Implementing Single-Sign-On for MariaDB

Proxy user authentication

About the speaker

IONOS

- Christian Roser
- 36y
- Photography, Guitar, Reptiles
- Working with databases for 10 years
- Responsible for operation of MySQL/MariaDB and PostgreSQL
  - Internal and external
  - 4.6mio
  - > 9k linux servers

IONOS – Your digital partner

Europe's biggest hoster

> 8.9 million
client contracts world wide

35 locations
in 9 countries all over the world

4,000 employees
from 70 nations

> 100,000 server
in use

22 million
managed domains

10 data centers
ISO 27001 certified

Overview IONOS Service Portfolio

From domains, to hosting and e-mail, cloud & office…

IONOS

Broad service portfolio

Domain & SSL	E-Mail & Office	Website Builder	Web Hosting	Cloud & Server

Domain	SSL	E-Mail	Cloud Storage	Website	Shop	Hosting	WP Hosting	Cloud	Server	vServer

Agenda

IONOS

- Scope
- Objective
- Implementation
  - MySQL
  - MariaDB
- Auth_proxy.so
- Conclusion
- Questions

Scope

IONOS

- Shared hosting database infrastructure
  - 4.5Mio customer databases
  - 2.8Mio Queries/s
  - 150GBit/s outgoing traffic
  - 280TB
  - 25k connects/s
  - Fully geo redundant
- MySQL 5.7, 8.0
- MariaDB 10.5, 10.6

Objective

- use cases
  - Passwordless access to database for logged in Customers
  - Access to customer database for technical support
- First Ideas
  - Store the customers cleartext password and use that
    - security
  - Create dedicated users, give permissions
    - Store dedicated user cleartext passwords and use
      - See above
    - Definer: triggers, views, ...
  - ...
  - `PROXY` Privilege

Excursion: PROXY Privilege

IONOS

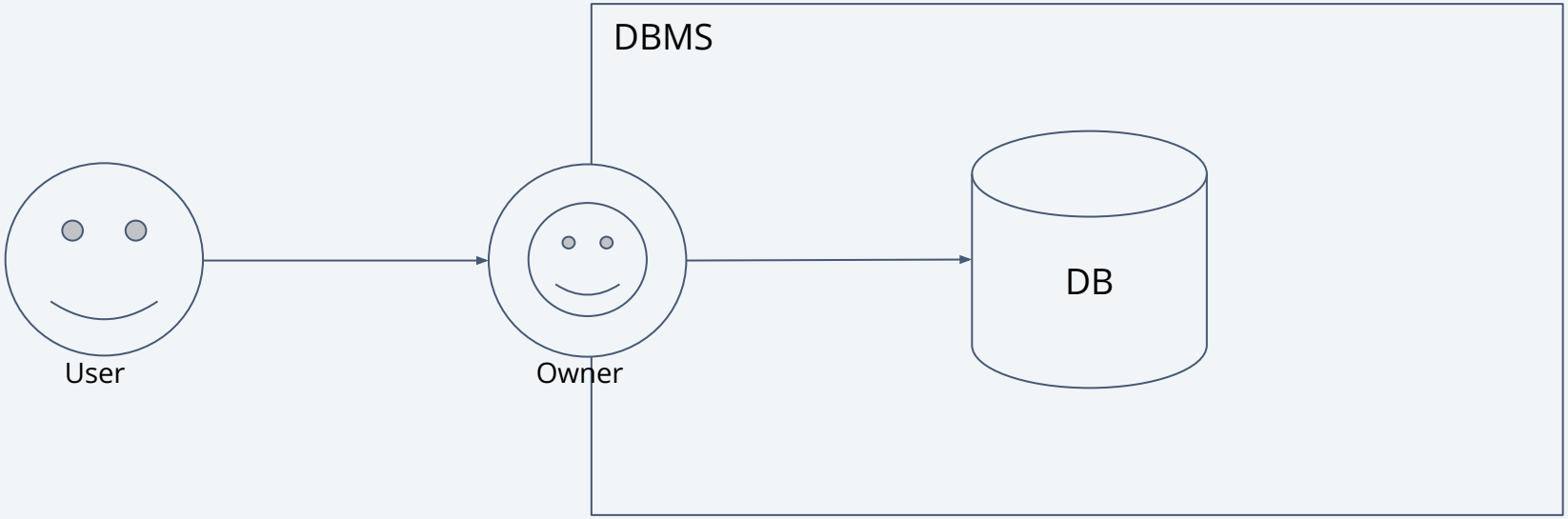
- Allows a user to act as proxy for another user
- Security feature to restrict plugin side user mappings
- Only possible with authentication plugins that support it
  - `mysql_native_password` does not

Implementation

MySQL

- User mapping with `PROXY` privilege
  - Instead of limiting it
- Server support for user mapping
  - `check_proxy_users`, `mysql_native_password_proxy_users` (>= MySQL 5.7)
- Two types of accounts
  - Owner
    - Has all permissions within the database
    - Can be locked
  - User
    - Can have limited lifetime
    - Only allowed to connect to DB and “become” Owner
    - Multiple users can exist (with different credentials)

Implementation



Implementation

SQL

```
-- Owner
CREATE SCHEMA testdb;
CREATE USER IF NOT EXISTS 'owner0815'@'%';
GRANT ALL PRIVILEGES ON `testdb`.* TO 'owner0815'@'%';

-- User
CREATE USER IF NOT EXISTS 'proxy4711'@'%';
GRANT PROXY ON 'owner0815'@'%' TO 'proxy4711'@'%';

mysql@linux:~$ mysql -u proxy4711 testdb

MySQL [(none)]> select user(), current_user();
+------------------+----------------+
| user()           | current_user() |
+------------------+----------------+
| proxy4711@client | owner0815@%    |
+------------------+----------------+
1 row in set (0,001 sec)
```

Implementation

MariaDB

- No such implementation like in MySQL
  - Porting `check_proxy_users` and `mysql_native_password_proxy_users` not planned
- Tested suggested solutions
  - MaxScale
  - Roles
  - Set Multiple passwords per user
  - (sudo concept)
- All tests made didn’t show necessary behaviour

auth_proxy.so

IONOS

- Include in my.cnf
  - `plugin_load = …;auth_proxy.so`
- Almost same user behaviour like on MySQL 5.7 with `check_proxy_users`, `mysql_native_password_proxy_users`
- Implements proxy user mapping from `mysql.proxies_priv` with `mysql_native_password` authentication

auth_proxy.so

SQL

```
-- Owner
GRANT ALL PRIVILEGES ON `testdb`.* TO `owner0815`@`%`;
GRANT USAGE ON *.* TO `owner0815`@`%`;

-- User
GRANT PROXY ON 'owner0815'@'%' TO 'proxy4711'@'%';
GRANT USAGE ON *.* TO `proxy4711`@`%` IDENTIFIED VIA
proxy USING '*D54C8CF5290EDFF3AE9923A0C1F5EA80097221B3'; -- aaaa

mysql@linux:~$ mariadb -u proxy4711 testdb

MariaDB [(none)]> select user(), current_user();
+-------------------+----------------+
| user()            | current_user() |
+-------------------+----------------+
| proxy4711@client | owner0815@%    |
+-------------------+----------------+
1 row in set (0,002 sec)
```

Conclusion

IONOS

- Authentication plugin allowed us to provide MariaDB on shared hosting platform
- Battle tested
  - As of now ~ 750k databases using auth_proxy.so
- Index on `mysql.proxies_priv (user)` might be beneficial
- Migration of 3.5mio MySQL 5.7 databases coming soon

auth_proxy.so

IONOS

... soon to be made available for the community

Questions?

Thank you!