***SESSION 10 PRIVILEGES /ROLES***

Last login: Fri Mar 18 10:08:16 2022 from 10.30.2.33

[student@oracledb19c ~]$ **su - oracle**

Password:

Last login: Tue Mar 8 11:54:15 EST 2022 on pts/1

The Oracle base remains unchanged with value /opt/oracle/app/oracle

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

SQL\*Plus: Release 19.0.0.0.0 - Production on Fri Mar 18 10:12:53 2022

Version 19.3.0.0.0

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

Last Successful login time: Tue Feb 22 2022 13:17:04 -04:00

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production

Version 19.3.0.0.0

SQL> **set pagesize 120**

SQL> **conn / as sysdba**

Connected.

SQL> **DESC dba\_sys\_privs**

Name Null? Type

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

GRANTEE VARCHAR2(128)

PRIVILEGE VARCHAR2(40)

ADMIN\_OPTION VARCHAR2(3)

COMMON VARCHAR2(3)

INHERITED VARCHAR2(3)

**🡪 This view shows only Sys Privs granted and not ROLES (like Resource)**

SQL> **SELECT COUNT(\*) FROM DBA\_SYS\_PRIVS;**

COUNT(\*)

----------

935

**\* It was 1038 different Sys Privs in Oracle 12c, 839 in 11g, and only 580 in 10g \***

SQL> **SELECT grantee, privilege, admin\_option FROM dba\_sys\_privs**

**WHERE grantee IN ('TOM','SCOTT','FOOBAR');**

GRANTEE

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

PRIVILEGE ADM

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

TOM

CREATE TABLE NO

FOOBAR

CREATE TABLE NO

SCOTT

UNLIMITED TABLESPACE NO

SQL> **GRANT CREATE TABLESPACE, SELECT\_CATALOG\_ROLE TO tom ;**

Grant succeeded.

**🡪 We can add in one statement both SYS PRIVS and ROLES**

SQL> **GRANT resource TO foobar;**

Grant succeeded.

SQL> **SELECT grantee, privilege, admin\_option FROM dba\_sys\_privs**

**WHERE grantee IN ('TOM','SCOTT','FOOBAR');**

GRANTEE

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

PRIVILEGE ADM

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

TOM

CREATE TABLE NO

FOOBAR

CREATE TABLE NO

SCOTT

UNLIMITED TABLESPACE NO

TOM

CREATE TABLESPACE NO

**🡪 Again, this view shows only Sys Privs granted and not ROLES (like 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 foobar;**

Grant succeeded.

SQL> **SELECT grantee, privilege, admin\_option FROM dba\_sys\_privs**

**WHERE grantee IN ('TOM','SCOTT','FOOBAR');**

GRANTEE

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

PRIVILEGE ADM

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

TOM

CREATE ANY TABLE YES

TOM

CREATE TABLE NO

FOOBAR

CREATE ANY TABLE NO

FOOBAR

CREATE TABLE NO

SCOTT

UNLIMITED TABLESPACE NO

TOM

CREATE TABLESPACE NO

6 rows selected.

SQL> **conn / as sysdba**

Connected.

SQL> **REVOKE CREATE ANY TABLE FROM tom;**

Revoke succeeded.

SQL> **SELECT grantee, privilege, admin\_option FROM dba\_sys\_privs**

**WHERE grantee IN ('TOM','SCOTT','FOOBAR');**

GRANTEE

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

PRIVILEGE ADM

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

TOM

CREATE TABLE NO

FOOBAR

CREATE ANY TABLE NO

FOOBAR

CREATE TABLE NO

SCOTT

UNLIMITED TABLESPACE NO

TOM

CREATE TABLESPACE 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 \***

***OBJECT PRIVILEGES AND CASCADING EFFECT***

\* **Notice that Tab (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> **grant SELECT, INSERT on SCOTT.DEPT to TOM with grant option;**

Grant succeeded.

SQL> **GRANT SELECT, DELETE ON scott.emp TO FOOBAR;**

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)

INHERITED VARCHAR2(3)

**🡪 This view shows only Tab (Object) Privs granted and by checking “grantor” column, you can see who granted that privilege**

SQL> **SELECT grantee, privilege, grantable, grantor, TABLE\_NAME**

**FROM dba\_tab\_privs**

**WHERE OWNER = 'SCOTT';**

GRANTEE

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

PRIVILEGE GRA

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

GRANTOR

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

TABLE\_NAME

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

FOOBAR

DELETE NO

SCOTT

EMP

TOM

INSERT YES

SCOTT

DEPT

FOOBAR

SELECT NO

SCOTT

EMP

TOM

SELECT YES

SCOTT

DEPT

SQL> **conn tom/cat**

Connected.

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

Grant succeeded.

SQL> **SELECT grantee, privilege, grantable, grantor, TABLE\_NAME**

**FROM dba\_tab\_privs**

**WHERE OWNER = 'SCOTT';**

GRANTEE

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

PRIVILEGE GRA

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

GRANTOR

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

TABLE\_NAME

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

FOOBAR

SELECT NO

TOM

DEPT

FOOBAR

DELETE NO

SCOTT

EMP

FOOBAR

SELECT NO

SCOTT

EMP

TOM

INSERT YES

SCOTT

DEPT

TOM

SELECT YES

SCOTT

DEPT

FOOBAR

INSERT NO

TOM

DEPT

6 rows selected.

SQL> **conn / as sysdba**

Connected.

SQL>

SQL> **REVOKE select, insert ON scott.dept FROM tom;**

Revoke succeeded.

SQL> **SELECT grantee, privilege, grantable, grantor, TABLE\_NAME**

**FROM dba\_tab\_privs**

**WHERE OWNER = 'SCOTT';**

GRANTEE

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

PRIVILEGE GRA

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

GRANTOR

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

TABLE\_NAME

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

FOOBAR

DELETE NO

SCOTT

EMP

FOOBAR

SELECT NO

SCOTT

EMP

**\* 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 19c Enterprise Edition Release 19.0.0.0.0 - Production

Version 19.3.0.0.0