

Riferimento Rapido chmod

Permessi file, modalità numerica e simbolica, bit speciali, umask

Modalità Numerica

Cifre Ottali dei Permessi

4	Lettura (r)
2	Scrittura (w)
1	Esecuzione (x)
0	Nessun permesso

Formato a Tre Cifre

```
chmod 755 file # rwxr-xr-x
chmod 644 file # rw-r--r--
chmod 700 file # rwx-----
chmod 600 file # rw-----
```

Calcolo delle Cifre

7 (4+2+1)	rwx — lettura, scrittura, esecuzione
6 (4+2)	rw- — lettura, scrittura
5 (4+1)	r-x — lettura, esecuzione
4	r-- — solo lettura
3 (2+1)	-wx — scrittura, esecuzione
2	-w- — solo scrittura
1	--x — solo esecuzione
0	--- — nessun permesso

Modalità Simbolica

Sintassi: [u_goa][+|=][rwxXst]

u	Utente (proprietario)
g	Gruppo
o	Altri
a	Tutti (u + g + o)
+	Aggiunge permesso
-	Rimuove permesso
=	Imposta permesso esatto

Esempi Simbolici

```
chmod u+x file # proprietario: aggiungi esecuzione
chmod g-w file # gruppo: rimuovi scrittura
chmod o=r file # altri: imposta solo lettura
chmod a+r file # tutti: aggiungi lettura
chmod u+x,g-w,o= file # operazioni combinate
```

Permessi Comuni

Preset Permessi File

644	rw-r--r--	File predefinito — proprietario rw, altri lettura
755	rwxr-xr-x	Script/binario — proprietario rwx, altri rx
600	rw-----	File privato — solo proprietario
400	r-----	Solo lettura privata (chiavi SSH)
666	rw-rw-rw-	File scrivibile da tutti (evitare)
777	rwxrwxrwx	Accesso completo per tutti (evitare)

Riferimento Rapido

```
chmod 644 *.html # file web: proprietario rw, tutti r
chmod 755 *.sh # script: proprietario rwx, tutti rx
chmod 600 ~/.ssh/id_* # chiavi SSH: solo proprietario
chmod 400 secret.pem # certificato: sola lettura
```

Permessi Directory

Significato dei Permessi per le Directory

r (4)	Elenca contenuto directory (ls)
w (2)	Crea/elimina file nella directory
x (1)	Accede (cd) alla directory
rx (5)	Lista + accesso (tipico per lettura)
rwx (7)	Controllo completo

refmint.com

Permessi Directory Comuni

```
chmod 755 dir/ # standard: proprietario rwx, altri rx
chmod 700 dir/ # privata: solo proprietario
chmod 750 dir/ # accesso gruppo: proprietario rwx, gruppo rx
chmod 1777 /tmp # sticky bit: solo il proprietario può eliminare
```

Bit Speciali

Setuid, Setgid, Sticky

Setuid (4xxx)	Esegue come proprietario del file (es. passwd)
Setgid (2xxx)	Esegue come gruppo del file / eredita gruppo dir
Sticky (1xxx)	Solo il proprietario può eliminare file (es. /tmp)

Impostare i Bit Speciali

```
chmod 4755 program # setuid: -rwsr-xr-x
chmod 2755 dir/ # setgid: drwxr-sr-x
chmod 1755 dir/ # sticky: drwxr-xr-t
chmod u+s program # setuid simbolico
chmod g+s dir/ # setgid simbolico
chmod +t dir/ # sticky bit simbolico
```

Ricorsivo

Modifiche Ricorsive ai Permessi

```
chmod -R 755 dir/ # imposta tutto a 755 ricorsivamente
chmod -R u+rwx dir/ # proprietario rw, +x solo su dir
chmod -R g-w dir/ # rimuovi scrittura gruppo/altri
```

File vs Directory con find

```
# imposta directory a 755, file a 644
find /path -type d -exec chmod 755 {} +
find /path -type f -exec chmod 644 {} +
```

X maiuscola — Esecuzione Condizionale

x (minuscola)	Aggiunge esecuzione a tutti i file e directory
X (maiuscola)	Aggiunge esecuzione solo a directory e file già eseguibili

umask

Come Funziona umask

umask	Mostra umask corrente
umask 022	File: 644, Directory: 755
umask 077	File: 600, Directory: 700
umask 002	File: 664, Directory: 775

Calcolo umask

```
# permesso predefinito meno umask = permesso effettivo
# File: 666 - 022 = 644 (rw-r--r--)
# Dir: 777 - 022 = 755 (rwxr-xr-x)
umask # mostra umask corrente
umask 022 # valore predefinito tipico
umask -S # mostra in notazione simbolica
```

Pattern Comuni

Casi d'Uso Quotidiani

Web root	chmod -R 755 /var/www/html
File config	chmod 600 app.conf
Directory SSH	chmod 700 ~/.ssh
SSH authorized_keys	chmod 600 ~/.ssh/authorized_keys
Directory condivisa	chmod 2775 /shared (setgid)
File log	chmod 640 /var/log/app.log
Script cron	chmod 755 /etc/cron.daily/myjob
Directory temporanea	chmod 1777 /tmp (sticky)

Visualizzare i Permessi

```
ls -l file.txt # mostra permessi
ls -ld dir/ # mostra permessi directory
stat -c '%A %a %n' * # simbolico + numerico + nome
getfacl file.txt # mostra ACL (se in uso)
```