13강 사용자 권한

사용 권한의 개념

- 오라클의 보안 정책은 크게 시스템 보안과 데이터 보안으로 구분한다.

- 시스템 보안은 데이터 베이스 자체에 대한 접근을 할 수 있는 권한을 설정하는 것 보통 사용자 계정과 암호로 인증받아야 한다는 것이다.
    - 시스템 권한

- 데이터 보안은 사용자가 자신이 생성한 객체에 대한 소유권을 가지므로 데이터 조회나 조작을 할 수 있지만 다른 사용자는 객체의 소유자로부터 접근 권한을 받아야 사용 가능하다는 것이다.
    - 객체 권한

사용 권한

- 대표적인 시스템 권한

권한	설명
CREATE SESSION	데이터베이스에 연결할 수 있는 권한
CREATE TABLE	테이블을 생성할 수 있는 권한
CREATE SEQUENCE	시퀀스를 생성할 수 있는 권한
CREATE VIEW	뷰를 생성할 수 있는 권한

사용 권한

- 사용자 계정을 만들기 위해서는 관리자 계정을 접속해야 한다.

SQL COMMAND LINE 에서는 conn system/비밀번호 를 이용해서 접속한다.
(단 관리자 비밀번호을 잊어버렸다면 로컬접속이라는 전제에 다음과 같이 접속이 가능하다.)
 - conn /as sysdba; 로 로그인 가능하다.

- 사용자 계정 생성

- create user 계정명 identified by 비밀번호;

=> 그냥 접속하면 접속 오류가 난다. 연결 권한이 없어서이다.

- 관리자 계정으로 연결 권한을 부여한다.

- grant create session to 계정명;

사용 권한

- 명령으로 현재 사용자 정보를 볼 수 있다.

- show user;

- 테이블을 만들어 보자.

- create table 테이블명(
        컬럼명 타입
);

⇒오류가 발생

- 권한을 부여한다.

- grant create table to 계정명;

- 다시 테이블을 만들어 본다.

사용 권한

- 테이블을 만들 때 다시 오류가 발생하는 것을 볼 수 있는데 테이블을 만들기 위해서는 테이블 스페이스를 사용할 수 있어야 하는데

테이블 스페이스란 용량을 차지하는 테이블, 뷰, 인덱스 등을 저장될수 있는 공간을 의미한다.

- 관리자로 접속해서 새로 생성한 계정이 사용가능 한 테이블 스페이스를 확인 해보자

- select username, default_tablespace
- from dba_users
- where username = '계정명';

- 조회하면 기본 테이블 공간을 SYSTEM인 것을 알 수 있고 사용자 계정 생성 당시 디폴트 테이블 스페이스를 할당하지 않아서 생기는 문제이다.
- 관리자 계정에서 테이블 공간을 할당 해준다.

- alter user usertest01 quota 100m on users;
- alter user usertest01 default tablespace users;

사용 권한

- 객체권한은 테이블 뷰 시퀀스 함수 등과 같이 객체 별로 사용할 수 잇는 권한으로 객체와 권한을 설정할 수 있는 명령어는 다음과 같다.

권한	TABLE	VIEW	SEQUENCE	PROCEDURE
ALTER	O		O	
DELETE	O	O		
EXECUTE				O
INDEX	O			
INSERT	O	O		
REFFERENCES	O			
SELECT	O	O	O	
UPDATE	O	O		

사용 권한

- 새로 생성한 계정에서 hr계정의 employee테이블을 조회 해보자

- select * from employee;
- select * from hr.employee;

- 당연하지만 오류가 발생한다 왜냐하면 테이블 조회 권한이 없기 때문이다.

- 해당 테이블의 소유자로부터 권한을 얻어야 조회가 가능하다.

- conn hr/비밀번호;
- grant select on hr.employee to (권한을 부여할)계정명;

- 이제 다시 새로 생성한 계정에 접속해서 hr계정의 employee테이블을 조회 해보자

사용 권한

- 관리자 계정에서 새로 생성한 계정의 비밀번호를 바꿔 줄 수 있다
- alter user 계정명 identified by 새로 고칠 비밀번호;

이후로는 새로 고친 비밀번호로 접속 해야 한다.

사용 권한

- 권한을 제거할 수 있다 = REVOKE
- 관리자로 접속해서 새로 생성한 계정의 접속 권한을 제거해 보자

- revoke create session from 계정명;

- 이후로 해당 계정으로 로그인이 불가하게 된다.
- 다시 권한을 부여한 뒤 계정에 접속해서 해당 계정이 가진 권한을 조회해보자

- select * from session_privs;

- 현재 접속한 계정이 가진 권한을 볼 수 있다

사용 권한 - WITH GRANT OPTION

- 추가 옵션
- WITH GRANT OPTION
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- 새로운 계정을 두개 생성한 다음 접속권한, 테이블 생성권한, 뷰 생성 권한을 부여한다.

사용 권한 - WITH GRANT OPTION

- 추가 옵션
- WITH GRANT OPTION
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- 새로운 계정을 두개 생성한 다음 접속권한, 테이블 생성권한, 뷰 생성 권한을 부여한다.

- conn system/1234;
- create user 계정명2 identified by 비밀번호;
- create user 계정명3 identified by 비밀번호;
- grant create session, create table, create view to 계정명2;
- grant create session, create table, create view to 계정명3;

사용 권한 - WITH GRANT OPTION

- 추가 옵션
- WITH GRANT OPTION
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- hr계정으로 접속해서 두번째 생성한 계정에 employee의 조회 권한을 부여하되 다른 사용자에게도 부여 가능하게 해봅니다.

사용 권한 - WITH GRANT OPTION

- 추가 옵션
- WITH GRANT OPTION
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- hr계정으로 접속해서 두번째 생성한 계정에 employee의 조회 권한을 부여하되 다른 사용자에게도 부여 가능하게 해봅니다. 세번째 생성한 계정은 다른 사용자에게 부여가 불가능하게 해봅니다.

- conn hr/비밀번호;
- grant select on hr.employee to 계정명2 with grant option;
- grant select on hr.employee to 계정명3;

- 두번째 계정에서 첫번째 계정에 hr.employee 조회 권한을 부여 해봅니다.

- 세번째 계정에서 첫번째 계정에 hr.employee 조회 권한을 부여 해봅니다.

사용 권한 - WITH GRANT OPTION

- 추가 옵션
- WITH GRANT OPTION
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- 두번째 계정에서 첫번째 계정에 hr.employee 조회 권한을 부여 해봅니다.

 - conn 계정명2/비밀번호;

 - grant select on hr.employee to usertest01;

세번째 계정에서 첫번째 계정에 hr.employee 조회 권한을 부여 해봅니다.

 - conn 계정명3/비밀번호;

 - grant select on hr.employee to usertest01; => 에러 발생

사용 권한 - PUBLIC

- 추가 옵션
- PUBLIC
  - 위 옵션을 주어서 권한을 설정하면 권한 부여 받은 사용자도 해당 권한을 또 다른 사용자에게 넘겨줄 수 있다.

- hr 계정으로 접속해서 hr.department 테이블의 접근 권한은 모든 사용자에게 부여한 다음 새로 생성한 각 3개의 계정에서 조회해 보자

- conn hr/비밀번호;
- grant select on hr.department to public;

- conn 계정명1/비밀번호;
- select * from hr.department;
- conn 계정명2/비밀번호;
- select * from hr.department;
- conn 계정명3/비밀번호;
- select * from hr.department;

권한 - PUBLIC

- 롤을 사용한 권한 부여

- 사용자를 생성한 후 사용하려면 다양한 종류의 권한을 부여해여 한다. 그러나 이런 권한을 일일이 부여하는 것은 번거롭다.
- 롤은 사용자에게 보다 간편하게 권한을 부여 할 수 있도록 관련 있는 권한 끼리 묶어 놓은 것이다.

롤 종류	롤에 부여된 권한
DBA	WITH ADMIN OPTION에 있는 모든 권한
CONNECT	ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW
RESOURCE	CREATE CLUSTER, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGER

권한 - PUBLIC

- 롤을 사용한 권한 부여
- DBA 롤은 시스템 자원을 무제한 적으로 사용하며 모든 권한을 부여하는 강력한 권한을 가진 롤이다.
- CONNECT 롤은 사용자가 데이터베이스에 접속 가능하도록 가장 기본적인 시스템 권한 8가지를 그룹화 한 것이다.
- RESOURCE 롤은 사용자가 객체(테이블,뷰, 인덱스)생성할 수 있도록 하기 위해 시스템 권한을 그룹화 한 것이다.

권한 - PUBLIC

- 롤을 사용한 권한 부여
- 새로운 계정4을 생성한후 CONNECT롤과 RESOURCE 롤을 부여해 본다.

- conn system/비밀번호;
- create user 계정명4 identified by 비밀번호;
- grant connect to 계정명;
- grant resource to 계정명;

권한 - PUBLIC

- CREATE ROLE문으로 사용자가 직접 롤을 생성할 수도 있다.
- 관리자 계정에서 롤을 직접 생성해 보자

- conn system/비밀번호;
- create role 롤 이름(roletest01);
- grant create session, create table, create view to 롤이름;
- grant 롤이름 to 계정 명;

권한 - PUBLIC

- 데이터 사전을 통해 부여된 권한에 대한 정보를 확인할 수 있다.

딕셔너리 명	설명
ROLE_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

권한 - PUBLIC

- 데이터 사전을 통해 부여된 권한에 대한 정보를 확인할 수 있다.

- conn system/비밀번호;
- select * from role_sys_privs

where role like '%TEST%';

- 현재 사용자에 부여된 롤을 확인하기 위한 데이터 사전은 USER_ROLE_PRIVS이다.
  - conn 계정명/비밀번호;
  - select * from user_role_privs;

- 롤 삭제 - 관리자 계정
  - DROP ROLE 롤이름;

권한 - PUBLIC

- 다만 객체 권한인 경우 소유자로 로그인한 후 부여해야 한다.
  - conn system/비밀번호;
  - create role 롤이름02;
  - conn hr/비밀번호;
  - grant select on employee to 롤이름02;
  - conn system/비밀번호;
  - grant 롤이름02 to 계정명;

사용자에게 롤이 부여되었는지 확인해보자
  - conn 계정명/비밀번호;
  - select * from hr.employee;

권한 - PUBLIC

- 사용자에게 롤이 부여되었는지 확인하기
  - conn 계정명/비밀번호;
  - select * from user_role_privs;

- 롤에 부여된 테이블과 관련된 권한 정보를 알려주는 데이터 사전 ROLE_TAB_PRIVS

- select * from role_tab_privs;