

Praktikum 4 : Zugriffsrechte von Dateien und Verzeichnissen

1 Vorbemerkung

1.1 Zugriffs- und Ausführungsberechtigungen

Mit dem Befehl „ls -l“ werden u.a. auch die aktuellen Berechtigungen ausgegeben.

```
user@debian:~$ ls -l [-n] [<name>]
```

```
-rwxrwxrwx count user group size date name
\_/ \_/ \_/      \_/ \_/              \_/
 u   g   o        |   |              +-- Datei-/Verzeichnisname
 |   |   |        |   |
 |   |   |        |   +----- Gruppe (Name oder GID)
 |   |   |        +----- Besitzer (Name oder UID)
 |   |   +----- (o) other - Rechte anderer Benutzer
 |   +----- (g) group - Rechte der Gruppe
 +----- (u) user - Rechte des Besitzers
```

Unter Linux werden folgende Berechtigungsgruppen für Dateien bzw. Verzeichnisse unterschieden.

Symbol	Berechtigungsgruppen
u	Besitzer (u ser) der Datei bzw. des Verzeichnisses
g	zugeordnete Gruppe (g roup) der Datei bzw. des Verzeichnisses
o	andere Nutzer (o ther) , die auf die Datei zugreifen möchten

Dabei können folgende Zugriffsrechte für jede Berechtigungsgruppe entweder gemeinsam durch die Summe der jeweiligen Oktalzahlen pro Berechtigungsgruppe (z.B. 755) oder durch ein separates Hinzufügen bzw. Entfernen spezifischer Rechte (z.B. u+r, o-w) eingestellt werden.

Symbol	Oktal	Bedeutung für Dateien	Bedeutung für Verzeichnisse
r	4	Lesen (read)	Auflisten des Inhalts
w	2	Schreiben/Löschen (write)	Erzeugen/Löschen von Dateien / Unterverzeichnisse
x	1	Ausführen (execute)	Zugriff auf Verzeichnis / Wechsel in Verzeichnis

Besitzer (u => user)			Gruppe (g => group)			Andere (o => other)		
1	1		1			1		1
r	w	x	r	w	x	r	w	x
2 ²	2 ¹	2 ⁰	2 ²	2 ¹	2 ⁰	2 ²	2 ¹	2 ⁰
4	2	1	4	2	1	4	2	1
6			2			5		

Erweiterte Ausführungs- und Zugriffsrechte werden durch die zusätzlich vorangestellte Summe der jeweiligen Oktalzahlen (z.B. 4755) oder durch das Hinzufügen bzw. Entfernen spezifischer Rechte (z.B. u+s) eingestellt und erscheinen an der Stelle vom Ausführungs-Bit (x).

Symbol	Oktal	Erweiterte Ausführungs- und Zugriffsrechte
s	4	SetUID-Bit für den Nutzer, Ausführen der Datei mit den Rechten des Besitzers
s	2	SetGID-Bit für die Gruppe, Ausführen der Datei mit den Rechten der Gruppe
t	1	sTicky-Bit, bei schreibbaren Verzeichnissen nur Löschen durch Besitzer der Datei

2 Übungsaufgaben

2.1 Vorbereitung

Führen Sie die folgenden Kommandos in einer separaten Konsole als Benutzer **"root"** aus, um die Veränderungen in der Verzeichnisstruktur während der Praktikumsdurchführung zu beobachten. Diese Konsolen sollen bei allen Aufgaben zu diesem Arbeitsblatt geöffnet sein.

Tipp: Zur Vereinfachung kann die Ausführung auch mit dem Skript **"pr04-watch.sh"** erfolgen.

pr04-watch.sh	Aufgabe des Kommandos
<code>watch -d "tree /home"</code>	
<code>watch -d "ls -lR /home"</code>	
<code>rm -i -r /home/user/[!S]*</code>	Löschen nicht benötigter Verzeichnisse (Erklärung später)

2.1.1 Datei- und Verzeichnisstruktur für Praktikum per Skript erstellen und löschen

Ermitteln Sie die Befehle, um vom Benutzer **"root"** folgende Aufgaben erfüllen zu können.

Kommando	Aufgabe des Kommandos
	Verzeichnisstruktur "/home/v1/v2" erstellen
	Programm "/bin/grep" nach "/home/v1/mygrep" kopieren
	Datei "/etc/passwd" nach "/home/v1/v2/d1" kopieren
	Verzeichnisstruktur "/home/v1" rekursiv löschen

Schreiben Sie die ersten drei Befehle mit **"nano /home/pr04-setup.sh"** bzw. den letzten Befehl mit **"nano /home/pr04-reset.sh"** zeilenweise in die entsprechende Dateien (Ende: STRG-x).

Die Ausführung als Skript kann vom Benutzer **"root"** durch **"sh /home/<skriptname>"** oder ggf. auch vom Benutzer **"user"** durch **"sudo sh /home/<skriptname>"** erfolgen.

Testen Sie das Erstellen der benötigten Datei- und Verzeichnisstruktur bzw. ihrem Entfernen über dem Aufruf der von Ihnen erstellten Skripts.

2.1.2 Automatisierte Wiederherstellung der benötigten Datei- und Verzeichnisstruktur

In dieser Aufgabe soll ein Skript in der Form erstellt werden, dass die benötigte Datei- und Verzeichnisstruktur einfach immer wieder komplett neu erstellt werden kann.

Schreiben Sie dazu die Skriptaufrufe vom Benutzer **"root"** in der vorherigen Aufgabe zeilenweise so in eine Datei, damit dies vom Benutzer **"root"** durch **"sh /home/pr04-rebuild.sh"** oder ggf. auch vom Benutzer **"user"** durch den Aufruf **"sudo sh /home/pr04-rebuild.sh"** realisiert wird.

Testen Sie das automatisierte Wiederherstellen der benötigten Datei- und Verzeichnisstruktur, indem Sie z.B. ein neues Verzeichnis in der Verzeichnisstruktur erstellen bzw. eine Datei hinein kopieren und danach wieder über das neu erstellte Skript in den Ausgangszustand zurücksetzen.

2.2 Befehle zur Kontrolle der Zugriffsrechte

Für dieses Praktikum werden folgende Kommandos zur Kontrolle der Zugriffsrechte verwendet. Führen Sie diese Befehle als Benutzer „*user*“ in einer neuen Konsole im Verzeichnis „*/home*“ aus.

Tipp: Nutzen Sie ggf. die Pfeil-Tasten oder alternativ das vorbereitete Skript, um die Befehle nicht immer wieder manuell eingeben zu müssen.

pr04-2.2.sh	Aufgabe des Kommandos
<code>ls -l v1/v2</code>	Lesetest für Verzeichnis " v2 "
<code>v1/mygrep user v1/v2/d1</code>	Ausführungs- und Lesetest für Dateien " mygrep " und " d1 "
<code>cp /etc/passwd v1/v2/d1</code>	Schreibtest für Datei " d1 " und Verzeichnis " v2 "

2.3 Zugriffsrechte von Dateien und Verzeichnissen

Stellen Sie vor jeder Aufgabe mit dem Skript "*pr04-rebuild.sh*" den Ausgangszustand wieder her.

Führen Sie anschließend folgende Aufgaben als Benutzer „*root*“ im Verzeichnis „*/home*“ aus, um neue Zugriffs- bzw. Ausführungsrechte für Dateien, Kommandos und Verzeichnisse zu vergeben. Ermitteln Sie die Aufgaben dieser Kommandos, achten Sie dabei in den „*watch*“-Fenstern auf die Änderungen an den betroffenen Dateien bzw. Verzeichnissen.

Testen Sie danach **exemplarisch (!)** die Auswirkung der neuen Rechte auf die in Aufgabe 2.2 vom Benutzer „*user*“ genutzten Kommandos, testen Sie ggf. die Rechte mit eigenen Einstellungen.

Tipp: Nutzen Sie ggf. die Pfeil-Tasten bzw. die vorbereiteten Skripts, um die Befehle nicht immer wieder manuell eingeben zu müssen.

2.3.1 Lese- und Schreibrechte sowie Besitzverhältnisse von Dateien

pr04-2.3.1.sh	Aufgabe/Ergebnis des Kommandos
<code>chmod 0 v1/v2/d1</code>	
<code>chmod o+r v1/v2/d1</code>	
<code>chmod g+r,o-r v1/v2/d1</code>	
<code>chgrp user v1/v2/d1</code>	
<code>chown user v1/v2/d1</code>	
<code>chmod 604 v1/v2/d1</code>	
<code>chown root:root v1/v2/d1</code>	

2.3.2 Ausführungsrechte von Dateien

pr04-2.3.2.sh	Aufgabe/Ergebnis des Kommandos
<code>chmod 740 v1/mygrep</code>	
<code>chmod +x v1/mygrep</code>	

2.3.3 Zugriffsrechte von Verzeichnissen

pr04-2.3.3.sh	Aufgabe/Ergebnis des Kommandos
<code>chmod -R 777 v1/v2</code>	
<code>chmod go-rwx v1/v2</code>	

Name:

Studiengang:

Gruppe:

3 Praxisaufgabe

Füllen Sie diesen Aufgabenzettel in **elektronischer** (!) Form aus und geben Sie ihn ausgedruckt beim nächsten Praktikum ab. Handschriftliche Ausarbeitungen werden nicht akzeptiert.

3.1 Zugriffsrechte mit entsprechender Systemkonfiguration

Auf Ihrem Rechner gibt es 5 Benutzer („*user01*“ bis „*user05*“) sowie im Verzeichnis „/home“ die Verzeichnisse „**public**“ und „**privat**“, worin jeweils eine Kopie „**d1**“ von „**/etc/passwd**“ liegt. Erzeugen Sie sich ggf. diese Struktur auf Ihrem Rechner (nicht Bestandteil der folgenden Aufgabe).

Vergeben Sie unter der gegebenen Struktur folgende Rechte:

Zugriffsrechte
Der Benutzer „ <i>user01</i> “ ist Eigentümer der beiden Verzeichnisse und hat vollen Zugriff.
Die Benutzer „ <i>user02</i> “, „ <i>user03</i> “ und „ <i>user04</i> “ haben ebenfalls vollen Zugriff auf das Verzeichnis „ public “, andere Benutzer dürfen die Inhalte von diesem Verzeichnis nur lesen.
Die Benutzer „ <i>user02</i> “ und „ <i>user03</i> “ dürfen die Inhalte vom Verzeichnis „ privat “ lesen, andere Benutzer sollen keinen Zugriff darauf haben.

Überlegen Sie, welche Vorgehensweise dafür notwendig ist. Beachten Sie, dass für diese Aufgabe ggf. auch Befehle der vorherigen Praktika notwendig sind. Erklären Sie stichpunktartig die Aufgabe der von Ihnen gewählten Befehle.

Kommando	Aufgabe des Kommandos

Überprüfen Sie Ihre erstellte Konfiguration für alle 5 Benutzer (!) wie folgt:

Lesetest: `"ls /home/<verzeichnis>"` und `"grep root /home/<verzeichnis>/passwd"`

Schreibtest: `"mkdir /home/<verzeichnis>/<user>"`

Nutzen Sie als **"root"** zur Vereinfachung dieser Tests die Form `"sudo -u <user> <kommando>"`.