Part 1. Database Administration Lab

Setup

This lab should be performed under the Oracle Linux VM provided in the course.

1. Start your Oracle Linux VM through the Oracle VM VirtualBox Manager.

2. Login as the oracle OS user.

   Username: **oracle**
   Password: **metcs674**

3. Open a terminal window by double-clicking the terminal icon (**Figure 1**).

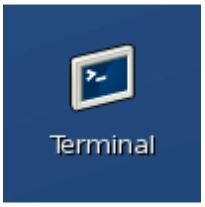

Figure 1. Terminal icon

4. Login to SQL*Plus as the Sys user as sysdba as shown below (**Figure 2**). The default password is **metcs674**.

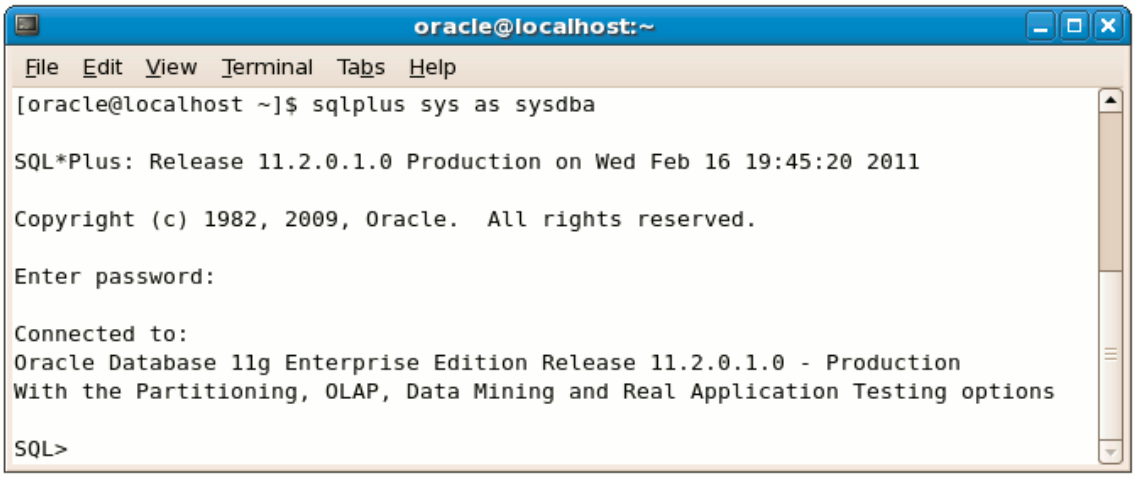

Figure 2. SQL*Plus Session

5. Create a new USER with your name. The password should be the same as your first name. Allocate the following parameters: default TABLESPACE users, TEMPORARY TABLESPACE temp, QUOTA 10M ON users, PASSWORD EXPIRE, ACCOUNT UNLOCK. You can allocate any profile.

```
2018-09-19 10:51:12 SYS AS SYSDBA> CREATE USER FARIBORZNOROUZI IDENTIFIED BY FARIBORZ
  2  DEFAULT TABLESPACE USERS
  3  TEMPORARY TABLESPACE TEMP
  4  QUOTA 10M ON USERS
  5  PASSWORD EXPIRE
  6  ACCOUNT UNLOCK;

User created.

2018-09-19 10:58:21 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

6. Alter the user password that you created in question 5. Change it to your last name.

```
2018-09-19 10:58:21 SYS AS SYSDBA> ALTER USER FARIBORZNOROUZI IDENTIFIED BY NOROUZI;

User altered.

2018-09-19 11:02:06 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

7. Create a user Profile called STUDENT. Assign your own resource and password limits.

```
2018-09-19 11:02:06 SYS AS SYSDBA> CREATE PROFILE STUDENT LIMIT
  2  CPU_PER_SESSION UNLIMITED
  3  SESSIONS_PER_USER 3
  4  CONNECT_TIME 120
  5  IDLE_TIME 20;

Profile created.

2018-09-19 11:14:20 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

8. Verify the results of the STUDENT profile by querying dba_profiles.

```
2018-09-19 11:14:20 SYS AS SYSDBA> SELECT * FROM DBA_PROFILES WHERE PROFILE = 'STUDENT';

PROFILE                        RESOURCE_NAME                    RESOURCE LIMIT
------------------------------ -------------------------------- -------- -----------------
STUDENT                        COMPOSITE_LIMIT                  KERNEL   DEFAULT
STUDENT                        SESSIONS_PER_USER                KERNEL   3
STUDENT                        CPU_PER_SESSION                  KERNEL   UNLIMITED
STUDENT                        CPU_PER_CALL                     KERNEL   DEFAULT
STUDENT                        LOGICAL_READS_PER_SESSION        KERNEL   DEFAULT
STUDENT                        LOGICAL_READS_PER_CALL           KERNEL   DEFAULT
STUDENT                        IDLE_TIME                        KERNEL   20
STUDENT                        CONNECT_TIME                     KERNEL   120
STUDENT                        PRIVATE_SGA                      KERNEL   DEFAULT
STUDENT                        FAILED_LOGIN_ATTEMPTS            PASSWORD DEFAULT
STUDENT                        PASSWORD_LIFE_TIME               PASSWORD DEFAULT
STUDENT                        PASSWORD_REUSE_TIME              PASSWORD DEFAULT
STUDENT                        PASSWORD_REUSE_MAX               PASSWORD DEFAULT
STUDENT                        PASSWORD_VERIFY_FUNCTION         PASSWORD DEFAULT
STUDENT                        PASSWORD_LOCK_TIME               PASSWORD DEFAULT
STUDENT                        PASSWORD_GRACE_TIME              PASSWORD DEFAULT

16 rows selected.

2018-09-19 11:16:43 SYS AS SYSDBA>
```

Applications Places System

oracle@localhost:~

9. Alter the Idle_Time for the STUDENT profile.

```
2018-09-19 11:39:46 SYS AS SYSDBA> ALTER PROFILE STUDENT LIMIT IDLE_TIME 10;

Profile altered.

2018-09-19 11:41:55 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

10. Alter User (Your_Name) to Use STUDENT profile.

```
2018-09-19 11:41:55 SYS AS SYSDBA> ALTER USER FARIBORZNOROUZI PROFILE STUDENT;

User altered.

2018-09-19 11:43:55 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

11. Show all values in the DEFAULT profile.

```
2018-09-19 11:43:55 SYS AS SYSDBA> SELECT * FROM DBA_PROFILES WHERE PROFILE = 'DEFAULT';

PROFILE                        RESOURCE_NAME                    RESOURCE LIMIT
------------------------------ -------------------------------- -------- -----------------
DEFAULT                        COMPOSITE_LIMIT                  KERNEL   UNLIMITED
DEFAULT                        SESSIONS_PER_USER                KERNEL   UNLIMITED
DEFAULT                        CPU_PER_SESSION                  KERNEL   UNLIMITED
DEFAULT                        CPU_PER_CALL                     KERNEL   UNLIMITED
DEFAULT                        LOGICAL_READS_PER_SESSION        KERNEL   UNLIMITED
DEFAULT                        LOGICAL_READS_PER_CALL           KERNEL   UNLIMITED
DEFAULT                        IDLE_TIME                        KERNEL   UNLIMITED
DEFAULT                        CONNECT_TIME                     KERNEL   UNLIMITED
DEFAULT                        PRIVATE_SGA                      KERNEL   UNLIMITED
DEFAULT                        FAILED_LOGIN_ATTEMPTS            PASSWORD UNLIMITED
DEFAULT                        PASSWORD_LIFE_TIME               PASSWORD UNLIMITED
DEFAULT                        PASSWORD_REUSE_TIME              PASSWORD UNLIMITED
DEFAULT                        PASSWORD_REUSE_MAX               PASSWORD UNLIMITED
DEFAULT                        PASSWORD_VERIFY_FUNCTION         PASSWORD NULL
DEFAULT                        PASSWORD_LOCK_TIME               PASSWORD 1
DEFAULT                        PASSWORD_GRACE_TIME              PASSWORD 7

16 rows selected.

2018-09-19 11:46:49 SYS AS SYSDBA>
```

Applications Places System

oracle@localhost:~

12. Create a Password Profile - limit failed login attempts to 2, password life time to 15, PASSWORD_REUSE_TIME to DEFAULT, and PASSWORD_REUSE_MAX is equal to 1.

```
2018-09-19 11:46:49 SYS AS SYSDBA> CREATE PROFILE PASSWORD LIMIT
  2  FAILED_LOGIN_ATTEMPTS 2
  3  PASSWORD_LIFE_TIME 15
  4  PASSWORD_REUSE_TIME DEFAULT
  5  PASSWORD_REUSE_MAX 1;

Profile created.

2018-09-19 11:55:19 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

13. Grant Select to Any Table to User Your_Name.

```
2018-09-19 11:55:19 SYS AS SYSDBA> GRANT SELECT ANY TABLE TO FARIBORZNOROUZI;

Grant succeeded.

2018-09-19 11:59:21 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

14. Revoke Select to Any Table granted in question 13.

```
2018-09-19 11:59:21 SYS AS SYSDBA> REVOKE SELECT ANY TABLE FROM FARIBORZNOROUZI;

Revoke succeeded.

2018-09-19 12:02:13 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

15. What data dictionary view can be used by a DBA to view system privileges granted to users? Show all columns in this view.

USER_SYS_PRIVS shows system privileges granted to the current user. It contains three columns inclusive: Grantee, Privilege and Admin option.

```
2018-09-21 09:08:33 SYS AS SYSDBA> DESC DBA_SYS_PRIVS;
 Name
      Null?     Type
 -----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-------------------------------------------------------- -------- ----------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
---------------------
 GRANTEE
      NOT NULL VARCHAR2(30)
 PRIVILEGE
      NOT NULL VARCHAR2(40)
 ADMIN_OPTION
ARCHAR2(3)

2018-09-21 09:40:13 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

16. What does the following query do?

```
SQL> SELECT * FROM DBA_SYS_PRIVS
WHERE GRANTEE = 'SCOTT';
```

This query shows all system privileges granted to user Scott.

```
2018-09-19 12:21:34 SYS AS SYSDBA> SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'SCOTT';

GRANTEE                        PRIVILEGE                                ADM
------------------------------ ---------------------------------------- ---
SCOTT                          CHANGE NOTIFICATION                      NO
SCOTT                          CREATE SYNONYM                           NO
SCOTT                          DROP ANY DIRECTORY                       NO
SCOTT                          CREATE ANY DIRECTORY                     NO
SCOTT                          CREATE VIEW                              NO
SCOTT                          UNLIMITED TABLESPACE                     NO
SCOTT                          ALTER SESSION                            NO
SCOTT                          CREATE TABLE                             NO

8 rows selected.

2018-09-19 12:24:20 SYS AS SYSDBA>
oracle@localhost:~
Applications  Places  System
```

17. Grant Select to User Your_Name on DEPT table.

DEPT table doesn't exist, therefore I create DEPT table first.

```
2018-09-19 12:38:58 SYS AS SYSDBA> CREATE TABLE DEPT(
  2  deptno number(2,0),
  3  deptname varchar2(20));

Table created.

2018-09-19 12:46:45 SYS AS SYSDBA> GRANT SELECT ON DEPT TO FARIBORZNOROUZI;

Grant succeeded.

2018-09-19 12:48:10 SYS AS SYSDBA>
oracle@localhost:~
Applications  Places  System
```

18. Revoke Select to User Your_Name for DEPT.

```
2018-09-19 12:48:10 SYS AS SYSDBA> REVOKE SELECT ON DEPT FROM FARIBORZNOROUZI;

Revoke succeeded.

2018-09-19 12:51:15 SYS AS SYSDBA>
oracle@localhost:~
Applications  Places  System
```

19. Show all object privileges granted to user YOUR_NAME.

Note: If necessary, grant an object privilege first (e.g. repeat command in Question 13) to get meaningful results.

```
2018-09-19 13:28:50 SYS AS SYSDBA> GRANT SELECT ON DEPT TO FARIBORZNOROUZI WITH GRANT OPTION;

Grant succeeded.

2018-09-19 13:30:42 SYS AS SYSDBA> SELECT PRIVILEGE FROM USER_TAB_PRIVS WHERE GRANTEE = 'FARIBORZNOROUZI';

PRIVILEGE
----------------------------------------
SELECT

2018-09-19 13:31:45 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

20. Show all object privileges granted to the current user.

```
2018-09-19 17:20:23 SYS AS SYSDBA> SELECT * FROM SESSION_PRIVS;

PRIVILEGE
----------------------------------------
ALTER SYSTEM
AUDIT SYSTEM
CREATE SESSION
ALTER SESSION
RESTRICTED SESSION
CREATE TABLESPACE
ALTER TABLESPACE
MANAGE TABLESPACE
DROP TABLESPACE
UNLIMITED TABLESPACE
CREATE USER
BECOME USER
ALTER USER
DROP USER
CREATE ROLLBACK SEGMENT
ALTER ROLLBACK SEGMENT
DROP ROLLBACK SEGMENT
CREATE TABLE
CREATE ANY TABLE
ALTER ANY TABLE
BACKUP ANY TABLE
DROP ANY TABLE
LOCK ANY TABLE
COMMENT ANY TABLE
SELECT ANY TABLE
INSERT ANY TABLE
```

Applications Places System

oracle@localhost:~

21. Show how to display all object privileges granted to other users.

Note: Create some users and grant them privileges first. Depending on the tables you use for this exercise, you might need to login with a privileged account and grant yourself privileges WITH GRANT OPTION.

```
2018-09-19 17:37:03 SYS AS SYSDBA> CREATE USER DAVID IDENTIFIED BY JONES
  2  DEFAULT TABLESPACE USERS
  3  TEMPORARY TABLESPACE TEMP
  4  QUOTA 15M ON USERS
  5  PASSWORD EXPIRE
  6  ACCOUNT UNLOCK;

User created.

2018-09-19 18:22:57 SYS AS SYSDBA> CREATE USER SAM IDENTIFIED BY LEE
  2  DEFAULT TABLESPACE USERS
  3  TEMPORARY TABLESPACE TEMP
  4  QUOTA 25 ON USERS
  5  PASSWORD EXPIRE
  6  ACCOUNT UNLOCK;

User created.

2018-09-19 18:27:00 SYS AS SYSDBA>
```

```
oracle@localhost:~
Applications  Places  System

2018-09-19 18:27:00 SYS AS SYSDBA> GRANT SELECT, UPDATE ON DEPT TO DAVID WITH GRANT OPTION;

Grant succeeded.

2018-09-19 18:34:25 SYS AS SYSDBA> GRANT SELECT, UPDATE ON DEPOT TO SAM WITH GRANT OPTION;
GRANT SELECT, UPDATE ON DEPOT TO SAM WITH GRANT OPTION
                         *
ERROR at line 1:
ORA-00942: table or view does not exist


2018-09-19 18:35:35 SYS AS SYSDBA> GRANT SELECT, UPDATE ON DEPT TO SAM WITH GRANT OPTION;

Grant succeeded.

2018-09-19 18:37:01 SYS AS SYSDBA>
```

```
oracle@localhost:~
Applications  Places  System

2018-09-19 18:52:00 SYS AS SYSDBA> SELECT PRIVILEGE FROM USER_TAB_PRIVS
  2  WHERE GRANTEE = 'DAVID' OR GRANTEE = 'SAM';

PRIVILEGE
----------------------------------------
UPDATE
UPDATE
SELECT
SELECT

2018-09-19 18:53:30 SYS AS SYSDBA>
```

```
oracle@localhost:~
Applications  Places  System
```

22. Create a Role called Developer.

```
2018-09-19 18:53:30 SYS AS SYSDBA> CREATE ROLE DEVELOPER;

Role created.

2018-09-19 19:06:50 SYS AS SYSDBA>
```

23. Grant Create Session to Developer.

```
2018-09-19 19:06:50 SYS AS SYSDBA> GRANT CREATE SESSION TO DEVELOPER WITH ADMIN OPTION;

Grant succeeded.

2018-09-19 19:12:46 SYS AS SYSDBA>
```

24. Grant Developer Role to Your_Name.

```
2018-09-19 19:12:46 SYS AS SYSDBA> GRANT DEVELOPER TO FARIBORZNOROUZI WITH ADMIN OPTION;

Grant succeeded.

2018-09-19 19:17:30 SYS AS SYSDBA>
```

25. Create a database link using FIXED USER credentials.

```
2018-09-19 19:31:01 SYS AS SYSDBA> CREATE DATABASE LINK DBLINK CONNECT TO FIXED_USER IDENTIFIED BY DOE USING 'CREDENTIALS';

Database link created.

2018-09-19 19:35:21 SYS AS SYSDBA>
```

Part 2. Hardening the Database Lab

Lock and Expire Default or Unused User Accounts

For security reasons you don't want to leave user accounts open in your database that are not used or needed. You can choose to lock the accounts or remove the user accounts. In this exercise you will lock the accounts and expire the passwords of users that will not be used in the labs. For this course we use the Oracle sample schemas, but in a production environment it is best practice not to install the sample schemas or remove them if they have been installed.

1. In SQL*Plus (as Sys as sysdba), run a query that shows the username and account status of all of the database users in the dba_users data dictionary view.

Accidently, I ran a query in question 2 first, consequently the result of the query is same with answer of question 3.

```
2018-09-24 19:15:49 SYS AS SYSDBA> SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
CH0306                         EXPIRED & LOCKED
OBE                            EXPIRED & LOCKED
CACHEADM                       EXPIRED & LOCKED
APP                            EXPIRED & LOCKED
HR_TRIG                        EXPIRED & LOCKED
SPATIAL_WFS_ADMIN_USR          EXPIRED & LOCKED
DIP                            EXPIRED & LOCKED
SH                             EXPIRED & LOCKED
IX                             EXPIRED & LOCKED
MDDATA                         EXPIRED & LOCKED
DEMO                           EXPIRED & LOCKED
HR1                            EXPIRED & LOCKED
ORACLE_OCM                     EXPIRED & LOCKED
OE1                            EXPIRED & LOCKED
TIMESTEN                       EXPIRED & LOCKED
XDBEXT                         EXPIRED & LOCKED
SAM                            EXPIRED & LOCKED
TTHR                           EXPIRED & LOCKED
SPATIAL_CSW_ADMIN_USR          EXPIRED & LOCKED
APEX_PUBLIC_USER               EXPIRED & LOCKED
XDBPM                          EXPIRED & LOCKED
PM                             EXPIRED & LOCKED
BI                             EXPIRED & LOCKED
XS$NULL                        EXPIRED & LOCKED
PLS                            EXPIRED & LOCKED
PHPDEMO                        EXPIRED & LOCKED
XFILES                         EXPIRED & LOCKED
```

2. Use alter user statements to lock the accounts of all users and expire the passwords of all users except the **Sys**, **System**, and **Sysman**, **App**, **HR**, **OE**, and **Scott** users.

   Ex. Lock and expire: **SQL> alter user OE1 account lock password expire;**
   Ex. Expire only: **SQL> alter user XDBPM password expire;**

```
oracle@localhost:~
File  Edit  View  Terminal  Tabs  Help
2018-09-20 10:39:33 SYS AS SYSDBA> set heading off
2018-09-20 10:40:44 SYS AS SYSDBA> spool runme.sql
2018-09-20 10:40:58 SYS AS SYSDBA> SELECT 'ALTER USER'||USERNAME||'PASSWORD EXPIRE ACCOUNT LOCK;'
  2  FROM DBA_USERS WHERE USERNAME NOT IN ('SYS','SYSTEM','SYSMAN','APP','HR','OE','SCOTT');

ALTER USERSPATIAL_WFS_ADMIN_USRPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERSPATIAL_CSW_ADMIN_USRPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERDIPPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERSHPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERIXPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERMDDATAPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERPMPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERBIPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERXS$NULLPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERORACLE_OCMPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERFREDPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USEROLAPSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERSI_INFORMTN_SCHEMAPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USEROWBSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERORDPLUGINSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERCTXSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERORDDATAPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERAPEX_040100PASSWORD EXPIRE ACCOUNT LOCK;
ALTER USEROWBSYS_AUDITPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERAPPQOSSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERWMSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USEREXFSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERORDSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERMDSYSPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERFLOWS_FILESPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USEROUTLNPASSWORD EXPIRE ACCOUNT LOCK;
ALTER USERCH0306PASSWORD EXPIRE ACCOUNT LOCK;
Applications  Places  System
```

3. Run a query again on dba_users to show that the **Sys**, **System**, and **Sysman**, **App**, **HR**, **OE**, and **Scott** accounts are "OPEN" and all other accounts are "EXPIRED & LOCKED".

   Note: The **dba_users_with_defpwd** data dictionary view will give you all users in an 11g database that are using default passwords.

   Note: In this lab, DO NOT alter the accounts or change the passwords of the "**App**" or "**HR**" users.

```
2018-09-21 11:24:04 SYS AS SYSDBA> SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
MGMT_VIEW                      EXPIRED & LOCKED
OUTLN                          EXPIRED & LOCKED
SYSTEM                         OPEN
SYS                            OPEN
OLAPSYS                        EXPIRED & LOCKED
OWBSYS                         EXPIRED & LOCKED
ORDPLUGINS                     EXPIRED & LOCKED
XDB                            EXPIRED & LOCKED
APEX_040100                    EXPIRED & LOCKED
OWBSYS_AUDIT                   EXPIRED & LOCKED
APPQOSSYS                      EXPIRED & LOCKED
EXFSYS                         EXPIRED & LOCKED
ORDSYS                         EXPIRED & LOCKED
SI_INFORMTN_SCHEMA             EXPIRED & LOCKED
ANONYMOUS                      EXPIRED & LOCKED
CTXSYS                         EXPIRED & LOCKED
ORDDATA                        EXPIRED & LOCKED
WMSYS                          EXPIRED & LOCKED
MDSYS                          EXPIRED & LOCKED
FLOWS_FILES                    EXPIRED & LOCKED
SYSMAN                         OPEN
CACHEADM                       EXPIRED & LOCKED
APP                            EXPIRED & LOCKED
HR_TRIG                        EXPIRED & LOCKED
SPATIAL_WFS_ADMIN_USR          EXPIRED & LOCKED
DIP                            EXPIRED & LOCKED
SH                             EXPIRED & LOCKED
```

Applications Places System

oracle@localhost:~

```
IX                             EXPIRED & LOCKED
MDDATA                         EXPIRED & LOCKED
DEMO                           EXPIRED & LOCKED
HR1                            EXPIRED & LOCKED
ORACLE_OCM                     EXPIRED & LOCKED
OE1                            EXPIRED & LOCKED
TIMESTEN                       EXPIRED & LOCKED
XDBEXT                         EXPIRED & LOCKED
SAM                            EXPIRED & LOCKED
TTHR                           EXPIRED & LOCKED
SPATIAL_CSW_ADMIN_USR          EXPIRED & LOCKED
APEX_PUBLIC_USER               EXPIRED & LOCKED
XDBPM                          EXPIRED & LOCKED
PM                             EXPIRED & LOCKED
BI                             EXPIRED & LOCKED
XS$NULL                        EXPIRED & LOCKED
PLS                            EXPIRED & LOCKED
PHPDEMO                        EXPIRED & LOCKED
XFILES                         EXPIRED & LOCKED
FRED                           EXPIRED & LOCKED
DAVID                          EXPIRED & LOCKED
HR                             OPEN
OE                             OPEN
SCOTT                          OPEN
OBE                            EXPIRED & LOCKED
CH0306                         EXPIRED & LOCKED
DBSNMP                         EXPIRED & LOCKED
FARIBORZNOROUZI                EXPIRED & LOCKED

55 rows selected.

2018-09-21 11:24:41 SYS AS SYSDBA>
```

Applications Places System

oracle@localhost:~

Implement Password Verification

"Choosing secure passwords and implementing good password policies are by far the most important defense for protecting against password based security threats." ("Oracle Database Security Checklist," 2008, p. 4) In this exercise you will change the default profile to alter the default parameters for password management including using a password verification function. The script, utlpwdmg_for_674.sql, is a modified version of the Oracle script utlpwdmg.sql provided with an 11g install and is edited to included Oracle and CIS security recommendations. utlpwdmg_for_674.sql creates a password verification function, "verify_function_11G", and assigns it to the default profile. The password verification function ensures that passwords are created with a minimum length of 10, and that passwords contain at least one digit, one character, and one symbol. The function also checks the password's complexity and checks it against the
username and previously used passwords.

1. Open a new terminal window and view the script using the less command.

   [oracle@localhost /]$ less /home/oracle/sql_scripts/utlpwdmg_for_674.sql

2. In SQL*Plus (as Sys as sysdba), run the **utlpwdmg_for_674.sql** script:

   SQL> @/home/oracle/sql_scripts/utlpwdmg_for_674.sql

Change the Passwords of Administrative Accounts

It is good security practice not to use the same passwords for the Oracle administrative accounts. In this exercise you will change the default passwords of the Sys, System, and Sysman accounts.

1. With the password command or alter user statement change the passwords of the Sys, System, and Sysman users. Create a unique password for each user.

   SQL> password system
   Changing password for system
   New password:
   Retype new password:

Password changed

Note: The "Old Password" for Sys is metcs674.

Note: You can also change passwords using the syntax "alter user <user> identified by <password>".

Note: Be sure that the new passwords are a minimum length of 10, and that the passwords contain at least one digit, one character, and one symbol.

```
2018-09-21 17:16:27 SYS AS SYSDBA> ALTER USER SYS IDENTIFIED BY CHETORY125BAHAL$
  2  ;

User altered.

2018-09-21 17:17:59 SYS AS SYSDBA> ALTER USER SYSTEM IDENTIFIED BY KHOBAM126SALAR#
  2  ;

User altered.

2018-09-21 17:23:28 SYS AS SYSDBA> ALTER USER SYSMAN IDENTIFIED BY KHODAHAFEZ125JON$;

User altered.

2018-09-21 17:25:25 SYS AS SYSDBA>
```

Verifying DBA Privileges

The Oracle DBA role should only be granted to those users who really need DBA privileges. Be selective and use caution with the DBA role. In this exercise you will look at all of the accounts that have the DBA role and revoke the DBA role from any user that does not need the role.

1. In SQL*Plus (as Sys as sysdba), run a query that shows the users that are assigned the DBA privilege excluding the Sys and System users.

   SQL> select grantee from dba_role_privs where granted_role='DBA' and grantee not in ('SYSTEM','SYS');

2. If there are any users with the DBA privilege other than Sys or Sytem, revoke the DBA privilege.

   SQL> revoke DBA from <user>

   Note: Replace **<user>** above with the user(s) returned in step 1.

```
2018-09-21 17:25:25 SYS AS SYSDBA> SELECT GRANTEE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA' AND GRANTEE NOT IN ('SYSTEM','SYS');

GRANTEE
------------------------------
PHPDEMO

2018-09-21 17:38:20 SYS AS SYSDBA> REVOKE DBA FROM PHPDEMO;

Revoke succeeded.

2018-09-21 17:39:43 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System 5:40 PM

Verifying Roles

It is good security practice to drop any predefined or user defined roles that are not used. In this exercise you will look at all of the roles in the database and drop the "manager" role because it is no longer used.

1. In SQL*Plus (as Sys as sysdba), run a query that shows all of the roles in the database.

   SQL> SELECT * FROM DBA_ROLES;

```
2018-09-21 17:39:43 SYS AS SYSDBA> SELECT * FROM DBA_ROLES;

ROLE                           PASSWORD AUTHENTICAT
------------------------------ -------- -----------
CONNECT                        NO       NONE
RESOURCE                       NO       NONE
DBA                            NO       NONE
SELECT_CATALOG_ROLE            NO       NONE
EXECUTE_CATALOG_ROLE           NO       NONE
DELETE_CATALOG_ROLE            NO       NONE
EXP_FULL_DATABASE              NO       NONE
IMP_FULL_DATABASE              NO       NONE
LOGSTDBY_ADMINISTRATOR         NO       NONE
DBFS_ROLE                      NO       NONE
AQ_ADMINISTRATOR_ROLE          NO       NONE
AQ_USER_ROLE                   NO       NONE
DATAPUMP_EXP_FULL_DATABASE     NO       NONE
DATAPUMP_IMP_FULL_DATABASE     NO       NONE
ADM_PARALLEL_EXECUTE_TASK      NO       NONE
GATHER_SYSTEM_STATISTICS       NO       NONE
JAVA_DEPLOY                    NO       NONE
RECOVERY_CATALOG_OWNER         NO       NONE
SCHEDULER_ADMIN                NO       NONE
HS_ADMIN_SELECT_ROLE           NO       NONE
HS_ADMIN_EXECUTE_ROLE          NO       NONE
HS_ADMIN_ROLE                  NO       NONE
GLOBAL_AQ_USER_ROLE            GLOBAL   GLOBAL
OEM_ADVISOR                    NO       NONE
OEM_MONITOR                    NO       NONE
WM_ADMIN_ROLE                  NO       NONE
JAVAUSERPRIV                   NO       NONE
```

Applications Places System

oracle@localhost:~

```
JMXSERVER                      NO       NONE
JAVA_ADMIN                     NO       NONE
CTXAPP                         NO       NONE
XDBADMIN                       NO       NONE
XDB_SET_INVOKER                NO       NONE
AUTHENTICATEDUSER              NO       NONE
XDB_WEBSERVICES                NO       NONE
XDB_WEBSERVICES_WITH_PUBLIC    NO       NONE
XDB_WEBSERVICES_OVER_HTTP      NO       NONE
ORDADMIN                       NO       NONE
OLAPI_TRACE_USER               NO       NONE
OLAP_XS_ADMIN                  NO       NONE
OWB_USER                       NO       NONE
OLAP_DBA                       NO       NONE
CWM_USER                       NO       NONE
OLAP_USER                      NO       NONE
SPATIAL_WFS_ADMIN              NO       NONE
WFS_USR_ROLE                   YES      PASSWORD
SPATIAL_CSW_ADMIN              YES      PASSWORD
CSW_USR_ROLE                   YES      PASSWORD
MGMT_USER                      NO       NONE
APEX_ADMINISTRATOR_ROLE        NO       NONE
OWB$CLIENT                     YES      PASSWORD
OWB_DESIGNCENTER_VIEW          NO       NONE
XFILES_USER                    NO       NONE
XFILES_ADMINISTRATOR           NO       NONE
TT_CACHE_ADMIN_ROLE            NO       NONE
DEVELOPER                      NO       NONE

59 rows selected.

2018-09-21 17:44:31 SYS AS SYSDBA>
```

2. Drop the MANAGER role.

   SQL> drop role manager;

```
2018-09-23 12:11:49 SYS AS SYSDBA> CREATE ROLE MANAGER;

Role created.

2018-09-23 12:12:26 SYS AS SYSDBA> DROP ROLE MANAGER;

Role dropped.

2018-09-23 12:13:56 SYS AS SYSDBA>
```

Verify the REMOTE_OS_AUTHENT Parameter

"Setting REMOTE_OS_AUTHENT to TRUE can cause a security exposure, because it lets someone using a non-secure protocol, such as TCP, perform an operating system authorized login (formerly referred to as an OPS$ login)." (“Oracle® Database Advanced Security Administrator's Guide 11g Release 2 (11.2),” n.d.). In this exercise you will verify that the REMOTE_OS_AUTHENT parameter is set to FALSE. The default parameter in 11g is FALSE.

1. In SQL*Plus (as Sys as sysdba), run the following command to show the value of the REMOTE_OS_AUTHENT parameter.

   SQL> show parameter REMOTE_OS_AUTHENT

```
2018-09-21 17:46:59 SYS AS SYSDBA> SHOW PARAMETER REMOTE_OS_AUTHENT;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
remote_os_authent                    boolean     FALSE
2018-09-21 17:52:18 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

Audit Operations of Sys user and SYSDBA and SYSOPER privileges

It is good security practice to audit the activities of the sys user and those users authenticated with SYSDBA or SYSOPER. In this exercise you will set the AUDIT_SYS_OPERATIONS parameter to TRUE. The default parameter in 11g is FALSE.

1. In SQL*Plus (as Sys as sysdba), run the following command to set the value of the AUDIT_SYS_OPERATIONS parameter.

   SQL> alter system set AUDIT_SYS_OPERATIONS=TRUE scope=spfile;

```
2018-09-21 17:52:18 SYS AS SYSDBA> ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE;

System altered.

2018-09-21 17:58:26 SYS AS SYSDBA>
```

oracle@localhost:~

Applications Places System

2. You must restart the instance for the change to take effect.

   SQL> shutdown immediate
   SQL> startup

```
2018-09-21 17:58:26 SYS AS SYSDBA> SHUTDOWN IMMEDIATE;
/
SDatabase closed.
Database dismounted.
TORACLE instance shut down.
2018-09-21 18:02:29 SYS AS SYSDBA> ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE
```

3. Verify that the audit_sys_operations parameter is set to TRUE.

SQL> show parameter audit_sys_operations;

```
2018-09-21 18:03:09 SYS AS SYSDBA> STARTUP;
ORACLE instance started.

Total System Global Area  456146944 bytes
Fixed Size                  1344840 bytes
Variable Size             360712888 bytes
Database Buffers           88080384 bytes
Redo Buffers                6008832 bytes
Database mounted.
Database opened.
21-SEP-18 SYS AS SYSDBA> SHOW PARAMETER AUDIT_SYS_OPERATIONS;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_sys_operations                 boolean     TRUE
21-SEP-18 SYS AS SYSDBA>
```

Applications Places System

oracle@localhost:~

Note: The audit records by default are written to $ORACLE_HOME/rdbms/audit, in UNIX/Linux, and the Event Log in Windows.