Chap15. 사용자, 권한, 롤 관리

- 15-1 사용자 관리
- 15-2 권한 관리
- 15-3 롤 관리

15-1 사용자 관리

- 사용자란?
  - 데이터베이스에 접속하여 데이터를 사용/관리하는 계정
  - 업무의 분할과 효율, 보안을 고려하여 생성

- 데이터베이스 스키마란?
  - 데이터를 저장 및 관리하기 위해 정의한 데이터베이스 구조의 범위를 분류

15-1 사용자 관리

- 사용자란?
  - 데이터베이스에 접속하여 데이터를 사용/관리하는 계정
  - 업무의 분할과 효율, 보안을 고려하여 생성

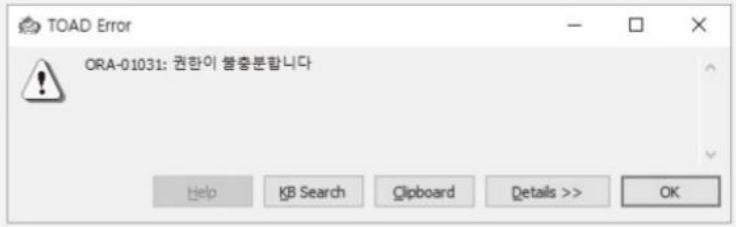
사용자 생성

```
CREATE USER 사용자 이름(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);
```

실습 15-1 SCOTT 계정으로 사용자 생성하기

```
01  CREATE USER ORCLSTUDY
02  IDENTIFIED BY ORACLE;
```

:: 결과 화면



15-1 사용자 관리

실습 15-2 SYSTEM 사용자로 접속 후 사용자 생성하기(SQL*PLUS)

```
01  CREATE USER ORCLSTUDY
02  IDENTIFIED BY ORACLE;
```

:: 결과 화면

```
C:₩>SQLPLUS SYSTEM/oracle

SQL*Plus: Release 11.2.0.1.0 Production on 목 5월 18 03:52:34 2017

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


다음에 접속됨:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> CREATE USER ORCLSTUDY
  2  IDENTIFIED BY ORACLE;

사용자가 생성되었습니다.

SQL>
```

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


경고: 이제는 ORACLE에 연결되어 있지 않습니다.
SQL>
```

실습 15-3 SYSTEM 사용자로 접속 후 ORCLSTUDY 사용자에게 권한 부여하기

```
01  GRANT CREATE SESSION TO ORCLSTUDY;
```

:: 결과 화면

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> GRANT CREATE SESSION TO ORCLSTUDY;

권한이 부여되었습니다.

SQL>
```

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL>
```

15-1 사용자 관리

- 사용자 정보 조회/변경/삭제

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

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

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

실습 15-5 사용자 삭제하기

```
01   DROP USER ORCLSTUDY;
```

:: 결과 화면

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> DROP USER ORCLSTUDY;

사용자가 삭제되었습니다.

SQL>
```

실습 15-4 사용자 정보(패스워드) 변경하기

```
01   ALTER USER ORCLSTUDY
02   IDENTIFIED BY ORCL;
```

:: 결과 화면

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> ALTER USER ORCLSTUDY
  2  IDENTIFIED BY ORCL;

사용자가 변경되었습니다.

SQL>
```

```
SQL> CONN ORCLSTUDY/ORACLE
ERROR:
ORA-01017: invalid username/password; logon denied


경고: 이제는 ORACLE에 연결되어 있지 않습니다.
SQL> CONN ORCLSTUDY/ORCL
연결되었습니다.
SQL>
```

15-2 권한 관리

- 권한
  - 접속 사용자에 따라 접근할 수 있는 데이터 영역을 지정
  - 시스템 권한, 객체 권한

- 시스템 권한
  - 사용자 생성, 정보 수정, 삭제, 데이터베이스 접근
  - 여러 자원과 객체 생성 및 관리 등의 권한을 포함

15-2 권한 관리

- 권한
  - 접속 사용자에 따라 접근할 수 있는 데이터 영역을 지정
  - 시스템 권한, 객체 권한

인터넷 카페의 경우 접속 사용자 등급에 따라 사용 가능한 메뉴가 다른데요. 데이터베이스도 이처럼 접속 사용자에 따라 사용 가능한 데이터가 달라지도록 설정할 수 있습니다. 바로 '권한'을 이용해서 말이죠.

15-2 권한 관리

- 권한
  - 시스템 권한, 객체 권한

시스템 권한이란?

오라클 데이터베이스의 시스템 권한(system privilege)은 사용자 생성과 정보 수정 및 삭제, 데이터베이스 접근, 오라클 데이터베이스의 여러 자원과 객체 생성 및 관리 등의 권한을 포함합니다. 이러한 내용은 데이터베이스 관리 권한이 있는 사용자가 부여할 수 있는 권한입니다. 다음은 시스템 권한의 일부이며 ANY 키워드가 들어 있는 권한은 소유자에 상관없이 사용 가능한 권한을 의미합니다.

시스템 권한 분류	시스템 권한	설명
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
	INERT 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
이하 생략		

15-2 권한 관리

- 권한
  - 시스템 권한 부여

기본 형식

```
GRANT [시스템 권한] TO [사용자 이름/롤(Role)이름/PUBLIC]
      ①                ②
[WITH ADMIN OPTION];
      ③
```

번호	설명
①	오라클 데이터베이스에서 제공하는 시스템 권한을 지정합니다. 한 번에 여러 종류의 권한을 부여하려면 쉼표(,)로 구분하여 권한 이름을 여러 개 명시해 주면 됩니다(필수).
②	권한을 부여하려는 대상을 지정합니다. 사용자 이름을 지정해 줄 수도 있고, 이후 소개할 롤(role)을 지정할 수도 있습니다. 여러 사용자 또는 롤에 적용할 경우 쉼표(,)로 구분합니다. PUBLIC은 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여하겠다는 의미입니다(필수).
③	WITH ADMIN OPTION은 현재 GRANT문을 통해 부여받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여받습니다. 현재 사용자가 권한이 사라져도, 권한을 재부여한 다른 사용자의 권한은 유지됩니다(선택).

O ORCLSTUD

15-2 권한 관리

- 권한
  - 시스템 권한 부여

실습 15-7 SYSTEM 계정으로 접속하여 사용자(ORCLSTUDY) 생성하기(SQL*PLUS)

```
01  CREATE USER ORCLSTUDY
02  IDENTIFIED BY ORACLE;
```

실습 15-8 사용자 권한 부여하기(SQL*PLUS)

```
01  GRANT RESOURCE, CREATE SESSION, CREATE TABLE TO ORCLSTUDY;
```

:: 결과 화면

```
SQL> CREATE USER ORCLSTUDY
  2  IDENTIFIED BY ORACLE;

사용자가 생성되었습니다.

SQL> GRANT CREATE SESSION, CREATE TABLE TO ORCLSTUDY;

권한이 부여되었습니다.

SQL>
```

```
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

SQL>
```

15-2 권한 관리

- 시스템 권한 취소

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

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> REVOKE RESOURCE, CREATE TABLE FROM ORCLSTUDY;

권한이 취소되었습니다.

SQL>
```

```
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


SQL>
```

15-2 권한 관리

- 객체 권한이란?
  - 특정 사용자가 생성한 객체와 관련된 권한

객체 권한 분류	객체 권한	설명
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

객체 권한 분류	객체 권한	설명
SEQUENCE(시퀀스)	ALTER	시퀀스 수정 권한
	SELECT	시퀀스의 CURRVAL과 NEXTVAL 사용 권한
PROCEDURE(프로시저)	(생략)	프로시저 관련 권한
FUNCTION(함수)	(생략)	함수 관련 권한
PACKAGE(패키지)	(생략)	패키지 관련 권한

이하 생략

15-2 권한 관리

객체 권한 부여

```
GRANT [객체 권한/ALL PRIVILEGES] -1
    ON [스키마.객체 이름] -2
    TO [사용자 이름/롤(Role)이름/PUBLIC] -3
    [WITH GRANT OPTION]; -4
```

번호	설명
1	오라클 데이터베이스에서 제공하는 객체 권한을 지정합니다. 한 번에 여러 종류의 권한을 부여하려면 쉼표(,)로 구분하여 권한을 여러 개 명시해 주면 됩니다. ALL PRIVILEGES는 객체의 모든 권한을 부여함을 의미합니다(필수).
2	권한을 부여할 대상 객체를 명시합니다(필수).
3	권한을 부여하려는 대상을 지정합니다. 사용자 이름을 지정해 줄 수도 있고 이후 소개할 롤(role)을 지정할 수도 있습니다. 여러 사용자 또는 롤에 적용할 경우 쉼표(,)로 구분합니다. PUBLIC은 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여하겠다는 의미입니다(필수).
4	WITH GRANT OPTION은 현재 GRANT문을 통해 부여받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여받습니다. 현재 권한을 부여받은 사용자의 권한이 사라지면, 다른 사용자에게 재부여된 권한도 함께 사라집니다(선택).

15-2 권한 관리

- 객체 권한 부여

실습 15-9 ORCLSTUDY 사용자에게 TEMP 테이블 권한 부여하기

```
01  CONN SCOTT/tiger

02  CREATE TABLE TEMP(
03     COL1 VARCHAR(20),
04     COL2 VARCHAR(20)
05  );

06  GRANT SELECT ON TEMP TO ORCLSTUDY;

07  GRANT INSERT ON TEMP TO ORCLSTUDY;
```

:: 결과 화면

```
SQL> CONN SCOTT/tiger
연결되었습니다.
SQL> CREATE TABLE TEMP (
  2    COL1  VARCHAR2(20),
  3    COL2  VARCHAR2(20)
  4  );

테이블이 생성되었습니다.

SQL> GRANT SELECT ON TEMP TO ORCLSTUDY;

권한이 부여되었습니다.

SQL> GRANT INSERT ON TEMP TO ORCLSTUDY;

권한이 부여되었습니다.
```

SCOTT 접속

SCOTT 소유의 TEMP 테이블 생성

ORCLSTUDY 사용자에게 TEMP 테이블에 SELECT 권한 부여

ORCLSTUDY 사용자에세 TEMP 테이블에 INSERT 권한 부여

15-2 권한 관리

- 객체 권한 부여

실습 15-10 ORCL에게 TEMP 테이블의 여러 권한을 한 번에 부여하기

```
01  GRANT SELECT, INSERT ON TEMP
02     TO ORCLSTUDY;
```

실습 15-11 ORCLSTUDY로 사용 권한을 부여받은 TEMP 테이블 사용하기

```
01  CONN ORCLSTUDY/ORACLE

02  SELECT * FROM SCOTT.TEMP;

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

04  SELECT * FROM SCOTT.TEMP;
```

:: 결과 화면

```
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
SQL>
```

15-2 권한 관리

객체 권한 취소

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

실습 15-12 ORCLSTUDY에 부여된 TEMP 테이블 사용 권한 취소하기

```
01  CONN SCOTT/tiger

02  REVOKE SELECT, INSERT ON TEMP FROM ORCLSTUDY;
```

:: 결과 화면

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

권한이 취소되었습니다.

SQL>
```

실습 15-13 ORCLSTUDY로 권한 철회된 TEMP 테이블 조회하기(실패)

```
01  CONN ORCLSTUDY/ORACLE

02  SELECT * FROM SCOTT.TEMP;
```

:: 결과 화면

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


SQL>
```

15-3 롤 관리

- 롤이란?
  - 여러 종류의 권한을 묶어 놓은 그룹
- 사전 정의된 롤
  - CONNECT

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

CONNECT 롤에서 뷰를 생성하는 CREATE VIEW 권한과 동의어를 생성하는 CREATESYNONYM 권한이 제외

  - RESOURCE

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

  - DBA

데이터베이스를 관리하는 시스템 권한을 대부분 가지고 있습니다.

15-3 롤 관리

- 사용자 정의 롤
  - 필요에 의해 직접 권한을 포함시켜 생성한 롤

① CREATE ROLE문으로 롤을 생성합니다.
② GRANT 명령어로 생성한 롤에 권한을 포함시킵니다.
③ GRANT 명령어로 권한이 포함된 롤을 특정 사용자에게 부여합니다.
④ REVOKE 명령어로 롤을 취소시킵니다.

실습 15-14 SYSTEM 계정으로 ROLESTUDY 롤 생성 및 권한 부여하기

```
01  CONN SYSTEM/oracle

02  CREATE ROLE ROLESTUDY;

03  GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SYNONYM
04    TO ROLESTUDY;
```

:: 결과 화면

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> CREATE ROLE ROLESTUDY;

롤이 생성되었습니다.

SQL> GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SYNONYM
  2     TO ROLESTUDY;

권한이 부여되었습니다.
```

실습 15-15 ORCLSTUDY 사용자에게 롤(ROLESTUDY) 부여하기

```
01  GRANT ROLESTUDY TO ORCLSTUDY;
```

:: 결과 화면

```
SQL> GRANT ROLESTUDY TO ORCLSTUDY;

권한이 부여되었습니다.
```

15-3 롤 관리

- 사용자 정의 롤
  - 필요에 의해 직접 권한을 포함시켜 생성한 롤

실습 15-16 ORCLSTUDY에 부여된 롤과 권한 확인하기

```
01  CONN ORCLSTUDY/ORACLE
02  SELECT * FROM USER_SYS_PRIVS;
03  SELECT * FROM USER_ROLE_PRIVS;
```

:: 결과 화면

```
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

SQL>
```

DBA_ROLE_PRIVS와 DBA_SYS_PRIVS 데이터 사전을 조회하려면 [WHERE GRANTEE = 'ORCLSTUDY'] 조건을 사용하세요.

부여된 롤 취소

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> REVOKE ROLESTUDY FROM ORCLSTUDY;

권한이 취소되었습니다.
```

롤 삭제

```
SQL> DROP ROLE ROLESTUDY;

롤이 삭제되었습니다.
```