

1. /etc/passwd:

- o für jeden lesbar
- o Inhalt:

```

Nutzer:x:NutzerId :GruppenId :NutzerN :HomeVerz :LoginShell
root :x: 0 : 0 : :/root :/bin/bash
//"Administrator"
//NutzerId = 0 --> hat vollen Systemzugriff
... :x:... :... :... :... :...
//Systemnutzer (zw. root und normalen Nutzern)
tux :x: 500 : 100 :tux :/home/tux :bin/bash
//eigener Nutzer
//GruppenId = 100 --> Users-Gruppe
    
```

2. /etc/shadow:

- o nur lesbar für Nutzer mit vollem Systemzugriff
- o Inhalt:

```

Nutzer:Passwort:NutzerId:GruppenId:Nutzername:Homever:LoginShell
//das Passwort wird hier verschlüsselt abgelegt
    
```

3. /etc/hosts:

- o primitiver Nameserver
- o Inhalt:

```

IP-Adresse Name Name(kurz)
    
```

4. /dev:

- o //es müssen nicht alle Geräte vorhanden sein
- o hda
- o hda1
- o sda
- o fd0
- o lp0 //1. parallele Schnittstelle
- o tty //Konsolen //aktive Konsole (im Moment)
- o tty1 //Konsolen
- o tty7 //grafische Oberfläche

5. Ausgabe des Kommandos: "ls -l":

- o Inhalt:

| Spalte: 1      | 2     | 3          | 4      | 5                         | 6                   |
|----------------|-------|------------|--------|---------------------------|---------------------|
| Dateieigensch. | Links | Eigentümer | Gruppe | Nummer<br>(Treiber,Gerät) | Name<br>(der Datei) |
|                |       |            |        | 3,0                       |                     |
|                |       |            |        | 3,1                       |                     |

6. Kommandos:

- "cp":
  - o cp /etc/hosts /dev/tty4 →öffnet die Datei in der 4. Konsole
- /lib/modules:
  - o Treiber,...
- /proc/modules:
  - o welche Treiber im Moment geladen sind

- /proc/mounts:
  - welche Dateien im Moment gemountet sind
- /tmp:
  - temporärer Zwischenspeicher, der von den laufenden Programmen genutzt wird

## 1. ...Der Verzeichnisbaum:

|/usr | /var | /opt | User-System (Anwender-Programme):

- /usr
  - /usr/X11R6 → grafische Benutzeroberfläche
  - /usr/local → zur Installation eigener Anwenderprogramme
    - "local" → wird beim Systemupdate nicht überschrieben
  - /usr/share/doc
    - /howto → Hilfetexte zu komplexen Themen (z.B. Netzwerk einrichten)
    - /packages → Dokumentationen/Hilfen zu Anwenderprogrammen
- /var:
  - veränderbare und wachsende Dateien
  - /log → Protokolldateien
    - /messages → Messages des Kernel und laufender Anwendungen
    - /boot.msg
  - /spool/mail
- /opt:
  - kommerzielle und große Anwendungen (sonst = /var)
  - /opt/kde

|/root | /home | Heimatverzeichnis

- /root:
  - eigene Dateien von root
  - /root/. ... → Konfigurationsdateien und -verzeichnisse
- /home:
  - /tux → eigene Dateien des Nutzers tux

|/mnt | /media | Mountverzeichniss

## 2. Zugriffsrechte:

- Standard:

| Datei       | Bedeutung der Zeichen |                  |                     | Standardeinstellung |      |       |        | Oktal |
|-------------|-----------------------|------------------|---------------------|---------------------|------|-------|--------|-------|
|             | r                     | w                | X                   | Typ                 | User | Group | Others |       |
| Norm Datei  | Lesen                 | Schreiben        | Ausführen           | -                   | rw-  | r--   | r--    | 644   |
| Verzeichnis | Anzeigen              | Inhalt<br>ändern | In Verz<br>wechseln | d                   | rwX  | r-X   | r-X    | 755   |

all = user+group+others

- Zugriffsrechte können auch in Oktalschreibweise ausgedrückt werden:
  - r = 4, w = 2, x = 1
- Sonderfälle:
  - t-Bit: → /tmp: d|rwX|rwX|rwt  
→ t-Bit: eingeschränktes Änderungsrecht: nur der Eigentümer darf löschen!
  - s-Bit → /bin/mount: -|rws|...|...  
→ wenn ein normaler User(!= Eigentümer) die Datei nutzen will, dann hat er dazu root-Rechte. (denn er muss zum Mounten die Mount-Tabelle ändern.)
  - S-Bit → ... ..  
→ Wer diese Dateien ausführt, der tut das mit den Rechten der Gruppe
- Kommando: "chmod"
  - Zugriffsrechte für Dateien und Verzeichnisse ändern
  - `chmod a+rx datei_xyz` → alle (a) erhalten zusätzlich (+) auf `datei_xyz` rx-Rechte (rx)
  - oder `umask...`

## 3. Die Shell:

- Zustände:
  1. Login Shell: → Passworteingabe
  2. Interaktive Shell: → wenn Passwort akzeptiert
- Standard-Shell: **bash** (bourne again shell)
  - Konfiguration der bash:
  - /etc/profile → Hauptkonfigurations-Datei
    - /etc/profile kann auch eventuell noch andere Dateien (profile.local, profile.dos, bash.bashrc, ... (und für „eigene Einstellungen“ : ~/bash.profile, ~/.profile, ~/.bashrc, ...)) aufrufen, aber das steht dann in der /etc/profile drin.
    - ...umask 022... → Zeile in /etc/profile  
→ verändert die Standardeigenschaften von normalen Dateien (666) auf 644 und von Verzeichnissen (777) auf 755.
  - #Make Path more comfortable ...  
... PATH = /usr/local/bin:/usr/bin:/usr/X11R6/bin:/bin  
▪ gibt an, wo die Dateien der Kommandos drin stehen → wo gesucht werden soll
  - test „\$UID“ = 0 && ...
    - „test...= 0“ → Bedingung prüfen
    - „&&...“ → nachfolgendes ausführen, falls true
    - „\$“ → Zugriff auf den Wert einer Variablen

- root-Kommandos:
  - auch „normale User“ können root-Kommandos ausführen
    - suchen der Datei mit **whereis**-Kommando
    - ausführen: Angabe mit komplettem Pfad
    - ABER: Zugriffsbeschränkung durch gegebene Rechte
- /etc/bash.bashrc:
  - Variable PS1 definiert den Prompt
    - Falls UID=0 → PS1 = „\h:\w#“
      - „\h“ → Rechnername
      - „\w“ → aktuelles Verzeichnis
      - linux:~# → Beispiel
    - sonst → PS1 = „\u@\h:\w>“
      - tux@linux:~> → Beispiel
- Variablen in Kommandos setzen:
  - PS1=„hallo“ → Variable=Wert
- **printenv** Kommando:
  - enthält die Werte von Variablen
    - HOME, PATH, PS1, PWD (→ Arbeitsverzeichnis), HLISTSIZE (sagt wie viele Kommandos sich die Shell merkt), HOSTNAME, USER (eingeloggter User)
    - echo \$PATH → gibt den Wert von PATH aus