Using MariaDB and MaxScale to meet GDPR

Maria Luisa Raviol
Senior Sales Engineer- MariaDB
GDPR

A Matter of Balance
GDPR

• It is the harmonization of:
  – **Processes**
    • Process flows
    • Prevention and reaction procedures
  – **Technological solutions**
    • Encryption
    • Preudonymisation
    • Anonymisation
    • Data Accessibility
    • Auditing
  – **Compliance**
    • Keep the pace with the regulation
GDPR - The Requirements

European companies and/or companies located outside EU that handle the data of EU citizens must guarantee:

- Data is protected
- Risk protection and prevention
- The harmonisation of processes and technology
• Companies need to have deep knowledge their Data Supply Chain
• All the W questions need to have an answer
• A top-down approach is usually recommended
GDPR says that:

- It is mandatory to “implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk including inter alia, as appropriate: the \textit{pseudonymisation} and \textit{encryption} of personal data ...”

Reference: GDPR Art 32
GDPR
- The Technology

The right technology will help businesses meet the requirements of GDPR both now and in the future

Must prevent:

- Unauthorised access to the database
- Unauthorised access to all the other database related files (log files, configuration files, passwords...)
- Data integrity breach
- Untrusted access to the database from the Clients
GDPR - The Technology

The right technology will help businesses meet the requirements of GDPR both now and in the future.

How to protect the database:

- Firewalling
- Autentication
- Data in motion encryption
- Tablespace encryption
- Data at rest encryption
- Backup encryption
- Auditing
GDPR - MariaDB Enterprise Security

- Detect and prevent attacks
  - Access management
  - Denial of service
  - SQL Injections
- Protect data at rest with encryption
  - Tablespaces, Individual tables, logs
- TSL/SSL Encryption
  - Protects data in motion
- Auditing for Security and Compliance
- MaxScale database firewall features
- MaxScale selective data masking
MariaDB TX - Security

- **MaxScale**
  - Firewall
  - Data Masking
  - Result Limiting

- **User Limit**
  - Queries / Hours
  - Updates / Hours
  - Connections / Hours
  - Max Connections
  - Max Query Time

- **Encrypted Connections**
  - Client - MaxScale
  - MaxScale - MariaDB
  - Client - MariaDB
  - MariaDB - MariaDB

- **Key Management**
  - AWS KMS
  - eperi GW

- **Authentication**
  - PAM (e.g., LDAP)

- **Authorization**
  - RBAC
  - Syslog

- **Auditing**
  - File

- **Encrypted Storage**
  - Data
  - Logs
  - Backups
MariaDB

Security Features
MariaDB TX - Firewalling and Data Masking
MariaDB MaxScale Concept

**Generic Core**
- Multi-threaded
- E-poll based
- Stateless
- Shares the thread pool

Flexible, easy to write plug-ins for
- Protocol support
- Authentication
- Parsing
- Database monitoring
- Load balancing & routing
- Query transformation & logging

**Insulates client applications from the complexities of backend database cluster**

**Simplify replication from database to other databases**

**Database Servers**

**Slaves**
MaxScale Firewalling - The Details

- A filter installed into the request processing chain.
- Rules define what constitutes a match:
  - wildcard, columns, function, regex, no where clause
  - when to apply
  - what users are affected
  - what statements are affected
- The filter mode defines what to do with a match:
  - allow => whitelist
  - block => blacklist
- `limit_queries` rule sensible only with blacklisting
  - match if more than N queries are made within a time period
MaxScale Filtering Rules

Database Firewall Filter

- Allow/Block queries that MATCH A SET OF RULES
- MATCH RULES FOR SPECIFIED USERS
- MATCH ON
  - date/time
  - a WHERE clause
  - query type
  - column match
  - a wildcard or regular expression or function name

- Protect against SQL injection
- Prevent unauthorized data access
- Prevent data damage

QUERY FAILED: 1141
ERROR: Required WHERE/HAVING clause is missing

DATABASE FIREWALL FILTER

| rule safe_select deny          |
| no_where_clause               |
| on_queries select             |
| rule safe_cust_select deny    |
| regex '.*from.*customers.*'   |
| user %app-user@% match        |
| all rules safe_cust_select    |
| safe_select                   |
MaxScale Security - DDoS Protection

DDoS Protection

**MAXIMUM ROWS FILTER**

- *Return zero rows to client if* number of rows in result set exceeds configured max limit
- *Return zero rows to client if* the size of result set exceeds configured max size in KB

QUERY

1. Clients
2. Database Servers
3. NumRows returned = 1000
4. MaxRowsLimit FILTER
   - Max Rows Limit = 500
   - NumRows Returned > MaxRows Limit
5. QUERY FAILED: 1141
   - ERROR: No rows returned
MaxScale Security - DDoS Protection

- Persistent connections to backend.
  - When server connections are logically closed, keep them in pool for reuse.

  ```
  [SomeServer]
  ...
  maxpersistpoolmax=30
  ```

- Client connection limitation.
  - Specify the maximum number of connections for a particular service.

  ```
  [SomeService]
  ...
  max_connections=100
  ```
MaxScale Security - DDoS Protection

- Cap the amount that can be returned.
  - By rows or by size or both
    
    ```
    [LimitSize]
    type=filter
    module=maxrows
    max_resultset_rows=500
    ```

  - Data will be returned to MaxScale, but MaxScale will not necessarily forward to client.

- Limit rate of queries using the firewall.

```
rule prevent_overload deny limit_queries 15 5 10
```
Security: Data Redaction

Data Redaction via Data Masking

Masking based on column name

- **DATABASE NAME, TABLE NAME CLASSIFIER MAY BE PROVIDED**
  - commerceDb.customerTbl.creditcardNum
  - customerTbl.creditcardNum
  - credicardNum

- **COLUMN CAN BE**
  - Fully or partially masked
  - Obfuscated

HIPPA, PCI and GDPR needs
MariaDB TX

Data in Motion Encryption
MariaDB TX - Data in Motion Encryption

Encrypted Connections

- Client - MaxScale
- MaxScale - MariaDB
- Client - MariaDB
- MariaDB - MariaDB

Key Management

- AWS KMS
- eperi GW

Encrypted Storage

- Data
- Logs
- Backups

Authentication

- PAM (e.g., LDAP)

Authorization

- RBAC

Auditing

- File
- Syslog

User Limit

- Queries / Hours
- Updates / Hours
- Connections / Hours
- Max Connections
- Max Query Time
Client-MaxScale-MariaDB Encryption

**Secured Connection**
- SSL between Clients and MaxScale
- SSL between MaxScale and MariaDB server

**Secured user access**
- LDAP/GSSAPI for secured single sign-on across OS platforms (Windows, Linux), applications and databases
Client-MariaDB and MariaDB-MariaDB Encryption

**Secured Connection**

SSL between Clients and MariaDB

SSL between MariaDB Master and Slaves

**Secured user access**

LDAP/GSSAPI for secured single sign-on across OS platforms (windows, linux), applications and databases
MariaDB TX

Data at Rest

Encryption
MariaDB TX - Data at Rest Encryption
Data-at-rest Encryption

- **Encrypting:**
  - Tables or tablespaces
  - Aria Tables
  - InnoDB Log files
  - Binary/relay Logs
  - Temporary files

- **Independent** of encryption capabilities of applications
- Based on encryption keys, key ids, key rotation and key versioning
- **Low performance** overhead
- **Transparent** to applications
Key Management Services

- Encryption plugin API offers choice
  - Plugin to implement the data encryption
  - Manage encryption Keys

- MariaDB Server options
  - Simple Key Management included
  - Amazon AWS KMS Plugin included
  - Eperi KMS for on premise key management – optional
MariaDB TX

Authentication Plugins
MariaDB TX - Authentication Plugins

- **MaxScale**
  - Firewall
  - Data Masking
  - Result Limiting

- **Encrypted Connections**
  - Client - MaxScale
  - MaxScale - MariaDB
  - Client - MariaDB
  - MariaDB - MariaDB

- **Authentication**
  - PAM (e.g., LDAP)

- **Authorization**
  - RBAC

- **Auditing**
  - File
  - Syslog

- **User Limit**
  - Queries / Hours
  - Updates / Hours
  - Connections / Hours
  - Max Connections
  - Max Query Time

- **Key Management**
  - AWS KMS
  - eperi GW

- **Encrypted Storage**
  - Data
  - Logs
  - Backups
Password Validation

MariaDB comes with two password validation plugins

- **simple_password_check plugin**
  - Can enforce a minimum password length
  - Guarantee that a password contains at least a specified number of upper and lowercase letters, digits, and punctuation characters

- **cracklib_password_check plugin**
  - A widely used library
  - Stop users from choosing easy to guess passwords. It includes checks for not allowing passwords based on the username or a dictionary word etc.
External Authentication

Single Sign On is getting mandatory in most Enterprises.

- **PAM-Authentication Plugin**
  - allows using `/etc/shadow` and any PAM based Authentication like LDAP

- **Kerberos-Authentication**
  - as a standardized network authentication protocol is provided
  - GSSAPI based on UNIX and SSPI based on Windows
MariaDB PAM Authentication

1. Ticket request
2. Service ticket
3. Here is my service ticket, authenticate me
4. Client / server session

GSS-API on Linux
- Red Hat Directory Server
- OpenLDAP

SSPI on Windows
- Active Directory

Ticket request

Service ticket

KDC

Client

MariaDB

Client / server session
MariaDB Role Based Access Control

Role: DBA
Permissions:
- Update Schema
- View Statistics
- Create Database

MariaDB 10
Database
Tables

Role: Developer

Role: Sysadmin
MariaDB TX

Auditing
MariaDB TX - Auditing

- Auditing
  - File
  - Syslog

- Encrypted Connections
  - Client - MaxScale
  - MaxScale - MariaDB
  - Client - MariaDB
  - MariaDB - MariaDB

- Authentication
  - PAM (e.g., LDAP)
  - RBAC

- Authorization
  - RBAC

- Key Management
  - AWS KMS
  - eperi GW

- Encrypted Storage
  - Data
  - Logs
  - Backups

- User Limit
  - Queries / Hours
  - Updates / Hours
  - Connections / Hours
  - Max Connections
  - Max Query Time
Auditing for Security and Compliance

MariaDB Audit Plugin

• Logs server activity
  – Who connected to the server
  – Source of connection
  – Queries executed
  – Tables touched

• File based or syslog based logging
• Monyog Audit log file filtering
MariaDB TX

Per User Limit
MariaDB TX - Per User Limit

- **MaxScale**
  - Firewall
  - Data Masking
  - Result Limiting

- **Encrypted Connections**
  - Client - MaxScale
  - MaxScale - MariaDB
  - Client - MariaDB
  - MariaDB - MariaDB

- **Authentication**
  - PAM (e.g., LDAP)

- **Authorization**
  - RBAC

- **Auditing**
  - File
  - Syslog

- **User Limit**
  - Queries / Hours
  - Updates / Hours
  - Connections / Hours
  - Max Connections
  - Max Query Time

- **Key Management**
  - AWS KMS
  - eperi GW

- **Encrypted Storage**
  - Data
  - Logs
  - Backups
New User Management Functions

- **MAX_*_PER_HOUR**
  - Create_User can limit the number of *queries*, *updates* or *connections* per hour.

- **MAX_USER_CONNECTIONS**
  - limits the number of *simultaneous* connections

- **MAX_STATEMENT_TIME**
  - any query (excluding stored procedures) **taking longer than the value of max_statement_time** (specified in seconds) to execute will be aborted. This can be set globally, by session, as well as per user and per query

- **SHOW CREATE USER**
  - is useful way to see the command required to create a user for auditing or the creation of similar accounts.
New User Management Functions

- Examples:
  - CREATE USER foo2@test IDENTIFIED BY 'password';
  
  CREATE USER 'foo4'@'test'
    REQUIRE ISSUER 'foo_issuer'
    SUBJECT 'foo_subject'
    CIPHER 'text'
  
  CREATE USER foo
    WITH MAX_QUERIES_PER_HOUR 10
    MAX_UPDATES_PER_HOUR 20
    MAX_CONNECTIONS_PER_HOUR 30
    MAX_USER_CONNECTIONS 40;
GRAZIE PER L’ATTENZIONE

Maria Luisa Raviol – Senior Sales Engineer