**HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT**

**HỆ QUẢN TRỊ CSDL MSSQL**

**I. Nội dung hướng dẫn**

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

[1. Cài đặt hệ quản trị CSDL an toàn. 1](#_Toc449443477)

[2. Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng 2](#_Toc449443478)

[3. Thiết lập chính sách tài khoản 4](#_Toc449443482)

[4. Phân quyền an toàn 5](#_Toc449443486)

[5. Cấu hình ghi log cho hệ quản trị CSDL. 10](#_Toc449443490)

[6. Cấu hình giới hạn truy cập. 11](#_Toc449443491)

**II. Chi tiết hướng dẫn**

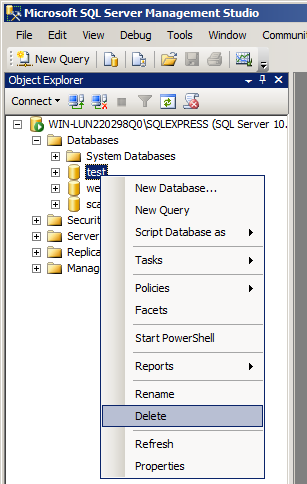
## **Cài đặt hệ quản trị CSDL an toàn.**

* SQL Server 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 SQL Server 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 phảm SQL Server: Tham khảo đường dẫn <https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20SQL%20Server>
* Đối với hệ thống cài mới: SQL Server phải được cài bản Service Pack mới nhất đối với từng phiên bản (Tham khảo: <https://technet.microsoft.com/en-us/sqlserver/ff803383.aspx>). Tại thời điểm hiện tại Service Pack tối thiểu cần phải cài đặt:
  + SP1 đối với SQL Server 2016
  + SP2 đối với SQL Server 2014
  + SP3 đối với SQL Server 2012
  + SP4 đối với SQL Server 2008
  + SP3 đối với SQL Server 2008 R2
* Các hệ thống đang hoạt động phải được cập nhật các bản vá bảo mật đã được TTANM và P.CNTT – TĐ cảnh báo.

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

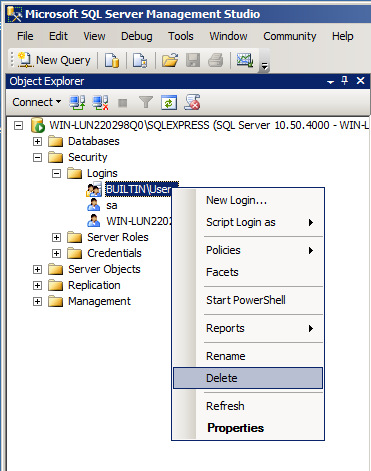
### **Xóa các tài khoản, các CSDL thừa, không sử dụng**

* Truy cập Microsoft Server Management Studio, xóa bỏ các CSDL không sử dụng:



Hình : Xóa CSDL thừa, không sử dụng

* Truy cập Microsoft Server Management Studio, xóa bỏ các tài khoản thừa, không sử dụng:



Hình : Xóa tài khoản thừa không sử dụng.

### **Thay đổi tên mặc định của tài khoản quản trị**

* Mặc định tài khoản quản trị là **sa**, để thay đổi tài khoản thực hiện lần lượt các câu lệnh:

ALTER LOGIN sa DISABLE

ALTER LOGIN sa WITH NAME = [ten\_moi]

ALTER LOGIN ten\_moi ENABLE

### **Tắt các hàm tương tác với tài nguyên hệ điều hành (hàm đọc, ghi file, thực thi câu lệnh hệ thống)**

* Vô hiệu hóa tính năng **xp\_cmdshell**, từ cửa sổ dòng lệnh SQL của Microsoft Server Management Studio thực thi câu lệnh sau:

EXEC sp\_configure 'show advanced', 1

RECONFIGURE

EXEC sp\_configure 'xp\_cmdshell',0

RECONFIGURE

## **Thiết lập chính sách tài khoản**

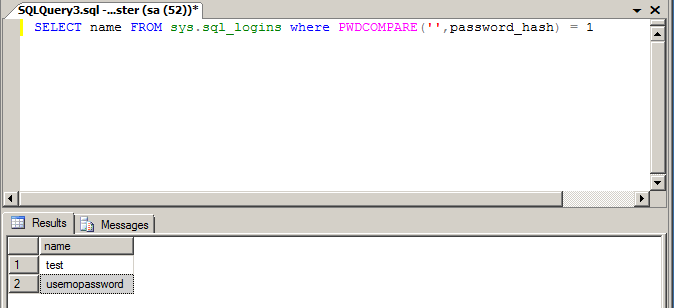
### **Không dùng tài khoản quản trị cho các ứng dụng để kết nối đến CSDL**

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

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

* Tìm tất cả các tài khoản có mật khẩu rỗng:

SELECT name FROM sys.sql\_logins where PWDCOMPARE('',password\_hash) = 1;

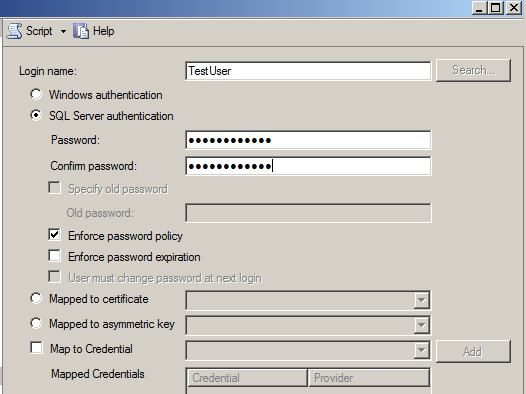


Hình : Danh sách tài khoản có mật khẩu rỗng.

* 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**

* Nếu sử dụng xác thực tài khoản SQL Server hỗ trợ (**SQL Server authentication**), 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.
* Khi tạo mới hoặc đặt mật khẩu cho tài khoản, trong cửa sổ tùy chọn, click chọn "Enforce password policy" để áp dụng chính sách tài khoản của hệ điều hành (đảm bảo máy chủ đã được cấu hình bảo mật an toàn toàn thông tin).



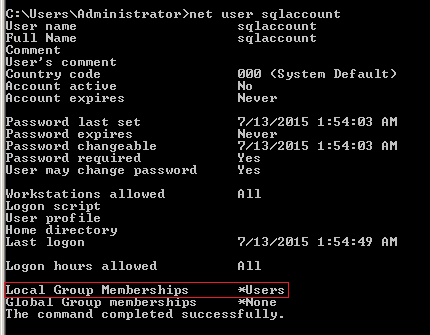
Hình : Tạo mới tài khoản.

## **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 MSSQL: Vào **Start 🡪 All Programs 🡪 Microsoft SQL Server 2008 R2🡪 Configuration Tools 🡪 SQL Server Configuration Manager**, chọn **SQL Server Services**. Trong cột ’Log On As’ là tài khoản đang chạy dịch vụ.
* Nếu là tài khoản build-in: không đượcl à Local System
* Nếu là tài khoản hệ điều hành: không được là Administrator, không thuộc nhóm Administrator, không được phép đăng nhập
* Cách kiểm tra tài khoản hệ điều hành: trong cửa sổ cmd sử dụng câu lệnh:

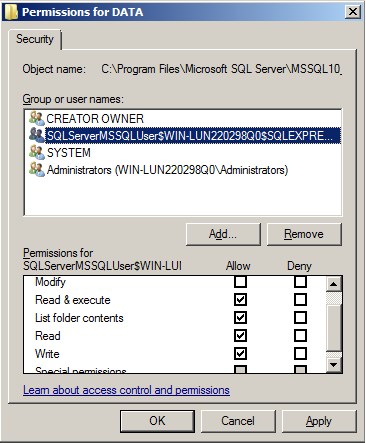
NET USER ‘ten\_tai\_khoan’



Hình : Xem thông tin người dùng

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

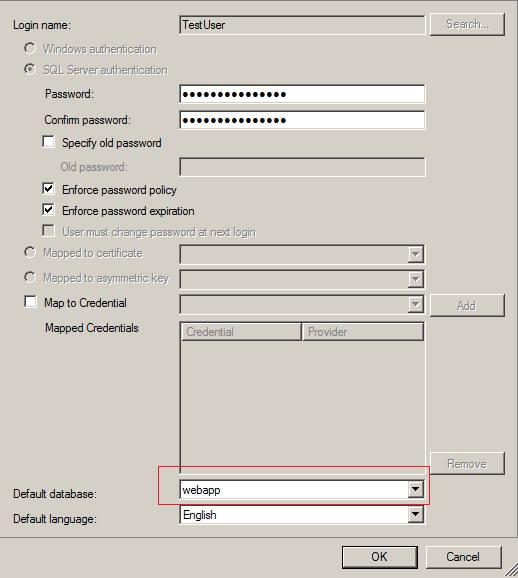
* Truy cập vào thư mục cài đặt MSSQL: C:\Program Files\Microsoft SQL Server\**MSSQL10\_50.SQLEXPRESS**\MSSQL (Lưu ý đường dẫn phần bôi đậm có thể khác đối với từng phiên bản khác nhau).
* Phân quyền cho thư mục chứa dữ liệu, thư mục chứa log, thư mục backup:
  + Chuột phải vào thư **DATA** chọn properties, trong tab security là danh sách quyền của người dùng đối với thư mục, loại bỏ các quyền thừa, sửa hoặc thêm quyền người dùng **SQLServerMSSQLUser**: có các quyền: Read & execute, list folder contents, read, write
  + Làm tương tự đối với thư mục **Log** và thư mục **Backup**



Hình : Phân quyền cho thư mục **DATA**.

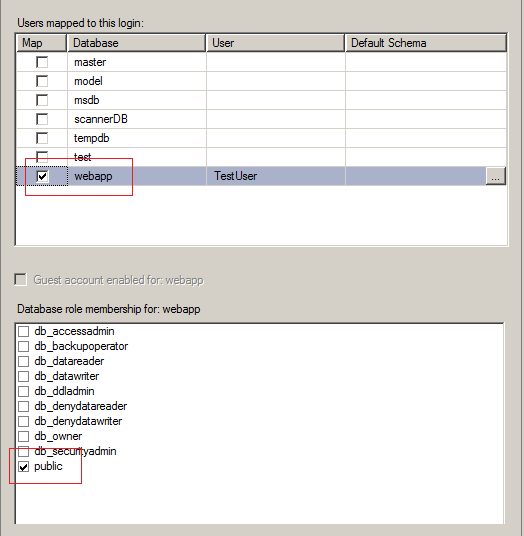
### **Với mỗi CSDL của ứng dụng, tạo tài khoản riêng và chỉ cấp quyền tác động trên CSDL đó**

* Gán quyền cho user vào CSDL cần kết nối: Vào **SQL Server Management Studio** 🡪 **Security 🡪 Logins 🡪** Chuột phải vào User cần phân quyền chọn **Properties 🡪** General 🡪 **Default database** 🡪 Chọn CSDL gán cho user.



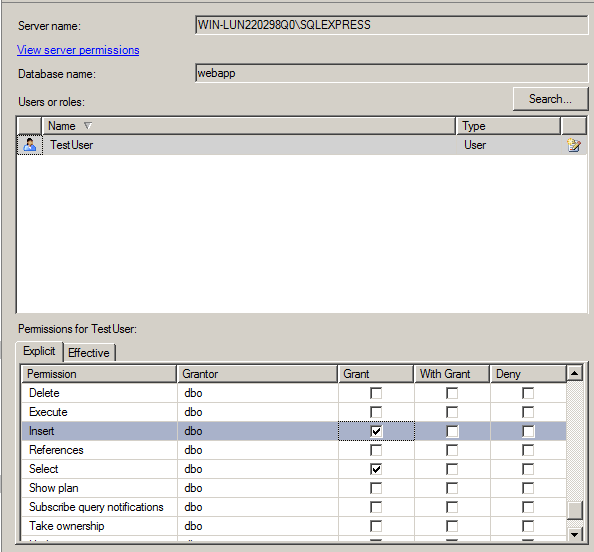
Hình : Chọn CSDL mặc định cho tài khoản

* Gán các quyền cho tài khoản ở mục **User Mapping**: Chọn CSDL mà tài khoản có quyền tác động, chú ý không gán quyền theo **Role**.



Hình : Chỉ chọn 1 CSDL và role public.

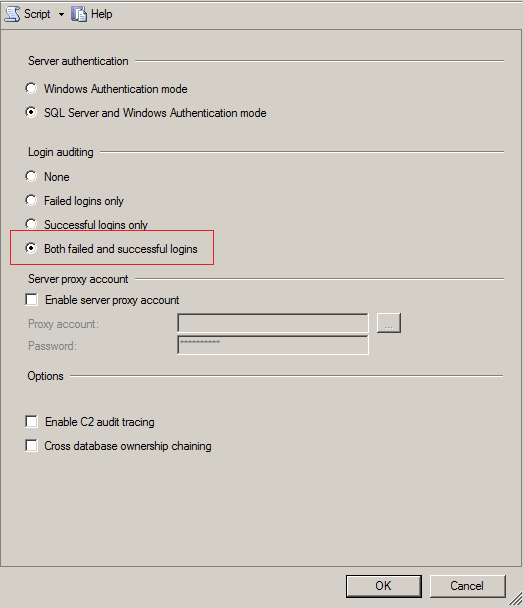
* Gán quyền cho CSDL: Gán quyền tối thiểu cho tài khoản của ứng dụng như SELECT, UPDATE, INSERT. Chuột phải vào CSDL cần phân quyền 🡪 Chọn **Properties** 🡪 **Permissions** 🡪 Chọn tài khoản cần gán quyền 🡪 Chọn các quyền tối thiểu cho tài khoản.



Hình : Chọn quyền tối thiểu cần thiết cho tài khoản.

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

* Bật tính năng ghi login audit, cấu hình ghi log cả đăng nhập thành công và không thành công:



Hình : Cấu hình ghi log cả đăng nhập thành công và không thành công.

## **Cấu hình giới hạn truy cập.**

* Cấu hình tường lửa mềm cho phép những ip nhất định được truy cập vào cổng của dịch vụ MSSQL (Tham chiếu theo Baseline thiết lập chính sách bảo mật trên hệ điều hành)