Administración de Bases de Datos

Tema 5
(parte 2 de 3)

Seguridad en las Bases de Datos

Privilegios de objeto

- Un **privilegio de objeto** es un derecho para realizar una acción particular sobre un objeto específico (tabla, vista, secuencia, procedimiento, disparador, etc.) que no se encuentre en el propio esquema del usuario
- El tipo de privilegio depende del tipo de objeto
- Normalmente se asignan a roles definidos para grupos de usuarios, aunque pueden ser otorgados a usuarios directamente
- De la misma manera que los privilegios de sistema, la concesión y revocación privilegios de objeto se realiza mediante las sentencias **GRANT** y **REVOKE** de SQL

- Un usuario posee todos los privilegios de objeto para los objetos contenidos en su esquema
- El propietario de un objeto puede otorgar cualquier privilegio sobre dicho objeto a otro usuario o a un rol

Todos los privilegios de objeto en: http://docs.oracle.com/cd/E11882_01/timesten.112/e21642/privileges.htm#TTSQL341

Privilegios para objetos TABLA

- Proporcionan seguridad a dos niveles: **LMD** y **LDD**

  - LMD: INSERT, UPDATE, DELETE y SELECT
    - Los privilegios de **INSERT** y **UPDATE** pueden otorgarse selectivamente sobre determinadas columnas de la tabla
    - Con un privilegio INSERT selectivo, sólo se pueden insertar tuplas con valores en las columnas especificadas. El resto de las columnas recibe el valor NULL
    - Con un privilegio UPDATE selectivo, sólo se pueden modificar valores de una columna específica

  - LDD: ALTER, INDEX y REFERENCES
    - Permiten modificar la estructura de una tabla, crear índices sobre una tabla y hacer referencias a una tabla, respectivamente

Privilegios para objetos VISTA

- Permiten la realización de varias operaciones de LMD

- Los privilegios de objeto sobre tablas que permiten operaciones LMD pueden aplicarse, de modo similar, sobre las **vistas**

- Para crear una vista es preciso poseer los siguientes privilegios:
  - el usuario que desee crear una vista debe poseer el privilegio **CREATE VIEW** (para crearla sobre su propio esquema) o **CREATE ANY VIEW** (para crearla sobre cualquier esquema)
  - el usuario debe haber recibido explícitamente los privilegios de **SELECT**, **INSERT**, **UPDATE** y/o **DELETE** sobre todos los objetos que soportan la vista o bien poseer los privilegios **SELECT ANY TABLE**, **INSERT ANY TABLE**, **UPDATE ANY TABLE** y/o **DELETE ANY TABLE**

Privilegios para objetos PROCEDIMIENTO o FUNCIÓN

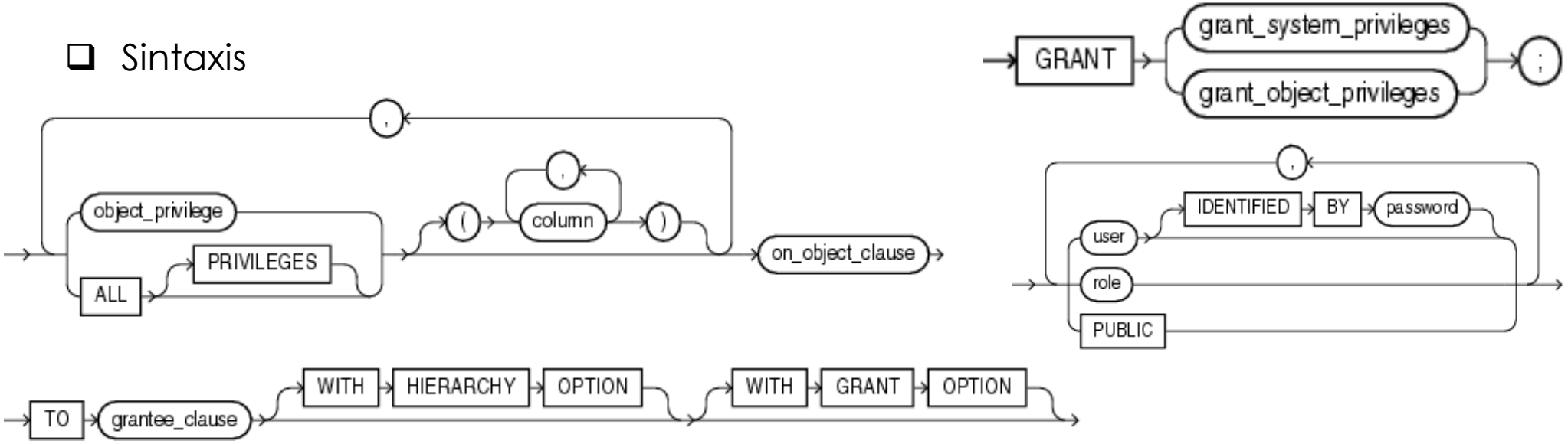
- El único privilegio necesario para ejecutar los procedimientos propios es **EXECUTE**
- Para ejecutar cualquier procedimiento se debe tener el privilegio **EXECUTE ANY PROCEDURE**
- Adicionalmente, el usuario propietario de un procedimiento debe poseer privilegios sobre los objetos que manipula el procedimiento
- Cuando se ejecuta un procedimiento, éste trabaja bajo el dominio de seguridad de su usuario propietario
- Antes de ejecutar un procedimiento, Oracle examina los privilegios del propietario del mismo. Si un privilegio necesario sobre un objeto referenciado en el procedimiento es revocado a su propietario, dicho procedimiento no puede ser ejecutado

Asignación de privilegios de objeto

- También se utiliza la sentencia **GRANT**
- Para otorgar un privilegio es necesario:
  - Ser propietario del objeto
  - Haber recibido el privilegio con la cláusula **WITH GRANT OPTION**
  - Tener el privilegio de sistema **ANY OBJECT PRIVILEGE**

Privilegios de objeto	Tablas	Vistas	Secuencias	Procedimientos Funciones Paquetes
ALTER	☑		☑	
DELETE	☑	☑		
EXECUTE				☑
INDEX	☑			
INSERT	☑	☑		
REFERENCES	☑			
SELECT	☑	☑	☑	
UPDATE	☑	☑		

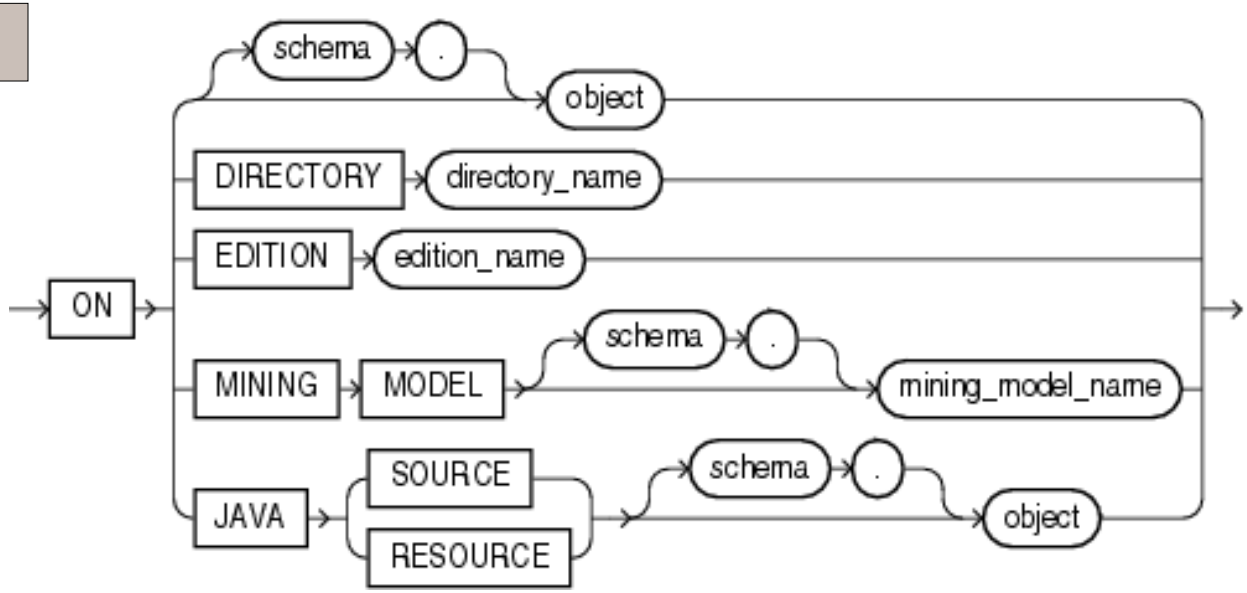
- Sintaxis



- **object_privilege** es el privilegio a ser otorgado
- **ALL PRIVILEGES** concede todos los privilegios que se tengan con la opción **WITH GRANT OPTION**
- El privilegio puede asignarse a un usuario o a todos los usuarios (**PUBLIC**)
- **column** especifica el nombre de una columna cuando se desea conceder permisos específicos a esas columnas (para INSERT, REFERENCES y UPDATE). Si no se especifica, los permisos se conceden para todas las columnas
- **WITH GRANT OPTION** tiene el mismo significado que en la asignación de privilegios de sistema
- **WITH HIERARCHY OPTION** concede el privilegio especificado a todos los subconjuntos del objeto (por ejemplo tablas derivadas de otras)

- Sintaxis

on_object_clause



- **on_object_clause** especifica el objeto sobre el cual se conceden los privilegios
- si *object* no se antecede con *schema*, Oracle supone que el objeto se ubica en el esquema del usuario

- Ejemplos de asignación de privilegios de objeto:

```
GRANT SELECT ON esq1.ventas TO usu_002;
```

Otorga el privilegio de consulta sobre la tabla **VENTAS** del esquema ***esq1*** al usuario ***usu_002***

```
GRANT REFERENCES (dni_empl),
      UPDATE (nombre_empl, sueldo)
   ON empleados
   TO usu_004;
```

Otorga varios privilegios sobre columnas específicas de la tabla **EMPLEADOS** al usuario ***usu_004***

```
GRANT ALL PRIVILEGES ON notas
TO usu_006
   WITH GRANT OPTION;
```

Se le conceden todos los privilegios sobre la tabla **NOTAS** al usuario ***usu_006***. Además, dicho usuario podrá conceder y revocar todos los privilegios a otros usuarios o roles

5.6. Roles

- Un rol es un grupo de privilegios con un nombre
- Puede ser otorgado a usuarios particulares de la base de datos o a otros roles
- Ventajas del uso de roles:
  - **Administración de privilegios reducida**. En lugar de otorgar explícitamente el mismo conjunto de privilegios a un grupo de usuarios, los privilegios para un grupo relacionado de usuarios pueden ser otorgados a un rol y, posteriormente, sólo se necesita asignar el rol a cada miembro del grupo de usuarios
  - **Gestión dinámica de privilegios**. Si los privilegios de un grupo deben cambiar, sólo es preciso cambiar el rol
  - **Disponibilidad selectiva de privilegios**. Los roles otorgados a un usuario pueden ser activados y desactivados selectivamente. Esto permite un control específico de los privilegios de un usuario en cualquier situación
  - **Seguridad específica de la aplicación**. El uso de un rol puede protegerse mediante una contraseña. Es preciso construir aplicaciones para activar específicamente un rol proporcionando una contraseña. Los usuarios no pueden activar el rol sin conocer la contraseña

Uso de ROLES

- La funcionalidad de los roles de la base de datos incluye los siguientes aspectos:

  - Un rol puede incluir privilegios de sistema y privilegios de objeto
  - Un rol puede ser otorgado a otros roles. Sin embargo, un rol no puede ser otorgado a sí mismo ni circularmente
  - Cualquier rol puede ser otorgado a cualquier usuario de la base de datos
  - Un rol otorgado a un usuario puede estar activado o desactivado. El dominio de seguridad de un usuario incluye los privilegios de todos los roles actualmente activos para ese usuario. Este dominio no incluye los privilegios de roles que no están actualmente activos para el usuario

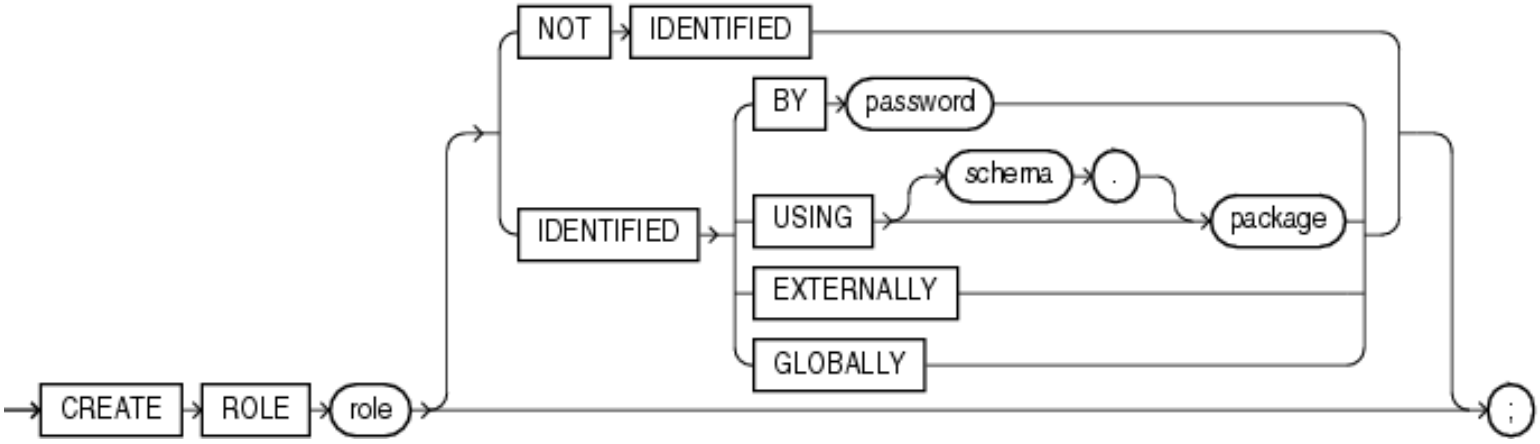
ROLES predefinidos

- Oracle proporciona roles predefinidos para ayudar a la administración de base de datos. Algunos de los más utilizados son:
  - **CONNECT**. Incluye sólo el privilegio CREATE SESSION
  - **RESOURCE**. Incluye los privilegios CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER y CREATE TYPE
  - **DBA**. Incluye todos los privilegios de sistema WITH ADMIN OPTION
  - **EXP_FULL_DATABASE**. Privilegios para exportaciones completas e incrementales de la base de datos
  - **IMP_FULL_DATABASE**. Privilegios para importaciones completas
  - **SELECT_CATALOG_ROLE**. Privilegio de consulta sobre las 1638 tablas del diccionario de datos
  - **DELETE_CATALOG_ROLE**. Privilegio de borrado en la tabla de auditoría de sistema (AUD$)

- Los roles CONNECT, RESOURCE y DBA se mantienen por compatibilidad con versiones anteriores de Oracle. No se asegura que sigan existiendo en un futuro.
- Se recomienda crear roles específicos en cada BD y asignarles los permisos necesarios, evitando el uso de roles predefinidos, con lo que no surgirán problemas si estos quedan obsoletos en futuras versiones

Gestión de ROLES

- Para crear un rol es necesario poseer el privilegio **CREATE ROLE**
- La sentencia SQL para crear un rol es **CREATE ROLE**:



- El nombre debe ser diferente a cualquier nombre de rol o usuario existente
- Inicialmente, cuando se crea un rol, éste no tiene privilegios asociados a él. Para asociar privilegios a un nuevo rol es necesario otorgárselos directamente, o bien otorgarle otros roles

http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_6012.htm#SQLRF01311

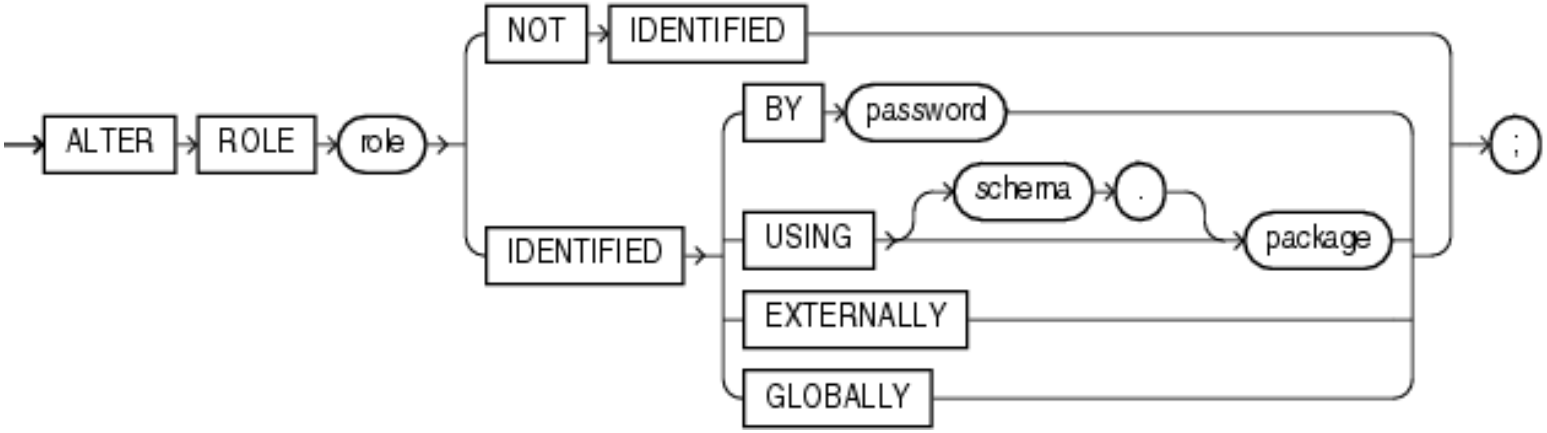
- La cláusula **NOT IDENTIFIED** indica que este rol está autorizado por la base de datos y que no se requiere contraseña para activarlo (por defecto)
- La cláusula **IDENTIFIED** indica que un usuario debe ser autorizado mediante el método especificado antes de activar el rol con la instrucción **SET ROLE** (más adelante se verá el significado de activación de roles)
- Ejemplos de creación de roles:

```
CREATE ROLE rol_general;
```

```
CREATE ROLE rol_general
   IDENTIFIED BY clave_rol_general;
```

Los usuarios a los que se le otorguen este rol deberán proporcionar la clave cada vez que quieran activar el rol por medio de la sentencia SET ROLE

- Se puede modificar el método de autenticación de un rol mediante la sentencia **ALTER ROLE**:



- Se debe tener el privilegio de sistema **ALTER ANY ROLE** o haber sido otorgado el rol con la opción **WITH ADMIN OPTION**

http://download.oracle.com/docs/cd/B19306_01/server.102/b14200/statements_2009.htm#sthref4413

- También se pueden eliminar roles. Cuando se borra un rol se revocan, automáticamente, los privilegios relacionados con ese rol a todos los usuarios o roles a quienes se hubiese otorgado el rol a borrar
- Debe poseerse el privilegio **DROP ANY ROLE** o haber sido concedido el rol con **WITH ADMIN OPTION**

http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_8029.htm#SQLRF01530

Concesión de privilegios a un ROL

- Para añadir privilegios a un rol se utiliza la sentencia GRANT de la misma forma que se asigna privilegios a los usuarios
- Ejemplos:

```
GRANT select on usuario1.ventas TO rol_general;

GRANT create trigger TO rol_general;
```

Asignación y revocación de ROLES

- Una vez asignados al rol los privilegios de sistema o privilegios sobre objetos deseados, se puede asignar el rol a un usuario o a otro rol utilizando una sintaxis similar

```
GRANT rol TO usuario | rol | PUBLIC;

GRANT rol TO usuario | rol | PUBLIC [WITH ADMIN OPTION];
```

- Ejemplos:

```
GRANT rol_general TO martinez;

GRANT rol_general TO otro_rol;
```

- Para asignar un rol, es necesario haber recibido el rol en cuestión con la cláusula **WITH ADMIN OPTION** o tener el privilegio de sistema **GRANT ANY ROLE**
- El rol asignado no se activa inmediatamente si el usuario ya está conectado

- Para revocar un rol de un usuario se utiliza un procedimiento similar al que se emplea para revocar privilegios
- Ejemplo:

```
REVOKE rol_general TO martinez;
```

ROLES predeterminados

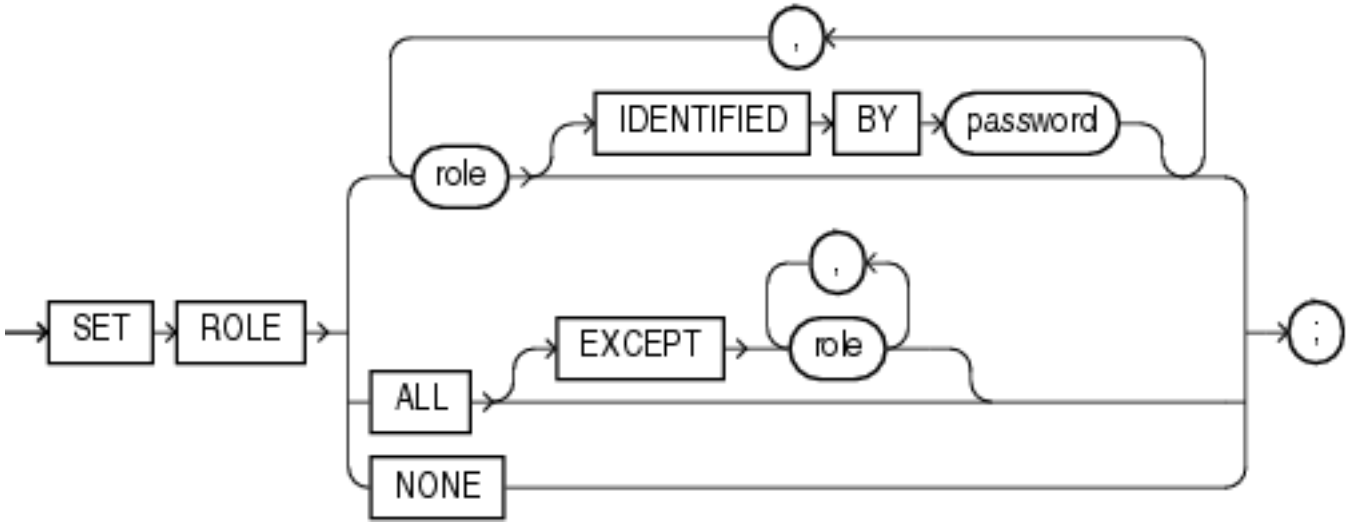
- Un **rol predeterminado** es aquel que automáticamente se activa al conectarse
- Si un rol sólo va a ser utilizado dentro del contexto de una aplicación, se puede comenzar con el rol desactivado en el momento en que el usuario inicie la sesión y luego activarlo y desactivarlo dentro de la aplicación
- Con la sentencia **ALTER USER** se limitan los roles predeterminados asignados a un usuario
- Sintaxis:

```
ALTER USER <usuario> DEFAULT ROLE <rol1>,…<roln>|

ALL [EXCEPT rol1 [,rol2]... ] |

NONE;
```

- Al crear un usuario, todos los roles asignados son predeterminados a menos que se limite con ALTER USER
- Durante una sesión, un usuario puede activar y desactivar roles mediante la sentencia **SET ROLE**
- Previamente los roles deben haber sido asignados al usuario



- En el momento de conectar con la base de datos, Oracle establece el dominio de seguridad del usuario activando los roles predeterminados
- El dominio de seguridad predeterminado del usuario contiene todos los privilegios otorgados explícitamente al usuario más todos aquellos privilegios incluidos en los roles predeterminados
- Cualquier operación autorizada por los privilegios incluidos en el dominio de seguridad puede ser ejecutada sin problemas

- Durante la sesión, el usuario o una aplicación puede usar **SET ROLE** para activar o desactivar los roles
- Ejemplos:

```
SET ROLE rol_general IDENTIFIED BY clave_rol;
```

→ Activa el ***rol_general*** (que se creó con clave) en la sesión actual

```
SET ROLE ALL EXCEPT rol_general;
```

→ Habilita todos los roles menos el ***rol_general***

Tablas y vistas relacionadas con privilegios y roles

ALL_OBJECTS	Objetos accesibles por el usuario
ALL_TABLES	Tablas accesibles por el usuario
ALL_TAB_COMMENT	Tablas y vistas accesibles por el usuario con un comentario
ALL_TAB_PRIVS_MADE	Concesiones del usuario y concesiones sobre los objetos del usuario
ALL_TAB_PRIVS_RECD	Concesiones sobre objetos para los cuales el usuario o PUBLIC es el receptor de la concesión
DBA_ROLE_PRIVS	Descripción de los roles otorgados a usuarios y roles
DBA_ROLES	Todos los roles que existen en la base de datos
DBA_SYS_PRIVS	Descripción de los privilegios de sistema otorgados a usuarios y roles
DBA_TAB_PRIVS	Todas las concesiones sobre objetos de la base de datos
ROLE_ROLE_PRIVS	Información sobre los roles otorgados a otros roles
ROLE_SYS_PRIVS	Información sobre privilegios de sistema otorgados a otros roles
ROLE_TAB_PRIVS	Información sobre privilegios de objeto otorgados a otros roles

Tablas y vistas relacionadas con privilegios y roles

SESSION_PRIVS	Privilegios que están actualmente disponibles al usuario conectado
SESSION_ROLES	Roles que el usuario tiene actualmente activados
TABLE_PRIVILEGES	Concesión de privilegios sobre objetos para los cuales el usuario es el que ha concedido, el destinatario, el propietario o el destinatario es PUBLIC
USER_CATALOG	Objetos propiedad del usuario
USER_ROLE_PRIVS	Roles que han sido otorgados al usuario
USER_SYS_PRIVS	Privilegios del sistema que han sido otorgados al usuario
USER_TAB_PRIVS	Concesión de privilegios sobre objetos para los cuales el usuario es el que ha concedido, el destinatario o el propietario
USER_TAB_PRIVS_MADE	Todas las concesiones sobre objetos que son propiedad del usuario
USER_TAB_PRIVS_RECD	Concesiones sobre objetos para los cuales el usuario es el que recibe la concesión