사용자 관리

업무 분할과 효율, 보안을 고려하여 업무에 따라 여러 사용자들을 나누는 것을 의미한다. 오라클 데이터 베이스는 테이블 · 인덱스 · 뷰 등 여러 객체가 사용자별로 생성되므로 업무별 사용자를 생성한 후에 각 사용자 업무에 맞는 데이터 구조를 만들어 관리하는 방식을 사용할 수 있다. 반대로 대표 사용자를 통해 업무에 맞는 데이터 구조를 먼저 정의한 뒤에 사용할 수 있는 데이터 영역을 각 사용자에게 지정해 줄 수도 있다.

■ 사용자(user)와 스키마(schema)

데이터베이스에서 데이터 간 관계, 데이터 구조, 제약 조건 등 데이터를 저장 및 관리하기 위해 정의한 데이터베이스 구조의 범위를 스키마를 통해 그룹 단위로 분류한다. 오라클에서는 스키마와 사용자를 구별하지 않고 사용하기도 한다.

- **user** : 데이터 베이스에 접속하여 데이터를 관리하는 계정
  데이터를 사용 및 관리하기 위해 오라클 데이터베이스에 접속하는 개체를 의미한다.
  ex) scott 계정
- **schema** : 사용자(user)와 연결된 객체
  ex) scott 이 생성한 테이블·뷰·제약조건·인덱스·시퀀스·동의어 등 계정에서 만든 모든 객체

■ 사용자 생성

```
CREATE USER 사용자이름(필수)
IDENTIFIED BY 패스워드(필수)
DEFAULT TABLESPACE 테이블 스페이스 이름(선택)
TEMPORARY TABLESPACE 테이블 스페이스(그룹) 이름(선택)
QUOTA 테이블 스페이스크기 ON 테이블 스페이스 이름(선택)
PROFILE 프로파일 이름(선택)
PASSWORD EXPIRE(선택)
ACCOUNT [LOCK / UNLOCK](선택);
```

사용자를 생성할 때는 CREATE USER 문을 사용한다.
옵션이 여러 가지 있지만 기본적으로 사용자 이름과 패스워드만 지정해주면 생성 가능하다.

```
-- SYSTEM 사용자로 접속 후 사용자 생성하기(SQLPlus)
$ SQLPLUS SYSTEM/oracle

CREATE USER ORCLSTUDY
IDENTIFIED BY ORACLE;
```

사용자 생성은 일반적으로 데이터 관리 권한을 가진 사용자가 권한을 갖고 있다.(오라클에서는 SYS , SYSTEM) scott 계정에서는 사용자를 생성할 권한이 없기 때문에 SQLPlus에서 SYSTEM 계정으로 로그인 한 뒤에 사용자를 생성해야 된다.

```
SQL> CONN ORCLSTUDY/ORACLE
ERROR:
ORA-01045: user ORCLSTUDY lacks CREATE SESSION privilege; logon denied


경고: 이제는 ORACLE에 연결되어 있지 않습니다.
```

사용자 생성만 하고 오라클에 접속했을 경우

- CONN (CONNECT) : SQLPlus로 DB에 접속한 상태에서 계정을 변경하는 명령어
- SHOW USER : 현재 접속한 계정명을 확인하는 명령어

그러나 CONN 명령어를 사용해 새로 생성한 ORCLSTUDY 사용자로 접속하면 접속되지 않는다.
이는 **사용자가 생성되긴 했지만 데이터베이스 연결을 위한 권한(CREATE SESSION 권한)은 부여받지 못했기 때문이다.**

```
-- SQLPlus에서 SYSTEM 사용자로 접속 후 ORCLSTUDY 사용자에게 권한 부여
$ SQLPLUS SYSTEM/oracle

GRANT CREATE SESSION TO ORCLSTUDY;
```

GRANT 명령어로 CREATE SESSION 권한을 주어야 데이터베이스 접속이 가능하다.

■ 사용자 정보 조회

```
SELECT * FROM ALL_USERS
WHERE USERNAME = 'ORCLSTUDY';
```

```
SELECT * FROM DBA_USERS
WHERE USERNAME = 'ORCLSTUDY';
```

```
SELECT * FROM DBA_OBJECTS
WHERE OWNER = 'ORCLSTUDY';
```

사용자, 또는 사용자 소유 객체 정보를 얻기 위해 위와 같이 데이터 사전을 사용할 수 있다.

■ 사용자 정보 변경

```
-- 사용자 정보(패스워드) 변경 (SYSTEM 계정에서 실행)
ALTER USER ORCLSTUDY
IDENTIFIED BY ORCL;
```

사용자 정보를 변경할 때는 ALTER USER 문을 사용한다.
사용자 정보 변경도 마찬가지로 SYS 나 SYSTEM 과 같은 관리계정에서 수행해야 한다.

■ 사용자 삭제

```
DROP USER ORCLSTUDY;


-- CASCADE 옵션을 사용하면 사용자와 객체 모두 삭제할 수 있다.
DROP USER ORCLSTUDY CASCADE;
```

사용자를 삭제할 때는 DROP USER 문을 사용한다. CASCADE 옵션을 사용하면 사용자와 객체를 모두 삭제할 수 있다.
삭제하려는 사용자가 다른 곳에서 접속하고 있다면 삭제되지 않으니 주의한다.

권한(Privilege) 관리

데이터 베이스에서는 접속 사용자에 따라 접근할 수 있는 데이터 영역과 권한을 지정해 줄 수 있다. 오라클에서는 권한을 시스템 권한(system privilege)과 객체 권한(object privilege)으로 분류한다.

1. 시스템 권한(System Privilege)

시스템 권한(system privilege)은 데이터베이스 관리 권한이 있는 사용자가 부여할 수 있는 권한이며, 사용자 생성과 정보 수정 및 삭제, 데이터베이스 접근, 오라클 데이터베이스의 여러 자원과 객체 생성 및 관리 등의 권한을 포함한다. 아래 표는 시스템 권한의 일부이고 ANY **키워드가 들어있는 권한은 소유자에 상관없이 사용 가능한 권한을 의미한다.**

시스템 권한 분류	시스템 권한	설 명
USER(사용자)	CREATE USER	사용자 생성 권한
	ALTER USER	생성된 사용자의 정보 수정 권한
	DROP USER	생성된 사용자의 삭제 권한
SESSION(접속)	CREATE SESSION	데이터베이스 접속 권한
	ALTER SESSION	데이터베이스 접속 상태에서 환경 값 변경 권한
TABLE(테이블)	CREATE TABLE	자신의 테이블 생성 권한
	CREATE ANY TABLE	임의의 스키마 소유 테이블 생성 권한
	ALTER ANY TABLE	임의의 스키마 소유 테이블 수정 권한
	DROP ANY TABLE	임의의 스키마 소유 테이블 삭제 권한
	INSERT ANY TABLE	임의의 스키마 소유 테이블 데이터 삽입 권한
	UPDATE ANY TABLE	임의의 스키마 소유 테이블 데이터 수정 권한
	DELETE ANY TABLE	임의의 스키마 소유 테이블 데이터 삭제 권한
	SELECT ANY TABLE	임의의 스키마 소유 테이블 데이터 조회 권한
INDEX(인덱스)	CREATE ANY INDEX	임의의 스키마 소유 테이블의 인덱스 생성 권한
	ALTER ANY INDEX	임의의 스키마 소유 테이블의 인덱스 수정 권한
	DROP ANY INDEX	임의의 스키마 소유 테이블의 인덱스 삭제 권한

VIEW(뷰)	(생략)	뷰와 관련된 여러 권한
SEQUENCE(시퀀스)	(생략)	시퀀스와 관련된 여러 권한
SYNONYM(동의어)	(생략)	동의어와 관련된 여러 권한
PROFILE(프로파일)	(생략)	사용자 접속 조건 지정과 관련된 여러 권한
ROLE(롤)	(생략)	권한을 묶은 그룹과 관련된 여러 권한

■ 시스템 권한 부여

```
GRANT [시스템 권한] TO [사용자 이름/롤(Role)이름/PUBLIC]
[WITH ADMIN OPTION];
```

- **[시스템 권한]**(필수) : 오라클 데이터베이스에서 제공하는 시스템 권한을 지정
  한 번에 여러 종류의 권한을 부여하려면 쉼표(,)로 구분하여 권한 이름을 여러 개 명시하면 된다.
- **[사용자 이름/롤(Role) 이름/** PUBLIC **]**(필수)
  : 권한을 부여하려는 대상 지정, 여러 사용자나 롤에 적용할 경우 마찬가지로 쉼표(,)로 구분
  PUBLIC **은 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여한다는 의미**
- **[WITH ADMIN OPTION]**(선택)
  : 현재 GRANT 문을 통해 부여받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여받는다.
  현재 사용자가 권한이 사라져도, 권한을 재부여한 다른 사용자의 권한은 유지된다.

```
-- ex) 권한관리 실습
-- 1) SYSTEM 계정으로 접속하여 사용자 ORCLSTUDY 생성(SQLPlus)
$ SQLPLUS SYSTEM/oracle

CREATE USER ORCLSTUDY
IDENTIFIED BY ORACLE;


-- 2) 사용자 권한부여
GRANT RESOURCE, CREATE SESSION, CREATE TABLE TO ORCLSTUDY;
```

RESOURCE 는 오라클 데이터 베이스에서 제공하는 롤(Role)중 하나이다. (롤은 여러 권한을 하나의 이름으로 묶어 권한 관련 작업을 간편하게 하려고 사용한다.) RESOURCE 를 지정하지 않으면 사용자에게 테이블 생성 권한을 부여해도 CREATE 문으로 테이블을 생성할 수 없거나 테이블이 생성되더라도 INSERT 문을 사용하면 ORA-01950 : 테이블 스페이스 USERS 권한이 없다 는 오류가 발생하기도 한다.

테이블 스페이스는 테이블이 저장되는 공간을 의미하며 따로 지정하지 않으면 기본 테이블 스페이스 USERS 가 할당된다. RESOURCE 롤에는 사용자를 생성할 때 사용 테이블 스페이스의 영역을 무제한 사용 가능(UNLIMITED TABLESPACE)하게 해 주는 권한이 포함되어 있기 때문에 RESOURCE 롤을 GRANT 문에 추가하면 별 문제 없이 사용자가 테이블을 생성하고 신규 데이터를 저장할 수 있다. UNLIMITED TABLESPACE 권한은 엄밀한 관리에 필요한 경우에는 적절하지 않아 사용자를 생성 및 수정할 때 QUOTA 절로 사용 영역에 제한을 두기도 한다. 이러한 이유로 오라클 데이터베이스 12C버전에서는 RESOURCE 롤에 UNLIMITED TABLESPACE 권한을 부여하지 않는다.

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> CREATE TABLE TEMP1(
  2     COL1 VARCHAR2(20),
  3     COL2 VARCHAR2(20)
  4  );

테이블이 생성되었습니다.

SQL> INSERT INTO TEMP1 VALUES ('USER', 'GRANT_TEST');

1 개의 행이 만들어졌습니다.

SQL> SELECT * FROM TEMP1;

COL1                 COL2
-------------------- --------------------
USER                 GRANT_TEST
```

권한 부여 결과

권한 부여를 하면 ORCLSTUDY 사용자로 데이터베이스 접속과 테이블 생성이 가능하다.
또한 ORCLSTUDY 소유 테이블을 생성했기 때문에 INSERT , SELECT 문을 사용할 수 있다.

■ 시스템 권한 취소

```
REVOKE [시스템 권한] FROM [사용자 이름/롤(Role)이름/PUBLIC];


-- ex) ORCLSTUDY 사용자의 권한 삭제(SQLPlus)
CONN SYSTEM/oracle
REVOKE RESOURCE, CREATE TABLE FROM ORCLSTUDY;
```

REVOKE 명령어를 사용하면 GRANT 명령어로 부여했던 권한을 취소할 수 있다.
위의 예시는 REVOKE 문을 사용하여 ORCLSTUDY 사용자의 RESOURCE , CREATE TABLE 권한을 취소하는 것이다.

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> CREATE TABLE TEMP2(
  2      COL1 VARCHAR2(20),
  3      COL2 VARCHAR2(20)
  4  );
CREATE TABLE TEMP2(
*
1행에 오류:
ORA-01031: 권한이 불충분합니다
```

권한 취소 결과

권한이 취소된 ORCLSTUDY 사용자는 더 이상 테이블을 생성할 수 없다.

2. 객체 권한(Object Privilege)

객체 권한(object privilege)은 특정 사용자가 생성한 테이블·인덱스·뷰·시퀀스 등과 관련된 권한이다. 아래의 표는 주로 사용하는 객체 권한 중 일부이다.
ex) SCOTT 소유 테이블에 ORCLSTUDY 사용자가 SELECT 나 INSERT 등의 작업이 가능하도록 허용

객체 권한 분류	객체 권한	설 명
TABLE(테이블)	ALTER	테이블 변경 권한
	DELETE	테이블 데이터 삭제 권한
	INDEX	테이블 인덱스 생성 권한
	INSERT	테이블 데이터 삽입 권한
	REFERENCES	참조 데이터 생성 권한
	SELECT	테이블 조회 권한
	UPDATE	테이블 데이터 수정 권한
VIEW(뷰)	DELETE	뷰 데이터 삭제 권한
	INSERT	뷰 데이터 삽입 권한
	REFERENCES	참조 데이터 생성 권한
	SELECT	뷰 조회 권한
	UPDATE	뷰 데이터 수정 권한
SEQUENCE(시퀀스)	ALTER	시퀀스 수정 권한
	SELECT	시퀀스의 CURRVAL 과 NEXTVAL 사용 권한
PROCEDURE(프로시저)	(생략)	프로시저 관련 권한
FUNCTION(함수)	(생략)	함수 관련 권한
PACKAGE(패키지)	(생략)	패키지 관련 권한
이하 생략(오라클 공식 문서 참고)		

■ 객체 권한 부여

```
GRANT [객체 권한/ALL PRIVILEGES]
  ON [스키마.객체 이름]
  TO [사용자 이름/롤(Role)이름/PUBLIC]
  [WITH GRANT OPTION];
```

- **[객체 권한/** ALL PRIVILEGES **]**(필수)
  : 객체 권한 지정. 한 번에 여러 종류의 권한을 부여하려면 쉼표(,)로 구분하여 권한을 여러 개 명시해주면 된다.
  ALL PRIVILEGES 로하면 객체의 모든 권한을 부여한다.
- **[스키마.객체 이름]** (필수) : 권한을 부여할 객체를 명시
- **[사용자 이름/롤(Role) 이름/** PUBLIC **]**(필수) : 권한을 부여하려는 대상.
  사용자 이름이나 롤(Role)을 지정할 수 있다. 마찬가지로 여러 사용자나 롤에 적용할 경우 쉼표(,)로 구분한다.
  PUBLIC 으로 하면 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여한다.

- **WITH GRANT OPTION**(선택)
  : 현재 GRANT 문을 통해 부여받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여한다.
  현재 권한을 부여받은 사용자의 권한이 사라지면, 다른 사용자에게 재 부여된 권한도 함께 사라진다.

```
-- ex 1) 객체 권한 부여 예시 (SQLPlus)
-- 1) SCOTT 계정으로 접속
CONN SCOTT/tiger

-- 2) SCOTT 소유의 TEMP 테이블 생성
CREATE TABLE TEMP(
    COL1 VARCHAR2(20),
    COL2 VARCHAR2(20)
);

-- 3) ORCLSTUDY 사용자에게 TEMP테이블의 SELECT와 INSERT권한 부여
GRANT SELECT, INSERT ON TEMP
   TO ORCLSTUDY;
```

```
-- ex 2) ORCLSTUDY로 사용권한을 부여받은 TEMP 테이블 사용 (SQLPlus)
-- 1) ORCLSTUDY 계정으로 접속
CONN ORCLSTUDY/ORACLE

-- 2) SCOTT계정의 테이블인 TEMP를 조회 (부여받은 SELECT 권한 확인)
SELECT * FROM SCOTT.TEMP;

-- 3) SCOTT계정의 TEMP테이블에 데이터 삽입 (부여받은 INSERT 권한 확인)
INSERT INTO SCOTT.TEMP VALUES('TEXT', 'FROM ORCLSTUDY');

-- 4) TEMP 테이블 조회
SELECT * FROM SCOTT.TEMP;
```

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> SELECT * FROM SCOTT.TEMP;

선택된 레코드가 없습니다.

SQL> INSERT INTO SCOTT.TEMP VALUES('TEXT', 'FROM ORCLSTUDY');

1 개의 행이 만들어졌습니다.

SQL> SELECT * FROM SCOTT.TEMP;

COL1                 COL2
-------------------- --------------------
TEXT                 FROM ORCLSTUDY
```

권한 부여 후 실행결과 (ex 2)

위처럼 권한을 부여받으면 사용자의 소유가 아닌 다른 계정의 테이블을 SELECT 하고 INSERT 하는 것이 가능하다.

■ 객체 권한 취소

```
REVOKE [객체 권한/ALL PRIVILEGES]
   ON [스키마.객체 이름]
 FROM [사용자 이름/롤(Role) 이름/PUBLIC]
 [CASCADE CONSTRAINTS/FORCE];
```

객체 권한의 취소도 시스템 권한과 마찬가지로 REVOKE 문을 사용한다.

```
-- ex) 객체 권한 취소 예시(SQLPlus)
-- 1) SCOTT 계정으로 접속
CONN SCOTT/tiger

-- 2) ORCLSTUDY에게 부여되었던 SELECT, INSERT 권한 취소
REVOKE SELECT, INSERT ON TEMP FROM ORCLSTUDY;

-- 3) ORCLSTUDY로 접속
CONN ORCLSTUDY/ORACLE

-- 4) 권한 철회된 TEMP 테이블 조회해보기
SELECT * FROM SCOTT.TEMP;
```

```
SQL> CONN SCOTT/tiger
연결되었습니다.
SQL> REVOKE SELECT, INSERT ON TEMP FROM ORCLSTUDY;

권한이 취소되었습니다.

SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> SELECT * FROM SCOTT.TEMP;
SELECT * FROM SCOTT.TEMP
                    *
1행에 오류:
ORA-00942: 테이블 또는 뷰가 존재하지 않습니다
```

객체 권한 취소 결과

REVOKE 로 권한을 취소하면 ORCLSTUDY 사용자는 더 이상 SCOTT 계정의 TEMP 테이블을 조회하거나 데이터를 삽입할 수 없다.
(보안상의 이유로 접근할 수 없는 테이블은 존재하지 않는다고 나온다.)

롤(Role) 관리

롤(role)은 여러 종류의 권한을 묶어놓은 그룹을 의미한다. 롤을 사용하면 여러 권한을 한 번에 부여하고 해제할 수 있어서 권한 관리 효율을 높일 수 있다. 롤은 오라클 데이터베이스를 설치할 때 기본으로 제공되는 사전 정의된 롤(predefined roles)과 사용자 정의 롤(user roles)로 나뉜다.

1. 사전 정의된 롤(Predefined roles)

사전 정의된 롤은 아래 나온 것들 외에도 여러 가지가 있다. (자세한 내용은 오라클 공식 문서 참조)

■ CONNECT 롤

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

사용자가 데이터베이스에 접속하는데 필요한 CREATE SESSION 권한을 가지고 있다.
오라클 9i 버전까지는 위의 8가지 권한을 가지고 있었지만 10g 버전부터 CREATE SESSION 권한만 있다.

■ RESOURCE 롤

```
CEATE TRIGGER, CREATE SEQUENCE, CREATE TYPE, CREATE PROCEDURE, CREATE CLUSTER,
CREATE OPERATOR, CREATE INDEXTYPE, CREATE TABLE
```

사용자가 테이블, 시퀀스를 비롯한 여러 객체를 생성할 수 있는 기본 시스템 권한을 묶어놓은 롤이다. 보통 새로운 사용자를 생성하면 CONNECT 롤과 RESOURCE 롤을 부여하는 경우가 많은데, 이는 CONNECT 롤에 CREATE SESSION 권한만 남아있기 때문에 객체 생성 권한을 함께 주기 위해서이다.

■ DBA 롤

데이터베이스를 관리하는 시스템 권한을 대부분 갖고 있다.

2. 사용자 정의 롤(user roles)

■ 사용자 정의 롤 생성

1. CREATE ROLE 문으로 롤을 생성한다.
2. GRANT 명령어로 생성한 롤에 권한을 포함시킨다.
3. GRANT 명령어로 권한이 포함된 롤을 특정 사용자에게 부여한다.
4. REVOKE 명령어로 롤을 취소시킨다.

사용자 정의 롤은 필요에 의해 직접 권한을 포함시킨 롤을 의미한다.
위의 절차를 따라 롤을 생성해서 사용할 수 있으며, 이미 존재하는 롤도 포함 가능하다.

```
-- ex) 롤 생성 및 권한부여 예시(SQLPlus)
-- 1) SYSTEM 계정으로 접속
CONN SYSTEM/oracle

-- 2) 롤 생성
CREATE ROLE ROLESTUDY;

-- 3) 권한 포함시키기
GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SYNONYM
   TO ROLESTUDY;

-- 4) 사용자에게 생성했던 롤(ROLESTUDY) 부여
GRANT ROLESTUDY TO ORCLSTUDY;
```

롤을 생성하고 부여하는 예시이다.

■ 사용자 정의 롤 취소 / 삭제

```
-- 부여된 롤 취소
REVOKE [롤 이름] FROM [롤을 부여한 사용자];

REVOKE ROLESTUDY FROM ORCLSTUDY;
```

```
-- 롤 삭제
DROP ROLE [롤 이름];

DROP ROLE ROLESTUDY;
```

REVOKE 명령어로 부여된 롤을 취소할 수 있고, DROP 명령어로 롤을 삭제할 수 있다.
롤을 삭제하면 해당 롤을 부여받은 모든 사용자의 롤이 취소(REVOKE)된다.

■ 부여된 롤과 권한 확인

```
CONN ORCLSTUDY/ORACLE
SELECT * FROM USER_SYS_PRIVS;
SELECT * FROM USER_ROLE_PRIVS;


-- DBA_SYS_PRIVS와 DBA_ROLE_PRIVS를 사용하는 경우
SEELCT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ORCLSTUDY';
SEELCT * FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'ORCLSTUDY';
```

사용자에게 현재 부여된 권한과 롤을 확인하려면 USER_SYS_PRIVS , USER_ROLE_PRIVS 데이터 사전을 사용하면 된다.
데이터 관리 권한을 가진 계정은 DBA_S_PRIVS , DBA_ROLE_PRIVS 를 사용해도 된다.

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> SELECT * FROM USER_SYS_PRIVS;

USERNAME                       PRIVILEGE                                ADM
------------------------------ ---------------------------------------- ---
ORCLSTUDY                      CREATE SESSION                           NO

SQL> SELECT * FROM USER_ROLE_PRIVS;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
ORCLSTUDY                      ROLESTUDY                      NO  YES NO
```

USER_SYS_PRIVS, USER_ROLE_PRIVS 조회 결과