



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



**BÀI GIẢNG MÔN
AN TOÀN ỨNG DỤNG WEB & CSDL**

CHƯƠNG 6 – CÁC CƠ CHẾ BẢO MẬT CƠ SỞ DỮ LIỆU

Giảng viên:

E-mail:

Khoa:

PGS.TS. Hoàng Xuân Dậu

dauhx@ptit.edu.vn

An toàn thông tin

NỘI DUNG CHƯƠNG 6

1. Xác thực, trao quyền và bảo mật mật khẩu
2. Bảo mật các đối tượng trong CSDL
3. Sử dụng mã hóa trong CSDL
4. Một số biện pháp bảo mật khác
5. Mô hình bảo mật ở một số DBMS

6.1 Xác thực, trao quyền và bảo mật mật khẩu

- ❖ Xác thực & trao quyền
- ❖ Bảo mật mật khẩu

6.1.1 Xác thực & trao quyền

- ❖ Điều khiển truy cập vào CSDL nói riêng hoặc các hệ thống nói chung dựa trên 2 dịch vụ:
 - Xác thực (Authentication): Là quá trình xác minh tính chân thực của các thông tin nhận dạng mà người dùng cung cấp.
 - Trao quyền (Authorization): Xác định các tài nguyên mà người dùng được phép truy nhập sau khi người dùng đã được xác thực.

6.1.1 Xác thực & trao quyền

❖ Thông tin nhận dạng người dùng có thể gồm:

- Bạn là ai (Who you are)?
 - CMND
 - Bằng lái xe
 - Vân tay,...
- Những cái bạn biết (What you know) ?
 - Tên truy nhập, mật khẩu,
 - Số PIN...
- Bạn có gì (What you have)?
 - Thẻ ATM
 - Thẻ tín dụng,...

6.1.1 Xác thực & trao quyền

❖ Xác thực 1 hoặc nhiều nhân tố:

- Xác thực 1 nhân tố: các nhân tố xác thực trong 1 nhóm kể trên.
 - VD: mật khẩu.
- Xác thực 2 nhân tố: các nhân tố xác thực trong 2 nhóm kể trên.
 - VD: Thẻ ATM + PIN.
- Xác thực 3 nhân tố: các nhân tố xác thực trong 3 nhóm kể trên.
 - VD: Thẻ ATM + Vân tay + PIN.

❖ Nguyên tắc chung: Số nhân tố sử dụng trong 1 quá trình xác thực càng nhiều thì nó càng an toàn:

- VD: Thẻ + vân tay + PIN cho mức an toàn rất cao.

6.1.1 Xác thực & trao quyền

❖ Xác thực là thành phần cơ sở của mô hình bảo mật



6.1.1 Xác thực & trao quyền

- ❖ Lựa chọn phương pháp xác thực phù hợp trong số các phương pháp xác thực sẵn có:
 - Không xác thực (No authentication / Trusted client)
 - Xác thực dựa trên hệ điều hành
 - Xác thực dựa trên hệ quản trị CSDL
 - Xác thực hỗn hợp (hệ điều hành hoặc hệ quản trị CSDL)

6.1.1 Xác thực & trao quyền

❖ Không nên sử dụng các phương pháp:

- Không xác thực hoặc
- Tin tưởng máy khách.

❖ Khuyến nghị:

- Nên sử dụng phương pháp xác thực dựa trên hệ điều hành do hệ điều hành có cơ chế quản lý thông tin người dùng tương đối tốt và cơ chế xác thực mạnh.

6.1.1 Xác thực & trao quyền

- ❖ Các phương pháp xác thực của một số DBMS cụ thể:
 - Các phương pháp xác thực hỗ trợ bởi DB2 UDB 8.2;
 - Các phương pháp xác thực hỗ trợ bởi MS SQL Server;
 - Các phương pháp xác thực hỗ trợ bởi Oracle Server.

6.1.1 Xác thực & trao quyền

- ❖ Các phương pháp xác thực hỗ trợ bởi DB2 UDB 8.2:
 - SERVER_ENCRYPT: Xác thực thực hiện trên máy chủ và máy khách phải cung cấp tên người dùng và mật khẩu;
 - KERBEROS: Sử dụng giao thức KERBEROS để xác thực máy khách. KERBEROS cho phép một máy khách xác thực và trao đổi khóa với một máy chủ dịch vụ nhờ sự hỗ trợ của máy chủ KERBEROS;
 - KRB_SERVER_ENCRYPT: Cho phép lựa chọn phương pháp xác thực sử dụng KERBEROS hoặc SERVER_ENCRYPT;
 - DATA_ENCRYPT: Tương tự SERVER_ENCRYPT, nhưng dữ liệu trao đổi trong cả phiên làm việc được mã hóa;

6.1.1 Xác thực & trao quyền

- ❖ Các phương pháp xác thực hỗ trợ bởi DB2 UDB 8.2:
 - DATA_ENCRYPT_CMP: Xác thực tương tự SERVER_ENCRYPT và truyền thông trong phiên làm việc được mã hóa nếu máy khách hỗ trợ và không được mã hóa nếu máy khách không hỗ trợ;
 - GSSPLUGIN: Phương pháp xác thực mở rộng, cho phép sử dụng bất kỳ một phương pháp xác thực nào tuân theo GSS API (Generic Security Service Application Program Interface);
 - GSS_SERVER_ENCRYPT: Phương pháp xác thực có thể là GSSPLUGIN hoặc SERVER_ENCRYPT.

6.1.1 Xác thực & trao quyền

- ❖ Các phương pháp xác thực hỗ trợ bởi MS SQL Server:
 - Xác thực bởi hệ điều hành (Windows authentication)
 - MS SQL hoàn toàn dựa vào hệ điều hành để xác thực người dùng và liên kết người dùng với các nhóm;
 - Là phương pháp xác thực Microsoft khuyến nghị sử dụng.
 - Xác thực hỗn hợp (Mixed authentication)
 - Xác thực bởi Windows
 - Được thực hiện nếu máy khách hỗ trợ NTLM (NT LAN Manager) hoặc Kerberos.
 - Xác thực bởi MS SQL Server

6.1.1 Xác thực & trao quyền

- ❖ Các phương pháp xác thực hỗ trợ bởi Oracle: Oracle hỗ trợ nhiều phương pháp xác thực, trong đó, 2 phương pháp được sử dụng phổ biến là:
 - Xác thực bởi hệ điều hành
 - Oracle hoàn toàn dựa vào hệ điều hành để xác thực người dùng và liên kết người dùng với các nhóm;
 - Xác thực bởi Oracle Server

6.1.1 Xác thực & trao quyền

- ❖ Vấn đề quản lý và sử dụng những người dùng có quyền quản trị CSDL:
 - Nhận dạng và có biện pháp giám sát những người dùng có quyền quản trị CSDL:
 - Tùy thuộc vào phương pháp xác thực, nhận dạng danh sách người dùng (người dùng của HĐH và của hệ quản trị CSDL) có quyền quản trị (administration) CSDL;
 - Giám sát hoạt động của người dùng quản trị trên CSDL.

6.1.1 Xác thực & trao quyền

- ❖ Vấn đề quản lý và sử dụng những người dùng có quyền quản trị CSDL:
 - Hạn chế đến tối thiểu số lượng người dùng có quyền quản trị trên CSDL.
 - Không sử dụng người dùng có quyền quản trị trong các thao tác dữ liệu của các ứng dụng.

6.1.2 Bảo mật mật khẩu

- ❖ Mặc dù có nhiều công nghệ xác thực, nhưng xác thực dựa trên mật khẩu vẫn là phương pháp được sử dụng phổ biến nhất trong xác thực người dùng CSDL;
- ❖ Lý do cho sự phổ biến của việc sử dụng mật khẩu:
 - Đảm bảo được mức an toàn tối thiểu;
 - Đơn giản, dễ sử dụng;
 - Chi phí cài đặt, quản lý và vận hành thấp.

6.1.2 Bảo mật mật khẩu

- ❖ Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:
 - Độ khó đoán của mật khẩu
 - Dùng nhiều loại ký tự
 - Chữ thường, hoa, chữ số, ký tự đặc biệt:
 - » abc1234: mật khẩu tồi
 - » aBc*1#24: mật khẩu tốt (về mặt tính toán)
 - Độ dài của mật khẩu
 - Mật khẩu người dùng tốt có chiều dài ≥ 8 ký tự
 - Mật khẩu quản trị tốt cần có chiều dài ≥ 10 ký tự
 - Mật khẩu cho truy nhập CSDL từ ứng dụng nên đảm bảo có đủ 4 loại ký tự và độ dài từ 10 ký tự trở lên.
 - Tuổi thọ của mật khẩu

6.1.2 Bảo mật mật khẩu

- ❖ Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:
 - Tuổi thọ của mật khẩu
 - Mật khẩu không hết hạn (không nên dùng)
 - Mật khẩu có thời hạn sống (thời gian sống của mật khẩu nên đặt phụ thuộc chính sách an ninh, an toàn của cơ quan, tổ chức.
 - Có thể là 1, 2, 3, hoặc 6 tháng.
 - Mật khẩu dùng 1 lần (ít dùng trong xác thực người dùng CSDL).

6.1.2 Bảo mật mật khẩu

- ❖ Tránh sử dụng các mật khẩu ngầm định hoặc mật khẩu "yếu":
 - Nhiều hệ quản trị CSDL, như SQL Server 7, 2000 cho phép user sa (có quyền quản trị hệ thống) không có mật khẩu (mật khẩu rỗng);
 - Sử dụng các mật khẩu ngắn, dễ đoán, như tên, ngày tháng năm sinh, tên đăng nhập ...
 - Dùng một mật khẩu (kể cả mật khẩu tốt) trên nhiều hệ thống.

6.1.2 Bảo mật mật khẩu

❖ Áp dụng chính sách quản lý mật khẩu "mạnh":

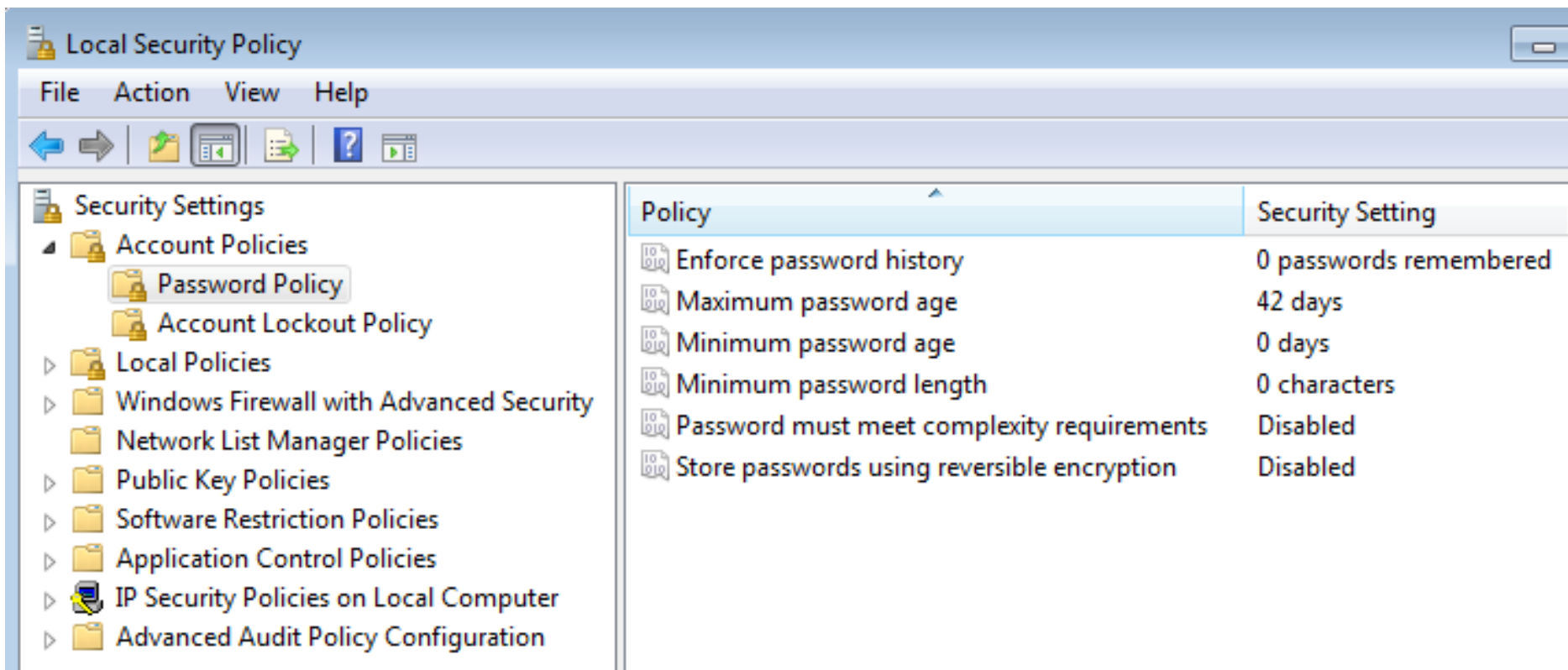
The screenshot shows the 'Login Properties - travelvisa' dialog box. On the left, a tree view under 'Select a page' includes 'General', 'Server Roles', 'User Mapping', 'Securables', and 'Status'. The 'General' tab is active. The main area has a 'Script' button and a 'Help' link. The 'Login name' field contains 'travelvisa' with a 'Search...' button. Below, 'Windows authentication' is unselected and 'SQL Server authentication' is selected. There are two password fields, both masked with dots. A checkbox for 'Specify old password' is unselected, with an 'Old password' field below it. At the bottom, 'Enforce password policy' and 'Enforce password expiration' are checked, while 'User must change password at next login' is unselected.

6.1.2 Bảo mật mật khẩu

- ❖ Áp dụng chính sách quản lý mật khẩu "mạnh": VD với MS SQL Server:
 - Enforce password policy: Bắt buộc áp dụng chính sách quản lý mật khẩu;
 - Enforce password expiration: Áp dụng thời gian hết hạn cho mật khẩu.
 - User must change password at next logon: Bắt buộc người dùng phải đổi mật khẩu ở lần đăng nhập tiếp theo.
- ❖ Chính sách quản lý mật khẩu được áp dụng là chính sách an ninh của hệ điều hành.

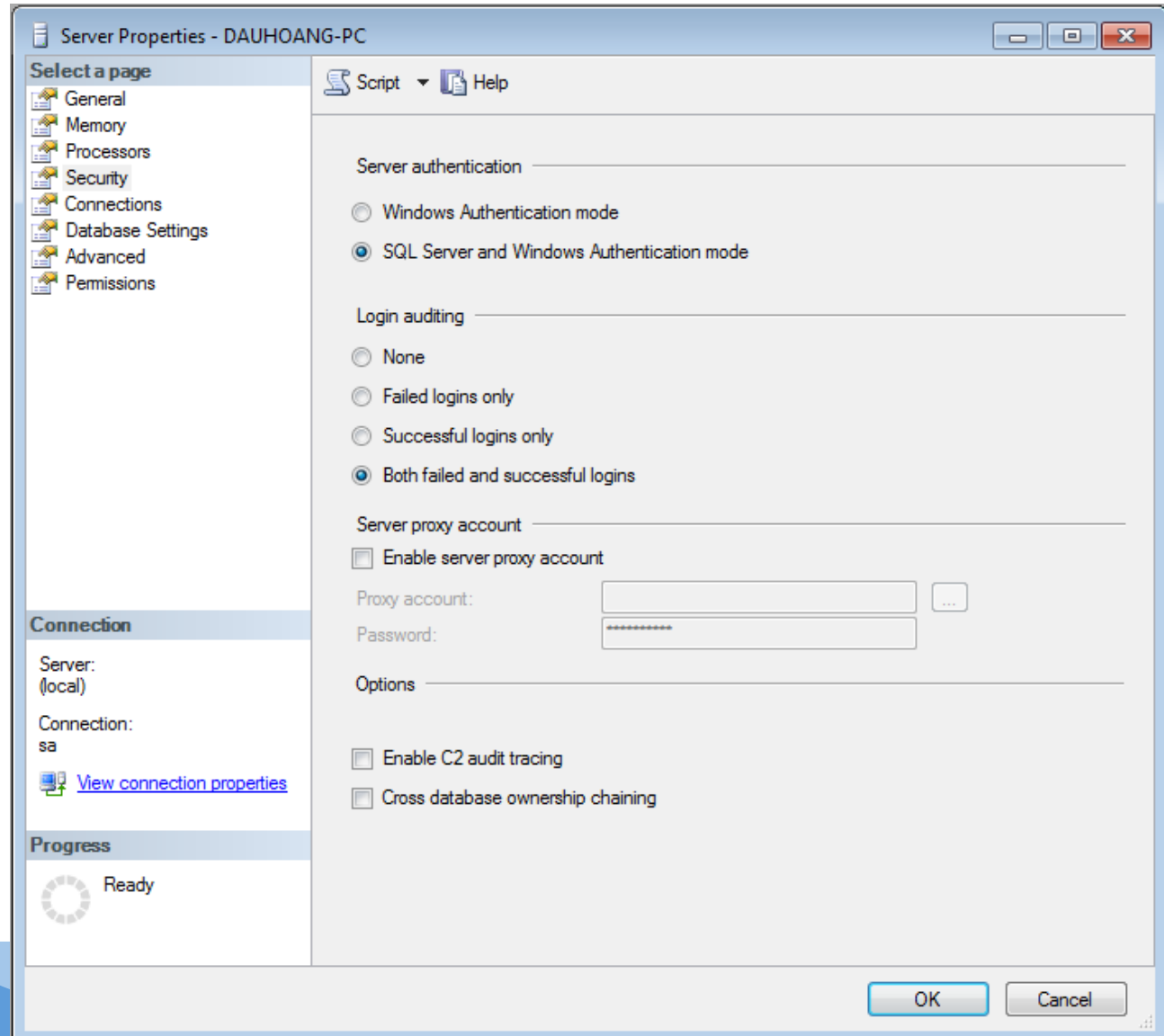
6.1.2 Bảo mật mật khẩu

- ❖ Chính sách quản lý mật khẩu được áp dụng là chính sách an ninh của hệ điều hành: MS Windows.



6.1.2 Bảo mật mật khẩu

❖ Ghi logs
đăng nhập
(MS SQL):



6.1.2 Bảo mật mật khẩu

- ❖ Dùng công cụ crack để kiểm tra mật khẩu CSDL:
 - SQLDict: <http://ntsecurity.nu/toolbox/sqldict/>

6.1.2 Bảo mật mật khẩu

❖ Sử dụng công cụ quản lý mật khẩu: KeePass



6.2 Bảo mật các đối tượng trong CSDL

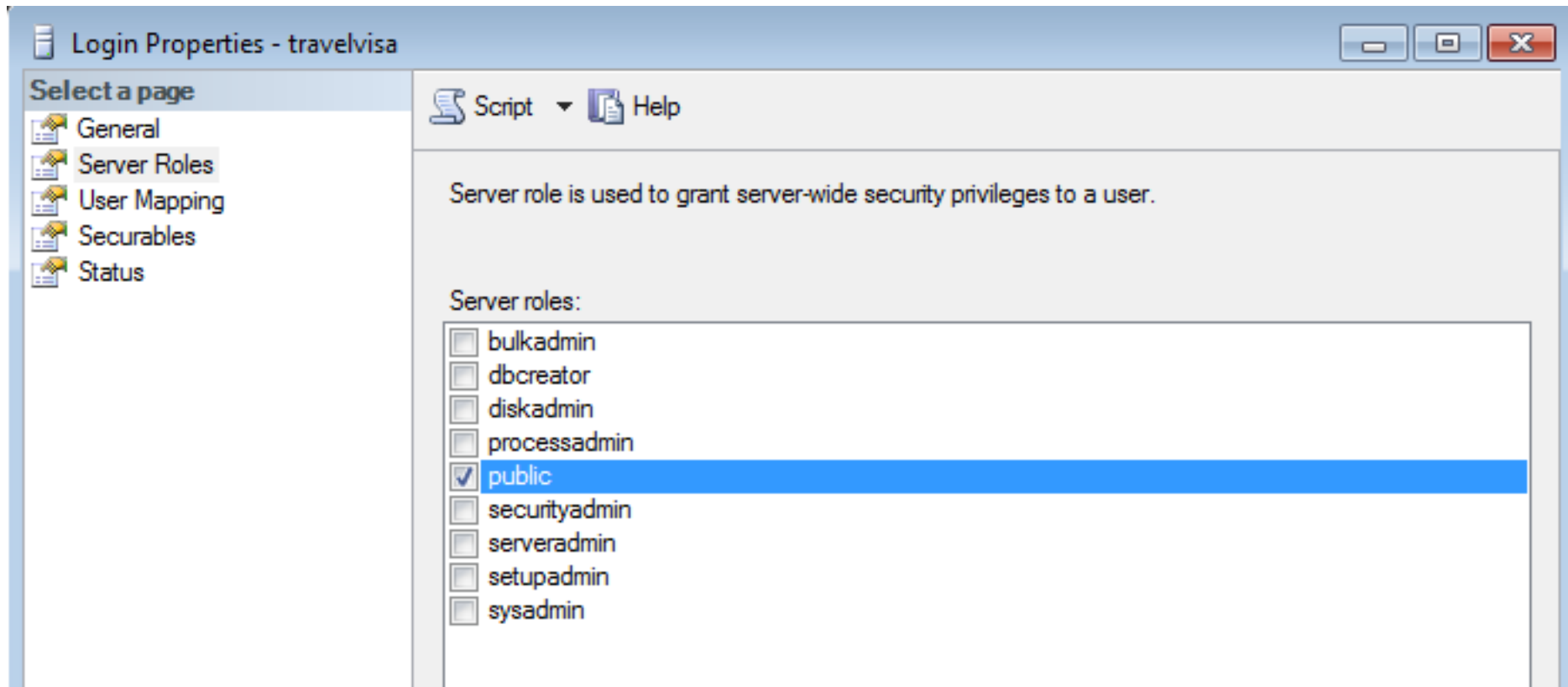
- ❖ Quyền truy nhập đến các đối tượng trong CSDL có thể được thiết lập tùy thuộc vào chính sách quản trị CSDL và ứng dụng.
- ❖ Mỗi tài khoản người dùng được cấp quyền truy nhập thông qua việc gán vào một hoặc một số nhóm vai trò (roles);
 - Một người dùng có thể truy nhập một hoặc một số CSDL;
 - Việc truy nhập vào từng đối tượng trong CSDL có thể được gán riêng.

6.2 Bảo mật các đối tượng trong CSDL

- ❖ Các đối tượng điển hình trong CSDL:
 - Các bảng dữ liệu (tables)
 - Các khung nhìn (views)
 - Các thủ tục, hàm (stored procedures, functions)
 - Các triggers

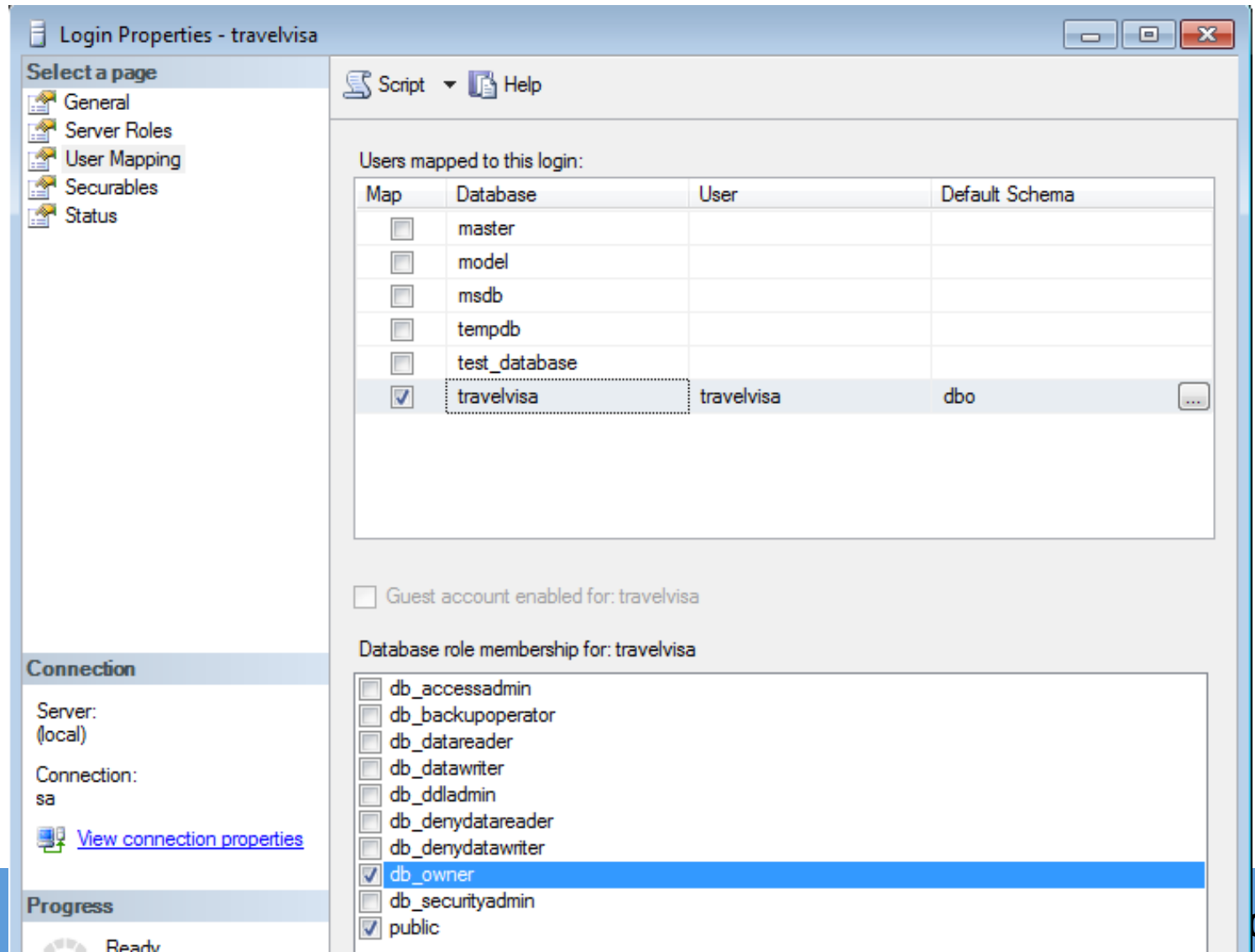
6.2 Bảo mật các đối tượng trong CSDL

- ❖ Gán tài khoản người dùng vào các server roles (MS-SQL)



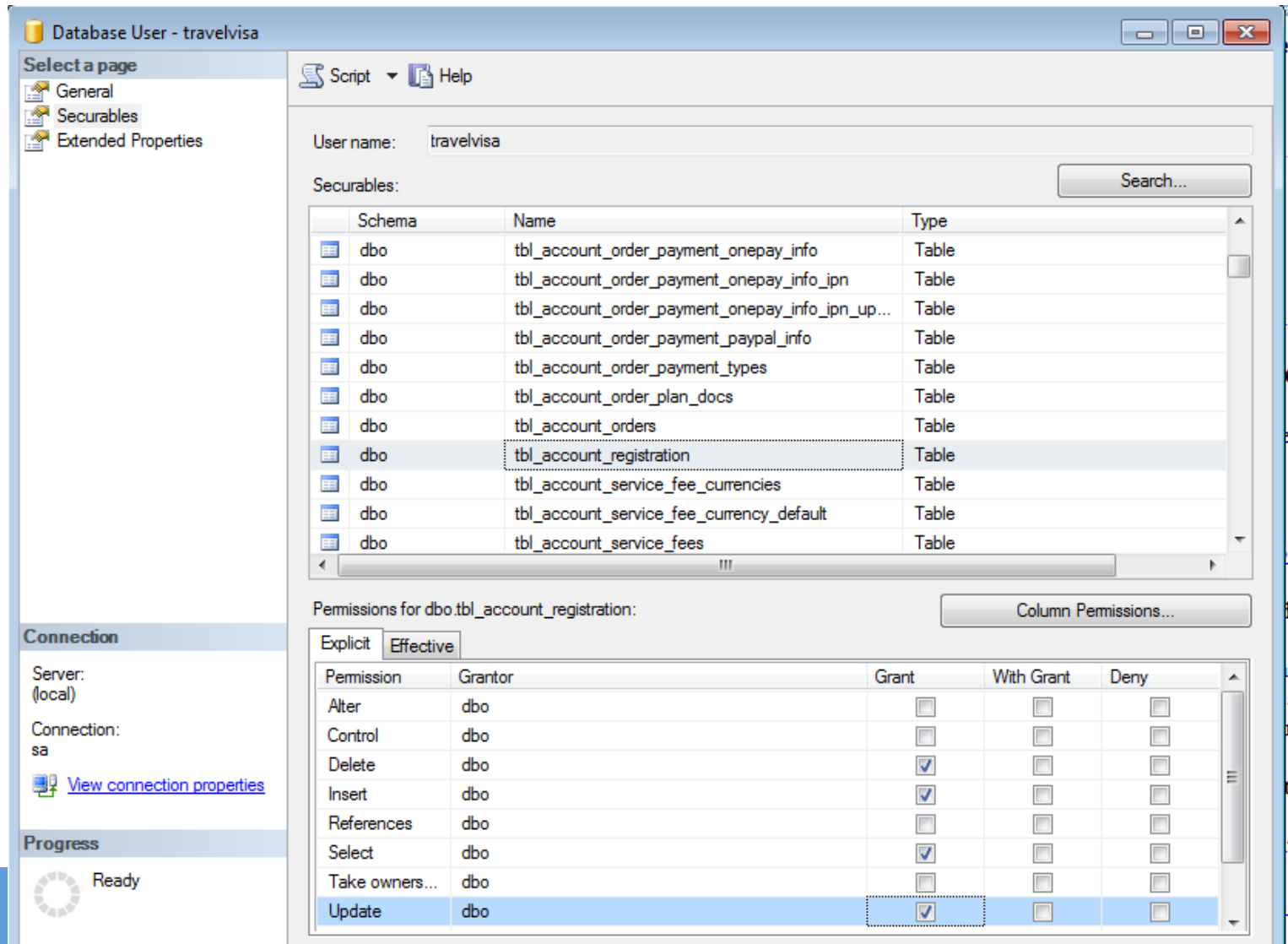
6.2 Bảo mật các đối tượng trong CSDL

- ❖ Gán quyền truy nhập CSDL và vai trò của người dùng trong CSDL



6.2 Bảo mật các đối tượng trong CSDL

- ❖ Cấp quyền truy nhập các đối tượng trong CSDL



6.2 Bảo mật các đối tượng trong CSDL

- ❖ Cấp hoặc hủy quyền truy nhập các đối tượng trong CSDL sử dụng lệnh (MS-SQL):
 - GRANT <quyền truy nhập> ON <đối tượng> TO <người dùng>: cấp quyền truy nhập đến đối tượng cho người dùng.
 - DENY <quyền truy nhập> ON <đối tượng> TO <người dùng>: từ chối truy nhập đến đối tượng cho người dùng.
 - REVOKE <quyền truy nhập> ON <đối tượng> FROM <người dùng>: hủy quyền truy nhập (do GRANT hoặc DENY tạo) đến đối tượng từ người dùng.

6.2 Bảo mật các đối tượng trong CSDL

❖ Quyền truy nhập gồm:

- Execute: với thủ tục, hàm và trigger
- SELECT, INSERT, UPDATE, DELETE và một số quyền khác với bảng, view.

6.3 Sử dụng mã hóa trong CSDL

- ❖ Giới thiệu về mã hóa CSDL
- ❖ Mã hóa dữ liệu trong bảng
- ❖ Mã hóa toàn bộ dữ liệu
- ❖ Mã hóa dữ liệu trên đường truyền
- ❖ Mã hóa dữ liệu sử dụng các thiết bị lưu trữ đặc biệt.

6.3 Sử dụng mã hóa – Giới thiệu

- ❖ Các kỹ thuật mã hóa có thể được sử dụng để bảo vệ dữ liệu lưu trong CSDL cũng như để bảo vệ cả CSDL.
- ❖ Hai phương pháp phổ biến được sử dụng:
 - Mã hóa (Encryption);
 - Băm.

6.3 Sử dụng mã hóa – Giới thiệu

❖ Hai phương pháp phổ biến được sử dụng:

■ Mã hóa (Encryption):

- Sử dụng các giải thuật mã hóa với khóa (key) để bảo vệ dữ liệu. Thông thường các giải thuật mã hóa khóa đối xứng được sử dụng.
- Các giải thuật mã hóa thông dụng: DES, 3DES, AES, RC2, RC4,...

■ Băm (Hashing):

- Sử dụng các giải thuật băm để chuyển đổi dữ liệu có độ dài bất kỳ thành chuỗi có độ dài cố định.
- Với hàm băm 1 chiều thì không giải mã được.
- Các giải thuật băm thông dụng: MD4, MD5, MD6, SHA1, SHA2, SHA3,...
- Thường được dùng để mã hóa mật khẩu.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu trong bảng

- ❖ Dữ liệu trong bảng có thể được mã hóa theo 2 hướng:
 - Sử dụng các hàm mã hóa/giải mã trong CSDL để mã hóa/giải mã khi thực hiện các thao tác ghi/đọc.
 - Các hệ quản trị CSDL cũ thường không hỗ trợ các hàm mã hóa/giải mã
 - Các hệ quản trị CSDL mới hỗ trợ các hàm mã hóa/giải mã ở mức hạn chế.
 - Mã hóa / giải mã dữ liệu tại lớp ứng dụng
 - Thư viện API của ứng dụng hỗ trợ các hàm mã hóa/giải mã mạnh.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu trong bảng

- ❖ Khi dữ liệu trong bảng được mã hóa sẽ gây khó khăn cho việc lập chỉ số và tìm kiếm.
 - Cần cân nhắc các dữ liệu cần mã hóa và chọn phương pháp mã hóa phù hợp;
 - Với các trường dữ liệu cần lập chỉ số và tìm kiếm (thường xuyên, đặc biệt là các trường khóa), không nên thực hiện mã hóa.
- ❖ Mã hóa sẽ làm tăng tải máy chủ CSDL hoặc máy chủ ứng dụng.
 - Cần lựa chọn phương pháp mã hóa và phần dữ liệu cần mã hóa cho phù hợp.

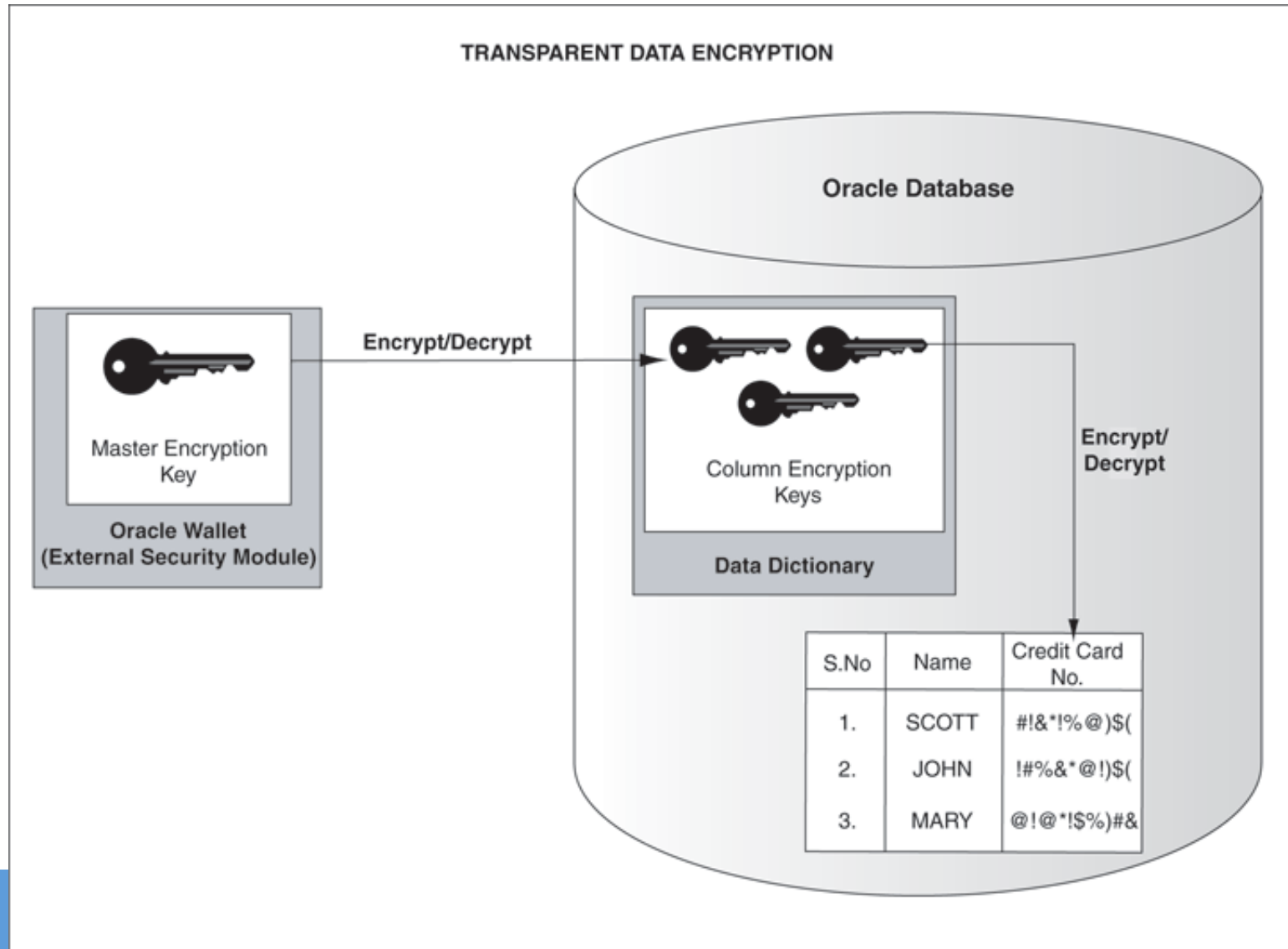
6.3 Sử dụng mã hóa – Mã hóa dữ liệu toàn bộ

- ❖ Dữ liệu trong các bảng và cả dữ liệu quản lý các bảng có thể được mã hóa nhờ các công nghệ đặc biệt thực hiện trực tiếp trên máy chủ CSDL;
 - Dữ liệu được mã hóa khi nó được ghi vào CSDL;
 - Dữ liệu được giải mã sau khi được đọc từ CSDL và nạp vào bộ nhớ.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu toàn bộ

- ❖ Công nghệ Transparent Data Encryption (TDE) cho phép mã hóa từng khối dữ liệu khi nó được ghi vào CSDL và giải mã khi khối được đọc ra từ CSDL;
- ❖ Công nghệ TDE được hỗ trợ bởi nhiều hệ quản trị CSDL:
 - MS-SQL
 - Oracle
 - IBM DB2.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu toàn bộ - TDE



6.3 Sử dụng mã hóa – Mã hóa dữ liệu toàn bộ - TDE

❖ Ưu điểm:

- Hoàn toàn trong suốt với người dùng.

❖ Nhược điểm:

- Tăng tải máy chủ CSDL;
- Nếu người dùng hoặc tin tặc có thể truy cập CSDL, thì hẳn ta có thể trích xuất dữ liệu từ CSDL theo cách thông thường → không bảo vệ được dữ liệu khỏi bị đánh cắp.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu truyền

- ❖ Dữ liệu trao đổi giữa máy khách và máy chủ CSDL có thể được bảo vệ sử dụng các kỹ thuật dựa trên mã hóa:
 - Sử dụng SSL/TLS:
 - Cần có chứng chỉ số khóa công khai cho máy chủ
 - Sử dụng hệ khóa công khai để trao đổi khóa phiên
 - Sử dụng khóa phiên để mã hóa dữ liệu
 - Sử dụng hàm băm có khóa (MAC/HMAC) để đảm bảo tính toàn vẹn dữ liệu
 - Xác thực thực thể
 - Đảm bảo tính bí mật, toàn vẹn và xác thực thông tin truyền.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu truyền

- ❖ Dữ liệu trao đổi giữa máy khách và máy chủ CSDL có thể được bảo vệ sử dụng các kỹ thuật dựa trên mã hóa:
 - Sử dụng IPSec
 - Tạo đường hầm/kênh giao tiếp an toàn giữa máy chủ và máy khách
 - Hai chế độ làm việc: Transport / Tunnel
 - Hai phương thức mã hóa: AH và ESP.
 - Nhược điểm:
 - Giảm hiệu năng hệ thống do các giao thức mã tiêu tốn nhiều tài nguyên tính toán và lượng dữ liệu truyền tăng đáng kể;
 - Chỉ nên áp dụng khi máy khách và máy chủ CSDL không ở cùng mạng LAN.

6.3 Sử dụng mã hóa – Mã hóa dữ liệu sử dụng TB đặc biệt

- ❖ Các thiết bị lưu trữ đặc biệt, có hỗ trợ mã hóa dữ liệu có thể được sử dụng để lưu trữ CSDL.
- ❖ Các thiết bị lưu trữ (thường là HDD và RAID) hỗ trợ sẵn khả năng mã hóa/giải mã, nên toàn bộ CSDL được bảo vệ bằng mã hóa.
- ❖ Nhược điểm:
 - Nếu người dùng hoặc tin tặc có thể truy cập CSDL, thì hẳn ta có thể trích xuất dữ liệu từ CSDL theo cách thông thường → không bảo vệ được dữ liệu khỏi bị đánh cắp.

6.4 Một số biện pháp bảo mật CSDL và ứng dụng khác

❖ Bảo vệ chuỗi kết nối CSDL (connection string):

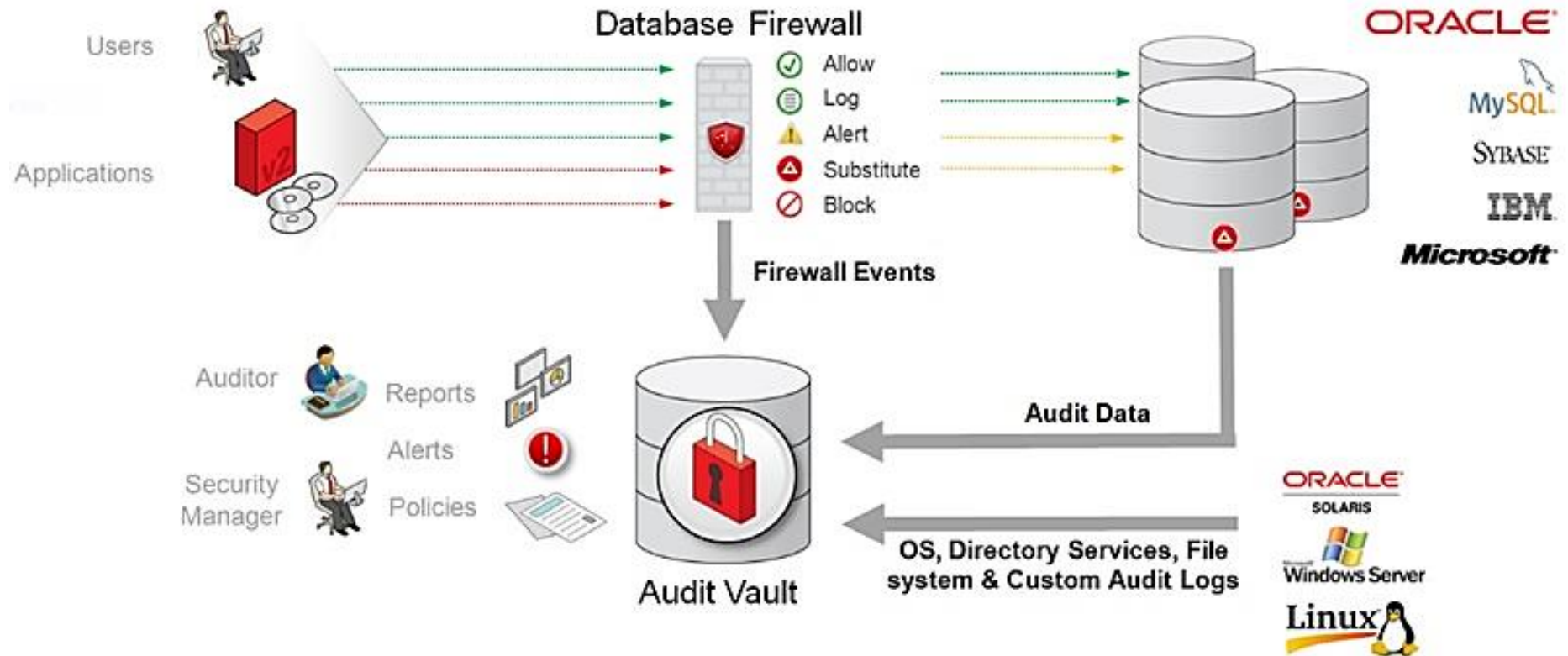
- Hầu hết các chuỗi kết nối được lưu trong các file ở dạng text → Có nguy cơ bị tin tặc lạm dụng.
- `ConnectionString= "Driver={SQL Server}; Network=DBMSSOCN; Server=192.168.0.10; Address=192.168.0.10; WSID=192.168.0.100; Database=CustomersDB; UID=test_user; PWD=Abc123456;"`
- Cần mã hóa các chuỗi kết nối CSDL để đảm bảo an toàn.

6.4 Một số biện pháp bảo mật CSDL và ứng dụng khác

❖ Tường lửa CSDL:

- Giám sát, phân tích các câu lệnh gửi đến CSDL
- Nếu phát hiện câu lệnh độc hại → ngăn chặn
- Phát hiện dựa trên tập các luật/chính sách đã định trước.
- Nhược điểm:
 - Làm giảm hiệu năng, do việc phân tích cú pháp các câu lệnh SQL và chạy các tập luật giám sát tiêu tốn nhiều tài nguyên tính toán.

6.4 Một số biện pháp bảo mật CSDL và ứng dụng khác



6.4 Một số biện pháp bảo mật CSDL và ứng dụng khác


- ❖ Sử dụng mật khẩu một lần (OTP – One Time Password) để xác thực các giao dịch ở mức ứng dụng:
 - Mật khẩu được sinh ra và chỉ được dùng 1 lần cho 1 phiên làm việc hoặc 1 giao dịch;
 - Mật khẩu thường được sinh ngẫu nhiên
 - Chuyển giao mật khẩu:
 - In ra giấy một danh sách mật khẩu để dùng dần
 - Gửi qua các phương tiện khác như SMS
 - Sử dụng các thiết bị chuyên dụng, như các e-token,...
 - Ưu điểm: an toàn hơn, tránh được tấn công kiểu replay (lấy được mật khẩu dùng lại).
 - Nhược điểm: người sử dụng khó nhớ mật khẩu.

6.4 Một số biện pháp bảo mật CSDL và ứng dụng khác

- ❖ Sử dụng các phương pháp xác thực form, trang web như CAPTCHA

Prove you're not a robot

☐ Skip this verification (phone verification may be required)



Type the text:

⌂ 🔊 ?

Đăng nhập hệ thống

Tên truy cập

Mật khẩu

D6AB1D

Nhập số trên

Đăng nhập

[Quên mật khẩu](#) | [Câu hỏi thường gặp](#)

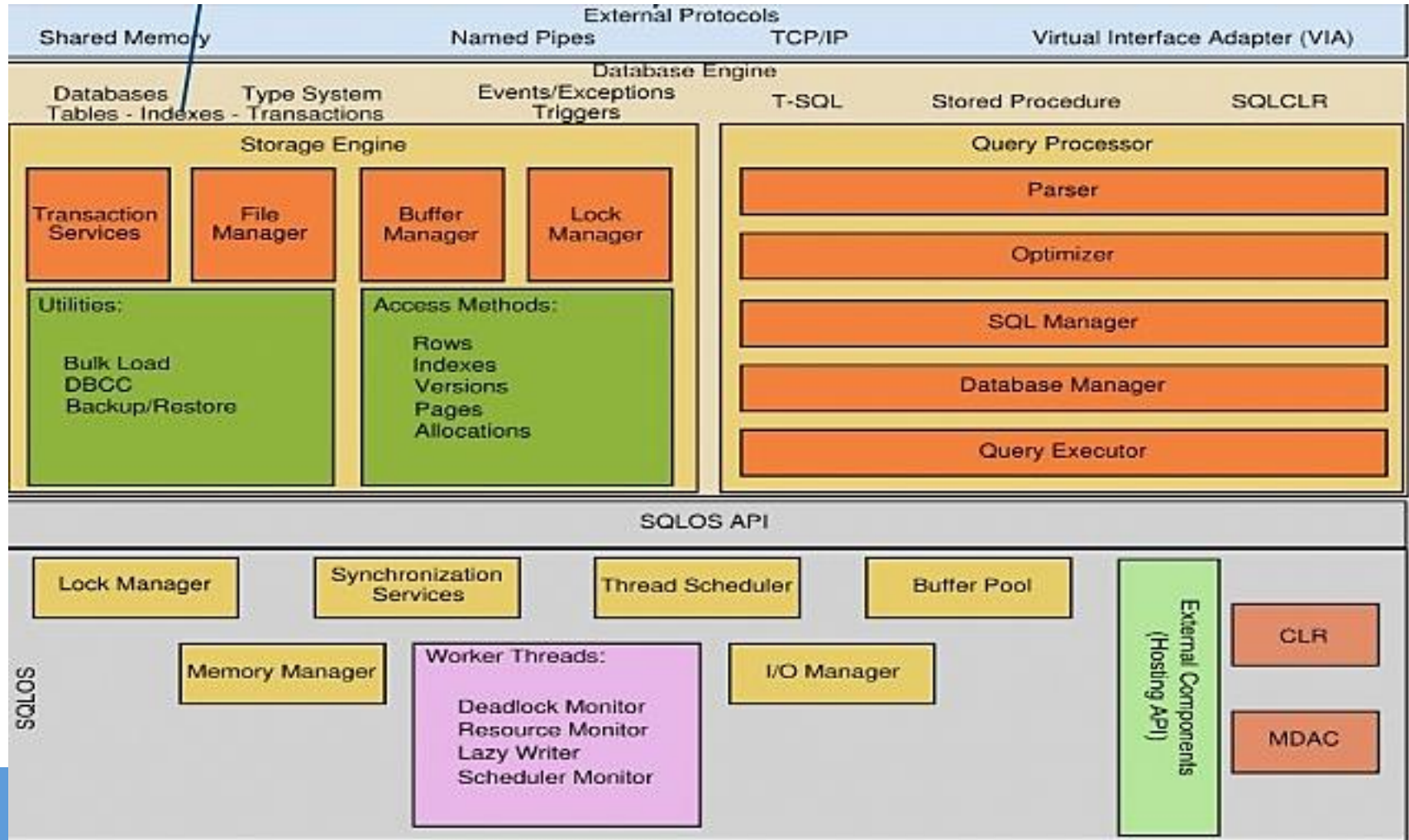
Hướng dẫn giao dịch an toàn

6.5 Mô hình bảo mật ở một số DBMS

- ❖ Bảo mật MS-SQL
- ❖ Bảo mật Oracle
- ❖ Bảo mật MySQL
- ❖ Một số mô hình quản lý tài khoản truy nhập trên các DBMS

6.5.1 Bảo mật MS-SQL

❖ Kiến trúc MS SQL Server



6.5.1 Bảo mật MS-SQL

❖ Các thành phần của MS SQL Server

- Databases: các CSDL
- Database files and file groups: các file CSDL và nhóm file
- Transaction logs: Logs giao dịch CSDL
- Backup and Recovery: Sao lưu và khôi phục
- Microsoft Cluster Server: Máy chủ liên kết chuỗi
- Protocols: Các giao thức
- Disaster recovery: Mô hình khôi phục sau thảm họa

6.5.1 Bảo mật MS-SQL

❖ Databases: các CSDL:

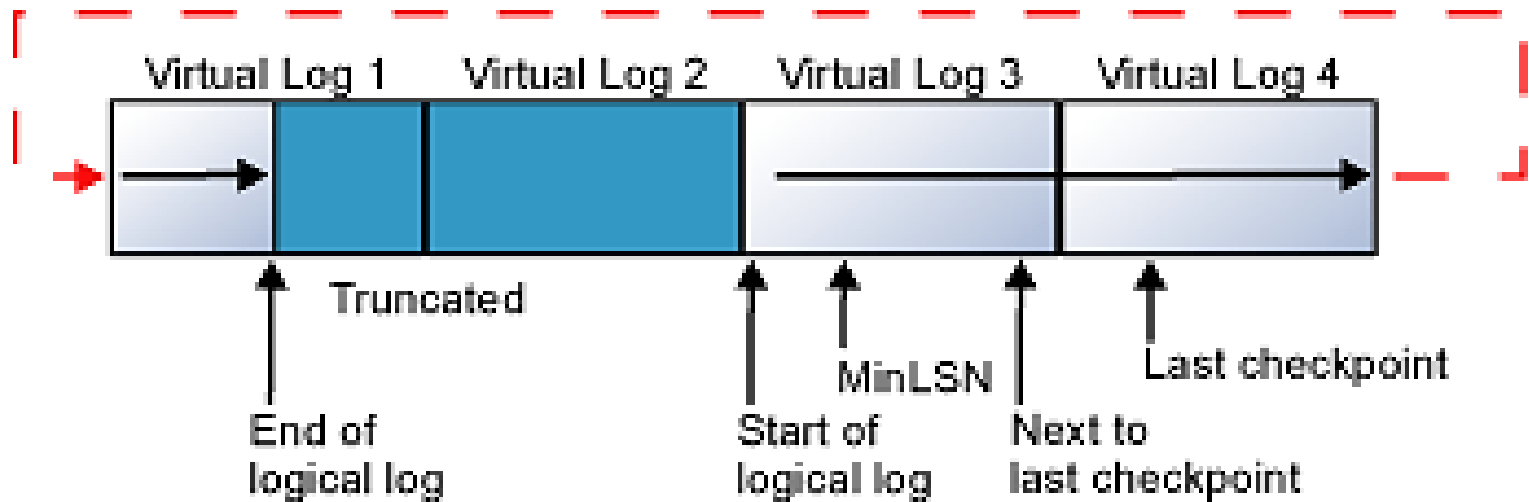
- CSDL hệ thống
 - Master: Chứa các dữ liệu hệ thống, bao gồm tài khoản truy nhập
 - MSDB: Chứa các siêu dữ liệu quản lý (Meta data)
 - Model: CSDL mẫu để tạo các CSDL khác
 - TempDB: Lưu trữ các đối tượng trung gian trong quá trình hoạt động.
- CSDL người dùng tạo: Người dùng tự tạo

6.5.1 Bảo mật MS-SQL

- ❖ Database files and file groups: các file CSDL và nhóm file:
 - Các file nhị phân
 - Các file dữ liệu (*.mdf, *.ndf)
 - Các file logs giao dịch (*.ldf)
 - Các file sao lưu
 - Các nhóm file (file dữ liệu và file log giao dịch)

6.5.1 Bảo mật MS-SQL

❖ Transaction logs: Logs giao dịch CSDL



6.5.1 Bảo mật MS-SQL

❖ Các mô hình phục hồi của SQL server:

- Simple (đơn giản)
- Full (đầy đủ)
- Bulk logs (Logs theo lô)

6.5.1 Bảo mật MS-SQL

❖ Các mô hình phục hồi của SQL server:

- Simple (đơn giản)
 - Không yêu cầu có sao lưu logs giao dịch
 - Các thay đổi từ lần sao lưu gần nhất sẽ không được bảo vệ
 - Chỉ có thể khôi phục từ bản sao lưu gần nhất.

6.5.1 Bảo mật MS-SQL

❖ Các mô hình phục hồi của SQL server:

- Full (đầy đủ)
 - Yêu cầu phải có sao lưu logs giao dịch
 - Có khả năng khôi phục đầy đủ (không mất dữ liệu)
 - Khả năng khôi phục từ một thời điểm cụ thể.

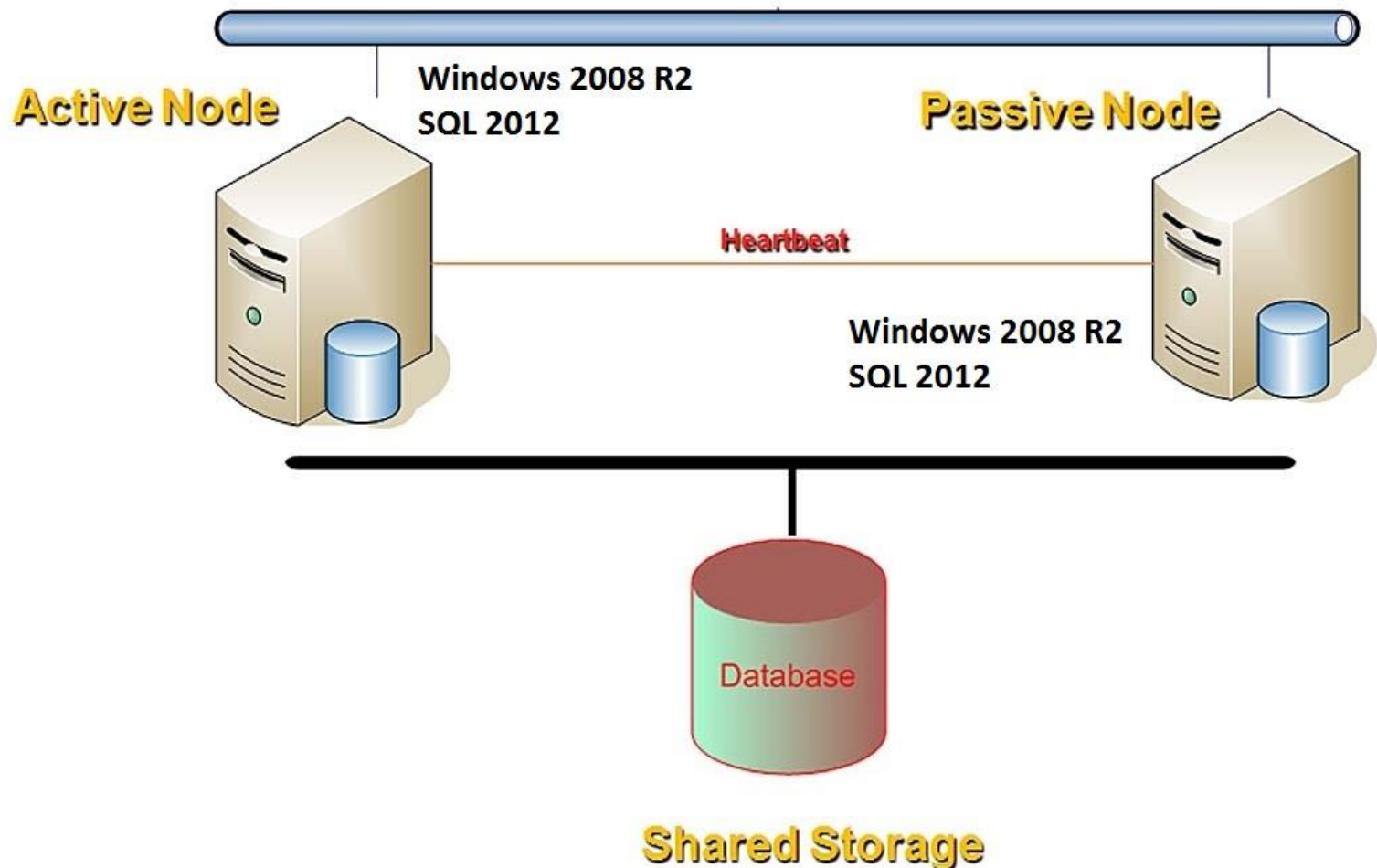
6.5.1 Bảo mật MS-SQL

❖ Các mô hình phục hồi của SQL server:

- Bulk logs (Logs theo lô)
 - Yêu cầu phải có sao lưu logs giao dịch
 - Có khả năng khôi phục đầy đủ (không mất dữ liệu)
 - Nếu log giao dịch bị hư hỏng, hoặc các thao tác tạo logs theo lô xuất hiện kể từ lần sao lưu gần đây nhất → các thay đổi từ lần sao lưu gần nhất có thể bị mất.
 - Không có khả năng khôi phục từ một thời điểm cụ thể.

6.5.1 Bảo mật MS-SQL

❖ Microsoft Cluster Server: Máy chủ liên kết chuỗi



6.5.1 Bảo mật MS-SQL

❖ Relational Engine (Mô tơ CSDL quan hệ)

- Bộ xử lý truy vấn (Query Processor)
- Gồm các thành phần cho phép dịch và thực hiện các câu truy vấn:
 - Yêu cầu dữ liệu từ Mô tơ lưu trữ
 - Xử lý dữ liệu
 - Trả về kết quả.
- Một số thành phần cụ thể:
 - Query processing
 - Memory management
 - Thread and task management
 - Buffer management
 - Distributed query processing.

6.5.1 Bảo mật MS-SQL

❖ Storage Engine (Mô tơ lưu CSDL)

- Lưu trữ dữ liệu
- Đọc và chuyển dữ liệu cho các thành phần khác theo yêu cầu.

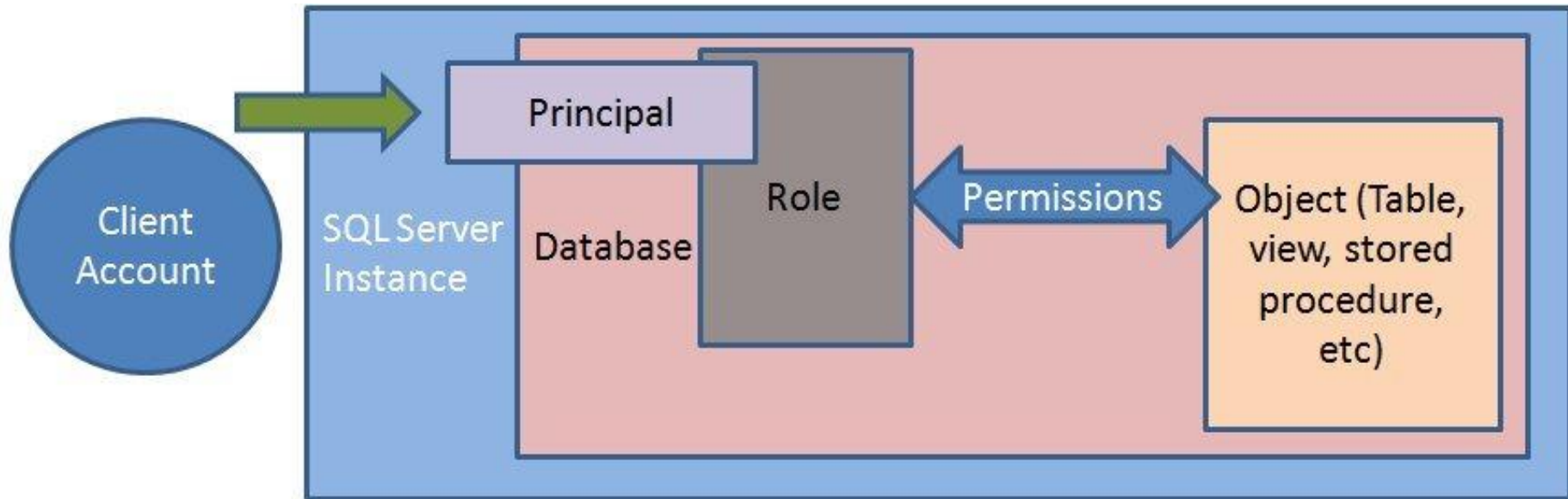
6.5.1 Bảo mật MS-SQL

❖ SQL OS (Mô đun giao tiếp với hệ điều hành của SQL)

- Memory management
- Buffer pool
- Log buffer
- Phát hiện và xử lý Deadlock
- Một số dịch vụ khác:
 - Xử lý ngoại lệ
 - Các mô đun ngoài, như Common Language Runtime (CLR)

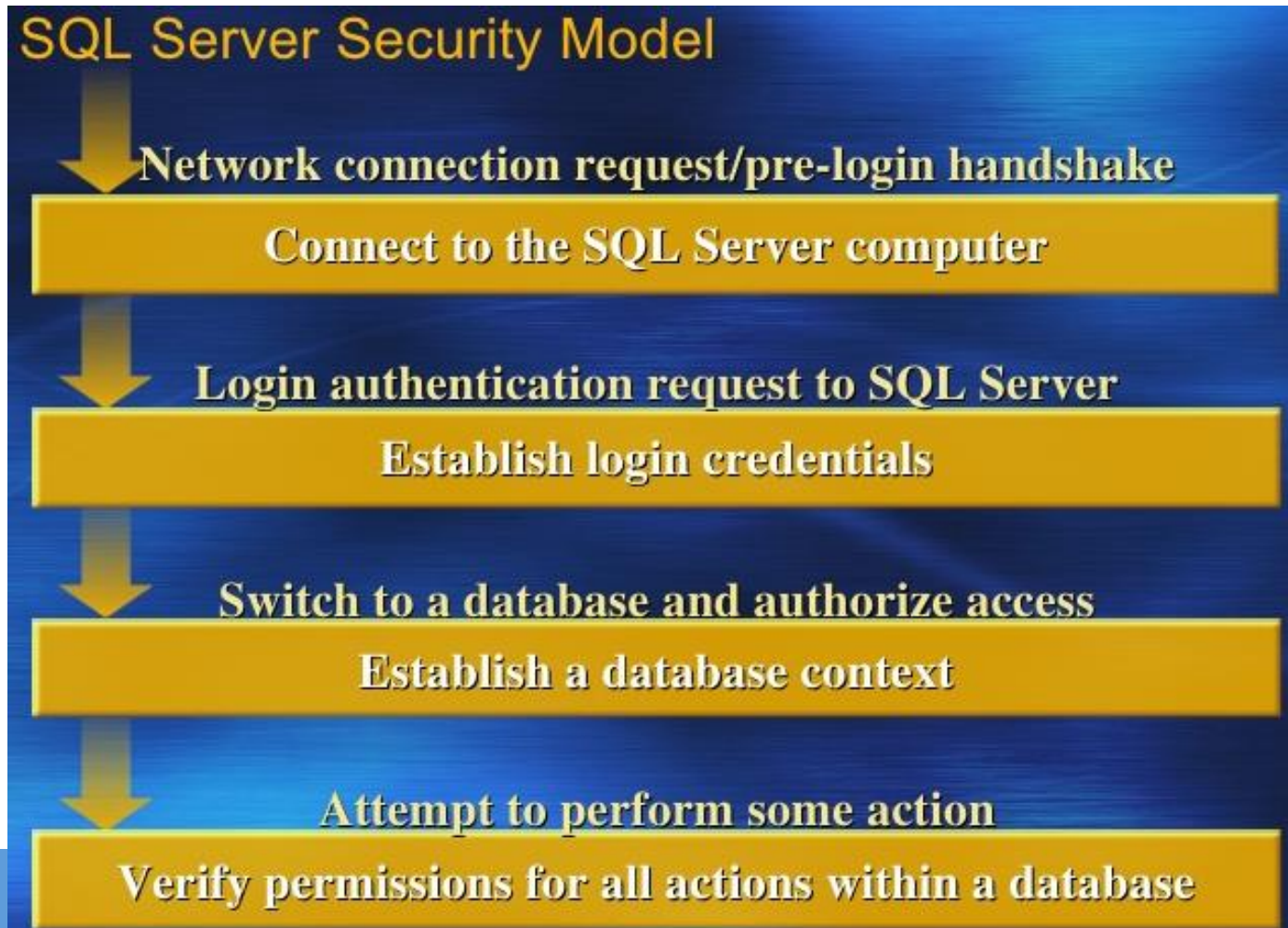
6.5.1 Bảo mật MS-SQL

❖ Mô hình an ninh của SQL Server



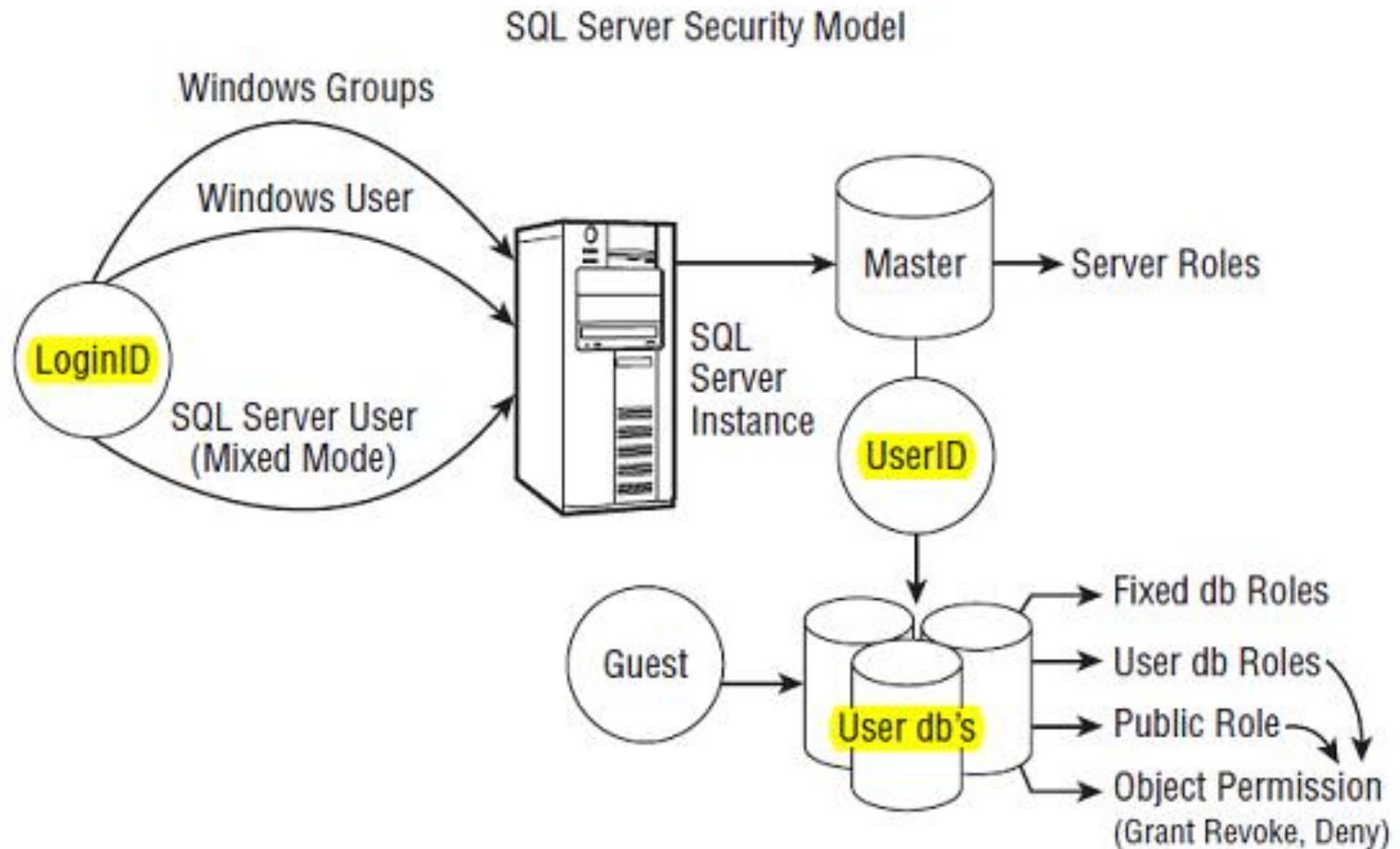
6.5.1 Bảo mật MS-SQL

❖ Mô hình an ninh của SQL Server



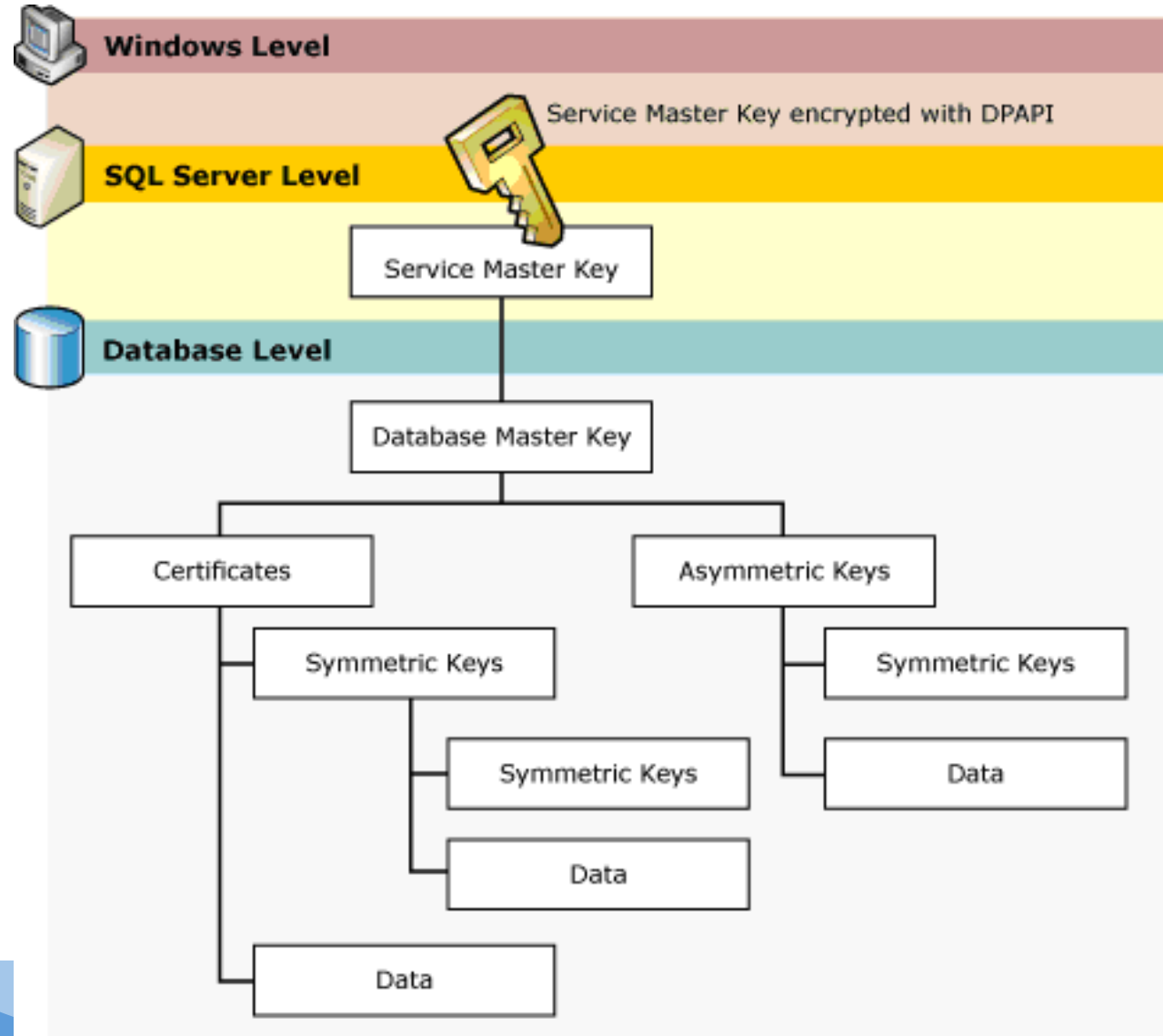
6.5.1 Bảo mật MS-SQL

❖ Mô hình an ninh của SQL Server



6.5.1 Bảo mật MS-SQL

- ❖ Các mức quản lý khóa của SQL Server

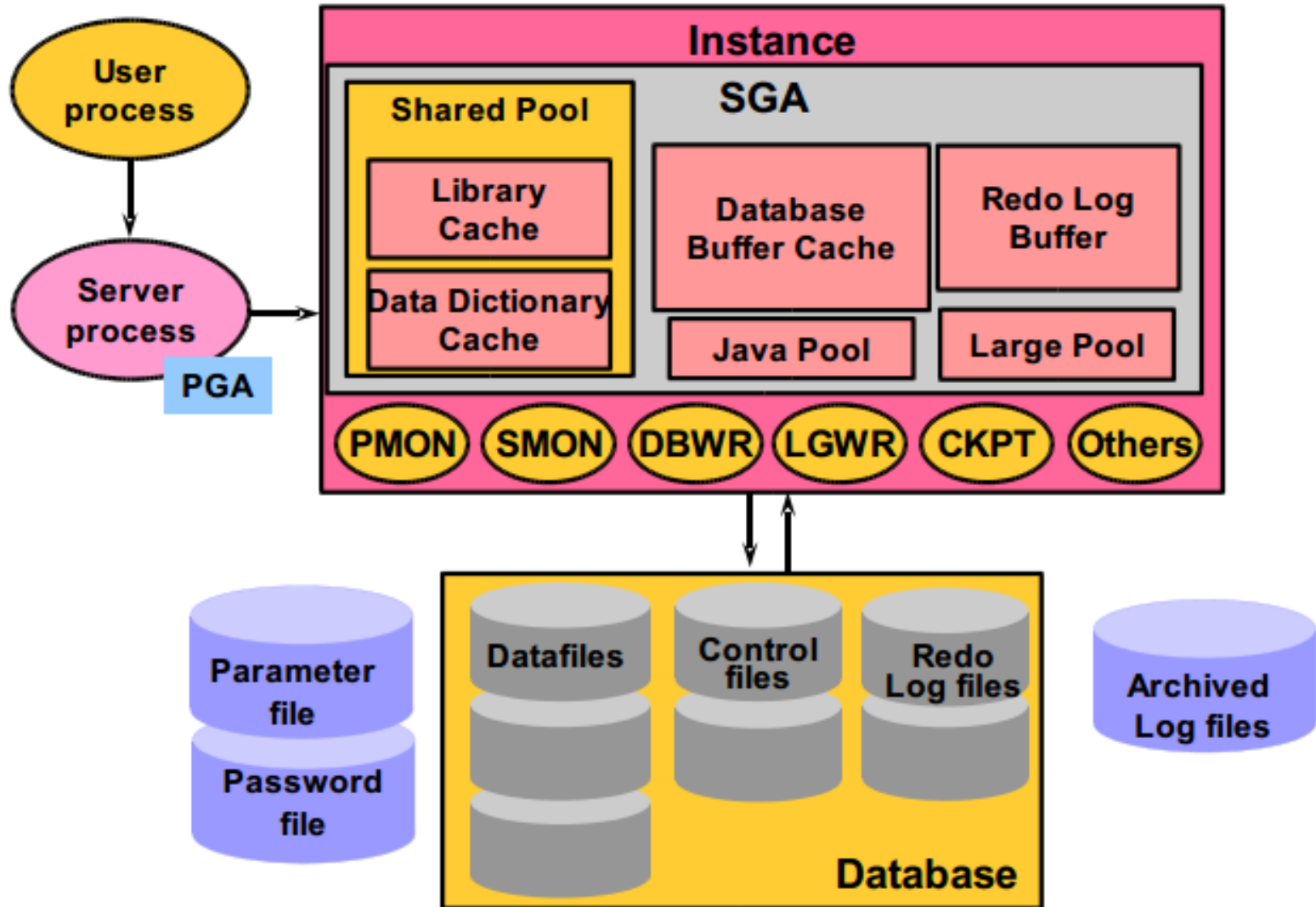


6.5.2 Bảo mật Oracle

- ❖ Kiến trúc hệ quản trị CSDL Oracle
- ❖ Các thành phần của Oracle
- ❖ Các vấn đề và các biện pháp bảo mật của Oracle

6.5.2 Bảo mật Oracle

❖ Kiến trúc Oracle



6.5.2 Bảo mật Oracle

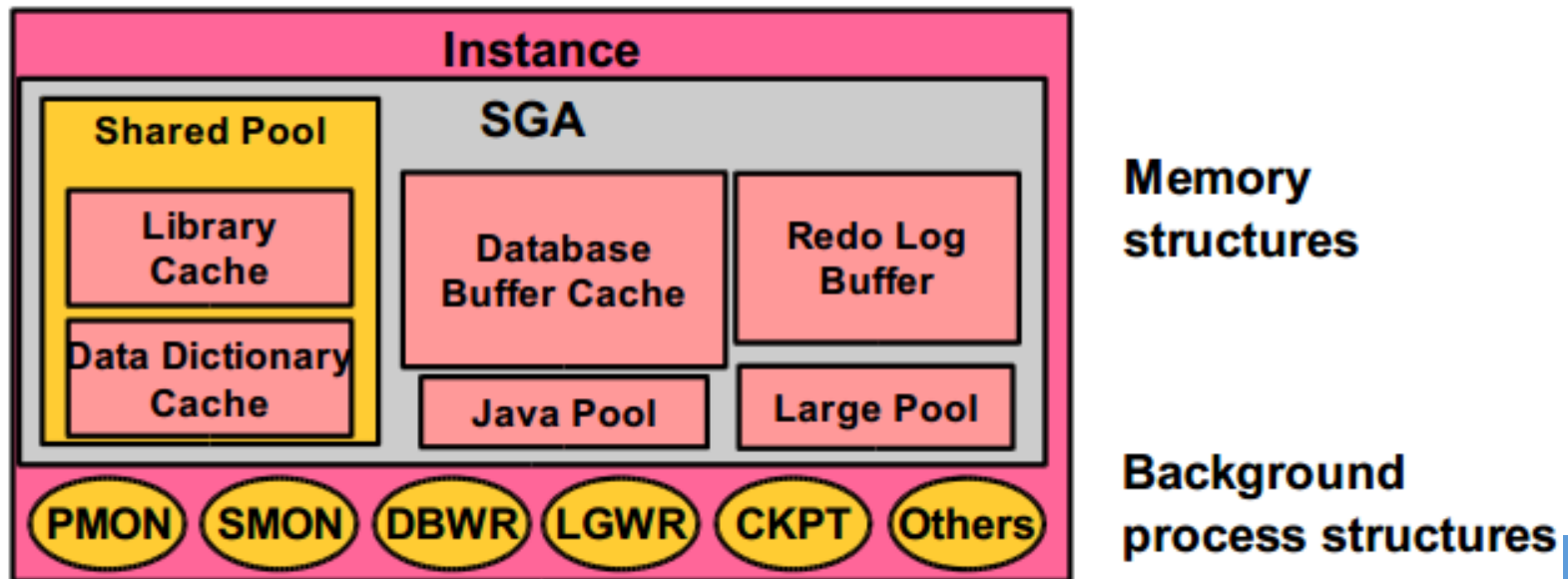
❖ Máy chủ Oracle (Oracle Server):

- Là một hệ quản trị CSDL (DBMS), với cách tiếp cận mở, toàn diện và tích hợp trong quản lý thông tin;
- Gồm 2 thành phần:
 - Một tiến trình Oracle (Oracle Instance)
 - CSDL Oracle (Oracle Database)

6.5.2 Bảo mật Oracle

❖ Một tiến trình Oracle (Oracle Instance):

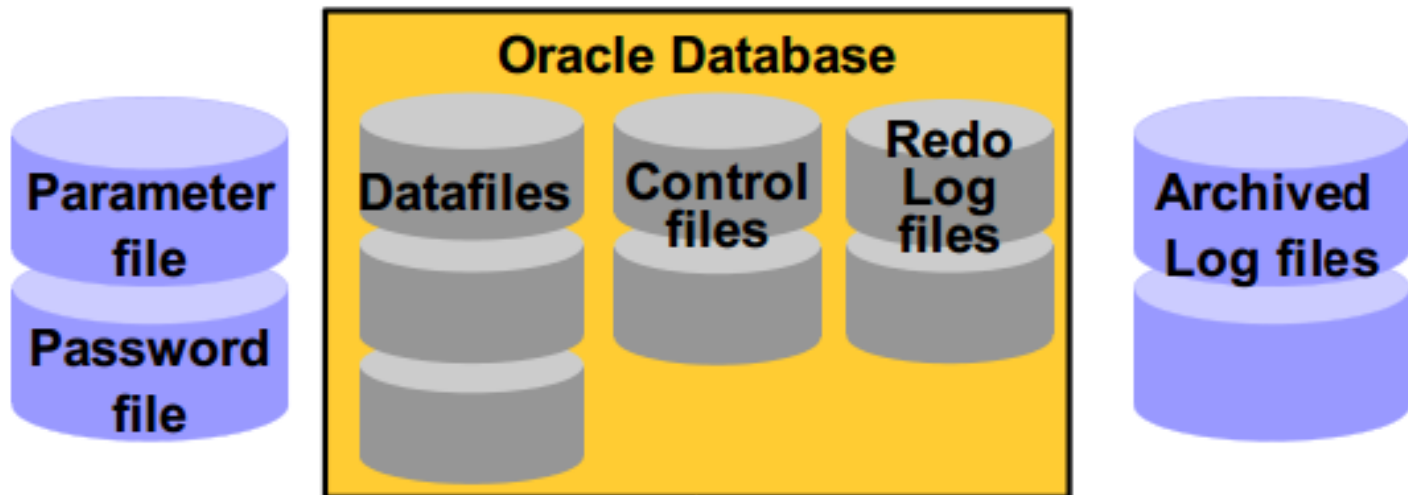
- Là phương tiện để truy nhập CSDL Oracle
- Thường xuyên mở một và chỉ một CSDL
- Bao gồm:
 - Các cấu trúc bộ nhớ (memory structures)
 - Các cấu trúc tiến trình ngầm (background process structures)



6.5.2 Bảo mật Oracle

❖ CSDL Oracle:

- Là một tập các dữ liệu mà được xử lý như các đơn vị
- Gồm 3 loại files: File dữ liệu, file điều khiển và file log redo.



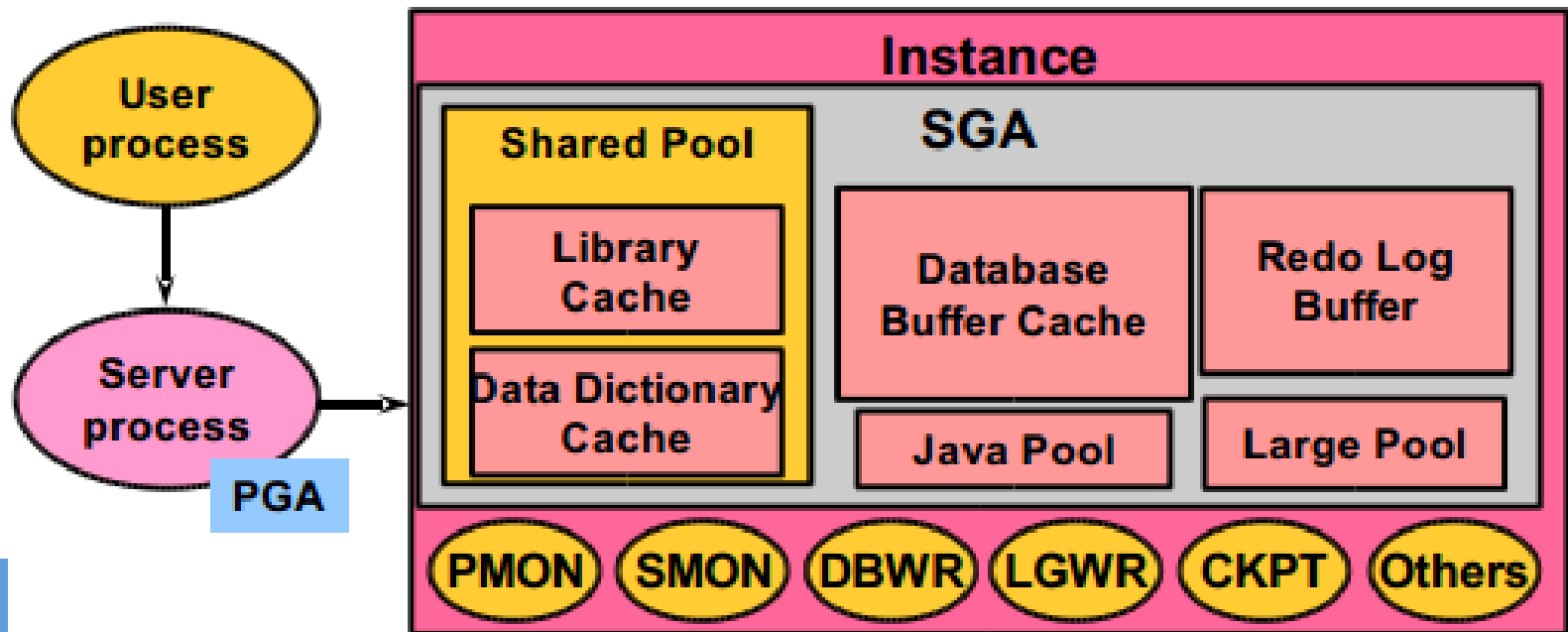
6.5.2 Bảo mật Oracle

- ❖ Các cấu trúc bộ nhớ: gồm 2 vùng bộ nhớ:
 - SGA (System Global Area):
 - Được cấp phát khi tiến trình (instance) được kích hoạt
 - Là một thành phần cơ bản của tiến trình Oracle
 - PGA (Program Global Area):
 - Được cấp phát khi máy chủ được kích hoạt.

6.5.2 Bảo mật Oracle

❖ SGA (System Global Area): Gồm một số thành phần:

- Shared Pool
- Database Buffer Cache
- Redo Log Buffer
- Một số cấu trúc bộ nhớ khác.



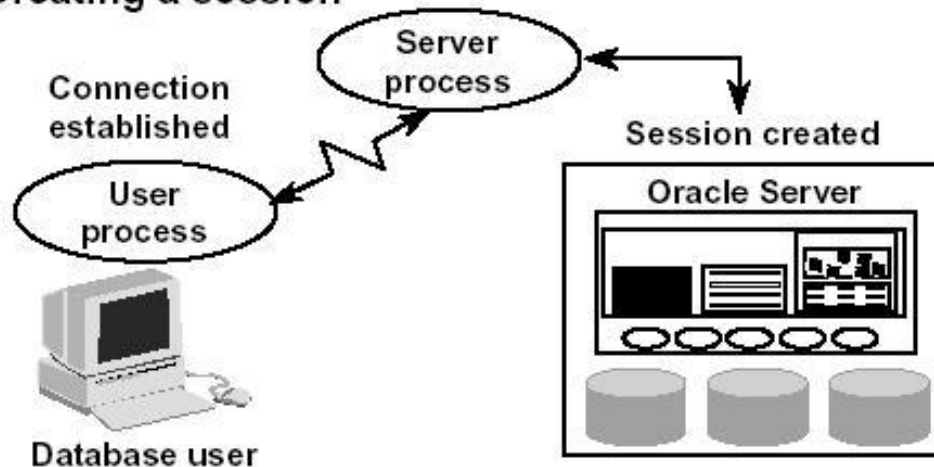
6.5.2 Bảo mật Oracle

❖ Các tiến trình oracle:

- Tiến trình người dùng (User process): được kích hoạt khi người dùng CSDL tạo kết nối đến máy chủ oracle;
- Tiến trình máy chủ (Server process): được kích hoạt và kết nối đến Oracle Instance khi người dùng thiết lập 1 phiên làm việc;
- Các tiến trình ngầm (Background processes): được kích hoạt khi Oracle Instance được kích hoạt.

Connecting to an Oracle Instance:

- Establishing a user connection
- Creating a session



6.5.2 Bảo mật Oracle

❖ Các tiến trình ngầm (Background processes):



- Database Writer (DBWn)
- Log Writer (LGWR)
- System Monitor (SMON)
- Process Monitor (PMON)
- Checkpoint (CKPT)
- Archiver (ARCn)

6.5.2 Bảo mật Oracle

❖ Các vấn đề bảo mật CSDL Oracle:

- Quản lý tài khoản
- Xác thực
- Quyền truy nhập và vai trò
- An toàn ứng dụng
- Truy nhập thông tin phiên người dùng sử dụng ngữ cảnh ứng dụng

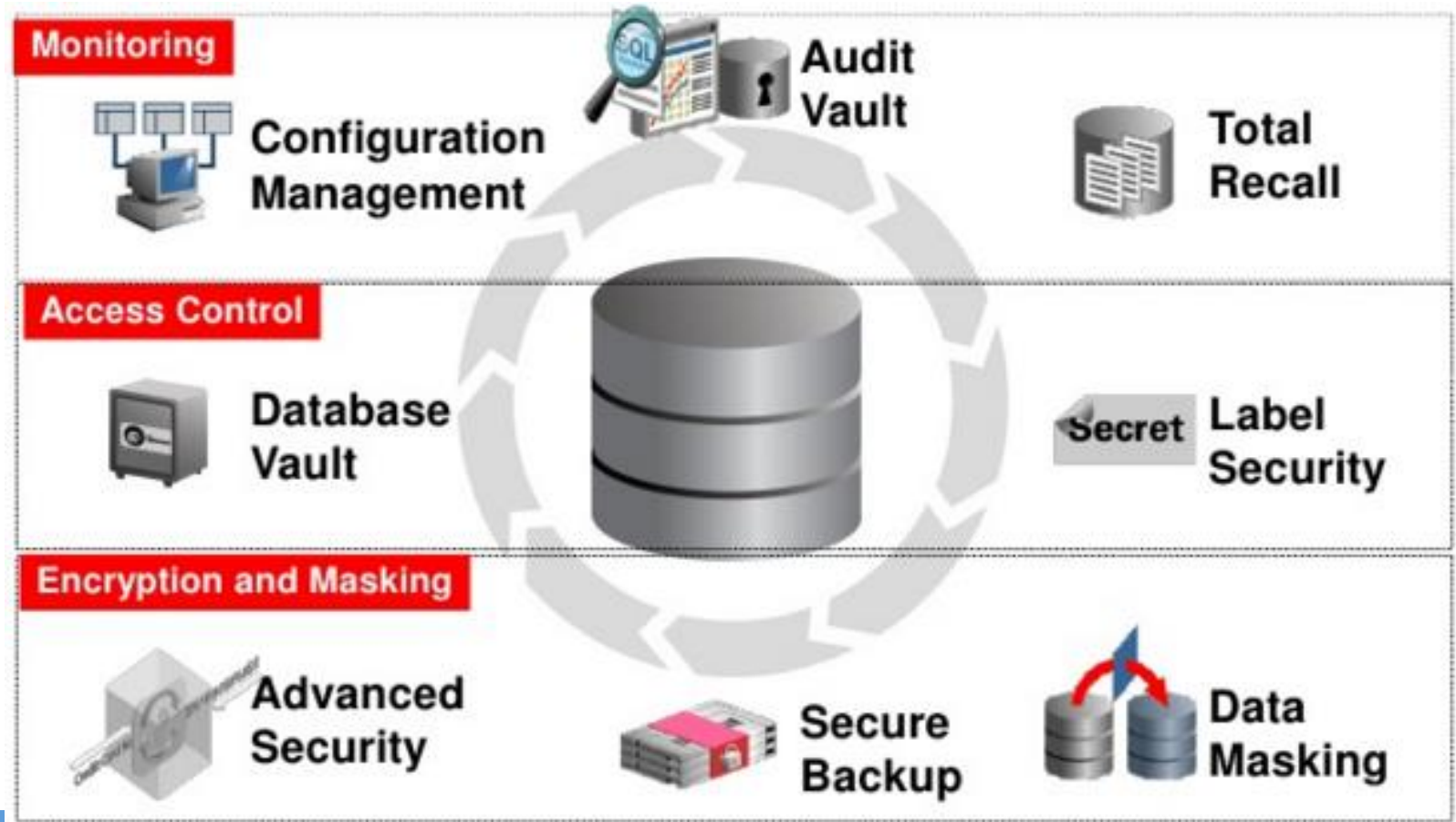
6.5.2 Bảo mật Oracle

❖ Các vấn đề bảo mật CSDL Oracle:

- Truy nhập CSDL theo mức dòng và cột sử dụng CSDL riêng ảo
 - Cho phép tạo các chính sách điều khiển truy cập ở mức dòng và cột dữ liệu;
 - Tự động thêm mệnh đề WHERE vào câu lệnh theo chính sách an toàn của CSDL riêng ảo;
 - Áp dụng trực tiếp lên các đối tượng của CSDL nên các biện pháp an ninh không thể bị bỏ qua.

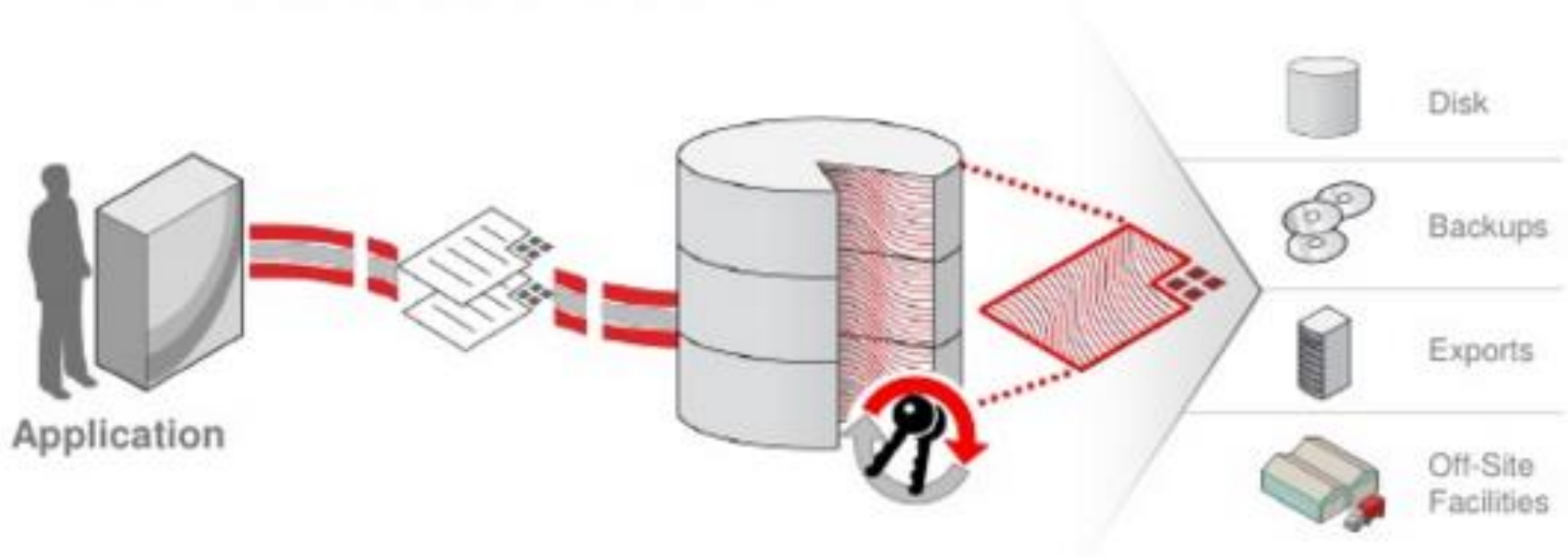
6.5.2 Bảo mật Oracle

❖ Các biện pháp bảo mật CSDL Oracle:



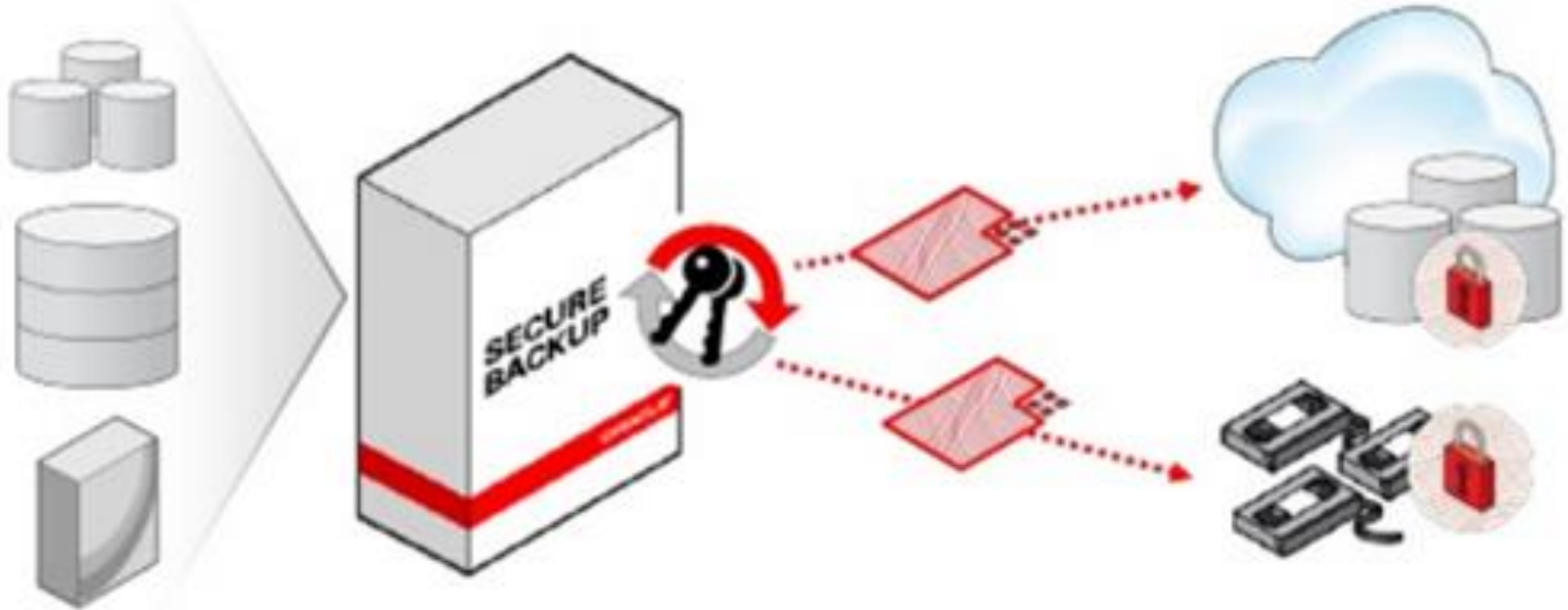
6.5.2 Bảo mật Oracle

- ❖ Oracle Advanced Security: Transparent Data Encryption
 - Dữ liệu được mã hóa ở mức CSDL, hoàn toàn trong suốt với người dùng



6.5.2 Bảo mật Oracle

- ❖ Oracle Secure Backup: Dữ liệu sao lưu được mã hóa và lưu ra băng từ hoặc lên các đám mây.



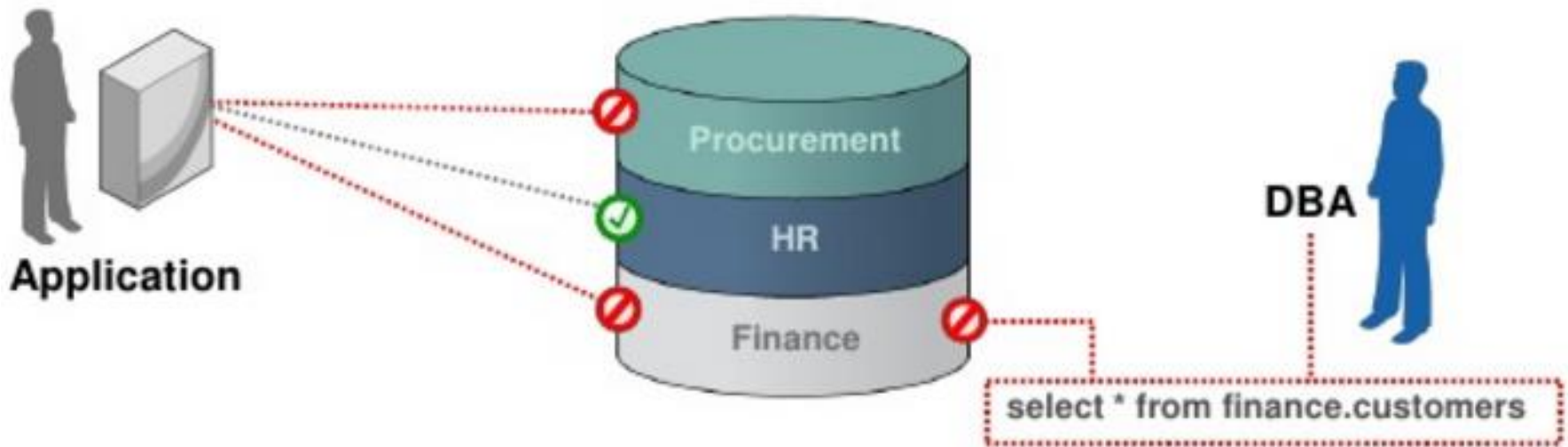
6.5.2 Bảo mật Oracle

- ❖ Oracle Data Masking: Các dữ liệu nhạy cảm được che (mask) trong môi trường phát triển.



6.5.2 Bảo mật Oracle

- ❖ Oracle Database Vault: Phân tách nhiệm vụ và điều khiển hạn chế quyền truy nhập của người dùng đặc quyền.



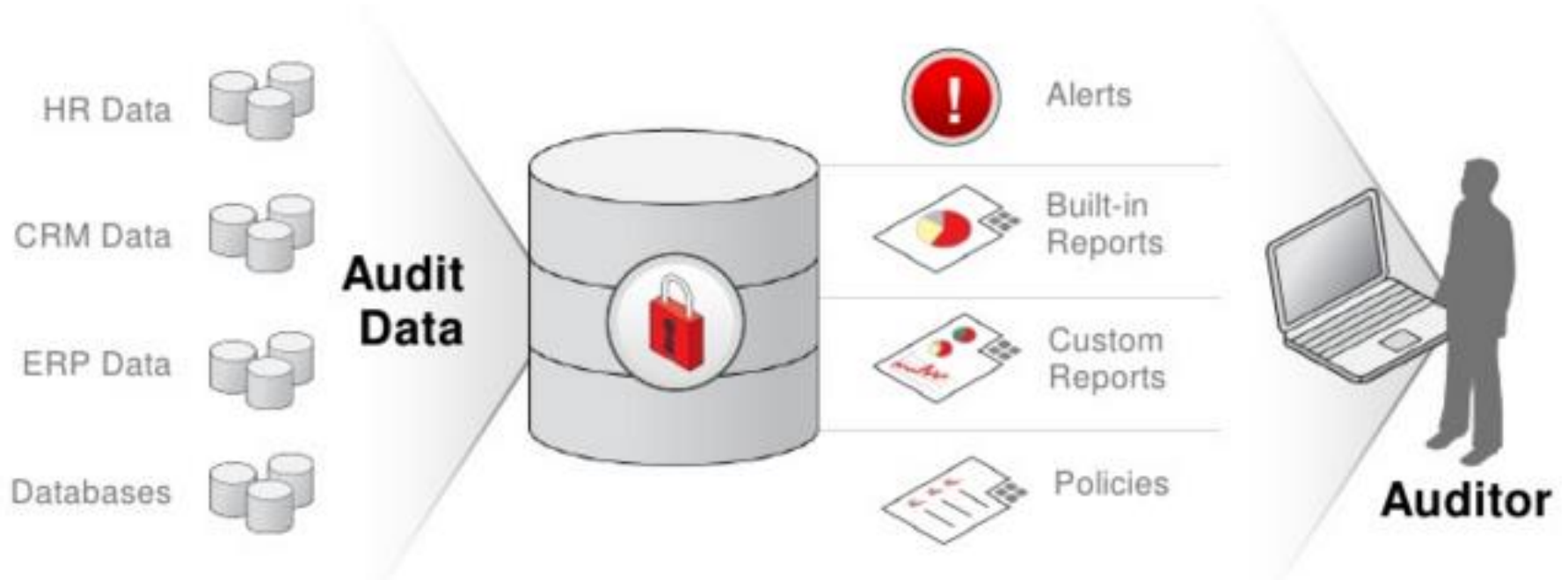
6.5.2 Bảo mật Oracle

- ❖ Oracle Database Vault: Phân loại dữ liệu cho điều khiển truy nhập.



6.5.2 Bảo mật Oracle

❖ Oracle Monitoring & Auditing: Giám sát tự động và báo cáo kiểm toán



6.5.2 Bảo mật Oracle

❖ Secure Change Tracking: Giám sát an toàn các thay đổi



6.5.2 Bảo mật Oracle

- ❖ Vulnerability Assessment & Secure Configuration: Đánh giá các lỗ hổng và cấu hình an toàn

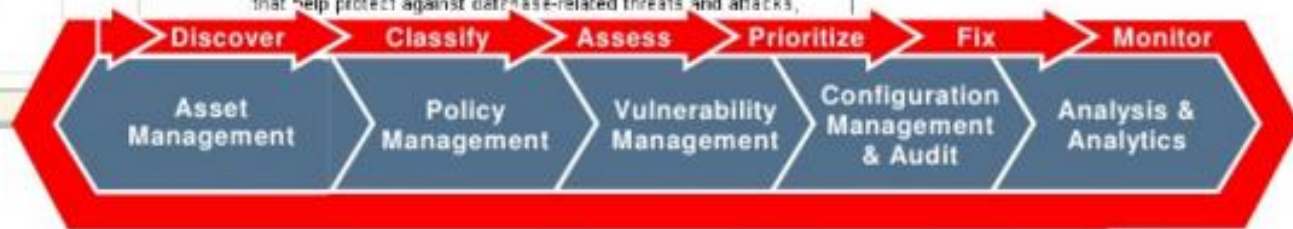
Policy Group Evaluation Results

[Evaluation Results](#) [Library](#) [Errors](#)

This table summarizes the policy group evaluations. Click the name of the policy group for detailed information. Page Refreshed Sep 17, 2008 4:48:43

Policy Group /	Version	Keywords	Average Compliance Score (%)	Targets	Target Type	Description
Secure Configuration for Oracle Database	1	Security	<div><div></div></div> 58	5	Database Instance	Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for the Oracle database. D
Secure Configuration for Oracle Listener	1	Security	<div><div></div></div> 90	3	Listener	Ensures adherence with best-practice security configuration settings that help protect against database-related threats and attacks.

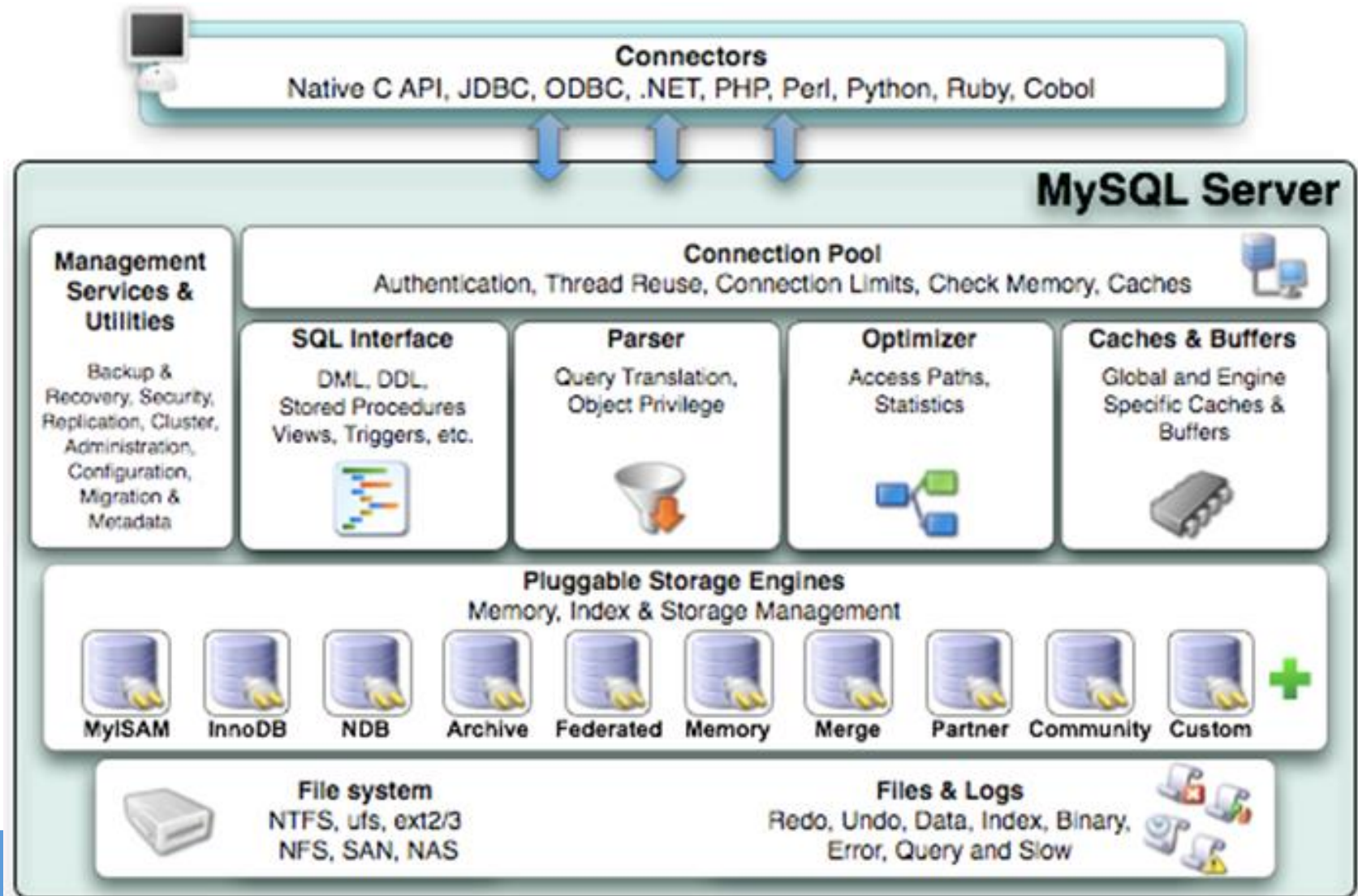
[Evaluation Results](#) [Library](#) [Errors](#)



6.5.3 Bảo mật MySQL

- ❖ Kiến trúc của MySQL
- ❖ Các thành phần của MySQL
- ❖ Mô hình bảo mật của MySQL

6.5.3 Bảo mật MySQL - Kiến trúc của MySQL

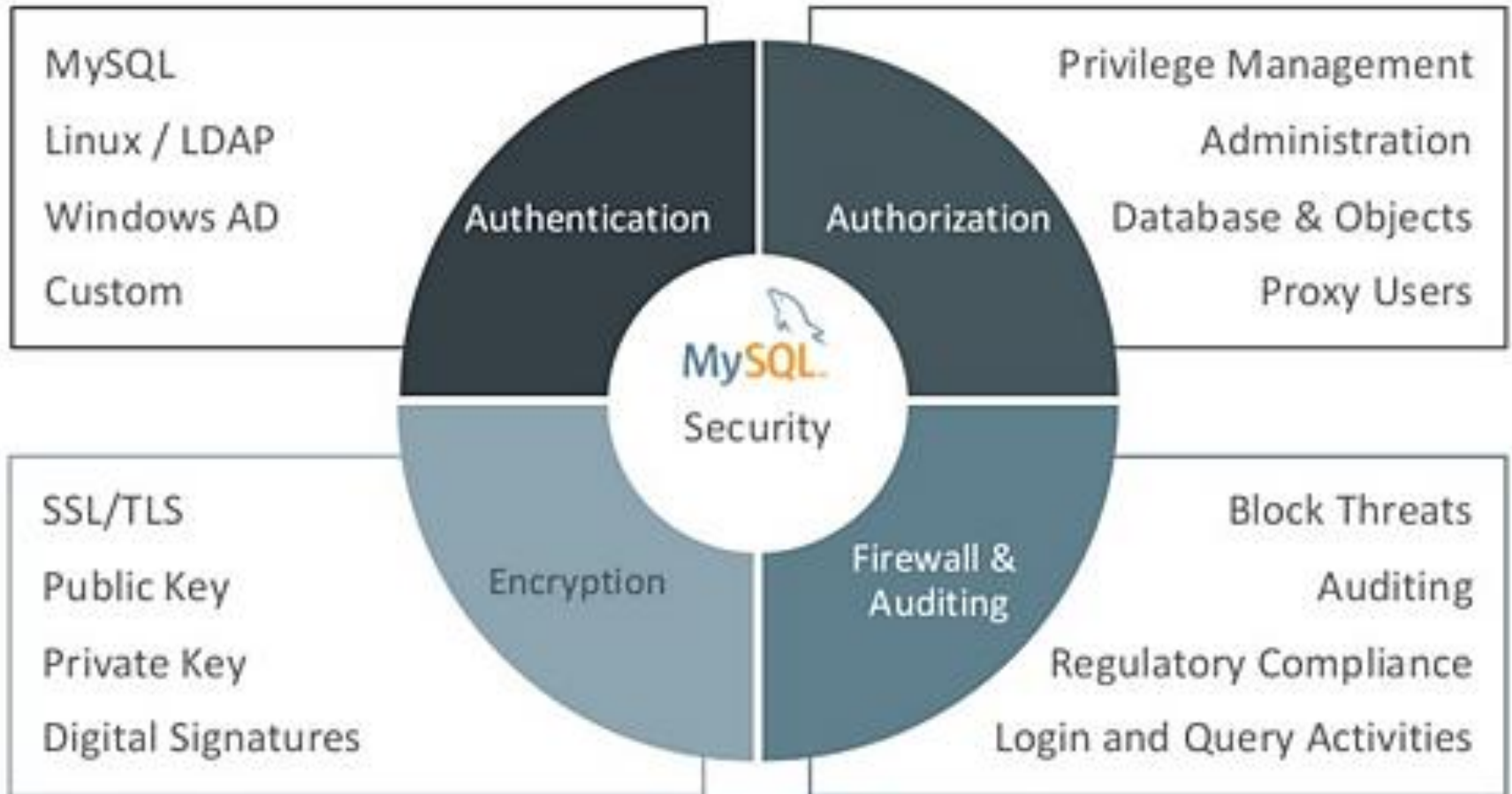


6.5.3 Bảo mật MySQL

- ❖ Các thành phần của MySQL
 - Connectors
 - Connection Pool
 - Query Engine
 - SQL Interface
 - Parser
 - Optimizer
 - Caches & Buffers
 - Pluggable Storage Engines
 - Files and Logs
 - Management Services & Utilities

6.5.3 Bảo mật MySQL

❖ Mô hình an ninh của MySQL



6.5.3 Bảo mật MySQL

❖ Authentication (Xác thực)

- Xác thực dựa trên hệ điều hành
 - Windows AD
 - Linux / LDAP
- Xác thực cung cấp bởi MySQL
- Xác thực Custom
 - Xác thực bằng phương pháp riêng/đặc thù.

6.5.3 Bảo mật MySQL

❖ Authorization (Trao quyền/ủy quyền)

- Quản lý đặc quyền
- Quản trị quyền
- Quản lý CSDL và các đối tượng
- Proxy users

6.5.3 Bảo mật MySQL

❖ Encryption (Mã hóa)

- SSL/TLS
- Public Key
- Private Key
- Digital Signatures

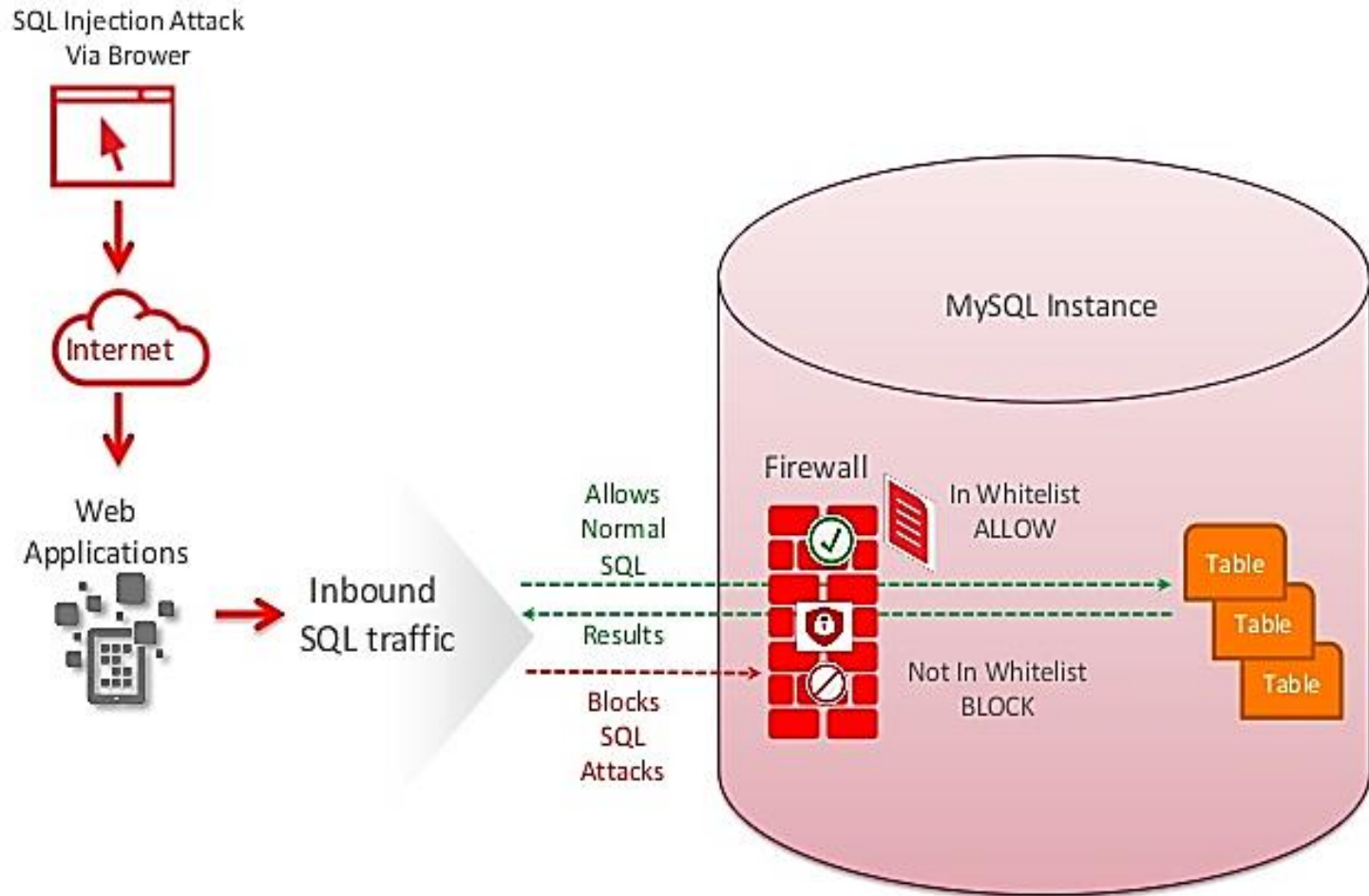
6.5.3 Bảo mật MySQL

❖ Firewall & Auditing (Tường lửa và Kiểm toán)

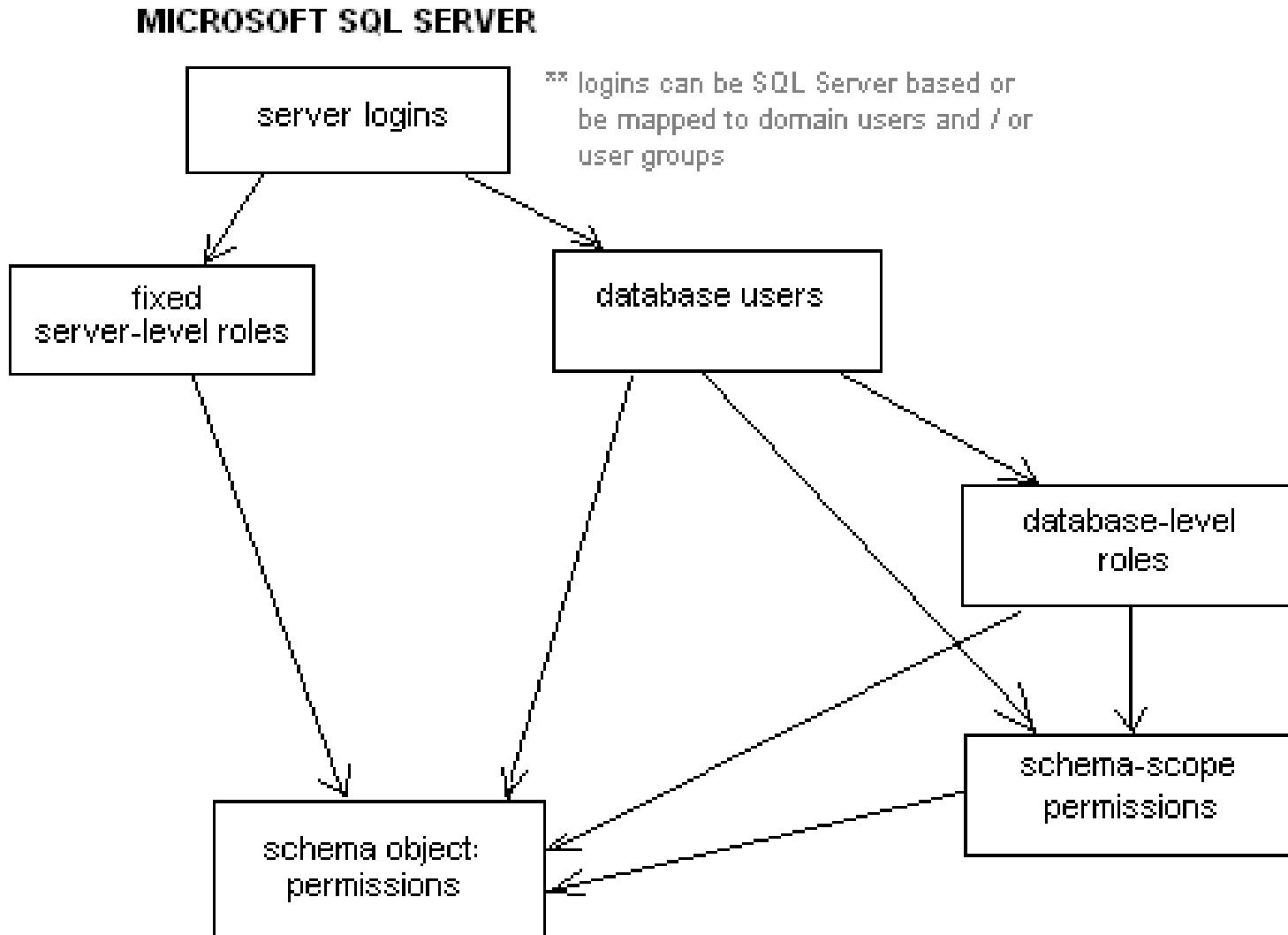
- Chặn các mối đe dọa
- Kiểm toán
- Giám sát việc tuân thủ chính sách an ninh
- Giám sát các hành vi đăng nhập và truy vấn.

6.5.3 Bảo mật MySQL

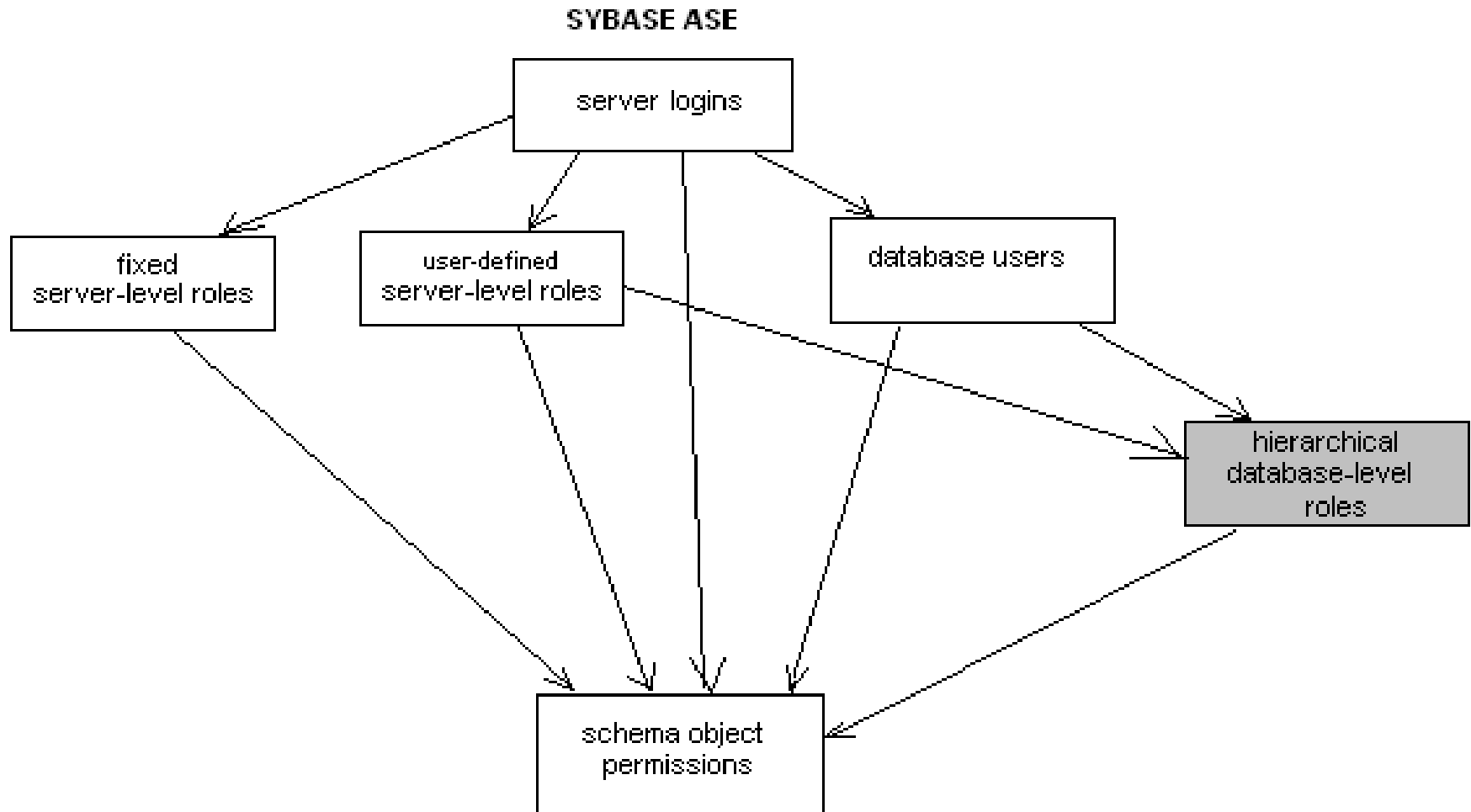
❖ MySQL Firewall



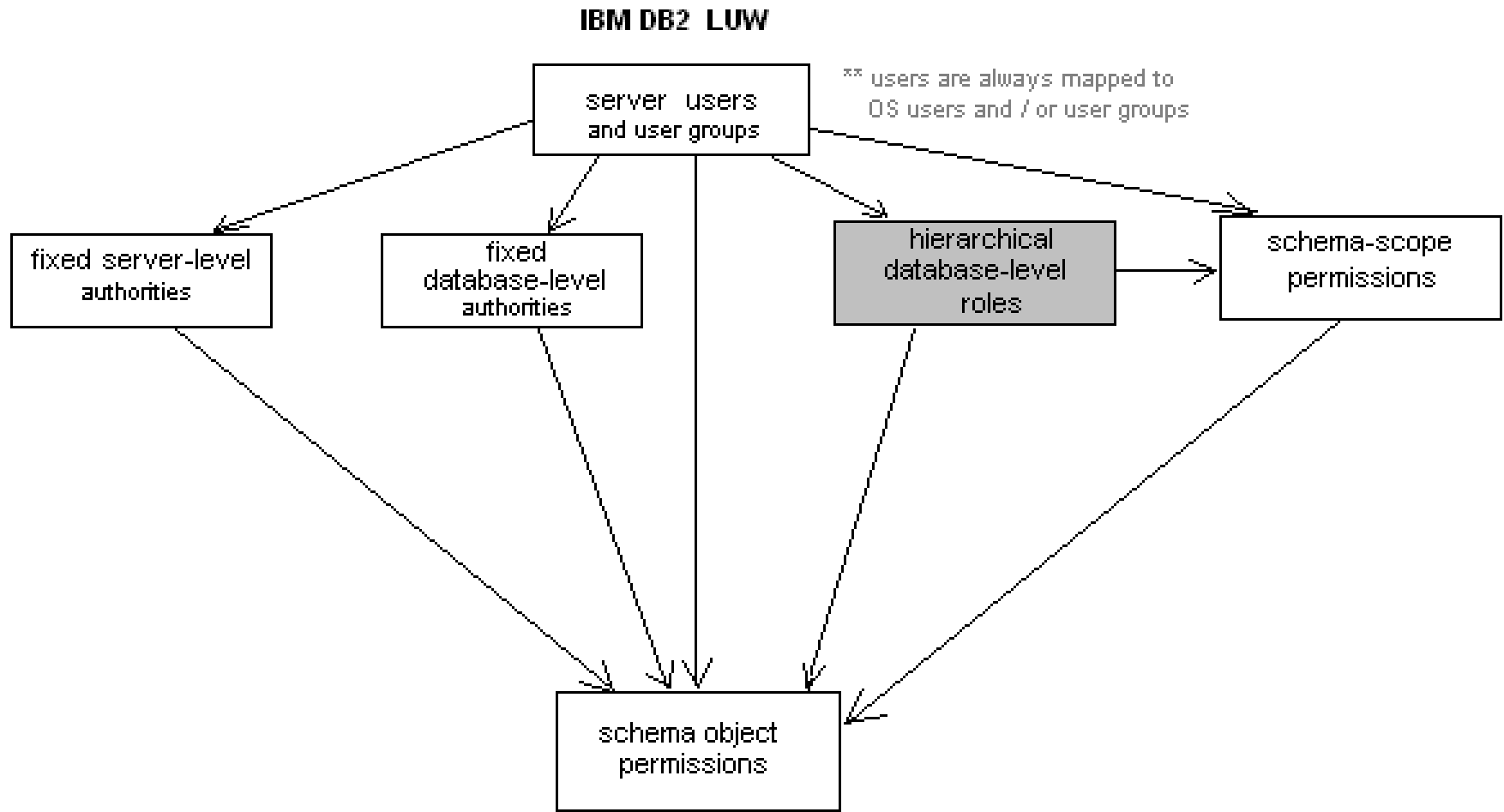
6.5.4 Một số mô hình QL t.khoản truy nhập trên các DBMS



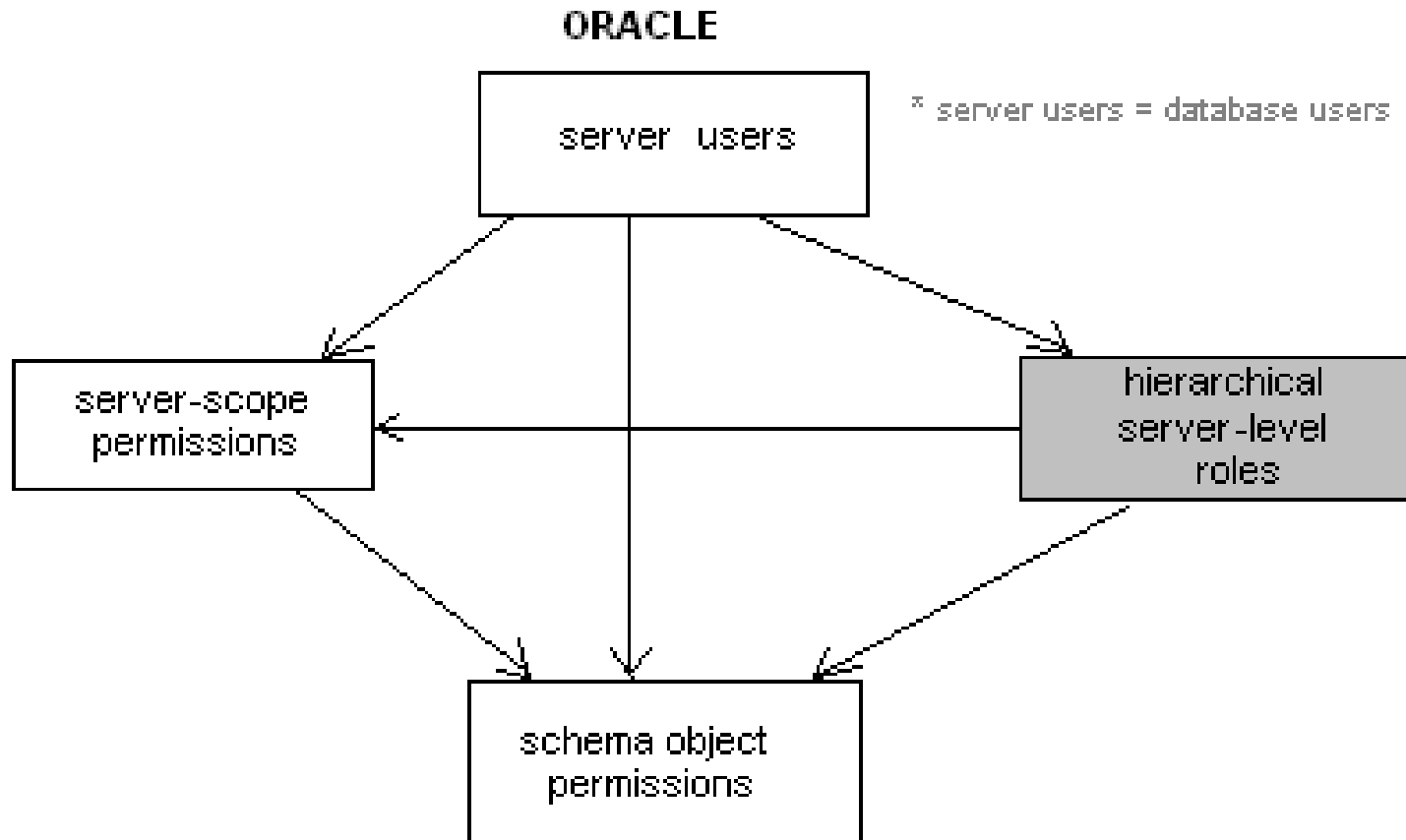
6.5.4 Một số mô hình QL t.khoản truy nhập trên các DBMS



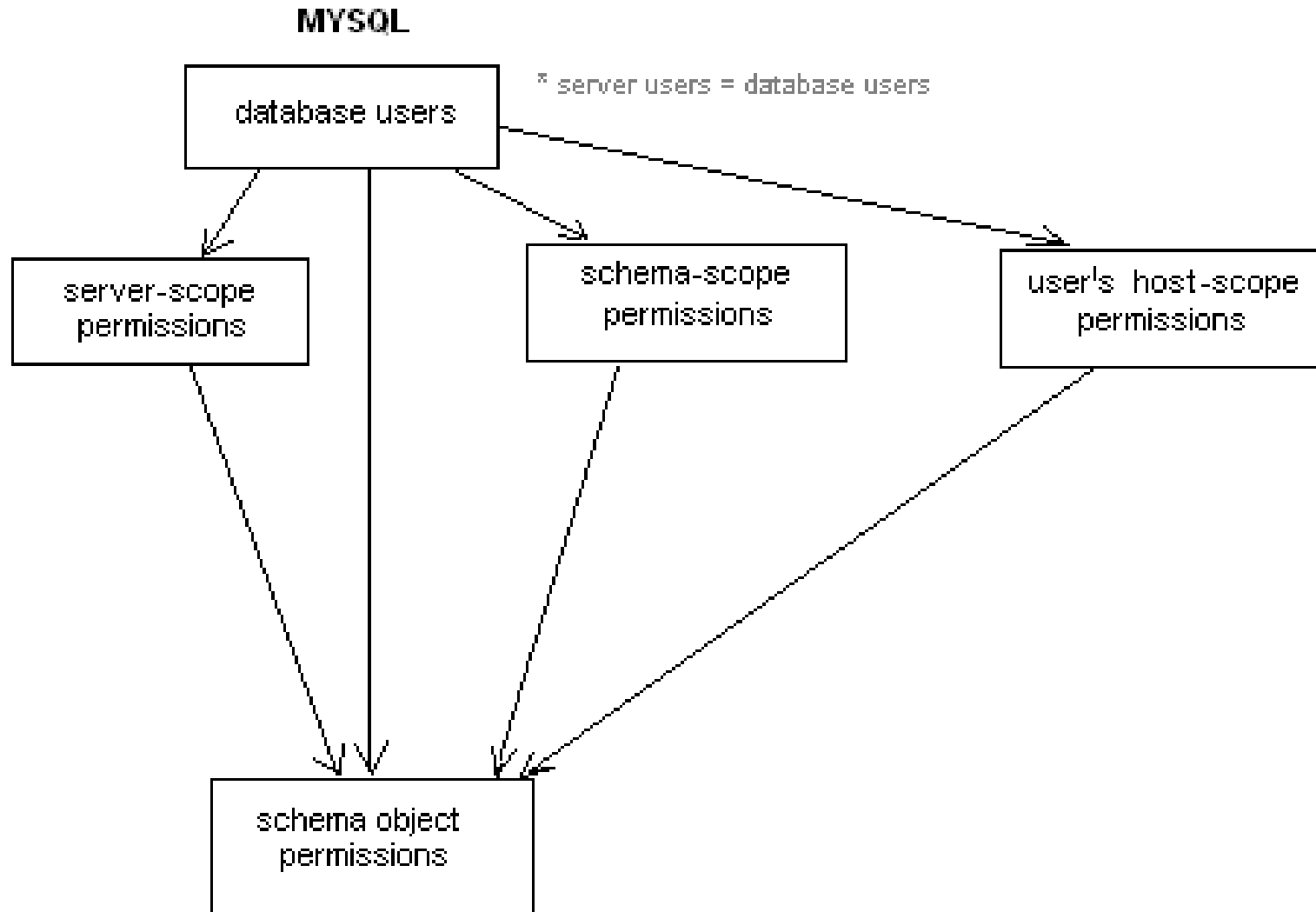
6.5.4 Một số mô hình QL t.khoản truy nhập trên các DBMS



6.5.4 Một số mô hình QL t.khoản truy nhập trên các DBMS



6.5.4 Một số mô hình QL t.khoản truy nhập trên các DBMS



Kiểm tra, đánh giá



Hình 6.23. Mô hình thực hiện bảo mật hạ tầng dữ liệu trọng yếu IBM Guardium

Các bước kiểm tra, đánh giá

- ❖ <http://www.micoresolutions.com/oracle-db-security-assessment/>
- ❖ Database user accounts: Kiểm tra tài khoản người dùng cơ sở dữ liệu
- ❖ Password policies: Kiểm tra chính sách quản lý mật khẩu
- ❖ Database auditing procedures: Kiểm tra thủ tục kiểm toán cơ sở dữ liệu
- ❖ - Operational procedures: Kiểm tra thủ tục vận hành
- ❖ - Data migration and refresh: Kiểm tra việc di chuyển và làm mới dữ liệu
- ❖ - Database configuration: Kiểm tra cấu hình cơ sở dữ liệu
- ❖ - Database system security patches: Kiểm tra việc cập nhật các bản vá cơ sở dữ liệu
- ❖ - Database access control: Kiểm tra cơ chế kiểm soát truy cập.