

Restart servisa nakon nadogradnje biblioteka



Za sigurnost poslužitelja pod Debianom nije dovoljno samo redovito pokretati naredbe "apt-get update && apt-get upgrade". Pri tome ne mislimo na određeno kašnjenje sigurnosnih zakrpi, ili na nešto slično, nego na činjenicu da se moraju restartati svi servisi koji ovise o nadograđenim bibliotekama.

Svježi primjer je **heartbleed**, a još svježiji je **poodle**. Sve dok ne pokrenete ponovo servise koji koriste nadograđene biblioteke, ranjivi ste. U slučaju OpenSSL-a, svakome je bilo jasno da bi trebalo restartati apache poslužitelj, ali OpenSSL koriste i drugi servisi. Sve njih treba zaustaviti i ponovo pokrenuti, ali kako znati koji su to? Uvijek možete restartati cijeli server, ali to znači prekid rada i do desetak minuta, što nije uvijek praktično.

Poslužiti ćemo se skriptom **checkrestart** iz paketa *debian-goodies* (za ovaj paket je jako malo ljudi uopće čulo, a ima toliko zanimljivih alata da mu vrijedi posvetiti poseban članak). Ovako izgleda (skraćeni) izlaz naredbe *checkrestart*:

```
# checkrestart
Found 56 processes using old versions of upgraded files
(23 distinct programs)
(19 distinct packages)
```

```
Of these, 16 seem to contain init scripts which can be used to restart them:
The following packages seem to have init scripts that could be used
to restart them:
```

```
bacula-fd:
    2678    /usr/sbin/bacula-fd
apache2.2-bin:
    1792    /usr/lib/apache2/mpm-prefork/apache2
    1790    /usr/lib/apache2/mpm-prefork/apache2
openssh-client:
    7987    /usr/bin/ssh-agent
    7977    /usr/bin/ssh
vsftpd:
    6546    /usr/sbin/vsftpd
...
```

```
These are the init scripts:
```

```
service bacula-fd restart
service apache2 restart
service ssh restart
service vsftpd restart
...
```

```
These processes do not seem to have an associated init script to restart
them:
```

```
python2.7-minimal:
    4758    /usr/bin/python2.7
perl-base:
    3594    /usr/bin/perl
```

```
mysql-server-core-5.5:
      8459      /usr/sbin/mysqld
```

Skripta prepoznaje procese koje treba restartati i odmah nudi i init skriptu s kojom to možete obaviti (preko naredbe "service"). No, za neke procese ne može pronaći odgovarajuću skriptu jer se naziv procesa razlikuje od naziva init skripte. To ćemo morati riješiti ručno, dok je za prepoznate servise moguće upotrijebiti sljedeće:

```
# checkrestart | grep --null service | xargs -0 sh -c
Stopping Bacula File daemon...: bacula-fd.
Starting Bacula File daemon...: bacula-fd.
Restarting web server: apache2 ... waiting .
Restarting OpenBSD Secure Shell server: sshd.
Stopping FTP server: vsftpd.
...
```

Ukoliko vam se ne da pamtiti ove opcije, možete jednostavno izlaz naredbe grep preumjeriti u datoteku, pa samo napraviti

```
# sh < datoteka.txt
```

Za one procese za koje nisu prepoznate init skripte, morat ćemo to napraviti sami. Najbolje je upotrijebiti naredbu "ps":

```
# ps -ef | grep python
root      3360      1  0 10:01 ?          00:01:14 /usr/bin/python
          /usr/bin/fail2ban-server -b -s /var/run/fail2ban/fail2ban.sock
list      4758      1  0 10:02 ?          00:00:00 /usr/bin/python
          /usr/lib/mailman/bin/mailmanctl -s -q start
...
```

Vidimo da se radi o servisima *fail2ban* i *mailman*, pa ih bez problema možemo restartati s odgovarajućom init skriptom. Identičan je postupak i s ostalim servisima koji su pisani u perlu, rubyju ili nečem trećem.

Ukoliko koristite *monit*, koji se ne starta iz skripte, jednostavno ga ubijte s naredbom kill - proces **init** će ga sam ponovo pokrenuti.

Checkrestart nije savršen (uostalom, o lažnim pozitivima možete pročitati u samoj man stranici), pa nemojte brinuti ako *chekrestart* prijavljuje da servis nije restartan. Ovo se uglavnom odnosi na mysql i programski jezik perl, ali možda će vam se pojaviti i za neke druge servise.

U sljedećoj distribuciji Debiana (Jessie) dolazi nam program inspiriran *checkrestartom*, nazvan *needrestart*. On se može instalirati i na wheezy, ali će nam trebati još i dva dodatna perl modula:

```
# apt-get install libmodule-scandeps-perl libmodule-find-perl
# wget -i http://ftp.hr.debian.org/debian/pool/main/libs/libsort-naturally-
perl/libsort-naturally-perl_1.03-1_all.deb
# wget http://ftp.hr.debian.org/debian/pool/main/n/needrestart/needrestart_1.2-7_all.
deb
```

Ukoliko vam je ovo prekomplikirano, uvijek možete jednostavno restartati poslužitelj, što zapravo i nije loše ukoliko ga dulje vrijeme niste restartali.

Zdravko Rašić

pon, 2014-10-20 07:53 - Zdravko Rašić **Kuharice:** [Linux](#) [1]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/1442>

Links

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