Restart servisa saslauthd obvezan kod promjene korisničke zaporke

Iako inspiracija za najveći broj članaka na Portalu za sistemce potiče upravo od upita koje zaprimamo na sys.help, od sada ćemo neke vaše upite prenositi nešto direktnije. Pod ovim mislimo da ćemo više pažnje posvetiti konkretnom upitu, te tome u čemu je točno problem. Smatramo da se tako može dodatno naučiti, jer promatranjem tuđih "grešaka u koracima" možemo promijeniti vlastiti način razmišljanja i tako spriječiti pojavu sličnih problema na vlastitom terenu.

Prvi slučaj je "klasičan", neki korisnik je svoju zaporku proslijedio spamerima, te je preko SASL-a poslužitelj postao centar za slanje spam poruka. Evo što nam je sistemac poslao o učinjenim koracima nakon što je identificirao korisnika:

```
1. promijenio sam korisniku lozinku za pristup mailu. NIJE POMOGLO
2. zaklju?ao sam korisnikov ra?un (passwd -l username) NIJE POMOGLO
3. preimenovao sam korisnikovo ime (usermod -d "/home/korisnik2" -m -l korisnik2 kori
snik) NIJE POMOGLO

Ne znam što više da poduzmem!? Imate li kakvu ideju da to prekinem.
```

Ono što nije učinio piše na http://sistemac.carnet.hr/node/752 [1], a to je da **nije restartao daemon saslauthd** (ne mislimo da bi trebali zapamtiti sve članke ikad objavljene na portalu, naravno). Zašto je to morao učiniti kada je promijenio korisnikovu zaporku, pa i username? Razlog leži u opciji "**-c**":

```
$ ps -ef |grep saslauthd
root       917     1  0 Apr15 ?        00:00:00 /usr/sbin/saslauthd -a pam -c -m /var
/spool/postfix/var/run/saslauthd -n 5
```

Opcija "-c" znači ovo:

```
 -c      Enable caching of authentication credentials
```

Dakle, saslauthd u memoriji čuva (*kešira*) korisničke podatke, te su ostali zapamćeni podaci za korisnika "korisnik", bez obzira što je promijenjen čak i username. Restart servisa rješava problem, jer se stari podaci brišu:

/etc/init.d/saslauthd restart

Iz ovoga smo naučili da trebamo provjeriti ima li neki servis internu privremenu memoriju, te izbrisati te podatke - što je obično najlakše napraviti restartom servisa.

NADOPUNA: ukoliko rabite autentikaciju korisnika i preko radiusa, ne zaboravite promijeniti i zaporku u LDAP-u, odnosno sustavu AAI@EduHr!

čet, 2015-04-16 15:15 - Podrška za CARNetove sistem-inženjere**Kuharice:** Linux [2]
Kategorije: Servisi [3]
sys.kuharica [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1538?page=0

Links
[1] https://sysportal.carnet.hr./node/752
[2] https://sysportal.carnet.hr./taxonomy/term/17
[3] https://sysportal.carnet.hr./taxonomy/term/28
[4] https://sysportal.carnet.hr./taxonomy/term/69