DCL,TCL

데이터베이스를 관리하기 위한 언어
GRANT, REVOKE, COMMIT, ROLLBACK

TCL 트렌젝션 제어 언어
COMMIT, ROLLBACK

▶ DCL(Data Control Language)

1. 권한 관리
2. 트랜잭션 관리

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

계정별로 객체를 따로따로 관리하기 때문에 주의해야 한다.

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

스캇

✓ 계정 조회

```
SELECT * FROM DBA_USERS;
```

관리자 계정으로만 사용할 수 있다

▶ DCL - 계정관리

✓ 계정 생성 계정도 하나의 객체이다

```
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

실제로는 PASSWORD 들어있지만 보이지 않는 것

▶ DCL - 계정관리

KH정보교육원

✓ 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~~; UNLOCK;
```

▶ DCL - 계정관리

✓ 계정 삭제

옵션

DROP USER <USERNAME> [CASCADE];

계정을 삭제하면 남아 있던 데이터들이 붕뜨게 됨
다 삭제하고 싶으면 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 테이블 생성하거나 삭제하거나 수정하거나

다수의 사용자가 공유하는 데이터베이스 정보에 대한 보안 설정함

데이터베이스에 접근하는 사용자마다 서로 다른 권한과 롤을 부여함 역할에 맞게

▶ DCL - 권한관리

✓ 시스템 권한

시스템 전반적인 구조를 위한

데이터베이스 접속 사용자 생성 및 오브젝트 생성 등의 권한 DBMS의 구조를 정의하기 위한 권한

데이터베이스 관리자가 가지고 있는 권한

- CREATE USER(사용자 계정 만들기)
- DROP USER(사용자 계정 삭제)
- DROP ANY TABLE(임의의 테이블 삭제)
- QUERY REWRITE(함수 기반 인덱스 생성 권한)
- BACKUP ANY TABLE(테이블 백업)

DDL

시스템 관리자가 사용자에게 부여하는 권한

관리자가 사용자한테

야 너 접속하게 해줄게

- CREATE SESSION (데이터베이스에 접속)
- CREATE TABLE (테이블 생성)
- CREATE VIEW (뷰 생성)
- CREATE SEQENCE (시퀀스 생성)
- CREATE PROCEDURE (프로시저 생성)

테이블좀 생성해라
뷰좀 생성해라
시퀀스좀 생성해라
프로시저좀 생성해라

객체 생성 권한

▶ DCL - 권한관리

특정 객체에 할당되는 권한 (따로따로 설정되는 권한)
EX) EMPLOYEE라는 테이블을 수정할 수 있는 권한

✓ 오브젝트 권한

특정 오브젝트
즉, 테이블,뷰, 시퀀스, 프로시져
에 대한 작업을 하기 위한 권한
예) 만들어져있는 테이블을 수정하거나, 데이터를 삽입하거나

해당 오브젝트에 대한 전반적인 작업을 위한 권한

권한	테이블	뷰	시퀀스	프로시져
ALTER	O		O	
DELETE	O	O		
SELECT	O	O	O	
UPDATE	O	O		
EXCUTE				O
INDEX	O			
INSERT	O	O		
REFERENCES	O			

▶ DCL - 권한관리

KH정보교육원

✓ 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;

연결 상태

- 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

KH정보교육원

✓ 계정에 부여된 시스템 권한 확인(관리자)

관리자만 사용할 수 있는 것

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

프리뷰즈

✓ 계정에 부여된 오브젝트 권한 확인(관리자)

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

✓ 현재 접속 계정 시스템 권한 확인

사용자 계정들도 사용할 수 있는 것

```
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;**

다른 사용자에게
이 권한을 부여할 수 있다.
(자신이 부여받은 권한을)

SESSION 권한

✓ WITH GRANT OPTION

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

오브젝트 권한

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

✓ PUBLIC

모든 사용자들이 공통으로 사용하는 객체, 테이블이라면 PUBLIC으로 지정할 수 있음

해당 권한을 모든 데이터베이스 유저에게 부여

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

▶ DCL – 권한관리(ROLE)

템플릿처럼 만들어 놓은것
A 룰 적용할게
A 안에 들어있던 권한들이 한번에 적용되는 것
회수하는 것도 마찬가지

사용자에게 허가 할 수 있는 권한들의 집합

ROLE을 이용하면 권한 부여와 회수에 용이함

묶음들이 기본적으로 만들어져있는 것이 있고
우리들이 필요하면 만들어 쓸 수 있음

사전에 정의된 롤

✓ CONNECT ROLE

연결을 하기 위해서는 어떤 권한들이 필요한지

사용자가 데이터 베이스에 접속 가능하도록 하기위한 권한이 있는 ROLE

CONNECT ROLE 이 부여되지 않으면 계정이 존재하더라도 해당 계정으로 접속을 할 수 없음

접속 할 때 필요했던 권한
CREATE SESSION

✓ RESOURCE ROLE

객체를 생성하기 위해서는 어떤 권한들이 필요한지

CREATE 구문을 통해 객체를 생성할 수 있는 권한을 모아 놓은 ROLE

CREATE TABLE
CREATE VIEW 등
다 적어주기 귀찮으니까 RESOURCE ROLE 한번만 적어도 다 부여할 수 있게
회수도 마찬가지

✓ DBA ROLE

대부분의 시스템 권한 및 기타 여러가지 ROLE 데이터베이스 관리자 권한이 다 부여됨

▶ DCL – 권한관리(ROLE)

KH정보교육원

✓ 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)

KH정보교육원

✓ 계정에 ROLE 부여

```
GRANT <ROLE,...> TO <계정명>;
```

✓ 계정에서 ROLE 제거

```
REVOKE <ROLE,...> FROM <계정명>;
```

✓ 계정에 부여된 룰 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

CREATE ROLE 명령으로 롤을 생성함

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

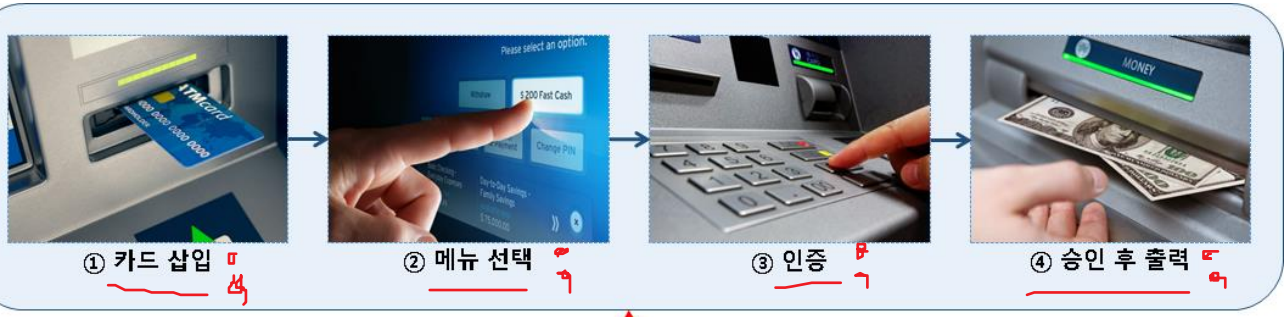
중간에 하나라도 잘못하면
(인증에서 비밀번호 틀림)
앞에 있던 것들 수행되면 안됨
원복이 되어야 함
처음부터 끝까지 정상적으로 다 완료가 돼야함
-> 최소 작업 단위 (논리적 작업 단위)

한꺼번에 수행되어야 할 최소의 작업 단위를 말함

논리적 작업 단위 (LUW, Logical Units of Work)

하나의 트랜잭션으로 이루어진 작업들은 반드시 한꺼번에 완료가 되어야 하며,
그렇지 않은 경우에는 한꺼번에 취소 되어야 함

처음부터 끝까지 다 정상적으로 수행될 때에만
완료돼야 하며 그렇지 않으면 처음으로 돌아가야 함



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

임시저장 포인트

세번째까지 수행했는데
네번째에 문제가 생김
처음으로 안가고 세번째로 돌아가게 하고 싶어

✓ ROLLBACK TO <savepoint명>

그냥 ROLLBACK -> 처음으로
ROLLBACK TO - > SAVEPOINT로

트랜잭션 작업을 취소하고 savepoint 시점으로 이동

▶ 데이터 딕셔너리(Data Dictionary)

KH정보교육원

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

수정이나 삭제하면 큰일남
구조 자체가 달라짐

✓ 분류

사용자가 쓰기 위해서 만든 테이블이 아니라
DBMS가 DBMS의 정보를 관리를 하기 위해서
알아서 만들어서 알아서 사용하는 테이블

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)

KH정보교육원

✓ USER_CONSTRAINTS

내 계정에 설정 돼 있는 제약조건

제약조건 관리하는 데이터 딕셔너리

✓ USER_CONS_COLUMNS

현재 계정에 설정돼 있는는 제약조건을 컬럼별로 관리

제약조건을 컬럼별로 관리하는 데이터 딕셔너리

✓ USER_TABLES

현재 계정에 만들어져 있는 테이블을 관리

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

✓ USER_TAB_COLS

현재 계정에 만들어져 있는 테이블들의 컬럼

테이블의 컬럼을 관리하는 데이터 딕셔너리