

Benutzer- und Rechte-Verwaltung Teil 2

Linux-Kurs der Unix-AG

Sebastian Weber

13. Dezember 2013



Benutzer und Gruppen

- ▶ jeder Benutzer hat eine eindeutige UID und ist einer primären Gruppe zugeordnet
- ▶ die primäre Gruppe wird durch die GID festgelegt
- ▶ Benutzer können Mitglied beliebig vieler sekundärer Gruppen sein
- ▶ Vergabe zusätzlicher Rechte durch Mitgliedschaft in sekundären Gruppen

Benutzer- und Gruppen-Datenbank (1)

- ▶ Benutzer- bzw. Gruppen-Informationen sind in einzelnen Dateien gespeichert
- ▶ Benutzer- und Gruppen-Datenbank für jeden Benutzer lesbar
- ▶ Passwort-Datenbank nicht für jeden Benutzer lesbar

- ▶ 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- und Gruppen-Datenbank (2)

Benutzer- bzw. Gruppen-Datenbank

- ▶ Benutzer: `/etc/passwd`
- ▶ Gruppenzugehörigkeiten: `/etc/group`

Passwortdatenbanken

- ▶ Benutzer-Passwörter: `/etc/shadow`
- ▶ Gruppen-Passwörter: `/etc/gshadow`

Grundsätzlicher Aufbau

- ▶ Spalten jeweils durch ein „:“ getrennt
- ▶ /etc/passwd:
 - ▶ Benutzername, Passwort („x“), UID, GID, GECOS (Kommentarfeld), home-Verzeichnis, Shell
- ▶ /etc/shadow:
 - ▶ Benutzername, Passwort (hashed), letzte Passwortänderung, Mindest- und Höchstalter des Passwortes, Warnung und Frist vor Passwort-Ablauf, Kontosperr
- ▶ Passwortspalte in der /etc/passwd und /etc/group enthalten ein „x“
 - ▶ Verweis auf /etc/shadow bzw. /etc/gshadow

Benutzer- und Gruppen-Datenbank (4)

Anmerkungen:

- ▶ Wert für letzte Passwortänderung und Kontosperrung steht für die Anzahl der Tage seit dem 01.01.1970
- ▶ „*“ oder „!“ bei Passwort verbietet Passwort-basierten Login
- ▶ kein Zeichen im Passwortfeld bedeutet, dass ein Login ohne Passwort möglich ist
- ▶ bei modernen Linux-Distributionen: Passwörter in /etc/shadow und /etc/gshadow sind in verschlüsselter Form (üblicherweise MD5-, SHA-256- oder SHA-512-Hash mit salt)

- ▶ 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

useradd

- ▶ erstellt einen neuen Benutzer für das System
- ▶ wichtige Optionen:
 - ▶ -c KOMMENTAR: Eintrag für das Kommentarfeld (GECOS)
 - ▶ -d HOME: Verzeichnis für das home-Verzeichnis
 - ▶ -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, in Kombination mit -o können bereits vergebene UIDs benutzt werden
- ▶ Argument:
 - ▶ Benutzername (Login-Name) des Benutzers

groupadd

- ▶ erstellt eine neue Gruppe
- ▶ wichtige Optionen:
 - ▶ -g GID: gibt die GID der neuen Gruppe an, in Kombination mit -o können bereits vergebene GIDs benutzt werden
- ▶ Argument:
 - ▶ Gruppen-Name der neuen Gruppe

- ▶ ändert einen Benutzer-Account
- ▶ wichtige Optionen:
 - ▶ `-d NEUES_HOME`: gibt das neue home-Verzeichnis des Benutzers an, in Kombination mit `-m` wird der Inhalt des aktuellen home-Verzeichnisses in das neue verschoben
 - ▶ `-G GRUPPE1,GRUPPE2...`: legt die sekundären Gruppen fest, in Kombination mit `-a` werden neue Gruppen hinzugefügt
 - ▶ `-u NEUE_UID`: ändert die aktuelle UID des Benutzer, in Kombination mit `-o` können bereits vergebene UID benutzt werden
 - ▶ `-g GRUPPE`: ändert die aktuelle GID des Benutzers, die neue Gruppe muss bereits existieren
- ▶ Argument:
 - ▶ Benutzernamen (Login-Name) des Benutzers

Debian-spezifisch: adduser, deluser, addgroup, delgroup

- ▶ nur bei Debian-basierte Systemen (Debian, (X,K,L)Ubuntu)

Vorteile:

- ▶ interaktiv, benutzerfreundlicher
- ▶ Standard-Einstellungen lassen sich konfigurieren

Argument:

- ▶ Benutzername bzw. Gruppenname

Alle Befehle

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