Vortrag Freiburger Linux Gruppe

Linux inside: Benutzer und ihre Rechte
Dateiberechtigungen

Inhalt

- Anzeige der Rechte von Dateien: ls
- Änderung der Rechte: chmod
- Besitzer der Datei ändern: chown
- Gruppe der Datei ändern: chgrp
- Weitere Dateibefehle
- Dateimaske / Rechtevererbung?
- Spezielle Rechte
- Arbeiten als Root

Anzeige der Rechte von Dateien: ls

- ls -l: Dateirechte, Besitzer, Gruppe, Größe, Datum, Uhrzeit der Änderung

```
insgesamt 4
-rw-r--r--. 1 zie szi 0  3. Nov 00:04 test
-rwxr-----. 1 szi szi 2  7. Nov 10:06 testszi
```

r: Lesen
w: Schreiben
x: Ausführen / Ins Verzeichnis wechseln

Drei Gruppen von Rechten:
Rechte für den Besitzer,
Rechte für die Gruppe,
Rechte für alle anderen

Anzeige der Rechte von Dateien: ls

- Das erste Zeichen der Rechte-Spalte zeigt den Dateityp:
  - - : normale Datei
  - b: block-orientiertes Gerät
  - c: zeichen-orientiertes Gerät (char device)
  - d: Verzeichnis / Directory
  - l: symbolische Verknüpfung / link
  - p: benannte Pipe
- Der Punkt am Ende zeigt an, dass es alternative Zugriffsmethoden wie Access Control Lists / SELinux gibt.

Für wen gelten welche Rechte?

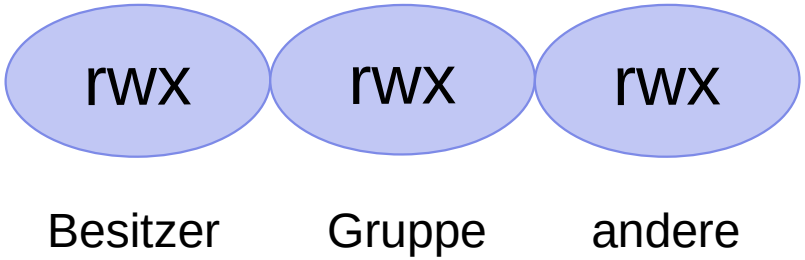
- Wenn der Besitzer auf die Datei zugreift, gelten (nur) die Rechte des Besitzers. Ein Besitzer kann also auch weniger Rechte haben als andere aus der gleichen Gruppe.
- Wenn ein Nutzer der gleichen Gruppe, aber nicht der Besitzer zugreift, gelten (nur) die Rechte der Gruppe.
- Wenn ein Nutzer einer anderen Gruppe zugreift, gelten die Rechte für alle anderen.
- Root darf alles, egal welche Rechte die Datei laut „ls -l“ hat.
- Ausführen von Programmen/Skripten geht nur, wenn neben x auch r gesetzt ist (also Lesen und Ausführen).

Änderung der Rechte: chmod

- Rechte werden für die drei folgenden Gruppen geändert:
  - u=User/Besitzer, g=Gruppe, o=other/alle anderen
- u+w: Schreibrechte für den Besitzer ergänzen
- g-w: Schreibrechte für die Gruppe entfernen
- o-r: Leserechte für alle anderen entfernen
- a-r: Leserechte für alle (Besitzer, Gruppe und andere) entfernen
- Aufruf: chmod u+w Dateiname

Rechte als Zahlen

- chmod 660 ergibt rw-rw----
- 4 = r (lesen)
- 2 = w (schreiben)
- 1 = x (ausführen)



Besitzer der Datei ändern: chown

- chown Nutzername Dateiname

Aus Sicherheitsgründen kann nur root auf einen anderen Besitzer ändern.
Bei einem normalen Nutzer muss die User-Id vorher und nachher gleich sein.
Sonst kann man ohne Spuren jemand anderem eine gefährliche Datei unterschieben.

https://qastack.com.de/superuser/697608/chown-operation-not-permitted
https://unix.stackexchange.com/questions/27350/why-cant-a-normal-user-chown-a-file/27374#27374

Gruppe der Datei ändern: chgrp

- chgrp Gruppenname Dateiname
- Es sind nur Gruppennamen zulässig, in denen der Besitzer drin ist.
- Die Änderung ist nur bei eigenen Dateien erlaubt.
- groups: Gruppennamen anzeigen, zu denen der aktuelle User gehört
- id: Ids zum Nutzer anzeigen

Weitere Dateibefehle

- mkdir: Verzeichnis anlegen
- cd: ins Verzeichnis wechseln (change directory)
- touch: Datei anlegen

Dateimaske / Rechtevererbung?

- Mit welchen Rechten wird eine Datei angelegt?
- Rechte,Nutzer und Gruppe einer neuen Datei werden nicht vom Verzeichnis "geerbt", in dem man arbeitet, sondern vom Nutzer, der die Datei anlegt und dessen umask.
- Bei "cp -p" werden so viel wie möglich Rechte behalten.
- umask -S/umask -p: Anzeigen der Rechte symbolisch/numerisch
- umask -p 0022 ist "u=rwx,g=rx,o=rx" → eine Datei bekommt dann rw-r--r--
- Also das Gegenteil von chmod: 7 heißt keine Rechte, 2 heißt kein Schreibrecht, 0 heißt alle Rechte.

Spezielle Rechte

- t: Sticky Bit
  - Das Sticky-Bit wird für gemeinsam genutzte Verzeichnisse verwendet.
  - Nur der Eigentümer einer Datei kann dort Dateien löschen oder umbenennen.
  - Beispiel: /tmp
  - https://de.wikipedia.org/wiki/Sticky_Bit

Spezielle Rechte

- s: Set Group ID
  - Ausführbare Programme mit setgid werden neben den Rechten des ausführenden Nutzers auch mit den Rechten der Gruppe ausgeführt, der die Datei gehört.
  - Bei Verzeichnissen mit setgid wird die Gruppe in den Unterverzeichnissen vererbt.
  - Für gemeinsam genutzte Verzeichnisse und Programme
  - Falls Programme unsicher programmiert sind, kann ein Sicherheitsrisiko bestehen.
  - https://de.wikipedia.org/wiki/Setgid

Spezielle Rechte

- s: set User id
  - Ausführbare Programme mit setuid werden zusätzlich zu den Rechten desjenigen Benutzers, der die Datei ausführt, auch mit den Rechten des Benutzers ausgeführt, dem die Datei gehört.
  - Beispiel su, sudo
  - Je nach Nutzung kann ein Sicherheitsrisiko bestehen, wenn Nutzer ohne spezielle Rechte so zu Rootrechten kommen können
  - https://de.wikipedia.org/wiki/Setuid

Alternative Rechte-Verwaltung

- SELinux
- und AppArmor
- sind Mandatory Access Control (MAC), zu Deutsch etwa: zwingend erforderliche Zugangskontrolle, beschreibt eine systembestimmte, auf Regeln basierende Zugriffskontrollstrategie
- Für jede Datei können spezielle Regeln vorgegeben werden, was mit dieser Datei erlaubt ist oder was das Programm tun darf.
- Sehr komplex – es bräuchte einen eigenen Vortrag dafür
- Beispiel: ls -Z

Arbeiten als Root

- su: Wechseln zu root (set user)
- su Nutzername: Wechsel zu anderem Nutzer (root, falls keiner angegeben)
- sudo: Kommando als anderer Nutzer ausführen
- sudo -i: Login als root
- sudo usermod -aG GRUPPENNAME BENUTZERNAME:

  Bestehenden Benutzer einer Gruppe zuordnen
- Datenschutz: root kann alle Dateien lesen, sollte das bei Dateien eines anderen Nutzers aber nicht tun.

Abschluss

- Vielen Dank für die Aufmerksamkeit

Verein deutscher Ingenieure Bezirk Schwarzwald www.vdi-schwarzwald.de

Linux User Group Freiburg www.lug-freiburg.de

Links

- https://xkcde.dapete.net/149/
- https://qastack.com.de/superuser/697608/chown-operation-not-permitted
- https://unix.stackexchange.com/questions/27350/why-cant-a-normal-user-chown-a-file/27374#27374

Quellenangaben

- https://www.gnu.org/software/coreutils/manual/coreutils.html
- https://de.wikipedia.org/wiki/Ls_(Unix)
- https://de.wikipedia.org/wiki/Chmod
- https://developer.ibm.com/tutorials/l-lpic1-103-3/
- https://developer.ibm.com/tutorials/l-lpic1-104-5/
- https://de.wikipedia.org/wiki/Sticky_Bit
- https://de.wikipedia.org/wiki/Setgid
- https://de.wikipedia.org/wiki/Setuid