Name: Sarvesh Kaushik Lab09

Instructor: Luke Papademas

**STEP 1:** **Using DCL ( Data Control Languages ) Statements**

Explain the following DCL statements, then execute the statements.

1. **GRANT SELECT On dept TO sam, lynnette;**

The above query will return error message as the user role SAM does not exists. To successfully execute above query, one must create a user profile SAM and execute the GRANT data control command.

****

1. **GRANT INSERT On dept TO scott;**

GRANT Data Control Command will be used to grant Insert permission on dept for user profile scott. Consider the following snapshot indicating successful insert grant for user scott.

****

3> **REVOKE SELECT, INSERT ON dept TO scott;**

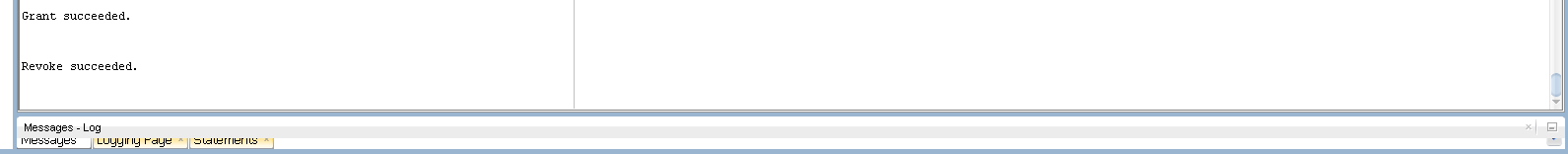
The above statement will cause the syntax error. We will have to edit above query and replace TO with FROM to get the desired results.

Moreover, We haven’t given the Select authorization to scott, it is important to first initiate the SELECT on scott and then revoke the select and previously assigned Insert.

The sequqnce in which queries will be executed are as follows,

GRANT SELECT On dept TO scott;

**REVOKE SELECT, INSERT ON dept FROM scott;**

****

4> **Create the role of Director of IT and assign the role to Tim Stokes**

**In order to create the role of the ITDirector we can use CREATE ROLE command as given below,**

**CREATE ROLE DIRECTOR\_OF\_IT;**

**after creating the role we will have to create a USER profile for TimStokes by using CREATE USER command as follows,**

**CREATE USER TimStokes IDENTIFIED BY SCOTT;**

**With help of data control command GRANT we can assign a specific role to the user as**

**GRANT DIRECTOR\_OF\_IT TO TimStokes;**

**Graphical user interface, text, application, Word

Description automatically generated**

**5> Create a new role named order\_entry with the password** **xyz123 .**

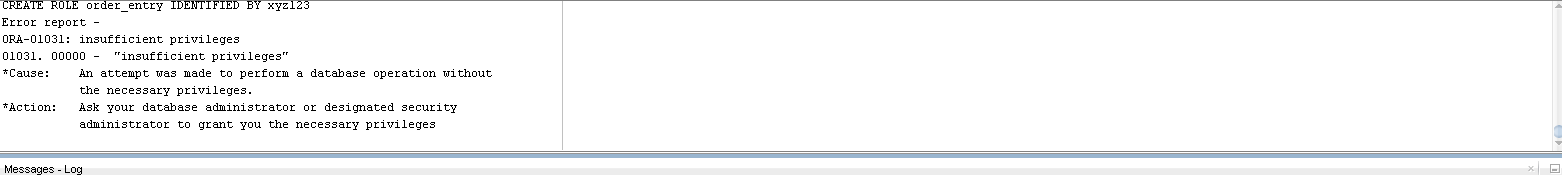
CREATE ROLE order\_entry IDENTIFIED BY xyz123

**The above query will create a new role named order\_entry and will be used to add the password for the role as xyz123.**

**GRANT operation will be used to add the permission for the user role.**

**GRANT SELECT On orders TO order\_entry;**

**GRANT SELECT On order\_items TO order\_entry;**

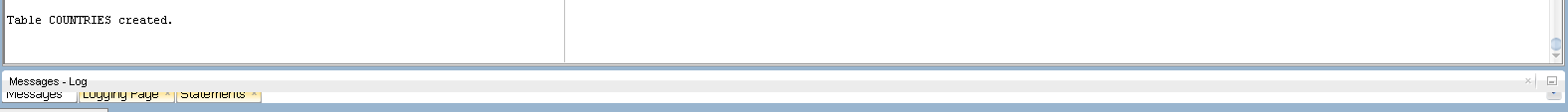
****

**Create the table countries and then execute the Commit.**

**CREATE TABLE countries**

**(COUNTRY\_ID CHAR(2) NOT NULL,**

**COUNTRY\_NAME VARCHAR2(40), REGION\_ID NUMBER);**



**Populating the Countries Table**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('CA','Canada', 2);**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('DE','Germany', 1);**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('UK','United Kingdom', 1);**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('US','United States of America', 2);**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('IN','India', 3);**

**Commit;**

**Execute a Commit and then select all fields from the table.**

**SELECT \* FROM COUNTRIES;**

**Graphical user interface, text, application

Description automatically generated**

**Insert the country Greece and execute a Commit statement.**

**Consider the following query performing the insert in countries**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID)**

**VALUES ('GR', 'Greece',1);**

**Commit;**

**Graphical user interface, application, Word

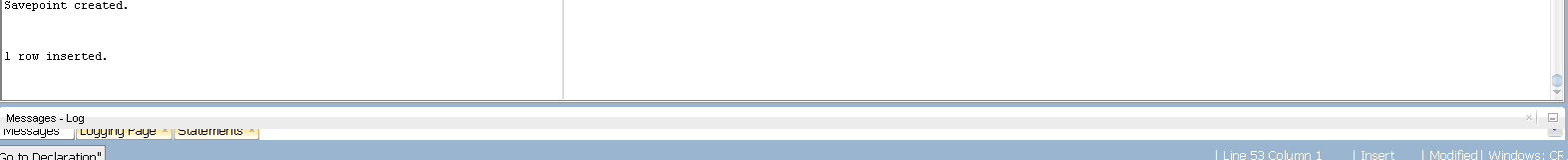
Description automatically generated**

**Create a SAVEPOINT using the initials of your first and last name as a prefix to the word SAVEPOINT ( e.g., fl\_countries\_1 ) .**

**SAVEPOINT SARVESH\_KAUSHIK;**

**Perform the Following Operations**

**INSERT INTO countries(COUNTRY\_ID, COUNTRY\_NAME, REGION\_ID) VALUES ('MX', 'Mexico',2);**

****

**SELECT \* FROM countries;**

**Graphical user interface

Description automatically generated**

**rollback TO SARVESH\_KAUSHIK;**

**Application

Description automatically generated with medium confidence**

**SELECT \* FROM countries;**

**commit;**

****

**In the above transactions we are first inserting a new record in the data table country. we are committing this transaction saving the details in the database. In the next step we are creating a save point which acts as a market to which partial rollback can be performed. After that we again insert a new record and select all the records from the database. The newly added record will be shown in the database.**

**If we perfom a rollback now the transaction will make previously inserted record invalid. We will see the transaction has successfully rollback to the savepoint SARVESH\_KAUSHIK.**

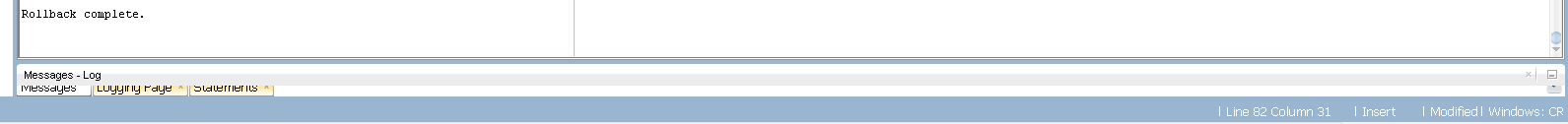
**Insert another record for the country of The Netherlands, then**

**INSERT INTO countries(COUNTRY\_ID,COUNTRY\_NAME,REGION\_ID)**

**VALUES ('NT', 'Netherlands',1);**

**Perform a rollback to the second SAVEPOINT, and then perform a select ( all fields ) for the table.**

**ROLLBACK TO SARVESH\_KAUSHIK;**



**SELECT \* FROM countries**

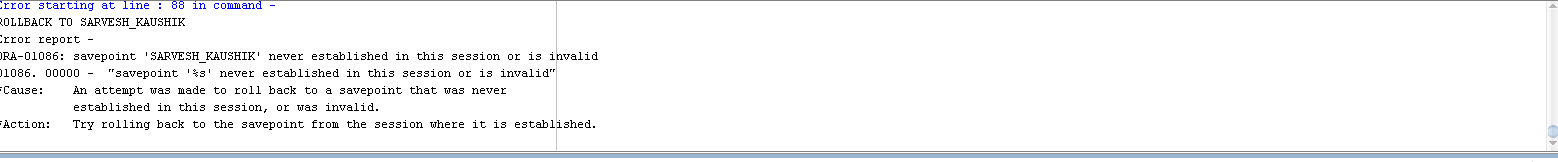
Graphical user interface, application, Word

Description automatically generated

**Perform a rollback to the first SAVEPOINT and paste your snapshot of the message received from the server.**

**ROLLBACK TO SARVESH\_KAUSHIK;**

**The Rollback to the first Savepoint will return error report as we have used the commit after the first rollback in our previous transaction. Due to which after using the commit, practically there is no SavePoint left before that SavePoint.**



**For each of the following scenarios, suggest what steps the DBA the IT Director should perform:**

**Tammy Smyth, a loyal employee who has worked for DDD Incorporated for ten years, announced her retirement and gave the " usual " two weeks’ notice.**

As a Tammy Smith is a former employee, she must be having a specific user role assigned to her in the organization. The role assigned to Tammy will have the privileges. The one of the significant step DBA and IT Director could perform is start the Privilege Revoking Schedule for Tammy.

As Tammy no longer organization employees, according to the organization policy she should only have access to those databases which are designed for the former employees. All the core employee privileges should be revoked from her account on hermoveout day.

**Jennie Sanders, as soon as she was suspected of employee theft, was immediately terminated. She ran the retail department for Big Blue Mart.**

As Jennie Sanders as committed a heinous crime it is responsibility of the DBA and IT director to prevent sensitive data and information from getting into wrong hands. IT Director should revoke all privileges from Jennies account and ban her account for Further access due the fraud she has committed.

**Marina Pappas, who currently works at the research and development facility as a chemist and formulates new products, has been recruited by another department to development the operations research program for the company. She has accepted the new position.**

The Organization can have employees working for more than one department. DBA and IT Director must verify that after taking the new role if Marina will be working with her previous department or not. Alter Role command would be useful to assign Maria on the new role with modified privileges. If she needs combination of the privileges from her previous role and all the privileges from the new role then DBA could create a Customized role for Maria allowing her to access the companies departmental database.

**What are the best practices to ensure security on a database using such an IDE as SQL Developer?**

The Effective Security Measures in the SQL Developer can be established with the help of Transaction Control Language and Data Control Language. The proper utilization of Grant and Revoke commands would allow authorized use profiles to access the sensitive information in the databases.

Oracle provides the DBA access to DBA Tab from the file menu. It can be effectively used to see the current user grants. The security can be established by setting up the strong admin username and the passwords.

Backup Servers are one of the important factors to consider when we see the database security. As the data stored on the server subject to data leak or data loss, to prevent data loss and ensure data integrity the backup server can be used to save the users private data securely. If the main server is down, you can always use the backup server to retrieve the correct data.

Prevent SQL Injection by utilizing the Stored Procedure in oracle developer instead of the direct queries for developing the web application. The stored procedures will provide an extra layer of abstraction that will allow server hide the actual query structure from the end user.

Distinguish between a role, a profile, and a privilege. Support your answer (please use APA for your citations).

In the oracle database the data governance is effectively established with TCL and DCL. The roles in the Oracle Developer implements visibility of different content in the database. The user profiles define the accessibility for a particular user in the database. Database privileges are allowing DBA to put a filter on database users functionality. Database Privileges comes under the Data Control Language and accomplished with the help of Grant and Revoke commands.

To create new user role following command can be used effectively.

CREATE ROLE rolenaame [IDENTFIED BY PASSOWRD]

To assign the privileges to the user following syntax can be effectively utilized.

**GRANT SELECT On dept TO sam, lynnette;**

**GRANT SELECT, INSERT On dept TO sam, lynnette;**

The new user profiles can be created by right clicking on the other user tab and creating new user with username and password. Moreover, New profile tab gives you the flexibility to Generate Roles. Assign the System Privileges, Assign the appropriate quotas and also help to write the SQL queries.

Graphical user interface, text, application, email

Description automatically generated

References:

*Database Security Guide*. (20018). Docs.Oracle.Com. <https://docs.oracle.com/cd/B19306_01/network.102/b14266/admusers.htm#DBSEG1000>

What is the danger to assigning / granting to PUBLIC?

The public role as its name suggest is a public. It is the common role that exists in every user database. Whenever the new role is created by default it is considered as a public role. Granting serious privileges to this role would allow all the database member to access the sensitive data and information accessible wide open.

In order to avoid severe data theft and unauthorized use of the data, It is extremely important to carefully differentiate the grant permission with the public and the other roles in the database.

Charles was given the order to grant specific privileges to Nick on Charles’ table named food\_club\_members. Nick is a new - hire and will be working with Charles to maintain and manipulate important database files for the Eats - a - Lot Corporation.

Instead of using the following code for Nick

Grant All on food\_club\_members to nick\_01\_user;

Charles used the code

Grant All on food\_club\_members to public;

which he immediately executed. Some unscrupulous employee began to download the entire food\_club\_members to their flash drive.

One of the important operations that Charles can perform is to instantly revoke the privileges from the account. The Revoke command can be effectively utilized for this purpose.

REVOKE ALL ON food\_club\_members FROM public;