

HOWTO zu den UNIX-Zugriffsrechten

(C) 2006-2014 T.Birnthaler/H.Gottschalk <howtos(at)ostc.de>
OSTC Open Source Training and Consulting GmbH
<http://www.ostc.de>

\$Id: unix-rights-HOWTO.txt,v 1.7 2014/11/03 16:16:18 tsbirn Exp \$

Dieses Dokument beschreibt die Standard Zugriffsrechte von UNIX-Systemen.

Standard DATEI-Zugriffsrechte:

r	Read	Datei-Inhalt lesbar (cat, more, less, lpr)
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	Verz. lesbar (ls)
w	Write	Verz. änderbar (Dateien anlegen/löschen/umbenennen verschieben: rm, mv, cp, ln, mkdir, rmdir)
x	eXecute	Wechsel in Verz. 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:

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

Beispiele von Rechte-Kombinationen für "chmod":

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