Kapitel 5

Nutzerverwaltung

Übersicht

Linux ist ein Mehrbenutzerbetriebssystem. Dementsprechend müssen im System den einzelnen Nutzern Rechte zugewiesen, um einen Rahmen abzustecken, was einzelne Nutzer auf einem System dürfen und eben auch nicht dürfen. Das Kapitel Nutzerverwaltung gibt Ihnen einen Einblick in die Struktuer der Nutzerverwaltung und deren Zugriffsrechte und zeigt Ihnen, wie Sie damit arbeiten können.

Lernziele
Nach Abschluss des Kapitels

- können Sie Nutzer und Gruppen anlegen sowie wichtige Änderungen vornehmen
- haben Sie eine Übersicht über die entsprechende Konfigurationen in der Nutzerverwaltung und
- Sie wissen, wie Sie Nutzern und Gruppen Rechte zuweisen und entziehen können.

5.1 Einleitung

Nutzerverwaltung und Rechtevergabe sind in Betriebssystemen wichtige Aufgaben der Systemadministration. Sie dienen nicht nur dem Schutz von persönlichen Daten einzelner Nutzer, die gemeinsam auf einem physikalischen System dienen. Auch zum Schutz des Systems gegen Angriff ist die Zuweisung von Nutzern und daran angelehnten Zugriffs- und Ausführungsrechten ein wesentlichen Bestandteil eines Schutzkonzeptes für einen Rechner oder ein Netzwerk.

5.2 Grundlagen der Nutzerverwaltung

Unix als Mehrbenutzerbetriebssystem erwartet eine dedizierte Anmeldung eines Nutzers durch eine Nutzername-Passwort-Kombination. Durch diesen Zwang zur Anmeldung soll sichergestellt werden, dass jeder Nutzer nur in für ihm zugewiesenen Bereichen Änderungen durchführen kann. Rechte der Nutzer betreffen auch das Ausführen von Programmen. Durch das Ausführen eines Programmes gehen auch automatisch alle Rechte des ausführenden Users an das ausgeführte Programm über. Dies ist wichtig, da damit das Programm auch erst in der Lage ist die Daten des Nutzers auch zu lesen. Programme können auch Schadprogramme sein (Viren, Würmer, Trojaner). Durch dieses Konzept wird damit auch sichergestellt, dass Schadsoftware nur mit den Rechten des aktuellen Nutzers ausgeführt werden kann. Es bedeutet aber auch, dass das Nutzermanagement und die Passwortvergabe ein essentieller Punkt in der Administration eines Systems sind.

5.3 Die Nutzerverwaltung

Nutzerdaten werden generell in der /etc/passwd verwaltet. Einsicht erhält man mit

```
1 $ less /etc/passwd
```

Der Aufbau der Datei: Name:Passwort:User-ID:Group-ID:Kommentar:Verzeichnis:Shell

Wichtig: nicht nur für reale Personen, sondern auch für Prozesse/Dienste/Daemons wird ein Nutzer angelegt. Dies ist aus Sicht der Sicherheit wichtig, da als Nutzer ausgeführte Programme auch mit Nutzerrechten versehen (z.B. Zugriffsrechte).

Erstellen eines Passwortes für den Nutzer passwd <nutzername>

Für sich selbst reicht die Eingabe:

```
1 $ passwd
```

Es wird nun nacheinander altes und neues Passwort abgefragt. Passwörter werden in der Regel in der /etc/shadow abgelegt, da die /etc/passwd frei auf dem System und damit angreifbar durch Bruteforce ist und mit Entschlüsselung das Passwortes damit das System geknackt werden könnte.

```
1 $ less /etc/shadow
```

Dies dürfte allerdings nicht zum Erfolg führen, da die Datei für die meisten Nutzer gesperrt ist.

Die Nutzerverwaltung muss nun allerdings nicht über die Bearbeitung einer Datei erfolgen, da das Anlegen eines Nutzers mehrere Schritte umfasst

- Anlegen des Eintrags in der passwd
- Anlegen eines Eintrags in der shadow
- Anlegen einer Gruppe
- Hinzufügen des Nutzers zur Gruppe
- Anlegen des Home-Verzeichnisses
- Anlegen der Basisstruktur im Home-Verzeichnis

Hierfür gibt mit adduser ein Tool, das diese Schritte nacheinander abarbeitet.

$adduser <nutzernamen>

mit Abfrage der relevanten Parameter/etc/shadow etc. durch adduser Für jeden Nutzer wird eigene Gruppe und Verzeichnis angelegt Homeverzeichnis wird auf Grundlage der /etc/skel erstellt.

```
1 cd /etc/skel
```

```
2 ls -a
```

Die Voreinstellungen für adduser werden in /etc/adduser.conf eingestellt. Es gibt auch useradd, dies erfordert allerdings manuelle Eingabe aller Punkte als Parameter.

Wechseln Sie auf die dritte Konsole und melden Sie sich dort als administrator root an:

```
1 adduser teststudent
```

Auf Konsole1 als student angemeldet bleiben Auf Konsole2 als teststudent anmelden Auf Konsole3 als Administrator angemeldet bleiben

Auch für das Löschen eines Nutzers gibt es einen Befehl

deluser [-Option] <nutzernamen> mit den Optionen -remove-home -remove-all-files -backup

Problem: Wenn beim löschen des Nutzers nicht alle Dateien entfernt werden, verbleiben Ruinen ohne Rechte.

Die Verwaltung von Gruppen erfolgt auf ähnlichem Weg:

Gruppendatei:

```
1 $ more /etc/group
```

Mit groups die Gruppen abfragen in denen man Mitglied ist.

```
1 $ groups
```

Neue Gruppe anlegen:

```
groupadd <gruppenname>
```

Nutzer zu Gruppe hinzufügen:

```
adduser <nutzername> <gruppenname>
```

Nutzer aus Gruppe löschen:

```
deluser <nutzername> <gruppenname>
```

Gruppe löschen:

```
delgroup <gruppenname>
deluser -group <gruppenname>
```

5.4 Grundlagen Rechteverwaltung

Betriebssysteme vergeben in der Regel Rechte, um auf Dateien und Verzeichnisse zugreifen zu dürften bzw. um zu vermeiden, dass unberechtigte Zugriff erhalten. Unix basierte Systeme verfolgen dabei einen einheitlichen und ausgereiften Ansatz, der eine sehr flexible Verteilung von Rechten für einzelne Nutzer und Gruppen von Nutzern erlaubt. Dieser Ansatz erfordert allerdings an einigen Stellen auch einige grundlegende Überlegungen, die der Administrator anstellen muss, um diese Rechte effizient zu verwalten.

Grundlage der Rechtevergabe sind die dem System bekannten Nutzer (User) und Gruppen (Groups). Diese können durch den Administrator angelegt und verwaltet werden. Wichtig ist dabei, dass im Dateisystem die Rechte über die UserID (UID) und GroupID (GID) verwaltet werden. Wird also ein Nutzer gelöscht und später mit gleichem Namen wieder angelegt, hat er in der Regel eine andere UID und damit nicht automatisch die gleichen Berechtigungen, wie der gelöschte Nutzer.

Auch in Netzwerken ist dies ein wichtiger Punkt, da beim Zugriff auf verteilte Ressourcen darauf geachtet werden muss, dass die Nutzerdaten entweder zentral verwaltet werden müssen oder aber alle Nutzer auf allen Maschinen die gleichen UIDs haben, um auf entsprechende Ressourcen zugreifen zu können.

5.5 Einsicht in die Berechtigungen

Zu jeder Datei werden Informationen gespeichert, ob und von wem sie gelesen, geschrieben oder ausgeführt werden kann.

Mit dem Befehl

```
ls -la
```

```
1
2
```

kann man sich den Inhalt des aktuellen Verzeichnisses inklusive der Zusatzinformationen anzeigen lassen.

Die Ausgabe des ls-Befehls sieht dann in etwa wie folgt aus:

```
1 drwxr-xr-x 3 wdorner wdorner  4096 2012-04-05 21:31 .
2 drwxr-xr-x 8 wdorner wdorner  4096 2012-04-05 21:29 ..
3 drwxr-xr-x 2 wdorner wdorner  4096 2012-04-05 21:29 test
4 -rw-r--r-- 1 wdorner wdorner 10240 2012-04-05 21:30 test.tar
```

Mit den Namen . und .. sind das aktuelle Directory und das übergeordnete Directory bezeichnet. Zur Erinnerung: In Unix ist alles Datei und somit sind auch die Verweise auf das aktuelle und übergeordnete Verzeichnis im Verzeichnisbaum Dateinamen, die man auch entsprechenden mit Befehlen adressieren kann.

Directories erkennt man an dem vorangestellten d zu Beginn der Anzeige einer Zeile. Bei regulären Dateien findet man stattdessen einen Bindestrich. Im Anschluss daran werden sowohl für Directories als auch Dateien die entsprechenden Berechtigungen in Buchstabentripeln angezeigt. Jedes Tripel hat dabei für die drei unterschiedlichen Zugriffsarten entweder den entsprechenden Buchstaben gesetzt (Zugriffsart erlaubt) oder einen Bindestrich (Zugriffsart nicht erlaubt).

Die Buchstaben bedeuten dabei:

x Die Datei ist ausführbar, also ein Programm oder ein Skript

r Die Datei darf gelesen werden

w In die Datei darf geschrieben werden

Diese Rechte existieren jeweils für drei verschiedene Nutzertypen: den Eigentümer bzw. Nutzer (user), die Gruppe (group) und alle restlichen Benutzer (others) Für diese drei unterschiedlichen Berechtigtigungsgruppen werden die Rechte in einer Reiche jeweils als Rechtetripel angezeigt:

user rwx group rwx others rwx

5.6 Änderung der Berechtigungen

Mit dem Befehl chown (change owner) kann einer Datei oder einem Verzeichnis ein anderer Besitzer zugeordnet werden. Dabei müssen dem Befehl chown mindestens zwei Parameter übergeben werden:

chown [Benutzername] [Dateiname/Verzeichnisname]

Der erste Parameter ist der neue Benutzername. Es folgen die Datei bzw. das Verzeichnis, das dem Benutzer zugeordnet werden soll. Zur Änderung des Eigentümers sind nur der bisherige Eigentümer und der Systemadministrator root berechtigt.

Mit chown lassen sich in der Standardeinstellung mit zwei Parametern die Rechte nur für ein Verzeichnis oder eine Datei ändern. Änderungen bei einem Verzeichnis wirken sich aber nicht automatisch auf die Dateien aus, die in diesem Verzeichnis liegen. Durch Optionen kann der chown-Befehl erweitert werden:

```
chown [-Optionen] [Benutzername] [Dateinamen/Verzeichnisname]
```

Änderungen können mit der -R Option auch rekursiv auf höhere Verzeichnisse und Dateien angewandt werden. Dies bedeutet, dass man damit die Rechte für das Verzeichnis und in Folge für alle darin enthaltenen Dateien und Verzeichnisse ändert.

Der zweite wichtige Befehl ist der chgrp Befehl um die Zuordnung einer Gruppe zu einer Datei zu ändern Eine Datei gehört nicht nur, wie bereits oben angeschnitten, einem Benutzer, sondern auch einer Gruppe. Durch das Gruppenkonzept kann nicht nur einer einzelnen, sondern einer definierten Gruppe von Personen Rechte an einer Datei zugewiesen werden.

Mit chgrp (change group) wird die Zuordnung einer Datei zu einer Gruppe geändert. Berechtigt ist ein Mitglied der Gruppe oder root. Der Aufbau des Befehls ist dabei identisch dem des chown-Befehls.

```
chgrp [-Optionen] [Nutzer] [Datei/Verzeichnis]
```

Eine Alternative, um Benutzer und Gruppen gleichzeitig zu ändern bietet der chown-Befehl. Diese Variante ist aber nicht auf allen Unix-Systemen einheitlich geregelt.

```
chown Benutzername:Gruppenname Datei/Verzeichnis
```

Übung

1. Wechseln Sie in das Home-Directory des aktuellen Nutzers.
2. Legen Sie mit dem Befehl mkdir ein neues Verzeichnis testrechte an.
3. Überprüfen Sie mit dem Befehl ls -la die Berechtigungen des neuen Verzeichnisses.
4. Wechseln Sie in das neue Verzeichnis.
5. Legen Sie mit dem Texteditor pico eine neue Datei text.txt an und geben Sie dort einen beliebigen kurzen Text ein.
6. Verlassen Sie den Pico und überprüfen Sie mit ls -la die Berechtigungen der neuen Datei.
7. Ändern Sie mit dem Befehl chgrp die Gruppe der Datei auf root.
8. Springen Sie ein Verzeichnis zurück und ändern Sie die Gruppe des Verzeichnisses testrechte auf root.
9. Überprüfen Sie die Änderung der Rechte mit ls -la.
10. Um diese Änderungen rückgängig zu machen, wechseln Sie bitte in das Homedirectory und wenden Sie den chown und chgrp Befehl mit der -R Option auf das testverzeichnis an und ändern Sie die Gruppe wieder auf die Gruppe mit Ihrem Nutzernamen.

11. Überprüfen Sie die Änderung der Rechte an Verzeichnis und nachgeordneter Datei mit ls -la.

5.7 Ändern von Rechten

Neben den Nutzern und den Gruppen, die die Berechtigungen für eine Datei halten sind auch die Arten von Berechtigungen essentiell. Sie lassen sich mit dem Befehl chmod ändern.

chmod [-Optionen] Nutzertyp+-=Nutzerrecht(e) Datei/Verzeichnis

Die wichtigesten Argumente sind an folgende Werte gebunden:

Nutzerrechte: rwx (r: read, w: write, x:execute)
Nutzertypen: ugoa (user, group, others, all)
Zuweisung: +-= (+: Recht wird neu zugewiesen, -: Recht wird entzogen, =: nachfolgende Rechtekonstellation wird gesetzt)

Übung

Im folgenden Beispiel werden wir einen Ordner sowie eine Datei darin anlegen und die Berechtigungen verändern.

1. Erstellen Sie im Home-Directory (cd) einen neuen Ordner testordner (mkdir testordner).
2. Sehen Sie die Berechtigungen dieses Ordners ein (ls -la)
3. Wechseln Sie in den neuen Ordner (cd testordner) und erstellen Sie mit dem Pico eine Datei testtext.txt
4. Sehen Sie die Berechtigungen ein (ls -la). Für die Datei sollte die Standardberechtigung gesetzt sein (rw-r–r–)
5. Ändern Sie die Berechtigung, so dass auch Mitglieder der Gruppe Schreibrechte auf der Datei besitzen:
6. Sehen Sie wieder die Rechte ein und die Einstellung sollte sich auf rw-rw-r– geändert haben.
7. Ändern Sie die Gruppe nun auf cdrom (nur als Beispiel):
8. Sehen sie die Rechte erneut ein (ls -la).
9. Rechte können auch rekursiv geändert werden, so dass sich die Änderungen auf Unterordner und deren Dateien auswirken.
10. Wechseln Sie zurück in das Home-Directory (cd ..).

11. Ändern Sie nun die Nutzerrechte dahingehend, dass others alle Rechte sowohl am Ordner testordner als auch der (aller) beinhaltenden Datei verlieren:

12. Überprüfen Sie die Wirkung auf den Ordner testordner als auch für die darin enthaltene Datei.

13. Wechseln Sie zurück in das Home-Directory (cd).

14. Die gegenteilige Operation ist etwas komplizierter, da ein chmod -R o+rx test bedeuten würde, dass auch die Datei testtext.txt ausführbar würde. An dieser Stelle hilft ein großes X, da dies bewirkt, dass die execute Option nur auf Verzeichnisse angewandt wird:

15. Versuchen Sie zum Ende der Übung die Rechte auf eine andere Art und Weise zu steuern und geben Sie ein:

16. Überprüfen Sie wie die Rechte verändert wurden (ls -la).

17. Recherchieren Sie (manpages, help-Option, Internet), was es mit diesem Zahlencode auf sich hat und wie dieser als System aufgebaut ist. Versuchen Sie durch 777 erzeugte Änderung wieder durch einen anderen Zahlencode rückgängig zu machen und die Rechte für den Ordner testordner auf rwxr-xr– zurückzusetzen.

5.8 Nummerische Codierung der Rechte

Es gibt auch eine nummerische Codierung für die Rechte. Hierbei gilt folgender Aufbau:

4 Lesen
2 Schreiben
1 Ausführen

Die Rechtekombination, die letztendlich zugewiesen wird ist die Summe dieser drei Werte. Die Werte liegen dabei zwischen 0 und 7. Darf also ein Nutzer lesen, schreiben und ausführen, ergibt sich der Wert 7, lesen und schreiben alleine wäre 6. Um den drei Berechtigungstypen (ugo) damit die rechte zuweisen zu können wird also eine Zahl mit drei Stellen übergeben.

Hierzu einige Beispiele:

777 entspricht den Berechtigungen rwxrwxrwx
666 dagegen wäre rw-rw-rw-
444 stünde für r--r--r--

Es können auch individuelle Rechte vergeben werden:
764 -> rwxrw-r--

Rechte können damit einfach per chmod geändert werden:

```
1 chmod 700 testdatei.txt
```

Damit würde der Datei testtext.txt nur Zugriff nur durch den Eigentümer (user) gewährt. Gruppenmitglieder und alle anderen wären damit vollständig ausgeschlossen.

Übungsaufgabe: Einführung Unix/Linux – Berechtigungen

1. Ändern von Nutzerrechten

   Im folgenden Beispiel werden wir einen Ordner sowie eine Datei darin anlegen und die Berechtigungen verändern.

   (a) Erstellen Sie im Home-Directory (cd) einen neuen Ordner testordner (mkdir testordner).

   (b) Sehen Sie die Berechtigungen dieses Ordners ein (ls -la)

   (c) Wechseln Sie in den neuen Ordner (cd testordner) und erstellen Sie mit dem Pico eine Datei testtext.txt

   (d) Sehen Sie die Berechtigungen ein (ls -la). Für die Datei sollte die Standardberechtigung gesetzt sein (rw-r–r–)

   (e) Ändern Sie die Berechtigung, so dass auch Mitglieder der Gruppe Schreibrechte auf der Datei besitzen:

   $ chmod g+w testtext.txt

   (f) Sehen Sie wieder die Rechte ein und die Einstellung sollte sich auf rw-rw-r– geändert haben.

   (g) Ändern Sie die Gruppe nun auf cdrom (nur als Beispiel):

   $ chgrp cdrom testtext.txt

   (h) Sehen sie die Rechte erneut ein (ls -la).

2. Rekursive Änderung der Rechte

   (a) Rechte können auch rekursiv geändert werden, so dass sich die Änderungen auf Unterordner und deren Dateien auswirken.

   (b) Wechseln Sie zurück in das Home-Directory (cd ..).

   (c) Ändern Sie nun die Nutzerrechte dahingehend, dass others alle Rechte sowohl am Ordner testordner als auch der (aller) beinhaltenden Datei verlieren:

   $ chmod – R o-rwx testordner

   (d) Überprüfen Sie die Wirkung auf den Ordner testordner als auch für die darin enthaltene Datei.

   (e) Wechseln Sie zurück in das Home-Directory (cd).

(f) Die gegenteilige Operation ist etwas komplizierter, da ein chmod -R o+rx test bedeuten würde, dass auch die Datei testtext.txt ausführbar würde. An dieser Stelle hilft ein großes X, da dies bewirkt, dass die execute Option nur auf Verzeichnisse angewandt wird:

$ chmod -R o+rX testordner

3. Nummerische Codierung der Rechte

(a) Versuchen Sie zum Ende der Übung die Rechte auf eine andere Art und Weise zu steuern und geben Sie ein:

$ chmod 777 testordner

(b) Überprüfen Sie wie die Rechte verändert wurden (ls -la).

(c) Recherchieren Sie (manpages, help-Option, Internet), was es mit diesem Zahlencode auf sich hat und wie dieser als System aufgebaut ist. Versuchen Sie durch 777 erzeugte Änderung wieder durch einen anderen Zahlencode rückgängig zu machen und die Rechte für den Ordner testordner auf rwxr-xr– zurückzusetzen.