MYONGJI UNIVERSITY

Authorization

Privileges & Roles

사용자 관리

- Syntax
  - 사용자 생성: CREATE USER *user* IDENTIFIED BY *passwd*;
  - 비밀번호 변경: ALTER USER *user* IDENTIFIED BY *passwd*;
  - 사용자 삭제: DROP USER *user* [CASCADE];
- 주의
  - 일반적으로 DBA의 일
  - 사용자를 생성하려면 CREATE USER 권한 필요
  - 생성된 사용자가 Login하려면 CREATE SESSION 권한 필요
  - 일반적으로 CONNECT, RESOURCE의 ROLE을 부여하면 일반사용자 역할을 할 수 있음

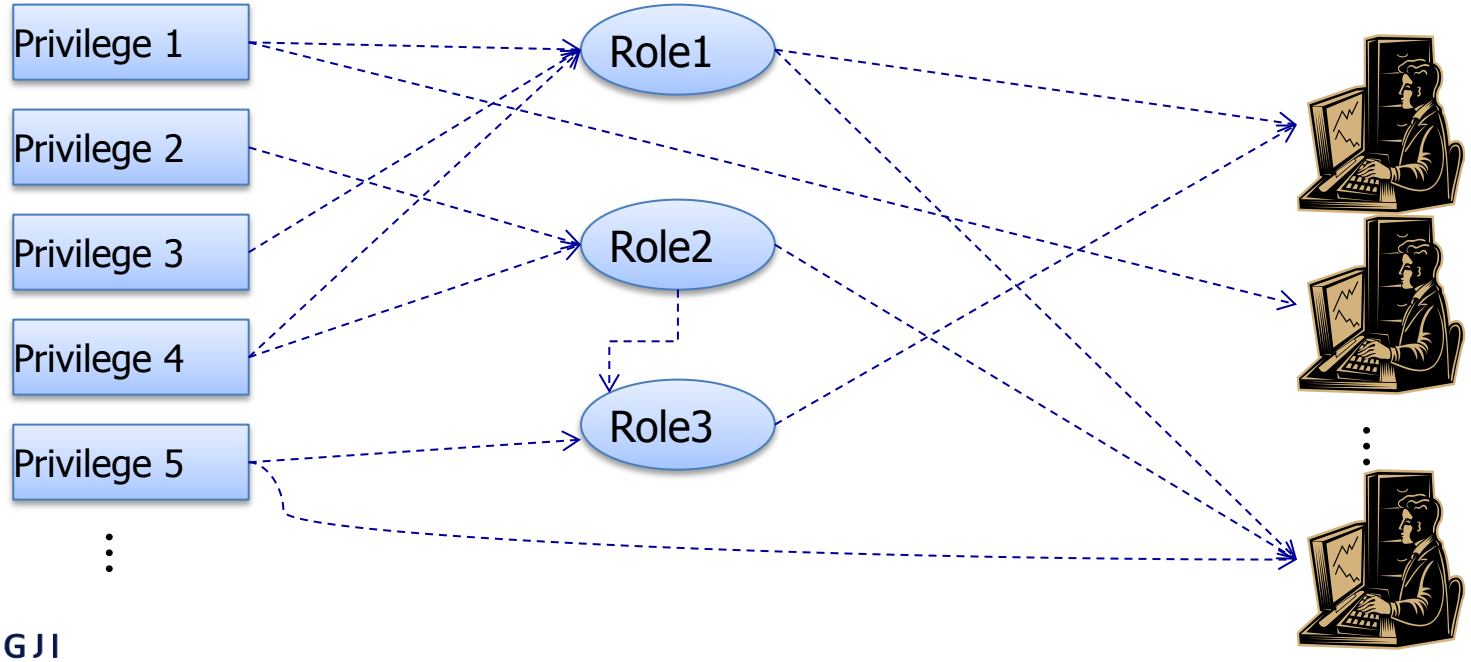
사용자 정보 확인

- 관련 Dictionary
  - USER_USERS: 현재 사용자 관련 정보
  - ALL_USERS: DB의 모든 사용자 정보
  - DBA_USERS: DB의 모든 사용자의 상세 정보 (DBA만 사용 가능)

```
SELECT * FROM USER_USERS;
```

권한(Privilege)과 롤(Role)

- 권한:
  - 사용자가 특정 SQL문을 실행하거나 특정 정보에 접근할 수 있는 권리
  - 종류: 시스템 권한(80여개) & 스키마 객체 권한
- 롤:
  - 권한을 쉽게 관리하기 위하여 특정한 종류별로 묶어놓은 그룹



GRANT / REVOKE

- 권한/롤을 부여하거나 회수
- 시스템 권한: 관리자로 수행 (ADMIN OPTION/GRANT ANY PRIVILEGE 권한)

```
GRANT create session TO user1;
```

```
REVOKE create session FROM user1;
```

- 스키마객체 권한

```
GRANT select ON emp TO user1;
```

```
REVOKE select ON emp FROM user1;
```

- WITH GRANT OPTION
  - 해당 권한을 받은 사람이 다시 제3자에게 권한을 부여할 수 있도록 하는 옵션
  - 권한을 REVOKE 하면 그 사람이 준 권한들도 함께 회수됨

```
GRANT select ON emp TO user2
WITH GRANT OPTION;
```

ROLE

- Role을 생성한 후 Role에 Privilege를 Grant하여 Role관리
  - 주로 DBA작업

```
CREATE ROLE reviewer;
GRANT select any table TO reviewer;
GRANT create session, resource TO reviewer;
```

- 특정 Role을 사용자에게 Grant / Revoke

```
GRANT reviewer TO user3;
```

권한 확인

- 관련 Dictionary
  - ROLE_SYS_PRIVS: System privileges granted to roles
  - ROLE_TAB_PRIVS: Table privileges granted to roles
  - USER_ROLE_PRIVS: Roles accessible by the user
  - USER_TAB_PRIVS_MADE: Object privileges granted on the user's object
  - USER_TAB_PRIVS_RECD: Object privileges granted to the user
  - USER_COL_PRIVS_MADE: Object privileges granted on the columns of the user's object
  - USER_COL_PRIVS_RECD: Object privileges granted to the user on specific columns
  - USER_SYS_PRIVS: Lists system privileges granted to the user

```
SELECT * FROM USER_ROLE_PRIVS;
SELECT * FROM ROLE_SYS_PRIVS;
```