KONTROLA PRISTUPA NA NIVOU SISTEMA DATOTEKA

Pristup resursima pod mrežnim operativnim sistemima (kao što je i *Linux*) je strogo kontrolisan. Sistem datoteka je fundamentalni resurs svake radne stanice ili servera, a kontrola pristupa datotekama i direktorijumima (dodela ovlašćenja za pristup i zaštita od neovlašćenog pristupa) ključna komponenta ozbiljnih zaštitnih polisa u svakom višekorisničkom sistemu.

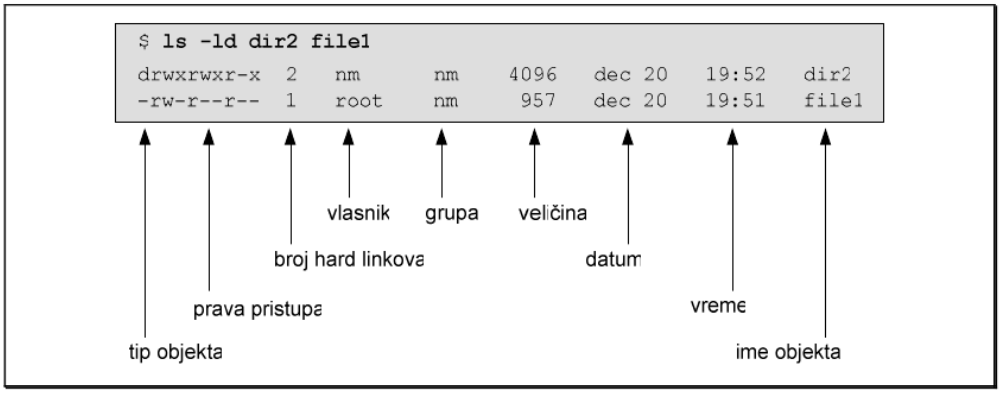
VLASNIČKI ODNOSI I PRAVA PRISTUPA

Jedna od najznačajnijih komponenti svake ozbiljne zaštitne politike je kontrola pristupa na nivou sistema datoteka. Kontrolom pristupa na nivou sistema datoteka određuju se:

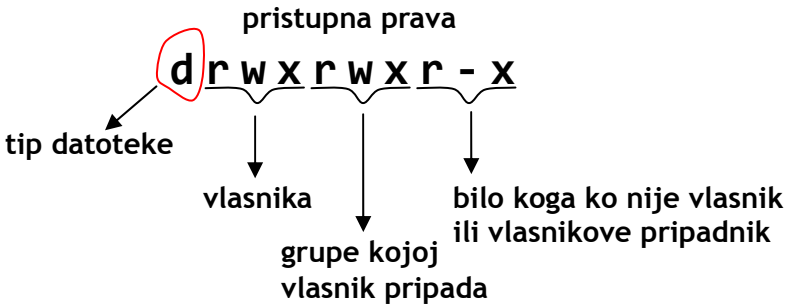
- skup korisnika koji mogu pristupiti objektima, odnosno datotekama i direktorijumima,
- nivo pristupa, odnosno skup akcija koje autorizovani korisnici mogu izvršiti nad tim objektima.

Kontrola pristupa na nivou sistema datoteka zasniva se na vlasničkim odnosima, odnosno vlasništvu nad objektima (pripadnost objekta korisnicima i grupama) i pravima pristupa. Prava pristupa se dodeljuju svakoj datoteci i direktorijumu.

Prava pristupa za datoteke i direktorijume najlakše se mogu odrediti pomću komande ls (list) sa parametrom -l (long), kao što je prikazano u sledećem primeru:



Kategorije pristupnih prava



1. Tip datoteke

Prvi karakter ukazuje na tip datoteke:

- **- (dash)** - je reč o običnoj, regularnoj datoteci
- **d** - reč je o direktorijumu
- **b** - blok uređaj - block special file

- **c** - karakter uređaj - character special file
- **l** - simbolički link
- **p** - imenovani pipe
- **s** - socket.

2. Prava pristupa

Sledećih devet znakova predstavljaju prava pristupa objektu za tri vlasničke kategorije, a to su vlasnik, grupa i ostali. Prva tri karaktera definišu prava pristupa vlasnika, druga tri prava pristupa grupe kojoj datoteka pripada i poslednja tri karaktera prava pristupa za ostale:

- **Vlasnik (owner)** najčešće je korisnik koji je kreirao objekat, osim ukoliko superuser (root) ne promeni vlasništvo. U tom slučaju, vlasnik je korisnik kome je vlasništvo dodeljeno. Vlasnik objekta može biti bilo koji korisnik sistema, regularan ili sistemski.
- **Grupa (group)** je korisnička grupa kojoj je datoteka formalno priključena. Za razliku od korisnika koji mogu pripadati većem broju grupa, objekti sistema datoteka **mogu pripadati samo jednoj grupi**, koja može biti regularna ili sistemska. Najčešće je to primarna grupa korisnika koji je objekat kreirao. Superuser naknadno može promeniti pripadnost objekta grupi.
- **Ostali (others, public)** su svi korisnici koji nisu ni vlasnik objekta, niti pripadaju grupi kojoj objekat pripada. Prava pristupa za svaku vlasničku kategoriju eksplicitno se dodeljuju svakom objektu prilikom kreiranja, a kasnije se mogu promeniti.

Pravo pristupa za svaku grupu se zadaje na isti način, sa istim rasporedom karaktera **rwx**:

- **pravo čitanja (`r - read`),**
- **pravo upisa (`w - write`),**
- **pravo izvršavanja (`x - execute`).**

Ukoliko se na odgovarajućoj poziciji nalazi crtica **`-`, pravo je ukinuto**.

Primeri.

```
$ ls -la ~/.bash_profile
-rw-r--r--    1    nm      nm    509     Mar 10     17:21     .bash_profile
$ ls -ld /bin /root
drwxr-xr-x    2    root    root  2048    Apr 1      20:16     /bin
drwxr-x---    7    root    root  1024    Apr 20     15:43     /root
```

Sistemski direktorijum /bin sadrži najčešće korišćene UNIX komande. Svim korisnicima sistema dato je pravo korišćenja direktorijuma bin. Svi korisnici sistema mogu da se pozicioniraju na direktorijum, mogu da pročitaju sadržaj i pokrenu komande koje se u njemu nalaze. Pravo upisa dato je jedino superuser-u. Sistemski direktorijum root je home direktorijum superusera, koji nad njim ima sva prava. Članovi grupe root mogu da pročitaju sadržaj direktorijuma i da se pozicioniraju na njega, dok je ostalim korisnicima pristup direktorijumu zabranjen.

Značenje prava za datoteke i direktorijume bitno se razlikuje.

	pristupna prava za datoteke	**pristupna prava za direktorijume**
read (r)	korisnik može pročitati sadržaj datoteke, odnosno može prikazivati datoteku na ekranu, štampati je ili kopirati;	korisnik može pročitati sadržaj direktorijuma, što zna i da korisnik može da izvrši komandu ls. **Napomena:** za prikaže detaljni listing direktorijuma (`ls -l`) je neophodno i x pravo nad direktorijumom
write (w)	korisnik može modifikovati sadržaj datoteke. **Napomena**: može obrisati datoteku samo ako mu je dato pravo upisa nad roditeljskim direktorijumom;	korisnik može modifikovati sadržaj direktorijuma, odnosno dodavati nove datoteke i brisati postojeće, kreirati i brisati poddirektorijume. **Napomena**: može obrisati direktorijum samo ako mu je dato pravo upisa nad roditeljskim direktorijumom;

execute (x)	korisnik može izvršavati datoteku, pod uslovom da se radi o shell programu ili o datoteci u binarnom izvršnom formatu;	korisnik se može pozicionirati na direktorijum (komandom cd), može prikazivati dugački listing (ls -l) sadržaja i pretraživati direktorijum (find).

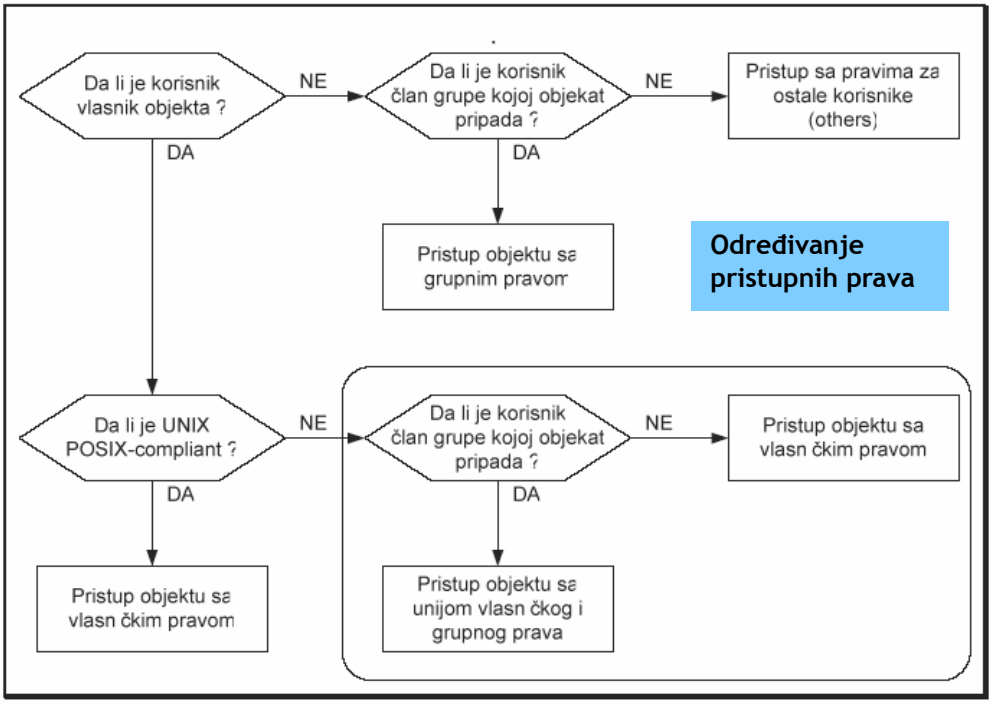
Svim datotekama i direktorijumima dodeljen je korisnički identifikator (UID) i grupni identifikator (GID) vlasnika. Kernel razrešava vlasničke odnose na osnovu ovih identifikatora.

```
$ ls -ln
-rw-rw-r--        1    859    861        20     dec 23     14:04     kyuss
-rw-rw-r--        1    859    861        20     dec 23     15:20     stoner
```

```
$ id
uid=859(nm) gid=861(nm) groups=861(nm),0(root)
```

UID i ime tekućeg korisnika, GID i imena primarne i svih grupa kojima tekući korisnik pripada

```
$ groups
nm root
```



PROMENA PRISTUPNIH PRAVA

Prava pristupa mogu promeniti isključivo vlasnici datoteka i direktorijuma, dok root kao superuser može da promeni pristupna prava svakom objektu.

Komanda **chmod** može se pokrenuti u **simboličkom (relative)** ili **oktalnom (absolute) režimu**.

Simbolički režim

Korisnik dodeljuje ili oduzima prava u odnosu na postojeća, dok se postojeća prava koja nisu specificirana argumentom komande ne menjaju. Format komande u simboličkom modu je:

```
$ chmod [-R] symbolic_mode[,...] objectname
```

primer: `$ chmod u=rwx myscript`

symbolic_mode sastoji se od tri komponente:

- vlasnička kategorija na koju se komanda odnosi: **vlasnik (u), grupa (g), others (o), sve kategorije (a)**;
- operator: **dodela prava (+), ukidanje prava (-), dodela tačno određenih prava (=)**;
- prava pristupa koja se dodeljuju ili oduzimaju: **r, w i/ili x**.

PRIMERI.

```
$ touch myfile
$ ls -l myfile
-rw-r--r--        1    nm      nm      0     dec 23     15:25     myfile

$ chmod go+w myfile
$ ls -l myfile
-rw-rw-rw-        1    nm      nm      0     dec 23     15:25     myfile
                                                  dodata prava upisa kategorijama group i others

$ chmod u-w myfile
$ ls -l myfile
-r--rw-rw-        1    nm      nm      0     dec 23     15:25     myfile
                                                    oduzeto pravo upisa vlasniku

$ chmod u=rw,go-w myfile
$ ls -l myfile
-rw-r--r--        1    nm      nm      0     dec 23     15:25     myfile
                  dodeljen skup prava rw vlasniku i ukinuto pravo upisa kategorijama group i others

$ chmod a= myfile
$ ls -l myfile
----------        1    nm      nm      0     dec 23     15:25     myfile
                                                        svima ukinuta sva prava
```

Parametar -R se koristi za rekurzivnu promenu pristupnih prava direktorijuma i svih objekata (poddirektorijuma i datoteka) koji se u njemu nalaze. Ukoliko se navede parametar -R, argument objectname mora biti direktorijum.

PRIMER.

```
$ ls -ld parent_dir
drwxr-xr-x        2    nm      nm      4096       Apr 28    09:10     parent_dir
$ ls -l parent_dir
parent_dir:
total 0
-rw-r--r--        1    nm      nm         0    Apr  28    09:09     dir1
-rw-r--r--        1    nm      nm         0    Apr  28    09:10     dir2
-rw-r--r--        1    nm      nm         0    Apr  28    09:09     file1
-rw-r--r--        1    nm      nm         0    Apr  28    09:09     file2
$ chmod -R o-rx parent_dir
$ ls -ld parent_dir
drwxr-xr-x        2    nm      nm      4096       Apr 28    09:10     parent_dir
$ ls -l parent_dir
parent_dir:
```

```
total 0
-rw-r--r-- 1 nm  nm        0     Apr  28     09:09 dir1
-rw-r--r-- 1 nm  nm        0     Apr  28     09:10 dir2
-rw-r--r-- 1 nm  nm        0     Apr  28     09:09 file1
-rw-r--r-- 1 nm  nm        0     Apr  28     09:09 file2
```

Oktalni režim

Komandom chmod u oktalnom režimu dodeljuju se prava pristupa svim vlasničkim kategorijama istovremeno. Prava koja korisnik navede kao argument komande eksplicitno zamenjuju postojeća prava (prethodna prava se ne prolongiraju), tako da se ovaj režim naziva apsolutnim. Komanda zatheva da se u ovom režimu kao argument navedu tri oktalne cifre od kojih svaka predstavlja prava pristupa za jednu vlasničku kategoriju.

Moguće oktalne vrednosti sa odgovarajućim pravima opisane su sledećom tabelom:

Oktalna vrednost	Suma prava po binarnoj vrednosti	Odgovarajuća prava	Definicija
7	4 + 2 + 1	r w x	čitanje, izmena i izvršavanje
6	4 + 2 + 0	r w –	čitanje i izmena
5	4 + 0 + 2	r – x	čitanje i izvršavanje
4	4 + 0 + 0	r – –	samo čitanje
3	0 + 2 + 1	– w x	izmena i izvršavanje
2	0 + 2 + 0	– w –	samo izmena
1	0 + 0 + 2	– – x	samo izvršavanje
0	0 + 0 + 0	– – –	bez prava pristupa

Sintaksa komande chmod u oktalnom režimu je sli na sintaksi komande u simboličkom režimu:

```
$ chmod [-R] absolute_mode objectname
```

Apsolutna prava formiraju se pomoću tri oktalne cifre kojima su predstavljena prava pristupa za vlasnika, grupu i ostatak sveta. Parametar -R se, kao i u simboličkom režimu, koristi za rekurzivnu promenu pristupnih prava direktorijuma i svih objekata koji se u njemu nalaze. U tom slučaju argument objectname mora biti direktorijum.

Napomena: Kada se koristi oktalni režim **moraju se navesti sve tri oktalne cifre** u tačnom redosledu (vlasničko pravo -grupno pravo - pravo za ostatak sveta).

```
$ ls -l betatest
-rw-rw-rw-   1   nm    nm 0 dec 23 15:25 betatest
$ chmod 555 betatest
$ ls -l betatest
-r-xr-xr-x   1   nm    nm 0 dec 23 15:25 betatest
$ ls -l denywrites
-rwxrwxrwx   1   nm    nm 0 dec 23 15:25 denywrites
```

```
$ chmod 755 denywrites
$ ls -l denywrites
-rwxr-xr-x   1   nm    nm 0 dec 23 15:25 denywrites
```

PROMENA VLASNIČKIH ODNOSA

UNIX postavlja inicijalne vlasničke odnose prilikom kreiranja datoteke ili direktorijuma. Korisnik koji kreira objekat postaje njegov vlasnik, a objekat se formalno pridružuje primarnoj grupi vlasnika.

Promena vlasnika

Komandom chown (change owner) root kao superuser može da promeni vlasnika objekta, a ukoliko konkretan sistem to dozvoljava, to može učiniti i vlasnik. Regularni korisnici Linux sistema mogu promeniti vlasničke odnose samo ako na sistemu nije aktiviran mehanizam disk kvote (disk quota), kojim se korisnicima ograničava iskorišćenje prostora na diskovima. Kada se za datoteku promeni vlasništvo, prava pristupa starog vlasnika određena su kategorijama group i others. Sledeće komande prikazuju sintaksu za promenu vlasništva:

```
# chown [-R] new_owner objectname

$ whoami
nm
$ ls -l myfile
-rw-r--r--        1    nm           nm      0    Apr 28       12:07     myfile
$ chown jsmith myfile
chown: changing ownership of `myfile': Operation not permitted
$ su
Password: ******
# chown jsmith myfile
# exit
exit
$ ls -l myfile
-rw-r--r--        1    jsmith       nm      0    Apr 28       12:07     myfile
```

Sticky bit (t)

Postavljanjem sticky bita za direktorijum uvodi se sledeće ograničenje: **bez obzira na pravo upisa koje korisnik ima nad tim direktorijumom, on u njemu ne može obrisati tuđe datoteke (odnosno datoteke kojima on nije vlasnik)**. Tipičan primer je sistemski direktorijum /tmp. Sticky bit se postavlja i ukida komandom `chmod` tako što se u simboličkom režimu svim vlasničkim kategorijama dodeli pravo t (chmod +t directory), a ukida oduzimanjem prava t.

```
$ ls -l public_dir
-rwxrwxrwx        1    nm       nm     4096       dec 23       15:25    public_dir1
$ chmod +t public_dir1
$ ls -l public_dir1
-rwxrwxrwt        1    nm       nm     4096       dec 23       15:25    public_dir1
$ chmod -t public_dir1
-rwxrwxrwx        1    nm       nm     4096       dec 23       15:25    public_dir1
```