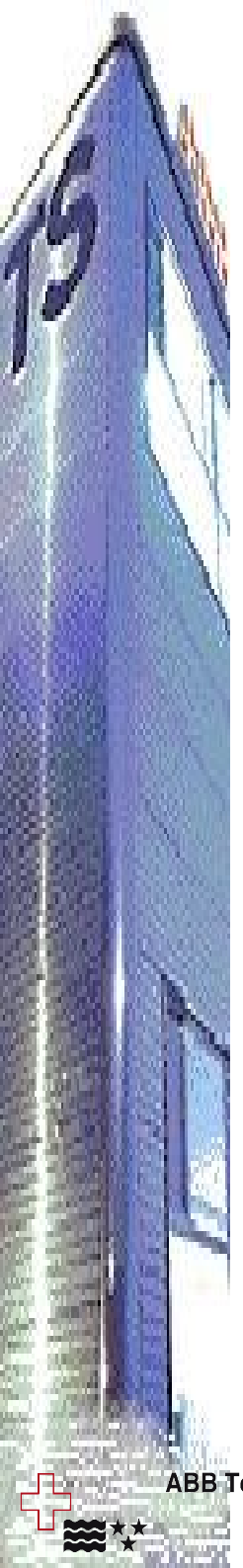
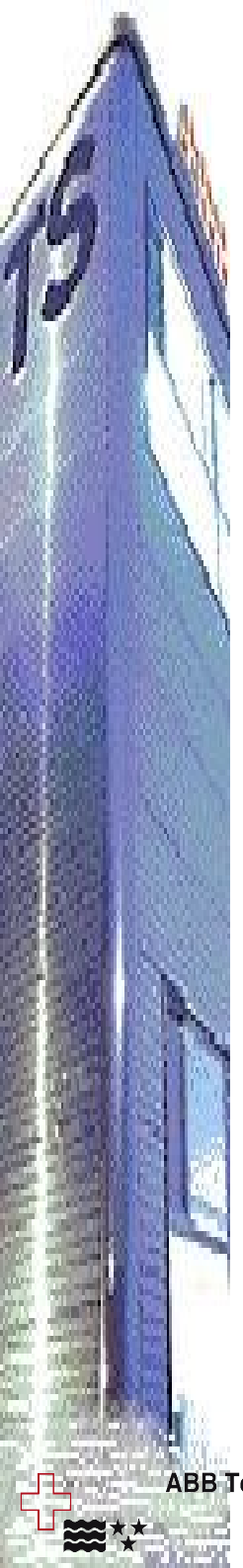


Benutzerverwaltung

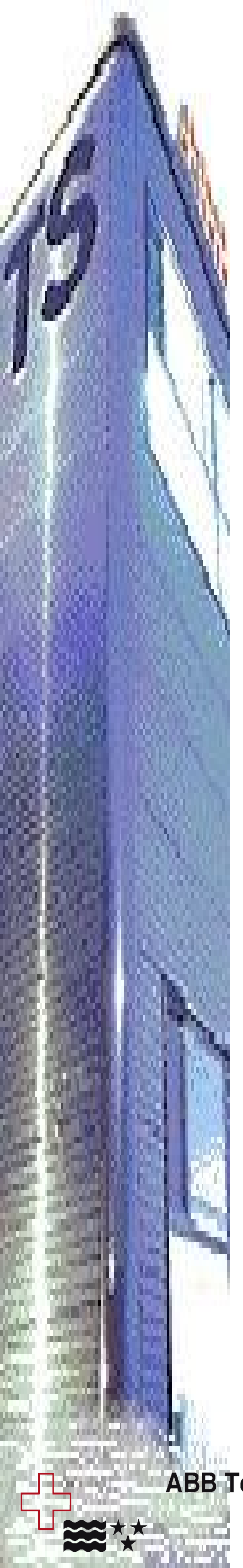
Ziele

- Das Benutzer- und Gruppenkonzept von Linux verstehen
- Die Struktur und Speicherung von Benutzer- und Gruppendaten kennen
- Die Kommandos zur Verwaltung von Benutzer und Gruppen anwenden können



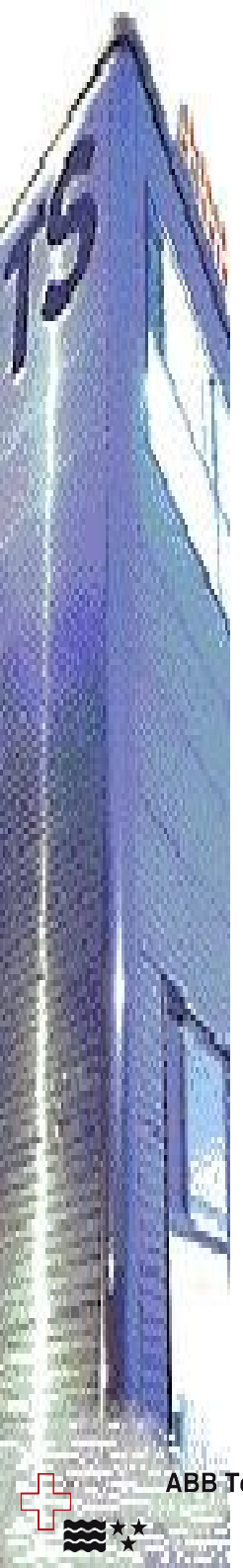
Wozu Benutzer?

- UNIX/Linux ist ein Multiuser-System
- Benutzer müssen sich am System anmelden
- Benutzer können auf gemeinsame Ressourcen zugreifen
  - Fileserver
  - Printserver
  - Koordination von mehrstufigen Arbeitsprozessen
  - Kommunikation in Arbeitsgruppen und Unternehmen



Benutzer und Gruppen

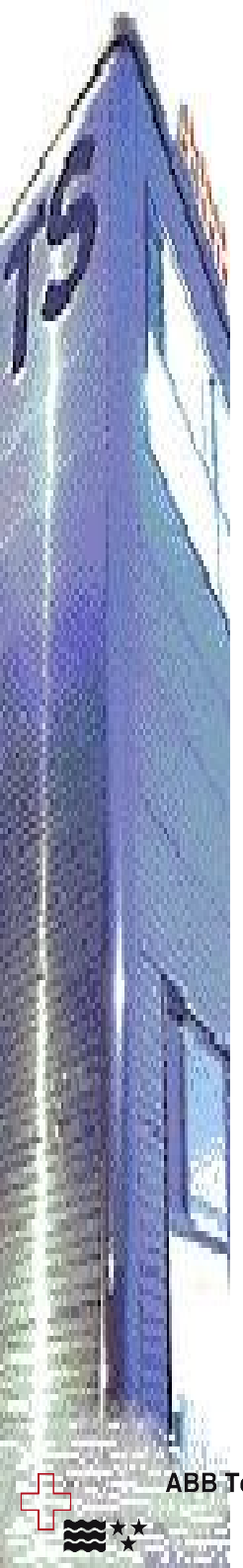
- Benutzer haben eine textuelle Kennung
- Benutzer haben eine im System eindeutige UID
  - der Benutzer „root“ hat die UID = 0
- Der Kernel arbeitet nur mit der UID
- mehrere Benutzer können dieselbe UID haben
- Benutzer haben ein Homeverzeichnis



Benutzer und Gruppen

(Fortsetzung)

- Benutzer gehören immer zu einer Gruppe
- Gruppen haben eine eindeutige GID
- Der Kernel arbeitet nur mit der GID
- Benutzer können Mitglied von mehreren Gruppen sein
- Gruppen haben kein Homeverzeichnis



Pseudobenutzer

- sind Systeminterne Benutzer
  - für administrative Funktionen
- haben kein Login
- haben i.d.R. kein Homeverzeichnis
- sind Programmen zugeordnet
  - meist Hintergrundprozessen
- es gibt auch Pseudo Gruppen
  - z.B. für den Zugriff auf Geräte

Benutzerdaten

- die zentrale Benutzerdatenbank ist die Datei:
  - `/etc/passwd`
- pro Benutzer eine Zeile im Format:

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <Benutzername>
  - sollte aus Kleinbuchstaben und Ziffern bestehen
  - Unix unterscheidet oft nur die ersten 8 Zeichen
  - Linux hat diese Einschränkung nicht
  - in heterogenen Netzen sollte darauf Rücksicht genommen werden

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <Kennwort>
  - traditionell das verschlüsselte Kennwort
  - bei heutigen UNIX/Linux ein »x«
  - das Kennwort steht dann in `/etc/shadow`
- Jeder Benutzer kann sein Kennwort mit dem Kommando `passwd` ändern

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <UID>
- Der Kernel arbeitet nur mit der UID
  - eine Zahl zwischen 0 und $2^{32} - 1$
- Konvention:
  - UIDs 0 - 99 sind für das System reserviert
  - UIDs 100 - 499 für Softwarepakete
  - UIDs ab 500 (oder 1000) sind für Benutzer

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <GID>
- Primäre Gruppe des Benutzers
  - jeder Benutzer kann bis zu 32 weiteren Gruppen angehören (ab Kernel 2.6 beliebig)
  - Zuordnung in `/etc/group`
- Konvention:
  - nobody:*:65533:
  - nogroup:*:65534:

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <GECOS>
  - steht für „General Electric Comprehensive Operating System“
- enthält diverse Informationen über den Benutzer
  - seinen »richtigen« Namen und optionale Informationen wie z.B. die Zimmer- oder Telefonnummer

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <Heimatverzeichnis>
  - persönlicher Bereich des Benutzers
  - Profildateien
  - ein Benutzer befindet sich unmittelbar nach der Anmeldung dort

Benutzerdaten

<Benutzername>:<Kennwort>:<UID>:<GID>:<GECOS>:<Heimatverzeichnis>:<Shell>

- <Shell>
  - ein Programm, das von *login* nach der Anmeldung gestartet wird
  - in der Regel eine Shell
  - erlaubte Shells sind in der Datei `/etc/shells` aufgelistet
  - der Benutzer kann mit `chsh` die Shell ändern

Die Datei /etc/passwd

- Beispiel:

```
root:x:0:0:Systemadministrator:/root:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/false
otto:x:4711:100:Otto Normal:/home/otto:/bin/bash
```

- Prinzipiell ist es auch möglich, die Benutzerdatenbank anderswo zu lagern
  - NIS Datenbank
  - LDAP Verzeichnisdienst (z.B. ADS)

Die Datei /etc/shadow

- nur root darf die Datei schreiben
  - Mitglieder der Gruppe shadow dürfen lesen
- ist nicht Pflicht, aber dringend empfohlen
- bei Linux heute Standard
- pro Benutzer eine Zeile im Format:

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

Benutzerdaten

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

- <Benutzername>
  - dieser muss dem Eintrag in der Datei `/etc/passwd` entsprechen

Benutzerdaten

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

- <Kennwort>
  - das verschlüsselte Kennwort des Benutzers
    - DES, MD5, Blowfish, AES
- leer = Benutzer kann ohne Kennwort anmelden
- ! oder * = Benutzer kann nicht anmelden

Benutzerdaten

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

- <Änderung>
  - Datum der letzten Kennwortänderung in Tagen seit dem 1. Januar 1970
- <Min> (Anzahl Tage)
  - bis das Kennwort geändert werden darf
- <Max> (Anzahl Tage)
  - Gültigkeit des Kennwort

Benutzerdaten

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

- <Warnung>
  - Tage vor dem Ablauf der <Max>-Frist
- <Frist>
  - Tage nach <Max>-Frist bis Konto gesperrt
- <Sperre>
  - Datum an dem das Konto gesperrt wird in Tagen seit dem 1. Januar 1970

Die Datei /etc/shadow

<Benutzername>:<Kennwort>:<Änderung>:<Min>:<Max>:<Warnung>:<First>:<Sperre>:<Reserviert>

- Beispiel:

```
root:04Nu7ytVSI9js:10734:0:10000::::
bin:*:8902:0:10000::::
daemon:*:8902:0:10000::::
lp:*:9473:0:10000::::
man:*:8902:0:10000::::
at:*:8902:0:10000::::
sshd:!:12989:0:99999:7:::
dh:$2a$05$h.mY51hDL/6GzHMGoyf8XOejUGFCk.DCPFRnWrcHw8KWssOEwhd20
   :12989:0:99999:7:::
```

Benutzerdaten Ändern

- die Datumswerte in der Benutzer-datenbank können einzeln geändert werden:
  - `chage [Optionen] user`
    - Optionen:

      `[-m mindays][-M maxdays][-d lastday]`
      `[-I inactive][-E expiredate][-W warndays]`
- Anzeigen der Werte
  - `chage -l user`

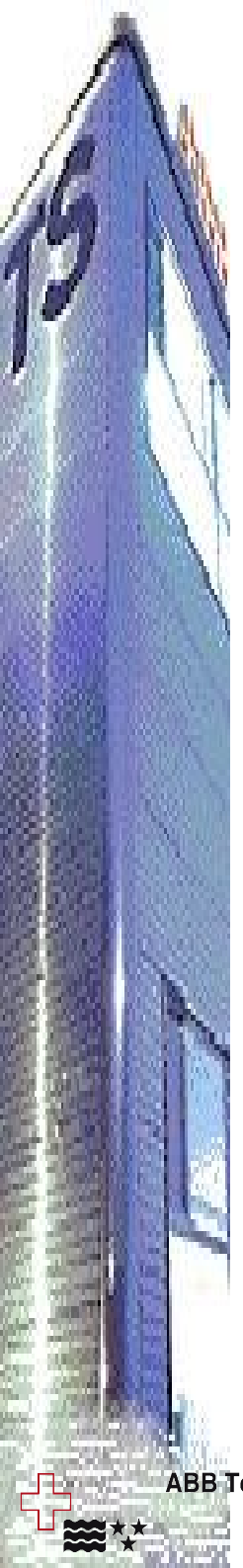
Verwaltung von Benutzerkonten

1. Einträge in der Datei `/etc/passwd`
   - gegebenenfalls in `/etc/shadow`
2. ein oder mehrere Einträge in der Gruppendatei `/etc/group`
3. Das Heimatverzeichnis wird erzeugt
   - evtl. eine Grundausstattung hinein kopiert
   - alles dem Benutzer übereignet

Verwaltung von Benutzerkonten

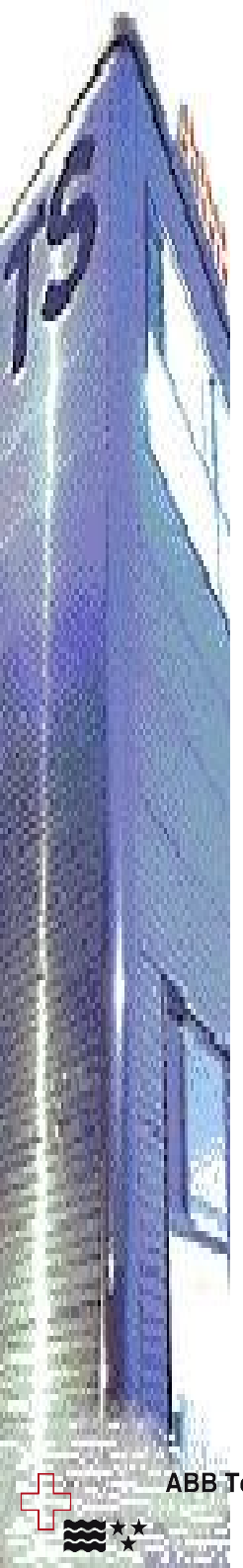
(Fortsetzung)

4. Wenn nötig, wird der Benutzer in weitere Listen eingetragen
   - z.B. für Plattenkontingente
   - Zugriffsberechtigung auf Datenbanken
   - spezielle Applikationen



Benutzerkonten einrichten

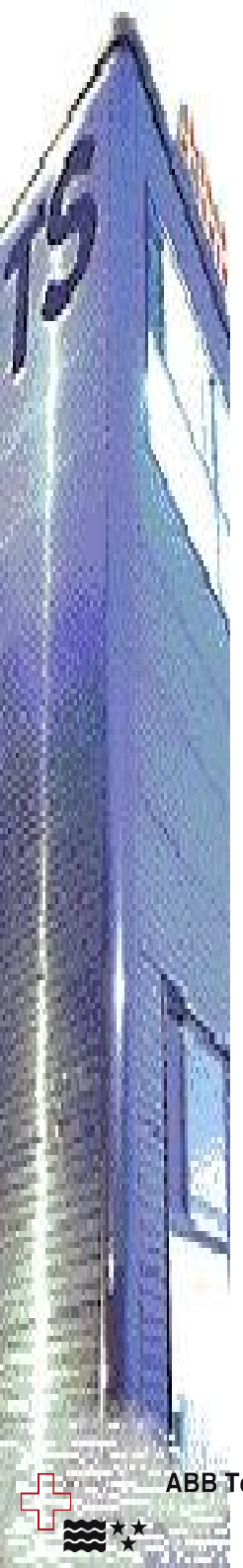
- jedes UNIX/Linux-Derivat bringt eigene grafische Werkzeuge zur Benutzer-verwaltung mit
- Ein Benutzerkonto kann natürlich auch „von Hand“ erstellt werden
- mit dem Kommandozeilen Programm `/usr/sbin/useradd`



Benutzerkonten einrichten

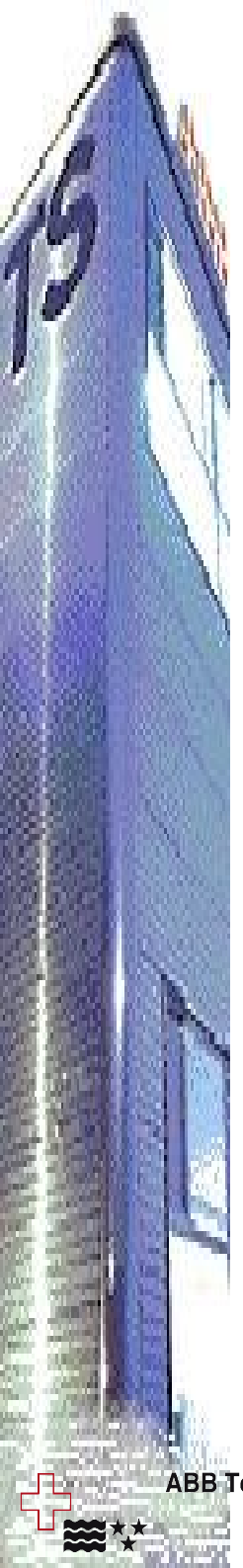
```
useradd [Optionen] <Benutzername>
```

-c “Kommentar“	Eintrag ins GECOS-Feld
-u <UID>	Numerische Benutzerkennung
-g <Gruppe>	Primäre Gruppe
-G <Gruppe>[,<Gruppe>]. . .	Weitere Gruppen
-d <Heimatverzeichnis>	
-s <Shell>	Login-Shell des Benutzers
-m	Legt das Heimatverzeichnis an



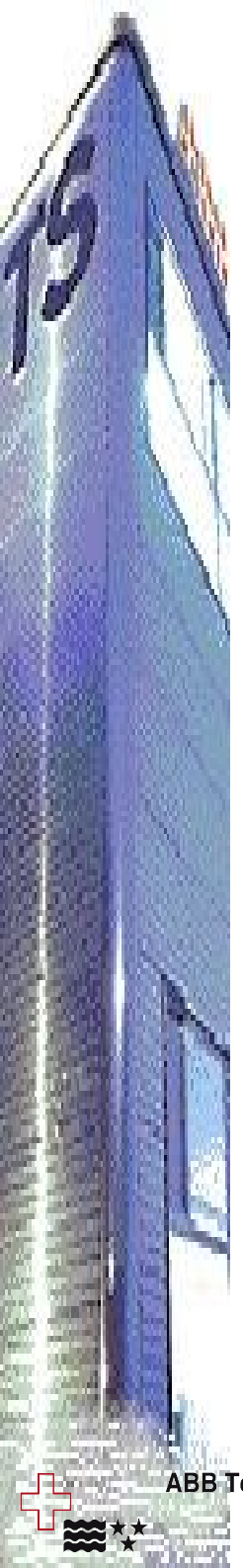
Benutzerkonten einrichten

- useradd verwendet default Werte
  - `/etc/default/useradd`
  - `/etc/skel` (Verzeichnis)
    - enthält z.B.
      `.profile, .Xdefaults .vimrc`
- Anzeigen oder ändern der Werte
- `useradd -D [Option] <Wert>`



Das Kommando `passwd`

- Der Befehl `passwd` dient der Vergabe von Benutzerkennwörtern
  - `passwd otto`
- nur „root“ kann Kennwörter vergeben
- Benutzer können ihr Kennwort ändern
  - Sie müssen ihr altes Kennwort kennen



Konten löschen und stilllegen

- Löschen eines Benutzerkontos durch entfernen der Einträge in
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/group`
  - Homeverzeichnis löschen
  - ev. Mailbox in `/var/mail` entfernen
  - ev. Spoolverzeichnis `/var/spool` räumen
  - ev. `crontab`-Dateien löschen

Konten löschen und stilllegen

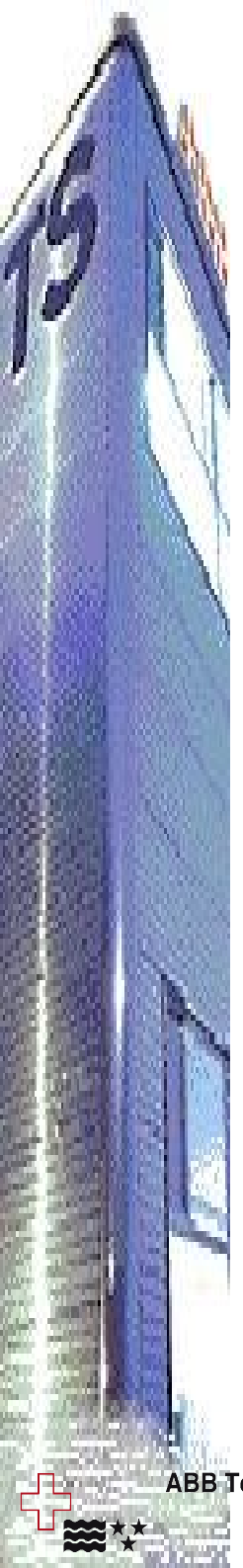
- mit dem Kommandozeilen Programm

```
/usr/sbin/userdel [-r] <Benutzername>
```

  - die Option `-r` entfernt Home und Mailbox

- andere Dateien des Benutzers müssen von Hand gelöscht werden

```
find / -uid <UID> -depth -exec rm -rf {} \;
```



Benutzerkonten und Gruppenzuordnung ändern

- traditionell, ändern der Dateien
  - `/etc/passwd`
  - `/etc/shadow`
  - `/etc/group`
- mit dem Kommandozeilen Programm
  - `usermod -g <Gruppe> <Benutzername>`
  - `chown -R tux /home/tux`
  - `chgrp -R users /home/tux`

Benutzerdatenbank direkt ändern

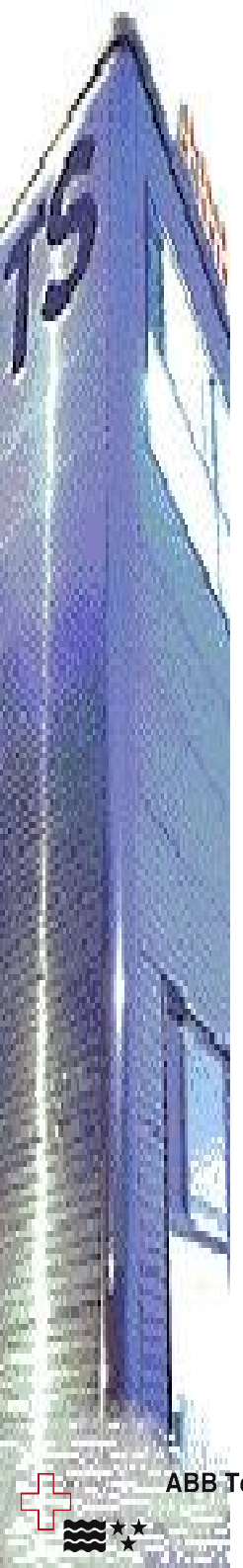
- das Kommando `vipw` ruft den Editor auf
  - ändert `/etc/passwd`
  - Option `-s` ändert `/etc/shadow`
- den Editor bestimmt die Variable
  - `VISUAL`

    oder
  - `EDITOR`

Fragen?

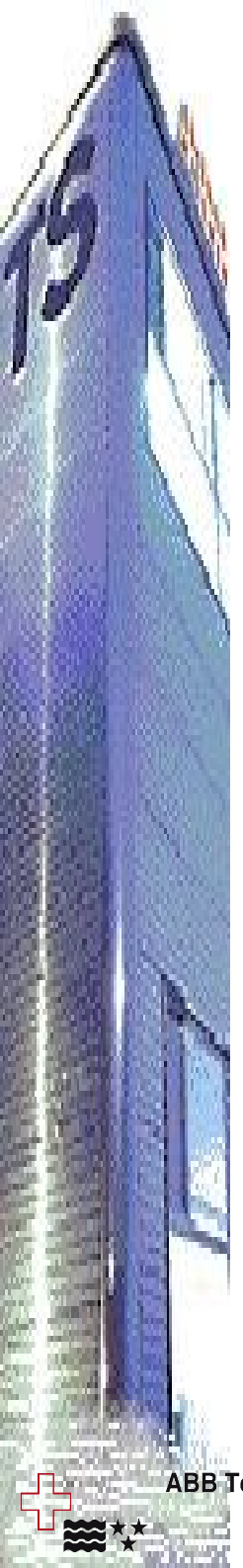
Übungen

- [2.6] Legen Sie den Benutzer test an. Wechseln Sie auf das Benutzerkonto test und legen Sie mit touch einige Dateien an, einige davon in einem anderen Ordner als dem Heimatverzeichnis (etwa /tmp). Wechseln Sie wieder zurück zu root und ändern Sie die UID von test.
- Was sehen Sie, wenn Sie mit ls die Dateien von Benutzer test auflisten?



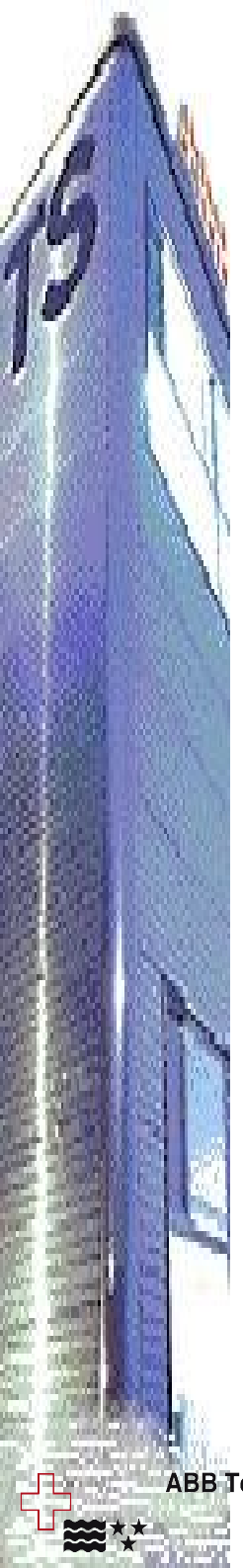
Übungen

- [2.7] Legen Sie einen Benutzer test1 über das entsprechende grafische Tool an, einen anderen, test2, mit Hilfe des Kommandos useradd und einen weiteren, test3, von Hand.
  Betrachten Sie die Konfigurationsdateien
- Können Sie problemlos unter allen drei Konten arbeiten?
  Legen Sie unter jedem Konto eine Datei an.



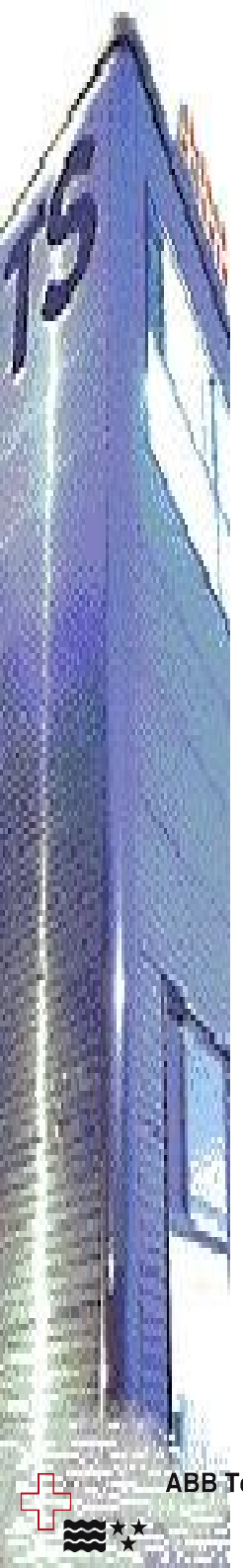
Übungen

- [2.8] Löschen Sie das Konto von Benutzer test2 und stellen Sie sicher, dass es auf dem System keine Dateien mehr gibt, die dem Benutzer gehören!



Übungen

- [2.9] Ändern Sie die UID des Benutzers test1.
- Was müssen Sie ausserdem tun?



Übungen

- [2.10] Ändern Sie das Heimatverzeichnis für Benutzer test1 um von /home/test1 in /home/user/test1

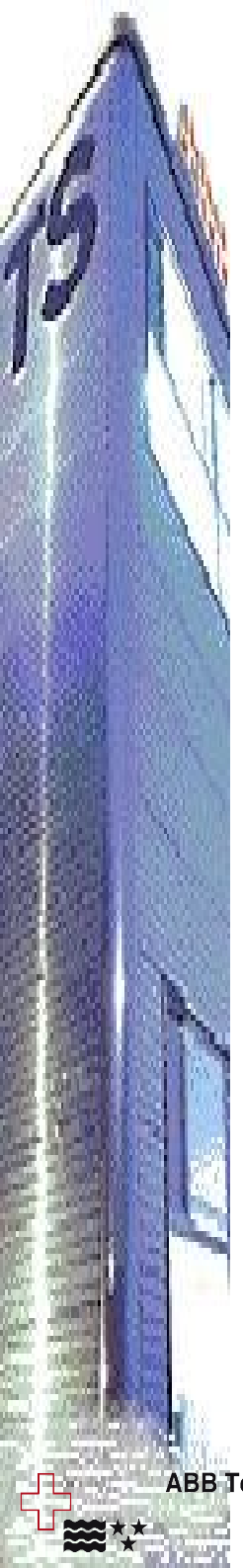
Kennwortverwaltung

- Kennwörter sind sehr wichtig für die Sicherheit im System
- `passwd -S franz`
  `franz LK 10/15/99 0 99999 7 0`
- `<Name> <Status> <MM/TT/JJ> <Min> <Max> <Warnung> <Frist>`
  - PS Kennwort ist gesetzt
  - LK gesperrtes Konto
  - NP kein Passwort gesetzt

Kennwortverwaltung

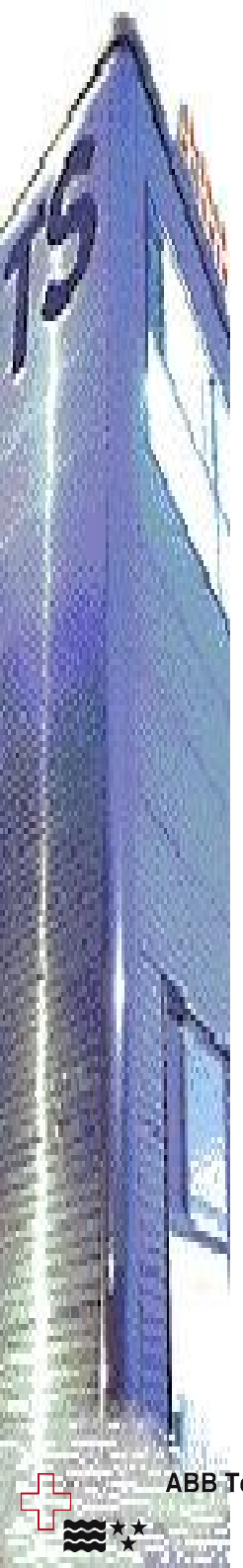
- Beispiele:
  - `passwd [-f|-s] <Benutzername>`
  - `passwd [-g] <Gruppenname>`
  - `passwd [-x <Max>] [-n <Min>]`
  - `passwd [-w <Warn>] [-i <Sperre>]`
  - `passwd [-l|-u|-d] <Benutzername>`

- `-d` Löscht ein vorhandenes Kennwort (Kann eine Sicherheitslücke verursachen!)



Auswahl von Kennwörtern

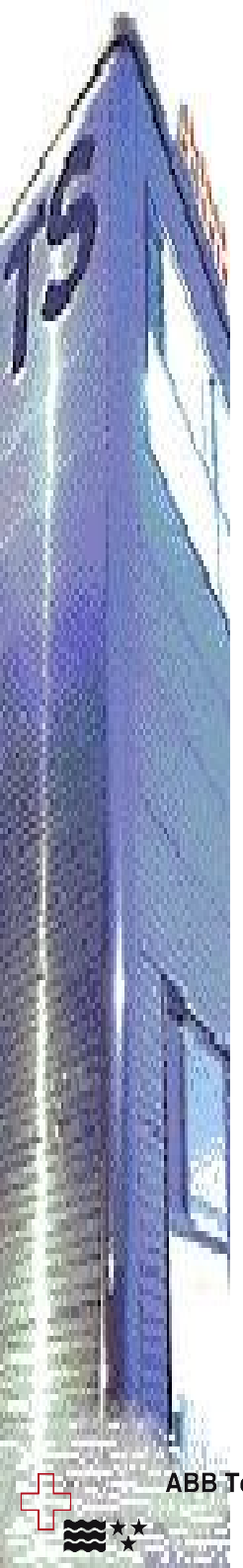
- Regeln für gute Kennwörter
  - Sie können alle Zeichen der Tastatur verwenden, sollten aber das Leerzeichen vermeiden
  - Es wird zwischen Gross- und Kleinschreibung unterschieden und Sie sollten auch beides verwenden
  - Im Kennwort sollten mindestens ein Sonderzeichen oder eine Zahl und zwei Buchstaben verwendet werden



Auswahl von Kennwörtern

(Fortsetzung)

- Das Kennwort sollte sich vom Benutzernamen unterscheiden (!)
- Vermeiden Sie Namen von Familienangehörigen, andere offensichtliche Kandidaten oder einfache Wörter aus dem Wörterbuch als Kennwort
- Ein Kennwort sollte mindestens 5 Zeichen, besser 8 Zeichen lang sein.
- Mehr als 8 Zeichen werden vom System möglicherweise nicht ausgewertet.

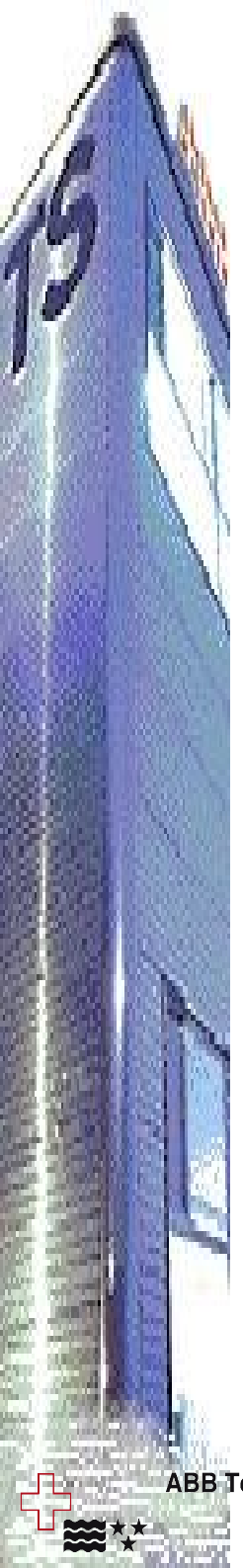


Übungen

- [2.11] Ändern Sie das Kennwort von Benutzer test1. Wie ändert sich die Datei /etc/shadow?
- Fragen Sie den Status zu diesem Kennwort ab.

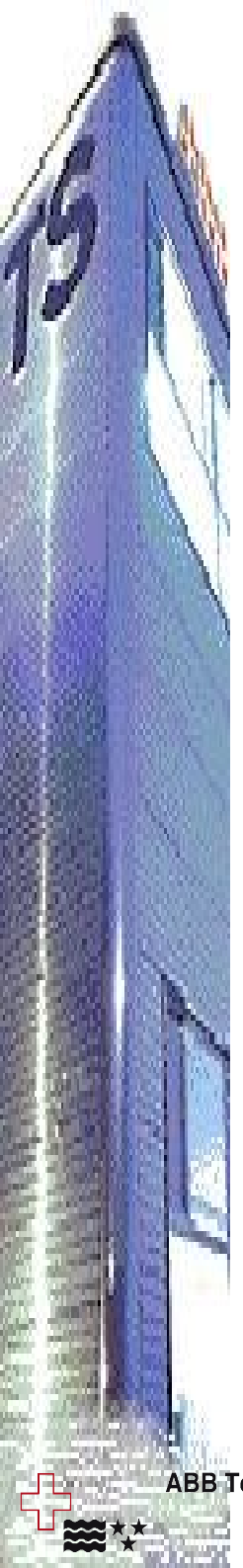
Übungen

- [2.12] Der Benutzer „trottel“ hat sein Kennwort vergessen. Wie können Sie ihm helfen?



Übungen

- [2.13] Stellen Sie die Bedingungen für das Kennwort von Benutzer test1 so ein, dass er sein Kennwort frühestens nach einer Woche und spätestens nach zwei Wochen ändern muss.
- Eine Warnung soll der Benutzer zwei Tage vor Ablauf dieser Zweiwochenfrist erhalten.
- Kontrollieren Sie anschliessend die Einstellungen!



Gruppenverwaltung

- jeder Benutzer gehört seiner „primären“ Gruppe an
  - steht in der Datei `/etc/passwd`
- jeder Benutzer kann beliebig vielen weiteren Gruppen angehören
  - steht in der Datei `/etc/group`
  - bis Kernel 2.4 maximal 32 Gruppen

Gruppenverwaltung

(Fortsetzung)

- das Kommando `id` zeigt ihre „primäre“ und alle weiteren Gruppen an
  - `id`

```
uid=500(tux) gid=100(users)
Gruppen=100(users),14(uucp),
16(dialout),17(audio),33(video)
```

- Das Kommando `groups` zeigt nur die Namen Ihrer Gruppen an

Gruppenverwaltung

(Fortsetzung)

- mit `newgrp` kann ein Benutzer seine primäre Gruppe wechseln
  - zurück gehts mit `exit`
- ein Benutzer kann auch in eine mit Passwort geschützte Gruppe wechseln
- ein Kommando kann mit einer anderen primären Gruppe ausgeführt werden
  - `sg <gruppe> -c <Kommando>`

Die Datei /etc/group/

- die Mitglieder einer Gruppe stehen in der Datei `/etc/group`
- für jede Gruppe im System eine Zeile
- jede Zeile hat vier Felder durch ":" getrennt

```
<Gruppenname>:<Kennwort>:<GID>:<Mitglieder>
```

- die Mitglieder sind durch "," getrennt aufgelistet

Die Datei /etc/group/

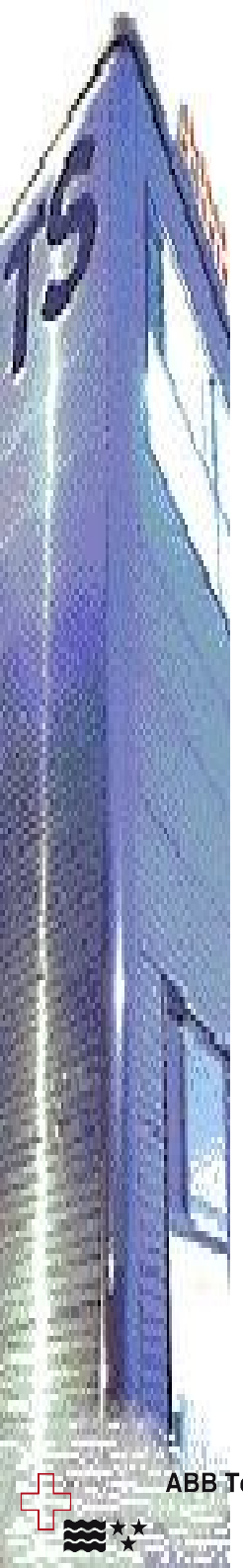
(Fortsetzung)

- ein Kennwort ist optional
  - ein “*“ verhindert einen Gruppenwechsel
  - ein “x“ verweist auf eine separate Kennwortdatei `/etc/gshadow`
  - Beispiel:

```
root:x:0:root
bin:x:1:root,daemon
users:x:100:
gruppe1:x:101:test1,test2
gruppe2:x:102:test2
```

Anlegen, Ändern und Löschen von Gruppen

- von Hand, durch Ändern der Datei `/etc/group` und ggf. `/etc/gshadow`
  - mit dem Kommando `vigr`
- Konvention:
  - die Gruppe 0 gehört immer „root“
  - Werte bis 99 sind meist Systemgruppen



Anlegen, Ändern und Löschen von Gruppen

- mit dem Kommando `groupadd` kann eine neue Gruppe erstellt werden
  - `groupadd [-g <GID>] <Gruppenname>`
- wird keine GID angegeben, so wird die nächste freie GID verwendet

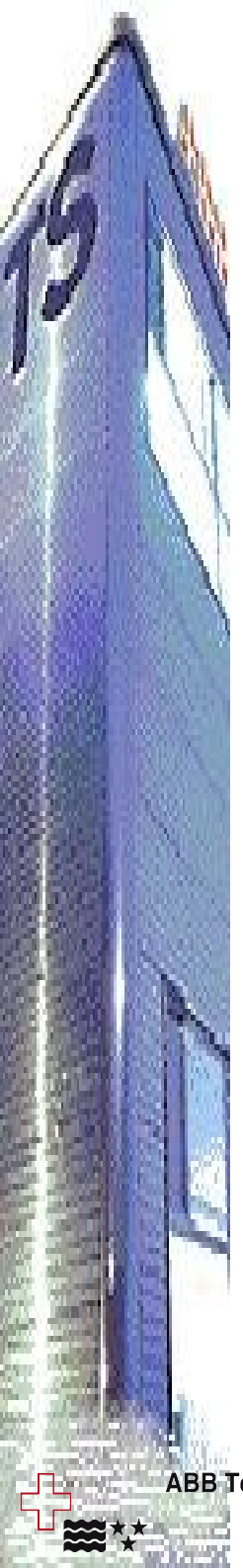
Anlegen, Ändern und Löschen von Gruppen

- Änderungen am Gruppennamen oder der GID werden mit `groupmod` gemacht
  - `groupmod [-g <GID>][-n <Name>] <Grpnamen>`
- beim Ändern von Namen bleibt die GID erhalten

Anlegen, Ändern und Löschen von Gruppen

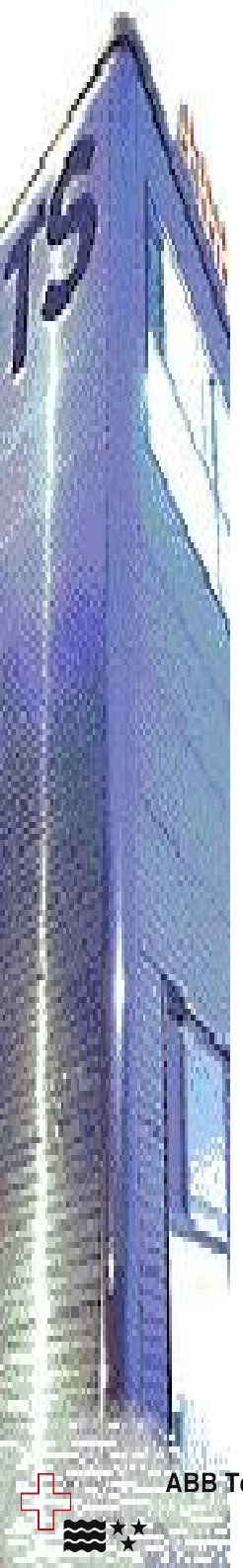
- Das Kommando `gpasswd` dient zur Manipulation von Gruppenkennwörtern
- einen Benutzer der Gruppe hinzufügen
  - `gpasswd -a <Benutzer> <Gruppe>`
- einen Benutzer aus der Gruppe löschen
  - `gpasswd -d <Benutzer> <Gruppe>`
- ein Gruppenadministrator benennen
  - `gpasswd -A <Benutzer>,... <Gruppe>`

Fragen?



Übungen

- [2.14] Wozu werden Gruppen gebraucht?
- Geben Sie mögliche Beispiele an!



Übungen

- [2.15] Können Sie ein Verzeichnis anlegen, auf das alle Mitglieder einer Gruppe Zugriff haben?

Aufgabe

- [2.16] Erstellen Sie eine zusätzliche Gruppe test.
  - Mitglied dieser Gruppe soll nur Benutzer test1 sein.
    Setzen Sie ein Gruppenkennwort.
  - Melden Sie sich als test1 und test2 an und wechseln Sie jeweils in die neue Gruppe!