Systeminformation

Mitschrift von Marc Landolt
Dozent: Daniel Honegger FHNW

Einleitung

1 Systemadministration

Aufgaben eines Systemadministrators:

System installieren<f
System Konfigurieren
Software installieren
Eigene Software Schreiben
Open Soruce → Paket machen
Private Anwendung für Firma → kein Paket
Sicherheitsupdates einspielen
0-day exploits auf Grund von Bugs geschrieben
Stack overflow / heap underflow
Wenn man sie bekommt sind es keine 0-day Exploits mehr
→ www.metasploit.org

Wie kann man z.B. Libraries so aufrufen dass Schadcode ausgeführt werden kann?
Windows: Je nach Service Pack alle Sprungadressen gleich
Linux: Kernelmodule werden bei jeder Distro in anderer Reihenfolge geladen
Exploits auf Linux läuft nicht auf allen Distros

Fazit: Im Windows ist man auf Virenscanner angewiesen unter Linux hat man eher noch einen Durchblick

Praxis beim Patchen
Patchdays
→ Firewall machen zu gewisser Zeit auf, damit die Server Patches, Virenscanner und andere Updates laden können…

Unterteilen des Netzes bei grösseren Netzen
High security Lohndatenbank, etc… können keine Patchs herunterladen
Medium Security nur bedingter zugriff, allenfalls Patchday
LowSecurity z.B. Abteilungsserver zum externen einloggen
Logfile machen und allenfalls mit Scripten überwachen

Neue Hardware einbauen und in Betrieb nehmen
TV karte / Gigabit Netzwerkkarten können unter Linux Probleme machen
Neuer Kernel → neues Kernelmodul (Treiber) von Hand installieren

Backup / Restore / Konsistenzprüfung
Disasterrecovery CD machen, Restore üben, Disasterrecovery durchspielen
Grössere Serverlandschaft: Textsystem! Grosser Aufwand, im Falle einer Katastrophe
hat man aber alles im Griff
Benuzer anlegen
Einloggen
Testen
VPN Testen. Häckchen gemacht?

Rechte vergeben

Mit Geschäftsleitung Service Level Agreement (SLA) **(Papier)** aushandeln, in dem alle Rechte und Verpflichtungen aufgeführt sind: für beide Parteien ein Schutz

z.B. IP's Loggen und ½ Jahr speichern

System am Laufen halten

Systemprotokolle auswerten **/var/log/messages**

Ungewöhnliche Vorkommnisse aufdecken

Hat jemand mit falscher Einstellung die DHCP log gefüllt? War es absicht?

Regelmässig reinschauen früher: HD mit logs gefüllt → kein einloggen mehr.

Virenscanner: -Schützt vor Viren und Würmern
-Verhindert das Benutzen von öffentlich zugänglichen Trojanern wie z.B. BackOrifice, Sub7 und all ihren Verwandte

Firewall: Unterbindet unerwünschte Verbindungen

IDS: überwacht das Netz zusätzlich auf Dinge wie NOP-Sleds (http://en.wikipedia.org/wiki/Buffer_overflow#Nop_sled_technique), bekannten Shellcode, und diverse andere aktivitäten womit fragwürdig bleibt in wiefern Exploit-Frameworks wie von www.metasploit.org in einer Kommerziellen Umgebung nützlich sind.

Script das auf allen Servern die Logfiles nach bestimmten Begriffen (in Datei) sucht und geben diese aus.
z.B. „Memory CRC Error"

1x im Monat kein Problem, mehrmals → Problem genauer ansehen, RAM könnte defekt sein.

Privat Rechner: Memory und andere Resourcen überwachen

Vielleicht entdeckt man etwas Falsches → korrigieren → mehr Performance

z.B. sinnlos Resourcen nutzender Indexdienst, oder Memory Leak einer Applikation

Lösen von Systemproblemen

Housekeeping

Disk nicht vollaufen lassen, alte Logs Packen, wichtig bei älteren Systemen

Allenfalls Maintainance Fenster z.B. Montag ab 2300 bis Di 04:00

z.B. zum Testen von Disaster Recovery etc

Verantwortungsgefühl gegenüber Firma und Server

Neu installieren geht nicht so einfach, da oft viel installiert ist

DB

Backup

…

Öffentliche Publikation von Infoseiten, die nicht existieren oder wo anders Abgelegt wurden → Support tagelang sinnlos belastet…

Sorgfalt

- Dokumentieren
- Sache nur machen, wenn man weiss das es funktioniert
  - Vorteil VMWare Enterprise: neue virtuelle Instanz zum testen

Kommunikation

- Mittlerer bis Grosser Betrieb
  - Global: gibt es überhaupt ein Zeitfenster zum ausprobieren?
  - → Kommunikation ist gefragt
- Leute Orientieren wenn man etwas gemacht hat → sonst Support sinnlos belastet
  - Supporter am Schluss der Böse

Dokumentation

- Wichtiger Punkt der niemand wichtig nimmt
  - 20% der Arbeitszeit müsste eingerechnet werden
- Von Änderungen (am besten Journal von jeder Maschine)
  - Wann wurde Patch von autoupdate eingespielt, meist nachträge in MSKB
  - Wie MS hat auch linux patch-days
  - Probieren nicht der richtige Weg
- Von Entscheidungen
- Nachvollziehbar (Datum, Version, Bezug)

VMWare Enterprise und Co.

In Serverfarm können Virtuelle Server im Laufenden Betrieb herum geschoben werden
Disk können nicht verschoben werden
→ Externes SAN (http://de.wikipedia.org/wiki/Storage_Area_Network)

1.1 Heutige Systeme

SystemV	Kommerziell
BSD → Debian	Universitär gewachsen

Heute: FSH (http://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard)

1.2 Konfigurationsdateien

Heutzutage wird folgendermassen Konfiguriert

BSD: **`/etc/*.cf`**
Linux: **`/etc/*.conf`**

Auch **`.rc`** ist eine Konfigurations Datei (resource)

z.B. **`ntp.conf`**
Zeitsynchronisations Konfiguratoin

rcntp start | tee –a log.out // **a**ll oder **a**ppend

1.2.1 Konfigurationsdateien eignen sich gut zum Dokumentieren

##	Linux
;	altes Unix
//	Java

1.3 script

Zeichnet alle Befehle und Ausgaben auf bis `exit` eingegeben wird

```
script scrlog.out
ls -l
exit

file scrlog.out
```

in **`scrlog.out`** sind nun Daten abgelegt nicht mehr ASCII da auch Farben und Steuerzeichen beinhaltet sind

Lässt man die datei mit more oder less anzeigen, werden die Steuerzeichen von der Shell interpretiert, wird es aber im vim angezeigt, sieht man auch die Steuerzeichen.

^M	Enter (Cariage Return) Windows immer CR und Linefeed

1.4 Prompt

Der Prompt kann Verändert werden und zwar lassen sich 3 Prompts definieren, diese werden in der PS1|2|3 Umgebungsvariabel gespeichert (env) sie überschreiben die Standardeinstellung

PS1
Für den Normalen Prompt der Shell
Ist im standardmässig in etwa folgendermassen denfiniert:

```
‹PS1=$user@$(/etc/hostname):$(pwd)\ ›
```

PS2
Für Dinge wie for

```
for i in 1 2 3 do
>
>ls
>done

PS2=>>
for i in 1 2 3 do
>>ls
>>done
```

PS3
Für Dinge wie z.B. select

```
select color in red blue white black
>do
>     echo $color is a color
>done

1) red
2) blue
3) white
4) black
#? 1
red is a color
```

Hier sehen wir sehr schön, wie zuerst der PS2 (>) gebraucht wird und danach der PS3 (#?)

Je nach Benutzer unterscheidet sich PS1|2|3 von den anderen

Root
Root@server:~#

user
user@server:~>
oder
user@server:$

2 Benutzerverwaltung

Sicherheitsmechanismen

- Schützen den Zugriff auf Systemdateien
- Schützen das System vor Modifikationen
  - z.B. Viren, Würmer
  - ungewolltem überschreiben
  - böswilliger Eingriff z.B. durch Hacker
- Schützen Benutzer vor anderen
  - Benutzer können selber entscheiden, wer welchen Zugriff auf ihre Dateien hat

FHNW bezahlt bandbreite nach Amerika, Russland, China etc… 160k /Jahr
P2P contermeasures

- Weisung: Filesharingtools, Filme werde untersucht, rechnschaft
- Packet Shaper gekauft, sehr minime Bandbreite, oder gar keine

Für Administrator sind Sicherheitsmechanismen aufgehoben

→ SELinux (vom amerkikanischen Geheimdienst NSA etwickelt zusammen mit Redhat)

- **S**ecurity **E**nhanced **Linux**
- Rollenbasiertes Rechtesystem
- Keinen „allmächtigen“ Administrator:
  - SELinux user der Rollen vergibt
  - SELinux User der DNS Zonen Konfiguriert, DNSadministrator
  - SELinux User der Webserver konfigurieren kann, Webadministrator
  - …

SELinux Relativ Komplex, aber alternative mit Attributen nicht praktikabel

- Vergibt für jede Applikation eine ID, so kann auch die Applikation ausgetauscht werden ohne dass die Rechte bekommen hat

APArmor (http://de.wikipedia.org/wiki/AppArmor)

- Applikationsbezogenes Rechtesystem
- Applikationsbezogene Rollen: so kann z.B. im firewall nur port 80 freigegeben werden, rechte auf /usr/bin/apache, falls die Datei ersetzt wird kann ich diese Rechte klauen

2.1 /etc/securetty

Legt fest von welchem Terminal aus root direkt einloggen darf

2.2 su (switch user)

`su`	wechselt zum Benutzer root
`su marc2`	wechselt zu User marc, bzw zum User root wenn nichts angegeben
`su – marc2`	wechselt zusätzlich ins Homeverzeichnis des Users marc2 (loginshell)

Benutzerwechsel wird in log Datei gespeichert:
/var/log/messages

'last' | head	anzeigen der ein- und ausgeloggten benutzer….

2.3 Crash (logs greppen)

Wenn jemand z.b. Exploits ausgeführt hat
Allenfalls auch an uptime ersichtlich

2.4 sudo (Superuser do)

Benutzer muss in **`/etc/sudoers`** sein, Vorteil, man muss nicht jedesmal das Passwort eingeben

Wheel Gruppe in sudoers

%wheel ALL=(ALL) SETENV: ALL

Oder sogar

%wheel ALL=(ALL) NOPASSWD SETENV: ALL

%users ALL=/sbin/mount /cdrom,/sbint/umount /cdrom

2.4.1 sudo für fortgeschrittene

sudong

2.5 vipw

öffnet die **/etc/passwd** Datei speziell, sprich macht eine Kopie **.passwd.edit.swp** welche editiert wird und schreibt diese dann zurück, versucht ein 2. Benutzer mit vipw die Datei zu editieren dann gibt's eine Meldung, denn wenn zwei die Datei editieren gewinnt der, der die Datei zuletzt zurück schreibt

vipw –s editiert shadows

exprot VISUAL=/usr/bin/vim → wird im vim wird geöffnent
export VISUAL=/usr/bin/emacs → wird im emacs geöffnet

Standart Editor ohne $VISUAL oder $EDITOR siehe man vipw

2.6 vigr

Pendant zu **vipw** für **/etc/group**

2.7 Gnome User Tools

Einfaches Tool zum editieren von Benutzer und Gruppen

```
gksu users-admin
```

2.8 Passwort bei anderen Applikationen

Aufpassen, allenfalls andere Applikationen wie z.B. Quota oder bestimmte FTPd's müssen auch noch geändert werden.

2.9 Konsolen tty 1-6

Loginkonsole 1 bis 6 ctrl-alt-f1 bis ctrl-alt-f6
Graphische Oberfläche ctrl-alt-f7-f10 (Grafikkarte 1-4)
native Treiber von SUSE arbeiten nicht mit dualhead ausser intel (die sind open source)

2.10 X11

2.10.1 Modeline

„1024x768“ 123 41 1024 1080 213 41234213 41243
Wenn kein Widescreen modus vorhanden dann kann man ihn selber basteln
Zahlen widerspiegeln unter anderem Auflösung h-sync v-sync, Strahl Rücklaufzeiten… etc

2.10.2 Serverlayout

Hardware

2.11 Dienste

Alle Dienste unter einem nichtpriviligierten laufen lassen seit es Hacker auf dem netz gibt…
Exploit für den Dämon schon haben sie eine Root Shell
Andernfalls brauchen sie noch ein Root exploit

2.12 PAM (Plugable Authentication Modul)

(Personal Access Module)
Schnittstelle für Applikationen auf

2.13 /var

Variable Daten

2.14 Bundestrojaner in Deutschland in Planung

Mit Systemkenntnissen ist das recht schlecht möglich → virtuelle Zugriffsumgebung für den Staat einrichten

2.14.1 Verschlüsselung in der Verschlüsselung

Plan A: → container in container
Plan B: Cryptofs zeigt container mit verschlüsselten Daten, die aber gar nicht verschlüsselt sind sondern nur irgendwelche Daten vom unverschlüsselten teil der Platte

2.15 Windows UID

Arbeitet afaik mit SID (Security Identifyer) → http://en.wikipedia.org/wiki/Security_Identifier

2.16 Homeverzeichnisse im Netz

Wenn kein Home vorhanden kann nicht eingeloggt werden!! (ausser Root)

2.17 Last

Zeigt logging logs, neustes zu oberst → **`last | head`**

2.18 useradd

fügt einen neuen Benutzer hinzu
macht eine entsprechende Gruppe

/etc/default/useradd	Default einstellungen für useradd
/etc/skel	Skelleton wird hineinkopiert

2.18.1 erstellen eines backup root accounts

useradd –home /root –g 0 –u 0 –o administrator

2.19 Editor

`view` Startet mc editor

2.20 adduser

fügt einen neuen Benutzer hinzu
macht eine entsprechende Gruppe
erstellt Homeverzeichnis und kopiert vorlagen aus /etc/skel

2.21 deluser / delgroup

pendant zu adduser
danach schauen ob es noch Dateien hat von diesem Benutzer:

2.21.1 Aufräumarbeiten

Sind noch Daten vorhanden und es wird ein neuer Benutzer mit der gleichen UID/GID eröffnet kann dieser die Daten des alten Benutzers lesen →

Daten im **`/var/mail`** entfernen
Daten im **`/var/spool`** entfernen
Crontab Dateien löschen des Users löschen

```
find / -uid <UID> -depth –exec rm –rf {} \;
```
//-depth, zuerst dateien, dann verzeichnise

```
find / -nouser -depth –exec rm –rf {} \;
```

`deluser –remove-home`	löscht home und mail spool
`deluser –backup /home`	macht username.tar.gz|bz2

2.22 userdel

`userdel –r`

2.23 usermod

`usermod –L marc2`	sperrt den Account temporär
`usermod –U marc2`	hebt die Sperre wieder auf
`usermod –g gruppe benutzer`	ändert die primäre gruppe (default gruppe)
`usermod –G abbts marc`	fügt den Benutzer marc der Gruppe abbts zu

passwd

passwd ändert das passwort des aktuellen Benutzers
passwd user ändert passwort von Benutzer (als root)

passwd –S zeigt informationen zum passwort an
PS Password Set
LK Locked Konto
NP No Psasword

passwd –d löscht passwort → Kein Passwort nicht zu empfehlen

anderes Beispiel (Debian)
passwd –m 7 –x 14 –w 2 oder
passwd --mindays 7 --maxdays 14 --warndays 2

mit [ctrl-d] kann eingabe abgebrochen werden

2.24 Windows mit Linux

Radius-ticket von LDAP kann Schnittstelle zwischen windows und unix übernehmen (smb)

2.25 /etc/passwd

Benutzer:Kennwort:UID:GID:GECOS:Homeverz:Shell

2.25.1 Benutzer

UNIX:
Benutzer: oft nur die ersten 8 Zeichen relevant
LINUX:
Benutzer: ganze länge

2.25.2 Kennwort

X bedeutet das Passwort ist im **/etc/shadows** abgelegt

2.25.3 UID

User ID mit der der Kernel arbeitet

0-99 Systemrelevante Sachen z.B Root LPD CRON
100-499 (-999) Software Pakete (z.B. mySqlDb)
Ab 500 (1000) Benutzer

2.25.4 GID

Group ID mit der der Kernel arbeitet
Ca.
0-99 Systemrelevante Sachen z.B Root LPD CRON
100-499 (-999) Software Pakete (z.B. mySqlDb)
Ab 500 (1000) Benutzer

Stuff: 50 (Debian)
Nobody: 65533
Nogroup: 65534

2.25.5 GECOS

Generel Electric Comprehensive Operating System
Richtiger Name: z.B. Marc Landolt

War für Finger
gestorben, bzw. abgestellt, man sieht ob User einen Account auf dem System hat
→ Brute force Attacke auf vorhandene User accounts

Homeverzeichnis

Profil daten
Datenfiles von Applikationen (.xyz)

2.25.6 Shell

Programm das ausgeführt wird
`/bin/bash`
`/bin/sync`

`/bin/false` angeben wenn nicht eingeloggt werden soll
Shell muss im **`/etc/shells`** liegen, hängt vom ftp Programm ab
(ftpshells)

2.26 WEITERE DIENSTE ZUM AUTHENTIFIZIEREN

NIS Datenbank (Network Information Service früher Yellow Pages)
LDAP Verzeichnisdienst (Kann an ActiveDirectory angekoppelt werden)

2.27 Plugable Authentication Modul (PAM)

Macht übersetzung für NIS LDAP

2.28 ONE TIME PASSWORD (z.B. im Internet Kaffe) PAM Modul

`ssh –l ueli 212.55.197.230`
Opt-md5

Rechner auf z.B. Natel

```
Using username "ueli".
Using keyboard-interactive authentication.
otp-md5 249 la9170 ext, Response:
Using keyboard-interactive authentication.
Password:
```

2.29 /etc/shadow

Verschlüsselungsalgorithmen

MD5 Beginnt mit: 1
1[…SALT….]$[….PW…..]

Blowfish Beginnt mit: $2uB

3DES veralted (Triple DES)
xxnnnnn…..n
x: Salt n: Passwort

Weiteres:
man 3 crypt

Aufbau

Benutzer:Kennwort:Änderungstag (UnixTimeStamp):Min:Max:Warning:First:Sperre:reserve

2.29.1 Benutzer

Muss mit Benutzer aus **`/etc/passwd`** übereinstimmen

2.29.2 Passwort

! bzw * gesperrt
Kein String angegeben kein passwort

2.29.3 Min

Wie lange muss passwort behalten werden

2.29.4 Max

Maximale gültigkeit des Passworts

2.29.5 Warnung

Wie viele tage vor ablauf der frist muss warnung ausgegeben werden um passwort noch ändern zu können

2.29.6 Frist (Gnadenfrist)

Nach Ablauf der $Max dürfen noch $Frist Tage lang eingeloggt werden

Min/Max/Warnung/Frist gilt nicht für root

2.30 UnixTimeStamp

```
perl -e 'print localtime(time()) . "\n"'
perl -e 'print localtime(1141408532) . "\n"'
```

2.31 gpasswd

ändert Gruppenpasswort
Gruppen haben kein Home Verzeichnis

2.32 Usermod

usermod –g abbts marc ändert die Primäre Gruppe eines Benutzers permanent
usermod –G abbts marc das hingegen fügt die den Benutzer nur der Gruppe hinzu

2.33 newgrp

Wechselt temporär die Gruppe, so dass Dateien mit einer bestimmten Gruppe angelegt werden, sofern der Benutzer Mitglied dieser Gruppe ist sonst:

Beispiel:

sudo groupadd neueGruppe	neue gruppe erstellen
sudo usermod –G neueGruppe Benutzer	Benutzer
su Benutzer	
newgrp neueGruppe	
touch neueDatei	
ls –l neueDatei	
exit	Wechselt zur normalen Gruppe

2.34 sg (Switch Group)

Gruppe wechseln

sg audio //wechselt die Primäre gruppe temporär auf audio

2.35 groupadd

fügt eine Gruppe hinzu, -o erlaubt auch non-unique Gruppen, also ein GID zu verwenden die schon gebraucht wird

2.36 Datei in eine Andere Gruppe verschieben

chgrp zielGruppe Datei verschiebt die Datei in die zielGruppe

2.37 Opensource Exploit framework

Metasploit http://www.metasploit.com/

2.38 Dateien im Verzeichnis mit Gruppe des Verz. Erstellen

chmod 2775 verzeichnis oder 2xxx
2=SGID Weitere Infos **man 2 chmod**

2.39 Mehrere Gruppen umbenennen

```
for i in 2 3 ; do groupmod –n group$i test$i; done
```

2.40 MALLOC (Systemroutine die speicher bereit stellt und adresse zurück gibt)

Root…: Zugriff per kmem //kernel memory
User: : Zugriff per System //Folglich malloc!=malloc

```
man malloc
```

2.41 /etc/gshadow

Im paket shadow oder so
Passwort wird sonst ins /etc/group geschrieben
im gshadow

root:x:0:root
benutzer:passwort:GID:mitglieder

2.42 PseudoBenutzer

Für administration
Für dienste
Kein Login, kein passwort gesestz
z.B. LP printer deamon
programm wird als root gestartet, dann werden die rechte weggenomen
z.B. zuerst einen TCP/UDP (port 0-1024) öffnen, dann kann herunter geswitcht werden auf anderen user

```
ls -l /dev/hd*
```

root CD-ROM →hda

2.43 Benutzer mit Passwort eröffnen (Geht nicht)

useradd –m –p $(md5crypt passwort)
tcllib: usr/lib/tcllib1.6/**md5crypt**/md5cryptc.tcl

useradd –m –p „$(grub-md5-crypt)“ vorsicht dollar zeichen → GEHT NICHT

OpenBSD *encrypt* command

xref: /src/crypto/openssh-4/md5crypt.c / .h

2.44 Root passwort vergessen

1. früher einfach /etc/passwd ändern
2. Single user mode starten, shadow editieren, allenfalls geht es pw zu löschen
3. wie 2 aber von benutzer mit bekanntem password hash kopieren

Bei SELINUX gibt es eine Checksumme für /etc/password bzw. /etc/shadow dann kann man es vergessen

2.45 Homedirectory auf SMB (Server Message Block)

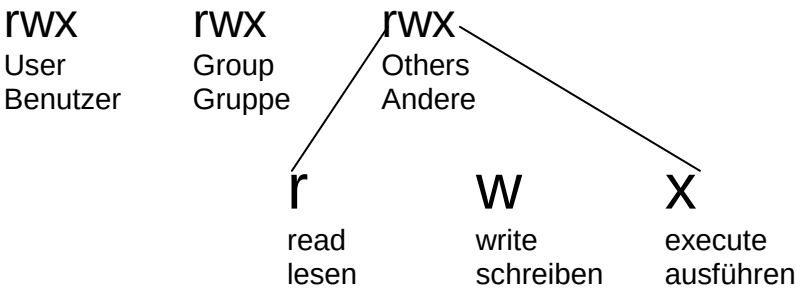
```
useradd –c „Test 1“ –g 2001 –d „smb://server/home“
```

3 Zugriffsrechte

3.1 Rechtekonzept

Unix: Nur EIN bestimmter Benutzer und EINE Bestimmte Gruppe

RWX (read/write/execute)
Die Berechtigungen werden z.B. mit **`ls -l`** in 3 Dreiergruppen dargestellt



3.1.1 r (read)

Datei
die entsprechende Datei darf zum lesen geöffnet werden

Verzeichnis
Im entsprechenden Verzeichnis darf dessen Inhalte gelesen werden

3.1.2 w (Write)

Datei
Schreibrecht auf eine Datei, aber auch löschen

Verzeichnis
Es dürfen Dateien erstellt werden

3.1.3 x (eXecute)

Datei
Die Datei darf mit den Berechtigungen des aktuellen Benutzers ausgeführt werden

Verzeichnis
Nur mit dem Executerecht in das Verzeichnis gewechselt werden. Besitzt ein Benutzer nur das Read recht, so kann er zwar den Inhalt anzeigen aber dennoch nicht in das Verzeichnis wechseln. Andererseits falls Verzeichnis nur 700 ist kann ein Benutzer der Gruppe auch in ein Unterverzeichnis in welches er Berechtigungen hat nicht erreicht werden, da im Hintergrund ein cd auf das Verzeichnis ausgeführt wird, also ein execute.

3.1.4 Abarbeitungsreihenfolge

Linux schaut zuerst den user an, ist der gleich und hat keine rechte, so wird hier abgebrochen, auch wenn ich in einer Gruppe wäre, die rechte hätte kann ich dennoch nichts machen. Hingegen kann der Benutzer ja seine Rechte ändern.

marc (user)	users (group)	others (others)	
0	7	7	ganze Welt kann alles aber marc nichts

3.1.5 setUID (Set user ID on execution)

Datei
Datei, wird mit den Rechten des Besitzers ausgeführt.

Verzeichnis
Auf z.B. FreeBSD können so Dateien und Unterverzeichnisse den Benutzer des Top Verzeichnisses erben, **anstelle des Benutzers vom erstellenden Prozess**.

suid Programme suchen

`find / -perm -4000 -ls`	Vorsicht das Minus bei -4000 ist nötig
**`...	wc –l`**	allenfals zur Kontrolle zählen und notieren

Beispiel:
`ls –l `which passwd``
-rw**s**r-x-r-x 1 root shadow 32916 Dec 11 20:47 /usr/bin/passwd

3.1.6 Hintertüren

Wurde allenfalls im C/C++ Code ein Strcpy anstelle eines StrnCpy verwendet so kann dies mittels Bufferoverflow missbraucht werden um Shellcode auszuführen und sich so -- falls das Programm root gehört -- Rootrechte auf der Maschine anzueignen. Andererseits kann so z.B. eine Hintertür eingebaut werden
`chmod backdoor u+s`
dann als root:
`chown root backdoor` //löscht suid-bit folglich muss das wieder gesetzt werden
`chmod backdoor u+s`

FAZIT> Vorsicht umask 4xxx mit root dingen

3.1.7 setGID (Set group ID on execution)

Datei
Die Datei wird unter dem Gruppe der Datei gestartet.

Verzeichnis (Für gruppenshare)
force all files and sub-directories created in them to be owned by the directory group and not the group of the user creating the file. SGID-Bit Für **Verzeichnisse** so dass es der Gruppe gehört so werden Dateien unter dieser Gruppe eröffnet

3.1.8 StickyBit

Datei
Die Datei wird im Speicher belassen, was vor allem früher von Bedeutung war. Heute Programmspezifische Bedeutungen

Verzeichnis
Nur der Eigentümer vom File kann das File löschen (vorausgesetzt, dass der Eigentümer auch Schreibrechte auf dem Verzeichnis hat).Beispielsweise im Verzeichnis für temporäre Dateien (/tmp) kann der Benutzer seine eigenen Dateien löschen. gemeinsam verwendet
/var/spool
/tmp
/usr/tmp

3.2 chmod (change file access permition)

Mit chmod können die Berechtigungen verändert werden

```
chmod [ugoa][+-=][rwxXst],[ugoa][+-=][rwxXst],... datei
chmod 4777 datei
```

u: User [4]
g: Group [2]
o: Others [1]
a: All 7

+: Hinzufügen
-: Löschen
=: genau diese Einstellung

r: read 4
w: write 2
x: execute

X: `chmod +X test*`
nur Verzeichnisse setzen z.B. setzt execute nur bei Verzeichnissen die mit test beginnen, nicht aber bei Dateien die mit test beginnen

u+s: SUID-Bit [4] Set user ID on execution
Wird als mit den Rechten des Besitzers ausgeführt (effective user)

g+s: SGID-Bit [2] Set group ID on execution
Auf Datei:
Datei wird mit den rechten der Gruppe ausgeführt
Auf Verzeichnis:
Dateien und Verzeichnisse werden mit den Gruppenrechten des Verzeichnisses erstellt und Verzeichnisse erhalten wiederum dieses Bit, rekursiv

Bei ls –l: Nur SUID-Bit nicht aber x-Bit gesetzt ergibt ein grosses S

t: Stick [1] (t-Mode)
User der erstellt kann rechte setzen und Datei auch wieder löschen, sonst niemand
(Nur Verzeichnisse) z.B. /var /tmp
Früher mit Bändern war es auch dazu, dass das Programm im Speicher blieb.
Vorsicht hineinkopieren verhält sich anders als hinein verschieben.

ls –l zeigt jeweils auch noch ein **`drwxrwx--T`** statt **`drwxrwx--t`** wobei das grosse **`T`** bedeutet, dass es kein ausführungsrecht hat

weiteres **`man 2 chmod`** bzw. **`man 2 stat`**

`chmod u+s`	//setzt SUID bit
`chmod g-s`	//löscht SGID bit
`chmod +t`	//setzt Sticky bit
`chmod –t`	//Löscht Sticky bit

3.3 Umask (user file creation mode mask)

Rechte die im Maximum vergeben werden. Vorsicht Beeinflusst nur Dateien die erstellt werden, nicht aber schon vorhandene Dateien.

3.3.1 Standardwerte

Datei: 666 (Soll eine Datei ausführbar sein muss dies mit chmod gemacht werden)
Verzeichnis: 777

3.3.2 Berechnung

1	Wert der umask	027	
2	Komplement	750	
3a	Zugriffsmodus neue Datei:	666	(Standard für Dateien)
3b	Zugriffsmodus neue Datei:	777	(Standard für Verzeichnisse)
4	Resultat (2 AND 3)	640	

Oder 666_8 AND NOT(027_8) = 640_8

3.3.3 Standartwerte

Typischerweise setzen in
/etc/boot

/etc/profile	für alle Benutzer
/etc/bashrc	für alle Benuzer (Bash)
/etc/cshrc	für alle Benutzer (csh)
~/.profile	
~/.bash_profile	
~/.bashrc	Letztes das kommt, folglich würde das hier gelten Und auch die standart von root vergebene umask überschrieben

Auf z.B. umask 0003

3.3.4 Datei zu einem Benutzer verschieben

Normalerweise kann nur root eine Datei zu einem anderen Benutzer verschieben
Der Empfänger muss eine Kopie des original machen, die gehört dann dem „Empfänger“

Ist man in entsprechender Gruppe kann man mit chgrp die Gruppe ändern womit auch jemand anders die Datei allenfalls verändern kann chmod x6x

`chgrp root list.sh`	geht nicht und soll auch nicht gehen.
`chgrp g+x list.sh`	ausführbar für Gruppe

3.3.5 xserver

Hat eigene umask, könnte man z.B. auf 0021 setzen…

3.3.6 Syntax

umask 027 ist das selbe wie umask u=rwx,g=rx,o=
Vorsicht hier keine Leerschläge!!

umask	oktale Anzeige
umask –S	Anzeige mit Buchstaben

3.3.7 Inside

umask 7 verwendet oktalzahl intern → 007

3.3.8 Beispiele

chmod –c 0070 verzeichnis kann nicht mehr gelesen werden, da ich als Benutzer kein recht mehr habe auch wenn ich noch in der entsprechenden Gruppe wäre.

umask=022	erstellt	rwx r-- r--
umask=006	erstellt	rw- rw- ---

```
umask
umask –S
umask 0000
umask –S
umask 0777              erstellt trotzdem nur 666 für dateien
touch test
ls –l

chmod a+rwx datei
chmod u+rw datei
chmod u=rwx,g+r,o=
chmod –x
chmod +x                auch von umask abhängig, nicht aber chmod o=x
umask 0022
touch datei1 datei2
chmod +x datei1
ls –l
umask 0027
chmod +x datei2
ls –l
```

3.4 Pam (Plugable Authentification Modul)

Systemlibrary die die Authentifizierung auf einem Linux System handhabt.
man pam

3.5 Eigentum an Prozessen

Mit sudo müsste man sich mal noch überlegen wie und wo die Speicher benutzt werden
Sudo speicher gehört root, bzw im gemeinsamen Speicher → Brause

Um Executables ausführen und Parameter zu übergeben müsste der Stack gemeinsam sein…

Wenn zwei Prozesse ein R (runing) haben ist es ein Mehrkern Prozessor

`ps –eo pid,euser,ruser,size,vsize,stat,comm`

Effektiver User / Realer User

Realer Benutzer ist der Reale menschliche Benutzer
Effektiver Benutzer ist nur anders wenn ein SUID Bit gesetzt ist

3.6 ps

`ps –u` //oder ps ax

Minus-Zeichen von systemV

Vorsicht verschiedene Distributionen geben bei ps ax oder ps ef nicht die gleichen ausgaben

Pstree

3.7 Lsattr (nur root)

Lsattr /var/log/messagges

3.8 Chattr (nur root)

Chattr +a /var/log/messages
Chattr –R –j /data/wichtig DATEN INS JOURNAL
Chattr –j /data/wichtig/nichtso

Ausprobieren

A	atime Access time, ls macht nur zugriff auf verzeichnis, nicht auf datei Kann auf notebook-rechner dafür sorgen, dass die platte nicht ständig läuft, logs ansehen → muss atime geändert werden
a	append only
d	wird von dump nicht gesichert
i	immutable Datei kann überhaupt nicht verändert werden
j	Schreibzugriffe auf dateiein werden im Journal gepuffert, DATENBANKEN!!!!! Inhalte der datei werden sonst nicht ins journaling eingetragen, so schon.
S	Schreibzugriffe werden synchron, also ohne interne pufferung, ausgeführt

KOMPLETTE LISTE UNTER `man chattr`

3.9 ls –lu –la –lc (sort by access, change… -time)

ls –lu
ls –la
ls –lc
ls –l –full-time Zeigt den ganzen timestamp, menschenlesbar

Weitere Attribute verändern
ls -l --time=ctime|atime|mtime

Creation **time**
Modification **time** standart anzeige von ls
Access **time** lesender zugriff, z.B. cat

La –lt sortiert nach zeit

3.10 Intermezzo

3.10.1 Pfad eines Programms angeben

which sh //gibt Pfad an

3.10.2 Shell builtins Hilfe

man bash-builtins //gibt Hilfe über builtins

3.10.3 Ausführbare Dateien (ELF Binaries)

file /bin/bash

ELF 32-bit LSB shared object, Intel 80386… , striped
- striped: Verteilt auf HD, früher bei band wichtig
- Intel 80386…: CPU architektur
- LSB: Little / Big endian,
- shared: Mit library

Tabulator function schaut auch ob eine datei ausführbar ist…

3.10.4 Wall und write

auf terminal schreiben
wall
write
in gruppe tty so hat es rechte auf die tty's → ls /dev/pts
cat datei | wall

4 Partitionen und Dateisysteme

Allenfalls auch auf Virutalbox, VMware, xen

1 Festplatte partitionieren
2 Linux FS erstellen können
3 Werkzeuge zur Dateisystemprüfung
    Fehlertabellen: zeigen Fehler an, reagieren bevor Ausfall
4 Lokale Dateisysteme in den Verzeichnisbaum einbinden
5 Platten Kontigentierung für Benutzer und Gruppen einrichten

4.1.1 Festplatte partitionieren

Festplatten lassen sich in Partitionen einteilen
Für grössere Systeme wurde fürher je eine Festplatte verteilt
    /etc
    /home
    ….
Dann partitioniert

Heute Cluster Filesystem freigegeben von Sun, so lassen sich festplatten einfach hineinhängen. Im prinzip stripeSet. Es werden zusätzlich Checksummen gebildet so können ienzelne Festplatten ohne Folgen ausfallen

Detaillierte Grafiken in Datei **disk.pdf** von Herr Honegger

4.1.2 Sektor 0 (von IBM, Intel, oder Berklay)

1. Sektor Master Boot Record: die ersten 512 Bytes = erste Partitionstabelle
Fängt zuäusserst an, ganzer kreis wird gebraucht, 512 Gebraucht, rest mit muster bzw sequenz, **Preamble**
Partitionstabelle

MBR: 446 Bytes Initial Program Loader
    4X16 Byte Tabelleneintrag
        1 Active 4 Start 4 End x Cylinder y Heads z Sektor 8-Bit
            LBA CHS FS Typ 83=swap
            Lineare Blockbeschreibung (Linear Block Adressing)

4.1.3 LBA (Logical Block Adressing)

$$LBA = \left(\left(c \cdot H + h\right) \cdot S\right) + s - 1$$

4.2 Plattentypen

SCSI: bis 15 Partitionen
Lizenzgebühren für Controller, Consortium
Rechenarbeit ausgelagert auf HD-Controller

IDE
IO interface, ohne intelligenz
63 Partitionen
2 Pro bus, Adressierung der Adresse mit Jumper

ATA
Erweiterung von IDE
80 Kabel 40 Daten dazwischen je eine Masse

SATA
Gleiches Protokoll wie ATA, aber über Serielle Leitung
Werden wie Scsi Platten behandelt

Ab Kernel 2.20 alles wie SCSI platten

+5V (1) gegenüber -5V (0) weniger Störanfällig als 5V(1) 0V(0)

4.2.1 Primäre Partitionen IBM

Max 4 Partitionen

1. OS
2. Daten

Swap war vom einfachen Dos nie Vorgesehen

4.2.2 Logische Partitionen zum weiteren unterteilen der 4 Partitionen

Weitere erste Sektoren
Früher auf der Oberfläche

4.2.3 Primäre Partitionen mit Unix

Unix Berkley System mit 8 Partitionen

4.2.4 Sektoren

Heute Dynamische Sektoren

4.2.5 Magnetisierung

Molekuler in die Festplatte hinein

4.2.6 Kopf

Hat abstand durch Luftspalt der durch die Rotation entsteht (Hartes Luftpolster)

4.2.7 Beschleunigung

Masse gross → Grosse energie Notebook platte läuft langsamer

4.2.8 Headcrash

80-100G im Betrieb da hartes Luftpolster
Horizontale Beschleunigung nicht so schlimm da hartes Luftpolster

4.3 Linux FS erstellen

4.3.1 Ext2 ext3 XFS

Standart Attribute überall gleich, erweiterte Attribute unterschiedlich, ACL
Siehe **`lsattr`**

Ext3 fs als Datei anlegen

```
dd if=/dev/zero of=/home/marc/disk1.img bs=1024 count=10000
```

if: input file
of: output file
bs: block size
count: size

`mkext3 –F disk1.img` oder **`sudo mkfs.ext3 –F disk1.ext3`**

F: file

```
sudo mount -o loop disk1.ext3 /media/image/
```

4.3.2 Bootfähige CD

Partitionstabelle auf cd.img machen und aktiv schalten → bootfähige CD-ROM, nur ext2, weil journaling auf ext3 keinen sinn macht, gibt aber nur Fehlermeldung läuft aber sonst

4.4 Inode Tabellen

Die Inode Tabelle enthält hinweise in welchem Block sich welche Datei befindet
Inode Tabellen sind mehrfach vorhanden und werden der reihe nach gebraucht, so dass es immer mehrere ältere Versionen gibt, sie wandern so zu sagen nach hinten.
So kann Disk wieder konsistent gemacht werden, meist automatisch beim Neustart nach z.B. Stromausfall. Das ist bei einem Journaling Filesystem nicht nötig, da an Hand des Journals die Konsistenz gewährleistet ist

Inode: Tabelle mit allen Stücken der Datei ?? ist das so?
VFAT: Stück entweder end of file oder zeiger auf nächstest stück

4.4.1 Inode Tabelle:

Name Zeiten (access, mod, change) Linkcount 13 Zeiger auf Lineare Blöcke

13 Zeiger
Bis 10 Block zeiger direkt auf block (direct adressed)
11. Block Zeigt auf inodeeintrag ohne namen (indirect adressed)
12. Block Zeigt auf inodeeintrag ohne namen (indirect adressed) und weiter verschachtelt
13. double indirect blocks
→ max 2.4TB grosse Dateien → grössere Blocksize beim erstellen des FS → grössere datei

4.4.2 Fallstricke

Ist eine System mit **Dualboot** z.B. **Windows / Linux** installiert, und wird z.B. Linux in den **Ruhezustand** versetzt, dann vom Windows Daten auf einer gemeinsam genutzten Partition verändert, kann es passieren, dass die **Inodetabelle** vom sich im Ruhezustand befindenden System die eigentlich korrekt von Windows veränderte Inode Tabelle überschreibt. Folgen können sein: Dateien die geschrieben wurden sind nicht sichtbar, im schlimmsten Fall ist die Partition nicht mehr zu gebrauchen. Folglich müssen beide Systeme so konfiguriert werden, dass sie vor dem Ruhezustand die inode Tabellen zurück schreiben und beim wiederaufnehmen des Betriebs diese wieder neu einliest. Alternativ kann die Inode Tabelle nicht im Speicher gelegen sein sondern immer direkt auf die Platte geschrieben werden.

4.4.3 Festplattenpartitionierung

Zuerst überlegen
- Home-Verzeichnisse
- SWAP
- Datenbanken / Anderes OS, Oracke DB

Dann mit **`fdisk`** Partitionieren

Vorteil von Partitionen, Gesammte Daten auf partition Backupen und zurückspielen

4.4.4 SWAP Doppelt (für Hotplugable?)

4.4.5 Windows Laufwerksbustaben zuordung

Erste Platte	1 C:		5 G:
Zweite Platte	2 D:	3 E:	4 F:

4.5 Sektoren

Normale Platte 64 Sektoren, wovon auf dem ersten Track nur der erste gebraucht wird: 63 Sektoren für Verschlüsslung, 2. System, Trojaner, Bootsektor virus

4.6 Partitionieren

Zuerst sollte immer die Partitionstabelle sichern:

4.6.1 Sichern

dd if=/dev/hda of=/dev/st0a //allenfalls eigenen title machen
scsi tape 0=1. Tape,

dd if=/dev/hda –bs=512 count=1 | hexdump
dd if=/dev/hda1 count=1 | gzip > hda1.dat.gzip
dd if=/dev/hda2 count=1

Nur MBR Sichern
dd if=/dev/had of=mbr_hda.dat bs=512 count=1
virenscanner durch disassembler lassen
disas mbr_hda.dat

Nur MBR Zurückschreiben
dd if=mbr_hda.dat bs=512 of=/dev/hda

native, ohne librarys, direct auf plattentreiber → Root sein

data/disk dubbing

cluster FS von sun anschauen

4.6.2 df

Disk free

4.6.3 MBR Anzeigen

cat mbr_hda.dat → Terminal verschossen
reset

deshalb besser more mbr_hda.dat
oder hexdump

der Masterbootrecord kann mit einem Disassembler betrachtet werden und so findet man allenfalls einen Bootsektor virus.

4.6.4 Disassembler

Schön menugesteuerter: biew

4.7 GPT

GUID – Partition Table Scheme NACHLESEN

4.7.1 GUID Partion Table(GPT)

Löschen mit

dd if=**/dev/zero** of=/dev/hdd bs=512 count=63

4.7.2 Meier: Ghost sei maske für dd

Inode Tabelle und mit dd gezielt einzelne Blöcke holen
cpio

4.7.3 Virus

dd abbild der verseuchten disk auf CD-ROM dann auf loopdevice mounten, so lässt er sich analysieren

4.8 Fdisk

Unix: Mehrere Primäre

DOS/WINDOWS: Nur eine Primäre von fdisk erstellen, doch system kann auch mit mehreren umgehen

fdisk –l /dev/hda

l: list
u: in Sektoren angeben

fdisk –l > konfiguration.txt
fdisk –lu >>konfiguration.txt

Menu [m|d|n|p|t|q|w]
m: Kommandoübersicht
d: Partition Löschen
n: neue Partition
p, 1, 1 (default) 1 (default) +1G (von bestehendem aus 1 GB mehr)
p: zeigt Partitionstabelle an
t: ändert die „Partition system id“ → z.B. SWAP Typ 82
q: quit, ohne änderung
w: write
x: expertenmodus
Sektorennummern ändern usw.

Disk hat auf chip identifikationsnummer

4.8.1 Sfdisk

Partitionstable manipulation, nicht interaktiv
sfdisk –d /dev/hda1 >hda1.parts //sichern
sfdisk –d /dev/hda1 <hda1.parts //restore

4.8.2 cfdisk

console-fdisk: für batch gesteuert partitionierung

4.8.3 Parted

4.8.4 Gparted

4.8.5 YaST2

4.8.6 DiskDruid

4.8.7 Mechanik der HD

Ganz fürher Schrittmotor
Früher Synchronisations Spur
    0xF6 an jedem Sektorenanfang, dann header mit spur / Sektornummer

0x55aa demiliter für partitionstabellen ende, oder bios/sektorende von iokarten mit bios

4.9 Laufwerke

Hda Primary Master
Hdb Primary Slave
Hdc Secondary Master
Hdd Secondary Slave

Hda1 - hda4 Primäre Partitionen
Hda5 - … Erweiterte

SCSI: /dev/sda …..

4.9.1 Mountertag auf jeder platte und an hand dieses tags das device zuordnen

4.9.2 Partitionen

/boot als erste Partition → am wenigsten Probleme

4.10 Devices

Jede Partition wird einem Device Driver zugeordnet: hda, hdb …
Kann je nach Reihenfolge Probleme. Tabelle neu sortieren:

Alternativ kann man einfach die Mounts ändern

4.11 Partitionstypen

Primär:

Erweiterte (Extendet):
Hat wieder Boottabelle

4.12 Erstellen eines Dateisystems

Lowlevelformat nur früher, heute schon lowlevel formatiert
Partitionierung
Filesystem pro partition erstellen, HiLevelformat
Inode bzw FAT

`Mke2fs –b 2048 /dev/hdd1` oder auch alternativ **`mkfs.ext2 mkfs.ext3`**
Was immer die Selbe hardgelinkte Datei ist was uns auch **`ls –li /sbin/mk*`** zeigt

-b	Blockgrösse
-c	überprifen auf defekte Blöcke
-i <anz>	inodedichte (hoch für Backup mit hardlinks differential) bytes per inode
-m <anteil>	**Datenblöcke die für root reserviert sind in %**
-j	erzeugt zusätzlich ein ext3 Journal

Nachträglich verändern bedingt mit tune2fs möglich

4.13 tune2fs [<optionen>] <Gerät>

Ändern von Parameter des Filesystemes nach dem Erstellen wenn allenfalls schon Daten drauf sind. VORSICHT GEBOTEN, nur verwenden wenn nicht gemountet, sonst werden Daten aus dem Speicher nicht zurück geschrieben

`tune2fs –e remount-ro /dev/hdd1`
-c <anz mounts>
-e
Continue
Remount-ro ← Sehr gut für raid
Panic (2. Raiddisk die ausfällt)
-i <anz Tage>
-l list contents of superblock
-L Lable
-f force

4.14 „Quota“ per tune2fs

df
tune2fs –l /dev/hdd

UUIN jede platte eine Eigene Nummer
Magic number
Se_super z.B. Readonly setzen
FS state
Error behaviour: continue (standard)
tune2fs -e continue | remount-ro | panic
Inode.count: maximale anz. Dateien
Reserved block count
Free blocks
Free inodes
First block 1
Blocksize
GTD blocks

tune2fs –m 20 disk1.dat 20% der Blocksreserviert, disk nur zu 80% füllbar
mount –o loop disk1.dat /media/festplatte
bei 10 mb platte
dd if=/dev/zero of=test count 8000 bs 1000
permission denied mount → dann sieht man rechte
mount –o loop disk1.dat /media/festplatte –o user=abbts
mount –o loop disk1.dat /media/festplatte –o uid= GEHT NICHT WIRD ER NACHHOLEN

4.14.1 reisertools

gleiches für reiser
mkreiserfs <Device>
ReiserV4 nicht aktiv gepflegt folglich nicht im kernel
Resize_reiserfs +|- <size> <Device>

4.15 Reperatur von Dateisystemen

Power off
Stromausfall
Fehler in FS

Fehlerhafte
-Verzeichnisseinträge
-Inodeeinträge
-datei in keinem Verz drinn
-datenblock zu mehreren verschiedenen datenblock

Nicht alle reparaturen können ganz ohne datenverlust vorgenommen wird
Buffer wird z.B. nicht gesichert, allenfalls journaling auf datei machen
Dateisystem ist aber danach wieder in konsistentes filesystem
Lost+Found bekommt blocks die mit neuer inode versehen werden

4.16 fsck

alle 3 Monate, von hand, da z.B. server nicht oft gebootet wird, kein automatischer fsck

4.16.1 Fsck.vfat dosfsck

Zum überprüfen von VFAT. Im package dosfstools
(**`sudo apt-get install dosfstools`**)

4.16.2 Fsck.ext2 e2fsck

-b <nr>	liest Den superblock mit <nr>
-f	auch im gemounteten zustand (Besser nicht)
-c	sucht defekte blöcke
-p	automatische reparatur
-v	informationen über status

4.16.3 Fsck.reiserfs reiserfsck

4.16.4 Fsck (filesystem check for Linux FS)

überprüft Filesystem

fsck -t <typ> <device>

fsck -y alles mit ja beantworten, falls 1000e von Fehlern

zum Reparieren sollte das FS ro gemountet oder besser ausgehängt sein

man stelle sich syslog vor der noch adresse hat und fsck der tabellen verändert

1. Die angegebenen Befehlsargumente werden geprüft.
2. Es wird kontrolliert, ob das gewählte Dateisystem eingehängt ist.
3. Das Dateisystem wird geöffnet.
4. Es wird geprüft, ob der Superblock lesbar ist.
5. Es wird geprüft, ob die Datenblöcke lesbar oder fehlerhaft sind.
6. Die Informationen aus dem Superblock über Inodes, Blöcke und Größen werden mit dem aktuellen Zustand des Systems verglichen.
7. Es wird überprüft, ob die Verzeichniseinträge mit den Inodes über¬einstimmen.
8 Es wird geprüft, ob jeder als belegt gekennzeichnte Datenblock exis¬tiert und genau einmal von einem mode referenziert wird.
9. Die Anzahl der Links in den Verzeichnissen wird mit den Link-Zäh¬lern der modes verglichen (muss übereinstimmen).
10. Die Gesamtzahl der Blöcke muss gleich sein der Anzahl der freien Blöcke plus der Anzahl der belegten Blöcke.

Dateien, deren inodes in keinem Verzeichnis eingetragen sind werden im Verzeichnis **lost+found** mit inodennummer als Namen eingetragen. Eine nicht leere Datei aber in keinem Verzeichnis eingetragen wird gelöscht, bzw .wird gefragt ob man sie löschen will

4.16.5 Superblock nicht lesbar

`e2fsck -f -b 8193` (muss superblock sein) **`/dev/hdd2`**
VORSICHT kopiert erst und kontrolliert dann ob OK

4.16.6 dumpe2fs

Tool zu anzeigen und manipulieren des Superblocks.
`man dumpe2fs`

4.16.7 debugfs

Zum Debuggern eines LinuxFS.

4.16.8 resiserfsck

4.16.9 reserfstune

4.16.10 debugreiserfs

reiserfs wird beim booten automatisch repariert vom kern, so viel wie er halt kann

4.17 mount

zum einhängen, „montieren“ eines Filesystems in ein Verzeichnis allenfalls (/usr firewall, router) und /opt ro mounten auf Serversystem.

```
mount –t ext3 –o user,ro /dev/hdd1 /mnt/testHD
```

Vorsicht, existieren Dateien unterhalb des mountpoints kann auf diese nicht mehr zugegriffen werden, oder sie können so versteckt werden

4.18 umount

… ist das Pendant zu mount um ein FS wieder auszuhängen. Es dürfen keine Benutzer mehr auf dem FS sein

`umount /dev/hdd1` oder **`umount /mnt/testHD`**
geht das nicht kann mit **`sudo lsof /mnt/testHD`** herausgefunden werden welcher User/Prozess noch zugreift und diesen mit **`kill -9 PID`** killen.

4.19 lsof (list open files)

siehe hier

4.20 /etc/fstab (file system table)

Zum Einbinden von Partitionen (Auch pseudofilesysteme wie -devpts, proc, usbfs)
(Im ram liegende inode tabelle)

Swap: Priorität festlegen, weniger bei langsamen hd's notfall

<filesystem>	<mountpoint>	<fstyp>	<options>	<dump>	<pass>
/dev/hdd1	/mnt/testHD	ext3	defaults,noauto	1	1

Options Leerlassen geht nicht → defaults

defaults	
noauto	Nicht automatisch mounten
ro	readonly
user	benutzer kann auch mounten
sync	files werden direkt geschrieben und nicht gecacht
exec	permit execution of binaries
noexec	gegenteil

dump
für dump befehl ohne parameter dumpt alles mit true im flag true

pass:
fsck order: reihenfolge für den fsck
0 wird nicht geckeckt, allefalls gut für grosse platten 1TB++ dauerte es zu lange

4.21 /etc/mtab (Mount table)

Die die wirklich gemountet sind, automatisch vom mounter erstellt
umount sieht in dieser liste nach zum unmounten /proc/mounts ist eine zuverlässigere Tabelle

4.22 LVM (für Datenablage, booten von lvm eher unvorteilhaft)

Volume Group aus Partition auf Platte 1 und eine von Platte 2, folglich wird's verteilt ähnlich auf Raid.
Und je ein schnitz Swap auf jeder platte

Volume gruppen können wieder partioniert werden
/home
/var
/temp
Alles auf lvm

4.23 free

Freier Speicher, bzw. aktuelle Speicherbelegung
Zeigt auch Buffers und Cache an
Zeigt auch Swap an

Free –ot

t: zeigt zusätzlich total an

4.24 SWAP

Heutige Distributionen fangen erst an zu swappen wenn der Speicher voll ist, früher war das bei 20% üblich, damit immer genügend Speicher verfügbar war.

Faustregel: 2-3xRam

Orakle 8GB Ram + 16GB Swap kann allenfalls zu wenig sein, sollte es sich zeigen, dass temporär mehr swap benötigt wird kann das wie unten beschrieben temporär vergrössert werden.

Auf Notebook allenfalls gar nicht zwingen nötig wenn 2 gb ram
Im notfall kann z.B. ein File als swap eingebunden werden, z.B. bei einer Meldung OUT OF MEMORY bei fast komplett reorganisierter Datenbank

4.25 swapon

swapon, so kann temporär der Swap-Speicher erweitert werden

-s status

4.25.1 Erweitern

```
Dd if=/dev/zero of=swapdatei bs=1024 count=10000
mkswap swapdatei
swapon swapdatei
swapon -s
```

swapoff swapdatei //versucht in andere swaps zu kopieren

swapon –a //mountet vom /etc/fstab 2. tabelle

4.26 Quota

(ext2, ext3, XFS. ReiserFS)
Um benutzerspezifische Limiten für jedes FS zu setzen empfiehlt es sich quota zu verwenden.

Packages: quota, quotatools

Für andere Dateisysteme gibt es „Pseudo Quotasysteme„

4.26.1 Arten von Quota

- Auf Benutzerebene
- Auf Gruppenebene

4.26.2 Arten der Implementierung

- Soft quota (Warning quota) z.B. mehr als 3 wochen drüber wird gesperrt
- Hard quota (Fixe limite)

Pro Dateisystem vergeben
/home:100MB
/var: 30MB
…
Vorteil der Datei: man kann scripten und muss so nicht 100 Benutzer einrichten

Das ganze wird von einem Kernelmodul gemacht und entsprechend beim mounten angegeben werden:

mount –**o remount,usrquota** /home //remount wäre nur nötig im lauffenden Betrieb
mount –**o usrquota,grpquota** /home //für Gruppenquota
→aquota.group
Quotaon –augv

a: All
u: User
g: group
v: verbose

quota –g Ziegt gruppenquota statt user quota an

oder in fstab:
/dev/hda5 /home ext3 defaults,usrquota 0 2

Wies funktioniert: Datei | quotamanager | filesystem

4.26.3 Anzeigen der quota

quota marc2

`quotacheck -avu`
→ quota.user datei des users root wo alles drinn steht (Binärfile)
→ Regelmässig durchführen um das quota zu kontrollieren → cronjob
→ Liste der Benutzer wer sie überschritten hat

→user → Email → automatische Benarchrichtigung ~/.profile

quotaon -avgu
-a alle aus fstab
-q quiet //nur wenn quote überschritten, login

quotaoff

quotatool
wenn quota installiert ist, gipt es start und Stopp scripte

4.26.4 Quota editieren (edquota)

`edquota -u hugo` //user hugo, [ctrl-o] [ctrl-x]
blocks zeigt benutzer platz an
soft zeigt softquota
hard zeigt hardquota
→ $EDITOR wird als Editor genommen
→ $VISUAL wird als Editor genommen
Sonst standard Editor

edquota –g gruppe //edit group quota, quote für ganze gruppe, selten gebraucht
//Benutzer könnte in eine andere Gruppe wechseln (newgrp)
edquota –p tux hugo //prototyp tux auf hugo kopieren, INIT
edquota –t 10[seconds|minutes|hours|days] //Frist für Softquota
→normaler Betrieb, vorallem Mailserver auf ca. 14 Tage (Ferien)

Via Samba Client sieht man nicht wenn Quota überschritten ist!

quotachech –f /mnt

QUOTA UND DB keine gute Mischung, auch .PST Dateien nicht, werden Inkonsistenz

4.26.5 Ganze Quotatabelle anzeigen

repquota –a
repquota –s //human readable

4.27VARIA

4.27.1 Backupraum

Sollte Rauchgeschottet sein, wegen russ, denn sonst sind Bänder nicht mehr zu gebrauchen

4.27.2 überlaufschutz (tune2fs)

für /tmp /var

4.27.3 Dateiattribute des ext-fs

Tannenbaus minix fs war nur zum schauen wie ein fs funktioniert, doch aber nicht zum wirklich brauchen, vor allem ab mehr als 20 dateien, keine inodes….

→Buch Brause

Reiser sei in Untersuchungshaft, er soll seine Frau ermordet haben, Knowhow träger seien verteilt…

4.27.4 /usr/local/bin entspricht einem /opt

5 Der Bootloader

5.1 Generell

BIOS sucht nach start ein Betriebssystem
Bootreihenfolge, linux braucht kein aktiv setzen der Partition, manche biosse schon

-Diskette
-CD-ROM
-Festplatte (nur die das Bios nativ unterstützt, d.h. die ersten 4)
-USB Gerät mit Bootsektor
-Netzwerk (PXE)

PoE Power over Ethernet
Über 90+2*5 meter max 3V
Spannungsabfall

MBR sieht immer gleich aus, doch der LOADER oder so im bootrecord in der ersten partition kann z.B. ntfs oder ext3 sein

Disketten und Memory-Sticks haben meist keine Partitionstabelle sondern ein superfloppy

Lilo Linux loader, allenfalls Raid Systeme oder LVM, um nativ darauf zu zugreifen
eLILO EFI-Basierte computer
GRUB grand unified Bootloader

5.1.1 Auch boot manager

Verschiedene Kernel Booten (beim neu kompliieren von kernel, falls man aus versehen modul vergisst oder so)
Verschiedene Betriebssysteme starten

5.2 LILO

Greift im Real Mode auf die Festplatte kann direkt block lesen, ohne device treiber, direkt kopf positionieren

1. L Bootsektor wird gelesen
2. I Lilo Maschinencode unter /boot/boot.b (2. Teil des Bootloaders)
3. L Map Datei /boot/map zuteilung der Physikalischen disk zu device /dev/hdax
4. O Begrüssungsnachricht / Menu /boot/message

Nur bis I boot.b konnte nicht geladen
Nur bis L map konnte nicht geladen werden
Bis O, message konnte nicht geladen werden

Lilo muss auf HDA / HDB sein bzw auf SDA / SDB kommt von früher her
Muss bei alten Systemen von bios erreichbar sein sprich in dien ersten 1024 Zylinder

5.2.1 Kernelparameter

Append=kernelparameter

5.2.2 Kernelparameters

init=/bin/bash	ersatz für init
ro	read only, damit fsck disk nicht noch ganz kaputt macht
<runlevel>	Startet in den angegebenen run-level
acpi=off	sehr buggy, acpi bios deaktivieren
vga=normal	Standard VGA Ausgabe (VESA CODE)
selinux=0	SE-Linux wird nicht gestartet

www.linuxwiki.../GRUB

5.2.3 Entfernen

Lilo –u der original bootloader wird zurückgeschrieben

dd if=/dev/zero of=/dev/hda bs=446 count=1	von hand löschen, parttabelle bleibt
xxd –g1 –l 512 /dev/hda1	wie hexdump

5.2.4 Konfiguration

/etc/lilo.conf z.B. bootkennwort
Linux eintrag
Windows eintrag
Default wird erster genommen, timer kann eingerichtet werden

Bei änderung muss der bootloader neu installiert werden
Das heisst bei änderungen an lilo.conf etc muss Im prinzip einfach lilo aufgerufen werden

Backup <datei>
Boot <device>
Delay <zeit>
Message <datei>
Password <code>
Prompt
Timeout <zeit>
vga=<modus> vesa (Normal 80x25, ext 80x50, ask →auswahl)
image=<kernel>
label=name
root=systempartition
initrd=<Datei> initial ramdisk
other=<gerät> z.b. für windows
loader=>Datei> meist /boot/chain.b

5.2.5 Lilo conf

```
boot = /dev/hda
delay = 40
compact
vga = normal
root = /dev/hda1
read-only
image = /zImage-1.5.99
        label = try
image = /zImage-1.0.9
```

```
        label = 1.0.9
image = /tamu/vmlinuz
        label = tamu
        root = /dev/hdb2
        vga = ask
other = /dev/hda3
        label = dos
        table = /dev/hda
```

5.3 GRUB (Grand unified Bootloader) open source

5.3.1 Manual: apt-get install grub-doc,

5.3.2 Teile

1. Teil: 446 Bite grosser bootroutine
2. Umfangreichere Routine die von derster stufe geladen wird
   →er kann mehr intelligenz haben da grösser

Grub versteht direkt verschiedene Filesysteme….

Grundeinstellungen /boot/grub/menu.lst

Default	standart menupunkt
Timeout	warten bis default genommen wird
Title	Betriebssystemeintrag
Kern	bootender kernel

(hd0,1)/boot/vmlinuz	=	hda	2. Partition	sda2
(hd1,1)/boot/vmlinuz	=	hdb	2. Partition	sdb2

(hd0,0): 1.hd 1. partiton

IDE und SCSI gleich

Initrd	gibt den ort der initial ram disk an, wo die Kernelmodule stehen
Root	legt für fremdsysteme die Systempartition fest
Chainloader +1	bezeichnet einen fremden zu laden bootloader
Makeactive	Macht die angesprochene partition temporär bootfähig (windows schreibt so nicht in den mbr beim suspendieren)
Hide, unhide	verstecken einer partition, mehrere windows booten c: → d: → error
Map	Vertauschen der Festplatten

/boot/grub/device.map

Neuinstallation von grub ist nur selten nötig

5.3.3 Installation

grub --batch –device-map=/boot/grub/device.map < /etc/grub.conf

oder

grub-install /dev/hda (bourn-shell script)

→geht in mbr

5.3.4 grubShell> (interaktiv)

grub

Find vmlinuz

Ls –l /boot/grub → Filesysteme

5.3.5 in shell booten (kernelparameter)

init=/bin/bash

Man bootet in den singe-user-mode:

1. beim boot im grup durch drücken der Taste "e" drücken die boot-parameter ändern.
2. den Kernel durch drücken der Taste "e" editieren. (e=editor)
3. beim Kernel hinten den String >>"single init=/bin/bash"<< (ohne Anführungszeichen) einfügen.
4. mit Enter bestätigen
5. durch drücken der Taste "b" booten

Jetzt befindet man sich im single-user-mode mit dem Root-User ohne ein Passwort zu benötigen.

Da die Platte aber read-only gemountet wird kann man das Passwort aber noch nicht ändern.

Um das Passwort zu ändern einfach folgendes eingeben:

1. mount / -o remount,rw
2. passwd
3. mount / -o remount,ro
4. sync
5. reboot

init=startet normalerweise init aber in userem fall startet er /bin/bash

→ zu vorherigem gebild: Rootsystem wird von grub gemountet

dann erübrigt sich die mounterei

5.3.6 Schutz

Grub Passwort
Pro menupunkt passwort möglich

Grub-md5-crypt passwort //dann ins /boot/grub/menu.lst kopieren

oder

Grubshell> md5crypt

Eintrag lock schaltet passwort ein

menu.lst:
password --md5 1.btkh$asdlfkjsadlfkjl

dann beim menupunkt z.b. nach initrd
lock

5.3.7 Showopts

Zeile für parameter

5.3.8 /etc/grub.conf bzw. /boot/menu.lst

Root (hd0,1)
Install /grub/dtage1 d (hd0)(hd0,1) /boot/brub/menu.lst

/grub = / aber davon weiss grub noch nichts
d: disk (f: floppy)

menu liegt auf partition2

View menu.lst

…

5.3.9 2 Varianten

title linux
kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 (hda2 für devicedriver)
initrd (hd0,1)/boot/initrd (minikern mit entsprechenden treiber, wird ins ram kopiert)

kann nur stagefiles laden

title einanderessystem
root (hd0,2)
makeactive
chainloader +1 geht in andere Partition springen (z.B. NTLDR 512Byte)
der startet dann NTLDR.COM, weil linux keine com dateien ausführen kann
+1 = 1. Sektor (kann weggelassen werden)

5.4 Loadlin

Aus dos starten

5.5 NTLDR (NT Loader, alle windows Systeme)

5.6 OpenBIOS

Ersetzt Bios, firmen nicht interessiert am herausgeben des Firmenknowhows, nur kleine community, wäre aber eine gute sache, bereits kleiner linux kern drinn

5.7 Syslinux

Minisysteme

5.8 PXELinux

Ohne menu zum booten ab netz

5.9 BootCamp

Apple boot manager

5.10 Mehrere Bootloader hintereinander

Nennt man chain

6 Systemstart und Systemstopp

Verschiedene Runlevel

In erster bank den langsamsten memory Modul, da bios auf der ersten bank schaut wie schnell dieser ist, und die anderen werden teilweise auch mit dieser geschwindigkeit betrieben

HD's haben heute funktionen die einem die Daten der Festplatte liefern, CHS LBA etc…

6.1 Hardware einrichten

0-640KB LO-Memory (im Realmode ansprechbar)
Startadresse xyz aa55 (wird über memory geblendet) (4KB blöcke)
Ausgeführt und dann steht z.B. standard vga zur verfügung
Früher dipswitches, für adresse
ISA Pnp Hat system die über kommuniziert werden

Heute PCI, 3 pinniges interface (Eprom) auf der Karte

6.2 Bootloader wird hineinkopiert

Im Realmode, sequentieller code, es kann kein prozess überprüfen ob es funktioniert hat.

6.3 Bios stellt Hardware interrupts bereit INT13h

Über die der kleine Bootloader die Festplatte und Tastautr etc. ansprechen kann und so in 416Bytes Platz hat, also mit der benutzung von Software Interrupts.

6.4 System soll nach dem laden des Kernels nicht mehr auf Bios zugreifen!

Prozessor kann einmal von Real mode in den protected mode schalten aber nicht umgekehrt, ausser per langsamem (einige ms) prozessor reset

6.4.1 Softice hängt vor der Interrupt service routine

Ausserdem dürfen diese im realtime system gewisse isr nur gewisse zeit warten,

HD darf nicht reentered ISR abarbeiten, Harddisk hat nur einen Kopf → warten bis dieser Kopf frei ist

6.4.2 64Bit system: 2 Terrabyte addressierbar

6.5 Init-Prozess (PID 1: braucht init-rd)

Damit z.B. disks (raid, scsi) etc angesprochen werden können

/sbin/init
→ ist statisch gelinkt, kann keine librarys laden weil noch kein zugriff auf z.B. HD
→ file → statically linked → Debian hat es dynamisch gelinkt

Es kann kein Signal gesendet werden (^Kill -9) da er kein message queue hat
Hat aber schnitstelle fürs Herunterfahren, aber systemcalls können nicht mit init prozess kommunizieren.

ps –ef | head

1 Init [5] //5 ist runlevel //debian meint init [2]

Ksoftirqd/0 //software interrupts
Ksoftirqd/1 //software interrupts des 2. Prozessors

Kblockd/0 //blockdeamon

6.5.1 Verwaltet startup scripts

Siehe /etc/inittab

6.5.2 Anmeldung auf virtuellen / hardware konsole

6.5.3 Einstellungen /etc/inittab

Parameterzeile von Bootloader wird an init prozess übergeben

Standard runlevel
Id:5:initdefault

Erstes auszuführendes skript
si::bootwait:/etc/init.d/boot //bei debian: si::sysinit:/etc/init.d/rcS

Linux Standard Base definiert das aber redhat hat noch /etc/rc.d/init.d/boot
LSBS

Zuerst wir
Proc
tempfs
gemountet…

6.5.4 Boot.d

/etc/init.d/boot.d vor runlevel steuerung
Scripte mit boot.xyz werden da gestartet

6.5.5 Runlevel

Boot
Runlevel 0: System.Halt
Runlevel 1, bzw Runlevel S : Einbenutzermodus ohne Netzwerk
Suse: runlevel s anders als 1: keine gemountet fs ausser tempfs
→Root fs fsck machen können
Runlevel 2: Mehrbenutzermodus ohne Netzwerk
Runlevel 3: Mehrbenutzermodus mit Netzwerk → standard runlevel für server
Runlevel 4: unbenütz, kann individuell konfiguriert werden, z.B. zum Datenbanken Schliessen per runlevel
→ ins 3: system noch verfügbar aber ohne datenbank
Runlevel 5 : Mehrbenutzermodus mit Netzwerk und grafischer Anmeldung
Runlevel 6: reboot

6.5.6 Runlevel 3 z.B. wenn man keine Grafikkarte hat.

Und per serial zugreift…

6.5.7 /Init.d/rc

Runlevel Steuerung, Es gibt auch ein rc.local

6.5.8 Insserv (suse)

Chkconfig, Nfs braucht protmapper

6.5.9 Runlevel

Abfrage des runlevels
`runlevel`
N 5

N: alter runlevel, none
5: aktueller runlevel

S: Start -> script.sh start parameter durch init gesendent
K: Kill -> script.sh stop

syslog restart system logfile: var/messages

rc4.d/S05network
sh network
./network stop

6.5.10 Nomchine.org (vnc like Applikation)

http://www.nomachine.com/

6.5.11 touch /etc/nologin

so kann man backup machen und niemand mehr mehr einloggen (Remotebenutzer, lokal einloggen geht)

6.5.12 Boot.local

Wird nach boot init // bei Debian müsste das /etc/init.d/rc.local sein.

7 Prozessverwaltung

Gestoppter Prozess muss immer noch message queue verwalten können

Die meisten grösseren Programme arbeiten heute mit Threads
→ wird von libraries zur verfügung gestellt

Prozesskontext:
Programm hat Header, was muss gemacht machen

Programmtext
Daten
Systeminformationen
- PID (init hat 1)
- Aktuelles Verzeichnis
- (userbezogenes Filesysteme)
- Umask (init-prozess hat 666)
- Prozessumgebung mit Variablen (environment variabeln)
  - Beim booten wird so kernelparameter übergeben, können nachträglich wieder Auslesen

Verlieren Kind prozesse ihre eltern, werden sie entweder gelöscht oder weiter nach oben gehängt

Multiprozessing muss gehandelt werden. Nicht parallele prozesse von einander abhängig → andere kerne, anderes Task Schedulling, ab frühling kein singelprozessor kernel mehr
→ nur noch eine Kernelversion testen

Prozess muss definierten zustand haben

Runnable (R)	läuft oder wird grad als nächster genommen Es ist auf einem Singelprozessor sein, dass man 2 Runnable Sieht, der der läuft und der der gleich dran kommt
Sleeping (S)	
Defunc (Z) (Zomby)	Prozess der nicht mehr funktioniert, kein parent prozess mehr Oder weil message queue nicht mehr funktioneirt Prozess ohne parent, kann auch keine Prozesszeit mehr Anfordern, ist tod, kann nie mehr laufen.
Stopped (T)	Modem das auf ring wartet, oder prozesse der mit ctrl-z oder mit kill gestoppt wird trägt sich in eine interrupt tabelle ein, es wird nur noch messagequeue abgefragt aber kein code mehr ausgefürht → wird allenfalls in swap ausgelagert
+	ist in den Speicher geladen, kommen als nächstes dran
s	kleines s zum swappen
N	nice grösser 0
<	kleiner nice wert

Ctrl-Z: haltet genau dort wo er gestoppt wird: Prozess Counter, etc wird gespeichert

Timeslots:
- Musiksystem muss anderes Taskswitching haben, → kürzere timeslotz, nicht 5 sondern 1 ms

oder: Realtime nur ein prozess dem genügend rechenzeit gewährt wird
- z.B. früher 5000x pro sekunde am zug

darf nicht auf z.B. IO warten sonst alles für die Katze

7.1 /proc

Ein Linux prozess schreibt alles in sein proc, Windows schreibt alles in eine Datenstruktur → lesen bei Windows komplizierter.

Macht grossen Prozess aber langsam, da das proc geschrieben werden muss… allenfalls wird das dann auch gelöscht, früher gab es kein proc, man musste informationen mit debugger holen

7.1.1 ps

ps	gibt nur aktuelle shell an
ps –p$$	erstes $ einleitung für Variabel. 2. $ die variabel $ (eigener prozess qed)
ps –p	full information
ps –e	alle Prozesse (oder auch –A)
ps –x	extendet: alle prozesse anzeigen (BSD Syntax)
ps –ejH	hierarchisch
ps –em	threads
ps –p	mit prozessnummer
ps –mp 2999	threads auf einem prozess (tread kann im src benannt werden)
ps –C	

ps –o eid,rid,tty,pid,ppid,state,cmd,**nice**
→man ps /ppid (teilweise gleich wie kopfzeile)

Pstree –H $(ps –C ssh-agent –o pid=) **MÖGLCIHE PRÜFUNGSFRAGE→pgrep**
Kill $(ps –o PID)

Threadinformationen steht im environment des Prozesses
z.B. Java läuft in einem Thread auf firefox → gutes Beisiel

7.1.2 top

Braucht sizing des terminals.
Load

Loadaverage: aktuell, Letzte minute, letzte 5 minute

→Nachos, alarmierungs tool suchen, anschauen

http://www.nagios.org/

B: bold

SHR shadow memory = swap
RES: reservierter speicher

7.1.3 pstree

-a Argumente anzeigen
-h/H zeigt einen Prozess markiert
-p zeigt PID
-u Zeigt Besitzerwechsel
-A/G benutz Ascii/Terminal-Grafik

7.1.4 kill

default signal: TERMINATE
kill –STOP programm entspricht ctrl-z
→ kann kein signal ausser continue im queue verarbeiten
fg schickt kill –CONT prozess
kill –TERMINATE programm entspricht ctrl-c

Weitere nützliche Befehle

7.1.5 killall

7.1.6 pkill

7.1.7 pgrep

7.1.8 jobs

7.1.9 xeyes

7.1.10 nice

-20 bis +19 negativer nicewert erhöht Priorität
Standard ist +10

7.1.11 renice

Priorität von alufendem programm verändern

7.1.12 ulimit (user limit)

zum testen
resourcenzuteilung für subprozesse, bash
man 3 ulimit ← API → **man bash-builtins /ulimit**

-a anzeige
-d schränkt die maximale grösse des datensegmentes eines prozesses ein
-r Schriänkt dateigrösse ein (nur ext2)
-n beschränkt die anzahl offener datein
-t schränkt die verfügbare cpu zeit ein
-u begrenzt die anzahl der prozesse
-v begrenzt den virutellen Speicher
-p Pipes, VORSICHT Standard auf 8 pipes
-s Stack VORSICHT Std 8MB, segmentation fault→shell beendet→keine Meldung

ulimit = ulimit –f

ulimit –f 20
dd if=/dev/zero of=f1 count=41
→File size limit exceeded

früher wurden Prozesse der reihe nach nummeriert, doch ist das durchschaubar für hacker

7.1.13 Scheduller prozess der thread von init ist weist zeit zu

Kann nicht gekillt werden
Hält sich an bestimmte regeln, lässt sich beim compilieren vom kernel eingestellt werden
-normal
-realtime

Interaktive prozesse erhalten mehr rechenzeit: Mausabfrage etc…
Will man z.B. grosses numbercrunshing machen muss man den prozessor so kompilieren, Netz langsamer, aber wenn er am rechnen ist muss er rechen, io prozesse weniger Priorität, aber vorsicht kann is straucheln kommen

7.1.14 /proc/PID/maps

Zeiger auf library

Reentered library für mehrere prozesse gleich

P pointer für einstiegspunkt
S stack

→ wo kann man stack overflow machen???

7.1.15 /proc/PID/environ

Environment

7.1.16 *.so (Static object)

7.1.17 Nohup

Veranlasst das betreffende program das signal sighup (signal hangup) zu ignorieren
Sighup wird an alle kindprozesse geschickt. **Man kann etwas machen und später dann schauen was gemacht wurde**

Macht nohup.out wo die Standardfehlerausgabe abgelegt wird, im aktuellens verz. ausser keine schreibrechte → home des users

xeyes & → kriegt keine sighup (bei älteren UX wird es noch geschickt)
→ gekillt bekommt parentID 1
→Würde defunct (zomby)

Kill -9 schickt kein hup mehr

7.1.18 Initprozess hat je nach distro eine konsole

Ctrl-alt-F9

8 Systemprotokollierung

Fleissiger admin liest diese Logfile

Vollzug einer Aufgabe
Fehlersituationen
- CRC
- Beschreiben eines speichers fehlgeschlagen
- Harddisk probleme

Warnungen

8.1.1 Xconsole

Kleines Terminal wo x11 hintergrund prozesse hinein schreiben

```
xconsole &
```

8.2 Syslog-Daemon

Veraltet, recht rudimentär, für erste mailserver gedacht, sendmail,
Schnittstelle zu systemlogfile
- → Socket /dev/log

Verbindungsloses netzwerkinterface → keine überprüfung → syslogNG

Cat datei | /dev/log VORSICHT

8.2.1 SyslogNG (apt-get install syslog-ng)

Syslogng → verbindungslos, verschlüsselt

Filter vielen funktionen: not, match,
match(„IN=“) and not match („OUT=“)

Facility(local0, local1….)

Destination console { pipe(„/dev/tty10“ owner(-1) gropu(-1) perm(-1))};

komplzierter

8.2.2 SyslogPE (premium eddition)

Kostenpflichtig, mit buffer, wo bestimmte anzahl messages zwischengespeichert werden kann ohne den ganzen socket zu blockieren, wenn z.B. jemand den Syslog server ddos

8.2.3 /etc/syslog.conf

```
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

# Logging for INN news system
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice

#
# Some `catch-all' logfiles.
#
*.=debug;\
        auth,authpriv.none;\
        news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         *

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;\
#       news.=crit;news.=err;news.=notice;\
#       *.=debug;*.=info;\
#       *.=notice;*.=warn       /dev/tty8

# The named pipe /dev/xconsole is for the `xconsole' utility.  To use it,
# you must invoke `xconsole' with the `-file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
# NOTE: adjust the list below, or you'll go crazy if you have a reasonably
#      busy site..
#
daemon.*;mail.*;\
        news.crit;news.err;news.notice;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole
```

Für syslogd oder syslogng, man syslog.conf → dort findet man die Kathegorien

Links: was geloggt werden soll, rechts: wohin loggen

kern.none Kathegorie Kern wird nicht in diese Datei / Device geloggt
mail.* alle mail meldungen speichern
Autpriv Vertrauliche Meldungen der Sicherheitsdienste

C programm z.B. ins local[0-7] schreiben, unterscheidbar

Prioritäten
None
Debug
INFOBRIEF notice
Warning
Err
Alert
Emerg letzte meldung vor dem absturtz

<kategorie>.<Priorität>[;<kategorie>.<priorität>

*: alles (platzhalter)
Mail.info alle meldungen des Mail-daemon mit Priorität info und höher
Mail.=info nur mledungen dieser Priorität
Mail.!info alles ausser info und höher
Mail.!=info alles ausser info

- Minus bedeutet, das nicht sofort ein sync gemacht wird, nicht direkt auf hd, kann sein, dass halbe minute nichts in syslog geschrieben wird

Datei dateiname mit absolutem pfad
| FIFO pipe
@ über das netz an eine anderen syslogd im netz schicken
Direkt auf device /dev/tty10 schreiben
User an user schicken
* an alle user schicken **<** *.emerg ***** **>**

Mail.none keine messages vom mail

Syslogd Stop
Syslogd start
Syslogd restart
kill –HUP <syslogd> oder kill –HUP $(pgrep syslogd)

8.2.4 Änderungen

/etc/syslog.conf anpassen, speichern
sudo kill –HUP $(pgrep syslogd)
log ansehen

8.2.5 Logger –p local0.err –t TEST “Hallo Welt”

Logger –p local0.err –t TEST “Hallo Welt”
p: priorität
t: Prozess ; Text….
U: direkt an sockent, z.B. /var/log

su login failure anzeigen… → /var/log/auth.log

8.2.6 Auf externen server loggen

. -@192.168.2.1

8.2.7 Logsurfer (log auswertung)

8.2.8 kKsystemlog

8.2.9 Kwatch

8.2.10 Kiwi

8.2.11 Logviewer

8.2.12 Swatch, logsurver (DFN-CERT)

8.2.13 xLogMaster (log auswertung)

8.2.14 Tivoli (log auswertung, grosses managementsystem von ibm)

Verbindungsfehler mit mail
Verbindungsaufbauzeit
etc…

6 monate aufbewahrungspflicht für mails an FH

Da syslogd mit handle auf datei arbeitet, kann die datei umbenannt werden → HUP schicken → neue log wird erstellt.

8.3 Logrotate (man logrotate)

konfigurationsbeispiele in: **/etc/logrotate.d** ganzes verzeichnis wird abgearbeitet

in **/etc/logrotate.conf** sind default werte angegeben.
ist kein daemon sondern wird von cron regelmässig gestartet

8.3.1 Infos zu logrotate

whereis logrotate
which logrotate
file $(sudo which logrotate)
ldd $(sudo which logrotate)

libpopt.so.0 /lob/lobpopt.so.0 (0xb7ee3000)
shared lobrary (so) wo im speicher

(.o) gegenteil von (.so) nicht shared

8.3.2 Konfigurationsdateien

dateext: hängt datum als erweiterung an

maxage 365

rotate 99 max 99 files

size 1024k maximale grösse

compress: komprimieren (es lässt sihc noch angeben welchen algorithmus)

notifempty es wird keine leere datei komprimiert

missingok logrotate prozess gibt keine fehlermeldung aus

postrotate oder prerotate
mailx …….. siehe unten…
/etc/init-d/syslog reload
endscript

8.3.3 MAILX

mailx –s „Logrotate gemacht“ marc.landolt@ml.ch </var/log/messages

-s subject

→ aber besser ein script machen, dass sich die Daten selber holt, dann muss man nicht an diversen orten mailadressen angeben

8.4 Crontab → kommt später

Crontab –l
L: list

8.4.1 cat /etc/crontab

8.5 dmesg

Ringpuffer anschauen (kernelparameter)
Messages vom kernel wenn syslog noch nicht läuft

Wird ausgelesen und in syslog übertragen, via socket /proc/kmsg

8.6 UUCP

Unix to Unix copy, vor 10 jahren gestorben

9 Datensicherung und Archivierung

Aufgabe des Admins (backup administrators)

Gründe
- Versehentliches Löschen (nicht primär sinn des Backups)
- Hardwarefehler
- Fehler des Betriebssystems
- Viren (defacing)

Medien
- Kopie auf anderes Dateisystem / Disk
- Externe Festplatte
- CD/DVD Medien
- Bandlaufwerke (Billigstes)

Gretchenfrage, wie sichert man das 18TB SAN der FHNW?
Raid kann allenfalls die beim wiederherstellen was falsch laufen, also braucht man ein backup!

Arten von sicherung
- Online Sicherung (continuous)
  - Wichtiger datenbestand sofort sichern
    - Vorsicht, dantenbanken etc inkonsisten, →snapshot
- Offlien sicherung
  - Sicherung zur zeit der geringster **Systemauslastung**, im Runlevel 1

Bänder übertragen magnetfeld auf 1 lage + / - → müssen nach einer bestimmten anzahl monate / jahre refrashen

Methoden
- Fullbackup
- Fullbackup + inkremental (1x pro woche full, am wochenende)
  a) Incrementierung seit letzer full = differetial
  b) Incrementierung selt letzer incrementierung

AUSTESTEN:
- Desaster recovery durchspielen, auf anderes system zurückspielen
- Logdateien beachten

9.1 Bandlaufwerke

Ausführung der Bandlaufwerke:
Teurer schrieben zwischendurch checksummen, ist eine stelle am band defekt, fehlt nur ein block, bei billigen ist der ganze datenbestand nach dem Fehler verloren

Bandlaufwerke sind character device
Heute kein rotierender kopf mehr, Gewisse LTO64 haben bis zu 128 Spuren
Schrägköpfe können anderen winkel haben → man kann im falle eines defekten laufwerks alte bänder nicht mehr lesen

Alle bandlaufwerke als scsi angesprochen

9.1.1 Rewinding device /dev/st0 (scsi tape 0)

DLT, LTO, die zweite Rolle im gerät selber

9.1.2 Non-rewinding device /dev/nst0 (non revinding scsi tape 1)

Man kann von da her einen 2. stream weiterschrieben

a-f /dev/nst0a

Man page von device je nach buchstabe noch z.b. kompression eingeschaltet

9.1.3 Am ende EOF

Wenn mehrere „Dateien“ auf Band , dann hat es am schluss zwei EOF

9.2 Bander Managen

9.2.1 mt (magnetic tape)

mt –f /dev/nst0 fsf 1 //std: /dev/tape → link machen

f: laufwerk angeben
fsf 1: forward skip file, spult bis zur endmarke des 1. filesets
→ Kathalog (z.b. 16. fileset sind homedaten fsf 15)
eof, weof: schreibt EOF-MARKE
bsf n: spult n Dateinen zurück
asf n: Absolute positionierung
eom: ende des beschriebenen bandes (eof eof)
rewind: zurückspulen
status: wo steht kopf?
erase: löscht band
offline, wirft aus
rewofflind: spuhlt zurück und wirft das band aus

9.2.2 über netzwerk (unverschlüsselt über remoteShell)

hugo@tapeserver.examloe.com:/dev/nst1
→mit cronjob auf backup server schicken

9.2.3 über ssh

mt –rsh-command=ssh oder Environment Variabel MT_RSH=ssh

9.2.4 Sichern im netz

Kommerziell
IBM Tivoli Sorage Manager
Legato
Backup EXEC
Open source
Amanda
Bacula
Rsync (speiegeung von daten)
Daten die gelöschen werden erst nach bestimmter zeit löschen (z.B. 1 Woche)
→ kitchensync zusatzmodul

9.2.5 tar (tape archive)

kommt aus zeit als es noch keine festplatten gab

heutige verwendung: Verzeichnisbaum komplett in eine Datei kopieren

tar <optionen> <Datei> ¦<verzeichnis>
sichert auch attribute

-c create
-f <Datei> erzeugt oder liest ein Archif aus <Datei> Kann auch gerät sein
-t test, zeigt den Inhalt des Archivs
-v ausführlicher Modus, verbose
-x auslesen der gespeicherten dateien
-z komprimiert mit gzip (auch mit neuerem winzip)
-j komprimiert mit bzip2 (bessere komprimierung, source verbreitung)

Standardmässig Relative pfadnamen

tar –cvf ~/data.tar data* alle dateien die mit data beginnen
cd /; tar –cvf home.tar /home früher gab es ohne cd endlosschlaufe
weil tar sich selber eintart, heute max 16x
tar –tvf home.tar
tar –cvf root@archiv:/dev/tape data* --rsh-command=ssh

9.2.6 Kopiert ganzes root filesystem (wie unter windows xcopy)

tar –cf - / | (cd /mnt; (cd /mnt; tar –xf -)
- heisst console
tar geht normalerweise nicht über mountpoints
( ) klammer erlaubt mehrere befehle aufs mal
CRC pro block, nach fehler kann nicht mehr gelesen werden
alternativ cp -r aber bekäme datumswerte und umask → rechte würden nicht kopiert
tar speichert auch datum und stellt dies wieder zurück

Tar löscht leading /
Also muss ich wenn ich absolut einttaren will ins home wechseln

Bzip tbz tar –j…
gzip tgz tar –z…

9.2.7 datei paken:

tar cvf verteichnis.tar vertechnis.txt
touch datei{1..3}
tar rvf verzeichnis.tar *.txt //anhängen

tar tvf verzeichnis.tar //anzeigen

gzip verzeichnis.tar

9.2.8 zcat verzeichnis.tar.gz ¦ more

9.2.9 zgrep

9.3 CPIO

Cpio-Archive sind ähnlich den tar-Archiven, kann beim eingang und ausgang formate angeben
-old ASCII, new ASCII
HPUX binary, HPUX old ASCII
Etc…

Effizienter als tar
Fehlerhafte stellen werden übersürungen
Braucht standard in und standard out
Option –depth
Es kann mit regulären ausdrücken gefiltert werden

cpio -o output
cpio -i input
cpio -p konvertieren

find / -maxdepth 1 –name '*' | cpio –ov >data-all
>> anhängen auch möglich

cpio –iv <data-all

9.4 Dump

Sichert ganzes FIlesystem
-Dump greift direkt auf dateisysteme zu
+eignet sich für incremental / differential
-sei russisches roulette (Liest inodes etc…)
→FS sollte unmounted sein oder zumindest read only
Es gibt dumps die mehrmals einliest, so dass keine inkosistenzen entstehen sollten

Touch /etc/dumpdates

Dump -<Stufe> -f <Laufwerk> <Dateisystem>

Dump -0 –f /dev/st0 /home

0 full
1 incremental -→ langsam
2 differential
Bis 9 man dump (zuvor: sudo apt-get install dump)

9.4.1 Auspacken mit Restore

restore –i –f /dev/st0

i: interaktiver mode
befehle: cd, ls, add, delete oder extract

automatisches restore
restore –rf /dev/st0

9.5 Partitionen sichern mit dd

Eignet sich für schnelles disasterrecovery

Dd if=/data/sda of=/dev/sdb
Die platten müssen die gleiche archithektur haben
Of kann grösser sein

Verweis iso mount loop

gpartimage, partimage wie dd liest aber nur gebrauchte blöcke
zum disk copieren, partitionen verändern…. Open src version sehr langsam

9.6 Erster komprimieren kostenpflichtig

Compress macht .Z datein
Zgrep
Zcat
Uncompress

9.7 Gzip

GNUzip .gz
Meherere dateien komprimieren tar und gzip kombiniert
gunzip

10 Zeitgesteuerte Vorgänge cron und at

10.1 At zu einem Zukünftigen zeitpunkt ausfüren

10.1.1 at (at time)

Mail Abwesenheitsmeldungen ein und ausschalten
Erinnerungsmail zu bestimmter zeit versenden
tTimer

at ist interaktiv

at 01:00 [today | tomorrow] [TT.MM.JJ|Monatsname Tag Jahr]

at> tar cvzf /dev/s50 $HOME
at> echo “Backup fertig” | mail –s Backup $USER
at> [Ctrl] [d] (=end of text / end of file)

Job 123 at 2003-11-08 01:00

at now + 5minutes
at now + 2 days
at noon + 2 hours

Umgebungsvariabeln werden vom absendenden Benutzer genommen und im Job gespeichert
AT gib keine rückmeldung, → mail machen im job oder syslog

10.1.2 atq (at –l)

gibt queue an

123	2003-11-08	01:00	a	hugo
			At job (jobklassifikation)	
123	2003-11-08	01:00	b	hugo
			Batch job (jobklassifikation)	
			z	wird mit sehr tiefer Priorität gestartet

10.1.3 atrm

job löschen

10.1.4 /etc/at-allow

10.1.5 /etc/at-deny

Gibt es beides gilt at-allow und deny wird gar nicht betrachtet…

10.1.6 Ausgabe

Gibt es ausgabe wie echo Hallo welt kommt das per mail, wenn es keine ausgabe gibt, wie z.B. echo Hallo Wellt Hallo.txt dann wird nichts gemailt. Folglich muss man mail explizit angeben

10.1.7 /var/spool/atjobs debian: /var/spool/cron/atjobs

a002003240 datei von at normales shellscript
b320952935 datei von batch normales shellscript
r…… ist at oder batch mit option –q

Prioritäten Reihenfolge
a b c d e … z
= bedeutet ist im moment am laufen

10.1.8 Atd

-b batch
-l load

Deamon

At deamon wird jede minute einmal aufgerufen.

Syntax der Bornshell

10.1.9 batch … details?

zu nächstmöglichen Zeitpunkt

z.B. Mail oder Printserver
um mituten oder sogar stunden verzögert

10.2 Cron Periodisch an bestimtent Tag / Monat … auführen

Logfiles rotieren
Temp Verzeichnis aufräumen

Deamon: crond

Ruft corntab in bestimmtem zeitinterval auf je nach einstellung alle minute
Verwendet Born-Shell (/bin/sh)
→ man nimmt am besten ein script mit dem

#!/bin/bash
#!/bin/perl
#!/bin/awk
#!/bin/php5

Wird vom einem Init-script gestartet

Aufgabenliste Crontab

Crondeamon loggt im prinzip mit dem environment des Absetzenden benutzers ein

10.2.1 Crontab man 5 crontab

Minuten	Stunden	Tag	Monat	wochentag
0-59	0-23	1-31	(1-12)	0-7
17	*	*	*	* bedeutet irgendwann

58	19	*	*	*	echo „gleich ist es 20 Uhr“
0,30	*	*	*	*	echo es ist punkt oder halb
0-59/10 */10		*	*	*	alle 10 minuten
1	0	13	*	5	Ver-ODERt jedem Freitag und jedem 13.

10	0	*	*	*	marc echo unter user marc ausgeführt mit rechten und env.

Es können auch englische namen verwendet werden. January

10.2.2 /etc/cron.d

Jobs hier drinn werden ausgeführt

10.2.3 %

Zeilentrenner → braucht man ein % zeichen muss man es escapen \%

10.2.4 -10 1 * * * /usr/bin/shell-script

Minuszeichen unterdrückt die ausgabe in den syslog im fehlerfalle

10.2.5 SHELL=/bin/bash

In crontab eintragen → dann läuft alles was cron startet in bash

10.2.6 >/dev/null 2>&1

so wird beides in dev null umgeleitet und es gibt kein mail

10.2.7 MAILTO=“ “ man 5 crontab

10.2.8 * * 13 * * * If (wochentag==5) && reboot….

Immer am Freitag den 13. etwas ausführen

10.2.9 Vorgehen

Offline script machen und dies dann wenn ausgetestet von Cron starten lassen

10.2.10 Cron.allow

Schliesst cron.deny aus
user die dürfen

10.2.11 Cron.deny

User die explizit nicht dürfen

crontab –e	crontab editieren $EDITOR $VISUAL wird genommen, erstellt pro user eine
crontab –l	zeigt crontab auf der konsole
crontab –r	löscht crontab des benutzers der eingeloggt ist

11 Hardware und Rechnerarchitekur

Linux bringt von haus aus relativ viel mit, Grosser overhead für den Kernel, was man gar nicht bräuchte.

Robust und Schlank → Kernel selber Kompilieren ohne overhead

Linux unterstützt verschiedene Mikroprozessoren

Bedingte Compilierung → Je nach Mikroprozessor und Busbreite

11.1.1 North Bridge

Verbindung CPU (Cache) ←→ Hauptspeier

11.1.2 South Bridge

Verbindung CPU ←→ IO → Bus, pci, pcmcia….
IDE
SCSI (Eigene Karte)
SATA

REST IN PEACE
Parallel, Seriell, Tastatur und Mausanschluss, heutige Mainboards haben sie nicht mehr

Nach dem laden des Bootloaders schaltet der CPU in den Protected mode

OpenBIOS.org → ESI = Enhanced Start Image → schnellerer start
Hardware so initialisieren dass man sie gleich brauchen kann
Bios löschen
NV-RAM
Systemur 64Byte speicher batteriegestützt
Nach falshen des biosses muss NV Ram gelöscht werden, da dies nicht mehr passt…

11.2 Motherboeard

Formfaktoren ändern alle paar jahre
DELL hat z.B. nicht kompatible fromfaktor standards

Zero Force Socke für prozessor auch meist am gleichen ort
Heute über 900 Pin

11.2.1 Memory

In der nähe des Prozessors

11.2.2 Spannungswandler

Mit kühlkörper, da prozessor sehr kleine Spannungen braucht

Mehrere Ampere bis mehrere 10 Ampere von Strom
Luft des prozessorkühler kühlt auch spannungswandler, luft wird von oben herab gedrückt

Pin 1 und Pin 100 der PCI karte muss gleich lange zuleitungen haben wenn cpu alles handelt

11.2.3 Chipsatz

Rückwertskompatibel, sonst brächte man ein NT nie mehr zum laufen

11.2.4 Bus

ISA: 8Mhz 8/16 Bit
Absolut keine konfiguration über bios → Jumper
Plug and play configurationen: /etc/modules.conf

EISA: 32 Bit
Per bios konfigurierbar

MCA (Microchannel)
10Mhz von IBM, wollte lizenz, niemand hat das unterstützt, nach einem jahr weg vom markt

PCI Bus (1990er Jahre) **[ist im prinzip hotplugable]**
32 bis 64 bit 33 bzw 66 Mhz übertragungsgeschwindigkeit
→ 100 MBit Karten, Grafikkarten
Heute bis 133Mhz bei 64 bit → viele daten
Hardware erkennung
→ jeder der Hardware entwickelt muss code entwickeln (Für markt) muss id beantragen
→ es gibt einige freie für laborzwecke
Karte am nächsten bei proz. Habe höchste Priorität ←
→ IRQ

AGB Bus
→ da pci zu langsam für video nicht über north bridge sondern direkt am prozessor dran
FAN-OUT 1 des Prozessors →

PCI-Express
Ausgeklügeltes Bussystem
Teilweise serieller buss
PCI-e serielle übertragung mit sehr hohen Taktraten

PCI-8 teil paralel teil seriell → kompelxität zwischen paralleler und selrieller daten

PCI-16 grosser teil Paralell → einfacher zu handhaben
→4fach gigabit karte
→CPU erweiterungen → Blade Server
Mehrere Prozessoren über buss anstecken

11.3 LSPCI

Lspci –v Detailierte informationen
Lspci –t Hierarchische darstellung
Lspci –n Klassen anzeige, klasse sagt was für ein typ gerät
Daten in form einer Klasse abgelegt

→ auch sichtbar in /proc/bus/pci
→für jeden bus ein verzeichnis angelegt
→dann z.B. geräte

00: Busnummer, ID Nummer
01. slot nummer
3 funktionsnummer

Bei notebook onboard z.B. Netzwerkkarte in direkten hardware
Und z.B. mini PCI
→modem, wireless

11.4 Meldearten

11.4.1 interrupt

Interrupt: Karte kann sich melden, wenn sie den bus will
→ karte einstecken, sie fordert per interrupt die inizialisierung an ….

11.4.2 IO adressierung, nicht so breit wie bus

11.4.3 Karten die direkt raum im speicherbereich belegen

11.4.4 DMA (früher, ISA)

Grafikkarte mit DMA? Vidoeram ←→ Ram
PCI hat kein DMA, autsch…

PCI bus arbeitet mit shared memory

DMA langsam weil über IO bus daten geladen wird
→ IO Bus leitungen länger → langsamer
→ via north bridge, die nahe am ram liegt

Northbridge soll scheinbar die MMU ersetzen

11.4.5 Busmastering

→ Karte sagt: ich hätte gern den bus

	IRQ und	IO Ports
COM 1	IRQ4 ttyS0	0x03f8
LPT1 IRQ	IRQ7 lp0	0x0378

REST IN PEACE

11.4.6 IRQ (Priorität der reihe nach)

IRQ 0	Timer (Waiting, Prozess schedulling)
IRQ 1:	Keyboard
IRQ 2:	Kaskade -→IRQ 8-16

USB-Keyboard → Netzwerkhat allenfalls höhere priorität, dDOS → keine zugriff mehr????

11.4.7 Adressen

Cat /proc/ioprits

0000-001f: dma1
0020-003f:pic1

Heute per pci Dynamisch

11.4.8 /proc/interrupts (IRQ)

Pro Kern ein interrupt counter

11.4.9 ISR

Prozessor hat für jeden irq einen Specherbereich wo die Sprungadresse hingeschrieben wird
Pointer tabelle fix vom Prozessor gegeben

ISR muss so programmiert werden, dass sie reentered ist, also für jeden aufruf einen eigenen stackpointer

11.5 OSS (Open Sound System)

Sndconfig

11.6 ALSA (Advanced Linux Sound Architecture)

11.6.1 Alsaconf (alsatools)

Mit userinterface

11.6.2 Alsamixer

11.6.3 Aplay

Aplay /usr/share/sounds/alsa/test.wav

11.6.4 Arecord

-Bietet möglichkeiten für plugins für soundkarte
-auch mehrere soundkarten möglich

11.6.5 Soundkartenmodulierung als Modemkarte nutzbar

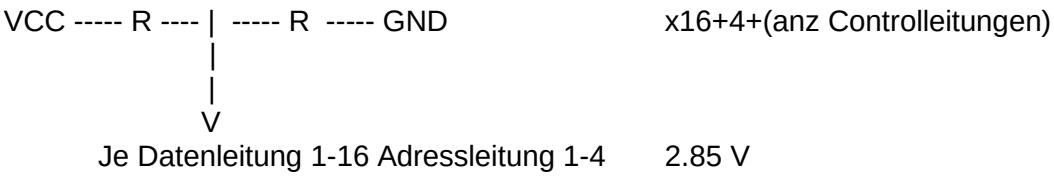
11.7 SCSI (8 und 16 bit / 3 bzw 4 adressleitungen)

Meistens eigener kontroller mit prozessor, crc bei raid 5
SATA muss der Prozessor IO organisieren, spührbar zu scsi
Verschiedene systeme, andere physikalische parameter, teilweise abwärtskompatibel

Controller ist auch ein gerät

Früher 50 Pin, davon jede zweite Masse gegen crosstalk

Jeder Scsi bus relativ niederohmig terminiert



Komplett in einem IC

Später mit feldeffekttransostoren statt R

11.7.1 Singelended

Spannung gegen masse
0 und 1 als signal

11.7.2 Low Voltage Diferential (LVD)

2 Schmitt-Trigger

Reagiert auf änderungen

11.7.3 High Voltage Differential

30V
20-30 Meter Kabel damit Taperoboter extern angeschlossen werden kann wegen rauch entwicklung im brandfall → Bänder würden zerstört

11.7.4 SAS (Seriell atached scsi)

(Nas/SAN) per glasfaser anschliessbar

11.8 Linux SCSI

1 Treiber für SCSI Hostadapter (Früher DMA) → hier allenfalls ATA/USB… treiber
2 Eine generische „Mittelschicht“ Hier greift das Betriebssystem zu
3 Treiber für verschiedene Geräte
- Platten
- Bandlaufwerk
- Scanner
- CD-ROM

11.8.1 Nummerierung

Host/Channel/ID/LUN
LUN=welcher arm auf der Platte oder im Tape Roboter

/dev/sda
/proc/scsi/…
…devices

11.8.2 Booten ab SCSI

Zuerst wird DIE genommen
Dann SATA
Dann SCSI

11.9 USB (im gegensatz zu firewire nicht differenziell)

Entwickelt für Maus und Tastatur und paralleler Drucker
Umstecken im Leufenden Betrieb

11.9.1 Max geräte: 127

Theoretische Werte → es geht was für header verloren

USB 1:1	1,5 MBit/s 12 MBIT/s	(Verdrillt)
USB 2.0	480 MBit/s	(Geschirmt)
USB 3.0	(Frühling 2008 soll verabschiedet werden, Herbst 2008 erste Geräte) Soll auch optischen Anschluss haben, noch nicht definitiv Aber billiger als Netzwerkequipment	

Flankensteilheit

11.9.2 Geschwindigkeit bei mehreren geräten

Halo Paket, wenn geräte langsam ist muss der Bus warten
Geräte auf die USB anschlüsse des Mainboards verteilen

11.9.3 üBERTRAGUNGSSYSTEM

Colision Detection

11.9.4 Deskriptor

Jedes gerät gehört zu einer klasse, klassen können unterklassen haben

11.9.5 Erstes gerät das eingesteckt wird hat höchste Priorität

11.9.6 Cat /proc/pci

11.9.7 Absicherung

Termosicherungen oder manchmal auch Schmelzsicherungen
5V / 500mA

Externe Disk Probleme beim Anlaufstrom: 3.5“ etwa 2-5 A

11.9.8 Controller interface

OHCI Compaq (viel knowhow im chip) REST IN PEACE
Open Host Controller Interface, können direkt auf memory zugreifen

UHCI das Knowhow ist im Treiber

11.9.9 Kern sieht auch bei mehreren Hosts nur einen

11.9.10 Kernelmodule

Usbcore.o
Uhci.o usb-uhci.o oder usb.ohci.o
Ehci-hdc.o (nur usb2.0)
Dann geräte
Usb_storage.o, usbserial.o

11.9.11 Treiber anzeigen

lsmod

Insmod later
Rmmod later

11.9.12 USBFS

/proc/bus/usb
In fstab ersichtlich

11.9.13 USBVIEW

Grafische darstellung der USB geräte, geht nur mit /proc/bus/usb/device

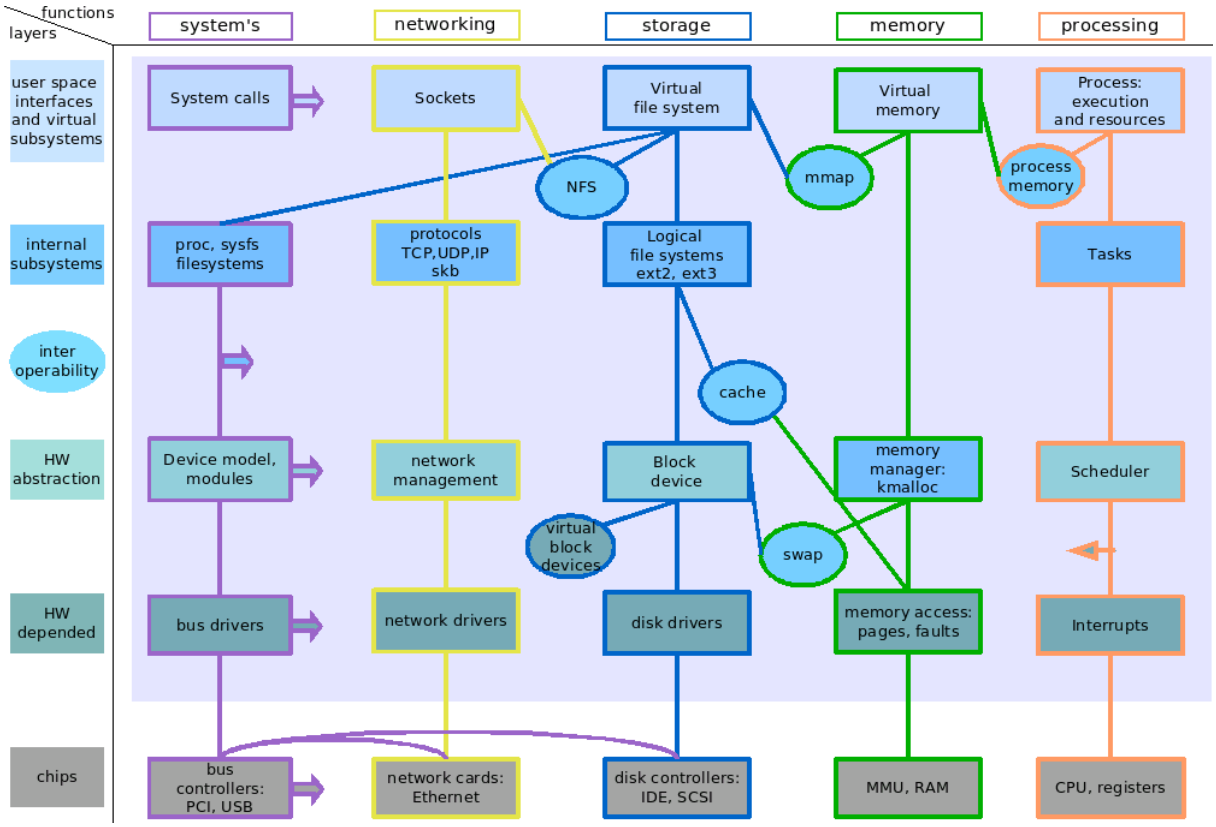
12 Der Linux-Kernel

Heutzutage weder für server noch für Workstation kompilierung nötig, aber für embeded systeme. Allenfalls noch für speziell gezüchtete Server

12.1 Kerneltypen

Modulare Kernel, problem Hacker kann kernelmodul laden. Bei statischem kernel geht das nicht → Firewall statischen kernel machen

Steuerung der Hardware
Netzwerk
Interkommunikation (Zwischen Prozessen)
    Kommunizieren über loopback interface
        z.B. firefox kommuniziert über loopback interface auf XServer
Zugriff auf Massenspeicher
Speicherverwaltung
    malloc
Prozessverwaltung
    Rechenzeit zuteilen



Socket ist im prinzip ein Port

12.1.1 Früher meist Monolytische Kernel

Wollte man eine weitere funktion musste man ein Object file generieren z.B. von dem Netzwerkkarten treiber und diesen in den Kernel linke.

Windows Monolytischer Kernel

Heuteige prozessoren können eingestellt werden, dass auf stack kein code mehr ausgeführt werden kann, heap kann schreibgeschützt werden

12.1.2 Microkernel

Nur noch task scheduller und hardware nahes, geladen wird im prinzip ein object file.
Modul muss genau zum kernel passen
Tabelle mit einstiegspunkten (Adressen)

12.1.3 Heute: Mischung von beiden

Kernelmodule dürfen keine gegenseitigen abhänigkeiten haben, sonst hat man bei aktuell 5Mio Zeilten code keine chance mehr den überblick zu halten.

12.1.4 Grafikkartentreiber

Closed Source Grafiktreiber meist massiv besser als Opensource

12.1.5 Kernel ist im Microkernel Teil sequentiell

12.2 Versionen

12.2.1 Uname

Uname -a
Uname –r
Uname –rv

Dinge nach punkt sind unter anderem Compier Optionen

z.B. 4GB
z.B. SMP Symmetrisches Multi processing

a: all
r: kernel release
v: Kernel version

12.2.2 /usr/src

cd /usr/

12.2.3 Ungerade Kernel

2.3, 2.5 etc sind Entwicklungskernel

3. Nummer ist bugfixes
    a. Motherbord chips
    b. Usb chips

c. etc.

installiert man einen vanill kernel unter suse läuft gewisse dinge nicht mehr, deshalb muss man den kernel der distro nehmen

12.3 Module anzeigen, laden und entladen

Ls /lib/modules/$(uname –r)

Liste aller Module ist in der Map datei modules.symbols abgelegt
*.ko Kernel Object

12.3.1 Modprobe

Modprobe –l
Modprobe –l | grep ram

Modprobe –r oder rmmod –a
Beide löschen unbenötigte kernelmodule aus dem speicher

12.3.2 lsmod

Lsmod
Autoclean automatisch geladen werden auch automatisch ungeladen

12.3.3 insmod

Insmod /lib/modules/2.6.18.xxx/kernel/fs/cramfs/cramfs.ko
→ ramdisk laden

12.3.4 /etc/modules.conf

Bsp:
Insmod 3c501 io=0x280 irq=5

12.3.5 modprobe

Geht in /etc/modules.conf schauen dann in
/lib/modules/kernel…/modules.dep schauen

12.3.6 modprobe.conf

????

12.3.7 modprobe.d

konfigurations-scripte die ausgeführt werden

suchte selber nach abhänigkeiten

1. modinfo
2. insmod alle benötigten

3. insmod modul

12.3.8 rmmod

12.3.9 modinfo

/lib/modules/2.6.xxxx/kernel/fs/vfat/vfat.ko
→zeile depends: fs → ../fat/fat.ko

12.3.10 depmod –a

Modulabhänigkeiten auflösen
Generiert /lib/modules/kernel…/modules.*

12.3.11 heutzutage kann kern über hardware detect selber treiber laden → kern ruft im prinzip das modprobe auf

kmod macht das (kmod deamon) derivat abhängig.

Modul alias

Alias eth0 3c501

12.4 Konfiguration des Lademechanismus

12.5 Kernel Kompilieren und installieren

Symtypes???
Symset???

apt-get install gcc dialog linux-source-$(uname –r)

make --help
make clean alle objektfiles löschen, configfile bleibt
make config (konfigfile anschauen, module mit m)
make menuconfig (SUSE package ncurses, DEBIAN pakage dialog afaik)
make cloneconfig
make xconfig braucht qt2 oder höher
lib-qt3-mt
make dep abhänigkeiten
make bzImage kompiliert den kernel
kernel ist danach im ./arch/i386 → /boot rechte anpassen
make modules
modules hat bestimmte header datei → interface
make modules_install
modules installieren
make install ???
bootmenu anpassen und zusätzlichen umbenannten vmlinux brauchen zu testen, sonst kann man zurück

keylogger schutz in dem man usb serial nicht in den kernel kompiiert

13 Software- und Paketverwaltung

apt-get gibt es bei den meisten distributionen

Pakete sind auf prozessor kompiliert → allenfalls schneller wenn man neu kompiliert
Gentoo ist ein linux, wo man alles kompilieren muss
Meist pakete so kompiliert, dass es auf möglichst vielen systemen läuft, sollte mal ein package nicht gehen fehlt allenfalls library oder muss halt doch von hand kompiliert werden

13.1 Pakete finden

www.rpmseek.com

13.2 src-version.tar kompilieren

Dreisatz

./configure	analys, sind alle libs header etc vorhanden
make	kompiliert, gelinkt
make install	installiert dateien da hin wie es im makefile steht

→/opt/bin sonst probleme beim deinstallieren oder so

Tar –xjf squid-2.5.STABLE4-tar-bz2

./configure ; make

./configure && make führt make nur aus, wenn configure erfolgreich

./configure && make && sudo makeinstall

13.3 Kompiler

GCC 2.9 beliebt, heute 4.x
→ 2.9 gibt objektcode der auf möglichst vielen systemen läuft
Allenfalls ist der offene von Intel ein bisschen intelligenter und schneller

13.4 Parser

Verantwortlich für das auslesen der Prozessor attribute aus dem /proc verzeichnis.
Wird in makefile geschrieben und so weiter

flex
Yacc
Bison

13.5 make distclean

löscht auch ausführbare dateien, löscht aber alle allfällig mehrfach verwendeten libraries
→ package generator →kommt noch

13.6 Programm ins home installieren

/configure --prefix=$HOME

13.6.1 Bei fehlern fehler eigrenzen, allenfalls problem mit libs

File programm
Ldd programm informationen über libraries

ln –sf libncurses….

13.6.2 Ldconfig baut linkcache neu

/etc/ld.so.conf sind alle Verzeichnisse aufgeführt
lib und usr/lib wird auch immer durchsucht
man könnte einfach hineinkopieren, aber dann gibt es ein durcheinander

ldconfig –p anzeigen der vorhandenen bibliotheken
ldconfig -d

13.7 Alles machen

./confrigure –prefix=$HOME && make all && make install

13.8 ./configure --help

13.9 Zielverzeichnis bei selbst kompiliertem

/usr/local/bin

13.10Funktionsweise makefile

MAKEFILE
all: blah doc
blah: blah.c blup.h
        gcc –o blah blah.c
doc: ……..

make blah
make doc
oder make all
dann make install   (braucht meist root rechte)

erstes ziel ist all, dies beinhaltet

das was da steht kann geprüft werden
sind weitere includes in der h datei werden die zwar vom compiler kompiliert aber zuvor nicht von make überprüft

Make prüft auch ob das objektfile schon vorhanden ist und ob es neuer ist als das c file

Squid z.B. ist in ein verzeichnis
/usr/local/squid
/usr/local/squid/bin
/usr/local/squid/lib
/usr/local/squid/man
Installiert, ist dann aber nur per absolutem pfad erreichbar, was aber keine rolle spielt, da dies sowiso nicht von einem normalen benutzer gestartet wird

13.11LD_LIBRARY_PATH

Ld.so.cache kann man neu generieren

13.12MANPATH

13.13Apropos squid

Funktioniert erst, wenn man für apropos für MANPATH in irgend einem startup scripts anpasst
→export MANPATH=$MANPATH:/usr/local/squid/man   (mit doppelpunkt getrennt)
→MANPATH=/usr/local/squid/man:$MANPATH
      export MANPATH

sudo catman   (macht index für das apropos)

14 Drucken unter Linux

14.1.1

netstat –antu

14.1.2 Iptables –I input_ext –p tcp –m udp –dport 514 –J ACCEPT

15 Hinweise zu Software Paketen

15.1 Firefox

about:config (in der adresszeile) zeigt die Konfigurationsseite von Firefox an

15.2 Entwicklungsrichtlinien für Linux Applikationen

Comming soon

Netzwerksachen: RFC

15.3 Versteckte Parameter

Parameter sind vielleicht nur im Source beschrieben und in der Doku gar nicht vorhanden

15.4 Xdpyinfo

Zeigt auflösung

15.5 Console im VGA modus

In /boot/grub/menu.lst bei der kernel zeile vga=791 eintragen

16 VirtalBox Guest Addons on debian

aptitude install gcc linux-headers-$(uname -r) make
dpkg-reconfigure xserver-xorg
vboxvideo und vboxmouse wählen!!!

Ordner mounten mit: mount –t vboxsf Daten /mnt/Daten

17 Debian übertragen

Paket neu bauen mit aktueller Konfiguration
dpkg -l|grep ^ii | awk '{print $2}' | xargs dpkg-repack

Ich möchte alle Pakete die auf ii (installiert) stehen mit der aktuellen Konfiguration neu bauen. Dies ist der Fall, wenn ich meine Software auf ein anderes System übertragen möchte, ohne sie neu zu konfigurieren.

dpkg –l

18 Knoppix

Knoppix 2 → bem boot geht nur in den runnlevel 2, d.h. ohne XSERVER

Oder
boot: knoppix lang=ch oder sg 2

Hilfe mit F1-6

Immer 2. Konsole öffnen falls erste verschossen wird

18.1.1 Human Readable

Ls –lh
-h //Human Readable → KB, MB

19 Mini Linux Systeme

Puppy linux
µLinux

20 Dnsstuff.ch

Administrator und so weiter einer ip

21 RAMDISK 10ns:10ms Zugriffszeit bei HD

/var/spool/(mail) für stark belasteten mailserver
→ Batteriegestütztes ram
→ oder daten gehen verloren

Datenbank in Ramdisk kopieren um schneller zu durchsuchen

21.1 Read Ahead

Dynamische Puffer mit festplatten daten im ram

21.2 Delyed write

Dynamische Puffer mit festplatten daten im ram
→ Linux Server nicht einfach ausschalten, bei tausenden von usern sicher noch daten offen

22 LVM (nicht für OS, knoppix keine chance)

dd if=/dev/zerl of=disk1.lvm bs=1024 count=21000 //mindestens 20 MB
losetup /dev/loop7 disk1.lvm //loopdevice 7 max 8 standart → kernelparam
→ kernel parameter /etc/sysconfig/sysctl
lvm
pvcreate /dev/loop7
vgcreate VolumeGroupName /dev/loop7
vgscan
ls /etc/lvm/archive
cat /etc/lvm/archive/Name_0000.vg
lvcreate –L 10 data –n home //in mb (10MB) auf extent aufgefüllt →12MB
lvcreate –L 4 data –n usr
lvdisplay

mount /dev/data/home /mnt…
df

mit grafischem tool verwalten und grösse verändern oder
→vgextend //disk hinzufügen (eSata: Hotswapable)
→lvresize –L+1 /dev/data/image / → +4

Mann muss nicht neu fromatieren, wird automatisch angepasst

Nicht wärend des betirebes nur ungemountet
→ suns (ZETA) cluster filesystem

LVM auch netzwerkfähig → Virtuelle Filesysteme

volume extent = block
logical extent

22.1 md treiber → macht software Raid

mdadm Multiple device
mindestens 2 disks
Raid 0 Stripe auch mit pv
Raid 1 Mirror

22.2 LVM

Schicht:
Partitionen mit flexiblen grenzen
Virtual group (vgrp) man sieht diese als physikalische disk
LVM
Md (aka linux software raid)
Platte

Pv physical volume
Vg Volume Group

Apropos = **`man –k`**
`$manpath=/user/share/man`
`Laytech compiler erstellt nroff man pages`

OsX sei im prinzip ein BSD

Mono: ActiveX für Linux

VORDIPLOM
Linux Grundlagen Kapitel
5
6
8

Systemadministration Kapitel
2
3
8
10
Folienkopiene, Eigene Scripte (aussage 05.02.2008 ca 11:15), Buch