Install mysql and configure SSL

Step 1: Install MySQL 8.0 RHEL 8

Refer to the following link:
https://www.tecmint.com/install-mysql-on-centos-8/

Step 2- Log into MySQL and enter the password created by you.
$ mysql -u root -p

```
[ec2-user@ip-172-31-37-142 ~]$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 51
Server version: 8.0.31 MySQL Community Server - GPL

Copyright (c) 2000, 2022, 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.
```

Step 3: Configure SSL for mysql server and the clients that will access the server.
`mkdir -p /etc/mysql/newcerts` `chown -R mysql:mysql /etc/mysql/newcerts`

Step 4: Create certificate authority.
```
cd /etc/mysql/newcerts
openssl genrsa 2048 > ca-key.pem
```

The following command will ask details of your certificate provider, provide a unique Common Name when asked :-

```
openssl req -new -x509 -nodes -days 1000 -key ca-key.pem > ca-cert.pem
```

for example:

```
[root@ip-172-31-37-142 ~]# mkdir -p /etc/mysql/newcerts
[root@ip-172-31-37-142 ~]# chown -R mysql:mysql /etc/mysql/newcerts
[root@ip-172-31-37-142 ~]# cd /etc/mysql/newcerts
[root@ip-172-31-37-142 newcerts]# openssl genrsa 2048 > ca-key.pem
[root@ip-172-31-37-142 newcerts]# 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]:IN
State or Province Name (full name) []:Karnataka
Locality Name (eg, city) [Default City]:Bangalore
Organization Name (eg, company) [Default Company Ltd]:MySQL
Organizational Unit Name (eg, section) []:Community
Common Name (eg, your name or your server's hostname) []:shubhra
Email Address []:shubhra.kumari@tessell.com
[root@ip-172-31-37-142 newcerts]#
```

Step 5: Create a certificate for the server using the CA certificate generated above.
Do not provide a password if asked in the next step
The Common Name used here **must** differ from the one used for the Certificate Authority above.

```
openssl req -newkey rsa:2048 -days 1000 -nodes -keyout server-key.pem > server-req.pem
openssl x509 -req -in server-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 > server-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]:IN
State or Province Name (full name) []:Karnataka
Locality Name (eg, city) [Default City]:Bangalore
Organization Name (eg, company) [Default Company Ltd]:MySQL
Organizational Unit Name (eg, section) []:Community
Common Name (eg, your name or your server's hostname) []:server-cert
Email Address []:shubhra.kumari@tessell.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
[root@ip-172-31-37-142 newcerts]#
```

Step 6: Create a certificate for the clients using the same CA certificate.
-You must provide the details for the client that will connect to the server.
-The Common Name used here **must** differ from the one used for the Certificate Authority **and** the Server certificate above.

```
openssl req -newkey rsa:2048 -days 1000 -nodes -keyout client-key.pem > client-req.pem
openssl x509 -req -in client-req.pem -days 1000 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 > client-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]:IN
State or Province Name (full name) []:Karnataka
Locality Name (eg, city) [Default City]:Bangalore
Organization Name (eg, company) [Default Company Ltd]:MySQL
Organizational Unit Name (eg, section) []:Community
Common Name (eg, your name or your server's hostname) []:client-cert
Email Address []:shubhra.kumari@tessell.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
[root@ip-172-31-37-142 newcerts]#
```

Step 7: Make sure following entries are present in `/etc/my.cnf` under the `[mysqld]` section
ssl ssl-ca=/etc/mysql/newcerts/ca-cert.pem ssl-cert=/etc/mysql/newcerts/server-cert.pem ssl-key=/etc/mysql/newcerts/server-key.pem

Step 8: Restart mysqld
`service mysqld restart`

```
[root@ip-172-31-37-142 newcerts]# service mysqld restart
Redirecting to /bin/systemctl restart mysqld.service
[root@ip-172-31-37-142 newcerts]#
```

Step 9: Ensure that mysql root is authenticated with SSL and has correct permissions
use your mysql root password here.
`mysql -u root -p`

CREATE USER 'root'@'%' IDENTIFIED BY 'your password' REQUIRE SSL;

```
mysql> CREATE USER 'root'@'%' IDENTIFIED BY '0L0kNkpVq(J' REQUIRE SSL;
Query OK, 0 rows affected (0.01 sec)
```

GRANT ALL ON *.* TO 'root'@'%';

```
mysql> GRANT ALL ON *.* TO 'root'@'%';
Query OK, 0 rows affected (0.00 sec)
```

mysql> quit

Client side configuration

- We can add global configuration in /etc/my.cnf file for all users to use SSL to connect to MySQL server.
  # cat /etc/my.cnf [client] ssl-ca=/tmp/ca-cert.pem ssl-cert=/tmp/client-cert.pem ssl-key=/tmp/client-key.pem

example:

- We can have client configuration for a specific user in its $HOME/.my.cnf
  # cat ~/.my.cnf [client] ssl-ca=/tmp/ca-cert.pem ssl-cert=/tmp/client-cert.pem ssl-key=/tmp/client-key.pem

Check for the ciphers:
`mysql> SHOW STATUS LIKE 'Ssl_cipher';`

```
mysql> SHOW STATUS LIKE 'Ssl_cipher';
+---------------+-------------------------+
| Variable_name | Value                   |
+---------------+-------------------------+
| Ssl_cipher    | TLS_AES_256_GCM_SHA384 |
+---------------+-------------------------+
1 row in set (0.01 sec)
```

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

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

```
show variables like '%%ssl%%'
--------------


+---------------+-----------------------------------------+
| Variable_name | Value                                   |
+---------------+-----------------------------------------+
| have_openssl  | YES                                     |
| have_ssl      | YES                                     |
| ssl_ca        | /etc/mysql/newcerts/ca-cert.pem         |
| ssl_capath    |                                         |
| ssl_cert      | /etc/mysql/newcerts/server-cert.pem     |
| ssl_cipher    |                                         |
| ssl_key       | /etc/mysql/newcerts/server-key.pem      |
+---------------+-----------------------------------------+
7 rows in set (0.01 sec)
```

Step 10: create a new MySQL user and database for remote MySQL clients.
mysql -u root -p mysql> CREATE DATABASE remotedb; mysql> CREATE USER 'remoteuser'@'mysql-client-ip' IDENTIFIED BY 'yourpassword' REQUIRE SSL;

```
mysql> create database remotedb;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE USER 'remoteuser'@'mysql-client-ip' IDENTIFIED BY '0L0kNkpVq(J' REQUIRE SSL;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON remotedb.* TO 'remoteuser'@'mysql-client-ip' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

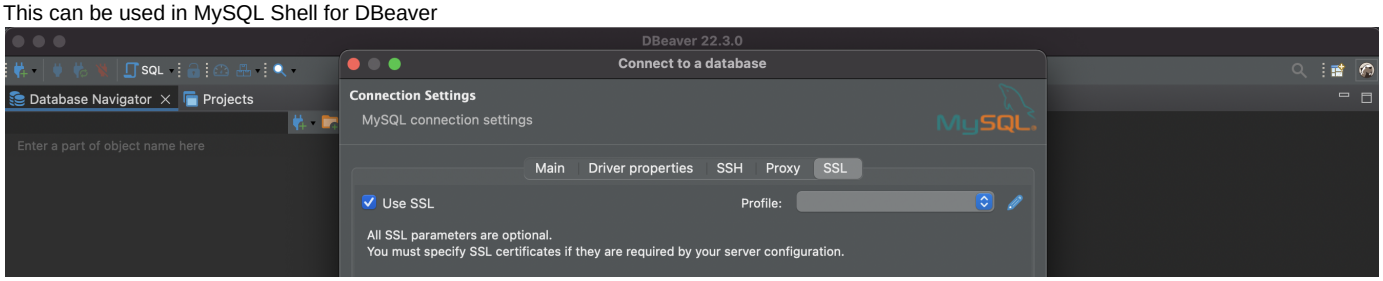
Step 11: create a MySQL user that will use the certificate. By default, with the loaded password policy, we also need to provide a password:
CREATE USER user1 IDENTIFIED BY '0L0kNkpVq(J' REQUIRE SUBJECT '/C=IN/ST=Karnataka/L=Bangalore/O=MySQL/OU=Community /CN=client-cert/emailAddress=shubhra.kumari@tessell.com';
Query OK, 0 rows affected (0.0114 sec)

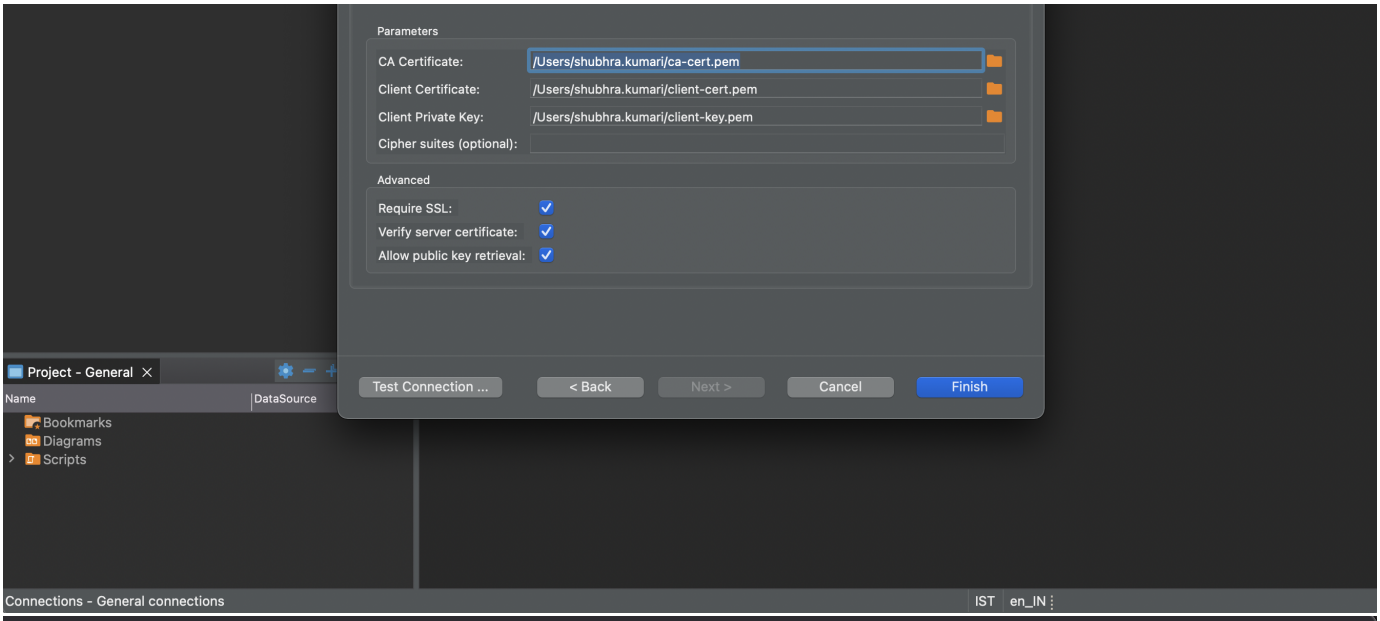
Step 12: yum install mysql-shell
https://dev.mysql.com/doc/mysql-shell/8.0/en/mysql-shell-install-macos-quick.html

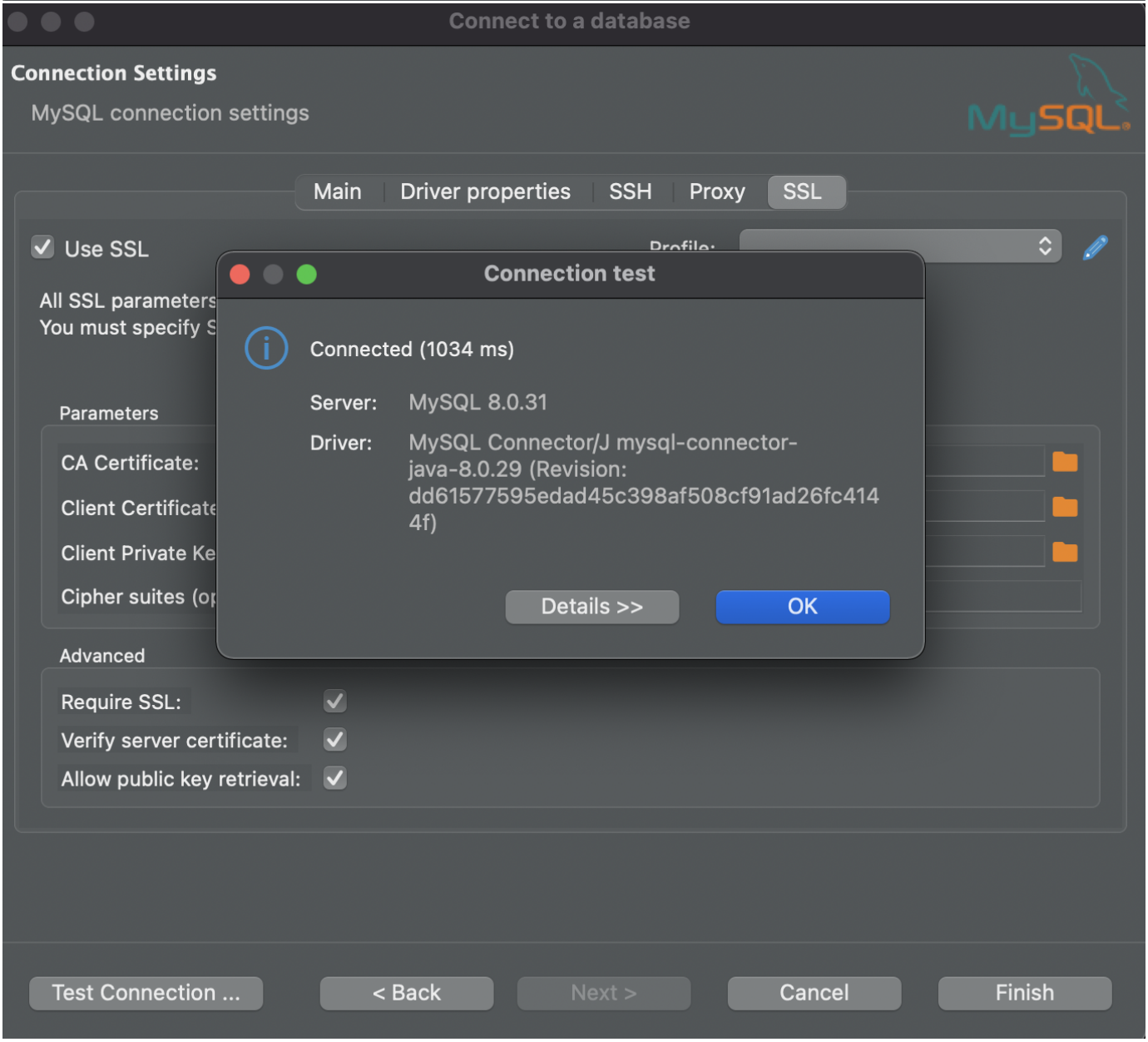
Step 13: Connecting
copy the contents of the certificate
mysqlsh --sql mysql://root@localhost --ssl-cert client-cert.pem --ssl-key client-key.pem

```
[root@ip-172-31-37-142 newcerts]# mysqlsh --sql mysql://root@localhost --ssl-cert client-cert.pem --ssl-key client-key.pem
Please provide the password for 'root@localhost': **********
```

This can be used in MySQL Shell for DBeaver




Parameters
CA Certificate:
/Users/shubhra.kumari/ca-cert.pem
Client Certificate:
/Users/shubhra.kumari/client-cert.pem
Client Private Key:
/Users/shubhra.kumari/client-key.pem
Cipher suites (optional):
Advanced
Require SSL:
Verify server certificate:
Allow public key retrieval:
Test Connection ...
< Back
Next >
Cancel
Finish
Project - General
Name
DataSource
Bookmarks
Diagrams
Scripts
Connections - General connections
IST
en_IN


Connect to a database
Connection Settings
MySQL connection settings
MySQL
Main
Driver properties
SSH
Proxy
SSL
Use SSL
Profile:
All SSL parameters
You must specify S
Parameters
CA Certificate:
Client Certificate
Client Private Ke
Cipher suites (op
Advanced
Require SSL:
Verify server certificate:
Allow public key retrieval:
Connection test
Connected (1034 ms)
Server: MySQL 8.0.31
Driver: MySQL Connector/J mysql-connector-java-8.0.29 (Revision: dd61577595edad45c398af508cf91ad26fc4144f)
Details >>
OK
Test Connection ...
< Back
Next >
Cancel
Finish