

# 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 verrouiller 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@ubuntu: ~/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@ubuntu: ~/mysql80/mysql-8.0.13-linux-glibc2.12-x86_64$ mkdir ssl_keys
```

2

```
pilou@ubuntu: ~/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@ubuntu: ~/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@ubuntu: ~/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]:

15

Locality Name (eg, city) []:

16

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

17

Organizational Unit Name (eg, section) []:

18

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

19

Email Address []:

20

Ignoring -days; not generating a certificate

21

Generating a RSA private key

22

.....+++++

23

.....+++++

24

writing new private key to '/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86\_64/ssl\_keys

25

-----

26

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

27

into your certificate request.

28

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

29

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 []:

44

An optional company name []:

45

Signature ok

46

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

47

Getting CA Private Key

48

writing RSA key

49

Ignoring -days; not generating a certificate

50

Generating a RSA private key

51

.....+++++

52

.....+++++

53

writing new private key to '/home/pilou/mysql80/mysql-8.0.13-linux-glibc2.12-x86\_64/ssl\_keys

54

-----

55

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

56

into your certificate request.

57

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

58

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 où se trouvent les différentes clés et certificats:

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





# 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@ubuntu: ~/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

□

15

```
mysql> status
```

16

```
-----
```

17

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

18

□

19

```
Connection id: 8
```

20

```
Current database:
```

21

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

22

```
SSL: Cipher in use is DHE-RSA-AES256-SHA
```

23

```
Current pager: stdout
```

24

```
Using outfile: ''
```

25

```
Using delimiter: ;
```

26

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

27

```
Protocol version: 10
```

28

```
Connection: localhost via TCP/IP
```

29

Server charsetset: utf8mb4

30

Db charsetset: utf8mb4

31

Client charsetset: utf8mb4

32

Conn. charsetset: 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:

---

Revision #6

Created 24 November 2019 14:22:10 by Admin

Updated 10 November 2021 06:30:53 by ggpilou2