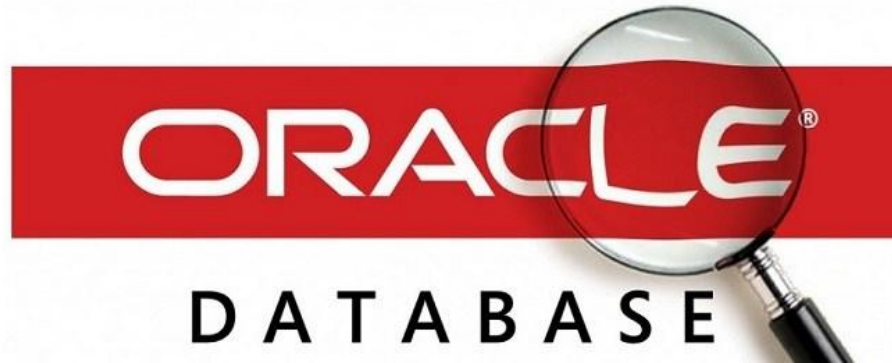


# CÔNG NGHỆ ORACLE

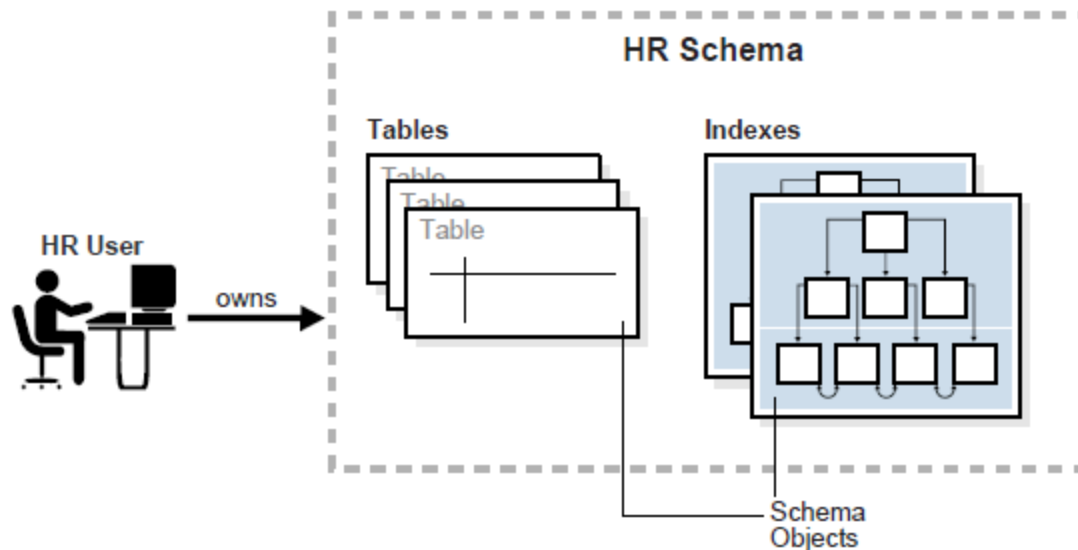


*TP. HCM 11/2017*

# Quản lý User, Privilege và Role

# Tổng quan về User

- User kết nối đến cơ sở dữ liệu bằng cách sử dụng một tài khoản (user account)
- Liên kết với một user account là một schema.

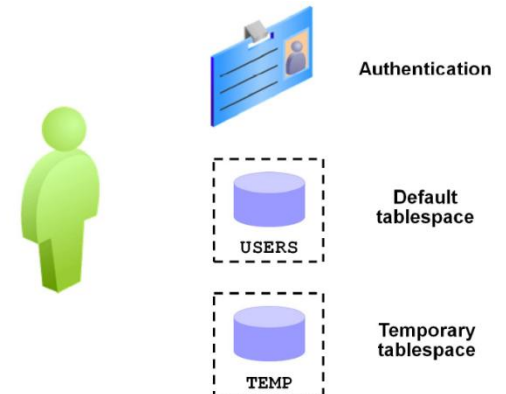


# Các user được định nghĩa sẵn bởi oracle

- Những user account sau được hình thành khi tạo database:
  - SYS, SYSTEM, SYSMAN, DBSNMP : người quản trị cơ sở dữ liệu (Database administrative user)
  - Các schema mẫu: HR, OE, SH, ...

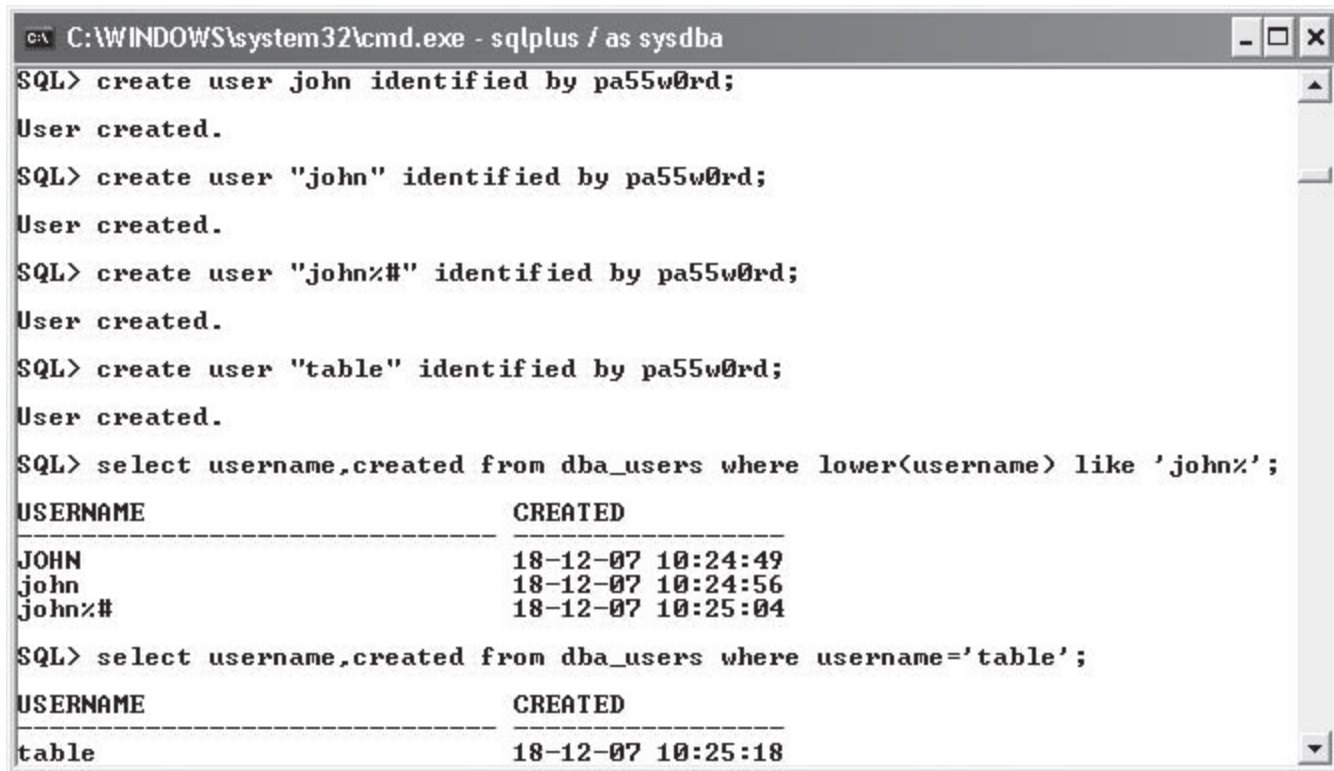
# Những thuộc tính của user account

- Mỗi user account có một vài thuộc tính được định nghĩa sẵn lúc khởi tạo.
- Chúng sẽ được áp cho các session kết nối tới account
- Những thuộc tính này là:
  - Username
  - Phương thức xác thực (Authentication method)
  - Tablespace mặc định (Default tablespace)
  - Hạn mức tablespace (Tablespace quotas)
  - Tablespace tạm (Temporary Tablespace)
  - User profile
  - Trạng thái account (Account status)



# Username

- username phải duy nhất trong database.
- username không được thay đổi khi đã được tạo.



```
C:\WINDOWS\system32\cmd.exe - sqlplus / as sysdba
SQL> create user john identified by pa55w0rd;
User created.
SQL> create user "john" identified by pa55w0rd;
User created.
SQL> create user "john%#" identified by pa55w0rd;
User created.
SQL> create user "table" identified by pa55w0rd;
User created.
SQL> select username,created from dba_users where lower(username) like 'john%';
USERNAME                                CREATED
-----                                -
JOHN                                     18-12-07 10:24:49
john                                     18-12-07 10:24:56
john%#                                   18-12-07 10:25:04
SQL> select username,created from dba_users where username='table';
USERNAME                                CREATED
-----                                -
table                                    18-12-07 10:25:18
```

# Tablespace mặc định và hạn mức

- Tablespace mặc định (default): được dùng khi một đối tượng (object) được tạo mà không chỉ rõ tablespace cho nó.
- Hạn mức Tablespace: là dung lượng tối đa được sử dụng trong một tablespace
- Mỗi một user account có một tablespace mặc định.

C:\WINDOWS\system32\cmd.exe - sqlplus / as sysdba

```
SQL> select username,DEFAULT_TABLESPACE,temporary_TABLESPACE from dba_users
2 where username='JOHN';
```

USERNAME	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE
JOHN	USERS	TEMP

```
SQL> alter user john quota 10m on users;
```

User altered.

```
SQL> alter user john quota unlimited on example;
```

User altered.

```
SQL> select TABLESPACE_NAME,BYTES,MAX_BYTES from dba_ts_quotas
2 where username='JOHN';
```

TABLESPACE_NAME	BYTES	MAX_BYTES
USERS	0	10485760
EXAMPLE	0	-1

```
SQL> select PROPERTY_NAME,PROPERTY_VALUE from database_properties
2 where property_name like '%TABLESPACE';
```

PROPERTY_NAME	PROPERTY_VALUE
DEFAULT_TEMP_TABLESPACE	TEMP
DEFAULT_PERMANENT_TABLESPACE	USERS



# Tablespace tạm

- Temporary tablespace chứa dữ liệu tạm thời chỉ tồn tại trong một phiên làm việc (session).
- Temporary tablespace được dùng để lưu trữ:
  - Kết quả sắp xếp (sort).
  - Table tạm và index tạm.
  - LOBs và cây B-tree tạm
- Để thay đổi temporary tablespace của một user:
  - `ALTER USER username TEMPORARY TABLESPACE tablespace_name;`

# Profile

- user's profile kiểm soát việc thiết lập mật khẩu và cung cấp một số quyền hạn nhất định trên nguồn tài nguyên.

CREATE PROFILE	app_user	
LIMIT SESSIONS_PER_USER		UNLIMITED
CPU_PER_SESSION		UNLIMITED
CPU_PER_CALL		3000
CONNECT_TIME		45
LOGICAL_READS_PER_SESSION		DEFAULT
LOGICAL_READS_PER_CALL		1000

```
ALTER USER sh PROFILE app_user ;
```

# Trạng thái account

- **OPEN:** account sẵn sàng để sử dụng.
- **LOCKED:** account đã bị khóa. Không một user nào có thể kết nối đến account đã bị lock.
- **EXPIRED:** mật khẩu đã hết hạn dùng, cần thay đổi mật khẩu mới.
- Để lock và unlock một tài khoản:
  - ALTER USER *username* ACCOUNT LOCK ;
  - ALTER USER *username* ACCOUNT UNLOCK ;
- Bắt người dùng thay đổi password:
  - ALTER USER *username* PASSWORD EXPIRE;

# Phương thức xác thực (Authentication Methods)

- Xác thực hệ điều hành (Operating system authentication)
- Xác thực dựa trên password file (Password file authentication)
- Xác thực trên password (Password authentication)
- External authentication
- Global Authentication

# Operating System and Password File Authentication

- Cấp cho user quyền SYSDBA hoặc SYSOPER
  - GRANT *[sysdba / sysoper]* TO *username* ;
- Sử dụng xác thực dựa trên password file:
  - CONNECT *username / password* [*@db\_alias*] AS [*SYSOPER / SYSDBA*] ;
- Sử dụng xác thực trên hệ điều hành:
  - CONNECT / AS [ *SYSOPER | SYSDBA* ] ;

# Xác thực dựa trên password

- Tạo user:

```
CREATE USER sidney
```

```
IDENTIFIED BY out_standing1
```

```
DEFAULT TABLESPACE example
```

```
QUOTA 10M ON example
```

- Thay đổi password:
  - ALTER USER *username IDENTIFIED BY password ;*
- Kết nối:
  - CONNECT *username / password [ @db\_alias ] ;*

# External authentication

- Create user "OPS\$JWACER\JOHN WATSON" identified externally;
  - John Watson: Windows logon ID
  - WACER: Windows domain (`echo %USERDOMAIN%`)
  - OPS\$: OS\_AUTHENT\_PREFIX  
(`select value from v$parameter where name='os_authent_prefix';`)
- A user logged as jwatson will be able to issue the command: `sqlplus /`

Note that the username must be in uppercase, and because of the illegal characters (a backslash and a space) must be enclosed in double quotes.

# Ví dụ: tạo user account

```
CREATE user helen IDENTIFIED BY tiger
```

```
CREATE user scott IDENTIFIED BY tiger  
DEFAULT tablespace tbspace_book  
TEMPORARY tablespace temp  
QUOTA 100m on tbspace_book QUOTA unlimited on  
example  
PROFILE developer_profile  
PASSWORD expire  
ACCOUNT unlock;
```



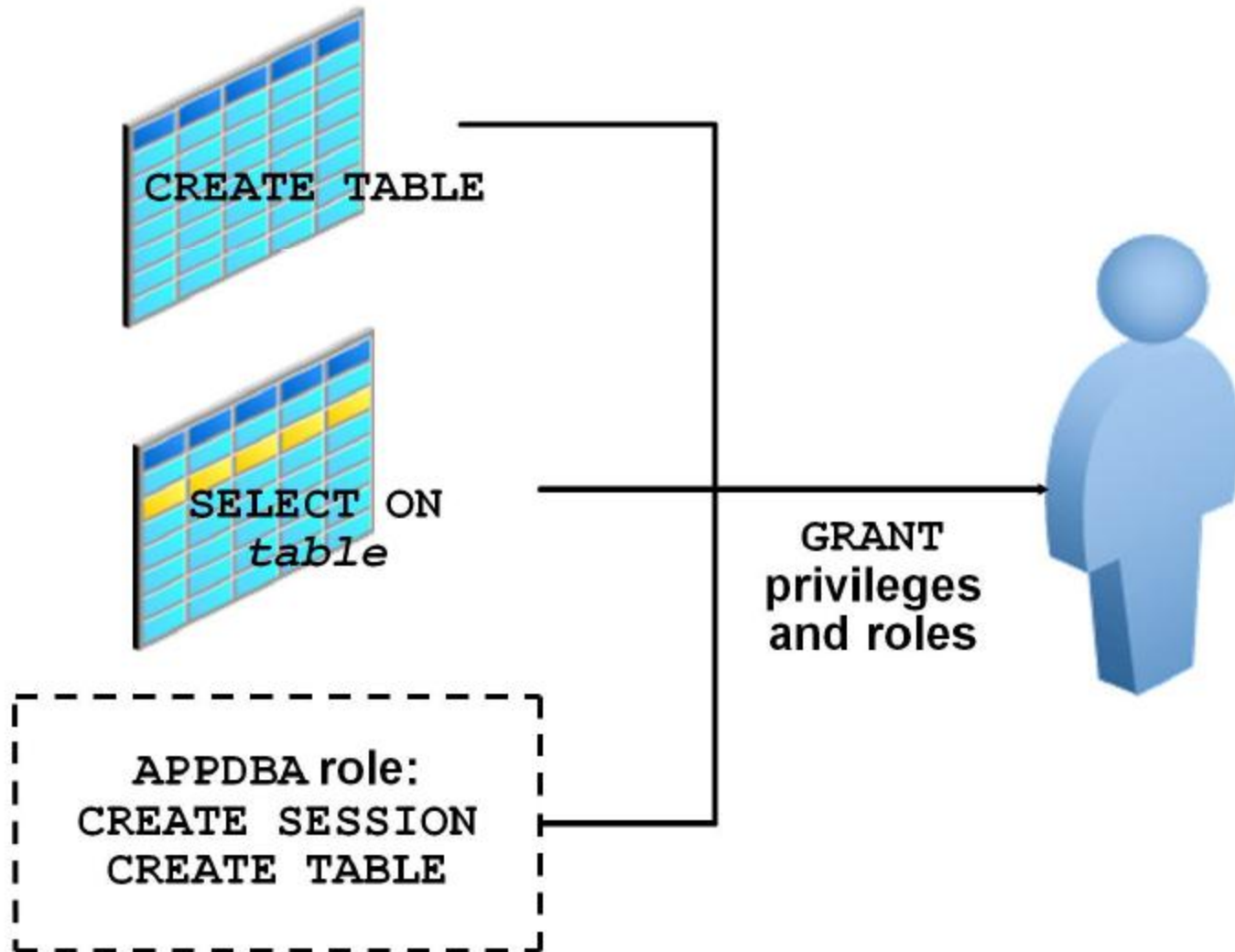
# Ví dụ: thay đổi thuộc tính của user account

- Thay đổi password:
  - alter user scott identified by lion;
- Thay đổi default và temporary tablespaces:
  - alter user scott default tablespace store\_data  
temporary tablespace temp;
- Thay đổi hạn mức tablespace:
  - alter user scott quota unlimited on store\_data quota 2M on users;
- Thay đổi profile:
  - alter user scott profile prod\_profile;
- Khóa account:
  - alter user scott account lock;

# Xóa một user

- Cú pháp:
  - DROP USER scott;
- Sử dụng CASCADE để xóa tất cả những object trong schema:
  - DROP USER scott CASCADE;

# Quản lý Privilege và Role



# Privilege

- **Privilege** là quyền để thực thi (execute) một câu lệnh SQL nào đó hoặc truy cập đến đối tượng (object) của user khác.
- Một số ví dụ về privilege:
  - Kết nối đến database (create a session)
  - Tạo bảng (Create a table)
  - Select dữ liệu từ table của user khác
  - Thực thi (execute) các stored procedure của user khác

# Privileges

- Privilege được chia làm 2 loại:
  - **System Privileges:** cho phép người dùng thao tác các hoạt động cụ thể trên database .
    - Ví dụ: CREATE TABLE, CREATE ANY TABLE, ALTER ANY TABLE, SELECT ANY TABLE ...
  - **Object Privileges:** quản lý việc truy cập đến một đối tượng (object) cụ thể trong database
    - SELECT ON <table>, DELETE ON <table> ...
    - Ví dụ: SELECT ON EMPLOYEE

# Cấp (Grant) và thu hồi (Revoke) Privilege

- Không một user chưa được cho phép nào có thể truy cập được đến cơ sở dữ liệu Oracle (kể cả kết nối).
- Privileges được cấp cho user account với lệnh GRANT và thu hồi nó với lệnh REVOKE.

# Grant System Privileges

- Cú pháp:
  - GRANT *privilege [, privilege...]* TO *username* [*WITH ADMIN OPTION*];

- Ví dụ:

GRANT create session, alter session, create table, create view, create sequence, create trigger, create procedure TO *username* ;

# Grant System Privileges: ADMIN Option

- User được cấp quyền (với cú pháp ADMIN OPTION) sau đó có thể cấp quyền này cho user khác
- Ví dụ:

```
connect system/oracle;  
grant create table to scott with admin option;
```

```
connect scott/tiger;  
grant create table to jon;
```



# Thu hồi (Revoke) System Privileges

- Để thu hồi một system privilege, người thu hồi trước đó phải được cấp (grant) quyền với ADMIN OPTION.
  - REVOKE DROP ANY TABLE FROM hr, oe;
- Việc thu hồi quyền trên system privilege sẽ không theo dây chuyền (cascade). Trái ngược với việc thu hồi quyền trên object privilege.

C:\WINDOWS\system32\cmd.exe - sqlplus / as sysdba

SQL>

SQL> grant create table to scott with admin option;

Grant succeeded.

SQL> connect scott/tiger;

Connected.

SQL> grant create table to jon;

Grant succeeded.

SQL> conn / as sysdba

Connected.

SQL> revoke create table from scott;

Revoke succeeded.

SQL> select privilege from dba\_sys\_privs where grantee='JON';

PRIVILEGE

-----  
CREATE SESSION

CREATE TABLE

SQL> \_

# Object Privileges

Object Privileges are



ALTER	Change the table definition with the ALTER TABLE statement.
DELETE	Remove rows from the table with the DELETE statement. <b>Note:</b> You must grant the SELECT privilege on the table along with the DELETE privilege.
INDEX	Create an index on the table with the CREATE INDEX statement.
INSERT	Add new rows to the table with the INSERT statement.
REFERENCES	Create a constraint that refers to the table. You cannot grant this privilege to a role.
SELECT	Query the table with the SELECT statement.
UPDATE	Change data in the table with the UPDATE statement.
	<b>Note:</b> You must grant the SELECT privilege on the table along with the UPDATE privilege.



# Cấp (Grant) Object Privileges

- Cú pháp:
  - GRANT *privilege ON [schema.]object TO username [WITH GRANT OPTION] ;*
- Ví dụ:
  - GRANT select on store.orders to scott;
  - GRANT select on store.customers to scott;
  - GRANT update (order\_status) on store.orders to scott;
  - GRANT all on store.regions to scott;

# Grant Object Privileges: GRANT OPTION

- Cho phép người được cấp quyền tiếp tục cấp quyền này cho user và role khác.

```
connect store/admin123;
```

```
grant select on customers to sales with grant option;
```

```
connect sales/sales;
```

```
grant select on store.customers to webapp with grant option;
```

```
conn webapp/oracle;
```

```
grant select on store.customers to scott;
```

# Thu hồi (Revoke) Object Privileges

- Để thu hồi một object privilege, thì người thu hồi phải chính là người đã cấp quyền này.

```
connect store/admin123;
```

```
grant select on customers to sales with grant option;
```

```
connect sales/sales;
```

```
grant select on store.customers to webapp;
```

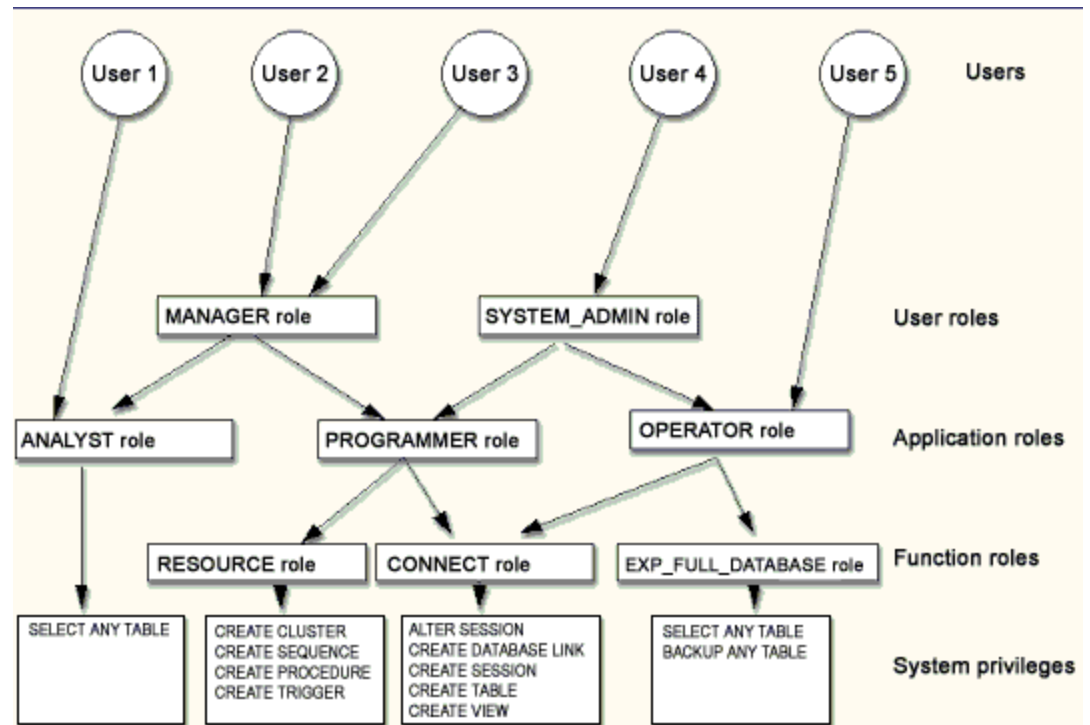
- connect store/admin123;

- **revoke** select on customers **from sales**;

- Việc thu hồi một object privilege sẽ theo dây chuyền (khác với việc thu hồi quyền trong system privilege)
  - Theo ví dụ trên thì sales, webapp sẽ không còn quyền select on store.customers.

# Roles

- Oracle cung cấp một phương thức để dễ dàng quản lý các privilege thông qua role
- Role chính là các privilege hoặc các role kết hợp lại với nhau



# Role định nghĩa sẵn

<b>CONNECT</b>	exists for backward compatibility, now it has only the CREATE SESSION privilege.
<b>RESOURCE</b>	this role can create data objects (such as tables) and procedural objects (such PL/SQL procedures). It also includes the UNLIMITED TABLESPACE privilege.
<b>DBA</b>	Has most of the system privileges, and several object privileges and roles

Ngoài ra cũng có một role đã được định nghĩa trước đó là PUBLIC, role này luôn được cấp cho database user account

grant select on hr.regions to public;

(all users will be able to query the HR.REGIONS table.)



# Tạo và cấp phát quyền cho Roles

- Cú pháp: `CREATE ROLE rolename [IDENTIFIED BY password];`
- grant privileges cho role

```
create role hr_junior;  
grant create session to hr_junior;  
grant select on hr.regions to hr_junior;  
grant select on hr.locations to hr_junior;  
grant select on hr.countries to hr_junior;
```

- Grant role cho role:

```
create role hr_senior;  
grant hr_junior to hr_senior with admin option;  
grant insert, update, delete on hr.employees to hr_senior;  
grant insert, update, delete on hr.job_history to hr_senior;
```

```
Grant hr_senior to scott;
```

# Loại bỏ Role ra khỏi user

- Để loại bỏ role ra khỏi user
  - REVOKE oe\_clerk FROM scott;
- Loại bỏ role từ tất cả user
  - REVOKE hr\_manager FROM public

# Xóa role

- `DROP ROLE hr_manager;`