Oracle Security

# Administering User Security

Mỗi 1 database user đều có:

* Unique username
* Password riêng
* Default tablespace
* Temporary tablespace
* User profile
* Cosumer group privileges
* An account status
* Có thể connect vào từ ngoài bằng cách sử dụng dblink

Schema:

* Là tập hợp các object được sở hữu bởi 1 user
* Có cùng tên với user

User đặc biệt:

* SYS:
  + Được gán DBA roles và có toàn bộ quyền hành vs DB với admin option
  + Có thể khởi động, shutdown DB và các lệnh liên quan tới hệ thống ( alter )
  + Sở hữu data dictionary và AWR
  + Được gán roles SYSDBA va SYSOPER( start
* System
  + Không thể stop vs start DB

Xác thực Administrator

* DBA phải có quyền tạo và delete file trên OS
* Người sử dụng khác ko có quyền tạo hoặc delete database file

Đối với kết nối của SYSDBA, SYSOPER, and SYSASM:

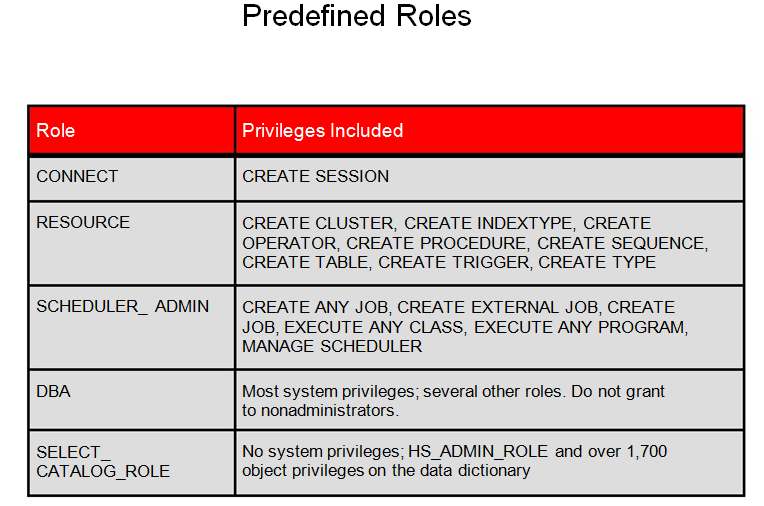
* DBA được xác thực bởi password file và 1 phương thức xác thực mạnh mẽ
* OS account name được xác thực bởi OS
* Khi kết nối tới database ko cần khai bao user/password nếu đã được xác thực bởi OS và Password ko được lưu trữ trên database

Privileges: Có 2 loại user privileges:

* System: cho phép user thao tác vs hệ thống
  + Alter system, alter database...
* Object: cho phép user truy cập vào các dữ liệu
  + Select, update, insert ....

Các privileges được gán vào các role:

* Dễ dàng quản lý các privileges
* Quản lý động các privileges ( thêm-xóa privileges từ các roles)



* Gán cho user dev: connect và resource, nếu cần thiết thì thêm Scheduler\_admin
* DBA Schema: (của User), được phép thao tác vs hệ thống nhưng ko được stop-start DB
* SYSOPER: Schema: (của Public)được phép thao tác vs hệ thống nhưng ko được thao tác với dữ liệu của người dùng
* SYSDBA: Schema( SYS) Role cao nhất của database toàn quyền vs DB

Sử dụng profile để quản lý User

* Điều khiển truy cập người dùng
  + Thời gian truy cập, số seesion tối đa...
* Quản lý tình trạng của account và hiệu lực của password

Sử dụng password để xác thực người dùng:

* Password ko được nhập sai quá 3 lần
* Phân biệt hoa thường, ký tự đặc biệt
* Không quá 30 ký tự( 30 bytes)
* Có thể sử dụng profile để control password
* Ví dụ:

CREATE PROFILE prof LIMIT

FAILED\_LOGIN\_ATTEMPTS 4

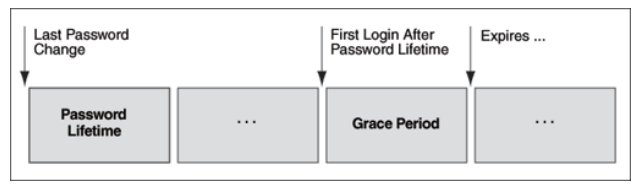
PASSWORD\_LOCK\_TIME 30

PASSWORD\_LIFE\_TIME 90

PASSWORD\_GRACE\_TIME 3;

ALTER USER johndoe PROFILE prof;

|  |  |  |
| --- | --- | --- |
| Parameter | Deffault setting | Mô tả |
| FAILED\_LOGIN\_ATTEMPTS | 10 | Số lần log on tối đa thất bại trước khi bị khóa account |
| PASSWORD\_GRACE\_TIME | 7 | Số ngày user phải đổi pass trước khi hết hạn |
| PASSWORD\_LIFE\_TIME | 180 | Số ngày có thể sử dụng password hiện tại |
| PASSWORD\_LOCK\_TIME | 1 | Số ngày khóa account nếu log in thất bại |
| PASSWORD\_REUSE\_MAX | UNLIMITED | Số lần đổi password bắt buộc trước khi sử dụng lại password hiện tại |
| PASSWORD\_REUSE\_TIME | UNLIMITED | Thời gian đổi password bắt buộc trước khi sử dụng lại password hiện tại |

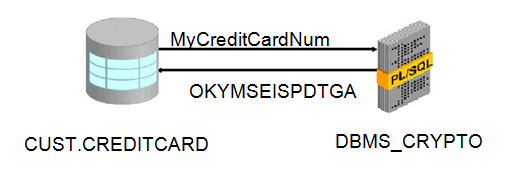


# Audit

* Khái niệm:Auditing có nghĩa là theo dõi, nắm bắt sự kiện nào đó và lưu trữ thông tin xảy ra trong hệ thống.
* Tác dụng: cho phép biết được những hành động xảy ra đối với đội tượng được quan tâm ( system, user, table...) để có biện pháp quản lý và xử lý khi gặp sự cố
* Thiệt hại:
  + Làm giảm hiệu năng của hệ thống
  + Tốn dung lượng lưu trữ của hệ thống
* Có 5 loại audit chính:
  + Mandatory auditing: Audit tất cả database.
  + Standard database auditing:
    - Sử dụng thao số Audit\_trail
    - Cho phép lựa chọn đối tượng cũng như thuộc tính cho audit cũng như các thuộc tính của audit
  + Value-based auditing: Mở rộng cho standard database auditing: không những chỉ ra khi nào event nào xảy ra mà còn cho phép biết biết chính xác giá trị thay đổi.
  + Fine-grained auditing (FGA): Mở rộng cho standard database auditing, cho phép biết chính xác câu lệnh SQL tạo nên event
  + SYSDBA (and SYSOPER) auditing: Auditing DBA,lưu trữ file ở ngoài DB
* Những loại hay sử dụng:
  + Audit DDL ( cho database, cho schema)
  + FGA

# Mã hóa dữ liệu

Mã hóa dữ liệu bằng cách sử dụng package DBMS\_CRTPTO của database



Cơ chế hoạt động: package này sẽ mã hóa dữ liệu bằng key ( random) sau đó nó cung cấp key cho user, khi user muốn truy cập vào dữ liệu thì bắt buộc phải nhập key.

Hàm sinh key: DBMS\_CRYPTO.RANDOMBYTES is based on RSA x9.31 PRNG.

Tác dụng:

* Tăng cường bảo mật dữ liệu

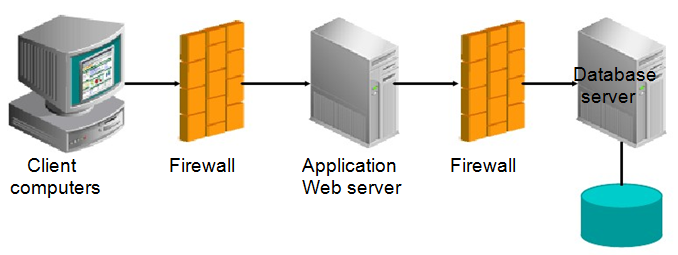
Thiệt hại:

* Khó khăn khi truy cập dữ liệu
* Giảm hiệu năng hoạt động của hệ thống
* Phiền phức khi phải quản lý thêm key
* Khó khăn khi mã hóa:
  + Indexed: Not supported
  + Large objects (LOBs): Chậm

# Network Security

Tăng cường khả năng bảo vệ của database trong mạng

* Use a firewall.
  + Sử dụng tường lửa chỉ cho phép ứng dụng liên quan tới database mới có thể truy cập tới database server



* Restrict IP addresses
  + Sử dụng SQLNET.ora để giới hạn các địa chỉ IP có thể truy cập tới database server. Ví dụ:

tcp.validnode\_checking = YES

tcp.excluded\_nodes = 192.168.10.100

tcp.invited\_nodes =

(192.168.10.101, 192.168.10.102)

* + Không nên sử dụng công nghệ này 1 mình vì địa chỉ IP có thể bị chiếm dụng hoặc luồng kết nối bị điều hướng
  + Nên kết hợp với giới hạn cổng và giao thức truy cập
* Encrypt network traffic.

Sử dụng TCPs/SSL để mã hóa đường truyền:

* + Tăng độ an toàn cho đường truyền
  + Làm giảm tốc độ đường truyền

(PROTOCOL=tcps)

(PORT = 2484)))

* Prevent remote administration
  + Tiến hành đặt password cho listener để đảm bảo listener ko bị sửa đổi

LSNRCTL> CHANGE\_PASSWORD

Old password: lsnrc80

New password: lsnrc90

Reenter new password: lsnrc90

LSNRCTL> SET PASSWORD

Password:

The command completed successfully

LSNRCTL> SAVE\_CONFIG

The command completed successfully

* + Tiến hành thêm tham số để bảo vệ listener ko thể bị thay đổi online

ADMIN\_RESTRICTIONS\_LISTENER=ON

* + Tiến hành enable chế độ log cho listener để theo dõi
    - Các client có request
    - Các thao tác đối với listener