Weihnachten für die Linux-Box

Paketverteilung für die CPU

Im zweiten Teil dieses Workshops wollen wir die Box so weit ausbauen, dass Sie die Paketverwaltung bedienen und eigene Benutzer anlegen und verwalten können. Weiters legen wir mit der Installation einer MySQL-Datenbank eine Grundlage, auf der viele wichtige Dienste der WCM-Linux-Box basieren werden.

von Martin Müller

An freien Softwarepaketen dürfen wir uns angesichts der im Sommer dieses Jahres gefällten Entscheidung des Europäischen Parlaments zu Softwarepatenten noch länger freuen, weshalb wir uns hier gleich mal anschauen, wie man auf unserer WCM-Linux-Box neue Pakete installieren und bereits installierte auf den neusten Stand bringen kann.

Bei der verwendeten Distribution Debian Sarge kommt der mächtige Paketmanager *apt* zum Einsatz. *apt* ist die Abkürzung für „A Package Tool" und besteht aus mehreren Teilpaketen wie *apt-get, apt-cache, apt-key* und so weiter. Die meisten Pakete werden bei der Grundinstallation schon eingespielt und stehen gleich zur Verfügung, einige Nützliche, wie *apt-show-versions* müssen erst mit Hilfe von *apt-get* installiert werden.

Die Basics

Die WCM-Linux-Box läuft, es wartet die Befehlszeile auf die Anmeldung eines Benutzers. Sollten Sie statt der Befehlszeile den grafischen Anmeldebildschirm von Gnome sehen, so schalten Sie bitte auf die Befehlszeile mit der Tasten-Kombination (STRG + ALT + F1) um. Generell gibts unter UN*X-Betriebsystemen sechs Befehlszeilen zwischen denen Sie mit STRG-ALT-F1 bis F6 jederzeit umschalten können.

Die Tastenkombination STRG +ALT+F7 bringt sie, falls vorhanden, zur grafischen Oberfläche wie Gnome oder KDE.

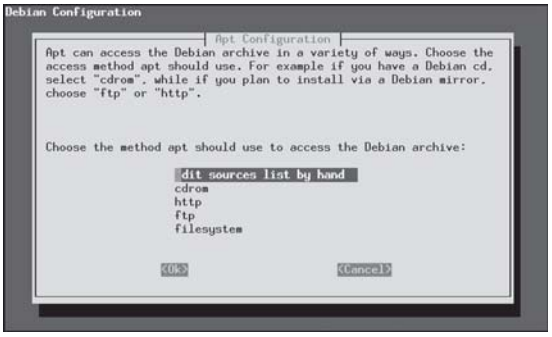
Alternativ melden Sie sich von einem anderem Rechner aus per SSH an der WCM-Linuxbox an. Wie das geht haben wir in der letzten WCM-Ausgabe beschrieben.

Wir melden uns an der Befehlszeile der Einfachkeit wegen als *root* an. Sie geben also beim Benutzernamen *root* ein, das Passwort ist das in der letzten Ausgabe gut gewählte *root-Passwort*.

Bitte achten Sie genau darauf was Sie nun tippen. Als Benutzer *root* haben Sie alle Rechte und Möglichkeiten, Sie können durch schlampige oder unbedachte Eingaben das System zerstören.

Quellenangaben

apt bezieht Paket-Informationen von unterschiedlichen Quellen. Nach der Installation sind diese Quellen als lokal von den Installationsmedien angegeben. Wenn wir also Pakete installieren, verlangt *apt* nach einer oder mehrer CDs oder DVDs. Dass diese Pakete nicht dem neuesten Stand entsprechen versteht sich von selbst. Die Software-Entwickler arbeiten ständig an Verbesserungen und stopfen, wenn sie aufgedeckt werden, Sicherheitslücken.



Zur Erleichterung beim Tippen führen wir folgendes Kommando aus: *source /etc/bash_completion* . Dadurch können Sie nicht nur Befehle, Dateipfade und Dateinamen durch drücken der TAB(ulator)-Taste vervollständigen, sondern auch Paketnamen die noch zur Disposition stehen.

Verfügt Ihre WCM-Linux-Box über keine Internetverbindung, so entfällt in diesem Fall die Konfiguration von *apt,* da von Beginn an CD als Installationsquelle eingestellt ist. Wollen Sie jedoch aktuelle Pakete aus dem Internet laden, müssen Sie die Konfigurationsdatei */etc/apt/sources-list* editieren. Wir erledigen dies entweder per Hand oder nehmen das Konfigurationstool *apt-setup* zu Hilfe.

Der Aufruf von *apt-setup* lässt nachfragen, von welcher Quelle installiert werden soll. Wir wählen durch Betätigen der Pfeiltasten *http* und bestätigen durch Drücken der TAB-Taste mit OK. Die Frage nach dem Spiegelserverstandort beantworten wir mit Österreich. Den Spiegelserver selbst wählen Sie nach Möglichkeit so, dass er möglichst nahe an Ihrem Standort liegt (Wien oder Graz) oder Sie lassen den Vorgabewert *ftp.at.debian.org* bestehen.

Da wir keinen HTTP-Proxy-Server vorgeschaltet haben, bestätigen Sie den nächsten Dialog einfach mit Enter. *apt* verbindet nun zur ausgewählten Quelle, lädt aktuelle Pakete nach und will zum Abschluss noch wissen, ob wir weitere Quellen hinzufügen wollen. Wir beantworten mit *Nein*, worauf die Konfiguration abgeschlossen ist.

Nun muss noch per Hand die Priorität der Quellen verändert werden. *pico /etc/apt/sources.list* veranlasst den Editor *pico* die Datei *sources.list* aus dem Verzeichnis */etc/apt/* zu laden.

Positionieren Sie den Cursor an den Beginn der Zeile die mit *deb file:///cdrom/* beginnt und drücken Sie die Tastenkombination STRG+K um die Zeile auszuschneiden. Begeben Sie sich nun mit dem Cursor ans Ende der Datei und drücken Sie STRG+U um die Zeile wieder einzufügen. Durch die Umstellung wird zuerst der Server im Internet befragt ob

```
deb http://ftp.at.debian.org/debian/ testing main non-free contrib
deb-src http://ftp.at.debian.org/debian/ testing main non-free contrib
deb http://security.debian.org/ stable/updates main contrib non-free
deb file:///cdrom/ sarge main
```

er Pakete bereit stellen kann, wird dieser nicht erreicht, wird von der lokalen Quelle im CD/DVD-Laufwerk installiert. Wollten Sie niemals Pakete von der lokalen Quelle installieren, so stellen Sie bitte an den Beginn der Zeile ein Raute-Zeichen (#). Der Eintrag wird somit ignoriert.

Offline und trotzdem aktuell

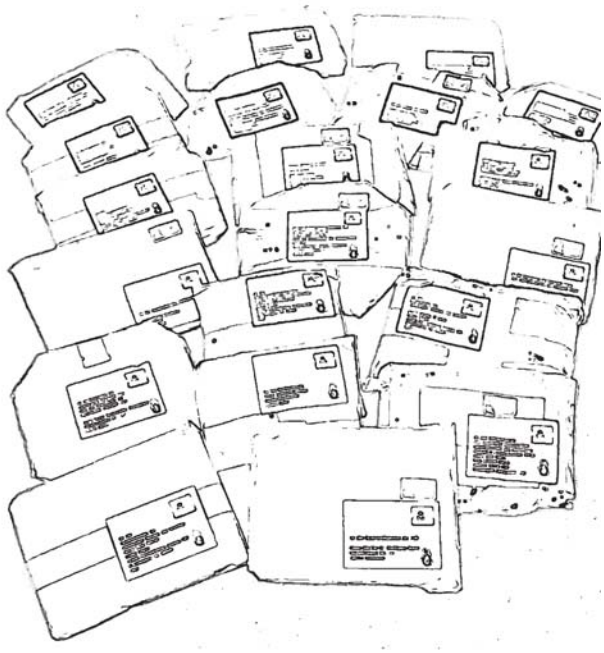
Erwähnenswert ist noch der Befehl *apt-cdrom*. Mit diesem Befehl können Sie zusätzliche CDs/DVDs einlesen und der *sources.list* hinzufügen. Gelegentlich wird dies benötigt, wenn Ihre WCM-Linux-Box ohne Internetanschluss ist und Sie trotzdem Pakete aktualisieren möchten die Sie zuvor an einem anderem Rechner herunter geladen haben.

Unsere Box weiß nun also woher Sie aktuelle Pakete bekommen kann. Welche Pakete in welcher Version sie beziehen kann, müssen wir sie erst einlesen lassen. *apt-get update* verbindet sich mit den Quellen die wir soeben konfiguriert haben und aktualisiert seinen Zwischenspeicher mit aktuellen Informationen. *apt-get update* sollte nur ein mal in 24 Stunden aufgerufen werden, um den Datenverkehr der Debian-Spiegelserver möglichst gering zu halten.

Der nächste Schritt wäre nun *apt-get install paketname* um ein Paket zu installieren. Da *apt-get* den genauen Paketnamen benötigt, wir jedoch keineswegs wissen können wie die Entwickler Ihre Pakete benennen, nehmen wir *apt-cache* zu Hilfe. *apt-cache search network* listet sämtliche Pakete auf, die in ihrer Beschreibung das Wort *network* haben. Kein Wunder dass diese Liste sehr lang ist.

Wir wollen nun eine kleine *apt*-Erweiterung, *apt-show-versions,* installieren. *apt-cache search apt* durchsucht den Cache nach sämtlichen Paketen die mit *apt* zu tun haben. Aus der ausgegebenen Liste suchen wir uns den richtigen Paketenamen und installieren dieses durch *apt-get install apt-show-versions.*

apt informiert ob andere Pakete, die zum Installationskandidaten in Abhängigkeit stehen, installiert oder aktualisiert werden müssen. Wenn dem so ist, müssen Sie mit *Y* die Installation bestätigen, oder mit *N* abbrechen. *apt* löst also Paket-Abhängigkeiten selbst auf! *apt* geht aber noch einen Schritt weiter und kann Pakte selbstständig entfernen die mit dem Installationskandidaten in Konflikt stehen. Natürlich werden Sie vor der Entfernung gewarnt und befragt was zu tun ist. Lesen Sie also die Ausgaben von *apt* genau durch bevor Sie antworten!



Nach erfolgten Sicherheitsabfragen installiert *apt-get* das Paket und seine Abhängigkeiten, aktualisiert seinen Programm-Cache und schließt die Installation gegebenenfalls mit einem optionalen Konfigurationsdialog ab. Fertig, Ihr erstes Paket ist installiert. Mit *apt-show-versions* erhalten Sie eine Liste der Installierten Pakete und deren Versionsnummer. Einschränken können Sie die Liste indem Sie die Suche mit dem Kommando *grep* filtern. *apt-show-versions | grep samba* listetet nur Pakete in deren Namen *samba* enthalten ist.

Neue Pakte warten

Nachdem seit der Veröffentlichung von Debian 3.1 Sarge schon einige Zeit ins Land gezogen ist, sind sicher schon einige installierte Pakte veraltet. Diese kann man nun in einem Rutsch auf den neuesten Stand bringen. Dazu reicht die Eingabe von *apt-get upgrade*. Es werden dadurch sämtliche installierte Programmversionen mit den aktuellen, durch *apt-get update* abgerufenen Versionen verglichen, eine Liste der Aktualisierungen und Abhängigkeiten erstellt und ausgegeben. Bei erstmaligem Aufruf beinhaltet die Liste mehr als 250 Pakete, die auch entsprechend schwer wiegen. 150 Megabyte an aktuellen Patches erfordern eine dicke Internetanbindung oder viel Zeit bis sich diese am Rechner befinden.

Beachten Sie, dass die ausgegebene Liste zweiteilig ist. Die obere Hälfte wird mit „Die folgenden Programme sind zurück gehalten worden:“ betitelt, die untere Hälfte beinhaltet Pakete die ohne weiteres installiert werden können. Sinn macht die Aufteilung deshalb, weil im oberen Teil Basisdienste und Systemprogramme betroffen sind. *apt* erreicht durch die Teilung dass Sie darauf aufmerksam werden, dass diese Dienste bei der Aktualisierung eventuell kurz unterbrochen werden könnten. Eine Aktualisierung dieser Pakte erreichen Sie mit dem Befehl *apt-get dist-upgrade*.

Nachdem die Pakte auf der WCM-Linux-Box gelandet sind, werden diese automatisch installiert. Einige der aktualisierten Pakte erfordern eine Konfiguration, weshalb Sie auch gleich die entsprechenden Dialoge präsentiert bekommen. Aus der Box „Konfigurationsdialoge“ können Sie die wichtigsten Einstellungen entnehmen.

Die Tastaturbelegung zur Steuerung von aptitude
Pfeiltaste nach unten / nach oben - Bewegt die Auswahl
Enter/Return - Klappt ein Verzeichnis auf/zu.

^ - Springt zum Verzeichnis, zu dem das Paket gehšrt.
+ - Markiert ein Paket zur Installation.
- - Markiert ein Paket zum Lšschen.
i - Zeigt die Beschreibung des Pakets an.
u - Aktualisiert die Liste der verfügbaren Pakete.
v - Zeigt die verfügbaren Versionen des Pakets an.
d - Zeigt die Abhängigkeiten des Pakets an.
g - Startet die Installation der ausgewählten Pakete.

Verschiedenen Hintergrundfarben innerhalb des Programmes erleichtern die Bedienung und haben folgende Bedeutung:

schwarz - Normalanzeige. Beim nächsten Installationsdurchlauf wird dieses Paket nicht verändert. Fett geschriebene Pakete sind bereits installiert.

grün - Das Paket wird installiert.

rot - Das Paket ist in einem unbrauchbaren Zustand oder kann nicht installiert werden.

hellblau - Das Paket wird mit einer neueren Programmversion aktualisiert.

weiß - Dieses Paket kšnnte aktualisiert werden, es wurde aber auf dem aktuellen Stand fixiert (hold).

rosa - Das Paket wird gelšscht.

Auch wird es passieren, dass neue Konfigurationsdateien mit dem Paket mitgebracht werden. Dann erhalten Sie eine Warnung und die Abfrage was mit der bisherigen Datei geschehen soll. Am Besten Sie schauen sich die Unterschiede zwischen der alten und neuen Datei durch drücken der Taste *d* an. Im darauf folgenden Fenster sehen Sie die Unterschiede markiert durch ein + und -. + kennzeichnet neue Zeilen, - kennzeichnet die vorhandene Datei. Außerdem wird durch die Zeichen @@ angegeben, welche Zeilen von der Änderung betroffen sind.

Eine weitere wichtige Operation ist das Entfernen von Paketen. *apt-get remove Paktename* entfernt das angegebene Paket, nicht jedoch ohne vorher die Abhängigkeiten bekannt zu geben. Falls Ihre Deinstallationsanweisung ein essentielles Paket betrifft, so werden die Abhängigkeiten derart viele sein, dass eine Deinstallation unmöglich wird.

Durch eine remove-Anweisung werden die Konfigurationsdateien meistens nicht entfernt. Dies kann sich dann schlecht auswirken, wenn Sie das Paket zu einem anderen Zeitpunkt neu installieren wollen und sich dann wundern warum nichts geht. Verwenden Sie daher den Zusatz —*purge remove* denn dann werden auch direkt abhängige Pakete sowie Konfigurationsdateien entfernt.

Die Pakete im Cache

Und wenn nach einem großen Update der Cache beinahe überquillt, so scheuen Sie bitte nicht davor von Zeit zu Zeit ein *apt-get clean* abzusetzen damit der Zwischenspeicher von nicht mehr benötigten Dateien gesäubert wird.

Sollte der Zwischenspeicher von apt einmal defekt sein, so kann dieser durch aufrufen von *apt-get check* wieder hergestellt werden. *apt* liest die Paketinformationen anhand der Datei */etc/apt/sources.list* erneut ein und gibt für eventuell nicht vorhandene Pakete eine Warnung aus. Anschließend wird das System analysiert. Für jedes Paket werden die Abhängigkeiten und Konflikte zu anderen Paketen geprüft und aufgelistet.

Sind Fehler aufgetreten, so können Sie versuchen diese mit dem Befehl *apt-get upgrade -f* zu beheben. Im schlimmsten Fall müssen Sie ein abhängiges Programmpaket manuell aus dem Internet downloaden und händisch installieren. Erste Anlaufstelle für die offiziellen Pakete ist *http://packages.debian.org/stable/*. Dort können Sie die einzelnen Bereiche nach dem gewünschten Paket durchsuchen.

Auf der detailierten Paket-Seite finden Sie dann sämtliche Abhängigkeiten und natürlich auch die Quellen von wo Sie das Paket beziehen können. Mit dem Befehl *wget http://ftp.at.debian.org/debian/pool/main/a/apt/apt_0.5.28.6_i386.deb* holen Sie zum Beispiel das Paket *apt* vom österreichischen Debian-Server in Ihr aktuelles Verzeichnis. Installieren können Sie es durch Eingabe von *dpkg -i apt_0.5.28.6_i386.deb.*

Wem die Befehlszeile zu mühsam ist, der kann sich auch gerne mit einer grafischen Installationshilfe auseinander setzen. Mit *aptitude* besteht die Möglichkeit, direkt bei der Paketauswahl die Paketbeschreibung zu sehen. Der Umgang ist ein bisschen gewöhnungsbedürftig, die wichtigsten Befehle sind in der Box aufgeführt. Wer sich im Softwaredschungel noch nicht so gut ausgekennt, hat mit *aptitude* ein gutes Werkzeug zur Hand, das auch gleich bei der Auswahl Konflikte und Abhängigkeiten anzeigt.

Debian bringt ein mächtiges und gleichzeitig einfaches Paketmanagement mit, dass natürlich auch automatisiert werden kann. *auto-apt* und *cron-apt* könnten für den Automatismus gesorgt werden - empfehlen möchte ich dies hier jedoch nicht. Wer nämlich nicht weiß welche Pakte ungefragt auf den Rechner gewandert sind, welche ausgetauscht oder installiert worden sind, tut sich bei einer Fehlersuche schwer. Außerdem erfordert es immer wieder Benutzereingaben bei der Installation die so unbeantwortet bleiben und weitere Updates verhindern. Es reicht also völlig aus, einmal im Monat längstens eine halbe Stunde Zeit zu investieren um den Update-Vorgang manuell zu starten und zu überwachen.

Und eines darf auf keinen Fall vergessen: *apt-get moo* sollte mindestens einmal täglich, am Besten vor Arbeitsbeginn, ausgeführt werden … ■

Die Antworten zu den Konfigurationsdialogen in alphabetischer Reihenfolge der Paketnamen ohne Anspruch auf Vollständigkeit:

Paketname	Auswahl
adduser	Nein
ca-certificates	Ja
cdrecord	nein
cupsys-bsd	Nein
cvs (Dialog 1)	Voreinstellung belassen
cvs (Dialog 2)	nein
debconf (Dialog 1)	Dialog
debconf (Dialog 2)	mittel
Exim v4 (Dialog 1)	Ja
Exim v4 (Dialog 2)	Voreinstellung belassen
Exim v4 (Dialog 3)	Voreinstellung belassen
Exim v4 (Dialog 5)	Voreinstellung belassen
man-db	nein
openssh-server	Nein
portmap	nein
smaba (Dialog 1)	deamons
samba (Dialog 2)	Ja
samba (Dialog 3)	Nein
uw-imapd (Dialog 1)	imap2 und ipmaps
uw-imapd (Dialog 2)	Nein

MySQL - Datenbank

Ein Schwergewicht leicht angewandt

Datenbanken umgeben seit jeher der Mythos, dass Sie schwer zu handhaben sind. Das stimmt dann, wenn es die Planung und Programmierung von großen Datenbanken geht, im kleinen Heim- oder Firmennetzwerk mit unter 50 Benutzern spielt dies jedoch eine untergeordnete Rolle. Durch diesen Artikel werden Sie in der Lage sein, das System einer MySQL-Datenbank zu verstehen und Sie auch administrieren zu können.

von Martin Müller

Den Begriff MySQL hat jeder der sich ein wenig mit Informationstechnologien beschäftigt schon gehört. MySQL ist ein Datenbank-Management-Sytem (DBMS), das 1994 von Michael „Monty" Widenius unter dem Aspekt eine möglichst schlanke und schnelle Datenbank zu schaffen entwickelt wurde. MySQL ist also ein ganzes Softwarebündel dass als Mittler zwischen der Datenbank und dem Benutzer dient. Es verfügt über einen verringerten Befehlssatz gegenüber anderen Datenbanken, spielt aber genau deshalb viele Vorteile gegenüber professionellen Datenbanksystem ein. Eine weitere Stärke von MySQL ist, dass sie relational ist, also dass Sie Tabellen untereinander in Beziehung stellen kann.

MySQL steht schon seit längerem unter der freien Lizenz GPL und ist sicher die verbreitetste Datenbank auf diesem Sektor. Ihre Schnelligkeit, Stabilität, Verfügbarkeit sowie breite Anwenderschaft sind ideale Voraussetzungen um diese Datenbank zur Grundlage für unsere WCM-Linux-Box zu machen.

MySQL setzt als Betriebssystem nicht zwingend eine Linux-Distribution voraus, sondern läuft auch auf anderen Plattformen wie MacOS X oder Windows. Die Datenbank zeigt sich sehr flexibel, weil Sie nicht nur einen einzigen Tabellentyp unterstützt, sondern mehrere Gleichzeitig. Dadurch erhöht sich die Möglichkeit unterschiedliche Sperrmechanismen oder sogar Transaktionen, wie sie bei extrem sicherheitskritischen Anwendungen erforderlich sind, einzusetzen. Die Bedienung der Datenbank erfolgt über die mitgebrachte Befehlszeile oder über einen Webserver der PHP-Scripten aufruft welche auf die Datenbank zugreifen können. Durch die von PHP zur Verfügung gestellte Schnittstelle kann man die Datenbank also über jeden Browser ansprechen. Eine wichtige Voraussetzung, da wir eine zentrale Datenbank benötigen werden.

Die Installation

Bevor wir die Datenbank ansprechen können, muss sie zunächst einmal installiert werden. Als Benutzer *root* an der Befehlszeile angemeldet, setzen wir den Befehl *apt-get install mysql-server mysql-client* ein, die Abfrage ob tatsächlich die beiden Pakete und deren Abhängigkeiten installiert werden sollen beantworten wir mit *ja*.

Die Debianentwickler haben das aktuelle Realease 5.0 als noch nicht stabil frei gegeben, weshalb wir mit der keineswegs schlechteren Version 4.1 arbeiten.

Bei der Installation werden die nötigen Verzeichnisse sowie Datenbank-Benutzer automatisch angelegt. Nach der Installation vergeben wir das root-Passwort für die Datenbank. Diese kann das Gleiche sein wie das root-Passwort für die WCM-Linux-Box. Wir empfehlen aus Sicherheitsgründen ein anderes zu wählen, da die Gefahr zu groß ist, dass bei einem Fehler in einem PHP-Script das Datenbankpasswort dem Anwender angezeigt wird.

mysqladmin -u root password 'SuperGeheim' weist dem Benutzer (-u) *root* das Passwort *SuperGeheim* zu.

Befehle die auch verstanden werden

Wir sind so weit, die Datenbank kann angesprochen werden. *mysql -u root -p* meldet uns als User *root* nach Eingabe des Passworts an der Datenbank an. Dass wir „in" der Datenbank arbeiten, erkennt man am Prompt der zu *mysql>* gewechselt hat. An der MySQL-Befehlszeile arbeitet man mit dem SQL-Syntax, der einem englischen Satz sehr ähnelt. *„SELECT vorname FROM angestellte WHERE vorname LIKE 'hannes'; „* sucht aus der Tabelle *angestellte,* aus deren Spalte *vorname* alle Einträge heraus, die den Inhalt *hannes* haben. Bitte beachten Sie dass Kommandos erst abgeschlossen sind, wenn Sie einen Semikolon (;) eingegeben haben! Sie können Befehle auch auf mehrere Eingabezeilen verteilen, ohne sie an die Datenbank zu senden. Erst der Semikolon veranlasst den Befehlsinterpreter die Anweisungen abzuarbeiten.

Sehen wir nun nach welche Tabellen MySQL schon mitbringt. *SHOW DATABASES;* zeigt uns *mysql* und *test* als bereits vorhanden an. *mysql* ist eine interne Tabelle die MySQL braucht um reibungslos zu funktionieren und in der man die Datenbank konfigurieren kann. Die Tabelle *test* ist als Spielwiese für erste Versuche gedacht.

Durch den folgenden kleinen Exkurs in den Befehlssatz von SQL werden Sie in der Lage sein, erste Versuche durchzuführen. Da wäre *USE test;* um eine Datenbank *test* zum Arbeiten auszuwählen, *CREATE TABLE angestellte (personalnr BIGINT NOT NULL PRIMARY KEY AUTO_INCREMENT, vorname VARCHAR(20), nachname VARCHAR (20));* legt in der aktuellen Datenbank eine Tabelle mit den Feldern *personalnr, vorname,* und *nachname* an. *vorname* und *nachname* sind Felder mit variabler Länge aber maximal 20 Zeichen lang, die *personalnr* wird durch *PRIMARY KEY* zum tabellenweiten einzigartigen Identifikationsmerkmal und bei jedem angelegten Datensatz automatisch um eins erhöht *(AUTO_ INCREMENT).* Weitere Merkmale von *personalnr* sind, dass das Feld nicht leer sein darf *(NOT NULL)* und dass es eine Ganzzahl ist *(BIGINT).*

Die Struktur

Die vorhandenen Tabellen lassen Sie sich durch *SHOW TABLES;* anzeigen, die Tabelle selbst wird durch *DESCRIBE Tabellenname;* ausgegeben. In die Tabelle tragen Sie Werte durch *INSERT INTO angestellte (personalnr, vorname, nachname) VALUES (1, 'Hannes', 'Schmidt')* ein. Bitte beachten Sie die Hochkommata bei den Namensangaben!

Wie Sie die Tabelle abfragen wurde weiter oben schon behandelt. †brigens lässt *DROP TABLE angestellte;* die Tabelle ohne Nachfrage im Datennirvana verschwinden. Sie verlassen die MySQL-Befehlszeile durch das Kommando *exit*.

Die MySQL-Datenbank ist nun eingerichtet, wir können lokal darauf zugreifen und damit arbeiten. Empfehlenswerte Lektüre die eine nähere Betrachtung Wert ist, finden Sie in englischer Sprache unter *http://dev.mysql.com/doc/refman/4.1/en/*.

In der nächsten Ausgabe wollen wir ein grafisches Web-Frontend installieren. ■

Reicht das Recht?

Sicherheitsgewinn durch Einschränkungen

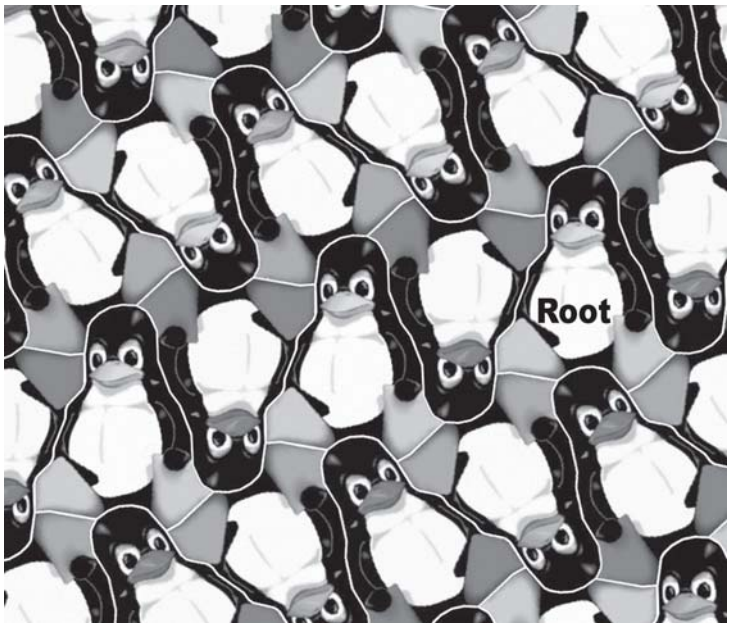
Die Benutzerwaltung an der Linux-Box ist eine heikle Angelegenheit. Durch unbedachte Benutzerwahl und großzügige Rechtevergabe öffnen sich Tür und Tor für Angreifer die im günstigsten Fall nur das System lahm legen wollen. Diesen und den schlimmste Fall, nämlich das Daten gestohlen oder manipuliert werden, wollen wir durch diese kurze Einführung jedenfalls unterbinden.

von Martin Müller

Bei jedem UN*X-basierenden Betriebsystem stellt die Rechteverteilung eine zentrale Stelle dar. Es werden schon bei der Installation im System Benutzer angelegt, die gewisse Rechte haben und somit Befehle ausführen oder nicht ausführen dürfen. Durch eine rigide Vergabe von Zugriffsrechten, lässt sich die Sicherheit am System immens erhöhen.

Jede Datei die unter Linux erstellt wurde, hat einen Eigentümer der wiederum einer Gruppe zugehört. So darf Benutzer A die Dateien von Benutzer B weder sehen noch verändern. Einige Linux-Distributionen verbieten Standard-Benutzern sogar, dass Sie auf die Internetschnittstelle *ppp0* zugreifen dürfen, weshalb diese Benutzer einer Gruppe zugeordnet werden müssen die dies darf (Gruppe *dailout*).

Sie erkennen schon: unterschiedliche Ressourcen wie Dateien oder Schnittstellen können für unterschiedliche Benutzer unterschiedlich zugänglich gemacht werden.



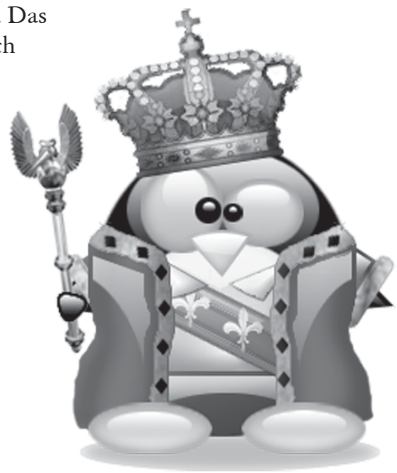
Eigenschaften einer Datei

Das liegt daran, dass für jede Ressource oder Datei Zugriffsbits gesetzt werden. Angezeigt werden diese, wenn Sie das List-Kommando *ls -la* ausführen. Durch den Zusatz *-l* wird tatsächlich in Listenform ausgegeben und durch *a* werden alle Dateien angezeigt. Sie erhalten eine Ausgabe die der in der Box *Verzeichnisliste* folgenden ähnlich ist.

Am Beginn der Zeile sehen Sie die in jeweils drei Gruppen unterteilte Rechtevergabe: Das erste Zeichen (d) ist nur dann gesetzt, wenn der Eintrag keine Datei, sondern ein Verzeichnis ist. Das Verzeichnis gehört natürlich auch jemanden, die zugewiesenen Rechte lesen durch die neun anschließenden Stellen aus.

Die ersten drei Stellen, die immer in der Kombination *rwx* anzutreffen sind, stehen für die Rechte die der Besitzer der Datei hat. *r* steht für Lesezugriff, *w* steht für die Schreibrechte, *x* steht für das Recht die Datei ausführen zu dürfen. Wird ein Bindestrich (-) angezeigt, so ist diese entsprechende Aktion nicht erlaubt.

Das zweite Triple steht für die Gruppe die der Datei zugehört, das letzte Triple zeigt die Rechte für alle anderen User an. Weiters sehen Sie in der Liste dass die Dateien alle dem User *martin* gehören und der Gruppe *staff* zugehörig sind. Somit dürfen alle



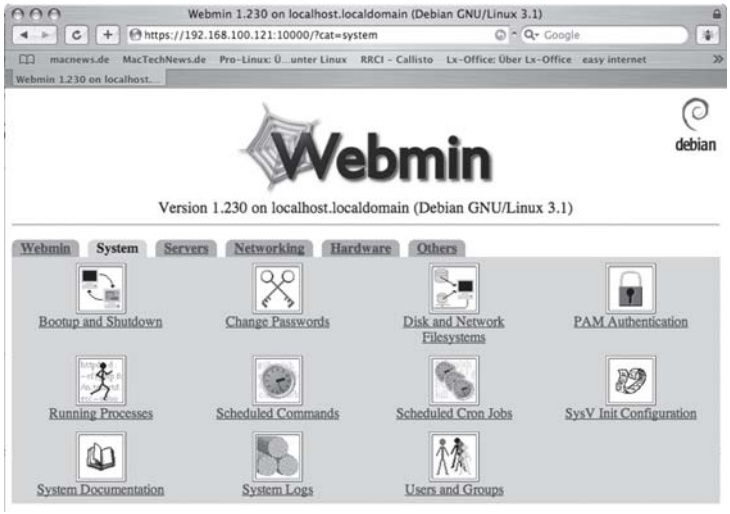
Was ist eine Datenbank?

Einfach verständliche Erklärung zu diesem Mysterium.

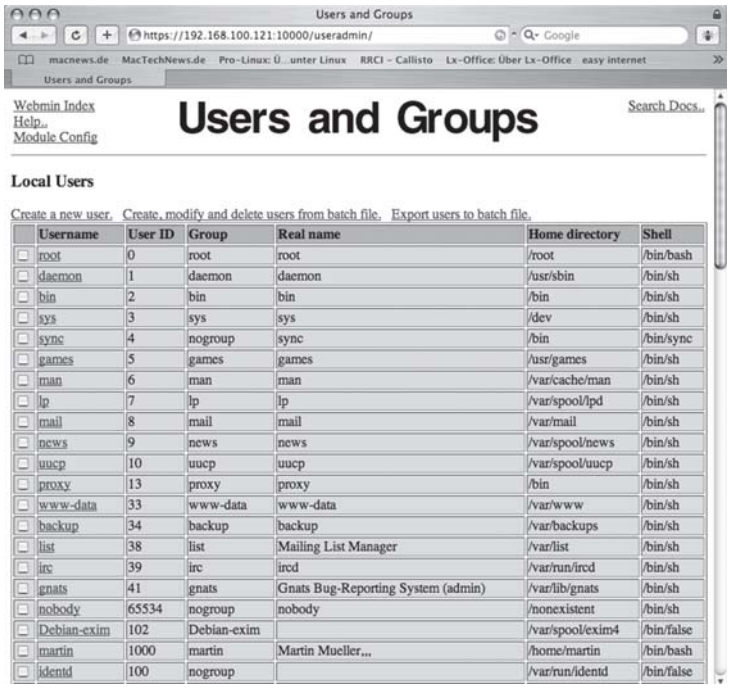
Eine Datenbank ist im übertragenen Sinne die elektronische Form eines Dokumentenschrankes. Sie enthält Daten und stellt diese dem Nutzer geordnet zur Verfügung. Um die Daten schnell zu finden wird ein Datenbankverwaltungssystem (engl. database management system, DBMS) benötigt. Dieses können sie sich wie einen Bibliothekar vorstellen, der genau weiss wo etwas abgelegt wurde und wie er die Bücher am besten ordnen muss. Das DBMS und die eigentlichen Daten der Datenbank (es können auch mehrere, verschiedene Datenbanken sein) nennt man Datenbanksystem (DBS).

Vergleicht man die Datenbank mit einem Dokumentenschrank, so kann man diesen ebenfalls in ein hierarchisches System unterteilen. In den einzelnen Regalen stehen Ringbuchordner und in diesen befinden sich wiederum Blätter auf denen Informationen stehen. Die einzelnen Ordner würden einem Datensatz entsprechen und die Informationen auf den Blättern wären schließlich Attribute.

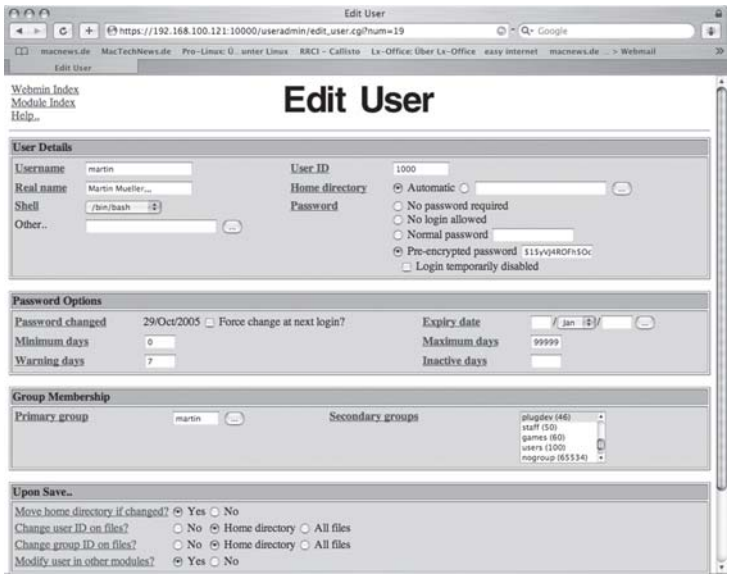
So wie die Ordner in Regalen stehen, so werden Datensätze zumeist in Tabellen gespeichert, wobei die Tabellen auch miteinander in Beziehung stehen können. So kann z.B. eine Tabelle Kundendaten mit Name, Adresse usw. haben und eine andere Produkte die gekauft wurden. *wan*



Webmins Abteilung zur Systemverwaltung



Das Interface zur Benutzer- und Gruppenverwaltung ist viel übersichtlicher als die entsprechenden Konfigurationsdatein



Die Detail-Seite des Webmin-Interface lässt wesentlich mehr Einstellungen zu, als die Systemtools zur Verfügung stellen.

Mitglieder der Gruppe *staff* die Dateien in diesem Verzeichnis lesen, nicht jedoch schreiben und ausführen.

root ist gottgleich?

Eine Besonderheit unter den Benutzern stellt *root* dar. Er darf grundsätzlich alles, auch wenn ihm die Ressource nicht gehört. Er kann Besitzer von Dateien ändern, Rechte vergeben, verändern und einschränken. Achten Sie bei der Vergabe von Rechten was Sie tun - setzen Sie für einen Systemdienst falsche Zugriffsrechte, kann es sein dass dieser nicht mehr ausgeführt wird und Sie das System zerstört haben.

Tägliche Vorgänge, wie neue Benutzer anlegen, sind auf der Kommandozeile recht schnell erledigt. Entweder sind Sie als *root* angemeldet, oder Sie setzen den Befehlen das Kommando *sudo* voran, welches Sie als *root* authentifiziert. Denn nur *root* darf neue User anlegen!

sudo adduser am Terminal abgesetzt, fragt zuerst nach Ihrem *root*-Passwort, anschließend werden Sie aufgefordert den Benutzernamen des neuen Users anzugeben. Es wird eine Gruppe für den Benutzer erstellt, der Benutzer selbst sowie sein Heimverzeichnis angelegt und gleich einige Konfigurationsdateien hinein kopiert. Zum Abschluss wird um sein gewünschtes Passwort gefragt. Die folgenden weiteren Angaben sind optional aber dennoch sinnvoll wenn diese ausgefüllt werden, da Sie im Falle eines Falles die Kontaktaufnahme mit dem neuen Benutzer erleichtern.

Ganz ähnlich läuft das Erstellen einer neuen Gruppe durch den Befehl *sudo addgroup* ab. Wollen Sie Benutzer einer weiteren Gruppen hinzufügen, so müssen Sie durch *pico /etc/group* die Gruppendatei editieren. Tragen Sie am Ende des entsprechenden Gruppeneintrags den Benutzer ein, der der Gruppe angehören soll. Wollen Sie mehrere Benutzer hinzufügen, so trennen Sie die Aufzählung durch einen Beistrich.

Dateirechte im Wechsel

Um Dateirechte zu manipulieren, gibt es drei Befehle. Mit *chown root test.txt* (*Ch*ange*Own*er) setzen Sie den Eigentümer der Datei *test.txt* auf *root*, *chgrp* arbeitet nach dem selben Muster für die Gruppenzugehörigkeit.

chmod verändert die Rechte an der Ressource. Abkürzungen für den Eigentümer (*u* User), die Gruppe (*g* Group), Andere (*o* Other) und alle (*a All*) folgen Anweisungen was zu tun ist. Mit Plus (+) erteilen Sie Rechte, mit Minus (-) entziehen Sie Rechte. *chmod a+r test.txt* vergibt somit für alle den Lesezugriff auf die Datei test.txt. *chmod go-rwx test.txt* entzieht der Gruppe und allen Anderen sämtliche Rechte.

Webmin machts

Da wir zu Beginn des Workshops die grafische Adminstrationshilfe *Webmin* installiert haben, können wir von jedem Rechner aus dem internen Netz darauf zugreifen. Durch Eingabe von https://192.168.123.1 in einem Internetbrowser gelangen wir zum Anmeldebildschirm wo wir uns als *root* anmelden.

Nach erfolgter Anmeldung gehen Sie in die Rubrik *System,* das letzte Symbol *Users and Groups* ist die Benutzerverwaltung.

Soviel zur Grundlagen der User- und Gruppenfunktionen. Wir werden in Zukunft aus Sicherheitsgründen auf eine datenbankbasierende Alternative setzten, die das unter Windows übliche ActiveDirectory vorerst ersetzen soll.

Grund dafür ist, das jeder Benutzer der irgendwie auf die WCM-Linux-Box zugreifen will, ein Benutzerkonto haben muss. Gelingt es nun einen Angreifer Benutzernamen und Passwort eines Benutzers zu ergattern, könnte er Dateien mit bösartigem Code in dessen Heimverzeichnis ablegen und von dort aus das System infiltrieren. Um dies zu umgehen verwenden wir eine MySQL-Tabll e in der sämtliche Benutzer, sozusagen virtuell, angelegt sind.

Ein voller Ersatz für ActiveDirectory ist diese Methode nicht, die richtige Konkurrenz zur Microsoft-Implementierung wäre das LDAP-Protokoll, welches wir zu einem späteren Zeitpunkt behandeln wollen. Bitte beachten Sie deshalb den MySQL-Artikel in dieser Ausgabe. ■