Kako omogućiti pristup MySQL-u preko mreže?

 U Službi za pomoć sistem-inženjerima često znamo dobiti upite kako promijeniti pretpostavljene vrijednosti u određenim servisima. Tako je prije nekog vremena jedan kolega želio otvoriti mrežni port preko kojeg bi mogao pristupiti svom MySQL poslužitelju, no to mu nije uspjelo. Port kojeg treba "osposobiti" je 3306. Taj port je iz sigurnosnih razloga zatvoren, jer je to još jedan način na koji udaljeni napadači mogu pokušati upasti na vaš poslužitelj.

Kao prvo, MySQL u osnovnoj konfiguraciji ne dopušta spajanje preko mrežnog *socketa*, nego isključivo preko Unix *socketa,* odnosno *socketa* na datotečnom sustavu. Da bismo omogućili pristup preko mreže, u konfiguraciji MySQL-a zakomentirajte sljedeće, ako već nije:

```
#skip-networking
```

Ponovo pokrenite mysql poslužitelj u slučaju da ste morali napraviti ovu izmjenu:

```
# /etc/init.d/mysql restart
```

No, to je samo predradnja za omogućavanje mrežne komunikacije. Nadalje je potrebno provjeriti što je upisano u datoteku /etc/hosts.allow (dio paketa **tcpd**):

```
mysqld: .domena.hr 127.0.0.1
```

Ovaj redak govori tcpd-u da dopusti spajanje na MySQL daemon samo računalima iz vaše domene i sa lokalnog poslužitelja. Ako se na MySQL želite spojiti s neke druge mreže, ili od kuće, ovdje možete dodati sva računala i mreže s kojih ćete se spajati, primjerice:

```
mysqld: .domena.hr .domena2.hr posluzitelj.negdje.hr 127.0.0.1 161.53.XXX.YYY
```

Ukoliko je ispred imena ".", smatra se da želite da se cijela poddomena može spajati na MySQL port. Ukoliko točke nema, smatra se da je to FQDN ime računala, i samo s njega će se moći spajati klijenti na MySQL port.

Ukoliko ne postoji redak "mysqld", to znači da je spajanje na MySQL daemon dopušten sa svih računala bilo gdje s Interneta, što naravno nikako nije poželjno. Upišite dakle barem "mysqld: .vasadomena.hr 127.0.0.1", što će omogućiti spajanje samo s lokalnog poslužitelja i vaše domene.

Napomena: pregledajte i datoteku /etc/hosts.deny, ukoliko tamo ima nekih unosa koji počinju sa "mysqld:" to znači da je za navedene domene i računala pristup **zabranjen**.

Zadnje što trebate provjeriti na samom poslužitelju je vatrozid, odnosno je li u vašim **iptables** pravilima propušten port 3306. Ovo ćete najlakše provjeriti tako da se probate spojiti na port 3306 s nekog računala izvan vaše lokalne mreže (možete i od kuće):

$ telnet mysql.domena.hr 3306
Trying 161.53.xxx.yyy...
telnet: Unable to connect to remote host: Connection refused

Ukoliko dobijete poruku poput ove, potrebno je otvoriti port 3306 za pristup izvana. Preporuka je otvoriti port za iste hostove koje ste naveli u /etc/hosts.allow.

Ukoliko i dalje imate problema sa spajanjem, provjerite MySQL-ove tablice s pravima pristupa korisnika i njihovim privilegijama. I ovdje trebate unijeti sve korisnike i računala s kojih se žele spajati (napomena: ovi korisnici u MySQL bazi nemaju nikakve veze s korisnicima na sustavu, nemojte to pobrkati!).

Primjerice, želite dopustiti korisniku "perica" spajanje s računala "perica.domena.hr" (ujedno kreirate tog korisnika):

```
$ mysql --user=root mysql --password
Password: <vaš password za root korisnika u MySQL-u>

mysql> GRANT ALL PRIVILEGES ON baza.* TO 'perica'@'perica.domena.hr'
    ->     IDENTIFIED BY 'neka_zaporka' WITH GRANT OPTION;
```

Gornji redak dopušta spajanje korisniku perica, ali i sva prava nad tablicama u bazi "baza".

Prošli smo ukratko sve korake koje je potrebno učiniti kako bi omogućili spajanje na MySQL s udaljenih mreža. Opet ćemo ponoviti da ovime otvarate više mogućnosti za potencijalnu provalu, ali pažljivim konfiguriranjem i praćenjem možete napraviti istovremeno fleksibilan, ali i siguran sustav. Većina sistem-inženjera vjerojatno ni nema potrebe za ovakvim načinom rada, jer im se svi servisi vrte na istom poslužitelju, ali dobro je znati kako podesiti mrežni način rada u slučaju potrebe.

- Logirajte [1] se za dodavanje komentara

čet, 2010-04-29 15:10 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/739

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/28