

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

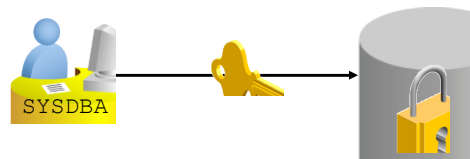
- **SYS:**
 - Owns the data dictionary and the Automatic Workload Repository (AWR)
 - Used for startup and shutdown of the database instance
- **SYSTEM:** Owns additional administrative tables and views
- **SYSBACKUP:** Facilitates Oracle Recovery Manager (RMAN) backup and recovery operations
- **SYSDG:**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

Oracle Database 12c Release 1 Installer - Installing database - Step 8 of 12

Privileged Operating System Groups

SYS privileges are required to create a database using operating system (OS) authentication. Membership in OS Groups grants the corresponding SYS privilege, eg. membership in OSDBA grants the SYSDBA privilege.

Database Administrator (OSDBA) Group: dba

Database Operator (OSOPER) Group (Optional): opdba

Database Backup and Recovery (OSBACKUPDBA) Group: bkpdba

Data Guard Administrative (OSDGDBA) Group: dgdba

Encryption Key Management Administrative (OSKMDBA) Group: kmdba

[Grant SYSBACKUP privileges to a group \(OSBACKUPDBA\).](#)
SYSBACKUP privileges are granted to members of the OSBACKUPDBA group.

[Grant SYSKM privileges to a group \(OSKMDBA\).](#)
SYSKM privileges are granted to members of the OSKMDBA group.

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

ORACLE Enterprise Manager Database Express 12c

Help SYSTEM Log Out

ORCL (12.1.0.1.0) Configuration Storage Security Performance

Users Page Refreshed 1:06:55 PM GMT+00

Actions: Create User Create Like Drop User Open Name

Account	Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created
CTXSYS	✓	Sat Mar 23, 2013 3:13...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 3:13...
DBSNMP	✓	Mon Apr 15, 2013 12:2...	SYSAUX	TEMP	MONITORING_PROFILE	Mon Sep 24, 2012 2:42...
DIP	✓	Sat Mar 23, 2013 2:32...	USERS	TEMP	DEFAULT	Mon Sep 24, 2012 2:32...
DVF	✓	Sat Mar 23, 2013 3:53...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 3:53...
DVSY	✓	Sat Mar 23, 2013 3:53...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 3:53...
EXFSYS	✓	Sat Mar 23, 2013 3:12...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 3:12...
FLWS_FILES	✓	Mon Sep 24, 2012 3:30...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 3:28...
GSMADMIN_INTERNAL	✓	Sat Mar 23, 2013 2:32...	SYSAUX	TEMP	DEFAULT	Mon Sep 24, 2012 2:32...
GSMCATUSER	✓	Sat Mar 23, 2013 2:46...	USERS	TEMP	DEFAULT	Mon Sep 24, 2012 2:46...
GSMUSER	✓	Sat Mar 23, 2013 2:32...	USERS	TEMP	DEFAULT	Mon Sep 24, 2012 2:32...
HR	✓	Sat Apr 13, 2013 12:42...	USERS	TEMP	DEFAULT	Wed Oct 10, 2012 2:03...

8

Creating a User

The first screenshot shows the 'Create User' dialog with the 'User Account' tab selected. The 'Name' field is 'HRDBA'. The 'Authentication' is set to 'Password'. The 'Password' and 'Confirm Password' fields are masked with asterisks. The 'Profile' is set to 'DEFAULT'. The 'Password Expired' and 'Account Locked' checkboxes are unchecked. The 'Show SQL' button is visible at the bottom.

The second screenshot shows the 'Create User' dialog with the 'Tablespaces' tab selected. The 'Default Tablespace' is set to 'USERS' and the 'Temporary Tablespace' is set to 'TEMP'. The 'OK', 'Cancel', and 'Show SQL' buttons are visible at the bottom.

9

Unlocking a User Account and Resetting the Password

The first screenshot shows the 'Users' page in Oracle Enterprise Manager. A callout points to 'Alter Account' in the Actions menu. Another callout points to the 'Account Locked' status of user 'OE', stating 'Password is expired and account is locked.'

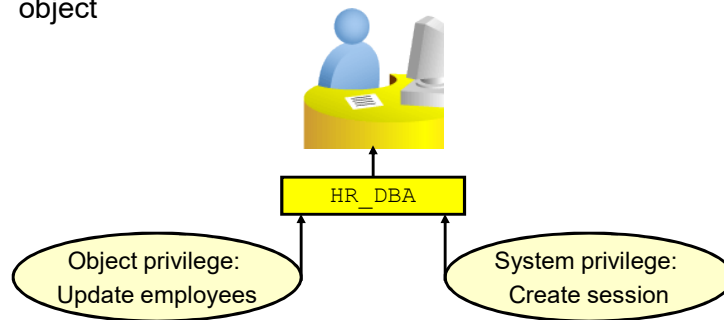
The second screenshot shows the 'Alter Account' dialog. A callout points to the 'Password' and 'Confirm Password' fields, stating 'Enter a new password and confirm.' Another callout points to the 'Account Locked' checkbox, stating 'Deselect "Account Locked".'

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

ORACLE Enterprise Manager Database Express 12c

ORCL (12.1.0.1.0) Configuration Storage Security Performance

Users

Actions: Create User, Create Like, Drop User

Account	Status	Expiration Date	Default Tablespace
HR	Locked	Sat Mar 23, 2013 3:53:...	SYSAUX
IX	Locked	Sat Mar 23, 2013 3:53:...	SYSAUX
CSW_USR_ROLE	Unlocked	Sat Mar 23, 2013 3:12:...	SYSAUX

Alter Privileges & Roles

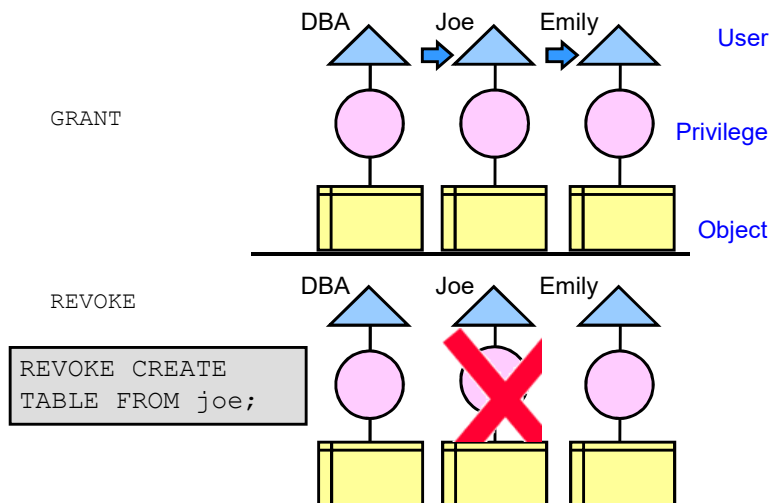
Name	Is Role
CREATE TABLE	
CREATE TABLESPACE	
CREATE TRIGGER	
CREATE TYPE	
CREATE USER	
CSW_USR_ROLE	✓

Name	With A...
ALTER SESSION	<input type="checkbox"/>
CREATE DATABASE LINK	<input type="checkbox"/>
CREATE SEQUENCE	<input type="checkbox"/>
CREATE SESSION	<input type="checkbox"/>
CREATE SYNONYM	<input type="checkbox"/>
CREATE VIEW	<input type="checkbox"/>
RESOURCE	<input type="checkbox"/>

Show SQL OK Cancel

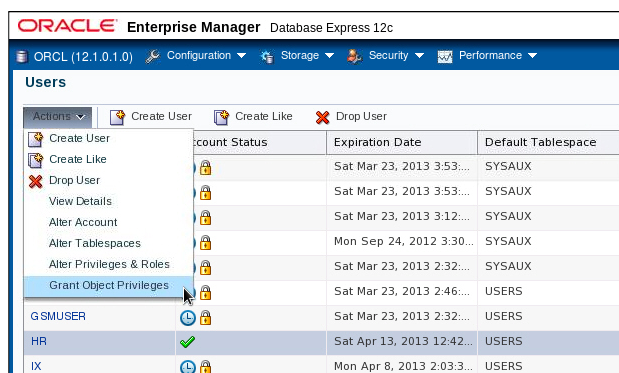
12

Revoking System Privileges with ADMIN OPTION



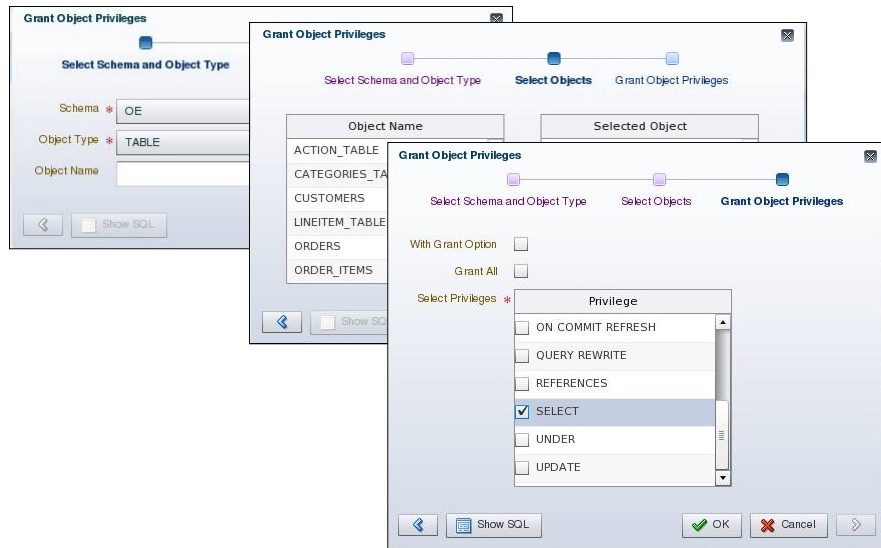
13

Granting Object Privileges



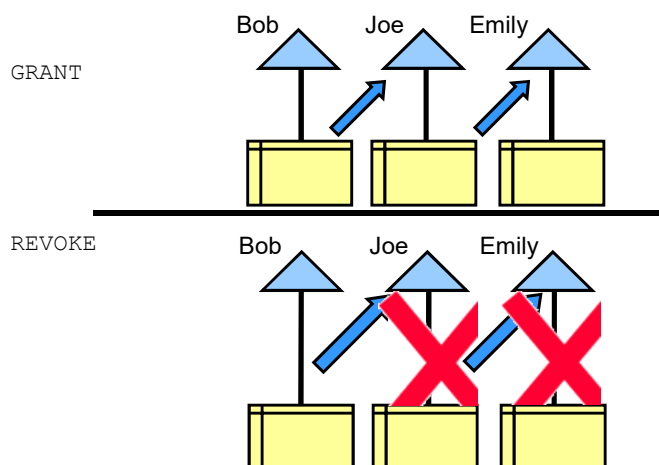
14

Object Privileges



15

Revoking Object Privileges with GRANT OPTION



16

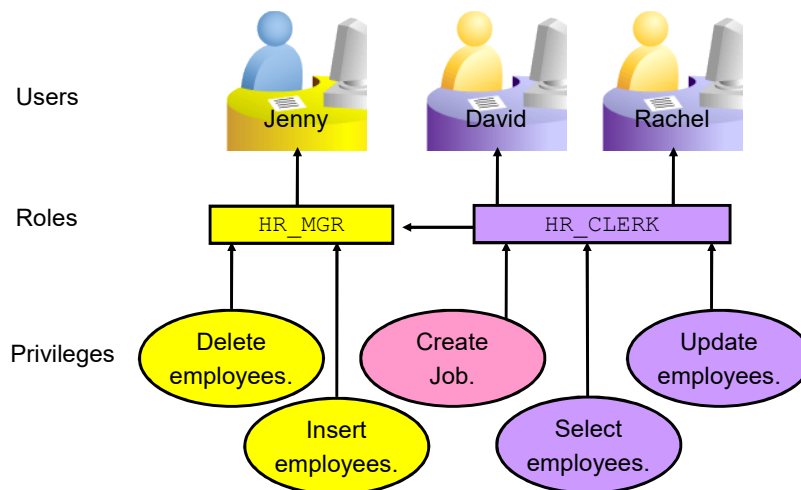
Using Roles to Manage Privileges

- 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

Creating a Role

Secure Roles

- Roles can be nondefault and enabled when required.

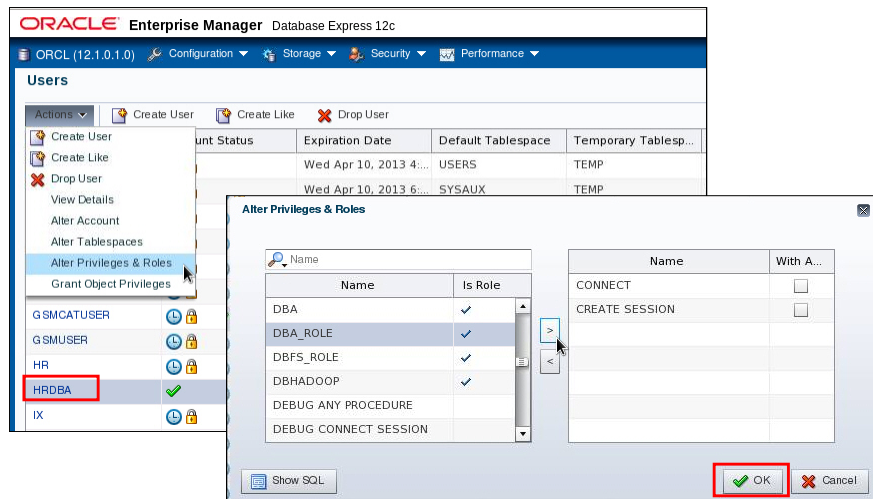
```
SET ROLE vacationdba;
```

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

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

21

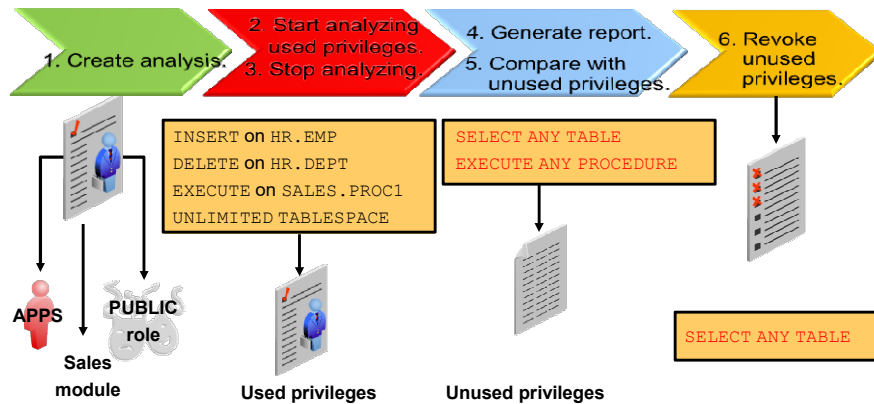
Assigning Roles to Users



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

The 'Create Profile' dialog box shows the 'General' tab with the following settings:

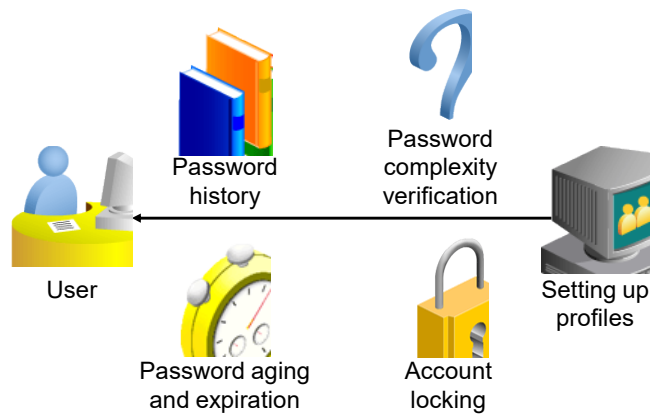
- CPU/Session (Sec./100): 1000
- CPU/Call (Sec./100): Unlimited
- Connect Time (Min.): Default
- Idle Time (min.): 60
- Concurrent Session (Per User): Unlimited
- Reads/Session (Blocks): Unlimited
- Reads/Call (Blocks): Unlimited
- Private SGA: Unlimited
- Composite Limit (Service Units): Unlimited

Buttons at the bottom include 'Show SQL', 'OK', 'Cancel', and a right arrow.

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

The screenshot shows the 'Create Profile' dialog box with the 'Password' tab selected. The settings are as follows:

Setting	Value
Expire in (days)	120
Lock (days past expiration)	7
Number of passwords to keep	2
Number of days to keep for	Unlimited
Complexity function	Default
Number of failed login attempts to lock after	3
Number of days to lock for	5

At the bottom, there are buttons for '< Back', 'Show SQL', 'OK', 'Cancel', and '> Next'.

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