|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |
| --- | --- |
| **STEP 1: Define a New Profile** |  |

Oracle provides the ability to set expirations, limit the reuse, and define the complexity of passwords. In addition, accounts can be locked if the password is entered incorrectly too many times. In this section of the lab we are going to create a custom profile that will then be applied to the SCOTT user.

1. To begin, log into your instance as the SYSTEM user.
2. Write SQL script that will create a new profile named SCOTT\_PROFILE that will do the following:
   * Limit the number of failed login attempts to 3 in a row.
   * Limit the overall connection time to 10 hours (we will give him a little leeway incase he has to work overtime).
   * Allow a session to be idle no more than 1 hour.
   * Change the password every 60 days.
   * Allow the user 3 days to change the password after it expires.
   * Not allow a previous password be reused before there have been three password changes.
3. Execute your pfile script and verify that the profile has been created by running a query against the DBA\_PROFILES view in the data dictionary. Limit your output to ONLY the SCOTT\_PROFILE parameters.

|  |  |
| --- | --- |
| **STEP 2: Testing the New Profile** |  |

Now that we have a new profile for the SCOTT user we need to verify that it works properly. For obvious reasons there are going to be parts of the profile that we cannot test within the confines of this lab due to time constraints, but we can test to verify that the SCOTT user is being controlled by the profile.

1. The first things we need to do is assign the profile to the SCOTT user. While still logged into your instance as the SYSTEM user write and execute the SQL command that will assign the SCOTT\_PROFILE profile to the SCOTT user.
2. Now log into SCOTT (password is TIGER). Remember that you must supply the database instance name when logging in from the SQL> prompt just as you do when using the login window, i.e. CONN SCOTT/TIGER@instance\_name.
3. There are several things that we can test related to the logging in and changing a password so here we go.
   * You should now be successfully connected to the SCOTT user. Write the connect command again using an incorrect password. NOTE: you should get a warning message stating that you are no longer connected to Oracle. That is fine, just keep trying to log in.
   * Repeat the above process until you get the **ORA-28000: the account is locked** error which will indicate that the profile is working here.
   * At this point we need to get the account unlocked so you will need to login to your instance as the SYSTEM user and unlock the SCOTT account **BUT DO NOT LOG BACK INTO THE SCOTT USER YET**.
   * Now we can test the password reuse parameter. To do this we must EXPIRE the current password. Write and execute the SQL command to expire the password for the SCOTT user.
   * Now log back into the SCOTT user. You should receive a message stating that the password has expired (**ORA-28001: the password has expired**) and then prompting you to change the password.
   * Try to reuse the TIGER password. You should receive the following - **ORA-28007: the password cannot be reused**.
4. Now log into the SCOTT user again and this time change the password to LION to complete this step of the lab.

|  |  |
| --- | --- |
| **STEP 3: Creating New User** |  |

1. Create a new user in your instance called Jeff identified by a password and assign the default profile to this user.
2. Assign the default tablespace users and temporary tablespace temp to the user.
3. Grant the necessary privilege to enable user to connect to the database.
4. Now create a new profile jeff\_prof and set certain limitations to this profile, namely:
   1. Limit the number of times that a wrong password can be entered to 2 before the account is locked.
   2. If the password exceeds the above limit, lock it for 2 days.
5. Now assign the new profile to Jeff.
6. Test the profile.
7. Create a role ‘Admin’ with the following privileges:-
   1. select, insert, update, delete on the tables location, student, faculty and term
8. Grant the role ‘Admin’ to Jeff.
9. Verify that Jeff has acquired the necessary privilege.