Administering User Security

Objectives

After completing this lesson, you should be able to:

- Create and manage database user accounts:
  - Authenticate users
  - Assign default storage areas (tablespaces)
- Grant and revoke privileges
- Create and manage roles
- Create and manage profiles:
  - Implement standard password security features
  - Control resource usage by users

Database User Accounts

Each database user account has:

- A unique username
- An authentication method
- A default tablespace
- A temporary tablespace
- A user profile
- An initial consumer group
- An account status

A schema:

- Is a collection of database objects that are owned by a database user
- Has the same name as the user account

3

Predefined Administrative Accounts

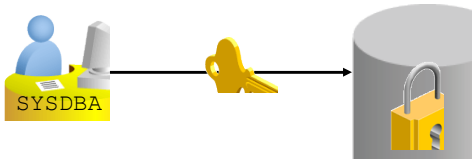
- `SYS`:
  - Owns the data dictionary and the Automatic Workload Repository (AWR)
  - Used for startup and shutdown of the database instance
- `SYSTEM`: Owns additional administrative tables and views
- `SYSBACKUP`: Facilitates Oracle Recovery Manager (RMAN) backup and recovery operations
- `SYSDG`: Facilitates Oracle Data Guard operations
- `SYSKM`: Facilitates Transparent Data Encryption wallet operations

4

Protecting Privileged Accounts

Privileged accounts can be protected by:

- Using a password file with case-sensitive passwords
- Enabling strong authentication for administrator roles



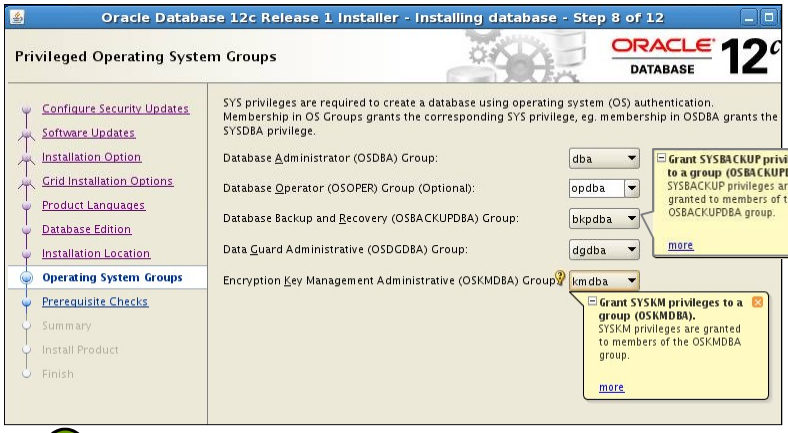
5

Authenticating Users

- Password: User definition includes a password that must be supplied when the user attempts to log in to the database
- External: Authentication by a method outside the database (operating system, Kerberos, or Radius)
- Global: Users are identified by using an LDAP-based directory service

6

OS Authentication and OS Groups



1

$ORACLE_HOME/rdbms/lib/config.[cs]

2

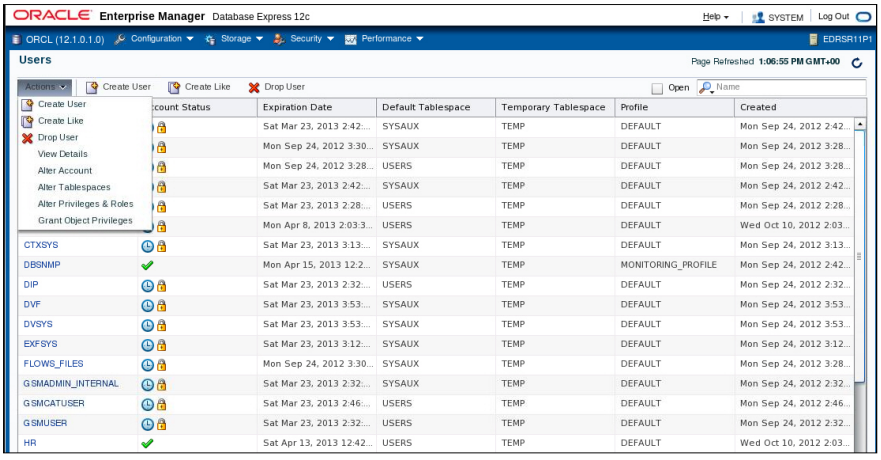
```
#define SS_DBA_GRP "dba"
#define SS_OPER_GRP "opdba"
#define SS_ASM_GRP ""
#define SS_BKP_GRP "bkpdba"
#define SS_DGD_GRP "dgdba"
#define SS_KMT_GRP "kmdba"
```

3

```
$ mv config.o config.o.orig
$ make -f ins_rdbms.mk ioracle
```

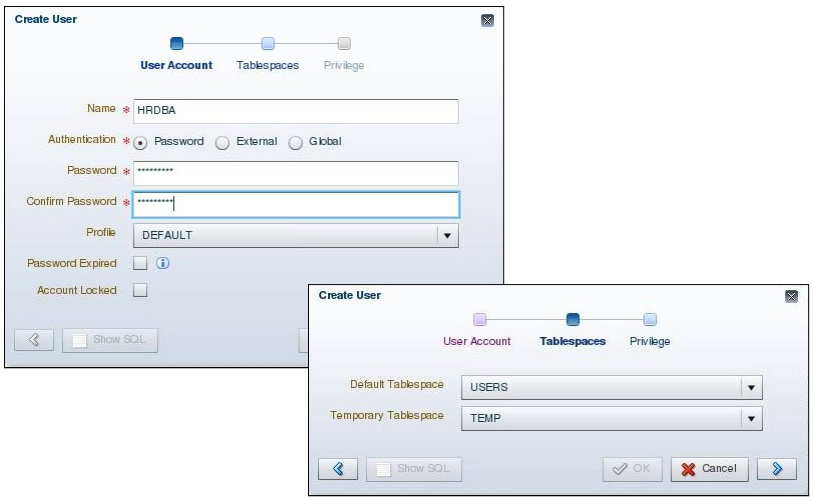
7

Managing Users



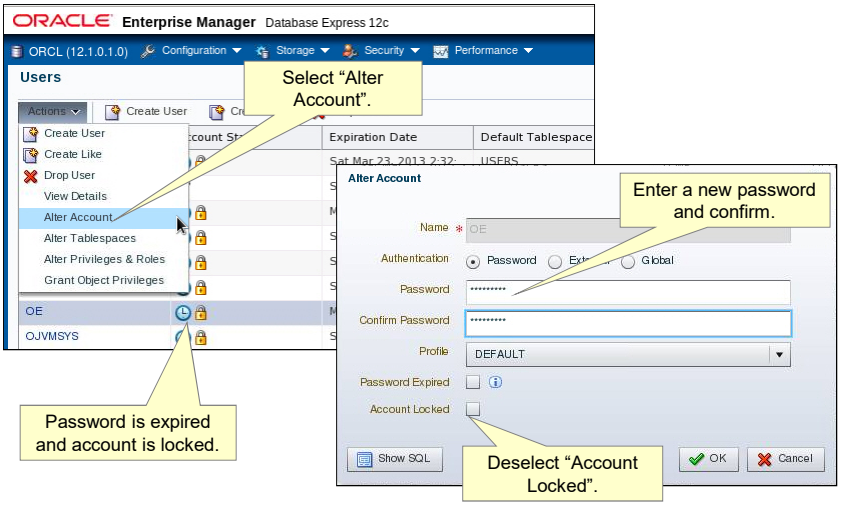
8

Creating a User



9

Unlocking a User Account and Resetting the Password

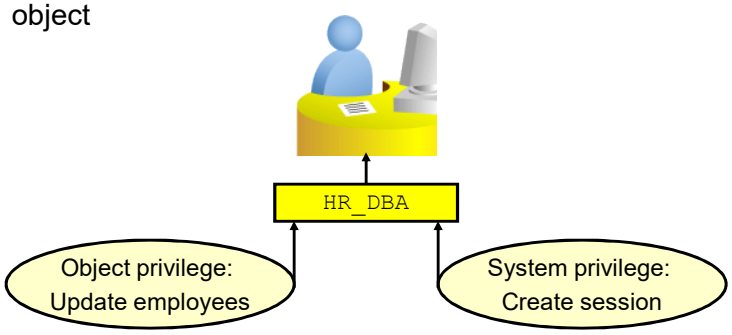


10

Privileges

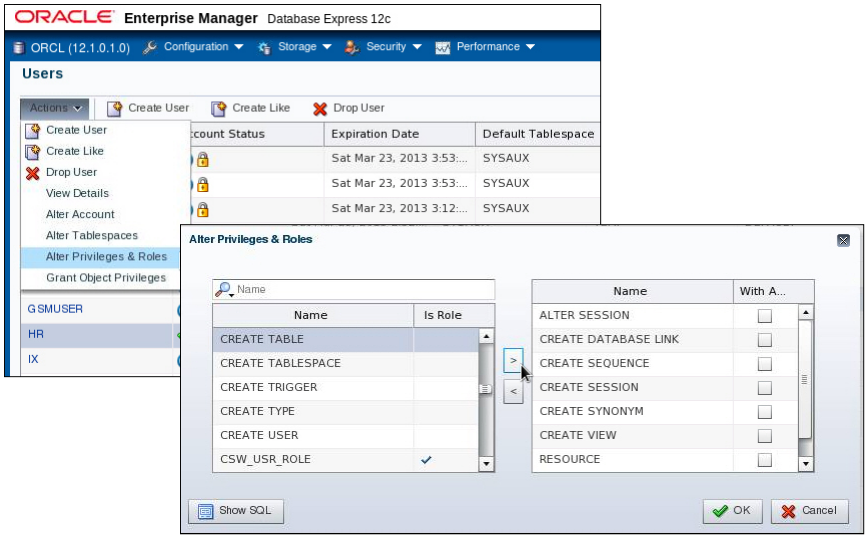
There are two types of user privileges:

- System: Enables users to perform particular actions in the database
- Object: Enables users to access and manipulate a specific object



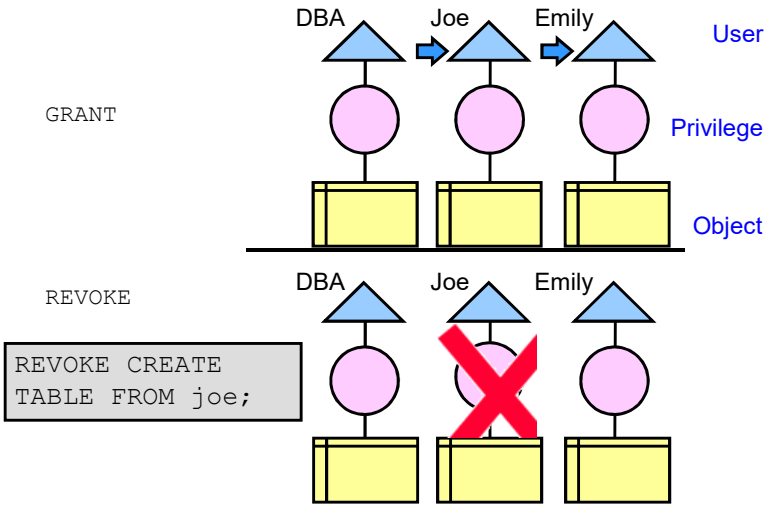
11

System Privileges



12

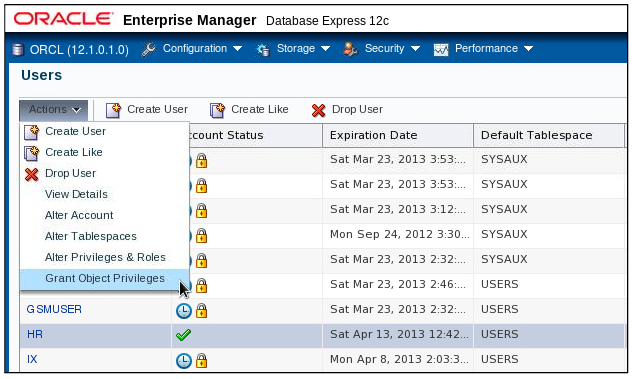
Revoking System Privileges with ADMIN OPTION




```
REVOKE CREATE
TABLE FROM joe;
```

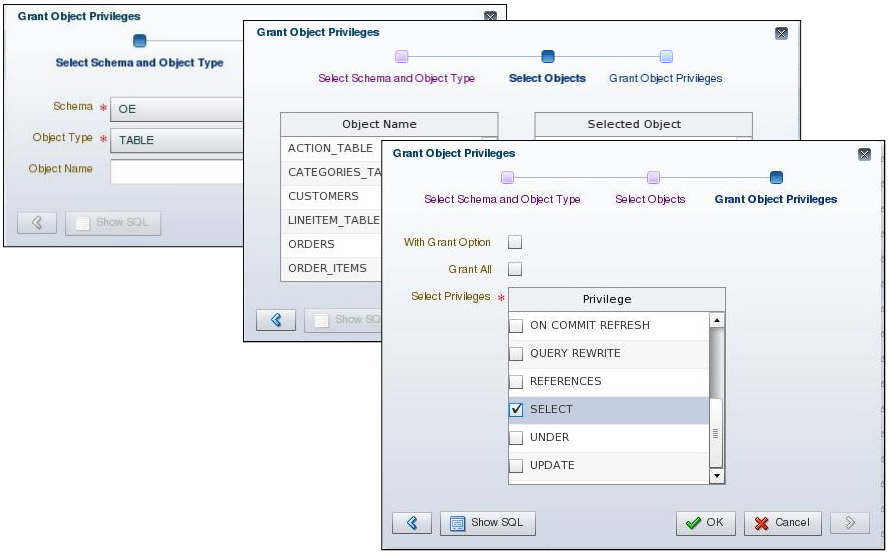
13

Granting Object Privileges



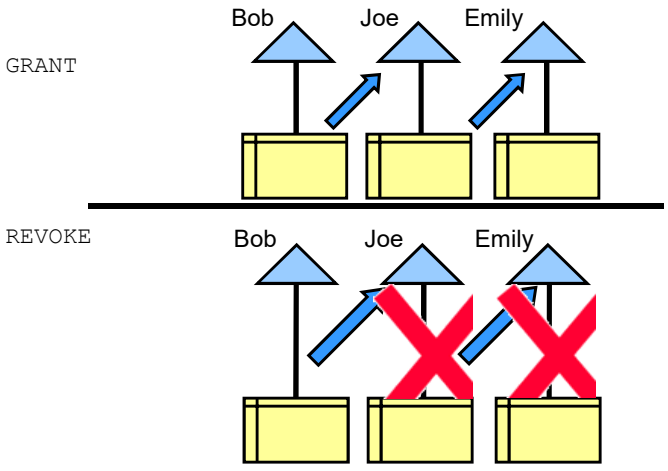
14

Object Privileges



15

Revoking Object Privileges with GRANT OPTION



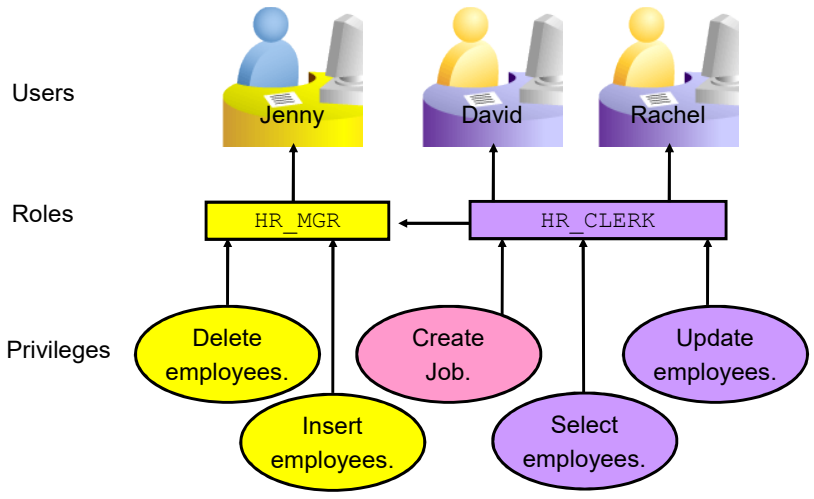
16

Using Roles to Manage Privileges

- Roles:
  - Used to group together privileges and roles
  - Facilitate granting of multiple privileges or roles to users
- Benefits of roles:
  - Easier privilege management
  - Dynamic privilege management
  - Selective availability of privileges

17

Assigning Privileges to Roles and Assigning Roles to Users



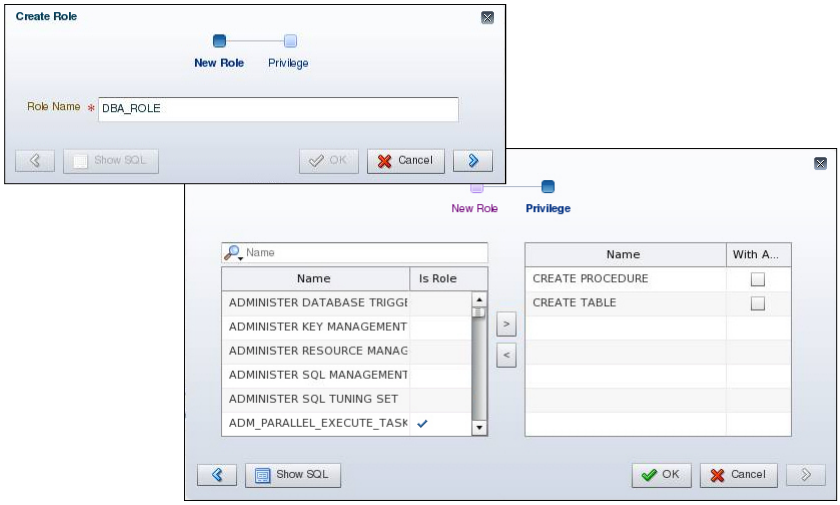
18

Predefined Roles

Role	Privileges Included
CONNECT	CREATE SESSION
DBA	Most system privileges; several other roles. Do not grant to non-administrators.
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
SELECT_CATALOG_ROLE	SELECT privileges on data dictionary objects

19

Creating a Role



20

Secure Roles

- Roles can be nondefault and enabled when required.

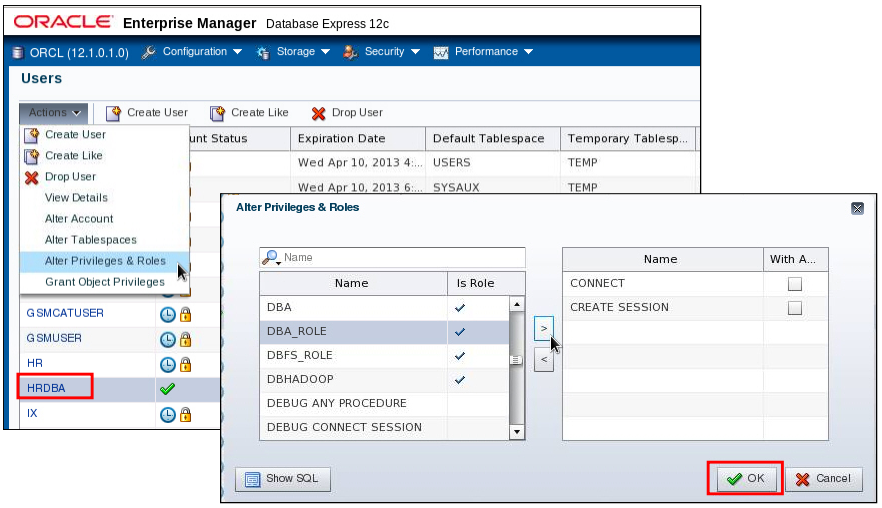
```
SET ROLE vacationdba;
```

- Roles can be protected through authentication.
- Roles can also be secured programmatically.

```
CREATE ROLE secure_application_role
IDENTIFIED USING <security_procedure_name>;
```

21

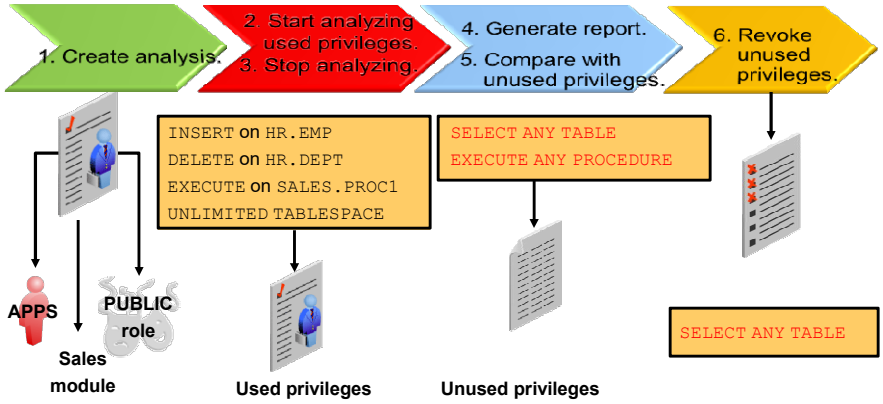
Assigning Roles to Users



22

Privilege Analysis

- Analyze used privileges to revoke unnecessary privileges.
- Use `DBMS_PRIVILEGE_CAPTURE` package.



23

Profiles and Users

Users are assigned only one profile at a time.

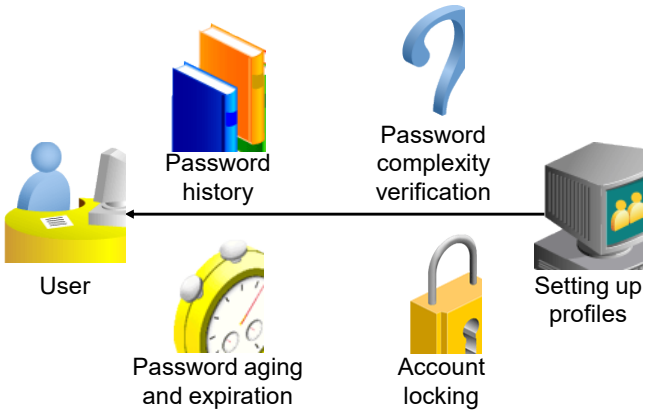
Profiles:

- Control resource consumption
- Manage account status and password expiration

Note: `RESOURCE_LIMIT` must be set to `TRUE` before profiles can impose resource limitations.

24

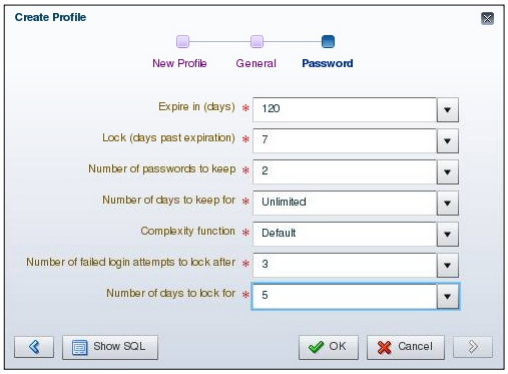
Implementing Password Security Features



Note: Do not use profiles that cause the `SYS`, `SYSMAN`, and `DBSNMP` passwords to expire and the accounts to be locked.

25

Creating a Password Profile



26

Supplied Password Verification Functions

- The following functions are created by the `$ORACLE_HOME/rdbms/admin/utlpwdmg.sql` script:
  - `VERIFY_FUNCTION_11g`
  - `ORA12C_VERIFY_FUNCTION`
  - `ORA12C_STRONG_VERIFY_FUNCTION`

- The functions require the following of passwords:
  - Have a minimum number of characters
  - Not be the username, username with a number, or username reversed
  - Not be the database name or the database name with a number
  - Have at least one alphabetic and one numeric character
  - Differ from the previous password by at least three letters

27

Modifications to the Default Profile

The `utlpwdmg.sql` script also modifies the `DEFAULT` profile as follows:

```
ALTER PROFILE DEFAULT LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX  UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
PASSWORD_LOCK_TIME 1
PASSWORD_VERIFY_FUNCTION
  ora12c_verify_function;
```

28

Assigning Quotas to Users

- Users who do not have the `UNLIMITED TABLESPACE` system privilege must be given a quota before they can create objects in a tablespace.
- Quotas can be:
  - A specific value in megabytes or kilobytes
  - Unlimited

29

Summary

In this lesson, you should have learned how to:

- Create and manage database user accounts:
  - Authenticate users
  - Assign default storage areas (tablespaces)
- Grant and revoke privileges
- Create and manage roles
- Create and manage profiles:
  - Implement standard password security features
  - Control resource usage by users

30