Osnove korištenja operacijskog sustava Linux

08. Vlasništvo i dozvole

Lucija Petricioli, Josip Žuljević
Nositelj: doc. dr. sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

10.01.2015

Sadržaj

Općenito o dozvolama (1)

- Nužno je osigurati odgovarajuću zaštitu svih korisnika
- Zaštita objekta (npr. direktorij, datoteka) se temelji na:
  - Objekt je vlasništvo korisnika i grupe
    - Njih ispisuje naredba `ls -l`
  - Uz objekt vezano je 9 bitova koji definiraju prava svih korisnika na taj objekt
    - Definiraju tko smije čitati, pisati i izvršavati/pretraživati

Općenito o dozvolama (2)

- Deset bitova piše se u simboličkom obliku `-rwxrwxrwx`
  - Prvi bit (-) označava vrstu datoteke
  - Prva grupa od tri bita (rwx) s lijeve strane definira prava za vlasnika (prvi bit je vrsta datoteke)
  - Druga grupa od tri bita (sredina) definira prava za grupu
  - Konačno, zadnja tri bita s desne strane definiraju prava za sve ostale

Općenito o dozvolama (3)

- Značenja pojedinih bitova su sljedeća:
  - r Dozvoljeno čitanje direktorija/datoteke
  - w Dozvoljeno pisanje u direktorij/datoteku
  - x Dozvoljeno izvršavanje datoteka/pretraživanje direktorija
- Primjeri

```
rwxr-xr-x
rw-r--r--
r--r--r--
```

Općenito o dozvolama (4)

- Način odlučivanja kada korisnik pokušava pristupiti datoteci/direktoriju:
  - Je li vlasnik datoteke isti kao korisnik koji pokušava pristupiti
    - Ako je, primjeni prva tri bita za odluku
  - Je li korisnik član grupe koja je vlasnik datoteke
    - Ako je, primjeni druga tri bita za odluku
  - Inače, primjeni zadnja tri bita za odluku
  - Vlasnik $\Rightarrow$ Grupa $\Rightarrow$ Ostali

Općenito o dozvolama (5)

- Primjer
  - Neka datoteka je vlasništvo korisnika student1
  - Grupa group1 je vlasnik datoteke i postavljene su sljedeće zastavice:

    `rwxr-x---`

    - student1 može čitati, pisati i izvršavati datoteku
    - student2, član grupe grupa1, može čitati i izvršavati datoteku
    - student3, koji nije član grupe grupa1, ne može niti čitati niti pisati niti izvršavati datoteku

Općenito o dozvolama (6)

- Primjer
  - Neka datoteka vlasništvo je korisnika student1
  - Grupa group1 je vlasnik datoteke i postavljene su sljedeće zastavice:

    `---rwxr-x`

    - student1 ne može niti čitati, niti pisati niti izvršavati datoteku
    - student2, član grupe grupa1, može čitati, pisati u datoteku i izvršavati datoteku
    - student3, nije član grupe grupa1, može čitati i izvršavati

Promjena dozvola (1)

- Promjena dozvola obavlja se naredbom `chmod`
- Sintaksa naredbe je:

```
chmod <dozvole> <objekt>
```

- Dozvole se mogu zadati oktalno i simbolički
- Moguće jer rekurzivno mijenjati prava

```
chmod -R <dozvole> <objekt>
```

Promjena dozvola (2)

- Oktalni prikaz dozvola

Oktalna znamenka	Binarno	Prava
0	000	`---`
1	001	`--x`
2	010	`-w-`
3	011	`-wx`
4	100	`r--`
5	101	`r-x`
6	110	`rw-`
7	111	`rwx`

Promjena dozvola (3)

Simbolički prikaz	Oznaka	Opis
Tko	a	Svi korisnici (vlasnik, vlasnikova grupa, svi ostali korisnici)
	g	Vlasnikova grupa
	o	Svi ostali korisnici
	u	Samo vlasnik
Operator	+	Dodaje mod
	-	Oduzima mod
	=	Postavlja potpunu vrijednost moda
Dozvola	r	Postavlja dozvolu čitanja
	w	Postavlja dozvolu pisanja
	x	Postavlja dozvolu izvršavanja

Promjena dozvola (5)

- Primjer (simbolički oblik)

`chmod ugo=rwx file1`

  - Vlasnik, grupa i ostali imaju sva dopuštenja

`chmod a=rwx file1`

  - Svi imaju sva dopuštenja
  - Identično prethodnoj naredbi

`chmod u=rwx,go=rx file1 file2`

  - Moguće je kombinirati dopuštenja
  - Vlasnik može sve dok ostali mogu čitati i izvršavati datoteke

`chmod g+w file1 file2 file3`

  - Dodavanje prava čitanja grupi

`chmod -x file1 file2`

  - Oduzimanje prava izvršavanja svim korisnicima

Promjena dozvola (6)

- Uobičajeni način omogućavanja pokretanja skripte je promjena dozvola nad tom skriptom
  - Dodavanje oznake x prvog terceta bitova
  - Pokretanje pomoću sintagme `./<ime-skripte>`

Vlasnik datoteke

- Vlasnik datoteke može bez obzira na trenutne dozvole promijeniti dozvole
  - Ne može zaobići trenutne dozvole
  - Ne može promijeniti vlasnika datoteke
  - Može obrisati datoteku

Podrazumijevane dozvole

- Kada se kreira nova datoteka ona prima neke podrazumijevane dozvole
  - Na podrazumijevane dozvole utječe se naredbom `umask`
  - Vrijednost `umask` varijable se XOR-a s vrijednosti 777 i to je nova dozvola datoteke
- Primjer: ako je `umask` postavljen na 022 tada će datoteke imati dozvolu 755
  - Naredba `umask` bez argumenata ispisuje trenutnu vrijednost
- Postavljanje vrijednosti umask obavlja se tako da se zada nova vrijednost (oktalno ili simbolički sa `-S`)

Promjena vlasnika (1)

- Promjena vlasnika datoteke ili direktorija obavlja se naredbom `chown`
- Ta naredba isključivo je dostupna administratoru!
- Sintaksa je:

```
chown <korisnicko ime> <objekt>
```

- Opcijom `-R` je moguće rekurzivno postavljanje prava

Promjena vlasnika (2)

- Moguće je istovremeno promijeniti korisnika i grupu
  - Prvi način

    ```
    $ chown <korisnik>:<grupa> <objekt>
    ```
  - Drugi način

    ```
    $ chown <korisnik>.  <objekt>
    ```
    - Točka označava grupu istog imena kao korisnik

Promjena grupe

- Promjena grupe datoteke ili direktorija obavlja se naredbom `chgrp`
- Ta naredba isključivo je dostupna administratoru!
- Sintaksa je:

```
chgrp <ime grupe> <objekt>
```

- Opcijom `-R` je moguće rekurzivno postavljanje prava

Naredba `sudo` (1)

- engl. *superuser do*
- Dozvole ne vrijede ako ste root
  - root može sve!!
- Naredbom `sudo` privremeno postajete drugi korisnik npr. root korisnik i imate sve ovlasti
  - Omogućuje davanje administratorskih ovlasti dodatnim korisnicima bez poznavanja lozinke roota

Naredba `sudo` (2)

- Sintaksa je

  `sudo <opcije> <naredba>`

  - Opcija `-u` zadaje korisnika pod čijim imenom se izvršava naredba, podrazumijeva se root

Datoteka `sudoers` (1)

- Popis korisnika i ovlasti je u `/etc/sudoers`
- Sastoji se od dvije vrste zapisa
  - Aliasa
  - Dopuštenja

```
root  ALL=(ALL) ALL
<tvoj-username> ALL=(ALL) ALL
```

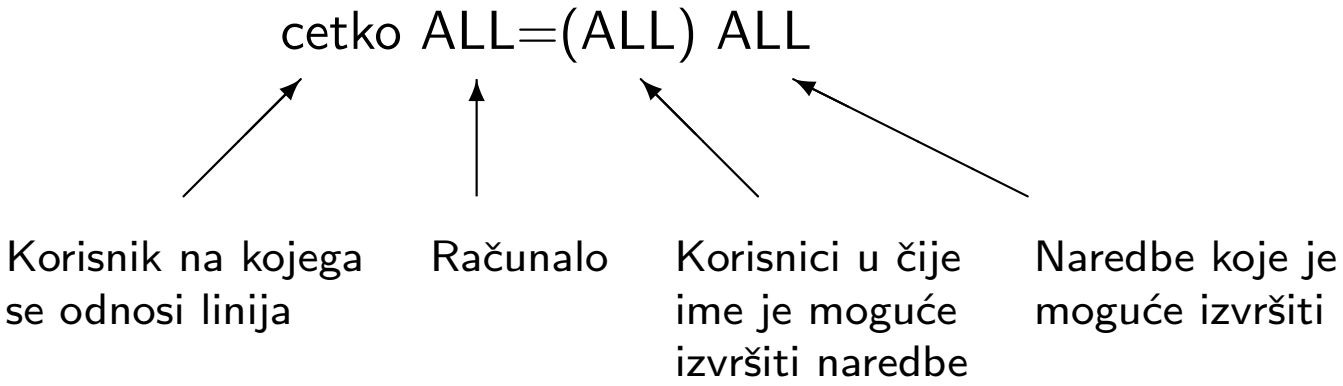
- Brisanjem root korisnika iz datoteke ograničava roota samo kod korištenja naredbe sudo – i dalje može sve!

Datoteka `sudoers` (2)

- Uvijek editirati naredbom `visudo`!
  - `visudo` upozorava na moguće greške
  - Neke distribucije dopuštaju mijenjanje datoteke samo pomoću `visudo`

Datoteka `sudoers` (3)

- Svaka linija označava pravilo



  - Korisnik cetko može na svim računalima kao bilo koji korisnik na sustavu izvršiti sve naredbe

Datoteka `sudoers` (4)

- Primjeri

  ```
  okosl ALL=(root) /usr/bin/apt-get, /usr/bin/vim
  ```

  - Moguće je definirati grupu

    ```
    %sudoers ALL=(root) /usr/bin/apt-get, /usr/bin/vim
    ```

  - Ili dopustiti pokretanje bez unošenja lozinke

    ```
    okosl ALL=(ALL) NOPASSWD: ALL
    ```

Datoteka `sudoers` (5)

- Postoje četiri vrste pseudonima (*alias*) za svaki od četiri dijela linije
  - Runas_Alias, User_Alias, Host_Alias, Cmnd_Alias
- Primjer

```
Cmnd_Alias SHUTDOWN_CMDS = /sbin/halt, /sbin/reboot
User_Alias USERS = tom, dick, harry, %admin
USERS ALL=(ALL) NOPASSWD: SHUTDOWN_CMDS
```

Literatura

- http://articles.slicehost.com/2010/7/17/using-chmod-part-1-symbolic-mode
- http://articles.slicehost.com/2010/7/17/using-chmod-part-2-octal-mode
- https://help.ubuntu.com/community/Sudoers

Naredbe

Naredba	Opis
chmod	promjena dozvola datoteke/direktorija
umask	promjena podrazumijevanih dozvola
chown	promjena vlasnika datoteke/direktorija
chgrp	promjena grupe datoteke/direktorija
sudo	kratkotrajne administratorske ovlasti