

ASGBD2 Tarea 3: Conexiones seguras

Objetivos:

- Verificar si una base de datos permite conexiones seguras.
- Comprender las distintas opciones de conexiones seguras SSL en los usuarios y configurarlas.
- Generan nuevos certificados y configurar la BD para que utilice estos certificados.

Requisitos:

- El servidor de base de datos a utilizar es la base de datos de mysql versión 5.7.28 instalada en la máquina virtual de Ubuntu
- Como cliente utilizamos la máquina virtual Windows con la herramienta Workbench

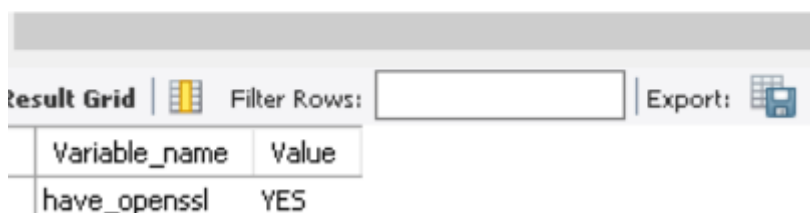
Ejercicio

1. **[0,5 puntos]** Verifica si el servidor de base de datos tiene soporte para openssl. Argumenta tu respuesta.
Desde el servidor

```
mysql> SHOW VARIABLES LIKE '%openssl%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_openssl  | YES   |
+-----+-----+
1 row in set (0.00 sec)
```

Desde el cliente Workbench

```
1 • show variables like '%openssl%'
```



Result Grid	Filter Rows:	Export:
Variable_name	Value	
have_openssl	YES	

2. **[0,5 puntos]** Verifica si el servidor de base de datos tiene activada la seguridad. Que muestre los parámetros relacionados con la seguridad.

```
mysql> show variables like '%ssl%'
-> ;
```

Variable_name	Value
admin_ssl_ca	
admin_ssl_capath	
admin_ssl_cert	
admin_ssl_cipher	
admin_ssl_crl	
admin_ssl_crlpath	
admin_ssl_key	
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	
performance_schema_show_processlist	OFF
ssl_ca	ca.pem
ssl_capath	
ssl_cert	server-cert.pem
ssl_cipher	
ssl_crl	
ssl_crlpath	
ssl_fips_mode	OFF
ssl_key	server-key.pem

```
25 rows in set (0,00 sec)

mysql>
```

1 • `show variables like '%ssl%'`

Result Grid		Filter Rows:	Export:	Wrap
Variable_name	Value			
have_openssl	YES			
have_ssl	YES			
ssl_ca	ca.pem			
ssl_capath				
ssl_cert	server-cert.pem			
ssl_cipher				
ssl_crl				
ssl_crlpath				
ssl_key	server-key.pem			

3. [0,5 puntos] Muestra el directorio donde se encuentran los certificados actualmente generados.

```
mysql> show variables like '%datadir%';
```

Variable_name	Value
datadir	/var/lib/mysql/

```
1 row in set (0.01 sec)
```

```

root@pedroperez2:/var/lib/mysql# ls *.pem
ca-key.pem  client-cert.pem  private_key.pem  server-cert.pem
ca.pem      client-key.pem   public_key.pem   server-key.pem
root@pedroperez2:/var/lib/mysql#

```

4. **[0,5 puntos]** ¿Cuál es la configuración actual del servidor para conexiones cifradas? Argumenta tu respuesta.

La opción `--ssl` especifica que el servidor permite, pero no requiere conexiones encriptadas. Esta opción está habilitada de manera predeterminada, por lo que no necesita especificarse explícitamente. Para requerir que los clientes se conecten usando conexiones encriptadas, se debe habilitar la variable del sistema `'require_secure_transport'`.

Para más información: <https://dev.mysql.com/doc/refman/8.0/en/using-encrypted-connections.html>

```

pedropq@pedroperez2: /etc/mysql
mysql> show variables like '%ssl%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| admin_ssl_ca  |      |
| admin_ssl_capath |      |
| admin_ssl_cert |      |
| admin_ssl_cipher |      |
| admin_ssl_crl |      |
| admin_ssl_crlpath |      |
| admin_ssl_key |      |
| 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 |      |
| performance_schema_show_processlist | OFF |
| ssl_ca        | ca.pem |
| ssl_capath    |      |
| ssl_cert      | server-cert.pem |
| ssl_cipher    |      |
| ssl_crl       |      |
| ssl_crlpath   |      |
| ssl_fips_mode | OFF  |
| ssl_key       | server-key.pem |
+-----+-----+
25 rows in set (0,00 sec)

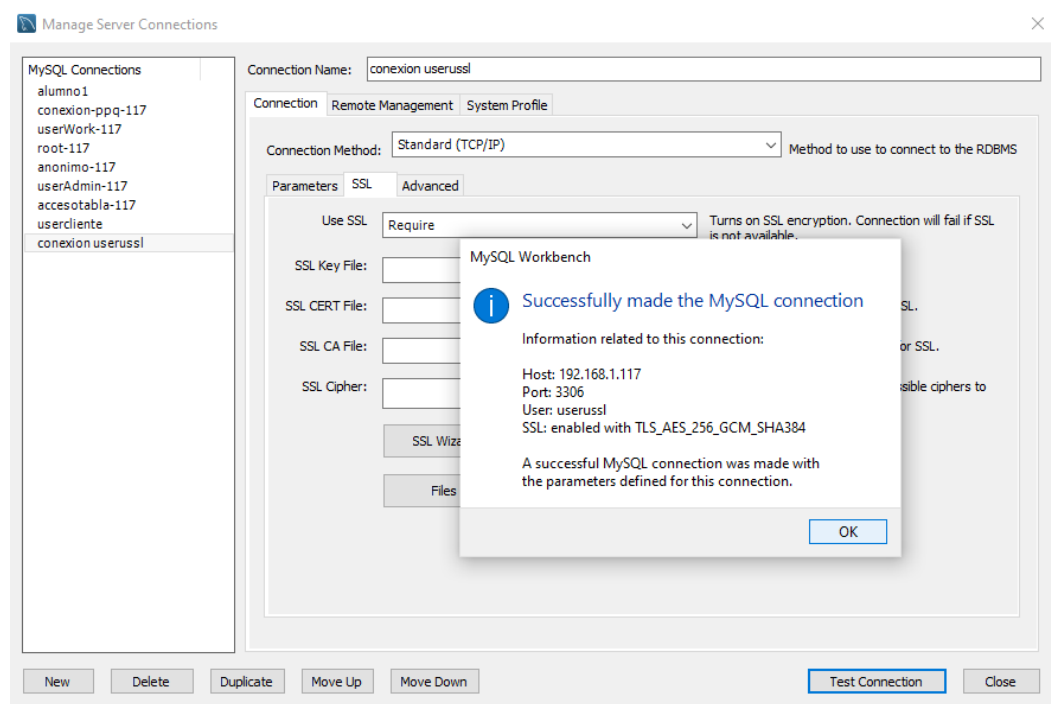
mysql> show variables like '%require_secure_transport%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| require_secure_transport | OFF |
+-----+-----+
1 row in set (0,00 sec)

mysql>

```

5. **[1,5 puntos]** Crea un usuario denominado `userussl`, que tenga la misma clave y que requiera que la conexión sea segura. Verifica la conexión desde la consola de Ubuntu y desde Workbench.

create user userussl@'%' identified by 'userussl' require ssl;



```
pedropq@pedroperez2:/etc/mysql$ mysql -u userussl -puserussl -h 127.0.0.1
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

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.

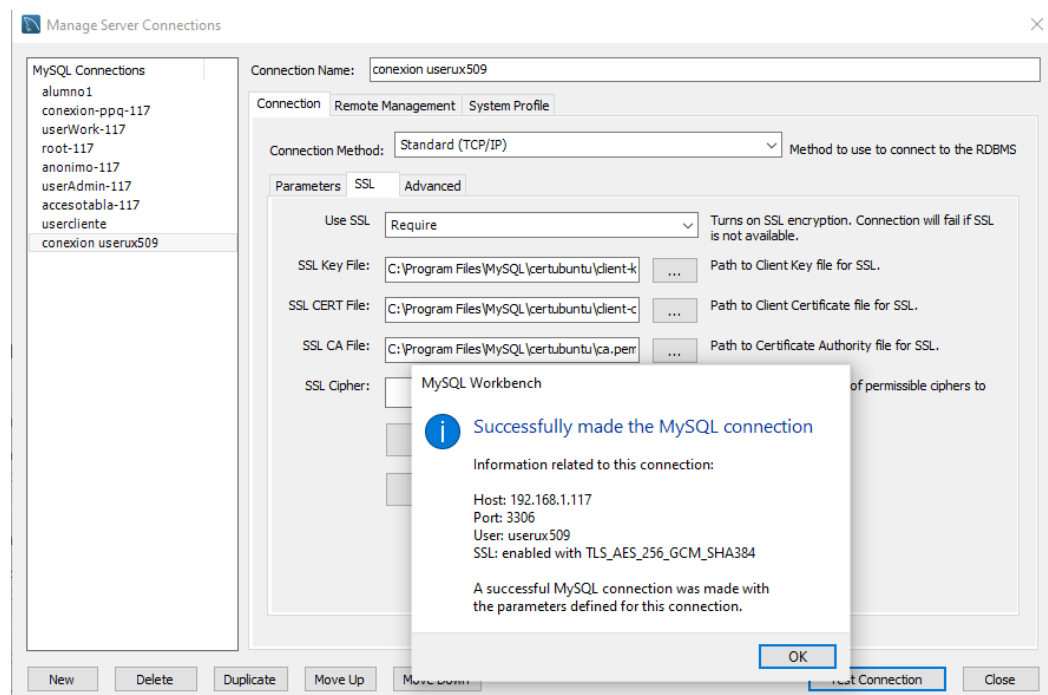
mysql>
```

6. [1,5 puntos]Crea un usuario denominado userux509 y misma password, que requiera que presente un certificado válido. Verifica la conexión desde la consola de Ubuntu y desde Workbench.

create user userux509@'%' identified by 'userux509' require x509;

Para poder realizar la conexión desde el workbench en la máquina Windows, lo primero que realizo es poner los certificados de la maquina Ubuntu en un

directorio de la maquina Windows, por ejemplo, en C:\Program Files\MySQL\certubuntu



```
root@pedroperez2:/var/lib/mysql# mysql -u userux509 -p --ssl-key='/var/lib/mysql/
/client-key.pem' --ssl-cert='/var/lib/mysql/client-cert.pem' -h 127.0.0.1
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 35
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

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>
```

mysql -u userux509 -p --ssl-key='/var/lib/mysql/client-key.pem' --ssl-cert='/var/lib/mysql/client-cert.pem' -h 127.0.0.1

7. [1 punto] Conéctate con el usuario userussl y muestra la información del certificado.

```
mysql> \s
-----
mysql Ver 8.0.27-0ubuntu0.20.04.1 for Linux on x86_64 ((Ubuntu))

Connection id:          36
Current database:
Current user:           userussl@localhost
SSL:                   Cipher in use is TLS_AES_256_GCM_SHA384
Current pager:         stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.27-0ubuntu0.20.04.1 (Ubuntu)
Protocol version:       10
Connection:             127.0.0.1 via TCP/IP
Server characterset:    utf8mb4
Db      characterset:    utf8mb4
Client characterset:    utf8mb4
Conn.  characterset:    utf8mb4
TCP port:               3306
Binary data as:         Hexadecimal
Uptime:                 3 hours 49 min 17 sec

Threads: 2  Questions: 189  Slow queries: 0  Opens: 242  Flush tables: 3  Open t
ables: 161  Queries per second avg: 0.013
-----
mysql>
```

8. [0,5 puntos] Verifica el periodo de validez del certificado.

```
mysql> show status like '%not%'
-> ;
+-----+-----+
| Variable_name | Value |
+-----+-----+
| Key_blocks_not_flushed | 0 |
| Mysqlx_notice_global_sent | 0 |
| Mysqlx_notice_other_sent | 0 |
| Mysqlx_notice_warning_sent | 0 |
| Mysqlx_notified_by_group_replication | 0 |
| Mysqlx_ssl_server_not_after | Oct  2 16:45:09 2031 GMT |
| Mysqlx_ssl_server_not_before | Oct  4 16:45:09 2021 GMT |
| Mysqlx_stmt_disable_notices | 0 |
| Mysqlx_stmt_enable_notices | 0 |
| Mysqlx_stmt_list_notices | 0 |
| Not_flushed_delayed_rows | 0 |
| Ssl_server_not_after | Oct  2 16:45:09 2031 GMT |
| Ssl_server_not_before | Oct  4 16:45:09 2021 GMT |
+-----+-----+
13 rows in set (0,00 sec)

mysql>
```

9. [0,5 puntos] Mira el contenido del certificado ca.pem, tienes que utilizar el openssl

```

root@pedroperez2:/var/lib/mysql# openssl x509 -text -in ca.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = MySQL_Server_8.0.26_Auto_Generated_CA_Certificate
        Validity
            Not Before: Oct  4 16:45:09 2021 GMT
            Not After : Oct  2 16:45:09 2031 GMT
        Subject: CN = MySQL_Server_8.0.26_Auto_Generated_CA_Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d4:06:b1:b8:b1:53:99:50:d8:63:90:94:31:55:
                    7a:ed:cl:c8:b3:ac:f9:3e:7d:2a:87:ae:28:e8:18:
                    01:d6:58:2c:db:b2:e7:fc:82:ec:7b:85:fa:2f:0a:

```

10. **[3 puntos]** Genera unos nuevos certificados y modifica la configuración de la bd para que utilice estos nuevos certificados, demuestra que esta utiliza los nuevos certificados y el periodo de validez generado.

Ver la utilidad <https://dev.mysql.com/doc/refman/8.0/en/mysql-ssl-rsa-setup.html>

Opciones que he utilizado

--verbose, --datadir

Creo un nuevo directorio nuevoscert dentro de /var/lib/mysql, la ruta completa es: /var/lib/mysql/nuevoscert

`# mysql_ssl_rsa_setup --datadir='/var/lib/mysql/nuevoscert' --verbose`

```

root@pedroperez2:/var/lib/mysql/nuevoscert# mysql_ssl_rsa_setup --datadir='/var/lib/mysql/nuevoscert' --verbose
2021-11-22 20:56:04 [NOTE] Destination directory: /var/lib/mysql/nuevoscert
2021-11-22 20:56:04 [NOTE] Executing : openssl version
OpenSSL 1.1.1f 31 Mar 2020
2021-11-22 20:56:05 [NOTE] Executing : openssl req -newkey rsa:2048 -days 3650 -nodes -keyout ca-key.pem -subj /CN=MySQL_Server_8.0.27_Auto_Generated_CA_Certificate -out ca-req.pem && openssl rsa -in ca-key.pem -out ca-key.pem
Ignoring -days; not generating a certificate
Generating a RSA private key
.....+++++
....+++++
writing new private key to 'ca-key.pem'
-----
writing RSA key
2021-11-22 20:56:05 [NOTE] Executing : openssl x509 -sha256 -days 3650 -ext

```

En el directorio se han generado:

```

root@pedroperez2:/var/lib/mysql/nuevoscert# ls -l
total 32
-rw----- 1 root root 1679 nov 22 20:56 ca-key.pem
-rw-r--r-- 1 root root 1107 nov 22 20:56 ca.pem
-rw-r--r-- 1 root root 1107 nov 22 20:56 client-cert.pem
-rw----- 1 root root 1675 nov 22 20:56 client-key.pem
-rw----- 1 root root 1679 nov 22 20:56 private_key.pem
-rw-r--r-- 1 root root 451 nov 22 20:56 public_key.pem
-rw-r--r-- 1 root root 1107 nov 22 20:56 server-cert.pem
-rw----- 1 root root 1675 nov 22 20:56 server-key.pem
root@pedroperez2:/var/lib/mysql/nuevoscert#

```

Cambio para que el grupo y usuario de todo lo creado sea mysql

chown -R mysql:mysql nuevoscrt

Modifico el fichero de configuración de mysql que se encuentra en /etc/mysql/my.cnf donde finalmente se encuentra

/etc/mysql/mysql.conf.d/ El fichero mysqld.cnf

```
# binlog_ignore_db = include_database_name

# variables de los nuevos certificados

ssl_ca=/var/lib/mysql/nuevoscrt/ca.pem
ssl_cert=/var/lib/mysql/nuevoscrt/server-cert.pem
ssl_key=/var/lib/mysql/nuevoscrt/server-key.pem
[client]
ssl-ca =/var/lib/mysql/nuevoscrt/ca.pem
ssl-cert = /var/lib/mysql/nuevoscrt/client-cert.pem
ssl-key = /var/lib/mysql/nuevoscrt/client-key.pem
```

Reinicio el servidor

Systemctl restart mysql

```
mysql> show variables like '%ssl%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| admin_ssl_ca  |      |
| admin_ssl_capath |      |
| admin_ssl_cert |      |
| admin_ssl_cipher |      |
| admin_ssl_crl |      |
| admin_ssl_crlpath |      |
| admin_ssl_key |      |
| 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 |      |
| performance_schema_show_processlist | OFF |
| ssl_ca        | /var/lib/mysql/nuevoscrt/ca.pem |
| ssl_capath    |      |
| ssl_cert      | /var/lib/mysql/nuevoscrt/server-cert.pem |
| ssl_cipher    |      |
| ssl_crl       |      |
| ssl_crlpath   |      |
| ssl_fips_mode | OFF  |
| ssl_key       | /var/lib/mysql/nuevoscrt/server-key.pem |
+-----+-----+
```


Compruebo la conexión con los nuevos certificados

```
root@pedroperez2:/etc/mysql/mysql.conf.d# mysql -u userux509 -p --ssl-key='/var/lib/mysql/nuevoscert/client-key.pem' --ssl-cert='/var/lib/mysql/nuevoscert/client-cert.pem' -h 127.0.0.1
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

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.
```

Información del usuario userux509 y su conexión segura

```
mysql> mysql \s
-----
mysql Ver 8.0.27-0ubuntu0.20.04.1 for Linux on x86_64 ((Ubuntu))

Connection id:          9
Current database:
Current user:            userux509@localhost
SSL:                    Cipher in use is TLS_AES_256_GCM_SHA384
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.27-0ubuntu0.20.04.1 (Ubuntu)
Protocol version:       10
Connection:             127.0.0.1 via TCP/IP
Server characterset:    utf8mb4
Db characterset:        utf8mb4
Client characterset:    utf8mb4
Conn. characterset:     utf8mb4
TCP port:               3306
Binary data as:         Hexadecimal
Uptime:                 7 min 55 sec

Threads: 2  Questions: 8  Slow queries: 0  Opens: 134  Flush tables: 3  Open tables: 53  Queries per second
avg: 0.016
```

Se han generado unos nuevos certificados para otros 10 años

```
mysql> show status like '%not%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| Key_blocks_not_flushed | 0 |
| Mysqlx_notice_global_sent | 0 |
| Mysqlx_notice_other_sent | 0 |
| Mysqlx_notice_warning_sent | 0 |
| Mysqlx_notified_by_group_replication | 0 |
| Mysqlx_ssl_server_not_after | Nov 20 20:56:05 2031 GMT |
| Mysqlx_ssl_server_not_before | Nov 22 20:56:05 2021 GMT |
| Mysqlx_stmt_disable_notices | 0 |
| Mysqlx_stmt_enable_notices | 0 |
| Mysqlx_stmt_list_notices | 0 |
| Not_flushed_delayed_rows | 0 |
| Ssl_server_not_after | Nov 20 20:56:05 2031 GMT |
| Ssl_server_not_before | Nov 22 20:56:05 2021 GMT |
+-----+-----+
13 rows in set (0,01 sec)
```