Roles y perfiles

[5.6.8] creación de roles

Los roles se crean usando esta sintaxis

```
CREATE ROLE rol  [NOT IDENTIFIED |
        IDENTIFIED {BY password  | EXTERNALLY | GLOBALLY | USING package}];
```

La opción IDENTIFIED hace que el rol sólo pueda utilizarse si el usuario se identifica con el método que indiquemos en esta instrucción. Las formas de identificarse son las mismas formas que se utilizan al identificar un usuario (vistas anteriormente), salvo que ahora disponemos de una nueva: la opción PACKAGE que hace que el rol sólo se pueda utilizar si usamos el paquete de aplicaciones indicado.

Por defecto un rol no requiere identificación.

[5.6.9] modificación de roles

Disponemos de la instrucción ALTER ROLE permite modificar la configuración del rol. Tiene las mismas opciones que CREATE ROLE y sólo se usa si deseamos establecer un nuevo método para autentificarnos.

[5.6.10] asignar y retirar privilegios a roles

Se realiza con la instrucción GRANT y se usa igual que cuando establecemos permisos a los usuarios, en la sintaxis de los comandos GRANT y REVOKE vistas anteriormente, simplemente se indicaría un nombre de rol en lugar de un nombre de usuario. Por ejemplo si deseamos asignar los privilegios **CREATE TABLE** y **CONNECT** a un rol llamado **rol1**. Se haría:

```
GRANT CREATE TABLE, CONNECT TO rol1;
```

De la misma forma, podemos quitar privilegios asignados a un rol mediante el comandol REVOKE:

```
REVOKE CREATE TABLE FROM rol1;
```

[5.6.11] asignar roles a usuarios

La sintaxis completa para asignar roles a un usuario es:

```
GRANT rol1 [,rol2 [,…]]
TO  {usuario|rol|PUBLIC [,{usuario|rol|PUBLIC} [,…] }
[WITH ADMIN OPTION]
```

Al igual que en las instrucciones anteriores, PUBLIC asigna el rol a todos los usuarios y WITH ADMIN OPTION permite al usuario al que se le concede el rol, conceder él dicho rol a otros usuarios/as.

[5.6.12] roles por defecto

Los usuarios tienen una serie de roles por defecto, estos son aquellos roles que van unidos al usuario, de modo que en cuanto un usuario lanza una sesión, los privilegios que contienen sus roles por defecto, comienzan a funcionar.

Cuando asignamos un rol mediante el comando GRANT, este pasa a ser un rol por defecto.

[5.6.13] roles predefinidos

Oracle dispone de una serie de roles predefinidos que se pueden asignar a los usuarios. Hay más de cincuenta roles predefinidos. Los clásicos son:

rol	significado
CONNECT	Permite crear sesiones. Se mantiene por compatibilidad
RESOURCE	Permite crear tablas y código PL/SQL del tipo que sea. Se mantiene por compatibilidad
DBA	Permite casi todo, excepto manejar la instancia de la base de datos

[5.6.15] asignar a un usuario un rol por defecto

Cuando se crea un usuario mediante CREATE USER, no disponemos de la posibilidad de asignar un rol por defecto. De hecho se le asigna automáticamente la opción ALL que hace que todos los roles que se le asignen en el futuro (mediante GRANT) pasarán a ser roles por defecto.

Por ello la instrucción que administra los roles por defecto es ALTER USER:

```
ALTER USER usuario
DEFAULT ROLE {rol1 [,rol2 [,…]| ALL [EXCEPT rol1 [,rol2[,…]] |NONE ]};
```

La opción ALL coloca a todos los roles como roles por defecto, EXCEPT especifica una lista de roles que no serán colocados como roles por defecto. NONE hace que no haya ningún rol por defecto. Finalmente podemos simplemente especificar la lista de roles que quedarán como roles por defecto.

[5.6.16] borrar roles

Lo hace la instrucción DROP ROLE, seguida del rol a borrar. Desde ese momento a los usuarios a los que se habían asignado el rol se les revoca.

[5.6.17] información sobre roles en el diccionario de datos

Existen varias vistas para examinar los roles.

Vista	Significado
DBA_ROLES	Muestra todos los roles de la base de datos
DBA_ROLES_PRIVS	Roles asignados a los usuarios
ROLE_ROLE_PRIVS	Roles asignados a otros roles
DBA_SYS_PRIVS	Privilegios de sistema asignados a usuarios y roles
ROLE_SYS_PRIVS	Privilegios de sistema asignados a roles
ROLE_TAB_PRIVS	Privilegios de objeto concedidos a roles
SESSION_ROLES	Roles en activo para el usuario actual

[5.7] administración de perfiles de Oracle

Los perfiles permiten limitar los recursos que los usuarios usan de la base de datos. Hay un perfil llamado DEFAULT que se aplica automáticamente a todos los usuarios y que les da recursos ilimitados sobre la base de datos. Para limitar el número de recursos se debe de activar (poniéndola el valor TRUE) la variable de sistema RESOURCE_LIMIT (que por defecto está a FALSE). Esto se hace así:

```
ALTER SYSTEM SET RESOURCE_LIMIT=TRUE;
```

En realidad hay dos tipos de parámetros de los perfiles:

- Perfiles de manejo de contraseñas, que gestionan el funcionamiento de las contraseñas para el usuario.

Variable de perfil	Significado
FAILED_LOGIN_ATTEMPTS	Número consecutivo de errores en las contraseñas antes de bloquear la cuenta. Por defecto son 10
PASSWORD_LOCK_TIME	Número de días hasta que se bloquea una cuenta si se supera el límite de intentos al meter una contraseña. Por defecto es uno
PASSWORD_LIFE_TIME	Números de días que tiene vigencia una contraseña. Por defecto es 180
PASSWORD_GRACE_TIME	Días que la contraseña se la concede un periodo extra de gracia tras consumir su tiempo de vida. Por defecto es 7
PASSWORD_REUSE_TIME	Número de días que una contraseña puede ser reutilizada
PASSWORD_VERIFY_FUNCTION	Función a la que se invoca cuando se modifica una contraseña con el fin de verificar su validez en base a las reglas de complejidad que deseemos

Sintaxis:

```
CREATE PROFILE perfil LIMIT parámetro1 valor1 [parametro2 valor [...]]
```

Los parámetros a especificar son los que aparecen en la tabla anterior. A cada parámetro se le indica un valor, o bien la palabra DEFAULT si deseamos que tome su valor por defecto, o bien UNLIMITED para indicar que el parámetro tomará un valor de infinito.

Ejemplo:

```
CREATE PROFILE programador LIMIT
                SESSIONS_PER_USER UNLIMITED
                CPU_PER_SESSION UNLIMITED
                IDLE_TIME 15
                CONNECT_TIME 150
                FAILED_LOGIN_ATTEMPTS 5
                PASSWORD_LOCK_TIME 2;
```

[5.7.1] modificar perfiles

La instrucción ALTER PROFILE funciona igual que CREATE PROFILE y es la encargada de hacer modificaciones a un perfil creado.

[5.7.2] borrar perfil

En este caso es DROP PROFILE seguida del nombre del perfil a eliminar. Se puede usar la palabra CASCADE para eliminar todas las restricciones que impidan borrar el perfil. Sintaxis:

```
DROP PROFILE nombrePerfil [CASCADE]
```

[5.7.3] asignar un perfil a un usuario

Cada usuario tiene un solo perfil. La instrucción de creación de usuarios (CREATE USER) dispone de la cláusula PROFILE para indicar el perfil que se asigna a ese usuario.

Si lo que deseamos es asignar un perfil a un usuario después de haberle creado, disponemos de la instrucción ALTER USER con la que podemos indicar el perfil. Ejemplo:

```
ALTER USER jsanchez PROFILE programador;
```