데이터 제어어
(Data Control Language : DCL)

데이터베이스 보안을 위한 권한

- 기업에서 보유하고 있는 데이터들은 자료 이상의 가치가 있으므로 외부에 노출되지 않도록 보안을 해야 함.
- 데이터베이스를 운영하려면 데이터베이스에 대한 적절한 보안 대책을 마련해야 함.
- 오라클은 다수의 사용자들이 데이터베이스에 저장된 정보를 공유해서 사용함.
- 하지만 정보의 유출이나 불법적인 접근을 방지하기 위해서 철저한 보안 대책이 필요함.
- 이러한 보안 대책을 위해서 데이터베이스 관리자가 있어야 함.
- 데이터베이스 관리자는 사용자가 데이터베이스의 객체(테이블, 뷰 등)에 대한 특정 권한을 가질 수 있도록 함으로서 다수의 사용자가 데이터베이스에 저장된 정보를 공유하면서도 정보에 대한 보안이 이루어지도록 함.
- 데이터베이스에 접근하기 위해서는 사용자가 이름과 암호를 입력해서 로그인 인증을 받아야 함.
- 이렇게 데이터베이스에 접속하는 사용자로부터 어떻게 데이터를 보안할 수 있을까요?
- 사용자마다 서로 다른 권한과 롤을 부여함으로서 보안을 설정할 수 있음.

권한의 역할과 종류

- 권한은 사용자가 특정 테이블을 접근할 수 있도록 하거나 해당 테이블에 SQL(SELECT/INSERT/UPDATE/DELETE) 문을 사용할 수 있도록 제한을 두는 것을 말함.
- 데이터베이스 보안을 위한 권한은 시스템 권한(System Privileges)과 객체 권한(Object Privileges)으로 나뉨.
- 시스템 권한은 사용자의 생성과 제거, DB 접근 및 각종 객체를 생성할 수 있는 권한 등 주로 DBA에 의해 부여되며 그 권한의 수가 80 가지가 넘기에 대표적인 시스템 권한만 정리함.

시스템 권한	기 능
CREATE USER	새롭게 사용자를 생성하는 권한
DROP USER	사용자를 삭제하는 권한
DROP ANY TABLE	임의의 테이블을 삭제할 수 있는 권한
QUERY REWRITE	함수 기반 인덱스를 생성하는 권한
BACKUP ANY TABLE	임의의 테이블을 백업할 수 있는 권한

데이터베이스를 관리하는 권한(Role)

- 시스템 관리자가 사용자에게 부여하는 권한임.
- 객체 권한은 객체를 조작할 수 있는 권한임.

시스템 권한	기 능
CREATE SESSION	데이터베이스에 접속할 수 있는 권한
CREATE TABLE	사용자 스키마에서 테이블을 생성할 수 있는 권한
CREATE VIEW	사용자 스키마에서 뷰를 생성할 수 있는 권한
CREATE SEQUENCE	사용자 스키마에서 시퀀스를 생성할 수 있는 권한
CREATE PROCEDURE	사용자 스키마에서 함수를 생성할 수 있는 권한

권한 부여하는 GRANT 명령어

- 사용자에게 시스템 권한 부여하기 위해서는 GRANT 명령어를 사용함.
- 만일 user_name 대신 PUBLIC을 기술하면 모든 사용자에게 해당 시스템 권한이 부여됨.
- PUBLIC 이란 DB 내에 있는 모든 계정 즉, 모든 계정을 의미함.
- 우선 데이터베이스 관리자로 접속함.
- 새로 생성된 user01에 데이터베이스에 접속할 수 있는 권한인 CREATE SESSION를 부여함.
- 다시 user01 사용자로 접속을 시도하면 이번에는 데이터베이스에 성공적으로 접속하게 됨.

옵션

- with admin option
  - 사용자에게 시스템 권한을 with admin option과 함께 부여하면 그 사용자는 데이터베이스 관리자가 아닌데도 불구하고 부여 받은 시스템 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여 받게 됨.

- with grant option
  - 사용자에게 객체 권한을 with grant option과 함께 부여하면 사용자는 객체를 접근할 권한을 부여 받으면서 그 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여 받게 됨.

권한(Role)

- 사용자에게 보다 효율적으로 권한을 부여할 수 있도록 여러 개의 권한을 묶어 놓은 것.
- 사용자를 생성했으면 그 사용자에게 각종 권한을 부여해야만 생성된 사용자가 데이터베이스를 사용할 수 있음.
- connect Role
  - 사용자가 데이터베이스에 접속 가능하도록 하기 위해서 다음과 같이 가장 기본적인 시스템 권한 8가지 묶어 놓은 권한.
  - alter session, create cluster, create database link, create sequence, create session, create synonym, create table, create view
- resource Role
  - 사용자가 객체(테이블, 시퀀스, 뷰)를 생성할 수 있도록 시스템 권한을 묶어 놓은 것.
  - create cluster, create procedure, create sequence, create table, create trigger
- DBA Role
  - 사용자들이 소유한 데이터베이스 객체를 관리하고 사용자들이 작성하고 변경하고 제거할 수 있도록 하는 모든 권한을 가짐.

롤 관련 데이터 딕셔너리

딕셔너리 명	설 명
ORLE_SYS_PRIVS	롤에 부여된 시스템 권한 정보
ROLE_TAB_PRIVS	롤에 부여된 테이블 관련 권한 정보
USER_ROLE_PRIVS	접근 가능한 롤 정보
USER_TAB_PRIVS_MADE	해당 사용자 소유의 오브젝트에 대한 오브젝트 권한 정보
USER_TAB_PRIVS_RECD	사용자에게 부여된 오브젝트 권한 정보
USER_COL_PRIVS_MADE	사용자 소유의 오브젝트 중 칼럼에 부여된 오브젝트 권한 정보
USER_COL_PRIVS_REDC	사용자에게 부여된 특정 칼럼에 대한 오브젝트 권한 정보

스키마(SCHMA)

- 객체를 소유한 사용자명을 의미.

- 객체 명 앞에 소속 사용자명을 기술함.
  - 예) SELECT * FROM SCOTT.EMP;

    - EMP 앞에 SCOTT은 EMP 테이블 객체를 소유한 사용자명임.

- 자신이 소유한 객체가 아닌 경우에는 그 객체를 소유한 사용자명을 반드시 기술해야 함.

사용자에게 부여된 권한 조회

- 현재 사용자와 관련된 권한을 조회 방법은?

- 사용자 권한과 관련된 데이터 딕셔너리 중에서 USER_TAB_PRIVS_MADE 데이터 딕셔너리는 현재 사용자가 다른 사용자에게 부여한 권한 정보를 알려줌.

- 만일 자신에게 부여된 사용자 권한을 알고 싶을 때에는 USER_TAB_PRIVS_RECD 데이터 딕셔너리를 조회하면 됨.