Sifrovani disku v OpenBSD pomoci SOFTRAID(4)

Vložil/a Merlyn [1], 5 Říjen, 2009 - 02:39

- Encryption [2]
- GNU/Linux a BSD [3]

Pro sifrovani disku na OpenBSD sem driv pouzival vnconfig. Ten bohuzel ma spoustu at uz uplne, nebo jenom trochu nevyhod. Jednou z nich je napriklad velikost "disku", ktera je omezena jenom okolo 7.2 GB. Disku pisu v uvozovkach proto, ze se vlastne ani nejedna o disk, ale o sifrovany soubor. Take se pro sifrovani pouziva napevno 128b blowfish. A posledni z nevyhod, ktere zminim je to, ze v GENERIC kernelu je zakompilovana podpora pouze pro ctyri takovato zarizeni. Ale abych jenom nekrivdil, protoze i tento zpusob ma minimalne jednu neoddiskutovatelnou vyhodu - touto je moznost jednoduse presunout soubor kam se nam zachce (nekam na server, na CD), aniz bysme se museli bat, ze kdyz nam na takoveto zalohy nekdo prijde, ze bude mit nase data. Tohle samozrejme jde udelat aj pri pouziti softraid, ale dd z disku uz neni takovy pohodlny jako jenom cp :-)

Na zacatek bych rekl neco o softraid. Pomoci softraid muzeme emulovat raid 0, 1, 4 a 5, ci udelat crypto raid. Standardne se pouziva AES XTS 256, v kodu je podpora i pro AES XTS 128, ale ta je momentalne pristupna pouze editaci zdrojovyho kodu.

V tomto prikladu budu sifrovat 512mB flashdisk.
Pro jednoduche vytvoreni crypto raidu nam bude stacit nekolik zakladnich nastroju. Nejprve se hodi disk, na kterym chcese udelat raid uplne vyprazdnit, a udelat na nem pomoci disklabel disk typu RAID (misto 4.2BSD).

```
# fdisk -e sd1
# disklabel -E sd1
```

A pote prikazem

```
# bioctl -c C -l /dev/sd1a softraid0
```

Budete vyzvani pro zadani Passphare a jeji zopakovani. O Passphare budete pozadani pokazdy (och, jak necekany :-))
Z nej vytvorit zasifrovany disk. Pomoci dmesg se podivejte jaky disk pribyl (a je SR CRYPTO), a s nim uz pak pracujete uplne normalne, takze fdisk, disklabel a mount.

```
# dmesg|tail -2
sd2 at scsibus2 targ 0 lun 0: <OPENBSD, SR CRYPTO, 003> SCSI2 0/direct fixed
sd2: 493MB, 512 bytes/sec, 1011570 sec total
# fdisk -e sd2
# disklabel -E sd2
# newfs /dev/rsd2a
# mount /dev/sd2a /mnt/crypto
```

Pro odpojeni pouzijte umount a

```
# bioctl -d sd2
```

A na zaver se hodi rict, ze CRYPTO raid je stale prohlasovan za experimental a nic nenasvedcuje tomu, ze by se v 4.6 melo neco zmenit. V 4.8 je crypto raid stale povazovan za experimental.

Pro vyznamy jednotlivych prepinacu a vubec samozrejme doporucuju precist aspon softraid(4) a bioctl(8).

URL článku: https://security-portal.cz/clanky/sifrovani-disku-v-openbsd-pomoci-softraid4

Odkazy:
[1] https://security-portal.cz/users/merlyn
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/gnu/linux-bsd