Źródło: *http://www.xlin.hg.pl/podstawy/prawa.html*

Prawa dostępu w Linuksie: CHOWN / CHMOD

W systemie operacyjnym Linux każdy plik i katalog posiada zestaw praw określający, kto ma dostęp do pliku i jakie ma prawa. Każdy plik lub katalog może mieć prawo czytania (read), pisania (write), i wykonywania.Każde z tych praw dostępu reprezentowane jest odpowiednią literą i posiada przypisany odpowiedni parametr cyfrowy.

Litera	Znaczenie	Parametr Liczbowy
r	prawo odczytu	4
w	prawo zapisu	2
x	prawo uruchomienia	1
-	brak praw dostępu	0

Do każdego pliku lub katalogu możemy wyszczególnić trzy zestawy takich praw:

- prawa właściciela
- prawa grupy
- prawa pozostałych użytkowników

Do wyświetlenia praw dostępu do plików możesz posłużyć się poleceniem `ls` z opcją `-l` przykład:

```
[waldek@localhost waldek]$ ls -l
razem 944
-rw-r--r--    1 waldek   waldek      16561 sty 28 16:38 blackbox-menu
drwxrwxr-x    6 waldek   waldek       4096 sty 25 19:18 loki/
lrw-rw-r--    1 waldek   waldek      86720 sty 26 15:56 snap.sna
```

Pierwsza kolumna składająca się z dziesięciu znaków opisuje prawa dostępu, przy czym pierwszy znak określa rodzaj pliku (np. - (minus) oznacza plik, d oznacza katalog, l dowiązanie itd).
Znak drugi, trzeci i czwarty określa prawa właściciela do pliku,
znak piąty, szósty i siódmy określa prawa grupy do której należy plik,
natomiast znak ósmy, dziewiąty i dziesiąty prawa innych użytkowników systemu.

Jak widać w powyższym przykładzie do pliku `blackbox-menu` przypisano następujące uprawnienia:

prawo odczytu i zapisu dla właściciela (rw-)
prawo odczytu dla grupy (r--)
prawo odczytu dla pozostałych użytkowników (r--)

Dodając do siebie odpowiednie paramatry, zestaw trzech praw możemy przedstawić za pomocą jednej cyfry.
Oto kilka najczęściej spotykanych kombinacji:

Prawa	Wartość	Znaczenie
---	0	brak praw
r--	4	prawo do odczytu
rw-	6	prawa do odczytu i zapisu
rwx	7	prawa do odczytu zapisu i uruchomienia
r-x	5	prawa do odczytu i uruchomienia
--x	1	prawo do uruchomienia

W ten sposób za pomocą trzech cyfr możemy przedstawić całkowity *(tzn. trzy zestawy)* zbiór praw dostępu do pliku *(pierwsza cyfra - prawa właściciela, druga cyfra - prawa grupy, trzecia - prawa dla pozostałych użytkowników)*.

Prawa dostępu	Wartość liczbowa	Znaczenie
-rw-------	600	prawa do odczytu i zapisu tylko dla właściciela pliku
-rw-r--r--	644	prawa odczytu i zapisu dla właściciela oraz odczytu dla wszystkich pozostałych użytkowników.
-rw-rw-rw-	666	prawa odczytu i zapisu dla wszystkich użytkowników.
-rwx------	700	wszystkie prawa (odczyt, zapis, uruchomienie) tylko dla właściciela pliku.
-rwxr-xr-x	755	prawa do odczytu, zapisu i uruchomienia dla właściciela pliku oraz odczytu i uruchomienia dla wszystkich innych użytkowników
-rwxrwxrwx	777	wszystkie prawa dla wszystkich użytkowników (ustawienie niebezpieczne)
-rwx--x--x	711	prawa odczytu zapisu i uruchomienia dla właściciela pliku oraz prawo uruchomienia dla pozostałych użytkowników.

drwx------	700	dotyczy prawa zapisu i odczytu w katalogu tylko przez właściciela. **Katalogom zawsze musi być ustawione prawo dostępu *x*.**
drwxr-xr-x	755	do takiego katalogu wszyskie prawa ma właściciel, a wszyscy pozostali użytkownicy mogą tylko odczytać jego zawartość.
drwx--x--x	711	wszystkie prawa ma właściciel. Katalog z takimi prawami dostępny jest także dla wszystkich pozostałych użytkowników, lecz jego zawartość jest przed nimi ukryta *(polecenie ls nie wyświetli listy plików umieszczonych w tak oznaczonym katalogu)*. Aby odczytać plik użytkownik musi znać jego nazwę.

Zmiana właścicieli plików

Do zmiany włąściciela pliku służy polecenie **chown**.
Należy mieć uprawnienia do takich zmian lub zalogować się jako *root* i napisać:
`chown nazwa_właściciela nazwa_pliku`
Przykładowo jeżeli chcesz plik *readme.txt* przypisać dla użytkownika *krystian* wydaj polecenie takiej treści:
`chown krystian readme.txt`

Isnieje możliwość zmiany właściciela całego katalogu (z podkatalogami), aby to zrobić użyj opcji *-R* np:
`chown -R krystian dokumenty`
i w ten sposób katalog *dokumenty* stał się własnością użytkownika *krystian*

Aby zmienić także przynależność do grupy należy dopisać nazwę nowej grupy do nazwy użytkownika, odzielając obie nazwy kropką:
`chown krystian.root readme.txt`
Użytkownik *krystian* przypisany został do grupy *root* i stał się właścicielem pliku *readme.txt*

Zmiana praw dostępu do plików

Do zmiany praw dostępu do plików w systemie Linux służy polecenie **chmod**.
Składnia polecenia przy wykorzystaniu metody cyfrowej wygląda tak:
`chmod prawa_dostępu nazwa_pliku`
`prawa_dostępu` to jedna z opisanych wyżej trzycyfrowych liczb.
Przykładowo aby zmienić prawa dostępu do pliku *readme.txt* na `-rw-------` (prawo odczytu i zapisu tylko dla właściciela pliku) musiusz napisać:
`chmod 600 readme.txt`
Gdybyś chciał zmienić prawa dostępu do wszystkich plików w danym katalogu i jego podkatalogach skorzystaj z opcji `-R` Przykładowo aby ustawić zestaw uprawnień `644` dla wszystkich plików w katalogu `/home/waldek/pub` napisz tak:
`chmod -R 644 /home/waldek/pub`
Inną metodą nadawania uprawnień jest metoda symboliczna, polega na zdefiniowaniu odpowiedniego ciągu pojedyńczych liter.W tabelce poniżej przedstawione są znaczenia poszczególnych liter.

Kto	Działanie	Uprawnienie
u użytkownik	+ dać	**r** odczyt
g grupa	- zabrać	**w** zapis
o inni	= przypisać	**x** wykonanie
a wszyscy	**s** suid	

Składnia polecenia przy wykorzystaniu tego sposobu wygląda następująco:

```
chmod [ugoa][+ - =][rwxs] nazwa_pliku
```

Przykłady:
`chmod +x playit` - plik *playit* może być uruchomiony przez dowolnego użytkownika.
`chmod u+x playit` - daje właścicielowi pliku *playit* prawo jego wykonania.
`chmod a-w readme` - odbiera wszystkim prawo do zapisu do pliku *readme*
`chmod a+r *` - daje wszystkim użytkownikom prawo do odczytu do wszystkich plików znajdujących się w danym katalogu.

W Linuksie istnieje specjalne prawo dostępu zwane **SUID** (SetUID). Normalnie program może być uruchomiony przez użytkownika który jest jego właścicielem, ale są sytuacje gdy program (należący do *roota*) musi być uruchomiony przez osobę, do której nie należy (np.*ping* należy do *roota* a mimo tego, może być uruchomiony przez innych użytkowników). Aby umożliwić pozostałym użytkownikom korzystanie z takich programów trzeba nadać im specjalny atrybut **SUID**. Aby to zrobić należy liczbę określającą prawa dostępu poprzedzić cyfrą **4**, przykład:

```
chmod 4755 /bin/ping
```
lub w metodzie symbolicznej użyj opcji **s**:
```
chmod +s /bin/ping
```
Prawa czytania, pisania i wykonania w takich plikach widoczne są jako **rws** a nie **rwx**
Bardzo dobrym narzędziem do wykonania opisanych tu operacji jest MidnightCommander (MC).