

EncFS



EncFS omogućava kreiranje virtualnog enkriptiranog datotečnog sustava. Zapravo, ne radi se o pravom datotečnom sustavu, no za svrhu koju mu mislimo namijeniti ovo uopće nije bitno. Bitna je činjenica da EncFS omogućava vrlo jednostavno enkriptiranje vaših podataka (datoteka i direktorija) unutar direktorija kojeg ste sami definirali.

Kao i neki programi za čuvanje zaporki, i EncFS koristi samo jednu. Ne postoji nikakva "**master**", "**sekundarna**" ili "**pomoćna**" zaporka. Ako enkriptirate svoje podatke i zaboravite zaporku, nećete ih više moći dekriptirati, zato oprez. Zaporku je moguće naknadno promijeniti, ako znate postojeću.

EncFS ćemo instalirati na uobičajen način:

```
# apt-get install encfs
...
The following NEW packages will be installed:
  encfs libboost-serialization1.42.0 librlog5
```

Možete instalirati i paket fuse-utils. EncFS radi preko **FUSE**-a, "**Filesystem in USErspace**", sučelja prema kernelu koje omogućuje korisničkim programima korištenje različitih virtualnih datotečnih sustava. Ovo se sve odvija iz korisničkog prostora, "*userspacea*", dakle iz svijeta neprivilegiranih, korisničkih programa.

Kako FUSE mora biti učitani u kernel, upotrijebit ćemo naredbu modprobe:

```
# modprobe fuse
```

Generiranje enkriptiranog direktorija je vrlo jednostavno, potrebno je navesti direktorij i točku montiranja, "*mount-point*" (enkriptirani direktorij i točka montiranja **moraju biti apsolutne staze**). Pogledajmo kako se koristi EncFS:

```
# encfs /root/enkriptirano /root/encfs-mount
The directory "/root/enkriptirano/" does not exist. Should it be created? (y,n)
The directory "/root/encfs-mount" does not exist. Should it be created? (y,n) y
Creating new encrypted volume.
Please choose from one of the following options:
  enter "x" for expert configuration mode,
  enter "p" for pre-configured paranoia mode,
  anything else, or an empty line will select standard mode.
?> p
```

```
Paranoia configuration selected.
```

```
Configuration finished. The filesystem to be created has
the following properties:
Filesystem cipher: "ssl/aes", version 3:0:2
Filename encoding: "nameio/block", version 3:0:1
...
```

Now you will need to enter a password for your filesystem. You will need to remember this password, as there is absolutely no recovery mechanism. However, the password can be changed later using `encfsctl`.

```
New Encfs Password:*****
Verify Encfs Password:*****
```

Nakon kreiranja direktorija i točke montiranja (jednostavno odgovorite "y"), odaberite "paranoičnu" konfiguraciju. Paranoična konfiguracija, za razliku od standardne, uključuje jaču enkripciju, što nam je dovoljno (256-bitni ključ, za razliku od standardnog 192-bitnog ključa). Ekspertni način ostavljam za neku drugu priliku.

Ostaje nam samo prebaciti neke datoteke u direktorij koji nam služi kao točka montiranja. Primjerice, želimo sačuvati i enkriptirati privatni mailbox:

```
# cp mail.private /root/encfs-mount/
# ls -l /root/encfs-mount/
-rw----- 1 root root 887 Apr 11 22:23 mail.private
# ls -l /root/enkriptirano/
-rw----- 1 root root 903 Apr 11 22:23 9TgzxdYbe-E-BAZyy1BR6Pnr
```

U direktoriju koji smo nazvali "enkriptirano" pojavit će se (nešto uvećana) datoteka, s neprepoznatljivim imenom, ali to je uistinu naš mailbox. Ovdje naravno možete smjestiti i druge datoteke i direktorije, koji će svi na isti način biti enkriptirani.

Neki korisnici cijeli svoj direktorij **\$HOME** enkriptiraju na ovakav način, dok neki čuvaju samo određene direktorije (primjerice, `.ssh`). Granica zapravo ne postoji, a recimo da je zanimljiva mogućnost kombinirati ovaj direktorij sa servisom **Dropbox**.

Kada završimo s uređivanjem i dodavanjem datoteka, enkriptirani direktorij možemo odmontirati:

```
# fusermount -u /root/encfs-mount/
# ls -l /root/enkriptirano/
-rw----- 1 root root 903 Apr 11 22:26 9TgzxdYbe-E-BAZyy1BR6Pnr
# ls -l /root/encfs-mount/
#
```

U točki montiranja više nema čitljivih datoteka, sve je ostalo enkriptirano u direktoriju `/root/enkriptirano/`.

Direktorij `/root/encfs-mount/` nakon demontiranja obrišite (ili ćete sljedeći put morati koristiti opciju "nonempty" kod postupka montiranja), ili jednostavno koristite drugu točku montiranja.

Datotečni sustav EncFS će se prikazati kao i svaki drugi montirani datotečni sustav, što možete provjeriti preko naredbe `df`:

```
# df | grep encfs
encfs                9614116    7011544    2504900    74% /root/encfs-mount
```

EncFS mogu, naravno, koristiti i obični korisnici. Sve što je potrebno je dodati ih u grupu "**fuse**":

```
# usermod -a -G fuse korisnik
```

Inače, direktorij se može montirati kao javan (--public). Kada se montira na ovaj način, svi korisnici mogu staviti svoje datoteke u enkriptiran direktorij. No, i nadalje se primjenjuju pravila koja su određena modom direktorija, odnosno datoteka (što određujemo poznatom naredbom "**chmod**"). Možda će većini biti zgodna mogućnost stavljanja sticky bita na enkriptirani direktorij, što će onemogućiti brisanje tuđih datoteka. Alternativno, može se odrediti grupa korisnika koja može koristiti navedeni direktorij. Sve zapravo ovisi o vašim potrebama i željama.

Kreiranje enkriptiranog direktorija s opcijom "--public" je nužno provesti kao korisnik root.

Kao što smo već napomenuli, zaporku enkriptiranog direktorija je moguće promijeniti. Evo kako:

```
# encfsctl passwd /enkriptirani_direktorij
Enter current Encfs password
EncFS Password:*****
Enter new Encfs password
New Encfs Password:*****
Verify Encfs Password:*****
Volume Key successfully updated.
```

Na kraju, spomenut ćemo da postoji još par zanimljivih mogućnosti (koje naravno možete pronaći u man stranicama), a to ostavljamo vama za vježbu (primjerice, može li se enkriptirani direktorij sam odmontirati nakon određenog vremena - može!).

sri, 2013-04-17 01:27 - Marko Jukić **Kuharice:** [Linux](#) [1]

Kategorije: [Software](#) [2]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1249>

Links

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

[2] <https://sysportal.carnet.hr/taxonomy/term/25>