HOCHSCHULE MITTWEIDA
University of Applied Sciences

Bundeskriminalamt

Betriebssysteme
Linux Grundlagen 2

Autor: Felix Fischer
Referent: Tim Wetterau
Stand: 11.05.2023

hs-mittweida.de

Agenda

1. Netzwerk-Konfiguration
2. Dateisysteme Überblick
3. Benutzer und Gruppen
4. Nutzungsverlauf

Netzwerk-Konfiguration

Interface-Konfiguration

- Für Debian/Ubuntu unter: /etc/network/interfaces
- Statische Konfiguration:

```
auto eth0
iface eth0 inet static
        address 192.168.0.100
        netmask 255.255.255.0
        gateway 192.168.0.1
```

Automatisch interface up bei physischer Verbindung

Interface eth0 statisch mit IPv4 konfigurieren

Zugewiesene IP-Adresse

Subnetzmaske (Netzwerkgröße)

Weiterleitungsknoten für externe Netzwerke

(C) 15.06.2023 Hochschule Mittweida

Interface-Konfiguration

- Für Debian/Ubuntu unter: /etc/network/interfaces
- dynamische Konfigurierung:

```
auto eth0
iface eth0 inet6 dhcp
```

  - Interface eth0 IPv6-Konfiguration über DHCP
  - DHCP-Optionen liefern DNS, …

- **IP-Konfiguration auslesen**
  - `ifconfig -a`
  - `netstat -ei`
  - `ip address`
- **Aktive Verbindungen und lauschende Ports auslesen**
  - `nestat –tulpen`
- **Statische Routen auslesen**
  - `route`

(C) 15.06.2023 Hochschule Mittweida

Interface-Konfiguration

- Für SUSE unter: /etc/sysconfig/network/<if>
- Statische Konfigurierung:

```
BOOTPROTO='static'
IPADDR='192.168.0.100'
MTU='1500'
NAME=''
NETMASK='255.255.255.0'
STARTMODE='auto'
USERCONTROL='no'
```

- Jedes Interface eigene Datei
- Dateiname ist interfacename

- Statische IP
- Maximal Transmission Unit (Nutzlastgröße)
- Automatisch interface up bei physischer Verbindung
- Einstellung über GUI nicht möglich

(C) 15.06.2023 Hochschule Mittweida

WLAN-Netzwerke

- **WLAN-Manager**
  - Konfiguration für Login
  - Passwort im Klartext
- Ubuntu: `/etc/NetworkManager/<WLAN-SSID>`
- Debian/SUSE: `/etc/wpa_supplicant/wpa_supplicant.conf`
- Red Hat/Fedora: `/etc/NetworkManager/<WLAN-SSID>`

→ **Konfiguration über eigenes Tool: `nmcli`**

(C) 15.06.2023 Hochschule Mittweida

Dateisysteme Überblick

Unterstützte Dateisysteme

```
Type search string, or <Enter> to show all codes:
0700 Microsoft basic data                  0c01 Microsoft reserved
2700 Windows RE                            3000 ONIE boot
3001 ONIE config                           3900 Plan 9
4100 PowerPC PReP boot                     4200 Windows LDM data
4201 Windows LDM metadata                  4202 Windows Storage Spaces
7501 IBM GPFS                              7f00 ChromeOS kernel
7f01 ChromeOS root                         7f02 ChromeOS reserved
8200 Linux swap                            8300 Linux filesystem
8301 Linux reserved                        8302 Linux /home
8303 Linux x86 root (/)                    8304 Linux x86-64 root (/)
8305 Linux ARM64 root (/)                  8306 Linux /srv
8307 Linux ARM32 root (/)                  8308 Linux dm-crypt
8309 Linux LUKS                            830a Linux IA-64 root (/)
830b Linux x86 root verity                 830c Linux x86-64 root verity
830d Linux ARM32 root verity               830e Linux ARM64 root verity
830f Linux IA-64 root verity               8310 Linux /var
8311 Linux /var/tmp                        8400 Intel Rapid Start
8500 Container Linux /usr                  8501 Container Linux resizable rootfs
8502 Container Linux /OEM customization    8503 Container Linux root on RAID
8e00 Linux LVM                             a000 Android bootloader
a001 Android bootloader 2                  a002 Android boot 1
Press the <Enter> key to see more codes, q to quit:
a003 Android recovery 1                    a004 Android misc
a005 Android metadata                      a006 Android system 1
a007 Android cache                         a008 Android data
a009 Android persistent                    a00a Android factory
a00b Android fastboot/tertiary             a00c Android OEM
a00d Android vendor                        a00e Android config
a00f Android factory (alt)                 a010 Android meta
a011 Android EXT                           a012 Android SBL1
a013 Android SBL2                          a014 Android SBL3
a015 Android APPSBL                        a016 Android QSEE/tz
a017 Android QHEE/hyp                      a018 Android RPM
a019 Android WDOG debug/sdi                a01a Android DDR
a01b Android CDT                           a01c Android RAM dump
a01d Android SEC                           a01e Android PMIC
a01f Android misc 1                        a020 Android misc 2
a021 Android device info                   a022 Android APDP
```

```
a023 Android MSADP                         a024 Android DPO
a025 Android recovery 2                    a026 Android persist
a027 Android modem ST1                     a028 Android modem ST2
a029 Android FSC                           a02a Android FSG 1
a02b Android FSG 2                         a02c Android SSD
Press the <Enter> key to see more codes, q to quit:
a02d Android keystore                      a02e Android encrypt
a02f Android EKSST                         a030 Android RCT
a031 Android spare1                        a032 Android spare2
a033 Android spare3                        a034 Android spare4
a035 Android raw resources                 a036 Android boot 2
a037 Android FOTA                          a038 Android system 2
a039 Android cache                         a03a Android user data
a03b LG (Android) advanced flasher         a03c Android PG1FS
a03d Android PG2FS                         a03e Android board info
a03f Android MFG                           a040 Android limits
a200 Atari TOS basic data                  a500 FreeBSD disklabel
a501 FreeBSD boot                          a502 FreeBSD swap
a503 FreeBSD UFS                           a504 FreeBSD ZFS
a505 FreeBSD Vinum/RAID                    a580 Midnight BSD data
a581 Midnight BSD boot                     a582 Midnight BSD swap
a583 Midnight BSD UFS                      a584 Midnight BSD ZFS
a585 Midnight BSD Vinum                    a600 OpenBSD disklabel
a800 Apple UFS                             a901 NetBSD swap
a902 NetBSD FFS                            a903 NetBSD LFS
a904 NetBSD concatenated                   a905 NetBSD encrypted
a906 NetBSD RAID                           ab00 Recovery HD
Press the <Enter> key to see more codes, q to quit:
af00 Apple HFS/HFS+                        af01 Apple RAID
af02 Apple RAID offline                    af03 Apple label
af04 AppleTV recovery                      af05 Apple Core Storage
af06 Apple SoftRAID Status                 af07 Apple SoftRAID Scratch
af08 Apple SoftRAID Volume                 af09 Apple SoftRAID Cache
af0a Apple APFS                            b300 QNX6 Power-Safe
bc00 Acronis Secure Zone                   be00 Solaris boot
bf00 Solaris root                          bf01 Solaris /usr & Mac ZFS
bf02 Solaris swap                          bf03 Solaris backup
bf04 Solaris /var                          bf05 Solaris /home
bf06 Solaris alternate sector              bf07 Solaris Reserved 1
bf08 Solaris Reserved 2                    bf09 Solaris Reserved 3
```

```
bf0a Solaris Reserved 4                    bf0b Solaris Reserved 5
c001 HP-UX data                            c002 HP-UX service
e100 ONIE boot                             e101 ONIE config
e900 Veracrypt data                        ea00 Freedesktop $BOOT
eb00 Haiku BFS                             ed00 Sony system partition
ed01 Lenovo system partition               ef00 EFI system partition
ef01 MBR partition scheme                  ef02 BIOS boot partition
f800 Ceph OSD                              f801 Ceph dm-crypt OSD
f802 Ceph journal                          f803 Ceph dm-crypt journal
Press the <Enter> key to see more codes, q to quit:
f804 Ceph disk in creation                 f805 Ceph dm-crypt disk in creation
f806 Ceph block                            f807 Ceph block DB
f808 Ceph block write-ahead log            f809 Ceph lockbox for dm-crypt keys
f80a Ceph multipath OSD                    f80b Ceph multipath journal
f80c Ceph multipath block 1                f80d Ceph multipath block 2
f80e Ceph multipath block DB               f80f Ceph multipath block write-ahead l
f810 Ceph dm-crypt block                   f811 Ceph dm-crypt block DB
f812 Ceph dm-crypt block write-ahead lo    f813 Ceph dm-crypt LUKS journal
f814 Ceph dm-crypt LUKS block              f815 Ceph dm-crypt LUKS block DB
f816 Ceph dm-crypt LUKS block write-ahe    f817 Ceph dm-crypt LUKS OSD
fb00 VMWare VMFS                           fb01 VMWare reserved
fc00 VMWare kcore crash protection         fd00 Linux RAID
```

Filesysteme unterstützt von gdisk

Linux unterstützt fast alle Filesysteme

(C) 15.06.2023 Hochschule Mittweida

Wichtige Dateisysteme

Dateisystem		technischer Stand	Von Betriebssystem unterstützt	Rechteverwaltung	Journaling
Btrfs		Standard in Suse Linux, optional bei allen Distributionen seit 2014	Linux,ReactOS	✔	Nur Metadaten
ext...	...2	Ehemaliges Standarddateisystem, sehr ausgereift, aber aufgrund fehlender Journal-Funktion sehr langsam bei den Dateisystem-Checks	Linux; BSD; Windows mit ext2fd oder ExtFS für Windows; MacOS X mit ExtFS-Treiber	✔	✘
	...3	Ehemaliges Standarddateisystem	Linux; BSD; Windows mit ext2fsd oder ExtFS für Windows; MacOS X mit ExtFS-Treiber	✔	✔
	...4	Aktuelles Standarddateisystem für Ubuntu	Linux; Windows mit ext2fd oder ExtFS für Windows; MacOS X mit ExtFS-Treiber	✔	✔
JFS		Kompromiss aus Schnelligkeit und Sicherheit	Linux; Unix; OS/2	✔	Nur Metadaten
ReiserFS		war lange Standarddateisystem vieler Distributionen	Linux; BSD; Windows mit kommerz. Zusatztreiber	✔	✔
Reiser4		experimentell, schon sehr lange in der Entwicklung	Linux (nur mit Kernelpatch)	✔	✔
XFS		ausgereift und stabil, im Desktop-Bereich aber nicht sehr verbreitet	Linux; Unix; BSD	✔	✔
FAT...	...12	Dateisysteme von Microsoft, als Installationsdateisystem für Linux nicht geeignet	Windows; Linux; BSD; Mac OS	✘	✘
	...16			✘	✘
	...32			✘	✘
exFAT		proprietär, speziell für Flash-Speicher, als Installationsdateisystem für Linux nicht geeignet	Windows; Linux, FreeBSD via FUSE-Treiber; Mac OS	✘	✘
NTFS		das Standarddateisystem von Windows XP, Vista, 7 und 8, als Installationsdateisystem für Linux nicht geeignet	Windows; Linux; BSD; Mac OS	in Linux nur bedingt verwendbar*	Nur Metadaten
ZFS		Standarddateisystem unter Solaris	Solaris; Linux; BSD	✔	✔

Quelle: https://wiki.ubuntuusers.de/Dateisystem/

/etc/fstab

- Beschreibung von Dateisystemen und deren Mount-Points
- Gleiche Einbindung nach
  - Neustart
  - Neuer Verbindung im Betrieb (USB-Stick, externe Festplatte, Netzwerkshare)
- Zeilenweise Einträge
  - Nur manuelle Einträge
  - Kennung (Devicepfad, UUID)
  - Tab oder Leerzeichen als Trennung
  - # als Kommentar
  - Leerzeilen werden ignoriert

(C) 15.06.2023 Hochschule Mittweida

/etc/fstab Eintrag

UUID=03b77228-ed4c-4218-910e-11b9f77c4b46 /backup ext4 defaults 0 2

Eindeutige Hardwarekennung

Alternativ: /dev/sda1 (ist abhängig von Verbindungsreihenfolge)

Mountingpoint (Einbindung ins FHS)

None = Swap (Auslagerungsspeicher)

Leerzeichen = \040

Tab = \011

Filesystemtyp

Optionen (nur Kommatrennung)

defaults = rw,suid,dev,exec,auto, nouser,async

Backup mit dump?

0 = nein, 1 = ja

Überprüfungsreihenfolge bei Boot

0 = keine Überprüfung

1 = zuerst (meist Root-FS)

2 = anschließend (meist zusätzliche Datenträger)

(C) 15.06.2023 Hochschule Mittweida

Partitionieren

fdisk

- Kommandozeilenprogramm
- Kennt Partitionierung mit
  - MBR (Master Boot Record) → als DOS bezeichnet
  - GPT (Globally Unique Identifier Partitioning Table)
  - SGI (Sillicon Graphics and Irix Partitionierung)
  - Sun (Sun Systems Partitionierung)

gdisk

- Kommandozeilenprogramm
- Kennt Partitionierungen mit
  - MBR (Master Boot Record)
  - BSD (auch BSD-Disklabel)
  - APM (Apple Partitioning Map)
  - GPT (Globally Unique Identifier Partitioning Table)

(C) 15.06.2023 Hochschule Mittweida

Formatieren

mkfs

- Kurz für: make filesystem
- Kommandozeilenprogramm
- Partition Formatieren
- Filesystem spezifische Unterprogramme
  - mkfs.bfs
  - mkfs.ext2
  - mkfs.ext3
  - mkfs.ext4
  - mkfs.msdos
  - mkfs.minix
  - mkfs.vfat

Beispiele:

```
mkfs -t ext4 /dev/sdb1
```

- 2. Festplatte
- 1. Partition
- Formatierung mit ext4

```
mkfs -t ntfs /dev/sdc4
```

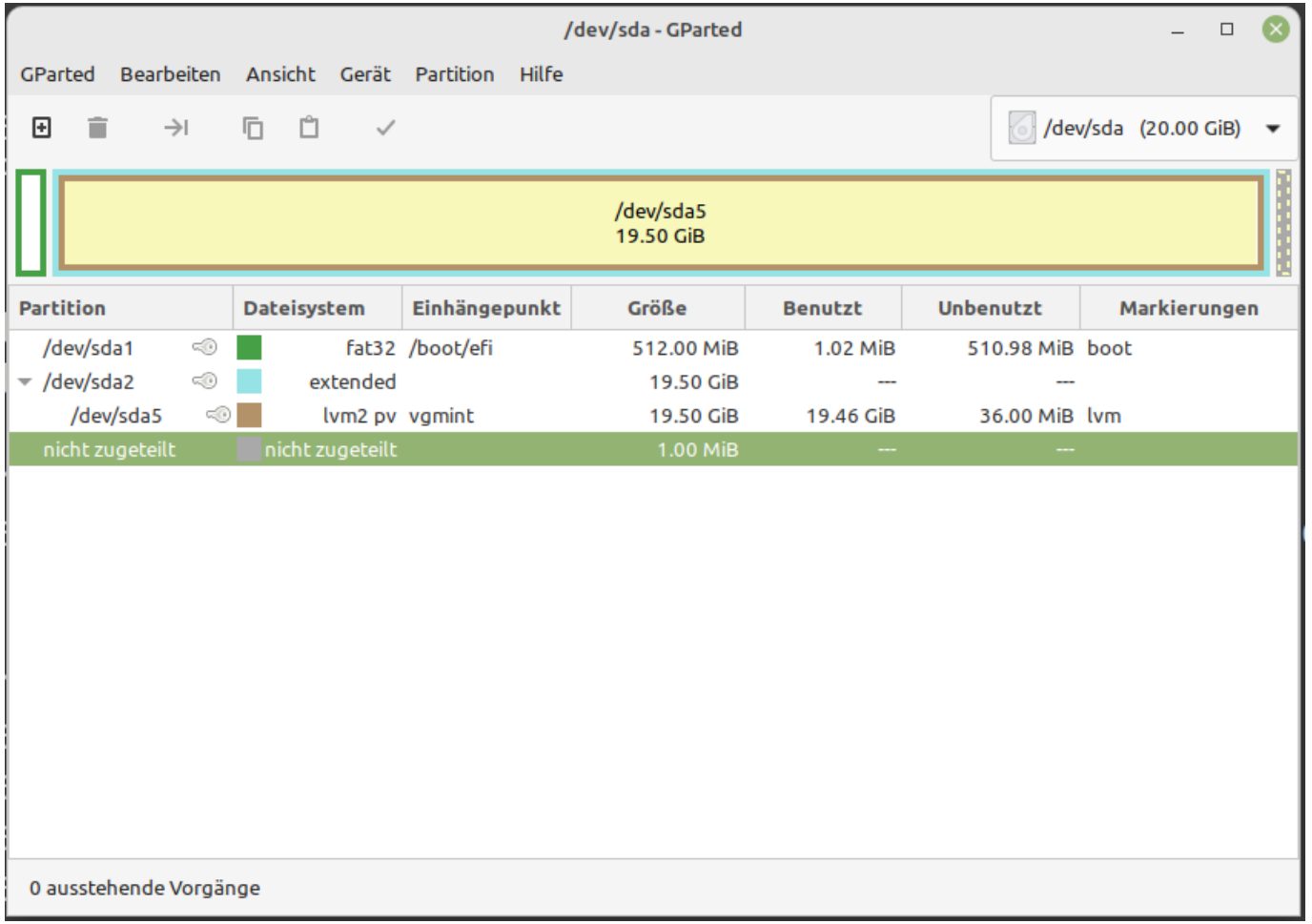
- 3. Festplatte
- 4. Partition
- Formatierung mit ntfs

(C) 15.06.2023 Hochschule Mittweida

Partitionieren und Formatieren

GParted

- Kurz für Gnome Partition Editor
- Graphische Oberfläche auf libparted
- Von vielen Distros verwendet
- Als eigene Distro (Live Version) erhältlich
- Kennt fast alle Partitionierungen
- Unterstützt viele Filesysteme
- Sehr ähnlich zur Windows Datenträgerverwaltung



(C) 15.06.2023 Hochschule Mittweida

RAID-Systeme

RAID-Systeme

- **RAID ~ Redundant Array of Independent Disks**
  - = Zusammenschaltung von Datenträgern zu einer virtuellen Festplatte
- Besitzt Superblock
  - Speichert Meta-Informationen über RAID
  - Hilfreich bei späterer erneuter Zusammensetzung bei Untersuchungen

Software-RAID	Hardware-RAID
Kein Hardware-Controller	Hardware-Controller
CPU übernimmt Berechnungen	Hardware-Controller übernimmt Berechnungen
Cache von Festplatten deaktiviert (sonst Datenverlust möglich)	Cache aktiv → Normale Schreiboperationen
Größerer Overhead durch Berechnung CPU	Wenig Overhead, da externe Berechung

(C) 15.06.2023 Hochschule Mittweida

Software-RAIDs

- **MDADM - Multiple Disk ADMinistration**
  - Linux Raid (0xFD MBR, 0xFD00 GPT) als Filesystem auf Partition
  - Version 1.0 Superblock am Ende der Partition
  - Version 1.1 Superblock am Anfang der Partition
  - Version 1.2 Superblock 4KB nach Anfang der Partition
- **LVM - Logical Volume Manager**
  - Dynamisch veränderbare Partitionen (auch über mehrere Datenträger)
  - Integriert in grub2 (Bootmanager)
- **ZFS – Zettabyte File System**
  - Software Raid in Filesystem integriert
  - Pools als Speicheraufteilung
  - Fehlererkennung über Merkle-Trees (Hash-Baum)

(C) 15.06.2023 Hochschule Mittweida

RAID-Varianten

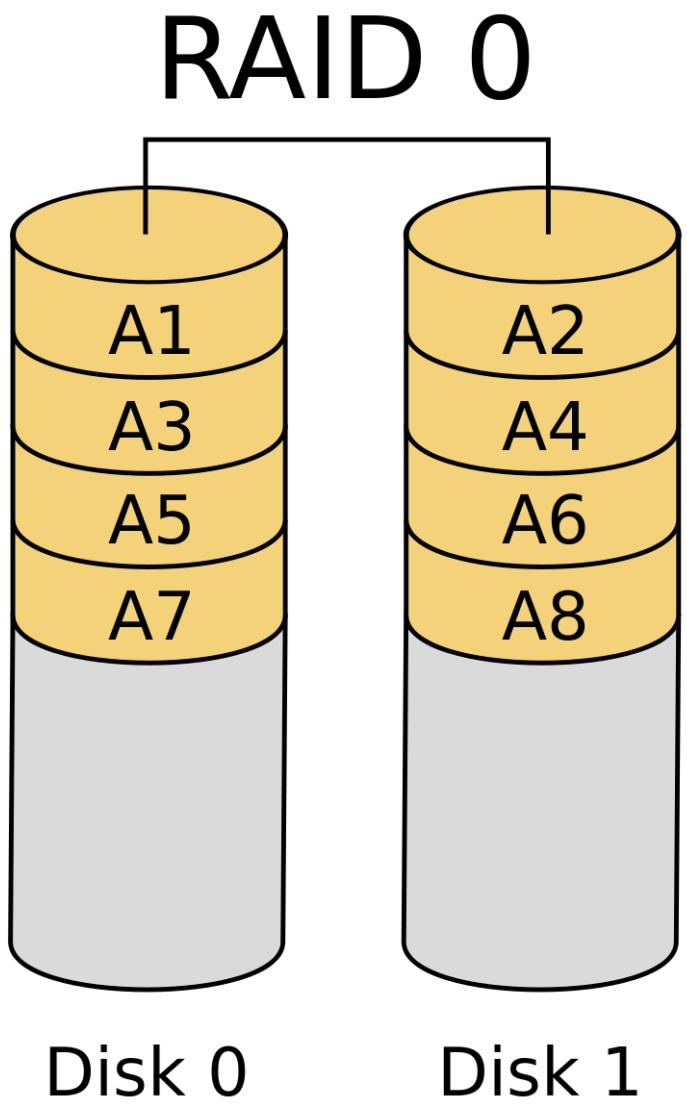
- **RAID-0 (Stripe)**
  - Speicherblöcke verteilen
- **RAID-1 (Mirror)**
  - Speicherblöcke spiegeln
- RAID-3
  - Bytes verteilen
  - Prüfsumme auf dedizierten Datenträger
- RAID-4
  - Speicherblöcke verteilen
  - Prüfsumme auf dedizierten Datenträger
- **RAID-5 (Parity)**
  - Speicherblöcke verteilen
  - Prüfsumme
- RAID-6
  - Speicherblöcke verteilen
  - 2 Prüfsummen
- **RAID-10**
  - 2 RAID-1-Systeme
  - Diese RAID-1 zusammengeführt mit RAID-0
- JBOD
  - Just a Bunch of Disk
  - Aneinanderkettung von Datenträgern

(C) 15.06.2023 Hochschule Mittweida

RAID-0

- Daten werden in Blöcke zerlegt
- Blöcke, wie Spielkarten der reihum an Festplatten verteilt

- Bei zwei Datenträgern
  - Doppelte Schreibgeschwindigkeit
  - Doppelte Lesegeschwindigkeit
  - Doppelte Ausfallwahrscheinlichkeit
  - 0% Speicherplatzverlust

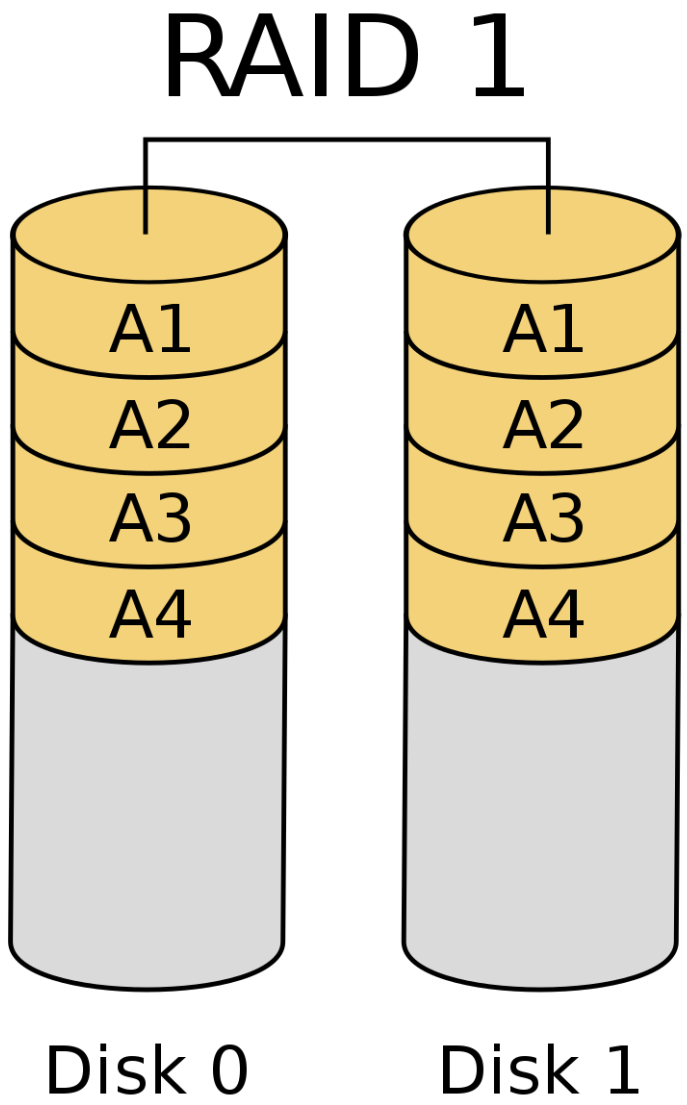


(C) 15.06.2023 Hochschule Mittweida

RAID-1

- Daten werden in Blöcke zerlegt
- Blöcke auf allen Datenträgern gespeichert

- Bei zwei Datenträgern
  - Halbe Schreibgeschwindigkeit
  - Doppelte Lesegeschwindigkeit
  - Halbe Ausfallwahrscheinlichkeit
  - 50% Speicherplatzverlust

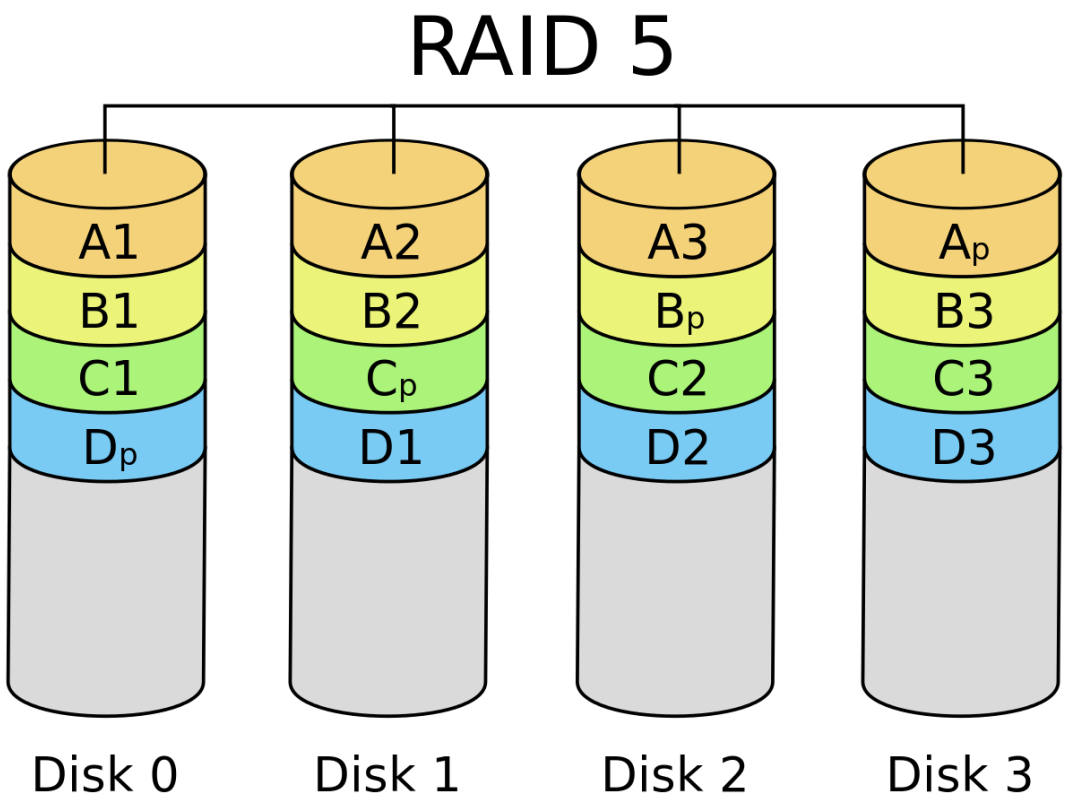


(C) 15.06.2023 Hochschule Mittweida

RAID-5

- Daten werden in Blöcke zerlegt
- Blöcke, wie Spielkarten der Reihum an Festplatten verteilt
- Prüfsumme in einem zusätzlichen Block

- **Bei vier Datenträgern**
  - **Fast Doppelte** Schreibgeschwindigkeit
  - Doppelte Lesegeschwindigkeit
  - verringerte Ausfallwahrscheinlichkeit
  - 25% Speicherplatzverlust (1/Anzahl der Festplatten)

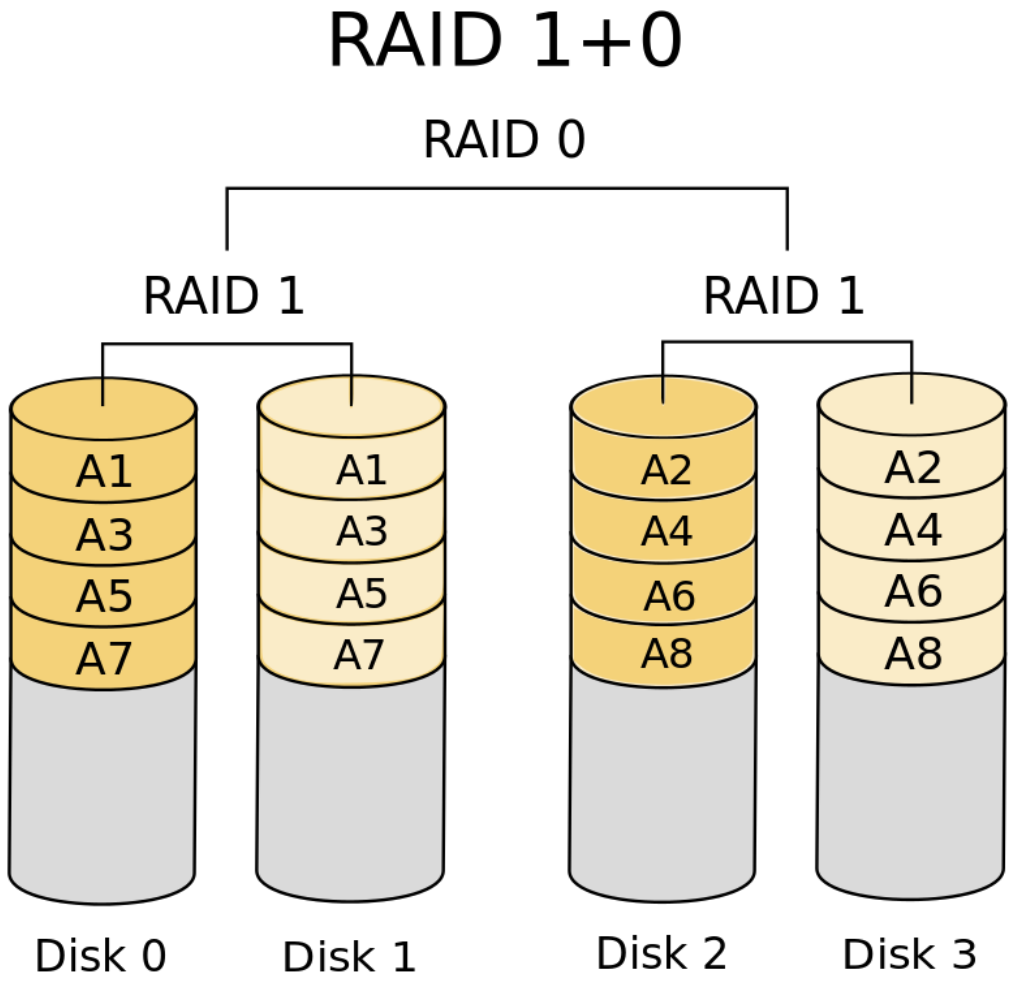


(C) 15.06.2023 Hochschule Mittweida

RAID-10

- Daten werden in Blöcke zerlegt
- Kombination der Vorteile von RAID-0 und RAID-1

- Bei vier Datenträgern
  - Fast Doppelte Schreibgeschwindigkeit
  - Doppelte Lesegeschwindigkeit
  - verringerte Ausfallwahrscheinlichkeit
  - 50% Speicherplatzverlust



(C) 15.06.2023 Hochschule Mittweida

Benutzer und Gruppen

Speicherorte Benutzer

- **`/etc/passwd`**
  - Lesbar von allen Nutzern
  - Auflistung von Benutzern
  - Enthielt früher Hash
- **`/etc/shadow`**
  - Speicherort von Passwort-Hash
- **`/etc/group`**
  - Gruppen und deren Nutzern
- **`/home oder /root`**
  - Private Dateien von Nutzern

(C) 15.06.2023 Hochschule Mittweida

/etc/passwd

`Hans:x:0:0:hans@hsmw.de:/home/hans:/bin/bash`

- Trennzeichen ist :
- Benutzername
- Passwort (x → Passwort in /etc/shadow)
- Benutzer-ID
- Gruppen-ID
- GECOS
  - Zusatzinfos: E-Mail, Telefonnummer, Kommentar
  - Getrennt durch ,
- Homeverzeichnis
- Standard-Shell

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```


(C) 15.06.2023 Hochschule Mittweida

/etc/shadow

Hans:6RTejg…8Cs$eLLfT8F…PD8tZCHAIAn61:19053:0:99999:7:::

- Trennzeichen ist :
- Benutzername
- Passwort ($Type$Salt$Hash)
  - $1: MD5
  - $2a: Blowfish
  - $2y: Eksblowfish
  - $5: SHA-256
  - $6: SHA-512
  - !, !!, * für kein Login möglich (meist /bin/false als Shell)
- Letzte Passwortänderung in Unix-Time
- Minimales Passwortalter
- Maximales Passwortalter
- Warnzeitraum bis ungültig
- Inaktivitätszeitraum
  - Zeit zwischen Passwort zu alt und Login verwehrt
- Deaktiviert Zeitstempel
- Unbenutzt / reserviert

(C) 15.06.2023 Hochschule Mittweida

/etc/group

`sudo:x:27:Hans,Peter`

- Trennzeichen ist :
- Gruppenname
- Passwort
- Gruppen-ID
- Mitgliederliste
  - Trennzeichen ist ,

- Jeder Nutzer ist mindestens in einer Gruppe
- Standardmäßig: gleicher Gruppenname, wie Benutzername

- Einige Distros haben Backups von passwd, shadow, group
- Backup automatisch erstellt bei Änderung

(C) 15.06.2023 Hochschule Mittweida

/home oder /root

- Unter `/root` für root-Nutzer
- Unter `/home` für alle anderen Nutzer
- Eigener Unterordner für Nutzer
- Manchmal auch weiter gegliedert in Abteilung
- Nicht jeder Benutzer besitzt Home-Verzeichnis
  - www-data
  - sshd
- Versteckte Ordner (. als erstes Zeichen)
  - Enthalten Konfigurationen
  - Jedes Programm eigener Unterordner

- **Standardordner bei Desktop-Linux**
  - Bilder (Pictures)
  - Dokumente (Documents)
  - Downloads (Downloads)
  - Musik (Music)
  - Öffentlich (Public)
  - Schreibtisch (Desktop)
  - Videos (Videos)
  - Vorlagen (Templates)
- .cache (Temporärer Speicher von Anwendungen)

(C) 15.06.2023 Hochschule Mittweida

Benutzerrechte

- Benutzerrechte über Datei-Zugriffsrechte
- Erinnerung: Alles ist eine Datei.
- **Leserechte** auf
  - Dateien anderer Nutzer = Leserechte auf `/home/userX`
- **Scheibrechte** auf
  - Festplatte 1 = Schreibrechte auf `/dev/sda`
  - Webserver-Dateien = Schreibrechte im Ordner `/var/www`
  - Passwortänderung = Schreibrechte auf `/etc/shadow`
- **Ausführrechte** von
  - Computer ausschalten = Ausführrechte auf `/sbin/shutdown`

(C) 15.06.2023 Hochschule Mittweida

Datei-Zugriffsberechtigung

drwxrwxrwx

- TypBesitzerGruppeAlleAnderen
- d: Dateityp
- r: Leserechte (read)
- w: Schreibrechte (write)
- x: Ausführrechte (execute)
- s: setuid (Ausführung mit Besitzer-rechten)
- s: setgid (Ausführung mit Gruppen-rechten)
- t: stickybit (Proramm verbleibt im Speicher nach Ausführungsende)

Dateitypen

- -: normale Datei
- d: Ordner (directory)
- b: Block-Device
- c: Zeichen (character)
- l: Softlink (symbolic link)
- n: Netzwerk (network)
- p: Pipe / First-in, First-out
- s: Socket

(C) 15.06.2023 Hochschule Mittweida

Berechtigung Beispiel

- Ausgabe von `ls -l /dev/sda`

```
brw-rw---- 1 root disk 8, 0 Apr 20 11:42 /dev/sda
```

- Besitzer ist root
- Gruppe ist disk
- b = block device (Speichermedium)
- root darf lesen und schreiben, aber nicht ausführen
- Gruppenmitglieder von disk dürfen lesen und schreiben, aber nicht ausführen
- Alle anderen dürfen weder lesen, schreiben noch ausführen

(C) 15.06.2023 Hochschule Mittweida

Berechtigung Beispiel

- Ausgabe von `ls -l /dev/sda`

```
brw-rw---- 1 root disk 8, 0 Apr 20 11:42 /dev/sda
```

- Anzahl an Hardlinks: 1
- Dateigröße: 8 Blöcke virtuell, 0 Blöcke reell
- Letzte Änderung am: 20. April 11:42 Uhr
- Dateiname: `/dev/sda`

(C) 15.06.2023 Hochschule Mittweida

Berechtigung Zahlencodierung

- Gruppen als eine Zahl zusammengefasst
- Berechtigung als Zahl addiert aus
  - r = 4
  - w = 2
  - x = 1

- **Beispiel**
  - rwxr--r-- → 744
  - --x--x--- → 110
  - r-xr-xr-x → 555

- Setuid = 4
- Setgid = 2
- Stickybit = 1

- **Beispiel**
  - rwsr--r-- → 4744
  - --srwS--- → 6160
  - r-xr-xr-t → 1555
  - r-sr---wT → 5542

(C) 15.06.2023 Hochschule Mittweida

Nutzungsverlauf

Unix-Zeitformat

- **Andere Bezeichnungen**
  - Unix-Time
  - Epoch-Time
  - Posix-Time
  - seconds since the Epoch
  - UNIX Epoch time
- **Beispiele:**
  - Folie erstellt um: 1650469006
  - Gründung EU: 1259625600
  - Aber, Apollo 11 mit Mondlandung 20. Juni 1969 in Unix-Time nicht möglich
- Natürliche Zahl (32Bit oder 64Bit)
- 0 entspricht 1. Januar 1970 um 0:00:00 Uhr UTC (Startzeitpunkt)
- Zeitpunkt = Start + Sekunden
- Schaltsekunden durch strecken/stauchen von Sekunden über langen Zeitraum

(C) 15.06.2023 Hochschule Mittweida

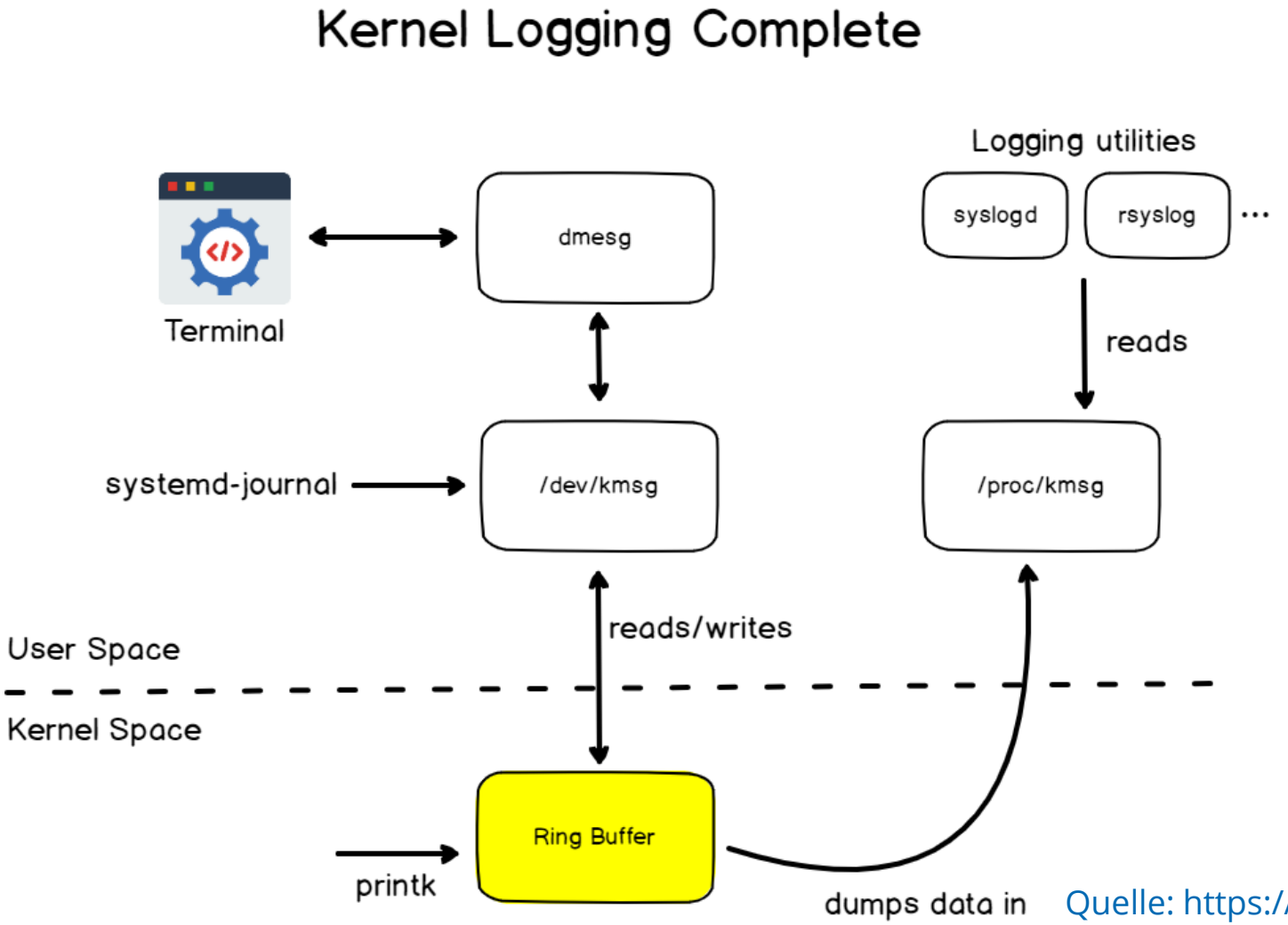
Linux-Logs

- Protokollierung von Ereignissen
  - Login
  - Zugriffe
  - Fehler
  - …
- Fehlererkennung / Administration
  - Dateibeschädigung
  - Fehlende Datenträger
  - …

- Eine Zeile = ein Eintrag
- Aufbau meist:
  - Timestamp
    - Unix-Time
    - ausgeschrieben in local time
    - Bootvorgang in ms nach Power on
  - Akteur / Auslöser
  - Eventbeschreibung
  - Neuer Status

(C) 15.06.2023 Hochschule Mittweida

Kernel-Logs



- Kernel Ring Buffer speichert Kernel-Logs
- /dev/kmsg als Interface
- dmesg als Programm für den Entnutzer
- Automatische Systemauswertung über
  - syslogd (local)
  - rsyslog (remote)

Quelle: https://devconnected.com/linux-logging-complete-guide/

(C) 15.06.2023 Hochschule Mittweida

Login-Logs

/var/log/auth.log

```
Apr 21 07:43:58 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 07:44:02 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session closed for user root
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session closed for user root
Apr 21 09:05:50 linuxmint-VirtualBox su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=pts/0
 ruser=linuxmint rhost=  user=root
Apr 21 09:05:51 linuxmint-VirtualBox su: FAILED SU (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox sudo: linuxmint : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 09:06:00 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 09:06:00 linuxmint-VirtualBox su: (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox su: pam_unix(su:session): session opened for user root by (uid=0)
(END)
```

sudo Befehl (Befehl mit root-Rechten)

(C) 15.06.2023 Hochschule Mittweida

Login-Logs

/var/log/auth.log

```
Apr 21 07:43:58 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 07:44:02 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session closed for user root
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session closed for user root
Apr 21 09:05:50 linuxmint-VirtualBox su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=pts/0
 ruser=linuxmint rhost=  user=root
Apr 21 09:05:51 linuxmint-VirtualBox su: FAILED SU (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox sudo: linuxmint : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 09:06:00 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 09:06:00 linuxmint-VirtualBox su: (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox su: pam_unix(su:session): session opened for user root by (uid=0)
(END)
```

CRON-Job als root (Zeitgesteuerte Ausführung)

(C) 15.06.2023 Hochschule Mittweida

Login-Logs

/var/log/auth.log

```
Apr 21 07:43:58 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 07:44:02 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session closed for user root
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session closed for user root
Apr 21 09:05:50 linuxmint-VirtualBox su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=pts/0
 ruser=linuxmint rhost=  user=root
Apr 21 09:05:51 linuxmint-VirtualBox su: FAILED SU (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox sudo: linuxmint : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 09:06:00 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 09:06:00 linuxmint-VirtualBox su: (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox su: pam_unix(su:session): session opened for user root by (uid=0)
(END)
```

Gescheiterter Login als root

(C) 15.06.2023 Hochschule Mittweida

Login-Logs

/var/log/auth.log

```
Apr 21 07:43:58 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 07:44:02 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:17:01 linuxmint-VirtualBox CRON[28491]: pam_unix(cron:session): session closed for user root
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 21 08:30:01 linuxmint-VirtualBox CRON[28499]: pam_unix(cron:session): session closed for user root
Apr 21 09:05:50 linuxmint-VirtualBox su: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0 tty=pts/0
 ruser=linuxmint rhost=  user=root
Apr 21 09:05:51 linuxmint-VirtualBox su: FAILED SU (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox sudo: linuxmint : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 09:06:00 linuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Apr 21 09:06:00 linuxmint-VirtualBox su: (to root) linuxmint on pts/0
Apr 21 09:06:00 linuxmint-VirtualBox su: pam_unix(su:session): session opened for user root by (uid=0)
(END)
```

Erfolgreicher Login als root

(C) 15.06.2023 Hochschule Mittweida

Weitere Log-Speicherorte

`/var/log/syslog` (Ubuntu/Debian)
`/var/log/messages` (Red Hat)

- Allgemeine System Logs

`/var/log/auth.log` (Ubunut/Debian)
`/var/log/secure` (Red Hat)

- Authentifikation (Login)

`/var/log/maillog`
`/var/log/mail.log`

- E-Mail

`/var/log/kern`

- Kernel-Logs

`/var/log/dmesg`

- Kernel-Logs über Geräte

`/var/log/faillog`

- Gescheiterte Logins Zusammenfassung (Befehl: faillog)

`/var/log/cron`

- Logs von Cron-Jobs

`/var/log/daemon.log`

- Logs von Hintergrundprozessen

`/var/log/httpd/`

- Webserver-Logs

`/var/log/mysqld.log`

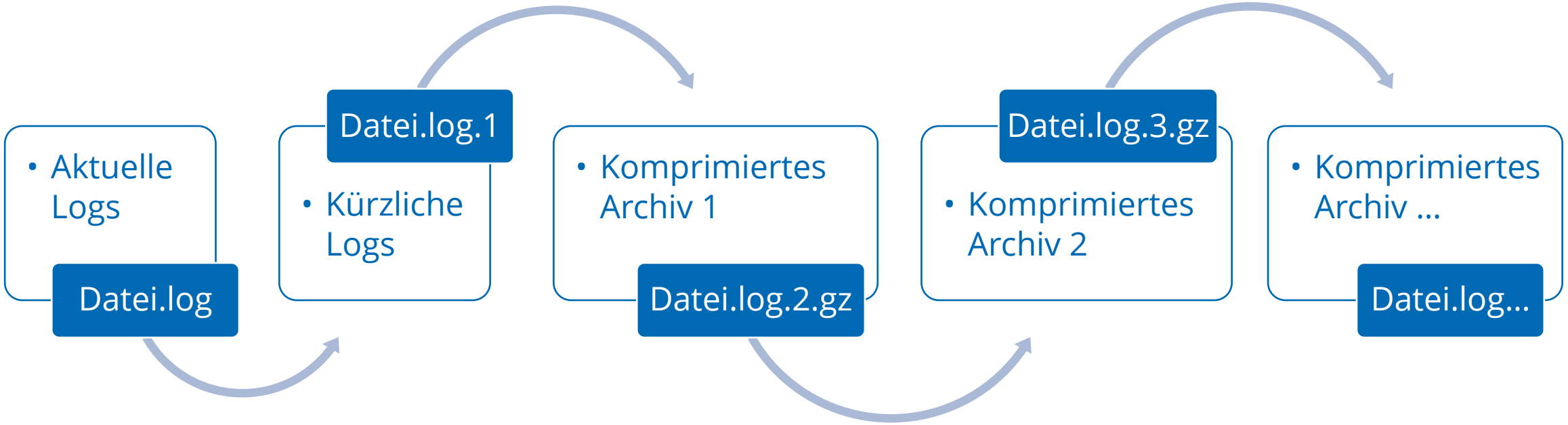
- SQL-Server Logs

`/var/log/xferlog`

- Logs von FTP-Übertragungen

(C) 15.06.2023 Hochschule Mittweida

Log-Archiv



(C) 15.06.2023 Hochschule Mittweida

Shell-Historie

- Speichert ausgeführte Befehle der Shell
- Jedoch keine Zeitstempel
  - Korrelation mit Logs notwendig
- Speicherort: `~/.bash_history`
- Beschrieben bei
  - Shell-Fenster schließen
  - Logout
- Vorher nur im RAM auslesbar
  - Befehl: history
  - Jede Shell-Instanz hat eigene History
  - genutzt bei Pfeiltasten

- **Indicator of Compromise**
  - Shell history wird durch cron geleert
  - ~/.bash_history durch Softlink ersetzt (z.B. auf /dev/null)
  - Änderungsdatum von ~/.bash_history korreliert nicht mit logout
    - ➢ Sehr wahrscheinlich manuelle Manipulation
    - ➢ Befehl gelöscht?

(C) 15.06.2023 Hochschule Mittweida

Dateizugriff

- Gespeichert im Filesystem
- Einige Filesysteme unterstützen diese Metadaten nicht
- Letzter Schreibzugriff:
  - fs –l <Datei>
  - date –r <Datei>
- Ausführliche Informationen
  - stat <Datei>
- **Achtung!**
  - root kann alles ändern

```
linuxmint@linuxmint-VirtualBox:~/disks$ ls -l
insgesamt 393268
-rw-rw-r-- 1 linuxmint linuxmint 134217728 Apr 20 15:05 disk1
-rw-rw-r-- 1 linuxmint linuxmint 134217728 Apr 20 15:05 disk2
-rw-rw-r-- 1 linuxmint linuxmint 134217728 Apr 20 15:05 disk3
-rw-rw-r-- 1 linuxmint linuxmint     38349 Apr 20 11:39 manpage.txt
-rw-rw-r-- 1 linuxmint linuxmint         2 Apr 20 17:12 test
linuxmint@linuxmint-VirtualBox:~/disks$ date -r disk1
Mi 20 Apr 2022 15:05:15 CEST
linuxmint@linuxmint-VirtualBox:~/disks$ stat disk1
  Datei: disk1
 Größe: 134217728       Blöcke: 262152     EA Block: 4096   Normale Datei
Gerät: fd00h/64768d     Inode: 1059378     Verknüpfungen: 1
Zugriff: (0664/-rw-rw-r--)  Uid: ( 1000/linuxmint)   Gid: ( 1000/linuxmint)
Zugriff: 2022-04-20 15:05:09.376448864 +0200
Modifiziert: 2022-04-20 15:05:15.360480843 +0200
Geändert: 2022-04-20 15:05:15.360480843 +0200
Geburt: -
```


(C) 15.06.2023 Hochschule Mittweida

Systemschnappschüsse

- timeshift als Softwarelösung
- Vergleichbar mit
  - Systemwiederherstellung (Windows)
  - Time Maschine (Apple)
- Nutzt rsync
  - rsync = Synchronisierung von Dateien
  - Bei timeshift: Speichern von Änderungen
- Entworfen für Speicherstände von
  - Einstellungen
  - Systemdateien
- Automatisierung möglich (täglich, wöchentlich, monatlich)

(C) 15.06.2023 Hochschule Mittweida

Zusammenfassung

Zusammenfassung

Sie kennen nun Speicherorte und den Aufbau der Netzwerk-Konfigurations-Dateien unter Linux. Sie können außerdem die WLAN-Konfiguration unter verschiedenen Distributionen auswerten.

Heute haben Sie einen Überblick über Dateisysteme und Partitions-möglichkeiten erhalten. Sie kennen darüber hinaus die notwendigen Programme zum Partitionieren und Formatieren. Sie wissen über die RAID-Versionen 0, 1, 5 und 10 Bescheid.

Sie wissen nun, wie Nutzer unter Linux gespeichert werden und wie deren Rechtevergabe funktioniert. Die Dateifreigabe können Sie interpretieren.

Auf einem System können Sie Spuren des Nutzungsverlaufs auswerten. Den Aufbau von Logs unter Linux haben Sie heute gelernt und können gegebenfalls Zeitangaben in Unix-Time in einem Zeitpunkt umrechnen.

(C) 15.06.2023 Hochschule Mittweida

Prof. Ronny Bodach

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
@ bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau| Raum 8-205
Am Schwanenteich 6b| 09648 Mittweida

Tim Wetterau B.Sc.

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de

Haus 6 | Grunert de Jacome Bau | Raum 6-031
Am Schwanenteich 4b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de