

5

QUẢN LÝ NGƯỜI DÙNG

➤ ***Giảng viên: Nguyễn Thị Thu Trang***

Nội dung chính

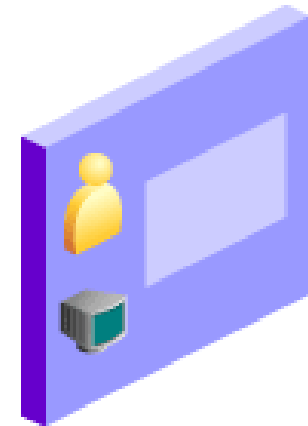
- ❖ Account
- ❖ Privilege
- ❖ Role
- ❖ Profile
- ❖ Bảo mật mật khẩu
- ❖ Hạn mức

Account (tài khoản)

❖ Mỗi tài khoản có đặc điểm:

- Tên duy nhất
- Dùng phương thức xác thực nhất định
- Có một tablespace mặc định
- Có một tablespace tạm
- Có danh sách các tài nguyên mà user được sử dụng
- Consumer group
- Có trạng thái

> Account
Xác thực
Privilege
Role
Profile
PW Security
Quota



Tạo tài khoản

Create User

Show SQL Cancel OK

General Roles System Privileges Object Privileges Quotas Consumer Group Privileges Proxy Users

★ Name

gues

Profile

DEFAULT

Authentication

Password

★ Enter Password

...

★ Confirm Password

...

For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace

users

Temporary Tablespace

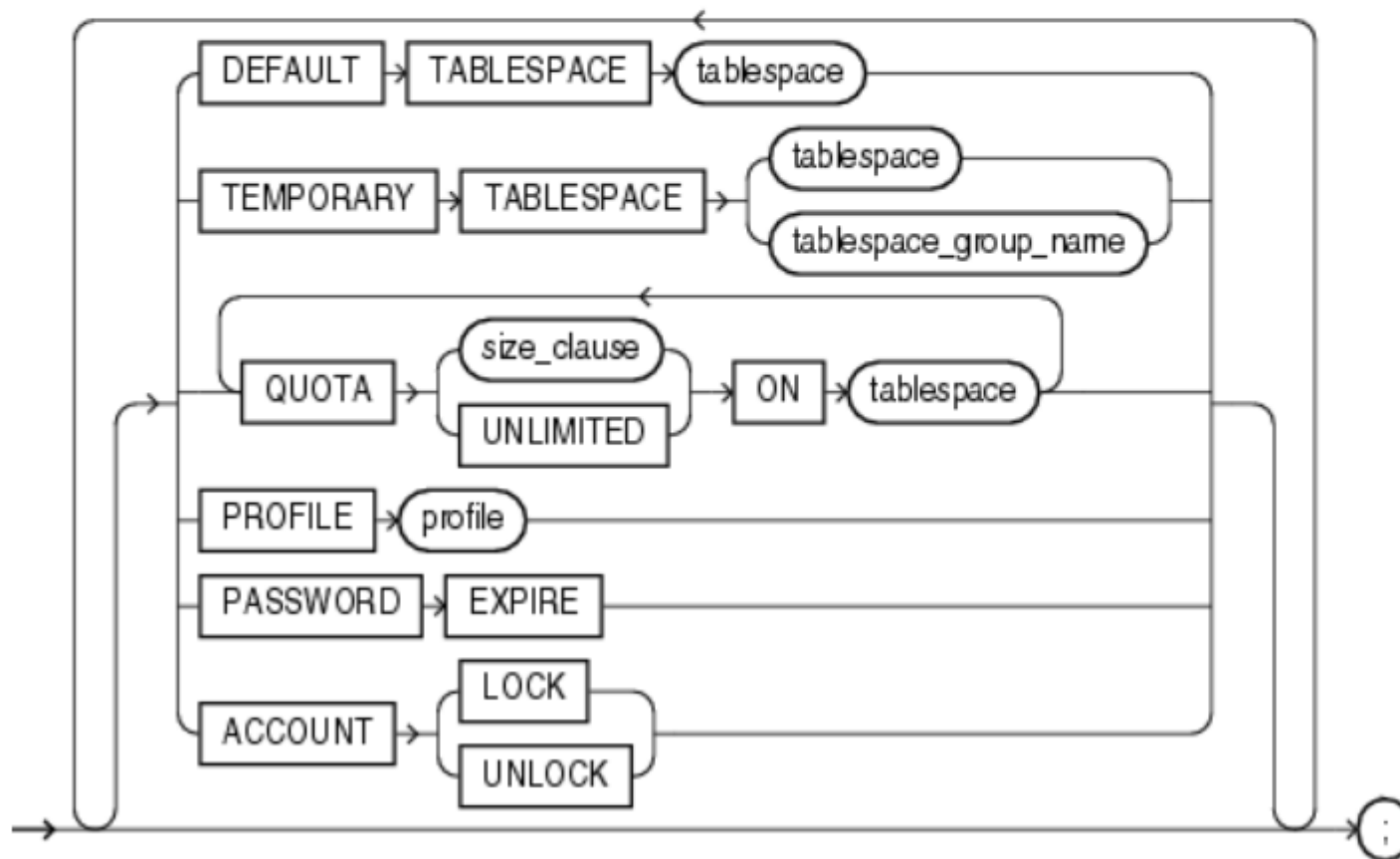
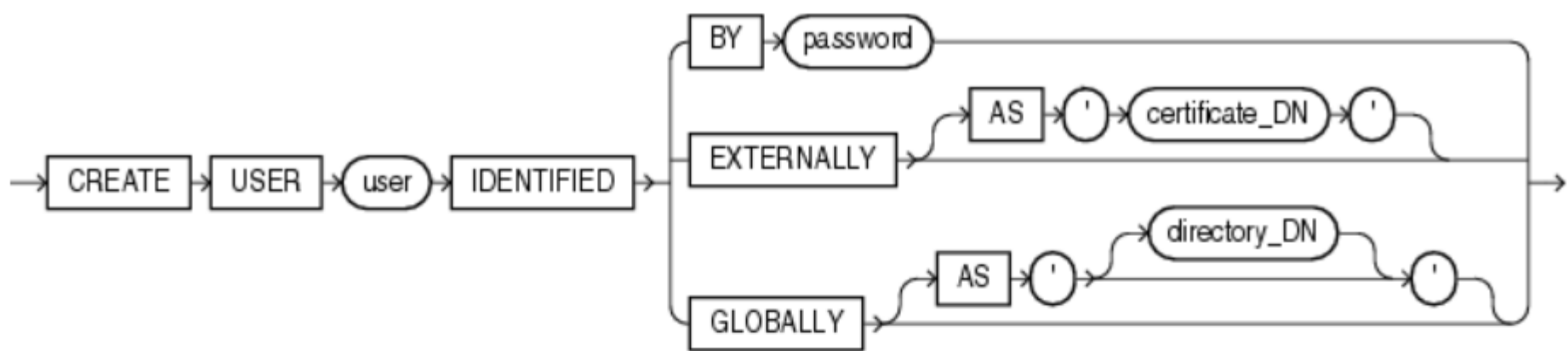
Temp

Status

☐ Locked ☒ Unlocked

General Roles System Privileges Object Privileges Quotas Consumer Group Privileges Proxy Users

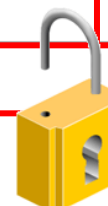
```
CREATE USER "GUES" PROFILE "DEFAULT" IDENTIFIED BY "*****" DEFAULT TABLESPACE "USERS" TEMPORARY TABLESPACE "TEMP" ACCOUNT UNLOCK
GRANT "CONNECT" TO "GUES"
```



Sửa tài khoản

Edit View Delete Actions							
Select	UserName ▲	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	
	ANONYMOUS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	<div> Create Like Expire Password Generate DDL Lock User Unlock User </div>
	BI	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	USERS	TEMP	DEFAULT	May 2, 2005 3:20:28 PM PDT
	CTXSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:56:15 PM PST
	DBSNMP	OPEN		SYSAUX	TEMP	MONITORING_PROFILE	Mar 15, 2005 3:47:59 PM PST
	DHAMBY	OPEN		USERS	TEMP	HRPROFILE	May 5, 2005 8:43:27 PM PDT
	DIP	EXPIRED & LOCKED		USERS	TEMP	DEFAULT	Mar 15, 2005 3:36:04 PM PST
	DMSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:55:30 PM PST
	EXFSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:54:58 PM PST
	HR	OPEN		USERS	TEMP	DEFAULT	May 2, 2005 3:20:27 PM PDT

Select the user, and click Unlock User.



Xác thực user

- Password
- External
- Global



Account
> **Xác thực**
Privilege
Role
Profile
PW Security
Quota

Edit User: HR

Actions Create Like Go Show SQL Revert Apply

General [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Groups](#) [Switching Privileges](#) [Proxy Users](#)

Name **HR**

Profile DEFAULT

Authentication Password

* Enter Password Password

* Confirm Password External

Global

For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace USERS

Temporary Tablespace TEMP

Status ☒ Locked ☐ Unlocked

Xác thực user (Authenticating Users)

❖ **Password:** Xác thực bởi Oracle database.

- Tạo mật khẩu khi kết nối

```
CREATE USER rajesh IDENTIFIED BY welcome;
```

❖ **External:** Xác thực bởi hệ điều hành

- Không cần chỉ định user hoặc password

```
CREATE USER ops$oracle IDENTIFIED EXTERNALLY;
```

❖ **Global:** Sử dụng tùy chọn Oracle Advanced Security, chứng thực toàn cầu (xác thực mạnh)

```
CREATE USER spy_master IDENTIFIED GLOBALLY AS 'CN=spy_master, OU=tier2,  
O=security, C=US';
```


Privilege (quyền)

Account
Xác thực
> Privilege
Role
Profile
PW Security
Quota



Loại quyền:

thống: cho phép r

o tác tấ

tương

h một

liệu

hiện một số

PRIVILEGE

là gì?

v cập và thực

hành trong cơ sở

**Sự cho phép thực thi một loại lệnh SQL
hoặc cho phép truy cập vào đối tượng
của người dùng khác**

Sửa bảng EMP

Tạo session

ORACLE

Quyền hệ thống

Edit User: HR

Actions

[General](#) [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Groups](#) [Switching Privileges](#) [Proxy Users](#)

System Privilege	Admin Option
ALTER SESSION	<input type="checkbox"/>
CREATE DATABASE LINK	<input type="checkbox"/>
CREATE SEQUENCE	<input type="checkbox"/>
CREATE SESSION	<input type="checkbox"/>
CREATE SYNONYM	<input type="checkbox"/>
CREATE VIEW	<input type="checkbox"/>
UNLIMITED TABLESPACE	<input type="checkbox"/>

Database Instance: orcl.oracle.com > Users > Edit User: HR

Logged in As SYS

Modify System Privileges

Available System Privileges

- ACCESS ANY WORKSPACE
- ADMINISTER ANY SQL TUNING SET
- ADMINISTER DATABASE TRIGGER
- ADMINISTER RESOURCE MANAGER
- ADMINISTER SQL TUNING SET
- ADVISOR
- ALTER ANY CLUSTER
- ALTER ANY DIMENSION
- ALTER ANY EVALUATION CONTEXT
- ALTER ANY INDEX

Selected System Privileges

- ALTER SESSION
- CREATE DATABASE LINK
- CREATE SEQUENCE
- CREATE SESSION
- CREATE SYNONYM
- CREATE VIEW
- UNLIMITED TABLESPACE

GRANT CREATE VIEW, CREATE SESSION TO HR WITH ADMIN OPTION

SQL

Quyền hệ thống

Loại	Quyền
Database	Alter database
	Alter system
	Audit system
	Audit any
Indexs	Create any index
	Alter any index
	Drop any index
Tablespace	Create tablespaces
	Alter tablespace
	Drop tablespace
	Manage tablespace

Loại	Quyền
Table	Create table
	Create any table
	Alter any table
	Drop any table
	Comment any table
	Select any table
	Insert any table
	Update any table
	Delete any table
	Lock any table
	Flashback any table

Quyền hệ thống

Session

CREATE SESSION	Permits the grantee to connect to the database. This privilege is required for user accounts, but may be undesirable for application owner accounts.
ALTER SESSION	Permits the grantee to execute ALTER SESSION statements.
ALTER RESOURCE COST	Permits the grantee to change the way that Oracle calculates resource cost for resource restrictions in a profile
RESTRICTED SESSION	Permits the grantee to change the way that Oracle calculates resource cost for resource restrictions in a profile

Quyền đối tượng

The screenshot illustrates the steps to grant object privileges in Oracle SQL Developer. The 'Object Privileges' window is open, and the 'Table' option is selected in the 'Select Object Type' dropdown. The 'Add Table Object Privileges' window is also open, showing the 'Available Privileges' list with 'DELETE', 'SELECT', 'UPDATE', and 'INSERT' selected. The 'Selected Privileges' window shows 'SELECT'.

Database | [Setup](#) | [Preferences](#) | [Help](#) | [Logout](#)

ed.
ontrol

Object Privileges | [Quotas](#) | [Consumer Groups](#) | [Switching Privileges](#) | [Proxy Users](#)

Select Object Type: Function (Add)

- Function
- Java Class
- Java Source
- Job Classes
- Jobs
- Package
- Procedure
- Programs
- Queue
- Schedules
- Sequence
- Snapshot
- Synonym
- Table

Object Privileges | [Quotas](#) | [Consumer Groups](#) | [Switching Privileges](#) | [Proxy Users](#)

Schema: SYS | Object: DBMS_STATS

Actions: Create Like (Go) (Show S...)

Add Table Object Privileges

* Select Table Objects
OE.CUSTOMERS,OE.INVENTORIES,OE.ORDERS

(SchemaName.Table,...)
Select object and then choose privileges to assign

Available Privileges

- ALTER
- DELETE
- INDEX
- INSERT
- REFERENCES
- UPDATE

Selected Privileges

- SELECT

GRANT DELETE, SELECT, UPDATE, INSERT ON STUDENT TO HR WITH GRANT OPTION;

Quyền đối tượng

❖ Sử dụng lệnh Grant

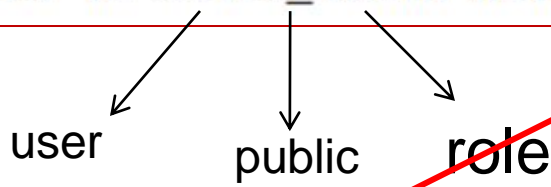
```
GRANT SELECT,INSERT,UPDATE,DELETE ON customers TO sales_manager;
```

❖ Public: là một user đặc biệt

```
GRANT SELECT ON customers TO public;
```

❖ With Grant Option: cho phép người được gán quyền có thể gán các quyền đó cho user khác

```
GRANT SELECT ON sales.customers TO sales_admin WITH GRANT OPTION;
```



Quyền đối tượng

	Table	View	Sequence	Function/ Procedure
Select	X	X	X	
Insert	X	X		
Update	X	X		
Delete	X	X		
Alter	X		X	
Debug	X	X		X
Index	X			
Reference	X	X		
Execute				X

Gỡ quyền

The screenshot shows the Oracle SQL Developer interface with the 'Object Privileges' tab selected. The table lists privileges for the 'STUDENT' object in the 'SYS' schema. The 'SELECT' privilege is selected, and the 'Delete' button is highlighted.

Select	Object Privilege	Schema	Object	Grant Option
<input type="radio"/>	EXECUTE	SYS	DBMS_STATS	<input type="checkbox"/>
<input type="radio"/>	INSERT	SYS	STUDENT	<input type="checkbox"/>
<input checked="" type="radio"/>	SELECT	SYS	STUDENT	<input type="checkbox"/>
<input type="radio"/>	UPDATE	SYS	STUDENT	<input type="checkbox"/>

```
REVOKE DELETE ON STUDENT FROM HR;
```

```
REVOKE DELETE, INSERT, UPDATE ON STUDENT FROM HR;
```

```
REVOKE ALL ON STUDENT FROM HR;
```


Cơ chế gỡ quyền

Marry tạo quyền cho Zachary

GRANT SELECT ANY TABLE
WITH ADMIN OPTION

Zachary

Zachary tạo quyền cho Rex

GRANT SELECT ANY TABLE

Rex

Xóa Zachary. Rex vẫn còn quyền

GRANT SELECT ANY TABLE

Rex

GRANT SELECT ON clients
WITH GRANT OPTION

Quyền hệ thống

GRANT SELECT ON
Marry.clients

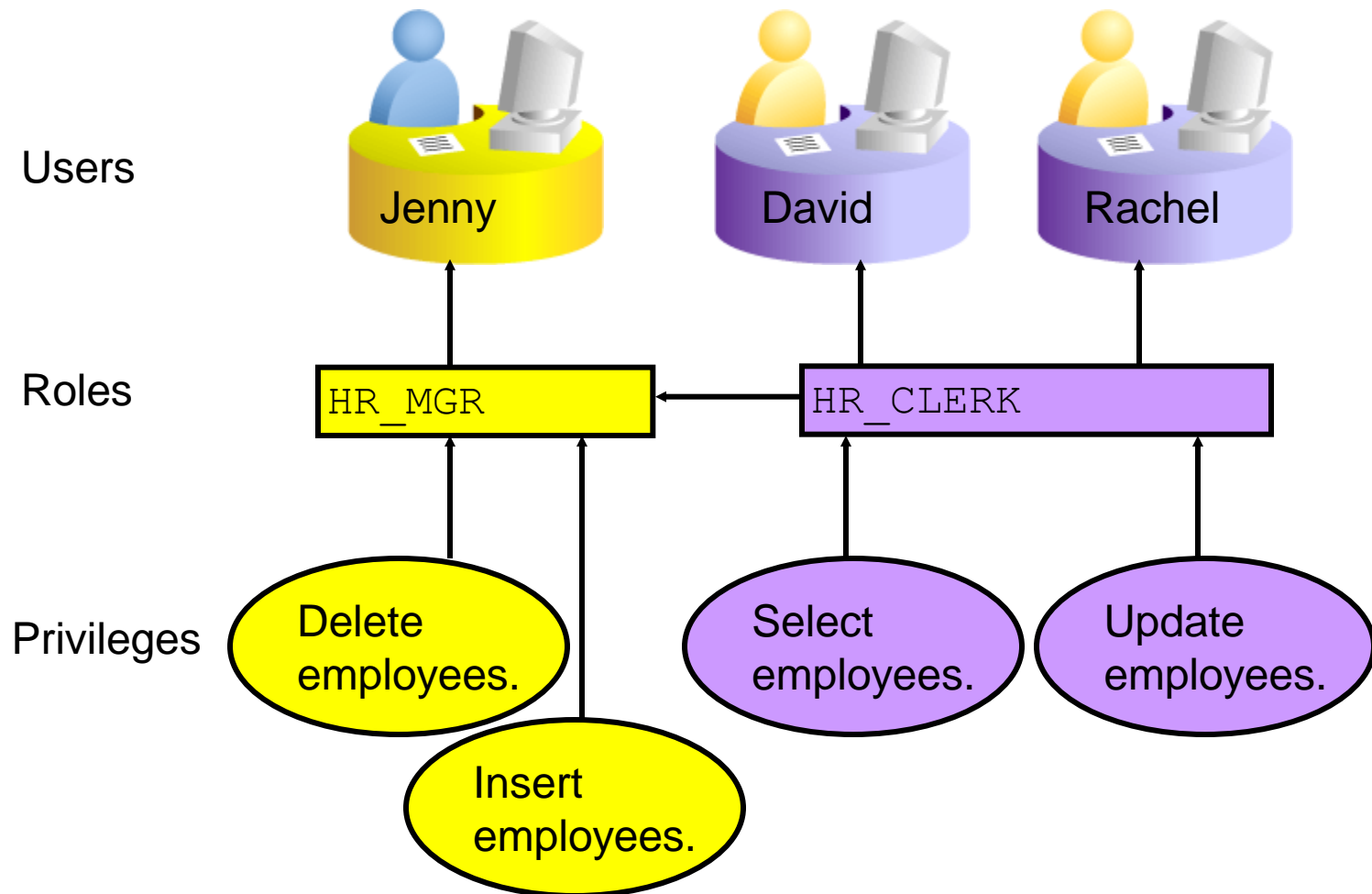
ROLE

Account
Xác thực
Privilege
> Role
Profile
PW Security
Quota

- ❖ Role là một nhóm quyền.
- ❖ Lợi ích của role:
 - Dễ dàng quản lý quyền
 - Quản lý quyền “động”
 - Bật/tắt quyền dễ dàng



Privilege, Role và user



Quản lý role

❖ Tạo và gán quyền cho role

```
CREATE ROLE Manager;  
GRANT CREATE SESSION, CREATE TABLE TO Manager WITH ADMIN OPTION;
```

❖ Gỡ quyền của role

```
REVOKE CREATE SESSION FROM Manager;
```

❖ Bật/tắt role

```
SET ROLE Manager;
```

```
SET ROLE ALL EXCEPT Manager;
```

```
SET ROLE NONE;
```

❖ Gán role cho user

```
Grant Manager to Gues;
```

❖ Xóa role

```
DROP ROLE Manager;
```

Quản lý role (sử dụng EM)

❖ Tạo role

Database Instance: [db1.abc.vn](#) > [Roles](#) > Create Role

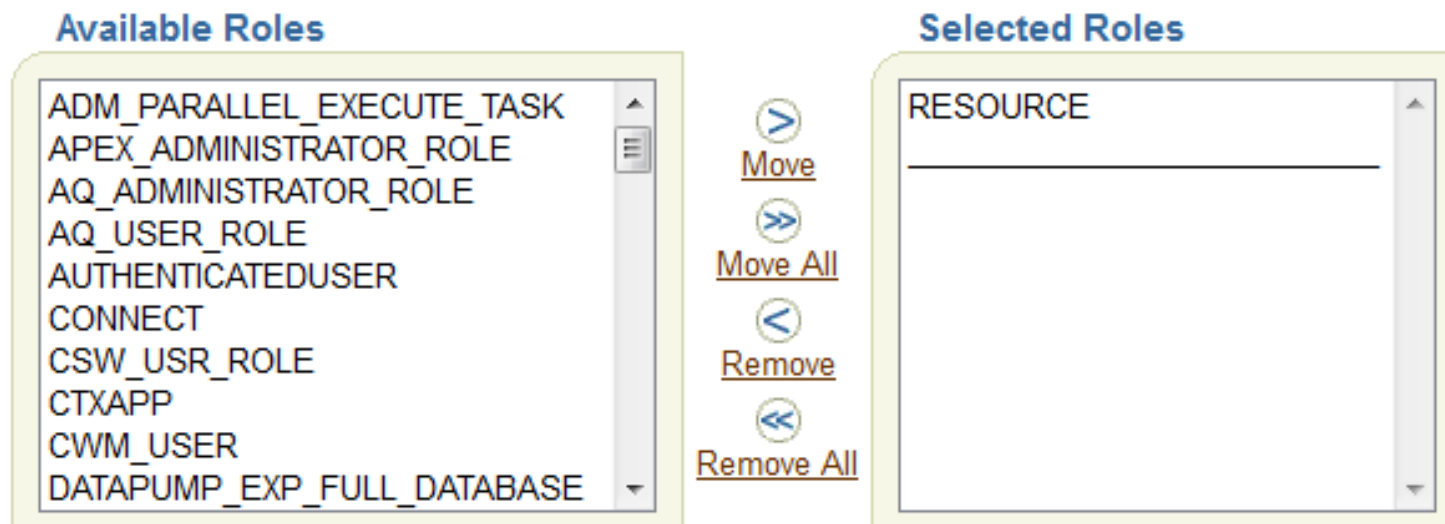
Create Role

General	Roles	System Privileges	Object Privileges	Consumer Groups	Switching Privileges
* Name <input type="text"/>					
Authentication	None	Authentication.			
<div><div>None</div><div>Password</div><div>External</div><div>Global</div></div>					

Quản lý role (sử dụng EM)...

❖ Gán role cho user

Modify Roles



Available Roles

- ADM_PARALLEL_EXECUTE_TASK
- APEX_ADMINISTRATOR_ROLE
- AQ_ADMINISTRATOR_ROLE
- AQ_USER_ROLE
- AUTHENTICATEDUSER
- CONNECT
- CSW_USR_ROLE
- CTXAPP
- CWM_USER
- DATAPUMP_EXP_FULL_DATABASE

Selected Roles

- RESOURCE

Move
Move All
Remove
Remove All

Account mặc định

❖ SYS

- Có role DBA
- Có toàn quyền
- Được phép tắt/bật dịch vụ
- Quản lý data dictionary
- Quản lý Automatic Workload Repository (AWR)

❖ SYSTEM

- Có role DBA
- Không có toàn quyền như SYS

Account mặc định

SYS	The SYS user owns all the internal Oracle tables that constitute the data dictionary. Normally, you should not perform any actions as the SYS user and should ensure that this account is locked down. Also, don't manually modify the underlying objects owned by the SYS user.
SYSTEM	SYSTEM is an additional support user that contains additional administrative tables and views. This account should also be locked down to prevent unauthorized use of it. The user SYSTEM has access to all objects in the database
DBSNMP	DBSNMP is a login used by the Enterprise Manager facility to monitor and gather performance statistics about the database
SYSMAN	SYSMAN is the equivalent of the SYS user for the Enterprise Manager facility. This Enterprise Manager administrator can create and modify other Enterprise Manager administrator accounts, as well as administer the database instance itself.

Các role mặc định

CONNECT	CREATE SESSION, Enables a user to connect to the database. Grant this role to any user or application that needs database access
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	It grants all system privileges, but does not include the privileges to start up or shut down the database. It is by default granted to user SYSTEM.
SELECT_ CATALOG_ ROLE	Không có quyền hệ thống nhưng có quyền HS_ADMIN_ROLE và hơn 1.700 quyền đối tượng đối tới data dictionary

Role mặc định

CONNECT	
	ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW

Các role mặc định

- ❖ SYSDBA is the highest system privilege (role) in oracle.
- ❖ SYSOPER system privilege (role) is limited than SYSDBA

SYSDBA	SYSOPER
<ul style="list-style-type: none">• Perform STARTUP and SHUTDOWN operations• ALTER DATABASE: open, mount, back up, or change character set• CREATE DATABASE• DROP DATABASE• CREATE SPFILE• ALTER DATABASE ARCHIVELOG• ALTER DATABASE RECOVER• Includes the RESTRICTED SESSION privilege• Allows a user to connect as user SYS.	<ul style="list-style-type: none">• Perform STARTUP and SHUTDOWN operations• CREATE SPFILE• ALTER DATABASE OPEN/MOUNT/BACKUP• ALTER DATABASE ARCHIVELOG• ALTER DATABASE RECOVER (Complete recovery only. Any form of incomplete recovery, such as UNTIL TIME CHANGE CANCEL CONTROLFILE requires connecting as SYSDBA.)• Includes the RESTRICTED SESSION privilege• Allows a user to perform basic operational tasks, but without the ability to look at user data.

Profile và user

Account
Xác thực
Privilege
Role
> Profile
PW Security
Quota

❖ Tại một thời điểm, mỗi user chỉ được gán **DUY NHẤT** một profile

❖ Profile

- Quản lý tài nguyên được phép dùng của user
- Quản lý trạng thái và ràng buộc về mật khẩu

Database Instance: orcl1 > Profiles > Create Profile

Create Profile

Show SQL Cancel OK

General Password

★ Name

Details

CPU/Session (Sec./100)

CPU/Call (Sec./100)

Connect Time (Minutes)

Idle Time (Minutes)

Database Services

Concurrent Sessions (Per User)

Reads/Session (Blocks)

Reads/Call (Blocks)

Private SGA (KBytes)

Composite Limit (Service Units)

Bảo mật mật khẩu



Chú ý: Không khóa và đặt thời gian hết hiệu lực đối với account SYS, SYSMAN, and DBSNMP.

Tạo mật khẩu cho profile

Create Profile

Show SQLCancelOK

GeneralPassword

Password

Expire in (days)90

Lock (days past expiration)10

History

Number of passwords to keepUNLIMITED

Number of days to keep for120

Complexity

Complexity functionVERIFY_FUNCTION

Failed Login

Number of failed login attempts to lock after3

Number of days to lock for5/1440

VERIFY_FUNCTION

❖ Oracle cung cấp hàm kiểm tra độ tin cậy của mật khẩu – *verify_function*

- Tối thiểu 4 kí tự
- Không trùng với username
- Có ít nhất 1 chữ cái, 1 chữ số và 1 kí tự đặc biệt
- Khác mật khẩu trước ít nhất 3 kí tự

❖ Hàm này không có sẵn, muốn sử dụng thì chạy script:

<oracle_home>/rdbms/admin/*utlpwdmg.sql*



Thiết lập hạn mức cho user

Account
Xác thực
Privilege
Role
Profile
PW Security
> Quota

- ❖ Hạn mức là dung lượng user được phép sử dụng trong 1 tablespace
- ❖ Có 2 loại hạn mức
 - Giá trị xác định (tính bằng MB hoặc KB)
 - Không có hạn mức

Edit User: GUES

Actions Create Like Go Show SQL Revert Apply

[General](#) [Roles](#) [System Privileges](#) [Object Privileges](#) **Quotas** [Consumer Group Privileges](#) [Proxy Users](#)

Tablespace	Quota	Value	Unit
EXAMPLE	None	0	MBytes
SYSAUX	None	0	MBytes
SYSTEM	Unlimited	0	MBytes
TEMP	Value	0	MBytes
UNDOTBS1	None	0	MBytes
USERS (Default)	None	0	MBytes

[General](#) [Roles](#) [System Privileges](#) [Object Privileges](#) **Quotas** [Consumer Group Privileges](#) [Proxy Users](#)

ORACLE

