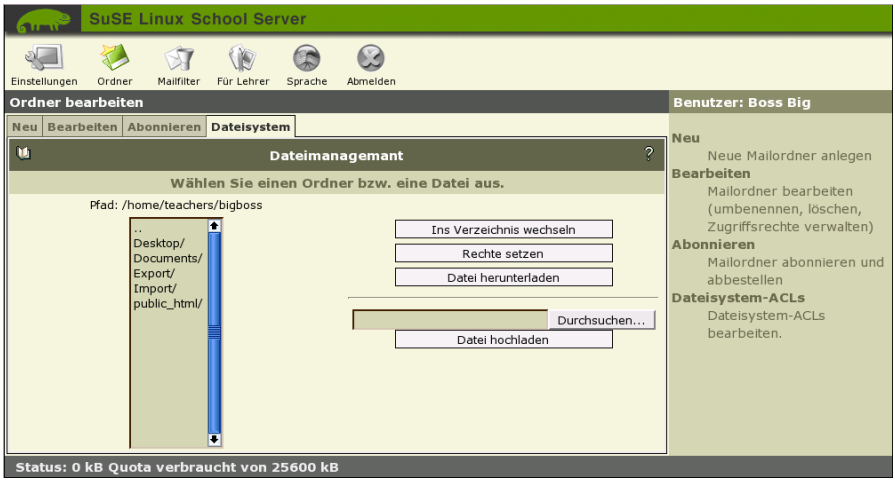


Abbildung A.1: *Dateimanagement*

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 SUSE LINUX 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.

E-Mail-Empfang über UUCP

Siehe Handbuch Seite: 79.

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.

Workstationbenutzer

Siehe Handbuch Seite: 88

Hinweis

Workstationbenutzer

Mit dem Hostname als Loginname und Passwort sollte man sich nur an den Wokrstation anmelden dessen Hostname identisch mit dem Loginname ist. Für die Windows-Clients und die automatisch installierten SuSE Linux Clients ist schon eine Sperre eingebaut die es verhindert, dass man sich mit vom Hostname abweichendem Workstationbenutzeraccount an einem Client anmeldet. Für Mac-Clients gibt es zur Zeit keine solche Beschränkung. Für andere 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 103
then
test $HOST = $USER || exit 1
fi
```

Datei 7: */etc/profile.local*

Hinweis

Links auf Windows-Desktop

Siehe Handbuch Seite: 114ff.

Für Windows-Clients wurden vorbereitend schon zusätzliche Links auf der Desktop-Oberfläche vorgesehen. Diese Links werden allerdings erst bei der zweiten Anmeldung eines Benutzers auch wirklich auf dem Desktop angezeigt.

(Sie finden die Vorgaben für neue Benutzer im Server-Verzeichnis `/etc/skel` auf dem SUSE LINUX School Server.)

Administration als Benutzer

Siehe Handbuch Seite: 167.

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

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

Achtung

Da das Zertifikat des SUSE LINUX School Server erst bei der Installation speziell für Ihre Schule ausgestellt wurde, kennt der Browser dieses Zertifikat natürlich nicht und gibt eine entsprechende Warnung aus.

Achtung

Nach der Anmeldung mit Ihrem Benutzernamen erreichen Sie einen Konfigurationsbereich, in dem Sie persönliche Einstellungen vornehmen können. Die einzelnen Menüpunkte werden in den folgenden Abschnitten erläutert.

...

Dateien verteilen und Dateien einsammeln

Siehe Handbuch Seite: 180

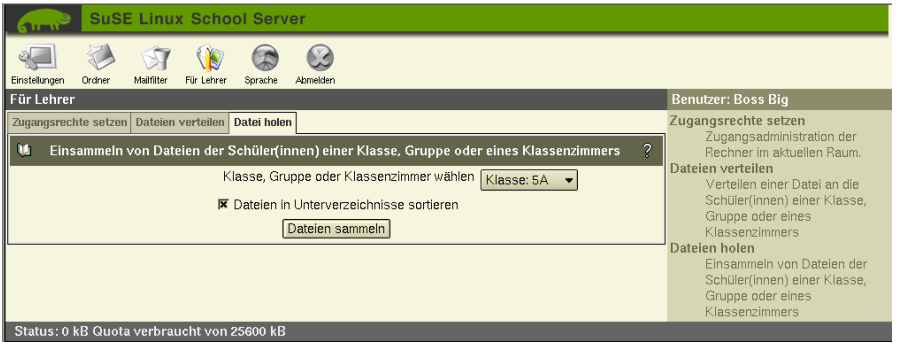


Abbildung A.2: *Dateien einsammeln*

Mit dem Menüpunkt 'Für Lehrer' → 'Datei holen' (siehe A.2) wird der Inhalt der Exportverzeichnisse der Schüler einer Klasse ins Importverzeichnis der Lehrkraft gelegt.

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

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

Angabe mehrerer Klassen beim Importieren von Listen

Wenn Sie während der Installation des SUSE LINUX School Servers die Homeverzeichnisse der Schüler nicht in Klassenverzeichnisse eingeordnet haben, können Sie beim automatischen Import über eine Datei – durch Leerzeichen getrennt – auch mehrere Klassen pro Schüler angeben. Bei Lehrern ist dies stehts der Fall.

Diese Angaben müssen allerdings den im SUSE LINUX School Server existierenden Klassen entsprechen!

So könnte eine Lehrerliste auch wie folgt aussehen:

```
NACHNAME:VORNAME:GEBURTSTAG:KLASSE:PASSWORT
Big:Boss:01.01.1961:ALL:system
Heidrich:Sieglinde:5.10.1969:7b 8b 9b:*
```

Datei 8:

- Lehrer Big Boss bekommt das Passwort „system“ und Rechte für alle Klassen.
- Lehrerin Sieglinde Heidrich bekommt ein zufällig generiertes Passwort und Rechte für die Klassen 7b, 8b und 9b.

Unterbrechungsfreie Stromversorgung (USV)

Schließen Sie die USV mit dem mitgelieferten Kabel an den ersten COM-Port des SUSE LINUX School Servers an und installieren Sie von der Installations-CD das Paket `apcupsd.rpm` über YaST2 → ‘Software installieren’.

Anschließend können Sie mit einem beliebigen Webbrowser die URL `https://admin/cgi-bin/multimon.cgi` aufrufen und sich über den Status Ihrer USV informieren.

Sollten Sie Anpassungen vornehmen müssen, editieren Sie bitte die Datei `/etc/apcupsd/apcupsd.conf`. Normalerweise ist das nicht nötig.

Tipp

Testen Sie die USV, indem Sie den Server ganz normal mit der Stromversorgung verbinden und nur das COM-Port-Kabel der USV eingesteckt lassen. Ziehen Sie dann im laufenden Betrieb das Stromkabel der USV ab und beobachten Sie die Meldungen auf der Kommandozeile und im Browserfenster.

Lassen Sie den Server wirklich herunterfahren und aktivieren Sie im Bios evtl. die Funktion für „Wake-On-Power-Failure“, um die korrekte Funktion aller Komponenten zu testen.

Schließen Sie zuletzt den Server wieder an die Stromversorgung der USV an und testen Sie noch einmal.

Tipp

Druckereinrichtung unter Windows 2000 und XP

Wenn Sie die am SUSE LINUX School Server eingerichteten Drucker unter Windows 2000 und Windows XP installieren möchten, müssen Sie folgendes beachten:

- Verwenden Sie für den lokalen Windowsadmin dasselbe Passwort wie für den Administrator des SUSE LINUX School Server oder geben Sie – angemeldet als lokaler Administrator – dem Administrator der Domäne auch lokal alle Administratorrechte.
- Melden Sie sich unter Windows als lokaler Administrator an und installieren Sie einen neuen Netzwerkdrucker. Wenn Sie dem Domänenadministrator entsprechende Rechte auf der lokalen Workstation gegeben habe, können Sie den Drucker natürlich auch installieren, wenn Sie als Domänenadmin angemeldet sind.

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 SUSE LINUX 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!

Hinweis

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. Am sichersten funktioniert dies, indem Sie den Server mit dem Befehl `telinit 1`in den Runlevel 1 herunterfahren und so die Daten auf eine andere Platte kopieren – dann gestaltet sich aber die Einbindung eines Backuprechner evtl. schwierig. Sie können deshalb auch nur einige wichtige Dienste kurzzeitig anhalten:

- `rcldap stop`
- `rccyrus stop`
- `rcpostfix stop`
- `rcsmbprint stop`
- `rcsmb stop`
- `rcnfsserver 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.

/etc-Verzeichnis Im Verzeichnis `/etc` befinden sich die Systemeinstellungen. Dieses Verzeichnis sollten Sie ebenso wie das Homeverzeichnis komplett kopieren.

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 Mailboxen 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 .`

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>`

Daten wiederherstellen

Um die Daten auf einem neuen System wieder einzuspielen, gehen Sie folgendermaßen vor:

Dienste abschalten Auch hier sollten Sie wieder den Server in den Runlevel 1 herunterfahren oder die betreffenden Dienste temporär abschalten.

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`.

SquidGuard

Das Programm SquidGuard wird am SUSE LINUX 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 SUSE LINUX School Server werden nicht alle diese Funktionalitäten genutzt. Eine Aufteilung nach Tageszeit oder gruppen- oder computerabhängige Zugriffsrechte findet nicht statt.

Nach einer Standardinstallation des SUSE LINUX 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 SUSE LINUX 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 SuSE 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

Die Firma SuSE stellt auf Ihrem FTP-Server aktuelle Filterlisten, sogenannte blacklists, zur Verfügung. Sie können mit dem Programmaufruf `/usr/bin/getlist-suse` diese Filterlisten auf Ihren Server herunterladen und installieren. Beachten Sie aber, dass Squid nach einem solchen Download neu gestartet wird und evtl. begonnene Downloads von Clients damit abgebrochen werden könnten.

Sie können diese Aktualisierung auch automatisieren, indem Sie in der Datei `/etc/crontab` den Eintrag
`0 2 * * 0 root /bin/bash /usr/bin/getlist-suse wait` mit einem Editor hinzufügen.

Externer LTSP-Terminalserver

Um neben dem SUSE LINUX 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 8.x oder 9.x installierter PC mit dem zusätzlichen Paket: Netzwerk/Server.
- Der Rechner ist am SUSE LINUX School Server angemeldet und erhält seine IP-Adresse über `DHCP`.
- Eingerichteter `LDAP- und NFS-Client` - wie unter 5 auf Seite 119 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.

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/`

folgende Pakete für Ihre Distribution in das Verzeichnis `/tmp/ltsp_tgz` (dieses müssen Sie evtl. vorher mit dem Befehl `mkdir -p /tmp/ltsp` erstellen) herunter: Paket `ltsp_core-3.0.9-i386.tgz`, Paket `ltsp_kernel-3.0.11-i386.tgz`, Paket `ltsp_x_core-3.0.4-i386.tgz` und Paket `ltsp_x_fonts-3.0.0-i386.tgz`.

Über ein Terminalfenster müssen die Pakete nun installiert werden. Machen Sie dazu bitte folgende Eingaben:

```
cd /tmp/ltsp
tar -xzf *.tgz

cd ltsp_core/
./install.sh
(Fragen mit y bzw. Return bestätigen)

cd ..
cd ltsp_kernel/
./install.sh

cd ..
cd ltsp_x_core/
./install.sh

cd ..
cd ltsp_x_fonts/
./install.sh

cd /opt/ltsp/templates
./ltsp_initialize

(die jeweiligen Fragen einfach
mit Return bzw. A bestätigen)
```

Datei 9: *Eingaben zur Installation des LTSP*

Die weitere Administration erfolgt über YaST2:

- 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

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.

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`

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 SUSE LINUX School Servers ist.)

[1] <IP >muss durch die vom SUSE LINUX School Server vergebene IP ersetzt werden.

Nach einem Neustart sollte der Terminalserver nun bald seinen Dienst aufnehmen können.

Einstellungen am SUSE LINUX School Server

Um einen zusätzlichen Terminalserver in Betrieb nehmen zu können, bedarf es einiger Änderungen am SUSE LINUX 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 SUSE LINUX School Servers negativ beeinflussen.

Hinweis

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 C.1 auf der nächsten Seite:

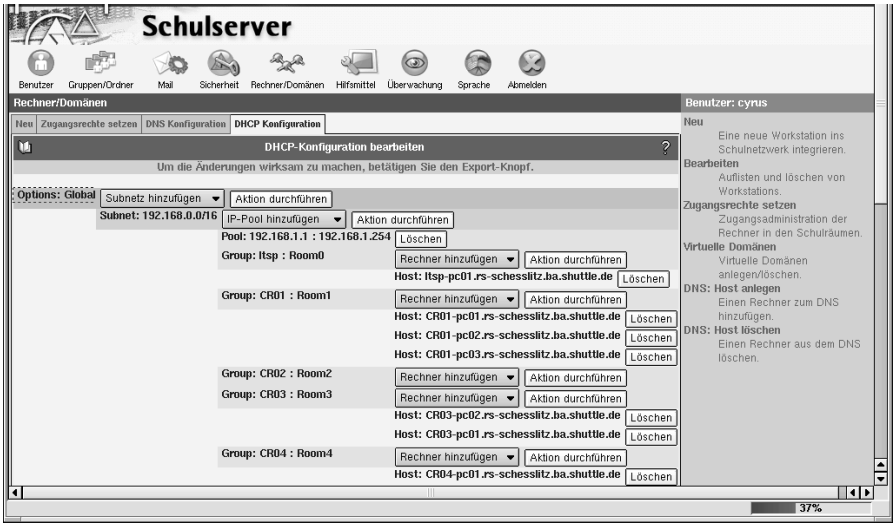


Abbildung C.1: *DHCP-Server-Einstellungen im Webfrontend*

`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.)

Dateien/Ordner kopieren

Im Abschnitt C auf Seite 234 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 SUSE LINUX 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 SUSE LINUX School Server kopiert werden.

Clients anmelden

Damit neue Clients booten können, müssen diese auch am SUSE LINUX School Server angemeldet werden – ohne Anmeldung gelangen die Clients sonst zwar in das pxe-Menü des SUSE LINUX 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.

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 10: *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 11: *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 12: *Xreset für kdm - Ergänzt um den Aufruf der Datei suicide*

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.

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.

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

Logfiles des Servers

Fast jeder Dienst, welcher auf dem SUSE LINUX 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 SUSE LINUX 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 SUSE LINUX 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 **??** auf Seite ??.

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.

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.

httpd/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.

httpd/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.

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 SUSE LINUX 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/squidGuard/logs/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/squidGuard/logs/blocked.log Wenn Sie die entsprechenden Veränderungen in der Konfigurationsdatei von SquidGuard vorgenommen haben (siehe Abschnitt *SquidGuard* auf Seite 229), so loggt SquidGuard jeden geblockten Aufruf einer Internetseite inkl. der Zeit, der IP-Adresse des Clients und des Namens des Benutzers hier mit.

Das SuSE Rettungssystem

Der SUSE LINUX 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.

Tipp

Legen Sie sich immer eine Boot- und Rettungsdiskette an, der geringe Aufwand für die Erzeugung und Pflege der Disketten steht in keinem Verhältnis zum Arbeitsaufwand und Zeitverlust, wenn Sie im Notfall keinen Zugriff auf Ihr System und auf das CD-ROM-Laufwerk haben.

Tipp

Vorbereitung

Für die Erstellung Ihres Rettungssystems benötigen Sie zwei fehlerfreie Disketten: eine als spätere Bootdiskette, die andere für das komprimierte Abbild eines kleinen Root–Dateisystems. Die Abbilddatei `bootdisk` für das Booten des Systems und die Datei `rescue` für das Root–Dateisystems finden Sie auf der ersten CD unter `boot`.

Es gibt drei Möglichkeiten, um die Diskette mit Root–Dateisystems anzulegen:

- mit YaST
- über eine Konsole mit den Linux–Befehlen

```
erde:~ #  /sbin/badblocks -v /dev/fd0 1440
erde:~ #  dd if=/media/cdrom/boot/rescue of=/dev/fd0 bs=18k
```

- über den DOS-Prompt Ihres Windows-Rechners (wobei `Q:` das CD-ROM-Laufwerk ist)

```
Q:\> cd \dosutils\rawrite
Q:\dosutils\rawrite> rawrite.exe
```

Die Rettungsdiskette basiert auf der libc5 (SuSE Linux 5.3), da es in dieser SuSE Linux–Version möglich ist, einige Programme wie z. B. fdisk oder e2fsck auf einer Diskette unterzubringen.

Hinweis

Die Rettungsdiskette lässt sich nicht mounten, da sie kein Dateisystem, sondern nur dessen komprimiertes Abbild enthält. Möchten Sie das Dateisystem einmal einsehen, dann lesen Sie nachfolgenden Absatz.

Hinweis

Wenn Sie das unkomprimierte Abbild einsehen möchten, müssen Sie die Abbilddatei dekomprimieren und dann als Benutzer `root` mounten. Unterstützt Ihr Linux-Kernel das *loop-Device*, geht der Vorgang wie folgt:

```
erde:~ #  cp /media/cdrom/boot/rescue /root/rescue.gz
erde:~ #  gunzip /root/rescue.gz
erde:~ #  mount -t ext2 -o loop /root/rescue /mnt
```

Das Rettungssystem starten

Das Rettungssystem wird von der selbst erstellten SuSE-Bootdiskette bzw. der bootbaren CD gestartet. Voraussetzung ist, dass das Disketten- bzw. CD-ROM/DVD-Laufwerk bootfähig ist; gegebenenfalls müssen Sie im CMOS-Setup die Boot-Reihenfolge ändern.

Nachfolgend die Schritte zum Starten des Rettungssystems:

1. Legen Sie die Bootdiskette (`bootdisk`) bzw. die erste CD oder DVD von SuSE Linux in das entsprechende Laufwerk ein und schalten Sie Ihr System ein.

2. Sie können entweder das System durchbooten lassen oder Sie wählen 'Rescue System' aus und können dann – falls notwendig – bei den 'boot options' Parameter angeben.

3. Nehmen Sie im linuxrc die erforderlichen Einstellungen für die Sprache und die Tastatur vor.

4. Wählen Sie im Hauptmenü den Punkt 'Installation/System starten'.

5. Wenn Sie mit der *Bootdiskette* gestartet haben, legen Sie nun die InstallationsCD oder die Diskette (`rescue`) mit dem komprimierten Abbild des Rettungssystems ein.

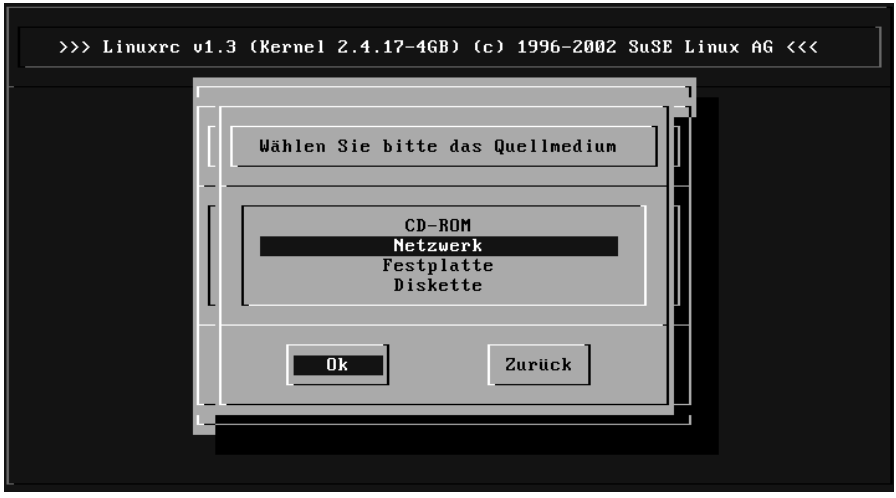


Abbildung E.1: *Quellmedium für das rescue-System*

6. Wählen Sie im Menü 'Installation/System starten' den Punkt 'Rettungssystem starten' und geben Sie dann das gewünschte Quellmedium an (s. Abb. E.1).

   Im Anschluss ein paar Hinweise zu den Auswahlmöglichkeiten:

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

   'Netzwerk' Um das `rescue`-System über eine Netzverbindung zu starten; der Treiber für die Netzwerkkarte muss zuvor geladen worden sein. In einem Untermenü stehen mehrere Protokolle zur Verfügung (s. Abb. E.2 auf der nächsten Seite): NFS, FTP, SMB etc.

Abbildung E.2: *Netzwerkprotokolle*

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

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

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

Das Rettungssystem benutzen

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

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

auch weitere Tools (grep, find, less etc.) wie auch das Programm telnet zu finden.

Zugriff auf das normale System

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

Nehmen wir als Beispiel einmal an, Ihr normales System setzt sich laut `/etc/fstab` wie in der Beispieldatei 13 beschrieben zusammen.

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

Datei 13: *Beispiel /etc/fstab*

Achtung

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

Achtung

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

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

Nun haben Sie Zugriff auf Ihr ganzes System und können z. B. Fehler in Konfigurationsdateien wie `/etc/fstab`, `/etc/passwd`, `/etc/inittab` beheben. Die Konfigurationsdateien befinden sich statt im Verzeichnis `/etc` jetzt im Verzeichnis `/mnt/etc`. Um selbst komplett verloren gegangene Partitionen mit dem Programm fdisk einfach wieder durch Neu-Anlegen zurückzugewinnen, sollten Sie sich einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls

```
erde:~ #  fdisk -l /dev/⟨disk⟩
```

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

Dateisysteme reparieren

Beschädigte Dateisysteme sind ein besonders ernster Anlass für den Griff zum Rettungssystem. Dateisysteme lassen sich grundsätzlich nicht im laufenden Betrieb reparieren. Bei schwereren Schäden lässt sich unter Umständen nicht einmal mehr das Root-Dateisystem mounten und der Systemstart endet in einer "kernel panic". Dann bleibt nur noch der Weg, die Reparatur „von außen“ unter einem Rettungssystem zu versuchen.

Im Rettungssystem des SUSE LINUX School Servers sind die Utilities e2fsck und dumpe2fs (zur Diagnose) enthalten. Damit beheben Sie die meisten Probleme.

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

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

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

Mit der Eingabe von

```
erde:~ #  e2fsck -p /dev/⟨Defekte_partition⟩
```

können Sie e2fsck dazu veranlassen, ein defektes Dateisystem automatisch zu reparieren – ohne dabei Sicherheitsabfragen an den Benutzer zu stellen. Sie sollten diese Funktion aber nur anwenden, wenn Sie wissen, was Sie da tun.

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 mittels `NIS` eingebundenen Nutzern oder 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 einmal 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 E auf Seite 251).
- Wechseln Sie anschließend in das gemountete Verzeichnis und bearbeiten Sie die Datei `shadow` mit dem `vi` (Eine Anleitung finden Sie im Anhang unter F auf Seite 255).
- 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.

Der Editor vi

Vorwort

Die in diesem Handbuch beschriebenen Möglichkeiten der Konfiguration des SUSE LINUX School Servers über das Web-Interface sollte Sie in nahezu allen Fällen in die Lage versetzen, alle für Sie relevanten Einstellungen und Optionen am System innerhalb einer übersichtlichen Administrationsumgebung durchzuführen. Die von Ihnen darin vorgenommenen Einstellungen werden automatisch in die betreffenden Konfigurationsdateien übernommen; die davon betroffenen Dienste werden bei Bedarf automatisch neu gestartet.

In einzelnen Fällen (wie z. B. bei sehr komplexen Konfigurationen) kann es jedoch sinnvoll sein, die entsprechenden Konfigurationsdateien direkt an einer Konsole des SUSE LINUX School Servers gemäß den geforderten Wünschen abzuändern. Um dies möglichst effizient und problemlos zu erreichen empfehlen wir Ihnen in einem solchen Fall die Verwendung des Editors vi, welcher sich auf nahezu jedem Unix ähnlichem Betriebssystem befindet.

Im folgendem Anhang geben wir Ihnen eine kurze Einführung in die Bedienung dieses Editors. Bitte gehen Sie jedoch bei allen Änderung am System sehr umsichtig vor und verändern Sie nur Optionen, von denen Sie genau wissen, dass Sie das von Ihnen gewünschte Ergebnis herbeiführen. Die Gefahr einer Fehlkonfiguration ist sehr groß; grundsätzlich sollten Sie immer zuerst die entsprechende Konfigurationsoption innerhalb des Web Interfaces verwenden.

Ferner können wir Ihnen auf Grund der damit möglichen weitreichenden Änderungen im Rahmen des Installationsupportes keine Unterstützung bei daraus eventuell resultierenden Problemen oder Fehlfunktionen des SUSE LINUX School Servers gewähren.

Bedienung des Editors vi

Die Bedienung des `vi` ist etwas gewöhnungsbedürftig. Er wird an dieser Stelle anderen Editoren vorgezogen, weil er zum einen auf jedem UNIX-ähnlichen Betriebssystem zur Verfügung steht und bei Linux zum standardmäßigen Installationsumfang gehört; zum anderen, weil seine Bedienung eindeutig ist und dadurch in der Regel keine Missverständnisse auftreten. Außerdem: wenn nichts geht, geht `vi`.

Die nun folgende Kurzanleitung sollte Sie in die Lage versetzen, mit Hilfe des `vi` z. B. diverse Konfigurationsdateien zu editieren.

Konzept: Der `vi` kennt 3 Betriebsarten (Modi):

- Befehlsmodus (engl. *command mode*)

  Jeder Tastendruck wird als Teil eines Befehls interpretiert.

- Einfügemodus (engl. *insert mode*)

  Tastendrucke werden als Texteingaben interpretiert.

- Komplexbefehlsmodus (engl. *last line mode*)

  Für komplexere Befehle, die in der letzten Zeile editiert werden.

Die wichtigsten Befehle des Befehlsmodus sind:

`i`	wechselt in den Eingabemodus (Zeichen werden an der aktuellen Cursorposition eingegeben).
`a`	wechselt in den Eingabemodus (Zeichen werden *nach* der aktuellen Cursorposition eingegeben).
`A`	wechselt in den Eingabemodus (Zeichen werden am Ende der Zeile angehängt).
`R`	wechselt in den Eingabemodus (überschreibt den alten Text).
`r`	wechselt zum Überschreiben *eines einzelnen* Zeichens in den Eingabemodus.
`s`	wechselt in den Eingabemodus (das Zeichen, auf dem der Cursor steht, wird durch die Eingabe überschrieben).
`C`	wechselt in den Eingabemodus (der Rest der Zeile wird durch den neuen Text ersetzt).
`o`	wechselt in den Eingabemodus (*nach* der aktuellen Zeile wird eine neue Zeile eingefügt).

Tabelle F.1: *Fortsetzung auf der nächsten Seite…*

`O`	wechselt in den Eingabemodus (*vor* der aktuellen Zeile wird eine neue Zeile eingefügt).
`x`	löscht das aktuelle Zeichen.
`dd`	löscht die aktuelle Zeile.
`dw`	löscht bis zum Ende des aktuellen Worts.
`cw`	wechselt in den Eingabemodus (der Rest des aktuellen Worts wird durch die Eingabe überschrieben).
`u`	nimmt den letzten Befehl zurück.
`J`	hängt die folgende Zeile an die aktuelle an.
`.`	wiederholt den letzten Befehl.
`:`	wechselt in den Komplexbefehlsmodus.

Tabelle F.1: *Einfache Befehle des Editors vi*

Allen Befehlen kann eine Zahl vorangestellt werden, die angibt, auf wieviele Objekte sich der folgende Befehl beziehen soll. So können durch Eingabe von `'3dw'` drei Wörter auf einmal gelöscht werden. Durch Eingabe von `'10x'` erreicht man das Löschen von zehn Zeichen ab der Cursorposition, `'20dd'` löscht 20 Zeilen.

Die wichtigsten Befehle des Komplexbefehlsmodus:

`:q!`	verlässt vi, ohne Änderungen zu speichern
`:w` ⟨*`dateiname`*⟩	speichert unter ⟨*dateiname*⟩
`:x`	speichert die geänderte Datei und verlässt den Editor
`:e` ⟨*`dateiname`*⟩	editiert (lädt) ⟨*dateiname*⟩
`:u`	nimmt den letzten Editierbefehl zurück

Tabelle F.2: *Komplexe Befehle des Editors vi*

Das Drücken der Taste (ESC) im Eingabemodus wechselt in den Befehlsmodus.

LDAP – Ein Verzeichnisdienst

LDAP (engl. *Lightweight Directory Access Protocol*) ist ein plattformunabhängiger Verzeichnisdienst, über den netzwerkweit wichtige Daten (wie z. B. Adressen, Telefonnummern oder auch Zugriffsberechtigungen) verwaltet und verteilt werden können.

Da der SUSE LINUX School Server LDAP für die Verwaltung und Administration einsetzt, möchten wir Ihnen in diesem Kapitel einen kurzen Überblick über die Funktionsweise und Hintergründe von LDAP geben.

Grundlagen zu LDAP

Innerhalb einer vernetzten Arbeitsumgebung ist es entscheidend, wichtige Informationen strukturiert und schnell abrufbar bereitzuhalten. Datenchaos droht nicht erst beim Benutzen des Internets. Ebenso schnell kann die Suche nach wichtigen Daten im betriebsinternen Netz ausarten: Was ist die Telefondurchwahl meines Kollegen XY? Wie lautet seine E-Mailadresse?

Dieses Problem löst ein Verzeichnisdienst, der ähnlich den Gelben Seiten (engl. *Yellow Pages*) im normalen Alltagsleben die gesuchten Informationen in gut strukturierter, schnell durchsuch- und abrufbarer Form bereithält.

Im Idealfall existiert ein zentraler Server, der die Daten in einem Verzeichnis vorhält und über ein bestimmtes Protokoll an alle Clients im Netzwerk verteilt. Die Daten sollten derart strukturiert sein, dass ein möglichst breites Spektrum von Anwendungen darauf zugreifen kann. So muss nicht jedes Kalendertool oder jeder E-Mailclient seine eigenen Datenbanken vorhalten, sondern kann auf den zentralen Bestand zurückgreifen. Dies verringert den Verwaltungsaufwand für die betreffenden Informationen beträchtlich. Die Verwendung eines offenen und standardisierten Protokolls wie LDAP stellt sicher, dass möglichst viele Clientapplikationen auf solche Informationen zugreifen können.

Ein Verzeichnis in diesem Kontext ist eine Art von Datenbank, die daraufhin optimiert ist, besonders gut und schnell les- und durchsuchbar zu sein:

- Um zahlreiche (gleichzeitige) Lesezugriffe zu ermöglichen, wird der Schreibzugriff auf einige wenige Aktualisierungen seitens des Administrators begrenzt. Herkömmliche Datenbanken sind daraufhin optimiert, in kurzer Zeit ein möglichst großes Datenvolumen aufzunehmen.

- Da Schreibzugriffe nur sehr eingeschränkt ausgeführt werden sollen, verwaltet man über einen Verzeichnisdienst möglichst unveränderliche, *statische* Informationen. Die Daten innerhalb einer konventionellen Datenbank ändern sich typischerweise sehr häufig (*dynamische* Daten). Telefonnummern in einem Mitarbeiterverzeichnis ändern sich nicht annähernd so häufig wie z. B. die Zahlen, die in der Buchhaltung verarbeitet werden.

- Werden statische Daten verwaltet, sind Updates der bestehenden Datensätze sehr selten. Bei der Arbeit mit dynamischen Daten, besonders wenn es um Datensätze wie Bankkonten und Buchhaltung geht, steht die Konsistenz der Daten im Vordergrund. Soll eine Summe an einer Stelle abgebucht werden, um sie an anderer Stelle hinzuzufügen, müssen beide Operationen gleichzeitig – innerhalb einer „Transaktion“ ausgeführt werden, um die Ausgeglichenheit des gesamten Datenbestandes sicherzustellen. Datenbanken unterstützen solche Transaktionen, Verzeichnisse nicht.

Kurzfristige Inkonsistenzen der Daten sind bei Verzeichnissen durchaus akzeptabel.

Das Design eines Verzeichnisdienstes wie LDAP ist nicht dazu ausgelegt, komplexe Update- oder Abfragemechanismen zu unterstützen. Alle auf diesen Dienst zugreifende Anwendungen sollen möglichst leicht und schnell Zugriff haben.

Verzeichnisdienste gab und gibt es, nicht nur in der Unix-Welt, viele. Novells NDS, Microsofts ADS, Banyans Street Talk und den OSI-Standard X.500.

LDAP war ursprünglich als eine schlanke Variante des DAP (engl. *Directory Access Protocol*) geplant, das für den Zugriff auf X.500 entwickelt wurde. Der X.500-Standard regelt die hierarchische Organisation von Verzeichniseinträgen.

LDAP ist um einige Funktionen des DAP erleichtert – wird deshalb manchmal scherzhaft auch als „X.500 lite“ bezeichnet – und kann plattformübergreifend und vor allem ressourcenschonend eingesetzt werden, ohne dass man auf die in X.500 definierten Eintragshierarchien verzichten müsste. Durch die Verwendung von TCP/IP ist es wesentlich einfacher, Schnittstellen zwischen aufsetzender Applikation und LDAP-Dienst zu realisieren.

Mittlerweile hat sich LDAP weiterentwickelt und kommt immer häufiger als Stand-alone-Lösung ohne X.500-Unterstützung zum Einsatz. Mit LDAPv3 (der Protokollversion, die Sie mit dem installierten Paket openldap2 vorliegen haben) unterstützt LDAP so genannte *Referrals*, mit deren Hilfe sich verteilte Datenbanken realisieren lassen. Ebenfalls neu ist die Nutzung von SASL (engl. *Simple Authentication and Security Layer*) als Authentifizerungs- und Sicherungsschicht.

LDAP kann nicht nur zur Datenabfrage von X.500-Servern eingesetzt werden, wie ursprünglich geplant war. Es gibt mit slapd einen Open Source Server, mit dem Objektinformationen in einer lokalen Datenbank gespeichert werden können. Ergänzt wird er durch slurpd, der für die Replikation mehrerer LDAP-Server zuständig ist.

Das Paket openldap2 besteht im Wesentlichen aus zwei Programmen.

slapd Ein Stand-alone-LDAPv3-Server, der Objektinformationen in einer BerkeleyDB-basierten Datenbank verwaltet.

slurpd Dieses Programm ermöglicht es, Änderungen an den Daten des lokalen LDAP-Servers an andere im Netz installierte LDAP-Server zu replizieren.

Zusätzliche Tools zur Systempflege `slapcat`, `slapadd`, `slapindex`

LDAP versus NIS

Traditionell verwendet der Unix-Systemadministrator zur Namensauflösung und Datenverteilung im Netzwerk den NIS-Dienst. Auf einem zentralen Server werden die Konfigurationsdaten aus den `/etc`-Dateien und Verzeichnissen `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` und `services` über die Clients im Netz verteilt. Als bloße Textdateien sind diese Dateien ohne größeren Aufwand wartbar. Allerdings wird die Verwaltung größerer Datenmengen aufgrund mangelnder Strukturierung schwierig. NIS ist nur für Unix-Plattformen ausgelegt, was einen Einsatz als zentrale Datenverwaltung im heterogenen Netz unmöglich macht.

Das Einsatzgebiet des LDAP-Dienstes ist im Gegensatz zu NIS nicht auf reine Unix-Netze beschränkt. Windows Server (ab 2000) unterstützen LDAP als Verzeichnisdienst. Ebenso bietet auch Novell einen LDAP-Dienst an. Zudem ist er nicht auf die oben genannten Aufgabengebiete beschränkt.

Das LDAP-Prinzip kann für beliebige Datenstrukturen verwendet werden, die zentral verwaltet werden sollen. Einige Anwendungsbeispiele wären zum Beispiel:

- Einsatz anstelle eines NIS-Servers
- Mailrouting (postfix, sendmail)
- Adressbücher für Mailclients wie Mozilla, Evolution, Outlook, ...
- Verwaltung von Zonenbeschreibungen für einen BIND9-Nameserver
- Verwalten von DHCP-Leases für einen DHCP-Server

Diese Aufzählung kann beliebig fortgesetzt werden, da LDAP im Gegensatz zu NIS erweiterbar ist. Die klar definierte hierarchische Struktur der Daten hilft bei der Verwaltung sehr großer Datenmengen, da sie besser durchsuchbar ist.

Aufbau eines LDAP-Verzeichnisbaums

Ein LDAP-Verzeichnis hat eine 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 wieder 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`.

An der Spitze der Verzeichnishierarchie liegt ein Wurzelelement `Root`. Diesem können in der nächsten Ebene entweder `c` (engl. *country*), `dc` (engl. *domainComponent*) oder `o` (engl. *organization*) untergeordnet werden.

Die Beziehungen innerhalb eines LDAP-Verzeichnisbaums werden am folgenden Beispiel (siehe Abbildung G.1) deutlich.

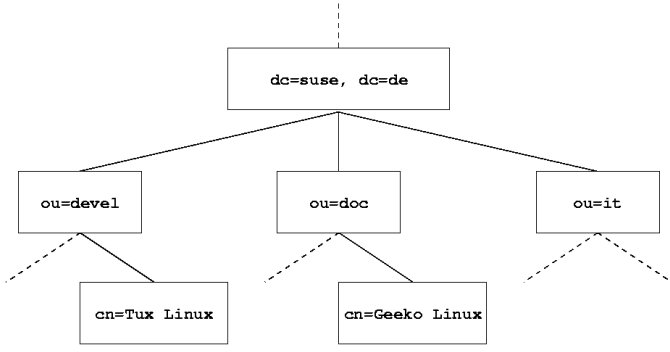


Abbildung G.1: *Aufbau eines LDAP-Verzeichnisses*

Die gesamte Abbildung umfasst einen fiktiven *Directory Information Tree*. Abgebildet sind die Einträge (engl. *entries*) auf drei Ebenen. Jeder Eintrag entspricht in der Abbildung einem Kästchen. Der vollständige gültige *Distinguished Name* für den fiktiven SuSE-Mitarbeiter `Geeko Linux` ist in diesem Fall `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Er setzt sich zusammen, indem der RDN `cn=Geeko Linux` zum DN des Vorgängereintrags `ou=doc,dc=suse,dc=de` hinzugefügt wird.

Die globale Festlegung, welche Typen von Objekten im DIT gespeichert werden sollen, geschieht über ein *Schema*. Der Typ eines Objekts wird durch die *Objektklasse* festgelegt. Die Objektklasse bestimmt, welche Attribute dem betreffenden

Objekt zugeordnet werden *müssen* bzw. *können*. Ein Schema muss demnach Definitionen aller Objektklassen und Attribute enthalten, die im gewünschten Einsatzszenario verwendet werden. Es existieren einige allgemein gebräuchliche Schemata (siehe RFC 2252 und 2256). Allerdings können auch benutzerdefinierte Schemata geschaffen werden oder mehrere Schemata ergänzend zueinander verwendet werden, wenn es die Umgebung erfordert, in der der LDAP-Server betrieben werden soll.

Tabelle G.1 gibt einen kleinen Überblick über die im Beispiel verwendeten Objektklassen aus `core.schema` und `inetorgperson.schema` samt zwingend erforderlicher Attribute und den passender Attributwerte.

Objektklasse	**Bedeutung**	**Beispieleintrag**	**erforderl. Attribute**
dcObject	*domainComponent* (Namensbestandteile der Domain)	suse	dc
organizationalUnit	*organizationalUnit* (Organisationseinheit)	doc	ou
inetOrgPerson	*inetOrgPerson* (Personenbezogene Daten für Intra-/Internet)	Geeko Linux	sn und cn

Tabelle G.1: *Häufig verwendete Objektklassen und Attribute*

In Ausgabe 1 sehen Sie einen beispielhaften Auszug aus einer Schema-Anweisung mit Erklärungen, der Ihnen beim Verstehen der Syntax neuer Schemata hilft.

```
...
#1 attributetype ( 2.5.4.11 NAME ( 'ou' 'organizationalUnitName' )
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )

...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5        DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7        MUST ou
#8        MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
```

```
                x121Address $ registeredAddress $ destinationIndicator $
                preferredDeliveryMethod $ telexNumber $
                teletexTerminalIdentifier $ telephoneNumber $
                internationaliSDNNumber $ facsimileTelephoneNumber $
                street $ postOfficeBox $ postalCode $ postalAddress
                $ physicalDeliveryOfficeName $ st $ l $ description) )
...
```

Ausgabe 1: *Auszug aus schema.core (Zeilennummerierung aus Verständnisgründen)*

Als Beispiel dient der Attributtyp `organizationalUnitName` und die zugehörige Objektklasse `organizationalUnit`. In Zeile 1 wird der Name des Attributs, sein eindeutiger OID (*Object Identifier*) (numerisch) sowie das Kürzel des Attributs gelistet. In Zeile 2 wird mit `DESC` eine kurze Beschreibung des Attributs eingeleitet. Hier ist auch der zugehörige RFC genannt, auf den die Definition zurückgeht. `SUP` in Zeile 3 weist auf einen übergeordneten Attributtyp hin, zu dem dieses Attribut gehört.

Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie bei der Attributsdefinition mit einem OID und dem Namen der Objektklasse. In Zeile 5 lesen Sie eine Kurzbeschreibung der Objektklasse. Zeile 6 mit dem Eintrag `SUP top` besagt, dass diese Objektklasse keine Unterklasse einer anderen Objektklasse ist. Zeile 7, beginnend mit `MUST`, führt alle Attributtypen auf, die zwingend in einem Objekt vom Typ `organizationalUnit` verwendet werden *müssen*. In Zeile 8 sind nach `MAY` alle Attributtypen gelistet, die in Zusammenhang mit dieser Objektklasse verwendet werden *können*.

Eine sehr gute Einführung in den Umgang mit Schemata finden Sie in der Dokumentation zu OpenLDAP in Ihrem installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

Serverkonfiguration mit slapd.conf

Ihr installiertes System enthält unter `/etc/openldap/slapd.conf` eine vollständige Konfigurationsdatei für Ihren LDAP-Server. Im Folgenden werden die einzelnen Einträge kurz beleuchtet und notwendige Anpassungen erklärt. Beachten Sie, dass Einträge mit führendem „#“ inaktiv sind. Um solche Einträge zu aktivieren, entfernen Sie dieses Kommentarzeichen.

Globale Anweisungen in slapd.conf

```
include /etc/openldap/schema/core.schema include
/etc/openldap/schema/inetorgperson.schema
```

Ausgabe 2: *slapd.conf: Include-Anweisung für Schemata*

Mit dieser ersten Anweisung in `slapd.conf` wird das Schema spezifiziert, nach dem Ihr LDAP-Verzeichnis organisiert ist (siehe Ausgabe 2 auf der vorherigen Seite). Der Eintrag `core.schema` ist zwingend erforderlich. Sollten Sie weitere Schemata benötigen, fügen Sie sie hinter dieser Anweisung ein (als Beispiel wurde hier `inetorgperson.schema` hinzugefügt). Weitere verfügbare Schemata finden Sie im Verzeichnis `/etc/openldap/schema/`. Soll NIS durch einen analogen LDAP-Dienst ersetzt werden, binden Sie hier das Schema `rfc2307bis.schema` ein. Informationen zu dieser Problematik entnehmen Sie der mitgelieferten OpenLDAP-Dokumentation.

```
pidfile /var/run/slapd.pid
argsfile /var/run/slapd.args
```

Ausgabe 3: *slapd.conf: pidfile und argsfile*

Diese zwei Dateien enthalten die PID (engl. *process id*) und einige Argumente, mit denen der slapd Prozess gestartet wird. An dieser Stelle ist keine Änderung erforderlich.

```
%
%

#
# Sample Access Control
#       Allow read access of root DSE
#       Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
#
access to dn="" by * read
access to *
       by self write
       by users read
       by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

Ausgabe 4: *slapd.conf: Zugangskontrolle*

Ausgabe 4 auf der vorherigen Seite ist der Ausschnitt aus `slapd.conf`, der die Zugangskontrolle zum LDAP-Verzeichnis auf dem Server regelt. Die Einstellungen, die hier im globalen Abschnitt der `slapd.conf` gemacht werden, gelten, soweit nicht im datenbankspezifischen Abschnitt eigene Zugangsregeln aufgestellt werden, die sie überschreiben. So wie hier wiedergegeben, können alle Benutzer lesend auf das Verzeichnis zugreifen, aber nur der Administrator (`rootdn`) kann auf diesem Verzeichnis schreiben. Das Regeln der Zugriffsrechte unter LDAP ist ein sehr komplexer Prozess. Daher hier einige Grundregeln, die Ihnen helfen, diesen Vorgang nachzuvollziehen.

- Jede Zugangsregel ist folgendermaßen aufgebaut:

```
access to <what> by <who> <access>
```

- ⟨*what*⟩ steht für das Objekt oder Attribut, zu dem Sie Zugang gewähren. Sie können einzelne Verzeichnisäste explizit durch separate Regeln schützen oder aber mit Hilfe regulärer Ausdrücke ganze Regionen des Verzeichnisbaums mit einer Regel abarbeiten. slapd wird alle Regeln in der Reihenfolge evaluieren, in der diese in der Konfigurationsdatei eingeführt wurden. Demnach führen Sie allgemeinere Regeln immer hinter spezifischeren auf. Die erste Regel, die slapd als zutreffend bewertet, wird ausgewertet und alle folgenden Einträge ignoriert.

- ⟨*who*⟩ legt fest, wer Zugriff auf die unter ⟨*what*⟩ festgelegten Bereiche erhalten soll. Auch hier können Sie durch die Verwendung passender regulärer Ausdrücke viel Aufwand sparen. Wiederum wird slapd nach dem ersten „Treffer“ mit der Auswertung von ⟨*what*⟩ abbrechen, d.h. spezifischere Regeln sollten wieder vor den allgemeineren aufgeführt werden. Folgende Einträge sind möglich (siehe Tabelle G.2):

Bezeichner	Bedeutung
*	ausnahmslos alle Benutzer
`anonymous`	nicht authentifizierte („anonyme“) Benutzer
`users`	authentifizierte Benutzer
`self`	Benutzer, die mit dem Zielobjekt verbunden sind
`dn=<regex>`	Alle Benutzer, auf die dieser reguläre Ausdruck zutrifft

Tabelle G.2: *Zugangsberechtigte Benutzergruppen*

- ⟨*access*⟩ spezifiziert die Art des Zugriffs. Es wird hier unterschieden zwischen den in Tabelle G.3 aufgeführten Möglichkeiten:

Bezeichner	Bedeutung
`none`	Zutritt verboten
`auth`	zur Kontaktaufnahme mit dem Server
`compare`	zum vergleichenden Zugriff auf Objekte
`search`	zur Anwendung von Suchfiltern
`read`	Leserecht
`write`	Schreibrecht

Tabelle G.3: *Zugriffsarten*

slapd vergleicht die vom Client angeforderte Berechtigung mit der in `slapd.conf` gewährten. Werden dort höhere oder gleiche Rechte gewährt als der Client anfordert, wird dem Client der Zugang erlaubt. Fordert der Client höhere Rechte als dort angegeben, erhält er keinen Zugang.

In Ausgabe 5 sehen Sie ein einfaches Beispiel für eine einfache Zugangskontrolle, die Sie durch Einsatz regulärer Ausdrücke beliebig ausgestalten können.

```
acess to dn.regex="ou=([^,]+),dc=suse,dc=de"
      by cn=administrator,ou=$1,dc=suse,dc=de write
      by user read
      by * none
```

Ausgabe 5: *slapd.conf: Beispiel für Zugangskontrolle*

Diese Regel besagt, dass zu allen `ou`-Einträgen nur der jeweilige Administrator schreibenden Zugang hat. Die übrigen authentifizierten Benutzer sind leseberechtigt und der Rest der Welt erhält keinen Zugang.

Tipp

Aufstellen von Access Regeln

Falls es keine `access to` Regel oder keine `by` ⟨*who*⟩ Anweisung greift, ist der Zugriff verboten. Nur explizit angegebene Zugriffsrechte werden gewährt. Für den Fall, dass keine einzige Regel aufgestellt wird, gilt das Standardprinzip: Schreibrecht für den Administrator und Leserecht für die übrige Welt.

Tipp

Detailinformationen und eine Beispielkonfiguration für LDAP-Zugriffsrechte finden Sie in der Online-Dokumentation des installierten openldap2-Pakets.

Neben der Möglichkeit, Zugriffskontrollen über die zentrale Serverkonfigurationsdatei (`slapd.conf`) zu verwalten, gibt es den Weg über ACIs (engl. *Access Control Information*). Mittels ACIs können die Zugangsinformationen zu einzelnen Objekten im LDAP-Baum selbst abgespeichert werden. Da diese Art der Zugangskontrolle noch nicht sehr verbreitet ist und von den Entwicklern als experimentell eingestuft wird, verweisen wir an dieser Stelle auf die entsprechende Dokumentation auf den Seiten des OpenLDAP-Projekts: `http://www.openldap.org/faq/data/cache/758.html`.

Datenbankspezifische Anweisungen in slapd.conf

```
database        ldbm
suffix          "dc=suse,dc=de"
rootdn          "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory       /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

Ausgabe 6: *slapd.conf: Datenbankspezifische Anweisungen*

In der ersten Zeile dieses Abschnitts (siehe Ausgabe 6) wird der Datenbanktyp festgelegt, hier LDBM. Über `suffix` in der zweiten Zeile wird festgelegt, für welchen Teil des LDAP-Verzeichnisbaumes dieser Server verantwortlich sein soll. Das folgende `rootdn` legt fest, wer Administratorzugriff auf diesen Server besitzt. Der hier angegebene Benutzer muss keinen LDAP-Eintrag besitzen oder als „normaler“ Benutzer existieren. Mit der `rootpw` Anweisung wird das Administratorpasswort gesetzt. Sie können hier statt `secret` auch den mit slappasswd erzeugten Hash des Administratorpassworts eintragen. Die `directory` Anweisung gibt das Verzeichnis an, in dem die Datenbankverzeichnisse auf dem Server abgelegt sind. Die letzte Anweisung, `index objectClass eq`, bewirkt, dass ein Index über die Objektklassen gepflegt wird. Ergänzen Sie hier unter Umständen einige Attribute, nach denen Ihrer Erfahrung nach am häufigsten gesucht wird. Wenn nachgestellt für die Datenbank eigene `Access` Regeln definiert werden, werden diese statt der globalen `Access` Regeln angewendet.

Start und Stopp des Servers

Ist der LDAP-Server fertig konfiguriert und sind alle gewünschten Einträge im LDAP-Verzeichnis nach dem unten beschriebenen Muster (siehe Abschnitt G) erfolgt, starten Sie den LDAP-Server als Benutzer `root` durch Eingabe des folgenden Befehls:

```
rcldap start
```

Möchten Sie den Server manuell wieder stoppen, geben Sie entsprechend `rcldap stop` ein. Die Statusabfrage über den Laufzustand des LDAP-Servers nehmen Sie mit `rcldap status` vor.

Um Start und Stopp des Servers beim Starten bzw. Herunterfahren des betreffenden Rechners zu automatisieren, nutzen Sie den YaST Runlevel-Editor oder Sie legen die entsprechenden Links der Start- und Stoppskripten mittels `insserv` auf der Kommandozeile selbst an.

Handhabung von Daten im LDAP-Verzeichnis

OpenLDAP gibt Ihnen als Administrator eine Reihe von Programmen an die Hand, mit denen Sie die Daten im LDAP-Verzeichnis verwalten können. Im Folgenden werden die vier wichtigsten von ihnen zum Hinzufügen, Löschen, Durchsuchen und Verändern des Datenbestandes kurz behandelt.

Daten in ein LDAP-Verzeichnis eintragen

Vorausgesetzt, die Konfiguration Ihres LDAP-Servers in `/etc/openldap/slapd.conf` ist korrekt und einsatzfähig, d.h. sie enthält die passenden Angaben für `suffix`, `directory`, `rootdn`, `rootpw` und `index`, können Sie nun mit der Aufnahme von Einträgen beginnen. OpenLDAP bietet hierfür den Befehl `ldapadd`.

Aus praktischen Gründen sollten Sie Objekte nach Möglichkeit gebündelt zur Datenbank hinzufügen. Zu diesem Zweck kennt LDAP das so genannte LDIF-Format (engl. *LDAP Data Interchange Format*). Eine LDIF-Datei ist eine einfache Textdatei, die aus beliebig vielen Attribut-Wert-Paaren bestehen kann. Für die zur Verfügung stehenden Objektklassen und Attribute schauen Sie in den in `slapd.conf` angegebenen Schemadateien nach. Die LDIF-Datei zum Anlegen eines groben Gerüsts für das Beispiel aus Abbildung G.1 auf Seite 263 sähe folgendermaßen aus (siehe Datei 14):

```
# Die Organisation SuSE
```

```
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SuSE AG
dc: suse

# Die Organisationseinheit Entwicklung (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# Die Organisationseinheit Dokumentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# Die Organisationseinheit Interne EDV (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Datei 14: *Beispiel für eine LDIF-Datei*

Hinweis

Kodierung der LDIF-Dateien

LDAP arbeitet mit UTF-8 (Unicode). Umlaute müssen demnach bei der Eingabe korrekt kodiert werden. Verwenden Sie einen Editor, der UTF-8 unterstützt (Kate oder neuere Versionen des Emacs). Andernfalls müssten Sie auf die Eingabe von Umlauten verzichten oder recode zum Umkodieren Ihrer Eingaben nach UTF-8 verwenden.

Hinweis

Speichern Sie die Datei unter `<datei>.ldif` ab und übergeben Sie sie mit folgendem Befehl an den Server:

```
ldapadd -x -D <dn des Administrators> -W -f <datei>.ldif
```

Die erste Option `-x` gibt an, dass in diesem Fall auf Authentifizierung über SASL verzichtet wird. `-D` kennzeichnet den Benutzer, der diese Operation vornimmt; hier geben Sie den gültigen DN des Administrators an, wie sie in `slapd.conf` konfiguriert wurde. Im konkreten Beispiel wäre dies `cn=admin,dc=suse,dc=de`. Mit `-W` umgehen Sie die Eingabe des Passworts

auf der Kommandozeile (Klartext) und aktivieren eine separate Passwortabfrage. Das betreffende Passwort wurde vorher in `slapd.conf` unter `rootpw` eingerichtet. `-f` übergibt die Datei. In Ausgabe 7 sehen Sie Aufruf von `ldapadd` im Detail.

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f beispiel.ldif
Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Ausgabe 7: *ldapadd von beispiel.ldif*

Die Benutzerdaten der einzelnen Mitarbeiter können Sie in separaten LDIF-Dateien angeben. Mit dem folgenden Beispiel `tux.ldif` (siehe Ausgabe 8) wird der Mitarbeiter `Tux` dem neuen LDAP-Verzeichnis hinzugefügt:

```
# Der Mitarbeiter Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Ausgabe 8: *LDIF-Datei für Tux*

Eine LDIF-Datei kann beliebig viele Objekte enthalten. Sie können ganze Verzeichnisbäume am Stück an den Server übergeben oder auch nur Teile davon wie zum Beispiel einzelne Objekte. Wenn Sie Ihre Daten relativ häufig ändern müssen, empfiehlt sich eine feine Stückelung in einzelne Objekte, da Ihnen dann das mühsame Suchen nach dem zu ändernden Objekt in einer großen Datei erspart bleibt.

Daten im LDAP-Verzeichnis ändern

Stehen in Ihrem Datensatz Änderungen an, verwenden Sie das Tool `ldapmodify`. Am einfachsten ändern Sie zuerst die betreffende LDIF-Datei und übergeben anschließend die geänderte Datei wieder an den LDAP-Server. Um

zum Beispiel die Telefonnummer des Mitarbeiters `Tux` von `+49 1234 567-8` auf `+49 1234 567-10` zu ändern, editieren Sie die LDIF-Datei wie in Ausgabe 9 gezeigt.

```
# Der Mitarbeiter Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Ausgabe 9: *Geänderte LDIF Datei tux.ldif*

Die geänderte Datei importieren Sie mit dem folgenden Befehl in das LDAP-Verzeichnis:

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Alternativ können Sie `ldapmodify` auch direkt die zu ändernden Attribute auf der Kommandozeile angeben. Hierbei gehen Sie wie folgt vor:

- Rufen Sie `ldapmodify` auf und geben Sie Ihr Passwort ein:

  ```
  ldapmodify -x -D cn=admin,dc=suse,dc=de -W
  Enter LDAP password:
  ```

- Geben Sie Ihre Änderungen nach der folgenden Syntax in genau dieser Reihenfolge an:

  ```
  dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
  changetype: modify
  replace: telephoneNumber
  telephoneNumber: +49 1234 567-10
  ```

Detaillierte Informationen zu `ldapmodify` und zur Syntax lesen Sie in der Manualpage von `ldapmodify` nach.

Daten aus einem LDAP-Verzeichnis suchen oder auslesen

OpenLDAP bietet mit `ldapsearch` ein Kommandozeilenwerkzeug zum Durchsuchen und Auslesen von Daten im LDAP-Verzeichnis. Ein einfaches Suchkommando hätte folgende Syntax:

```
ldapsearch -x -b "dc=suse,dc=de(objectClass=*)"
```

Die Option `-b` legt die Suchbasis, d.h. den Baumbereich, in dem gesucht werden soll, fest. In diesem Fall ist dies `dc=suse,dc=de`. Möchten Sie eine verfeinerte Suche auf bestimmten Unterbereichen des LDAP-Verzeichnisses ausführen

(z.B. nur über die Abteilung `devel`), übergeben Sie diesen Bereich mittels `-b` an `ldapsearch`. `-x` legt die Verwendung einfacher Authentifizierung fest. Mit `(objectClass=*)` legen Sie fest, dass Sie alle in Ihrem Verzeichnis enthaltenen Objekte auslesen wollen. Verwenden Sie dieses Kommando nach dem Aufbau eines neuen Verzeichnisbaumes, um zu überprüfen, ob alle Ihre Einträge korrekt übernommen wurden und der Server in der gewünschten Form antwortet. Weitere Informationen zum Gebrauch von `ldapsearch` finden Sie in entsprechenden Manualpage (`man ldapsearch`).

Daten aus einem LDAP-Verzeichnis löschen

Löschen Sie nicht mehr erwünschte Einträge mittels `ldapdelete`. Die Syntax ähnelt der der oben beschriebenen Kommandos. Um beispielsweise den Eintrag von `Tux Linux` im Ganzen zu löschen geben Sie folgendes Kommando ein:

```
ldapdelete -x -D "cn=admin,dc=suse,dc=deW cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

Weitere Informationen

Komplexere Themen wie die SASL-Konfiguration oder das Aufsetzen eines replizierenden LDAP-Servers, der sich die Arbeit mit mehreren „slaves“ teilt, wurden in diesem Kapitel bewusst ausgeklammert. Detaillierte Informationen zu beiden Themen finden Sie im *OpenLDAP 2.1 Administrator's Guide* (Links siehe unten).

Auf den Webseiten des OpenLDAP-Projekts stehen ausführliche Dokumentationen für Anfänger und fortgeschrittene LDAP-Benutzer bereit:

OpenLDAP Faq-O-Matic Eine sehr ergiebige Frage- und Antwortsammlung rund um Installation, Konfiguration und Benutzung von OpenLDAP. `http://www.openldap.org/faq/data/cache/1.html`.

Quick Start Guide Eine knappe Schritt-für-Schritt-Anleitung zum ersten eigenen LDAP-Server. `http://www.openldap.org/doc/admin21/quickstart.html` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`

OpenLDAP 2.1 Administrator's Guide Eine ausführliche Einführung in alle wichtigen Bereiche der LDAP-Konfiguration inkl. Access Controls und Verschlüsselung.

`http://www.openldap.org/doc/admin21/` oder im installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`

Weiterhin beschäftigen sich folgende Redbooks von IBM mit dem Thema LDAP:

Understanding LDAP Eine sehr ausführliche, allgemeine Einführung in die Grundprinzipien von LDAP.
`http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`

LDAP Implementation Cookbook Zielgruppe sind speziell Administratoren von *IBM SecureWay Directory*. Jedoch sind auch wichtige allgemeine Informationen zum Thema LDAP enthalten.
`http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf`

Gedruckte, englischsprachige Literatur zu LDAP:

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2. Aufl., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Ultimative Nachschlagewerke zum Thema LDAP sind die entsprechenden RFCs (engl. *Request for comments*) 2251 bis 2256.

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 SUSE LINUX 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 SUSE LINUX 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.

Dial on Demand
Diese Art der Einwahl in das Internet (Einwahl bei Bedarf) wird verwendet, wenn der SUSE LINUX School Server nicht über eine Standleitung an das Internet angebunden ist. Zum Versenden oder Abrufen von E-Mails wird automatisch eine Verbindung zum Provider aufgebaut.

DNS (engl. *Domain Name Service*)
siehe 'Nameserver', S. 279

Fetch Mail
Fetch Mail ist eine spezielle Funktion des SUSE LINUX School Server und nicht identisch mit dem ähnlich lautenden Paket `fetchmail`. Bei dem Abruf von E-Mails eines POP3- oder IMAP-Servers wird die Funktion Fetch Mail automatisch verwendet. Diese ist aber nur dann nötig, wenn der SUSE LINUX School Server nicht über eine vom Internet erreichbare IP-Nummer verfügt bzw. nicht über einen mx-Eintrag in fremden Nameservern bekannt ist.
Fetch Mail beherrscht das Multidropverfahren (s. Abschn. zu *Multidrop*).

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 SUSE LINUX School Server ist dies die primäre Gruppe `users`. Jeder Benutzer kann weiteren Gruppen angehören, die als sekundäre Gruppen bezeichnet werden.

IMAP (engl. *Internet Mail Access Protocol*)
IMAP ist zuständig für Zugriffe von Clients auf die Ordner des SUSE LINUX School Server. Die Daten (Mails) bleiben dabei zentral auf dem Server gespeichert. Dies ermöglicht die Verwendung von gemeinsamen Ordnern. Die TCP/IP Verbindung über IMAP findet auf Port `143` statt. Weitere Spezifikationen finden Sie u. a. in RFC 2060.

LDAP (engl. *Lightweight Directory Access Protocol*)
Der SUSE LINUX School Server verwendet eine Datenbank, um nahezu alle Benutzerinformationen zu speichern. Auf diese Datenbank wird mit-

tels 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/`

Mailingliste
siehe ‘Gruppen’, S. 278

Multidrop
Hierbei handelt es sich um ein Postfach (POP3, siehe S. 280), in dem die E-Mails einer gesamten Domain gespeichert werden. Die Mail wird von dort mittels POP3 abgeholt und auf dem Zielsystem verteilt.

Eine E-Mail besteht aus einem Umschlag (engl. *Envelope*), Kopf (engl. *Header*) und Körper (engl. *Body*). Der Umschlag wird während des Transportes von MTA (engl. *Mail Transfer Agent*) zu MTA generiert; vergleichbar mit dem Poststempel der Briefpost. Ist die Mail einmal abgelegt, ist der Umschlag verschwunden. Wird die Mail von einem Benutzer an einen anderen geschickt, ist dies kein Problem, sind jedoch Benutzer auf einer Mailingliste eingetragen, so lautet die Zieladresse `To:mailingliste@domain.de` für jeden Benutzer, an den diese Mail geht. Der eigentliche Empfänger wird dann während des Transportes mittels des SMTP-Kommandos `RCPT TO` übertragen. Nachdem die Mail am Zielserver angekommen ist, geht diese Information verloren. Nun nicht ganz, denn die Zieladresse hinterlässt „Spuren“ in Form von „Received:“-Zeilen im Mail-Header, aus denen der eigentliche Empfänger ermittelt werden kann. Da diese Informationen aber nicht genormt sind, jeder MTA diese Zeilen also anders schreibt, kann es immer wieder zu Fehlern bei der Mailzustellung kommen. Die Verwendung von Multidrop-Postfächer sollte aus diesem Grund vermieden werden.

Nameserver (DNS)
Ein Nameserver dient zum Auflösen von Rechnernamen in IP-Adressen und umgekehrt. Der SUSE LINUX 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 SUSE LINUX 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-Eintrag 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 und 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.

POP3 (engl. *Post Office Protocol*)

Dieses Protokoll dient dazu, um E-Mails von einem dafür eingerichteten Mailserver abzuholen. Dazu wird eine TCP/IP-Verbindung auf Port `110` mit dem Server aufgebaut und mit einfachen Kommandos wie `HELO`, `USER`, `PASS` usw. der Datentransfer geregelt.

Der SUSE LINUX School Server ist standardmäßig für POP3 eingerichtet, so dass ein Client E-Mails über dieses Protokoll abholen kann. Auch Fetch Mail (siehe S. 278) kann POP3 verwenden, um Mails von anderen Server (Provider) abzuholen. Weitere Beschreibung finden Sie in RFC 1939 (siehe S. 281).

Postfix

Postfix ist ein MTA (engl. *Mail Transfer Agent*). Die komplette Dokumentation zu Postfix, einschließlich einer Frage- und Antwortliste (FAQ), finden Sie unter `http://www.postfix.org/`.

Aus Sicherheitsgründen laufen Teile von postfix auf dem SUSE LINUX School Server in einer `changeroot`-Umgebung unter `/var/spool/postfix/`. Bei manuellen Änderungen an Konfigurationsdateien unter `/etc/`, müssen diese nach `/var/spool/postfix/etc/` übernommen werden. Starten Sie dazu SuSEconfig.

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 ist bei 200 Benutzer mit durchschnittlich 5 MB Platzbedarf der Speicherplatzbedarf der Festplatte bereits 1000 MB.

Relayhost
Ist ein „direktes“ Verschicken von Mails in das Internet nicht möglich, muss ein Relayhost angeben werden. Dieser ist ein Rechner Ihres Providers, der Mails an externe Adressen via SMTP (siehe S. 281) annimmt und weiterleitet. Die Angabe eines Relayhosts ist notwendig, wenn eine Dial-up-Verbindung zum Internet benutzt wird (keine feste IP-Adresse für den Server).
Den für Sie erreichbaren Relayhost erfahren Sie von Ihrem Provider.

RFC (engl. *Requests For Comments*)
RFCs beschreiben Protokolle und legen zum Teil auch Standards fest. Sie finden eine Auflistung aller RFCs unter `http://the.rfceditor.org/`.

SASL (engl. *Simple Authentication and Security Layer*)
Weitere Informationen zur Authentifizierung von Mailclients gegenüber dem Server finden Sie in der Manpage `man sasl` sowie der RFC 2222.

SIEVE (engl. *Sieb*)
Diese „genormte“ Sprache dient der Erstellung von Mailfiltern.

Mit dem SIEVE-Editor können Sie eigene Filter-Skripte erstellen oder existierende Skripte einfügen. Eine Beschreibung zur Skriptsprache finden Sie in der RFC 3028 oder unter `http://www.cyrusoft.com/sieve/`.

SMTP (engl. *Simple Mail Transport Protocol*)
Über SMTP werden Mails an den SUSE LINUX School Server gesendet, der wiederum SMTP verwendet, um Mails an andere Mailserver im Internet (Relayhost) zu senden. Dazu wird eine TCP/IP-Verbindung auf Port `25` verwendet.
Eine genaue Beschreibung finden Sie in der RFC 2821.

SSL (engl. *Secure Socket Layer*)
siehe ‘TLS’, S. 281

TLS (engl. *Transport Layer Security*)
TLS dient zur Verschlüsselung der zu übertragenden Daten.
Eine eingehende Beschreibung finden Sie in RFC 2246.

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.

UUCP (engl. *Unix to Unix CoPy*)
Hierbei handelt es sich um ein Protokoll zur Übertragung von Dateien zwischen verschiedenen Computern, insbesondere solchen mit dem Betriebssystem Unix, über große Entfernungen. Die Verbindung zwischen den Computern wird dabei nur bei Bedarf oder in regelmäßigen Abständen aufgebaut.

UUCP wird beim SUSE LINUX School Server bei Bedarf zur Übermittlung von E-Mail und News eingesetzt.

Zertifikat
Ein Zertifikat ist der „Personalausweis“ für einen Benutzer, der ihm gestattet, bestimmte Dienste auf dem SUSE LINUX 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. 277)

YaST und SuSE Linux Lizenzbestimmungen

Gegenstand dieser Lizenz ist das Programm YaST2 (engl. *Yet another Setup Tool 2*), der Name „YaST“ sowie SuSE Linux, die Linux-Distribution der SuSE Linux AG., alle aus YaST2 abgeleiteten Programme und alle auf YaST2 vollständig oder auszugsweise abgeleiteten Werke oder Namen sowie die Benutzung, Verwendung, Archivierung, Vervielfältigung und Weitergabe von YaST2, aller aus YaST2 abgeleiteten Programme und alle vollständig oder auszugsweise abgeleiteten Werke. Das Programm YaST2 mit allen Quellen ist im Sinne des Urheberrechts geistiges Eigentum der SuSE Linux AG. Der Name YaST ist ein eingetragenes Warenzeichen der SuSE Linux AG. Im folgenden tritt die SuSE Linux AG als Lizenzgeber auf, und jeder Benutzer oder Bearbeiter von YaST2 oder daraus vollständig oder auszugsweise abgeleiteten Werke sowie jede Person, die YaST2 oder SuSE Linux archiviert, vervielfältigt und verbreitet, ist Lizenznehmer der SuSE Linux AG.

Durch die Bearbeitung, Benutzung, Verwendung, Archivierung, Vervielfältigung und Weitergabe von YaST2 werden die folgenden Lizenzbestimmungen anerkannt.

Nur diese Lizenz gibt dem Lizenznehmer das Recht, YaST2 oder daraus abgeleitete Werke zu benutzen, zu vervielfältigen, zu verteilen oder zu verändern. Diese Handlungen sind durch das Urheberrecht untersagt, wenn diese Lizenz nicht anerkannt wird. Wird diese Lizenz im ganzen anerkannt und befolgt, ist sie auch ohne schriftliche Zustimmung des Lizenznehmers gültig.

1. Benutzung

   YaST2 und SuSE Linux dürfen für private und kommerzielle Zwecke unter Beachtung der Urheberrechte und Lizenzbestimmungen der installierten Pakete und Programme genutzt werden. Die Benutzung von YaST2, auch bei Verwendung einer modifizierten Version, befreit insbesondere den Lizenznehmer *nicht* von der gebotenen Sorgfaltspflicht gegenüber den Lizenzbestimmungen der durch YaST2 oder darauf basierenden Werken installierten Pakete und Programme.

2. Bearbeitung

   Alle aus YaST2 abgeleiteten Programme und alle vollständig oder auszugsweise abgeleiteten Werke sind auf dem Eröffnungsbildschirm mit dem eindeutigen Hinweis *Modifizierte Version* zu versehen. Des Weiteren hat der Bearbeiter seinen Namen, einen Hinweis, dass die SuSE Linux AG für die *Modifizierten Version* keinen Support leistet und den Ausschluss jedweder Haftung auf dem Eröffnungsbildschirm anzugeben. Als *Modifizierte Version* gilt jede Änderung in den Quellen, die nicht von der SuSE Linux AG durchgeführt wird. Der Lizenznehmer hat das Recht, seine Kopie der Quellen von YaST2 zu verändern, wodurch ein auf dem Programm YaST2 basierendes Werk entsteht, vorausgesetzt, dass die folgenden Bedingungen erfüllt sind:

   (a) Jede Änderung muss in den Quellen mit Datum und Bearbeiter vermerkt sein. Die veränderten Quellen müssen nach Abschnitt 3, zusammen mit dieser unveränderten Lizenz, dem Benutzer zu Verfügung gestellt werden.

   (b) Der Lizenznehmer ist verpflichtet, dass jede von ihm verbreitete Arbeit, die ganz oder teilweise von YaST2 oder Teilen von YaST2 abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.

   (c) Die Änderung dieser Lizenz durch einen Lizenznehmer, auch nur teilweise, ist untersagt.

   Die SuSE Linux AG behält sich das Recht vor, unentgeltlich Teile oder alle Änderungen einer modifizierten Version von YaST2 in die offizielle Version von YaST2 aufzunehmen. Der Lizenznehmer hat darauf keinen Einfluss.

3. Weitergabe

   Es ist untersagt, ohne vorherige schriftliche Genehmigung der SuSE Linux AG YaST2 oder SuSE Linux gegen Entgelt zu vervielfältigen oder unberechtigt vervielfältigte Datenträger zu verbreiten. Die Verteilung gegen

Entgelt des Programms YaST2, dessen Quellen, ob vollständig oder teilweise verändert oder unverändert, und der daraus abgeleiteten Werke bedürfen der vorherigen schriftlichen Zustimmung der SuSE Linux AG.

Alle aus YaST2 abgeleiteten Programme und alle vollständig oder auszugsweise abgeleiteten Werke dürfen nach 2b nur mit den veränderten Quellen und dieser Lizenz weitergegeben werden. Die kostenfreie Bereitstellung von YaST2 oder daraus abgeleiteten Werken zusammen mit SuSE Linux auf FTP-Servern und Mailboxen ist unter Beachtung der Lizenzen der Software gestattet.

4. Gewährleistung

   Für YaST2 oder daraus abgeleitete Werke und SuSE Linux ist jegliche Gewährleistung ausgeschlossen. Die Gewährleistung der SuSE Linux AG erstreckt sich nur auf fehlerfreie Datenträger.

   Die SuSE Linux AG stellt YaST2 und SuSE Linux so zur Verfügung, „WIE ES IST“, ohne jedwede Gewährleistung, ohne die Tauglichkeit für einen bestimmten Zweck oder die Verwendbarkeit zu garantieren. Insbesondere haftet SuSE nicht für entgangenen Gewinn, ausgebliebene Einsparungen oder Schäden aus Ansprüchen Dritter gegenüber dem Lizenznehmer. Die SuSE Linux AG haftet auch nicht für sonstige mittelbare oder unmittelbare Folgeschäden, insbesondere nicht für den Verlust oder die Erstellung aufgezeichneter Daten.

   Die Beachtung der jeweiligen Lizenzen und Urheberrechte der installierten Software obliegt allein dem Benutzer von YaST2 und SuSE Linux.

5. Rechte

   Es werden keine weiteren Rechte an YaST2 oder an SuSE Linux als die in dieser Lizenz behandelten eingeräumt. Ein Verstoß gegen diese Lizenz beendet automatisch die Rechte des Lizenznehmers. Jedoch werden die Rechte Dritter, die vom Lizenznehmer Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese Lizenz in allen Teilen anerkannt und befolgt wird. Falls dem Lizenznehmer aufgrund eines Gerichtsurteils, Patentbestimmungen, Lizenzbestimmungen oder aus einem anderen Grund Bedingungen oder Verpflichtungen auferlegt werden, die dieser Lizenz ganz oder in Teilen widersprechen, so wird der Lizenznehmer ausdrücklich nur mit vorheriger schriftlicher Zustimmung der SuSE Linux AG von dieser Lizenz und ihren Bedingungen ganz oder teilweise befreit. Es ist das Recht der SuSE Linux AG, diese Zustimmung ohne Angabe von Gründen zu verweigern.

6. Weitere Einschränkungen

Wenn die Verbreitung oder Benutzung von YaST2 und SuSE Linux oder Teilen von SuSE Linux in einem Staat entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann die SuSE Linux AG eine explizite geographische Begrenzung der Verbreitung von YaST2 und SuSE Linux oder Teilen von SuSE Linux angeben, mit der diese Staaten ganz oder teilweise von der Verbreitung ausgeschlossen werden. In einem solchen Fall beinhaltet diese Lizenz die ganze oder teilweise Beschränkung, als wäre sie in dieser Lizenz niedergeschrieben.

Merkzettel

Supportinformationen

Hier finden Sie noch einmal alle Angaben, die Sie vor der Kontaktaufnahme mit unserem Support bereithalten sollten. Damit Probleme möglichst schnell geklärt werden können, sollte sich der Server (und ein Client) in Ihrer Reichweite befinden.

VORNAME:	
NAME:	
FIRMA:	
STRASSE:	
LAND:	
PLZ:	
ORT:	
REGCODE: (Produktregistrierungscode)	
EMAIL:	

Hardwareinformationen

Versuchen Sie hier möglichst umfangreiche Angaben zur Hardware des Servers zu sammeln.

Prozessor(en)/ Taktfrequenz:		Grafikkarte:	
Mainboard:		Arbeitsspeicher (RAM):	
SCSI- oder Raid-Controller	Hersteller, Serie	Treiber	
Festplatte(n)	Hersteller, Serie		
CD-ROM	Hersteller, Serie:		
Netzwerkkarte eth0	Hersteller, Treiber	Subnetz bzw. DSL	MAC-Adr.
Netzwerkkarte eth1	Hersteller, Treiber	Subnetz bzw. DSL	MAC-Adr.
Netzwerkkarte eth2	Hersteller, Treiber	Subnetz bzw. DSL	MAC-Adr.
ISDN-Karte	Hersteller, Treiber		

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

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`		
`Schuladmin`	`admin`		
`Mailserver`	`mailadmin`		

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

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)

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

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:

Index

D

E

F

G

I

K

L