

PRAVA PRISTUPA

Darko Novaković



Kao što sam naveo u prvom članku, Linux je još u startu osmišljen kao multikorisnički sistem. To znači da na sistemu može da radi više korisnika istovremeno. Da bi mogli da rade, korisnici se sa svojih radnih stanica moraju ulogovati (prijaviti) na sistem. Proces prijavljivanja na sistem je, u stvari, dostavljanje sistemu svoga korisničkog imena i lozinke, tako da sistem može da vodi računa da korisnik ne može da pristupi fajlovima kojima nije ovlašćen da pristupi. Običnom korisniku sistema nisu dozvoljene bilo koje osetljivije operacije na sistemu, kao npr. instaliranje novog softvera. Samo "root" korisnik, ili superkorisnik (superuser) ima prava da vrši bilo kakve promene i da pristupi svim fajlovima. Pametno je prijavljivati se na sistem kao "root" samo kada je neophodno, a ne u svakoj prilici. Time se izbegava npr. nenamerno brisanje sistemskih fajlova i bilo koje drugo oštećenje sistema prouzrokovano neograničenim ovlašćenjima "root" korisnika.

Prava pristupa fajlovima i direktorijumima

Svaki fajl na sistemu pripada nekom korisniku i grupi korisnika. Svaka od ovih grupa korisnika ili neka druga može biti ovlašćena da piše (write), čita (read) ili izvrši (execute) fajl. "Root" korisnik je taj koji formira grupe korisnika. Grupa se sastoji od korisnika kojima se dodeljuju ista prava pristupa. Npr. na jednom fakultetu jedna grupa korisnika mogu biti studenti prve i druge godine, druga grupa su studenti viših godina studija i postdiplomskih studija, sledeća grupa mogu biti asistenti i profesori, sledeća radnici fakulteta u administraciji i, konačno, grupa administratora sistema (root korisnici). Jedan korisnik može biti u više grupa. Pomoću komande **groups**, svaki korisnik može da proveru u kojim se sve grupama nalazi.

Prava pristupa fajlovima su veoma jednostavno organizovana. Za neki fajl, prava pristupa se mogu videti primenom komande **ls -l**.

Posle primene sledeće komande:

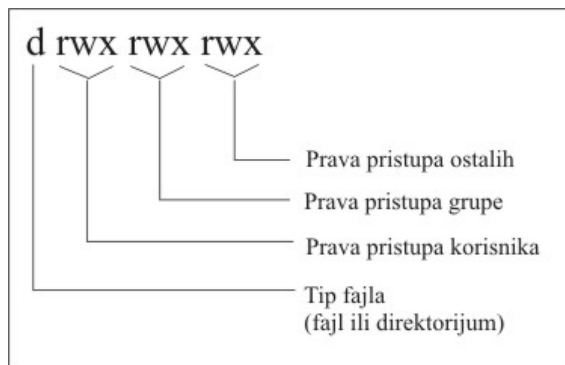
```
~/test>ls -l
```

u nizu izlistanih fajlova pozabavićemo se sa ovim:

```
-rw-r--r--    1 darko  users 411 2003-11-24 12:34 prvarh.tar.gz
```

Dakle, fajl prvarh.tar.gz pripada korisniku darko, koji pripada grupi users, veličine je 411 bajtova, a kreiran 24 novembra 2003 godine u 12 sati i 34 minuta.

Međutim, nas zanima prva kolona ovog reda sa svojih 10 znakova koja, kada je kompletna, izgleda kao na slici:



Na svakom od 10 mesta može da stoji odgovarajući znak kao na slici ili crtica, '-'. Ako je prvi znak crtica, onda je u pitanju fajl, dok 'd' označava direktorijum, 'l' link, 'b' blok uređaj. Za sve ostale znakove (na ostalih 9 mesta) smisao crtice je isti: ona označava da korisnik (vlasnik fajla) , grupa (grupa-vlasnik fajla) ili ostali nemaju prava pristupa odgovarajuće kategorije. Postoje 3 kategorije pristupa fajlu:

- r- čitanje
- w- upis
- x- izvršavanje

i kao što se sa slike vidi, oni se postavljaju za svaki od 3 gore definisana skupa korisnika. U našem slučaju, prvarh.tar.gz je fajl (prva crtica), vlasnik je korisnik darko i on ima prava da čita i piše u fajl (rw-), grupa korisnika koja je vlasnik fajla je users i svi korisnici iz te grupe mogu samo da čitaju fajl (r--), a i svi ostali mogu samo da čitaju ovaj fajl (r--). Primitimo da ovo nije fajl koji se može izvršavati, pa zato i nema smisla postavljati kategoriju pristupa x.

Što se prava pristupa direktorijumu tiče, tumačenje kategorija pristupa je po prirodi stvari nešto drugačiji. Ovo ćemo pokazati na sledećem primeru:

drwxr-xr-x 4 darko users 96 2003-09-05 16:26 Programi

Oznaka 'd' kaže nam da je Programi direktorijum, prvo rwx predstavlja prava pristupa vlasnika direktorijuma:

- r sadržaj direktorijuma Programi može da se čita
- w mogu se kreirati novi fajlovi (kao i brisati stari!)
- x može se ući u (engl. change to) direktorijum (na njega se može primeniti komanda cd)

Zatim, r-x znači da korisnici iz grupe users mogu da pročitaju sadržaj direktorijuma i da mu pristupe, ali da ne mogu da kreiraju ili brišu fajlove u njemu. Isto važi i za sve ostale korisnike (poslednje r-x).

Menjanje prava pristupa

Ovo može da uradi samo vlasnik fajla (direktorijuma) i naravno "root" korisnik primenom komande **chmod**. Ova komanda ima sledeći oblik:

chmod [opcije] mod fajlovi

Mod može biti numerički ili izraz u formi *ko opkod pravo*. U tabeli su date moguće vrednosti i njihovo objašnjenje, a evo i nekoliko primera.

Fajlu iz gornjeg primera, `prvarh.tar.gz`, možemo promeniti prava pristupa na sledeći način:

`~/test>chmod go+w prvarh.tar.gz`

Ovim smo grupi (g) i svim ostalima (o) dodelili (+) pravo upisivanja (w). Naravno, ovo nije mnogo smisleno i tako nešto verovatno nećete poželeti da uradite u praksi ako je taj fajl takav da mu samo vi treba da pristupite (bitan sadržaj).

Nekoliko izmena, ako se odvoje zarezima, može se obaviti samo sa jednom `chmod` komandom.

U slučaju numeričkog načina menjanja prava pristupa pomoću komande `chmod`, potrebno je sabrati sva prava pristupa koji želimo dodati za svaki skup korisnika (vlasnika, grupu, sve ostale – tim redom!) i taj niz brojeva zapisan bez razmaka postaviti kao parametar `chmod` komandi. Kao primer uzeću hipotetički fajl sa imenom file:

`~>chmod 761 file`

Posle gornje komande, nad fajlom file postavljena su sva prava za vlasnika fajla (7=4+2+1), za grupu prava čitanja i upisivanja (6=4+2), a za sve ostale samo pravo izvršavanja (1).

Ostale oznake iz tabele vezane za prava pristupa objasnićemo narednog meseca.

Do sledećeg puta kada ćemo nastaviti priču o pravima nad fajlovima i direktorijumima, ostavljam vas da se igrate na ovu temu, ali oprezno!

<i>mod</i>					
<i>ko</i>		<i>opkod</i>		<i>pravo</i>	
karakter	objašnjenje	karakter	objašnjenje	karakter	objašnjenje
u	korisnik	+	Dodaj pravo	r	čitanje
g	grupa	-	Oduzmi pravo	w	pisanje
o	ostali	=	Dodeli pravo	x	izvršavanje
a	svi (podrazumeva se ako se ne navede drugačije)		(i ukloni prava na nespecificovanim poljima)	s	Postavljanje korisnikovog ili grupnog ID-a
				t	Sticky bit (čuva tekst mod-za fajlove, ili sprečava da oni koji nisu vlasnici uklone fajlove-za direktorijum)
				u	Tekuće pravo korisnika
				g	Tekuće pravo grupe

<i>mod</i>	
o	Tekuće pravo ostalih
Numerički način	
4	čitanje
2	upisivanje
1	izvršavanje
Dodatna četvrta cifra	
4	Biće naknadno objašnjeno
2	
1	