**HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO**

**MẬT HỆ QUẢN TRỊ CSDL MYSQL**

## **I. Nội dung hướng dẫn**

* Hướng dẫn thiết lập an toàn cho CSDL MySQL nhằm đảm bảo 6 tiêu chuẩn ATTT bao gồm:

[1. Cài đặt Hệ quản trị CSDL an toàn. 1](#_Toc449443929)

[2. Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng 1](#_Toc449443930)

[3. Thiết lập chính sách tài khoản 4](#_Toc449443933)

[4. Phân quyền an toàn 5](#_Toc449443937)

[5. Cấu hình ghi log cho hệ quản trị CSDL 7](#_Toc449443939)

[6. Cấu hình giới hạn truy cập 7](#_Toc449443940)

**II. Chi tiết hướng dẫn**

## **Cài đặt Hệ quản trị CSDL an toàn.**

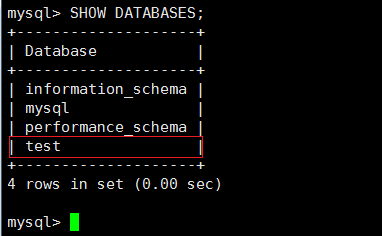
* Hệ quản trị cơ sở dữ liệu MySQL phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật (Tham chiếu hướng dẫn thiết lập ATTT cho hệ điều hành máy chủ).
* Phiên bản MySQL được phép sử dụng là phiên bản vẫn được nhà sản xuất duy trì các bản vá cập nhật:
* Thông tin về vòng đời các sản phầm MySQL tham khao đường dẫn <https://www.mysql.com/support/supportedplatforms/database.html>
* Đối với hệ thống cài mới: Sử dụng MySQL phiên bản mới nhất (Tham khảo: <http://dev.mysql.com/downloads/mysql>). Tại thời điểm hiện tại phiên bản tối thiểu được phép cài đặt là:
  + Đối với dòng 5.5 là phiên bản **5.5.54**
  + Đối với dòng 5.6 là phiên bản **5.6.35**
  + Đối với dòng 5.7 là phiên bản **5.7.17**
* Các hệ thống đang hoạt động phải được cập nhật các bản vá bảo mật đã được TTANM và P.CNTT – TĐ cảnh báo.
* Không sử dụng các bộ cài tích hợp sẵn như: Xampp, wampp, appserver.

## **Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng**

### Xóa các tài khoản, các CSDL thừa, không sử dụng

* Liệt kê danh sách các CSDL:

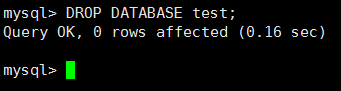
mysql> SHOW DATABASES;



Hình : Không được xóa các CSDL của hệ thống: information\_schema, mysql, performance\_schema.

* Xóa các CSDL thừa:

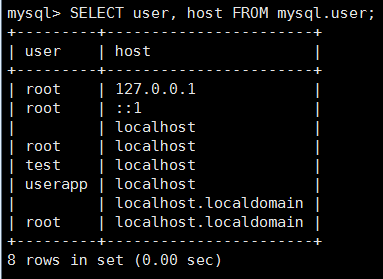
mysql> DROP DATABASE ‘ten\_CSDL’;



Hình : Xóa CSDL ‘test’

* Liệt kê danh sách các tài khoản có trong bảng mysql:

mysql> SELECT user, host FROM mysql.user;



Hình : Danh sách tài khoản.

* Xóa tài khoản thừa:

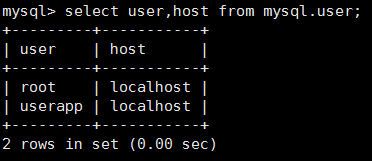
Đối với phiên bản từ 5.0 trở lên có thể sử dụng:

mysql> DROP USER ‘ten\_user’@’ten\_host’;

Với phiên bản cũ hơn

mysql> DELETE FROM mysql.user WHERE user = 'ten\_user' and host = 'dia\_chi\_host';

mysql> FLUSH PRIVILEGES;



Hình : Sau khi xóa tài khoản thừa.

Thay đổi tên mặc định của tài khoản quản trị.

* Mặc định tài khoản quản trị là ’root’, để thay đổi sử dụng câu lệnh:

Đối với phiên bản từ 5.0.2 trở lên:

mysql> RENAME USER root TO ten\_moi;

Đối với phiên bản cũ hơn:

mysql> UPDATE user SET user = 'ten\_moi' WHERE user = 'root';

mysql> FLUSH PRIVILEGES;

### Tắt các hàm tương tác với tài nguyên của hệ điều hành

* Vô hiệu hóa, thu hồi các quyền tương tác với file của hệ điều hành (Xem mục 4.3)

## **Thiết lập chính sách tài khoản**

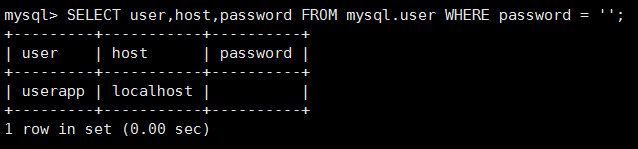
### Không dùng tài khoản quản trị cho các ứng dụng để kết nối đến CSDL.

* Không dùng tài khoản quản trị **root** (tài khoản đã đổi tên có quyền tương đương tài khoản **root**) cho các ứng dụng kết nối tới CSDL.

### Tất cả các tài khoản phải có mật khẩu

* Liệt kê danh sách các tài khoản không có mật khẩu

mysql> SELECT user,host,password FROM mysql.user WHERE password = '';



Hình : Liệt kê tài khoản có mật khẩu rỗng.

* Đặt mật khẩu cho những tài khoản liệt kê được, mật khẩu phải tuân theo đúng quy định của Tập đoàn (tham khảo mục 3.3).

### Các tài khoản phải được đặt mật khẩu theo đúng quy định của Tập đoàn:

* Các tài khoản phải có mật khẩu, mât khẩu tối thiểu 8 ký tự bao gồm: ký tự chữ, số và ký tự đặc biệt.
* Đối với tạo mới tài khoản:

mysql> CREATE USER 'ten\_user'@'dia\_chi\_host' IDENTIFIED BY 'mat\_khau';

* Đặt mật khẩu cho những tài khoản đã tồn tại:

Đối với phiên bản từ 5.0 trở lên

mysql> SET PASSWORD FOR 'ten\_user'@'dia\_chi\_host' = PASSWORD('mat\_khau');

Với phiên bản cũ hơn:

mysql> UPDATE mysql.user SET password = PASSWORD('mat\_khau') WHERE user = 'ten\_user' AND host ='dia\_chi\_host';

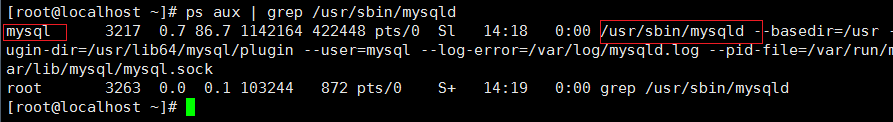
mysql> FLUSH PRIVILEGES;

## **Phân quyền an toàn**

Không dùng các tài khoản quản trị, nhóm quản trị: root, Administrator, Local System,... để chạy dịch vụ CSDL.

* Kiểm tra tài khoản đang chạy dịch vụ MySQL:

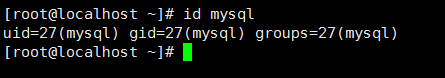
# ps aux | grep /usr/sbin/mysqld



Hình : Thông tin tiến trình chạy dịch vụ MySQL

* Kiểm tra tài khoản có thuộc nhóm quản trị không:

# id 'ten\_tai\_khoan'



Hình : Thông tin tài khoản chạy dịch vụ MySQL

* Kiểm tra tài khoản có được đăng nhập hay không:

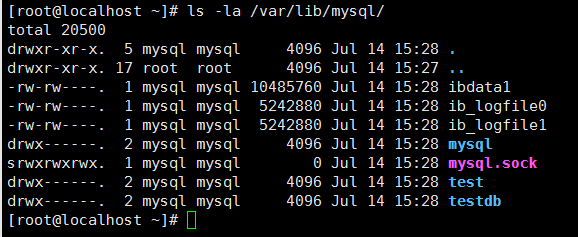
# passwd -S 'ten\_tai\_khoan'



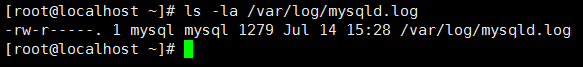
Hình : Đảm bảo rằng tài khoản đã bị khóa, không được đăng nhập

### Phân quyền tối thiểu cho các thư mục chứa dữ liệu, thư mục chứa log, thư mục backup (nếu có)

* Thư mục chứa dữ liệu sẽ được cấu hình bởi tham số **datadir** trong file cấu hình của MySQL (/etc/my.conf). Nếu không có cấu hình này thì mặc định sẽ là /var/lib/mysql/.
* Sử dụng câu lệnh: ls –la duong\_dan\_thu\_muc. Đảm bảo rằng các file, thư mục trong này có owner là root hoặc mysql (tài khoản chạy dịch vụ), nhóm other không được có quyền tác động.

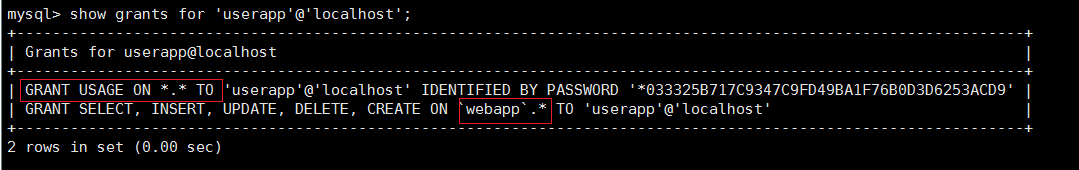


* Kiểm tra quyền của file log: Mặc định MySQL ghi error log được cấu hình trong file my.conf với cấu hình **log-error**, kiểm tra quyền của file này:



* Với mỗi CSDL của ứng dụng, tạo tài khoản riêng và chỉ cấp quyền tác động trên CSDL đó.
* Kiểm tra quyền của tài khoản

mysql> SHOW GRANTS FOR 'ten\_tai\_khoan'@'dia\_chi\_host';

Hình 9: Xem thông tin quyền của tài khoản.

* Đảm bảo quyền global (**\*.\***) không có các quyền **FILE**, và các quyền quản trị như **GRANT**, **SUPPER**, **PROCESS**, **RELOAD**, **SHUTDOWN**,... và chỉ có quyền tác động trên một CSDL.
* Để loại bỏ quyền của 1 tài khoản:

mysql> REVOKE ten\_quyen ON 'ten\_csdl' FROM 'ten\_tai\_khoan'@'dia\_chi\_host';

mysql> FLUSH PRIVILEGES;

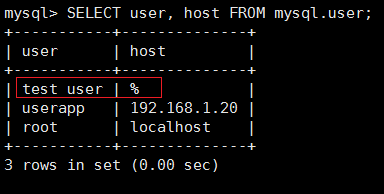
## **Cấu hình ghi log cho hệ quản trị CSDL**

* Mặc định MySQL không có tính năng ghi auditlog.

## **Cấu hình giới hạn truy cập**

* Các tài khoản chỉ được kết nối từ một host cố định
* Liệt kê danh sách tài khoản

mysql> SELECT user, host FROM mysql.user;



Hình : Loại bỏ các tài khoản có host là ’%’

* Cấu hình giới hạn truy cập trên tường lửa mềm
* Cấu hình giới hạn chỉ những ip của những tài khoản liệt kê ở mục trên được kết nối tớ cổng của dịch vụ (Tham chiếu Baseline thiết lập chính sách bảo mật trên hệ điều hành).