Osnove korištenja operacijskog sustava Linux

05. Korisnici i grupe, vlasništvo i dozvole

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

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

09.12.2017

Sadržaj

Osnovni pojmovi (1)

- Linux je višekorisnički operacijski sustav
- Uloge višekorisničkog rada u OS-u:
  - Zaštita privatnosti
  - Specifične postavke i podaci
  - Sprečavanje zlouporabe
  - Pravedna raspodjela resursa

Osnovni pojmovi (2)

- Terminal – U/I naprava za komunikaciju korisnika s računalom
- Nekada fizički uređaj, danas programski emulatori
- Omogućuju korisniku prikaz *ljuske* - npr. `bash`
- Prijava na sustav
  - Prijava lozinkom ili drugim vjerodajnicama (npr. RSA)
  - Odmah po prijavi u sustav korisnik je smješten u svoj matični direktorij
- Odjava iz sustava
  - Iz `bash` ljuske ostvaruje se:
    - naredbom `logout`
    - `exit`
    - kombinacijom `CTRL+D` - slanje signala `SIGQUIT`
  - Terminal otvara upit za prijavu novog korisnika

Osnovni pojmovi (3)

- Terminali su predstavljeni datotekama uređaja:

  `tty0, tty1, tty2, ...`
  - Terminalima upravlja upravljački program - `getty`
  - Kod modernih - virtualnih - terminala korisnik može s istog mjesta koristiti više terminala
  - Između terminala se prebacuje sa Ctrl+Alt+F1...F7
  - Ctrl+Alt+F7 vraća u konzolu s grafičkim sučeljem (npr. X)

  `pts/N`
  - Označavaju pseudoterminale - programski emulirane
  - Oni su "terminal" na koji se danas najčešće misli
    Npr. `gnome-terminal`

Baza passwd (1)

- Temeljna datoteka s korisnicima je `/etc/passwd`
  - Povezuje korisničko ime i UID
  - Nekada je u njoj bila i lozinka
  - Vrlo loše sa sigurnosne strane - ne može se zabraniti njeno čitanje jer mnoštvo aplikacija ovisi o podacima u toj datoteci
- Sadrži jedan zapis po liniji oblika

  Korisničko ime:Lozinka:UID:GID (primarna grupa):Info:Matični direktorij:Korisnička ljuska

  `root:x:0:0:root:/root:/bin/bash`
- Uređivanje naredbom `vipw`
  - Zaštita od paralelnog uređivanja
  - Osnovno parsiranje i sintaksna provjera

Baza passwd (2)

- Korisnici navedeni u passwd datoteci ne moraju biti (i uglavnom nisu) interaktivni korisnici
- Neke korisnike koriste servisi koji ne trebaju izravno logiranje u ljusku.

- Matični direktorij korisnika ne mora biti zadan ako se ne radi o interaktivnom korisniku
- Ljuska određuje koji se program koristi prilikom prijave korisnika

  `/bin/bash` - Moguća vrijednost za interaktivnog korisnika
  `/bin/false` - Moguća vrijednost za korisnika bez mogućnosti prijave na sustav

Datoteka passwd

```
#!/bin/bash

# ispisi datoteku /etc/passwd


# ispisi liniju sa svojim userom/imenom
```

Datoteka passwd

```
#!/bin/bash

# ispisi datoteku /etc/passwd
cat /etc/passwd

# ispisi liniju sa svojim userom
cat /etc/passwd | grep darko
```

Baza shadow

- Ako u passwd bazi na mjestu lozinke stoji `x` tada se sigurnosni podaci o korisniku nalaze u datoteci `/etc/shadow`
  - Sadrži kriptirane lozinke, te dodatne podatke o njihovom trajanju
  - Čitljiva je isključivo root korisniku

- Sadrži jedan zapis po liniji oblika

Korisničko ime:Lozinka:Polja s dodatnim podacima

```
root:T3RqrzxU1MAH3F3wtuQu/:13284:0:99999:7:::
```

Naredba `who`

- Naredba može prikazati podatke o korisniku
- Primjer ispisa

```
$ who
cetko   tty7    2010-11-11   12:01   (:0)
cetko   pts/0   2010-11-11   17:08   (:0)
cetko   pts/1   2010-11-11   17:08   (:0)
cetko   pts/2   2010-11-11   17:12   (:0)
```

- Poseban oblik naredbe `who` je `who am i` kao i `who mom likes`
  - Ispisuje tko je trenutni korisnik na trenutnom terminalu
- Varijanta te naredbe je `whoami`
  - Ispisuje samo korisničko ime

Naredba `finger`

- Drugi način prikaza trenutno aktivnih korisnika
- Prikazuje trenutno logirane korisnike, ili prikazuje detaljnije podatke o nekom korisniku
- Prikazuje dodatne podatke
  - Iz `Info` polja u passwd bazi
  - Čita ih iz datoteka `.project` i `.plan` u matičnom direktoriju
- Ako joj zadamo parametar pretražuje korisnika
  - Pretraživanje se obavlja po korisničkom imenu i pravom imenu

Naredba w

- Primjer ispisa

```
USER     TTY      FROM   LOGIN@   IDLE    JCPU    PCPU    WHAT
cetko    tty7     :0     12:01    5:32m   3:45    9.67s   awesome
cetko    pts/0    :0     17:29    3:21    0.33s   0.33s   bash
cetko    pts/1    :0     7:31     1:06    0.33s   0.33s   bash
cetko    pts/5    :0     17:23    0.00s   0.32s   0.00s   w
```

root

- Operacijski sustav korisnike identificira preko jedinstvenog identifikatora

  UID (User ID)

- Jedan korisnik se posebno tretira

  root **UID=0**

- **root može sve!**
  - **Nije preporučljivo ulogiravati se i/ili raditi kao root!**
  - Raditi kao običan korisnik pa tek kad je nužno prebaciti se na root korisnika - ako je ikako moguće, kroz `sudo`

sudo

- Sučelje za privremeno dobivanje administrativnih ovlasti
- sudo mogu izvršiti svi korisnici prema dozvolama definiranima u datoteci

  `/etc/sudoers`
- Uređivanje naredbom `visudo`, iz istih razloga kao i `vipw`

```
dino      ALL = (ALL) ALL
dominik   marvin,magrathea = (dino) /bin/dd

%kset     ALL = NOPASSWD: /sbin/umount /media/cdrom0
```

sudo funfacts

- Pokretanjem naredbe `sudo` s flagom `-u` moguće je naredbu izvršiti kao drugi korisnik. Primjerice:
  `$ sudoedit -u www ~www/htdocs/index.html`
  Uredi file kao korisnik `www`
- Analogna operacija je `sudo -g grupa superkulnaredba` koja će pokrenuti naredbu dostupnu korisniku grupe `grupa`

Sudoers sintaksa

Pogledajmo još jednom malo detaljnije primjer iz prethodnog slajda:
`dino ALL = (ALL) ALL`
možemo generalizirati kao:
`User Host = (Runas) Commands`
Gdje unos tumačimo kao: "User may run Command as the Runas user on Host"
Runas opcija govori koji `sudo -u` odnosno `sudo -g` će biti prihvaćeni, a koji odbijeni.

Sudoers Runas

Bitno je napomenuti da trenutna konfiguracija odobrava
`sudo -u dominik naredba1`,
ali ne odobrava `sudo -g nkosl naredba1` gdje je `nkosl` grupa kojoj dominik pripada.
Da bismo to popravili korigiramo naš unos u:
`dino ALL = (ALL:ALL) ALL`
Sada unos tumačimo kao: "User dino može pokretati sve naredbe i kao svaki user i kao svaka grupa"

Sudoers naprednije korištenje

- Ponekad se nalazimo u situaciji gdje bismo rado definirali skup pravila za određen skup korisnika. U takvim slučajevima koristimo varijablu Alias.

```
User_Alias      FULLTIMERS = millert, mikef, dowdy
User_Alias      WEBMASTERS = will, wendy, wim
```

- Fulltimerima bismo željeli dopustiti da rade što god žele bez da ih se pita za password. Webmasterima bismo željeli dopustiti samo da mogu raditi naredbe koje grupa www odobrava, a johnu odobravamo da mijenja lozinke za sve osim za roota

Sudoers rješenje problema

```
# fultimeri mogu pokretati sve,
# sa svih hostova i ne pitam ih za password
FULLTIMERS      ALL=NOPASSWD: ALL
# webmasteri mogu pokretati naredbe kao www
WEBDEVELOPERS ALL=(www) ALL
# john ne moze mijenjati root lozinke
john ALL= /usr/bin/passwd [A-z]*,
                  !/usr/bin/passwd root
```

Grupe (1)

- Korisnici se grupiraju u korisničke grupe
  - Administracija korisnika
  - Dijeljenje podataka
  - Zajedničke dozvole
- Svaki korisnik ima

  Primarnu grupu
  - Zapisana u datoteci `etc/passwd`

  Sekundarne grupe
  - Sve grupe kojima korisnik pripada

Grupe (2)

- Slično kao i za korisnike za grupe se koristi groups baza u datoteci `/etc/group`
- Sadrži jedan zapis po liniji oblika

  Ime grupe:Lozinka:GID:Popis korisnika

  ```
  cdrom:x:24:linux,dominik,dino
  ```

- Grupe također imaju posebnu datoteku za lozinke `/etc/gshadow`
- Operacijski sustav i s grupama radi preko jedinstvenog identifikatora **GID (Group ID)**
- Naredbom `id` saznajemo sve grupe u koje korisnik pripada

  ```
  uid=1000(user) gid=1000(user)
  groups=1000(user),4(adm)...
  ```

- Privremena prijava u druge grupe naredbom `newgrp`

Upravljanje korisnicima

- Osnovne operacije s korisnicima
  - Dodavanje novog korisnika

    `adduser`
  - Promjena lozinke korisnika

    `passwd`
  - Promjena podataka o korisniku

    `usermod`
  - Uklanjanje korisnika

    `deluser`
- Analogne naredbe postoje i za grupe

  `groupadd, groupmod, groupdel`

Mijenjanje korisnika

- Vrlo bitna naredba `su` (engl. *switch user*)
- Dva bitna oblika naredbe
  - `su <korisnicko ime>` - zadržava svojstva okoline (varijable i slično)
  - `su - <korisnicko ime>` - stvara novu okolinu, svojstvenu korisniku
- Bez argumenata mijenja korisnika u `root`

Upravljanje korisnicima

- Stvaranje novog korisnika

```
$ adduser <korisnik>
```

- Dodavanje korisnika postojećoj grupi

```
$ usermod -aG <grupa> <korisnik>
```

ili

```
$ adduser <korisnik> <grupa>
```

- Stvaranje nove grupe

```
$ addgroup <grupa>
```

ili

```
$ adduser --group <grupa>
```

Promjena podataka o korisniku

- Promjena podataka o korisniku
  - Mogu se mjenjati svi podaci

    `usermod <opcije> <username>`
  - Promjena ljuske, opcija `-s <shell>`
  - Promjena matičnog direktorija, opcija `-d <dir>`
- Ljuska korisnika može se promijeniti i naredbom `chsh`
- Naredba `chfn` mijenja dodatne podatke o korisnicima

  Finger podaci - `Info` polje
- Lozinka se mijenja naredbom `passwd`

Upravljanje korisnicima

- Brisanje kreiranog korisnika

```
$ deluser <korisnik>
```

- Brisanje korisnika iz grupe

```
$ deluser <korisnik> <grupa>
```

- Brisanje grupe

```
$ delgroup <grupa>
```

ili

```
$ deluser --group <grupa>
```

Upravljanje korisnicima

- Kod stvaranja korisnika se može definirati lokacija matičnog direktorija i njegovo brisanje zajedno sa korisnikom
- Navedene naredbe su sučelja drugih naredbi

  `adduser` ⇒ `useradd`
  `deluser` ⇒ `userdel`
  `addgroup` ⇒ `groupadd`
  `delgroup` ⇒ `groupdel`

- Sve prethodne akcije se mogu napraviti i navedenim naredbama

Rekapitulacija

- Kreirajte dva usera, test1 i test2.
- Uredite `/etc/sudoers` na način da omogućite useru test1 pokretanje naredbe `touch` kao user test2. Napomena: Naredba `touch` u `/usr/bin/touch`.
- Ulogirajte se kao test1 i provjerite jeste li dobro odradili gore navede korake
- Na kraju izbrišite oba usera

Rekapitulacija - rješenje

- Kreirajte dva usera, test1 i test2.
  `sudo useradd test1 && sudo useradd test2` – potrebno postaviti i passwd za svakog
- Uredite `/etc/sudoers` na način da omogućite useru test1 pokretanje naredbe `touch` kao user test2. Napomena: Naredba `touch` u `/usr/bin/touch`.
  kroz `sudo visudo` dodajemo:
  `test1 ALL=(test2) NOPASSWD: /usr/bin/touch`
- Ulogirajte se kao test1 i provjerite jeste li dobro odradili gore navede korake
  `su test1`
  Primjetite da niste u mogucnosti pokrenuti `sudo -u test1 touch` makar ste ulogirani kao test1
  `sudo userdel -r test1 && sudo userdel -r test2`

Upravljanje korisnicima

- Ako kod stvaranja korisnika nisu definirani parametri, koriste se postavke u `/etc/adduser.conf`
- U matičnom direktoriju se stvaraju predefinirane datoteke
  - Raspored početnih datoteka je definiran u direktoriju `/etc/skel` (engl. *skeleton*)
- Zadatak
  - Proučiti opcije u datoteci `/etc/adduser.conf`
  - Izlistati direktorij `/etc/skel` i matični direktorij

Naredbe

Naredba	Opis
Ctrl+D	odjava iz terminala
logout	odjava iz terminala
who	prikazuje podatke o korisniku
who am i	ispisuje korisnika u trenutnom terminalu
whoami	ispisuje isključivo korisničko ime korisnika u terminalu
finger	ispisuje trenutno aktivne korisnike
su	izmjena korisnika
newgrp	prijava u drugu grupu
usermod	izmjena podataka o korisniku
passwd	promjena korisničke lozinke

Dozvole (1)

- Naredba `ls -l` ispisuje informacije o vlasnicima i dozvolama objekta

```
$ ls -l datoteka.txt
-rw-r--r-- 1 pero users 0 Jan 4 23:19 datoteka.txt
```

- Objekt je vlasništvo korisnika i grupe
  - Drugo polje označava vlasnika - korisnika (`pero`)
  - Treće polje označava vlasnika - grupu (`users`)
- Prvo polje u prvom bitu sadrži oznaku tipa datoteke, a ostalih 9 bitova se nazivaju **mode** objekta

Dozvole (2)

- **mode** definira dozvoljene operacije na svakom objektu
- Devet bitova dijele se u tri grupe od koji svaka čini jedan troznamenkasti binarni broj
- Svaki troznamenkasti binarni broj se može prikazati jednom oktalnom znamenkom
- Svaka oktalna znamenka modea predstavlja skup dozvola koje su dodijeljene sljedećim korisnicima objekta i to:
  - Prva oktalna znamenka definira prava za vlasnika - korisnika **user**
  - Druga oktalna znamenka definira prava za vlasnika - grupu **group**
  - Treća oktalna znamenka definira prava za sve ostale **others**

Dozvole (3)

- Značenja pojedinih bitova svake znamenke
  - r **read** - Dozvoljeno čitanje
  - w **write** - Dozvoljeno pisanje
  - x **execute** - Dozvoljeno izvršavanje / pretraživanje direktorija
- Svaki pojedini bit može biti u stanju
  - **uključen** - operacija dozvoljena
  - **isključen** - operacija zabranjena

- **Primjer 1**

$\texttt{rwxr-xr-x} = 111101101_2 = 755_8$

	r	**w**	**x**
user	+	+	+
group	+	-	+
others	+	-	+

Dozvole (4)

- **Primjer 2**

`rw-r--r--` = 644

	r	w	x
user	+	+	-
group	+	-	-
others	+	-	-

- **Primjer 3**

`r--r--r--` = 444

	r	w	x
user	+	-	-
group	+	-	-
others	+	-	-

Promjena dozvola (1)

- Promjena modea obavlja se naredbom `chmod`

```
chmod <mode> <objekt>
```

- Mode se može zadati oktalno i simbolički
- Moguće jer rekurzivno mijenjati prava

```
chmod -R <mode> <objekt>
```

- **Vlasnik** datoteke može bez obzira na trenutni mod
  - promijeniti mode
  - obrisati datoteku

Promjena dozvola (2)

- **Primjer 4**

```
chmod ugo=rwx file1
```

	r	w	x
user	+	+	+
group	+	+	+
others	+	+	+

  - Alternativno:

```
chmod a=rwx file1
chmod 777 file1
```

- **Primjer 5**

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

ili `chmod 755 file1 file2`

Promjena dozvola (3)

- **Primjer 6**

```
chmod g+w file1 file2 file3
```

	r	w	x
user	*	*	*
group	*	+	*
others	*	*	*

- **Primjer 7**

```
chmod -x file1
```

ili

```
chmod a-x file1
```

	r	w	x
user	*	*	-
group	*	*	-
others	*	*	-

Izvršavanje datoteka

- Svaka datoteka na UNIX sustavu može biti izvršna (*executable*)
- Skripta se, tako, može izvršiti korištenjem zadanog interpretora
- Postavljanjem `x` dozvole svaka se datoteka može izvršiti izravnim pozivanjem

/home/linux/skripta.sh mode 755

```
#!/bin/bash
echo "Skripta je pokrenuta"
```

```
~$ /home/linux/skripta.sh
Skripta je pokrenuta
~$ ./skripta.sh
Skripta je pokrenuta
```

Promjena dozvola (4)

- Naredba `chmod` može prihvatiti poseban argument prilikom simboličkog zadavanja modea

  `X` (veliko X)
  - Direktorijima postavlja `x` dozvolu
  - Ostalim datotekama ne mijenja mod
  - Omogućuje listanje direktorija bez dodavanja dozvole za izvršavanje datoteka
  - Koristan prilikom rekurzivne promjene modea:

    ```
    chmod -R a+X dir1
    ```
  - Ukoliko direktorij nema postavljen execute bit, nije moguć pregled sadržaja

Posebne dozvole (1)

Sticky bit

Sticky bit / Text mode

- **Kod direktorija**

  Dozvoljava brisanje direktorija **samo** vlasniku i root korisniku

- **Kod datoteka**

  Nakon izvršavanja datoteke proces ostaje u memoriji

- Simbolički se označava s velikim `T` na mjestu `x` dozvole za *others* korisnike

```
-rwxr--r-T 1 pero users 0 Jan 4 23:21 datoteka.txt
```

- Ako *others* ujedno ima i `x` dozvolu tada se sticky bit označava s malim `t`
- Danas je sticky bit relevantan samo za direktorije.

Posebne dozvole (2)

SUID i SGID

- Za razumijeti preostala dva posebna bita potrebno je shvatiti što se događa s dozvolama korisnika koji pokreće izvršnu datoteku
- Svaki proces se pokreće s UID i GID primarne grupe korisnika koji ga je pozvao. Pokrenuti proces ima sve ovlasti tog korisnika

Set user ID (SUID) i **Set group ID (SGID)**

- Postavljanjem ovih bitova u mode datoteke proces koji pokreće datoteku dobiva dozvole **vlasnika** - **korisnika** (SUID bit), odnosno **vlasnika** - **grupe** (SGID) izvršne datoteke

Posebne dozvole (3)

SUID i SGID

- Simbolički se označava s velikim `S` na mjestu `x` dozvole za određenu grupu korisnika

```
-rwSr--r-x 1 pero users 0 Jan 4 23:21 datoteka.txt      SUID
-rw-r-Sr-x 1 pero users 0 Jan 4 23:21 datoteka.txt      SGID
```

- Primijetite da SUID, odnosno SGID ne impliciraju `x` dozvolu vlasnicima datoteke. U gornjem primjeru samo *others* imaju pravo izvršiti datoteku i u tom trenutku će isti dobiti prava vlasnika.
- Ako vlasnik, *user* ili *group* ujedno ima i `x` dozvolu tada se posebni bitovi označavaju s malim `s`

Posebne dozvole (4)

Promjena dozvola

- Posebne dozvole se također mijenjaju naredbom `chmod`
- Ispred uobičajene tri znamenke dodaje se još jedna čiji bitovi odgovaraju posebnim dozvolama
  - **Prvi bit** - SUID
  - **Drugi bit** - SGID
  - **Treći bit** - Sticky bit

- **Primjer 8**

```
$ chmod 5754 file1
$ ls -l file1
-rwsr-xr-T 1 pero users 0 Jan 4 23:23 file1
```

  - Alternativno:

```
$ chmod u=rwxs,g=rx,o=rt file1
```

Zadani mode (1)

- Kreiranjem novog objekta on poprima zadani mode
- Definira ga trenutni filesystem i procesi koji kreiraju objekt

- Primjenom **umask** mogu se ograničiti dozvole koje postavljaju nadređeni procesi
- umask ima isti format kao i mode, no s različitim značenjem bitova
  - **1** - Isključuje dozvolu na poziciji bita
  - **0** - Ne mijenja dozvolu koju je postavio nadležni proces

Zadani mode (2)

- Naredbom `umask` se mijenja trenutni umask
  - **Bez argumenata** - ispisuje trenutnu vrijednost u oktalnom obliku
  - **Argument -S** - ispisuje trenutnu vrijednost u simboličkom obliku
  - **Argument 4 oktalne znamenke** - mijenja vrijednost umaska

    Prva oktalna znamenka je za specijalne modove

- U datoteci s popisom montiranih datotečnih sustava, `/etc/fstab` se mogu navesti tri vrste maski
  - **umask** - Odnosi se na sve vrste datoteka
  - **fmask** - Odnosi se na sve regularne datoteke
  - **dmask** - Odnosi se na sve direktorije
- Ove vrste maski se mogu navesti i prilikom korištenja naredbe `mount`

Promjena vlasnika

- Promjena vlasnika objekta obavlja se naredbom `chown`

```
chown <korisnik> <objekt>
```

- Promjena grupe objekta obavlja se naredbom `chgrp`

```
chgrp <grupa> <objekt>
```

ili `chown :<grupa> <objekt>`

- Moguće je istovremeno promijeniti korisnika i grupu

```
$ chown <korisnik>:<grupa> <objekt>
```

```
$ chown <korisnik>:  <objekt>
```

Postavlja korisnika i grupu koja odgovara primarnoj grupi korisnika