**Session 12 CREATING / ALTERING ROLES**

[oracle@oracledb19c ~]$ **sqlplus /nolog**

SQL\*Plus: Release 19.0.0.0.0 - Production on Tue Mar 22 11:40:29 2022

Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

SQL> set pagesize 120

SQL>

SQL> **conn / as sysdba**

Connected.

SQL> **CREATE ROLE dev; 🡪 only DBA can create a Role**

Role created.

SQL> **GRANT connect, resource, unlimited tablespace TO dev;**

GRANT connect, resource, unlimited tablespace TO dev

\*

ERROR at line 1:

ORA-01931: cannot grant UNLIMITED TABLESPACE to a role

**\* 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. \***

SQL> **GRANT connect, resource TO dev; 🡪 we can place other Roles into a Role**

Grant succeeded.

SQL> **GRANT create any table TO dev; 🡪 we can place Sys Priv(s) into a Role**

Grant succeeded.

SQL> **GRANT select, insert ON scott.dept TO dev;**

**🡪 we can place Tab (Object) Priv(s) into a Role**

Grant succeeded.

SQL> **GRANT dev TO foobar; 🡪 then we can add this Role to a User**

Grant succeeded.

SQL> **DESC dba\_roles**

Name Null? Type

----------------------------------------- -------- -------------------------

ROLE NOT NULL VARCHAR2(128)

ROLE\_ID NOT NULL NUMBER

PASSWORD\_REQUIRED VARCHAR2(8)

AUTHENTICATION\_TYPE VARCHAR2(11)

COMMON VARCHAR2(3)

ORACLE\_MAINTAINED VARCHAR2(1)

INHERITED VARCHAR2(3)

IMPLICIT VARCHAR2(3)

EXTERNAL\_NAME VARCHAR2(4000)

**🡪 this view gives us all Roles (pre-defined and custom-defined) in the Database**

SQL> **SELECT role FROM dba\_roles;**

ROLE

-----------------------------------------------------------------------------

**CONNECT**

**RESOURCE**

**DBA**

PDB\_DBA

AUDIT\_ADMIN

AUDIT\_VIEWER

SELECT\_CATALOG\_ROLE

EXECUTE\_CATALOG\_ROLE

CAPTURE\_ADMIN

EXP\_FULL\_DATABASE

IMP\_FULL\_DATABASE

CDB\_DBA

Etc …

DV\_REALM\_RESOURCE

**DEV**

90 rows selected. **🡪 this means, there are 89 pre-defined Roles in 19c,**

**While In Oracle12c we had 92 pre-defined Roles, in 11g we had 56 and in 10g only 33 roles**

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)

INHERITED 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','FOOBAR','DEV')**

**ORDER BY 1;**

GRANTEE

-----------------------------------------------------------------------------

GRANTED\_ROLE

-----------------------------------------------------------------------------

DEV

RESOURCE

DEV

CONNECT

FOOBAR

DEV

FOOBAR

RESOURCE

FOOBAR

CONNECT

SCOTT

CONNECT

SCOTT

RESOURCE

TOM

CONNECT

TOM

SELECT\_CATALOG\_ROLE

9 rows selected.

SQL> **conn tom/cat**

Connected.

SQL> **DESC dba\_objects**

Name Null? Type

----------------------------------------- -------- -------------------------

OWNER VARCHAR2(128)

OBJECT\_NAME VARCHAR2(128)

SUBOBJECT\_NAME VARCHAR2(128)

OBJECT\_ID NUMBER

DATA\_OBJECT\_ID NUMBER

OBJECT\_TYPE VARCHAR2(23)

CREATED DATE

LAST\_DDL\_TIME DATE

TIMESTAMP VARCHAR2(19)

STATUS VARCHAR2(7)

TEMPORARY VARCHAR2(1)

GENERATED VARCHAR2(1)

SECONDARY VARCHAR2(1)

NAMESPACE NUMBER

EDITION\_NAME VARCHAR2(128)

SHARING VARCHAR2(18)

EDITIONABLE VARCHAR2(1)

ORACLE\_MAINTAINED VARCHAR2(1)

APPLICATION VARCHAR2(1)

DEFAULT\_COLLATION VARCHAR2(100)

DUPLICATED VARCHAR2(1)

SHARDED VARCHAR2(1)

CREATED\_APPID NUMBER

CREATED\_VSNID NUMBER

MODIFIED\_APPID NUMBER

MODIFIED\_VSNID NUMBER

SQL> **conn / as sysdba**

Connected.

SQL> **ALTER USER tom DEFAULT ROLE ALL EXCEPT select\_catalog\_role;**

User altered.

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

SQL> **conn tom/cat**

Connected.

SQL> **DESC dba\_objects**

ERROR:

ORA-04043: object "SYS"."DBA\_OBJECTS" 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> REM DEFAULT ROLE { all | all except | role1, role2, ...| NONE}

SQL> **conn / as sysdba**

Connected.

SQL> **SELECT granted\_role, default\_role FROM dba\_role\_privs**

**WHERE grantee = 'TOM';**

GRANTED\_ROLE

-----------------------------------------------------------------------------

DEFAULT

-------

CONNECT

YES

SELECT\_CATALOG\_ROLE

NO

SQL> **conn tom/cat**

Connected.

SQL> **select \* from session\_privs; 🡪 User can check what Sys Privs he/she has**

PRIVILEGE

----------------------------------------

SET CONTAINER

CREATE TABLE

CREATE TABLESPACE

CREATE SESSION

SQL> **select \* from session\_roles; 🡪 User can check what Roles are Enabled now, and that is different from what Roles may be granted to him/her**

ROLE

-----------------------------------------------------------------------------

CONNECT

SQL> **set role dba;**

set role dba

\*

ERROR at line 1:

ORA-01924: role 'DBA' not granted or does not exist

**🡨 Regular User can not enable a Role for himself/herself, if that role was not granted in the first place (to that User). Even DBA can not do that, without granting that Role firstly.**

SQL> **set role select\_catalog\_role;**

Role set.

SQL> **desc dba\_objects**

Name Null? Type

----------------------------------------- -------- -------------------------

OWNER VARCHAR2(128)

OBJECT\_NAME VARCHAR2(128)

SUBOBJECT\_NAME VARCHAR2(128)

OBJECT\_ID NUMBER

DATA\_OBJECT\_ID NUMBER

OBJECT\_TYPE VARCHAR2(23)

CREATED DATE

LAST\_DDL\_TIME DATE

TIMESTAMP VARCHAR2(19)

STATUS VARCHAR2(7)

TEMPORARY VARCHAR2(1)

GENERATED VARCHAR2(1)

SECONDARY VARCHAR2(1)

NAMESPACE NUMBER

EDITION\_NAME VARCHAR2(128)

SHARING VARCHAR2(18)

EDITIONABLE VARCHAR2(1)

ORACLE\_MAINTAINED VARCHAR2(1)

APPLICATION VARCHAR2(1)

DEFAULT\_COLLATION VARCHAR2(100)

DUPLICATED VARCHAR2(1)

SHARDED VARCHAR2(1)

CREATED\_APPID NUMBER

CREATED\_VSNID NUMBER

MODIFIED\_APPID NUMBER

MODIFIED\_VSNID NUMBER

**🡨 The browsing dictionary 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)

INHERITED VARCHAR2(3)

**🡨 This view shows ALL SYSTEM PRIVS granted to ROLES**

SQL> **SELECT role, privilege, admin\_option**

**from role\_sys\_privs**

**WHERE ROLE = 'CONNECT';**

ROLE

-----------------------------------------------------------------------------

PRIVILEGE ADM

---------------------------------------- ---

CONNECT

SET CONTAINER NO

CONNECT

CREATE SESSION NO

SQL> **SELECT privilege FROM role\_sys\_privs**

**WHERE role = 'RESOURCE';**

PRIVILEGE

----------------------------------------

CREATE SEQUENCE

CREATE PROCEDURE

CREATE CLUSTER

CREATE INDEXTYPE

CREATE OPERATOR

CREATE TYPE

CREATE TRIGGER

CREATE TABLE

8 rows selected.

SQL> **SELECT COUNT(privilege) FROM role\_sys\_privs**

**WHERE role = 'DBA';**

COUNT(PRIVILEGE)

----------------

235

SQL> **select privilege from role\_sys\_privs**

**where role = 'DEV';**

PRIVILEGE

----------------------------------------

CREATE ANY TABLE

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)

INHERITED VARCHAR2(3)

**🡨 This view shows ALL OBJECT PRIVS granted to ROLES**

SQL> **SELECT owner, table\_name, privilege FROM role\_tab\_privs**

**WHERE ROLE = 'DEV';**

OWNER

-----------------------------------------------------------------------------

TABLE\_NAME

-----------------------------------------------------------------------------

PRIVILEGE

----------------------------------------

SCOTT

DEPT

INSERT

SCOTT

DEPT

SELECT

SQL> **DESC role\_role\_privs**

Name Null? Type

----------------------------------------- -------- -------------------------

ROLE VARCHAR2(128)

GRANTED\_ROLE VARCHAR2(128)

ADMIN\_OPTION VARCHAR2(3)

COMMON VARCHAR2(3)

INHERITED VARCHAR2(3)

**🡨 This view shows ALL ROLES granted to OTHER ROLES**

SQL> **SELECT GRANTED\_ROLE FROM ROLE\_ROLE\_PRIVS**

**where role = 'RESOURCE';**

GRANTED\_ROLE

-----------------------------------------------------------------------------

SODA\_APP

SQL> **SELECT GRANTED\_ROLE FROM ROLE\_ROLE\_PRIVS**

**WHERE role = 'DEV';**

GRANTED\_ROLE

-----------------------------------------------------------------------------

RESOURCE

CONNECT

SQL> **SELECT COUNT(GRANTED\_ROLE) FROM ROLE\_ROLE\_PRIVS**

**WHERE role = 'DBA';**

COUNT(GRANTED\_ROLE)

-------------------

17

SQL> **EXIT**