

Link: <https://www.tecchannel.de/a/workshop-linux-hardening,2034441>

Systeme grundlegend absichern Workshop: Linux-Hardening

Datum: 28.07.2011
Autor(en): Thomas Steudten

Die Optionen von Linux sind sehr vielschichtig. Unzählige Pakete sind verfügbar, Benutzerverwaltung, Netzwerk- und Dateizugriff lassen sich oft beliebig konfigurieren. Doch wer darf was, und welche Komponenten werden überhaupt benötigt? Linux-Hardening widmet sich speziell dieser Frage, um das System möglichst sicher zu machen.

Ein Linux-System in der Funktion als Server bietet zahlreiche Netzwerk-Services an. Zwar werden nicht alle gebraucht, doch sie bieten einen recht freien Zugriff auf Ressourcen. Und auch ein benötigter Service sollte nicht jedem System und Benutzer den Zugriff erlauben.

Nachdem ein grundlegender Funktionstest erfolgreich durchlaufen ist, empfiehlt es sich im nächsten Schritt, das Linux-System an die Bedürfnisse anzupassen. Allgemein spricht man hier im anglizistischen Sprachgebrauch von "Customizing" oder speziell von "Hardening", wenn das System wirklich nur die vorgegebenen Aufgaben und Anforderungen erfüllen soll. Es sollten also nur die notwendigen Prozesse mit minimalen Rechten aktiv sein.

[Hinweis auf Bildergalerie: **Bildergalerie: Linux-Server-Distributionen**] ^{gal1}

Grob kann man den Zugriff auf ein Linux-System differenzieren nach dem Zugriff von außen auf das System (über die lokale Konsole oder das Netzwerk), dem ausgehenden Netzwerkverkehr und den erlaubten Aktionen auf dem System (von innen). Deaktivieren wir das Netzwerk-Interface, so kann ein Benutzer, der Zugriff zum System über die Konsole erhalten hat, noch Daten manipulieren oder über die vorhandenen I/O-Schnittstellen (USB, Firewire, FiberChannel, eSata) diese kopieren.

1. Hardening

Ein IT-System mit dem Betriebssystem Linux sicherer zu machen ermöglicht auch einen Blick hinter die Kulissen, und dabei kann man einige grundlegende Fragen beantworten:

- Was wird benötigt?
- Was läuft wann auf dem System?
- Welche Logins existieren? Sind Passwörter gesetzt oder Accounts gesperrt?
- Wie erfolgt der Netzwerkzugriff von und zu welchen Ports?
- Wie erfolgt der Aufruf des Prozesses und in welchem Kontext?
- Welche Zugriffsrechte werden benötigt?
- Wer darf was auf diesem System?

Einem Desktop-System mit immer dem gleichen Benutzer braucht man in der Regel keine restriktiven Vorgaben zu machen. Aber auch hier gilt: Je restriktiver, desto sicherer. Zudem lässt sich eine "Stateful"-Firewall, wenn diese schon im Kernel vorhanden ist, mit einfachen Mitteln in kurzer Zeit aktivieren.

Grundsätzlich zeigt sich, dass über die Jahre die Linux-Distributionen restriktiver mit Ressourcen und Zugängen umgehen. Der X11-Window-Server erlaubt keinen oder nur lokalen Netzwerkzugriff, die Firewall gestattet lediglich eingehende Antwortpakete, der Nameserver verrichtet seine Tätigkeit in einem Chroot-Umfeld, und viele privilegierte Prozesse verwerfen ihre Rechte.

2. Aus der Praxis

Ein Prozess mit Root-Rechten (privilegierter Prozess), der vollen Zugriff auf das Dateisystem hat und an keine Prozesslimits stößt, ist für viele Applikationsentwickler der Idealfall. So braucht man sich im Vorfeld keine Gedanken über Zugriffsrechte und Isolation zu machen.

Allerdings gibt es dafür eine Reihe von Nachteilen:

- **Ressourcen:** Jedem Prozess werden standardmäßig nur begrenzte Ressourcen (etwa Speichernutzung, Datei-Handles oder Rechenzeit) zugewiesen, die sich per "ulimit" ansehen und modifizieren lassen. Die Softlimits lassen sich bis zum Hardlimit ausreizen, und viele Werte sehen als Vorgabe "unlimited", also nicht begrenzt, vor. Als Benutzer mit Root-Rechten kann man aber auch die Hardlimits entsprechend mit zum Systemmaximum inkrementieren, sodass eine eigentliche Begrenzung für das System nicht mehr zum Tragen kommt.
- **Dateisystem - reservierte Blöcke:** Die meisten Dateisysteme reservieren eine Anzahl an Blöcken für Prozesse mit der Benutzer-ID 0. Ein nicht privilegierter Prozess sollte also niemals in der Lage sein, ein Dateisystem zu 100 Prozent zu füllen, wenn diese Reserve vorhanden ist. Ein Prozess, der mit Root-Rechten gestartet wurde und diese auch nicht verändert, kann diese reservierten Blöcke ebenfalls nutzen, was ein Eingreifen des Systemadministrators massiv erschwert, da im Dateisystem kein freier Platz mehr vorhanden ist, der für einen normalen Betrieb notwendig wäre.
- **Dateisystem - Quota:** Mit Quota bezeichnet man ein Accounting für die Nutzung von Dateiblöcken und I-Nodes pro Benutzer- und Gruppen-ID. Es wird auch hier nach Soft- und Hardlimits differenziert, wobei Letzteres nach dem Überschreiten des (größeren) Softlimits für eine vorgegebene Zeit zur Anwendung kommt.
- Zwar lassen sich auch für den User "Root"-Quotalimits auf Dateisystemebene setzen, aber wenn eine Datei keinem definierten Benutzer oder Daemon-Account zugeordnet wurde, ist der Eigentümer meist "Root", und damit fallen dann sehr viele Dateien unter das Accounting. Von daher betrachtet empfiehlt es sich kaum, dieses Limit zu setzen.
- **Zugriffsrechte:** Der Prozess mit der Benutzer-ID 0 hat auch vollen Zugriff auf alle lokalen Dateisysteme, kann daher leicht vieles löschen, Prozesse starten oder beenden. Die klassische Zugriffskontrolle mit "Root darf alles", ist daher ein Risiko. Eine erweiterte Zugriffskontrolle, wie beispielsweise bei Security Enhanced Linux (SELinux) oder AppArmor, bietet hier auch die Möglichkeit, diese Zugriffe zu kontrollieren. Allgemein sollten Prozesse, wann immer möglich, nicht mit den vollen Rechten im System (UID und/ oder GID=0) aktiv sein. Denn sollte es einem anderen Prozess oder Benutzer möglich sein, über den privilegierten Prozess Aktionen auszuführen, so erfolgt dies ohne Restriktionen. Dies wird noch oft beim sogenannten Buffer-Overflow, das heißt dem Überschreiben von Daten und Ausführen von Programmcode auf dem Stack, ausgenutzt.

3. Privilegien

Linux- wie auch traditionelle Unix-Implementierungen unterscheiden nach privilegierten (effektive Benutzer-ID ist null) und nicht privilegierten Prozessen. Erstere umgehen die meisten Kernel-Zugriffskontrollen. Die anderen durchlaufen die vollen Zugriffskontrollen, basierend auf den Prozessrechten (normalerweise: die effektive UID, effektive GID und zusätzliche Gruppenzugehörigkeit).

Seit Kernel 2.2 unterteilt Linux die privilegierten Zugriffsrechte, den sogenannten Capabilities, die auf Thread-Basis unabhängig voneinander de- und aktiviert werden können.

4. Ansatzpunkte für Hardening

Möchte man ein Linux-System härten, so bieten sich nachfolgende Ansatzpunkte an:

Netzwerk:

- Kommunikation ausschließlich über Sockets oder Localhost für lokalen Zugriff
- tcp-wrapper, xinetd und Applikations-Zugriffsrestriktionen nutzen
- Integrierte Firewall 'iptables' eingehend nur für notwendige Ports und Protokolle öffnen
- Syslog- und Audit-Protokolle aktivieren und auf einem anderen System kopieren
- Unsichere Protokolle und Services durch sicherere Ausführungen ersetzen

Prozesse:

- Nur notwendige Prozesse starten
- Prozesse nicht als root (uid=0) laufen lassen, sondern als unprivilegierte Prozesse
- Prozess-Limits (ulimits) für Speicher, Anzahl Datei-Handles, Prozesslaufzeit usw. nutzen
- Prozesse in einer Chroot-Umgebung einrichten
- Virtualisierung nutzen (qemu, kvm, xen, lxc)

Ressourcen:

- AppArmor oder SELinux aktivieren
- ACLs einsetzen
- Mandatory Access Controls (MAC)
- I/O-Ports über den udev-daemon deaktivieren

5. Hardening: Virtualisierung & SELinux

Die Linux Container (lxc) bieten die Möglichkeit, einzelne Prozesse oder ein vollständiges Betriebssystem vom laufenden System zu isolieren und eine Ressourcensteuerung zu implementieren.

Auch andere Virtualisierungslösungen wie qemu, KVM, XEN oder VMware trennen das laufende System vom Gastsystem und bieten so zwar einen erhöhten Verwaltungsaufwand, aber eine gewisse Isolierung ist vorhanden.

6. SELinux

Sind Dateien und Verzeichnisse beim Einsatz von SELinux korrekt mit einem Label versehen, dann wird jeder Zugriff überwacht. Aktivieren lässt es sich zu jeder Zeit per "setenforce enforcing", wobei hier zwischen den beiden Modi gewechselt wird. Der Vorgang "labeln" ordnet jedem Dateiojekt einen Kontext zu, beispielsweise "f_tmp" für Prozesse und Verzeichnisse, die nach /tmp oder /var/tmp schreiben dürfen.

Zwei wesentliche Modi kommen hier im täglichen Betrieb vor:

- permissive
- enforced

Der Permissive-Modus unterscheidet sich vom Enforced-Modus dadurch, dass dieser einen Zugriff zwar überwacht und loggt, aber nicht verweigert. Auch kann SELinux so konfiguriert werden, dass der Modus erst nach einem Neustart geändert werden kann.

Konfigurationsdateien für SELinux finden sich unter /etc/selinux.

7. Hardening: tcpwrapper, xinetd & udev

Bei Netzwerkdiensten, die nicht über den `inetd` beziehungsweise `xinetd` gestartet werden und sich somit der einfachen Zugriffskontrolle und -überwachung dort entziehen, lässt sich die Konfiguration meist über `tcpwrapper` aktivieren. Ob ein Prozess diese Methoden nutzen kann, verrät ein Blick in die Manualseite; man kann aber auch nachsehen, ob die notwendige Shared-Library - sinngemäß "libwrap"-- eingebunden ist.

```
# ldd /usr/sbin/snmpd | grep --color libwrap
```

```
libwrap.so.0 => /lib64/libwrap.so.0
```

Die Zugriffssteuerung erfolgt hierbei im Wesentlichen über zwei Konfigurationsdateien im /etc-Verzeichnis:

- /etc/hosts.allow
- /etc/hosts.deny

Deren Aufbau ist durch folgende Zeile charakterisiert:

```
Prozessnamen : System [ : shell_command]
```

8. xinetd

Über die Konfigurationen des neuen Superdaemons `xinetd` kann der Zugriff auf einen Netzwerkservice vielfältig beschränkt und überwacht werden. Eine White- oder Blacklist (`only_from`, `no_access`) für IP-Adressen, Host-Namen und Netzwerknamen, ein Zeitfenster (`access_times`) oder eine Zugriffssperre bei hoher Systemlast (`max_load`) sind nur einige davon. Ein erfolgreicher oder misslungener Zugriff kann ebenso geloggt werden. Die Möglichkeit, den neuen Prozess mit anderer User- und Gruppen-ID auszuführen, sollte man nutzen. Mit der `"bind/interface"`-Option kann der Service auf ein definiertes Netzwerk-Interface fixiert und so beispielsweise der Zugriff über `telnet` nur aus dem LAN heraus aktiviert werden.

Bei einem Stand-alone-Daemon, der seinen I/O-Verkehr nicht über die Dateihandle `stdin` und `stdout` abwickelt, bleibt nur die Möglichkeit, über den `tcpwrapper` oder letztendlich über die Firewall eine Zugriffskontrolle zu implementieren. Die Möglichkeit, über `openSSH` einen Tunnel aufzubauen, erschwert die Kontrolle der Zugriffe.

Wenn möglich, sollte ein Netzwerkservice immer auf den Host-Namen `"localhost"` beziehungsweise die IP `127.0.0.1` oder das Interface `"lo"` gebunden werden. Denn nur so ist ein Zugriff darauf ausschließlich vom gleichen System möglich, und es können auch Firewall-Regeln mit dem Interface `"lo"` definiert werden.

9. udev

Wurden die sogenannten Device-Knoten im Verzeichnis `"https://www.computerwoche.de/dev"` vor einiger Zeit noch statisch per `"mknod"` angelegt, übernimmt dies heute der `"udev"`-Daemon. Dieser ist in der Lage, anhand von speziellen Merkmalen der Hardware, wie Hersteller, Seriennummer oder Typ, den Device-Knoten immer mit dem gleichen Namen und der gleichen Major- und Minor-Nummer anzulegen, auch wenn Letztere in neueren Kernels keine große Rolle mehr spielen.

Die Systemregeln unter `/lib/udev/rules.d` können durch eigene Regeln unter `/etc/udev/rules.d` ersetzt und somit auch deaktiviert werden.

10. Secure Shell (SSH)

Die Secure Shell ist mittlerweile der De-facto-Standard, wenn es um Remote-Logins, Port-Weiterleitung, `secure-ftp` und Tunneling geht. Von daher sollte SSH gegenüber `telnet`, `rlogin` und `ftp` bevorzugt werden.

Die Konfiguration erfolgt über die Dateien im Verzeichnis `/etc/ssh/`:

- für den Serverprozess: `/etc/ssh/sshd_config`
- für den Client: `/etc/ssh/ssh_config`

Die eigenen Keys finden sich dann im Home-Verzeichnis `$HOME/.ssh` und heißen normalerweise je nach Schlüssel-Type `id_rsa*` und `id_dsa*` für die privaten Schlüssel und tragen die Endung `".pub"` für die öffentlichen Schlüssel.

Über die Konfigurationsdatei `config` kann jeder Benutzer noch individuelle Einstellungen vornehmen. In der Datei `known_hosts` merkt sich der Client-SSH die kontaktierten Systeme in Form des öffentlichen Systemschlüssels aus `/etc/ssh/ssh_host*.pub`. Der SSH-Client würde also bemerken, wenn sich ein Host-Schlüssel verändert hat, und somit eine Man-in-the-Middle-Attacke erkennen.

Ist der Zugriff für ein oder mehrere Systeme auf einen IP-Port über die IP-Adresse oder die Host-Namen per `tcpwrapper`, `xinetd`-Konfiguration oder die `iptables`-Firewall freigeschaltet, sollte man auf jeden Fall die Applikation und die Services individuell für die notwendigen Zugriffsarten konfigurieren. Für die Secure-Shell (SSH) empfiehlt es sich, nur den Zugriff über die vorher generierten Schlüssel (Public/ Private Keys) zu erlauben und die interaktive Passwort-Authentifizierung zu verbieten:

```
PasswordAuthentication no
```

```
UsePAM no
```

Die Verzeichnisrechte auf `$HOME/.ssh` sollten restriktiv gesetzt werden, ansonsten verweigert der SSH-Daemon schon mal den erwarteten Login über den öffentlichen Key (Option "StrictModes yes").

11. Capabilities

Neben einer `chroot`-Umgebung und dem Ausführen unter einer Benutzer- und Gruppen-ID größer null kann ein Prozess noch selektiv seine Freiheiten begrenzen. Die `Capabilities`, das heißt die Rechte eines privilegierten Threads, kann dieser je nach Bedarf deaktivieren und somit seine Privilegien begrenzen. Die Liste der möglichen `Capabilities` wächst mit der Zeit.

Als Beispiel kann ein Prozess oder auch Thread, der mit der effektiven Benutzer-ID 0 gestartet wurde und das Privileg "CAP_NET_BIND_SERVICE" deaktiviert hat, sich nicht mehr auf einen Netzwerk-Port unterhalb der Port-Nummer 1024 binden.

12. Fazit

Mit wenig Aufwand lässt sich in aktuellen Distributionen das Linux-System den Bedürfnissen anpassen und auch gleich besser absichern. Auch wenn der Aufwand für den Betrieb dafür größer ist, das Resultat rechtfertigt diesen in jedem Fall.

Ein System-Hardening über die integrierte Firewall, den Zugriffsschutz über `tcpwrapper` oder den `Inet-Superdaemon` sollte heute eine Selbstverständlichkeit sein. (cvi)

Bildergalerien im Artikel:

[gal1](#) **Bildergalerie: Linux-Server-Distributionen**

Die Standard-Installation von Red Hat Enterprise Linux ist eine grundlegende Server-Installation. Sie können jetzt optional ein anderes Software-Set wählen.

Basis-Server
 Datenbank-Server
 Web-Server
 Virtueller Host
 Desktop
 Software-Entwicklung-Workstation

Bitte wählen Sie alle zusätzlichen Repositories, die Sie für die Softwareinstallation verwenden möchten.

Hochverfügbarkeit
 Lastverteiler
 Red Hat Enterprise Linux
 Resilient Storage

+ Zusätzliche Software-Repositories hinzufügen

Repository ändern

Sie können die Software-Auswahl jetzt weiter anpassen, oder nach Fertigstellung der Installation via Software-Verwaltung-Anwendung.

Später anpassen Jetzt anpassen

← Zurück

→ Weiter

RHEL - Einsatzgebiet

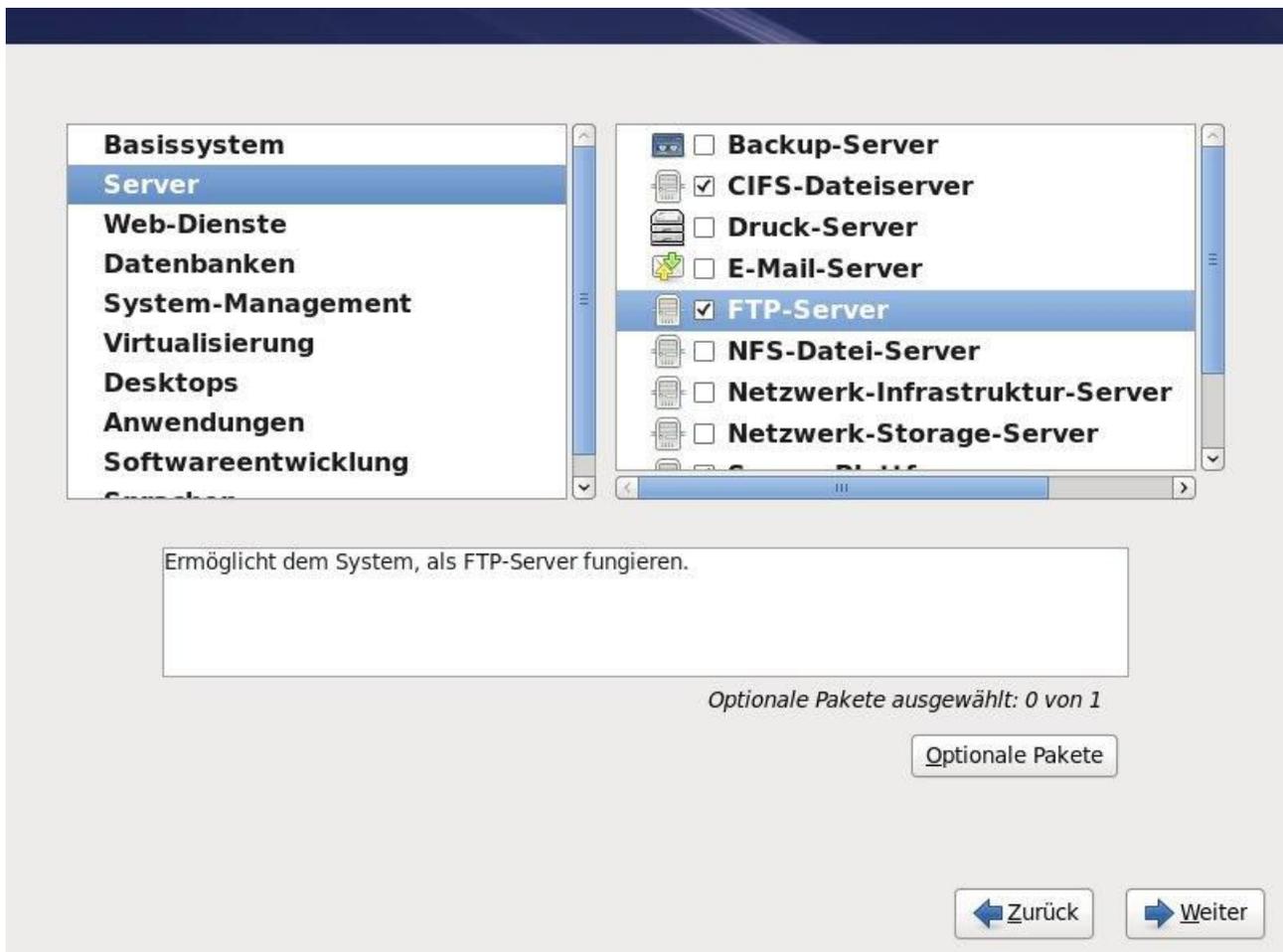
Welche Art von Server bestimmen Sie in dieser Maske.

Foto: Jürgen Donauer



Empfehlenswerte Linux-Distributionen für Server.

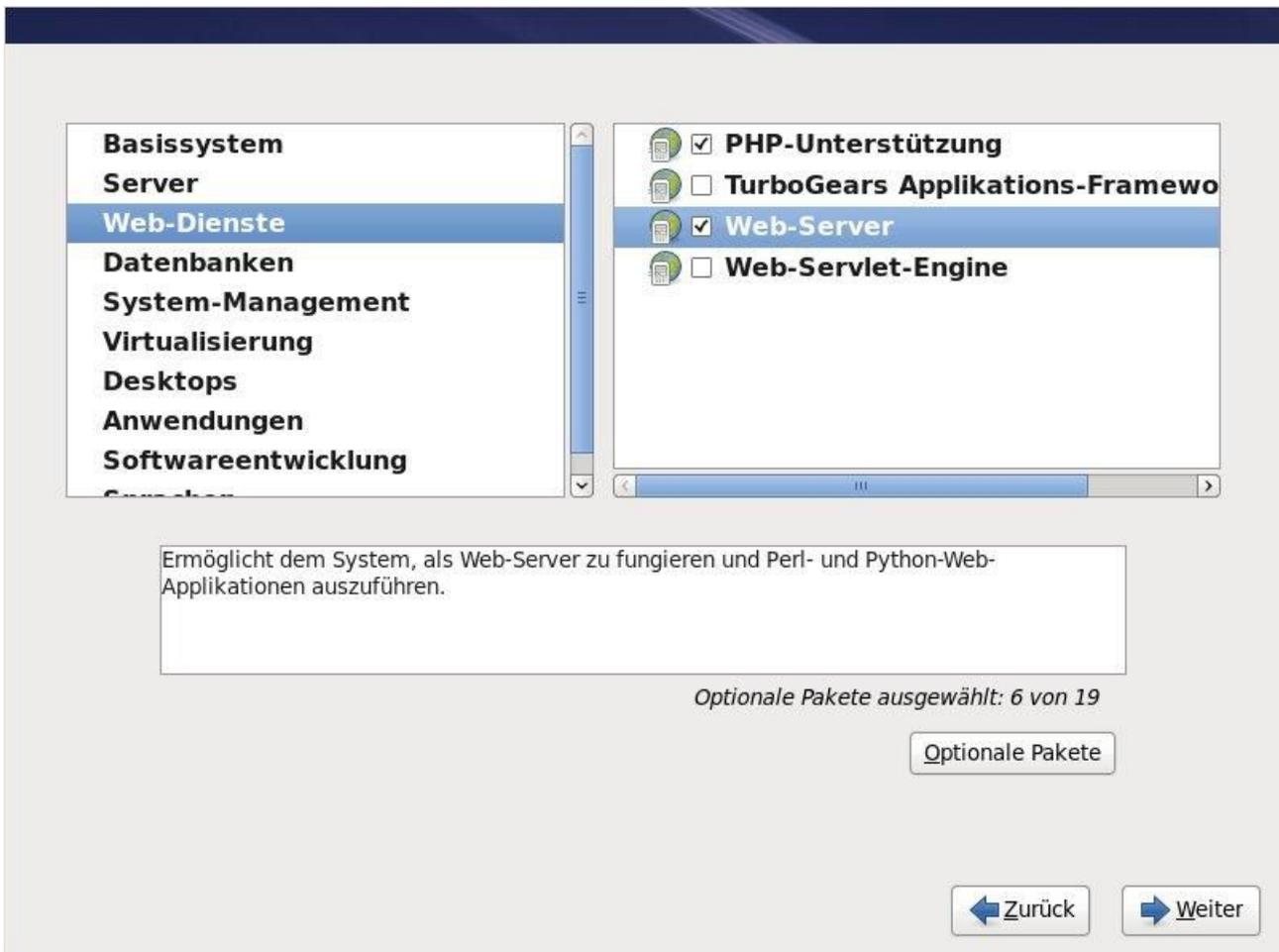
Foto: fotolia.com/julien tromeur; Strato



RHEL - Mehrwert

Sie können bereits während der Installation Zusatzpakete angeben und einspielen lassen.

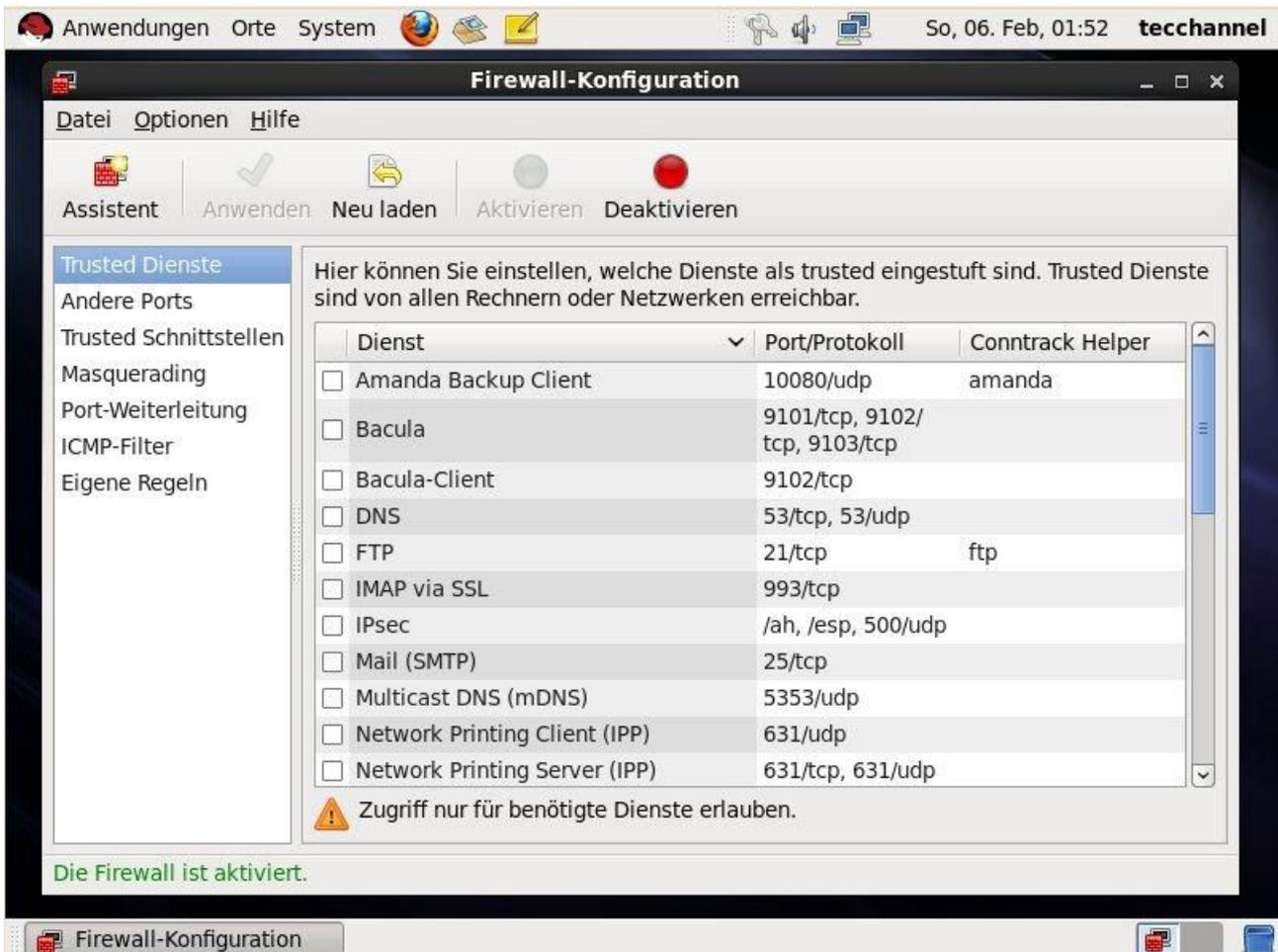
Foto: Jürgen Donauer



RHEL - Webserver

Beim Basis-Server ist die Webunterstützung per Standard nicht dabei.

Foto: Jürgen Donauer



RHEL - Grafisch

Sollten Sie eine grafische Benutzeroberfläche installiert haben, gibt es auch entsprechende Administrationswerkzeuge.

Foto: Jürgen Donauer

Welche Art von Installation bevorzugen Sie?

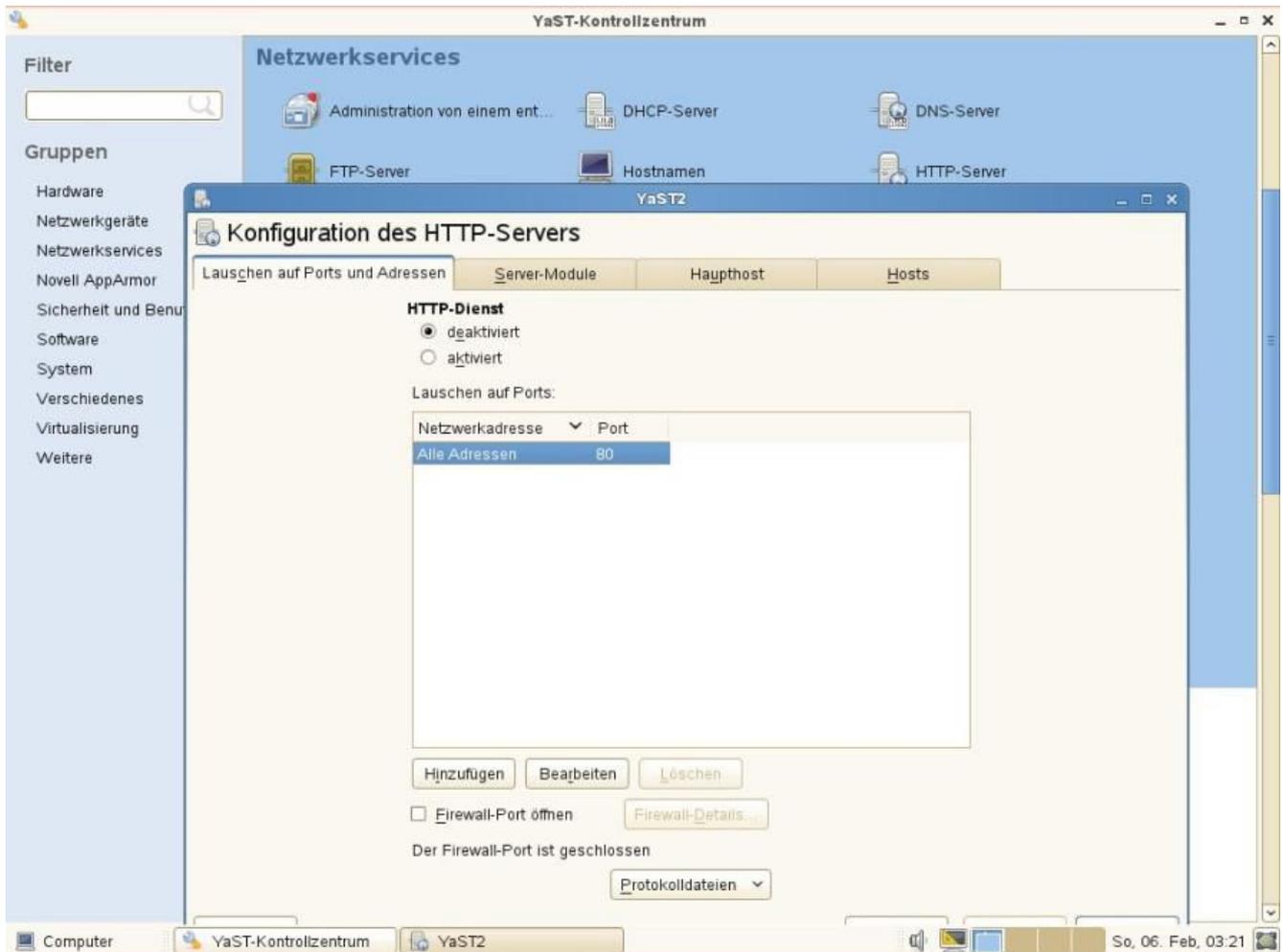
-  **Gesamten Platz verwenden**
Entfernt alle Partitionen auf den ausgewählten Laufwerk(en). Beinhaltet auch Partitionen, die von anderen Betriebssystemen erstellt wurden.
Hinweis: Diese Option löscht alle Daten von den ausgewählten Laufwerk(en). Eine Sicherung der Daten wird empfohlen.
 -  **Bestehende(s) Linux-System(e) ersetzen**
Entfernt nur Linux-Partitionen (die von einer vorherigen Linux-Installation erstellt wurden). Entfernt nicht andere Partitionen auf Ihren Laufwerk(en) (z.B. VFAT oder FAT32).
Hinweis: Diese Option löscht alle Daten von den ausgewählten Laufwerk(en). Eine Sicherung der Daten wird empfohlen.
 -  **Aktuelles System verkleinern**
Verkleinert die bestehenden Partitionen um freien Platz für die Standard-Partitionierung zu schaffen.
 -  **Freien Platz verwenden**
Behält Ihre momentanen Daten und Partitionen bei und benutzt nur den unpartitionierten Platz auf den ausgewählten Laufwerk(en), vorausgesetzt, es ist genügend freier Platz zur Verfügung.
 -  **Maßgeschneidertes Layout erstellen.**
Manuelles Erstellen eines eigenen Layouts auf den ausgewählten Laufwerken mit Hilfe des Partitionswerkzeuges.
- System verschlüsseln
- Partitions-Layout noch einmal überprüfen und ändern

 Zurück

Weiter 

RHEL - Platzwahl

Hier partitionieren Sie das System.
Foto: Jürgen Donauer



Novell SLES - Webserver

In dieser Maske können Sie Apache konfigurieren.

Foto: Jürgen Donauer



Novell SLES - Sicherheit

SLES setzt auf AppArmor, das Sie ebenfalls grafisch administrieren können.

Foto: Jürgen Donauer

Boot from Hard Disk

Installation

Repair Installed System

Rescue System

Check Installation Media

Firmware Test

Memory Test

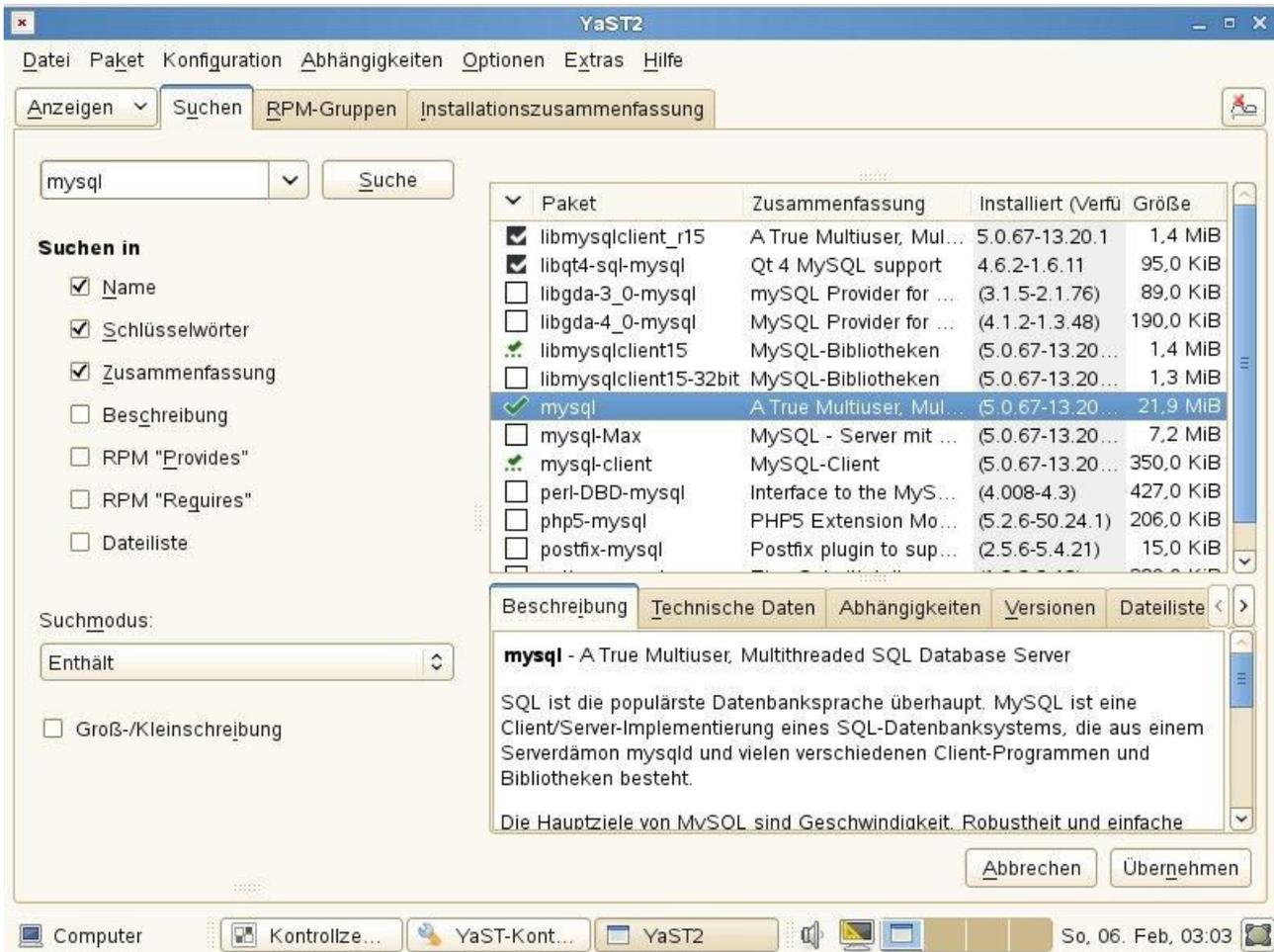
Boot Options |

F1 Help F2 Language F3 Video Mode F4 Source F5 Kernel F6 Driver
English (US) 800 x 600 CD-ROM Default No

Novell SLES - Startbildschirm

Der erste Bildschirm von SUSE Linux Enterprise Server.

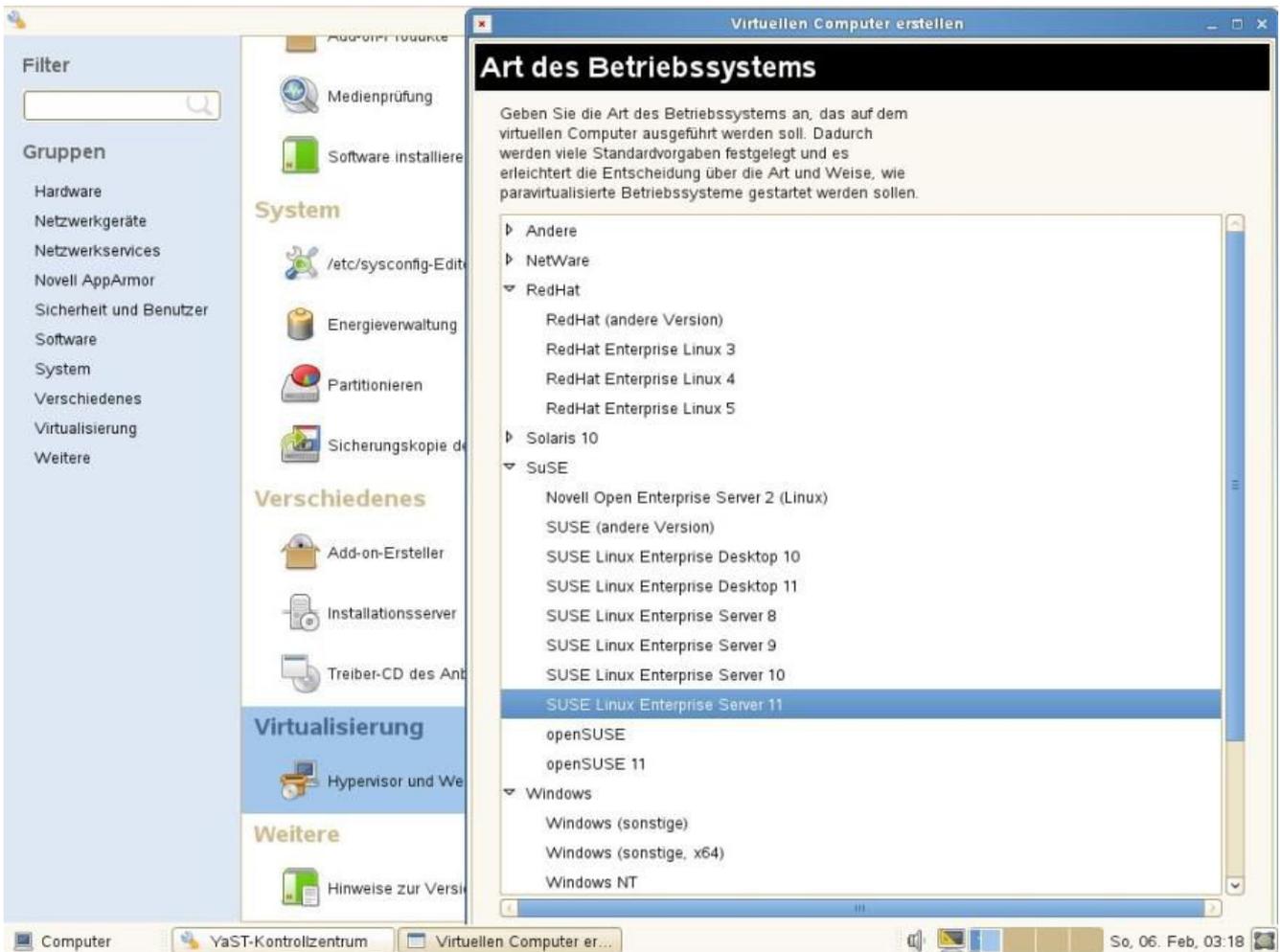
Foto: Jürgen Donauer



Novell SLES - YaST

Yet another Setup Tool ist das Rückgrad der Linux-Distribution.

Foto: Jürgen Donauer



Novell SLES - Virtualisierung

Welches Betriebssystem hätten denn gerne?

Foto: Jürgen Donauer



Ubuntu

Auch die Server-Variante lässt sich auf Deutsch installieren.

Foto: Jürgen Donauer

[!] Select a language

Die Übersetzung des Installers ist für die gewählte Sprache nicht ganz vollständig.

Die Wahrscheinlichkeit, dass Sie auf einen Dialog treffen, der nicht in die ausgewählte Sprache übersetzt ist, ist sehr klein, kann aber nicht komplett ausgeschlossen werden.

Die Installation in der gewählten Sprache fortsetzen?

<Zurück>

<Ja>

<Nein>

<Tab> Nächste Option <Leertaste> Auswählen <Enter> Knöpfe aktivieren

Ubuntu - Sprache

Allerdings ist die Übersetzung laut eigenen Angaben noch nicht vollständig.

Foto: Jürgen Donauer

[!] Netzwerk einrichten

Bitte geben Sie den Namen dieses Rechners ein.

Der Rechnername ist ein einzelnes Wort, das Ihren Rechner im Netzwerk identifiziert. Wenn Sie Ihren Rechnernamen nicht kennen, fragen Sie den Netzwerkadministrator. Wenn Sie ein lokales Heimnetz aufbauen, ist es egal, was Sie angeben.

Rechnername:

ubuntu-server

<Zurück>

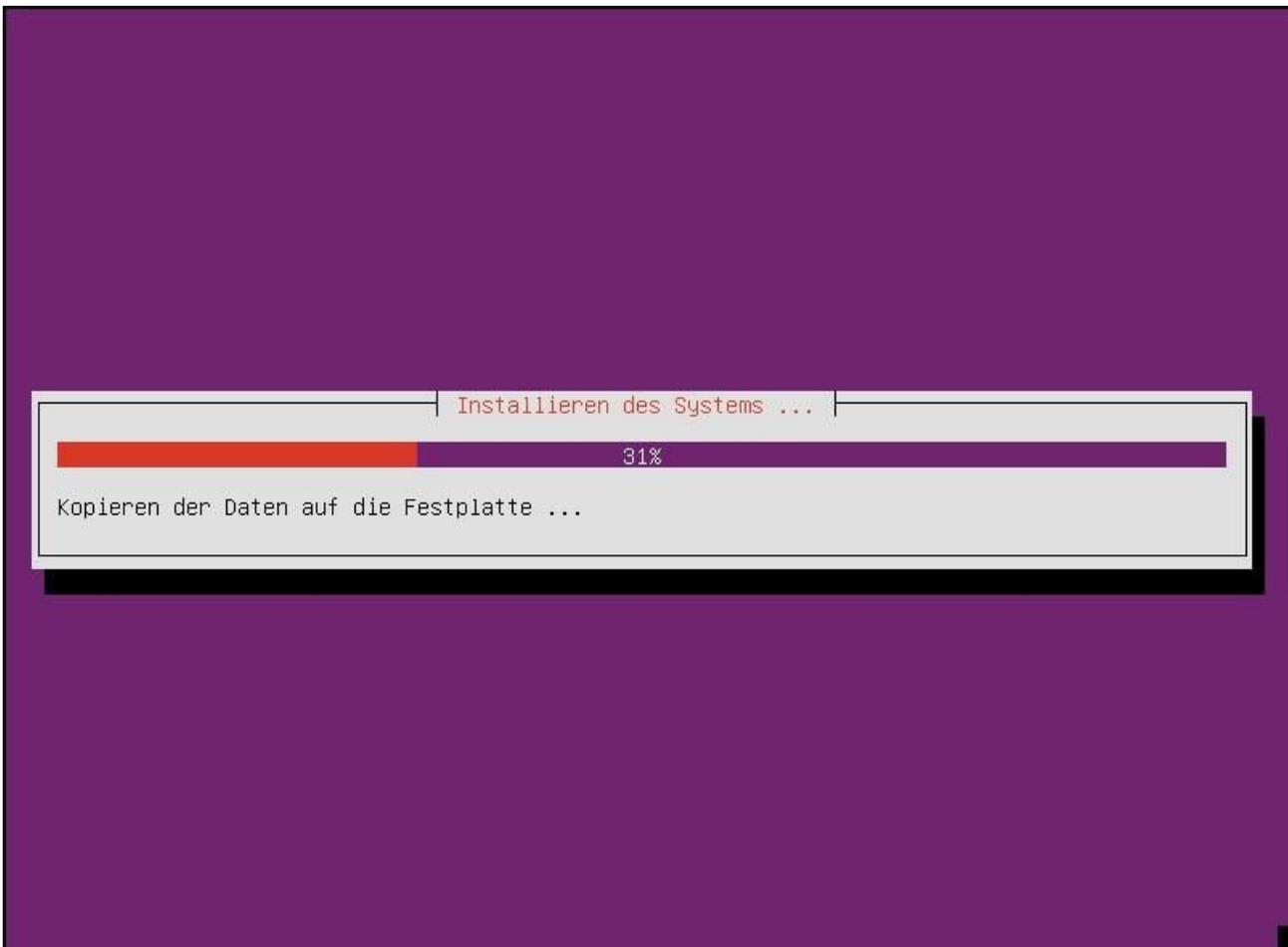
<Weiter>

<Tab> Nächste Option <Leertaste> Auswählen <Enter> Knöpfe aktivieren

Ubuntu - Name

Taufen Sie ihren Server in dieser Maske.

Foto: Jürgen Donauer



Ubuntu - Installation

Je nach Rechner, dauert das eine gewisse Zeit.

Foto: Jürgen Donauer

[!] Softwareauswahl

Momentan ist nur das Wichtigste des Systems installiert. Um das System an Ihre Bedürfnisse anzupassen, können Sie eine oder mehrere der folgenden vordefinierten Software-Sammlungen installieren.

Welche Software soll installiert werden?

- OpenSSH server
- DNS server
- LAMP server
- Mail server
- PostgreSQL database
- Print server
- Samba file server
- Tomcat Java server
- Virtual Machine host
- Manual package selection

<Weiter>

<Tab> Nächste Option <Leertaste> Auswählen <Enter> Knöpfe aktivieren

Ubuntu - Dienste

Hier können Sie bestimmen, welche Aufgaben ihr Server erledigen soll. Sie können das später natürlich ausweiten.

Foto: Jürgen Donauer

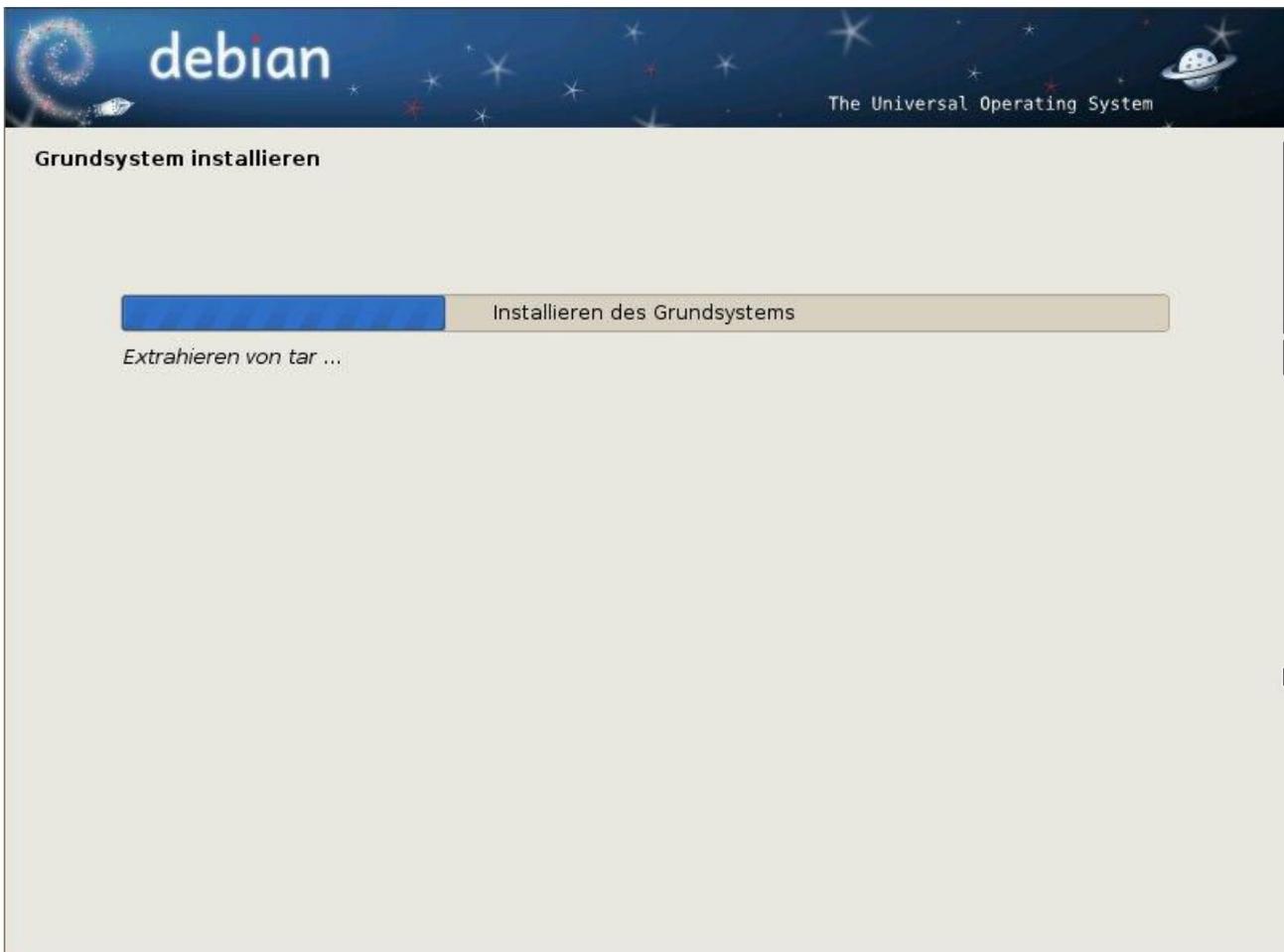
```
Ubuntu 12.10 ubuntu-server tty1
```

```
ubuntu-server login:
```

Anmelden

Ubuntu Server bringt per Standard keine grafische Oberfläche mit sich.

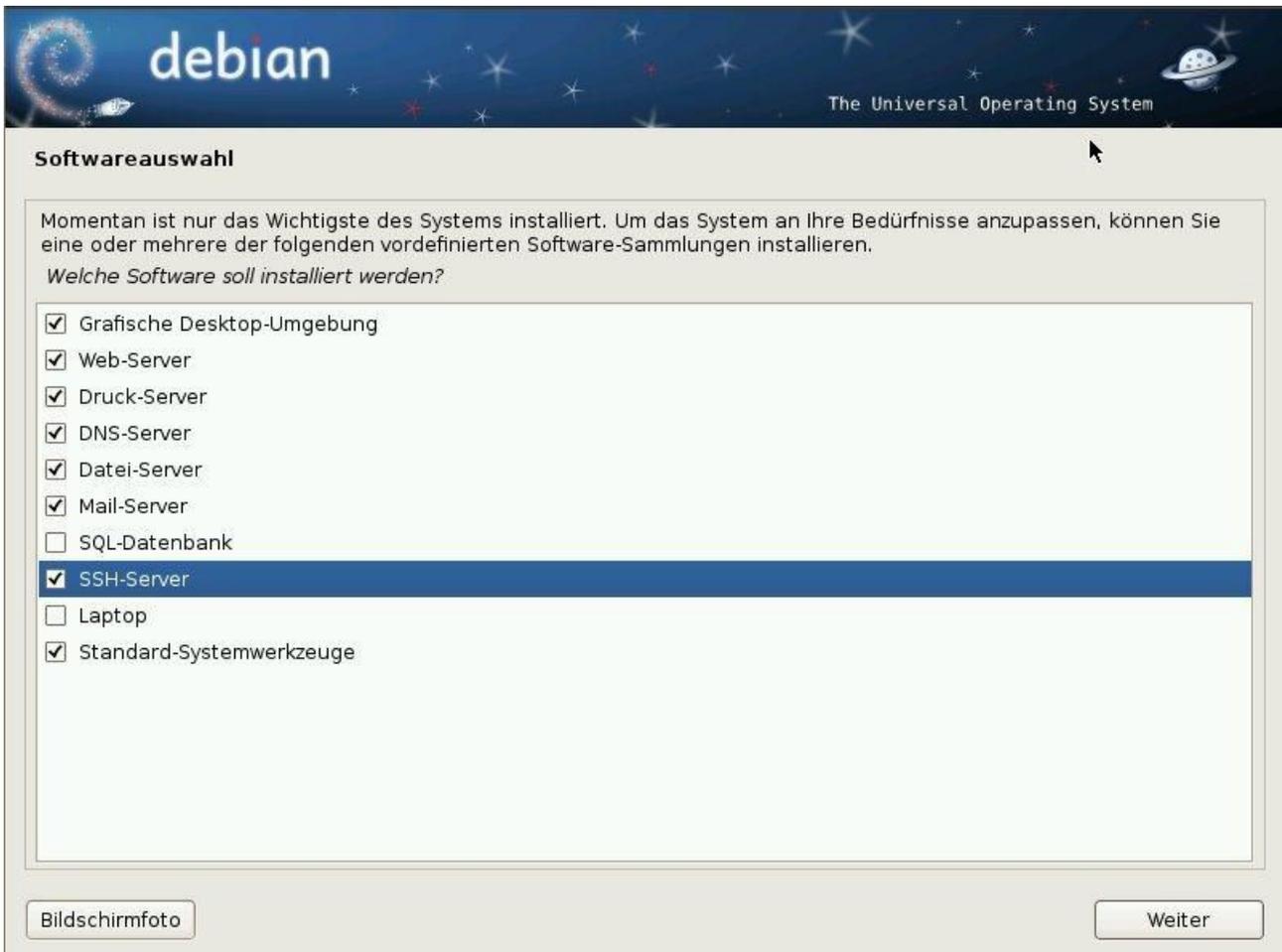
Foto: Jürgen Donauer



Debian - Geduld

Die Installation von Debian kann nach Hardware schon etwas dauern.

Foto: Jürgen Donauer



Debian - Paket-Auswahl

Dass Debian kein reines Desktop-System ist, sollte dieses Bild deutlich beweisen.

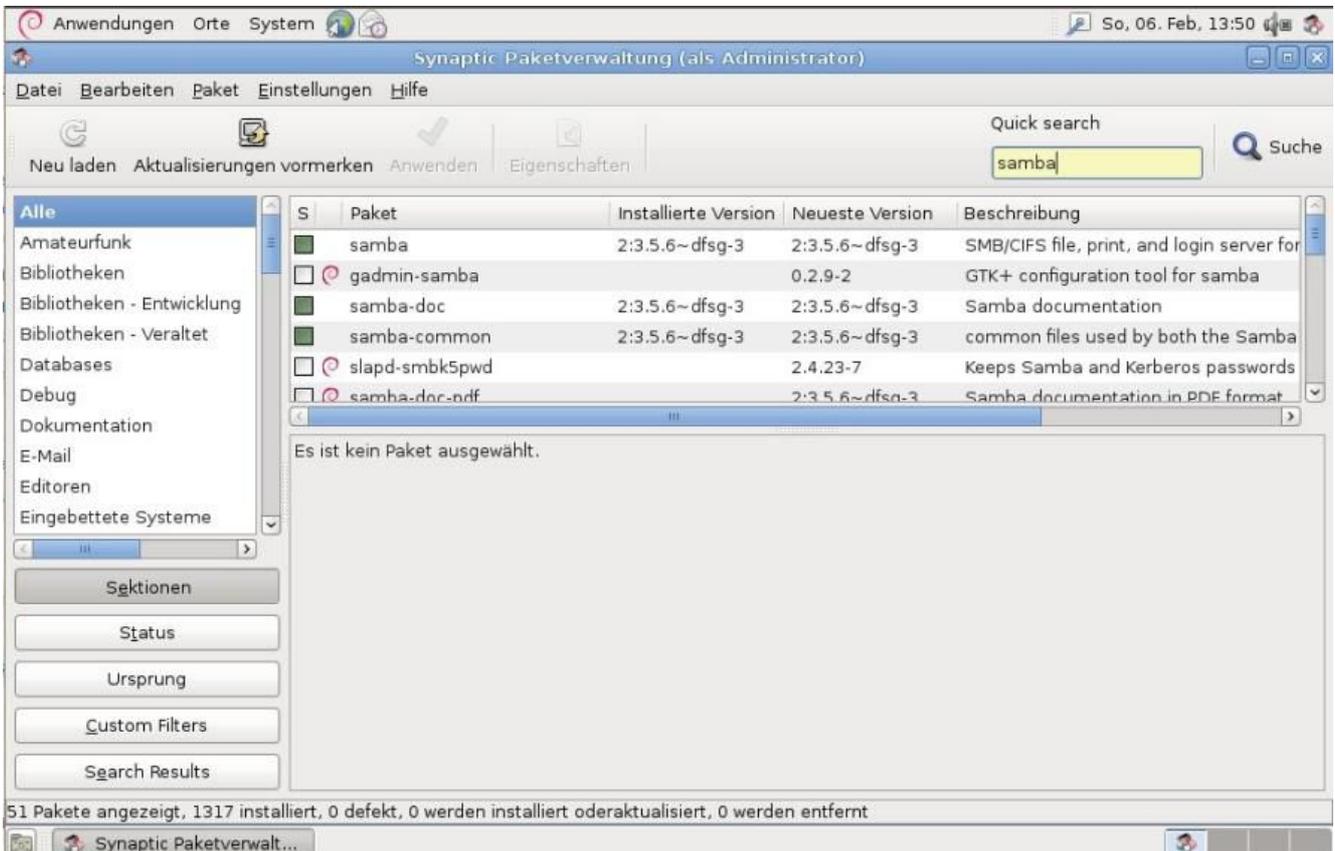
Foto: Jürgen Donauer



Debian - Squeeze

Seit kurzer Zeit ist Debian 6.0.0 verfügbar.

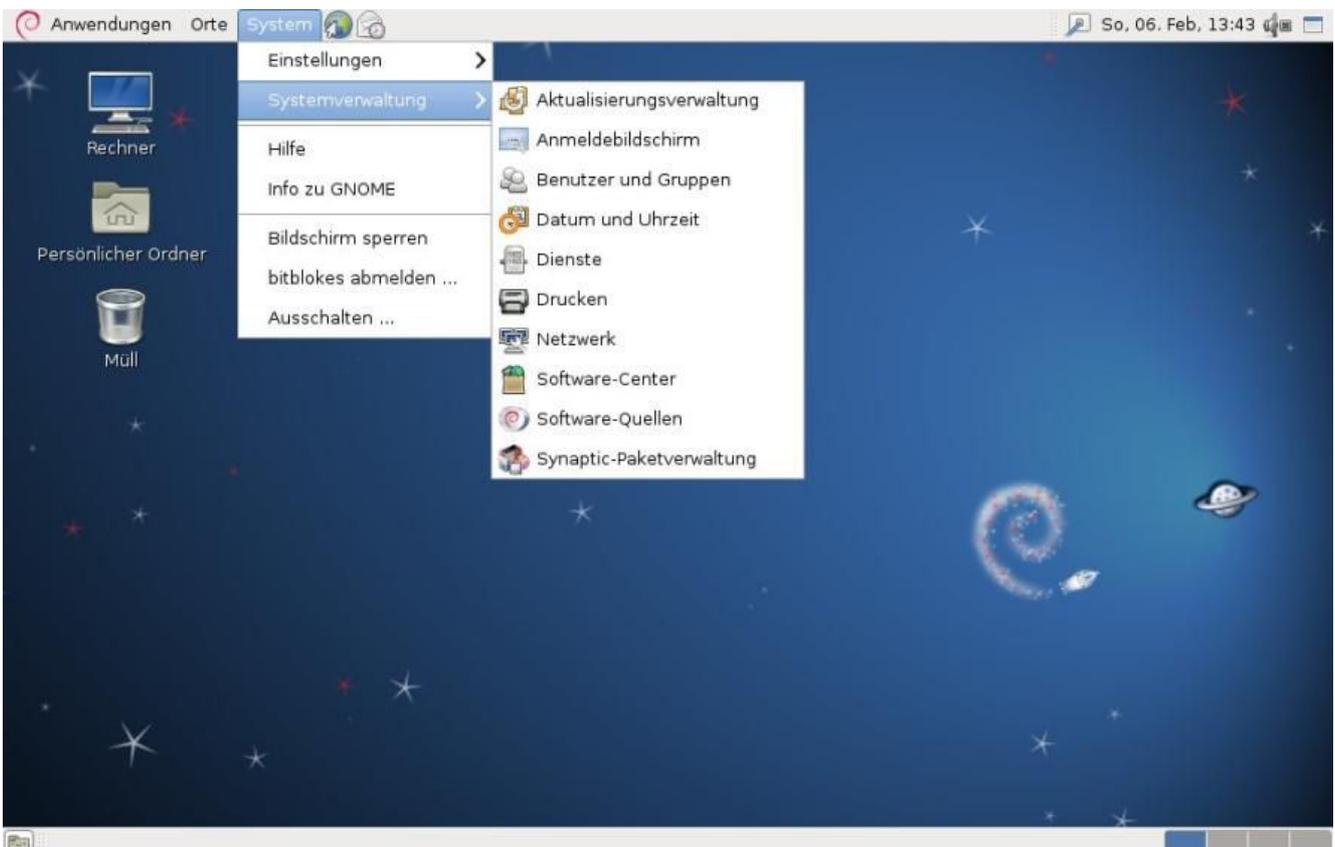
Foto: Jürgen Donauer



Debian - Paketverwaltung

Mit Synaptic können Sie das riesige Debian-Repository benutzen.

Foto: Jürgen Donauer



Debian - Grafische Benutzeroberfläche

Unter anderem stellt Debian GNOME zur Verfügung.

Foto: Jürgen Donauer

COLLAX Flexible IT **tecchannel.example.com** Collax Business Server Version: 5.0.22 Lizenznummer: CBST1482882629F0 admin@tecchannel.example.com

Systeminformationen

Status/CPU RAM Dateisystem Dateisystem-Nutzung Festplatten Netzwerk

Status

Systemzeit 05:42:14, 06.02.2011
 Systemlaufzeit 30 Minute(n) 20 Sekunde(n)
 Systemlast 0.23, 0.31, 0.28

CPU

Hersteller GenuineIntel
 Modell Intel(R) Core(TM)2 Duo CPU P8700 @ 2.53GHz
 Geschwindigkeit 144.900 MHz
 Cachegröße 6.000 Mbyte

Graphen

Service	avg	max
User	4.01 %	18.46 %
Low Prio	0.01 %	0.39 %
System	9.36 %	68.23 %
IRQ	0.04 %	0.17 %
Soft-IRQ	0.17 %	0.73 %
I/O wait	0.53 %	2.67 %

CPU Load (%) by Service

Collax GmbH, Copyright 2005-2011. All rights reserved.

Collax - Nagios integriert

Der Collax Business Server bietet eingebaute Monitoring-Software

Foto: Jürgen Donauer

... so simple! **COLLAX** Flexible IT

Boot from Hard Disk
Collax Business Server Install
 Collax Business Server Live CD
 File system check
 Memory Test

Boot Options |

F2 Language F3 Display F4 Video Mode
 English Silent 1024 x 768

Collax - So simple: Stimmt!

Collax Business Server ist in wenigen Schritten installiert.

Foto: Jürgen Donauer

COLLAX Flexible IT **tecchannel.example.com** Collax Business Server Version: 5.0.22 Lizenznummer: CBST1482882629F0
admin@tecchannel.example.com >>> ? X

System
Assistenten
Grundkonfiguration
Stammdaten
Intranet
Internetzugang
Registrierung
Benutzer
Mailserver
Webproxy
Dateifreigaben
Datensicherung

Assistenten

Einstellungen

Assistent für den Mailserver

Geben Sie an, in welchem Modus Sie Ihre E-Mails erhalten.

Die E-Mails können von Ihrem Mail-Anbieter auf dessen Server zwischengespeichert sein. Der Collax Server wird Ihre E-Mails dann regelmäßig beim Anbieter abholen.

Als zweite Möglichkeit können Sie E-Mails direkt empfangen. In diesem Fall brauchen Sie einen Eintrag im öffentlichen DNS, einen sogenannten MX-Record. Dies ist in der Regel nur mit einer festen öffentlichen IP-Adresse möglich.

Empfangsmodus:

Collax GmbH. Copyright 2005-2011. All rights reserved.

Collax - Wizard

Die Assistenten sind eine Wohltat und man kann auch mit weniger tiefem Wissen zum Beispiel einen Mailserver konfigurieren.

Foto: Jürgen Donauer

COLLAX Flexible IT tecchannel.example.com Collax Business Server Version: 5.0.22 Lizenznummer: CBST1482882629F0 admin@tecchannel.example.com >>> ? X

System

- > Benutzungsrichtlinien
- > Netzwerk
- > Mail und Messaging
- > Serverdienste

Assistenten

- File-Shares
 - Allgemein
 - Verzeichnisse
 - Synchronisation
 - Virtuelle Hosts
- SMB-/CIFS-Server
 - Allgemein
 - Für ADS vorbereiten
 - Windows-Gruppen Zuordnung
- Webserver
 - Allgemein
 - Webserver-Logs
- Datenbanken
 - MySQL
 - MySQL-Administration
- NTP
 - Konfiguration
- Druckerdienst
 - Konfiguration

Einstellungen

- > Filter
- > Systembetrieb

Collax GmbH, Copyright 2005-2011.
All rights reserved.

MySQL-Administration

Bitte Datenbank auswählen

- bacula (33)
- information_schema (17)
- mysql (17)
- phpmyadmin (8)
- test (0)

localhost

- Server Version: 5.0.77
 - Protokoll-Version: 10
 - Server: Localhost via UNIX socket
 - Benutzer: admin@localhost
- MySQL-Zeichensatz: **UTF-8 Unicode (utf8)**
- Zeichensatz / Kollation der MySQL-Verbindung:
 - utf8_unicode_ci
- Neue Datenbank anlegen**
- Kollation
- Anlegen
- MySQL-Laufzeit-Informationen anzeigen
- MySQL-System-Variablen anzeigen
- Prozesse
- Zeichensätze und Kollationen
- Tabellenformate
- Die Rechte neu laden
- Rechte
- Datenbanken
- Exportieren
- Importieren
- Neu anmelden

phpMyAdmin - 2.11.9.6

- MySQL-Client-Version: 5.0.77
- Verwandte php-Erweiterungen: mysql
- Sprache - Language: Deutsch - German
- Oberflächendesign: Original
- Schriftgröße: 82%
- phpMyAdmin-Dokumentation
- phpMyAdmin Wiki
- Offizielle phpMyAdmin-Homepage
- [ChangeLog] [Subversion] [Lists]

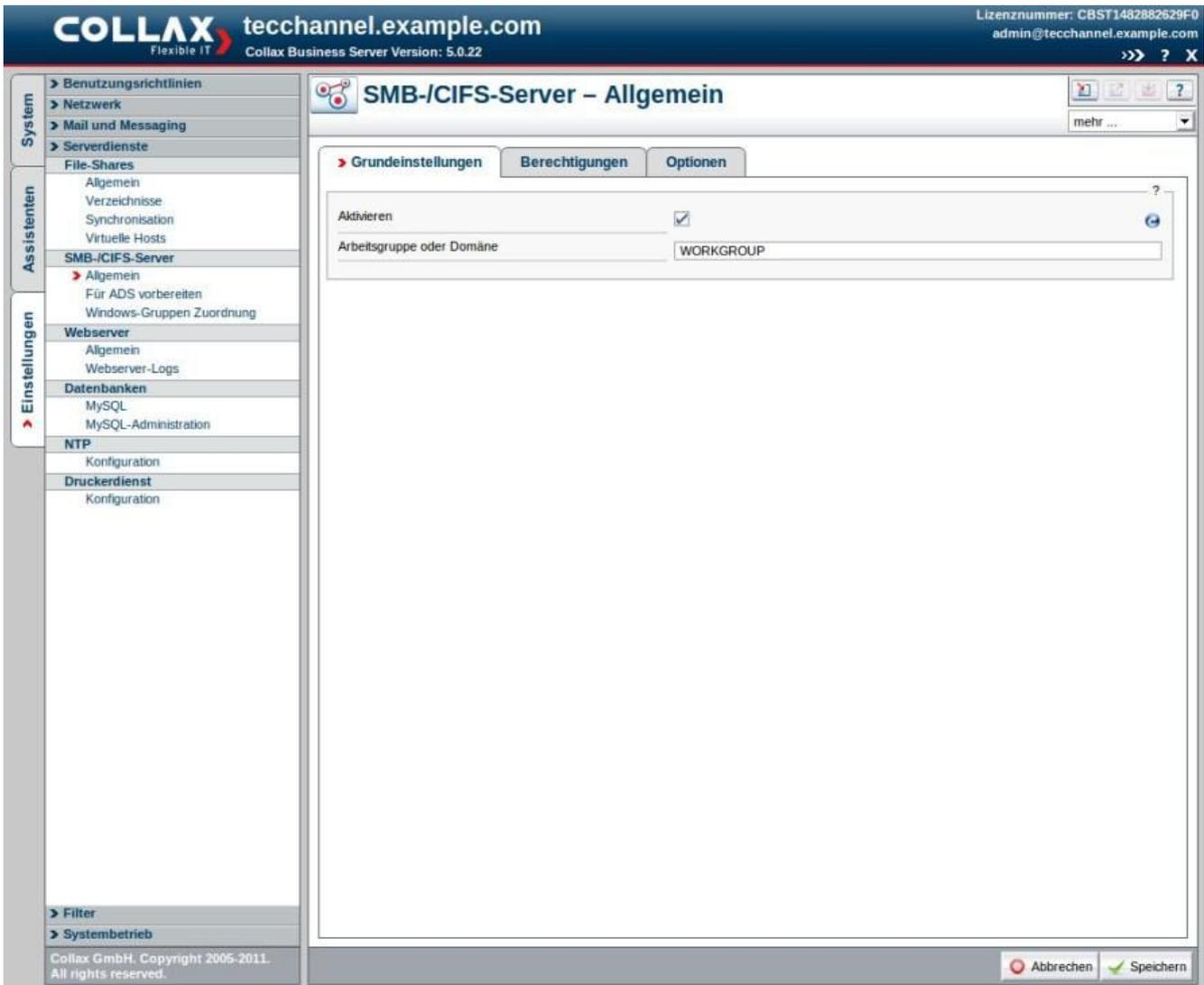
phpMyAdmin

Neues phpMyAdmin-Fenster

Collax - phpMyAdmin

Collax setzt bei der Datenbank-Administration auf bewährte Open-Source-Software

Foto: Jürgen Donauer



Collax - Datei- und Druck-Server

SMB- und CIFS-Dienste dürfen bei keinem Linux-Server fehlen.

Foto: Jürgen Donauer



SME Server™

- To install or upgrade type: `sme <ENTER>`.
- Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _

SME Server

Basiert auf CentOS, das wiederum auf die quelloffenen Pakete von Red Hat setzt.
Foto: Jürgen Donauer

Welcome to SME Server



<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

SME Server - Testen

Vor einer Installation können Sie das medium auf Fehler prüfen lassen.

Foto: Jürgen Donauer

Welcome to SME Server

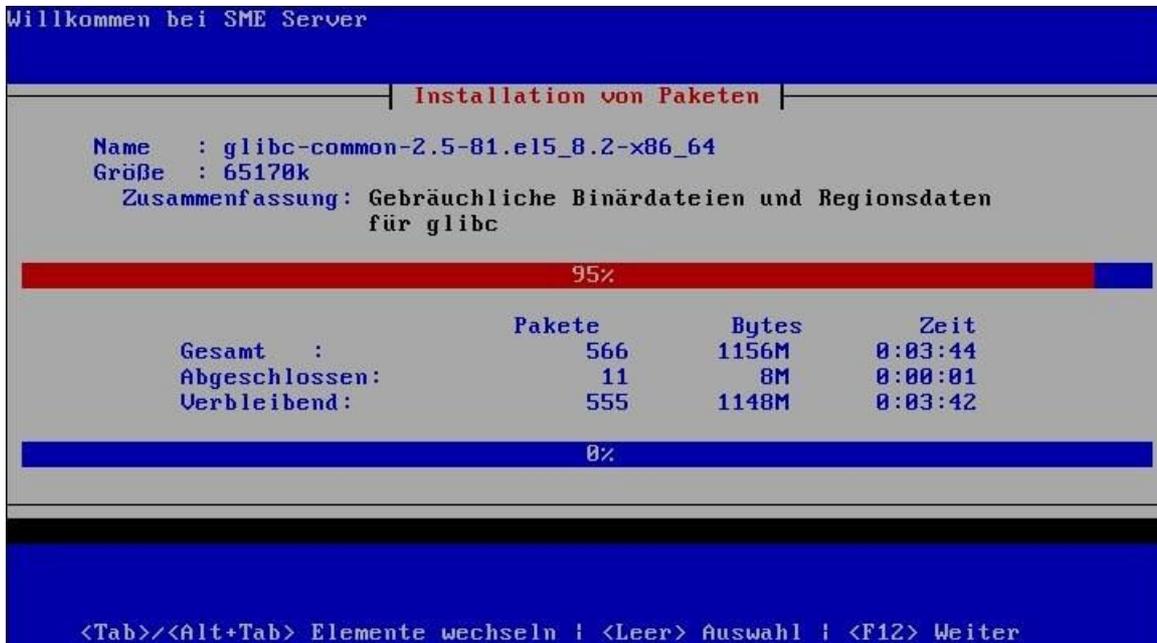


<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

SME Server - Sprache

Sie können das System auch auf Deutsch installieren.

Foto: Jürgen Donauer



SME Server -

Installation

Das Einspielen der Pakete hängt vom eingesetzten Rechner ab.

Foto: Jürgen Donauer



SME Server -

Datensicherung

Haben Sie eine Datensicherung, können Sie diese an diesem Punkt wieder einspielen.

Foto: Jürgen Donauer



SME Server - Netzwerk
Während der Installation können Sie eine IP-Adresse festlegen.
Foto: Jürgen Donauer



Username:

Password:

SME Server - Administration
SME Server können Sie bequem via Browser administrieren.
Foto: Jürgen Donauer

Collaboration

- Users
- Groups
- Quotas
- Pseudonyms
- Information bays

Administration

- Backup or restore
- View log files
- Mail log file analysis
- Reboot or shutdown

Security

- Remote access
- Local networks
- Port forwarding
- Proxy settings

Configuration

- Software installer
- Date and time
- Workgroup
- Directory
- Printers
- Hostnames and addresses
- Domains
- E-mail
- Antivirus (ClamAV)
- Review configuration

Miscellaneous

- Support and licensing
- Create starter web site

Welcome to the server manager

Welcome to SME Server, the leading Linux distribution for small and medium enterprises. SME Server is brought to you by [SME Server, Inc.](#), a non-profit corporation that exists to provide marketing and legal support for SME Server.

SME Server is freely available under the GNU General Public License and is only possible through the efforts of the SME Server community. However, the availability and quality of SME Server is dependent on meeting our expenses, such as hosting costs, server hardware, etc.

As such, we ask for a small donation to offset costs and fund further development.

Please visit <http://www.smeserver.org/donate/> to donate.

This software comes with ABSOLUTELY NO WARRANTY. Please [click here](#) to view detailed support, warranty and licensing information.

To perform a system administration function, click one of the links in the menu on the left of your screen.

SME Server 8.0
Copyright 1999-2006 Mitel Corporation
All rights reserved.
Copyright 2006 SME Server, Inc.

SME Server - Angemeldet

Hier sehen Sie die Möglichkeiten, die Ihnen SME Server zur Verfügung stellt.

Foto: Jürgen Donauer

Collaboration

- Users
- Groups
- Quotas
- Pseudonyms
- Information bays

Administration

- Backup or restore
- View log files
- Mail log file analysis
- Reboot or shutdown

Security

- Remote access
- Local networks
- Port forwarding
- Proxy settings

Configuration

- Software installer
- Date and time
- Workgroup
- Directory
- Printers
- Hostnames and addresses
- Domains
- E-mail

- Antivirus (ClamAV)
- Review configuration

Miscellaneous

- Support and licensing
- Create starter web site

Antivirus settings

General Settings

If this option is enabled then the filesystem will be scanned for viruses. A report of any found viruses will be emailed to the administrator.

Scan filesystem

Quarantine infected files

ClamAV and db versions 0.97.4/15608/Wed Nov 21 04:53:48 2012

Save

SME Server 8.0
Copyright 1999-2006 Mitel Corporation
All rights reserved.
Copyright 2006 SME Server, Inc.

SME Server - ClamAV

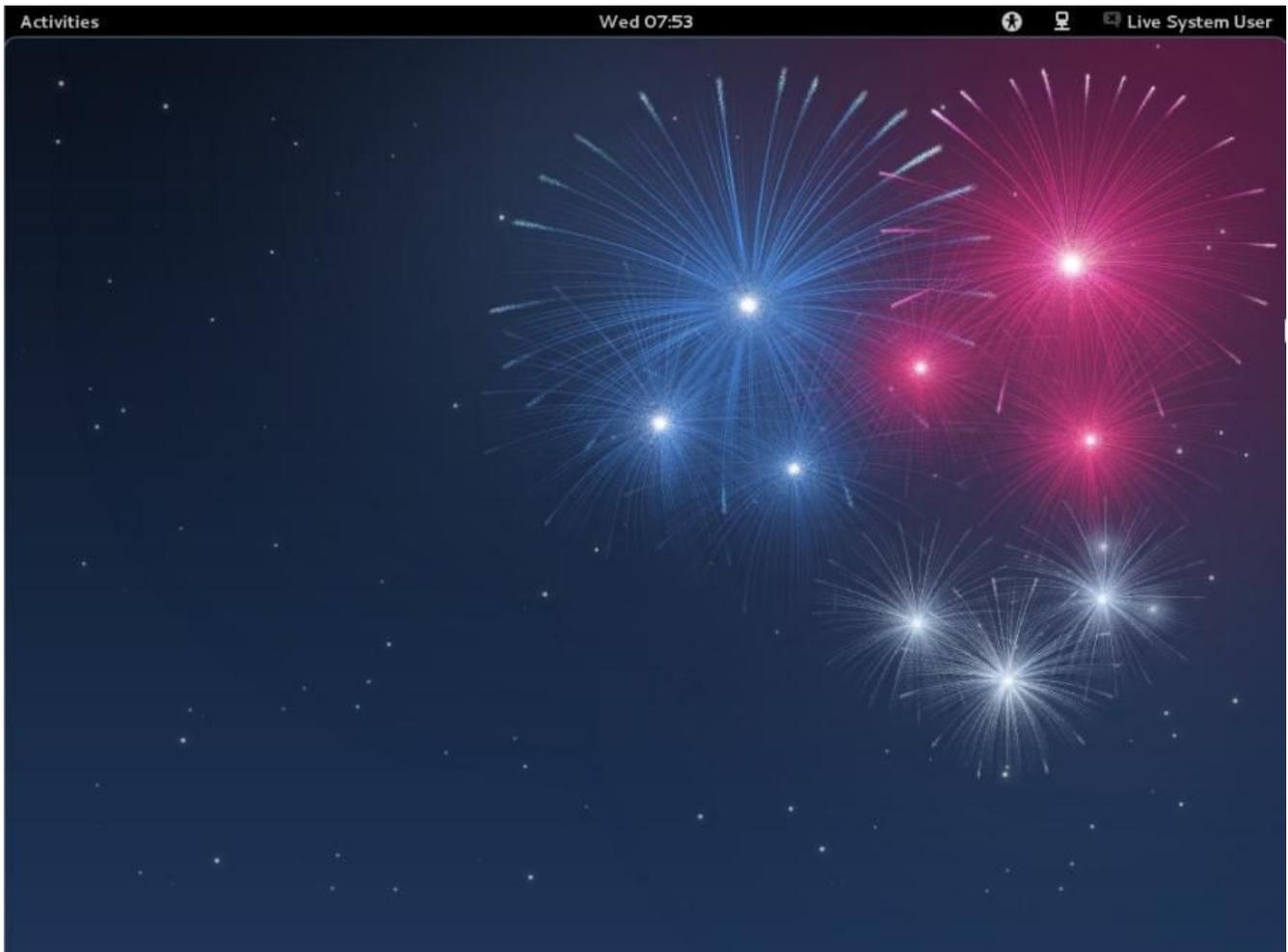
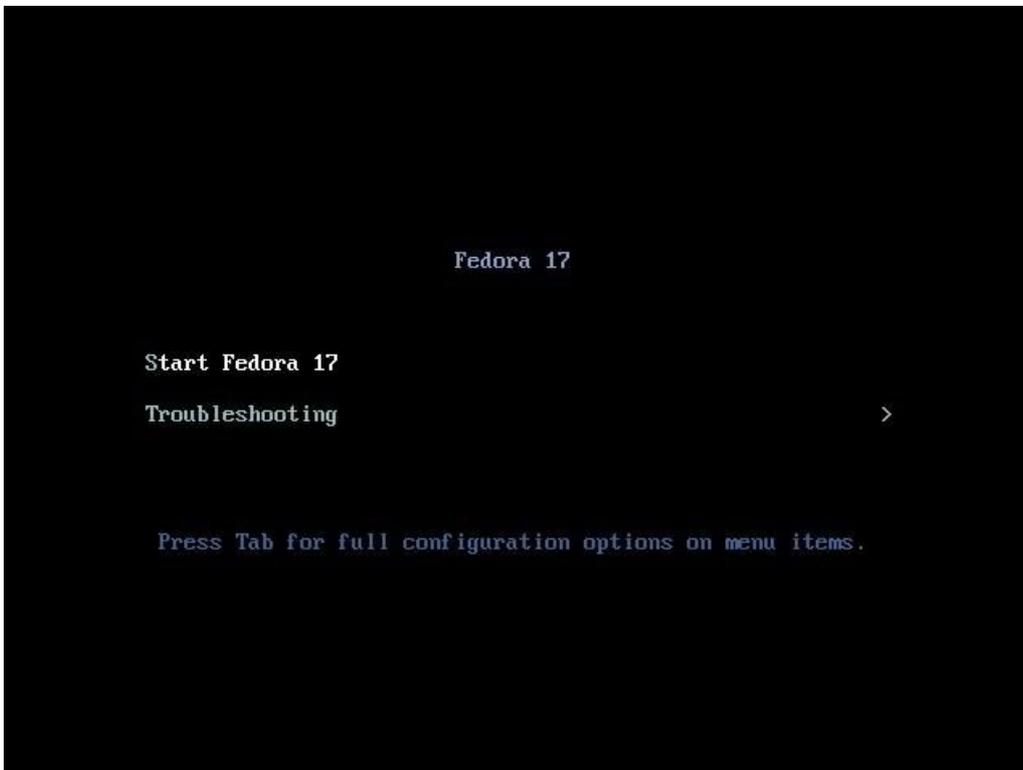
Sie können den Virenschanner so einstellen, dass er einmal täglich auf Malware prüft und diese dann in Quarantäne sperrt.

Foto: Jürgen Donauer

Fedora 17

Die derzeit aktuelle Version der Linux-Distribution. Version 18 ist für Januar 2013 geplant.

Foto: Jürgen Donauer



Fedora 17 - Oberfläche

Fedora setzt per Standard auf GNOME.

Foto: Jürgen Donauer



Fedora 17 - Anwendungen

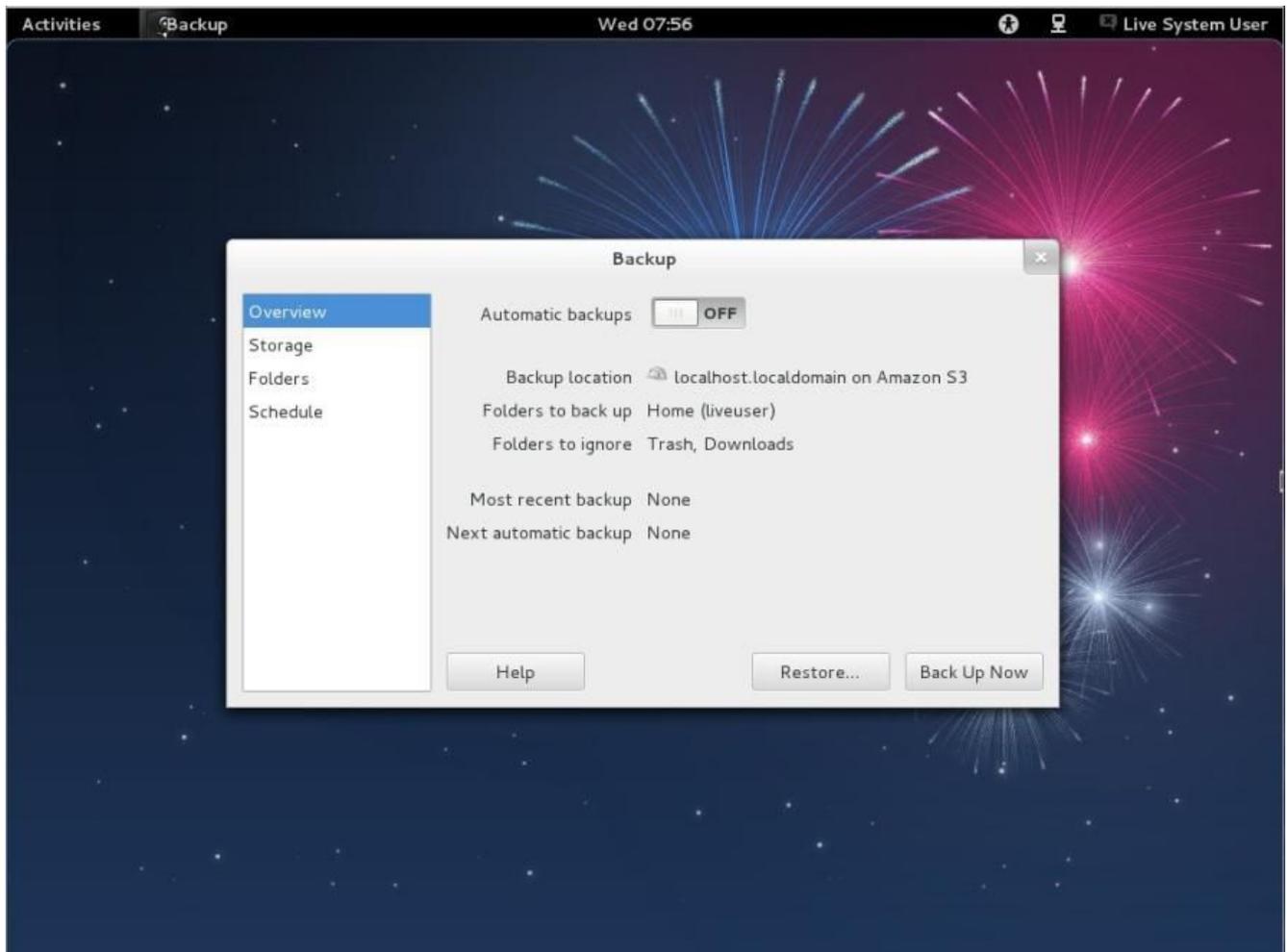
Das von Red Hat gesponserte Betriebssystem bringt diverse Applikationen vorinstalliert mit sich.
Foto: Jürgen Donauer



Fedora 17 - Browser

Mozillas Firefox ist auch mit von der Partie.

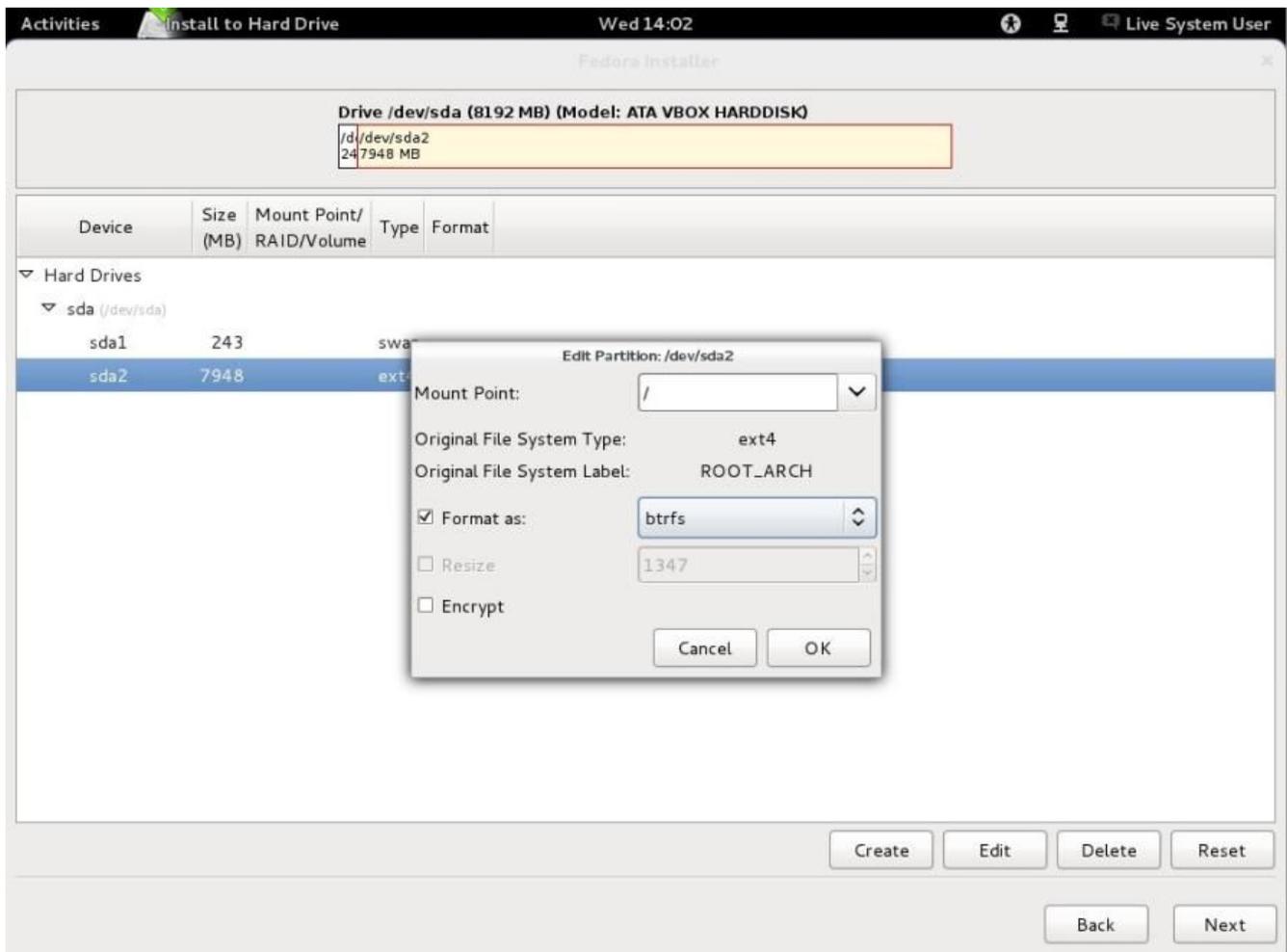
Foto: Jürgen Donauer



Fedora 17 - Datensicherung

Automatische Backups mit Fedora 17.

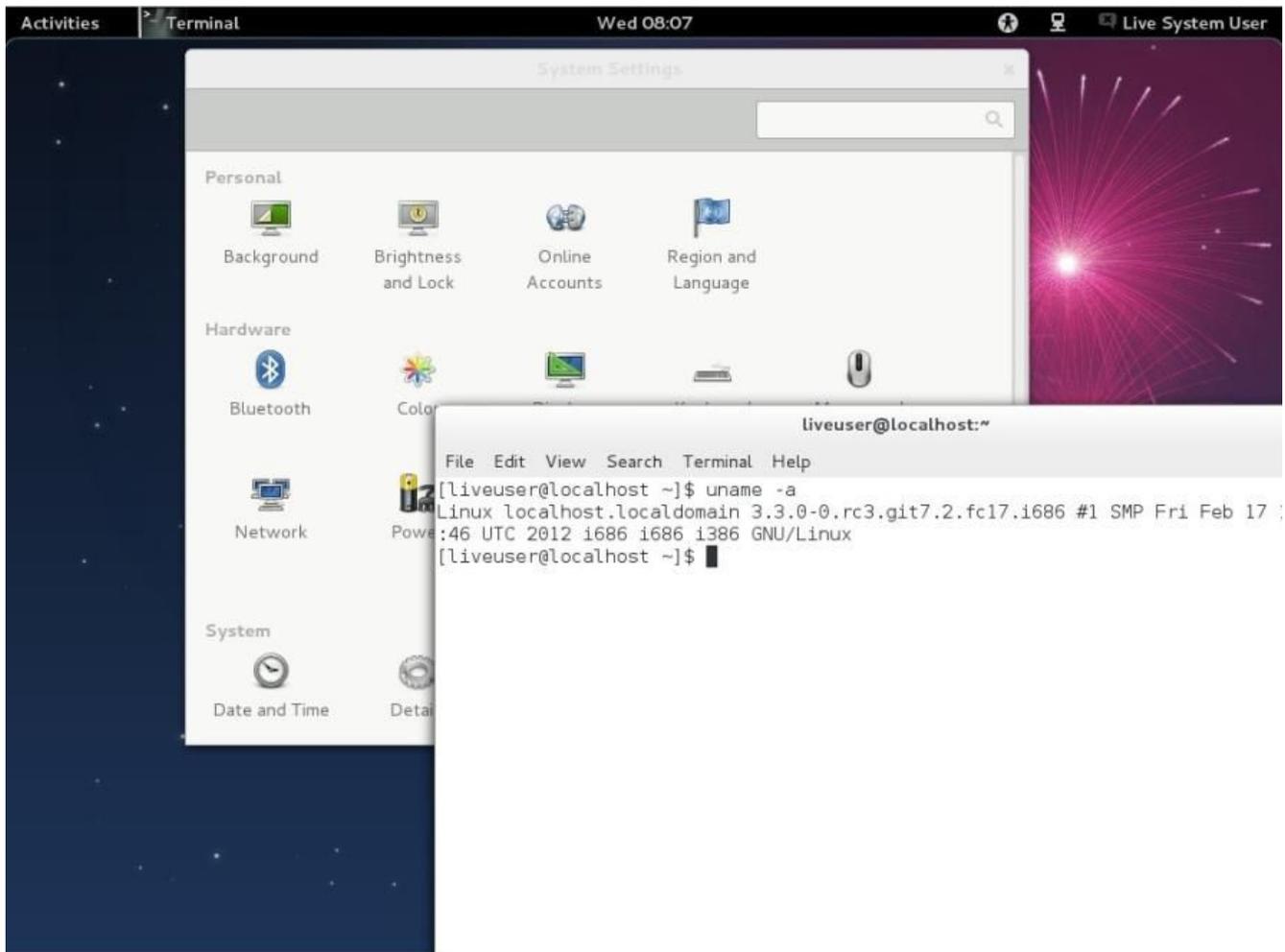
Foto: Jürgen Donauer



Fedora 17 - Dateisysteme

Unterstützung für Btrfs ist auch während der Installation vorhanden.

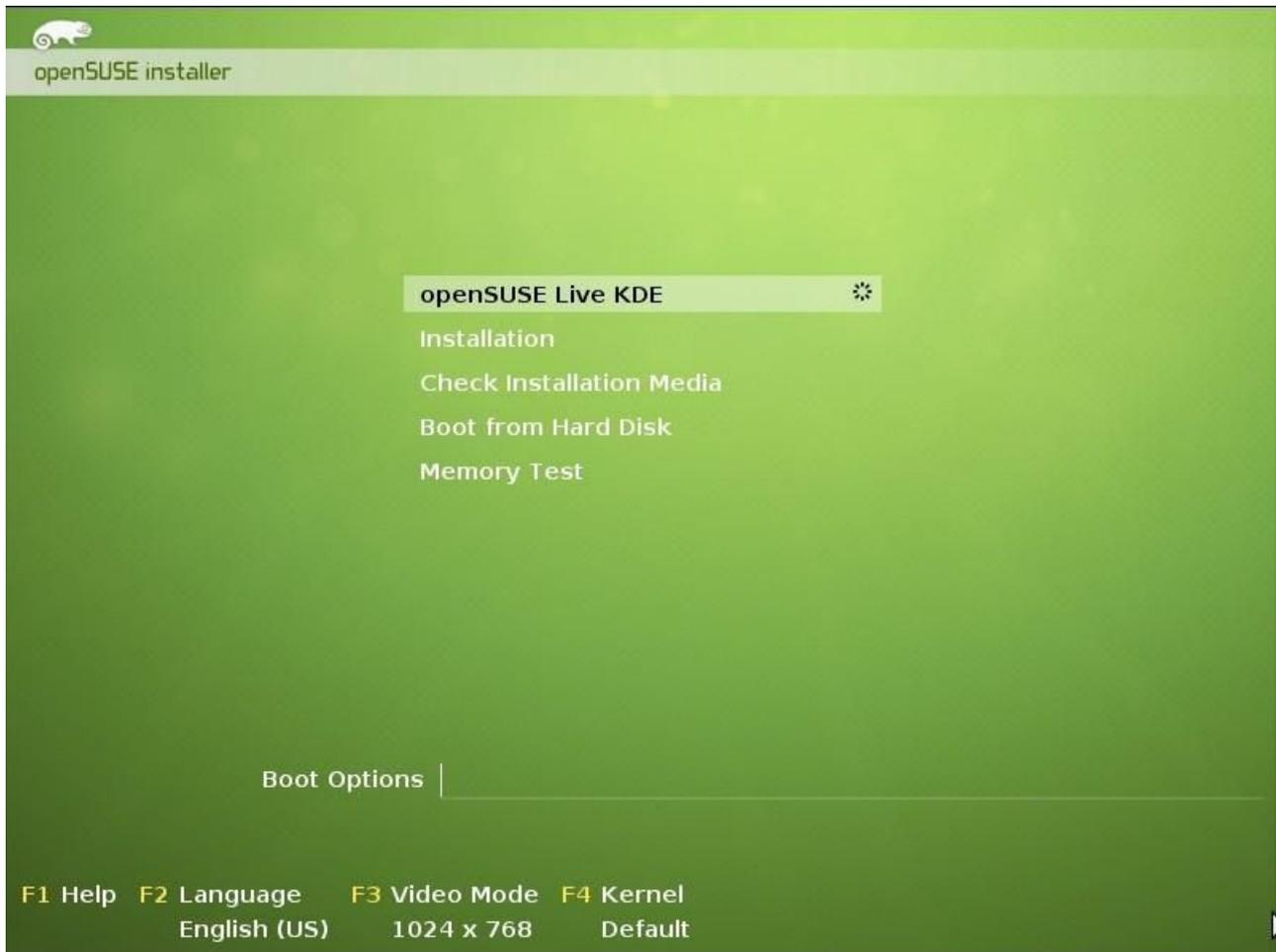
Foto: Jürgen Donauer



Fedora 17 - Kernel

Fedora 17 setzt auf Linux 3.3.

Foto: Jürgen Donauer



openSUSE

Ausprobieren oder Installieren?

Foto: Jürgen Donauer

Live-Installationseinstellungen

Wählen Sie Installieren, um eine Neuinstallation mit den angezeigten Werten durchzuführen. [more](#)

Für Änderungen eine Überschrift anklicken oder das *Ändern ...*-Menu unten benutzen.

Installation

- ✓ Willkommen
- ✓ Zeitzone
- ✓ Festplatte
- ✓ Benutzereinstellungen
- ▶ **Installationseinstellungen**
- Installation durchführen

Konfiguration

- Automatische Konfiguration
- Benutzer

System

- System: innotek GmbH - VirtualBox (1.2)
- Prozessor: Intel(R) Core(TM) i5 CPU M 480 @ 2.67GHz
- Hauptspeicher: 1.016 MB

Partitionierung

- Root-Partition /dev/sdc1 (5.00 GB) mit ext4 erstellen
- Volume /dev/sdc2 (3.00 GB) für /home mit ext4 erstellen
- /dev/sda2 als swap verwenden
- /dev/sdb5 als swap verwenden
- /dev/sdd5 als swap verwenden

Systemstart

- Bootloader-Typ: GRUB2
- Status Lokation: /dev/sda (MBR)

Länderspezifische Einstellungen

- Sprache: Deutsch
- Zusätzliche Sprachen: Englisch (US)
- Tastaturbelegung: Deutsch

Zeitzone

- Europa / Deutschland - Rechneruhr eingestellt auf UTC (GMT) 2012-07-14 - 09:00:28

Benutzereinstellungen

- Benutzer bitblokes (bitblokes) konfiguriert
- Root-Passwort factalant

Ändern ... ▾

Help Hinweise zur Version anzeigen Abbrechen Zurück Installieren

openSUSE - Installation

Das Einspielen übernimmt YaST.

Foto: Jürgen Donauer

Desktop

Live-CD User (linux) on linux.site

Search:

Favorites:

- Web Browser
- Personal Information Manager
- Word Processor
- Audio Player
- File Manager
- Configure Desktop
- Help
- Terminal

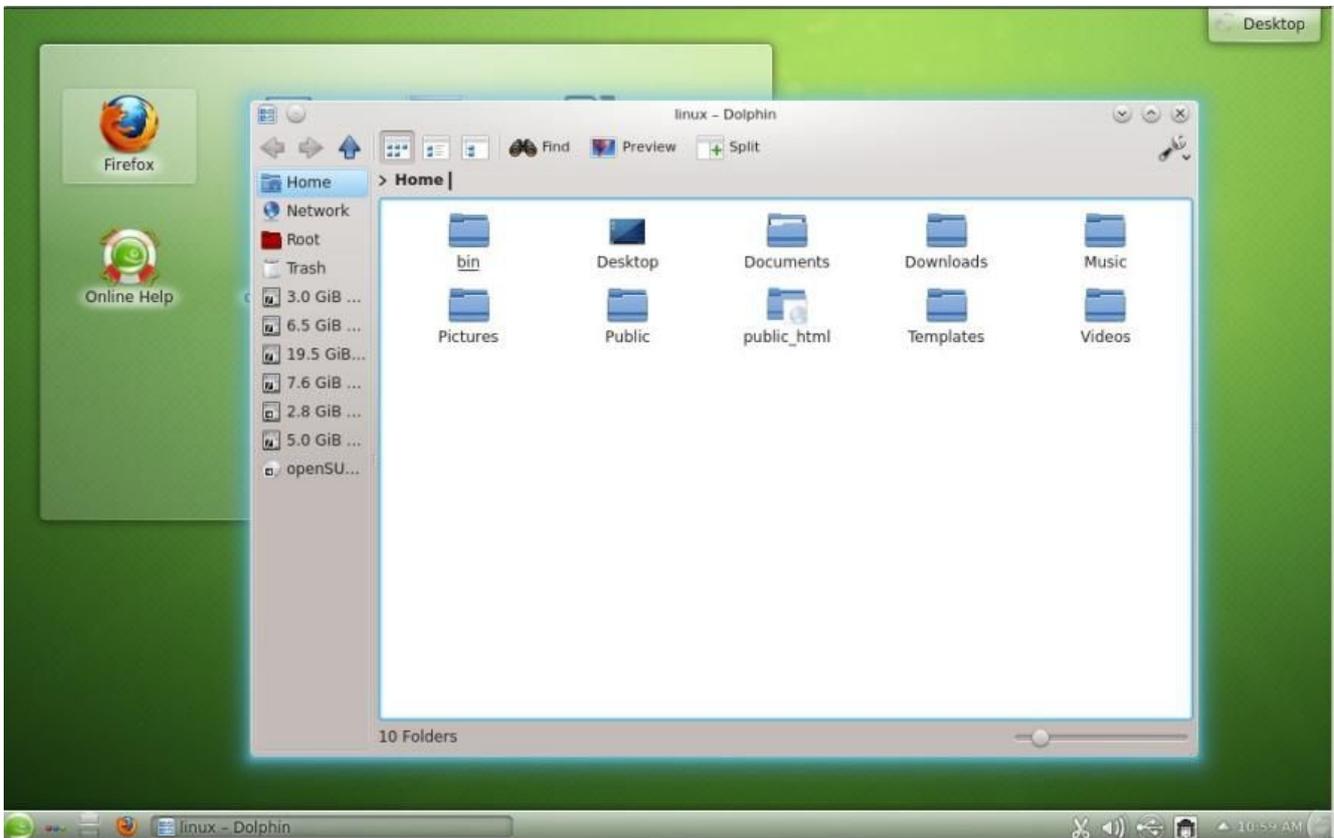
Favorites Applications Computer Recently Used Leave

10:57 AM

openSUSE - KDE

Sie können zwischen KDE oder GNOME wählen.

Foto: Jürgen Donauer



openSUSE - Dateimanager

Dolphin ist KDEs Standard-Dateimanager.

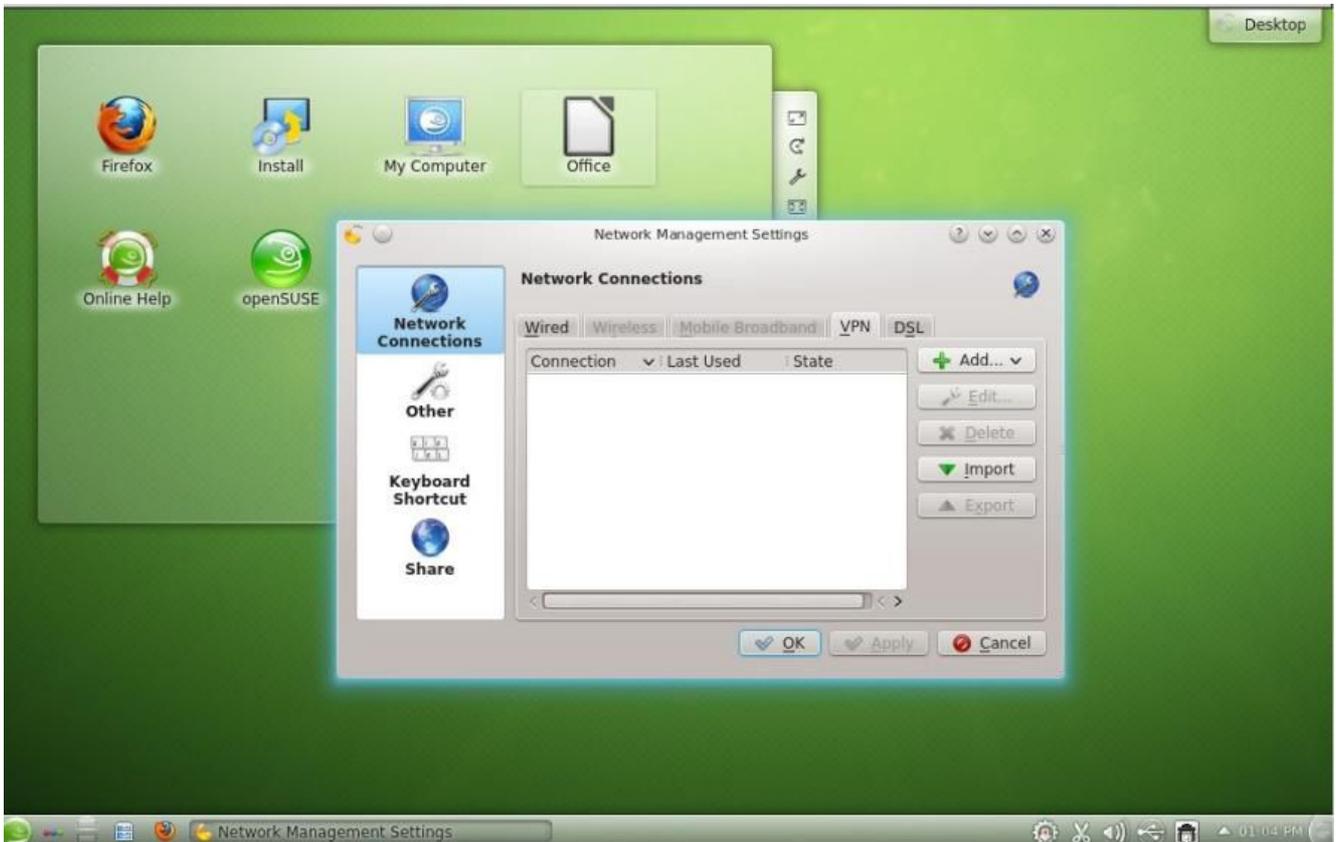
Foto: Jürgen Donauer



openSUSE - Kontrollzentrum

YaST übernimmt alle administrativen Aufgaben.

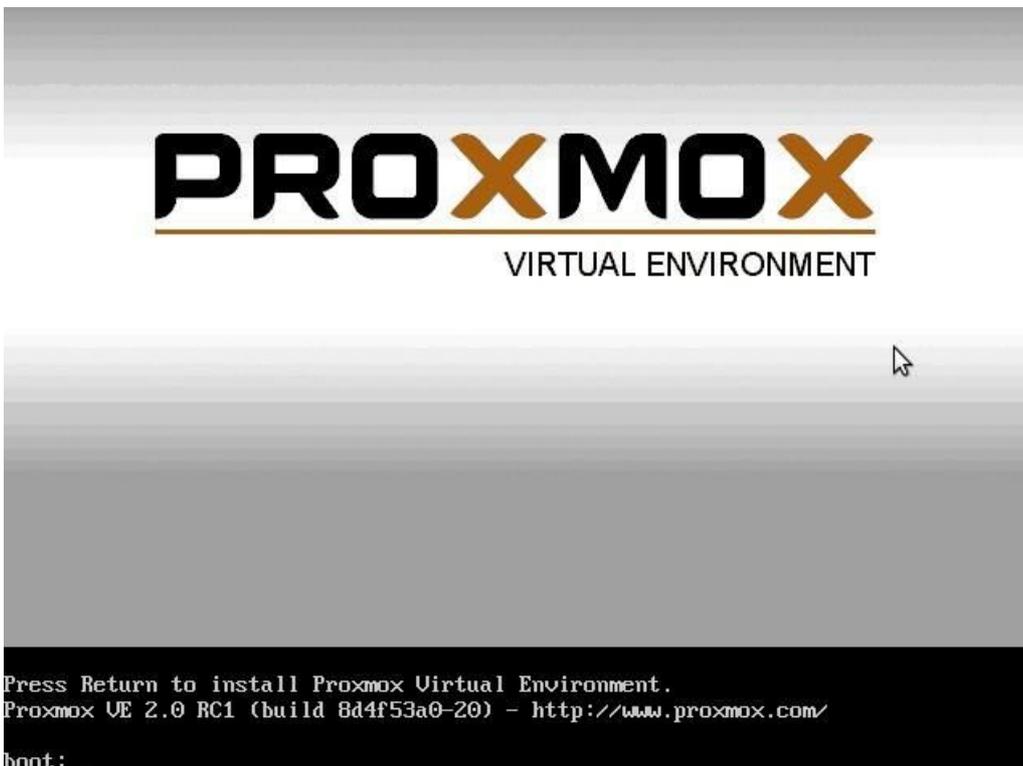
Foto: Jürgen Donauer



openSUSE - Kommunikation

Die Netzwerkeinstellungen bieten auch VPN an.

Foto: Jürgen Donauer



Virtuelle Umgebung

Proxmox 2.0 eignet sich zum Konsolidieren von Servern.

Foto: Jürgen Donauer



Proxmox License Agreement

The following copyright applies to the Proxmox Virtual Environment compilation and any part of Proxmox Virtual Environment it does not conflict with. Whenever this policy does conflict with the copyright of any individual portion of Proxmox Virtual Environment, it does not apply.

GNU AFFERO GENERAL PUBLIC LICENSE
Version 3, 19 November 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights

Proxmox - Lizenz

Nach Bestätigung geht es weiter.

Foto: Jürgen Donauer



Location and Time Zone selection

The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.

Press the Next button to continue installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

Country

Time zone

Keyboard Layout

[Abort](#)

[Next](#)

Proxmox - Zeitzone

Ein Installations-Assistent nimmt Sie an die Hand.

Foto: Jürgen Donauer



Administration Password and E-Mail Address

Proxmox Virtual Environment is a full featured GNU/Linux system based on Debian. Therefore you should use a strong password with at least 5 characters.

All administrative emails are sent to the specified address.

Press the Next button to continue installation.

- **Password:** Please use strong passwords. Your password should be 8 or more characters in length. Also combine letters, numbers, and symbols.
- **E-Mail:** Administrator email address.

Password

Confirm

E-Mail

[Abort](#)[Next](#)

Proxmox - Kennwort

Hier geben Sie Passwort und E-Mail-Adresse an.

Foto: Jürgen Donauer



Install



Just Start



Webbased

Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the configuration interface after installation.

Afterwards press the Next button to continue installation. The installer will then partition your hard disk and start copying packages.

- **IP address:** Set the IP address for the Proxmox Virtual Environment.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Hostname (FQDN): proxmox.example.com

IP Address: 192 . 168 . 100 . 195

Netmask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 100 . 138

DNS Server: 192 . 168 . 100 . 1

Abort

Next

Proxmox - Netzwerk

Bereits während der Installation lassen sich notwendige Einstellungen angeben.

Foto: Jürgen Donauer

```
Starting OpenBSD Secure Shell server: sshd.  
Starting pve cluster filesystem : pve-cluster.  
clvmd: cluster not configured.  
Starting periodic command scheduler: cron.  
unable to load kvm module  
Starting PVE Daemon: pvedaemon.  
Starting OpenVZ: ..done  
Bringing up interface venet0: ..done  
Container(s) not found  
Starting web server: apache2.  
Starting PVE Status Daemon: pvstatd.
```

Welcome to the Proxmox Virtual Environment. Please use your web browser to configure this server - connect to:

<https://192.168.100.195:8006/>

Debian GNU/Linux 6.0 proxmox tty1

proxmox login: _

Proxmox - Anmelden

Wie man sieht, basiert Proxmox 2.0 auf Debian 6 "Squeeze".

Foto: Jürgen Donauer

PROXMOX Proxmox Virtual Environment Version 2.0-27/8d4f53a0 You are logged in as 'root@pam' Logout Create VM Create CT

Server View Datacenter

Search:

Type	Description	Disk usage	Memory usage	CPU usage	Uptime
node	proxmox	13.8%	17.2%	0.2% of 1CPU	00:02:40
storage	local (proxmox)	1.6%			-

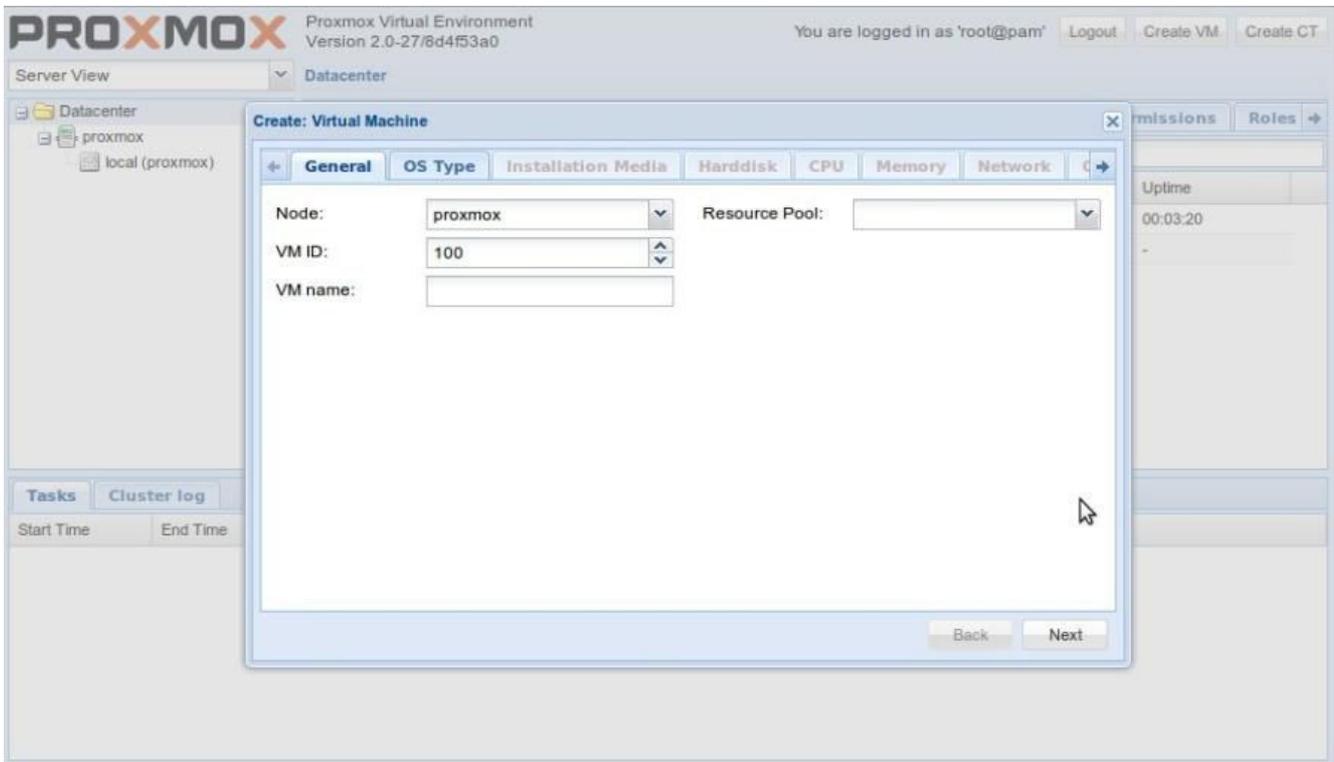
Tasks Cluster log

Start Time	End Time	Node	User name	Description	Status
------------	----------	------	-----------	-------------	--------

Proxmox - Administration

So sieht die Oberfläche für den Systemverwalter aus.

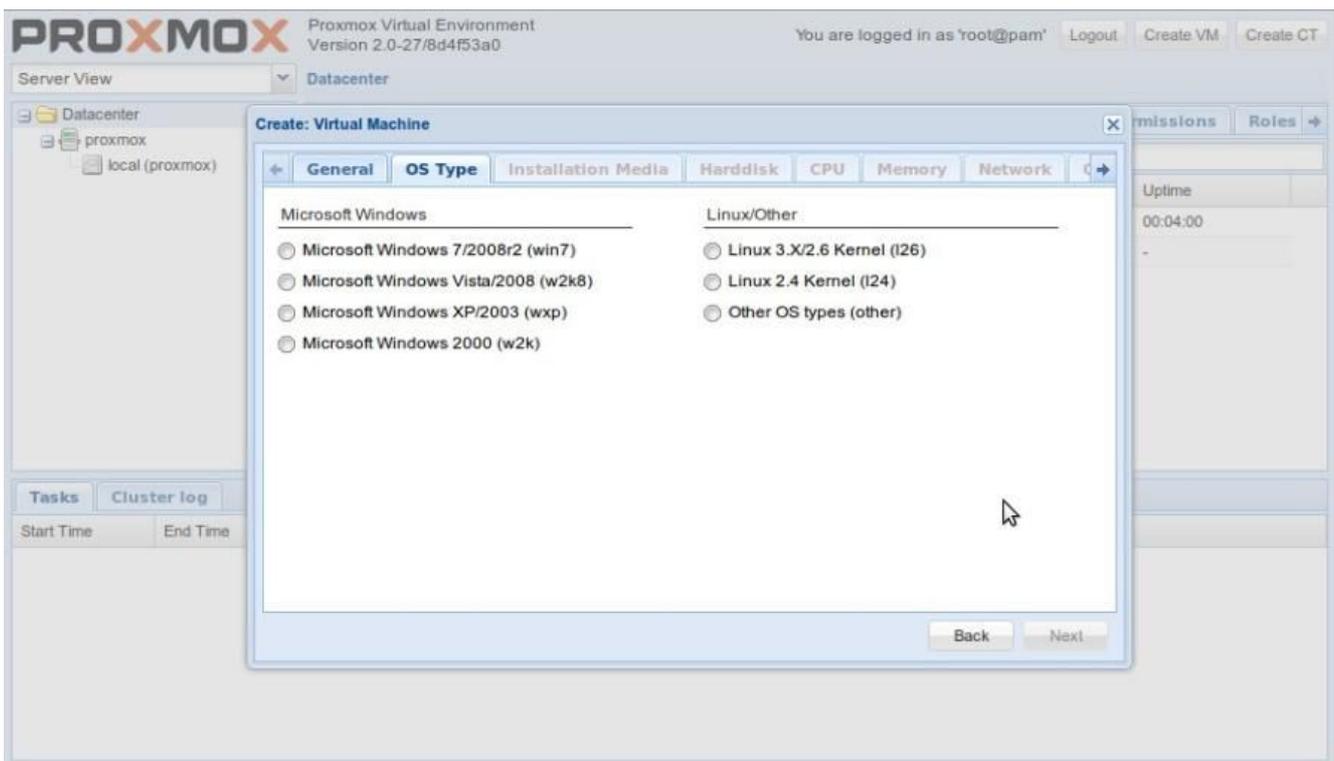
Foto: Jürgen Donauer



Proxmox - neue VM

Hier können Sie eine neue virtuelle Maschine erstellen.

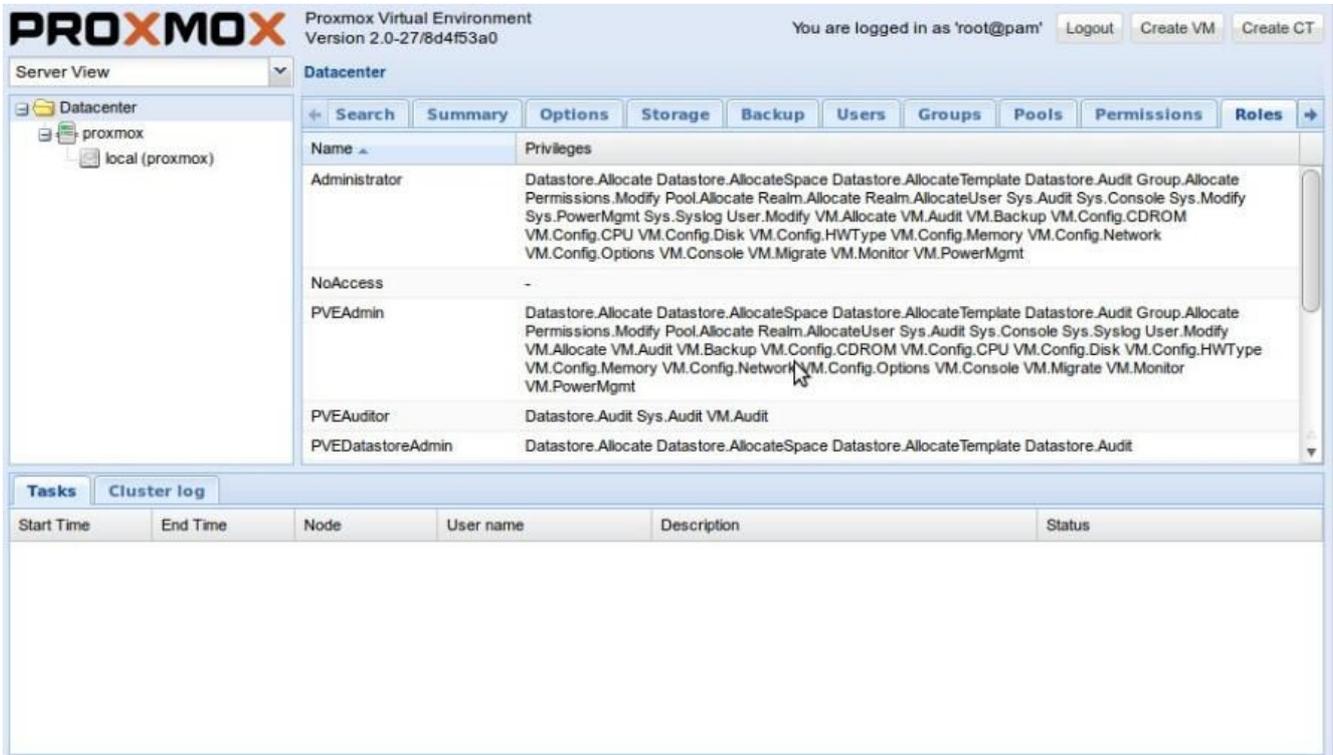
Foto: Jürgen Donauer



Proxmox - Betriebssystem

Proxmox unterstützt auch Windows 7.

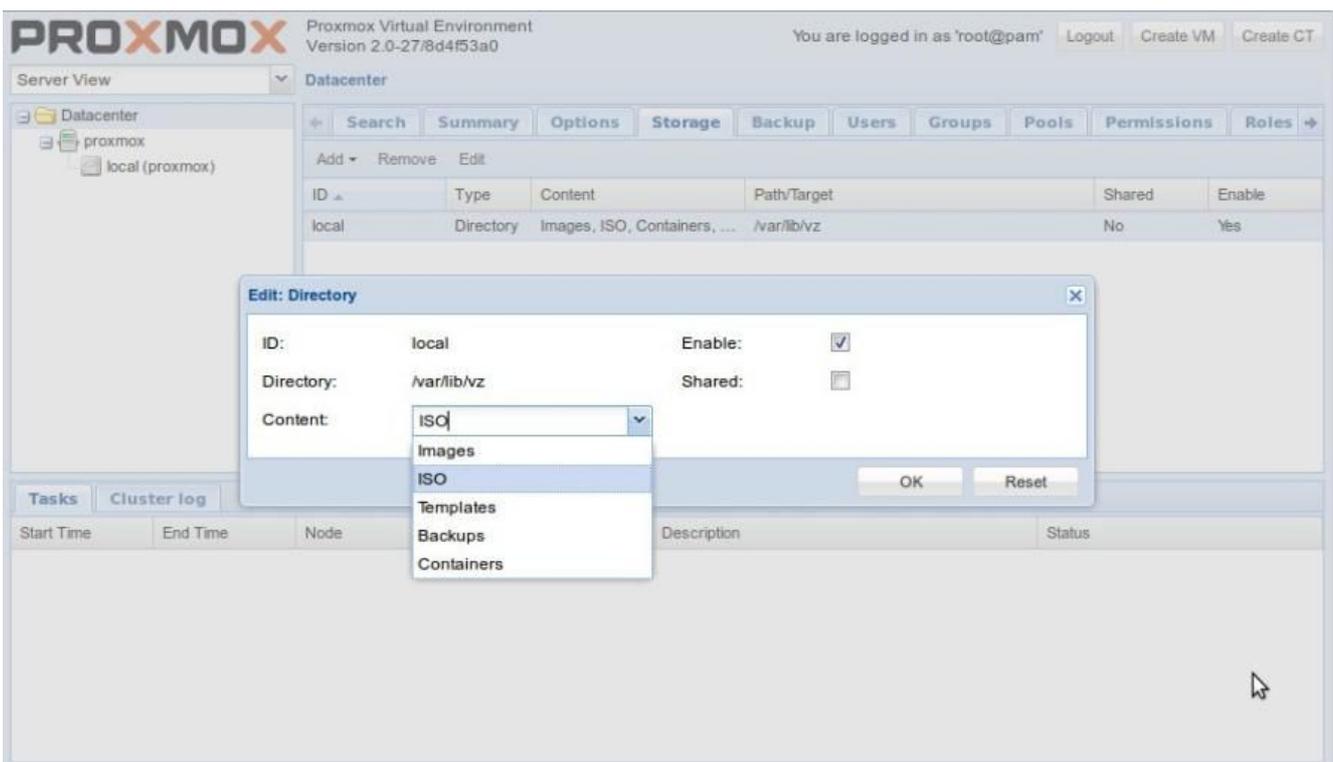
Foto: Jürgen Donauer



Proxmox - Rollen

Wie viele Rechte die einzelnen Nutzer haben, bestimmen Sie hier.

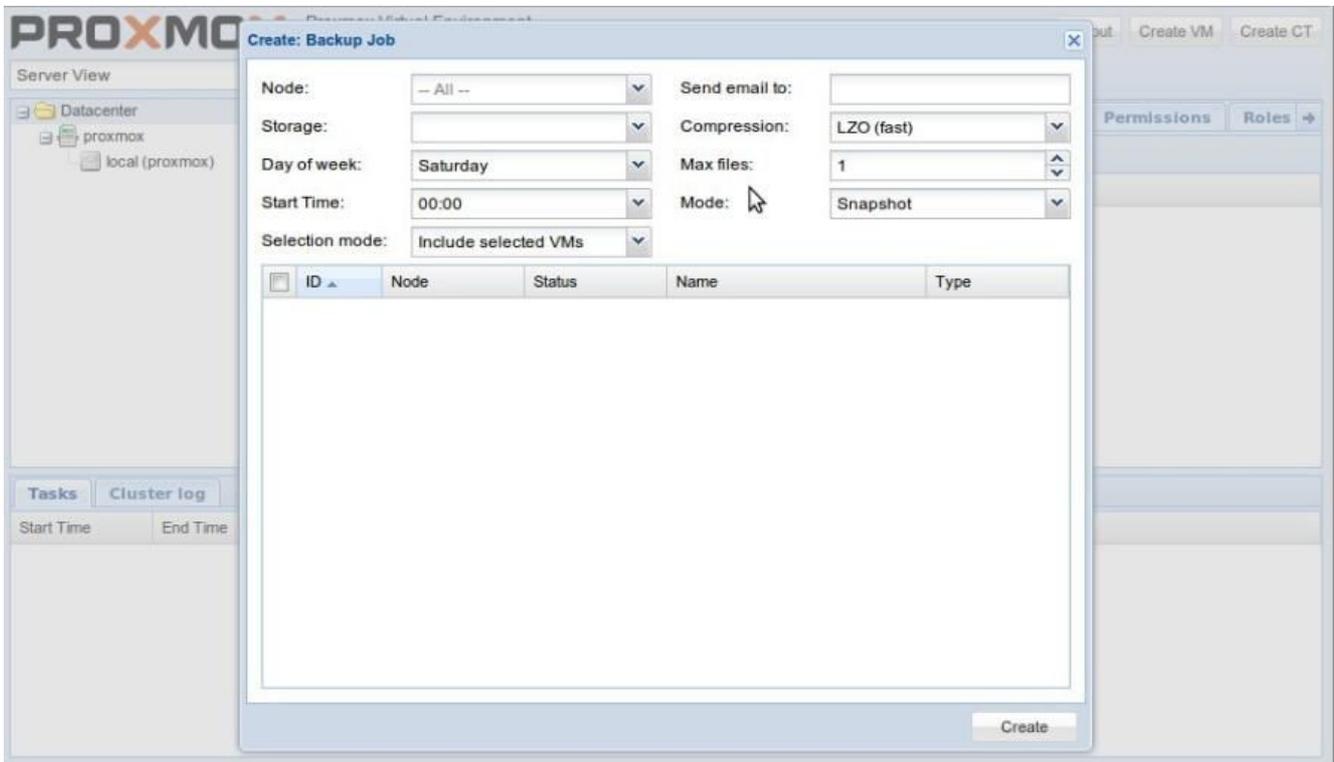
Foto: Jürgen Donauer



Proxmox - Speicher

Hier konfigurieren Sie ISO-Abbilder und andere Speicherorte.

Foto: Jürgen Donauer



Proxmox - Datensicherung

Backups sind auf Systemen wie Proxmox Pflicht. Das Betriebssystem macht diese Aufgabe zu einem Kinderspiel.

Foto: Jürgen Donauer

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.