**[ VII-1 ] 사용자 관리 (DCL)**

**데이터베이스보안을 위한 권한, 사용자 생성, 권한부여, 객체권한**

1. 데이터베이스 보안을 위한 권한
   * 데이터베이스관리자가 가지고 있는 시스템 권한
     + CREATE USER : 사용자 생성 권한
     + DROP USER : 사용자를 삭제하는 권한
   * 시스템관리자가 사용자에게 부여하는 권한
     + CREATE SESSION : 데이터베이스에 접속할 수 있는 권한
     + CREATE TABLE : 테이블을 생성할 수 있는 권한
     + CREATE VIEW
     + CREATE SEQUENCE
2. 사용자 생성과 삭제하기
   * 사용자 계정 생성 : CREATE USER user\_name IDENTIFIED BY password;
   * 사용자 계정 삭제 : DROP USER user\_name CASCADE;
   * 예제
     + 사용자계정 scott을 삭제
       - DROP USER scott CASCADE;
     + 사용자계정 scott을 비밀번호 tiger로 생성

* CREATE USER scott IDENTIFIED BY tiger;
  + - 사용자계정 kim을 비밀번호 1111로 생성
* CREATE USER scott IDENTIFIED BY tiger;
  + - 사용자계정 kim의 비밀번호 변경
* ALTER USER kim IDENTIFIED BY tiger;

1. 권한 부여
   * 문법 : GRANT 권한명 또는 롤명 TO user\_name;
   * user\_name 대신 PUBLIC을 쓰면 DB내의 모든 계정을 의미.
   * 권한을 부여하지 않고 사용자계정만 생성하면 접속도 불가
   * 예제
     + GRANT CREATE SESSION TO SCOTT;
     + SHOW USER;
     + SCOTT으로 접속한 후, @d:/mega\_IT/demo.sql; 수행후 SELECT \* FROM TAB; 실행해도 테이블생성 안 됨.
   * 롤생성 예제
     + CREATE ROLE ROLLEX1;
     + GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO ROLLEX1;
     + GRANT ROLEX1 TO SCOTT;
     + 위의 명령 수행 후 @d:/mega\_IT/demo.sql; 수행하면 SELECT \* FROM TAB;을 통해 테이블이 생성된 것을 볼 수 있다.
     + GRANT DBA TO SCOTT;
2. 객체 권한
   * 문법 : GRANT 권한명 또는 ALL ON 객체명 TO user\_name;

|  |  |  |  |
| --- | --- | --- | --- |
| 권 한 | TABLE | VIEW | SEQUENCE |
| ALTER | v |  | v |
| DELETE | v | v |  |
| EXECUTE |  |  |  |
| INDEX | v |  |  |
| INSERT | v | v |  |
| REFERENCES | v |  |  |
| SELECT | v | v | v |
| UPDATE | v | v |  |

* + 예시

CREATE OR REPLACE VIEW EMPv1

AS SELECT \* FROM EMP WHERE DEPTNO=10 WITH READ ONLY;

CREATE OR REPLACE VIEW EMPv2

AS SELECT EMPNO, ENAME, SAL, COMM FROM EMP;

* + - GRANT SELECT ON SCOTT.EMPv1 TO KIM;
    - GRANT SELECT ON SCOTT.EMPv2 TO KIM;
    - GRANT INSERT ON SCOTT.EMPv2 TO KIM;
    - GRANT UPDATE(SAL, COMM) ON SCOTT1.EMPv2 TO KIM;
    - GRANT ALL ON SALGRADE TO KIM;
  + 롤생성 예
    - CREATE ROLE ROLLEX2;
    - GRANT ALL ON SCOTT.EMP TO ROLLEX2;
    - GRANT ALL ON SCOTT.DEPT TO ROLLEX2;
    - GRANT ROLLEX2 TO KIM;

1. 권한 박탈
   * 문법 : REVOKE 권한명 또는 ALL ON 객체명 FROM user\_name;

REVOKE 권한명 FROM user\_name

* + 예시
    - REVOKE SELECT ON SCOTT.EMPv1 FROM KIM;
    - REVOKE SELECT ON SCOTT.EMPv2 FROM KIM;
    - REVOKE UPDATE(SAL, COMM) ON SCOTT1.EMPv2 FROM KIM;
    - REVOKE ALL ON SALGRADE FROM KIM;
    - REVOKE DBA FROM SCOTT;

<요점>

--1. 계정만드는 명령어 CREATE USER 계정 IDENTIFIED BY 비번;

--2. 권한 부여 GRANT 권한 TO 계정;

--3. 권한 박탈 REVOKE 권한 FROM 계정;

--4. 계정 삭제 DROP USER 계정 CASCADE; (계정 삭제는 로그아웃일 경우만 가능)

CREATE USER KIM IDENTIFIED BY KIM;

ALTER USER KIM IDENTIFIED BY tiger;

grant CREATE SESSION TO KIM;

SHOW USER ;

CREATE ROLE ROLLEX1;

GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO ROLLEX1;

GRANT ROLLEX1 TO KIM;

GRANT SELECT ON EMPv1 TO KIM;

GRANT all ON SALGRADE TO KIM;

select \* from SALGRADE;

delete from salgrade where grade=6;

commit;

revoke all on salgrade from KIM;

drop user kim cascade;