Inhalt

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 5 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 6 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

1 Apache und Samba

Mit Apache und Samba stehen unter Mac OS X zwei leistungsfähige Server zur Verfügung. Dieses Extra-Kapitel bietet Ihnen Anleitung zur detaillierten Konfiguration.

1.1 Der Webserver Apache

Jeder Rechner ein Webserver

Mac OS X bringt von Haus aus den populärsten Webserver mit: Apache. Apache ist das wohl populärste Programm aus dem Open Source-Bereich und sein Name deutet schon auf seine Herkunft hin. Es stammt nicht, wie vielleicht das Logo mit der Feder vermuten lässt, von einem nordamerikanischen Indianerstamm. Im Laufe der Weiterentwicklung des freigegebenen NCSA-Servers wurden immer mehr Korrekturen und Erweiterungen, so genannte Patches, eingearbeitet.

Nicht nur zum Testen

Die Einrichtung eines Webservers auch im lokalen Netzwerk, ohne gleich eine Domain mit diesem zu betreiben, kann sich dennoch lohnen. Wenn Sie als Web-Designer arbeiten, können Sie in einer geschützten Umgebung Programme testen und entwickeln, ohne Gefahr zu laufen, bei einem Server eines Dienstleisters Schaden anzurichten. Außerdem gibt es mittlerweile einige ernst zu nehmende Programme wie eGroupWare, die Ihnen bei der Büroorganisation gute Dienste leisten können.

1.1.1 Grundlegende Konfiguration

Start über Systemeinstellungen

Sie können den Webserver starten, indem Sie in den Systemeinstellungen im Feld **Sharing** den Dienst **Personal Web Sharing** aktivieren. Der Daemon `httpd`, der den eigentlichen Webserver darstellt, wartet nun auf Verbindungsanfragen am Port 80. Sind Sie mit dem Internet verbunden, so führt die Eingabe von http:// gefolgt von Ihrer IP-Nummer zum Aufruf der Webseite. Welche IP-Nummer Ihnen gerade zugewiesen ist, wird unten im Fenster der Systemeinstellungen angegeben. Aber auch wenn Sie nicht mit dem Internet verbunden sind, steht Ihnen der Webserver unter der Adresse http://127.0.0.1 oder http://localhost zur Verfügung. Wenn Sie diese Seite aufrufen, finden Sie auf der dargestellten Webseite einen kleinen Link auf die vollständige Dokumentation des Webservers. Diese wird mit dem Betriebssystem installiert und kann eine wertvolle Hilfe sein, um Funktionen nachzuschlagen und Fehler auszuwerten.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 7 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Abbildung 1.1 Die Beispielseite des Webservers

Restriktive Einstellungen

Solange Sie die Einstellungen des Webservers nicht ändern, werden nur einfache HTML-Dateien und Bilder angezeigt. CGI-Skripte oder Zugriffe auf eine Datenbank finden noch nicht statt. Die Konfigurationsdateien für den Webserver liegen im Verzeichnis **/etc/httpd**. Die Einstellungen werden in der Datei **httpd.conf** vorgenommen. In der Dokumentation von Apache werden die einzelnen Vorgaben auch als Direktiven, also Anweisungen an den Server bezeichnet. Sie finden in dem Verzeichnis ferner eine Datei **httpd.conf.default**. Diese ist eine Sicherheitskopie für den Fall, dass eine Fehlkonfiguration den Server lahm legt und die Ermittlung des Fehlers schwierig ist. Mit dieser Datei können Sie den ursprünglichen Zustand wiederherstellen.

Neustart notwendig

Damit die Änderungen an der Datei **httpd.conf** wirksam werden, muss der Webserver neu gestartet werden. Die Methode mit `kill -SIGHUP` ist nicht empfehlenswert. Der Apache bringt sein eigenes Skript zum Starten und Beenden mit. Dies wird von dem StartupItem **Web Server** angesprochen. Sie können sich daher zum Neustart des Webservers des Programms `SystemStarter` bedienen. Mit der Eingabe

```
sudo SystemStarter restart Web\ Server
```

starten Sie den Server neu. Liegt in der Datei **httpd.conf** kein Fehler vor, so lautet die Ausgabe:

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 8 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

```
Restarting Apache web server
/usr/sbin/apachectl restart: httpd restarted
Startup complete.
```

Das Skript `apachectl` dient zum Neustart des Servers. Wenn die Datei **httpd.conf** fehlerhaft ist, erhalten Sie an dieser Stelle eine Fehlermeldung und das Programm `httpd` bricht den Startvorgang ab.

Pfadangaben zu den Dateien

Die meisten Einstellungen in der Datei **httpd.conf** müssen und sollten Sie nicht ändern. Dass der Apache mit PID-Dateien arbeitet und wo diese liegen, ist für den normalen Betrieb unerheblich. Ebenso können Sie Einstellungen wie `timeout` und `KeepAlive` mit den erprobten Standardwerten belassen. Welche Dateien der Webserver bei einem Aufruf darstellt, wird in der Angabe `DocumentRoot` festgelegt. In den normalen Einstellungen wird hier das Verzeichnis **/Library/WebServer/Documents** genutzt. Wenn Sie sich dessen Inhalt anschauen, finden Sie dort mehrere Dokumente, die mit der Bezeichnung index.html besitzen. Als Dateikennung findet sich ein Kürzel, das für die entsprechende Sprachversion steht. Die Datei **index.html.de** enthält die Datei, die in Abbildung 1.1 angezeigt wird. Wäre im Browser eine andere Sprache als Standard festgelegt worden, würde die Anzeige in der jeweiligen Lokalisierung erfolgen. Der Webserver ist zu diesem Verhalten in der Lage, da er über ein Erweiterungsmodul verfügt, das die zu verwendende Sprache mit dem Browser des Benutzers aushandeln kann. Wenn Sie anstatt **/Library/WebServer/Documents** ein anderes Verzeichnis für Ihre Dateien verwenden möchten, können Sie den Pfad ändern und den Server neu starten.

1.1.2 Die Protokolle und ihr Format

Fehler- und Zugriffsprotokoll

Jeder Zugriff auf den Webserver wird von diesem protokolliert. Genau genommen erfolgt dies in zwei unterschiedlichen Dateien. Die Datei **error_log** im Verzeichnis **/var/log/httpd** enthält alle Fehlermeldungen des Servers in Bezug auf nicht gefundene Dateien oder fehlerhafte CGI-Skripte. Die Datei **access_log** im gleichen Verzeichnis protokolliert alle Seitenabrufe. Die Form dieses Protokolls, das innerhalb der Datei **httpd.conf** als `CustomLog` bezeichnet wird, können Sie mit der Angabe `LogFormat` festlegen. Es sind bereits vier Formen (`combined`, `common`, `referrer` und `agent`) vordefiniert worden. Während die Formate `referrer` und `agent` lediglich die herleitenden Links beziehungsweise den verwendeten Browser protokollieren, geben die Formate `combined` und `common` umfangreich Aufschluss über die Herkunft der Besucher, die ab-

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 9 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

gerufenen Seiten, die Verweildauer und den verwendeten Browser. In der Voreinstellung wird aufgrund der Zeile

```
CustomLog "/private/var/log/httpd/access_log"common
```

das Format `common` verwendet. Dies hat den Vorteil, dass die erzeugten Protokolle von einem Programm wie Webalizer ohne weitere Einstellungen statistisch aufbereitet werden können, da das Format `common` de facto ein Standard ist. Die Vorgaben der einzutragenden Daten werden in dem Bereich zwischen den Anführungszeichen definiert. Die Angabe

```
"%h %l %u %t \"%r\" %>s %b"
```

protokolliert sowohl die IP-Nummer `%h` des Besuchers, den Zeitpunkt des Abrufes `%t` als auch die aufgerufene Datei `\"%r\"` sowie den Status Code des Abrufs. Sie können sich anhand der mitgelieferten Dokumentation Ihr eigenes Format erstellen, indem Sie die entsprechenden Platzhalter wie `%t` an die gewünschte Stelle setzen, Ihrem Format einen Namen geben und mit der Direktive `CustomLog` zuweisen.

Verschiedene Codes

Jeder Abruf erhält einen Status Code zugewiesen. Eine Übersicht der am meisten verwendeten können Sie Tabelle 1.1 entnehmen. Diese Codes werden in der Protkolldatei an der Stelle `%>s` notiert. Sie sind ein wichtiges Hilfsmittel, um Fehler zu finden oder den Besucher auf eine spezielle Seite umzuleiten.

Wert	Bedeutung
200	OK – Die angeforderte Datei konnte ohne Probleme abgerufen werden.
304	Not Modified – Die angeforderte Datei wurde seit dem letzten Zugriff des Besuchers nicht verändert und wird nicht erneut übertragen.
400	Bad Request – Der Webserver konnte die Anforderung nicht interpretieren.
403	Forbidden – Dem Besucher fehlen die Zugriffsrechte, um die Datei aufzurufen.
404	Not Found – Die angeforderte Datei existiert nicht.
500	Internal Server Error – Es liegt ein Fehler in der Konfiguration des Webservers vor. Dies kann aus einer fehlerhaften Konfigurationsdatei rühren oder ein CGI-Skript arbeitet nicht korrekt.

Tabelle 1.1 Status Codes des Webservers

1.1.3 Auswertung mit dem Webalizer

Erfolgskontrolle im WWW

Bei einer Webseite geben die Protokolle detaillierten Aufschluss über die Zugriffszahlen, woher die Besucher gekommen sind und welche Seiten sie

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 10 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

abgerufen haben. Das Programm Webalizer wertet diese Protokolle grafisch aus und erstellt Statistiken, die Ihnen schnell Informationen liefern, wie erfolgreich Ihre Webseite ist. Sie können Webalizer per Hand installieren, indem Sie das Programm `webalizer` in ein Verzeichnis, zum Beispiel **/usr/bin** oder **/opt/local/bin**, kopieren, das Sie in Ihrer `PATH`-Variable eingetragen haben. Ferner finden Sie im heruntergeladenen Archiv eine Datei **sample.conf** die Sie ins Verzeichnis **/etc** mit dem Namen **webalizer.conf** kopieren können. In dieser werden die generellen Einstellungen des Programms vorgenommen. Stehen Ihnen die Protokolle Ihrer Webseite zur Verfügung, wenn Sie zum Beispiel über eine eigene Domain oder gar einen eigenen Server verfügen, dann können Sie diese auf Ihren Rechner herunterladen.

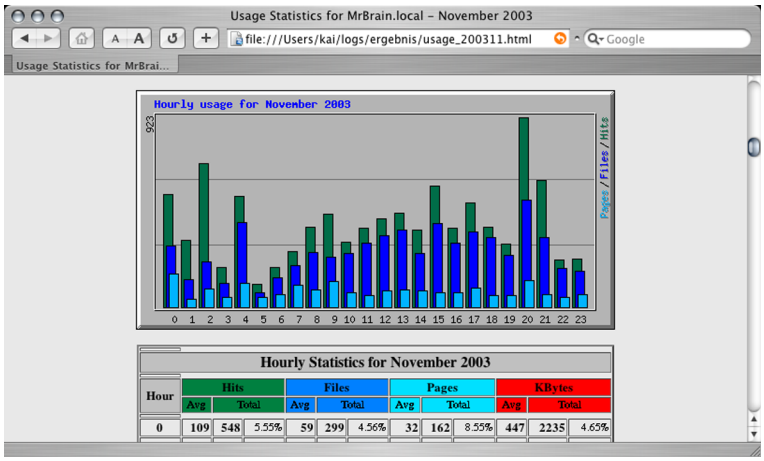

Abbildung 1.2 Die Zugriffe auf Ihre Webseite können Sie mit Webalizer auswerten.

Einstellungen vornehmen

In der Datei **webalizer.conf** müssen Sie noch einige Einstellungen vornehmen, damit Ihnen das Programm einigermaßen akkurate Statistiken erstellt. Zuerst müssen Sie bei der Angabe `LogFile` die auszuwertende Datei angeben. Sie können dies auch wie in der Grundeinstellung weiterhin mit einer Raute auskommentiert lassen und müssen dann die auszuwertende Datei am Prompt eingeben. Da Sie bei der Standardausgabe auch mehrere Dateien mit Hilfe von Joker-Zeichen auf einmal analysieren können, ist Letzteres praktischer, wenn Ihnen die Protokolle wöchentlich zur Verfügung stehen und Sie mehrere Dateien auswerten müssen. Die Angabe `OutputDir` legt das Verzeichnis fest, in dem die Auswertung gespeichert werden soll. Wenn Sie mehrere Protokolldateien in einer Statistik zusammenfassen möchten, sollten Sie bei `Incremental` die Einstellung auf `yes` ändern. In diesem Fall merkt sich das Programm

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 11 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

vorhergehende Auswertungen in einer Datei **webalizer.current** und berücksichtigt diese. Sie können sich so eine Statistik von Januar bis Juli erstellen, ohne dass die im Juli erstellte Analysen diejenige vom Beginn des Jahres überschreibt. Das Aussehen und die auszuwertenden Daten können Sie mit weiteren Optionen definieren, wobei die mitgelieferte Voreinstellungsdatei recht gut kommentiert ist.

Bezug: **http://www.mrunix.net/webalizer/**

1.1.4 Die Seiten der einzelnen Benutzer

Abbildung 1.3 Jeder Benutzer verfügt über seine eigene persönliche Seite.

Ein Modul sorgt für die Umleitung

Wenn Sie die Adresse http://127.0.0.1 um eine Tilde und den Namen eines Benutzers ergänzen, werden Sie auf eine andere Seite umgeleitet. Der Aufruf von http://127.0.0.1/~kai leitet Sie (siehe Abbildung 1.3) auf die persönliche Seite des Benutzers. Die Dateien, die hier angezeigt werden, finden sich im persönlichen Verzeichnis des Benutzers im Unterordner **Web-Sites**. Ersetzen Sie hier die Datei **index.html** durch eine andere, so wird stattdessen dieser Inhalt angezeigt. Verantwortlich für diese Umleitung sind zwei Einstellungen in der Datei **httpd.conf**. Die letzte Zeile der Datei lautet:

```
Include /private/etc/httpd/users/*.conf
```

Modulare Architektur

Das Zeichen `*` wird durch den Namen des Benutzers ersetzt. Für diesen Vorgang zuständig ist das Modul `mod_userdir`. Das Programm Apa-

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 12 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

che ist so aufgebaut, dass je nach Bedarf weitere Programmteile, die Module, geladen werden können. Diese Module erweitern den Funktionsumfang des Webservers um einige Funktionen. Die verfügbaren Module werden im ersten Drittel der Datei **httpd.conf** freigegeben oder durch eine vorangestellte Raute # gesperrt. Die entsprechenden Dateien, die den Programmcode der Module enthalten, werden im Verzeichnis **/usr/libexec/httpd** gespeichert. Mit der Zeile

```
LoadModule userdir_module libexec/httpd/mod_userdir.so
```

wird das für die Weiterleitung zuständige Modul geladen. Da die Abarbeitung von Anfragen mit Hilfe der Module abhängig von der Reihenfolge ist, sollten Sie die Zeilen in diesem Bereich nicht vertauschen. Der folgende Bereich in der Konfigurationsdatei aktiviert die eingebundenen Module. Hier aktiviert der Eintrag `AddModule mod_userdir.c` das entsprechende Modul. Würden Sie beide Einträge mit # auskommentieren, würde die beschriebene Weiterleitung nicht mehr funktionieren.

1.1.5 Unterstützung für Rendezvous

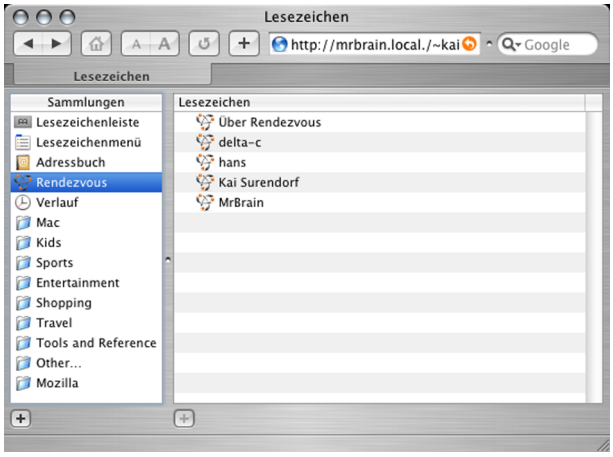

Abbildung 1.4 Der Apache unterstützt Rendezvous von Haus aus.

Automatische Kommunikation

Wenn Sie in Ihrem Netzwerk oder auch nur auf Ihrem Rechner den Webserver aktivieren, so kommuniziert er seine Aktivität seit der Version 10.2.4 über das Netzwerk mit Hilfe der Rendezvous-Technologie. Im Browser Safari können Sie daher bei den Lesezeichen den Punkt **Rendezvous** auswählen (siehe Abbildung 1.4). Hier erscheinen automatisch alle Webserver, die in Ihrem lokalen Netzwerk aktiv sind. Zuständig für diese Kommunikation ist das Modul mit der Bezeichnung `rendez-`

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 13 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

vous_apple_module. Seine Einstellungen werden gegen Ende der Datei vorgenommen. Sie finden dort folgenden Eintrag:

```
<IfModule mod_rendezvous_apple.c>
# Only the pages of users who have edited their
# default home pages will be advertised on Rendezvous.
RegisterUserSite customized-users
#RegisterUserSite all-users
# Rendezvous advertising for the primary site is off by
default.
RegisterDefaultSite
</IfModule>
```

Mit dem Eintrag `RegisterDefaultSite` wird das Modul angewiesen, die oberste Ebene des Webservers im lokalen Netzwerk mit dem Namen Ihres Rechners zu kommunizieren. Wird dieser Eintrag ausgewählt, so wird Ihr Rechner direkt mit seiner IP-Nummer aufgerufen. Dies entspräche dem direkten Aufruf mit http://, gefolgt von der IP-Nummer Ihres Rechners. Mit der Angabe `RegisterUserSite` können Sie einschränken, welche Benutzer mit ihren Webseiten im Netz präsent sein sollen und welche nicht via Rendezvous kommuniziert werden. Die Angabe `customized-users` beschränkt die Liste auf diejenigen Benutzer, die Änderungen an ihrem Konto vorgenommen haben. Mit `all-users` würde diese Einschränkung ignoriert. Eine dritte Möglichkeit, Adressen automatisch via Rendezvous zu kommunizieren, besteht in der Direktive `RegisterResource` gefolgt von dem Namen und dem Verzeichnis, auf das umgeleitet wird. Fügen Sie einen Eintrag `RegisterResource ProjektA test` in die Datei ein, so erscheint im Menü Rendezvous von Safari ein Eintrag ProjektA, der Sie auf das Verzeichnis **test** umleitet und damit der Eingabe http://Rechnername/test in der Adresszeile des Browsers entspricht. Arbeiten Sie in einem kleinen Team im Netzwerk, können Sie mit Rendezvous schnell Kürzel für einzelne Projektbereiche vergeben oder, wenn Sie ein Produkt wie Zope einsetzen, auch auf diesen Server verweisen. Da Zope standardmäßig auf Port 8080 lauscht, soll ein Kürzel mit der Bezeichnung Zope erstellt werden, das auf die Adresse http://rechnername:8080/ verweist. Der Eintrag hierfür lautet `RegisterResource Zope . 8080`. Der Punkt zwischen der Portnummer und der Bezeichnung steht für die oberste Ebene des Webservers.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 14 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

1.1.6 Virtuelle Hosts

Mehre Domains mit einer IP-Nummer

Der Apache ist in der Lage, auf einem Rechner mehrere Domains zu verwalten. Dies bedeutet, dass einer IP-Nummer mehrere Domains zugewiesen werden können, die jeweils auf ein anderes Verzeichnis deuten. Die Vorgabe, welche Domain auf welches Verzeichnis zeigt, wird mittels der Direktive `VirtualHost` vorgenommen. In der Standardeinstellung ist die Verwendung dieser virtuellen Host deaktiviert. Sie benötigen sie eigentlich erst dann, wenn Sie selbstständig eine Domain auf Ihrem Rechner betreiben wollen. Ansonsten ist die Arbeit mit Rendezvous und der Angabe `RegisterResource` einfacher und effizienter. Um die Verwendung virtuellers Hosts zu aktivieren, entfernen Sie die Raute in der Zeile `NameVirtualHost *:80`. Anschließend müssen Sie für jede Domain einen entsprechenden Eintrag vornehmen. Dieser muss wenigstens folgende Einträge aufweisen:

```
<VirtualHost *>
ServerName Domain.tld
DocumentRoot /Verzeichnis/fuer/Domain
</VirtualHost>
```

Mit diesem Eintrag werden alle Anfragen, die über Domain.tld kommen, mit den Daten des angegebenen Verzeichnisses beantwortet. Sie können natürlich noch weitere Einstellungen vornehmen. In der Dokumentation des Webservers finden Sie ausführliche Erläuterungen.

1.1.7 Tricks mit der Datei .htaccess und darüber hinaus

Konfiguration im Verzeichnis

Bisher ist der Webserver nur in der Lage, einfache Texte und Grafiken im World Wide Web zur Verfügung zu stellen. Um auch ein Kontaktformular, das etwaige Kundenanfragen weiterleitet, oder eine Vebrindung mit der MySQL-Datenbank aufzunehmen, müssen die restriktiven Vorgaben ein wenig gelockert werden. Dabei sind dennoch einige Sicherheitsvorgaben zu beachten. Die Grundeinstellung für Verzeichnisse wird durch folgende Zeilen festgelegt:

```
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
```

Sie haben zur Folge, dass keine der nachfolgend besprochenen Aktionen möglich ist, und durch `AllowOverride` wird verhindert, dass diese Restriktion mit der Datei **.htaccess** überschrieben werden kann. Diese

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 15 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Einstellung gilt für alle Verzeichnisse, für die Sie nichts anderes vorgeben. Wenn Sie im Verzeichnis **/Library/WebServer/Documents** ein Unterverzieichnis **Projekt** erstellen und planen, in diesem die nachstehend erläuterten Funktionen zu nutzen, müssen Sie die entsprechenden Freigaben in der Datei **httpd.conf** erteilen. Hierzu erstellen Sie unter dem obigen Eintrag die Konfiguration für dieses weniger restriktiv eingestellte Verzeichnis. Sie könnte folgendermaßen aussehen:

```
<Directory /Library/WebServer/Documents/Projekt>
Options ExecCGI Includes FollowSymLinks
AllowOverride All
</Directory>
```

Mit der ersten Zeile wird das Verzeichnis angegeben, für das die Einstellungen gelten. Die Direktive `AllowOverride All` erlaubt die uneingeschränkte Verwendung der Datei **.htaccess**. Die angegebenen Optionen ermöglichen die Verwendung von CGI-Skripten (`ExecCGI`) sowie von Server Side Includes (`Includes`). Ferner ist es mögliche, symbolische Links in dem Verzeichnis zu erstellen, deren Funktionsfähigkeit nicht eingeschränkt ist. Welche Optionen Sie in Verbindung mit `Options` verwenden können, ist in Tabelle 1.2 aufgeführt.

Option	Bedeutung
None	Keine der aufgeführten Optionen ist möglich.
All	Alle Optionen mit Ausnahme von MultiViews werden verwendet.
Indexes	Ist keine Datei index.html oder index.php im Verzeichnis vorhanden, so wird beim Abruf des Verzeichnisses ohne Angabe einer Datei dessen Inhalt dargestellt. Dies kann ein Sicherheitsrisiko sein und sollte nicht verwendet werden.
Includes	Die Verwendung von Server Side Includes wird ermöglicht.
Follow-Symlinks	Symbolische Verknüpfungen werden verfolgt, auch außerhalb des Verzeichnisses. Dies ist ein Sicherheitsrisiko.
ExecCGI	CGI-Skripte können ausgeführt werden.
Muliviews	Mit dieser Option und dem zugehörigen Modul können Daten in Abhängigkeit von den Einstellungen des Surfers übertragen werden. Die Methode ist sehr rechenintensiv und im praktischen Einsatz kaum zu empfehlen.

Tabelle 1.2 Optionen für Verzeichnisse

Benutzer gesondert konfiguriert

Beachten Sie, dass die Konfigurationen der Verzeichnisse der Benutzer Ihres System, die zum Beispiel unter http://mrbrain.local/ kai/ zu errei-

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 16 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

chen sind, nicht in der Datei **httpd.conf** vorgenommen werden. Für jeden Benutzer finden Sie im Verzeichnis **/etc/httpd/users** eine eigene Konfigurationsdatei mit seinem Namen, die die Einstellungen für den Ordner **Web-Site** in seinem persönlichen Verzeichnis enthält. Um CGI-Skripte im Verzeichnis des Benutzers `kai` zu erlauben, müssen Sie die Datei **kai.conf** entsprechend ändern.

Server Side Includes

Server Side Includes (SSI) sind Platzhalter in einer HTML-Datei, in die der Webserver vor dem Versand an den Empfänger die jeweiligen Werte einfügt. Um Server Side Includes überhaupt verwenden zu können, müssen Sie bei den Zeilen

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

die eventuell noch vorhandene Raute # zu Beginn entfernen. Mit diesen Einstellungen werden Dateien, die auf **.shtml** enden, bearbeitet. Ein Beispiel für die Verwendung eines Server Side Include ist in Listing 1.1 zu finden.

Listing 1.1 Beispiel für die Verwendung von SSI

```
<html>
<head>
<title>
Beispiel fuer die Verwendung von SSI
</title>
</head>
<body>
<p>
Diese Datei wurde zuletzt am
<!--#echo var="LAST_MODIFIED"-->
bearbeitet.
</body>
</html>
```

Wenn Sie die Zeilen aus Listing 1.1 in einem Verzeichnis speichern, in dem Server Side Includes verwendet werden, so wird die Zeile `<!--#echo var="LAST_MODIFIED"-->` durch das Änderungsdatum der Datei ersetzt, wie in Abbildung 1.5 zu sehen.

Fehler umleiten

In einem Verzeichnis, das mit der Direktive `AllowOverride All` versehen wurde, können Sie die Datei **.htaccess** effizient einsetzen. Diese Datei hat die Aufgabe, einige Voreinstellungen des Webservers zu über-

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 17 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

schreiben. Dies betrifft zum Beispiel die Umleitung von nicht gefundenen Dateien auf eine generelle Fehlerseite oder die Verweigerung der Kommunikation mit ganz bestimmten IP-Nummern. Da der Dateiname mit einem Punkt beginnt, ist sie im Finder unsichtbar. Es handelt sich um eine einfache Textdatei und die in ihr vorgenommenen Einstellungen gelten für das Verzeichnis, in dem sie abgelegt wurde, und dessen Unterverzeichnisse. Da der Webserver, wenn er eine Datei nicht findet, den Fehler-Code 404 aussendet und anschließend die eher unscheinbare Standard-Fehlerseite ausgibt, wäre eine Umleitung bei nicht vorhandenen Dateien auf eine entsprechende Seite sinnvoll. Mit der Zeile `ErrorDocument 404 fehler.shtml` wird immer, wenn eine Datei nicht gefunden wurde, der Inhalt der Datei **fehler.shtml** ausgegeben. Um jemandem, der sich wahrscheinlich unbefugt Zugriff auf Ihre Daten verschaffen möchte, gleich mit einer entsprechenden Erklärung zu begegnen, können Sie im Falle des Fehler-Codes 403 diesen auf eine passende Seite umleiten. Hierzu fügen Sie in der Datei **.htaccess** die Zeile `ErrorDocument 403 verboten.shtml` ein. Beachten Sie, dass sich Änderungen an der Datei sofort auswirken und keinen Neustart des Servers erfordern.

Abbildung 1.5 Die SSI-Angabe wurde durch das Änderungsdatum ersetzt.

Rechner sperren

Manchmal kommt es vor, dass Sie einen Rechner vom Besuch Ihrer Webseiten ganz ausschließen oder den Zugriff auf Ihr internes Netzwerk begrenzen möchten. Mit der Direktive `Order deny,allow` gefolgt von einer Liste von IP-Nummern können Sie die Nutzung Ihres Webservers einschänken. Mit den Zeilen

```
Order deny,allow
Allow from all
Deny from 192.90.121.10
```


K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 18 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

wird dem Rechner mit der angegebenen IP-Nummer der Zugriff verweigert. Weitere IP-Nummern können Sie pro Zeile hinzufügen. Sie können natürlich den Server auch generell sperren und nur für bestimmte IP-Nummern freigeben. In diesem Fall würden Sie mit

```
Order deny,allow
Deny from all
Allow from 192.90.121.10
```

den Zugriff auf den zuerst gesperrten Rechner begrenzen.

Verzeichnisse mit Passwörtern schützen

Der Webserver ist in der Lage, Verzeichnisse nur nach Eingabe eines Benutzernamens und eines Passwortes freizugeben. Da die Passwörter unverschlüsselt durch das Netz übertragen werden, eignet sich dieser Schutz kaum für sensible Daten. Aber um Unbefugten keinen Einblick in die eigenen Entwürfe für Webseiten zu gestatten, ist er gut genug. Auch in Verbindung mit einer eigenen iDisk erfüllt dieser Schutz durchaus seinen Zweck. Hierzu fügen Sie der Datei **.htaccess** zuerst folgende Zeilen hinzu:

```
AuthName "Restricted"
AuthType Basic
AuthUserFile .htpasswd
require valid-user
```

Damit ist das Verzeichnis vorerst gesperrt und der Browser des Besuchers fordert diesen zur Eingabe einer Benutzerkennung und eines Passwortes auf. Diese werden nicht in der NetInfo-Datenbank gespeichert, sondern in einer weiteren Textdatei **.htpasswd**, die mit der dritten Zeile vorgegeben wurde. Diese Datei können Sie nicht von Hand bearbeiten. Sie wird mit Hilfe des Befehls `htpasswd` erstellt. Wechseln Sie hierzu in das Verzeichnis, das Sie schützen wollen und in dem bereits die entsprechend geänderte Datei **.htaccess** liegt. Mit dem Befehl `htpasswd -c .htpasswd kai` erstellen Sie die Datei und legen gleichzeitig den Benutzer `kai` an. Anschließend werden Sie nach einem Passwort für diesen Benutzer gefragt und gebeten, es zu bestätigen. Wenn die Meldung `Adding password for user kai` erscheint, wurde die Datei erfolgreich angelegt und der Benutzer `kai` ist in Kombination mit dem vergebenen Passwort in der Lage, das Verzeichnis aufzurufen. Um weitere Benutzer hinzuzufügen, rufen Sie `htpasswd` ohne die Option `-c` auf. Diese würde eine neue Datei erstellen und die vorhandenen Einträge überschreiben. Um einen Benutzer aus dieser Datei zu löschen, können Sie sie in einem Editor öffnen und die Zeile, die mit dem Namen des Benutzers beginnt, entfernen.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 19 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

1.1.8 PHP, Perl und Python aktivieren

Benötigte Module aktivieren

Zwar werden die benötigten Module für PHP- und CGI-Skripte in Perl oder Python bei der Installation von Mac OS X mitgebracht, aber sie sind nicht aktiv. Um die Verwendung von in PHP geschrieben Skripten zu ermöglichen, müssen Sie gegebenenfalls die Raute # bei diesen Einträgen entfernen:

```
LoadModule php4_module libexec/httpd/libphp4.so
AddModule mod_php4.c
```

Anschließend werden alle Dateien, die auf **.php** enden, als PHP-Skripte ausgeführt. Um die Funktion zu testen, erstellen Sie eine Datei **test.php** wie in Listing 1.2 gezeigt.

Listing 1.2 Informationen über PHP aufrufen

```
<?PHP
phpinfo();
?>
```

Anschließend rufen Sie die Datei im Browser auf, etwa mit http://127.0.0.1/test.php. Ist PHP aktiv, so wird die Ausgabe der in Abbildung 1.6 ähneln.

Abbildung 1.6 Die erfolgreiche Aktivierung von PHP kann mit dem Befehl phpinfo() überprüft werden.

Die aufgerufene Funktion `phpinfo()` gibt Ihnen im Browser detaillierte Informationen über die verfügbaren PHP-Module.

Add-Handler für Perl benötigt

Um die Verwendung von Perl, Python oder einer anderen Skriptsprache zu

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 20 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

ermöglichen, muss zuerst ebenfalls das benötigte Modul aktiviert werden. Löschen Sie, falls vorhanden, die Raute # bei folgenden Zeilen:

```
LoadModule perl_module libexec/httpd/libperl.so
AddModule mod_perl.c
```

und prüfen Sie, dass die Zeilen

```
LoadModule cgi_module libexec/httpd/mod_cgi.so
AddModule mod_cgi.c
```

ebenfalls nicht auskommentiert sind. Ferner muss dem Webserver mitgeteilt werden, dass Dateien mit der Endung **.cgi** als Skripte zu behandeln sind. Hierfür ist die Direktive `AddHandler cgi-script .cgi` zuständig. Alle Skripte, die ausgeführt werden sollen, müssen Sie mit `chmod 755 Skript` als ausführbar markieren. Um die Aktivierung zu testen, können Sie das kleine Python-Skript aus Listing 1.3 in einem freigegebenen Ordner mit dem Namen **test.cgi** speichern, die Zugriffsrechte mit `chmod 755 test.cgi` auf ausführbar setzen und es im Browser aufrufen. In diesem sollte dann nur der Satz `CGI-Skripte sind aktiviert` erscheinen.

Listing 1.3 Ein CGI-Skript in Python

```
#!/usr/bin/python
import cgi
print "Content-Typ: text/plain \n\n"
print "CGI-Skripte sind aktiviert"
```

1.1.9 Die eigene iDisk mit WebDav

WebDav aktivieren

Vielleicht kennen Sie von Apple das Angebot .Mac. Dort ist auch eine virtuelle Festplatte enthalten, die Sie im Finder mit dem Menü `Mit Server verbinden` in Ihr bestehendes Dateisystem wie eine weitere Festplatte einbinden können. Mit WebDav können Sie unter anderem die Kalender von iCal im Netzwerk publizieren und anderen Nutzern zum Abonnement freigeben. Außerdem können Sie sich die Konfiguration eines FTP-Servers ersparen, wenn nur einige Dateien übertragen werden sollen.

Dahinter steht das Protokoll WebDav, das auf HTTP aufbaut. Es ermöglicht dem Webserver, Verzeichnisse für zum Beispiel den Finder von Mac OS X freizugeben und auch Schreibzugriffe zuzulassen. Der Ordner verhält sich also vergleichbar mit einer Partition einer Festplatte. Das notwendige Modul für den Apache bringt Mac OS X von Haus aus mit. Entfernen Sie das Kommentarzeichen aus den Zeilen

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 21 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

```
LoadModule dav_module libexec/httpd/libdav.so
AddModule mod_dav.c
```

so steht es dem Webserver zur Verfügung. Da es sich bei WebDav um kein vollwertiges Dateisystem handelt, führt das Modul selbst Buch darüber, welche Datei gerade geöffnet ist und welche nicht. Dies erfolgt mittels so genannter Lock-Dateien. Fügen Sie am Ende der Datei **httpd.conf** die Zeile `DAVLockDB /var/tmp` hinzu. In diesem Verzeichnis werden dann die Lock-Dateien gespeichert.

Abbildung 1.7 Die Verbindung mit einem WebDav Server erfolgt über den Finder.

Erstellen Sie dann unter **/Library/WebServer/Documents/** ein Verzeichnis, dass via WebDav freigegeben werden soll. In der Datei **httpd.conf** muss nun die Einstellung für die Verwendung von WebDav für dieses Verzeichnis vorgenommen werden. Dazu wird ein `<Directory>`-Eintrag benötigt, der die speziellen Zugriffsrechte festlegt. Die Angaben aus Listing 1.4 müssen Sie der Datei **httpd.conf** hinzufügen, wobei `Webdav` durch das freizugebende Verzeichnis zu ersetzen ist. Mit der Direktive `DAV On` wird das WebDav-Modul für dieses Verzeichnis und seine Unterverzeichnisse aktiviert. Damit der Webserver Änderungen an dem Verzeichnis vornehmen kann, muss er und seine Gruppe zum Eigentümer gemacht werden. Mit `sudo chown www Webdav` und `sudo chgrp www Webdav` übergeben Sie das Verzeichnis an den Webserver.

Zugriffsrechte setzen

Listing 1.4 Der Eintrag in der Datei httpd.conf für das freigegebene Verzeichnis

```
<Directory /Library/WebServer/Documents/Webdav>
    DAV On
    AllowOverride None
    Options None
</Directory>
```

Mit den beiden Werten `None` wird verhindert, dass Dateien wie **.htaccess**

Verzeichnis schützen

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 22 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

auf dem Server hinterlegt oder Programme ausgeführt werden können. Nach einem Neustart des Webservers können Sie sich über den Finder bei der Adresse http://127.0.0.1/Webdav bei dem Server anmelden. Andere Benutzer müssen Ihre aktuelle IP-Nummer verwenden.

Ein unsicheres Protokoll

WebDav ist ein sehr unsicheres Protokoll. Zwar lässt es sich noch ein wenig sicherer machen als hier beschrieben, aber Sie sollten bedenken, dass die gesamte Kommunikation unverschlüsselt verläuft. Für sensible Daten ist WebDav nicht geeignet.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 23 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

1.2 Mit Windows Samba tanzen

1.2.1 Aufgaben und Aufbau von Samba

Server Message Blocks

Der Name Samba deutet nicht auf das Rhythmusgefühl der Programmierer hin, sondern stammt von dem Server Message Block (SMB) genannten Protokoll, auf das die Kommunikation innerhalb von Windows-Netzwerken beruht. Samba ist eine Umsetzung dieses Protokolls. Server Message Blocks unterteilen Netzwerke nicht in IP-Nummern, sondern in Domänen, und jeder Rechner hat innerhalb dieser Domainen einen eindeutigen Namen, anhand dessen er identifiziert wird. Später wurde das SMB-Protokoll auch um die Verbindung mit TCP/IP Netzwerken ergänzt

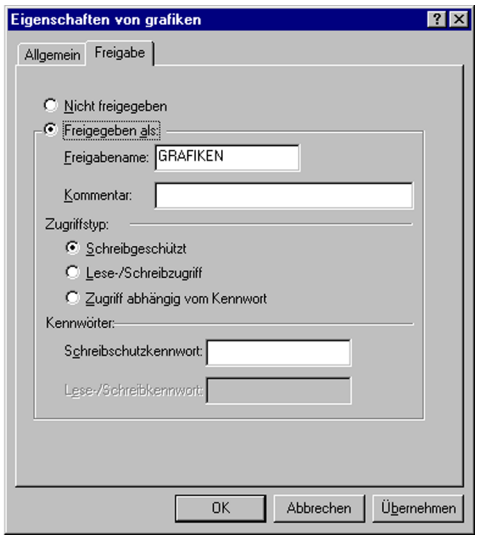

Abbildung 1.8 Unter Windows können Ordner im Fenster Eigenschaften freigegeben werden.

Kommunikation über den Finder

Wenn auf einem Windows-Rechner Dateien und Ordner freigegeben wurden, ist der Zugriff über den Finder die bequemste Variante. Wählen Sie hierzu den Menüpunkt **Mit Server verbinden** aus und geben Sie anschließend die URL `smb://` gefolgt von der IP-Nummer oder dem Namen des Rechners an, mit dem Sie eine Verbindung aufnehmen möchten.

Eine Sammlung von Programmen

Bei dem, was Samba genannt wird, handelt es sich um eine Sammlung von Programmen für die unterschiedlichsten Zwecke in der Kommunikation mit Windows-Rechnern. Das Rückgrat bilden zwei Daemons, die im Hintergrund die zwei wesentlichen Funktionen erfüllen.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 24 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Abbildung 1.9 Die Verbindung erfolgt mit Hilfe des Finders.

- **nmbd** Dieser Daemon fungiert als Nameserver, ähnlich eines DNS im Internet, der die Namen von Rechnern wie MrBrain.local, die Sie in den Systemeinstellungen für Ihren Rechner vorgeben können, in die Namen innerhalb eines SMB-Netzwerk auflösen kann und die passende IP-Nummer auf eine entsprechende Anfrage zurückgibt.
- **smbd** Mit `smbd` wird die Fähigkeit, auf Dateien von Windows-Rechnern zugreifen zu können, realisiert. Ebenso steht er im Hintergrund als Server für eingehende Anfragen von Windows-Rechnern zur Verfügung. Bei `smbd` handelt es sich also um das zentrale Element von Samba. Er wird aktiviert, wenn Sie in den Systemeinstellungen den Punkt **Windows Sharing** aktivieren.

Neben diesen zwei Kernprogrammen gibt es noch eine Reihe von kleineren Programmen, die Ihnen die Arbeit innerhalb eines heterogenen Netzwerkes leichter machen.

Rechner finden

Mit dem Programm `findsmb` (siehe Abbildung 1.10) können Sie sich die Rechner in Ihrem lokalen Netzwerk anzeigen lassen, die mit Hilfe des SMB-Protokolls angesprochen werden können.

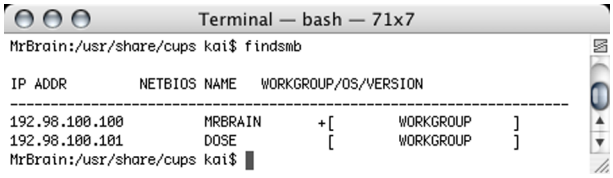

Abbildung 1.10 Mit dem Programm findsmb können im Netzwerk vorhandene Rechner angezeigt werden.

Um gezielt die IP-Nummer eines Rechners mit Hilfe seines Namens herauszufinden, können Sie den Befehl `nmblookup` gefolgt von dem Namen des Rechners eingeben. Der Aufruf von `nmblookup Dose` führt im lokalen Netzwerk des Autors zu folgendem Ergebnis:

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 25 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

```
querying Dose on 192.98.100.255
192.98.100.101 Dose<00>
```

Anzeiges des Status

Der Rechner mit dem Namen Dose hat die IP-Nummer 192.98.100.101 zugewiesen bekommen. Um sich kurz einen Überblick über die Auslastung Ihres Samba Server zu verschaffen, können Sie den Befehl `smbstatus` eingeben.

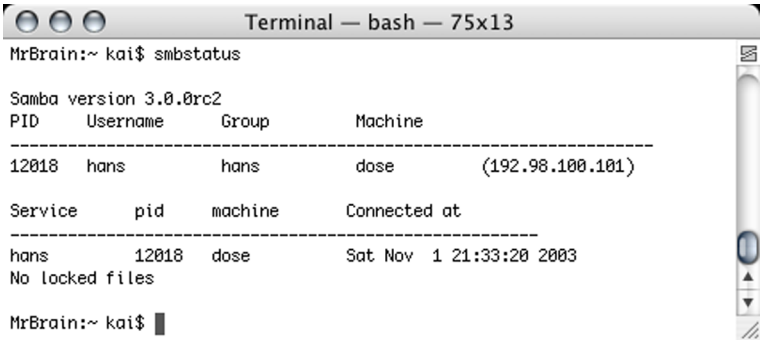

Abbildung 1.11 Die Auslastung des Samba Servers

Zugriff über das Terminal

Mit dem Programm `smbclient` können Sie vom Terminal aus auf einen Windows-Rechner zugreifen und müssen nicht den Weg über den Finder gehen. Um zum Beispiel regelmäßig Daten von einem Windows-Rechner mit Hilfe eines cron-Jobs zu kopieren, ist dieses Programm sehr hilfreich. Der Aufruf erfolgt in der Form

```
smbclient Rechner Benutzer
```

und anschließend können Sie ähnlich wie das FTP-Programm Dateien kopieren, verschieben und auf Ihren Rechner kopieren. Mit `smbclient //Dose/grafik -U hans` würden Sie sich auf dem Rechner `Dose` anmelden, um als Benutzer `hans` auf das freigegebene Verzeichnis `grafik` zuzugreifen. Anschließend werden Sie nach dem Passwort von hans gefragt und bei erfolgter Anmeldung ändert sich der Prompt am Terminal in `smb: \>`. Alle weiteren Eingaben werden jetzt von dem Programm `smbclient` ausgeführt. Beispielsweise würde `ls` Ihnen nun den Inhalt des Verzeichnisses auf dem Windows-Rechner anzeigen. Mit `exit` kann das Programm wieder beendet werden. Besonders hilfreich für die Datensicherung in einem Netzwerk ist die Option `-T`, die eine ähnliche Funktionalität wie der Befehl `tar` zur Verfügung stellt.

Neu in Version 3

Die wesentliche Neuerung in der Version 3.0, die mit Mac OS X Version 10.3 installiert wird, besteht in der Unterstützung des Kerberos-Protokolls

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 26 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

zur Authentifizierung von Benutzern. Neben vielen weiteren Verbeserungen im Detail ist das Programm `net` hinzugekommen, mit dem Administratoren von einem UNIX-System aus einen Windows-Rechner verwalten können.

1.2.2 Samba konfigurieren und anpassen

Die Datei /etc/smb.conf

Die Einstellungen des Samba Servers, der Ordner und Drucker für Windows-Rechner zur Verfügung stellt, werden in der Datei **/etc/smb.conf** vorgenommen. Das Format dieser Datei unterscheidet sich von anderen Konfigurationsdateien wie **httpd.conf** darin, dass Einträge in Gruppen organisiert sind. Sie werden wie in Listing 1.5 Blöcke finden, die mit eckigen Klammern beginnen und nachfolgend die einzelnen Optionen. Kommentare können wie bekannt mit der Raute (#) oder auch dem Semikolon (;) eingeleitet werden. Sie müssen aber in einer eigenen Zeile für sich stehen. Ferner müssen keine Anführungszeichen verwendet werden, um die einer Option zugewiesenen Werte zu kennzeichnen. Der Daemon `smbd` liest die Konfigurationsdatei alle sechzig Sekunden neu ein. Sie müssen Ihn daher nicht neu starten, um Änderungen in Kraft treten zu lassen.

Neustart nicht erforderlich

Die Konfiguration von Samba im Detail ist ein sehr komplexes Thema. Viele mögliche Fehler lassen es ratsam erscheinen, vor großen Änderungen eine Sicherheitskopie der Datei **/etc/smb.conf** anzulegen. Um zu prüfen, ob die Datei wenigstens formal korrekt ist, können Sie den Befehl `testparm` ohne weitere Optionen aufrufen.

Das Konzept der Shares

Die mit eckigen Klammern begonnenen Abschnitte innerhalb der Datei **smb.conf** definieren Eintrittspunkte, an denen sich ein Benutzer von einem Windows-Rechner aus anmelden kann. Sie werden innerhalb der Dokumentation von Samba Shares genannt. In Listing 1.5 wird unter dem Eintrag `[global]` die Einstellung für den Server an sich vorgenommen. Die Einstellungen beinhalten Vorgaben für die Authentifizierungsmethode, wobei der Eintrag `opendirectory` die Einbindung der NetInfo-Datenbank ermöglicht.

Listing 1.5 Die globalen Einstellungen des Samba Servers

```
[global]
  guest account = unknown
  encrypt passwords = yes
  auth methods = guest opendirectory
  passdb backend = opendirectorysam guest
  printer admin = @admin, @staff
```


K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 27 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

```
server string = Mac OS X
unix charset = UTF-8-MAC
display charset = UTF-8-MAC
dos charset = 437
use spnego = no
client ntlmv2 auth = no
```

Zugriff freigeben und sperren

Wenn Ihr Netzwerk etwas umfangreicher geworden ist, können Sie den Zugriff anhand der IP-Nummer einschränken. Hierzu stehen die Direktiven `hosts allow` und `hosts deny` zur Verfügung. Wenn nur der Rechner mit der IP-Nummer 192.98.100.101 Zugriff auf die über Samba zur Verfügung gestellten Ordner und Drucker erhalten soll, können Sie im Abschnitt `[global]` die Zeile

```
hosts allow = 192.98.100.101
```

hinzufügen. Anschließend kann nur dieser Rechner auf den Samba-Server zugreifen. Um einen Rechner explizit auszuschließen, den anderen aber freien Zugriff zu ermöglichen, fügen Sie eine Zeile in der Form

```
hosts deny = 192.98.100.101
```

in den Abschnitt `[global]` ein. Mehrere Rechner können Sie sperren, indem Sie die IP-Nummern getrennt durch Leerzeichen angeben. Die Kombination der Direktiven `hosts allow` und `hosts deny` ist möglich und hat zur Konsequenz, dass der zugreifende Rechner unter `hosts allow` aufgeführt sein muss.

Mehrere virtuelle Server

Es kann vorkommen, dass Sie einen Rechner unter mehreren Namen in einem SMB-Netzwerk verwenden möchten. Ein Szenario hierfür wäre, wenn zwei Server, die unter verschiedenen Namen fungieren, auf einen Rechner zusammengelegt werden sollen. In diesem Fall müssten bei allen Rechnern im Netzwerk Änderungen vorgenommen werden, da ja einer der Server aus dem Netzwerk mit seinem Namen verschwinden würde. Mit der Direktive `netbios aliases` können Sie hingegen einen Server unter mehreren Namen im Netzwerk kommunizieren. Der Eintrag

```
netbios aliases = grafik buchhaltung
```

lässt Ihren Rechner sowohl unter dem Namen `grafik` als auch `buchhaltung` fungieren. Wenn dies vorher zwei separate Rechner waren, so müssen von Seiten der Anwender im Netzwerk keine weiteren Änderungen mehr vorgenommen werden.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 28 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Der Abschnitt in Listing 1.6 betrifft die Konfiguration der Benutzerverzeichnisse. Wenn sich von einem Windows-Rechner der Benutzer `hans` anmeldet, dann wird er aufgrund dieses Eintrages automatisch an sein persönliches Verzeichnis auf dem Apple-Rechner verwiesen. Den Eintrag `comment` können Sie nach Belieben ändern. Er erscheint unter Windows als Erläuterung innerhalb der Netzwerkumgebung. Mit der Direktive `read only = no` wird den Benutzern Schreibzugriff ermöglicht. Mit der Direktive `bowseable = no` wird verhindert, dass die gesamte Liste der Benutzerverzeichnisse aufgelistet wird. Würden Sie diese Angabe auf `yes` setzen, dann würde bei der Anmeldung einem Benutzer die gesamte Liste der auf diesem Server angelegten Benutzerkonten zur Verfügung stehen. So wird er direkt in sein eigenes Verzeichnis umgeleitet.

Listing 1.6 Die Konfiguration für die Ordner der Benutzer

```
[homes]
   comment = User Home Directories
   browseable = no
   read only = no
```

Drucker und Samba

In Listing 1.7 finden Sie den recht kurzen Eintrag zur Konfiguration der Drucker. Die Liste der Drucker, die über Samba von einem Windows-Rechner angesprochen werden, wird nicht von Samba selbst verwaltet, sondern beruht auf den Einträgen in der Datei **/etc/printcap**. Diese wird von CUPS verwaltet. Die Angabe `path` definiert, wo die Druckaufträge zwischengespeichert werden. Die Angabe `printable` ist für diesen Bereich Pflicht, da Samba sonst die Arbeit verweigert.

Listing 1.7 Die Einstellung der Drucker

```
[printers]
  path = /tmp
  printable = yes
```

Eigene Shares erstellen

In der bisherigen Konfiguration ist es möglich, dass ein Benutzer von einem Windows-Rechner auf sein persönliches Verzeichnis zugreifen kann. Um weitere Verzeichnisse freigeben zu können, müssen Sie eigene Shares in der Datei **smb.conf** definieren. Alle Möglichkeiten der Konfiguration von Samba durchzugehen, wäre hier zu viel. Der Befehl `man smb.conf` ruft die umfangreiche Dokumentation auf. An dieser Stelle soll lediglich in einem Beispiel eine Partition der Festplatte freigegeben werden. Nehmen Sie an, dass unter **/Volumes/Netz** eine Partition existiert, die unter dem Namen `Netzplatte` im Netzwerk freigegeben wird. Die einfachste Variante ist es, wie in Listing 1.8 gezeigt, einen kurzen Eintrag in der

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 29 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Datei **smb-conf** vorzunehmen. Sobald `smbd` die Konfiguration neu eingelesen hat, steht die Partition allen Rechnern im Netzwerk zur Verfügung. Der Eintrag `writeable` ist notwendig, da die Standardvorgaben lediglich Lesezugriff erlauben.

Listing 1.8 Eine Partition als Share freigeben

```
[Netzplatte]
   comment = Netzwerkplatte unter Mac OS X
   path = /Volumes/Netz
   writeable = yes
```

1.2.3 Einfachere Administration mit SWAT

Nur mit Panther

Die Bearbeitung der Datei **smb.conf** per Hand kann zu einem mühseligen Prozedere werden. Ab Mac OS X Version 10.3 existiert mit SWAT eine etwas komfortablere Möglichkeit. Wenn Sie SWAT aktivieren, können Sie anschließend über den URL http://127.0.0.1:901 auf das Menü zugreifen. SWAT stellt Ihnen in Form einer Webseite Formulare zur Verfügung (siehe Abbildung 1.12), mit denen Sie neue Shares eingeben und vorhandene modifizieren können.

Erstellen Sie, bevor Sie mit SWAT arbeiten, eine Sicherheitskopie der Datei **smb.conf**. Diese wird von SWAT überschrieben, und da Ihnen SWAT alle Möglichkeiten der Konfiguration zur Verfügung stellt, sind Fehler am Anfang sehr wahrscheinlich. Ferner wird SWAT als Super User ausgeführt. Dies bedeutet, dass Sie einerseits den Benutzer root aktivieren müssen. Es bedeutet andererseits aber auch, dass Sie, wenn Sie mit dem Internet verbunden sind und die Firewall deaktiviert haben, eine große Sicherheitslücke öffnen.

Aktivierung durch xinetd

SWAT wird durch den Daemon `xinetd` aufgerufen, sobald eine Anfrage über den SWAT zugewiesenen Port erfolgt. Um SWAT einen Port, bevorzugt 901, zuzuweisen, öffnen Sie die Datei **/etc/services** und fügen dieser an der passenden Stelle in der Liste den Eintrag `swat 901/tcp` hinzu. Falls Sie für Port 901 Einträge mit der Bezeichnung `smpnameres` finden, so können Sie diese auskommentieren. Der zweite Schritt besteht darin, `xinetd` auf eine Anfrage auf Port 901 hin, SWAT starten zu lassen. Hierzu müssen Sie die Datei **/etc/xinetd.d/swat** bearbeiten. Den Eintrag `disable = yes` müssen Sie in `disable = no` ändern. Nach einem Neustart steht SWAT unter der URL http://127.0.0.1:901 bereit.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 30 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

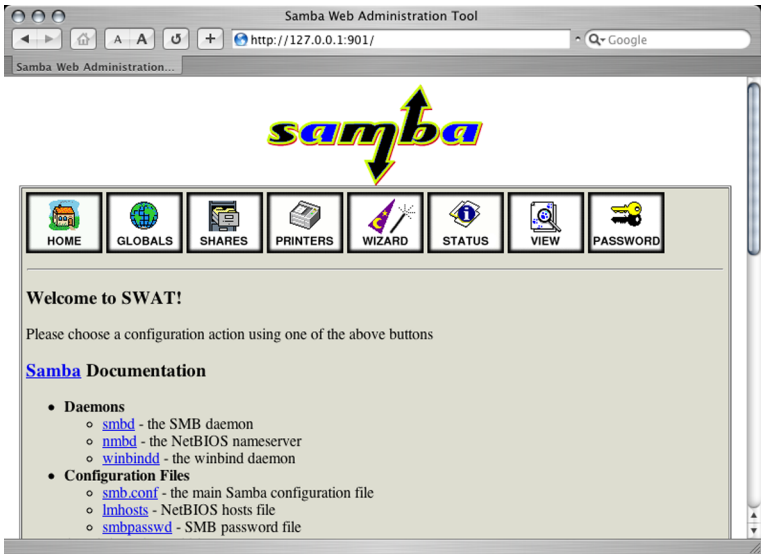

Abbildung 1.12 Mit SWAT kann Samba über einen Browser verwaltet werden.

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 31 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 32 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Anhang

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 33 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 34 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand

Index

K. Surendorf, UNIX fuer Mac OS X - Anwender Berlin November 2003 Galileo Press, ISBN: 3-89842-385-9
Layout: gp97.cls, Version 1.6 (05. September 2002), (C) Daniel Lauer, Bonn Mit TeX bearbeitet am 5. Oktober 2004, 17:27 Uhr
S. 35 Einstellungen: mit Marginalien mit Anleser neue Rechtschreibung mit Seitenrand