

DCL, TCL

GRANT, REVOKE, COMMIT, ROLLBACK

TCL
COMMIT, ROLLBACK

▶ DCL(Data Control Language)

DB에 대한 보안, 무결성, 복구등 DBMS를 제어하기 위한 언어
GRANT(유저 권한 생성), REVOKE(유저 권한 삭제)

- 사용자의 권한이나, 관리자 설정 등을 처리

COMMIT(실행), ROLLBACK(복구)

- COMMIT, ROLLBACK 은 트랜잭션에 관련된 언어로 TCL로 구분하기도 함

▶ DCL - 계정관리

데이터베이스를 사용하기 위한 계정

데이터베이스에 접근하기 위해서는 해당 사용자로 로그인해서 사용해야 함

✓ 데이터베이스 관리자 계정

데이터베이스의 생성과 관리를 담당하는 계정
모든 권한과 책임을 가지는 계정

✓ 데이터베이스 사용자 계정

데이터베이스에 대하여 질의, 갱신, 보고서 작성 등의 작업을 수행할 수 있는 계정
업무에 필요한 최소한의 권한만 가지는 것을 원칙으로 함

▶ DCL - 계정관리

✓ Oracle 기본 생성 계정

오라클 데이터베이스를 설치하면 기본적으로 제공되는 계정

1. SYS : 기본 관리자 계정
2. SYSTEM : 기본 관리자 계정
3. SCOTT (교육용 샘플 계정) : 버전에 따라 잠겨 있을 수 있음
4. HR계정 (샘플계정) : 처음에는 잠겨져 있고, 11G에서는 없음

✓ 계정 조회

```
SELECT * FROM DBA_USERS;
```

▶ DCL - 계정관리

✓ 계정 생성

CREATE USER <USERNAME>

IDENTIFIED BY [PASSWORD]

DEFAULT TABLESPACE [TABLESPACE_NAME]

TEMPORARY TABLESPACE [TEMP_TABLESPACE_NAME]

QUOTA [SIZE / UNLIMITED] ON [TABLESPACE_NAME]

PROFILE [PROFILE | DEFAULT]

PASSWORD EXPIRE

ACCOUNT [LOCK | UNLOCK];

IDENTIFIED BY [PASSWORD] : 해당 유저의 비밀번호를 설정하는 옵션

DEFAULT TABLESPACE [TABLESPACE_NAME] : 기본 테이블스페이스 지정

TEMPORARY TABLESPACE [TEMP_TABLESPACE_NAME] : 임시 테이블스페이스 지정

QUOTA [SIZE / UNLIMITED] ON [TABLESPACE_NAME] :

특정 테이블스페이스에 해당 유저가 사용할 수 있는 공간 용량을 설정하는 옵션

PROFILE [PROFILE | DEFAULT] : user의 password나 resource에 대해 제한

PASSWORD EXPIRE : 최초 접속 시 password 재설정

ACCOUNT [LOCK | UNLOCK] : 계정에 대한 lock 상태

▶ DCL - 계정관리

✓ 계정 생성

- KUSER 라는 이름의 계정을 생성하면서 비밀번호를 KUSERPASS로 설정하고 계정 잠금

CREATE USER KUSER

IDENTIFIED BY KUSERPASS

ACCOUNT LOCK;

USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS
KH	48	(null)	OPEN
SYS	0	(null)	OPEN
SYSTEM	5	(null)	OPEN
ANONYMOUS	35	(null)	OPEN
APEX_PUBLIC_USER	45	(null)	LOCKED
KUSER	51	(null)	LOCKED

▶ DCL - 계정관리

✓ 계정 수정

ALTER USER <USERNAME>

IDENTIFIED BY [PASSWORD]

DEFAULT TABLESPACE [TABLESPACE_NAME]

TEMPORARY TABLESPACE [TEMP_TABLESPACE_NAME]

QUOTA [SIZE / UNLIMITED] ON [TABLESPACE_NAME]

ACCOUNT [LOCK | UNLOCK];

✓ 계정 비밀번호 수정

ALTER USER KUSER IDENTIFIED BY KPASS;

✓ 계정 잠금 해제

ALTER USER KUSER ACCOUNT LOCK;

▶ DCL - 계정관리

✓ 계정 삭제

```
DROP USER <USERNAME> [CASCADE];
```

CASCADE : 계정과 관련된 모든 데이터베이스 스키마가 데이터 사전으로부터 삭제되고 모든 스키마 객체도 물리적으로 삭제

```
DROP USER KUSER;
```


▶ DCL - 권한관리

사용자가 특정 테이블에 접근할 수 있도록 하거나, 해당 테이블에 SQL문을 사용할 수 있도록 제한을 두는 것

사용자가 데이터베이스의 객체(테이블, 뷰 등)에 대한 특정 권한을 가질 수 있게 함

다수의 사용자가 공유하는 데이터베이스 정보에 대한 보안 설정함

데이터베이스에 접근하는 사용자마다 서로 다른 권한과 롤을 부여함

▶ DCL - 권한관리

✓ 시스템 권한

데이터베이스 접속 사용자 생성 및 오브젝트 생성 등의 권한 DBMS

데이터베이스 관리자가 가지고 있는 권한

CREATE USER(사용자 계정 만들기)

DROP USER(사용자 계정 삭제)

DDL

DROP ANY TABLE(임의의 테이블 삭제)

QUERY REWRITE(함수 기반 인덱스 생성 권한)

BACKUP ANY TABLE(테이블 백업)

시스템 관리자가 사용자에게 부여하는 권한

가

CREATE SESSION (데이터베이스에 접속)

CREATE TABLE (테이블 생성)

CREATE VIEW (뷰 생성)

CREATE SEQUENCE (시퀀스 생성)

CREATE PROCEDURE (프로시저 생성)

▶ DCL - 권한관리

(EX) EMPLOYEE)

2. ✓ 오브젝트 권한

해당 오브젝트에 대한 전반적인 작업을 위한 권한

권한	테이블	뷰	시퀀스	프로시저
ALTER	O		O	
DELETE	O	O		
SELECT	O	O	O	
UPDATE	O	O		
EXECUTE				O
INDEX	O			
INSERT	O	O		
REFERENCES	O			

▶ DCL - 권한관리

✓ 시스템 권한 부여

```
GRANT <권한,...> TO <USER>;
```

✓ 오브젝트 권한 부여

```
GRANT <권한,...> ON <OBJECT_NAME> TO <USER>;
```

✓ 시스템 권한 제거

```
REVOKE <권한,...> FROM <USER>;
```

✓ 오브젝트 권한 제거

```
REVOKE <권한,...> ON <OBJECT_NAME> FROM <USER>;
```

▶ DCL - 권한관리

✓ 시스템 권한 부여

- KUSER 계정에 접속 권한 부여

GRANT CREATE SESSION TO KUSER;

- KUSER 계정에 KH계정의 EMPLOYEE 테이블 조회 권한 부여

GRANT SELECT ON KH.EMPLOYEE TO KUSER;

- KUSER 계정에 부여된 KH계정의 EMPLOYEE 테이블 조회 권한 제거

REVOKE SELECT ON KH.EMPLOYEE FROM KUSER;

- KUSER 계정에 부여된 접속 권한 제거

REVOKE CREATE SESSION FROM KUSER;

▶ DCL - 권한관리

✓ 계정에 부여된 시스템 권한 확인(관리자)

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = '계정명';
```

✓ 계정에 부여된 오브젝트 권한 확인(관리자)

```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE = '계정명';
```

✓ 현재 접속 계정 시스템 권한 확인

```
SELECT * FROM SESSION_PRIVS;
```

✓ 현재 접속 계정 오브젝트 권한 확인

```
SELECT * FROM USER_TAB_PRIVS_RECD;
```

▶ DCL - 권한관리

✓ WITH ADMIN OPTION

사용자에게 시스템 권한을 부여할 때 사용
권한을 부여 받은 사용자는 다른 사용자에게 권한을 지정할 수 있음

```
GRANT <권한> TO <USER> WITH ADMIN OPTION;
```

✓ WITH GRANT OPTION

사용자가 해당 객체에 접근할 수 있는 권한을 부여 받으면서 그 권한을 다른 사용자에게 다시 부여할 수 있음

```
GRANT <권한> ON <OBJECT_NAME> TO <USER> WITH GRANT OPTION;
```

✓ PUBLIC

해당 권한을 모든 데이터베이스 유저에게 부여

```
GRANT <권한> ON <OBJECT_NAME> TO PUBLIC;
```

▶ DCL – 권한관리(ROLE) AA

가

사용자에게 허가 할 수 있는 권한들의 집합
ROLE을 이용하면 권한 부여와 회수에 용이함

✓ CONNECT ROLE

사용자가 데이터 베이스에 접속 가능하도록 하기위한 권한이 있는 ROLE
CONNECT ROLE 이 부여되지 않으면 계정이 존재하더라도 해당 계정으로 접속
을 할 수 없음 CREATE SESSION

✓ RESOURCE ROLE

CREATE 구문을 통해 객체를 생성할 수 있는 권한을 모아 놓은 ROLE
CREATE TABLE
CREATE VIEW

RESOURCE ROLE

✓ DBA ROLE

가

대부분의 시스템 권한 및 기타 여러가지 ROLE

▶ DCL – 권한관리(ROLE)

✓ ROLE에 부여된 권한 확인

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'ROLE';
```

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'CONNECT';
```

GRANTEE	PRIVILEGE	ADMIN_OPTION
CONNECT	CREATE SESSION	NO

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'RESOURCE';
```

GRANTEE	PRIVILEGE	ADMIN_OPTION
RESOURCE	CREATE TRIGGER	NO
RESOURCE	CREATE SEQUENCE	NO
RESOURCE	CREATE TYPE	NO
RESOURCE	CREATE PROCEDURE	NO
RESOURCE	CREATE CLUSTER	NO
RESOURCE	CREATE OPERATOR	NO
RESOURCE	CREATE INDEXTYPE	NO
RESOURCE	CREATE TABLE	NO

▶ DCL – 권한관리(ROLE)

✓ 계정에 ROLE 부여

```
GRANT <ROLE,...> TO <계정명>;
```

✓ 계정에서 ROLE 제거

```
REVOKE <ROLE,...> FROM <계정명>;
```

✓ 계정에 부여된 롤 확인

```
SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE = '계정명';
```

```
GRANT CONNECT, RESOURCE TO KUSER;
```

```
SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE = 'KUSER';
```

```
REVOKE CONNECT, RESOURCE FROM KUSER;
```

▶ DCL – 권한관리(ROLE)

✓ 사용자 정의 ROLE

ROLE 생성은 반드시 DBA권한이 있는 사용자만 할 수 있음

- ROLE 생성

```
CREATE ROLE <ROLE이름>;
```

- 생성된 ROLE에 권한 추가

```
GRANT <권한종류,...> TO <ROLE이름>;
```

- ROLE 삭제

```
DROP ROLE <ROLE이름>;
```

▶ TCL(Transaction Control Language)

트랜잭션 관리 처리 언어

COMMIT(트랜잭션 종료처리후 저장), ROLLBACK(트랜잭션 취소),
SAVEPOINT(임시저장)

✓ 트랜잭션

한꺼번에 수행되어야 할 최소의 작업 단위를 말함

논리적 작업 단위 (LUW, Logical Units of Work)

하나의 트랜잭션으로 이루어진 작업들은 반드시 한꺼번에 완료되어야 하며,
그렇지 않은 경우에는 한꺼번에 취소되어야 함



① 카드 삽입



② 메뉴 선택



③ 인증



④ 승인 후 출력

↑
하나의 트랜잭션

▶ TCL(Transaction Control Language)

✓ COMMIT

트랜잭션 작업이 정상 완료 되면 변경 내용을 영구히 저장(모든 savepoint 삭제)

✓ ROLLBACK

트랜잭션 작업을 모두 취소하고 최근 commit 시점으로 이동

✓ SAVEPOINT <savepoint명>

현재 트랜잭션 작업 시점에 이름을 지정함
하나의 트랜잭션 안에서 구역을 나눌수 있음

✓ ROLLBACK TO <savepoint명>

트랜잭션 작업을 취소하고 savepoint 시점으로 이동

▶ 데이터 딕셔너리(Data Dictionary)

자원을 효율적으로 관리하기 위해 다양한 정보를 저장하는 시스템 테이블
사용자가 테이블을 생성하거나, 사용자를 변경하는 등의 작업을 할 때 데이터베이스 서버에 의해 자동으로 갱신되는 테이블
사용자는 데이터 딕셔너리의 내용을 직접 수정하거나 삭제할 수 없음

✓ 분류

1. DBA_XXX : 데이터베이스 관리자만 접근이 가능한 객체 등의 정보 조회
(모든 객체에 대해 조회 가능)
2. ALL_XXX : 자신의 계정 + 권한을 부여 받은 객체 정보를 조회
3. USER_XXX : 자신의 계정이 소유한 객체 등에 관한 정보 조회

▶ 데이터 딕셔너리(Data Dictionary)

✓ USER_CONSTRAINTS

제약조건 관리하는 데이터 딕셔너리

✓ USER_CONS_COLUMNS

제약조건을 컬럼별로 관리하는 데이터 딕셔너리

✓ USER_TABLES

테이블을 관리하는 데이터 딕셔너리

자신의 계정이 소유한 객체 등에 관한 정보를 조회 할 수 있는 딕셔너리 뷰

✓ USER_TAB_COLS

테이블의 컬럼을 관리하는 데이터 딕셔너리