Version : **2022.01**

Dernière mise-à-jour : 2022/11/08 18:02

SER404 - Journalisation et Sécurité

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**,
- 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@centos7 ~]# vi /etc/my.cnf
[root@centos7 ~]# cat /etc/my.cnf
[mysqld]
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
# 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 mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd

[mysqld_safe]
log-error=/var/log/mariadb/mariadb.log
pid-file=/var/run/mariadb/mariadb.pid

#
# include all files from the config directory
#
!includedir /etc/my.cnf.d

[root@centos7 ~]# systemctl restart mariadb
[root@centos7 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-11-02 14:32:14 CET; 6s ago
  Process: 24045 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
```

```
  Process: 24009 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
 Main PID: 24044 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─24044 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─24248 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysq...

Nov 02 14:32:11 centos7.fenestros.loc systemd[1]: Starting MariaDB database s...
Nov 02 14:32:12 centos7.fenestros.loc mariadb-prepare-db-dir[24009]: Database...
Nov 02 14:32:13 centos7.fenestros.loc mysqld_safe[24044]: 171102 14:32:13 mys...
Nov 02 14:32:13 centos7.fenestros.loc mysqld_safe[24044]: 171102 14:32:13 mys...
Nov 02 14:32:14 centos7.fenestros.loc systemd[1]: Started MariaDB database se...
Hint: Some lines were ellipsized, use -l to show in full.
```

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

```
[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)]> 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 (0.01 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 (0.00 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 (0.00 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 (0.00 sec)

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
| general_log      | ON          |
| general_log_file | centos7.log |
+------------------+-------------+
2 rows in set (0.00 sec)

MariaDB [(none)]> exit
Bye
[root@centos7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
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)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| CarnetAdresses     |
| Nombres            |
```

```
| ligue1             |
| mysql              |
| performance_schema |
| test               |
+--------------------+
12 rows in set (0.01 sec)

MariaDB [(none)]> exit
Bye
[root@centos7 ~]#

[root@centos7 ~]# cat /var/lib/mysql/centos7.log
/usr/libexec/mysqld, Version: 5.5.56-MariaDB (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command    Argument
171102 14:38:55     3 Query    SHOW GLOBAL VARIABLES LIKE 'general_log%'
171102 14:39:11     3 Quit
171102 14:39:24     4 Connect    root@localhost as anonymous on
            4 Query    select @@version_comment limit 1
171102 14:39:47     4 Query    SHOW DATABASES
171102 14:40:24     4 Quit
```

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

En ajoutant la directive **log_output = TABLE** au fichier **/etc/my.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/centos7.log** :

```
[root@centos7 ~]# vi /etc/my.cnf
[root@centos7 ~]# cat /etc/my.cnf
[mysqld]
slow_query_log
```

```
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
log_output = TABLE
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
# 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 mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd

[mysqld_safe]
log-error=/var/log/mariadb/mariadb.log
pid-file=/var/run/mariadb/mariadb.pid

#
# include all files from the config directory
#
!includedir /etc/my.cnf.d

[root@centos7 ~]# systemctl restart mariadb

[root@centos7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
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)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
```

```
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
| general_log      | OFF         |
| general_log_file | centos7.log |
+------------------+-------------+
2 rows in set (0.00 sec)

MariaDB [(none)]> SET GLOBAL general_log = 'ON';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> SHOW GLOBAL VARIABLES LIKE 'general_log%';
+------------------+-------------+
| Variable_name    | Value       |
+------------------+-------------+
| general_log      | ON          |
| general_log_file | centos7.log |
+------------------+-------------+
2 rows in set (0.01 sec)

MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| CarnetAdresses     |
| Nombres            |
| ligue1             |
| mysql              |
| performance_schema |
| test               |
+--------------------+
12 rows in set (0.01 sec)
```

```
MariaDB [(none)]> SELECT * FROM mysql.general_log;
+----------------------------+----------------------------+-----------+-----------+--------------+---------------
----------------------------+
| event_time                 | user_host                  | thread_id | server_id | command_type | argument
|
+----------------------------+----------------------------+-----------+-----------+--------------+---------------
----------------------------+
| 2017-11-02 15:34:27.247638 | root[root] @ localhost [] |         2 |         0 | Query        | SHOW GLOBAL
VARIABLES LIKE 'general_log%' |
| 2017-11-02 15:34:50.736688 | root[root] @ localhost [] |         2 |         0 | Query        | SHOW DATABASES
|
| 2017-11-02 15:34:58.497535 | root[root] @ localhost [] |         2 |         0 | Query        | SELECT * FROM
mysql.general_log           |
+----------------------------+----------------------------+-----------+-----------+--------------+---------------
----------------------------+
3 rows in set (0.01 sec)

MariaDB [(none)]> exit
Bye

[root@centos7 ~]# cat /var/lib/mysql/centos7.log
/usr/libexec/mysqld, Version: 5.5.56-MariaDB (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command    Argument
171102 14:38:55     3 Query    SHOW GLOBAL VARIABLES LIKE 'general_log%'
171102 14:39:11     3 Quit
171102 14:39:24     4 Connect    root@localhost as anonymous on
            4 Query    select @@version_comment limit 1
171102 14:39:47     4 Query    SHOW DATABASES
171102 14:40:24     4 Quit
/usr/libexec/mysqld, Version: 5.5.56-MariaDB (MariaDB Server). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command    Argument
```

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
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

Droit	Description
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,
- DEFINIR : 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

L'utilisateur anonyme

Lors de l'installation de MariaDB deux utilisateurs sont créés:

- **root**
  - l'administrateur du serveur
- **anonyme**
  - l'utilisateur n'ayant accès qu'à la base **test** et à toutes les bases commençant par **test**

Pour des raisons de sécurité, l'utilisateur anonyme ainsi que les bases test doivent être supprimés.

Procédez donc comme suit pour supprimez l'utilisateur anonyme :

```
[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]> SELECT user, host, password FROM user;
+-------+-----------------------+-------------------------------------------+
| user  | host                  | password                                  |
+-------+-----------------------+-------------------------------------------+
| root  | localhost             | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| root  | centos7.fenestros.loc |                                           |
| root  | 127.0.0.1             |                                           |
| root  | ::1                   |                                           |
|       | localhost             |                                           |
|       | centos7.fenestros.loc |                                           |
| user1 | localhost             | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-------+-----------------------+-------------------------------------------+
7 rows in set (0.00 sec)

MariaDB [mysql]> DELETE FROM user WHERE user ='';
Query OK, 2 rows affected (0.00 sec)

MariaDB [mysql]> SELECT user, host, password FROM user;
+-------+-----------------------+-------------------------------------------+
| user  | host                  | password                                  |
+-------+-----------------------+-------------------------------------------+
| root  | localhost             | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| root  | centos7.fenestros.loc |                                           |
| root  | 127.0.0.1             |                                           |
| root  | ::1                   |                                           |
| user1 | localhost             | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-------+-----------------------+-------------------------------------------+
5 rows in set (0.00 sec)

MariaDB [mysql]>
```

Pour supprimer **l'accès** aux bases de données **test**, saisissez la commande suivante:

```
MariaDB [mysql]> DELETE FROM db WHERE db LIKE 'test%';
Query OK, 2 rows affected (0.01 sec)

MariaDB [mysql]>
```

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

```
MariaDB [mysql]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [mysql]>
```

La table user

Visualisez la table user:

```
MariaDB [mysql]> DESCRIBE user;
+------------------------+-----------------------------------+------+-----+---------+-------+
| Field                  | Type                              | Null | Key | Default | Extra |
+------------------------+-----------------------------------+------+-----+---------+-------+
| Host                   | char(60)                          | NO   | PRI |         |       |
| User                   | char(16)                          | 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       |       |
| 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    |       |
+--------------------------+----------------------------------------+------+-----+---------+-------+
42 rows in set (0.01 sec)

MariaDB [mysql]>
```

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

Champs	Longueur
User	16
Host	60

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. 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 (0.01 sec)

MariaDB [mysql]> SELECT old_password('root');
+----------------------+
| old_password('root') |
+----------------------+
| 67457e226a1a15bd     |
+----------------------+
1 row in set (0.00 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
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
BLACKHOLE	ACTIVE	STORAGE ENGINE	NULL	GPL
InnoDB	ACTIVE	STORAGE ENGINE	NULL	GPL
INNODB_RSEG	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_UNDO_LOGS	ACTIVE	INFORMATION SCHEMA	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_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_STATS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_TABLE_STATS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_INDEX_STATS	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_POOL_PAGES	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_POOL_PAGES_INDEX	ACTIVE	INFORMATION SCHEMA	NULL	GPL
INNODB_BUFFER_POOL_PAGES_BLOB	ACTIVE	INFORMATION SCHEMA	NULL	GPL
XTRADB_ADMIN_COMMAND	ACTIVE	INFORMATION SCHEMA	NULL	GPL

```
| INNODB_CHANGED_PAGES           | 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     |
| FEDERATED                      | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| ARCHIVE                        | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| PERFORMANCE_SCHEMA             | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| Aria                           | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
| FEEDBACK                       | DISABLED | INFORMATION SCHEMA | NULL    | GPL     |
| partition                      | ACTIVE   | STORAGE ENGINE     | NULL    | GPL     |
+--------------------------------+----------+--------------------+---------+---------+
42 rows in set (0.01 sec)

MariaDB [mysql]>
```

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.

LAB #1 - Perte du Mot de Passe de l'Administrateur

Dans le cas de la perte du mot de passe de l'administrateur de MariaDB, une solution consiste en une connexion qui détourne la vérification des droits des utilisateurs.

Arrêtez le serveur MariaDB avec la commande **systemctl stop mariadb**. Lancez ensuite le serveur MariaDB en invocation **directe** en utilisant la commande **suivante** (c'est plus clair Gregory !!!!!) :

```
[root@centos7 ~]# /usr/libexec/mysqld --skip-grant-tables --console --socket=/tmp/depannage.sock --user=mysql &
```

```
[1] 20768
[root@centos7 ~]# 171102 15:58:56 [Note] /usr/libexec/mysqld (mysqld 5.5.56-MariaDB) starting as process 20768
...
171102 15:58:56 [Warning] Although a path was specified for the --log-slow-queries option, log tables are used.
To enable logging to files use the --log-output=file option.
171102 15:58:56 InnoDB: The InnoDB memory heap is disabled
171102 15:58:56 InnoDB: Mutexes and rw_locks use GCC atomic builtins
171102 15:58:56 InnoDB: Compressed tables use zlib 1.2.7
171102 15:58:56 InnoDB: Using Linux native AIO
171102 15:58:56 InnoDB: Initializing buffer pool, size = 128.0M
171102 15:58:56 InnoDB: Completed initialization of buffer pool
171102 15:58:56 InnoDB: highest supported file format is Barracuda.
171102 15:58:56  InnoDB: Waiting for the background threads to start
171102 15:58:57 Percona XtraDB (http://www.percona.com) 5.5.52-MariaDB-38.3 started; log sequence number
594794225
171102 15:58:57 [Note] Plugin 'FEEDBACK' is disabled.
171102 15:58:57 [ERROR] mysqld: File '/var/log/mysql-slow.log' not found (Errcode: 13)
171102 15:58:57 [ERROR] Could not use /var/log/mysql-slow.log for logging (error 13). Turning logging off for the
whole duration of the MySQL server process. To turn it on again: fix the cause, shutdown the MySQL server and
restart it.
171102 15:58:57 [Note] Server socket created on IP: '0.0.0.0'.
171102 15:58:57 [Note] /usr/libexec/mysqld: ready for connections.
Version: '5.5.56-MariaDB'  socket: '/tmp/depannage.sock'  port: 3306  MariaDB Server
```

Appuyez sur la touche ↵ Entrée et connectez-vous au serveur MariaDB sur le socket utilisé :

```
[root@centos7 ~]# mysql --socket=/tmp/depannage.sock
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1
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)]>
```

Definissez de nouveau le mot de passe de l'utilisateur root :

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('fenestros');
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>
```

Sortez de mysql et testez la connexion avec le nouveau mot de passe :

```
MariaDB [(none)]> exit
Bye
[root@centos7 ~]# mysql -u root -p --socket=/tmp/depannage.sock
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
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)]>
```

Tuez maintenant le processus de mysqld et relancez le serveur normalement :

```
MariaDB [(none)]> exit
Bye
[root@centos7 ~]# ps aux | grep mysqld
mysql    20768  0.3  4.3 909024 89472 pts/0    Sl   15:58   0:00 /usr/libexec/mysqld --skip-grant-tables --
```

```
console --socket=/tmp/depannage.sock --user=mysql
root     21853  0.0  0.0 114692   960 pts/0    S+   16:02   0:00 grep --color=auto mysqld
[root@centos7 ~]# kill -9 20768
[root@centos7 ~]# systemctl start mariadb
[1]+  Killed                  /usr/libexec/mysqld --skip-grant-tables --console --socket=/tmp/depannage.sock --
user=mysql
[root@centos7 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-11-02 16:02:36 CET; 10s ago
  Process: 22053 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
  Process: 22021 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
 Main PID: 22052 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─22052 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─22267 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysq...

Nov 02 16:02:33 centos7.fenestros.loc systemd[1]: Starting MariaDB database s...
Nov 02 16:02:34 centos7.fenestros.loc mariadb-prepare-db-dir[22021]: Database...
Nov 02 16:02:35 centos7.fenestros.loc mysqld_safe[22052]: 171102 16:02:35 mys...
Nov 02 16:02:35 centos7.fenestros.loc mysqld_safe[22052]: 171102 16:02:35 mys...
Nov 02 16:02:36 centos7.fenestros.loc systemd[1]: Started MariaDB database se...
Hint: Some lines were ellipsized, use -l to show in full.
```

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@centos7 ~]# cat .mysql_history
...
SHOW GLOBAL VARIABLES LIKE 'general_log%';
SET GLOBAL general_log = 'ON';
SHOW GLOBAL VARIABLES LIKE 'general_log%';
SHOW DATABASES;
SELECT * FROM mysql.general_log;
```

```
USE mysql;
SELECT user, host, password FROM user;
DELETE FROM user WHERE user ='';
SELECT user, host, password FROM user;
DELETE FROM db WHERE db LIKE 'test%';
FLUSH PRIVILEGES;
DESCRIBE user;
SELECT password('root');
SELECT old_password('root');
SHOW PLUGINS;
FLUSH PRIVILEGES;
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('fenestros');
```

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  | centos7.fenestros.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  | centos7.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@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]> 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 |
| centos7.fenestros.loc | root  |                                           |
| 127.0.0.1             | root  |                                           |
| ::1                   | root  |                                           |
| localhost             | user2 | *1F48A8CB9F3BAAE4504A9A4549B0AA290BD4E27B |
| localhost             | user1 | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
```

```
+----------------------+-------+-------------------------------------------+
6 rows in set (0.00 sec)

MariaDB [mysql]>
```

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

```
[root@centos7 ~]# mysql -u user2 -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)]> SHOW databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0.00 sec)

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

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:

```
mysql> 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:

```
mysql> 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** :

```
mysql> 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** :

```
mysql> GRANT usage ON *.* TO utilisateur@host IDENTIFIED BY 'nouveau_mot_de_passe'; [Entrée]
```

En utilisant **UPDATE USER** :

```
mysql> 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:

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'have_openssl';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| have_openssl  | YES   |
+---------------+-------+
1 row in set (0.00 sec)

MariaDB [(none)]>
```

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 :

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'have_openssl';
+---------------+----------+
| Variable_name | Value    |
+---------------+----------+
| have_openssl  | DISABLED |
+---------------+----------+
1 row in set (0.00 sec)

MariaDB [(none)]>
```

Openssl

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

```
MariaDB [(none)]> exit
Bye
[root@centos7 ~]# ls -lR /etc/pki
/etc/pki:
total 4
drwxr-xr-x. 6 root root   57 Feb 20  2017 CA
drwxr-xr-x. 4 root root   69 Jun 25 12:48 ca-trust
drwxr-xr-x. 2 root root   20 Jun 25 12:48 java
drwxr-xr-x. 2 root root   97 Jun 25 12:48 nssdb
drwxr-xr-x. 2 root root 4096 May  9 15:11 rpm-gpg
drwx------. 2 root root    6 Nov  5  2016 rsyslog
drwxr-xr-x. 5 root root   76 Jun 25 12:48 tls

/etc/pki/CA:
total 0
drwxr-xr-x. 2 root root 6 Feb 20  2017 certs
drwxr-xr-x. 2 root root 6 Feb 20  2017 crl
drwxr-xr-x. 2 root root 6 Feb 20  2017 newcerts
```

```
drwx------. 2 root root 6 Feb 20  2017 private

/etc/pki/CA/certs:
total 0

/etc/pki/CA/crl:
total 0

/etc/pki/CA/newcerts:
total 0

/etc/pki/CA/private:
total 0

/etc/pki/ca-trust:
total 8
-rw-r--r--. 1 root root 980 Jun 13 18:22 ca-legacy.conf
drwxr-xr-x. 5 root root  54 Jun 25 12:48 extracted
-rw-r--r--. 1 root root 166 Jun 13 18:22 README
drwxr-xr-x. 4 root root  76 Jun 25 12:48 source

/etc/pki/ca-trust/extracted:
total 4
drwxr-xr-x. 2 root root  33 Jun 25 12:48 java
drwxr-xr-x. 2 root root  45 Jun 25 12:48 openssl
drwxr-xr-x. 2 root root  97 Jun 25 12:48 pem
-rw-r--r--. 1 root root 560 Jun 13 18:22 README

/etc/pki/ca-trust/extracted/java:
total 200
-r--r--r--. 1 root root 197507 Jun 25 12:48 cacerts
-rw-r--r--. 1 root root    726 Jun 13 18:22 README

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

```
total 356
-r--r--r--. 1 root root 356404 Jun 25 12:48 ca-bundle.trust.crt
-rw-r--r--. 1 root root    787 Jun 13 18:22 README

/etc/pki/ca-trust/extracted/pem:
total 676
-r--r--r--. 1 root root 218221 Jun 25 12:48 email-ca-bundle.pem
-r--r--r--. 1 root root 192481 Jun 25 12:48 objsign-ca-bundle.pem
-rw-r--r--. 1 root root    898 Jun 13 18:22 README
-r--r--r--. 1 root root 271040 Jun 25 12:48 tls-ca-bundle.pem

/etc/pki/ca-trust/source:
total 4
drwxr-xr-x. 2 root root   6 Jun 13 18:29 anchors
drwxr-xr-x. 2 root root   6 Jun 13 18:29 blacklist
lrwxrwxrwx. 1 root root  59 Jun 25 12:48 ca-bundle.legacy.crt -> /usr/share/pki/ca-trust-legacy/ca-
bundle.legacy.default.crt
-rw-r--r--. 1 root root 932 Jun 13 18:22 README

/etc/pki/ca-trust/source/anchors:
total 0

/etc/pki/ca-trust/source/blacklist:
total 0

/etc/pki/java:
total 0
lrwxrwxrwx. 1 root root 40 Jun 25 12:48 cacerts -> /etc/pki/ca-trust/extracted/java/cacerts

/etc/pki/nssdb:
total 124
-rw-r--r--. 1 root root 65536 May 30 16:09 cert8.db
-rw-r--r--. 1 root root  9216 May 30 16:09 cert9.db
-rw-r--r--. 1 root root 16384 May 30 16:09 key3.db
```

```
-rw-r--r--. 1 root root 11264 May 30 16:09 key4.db
-rw-r--r--. 1 root root   451 May 30 16:08 pkcs11.txt
-rw-r--r--. 1 root root 16384 May 30 16:09 secmod.db

/etc/pki/rpm-gpg:
total 16
-rw-r--r--. 1 root root 1726 Mar  8  2011 RPM-GPG-KEY-adobe-linux
-rw-r--r--. 1 root root 1690 Nov 29  2016 RPM-GPG-KEY-CentOS-7
-rw-r--r--. 1 root root 1004 Nov 29  2016 RPM-GPG-KEY-CentOS-Debug-7
-rw-r--r--. 1 root root 1690 Nov 29  2016 RPM-GPG-KEY-CentOS-Testing-7

/etc/pki/rsyslog:
total 0

/etc/pki/tls:
total 16
lrwxrwxrwx. 1 root root    49 Jun 25 12:48 cert.pem -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
drwxr-xr-x. 2 root root  4096 Jun 25 12:48 certs
drwxr-xr-x. 2 root root    69 Apr 15  2017 misc
-rw-r--r--. 1 root root 10923 Feb 20  2017 openssl.cnf
drwxr-xr-x. 2 root root     6 Feb 20  2017 private

/etc/pki/tls/certs:
total 12
lrwxrwxrwx. 1 root root   49 Jun 25 12:48 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
lrwxrwxrwx. 1 root root   55 Jun 25 12:48 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracted/openssl/ca-
bundle.trust.crt
-rwxr-xr-x. 1 root root  610 Feb 20  2017 make-dummy-cert
-rw-r--r--. 1 root root 2388 Feb 20  2017 Makefile
-rwxr-xr-x. 1 root root  829 Feb 20  2017 renew-dummy-cert

/etc/pki/tls/misc:
total 24
-rwxr-xr-x. 1 root root 5178 Feb 20  2017 CA
```

```
-rwxr-xr-x. 1 root root  119 Feb 20  2017 c_hash
-rwxr-xr-x. 1 root root  152 Feb 20  2017 c_info
-rwxr-xr-x. 1 root root  112 Feb 20  2017 c_issuer
-rwxr-xr-x. 1 root root  110 Feb 20  2017 c_name

/etc/pki/tls/private:
total 0
[root@centos7 ~]#
```

Activer SSL

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

```
[root@centos7 ~]# systemctl stop mariadb
[root@centos7 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Thu 2017-11-02 16:34:56 CET; 7s ago
  Process: 22053 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
  Process: 22052 ExecStart=/usr/bin/mysqld_safe --basedir=/usr (code=exited, status=0/SUCCESS)
  Process: 22021 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
 Main PID: 22052 (code=exited, status=0/SUCCESS)

Nov 02 16:02:33 centos7.fenestros.loc systemd[1]: Starting MariaDB database s...
Nov 02 16:02:34 centos7.fenestros.loc mariadb-prepare-db-dir[22021]: Database...
Nov 02 16:02:35 centos7.fenestros.loc mysqld_safe[22052]: 171102 16:02:35 mys...
Nov 02 16:02:35 centos7.fenestros.loc mysqld_safe[22052]: 171102 16:02:35 mys...
Nov 02 16:02:36 centos7.fenestros.loc systemd[1]: Started MariaDB database se...
Nov 02 16:34:52 centos7.fenestros.loc systemd[1]: Stopping MariaDB database s...
Nov 02 16:34:56 centos7.fenestros.loc systemd[1]: Stopped MariaDB database se...
Hint: Some lines were ellipsized, use -l to show in full.
```

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

```
[root@centos7 ~]# mkdir /etc/pki/mysql
[root@centos7 ~]# cd /etc/pki/mysql/
[root@centos7 mysql]# openssl genrsa 2048 > ca-key.pem
Generating RSA private key, 2048 bit long modulus
.........................................+++
.......+++
e is 65537 (0x10001)
```

Créez ensuite le fichier ca-cert.pem :

```
[root@centos7 mysql]# openssl genrsa 2048 > ca-key.pem
Generating RSA private key, 2048 bit long modulus
.....................................................................................................
.....................................................+++
.........................+++
e is 65537 (0x10001)

[root@centos7 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) []:centos7.fenestros.loc
Email Address []:infos@i2tch.co.uk
[root@centos7 mysql]# ls -l
total 8
```

```
-rw-r--r--. 1 root root 1476 Nov  3 07:36 ca-cert.pem
-rw-r--r--. 1 root root 1675 Nov  3 07:34 ca-key.pem
[root@centos7 mysql]#
```

Créer ensuite le certificat du serveur :

```
[root@centos7 mysql]# openssl req -newkey rsa:2048 -days 1000 -nodes -keyout server-key.pem > server-req.pem
Generating a 2048 bit 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) []:server7.fenestros.loc
Email Address []:infos@i2tch.co.uk

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@centos7 mysql]#

[root@centos7 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=server7.fenestros.loc/emailAddress=infos@i2tch.co.uk
Getting CA Private Key
[root@centos7 mysql]#
```

Créer maintenant le certificat du client:

```
[root@centos7 mysql]# openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client-key.pem > client-req.pem
Generating a 2048 bit 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) []:centos7.fenestros.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@centos7 mysql]# ls -l
total 28
-rw-r--r--. 1 root root 1476 Nov  3 07:36 ca-cert.pem
-rw-r--r--. 1 root root 1675 Nov  3 07:34 ca-key.pem
-rw-r--r--. 1 root root 1704 Nov  3 07:39 client-key.pem
-rw-r--r--. 1 root root 1066 Nov  3 07:39 client-req.pem
-rw-r--r--. 1 root root 1346 Nov  3 07:38 server-cert.pem
-rw-r--r--. 1 root root 1704 Nov  3 07:37 server-key.pem
-rw-r--r--. 1 root root 1082 Nov  3 07:37 server-req.pem

[root@centos7 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=centos7.fenestros.loc/emailAddress=infos@i2tch.eu
Getting CA Private Key
```

Vérifiez ensuite vos certificats :

```
[root@centos7 mysql]# openssl verify -CAfile ca-cert.pem server-cert.pem client-cert.pem
server-cert.pem: OK
client-cert.pem: OK
```

Modifiez votre fichier my.cnf :

```
[root@centos7 mysql]# vi /etc/my.cnf
[root@centos7 mysql]# cat /etc/my.cnf
[mysqld]
slow_query_log
slow_query_log_file = /var/log/mysql-slow.log
long-query-time = 2
log_output = TABLE
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
# Disabling symbolic-links is recommended to prevent assorted security risks
```

```
symbolic-links=0
# 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 mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd

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

[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

[mysqld_safe]
log-error=/var/log/mariadb/mariadb.log
pid-file=/var/run/mariadb/mariadb.pid

#
# include all files from the config directory
#
!includedir /etc/my.cnf.d
```

Démarrez votre serveur MariaDB :

```
[root@centos7 mysql]# systemctl start mariadb
```

Vérifiez que MariaDB fonctionne en mode SSL :

```
[root@centos7 mysql]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
```

```
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)]> show status like 'Ssl_cipher';
+---------------+---------------------------+
| Variable_name | Value                     |
+---------------+---------------------------+
| Ssl_cipher    | DHE-RSA-AES256-GCM-SHA384 |
+---------------+---------------------------+
1 row in set (0.01 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 (0.01 sec)

MariaDB [mysql]>
```

Contrôlez que l'utilisateur a été supprimé:

```
MariaDB [mysql]> SELECT host, user, password FROM user;
+-----------------------+-------+-------------------------------------------+
| host                  | user  | password                                  |
+-----------------------+-------+-------------------------------------------+
```

```
| localhost             | root  | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| centos7.fenestros.loc | root  |                                           |
| 127.0.0.1             | root  |                                           |
| ::1                   | root  |                                           |
| localhost             | user1 | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-----------------------+-------+-------------------------------------------+
5 rows in set (0.01 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' REQUIRE SSL;
Query OK, 0 rows affected (0.00 sec)

MariaDB [mysql]>
```

Contrôlez que l'utilisateur a été ajouté:

```
MariaDB [mysql]> SELECT host, user, password FROM user;
+-----------------------+-------+-------------------------------------------+
| host                  | user  | password                                  |
+-----------------------+-------+-------------------------------------------+
| localhost             | root  | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| centos7.fenestros.loc | root  |                                           |
| 127.0.0.1             | root  |                                           |
| ::1                   | root  |                                           |
| localhost             | user2 |                                           |
| localhost             | user1 | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-----------------------+-------+-------------------------------------------+
6 rows in set (0.00 sec)

MariaDB [mysql]>
```

Donnez à user2 un mot de passe:

```
MariaDB [mysql]> SET PASSWORD FOR 'user2'@'localhost'=PASSWORD('toto2');
Query OK, 0 rows affected (0.00 sec)

MariaDB [mysql]>
```

Contrôlez que le mot de passe a été ajouté:

```
MariaDB [mysql]> SELECT host, user, password FROM user;
+-----------------------+-------+-------------------------------------------+
| host                  | user  | password                                  |
+-----------------------+-------+-------------------------------------------+
| localhost             | root  | *00269BA49BEC800F9CCF34C20C1FD83E0236B89A |
| centos7.fenestros.loc | root  |                                           |
| 127.0.0.1             | root  |                                           |
| ::1                   | root  |                                           |
| localhost             | user2 | *9296FFD029BFAE29EDDC1E57E53F4A8E555895B8 |
| localhost             | user1 | *34D3B87A652E7F0D1D371C3DBF28E291705468C4 |
+-----------------------+-------+-------------------------------------------+
6 rows in set (0.00 sec)

MariaDB [mysql]>
```

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

```
MariaDB [mysql]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [mysql]>
```

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

```
MariaDB [mysql]> exit
```

```
Bye
[root@centos7 mysql]# mysql -u user2 -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)]>
```

Copyright © 2022 Hugh Norris.