

Sudo: najčešća uporaba i konfiguracija



Naredba **sudo** omogućava administratoru sustavu raspodjelu zaduženja, tako što drugim korisnicima omogućava pokretanje određenih naredbi kao 'root' korisnik, a da im pri tome ne mora reći zaporku root korisnika.

Iako je izrazito fleksibilna u definiranju tko i što može izvršiti, uporaba naredbe sudo se obično ograničava na nekolicinu korisnika s dovoljnim znanjem za obavljanje određenih administrativnih zadataka (ili onih zadataka gdje je potrebna samo viša razina ovlasti).

Uporaba naredbe sudo je jednostavna, no prije toga moramo definirati korisnike koji mogu rabiti ovu naredbu. Konfiguracijsku datoteku /etc/sudoers uređujemo pomoću posebne naredbe **visudo**.

VAŽNO: iako se konfiguracijska datoteka /etc/sudoers može editirati i direktno, činite to isključivo preko naredbe 'visudo', koja ujedno vrši i sintaktičku provjeru. Naredba sudo neće raditi ako postoji greška u konfiguraciji, što može dovesti do određenih problema (izgubite administratorski pristup jer se ne sjećate ili nemate rootovu zaporku, primjerice)!

Dakle, dodajmo nekoliko korisnika u datoteku /etc/sudoers:

```
# visudo
root    ALL=(ALL) ALL
pero    ALL=(ALL) ALL
marko   ALL=(ALL) ALL
```

Dodali smo korisnike (root, pero, marko) koji mogu pokrenuti bilo koju naredbu, ali s privilegijama root korisnika. Uporaba je:

```
$ sudo naredba
```

Konkretnije, pretpostavimo da smo korisnik 'marko':

```
marko@stroj$ sudo id
Password: <korisnikova zaporka>
uid=0(root) gid=0(root) groups=0(root)
```

Korisnik mora na naredbenoj liniji otkucati **svoju vlastitu** zaporku, i ta naredba će se izvršiti pod ovlastima root korisnika. To možemo vidjeti iz gornjeg primjera, gdje je uid (user id) jednak nuli, dakle root korisniku.

Ukoliko želite izvršiti još koju naredbu, nećete biti ponovno upitani za zaporku neko vrijeme (15 minuta). Nakon isteka tog vremena, opet će se pojaviti upit o zaporki. Naravno, ovo se događa iz sigurnosnih razloga.

Ukoliko korisnik ne otkuca dobru zaporku, dobit će poruku o grešci:

```
marko@stroj$ sudo vi /etc/postfix/main.cf
We trust you have received the usual lecture from the local System Administrator.
It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
Password: *****
```

```
marko is not in the sudoers file. This incident will be reported.
```

Svi se pokušaji pokretanja naredbe sudo zapisuju u syslog:

```
Mar 27 15:58:33 stroj sudo: marko : TTY=pts/6 ; PWD=/home/marko ;
USER=root ; COMMAND=/usr/bin/vi /etc/postfix/main.cf
Mar 27 22:13:17 stroj sudo: (pam_unix) authentication failure; logname=marko
uid=0 euid=0 tty=pts/6 ruser= rhost= user=marko
```

Ukoliko korisniku želimo ograničiti prava, možemo navesti naredbe koje može pokretati kao root:

```
koordinator ALL = /usr/bin/passwd [A-z]*, !/usr/bin/passwd root, /sbin/reboot
```

Gornji redak omogućuje korisniku 'koordinator' da mijenja zaporku bilo kome osim root korisniku, te da restarta poslužitelj. Druge naredbe ne može izvršavati.

```
webmaster ALL = (www-data) NOPASSWD: ALL
```

Korisniku 'webmaster' gornjim retkom omogućava da izvršava bilo koju naredbu kao korisnik 'www-data', i to tako da ne mora unositi zaporku:

```
webmaster@stroj$ sudo -u www-data vi index.html
www-data@stroj$
```

Kao što smo rekli, svi se pokušaji, i uspješni i neuspješni, zapisuju u syslog. No, možda bi bilo dobro imati te logove izdvojene u posebnu datoteku kako biste lakši mogli nadgledati tko je i kada pokretao naredbu sudo.

Citirat ćemo dio iz manuala za sudoers (man sudoers):

```
logfile      Path to the sudo log file (not the syslog log file).
              Setting a path turns on logging to a file; negating this
              option turns it off.
syslog       Syslog facility if syslog is being used for logging
              (negate to disable syslog logging). Defaults to authpriv.
```

Postupit ćemo po naputku, i u datoteku /etc/sudoers upisati:

```
Defaults:ALL !syslog
Defaults:ALL logfile=/var/log/secure.log
```

Ovo će izgasiti zapisivanje preko sysloga, te zapisivati isključivo u /var/log/secure.log, što može

olakšati administriranje.

Za složenije konfiguracije postoje brojni primjeri u manualu za sudo i sudoers, kao i web stranica projekta na <http://www.sudo.ws> [1].

- [Logirajte](#) [2] se za dodavanje komentara

čet, 2009-04-30 09:10 - Željko BorošKuharice: [Linux](#) [3]

Kategorije: [Software](#) [4]

Vote: 0

No votes yet

Sudo - trikovi i savjeti



U ovoj e-knjizi će se nalaziti članci o naredbi sudo, korisnoj i vrlo upotrebljivoj naredbi. Mogućnosti ove naredbe su brojne, od davanja dijela administratorskih privilegija nekim korisnicima, ili skupinama korisnika, do pokretanja određenih administrativnih naredbi bez kucanja passworda za korisnika root.

U nekim distribucijama je korisnik root izbačen (u smislu da se ne može prijaviti na sustav), te se administrativni zadaci izvršavaju isključivo preko naredbe sudo. Uz pravilnu konfiguraciju naredbe, administracija sustava će sasvim sigurno biti lakša i sigurnija.

- [Logirajte](#) [2] se za dodavanje komentara

Sudo i aliasi



Naredbu sudo koristimo svi, ali većina to čini na najjednostavniji mogući način. I to je

sasvim u redu, pokretati naredbe u privilegiranom načinu rada je za neke svrhe sasvim dovoljno. No, ukoliko ste pokušali ponešto više, mogli ste vidjeti da treba još ponešto naučiti. Konkretno, ne rade aliasi unutar sudo naredbe.

Primjer:

```
$ alias la="ls -al"
$ sudo la
[sudo] password for korisnik:
sudo: la: command not found
```

Ovo se događa zbog načina na koji se obrađuje naredba sudo. Procjenjuje se (evaluira) samo prva naredba radi li se o aliasu, ne i ostatak. Dakle, bash provjerava samo je li sudo alias, ne i je li "la" alias. Kako bi postigli to da bash procjenjuje i ostatak retka kao alias, upotrijebit ćemo mali trik:

```
$ alias sudo="sudo "
```

Dodali smo samo razmak na kraj naredbe sudo. Ovo, po manualu, znači da će ljuska (shell) pokušati protumačiti i ostatak naredbenog retka kao alias. Pogledajmo:

```
$ alias sudo="sudo "
$ sudo la
total 137540
drwxr-xr-x 43 korisnik korisnik      4096 Dec 31 14:16 .
drwxr-xr-x 12 root  root          4096 Mar  9 2012 ..
-rw-r--r--  1 korisnik korisnik      0 Jan 14  2003 .addressbook
...
```

Eto, sada rade aliasi preko naredbe sudo.

No, to nam nije dosta. U .bashrc datoteci u \$HOME direktoriju root korisnika imali smo definiran alias:

```
# alias aa="apt-get -qq update && apt-get -y dist-upgrade"
```

Ovime smo htjeli pojednostaviti redovite nadogradnje samo s naredbom od dva slova. Kada smo u root shellu, ovo radi. No, sudo ne radi, čak i kad upotrijebimo ovaj trik:

```
$ sudo aa
E: Could not open lock file /var/lib/dpkg/lock - open (13: Permission denied)
E: Unable to lock the administration directory (/var/lib/dpkg/), are you root?
```

Ovdje je riječ o pokretanju podljuske (subshella), te se zadnji dio očigledno na izvršava pod ovlastima root korisnika.

Možda se ovo može riješiti na neki drugi način, no nama se učinio najjednostavniji način napraviti skriptu "aa" koja će napraviti isto što i alias i smjestiti je negdje u naš \$HOME direktorij:

```
$ cat $HOME/bin/aa
apt-get -qq update && apt-get -y dist-upgrade
$ sudo aa
[sudo] password for korisnik:
sudo: aa: command not found
```

Zašto bash odjednom ne prepozna naredbu "aa", kad se \$HOME/bin nalazi u \$PATH? Problem leži u činjenici da sudo "čisti" putanju s retkom u konfiguraciji:

```
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
```

(ukoliko ovakav redak nemate, možda nećete ni imati ovaj problem)

Da bi stvar proradila, potrebno je dodati naš direktorij u "secure_path" (**obavezno** radite s naredbom "visudo"):

```
Defaults secure_path="/home/korisnik/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
```

(ekspanzija znaka "~" ne radi, morate navesti punu klasičnu putanju)

Nakon toga je sve u redu:

```
$ sudo aa
[sudo] password for korisnik:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Ovo možda nije najelegantnije rješenje, ali nama radi (TM).

- [Logirajte](#) [2] se za dodavanje komentara

sri, 2014-12-31 14:49 - Petar TalerKuharice: [Linux](#) [3]
[Za sistence](#) [5]

Kategorije: [Operacijski sustavi](#) [6]

Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/564>

Links

[1] <http://www.sudo.ws>

[2] <https://sysportal.carnet.hr/sysportallogin>

[3] <https://sysportal.carnet.hr/taxonomy/term/17>

[4] <https://sysportal.carnet.hr/taxonomy/term/25>
[5] <https://sysportal.carnet.hr/taxonomy/term/22>
[6] <https://sysportal.carnet.hr/taxonomy/term/26>