Hướng dẫn cài đặt MySQL trên VPS centos 7

Link tài liệu tham khảo: https://www.howtoforge.com/tutorial/how-to-enable-ssl-and-remote-connections-for-mysql-on-centos-7/

Link video tham khảo: <https://www.youtube.com/watch?v=nfOEeFRV1xs>

1. **Install MySQL**

* Thêm kho lưu trữ mới cho MySQL bằng lệnh yum bên dưới.

*yum localinstall* [*https://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm*](https://dev.mysql.com/get/mysql57-community-release-el7-9.noarch.rpm)

* Bạn sẽ được yêu cầu cài đặt một gói mới, nhập 'y' và nhấn 'Enter' để xác nhận.
* Bây giờ bạn có thể cài đặt MySQL phiên bản 5.7 mới nhất vào máy chủ như sau:

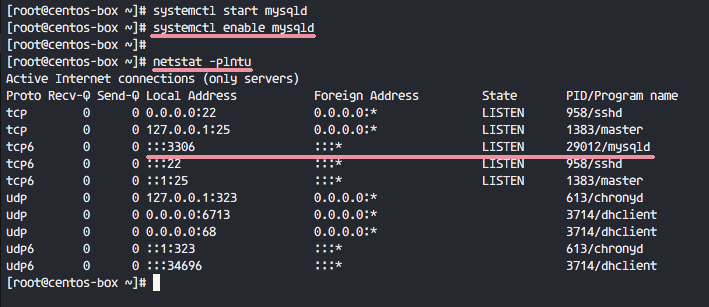
*yum -y install mysql-community-server*

* Khi quá trình cài đặt đã hoàn tất, hãy khởi động dịch vụ MySQL và cho phép nó chạy tự động tại thời điểm khởi động bằng lệnh systemctl.

*systemctl start mysqld  
systemctl enable mysqld*

* Đảm bảo MySQL đang chạy bằng cách kiểm tra cổng được sử dụng bởi MySQL (3306). Kiểm tra nó bằng lệnh netstat bên dưới.

*netstat -plntu*



## 2. Configure the MySQL Root Password

* Theo mặc định, MySQL 5.7 tạo mật khẩu gốc mặc định cho bạn khi khởi động dịch vụ lần đầu tiên. Mật khẩu được lưu trữ trong tệp nhật ký MySQL '/var/log/mysqld.log'.
* Để xem mật khẩu gốc MySQL mặc định, bạn có thể sử dụng lệnh grep bên dưới.

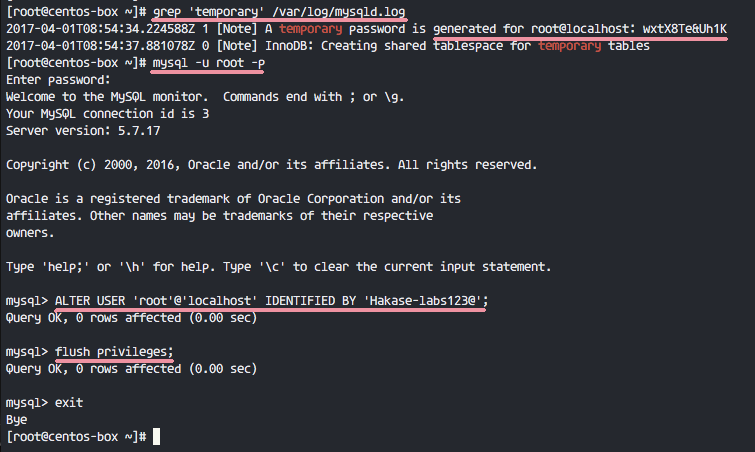
*A temporary password is generated for root@localhost: wxtX8Te&Uh1K*

* Kết nối với MySQL shell bằng mật khẩu mặc định và thay thế mật khẩu bằng mật khẩu của riêng bạn.

*mysql -u root -p  
TYPE IN DEFAULT PASSWORD*

* Bây giờ hãy thay thế mật khẩu mặc định bằng mật khẩu của riêng bạn. Trong hướng dẫn này, tôi sẽ sử dụng **'Hakase-labs123@'** làm mật khẩu gốc MySQL mới. Chạy các truy vấn MySQL bên dưới.

*ALTER USER 'root'@'localhost' IDENTIFIED BY 'Hakase-labs123@';  
flush privileges;  
exit;*



* Bây giờ bạn có thể kết nối lại với mật khẩu mới **'Hakase-labs123@'**.

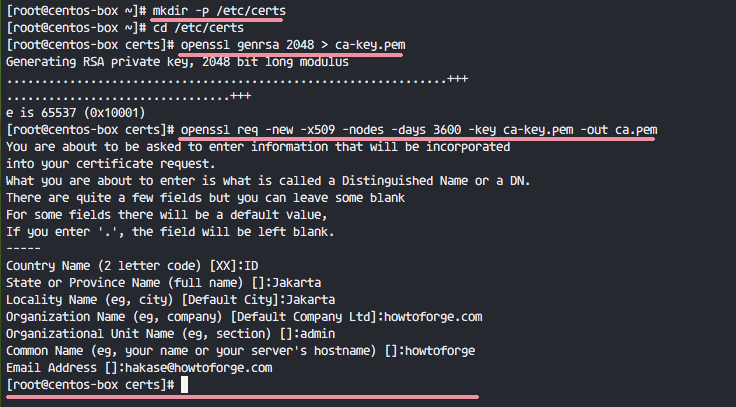
*mysql -u root -p  
TYPE NEW PASSWORD 'Hakase-labs123@'*

## 3.Generate New Self-Signed Certificate Files

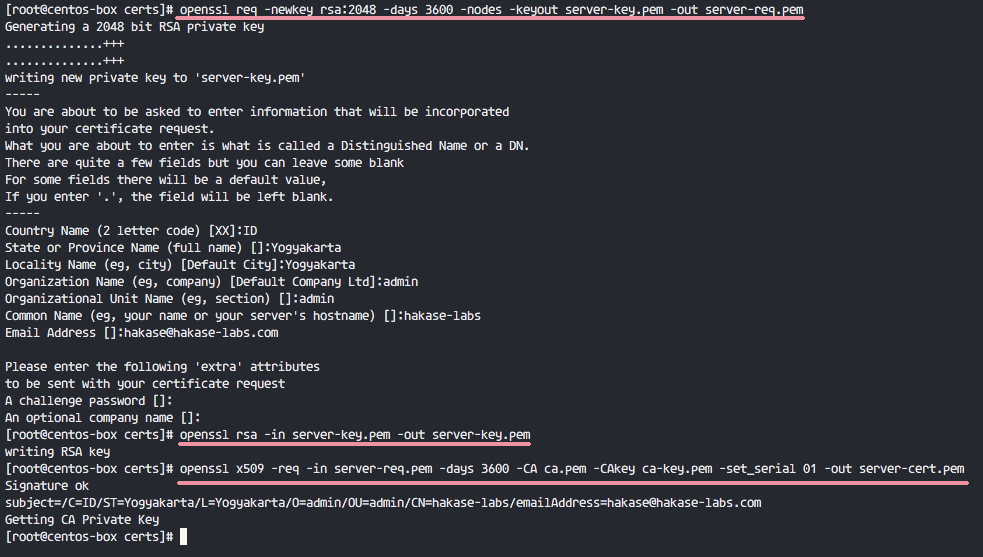
* Theo mặc định, MySQL 5.7 có các tệp chứng chỉ SSL riêng trong thư mục '/ var / lib / mysql'. Nhưng trong hướng dẫn này, tôi sẽ chỉ cho bạn cách tạo tệp Chứng chỉ SSL của riêng bạn bằng OpenSSL, sau đó định cấu hình chúng bằng MySQL.
* Trong bước này, chúng tôi sẽ tạo các tệp chứng chỉ tự ký mới. Chúng tôi cần 3 chứng chỉ, **CA Certificate**, **Server Certificate and Key**, **Client Certificate and Key**. Chúng tôi sẽ tạo chúng bằng **OpenSSL**.
* Tạo một thư mục mới cho các tệp chứng chỉ SSL '/etc/certs/' và chuyển đến thư mục đó.

*mkdir -p /etc/certs  
cd /etc/certs*

* Tạo tệp **ca.pem  CA certificate** mới.

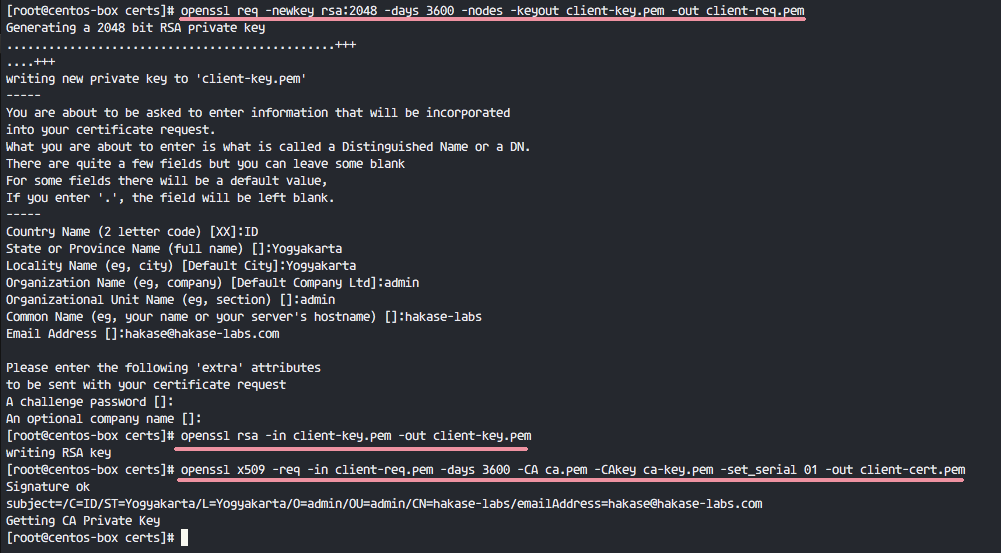
*openssl genrsa 2048 > ca-key.pem  
openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca.pem*

* Tiếp theo, chúng ta phải tạo **server-side certificates**. Tạo chứng chỉ máy chủ mới các tệp **server-cert.pem** và **server-key.pem**. Tạo tệp chứng chỉ mới, xóa cụm mật khẩu và ký chúng bằng chứng chỉ CA.

*openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out server-req.pem  
openssl rsa -in server-key.pem -out server-key.pem  
openssl x509 -req -in server-req.pem -days 3600 -CA ca.pem -CAkey ca-key.pem -set\_serial 01 -out server-cert.pem*

* Bây giờ tạo các tệp chứng chỉ cho máy khách. Máy chủ MySQL sẽ chỉ chấp nhận kết nối từ xa từ máy khách có các tệp chứng chỉ này. Tạo tệp chứng chỉ ứng dụng khách mới, xóa cụm mật khẩu và ký chúng bằng chứng chỉ CA.

*openssl req -newkey rsa:2048 -days 3600 -nodes -keyout client-key.pem -out client-req.pem  
openssl rsa -in client-key.pem -out client-key.pem  
openssl x509 -req -in client-req.pem -days 3600 -CA ca.pem -CAkey ca-key.pem -set\_serial 01 -out client-cert.pem*

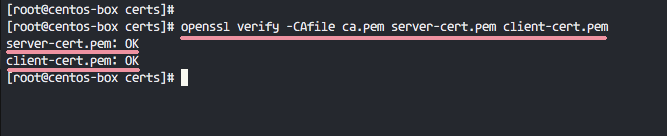


**\* Note: *Thông tin chứng chỉ CA phải khác với thông tin máy khách và máy chủ.***

* Tất cả các chứng chỉ mà chúng tôi yêu cầu cho thiết lập này đã được tạo. Bây giờ chúng ta có thể xác minh các tệp chứng chỉ bằng lệnh bên dưới.

*openssl verify -CAfile ca.pem server-cert.pem client-cert.pem*

* Đảm bảo không có lỗi, kết quả như bên dưới.



* Tất cả các tệp Chứng chỉ đã được xác minh. Thay đổi chủ sở hữu của thư mục chứng chỉ thành người dùng 'mysql' và thay đổi quyền của tất cả các tệp chính.

*chown -R mysql:mysql /etc/certs/  
chmod 600 client-key.pem server-key.pem ca-key.pem*

## 4.Enable SSL for MySQL

* Trong bước này, chúng tôi sẽ kích hoạt SSL cho MySQL. Trước khi bắt đầu cấu hình và kích hoạt SSL trên MySQL, chúng ta cần sao lưu các tệp chứng chỉ mặc định vào thư mục sao lưu mới.
* Tạo thư mục sao lưu mới '**mysql-certs**' cho tất cả các chứng chỉ.

*mkdir -p ~/mysql-certs/*

* Đi tới thư mục '/var/lib/mysql' và di chuyển tất cả các chứng chỉ mặc định vào thư mục sao lưu.

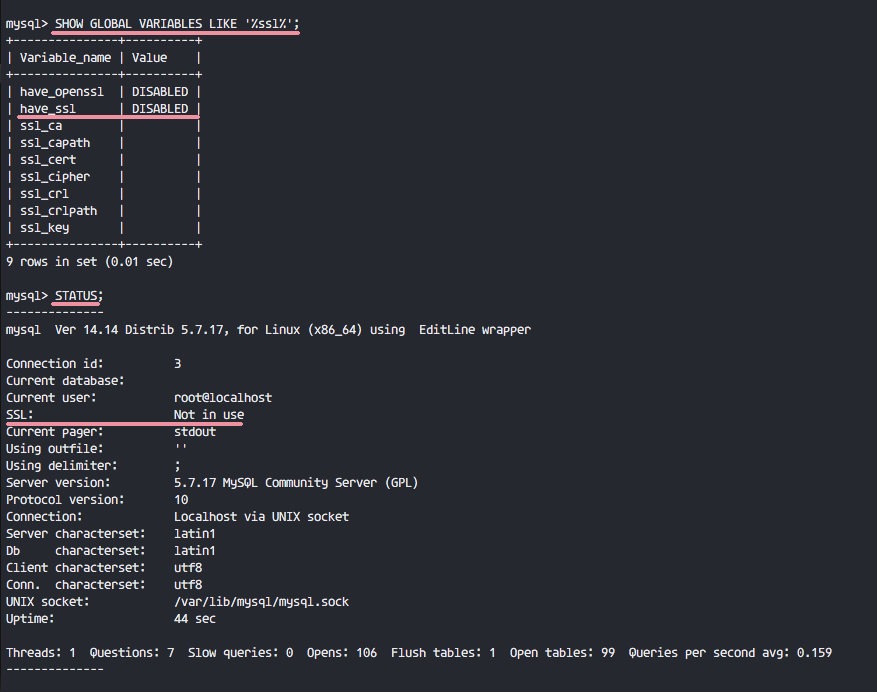
*cd /var/lib/mysql/  
mv ca.pem ca-key.pem ~/mysql-certs/  
mv server-key.pem server-cert.pem ~/mysql-certs/  
mv client-key.pem client-cert.pem ~/mysql-certs/  
mv private\_key.pem public\_key.pem ~/mysql-certs/*

* Bây giờ khởi động lại dịch vụ MySQL.

*systemctl restart mysqld*

* Tiếp theo, kiểm tra SSL từ MySQL shell. Đăng nhập vào mysql bằng mật khẩu mới:

*SHOW GLOBAL VARIABLES LIKE '%ssl%';  
STATUS;*

* Bạn sẽ thấy trạng thái SSL là ‘DISABLED’ và người dùng gốc đã được kết nối mà không có SSL.
* Tiếp theo, chúng tôi sẽ kích hoạt kết nối SSL cho MySQL. Chúng tôi phải chỉnh sửa tệp cấu hình MySQL tệp **'my.cnf'** bằng **vim or nano**.

*vim /etc/my.cnf*

* Trong phần **'[mysqld]'**, hãy dán cấu hình bên dưới.

*# Type your own certificates directory  
ssl-ca=/etc/certs/ca.pem  
ssl-cert=/etc/certs/server-cert.pem  
ssl-key=/etc/certs/server-key.pem*

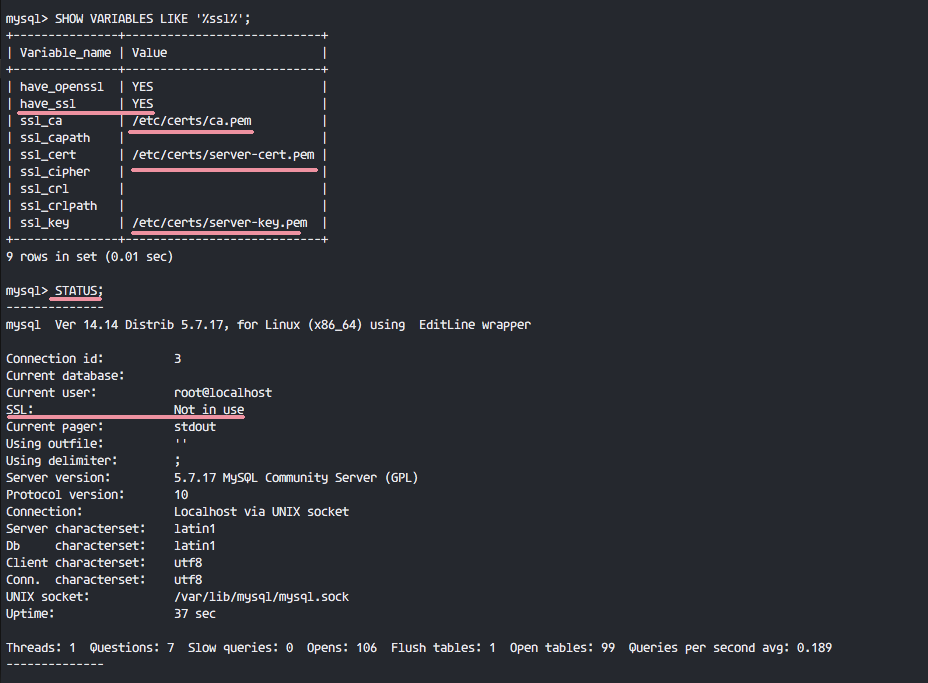
* Lưu tệp và thoát vim, khởi động lại dịch vụ MySQL.

*systemctl restart mysqld*

* Bây giờ đăng nhập lại vào MySQL và kiểm tra SSL.

*mysql -u root -p  
TYPE NEW PASSWORD 'Hakase-labs123@'*

* Chạy truy vấn bên dưới để đảm bảo giá trị phần SSL là **'YES'**.

*SHOW VARIABLES LIKE '%ssl%';  
STATUS;*

* Bạn sẽ thấy rằng SSL cho MySQL đã được kích hoạt, nhưng người dùng root vẫn không được kết nối bằng kết nối SSL.
* Để buộc tất cả kết nối người dùng cục bộ với SSL, hãy chỉnh sửa lại tệp cấu hình mysql **'my.cnf'**.

*vim /etc/my.cnf*

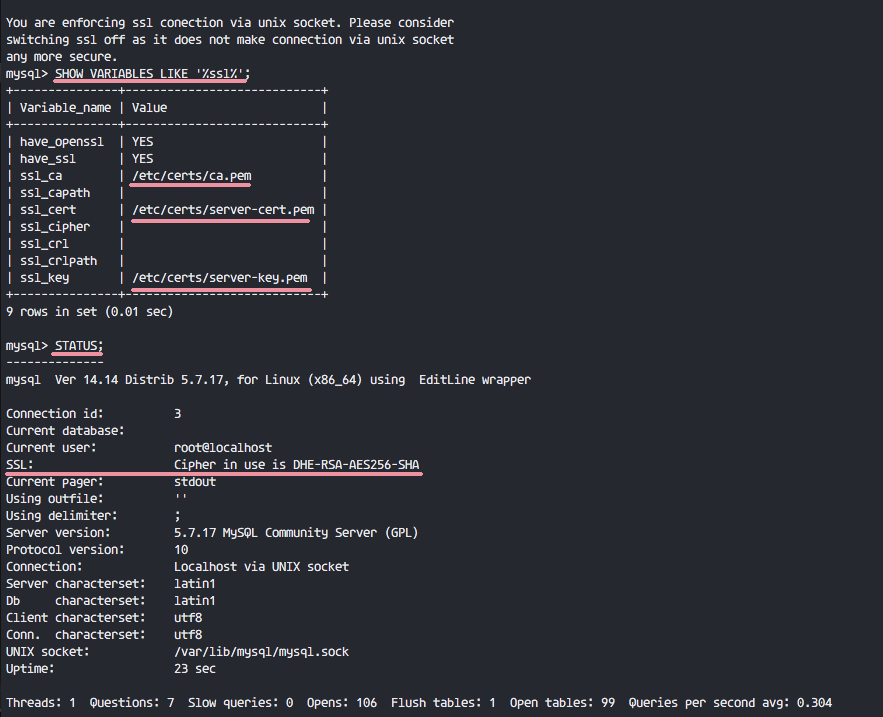
* Dán cấu hình bên dưới vào cuối dòng.

*[client]  
ssl-ca=/etc/certs/ca.pem  
ssl-cert=/etc/certs/client-cert.pem  
ssl-key=/etc/certs/client-key.pem*

* Lưu và thoát, sau đó khởi động lại MySQL.

*systemctl restart mysqld*

* Kết nối lại với MySQL và kiểm tra kết nối và SSL được kích hoạt.

*mysql -u root -p  
TYPE NEW PASSWORD 'Hakase-labs123@'  
   
   
SHOW VARIABLES LIKE '%ssl%';  
STATUS;*

* SSL đã được bật và kết nối cục bộ cũng sử dụng SSL.

## 5.Enable Remote Connections

* Trong các bước trên, chúng tôi đã bật SSL cho máy chủ MySQL và các kết nối cục bộ buộc phải sử dụng SSL. Trong bước này, chúng tôi sẽ kích hoạt kết nối từ xa cho MySQL, nhưng chúng tôi chỉ cho phép các máy khách có tệp chứng chỉ được CA của chúng tôi ký kết nối với máy chủ MySQL.
* Chỉnh sửa tệp cấu hình MySQL bằng vim

*vim /etc/my.cnf*

* Dán cấu hình này bên dưới vào cuối phần **'[mysqld]'**.

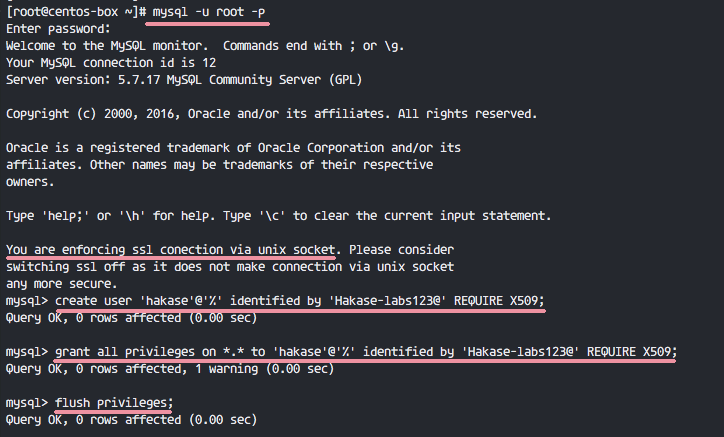
*bind-address = \*  
require\_secure\_transport = ON*

* Lưu tệp và thoát khỏi trình chỉnh sửa, khởi động lại MySQL.

*systemctl restart mysqld*

* Tiếp theo, tạo một người dùng mới cho kết nối từ xa. Tôi sẽ tạo một người dùng mới có tên **'hakase'** với mật khẩu **'Hakase-labs123 @'** và cấp tất cả các đặc quyền cho người dùng **'hakase'**. Người dùng **'hakase'** sẽ chỉ có thể kết nối với khóa Chứng chỉ.

*mysql -u root -p  
TYPE NEW PASSWORD 'Hakase-labs123@'  
   
create user 'hakase'@'%' identified by 'Hakase-labs123@' REQUIRE X509;  
grant all privileges on \*.\* to 'hakase'@'%' identified by 'Hakase-labs123@' REQUIRE X509;  
flush privileges;*

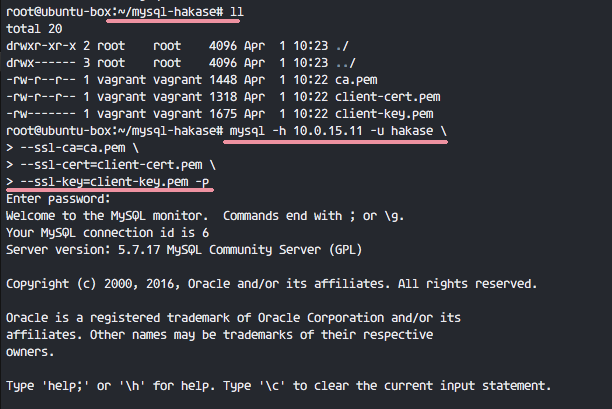
*  Người dùng mới cho kết nối từ xa đã được tạo.
* Ghi chú: Bạn có thể thấy '1 cảnh báo' trong kết quả truy vấn mysql. Đó chỉ là cảnh báo về việc sử dụng truy vấn ALTER USER thay vì GRANT vì truy vấn 'GRANT' sẽ không được chấp nhận trong bản phát hành tiếp theo.

## 6.Testing

* Trong phần cuối cùng của hướng dẫn này, chúng tôi sẽ kiểm tra xem liệu người dùng mới có tên 'hakase' có thể kết nối từ xa với máy chủ MySQL bằng các tệp chứng chỉ hay không. Ba chứng chỉ cho máy khách phải được tải xuống.
  + CA certificate - **ca.pem**
  + Client certificate - **client-cert.pem**
  + Client key - **client-key.pem**
* Tôi đã đăng nhập vào một hệ thống Linux khác và cài đặt các gói máy khách mysql ở đó. Sau đó, tôi đã tải xuống tất cả các tệp chứng chỉ ứng dụng khách với SCP. Bây giờ tôi sẽ kết nối với máy chủ MySQL với các tệp chứng chỉ.

*mysql -h 10.0.15.11 -u hakase \  
--ssl-ca=ca.pem \  
--ssl-cert=client-cert.pem \  
--ssl-key=client-key.pem -p*

* 10.0.15.11 = Địa chỉ IP của MySQL Server.

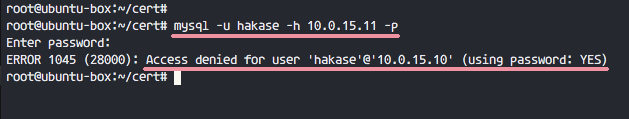


* Bạn có thể xem trạng thái kết nối với truy vấn này bên dưới.

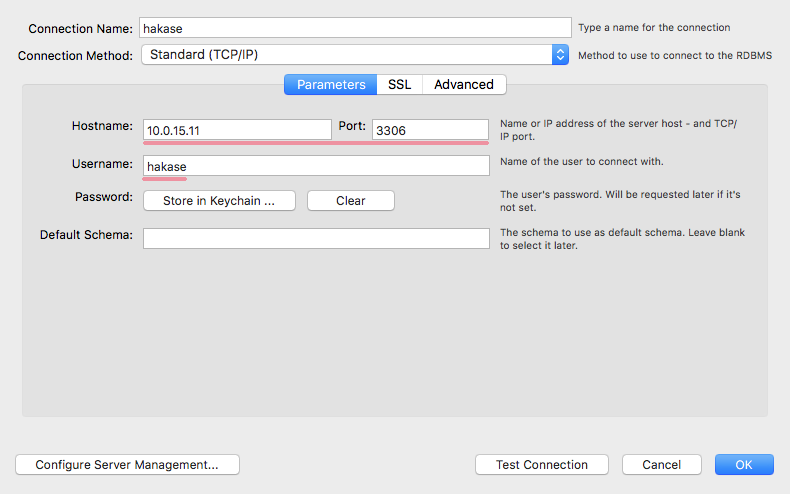
*STATUS;*



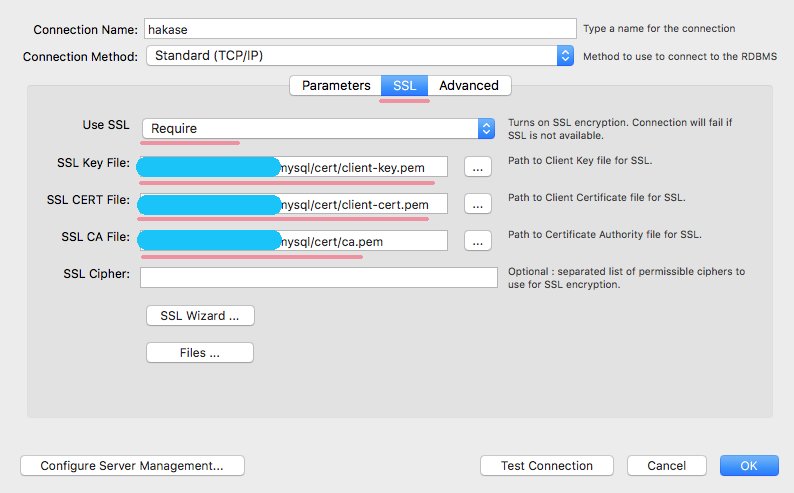
* Người dùng **hakase** với địa chỉ **IP 10.0.15.10** Đã kết nối với máy chủ MySQL có địa **chỉ IP 10.0.15.11**, kết nối qua TCP / IP trên cổng **3306** và sử dụng **SSL**.
* Khi bạn cố gắng kết nối mà không có tệp Chứng chỉ, bạn sẽ thấy lỗi như bên dưới.

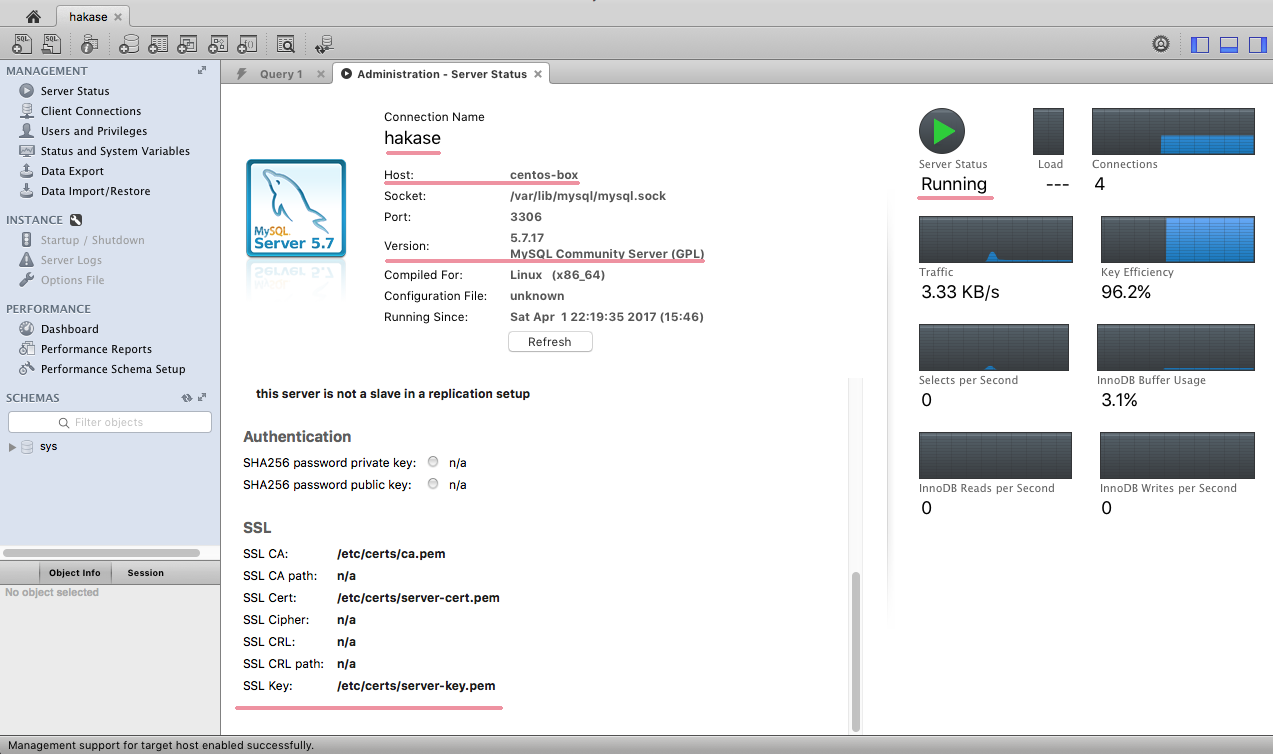


* Tiếp theo, tôi sẽ kiểm tra với MySQLWorkbench GUI từ máy chủ của tôi.



* Cấu hình SSL - Cài đặt SSL.



* Và bên dưới kết quả của kết nối với tệp Chứng chỉ máy khách SSL.
*  Một người dùng mới đã kết nối thành công từ xa với máy chủ cơ sở dữ liệu MySQL bằng kết nối SSL. Khi người dùng cố gắng kết nối mà không có tệp Chứng chỉ, kết quả sẽ bị 'từ chối'. Cài đặt và cấu hình MySQL với kết nối SSL đã thành công.