Managing User Profiles

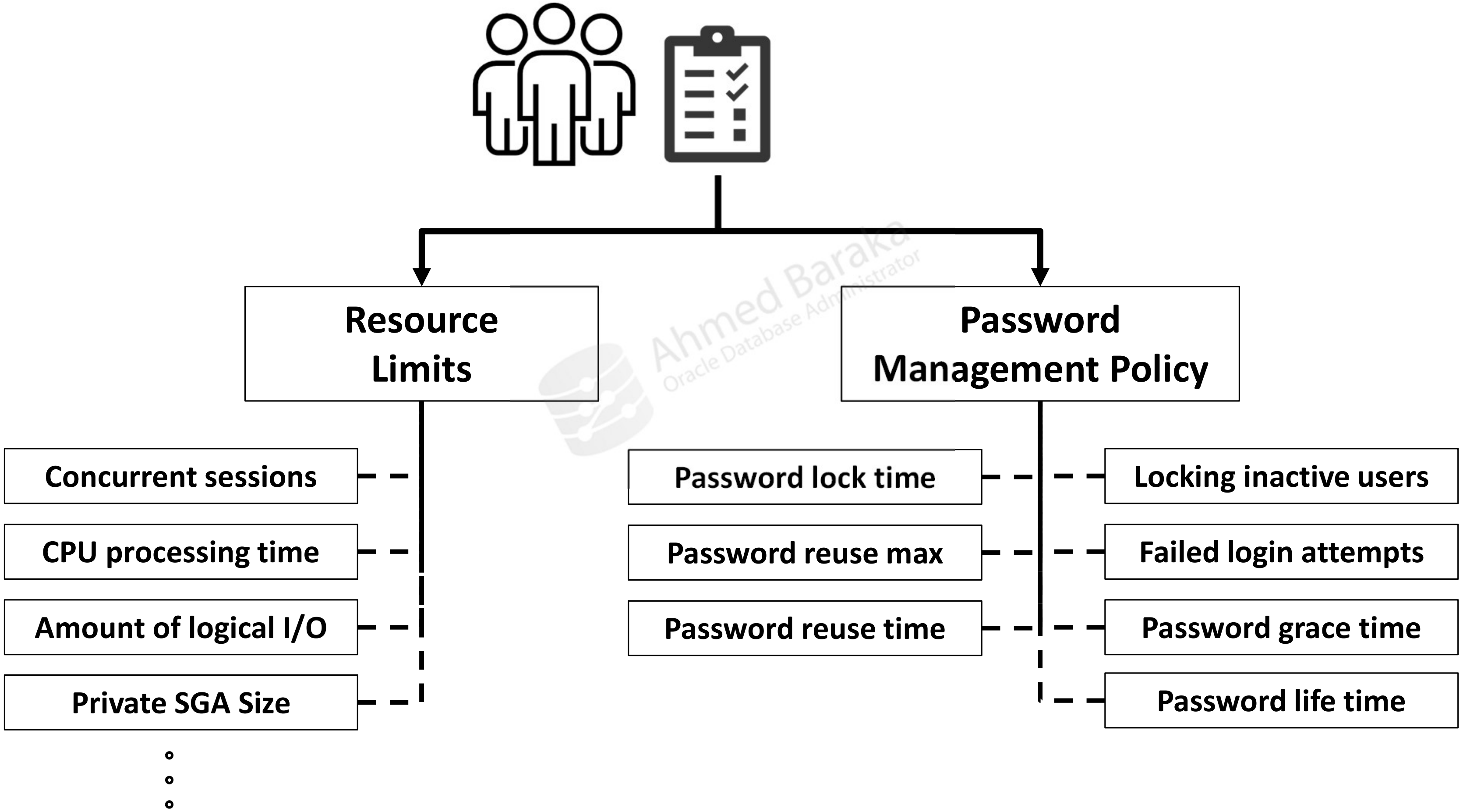
By Ahmed Baraka

Objectives

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

- Describe the user profile benefits
- Describe the password parameters in user profiles
- Describe the password change lifecycle
- Describe the resource limit parameters in user profiles
- Use user profiles
- Enable password complexity verification functions
- Obtain information about user passwords and profiles
- Implement gradual password rollover for applications
- Describe the general guide on using user profiles

User Profiles



Resource Limits

- Concurrent sessions
- CPU processing time
- Amount of logical I/O
- Private SGA Size
- ⋮

Password Management Policy

- Password lock time
- Password reuse max
- Password reuse time
- Locking inactive users
- Failed login attempts
- Password grace time
- Password life time

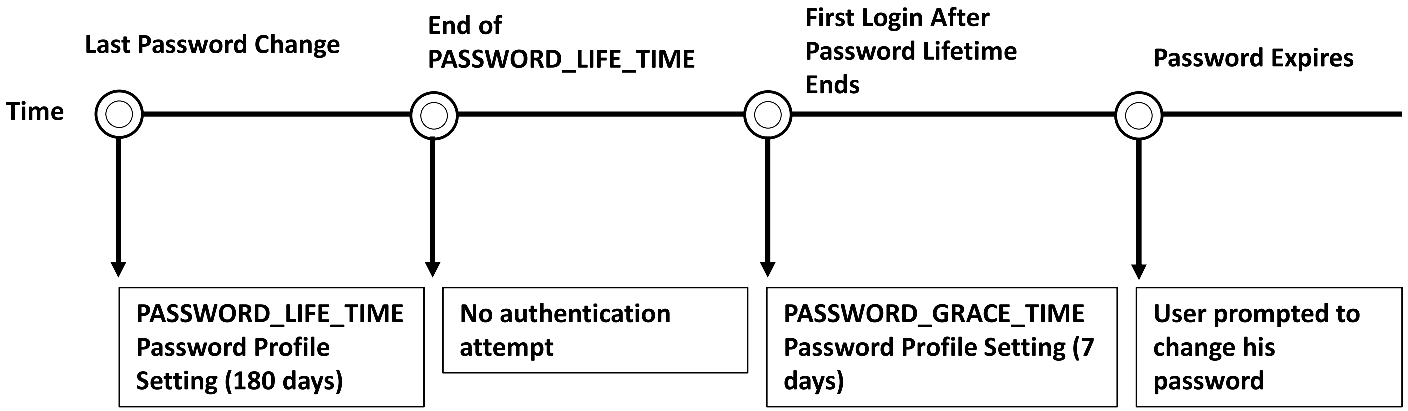
Password Parameters in User Profiles

Parameter	DEFAULT	Description
`INACTIVE_ACCOUNT_TIME`	UNLIMITED	Number of inactive days after which the account is locked
`FAILED_LOGIN_ATTEMPTS`	10	The maximum times a user can try to login and to fail before locking the account
`PASSWORD_GRACE_TIME`	7	Sets the number of days that a user has to change his or her password before it expires.
`PASSWORD_LIFE_TIME`	180	The number of days the user can use his or her current password.
`PASSWORD_LOCK_TIME`	1	the number of days an account will be locked after the specified number of consecutive failed login attempts.
`PASSWORD_REUSE_MAX`	UNLIMITED	The number of days after which a password can be reused
`PASSWORD_REUSE_TIME`	UNLIMITED	number of days before which a password cannot be reused.

Password Parameters in User Profiles

Parameter	DEFAULT	Description
PASSWORD_VERIFY_FUNCTION	NULL	Sets the password complexity function

Password Change Lifecycle



Time

Last Password Change

End of PASSWORD_LIFE_TIME

First Login After Password Lifetime Ends

Password Expires

PASSWORD_LIFE_TIME Password Profile Setting (180 days)

No authentication attempt

PASSWORD_GRACE_TIME Password Profile Setting (7 days)

User prompted to change his password

DBA_USERS.ACCOUNT_STATUS	OPEN	EXPIRED (GRACE)	EXPIRED
Error Message	None	ORA-28002: The password will expire in n days.	ORA-28001: The password has expired
Prompted for new password?	No	No	Yes

Some applications are not compatible with this stage.

Resource Limit Parameters in User Profiles

Parameter	DEFAULT	Description
SESSIONS_PER_USER	UNLIMITED	Maximum number of concurrent sessions for the user
CPU_PER_SESSION	UNLIMITED	CPU time limit for a session, expressed in hundredth of seconds
CPU_PER_CALL	UNLIMITED	The CPU time limit for a call (a parse, execute, or fetch), expressed in hundredths of seconds
CONNECT_TIME	UNLIMITED	The total elapsed time (in minutes) limit for a session
IDLE_TIME	UNLIMITED	The permitted period of continuous inactive time during a session, in minutes
LOGICAL_READS_PER_SESSION	UNLIMITED	The permitted number of data blocks read in a session
LOGICAL_READS_PER_CALL	UNLIMITED	The permitted number of data blocks read for a call to process a SQL statement
PRIVATE_SGA	UNLIMITED	The amount of private space a session can allocate
COMPOSITE_LIMIT	UNLIMITED	The total resource cost for a session, expressed in service units

Password Limits in DEFAULT Profile

```
SQL> SELECT RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE
PROFILE='DEFAULT' AND  RESOURCE_TYPE ='PASSWORD' ;

RESOURCE_NAME                    LIMIT
-------------------------------- --------------------------
FAILED_LOGIN_ATTEMPTS            10
PASSWORD_LIFE_TIME               180
PASSWORD_REUSE_TIME              UNLIMITED
PASSWORD_REUSE_MAX               UNLIMITED
PASSWORD_VERIFY_FUNCTION         NULL
PASSWORD_LOCK_TIME               1
PASSWORD_GRACE_TIME              7
INACTIVE_ACCOUNT_TIME            UNLIMITED
```

Using User Profiles

1. Decide about the required profiles and their settings
2. Create the profiles
3. Assign the profiles to the users

Creating User Profiles

- **CREATE PROFILE** system privilege is required
- To create a profile:

```
CREATE PROFILE emp_prof LIMIT
 FAILED_LOGIN_ATTEMPTS 6
 PASSWORD_LIFE_TIME 60
 PASSWORD_REUSE_TIME 60
 PASSWORD_REUSE_MAX 5
 PASSWORD_LOCK_TIME 1/24
 PASSWORD_GRACE_TIME 10
 PASSWORD_VERIFY_FUNCTION DEFAULT
 SESSIONS_PER_USER UNLIMITED
 CPU_PER_SESSION UNLIMITED
 CONNECT_TIME 50
 LOGICAL_READS_PER_SESSION DEFAULT
 COMPOSITE_LIMIT 7500000;
```

Assigning a Profile to a User

- To assign a profile to a user:

```
ALTER USER scott PROFILE emp_prof;
```

- At the time of user creation

```
CREATE USER scott
 IDENTIFIED BY HisPassword
 DEFAULT TABLESPACE users
 TEMPORARY TABLESPACE temp
 QUOTA 500K ON users
 PROFILE clerk;
```

- To know the currently assigned profile for a user:

```
SELECT PROFILE FROM DBA_USERS WHERE USERNAME='HR'
```

Modifying Profile Parameters

- User **ALTER PROFILE** statement:

```
ALTER PROFILE hr_prof LIMIT
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 15
INACTIVE_ACCOUNT_TIME 30;
```

About ORA_STIG_PROFILE User Profile

- Is designed for Security Technical Implementation Guide compliance.

```
SELECT RESOURCE_NAME, LIMIT FROM dba_profiles WHERE
PROFILE='ORA_STIG_PROFILE';

RESOURCE_NAME                    LIMIT
-------------------------------- --------------------
IDLE_TIME                        15
FAILED_LOGIN_ATTEMPTS            3
PASSWORD_LIFE_TIME               60
PASSWORD_REUSE_TIME              365
PASSWORD_REUSE_MAX               10
PASSWORD_VERIFY_FUNCTION         ORA12C_STIG_VERIFY_FUNCTION
PASSWORD_LOCK_TIME               UNLIMITED
PASSWORD_GRACE_TIME              5
INACTIVE_ACCOUNT_TIME            35
...
```

About Password Complexity Verification Functions

- Verifies that the account new passwords complies with the password complexity standard
- Four functions are provided in **`$ORACLE_HOME/rdbms/admin/catpvf.sql`**
  - **`ora12c_stig_verify_function`**
  - **`ora12c_strong_verify_function`**
  - **`ora12c_verify_function`**
  - **`verify_function_11G`**
- They apply for non-SYS users
- Set a verification function in the **`DEFAULT`** profile
- You can create your own function

About ora12c_stig_verify_function

- The password has at least 15 characters
- The password has at least 1 lower case character and at least 1 upper case character
- The password has at least 1 digit
- The password has at least 1 special character
- The password differs from the previous password by at least 8 characters

Enabling Password Complexity Verification

1. Login with an account with administrative privileges
2. If the functions are not already there, create them.

```
@$ORACLE_HOME/rdbms/admin/catpvf.sql
```

3. Decide which function to use (or create your own)
4. Grant the users who must use the function the **EXECUTE** privilege:

```
GRANT scott EXECUTE ON ora12c_strong_verify_function;
```

5. In the user profile, set the **PASSWORD_VERIFY_FUNCTION** setting:

```
ALTER PROFILE default LIMIT
PASSWORD_VERIFY_FUNCTION ora12c_strong_verify_function
```

Obtain Information About Account Passwords

View	Column	Description
DBA_USERS	EXPIRY_DATE	The password expiration date
DBA_USERS	LAST_LOGIN	The user's last login time
DBA_USERS	LOCK_DATE	Date the account was locked if account status was LOCKED
DBA_USERS	PROFILE	User resource profile name
DBA_USERS	LAST_LOGIN	The time of the last user login (not populated for admins)
DBA_USERS	PASSWORD_CHANGE_DATE	Last password change time (19c+)
SYS.USER$	PTIME	Last password change time

Obtain Information About User Profiles

Column	Description
DBA_PROFILES	Displays all profiles and their limits
USER_PASSWORD_LIMITS	Retrieves the password profile parameters that are assigned to the user
USER_RESOURCE_LIMITS	Retrieves the resource limits for the current user

Gradual Database Password Rollover for Applications

- Allows the application account password to be updated without application downtime
- Available in 19.12 and 21c
- Is set by specifying **PASSWORD_ROLLOVER_TIME**
  - Minimum one hour (1/24) and maximum 60 days

```
ALTER PROFILE hr_profile LIMIT PASSWORD_ROLLOVER_TIME 1;
```

- When it is active and the password is reset, the **DBA_USERS.ACCOUNT_STATUS** column is '**OPEN & IN ROLLOVER**'
- To disable the gradual password rollover set **PASSWORD_ROLLOVER_TIME** limit to 0

Using User Profiles: General Guide

- Categorize the users and create a profile for each category
- If there is a password usage policy, implement it.
  - If there is no password usage policy, create one.
- If the database user is used by all application users:
  - Make schema-only account
  - Consider implementing “Gradual database password rollover for applications”.
- For resource limit settings, it is recommended to go for the resource manager in Oracle database

Summary

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

- Describe the user profile benefits
- Describe the password parameters in user profiles
- Describe the password change lifecycle
- Describe the resource limit parameters in user profiles
- Use user profiles
- Enable password complexity verification functions
- Obtain information about user passwords and profiles
- Implement gradual password rollover for applications
- Describe the general guide on using user profiles