

## Session 12 CREATING / ALTERING ROLES

The Oracle base remains unchanged with value /opt/oracle  
[oracle@oracloud12c ~]\$ **sqlplus /nolog**

SQL\*Plus: Release 12.1.0.2.0 Production on Mon Mar 26 21:11:56 2018

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

SQL> set pagesize 200

SQL> **CONN / AS SYSDBA**

Connected.

In DATABASE EXPRESS we will create a new Role named DEV by going **Security → Roles → Create Role** and then filling fields in 2 pages like below:

### 1) Create Role

ROLE NAME: **DEV**

### 2) Privileges ← Only System privs and Roles can be added here

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

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

```
create role DEV not identified;  
grant CONNECT, RESOURCE to DEV;
```

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

\* Since Oracle 12c **UNLIMITED TABLESPACE** system privilege is not included in the **RESOURCE** role and can not be granted to a Role. It may be given only to the User. In order to add some Object privileges to a created role we need to edit it later, in DB Express or on command line \*

In DATABASE EXPRESS we will grant some Object Privileges to our new Role DEV by going **Security → Roles → select DEV** and then under Tab called **Object Privileges** 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

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 DEV;
```

Now, click **OK** and again **OK** and Role DEV will be modified.

```
SQL> SELECT role FROM dba_roles ;
```

```
ROLE
```

```
-----  
CONNECT  
RESOURCE  
DBA  
AUDIT_ADMIN  
AUDIT_VIEWER  
SELECT_CATALOG_ROLE  
EXECUTE_CATALOG_ROLE  
DELETE_CATALOG_ROLE  
Etc...  
DEV
```

88 rows selected. → In Oracle11g we had 56 and in 10g only 33 pre-defined Roles

```
SQL> GRANT dev TO jane;
```

Grant succeeded.

```
SQL> desc dba_role_privs;
```

Name	Null?	Type
GRANTEE		VARCHAR2 (128)
GRANTED_ROLE		VARCHAR2 (128)
ADMIN_OPTION		VARCHAR2 (3)
DELEGATE_OPTION		VARCHAR2 (3)
DEFAULT_ROLE		VARCHAR2 (3)
COMMON		VARCHAR2 (3)

← This view shows ALL ROLES granted to either USERS or ROLES

```
SQL> SELECT grantee, granted_role FROM dba_role_privs  
WHERE grantee IN ('SCOTT','TOM','JANE','DEV')  
ORDER BY grantee;
```

```
GRANTEE
```

```
-----  
GRANTED_ROLE
```

```
-----  
DEV
```

```
RESOURCE
```

```
DEV
CONNECT
```

```
JANE
RESOURCE
```

```
JANE
CONNECT
```

```
JANE
DEV
```

```
SCOTT
RESOURCE
```

```
SCOTT
CONNECT
```

```
TOM
SELECT_CATALOG_ROLE
```

```
TOM
CONNECT
```

9 rows selected.

```
SQL> ALTER USER TOM DEFAULT ROLE ALL EXCEPT select_catalog_role;
User altered.
```

```
SQL> conn tom/cat
Connected.
```

```
SQL> desc dba_tables
ERROR:
ORA-04043: object "SYS"."DBA_TABLES" does not exist
```

← Tom lost ability to browse Data Dictionary, because select\_catalog\_role is not default now and Tom will not have it upon Login

```
SQL> conn / as sysdba
Connected.
```

← The role is enabled only if is the part of the DEFAULT ROLE group or if it is manually enabled with the ALTER USER .. DEFAULT ROLE or SET ROLE command.

```
SQL> SELECT granted_role, default_role FROM dba_role_privs
WHERE grantee = 'TOM';
```

```
GRANTED_ROLE
```

```
-----
```

```
DEF
```

```
----
```

```
SELECT_CATALOG_ROLE
NO
```

```
CONNECT
YES
```

```
SQL> CONN TOM/cat
Connected.
```

```
SQL> select * from session_privs;
```

```
PRIVILEGE
```

```
-----
SET CONTAINER
CREATE TABLE
CREATE TABLESPACE
CREATE SESSION
```

```
SQL> SELECT * FROM SESSION_ROLES;
```

```
ROLE
```

```
-----
CONNECT
```

```
SQL> SET ROLE select_catalog_role;
Role set.
```

```
SQL> desc dba_tables
```

Name	Null?	Type
-----	-----	-----
OWNER	NOT NULL	VARCHAR2 (128)
TABLE_NAME	NOT NULL	VARCHAR2 (128)
TABLESPACE_NAME		VARCHAR2 (30)
CLUSTER_NAME		VARCHAR2 (128)
IOT_NAME		VARCHAR2 (128)
STATUS		VARCHAR2 (8)
PCT_FREE		NUMBER
PCT_USED		NUMBER
INI_TRANS		NUMBER
MAX_TRANS		NUMBER
INITIAL_EXTENT		NUMBER
NEXT_EXTENT		NUMBER
MIN_EXTENTS		NUMBER
MAX_EXTENTS		NUMBER
PCT_INCREASE		NUMBER
FREELISTS		NUMBER
FREELIST_GROUPS		NUMBER
LOGGING		VARCHAR2 (3)
BACKED_UP		VARCHAR2 (1)
NUM_ROWS		NUMBER
BLOCKS		NUMBER
EMPTY_BLOCKS		NUMBER

AVG_SPACE	NUMBER
CHAIN_CNT	NUMBER
AVG_ROW_LEN	NUMBER
Etc ...	

← The browsing role is back, but other roles are out, because SET ROLE command sets only that role and unsets (disables) all other roles

```
SQL> SELECT * FROM SESSION_ROLES;
```

```
ROLE
```

```
-----
SELECT_CATALOG_ROLE
HS_ADMIN_SELECT_ROLE
```

```
SQL> SET ROLE ALL;
Role set.
```

```
SQL> SELECT * FROM SESSION_ROLES;
```

```
ROLE
```

```
-----
CONNECT
SELECT_CATALOG_ROLE
HS_ADMIN_SELECT_ROLE
```

```
SQL> CONN / AS SYSDBA
Connected
```

```
SQL> DESC ROLE_SYS_PRIVS
```

Name	Null?	Type
-----	-----	-----
ROLE		VARCHAR2 (128)
PRIVILEGE		VARCHAR2 (40)
ADMIN_OPTION		VARCHAR2 (3)
COMMON		VARCHAR2 (3)

← This view shows ALL SYSTEM PRIVS granted to ROLES

```
SQL> select * from role_sys_privs
      WHERE ROLE = 'CONNECT';
```

```
ROLE
```

```
-----
PRIVILEGE                                ADM  COM
-----  ---  ---
CONNECT
SET CONTAINER                            NO   YES

CONNECT
CREATE SESSION                            NO   YES
```

```
SQL> select privilege from role_sys_privs
      where role = 'RESOURCE';
```

```
PRIVILEGE
```

```
-----
CREATE SEQUENCE
CREATE TRIGGER
CREATE CLUSTER
CREATE PROCEDURE
CREATE TYPE
CREATE OPERATOR
CREATE TABLE
CREATE INDEXTYPE
```

```
8 rows selected.
```

```
SQL> select privilege from role_sys_privs
      where role = 'CONNECT';
```

```
PRIVILEGE
```

```
-----
SET CONTAINER
CREATE SESSION
```

```
SQL> select privilege from role_sys_privs
      where role = 'DEV';
```

```
no rows selected
```

```
SQL> DESC ROLE_TAB_PRIVS
```

Name	Null?	Type
-----	-----	-----
ROLE		VARCHAR2 (128)
OWNER		VARCHAR2 (128)
TABLE_NAME		VARCHAR2 (128)
COLUMN_NAME		VARCHAR2 (128)
PRIVILEGE		VARCHAR2 (40)
GRANTABLE		VARCHAR2 (3)
COMMON		VARCHAR2 (3)

← This view shows ALL OBJECT PRIVS granted ROLES

```
SQL> SELECT owner, table_name, privilege FROM role_tab_privs
      WHERE ROLE = 'DEV';
```

```
OWNER
```

```
-----
TABLE_NAME
```

```
-----
PRIVILEGE
```

```
SCOTT
DEPT
SELECT
```

```
SCOTT
DEPT
INSERT
```

← This view shows ALL ROLES granted to OTHER ROLES

```
SQL> DESC ROLE_ROLE_PRIVS
```

Name	Null?	Type
ROLE		VARCHAR2 (128)
GRANTED_ROLE		VARCHAR2 (128)
ADMIN_OPTION		VARCHAR2 (3)
COMMON		VARCHAR2 (3)

```
SQL> SELECT GRANTED_ROLE FROM ROLE_ROLE_PRIVS
      where role = 'RESOURCE';
```

no rows selected

```
SQL> SELECT GRANTED_ROLE FROM ROLE_ROLE_PRIVS
      where role = 'DEV';
```

```
GRANTED_ROLE
```

```
-----
CONNECT
RESOURCE
```

```
SQL> select count(granted_role) FROM ROLE_ROLE_PRIVS
      where role = 'DBA';
```

```
COUNT (GRANTED_ROLE)
-----
19
```

```
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
```