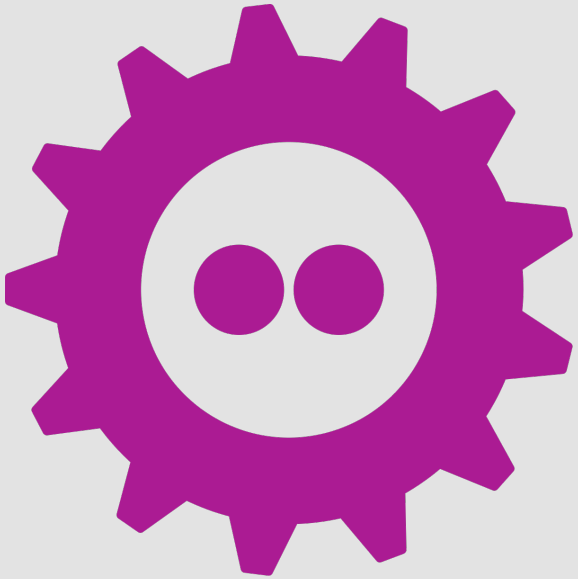
Data-at-Rest-Encryption

Overview



Hrvoje Matijakovic
QA Engineer, Percona

FOSDEM
February 1st, 2020
Brussels, Belgium

PERCONA

Agenda

- Why use Data at Rest Encryption
- What's get written to disk
- What's getting and not getting encrypted
- Key Management
- Backup and restore
- Summary

Data-at-Rest-Encryption?

What?

Why?

What's getting written to disk

- System tablespace
- Undo tablespace
- File-per-table tablespace
- Redo Log
- General tablespaces
- Temporary tablespaces
- Other log files

What's getting written to disk (but not encrypted)

Not getting encrypted:

- Other storage engines: MyRocks/TokuDB/MyISAM [1]
- Slow query log and error log
- Audit log [2]

What's getting written to disk (but not encrypted)

Exceptions

1. Aria in MariaDB (only storage engine, not the logs)
2. Audit log in MySQL 8.0 (E)

Key Management

MariaDB

- File key management plugin
- AWS key management plugin
- Eperi key management plugin [*]

Percona Server

- Keyring file plugin
- Keyring Vault plugin

MySQL

- Keyring file plugin
- Few more but only available for enterprise edition

System tablespace encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015), controlled with **`innodb_encrypt_tables`**
- Available in Percona Server since 5.7.23-24 (currently experimental)
- Controlled by: `innodb_sys_tablespace_encrypt` variable
- Not available in MySQL 5.7

8.0

- Available in Percona Server since 8.0.13 (GA since 8.0.16)
- Not available in MySQL 8.0
- Controlled by: `innodb_sys_tablespace_encrypt` variable

mysql System tablespace encryption

8.0

- Encryption possible in Percona Server since 8.0.13 (GA since 8.0.16)
- Available in MySQL 8.0.16
- Example:

```
ALTER TABLESPACE mysql ENCRYPTION = 'Y';
```

Undo tablespace encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015), controlled by **`innodb_encrypt_log`**
- Available in Percona Server since 5.7.23-24 (currently experimental), controlled by **`innodb_undo_log_encrypt`** variable
- Not available in MySQL 5.7

8.0

- GA in MySQL since 8.0.11 (04/2018)

  GA in Percona Server since 8.0.13-3 (12/2018)
- controlled by **`innodb_undo_log_encrypt`** variable

File-per-table tablespace encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015)
- Available in MySQL 5.7.11 (04/2016)
- Available in Percona Server since 5.7.11 (via upstream merge)
- Example:

```
CREATE TABLE t1 (c1 INT) ENCRYPTION='Y';
```

Redo log encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015), controlled by: `innodb_encrypt_log` variable
- Available in Percona Server 5.7.23-24 (currently experimental) Controlled by: `innodb_redo_log_encrypt` variable
- Not available in MySQL 5.7

8.0

- GA in MySQL 8.0.11 (04/2018)
- GA in Percona Server since 8.0.16-7 (08/2019)
- Controlled by: `innodb_redo_log_encrypt` variable

General tablespaces encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015)
- Available in Percona Server since 5.7.21-21 (GA since 04/2018)
- Not available in MySQL 5.7

8.0

- Available in MySQL since 8.0.13

Temporary tablespaces encryption

5.7

- Available in MariaDB since 10.1 (GA since 10/2015), controlled by: **`encrypt-tmp-disk-tables`** and **`encrypt-tmp-files`**
- Available in Percona Server since 5.7.21-21 (currently experimental)
- Controlled by **`innodb_temp_tablespace_encrypt`** and **`encrypt_tmp_files`**
- Not available in MySQL 5.7

8.0

- GA in Percona Server since 8.0.16-7 (08/2019)
- Not available in MySQL 8.0

PERCONA

Replication: Binary/Relay log encryption

5.7

- In MariaDB GA since 10.1
- In Percona Server GA since 5.7.21-21 (04/2018)
- Not available in MySQL 5.7
- Controlled by: **`encrypt_binlog`** variable

8.0

- Available in MySQL since 8.0.14 (01/2019)
- Percona Server switched to MySQL implementation in Percona Server 8.0.15 (03/2019)
- Controlled by: **`binlog_encryption`** variable

Backups

- Percona XtraBackup
- mariabackup
- mysqldump

Encrypt all the things!

MariaDB 10.4

```
plugin_load_add = file_key_management

file_key_management_filename = /etc/mysql/keys.enc

file_key_management_filekey = FILE:/etc/mysql/.key

file_key_management_encryption_algorithm = aes_cbc

innodb_encrypt_log = ON

innodb_encrypt_tables = FORCE

encrypt_binlog = ON

encrypt_tmp_disk_tables = ON

encrypt_tmp_files = ON

aria_encrypt_tables = ON
```

Encrypt all the things!

Percona Server 8.0

```
vault_url = https://10.10.13.13:8200
secret_mount_point = secret
token = 2bba4fbb-0a09-a114-0e12-10503b42a20b
vault_ca = /secret/ps_keyring_plugins/secret.cer

# Global TS
innodb_encrypt_tables=ON
# System TS
innodb_sys_tablespace_encrypt=ON
# Temp TS and temp files
innodb_temp_tablespace_encrypt=ON
encrypt_tmp_files=ON
# Binary log
binlog_encryption=ON
# Logs
innodb_redo_log_encrypt=ON
innodb_undo_log_encrypt=ON
```

Encrypt all the things!

MySQL 8.0

```
# plugin load

early-plugin-load=keyring_file.so

keyring_file_data=/var/lib/mysql/keyring

# Logs

innodb_redo_log_encrypt=ON

innodb_undo_log_encrypt=ON

# General TS

default_table_encryption=ON

# Binary log

binlog_encryption=ON
```

Summary

encrypted in:	MariaDB 10.4	Percona Server 8.0	MySQL 8.0
System tablespace	Yes	Yes	No
mysql system tablespace	*	Yes	Yes
Undo tablespace	Yes	Yes	Yes
File-per-table tablespace	Yes	Yes	Yes
Redo Log	Yes	Yes	Yes
General tablespaces	Yes	Yes	Yes
Temporary tablespaces	Yes	Yes	No
Other log files	No	No	No
Non-InnoDB data	Aria	No	No
Key Mangement	File, aws kvm, eperi	File, HC Vault	File (5 more as EE)

More information

How Transparent Data Encryption is built in MySQL and Percona Server

Room: UA2.114 (Baudoux) @ **2PM / 14:00**

Resources

- MariaDB Data-at-Rest Encryption Overview
- MySQL InnoDB Data-at-Rest Encryption
- Percona Server Transparent Data Encryption
- Comparing Data At-Rest Encryption Features for MariaDB, MySQL and Percona Server for MySQL
- MySQL Encryption: Talking About Keyrings
- MySQL Encryption: Master Key Encryption in InnoDB
- File Key Management Encryption Plugin
- AWS Key Management Encryption Plugin
- Using Mariabackup with Data-at-Rest Encryption
- Encrypted InnoDB tablespace backups with Percona XtraBackup

Thank you!

About me

- Hrvoje Matijakovic
- QA Engineer at Percona
- @hrvojem
- hrvoje.matijakovic@percona.com


OPEN SOURCE DATABASE CONFERENCE
PERCONA
LIVE
2020
MAY 18 20
AUSTIN, TEXAS
Percona Live is the one and only event where all of the open source database solution companies come together with the community
MySQL, Mongo, Postgres, Elastic, Redis and more
Percona Live brings them to you.
- 3 Days
- Hands-on tutorials,
- Breakout sessions,
- Keynote addresses,
- Expo Hall
- Networking
- Lots of Fun!
Use PRESENTER for 20% off! Register now at perconalive.com

PERCONA