



# Estableciendo Sesiones SSL en MySQL



# Estableciendo Sesiones SSL en MySQL

## Objetivos:

- Crear la infraestructura de certificados X.509 necesaria para incorporar servicios de seguridad en el acceso a un Base de Datos
- Establecer de forma práctica sesiones seguras en MySQL
- Captura del tráfico en el acceso a la BD



# Índice

- Creación de la Infraestructura necesaria para el establecimiento de accesos seguros SSL
  - Usuario cliente\_ssl0: Cliente SSL sin Autenticación de usuario
  - Usuario cliente\_ssl: Cliente SSL con Autenticación de usuario
- Gestión del servidor MySQL para el arranque con servicios de seguridad
- Creación de los usuarios con los específicos servicios de seguridad requeridos.
- Captura Tráfico SSL

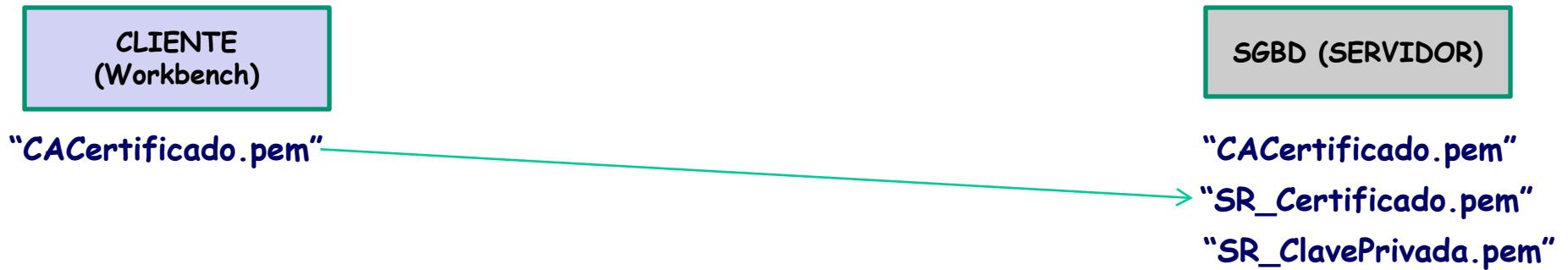


# Índice (II)

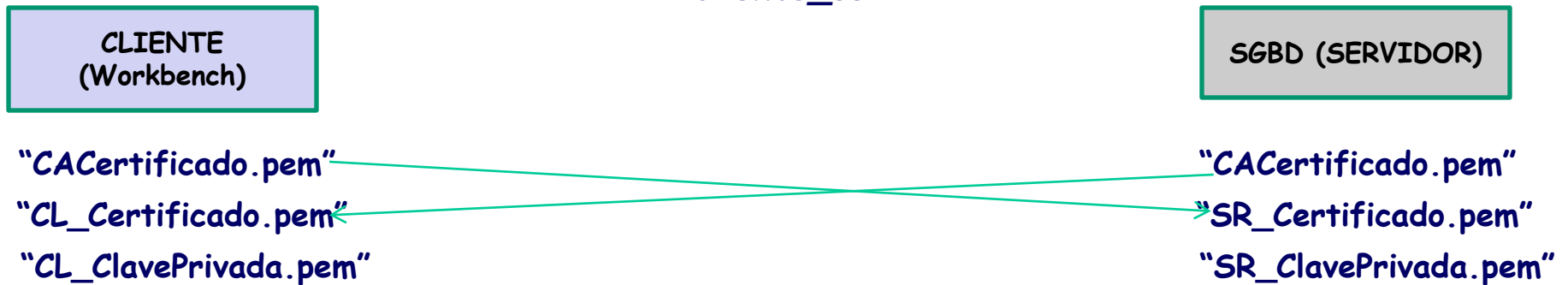
1. Crear certificado y clave Autoridad de Certificación
2. Crear Ficheros Certificados y Clave Servidor
3. Crear Ficheros Certificados y Clave Cliente
4. Comprobar SSL
5. Configuración Manual SSL
6. Configuración Automática SSL
7. Crear *cliente\_ssl0*
8. Crear *cliente\_ssl0*
9. Captura de Tráfico

# Infraestructura de Seguridad

## 1. Protocolo SSL sin Autenticación de cliente *cliente\_ssl0*



## 2. Protocolo SSL con Autenticación de cliente *cliente\_ssl*





# 1. Crear Certificados y Clave CA

`openssl>`

`genrsa -out CAClavePrivada.pem 4096`

(Generamos un par de claves pública y privada. Obtenemos el fichero "CAClavePrivada.pem" conteniendo la clave privada de la CA)

`req -new -x509 -days 3650 -key CAClavePrivada.pem -out CACertificado.pem`

(Obtenemos un certificado autofirmado, fichero "CACertificado.pem", que será el certificado de la CA)

`x509 -inform PEM -in CACertificado.pem -outform DER -out CACertificado.crt`

(Podemos convertir el formato \*.pem del certificado a formato \*.crt)



## 2.Crear Certificados y Clave SR (I)

```
genrsa -out SR_ClavePrivada.pem 1024
```

(Generamos un par de claves pública y privada para el usuario. Obtenemos el fichero "SR\_ClavePrivada.pem" conteniendo la clave privada del servidor)

```
req -new -key SR_ClavePrivada.pem -out SR_Peticion.csr
```

(Creamos un certificado de usuario y creamos una petición a la espera que la firme la CA)

```
x509 -req -days 365 -in SR_Peticion.csr -CA CACertificado.pem  
-CAkey CAClavePrivada.pem -set_serial 01 -out SR_Certificado.pem
```

(obtenemos un certificado firmado por la CA, listo para ser utilizado en el Gestor de la BD, servidor)



## 2.Crear Certificados y Clave SR (II)

```
x509 -inform PEM -in SR_Certificado.pem -outform DER  
-out SR_Certificado.crt
```

(opcionalmente podemos obtener el fichero del certificado del servidor en formato \*.crt)

```
pkcs12 -export -in SR_Certificado.pem -inkey SR_ClavePrivada.pem  
-out SR_Certificado.p12
```

(opcionalmente podemos obtener el fichero del certificado del servidor en formato \*.p12, incorporando la clave privada)





### 3.Crear Certificados y Clave CL (I)

```
genrsa -out CL_ClavePrivada.pem 1024
```

(Generamos un par de claves pública y privada para el usuario. Obtenemos el fichero "CLClavePrivada.pem" conteniendo la clave privada del cliente)

```
req -new -key CL_ClavePrivada.pem -out CL_Peticion.csr
```

(Creamos un certificado de usuario y creamos una petición a la espera que la firme la CA)

```
x509 -req -days 365 -in CL_Peticion.csr -CA CACertificado.pem  
-CAkey CAClavePrivada.pem -set_serial 02 -out CL_Certificado.pem
```

(obtenemos un certificado firmado por la CA, listo para ser utilizado en el cliente)



## 3. Crear Certificados y Clave CL (II)

```
x509 -inform PEM -in CL_Certificado.pem -outform DER  
-out CL_Certificado.crt
```

(opcionalmente podemos obtener el fichero del certificado del cliente en formato \*.crt)

```
pkcs12 -export -in CL_Certificado.pem -inkey CL_ClavePrivada.pem  
-out CL_Certificado.p12
```

(opcionalmente podemos obtener el fichero del certificado del cliente en formato \*.p12, incorporando la clave privada)

## 4. Comprobar SSL

1. Desde el servidor MySQL (abrir una consola en Dir *C:\xampp\mysql\bin*)  
`mysqld --ssl`  
[ERROR] mysql: unknown option '--ssl' -> Esto indica que no soporta SSL

2. Desde un cliente (abrir una consola en Directorio:  
*C:\Program Files\MySQL\MySQL Workbench 6.2 CE*)

`mysql -u root`

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

Your MySQL connection id is 1

Server version: 5.1.37 Source distribution

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

`mysql> SHOW VARIABLES LIKE "have_ssl";`

```
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_ssl      | YES   |
+-----+-----+
1 row in set (0.00 sec)
```



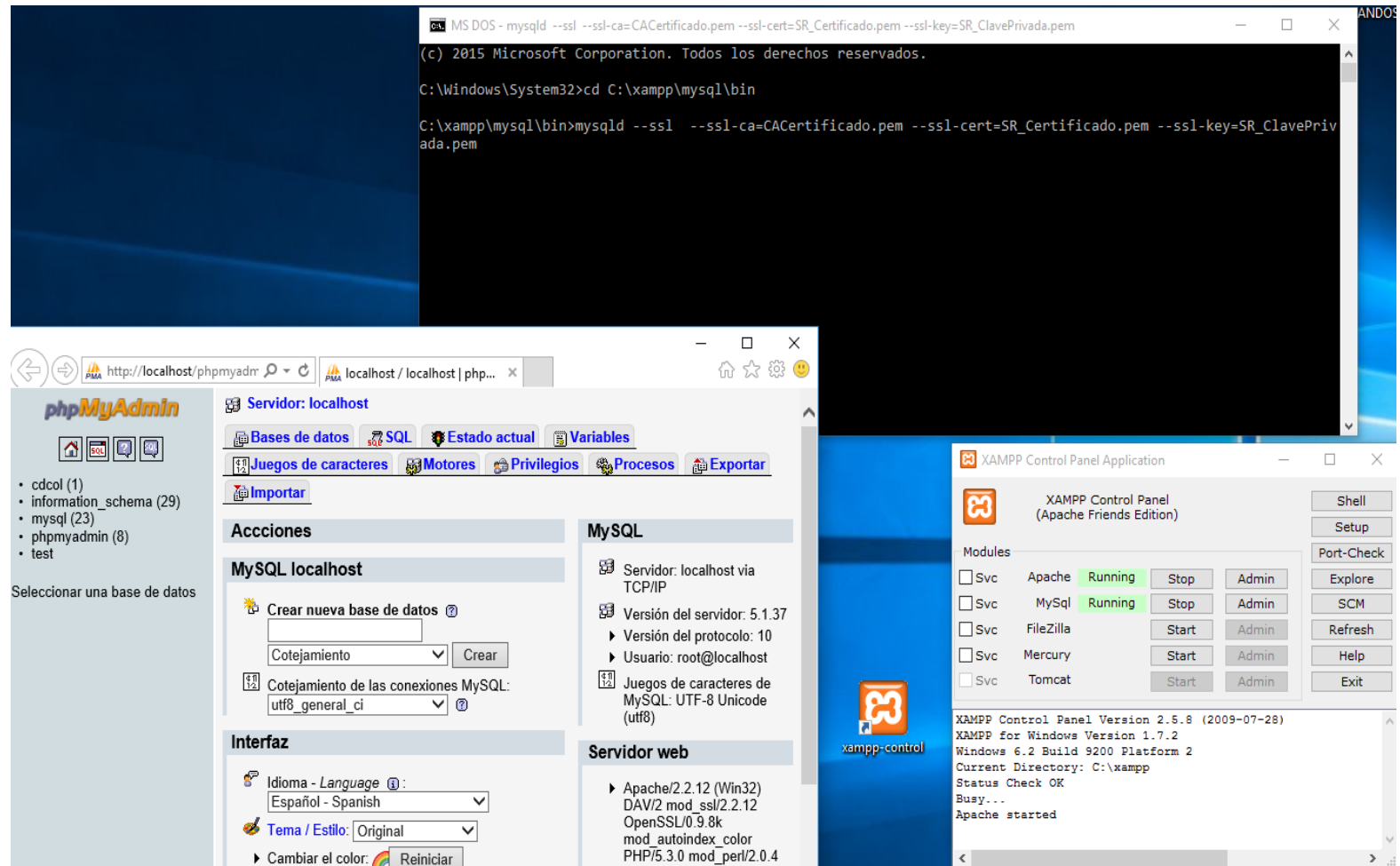
## 5. Configuración Manual SSL (I)

1. Se copiarán en el directorio "*C:\xampp\mysql\bin*" los *ficheros: CACertificado.pem, SR\_Certificado.pem y SR\_ClavePrivada.pem*
2. Se abrirá una consola en el directorio "*C:\xampp\mysql\bin*" y se ejecutará el comando *(Arranque manual del Servidor MySQL):*

```
mysqld --ssl --ssl-ca=CACertificado.pem --ssl-cert=SR_Certificado.pem  
--ssl-key=SR_ClavePrivada.pem
```

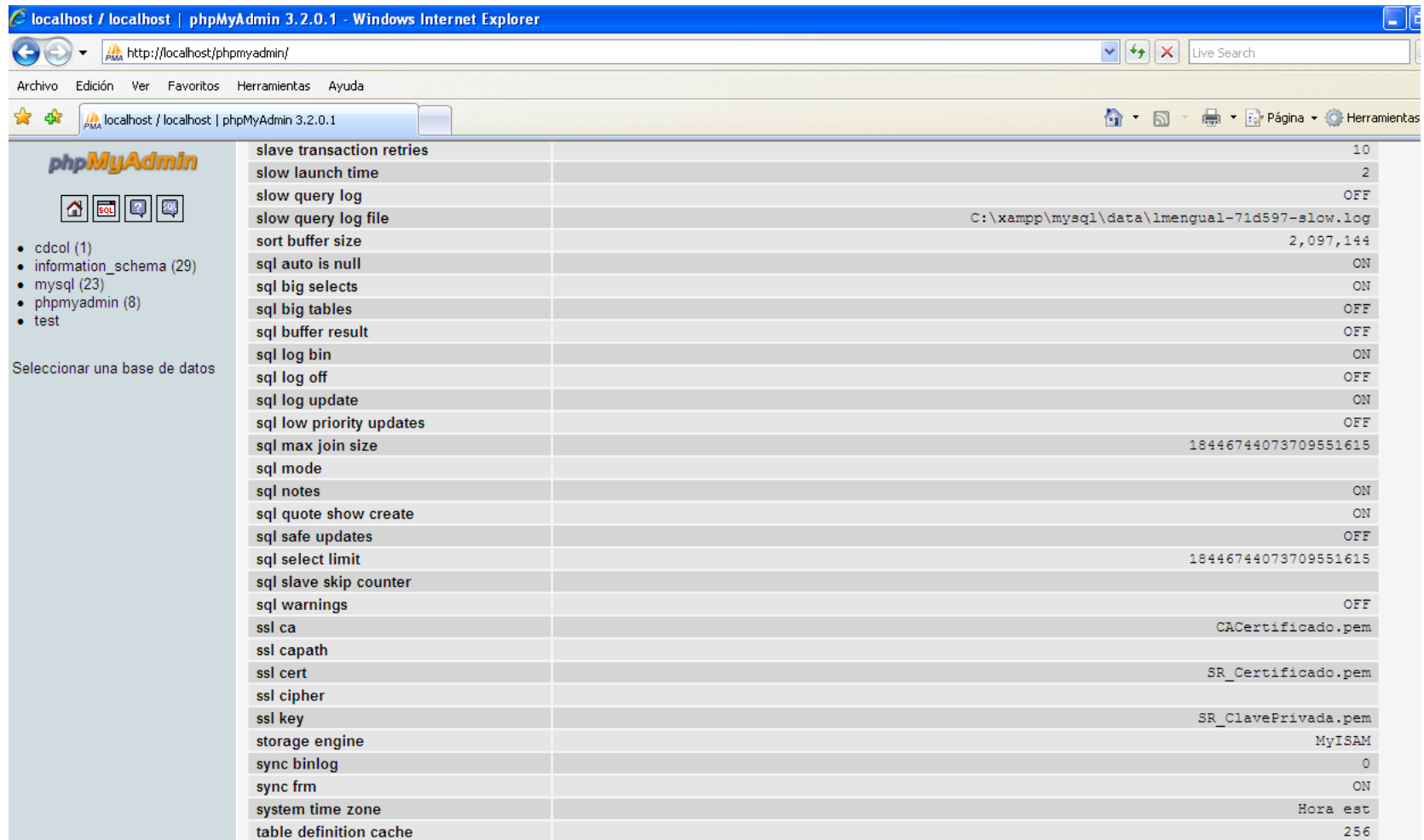
# 5. Configuración Manual SSL (II)

## Arranque manual Gestor MySQL



# 5. Configuración Manual SSL (III)

## Arranque manual Gestor MySQL: Variables SSL



The screenshot shows the phpMyAdmin 3.2.0.1 interface in a Windows Internet Explorer browser. The address bar shows 'http://localhost/phpmyadmin/'. The left sidebar contains a list of databases: cdcol (1), information\_schema (29), mysql (23), phpmyadmin (8), and test. Below this is a link 'Seleccionar una base de datos'. The main content area displays a table of MySQL variables.

slave transaction retries	10
slow launch time	2
slow query log	OFF
slow query log file	C:\xampp\mysql\data\lmengual-71d597-slow.log
sort buffer size	2,097,144
sql auto is null	ON
sql big selects	ON
sql big tables	OFF
sql buffer result	OFF
sql log bin	ON
sql log off	OFF
sql log update	ON
sql low priority updates	OFF
sql max join size	18446744073709551615
sql mode	
sql notes	ON
sql quote show create	ON
sql safe updates	OFF
sql select limit	18446744073709551615
sql slave skip counter	
sql warnings	OFF
ssl ca	CACertificado.pem
ssl capath	
ssl cert	SR_Certificado.pem
ssl cipher	
ssl key	SR_ClavePrivada.pem
storage engine	MyISAM
sync binlog	0
sync frm	ON
system time zone	Hora est
table definition cache	256



# 5. Configuración Manual SSL (IV)

## Conexión Cliente manual root ssl

1. Se copiará el fichero CACertificado.pem en el directorio

*C:\Program Files\MySQL\MySQL Workbench 6.2 CE*

2. Se abrirá una consola en el directorio anterior

3. 3. Se ejecutará el comando

`mysql -u root --ssl-ca=CACertificado.pem`

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

Your MySQL connection id is 3

Server version: 5.1.37 Source distribution

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

Ahora comprobamos que la conexión se ha establecido con ssl

```
mysql> SHOW STATUS LIKE "ssl_cipher";
```

+-----+-----+	
Variable_name	Value
+-----+-----+	
Ssl_cipher	DHE-RSA-AES256-SHA
+-----+-----+	

# 5. Configuración Manual SSL (V)

## Conexión Cliente manual root ssl

mysql> \s

-----

mysql Ver 14.14 Distrib 5.5.16, for Win32 (x86)

Connection id: 3  
Current database:  
Current user: root@localhost  
SSL: Cipher in use is DHE-RSA-AES256-SHA  
Using delimiter: ;  
Server version: 5.1.37 Source distribution  
Protocol version: 10  
Connection: localhost via TCP/IP  
Server characterset: latin1  
Db characterset: latin1  
Client characterset: cp850  
Conn. characterset: cp850  
TCP port: 3306  
Uptime: 30 sec

Threads: 3 Questions: 22 Slow queries: 0 Opens: 19 Flush tables: 1 Open tables: 12 Queries per second avg: 0.733

-----





# 5. Configuración Manual SSL (VI)

## Conexión Cliente manual root ssl

Si no están bien cargados los certificados saldría lo siguiente:

```
mysql -u root --ssl-ca=CACertificado.pem  
(Directorio C:\Program Files\MySQL\MySQL Workbench 6.2 CE)
```

```
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 9  
Server version: 5.1.37 Source distribution
```

Copyright (c) 2000, 2011, 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> SHOW STATUS LIKE "ssl_cipher";
```

```
+-----+-----+  
| Variable_name | Value |  
+-----+-----+  
| Ssl_cipher    |      |  
+-----+-----+  
1 row in set (0.00 sec)
```



# 5. Configuración Manual SSL (VII)

## Conexión Cliente manual root ssl

```
mysql> \s
```

```
-----  
mysql Ver 14.14 Distrib 5.5.16, for Win32 (x86)
```

```
Connection id:          9  
Current database:  
Current user:           root@localhost  
SSL:                    Not in use  
Using delimiter:        ;  
Server version:         5.1.37 Source distribution  
Protocol version:       10  
Connection:             localhost via TCP/IP  
Server characterset:    latin1  
Db characterset:        latin1  
Client characterset:    cp850  
Conn. characterset:     cp850  
TCP port:               3306  
Uptime:                 5 min 46 sec
```

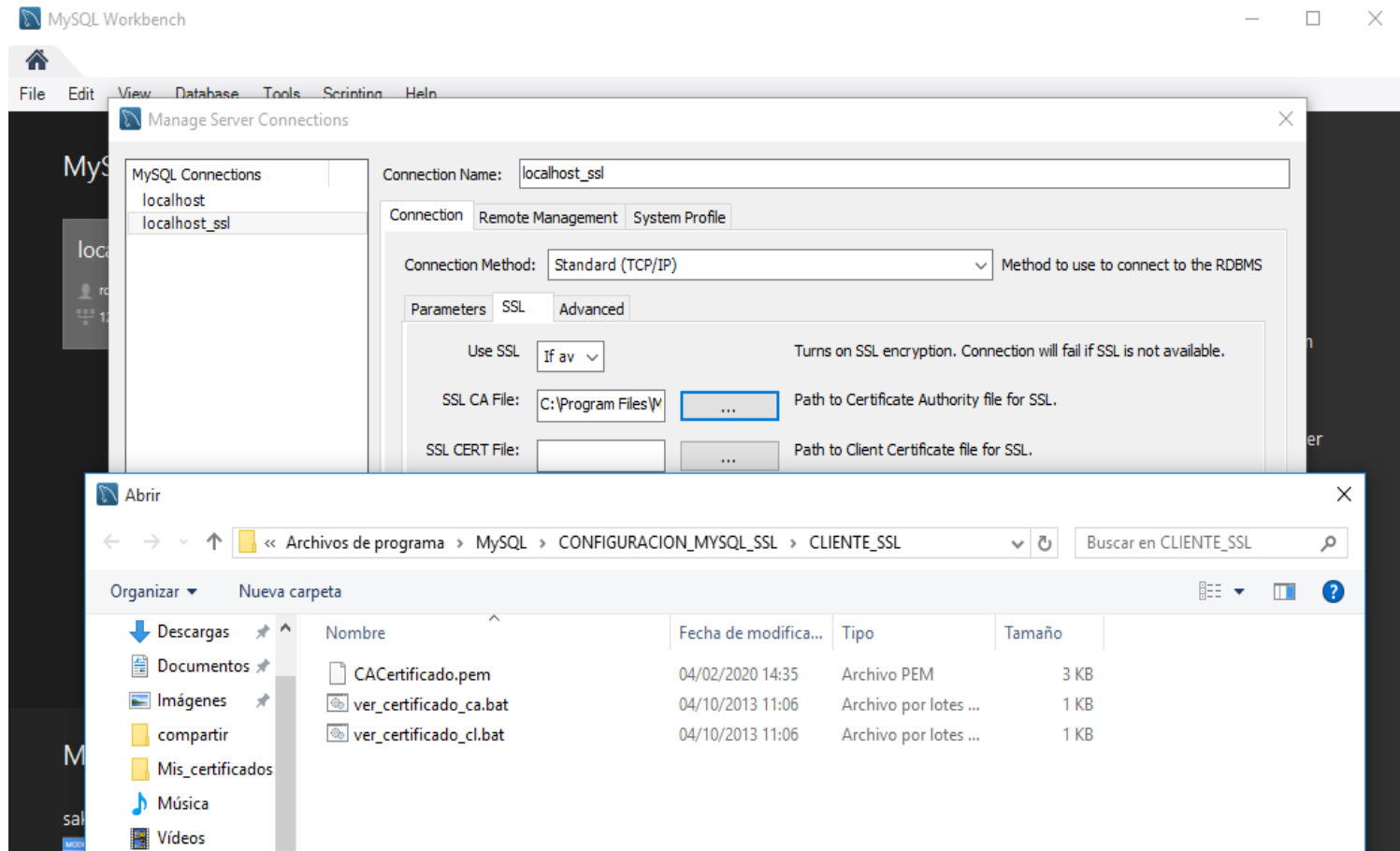
```
Threads: 1 Questions: 59 Slow queries: 0 Opens: 20 Flush tables: 1 Open tab  
les: 13 Queries per second avg: 0.170
```

```
-----
```

# 5. Configuración Manual SSL (VIII)

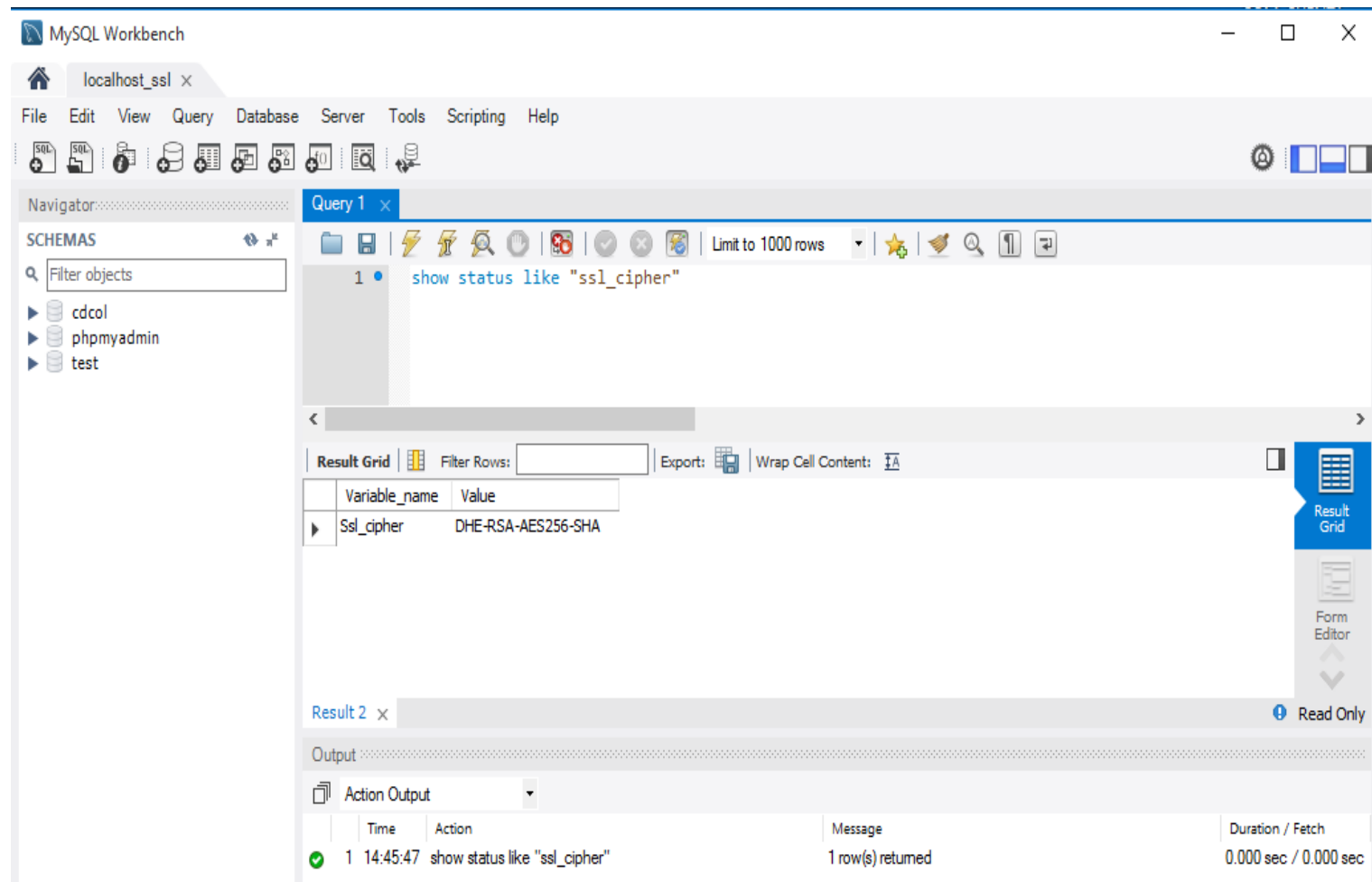
## Conexión Cliente worbench root ssl (localhost\_ssl)

1. Se selecciona el directorio  
C:\Program Files\MySQL\CONFIGURACION\_MYSQL\_SSL\CLIENTE\_SSL
2. Se copia en ese directorio en fichero CACertificado.pem



# 5. Configuración Manual SSL (IX)

## Conexión Cliente worbench root ssl (localhost\_ssl)



The screenshot displays the MySQL Workbench interface with the 'localhost\_ssl' connection selected. The 'Query' tab is active, showing a query: `show status like "ssl_cipher"`. The 'Result Grid' shows a single row with the variable `Ssl_cipher` and the value `DHE-RSA-AES256-SHA`. The 'Output' tab at the bottom shows the execution log with a successful status (green checkmark) and the message '1 row(s) returned'.

MySQL Workbench

localhost\_ssl x

File Edit View Query Database Server Tools Scripting Help

Navigator

SCHEMAS

Filter objects

- cdcol
- phpmyadmin
- test

Query 1 x

show status like "ssl\_cipher"

Limit to 1000 rows

Result Grid

Variable_name	Value
Ssl_cipher	DHE-RSA-AES256-SHA

Result 2 x

Read Only

Output

Action Output

	Time	Action	Message	Duration / Fetch
✓	1 14:45:47	show status like "ssl_cipher"	1 row(s) returned	0.000 sec / 0.000 sec



# 6. Configuración Automática SSL (I)

## Fichero configuración: "my.ini"

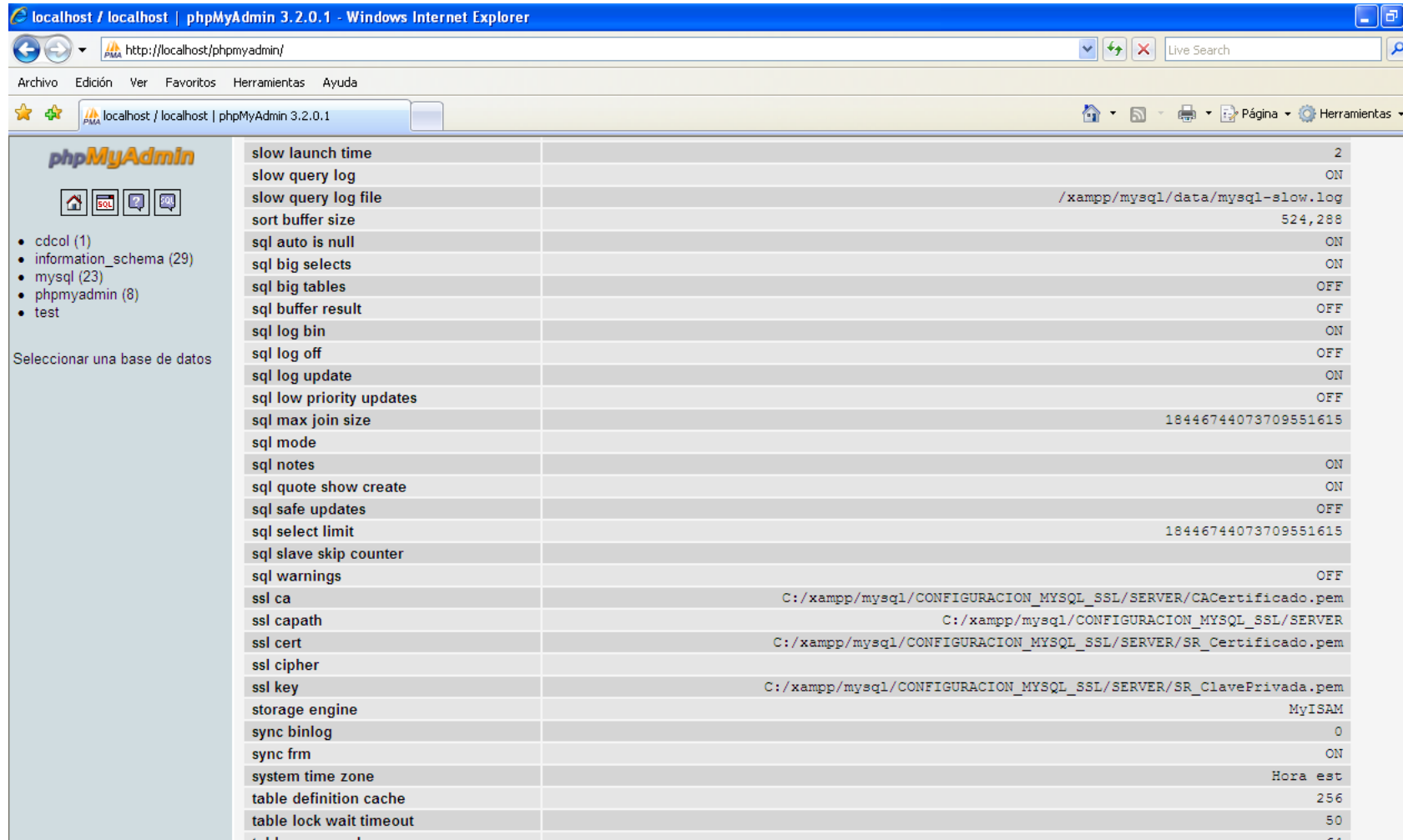
# INSERTAR CONFIGURACION DE SEGURIDAD:

```
# *****  
ssl  
ssl-ca = "C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/CACertificado.pem"  
ssl-cert = "C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/SR_Certificado.pem"  
ssl-key = "C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/SR_ClavePrivada.pem"  
ssl-capath = "C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER"  
  
# *****
```

- Con el *Gestor MySQL* parado hay que editar el fichero de configuración "my.ini" ("C:\xampp\mysql\bin\my.ini ") e insertar las líneas anteriores, guardar y cerrar el fichero.
- Copiar los certificados en el directorio especificado.
- Finalmente, reiniciar el *Gestor MySQL* pinchando el botón *mysql start* del panel de control *xampp*.

# 6. Configuración Automática SSL (II)

## Arranque automático Gestor MySQL: Variables SSL



The screenshot shows the phpMyAdmin 3.2.0.1 interface in a Windows Internet Explorer browser. The left sidebar contains a list of databases: cdcol (1), information\_schema (29), mysql (23), phpmyadmin (8), and test. The main area displays a table of MySQL variables. The variables are listed in the first column, and their values are in the second column. The variables are sorted alphabetically. The variables shown are: slow\_launch\_time, slow\_query\_log, slow\_query\_log\_file, sort\_buffer\_size, sql\_auto\_is\_null, sql\_big\_selects, sql\_big\_tables, sql\_buffer\_result, sql\_log\_bin, sql\_log\_off, sql\_log\_update, sql\_low\_priority\_updates, sql\_max\_join\_size, sql\_mode, sql\_notes, sql\_quote\_show\_create, sql\_safe\_updates, sql\_select\_limit, sql\_slave\_skip\_counter, sql\_warnings, ssl\_ca, ssl\_capath, ssl\_cert, ssl\_cipher, ssl\_key, storage\_engine, sync\_binlog, sync\_frm, system\_time\_zone, table\_definition\_cache, table\_lock\_wait\_timeout, and table\_open\_cache.

slow launch time	2
slow query log	ON
slow query log file	/xampp/mysql/data/mysql-slow.log
sort buffer size	524,288
sql auto is null	ON
sql big selects	ON
sql big tables	OFF
sql buffer result	OFF
sql log bin	ON
sql log off	OFF
sql log update	ON
sql low priority updates	OFF
sql max join size	18446744073709551615
sql mode	
sql notes	ON
sql quote show create	ON
sql safe updates	OFF
sql select limit	18446744073709551615
sql slave skip counter	
sql warnings	OFF
ssl ca	C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/CACertificado.pem
ssl capath	C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER
ssl cert	C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/SR_Certificado.pem
ssl cipher	
ssl key	C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/SR_ClavePrivada.pem
storage engine	MyISAM
sync binlog	0
sync frm	ON
system time zone	Hora est
table definition cache	256
table lock wait timeout	50
table open cache	64

# 6. Configuración Automática SSL (III)

## Conexión Cliente worbench root ssl (localhost\_ssl)

The screenshot shows the MySQL Workbench interface with a connection named 'localhost\_ssl' selected. The 'Query' tab is active, displaying the query 'show status like "ssl\_cipher"'. The 'Result Grid' shows the output of the query, which is 'DHE-RSA-AES256-SHA'. The 'Output' tab is also visible, showing the execution details of the query.

**Query 1**

```
show status like "ssl_cipher"
```

**Result Grid**

Variable_name	Value
Ssl_cipher	DHE-RSA-AES256-SHA

**Result 2** (Read Only)

**Output**

Action Output

	Time	Action	Message	Duration / Fetch
✓	1 14:45:47	show status like "ssl_cipher"	1 row(s) returned	0.000 sec / 0.000 sec



## 7.Crear cliente\_ssl0 (I)

- En esta fase vamos a crear un usuario en el *Gestor Mysql* denominado *cliente\_ssl0*.
- Este usuario de forma obligatoria, ya no opcional, deberá utilizar el protocolo *SSL*
  - No puede acceder sin el protocolo *SSL*.
- A este cliente no se le exigirá autenticación



## 7. Crear cliente\_ssl0 (II)

### Privilegios/Requisitos usuario

Vamos a crear el usuario *cliente\_ssl0* en el *Gestor Mysql* desde la cuenta del administrador *root* entrando al *Gestor MySQL* bien con el cliente *localhost* o *localhost\_ssl* invocando los siguientes comandos:

```
GRANT ALL PRIVILEGES ON *.* TO 'cliente_ssl0'@'%' IDENTIFIED BY 'ssl'  
WITH GRANT OPTION;
```

(Crear el usuario *cliente\_ssl0* con clave *ssl*)

```
GRANT ALL PRIVILEGES ON *.* TO 'cliente_ssl0'@'%' IDENTIFIED BY 'ssl'  
REQUIRE SSL;
```

(Al cliente *cliente\_ssl0* con clave *ssl* se le exige utilizar *SSL*)

```
SHOW GRANTS FOR cliente_ssl0;
```

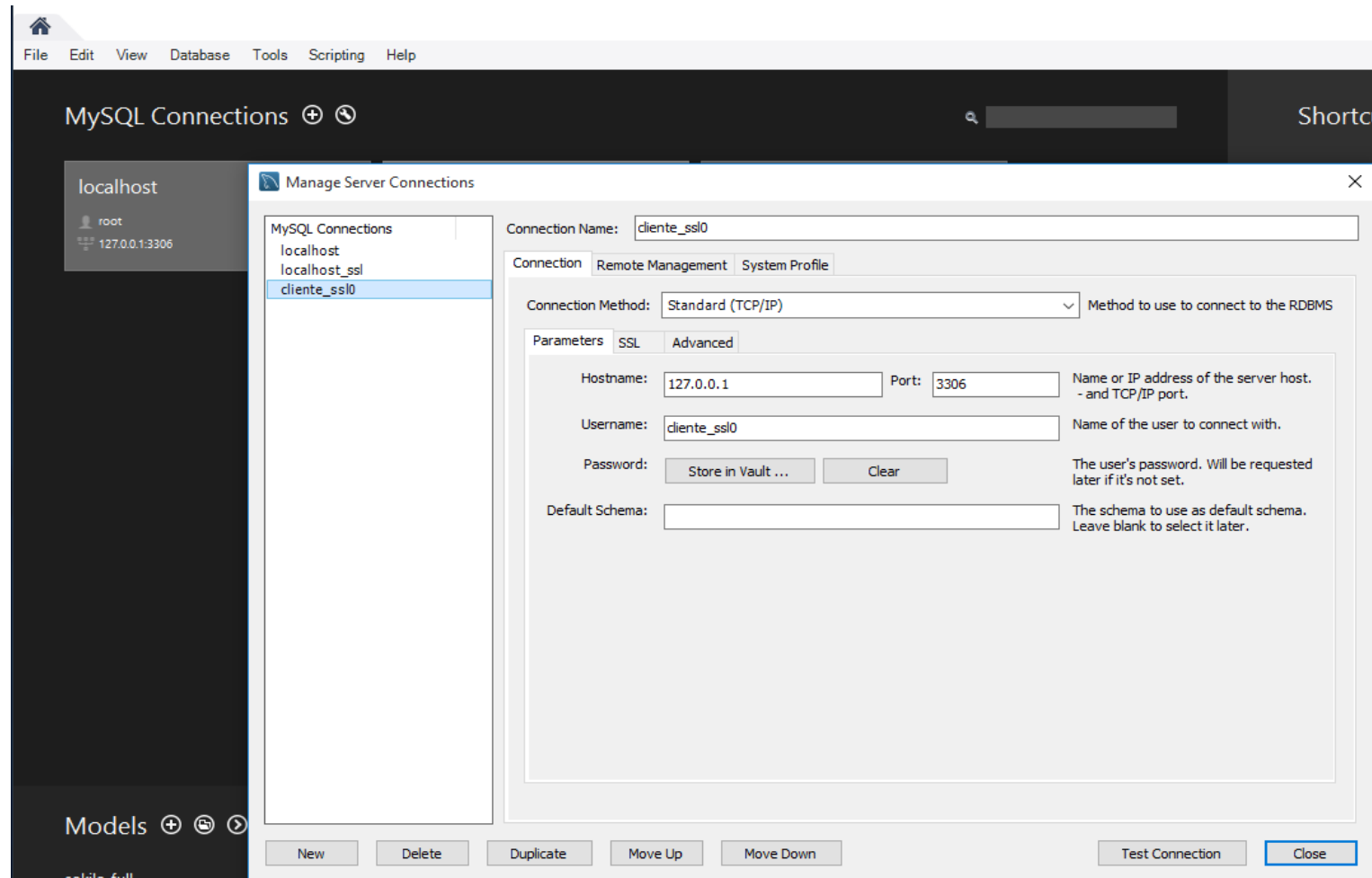
(Vemos los privilegios/requisitos creados para este usuario)

->

```
'GRANT ALL PRIVILEGES ON *.* TO \'cliente_ssl0\'@\'%\'  
PASSWORD \'*035E199C2E188B7300132D5C991D9E002AB5C150\'  
REQUIRE SSL WITH GRANT OPTION'
```

# 7. Crear cliente\_ssl0 (II)

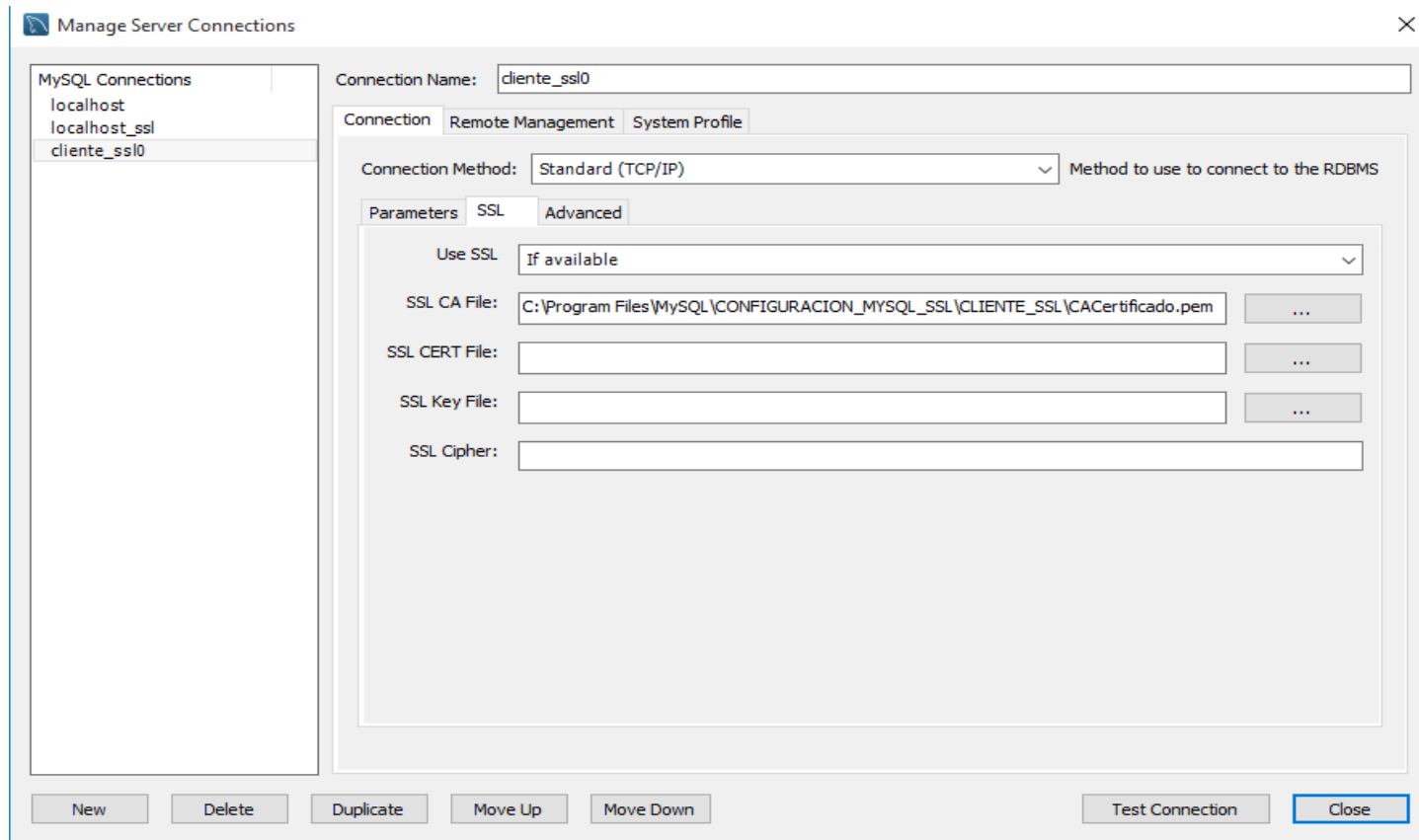
## Conexión Cliente worbench cliente\_ssl0



# 7. Crear cliente\_ssl0 (III)

## Conexión Cliente worbench cliente\_ssl0

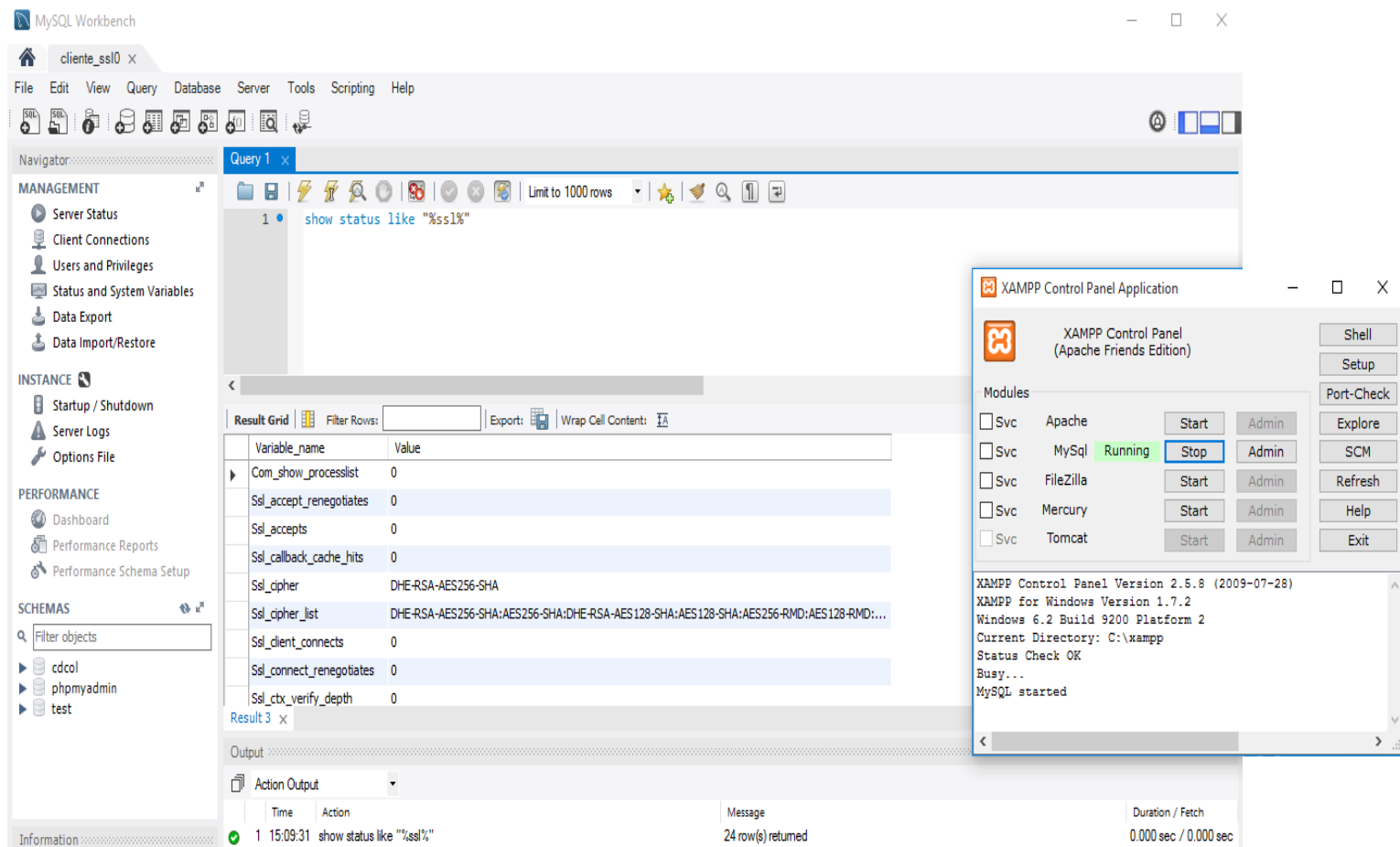
1. Se selecciona el directorio  
C:\Program Files\MySQL\CONFIGURACION\_MYSQL\_SSL\CLIENTE\_SSL
2. Se copia en ese directorio en fichero CACertificado.pem (esto se hizo ya con el usuario localhost\_ssl)



# 7. Crear cliente\_ssl0 (IV)

## Conexión Cliente worbench cliente\_ssl0

SHOW STATUS LIKE "%ssl%"



The screenshot displays the MySQL Workbench interface with a query window open, showing the command `show status like "%ssl%"`. The results are displayed in a table with columns `Variable_name` and `Value`. The XAMPP Control Panel is also visible, showing the status of various services. The MySQL service is running, and the SSL status is being checked.

Variable_name	Value
Com_show_processlist	0
Ssl_accept_renegotiates	0
Ssl_accepts	0
Ssl_callback_cache_hits	0
Ssl_cipher	DHE-RSA-AES256-SHA
Ssl_cipher_list	DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA:AES256-RMD:AES128-RMD:...
Ssl_client_connects	0
Ssl_connect_renegotiates	0
Ssl_ctx_verify_depth	0

XAMPP Control Panel Application

XAMPP Control Panel (Apache Friends Edition)

Modules

- ☐ Svc Apache Start Admin
- ☒ Svc MySQL Running Stop Admin
- ☐ Svc FileZilla Start Admin
- ☐ Svc Mercury Start Admin
- ☐ Svc Tomcat Start Admin

XAMPP Control Panel Version 2.5.8 (2009-07-28)  
XAMPP for Windows Version 1.7.2  
Windows 6.2 Build 9200 Platform 2  
Current Directory: C:\xampp  
Status Check OK  
Busy...  
MySQL started

Output

Action Output

Time	Action	Message	Duration / Fetch
1 15:09:31	show status like "%ssl%"	24 row(s) returned	0.000 sec / 0.000 sec



## 8. Crear cliente\_ssl (I)

- En esta fase vamos a crear un usuario en el *Gestor Mysql* denominado *cliente\_ssl*.
- Este usuario de forma obligatoria, ya no opcional deberá utilizar el protocolo *SSL*
  - No puede acceder sin el protocolo *SSL*.
- A este cliente se le exigirá autenticación



## 8. Crear cliente\_ssl (II)

### Privilegios/Requisitos usuario

Vamos a crear el usuario *cliente\_ssl* en el *Gestor Mysql* desde la cuenta del administrador *root* entrando al *Gestor MySQL* bien con el cliente *localhost* o *localhost\_ssl* invocando los siguientes comandos:

```
GRANT ALL PRIVILEGES ON *.* TO 'cliente_ssl'@'%' IDENTIFIED BY 'ssl'  
WITH GRANT OPTION;
```

(Crear el usuario *cliente\_ssl* con clave *ssl*)

```
GRANT ALL PRIVILEGES ON *.* TO 'cliente_ssl'@'%' IDENTIFIED BY 'ssl'  
REQUIRE SSL;
```

(Al cliente *cliente\_ssl* con clave *ssl* se le exige utilizar *SSL*)

```
GRANT ALL PRIVILEGES ON *.* TO 'cliente_ssl'@'%' IDENTIFIED BY 'ssl'  
REQUIRE X509;
```

(Al cliente *cliente\_ssl* con clave *ssl* se le exige autenticación a través de un Certificado digital *X.509*)

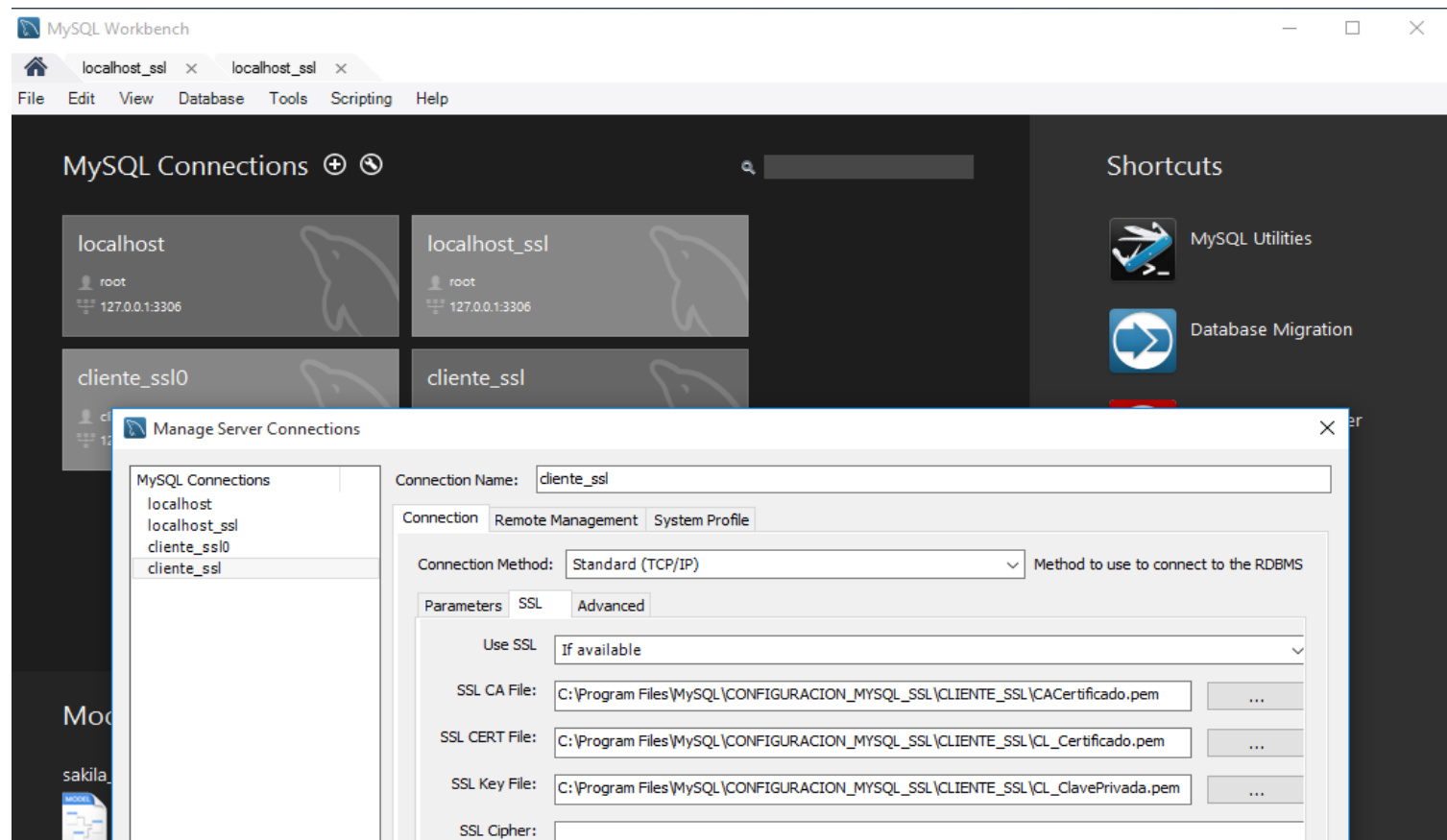
```
SHOW GRANTS FOR cliente_ssl;
```

```
'GRANT ALL PRIVILEGES ON *.* TO \'cliente_ssl\'@\'%\'  
PASSWORD \'*035E199C2E188B7300132D5C991D9E002AB5C150\'  
REQUIRE X509 WITH GRANT OPTION'
```

# 8. Crear cliente\_ssl (III)

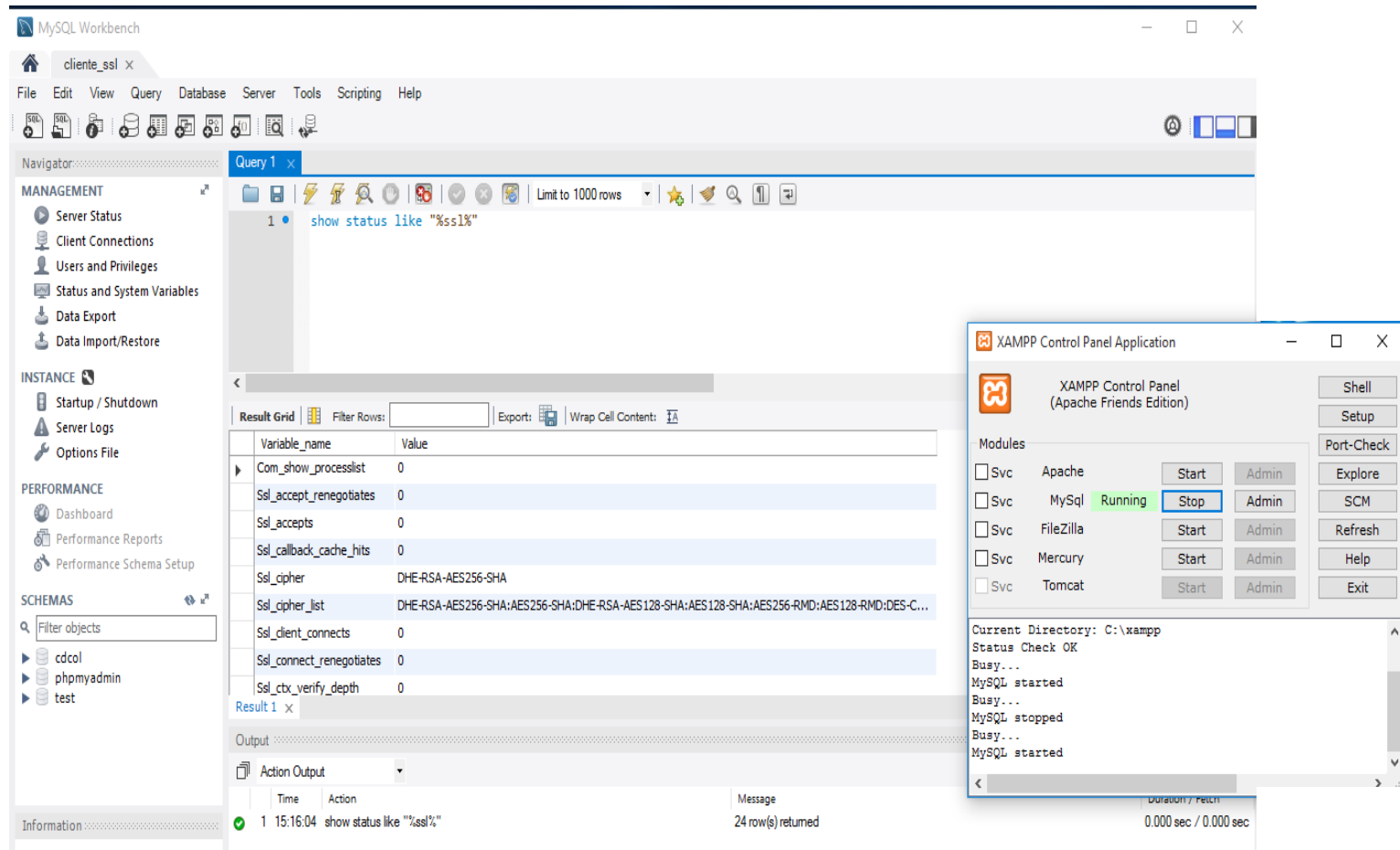
## Conexión Cliente worbench cliente\_ssl

1. Se selecciona el directorio  
C:\Program Files\MySQL\CONFIGURACION\_MYSQL\_SSL\CLIENTE\_SSL
2. Se copia en ese directorio los ficheros CACertificado.pem  
CL\_Certificado.pem y CL\_ClavePrivada.pem.



# 8. Crear cliente\_ssl (IV)

## Conexión Cliente worbench cliente\_ssl



The image shows a screenshot of a computer screen with two windows open. The background window is MySQL Workbench, and the foreground window is the XAMPP Control Panel Application.

**MySQL Workbench:**

- Tab: cliente\_ssl x
- Query 1: `show status like "%ssl%"`
- Result Grid:

Variable_name	Value
Com_show_processlist	0
Ssl_accept_renegotiates	0
Ssl_accepts	0
Ssl_callback_cache_hits	0
Ssl_cipher	DHE-RSA-AES256-SHA
Ssl_cipher_list	DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA:AES256-RMD:AES128-RMD:DES-C...
Ssl_client_connects	0
Ssl_connect_renegotiates	0
Ssl_ctx_verify_depth	0

**XAMPP Control Panel Application:**

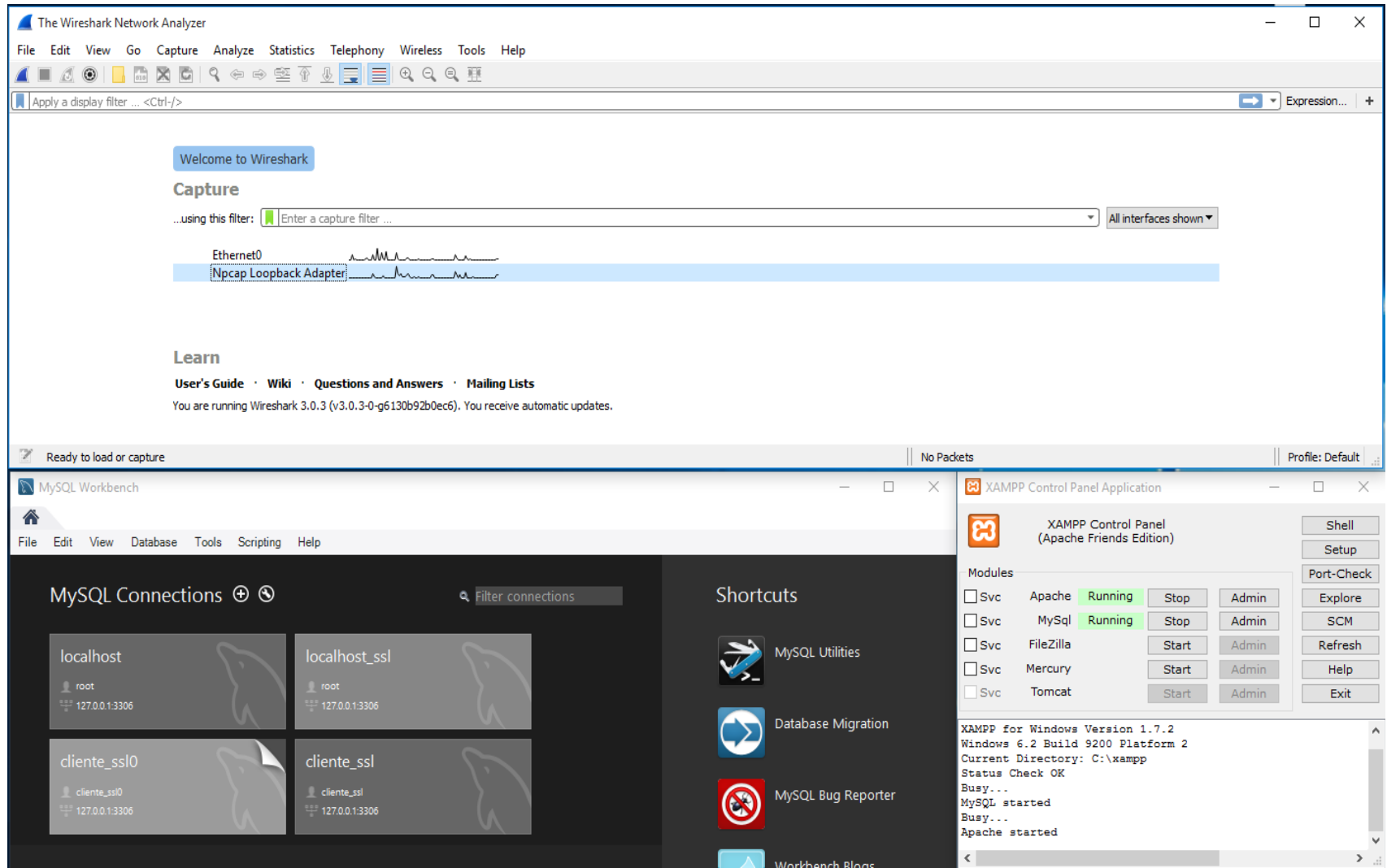
- Modules:

Svc	Module	Status	Action
<input type="checkbox"/>	Apache	Stopped	Start Admin
<input checked="" type="checkbox"/>	MySQL	Running	Stop Admin
<input type="checkbox"/>	FileZilla	Stopped	Start Admin
<input type="checkbox"/>	Mercury	Stopped	Start Admin
<input type="checkbox"/>	Tomcat	Stopped	Start Admin

Current Directory: C:\xampp  
Status Check OK  
Busy...  
MySQL started  
Busy...  
MySQL stopped  
Busy...  
MySQL started



# 8. Captura de Tráfico



# 8. Captura de Tráfico cliente\_ssl0

The screenshot displays two windows: Wireshark at the top and XAMPP Control Panel at the bottom.

**Wireshark Window:**

- Title: \*Npcap Loopback Adapter
- Menu: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Filter: Apply a display filter ... <Ctrl-/>
- Table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
14	0.131611	127.0.0.1	127.0.0.1	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
16	0.131661	127.0.0.1	127.0.0.1	TLSv1	139	Application Data
18	0.131764	127.0.0.1	127.0.0.1	TLSv1	171	Application Data
31	5.868367	127.0.0.1	127.0.0.1	TLSv1	148	Client Hello
33	5.874812	127.0.0.1	127.0.0.1	TLSv1	1434	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
35	5.878678	127.0.0.1	127.0.0.1	TLSv1	200	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
37	5.879292	127.0.0.1	127.0.0.1	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
39	5.879356	127.0.0.1	127.0.0.1	TLSv1	155	Application Data
41	5.879502	127.0.0.1	127.0.0.1	TLSv1	107	Application Data
43	5.879565	127.0.0.1	127.0.0.1	TLSv1	107	Application Data

Packet 31 details:

- Frame 31: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 49466, Dst Port: 3306, Seq: 37, Ack: 61, Len: 94
- Transport Layer Security

Hex dump and ASCII view of the packet data are visible below the details pane.

**XAMPP Control Panel Window:**

- Title: XAMPP Control Panel Application
- Subtitle: XAMPP Control Panel (Apache Friends Edition)
- Buttons: Shell, Setup, Port-Check, Explore, SCM, Refresh, Help, Exit
- Modules section:

Module	Status	Start	Stop	Admin
Svc Apache	Running	Start	Stop	Admin
Svc MySQL	Running	Start	Stop	Admin
Svc FileZilla	Stopped	Start	Stop	Admin
Svc Mercury	Stopped	Start	Stop	Admin
Svc Tomcat	Stopped	Start	Stop	Admin

Bottom status bar: Busy... Apache stopped Busy...

# 8. Captura de Tráfico *cliente\_ssl*

The screenshot displays two windows: Wireshark at the top and XAMPP Control Panel at the bottom.

**Wireshark Window:**

- Title: \*Npcap Loopback Adapter
- Filter: Apply a display filter ... <Ctrl-/>
- Table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
16	1.450491	127.0.0.1	127.0.0.1	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
18	1.450546	127.0.0.1	127.0.0.1	TLSv1	139	Application Data
20	1.450756	127.0.0.1	127.0.0.1	TLSv1	171	Application Data
34	7.199124	127.0.0.1	127.0.0.1	TLSv1	148	Client Hello
36	7.210442	127.0.0.1	127.0.0.1	TLSv1	1434	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
38	7.224723	127.0.0.1	127.0.0.1	TLSv1	1338	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
40	7.329910	127.0.0.1	127.0.0.1	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
42	7.330019	127.0.0.1	127.0.0.1	TLSv1	155	Application Data
44	7.330158	127.0.0.1	127.0.0.1	TLSv1	107	Application Data
46	7.330209	127.0.0.1	127.0.0.1	TLSv1	107	Application Data

Below the table, the packet details for Frame 36 are shown:

- Frame 36: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
- Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 3306, Dst Port: 49470, Seq: 61, Ack: 131, Len: 1380
- Transport Layer Security

The packet bytes section shows the raw data in hexadecimal and ASCII.

**XAMPP Control Panel Window:**

- Title: XAMPP Control Panel Application
- Subtitle: XAMPP Control Panel (Apache Friends Edition)
- Modules list:

Module	Status	Start	Admin
Apache	Running	Start	Admin
MySQL	Running	Stop	Admin
FileZilla	Stopped	Start	Admin
Mercury	Stopped	Start	Admin
Tomcat	Stopped	Start	Admin

Buttons on the right: Shell, Setup, Port-Check, Explore, SCM, Refresh, Help, Exit.

Bottom status bar: Busy... Apache stopped, Busy... MySQL started.

# ERRORES DE CONFIGURACIÓN:

"SSL connection error: ASN: bad other signature confirmation."

1. El fichero "CACertificado.pem" en el cliente no es correcto no verifica certificado Servidor.
2. El fichero "SR\_Certificado.pem" en el servidor no es correcto. No esta firmado por la autoridad "CACertificado.pem".

"Access denied for user ...."

No existe el fichero clave privada del servidor "SR\_ClavePrivada.pem" o el fichero de certificado del servidor "SR\_Certificado.pem" o ambos.

"SSL connection error: unable verify peer checksum"

El fichero clave privada del servidor no es el correcto "SR\_ClavePrivada.pem".

"SSL connection error: protocol version mismatch"

El fichero "CACertificado.pem" en el servidor no es correcto no verifica certificado "CL\_Certificado.pem" en cliente\_SSL