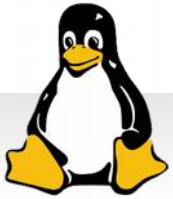
Vorbereitung auf LPIC-1

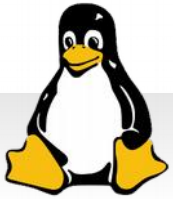
- Georg Schönberger
- XORTEX eBusiness GmbH

- Version 30. März 2016



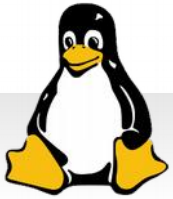
Kurz über mich...

- Studium Computer- und Mediensicherheit
  - Gitter-basierende Kryptosysteme
- Studium Sichere Informationssysteme
  - Auslagerung der IPSec-Verschlüsselung auf Grafikkarten
- Jobs
  - F&E in Hagenberg
  - Thomas-Krenn.AG
  - XORTEX
  - Autor (IT-Admin, LinuxUser)



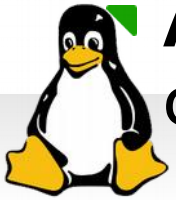
Meine Tätigkeiten

- Betreuung Server-Infrastruktur
  - Ceph Cluster
  - Ansible
- Betreuung DRBD-Cluster mit LXC-Container
- Entwicklung von Monitoring-Plugins
- Entwicklung von Performance-Tests
  - http://git.thomas-krenn.com
- Verbesserung der internen/externen Sicherheit
- Zertifizierungen
  - Network+, Server+, Linux Essentials, LPIC-1, LPIC-2

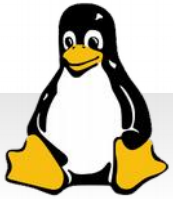


Die LVA

- Vorbereitung auf LPIC-1 Version 4
  - Exam 101 und Exam 102
- Themen
  - LPIC-1 Objectives V4 (wiki.lpi.org)
- Guides
  - **Achtung – Version 3:**
    - Learn Linux, 101: A roadmap for LPIC-1 (ibm.com)
    - GNU/Linux Administration Manuals (nongnu.org)
- Bücher
  - LPIC-1: Sicher zur erfolgreichen Linux-Zertifizierung (Harald Maaßen)
  - **Achtung – Version 3:** LPIC-1. Vorbereitung auf die Prüfung des Linux Professional Institute (Peer Heinlein)

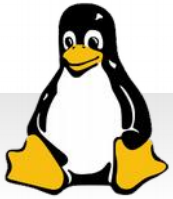


Objectives: Exam 101



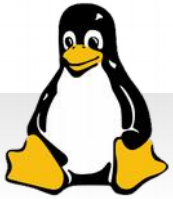
Topic 101: System Architecture

- Peripherie
- Module
- Virtuelle Dateisysteme (*sysfs*, *procfs*)
- Boot-Vorgang
- Runlevel



101.1 Determine and configure hardware settings

- Kernel Module
- */proc*
- */sys*

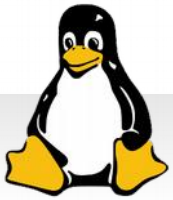


Kernel Module

- Welchen Kernel verwende ich gerade?

```
:~$ uname -a
Linux lin1 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64 GNU/Linux
:~$ uname -r
3.2.0-4-amd64
```

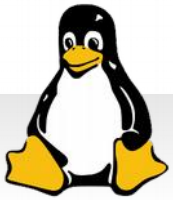
- Kernel verwendet Module
  - Z.B. als ladbare Treiber
- Unter Umständen gibt es pre-compiled Module, die nur unter einem Kernel laufen
  - Hilfreich – DKMS schafft Abhilfe beim Neu-Installieren von Kerneln
    - DKMS (help.ubuntu.com)



Kernel Module

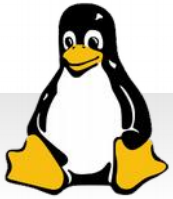
- Wichtige Dateien
  - */etc/modprobe.d* → Konfiguration
  - */lib/modules/modules.dep* → Abhängigkeiten zwischen Modulen
  - */boot/System.map-`uname-r`* → Lookup zwischen Symbol-Namen und Adressen im Speicher
    - Kernel HOWTO - System.map (faqs.org)
  - */lib/modules* Verzeichnis

```
# ls /lib/modules/`uname -r`
build           modules.builtin    modules.devname  modules.symbols.bin
kernel          modules.builtin.binmodules.order source
modules.alias   modules.dep        modules.softdep  updates
modules.alias.bin  modules.dep.bin modules.symbols
```



Kernel Module

lsmod	Gerade geladene Module anzeigen, greift auf */proc/modules* zu.
modinfo	Information zu einem Modul anzeigen.
insmod	Ein Modul laden, in Kernel „einfügen“. Abhängigkeiten werden geprüft, aber nicht aufgelöst.
rmmod	Modul entladen, kein absoluter Pfad notwendig (greift auf */prod/modules* zu).
modprobe	Kernel Module verwalten, mit Abhängigkeiten laden, entladen etc.
depmod	Generiert *modules.dep* und *System.map* Dateien.

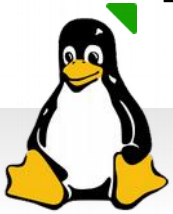


/proc, */sys* und */dev*

- Virtuelle Datei-Systeme, über die der Kernel Informationen weiter gibt
  - Nicht persistent
- */proc*

```
$ for PID in `pidof bash`; do cat /proc/$PID/status | grep VmRSS; done
VmRSS:       4836 kB
VmRSS:       4532 kB
```

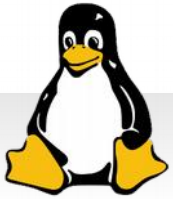
  - Informationen über Prozesse
    - */proc/sys/kernel* oder */proc/version*
  - */proc/sys* nicht Teil von sysfs, bearbeitet mit *sysctl*
- */sys*
  - *sysfs* seit Kernel 2.6, „aufräumen“ von */proc*
  - Devices, Treiber, Bus-Informationen
  - Treiber nutzen sysfs-API



/dev und *udev*

- */dev*
  - Früher, Gerätedateien für Peripherie, statisch
  - Kernel „exportiert“ Geräte in Userspace
  - IDE und SCSI → */dev/hd* und */dev/sd*
  - Primäre und erweiterte Partitionen (erste logische Nummer 5)
- *userspace dev*
  - Dynamische Vorgehensweise
    - *udevd* kümmert sich um Zuweisung
    - Erstellt Einträge unter */dev*
    - Konfiguration unter */etc/udev*

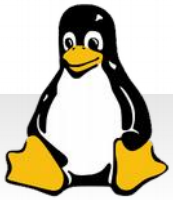
```
# service udev status
[ ok ] udevd is running.
# ls /etc/udev/
links.conf  rules.d  udev.conf
```



Peripherie

- SCSI Geräte

```
$ cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA      Model: Samsung SSD 840  Rev: DXM0
  Type:   Direct-Access                    ANSI  SCSI revision: 05
Host: scsi1 Channel: 00 Id: 00 Lun: 00
  Vendor: MATSHITA Model: DVD-RAM UJ892    Rev: SB01
  Type:   CD-ROM                           ANSI  SCSI revision: 05
$ cat /proc/scsi/usb-storage/9
   Host scsi9: usb-storage
       Vendor: SONY
      Product: WALKMAN
```



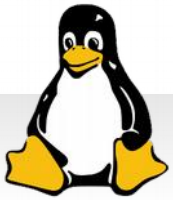
Peripherie

- Anzeigen
  - Gerätenummern und Namen
  - *lsusb*

```
:~$ lsusb
Bus 002 Device 002: ID 8087:0020 Intel Corp. Integrated Rate Matching Hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 17ef:480f Lenovo Integrated Webcam [R5U877]
Bus 001 Device 004: ID 045e:0745 Microsoft Corp. Nano Transceiver v1.0 for Bluetooth
Bus 001 Device 002: ID 8087:0020 Intel Corp. Integrated Rate Matching Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

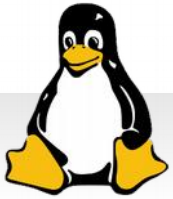
  - *lspci*
    - *-v* Verbose Informationen anzeigen

```
:~$ lspci | grep -i ethernet
00:19.0 Ethernet controller: Intel Corporation 82577LM Gigabit Network Connection (rev 06)
```



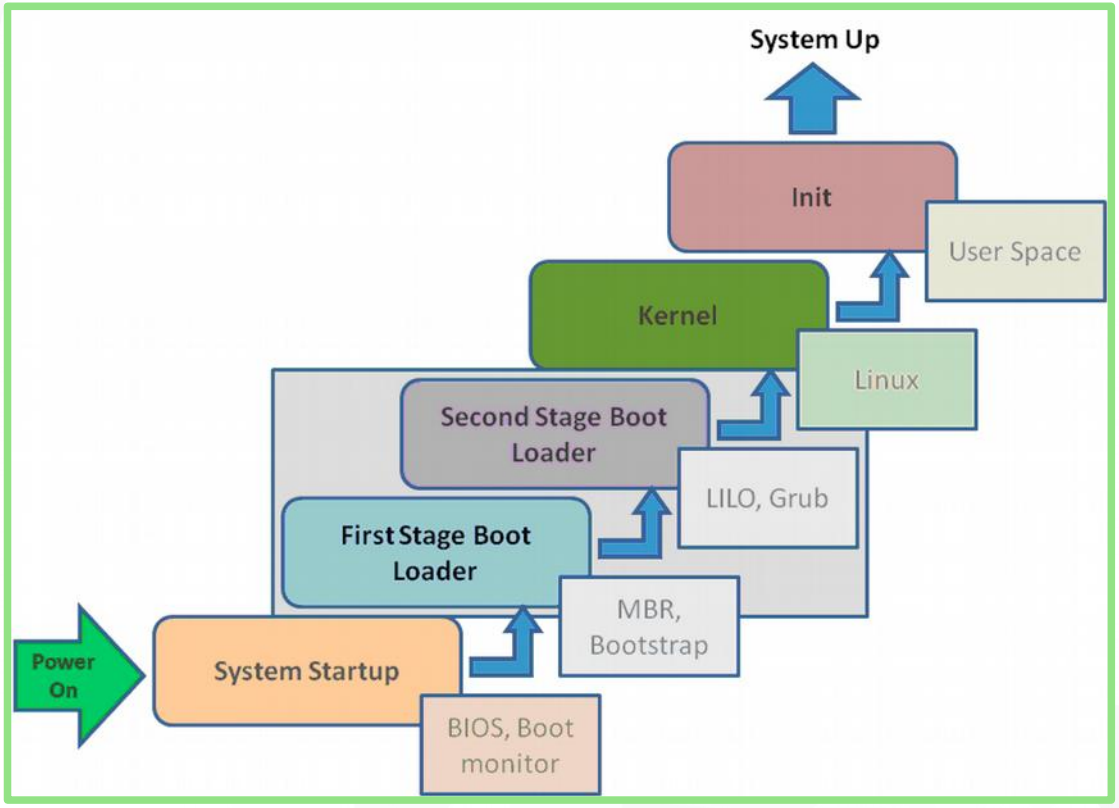
101.2 Boot the System

- Systemstart
- BIOS
- Bootloader
- *dmesg*



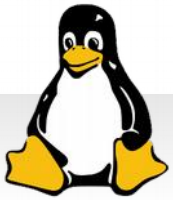
Systemstart

- Boot-Strap oder Henne-Ei Problem
  - Brauche Software um Software zu laden
- Partitionstabelle im Master Boot Record
  - 512 Byte Groß
  - Lädt direkt nächste Stufe des Bootloaders, z.B. GRUB
  - Sucht nach startfähiger Partition → Bootloader



linux-boot-sequence (sureshcore.blogspot.co.at)

```
# dd bs=512 count=1 if=/dev/sda 2>/dev/null| strings
```



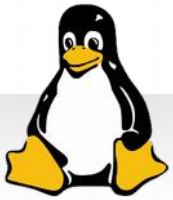
Initramfs und Start-Protokoll

- Initiale RAM Disk, als *tmpfs* geladen
- Beinhaltet Kernel Module und Tools zum Initialisieren
- Wird benötigt, um eigentliches *rootfs* zu laden

```
# file /boot/initrd.img-3.2.0-4-amd64
/boot/initrd.img-3.2.0-4-amd64: gzip compressed data, from Unix, last
modified: Sun Sep  7 10:36:50 2014
```

- *update-initramfs*
  - Verwaltet *cpio* Archiv
  - Bei Kernel oder Module Updates

```
$ grep initrd /boot/grub/grub.cfg  | head -n 1
    initrd   /boot/initrd.img-3.13.0-77-generic
```



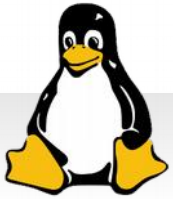
Kernel Paramter

- Beim Boot über Grub-Menü oder Grub-Konfiguration
  - Über *E* im Menü die Optionen editieren

```
$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.13.0-73-generic root=UUID=81935978-2cfc-4fee-b2fd-56c29e4cef23
ro quiet splash vt.handoff=7
```

- *dmesg* → Gibt den Kernel Ring Buffer aus
  - Beinhaltet viele Nachrichten → filtern oder pipen

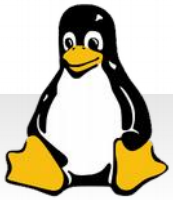
```
# dmesg| grep sda
[    1.294448] sd 2:0:0:0: [sda] 16777216 512-byte logical blocks: (8.58
GB/8.00 GiB)
[    1.294483] sd 2:0:0:0: [sda] Write Protect is off
[    1.294485] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[    1.294499] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled,
doesn't support DPO or FUA
[    1.295866]  sda: sda1 sda2 < sda5 sda6 sda7 sda8 sda9 >
[    1.297069] sd 2:0:0:0: [sda] Attached SCSI disk
```



Start-Protokoll

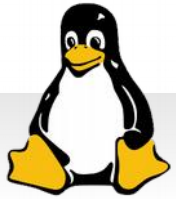
- */var/log/messages*
  - Log-Nachrichten werden länger aufgehoben
  - *dmesg* nur temporär

```
# grep sda /var/log/messages
Mar 28 09:02:24 lin1 kernel: [    3.636080] Adding 473084k swap on /dev/sda7.  Priority:-1 extent
Mar 28 09:02:24 lin1 kernel: [    3.639583] EXT4-fs (sda1): re-mounted. Opts: (null)
Mar 28 09:02:24 lin1 kernel: [    3.790040] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
Mar 28 09:02:24 lin1 kernel: [    4.486311] EXT4-fs (sda9): mounted filesystem with ordered data
Mar 28 09:02:24 lin1 kernel: [    4.504813] EXT4-fs (sda8): mounted filesystem with ordered data
Mar 28 09:02:24 lin1 kernel: [    4.525994] EXT4-fs (sda5): mounted filesystem with ordered data
Mar 28 09:02:24 lin1 kernel: [    4.548658] EXT4-fs (sda6): mounted filesystem with ordered data
```



101.3 Change runlevels / boot targets and shutdown or reboot system

- Runlevel
- System starten
- System anhalten



Systemstart und *init*

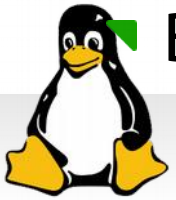
- Kernel übergibt Kontrolle an *init* Prozess

```
# pidof init
1
# pstree
init─┬─VBoxService───7*[{VBoxService}]
     ├─acpid
     ├─atd
     ├─cron
```

- Runlevel, Zustände/Funktionsstufen des Systems
  - Ubuntu Upstart Runlevels (upstart.ubuntu.com)

```
root@lin1:~# grep Runlevel /etc/inittab
# Runlevel 0 is halt.
# Runlevel 1 is single-user.
# Runlevels 2-5 are multi-user.
# Runlevel 6 is reboot.
```

- */etc/inittab*
  - Haupt-Konfigurationsdatei für *init* basierte Systeme
  - Bei Ubuntu o. Derivaten mit *upstart*/*systemd* nicht mehr



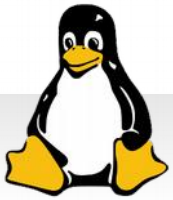
Systemstart und *init*

- *runlevel* → gibt letzten und aktuellen Level aus
- *telinit q* → Lässt *init* die Datei *inittab* neu einlesen
- */etc/init.d* oder */etc/rc.d*
  - *Init Script base directory*
  - Skripte, die beim Wechsel der Runlevel involviert sind

```
# ls -la /etc/rc2.d/
total 9
drwxr-xr-x  2 root root 1024 Mar 28 10:37 .
drwxr-xr-x 76 root root 6144 Mar 28 10:34 ..
-rw-r--r--  1 root root  677 Jul 14  2013 README
lrwxrwxrwx  1 root root   14 Sep  7  2014 S01motd -> ../init.d/motd
lrwxrwxrwx  1 root root   17 Sep  7  2014 S13rpcbind -> ../init.d/rpcbind
```

- Z.B. für SSH-Server

```
# vi /etc/init.d/ssh
# find /etc/rc*.d | grep -i ssh
/etc/rc2.d/S17ssh
/etc/rc3.d/S17ssh
/etc/rc4.d/S17ssh
/etc/rc5.d/S17ssh
```



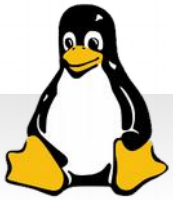
Systemstart und *init*

- Init Skripte verwalten, über symbolische Links
  - *update-rc.d*
  - Beispiele in *man update-rc.d*

```
# update-rc.d exim4 defaults
```

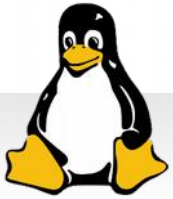
- Weitere Kommandos
  - *runlevel* → Runlevel anzeigen
  - *init* oder *telinit* → Runlevel wechseln
  - *shutdown* → System herunterfahren
  - *halt* oder *poweroff* → System stoppen
  - *reboot* → System neu starten

```
$ who -r
         run-level 2  2016-01-01 11:38
```



systemd

- Ist eine Alternative zu *SysVinit* und abwärtskompatibel
  - Startet genau wie *upstart* Dienste parallel
    - Systemd for Upstart Users (wiki.ubuntu.com)
    - Managing services with systemd (redhat.com)
  - Kommuniziert über Sockets
- *systemctl* als Werkzeug
  - Units entsprechen Startskripte von *SysVinit*
  - Unter */lib/systemd/system* zu finden
  - Aktivierte Units werden nach */etc/sytemd/system* verknüpft
    - Analog zu symbolische Links von *init* → *rcX-d*



systemd - systemctl

- Units verwalten
  - Vgl. über *service* oder *update-rc.d* von *init*

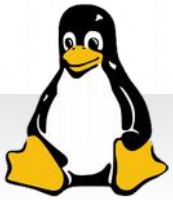
```
# systemctl start bluetooth.service
# systemctl stop bluetooth.service
# systemctl enable bluetooth.service
# systemctl disable bluetooth.service
# systemctl status sshd.service
```

- Targets stellen Runlevel ein

```
# systemctl get-default
# systemctl isolate runlevel3.target
# systemctl set-default multi-user.target
# systemctl isolate multi-user.target
# systemctl rescue
# systemctl isolate reboot.target
```

- System kontrollieren

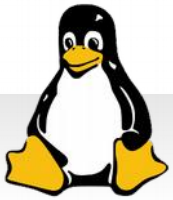
```
# systemctl reboot
# systemctl poweroff
```



System herunterfahren

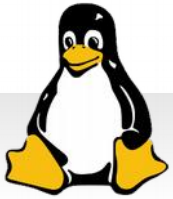
- System anhalten oder neu starten
  - *telinit 0* ist *halt*
  - Sauber herunterfahren mit
    - *shutdown -F* → Dateisystem-Check
    - *shutdown -h now*
    - *shutdown -k* → Schickt nur Nachricht aus
    - *shutdown -r now* oder *reboot*

```
# shutdown -h now
# shutdown -r now
# shutdown -k now 'Not really shutting down...'
Broadcast message from root@lin1 (pts/0) (Sat Apr 18 19:03:14 2015):
Not really shutting down...
The system is going down to maintenance mode NOW!
Shutdown cancelled.

# echo 'WARNING' | wall -t 1
Broadcast Message from root@lin1
        (/dev/pts/0) at 19:05 ...
WARNING
```



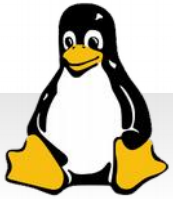
Topic 102: Linux Installation and Package Management

- Dateisystem und Formatierung
- Bootloader installieren
- Shared Libaries (Windows DLLs)
- Package Management
  - *dpkg, apt*
  - *rpm, yum*



102.1 Design hard disk layout

- Festplattenaufteilung
- Partitionierung



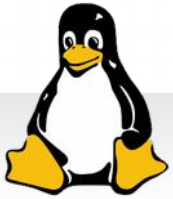
Partitionsplanung

- Verzeichnisstruktur in Partitionen unterteilen

```
$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0     8G  0 disk
├─sda1   8:1    0   333M  0 part /
├─sda2   8:2    0     1K  0 part
├─sda5   8:5    0   2.8G  0 part /usr
├─sda6   8:6    0   1.4G  0 part /var
├─sda7   8:7    0   462M  0 part [SWAP]
├─sda8   8:8    0   241M  0 part /tmp
└─sda9   8:9    0   2.8G  0 part /home
```

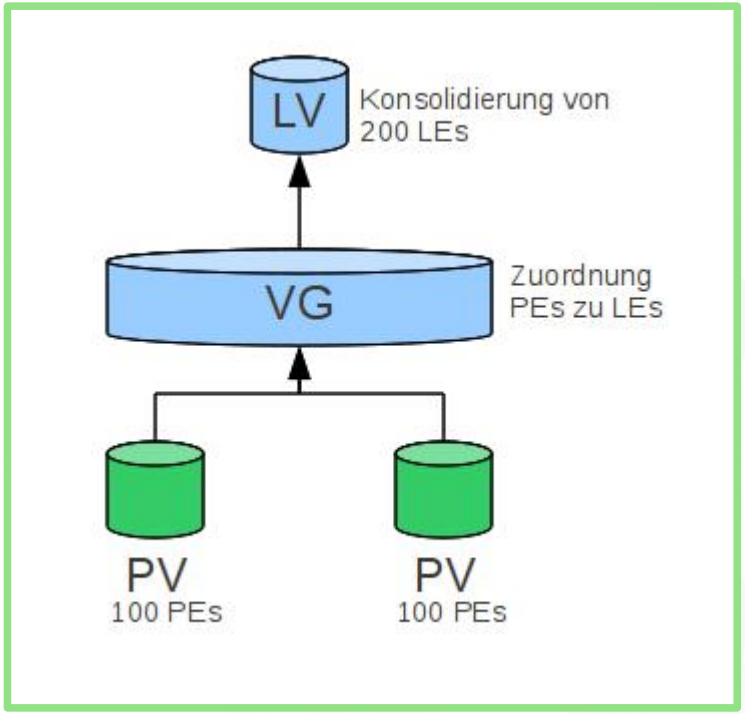
```
$ lsblk
NAME           MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda              8:0    0 238,5G  0 disk
├─sda1           8:1    0  18,6G  0 part  /
├─sda2           8:2    0   218G  0 part  /home
└─sda3           8:3    0   1,9G  0 part
  └─cryptswap1
  (dm-0)       252:0    0   1,9G  0 crypt [SWAP]
sr0            11:0    1  1024M  0 rom
```

- Welche Dateisysteme werden in Backup inkludiert?
- Welche Vorteile bringt die Aufteilung?
- Wird eine separate Boot-Partition benötigt?
  - UEFI
  - RAID

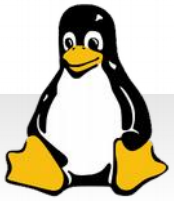


Partitionsplanung – LVM

- Logical Volume Manager
  - LVM Grundlagen (thomas-krenn.com)
  - Abstraktionsschicht
    - Erleichtert nachträgliche Erweiterung
    - PV → VG → LV
  - Eigener Partitionstyp *0x8E*
- Kommandos
  - *pvcreate, pvdisplay*
  - *vgcreate, vgdisplay*
  - *lvcreate, lvdisplay*

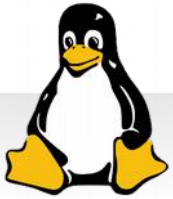


LVM Grundlagen (thomas-krenn.com)



102.2 Install a boot manager

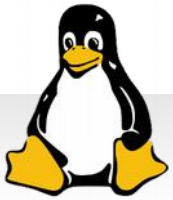
- Boot Manager, MBR
- GRUB



Boot Manager

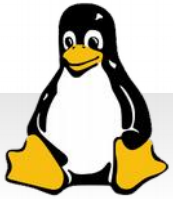
- Oder auch Boot-Strap-Loader
- BIOS lädt Sektor 0 oder sucht auf startfähigen Laufwerken nach Loader
- Loader sucht Kernel und übergibt Kontrolle an diesen
- GRUB Legacy
  - Stages: *stage1* → *stage1,5* → *stage2*
  - *root (boot)* → *kernel + rootfs* → *initrd* → *boot*
  - Konfigurations-Dateien
    - */boot/grub/device.map* → Zuordnung Gerätenamen
    - */boot/grub/menu.lst* → Boot Entries für OS
    - */etc/grub.conf* → Parameter/Optionen Grub Shell

```
$ cat /boot/grub/device.map
(hd0)    /dev/disk/by-id/ata-VBOX_HARDDISK_VB71db8ada-aeb000d1
```



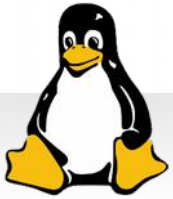
Boot Manager

- GRUB 2
  - Neuer Bootloader, mit Legacy nicht viel gemeinsam
  - Konfigurations-Dateien
    - */etc/default/grub* → Haupt-Konfiguration
    - */etc/grub.d*
    - */boot/grub/grub.cfg*
      - Wird durch ***grub-mkconfig*** bzw. ***update-grub*** erstellt
    - Nur Dateien unter */etc* editieren
  - S.a. Grub2 (help.ubuntu.com)



102.3 Manage shared libraries

- Systembibliotheken
  - *ldd*, *ldconfig*

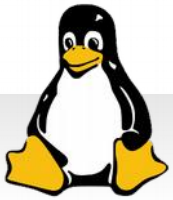


Shared Libraries

- Unter Windows DLLs, unter Linux *.so* → Shared Objects
- *Dynamic linked* Programme verwenden diese Bibliotheken → vs. *static linked*
- *ldd* Kommando

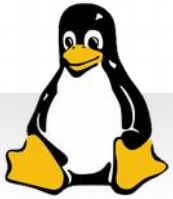
```
# ldd /bin/grep
    linux-vdso.so.1 =>  (0x00007fffcf9ff000)
    libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007fdb983d3000)
    libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fdb98048000)
    /lib64/ld-linux-x86-64.so.2 (0x00007fdb985de000)
```

- *ldconfig* → baut Library Cache auf
  - */etc/ld.so.conf* und */etc/ld.so.conf.d*
  - Cache in → */etc/ld.so.cache*
- Zusätzliche Bibl. über *LD_LIBRARY_PATH* einbinden



102.4 Use Debian package management

- Debian Packages
  - *dpkg*
  - *apt-get*



Debian Packages

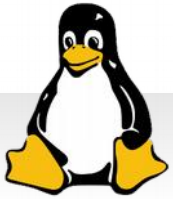
- *.deb* dateien

```
# dpkg-deb -c sysstat_10.0.5-1_amd64.deb
drwxr-xr-x root/root         0 2012-05-21 08:48 ./
drwxr-xr-x root/root         0 2012-05-21 08:47 ./var/
drwxr-xr-x root/root         0 2012-05-21 08:47 ./var/log/
drwxr-xr-x root/root         0 2012-05-21 08:47 ./var/log/sysstat/
drwxr-xr-x root/root         0 2012-05-21 08:47 ./etc/
drwxr-xr-x root/root         0 2012-05-21 08:47 ./etc/sysstat/
```

- Name, Version, Release, Architektur
- Konfigurations-Dateien
  - */etc/dpkg/dpkg.cfg* → Optionen für dpkg
  - */var/lib/dpkg/info* → Dateien für Installation

```
# ls /var/lib/dpkg/info/grep.*
/var/lib/dpkg/info/grep.list  /var/lib/dpkg/info/grep.md5sums
```

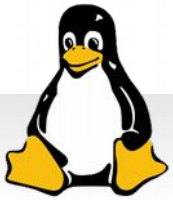
  - */var/lib/dpkg/status* → Info, über Installationsstatus



Debian Packages

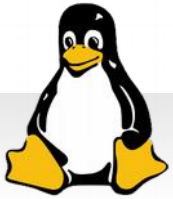
- */var/lib/dpkg/available* → Verfügbare Packages
- *apt* → Advanced Package Tool
  - */etc/apt/apt.conf*
  - */etc/apt/sources.list* und */etc/apt/sources.list.d*
- Mit *dpkg* Packages verwalten

dpkg -i	Installieren
dpkg -r	Entfernen
dpkg -P	Entfernen + Purge
dpkg -s	Status zu Package
dpkg -L	Dateien von Packages auflisten
dpkg -C	Packages auflisten, die nur teilweise installiert sind
dpkg -l $PATTERN	Packages auflisten, die Pattern matchen
dpkg-reconfigure	Package neu konfigurieren



apt-get, *apt-cache* und *aptitude*

- *apt-get* → Front-End für *dpkg*
  - Löst automatisch Abhängigkeiten auf
  - Arbeitet mit Repos in */etc/apt/sources.list*
  - Erledigt Suchen, Installieren, Entfernen, Upgrade, Status u.v.m
- *apt-cache*
  - Sucht nach Paketen
  - Arbeitet mit Cache in */var/cache/apt*
- *aptitude*
  - Im Prinzip noch eine Stufe über apt
  - Auch *ncurses* Interface im Terminal möglich



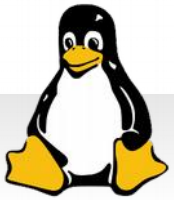
rpm - Red Hat Package Manager

- Auch von CentOS verwendet
  - */etc/rpmrc*

rpm -i	Installieren
rpm -U	Upgrade durchführen
rpm -e	Package entfernen
rpm -q	Informationen abfragen
rpm -q -i -p	Detail Informationen + Dateien auflisten
rpm -v	Verbose Ausgabe
rpm -h	Fortschritt via # Zeichen

- *rpm2cpio*
  - Extrahiert *cpio* Archiv aus *rpm* Package

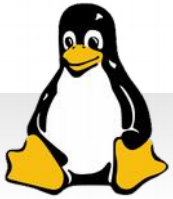
```
# rpm2cpio mediawiki-1.15.1-50.fc11.src.rpm | cpio -idmv
```



rpm - Red Hat Package Manager

- *-- force, -- nodeps*
- Package Informationen abfragen

rpm -q PACKAGE	Info zu PACKAGE
rpm -qf FILE	Zu welchem Package gehört FILE
rpm -qa	Alle Packages auflisten
rpm -qR	Abhängigkeiten auflisten
rpm -ql	Dateien in Package auflisten
rpm -qc	Konfigurationsdateien auflisten
rpm -qd	Dokumentationsdateien aufisten
rpm -qi	Umfangreiche Informationen anzeigen
rpm -V	Verify von Package durchführen

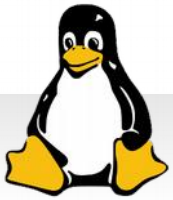


yum

- *yum* arbeitet wie *apt* mit Paketquellen
- Haupt-Konfiguration → */etc/yum.conf*
  - *.repo* Dateien
    - */etc/yum.repos.d/* → */etc/apt/sources.list.d*

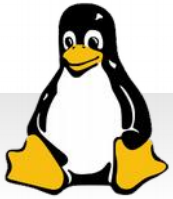
```
# yum repolist
[…]
# tail ...
[repository]
name=repository_name
baseurl=repository_url
```

yum search	Packages suchen
yum install	Packages installieren
yum remote	Package entfernen
yum update	Packages komplett upgraden/aktualisieren
yum list	Informationen über Packages
yum info	Detail Informationen zu einem Package
yum deplist	Abhängigkeiten auflisten
yumdownloader	Lädt Package nur herunter



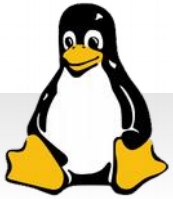
Topic 103: GNU and Unix Commands

- Auf der Kommandozeile arbeiten
- Text Streams und Filter
- Dateien suchen
- Prozesse verwalten
- Editor *vi*



103.1 Work on the command line

- Auf der Kommandozeile arbeiten
  - Kommandofolgen verknüpfen
  - Shell-Umgebung verwenden und anpassen
  - Umgebungsvariablen



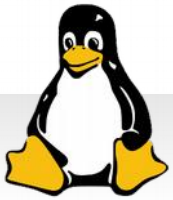
Shell Kommandos

- Kommando – Optionen – Argumente
- Übergabe der Optionen
  - Short - oder Long Options --, manchmal auch nichts davon

```
# tar --extract -z -f sysstat.tar.gz
# tar xzf sysstat.tar.gz
```

  - Beschreibung der Optionen in den man Pages
- Ein Kommando startet immer auch einen Prozess

```
# sleep 100
^Z
[1]+  Stopped                 sleep 100
# ps -eF --forest
root      2254     1  0 12483  1208  /usr/sbin/sshd
root      2401  2254  0 17822  3640        \_ sshd: lin1 [priv]
lin1      2403  2401  0 17822  1636          \_ sshd: lin1@pts/0
lin1      2404  2403  0  5112  3236            \_ -bash
root      2486  2404  0  8407  1856              \_ sudo -i
root      2487  2486  0  5037  3044                \_ -bash
root      2870  2487  0  1399   324                  \_ sleep 100
root      2915  2487  0  4246  1288                    \_ ps -eF --forest
```



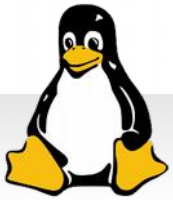
Umgebungs- und Shell-Variablen

- Variablen nehmen Werte auf

```
# printenv | grep PATH
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

  - Umgebungs-Variablen gelten für alle Shells
    - Werden automatisch exportiert
  - Shell-Variablen müssen in Shells neu deklariert werden
- Konfigurations-Dateien

/etc/profile, ~./profile	Erste Config, setzt erstmals $PATH
/etc/bashrc	Systemweite Einstellungen, Alias, Funktionen, von .bashrc eingelesen
~/.bash_profile	Sofort nach /etc/profile ausgeführt, zus. Pfadanweisungen und User-Variablen
~/.bash_login	Alternative zu bash_profile
~/.bashrc	Aufruf bei jeder neuen Shell
~/.bash_logout	Optional bei Abmeldung



Umgebungs- und Shell-Variablen

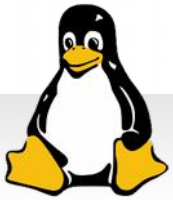
- Variablen anzeigen

```
$ printenv | grep bash
SHELL=/bin/bash
$ env VARFOO="foobar" command options
$ set | grep BASH | head -n 3
BASH=/bin/bash
BASHOPTS=checkwinsize:cmdhist:complete_fullquote
BASH_ALIASES=()
```

- Variablen definieren, beliebte Variablen

```
$ FOO='bar'
$ set | grep FOO
FOO=bar
$ printenv | grep FOO
$ echo $FOO
bar
$ bash
$ echo $FOO

$ exit
exit
~$ unset FOO
```

```
$ echo $HISTSIZE
1000
$ echo $PS1
\[\e]0;\u@\h: \w\a\]$
{debian_chroot:+($debian_chroot)}\
[\033[01;32m\]\u@\h\[\033[00m\]:\
[\033[01;34m\]\w\[\033[00m\]\$
$ echo $?
0
$ echo $PWD
/home/foobar
```



$PATH und man Pages

- Programme darin können relativ aufgerufen werden

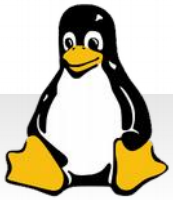
```
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:
```

- Mit *which* absoluten Pfad prüfen

```
$ which adduser
/usr/sbin/adduser
```

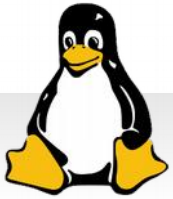
- In aktuellem Verzeichnis ./voranstellen
- In man Pages nach Hilfe suchen
  - Sektion 5 oft hilfreich
  - Andere Hilfen
    - *whatis*
    - *apropos*

```
$ whatis adduser
adduser (8)           - add a user or group to the system
$ apropos adduser
adduser.conf (5)      - configuration file for adduser(8) and
                        addgroup(8)
adduser (8)           - add a user or group to the system
```



103.2 Process Text Streams using Filters

- Text Dateien bearbeiten und Eingabe/Ausgabe um-/weiter-leiten
  - *cat*
  - *cut*
  - *sed*
  - *split*
  - *grep*



Texte ausgeben und manipulieren

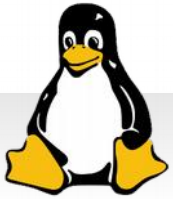
- Über Pipe Ausgabe von Kommando 1 an Kommando 2 leiten

```
# cat /etc/passwd | cut -d: -f 3
[...]
103
1000
1001
```

- *cat* ↔ *tac*
- *head* ↔ *tail*

```
$ tail -n 5 /var/log/dmesg
[   10.742391] iwlwifi 0000:03:00.0: Radio type=0x0-0x3-0x1
[   10.972316] ip_tables: (C) 2000-2006 Netfilter Core Team
[   10.986841] Bridge firewalling registered
```

- *less*
  - Text-Dateien anzeigen
  - Vorteile gegenüber *more*
- *expand* ↔ *unexpand*
  - Tabstopps und Leerzeichen konvertieren

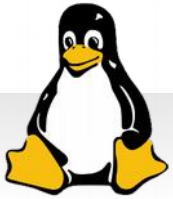


Texte ausgeben

- *nl* gibt Zeilennummern aus

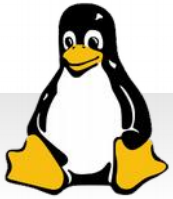
```
# nl /etc/passwd
     1   root:x:0:0:root:/root:/bin/bash
     2   daemon:x:1:1:daemon:/usr/sbin:/bin/sh
     3   bin:x:2:2:bin:/bin:/bin/sh
     4   sys:x:3:3:sys:/dev:/bin/sh
# cat /etc/passwd | tr lin LIN
LIN1:x:1000:1000:LIN1,,,:/home/LIN1:/bIN/bash
```

- *wc* → zählt Zeilennummern
- *hexdump*
- *od* → Octal dump, binärer Dump von Dateien
- *sort* → *uniq*
- *cut* → *paste* → *join* (evtl. *tr*, um Zeichen zu ersetzen)
- *split* → Datei in mehrere Teile aufteilen
  - Mit *cat* wieder zusammenführen



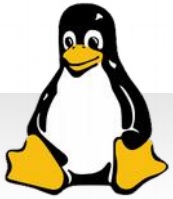
103.3 Basic File Management

- Dateien und Verzeichnisse verwalten
- *find* vs. *locate*
- *tar*
- *cpio*
- *dd*



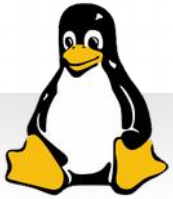
Dateien verwalten und komprimieren

- Learn Linux, 101: File and directory management (ibm.com)
- Dateien und Verzeichnisse
  - wechseln, erstellen, kopieren, verschieben, löschen, auflisten, komprimieren, Archive erstellen
    - *gzip*, *gunzip*, *bzip2*, *tar*
- Dateien finden
  - *find* mit Wildcards und Regular Expressions (Wildcards)
- *cpio* und *dd*
  - Z.B. Backup mit *cpio* in ein Verzeichnis
- *file* Kommando



103.4 Use Streams, Pipes and Redirects

- Standard Ein- und Ausgabe umleiten
- Pipes
- *tee*
- *xargs*



Standard Ein- und Ausgabe

- Ströme 0, 1 und 2
  - Von einander getrennt → Fehler separat behandeln

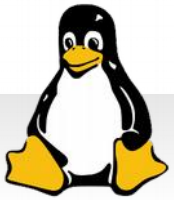
```
$ ./myscript 2>error.log 1>status.log
$ ./myscript >all.log 2>&1
$ ./myscript >> append.log
```

- Aus- und Eingabe verknüpfen → Pipes
- *tee* → Kreuzung

```
$ ssh lin1@192.168.80.128 | tee lin1.log
```

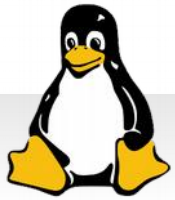
- *xargs* → sammelt Argumente und führt Befehl aus

```
$ ls . | xargs du -h
find . -type f -print0 | xargs -0 grep 127.0.0.1
./listenPorts.txt:tcp    0   0   127.0.0.1:25   0.0.0.0:*   LISTEN
```



103.5 Create, Monitor and kill Processes

- *kill, killall*
- *top, free, uptime*
- *ps, pgrep*
- *fg* und *bg*

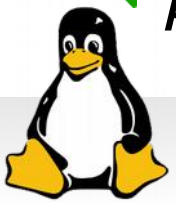


Prozesse und IDs

- *ps* oder *pstree* → alle aktuell laufenden Prozesse anzeigen

```
# ps aux | wc -l
74
# ps -C sshd
  PID TTY          TIME CMD
 2405 ?        00:00:00 sshd
 2490 ?        00:00:00 sshd
# ps -A | grep cron
 2007 ?        00:00:00 cron
```

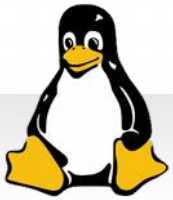
- *top* → Prozesse in Echtzeit ansehen
  - Kann auch Signale an PIDs senden, *renice* ausführen
- *kill* → sendet Signale an Prozesse (*kill -l*, *kill -s*)
  - Ohne Option Signal 15 → *SIGTERM*
  - *Strg + C* → *SIGINT* → Unterschied zu SIGTERM?
- *killall* → verwendet Prozessnamen
  - *pgrep* und *pkill* auch



Prozesse im Hinter-/Vordergrund

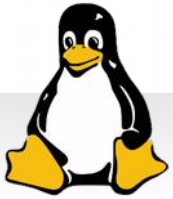
- Mit *Strg + z*, *SIGTSTP* senden und vorübergehend stoppen
- Mit *&* gleich in den Hintergrund schicken
- Jobs verwalten
  - *jobs* zeigt laufende Tasks an, *jobs -l* auch PIDs
  - *bg* → im Hintergrund weiter laufen lassen
  - *fg* → wieder in den Vordergrund holen
  - Mit *nohup* und *screen* unabhängig von Shell laufen lassen

```
# updatedb &
[1] 2893
# jobs
[1]+  Done                    updatedb
# apt-get update
0% [Connecting to ftp.at.debian.org] [Connecting to security.debian.org]^Z
[1]+  Stopped                 apt-get update
root@lin1:~# jobs
[1]+  Stopped                 apt-get update
```



103.6 Modify Process Execution Priorities

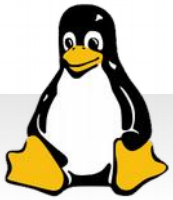
- Prioritäten von Jobs und Priorität ändern
- *nice* und *ionice*
- *renice*
- *top*



Prioritäten von Prozessen

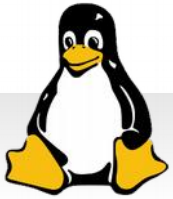
- *nice* fügt Prozessen beim Starten einen *nice* Wert hinzu
  - *nice* Wert ist nicht gleich *PR*, beeinflusst diese aber
  - höherer *nice* Wert → „netter“ zu anderen Prozessen
  - negativer Wert priorisiert daher Prozess
  - *nice* Wert → -20 bis +19, ohne Option 10
- *renice* → zur Laufzeit ändern
  - Im Gegensatz zu *nice* keine Bindestriche bei Zahlen
  - Mit *-u* Prozesse eines ganzen Benutzers abändern

```
# nice --3 uptime
 10:33:54 up  3:10,  2 users,  load average: 0.00, 0.01, 0.05
# renice -3 2977
2977 (process ID) old priority -3, new priority -3
# ps aux | grep 2977
root      2977  0.0  0.5   9956  2824 ?        S<s  10:33   0:00 dhclient
root      2999  0.0  0.1   7832   868 pts/0    S+   10:36   0:00 grep 2977
# top -b -n 1 | grep 2977
 2977 root      17  -3  9956 2824  528 S   0.0  0.6   0:00.00 dhclient
```



103.7 Search Text Files using Regular Expressions

- *Patterns*
- *grep*
- *fgrep*
- *egrep*
- *sed*



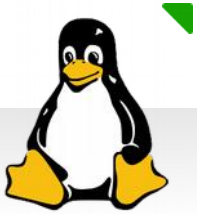
Regular Expressions

- Manche Platzhalter in Shell anders als in Regex
  - Z.B. *?*
- Regular Expression Cheat Sheet

```
# grep -v ^[#] /etc/apt/sources.list | grep -v ^$
# grep 'sshd\[.*opened' /var/log/auth.log
# grep '^Sep 15' /var/log/auth.log
```

- Streaming Editor → *sed*
  - Gibt Ergebnisse auf *STDOUT* aus
    - *-i* → in Place Ersetzen, evtl. Backup Datei anlegen
    - *-g* → global und nicht nur erstes Vorkommen
    - *y* → Ein Zeichen übersetzen
    - *s* → Substitute (auch mehrere Zeichen)
    -

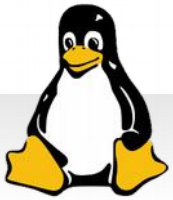
```
# sed 's/lin1/LIN1/g' /etc/passwd
# sed 'y/:/;/' /etc/passwd
```



grep, *egrep* und *fgrep*

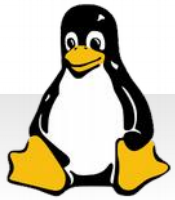
- Nach regulären Ausdrücken in Dateien suchen
  - Wichtige Optionen → *-i*, *-E*, *-n*, *-v*, *-c*
  - Linux grep command with 14 different examples
  - grep regular expression syntax

```
$ grep -v -E $^ /etc/apt/sources.list
$ grep -E main$ /etc/apt/sources.list
$ grep -e main$ -e universe$ /etc/apt/sources.list
$ grep -E 'main|universe' /etc/apt/sources.list
$ grep -f pattern.txt /etc/apt/sources.list
$ grep -n -f pattern.txt /etc/apt/sources.list
$ grep -E -A 5 -B 5 main$ /etc/apt/sources.list
$ grep 'http:\/\/' /etc/apt/sources.list
$ fgrep --binary-files=text -C 50 "samsung" magician
```



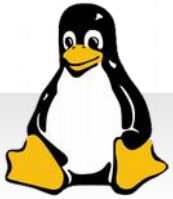
103.8 Perform basic File Editing Operations using vi

- Navigieren
- *vi* Modi
- Text editieren, kopieren, löschen, ersetzen, finden



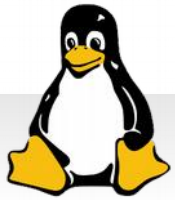
vi – Interaktiver Editor

- Einfügemodus → *i*, *I*, *a*, *A*
  - Wichtige Optionen → *-i*, *-E*, *-n*, *-v*, *-c*
  - Speichern → *:w*, *:w!*, *:wq*, *:x*, *ZZ*
  - Beenden → *:q*, *:q!*
  - Navigation → *h*, *j*, *k*, *l*, *GG*, *gg*
    - Auch mit Multiplikator → *2j5l*
  - Copy und Paste
    - *yy*, *p*, *P*, *dd*, *D*, *cc*, *C*, *o*, *O*
  - Suchen
    - */regexp*
    - Vor und zurück → *n*, *N*



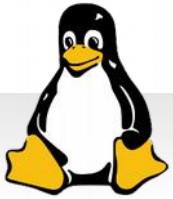
Topic 104: Devices, Linux Filesystems, Filesystem Hierarchy Standard

- Partitionen und Dateisysteme
- Dateisysteme warten
- *mount* und *umount*
- Quotas
- Datei Berechtigungen (Permissions)
- Symbolische und Hard Links



104.1 Create Partitions and Filesystems

- Partitionen und Dateisysteme
- reiserfs, BtrFS
- *gdisk* und *parted*



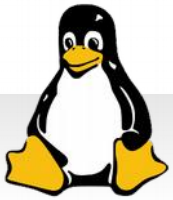
fdisk

- Verwaltet und Erzeugt Partitionen
  - Test mit Loop Device

```
# dd if=/dev/zero of=testPT.file bs=1M count=100
# losetup -f
/dev/loop0
# losetup /dev/loop0 testPT.file
# fdisk /dev/loop0
```

  - *o* → Erzeugt neue Partition Tabelle, *p* zeigt sie an
  - *w* → Schreibt Änderungen auf Device
  - *n* → erstellt neue Partition
    - *p* → Primary
    - First Sector und Last Sector
    - Id → 0x83 für Linux
      - *t* → change ID
      - *L* → List ID Codes

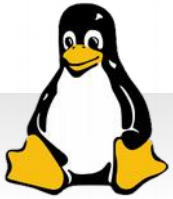
```
$ sudo fdisk -l /dev/sda
$ cat /proc/partitions
$ lsblk
```



GPT – Guid Partition Table

- GUID Partition Table (thomas-krenn.com)
- Ab 4TB GPT zwingend notwendig
- Mit *gdisk* partitioniert

```
# gdisk -l /dev/loop0
GPT fdisk (gdisk) version 0.8.5

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
Disk /dev/loop0: 204800 sectors, 100.0 MiB
Logical sector size: 512 bytes
Disk identifier (GUID): 402DBCDD-42A0-42C4-8439-DB0454E5CC31
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 204766
Partitions will be aligned on 2048-sector boundaries
Total free space is 2014 sectors (1007.0 KiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048          204766   99.0 MiB    8300  Linux filesystem
```

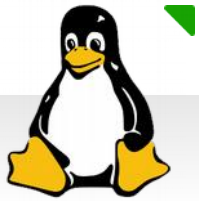


Formatieren der Dateisysteme

- Partition wird nach dem Erstellen formatiert
- Werkzeug Frontends → *mkfs*

```
# mkfs
mkfs           mkfs.cramfs   mkfs.ext3     mkfs.ext4dev
mkfs.bfs       mkfs.ext2     mkfs.ext4     mkfs.minix
# apt-cache search mkfs
btrfs-tools - Checksumming Copy on Write Filesystem utilities
dosfstools - utilities for making and checking MS-DOS FAT filesystems
exfat-utils - utilities to create, check, label and dump exFAT filesystem
hfsprogs - mkfs and fsck for HFS and HFS+ file systems
jfsutils - utilities for managing the JFS filesystem
ufsutils - UFS filesystems utilities
xfsprogs - Utilities for managing the XFS filesystem
```

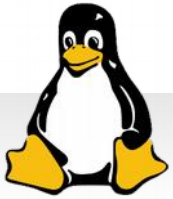
- *mke2fs, mkfs.**
  - *ext3 = ext2 + Journal*
  - *ext4*
    - Online Defragmentierung, Zeitstempel, Preallokation, Fragmentierung



Formatieren der Dateisysteme

```
$ sudo gdisk -l /dev/loop0 | grep 83
Disk identifier (GUID): 839DB0C9-CD8D-4A23-817E-EBEA2A08A8E8
   1            2048          204766   99.0 MiB    8300  Linux filesystem
$ sudo tune2fs -l /dev/loop0
tune2fs 1.42.9 (4-Feb-2014)
tune2fs: Bad magic number in super-block while trying to open /dev/loop0
Couldn't find valid filesystem superblock.
$ sudo mkfs.ext4 -L loopfs /dev/loop0
mke2fs 1.42.9 (4-Feb-2014)
Discarding device blocks: done
Filesystem label=loopfs
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
25688 inodes, 102400 blocks
[…]
$ sudo tune2fs -l /dev/loop0 | grep Free
Free blocks:              93504
Free inodes:              25677
$ sudo blkid
/dev/loop0: LABEL="loopfs" UUID="9faccab0-df90-4d01-9039-61a6197bbcea" TYPE="ext4"
```

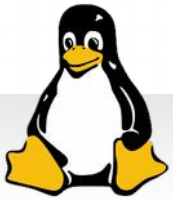
- *tune2fs -j* → Fügt ext2 Journal hinzu



mkswap

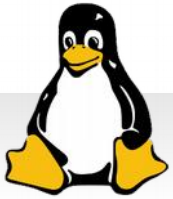
- Swap Partition
  - Mit *mkswap* formatieren (verschlüsseln mit *cryptsetup*)
  - *swapon* für Partition aufrufen
  - *swapoff* leert Swap aus
  - In */etc/fstab* eintragen
- Swap-Datei
  - Mit *fallocate* oder *dd* Datei für Swap erstellen

```
# cat /proc/swaps
Filename                Type     Size Used Priority
/dev/sda7                                partition    473084   0    -1
# grep -i swap /proc/meminfo
SwapCached:            0 kB
SwapTotal:        473084 kB
SwapFree:         473084 kB
# free -m | grep Swap
Swap:           461          0        461
```



104.2 Maintain the Integrity ofFfilesystems

- Integrität von Dateisystemen
- Freier Platz und Inodes
- Dateisysteme reparieren

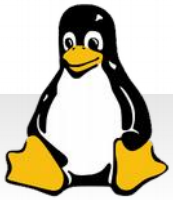


fsck und *e2fsck*

- Dateisystem Check durchführen
  - *shutdown -hF*
  - Vorher *umount* → aushängen
  - Für ext* Dateisysteme → *e2fsck*

```
# ls -li /sbin/fsck.ext4
322 lrwxrwxrwx 1 root root 6 Mar 21  2013 /sbin/fsck.ext4 -> e2fsck
# ls /sbin/fsck*
/sbin/fsck         /sbin/fsck.ext2  /sbin/fsck.ext4     /sbin/fsck.minix
/sbin/fsck.cramfs  /sbin/fsck.ext3  /sbin/fsck.ext4dev  /sbin/fsck.nfs
```

-f	Erzwingt Prüfung, wenn FS clean ist
-A	Alle in fstab geführten Dateisysteme prüfen
-t	Dateisystem Typ spezifizieren
-c	Check, suche nach defekten Blöcken
-y	Alle Fragen mit -yes beantworten

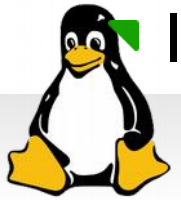


tune2fs und *debugfs*

- Bearbeiten der Dateisystem Parameter
  - Intervalle für automatische Prüfung → *-c* und *-i*
  - Aktuelle Statistiken anzeigen → *-l*
  - Journal hinzufügen → *-j*

```
# tune2fs -l /dev/disk/by-uuid/1da79872-1f9c-4ced-8946-270430cd0f18
tune2fs 1.42.5 (29-Jul-2012)
Filesystem volume name:   <none>
Last mounted on:          /
[...]
Default mount options:    user_xattr acl
Filesystem state:         clean
Errors behavior:          Continue
Filesystem OS type:       Linux
[...]
```

- Dateisystem interaktiv debuggen
  - Gelöschte Inodes anzeigen → *lsdel*
  - Inodes wieder herstellen → *dump*

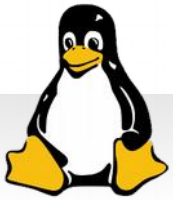


df und *du*

- Verbrauch der inodes → *df -i*
- Ressourcen Belegung → *du*

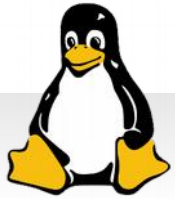
```
# df -h
Filesystem                                              Size  Used Avail Use% Mounted on
rootfs                                                  323M  166M  141M  55% /
udev                                                     10M     0   10M   0% /dev
tmpfs                                                    50M  260K   50M   1% /run
/dev/disk/by-uuid/1da79872-1f9c-4ced-8946-270430cd0f18  323M  166M  141M  55% /
tmpfs                                                   5.0M     0  5.0M   0% /run/lock
tmpfs                                                   192M     0  192M   0% /run/shm
/dev/sda9                                               2.8G   69M  2.6G   3% /home
/dev/sda8                                               234M  6.1M  216M   3% /tmp
/dev/sda5                                               2.8G  696M  2.0G  27% /usr
/dev/sda6                                               1.4G  225M  1.1G  18% /var
```

```
# du -sh
8.4M .
# du -sh *
382K sysstat_10.0.5-1_amd64.deb
381K sysstat.tar.gz
7.6M testPT.file
du -sch /etc
15M  /etc
# 15M    total
```



104.3 Control mounting and unmounting of Filesystems

- */etc/fstab*
- *mount*
- *umount*



mount

- Einträge in */etc/fstab* werden automatisch eingehängt

```
# mount | grep sda
/dev/sda9 on /home type ext4 (rw,relatime,user_xattr,barrier=1,data=ordered)
/dev/sda8 on /tmp type ext4 (rw,relatime,user_xattr,barrier=1,data=ordered)
/dev/sda5 on /usr type ext4 (rw,relatime,user_xattr,barrier=1,data=ordered)
/dev/sda6 on /var type ext4 (rw,relatime,user_xattr,barrier=1,data=ordered)
```

- Optionen, Pfad, Mountpoint

```
# mount -t ext4 /dev/loop0 /mnt/
# mount | grep loop
/dev/loop0 on /mnt type ext4 (rw,relatime,user_xattr,barrier=1,data=ordered)
```

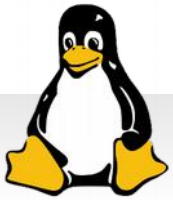
  - Z.B. read-only

```
# mount -t ext4 -r /dev/loop0 /mnt/
```

  - *-o* übergibt Mount-Optionen

```
# mount -o remount,rw /mnt/
```

    - Bei SMB z.B. *-t smbfs -o username=test,password=test*

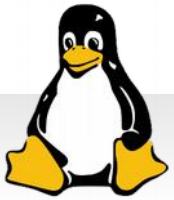


mount und *umount*

- NFS und Samba

```
# mount example.hostname.com:/ubuntu /local/ubuntu
# mount -t cifs -o username=smbuser //192.168.56.101/smbuser /media/
```

- *umount* hängt Mountpoint aus
  - Z.B. wenn *fsck* ausgeführt werden soll
  - Normalerweise nur von *root* ausführbar
    - Außer in *fstab* anders angegeben
      - *user* → Derselbe oder root kann es aushängen
      - *users* → Beliebiger Nutzer kann es aushängen
      - *nouser* → Auf root beschränkt

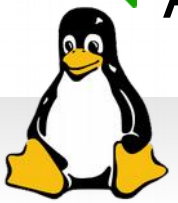


fstab und *mtab*

- *man 5 fstab*

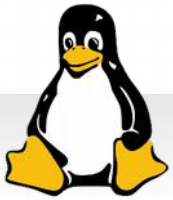
```
# <file system> <mount point>                 <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=1da79872-1f9c-4ced-8946-270430cd0f18 /   ext4    errors=remount-ro  0       1
```

  - *dump* → Vormerkung für Sicherungsprogramm
  - *pass* → *fsck* Check bei Systemstart
    - *0* → kein Check
    - *1* → vorzugsweise Check
    - *2* → Check, nach jenen unter 1
- Beim Mount werden Dateisysteme mit Optionen in */etc/mtab* eingetragen
  - Außer *-n* wurde verwendet → in */proc/mounts* immer da



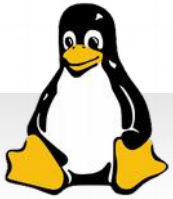
fstab Mount-Optionen

auto	Automatisch über *mount -a*
noauto	Nicht automatisch über *mount -a*
usrquote	Quotas auf Benutzerebene
grpquota	Quotas auf Gruppenebene
suid	Einsatz von suid Bit möglich
nosuid	Kein Einsatz von suid Bit möglich
exec	Erlaubt ausführen von Dateien
noexec	Verhindert ausführen von Dateien
ro	Read-Only Modus
rw	Read-Write Modus
user	Normale einhängen, derselbe o. root aushängen
nouser	Nur root einhängen
users	Normale einhängen, beliebige aushängen
defaults	rw, suid, dev, exec, auto, nouser, async



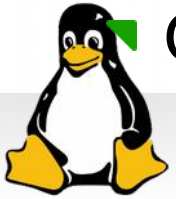
104.4 Manage Disk Quotas

- *quota*
- *edquota*
- *repquota*
- *quotaon*



Quotas

- User oder Group Limits
- Hard oder Soft Limits
  - Bei Hard Limit wird Schreibzugriff verweigert
  - Bei Soft Limit wird Grace Time aktiv
- Beziehen sich immer auf Dateisystem bzw. Partition
  - In */etc/fstab* → *usrquota*, *grpquota*
  - *aquota.user* und *aquota.group* anlegen
- Quotas einrichten (debian-administration.org)
  - *quotaon*
  - *quotacheck*
  - *quotaoff*
  - Optionen *-a*, *-u*, *-g*, *-v*

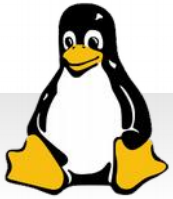


Quotas

- *edquota*
  - Editiert Quotas, definiert Limits → *-p* „klont“ Quotas
  - Editor *vi* wird verwendet
  - Verwendet Block Size, mit *dumpe2fs* prüfen

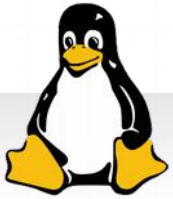
```
$ sudo dumpe2fs /dev/loop0 | grep 'Block size'
dumpe2fs 1.42.9 (4-Feb-2014)
Block size:               1024
```

- *quota*
  - Auskunft/Status über aktuelle Quotas
- *repquota*
  - Erstellt Bericht über Quotas
- How To Enable User and Group Quotas (digitalocean.com)



104.5 ManageFile Permissions and Ownership

- *chown*
- *chgrp*
- *chmod*
- *umask*



Berechtigungen

- *chmod* → *rwx*, Oktal Zahlen als Tripel, absolut angeben
  - *-R* → rekursiv
- SUID oder Setuid
  - Im Kontext des Besitzers ausgeführt

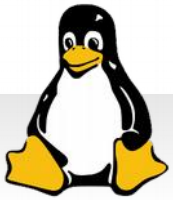
```
# ls -la /usr/bin/passwd
-rwsr-xr-x 1 root root 51096 May 25  2012 /usr/bin/passwd
```

- GUID oder Setgid
  - Im Kontext der Gruppe ausgeführt

```
# ls -la /usr/bin/wall
-rwxr-sr-x 1 root tty 23056 Dec 11  2012 /usr/bin/wall
```

- Nach solchen Dateien suchen

```
# find / -type f -perm -4000 -o -perm -2000
# find / -type f -perm -u+s
# find / -type f -perm -g+s
```



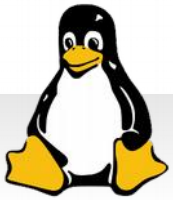
Berechtigungen

- Setgid auf Verzeichnisse
  - Erstellte Dateien/Verzeichnisse gehören User des Verzeichnisses
  - Nicht dem, der die Dateien/Verzeichnisse erstellt hat
- Sticky Bit
  - Nur Besitzer der Datei, des Verzeichnisses oder root kann löschen
  - Z.B. /tmp Verzeichnis

```
$ ls -ld /tmp/
drwxrwxrwt 8 root root 4096 Feb 27 15:58 /tmp/
```

- *chown* und *chgrp*

```
# chown :root error.txt
# ls -la error.txt
-rw-r--r-- 1 lin1 root 47 Sep 16  2014 error.txt
# chgrp lin1 error.txt
```



umask

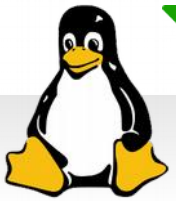
- Welche Berechtigungen erhalten neue Dateien/Verzeichnisse
  - *umask* wird von 0777 und 0666 abgezogen

```
# umask
0022
```

- Ubuntu setzt für Benutzer

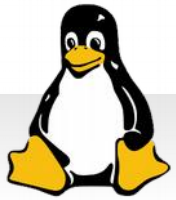
```
$ umask
0002
$ mkdir test
$ ls -ld test/
drwxrwxr-x 2 gschoenb gschoenb 4096 Apr  7 17:34 test/
```

  - User Private Groups helfen dabei, die *umask* auf 0002 zu „lockern“
  - Setgid erleichtert Zusammenarbeit
    - Kein manuelles Ändern der Rechte nötig



104.6 Create and change Hard and Symbolic Links

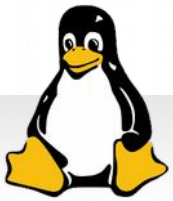
- *ln*
- *ls -i*



Symbolic und Hard Links

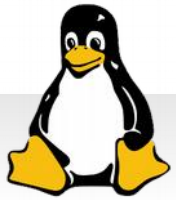
- Soft → ein Zeiger auf eine Datei/Verzeichnis
  - Auf Cross Dateisystem
  - Hat Berechtigungen der Ziel-Datei
  - Bleibt erhalten, auch wenn Ziel gelöscht wird
- Hard → Verwendet den selben Inode
  - Nur auf Dateien und nicht Cross Dateisystem
  - Im Nachhinein nicht mehr von Ziel zu unterscheiden

```
$ ln -s pattern.txt patternsl
$ ll patternsl
lrwxrwxrwx 1 gschoenb gschoenb 11 Feb 27 19:00 patternsl -> pattern.txt
$ rm pattern.txt
$ find . -xtype l
./patternsl
$ cat patternsl
cat: patternsl: No such file or directory
$ ln pattern.txt patternhl
 ls -li pattern*
1853712 [...] patternhl
1848274 [...] patternsl -> pattern.txt
1853712 [...] pattern.txt
```



104.7 Find System Files and place Files in the correct Location

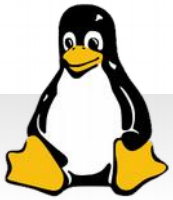
- FHS
- Orte von wichtigen Dateien verstehen
- Dateien finden
  - *find*
  - *locate*
  - *whereis*



FHS

- Unterteilung v.a. bei Partitionierung und Sicherung wichtig
  - Abgrenzung der unterschiedlichen Daten durch Partitionierung
    - Spez. Mount-Optionen für Betrieb
  - Ein Ressourcen-Engpass einer Partition beeinflusst restliches System nicht
  - Einfachere Möglichkeit der Daten-Sicherung
    - Virt. Dateisysteme ausnehmen

```
$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0     8G  0 disk
├─sda1   8:1    0   333M  0 part /
├─sda2   8:2    0     1K  0 part
├─sda5   8:5    0   2.8G  0 part /usr
├─sda6   8:6    0   1.4G  0 part /var
├─sda7   8:7    0   462M  0 part [SWAP]
├─sda8   8:8    0   241M  0 part /tmp
└─sda9   8:9    0   2.8G  0 part /home
```

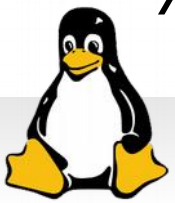


Dateien auffinden

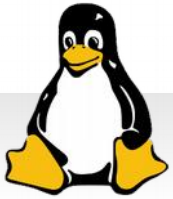
- *whereis*
- *which*
  - Pfadname des Programms, das ausgeführt werden würde
- *whatis* und *apropos* beziehen man Pages mit ein
- *find*
  - *-user*, *-group*, *-ctime*, *-size*, *-perm*,

```
# find / -type f -name ssh*
/etc/init.d/ssh
/etc/pam.d/sshd
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_rsa_key.pub
[...]
```

- *locate* nutzt Datenbank → */var/lib/mlocate/mlocate.db*
  - */etc/updatedb.conf* → *PRUNEPATHS*, *NETPATHS*

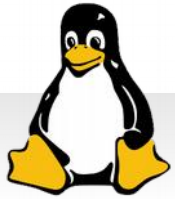


Objectives: Exam 102



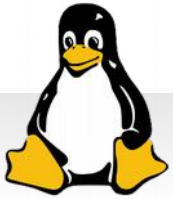
Topic 105: Shells, Scripting and Data Management

- Shell Umgebung anpassen
- Shell Skripte



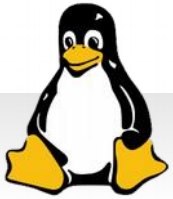
105.1 Customize and use the Shell Environment

- */etc/profile*
- *export*
- *set*
- *bashrc*
- *alias*



Variablen

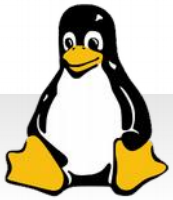
- Umgebungsvariablen gelten für alle Shells, Shellvariablen nur für die aktuelle
- Exports gelten nur für untergeordnete, nicht für übergeordnete Shells
- *set* und *env* zeigen Shell- und Umgebungs-Variablen
  - *unset* löscht Variablen
- *alias* setzt Alternative Namen für ein Kommando
- Unterschiede verstehen
  - Shell-Variable vs. Umgebungsvariable
  - *export* und Sub-Shells



Kommandos und Shell Konfiguration

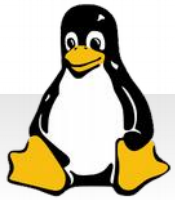
- Verkettungen
  - *&& || ;*
- Abtrennung
  - *|*
- S.a. Folie 46
  - Konfigurationen mit *source* einlesen

~/.bashrc	Ursprüngliche Config, auf jeden fall eingelesen, auch bei neuer Shell
~/.bash_profile	Bei Neuanmeldung, nach */etc/profile*
~/.bash_login	Alternative zu *.bash_profile*
~/.bash_logout	Ausgeführt, wenn Benutzer sich abmeldet
~/.profile	Wird ausgeführt wenn bash_profile und bash_login nicht existieren
/etc/skel	Vorlage-Dateien für neue Benutzer



105.2 Customize or write simple Scripts

- *for*
- *while*
- *test*
- *read*
- *exec*

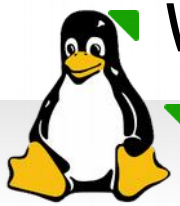


Shell Skripte

- Einfach Skripte schreiben – Interpreter richtig wählen

```
#!/bin/bash

sum=0
while test $# -gt 0
        do
                let sum=sum+$1
                shift
        done
echo Your sum is $sum
unset sum
exit 0
```

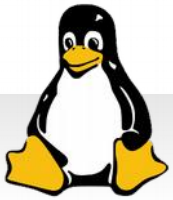
- *let* evaluiert arithmetische Operationen
- *test* Kommando
  - *-d* → ist Verzeichnis
  - *-u* → SUID-Bit ist gesetzt
  - Werte miteinander vergleichen
    - *-eq, -ne, -gt, -ge, -lt, -le*



Shell Skripte

- if Checks
- [ ] und [[ ]]
  - *test* und *extended test*
  - Test Constructs (tldp.org)
- Übergabe-Parameter
  - *$0*, *$1* und *$2*
- Rückgabewerte

```
if /bin/true; then
    echo "true"
fi
if grep -q root /etc/passwd; then
    echo "root user found"
fi
```

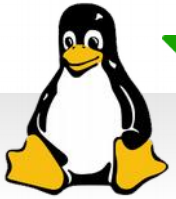


Shell Skripte

- *for* Schleifen und Backticks

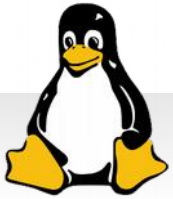
```
#!/bin/bash

for d in `find /home -name '*.txt'`
do
        echo -e "$d"
done
unset d
exit 0
```

- *echo* kann auch an *mail* übergeben werden
  - MTA wird benötigt, außer nur lokale Postfächer
    - *dpkg-reconfigure exim4-config*
- Scipt-Pfade
  - */usr/bin*
  - */usr/local/bin*
    - Evtl. symbolischen Link anlegen



105.3 SQL data management

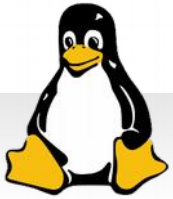
- *insert*
- *update*
- *select*
- *delete*
- *group by*
- *order by*
- *join*



MySQL Software

- Server und Client
  - Employee test Datenbank (github.com)

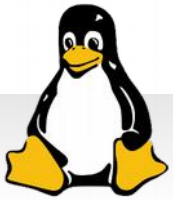
```
$ apt-cache search mysql-server
mysql-server - MySQL database server (metapackage depending on the latest
version)
mysql-server-5.5 - MySQL database server binaries and system database setup
mysql-server-core-5.5 - MySQL database server binaries
$ sudo apt-get install mysql-server
[...]
$ ps aux | grep mysql
mysql     3197  0.0 62.0 625564 40652 ?        Ssl  17:41   0:00
/usr/sbin/mysqld
$ mysql -u root -p
Enter password:
[…]
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)
~/test_db-master# mysql -u root -p < employees.sql
```



MySQL Kommandos

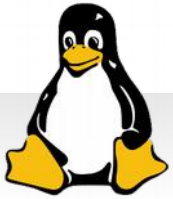
- Useful mysql commands (centoshelp.org)

```
SELECT e.last_name, s.salary
FROM employees e
LEFT JOIN salaries s ON e.emp_no = s.emp_no
LIMIT 0 , 30
-----------------
INSERT INTO  `employees`.`employees` (
`emp_no` ,
`birth_date` ,
`first_name` ,
`last_name` ,
`gender` ,
`hire_date`
)
VALUES (
'9999',  '2015-05-15',  'Peter',  'Paul',  'M',  '2015-05-15'
);
-----------------
select first_name from employees;
select count(*) from employees;
select salary from salaries where emp_no='10001';
select first_name from employees where emp_no=10001;
update employees set first_name='Giorgio' where emp_no=10001;
select salary from salaries order by salary asc limit 0,10;
select first_name, count(*) from employees group by first_name;
select max(emp_no) from employees;
delete from employees where emp_no=10000;
```



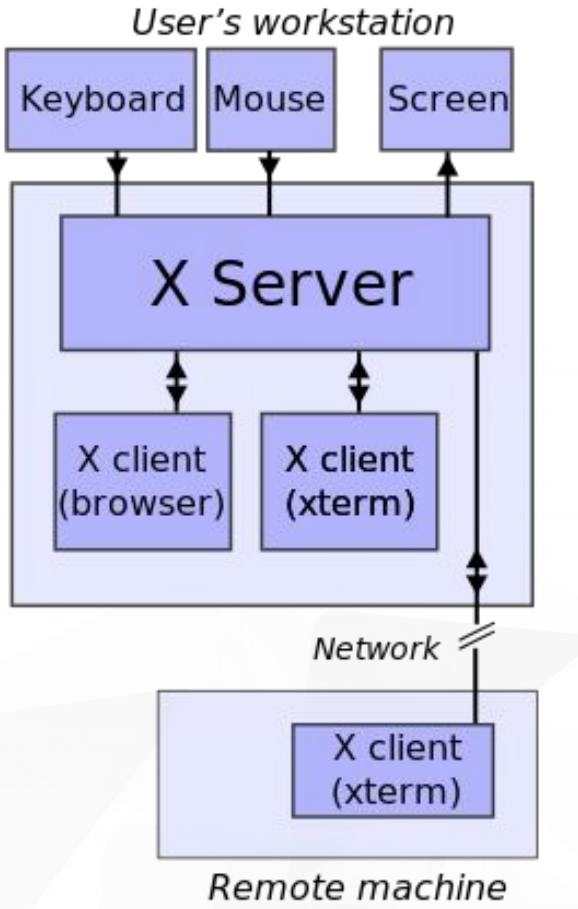
106 User Interfaces and Desktops

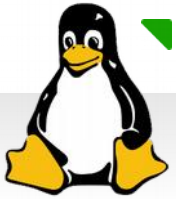
- X11
- Display Manager
- Accessibility



X11 installieren und konfigurieren

- X-Server → Komm. über Kernel und Module mit Hardware
  - Nur für Ausgabe zuständig, kein Einfluss auf Aussehen
    - Benutzer sitzt am X-Server
    - Client führt rechen-intensive Tasks aus
- X-Client → Komm. mit Server, ein Programm sendet verarbeitete Daten an Server
- Window-Manager → ist ein X-Client, Aussehen
- Display-Manager → Auth. von Benutzern



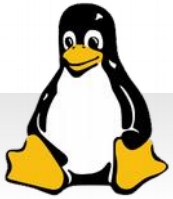


X11 installieren und konfigurieren

- *startx* startet *xinit*
  - Initialisiert X-Window, startet X-Server inkl. Window-Manager

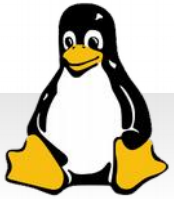
xinitrc	xinit Startscript
xserverrc	X-Server Startscript
.xinitrc	User xinit
.xserverrc	User X-Server
.Xresources	User spez. Einstellungen
/etc/X11/xorg.conf	X Hauptkonfigurationsdatei

- X-Terminals
  - Für konsolen-basierte Programme → *xterm*
- *xhost* erlaubt Zugriff von *X-Client* auf seinen *X-Server*
  - *DISPLAY* Variable muss auf *X-Server* umgestellt werden



X Programme und Displaymanager

- *xwininfo*
  - Informationen über ein einzelnes Fenster
- *xdpyinfo*
  - Informationen über X-Server
- Displaymanager einrichten
  - Kommandos: *xdm*, *lightdm*
  - Wird mit entsprechendem Runlevel gestartet
  - */etc/lightdm/lightdm.conf*

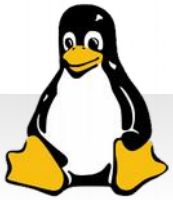


xorg.conf und Font-Server

- Unterschiedliche *Sections* für Konfiguration

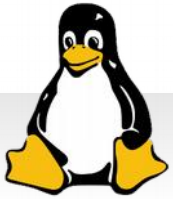
Files	Pfade (Fontpath, RgbPath)
Input Device	Tast. u. Maus (Driver, Identifier)
Monitor	Techn. Spez. des Monitors
Modes	Monitor Modi (Auflösung etc.)
Device	Grafikkarte
Screen	Führt Device und Monitor unter einem Identifier zusammen

- X-Fontserver
  - zentrale Verwaltung von Fonts
- Display-Manager
  - lightdm und */etc/lightdm*



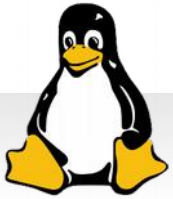
106.3 Accessibility

- Slow/Bounce/Toggle Keys.
- Mouse Keys.
- High Contrast/Large Print Desktop Themes.
- Screen Reader.
- Braille Display



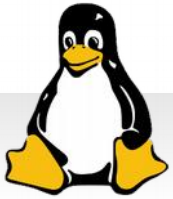
Accessibility

- Barrierefreiheit
- Seebehinderung
  - Screenreader und Brailleschrift (*Orca*, *Emacspeak*)
    - *Orca* enthält auch Bildschirmlupe
    - *BRLTTY* als Daemon von Orca
- Motorisch
  - Klebrige Tasten vs. Tastenverzögerung (*sticky*, *slow/bounce*)
- Screen Magnifier und On-Screen Keyboard
  - *GOK* → Tastatur für Gesten
- Window-Manager (kontrastreich)



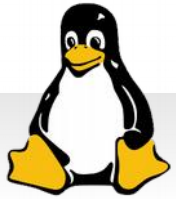
107 Administrative Tasks

- Benutzerkonten
- Gruppenkonten
- Systemdateien



107.1 Manage user and group Accounts and related System Files

- */etc/passwd*
- */etc/shadow*
- */etc/group*
- */etc/skel*

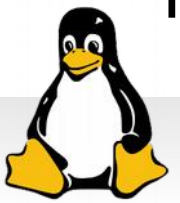


Linux Benutzer

- Benutzer und Gruppen greifen auf Ressourcen zu
  - Gekennzeichnet durch *uid* und *gid*
- Super-User im System → *sudo*
- Zugehörigkeit des Benutzers definiert in
  - */etc/passwd*
    - Durch Doppelpunkt getrennte Felder, für Benutzerinformationen (was bedeuten Felder?)

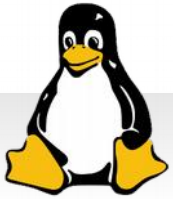
```
$ man 5 passwd
```

  - */etc/shadow* → Passwort-Hashes der Benutzer
  - */etc/group* → Gruppen und Zugehörigkeiten am System
  - /etc/gshadow → Passwort-Hashes von Gruppen-Passwörtern



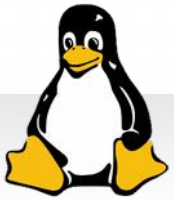
Benutzer verwalten

- *useradd* → */etc/default/useradd*
  - *-d* setzt Home-Verzeichnis
  - *-s* definiert Shell (z.B. */bin/false* für inaktive Benutzer)
  - *-u* legt *uid* fest
- *userdel*
  - *-r* löscht auch Home-Verzeichnis
- *usermod*
  - *-L* deaktiviert Benutzerkonto
- *passwd* → ändert Passwort
  - aber auch *-i* oder *-l*
- *chage* → Werte für Kennwortänderungen



Gruppen verwalten

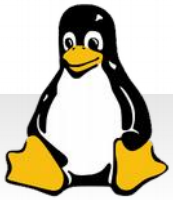
- *groupadd* → in */etc/group* eingetragen
  - *-g* legt gid fest
- *groupdel*
- *groupmod*
  - *-n* vergibt neuen Namen für Gruppe
- *gpasswd* → ändert Gruppenkennwort
- *newgrp* → keine Administration, sondern als neue Gruppe anmelden
  - Neue Shell wird gestartet



Shadow System verwalten

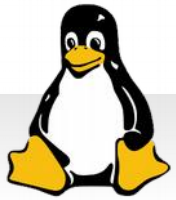
pwconv	erstellt und aktualisiert */etc/shadow*
pwunconv	zurück nach */etc/passwd*
pwck	Konsistenzprüfung, z.B. ob Homes existieren
grpconv	Pendant zu *pwconv*
grpunconv	Pendant zu *pwunconv*
grpck	Pendant zu pwck
getent	Lokale Datenbanken abfragen
id	Benutzer- und Gruppen-IDs abfragen

```
$ getent passwd gschoenb
gschoenb:x:1000:1000:Gschoenb,,,:/home/gschoenb:/bin/bash
$ getent group gschoenb
gschoenb:x:1000:
$ sudo getent shadow gschoenb
gschoenb:
$6$T6JOOVRR$gbVohMpFJh8rrVlhrBZ5NOwd7a9By5eLQoPlkQkkMv3enStrWFdgIWZrvqFPcSFG
0LsuaOL7zOIHOxp5yhXYI/:16057:0:99999:7:::
```



107.2 Automate System Administration Tasks by scheduling Jobs

- */etc/cron.{d,daily,hourly,monthly,weekly}/*
- */etc/at.deny*
- */etc/at.allow*
- */etc/crontab*
- */etc/cron.allow*
- */etc/cron.deny*
- */var/spool/cron/*

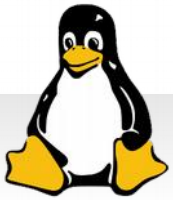


cron

- Gutes Beispiel → *logrotate* (rotiert Log-Dateien)
- Hilfe zu *cron* Dateien

```
$ man 5 crontab
        field          allowed values
        -----          --------------
         minute         0-59
         hour           0-23
         day of month   1-31
         month          1-12 (or names, see below)
         day of week    0-7 (0 or 7 is Sun, or use names)
[…]
00  08   *   *   1-5  $HOME/bin/dosomething
```

- Daemon → *crond*
- Letztes Feld legt auszuführendes Programm fest
- Aufgaben mit cron und atd zeitlich festlegen (debian-handbook.info)



cron

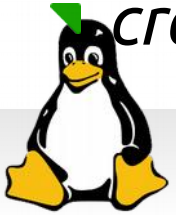
- Skripte in Verzeichnisse werden ausgeführt
  - *sh/bash* Skripte ohne Endung
  - *MAILTO* Variable

```
# grep cron /var/log/syslog
[...]
(root) CMD (   cd / && run-parts --report /etc/cron.hourly)
$ sudo find /etc/ -type d -name '*cron.*'
/etc/cron.monthly
/etc/cron.weekly
/etc/cron.d
/etc/cron.daily
/etc/cron.hourly
```

- *cron.d* erlaubt Angabe eines Users, unter dem Job läuft

```
8 * * * * root if test -x /usr/sbin/apticron; then
/usr/sbin/apticron --cron; else true; fi
```

- *crontab* → fügt Einträge hinzu, listet Einträge auf

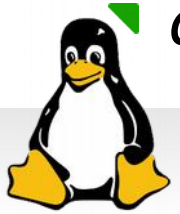


anacron und *at*

- *anacron*
  - Holt verpasste Jobs nach → für Systeme, die nicht ständig laufen
  - */etc/anacrontab*, delay Angabe
- *at* Jobs
  - Jobs einmalig ausführen, via *-f* aus Datei
  - Daemon *atd*
  - *at* → *atrm* → *atq*

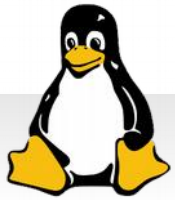
```
$ at 09:00 27.07.16 ...
```

- *cron.allow* → *cron.deny*, *at.allow* → *at.deny*
  - *cron* → Keine von beiden Dateien → alle Benutzer
  - *at* → Keine von beiden Dateien → nur root



107.3 Localisation and Internationalisation

- *tzselect*
- *date*
- *iconv*
- */etc/timezone*
- */etc/localtime*



Zeitzonen und Lokalisation

- *tzselect* verwendet */usr/share/zoneinfo/*
- */etc/localtime* ist Kopie von Dateien in *zoneinfo*
- */etc/timezone* beinhaltet auch Namen der Zone
- Umgebungsvariable *TZ* → vorübergehend setzen

```
$ sudo dpkg-reconfigure tzdata
```

- Umgebungsvariablen Lokalisation

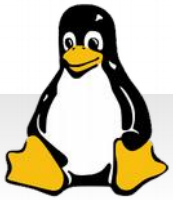
```
$ man locale
$ locale
LANG=en_US.UTF-8
LANGUAGE=
LC_CTYPE="en_US.UTF-8"
[...]
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=en_US.UTF-8
```

- *LC_ALL* / *LC_LANG* überschreiben andere Einträge, *LANG* spring ein → oder überschreibt wenn manuell exportiert

Zeitzonen und Lokalisation

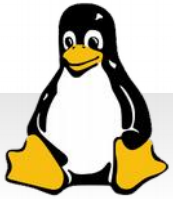
- *locale -a* zeigt Einstellungen an
- */etc/default/locale* → *permanent setzen*
  - *update-locale* setzt Einstellungen
  - *dpkg-reconfigure locales* aktualisert
- *locale-gen* generiert fehlende Locales
- Zeichensätze
  - Via *iconv* konvertieren

```
$ iconv -f UTF-16LE -t UTF-8 transactions_2016-01.csv
```



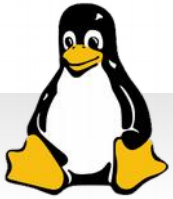
108 Essential System Services

- Systemzeit
- Logging
- MTA Basics



108.1 Maintain System Time

- */usr/share/zoneinfo/*
- */etc/timezone*
- */etc/localtime*
- */etc/ntp.conf*
- *date*
- *hwclock*



date und *ntp*

- *date* → Systemzeit anzeigen und einstellen, Ausgabe generieren
- *hwclock* → --*systohc* → --*hctosys*, Hardware Uhr mit Systemzeit abgleichen

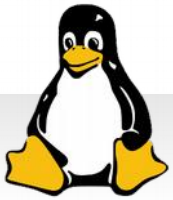
```
$ sudo hwclock --show
Sam 26 Mär 2016 09:17:22 CET  -0.703628 seconds
```

- NTP
  - *ntpdate* → Systemzeit mit NTP synchronisieren
  - *ntpd* → Daemon zum regelmäßigen Update
    - */etc/ntp.conf* und */etc/ntp.drift*

```
server 0.pool.ntp.org
```

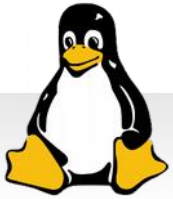
    - *ntpq* → fragt Daemon Einstellungen ab
    - *ntpdc*

```
# ntpdc
ntpdc> sysinfo
system peer:          time2.mediainvent.at
system peer mode:     client
```



108.2 System Logging

- *syslog.conf*
- */var/log/*
- *logrotate*
- */etc/logrotate.conf*
- */etc/logrotate.d/*

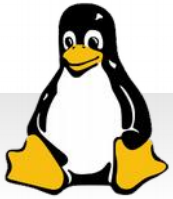


Logging

- *syslogd* (*SysVinit*) und *journald* (*systemd*)
  - Verzeichnis */var/log*
- */etc/syslog.conf* oder */etc/rsyslog.conf*
  - *facility.level action*

facility	Protkollierende Einrichtung (auth, daemon, kern, mail). Auch z.B. local0
level	Grad (debug, info, notice, err)
action	Ziel für Protokollierung

```
mail.err                        /var/log/mail.err
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages
# minus avoids syncing after each log message
```



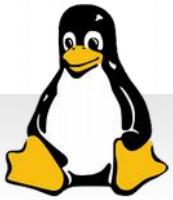
Logdateien

- */var/log* Verzeichnis aufsuchen

```
# tailf /var/log/messages
May 15 08:22:57 lin1 kernel: [    5.544494] RPC: Registered udp transport module.
May 15 08:22:57 lin1 kernel: [    5.544494] RPC: Registered tcp transport module.
[…]
# grep sshd /var/log/auth.log | tail
May  3 20:09:25 lin1 sshd[2366]: pam_unix(sshd:session): session closed for user lin1
May  9 09:30:14 lin1 sshd[2312]: Server listening on 0.0.0.0 port 22.
```

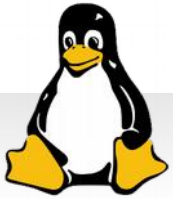
- Mit *logger* können eigene Meldungen geloggt werden

```
# logger -t LPIC1 "Run logger on Debian"
# echo $?
0
# grep LPIC1 /var/log/messages
May 16 09:29:19 lin1 LPIC1: Run logger on Debian
```



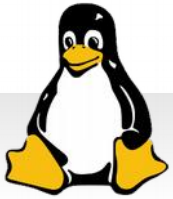
logrotate und *systemd*

- Rotiert Logs, komprimiert sie bei Bedarf auch und hebt sie bestimmte Zeit auf
- */etc/logrotate-.conf*
  - Konfigurationen in *logrotate.d*
- *systemd*
  - Logging via *journald* in */var/log/journal*
  - Keine reinen Text-Dateien → *journalctl* (*-f, -n, -e*)
  - */etc/systemd/journald.conf*
    - *Storage* → Wie wird Journal gespeichert
    - *Compress* → xy-Komprimierung
    - *MaxFileSec* → max. Zeit für Journal-Eintrag



108.3 Mail Transfer Agent (MTA) basics

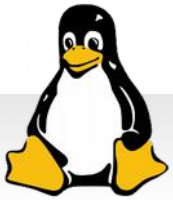
- *newaliases*
- *mail*
- *mailq*
- *postfix*
- *sendmail*



Begriffe

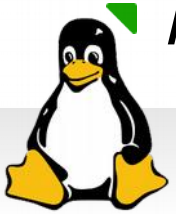
MUA	Mail User Agent (Mail Client)
MDA	Mail Delivery Agent (entscheidet über Mail-Verarbeitung, z.B. Lokal oder Weitergabe an MTA). Bespiele procmail, maildrop.
MTA	Mail Transfer Agent (Zustellung der Mail über SMTP, am Ziel-Server übernimmt MDA). Beispiele sendmail, postfix, qmail, exim.

- Endgültige Auslieferung über IMAP oder POP in Mail-Boxen
- Log-Verzeichnis
  - */var/log/mail*
    - Welche Mails wurden vom System verarbeitet



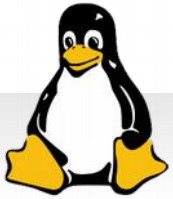
Konfigurations-Dateien

- */etc/aliases* → Nachrichten umleiten, einen Mail-Alias anlegen
- Datei mit *newaliases* neu einlesen, oder *sendmail -bi*
- User kann auch *.forward* erstellen, „Nachsendeauftrag“
- */var/spool/mail* → MDA liefert Mails lokal aus, Benutzer-Mails
  - */var/mail* of symbolischer Link
- */var/spool/mqueue* → MDA holt Nachrichten aus Warteschlange
- */etc/mail/sendmail.cf*
- */etc/postfix*
  - *main.cf* → *myhostname, mydomain*
  - *master.cf* → *postfix interne Konfiguration*



108.4 Manage Printers and Printing

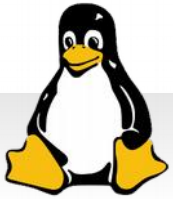
- CUPS
- User print Queues
- *lpd*



Druckersystem

- Queue oder Spooler
- LPD → Line Printer Daemon (*lpd* oder *cups*)
  - Lokal oder an anderen Hosts
- Queue in */etc/printcap* oder */var/run/cups/printcap*
  - Liegt unter */var/spool*
  - Device → */dev/lp0*

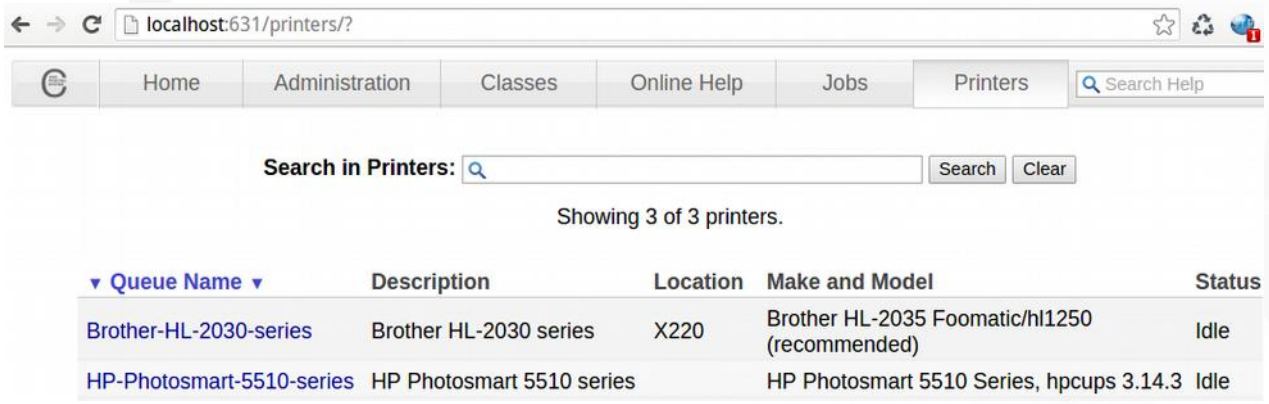
lpr	Aufträge an Drucker senden
lpq	Zeigt Warteschlangen an
lprm	Löscht Aufträge in Warteschlangen
lpc	Interaktive Kommandos, start, stop, status, topq
lpstat	Status Informationen
lpoptions	Drucker Einstellungen anzeigen und setzen
lpadmin	Drucker einrichten
lpinfo	Verfügbare Drucker PPD

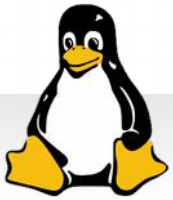


CUPS

- *CUPS* → Common Unix Printing System
  - Basiert auf *IPP*, Internet Printing Protokoll
  - HTTP Server für IPP Requests
  - */etc/cups* → Web-Interface lokal Port 631
- *CUPS* Versionen der Kommandos
  - *lp* und *lpr*

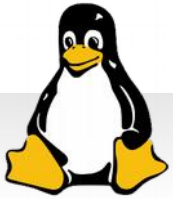
```
$ lpr -o sides=two-sides-long-edge manual.pdf
$ lpr -o landscape sign.ps
```





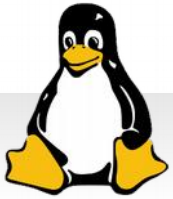
CUPS

- Daten werden in Postscript umgewandelt
  - *mime.types* → erkennt Format
  - *mime.convs* → Zumeist *pstops (CUPS* spezifisch*)*
- Postscript wird drucker-spezifisch umgewandelt
  - PCL oder ESC/P mit Ghostscript
  - Über Backends zu Drucker(-Server) → */usr/lib/cups/backend*
- *PPD* Dateien
  - Printer Description, was unterstützt Drucker
- */etc/cups/printers.conf*
- */etc/cups/cupsd.conf*
  - *Allow* für Netzwerk



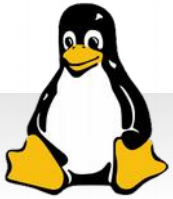
109 Networking Fundamentals

- TCP, UDP
- Ports und Services
- Subnetting

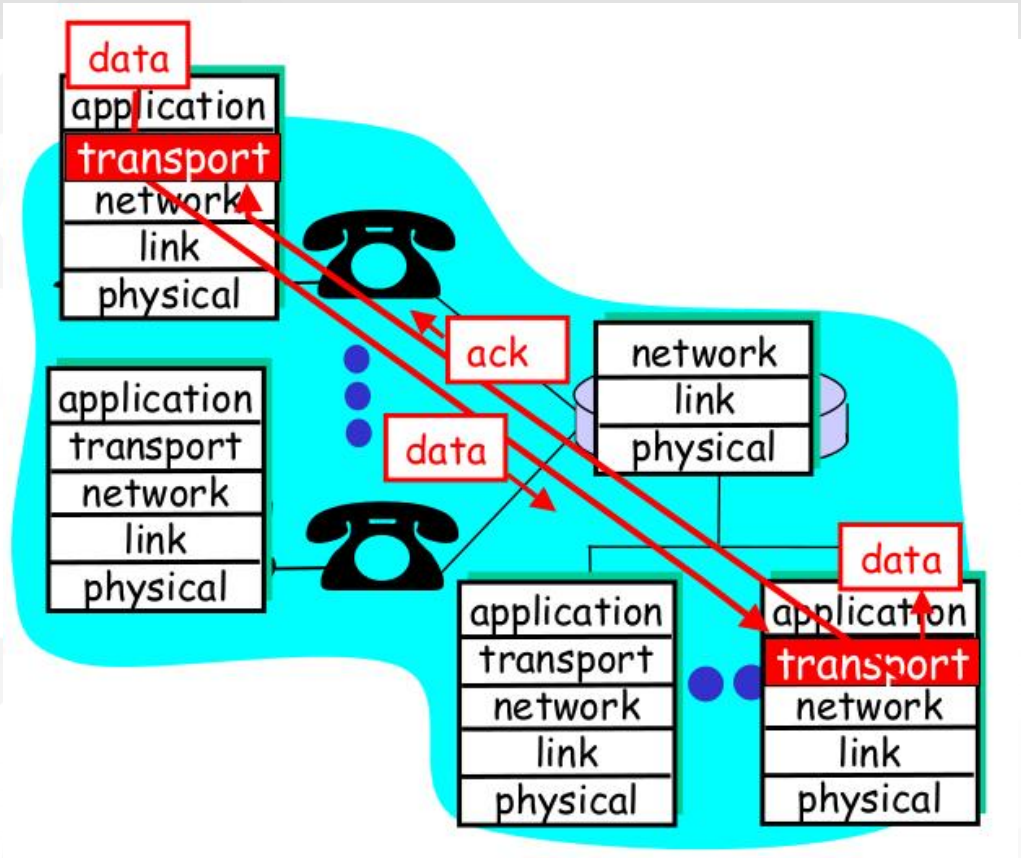


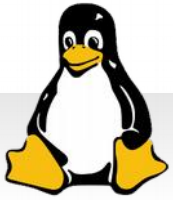
109.1 Fundamentals of internet protocols

- */etc/services*
- IPv4, IPv6
- Subnetting
- TCP, UDP, ICMP

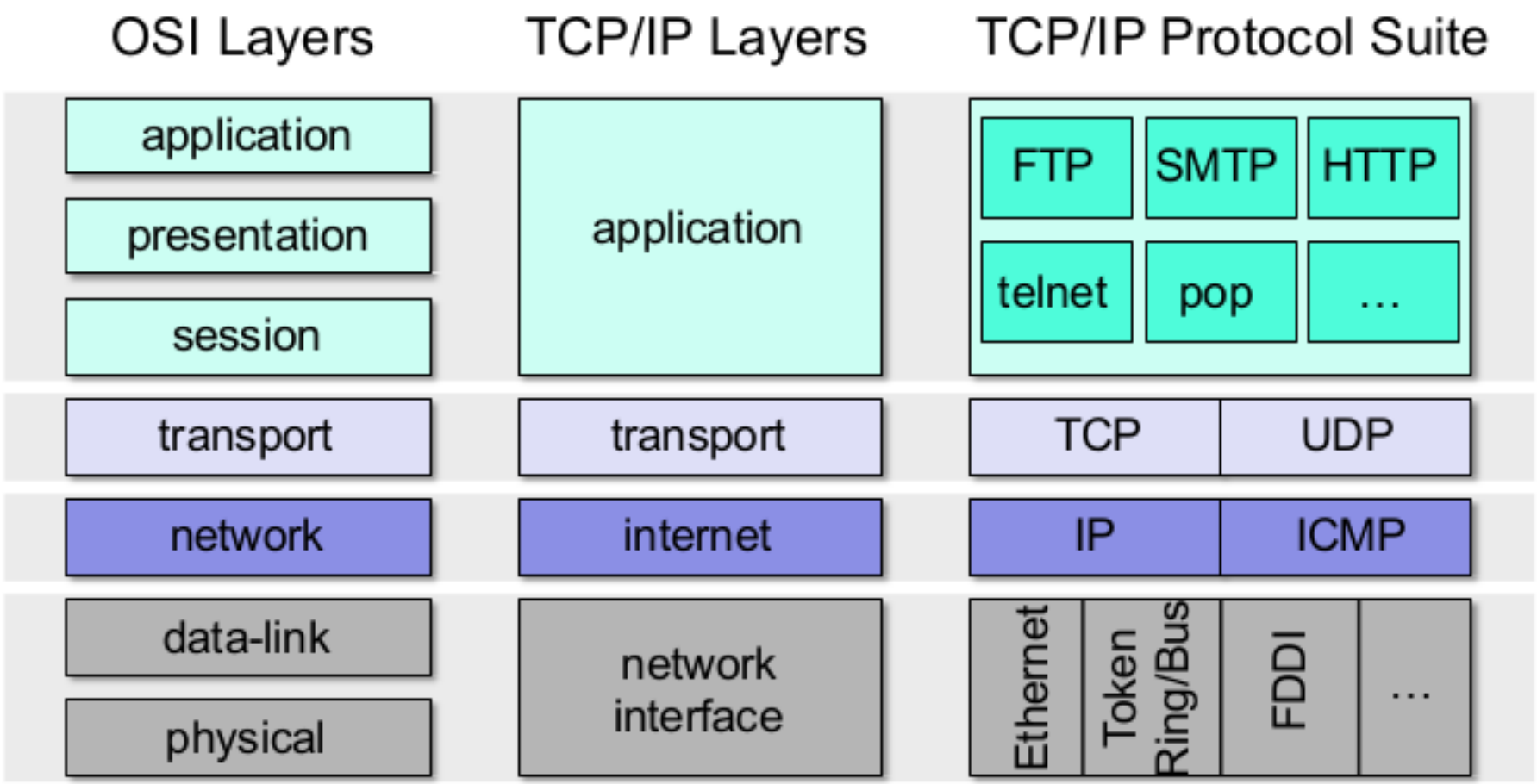


Schichtenmodell

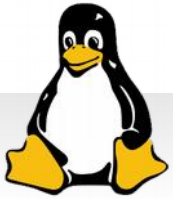




Schichtenmodell



http://ti.tuwien.ac.at/cps/teaching/courses/deterministic-networking/lecture-slides/detnet01_networking_basics.pdf , F. 23



TCP

- Transmission Control Protocol
- Setzt Segmente ein
- Zuverlässig, verbindungsorientiert, paket-vermittelnd
- Implementierung der Transportschicht
- 3 Wege Handshake

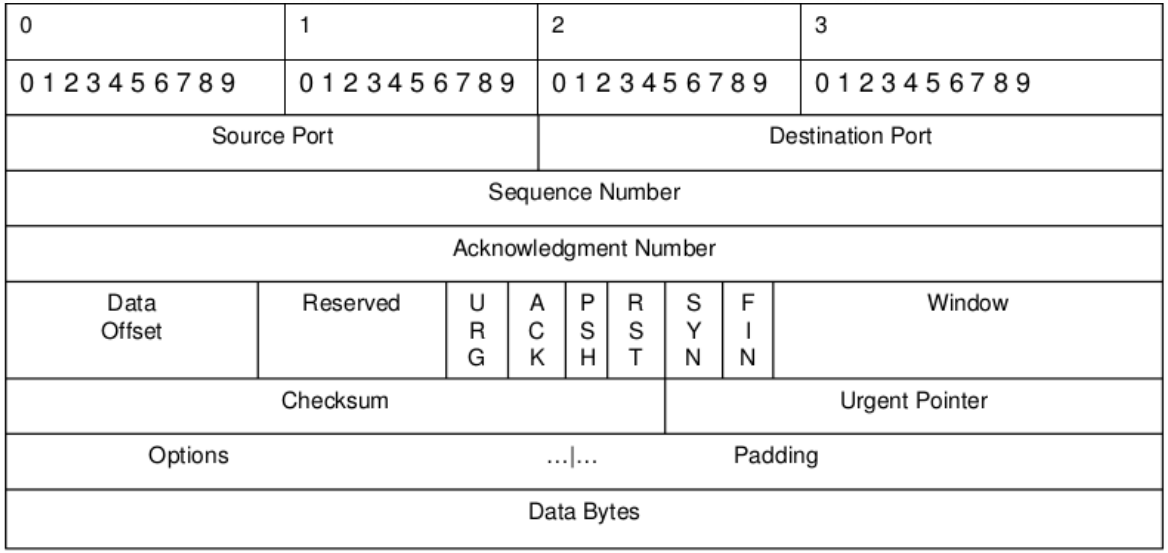
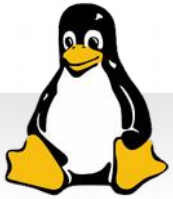


Figure 4-10 TCP: Segment format

IBM TCP/IP Tutorial and Technical Overview, S. 150

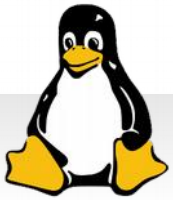


UDP und IP

- UDP
  - UDP Datagram, Verbindungslos, unabhängige Pakete
  - Kein Handshake, Kein Flow Control
- IP Datagram, verbindungslos und nicht verlässlich
  - v4 32 Bit, v6 128 Bit Adressen
- ARP

```
$ ip neighbour show
$ arp
```

```
:~$ ipcalc 10.0.0.1/24
Address:   10.0.0.1             00001010.00000000.00000000. 00000001
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   10.0.0.0/24          00001010.00000000.00000000. 00000000
HostMin:   10.0.0.1             00001010.00000000.00000000. 00000001
HostMax:   10.0.0.254           00001010.00000000.00000000. 11111110
Broadcast: 10.0.0.255           00001010.00000000.00000000. 11111111
Hosts/Net: 254                   Class A, Private Internet
```



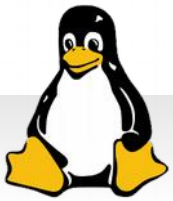
Subnetting

- CIDR erlaubt Aufteilung in Netze

```
Network:   156.17.4.64/26          10011100.00010001.00000100.01 000000
Netmask:   255.255.255.192 = 26    11111111.11111111.11111111.11 000000
HostMin:   156.17.4.65             10011100.00010001.00000100.01 000001
HostMax:   156.17.4.126            10011100.00010001.00000100.01 111110
                                =
Network:   156.17.4.64/27          10011100.00010001.00000100.010 00000
Netmask:   255.255.255.224 = 27    11111111.11111111.11111111.111 00000
HostMin:   156.17.4.65             10011100.00010001.00000100.010 00001
HostMax:   156.17.4.94             10011100.00010001.00000100.010 11110
                                +
Network:   156.17.4.96/27          10011100.00010001.00000100.011 00000
Netmask:   255.255.255.224 = 27    11111111.11111111.11111111.111 00000
HostMin:   156.17.4.97             10011100.00010001.00000100.011 00001
HostMax:   156.17.4.126            10011100.00010001.00000100.011 11110
```

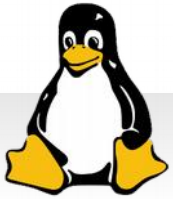
Ports

```
$ grep -E '\s20\/|\s21\/|\s22\/|\s23\/|\s25\/|\s53\/|
\s80\/|\s110\/|\s123\/|\s139\/|\s143\/|\s161\/|\s162\/|
\s389\/|\s443\/|\s465\/|\s514\/|\s636\/|\s993\/|\s995\/' /etc/services
ftp-data  20/tcp
ftp       21/tcp
fsp       21/udp        fspd
ssh       22/tcp                  # SSH Remote Login Protocol
ssh       22/udp
telnet         23/tcp
smtp      25/tcp        mail
domain         53/tcp                  # Domain Name Server
domain         53/udp
http      80/tcp        www       # WorldWideWeb HTTP
http      80/udp                  # HyperText Transfer Protocol
pop3      110/tcp       pop-3          # POP version 3
pop3      110/udp       pop-3
ntp       123/tcp
ntp       123/udp                 # Network Time Protocol
netbios-ssn    139/tcp                 # NETBIOS session service
netbios-ssn    139/udp
imap2          143/tcp       imap      # Interim Mail Access P 2 and 4
imap2          143/udp       imap
snmp      161/tcp                 # Simple Net Mgmt Protocol
snmp      161/udp
snmp-trap 162/tcp       snmptrap  # Traps for SNMP
snmp-trap 162/udp       snmptrap
ldap      389/tcp           # Lightweight Directory Access Protocol
ldap      389/udp
https          443/tcp                 # http protocol over TLS/SSL
https          443/udp
urd       465/tcp       ssmtp smtps  # URL Rendesvous Directory for SSM
shell          514/tcp       cmd       # no passwords used
syslog         514/udp
ldaps          636/tcp                 # LDAP over SSL
ldaps          636/udp
imaps          993/tcp                 # IMAP over SSL
imaps          993/udp
pop3s          995/tcp                 # POP-3 over SSL
pop3s          995/udp
```



109.2 Basic Network Configuration

- */etc/hostname*
- */etc/hosts*
- */etc/nsswitch.conf*
- *ifconfig*
- *ifup*
- *ifdown*
- *ip*

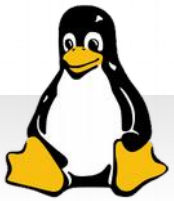


Konfiguration

- *hostname* und *hosts*
- *resolv.conf*
  - Nameserver, Domain (inkl. *search* → auto append)
- *nsswitch.conf*
  - Verhalten von Applikationen, z.B. PAM (LDAP AUTH)
- *ifconfig*
- *ifup* und *ifdown*
- *route* für Routing-Tabellen
  - *add default gw, add -net*

```
root@lin1:~# cat /etc/hostname
lin1
# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    lin1
```

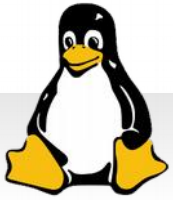
```
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
10.0.2.0        *               255.255.255.0   U     0      0        0 eth0
192.168.56.0    *               255.255.255.0   U     0      0        0 eth1
```



Kommando *ip*

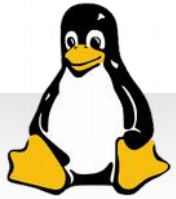
- Linux ip Kommando (thomas-krenn.com)
- *arp*
  - *-n* → numerische Ausgabe
  - *ip neighbour show*
- *ping*
  - *-c* → Count, Anzahl der Pings
  - -U → User zu User Latenz
  - Response Time und TTL
  - Für IPv6 *ping6*
- *mtr*

```
$ mtr -c 25 -r -n -b 8.8.8.8
Start: Sat Mar 26 17:21:40 2016
HOST: gschoenb-T410                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.0.138                  0.0%    25    5.5   9.5   2.7  31.6   7.2
  2.|-- 93.82.71.254                84.0%    25  20880 20818 20721 20880  68.7
  3.|-- 195.3.66.149                 0.0%    25   50.7  48.1  21.5  99.8  26.4
```



109.3 Basic Network Troubleshooting

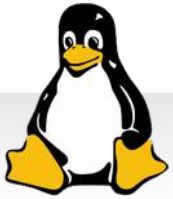
- *ifconfig*
- *ip*
- *ifup*
- *ifdown*
- *route*
- *host*
- *hostname*
- *dig*



Fehlersuche

- Mehrere Schritte sinnvoll

ip (ifconfig)	Netzwerkkonfiguration und Interfaces prüfen
ping	ICMP Echo Requests, localhost, default Gateway, Outside Hosts
traceroute	Response Time und TTL, -n unterdrückt Namensauflösung
tracepath, tracepath6	Routen prüfen, inkl. MTU, auch für IPv6
netstat	Diagnose-Programm, am besten filtern
nmap	Port Scanner, per Default TCP SYN Scan
telnet	Logon via telnet Protokoll
nslookup, dig	Namensauflösung

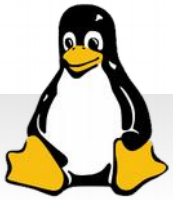


Fehlersuche

- Suche von Hops zwischen Hosts
- *tracepath* → untersucht zusätzlich MTU
- *netstat* → anzeigen von Verbindungen

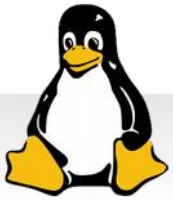
```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

```
$ traceroute -n 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.0.138  8.206 ms  8.146 ms  8.039 ms
 2  93.82.71.254  28.667 ms  36.018 ms  59.344 ms
 3  195.3.66.149  28.479 ms  28.479 ms  28.437 ms
```



109.3 Configure Client side DNS

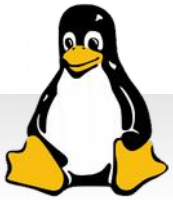
- */etc/hosts*
- */etc/resolv.conf*
- */etc/nsswitch.conf*
- *host*
- *dig*



DNS Abfragen

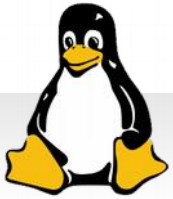
host	Einfache Abfragen inkl. Reverse-Lookup, auch Typ mit -t möglich, verwendet /etc/resolv.conf
dig	DNS Server wählbar, umfangreich
nslookup	Soll irgendwann abgelöst werden, interaktiv
getent hosts	hosts Datenbank abfragen

```
# host -t MX orf.at
orf.at mail is handled by 10 orfmx02.t-systems.at.
# dig www.orf.at @194.232.104.139
# dig -x 194.232.104.142
```



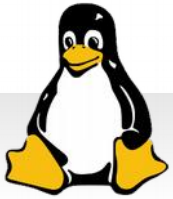
110 Security

- Host Security
- Verschlüsselung



110.1 Perform Security Administration Tasks

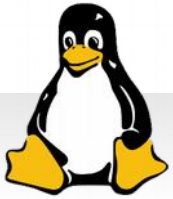
- *find*
- *fuser*
- *lsof*
- *nmap*
- *chage*
- *sudo*
- */etc/sudoers*



Systeme absichern

- Permissions mit *find* prüfen
  - *u+s, g+s*
  - *noexec, nosuid*
- *nmap*, *netstat*
- *socket*
  - Web-Server simulieren
- Offene Dateien mit *lsof*
- Dateien und Sockets mit *fuser*

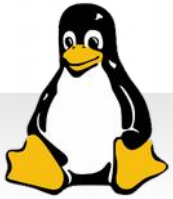
```
# lsof /home/
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
bash    2416 lin1  cwd    DIR    8,9     4096   12 /home/lin1
sudo    2638 root  cwd    DIR    8,9     4096   12 /home/lin1
```



System absichern

- Ressourcenverwendung
  - *ulimit* in */etc/profile*
- Hard und Soft Limits

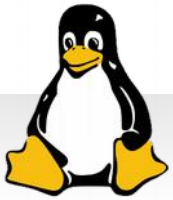
```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
[…]
# ulimit -c 20000
# ulimit -d 15000
# help ulimit
[...]
    Options:
      -S use the `soft' resource limit
      -H use the `hard' resource limit
      -a all current limits are reported
      -b the socket buffer size
      -c the maximum size of core files created
      -d the maximum size of a process's data segment
      -e the maximum scheduling priority (`nice')
```



Offene Dateien

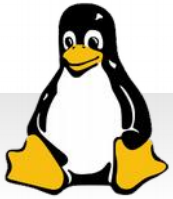
- *lsof* PATH
  - *-t* → Übergabe an *kill* mit terse Output
  - *-i :80* → Prozesse mit Netzwerk-Verbindungen
- *fuser*

```
# fuser -m -u /home/lin1
/home/lin1:           2408c(lin1)  2524c(root)  2805c(lin1)
# ps aux | grep 2805
lin1      2805  0.0  0.6  20476  3192 tty1     S+   21:17   0:00 -bash
# fuser -n tcp 80
80/tcp:               3077
# ps aux| grep 3077
root      3077  0.0  0.1   6176   660 pts/0    S+   21:40   0:00 socket -sl 8
```



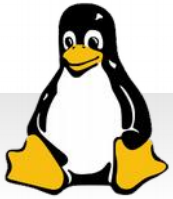
Superuser und angemeldete User

- *su* → *exit*
- *su -l* → zu Benutzer Environment wechseln
- *sudo* → Befehl mit Superuser Rechten ausführen
- *visudo* → */etc/sudoers*
- Angemeldete User
  - *w* → Wer ist aktuell angemeldet
  - *who*
  - *last* → */var/log/wtmp*
    - Wer war zuletzt angemeldet
- */etc/nologin*
  - Verhindern, dass sich Benutzer interaktiv anmeldet



110.2 Setup Host Security

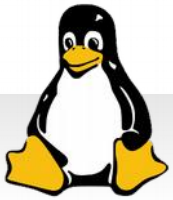
- */etc/nologin*
- */etc/passwd*
- */etc/shadow*
- */etc/xinetd.d/*
- */etc/xinetd.conf*
- */etc/inetd.d/*
- */etc/inetd.conf*



inetd und *xinetd*

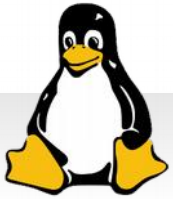
- Weniger frequentierte Hosts (FTP, SMTP) über *inetd* oder *xinetd* laufen lassen
- Lauscht stell-vertretend an Ports der Services
  - TCP Wraper führt Ziel-Service aus
- *inetd*
  - */etc/inetd.conf*
  - *tcpdchk* → Konfiguration prüfen
- *xinetd*
  - Nachfolger von *inetd*

```
# ls /etc/xinetd.*
/etc/xinetd.conf

/etc/xinetd.d:
chargen  daytime  discard  echo  time
```



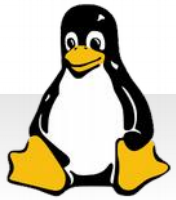
TCP Wrapper

- *xinetd* Integriert TCP-Wrapper
- TCP-Wrapper Konfiguration gilt für beide
- */etc/hosts.allow* → gibt es darin zutreffende Regel, wird Zugriff erlaubt (egal ob es zugeöriges *deny* gibt)
- */etc/hosts.deny* → Gibt es zutreffende Regel, wird Zugriff verweigert
  - *ALL : ALL*
- Keine Einträge in beiden → Zugriff erlaubt
- Ist eine Datei nicht vorhanden → wie Datei leer



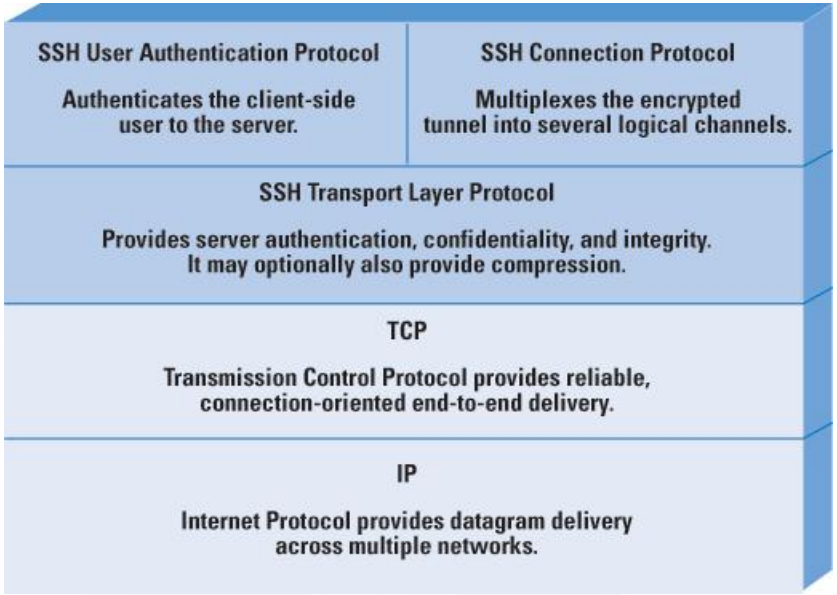
110.3 110.3 Securing Data with Encryption

- *ssh*
- *ssh-keygen*
- *~/.ssh/id_rsa and id_rsa.pub*
- *~/.ssh/id_dsa and id_dsa.pub*
- *~/.ssh/authorized_keys*
- *ssh_known_hosts*
- *gpg*



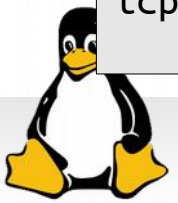
SSH

- Secure Shell Server
  - *ssh SERVER*
  - *ssh USER@SERVER*
  - *ssh -l USER SERVER*
  - *ssh -l USER -p PORT SERVER*
  - *ssh -X USER@SERVER*
- SSH Forwarding
- Open SSH Client, Putty



http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_12-4/124_ssh_fig01_lg.jpg

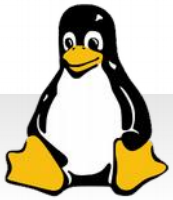
```
$ sudo service ssh status
[ ok ] sshd is running.
$ sudo netstat -tlnp | grep ssh
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2660/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      2660/sshd
```



Konfigurations-Dateien

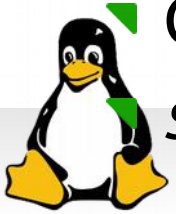
/etc/ssh/sshd_config	SSH Server, Port, Protocol Version, ListenAddress
/etc/ssh/ssh_config	Client-seitige Konfiguration
/etc/ssh/ssh_known_hosts	Öffentl. Schlüssel bekannter Hosts
/etc/sshrc oder */etc/ssh/sshrc*	Skript, dass vor Laden der Shell bei SSH-Auth ausgeführt wird

- Auch über *hosts.allow* und *hosts.deny* einschränkbar
- *known_hosts*
  - Server präsentiert Fingerprint
  - Prüfen ob Host wirklich der richtige ist (MITM)



Public Key Authentifizierung

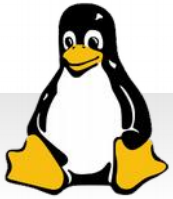
- OpenSSH Public Key Authentifizierung unter Ubuntu (thomas-krenn.com)
- *ssh-keygen*
  - *-t* → Typ
  - *-b* → Bitlänge
  - -A → Für Host Keys (*strict checking)*
- Passphrase verwenden → Private Key wird verschlüsselt
  - *.pub* ist zugehöriger Public Key
- Public Key in *authorized_keys* eintragen → Auth. am Zielsystem erlauben
  - *ssh-copy-id*
  - Copy-Paste des Public Keys
  - *ssh-agent* und *ssh-add*



GnuPG

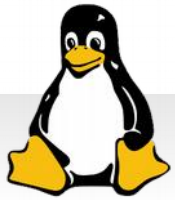
- GNU Privacy Guard
  - Asymmetrische Verschlüsselung
  - Signaturen
- Kommandos
  - Konfiguration in *.gnupg*

gpg --gen-key	*Schlüssel generieren*
gpg --encrypt	*Verschlüsseln*
gpg --decrypt	*Entschlüsseln*
gpg --gen-revoke	*Widerrufs-Zertifikat erstellen*
gpg --import	*Schlüssel importieren*
gpg --export --armor	*Schlüssel als Text exportieren*
gpg -r	*Receiver angeben*



Abschließende Fragen?

- Ansonsten danke für die Teilnahme an LPIC-1!



Copyright

- Folien
  - Autor: Georg Schönberger
- Libreoffice Template
  - Lizenz: CC-by-sa-v3
  - LibreOffice Presentation Templates 1.0 (templates.libreoffice.org)
- Tux-Grafik
  - Autor: Larry Ewing
  - Tux-simple.svg (commons.wikimedia.org)