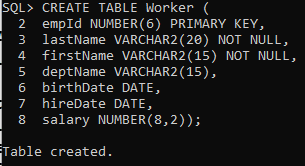
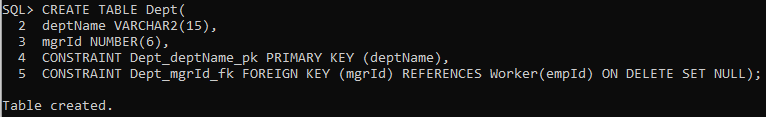
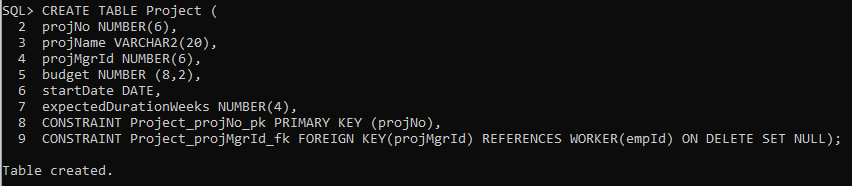
**Chapter 8 - Laboratory Exercise: Exploring Oracle’s Authorization System – Tom Alex**

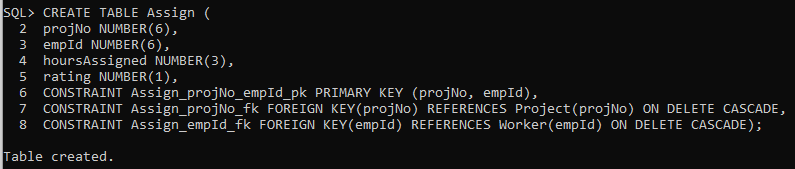
**Step 8.1 - Open the text file called: *Fig\_5.3\_DDL&InsertsforWorkerDeptProjectAssign.txt* located in this directory.**

**Step 8.2 - Create the Worker, Dept, Project, and Assign tables in the database as shown in Figure 5.3 in the textbook.** Show your work by providing screenshots of executing the CREATE TABLE SQL statements in the database.

****

****

****

****

**Step 8.3 - For each step: Draw an authorization graph by hand or by using a drawing tool, showing the privileges given. Design SQL statements that will be executed in the database. Then execute the SQL statements in the database.** Show your work by providing screenshots of executing the SQL statements in the database along with the results.

Step 8.3.a - Create five users: U100, U101, U102, U103, and U104.

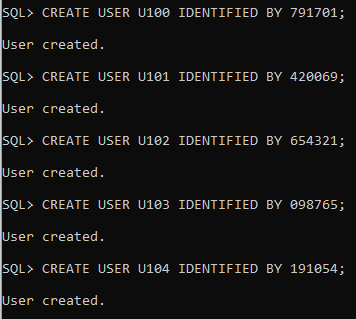
CREATE USER U100 IDENTIFIED BY 791701;

CREATE USER U101 IDENTIFIED BY 420069;

CREATE USER U102 IDENTIFIED BY 654321;

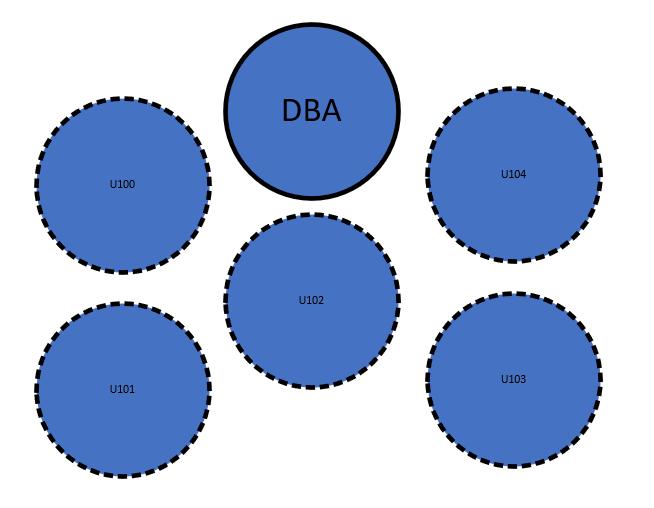
CREATE USER U103 IDENTIFIED BY 098765;

CREATE USER U104 IDENTIFIED BY 191054;



No privileges given yet.

Authorization graph for 8.3a on next page



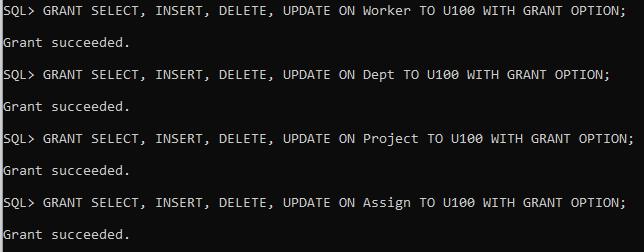
Step 8.3.b - Give user U100 the SELECT, INSERT, DELETE, UPDATE privileges on all four tables, with grant option.

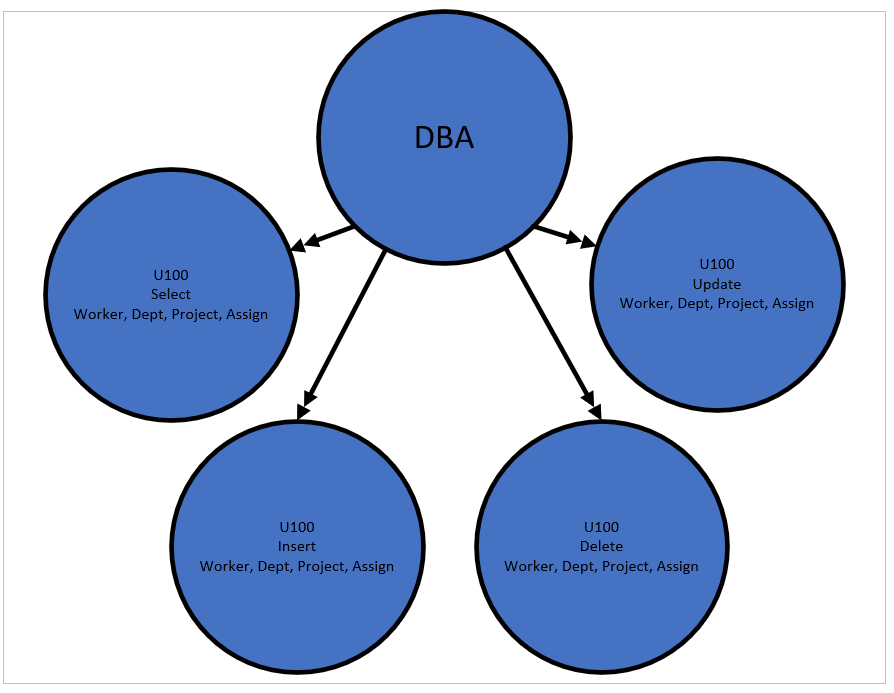
GRANT SELECT, INSERT, DELETE, UPDATE ON Worker TO U100 WITH GRANT OPTION;

GRANT SELECT, INSERT, DELETE, UPDATE ON Dept TO U100 WITH GRANT OPTION;

GRANT SELECT, INSERT, DELETE, UPDATE ON Project TO U100 WITH GRANT OPTION;

GRANT SELECT, INSERT, DELETE, UPDATE ON Assign TO U100 WITH GRANT OPTION;





Step 8.3.c - Connect as U100 and pass the SELECT privilege on all four tables to U101 and U102, with grant option.

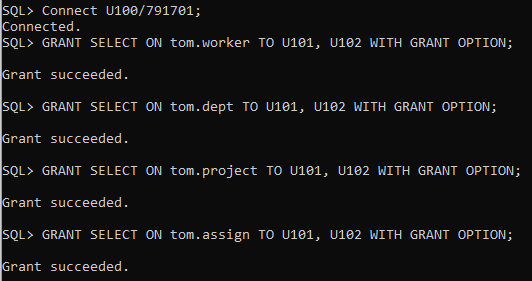
Connect U100/791701;

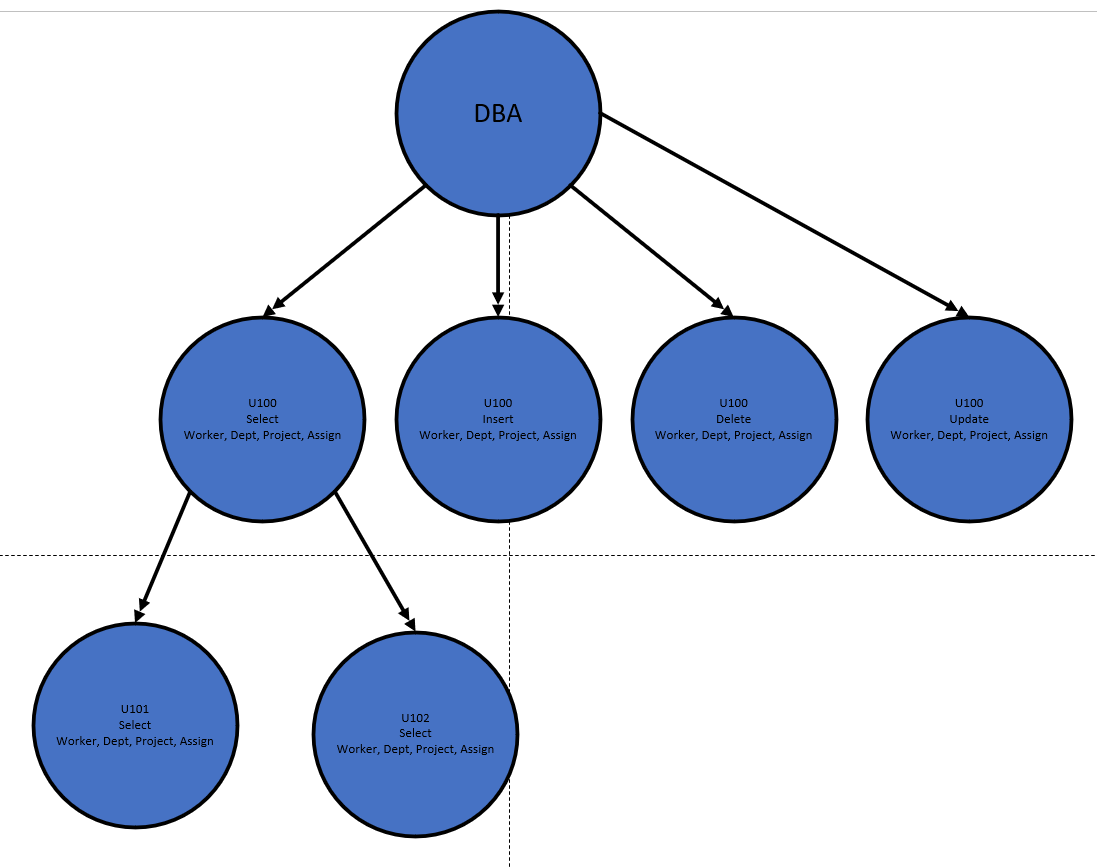
GRANT SELECT ON tom.worker TO U101, U102 WITH GRANT OPTION;

GRANT SELECT ON tom.dept TO U101, U102 WITH GRANT OPTION;

GRANT SELECT ON tom.project TO U101, U102 WITH GRANT OPTION;

GRANT SELECT ON tom.assign TO U101, U102 WITH GRANT OPTION;

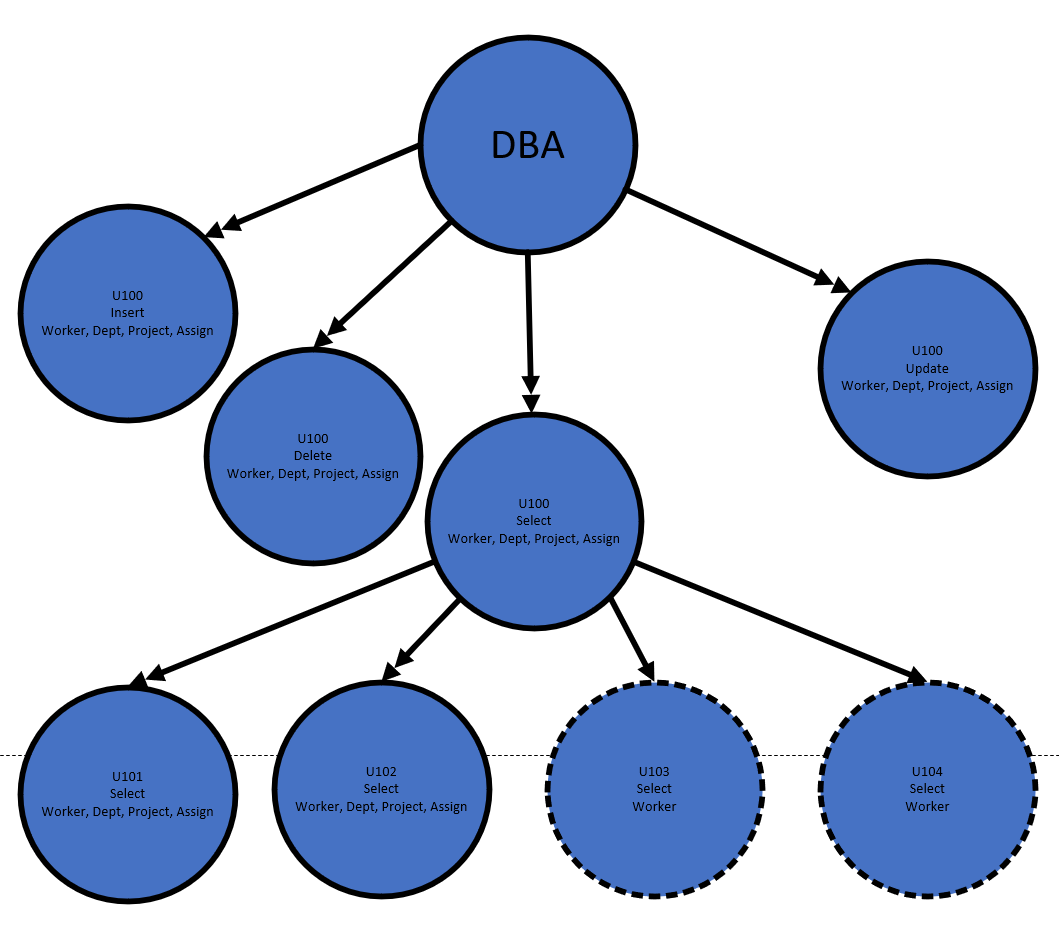


****

Step 8.3.d - Still acting as U100, pass the SELECT privilege on Worker to U103 and U104, without the grant option.

GRANT SELECT ON tom.worker TO U103, U104;



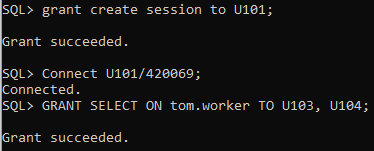


Step 8.3.e - Connect as U101 and pass the SELECT privilege on Worker to U103 and U104, without the grant option.

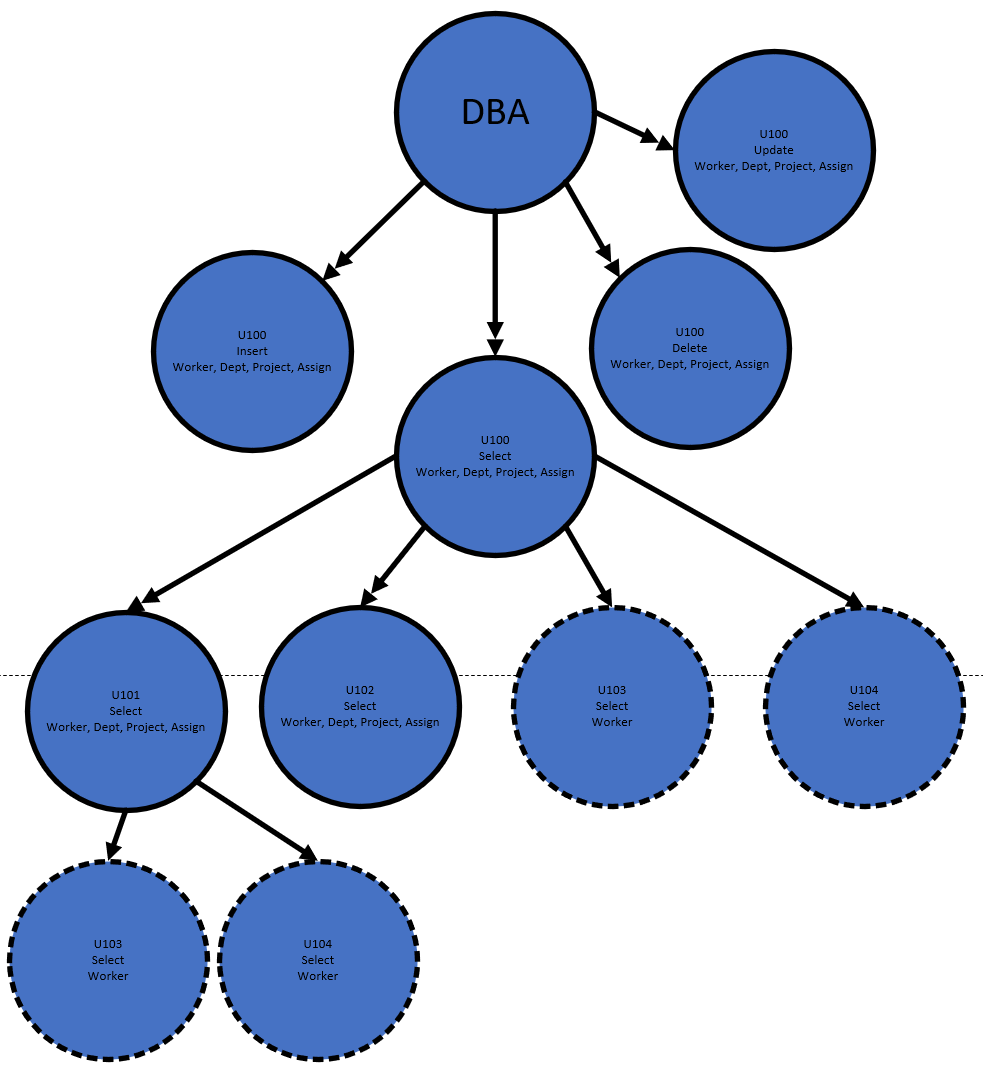
Grant create session to U101;

Connect U101/420069;

GRANT SELECT ON tom.worker TO U103, U104;



**Authorization graph for 8.3e on next page.**



Step 8.3.f - Connect as U100 and revoke all privileges you granted to U101.

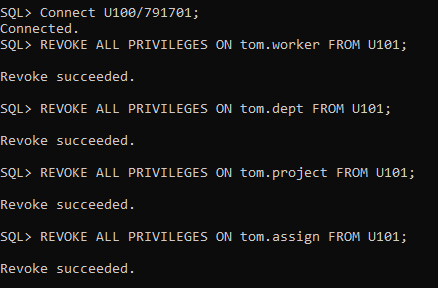
Connect U100/791701;

REVOKE ALL PRIVILEGES ON tom.worker FROM U101;

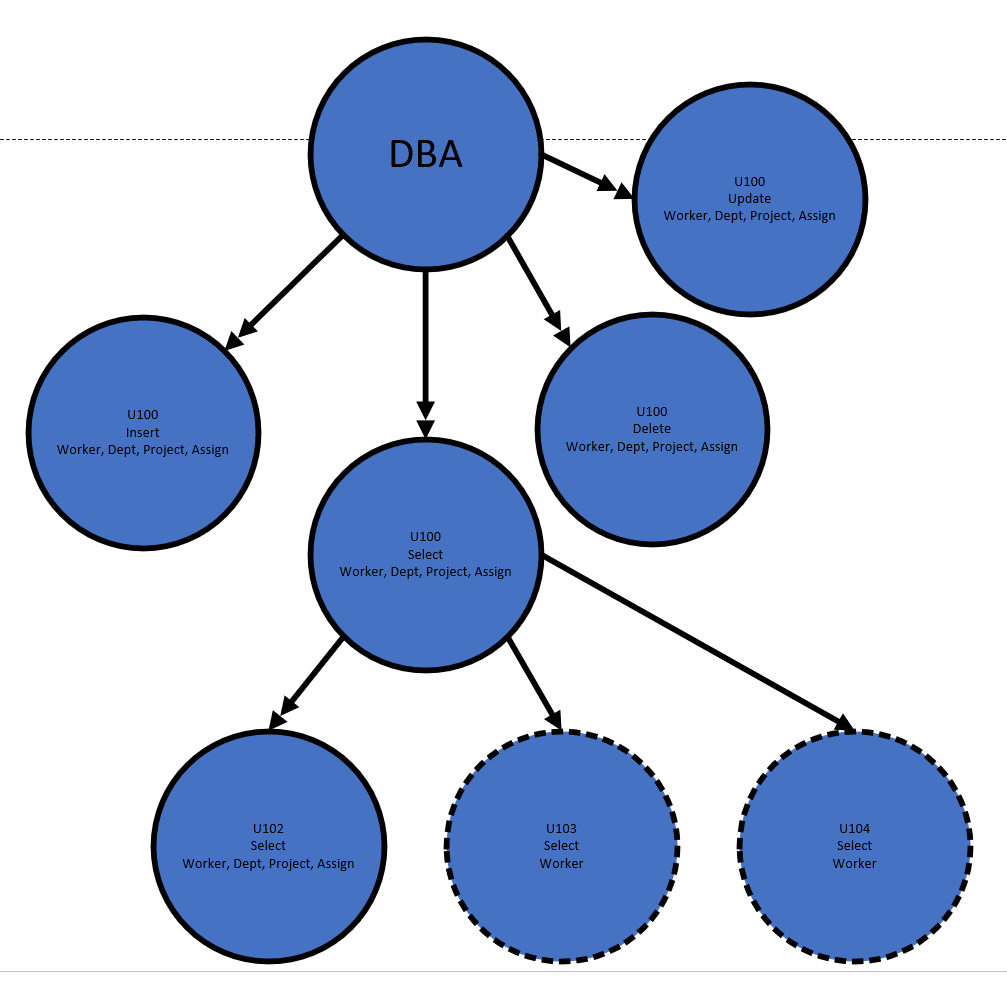
REVOKE ALL PRIVILEGES ON tom.dept FROM U101;

REVOKE ALL PRIVILEGES ON tom.project FROM U101;

REVOKE ALL PRIVILEGES ON tom.assign FROM U101;

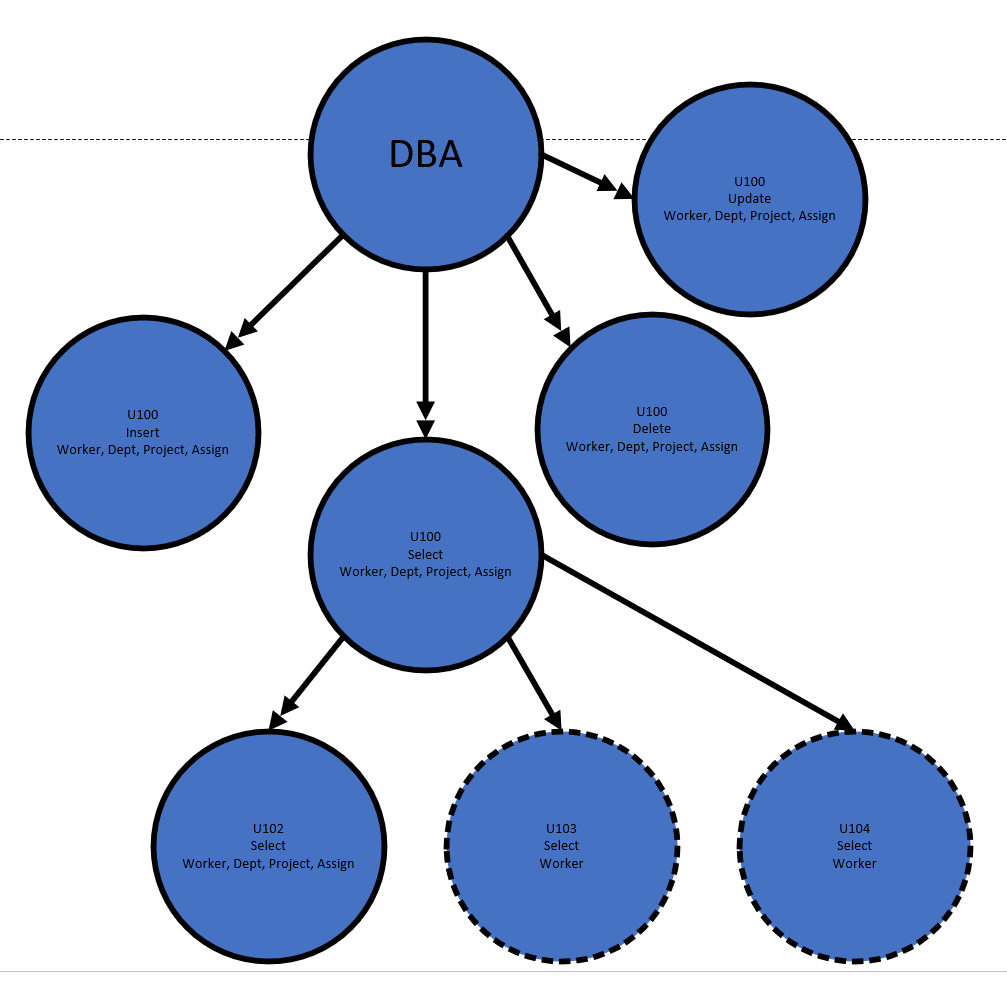


**Authorization graph for 8.3f on next page.**



Step 8.3.g - From the authorization graph, determine what privileges, if any, the remaining users should still have.

* user U100 has SELECT, INSERT, DELETE, UPDATE privileges on all four tables, with grant option.
* user U102 has SELECT privilege on all four tables, with grant option.
* user U103 has SELECT privilege on all Worker table, without grant option.
* user U104 has SELECT privilege on all Worker table, without grant option.



Step 8.3.h - Confirm these privileges by selecting the table privileges for each user from the sys.dba\_tab\_privs data dictionary view. Use the following format and display your results:

col owner format a20

col table\_name format a15

col privilege format a10

col grantee format a10

SELECT owner,privilege,table\_name,grantee

FROM sys.dba\_tab\_privs

WHERE grantee like 'U1%'

ORDER BY grantee, table\_name, privilege;

