

# Referensi Cepat chmod

Izin file, mode numerik & simbolik, bit khusus, umask

## Mode Numerik

### Digit Oktal Izin

<b>4</b>	Baca (r)
<b>2</b>	Tulis (w)
<b>1</b>	Eksekusi (x)
<b>0</b>	Tanpa izin

### Format Tiga Digit

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

### Perhitungan Digit

<b>7 (4+2+1)</b>	rwx — baca, tulis, eksekusi
<b>6 (4+2)</b>	rw — baca, tulis
<b>5 (4+1)</b>	r-x — baca, eksekusi
<b>4</b>	r- — baca saja
<b>3 (2+1)</b>	-wx — tulis, eksekusi
<b>2</b>	-w- — tulis saja
<b>1</b>	--x — eksekusi saja
<b>0</b>	--- — tanpa izin

## Mode Simbolik

### Sintaks: [ugoa][+=[rwxXst]

<b>u</b>	User (pemilik)
<b>g</b>	Group
<b>o</b>	Others (lainnya)
<b>a</b>	Semua (u+g+o)
<b>+</b>	Tambah izin
<b>-</b>	Hapus izin
<b>=</b>	Set izin tepat

### Contoh Simbolik

```
chmod u+x file # owner: add execute
chmod g-w file # group: remove write
chmod o=r file # others: set read only
chmod a+r file # all: add read
chmod u+x,g-w,o= file # combined operations
```

## Izin Umum

### Preset Izin File

<b>644</b>	<b>rwx-r-xr-x</b>	File default — pemilik rw, lainnya baca
<b>755</b>	<b>rwxr-xr-x</b>	Script/binary — pemilik rwx, lainnya rx
<b>600</b>	<b>rwx-----</b>	File privat — pemilik saja
<b>400</b>	<b>r-----</b>	Baca saja privat (SSH key)
<b>666</b>	<b>rwx-rwx-rwx</b>	File world-writable (hindari)
<b>777</b>	<b>rwxrwxrwx</b>	Akses penuh semua pihak (hindari)

## Referensi Cepat

```
chmod 644 *.html # web files: owner rw, world r
chmod 755 *.sh # scripts: owner rwx, world rx
chmod 600 ~/.ssh/id_* # SSH keys: owner only
chmod 400 secret.pem # certificate: read-only
```

## Izin Direktori

### Arti Izin untuk Direktori

<b>r (4)</b>	Tampilkan isi direktori ( <b>ls</b> )
<b>w (2)</b>	Buat/hapus file di direktori
<b>x (1)</b>	Masuk ke direktori ( <b>cd</b> )
<b>rx (5)</b>	Tampilkan + akses (khas untuk baca)
<b>rwx (7)</b>	Kontrol penuh

refmint.com

## Izin Direktori Umum

```
chmod 755 dir/ # standard: owner rwx, others rx
chmod 700 dir/ # private: owner only
chmod 750 dir/ # group access: owner rwx, group rx
chmod 1777 /tmp # sticky bit: only owner can delete
```

## Bit Khusus

### Setuid, Setgid, Sticky

**Setuid (4xxx)** Jalankan sebagai pemilik file (mis. **passwd**)  
**Setgid (2xxx)** Jalankan sebagai group file / warisi group direktori  
**Sticky (1xxx)** Hanya pemilik yang bisa hapus file (mis. **/tmp**)

### Mengatur Bit Khusus

```
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 # symbolic setuid
chmod g+s dir/ # symbolic setgid
chmod +t dir/ # symbolic sticky bit
```

## Rekursif

### Perubahan Izin Rekursif

```
chmod -R 755 dir/ # set all to 755 recursively
chmod -R u+rwx dir/ # owner rw, +x on dirs only
chmod -R go-w dir/ # remove group/other write
```

### File vs Direktori dengan find

```
# set directories to 755, files to 644
find /path -type d -exec chmod 755 {} +
find /path -type f -exec chmod 644 {} +
```

### X Besar — Eksekusi Kondisional

**x (huruf kecil)** Tambah execute ke semua file dan direktori  
**X (huruf besar)** Tambah execute hanya ke direktori dan file yang sudah executable

## umask

### Cara Kerja umask

**umask** Tampilkan umask saat ini  
**umask 022** File: 644, Direktori: 755  
**umask 077** File: 600, Direktori: 700  
**umask 002** File: 664, Direktori: 775

### Perhitungan umask

```
# default permission minus umask = effective
# Files: 666 - 022 = 644 (rw-r--r--)
# Dirs: 777 - 022 = 755 (rwxr-xr-x)
umask # display current umask
umask 022 # typical default
umask -S # show in symbolic notation
```

## Pola Umum

### Kasus Penggunaan Sehari-hari

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

## Melihat Izin

```
ls -l file.txt # show permissions
ls -ld dir/ # show directory permissions
stat -c '%A %a %n' * # symbolic + numeric + name
getfacl file.txt # show ACLs (if in use)
```