



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN**

**IMPLEMENTACIÓN DEL SISTEMA DE
PROTECCIÓN DE DATOS “ORACLE® SECURE
BACKUP” EN LA SIIM DEL IFE**

**DESARROLLO DE UN
CASO PRÁCTICO**

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN**

P R E S E N T A :

DANIEL GARCÍA GARCÍA



**ASESOR:
ING. CÉSAR FRANCISCO GERMÁN ROSAS**

MÉXICO, 2014.



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Todas las marcas y marcas registradas mostradas en este trabajo, así como todos los logotipos, son propiedad de sus respectivos fabricantes. Las marcas Oracle y “Oracle Secure Backup” son marcas o marcas registradas de Oracle Corporation y/o sus afiliados.

Agradecimientos

A mis padres,

Que son el pilar de mi vida y quienes siempre me han dado su incondicional apoyo, agradezco que continuamente me hayan alentado a salir adelante y el haberme dado la oportunidad de superarme.

Con cariño, admiración y respeto, les dedico este logro profesional producto de sus incontables sacrificios y esfuerzos.

Gracias por todo.

A mi asesor y revisores,

Quisiera expresar mi gratitud por su paciencia y comprensión, gracias a su vasto conocimiento y acertadas recomendaciones he podido concluir de forma satisfactoria este proyecto.

Índice general

INTRODUCCIÓN	1
CAPÍTULO I PROBLEMÁTICA	3
CAPÍTULO II ARQUITECTURA DEL MOTOR DE BD ORACLE	8
2.1 BASE DE DATOS E INSTANCIA	8
2.2 ESTRUCTURAS DE MEMORIA Y PROCESOS	9
2.2.1 System Global Area (SGA)	9
2.2.2 Procesos de Background	11
2.3 ARCHIVOS	14
2.4 MODO ARCHIVELOG VS. NOARCHIVELOG	17
CAPÍTULO III COPIAS DE SEGURIDAD FÍSICAS EN ORACLE	18
3.1 COPIAS DE SEGURIDAD GESTIONADAS POR EL USUARIO	19
3.1.1 Offline backup gestionado por el usuario	19
3.1.2 Online backup gestionado por el usuario	22
3.2 COPIAS DE SEGURIDAD GESTIONADAS POR EL SERVIDOR	24
3.2.1 Recovery Manager (RMAN)	25
3.2.2 Offline backup gestionado por el servidor	26
3.2.3 Online backup gestionado por el servidor	29
CAPÍTULO IV ARQUITECTURA DE “ORACLE SECURE BACKUP”	31
4.1 DOMINIO ADMINISTRATIVO	32
4.2 USUARIOS, CLASES Y PRIVILEGIOS	33
4.3 DISPOSITIVOS DE CINTA	35
4.3.1 Unidades de cinta	35
4.3.2 Librería de cintas	36
4.4 FAMILIA DE MEDIOS	38
4.5 SELECTOR DE ALMACENAMIENTO DE COPIAS DE SEGURIDAD	38
4.6 INTERFACES DE ORACLE SECURE BACKUP	39
CAPÍTULO V INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE	40
5.1 INSTALACIÓN DE ORACLE SECURE BACKUP	40
5.1.1 Copia del software de instalación de OSB	41
5.1.2 Instalación del servidor OSB	41
5.2 CONFIGURACIÓN DE ORACLE SECURE BACKUP	43
5.2.1 Configuración de usuario	44
5.2.2 Configuración de hosts	44
5.2.3 Configuración de librería de cintas	45

5.2.4 Configuración de familia de medios	48
5.2.5 Configuración del selector de almacenamiento	49
5.2.6 Inventario de cintas magnéticas.....	49
5.3 CONFIGURACIÓN DE RMAN	50
CAPÍTULO VI RESULTADOS (CASOS DE PRUEBA)	54
6.1 EJECUCIÓN DE UN BACKUP COMPLETO DE LA BD.....	54
6.2 VALIDACIÓN DE UN BACKUP DE LA BD	62
6.3 RESTAURACIÓN Y VALIDACIÓN DE UN DATAFILE.....	64
CONCLUSIONES	66
BIBLIOGRAFÍA	68
MESOGRAFÍA	70

Índice de figuras

Figura 1 Componentes BD SIIM IFE.....	5
Figura 2 Conexión de componentes.....	6
Figura 3 Librería IBM TS3100.....	6
Figura 4 Arquitectura de BD con OSB instalado.....	7
Figura 5 Instancia y Base de datos.....	9
Figura 6 Estructuras de memoria y procesos Oracle.....	10
Figura 7 Datafiles y tablespaces.....	14
Figura 8 Reutilización de Online redo log files.....	15
Figura 9 Ubicación de Datafiles, Control files, Onlie redo logs y Spfile.....	21
Figura 10 Dominio administrativo con un solo host.....	33
Figura 11 Usuarios, clases y privilegios.....	34
Figura 12 Componentes principales de una unidad de cinta.....	36
Figura 13 Librería de cintas.....	37
Figura 14 Interfaces de OSB.....	39
Figura 15 Parámetros SCSI requeridos por OSB.....	45

INTRODUCCIÓN

Hoy en día la mayoría de las empresas mantienen grandes cantidades de datos, gastan miles e incluso millones de pesos para mantener protegidos los sistemas informáticos y la información que los alimenta, contar con los mecanismos que permitan tener disponible dicha información, es de suma importancia. Pues en la mayoría de los casos, no mantener la continuidad del negocio puede repercutir en cuantiosas pérdidas económicas, inclusive, en organizaciones como compañías aéreas y sistemas de salud, la seguridad personal se puede poner en riesgo y por consiguiente derivar en la adquisición de problemas legales.

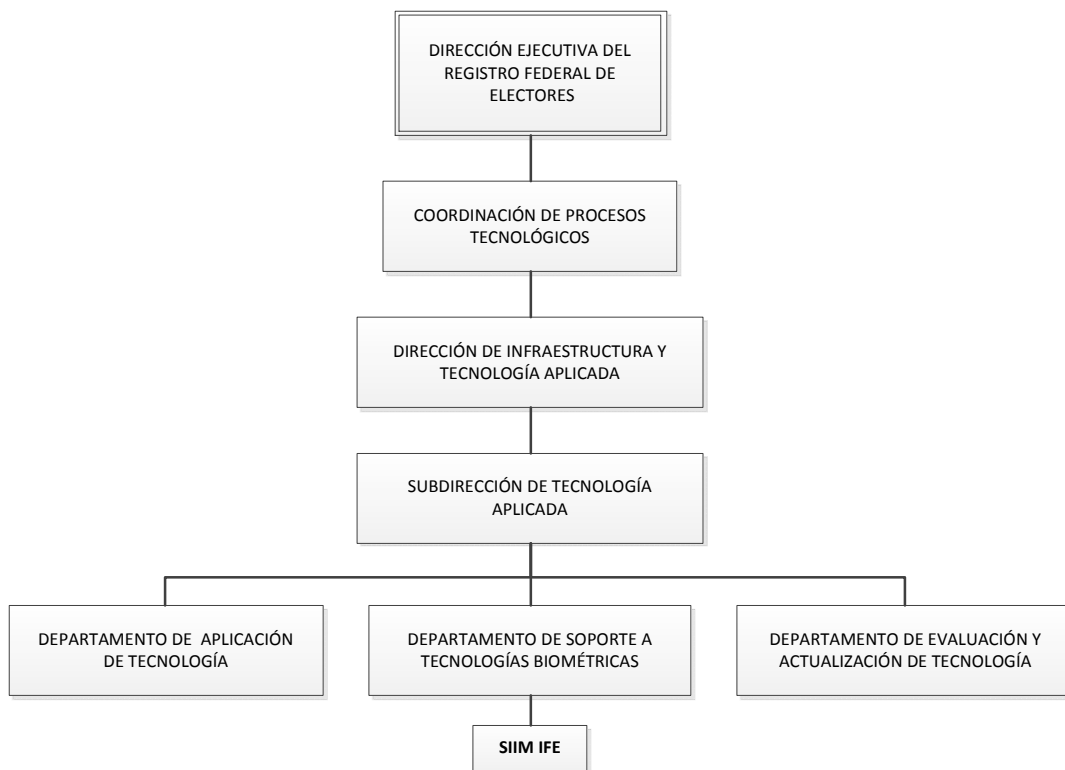
Ante la situación anterior, gran parte de las empresas u organizaciones buscan implementar una solución donde exista un equilibrio entre costo-beneficio y se garantice la disponibilidad de un sistema. Indudablemente, hay varias formas de resolver el problema: que van desde la implementación de entornos de alta disponibilidad, normalmente difíciles de costear puesto que involucra la réplica de hardware y software, hasta la implementación de soluciones más rentables, como los sistemas de respaldo, que permiten la recuperación de información ante cualquier posible incidente.

Un ejemplo de un sistema de respaldos rentable es “Oracle Secure Backup”, que básicamente es una herramienta de software utilizada para hacer respaldos y recuperaciones de BD Oracle en cintas magnéticas, así mismo, permite hacer el respaldo y recuperación del sistema de archivos de un sistema operativo.

En el presente trabajo, se mostrarán los elementos necesarios para realizar una correcta implementación del sistema de protección de datos “Oracle Secure Backup”, particularmente, se describirán las bases para poder desplegar el sistema y se espera que dichas bases puedan servir como referencia para implementaciones más complejas.

La decisión de mostrar la implementación de un sistema de protección de datos en el presente documento, resultó de la participación personal en la implantación de la solución “Oracle Secure Backup” en un sistema perteneciente al Instituto Federal Electoral (ahora INE), conocido como SIIM IFE «Solución Integral de Identificación Multibiométrica IFE». La SIIM IFE es un sistema automatizado encargado de realizar cotejos biométricos para determinar la autenticidad de una persona, el sistema emplea los rasgos físicos de las personas (huellas dactilares y rostro) para realizar las comparaciones biométricas.

El siguiente diagrama muestra la ubicación de la SIIM IFE dentro de la estructura organizacional del Instituto Federal Electoral.



En las siguientes páginas se expondrán los conceptos básicos y la terminología utilizada en la implementación del sistema de protección de datos “Oracle Secure Backup”. Lo importante de este proyecto, es que los conceptos aplicados para implantar el sistema de protección de datos dentro de la SIIM IFE no se limitan a dicho sistema, pues pueden ser aplicados en cualquier sistema gestor de base de datos Oracle ya que la dependencia con aplicaciones de terceros es nula.

Capítulo I

Problemática

La implementación del sistema de protección de datos “Oracle Secure Backup” dentro de la SIIM IFE se realizó principalmente para solucionar un problema de indisponibilidad presentado al momento de ejecutar las copias de seguridad de una BD Oracle. El problema consistía en que la BD quedaba inaccesible a los usuarios durante los fines de semana, por un periodo de aproximadamente 15 horas mientras se realizaba el respaldo de la misma, lo anterior, derivado de una mala elección del esquema de respaldos (Offline Backup).

Aunque existen otras alternativas para solucionar un problema de indisponibilidad de una BD Oracle, como lo es un sistema Oracle RAC (Real Application Clusters) o Oracle Data Guard, estas soluciones no siempre son las más viables y rentables. El hecho de optar por una implementación RAC o Data Guard implica contar con una duplicidad de hardware que soporte las mismas cargas de trabajo que el sistema principal, además, es necesario realizar la adquisición de licencias y contar con personal capacitado para desplegar este tipo de soluciones, en caso contrario, se tendría que hacer una inversión tanto en infraestructura tecnológica como en recursos humanos capacitados, e incluso, en soporte técnico por parte del fabricante.

Otra opción para mantener la disponibilidad de una BD es el uso de sistemas RAID (Redundant Array of Independent Disks), que son sistemas de almacenamiento de datos que usan múltiples unidades de almacenamiento (discos duros) entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios

dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto¹.

El problema de los sistemas RAID es que dependiendo del nivel de RAID implementado (RAID 1 o RAID 5 los más utilizados) se puede elevar o disminuir el costo de la solución lo que provoca que en ocasiones no sean tan rentables como parecen. También hay que tomar en cuenta que este tipo de soluciones solo puede proteger la BD ante las fallas de un medio (disco duro) ya que frente a los errores provocados por los usuarios (p. ej. el borrado de una tabla) poco pueden hacer este tipo de sistemas.

Haciendo un análisis de las alternativas anteriores, se optó por la implementación del sistema “Oracle Secure Backup” ya que es un sistema rentable y capaz de lograr un equilibrio entre costo-beneficio, prácticamente, “Oracle Secure Backup” no requiere de grandes cambios en la infraestructura de hardware, su licenciamiento viene dado por el número de unidades de lectura/escritura que se utilicen para hacer los respaldos, y en cuanto a los dispositivos de lectura/escritura muchas veces se puede reutilizar hardware ya existente. Oracle recomienda en sus mejores prácticas la utilización de un robot de cintas de última generación, pues el uso de un robot ayuda a mejorar el performance de las copias de seguridad y automatizar la ejecución de las mismas.

A continuación, se mostrarán los componentes y la arquitectura original de la BD de la SIIM IFE antes de implementar “Oracle Secure Backup” (OSB por sus siglas en ingles).

CANTIDAD	EQUIPO	IMAGEN
1	<p align="center">Unidad de cinta LTO4</p> <p>- Unidad de lectura/escritura de cintas magnéticas IBM Ultrium 4 (LTO4²) Tape Drive, 3Gbps SAS.</p>	

¹ <http://es.wikipedia.org/wiki/RAID>

² LTO (Linear Tape-Open) es una tecnología de cinta magnética de almacenamiento de datos.


1	<p>Sistema de almacenamiento IBM DS3524</p> <ul style="list-style-type: none"> - 2 módulos de control con fibra óptica y puerto SAS. - 2GB de Cache. - Licencia Turbo Performance. - 24x300GB 10K RPM SAS 2.5" HDD. 	
1	<p>Servidor IBM Power 720 Modelo 8202-E4C</p> <ul style="list-style-type: none"> - Sistema Operativo AIX 5.3 ML7. - Puerto Serial con conector tipo RJ45. - 2x300GB 10K RPM SFF SAS Disk Drive. - Adaptador de red 4-Port 10/100/1000 Base-TX. - Adaptador de fibra óptica 8 Gigabit PCI Express Dual Port. - Unidad SATA Slimline DVD-RAM. - Adaptador PCIe Dual-x4 SAS. - Controladora interna de discos duros 8 SFF Bays/175MB RAID/Dual IOA. - Memoria RAM 16GB (4x4GB). - Procesador POWER7 4-cores 3.0 GHz. - Oracle Database 10g Enterprise Edition Release 10.2.0.1.0. 	

Figura 1 Componentes BD SIIM IFE

La conexión de los componentes anteriores fundamentalmente consistía en una conexión directa de cada uno de los elementos con el servidor IBM Power 720, el sistema de almacenamiento IBM DS3524 se conectaba por medio de fibra óptica y la unidad de cinta magnética a través de una interfaz SAS (Interfaz de transferencia de datos en serie, sucesor del SCSI - Small Computer System Interface - paralelo) como se muestra en la Fig. 2.

El esquema de respaldos en esta arquitectura era muy sencillo, básicamente la BD Oracle permanecía apagada mientras se hacía uso de una utilidad del sistema operativo (comando `tar`) para hacer el respaldo de los archivos de BD en la unidad de cinta, el esquema era ineficiente puesto que la BD no podía ser explotada mientras se realizaban las operaciones de copia de seguridad. En el capítulo III se mostrará con mayor detalle este tipo de respaldos.

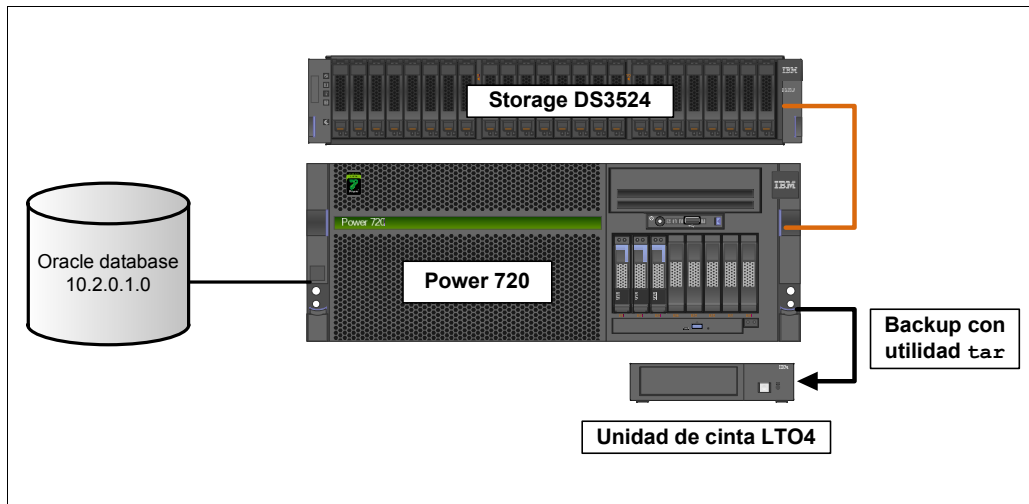


Figura 2 Conexión de componentes

Después de la implementación del sistema “Oracle Secure Backup” los cambios realizados en la infraestructura de hardware fueron mínimos, únicamente se reemplazó la unidad de cinta magnética por una librería/robot de cintas IBM TS3100 (Fig. 3) con conexión de fibra óptica. A nivel software, solo se realizó la instalación del sistema de protección de datos OSB en el servidor que alojaba el motor de BD Oracle (Power 720).

CANTIDAD	EQUIPO	IMAGEN
1	<p>Librería de cintas IBM LTO Ultrium 5, 4 y 3 TS3100</p> <ul style="list-style-type: none"> - Conexión de Fibra óptica (LTO 4 y 5). - Modo de acceso secuencial o aleatorio con lector de código de barras. - Formato 2U con 24 ranuras para cartuchos de datos. - Gestión remota de biblioteca (librería) a través de una interfaz web. - Velocidad de transferencia de datos nativa Ultrium 5 de 140 MBps, Ultrium 4 de 120 MBps, Ultrium 3 de 80 MBps. 	

Figura 3 Librería IBM TS3100

La arquitectura final una vez implementado el sistema de protección de datos OSB se puede observar en la siguiente figura:

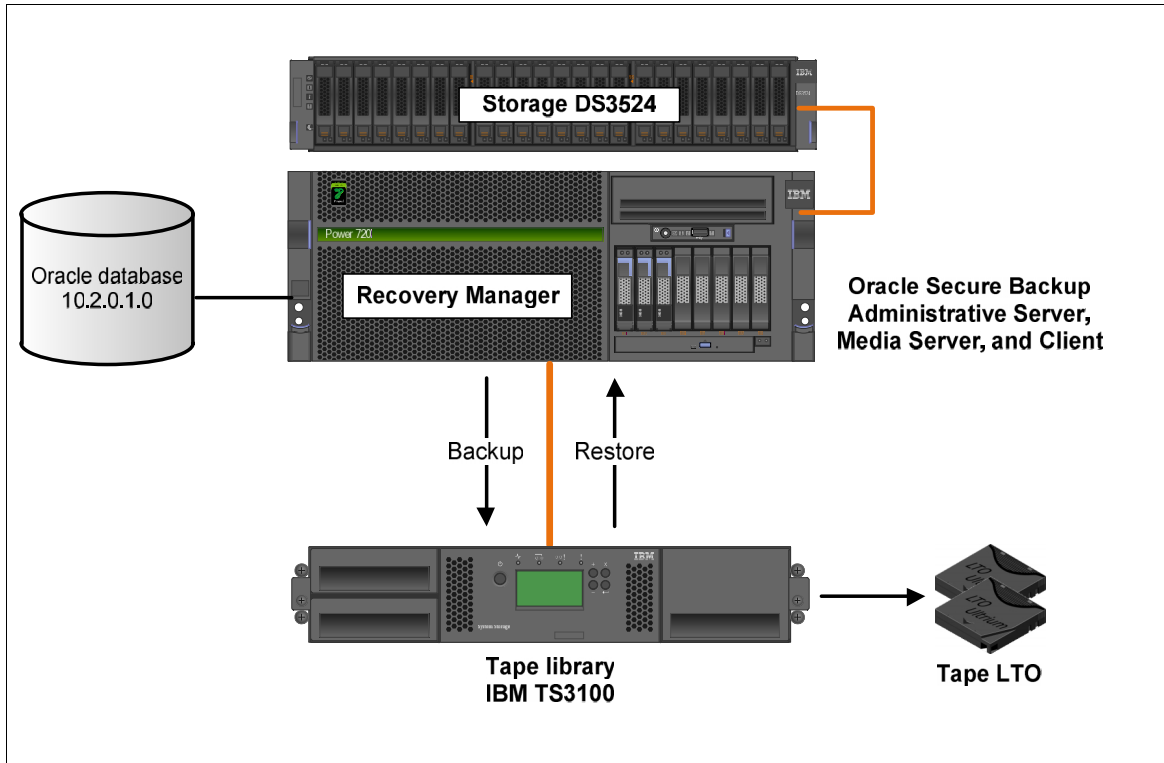


Figura 4 Arquitectura de BD con OSB instalado

Por el momento no se entrará en mayor detalle sobre el esquema de respaldos en esta arquitectura, en los siguientes capítulos se proporcionará una introducción a los conceptos básicos que son necesarios para entender la implementación de OSB, se expondrá el procedimiento de instalación y configuración de software, y finalmente se mostrará la ejecución de un respaldo usando el esquema “Online Backup” de RMAN³ junto con el sistema de protección de datos “Oracle Secure Backup”.

³ RMAN (Recovery Manager) es una utilidad de copias de seguridad para bases de datos Oracle.

Capítulo II

Arquitectura del motor de BD Oracle

Este capítulo se enfoca en los conceptos y estructuras del núcleo de la BD Oracle. Una vez que se entienda la arquitectura del servidor Oracle, se tendrá el contexto para entender el resto de características del sistema gestor de base de datos.

2.1 Base de datos e instancia

Estos son dos conceptos fundamentales para entender la arquitectura de Oracle, cuando se utilizan en el contexto de Oracle parecen causar una gran confusión. En la terminología de Oracle las definiciones de estos términos son las siguientes⁴:

- *Base de datos*: Es una colección de archivos físicos del sistema operativo, en Oracle el término base de datos se refiere al almacenamiento físico de la información.
- *Instancia*: Es un conjunto de procesos y un área de memoria compartida, se refiere al software que se ejecuta en el servidor y proporciona acceso a la información en la base de datos.

La instancia se ejecuta en el servidor y la base de datos se almacena en los discos conectados al servidor, la figura 5 ilustra esta relación.

La relación que existe entre la base de datos y la instancia es sumamente importante, ya que mientras la instancia esté en funcionamiento los datos pueden entrar y salir de la base de datos cambiando el estado físico de la base, si la instancia se encuentra abajo o no está

⁴ KYTE, Thomas. "Expert Oracle Database Architecture: Oracle Database 9i, 10g, and 11g Programming Techniques and Solutions". p. 52.

en funcionamiento, los usuarios no podrán acceder a la base de datos a pesar de que esta exista físicamente.

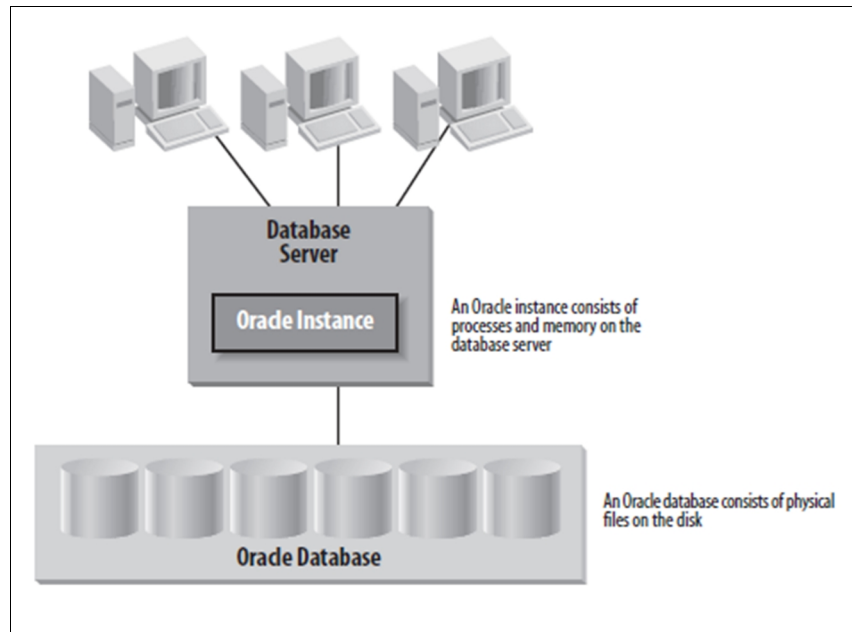


Figura 5 Instancia y Base de datos

2.2 Estructuras de memoria y procesos

En la sección anterior se mencionó que una instancia es un conjunto de procesos y un área de memoria compartida, pero no se abordó con gran detalle cada uno de esos procesos (PMON, SMON, LGWR, DBW n , CKPT) y el área de memoria compartida (SGA).

En esta sección se expondrá con mayor detalle cada uno de los procesos y las estructuras de memoria que conforman una instancia de Oracle.

2.2.1 System Global Area (SGA)

La estructura de memoria principal dentro del motor de base de datos Oracle es el Área Global del Sistema o System Global Area.

Está definida como una región de memoria compartida que contiene, además de los datos e información de una instancia Oracle, los parámetros de configuración y los datos que se estén extrayendo o manipulando en ese momento. Cada instancia Oracle tiene su propia SGA, administrando óptimamente los recursos del sistema.

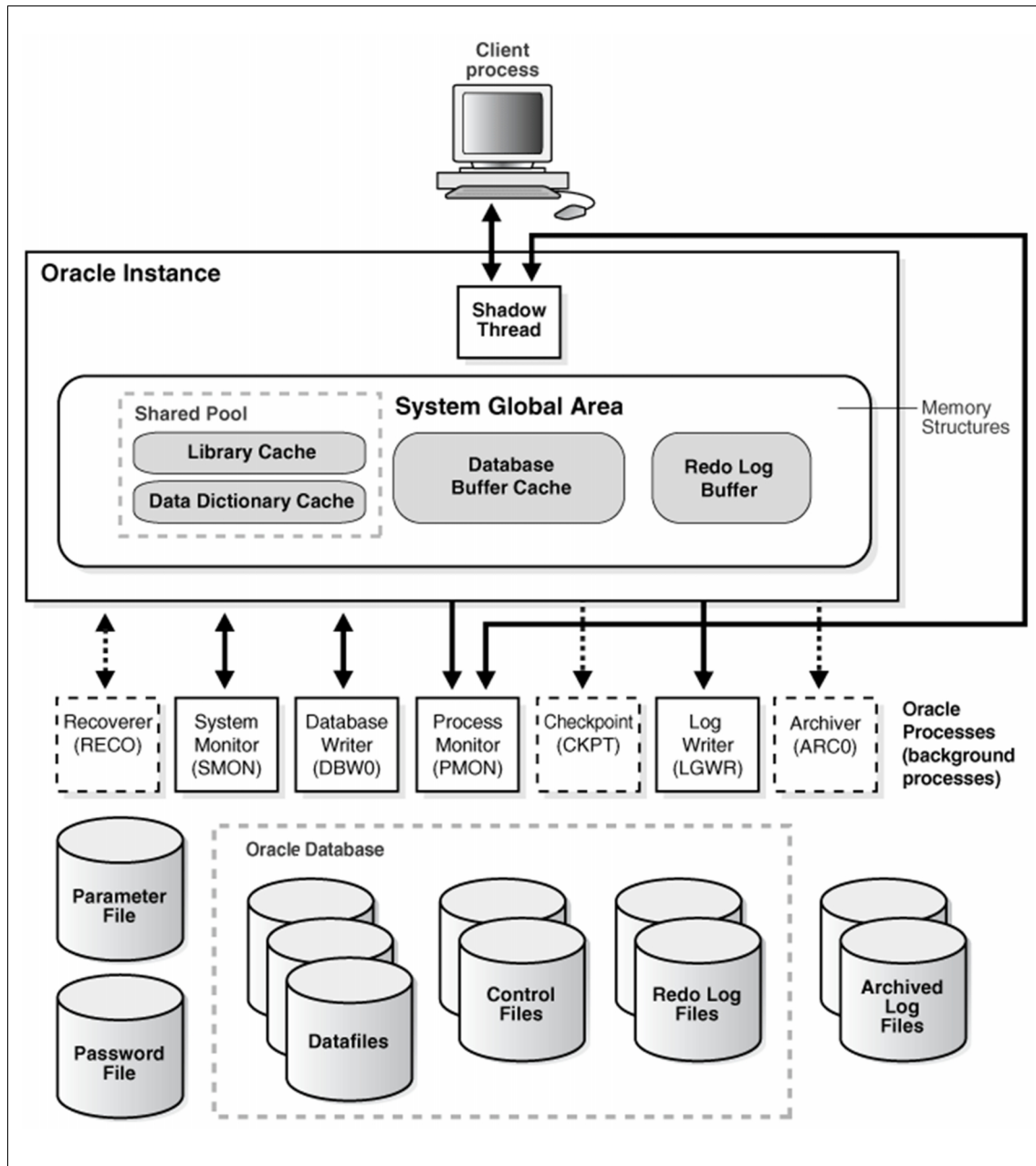


Figura 6 Estructuras de memoria y procesos Oracle

La SGA está compuesta por tres principales elementos:

- Database Buffer Cache.
- Redo Log Buffer.
- Shared Pool.

Shared Pool: La Shared Pool es una sección de la SGA que contiene estructuras de memoria compartida, tales como áreas específicas para SQL (Library Cache). Este tipo de segmentos de memoria son requeridos exclusivamente para expresiones de SQL solicitadas a la base de datos. Un área compartida (Shared Pool) contiene por ejemplo, el plan de ejecución de una sentencia, texto de la sentencia y lista de objetos referenciados.

También se almacena en la zona de SQL compartido (Shared Pool) la caché del diccionario. La información sobre los objetos de la BD se encuentra almacenada en las tablas del diccionario, cuando esta información se necesita, se leen las tablas del diccionario y su información se guarda en la caché del diccionario de la SGA.

Database Buffer Cache: Los buffers de una base de datos, se encargan de almacenar la información extraída más recientemente. Al juego de buffers de una base de datos se le conoce como Database Buffer Cache. El Database Buffer Cache mantiene los bloques de datos más usados y más recientes en memoria. Esto es para disminuir la entrada y salida de datos de un disco duro, lo que propicia una mejora en el desempeño.

Redo Log Buffer: El Redo Log Buffer de una SGA contiene todos los cambios hechos a la base de datos. Cualquier cambio producido en la base de datos, es reflejado en tiempo real en el Redo Log Buffer que constantemente está escribiendo en los archivos redo log, los cuales son indispensables en caso de ser necesaria una recuperación de información.

2.2.2 Procesos de Background

Oracle genera un conjunto de procesos de background para cada instancia (se les asigna esta denominación porque no corren en un entorno en el que el usuario final los pueda identificar, un DBA o administrador de sistemas con los permisos adecuados puede monitorear este tipo de procesos). Los procesos de background desarrollan las funciones que de otra forma serían manejadas por múltiples programas en cada proceso generado por un usuario⁵.

Los procesos de background en el servidor son el enlace entre las estructuras físicas y de memoria. A continuación, se describen los procesos de background más importantes en Oracle y el papel que juega cada uno en la gestión de la BD.

⁵ <http://www.infor.uva.es/~jvegas/cursos/bd/orarq/orarq.html>

Antes de continuar, es importante mencionar que en esta sección se hará referencia a varios tipos de archivos como los datafiles, control files, redo logs, etc. de los cuales todavía no se proporciona una definición. Si se quiere saber la definición, en la próxima sección (2.3 Archivos) se puede encontrar la descripción de cada uno.

System Monitor (SMON): El proceso SMON es el supervisor del sistema y se encarga de todas las recuperaciones que sean necesarias durante el arranque. Esto puede ser necesario si la BD se paró inesperadamente por fallo físico, lógico u otras causas. Este proceso realiza la recuperación de la instancia de BD a partir de los archivos redo log. Además limpia los segmentos temporales no utilizados y compacta los huecos libres contiguos en los archivos de datos (datafiles).

Process Monitor (PMON): Este proceso restaura las transacciones no validadas de los procesos de usuario que abortan, liberando los bloqueos y los recursos de la SGA. Asume la identidad del usuario que ha fallado, liberando todos los recursos de la BD que estuviera utilizando, y anula la transacción cancelada.

Database Writer (DBW n): El proceso DBW n es el responsable de gestionar el contenido de los buffers de datos y la caché del diccionario. Es el único proceso que puede escribir en la BD, esto asegura la integridad. Se encarga de escribir los bloques de datos modificados por las transacciones, tomando la información del buffer de la BD cuando se valida una transacción. Cada validación no se lleva a la BD física de manera inmediata sino que los bloques de la BD modificados se vuelcan a los archivos de datos periódicamente o cuando sucede algún checkpoint o punto de sincronización, mientras, para que se mantenga la integridad y coherencia de la BD, todas las operaciones se guardan en los archivos redo log. El proceso de escritura es asíncrono y puede realizar grabaciones multibloque para aumentar la velocidad.

Log Writer (LGWR): El proceso LGWR es el encargado de escribir los registros redo log en los archivos redo log. Los registros redo log siempre contienen el estado más reciente de la BD, ya que puede que el DBW n deba esperar para escribir los bloques modificados desde el buffer de datos a los archivos de datos.

Conviene tener en cuenta que el LGWR es el único proceso que escribe en los archivos de redo log y el único que lee directamente los buffers de redo log durante el funcionamiento normal de la BD.

Los redo log buffers almacenan una copia de las transacciones que se llevan a cabo en la BD. Así, aunque los archivos de DB no se actualicen en ese instante con los buffers de BD, la operación queda guardada y se puede reproducir. Oracle no tiene que consumir sus recursos escribiendo el resultado de las modificaciones de los datos en los archivos de datos de manera inmediata. Esto se hace porque los registros de redo log casi siempre tendrán un tamaño menor que los bloques afectados por las modificaciones de una transacción, y por lo tanto el tiempo que emplea en guardarlos es menor que el que emplearía en almacenar los bloques sucios (usados/modificados) resultado de una transacción; que ya serán trasladados a los archivos por el DBWn.

El LGWR es un proceso único, para asegurar la integridad es asíncrono. Además, permite las grabaciones multibloque.

Checkpoint (CKPT): Este proceso escribe en los archivos de control los checkpoints o puntos de sincronización. Estos puntos de sincronización son referencias al estado coherente de todos los archivos de la BD en un instante determinado. Esto significa que los bloques sucios de la BD se vuelcan a los archivos de BD, asegurándose de que todos los bloques de datos modificados desde el último checkpoint se escriben realmente en los archivos de datos y no sólo en los archivos redo log; y que los archivos de redo log también almacenan los registros de redo log hasta el último instante. La secuencia de puntos de control se almacena en los archivos de datos, en los archivos redo log y en los archivos de control.

Archiver (ARCn): El proceso archivador tiene que ver con los archivos redo log. Por defecto, estos archivos se reutilizan de manera cíclica de modo que se van perdiendo los registros redo log que tienen una cierta antigüedad. Cuando la BD se ejecuta en modo ARCHIVELOG, antes de reutilizar un archivo redo log el proceso ARCn realiza una copia del mismo. De esta manera se mantiene una copia de todos los registros redo log por si fueran necesarios para una recuperación.

Recoverer (RECO): El proceso de recuperación está asociado a una arquitectura distribuida (p. ej. Oracle RAC). En un servidor distribuido los datos se encuentran

repartidos en varias ubicaciones físicas, y estas se han de mantener sincronizadas. Cuando una transacción distribuida se lleva a cabo puede que ocurran problemas en la red de comunicación y estos ocasionen que una de las ubicaciones no aplique las modificaciones debidas. Esta transacción dudosa debe ser resuelta de algún modo, y esa es la tarea del proceso recuperador.

2.3 Archivos

Como se mencionó en la sección 2.1, una base de datos es una colección de archivos, estos archivos son las estructuras físicas que conforman la BD y en Oracle existen diferentes tipos de archivos, los más importantes son los siguientes:

Datafiles: Los archivos de datos desarrollan la función más importante dentro del sistema Oracle, en ellos se deposita toda la información de la base de datos (tablas, índices y otros objetos de la BD). Estos archivos no pueden ser leídos por utilerías del sistema operativo directamente, como podrían ser un more en UNIX o un notepad en Windows. La única forma de acceder a los contenidos es vía SQL.

Solo son modificados por el proceso DBWn y en ellos se vuelcan los bloques modificados de la SGA cuando sucede un checkpoint. Un datafile está asociado exclusivamente a un tablespace⁶, mientras que éste puede tener uno o más datafiles. En la siguiente imagen se muestra la relación entre datafiles y tablespaces.

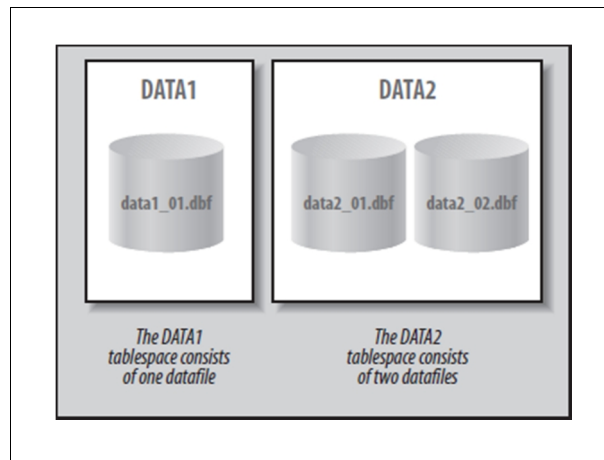


Figura 7 Datafiles y tablespaces

⁶ Se denominan tablespaces a las unidades lógicas en que se encuentra dividida una base de datos. Son usadas para agrupar estructuras físicas.

Online redo log files: Los archivos redo log almacenan los cambios realizados a la base de datos producto de las transacciones y actividades internas de Oracle. Estos archivos permiten mantener la consistencia de la base de datos, Oracle generalmente conserva los bloques modificados en memoria por un tiempo, cuando se produce un fallo por ejemplo, algunos bloques modificados podrían no haber sido escritos a los archivos de datos. El registro de los cambios en los archivos redo log se puede utilizar para reproducir los cambios perdidos en el momento que se produjo el error, protegiendo así la integridad de las transacciones.

Además, los redo log files son utilizados para “deshacer” operaciones cuando una sentencia ROLLBACK es ejecutada. El propósito principal de los archivos redo log es ser utilizados en caso de que ocurra una falla de instancia o de un medio (disco duro).

Los archivos redo log funcionan de manera cíclica (Figura 8). Una vez que el archivo en el que se está escribiendo la información ha alcanzado el tamaño predefinido, el sistema escribe las siguientes transacciones en el archivo subsecuente. Cuando concluye la escritura en el último archivo de la secuencia, se empezará a escribir nuevamente en el primer archivo.

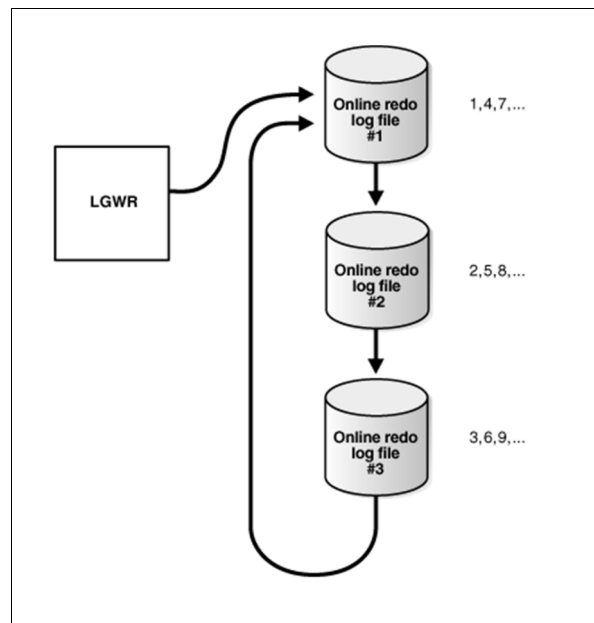


Figura 8 Reutilización de Online redo log files

Archived redo log files: Como ya se mencionó los redo log files funcionan de manera cíclica, lo cual implica que cuando el ultimo archivo redo log está lleno se tendrá que reutilizar el primer archivo redo log para continuar escribiendo, esta forma de funcionamiento provoca que la información almacenada en los archivos redo log se

sobrescriba y por lo tanto se pierda. Para evitar la pérdida de la información al momento de reutilizar un archivo redo log se utilizan los archivos archived redo log, la finalidad de los archivos archived redo log es archivar/almacenar la información contenida en los redo log files antes de que estos se sobrescriban. El proceso encargado de archivar los redo log files es el proceso ARC*n* y como producto del archivado se generan archivos archived redo log.

Control files: Los archivos de control mantienen la información de todos los archivos que conforman la BD. Son utilizados para mantener la consistencia interna y guiar las operaciones de recuperación, estos archivos son imprescindibles para que la BD pueda arrancar. Los control files contienen información clave sobre el estado de la BD, incluyendo:

- Fecha de creación y nombre de la BD.
- Información de los tablespaces.
- Nombres y ubicaciones de los datafiles y redo log files.
- Información de arranque y parada de la BD.
- Estado online y offline de los datafiles.
- Información de los archived redo log.
- Información de RMAN.
- Información sobre los checkpoints.

Además de proporcionar información fundamental para el inicio de la BD, los archivos de control son también usados cuando se elimina una base de datos. Es recomendable tener múltiples copias en distintos discos, mínimo dos, para protegerlos de fallos de disco.

PFILE y SPFILE: Oracle ofrece dos diferentes tipos de archivos de parámetros, mutuamente excluyentes, que se pueden utilizar para configurar el motor de BD: el PFILE y el SPFILE.

El PFILE: es un archivo basado en texto y ha sido el archivo utilizado por Oracle durante más de una década. En el PFILE se encuentran algunos de los ajustes de la base de datos, estos ajustes indican a Oracle cómo ha de iniciar una base de datos: cantidad de memoria a asignar, dónde están los archivos de control, dónde serán almacenados los archived redo logs, etc. El archivo PFILE está en formato texto plano por lo que es editable directamente

con cualquier editor como vi o notepad, actualmente, en versiones de Oracle 9i, 10g, 11g y 12c no suele usarse pues por defecto se utiliza el archivo SPFILE.

El SPFILE difiere con el PFILE en que no es editable directamente, esto debido a que es un archivo binario. Como el archivo de parámetros SPFILE no es editable directamente, Oracle permite gestionar el SPFILE a través del comando “ALTER SYSTEM”. El archivo SPFILE puede ser copiado por RMAN, lo que significa que es más fácil de recuperar. Además, el archivo SPFILE permite hacer cambios dinámicos a los parámetros que son persistentes.

Una de las ventajas más importantes del SPFILE es que Oracle ha introducido muchas características de ajuste automático en el núcleo de la base de datos, sin un SPFILE, Oracle no podría autoajustar su base de datos.

El SPFILE utiliza el mismo formato para el nombre del archivo que el PFILE, excepto que la palabra "spfile" sustituye a la palabra "init". Por ejemplo, si el ORACLE_SID de nuestra Base de datos es TEST, el SPFILE resultante se llamará “spfileTEST.ora”.

2.4 Modo archivelog vs. noarchivelog

Una base de datos Oracle puede trabajar en uno de los dos modos: ARCHIVELOG o NOARCHIVELOG. Por defecto, la BD es creada en modo NOARCHIVELOG. Este modo permite operaciones normales en la base de datos, pero no provee la capacidad de realizar operaciones de recuperación a un punto en el tiempo o copias de seguridad en línea (Online backup's). Si se desea realizar copias de seguridad en línea, la base de datos debería ejecutarse en modo ARCHIVELOG. En modo ARCHIVELOG la base de datos hace copias de todos los online redo logs a través del proceso ARC*n*, hacia una o más ubicaciones.

En modo NOARCHIVELOG las copias de seguridad se tendrán que hacer fuera de línea (Offline backup), es decir, con la base de datos parada. En caso de ser necesario un RESTORE todos los cambios que se hayan producido en la BD desde que se realizó el último backup se perderían.

Es recomendable activar el modo ARCHIVELOG en entornos donde la pérdida de información no está permitida, una buena práctica es mantener todas las bases de datos de producción funcionando en modo ARCHIVELOG.

Capítulo III

Copias de seguridad físicas en Oracle

En una base de datos Oracle existen 2 tipos de copias de seguridad: copias de seguridad físicas y copias de seguridad lógicas.

Las copias de seguridad físicas son respaldos de los archivos físicos usados para el almacenamiento y recuperación de la base de datos, como son los datafiles, control files, y archived redo logs. En última instancia, toda copia de seguridad física es una copia de los archivos que almacenan la información de la BD en una ubicación diferente, esta ubicación puede ser un disco duro o una cinta magnética.

Las copias de seguridad lógicas contienen datos lógicos (p. ej. tablas o procedimientos almacenados) exportados de una base de datos con la utilidad `export` y almacenados en un archivo binario, el archivo puede ser importado más tarde en una BD empleando la utilidad `import` de Oracle.

En este capítulo solo se tratarán las copias de seguridad físicas de una base de datos Oracle, debido a que las copias de seguridad lógicas no son la mejor opción para respaldar grandes BD (los respaldos lógicos se pueden usar como complemento de los respaldos físicos). Las copias de seguridad físicas pueden ser clasificadas de la siguiente manera:

- Copias de seguridad gestionadas por el usuario (Offline y Online).
- Copias de seguridad gestionadas por el servidor (Offline y Online).

Cada una de las copias de seguridad puede ser realizada en línea (Online backup) o fuera de línea (Offline backup).

Las copias de seguridad “Offline” implican parar la base de datos en modo normal y copiar todos los archivos sobre los que se asienta, por consiguiente, la BD permanecerá inaccesible para todos los usuarios mientras se realizan las copias de seguridad. Antes de parar la BD

hay que parar también todas las aplicaciones que estén trabajando con la base de datos, una vez realizada la copia de los archivos, la base de datos se puede volver a arrancar.

Las copias de seguridad “Online” se realizan mientras la BD está abierta y funcionando, son la mejor opción cuando los requisitos de disponibilidad son altos. Es recomendable ejecutar las copias de seguridad cuando las cargas de trabajo en la BD sean pequeñas, esto con la finalidad de afectar lo menos posible el desempeño de la base de datos.

3.1 Copias de seguridad gestionadas por el usuario

Las copias de seguridad gestionadas por el usuario son aquellas en donde se requiere mayor intervención por parte del usuario, se emplean las utilidades del sistema operativo junto con algunos comandos de SQL *Plus para hacer el respaldo de los archivos que conforman la base de datos.

3.1.1 Offline backup gestionado por el usuario.

En una copia de seguridad Offline (cold backup) gestionada por el usuario, la base de datos debe permanecer cerrada mientras se ejecuta la copia de los archivos que conforman la BD, básicamente los pasos a seguir para hacer este tipo de respaldo son los siguientes:

1. Apagar la base de datos completamente.
2. Respaldar todos los datafiles, control files, online redo logs (opcional) y los archivos de parámetros empleando las utilidades del sistema operativo (`cp`, `dd`, `tar` en UNIX/Linux o `copy` en Windows).
3. Iniciar la base de datos.

Los pasos anteriores son aplicables para cuando la base de datos esta funcionando en modo NOARCHIVELOG. En este modo la base de datos solo podrá ser recuperada hasta el punto en el que se encontraba al momento de hacer la copia de seguridad, esto quiere decir que los cambios hechos en la BD después de realizar la copia de seguridad no podrán ser recuperados.

La base de datos de la SIIM IFE utilizaba este esquema de respaldos antes de la implementación del sistema OSB, como se mencionó en el capítulo I, el esquema es ineficiente puesto que la base de datos debe permanecer fuera de línea durante todo el

proceso de respaldo. Además, como ya se dijo, la BD solo podrá ser recuperada al estado en el que se encontraba al momento de ejecutar el respaldo.

En instrucciones de Oracle los tres pasos anteriores se traducen a la ejecución de los siguientes comandos:

1. Apagar la base de datos completamente.

```
[oracle@afisdb ~]$ sqlplus / as sysdba
SQL*Plus: Release 10.2.0.1.0 - Production on Sat Jun 8 17:26:27 2013
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Connected to an idle instance.
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL>
```

2. Respalidar todos los datafiles, control files, online redo logs (opcional) y archivos de parámetros.

```
[oracle@afisdb ~]$ tar -cf /dev/rmt0 /oradata
```

En el caso de la base de datos de la SIIM IFE se utilizaba el comando `tar` del sistema operativo para almacenar los archivos de la BD en cinta magnética.

- c: Parámetro utilizado para la creación de un nuevo archivo conformado por los directorios o archivos indicados al final del comando `tar` (`/oradata` en este caso).
- f `/dev/rmt0`: Parámetro utilizado para indicar el lugar donde se escribirán los archivos. En el sistema operativo AIX el dispositivo `/dev/rmt0` está ligado a la unidad de cinta magnética.

En la BD de la SIIM IFE se conocía con anticipación la ubicación de los datafiles, control files, y online redo logs. Todos estos archivos se encontraban almacenados en el directorio `/oradata`, por lo que la copia de seguridad de la BD se limitaba a hacer un respaldo de dicho directorio.

Para los casos donde no se conozca con anticipación la ubicación de los archivos de la base de datos, se puede hacer uso de las siguientes consultas (fig. 9) para determinar la ubicación de cada uno de los archivos.

```

/* LISTAR UBICACIÓN DE LOS DATAFILES */

SQL> select name from v$datafile;

NAME
-----
/oradata/AFIS/system01.dbf
/oradata/AFIS/users01.dbf
/oradata/AFIS/data/AFIS_data_1.dbf
/oradata/AFIS/data/AFIS_data_2.dbf
/oradata/AFIS/data/app/AFIS_data_app_3.dbf
/oradata/AFIS/idx/AFIS_idx_1.dbf
/oradata/AFIS/idx/AFIS_idx_2.dbf
/oradata/AFIS/undo/AFIS_undo_1.dbf
/oradata/AFIS/bin9_b/AFIS_bin9_8.dbf
/oradata/AFIS/bin9_a/AFIS_bin9_9.dbf
/oradata/AFIS/bin9_b/AFIS_bin9_10.dbf
/oradata/AFIS/bin9_a/AFIS_bin9_11.dbf
/oradata/AFIS/idx/alphabinary/AFIS_idx_alphabinary_1.dbf
...
-- Se omite parte de la salida por cuestiones de simplicidad

/* LISTAR UBICACIÓN DE LOS CONTROLFILES */

SQL> select name from v$controlfile;

NAME
-----
/oradata/AFIS/control01.ctl
/oradata/AFIS/control02.ctl
/oradata/AFIS/control03.ctl

/* LISTAR UBICACIÓN DE LOS ONLINE REDO LOGS */

SQL> select member from v$logfile;

MEMBER
-----
/oradata/AFIS/redo01.log
/oradata/AFIS/redo02.log
/oradata/AFIS/redo03.log

/* LISTAR UBICACIÓN DEL ARCHIVO DE PARÁMETROS SPFILE */

SQL> select name, value from v$parameter where name = 'spfile';

NAME          VALUE
-----
spfile        /oradata/AFIS/spfileAFIS.ora

```

Figura 9 Ubicación de Datafiles, Control files, Onlie redo logs y Spfile

3. Finalmente, una vez terminada la copia de seguridad hay que iniciar la base de datos.

```
SQL> startup;
```

3.1.2 Online backup gestionado por el usuario.

Oracle tiene la posibilidad de ejecutar copias de seguridad en línea (hot backup's) manejadas por el usuario, para ello, es necesario que la base de datos esté funcionando en modo ARCHIVELOG. La ventaja de hacer un respaldo en línea es que la base de datos puede permanecer abierta mientras se ejecuta la copia de seguridad, por consiguiente, los usuarios podrán conectarse a la BD mientras se lleva a cabo el proceso de respaldo. Para hacer una copia de seguridad en línea es necesario ejecutar el siguiente procedimiento:

1. Asegurarse de que la base de datos está funcionando en modo ARCHIVELOG.
2. Usar el comando **alter database begin backup** para poner los datafiles que conforman la BD en modo copia de seguridad en línea.
3. Respalidar los archivos datafiles que conforman la base de datos haciendo uso de las utilidades del sistema operativo.
4. Poner los datafiles fuera del modo copia de seguridad en línea usando el comando **alter database end backup**.
5. Hacer que el actual online redo log sea archivado, usar el comando **alter system switch logfile**.
6. Una vez que el actual online redo log ha sido archivado, respaldar todos los archivos archived redo log. Hacer uso de las utilidades del sistema operativo para realizar el respaldo de los archivos.

A continuación se muestra la ejecución de los pasos anteriores en el servidor de base de datos Oracle.

1. Asegurarse de que la base de datos está funcionando en modo ARCHIVELOG.
-

```
/* CONSULTA PARA DETERMINAR SI LA BD ESTA FUNCIONANDO EN MODO ARCHIVELOG */
```

```
SQL> select log_mode from v$database;
```

```
LOG_MODE  
-----  
ARCHIVELOG
```

```
SQL>
```

```
/* COMANDO PARA SABER SI LA BD ESTA FUNCIONANDO EN MODO ARCHIVELOG  
Y LA UBICACIÓN DE LOS ARCHIVED REDO LOG */
```

```
SQL> archive log list;
```

Database log mode	Archive Mode
Automatic archival	Enabled
Archive destination	/oradata/AFIS/arch1/
Oldest online log sequence	513
Next log sequence to archive	514
Current log sequence	514

Si la base de datos no se encuentra funcionando en modo ARCHIVELOG, apagar la BD con el comando **shutdown immediate** e iniciarla en modo mount con **startup mount**. Poner la base de datos en modo ARCHIVELOG usando el comando **alter database archivelog** y finalmente abrir la BD con **alter database open**.

2. Usar el comando **alter database begin backup** para poner los datafiles que conforman la BD en modo copia de seguridad en línea.

```
SQL> alter database begin backup;
```

```
Database altered.
```

```
SQL>
```

3. Respalidar los archivos datafiles que conforman la base de datos haciendo uso de las utilidades del sistema operativo.

```
[oracle@afisdb ~]$ tar -cf /dev/rmt0 /oradata
```

4. Poner los datafiles fuera del modo copia de seguridad en línea usando el comando **alter database end backup**.

```
SQL> alter database end backup;  
  
Database altered.  
  
SQL>
```

5. Hacer que el actual online redo log sea archivado, usar el comando **alter system switch logfile**.

```
SQL> alter system switch logfile;  
  
System altered.  
  
SQL>
```

6. Una vez que el actual online redo log ha sido archivado, respaldar todos los archivos archived redo log. Hacer uso de las utilidades del sistema operativo para realizar el respaldo de los archivos.

```
[oracle@afisdb ~]$ tar -cf /dev/rmt0 /oradata/AFIS/arch1/
```

Nota: En este tipo de respaldos cuando la base de datos se coloca en modo `begin backup`, Oracle internamente hace que los datafiles comprendidos en la BD no sean escritos por el proceso `DBWn` y todos los cambios ocurridos a nivel bloque son escritos en los redo logs (se tendrá la copia de cada bloque cambiado), por lo tanto, se genera gran cantidad de redo logs debido a que se está escribiendo más información de lo normal. Oracle recomienda ejecutar este tipo de copias de seguridad en los horarios más libres.

3.2 Copias de seguridad gestionadas por el servidor

Las copias de seguridad gestionadas por el servidor son aquellas en donde la intervención por parte del usuario o DBA (Administrador de Base de Datos) es mínima, las copias de

seguridad se ejecutan haciendo uso del Recovery Manager (RMAN), una herramienta que el motor de BD Oracle pone a disposición de los usuarios para hacer respaldos y recuperaciones de la base de datos. En este tipo de respaldos la administración de las copias de seguridad se facilita, puesto que el servidor (en los archivos de control) permite almacenar metadatos de los respaldos ejecutados.

3.2.1 Recovery Manager (RMAN)

El Recovery Manager es la principal herramienta para la ejecución de copias de seguridad y recuperaciones en Oracle, es una herramienta que viene incluida con el motor de BD. No es necesario pagar una licencia adicional para poder usar RMAN, como es el caso de otros productos de Oracle (p. ej. Oracle Enterprise Manager Grid Control). Desde su introducción en la versión 8 de Oracle, RMAN ha tenido considerables mejoras hasta el punto en el que ha llegado a convertirse en la herramienta más poderosa para el respaldo y recuperación de bases de datos. Poniendo a disposición de los usuarios, su amplia gama de sofisticadas y poderosas capacidades.

RMAN tiene una perfecta integración con la interfaz gráfica de usuario Oracle Enterprise Manager (OEM), se pueden realizar operaciones de respaldo a través del cliente RMAN o por medio del Oracle Enterprise Manager. RMAN también permite el uso de componentes adicionales como la “Media Management Layer (MML)” o “Capa de Manejo de Medios” con la finalidad de hacer la estrategia de respaldo y recuperación más fácil y robusta.

Básicamente la “Capa de Manejo de Medios” es un software para interactuar con las unidades de cinta magnética y automatizar el manejo de las mismas. El Recovery Manager únicamente puede interactuar de forma directa con unidades de disco, por esta razón, si se desea utilizar cintas magnéticas como medio de almacenamiento de los respaldos, es necesario utilizar una “Capa de Manejo de Medios”. Existen varias aplicaciones en el mercado que se desempeñan como MML, entre las más conocidas y comerciales están: IBM Tivoli Storage Manager, Symantec NetBackup, EMC NetWorker, HP Data Protector y Oracle Secure Backup, esta última se tratará con mayor detalle en el próximo capítulo.

A continuación, se listan algunas de las ventajas de utilizar RMAN frente a un esquema de respaldos gestionado por el usuario:

- Uso de comandos simples para hacer las copias de seguridad y recuperaciones.
 - Gestión automática de los archivos de las copias de seguridad sin la intervención del DBA.
-

- Borrado automático de copias de seguridad con “datafiles” y “archived redo logs” innecesarios.
- Se puede tener informes detallados de las acciones ejecutadas durante el proceso de respaldo.
- Ayuda considerable al momento de duplicar una base de datos.
- Es posible probar si se puede recuperar la base de datos sin tener que restaurar los datos.
- Se pueden verificar las copias de seguridad disponibles y determinar si son útiles para una recuperación.
- Es posible hacer copias de seguridad incrementales.
- Es posible hacer copias de seguridad cifradas.
- Se puede usar la ventaja de compresión de bloques no usados, RMAN salta los bloques no usados y omite su respaldo.

Si se desea conocer todas las características, capacidades, conceptos básicos y terminología de RMAN, se puede consultar la documentación oficial de Oracle que cuenta con mayor detalle sobre cada uno de los puntos mencionados. Particularmente, se recomienda consultar los siguientes documentos que pueden ser de gran ayuda:

“Oracle Database Backup and Recovery Basics 10g Release 2 (10.2)”

“Oracle Database Backup and Recovery Reference 10g Release 2 (10.2)”

“Oracle Database Backup and Recovery Advanced User's Guide 10g Release 2 (10.2)”

3.2.2 Offline backup gestionado por el servidor.

Para hacer una copia de seguridad fuera de línea gestionada por el servidor, es necesario utilizar RMAN. Dependiendo de los requerimientos del negocio, será necesario configurar RMAN para cumplir con las políticas de respaldo de la organización o la empresa, por ejemplo, habrá que configurar una política de retención para determinar cuánto tiempo se mantendrán activas las copias de seguridad antes de ser consideradas obsoletas. También, podría ser necesario instalar y configurar una “Capa de Manejo de Medios” si lo que se quiere es almacenar los respaldos en cintas magnéticas. Por el momento, el siguiente ejemplo solo se limita a mostrar los pasos necesarios para hacer un respaldo sin entrar en mayor detalle sobre la configuración de RMAN.

Para hacer un Offline backup gestionado por el servidor, se tiene que apagar la BD y posteriormente iniciarla en modo “mount”, que es la forma en que debe estar para ejecutar

el respaldo. Una vez montada la base de datos simplemente hay que usar el comando **backup database** y la copia de seguridad será realizada. Aquí un ejemplo de los comandos que se tendrían que utilizar para realizar un “Offline backup” gestionado por el servidor.

```
/* CONEXIÓN DE RMAN CON LA BD A RESPALDAR */
[oracle@afisdb ~]$ rman target /
Recovery Manager: Release 10.2.0.1.0 - Production on Sat Jun 15 14:53:28 2013
Copyright (c) 1982, 2005, Oracle. All rights reserved.
connected to target database: AFIS (DBID=2363544759)
/* APAGADO DE LA BD */
RMAN> shutdown immediate;
using target database control file instead of recovery catalog
database closed
database dismounted
Oracle instance shut down
/* INICIAR BD EN MODO MOUNT */
RMAN> startup mount;
connected to target database (not started)
Oracle instance started
database mounted
Total System Global Area      3154116608 bytes
Fixed Size                     2024176 bytes
Variable Size                  671091984 bytes
Database Buffers               2466250752 bytes
Redo Buffers                   14749696 bytes
/* EJECUCIÓN DEL RESPALDO DE LA BD */
RMAN> backup database;
Starting backup at 15-JUN-13
allocated channel: ORA_SBT_TAPE_1
channel ORA_SBT_TAPE_1: sid=157 devtype=SBT_TAPE
channel ORA_SBT_TAPE_1: Oracle Secure Backup
allocated channel: ORA_SBT_TAPE_2
channel ORA_SBT_TAPE_2: sid=155 devtype=SBT_TAPE
channel ORA_SBT_TAPE_2: Oracle Secure Backup
channel ORA_SBT_TAPE_1: starting full datafile backupset
channel ORA_SBT_TAPE_1: specifying datafile(s) in backupset
input datafile fno=00001 name=/oradata/AFIS/system01.dbf
input datafile fno=00687 name=/oradata/AFIS/bin3_a/AFIS_bin3_1.dbf
input datafile fno=00689 name=/oradata/AFIS/bin3_a/AFIS_bin3_3.dbf
```

```
input datafile fno=00691 name=/oradata/AFIS/bin3_a/AFIS_bin3_5.dbf
input datafile fno=00693 name=/oradata/AFIS/bin3_a/AFIS_bin3_7.dbf
input datafile fno=00695 name=/oradata/AFIS/bin3_a/AFIS_bin3_9.dbf
input datafile fno=00697 name=/oradata/AFIS/bin3_a/AFIS_bin3_11.dbf
input datafile fno=00699 name=/oradata/AFIS/bin3_a/AFIS_bin3_13.dbf
input datafile fno=00701 name=/oradata/AFIS/bin3_a/AFIS_bin3_15.dbf
input datafile fno=00703 name=/oradata/AFIS/bin3_a/AFIS_bin3_17.dbf
input datafile fno=00705 name=/oradata/AFIS/bin3_a/AFIS_bin3_19.dbf
input datafile fno=00707 name=/oradata/AFIS/bin3_a/AFIS_bin3_21.dbf
input datafile fno=00709 name=/oradata/AFIS/bin3_a/AFIS_bin3_23.dbf
input datafile fno=00711 name=/oradata/AFIS/bin3_a/AFIS_bin3_25.dbf
input datafile fno=00713 name=/oradata/AFIS/bin3_a/AFIS_bin3_27.dbf
input datafile fno=00715 name=/oradata/AFIS/bin3_a/AFIS_bin3_29.dbf
input datafile fno=00717 name=/oradata/AFIS/bin3_a/AFIS_bin3_31.dbf
input datafile fno=00719 name=/oradata/AFIS/bin2_a/AFIS_bin2_1.dbf
input datafile fno=00721 name=/oradata/AFIS/bin2_a/AFIS_bin2_3.dbf
input datafile fno=00723 name=/oradata/AFIS/bin2_a/AFIS_bin2_5.dbf
input datafile fno=00725 name=/oradata/AFIS/bin2_a/AFIS_bin2_7.dbf
input datafile fno=00727 name=/oradata/AFIS/bin2_a/AFIS_bin2_9.dbf
input datafile fno=00729 name=/oradata/AFIS/bin2_a/AFIS_bin2_11.dbf
input datafile fno=00731 name=/oradata/AFIS/bin2_a/AFIS_bin2_13.dbf
input datafile fno=00733 name=/oradata/AFIS/bin2_a/AFIS_bin2_15.dbf
input datafile fno=00735 name=/oradata/AFIS/bin2_a/AFIS_bin2_17.dbf
input datafile fno=00737 name=/oradata/AFIS/bin2_a/AFIS_bin2_19.dbf
...
.
piece handle=36oc8q0b_1_1 tag=TAG20130615T153422 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:40:43
channel ORA_SBT_TAPE_2: finished piece 1 at 15-JUN-13
piece handle=37oc8q0s_1_1 tag=TAG20130615T153422 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE 2: backup set complete, elapsed time: 00:37:52
Finished backup at 15-JUN-13

Starting Control File and SPFILE Autobackup at 15-JUN-13
piece handle=c-2363544759-20130615-05 comment=API Version 2.0,MMS Version
10.4.0.3
Finished Control File and SPFILE Autobackup at 15-JUN-13

/* COLOCA BD EN MODO OPEN (MODO EN EL QUE NORMALMENTE TRABAJA LA BD) */

RMAN> alter database open;

database opened

RMAN>
```

Este tipo de respaldos no es muy utilizado debido a que la BD debe permanecer cerrada mientras se ejecutan las copias de seguridad, pero comparado con el esquema “Offline backup gestionado por el usuario”, aporta grandes ventajas pues el respaldo de la BD se limita a la ejecución de un comando (`backup database`).

3.2.3 Online backup gestionado por el servidor.

Es uno de los esquemas más utilizados para realizar el respaldo de una base de datos Oracle, debido que la BD puede permanecer abierta y funcionando mientras se ejecuta la copia de seguridad. A lo anterior, se suma que la BD puede ser recuperada a un punto en el tiempo y que la gestión de los archivos a respaldar queda a cargo de la utilidad RMAN. Al igual que el esquema “Offline backup gestionado por el servidor”, RMAN podría requerir de cierta configuración para cumplir con las políticas de respaldo de la empresa. Para el caso particular de este trabajo, la configuración de RMAN utilizada en la base de datos de la SIIM IFE se abordará en el capítulo V.

La forma de realizar una copia de seguridad en línea gestionada por el servidor, se reduce a la ejecución de las dos siguientes instrucciones:

1. Asegurarse de que la base de datos está funcionando en modo ARCHIVELOG.

```
SQL> select log_mode from v$database;
```

```
LOG_MODE  
-----  
ARCHIVELOG
```

2. Conectarse a RMAN y ejecutar el comando **backup database** para comenzar con el proceso de respaldo de toda la base de datos.

```
[oracle@afisdb ~]$ rman target /
```

```
Recovery Manager: Release 10.2.0.1.0 - Production on Sat Jun 15 16:14:09 2013
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
connected to target database: AFIS (DBID=2363544759)
```

```
RMAN> backup database;
```

```
Starting backup at 15-JUN-13  
using target database control file instead of recovery catalog  
allocated channel: ORA_SBT_TAPE_1  
channel ORA_SBT_TAPE_1: sid=143 devtype=SBT_TAPE  
channel ORA_SBT_TAPE_1: Oracle Secure Backup  
allocated channel: ORA_SBT_TAPE_2  
channel ORA_SBT_TAPE_2: sid=142 devtype=SBT_TAPE  
channel ORA_SBT_TAPE_2: Oracle Secure Backup  
channel ORA_SBT_TAPE_1: starting full datafile backupset
```

```

channel ORA_SBT_TAPE_1: specifying datafile(s) in backupset
input datafile fno=00001 name=/oradata/AFIS/system01.dbf
input datafile fno=00687 name=/oradata/AFIS/bin3_a/AFIS_bin3_1.dbf
input datafile fno=00689 name=/oradata/AFIS/bin3_a/AFIS_bin3_3.dbf
input datafile fno=00691 name=/oradata/AFIS/bin3_a/AFIS_bin3_5.dbf
input datafile fno=00693 name=/oradata/AFIS/bin3_a/AFIS_bin3_7.dbf
input datafile fno=00695 name=/oradata/AFIS/bin3_a/AFIS_bin3_9.dbf
input datafile fno=00697 name=/oradata/AFIS/bin3_a/AFIS_bin3_11.dbf
input datafile fno=00699 name=/oradata/AFIS/bin3_a/AFIS_bin3_13.dbf
input datafile fno=00701 name=/oradata/AFIS/bin3_a/AFIS_bin3_15.dbf
input datafile fno=00703 name=/oradata/AFIS/bin3_a/AFIS_bin3_17.dbf
input datafile fno=00705 name=/oradata/AFIS/bin3_a/AFIS_bin3_19.dbf
input datafile fno=00707 name=/oradata/AFIS/bin3_a/AFIS_bin3_21.dbf
input datafile fno=00709 name=/oradata/AFIS/bin3_a/AFIS_bin3_23.dbf
input datafile fno=00711 name=/oradata/AFIS/bin3_a/AFIS_bin3_25.dbf
input datafile fno=00713 name=/oradata/AFIS/bin3_a/AFIS_bin3_27.dbf
input datafile fno=00715 name=/oradata/AFIS/bin3_a/AFIS_bin3_29.dbf
input datafile fno=00717 name=/oradata/AFIS/bin3_a/AFIS_bin3_31.dbf
input datafile fno=00719 name=/oradata/AFIS/bin2_a/AFIS_bin2_1.dbf
input datafile fno=00721 name=/oradata/AFIS/bin2_a/AFIS_bin2_3.dbf
input datafile fno=00723 name=/oradata/AFIS/bin2_a/AFIS_bin2_5.dbf
input datafile fno=00725 name=/oradata/AFIS/bin2_a/AFIS_bin2_7.dbf
input datafile fno=00727 name=/oradata/AFIS/bin2_a/AFIS_bin2_9.dbf
input datafile fno=00729 name=/oradata/AFIS/bin2_a/AFIS_bin2_11.dbf
input datafile fno=00731 name=/oradata/AFIS/bin2_a/AFIS_bin2_13.dbf
input datafile fno=00733 name=/oradata/AFIS/bin2_a/AFIS_bin2_15.dbf
input datafile fno=00735 name=/oradata/AFIS/bin2_a/AFIS_bin2_17.dbf
input datafile fno=00737 name=/oradata/AFIS/bin2_a/AFIS_bin2_19.dbf
input datafile fno=00739 name=/oradata/AFIS/bin2_a/AFIS_bin2_21.dbf
...
..
.
input datafile fno=00549 name=/oradata/AFIS/bin16_b/AFIS16_bin_46.dbf
input datafile fno=00558 name=/oradata/AFIS/bin15_b/AFIS15_bin_8.dbf
channel ORA_SBT_TAPE_2: starting piece 1 at 15-JUN-13
channel ORA_SBT_TAPE_1: finished piece 1 at 15-JUN-13
piece handle=410c8sd0_1_1 tag=TAG20130615T211433 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:43:36
channel ORA_SBT_TAPE_2: finished piece 1 at 15-JUN-13
piece handle=430c8sha_1_1 tag=TAG20130615T211433 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_2: backup set complete, elapsed time: 00:50:04
Finished backup at 15-JUN-13

Starting Control File and SPFILE Autobackup at 15-JUN-13
piece handle=c-2363544759-20130615-07 comment=API Version 2.0,MMS Version
10.4.0.3
Finished Control File and SPFILE Autobackup at 15-JUN-13

RMAN>

```

Es recomendable ejecutar las copias de seguridad “Online” durante periodos donde la base de datos tenga pequeñas cargas de trabajo, de lo contrario, se podría afectar el desempeño si se ejecutan en horarios donde exista un gran flujo de transacciones.

Capítulo IV

Arquitectura de “Oracle Secure Backup”

OSB es un software que permite la creación de respaldos en cintas magnéticas y la recuperación de los mismos, gestiona tanto los respaldos como las recuperaciones de forma centralizada. El software está especializado en el respaldo de bases de datos Oracle, aunque también tiene la posibilidad de respaldar el sistema de archivos de los sistemas operativos más comunes/comerciales en la gama de servidores (Windows, Linux, AIX, HP-UX, Solaris). Así mismo, es compatible con el protocolo NDMP (Network Data Management Protocol), que es un protocolo utilizado para realizar copias de seguridad basadas en red.

El sistema Oracle Secure Backup es una “Capa de Manejo de Medios” para RMAN, proporciona una interfaz SBT⁷ (System Backup Tape) que RMAN puede usar para respaldar los archivos de la base de datos en una cinta magnética. OSB es el gestor de medios que mejor se integra con Oracle Enterprise Manager (OEM), se pueden manejar las cintas magnéticas, los servidores de medios y los dispositivos de cinta usando el OEM.

Entre las características más destacadas de OSB se encuentran las siguientes:

- Proporciona soporte para la mayoría de las unidades de cinta y bibliotecas de cinta en un entorno SAN (Storage Area Network), SCSI (Small Computer System Interface) o Gigabit Ethernet.
- Soporte para el protocolo de internet v4 (IPv4) y protocolo de internet v6 (IPv6).
- Soporte para dispositivos conectados por fibra óptica.
- Permite el uso de comodines y listas de exclusión al momento de especificar los archivos a respaldar.
- Usa posicionamiento directo y restauración de acceso directo para evitar la lectura innecesaria de bloques de cinta al momento de localizar archivos.

⁷ SBT es una librería de software que RMAN utiliza para realizar las copias de seguridad a un sistema de almacenamiento de otro fabricante. La interfaz SBT se ajusta a un API publicada por Oracle y es proporcionada por el fabricante del sistema de almacenamiento.

- Características altamente configurables de cifrado a partir de Oracle 9i.
- Soporta compresión rápida de copias de seguridad a partir de Oracle 11.1.0.6.
- Proporciona informes sobre el progreso de las copias de seguridad y restauraciones.
- Ofrece una integración perfecta con RMAN.
- Integración con Oracle Enterprise Manager Database y Grid Control, a partir de Oracle Database 10g Release 2.

A continuación, se describen los componentes básicos que conforman la arquitectura del sistema de protección de datos OSB.

4.1 Dominio Administrativo

Un dominio administrativo es un grupo de hosts (servidores) administrados como una unidad común para realizar las operaciones de copia de seguridad y restauración. Al momento de configurar OSB se asigna un role a cada host en el dominio. Un único host puede tener uno o más de los siguientes roles⁸:

Administrative server: El servidor de administración ejecuta el planificador (scheduler), que inicia y supervisa cada trabajo de copia de seguridad. El planificador también mantiene un catálogo de las copia de seguridad con metadatos para todas las operaciones de respaldo y restauración realizadas en el dominio administrativo.

Cada dominio administrativo debe de tener solo un servidor de administración, encargado de retener la configuración de los demás equipos que conforman el dominio, el servidor de administración puede correr otras aplicaciones además del OSB.

Media server: El servidor de medios alberga los dispositivos de almacenamiento secundarios, como las unidades de cinta o bibliotecas de cintas, es el encargado de transferir los datos desde y hacia las cintas magnéticas (volúmenes). Al menos un servidor de medios debe estar definido para cada dominio administrativo.

Client: Un cliente es un host cuyos datos locales serán respaldados por OSB. Uno o más clientes deberán definirse en cada dominio administrativo, cualquier host donde está instalado Oracle Secure Backup puede ser un cliente, incluyendo los hosts que también son

⁸ FREEMAN, G. Robert. “Oracle RMAN 11g Backup and Recovery”. p. 117.

servidores de medios o el servidor de administración. La mayoría de los hosts en el dominio administrativo son clientes.

La figura 10 muestra un dominio administrativo OSB que contiene un solo host, este host asume los roles de servidor de administración, servidor de medios, y cliente. Una base de datos Oracle y una librería de cintas conectada localmente están configuradas para el host. En la figura se puede observar la arquitectura más sencilla del sistema OSB, arquitecturas más complejas comúnmente implementan cada uno de los roles en servidores físicos diferentes.

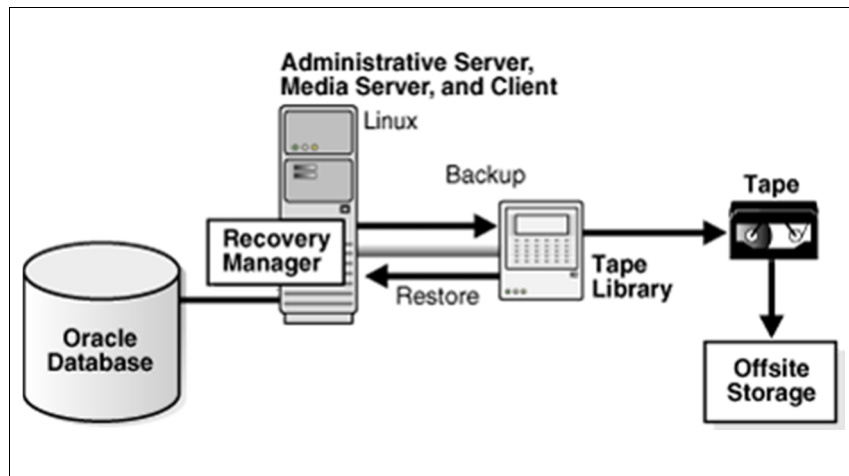


Figura 10 Dominio administrativo con un solo host

4.2 Usuarios, clases y privilegios

Oracle Secure Backup utiliza el servidor de administración para mantener consistente la identidad de los usuarios en el dominio administrativo, en el servidor de administración se almacena información de los usuarios de OSB así como de sus privilegios.

Es importante saber que el espacio de nombres de usuarios OSB es distinto al espacio de nombres de usuarios de Linux, Unix y Windows. Esto quiere decir, que si se inicia sesión en un host del dominio administrativo con el usuario `backup_user` del sistema operativo, y existe un usuario de OSB en el dominio administrativo que se llame `backup_user`, estas cuentas serán manejadas de forma separada aunque tengan el mismo nombre.

En OSB una clase no es más que un conjunto de privilegios asociados a un usuario. Una clase es similar a un grupo de Unix o Linux pero con un poco más de detalle en cuanto a los privilegios de acceso. Como se muestra en la siguiente figura, múltiples usuarios pueden estar asignados a una clase, pero cada usuario solo puede ser miembro de una clase.

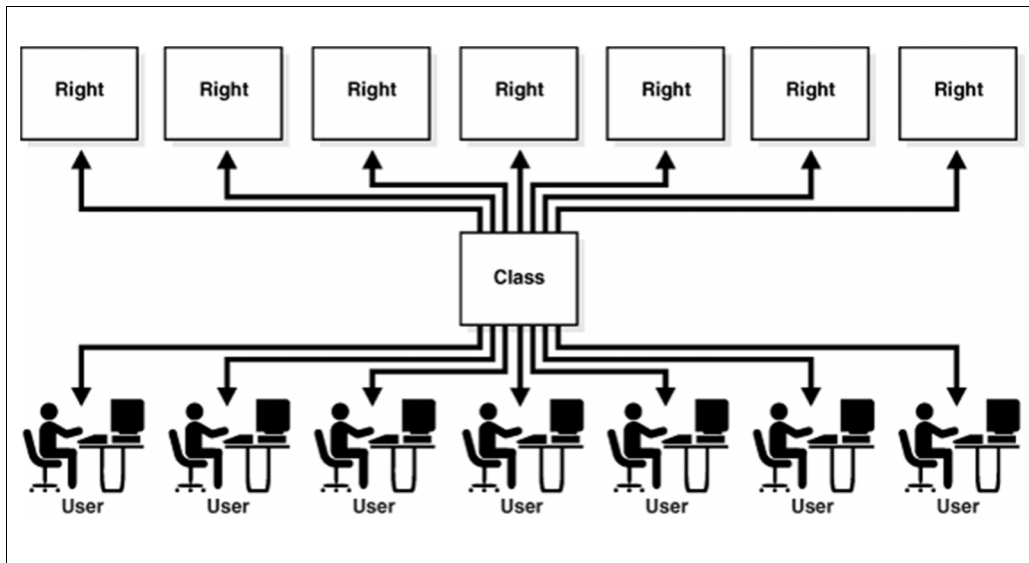


Figura 11 Usuarios, clases y privilegios

Las siguientes clases son clave para entender los privilegios de un usuario de Oracle Secure Backup:

admin: Esta clase es utilizada para la gestión global del dominio administrativo. La clase admin tiene todos los privilegios necesarios para modificar las configuraciones del dominio administrativo y realizar las operaciones de respaldo y restauración.

operator: La clase operador es utilizada para las operaciones normales del día a día, esta clase no tiene privilegios para cambiar la configuración del dominio administrativo, pero tiene todos los permisos para ejecutar las operaciones de respaldo y restauración.

oracle: Esta clase es similar a la clase operator. La clase oracle tiene todos los privilegios necesarios para modificar los parámetros de configuración de la base de datos Oracle y realizar copias de seguridad de la base de datos. Los miembros de la clase son generalmente usuarios OSB que se mapean a las cuentas del sistema operativo donde está instalado el motor de base de datos Oracle.

user: La clase user otorga a los usuarios de OSB permisos para interactuar de forma limitada con su dominio. Esta clase permite a los usuarios navegar por sus propios datos en el catálogo de OSB y permite llevar a cabo restauraciones basadas en el usuario.

reader: Esta clase permite a sus miembros sólo modificar el nombre y la contraseña de su cuenta de usuario y navegar por su propio catálogo. Al crear un usuario en la clase reader, debe asignarse el usuario a un usuario y grupo validos del sistema operativo.

monitor: Los usuarios de esta clase no pueden realizar operaciones de respaldo o restauración, modificaciones al dominio administrativo, o recibir notificaciones por correo electrónico. Esta clase solo permite que los usuarios tengan acceso a los metadatos de las copias de seguridad, ver información acerca de los dispositivos, listar los trabajos ejecutados y ver la configuración del dominio.

4.3 Dispositivos de cinta

Oracle Secure Backup mantiene información de cada unidad de cinta y librería de cintas de modo que estas puedan ser utilizadas para las copias de seguridad y restauraciones tanto locales como en red. Los dispositivos de cinta se pueden configurar durante la instalación de OSB o agregar un nuevo dispositivo de cinta a un dominio administrativo existente. Cuando se configura un dispositivo de cinta, la tarea básica es informar a OSB acerca de la existencia del dispositivo de cinta y luego especificar qué servidor de medios puede comunicarse con este dispositivo de cinta.

4.3.1 Unidades de cinta

Una unidad de cinta es un dispositivo de cinta que utiliza motores controlados de forma precisa para enrollar una cinta de un carrete (bobina) a otro. El funcionamiento básico consiste en pasar por una cabeza de lectura y escritura la cinta magnética mientras se realiza el proceso de bobinado, la mayoría de los sistemas de cinta magnética usan un pequeño carrete fijo dentro de un cartucho para proteger la cinta y hacer el manejo de la misma más fácil. La siguiente imagen muestra los componentes básicos de una unidad de cinta magnética.

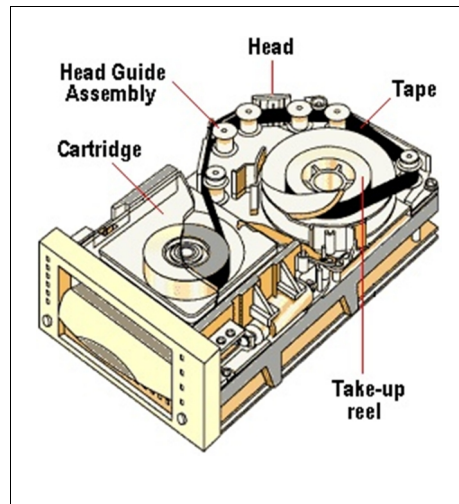


Figura 12 Componentes principales de una unidad de cinta

Un cartucho de cinta magnética es el almacenamiento de acceso secuencial en el que escribe una unidad de cinta. La cinta magnética tiene un comienzo y un final, lo que significa que para acceder a los datos en el centro de la cinta, un dispositivo de cinta debe leer desde el comienzo de la cinta hasta el lugar donde se localizan los datos deseados.

En un formato típico, una unidad de cinta escribe datos en la cinta magnética por bloques, la unidad de cinta escribe cada bloque en una sola operación, dejando espacios entre los bloques. La cinta funciona de manera continua durante la operación de escritura.

4.3.2 Librería de cintas

Una biblioteca de cintas o librería de cintas es un dispositivo de almacenamiento que contiene una o más unidades de cinta, una serie de ranuras (slots) para retener los cartuchos de cinta, un lector de códigos de barras para identificar los cartuchos y un método automatizado para cargar las cintas (un robot). La figura 13 ilustra una librería de cintas que contiene cuatro unidades de cinta.

Oracle Secure Backup automatiza la gestión de librerías de cintas, lo que permite un uso seguro y eficiente de sus capacidades. Controla los robots de la librería de cintas de manera que las cintas pueden ser manejadas fácilmente. OSB es compatible con las siguientes características de las librerías de cintas:

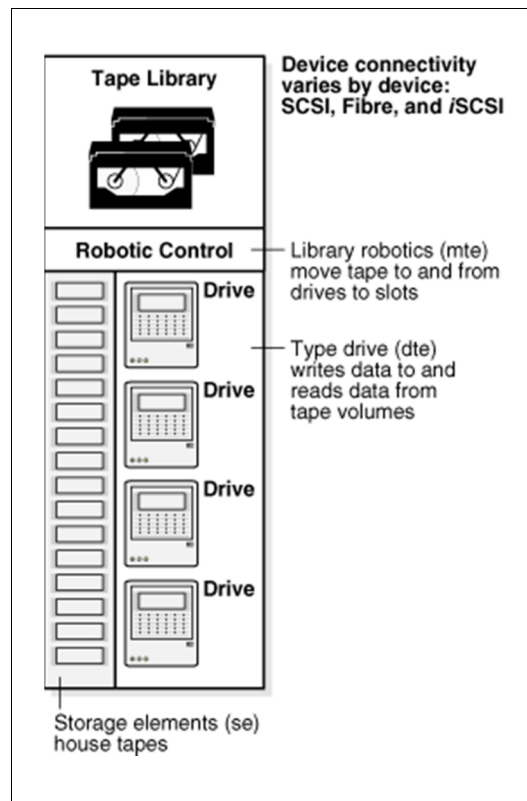


Figura 13 Librería de cintas

- Carga y descarga automática de los volúmenes

Cuando se agrega una librería de cintas a un dominio administrativo, se configura en el modo de montaje automático por defecto. En este modo, Oracle Secure Backup envía comandos al brazo robótico de la librería de cintas para montar o desmontar las cintas que se usarán en las copias de seguridad y restauraciones. Cuando se necesita un nuevo volumen, Oracle Secure Backup busca en la librería de cintas hasta que encuentra el volumen adecuado. Si las cintas necesarias están contenidas en los elementos de almacenamiento de la librería de cintas, entonces no se requiere la intervención del operador para cargar los volúmenes necesarios.

- Lectura de códigos de barras

Un código de barras es un código de símbolos que se aplica físicamente a los volúmenes para fines de identificación. Algunas librerías de cintas tienen un lector de código de barras automatizado. Oracle Secure Backup puede utilizar los códigos de barras para identificar las cintas en una librería de cintas.

- Limpieza automática de la unidad de cinta

Oracle Secure Backup puede comprobar los requisitos de limpieza cuando una cinta es cargada o descargada de una unidad de cinta. Si es necesaria la limpieza, entonces Oracle Secure Backup primero carga un cartucho de limpieza, espera a que el ciclo de limpieza termine, mueve el cartucho de limpieza a su slot de almacenamiento original, y continúa con la carga o descarga de la cinta solicitada.

4.4 Familia de medios

Una familia de medios es una clasificación lógica de volúmenes que comparten atributos comunes. Los volúmenes de una familia comparten un patrón de nomenclatura y políticas utilizadas para escribir y mantener los datos de las copias de seguridad.

Una familia de medios puede tener cualquiera de las siguientes políticas de caducidad de volumen: caducidad gestionada por contenido (por defecto) o caducidad gestionada por tiempo. Los volúmenes que contengan una política de caducidad gestionada por contenido, deberán expirar sólo cuando cada pieza del backup grabado en un volumen sea marcada como eliminada. Los volúmenes con una política de caducidad gestionada por tiempo, expiran cuando sobrepasan la duración expresada por la suma del tiempo de la ventana de escritura (si se especifica), el período de retención, y la hora de creación del volumen.

La única familia de medios que viene configurada por defecto en OSB es “RMAN-DEFAULT”, que es una familia de medios con una política de caducidad gestionada por contenido. Es utilizada sólo para las copias de seguridad de RMAN y no se puede borrar o cambiar el nombre de esta familia de medios, aunque se pueden modificar algunos de sus atributos.

4.5 Selector de almacenamiento de copias de seguridad

Un selector de almacenamiento de copias de seguridad asocia un backup de RMAN con una familia de medios (Media Family) de OSB. Por ejemplo, si se tiene una BD llamada ORCL se puede especificar a RMAN que las copias de seguridad sean almacenadas en una familia de medios previamente creada con el nombre “RMAN-ORCL”. Esto permite la agrupación de las copias de seguridad de una BD y hace que la gestión de los respaldos sea más sencilla para el usuario.

4.6 Interfaces de Oracle Secure Backup

Las siguientes interfaces están disponibles para interactuar y acceder a las funciones de Oracle Secure Backup:

Oracle Secure Backup command-line interface (obtool): Este programa de línea de comandos es la principal interfaz de OSB. Permite realizar las tareas de administración y configuración, así como el manejo de los medios de almacenamiento y las operaciones de respaldo y restauración de los ficheros en los sistemas de archivos.

Oracle Enterprise Manager Database Control and Grid Control: Esta es la interfaz gráfica de usuario (GUI) preferida para manejar OSB. La mayoría de tareas pueden ser realizadas vía OEM.

Oracle Secure Backup Web tool: Es una interfaz grafica basada en web con la que se puede configurar un dominio administrativo, navegar en el catálogo de copias de seguridad, gestionar los datos de restauraciones, y realizar ciertas tareas que no es posible hacer en OEM. La interfaz Web tool expone todas las funciones de obtool.

Recovery Manager command-line interface: La interfaz de línea de comandos de RMAN puede ser usada para configurar e iniciar copias de seguridad y restauraciones de una BD usando OSB. La librería SBT de OSB debe de existir en el host que aloja la base de datos a respaldar para que RMAN pueda hacer respaldos y restauraciones usando OSB.

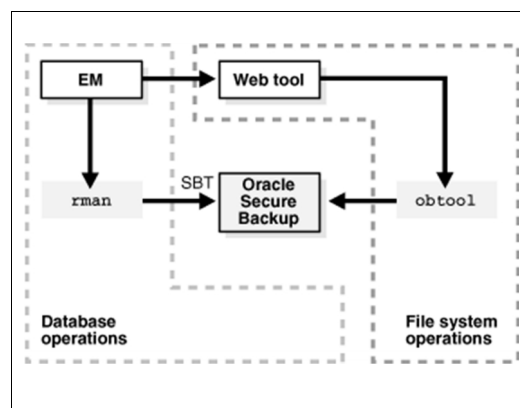


Figura 14 Interfaces de OSB

Capítulo V

Instalación y configuración de software

En el presente capítulo se abordará la instalación y configuración del sistema de protección de datos Oracle Secure Backup, el proceso de instalación se basa en la arquitectura mostrada en la figura 4 del capítulo I, en dicha arquitectura se contaba con un motor de BD Oracle instalado sobre un sistema operativo AIX, por lo tanto, la instalación del sistema operativo y la base de datos no serán tratados en este capítulo. Si se requiere saber más sobre la instalación de dichos componentes, se aconseja consultar la documentación oficial de cada uno de los productos, particularmente, se recomiendan revisar los siguientes documentos:

- *“AIX Version 5.3 Installation and migration”*⁹
- *“Oracle Database Installation Guide 10g Release 2 (10.2) for AIX 5L Based Systems (64-Bit)”*¹⁰

5.1 Instalación de Oracle Secure Backup

Para instalar OSB en el sistema operativo AIX se necesitan al menos 610MB de espacio libre en disco duro, se recomienda una memoria RAM de 4GB y un procesador de dos o más núcleos.

El medio de instalación de OSB puede ser un CD-ROM o un archivo ZIP descargado desde el sitio web de Oracle Technology Network (OTN). El contenido del CD-ROM y el archivo descargado es el mismo.

⁹ http://www-01.ibm.com/support/knowledgecenter/ssw_aix_53/com.ibm.aix.install/doc/insgdrf/insgdrf-kickoff.htm?lang=en

¹⁰ http://docs.oracle.com/cd/B19306_01/install.102/b19075/toc.htm

5.1.1 Copia del software de instalación de OSB

Es necesario hacer la copia del medio de instalación en algún directorio del servidor donde será instalado OSB.

En caso de haber descargado el archivo ZIP desde OTN y almacenarlo en otro equipo que no sea el servidor de instalación, habrá que hacer la transferencia del archivo usando una aplicación para tal fin (FileZilla, WinSCP, etc).

En el caso de la SIIM IFE el software de instalación fue colocado en un directorio que se creó para almacenar temporalmente el software en el servidor de BD Oracle.

```
[root@afisdb ~]# mkdir -p /home/osb-10.4.0.3.0_aix_release
```

5.1.2 Instalación del servidor OSB

Es recomendable crear el siguiente directorio para almacenar los archivos binarios (ejecutables) producto de la instalación de OSB, antes de ejecutar el script de instalación.

```
[root@afisdb ~]# mkdir -p /usr/local/oracle/backup
```

Una vez creado el directorio, ubicarse dentro de él y ejecutar el script de instalación (archivo setup) ubicado en la carpeta donde se copió el software de instalación.

```
[root@afisdb ~]# cd /usr/local/oracle/backup
[root@afisdb backup]# /home/osb-10.4.0.3.0_aix_release/setup

Welcome to Oracle's setup program for Oracle Secure Backup. This
program loads Oracle Secure Backup software from the CD-ROM to a
filesystem directory of your choosing.

This CD-ROM contains Oracle Secure Backup version 10.4.0.3.0_AIX.PPC64.

Please wait a moment while I learn about this host... done.

- - - - -
  1. ibm64 (AIX)
     administrative server, media server, client
- - - - -

Loading Oracle Secure Backup installation tools... done.
```



```
Loading linux86_64 administrative server, media server, client... done.

- - - - -
Loading of Oracle Secure Backup software from CD-ROM is complete.
You may unmount and remove the CD-ROM.

Would you like to continue Oracle Secure Backup installation with
'installob' now? (The Oracle Secure Backup Installation Guide
contains complete information about installob.)
Please answer 'yes' or 'no' [yes]:yes

- - - - -

Welcome to installob, Oracle Secure Backup's installation program.

For most questions, a default answer appears enclosed in square brackets.
Press Enter to select this answer.

Please wait a few seconds while I learn about this machine... done.

Have you already reviewed and customized install/obparameters for your
Oracle Secure Backup installation [yes]? yes

- - - - -

Oracle Secure Backup is not yet installed on this machine.

Oracle Secure Backup's Web server has been loaded, but is not yet configured.

Choose from one of the following options. The option you choose defines
the software components to be installed.

Configuration of this host is required after installation completes.

You can install the software on this host in one of the following ways:
  (a) administrative server, media server and client

  (b) media server and client

  (c) client

If you are not sure which option to choose, please refer to the Oracle
Secure Backup Installation Guide. (a,b or c) [a]? a

Beginning the installation. This will take just a minute and will produce
several lines of informational output.

You must now enter a password for the Oracle Secure Backup encryption
key store. Oracle suggests you choose a password of at least 8
characters in length, containing a mixture of alphabetic and numeric
characters.

Please enter the key store password: password
Re-type password for verification: password

You must now enter a password for the Oracle Secure Backup 'admin' user.
Oracle suggests you choose a password of at least 8 characters in length,
containing a mixture of alphabetic and numeric characters.

Please enter the admin password: password
```

```

Re-type password for verification: password

You should now enter an email address for the Oracle Secure Backup 'admin'
user. Oracle Secure Backup uses this email address to send job summary
reports and to notify the user when a job requires input. If you leave this
blank, you can set it later using the obtool's 'chuser' command.

Please enter the admin email address:

Installing Oracle Secure Backup on afisdb (aix version 5.3)
generating links for client installation updating /etc/ld.so.conf
checking Oracle Secure Backup's configuration file (/etc/obconfig)
setting Oracle Secure Backup directory to /usr/local/oracle/backup in
/etc/obconfig
setting local database directory to /usr/etc/ob in /etc/obconfig
setting temp directory to /usr/tmp in /etc/obconfig
protecting the Oracle Secure Backup directory
creating /etc/rc.d/init.d/observed
activating observed via chkconfig
Starting Oracle Secure Backup service daemon (/etc/observed)

Is afisdb connected to any tape libraries that you'd like to use with
Oracle Secure Backup [no]? no

Is afisdb connected to any tape drives that you'd like to use with
Oracle Secure Backup [no]? no

Installation summary:

  Installation  Host      OS      Driver      OS Move      Reboot
  Mode          Name     Name    Installed?  Required?    Required?

  admin         afisdb   aix     no          no           no

Oracle Secure Backup is now ready for your use.

[root@afisdb backup]#
[root@afisdb backup]#

```

5.2 Configuración de Oracle Secure Backup

Antes de empezar a utilizar OSB junto con RMAN es necesario hacer algunas configuraciones, entre ellas la configuración de los dispositivos de cinta, familia de medios, usuarios, selector de medios de almacenamiento, etc. En las siguientes secciones se mostrarán los comandos necesarios para realizar dichas configuraciones, pero se omitirá la explicación detallada sobre cada uno de sus parámetros. La información sobre los parámetros puede ser consultada en el manual de referencia de OSB (ver bibliografía).

Como ya se mencionó en el capítulo anterior, existen varias interfaces para interactuar con Oracle Secure Backup, por cuestiones de velocidad y espacio, en esta sección solo se

mostrará el uso de la interfaz `obtool`. Aunque todas las configuraciones pueden ser hechas usando Oracle Enterprise Manager o la interfaz Web tool de OSB.

5.2.1 Configuración de usuario

Para poder realizar una copia de seguridad de una BD Oracle usando OSB, primero debe existir un usuario OSB con los permisos adecuados para hacer respaldos a través de RMAN y la utilidad de línea de comandos `obtool`. Por defecto, OSB durante el proceso de instalación crea un usuario llamado “admin”, este usuario tiene todos los privilegios para administrar el dominio de OSB pero carece de autorización para ser usado por RMAN. Para poder autorizar a un usuario el uso de RMAN y la línea de comandos es necesario ejecutar el siguiente comando de OSB.

```
### LOGIN EN obtool USANDO EL USUARIO: admin Y PASSWORD: password

[root@afisdb ~]# obtool -u admin -p password

### AUTORIZAR AL USUARIO admin PARA HACER BACKUP'S CON RMAN

ob> chuser --addpreauth *:*:*+'cmdline'+ 'rman' 'admin'
ob>
```

5.2.2 Configuración de hosts

Durante el proceso de instalación de OSB se configuran los roles que tendrá cada host en el dominio administrativo, en la instalación de OSB que se mostró en la sección anterior (sección 5.1), se configuro el host “afisdb” para que se le asignarán los roles de: servidor de administración, servidor de medios y cliente. Pero también, durante el proceso de instalación no se configuro ningún dispositivo de cinta, por lo que el script de instalación solo asigno los roles de servidor de administración y cliente al host “afisdb”. A causa de esto, habrá que asignar de forma manual el role de servidor de medios al host “afisdb” usando el siguiente comando de OSB:

```
### ASIGNA LOS ROLES: SERVIDOR DE ADMINISTRACIÓN, CLIENTE
### Y SERVIDOR DE MEDIOS AL HOST "afisdb"

ob> chhost --roles 'client','admin','mediaserver' 'afisdb'
ob>
```

5.2.3 Configuración de librería de cintas

Para configurar un dispositivo de cinta en OSB primero es necesario contar con ciertos parámetros SCSI del dispositivo de cinta. Los parámetros necesarios se ilustran en la siguiente figura.

Platform	Linux	HP-UX	AIX
Host bus adapter	x	x	
SCSI bus address	x	x	
SCSI bus name-instance	x	x	x
Target ID	x	x	x
SCSI LUN	x	x	x

Figura 15 Parámetros SCSI requeridos por OSB

Para un sistema AIX estos parámetros pueden ser obtenidos usando la herramienta `obscan` que se puede encontrar en el medio de instalación de OSB, en el directorio `cdtools`.

La herramienta `obscan` determina el parámetro Target ID y LUN de cada dispositivo de cinta conectado al servidor, para usar la herramienta es necesario ejecutarla como usuario “root” del sistema operativo.

```
### /dev/fscsi2 ES EL NOMBRE DEL DISPOSITIVO DE FIBRA CON EL QUE FUE RECONOCIDA
### LA LIBRERÍA DE CINTAS EN EL SISTEMA OPERATIVO (S.O)

[root@afisdb ~]# obscan /dev/fscsi2

obscan version 10.4.0.3 (AIX)
Copyright (c) 1992, 2012, Oracle. All rights reserved.

DEVICE information for /dev/fscsi2

Target-id : 2, Lun : 0
  Vendor : IBM   Product : 3573-TL   World Wide Name : 1008023045576729

Target-id : 2, Lun : 1
  Vendor : IBM   Product : ULT3580-TD5   World Wide Name : 1008023045576729

Target-id : 2, Lun : 2
  Vendor : IBM   Product : ULT3580-TD5   World Wide Name : 1008023045576729

Total count of Media Changers and/or Tape devices found : 3
```

En este caso, se encontró conectada la librería de cintas IBM TS3100 con dos unidades de cinta (drives). Una vez que se tienen los datos anteriores, es necesario crear los dispositivos en el sistema operativo que posteriormente serán adjuntados/asociados a los dispositivos creados en OSB. Para crear un dispositivo del tipo librería en el sistema operativo, es necesario ejecutar el comando `makedev` que se encuentra en el directorio: `/usr/local/oracle/backup/install` producido durante la instalación de OSB.

```
[root@afisdb install]# makedev

### ESPECIFICAR EL NÚMERO DEL DISPOSITIVO QUE SE CREARÁ EN EL S.O, EN ESTE
### EJEMPLO SE CREARÁ EL DISPOSITIVO /dev/obl0

Enter logical unit number 0-31 [0]: 0

### ESPECIFICAR EL TIPO DE DISPOSITIVO QUE SE CREARÁ

Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
tape library [d]: l

### NOMBRE DEL DISPOSITIVO CON EL QUE FUE RECONOCIDA LA LIBRERÍA EN EL S.O

Enter SCSI bus name: fscsi2

### TARGET ID DE LA LIBRERÍA DE CINTAS (obtenido con obscan)

Enter SCSI target id 0-16777215: 2

### NÚMERO DE LUN DE LA LIBRERÍA DE CINTAS (obtenido con obscan)

Enter SCSI logical unit number (lun) 0-7 [0]: 0
/dev/obl0 created
```

Para crear los dispositivos de tipo unidad de cinta, ejecutar el comando `makedev` pero al momento de especificar el tipo de dispositivo teclear la letra “d”, que indica que el dispositivo a crear es una unidad de cinta (drive tape).

```
### CREACIÓN DEL DRIVE TAPE 0

[root@afisdb install]# makedev

Enter logical unit number 0-31 [0]: 0
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
tape library [d]: d
Enter SCSI bus name: fscsi2
Enter SCSI target id 0-16777215: 2
Enter SCSI logical unit number (lun) 0-7 [0]: 1
/dev/obt0 created
```

```
### CREACIÓN DEL DRIVE TAPE 1

[root@afisdb install]# makedev

Enter logical unit number 0-31 [0]: 1
Enter 'd' if this device is a tape drive or 'l' if a SCSI-2 addressable
  tape library [d]: d
Enter SCSI bus name: fscsi2
Enter SCSI target id 0-16777215: 2
Enter SCSI logical unit number (lun) 0-7 [0]: 2
/dev/obt1 created
```

Después de haber ejecutado los comandos anteriores, se habrán creado los siguientes dispositivos en directorio /dev del sistema operativo.

```
[root@afisdb]# ls -l /dev/ob*

crw-rw-rw- 1 root sys 0, 0 Jun 15 15:30 /dev/obl0
crw-rw-rw- 1 root sys 0, 0 Jun 15 15:40 /dev/obt0
crw-rw-rw- 1 root sys 0, 0 Jun 15 15:55 /dev/obt1

[root@afisdb]#
```

Los dispositivos creados sirven como puntos de asociación y están ligados al dispositivo de cinta físico. Una vez creados los puntos de asociación, se tendrán que crear los dispositivos lógicos en OSB, que posteriormente serán asociados/adjuntados a los dispositivos del sistema operativo previamente creados.

Los comandos para crear los dispositivos lógicos en OSB y crear la asociación son los siguientes:

```
### CREACIÓN DE LA LIBRERÍA "LIBRARY0" EN OSB

ob> mkdev --type 'library' --inservice' --debug 'yes' --barcodereader 'yes' --
unloadrequired 'yes' --ejection 'auto' 'LIBRARY0'

### ADJUNTA O ASOCIA EL DISPOSITIVO /dev/obl0 (medium changer)
### A LA LIBRERÍA "LIBRARY0" PREVIAMENTE CREADA

ob> chdev --addattach 'afisdb': '/dev/obl0' 'LIBRARY0'
```

```

### CREA LA UNIDAD DE CINTA "DRIVE0" Y LA LIGA A LA LIBRERÍA "LIBRARY0"
### PREVIAMENTE CREADA EN OSB

ob> mkdev --type 'tape' --'inservice' --debug 'yes' --library 'LIBRARY0' --
erate '8' --dte '1' --uselist all --automount 'yes' 'DRIVE0'

### ADJUNTA O ASOCIA EL DISPOSITIVO /dev/obt0 (drive tape0)
### A LA UNIDAD DE CINTA "DRIVE0"

ob> chdev --addattach 'afisdb': '/dev/obt0' 'DRIVE0'

### CREA LA UNIDAD DE CINTA "DRIVE1" Y LA LIGA A LA LIBRERÍA "LIBRARY0"
### PREVIAMENTE CREADA EN OSB

ob> mkdev --type 'tape' --'inservice' --debug 'yes' --library 'LIBRARY0' --
erate '8' --dte '2' --uselist all --automount 'yes' 'DRIVE1'

### ADJUNTA O ASOCIA EL DISPOSITIVO /dev/obt1 (drive tapel)
### A LA UNIDAD DE CINTA "DRIVE1"

ob> chdev --addattach 'afisdb': '/dev/obt1' 'DRIVE1'
ob>

```

Finalmente, para comprobar que la librería de cintas y sus unidades de cinta correspondientes fueron creadas en Oracle Secure Backup, ejecutar el siguiente comando que deberá mostrar los dispositivos creados en OSB.

```

ob> lsdev
library          LIBRARY0          in service
drive 1          DRIVE0            in service
drive 2          DRIVE1            in service

```

5.2.4 Configuración de familia de medios

Por defecto la instalación de OSB crea un Media Family (Familia de Medios) para los respaldos hechos por RMAN, el nombre de este Media Family es "RMAN-DEFAULT" y tiene ciertas políticas de caducidad que podrían no ser útiles para todos los respaldos. Si en RMAN no se especifica el Media Family que se usará al momento de hacer el respaldo, entonces OSB automáticamente asigna el Media Family "RMAN-DEFAULT" a la copia de seguridad.

En la instalación de OSB de la SIIM IFE se creó el Media Family “MF_ORARW2”, que es utilizado por RMAN para hacer las copias de seguridad de la base de datos. Este Media Family tiene asignada una política de caducidad gestionada por contenido y una ventana de escritura de 1 mes.

```
ob> mkmf --vidunique --writewindow '1months' --contentmanaged --append  
'MF_ORARW2'
```

5.2.5 Configuración del selector de almacenamiento

La creación de un selector de almacenamiento de copias de seguridad, se realiza con la finalidad de que OSB lo utilice para asociar una copia de seguridad ejecutada por RMAN con un Media Family de OSB. Esto evita que cada vez que se ejecute una copia de seguridad de la BD, en RMAN se tenga que especificar el Media Family en el que será almacenada la copia de seguridad.

En la implementación de OSB de la SIIM IFE se creó el selector de almacenamiento “BS-RMAN-AFIS” que asocia y agrupa los respaldos de la BD Oracle bajo el Media Family “MF_ORARW2”. El comando usado para crear un selector de almacenamiento de copias de seguridad es el siguiente:

```
ob> mkssel --content '*' --dbname '*' --dbid '*' --host 'afisdb' -f 'MF_ORARW2'  
--copynum '*' --encryption 'off' --waittime forever 'BS-RMAN-AFIS'
```

5.2.6 Inventario de cintas magnéticas

El último paso a realizar para que OSB quede configurado completamente, es introducir los cartuchos de cinta en la librería IBM TS3100 y realizar un inventario para que OSB pueda determinar el número y tipo de volúmenes con los que cuenta. Un inventario en la librería de cintas se puede hacer usando el siguiente comando de OSB.

```
ob> inventory -L LIBRARY0 -f
```


5.3 Configuración de RMAN

Después de haber terminado la configuración de OSB es posible hacer copias de seguridad de la BD Oracle usando RMAN, pero hay que tener en cuenta que las copias de seguridad se realizarán usando los parámetros por defecto de RMAN. Si dichos parámetros no cumplen con las políticas de respaldo de la empresa u organización, será necesario configurar los parámetros de acuerdo a las necesidades.

En esta sección se mostrará la configuración de RMAN utilizada en la SIIM IFE y únicamente se entrará a detalle en aquellos parámetros cuya configuración fue cambiada.

Para cambiar la configuración de un parámetro de RMAN se utiliza el comando `configure` y para mostrar la configuración de todos los parámetros el comando `show all`.

```
/* CONFIGURACIÓN (PARÁMETROS) POR DEFECTO DE RMAN */  
  
RMAN> show all;  
  
RMAN configuration parameters are:  
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default  
CONFIGURE BACKUP OPTIMIZATION OFF; # default  
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default  
CONFIGURE CONTROLFILE AUTOBACKUP OFF; # default  
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default  
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default  
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default  
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default  
CONFIGURE MAXSETSIZE TO UNLIMITED; # default  
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default  
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default  
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default  
CONFIGURE SNAPSHOT CONTROLFILE NAME TO  
'/u01/app/oracle/product/10.2.0/db_1/dbs/snapcf_AFIS.f'; # default  
  
RMAN>
```

Cada uno de los parámetros anteriores tiene una función específica, si se quiere saber para qué sirve cada uno de los parámetros, lo más conveniente es consultar la siguiente documentación oficial de Oracle.

“Oracle Database Backup and Recovery Basics 10g Release 2 (10.2)”

“Oracle Database Backup and Recovery Advanced User's Guide 10g Release 2 (10.2)”

“Oracle Database Backup and Recovery Quick Start Guide 10g Release 2 (10.2)”

Los parámetros modificados en la implementación de RMAN de la SIIM IFE son los que a continuación se listan:

RETENTION POLICY: Este parámetro se utiliza para controlar el tiempo que RMAN mantendrá las copias de seguridad antes de ser consideradas obsoletas. El parámetro puede ser configurado por el "número" de copias de seguridad realizadas, o por un número de "días" a mantener una copia de seguridad.

- Por número de copias: RMAN deberá mantener n número de copias de seguridad y las restantes considerarlas obsoletas (empezando por la más antigua). En otras palabras, si el número de copias de seguridad excede el valor de n , las copias restantes serán consideradas obsoletas empezando por la más antigua. Para configurar una política de retención basada en el número de copias se usa el siguiente comando.

```
CONFIGURE RETENTION POLICY TO REDUNDANCY 1;
```

- Por número de días de retención: Oracle debe mantener n días una copia de seguridad antes de ser considerada obsoleta. Las copias de seguridad que no superan el valor de n contando a partir del momento que fueron creadas, son consideradas vigentes, y las copias que superan el valor de n son consideradas obsoletas. Para configurar una política de retención basada en el número de días se utiliza el comando:

```
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 7 DAYS;
```

La configuración de RMAN de la SIIM IFE tiene una política de retención basa en el número de días, se establecieron 14 días como el periodo de retención de las copias de seguridad.

```
RMAN> CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 14 DAYS;
```

```
new RMAN configuration parameters:  
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 14 DAYS;  
new RMAN configuration parameters are successfully stored
```

DEFAULT DEVICE TYPE: Configura el tipo de dispositivo por defecto que será usado para las operaciones de respaldo y restauración. Por defecto, RMAN envía todas las copias de seguridad a un directorio específico del sistema operativo en el disco duro. El parámetro `DEFAULT DEVICE TYPE` puede ser utilizado para indicar a RMAN cuál será el tipo de dispositivo que se usará por defecto para las copias de seguridad: cinta magnética o disco duro (`SBT_TAPE` o `DISK`).

Si se establece `SBT_TAPE` como dispositivo por defecto, se habilitan algunos otros parámetros que deberán cambiarse solo si las políticas de respaldo de la organización lo requieren, de otra manera se recomienda dejar los valores asignados de forma automática.

```
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F';
CONFIGURE DEVICE TYPE SBT_TAPE PARALLELISM 1 BACKUP TYPE TO BACKUPSET;
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
```

En la configuración de la SIIM IFE, se estableció la cinta magnética como el dispositivo por defecto para las operaciones de respaldo y restauración de la BD Oracle.

```
RMAN> CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';

new RMAN configuration parameters:
CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
new RMAN configuration parameters are successfully stored
```

CONTROLFILE AUTOBACKUP: Permite respaldar de forma automática los archivos de control (control files) y el archivo de parámetros (spfile) de la BD al término de cada copia de seguridad. Los posibles valores que puede tomar son `ON` y `OFF`, si está activado se realizará la copia de los archivos de control y del archivo de parámetros, de lo contrario, se omitirá la copia de los archivos. En la configuración de la SIIM IFE el parámetro se encuentra activado.

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;

new RMAN configuration parameters:
CONFIGURE CONTROLFILE AUTOBACKUP ON;
new RMAN configuration parameters are successfully stored
```

DEVICE TYPE PARALLELISM: En realidad este parámetro solo se llama `DEVICE TYPE`, se utiliza para establecer el número de canales que RMAN utilizará para realizar un trabajo de copia de seguridad o restauración, incrementar el grado de paralelismo puede ayudar debido a que incrementa el número de canales usados para las operaciones de lectura y escritura.

El grado de paralelismo en la SIIM IFE está establecido a 2, lo que implica que cada vez que se ejecute una copia de seguridad se abrirán dos canales hacia el servidor de base de datos para hacer el respaldo.

```
RMAN> CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 2 BACKUP TYPE TO BACKUPSET;

new RMAN configuration parameters:
CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 2 BACKUP TYPE TO BACKUPSET;
new RMAN configuration parameters are successfully stored
```

Finalmente, se muestra la configuración de RMAN una vez hecha la modificación de los parámetros anteriormente mencionados. Con esto, RMAN y OSB se encuentran completamente configurados para ejecutar las copias de seguridad de la BD Oracle.

```
RMAN> show all;

RMAN configuration parameters are:
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 14 DAYS;
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F'; #
default
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default
CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 2 BACKUP TYPE TO BACKUPSET;
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO
'/u01/app/oracle/product/10.2.0/db_1/dbs/snapcf_AFIS.f'; # default
```

Capítulo VI

Resultados (Casos de prueba)

En este capítulo se expondrá el mecanismo de respaldo utilizado en la base de datos de la SIIM IFE, así como algunos mecanismos de validación de las copias de seguridad realizadas.

6.1 Ejecución de un backup completo de la BD

Básicamente un backup completo consiste en respaldar los archivos de datos (datafiles), los archivos de control (control files), los ficheros redo log archivados (archived redo logs) y el archivo de parámetros (spfile o init.ora) de la BD. Existen sentencias en RMAN que permiten hacer el respaldo de cada uno de los archivos mencionados, pero en esta sección se usará la configuración de RMAN previamente mostrada en el capítulo anterior. Entonces, para hacer un backup completo de la BD solo será necesario ejecutar la siguiente sentencia que se encarga de respaldar todos los datafiles y archived redo logs. Los archivos de control y el spfile se respaldan de manera automática al estar activado el parámetro `CONTROLFILE AUTOBACKUP` de RMAN.

```
RMAN> backup database plus archivelog;
```

Es importante que después de respaldar los archivos archived redo logs, estos sean eliminados, debido a que podrían saturar el espacio en disco duro si no se depuran de forma constante. Para que RMAN elimine los archivos archived redo logs de forma automática una vez que estos sean respaldados, se puede agregar al final de la sentencia anterior el comando `delete all input`.

```
RMAN> backup database plus archivelog delete all input;
```

Utilizando esta sentencia, se muestra a continuación un ejemplo de cómo se realiza un backup completo de la BD Oracle de la SIIM IFE, que emplea la configuración de RMAN y OSB expuesta en el capítulo V.

```
RMAN> backup database plus archivelog delete all input;

Starting backup at 22-JUN-13
current log archived
released channel: ORA_DISK_1
using channel ORA_SBT_TAPE_1
using channel ORA_SBT_TAPE_2
channel ORA_SBT_TAPE_1: starting archive log backupset
channel ORA_SBT_TAPE_1: specifying archive log(s) in backup set
input archive log thread=1 sequence=41 recid=1 stamp=858801798
input archive log thread=1 sequence=42 recid=2 stamp=730245503
input archive log thread=1 sequence=43 recid=3 stamp=730245696
input archive log thread=1 sequence=44 recid=4 stamp=730245726
input archive log thread=1 sequence=45 recid=5 stamp=818177413
input archive log thread=1 sequence=46 recid=6 stamp=818178523
input archive log thread=1 sequence=47 recid=7 stamp=818180066
input archive log thread=1 sequence=48 recid=8 stamp=818180615
input archive log thread=1 sequence=49 recid=9 stamp=818180847
input archive log thread=1 sequence=50 recid=10 stamp=818181332
input archive log thread=1 sequence=51 recid=11 stamp=818181728
input archive log thread=1 sequence=52 recid=12 stamp=818182341
input archive log thread=1 sequence=53 recid=13 stamp=818183669
input archive log thread=1 sequence=54 recid=14 stamp=818183701
input archive log thread=1 sequence=55 recid=15 stamp=818183761
input archive log thread=1 sequence=56 recid=16 stamp=818183763
input archive log thread=1 sequence=57 recid=17 stamp=818183764
input archive log thread=1 sequence=58 recid=18 stamp=818183765
input archive log thread=1 sequence=59 recid=19 stamp=818175137
input archive log thread=1 sequence=60 recid=20 stamp=818198734
input archive log thread=1 sequence=61 recid=21 stamp=818202376
input archive log thread=1 sequence=62 recid=22 stamp=858952186
input archive log thread=1 sequence=63 recid=23 stamp=859334786
input archive log thread=1 sequence=64 recid=24 stamp=859334823
input archive log thread=1 sequence=65 recid=25 stamp=859334875
input archive log thread=1 sequence=66 recid=26 stamp=859334903
input archive log thread=1 sequence=67 recid=27 stamp=859334933
input archive log thread=1 sequence=68 recid=28 stamp=859334962
input archive log thread=1 sequence=69 recid=29 stamp=859334980
input archive log thread=1 sequence=70 recid=30 stamp=859335017
channel ORA_SBT_TAPE_1: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_2: starting archive log backupset
channel ORA_SBT_TAPE_2: specifying archive log(s) in backup set
input archive log thread=1 sequence=71 recid=31 stamp=859335067
input archive log thread=1 sequence=72 recid=32 stamp=859335118
input archive log thread=1 sequence=73 recid=33 stamp=859335480
input archive log thread=1 sequence=74 recid=34 stamp=859339995
input archive log thread=1 sequence=75 recid=35 stamp=859384851
```

```

input archive log thread=1 sequence=76 recid=36 stamp=859399227
input archive log thread=1 sequence=77 recid=37 stamp=859408554
input archive log thread=1 sequence=78 recid=38 stamp=859413015
input archive log thread=1 sequence=79 recid=39 stamp=859413848
input archive log thread=1 sequence=80 recid=40 stamp=859414511
input archive log thread=1 sequence=81 recid=41 stamp=859414763
input archive log thread=1 sequence=82 recid=42 stamp=859415500
input archive log thread=1 sequence=83 recid=43 stamp=859415910
input archive log thread=1 sequence=84 recid=44 stamp=859416388
input archive log thread=1 sequence=85 recid=45 stamp=859418233
input archive log thread=1 sequence=86 recid=46 stamp=859418855
input archive log thread=1 sequence=87 recid=47 stamp=859420408
input archive log thread=1 sequence=88 recid=48 stamp=859420534
input archive log thread=1 sequence=89 recid=49 stamp=859420685
input archive log thread=1 sequence=90 recid=50 stamp=859420954
input archive log thread=1 sequence=91 recid=51 stamp=859421102
input archive log thread=1 sequence=92 recid=52 stamp=859421544
input archive log thread=1 sequence=93 recid=53 stamp=859422163
input archive log thread=1 sequence=94 recid=54 stamp=859422326
input archive log thread=1 sequence=95 recid=55 stamp=859422547
input archive log thread=1 sequence=96 recid=56 stamp=859423104
input archive log thread=1 sequence=97 recid=57 stamp=859423529
input archive log thread=1 sequence=98 recid=58 stamp=859424181
input archive log thread=1 sequence=99 recid=59 stamp=818786821
input archive log thread=1 sequence=100 recid=60 stamp=818787172
channel ORA_SBT_TAPE_2: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_1: finished piece 1 at 22-JUN-13
piece handle=83ocr6_1_1 tag=TAG20130622T164252 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:05:17
channel ORA_SBT_TAPE_1: deleting archive log(s)
archive log filename=/oradata/AFIS/arch1/1_41_858796023.arc recid=1
stamp=858801798
archive log filename=/oradata/AFIS/arch1/1_42_858796023.arc recid=2
stamp=730245503
archive log filename=/oradata/AFIS/arch1/1_43_858796023.arc recid=3
stamp=730245696
...
.
archive log filename=/oradata/AFIS/arch1/1_98_858796023.arc recid=58
stamp=859424181
archive log filename=/oradata/AFIS/arch1/1_99_858796023.arc recid=59
stamp=818786821
archive log filename=/oradata/AFIS/arch1/1_100_858796023.arc recid=60
stamp=818787172
Finished backup at 22-JUN-13

Starting backup at 22-JUN-13
using channel ORA_SBT_TAPE_1
using channel ORA_SBT_TAPE_2
channel ORA_SBT_TAPE_1: starting full datafile backupset
channel ORA_SBT_TAPE_1: specifying datafile(s) in backupset
input datafile fno=00001 name=/oradata/AFIS/system01.dbf
input datafile fno=00687 name=/oradata/AFIS/bin3_a/AFIS_bin3_1.dbf
input datafile fno=00689 name=/oradata/AFIS/bin3_a/AFIS_bin3_3.dbf
input datafile fno=00691 name=/oradata/AFIS/bin3_a/AFIS_bin3_5.dbf
input datafile fno=00693 name=/oradata/AFIS/bin3_a/AFIS_bin3_7.dbf
input datafile fno=00695 name=/oradata/AFIS/bin3_a/AFIS_bin3_9.dbf
input datafile fno=00697 name=/oradata/AFIS/bin3_a/AFIS_bin3_11.dbf

```

input datafile fno=00699 name=/oradata/AFIS/bin3_a/AFIS_bin3_13.dbf
input datafile fno=00701 name=/oradata/AFIS/bin3_a/AFIS_bin3_15.dbf
input datafile fno=00703 name=/oradata/AFIS/bin3_a/AFIS_bin3_17.dbf
input datafile fno=00705 name=/oradata/AFIS/bin3_a/AFIS_bin3_19.dbf
input datafile fno=00707 name=/oradata/AFIS/bin3_a/AFIS_bin3_21.dbf
input datafile fno=00709 name=/oradata/AFIS/bin3_a/AFIS_bin3_23.dbf
input datafile fno=00711 name=/oradata/AFIS/bin3_a/AFIS_bin3_25.dbf
input datafile fno=00713 name=/oradata/AFIS/bin3_a/AFIS_bin3_27.dbf
input datafile fno=00715 name=/oradata/AFIS/bin3_a/AFIS_bin3_29.dbf
input datafile fno=00717 name=/oradata/AFIS/bin3_a/AFIS_bin3_31.dbf
input datafile fno=00719 name=/oradata/AFIS/bin2_a/AFIS_bin2_1.dbf
input datafile fno=00721 name=/oradata/AFIS/bin2_a/AFIS_bin2_3.dbf
input datafile fno=00723 name=/oradata/AFIS/bin2_a/AFIS_bin2_5.dbf
input datafile fno=00725 name=/oradata/AFIS/bin2_a/AFIS_bin2_7.dbf
input datafile fno=00727 name=/oradata/AFIS/bin2_a/AFIS_bin2_9.dbf
input datafile fno=00729 name=/oradata/AFIS/bin2_a/AFIS_bin2_11.dbf
input datafile fno=00731 name=/oradata/AFIS/bin2_a/AFIS_bin2_13.dbf
input datafile fno=00733 name=/oradata/AFIS/bin2_a/AFIS_bin2_15.dbf
input datafile fno=00735 name=/oradata/AFIS/bin2_a/AFIS_bin2_17.dbf
input datafile fno=00737 name=/oradata/AFIS/bin2_a/AFIS_bin2_19.dbf
input datafile fno=00739 name=/oradata/AFIS/bin2_a/AFIS_bin2_21.dbf
input datafile fno=00741 name=/oradata/AFIS/bin2_a/AFIS_bin2_23.dbf
input datafile fno=00743 name=/oradata/AFIS/bin2_a/AFIS_bin2_25.dbf
input datafile fno=00745 name=/oradata/AFIS/bin2_a/AFIS_bin2_27.dbf
input datafile fno=00747 name=/oradata/AFIS/bin2_a/AFIS_bin2_29.dbf
input datafile fno=00749 name=/oradata/AFIS/bin2_a/AFIS_bin2_31.dbf
input datafile fno=00751 name=/oradata/AFIS/bin2_a/AFIS_bin2_33.dbf
input datafile fno=00753
name=/oradata/AFIS/MBS/idxalphabin/MBS_idx_alphabinary_1.dbf
input datafile fno=00755
name=/oradata/AFIS/MBS/idxalphabin/MBS_idx_alphabinary_3.dbf
input datafile fno=00757
name=/oradata/AFIS/MBS/idxalphabin/MBS_idx_alphabinary_5.dbf
input datafile fno=00759 name=/oradata/AFIS/MBS/idx/MBS_idx_2.dbf
input datafile fno=00761 name=/oradata/AFIS/MBS/idx/MBS_idx_4.dbf
input datafile fno=00763 name=/oradata/AFIS/MBS/idx/MBS_idx_6.dbf
input datafile fno=00765 name=/oradata/AFIS/MBS/idx/MBS_idx_8.dbf
input datafile fno=00767 name=/oradata/AFIS/MBS/idx/MBS_idx_10.dbf
input datafile fno=00769 name=/oradata/AFIS/MBS/idx/MBS_idx_12.dbf
input datafile fno=00771 name=/oradata/AFIS/MBS/data/MBS_data_2.dbf
input datafile fno=00773 name=/oradata/AFIS/MBS/data/MBS_data_4.dbf
input datafile fno=00775 name=/oradata/AFIS/MBS/data/MBS_data_6.dbf
input datafile fno=00777 name=/oradata/AFIS/MBS/data/MBS_data_8.dbf
input datafile fno=00779 name=/oradata/AFIS/MBS/data/MBS_data_10.dbf
input datafile fno=00781 name=/oradata/AFIS/MBS/data/MBS_data_12.dbf
input datafile fno=00783 name=/oradata/AFIS/MBS/data/MBS_data_14.dbf
input datafile fno=00785 name=/oradata/AFIS/MBS/data/MBS_data_16.dbf
channel ORA_SBT_TAPE_1: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_2: starting full datafile backupset
channel ORA_SBT_TAPE_2: specifying datafile(s) in backupset
input datafile fno=00003 name=/oradata/AFIS/sysaux01.dbf
input datafile fno=00688 name=/oradata/AFIS/bin3_b/AFIS_bin3_2.dbf
input datafile fno=00690 name=/oradata/AFIS/bin3_b/AFIS_bin3_4.dbf
input datafile fno=00692 name=/oradata/AFIS/bin3_b/AFIS_bin3_6.dbf
input datafile fno=00694 name=/oradata/AFIS/bin3_b/AFIS_bin3_8.dbf
input datafile fno=00696 name=/oradata/AFIS/bin3_b/AFIS_bin3_10.dbf
input datafile fno=00698 name=/oradata/AFIS/bin3_b/AFIS_bin3_12.dbf
input datafile fno=00700 name=/oradata/AFIS/bin3_b/AFIS_bin3_14.dbf
input datafile fno=00702 name=/oradata/AFIS/bin3_b/AFIS_bin3_16.dbf
input datafile fno=00704 name=/oradata/AFIS/bin3_b/AFIS_bin3_18.dbf


```

input datafile fno=00706 name=/oradata/AFIS/bin3_b/AFIS_bin3_20.dbf
input datafile fno=00708 name=/oradata/AFIS/bin3_b/AFIS_bin3_22.dbf
input datafile fno=00710 name=/oradata/AFIS/bin3_b/AFIS_bin3_24.dbf
input datafile fno=00712 name=/oradata/AFIS/bin3_b/AFIS_bin3_26.dbf
input datafile fno=00714 name=/oradata/AFIS/bin3_b/AFIS_bin3_28.dbf
input datafile fno=00716 name=/oradata/AFIS/bin3_b/AFIS_bin3_30.dbf
input datafile fno=00718 name=/oradata/AFIS/bin3_b/AFIS_bin3_32.dbf
input datafile fno=00720 name=/oradata/AFIS/bin2_b/AFIS_bin2_2.dbf
input datafile fno=00722 name=/oradata/AFIS/bin2_b/AFIS_bin2_4.dbf
input datafile fno=00724 name=/oradata/AFIS/bin2_b/AFIS_bin2_6.dbf
input datafile fno=00726 name=/oradata/AFIS/bin2_b/AFIS_bin2_8.dbf
input datafile fno=00728 name=/oradata/AFIS/bin2_b/AFIS_bin2_10.dbf
input datafile fno=00730 name=/oradata/AFIS/bin2_b/AFIS_bin2_12.dbf
input datafile fno=00732 name=/oradata/AFIS/bin2_b/AFIS_bin2_14.dbf
input datafile fno=00734 name=/oradata/AFIS/bin2_b/AFIS_bin2_16.dbf
input datafile fno=00736 name=/oradata/AFIS/bin2_b/AFIS_bin2_18.dbf
input datafile fno=00738 name=/oradata/AFIS/bin2_b/AFIS_bin2_20.dbf
input datafile fno=00740 name=/oradata/AFIS/bin2_b/AFIS_bin2_22.dbf
input datafile fno=00742 name=/oradata/AFIS/bin2_b/AFIS_bin2_24.dbf
input datafile fno=00744 name=/oradata/AFIS/bin2_b/AFIS_bin2_26.dbf
input datafile fno=00746 name=/oradata/AFIS/bin2_b/AFIS_bin2_28.dbf
input datafile fno=00748 name=/oradata/AFIS/bin2_b/AFIS_bin2_30.dbf
input datafile fno=00750 name=/oradata/AFIS/bin2_b/AFIS_bin2_32.dbf
input datafile fno=00752 name=/oradata/AFIS/bin2_b/AFIS_bin2_34.dbf
input datafile fno=00754
name=/oradata/AFIS/MBS/idxalphabin/MBS_idx_alphabinary_2.dbf
input datafile fno=00756
name=/oradata/AFIS/MBS/idxalphabin/MBS_idx_alphabinary_4.dbf
input datafile fno=00758 name=/oradata/AFIS/MBS/idx/MBS_idx_1.dbf
input datafile fno=00760 name=/oradata/AFIS/MBS/idx/MBS_idx_3.dbf
input datafile fno=00762 name=/oradata/AFIS/MBS/idx/MBS_idx_5.dbf
input datafile fno=00764 name=/oradata/AFIS/MBS/idx/MBS_idx_7.dbf
input datafile fno=00766 name=/oradata/AFIS/MBS/idx/MBS_idx_9.dbf
input datafile fno=00768 name=/oradata/AFIS/MBS/idx/MBS_idx_11.dbf
input datafile fno=00770 name=/oradata/AFIS/MBS/data/MBS_data_1.dbf
input datafile fno=00772 name=/oradata/AFIS/MBS/data/MBS_data_3.dbf
input datafile fno=00774 name=/oradata/AFIS/MBS/data/MBS_data_5.dbf
input datafile fno=00776 name=/oradata/AFIS/MBS/data/MBS_data_7.dbf
input datafile fno=00778 name=/oradata/AFIS/MBS/data/MBS_data_9.dbf
input datafile fno=00780 name=/oradata/AFIS/MBS/data/MBS_data_11.dbf
input datafile fno=00782 name=/oradata/AFIS/MBS/data/MBS_data_13.dbf
input datafile fno=00784 name=/oradata/AFIS/MBS/data/MBS_data_15.dbf
channel ORA_SBT_TAPE_2: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_2: finished piece 1 at 22-JUN-13
piece handle=86ocrctu_1_1 tag=TAG20130622T165415 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_2: backup set complete, elapsed time: 00:19:27
channel ORA_SBT_TAPE_2: starting full datafile backupset
channel ORA_SBT_TAPE_2: specifying datafile(s) in backupset
input datafile fno=00002 name=/oradata/AFIS/undotbs01.dbf
input datafile fno=00624 name=/oradata/AFIS/bin5_b/AFIS_bin5_2.dbf
input datafile fno=00625 name=/oradata/AFIS/bin5_a/AFIS_bin5_3.dbf
input datafile fno=00626 name=/oradata/AFIS/bin5_b/AFIS_bin5_4.dbf
input datafile fno=00627 name=/oradata/AFIS/bin5_a/AFIS_bin5_5.dbf
input datafile fno=00628 name=/oradata/AFIS/bin5_b/AFIS_bin5_6.dbf
input datafile fno=00629 name=/oradata/AFIS/bin5_a/AFIS_bin5_7.dbf
input datafile fno=00630 name=/oradata/AFIS/bin5_b/AFIS_bin5_8.dbf
input datafile fno=00631 name=/oradata/AFIS/bin5_a/AFIS_bin5_9.dbf
input datafile fno=00632 name=/oradata/AFIS/bin5_b/AFIS_bin5_10.dbf
input datafile fno=00633 name=/oradata/AFIS/bin5_a/AFIS_bin5_11.dbf

```

```
input datafile fno=00634 name=/oradata/AFIS/bin5_b/AFIS_bin5_12.dbf
input datafile fno=00635 name=/oradata/AFIS/bin5_a/AFIS_bin5_13.dbf
input datafile fno=00636 name=/oradata/AFIS/bin5_b/AFIS_bin5_14.dbf
input datafile fno=00637 name=/oradata/AFIS/bin5_a/AFIS_bin5_15.dbf
input datafile fno=00638 name=/oradata/AFIS/bin5_b/AFIS_bin5_16.dbf
input datafile fno=00639 name=/oradata/AFIS/bin5_a/AFIS_bin5_17.dbf
input datafile fno=00640 name=/oradata/AFIS/bin5_b/AFIS_bin5_18.dbf
input datafile fno=00641 name=/oradata/AFIS/bin5_a/AFIS_bin5_19.dbf
input datafile fno=00642 name=/oradata/AFIS/bin5_b/AFIS_bin5_20.dbf
input datafile fno=00643 name=/oradata/AFIS/bin5_a/AFIS_bin5_21.dbf
input datafile fno=00644 name=/oradata/AFIS/bin5_b/AFIS_bin5_22.dbf
input datafile fno=00645 name=/oradata/AFIS/bin5_a/AFIS_bin5_23.dbf
input datafile fno=00646 name=/oradata/AFIS/bin5_b/AFIS_bin5_24.dbf
input datafile fno=00647 name=/oradata/AFIS/bin5_a/AFIS_bin5_25.dbf
input datafile fno=00648 name=/oradata/AFIS/bin5_b/AFIS_bin5_26.dbf
input datafile fno=00649 name=/oradata/AFIS/bin5_a/AFIS_bin5_27.dbf
input datafile fno=00650 name=/oradata/AFIS/bin5_b/AFIS_bin5_28.dbf
input datafile fno=00651 name=/oradata/AFIS/bin5_a/AFIS_bin5_29.dbf
input datafile fno=00652 name=/oradata/AFIS/bin5_b/AFIS_bin5_30.dbf
input datafile fno=00653 name=/oradata/AFIS/bin5_a/AFIS_bin5_31.dbf
input datafile fno=00654 name=/oradata/AFIS/bin5_b/AFIS_bin5_32.dbf
input datafile fno=00655 name=/oradata/AFIS/bin4_a/AFIS_bin4_1.dbf
input datafile fno=00656 name=/oradata/AFIS/bin4_b/AFIS_bin4_2.dbf
input datafile fno=00657 name=/oradata/AFIS/bin4_a/AFIS_bin4_3.dbf
input datafile fno=00658 name=/oradata/AFIS/bin4_b/AFIS_bin4_4.dbf
input datafile fno=00659 name=/oradata/AFIS/bin4_a/AFIS_bin4_5.dbf
input datafile fno=00660 name=/oradata/AFIS/bin4_b/AFIS_bin4_6.dbf
input datafile fno=00661 name=/oradata/AFIS/bin4_a/AFIS_bin4_7.dbf
input datafile fno=00662 name=/oradata/AFIS/bin4_b/AFIS_bin4_8.dbf
input datafile fno=00663 name=/oradata/AFIS/bin4_a/AFIS_bin4_9.dbf
input datafile fno=00664 name=/oradata/AFIS/bin4_b/AFIS_bin4_10.dbf
input datafile fno=00665 name=/oradata/AFIS/bin4_a/AFIS_bin4_11.dbf
input datafile fno=00666 name=/oradata/AFIS/bin4_b/AFIS_bin4_12.dbf
input datafile fno=00667 name=/oradata/AFIS/bin4_a/AFIS_bin4_13.dbf
input datafile fno=00668 name=/oradata/AFIS/bin4_b/AFIS_bin4_14.dbf
input datafile fno=00669 name=/oradata/AFIS/bin4_a/AFIS_bin4_15.dbf
input datafile fno=00670 name=/oradata/AFIS/bin4_b/AFIS_bin4_16.dbf
input datafile fno=00671 name=/oradata/AFIS/bin4_a/AFIS_bin4_17.dbf
input datafile fno=00672 name=/oradata/AFIS/bin4_b/AFIS_bin4_18.dbf
input datafile fno=00673 name=/oradata/AFIS/bin4_a/AFIS_bin4_19.dbf
input datafile fno=00674 name=/oradata/AFIS/bin4_b/AFIS_bin4_20.dbf
input datafile fno=00675 name=/oradata/AFIS/bin4_a/AFIS_bin4_21.dbf
input datafile fno=00676 name=/oradata/AFIS/bin4_b/AFIS_bin4_22.dbf
input datafile fno=00677 name=/oradata/AFIS/bin4_a/AFIS_bin4_23.dbf
input datafile fno=00678 name=/oradata/AFIS/bin4_b/AFIS_bin4_24.dbf
input datafile fno=00679 name=/oradata/AFIS/bin4_a/AFIS_bin4_25.dbf
input datafile fno=00680 name=/oradata/AFIS/bin4_b/AFIS_bin4_26.dbf
input datafile fno=00681 name=/oradata/AFIS/bin4_a/AFIS_bin4_27.dbf
input datafile fno=00682 name=/oradata/AFIS/bin4_b/AFIS_bin4_28.dbf
input datafile fno=00683 name=/oradata/AFIS/bin4_a/AFIS_bin4_29.dbf
input datafile fno=00684 name=/oradata/AFIS/bin4_b/AFIS_bin4_30.dbf
input datafile fno=00685 name=/oradata/AFIS/bin4_a/AFIS_bin4_31.dbf
input datafile fno=00686 name=/oradata/AFIS/bin4_b/AFIS_bin4_32.dbf
channel ORA_SBT_TAPE_2: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_1: finished piece 1 at 22-JUN-13
piece handle=850crctt_1_1 tag=TAG20130622T165415 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:22:34
channel ORA_SBT_TAPE_1: starting full datafile backupset
channel ORA_SBT_TAPE_1: specifying datafile(s) in backupset
```

```
input datafile fno=00004 name=/oradata/AFIS/users01.dbf
input datafile fno=00561 name=/oradata/AFIS/bin15_a/AFIS15_bin_11.dbf
input datafile fno=00562 name=/oradata/AFIS/bin15_b/AFIS15_bin_12.dbf
input datafile fno=00563 name=/oradata/AFIS/bin15_a/AFIS15_bin_13.dbf
input datafile fno=00564 name=/oradata/AFIS/bin15_b/AFIS15_bin_14.dbf
input datafile fno=00565 name=/oradata/AFIS/bin15_a/AFIS15_bin_15.dbf
input datafile fno=00566 name=/oradata/AFIS/bin15_b/AFIS15_bin_16.dbf
input datafile fno=00567 name=/oradata/AFIS/bin15_a/AFIS15_bin_17.dbf
input datafile fno=00568 name=/oradata/AFIS/bin15_b/AFIS15_bin_18.dbf
input datafile fno=00569 name=/oradata/AFIS/bin15_a/AFIS15_bin_19.dbf
input datafile fno=00570 name=/oradata/AFIS/bin15_b/AFIS15_bin_20.dbf
input datafile fno=00571 name=/oradata/AFIS/bin15_a/AFIS15_bin_21.dbf
input datafile fno=00572 name=/oradata/AFIS/bin15_b/AFIS15_bin_22.dbf
...
.
input datafile fno=00486 name=/oradata/AFIS/bin17/AFIS17_bin_16.dbf
input datafile fno=00495 name=/oradata/AFIS/bin17/AFIS17_bin_25.dbf
input datafile fno=00504 name=/oradata/AFIS/bin17/AFIS17_bin_34.dbf
input datafile fno=00513 name=/oradata/AFIS/bin16_a/AFIS16_bin_9.dbf
input datafile fno=00522 name=/oradata/AFIS/bin16_b/AFIS16_bin_18.dbf
input datafile fno=00531 name=/oradata/AFIS/bin16_a/AFIS16_bin_27.dbf
input datafile fno=00540 name=/oradata/AFIS/bin16_b/AFIS16_bin_44.dbf
input datafile fno=00549 name=/oradata/AFIS/bin16_b/AFIS16_bin_46.dbf
input datafile fno=00558 name=/oradata/AFIS/bin15_b/AFIS15_bin_8.dbf
channel ORA_SBT_TAPE_1: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_2: finished piece 1 at 22-JUN-13
piece handle=8gocrdbb_1_1 tag=TAG20130622T165415 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_2: backup set complete, elapsed time: 00:21:00
channel ORA_SBT_TAPE_1: finished piece 1 at 22-JUN-13
piece handle=8hocrdd6_1_1 tag=TAG20130622T165415 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:25:47
Finished backup at 22-JUN-13

Starting backup at 22-JUN-13
current log archived
using channel ORA_SBT_TAPE_1
using channel ORA_SBT_TAPE_2
channel ORA_SBT_TAPE_1: starting archive log backupset
channel ORA_SBT_TAPE_1: specifying archive log(s) in backup set
input archive log thread=1 sequence=101 recid=61 stamp=818787798
channel ORA_SBT_TAPE_1: starting piece 1 at 22-JUN-13
channel ORA_SBT_TAPE_1: finished piece 1 at 22-JUN-13
piece handle=8iocrdem_1_1 tag=TAG20130622T213118 comment=API Version 2.0,MMS
Version 10.4.0.3
channel ORA_SBT_TAPE_1: backup set complete, elapsed time: 00:03:26
channel ORA_SBT_TAPE_1: deleting archive log(s)
archive log filename=/oradata/AFIS/arch1/1_101_858796023.arc recid=61
stamp=818787798
Finished backup at 22-JUN-13

Starting Control File and SPFILE Autobackup at 22-JUN-13
piece handle=c-2363544759-20130622-00 comment=API Version 2.0,MMS Version
10.4.0.3
Finished Control File and SPFILE Autobackup at 22-JUN-13

RMAN>
```

Durante el proceso de copia de seguridad es posible monitorear las tareas que ejecuta el servidor OSB y saber en qué volúmenes son almacenados los respaldos. Existe una gran variedad de comandos OSB que sirven para depurar las operaciones de respaldo y recuperación, pero aquí, solo se muestran tres de los más utilizados.

```

### MOSTRAR LOS JOBS QUE SE ESTAN EJECUTANDO

ob> lsjob

```

Job ID	Sched time	Contents	State
admin/61	none	database AFIS (dbid=2363544759)	completed
admin/61.1	none	archivelog backup	completed
admin/61.2	none	archivelog backup	completed

```

### MOSTRAR INFORMACIÓN MAS DETALLADA SOBRE LOS JOBS

ob> catxcr admin/61.2

2013/06/22.16:52:57

2013/06/22.16:52:57
2013/06/22.16:52:57          Transcript for job admin/61.2 running on afisdb
2013/06/22.16:52:57
Volume label:
  Volume tag:          A00001L5
  Volume UUID:         f8089c32-bddd-1030-b231-0800270b618a
  Volume ID:           MF_ORARW2-000041
  Volume sequence:     1
  Volume set owner:    root
  Volume set created:  Sat Jun 22 16:53:05 2013
  Volume set closes:   Sat Jul 22 17:08:05 2013 (no writes after this time)
  Media family:        MF_ORARW2
  Volume set expires:  never; content manages reuse

### MOSTRAR LOS VOLUMENES EXISTENTES EN LA LIBRERÍA DE CINTAS

ob> lsvol -L LIBRARY0

Inventory of library LIBRARY0:
  in 1:          volume MF_ORARW2-000041, barcode A00001L5, 167936 kb
remaining, content manages reuse,
  in 2:          volume MF_ORARW2-000042, barcode A00002L5, 86016 kb
remaining, content manages reuse,
  in 3:          volume MF_ORARW2-000043, barcode A00003L5, 203776 kb
remaining, content manages reuse,
  in 4:          volume MF_ORARW2-000044, barcode A00004L5, 203776 kb
remaining, content manages reuse,
  in 5:          volume MF_ORARW2-000038, barcode A00005L5, 167936 kb
remaining, content manages reuse,

```

```

in 6: volume MF_ORARW2-000039, barcode A00006L5, 203776 kb
remaining, content manages reuse,
in 7: volume MF_ORARW2-000040, barcode A00007L5, 203776 kb
remaining, content manages reuse,
in 8: barcode A00008L5
in 9: barcode A00009L5
in 10: barcode A00010L5
in 11: barcode A00011L5
in 12: barcode A00012L5
in 13: barcode A00013L5
in 14: barcode A00014L5
in 15: barcode A00015L5
in 16: barcode A00016L5
in 17: barcode A00017L5
in 18: barcode A00018L5
in 19: barcode A00019L5
in 20: barcode A00020L5
in 21: barcode A00021L5
in 22: barcode A00022L5
in 23: barcode CLN023L5
ob>

```

6.2 Validación de un backup de la BD

La mayoría de las veces las copias de seguridad realizadas con RMAN cuentan con un alto grado de fiabilidad, pero también es cierto que la mayoría de las veces los administradores reutilizan las cintas magnéticas y esto provoca que las copias de seguridad dejen de ser 100% fiables. Se puede validar la integridad de un backup almacenado en cinta utilizando la sentencia `restore ... validate`.

La sentencia solamente leerá los archivos de la cinta magnética pero no realizará ninguna escritura de los datos en disco.

```

RMAN> restore database validate;

Starting restore at 23-JUN-13
using channel ORA_SBT_TAPE_1
using channel ORA_SBT_TAPE_2
using channel ORA_DISK_1

channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 86ocrctu_1_1
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 85ocrctt_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=86ocrctu_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:41:57
channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 88ocrd2o_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=85ocrctt_1_1 tag=TAG20130622T165415

```

```
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:42:58
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 87ocrd2j_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=88ocrd2o_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:40:35
channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 89ocrd4j_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=87ocrd2j_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:41:41
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 8aocrd60_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=89ocrd4j_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:52:01
channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 8bocrd6s_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=8aocrd60_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:41:56
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 8cocrd7o_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=8cocrd7o_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:45:37
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 8eocrd8p_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=8bocrd6s_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:40:40
channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 8docrd84_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=8docrd84_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:46:36
channel ORA_SBT_TAPE_1: starting validation of datafile backupset
channel ORA_SBT_TAPE_1: reading from backup piece 8gocrdbb_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=8eocrd8p_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:48:54
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 8focrdb8_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=8gocrdbb_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: validation complete, elapsed time: 00:50:51
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=8focrdb8_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:48:43
channel ORA_SBT_TAPE_2: starting validation of datafile backupset
channel ORA_SBT_TAPE_2: reading from backup piece 8hocrdd6_1_1
channel ORA_SBT_TAPE_2: restored backup piece 1
piece handle=8hocrdd6_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_2: validation complete, elapsed time: 00:40:45
Finished restore at 23-JUN-13
```

```
RMAN>
```

Nota: Se debe tener demasiado cuidado el momento de usar la sentencia `restore database validate`, hay que asegurarse de que la palabra `validate` es agregada al final de la sentencia, pues de no hacerlo, se estaría haciendo una restauración completa de la base de datos, lo que implica que los datos leídos de la cinta realmente sean escritos a disco.

6.3 Restauración y validación de un datafile

Dentro de las fallas más comunes ocurridas en una BD Oracle se encuentra el daño de los archivos de datos (datafiles), este tipo de errores se puede solucionar de manera muy sencilla usando RMAN y OSB. Prácticamente la validación de un datafile (antes de que sea restaurado) se puede realizar de la misma forma en que se valida toda una BD. Usando el comando `restore ... validate`.

Debido a que en la sección anterior ya se mostró el uso de la sentencia `restore ... validate`, en este ejemplo se aprovechará el tiempo que tarda en ser restaurado un datafile para mostrar otra forma de validar los archivos de una BD. Esta forma de validación consiste en escribir realmente los datos en disco, por lo que realmente se estaría llevando a cabo la restauración de los datos.

Los pasos a seguir para realizar una restauración y recuperación de un datafile son los siguientes:

1. Poner el datafile dañado en modo fuera de línea.

```
RMAN> sql "alter database datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf'
offline";

sql statement: alter database datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf'
offline
```

2. Restaurar el datafile dañado.

```
RMAN> restore datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf';

Starting restore at 23-JUN-13
allocated channel: ORA_SBT_TAPE_1
channel ORA_SBT_TAPE_1: sid=157 devtype=SBT_TAPE
channel ORA_SBT_TAPE_1: Oracle Secure Backup
```

```
allocated channel: ORA_SBT_TAPE_2
channel ORA_SBT_TAPE_2: sid=155 devtype=SBT_TAPE
channel ORA_SBT_TAPE_2: Oracle Secure Backup
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=154 devtype=DISK

channel ORA_SBT_TAPE_1: starting datafile backupset restore
channel ORA_SBT_TAPE_1: specifying datafile(s) to restore from backup set
restoring datafile 00479 to /oradata/AFIS/bin17/AFIS17_bin_9.dbf
channel ORA_SBT_TAPE_1: reading from backup piece 8aocrd60_1_1
channel ORA_SBT_TAPE_1: restored backup piece 1
piece handle=8aocrd60_1_1 tag=TAG20130622T165415
channel ORA_SBT_TAPE_1: restore complete, elapsed time: 00:15:35
Finished restore at 23-JUN-13
```

3. Recuperar el datafile dañado, esta sentencia aplica los últimos cambios ocurridos desde que el datafile fue respaldado.

```
RMAN> recover datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf';

Starting recover at 23-JUN-13
using channel ORA_SBT_TAPE_1
using channel ORA_SBT_TAPE_2
using channel ORA_DISK_1

starting media recovery
media recovery complete, elapsed time: 00:01:03

Finished recover at 23-JUN-13
```

4. Poner nuevamente el datafile en línea.

```
RMAN> sql "alter database datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf''
online";

sql statement: alter database datafile '/oradata/AFIS/bin17/AFIS17_bin_9.dbf'
online
```

Nótese que en el paso 2 de este ejemplo realmente se está haciendo la restauración del datafile dañado, pues al omitir la sentencia `validate` (al final de la línea) RMAN escribe los datos leídos de la cinta magnética a disco.

CONCLUSIONES

La mejor forma de proteger la información de una empresa, sin importar las dimensiones de la organización, es implementar un buen plan de recuperación de desastres. El plan debe incluir un sistema de respaldo y recuperación que permita mantener los datos a salvo sin interrumpir la continuidad del negocio.

En el presente trabajo, se mostraron los diversos mecanismos utilizados para respaldar bases de datos Oracle, y aunque faltó profundizar un poco en los mecanismos de recuperación, no por ello deberían considerarse menos importantes. Exponer todos los mecanismos de recuperación de una base de datos es una tarea ardua y sería necesario desarrollar un trabajo de igual o mayor extensión al aquí presentado.

Si bien es cierto que el objetivo principal del presente proyecto era únicamente implementar un sistema de copias de seguridad “Online” de bases de datos Oracle, durante el desarrollo del proyecto, se descubrió que el presente trabajo también puede servir como base para proyectos que pretendan implementar o estudiar un plan de recuperación de BD Oracle. Puesto que para diseñar un buen plan de recuperación, es necesario conocer a profundidad la arquitectura del motor de BD y los mecanismos de respaldo.

De lo anterior, se concluye que la implementación de un sistema de respaldos no es el único factor a tomar en cuenta al momento de proteger los datos. Si bien es importante contar con una copia de los datos, es mucho más importante contar con un plan de recuperación de desastres, que contemple la validación de dichas copias de seguridad y garantice la recuperación de la información ante cualquier posible incidente. No serviría de nada contar con una copia de la información, si no se sabe de antemano que la copia de seguridad almacena datos consistentes y por lo menos han sido validados en una ocasión.

Es importante mencionar que un plan de recuperación de desastres debe tomar en cuenta todos los factores que afectan e interactúan con la información, desde los recursos de hardware e infraestructura física, hasta el personal que se encargará de poner en práctica los procesos del plan de recuperación.

No todas las empresas son capaces de solventar económicamente un plan de recuperación de desastres integral, pero debería de tomarse en cuenta que hay veces que resulta más costoso recuperar el trabajo de meses o años invertidos en un sistema, que costear un plan de recuperación. En el peor de los casos, si una empresa u organización no cuenta con los recursos suficientes, siempre será mejor tratar de salvaguardar los sistemas más delicados y propensos a fallas, o aquellos que tratan y almacenan información difícil de recuperar.

En el mundo de la informática hay multitud de sistemas que pueden ser utilizados para proteger la información, usar uno u otro depende de los requerimientos de operación del negocio, de que tanto se valore la información con la que se trabaja, y sobre todo, del presupuesto destinado al plan de recuperación de desastres. El cuidado de la información de un sistema debería de verse como una inversión, que puede rendir frutos a corto o largo plazo.

En el caso particular de la SIIM IFE, los beneficios obtenidos por la implantación del sistema OSB fueron: la eliminación de indisponibilidad en la BD, el ahorro de espacio en cintas magnéticas, la automatización del proceso de respaldo, una mejoría en el tiempo empleado para hacer el backup, y finalmente, el ahorro de los recursos humanos -horas hombre- encargados de ejecutar las copias de seguridad de forma manual.

BIBLIOGRAFÍA

- [1] Fernandez, Iggy, *Beginning Oracle Database 11g Administration : From Novice to Professional*, Apress, New York 2009.
 - [2] Freeman, Robert G., and Matthew Hart, *Oracle Rman 11g : Backup and Recovery*, Oracle Press/McGraw-Hill, New York 2010.
 - [3] Greenwald, Rick, Robert Stackowiak, and Jonathan Stern, *Oracle Essentials : Oracle Database 11g*, 4th ed., O'Reilly, Sebastopol California 2008.
 - [4] Hart, Matthew, and Robert G. Freeman, *Oracle Database 10g Rman Backup & Recovery*, McGraw-Hill, New York 2007.
 - [5] Jesse, Scott, William Burton, and Bryan Vongray, *Oracle Database 11g Release 2 High Availability : Maximize Your Availability with Grid Infrastructure, Oracle Real Application Clusters, and Oracle Data Guard*, 2nd ed., McGraw-Hill, New York 2011.
 - [6] Kuhn, Darl, Sam R. Alapati, and Arup Nanda, *Rman Recipes for Oracle Database 11g : A Problem-Solution Approach*, Apress, New York, 2007.
 - [7] Kuhn, Darl, and Scott Schulze, *Oracle Rman : Pocket Reference*, 1st ed., O'Reilly, Sebastopol California 2002.
 - [8] Kyte, Thomas, *Effective Oracle by Design*, McGraw-Hill/Osborne, New York 2003.
 - [9] Kyte, Thomas, *Expert Oracle Database Architecture : 9i and 10g Programming Techniques and Solutions*, Apress, New York 2005.
 - [10] Lewis, Jonathan, *Oracle Core : Essential Internals for Dbas and Developers*, Apress, New York 2011.
-

- [11] Loney, Kevin, *Oracle Database 10g : The Complete Reference*, McGraw-Hill/Osborne, Emeryville California 2004.

 - [12] Loney, Kevin, Bob Bryla, and TUSC (Firm), *Oracle Database 10g : DbA Handbook*, McGraw-Hill/Osborne, New York 2005.

 - [13] Niemiec, Richard J., *Oracle Database 10g Performance Tuning : Tips & Techniques*, McGraw-Hill, New York 2007.
-

MESOGRAFÍA

- [1] IBM Corporation, *AIX 5.3 Installation and migration*, [Fecha de consulta: 5 de Septiembre de 2014], disponible en: http://www-01.ibm.com/support/knowledgecenter/ssw_aix_53/com.ibm.aix.install/doc/insgdrf/insgdrf-kickoff.htm?lang=en

 - [2] Oracle Corporation, *Oracle Database Backup and Recovery Advanced User's Guide 10g Release 2 (10.2)*, [Fecha de consulta: 10 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/B19306_01/backup.102/b14191/toc.htm

 - [3] Oracle Corporation, *Oracle Database Backup and Recovery Basics 10g Release 2 (10.2)*, [Fecha de consulta: 10 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/B19306_01/backup.102/b14192/toc.htm

 - [4] Oracle Corporation, *Oracle Database Backup and Recovery Quick Start Guide 10g Release 2 (10.2)*, [Fecha de consulta: 10 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/B19306_01/backup.102/b14193/toc.htm

 - [5] Oracle Corporation, *Oracle Database Backup and Recovery Reference 10g Release 2 (10.2)*, [Fecha de consulta: 10 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/B19306_01/backup.102/b14194/toc.htm

 - [6] Oracle Corporation, *Oracle Database Installation Guide 10g Release 2 (10.2) for AIX 5L Based Systems (64-Bit)*, [Fecha de consulta: 5 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/B19306_01/install.102/b19075/toc.htm

 - [7] Oracle Corporation, *Oracle Secure Backup Administrator's Guide Release 10.4*, [Fecha de consulta: 17 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/E26569_01/doc.104/e21476/toc.htm
-

- [8] Oracle Corporation, *Oracle Secure Backup Installation and Configuration Guide Release 10.4*, [Fecha de consulta: 17 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/E26569_01/doc.104/e21477/toc.htm

 - [9] Oracle Corporation, *Oracle Secure Backup Reference Release 10.4*, [Fecha de consulta: 17 de Septiembre de 2014], disponible en: http://docs.oracle.com/cd/E26569_01/doc.104/e21480/toc.htm

 - [10] Vegas, Jesús, *ORACLE: Arquitectura*, [Fecha de consulta: 27 de Agosto de 2014], disponible en: <http://www.infor.uva.es/~jvegas/cursos/bd/orarq/orarq.html>

 - [11] Wikipedia, La enciclopedia libre, *RAID*, [Fecha de consulta: 27 de Agosto de 2014], disponible en: <http://es.wikipedia.org/wiki/RAID>
-