

HOWTO zu den UNIX-Zugriffsrechten

(C) 2006 T.Birnthaler/H.Gottschalk <howtos(at)ostc.de>

OSTC GmbH, <http://www.ostc.de>

\$Id: unix-rights-HOWTO.txt,v 1.3 2008-12-18 18:47:27 tsbirn Exp \$

Dieses Dokument beschreibt die Zugriffsrechte von UNIX-Systemen.

Standard-Datei-Zugriffsrechte:

r	read	Datei-Inhalt lesbar (cat, more, less)
w	write	Datei-Inhalt veränderbar (echo "TEXT" > DATEI)
x	execute	Datei als Programm ausführbar (CMD)
s	setuserid	Pgm ausführen unter Benutzerkennung des Besitzers
s	setgroupid	Pgm ausführen unter Gruppenkennung der Besitzer-Gruppe
t	sticky	Pgm nach Start im Speicher/Swap halten (VERALTET!)

Standard-Verzeichnis-Zugriffsrechte:

r	read	Verzeichnis lesbar (ls)
w	write	Verzeichnis änderbar (Dateien anlegen/löschen/umbenennen verschieben: rm, mv, cp, ln, mkdir, rmdir)
x	execute	Wechsel in Verzeichnis erlaubt (cd)
s	setuserid	---
s	setgroupid	Neue Dateien/Verz. automatisch Besitzer-Gruppe des Verz. zuordnen, neue Verz. haben auch setgroupid gesetzt
t	sticky	Nur Datei/Verz.-Besitzer (oder root) darf Dateien löschen

Dateirechte in oktaler + symbolischer Form:

Oktal	Symbolisch	WER	ERHAELT	WAS
0	---	u = User		r = Read
1	--x	g = Group	+ = Hinzufügen	w = Write
2	-w-	o = Other	- = Wegnehmen	x = eXecute
3	-wx	a = All	= = Setzen	s = SetUID/GID-Recht
4	r--	= ugo		t = Sticky-Recht
5	r-x			
6	rw-	Read = 4, Write = 2, Execute = 1		
7	rwx	User = 700, Group = 070, Other = 007		
		u+s = 4000 = SetUID (ausführbare Dateien)		
		g+s = 2000 = SetGID (ausführbare Dateien + Verz.)		
		u+t = 1000 = Sticky (Verzeichnisse)		

Beispiele von Rechtekombinationen für "chmod":

Oktal	Symbolisch	chmod	FILE/DIR...
		chmod 644	FILE...
		chmod 660	FILE...
700	u+rwx,go-rwx	chmod 600	FILE...
070	g+rwx,uo-rwx	chmod 755	DIR...
007	o+rwx,ug-rwx	chmod 770	DIR...
777	a+rwx	chmod 700	DIR...
1000	u+s	chmod ug+rwx,a-rwx	FILE/DIR...
2000	g+s	chmod a+x	FILE/DIR...
4000	o+t	chmod go-w	FILE/DIR...