

권한

사용자 생성
시스템 권한
역할(ROLE)
비밀번호 변경
객체 권한



권한(Privilege)은 특정 SQL 문장을 실행하기 위한 권리입니다. 데이터베이스 관리자(DBA)는 데이터베이스와 그 객체에 대한 액세스를 사용자에게 부여하는 능력을 갖춘 상급 사용자입니다.

사용자는 데이터베이스에 액세스하기 위해 시스템 권한(System Privilege)이 필요하고 데이터베이스에서 객체의 내용을 조작하기 위해 객체 권한(Object Privilege)이 필요합니다.

사용자는 관련 권한들의 이름 있는 그룹인 Role이나 다른 사용자에게 추가로 권한을 부여하기 위해 권한을 가질 수 있습니다.

사용자와 롤에 대해 시스템 권한과 객체 권한을 부여할 수 있습니다. 시스템 권한은 대개 데이터베이스 관리자(DBA)에 의해 제공됩니다. 객체 권한은 대개 객체의 소유주에 의해 제공됩니다.

표 1. DBA의 주요 권한

시스템 권한	승인 작업
→ CREATE USER	다른 오라클 사용자 생성을 피수여자에게 허용(DBA 역할을 위해 필요한 권한)
→ DROP USER	다른 사용자 제거
→ DROP ANY TABLE	임의의 스키마에서 테이블 제거
→ BACKUP ANY TABLE	export 유틸리티로 임의의 스키마에서 임의의 테이블 백업

* 스키마(Schema) 는 테이블(Table) , 뷰(View), 시퀀스(Sequence) 같은 객체의 모음입니다. 스키마는 데이터베이스 사용자에게 의해 소유되고 사용자와 동일이름을 가집니다.

* 실습을 위해서 SQL Plus 또는 SQL Command Line을 이용해야 합니다.

```

C:\Windows\system32\cmd.exe - sqlplus
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Park>sqlplus

SQL*Plus: Release 11.2.0.2.0 Production on 월 9월 23 22:17:46 2019

Copyright (c) 1982, 2014, Oracle. All rights reserved.

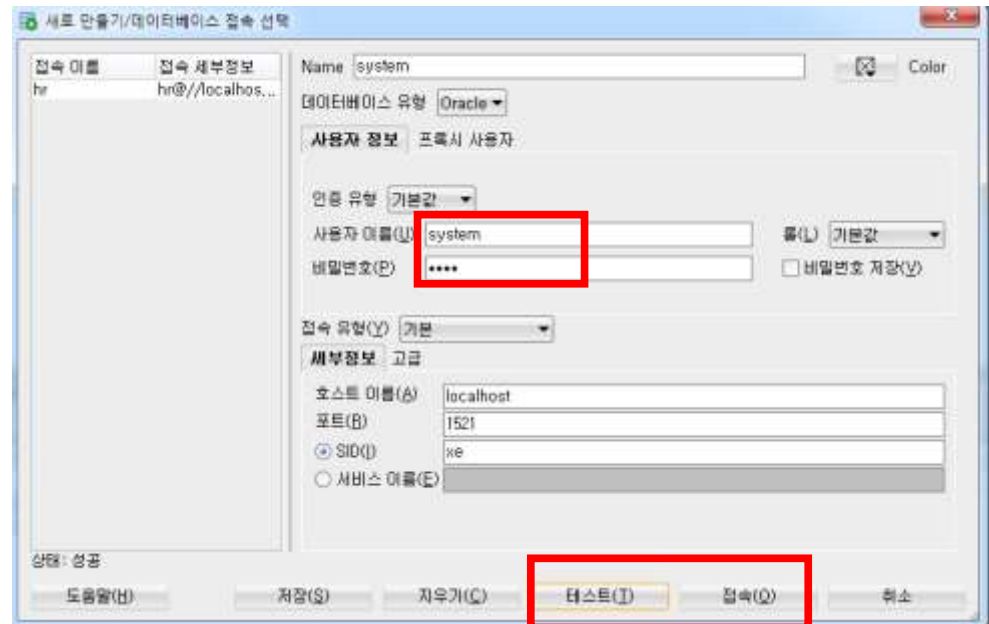
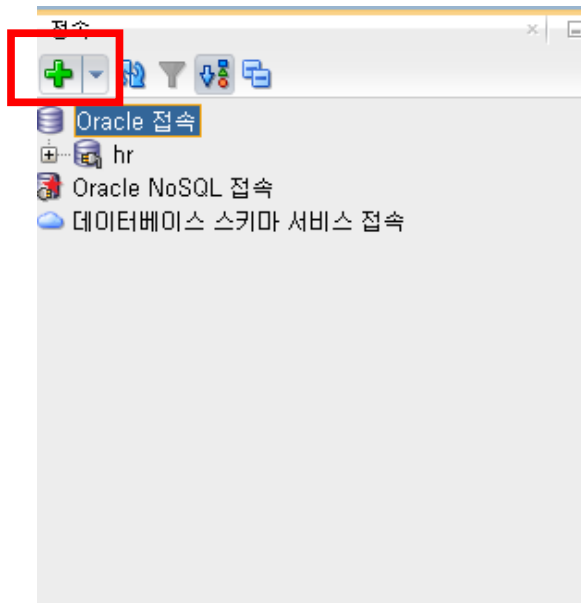
Enter user-name: system
Enter password:

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production
SQL> _

```

cmd
>sqlplus
>system
>비번

또는 sqlDeveloper를 이용합니다




권한
사용자 생성
시스템 권한
역할(ROLE)
비밀번호 변경
객체 권한



사용자 계정 생성

DBA는 CREATE USER 문장을 실행하여 사용자를 생성합니다. 사용자는 이때에는 어떤 권한도 가지지 않습니다. DBA는 이때 그 사용자에게 여러 권한을 부여합니다. 이 권한은 데이터베이스 수준에서 사용자가 할 수 있는 것이 무엇인가를 결정합니다. 슬라이드는 사용자 생성을 위해 요약된 구문을 제공합니다.



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

구문 형식에서...

- *user_name*: 생성되어야 하는 사용자 이름(아이디)입니다.
- *password*: 사용자의 로그인 비밀번호를 지정합니다.

다음 구문은 사용자를 생성합니다. 사용자를 생성하기 위해서 DBA 권한을 가진 사용자로 접속해야 합니다. **사용자의 아이디는 heojk이며, 비밀번호는 jinkyounng입니다.**

```
SQL> CONN sys /as sysdba
Enter password: <- sys 계정의 비밀번호를 입력하세요.
Connected.
SQL> CREATE USER heojk
  2 IDENTIFIED BY jinkyounng;

User created.
```

- SQL Developer에서 실행하려면 sys 계정으로 [새 접속]을 생성해야 합니다. 그러므로 SQL Plus 또는 SQL Command Line에서 실행하세요.

권한 사용자 생성 시스템 권한 역할(ROLE) 비밀번호 변경



생성된 계정에 권한 부여

일단 사용자가 생성되었다면, DBA는 사용자에게 대한 특정 시스템 권한을 부여할 수 있습니다. DBA는 사용자에게 시스템 권한을 부여하기 위해 GRANT 문장을 사용합니다. 일단 사용자가 권한을 부여받았으면, 사용자는 즉시 그 권한을 사용할 수 있습니다.

```
GRANT privilege [, privilege ...]  
TO    user_name [, user_name ...]  
WITH ADMIN OPTION;
```

구문 형식에서...

- *privilege* : 허가되는 시스템 권한입니다.
- *user_name* : 사용자 이름(아이디)입니다.
- WITH ADMIN OPTION : 시스템 권한을 부여하면서 그 권한을 제3자에게도 부여할 수 있는 권한을 줍니다. 이미 부여받은 시스템 권한은 해제 안 됩니다. B가 A에게 받은 시스템 권한을 C에게 부여했다면 A의 권한을 B에게 부여했다가 다시 회수하더라도 C에게 이미 부여된 시스템 권한은 해제 안 됩니다.

애플리케이션 개발자는 다음 시스템 권한을 가질 수 있습니다.

표 2. 시스템 권한

시스템 권한	승인 작업
CREATE SESSION	데이터베이스로 접속
CREATE TABLE	사용자의 스키마에서 테이블 생성
CREATE SEQUENCE	사용자의 스키마에서 시퀀스 생성
CREATE VIEW	사용자의 스키마에서 뷰 생성
CREATE PROCEDURE	사용자의 스키마에서 내장된 프로시저, 함수, 패키지 생성

다음 구문은 사용자 heojk에게 로그인 권한을 부여합니다.

```
SQL> GRANT create session TO heojk;
```

```
Grant succeeded.
```

다음 구문은 사용자 heojk에게 테이블, 시퀀스, 뷰를 생성하기 위해 권한을 부여합니다.

```
SQL> GRANT create table, create sequence, create view TO heojk;  
  
Grant succeeded.
```

CREATE TABLE 권한이 있더라도 디폴트 테이블 스페이스를 지정해 주고 테이블 스페이스 할당량을 정해줘야 테이블 생성이 가능합니다.

```
SQL> CONN heojk  
Enter password: <- heojk 계정의 비밀번호를 입력하세요.  
Connected.  
SQL> CREATE TABLE test (data VARCHAR2(10));  
CREATE TABLE test (data VARCHAR2(10))  
*  
ERROR at line 1:  
ORA-01950: no privileges on tablespace 'SYSTEM'
```

다음 구문은 DBA 사용자가 heojk 사용자에게 디폴트 테이블 스페이스를 USERS 테이블 스페이스로 지정합니다. USERS 테이블 스페이스를 사용할 수 있는 용량의 최대 제한이 설정합니다.

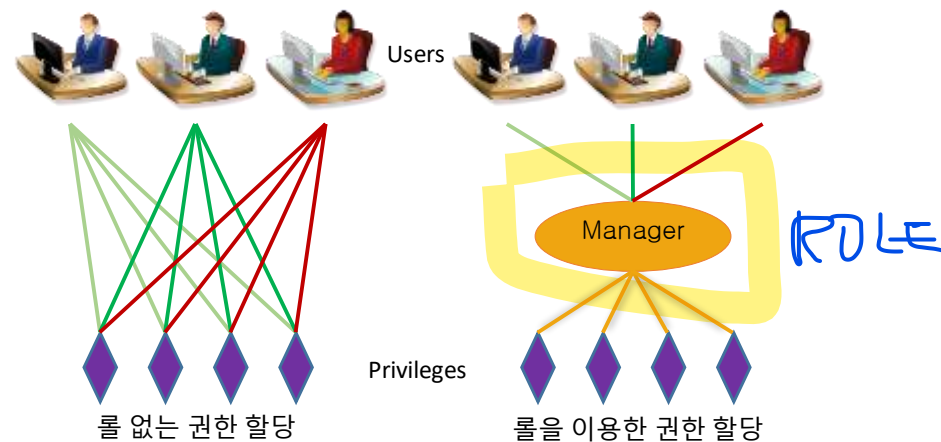
```
SQL> CONN sys /as sysdba
Enter password: <- sys 계정의 비밀번호를 입력하세요.
Connected.
SQL> ALTER USER heojk
  2 DEFAULT TABLESPACE USERS
  2 QUOTA UNLIMITED ON USERS;

User altered.

SQL> CONN heojk
Enter password: <- heojk 계정의 비밀번호를 입력하세요.
Connected.
SQL> CREATE TABLE test (data VARCHAR2(10));

Table created.
```

롤(ROLE)은 사용자에게 대해 부여될 수 있는 관련 권한의 그룹입니다. 롤은 권한을 부여하고 철회하는 것을 수행하고 유지하기 쉽게 합니다. 한 사용자가 여러 롤을 액세스할 수 있고 다른 여러 사용자에게 같은 롤을 지정할 수 있습니다.



롤을 사용하려면 우선 DBA는 롤을 생성해야 합니다. 롤이 생성되면, DBA는 롤에 대한 권한뿐만 아니라 롤을 사용자에게 할당하기 위한 GRANT 문장을 사용할 수 있습니다.

```
CREATE    ROLE  role_name;
```

구문 형식에서...

- *role_name* : 생성되어야 할 롤의 이름입니다.

* 오라클에 디폴트로 존재하는 **CONNECT, RESOURCE, DBA** 롤 등을 이용하면 해당 롤을 이용해서 쉽게 사용자에게 권한을 부여할 수 있습니다.

이제 사용자를 생성해서 테이블을 생성하고 사용할 수 있습니다.

아래 방법은 system계정으로 사용자 계정 생성과, 권한 부여를 초간단 하게 하는 방법입니다

```
CREATE user jsp IDENTIFIED BY jsp;  
--이미 지정된 권한부여 (테이블, 시퀀스, 뷰)  
GRANT connect, resource TO jsp;
```

권한 사용자 생성 시스템 권한 역할(ROLE) 비밀번호 변경



사용자 계정이 생성되었을 때, 각 사용자는 DBA가 초기화한 비밀번호를 갖게 됩니다. 사용자는 ALTER USER 문장을 사용하여 자신의 비밀번호를 수정할 수 있습니다.

```
ALTER USER user_name  
IDENTIFIED BY password;
```

구문 형식에서...

- *user_name* : 사용자 이름입니다.
- *password* : 새 비밀번호를 지정합니다.

다음 구문은 Eric이 관리자가 처음 지정한 비밀번호 apple123으로 접속합니다. 이후 Eric은 자신의 비밀번호를 eric123으로 변경합니다. 비밀번호가 변경된 후 eric123 비밀번호로 다시 접속합니다.

```
SQL> conn eric/apple123
Connected.
SQL> ALTER USER eric IDENTIFIED BY eric123;

User altered.

SQL> conn eric/eric123;
Connected.
SQL>
```