데이터베이스 롤 권한 제어

롤의 정의

❖ 롤(ROLE)

- ㅇ 여러 개의 권한을 하나의 역할에 매핑시킨 것
- ㅇ 개별 권한을 하나씩 배정 하는 것보다 역할을 배정하여 권한을 부여할 수 있음

❖ 롤의 종류

- o CONNECT 롤
 - 데이터베이스 접속 등 가장 대표적인 8가지 권한을 묶어 놓음.
 - ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW
- o RESOURCE 롤
 - 사용자 객체(테이블, 뷰, 인덱스) 생성 권한을 묶어 놓음.
 - CREATE CLUSTER, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER
- o DBA 롤
 - 데이터베이스, 사용자 관리에 필요한 권한을 묶어 놓음

롤의 정의

❖ 시스템 관리자 계정에서 롤 부여

GRANT CONNECT, RESOURCE TO WEB;

❖ 사용자 롤 정의

ㅇ 형식

CREATE ROLE role_name;
GRANT privilege_name TO role_name;

❖ 작업 순서

① 롤을 생성합니다.(데이터베이스 관리자)

② 롤에 권한을 부여합니다. (데이터베이스 관리자 혹은 특정 사용자)

③ 사용자에 롤을 부여합니다.(데이터베이스 관리자)

❖ 작업순서

o 롤 생성(DBA)

CREATE ROLE ROLE_NAME

o 롤에 권한 부여(DBA 또는 객체 소유자)

GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO ROLE_NAME

또는

GRANT OBJECT_PRIV TO ROLE_NAME

ㅇ 사용자에게 롤 부여(DBA)

GRANT ROLE_NAME TO USER_NAME;

❖ 롤 생성하여 시스템 권한 할당하기

o SYS 계정으로 작업

```
CREATE ROLE MROLE;

GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO MROLE;

CREATE USER USER01 IDENTIFIED BY USER01;

GRANT MROLE TO USER01;
```

❖ 롤을 생성하여 객체 권한 할당하기

o SYS 계정으로

CREATE ROLE MROLE2;

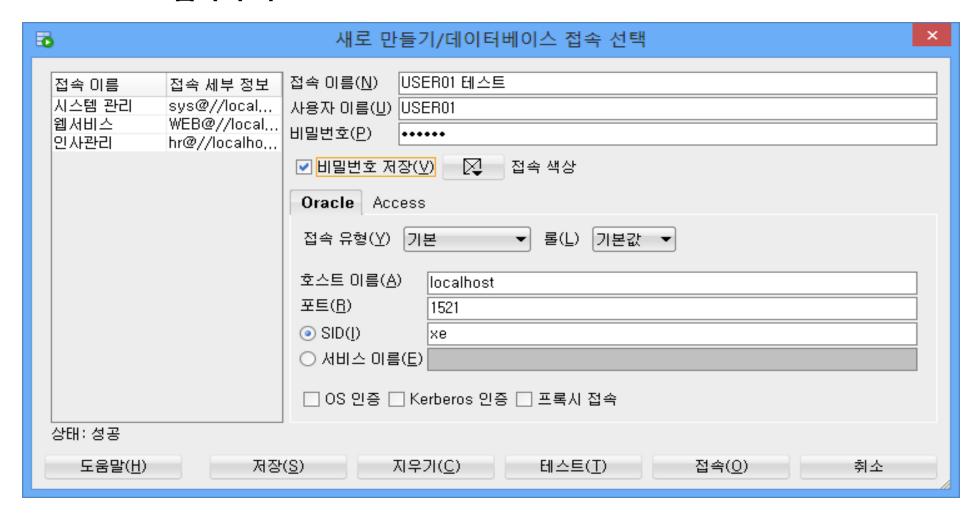
o HR 계정으로

GRANT SELECT ON EMPLOYEES TO MROLE2; GRANT SELECT ON DEPARTMENTS TO MROLE2;

o SYS 계정으로

GRANT MROLE2 TO USER01;

❖ USER01 접속 추가



❖ USER01 계정

```
SELECT * FROM HR.EMPLOYEES;
SELECT * FROM HR.DEPARTMENTS;
```

롤 회수와 롤 제거하기

❖ 롤 회수

ㅇ 형식

REVOKE ROLE role_name FROM user_name;

❖ 롤 제거

ㅇ 형식

DROP ROLE role_name;