

SISTEMI ZA UPRAVLJANJE BAZAMA PODATAKA

---

**SIGURNOST MARIADB BAZE PODATAKA**

Svetlana Mančić 1423

## SIGURNOST BAZE PODATAKA

- ▶ Bezbednosni zahtevi
  - ▶ CIA
- ▶ Bezbednosne pretnje
  - ▶ Man-in-the-Middle, DoS, neovlašćeni pristup, curenje podataka, oštećenje podataka
- ▶ Bezbednosne mere
  - ▶ Firewall, IDS/IPS sistemi, kontrola pristupa, autentifikacija, enkripcija

## KONTROLA PRISTUPA

- ▶ Diskreciona kontrola pristupa
  - ▶ Zasniva se na konceptima prava pristupa i mehanizmima dodele privilegija korisnicima kroz GRANT i REVOKE komande
- ▶ Obavezna kontrola pristupa
  - ▶ Bell-LaPadula model, opisan objektima, subjektima, bezbednosnim klasama i dozvolama
- ▶ Kontrola pristupa bazirana na ulogama
  - ▶ Ulogom se definiše skup privilegija, koje ima korisnik za kog se ona vezuje.

## BEZBEDNOST MARIADB BAZE

- ▶ MariaDB pokreće se od strane mysql korisnika, u grupi mysql.
- ▶ Mariadb-secure-installation
  - ▶ Zabrana udaljenog root pristupa
  - ▶ Brisanje test baze
  - ▶ Brisanje anonimnih korisnika

```
(kali㉿kali)-[/var/lib/mysql]
$ ls -al
total 123352
drwxr-xr-x  6 mysql mysql    4096 Jul 17 13:07 .
drwxr-xr-x 81 root  root    4096 Jun 27 18:28 ..
-rw-rw----  1 mysql mysql 417792 Jul 17 13:07 aria_log.00000001
-rw-rw----  1 mysql mysql   52 Jul 17 13:07 aria_log_control
drwx-----  2 mysql mysql   4096 Jun 28 06:27 db1
-rw-rw----  1 mysql mysql 12288 Jul 17 13:07 ddl_recovery-backup.log
-rw-rw----  1 mysql mysql   9 Jul 17 13:07 ddl_recovery.log
-rw-r--r--  1 root  root     0 Jun 27 18:28 debian-10.11.flag
-rw-rw----  1 mysql mysql   910 Jun 27 18:28 ib_buffer_pool
-rw-rw----  1 mysql mysql 12582912 Jun 27 18:28 ibdata1
-rw-rw----  1 mysql mysql 100663296 Jul 17 13:07 ib_logfile0
-rw-rw----  1 mysql mysql 12582912 Jul 17 13:07 ibtmp1
-rw-rw----  1 mysql mysql     0 Jun 27 18:28 multi-master.info
drwx-----  2 mysql mysql   4096 Jun 27 18:28 mysql
-rw-r--r--  1 root  root     15 Jun 27 18:28 mysql_upgrade_info
drwx-----  2 mysql mysql   4096 Jun 27 18:28 performance_schema
drwx-----  2 mysql mysql  12288 Jun 27 18:28 sys
```

Slika 1. MariaDB datoteke - vlasništvo i dozvole

# SIGURNOST MARIADB BAZE PODATAKA

- ▶ mysql\_native\_password
- ▶ mysql\_old\_password
- ▶ ed25519
- ▶ gssapi
- ▶ pam
- ▶ unix\_socket
- ▶ named\_pipe

```
MariaDB [(none)]> set old_passwords=0;  
Query OK, 0 rows affected (0.000 sec)  
  
MariaDB [(none)]> create user alex identified by 'password';  
Query OK, 0 rows affected (0.004 sec)
```

*Slika 2. mysql\_native\_password auth*

```
MariaDB [(none)]> create user aleks identified via ed25519 using password('password');  
Query OK, 0 rows affected (0.008 sec)
```

*Slika 3. Ed25519 auth*

## PRIVILEGIJE

- ▶ Globalne privilegije
- ▶ Privilegije nad bazom
- ▶ Privilegije nad tabelom
- ▶ Privilegije nad kolonama
- ▶ Privilegije nad funkcijama
- ▶ Privilegije nad procedurama

```
MariaDB [(none)]> grant select on *.* to 'maria';  
Query OK, 0 rows affected (0.003 sec)
```

*Slika 4. Globalne privilegije*

```
MariaDB [(none)]> grant select on db1.* to 'maria';  
Query OK, 0 rows affected (0.002 sec)
```

*Slika 5. Privilegije nad bazom*

```
MariaDB [db1]> grant select,insert,update on db1.user to 'maria';  
Query OK, 0 rows affected (0.002 sec)
```

*Slika 6. Privilegije nad tabelom*

```
MariaDB [db1]> grant select(firstname,lastname,age) on db1.user to 'maria';  
Query OK, 0 rows affected (0.003 sec)
```

*Slika 7. Privilegije nad kolonama*



# KONTROLA PRISTUPA BAZIRANA NA ULOGAMA

```
MariaDB [(none)]> create role admin;  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [(none)]> create role developer;  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [(none)]> create role analyst;  
Query OK, 0 rows affected (0.003 sec)
```

Slika 8. Kreiranje uloga

```
MariaDB [db1]> grant all privileges on db1.* to admin;  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [db1]> grant select,insert,update on db1.user to developer;  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [db1]> grant select on db1.user to analyst;  
Query OK, 0 rows affected (0.003 sec)
```

Slika 9. Dodela privilegija ulogama

```
MariaDB [db1]> grant admin to marija;  
Query OK, 0 rows affected (0.006 sec)  
  
MariaDB [db1]> grant developer to marko;  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [db1]> grant analyst to jovan;  
Query OK, 0 rows affected (0.002 sec)
```

Slika 10. Dodela uloga korisnicima

# KONTROLA PRISTUPA BAZIRANA NA ULOGAMA

```
(kali@kali)-[/var/lib/mysql]
$ mariadb -u marija -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 40
Server version: 10.11.8-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use db1;
ERROR 1044 (42000): Access denied for user 'marija'@'%' to database 'db1'
MariaDB [(none)]> set role analyst;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> use db1;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [db1]> insert into user values ('Stefan',50);
ERROR 1142 (42000): INSERT command denied to user 'marija'@'localhost' for table `db1`.`user`
MariaDB [db1]> select * from user;
+-----+-----+
| name  | age  |
+-----+-----+
| Maria | 20   |
| Jovan | 25   |
| Marko | 35   |
+-----+-----+
3 rows in set (0.001 sec)
```

Slika 11. Demonstracija analyst uloge



# KONTROLA PRISTUPA BAZIRANA NA ULOGAMA

```
MariaDB [db1]> set role developer;
Query OK, 0 rows affected (0.001 sec)

MariaDB [db1]> insert into user values ('Stefan',50);
Query OK, 1 row affected (0.002 sec)

MariaDB [db1]> delete from user where name='Jovan';
ERROR 1142 (42000): DELETE command denied to user 'marija'@'localhost' for table `db1`.`user`

MariaDB [db1]> select * from user;
+-----+-----+
| name | age |
+-----+-----+
| Maria | 20 |
| Jovan | 25 |
| Marko | 35 |
| Stefan | 50 |
+-----+-----+
4 rows in set (0.001 sec)

MariaDB [db1]> select * from cities;
ERROR 1142 (42000): SELECT command denied to user 'marija'@'localhost' for table `db1`.`cities`
```

Slika 12. Demonstracija developer uloge

# KONTROLA PRISTUPA BAZIRANA NA ULOGAMA

```
MariaDB [db1]> set role admin;lient.cnf
Query OK, 0 rows affected (0.001 sec)

MariaDB [db1]> select * from user;
+-----+-----+
| name  | age  |
+-----+-----+
| Maria | 20   |
| Jovan | 25   |
| Marko | 35   |
| Stefan | 50   |
+-----+-----+
4 rows in set (0.001 sec)

MariaDB [db1]> delete from user where name='Jovan';
Query OK, 1 row affected (0.002 sec)

MariaDB [db1]> select * from user;
+-----+-----+
| name  | age  |
+-----+-----+
| Maria | 20   |
| Marko | 35   |
| Stefan | 50   |
+-----+-----+
3 rows in set (0.001 sec)

MariaDB [db1]> select * from cities;
+-----+
| city  |
+-----+
| Nis   |
| Pirot |
| Beograd |
| Kragujevac |
| Leskovac |
+-----+
5 rows in set (0.001 sec)
```

Slika 13. Demonstracija admin uloge

ENKRIPCIJA U TRANZITU

```
(kali@kali)-[/etc/mysql/mariadb.conf.d]
$ tshark -z follow,tcp,ascii,0 -P -r /home/kali/Documents/baze/mariadb.pcap
1 0.000000 192.168.64.4 → 192.168.64.4 MySQL 95 Request Query
2 0.000685 192.168.64.4 → 192.168.64.4 MySQL 251 Response TABULAR Respons
3 0.000724 192.168.64.4 → 192.168.64.4 TCP 72 35460 → 3306 [ACK] Seq=24 A

Follow: tcp,ascii
Filter: tcp.stream eq 0
Node 0: 192.168.64.4:35460
Node 1: 192.168.64.4:3306
23
.....select * from user
179
.....*.def.db1.user.user.name.name .. !.....(....def.db1.user.user.age.
ovan.50.....Maria.20 ...
... ".
```

Slika 14. Neenkriptovan mrežni saobraćaj

```
(kali@kali)-[/etc/mysql]
$ tshark -z follow,tcp,ascii,0 -P -r /home/kali/Documents/baze/mariadb.pcap
1 0.000000 192.168.64.4 → 192.168.64.4 TCP 117 48276 → 3306 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=45 TS
val=772318935 TSecr=772304235 [TCP segment of a reassembled PDU]
2 0.000678 192.168.64.4 → 192.168.64.4 TCP 273 3306 → 48276 [PSH, ACK] Seq=1 Ack=46 Win=512 Len=201
TSval=772318936 TSecr=772318935 [TCP segment of a reassembled PDU]
3 0.000712 192.168.64.4 → 192.168.64.4 TCP 72 48276 → 3306 [ACK] Seq=46 Ack=202 Win=511 Len=0 TSval=
772318936 TSecr=772318936

Follow: tcp,ascii
Filter: tcp.stream eq 0
Node 0: 192.168.64.4:48276
Node 1: 192.168.64.4:3306
45
....(.;.....J..D ... ?..(uR3.....T/\..TT....I..
201
.....i.....) ..T....
..M.4....t.2M..i.L.....CV.z_..W..j`.....# ..s=B0.....C).6.-..x.....P[.....T....zb;G.Y.bp.j ..{A%...c....?.
Y....C.t ... h ... JT&|.....H.1z ... c.: ..XOD*....
```

Slika 17. Enkriptovan mrežni saobraćaj

```
#CA key generating
openssl genrsa 4096 > /etc/mysql/ssl/ca-key.pem /mysql/ssl/
#CA certificate generating
openssl req -new -x509 -nodes -days 365000 \
-key /etc/mysql/ssl/ca-key.pem \root root 4096 Jun 1
-out /etc/mysql/ssl/ca-cert.pem root root 4096 Jun 1
#Server key generating
openssl req -newkey rsa:2048 -days 365000 -nodes \3272 Jun 1
-keyout /etc/mysql/ssl/server-key.pem \t 1704 Jun 1
-out /etc/mysql/ssl/server-req.pem t root 956 Jun 1
openssl rsa -in /etc/mysql/ssl/server-key.pem \t 956 Jun 1
-out /etc/mysql/ssl/server-key.pem
#Signing server certificate
openssl x509 -req -in /etc/mysql/ssl/server-req.pem \
-days 365000 -CA /etc/mysql/ssl/ca-cert.pem \UEST
-CAkey /etc/mysql/ssl/ca-key.pem \TELMAKGA1UEBjMCQ
-set_serial 01 -out /etc/mysql/ssl/server-cert.pem
#Client key generating
openssl req -newkey rsa:2048 -days 365000 -nodes \FbeT0z34Pl
-keyout /etc/mysql/ssl/client-key.pem \Ufr276ddeHVjQ
-out /etc/mysql/ssl/client-req.pem vzj13HSwaEXH-EYH2
openssl rsa -in /etc/mysql/ssl/client-key.pem \pM3EXq4qPcn4
-out /etc/mysql/ssl/client-key.pem AQCbZ4vpGR+GzMct7
#Signing client certificate
openssl x509 -req -in /etc/mysql/ssl/client-req.pem \bUP07v
-days 365000 -CA /etc/mysql/ssl/ca-cert.pem \JvYEbCh
-CAkey /etc/mysql/ssl/ca-key.pem \W11bzPWTq2hjR97q+
-set_serial 01 -out /etc/mysql/ssl/client-cert.pem
#Certificate verification
openssl verify -CAfile /etc/mysql/ssl/ca-cert.pem \
/etc/mysql/ssl/server-cert.pem \ /etc/mysql/ssl/
/etc/mysql/ssl/client-cert.pem
```

Slika 15. Kreiranje sertifikata i ključeva

```
[mariadb] r-key.pem
/server-key.pem
##Data-in-Transit Encryption
ssl-ca=/etc/mysql/ssl/ca-cert.pem
ssl-cert=/etc/mysql/ssl/server-cert.pem
ssl-key=/etc/mysql/ssl/server-key.pem
tls_version=TLSv1.2,TLSv1.3 .pem
```

Slika 16. Konfigurisanje TLS

# ENKRIPCIIJA U MIROVANJU

- ▶ Enkripcija tabela onemogućava pristup podacima, čak iako dođe do krađe fizičkih uređaja na kojima se skladište.
- ▶ Za InnoDB skladište moguća je :
  - ▶ Enkripcija svih prostora tabela
  - ▶ Enkripcija pojedinačnih tabela
  - ▶ Enkripcija svih prostora tabela osim određenih tabela
- ▶ Za upravljanje ključevima koriste se posebni pluginovi:
  - ▶ File Key Management Plugin
  - ▶ AWS Key Management Plugin
  - ▶ Hashicorp Key Management Plugin



# ENKRIPCIJA U MIROVANJU

```
(kali@kali)-[~/Documents/baze]
$ cat generisanje-kljuceva.sh
(echo -n "1;" ; openssl rand -hex 32) | sudo tee -a /etc/mysql/encryption/keyfile
(echo -n "10;" ; openssl rand -hex 32) | sudo tee -a /etc/mysql/encryption/keyfile
```

Slika 18. Generisanje ključeva za enkripciju

```
(kali@kali)-[~/Documents/baze]
$ cat /etc/mysql/encryption/keyfile
1;3cf6b683dfcab700b0a98d3382c7565b17ea4cda2d38c702f9b56760434e7083
10;e50571ee911e69b439cd5a416e1a8cde6a3a869e2ed28e6303234faf6a641da9
```

Slika 19. Sadržaj fajla sa ključevima

```
openssl rand -hex 128 | sudo tee /etc/mysql/encryption/keyfile.key

openssl enc -aes-256-cbc -md sha1 \
  -pass file:/etc/mysql/encryption/keyfile.key \
  -in /etc/mysql/encryption/keyfile \
  -out /etc/mysql/encryption/keyfile.enc
```

Slika 20. Enkripcija fajla sa ključevima

```
[mariadb]

##File Key Management
plugin_load_add = file_key_management
file_key_management_filename = /etc/mysql/encryption/keyfile.enc
file_key_management_filekey = FILE:/etc/mysql/encryption/keyfile.key
file_key_management_encryption_algorithm = aes_ctr

##InnoDB Encryption Setup
innodb_encrypt_tables = ON
innodb_encrypt_log = ON
innodb_encryption_threads = 4
innodb_default_encryption_key_id = 1

##Temp & Log Encryption
encrypt-tmp-disk-tables = 1
encrypt-tmp-files = 1
encrypt_binlog = ON
```

Slika 21. Konfiguracija servera

|  |                     |
|--|---------------------|
| (kali@kali)-[/var/lib/mysql]                 |                     |
| \$ sudo strings ./db1/cities.ibd   head -n 5 |                     |
| Rdcj`e                                       | ERROR 1030 (HY000): |
| jGK  | MariaDB [db1]>      |
| J Z  | ERROR 1030 (HY000): |
| EhRpO_K                                      | MariaDB [db1]>      |
| LWC  | Query OK, 0 row     |

Slika 22. Enkriptovani podaci tabele cities

**HVALA NA PÁŽŇNJI!**