Using OS Authentication

By Ahmed Baraka

Objectives

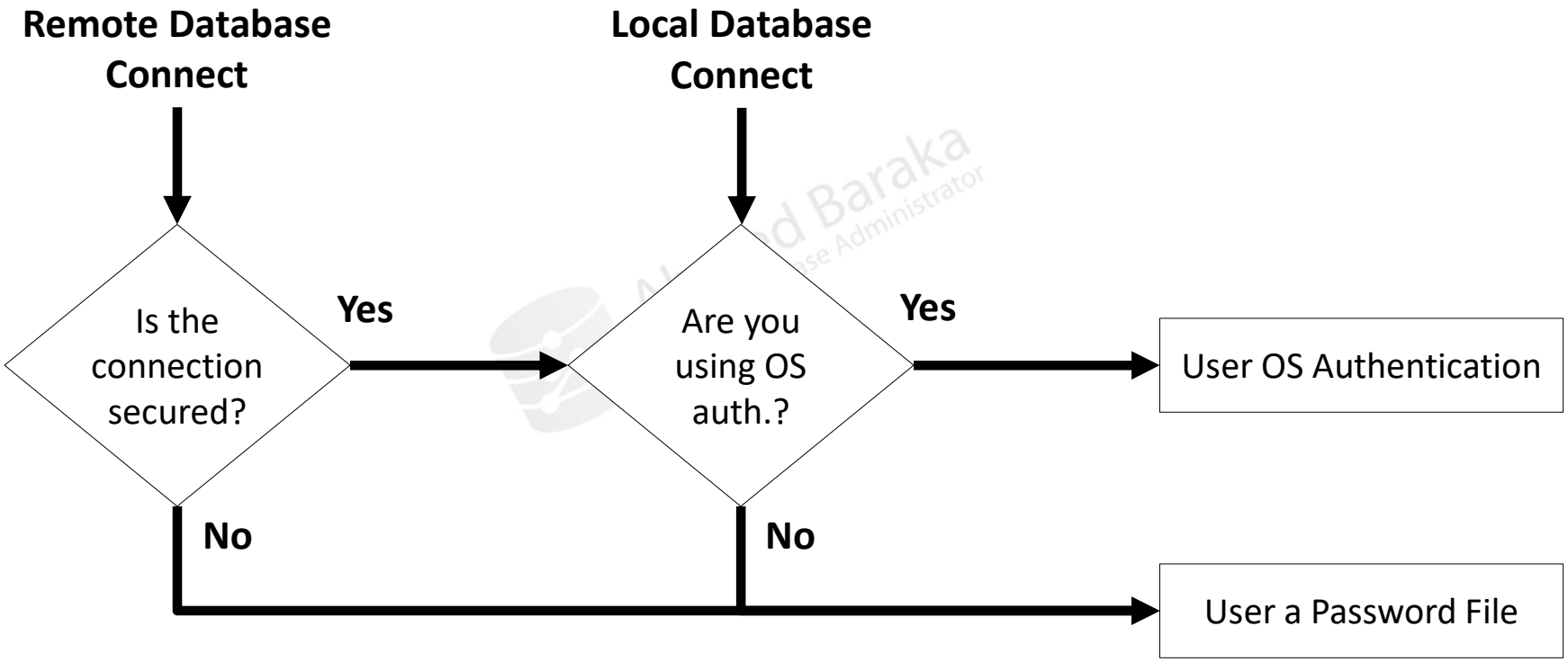
In this lecture, you will learn how to perform the following:

- Understand database administrator authentication
- Describe administrative OS authentication groups
- Allow administrative OS authentication to OS users
- Create OS-authenticated normal users

Authentication Methods

- **Oracle Database**
- **Operating system**
  - **Administrative**
  - **Non-administrative**
- **Password file**
- **Network**
  - directory-based authentication service, such as Oracle Internet Directory and MS Active Directory
  - SSL
  - Third-Party Services: Kerberos, Public Key Infrastructure (PKI), the Remote Authentication Dial-In User Service (RADIUS)

Database Administrator Authentication Flowchart



About Database Administrator Authentication

- To connect to Oracle Database as a privileged user over a nonsecure connection, the user must be authenticated by the password file.
- If no password file is there, we can only connect using OS authentication.

About Administrative OS Authentication Groups

- User belongs to a special OS group

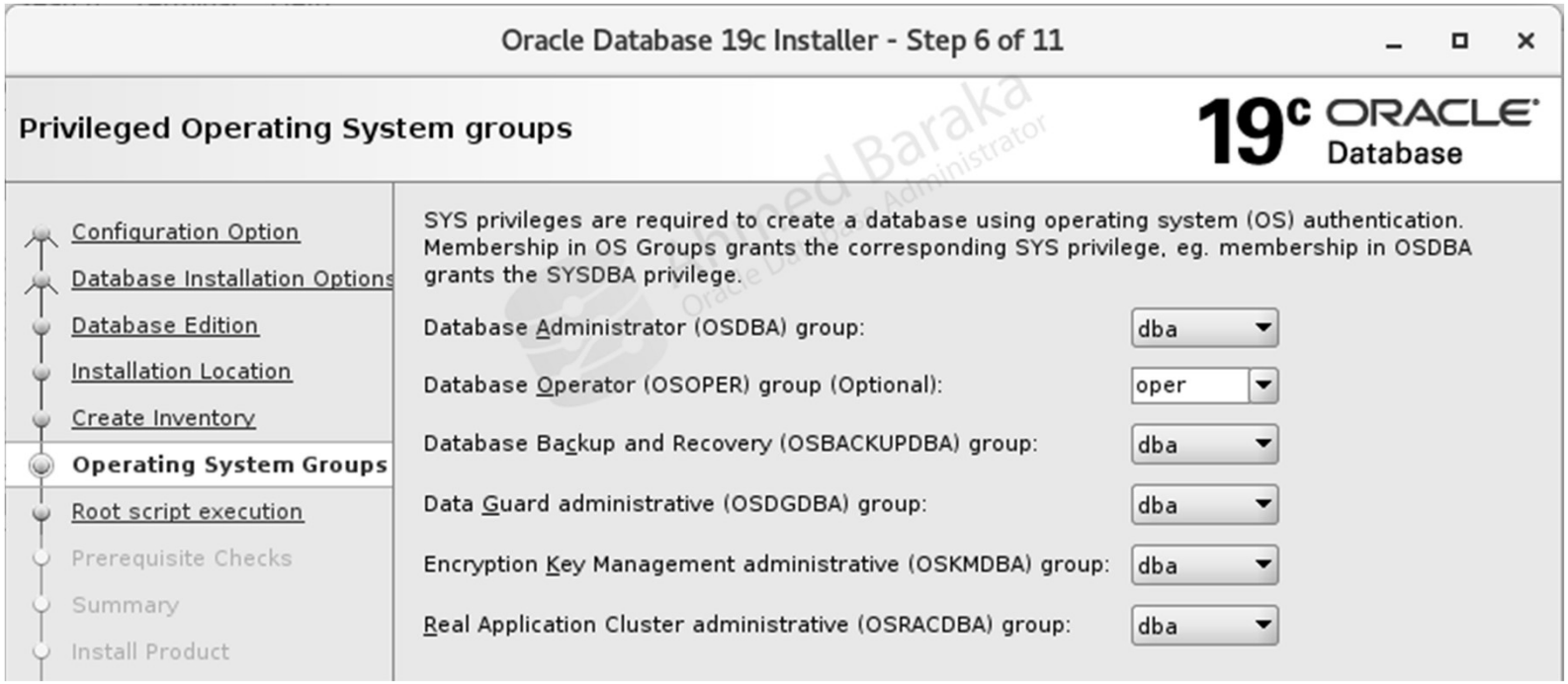
Admin. Priv.	Linux Group	Windows Group	Schema	OS dbca Group
SYSDBA	dba	ORA_DBA	SYS	OSDBA
SYSOPER	oper	ORA_OPER	PUBLIC	OSOPER
SYSBACKUP	backupdba	ORA_HOMENAME_SYSBACKUP	SYSBACKUP	OSBACKUPDBA
SYSDG	dgdba	ORA_HOMENAME_SYSDG	SYSDG	OSDGDBA
SYSKM	kmdba	ORA_HOMENAME_SYSKM	SYSKM	OSKMDBA
SYSRAC	racdba	ORA_HOMENAME_SYSRAC	SYSRAC	OSRACDBA

- Examples

```
sqlplus / as sysdba
sqlplus / as sysbackup
```

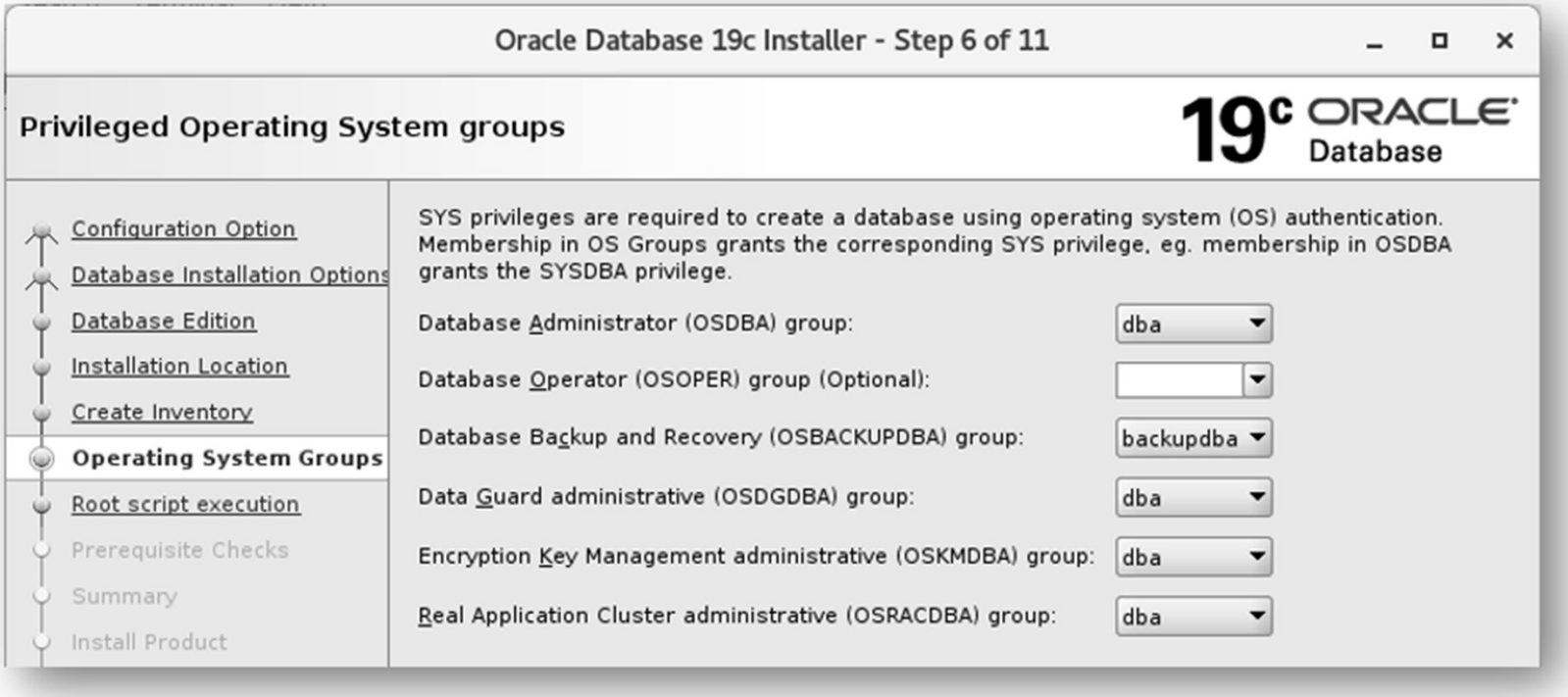
Defining Administrative OS Groups in dbca

- Administrative groups are defined at the database software installation:



Defining Administrative OS Groups in dbca

- An example when database backup group is defined:



Allowing Administrative OS Authentication to OS Users

- To allow an OS user to login to the database as one of the administrative accounts, add the account to the appropriate operating-system defined groups.

```
usermod -G oper user1
```

- The user can then login to the database using OS authentication method using the granted administrative privilege:

```
[user1@srv1 ~]$ export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/db_1
[user1@srv1 ~]$ export ORACLE_SID=oradb
[user1@srv1 ~]$ export
PATH=$PATH:/u01/app/oracle/product/19.0.0/db_1/bin
[user1@srv1 ~]$ sqlplus / as sysoper
Connected to: Oracle Database 19c Enterprise Edition Release ...
```

Using Administrative OS Authentication in Windows

- The client and database host computers must be on a Windows domain
- The net service name for the remote database must be specified:

```
CONNECT /@net_service_name AS SYSDBA
CONNECT /@net_service_name AS SYSOPER
CONNECT /@net_service_name AS SYSBACKUP
CONNECT /@net_service_name AS SYSDG
CONNECT /@net_service_name AS SYSKM
```

About OS Authentication of Normal Users

- The authentication is performed by the OS, no password is provided to the database
- The user must be created in the OS and in the DB
  - The db username must be prefixed with the value of the parameter **`OS_AUTHENT_PREFIX`** (default **`OPS$`**)
- Normally not needed for production systems

Creating OS-Authenticated Normal Users in a non-CDB Database

1. Create the OS user (if it does not exist):

```
useradd sam
```

2. Retrieve the value of **OS_AUTHENT_PREFIX** (default **OPS$**)
   - It can be changed to any value including the null (not recommended)
3. Create the DB user and grant any required privileges to it:

```
CREATE USER ops$sam IDENTIFIED EXTERNALLY;
```

4. As the OS user, login to the database:

```
su - sam
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db_1
export ORACLE_SID=oradb
export PATH=$PATH:$ORACLE_HOME/bin
sqlplus /
```

Creating OS-Authenticated Normal Users in a CDB

- Challenges:
  - **OS_AUTHENT_PREFIX** and **COMMON_USER_PREFIX** values are different
  - Common usernames should be prefixed with C## but Linux does not allow creating users containing # character
- A solution:

```
ALTER SYSTEM SET OS_AUTHENT_PREFIX='' SCOPE=SPFILE;
ALTER SYSTEM SET COMMON_USER_PREFIX='ZZ' SCOPE=SPFILE;
shutdown immediate
startup

CREATE USER ZZUSER1 IDENTIFIED EXTERNALLY CONTAINER=ALL;
GRANT CREATE SESSION TO ZZUSER1 ;
```

- Best practice: avoid it all together.

Security Caution

- With the default settings, system administrator can login as SYS

Summary

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

- Understand database administrator authentication
- Describe administrative OS authentication groups
- Allow administrative OS authentication to OS users
- Create OS-authenticated normal users