

Hauke Goos-Habermann
Stand 2015/07

Neu: Mit Referenz

Inhaltsverzeichnis

1	Workshopvorbereitungen	7
1.1	Was muß ich mitbringen?	7
1.2	Debian-Admin-Workshop-Appliance	7
1.3	Die beiden VMs	7
1.4	Import	8
1.5	Benutzer und Paßworte	8
2	Grundlagen	9
2.1	"root" werden	9
2.2	Distribution und Hardware	9
2.3	Partitionierung, Mountpunkte, Laufwerksfüllstand	10
2.4	Pfadangaben	10
2.5	Die Arbeit beschleunigen	10
2.6	Praktische Helfer	11
2.7	Kopieren, verschieben, löschen	12
2.8	Benutzer und Gruppen	12
2.9	Zugriffsrechte	12
2.9.1	Besitzer und Gruppe ändern	13
2.9.2	Zugriffsrechte ändern	13
2.10	Dateien Suchen und finden	13
2.11	man und --help	14
2.12	Befehle nach Stichwort suchen	14
2.13	Neustart und Herunterfahren	14
3	Was ist wo?	15
4	Dienste und Dämonen	17
4.1	SysVinit	17
4.2	Upstart	17
4.3	systemd	18
5	Netzwerk	19
5.1	Aktuelle Netzwerkeinstellungen	19
5.2	Netzwerkfehler identifizieren	20
5.3	Netzwerkeinstellungen per Hand	20
5.3.1	Statische IP	20
5.3.2	Dynamische IP	21
5.4	Netzwerkeinstellungen über Dateien	21
5.5	Fernzugriff	22

5.6 Kopieren über das Netzwerk	22
6 Paketverwaltung	25
6.1 Quellen einrichten	25
6.2 Software verwalten	25
6.2.1 (De)Installation und Aktualisierung	25
6.2.2 Informationen zu Paketen	26
6.2.3 Problemlösung	26
6.3 debconf	26
6.4 Installation automatisieren	27
7 Pakete bauen	29
7.1 Pakete aus Debian-Quellen	29
7.2 Pakete aus Quelltexten	29
8 Sichern	31
8.1 Sicherung von Dateien/Verzeichnissen	31
8.2 Wiederherstellung von Dateien/Verzeichnissen	31
8.3 Sichern von Partitionen und ganzen Festplatten	32
8.3.1 Kleiner Leitfaden	32
8.4 Wiederherstellen von ganzen Festplatten oder Partitionen	44
8.5 Sicherungen in VirtualBox	45
9 Notfallkoffer	47
9.1 Ausfälle anderer Art	47
10 Fehler identifizieren (und lösen)	49
10.1 Suchmaschinen füttern	49
10.2 "Programmgesprächigkeit" erhöhen	49
10.3 Systemfehler finden	49
10.4 Was läuft?	50
10.5 Wer sendet?	50
10.6 Programme belauschen	50
10.7 Unterschiede zwischen Systemen	50
11 Bootmanager und Live-Linux	53
11.1 Live-Linux booten	53
11.2 GRUB reparieren	54
11.3 Aufräumarbeiten	54
12 Paßwort vergessen	55
13 Was gibt es sonst noch? – Befehlsübersicht	57
13.1 Automatisch zu einer Zeit ausführen	57
13.2 Benutzer- und Gruppen	57
13.2.1 Benutzerverwaltung	57
13.2.2 Benutzer wechseln bzw. Kommandos unter anderem Konto ausführen	57
13.2.3 Gruppenverwaltung	57
13.3 Datenrettung	58
13.4 Datenträgerüberprüfung	58

13.5	Formatieren	58
13.6	Datensicherung	58
13.7	Dateien konvertieren	58
13.8	Dateien und Dateiteile	58
13.9	Textdateien editieren	58
13.9.1	Zeilen sortieren / durcheinanderwürfeln	58
13.9.2	Zeichen einfügen und entfernen	59
13.9.3	Menschgesteuerte Editoren	59
13.9.4	Skriptgesteuerte Editoren	59
13.10	Dateien vergleichen	59
13.11	Packen und entpacken	59
13.11.1	Packer für einzelne Dateien	59
13.11.2	Packer für mehrere Dateien	59
13.12	Bilder konvertieren/bearbeiten	59
13.13	Drucker	59
14	Lizenz und weitere Informationen	61
14.1	Lizenz	61
14.2	Weitere Informationen	61

Kapitel 1

Workshopvorbereitungen

1.1 Was muß ich mitbringen?

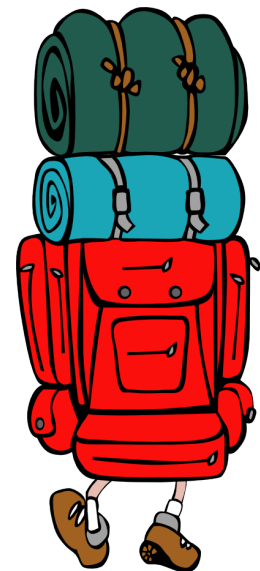
Zum Workshop mitzubringen sind: Laptop mit installiertem VirtualBox und darin importierter Debian-Admin-Workshop-Appliance, sowie funktionierendes W-Lan bzw. Netzwerkkarte (+ Kabel) und dieses Workshop-PDF. Sowie eine aktuelle ISO-Datei der Live-Linux-Distribution Knoppix ¹ (ca. 700 MB).

1.2 Debian-Admin-Workshop-Appliance

Für den Workshop wurden extra zwei virtuelle Maschinen (VMs) erstellt und in ein Installationspaket verpackt. Dieses Installationspaket – auch Appliance genannt – kann nun auf anderen Rechnern importiert werden, um die beiden VMs zu erhalten. Das Installationspaket kann von der Projektseite ² (oder als Kurzurl: <http://is.gd/k1jrV7>) heruntergeladen werden.

1.3 Die beiden VMs

Bei den beiden VMs handelt es sich um ein mit m23 ³ aufgesetztes Debian ⁴ Wheezy (erweitert um systemd ⁵ aus testing), auf dem die Aufgaben des Workshops gelöst werden sollen und eine VM mit der Firewalldistribution IPCop ⁶, die als virtueller Router genutzt wird. Die letztere VM muß während des Workshops zwecks Internetverbindung angeschaltet sein, braucht jedoch nicht verändert zu werden.



¹<http://www.knopper.net/knoppix-mirrors/>

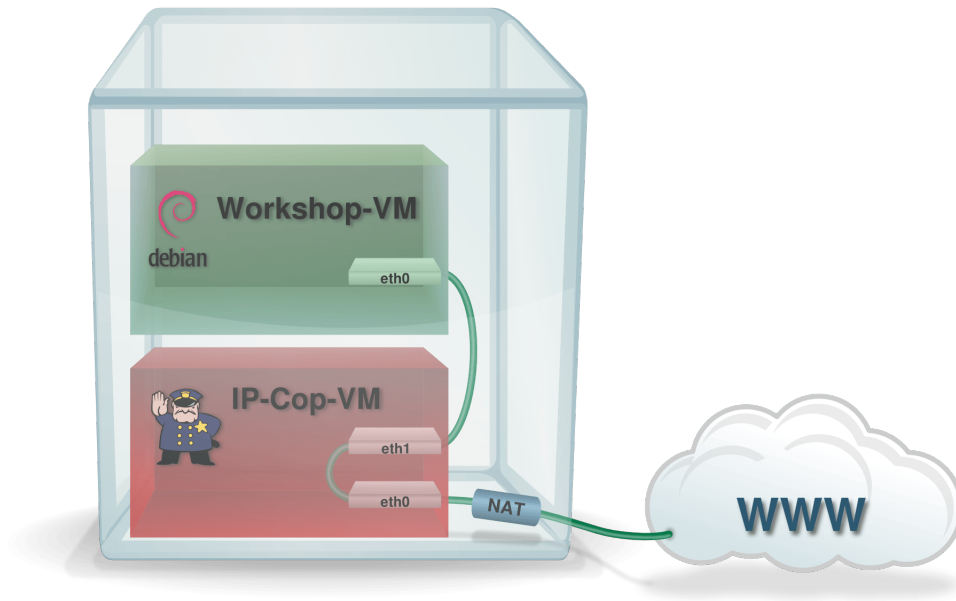
²<http://sf.net/projects/dodger-tools/files/vms/Debian-WS2a.ova/download>

³<http://m23.sf.net>

⁴<http://debian.org>

⁵<http://de.wikipedia.org/wiki/Systemd>

⁶<http://www.ipcop.org>



1.4 Import

Das Installationspaket läßt sich unter VirtualBox ⁷ importieren. Hierzu lädt man VirtualBox für das eigene Betriebssystem herunter und installiert es, wie auf der VirtualBox-Seite angegeben. Danach startet man VirtualBox und importiert die Appliance wie folgt:

-
-
- Dann die heruntergeladene Datei `Debian-WS.ova` auswählen.
-
- Wichtig: "*Zuweisen neuer MAC-Adressen für alle Netzwerkkarten*" bleibt **DEAKTIVIERT**.
-
- Etwas warten ... (die "Debian-Admin-Workshop"-VM kann absichtlich keine Netzwerkverbindung aufnehmen, daher dauert hier das Starten etwas länger)
- Fertig

1.5 Benutzer und Paßworte

Nutzername / Paßwort für die "Debian-Admin-Workshop"-VM: `test / test` und `root / test`. Für die "IPCop"-VM: `root / testtest` (nur der Vollständigkeit halber erwähnt, wird nicht benötigt). Die Weboberfläche von IPCop ist zudem über HTTPS auf dem Port 8443 mit `admin/testtest` zu erreichen (`https://192.168.1.4:8443`) – dies allerdings nur innerhalb des abgetrennten virtuellen Subnetzwerkes und nicht direkt vom Gastgeber-Rechner.

⁷<http://www.virtualbox.org>

Kapitel 2

Grundlagen

2.1 "root" werden

"Ich bin root, ich darf das!". Aber wie wird man root? Unter Debian hilft das Kommando `su ↵`, unter Ubuntu und anderen `sudo bash ↵`. Für alles, was nun folgt, werden entweder root-Rechte benötigt oder es stellt keinen Nachteil dar, diese Schritte als root durchzuführen.

Aber immer bedenken: "Mit großer Macht kommt auch große Verantwortung".

Im "wahren Leben" sollte man sich vor jeder Eingabe auf der Kommandozeile gut überlegen, ob Rootrechte notwendig sind und diese so selten wie möglich einsetzen. Wenn man nicht weiß, ob man root sein muß, um eine bestimmte Aktion durchführen zu können, sollte man es zunächst ohne Rootrechte versuchen – normalerweise weist einen das System darauf hin, wenn dies nicht erfolgreich war.

Es ist auch möglich, jedem Root-Befehl ein `sudo ↵` voranzustellen, ohne sich zuvor als root eingeloggt zu haben. Dies erfordert jedoch, daß das Programm "sudo" auf dem Rechner auch installiert ist - und der eigene Benutzer auf Ubuntu und -Derivaten Mitglied der Gruppe "sudo" ist.



2.2 Distribution und Hardware

Wo bin ich denn hier?

Grundlegende Informationen zum Rechner (Architektur, etc.) bietet die Ausgabe von `uname -a ↵`. Die Bezeichnung der Distribution läßt sich durch ein einfaches `cat /etc/issue ↵` oder `lsb_release -a ↵` ermitteln.

`uname -a ↵` gibt Informationen über den Namen, die Architektur, den Kernel und den Prozessor des Systems aus. Der Parameter -a oder --all sagt uname, daß es alle Informationen ausgeben soll. Mit `hwinfo ↵`, `dmidecode ↵`, `lspci ↵`, `lsusb ↵` und `lscpu ↵` können Hardware-Informationen ermittelt werden.

Informationen über den Arbeits- und Swapspeicher gibt es mit `free ↵`

`cat ↵` ist ein GNU-Werkzeug, das Inhalte von Dateien einliest und auf die Standardausgabe (in diesem Fall das Terminal) ausgibt. In der Datei `/etc/issue` ist der Name der Distribution angegeben.

Über `lsb_release -a ↵` können die Distributions-Informationen über die LSB-Schnittstelle (Linux Standard Base ¹) ausgelesen werden.

¹http://de.wikipedia.org/wiki/Linux_Standard_Base

2.3 Partitionierung, Mountpunkte, Laufwerksfüllstand

Partitionen und weitere (Pseudo-)Dateisysteme werden in den Verzeichnisbaum eines Linux-Systems eingehängt (gemountet). Über `fdisk -l` oder `parted -l` werden die Partitionen auf allen Laufwerken ausgegeben. `mount` gibt eine Übersicht über den Einhängestatus und `df` zeigt den Füllstand an.

2.4 Pfadangaben

Linux kennt zwei verschiedene Arten von Pfadangaben, die zu einer Datei oder einem Verzeichnis führen:

- Die absolute Pfadangabe: `/etc/apt/sources.list`
- Die relative Pfadangabe. Hier: Die Datei eine Ebene über dem aktuellen Verzeichnis: `../datei.txt`
- Die relative Pfadangabe. Hier: Die Datei eine Ebene unter dem aktuellen Verzeichnis: `unterverzeichnis/datei.txt`
- Ausführen einer Datei im aktuellen Verzeichnis: `./mein-Shell-Skript.sh`
- Verwenden einer Datei im aktuellen Verzeichnis (mit einem Programm): `nano datei.txt`
- Datei im Heimatverzeichnis (`~`) des aktuellen Benutzers: `~/datei.txt`

2.5 Die Arbeit beschleunigen

Auch wenn es in Filmen "cool" aussieht, wenn "Hacker" wüst auf ihre Tastatur einhacken, sollte man unnötige Schreibarbeit vermeiden, da Tippen fehleranfällig ist und die BASH² einem viel Arbeit abnehmen kann.

Hierzu ein paar "Tipps" zum Vermeiden von "Tippen":

- Mit den Tasten `↑` und `↓` kann man durch die bereits eingegebenen Befehlszeilen blättern.
- Die Tasten `←` und `→` bewegen den Cursor in der aktuellen Zeile.
- `Strg+r` startet die Suche in bereits eingegebenen Kommandozeilen. Danach gibt man einen Suchbegriff ein, worauf die erste passende Zeile als Vorschlag angezeigt wird. Gibt es mehrere auf den Suchbegriff passende Zeilen, so zaubert `Strg+r` die jeweils nächste Zeile auf den Bildschirm. Möchte man den Vorschlag annehmen, so drückt man abschließend `↵`.
- Wenn es um Befehle (und ggf. deren Parameter), Dateien und Verzeichnisse geht, reicht es, die (eindeutigen) Anfangsbuchstaben einzugeben und anschließend `→` (Tabulator-Taste) zu drücken. Gibt es nur einen Befehl (, Datei, ...), der mit den Buchstaben beginnt, so erscheint dieser auf der Kommandozeile. Sollte das nicht der Fall sein, so hilft ein weiterer Druck auf `→`, um alle passenden Befehle (...) aufzulisten. Anschließend hilft die Erweiterung der bereits eingegebenen Buchstaben um weitere, damit der Befehl (...) eindeutig gefunden werden kann. Sind genug eindeutige Buchstaben eingegeben, so vervollständigt `→` abschließend.
- Das Paket "gpm" erweitert die tastaturbasierte Kommandozeile um einen Mauszeiger. Durch Klicken und Ziehen des Zeigers können Textbereiche markiert und durch Klicken der mittleren Maustaste (bzw. durch gleichzeitiges Drücken von linker und rechter Maustaste) der Text an der Position des Textcursors wieder eingefügt werden.
- `Shift+←` Springt mit dem Cursor ein Wort nach links.
- `Shift+→` Springt mit dem Cursor ein Wort nach rechts.
- `Shift+Bild↑`: Vorherige Bildschirmseite.
- `Shift+Bild↓`: Nachfolgende Bildschirmseite.

²http://de.wikipedia.org/wiki/Bourne-again_shell

- `Strg + u` löscht alles links vom Cursor.
- `Strg + w` löscht das letzte Wort links vom Cursor.
- `Alt + d` löscht das nächste Wort (bzw. den nächsten Wortteil) rechts vom Cursor.
- `Strg + w` löscht das letzte Wort links vom Cursor.
- `Strg + s` verhindert (in einigen Shells) die Eingabe von weiteren Befehlen.
- `Strg + q` hebt die Sperrung wieder auf.

Hinweis

Eine Installation von Software auf der Workshop-VM ist allerdings erst möglich, wenn das Netzwerk repariert wurde! (siehe Seite 19)

2.6 Praktische Helfer

Der Zweispaltendateimanager "Midnight Commander"³ (Paket "mc") ist ein praktisches Werkzeug für viele Dateioperationen (Aufruf mit `mc ↵`).

Wer vi, vim und Konsorten mag und damit umzugehen weiß, wird mit dem wenig kryptischen Texteditor "Nano" wenig anfangen können. Wer es aber lieber einfach mag, findet in diesem einen gut zu bedienenden Editor für alle Textdateien (Aufruf mit `nano <Name der existierenden oder neuen Datei> ↵`). Nano kann sowohl eine vorhandene Datei öffnen, als auch neue anlegen.

```

GNU nano 2.2.6                               Datei: /tmp/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.13.123
    netmask 255.255.255.0
    network 192.168.13.0
    broadcast 192.168.13.255
    gateway 192.168.13.1

^G Hilfe           ^O Speichern      ^R Datei öffnen  ^Y Seite zurück  ^K Ausschneiden  ^C Cursor
^X Beenden        ^J Ausrichten    ^W Wo ist       ^V Seite vor    ^U Ausschn. rück ^T Rechtschr.

```

Mit der Tastenkombination `Strg + x` beendet man Nano wieder. Sollte man Änderungen an der Datei vorgenommen haben, so fragt Nano aber vorher, ob diese gespeichert werden sollen. Die Suchfunktion startet man mit `Strg + w` . Weitere Funktionen stehen unteren Rand im Editor, wobei "^" für die Taste `Strg` .

³http://de.wikipedia.org/wiki/Midnight_Commander

2.7 Kopieren, verschieben, löschen

Wem "mc" zu komfortabel sein sollte oder wenn "mc" nicht zur Verfügung steht, gibt es natürlich Kommandozeilenwerkzeuge für alle Dateioperationen:

- Verzeichnis(se) anlegen: `mkdir <Verzeichnisname1> <Verzeichnisname2>`
- Datei(en) kopieren: `cp <Datei1> <Datei2> <Zielverzeichnis>`
- Datei kopieren und umbenennen: `cp <Datei> <Datei neuer Name>`
- Datei in anderes Verzeichnis kopieren und umbenennen: `cp <Datei> <Pfad/Datei neuer Name>`
- Verzeichnis(se) kopieren: `cp -r <Verzeichnis1> <Verzeichnis2> <Zielverzeichnis>`
- Datei(en) verschieben: `mv <Datei1> <Datei2> <Zielverzeichnis>`
- Datei umbenennen: `mv <Datei> <Datei neuer Name>`
- Datei(en) löschen: `rm <Datei1> <Datei2>`
- Leere(s) Verzeichis(se) löschen: `rmdir <Verzeichnis1> <Verzeichnis2>`
- Verzeichis(se) mit Unterverzeichnissen und Dateien löschen: `rm -r <Verzeichnis1> <Verzeichnis2>`

Sollen beim Kopieren die Zugriffsrechte mitkopiert werden, so bewirkt dies der zusätzliche Parameter `-a`.

2.8 Benutzer und Gruppen

Damit alles seine Ordnung hat, benötigt sowohl jeder menschliche Benutzer als auch jeder Dienst/Dämon (siehe Seite 17) eine Benutzerkennung für die Anmeldung am System. Welche Benutzerkonten das System kennt, verrät `getent passwd` und wer derzeit angemeldet ist `users` bzw. `who`. Die Liste der Benutzer, die in der Vergangenheit angemeldet waren, gibt `last` aus. Eine Komplettübersicht (Benutzerkennung + Nummer, primäre Gruppe + Nummer und alle weiteren Gruppen + Nummern, in denen der Benutzer ist) des eigenen Benutzers erhält man mit `id`.

Benutzer sind meist zusätzlich in einer Reihe von Gruppen, da ansonsten die Zugriffsverwaltung unnötig kompliziert würde. So gibt es Gruppen, die den Zugriff auf Soundkarte oder Scanner erlauben. Jeder Benutzer, der in diesen Gruppen ist, darf also Soundkarte und Scanner benutzen, die anderen bleiben außen vor. Die Gruppen, in denen man selbst ist, ermittelt `groups` und alle dem System bekannten Gruppen `getent group`.

Hinweis

Mehr zu Benutzern und Gruppen (siehe Seite 57)

2.9 Zugriffsrechte

Unter Linux besitzen jede Datei und jedes Verzeichnis Zugriffsrechte, die regeln, wer wie und ob zugreifen darf. Mit `ls -l` kann man sich die ausführliche Liste der Dateien und Verzeichnisse (inklusive Zugriffsrechten) ausgeben lassen.

```

1 lrwxrwxrwx 1 peter gruppea      13  4. Apr 2012  todo.txt -> /backup/todo.txt
2 -rw-r--r-- 1 paul  gruppeb    65536  1. Jan 2012  Paulschreibt-andere-lesen.txt
3 -rw-rw-r-- 1 peter gemeinsamegruppe 128 18. Aug 2013  Gruppentext.txt
4 -rw----- 1 paul  paul      7889 21. Jul 23:26 Paulsgeheime_Gedanken.txt
5 drwxr-xr-x 2 paul  paul      4096 23. Jul 2012  Paulschreibt-andere-lesen

```

Das Schema ist folgendes:

<Typ><BBB><GGG><AAA> <H> <Benutzer> <Gruppe> <Größe> <Änderungszeit> <Datei-/Verzeichnisname>

Der Typbezeichnung, bei der "-" für eine Datei, "d" für ein Verzeichnis und "l" für einen symbolischen Link steht, folgt ein Block von 3 * 3 Zeichen. Dabei steht der erste Block für die Rechte des Besitzers, der zweite für die Rechte der Gruppe und der letzte für alle anderen. "r" steht für das Leserecht, "w" für das Schreib-/Änderungsrecht und "x" für das Ausführungsrecht. Nach den Rechten folgt eine Angabe der Anzahl der Hardlinks ⁴ auf die Datei (mind. 1) oder das Verzeichnis (mind. 2). Danach kommen der Name des Besitzers, dann der der Gruppe, die Dateigröße, dann die Änderungszeit und abschließend der Name der Datei bzw. des Verzeichnisses oder Informationen über den symbolischen Link.

`ls` steht dabei für "list" und ist damit wohl einer der am häufigsten genutzten Shell-Befehle. Der Parameter `-l` sorgt dafür, daß sovielen Informationen wie möglich über die aufgelisteten Dateien und Verzeichnisse ausgegeben werden. Ein zusätzliches `-a` zeigt alle, also auch versteckte, Dateien an.

2.9.1 Besitzer und Gruppe ändern

- Besitzer ändern: `chown <Neuer Besitzer> <Datei-/Verzeichnisname>`
- Gruppe ändern: `chgrp <Neue Gruppe> <Datei-/Verzeichnisname>`
- Besitzer und Gruppe ändern: `chown <Neuer Besitzer>:<Neue Gruppe> <Datei-/Verzeichnisname>`

Sollen bei den Verzeichnissen die Unterverzeichnisse und enthaltene Dateien mit eingeschlossen werden, so kommt noch der Parameter `-R` hinzu.

2.9.2 Zugriffsrechte ändern

Die Zugriffsrechte für Besitzer, Gruppe und Andere können jeweils als Zahl angegeben werden. Das Leserecht hat den Wert 4, das Schreib-/Änderungsrecht "2" und das Ausführenrecht "1". Sollen mehrere Rechte vergeben werden, so werden die Werte einfach addiert (z.B. Lesen (4) + Schreiben (2) = 6). Das Ändern der Rechte geschieht mit `chmod <BGA> <Datei-/Verzeichnisname>`.

Beispiel: `chmod 754 info.txt` erlaubt dem Besitzer das Lesen, Schreiben und Ausführen, der Gruppe das Lesen und Ausführen und anderen das Lesen der Datei `info.txt`.

Sollen hierbei Verzeichnisse, Unterverzeichnisse und enthaltene Dateien mit eingeschlossen werden, so kommt ebenfalls der Parameter `-R` hinzu.

Alternativ können auch symbolische Parameter verwendet werden: Zugriffsrechte werden hierbei mit einem "+" hinzu, mit einem "-" entfernt und mit "=" überschrieben. Das Leserecht hat das Symbol "r", das Schreib-/Änderungsrecht "w" und das Ausführenrecht "x". Der Besitzer hat das Kürzel "u" (user), die Gruppe "g" (group) und Andere "o" (others). Sollen Rechte für alle drei Gruppen gleichzeitig geändert werden, so lautet das Kürzel "a" (all).

Beispiele: `chmod u-wx info.txt` entzieht dem Benutzer das Recht auf Schreiben und Ausführen, behält aber ein ggf. vorhandenes Lesen-Recht bei. Mit `chmod g=rx info.txt` darf die Gruppe Lesen und Ausführen, aber nicht Schreiben, da kein "x" mitangegeben ist.

2.10 Dateien Suchen und finden

Häufig ist es nötig, Dateien zu finden. Hierbei helfen die Programme `grep` und `find`. Weiterhin gibt es noch `locate`, was sehr schnell, jedoch auf einen regelmäßig aktualisierten Suchindex (`updatedb`) angewiesen ist,

⁴<http://de.wikipedia.org/wiki/Hardlink>

sowie `whereis`, das in Standardpfaden nach Dateien sucht, die zu einem angegebenen Programm gehören.

- Dateien im aktuellen Verzeichnis und Unterverzeichnissen (`-r`) suchen, deren Inhalt die Zeichenkette "test" enthält: `grep test -r .`

- Groß-/Kleinschreibung von "test" ignorieren (`-i`): `grep test -r -i .`

- Nur Dateinamen (`-l`) mit Treffern ausgeben: `grep test -r -i -l .`

- Datei-/Verzeichnisnamen, die "test" enthalten, im aktuellen Verzeichnis und Unterverzeichnissen suchen:

```
find | grep test
```

Hierbei gibt `find` (ohne Parameter) einfach alle Datei- und Verzeichnisnamen aller Unterverzeichnisse aus und "grep" sucht in dieser Ausgabe nach dem Suchbegriff. Der senkrechte Strich dazwischen (das Pipe-Symbol) sorgt dafür, daß die Ausgabe des ersten Programmes an das nachfolgend angegebene Programm übergeben wird.

Den absoluten Pfad von ausführbaren Dateien ermittelt man mit `type <Befehl>`.

2.11 man und --help

Wenn mal kein Netz zur Verfügung stehen sollte oder weil es bei einigen Dingen einfach schneller ist, Hilfetexte direkt aus dem System zu bekommen, soll das Kommando `man <Befehl>` nicht unerwähnt bleiben. Neben "man" bieten viele Programme auch eine eingebaute (meist kürzere) Hilfe an, die mittels `<Programm> --help` aufgerufen wird. Wenn `--help` nicht zum Erfolg führt, kann der Parameter auch (nach absteigender gefühlter Vorkommenshäufigkeit sortiert) `-help`, `-h` oder `-?` heißen. Alternativ kann das Programm den Hilfetext auch ausgeben, wenn kein Parameter oder ein ungültiger Parameter angegeben wird. Einfach mal ausprobieren...

2.12 Befehle nach Stichwort suchen

Will man nur eine kurze Erklärung zu einem Kommando bekommen, so hilft `whatis <Befehl>` weiter.

Umgekehrt geht es allerdings auch: `apropos <Stichwort>` liefert passende Kommandos, die zu einem Stichwort passen. Möchte man die Ausgabe auf Programme eingrenzen, so liefert

`apropos <Stichwort> | grep '(1)'` eine solche Liste. Andernfalls werden auch Befehle von Programmierschnittstellen aufgelistet, die nicht von der Kommandozeile aus verfügbar sind.

2.13 Neustart und Herunterfahren

Hin und wieder muß selbst ein Linux-Rechner neugestartet werden. Sei es nur, um zu überprüfen, ob eine neue Konfiguration auch nach dem nächsten Booten noch funktioniert. `reboot` fährt den Rechner sauber herunter, beendet dabei alle (auch im Hintergrund) laufenden Programme und startet den Rechner neu. Falls dies nicht funktionieren sollte, führt `reboot -f` einen sofortigen Neustart aus, bei dem auch Daten verlorengehen können. Wenn sich der Rechner nach Abschluß der administrativen Tätigkeit eine Ruhepause verdient hat, so kann man ihm mit `poweroff` ausschalten.

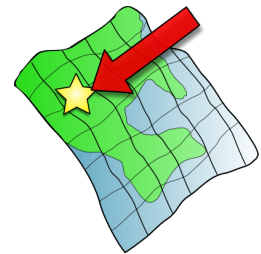
Kapitel 3

Was ist wo?

Ein kleiner Wegweiser durch den Linux-Verzeichnisbaum.

- Ausführbare Dateien für alle Benutzer: `/bin` und `/usr/bin`
- Ausführbare Dateien für root: `/sbin` und `/usr/sbin`
- Gerätedateien: `/dev`
- Kernel und Initrd: `/boot`
- grub: `/boot/grub`
- Globale Einstellungen: `/etc`
- Globale Programmeinstellungen: `/etc/Programmname` oder `/etc/default/Programmname`
- Benutzerverzeichnisse: `/home/Benutzername`
- Start-/Stop-Skripte: `/etc/init.d`
- Protokolldateien: `/var/log`

Siehe auch Filesystem Hierarchy Standard (FHS) ¹



¹http://de.wikipedia.org/wiki/Filesystem_Hierarchy_Standard

Kapitel 4

Dienste und Dämonen

Die Dämonen sind die dienstbaren Geister des Systems oder einfach ausgedrückt, Programme, die im Hintergrund unauffällig ihren Dienst versehen (bzw. sollten). Der Apache-Webserver z.B. läuft als Dämon, um Seitenanfragen entgegenzunehmen und zu beantworten. Doch auch auf reinen Desktopsystemen laufen eine Reihe von Dämonen wie z.B. ein Dämon zum automatischen Apassen der CPU-Taktfrequenz. Viele Dämonen werden direkt beim Systemstart mitgestartet.



4.1 SysVinit

Das SysVinit¹ ist zwar schon etwas in die Jahre gekommen, aber in der einen oder anderen Form noch auf vielen Systemen vorhanden. Es ist der erste Prozeß, der beim Hochfahren vom Kernel gestartet wird und sorgt dann dafür, daß die anderen Dienste in einer festgelegten Reihenfolge gestartet werden. Daher kann es nicht schaden, sich damit auseinanderzusetzen:

- Liste aller Dämonen ausgeben: `service --status-all ↵`
- (Gestoppten) Dämon starten: `/etc/init.d/<Dämon> start ↵` oder `service <Dämon> start ↵`
- (Gestarteten) Dämon stoppen: `/etc/init.d/<Dämon> stop ↵` oder `service <Dämon> stop ↵`
- (Laufenden) Dämon beenden und neu starten: `/etc/init.d/<Dämon> restart ↵` oder `service <Dämon> restart ↵`

Neben den Kommandos "start", "stop" und "restart" können je nach Dämon weitere hinzukommen. Normalerweise verrät `/etc/init.d/<Dämon> ↵` die möglichen Kommandos.

4.2 Upstart

Upstart² ist eine Alternative zum klassischen SysVinit und wird unter Anderem bei Ubuntu verwendet. Teilweise sind auf ein und demselben System auch beide – SysVinit und upstart – anzutreffen, was auch gelegentlich zu Problemen durch eine von der Planung abweichende Startreihenfolge führen kann.

- Liste aller Dämonen ausgeben: `initctl list ↵`

¹<http://de.wikipedia.org/wiki/SysVinit>

²<http://de.wikipedia.org/wiki/Upstart>

- (Gestoppten) Dämon starten: `initctl start <Dämon>`
- (Gestarteten) Dämon stoppen: `initctl stop <Dämon>`

4.3 systemd

systemd³ ist ein weiteres init-System, das ab Debian 8 Jessie und in den kommenden Ubuntu-Veröffentlichungen zum Standard wird. Angeblich soll es sogar den BAFH-Ausredekalendar und einen Quake-Server enthalten...

- Liste aller Dämonen ausgeben: `systemctl -all`
- (Gestoppten) Dämon starten: `systemctl start <Dämon>`
- (Gestarteten) Dämon stoppen: `systemctl stop <Dämon>`
- Status- und Loginformationen über Dämon abfragen: `systemctl status <Dämon>`
- Loginformationen über Dämon abfragen: `journalctl -u cron`

Die Service-Dateien, die quasi die Funktion der Initskripte übernehmen liegen in den Verzeichnissen `/lib/systemd/system` und `/etc/systemd/system`. Sollten in beiden Verzeichnissen gleichlautende `.service`-Dateien liegen, so haben die aus `/etc/systemd/system` Vorrang.

Hinweis

Zumindest unter Debian 8 sind unter `/etc/init.d/<Dämon>` die Initskripte vorhanden, sodaß man weiterhin die Vorzüge der Autovervollständigung mit `TAB` genießen kann.

³<http://de.wikipedia.org/wiki/Systemd>

Kapitel 5

Netzwerk

Was wäre das Leben ohne Netzwerk? Ziemlich öde oder vielleicht auch deutlich produktiver (ohne die ganzen Ablenkungen)... Jedenfalls kann es nützlich sein, wenn man weiß, wie man das Netzwerk selbst einrichtet. Bei der Workshop-VM ist es zumindest zunächst kaputt...



5.1 Aktuelle Netzwerkeinstellungen

Das Kommando `ifconfig` gibt einen einfachen Überblick über die aktuellen Einstellungen aller aktiven Netzwerkkarten:

```
1 eth0      Link encap:Ethernet  Hardware Adresse 00:f3:ab:77:3d:28
2          inet Adresse:192.168.1.123  Bcast:192.168.1.255  Maske:255.255.255.0
3          inet6-Adresse: fe80::200:f0fe:fe83:83f6/64  Gueltigkeitsbereich:Verbindung
4          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metrik:1
5          RX packets:850053  errors:0  dropped:0  overruns:0  frame:0
6          TX packets:533491  errors:0  dropped:0  overruns:0  carrier:0
7          Kollisionen:0  Sendewarteschlangenlaenge:1000
8          RX bytes:1021113415 (973.8 MiB)  TX bytes:63432614 (60.4 MiB)
9          Interrupt:19
10
11 lo       Link encap:Lokale Schleife
12          inet Adresse:127.0.0.1  Maske:255.0.0.0
13          inet6-Adresse: ::1/128  Gueltigkeitsbereich:Maschine
14          UP LOOPBACK RUNNING  MTU:16436  Metrik:1
15          RX packets:917067  errors:0  dropped:0  overruns:0  frame:0
16          TX packets:917067  errors:0  dropped:0  overruns:0  carrier:0
17          Kollisionen:0  Sendewarteschlangenlaenge:0
18          RX bytes:725063143 (691.4 MiB)  TX bytes:725063143 (691.4 MiB)
19
20 wlan0    Link encap:Ethernet  Hardware Adresse 00:2e:2d:56:34:cc
21          UP BROADCAST MULTICAST  MTU:1500  Metrik:1
22          RX packets:0  errors:0  dropped:0  overruns:0  frame:0
23          TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
24          Kollisionen:0  Sendewarteschlangenlaenge:1000
25          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

In diesem Beispiel kennt das System drei Netzwerkanschlüsse:

- Die "echte" Netzwerkkarte für kabelgebundenes Netzwerk (ab Zeile 1)
- Die "lokale Schleife" oder das "Loopback" (ab Zeile 11), eine "Art Netzwerk" (tm), das die Kommunikation von lokal installierten Servern und Clients untereinander erlaubt (sodaß man z.B. auf die nur lokal vorhandenen Webseiten, die von einem lokal installierten Server generiert werden, auch lokal zugreifen kann)

- Die WLAN-Karte (ab Zeile 20). Diese hat aktuell keine "inet Adresse" bzw. "inet6-adresse", also keine IP - sie ist damit nicht aktiv.

5.2 Netzwerkfehler identifizieren

Wenn das Netzwerk streikt, kann folgende Testreihe zum Erkennen des Fehlers beitragen:

- Hat die Netzwerkkarte(n) eine "richtige" IP?: `ifconfig ↵`
- Welche Router/Gateway(s) sind gesetzt?: `route -n ↵`
- Kann der Router/Gateway "gepingt" werden?: `ping <Router-IP> ↵`
- Kann ein Server im Internet erreicht werden?: `ping 8.8.8.8 ↵`
- Funktioniert die Namensauflösung?: `ping heise.de ↵`

Sollten alle Tests bestanden sein, so liegt anscheinend kein Fehler vor. Ansonsten kann auch schon einmal das Netzkabel herausgerutscht sein (abgebrochene Plastiknasen bei den Steckern), der Router ausgefallen oder falls `ifconfig ↵` die Netzwerkkarte gar nicht auflistet, der Netzkartentreiber fehlen.

Hat die Netzwerkkarte die falsche Bezeichnung (z.B. eth1 statt eth0), so kann dies daran liegen, daß durch udev¹ ein neuer Name vergeben wurde. In diesem Fall sollte man:

- Die udev-Regeldatei für Netzwerkkarten als Backup in ein anderes Verzeichnis verschieben. Die Datei ist `/etc/udev/rules.d/` wobei die Shell das Sternchen automatisch durch die Zahl ersetzt, die die Auswertungsreihenfolge der Regeln im Verzeichnis beschreibt und auf verschiedenen Systemen unterschiedlich sein kann. Das Verschieben geschieht schließlich mit `mkdir /etc/udevbackup ↵` und `mv /etc/udev/rules.d/*-persistent-net.rules /etc/udevbackup/*-persistent-net.rules ↵`
- Danach den Rechner neu starten: `reboot ↵`

5.3 Netzwerkeinstellungen per Hand

Wenn gar nichts mehr geht, kann man einen Rechner relativ einfach wieder ins Netz bringen. Dieses sollte man auf der Workshop-VM unbedingt tun, damit weitere Programme (mc, gpm, ...) installiert und auch das Debian-System aktualisiert werden können.

5.3.1 Statische IP

Mit drei Zeilen werden alle nötigen Einstellungen vorgenommen. Im Beispiel soll die erste Netzwerkkarte (eth0) des eigenen Rechners die IP "192.168.1.123" zugewiesen bekommen. Die IP des Routers/Gateways ist "192.168.1.4" und der öffentliche nicht zensierende DNS-Server besitzt die IP "85.88.19.10". Diese Einstellungen sind jedoch temporär und gehen nach dem nächsten Booten wieder verloren.

- IP setzen: `ifconfig eth0 192.168.1.123 ↵`
Hiermit wird für die Netzwerkkarte (eth0) die IP auf 192.168.1.123 gesetzt.
- Gateway: `route add -net default gw 192.168.1.4 ↵`
Jetzt teilt man dem System noch mit, über welchen Computer (Router) es das Internet erreichen kann. In diesem Fall ist das die IPCop-VM.

¹<http://de.wikipedia.org/wiki/Udev>

- DNS: `echo 'nameserver 85.88.19.10' > /etc/resolv.conf ↵`

Nun benötigt das System noch eine Angabe dazu, welcher DNS-Server zur Namensauflösung genutzt werden soll. Dieser wird in die Datei `/etc/resolv.conf` eingetragen.

Hinweis

Eine falsche Route kann mit `route del -net default gw <IP des falschen Routers> ↵` gelöscht werden.

5.3.2 Dynamische IP

Werden Netzwerkeinstellungen dynamisch durch einen DHCP-Server vergeben, so holt `dhclient ↵` die Informationen direkt vom DHCP-Server. Sollte das nicht funktionieren, so hilft ggf. `dhclient -r eth0 ↵`, wodurch die Bindung der 1. Netzwerkkarte an den DHCP-Server gelöst wird und dann `dhclient eth0 ↵` zum erneuten Konfigurieren der Netzwerkkarte mit den Angaben des DHCP-Servers.

Hinweis

Bei der Workshop-VM funktionieren beide Methoden, da die IPCop-VM auch einen DHCP-Server bereitstellt.

Hinweis

Wenn einmal nicht klar ist, welche Maschine eigentlich als DHCP-Server fungiert, kann man dies in der Datei `/var/lib/dhcp/dhclient.leases` nachschauen. Die IP des DHCP-Servers findet sich in der Zeile, die mit "option dhcp-server-identifizier" beginnt.

5.4 Netzwerkeinstellungen über Dateien

Damit die Einstellungen nicht bei jedem Neustart verlorengehen, werden diese in der Datei `/etc/network/interfaces` definiert. Als Orientierung können diese beiden Beispiele (statische und dynamische Adreßzuweisung) für `/etc/network/interfaces` dienen:

```

1 #Statische IP
2 allow-hotplug eth0
3 iface eth0 inet static
4     address 192.168.1.123
5     netmask 255.255.255.0
6     network 192.168.1.0
7     broadcast 192.168.1.255
8     gateway 192.168.1.100
9
10 #Dynamische IP (DHCP):
11 allow-hotplug eth0
12 iface eth0 inet dhcp

```

Die IP des DNS-Servers landet in der Datei `/etc/resolv.conf` mit folgender Notation: `nameserver 85.88.19.10`

Diese schreibt man z.B. mit `nano /etc/resolv.conf ↵` oder

`echo 'nameserver 85.88.19.10' > /etc/resolv.conf ↵`.

Daß die Änderungen wirksam werden, bewirkt `/etc/init.d/networking restart ↵`. Sollte das nicht funktionieren, hilft ein Neustart mit `reboot ↵`.

5.5 Fernzugriff

Auf die Shell von Linux-Systemen kann (bei entsprechender Einstellung) auch über das Netzwerk zugegriffen werden. Dieser Zugriff erfolgt in der Regel mittels Secure Shell (SSH²). Das Installationspaket, das hierfür benötigt wird heißt "openssh-server" (auf dem Zielrechner zu installieren) bzw. "openssh-client" (auf dem Rechner, an dem man arbeitet zu installieren).

Hinweis

Da die Workshop-VM sich in einem eigenen, vom Netzwerk des Gastgeber-Rechners getrennten, virtuellen Netzwerk befindet, ist eine direkte SSH-Verbindung vom Host-Rechner, auf dem die Virtualisierungssoftware läuft, zur Workshop-VM ohne weitere Einstellungen an der IPCop-Maschine / Änderungen an der Netzwerkkonfiguration der VM nicht möglich. Zum Ausprobieren empfiehlt sich daher hier das Herstellen einer Verbindung von der Workshop- zur IPCop-VM, auf der ein SSH-Server (auf Port 8022) läuft.

Ein "Anruf" mit SSH sieht dann so aus:

```
ssh -p <Port> <Benutzer>@<Rechner> ↵
```

Die Angabe `-p <Port>` wird nur dann benötigt, wenn der SSH-Server auf einem anderen als dem Standard-Port 22 lauscht. Mit "`<Benutzer>`" ist der Benutzer auf dem entfernten Rechner gemeint. Sind der Benutzername auf lokalem und entfernten System identisch, kann die Angabe von "`<Benutzer>@`" entfallen. "`<Rechner>`" steht für die IP des Rechners oder dessen auflösbaren Namen. Wird als zusätzlicher Parameter `-X` angegeben, so können sogar grafische Programme auf dem entfernten Rechner ausgeführt und die Ausgabe auf dem lokalen System benutzt werden, falls auf diesem ein X-Server installiert ist.

Zum Einloggen auf der IPCop-VM führt man folgende Zeile aus:

```
ssh -p 8022 root@192.168.1.4 ↵
```

Die dabei erscheinende Frage, ob man mit dem Verbindungsaufbau fortfahren möchte, ist mit "yes" zu Bejahen. Das Paßwort für den root-Benutzer ist "testtest". "root@ipcop" am Anfang der Eingabezeile zeigt da, daß man sich als Benutzer "root" auf dem Rechner "ipcop" befindet.

Hinweis

Die SSH-Shell kann mit der Tastenkombination `Strg + d` oder `exit ↵` beendet werden.

5.6 Kopieren über das Netzwerk

Für das Kopieren von Dateien und Verzeichnissen zwischen entferntem und lokalem System gibt es die Programme SCP³ und rsync⁴, wobei rsync mächtiger (Fortsetzen von abgebrochenen Kopieraktionen, "intelligentes" Kopieren, ...), aber auch nicht auf jedem System installiert, ist.

Beispiele:

- Datei /etc/issue von der IPCop-VM in das Verzeichnis /tmp auf die Debian-VM kopieren (Achtung: Großes "P" bei der Portangabe): `scp -P 8022 root@192.168.1.4:/etc/issue /tmp ↵`

- Lokales Verzeichnis "Adminzeug" mit Unterverzeichnissen `-r` in das Heimatverzeichnis von "admin" kopieren: `scp -r Adminzeug admin@entfernteKiste:~ ↵`

- Dasselbe mit rsync: `rsync -Pazy Adminzeug admin@entfernteKiste:~ ↵`

²<http://de.wikipedia.org/wiki/Ssh>

³http://de.wikipedia.org/wiki/Secure_Copy

⁴<http://de.wikipedia.org/wiki/Rsync>

Die Parameterkombination `-Pazy` steht dabei für Fortschrittsanzeige `-P`, Archivmodus `-a` (mit Unterverzeichnissen, symbolische Links als symbolische Links, Berechtigungen erhalten, Änderungszeiten erhalten, Gruppenzugehörigkeit erhalten, Besitzer erhalten, Gerätedateien und Spezialdateien erhalten), Dateien komprimiert übertragen `-z`, Optimierung der übertragenen Datenmenge `-y`.

Kapitel 6

Paketverwaltung

(Fast) Jede Linux-Distribution verwendet eine Paketverwaltung, um Software zu installieren, deinstallieren oder zu aktualisieren. Bei Debian und abgeleiteten Distributionen wird APT ¹ verwendet.



6.1 Quellen einrichten

Damit APT weiß, von wo die Pakete heruntergeladen/kopiert werden können, werden in der Datei `/etc/apt/sources.list` und/oder in `.list`-Dateien unter `/etc/apt/sources.list.d/` die Quellen festgelegt.

```
1 #Binär-Pakete
2 deb http://ftp.de.debian.org/debian/ wheezy main non-free contrib
3 deb http://security.debian.org/ wheezy/updates main contrib non-free
4 deb http://www.deb-multimedia.org wheezy main non-free
5
6 #Quellcode-Pakete
7 deb-src http://ftp.de.debian.org/debian/ wheezy main non-free contrib
8
9 #Lokale Paketquelle
10 deb file:/meinmirror/ wheezy main non-free contrib
11
12 #CD/DVD
13 deb cdrom:[Debian DVD]/ wheezy main non-free contrib
```

Hinter der Angabe der jeweiligen Art der Quelle ("*deb*" für fertige binäre Pakete, "*deb-src*" für Quellcode) folgen die Angabe der Quelladresse, der Version (hier *wheezy* + *testing*) und der Archivbereiche, aus denen Software geladen werden soll.

"*main*" beschreibt hierbei den Teil der Quelle, der ausschließlich Software enthält, die fest zur Distribution gehört. "*non-free*" enthält Software, die nach den Debian Free Software Guidelines ² als unfrei gilt, und "*contrib*" schließlich enthält Inhalte, die zwar selbst nach dieser Richtlinie als frei gelten, aber von Software aus *non-free* abhängig sind.

6.2 Software verwalten

6.2.1 (De)Installation und Aktualisierung

- Informationen über installierbare Pakete aktualisieren: `apt-get update`
- Installierbare Pakete suchen: `apt-cache search <Suchbegriff>`

¹http://de.wikipedia.org/wiki/Advanced_Packaging_Tool

²http://de.wikipedia.org/wiki/Debian_Free_Software_Guidelines

- Paket(e) installieren: `apt-get install <Paket1> <Paket2>`
- Paketdatei(en) installieren: `dpkg -i <Paket1.deb> <Paket2.deb>`
- Paket(e) entfernen: `apt-get remove <Paket1> <Paket2>`
- Installierte Pakete aktualisieren: `apt-get upgrade`
- Installierte Pakete aktualisieren (ggf. werden zusätzliche Pakete installiert): `apt-get dist-upgrade`

6.2.2 Informationen zu Paketen

- Liste (de)installierter Pakete: `dpkg --get-selections`
- Liste der installierten Pakete für die Benutzung mit `apt-get install`:

```
dpkg --get-selections | grep -v deinstall$ | tr -d '[:blank:]' | sed 's/install$/g' | awk -v ORS="" '{print($0" ")}'
```

- Alle Dateien in einem installierten Paket auflisten: `dpkg -L <Paket>`
- Welches *installierte* Paket enthält Datei/Verzeichnis?: `dpkg -S <Datei/Verzeichnis>`
- Informationen zu einem installierten Paket abfragen: `dpkg -s <Paketname>`
- Paketinhalte von verfügbaren Paketen aktualisieren: `apt-file update`
- Welches *verfügbare* Paket enthält Datei/Verzeichnis?: `apt-file search <Datei/Verzeichnis>`

6.2.3 Problemlösung

Wurde die Installation von Paketen unterbrochen (z.B. wegen nicht erfüllter Abhängigkeiten nach einer manuellen Paketinstallation mittels `dpkg -i Paket.deb`), so kann diese mit `apt-get install -f` wieder aufgenommen werden.

In seltenen Fällen (meist, wenn in der Paketquellenliste Quellen kombiniert werden, die nicht zusammenpassen)

kann der "Holzhammer" nötig sein, um ein Paket dennoch zu installieren: `dpkg -i --force-all Paketname.deb`

Dies sollte aber nur der letzte Lösungsansatz sein.

Wurde das Paket bereits mit APT heruntergeladen, so befindet es sich im Verzeichnis `/var/cache/apt/archives/`.

6.3 debconf

Einige Pakete bringen Konfigurationsdialoge mit. Die dort eingegebenen Daten werden in der `debconf`³ abgelegt und dann von einem Skript im jeweiligen Paket verarbeitet. Möchte man die Konfiguration eines Paketes nachträglich ändern, so geschieht dies über den Befehl `dpkg-reconfigure <Paketname>`.

Die `debconf` kann mittels `debconf-get-selections` (aus dem Paket "`debconf-utils`") ausgegeben bzw. in eine Datei umgeleitet (z.B. `debconf-get-selections > debconf.bak`) werden. Einzelne Werte oder auch die komplette `debconf`

können mit `debconf-set-selections <Debconf-Datei>` wiederhergestellt werden, wobei sich die Datei an dieselbe Syntax wie die Ausgabe von "`debconf-get-selections`" halten muß.

³http://de.wikipedia.org/wiki/Debconf_%28Software%29

6.4 Installation automatisieren

Betreut man eine Reihe von Rechnern oder Webservern, wird es lästig, da (Sicherheits-)Aktualisierungen regelmäßig eingespielt werden wollen. Für diese Zwecke gibt es Spezialisten wie z.B. das Softwareverteilungssystem m23⁴, die dem (genervten, nachlässigen, ...) Administrator die Arbeit erleichtern.

Möchte man die Systeme aber nur automatisch aktualisieren, reicht auch das Paket "*cron-apt*". Nach der Installation muß es aber noch konfiguriert werden, da es ansonsten nur neue Pakete herunterlädt, aber nicht installiert. Im Verzeichnis `/etc/cron-apt/action.d` legt man dazu die Dateien mit dem folgenden Inhalt ab bzw. ändert deren Inhalt:

- 0-update

```
1 update -o quiet=2
```

- 3-download

```
1 autoclean -y
2 upgrade -d -y -o APT::Get::Show-Upgraded=true
```

- 5-upgrade

```
1 upgrade -y
```

- 9-notify

```
1 -q -q --no-act upgrade
```

Nun läuft cron-apt einmal täglich (bei Debian z.B. jeden Morgen um 4 Uhr), was aber auch in der Datei `/etc/cron.d/cron-apt` anders eingestellt werden kann.

In der Datei `/etc/cron-apt/config` stellt man bei den Parametern `MAILTO="<Mail>"` die eMail-Adresse desjenigen ein, der Informationen über den Abschluß der cron-apt-Aktionen zugeschickt bekommen soll und bei `MAILON="<Typ>"` die Art der Benachrichtigung. Hierbei kann "*<Typ>*" "*always*" sein, wenn man über jede Aktion informiert werden möchte oder "*upgrade*", um nur dann informiert zu werden, wenn Pakete aktualisiert wurden. Damit die Benachrichtigung funktioniert, muß allerdings ein funktionsfähiger Mailserver auf dem System vorhanden sein.

⁴<http://m23.sf.net>

Kapitel 7

Pakete bauen

Nur vorgefertigte Pakete zu benutzen wäre doch langweilig, oder? Also die Systemwerkzeuge angeschmissen und flugs ein Paket gebastelt.



7.1 Pakete aus Debian-Quellen

Am einfachsten bekommt man den Quelltext eines Debian-Paketes, indem man `apt-get source <Paketname>` in einem neuen Verzeichnis ausführt. APT lädt daraufhin den Quelltext herunter und entpackt ihn auch gleich. Damit dies funktioniert, müssen in der Paketquellenliste (siehe Seite 25) aber nicht nur die Binärquellen, sondern auch die Quelltextquellen eingetragen sein. Ein Aufruf von

`apt-get build-dep <Paketname>` versorgt das System zudem mit allen Entwicklerpaketen, die benötigt werden, um das Paket zu bauen. Nachdem alles an Ort und

Stelle ist, wechselt man in das Quell-Verzeichnis des Paketes `cd <Quellverzeichnis>` und startet den

Kompilierungs- und Paketierungsvorgang mit `dpkg-buildpackage -us -uc`. Nach einiger Zeit sollten sich die Debian-Pakete (Endung `.deb`) im Verzeichnis darüber befinden und installieren lassen.

Doch wozu das Ganze? Manchmal kann es nützlich sein, ein Paket selbst zu erstellen, nachdem man einen Patch auf den Quelltext angewandt oder anderweitige Veränderungen vorgenommen hat.

7.2 Pakete aus Quelltexten

Häufiger dürfte der Fall sein, daß es die gewünschte Software nicht oder nur in einer älteren Version in der Paketquelle der Distribution gibt. Das Vorgehen läuft häufig (ggf. mit kleinen Abwandlungen) wie folgt ab:

- Quelltext herunterladen und in einem neuen Verzeichnis entpacken.
- In das Quelltextverzeichnis wechseln.

• `./configure --prefix=/usr`

• `make`

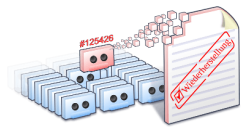
- Nachdem die Software erfolgreich kompiliert wurde, kann diese nun mit `checkinstall -D` in ein Debian-Paket verwandelt werden.

Die Installation der deb-Datei und das Entfernen erfolgt wie im Kapitel "Paketverwaltung" (siehe Seite 25) beschrieben.

Kapitel 8

Sichern

Bevor man anfängt, potentiell oder wirklich gefährliche Dinge zu tun, sollte man an die Sicherung von wichtigen bzw. allen Daten denken und natürlich auch durchführen. Denn einmal verlorengegangene Daten lassen sich nun einmal nicht oder nur mit viel Mühe und Glück wiederbeschaffen. Eine Sicherung mag zwar lästig erscheinen, ist aber im Gegensatz zum Verlust ein nur geringes Übel.



8.1 Sicherung von Dateien/Verzeichnissen

Dateien und Verzeichnisse lassen sich ganz einfach sichern.

Möchte man z.B. eine neue Konfiguration ausprobieren, sollte man vor dem Editieren der entsprechenden Konfigurationsdatei eine Sicherungskopie anlegen z.B. mit `cp <Konfdatei> <Konfdatei.bak>` .

Sollen mehrere Dateien oder Verzeichnisse mitsamt den Unterverzeichnissen gesichert werden, so bietet sich die Erstellung eines komprimierten tar-Archives mittels

```
tar cfvj <Sicherungsarchiv.tar.bz2> <Dateien und Verzeichnisse>
```

an. Der Aufruf für die Sicherung der kompletten Apache-Konfiguration könnte z.B. so aussehen:

```
tar cfvj /sicherungen/Apache-Konfig.tar.bz2 /etc/apache2
```

Natürlich ist es auch möglich, Dateien und Verzeichnisse in ein neues Verzeichnis zu kopieren. Dies geschieht (inklusive Anlegen des Backupverzeichnisses) mit

```
mkdir -p <Backupverzeichnis>; cp -r <Dateien und Verzeichnisse> <Backupverzeichnis>
```

8.2 Wiederherstellung von Dateien/Verzeichnissen

Die zur Wiederherstellung einer Datei kann die Backupdatei mittels `mv <Konfdatei.bak> <Konfdatei>` in die Ursprungsdatei umbenannt werden.

Wurde eine Sicherung mittels `tar` durchgeführt, so geschieht die Wiederherstellung mittels

```
tar xfvj <Sicherungsarchiv.tar.bz2>
```

. Enthält die tar-Datei absolute Pfadangaben (siehe Seite 10), so muß man vor Ausführung des Befehls in das "/"-Verzeichnis wechseln, ansonsten in das Verzeichnis, in dem der tar-Sicherungsbefehl ausgeführt werden.

Hinweis

Möchte man nur Teile des tar-Backups wiederherstellen, so entpackt man dies in einem neuen Verzeichnis unter /tmp und kopiert die gewünschten Dateien wieder an ihren Ursprungsort.

Der Einfachheit halber sollte man Sicherungen, die mit `cp` in ein Backupverzeichnis gesichert wurden, mit dem

Midnight Commander via `mc <Backupverzeichnis> <Konfigurationsverzeichnis>` zurückkopieren. Hierbei hat man auch gleich die Kontrolle über die zu überschreibenden Dateien.

8.3 Sichern von Partitionen und ganzen Festplatten

Sollte man etwas wirklich Gefährliches wie z.B. das Verschieben von Partitionen vorhaben, bietet es sich an, die betreffende Festplatte vorher komplett zu sichern. Auch kann es vor umfangreichen Updates nicht schaden, ein Backup der Systempartition zu erstellen.

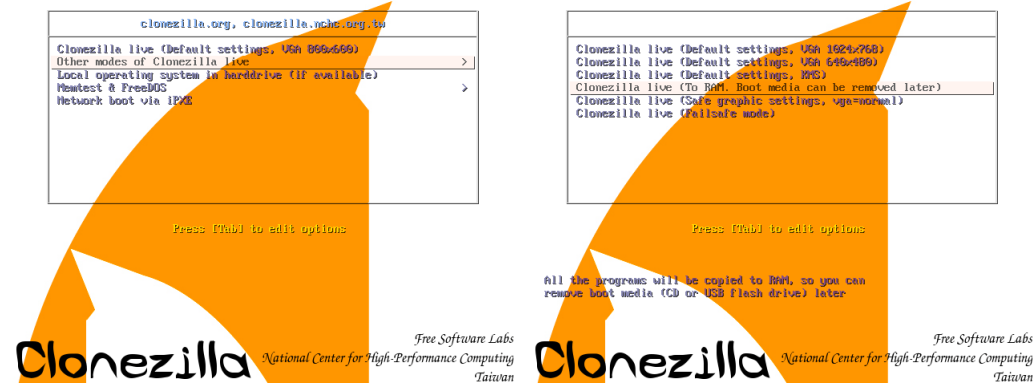
Bei dieser Aufgabe hilft das Live-Linux Clonezilla ¹, das sowohl von einer CD/DVD als auch mittels USB-Stick (der mit UNetbootin ² geschrieben wurde) gebootet werden kann.

8.3.1 Kleiner Leitfaden

Das Clonezilla-Live-Linux mag am Anfang etwas verwirrend sein. Daher folgt hier ein kleiner Leitfaden für die Sicherung einer Partition als komprimierte Archive auf eine andere Partition zum Kennenlernen der grundlegenden Arbeitsweise mit Clonezilla. Diese andere Partition kann sich auf einer internen oder externen Festplatte oder einem USB-Stick befinden.

Hinweis
Es ist auch möglich, die Archivdateien auf einem Netzwerklaufwerk (Samba, SSH, NFS) abzulegen. Unter Clonezilla gibt es allerdings auch die Möglichkeit, 1:1-Kopien von einer Festplatte bzw. Partitionen auf eine andere (USB-)Festplatte zu klonen. Daher mag auch der Name kommen...

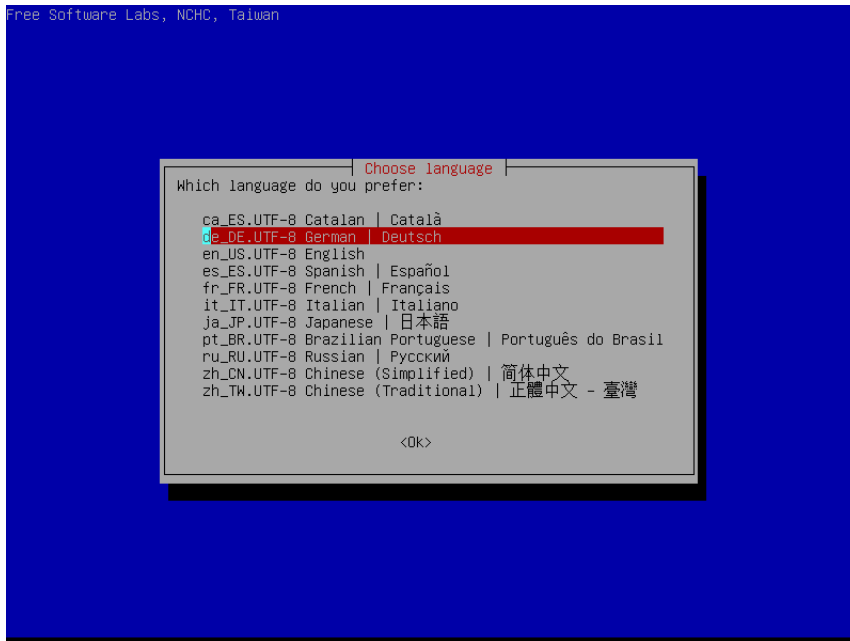
Bootmodus



Als erstes erscheint ein Auswahlménü, bei dem man **Other modes of Clonezilla live** und dann im folgenden Bildschirm **Clonezilla live (To RAM. Boot media can be removed later)** auswählt. Diese Betriebsart hat die Vorteil, daß man sein Ruhe vor einer ansonsten deutlich mehr lärmenden CD/DVD hat und den Boot-USB-Stick abziehen kann, womit man eine weitere freie USB-Buchse bekommt.

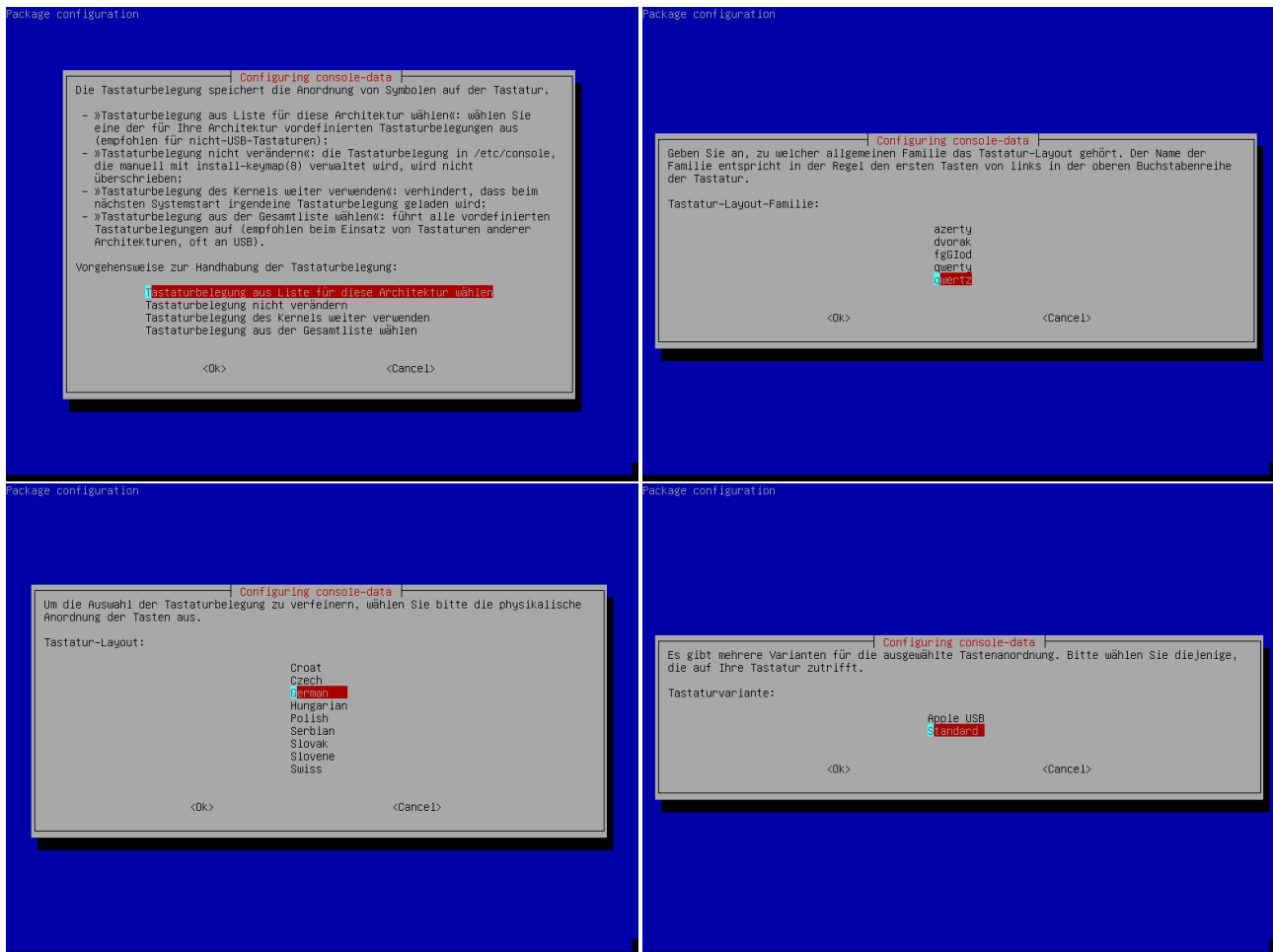
¹<http://clonezilla.org/>
²<http://unetbootin.sourceforge.net/>

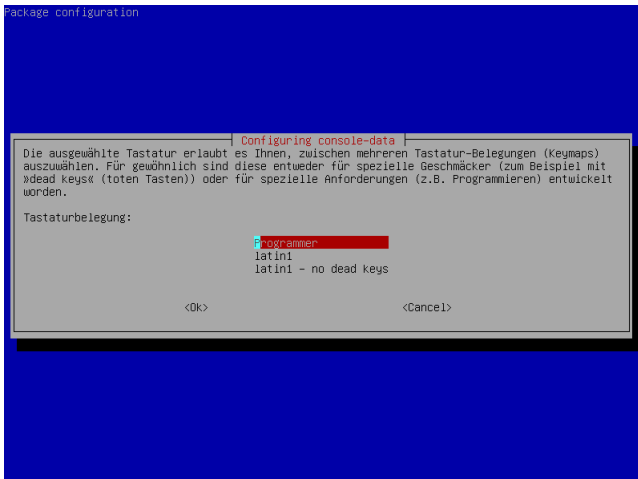
Sprache



Nach dem Booten des Live-Linux erscheint ein Dialog zur Auswahl der Sprache. Falls nicht anders gewünscht, empfiehlt sich hier `de_DE.UTF-8 German | Deutsch`

Tastatur

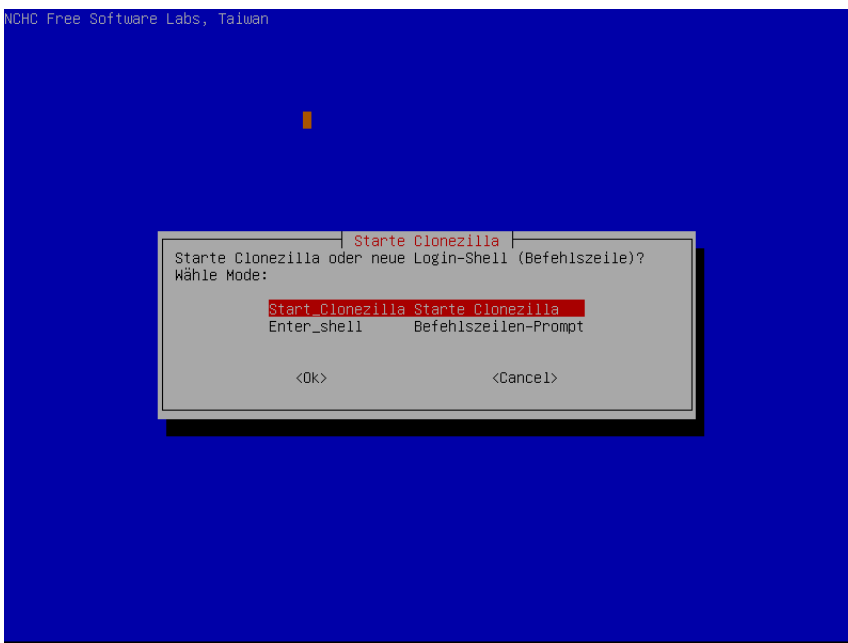




Um die Konfiguration einer deutschen Tastatur geht es gleich darauf in fünf Menüs:

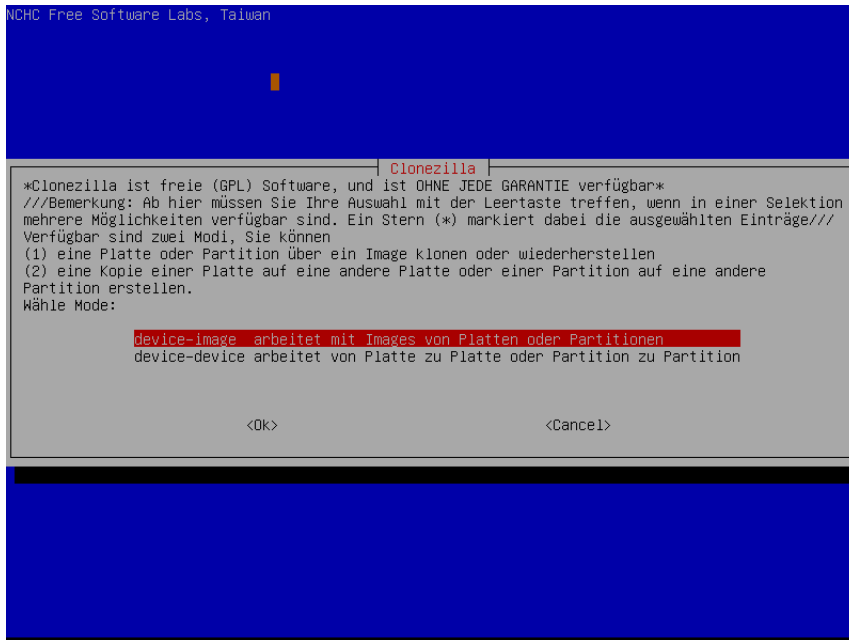
Tastaturbelegung aus Liste für diese Architektur wählen , dann , dann , dann und abschließend .

Clonezilla starten



Hierauf folgt der eigentliche Start der Clonezilla-Software durch .

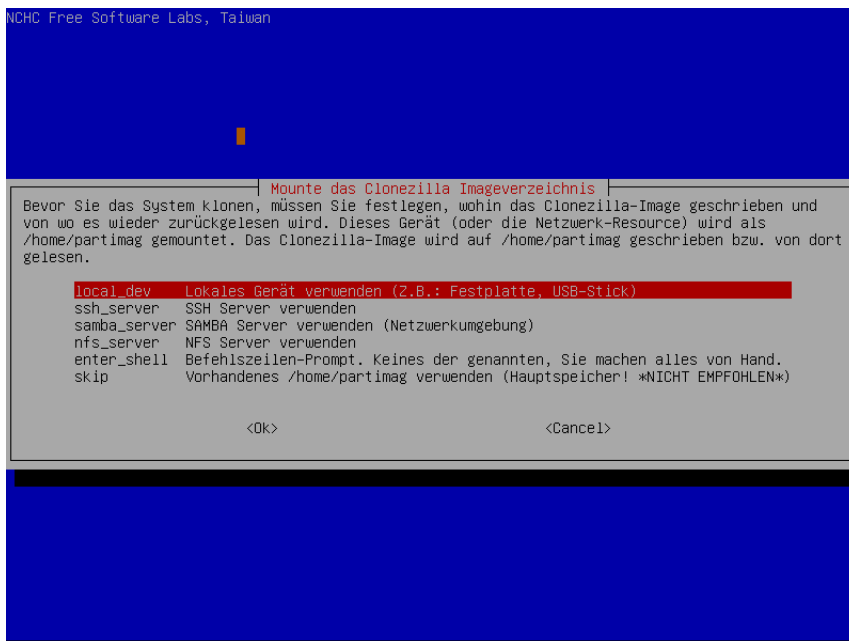
Datei- oder Klon-Modus



In den meisten Fällen wird man eine Festplatte bzw. Partitionen als (komprimierte) Dateien sichern wollen:

device-image arbeitet mit Images von Platten oder Partitionen .

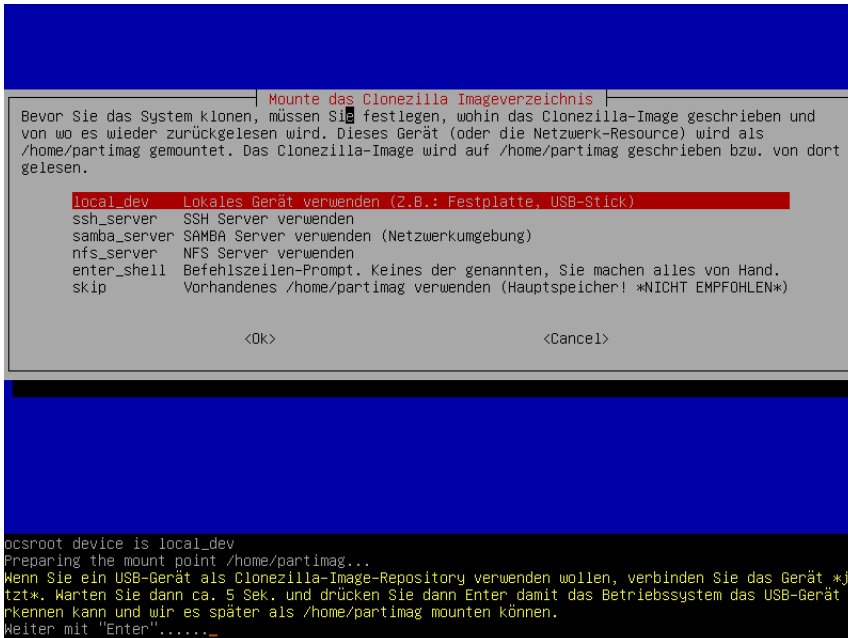
Backup-Medientyp




In diesem Dialog wird ausgewählt, auf welchen Medientyp die Archive geschrieben werden sollen. Im Beispiel:

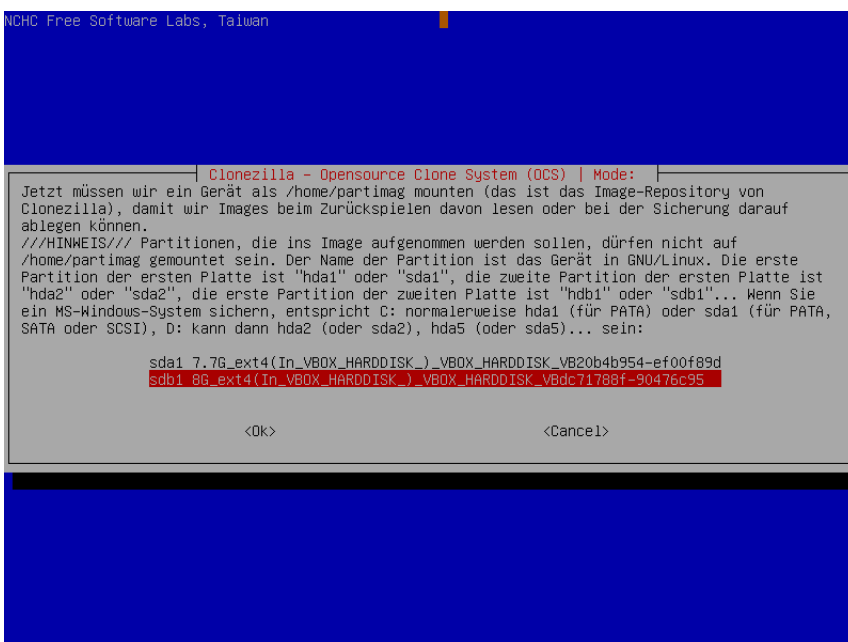
local_dev Lokales Gerät verwenden (Z.B. Festplatte, USB-Stick) .


Laufwerk spätestens jetzt anschließen



Sollte ein externes Laufwerk noch nicht an den Rechner angeschlossen sein, so ist es nun ein ausgezeichnetes Zeitpunkt, dies sofort nachzuholen. Ist das Laufwerk wirklich angeschlossen, so bestätigt man dies noch mit .

Laufwerksbestätigung




In der folgenden Liste sollte nun auch das gewünschte Laufwerk auftauchen, welches man auswählt und anschließend mit  abnickt.

Freier Speicher

```

Belegter Platz auf dem Dateisystem
*****
df: '/filesystem.squashfs': No such file or directory
Filesystem      Size  Used Avail Use% Mounted on
rootfs          188M  7,0M  181M   4% /
sysfs            0      0      0   - /sys
proc            0      0      0   - /proc
udev            10M    0     10M   0% /dev
devpts          0      0      0   - /dev/pts
tmpfs           38M   236K   38M   1% /run
/dev/shm        100M   95M   4,9M  96% /live/image
tmpfs           188M  7,0M  181M   4% /live/cow
aufs            188M  7,0M  181M   4% /
tmpfs           188M    0   188M   0% /live
tmpfs           5,0M    0   5,0M   0% /run/lock
tmpfs           76M    0   76M   0% /run/shm
fusectl         0      0      0   - /sys/fs/fuse/connections
tmpfs           188M    0   188M   0% /tmp
rpc_pipefs      0      0      0   - /var/lib/nfs/rpc_pipefs
/dev/sdb1       7,8G  1,3G  6,1G  18% /tmp/local-dev
/dev/sdb1       7,8G  1,3G  6,1G  18% /home/partimag
*****
Weiter mit "Enter".....

```

Den Überblick über den freien Speicher aller gemounteten Laufwerke schließt man mit  .

Backupverzeichnis

```

NDHC Free Software Labs, Taiwan

```


Clonezilla - Opensource Clone System (OCS)

In welches Verzeichnis soll das Clonezilla-Image gespeichert werden (nur eine Verzeichnis-Ebene wird angezeigt und das Clonezilla-Image selbst wird übersprungen. Leerzeichen im Verzeichnisnamen werden NICHT angezeigt)?:

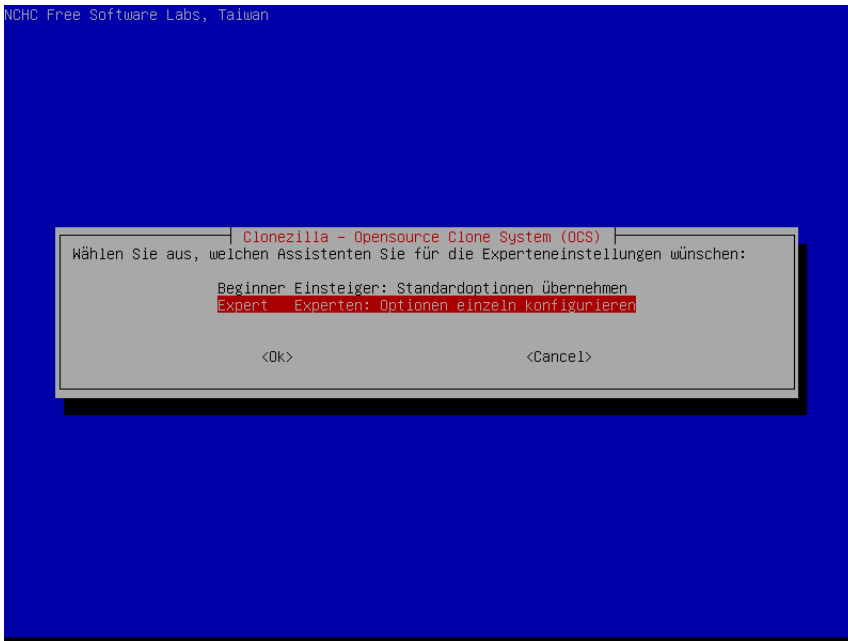
/ Oberstes_Verzeichnis_des_lokalen_Geräts

lost+found Jun_14

<Ok> <Cancel>

Sollten sich auf dem Backup-Laufwerk mehrere Verzeichnisse befinden, kann man noch das Verzeichnis für das Backup auswählen, ansonsten tut es auch  .

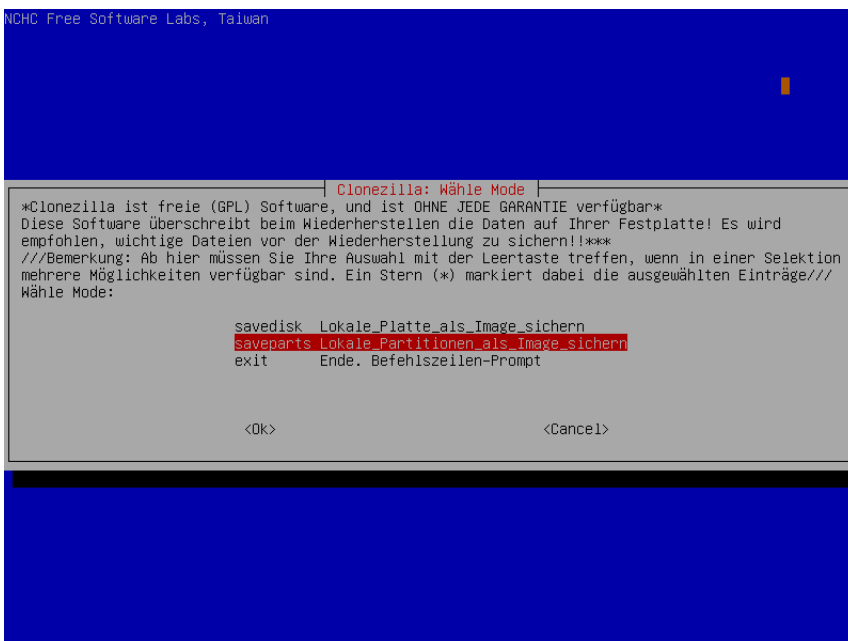
Experten-Optionen



Wenn man bis hierher gekommen ist, will man wohl auch alle Funktionen und Einstellungen und macht deshalb

```
Expert Experten: Optionen einzeln konfigurieren ↵ .
```

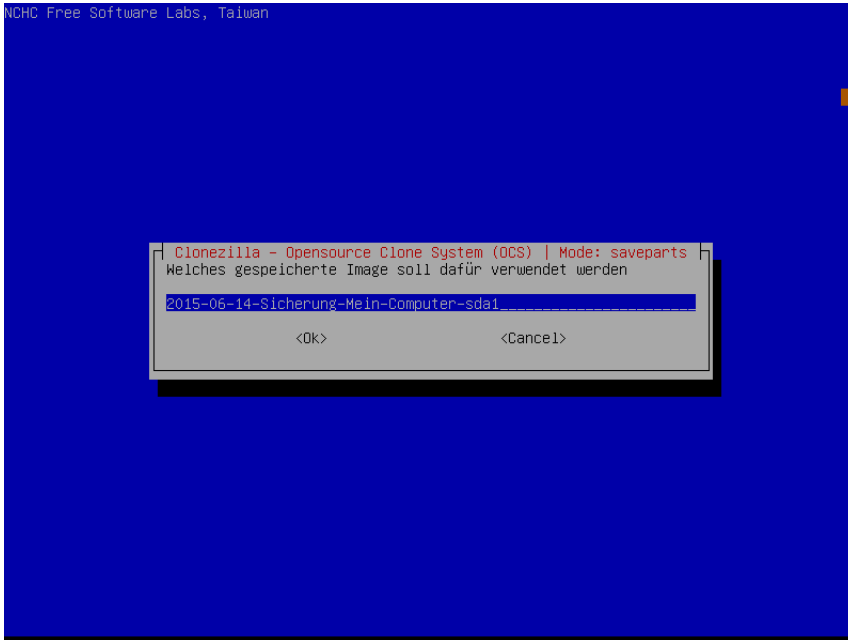
Sicherung als Dateien




In diesem Beispiel geht es um die Sicherung einer Partition, daher:

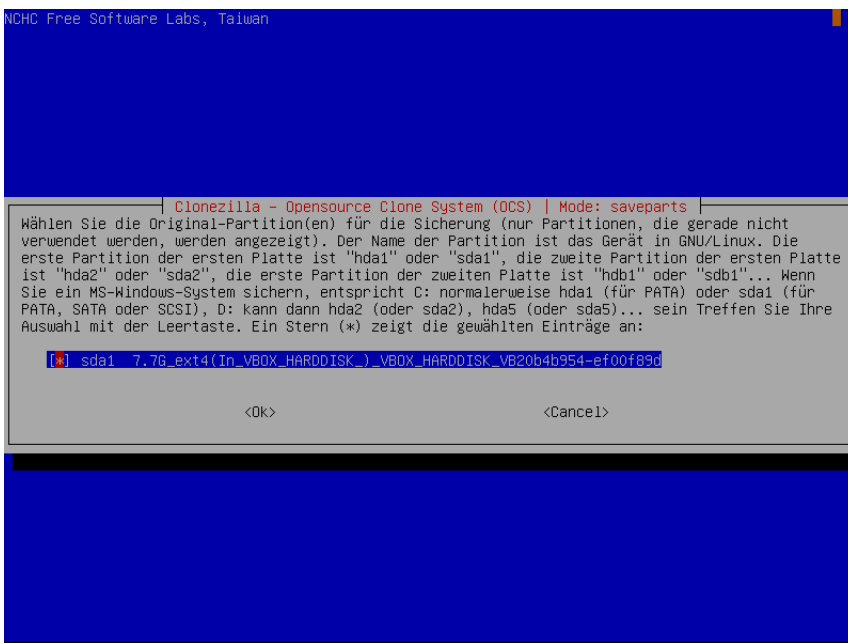
```
saveparts Lokale_Partitionen_als_Image_sichern ↵ .
```

Backupname



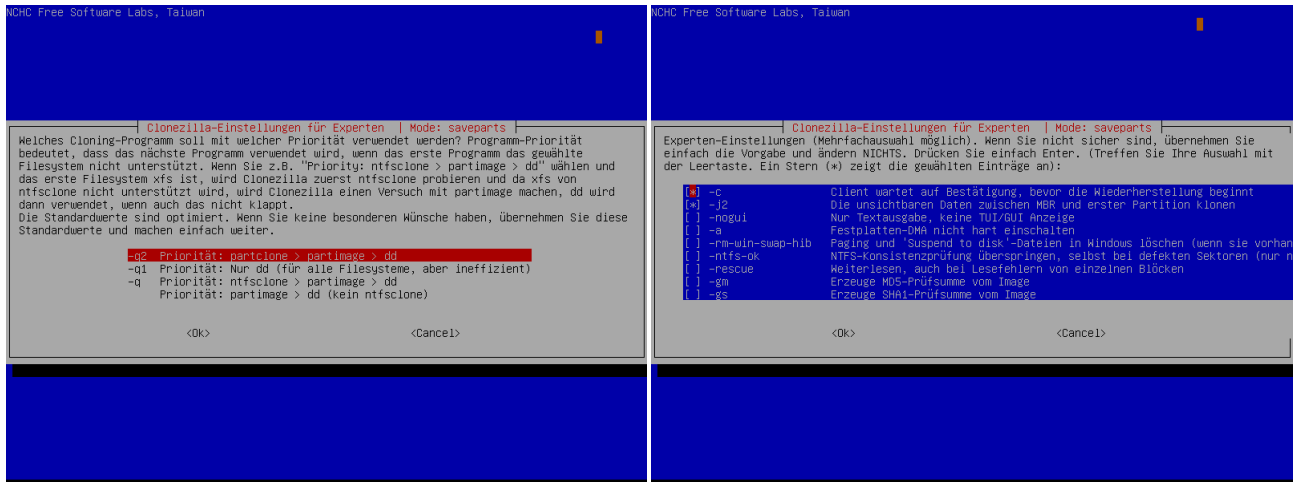
Nun gibt man einen Namen für das zu erstellende Backup an. Hierbei handelt es sich um den Namen für das Verzeichnis, in dem alle Informationen zur Wiederherstellung der Partition abgelegt werden. Der Name sollte sowohl ein Datum, als auch Hinweise darauf enthalten, was (also Betriebssystem, Rechnername, ggf. spezielle Konfiguration, Software, etc.) gesichert wurde. Anschließend:  .

Zu sichernde Partition



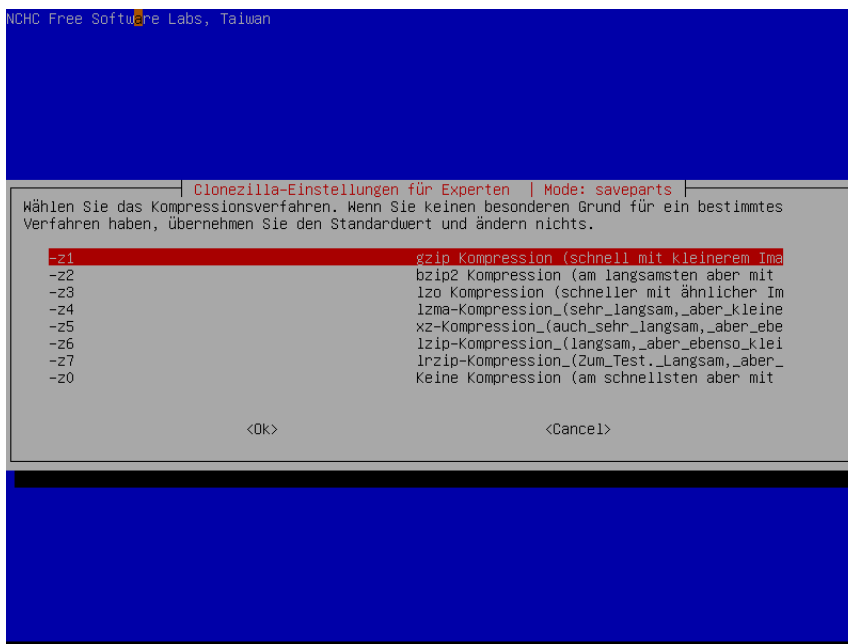
Nun wählt man noch die Partition(en) aus, die gesichert werden soll(en). Bestätigung mit  .


Weitere Optionen



Die Voreinstellungen bei den Experteneinstellungen in den beiden folgenden Dialogen "-q2" und "-c -j2" können beibehalten werden.

Kompression

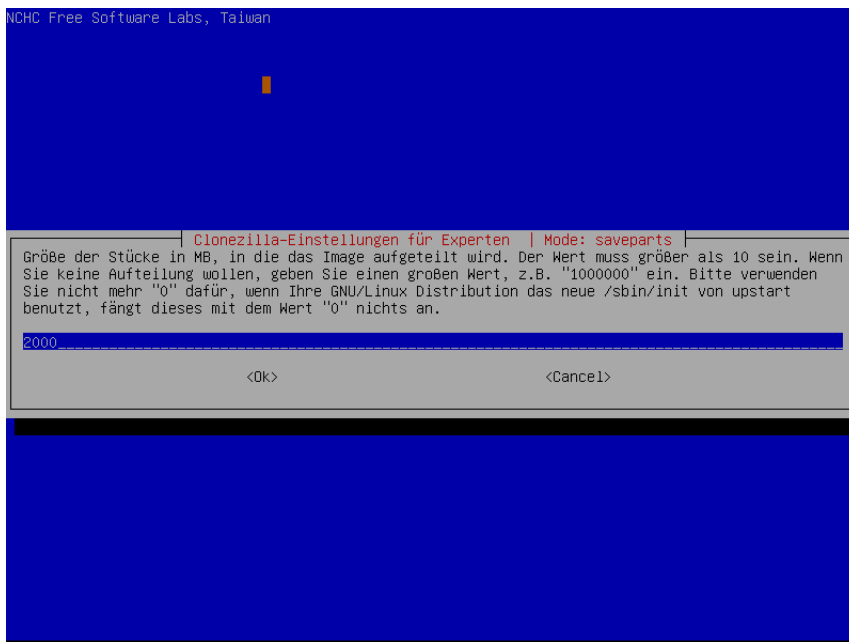


Nun ist es an der Zeit, Kompressionsmethode für die Archive festzulegen. Jeder der aufgelisteten Algorithmen sorgt dafür, daß zum Anlegen der Archivdateien weniger Speicher benötigt wird, als die Ursprungspartition groß ist. Bessere Kompression benötigt allerdings auch mehr Rechenzeit. "gzip" ist relativ schnell, produziert aber auch große Dateien. "lzma" und "xz" führen zu kleinen Dateien, benötigen aber deutlich länger. Als Kompromiß bietet sich noch "bzip2" an. Ist auf dem Backuplaufwerk viel Speicher frei und die CPU langsam, so sollte man "gzip" verwenden. Im umgekehrten Fall "xz". Nach der Auswahl:  .

Hinweis

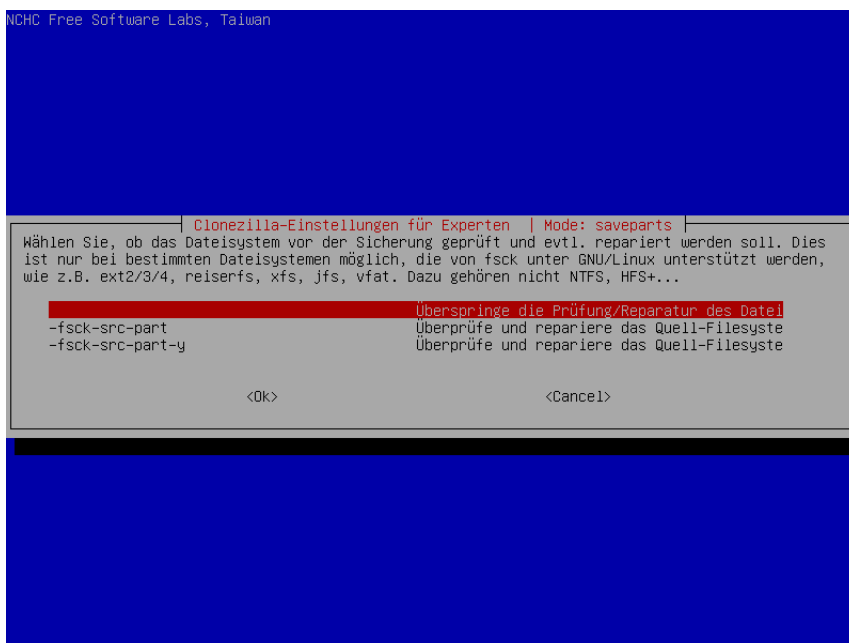
Verfügt die CPU über mehrere Kerne, so sollte man einen "parallelen" Algorithmus verwenden. Dieser verteilt die Rechenlast auf alle Kerne und führt schneller zum Ziel.

Backupdateigröße



Die Aufteilungsgröße für die Archivdateien kann beibehalten werden. Daher: ↵ .

Quellpartitionsprüfung



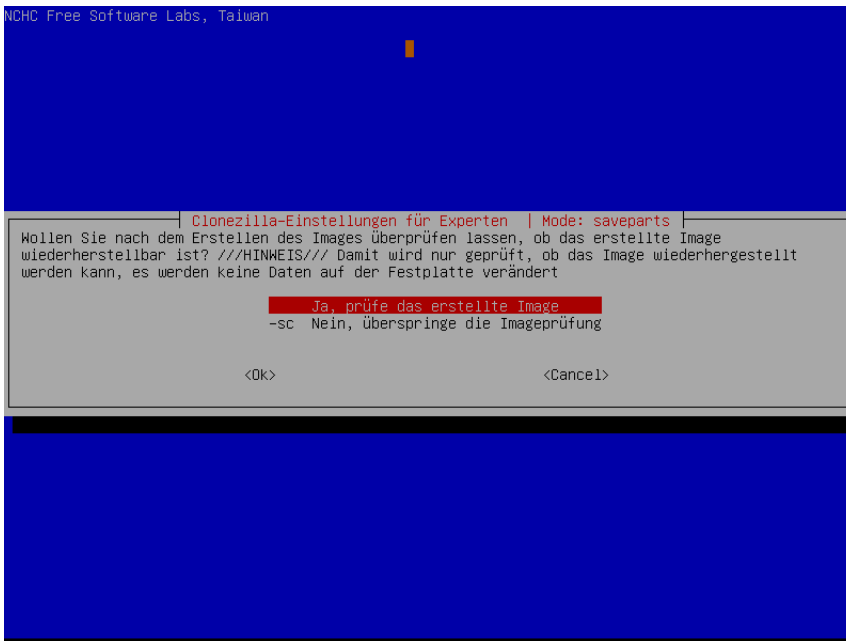
Eine Prüfung der Quellpartition ist in den meisten Fällen nicht nötig:

↵ .

Hinweis

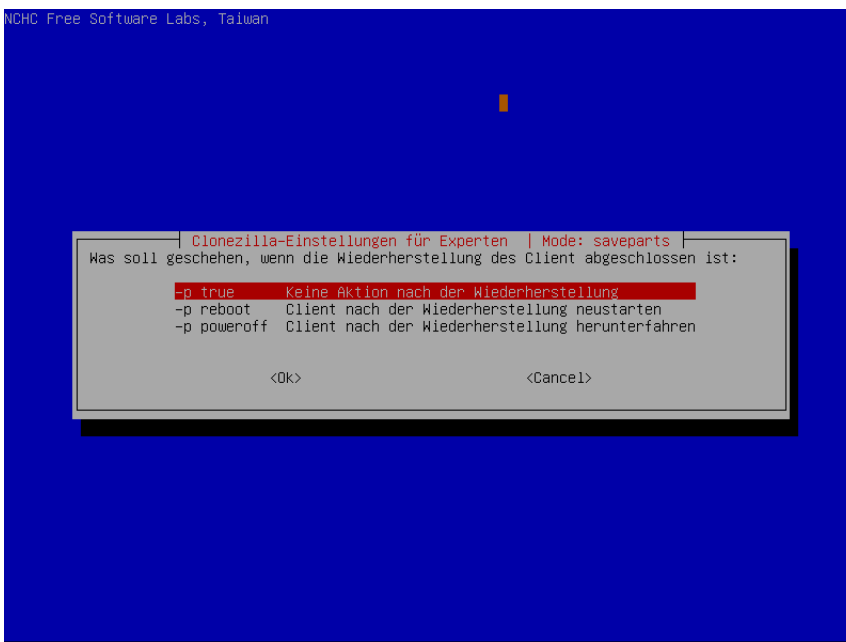
Bei Problemfällen macht Sinn, vor der Reparatur eines Dateisystems eine Sicherungskopie anzulegen. Nach der Sicherung des (kaputten) Dateisystems können Wiederherstellungsmaßnahmen durchgeführt werden, ohne die ggf. noch vorhandenen Daten weiter zu gefährden, da es von diesen ja noch ein Backup gibt.

Backupprüfung



Das erstellte Backup sollte hingegen überprüft werden: .

Nach-Backup-Optionen



Nach der Sicherung kann man den Rechner automatisch Herunterfahren oder Neustarten lassen. Auch kann man hinterher wieder zu Clonezilla zurückkehren. Im Beispiel: .

Hinweis

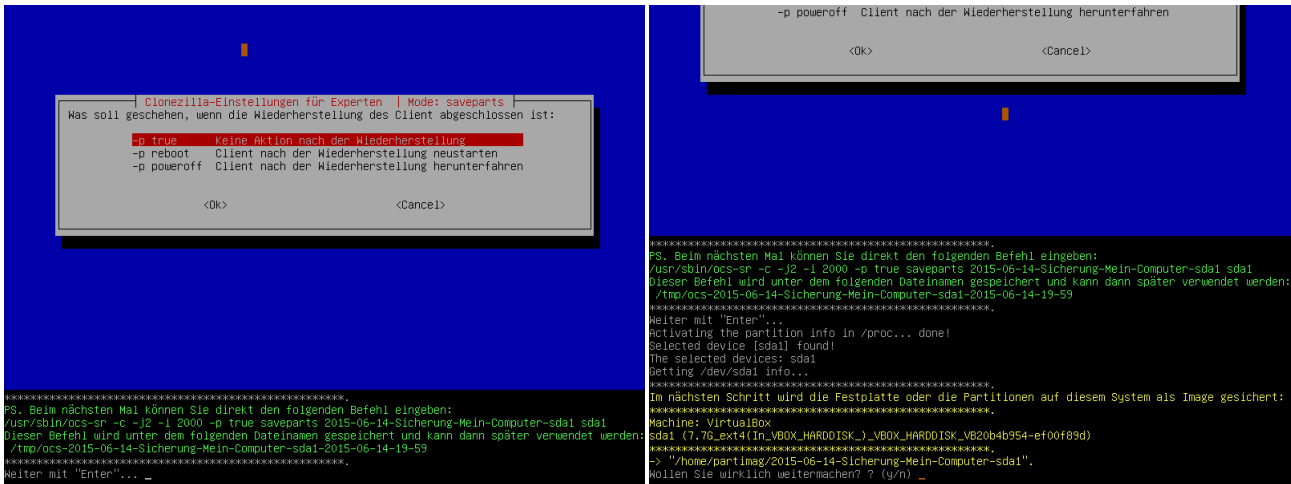
"Wiederherstellung" ist hier ein Übersetzungsfehler, da die Sicherung ja angelegt und nicht wiederhergestellt wird.

Hinweis

Für ein unbeaufsichtigtes lange laufendes Backup (z.B. über Nacht) bietet sich

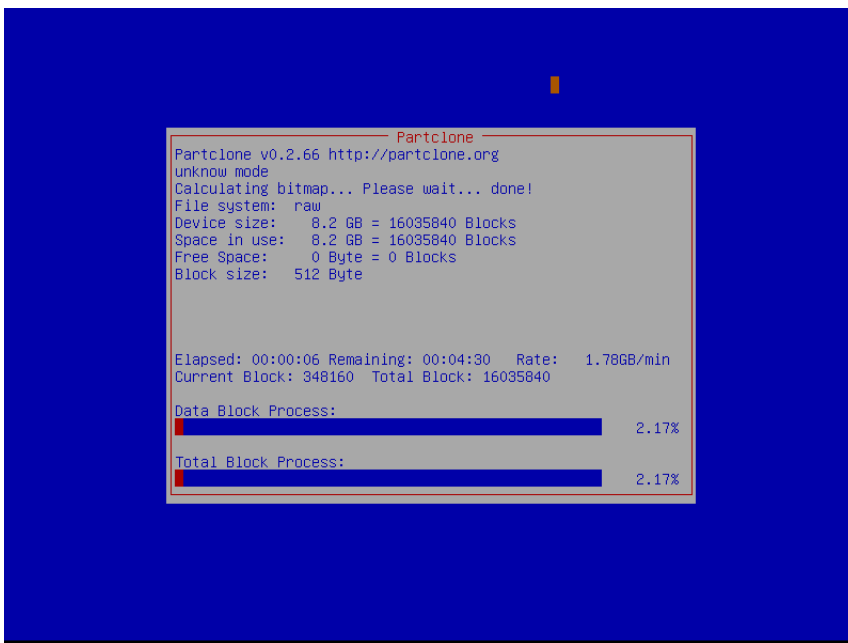
an.

Doppelte Bestätigung



Da das Erstellen eines Backups ja sehr gefährlich ist, muß dieses zweifach bestätigt werden: Zuerst mit und dann nochmals mit .

Warten aufs Ende



Nun heißt es Geduld haben und den Statusbalken anstarren bzw. etwas Sinnvolleres tun.

Statusbericht

```

This is not an image for whole disk. Skip checking swap partition info...
*****
Checking the MBR in the image "2015-06-14-Sicherung-Mein-Computer-sda1"...
MBR file found!
*****
Checking the partition sda1 in the image "2015-06-14-Sicherung-Mein-Computer-sda1"...
Image was saved by dd. No need to check the file system integrity.
*****
Alle Images von Partitionen oder logischen Volumes in diesem Image wurden überprüft und können wieder
hergestellt werden: 2015-06-14-Sicherung-Mein-Computer-sda1
Summary of image checking:
=====
Partition table file found!
This is not an image for whole disk. Skip checking swap partition info...
MBR file found!
Image was saved by dd. No need to check the file system integrity.
Alle Images von Partitionen oder logischen Volumes in diesem Image wurden überprüft und können wieder
hergestellt werden: 2015-06-14-Sicherung-Mein-Computer-sda1
=====
*****
Checking if udevd rules have to be restored...
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...

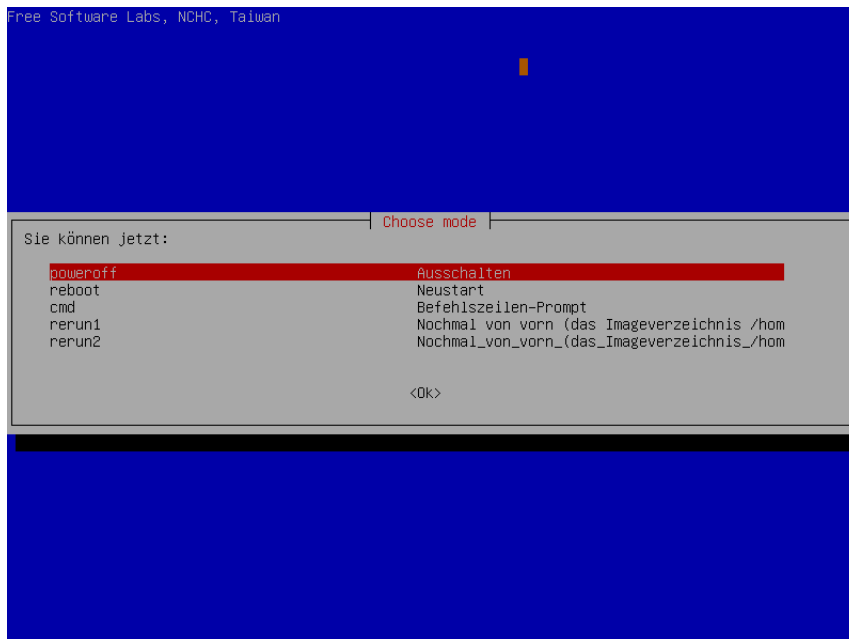
Ending /usr/sbin/ocs-sr at 2015-06-14 20:10:53 UTC...
*****
Wenn Sie Clonezilla erneut verwenden wollen:
(1) Öffnen Sie einen Befehlszeilen-Prompt auf dieser Konsole (Console 1)
(2) Geben Sie "exit" oder "logout" ein
*****
Wenn alles erledigt ist, müssen Sie 'poweroff' oder 'reboot' eingeben oder Poweroff/Reboot übers Men
ü durchführen. Andernfalls könnte ein beschreibbares Gerät (wie ein USB-Stick), das gemountet ist, d
urch die fehlerhafte Behandlung beim nächsten Mal NICHT mehr BOOTBAR sein!
*****
Weiter mit "Enter"...

```

Nach Beendigung der Sicherung und Überprüfung des Backups schließt man den Übersichtsbildschirm mit



Was nun?



Ganz zum Schluß gibt es wieder die Möglichkeit, den Rechner herunterzufahren oder neuzustarten, einen Kommandozeile zu öffnen oder Clonezilla wieder von vorn zu beginnen.


8.4 Wiederherstellen von ganzen Festplatten oder Partitionen

Die Wiederherstellung mit Clonezilla geschieht analog, bis auf ein paar weniger Optionen und daß auf der Zielpartition bzw. dem Ziellaufwerk alle Daten überschrieben werden.

8.5 Sicherungen in VirtualBox

Unter VirtualBox kann der aktuelle Zustand der ganzen VM inklusive Festplatte, laufender Programme, etc. gesichert werden.

Dazu wählt im Fenster der VM  aus und gibt eine Namen für den Sicherungspunkt an und klick abschließend auf "OK".

Um zu diesem Sicherungspunkt zurückzukehren wählt man . Im kommenden Dialog noch "die virtuelle Maschine ausschalten" wählen und "Zurückkehren auf Sicherungspunkt '<zuvor vergebener Name>'" an-haken.

Beim nächsten Start der VM ist diese dann wieder an der Stelle des Sicherungspunktes.

Kapitel 9

Notfallkoffer

Jeder Administrator sollte – für den Fall eines Falles – einen "Notfallkoffer" bereithalten. Doch was sollte darin sein?



- Eine halbwegs aktuelle Knoppix-CD(-RW) ¹, sowie ein Knoppix, das mittels UNetbootin ² auf einen USB-Stick geschrieben wurde – denn es soll ja bekanntlich auch Rechner ohne optische Laufwerke geben...
- Genauso sollte auch eine Clonezilla ³-CD, sowie ein USB-Stick nicht fehlen, um Festplatten und Partitionen zu kopieren, sichern und wiederherzustellen.
- Zum Partitionieren und Formatieren eignet sich GParted Live ⁴, welches als CD- und USB-Abbild verfügbar ist.
- Je nach Geschmack gibt es noch eine Reihe weiterer Live-Linuxe mit verschiedenen Schwerpunkten wie z.B. Finnix ⁵ oder Grml ⁶.

9.1 Ausfälle anderer Art

Ein Administrator sollte sich außerdem darüber Gedanken machen, ob – falls ihm etwas zustößt oder er aus anderen Gründen verhindert ist – es anderen Personen möglich ist, seine Aufgaben zu übernehmen. Für diesen Fall sollte er – je nach Wichtigkeit der administrierten Rechner – einen Notfall-Umschlag mit Paßwörtern oder eine verschlüsselte Datei an einem sicheren Ort deponieren, der den möglichen Vertretern jedoch bekannt sein sollte. Bei einigen Accounts sind hierbei natürlich die AGB des jeweiligen Anbieters zu beachten, die eine Paßwortweitergabe untersagen. Ein Ausweg kann hier das Anlegen zusätzlicher Administrator-Accounts sein.

¹<http://www.knoppix.org/>

²<http://unetbootin.sourceforge.net/>

³<http://clonezilla.org/>

⁴<http://gparted.sourceforge.net>

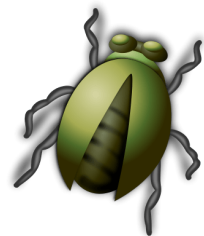
⁵<http://www.finnix.org>

⁶<https://grml.org>

Kapitel 10

Fehler identifizieren (und lösen)

Fehler sind lästig, aber letztendlich bei komplexen Systemen leider nicht zu vermeiden. Bei den meisten Fehlern ist man zum Glück nicht auf sich allein gestellt und das Internet und die Suchmaschine des Vertrauens (bzw. des geringsten Mißtrauens) bietet für fast jeden Fehler eine passende Lösung. Um diese zu finden sind gute Suchbegriffe nötig. Neben der Fehlersuche und Testreihen geht es in diesem Kapitel um die Gewinnung von möglichst guten Suchbegriffen.



10.1 Suchmaschinen füttern

Als Faustregel gilt, daß die Suchmaschine mit exakten Fehlermeldungen (ggf. bereinigt von persönlichen Informationen wie Rechner- oder Benutzername, etc.) gefüttert werden sollte. Zu der Fehlermeldung selbst sollte der Name des fehlerproduzierenden Programmes hinzugenommen werden. Sollten die Suchergebnisse zu umfangreich oder unpassend ausfallen, so ist es sinnvoll, die Suchanfrage um den Namen der Distribution (Debian, Ubuntu, ...) und ggf. den Releasenamen (z.B. Wheezy, Quantal, ...) oder ganz allgemein um "Linux" zu erweitern.

10.2 "Programmgesprächigkeit" erhöhen

Viele (Kommandozeilen-)Programme bieten die Möglichkeit, diese "gesprächiger" zu machen und so weitergehende Informationen über den Programmablauf (inklusive genauerer Fehlermeldungen) zu gewinnen. Bei vielen Programmen verbirgt sich diese Funktionalität hinter einer "verbose"-Option, die oft mit `-v` oder `-V` aktiviert wird. Alternativ kann diese auch unter den Begriff "debug" oder "log" fallen. Der genaue Name der Option und weiterer Parameter stehen entweder in der Manpage oder können über die eingebaute Hilfefunktion (siehe Seite 14) des Programmes abgerufen werden.

10.3 Systemfehler finden

Eine wichtige Anlaufstelle für Systemfehler sind die Ausgabe von `dmesg` und die Dateien unter `/var/log` und in den (ggf. existierenden) Unterverzeichnissen. Hier befinden sich Logdateien diverser Programme. Bei dieser Vielzahl an Logdateien kann aber schon mal die Übersicht verlorengehen. Hier hilft der Einzeiler

```
ls -lt /var/log/ | head
```

, der die Dateien nach der Änderungszeit sortiert, wobei die neuesten ganz oben stehen. Dies sollte man möglichst schnell nach dem Auftreten eines Fehlers machen, da ansonsten andere Programme neuere Logdateien schreiben könnten und somit die interessante Datei aus der Auflistung "herauswandert". Schließlich beschränkt `head` die Ausgabe auf 10 Zeilen.

Die so gefundene Datei sollte nun ausgiebig mit `less` oder `nano` begutachtet werden, um Fehlermeldungen und andere Hinweise auf das Problem zu finden.

10.4 Was läuft?

Auf einem Linuxrechner läuft eine Vielzahl von Programmen gleichzeitig. Welche diese sind, verrät `ps -A`. Sollte sich ein (eigentlich) laufendes Programm nicht darunter befinden, so sollte man diesem seine besondere Aufmerksamkeit schenken.

Möchte man ein Programm (bzw. Prozeß) beenden, so geschieht dies durch `kill <Prozeßnummer>` bzw.

`killall <Prozeßname>`. Sollte sich der Prozeß nicht zum Beenden bewegen lassen, so hilft der zusätzliche

Parameter `-9`. Also: `kill -9 <Prozeßnummer>` bzw. `killall -9 <Prozeßname>`

Etwas komfortabler geht es über `top` oder sogar in Farbe mittels `htop`.

10.5 Wer sendet?

Genauso interessant wie die Frage nach den laufenden Programmen kann die Frage danach sein, wer wohin sendet bzw. wer auf welchen Ports lauscht. Die Frage beantwortet `netstat -a`

Ein anderes nützliches Programm hierzu ist `iftop`, welches die Bandbreitenauslastung pro Netzwerkkarte und verbundenem Server anzeigt.

Noch genauer geht es mit `wireshark`. Dies erlaubt es, alle Pakete, die über eine Netzwerkschnittstelle übertragen werden, aufzuzeichnen und zu analysieren.

10.6 Programme belauschen

NSA läßt grüßen: Das Programm `strace` belauscht andere Programme und erstellt ein detailliertes Protokoll. Da `strace` eine Menge Informationen sammelt, sollten diese von der Fehlerausgabe direkt in eine Datei umgeleitet werden. Ein Aufruf könnte folgendermaßen aussehen:

```
strace -f -o /tmp/nsa.log <zu belauschendes Programm zzgl. Parameter>
```

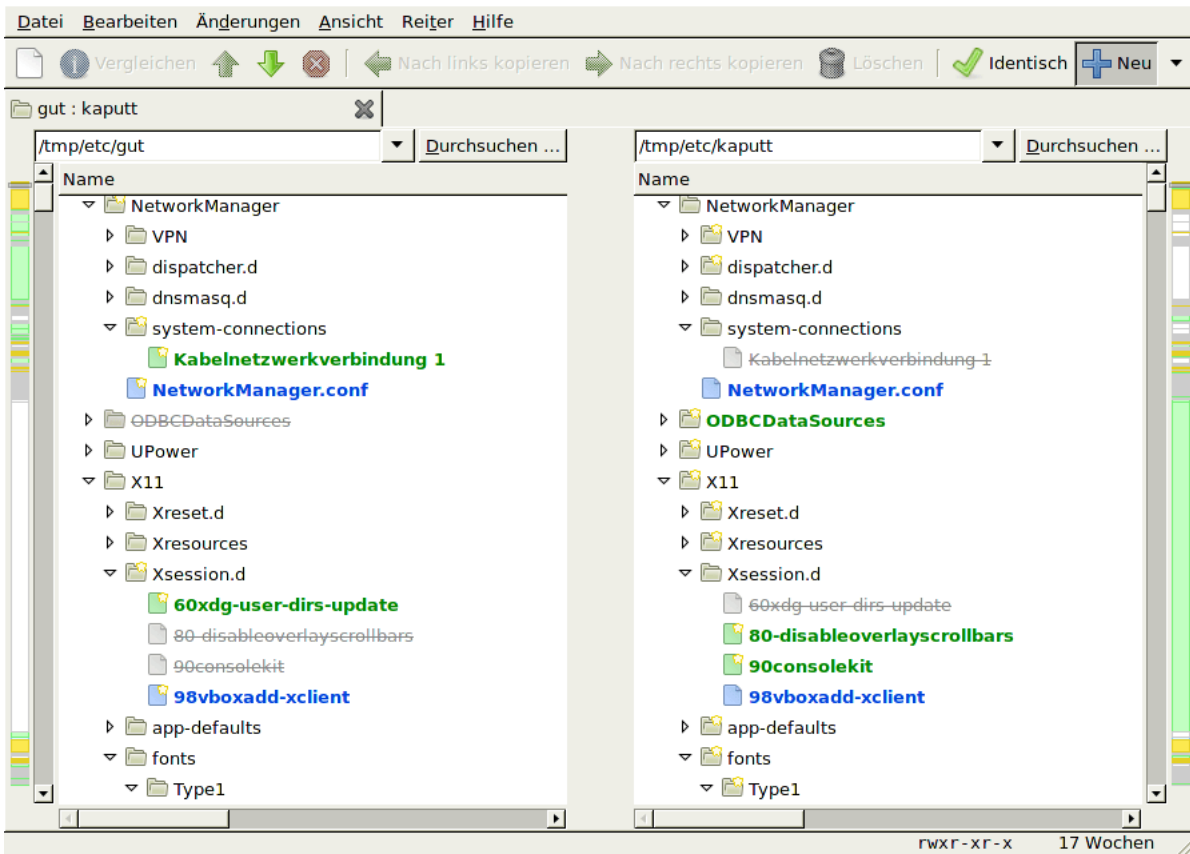
Dieser Aufruf startet das angegebene Programm und schreibt alle Informationen (`-f` : auch der Kindprozesse) in die Datei `/tmp/nsa.log`. Diese Datei sollte man nun genau begutachten. Geht es z.B. um Fehler mit nicht gefundenen Dateien, so kann man diese in der Logdatei leicht mit den Suchbegriffen `"ENOENT"` und `"open"` finden.

10.7 Unterschiede zwischen Systemen

Es kommt leider auch immer wieder vor, daß zwei eigentlich gleiche Systeme sich unterschiedlich verhalten oder eines sogar mit Fehlermeldungen um sich schmeißt und einfach nicht das tut, was es tun sollte. Kann dann keine Neuinstallation vorgenommen werden (oder steht der Ehrgeiz des Administrators dieser Lösungsmöglichkeit entgegen), so kann ein Vergleich beider Maschinen auf das dahinterliegende Problem hinweisen.

Meist liegt dann das Problem in der Konfiguration und somit im Verzeichnis `/etc`. Für die Analyse sollte man dann die beiden `/etc`-Verzeichnisse auf den eigenen Arbeitsplatzrechner kopieren (z.B. mit `rsync` oder `scp` (siehe Seite 22)) und dann mit einem Vergleichswerkzeug wie `"Meld"`¹ analysieren.

¹<http://meldmerge.org/>



Hinweis

Auf der Kommandozeile hilft `diff -r <Verzeichnis 1> <Verzeichnis 2>` .

Kapitel 11

Bootmanager und Live-Linux

Der Bootmanager (meist kommt GRUB ¹ zum Einsatz) sorgt dafür, daß ein oder auch mehrere Betriebssysteme starten können. Aus verschiedenen (eher seltenen) Gründen kann es dazu kommen, daß der Bootmanager beschädigt wird und somit kein Booten mehr möglich ist. Eine Neuinstallation des Betriebssystems ist normalerweise nicht notwendig. Mit ein bißchen "Adminmagie" läßt sich der GRUB-Bootmanager "wiederbeleben".



11.1 Live-Linux booten

In diesem Abschnitt geht es um das Booten eines Live-Linux und den Wechsel auf das System der Festplatte. Dieses Vorgehen ist nicht nur bei GRUB-Problemen nützlich, sondern auch bei anderen Fehlern, bei denen das installierte System nicht mehr gestartet werden kann.

- Live-Linux booten (z.B. Knoppix ²) und bei Knoppix direkt beim Startbildschirm `knoppix 2` (Textmodus) eingeben. Bei anderen Live-Linuxen eine root-Shell starten.
- Nun die richtige Festplatte mit der Partition des Betriebssystems ermitteln: `parted /dev/sda print` (wenn dies nicht die richtige Festplatte sein sollte: Weiter mit `sdb`, `sdc`, ...).
- Die Partition des Betriebssystems (z.B. an Größe und dem Dateisystem (`ext3`, `ext4`, ...) zu erkennen) finden. Der komplette Geräte- und Partitionsname setzt sich aus `/dev/<Festplattengerät><Partitionsnummer>` zusammen. Also z.B. `/dev/sda1`.
- Im Live-Linux ein Verzeichnis zum Einhängen anlegen: `mkdir /mnt/linux`
- Die Partition im Verzeichnis einhängen: z.B. `mount /dev/sda1 /mnt/linux`
- Das aktuelle System wechseln: `chroot /mnt/linux`
- BASH starten: `bash`
- Sicherstellen, daß das (neue) root-Dateisystem wirklich beschrieben werden kann: `mount -o remount,rw /`
- Die `sys`- und `proc`-Pseudodateisysteme einhängen: `mount /proc; mount /sys`

¹http://de.wikipedia.org/wiki/Grand_Unified_Bootloader

²<http://www.knoppix.org/>

11.2 GRUB reparieren

Dies ist wirklich GRUB-spezifisch...

- Falls `/dev` leer sein sollte oder bei GRUB-Fehlern: `cd /dev; MAKEDEV generic ↵`
- GRUB neu in Systemplatte (hier `/dev/sda`) installieren: `grub-install -f /dev/sda ↵`
- GRUB-Einstellungen aktualisieren: `update-grub ↵`

11.3 Aufräumarbeiten

Das hier sollte am Schluß einer jeden Live-Linux-Sitzung gemacht werden:

- Sicherstellen, daß die Daten auf die Festplatte geschrieben wurden: `sync ↵`
- Rechner neu starten: `reboot -f ↵`
- CD/DVD aus dem Laufwerk nehmen bzw. USB-Stick abziehen.

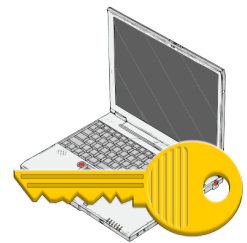
Kapitel 12

Paßwort vergessen

Es sollte natürlich nicht vorkommen (vor allem nicht beim Administrator), aber in der Praxis geschieht es angeblich öfter, daß Paßwörter vergessen werden...

Wenn es sich um die Paßwörter von lokalen Benutzern (auch "root" gehört dazu) handelt, ist es nicht schwer, ein neues Paßwort zu setzen. Das Vorgehen ist dabei – bis auf den GRUB-spezifischen Teil – wie im Kapitel "Bootmanager und Live-Linux" (siehe Seite 53).

An Stelle des GRUB-Teiles tritt ein simpler Aufruf von `passwd ↵`, wenn das root-Paßwort neu gesetzt werden soll. Hat hingegen ein Benutzer sein Paßwort vergessen, so wird dieses mit `passwd <Benutzername> ↵` geändert.



Kapitel 13

Was gibt es sonst noch? – Befehlsübersicht

In diesem Kapitel gibt es eine kleine Auswahl nützlicher Befehle. Eine genauere Beschreibung des jeweiligen Befehls, Parameter und weitere Informationen gibt

`man <Befehl>` bzw. `info <Befehl>` aus. Welches Paket den jeweiligen Befehl enthält, verrät `apt-file search bin/<Befehl>`.



13.1 Automatisch zu einer Zeit ausführen

`at` : Einmalige Ausführung eines Programmes zu einer bestimmten Zeit. Mit `atrm` kann der Auftrag wieder gelöscht und mit `atq` eine Liste der wartenden Aufträge ausgegeben werden.

`crontab` : Programm und Konfiguration für die wiederholte automatische Ausführung von Programmen zu bestimmten Zeitpunkten.

13.2 Benutzer- und Gruppen

13.2.1 Benutzerverwaltung

`adduser <Benutzername>` : Neuen Benutzer erstellen.

`adduser <Benutzername> <Gruppe>` : Benutzer zu einer Gruppe hinzufügen.

`deluser <Benutzername>` : Löscht den Benutzer.

`usermod` : Diverse Einstellungen des Benutzerkontos ändern.

13.2.2 Benutzer wechseln bzw. Kommandos unter anderem Konto ausführen

`su` : Wechselt den Benutzer.

`sudo` : Führt ein Kommando als anderer Benutzer (z.B. root) aus.

`visudo` : Verwaltet die Benutzer, die sudo benutzen dürfen.

13.2.3 Gruppenverwaltung

`addgroup <Gruppenname>` : Neue Gruppe erstellen.

`delgroup <Gruppenname>` : Löscht eine Gruppe.

13.3 Datenrettung

`ddrescue` : Liest alle noch lesbaren Sektoren eines Blockgerätes in eine Abbild-Datei.

`dvdaster` : Liest alle noch lesbaren Sektoren einer CD/DVD in eine ISO-Datei.

`photorec` : Stellt (bzw. versucht) gelöschte Dateien wieder her.

13.4 Datenträgerüberprüfung

`fsck /dev/<Gerät>` : Überprüft das Dateisystem (zusätzlich auch die Sektoren der Festplatte etc.) des angegebenen Gerätes. Durch Parameter bzw. auf Nachfrage beim Benutzer kann das Dateisystem (automatisch) repariert werden.

13.5 Formatieren

`mkfs.ext3 /dev/<Gerät>` : Legt auf dem Gerät ein ext3-Dateisystem an. Statt "ext3" gibt es viele weitere unterstützte Dateisysteme. `mkfs.` verrät die passenden Befehle.

13.6 Datensicherung

`attic` und `bup` : Deduplizierende Backupsysteme, die nur die Unterschiede von einem Backuplauf zum nächsten speichern und somit sehr effizient mit dem Backupspeicher umgehen.

`bareos` : Umfangreiches Backupsystem für die Sicherung über das Netzwerk.

`obnam` : Deduplizierendes Backupsystem mit Verschlüsselung und Uploadfunktion.

`rsync` : Dateien und Verzeichnisse über das Netzwerk kopieren.

`storeBackup` : Erstellt komprimierte Backups auf lokale Laufwerke und spart Speicherplatz durch Hardlinks.

13.7 Dateien konvertieren

`dd` : Diverse Konvertieroptionen (z.B. Änderung von Groß- und Kleinschreibung) von Dateien.

`recode utf-8.. <Datei>` : Datei von UTF-8 in lokalen Zeichensatz konvertieren.

`xxd <Datei>` : Datei als Hexcodes ausgeben.

13.8 Dateien und Dateiteile

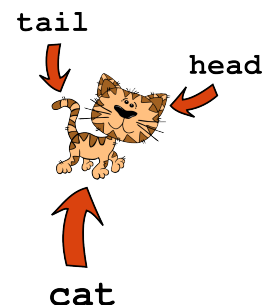
`cat <Datei>` : Datei komplett ausgeben. (Geht auch mit mehreren Dateien)

`head -5 <Datei>` : Die ersten 5 Zeilen der Datei ausgeben.

`tail -10 <Datei>` : Die letzten 10 Zeilen der Datei ausgeben.

`cut -d', ' -f2 <Datei>` : Gibt die zweite Spalte der Datei aus, bei der alle Spalten durch "," getrennt sind.

`split -b 10M <Datei>` : Datei in 10 MB große Dateien aufteilen.



13.9 Textdateien editieren

13.9.1 Zeilen sortieren / durcheinanderwürfeln

`sort <Datei>` gibt die Zeilen einer Datei sortiert aus.

`unsort <Datei>` würfelt die Zeilen in einer Datei durcheinander und gibt diese aus.

`uniq <Datei>` entfernt bei der Ausgabe der Datei bereits vorgekommene Zeilen.

13.9.2 Zeichen einfügen und entfernen

`tr` entfernt (mehrfach vorkommende) Zeichen.

`fold` bricht Zeilen nach einer bestimmten Länge oder Leerzeichen um.

13.9.3 Menschgesteuerte Editoren

In dieser Kategorie stehen Editoren, die direkt durch den Benutzer verwendet werden.

`emacs` : Sehr mächtiger, aber auch komplizierter Editor.

`mcedit` : Einfach zu bedienender Editor. Teil des Midnight Commanders.

`nano` : Ein anderer leicht zu bedienender Editor.

`vi(m)` : Mächtiger, nicht intuitiv zu bedienender Editor mit vielen Steuerkommandos.

13.9.4 Skriptgesteuerte Editoren

Hier stehen die Editoren, die automatisch komplette Texte anhand eines Skriptes bearbeiten.

`awk` : awk ist eine sehr mächtige Programmiersprache für die Bearbeitung von strukturierten Texten (z.B. CSV- oder Konfigurationsdateien).

`sed` : Der "Stream Editor" ist quasi der kleine Bruder von awk und reicht für die meisten Bearbeitungsaufgaben aus.

13.10 Dateien vergleichen

`diff <Datei 1> <Datei 2>` vergleicht üblicherweise Textdateien und listet Unterschiede auf, kann aber auch mit binären Dateien umgehen.

`cmp <Datei 1> <Datei 2>` vergleicht Dateien ausschließlich binär.

`xdelta delta <Datei 1> <Datei 2> <Diff-Datei>` erzeugt eine binäre Diff-Datei mit den Unterschieden von Datei 1 zu Datei 2 in Diff-Datei.

`xdelta patch <Datei 1> <Diff-Datei> <Datei 2>` erzeugt aus der Ursprungsdatei Datei 1 und der binären Diff-Datei die Datei 2.

13.11 Packen und entpacken

13.11.1 Packer für einzelne Dateien

Diese Packer komprimieren jeweils eine einzelne Datei zu einer komprimierten Fassung, können aber durch Parameter auch Datenströme (de)komprimieren:

`gzip` / `gunzip` , `bzip2` / `bzcat` , `xz` / `xzcat` und `lzma` .

13.11.2 Packer für mehrere Dateien

Diese Packer fassen mehrere Dateien und Verzeichnisse zu einem komprimierten Archiv zusammen:

`zip` , `tar` und `7z` .

13.12 Bilder konvertieren/bearbeiten

`convert` / `mogrify` : Bilder in andere Dateiformate umwandeln, diverse Grafikfilter wie "weichzeichnen" oder "in Graustufen umwandeln", Bilder zuschneiden und kombinieren, etc.

13.13 Drucker

Drucker können auch mit einem Webbrowser über die Adresse "http://localhost:631" verwaltet werden.

`cupsaccept` und `cupsreject` : Den CUPS-Druckserver anweisen, Druckaufträge zu akzeptieren oder diese abzulehnen.

`cupsenable` und `cupsdisable` : Aktiviert und deaktiviert Drucker bzw. Druckerklassen.

`lpadmin` Verwaltet Drucker und Druckerklassen.

`lpadmin -p <Drucker> -E -v parallel:/dev/lp1 -m <drucker.ppd> ↵` : Fügt einen neuen Drucker mit dem dem Namen <Drucker> am LPT1-Port hinzu und verwendet den PPD-Druckertreiber `drucker.ppd`.

`lpmove` Verschiebt einen Druckauftrag auf einen anderen Drucker.

`lpstat` Übersicht über die Druckaufträge.

Kapitel 14

Lizenz und weitere Informationen

14.1 Lizenz



Namensnennung-NichtKommerziell 3.0 Deutschland

Sie dürfen:

- den Inhalt vervielfältigen, verbreiten und öffentlich aufführen
- Bearbeitungen anfertigen

Zu den folgenden Bedingungen:



Namensnennung. Sie müssen den Namen des Autors/Rechtsinhabers nennen.



Keine kommerzielle Nutzung. Dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter die dieser Inhalt fällt, mitteilen.
- Jede dieser Bedingungen kann nach schriftlicher Einwilligung des Rechtsinhabers aufgehoben werden.

Die gesetzlichen Schranken des Urheberrechts bleiben hiervon unberührt. Hier ist eine Zusammenfassung des Lizenzvertrags in allgemeinverständlicher Sprache: <http://creativecommons.org/licenses/by-nc/3.0/de/legalcode>

14.2 Weitere Informationen

Weitere Informationen zu den Schulungs- und Beratungsangeboten von goos-habermann.de erhalten Sie unter <http://www.goos-habermann.de/index.php?s=SchulungBeratung>. Die Entwicklungsdienstleistungen finden Sie unter <http://www.goos-habermann.de/index.php?s=Entwicklung>.