Session 11 GRANTING / REVOKING SYSTEM / OBJECT PRIVILEGES

```
The Oracle base remains unchanged with value /opt/oracle
 [oracle@oracloud12c ~]$ sqlplus / as sysdba

SQL*Plus: Release 12.1.0.2.0 Production on Thu Mar 22 10:30:29 2018

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

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options

SQL> set pagesize 200
```

In DATABASE EXPRESS we will create a new User (Account or Schema) named JANE by going Security → Users → Create User and then filling fields in 3 pages like below:

1) User Account

NAME: **JANE**

AUTHENTICATION choose button **PASSWORD**

PASSWORD: **jane**

PROFILE from the list pick **PROG**

PASSWORD EXPIRED leave this box **unchecked**

ACCOUNT LOCKED leave this box **unchecked**

2) Tablespace

DEFAULT TBSP from the list pick **MINE**

TEMPORARY TBSP from the list pick **TEMP**

3) Privilege

In the left pane find role **CONNECT** and promote it to the right pane

Now click on button **SHOW SQL** that will display the commands like below

```
create user JANE identified by ****** profile PROG account unlock
default  tablespace  MINE temporary tablespace TEMP;

grant CONNECT to  JANE;
```

Now, **click OK and again OK** and user will be created in DB Express.

*** We need to give our new user some space in her default tablespace (to be able to Add/Modify rows) ***

```
SQL> ALTER USER jane QUOTA 5M ON mine;
User altered.

SQL> SELECT username, account_status, default_tablespace, profile
     FROM dba_users
     WHERE  created > '31-JAN-18';

USERNAME
--------------------------------------------------------------------------------
ACCOUNT_STATUS                   DEFAULT_TABLESPACE
-------------------------------- ------------------------------
PROFILE
--------------------------------------------------------------------------------
TOM
OPEN                             MINE
DEFAULT

FOOBAR
OPEN                             MINE
PROG

JANE
OPEN                             MINE
PROG


SQL> DESC dba_sys_privs
 Name                                      Null?    Type
 ----------------------------------------- -------- --------------
 GRANTEE                                            VARCHAR2(128)
 PRIVILEGE                                          VARCHAR2(40)
 ADMIN_OPTION                                       VARCHAR2(3)
 COMMON                                             VARCHAR2(3)

SQL> SELECT COUNT(*) FROM DBA_SYS_PRIVS;

  COUNT(*)
----------
       997
```

*** It was 839 sys privs in Oracle 11g, and 580 in Oracle 10g ***

```
SQL> SELECT * FROM dba_sys_privs
     WHERE  grantee IN ('TOM','JANE','FOOBAR');

GRANTEE
--------------------------------------------------------------------------------
PRIVILEGE                                ADM COM
```

```
---------------------------------------- --- ---
TOM
CREATE TABLE                             NO  NO

FOOBAR
CREATE TABLE                             NO  NO
```

Jane does NOT have any system privileges granted yet (only Connect role)

```
SQL> GRANT CREATE TABLESPACE, SELECT_CATALOG_ROLE TO  tom ;
Grant succeeded.
```

We can add in one statement both SYS PRIVS and ROLES

```
SQL> GRANT CREATE TABLE,  RESOURCE TO  jane ;
 Grant succeeded.

SQL> SELECT * FROM dba_sys_privs
     WHERE  grantee IN ('TOM','JANE');

GRANTEE
--------------------------------------------------------------------------------
PRIVILEGE                                ADM COM
---------------------------------------- --- ---
TOM
CREATE TABLE                             NO  NO

JANE
CREATE TABLE                             NO  NO

TOM
CREATE TABLESPACE                        NO  NO
```

This view shows only sys privs granted and not ROLES (like Resource and Select_catalog_role)

SYSTEM PRIVILEGES AND CASCADING EFFECT

```
SQL> GRANT create any table TO tom
     WITH  ADMIN OPTION;

Grant succeeded.

SQL> CONN TOM/cat
Connected.
SQL> GRANT create any table TO jane;

Grant succeeded.

SQL> conn system/seneca
Connected.
SQL>
SQL> REVOKE create any table FROM tom;
```

```
Revoke succeeded.

SQL> CONN JANE/jane
Connected.
SQL> CREATE TABLE tom.play (
           col1 NUMBER(5) );

Table created.
```

← She can still create tables for other accounts

```
SQL> conn system/seneca
Connected.

SQL> SELECT * FROM dba_sys_privs
     WHERE  grantee IN ('TOM','JANE');

GRANTEE
--------------------------------------------------------------------------------
PRIVILEGE                                ADM COM
---------------------------------------- --- ---
TOM
CREATE TABLE                             NO  NO

JANE
CREATE TABLE                             NO  NO

TOM
CREATE TABLESPACE                        NO  NO

JANE
CREATE ANY TABLE                         NO  NO
```

*** This shows that revoking SYSTEM privilege from the user in the middle of the user chain will NOT cascade and break the chain, so user at the end of the chain will RETAIN it ***

In DATABASE EXPRESS we will grant some Object Privileges to user TOM by going Security → Users → select TOM and then under Tab called Object Privilges filling fields in 3 pages like below:

1) Select Schema

SCHEMA: pick from list **SCOTT**

OBJECT TYPE: pick from list **TABLE**

OBJECT NAME: **DEPT**

2) Select Objects

Just promote **DEPT** from the left to the right pane

3) Grant Privileges

Check the box for **Grantable**

Choose **INSERT** and **SELECT** in the left pane and promote it to the right pane

Now click on button **SHOW SQL** that will display the commands like below

```
grant SELECT, INSERT on SCOTT.DEPT to TOM with grant option;
```

Now, **click OK and again OK** and these 2 object privileges will be added to TOM

OBJECT PRIVILEGES AND CASCADING EFFECT

* **Notice that Object Privs can be granted by both DBA and OWNER of the object (here the object is table), unlike for System Privs that may be granted only by DBA ***

```
SQL> CONN TOM/cat ← He can grant his 2 object privs further and one will be given to Jane
Connected.
SQL> GRANT select ON scott.dept TO jane;
Grant succeeded.

SQL> desc dba_tab_privs
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------
 GRANTEE                                            VARCHAR2(128)
 OWNER                                              VARCHAR2(128)
 TABLE_NAME                                         VARCHAR2(128)
 GRANTOR                                            VARCHAR2(128)
 PRIVILEGE                                          VARCHAR2(40)
 GRANTABLE                                          VARCHAR2(3)
 HIERARCHY                                          VARCHAR2(3)
 COMMON                                             VARCHAR2(3)
 TYPE                                               VARCHAR2(24)

SQL> SELECT grantee, privilege, grantable, grantor
     FROM   dba_tab_privs
     WHERE OWNER = 'SCOTT' AND TABLE_NAME = 'DEPT';

GRANTEE
--------------------------------------------------------------------------------
PRIVILEGE                                GRA
---------------------------------------- ---
GRANTOR
--------------------------------------------------------------------------------
TOM
SELECT                                   YES
SCOTT

TOM
INSERT                                   YES
SCOTT
```

```
JANE
SELECT                                         NO
TOM


SQL> CONN scott/tiger
Connected.
SQL> REVOKE select ON scott.dept FROM tom;

Revoke succeeded.

SQL> CONN JANE/jane
Connected.
SQL> SELECT * FROM scott.dept;
SELECT * FROM scott.dept
                  *
ERROR at line 1:
ORA-01031: insufficient privileges
```

She lost her SELECT privilege by the cascade effect, we can see in the view the same thing

```
SQL> CONN SYSTEM/seneca
Connected.
SQL> SELECT grantee, privilege, grantable, grantor
     FROM   dba_tab_privs
     WHERE OWNER = 'SCOTT' AND TABLE_NAME = 'DEPT';

GRANTEE
--------------------------------------------------------------------------------
PRIVILEGE                                GRA
---------------------------------------- ---
GRANTOR
--------------------------------------------------------------------------------
TOM
INSERT                                   YES
SCOTT
```

*** This shows that revoking the OBJECT privilege from the user in the middle of the user chain will CASCADE and break the chain, so the user at the end of the chain will LOSE it ***

```
SQL> exit
Disconnected from Oracle Database 12c Enterprise Edition Release
12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options
[oracle@oracloud12c ~]$ exit
logout
```