Version : **2022.01**

Dernière mise-à-jour : 2022/11/10 07:16

SER804 - Journalisation et Sécurité

Contenu du Module

Fichiers Logs

Les fichiers journaux du serveur MySQL se trouvent dans le répertoire **/var/lib/mysql/** sauf dans le cas où la configuration dans **/etc/my.cnf** stipule autrement. MariaDB utilise quatre journaux différents :

- Le journal des erreurs (*Error log*),
- Le journal binaire (*Binary Log*),
- Le journal des requêtes lentes (*Slow Query Log*),
- Le journal général (*General Query log*).

Le Journal des Erreurs

Par défaut, seul le journal des erreurs est activé par la directive suivante dans le fichier **/etc/my.cnf** :

```
...
log-error=/var/log/mariadb/mariadb.log
...
```

Le Journal Binaire

Le journal binaire, aussi appelé **binlog**, est chargé de stocker sous format binaire toutes les requêtes qui modifient les objets de la base de données. Il est activé par l'addition de l'option **log-bin** dans le fichier **/etc/my.cnf**. Son fichier d'index est spécifié par l'option **log-bin-index**. Ce fichier contient la liste de tous les fichiers binlogs depuis la dernière purge et permet d'identifier le binlog en cours d'utilisation. Le binlog est l'élément central à la réplication.

Le premier binlog créé est nommé **nom-fichier.000001**. Le passage au binlog suivant, dénommé **nom-fichier.000002** a lieu dans trois cas spécifiques :

- le serveur est redémarré,
- la taille maximale définie par l'option **max_binlog_size** est atteinte,
- la commande **FLUSH LOGS** est exécutée.

Pour purger les anciens binlogs il convient de :

- soit fixer la valeur de l'option **expire_logs_days** dans le fichier **/etc/my.cnf.d/mariadb-server.cnf**,
- soit utiliser la commande **PURGE BINARY LOGS BEFORE** suivi par une date,
- soit utiliser la commande **PURGE BINARY LOGS TO** suivi par un numéro de journal,
- soit supprimer tous les fichiers et repartir d'un fichier .000001 avec la commande **RESET MASTER**.

Le Journal des Requêtes Lentes

Le journal des requêtes lentes permet d'identifier les requêtes lentes. Une fois activé graĉe à l'option **slow_query_log**, toutes les requêtes dépassant la valeur en secondes de l'option **long_query_time** seront consignées. Les informations peuvent être stockées soit dans un fichier spécifié par l'option **slow_query_log_file** soit dans une table dédiée nommée **slow_log** dans le schéma **mysql**. Le choix est fait en éditant l'option **log_output** :

- FILE : les informations sont stockées dans un fichier,
- TABLE : les informations sont stockées dans la table,
- FILE,TABLE : les informations sont stockées dans un fichier **et** dans la table,
- NONE : pas de journalisation.

Par exemple :

```
[mysqld]
...
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
...
```

Par exemple :

```
[root@centos8 ~]# vi /etc/my.cnf.d/mariadb-server.cnf
[root@centos8 ~]# cat /etc/my.cnf.d/mariadb-server.cnf
#
# These groups are read by MariaDB server.
```

```
# Use it for options that only the server (but not clients) should see
#
# See the examples of server my.cnf files in /usr/share/mysql/
#

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
# Settings user and group are ignored when systemd is used.
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mysqld/mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
log-error=/var/log/mariadb/mariadb.log
pid-file=/run/mariadb/mariadb.pid
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2


#
# * Galera-related settings
#
[galera]
# Mandatory settings
#wsrep_on=ON
#wsrep_provider=
#wsrep_cluster_address=
#binlog_format=row
#default_storage_engine=InnoDB
#innodb_autoinc_lock_mode=2
```

```
#
# Allow server to accept connections on all interfaces.
#
#bind-address=0.0.0.0
#
# Optional setting
#wsrep_slave_threads=1
#innodb_flush_log_at_trx_commit=0

# this is only for embedded server
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here
[mariadb]

# This group is only read by MariaDB-10.3 servers.
# If you use the same .cnf file for MariaDB of different versions,
# use this group for options that older servers don't understand
[mariadb-10.3]

[root@centos8 ~]# systemctl restart mariadb
[root@centos8 ~]# systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-11-09 00:34:09 EST; 12s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 25692 ExecStartPost=/usr/libexec/mysql-check-upgrade (code=exited, status=0/SUCCESS)
  Process: 25622 ExecStartPre=/usr/libexec/mysql-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)
  Process: 25594 ExecStartPre=/usr/libexec/mysql-check-socket (code=exited, status=0/SUCCESS)
 Main PID: 25661 (mysqld)
   Status: "Taking your SQL requests now..."
```

```
    Tasks: 30 (limit: 100949)
   Memory: 71.2M
   CGroup: /system.slice/mariadb.service
           └─25661 /usr/libexec/mysqld --basedir=/usr

Nov 09 00:34:09 centos8.ittraining.loc systemd[1]: Starting MariaDB 10.3 database server...
Nov 09 00:34:09 centos8.ittraining.loc mysqld[25661]: 2022-11-09  0:34:09 0 [Note] /usr/libexec/mysqld (mysqld
10.3.28-MariaDB-log) starting as process 25661 ...
Nov 09 00:34:09 centos8.ittraining.loc systemd[1]: Started MariaDB 10.3 database server.
```

L'interrogation de MariaDB démontre la prise en compte des directives :

```
[root@centos8 ~]# mysql -u root -p
Enter password: fenestros
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'slow_query_log%';
+---------------------+--------------------------+
| Variable_name       | Value                    |
+---------------------+--------------------------+
| slow_query_log      | ON                       |
| slow_query_log_file | /var/log/mysql-slow.log |
+---------------------+--------------------------+
2 rows in set (0.001 sec)

MariaDB [(none)]>
```

Il est aussi possible de désactiver et d'activer le journal à chaud :

```
MariaDB [(none)]> SET GLOBAL slow_query_log = 'OFF';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'slow_query_log%';
+---------------------+-------------------------+
| Variable_name       | Value                   |
+---------------------+-------------------------+
| slow_query_log      | OFF                     |
| slow_query_log_file | /var/log/mysql-slow.log |
+---------------------+-------------------------+
2 rows in set (0.000 sec)

MariaDB [(none)]>
```

Important - La valeur par défaut de **long-query-time** est **10** secondes !!. La valeur recommandée est 1 ou 2 secondes.

Le Journal Général

Le journal général permet de consigner les requêtes valides et les informations de connexion/déconnexion des clients. Il n'est pas conseillé d'activer ce journal en production car il crée une surcharge importante. De la même manière que le journal des requêtes lentes, le journal général peut être écrit dans un fichier ou dans une table dénommée **mysql.general_log**. Encore une fois c'est la valeur de la directive **log_output** qui détermine la destination finale :

- FILE : les informations sont stockées dans un fichier,
- TABLE : les informations sont stockées dans la table,
- FILE,TABLE : les informations sont stockées dans un fichier **et** dans la table,
- NONE : pas de journalisation.

```
MariaDB [(none)]> SET GLOBAL general_log = 'ON';
```

```
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
| general_log      | ON          |
| general_log_file | centos8.log |
+------------------+-------------+
2 rows in set (0.000 sec)

MariaDB [(none)]> exit
Bye
[root@centos8 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| Nombres            |
| information_schema |
| ligue1             |
| mysql              |
| performance_schema |
+--------------------+
5 rows in set (0.000 sec)
```

```
MariaDB [(none)]> exit
Bye
[root@centos8 ~]#
```

Consultez maintenant le journal :

```
[root@centos8 ~]# cat /var/lib/mysql/centos8.log
/usr/libexec/mysqld, Version: 10.3.28-MariaDB-log (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command  Argument
221109  0:38:35      8 Query    SHOW GLOBAL VARIABLES LIKE 'general_log%'
221109  0:38:54      8 Quit
221109  0:39:10      9 Connect  root@localhost as anonymous on
                     9 Query    select @@version_comment limit 1
221109  0:39:21      9 Query    SHOW DATABASES
221109  0:39:33      9 Quit
```

Important - Notez la valeur par défaut du nom du fichier **general_log_file**.

En ajoutant la directive **log_output = TABLE** au fichier **/etc/my.cnf.d/mariadb-server.cnf** et en **redémarrant le serveur**, on note que les traces sont maintenant dirigées vers la table **mysql.general_log** au lieu du fichier **/var/lib/mysql/centos8.log** :

```
[root@centos8 ~]# vi /etc/my.cnf.d/mariadb-server.cnf
[root@centos8 ~]# cat /etc/my.cnf.d/mariadb-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# See the examples of server my.cnf files in /usr/share/mysql/
#
```

```
# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
# Settings user and group are ignored when systemd is used.
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mysqld/mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
log-error=/var/log/mariadb/mariadb.log
pid-file=/run/mariadb/mariadb.pid
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
log_output = TABLE



#
# * Galera-related settings
#
[galera]
# Mandatory settings
#wsrep_on=ON
#wsrep_provider=
#wsrep_cluster_address=
#binlog_format=row
#default_storage_engine=InnoDB
#innodb_autoinc_lock_mode=2
#
# Allow server to accept connections on all interfaces.
#
#bind-address=0.0.0.0
```

```
#
# Optional setting
#wsrep_slave_threads=1
#innodb_flush_log_at_trx_commit=0

# this is only for embedded server
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here
[mariadb]

# This group is only read by MariaDB-10.3 servers.
# If you use the same .cnf file for MariaDB of different versions,
# use this group for options that older servers don't understand
[mariadb-10.3]

[root@centos8 ~]# systemctl restart mariadb

[root@centos8 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
```

```
| general_log      | OFF         |
| general_log_file | centos8.log |
+------------------+-------------+
2 rows in set (0.001 sec)

MariaDB [(none)]> SET GLOBAL general_log = 'ON';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
| general_log      | ON          |
| general_log_file | centos8.log |
+------------------+-------------+
2 rows in set (0.107 sec)

MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| Nombres            |
| information_schema |
| ligue1             |
| mysql              |
| performance_schema |
+--------------------+
5 rows in set (0.000 sec)

MariaDB [(none)]> SELECT * FROM mysql.general_log;
+----------------------------+---------------------------+-----------+-----------+--------------+---------------
---------------------------+
| event_time                 | user_host                 | thread_id | server_id | command_type | argument
|
```

```
+----------------------------+----------------------------+-----------+-----------+--------------+---------------
----------------------------+
| 2022-11-09 00:45:01.062906 | root[root] @ localhost [] |         8 |         1 | Query        | SHOW GLOBAL
VARIABLES LIKE 'general_log%' |
| 2022-11-09 00:45:14.114290 | root[root] @ localhost [] |         8 |         1 | Query        | SHOW DATABASES
|
| 2022-11-09 00:45:26.217521 | root[root] @ localhost [] |         8 |         1 | Query        | SELECT * FROM
mysql.general_log           |
+----------------------------+----------------------------+-----------+-----------+--------------+---------------
----------------------------+
3 rows in set (0.000 sec)

MariaDB [(none)]> exit
Bye
[root@centos8 ~]# cat /var/lib/mysql/centos8.log
/usr/libexec/mysqld, Version: 10.3.28-MariaDB-log (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command  Argument
221109  0:38:35      8 Query    SHOW GLOBAL VARIABLES LIKE 'general_log%'
221109  0:38:54      8 Quit
221109  0:39:10      9 Connect  root@localhost as anonymous on
                     9 Query    select @@version_comment limit 1
221109  0:39:21      9 Query    SHOW DATABASES
221109  0:39:33      9 Quit
/usr/libexec/mysqld, Version: 10.3.28-MariaDB-log (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command  Argument
[root@centos8 ~]#
```

Important - Notez que la valeur de la directive **general_log** était **OFF** après le redémarrage du serveur.

Sécurité

Le système de sécurité sous MariaDB se repose sur des **privilèges** qui utilisent trois données:

- Le nom de l'utilisateur
- Le mot de passe de l'utilisateur
- Le nom de l'ordinateur ou l'adresse IP d'où se connecte l'utilisateur

Il est important de noter qu'il n'y a pas de corréspondance entre les noms d'utilisateurs et les mots de passe sous MariaDB et ceux du système d'exploitation.

Les privilèges sont stockées dans cinq tables de la base **mysql**:

- **user**,
  - La table **user** stocke les privilèges globaux des utilisateurs,
- **db**,
  - La table **db** stocke quels utilisateurs peuvent se connecter à partir de quels hôtes sur quelles bases de données,
- **host**,
  - Cette table est un complément de la table précédente. Dans le cas où le champ **host** est laissé en blanc dans la table db, MariaDB cherchera ces informations dans la table **host**,
- **tables_priv**,
  - Cette table stocke des privilèges spécifiques aux tables,
- **columns_priv**,
  - Cette table stocke des privilèges spécifiques aux colonnes.

Privilèges d'Administration

Droit	Description
CREATE TEMPORARY TABLES	Créer des tables temporaires
CREATE USER	Créer, modifier, supprimer des utilisateurs avec les commandes CREATE, DROP et RENAME
FILE	Lire et écrire dans des fichiers sur le serveur avec les commandes SELECT ... INTO OUTFILE, LOAD DATA
GRANT OPTION	Transmettre ses privilèges à un autre utilisateur
LOCK TABLES	Verrouiller des tables

Droit	Description
PROCESS	Voir les threads
PROXY	Activer le mode proxy
RELOAD	Réinitialiser des tables, journaux, statistiques avec les commandes FLUSH et RESET
REPLICATION CLIENT	Superviser la réplication avec les commandes SHOW MASTER STATUS, SHOW SLAVE STATUS
REPLICATION SLAVE	Récupérer les évenements du journal binaire du Maître
SHOW SCHEMAS/DATABASES	Voir la liste des bases de données
SHUTDOWN	Arrêter le serveur avec la commande mysqladmin shutdown
SUPER	Exécuter les commandes CHANGE MASTER TO, KILL, SET GLOBAL etc

Privilèges au Niveau des Schémas

Droit	Description
ALTER	Modifier le schéma et les tables avec les commandes ALTER SCHEMA/DATABASE/TABLE
CREATE	Créer des schémas et des tables avec les commandes CREATE SCHEMA/DATABASE/TABLE
CREATE TEMPORARY TABLE	Créer des tables temporaires
CREATE VIEW	Créer des vues
DELETE	Effacer des enregistrements
DROP	Supprimer des schémas et des tables avec les commandes DROP SCHEMA/DATABASE/TABLE
EVENT	Créer des évènements dans l'ordonnanceur
GRANT OPTION	Transmettre ses privilèges à un autre utilisateur
INDEX	Créer et supprimer des index avec les commandes CREATE/DROP INDEX
INSERT	Insérer des enregistrements dans une table
LOCK TABLES	Verrouiller des tables
SELECT	Afficher des enregistrements d'une table ainsi que la structure de la table avec les commandes SELECT, DESCRIBE, SHOW CREATE TABLE
SHOW VIEW	Voir le code SQL d'une vue avec la commande SHOW CREATE VIEW
UPDATE	Modifier des enregistrements d'une table

Important - Les privilèges liés aux schémas ne prennent effet que lors de la prochaine connexion à ce premier.

Privilèges au Niveau des Tables

Droit	Description
ALTER	Modifier les tables
CREATE	Créer des tables
DELETE	Effacer des enregistrements
DROP	Supprimer des tables
GRANT OPTION	Transmettre ses privilèges à un autre utilisateur
INDEX	Créer et supprimer des index
INSERT	Insérer des enregistrements dans une table
SELECT	Afficher des enregistrements d'une table ainsi que la structure de la table avec les commandes SELECT, DESCRIBE, SHOW CREATE TABLE
TRIGGER	Créer/supprimer des déclencheurs
UPDATE	Modifier des enregistrements d'une table

Important - Les privilèges liés aux tables prennent effet immédiatement.

Privilèges au Niveau des Colonnes

Droit	Description
INSERT	Insérer des enregistrements dans une table
SELECT	Afficher des enregistrements d'une table ainsi que la structure de la table avec les commandes SELECT, DESCRIBE, SHOW CREATE TABLE
UPDATE	Modifier des enregistrements d'une table

Important - Les privilèges liés aux colonnes prennent effet immédiatement.

Privilèges pour les Routines Stockées

Droit	Description
CREATE ROUTINE	Créer des procédures et fonctions stockées
ALTER ROUTINE	Modifier des procédures et fonctions stockées
EXECUTE	Exécuter des procédures et fonctions stockées
GRANT OPTION	Transmettre ses privilèges à un autre utilisateur

Lors de la création d'une routine stockées ou une vue, le créateur peut choisir si la routine ou la vue sera exécuter par la suite avec :

- INVOKER : les droits de l'utilisateur appelant,
- DEFINER : les droits du créateur.

Cette possibilité est donner par l'utilisation de la commande **SQL SECURITY**. Par exemple :

```
> CREATE SQL SECURITY INVOKER VIEW V_EQUIPE AS SELECT id_equipe, nom, stade, ville, points, buts, entraineur FROM equipe; [Entrée]
```

Limitations des Ressources

Droit	Description
MAX_QUERIES_PER_HOUR	Limiter le nombre de requêtes par heure
MAX_UPDATES_PER_HOUR	Limiter le nombre de UPDATE par heure
MAX_CONNECTIONS_PER_HOUR	Limiter le nombre de connexions par heure
MAX_USER_CONNECTIONS	Limiter le nombre de connexions simultanées

La table user

```
[root@centos7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
```

```
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE mysql;
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 [mysql]>
```

Visualisez la table user:

```
MariaDB [mysql]> DESCRIBE user;
+------------------------+-----------------------------------+------+-----+----------+-------+
| Field                  | Type                              | Null | Key | Default  | Extra |
+------------------------+-----------------------------------+------+-----+----------+-------+
| Host                   | char(60)                          | NO   | PRI |          |       |
| User                   | char(80)                          | NO   | PRI |          |       |
| Password               | char(41)                          | NO   |     |          |       |
| Select_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Insert_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Update_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Delete_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Create_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Drop_priv              | enum('N','Y')                     | NO   |     | N        |       |
| Reload_priv            | enum('N','Y')                     | NO   |     | N        |       |
| Shutdown_priv          | enum('N','Y')                     | NO   |     | N        |       |
| Process_priv           | enum('N','Y')                     | NO   |     | N        |       |
| File_priv              | enum('N','Y')                     | NO   |     | N        |       |
| Grant_priv             | enum('N','Y')                     | NO   |     | N        |       |
| References_priv        | enum('N','Y')                     | NO   |     | N        |       |
```

```
| Index_priv              | enum('N','Y')                          | NO   |     | N          |         |
| Alter_priv              | enum('N','Y')                          | NO   |     | N          |         |
| Show_db_priv            | enum('N','Y')                          | NO   |     | N          |         |
| Super_priv              | enum('N','Y')                          | NO   |     | N          |         |
| Create_tmp_table_priv   | enum('N','Y')                          | NO   |     | N          |         |
| Lock_tables_priv        | enum('N','Y')                          | NO   |     | N          |         |
| Execute_priv            | enum('N','Y')                          | NO   |     | N          |         |
| Repl_slave_priv         | enum('N','Y')                          | NO   |     | N          |         |
| Repl_client_priv        | enum('N','Y')                          | NO   |     | N          |         |
| Create_view_priv        | enum('N','Y')                          | NO   |     | N          |         |
| Show_view_priv          | enum('N','Y')                          | NO   |     | N          |         |
| Create_routine_priv     | enum('N','Y')                          | NO   |     | N          |         |
| Alter_routine_priv      | enum('N','Y')                          | NO   |     | N          |         |
| Create_user_priv        | enum('N','Y')                          | NO   |     | N          |         |
| Event_priv              | enum('N','Y')                          | NO   |     | N          |         |
| Trigger_priv            | enum('N','Y')                          | NO   |     | N          |         |
| Create_tablespace_priv  | enum('N','Y')                          | NO   |     | N          |         |
| Delete_history_priv     | enum('N','Y')                          | NO   |     | N          |         |
| ssl_type                | enum('','ANY','X509','SPECIFIED')      | NO   |     |            |         |
| ssl_cipher              | blob                                   | NO   |     | NULL       |         |
| x509_issuer             | blob                                   | NO   |     | NULL       |         |
| x509_subject            | blob                                   | NO   |     | NULL       |         |
| max_questions           | int(11) unsigned                       | NO   |     | 0          |         |
| max_updates             | int(11) unsigned                       | NO   |     | 0          |         |
| max_connections         | int(11) unsigned                       | NO   |     | 0          |         |
| max_user_connections    | int(11)                                | NO   |     | 0          |         |
| plugin                  | char(64)                               | NO   |     |            |         |
| authentication_string   | text                                   | NO   |     | NULL       |         |
| password_expired        | enum('N','Y')                          | NO   |     | N          |         |
| is_role                 | enum('N','Y')                          | NO   |     | N          |         |
| default_role            | char(80)                               | NO   |     |            |         |
| max_statement_time      | decimal(12,6)                          | NO   |     | 0.000000   |         |
+-------------------------+----------------------------------------+------+-----+------------+---------+
47 rows in set (0.001 sec)
```

```
MariaDB [mysql]>
```

Notez la longueur des champs **User** et **Host** :

Champs	Longueur
Host	60
User	80

Mots de Passe

Les mots de passe sous MariaDB sont hachés avant d'être stockés. Le type de hachage a été modifié à partir de la version 4.1.1 de MySQL. Cet ancien type de hachage est pourtant toujours disponible avec la fonction **old_password** :

```
MariaDB [mysql]> SELECT password('root');
+-------------------------------------------+
| password('root')                          |
+-------------------------------------------+
| *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B |
+-------------------------------------------+
1 row in set (0.000 sec)

MariaDB [mysql]> SELECT old_password('root');
+----------------------+
| old_password('root') |
+----------------------+
| 67457e226a1a15bd     |
+----------------------+
1 row in set (0.000 sec)

MariaDB [mysql]>
```

MariaDB utilise des Plug-ins d'authentification. La méthode d'authentification par défaut est implémenté par le plug-in **mysql-native-password** :

```
MariaDB [mysql]> SHOW PLUGINS;
+------------------------------+----------+--------------------+---------+---------+
| Name                         | Status   | Type               | Library | License |
+------------------------------+----------+--------------------+---------+---------+
| binlog                       | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| mysql_native_password        | ACTIVE   | AUTHENTICATION     | NULL    | GPL     |
| mysql_old_password           | ACTIVE   | AUTHENTICATION     | NULL    | GPL     |
| wsrep                        | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| CSV                          | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| MEMORY                       | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| MyISAM                       | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| MRG_MyISAM                   | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| CLIENT_STATISTICS            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INDEX_STATISTICS             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| TABLE_STATISTICS             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| USER_STATISTICS              | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| SQL_SEQUENCE                 | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| ARCHIVE                      | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| BLACKHOLE                    | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| FEDERATED                    | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| InnoDB                       | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| INNODB_TRX                   | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_LOCKS                 | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_LOCK_WAITS            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMP                   | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMP_RESET             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMPMEM                | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMPMEM_RESET          | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMP_PER_INDEX         | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_CMP_PER_INDEX_RESET   | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_BUFFER_PAGE           | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_BUFFER_PAGE_LRU       | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_BUFFER_POOL_STATS     | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_METRICS               | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
```

```
| INNODB_FT_DEFAULT_STOPWORD    | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_FT_DELETED             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_FT_BEING_DELETED       | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_FT_CONFIG              | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_FT_INDEX_CACHE         | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_FT_INDEX_TABLE         | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_TABLES             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_TABLESTATS         | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_INDEXES            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_COLUMNS            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_FIELDS             | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_FOREIGN            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_FOREIGN_COLS       | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_TABLESPACES        | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_DATAFILES          | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_VIRTUAL            | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_MUTEXES                | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_SYS_SEMAPHORE_WAITS    | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| INNODB_TABLESPACES_ENCRYPTION | ACTIVE   | INFORMATION SCHEMA | NULL    | BSD     |
| INNODB_TABLESPACES_SCRUBBING  | ACTIVE   | INFORMATION SCHEMA | NULL    | BSD     |
| Aria                          | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| PERFORMANCE_SCHEMA            | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| SEQUENCE                      | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| FEEDBACK                      | DISABLED | INFORMATION SCHEMA | NULL    | GPL     |
| user_variables                | ACTIVE   | INFORMATION SCHEMA | NULL    | GPL     |
| partition                     | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
+-------------------------------+----------+--------------------+---------+---------+
56 rows in set (0.001 sec)

MariaDB [mysql]> exit
Bye
```

Important - Le plug-in **mysql_old_password** implémente l'ancien type de hachage. Les

modifications des mots de passe ne prennent effet que lors de la connexion suivante du l'utilisateur. MariaDB propose 5 types de hachage : crc32, MD5, SHA1, PASSWORD et OLD_PASSWORD. Les algorithmes PASSWORD et OLD_PASSWORD de MariaDB sont internes à MariaDB.

Veuillez noter que toutes les requêtes saisies sont journalisées dans votre fichier historique de MariaDB. Par défaut ce fichier est **~/.mysql_history**. Les mots de passe saisis sont en clair :

```
[root@centos8 ~]# tail .mysql_history
SELECT user, host, password FROM user;
DESCRIBE user;
SELECT password('root');
SELECT old_password('root');
SHOW PLUGINS;
FLUSH PRIVILEGES;
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('fenestros');
use mysql;
update user set password=PASSWORD("mysql") where User='root';
flush privileges;
```

Il convient donc de protéger ce fichier !

Important - Pour ne pas garder trace de l'historique, il est pratique courante de créer un lien symbolique vers /dev/null : # ls -s /dev/null $HOME/.mysql_history

La connexion

Lors de la connexion d'un utilisateur, MariaDB utilise les trois champs **User**, **Password** et **Host**. MariaDB trie la table ainsi obtenue du privilège le plus

restrictif au privilège le moins restrictif.

La table suivante:

```
+-------+-------------------------+-------------------------------------------+
| user  | host                    | password                                  |
+-------+-------------------------+-------------------------------------------+
| root  | localhost               | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| root  | centos8.ittraining.loc |                                           |
| root  | 127.0.0.1               |                                           |
| root  | ::1                     |                                           |
| user1 | localhost               | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-------+-------------------------+-------------------------------------------+
```

est vue par MariaDB ainsi:

```
+-------+-----------------------+-------------------------------------------+
| user  | host                  | password                                  |
+-------+-----------------------+-------------------------------------------+
| root  | 127.0.0.1             |                                           |
| root  | ::1                   |                                           |
| root  | localhost             | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| user1 | localhost             | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
| root  | centos8.fenestros.loc |                                           |
+-------+-----------------------+-------------------------------------------+
```

Prenons le cas d'une connexion de root à partir du localhost. Dans ce cas, MariaDB commence par rechercher l'hôte **localhost**. Deux lignes correspondent:

```
...
| root  | localhost             | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| user1 | localhost             | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
...
```

MariaDB recherche ensuite le nom de l'utilisateur, dans notre cas **root**. Une ligne correspond:

```
...
| root  | localhost             | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
...
```

MariaDB compare ensuite le mot de passe saisi par root avec le mot de passe crypté dans la table. Dans le cas où les deux mots de passe sont équivalents, l'accès est accordé. Dans le cas contraire, l'accès est refusé.

La commande GRANT

La commande **GRANT** permet de:

- créer un utilisateur,
- accorder des privilèges à cet utilisateur.

La commande prend la forme suivante:

```
mysql> GRANT privileges [columns] ON objet TO utilisateur [IDENTIFIED BY 'password'] [WITH GRANT OPTION];
[Entrée]
```

où:

- **privilèges** est une liste de privilèges séparés par des virgules,
  - les privilèges sont **all, all privileges, alter, create, create temporary tables, delete, drop, execute, file, index, insert, lock tables, process, references, reload, select, show databases, shutdown, super, update, usage, create user, create view, show view, create routine, alter routine**,
  - dans le cas où le privilège est **usage**, l'utilisateur est seulement créé, sans privilèges supplémentaires. Autrement dit ce privilège donne le droit de se connecter à MariaDB,
- **[columns]** est optionnel. Cette directive permet de spécifier que les privilèges portent sur une ou plusieurs colonnes, séparées par des virgules, de la table spécifiée par **objet**,
- **objet** est une base ou une table
- **WITH GRANT OPTION** donne le droit à l'utilisateur de donner ses propres privilèges à un autre utilisateur.

Saisissez la commande suivante pour créer un nouvel utilisateur:

```
[root@centos8 ~]# mysql -uroot -p
Enter password: fenestros
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE mysql;
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 [mysql]> GRANT usage ON *.* TO user2@localhost IDENTIFIED BY 'motdepasse';
Query OK, 0 rows affected (0.00 sec)

MariaDB [mysql]>
```

Important - La **portée des droits *.*** implique tous les objets. La portée des droits peut également être de type **schema.***, autrement dit tous les objets d'une base ou de type **schema.table** pour une table précise.

Vous pouvez aussi utiliser * qui implique tous les objets de la base courante dans le cas où la commande **USE** a été utilisée.

Vérifiez que l'utilisateur a bien été créé :

```
MariaDB [mysql]> SELECT host, user, password FROM user;
+-----------------------+-------+-------------------------------------------+
| host                  | user  | password                                  |
+-----------------------+-------+-------------------------------------------+
| localhost             | root  | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| centos8.fenestros.loc | root  |                                           |
| 127.0.0.1             | root  |                                           |
| ::1                   | root  |                                           |
| localhost             | user1 | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
| localhost             | user2 | *1F48A8CB9F3BAAE4504A9A4549B0AA290BD4E27B |
+-----------------------+-------+-------------------------------------------+
6 rows in set (0.00 sec)

MariaDB [mysql]> exit
bye
```

Connectez-vous maintenant à MariaDB avec le compte d'user2 :

```
[root@centos8 ~]# mysql -uuser2 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
```

```
1 row in set (0.000 sec)

MariaDB [(none)]> USE mysql;
ERROR 1044 (42000): Access denied for user 'user2'@'localhost' to database 'mysql'
MariaDB [(none)]> exit
Bye
```

Notez que l'utilisateur **user2** n'a pas accès aux bases de données ! En effet, il ne peut que se connecter à MariaDB.

La commande REVOKE

La commande REVOKE est utilisée pour retirer les privilèges. La commande REVOKE ne permet **pas** de supprimer l'utilisateur. Pour supprimer un utilisateur, il convient d'utiliser la commande SQL **DELETE**.

La commande REVOKE prend la forme suivante:

```
MariaDB [(none)]> REVOKE privileges [columns] ON objet FROM utilisateur; [Entrée]
```

Par exemple pour retirer les privilèges de l'utilisateur **user2**, connectez-vous à mysql en tant que **root** et saisissez la commande suivante:

```
MariaDB [(none)]> REVOKE all ON *.* FROM user2@localhost; [Entrée]
```

Notez l'utilisation du mot clef **all** pour enlever tous les privilèges.

Modifier le mot de passe d'un utilisateur

Pour modifier le mot de passe d'un utilisateur, trois commandes SQL existent.

En utilisant **SET PASSWORD** :

```
MariaDB [(none)]> SET PASSWORD FOR utilisateur@host=PASSWORD('nouveau_mot_de_passe'); [Entrée]
```

Notez l'utilisation de la directive **PASSWORD()** pour encrypter le mot de passe.

En utilisant **GRANT** :

```
MariaDB [(none)]> GRANT usage ON *.* TO utilisateur@host IDENTIFIED BY 'nouveau_mot_de_passe'; [Entrée]
```

En utilisant **UPDATE USER** :

```
MariaDB [(none)]> UPDATE user SET PASSWORD=PASSWORD('nouveau_mot_de_passe') WHERE user='utilisateur' AND
host='host'; [Entrée]
```

Important - N'oubliez pas qu'après chaque modification, vous devez utiliser la commande **FLUSH PRIVILEGES**.

A Faire : Utilisez **SET PASSWORD** et **UPDATE USER** à tour de rôle pour modifier le mot de passe de l'utilisateur **user2** et connectez-vous après chaque modification pour vérifier que cette dernière a été réussie,

Sécuriser l'échange de données

Pour vérifier si votre instance de MariaDB peut fonctionner avec **openssl**, il convient de saisir la commande suivante:

```
[root@centos8 ~]# mysql -uroot -p
Enter password: fenestros
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 10.3.28-MariaDB-log MariaDB Server
```

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW VARIABLES LIKE 'have_openssl';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| have_openssl  | YES   |
+---------------+-------+
1 row in set (0.001 sec)

MariaDB [(none)]> exit
Bye
```

votre instance de MariaDB peut accepter des connexions sécurisées. Si la variable **have_openssl** indique **DISABLED**, cela signifie que le support est disponible mais non activé :

Openssl

Lors de l'installation du paquet **openssl**, une clef privée et un certificat d'exemple ont été générés dans le répertoire **/etc/pki** :

```
[root@centos8 ~]# ls -lR /etc/pki | more
/etc/pki:
total 0
drwxr-xr-x. 4 root   root    73 Jun 16  2021 ca-trust
drwxr-xr-x. 2 root   root     6 Jun 29  2021 consumer
drwxr-xr-x. 2 root   root     6 Jun 29  2021 entitlement
drwxr-xr-x. 2 root   root   111 Jul 19  2021 fwupd
drwxr-xr-x. 2 root   root   111 Jul 19  2021 fwupd-metadata
drwxr-xr-x. 2 root   root    21 Jun 16  2021 java
drwxr-xr-x. 2 root   root   103 Jun 16  2021 nssdb
drwxrwx---. 2 pesign pesign  54 Jul 19  2021 pesign
```

```
drwxrwxr-x. 2 pesign pesign  54 Jul 19  2021 pesign-rh-test
drwxr-xr-x. 2 root   root     6 Jun 16  2021 product
drwxr-xr-x. 2 root   root     6 Jun 16  2021 product-default
drwxr-xr-x. 2 root   root    73 Jun 16  2021 rpm-gpg
drwx------. 2 root   root     6 Jun  1  2021 rsyslog
drwxr-xr-x. 5 root   root   104 Jun 16  2021 tls

/etc/pki/ca-trust:
total 8
-rw-r--r--. 1 root root 980 Aug 11  2020 ca-legacy.conf
drwxr-xr-x. 6 root root  70 Jun 16  2021 extracted
-rw-r--r--. 1 root root 166 Aug 11  2020 README
drwxr-xr-x. 4 root root  80 Jun 16  2021 source

/etc/pki/ca-trust/extracted:
total 4
drwxr-xr-x. 2 root root  39 Jun 16  2021 edk2
drwxr-xr-x. 2 root root  35 Jun 16  2021 java
drwxr-xr-x. 2 root root  47 Jun 16  2021 openssl
drwxr-xr-x. 2 root root 101 Jun 16  2021 pem
-rw-r--r--. 1 root root 560 Aug 11  2020 README

/etc/pki/ca-trust/extracted/edk2:
total 160
-r--r--r--. 1 root root 156842 Jun 16  2021 cacerts.bin
-rw-r--r--. 1 root root    566 Aug 11  2020 README

/etc/pki/ca-trust/extracted/java:
total 160
-r--r--r--. 1 root root 157499 Jun 16  2021 cacerts
-rw-r--r--. 1 root root    726 Aug 11  2020 README

/etc/pki/ca-trust/extracted/openssl:
total 248
```

```
-r--r--r--. 1 root root 249827 Jun 16  2021 ca-bundle.trust.crt
-rw-r--r--. 1 root root    787 Aug 11  2020 README

/etc/pki/ca-trust/extracted/pem:
total 376
-r--r--r--. 1 root root 163655 Jun 16  2021 email-ca-bundle.pem
-r--r--r--. 1 root root      0 Jun 16  2021 objsign-ca-bundle.pem
-rw-r--r--. 1 root root    898 Aug 11  2020 README
-r--r--r--. 1 root root 216090 Jun 16  2021 tls-ca-bundle.pem

/etc/pki/ca-trust/source:
total 4
drwxr-xr-x. 2 root root   6 Aug 11  2020 anchors
drwxr-xr-x. 2 root root   6 Aug 11  2020 blacklist
--More--
[q]
```

Activer SSL

Pour configurer MariaDB pour SSL, il convient d'abord d'arrêter le service :

```
[root@centos8 ~]# systemctl stop mariadb
```

Dans cet exemple, vous allez créer vos propres clefs et certificats. Commencez par créer une cléf :

```
[root@centos8 ~]# mkdir /etc/pki/mysql
[root@centos8 ~]# cd /etc/pki/mysql/
[root@centos8 mysql]# openssl genrsa 2048 > ca-key.pem
Generating RSA private key, 2048 bit long modulus (2 primes)
...+++++
.....+++++
e is 65537 (0x010001)
```

Créez ensuite le fichier ca-cert.pem :

```
[root@centos8 mysql]# openssl req -new -x509 -nodes -days 1000 -key ca-key.pem > ca-cert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LIMITED
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []:centos8.ittraining.loc
Email Address []:infos@i2tch.co.uk
[root@centos8 mysql]#
```

Créer ensuite le CSR du serveur :

```
[root@centos8 mysql]# openssl req -newkey rsa:2048 -days 1000 -nodes -keyout server-key.pem > server-req.pem
Ignoring -days; not generating a certificate
Generating a RSA private key
......+++++
....+++++
writing new private key to 'server-key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LIMITED
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []:server8.ittraining.loc
Email Address []:infos@i2tch.loc

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@centos8 mysql]#
```

Créer ensuite le certificat du serveur :

```
[root@centos8 mysql]# openssl x509 -req -in server-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
Signature ok
subject=C = GB, ST = SURREY, L = ADDLESTONE, O = I2TCH LIMITED, OU = TRAINING, CN = server8.ittraining.loc,
emailAddress = infos@i2tch.loc
Getting CA Private Key
[root@centos8 mysql]#
```

Créer maintenant le certificat du client:

```
[root@centos8 mysql]# openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client-key.pem > client-req.pem
Ignoring -days; not generating a certificate
Generating a RSA private key
..........................+++++
..+++++
writing new private key to 'client-key.pem'
-----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:IDF
Locality Name (eg, city) [Default City]:PARIS
Organization Name (eg, company) [Default Company Ltd]:I2TCH EUROPE
Organizational Unit Name (eg, section) []:FORMATION
Common Name (eg, your name or your server's hostname) []:centos8.ittraining.loc
Email Address []:infos@i2tch.eu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

[root@centos8 mysql]# ls -l
total 28
-rw-r--r--. 1 root root 1497 Nov  9 01:41 ca-cert.pem
-rw-r--r--. 1 root root 1675 Nov  9 01:37 ca-key.pem
-rw-------. 1 root root 1704 Nov  9 01:46 client-key.pem
-rw-r--r--. 1 root root 1070 Nov  9 01:47 client-req.pem
-rw-r--r--. 1 root root 1346 Nov  9 01:45 server-cert.pem
-rw-------. 1 root root 1704 Nov  9 01:42 server-key.pem
-rw-r--r--. 1 root root 1082 Nov  9 01:44 server-req.pem

[root@centos8 mysql]# openssl x509 -req -in client-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > client-cert.pem
Signature ok
subject=C = FR, ST = IDF, L = PARIS, O = I2TCH EUROPE, OU = FORMATION, CN = centos8.ittraining.loc, emailAddress
```

```
= infos@i2tch.eu
Getting CA Private Key
```

Vérifiez ensuite vos certificats :

```
[root@centos8 mysql]# openssl verify -CAfile ca-cert.pem server-cert.pem client-cert.pem
server-cert.pem: OK
client-cert.pem: OK
```

Modifiez le propriétaire de tous les fichiers dans le répertoire **/etc/pki/mysql** :

```
[root@centos8 mysql]# chown -R mysql:mysql /etc/pki/mysql
```

Modifiez votre fichier **/etc/my.cnf.d/mariadb-server.cnf** :

```
[root@centos8 mysql]# vi /etc/my.cnf.d/mariadb-server.cnf
[root@centos8 mysql]# cat /etc/my.cnf.d/mariadb-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# See the examples of server my.cnf files in /usr/share/mysql/
#

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
# Settings user and group are ignored when systemd is used.
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mysqld/mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd
[mysqld]
datadir=/var/lib/mysql
```

```
socket=/var/lib/mysql/mysql.sock
log-error=/var/log/mariadb/mariadb.log
pid-file=/run/mariadb/mariadb.pid
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
log_output = TABLE

ssl-ca=/etc/pki/mysql/ca-cert.pem
ssl-cert=/etc/pki/mysql/server-cert.pem
ssl-key=/etc/pki/mysql/server-key.pem



#
# * Galera-related settings
#
[galera]
# Mandatory settings
#wsrep_on=ON
#wsrep_provider=
#wsrep_cluster_address=
#binlog_format=row
#default_storage_engine=InnoDB
#innodb_autoinc_lock_mode=2
#
# Allow server to accept connections on all interfaces.
#
#bind-address=0.0.0.0
#
# Optional setting
#wsrep_slave_threads=1
#innodb_flush_log_at_trx_commit=0

# this is only for embedded server
```

```
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here
[mariadb]

# This group is only read by MariaDB-10.3 servers.
# If you use the same .cnf file for MariaDB of different versions,
# use this group for options that older servers don't understand
[mariadb-10.3]
```

Modifiez votre fichier **/etc/my.cnf.d/client.cnf** :

```
[root@centos8 mysql]# vi /etc/my.cnf.d/client.cnf
[root@centos8 mysql]# cat /etc/my.cnf.d/client.cnf
#
# These two groups are read by the client library
# Use it for options that affect all clients, but not the server
#


[client]

ssl-ca=/etc/pki/mysql/ca-cert.pem
ssl-cert=/etc/pki/mysql/client-cert.pem
ssl-key=/etc/pki/mysql/client-key.pem

# This group is not read by mysql client library,
# If you use the same .cnf file for MySQL and MariaDB,
# use it for MariaDB-only client options
[client-mariadb]
```

Démarrez votre serveur MariaDB :

```
[root@centos8 mysql]# systemctl start mariadb
[root@centos8 mysql]# systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-11-09 02:06:20 EST; 11s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 27397 ExecStartPost=/usr/libexec/mysql-check-upgrade (code=exited, status=0/SUCCESS)
  Process: 27326 ExecStartPre=/usr/libexec/mysql-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)
  Process: 27301 ExecStartPre=/usr/libexec/mysql-check-socket (code=exited, status=0/SUCCESS)
 Main PID: 27366 (mysqld)
   Status: "Taking your SQL requests now..."
    Tasks: 30 (limit: 100949)
   Memory: 71.8M
   CGroup: /system.slice/mariadb.service
           └─27366 /usr/libexec/mysqld --basedir=/usr

Nov 09 02:06:20 centos8.ittraining.loc systemd[1]: Starting MariaDB 10.3 database server...
Nov 09 02:06:20 centos8.ittraining.loc mysql-prepare-db-dir[27326]: Database MariaDB is probably initialized in
/var/lib/mysql already, nothing is done.
Nov 09 02:06:20 centos8.ittraining.loc mysql-prepare-db-dir[27326]: If this is not the case, make sure the
/var/lib/mysql is empty before running mysql-prepare-db-dir.
Nov 09 02:06:20 centos8.ittraining.loc mysqld[27366]: 2022-11-09  2:06:20 0 [Note] /usr/libexec/mysqld (mysqld
10.3.28-MariaDB-log) starting as process 27366 ...
Nov 09 02:06:20 centos8.ittraining.loc mysqld[27366]: 2022-11-09  2:06:20 0 [Warning] Although a path was
specified for the --log-slow-queries option, log tables are used. To enable logging to files use the -->
Nov 09 02:06:20 centos8.ittraining.loc systemd[1]: Started MariaDB 10.3 database server.
```

Vérifiez que MariaDB fonctionne en mode SSL :

```
[root@centos8 mysql]# mysql -u root -p
Enter password: fenestros
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
```

```
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show status like 'Ssl_cipher';
+---------------+------------------------+
| Variable_name | Value                  |
+---------------+------------------------+
| Ssl_cipher    | TLS_AES_256_GCM_SHA384 |
+---------------+------------------------+
1 row in set (0.000 sec)

MariaDB [(none)]>
```

Supprimez votre utilisateur user2:

```
MariaDB [(none)]> USE mysql;
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 [mysql]> DELETE FROM user WHERE User='user2';
Query OK, 1 row affected (0.000 sec)

MariaDB [mysql]>
```

Créez maintenant votre utilisateur **user2** afin que celui-ci se connecte en utilisant SSL:

```
MariaDB [mysql]> GRANT usage ON *.* TO user2@localhost IDENTIFIED BY 'motdepasse' REQUIRE SSL;
Query OK, 0 rows affected (0.000 sec)
```

```
MariaDB [mysql]>
```

Saisissez enfin la commande suivante pour mettre à jour les privilèges:

```
MariaDB [mysql]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [mysql]>
```

Connectez-vous maintenant en utilisant le compte d'user2.

```
MariaDB [mysql]> exit
Bye

[root@centos8 mysql]# mysql -u user2 -p
Enter password: motdepasse
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 10.3.28-MariaDB-log MariaDB Server

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```
