15.1 Prüfungsvorbereitung und Wiederholung

Diese Seite fasst die wichtigsten Linux-Themen für die IHK-Prüfung zusammen.

Der Fokus liegt nicht auf auswendig gelernten Einzelbefehlen, sondern auf Verständnis:

- Was macht Linux als Betriebssystem?
- Wie ist das Dateisystem aufgebaut?
- Wie funktionieren Benutzer und Rechte?
- Wie prüft man Dienste?
- Wie grenzt man Fehler ein?
- Wie liest man Logs?
- Wie arbeitet man sicher auf Servern?
- Wie argumentiert man fachlich sauber?

Für Fachinformatiker Systemintegration ist Linux besonders relevant, weil viele Server, Container, Netzwerkdienste, Monitoring-Systeme, Firewalls, NAS-Systeme und Cloud-Umgebungen auf Linux basieren.

Merksatz:

> In der Prüfung zählt nicht nur der Befehl,
> sondern die richtige fachliche Einordnung.

Lernziele

Nach dieser Seite solltest du wiederholen können:

- Linux-Grundbegriffe
- Dateisystem und wichtige Pfade
- Dateioperationen
- Benutzer, Gruppen und Rechte
- Prozesse, Dienste und systemd
- Paketverwaltung

- Netzwerkdiagnose
- Speicher,
  Mounts
  und Dateisysteme
- Logs,
  Monitoring
  und Fehlersuche
- Shell,
  Pipes
  und Umleitungen
- Bash-Scripting
- Sicherheit,
  Backup
  und Automatisierung
- Linux im Serverbetrieb

Linux-Grundlagen wiederholen

Begriff	Bedeutung
Linux	Betriebssystemkern, im Alltag oft komplette Distribution gemeint
Kernel	Kern des Betriebssystems
Distribution	Linux-Kernel plus Software, Paketmanager und Systemwerkzeuge
Shell	Befehlsinterpreter
Bash	verbreitete Linux-Shell
Terminal	Eingabeumgebung für Shell-Befehle
root	administrativer Hauptbenutzer
sudo	gezielte Ausführung mit erhöhten Rechten
Paketmanager	installiert und aktualisiert Softwarepakete

Merksatz:

Linux ist streng genommen der Kernel,
im Alltag meint man oft die gesamte Distribution.

Kernel, Distribution und Shell unterscheiden

Begriff	Aufgabe
Kernel	verwaltet Hardware, Speicher, Prozesse und Systemzugriffe
Distribution	stellt komplettes nutzbares Betriebssystem bereit
Shell	nimmt Befehle entgegen und startet Programme
Terminal	Fenster oder Umgebung zur Eingabe von Befehlen

Typische Prüfungsfalle:

> Linux,
> Distribution,
> Shell
> und Terminal werden durcheinandergeworfen.

IHK-sicher:

> Der Kernel ist der Betriebssystemkern.
> Eine Distribution kombiniert den Kernel mit Systemprogrammen,
> Paketverwaltung,
> Diensten
> und optional grafischer Oberfläche.

Wichtige Linux-Verzeichnisse

Pfad	Bedeutung
/	Root-Verzeichnis des Dateisystems
/home	Benutzerverzeichnisse
/root	Home-Verzeichnis des Root-Benutzers
/etc	Konfigurationsdateien
/var	veränderliche Daten
/var/log	Logdateien
/tmp	temporäre Dateien
/usr	Programme und Ressourcen
/bin	wichtige Benutzerprogramme
/sbin	wichtige Systemprogramme
/dev	Gerätedateien

Pfad	Bedeutung
/proc	Prozess- und Kernelinformationen
/sys	System- und Geräteinformationen
/mnt	manuelle Mountpoints
/media	Wechselmedien
/opt	optionale Zusatzsoftware
/srv	Dienstdaten

Merksatz:

> /etc für Konfiguration.
> /var/log für Logs.
> /home für Benutzer.
> / ist die Wurzel des Dateisystems.

Absolute und relative Pfade

Pfadart	Bedeutung	Beispiel
absolut	beginnt bei /	/etc/hosts
relativ	abhängig vom aktuellen Verzeichnis	dokumente/datei.txt

Wichtige Zeichen:

Zeichen	Bedeutung
/	Root-Verzeichnis oder Pfadtrenner
.	aktuelles Verzeichnis
..	übergeordnetes Verzeichnis
~	eigenes Home-Verzeichnis

Prüfungsfalle:

> Relativer Pfad hängt immer davon ab,
> wo man sich gerade befindet.

Merksatz:

Absoluter Pfad beginnt mit /.

Dateien anzeigen und bearbeiten

Aufgabe	Befehl
Verzeichnisinhalt anzeigen	ls
ausführlich anzeigen	ls -l
versteckte Dateien anzeigen	ls -a
aktuelle Position anzeigen	pwd
Verzeichnis wechseln	cd
Dateiinhalt anzeigen	cat
lange Datei lesen	less
Anfang anzeigen	head
Ende anzeigen	tail
live mitlesen	tail -f
Datei erstellen	touch
Datei bearbeiten	nano
kopieren	cp
verschieben oder umbenennen	mv
löschen	rm
Verzeichnis erstellen	mkdir
Datei suchen	find
Text suchen	grep

Merksatz:

cat für kleine Dateien.
less für lange Dateien.
tail -f für Live-Logs.

---

find und grep unterscheiden

Befehl	Sucht
find	Dateien und Verzeichnisse

Befehl	Sucht
grep	Text innerhalb von Dateien oder Ausgaben

Beispiele:

```
find /etc -name "*ssh*"

grep "PermitRootLogin" /etc/ssh/sshd_config
```

Prüfungsfalle:

```
find sucht Dateinamen oder Dateieigenschaften.
grep sucht Inhalte.
```

Merksatz:

```
find sucht Dateien.
grep sucht Text.
```

Benutzer, Gruppen und Rechte

Linux-Rechte gelten klassisch für:

```
Besitzer

Gruppe

Andere
```

Die Rechte sind:

Recht	Bedeutung bei Dateien	Bedeutung bei Verzeichnissen
r	lesen	Inhalt auflisten
w	schreiben	Einträge erstellen, löschen, umbenennen
x	ausführen	Verzeichnis betreten

Wichtige Befehle:

Befehl	Zweck
whoami	aktuellen Benutzer anzeigen
id	UID, GID und Gruppen anzeigen
groups	Gruppen anzeigen
chmod	Rechte ändern
chown	Besitzer ändern
chgrp	Gruppe ändern
sudo	Befehl mit erhöhten Rechten ausführen

Merksatz:

> Bei Verzeichnissen bedeutet x:
> betreten.

Numerische Rechte wiederholen

Zahl	Rechte
0	---
1	--x
2	-w-
3	-wx
4	r--
5	r-x
6	rw-
7	rwx

Typische Rechte:

Rechte	Bedeutung
644	normale Datei
600	private Datei
755	Programm oder öffentlich betretbares Verzeichnis
700	privates Verzeichnis oder privates Skript
777	jeder darf alles, meist unsicher

Merksatz:

```
r=4,
w=2,
x=1.
```

Root, sudo und Sicherheit

Begriff	Bedeutung
root	administrativer Hauptbenutzer
sudo	einzelne Befehle mit erhöhten Rechten ausführen
su	Benutzer wechseln
/root	Home-Verzeichnis von root
/	Root-Verzeichnis des Dateisystems

Prüfungsfalle:

```
root,
/root
und /
sind nicht dasselbe.
```

IHK-sicher:

```
Administrative Rechte sollten gezielt und nachvollziehbar genutzt werden.
Dauerhaftes Arbeiten als root erhöht das Risiko für Fehlbedienung und Schäden.
```

Merksatz:

```
Root-Rechte bewusst und nur bei Bedarf verwenden.
```

Prozesse und Dienste

Begriff	Bedeutung
Prozess	laufendes Programm
PID	eindeutige Prozess-ID

Begriff	Bedeutung
Dienst	Hintergrundprogramm mit Aufgabe
Daemon	Hintergrundprozess
systemd	Dienst- und Init-System vieler Distributionen
Unit	Verwaltungseinheit von systemd
.service	Dienst-Unit

Wichtige Befehle:

Befehl	Zweck
ps aux	Prozesse anzeigen
top	Prozesse live anzeigen
htop	komfortabler Prozessmonitor, falls installiert
kill	Signal an Prozess senden
systemctl status dienst	Dienststatus prüfen
journalctl -u dienst	Dienstlogs anzeigen

Merksatz:

> Prozess = läuft.
> Dienst = Hintergrundaufgabe.

---

systemctl sicher unterscheiden

Befehl	Bedeutung
systemctl start dienst	startet jetzt
systemctl stop dienst	stoppt jetzt
systemctl restart dienst	startet neu
systemctl reload dienst	lädt Konfiguration neu, falls unterstützt
systemctl enable dienst	aktiviert Autostart
systemctl disable dienst	deaktiviert Autostart
systemctl status dienst	zeigt Status
systemctl is-active dienst	prüft, ob Dienst läuft
systemctl is-enabled dienst	prüft Autostart

Prüfungsfalle:

> start und enable sind nicht dasselbe.

Merksatz:

> active heißt:
> läuft jetzt.
> enabled heißt:
> startet beim Boot.

Paketverwaltung

Distribution	Paketmanager
Debian / Ubuntu	apt
Fedora / Rocky Linux	dnf
openSUSE	zypper
Arch Linux	pacman
Alpine Linux	apk

Wichtige apt-Befehle:

Befehl	Bedeutung
apt update	Paketlisten aktualisieren
apt upgrade	installierte Pakete aktualisieren
apt install paket	Paket installieren
apt remove paket	Paket entfernen
apt purge paket	Paket inklusive Konfiguration entfernen
apt search begriff	Paket suchen
apt show paket	Paketinformationen anzeigen
apt autoremove	nicht mehr benötigte Abhängigkeiten entfernen

Merksatz:

> apt update holt Listen.
> apt upgrade installiert Updates.

Repository, Paket und Abhängigkeit

Begriff	Bedeutung
Paket	verwaltete Softwareeinheit
Repository	Paketquelle
Abhängigkeit	zusätzlich benötigtes Paket
Paketmanager	Werkzeug zur Paketverwaltung
Patchmanagement	geplanter Umgang mit Updates

Prüfungsfalle:

> Manuelle Installation von Webseiten ist unter Linux-Servern meist nicht der Standardweg.

IHK-sicher:

> Paketmanager installieren Software kontrolliert,
> lösen Abhängigkeiten auf
> und stellen Updates bereit.

Merksatz:

> Repository = Paketquelle.

Netzwerkdiagnose

Aufgabe	Befehl
IP-Adressen anzeigen	ip addr
Schnittstellen anzeigen	ip link
Routing anzeigen	ip route
Erreichbarkeit prüfen	ping
DNS prüfen	dig oder nslookup
Ports anzeigen	ss -tulpen
HTTP/HTTPS prüfen	curl
Hostname anzeigen	hostname
DNS-Status prüfen	resolvectl status

Aufgabe	Befehl
SSH-Verbindung herstellen	ssh benutzer@server

Merksatz:

> Erst IP,
> dann Route,
> dann DNS,
> dann Port,
> dann Dienst.

Typische Netzwerkauswertung

Ergebnis	Wahrscheinliche Richtung
keine IP-Adresse	DHCP oder Interface
Gateway nicht erreichbar	lokales Netz, VLAN, Gateway
externe IP nicht erreichbar	Routing, NAT oder Firewall
IP erreichbar, Name nicht	DNS
Dienst läuft, Port nicht erreichbar	Firewall, Bind-Adresse, Port
Port lauscht auf 127.0.0.1	nur lokal erreichbar
Connection refused	Dienst oder Port lehnt ab
Connection timed out	Firewall, Routing oder Ziel nicht erreichbar

Merksatz:

> ping prüft ICMP,
> nicht den Dienst.

SSH wiederholen

Begriff	Bedeutung
SSH	sichere Fernadministration
TCP 22	Standardport für SSH
ssh	Client-Befehl
sshd	SSH-Serverdienst

Begriff	Bedeutung
authorized_keys	erlaubte öffentliche Schlüssel
known_hosts	bekannte Server-Host-Keys
privater Schlüssel	bleibt geheim
öffentlicher Schlüssel	darf auf Server

Sicherheitsregel:

```
Direkten Root-Login vermeiden.
Besser normaler Benutzer plus sudo.
```

Merksatz:

```
Öffentlicher Schlüssel auf Server.
Privater Schlüssel bleibt geheim.
```

Firewall wiederholen

Eine Firewall-Regel sollte enthalten:

```
Quelle

Ziel

Protokoll

Port

Richtung

Aktion

Zweck
```

Typische Werkzeuge:

Werkzeug	Einordnung
ufw	einfache Firewall-Oberfläche, häufig Ubuntu

Werkzeug	Einordnung
firewalld	Firewall-Verwaltung mit Zonen
nftables	moderner Firewall-Unterbau
iptables	klassisches Firewall-Werkzeug

Merksatz:

> Port allein ist keine vollständige Firewall-Regel.

Speicher und Mounts

Begriff	Bedeutung
Datenträger	physisches oder virtuelles Speichermedium
Partition	Bereich auf einem Datenträger
Dateisystem	Organisationsform für Dateien
Mountpoint	Einhängepunkt im Verzeichnisbaum
fstab	automatische Mounts beim Systemstart
UUID	eindeutige Kennung eines Dateisystems
Swap	Auslagerungsspeicher

Wichtige Befehle:

Befehl	Zweck
lsblk	Datenträger und Partitionen anzeigen
lsblk -f	Dateisysteme und UUIDs anzeigen
df -h	Speicherplatz prüfen
df -i	Inodes prüfen
du -sh ordner	Ordnergröße anzeigen
mount	Mounts anzeigen oder einhängen
umount	aushängen
findmnt	Mounts strukturiert anzeigen
free -h	RAM und Swap anzeigen

Merksatz:

```
df zeigt Dateisysteme.
du zeigt Ordnergrößen.
```

---

fstab wiederholen

Die Datei:

```
/etc/fstab
```

legt fest, welche Dateisysteme beim Start automatisch eingebunden werden.

Wichtige Prüfungen nach Änderung:

```
cp /etc/fstab /etc/fstab.bak

mount -a

findmnt

df -h
```

Prüfungsfalle:

```
/dev/sdb1 kann sich ändern.
UUIDs sind für dauerhafte Mounts oft stabiler.
```

Merksatz:

```
fstab nie ungetestet ändern.
```

Logs und Monitoring

Aufgabe	Befehl
systemd-Journal anzeigen	journalctl
Dienstlogs anzeigen	journalctl -u dienst
Logs live anzeigen	journalctl -f

Aufgabe	Befehl
Logs seit Boot anzeigen	journalctl -b
Kernelmeldungen anzeigen	dmesg
Logdatei lesen	less logfile
Logdatei live lesen	tail -f logfile
Logs filtern	grep
Dienststatus prüfen	systemctl status dienst
CPU und Prozesse prüfen	top
RAM prüfen	free -h
Speicher prüfen	df -h

Merksatz:

> Dienstproblem:
> status prüfen,
> dann Logs lesen.

Typische Logorte

Ort	Bedeutung
/var/log	klassische Logdateien
/var/log/syslog	allgemeine Logs, häufig Debian/Ubuntu
/var/log/messages	allgemeine Logs, häufig RHEL/Fedora-Umfeld
/var/log/auth.log	Authentifizierung, häufig Debian/Ubuntu
/var/log/secure	Authentifizierung, häufig RHEL/Fedora-Umfeld
journalctl	systemd-Journal
dmesg	Kernelmeldungen

Merksatz:

> Nicht jede Distribution nutzt dieselben Logdateinamen.

Shell, Pipes und Umleitungen

Zeichen / Befehl	Bedeutung

|	Pipe, Ausgabe an nächsten Befehl
>	Ausgabe in Datei schreiben und überschreiben
>>	Ausgabe anhängen
<	Datei als Eingabe nutzen
2>	Fehlerausgabe umleiten
&>	Ausgabe und Fehler gemeinsam umleiten
/dev/null	Ausgabe verwerfen
;	Befehle nacheinander
&&	nächster Befehl nur bei Erfolg
||	nächster Befehl nur bei Fehler
$?	Exit-Code des letzten Befehls

Merksatz:

> überschreibt.
>> hängt an.
2> leitet Fehler um.

---

stdin, stdout und stderr

Kanal	Nummer	Bedeutung
stdin	0	Standardeingabe
stdout	1	Standardausgabe
stderr	2	Standardfehler

Prüfungsfalle:

Fehlermeldungen gehen nicht automatisch über stdout.
Deshalb reicht > nicht immer,
um Fehler umzuleiten.

Merksatz:

0 Eingabe,
1 Ausgabe,
2 Fehler.

Bash-Scripting wiederholen

Element	Bedeutung
#!/bin/bash	Shebang für Bash
chmod +x script.sh	Skript ausführbar machen
./script.sh	Skript aus aktuellem Verzeichnis starten
$1	erster Parameter
$#	Anzahl Parameter
"$@"	alle Parameter sauber einzeln
$?	Exit-Code des letzten Befehls
if	Bedingung
for	Schleife über Werte
while	Schleife solange Bedingung wahr ist
case	Auswahl nach Muster
read	Benutzereingabe lesen
function	wiederverwendbarer Skriptblock

Merksatz:

```
Skripte automatisieren Befehle,
aber auch Fehler,
wenn sie schlecht geschrieben sind.
```

Sichere Bash-Regeln

Wichtige Regeln:

```
Variablen meistens quoten

"$VARIABLE"

Parameter prüfen

Exit-Codes beachten
```

```
gefährliche Befehle vorher testen

absolute Pfade nutzen,
besonders bei cron

Logs schreiben

Skripte zuerst in Testumgebung prüfen

Kommentare für Zweck und Ablauf nutzen
```

Typische strenge Optionen:

```
set -euo pipefail
```

Merksatz:

```
In Skripten erst prüfen,
dann handeln.
```

Sicherheit wiederholen

Wichtige Sicherheitsprinzipien:

Thema	Kerngedanke
Least Privilege	nur notwendige Rechte
Updates	bekannte Schwachstellen schließen
Firewall	unnötige Zugriffe blockieren
SSH-Härtung	sicheren Administrationszugang
Dienstkonten	Dienste nicht unnötig als root
Logging	Ereignisse nachvollziehen
Monitoring	Probleme früh erkennen
Backups	Wiederherstellung ermöglichen
Dokumentation	Betrieb nachvollziehbar machen

Merksatz:

Sicherheit ist kein einzelner Befehl,
sondern ein Betriebskonzept.

Backup wiederholen

Begriff	Bedeutung
Backup	Sicherung von Daten
Restore	Wiederherstellung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Vollbackup	vollständige Sicherung
inkrementell	Änderungen seit letztem Backup
differentiell	Änderungen seit letztem Vollbackup
Snapshot	Zustand zu einem Zeitpunkt
3-2-1-Regel	mehrere Kopien, unterschiedliche Orte, externe Kopie

Merksatz:

RPO = Datenverlust.
RTO = Wiederherstellungszeit.

Automatisierung wiederholen

Werkzeug	Zweck
Bash-Skript	Befehlsfolge automatisieren
cron	zeitgesteuerte Aufgaben
systemd Timer	zeitgesteuerte systemd-Units
logrotate	Logs rotieren
Monitoring	Zustand überwachen
Alerting	bei Problemen benachrichtigen

Wichtig:

Automatisierung braucht Logs,
Exit-Codes,
Monitoring
und Dokumentation.

Merksatz:

Automatisierung ohne Kontrolle kann unbemerkt ausfallen.

Linux im Serverbetrieb wiederholen

Typische Serverrollen:

Rolle	Beispiel
Webserver	nginx, Apache
Datenbankserver	PostgreSQL, MariaDB
Dateiserver	Samba, NFS
DNS-Server	BIND, Unbound
DHCP-Server	DHCP-Dienst
Container-Host	Docker, Podman
Backupserver	Backupdienste
Monitoringserver	Überwachungssystem
Reverse Proxy	nginx, Proxy-Dienst
VPN-Server	WireGuard, OpenVPN

Merksatz:

Server ist eine Rolle,
nicht nur ein bestimmtes Gerät.

Standardports wiederholen

Dienst	Port
SSH	TCP 22
DNS	TCP/UDP 53

Dienst	Port
DHCP	UDP 67/68
HTTP	TCP 80
HTTPS	TCP 443
SMB	TCP 445
MySQL/MariaDB	TCP 3306
PostgreSQL	TCP 5432
SMTP	TCP 25
IMAP	TCP 143
IMAPS	TCP 993
POP3	TCP 110
POP3S	TCP 995
NTP	UDP 123

Merksatz:

> Port immer mit Protokoll nennen:
> TCP oder UDP.

Typische IHK-Fehlerfragen

Fehlerbild	Erste sinnvolle Prüfungen
Dienst startet nicht	systemctl status, journalctl -u, Konfiguration, Rechte, Port
Webseite nicht erreichbar	Dienst, Port, curl lokal, Firewall, DNS, Logs
SSH geht nicht	Netzwerk, Port 22, sshd, Firewall, Benutzer, Schlüssel
Speicher voll	df -h, df -i, du -sh, Logs, Backups
DNS geht nicht	IP-Test, dig, resolv.conf, DNS-Server, /etc/hosts
Permission denied	whoami, id, ls -l, ls -ld, Gruppen
No such file	pwd, ls, Pfad, Groß-/Kleinschreibung, Mount
Containerdaten weg	Volumes, Bind Mounts, Container-Dateisystem
Backup fehlgeschlagen	Logs, Ziel, Rechte, Speicher, Netzwerk
System langsam	top, free -h, df -h, iowait, Logs

Merksatz:

```
Fehlerbild lesen,
Ebene erkennen,
gezielt prüfen.
```

Fehlersuche: Standardreihenfolge

Bei vielen Linux-Problemen hilft diese Reihenfolge:

```
1. Fehler genau lesen

2. betroffenen Bereich bestimmen

3. letzte Änderung prüfen

4. Status prüfen

5. Logs prüfen

6. Ressourcen prüfen

7. Rechte prüfen

8. Netzwerk prüfen

9. Konfiguration prüfen

10. Maßnahme dokumentieren
```

Merksatz:

```
Nicht raten,
sondern eingrenzen.
```

Von innen nach außen prüfen

Bei Dienstproblemen:

1. Läuft der Prozess?

2. Läuft der Dienst laut systemctl?

3. Gibt es Fehler in journalctl?

4. Lauscht der Port lokal?

5. Antwortet der Dienst lokal?

6. Antwortet der Dienst über Server-IP?

7. Funktioniert Zugriff aus dem Netzwerk?

8. Stimmen DNS,
   Firewall
   und Anwendung?

Merksatz:

Erst lokal prüfen,
dann Netzwerk,
dann DNS,
dann Anwendung.

Häufige Prüfungsfallen

Falle	Richtig denken
ping geht, also Dienst geht	ping prüft nicht TCP/UDP-Dienst
Dienst läuft, also erreichbar	Port, Firewall und Bind-Adresse prüfen
apt update installiert Updates	apt update aktualisiert Paketlisten
enable startet Dienst sofort	enable aktiviert Autostart
/ und /root verwechseln	/ Dateisystemwurzel, /root Root-Home
x bei Verzeichnissen vergessen	x bedeutet betreten
chmod 777 als Lösung	unsicher und meist falsch
Backup ohne Restore-Test	unzuverlässig

Falle	Richtig denken
Snapshot als Backup-Konzept	nicht automatisch ausreichend
cron wie normale Shell behandeln	andere Umgebung
> und >> verwechseln	> überschreibt, >> hängt an
stderr vergessen	Fehlerkanal ist 2

Kleine Prüfungsaufgaben mit Kurzantwort

Aufgabe	Kurzantwort
Aktuelle IP anzeigen	ip addr
Standardgateway anzeigen	ip route
Dienststatus prüfen	systemctl status dienst
Dienstlogs anzeigen	journalctl -u dienst
Speicherplatz prüfen	df -h
Inodes prüfen	df -i
RAM prüfen	free -h
Prozesse prüfen	ps aux oder top
offene Ports anzeigen	ss -tulpen
Text in Datei suchen	grep "text" datei
Datei suchen	find /pfad -name "datei"
Datei ausführbar machen	chmod +x datei
Besitzer ändern	chown benutzer datei
Paketlisten aktualisieren	apt update
Pakete aktualisieren	apt upgrade
SSH verbinden	ssh benutzer@server

IHK-sichere Kurzformulierungen

Linux ist ein Mehrbenutzersystem, das Zugriffe über Benutzer, Gruppen und Rechte steuert.

Ein absoluter Pfad beginnt mit /, ein relativer Pfad bezieht sich auf das aktuelle Verzeichnis.

Dienste werden auf vielen Distributionen mit systemd verwaltet. systemctl dient zur Verwaltung der Dienste, journalctl zur Auswertung der Logs.

apt update aktualisiert Paketlisten, apt upgrade aktualisiert installierte Pakete.

ping prüft ICMP-Erreichbarkeit, ersetzt aber keinen Test eines TCP- oder UDP-Dienstes.

df -h zeigt freien und belegten Speicherplatz von Dateisystemen, du -sh zeigt die Größe eines Verzeichnisses.

RPO beschreibt den maximal akzeptablen Datenverlust, RTO die maximal akzeptable Wiederherstellungszeit.

Ein Backup ist erst zuverlässig, wenn ein Restore erfolgreich getestet wurde.

Abschluss-Merksätze

Linux verstehen heißt:
Struktur,
Rechte,
Dienste,
Logs
und Netzwerk verstehen.

Nicht jeder Fehler ist ein Linux-Fehler.
Oft ist es Netzwerk,
DNS,
Rechte,
Speicher,
Dienst
oder Konfiguration.

Befehle sind Werkzeuge.
Entscheidend ist,
wann man welchen Befehl warum nutzt.

In der Prüfung immer fachlich sauber begründen.

Erst prüfen,
dann ändern.

Erst sichern,
dann konfigurieren.

Erst lokal testen,
dann extern testen.

Erst Logs lesen,
dann Maßnahmen ableiten.

Keine pauschalen 777-Rechte.

Kein blindes sudo.

Keine ungetesteten fstab-Änderungen.

Kein Backup ohne Restore-Test.

Keine Automatisierung ohne Logs.

Keine Serveränderung ohne Dokumentation.