MySQL Security

DOAG Konferenz 2021, virtuell

Oli Sennhauser

Senior Berater, FromDual GmbH

https://www.fromdual.com/presentations

Über FromDual GmbH

www.fromdual.com

Support

Beratung

remote-DBA

Schulung

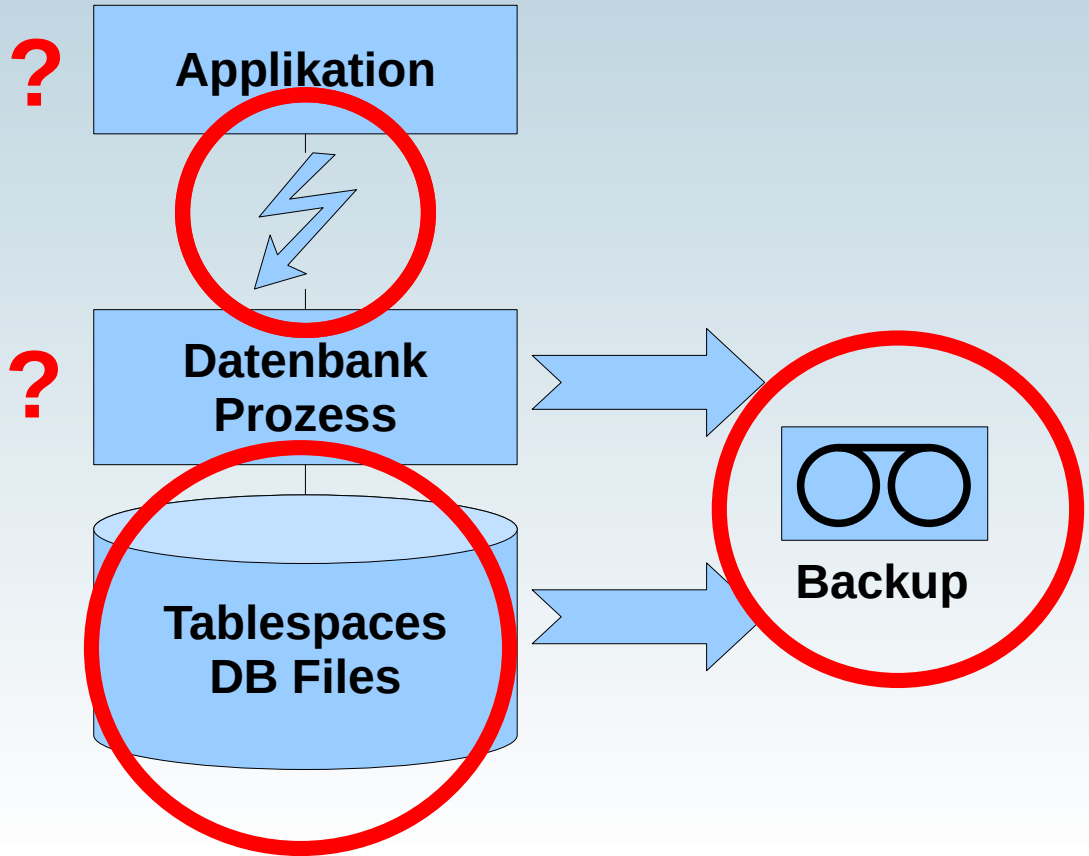
Inhalt

MySQL Security

- Data-in-Transit verschlüsseln (Datenbankverbindung)
- User Management (SSL, etc.)
- Data-at-Rest verschlüsseln (auf Platte)
- Backup verschlüsseln

Allgemeine Übersicht

- Transparent Data Encryption (TDE)
  - Data-in-Transit (DB-Verbindung)
  - Data-at-Rest (Daten auf Platte)



Verbindung verschlüsseln

- **Datenbankverbindung:**

  Client/Applikation → Datenbank
- **MySQL-Protokol: Transport Layer Security (TLS)**
  - **Alte Bezeichnung: Secure Sockets Layer (SSL)**
- **Ablauf:**
  - **TLS Handshake (Schlüsselaustausch und Authentisierung)**
  - **TLS Record (sym. Schlüssel f. Datenübertragung)**
- **Protokoll-Versionen: TLS ~~1.0, 1.1, 1.2~~, 1.3 (2018)**

Server Zertifikate + Schlüssel


```
SQL> ll $datadir/*.pem | grep -v client
-rw------- 1 mysql mysql 1680 Jul  7  2021 ca-key.pem
-rw-r--r-- 1 mysql mysql 1112 Jul  7  2021 ca.pem
-rw------- 1 mysql mysql 1676 Jul  7  2021 private_key.pem
-rw-r--r-- 1 mysql mysql  452 Jul  7  2021 public_key.pem
-rw-r--r-- 1 mysql mysql 1112 Jul  7  2021 server-cert.pem
-rw------- 1 mysql mysql 1680 Jul  7  2021 server-key.pem
```

Important

Generation of certificate files by MySQL helps lower the barrier to using TLS. However, these certificates are self-signed, which is not very secure. After you gain experience using the files generated by MySQL, consider obtaining a CA certificate from a registered certificate authority.

?

```
shell> ./bin/mysql_ssl_rsa_setup --verbose --datadir=/var/lib/mysql
```

Wozu sind die Files da

- Certificate Authority (CA)
  - `ca.pem` - Certificate Authority (CA) Zertifikat
  - `ca-key.pem` - CA privater Schlüssel
- Server
  - `private_key.pem` - Privater Teil des privaten/öffentlichen Schlüsselpaares
  - `public_key.pem` – Öffentlicher Teil des privaten/öffentlichen Schlüsselpaares
  - `server-cert.pem` - Zertifikat des öffentlichen Schlüssels
  - `server-key.pem` - Privater Schlüssel

Server Konfiguration

- In `my.cnf` anpassen:

```
SQL> SHOW GLOBAL VARIABLES LIKE 'ssl%';
+---------------+-----------------------------------------------+
| Variable_name | Value                                         |
+---------------+-----------------------------------------------+
| ssl_ca        | ca.pem                                        |
| ssl_cert      | server-cert.pem                               |
| ssl_cipher    | TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384 |
| ssl_key       | server-key.pem                                |
+---------------+-----------------------------------------------+

SQL> SHOW GLOBAL VARIABLES LIKE 'tls_version%';
+---------------+---------------------------------+
| Variable_name | Value                           |
+---------------+---------------------------------+
| tls_version   | TLSv1,TLSv1.1,TLSv1.2,TLSv1.3 |
+---------------+---------------------------------+
```

TLS/SSL global erzwingen

- **Global auf Server-Ebene**

```
SQL> SHOW GLOBAL VARIABLES LIKE 'require%';
+--------------------------+-------+
| Variable_name            | Value |
+--------------------------+-------+
| require_secure_transport | ON    |
+--------------------------+-------+


shell> mysql -uapp --host=127.0.0.1 --password=secret --ssl-mode=DISABLED
WARNING: no verification of server certificate will be done. Use
--ssl-mode=VERIFY_CA or VERIFY_IDENTITY.
ERROR 3159 (HY000): Connections using insecure transport are prohibited while
--require_secure_transport=ON.

shell> mysql -uapp --host=127.0.0.1 --password=secret --ssl-mode=REQUIRED
OK
```

TLS/SSL erzwingen pro User

- **Auf Account-Ebene**

```
SQL> ALTER USER 'app'@'%' REQUIRE SSL;

SQL> SELECT user, host, ssl_type FROM mysql.user WHERE user='app';
+------+------+----------+
| user | host | ssl_type |
+------+------+----------+
| app  | %    | ANY      |
+------+------+----------+
```

Client Konfiguration


```
SQL> ll client-*.pem
-rw-r--r-- 1 mysql mysql 1112 Jul  7  2019 client-cert.pem
-rw------- 1 mysql mysql 1680 Jul  7  2019 client-key.pem
```

- Client
  - `client-cert.pem` – Zertifikat
  - `client-key.pem` – Privater Schlüssel

```
[client]

ssl-ca      = /home/user/tls/data/ca.pem
ssl-cert    = /home/user/tls/client-cert.pem
ssl-key     = /home/user/tls/client-key.pem
```

Verbindungsstatus prüfen

- **Client-seitig:**

```
SQL> SHOW SESSION STATUS LIKE 'ssl_cipher';
+---------------+-------------------------+
| Variable_name | Value                   |
+---------------+-------------------------+
| Ssl_cipher    | TLS_AES_256_GCM_SHA384 | → otherwise empty string
+---------------+-------------------------+
```

Verbindungsstatus prüfen

- **Server-seitig:**

```
SQL> SELECT processlist_id, processlist_user AS user, processlist_host AS host
     , connection_type, thread_id
  FROM performance_schema.threads
 WHERE type = 'FOREGROUND' AND connection_type IS NOT NULL;
+----------------+------------+-----------+-----------------+-----------+
| processlist_id | user       | host      | connection_type | thread_id |
+----------------+------------+-----------+-----------------+-----------+
|             27 | root       | localhost | Socket          |        66 |
|             32 | app        | localhost | SSL/TLS         |        71 |
|             38 | fpmmm_agent | localhost | TCP/IP          |        77 |
+----------------+------------+-----------+-----------------+-----------+

SQL> SELECT * FROM performance_schema.status_by_thread
 WHERE variable_name ='Ssl_cipher';
+-----------+---------------+------------------------+
| THREAD_ID | VARIABLE_NAME | VARIABLE_VALUE         |
+-----------+---------------+------------------------+
|        66 | Ssl_cipher    |                        |
|        71 | Ssl_cipher    | TLS_AES_256_GCM_SHA384 |
|        77 | Ssl_cipher    |                        |
+-----------+---------------+------------------------+
```

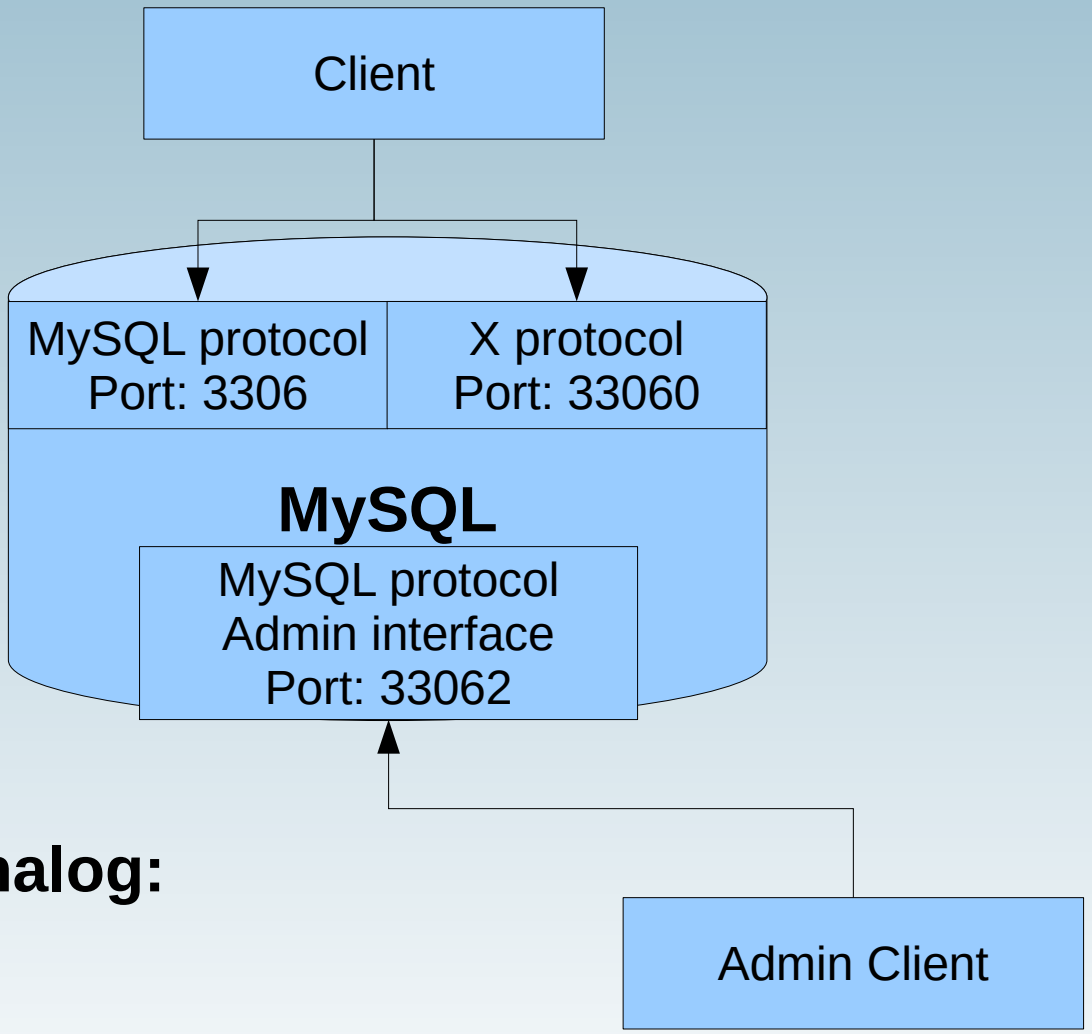
Zertifikats-Ablaufdatum

- **Default: 10 Jahre!**

```
SQL> SHOW GLOBAL STATUS LIKE 'ssl_server_not%';
+-----------------------+---------------------------+
| Variable_name         | Value                     |
+-----------------------+---------------------------+
| Ssl_server_not_after  | Jul  4 17:43:20 2029 GMT |
| Ssl_server_not_before | Jul  7 17:43:20 2019 GMT |
+-----------------------+---------------------------+
```

- **Gehört ins Monitoring! Da denkt in 10 Jahren niemand mehr dran...**

TLS für andere Interfaces



- **Konfiguration analog:**
  - `mysqlx_ssl_…`
  - `admin_ssl_...`

User Management I


```
ALTER USER …
```

- SSL:

```
… REQUIRE {SSL|NONE};
```

- Accounts ablaufen lassen:

```
… PASSWORD EXPIRE {NEVER|INTERVAL n DAY};
```

- Accounts sperren:

```
… ACCOUNT {LOCK|UNLOCK};
```

- Anzahl Verbindungen limitieren

```
… WITH MAX_USER_CONNECTIONS = 50;
```

User Management II


```
ALTER USER …
```

- Passwort History:

```
… PASSWORD HISTORY 6;
```

- Passwort wiederverwenden:

```
… PASSWORD REUSE INTERVAL 180 DAY;
```

- Sperre nach fehlerhaftem Login (2 Tage):

```
… FAILED_LOGIN_ATTEMPTS 3
PASSWORD_LOCK_TIME 2;
```

Data-at-Rest Encryption

- **Was ist das Problem (DB files)?**

```
shell> hexdump -C bank_account.ibd
...
00010060  02 00 1c 69 6e 66 69 6d  75 6d 00 05 00 0b 00 00  |...infimum......|
00010070  73 75 70 72 65 6d 75 6d  0a 00 00 00 10 00 27 00  |supremum......'.|
00010080  00 00 01 00 00 00 01 2f  14 81 00 00 01 37 01 10  |......./.....7..|
00010090  48 61 6e 73 20 4d 65 69  65 72 80 0f 42 40 00 0d  |Hans Meier..B@..|
000100a0  00 00 00 18 00 4e 00 00  00 02 00 00 00 01 2f 15  |.....N........./.|
000100b0  82 00 00 01 07 01 10 46  72 69 74 7a 20 4d c3 bc  |.......Fritz M..|
000100c0  6c 6c 65 72 80 00 30 39  43 07 00 00 00 20 ff a0  |ller..09C.... ..|
000100d0  00 00 00 04 00 00 00 01  2f 1a 81 00 00 01 08 01  |......../.......|
000100e0  10 41 41 41 20 42 42 42  80 01 2a ff 15 07 00 00  |.AAA BBB..*.....|
000100f0  00 28 ff dc 00 00 00 03  00 00 00 01 2f 1b 82 00  |.(........../...|
00010100  00 01 09 01 10 59 59 59  20 5a 5a 5a 80 00 30 39  |.....YYY ZZZ..09|
00010110  43 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |C...............|
...
```

- **Oder «einfach» Files wegkopieren...**

Konzept

- 2 Stufige Verschlüsselung:
  - 1. Tablespace Key (im Tablespace Header)
  - 2. Master Key Ver-/Entschlüssel von TS Key
- Tablespace Key ändert nie
- Master Key ändern → Master Key Rotation
- CE: plugin/component: Keyring File
  - File lokal auf dem Host
- NICHT PCI, FIPS compliant
  - → EE: okv, aws, hashicorp

Keyring Plugin + Functions

- Keyring Plugin

```
[mysqld]

plugin_dir        = /home/mysql/product/mysql-8.0/lib/plugin
keyring_file_data = /home/mysql/database/mysql-80/etc/keyring
early_plugin_load = keyring_file.so
```

- Keyring Funktionen

```
use mysql

INSTALL PLUGIN keyring_udf SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_generate RETURNS INTEGER SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_fetch RETURNS STRING SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_length_fetch RETURNS INTEGER SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_type_fetch RETURNS STRING SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_store RETURNS INTEGER SONAME 'keyring_udf.so';
CREATE FUNCTION keyring_key_remove RETURNS INTEGER SONAME 'keyring_udf.so';
```

Keyring Abfragen


```
SQL> SELECT PLUGIN_NAME, PLUGIN_STATUS
  FROM INFORMATION_SCHEMA.PLUGINS
 WHERE PLUGIN_NAME LIKE 'keyring%';
+--------------+---------------+
| PLUGIN_NAME  | PLUGIN_STATUS |
+--------------+---------------+
| keyring_file | ACTIVE        |
| keyring_udf  | ACTIVE        |
+--------------+---------------+

SQL> SELECT keyring_key_generate('MyKey', 'AES', 32);
1

SQL> SELECT * FROM performance_schema.keyring_keys;
+--------+----------------+----------------+
| KEY_ID | KEY_OWNER      | BACKEND_KEY_ID |
+--------+----------------+----------------+
| MyKey  | root@localhost |                |
+--------+----------------+----------------+

SQL> SELECT keyring_key_type_fetch('MyKey');
AES

SQL> SELECT keyring_key_length_fetch('MyKey');
32
```

Data-at-Rest Encryption

- Welche Dateien?
  - Tablespaces (file-per-table, general, system)
  - REDO logs
  - UNDO logs
  - Binary Logs / Relay Logs
  - Doublewrite (Buffer) Files (automatisch)
  - Temporary Table/Tablespace (nicht implementiert?)
  - InnoDB System Tablespace NICHT supportet!

Ebenen von Verschlüsselung

- **Global:**

```
SQL> SET GLOBAL default_table_encryption = ON;
SQL> SET GLOBAL innodb_redo_log_encrypt = ON;
SQL> SET GLOBAL innodb_undo_log_encrypt = ON;
SQL> SET GLOBAL binlog_encryption = ON;
```

- **Schema (nur default für Tabellen)!:**

```
SQL> CREATE SCHEMA test DEFAULT ENCRYPTION = 'Y';
```

- **Tabelle oder Tablespace:**

```
SQL> ALTER TABLE t1 ENCRYPTION = 'Y';
Query OK, 4 rows affected (1.34 sec)
```

Key rotieren

- **Blockierender Befehl (Lock):**

```
SQL> ALTER INSTANCE ROTATE INNODB MASTER KEY;

SQL> SELECT * FROM performance_schema.keyring_keys;
+------------------------------------------------+----------------+----------------+
| KEY_ID                                         | KEY_OWNER      | BACKEND_KEY_ID |
+------------------------------------------------+----------------+----------------+
| MyKey                                          | root@localhost |                |
| INNODBKey-b5c1ef0b-a0de-11e9-b41a-acfdcee57bd5-1 |                |                |
| INNODBKey-b5c1ef0b-a0de-11e9-b41a-acfdcee57bd5-2 |                |                |
+------------------------------------------------+----------------+----------------+
```

Backup verschlüsseln

- **MySQL Enterprise Backup**

  `--encrypt {--key | --key-file}`

```
shell> mysqldump --all-databases --single-transaction --triggers \
  --routines | openssl enc -aes-256-cbc -k mypass > full_backup.sql.enc

shell> xtrabackup --backup –target-dir=/data/backups \
--encrypt=AES256 {--encrypt-key='...' | --encrypt-key-file=...}
```

Fazit

- **Verschlüsseln (auf Disk) ist NICHT ganz trivial!**
- **Relativ neu**

  → Ausgiebig testen um Stolperfallen und Bugs zu vermeiden.

- **Das ist NICHT mehr KISS!!!**

- **Auch der NSA kann Euch das auf die Schnelle nicht mehr entschlüsseln!**

Q & A

Fragen ?

Diskussion?

Wir haben Zeit für ein persönliches Gespräch...

- **FromDual bietet neutral und unabhängig:**
  - **Beratung**
  - **Remote-DBA**
  - **Support für MariaDB, MySQL und Galera Cluster**
  - **Schulung**

www.fromdual.com/presentations