Seguridad en el SGBD Oracle

Esther Gadeschi Díaz, Antonio García Domínguez y Juan Boubeta Puig

Seguridad y Competencias Profesionales
Curso 2011-2012
24 noviembre 2011

1. Inicio de Oracle y SQL*Plus

En esta práctica se supone que tenemos acceso a una máquina con Oracle 10g XE (eXpress Edition) instalado y con la posibilidad de abrir SQL*Plus con los usuarios SYS y SYSTEM o con derechos de administración a bajo nivel de la base de datos («*as sysdba*»).

También se asume que se tiene acceso a la documentación oficial de Oracle 10g, disponible desde `http://www.oracle.com/pls/db102/homepage`. Se harán referencias a sus libros y secciones cuando sea necesario. En general, se recomienda descargar los PDF de los libros «2 Day DBA» y «Database Administrator's Guide».

Esta primera sección se dedica a instalar Oracle (si es necesario) y lanzar SQL*Plus.

1.1. Ordenadores del aula

Los ordenadores del aula ya incluyen una instalación local del SGBD Oracle 10g en su edición Express. Para utilizarla, se deberá iniciar sesión en la cuenta **oracle** con la contraseña suministrada por el profesor.

Una vez iniciada la sesión, se puede entrar a una terminal SQL*Plus a través de la entrada correspondiente del menú KDE.

Si se desea acceder desde terminal, puede ejecutarse la siguiente orden:

```
> source /usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle_env.sh
```

A partir de entonces, se podrán utilizar las órdenes de la sección 1.3.

1.2. Instalación en Ubuntu 10.10

Para instalar el SGBD Oracle 10g XE bajo una distribución GNU/Linux Ubuntu 10.10 «Maverick», o cualquier otra distribución basada en Debian relativamente reciente, se pueden seguir los pasos que veremos a continuación.

Existen otras guías, como las de `http://www.oracle.com/technology/tech/linux/install/xe-on-kubuntu.html` y de `https://help.ubuntu.com/`

`community/Oracle10g`, que son más completas y pueden resultar en configuraciones más seguras, pero pueden ser más complejas de realizar.

Una vez se sigan estos pasos, se podrán utilizar las órdenes de la sección 1.3. Se recomienda usar la cuenta **oracle** para ejecutarlas, ya que los permisos por defecto de los ficheros que instala Oracle no están del todo bien, y añadir nuestro usuario al grupo **dba** puede que no sea suficiente.

1. Descargar el `.deb` desde la página oficial de Oracle.
2. Instalar las dependencias del `.deb` manualmente:

   ```
   > sudo aptitude install libaio1 bc
   ```

3. Instalar el `.deb` de Oracle 10g XE:

   ```
   > sudo dpkg -i (ruta al .deb)
   ```

4. Ejecutar el guión de configuración, posiblemente evitando que Oracle se arranque al inicio, para evitar la carga de rendimiento que supone:

   ```
   > sudo /etc/init.d/oracle-xe configure
   ```

5. Dar una contraseña al usuario **oracle**:

   ```
   > sudo passwd oracle
   ```

6. Iniciar sesión como el usuario **oracle**, y añadir la siguiente línea a nuestro `~/.profile` o `~/.bashrc`:

   ```
   source /usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin/oracle_
       env.sh
   export EDITOR=mieditordetextopreferido
   ```

7. Cerrar sesión y volver a iniciarla, para que los cambios en nuestros ficheros de configuración personales surtan efecto.

1.3. Entrada en SQL*Plus desde la línea de órdenes

Una vez se hayan seguido estos pasos, se puede entrar en una terminal SQL*Plus o bien desde la entrada del menú correspondiente, o mediante alguna de estas órdenes:

- En general, si queremos entrar con un determinado usuario con los permisos normales:

  ```
  > sqlplus miusuario@localhost
  ```

- Si hemos levantado Oracle desde este mismo usuario del sistema operativo:

```
> sqlplus miusuario
```

- Si queremos realizar acciones de administración, como iniciar o detener la instancia de la base de datos en memoria, ejecutaremos esta orden desde el mismo usuario del sistema operativo que inició la instancia en ejecución de Oracle (si está iniciada) o desde cualquier usuario del grupo **dba** (si no estaba iniciada):

```
> sqlplus / as sysdba
```

Para salir, use la orden QUIT de SQL*Plus.

2. Configuración y auditorías

1. Vaya al directorio $HOME del usuario **oracle** y localice los siguientes tipos de ficheros:
   - Ficheros de control y datos (`.dbf`).
   - Ficheros de recuperación (`.log`).
   - Ficheros de auditoría (`.trc`, entre otros).
   - Parámetros de configuración de la instancia (`init.ora`).
2. Estudie el fichero `init.ora` y sus órdenes. ¿Está la auditoría activada?
3. Inicie SQL*Plus, y compruebe qué parámetros están activos en su sesión, con:

   ```
   > show parameters
   ```

   ¿Qué valor tiene PLSQL_WARNINGS? ¿Sabría decir qué significa? Refiérase a la parte 1 de «Database Reference».
4. Utilice las vistas estáticas del diccionario de datos descritas en (parte 2 del anterior libro) para ver qué usuarios existen, qué privilegios tienen y cuáles son los *tablespace* que existen en la base de datos.
5. Examine las vistas dinámicas de rendimiento (descritas en la parte 3 del anterior libro) `v$filestat`, `v$database` y `v$parameter`. ¿Qué tipo de información contienen?
6. Cierre la instancia de la base de datos de forma normal. Para ello, tendrá que entrar con derechos de administrador y ejecutar la orden:

   ```
   shutdown immediate;
   ```

7. Vuelva a levantarla. Podríamos ejecutar simplemente «*startup*», pero vamos a hacerlo en dos pasos, ya que nos hará falta en un ejercicio posterior. Primero iniciaremos la instancia, pero no la abriremos al resto de los usuarios, y luego abriremos dicha instancia:

```
startup mount;
alter database open;
```

3. Gestión de usuarios y privilegios

Para esta parte, necesitará distinguir los conceptos de «usuario», «esquema», «rol» y «perfil»:

- Todo usuario en la base de datos posee una serie de objetos, que se guardan en su esquema.
- Un rol reúne una serie de privilegios, de forma que puedan asignarse y retirarse en bloque a una serie de usuarios. Los privilegios pueden ser sobre objetos de la base de datos, o sobre el sistema completo.
- Un perfil también reúne una serie de limitaciones a aplicar sobre distintos usuarios, pero tratan sobre restricciones de rendimiento (número de sesiones, CPU y memoria a dedicar, etc.) y de contraseñas (caducidad y número de intentos, entre otros).

Los pasos a seguir en esta parte de la práctica son:

1. Utilizando la orden **CREATE USER** (refiérase a «SQL Reference», capítulo 7) y otras órdenes que considere necesarias, cree un usuario que tenga las siguientes características:
   - Clave de acceso y cuota de espacio de 1 MiB en su «tablespace» por omisión (`users`). Mire las cláusulas de la orden **CREATE USER**.
   - Perfil con un número de intentos de contraseña y número de sesiones limitados. Use **CREATE PROFILE** para crearlo antes de asignárselo al usuario.
   - Tendrá el rol estándar **CONNECT** y otro rol (protegido por contraseña) que le permitirá consultar cualquier tabla de cualquier esquema y crear sinónimos públicos. Los roles son creados con **CREATE ROLE**, dados con **GRANT**, quitados con **REVOKE** y activados con **SET ROLE**.
2. Ahora cree otro usuario, protegido por contraseña, que tenga el rol **CONNECT** y el rol **DBA**, con la posibilidad de propagar su rol **DBA** (revise las cláusulas de la orden **GRANT**).

3. Pruebe a entrar como dicho usuario (use la orden **CONNECT** de SQL*Plus). ¿Puede acceder a las vistas estáticas del diccionario de datos que empiezan por DBA?

4. Otórguele el rol **DBA** a su primer usuario, y entre como él. ¿Pueden también acceder a las vistas anteriores desde este rol?

5. ¿Puede quitarle el rol **DBA** al usuario que se lo dió?

6. Entre como **SYSTEM** y quítele el rol **DBA** al primer usuario al que se lo dió.

7. ¿Sigue pudiendo acceder a las vistas para administradores desde alguno de los dos usuarios anteriores?

4. Copias de seguridad

Para realizar esta parte, se recomienda haber creado una tabla en alguno de los usuarios creados en el apartado anterior y haberle añadido algunos datos. Por ejemplo:

```
1  CREATE TABLE prueba (
2    id INTEGER PRIMARY KEY,
3    nombre VARCHAR(30) NOT NULL
4  );
5
6  INSERT INTO prueba VALUES (1, 'A');
7  INSERT INTO prueba VALUES (2, 'B');
8  INSERT INTO prueba VALUES (3, 'C');
9  INSERT INTO prueba VALUES (4, 'D');
```

Para cada uno de estos apartados, deberá preparar esta tabla (o cualquier otra) con sus valores, hacer una copia de seguridad de ella como mínimo con las herramientas que se indiquen, borrar la tabla (use **DROP TABLE**) y recuperarla a través de la base de datos.

4.1. Copias lógicas: import y export

Las copias de seguridad creadas mediante las herramientas *import* y *export* son de tipo lógico, consistiendo básicamente en una serie de órdenes SQL que reproducen el estado actual de la parte de la base de datos que hayamos indicado. Suelen ser útiles cuando queremos cambiar de SGBD o cambiar de versión.

Las herramientas son muy sencillas de utilizar, aunque no disponen de toda la funcionalidad (y complejidad) de *rman*. Pruebe a exportar el esquema de su usuario con:

```
> exp miusuario@localhost
```

Para importar, sitúese bajo el mismo directorio donde esté `expdata.dmp` y ejecute:

```
> imp miusuario@localhost
```

4.2. Copias físicas: RMAN

rman es una herramienta más avanzada que *import* y *export*, y opera a nivel físico. Permite, entre otras cosas, gestionar de forma automatizada las copias de seguridad realizadas a un área especial (conocida como «flash recovery area»), y llevarlas finalmente a cinta.

Puede hacer copias de seguridad no sólo de los datos de la base de datos, sino de otros recursos como los ficheros de control o de parámetros de la instancia o los registros de recuperación (*redo logs*). Además, permite mantener copias de seguridad incrementales, tanto progresivas como diferenciales.

En este apartado sólo veremos una parte muy limitada de sus funcionalidades; para más detalles, refiérase a los libros «Backup and Recovery».

Siga estos pasos e indique qué resultados va obteniendo:

1. Necesitamos configurar la base de datos para que archive los registros de recuperación antiguos, en vez de sobreescribirlos, o no podremos usar *rman*.

   Con SQL*Plus abierto para tener derechos de administrador, eche abajo la instancia de la base de datos e iníciela montada, pero no abierta. Ejecute la siguiente orden:

   ```
   ALTER DATABASE ARCHIVELOG;
   ```

   Compruebe que ha cambiado debidamente la configuración de la BD con:

   ```
   SELECT dbid, log_mode FROM v$database;
   ```

   Abra la instancia con:

   ```
   ALTER DATABASE OPEN;
   ```

2. Ya podemos ejecutar *rman*. Ejecute:

   ```
   > rman target /
   ```

   Compruebe que se conecta con éxito.

3. Active la copia de seguridad automática no sólo de los datos, sino también de los ficheros de configuración, con:

   ```
   CONFIGURE CONTROLFILE AUTOBACKUP ON;
   ```

4. Ahora, haga una copia de seguridad completa a la *flash recovery area* con:

   ```
   BACKUP DATABASE;
   ```

5. Salga con QUIT y compruebe que se han creado los ficheros en el directorio `~/app/oracle/flash_recovery_area`.

Ahora puede borrarse la tabla y recuperarla. Para ello, entre otra vez en *rman* y siga estos pasos:

1. Eche abajo la base de datos e iníciela montada pero no abierta, tal y como haría en SQL*Plus.

2. Recupere los datos a partir de la copia de seguridad con:

```
RESTORE DATABASE;
RECOVER DATABASE;
```

3. Abra la base de datos con:

```
ALTER DATABASE OPEN;
```

Salga, entre como su usuario en SQL*Plus y compruebe que ha recuperado la tabla.