

Integridad de los datos: transacciones, backup y recuperación (II)

Administración de Bases de Datos

Curso 2018-2019

Jesús Correas, Mercedes G. Merayo, Yolanda García

**Departamento de Sistemas Informáticos y Computación
Universidad Complutense de Madrid**



Copia de seguridad y recuperación

Para planificar la copia de seguridad (backup) de un sistema hay que tener claras algunas cuestiones:

- **¿Qué se debe copiar? ¿Con qué objetivo?** Para recuperar la BD en su estado actual, o en cualquier instante pasado.
- **¿Qué estrategia de backup utilizar?** Cada caso es distinto. Puede haber *service level agreements* (**SLA**).
- **¿Cómo se debe copiar? ¿Dónde?** Con qué herramientas (y de qué modo: total, parcial, incremental).
- **¿Qué disponibilidad debe tener la BD?** Si puede estar offline o es un sistema 24/7.

Copias de seguridad. Qué se debe copiar

- **Qué se debe copiar:**

- ▶ **Datafiles, controlfile**
- ▶ Ficheros de **redo log online**.
- ▶ Si la BD está en modo *archive*log, **archivo de ficheros de redo log** desde el último backup.
- ▶ Ficheros de configuración:
init.ora, spfile<SID>.ora, sqlnet.ora, tnsnames.ora

- **Qué se debe poder recuperar:**

- ▶ Si se quiere tener **cualquier versión de la base de datos** de cualquier momento del último año: backups completos / incrementales y archivos de *redo log* para recuperar la información de cualquier instante.
- ▶ Backup completo al cierre de cada mes/año/ejercicio para archivo histórico.
- ▶ Aunque se quiera solo el **estado actual**, es conveniente tener algunos backups anteriores.

Copias de seguridad. Estrategia de backup

La **estrategia** depende de las necesidades de la instalación:

- La **frecuencia** de los backups es inversamente proporcional al tiempo de recuperación (MTTR).
- Se puede utilizar un área en disco (*fast recovery area*) para recuperar la BD rápidamente sin recurrir a almacenamiento en cinta.
- Si los datos cambian poco, es conveniente hacer backups **incrementales**.
- Si hay muchos cambios en los datos y muy frecuentes, es mejor hacer backups **completos** (*full backups*).
- Cada aplicación puede requerir distinto tipo de backups: backups **parciales** (algunos tablespaces/datafiles) vs. **totales** (toda la BD).

Copias de seguridad. Cómo copiar. Disponibilidad

- **Cómo se debe copiar:**

- ▶ **user-managed** backups: Utilizando herramientas externas a la BD: `cp`, `dd`, etc.
- ▶ **server-managed** backups: Oracle proporciona RMAN, una herramienta para realizar copias de seguridad

- **Disponibilidad de la BD:**

- ▶ Si la BD puede estar offline en algunos periodos para realizar backups, se pueden hacer backups *en frío* (*closed* o *consistent*).
 - ▶ O bien es un sistema 24/7 y deben hacerse los backups con la base de datos abierta y los usuarios trabajando, se deben hacer backups *en caliente* (*open* o *inconsistent*).
- La base de datos debe estar en modo *archive*log para poder hacer backups en caliente o parciales.
 - Solo se pueden hacer backups incrementales con RMAN.

Fast Recovery Area

- (antes denominada “Flash recovery area”)
- Es un **área de disco** para recuperar el estado de la BD.
- Contiene una serie de ficheros relacionados con copias de seguridad.
- Puede contener:
 - ▶ Copias de controlfiles,
 - ▶ Ficheros de *redo log* online,
 - ▶ Archivo de ficheros de *redo log*,
 - ▶ Logs de *flashback*,
 - ▶ copias de datafiles, y
 - ▶ Backups realizados por RMAN (si se utiliza).
- Este área está gestionada por la instancia de Oracle, y se puede fijar una **cuota de disco**.
- Puede servir de caché de backups para recuperar la BD rápidamente.
- Si se utiliza RMAN, se pueden mantener en este área varios backups de acuerdo con una **política de retención** configurable.

Copia de seguridad *en frío*

- La copia en frío también se denomina **consistente** porque al estar la BD offline todos los cambios están en los datafiles.
- Antes hay que cerrar la BD con la opción `NORMAL`, `IMMEDIATE` o `TRANSACTIONAL`.
- En un backup en frío **se debe copiar lo siguiente:**
 - ▶ Un **controlfile** (`SELECT NAME FROM v$controlfile`)
También puede obtenerse del valor del parámetro `CONTROL_FILES`.
Basta con copiar un solo fichero.
 - ▶ Los **datafiles** (`SELECT NAME FROM v$datafile`)
 - ▶ El **fichero de parámetros** de inicialización (parámetro `SPFILE`), y en general todos los ficheros `.ora`.
- **No es necesario copiar los ficheros de redo log**, pues la BD se ha cerrado limpiamente.
- La BD puede estar en modo *archivelog* o *noarchivelog*.

Copia de seguridad *en caliente*

- También llamada **inconsistente**: los datafiles no tienen todos los cambios, pues la BD está abierta y ejecutando transacciones.
- La BD **debe estar en modo archive log**.
- En un backup en caliente se debe copiar lo siguiente:
 - ▶ El **controlfile**.
 - ▶ Los **datafiles**.
 - ▶ El **archivo de ficheros de redo log**.
- El controlfile se debe copiar de forma especial, pues está siendo modificado por la BD:

```
alter database backup controlfile to [trace as] 'fic';
```
- Antes de copiar los datafiles se debe poner la BD o tablespace en **modo BACKUP**. En este modo:
 - ▶ en el fichero de *redo log* se guardan bloques completos, en lugar de fragmentos de bloque.
 - ▶ El proceso LGWR es menos eficiente y el *redo log* es más grande.
- Después de copiar los datafiles, se debe archivar y copiar el *redo log*.

Backups parciales: tablespaces y datafiles individuales

- No se puede copiar por separado el tablespace `SYSTEM`.
- Se deben realizar los siguientes pasos:
 1. Poner tablespace offline (`ALTER TABLESPACE ... OFFLINE NORMAL`)
 2. Copiar los datafiles (con la herramienta que sea).
 3. Poner el tablespace online (`ALTER TABLESPACE ... ONLINE`)
 4. Archivar el fichero de *redo log* online para poder recuperar el tablespace a partir del archivo de *redo log* (`ALTER SYSTEM ARCHIVE LOG CURRENT`)
- También se puede copiar el controlfile y el archivo de ficheros *redo log* por separado
(`ALTER DATABASE BACKUP CONTROLFILE TO '/disk/cf.bak';`
`SELECT NAME FROM v$archived_log;`)
- Después se pueden verificar los datafiles copiados por si tuvieran errores con `DBVERIFY`.
- Se pueden hacer copias individuales **inconsistentes** poniendo el tablespace en modo `BACKUP`.

Recuperación de un *backup* después de un fallo de disco

- La recuperación es diferente en función del tipo de ficheros de disco que se pierdan:
 - ▶ **Datafiles de SYSTEM o con segmentos de undo activos:** La instancia se cierra automáticamente.
 - ★ Si el fallo es temporal, basta con volver a abrir la BD;
 - ★ Si es permanente, se deben restaurar los datafiles de un backup.
 - ▶ **Otros datafiles:** No es necesario apagar la BD, basta con poner los tablespaces afectados offline y restaurar los datafiles de un backup.
 - ▶ **Controlfile:** Si se pierde una copia, se debe restaurar con otra de las copias disponibles o modificar el parámetro `CONTROL_FILES` y abrir la BD. Si se pierden todas las copias, se debe restaurar de un backup y abrir la BD con la opción `RESETLOGS`.
 - ▶ **Algunos archivos de redo log** necesarios para recuperar la BD: Se deben restaurar de un backup.
 - ▶ **El fichero de parámetros:** Se debe restaurar de un backup.
- Existen procedimientos para recuperar la BD cuando no se dispone de backup del controlfile y se han perdido todas las copias, o del archivo de ficheros de *redo log*, pero puede perderse información de la BD.

Server-managed backups: RMAN

- Es posible hacer copias de seguridad utilizando herramientas externas a Oracle (*user-managed backups*).
- Sin embargo, Oracle recomienda utilizar **Recovery Manager** RMAN para hacer *server-managed backups*.
- RMAN permite hacer copias de seguridad más eficientemente que otros mecanismos de administración de backups:
 - ▶ **Backups incrementales**: solo copian los bloques modificados de los datafiles.
 - ▶ Restauración y recuperación a nivel de bloque (solo repara los bloques incorrectos del datafile).
 - ▶ Aplicación de backups incrementales a backups totales.
 - ▶ Detección de errores en datafiles antes de que se acceda a los bloques defectuosos.

Otras recomendaciones para realizar copias de seguridad

- Mantener un “redundancy set” online pero en un disco separado con:
 - ▶ El último backup de **datafiles**, **controlfile**.
 - ▶ Ficheros actuales de **redo log**.
 - ▶ Archivo de ficheros de *redo log* desde el último backup.
- En grandes instalaciones se utilizan cintas de gran capacidad. No es recomendable reutilizar las cintas.
- En instalaciones pequeñas se pueden utilizar otras herramientas más sencillas: Oracle Data Pump, tablespaces transportables.
- Para cargar datos de otros sistemas se puede utilizar SQL*Loader.

Posibles trabajos relacionados con integridad de los datos, backup y recuperación

- **Recovery Manager RMAN.**

- ▶ copias y recuperación básica, política de retención de backups.
- ▶ catálogo de copias de seguridad de múltiples BDs.
- ▶ **Data Recovery Advisor DRA.** Herramienta para diagnóstico de problemas de BDs.

- **Real Application Clusters RAC.**

- **Automatic Storage Management (ASM).** Ventajas e inconvenientes, cómo se trabaja con este tipo de almacenamiento, arquitectura, etc.