13장 사용자 권한

이번 장에서는 사용자를 생성하고 시스템 권한과 객체 권한을 부여하는 방법을 학습합니다. 또한 여러 가지 권한을 포함하는 권한의 집합인 롤에 대해서 학습하며 데이터베이스 객체 이름에 대해서 별칭을 줄 수 있는 동의어에 대해서 학습합니다.

학습 내용

- 사용 권한
- 롤을 사용한 권한 부여
- 동의어

학습목표

- 데이터베이스 보안을 위해 시스템 권한과 객체 권한을 사용자에게 설정할 수 있습니다.
- 롤에 여러 가지 권한을 포함시켜 보다 간단하게 사용자에게 권한 부여를 할 수 있습니다.
- 객체를 간단하게 접근하도록 하기 위해 객체 이름에 동의어를 정의할 수 있습니다.

01. 사용 권한

- 사용 권한은 시스템 권한(System Privileges)과 객체 권한(Object Privileges)으로 나뉩니다.

- 시스템 권한에는 사용자의 생성과 제거, 자원 관리가 있습니다.

시스템 권한	기능
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
CREATE SESSION	데이터베이스에 연결할 수 있는 권한

01. 사용 권한

- 권한을 부여받기 위한 사용자를 CREATE USER 문을 사용하여 생성
- 다음은 사용자 생성을 위한 CREATE USER 명령어의 형식입니다.

```
CREATE USER user_name
IDENTIFIED BY password;
```

01. 사용 권한

- 사용자에게 시스템 권한 부여하기 위해서는 GRANT 명령어를 사용합니다.

```
GRANT privilege_name,
TO user_name;
```

- 새로 생성된 user에 데이터베이스에 데이터베이스 관리자로 접속해서 할 수 있는 권한인 CREATE SESSION를 부여합니다.

객체 권한

- 객체 권한은 특정 객체에 조작을 할 수 있는 권한입니다. 객체의 소유자는 객체에 대한 모든 권한을 가집니다.

- 다음은 객체와 권한 설정할 수 있는 명령어를 매핑시켜 놓은 표입니다.

권 한	TABLE	VIEW	SEQUENCE	PROCEDURE
ALTER	v		v	
DELETE	v	v		
EXECUTE				v
INDEX	v			
INSERT	v	v		
REFERENCES	v			
SELECT	v	v	v	
UPDATE	v	v		

객체 권한

- 객체 권한은 테이블이나 뷰나 시퀀스나 함수 등과 같은 객체별로 DML문(SELECT, INSERT, DELETE)을 사용할 수 있는 권한을 설정하는 것입니다.

- 다음은 객체에 권한을 부여하기 위한 형식입니다.

```
GRANT privilege_name [(column_name)] | ALL ①
ON object_name | role_name | PUBLIC ②
TO user_name; ③
```

- GRANT 명령어의 형식은 어떤 객체(②)에 어떠한 권한(①)을 어느 사용자(③)에게 부여하는가를 설정합니다. 시스템 권한과 차이점이 있다면 ON 옵션이 추가된다는 점입니다. ON 다음에 테이블 객체나 뷰 객체 등을 기술합니다.

객체 권한

- 특정 객체에 대한 권한은 그 객체를 만든 사용자에게만 기본적으로 주어집니다.
- 우리가 지금까지 사용했던 EMP 테이블은 hr 사용자 소유의 테이블입니다.
- 그러므로 다음과 같이 hr 사용자로 로그인해서 usertest01 사용자가 테이블 객체 EMP를 조회할 수 있도록 권한 부여를 해야 합니다.

객체 권한

❖ 객체 권한은 객체를 갖고 있는 사용자로 접속한 후에 사원을 조회할 수 있는 SELECT 권한을 usertest01에게 부여합니다.

1. hr로 접속하여 사원 테이블 조회 권한 부여하기

```
CONN hr/1234
```

2. hr 사용자 소유의 employee 테이블을 조회(SELECT)할 수 있는 권한을 usertest01 이란 사용자에게 부여합니다.

```
grant select on hr.employee to usertest01;
```

객체 권한

3. 권한 부여가 되었다면 다시 usertest01로 로그인하여 사원 테이블에 접속해 봅시다.

```
conn usertest01/pass1;
select * from hr.employee;
```

권한 제거

- REVOKE 문은 데이터베이스 관리자나 권한을 부여한 사용자가 다른 사용자에게 부여한 시스템 권한을 박탈하기 위한 명령어입니다.

```
REVOKE {privilege_name | all}
ON object_name
FROM {user_name | role_name | public};
```

권한 제거

❖ usertest01로부터 create session 권한 제거하기

```
conn system/1234;
revoke create session from usertest01;
```

WITH GRANT OPTION

- 사용자에게 객체 권한을 WITH GRANT OPTION과 함께 부여하면 그 사용자는 그 객체를 접근할 권한을 부여 받으면서 그 권한을 다른 사용자에게 부여 할 수 있는 권한도 함께 부여받게 됩니다.

- SYSTEM으로 로그인하여 사용자를 새로 생성한 후 데이터베이스에 연결할 수 있는 CREATE SESSION과 CREATE TABLE, CREATE VIEW 권한을 부여합니다.

WITH GRANT OPTION

- WITH GRANT OPTION을 지정하였기에 다른 사용자에게 객체권한을 부여할 수 있습니다.

1. hr 사용자로 접속합니다.

```
conn hr/1234;
grant select on hr.employee to usertest02 with
grant option;
```

2. usertest01에게 hr.employee를 SELECT하는 권한을 WITH GRANT OPTION으로 부여합니다.

```
conn usertest02/pass2;
grant select on hr.employee to usertest01;
```

02. 롤

- 여러 사용자에게 부여된 권한을 수정하고 싶을 때에도 일일이 사용자마다 권한을 수정하지 않고 롤만 수정하면 그 롤에 대한 권한 부여를 한 사용자들의 권한이 자동 수정됩니다. 이 밖에 롤을 활성화 비활성화 함으로서 일시적으로 권한을 부여했다 철회할 수 있으므로 사용자 관리를 간편하고 효율적으로 할 수 있습니다.

02. 롤

- 롤은 오라클 데이터베이스를 설치하면 기본적으로 제공되는 사전 정의된 롤과 사용자가 정의한 롤로 구분됩니다.

- 사용자가 직접 롤을 정의하는 방법은 복잡하므로 사전에 정의된 롤부터 살펴보도록 합시다.

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 TRIGGER

02. 롤

- 일반적으로 데이터베이스 관리자는 새로운 사용자를 생성할 때 CONNECT 롤과 RESOURCE 롤을 부여합니다.

```
conn system/1234;
create user usertest04 identified by pass4;
grant connect to usertest04 ;
grant resource to usertest04 ;
```

02. 롤

- CREATE ROLE 문은 사용자가 직접 정의해서 사용하는 롤을 생성

```
CREATE ROLE role_name [NOT IDENTIFIED |
IDENTIFIED
{BY password | EXTERNALLY} ];
```

- 생성한 롤은 GRANT로 사용자에게 권한을 부여합니다.

```
GRANT privilege_name TO role_name;
```

02. 롤

❖ 사용자 정의 롤 생성및 권한 부여하기

```
conn system/1234;
create role roletest01;
grant create session, create table, create view
to roletest01;
grant roletest01 to usertest01;
```

02 롤

❖ 다음은 롤 관련 데이터 사전을 정리한 표입니다.

사전 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

02. 롤

❖ DROP ROLE 문으로 롤 제거

```
DROP ROLE role_name FROM user_name;
```

```
conn system/1234;
drop role roletest01;
```

02. 롤

❖ 객체 권한을 롤에 부여하기

```
conn system/1234;
create role roletest02;
conn hr/1234;
grant select on employee to roletest02;
conn system/1234;
grant roletest02 to usertest01;
```

03. 동의어

- 동의어는 다른 데이터베이스 객체에 대한 별칭입니다. CREATE SYNONYM 문으로 동의어를 새롭게 정의합니다.

```
CREATE [PUBLIC] SYNONYM synonym_name
FOR user_name.object_name;
```

- 동의어는 개별 사용자를 대상으로 하는 비공개 동의어와 전체 사용자를 대상으로 한 공개 동의어가 있습니다.

- 비공개 동의어

  - **객체에 대한 접근 권한을 부여받은 사용자가 정의한 동의어로 해당 사용자만 사용할 수 있다.**

- 공개 동의어

  - **권한을 주는 사용자가 정의한 동의어로 누구나 사용할 수 있다. 공개 동의어는 DBA 권한을 가진 사용자만이 생성할 수 있다. SYNONYM 앞에 PUBLIC를 붙여서 정의한다.**

03. 동의어

❖ 테이블 조회 권한 부여하기

```
grant select on sampletbl to hr;
```

```
conn hr/1234;
select * from sampletbl;
```

❖ 다른 소유자의 테이블 조회하기

```
select * from system.sampletbl;
```

03. 동의어

❖ 전용 동의어 생성하기

```
conn hr/1234;
create synonym priv_sampletbl for
system.sampletbl;
```

```
select * from priv_sampletbl;
```

03. 동의어

❖ 공용 동의어 정의하기

```
conn system/1234;
create public synonym pub_sampletbl for
system.sampletbl;
```

```
conn hr/1234;
select * from pub_sampletbl;
```

03. 동의어

❖ DROP SYNONYM 문으로 동의어를 제거

```
DROP SYNONYM synonym_name;
```

```
conn hr/1234;
drop synonym priv_sampletbl;
```