

Benutzer- und Rechte-Verwaltung Teil 2

Linux-Kurs der Unix-AG

Andreas Teuchert

3. Juni 2014



Benutzer und Gruppen

- ▶ jeder Benutzer hat eine User-ID (UID)
- ▶ jede Gruppe hat eine Group-ID (GID)
- ▶ jeder Benutzer hat eine primäre Gruppe und beliebig viele sekundäre Gruppen
- ▶ primäre Gruppe wird auch als GID des Benutzers bezeichnet

- ▶ listet die UID, GID und Gruppenzugehörigkeiten auf
- ▶ wichtige Optionen:
 - ▶ -u: zeigt die UID an
 - ▶ -g: zeigt die GID der primären Gruppe an
 - ▶ -G: listet die GIDs aller Gruppen auf (primäre und sekundäre)
 - ▶ -n: nur in Kombination mit -u, -g und/oder -G: zeigt den zugehörigen Namen anstatt der ID an
- ▶ Argument:
 - ▶ optional: Benutzername eines anderen Benutzers
 - ▶ ohne Argument: wie Aufruf mit eigenem Benutzernamen

groups

- ▶ listet die Gruppenzugehörigkeiten auf
- ▶ hat keine Optionen
- ▶ Argument:
 - ▶ optional: Benutzername eines anderen Benutzers
 - ▶ ohne Argument: wie Aufruf mit eigenem Benutzernamen

Benutzer- bzw. Gruppen-Datenbank

- ▶ Benutzer: /etc/passwd
- ▶ Gruppen: /etc/group
- ▶ für alle Benutzer lesbar
- ▶ für root schreibbar

Passwortdatenbanken

- ▶ Benutzerpasswörter: /etc/shadow
- ▶ Gruppenpasswörter: /etc/gshadow
- ▶ nur für root les- und schreibbar
- ▶ Gruppenpasswörter werden äußerst selten benutzt

- ▶ sieben Spalten, durch „:“ getrennt
1. Benutzername
 2. Passwort („x“: Passwort steht in /etc/shadow)
 3. UID
 4. GID (der primären Gruppe)
 5. GECOS (Kommentarfeld, üblicherweise Name)
 6. home-Verzeichnis
 7. Shell (bei normalen Benutzern üblicherweise /bin/bash)

- ▶ neun Spalten, durch „:“ getrennt
1. Benutzername
 2. Passwort (gehasht)
 3. letzte Passwortänderung (in Tagen seit 01.01.1970)
 4. Mindestalter des Passwortes (in Tagen)
 5. Höchstalter des Passwortes (in Tagen)
 6. Warnfrist vor Passwortablauf (in Tagen)
 7. Zeit bis zur entgeltigen Sperre nach Ablauf (in Tagen)
 8. Ablaufdatum des Accounts (in Tagen seit 01.01.1970)
 9. reserviert (nicht benutzt)

- ▶ vier Spalten, durch „:“ getrennt
1. Gruppenname
 2. Gruppenpasswort („x“: Passwort steht in /etc/gshadow)
 3. Gruppen-ID
 4. Liste der Mitglieder
- ▶ Mitglieder sind alle Benutzer, die diese Gruppe als sekundäre Gruppe haben

Anmerkungen

- ▶ „*“ oder „!“ am Anfang des Passwortfelds in `/etc/shadow` verbietet Passwort-basierten Login
- ▶ „!“ wird benutzt um Benutzer zu sperren oder Login zu deaktivieren
- ▶ kein Zeichen im Passwortfeld bedeutet, dass ein Login ohne Passwort möglich ist (funktioniert i. d. R. nur lokal)
- ▶ bei modernen Linux-Distributionen: Passwörter in `/etc/shadow` und `/etc/gshadow` sind gehasht
- ▶ (kryptographischer) Hash: Einwegverschlüsselung

- ▶ setzt ein neues Passwort für einen Benutzer
- ▶ zeigt Informationen über Benutzer-Accounts an
- ▶ wichtige Optionen:
 - ▶ -S: zeigt Status-Informationen an:
 - ▶ Benutzernamen
 - ▶ Account-Status (**L**ocked, **N**o **P**assword, **P**assword)
 - ▶ letzte Passwortänderung als Datum
 - ▶ Mindest- und Höchst-Alter des Passwortes
 - ▶ Warnung und Frist vor Passwort-Ablauf
 - ▶ -d: löscht das Passwort eines Benutzers
 - ▶ -l: sperrt den Account eines Benutzers
 - ▶ -u: entsperrt den Account eines Benutzers
- ▶ Argument:
 - ▶ optional: Benutzername (nur root kann Passwörter anderer Benutzer ändern, löschen und Accounts (ent)sperren)
 - ▶ ohne Argument: wie Aufruf mit eigenem Benutzernamen

- ▶ erstellt einen neuen Benutzer für das System
- ▶ wichtige Optionen:
 - ▶ -c KOMMENTAR: Eintrag für das Kommentarfeld (GECOS)
 - ▶ -m: erstellt das home-Verzeichnis für den Benutzer (bei Standard-Einstellung wird kein home-Verzeichnis erstellt)
 - ▶ -g GID: primäre Gruppe als GID oder Name
 - ▶ -G GRUPPE1 ,GRUPPE2: sekundäre Gruppe(n) als GID oder Name, jeweils mit einem Komma getrennt
 - ▶ -u UID: UID des neuen Benutzers
 - ▶ -s SHELL: Shell des Benutzers
- ▶ Argument:
 - ▶ Benutzername (Login-Name) des Benutzers

useradd – Beispiel

- ▶ Benutzer anlegen:

```
useradd -c "Test-Benutzer" -m -g 100  
-G video,plugdev -u 1002 -s /bin/bash testuser
```

- ▶ die Gruppen `video` und `plugdev` geben dem Benutzer Zugriff auf Video-Geräte und erlauben es, Wechseldatenträger einzubinden
- ▶ `GID 100` muss vorher schon existieren
- ▶ unter Debian/Ubuntu: `GID 100: Gruppe users`
- ▶ Passwort setzen: `passwd testuser`

- ▶ enthält Konfigurationsdateien für neu angelegte Benutzer
- ▶ z. B. `.bashrc`
- ▶ Inhalt wird beim Anlegen des Benutzers ins Home kopiert

groupadd

- ▶ erstellt eine neue Gruppe
- ▶ wichtige Optionen:
 - ▶ -g GID: gibt die GID der neuen Gruppe an
- ▶ Argument:
 - ▶ Gruppen-Name der neuen Gruppe

usermod

- ▶ ändert einen Benutzer-Account
- ▶ wichtige Optionen:
 - ▶ `-G GRUPPE1, GRUPPE2 . . .`: legt die sekundären Gruppen fest, in Kombination mit `-a` werden neue Gruppen hinzugefügt
 - ▶ `-u NEUE_UID`: ändert die aktuelle UID des Benutzers
 - ▶ `-g GRUPPE`: ändert die aktuelle GID des Benutzers, die neue Gruppe muss bereits existieren
 - ▶ `-c` und `-s` analog zu `useradd`
- ▶ Argument:
 - ▶ Benutzernamen (Login-Name) des Benutzers

Debian-spezifisch: adduser, deluser, addgroup, delgroup

- ▶ nur bei Debian-basierte Systemen

Vorteile

- ▶ interaktiv: keine Optionen notwendig
- ▶ sinnvolle Standardeinstellungen für GID und Shell
- ▶ adduser legt Home automatisch an

Argumente

- ▶ Benutzername bzw. Gruppenname

Alle Befehle

Befehl	Optionen	Argument
id	-u, -g, -G, -n	[Benutzername]
groups		[Benutzername]
passwd	-S, -d, -l, -u	[Benutzername]
useradd	-c, -m, -g, -G, -u, -s	Benutzername
groupadd	-g	Gruppen-Name
usermod	-G, -a, -u, -g, -c, -s	Benutzername