Benutzer- und Rechte-Verwaltung Teil 2

Linux-Kurs der Unix-AG

Zinching Dang

26. November 2012

Zugriffsrechte (1)

- definieren, welche Benutzer welche Dateien lesen, schreiben und ausführen dürfen (**r**ead, **w**rite, e**x**ecute)
- sind jeder Datei und jedem Verzeichnis zugeordnet
- sind auf drei Ebenen definiert:
  - Besitzer: Zugriffsrechte für den Besitzer der Datei/des Verzeichnisses
  - Gruppe: Zugriffsrechte für alle Benutzer einer Gruppe
  - Gesamtheit aller Benutzer

Zugriffsrechte (2)

- das spezifischste Recht gilt für den Benutzer
  - Gruppenrechte überschreiben die Rechte für die Gesamtheit aller Benutzer
  - Besitzerrechte überschreiben die Gruppenrechte und die Rechte für die Gesamtheit

Zugriffsrechte (3)

Arten von Zugriffsrechten

- Leserecht: **r**ead
  - notwendig, um den Inhalt einer Datei/eines Verzeichnisses anzuzeigen
- Schreibrecht: **w**rite
  - notwendig, um eine Datei/ein Verzeichnis zu modifizieren
- Ausführungsrecht: e**x**ecute
  - bei Dateien: notwendig, um eine Datei als Programm zu starten
  - bei Verzeichnissen: notwendig, um auf das Verzeichnis zuzugreifen
  - ein `s` anstatt `x` steht für ein gesetztes SUID- bzw. SGID-Bit

Zugriffsrechte (4)

besondere Zugriffsrechte

- Set-UID-Bit (SUID-Bit, **s**)
  - startet ein Programm **immer** mit den Rechten des Besitzers
  - hat nur eine Wirkung auf Dateien
- Set-GID-Bit (SGID-Bit, **s**)
  - bei Dateien: startet ein Programm **immer** mit den Rechten der Gruppe
  - bei Verzeichnissen: neu erstellte Dateien und Ordner „erben“ die Gruppe des Verzeichnisses
- Sticky Bit (**t**)
  - Dateien, welche sich in einem Verzeichnis mit diesem Attribut befinden, können nur von dem Besitzer der Datei oder des Verzeichnisses (oder `root`) gelöscht werden

chmod

- ändert die Zugriffsrechte von Dateien und Verzeichnissen
- symbolische und numerische (oktale) Notation möglich
  - symbolisch: [ugoa][+-=][rwxXst]
  - oktal: [0-7][0-7][0-7][0-7]
- wichtige Optionen
  - `-c`: bei Modifikation anzeigen, was durchgeführt wurde
  - `-R`: rekursiv Dateien und Verzeichnisse ändern
- Argumente:
  - neue Zugriffsrechte (oktale oder symbolische Darstellung) und Datei/Verzeichnis

chown

- ändert den Besitzer und Gruppe von Dateien und Verzeichnissen
- wichtige Optionen:
  - `-c`: bei Modifikation anzeigen, was durchgeführt wurde
  - `-R`: rekursiv Dateien und Verzeichnisse ändern
- Argumente:
  - neuer Benutzer und Datei/Verzeichnis
  - optional: neue Gruppe, durch „:“ vom Benutzer getrennt

Benutzer- und Gruppen-Datenbank (1)

- Benutzer- bzw. Gruppen-Informationen sind in einzelnen Dateien gespeichert:
  - Benutzer: `/etc/passwd`
  - Benutzer-Passwörter: `/etc/shadow`
  - Gruppenzugehörigkeiten: `/etc/group`
  - Gruppen-Passwörter: `/etc/gshadow`
- Benutzer- und Gruppen-Datenbank für jeden Benutzer lesbar
- Passwort-Datenbank nicht für jeden Benutzer lesbar

Benutzer- und Gruppen-Datenbank (2)

Grundsätzlicher Aufbau

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

Benutzer- und Gruppen-Datenbank (3)

Anmerkungen:

- Wert für letzte Passwort-Änderung und Konto-Sperre 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)

passwd

- ändert das aktuelle Passwort eines Benutzers
- 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 (lokaler Login ohne Passwort danach möglich)
  - `-l`: sperrt den Account eines Benutzers
  - `-u`: entsperrt den Account eines Benutzers
- Argument:
  - optional: Benutzername (nur `root` kann Passwörter anderer Benutzer ändern)
  - 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

usermod

- ändert einen Benutzer-Account
- wichtige Optionen:
  - `-d NEUES_HOME`: gibt das neue (`home`)-Verzeichnis des Benutzers an, in Kombination mit `-m` wird das aktuelle `home`-Verzeichnis 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

Spickzettel

Alle Befehle

Befehl	Optionen	Argument
`passwd`	`-S`, `-d`, `-l`, `-u`	[Benutzername]
`chmod`	`-c`, `-R`	Zugriffsrechte, Datei
`chown`	`-c`, `-R`	Besitzer:Gruppe, Datei
`useradd`	`-c`, `-d`, `-m`, `-g`, `-G`, `-u`	Benutzername
`groupadd`	`-g`	Gruppen-Name
`usermod`	`-d`, `-G`, `-u` , `-g`	Benutzername