Securité

- Authentification Simple et administration des droits
- Connection et SSL
- Installation de SSL avec MariaDB sous Debian

Authentification Simple et administration des droits

MySQL implémente un système sophistiqué de contrôle d'accès et de privilèges qui vous permet de créer des règles d'accès complètes pour la gestion des opérations client et d'empêcher efficacement les clients non autorisés d'accéder au système de base de données.

Le contrôle d'accès MySQL comporte deux étapes lorsqu'un client se connecte au serveur:

- Vérification de la connexion: un client qui se connecte au serveur de base de données MySQL doit avoir un nom d'utilisateur et un mot de passe valides. De plus, l'hôte à partir duquel le client se connecte doit correspondre à l'hôte dans la table de droits MySQL.
- Vérification de la demande: une fois la connexion établie avec succès, MySQL vérifie, pour chaque instruction émise par le client, si le client dispose des privilèges suffisants pour exécuter cette instruction. MySQL peut vérifier un privilège au niveau de la base de données, de la table et du champ.

Création de comptes d'utilisateurs à l'aide de l'instruction MySQL CREATE USER

MySQL fournit l'instruction CREATE USER qui vous permet de créer un nouveau compte utilisateur.
La syntaxe de l'instruction CREATE USER est la suivante:
CREATE USER ''compte_utilisateur'' IDENTIFIED BY ''mot de passe'';

Le compte utilisateur au format 'nom_utilisateur' @ 'nom_hôte' est suivi de la clause CREATE USER.

Le mot de passe est spécifié dans la clause IDENTIFIED BY. Le mot de passe doit être en texte clair. MySQL chiffrera le mot de passe avant de sauvegarder le compte utilisateur dans la table user.

```
CREATE USER myuser@localhost IDENTIFIED BY 'myuser';
Query OK, 0 rows affected (0,06 sec)
```

Puis la connexion peut s'établir ainsi:

```
./bin/mysql -u myuser -h localhost -p
```

L'utilisateur peut se connecter mais n'a pour l'instant aucun droit

```
show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0,00 sec)
```

Les droits de notre utilisateurs sont ainsi:

```
SHOW GRANTS FOR 'myuser'@'localhost';
+-----------------------------------------+
| Grants for myuser@localhost |
+-----------------------------------------+
| GRANT USAGE ON *.* TO `myuser`@`localhost` |
+-----------------------------------------+
1 row in set (0,00 sec)
```

creation d'un utilisateur avec un plugin d'authentification

Il est possible d'utiliser un plugin d'authentification spécifique ici un plugin sha256

```
CREATE USER 'sha256user'@'localhost'
-> IDENTIFIED WITH sha256_password BY 'password';
```

Augmentation de la sécurité via le plugin de validation de password

Le plugin validate_password sert à tester les mots de passe et à améliorer la sécurité. Le plugin expose un ensemble de variables système qui vous permettent de définir une politique de mot de passe.

```
mysql> INSTALL PLUGIN validate_password SONAME 'validate_password.so';
Query OK, 0 rows affected, 1 warning (0,07 sec)

mysql> SELECT PLUGIN_NAME, PLUGIN_STATUS
-> FROM INFORMATION_SCHEMA.PLUGINS
-> WHERE PLUGIN_NAME LIKE 'validate%';
+-------------------+--------------+
| PLUGIN_NAME | PLUGIN_STATUS |
+-------------------+--------------+
| validate_password | ACTIVE |
+-------------------+--------------+
1 row in set (0,00 sec)
```

On teste maintenant la création d'un mot de passe pauvre

```
create user 'bob'@'%' IDENTIFIED BY 'test';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
```

Il est possible de charger une strategie de validation:

- La stratégie LOW teste uniquement la longueur du mot de passe. Les mots de passe doivent comporter au moins 8 caractères. Pour changer cette longueur, modifiez validate_password_length.

- La stratégie MEDIUM ajoute les conditions selon lesquelles les mots de passe doivent contenir au moins un caractère numérique, un caractère minuscule, un caractère majuscule et un caractère spécial (non alphanumérique). Pour modifier ces valeurs, modifiez validate_password_number_count, validate_password_mixed_case_count et validate_password_special_char_count.
- La stratégie STRONG ajoute la condition selon laquelle les sous-chaînes de mot de passe de longueur égale ou supérieure à 4 ne doivent pas correspondre aux mots du fichier de dictionnaire, s'il en a été spécifié. Pour spécifier le fichier de dictionnaire, modifiez validate_password_dictionary_file.

Ici on selectionne la stratégie medium par défaut

```
SET GLOBAL validate_password_policy = 1;
Query OK, 0 rows affected (0,00 sec)

mysql> create user 'bob'@'%' identified by 'aA!12345678';
Query OK, 0 rows affected (0,05 sec)
```

Assignation d'un droit a un utilisateur

La commande GRANT permet d'associer un droit à un utilisateur. Nous donnons ici le droit show databases à l'utilisateur myuser

```
mysql> grant show databases on *.* TO 'myuser'@'localhost';
Query OK, 0 rows affected (0,13 sec)

mysql> \q
Bye
```

Nous pouvons maintenant le tester

```
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ ./bin/mysql -u myuser -h
localhost -p
mysql> show databases;
+--------------------+
| Database |
```

```
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| sys |
| testUtf8 |
| testdb |
+--------------------+
6 rows in set (0,00 sec)
```

Mise en place de Rôle

En règle générale, vous avez plusieurs utilisateurs avec le même ensemble de privilèges. Le moyen d'octroyer et de révoquer des privilèges à plusieurs utilisateurs de modifier les privilèges de chaque utilisateur individuellement demande beaucoup de temps.

Pour faciliter les choses, MySQL a fourni un nouvel objet appelé role, qui est une collection nommée de privilèges.

Si vous souhaitez accorder le même ensemble de privilèges à plusieurs utilisateurs, procédez comme suit:

- Tout d'abord, créez un nouveau rôle.
- Deuxièmement, accordez des privilèges au rôle.
- Troisièmement, accordez le rôle aux utilisateurs.

Si vous souhaitez modifier les privilèges des utilisateurs, vous devez modifier uniquement les privilèges du rôle attribué. Les modifications prendront effet pour tous les utilisateurs auxquels le rôle a été attribué.

Nous allons créer une base de données exemple:

```
CREATE DATABASE crm;
Query OK, 1 row affected (0,05 sec)

mysql> use crm;
Database changed
mysql> CREATE TABLE customer(
-> id INT PRIMARY KEY AUTO_INCREMENT,
```

```
-> first_name varchar(255) NOT NULL,
-> last_name VARCHAR(255) NOT NULL,
-> phone VARCHAR(15) NOT NULL,
-> email VARCHAR(255)
-> );
Query OK, 0 rows affected (0,11 sec)

mysql> INSERT INTO customer(first_name,last_name,phone,email)
-> VALUES('John','Doe','(408)-987-7654','john.doe@mysql.org'),
-> ('Lily','Bush','(408)-987-7985','lily.bush@mysql.org');
Query OK, 2 rows affected (0,06 sec)
Records: 2 Duplicates: 0 Warnings: 0
```

Puis nous créons 3 rôle permettant respectivement d^'etre un super utilisateur de la base, de pouvoir la lire et de pouvoir l'écrire

```
mysql> CREATE ROLE crm_dev, crm_read, crm_write;
Query OK, 0 rows affected (0,05 sec)

mysql> GRANT ALL ON crm.* TO crm_dev;
Query OK, 0 rows affected (0,07 sec)

mysql> GRANT SELECT ON crm.* TO crm_read;
Query OK, 0 rows affected (0,11 sec)

mysql> GRANT INSERT, UPDATE, DELETE ON crm.* TO crm_write;
Query OK, 0 rows affected (0,05 sec)
```

Puis nous créons des utilisateurs

```
mysql> -- developer user
mysql> CREATE USER crm_dev1@localhost IDENTIFIED BY 'Secure$1782';
Query OK, 0 rows affected (0,03 sec)

mysql> -- read access user
mysql> CREATE USER crm_read1@localhost IDENTIFIED BY 'Secure$5432';
Query OK, 0 rows affected (0,01 sec)
```

```
mysql> -- read/write users
mysql> CREATE USER crm_write1@localhost IDENTIFIED BY 'Secure$9075';
Query OK, 0 rows affected (0,01 sec)

mysql> CREATE USER crm_write2@localhost IDENTIFIED BY 'Secure$3452';
Query OK, 0 rows affected (0,14 sec)
```

Enfin nous associons nos utilisateurs a nos rôle

```
mysql> GRANT crm_dev TO crm_dev1@localhost;
Query OK, 0 rows affected (0,08 sec)

mysql>
mysql> GRANT crm_read TO crm_read1@localhost;
Query OK, 0 rows affected (0,01 sec)

mysql>
mysql> GRANT crm_read, crm_write TO crm_write1@localhost, crm_write2@localhost;
Query OK, 0 rows affected (0,11 sec)
```

Il est possible de voir les droits d'un utilisateur, qui sont en fait les droits de l'utilisateur associé aux roles:

```
SHOW GRANTS FOR crm_dev1@localhost;
+-----------------------------------------------+
| Grants for crm_dev1@localhost |
+-----------------------------------------------+
| GRANT USAGE ON *.* TO `crm_dev1`@`localhost` |
| GRANT `crm_dev`@`%` TO `crm_dev1`@`localhost` |
+-----------------------------------------------+
2 rows in set (0,00 sec)
```

Pour voir les droits d'un utilisateur en fonction d'un rôle, il faut le demander explicitement via la clause USING

```
mysql> SHOW GRANTS FOR crm_write1@localhost USING crm_write;
+-----------------------------------------------------------------+
| Grants for crm_write1@localhost |
+-----------------------------------------------------------------+
| GRANT USAGE ON *.* TO `crm_write1`@`localhost` |
| GRANT INSERT, UPDATE, DELETE ON `crm`.* TO `crm_write1`@`localhost` |
| GRANT `crm_read`@`%`,`crm_write`@`%` TO `crm_write1`@`localhost` |
+-----------------------------------------------------------------+
3 rows in set (0,00 sec)
```

Les droits sont associé a un rôle. Lors de la connection à MySQL, l'utilisateur doit spécifier le rôle qu'il souhaite utiliser

```
pilou@lubuntu: ~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ ./bin/mysql -u crm_read1 -h
localhost -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 8.0.13 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> select current_role();
+---------------+
| current_role() |
+---------------+
| NONE |
+---------------+
1 row in set (0,00 sec)

mysql> SET ROLE crm_read;
Query OK, 0 rows affected (0,00 sec)

mysql> select current_role() ;
```

```
+----------------+
| current_role() |
+----------------+
| `crm_read`@`%` |
+----------------+
1 row in set (0,00 sec)

mysql> use crm;
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
```

connexion via PAM

Les plugins d'authentification sont multiples en version entreprise et sont souvent en version GPL avec mariadb.
Il est possible d'authentifier les utilisateurs via PAM en utilisant le systeme unix pour les authentifier en lieu et place de MySQL.
Sous mariadb installer le plugin auth_pam

```
INSTALL SONAME 'auth_pam';
```

Puis créer un utilisateur qui pourras se connecter via pam

```
CREATE USER 'test_pam'@'localhost' IDENTIFIED VIA pam USING 'mariadb';
```

Créer l'utilisateur sous Linux (ici ubuntu)

```
addUser test_pam
```

Dans le repertoire /etc/pam.d on va editer la configuration pam de MySQL en demandant a ce que la vérification des utilisateurs se fasse via les comptes Unix

```
#%PAM-1.0
@include common-auth
@include common-account
@include common-session-noninteractive
```

Connection et SSL

maximum de connection et maximum de connection utilisateur

- max_user_connections : Le nombre maximum de connexions simultanées autorisées sur un compte utilisateur MySQL donné. Une valeur de 0 (valeur par défaut) signifie «aucune limite».Cette variable a une valeur globale qui peut être définie au démarrage ou à l'exécution du serveur. Il a également une valeur de session en lecture seule qui indique la limite effective de connexion simultanée qui s'applique au compte associé à la session en cours.
- max_connections Le nombre maximum autorisé de connexions client simultanées

Par défaut dans l'installation :

15

1

```
mysql> select @@max_user_connections ;
```

2

```
+------------------------+
```

3

```
| @@max_user_connections |
```

4

```
+------------------------+
```

5

```
| 0 |
```

6

```
+------------------------+
```

7

```
1 row in set (0,00 sec)
```

8

```
□
```

9

```
mysql> select @@max_connections ;
```

10

```
+-------------------+
```

11

```
| @@max_connections |
```

12

```
+-------------------+
```

13

```
| 151 |
```

14

```
+-------------------+
```

15

```
1 row in set (0,00 sec)
```

Un bon conseil est de fixer max_user_connections à 50 à 75% de vos paramètres max_connections. Vous définissez cette valeur dans la section mysqld de votre my.cnf:

2

1

```
max_connections = 400
```

2

```
max_user_connections=200
```

maximum de connection pour un utilisateur

Le settings précédent concerne une mise en place assez globale du nombre de connection.
Il est possible de signifier des limits plus fine en terme de temps et de ressources
Il existe différents types de limites pouvant être utilisés:

- MAX_QUERIES_PER_HOUR Limite le compte à X requêtes par heure.
- MAX_UPDATES_PER_HOUR Limite le compte à X relevés UPDATE par heure.
- MAX_CONNECTIONS_PER_HOUR Limite le compte à un total de X connexions par heure.
- MAX_USER_CONNECTIONS Limite le compte à un total de X connexions simultanées pour le compte.

Par exemple, on limite le nombre de connection de myuser à 5

2

1

```
mysql> ALTER USER 'myuser'@'localhost'  WITH MAX_USER_CONNECTIONS 5;
```

2

```

```

LOCK et Unlock Account

Account lock et Account unlock permette de vérrouiller ou pas un utilisateur

```
9

1
ALTER USER 'myuser'@'localhost'  ACCOUNT LOCK;

2
Query OK, 0 rows affected (0,09 sec)

3


4
mysql> \q

5
Bye

6
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ ./bin/mysql -u myuser -h localh

7
Enter password:

8
ERROR 3118 (HY000): Access denied for user 'myuser'@'localhost'. Account is locked.

9

```

Mise en place de SSL

Pour l'instant la connection entre le client et le serveur est faite en claire.

23

1

```
status
```

2

```
--------------
```

3

```
./bin/mysql  Ver 8.0.13 for linux-glibc2.12 on x86_64 (MySQL Community Server - GPL)
```

4

```

```

5

```
Connection id:		10
```

6

```
Current database:
```

7

```
Current user:		root@localhost
```

8

```
SSL:			Not in use
```

9

```
Current pager:		stdout
```

10

```
Using outfile:		''
```

11

```
Using delimiter:	;
```

12

```
Server version:		8.0.13 MySQL Community Server - GPL
```

13

```
Protocol version:	10
```

14

```
Connection: Localhost via UNIX socket
```

15

```
Server characterset: utf8mb4
```

16

```
Db characterset: utf8mb4
```

17

```
Client characterset: utf8mb4
```

18

```
Conn. characterset: utf8mb4
```

19

```
UNIX socket: /tmp/mysql.sock
```

20

```
Uptime: 29 min 39 sec
```

21

```

```

22

```
Threads: 2 Questions: 22 Slow queries: 0 Opens: 136 Flush tables: 2 Open tables: 106 Queries
```

23

```
--------------
```

Création de l'autorité de certification

Exécutez les commandes suivantes pour créer les clés de l'autorité de certification (CA):

```
7

1
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ mkdir ssl_keys

2
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ openssl genrsa 2048 > ./ssl_key

3
Generating RSA private key, 2048 bit long modulus (2 primes)

4
.....................................................................+++++

5
.............................+++++

6
e is 65537 (0x010001)

7
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ openssl req -sha1 -new -x509 -r
```

Création de la clef serveur et du certificat serveur

Exécutez les commandes suivantes pour créer la clé SSL et le certificat du serveur:

```
3

1
openssl req -sha1 -newkey rsa:2048 -days 3650 -nodes -keyout ./ssl_keys/server-key.pem > ./s

2
openssl x509 -sha1 -req -in ./ssl_keys/server-req.pem -days 3650 -CA ./ssl_keys/ca-cert.pem

3
openssl rsa -in ./ssl_keys/server-key.pem -out ./ssl_keys/server-key.pem
```

Création de la clef serveur et du certificat client

Exécutez les commandes suivantes pour créer la clé SSL et le certificat du client:

3

1

```
openssl req -sha1 -newkey rsa:2048 -days 3650 -nodes -keyout ./ssl_keys/client-key.pem > ./s
```

2

```
openssl x509 -sha1 -req -in ./ssl_keys/client-req.pem -days 3650 -CA ./ssl_keys/ca-cert.pem
```

3

```
openssl rsa -in ./ssl_keys/client-key.pem -out ./ssl_keys/client-key.pem
```

Sortie de OpenSSL

Pour avoir de bon certifiact, il est important de selectionner des CN différents pour les CA, server et client

77

1

```
pilou@lubuntu:~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ ./ssl.sh
```

2

```
Generating RSA private key, 2048 bit long modulus (2 primes)
```

3

```
.....................................................+++++
```

4

```
.............................+++++
```

5

```
e is 65537 (0x010001)
```

6

```
You are about to be asked to enter information that will be incorporated
```

7

```
into your certificate request.
```

8

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

9

```
There are quite a few fields but you can leave some blank
```

10

```
For some fields there will be a default value,
```

11

```
If you enter '.', the field will be left blank.
```

12

```
-----
```

13

```
Country Name (2 letter code) [AU]:
```

14

```
State or Province Name (full name) [Some-State]:
```

```
Locality Name (eg, city) []:
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
```

```
Organizational Unit Name (eg, section) []:
```

```
Common Name (e.g. server FQDN or YOUR name) []:CA
```

```
Email Address []:
```

```
Ignoring -days; not generating a certificate
```

```
Generating a RSA private key
```

```
.............+++++
```

```
.....................................+++++
```

```
writing new private key to '/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys
```

```
-----
```

```
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
```

30

```
For some fields there will be a default value,
```

31

```
If you enter '.', the field will be left blank.
```

32

```
-----
```

33

```
Country Name (2 letter code) [AU]:
```

34

```
State or Province Name (full name) [Some-State]:
```

35

```
Locality Name (eg, city) []:
```

36

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
```

37

```
Organizational Unit Name (eg, section) []:
```

38

```
Common Name (e.g. server FQDN or YOUR name) []:server
```

39

```
Email Address []:
```

40

```
□
```

41

```
Please enter the following 'extra' attributes
```

42

```
to be sent with your certificate request
```

43

```
A challenge password []:
```

```
An optional company name []:
```

```
Signature ok
```

```
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = server
```

```
Getting CA Private Key
```

```
writing RSA key
```

```
Ignoring -days; not generating a certificate
```

```
Generating a RSA private key
```

```
.................................+++++
```

```
.....................+++++
```

```
writing new private key to '/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys
```

```
-----
```

```
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
```

59

```
For some fields there will be a default value,
```

60

```
If you enter '.', the field will be left blank.
```

61

```
-----
```

62

```
Country Name (2 letter code) [AU]:
```

63

```
State or Province Name (full name) [Some-State]:
```

64

```
Locality Name (eg, city) []:
```

65

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
```

66

```
Organizational Unit Name (eg, section) []:
```

67

```
Common Name (e.g. server FQDN or YOUR name) []:client
```

68

```
Email Address []:
```

69

```
□
```

70

```
Please enter the following 'extra' attributes
```

71

```
to be sent with your certificate request
```

72

```
A challenge password []:
```

73

```
An optional company name []:
```

74

```
Signature ok
```

75

```
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = client
```

76

```
Getting CA Private Key
```

77

```
writing RSA key
```

Modification de MySQL

Il faut indiquer à MySQL ou se trouve les différentes clefs et certificat:

24

1
```
[mysqld]
```

2
```
port = 3306
```

3
```
socket = /tmp/mysql.sock
```

4
```
skip-external-locking
```

5
```
key_buffer_size = 16K
```

6
```
max_allowed_packet = 1M
```

7
```
table_open_cache = 4
```

8
```
sort_buffer_size = 64K
```

9
```
read_buffer_size = 256K
```

10
```
read_rnd_buffer_size = 256K
```

11
```
net_buffer_length = 2K
```

12
```
thread_stack = 128K
```

13
```
table_open_cache=500
```

14
```
secure_file_priv=/tmp
```

15

```
max_connections = 400
```

16

```
max_user_connections=200
```

17

```
ssl-ca=/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/ca-cert.pem
```

18

```
ssl-cert=/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/server-cert.pem
```

19

```
ssl-key=/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/server-key.pem
```

20

```
ssl-cipher=DHE-RSA-AES256-SHA
```

21

```

```

22

```
[client]
```

23

```
ssl-cert=/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/client-cert.pem
```

24

```
ssl-key=/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/client-key.pem
```

Après redemarrage, le serveur signale que le certificat est auto signé

2

1

```
2019-01-05T08:44:05.815408Z 0 [Warning] [MY-010068] [Server] CA certificate
```

2

```
/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/ca-cert.pem is self signed.
```

et les parametre SSL sont bien chargé

```
SHOW VARIABLES LIKE '%ssl%';
+-------------------+-----------------------------------------------------------------------------
| Variable_name |  Value |
 +-------------------+-----------------------------------------------------------------------------
| have_openssl |  YES |
| have_ssl |  YES |
| mysqlx_ssl_ca | |
| mysqlx_ssl_capath | |
| mysqlx_ssl_cert | |
| mysqlx_ssl_cipher | |
| mysqlx_ssl_crl | |
| mysqlx_ssl_crlpath | |
| mysqlx_ssl_key | |
```

```
| ssl_ca | /home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/ca-cert.pem |
| ssl_capath | |
| ssl_cert | /home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/server-cert.pe
| ssl_cipher | |
| ssl_crl | |
| ssl_crlpath | |
| ssl_fips_mode | OFF |
| ssl_key | /home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64/ssl_keys/server-key.pem
+--------------------+------------------------------------------------------------------------
17 rows in set (0,01 sec)
```

Test

Nous allons nous connecter en SSL sur le serveur en demandant explicitement a utiliser la connection TCP (ce qui force l'utilisation de SSL)

34

1

```
pilou@lubuntu: ~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ ./bin/mysql --defaults-file=/hc
```

2

```
Enter password:
```

3

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

4

```
Your MySQL connection id is 8
```

5

```
Server version: 8.0.13 MySQL Community Server - GPL
```

6

```

```

7

```
Copyright (c) 2000, 2018, Oracle and/or its affiliates.  All rights reserved.
```

8

```

```

9

```
Oracle is a registered trademark of Oracle Corporation and/or its
```

10

```
affiliates.  Other names may be trademarks of their respective
```

11

```
owners.
```

12

```

```

13

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

14

```

```

```
mysql> status
--------------
./bin/mysql  Ver 8.0.13 for linux-glibc2.12 on x86_64 (MySQL Community Server - GPL)

Connection id:          8
Current database:
Current user:           root@localhost
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.13 MySQL Community Server - GPL
Protocol version:       10
Connection:             localhost via TCP/IP
```

```
Server characterset: utf8mb4
```

30

```
Db characterset: utf8mb4
```

31

```
Client characterset: utf8mb4
```

32

```
Conn. characterset: utf8mb4
```

33

```
TCP port: 3306
```

34

```
Uptime: 20 sec
```

Installation de SSL pour MariaDB

Créez un répertoire nommé ssl dans le répertoire /etc/mysql/

3

1

```
$ cd /etc/mysql
```

2

```
$ sudo mkdir ssl
```

3

```
$ cd ssl
```

```
4

1
La valeur du nom commun utilisée pour les certificats/clés du serveur et du client doit être

2
Nom commun de l'AC : administrateur MariaDB

3
Nom commun du serveur : serveur MariaDB

4
Nom commun du client : client MariaDB
```

Tapez la commande suivante pour créer une nouvelle autorité de certification:

Installation de SSL avec MariaDB sous Debian

Modifiez le fichier /etc/mysql/mariadb.conf.d/50-server.cnf (ou /etc/mysql/mariadb.cnf) comme suit :zLa valeur du nom commun utilisée pour les certificats/clés du serveur et du client doit être différente de la valeur du nom commun utilisée pour le certificat CA. Pour éviter tout problème, je les règle comme suit. Sinon, vous obtiendrez une erreur d'échec de la vérification de la certification. Par conséquent, définissez-le comme suit :
Nom commun de l'AC : administrateur MariaDB
Nom commun du serveur : serveur MariaDB
Nom commun du client : client MariaDB

Créez un répertoire nommé ssl dans le répertoire /etc/mysql/

```
$ cd /etc/mysql
$ sudo mkdir ssl
$ cd ssl
```

Tapez la commande suivante pour créer une nouvelle clé CA :

```
sudo openssl genrsa 4096 > ca-key.pem
```

Tapez la commande suivante pour générer le certificat à l'aide de cette clé :

```
$ sudo openssl req -new -x509 -nodes -days 365000 -key ca-key.pem -out ca-cert.pem
```

Maintenant, vous devez avoir deux fichiers comme suit :

- /etc/mysql/ssl/ca-cert.pem – Fichier de certificat pour l'autorité de certification (CA).
- /etc/mysql/ssl/ca-key.pem – Fichier clé pour l'autorité de certification (CA).

Créer le certificat SSL du serveur

Pour créer la clé du serveur, exécutez :

```
sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout server-key.pem -out server-req.pem
```

Ensuite, créer la clé RSA du serveur, saisissez :

```
openssl rsa -in server-key.pem -out server-key.pem
```

Enfin, signez le certificat du serveur, exécutez :

```
openssl x509 -req -in server-req.pem -days 365000 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 -out server-cert.pem
```

Maintenant, vous devez avoir des fichiers supplémentaires :

- /etc/mysql/ssl/server-cert.pem – Fichier de certificat du serveur MariaDB.
- /etc/mysql/ssl/server-key.pem – Fichier de clé du serveur MariaDB.

Vous devez utiliser les deux fichiers ci-dessus sur le serveur MariaDB lui-même et sur tout autre nœud que vous allez utiliser pour le trafic de cluster/réplication. Ces deux fichiers sécuriseront la communication côté serveur.

Configurer le serveur MariaDB pour utiliser SSL

Modifiez le fichier /etc/mysql/mariadb.conf.d/50-server.cnf comme suit :

```
### MySQL Server ###
## Securing the Database with ssl option and certificates ##
## There is no control over the protocol level used.  ##
##  mariadb will use TLSv1.0 or better.   ##
#ssl
ssl-ca=/etc/mysql/ssl/ca-cert.pem
ssl-cert=/etc/mysql/ssl/server-cert.pem
ssl-key=/etc/mysql/ssl/server-key.pem
## Set up TLS version here.  For example TLS version 1.2 and 1.3 ##
tls_version = TLSv1.2,TLSv1.3
```

Enregistrez et fermez le fichier. Sécurisez les clés à l'aide de la commande chmod/commande chown :

```
 sudo chown -Rv mysql:root /etc/mysql/ssl/
```