

# **Administrative Accounts and Privileges**

**By Ahmed Baraka**

# Objectives

---

In this lecture, you will learn how to perform the following:

- Describe the administrative accounts and privileges
- Describe the difference between SYSDBA and SYSOPER privileges
- Describe the difference between SYS and SYSTEM accounts



# Administrative User Accounts

---

Admin User Account	Administrative Privilege	Authorized Operations	Password Location
<b>SYS</b>	<b>SYSDBA</b>	The most powerful administrative privilege, including starting up and shutting down the database	Password File (12.2)
<b>SYSTEM</b>	<b>DBA</b> (role)	Manage database objects and configurations	DB
<b>SYSBACKUP</b>	<b>SYSBACKUP</b>	Can perform backup and recovery operations	DB + Password F.
<b>SYSDG</b>	<b>SYSDG</b>	Can perform Data Guard operations.	DB + Password F.
<b>SYSKM</b>	<b>SYSKM</b>	Can perform Transparent Data Encryption (TDE) keystore operations	DB + Password F.
<b>SYSRAC</b>	<b>SYSRAC</b>	Used by Oracle Clusterware to perform Oracle RAC operations	DB + Password F.

# Administrative User Accounts

---

- They are accounts who are granted one or more **administrative privileges**
- **sys** is the superuser who can perform all the administrative privileges
- **SYSTEM** is granted the DBA role and not any administrative privileges
- They must use the keywords corresponding to their administrative privilege when connecting to the Oracle database (like **SYSDBA** or **SYSOPER**)
- Their passwords are saved in the password file

# About Administrative Privileges

---

- Use to implement the **role separation** concept
- A user currently connected as **SYSDBA** can grant or revoke any administrative privilege to or from another user.
- A user currently connected as **SYSOPER** cannot grant any administrative privilege to another user and cannot revoke any administrative privilege from another user.
- A user currently connected as other privileges (**SYSBACKUP**, **SYSDG**, **SYSKM**) can grant to or revoke from another user the same privileges
- Administrative privileges cannot be granted to roles.
- To retrieve the users administrative privileges:

```
SELECT USERNAME, SYSDBA, SYSOPER, SYSASM, .. FROM V$PWFILERS_USERS;
```

# About SYSDBA and SYSOPER System Privileges

---

- Privileges required to perform high-level administrative operations: starting, shutting down, backing up, or recovering the database
- Users with **SYSOPER** privilege cannot access user data
- Can assess the instance even when it is not open
- The privileges are automatically granted to **SYS**
- Like all other administrative privileges, can be granted/revoked using **GRANT** and **REVOKE** statements.

```
GRANT SYSDBA TO SCOTT;
```

# Administrative Privileges and their Default Schemas

---

- We a user logs on with an administrative privileges, the current schema becomes the privilege default schema

```
sqlplus c##adam/ABcd##1234 as sysdba
```

```
SQL> show user  
USER is "SYS"
```

```
sqlplus c##adam/ABcd##1234 as sysoper
```

```
SQL> show user  
USER is "PUBLIC"
```

```
sqlplus c##adam/ABcd##1234
```

```
SQL> show user  
USER is "C##ADAM"
```

Admin Privilege	Default Schema
SYSDBA	SYS
SYSOPER	PUBLIC
SYSBACKUP	SYSBACKUP
SYSDG	SYSDG
SYSKM	SYSKM
SYSRAC	SYSRAC

# About SYS and SYSTEM Accounts

---

- **SYS:**

- Is granted the **DBA** role, **SYSDBA** privilege, as well as several other roles.
- Has all privileges with **ADMIN OPTION**
- Owns the data dictionary and the Automatic Workload Repository (AWR)
- Can startup, shutdown, and some maintenance commands
- Must login: `sqlplus sys/mypassword as sysdba`
- Its password is saved in the password file

- **SYSTEM**

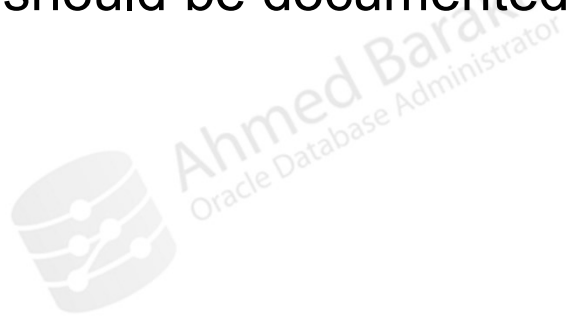
- account is granted the **DBA**, **MGMT\_USER**, and **AQ\_ADMINISTRATOR\_ROLE** roles but not the **SYSDBA**
- Cannot change db instance state or perform backup and recovery
- Its password is saved in the data dictionary



# Using Administrative Privileges Best Practices

---

- Apply the principle of least privileges
  - Create two accounts for individuals who need DBA tasks
- Grant/revoke requests should be documented and approved



# Summary

---

In this lecture, you should have learnt how to perform the following:

- Describe the administrative accounts and privileges
- Describe the difference between SYSDBA and SYSOPER privileges
- Describe the difference between SYS and SYSTEM accounts

