# INFS602 Physical Database Design

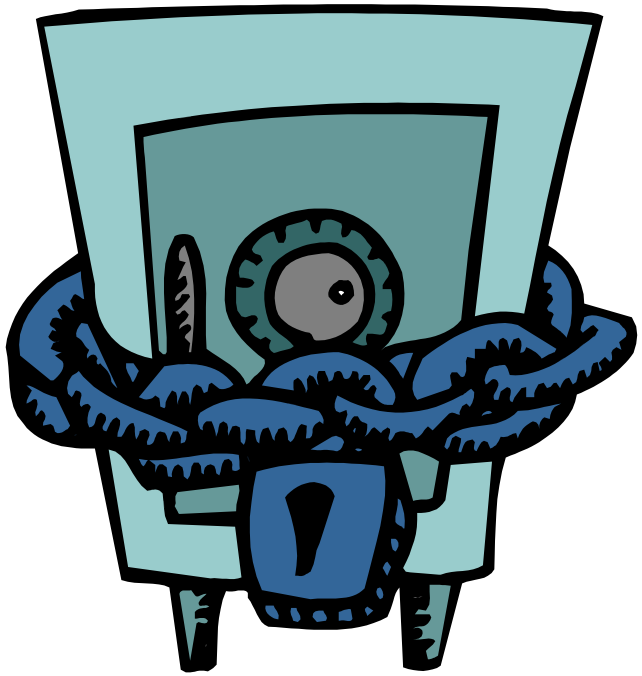
Database Security

# Learning Outcomes

- Develop a simple security policy for a multi-user database system
- Create and assign **profiles** to users
- Identify and assign **system** and **object privileges** to users
- Create and modify **roles**

# Database Security

- Protection of the data against accidental or intentional loss, destruction, or misuse



# Threats to Database Security

- Accidental losses
- Theft and fraud
- Loss of privacy, confidentiality
- Loss of data integrity
- Loss of availability

# A Data Security Plan

- Administration policies, standards and procedures.
  - Policies
    - All users must have passwords.
    - Passwords must be changed every six months.
  - Standards
    - A password must have a minimum of six characters.
  - Procedures
    - To create an account.
      - The end user sends a written request for an account creation to the DBA.
      - The DBA approves the request ….
- Physical protections
- Data management protection software.

# Managing Users and Resources

- When you create a database user (account), you specify the following attributes of the user:
  - User name
  - Authentication method
  - Default tablespace
  - Temporary tablespace
  - Other tablespaces and quotas
  - User profile

# Data Management Controls

- Views
- Authentication
- Authorisation
- Encryption procedures
- Backup, journaling and check pointing

# User Accounts

- Each Oracle database has a list of valid database users.
- The database contains several default accounts, including the default administrative account SYSTEM
- To access a database, a user must provide a valid **user name** and **authentication credential**.

# Authorisation

- Restrict access to data
- Restrict user actions when accessing data

Authorisation table for Salespeople

| | Customer Records | Order Records |
|---|---|---|
| Read | | |
| Insert | | |
| Modify | | |
| Delete | | |

# Authorisation

- Restrict access to data
- Restrict user actions when accessing data

Authorisation table for Salespeople

| | Customer Records | Order Records |
|---|---|---|
| Read | ✓ | ✓ |
| Insert | ✓ (?) | ✓ |
| Modify | ✓ Log | ✓ Log |
| Delete | ○ No | ✓ (?) |

# ORACLE Security

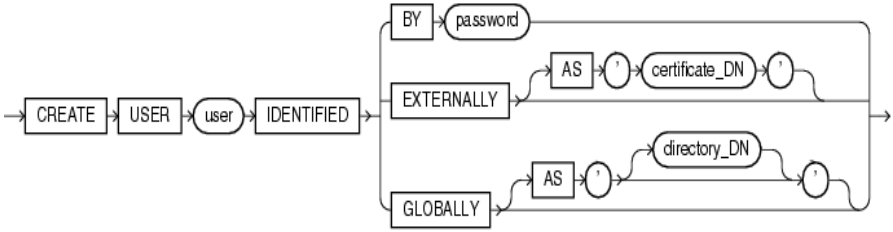
- Security domain
  - Authentication mechanism
  - Tablespace quotas
  - Default tablespace
  - Temporary tablespace
  - Account locking
  - Resource limits, via profiles
  - Direct privileges, both system and object privileges
  - Role privileges

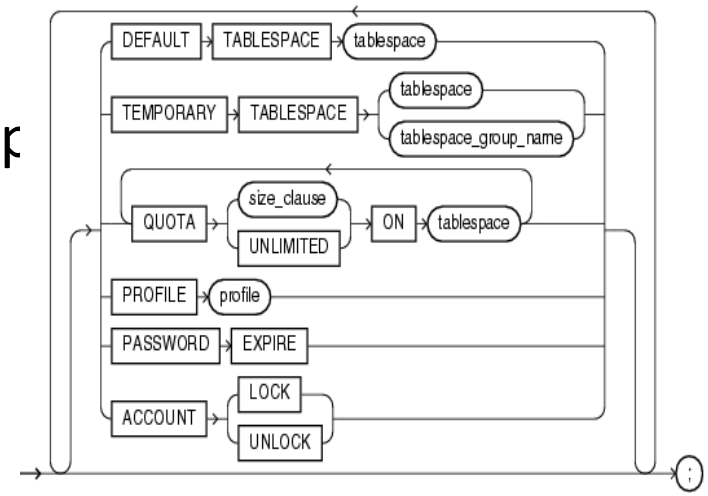
# Checklist for Creating Users

- Choose a username and authentication mechanism (password, token, other)
- Identify tablespaces in which the user needs to store objects
- Decide on quotas for each tablespace
- Create a user
  - Assign quota on default tablespace, and any other tablespaces needed for user
  - Assign a temporary tablespace
- Grant privileges and roles to the user

# Creating a New User

- CREATE USER james
- IDENTIFIED BY banana
- DEFAULT TABLESPACE ts_01
- TEMPORARY TABLESPACE temp
- QUOTA 15M ON ts_01
- QUOTA 10M ON ts_02
- PASSWORD EXPIRE;




```
CREATE USER books_admin IDENTIFIED BY MyPassword;
```

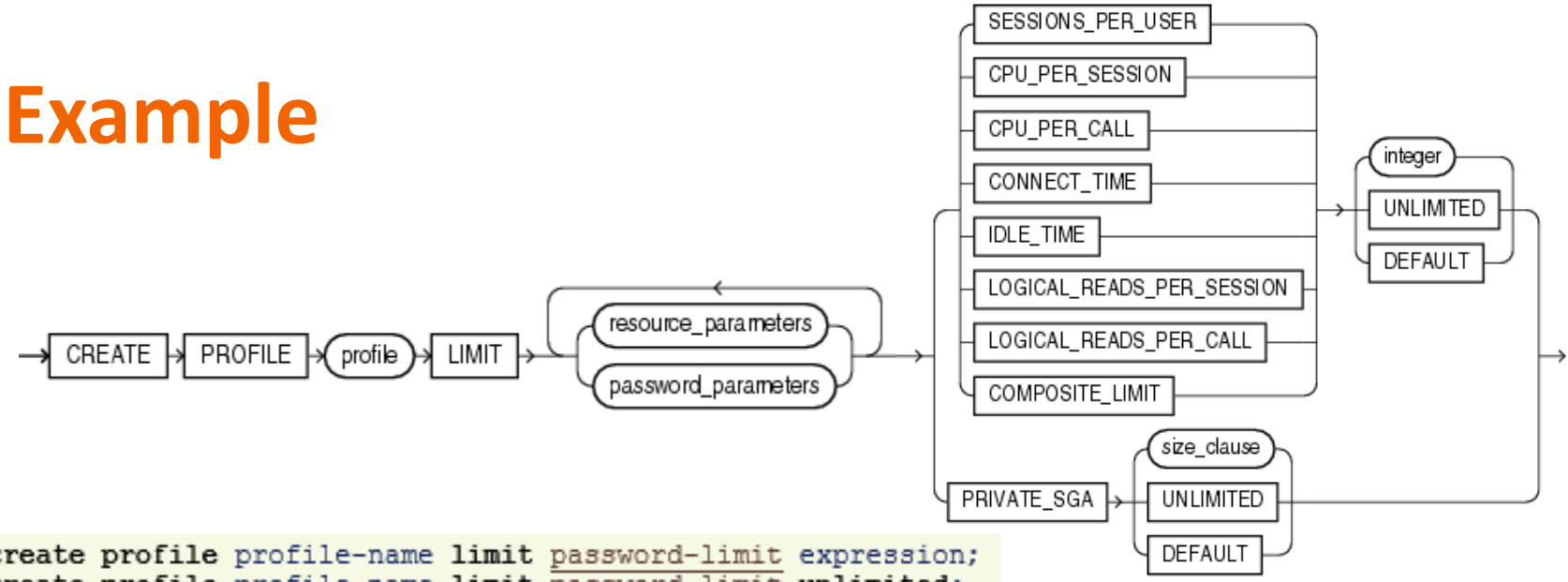
# Profiles

- A Profile is a named set of resource limits
- A DEFAULT profile is automatically created by the oracle server
- Profiles are used to:
  - Restrict users from performing some operations that require heavy use of resources
  - Ensure that users log off the database
  - Enable group resource limits for similar users
  - Control the use of passwords

# Creating a Profile: Resource Limit

- CREATE PROFILE developer_profile LIMIT
- SESSIONS_PER_USER 2
- CPU_PER_SESSION 10000
- IDLE_TIME 60
- CONNECT_TIME 480;

# Example




```
create profile profile-name limit password-limit expression;
create profile profile-name limit password-limit unlimited;
create profile profile-name limit password-limit default;
```

```
create profile
  appl_profile
limit
  sessions_per_user               2   --
  cpu_per_session             10000   -- hunderth of seconds
  cpu_per_call                    1   -- hunderth of seconds
  connect_time            unlimited   -- minutes
  idle_time                      30   -- minutes
  logical_reads_per_session   default  -- db blocks
  logical_reads_per_call      default  -- db blocks
  -- composite_limit          default  --
  private_sga                    20M   --
  failed_login_attempts            3   --
  password_life_time              30   -- days
  password_reuse_time             12   --
  password_reuse_max      unlimited   --
  password_lock_time          default  -- days
  password_grace_time              2   -- days
  password_verify_function      null;
```

# Resource Limits

| Resource | Description |
|---|---|
| CPU_PER_SESSION | Total CPU time measured in hundredths of seconds |
| SESSIONS_PER_USER | Number of concurrent sessions allowed for each username |
| CONNECT_TIME | Elapsed connect time measured in minutes |
| IDLE_TIME | Period of inactive time measured in minutes |
| LOGICAL_READS_PER_SESSION | Number of data blocks (physical and logical reads) |
| PRIVATE_SGA | Private space in the SGA measured in bytes |
| CPU_PER_CALL | CPU time per call in hundredths of seconds |
| LOGICAL_READS_PER_CALL | Number of data blocks |

# Assigning Profiles to a User

- Profiles are assigned to users as part of the CREATE USER or ALTER USER commands.

| For a New User | For an Existing User |
| --- | --- |
| CREATE USER jane<br>IDENTIFIED BY banana<br>DEFAULT TABLESPACE ts_01<br>TEMPORARY TABLESPACE temp<br>QUOTA 15m ON ts_01<br>PASSWORD EXPIRE<br>PROFILE developer_profile; | ALTER USER james PROFILE<br>developer_profile; |

A default profile can be created – a default already exists within Oracle named DEFAULT – it is applied to any user not assigned another profile.

# Managing Privileges

- Two types of privileges:

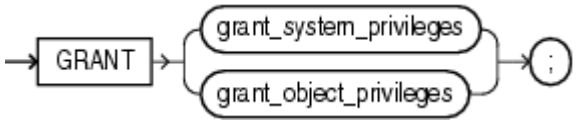
1- System privilege – enables users to perform a particular action in the database

2- Object privilege – enables users to access and manipulate a specific object

# System Privileges

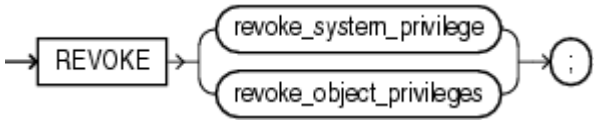
- There are over 100 system privileges
- System privileges can be classified as follows
  - Enabling system-wide operations e.g. CREATE SESSION, CREATE TABLESPACE
  - Enabling management of objects in a user's own schema e.g. CREATE TABLE
  - Enabling management of objects in any schema e.g. CREATE ANY TABLE

# Granting and Revoking System Privileges




GRANT privilege_name
ON object_name
TO {user_name |PUBLIC |role_name}
[WITH GRANT OPTION];

- GRANT CREATE SESSION, CREATE TABLE TO user1;
- GRANT CREATE  SESSION TO james WITH ADMIN OPTION;




REVOKE privilege_name
ON object_name
FROM {user_name |PUBLIC |role_name}

- REVOKE CREATE TABLE FROM user1;
- REVOKE CREATE SESSION FROM james

# Object Privileges

- Each object privilege that is granted authorises *the grantee* to perform *some operation* on the object.

- Object privilege examples.

  - Alter table.
  - Delete table, delete view.
  - Insert table, insert view.
  - References table.
  - Select table, select view.
  - Update table, update view.

# Granting and Revoking Object Privileges

- GRANT SELECT, INSERT, DELETE ON emp TO james, jane;
- GRANT ALL ON department TO james;
- REVOKE SELECT, INSERT ON emp TO james;
- REVOKE ALL ON department TO james;

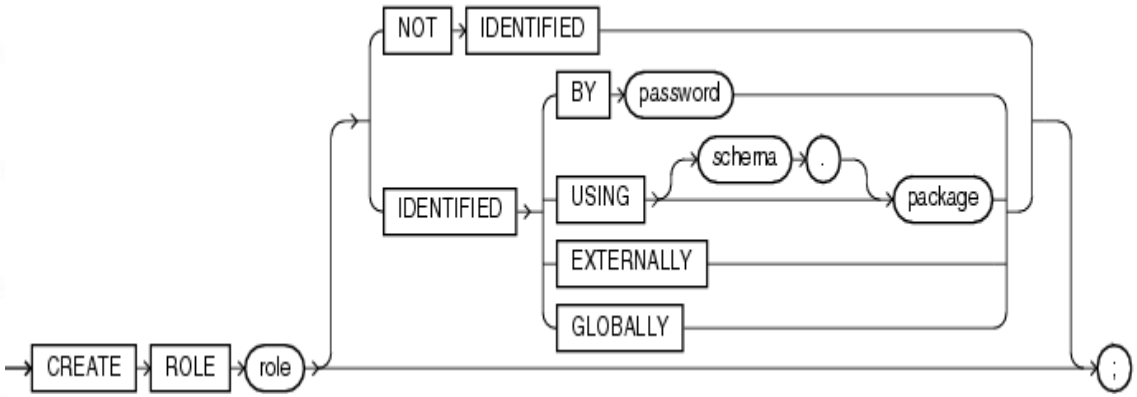
# Displaying System and Object Privileges

- Query the DBA_SYS_PRIVS
  - to list system privileges granted to users and roles.
- Query DBA_TAB_PRIVS
  - to list all object privileges granted to the specified user.
- Query DBA_COL_PRIVS
  - to list all the column specific privileges that have been granted to the user.

# Roles

- A role is a named group of related privileges that are granted to users or other roles.
- Roles are granted and revoked from users in the same way privileges are.
- Benefits of roles.
  - Reduced granting of privileges.
  - Dynamic privilege management.

# Creating and Assigning Roles



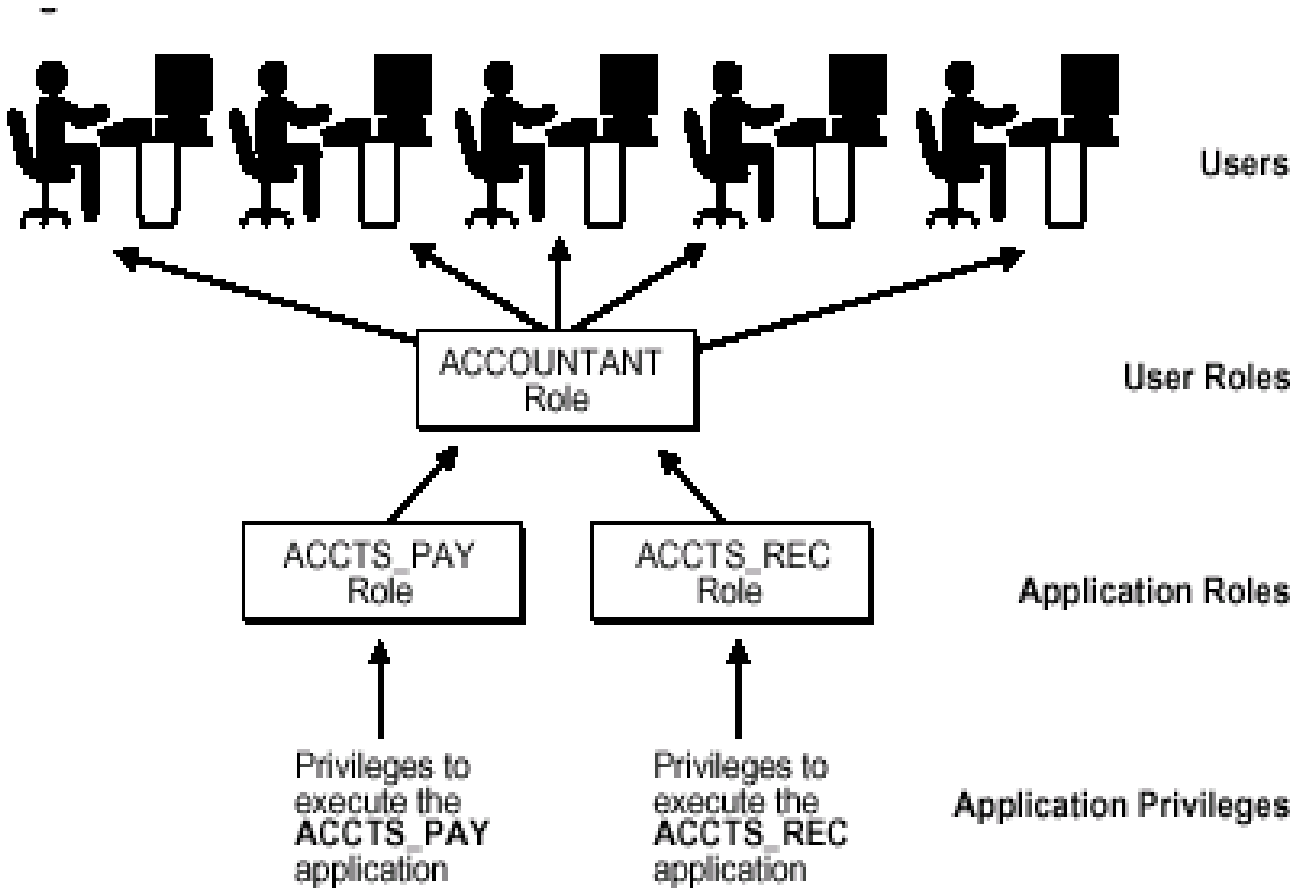

CREATE ROLE role_name
[IDENTIFIED BY password];

- CREATE ROLE mgmt_role;
- GRANT SELECT, INSERT, DELETE ON emp TO mgmt_role;
- GRANT mgmt_role TO jack;

# Predefined Roles

| Role Name | Privileges Granted to Role |
|---|---|
| CONNECT | ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, **CREATE SESSION**, CREATE SYNONYM, CREATE TABLE, CREATE VIEW |
| RESOURCE | CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, CREATE TYPE |
| DBA | ALL system privileges WITH ADMIN OPTION |

# Using Roles For End-user Privilege Management



# References


- Hoffer J.A., Prescott M.B., & McFadden "*Modern Database Management", 8th Ed. (not so useful)*
- *Oracle 11g Security Guide*- Chapters 3, 5, 7, 11
- *Oracle 11g Administrators Guide*- Chapter 22
- Ramakrishnan R. & Gehrke J. "*Database Management Systems*", Ch 21. (better)
- Elmasri, Navathe; *Fundamentals of Database Systems; 4th Ed.* Ch 23.