

Hinweis: Falls ein Command nicht funktioniert → sudo davor schreiben, sonst arg -help verwenden

Lizenzmodelle

Modell	Beschreibung
Prop. Lizenz	Closed Source, kein Zugriff auf Code, Distribution/Modifikation verboten
Free S-ware	Viel Freiheiten (Nutzen, Untersuchen, Weitergeben, Ändern), meist offen
Open Source	Quellcode offen (pflicht), Nutzung/Änderung/Weitergabe erlaubt
Shareware	Kostenlos testen, volle Nutzung nach Bezahlung
Freeware	Kostenlos nutzbar, Source meist nicht offen
Public Domain	Ohne Urheberrecht, frei nutzbar/änderbar
Kommerziell	Bezahlpflichtig, Nutzung nur nach Lizenzbedingungen

Gegenüberstellung

Modell	Quellcode	Kosten	Freiheit	Weitergabe/Änderung
Proprietär	Geschl.	Kostenpflichtig	Stark begrenzt	Verboten
Free S-ware	Offen	Oft kostenlos	Sehr hoch	Erlaubt & erwünscht
Open Source	Offen	Frei/Kosten	Hoch	Je nach Lizenz
Shareware	Geschl.	Test, dann Kosten	Eingeschränkt	Nicht erlaubt
Freeware	Geschl.	Kostenlos	Nutzung frei	Meist nicht erlaubt
Public Domain	Variabel	Kostenlos	Komplett frei	Ohne Einschränkung
Kommerziell	Geschl.	Kostenpflichtig	Eingeschränkt	Nicht erlaubt

Hypervisor

Begriff	Beschreibung
Typ 1	Hypervisor direkt auf H-ware
Typ 2	Hypervisor auf Host OS
Gast-OS	Läuft in VM, nutzt virtuelle HW
Hypervisor	Schicht zwischen HW und Gast-OS (z. B. VBox)
Host-OS	Basis-OS (bei Typ 2), z. B. Linux, Windows
H-ware	CPU, RAM, Disk, Netz, wird vom Hypervisor verteilt

Paketmanager (APT)

Befehl	Bedeutung
apt update	Paketlisten aktualisieren
apt upgrade	Installierte Pakete aktualisieren
apt install X	Paket installieren
apt remove X	Paket entfernen, Config bleibt
apt purge X	Paket inkl. Config entfernen
apt search X	Paket suchen
apt show X	Paketdetails
apt list X --installed	Installierte Pakete anzeigen

Update vs. Upgrade

- update: nur Listen
- upgrade: installiert neue Versionen

Vorteile: Automatische Abhängigkeiten, zentrale Updates, Sicherheit, Integration, einfache Verwaltung

Dateisysteme

FS	Kompatibilität	Max. Datei	Besonderheiten	Nutzung
FAT32	Sehr hoch	4 GB	Kein Rechtemgmt	USB/SD
NTFS	Win, Linux	>16 TB	Rechte, Journaling	Windows, Extern
EXT4	Linux	16 TB	Stabil, Journaling	Linux
Btrfs	Linux	16 EB	Snapshots, Subvolumes	Flexibel
ZFS	Linux/BSD	16 EB+	Datenintegrität, Snapshots	Server/NAS

- **MBR:** max. 2 TB, 4 primär
- **GPT:** modern, >2 TB, bis 128

Gruppen & Nutzer

Schritt	Befehl	Beschreibung
Gruppe	groupadd testgruppe	Gruppe anlegen
User	useradd -m -s /bin/bash testuser	User anlegen
PW	echo "testuser:test" chpasswd	Passwort setzen
Gruppe+	usermod -aG testgruppe testuser	User zur Gruppe
Prüfen	groups testuser	Zugehörigkeit anzeigen

Fehlerbehebung:

1. Prozesse & Ressourcen

Befehl	Stichworte
ps aux \ less	Prozesse
top / htop	CPU-Last
kill -9 <PID>	Prozess killen
Info	Prozess ≠ Service

Prozess: Laufendes Programm im RAM

Service: spezieller Prozess wo **immer** im Hintergrund läuft

2. Ressourcen belasten

Befehl	Stichworte
apt install stress	Tool
stress --cpu 2 --timeout 20	CPU-Load
htop	Last sichtbar
Info	Load Avg > Kerne = kritisch

3. Speicherplatz & Dateisystem

Befehl	Stichworte
du -h --max-depth=1 /	Platzverbrauch
fallocate -l 1G bigfile.img	Platte füllen
Info	/var/log voll = keine Logs /home voll = User blockiert

4. Services & Systemkontrolle

Befehl	Stichworte
systemctl status ssh	Status
systemctl stop/start ssh	Stop/Start
systemctl disable/enable ssh	Boot deaktiv/aktiv

5. Systemleistung & Logs

Befehl	Stichworte
free -h	RAM/Swap
uptime	Load Avg
/var/log/syslog	Logs
Info von: Auf	Zeit, Host, Prozess, Msg

6. Fehleranalyse – langsames System

Befehl	Stichworte
top / htop	Prozesse
free -h	RAM
df -h	Speicher
cat /var/log/syslog	Logs

7. Fehleranalyse - Dienst nicht verfügbar

Befehl	Stichworte
ping <Server>	Netzwerk
systemctl status <dienst>	Status
ss -tuln	Ports
journalctl -u <dienst>	Logs
systemctl restart <dienst>	Neustart

Hardlink: Ein zweiter Verweis auf die gleiche Datei im Dateisystem (zeigt direkt auf den

Inode). Löscht man die Originaldatei, bleibt der Inhalt über den Hardlink erhalten.

SymLink (Softlink): Eine Art „Verknüpfung“, die nur auf den Pfad/Zielnamen einer Datei zeigt. Wird das Original gelöscht oder verschoben, zeigt der Link ins Leere („broken link“).

Inode = Index Node

Partitionen erstellen

Schritt	Befehl	Hinweis
Anzeigen	lsblk	Festplatten & Partitionen
Details	fdisk -l	Infos & Größen
Erstellen	fdisk /dev/sdX	n neu, w speichern
Format	mkfs.ext4 /dev/sdX1	FS erstellen
Mountdir	mkdir /mnt/testpartition	Verzeichnis
Mounten	mount /dev/sdX1 /mnt/testpartition	Einbinden
Testen	df -Th	Eingebundene prüfen
Automount	/etc/fstab	/dev/sdX1 /mnt/testpartition ext4 defaults 0 2

Linux-Verzeichnisse

Pfad	Zweck
/bin	Basisprgm. für Nutzer
/sbin	Adminprgm (Root)
/dev	Geräte
/etc	Konfigs
/home	Userdaten
/lib	Bibliotheken
/media	Wechselmedien
/mnt	Temporäre Mounts
/opt	Zusatzsoftw.
/proc	Virt. FS, Prozesse
/run	Laufzeitdaten
/srv	Servicedaten
/sys	Kernel-/Hardwr Info
/tmp	Temporäre Dateien
/usr	Nutzerprgm, Libs
/var	Logs, DBs, Spools

Rechte

Rechte	Symbol	Oktal
Keine	---	0
Nur Ausführen	--x	1
Nur Schreiben	-w-	2
Schreiben + Ausführen	-wx	3
Nur Lesen	r--	4
Lesen + Ausführen	r-x	5
Lesen + Schreiben	rw-	6
Lesen + Schreiben + Ausführen	rwX	7

Netzwerk

Ports

- ss -tulwn -> aktive Dienste

Risiko: unnötige Ports schließen

Firewall

- ufw enable
- ufw allow ssh
- ufw deny 80/443 -> Web blockiert
- ufw reset

Virens Scanner

- apt install clamav
- clamscan -r /home/student
- Ergebnis: OK / FOUND

Reflexion

Präventiv: Firewall, Updates, Echtzeit-AV

Reaktiv: Scan, Logs, Incident Response

Unternehmen: Segmentierung, zentrale Firewall, Monitoring, Backups, MFA

Aktion	Befehl	Erklärung
Besitzer ändern	sudo chown benutzer:gruppe \$PATH	Besitzer und Gruppe setzen
Nur Gruppe ändern	sudo chown :gruppe \$PATH	Gruppe ändern
Rechte setzen	sudo chmod 777 \$PATH	Lesen/Schreiben/Ausführen (Oktal)
Rechte rekursiv	sudo chmod -R 770 \$PATH	Alle Unterordner und Dateien
Setgid auf Ordner	sudo chmod g+s \$PATH	Neue Dateien erben Gruppenzugehörigkeit
Benutzer zur Gruppe hinzufügen	sudo usermod -aG gruppe benutzer	Benutzer wird Mitglied der Gruppe
Neue Gruppe anlegen	sudo groupadd gruppe	Gruppe erstellen
Rechte prüfen	ls -l \$PATH	Zeigt Symbole (rwx) an
Offene Ports prüfen (Dienst)	sudo ss -tulwn	Netzwerk-/Portrechte prüfen
Dienststatus prüfen	sudo systemctl status dienst	Prüft, ob Service läuft

Gruppenrechte / Benutzerrechte bearbeiten

1. Position: User
2. Position: Gruppe
3. Position: Andere

Wichtige Befehle / Programme:

- nano: einfacher Editor
- vi: mächtiger Editor (Basisbefehle lernen)
- touch, cat, more, less, head, tail, file: Dateien erstellen, anzeigen, Infos prüfen
- echo: Text direkt in Dateien schreiben